VE AdminHelp v9.6

Table of Contents

Welcome 1
Attributions, Copyrights, and Trademarks 1
About the Online Help System 13
Get Started 15
Dashboard 15
Get Started with Dell Data Protection 17
Navigation 17
Dashboard 18
Populations 18
Compliance Reporter 18
Management 18
Change the Superadmin Password 18
Components 19
Default Port Values 19
Remote Management Console 19
Proxy Servers 19
Types of Proxy Servers 20
Policy Proxy 20
Time Slotting 20
Polling 20
Poll Triggers 20
Failed Poll Attempts 21
General Information 21
Navigate the DDP Server 23
Navigation 23
Dashboard 23
Populations 23
Compliance Reporter 23
Management 23
Masthead icons 23
Disconnected Mode 23
Client Activation 23

Remote Management Console 24
Functionality 24
Dashboard 24
Dashboard 24
Notifications List 27
Notification Types 27
Priority Levels 28
Endpoint Protection Status 28
Protection Status 28
Threat Protection Status 29
Threat Protection Status for Severity Level 29
Advanced Threat Prevention Events 29
Advanced Threats by Priority 30
Advanced Threat Prevention Classifications 31
Advanced Threats Top Ten 32
Endpoint Protection History 32
Endpoint Inventory History 32
Summary Statistics 32
Endpoint OS Report 33
Platform Report 33
Populations 33
Populations 34
Enterprise 34
View or Modify Enterprise-Level Policies 34
View Threat Events 34
Manage Enterprise Advanced Threats 35
Advanced Threats tab 35
Advanced Threat Events tab 35
Domains 35
Domains 36
Add a Domain 36
Users 36
Add a User to a Domain 36
User Groups 37

Add a User Group....37
Add Non-Domain Users....37
View or Modify Domain Policies and Information....37
Domain Details & Actions....38
Domain Members....38
Domain Settings....39
Domain Key Server....39
User Groups....40
User Groups....40
Add a User Group....40
Remove User Groups....40
Find User Groups....40
View or Modify User Group Policies and Information....41
User Group Details & Actions....41
User Group Members....42
User Group Admin....42
Modify Group Precedence....42
Assign or Modify Administrator Roles....43
View Reconciliation Date....43
View Policy Proxy State....43
Users....44
Users....44
Add a User to a Domain....44
Remove Users....44
Find Users....45
Deactivate/Suspend Users....45
Reinstate Suspended Users....45
View or Modify User Policies and Information....46
VDI User Policies....46
Policy and Configuration Requirements for VDI Users....47
User Details & Actions....47
User Endpoints....48
User Groups....49
User Admin....49

View Reconciliation Date 49
View Policy Proxy State 49
Issue a User Decryption Policy 50
Endpoint Groups 50
Endpoint Groups 50
Types of Endpoint Groups 50
Add an Endpoint Group 50
Endpoint Groups Specification 51
Endpoint Group Specification 51
Operators and Expressions 52
Summary 53
Examples 53
Modify Group Precedence 54
View Endpoints in an Endpoint Group 54
View or Modify Endpoint Group Policies and Information 55
Endpoint Group Details & Actions 55
Endpoint Group Members 55
Endpoints 56
Endpoints 56
Add Endpoints 56
Remove Endpoints 56
Find Endpoints 56
View or Modify Endpoint Policies and Information 56
View Effective Policy 57
Endpoint Details & Actions 58
Endpoint Detail 58
Shield Detail 59
Manager Detail (Windows only) 62
States 62
Threat Protection Detail (Windows only) 64
Advanced Threat Prevention Detail 64
Mobile Device Detail 64
Cloud Device Control 64
SED Device Control (Windows only) 65

Endpoint Users 65
Shielded 65
Cloud 66
Endpoint Groups 66
VDI Endpoint Groups 66
Policy and Configuration Requirements for VDI Endpoint Groups 66
Endpoint Threat Events 67
Endpoint Advanced Threats 68
List of Events 68
Configure the Threat List 69
Export 69
Quarantine 69
Waive 69
Exploit Attempts 69
Endpoint Advanced Threat Events 70
Server Encryption Clients 71
Suspend a Server Encryption Client 71
Reinstate a Suspended Server Encryption Client 71
Commands for Self-Encrypting Drives 71
Priority of Commands for Self-Encrypting Drives 71
Allow PBA Login Bypass 72
Unlock a Self-Encrypting Drive 72
Remove Users from Endpoint with Self-Encrypting Drive 73
Lock a Self-Encrypting Drive 73
Send Wipe Command to Self-Encrypting Drive 73
Administrators 74
Assign or Modify Administrator Roles 74
Administrator Roles 74
Delegate Administrator Rights 77
Compliance Reporter 78
View Audit Events (Geolocation) 78
Event Data 79
Export Events to a SIEM/Syslog Server 79
Management 79

Commit Policies 79
Log Analyzer 80
Recovery 80
Recover Data - EMS Authentication Failure 80
Recover Data - BitLocker Manager 83
SED Recovery 83
SED Authentication Failure 83
SED Endpoint Recovery 83
Recover Endpoint 84
Windows Recovery 84
SED Recovery 84
EMS Recovery 84
Mac Recovery 84
License Management 84
License Management 84
Upload Client Access Licenses 84
View or Add License Notifications 85
CAL Information 85
Licensing 85
Dropbox Management 88
Remove a Dropbox for Business User 88
Advanced Threat Prevention Services Management 88
Product Notifications 89
Receive product notifications 89
Stop receiving product notifications 89
Alerts Management 89
Notification Management 89
Configure SMTP Settings 89
External User Management 90
Change the Superadmin Password 91
Manage Policies 93
Manage Security Policies 93
Windows Encryption 94
Variables 103

%CSIDL:name% 103
%HKCU:regpath% 105
%HKLM:regpath% 105
%ENV:envname% 105
%% 105
Windows Policies that Require Reboot 105
Windows Policies that Require Logoff 105
Advanced Windows Encryption 105
Variables 137
%CSIDL:name% 137
%HKCU:regpath% 139
%HKLM:regpath% 139
%ENV:envname% 139
%% 139
Windows Policies that Require Reboot 139
Windows Policies that Require Logoff 139
Authentication 139
Advanced Authentication 140
Threat Prevention 143
Advanced Threat Prevention 146
Client Firewall Settings and Rules 168
Client Firewall Options 169
Client Firewall Rules 171
Secure Lifecycle 174
Advanced Secure Lifecycle 177
Set Cover Page Policies 184
Removable Media Encryption 184
Removable Media Policies that Require Logoff 187
Advanced Removable Media Encryption 187
Removable Media Policies that Require Logoff 196
Mobile Protection 196
Advanced Mobile Protection 197
Mac Encryption 202
Advanced Mac Encryption 204

Port Control 205
Advanced Port Control 206
Global Settings 207
Referenced Topics 211
Advanced Threat Events tab fields and filters 211
Temporarily Block Activations 211
Cloud Profile Update 212
Set the Server Connection Retry Interval 212
Advanced Threat Prevention Classifications 212
Remove System Data Encryption (SDE) 212
Designate a Threat Protection Signature Update Server 212
Disconnected Mode Policy Examples 213
Global Allow policy example 213
Quarantine List and Safe List policy example 216
Enable Compatibility Mode for Memory Protection 217
Encryption Rules 218
Protected Directories 218
Modifiers – What they are and what they do 220
Using the Override Modifier 220
Encrypting/Not Encrypting Extensions 221
Examples of extension inclusions/exclusion 221
Encrypting/Not Encrypting Directories 221
Examples of folder inclusion/exclusion 221
Sub-directories and Precedence of Directives 222
Example of sub-directories 222
Example 1 of competing directives: 222
Example 2 of competing directives: 222
Example 3 of competing directives: 222
Environment Variables, KNOWNFOLDERID constants, and CSIDL 223
Application Data Encryption (ADE) 224
Example Policies for Common/User Key Encryption 224
System Data Encryption (SDE) 225
Policies for SDE Encryption 225
Notes 230

Protection of SystemRoot 230
External Media Shield (EMS) 230
What Happens When Policies Tie 230
Generic Drive Statements 230
Enroll for Advanced Threat Prevention Agent Auto Updates 231
Receive agent auto updates 231
Stop receiving agent auto updates 231
Export Secure Lifecycle Audit Events to a SIEM Server 231
Localizable Policies 232
Localize Policies Displayed on the Endpoint Computer 233
Log In 234
Log Out 235
Manage Enterprise Advanced Threats - Agents 235
Manage Enterprise Advanced Threats - Certificate 235
Manage Enterprise Advanced Threats - Cylance Score and Threat Model Updates 236
Threat Model Updates 236
Manage Enterprise Advanced Threats - Global List 237
Global Quarantine 237
Safe 238
Unassigned 239
Manage Enterprise Advanced Threats - Options 240
Manage Enterprise Advanced Threats - Protection 240
Threats 240
File Details 242
Script Control Table 243
Persistent vs. Non-Persistent VDI 243
Policies Set by Application Control 243
Advanced Authentication 244
Advanced Mac Encryption 247
Advanced Mobile Protection 247
Advanced Port Control 253
Advanced Removable Media Encryption 254
Removable Media Policies that Require Logoff 262
Advanced Secure Lifecycle 263

Set Cover Page Policies 269
Advanced Windows Encryption 270
Variables 301
%CSIDL:name% 301
%HKCU:regpath% 303
%HKLM:regpath% 303
%ENV:envname% 303
%% 303
Windows Policies that Require Reboot 303
Windows Policies that Require Logoff 304
Advanced Threat Prevention 304
Client Firewall Settings and Rules 326
Client Firewall Options 326
Client Firewall Rules 328
Notifications List 332
Protected 334
Provision Advanced Threat Prevention Service 336
Provision service 336
Recover service 336
Remove HCA-Based Encryption 336
Secure Lifecycle Audit Events 336
Map visualization 336
Columns and filters 337
Options in the Columns dropdown 338
Examples of Map Visualization and Column Filters 338
Example of drilling in at the map level 339
Cloud Encryption audit events 339
Protected Office Document audit events 339
Set Policies to Protect Office Documents in Mac 340
Set Protected Office Document Policies 340
Set Policies to Protect Office Documents in Mobile Devices 340
Set Protected Office Document Policies 340
Set Policies to Protect Office Documents in Windows 341
Set Policies for Protected Office Documents 341

Determine Impact on Windows Users for Opt-in or Force Protected Modes 342
Enable Both Cloud Encryption and Protected Office Documents 344
Suspend Users 344
Syslog Event Types 345
Syslog IP Addresses 348
Threat Protection Policy Overview 348
Client Options Policies 348
Client Firewall Policies 349
Client Firewall options 349
Client Firewall rules 349
Malware Protection Policies 349
Types of Malware Protection 349
Configurable Actions - After Threat is Detected 350
Reputation Service Sensitivity policies 351
Web Protection Policies 351
Threat Data Report 352
Export Data 352
Upload Client Access Licenses 352

Welcome

Attributions, Copyrights, and Trademarks

Dell Data Protection | Encryption is a trademark of Dell Inc.

Protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

The software described in this help system is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Third Party Software

I. OpenSSL License - Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

A. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

B. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

C. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)".

D. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

E. Products derived from this software may not be called "OpenSSL" * nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

F. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)" THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

a. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

c. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

d. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)" THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.].

II. Portions of this product use Commons IO, Commons DBCP, and Commons LANG. You may obtain a copy of the licenses at http://www.apache.org/licenses/LICENSE-2.0.

III. Portions of this product use OrientDB. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

IV. Portions of this product use Apache Wink. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

V. Portions of this product use Jackson JSON. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

VI. Portions of this product use Jetty. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

VII. Portions of this product use ActiveMQ. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

VIII. Portions of this product use jasypt. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

IX. Portions of this product make use of zlib. You may obtain a copy of the license at http://www.zlib.net/zlib_license.html.

/* zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.7, May 2nd, 2012 Copyright (C) 1995-2012 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

A. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

B. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

C. This notice may not be removed or altered from any source distribution. Jean-loup Gailly Mark Adler jloup@gzip.org madler@alumni.caltech.edu.

X. Portions of this product make use of Apache Tomcat (www.apache.org). You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XI. Portions of this product make use of Apache Commons HTTPClient. You may obtain a copy of the license at http://opensource.org/licenses/apache2.0.

XII. Portions of this product make use of log4net. You may obtain a copy of the license at http://logging.apache.org/log4net/license.html.

XIII. Portions of this product make use of MVVM Light Toolkit. You may obtain a copy of the license at http://mvvmlight.codeplex.com/license.

XIV. Portions of this product make use of Apache JDBCLog, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XV. Portions of this product make use of Apache Log4J, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XVI. Portions of this product make use of Apache Struts, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XVII. Portions of this product make use of Struts2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XVIII. Portions of this product make use of Struts Beanutils, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XIX. Portions of this product make use of Struts Digester, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XX. Portions of this product make use of Apache xmlrpc, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XXI. Portions of this product make use of Bean Scripting Framework (http://commons.apache.org/bsf/), Apache License, Version 2.0, January 2004 http://commons.apache.org/license.html.

XXII. Portions of this product make use of Apache Commons CLI (http://commons.apache.org/cli/), Apache License, Version 2.0, January 2004 http://commons.apache.org/license.html.

XXIII. Portions of this product make use of Apache Commons EL (http://commons.apache.org/el/), Apache License, Version 2.0, January 2004 http://commons.apache.org/license.html.

XXIV. Portions of this product make use of Groovy. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.html.

XXV. Portions of this product make use of H2. You may obtain a copy of the license at http://www.h2database.com/html/license.html.

XXVI. Portions of this product make use of Spring.net Application Framework. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.html.

XXVII. Portions of this product make use of Java Service Wrapper (http://www.tanukisoftware.com/en/index.php). You may obtain a copy of the license at http://wrapper.tanukisoftware.com/doc/english/licenseOverview.html.

XXVIII. Portions of this product make use of Xalan. You may obtain a copy of the license at http://xml.apache.org/xalan-j/.

XXIX. Portions of this product make use of FreeMarker. You may obtain a copy of the license at http://freemarker.sourceforge.net/docs/app_license.html.

XXX. Portions of this product make use of Velocity. You may obtain a copy of the license at http://velocity.apache.org/.

XXXI. Portions of this product make use of MSV. You may obtain a copy of the license at http://opensource.org/licenses/apache2.0.

XXXII. Portions of this product make use of FLIB. You may obtain a copy of the license at http://opensource.org/licenses/artistic-license.html.

XXXIII. Portions of this product makes use of libraries developed by Boost (http://www.boost.org/users/license.html), under the following license: Boost Software License - Version 1.0 - August 17th, 2003.

XXXIV. Portions of this product make use of ANTLR. You may obtain a copy of the license at http://antlr.org/license.html.

XXXV. Portions of this product make use of BIRT. You may obtain a copy of the license at http://www.eclipse.org/org/documents/epl-v10.php.

XXXVI. Portions of this product make use of the getopt function, Copyright © 1987-2002 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

A. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

B. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

C. Neither the names of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

XXXVII. Portions of this product make use of the SHA-2 algorithm, Copyright © 2002, Dr. Brian Gladman (brg@gladman.me.uk), Worcester, UK. All rights reserved.

A. LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. Distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;

2. Distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;

3. The copyright holder's name is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided "as is" with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

XXXVIII. Portions of this product make use of STLport. A copy of the license may be obtained at http://www.stlport.org/doc/license.html.

A. License Agreement:

Boris Fomitchev grants Licensee a non-exclusive, non-transferable, royalty-free license to use STLport and its documentation without fee.

By downloading, using, or copying STLport or any portion thereof, Licensee agrees to abide by the intellectual property laws and all other applicable laws of the United States of America, and to all of the terms and conditions of this Agreement.

Licensee shall maintain the following copyright and permission notices on STLport sources and its documentation unchanged:

Copyright 1999,2000 Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

The Licensee may distribute binaries compiled with STLport (whether original or modified) without any royalties or restrictions.

The Licensee may distribute original or modified STLport sources, provided that:

- The conditions indicated in the above permission notice are met;
- The following copyright notices are retained when present, and conditions provided in accompanying permission notices are met :

Copyright 1994 Hewlett-Packard Company - Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright

notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1996,97 Silicon Graphics Computer Systems, Inc. - Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1997 Moscow Center for SPARC Technology - Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Moscow Center for SPARC Technology makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

XXXIX. Portions of this product make use of The Legion of Bouncy Castle Software. Copyright (c) 2000 - 2016 The Legion Of The Bouncy Castle. You may obtain a copy of the license at http://www.bouncycastle.org/licence.html.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Note: Our license is an adaptation of the MIT X11 License and should be read as such.

License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

XL. Portions of this product make use of ResizableLib. You may obtain a copy of the license at http://opensource.org/licenses/artistic-license-1.0.

XLI. Portions of this product make use of Spring Framework. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XLII. Portions of this product use $File:

A. LEGAL NOTICE,v 1.15 2006/05/03 18:48:33 christos Exp $. Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995. Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas. This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

XLIII. Portions of this product use UFSD – Paragon NTFS for Windows Driver based on Paragon Universal File System Driver (UFSD) Technology. Copyright (C) 2008 Paragon Technologie GmbH. All rights reserved. This software is provided 'as-is', without any express or implied warranty.

XLIV. Portions of this product use JDBC drivers - licensed from DataDirect Technologies.

XLV. Portions of this product make use of DIMime, available at http://www.zeitungsjunge.de/delphi/mime/.

XLVI. Portions of this product make use of RSA Security Inc. PKCS #11 Crypto Token Interface (Cryptoki).

XLVII. This software uses following 3'rd party libraries:

1. urwid

Copyright (C) 2004-2012 Ian Ward

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

1. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

"Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

   You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

   If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

   a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

   b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

   The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

   a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

   b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

   You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

   a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

   b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

XLVIII. Portions of this product use DropNet. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XLIX. Portions of this product use Hardcodet WPF NotifyIcon 1.0.8. You may obtain a copy of the license at http://www.codeproject.com/info/cpol10.aspx.

L. Portions of this product use MahApps.Metro 1.2.4.0. You may obtain a copy of the license at http://opensource.org/licenses/ms-pl.

LI. Portions of this product use Microsoft Practices Enterprise Library 6.0.1304.0. You may obtain a copy of the license at http://opensource.org/licenses/ms-pl.

LII. Portions of this product use Microsoft Practices Prism 4.1. You may obtain a copy of the license at http://opensource.org/licenses/ms-pl.

LIII. Portions of this product use Microsoft Practices Unity 2.1. You may obtain a copy of the license at http://opensource.org/licenses/ms-pl.

LIV. Portions of this product use RestSharp 105.2.3. You may obtain a copy of the license at https://github.com/restsharp/RestSharp/blob/master/LICENSE.txt.

LV. Portions of this product use System.Data.SQLite 1.0.102.0. You may obtain a copy of the copyright statement at http://www.sqlite.org/copyright.html.

LVI. Portions of this product use android-passwordsafe 0.6.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LVII. Portions of this product use Dropbox.NET 3.4.0. You may obtain a copy of the license at https://github.com/dropbox/dropbox-sdk-dotnet/blob/master/LICENSE.

LVIII. Portions of this product use Newtonsoft JSON 9.0.1. You may obtain a copy of the license at https://raw.githubusercontent.com/JamesNK/Newtonsoft.Json/master/LICENSE.md.

LIX. Portions of this product use NT Security Classes for .NET. You may obtain a copy of the license at http://www.codeproject.com/info/cpol10.aspx.

LX. Portions of this product use Prism Core 6.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXI. System.IdentityModel.Tokens.Jwt 4.0.2. You may obtain a copy of the license at https://github.com/AzureAD/azure-activedirectory-identitymodel-extensions-for-dotnet/blob/master/LICENSE.txt.

LXII. Portions of this product use Unity 4.0.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXIII. Portions of this product use the Dropbox Android SDK 1.6.3. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXIV. Portions of this product use the Dropbox json_simple-1.1.jar. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXV. Portions of this product use the Box Android Library V2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXVI. Portions of this product use the Box Java Library V2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXVII. Portions of this product use Apache HttpClient Cache 4.2.5. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXVIII. Portions of this product use Apache HttpClient 4.2.5. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXIX. Portions of this product use Apache HttpCore 4.2.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXX. Portions of this product use Apache HttpClient Mime 4.2.5. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXI. Portions of this product use Apache Commons IO 2.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXII. Portions of this product use Apache Commons Lang 2.6. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXIII. Portions of this product use JUnit 4.11. You may obtain a copy of the license at https://www.eclipse.org/legal/epl-v10.html.

LXXIV. Portions of this product use EasyMock 3.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXV. Portions of this product use Jackson Databind 2.4.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXVI. Portions of this product use Jackson Core 2.4.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXVII. Portions of this product use Jackson Annotations 2.4.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXVIII. Portions of this product use Apache Maven Wagon 2.2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXIX. Portions of this product use Scribe OAuth Library 1.3.0. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXXX. Portions of this product use JSON Web Token Support for the JVM 0.6.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXI. Portions of this product use OneDrive SDK Android 1.2.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXXXII. Portions of this product use Microsoft Services MSA Auth 0.8.4. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXXXIII. Portions of this product use Adal 1.1.7. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXIV. Portions of this product use Google API Client Library for Java with Android Platform Extensions and GSON Extensions 1.20.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXV. Portions of this product use Google Drive API V3 Rev 170 1.22.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXVI. Portions of this product use Backport Util Concurrent 3.1. You may obtain a copy of the license at https://creativecommons.org/publicdomain/zero/1.0.

LXXXVII. Portions of this product use Apache Commons Logging 1.1.3. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXVIII. Portions of this product use Flurry Analytics 4.1.0. You may obtain a copy of the license at https://developer.yahoo.com/flurry/legal-privacy/terms-service/flurry-analytics-terms-service.html.

LXXXIX. Portions of this product use kSOAP2 3.4.0. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XC. Portions of this product use FindBugs Jsr305. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCI. Portions of this product use Google Gson 2.3.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCII. Portions of this product use Hockey SDK 3.0.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XCIII. Portions of this product use Picasso 2.5.2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCIV. Portions of this product use Circular Floating Action Menu Library 1.0.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XCV. Portions of this product use Apache Commons Codec 1.8. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCVI. Portions of this product use Apache Commons Compress 1.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCVII. Portions of this product use One Password App Extension 1.8. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XCVIII. Portions of this product use Azure Active Directory Authentication Library 1.2.9. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XCIX. Portions of this product use AF Networking 2.6.3. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

C. Portions of this product use Box iOS SDK 1.0.11. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CI. Portions of this product use CT Assets Picker Controller 2.9.5. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CII. Portions of this product use Google API Objective C Client 1.0.422. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CIII. Portions of this product use Google GTM HTTP Fetcher 1.0.141. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CIV. Portions of this product use Google GTM OAuth 2 1.0.126. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CV. Portions of this product use Hockey SDK iOS 3.8.6. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CVI. Portions of this product use libextobjc 0.4.1. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CVII. Portions of this product use libPhoneNumber iOS 0.8.11. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CVIII. Portions of this product use MBProgressHUD 0.9.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CIX. Portions of this product use NSData Base64 1.0.0. You may obtain a copy of the license at http://opensource.org/licenses/Zlib.

CX. Portions of this product use OneDrive SDK iOS 1.1.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXI. Portions of this product use RNCryptor 3.0.1. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXII. Portions of this product use SSZipArchive 1.1. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXIII. Portions of this product use SVProgressHUD 2.0.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXIV. Portions of this product use WEPopover 1.0.0. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXV. Portions of this product use XMLDictionary. You may obtain a copy of the license at http://opensource.org/licenses/Zlib.

CXVI. Portions of this product use NHNetworkTime 1.7. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CXVII. Portions of this product use the Dropbox iOS SDK. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXVIII. Portions of this product use Flurry iOS SDK 5.3.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

Trademarks

iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano® are trademarks of Apple Inc., registered in the U.S. and other countries.

Android and the Android Logo are trademarks or registered trademarks of Google, Inc. in the United States and other countries.

About the Online Help System

Version: **9.6**

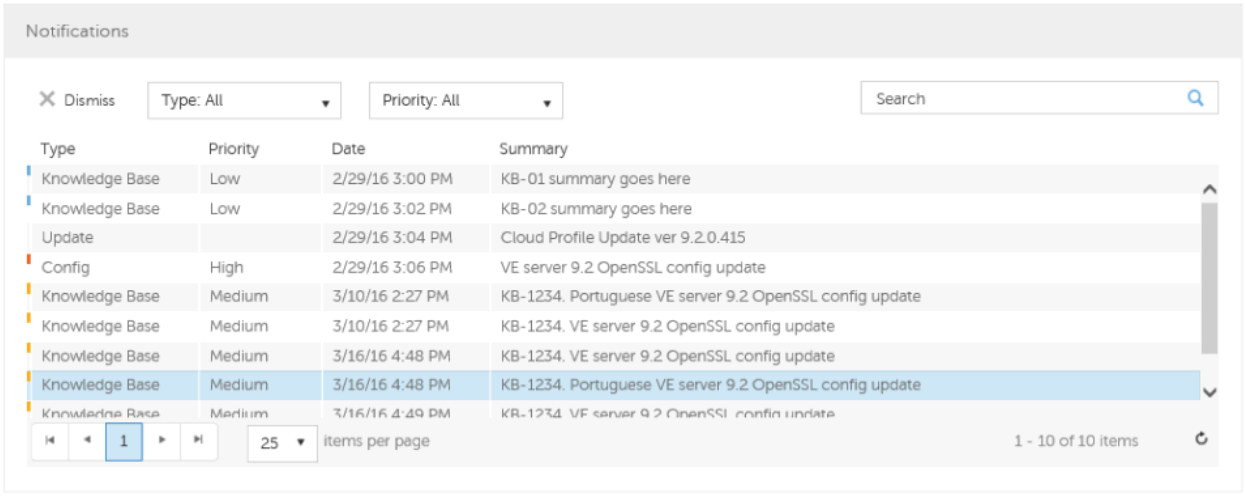
Get Started

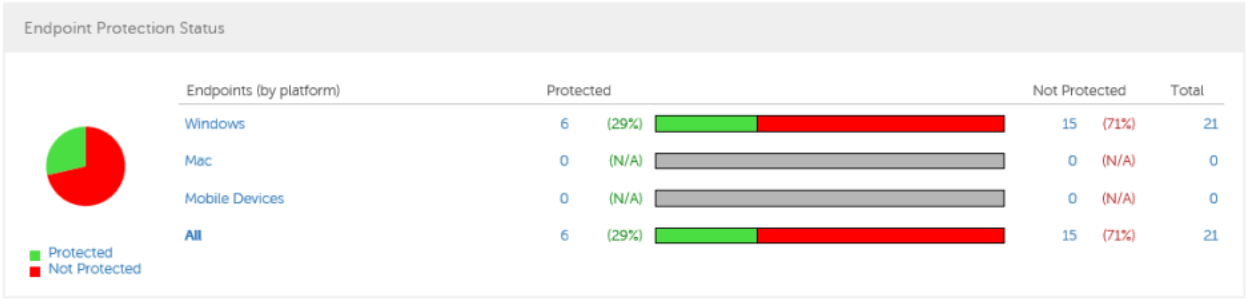
Dashboard

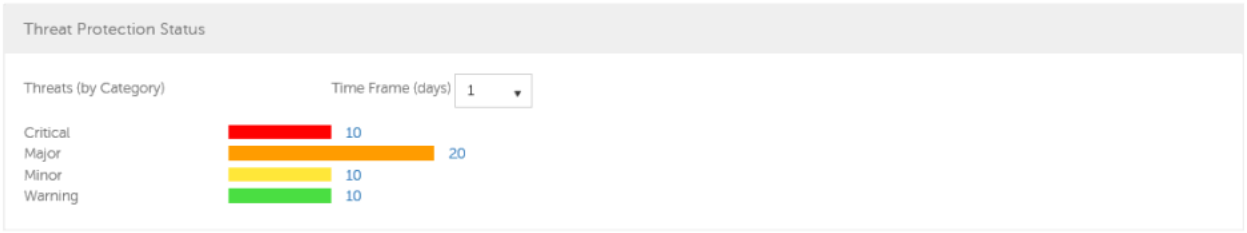
The Dashboard displays an overview of status information for your enterprise. You can access more detailed information directly from the Dashboard by clicking its statistics, graphs, and chart legends.

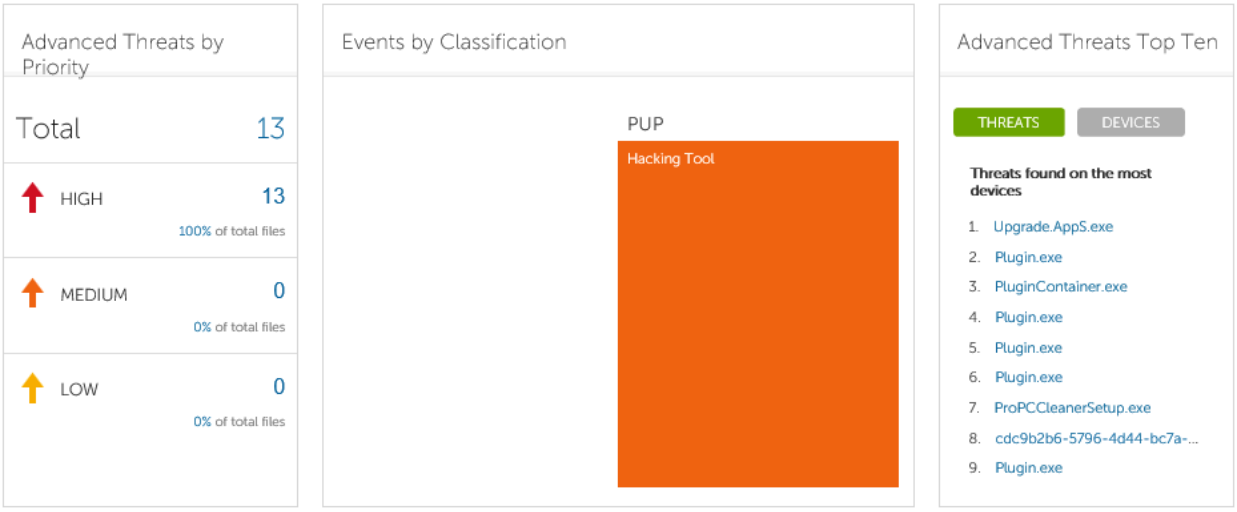
The images below reflect what you may see in the Dashboard. Content may vary based on the features installed and enabled on your Dell Data Protection Server and endpoints.

Click an area below to view a description of the detail you can access by clicking the same area in your Dashboard.

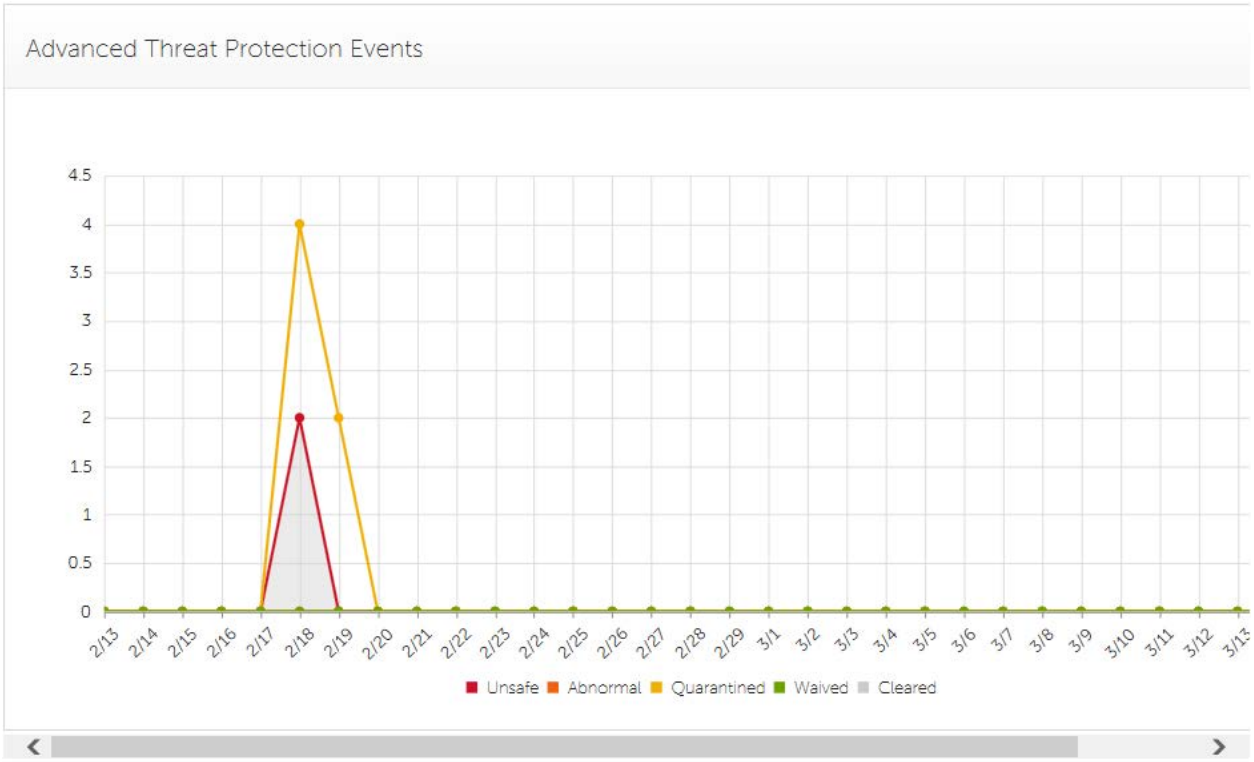


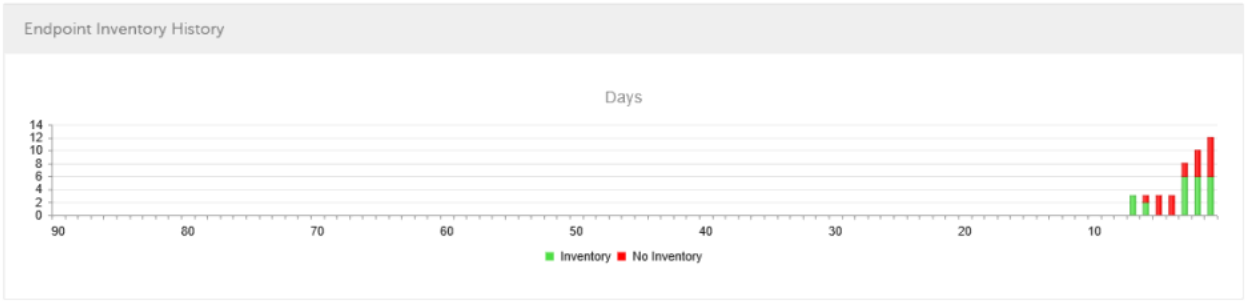






Note: An Advanced Threat Prevention event is not necessarily a threat. An event is generated when a recognized file or program is quarantined, safe listed, or waived. Threats are a category of events that are newly detected as potentially unsafe files or programs and require guided remediation.





Summary Statistics

Domains	3	Windows	13
User Groups	2	Mac	0
Endpoint Groups	2	Mobile Device	0
AD Users	11	All	13
Local Users	0		
Endpoints	13		
Protected	3		
Not-Protected	10		
Shields	7		
Managers	10		
Modified Policies	0		

Get Started with Dell Data Protection

- Log in to the Remote Management Console.
- Add Client Access Licenses, as needed.
- Add Domains from your directory server.
- If you require that users receive non-default policies upon activation, modify policies at the appropriate level.
- Add Groups and Users, as necessary.
- Assign Administrators, as necessary.
- Deploy clients.

Navigation

The Remote Management Console is a central control center that the administrator can use to deploy and monitor Dell Data Protection for the enterprise. It consists of security and configuration settings that are applied through policy to groups called Populations.

The menu pane allows you to access the following:

Dashboard

The Remote Management Console opens to the Dashboard. The Dashboard provides graphs and statistics on endpoint and threat protection as well as summary statistics on populations and operating systems.

Populations

A population is a grouping for which security policies, settings, and actions can be configured. For example, you can apply security policies at the Enterprise, Domain, User Group, User, Endpoint Group, and Endpoint levels. For more information about Populations, see Populations. For more information about security policies, see Manage Security Policies.

Compliance Reporter

Launches Compliance Reporter, a tool that provides reports on the protection state of your environment and endpoints, deployment issues that require action, and devices within the network.

Management

Allows you to commit policies, perform recovery, and manage licenses, services, alerts, and Secure Lifecycle external users.

Change the Superadmin Password

1. In the masthead at the top of the screen, click the gear icon and select **Change superadmin password**.
2. Enter the Current Password.
3. Enter the New Password.

   The new password must be at least 6 characters, contain at least one capital letter and one of these characters: **~@#$%^*()|?!{}[]**.
4. Confirm the New Password.
5. Click **Update**.

Components

Default Port Values

Dell Compatibility Server: TCP/1099 (closed)

Dell Compliance Reporter: HTTP(S)/8084

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888

Dell Policy Proxy: TCP/8000/8090

Dell Security Server: HTTPS/8443

Dell Forensic Server: HTTPS/8448

Client Authentication: HTTPS/8449 (If using Server Encryption)

Remote Management Console: HTTPS/8443

Client Communication if using Advanced Threat Protection: HTTPS/TCP/443

Beacon server if using Secure Lifecycle: HTTP/8446

NTP Time Synchronization: TCP and UDP/123 (For more information, refer to https://help.ubuntu.com/10.04/serverguide/NTP.html.)

Remote Management Console

The Remote Management Console is the security administration piece Dell Data Protection. The Remote Management Console allows administrators to monitor the state of endpoints, policy enforcement, and protection across the enterprise.

For increased security, the Remote Management Console separates administrator duties into administrator roles. For example, the Security Administrator can change and commit security policies for the entire enterprise, groups of users, or individual users.

The Remote Management Console has the following features.

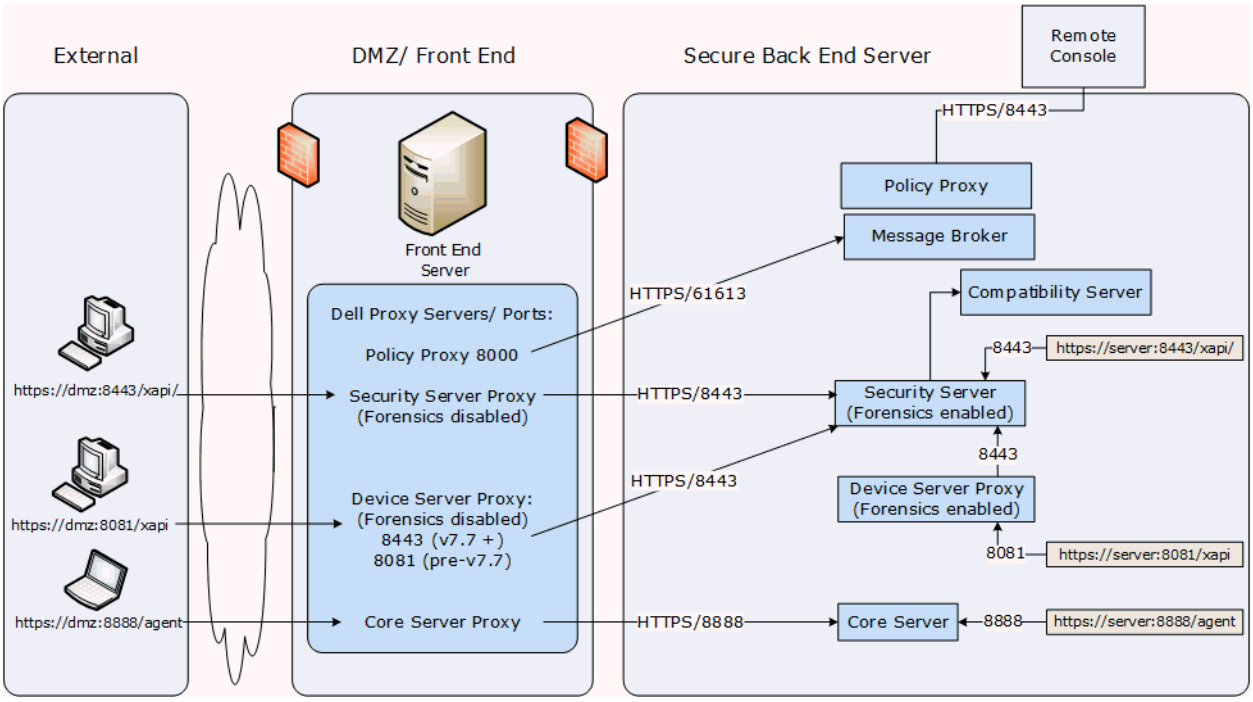
- Centralized management of diverse mobile devices
- "No change", read-only integration with existing enterprise directory servers
- Role-based mobile security policy creation and management
- Administrator-assisted device recovery
- Separation of administrative duties
- Automatic distribution of mobile security policies
- Mobile device inventory
- Searchable, ODBC-compliant system logs
- Trusted paths for communication between components
- Unique encryption key generation and automatic secure key escrow
- Centralized compliance auditing and reporting

Proxy Servers

Beginning with v8.1, the Proxy Server implementation, deployment and installation have been simplified. The new Proxy Server is a simplified web server with a single web application.

Types of Proxy Servers

- Security Server Proxy (defaults to 8443)
- Core Server Proxy (defaults to 8888)
- Device Server Proxy (defaults to 8081) see **Note**



Note: The purpose of Device Server Proxy is to support legacy Shields (pre-v8.0) that communicate with port 8081. Newer Shields (v8.0 and later) are configured by the client installer to communicate with the Security Server (or Security Server Proxy) on port 8443. The full Device Server is not installed in v8.1. The Device Server Proxy forwards all communications to the Security Server behind the firewall.

Policy Proxy

Policy Proxy serves as intermediary between the VE Server and the Shield, delivering information from each to the other.

Time Slotting

In order to prevent VE Server traffic jams, Policy Proxies use a configurable time slotting mechanism that allows them to independently choose well-distributed time slots for communicating with the VE Server.

Polling

On every poll, the endpoint authenticates, checks for policy updates, and uploads inventory. A successful authentication is required for the process to begin.

Poll Triggers

To poll, a user must be logged in. On the next user login, another poll will occur. The poll information needed is only available per user, and when that user is logged in.

Other times a poll occurs are as follows:

- Immediately upon login, after keys are unlocked.
- When a network status update is signaled by the operating system (cable plugged in, wireless network connected, VPN goes live).
- When the polling period elapses, as specified by policy.

Failed Poll Attempts

Policy Proxy poll attempts are based on a timer. When a poll attempt fails, the timer is reset. The length of time set for the next attempt is based on when the attempt failed. If the device misses a poll when the device is powered off, the timer will be triggered when the device is next powered on.

If the poll attempt failed while making the attempt, the time is set to one tenth the policy value for the polling interval. For example - If the polling interval is 100 minutes, then the next interval after a failed attempt will be 10 minutes. If it fails again, the next interval will still be 10 minutes. The interval will remain 10 minutes until a successful poll, after which it will return to 100 minute intervals.

General Information

- Policy Proxy is generally installed on only a few machines.
- Creates inventory information for the VE Server.
- Passes on to the VE Server device inventory it receives when the Windows Shield successfully retrieves policies.
- Securely distributes security policies and encryption keys to devices via the network when contacted.
- May be in your DMZ.
- Always belongs to a group. By default, all Policy Proxies belong to the same group.

Navigate the DDP Server

Navigation

The Remote Management Console is a central control center that the administrator can use to deploy and monitor Dell Data Protection for the enterprise. It consists of security and configuration settings that are applied through policy to groups called Populations.

The menu pane allows you to access the following:

Dashboard

The Remote Management Console opens to the Dashboard. The Dashboard provides graphs and statistics on endpoint and threat protection as well as summary statistics on populations and operating systems.

Populations

A population is a grouping for which security policies, settings, and actions can be configured. For example, you can apply security policies at the Enterprise, Domain, User Group, User, Endpoint Group, and Endpoint levels. For more information about Populations, see Populations. For more information about security policies, see Manage Security Policies.

Compliance Reporter

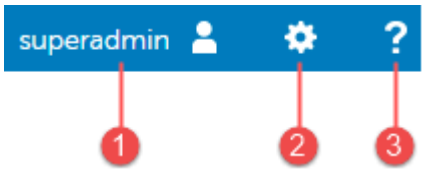
Launches Compliance Reporter, a tool that provides reports on the protection state of your environment and endpoints, deployment issues that require action, and devices within the network.

Management

Allows you to commit policies, perform recovery, and manage licenses, services, alerts, and Secure Lifecycle external users.

Masthead icons

The following icons display on the masthead:



(1) Logged in user - The user icon and name of the user that is currently logged on.

(2) Gear icon - From the gear icon, you can Change the Superadmin Password, view information about the Dell Data Protection Server, get Dell ProSupport contact information, and log out.

(3) Question mark icon - From the question mark icon, you can open a help topic that explains the current screen in the Remote Management Console.

Disconnected Mode

Disconnected mode allows a Dell Data Protection Server to manage Advanced Threat Prevention endpoints without a provisioned and hosted Advanced Threat Prevention service. The DDP Server captures all event and threat data in Disconnected mode.

To determine if a DDP Server is running in Disconnected mode, click the gear icon at the top right of the Remote Management Console and select **About**. The About screen indicates that a DDP Server is in Disconnected mode, below the DDP Server version.

Disconnected mode is different than a standard installation of DDP Server in the following ways.

Client Activation

An install token is generated when the administrator uploads an Advanced Threat Prevention license, which allows the Advanced Threat Prevention client to activate.

Remote Management Console

The following items are ***not available*** in the Remote Management Console:

Dashboard Notifications and the following areas specific to Advanced Threat Prevention: Advanced Threats by Priority, (Advanced Threat) Events by Classification, Advanced Threats Top Ten, and Advanced Threat Prevention Events.

(Left navigation pane) **Dropbox Management**, which allows administrators to register to remove Dropbox for Business users and their data.

(Left navigation pane) **Services Management**, which allows enabling of the Advanced Threat Prevention service and Product Notifications enrollment.

Enterprise > Advanced Threats tab, which provides a dynamic display of detailed events information for the entire enterprise, including a list of the devices on which events occurred and any actions taken on those devices for those events.

The following items ***have been added*** to the Remote Management Console to support Disconnected Mode:

Dashboard Threat Protection Status area, which displays Threats (by Category): Critical, Major, Minor, and Warning.

Enterprise > Advanced Threat Events tab, which lists events information for the entire enterprise based on information available in Disconnected Mode.

Functionality

The following functionality is not available:

DDP Server upgrade, update, and migration

Cloud profile update

Virtual Edition auto update, when installed on a VE - update must be done manually

Advanced Threat Protection auto update

Upload of Unsafe or Abnormal Executable files for Advanced Threat Prevention analysis

Advanced Threat Prevention File upload and Log File upload

The following functionality differs:

The Global Safe List is imported to the DDP Server from the Advanced Threat Prevention service, with the Global Allow policy. For more information, see the Global Allow policy.

The DDP Server provides the Quarantine List and Safe List, which are supported at both the Enterprise level (Global) and the Endpoint level. For more information, see the Quarantine List and Safe List policies.

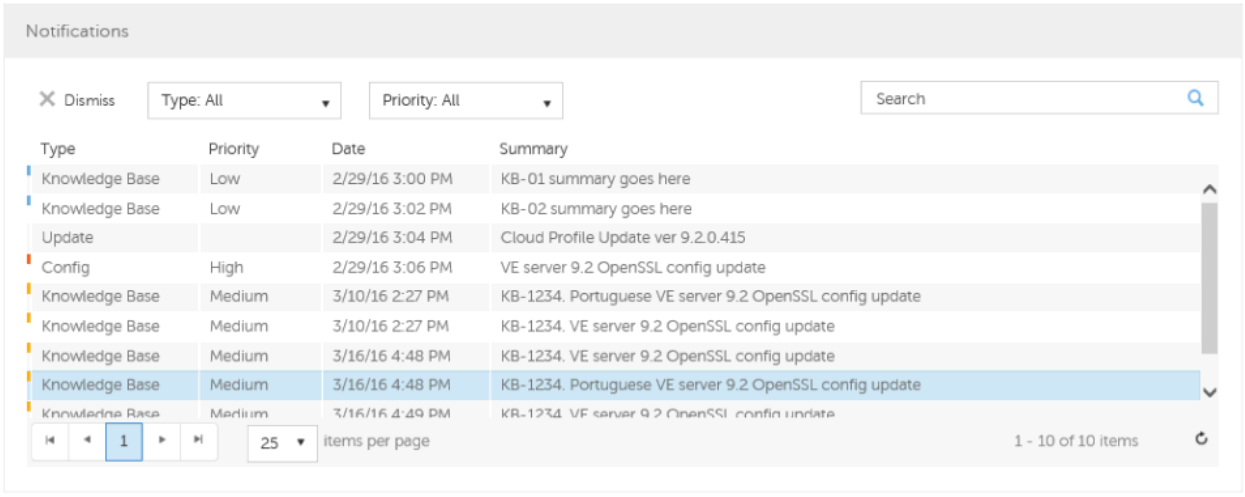
Dashboard

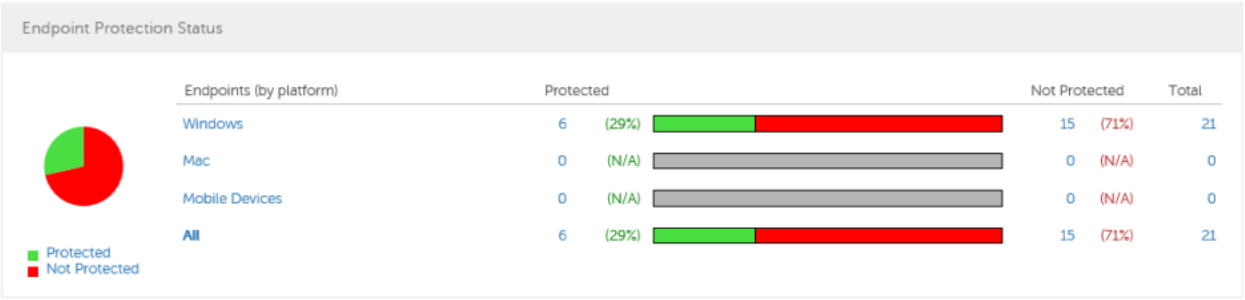
Dashboard

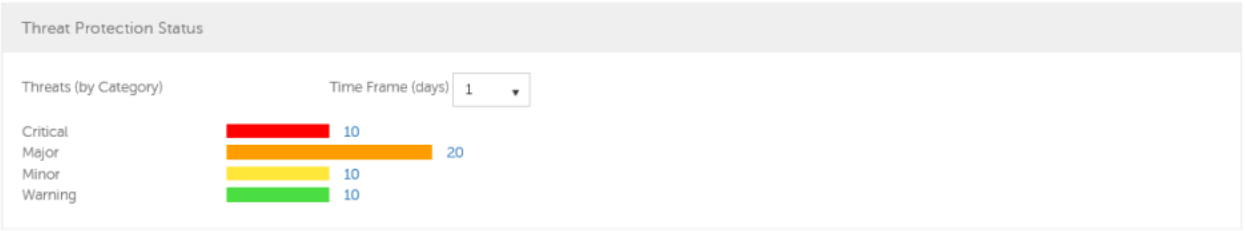
The Dashboard displays an overview of status information for your enterprise. You can access more detailed information directly from the Dashboard by clicking its statistics, graphs, and chart legends.

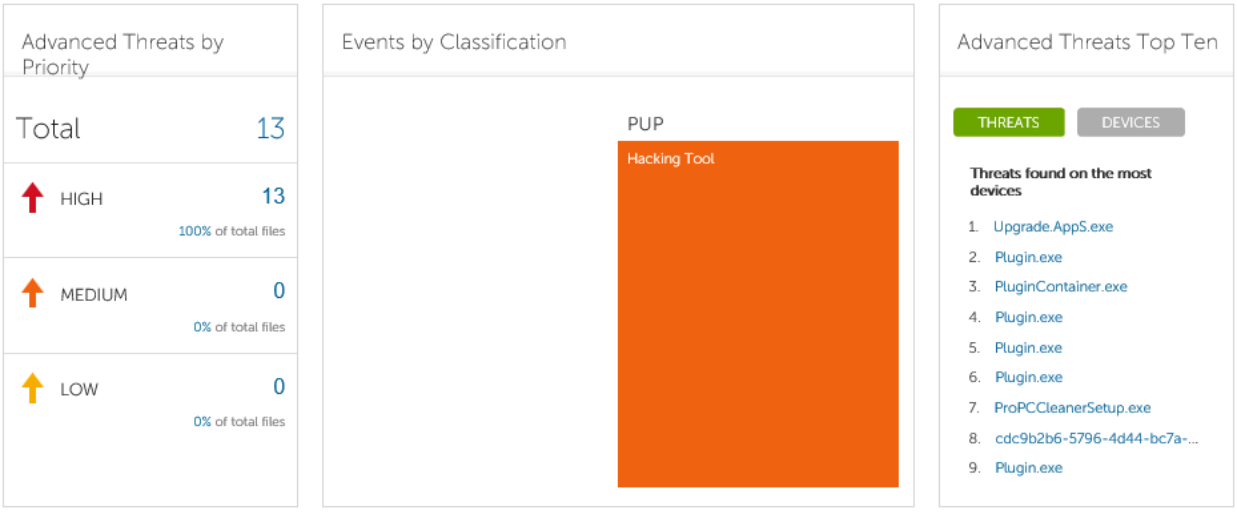
The images below reflect what you may see in the Dashboard. Content may vary based on the features installed and enabled on your Dell Data Protection Server and endpoints.

Click an area below to view a description of the detail you can access by clicking the same area in your Dashboard.

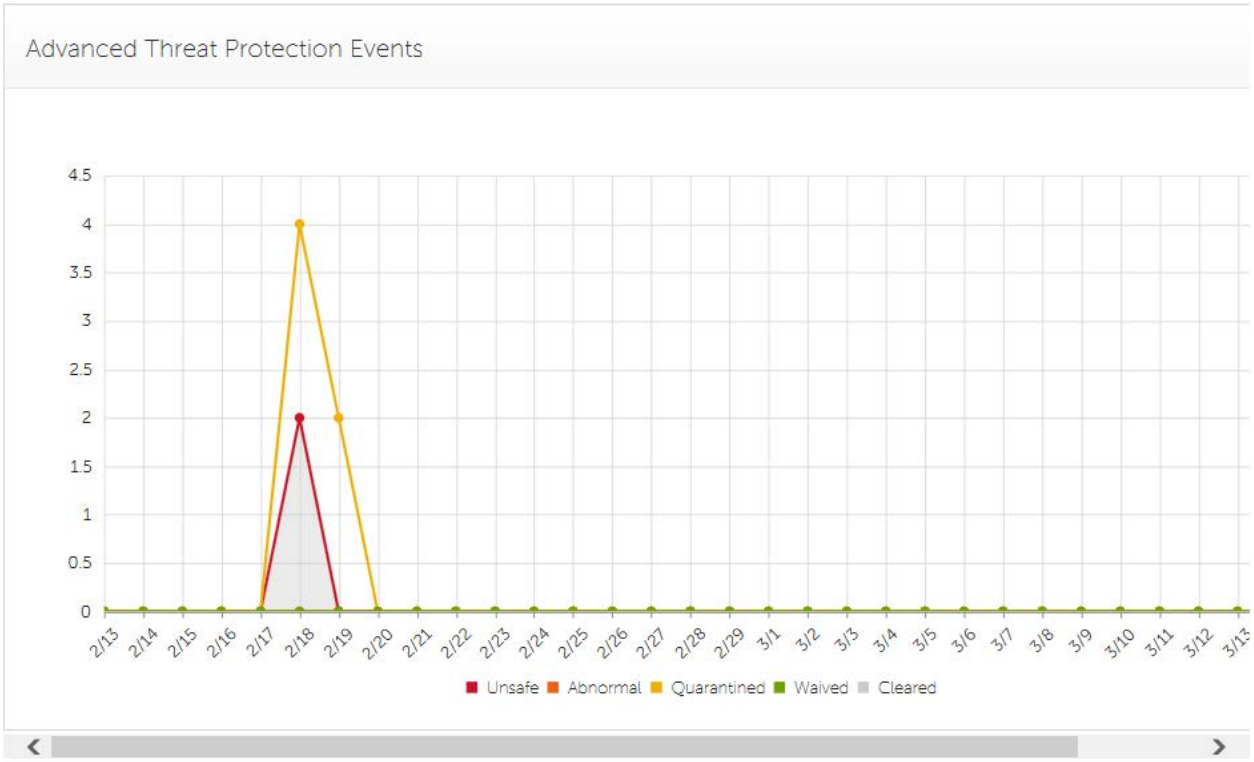


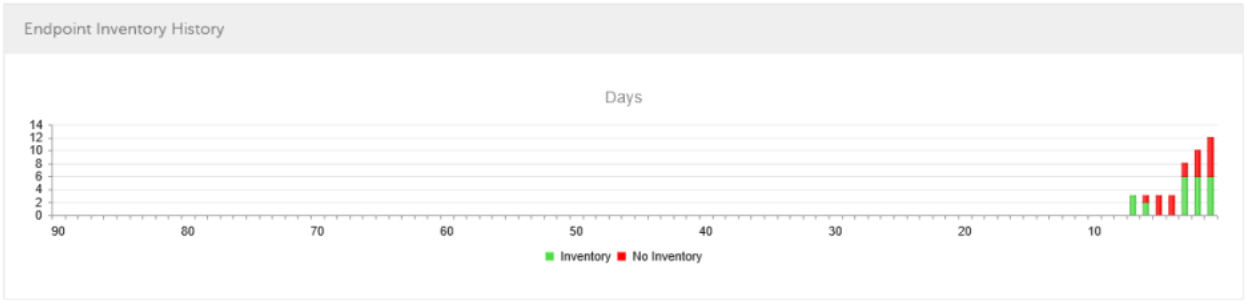


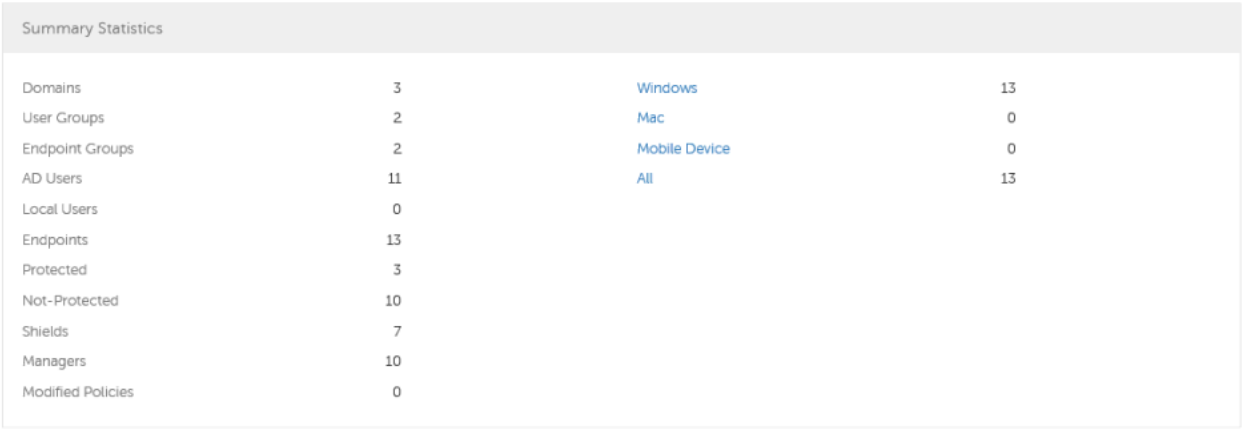




Note: An Advanced Threat Prevention event is not necessarily a threat. An event is generated when a recognized file or program is quarantined, safe listed, or waived. Threats are a category of events that are newly detected as potentially unsafe files or programs and require guided remediation.







Notifications List

The Notifications list provides a configurable summary of news, alerts, and events to display on the Dashboard or to be sent as email notifications. For more information, see Dashboard Field Descriptions and Notification Management.

Notification Types

You can select the notification types to include in the list. Notifications of the remaining types are hidden.

Types include:

Update - News of upcoming product updates. To view and receive product updates, you must enroll to receive them. Select **Services Management > Product Notifications**, click **On**, then click **Save Preferences**.

Config - News about configuration changes.

Knowledge Base - Summaries and links to knowledge base articles with in-depth technical information such as work-arounds and configuration methods.

Announcement - News of upcoming releases and new products.

License - Alerts when your volume license availability is low, or when your client access license count is has been exceeded.

Threat Protection - A threat alert from Advanced Threat Prevention.

Advanced Threat Event - An event detected by Advanced Threat Prevention.

Threat Event - An event detected by Threat Protection.

Certificate - Certificate expiration notification.

DDP Server Exceptions - A Dell Data Protection Server communication issue is impacting deliveries of the following notifications: Threat Protection, Update, Config, Knowledge Base, and Announcement.

After selecting one or more types, click in the neutral space above the list to apply the selections.

Select **Clear selected items** to reset the selections in this drop-down list.

Priority Levels

Note: Notification priority levels are not related to priority levels displayed on the Dashboard other than in the Notifications area.

Priorities are Critical, High, Medium, and Low. These priority levels are only relative to one another within a type of notification.

You can select the priority levels of notifications to include in the Dashboard Notifications area or email notifications lists. Notifications of the remaining priority levels are not included in the Dashboard or email notifications lists.

In the Dashboard, after selecting one or more priority levels, click in the neutral space above the drop-down list to apply your selections.

Select **Clear selected items** to reset the selections in this drop down list. All notifications will display (unless filtered elsewhere).

Endpoint Protection Status

In the Endpoint Protection Status section of the Dashboard, you can view endpoint status by platform: Windows, Mac, Mobile Devices, and All Platforms with a numeric value and bar chart that shows the numbers of protected and unprotected endpoints. A pie chart representing total protected and unprotected endpoints displays on the left.

Click a value to display a list of the endpoints represented in the value.

Protection Status

To access this page, click a link in the Dashboard's Endpoint Protection Status graph. You can click a specific platform type or **All**. The page provides protection details on the endpoints within that platform.

Platform - Windows, Mac, Mobile Devices, All, Protected, or Not Protected

Endpoint ID - Value that uniquely identifies the endpoint.

Protected - A green check mark indicates the endpoint is protected. The protection status of a Windows workstation is derived from the current encryption policies and encryption states of the Shield users, as well as the current device encryption policy and state of the endpoint. On the dashboard's Endpoint Protection Status graph, you can select endpoints by platform, protected endpoints, non-protected endpoints, or all endpoints. See Protected.

Shield Inventory Received - The date and time that the inventory was received by the Enterprise Server and placed in the queue.

Shield Inventory Processed - The date and time that the inventory was picked up from the queue and processed. (**Note**: If the Server is under load, the Processed and Received times may be different, but usually they will be the same.)

Agent Inventory Received - The date and time that the inventory was received by the Enterprise Server and placed in the queue.

Agent Inventory Processed - The date and time that the inventory was picked up from the queue and processed (**Note**: If the Server is under load, the Processed and Received times may be different, but usually they will be the same.)

Shield - If encryption is installed on the endpoint, an icon displays.

Manager (Windows only) - If installed on the endpoint, an icon displays. This includes endpoints with activated PBA, HCA, SED, or BitLocker Manager.

Threat Protection Status

Threat Protection monitors the network for viruses, spyware, unwanted programs, suspicious communications through the firewall, and unsafe websites and downloads.

The Threat Protection Status pane shows threats by category: Critical, Major, Minor, and Warning. Each category is listed in a colored bar chart with a numerical value for the corresponding number of threats found during the time frame.

The time frame is selectable, in days: 1, 7, 14, 30, 60, and 90 days.

Click a Threat Category value to display a detailed list of threats included in the category.

Threat Protection Status for Severity Level

To access this page, click a value on the Dashboard's Threat Protection Status graph.

This page provides a detailed view of threats based on individual severity levels and devices that have a threat within that severity level. The columns list the specific counts for each type of threat event on a device.

Dropdown list of severity levels - Select a different option from the list (Critical, Major, Minor, Warning, Information). **Critical** is the most dangerous threat to the endpoint, and **Information** is just a notification of an event that is unlikely to harm the endpoint.

Dropdown list of days - Select a time frame option: 1, 7, 14, 30, 60, and 90 days.

Platform - The platform type

Device ID - Value that uniquely identifies the target device. Click a link to view information about that endpoint.

Event Count columns - For each device, lists the number for each of the following threat events:

> Malware/Exploit - Includes counts for viruses, spyware, and unwanted programs. This could be exploited buffer overflows that seek to execute arbitrary code on a device or attempts to exploit browser vulnerabilities. Counts may include malware that executes from within memory space.
>
> Web Filter - Includes threats related to web browsing and downloads.
>
> Web Protection - Includes threats related to web browsing and downloads.
>
> Firewall - Includes suspicious communications related to incoming or outgoing traffic and any attacks.
>
> Uncategorized - Lists the number of threats that do not belong in other event counts.

Advanced Threat Prevention Events

The Advanced Threat Prevention Events pane displays a time line of Advanced Threat events over the course of a month, by file type as assigned by Advanced Threat Prevention.

Click a file type for details of the events of that type.

File types include:

Unsafe - A suspicious file with a high score (-60 to –100) likely to be malware

Abnormal - A suspicious file with a lower score (-1 to –59) less likely to be malware

Quarantined - A file that is moved from its original location, stored in the Quarantine folder, and prevented from executing on a specific device.

Waived - A file allowed to execute on a specific device.

Cleared - A file that has been cleared within the organization. Cleared files include files that are Waived, added to the Safe list, and deleted from the Quarantine folder on a device.

For more detail about events, see Advanced Threat Prevention Classifications and Advanced Threats Top Ten

Advanced Threats by Priority

Advanced Threats by Priority classifies suspicious files by priority levels of High, Medium, and Low. This prioritization helps administrators determine which threats and devices to address first. To view a list of threats with the corresponding priority level, click a value in the Advanced Threats by Priority field on the Dashboard.

Files are analyzed for the following attributes:

- The file has a Cylance score greater than 80.

  A score is assigned to each file that is deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.
- The file is currently running.
- The file has been run previously.
- The file is set to auto run.
- The file is detected by Execution Control.

Files are prioritized based on the number of the above attributes it has:

Low = 0-1 attributes

Medium = 2-3 attributes

High = 4-5 attributes

As an example, following is the analysis of three threats:

Threat 1

Attribute	Attribute Value	Score
Cylance score	90	+1
Currently running on any device	True	+1

Ever run on any device	True	+1
Set to auto run on any device	True	+1
Detected by Execution Control	False	+0
	Total score	**5: High Priority**

Threat 2

Attribute	Attribute Value	Score
Cylance score	20	+0
Currently running on any device	True	+1
Ever run on any device	False	+0
Set to auto run on any device	True	+1
Detected by Execution Control	False	+0
	Total score	**2: Medium Priority**

Threat 3

Attribute	Attribute Value	Score
Cylance score	20	+0
Currently running on any device	False	+0
Ever run on any device	False	+0
Set to auto run on any device	False	+0
Detected by Execution Control	True	+5
	Total score	**5: High Priority**

Advanced Threat Prevention Classifications

Advanced Threat Prevention can provide details on the static and dynamic characteristics of files. This allows administrators to not only block threats, but also to understand threat behavior in order to further mitigate or respond to threats.

Threat Classification

Threats are classified based on the following:

1. Threats are classified by the type of threat, including malware (for example, trojans and downloaders) and potentially unwanted programs (for example, adware, hacking tools, and portable applications.
2. A **Score** is assigned to each file. Negative scores, from -1 to -100 denote files that are deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the negative number, the greater the confidence.
3. The file is assigned a type, based on the score.

   File Types:

   - Unsafe: A file with a score ranging from -60 to -100. An Unsafe file is one in which the Advanced Threat Prevention agent finds attributes that greatly resemble malware.
   - Abnormal: A file with a score ranging from -1 to -59. An Abnormal file has a few malware attributes but fewer than an unsafe file, thus is less likely to be malware.

   Note: Occasionally, a file may be classified as Unsafe or Abnormal even though the score displayed doesn't match the range for the classification. This could result from updated findings or additional file analysis after the initial detection. For the most up-to-date analysis, enable **Auto Upload** in the Device Policy.
4. The file is given a **Priority Level**. The priority level helps administrators determine which threats and devices to address first. For more information, see Advanced Threats by Priority.

Advanced Threats Top Ten

Click **Threats** to view the threats found on the largest number of devices.

Click a threat to display additional information about the threat. Details display on a new page.

Click **Devices** to view a list of devices that have the largest number of threats.

Click a device to display additional information about the device. Details display on a new page.

Endpoint Protection History

This graph gives a time line snapshot of the past 90 days of the total number of endpoints that are protected and total number that are not protected. This graph is especially useful during initial deployment, when moving toward complete protection.

The green bars represent the total number of protected endpoints. The red bars represent the total number of endpoints that are not protected.

Endpoint Inventory History

This graph gives a time line snapshot of the past 90 days of the total number of endpoints that have communicated with and sent inventory to the EE Server/VE Server and the total number that have not sent inventory.

Summary Statistics

Summary Statistics provides a breakdown of the following:

- Domains

- User groups
- Endpoint groups
- AD users
- Local users
- Endpoints
- Protected
- Not protected
- Shields
- Managers
- Modified policies

Summary Statistics provides a breakdown of endpoints by platform, with a link to a detailed report for the selected platform:

- Windows
- Mac
- Mobile device
- All

Endpoint OS Report

To access this page, click a platform link on the Dashboard's Summary Statistics. If you click **All** and the Platform Report page opens, click **view** in the OS Report column.

OS/Version - Operating system name and version as reported in the endpoint's inventory

Count - Number of endpoints or devices

Shielded - Number of shielded endpoints for that OS and version

Unshielded - Number of unshielded endpoints for that OS and version

Platform Report - Click **view** for a report on all the platforms

Endpoint List - Click the icon to navigate to the Endpoints page and the list of endpoints for that OS and version

Platform Report

To access this page, click **All** on the Dashboard's Summary Statistics. If you click a specific platform link and access the Endpoint OS Report page, click **view** in the Platform Report column.

Platform - Windows, Mac, and MDM (Mobile Device Management)

Count - Number of endpoints or devices for that platform

Shielded - Number of shielded endpoints for that platform

Unshielded - Number of unshielded endpoints for that platform

OS Report - Click **view** for a report based on each operating system/version for that platform

Endpoint List - Click the icon to navigate to the Endpoints page and the list of endpoints for that platform

Populations

Populations

A population is a grouping for which policies, settings, and actions can be configured.

To access a Populations page, click **Populations** in the left pane of the Remote Management Console and select a Population, for example, **Populations > Enterprise**.

Tabs available on each Populations page provide information, allow you to edit detail of the Population, and provide configuration options for that Population. The table lists the tabs available for each Population.

Populations	Security Policies	Details & Actions	Members	Settings	Key Server	Endpoint Groups	Endpoints	User Groups	Users	Admin	Threat Events	Advanced Threat Events
Enterprise	•										•	•
Domains	•	•	•	•	•							
User Groups	•	•	•							•		
Users	•	•					•	•		•		
Endpoint Groups	•	•	•									
Endpoints	•	•				•			•		•	•
Administrators		•								•		

To access the tabs for each Population:

- Enterprise - Click **Populations > Enterprise**.
- Populations other than Enterprise - Click a Population link, then search for or click a Domain, User Group, User, Endpoint Group, Endpoint, or Administrator link.

Note: The tabs available for an Administrator may vary, depending on the role.

Enterprise

View or Modify Enterprise-Level Policies

To view or modify Enterprise-level policies, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Click the **Security Policies** tab.
3. Select the technology group, such as Windows Encryption, or policy group, such as Policy-Based Encryption, to view or modify.

View Threat Events

Threats are categorized as Malware/Exploit, Web Filter, Firewall, or Uncategorized events. The list of threat events can be sorted by any of the column headers. You can view threat events for the entire enterprise or for a specific endpoint. To view threat events of a specific endpoint, from the Enterprise Threat Events tab, select the endpoint's device in the Device ID column.

To view threat events in the enterprise, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Click the **Threat Events** tab.
3. Select the desired severity level and time period for which to display events.

To view threat events on a specific endpoint, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a Hostname, then the **Threat Events** tab.

Manage Enterprise Advanced Threats

Advanced Threats tab

If the Advanced Threat Prevention service is provisioned and licenses are available, the Advanced Threats tab provides a dynamic display of detailed events information for the entire enterprise, including a list of the devices on which events occurred and any actions taken on those devices for those events. For information about provisioning the service, see Provision Advanced Threat Prevention Service.

To access the Enterprise Advanced Threats tab, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threats** tab.

Information about events, devices, and actions are organized on the following tabs:

Protection - Lists potentially harmful files and scripts and details about them, including the devices on which the files and scripts are found.

Agents - Provides information about devices running the Advanced Threat Prevention client as well as the option to export the information or remove devices from the list.

Global List - Lists files in the Global Quarantine and Safe list and provides the option to move files to these lists.

Options - Provides a way to integrate with Security Information Event Management (SIEM) software using the Syslog feature as well as export Advanced Threat data.

Certificate - Allows certificate upload. After upload, certificates display on the Global List tab and can be Safe listed.

Tables on the tabs can be organized in these ways:

Add or remove columns from the table - Click the arrow next to any column header, select **Columns**, then select the columns you want to see. Clear the check box of columns you want to hide.

Sort the data - Click a column header.

Group by a column - Drag the column header up, until it turns green.

Filter based on data of one column - click the down-arrow on any column to display the context menu, and select **Filter**.

Advanced Threat Events tab

The Advanced Threat Events tab displays information about events for the entire enterprise based on information available in the Dell Data Protection Server.

The tab displays if the Advanced Threat Prevention service is provisioned and licenses are available.

To export data from the Advanced Threat Events tab, click the **Export** button and select **Excel** or **CSV** file format.

Note: Excel files are limited to 65,000 rows. CSV files have no size limit.

For a list of fields and filters on the tab, see Advanced Threat Events tab fields and filters.

Domains

Domains

On the Domains page, you can add a domain or search and select a domain to View or Modify Domain Information.

Add a Domain

To add a Domain, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. On the Domains page, click **Add**.
3. Complete the fields on the Add Domains page.

   Host Name - Enter the fully qualified host name or the computer name and domain portion of the hostname (for example, <computer_name>.<domainname>.com) for the enterprise directory server.

   Port - Enter a port for the directory server. If you do not specify a port, the default port of 389 is used. The secure port, 636, uses an SSL connection instead of clear text. Global catalog ports are 3268 (clear-text) and 3269 (secure).

   Distinguished Name - This field is populated when you tab from the completed Host Name field or refresh the URL. If necessary, correct the entry to reflect the domain (for example, DC=domainname, DC=com).
   Secure LDAP - Select this check box for LDAPS.

   User Name - Enter a User Name with rights for the domain to read and run queries on the enterprise directory server. The format *must* be UPN, such as user@domain.com. The credentials are domain-specific. VE does not fully observe trusted relationships between domains.

   Password - Enter a Password with rights for the domain to read and run queries on the enterprise directory server. The credentials are domain-specific. VE does not fully observe trusted relationships between domains.
4. In the Domain Alias area, enter the domain name or other alias and click **Add**. It is recommended that you add a pre-Windows 2000 domain name as an alias. You may enter any UPN suffixes that are allowed for the domain and are configured in the enterprise directory server.

   A Domain Alias is a mapping the DDP Server uses to select which domains to search to locate users that might match the suffix in the UPN.
5. Click **Add Domain**.

Users

Users are added through reconciliation. Reconciliation is the automated process the DDP Server uses to compare user data in the DDP Server database with user data in the enterprise directory server and update the DDP Server database when necessary.

Click a User Name to view details about the user. Click an arrow next to a User Name to view the Common Name, sAM Account Name, and User Principal Name.

Add a User to a Domain

1. In the left pane, click **Populations > Users**.
2. On the Users page, click **Add**.
3. In the Add Users by Domain dialog, select a domain from the pull-down list.
4. In the Full name field, enter the exact text for the user name or use the wildcard character (*). For best results, use non-wild card characters at the beginning of the filter (e.g., User* instead of *ser).

5. Select Common Name, Universal Principal Name, or sAMAccountName from the pull-down list.

   A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a Domain or Group but does not appear in the Domain or Group Members list in the Remote Management Console, ensure that all three names are properly defined for the user in the enterprise directory server.

6. Click **Search**. Depending on the size, this may take a few minutes to populate.

   If the query is too large, a dialog prompts you to revise the query.

7. Select users from the directory user list to add to the Domain. The user names are added to the field below the list.

8. Click **X** to remove the user name from the field or click **Add**.

User Groups

On the User Groups page, you can add a user group or search and select a user group to View or Modify User Group Policies and Information.

Add a User Group

1. In the left pane, click **Populations > User Groups**.
2. On the User Groups page, click **Add**.
3. In the Add Groups by Domain dialog, select a domain from the pull-down list.
4. In the Search field, enter the exact text for the group name or use the wildcard character (*).
5. Click **Search**. Depending on the size, this may take a few minutes to populate.
6. Select a group from the list to add to the Domain. The group name is added to the field below the list.

   Click the **X** in the group name to remove the group name from the field.

7. Click **Add**.

Notes:

Universal security groups are not supported.

Nested Groups are not supported.

Only User Groups with a Group Scope of Universal are supported for domains that connect through the Global Catalog Port.

Add Non-Domain Users

To add non-domain users, the non-domain activation feature can be enabled by contacting Dell ProSupport and requesting instructions.

View or Modify Domain Policies and Information

1. In the left pane, click **Populations > Domains**.
2. Search or select the appropriate Domain Name to display Domain Detail.

   When you click a Domain, the Domain Detail page displays.

3. Click the tab that corresponds with the action you want to perform:

   Security Policies - To view or modify policies of the Domain, click **Security Policies**.

Details & Actions - To view properties of the Domain, click **Details & Actions**

Members - To view, add, or modify information for Groups and Users within the Domain. For instructions on how to perform these tasks, refer to the appropriate topic:

Add Users to Domain

Add User Groups

View or Modify User Information

View or Modify User Group Information

Settings - To configure LDAP settings for the Domain, click **Settings**. Refer to Add Domains for instructions.

Domain Details & Actions

The Domain Details & Actions tab lists the properties of a domain.

To access the Domain Details & Actions tab, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. Search or select a Domain Name, then the **Details & Actions** tab.

Details displayed on the Domain Details & Actions tab:

Domain Name - Name of the domain server. This should match the domain name in the title of the page.

Location - The location (path) of the domain within the enterprise structure. This information is derived from the fully qualified host name or the computer name and domain portion of the hostname entered when the domain was added. Example: /com/enterpriseserver

LDAP Url - URL to the active directory. This field is populated after adding the domain. The information is derived from the completed Host Name field.

Example - LDAP://domainname.com:portnumber/DC=domainname,DC=com

To configure LDAP settings for the domain, click the **Settings** tab.

Status - Describes the health of the domain server (Good, Fair, Poor).

Domain Members

This page allows you to view, add, or modify information for Groups and Users within the Domain.

To access the Domain Members tab, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. Search or select a Domain Name, then the **Members** tab.

From this tab, you can perform these actions:

Add Users to Domain - Allows you to add users by domain

Add Group - Allows you to add a user group by domain

Select to view the following information about Groups & Users, Users only, or Groups only:

User/Group - Each user or user group in the Domain. Click an entry to view details.

Distinguished Name

CN is the common name, either a user or group name.

OU is the organizational unit name, for example, Dallas.

DC are domain components, for example, DC=Organization, DC=com

Common Name - For a user, the user name; for a group, the group name

User - Column displays a green checkmark

Group - Column displays a green checkmark

Domain Settings

This page allows you to configure or modify LDAP settings for the Domain.

To access the Domain Settings tab, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. Search or select a Domain Name, then the **Settings** tab.

On the Domain Settings tab, you can view this information:

Directory URL - Lists the current URL for the enterprise directory server. If you modify the settings, click **Refresh URL**.

Host Name - The fully qualified host name or the computer name and domain portion of the hostname (for example, <computer_name>.<domainname>.com) for the enterprise directory server.

Port - The port for the directory server. If you do not specify a port, the default port of 389 is used. The secure port, 636, uses an SSL connection instead of clear text. Global catalog ports are 3268 (clear-text) and 3269 (secure).

Distinguished Name - This field is populated when you tab from the completed Host Name field or refresh the URL. If necessary, correct the entry to reflect the domain (for example, DC=domainname, DC=com).

Secure LDAP - Select this check box for LDAPS.

User Name - The User Name with rights to read and run queries on the enterprise directory server. The format *must* be UPN, such as user@domain.com.

Password - Enter a Password with rights to read and run queries on the enterprise directory server.

Alias - A mapping that the DDP Server uses to select which domains to search to locate users that might match the suffix in the UPN. The domain name or other alias. It is recommended that you add a pre-Windows 2000 domain name as an alias. You may enter any UPN suffixes that are allowed for the domain and are configured in the enterprise directory server.

Click **Add**, and the entry populates the field below.

Select an alias in the list, and click **Remove Selected**.

Update Domain - Click to update changes.

Domain Key Server

This page allows you to view or modify components for use with Kerberos Authentication/Authorization.

Account - Enter an account name.

Click **Add Account**, and the entry populates the field below.

Select an account in the list, and click **Remove Selected**.

To access the Domain Key Server tab, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. Search or select a Domain Name, then the **Key Server** tab.

User Groups

User Groups

On the User Groups page, you can add a user group or search and select a user group to View or Modify User Group Policies and Information.

Add a User Group

1. In the left pane, click **Populations > User Groups**.
2. On the User Groups page, click **Add**.
3. In the Add Groups by Domain dialog, select a domain from the pull-down list.
4. In the Search field, enter the exact text for the group name or use the wildcard character (*).
5. Click **Search**. Depending on the size, this may take a few minutes to populate.
6. Select a group from the list to add to the Domain. The group name is added to the field below the list.

   Click the **X** in the group name to remove the group name from the field.
7. Click **Add**.

Notes:

Universal security groups are not supported.

Nested Groups are not supported.

Only User Groups with a Group Scope of Universal are supported for domains that connect through the Global Catalog Port.

Remove User Groups

1. In the left pane, click **Populations > User Groups**.
2. Click a Group Name link or enter a filter to search for available Groups.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.
3. Select a row to highlight it.
4. At the top, click **Delete**.

   Note: As another option, click a Group Name link and select the **Details & Actions** tab. Click **Remove Group**.

If you remove a User Group that has Administrative privileges and later re-add the Group, it remains an Administrator Group.

Find User Groups

1. In the left pane, click **Populations > User Groups**.
2. Enter a filter to search for available Groups.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.

3. Click **Search**.

   A Group or list of Groups displays, based on your search filter.

View or Modify User Group Policies and Information

1. In the left pane, click **Populations > User Groups**.
2. Search or select the appropriate Group Name to display User Group Detail.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.

   When you click a Group Name, the User Group Detail page displays.
3. Click the tab that corresponds with the action you want to perform:

   Security Policies - To view or modify policies of the Group, click **Security Policies**.

   Details & Actions - To view properties of the Group, click **Details & Actions**. Viewable information includes:
   Group Name: Group1 (Domain\Group1)
   Distinguished Name: CN=Group1, OU=Dallas, DC=Organization, DC=com
   Common Name: Group1
   Last Modified in Directory - date and timestamp
   Last Reconciled - date and timestamp

   Members - To view or modify the information of a User in the Group, click **Members**. The list of Users in the Group displays. Click a User to view the User's Security Policies, Details & Actions, Endpoints, User Groups, and Admin. For instructions on how to view or modify User information, refer to View or Modify User Information.

   Admin - To view, assign, or modify Administrator Roles assigned to the Group, click **Admin**. Select or deselect Administrator Roles to modify Administrator Roles assigned to the Group. For more information about privileges available to each Administrator Role, refer to Administrator Roles.
4. If modified, click **Save**.

User Group Details & Actions

The User Group Details & Actions tab lists the properties of a selected user group.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a Group Name, then the **Details & Actions** tab.

Remove Group

The **Remove Group** command permanently removes this user group from the DDP server.

Details:

Group Name - Name of the user group <user group>(<domain name>\<user group>). This should match the user group name in the title of the page.

Distinguished Name - CN=Group1, OU=Dallas, DC=Organization, DC=com

CN is the common name

OU is the organizational unit name

DC are domain components

Common Name - non-technical name of the user group

Last Modified - Date/time stamp of the last time this information changed.

Last Reconciled - Date/time stamp of the last time this information was reconciled.

User Group Members

This page displays information about each user within the user group.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a Group Name, then the **Members** tab.

User - Each user in that user group

Distinguished Name - CN=Group1, OU=Dallas, DC=Organization, DC=com

CN is the common name

OU is the organizational unit name

DC are domain components

Common Name - non-technical name of the user group

User Group Admin

This page allows you to assign, modify, or view Administrator roles for a group.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a Group Name, then the **Admin** tab.

Administrator Roles - Assign or modify roles for a group membership and click **Save**.

Delegated Roles - Delegate Administrator rights for the Group to a User.

Related topics:

Administrator Roles

Assign or Modify Administrator Roles

Delegate Administrator Roles

Modify Group Precedence

Note: Precedence of VDI Endpoint Groups (Non-Persistent and Persistent) is set at **Max**. This level ***must*** remain at **Max** precedence. Ensure that policies for VDI Endpoint Groups are set according to Policy and Configuration Requirements for VDI Endpoint Groups.

The Group Precedence feature is used to determine policy arbitration for effective policies that include multiple groups. Group precedence creates a weight associated with the specific group it is assigned to, and that weight is used in policy arbitration for all policy overrides. Policy overrides are used from the group with higher precedence when two (or more) separate groups in a policy arbitration map have different precedence. Normal per-policy arbitration takes place when all groups in a policy arbitration map have the same precedence.

For a specific User Group or Endpoint Group to carry the highest weight, set the precedence to Max. Conversely, set the precedence to Min for the specific group to carry the lowest weight. The default value for User Groups is Min. The default value for Endpoint Groups is Medium.

To change Group Precedence:

1. In the left pane, click **Populations > Endpoint Groups** (or **User Groups**).

2. Select the appropriate group.
3. In the Precedence drop-down on the Securities Policies tab, select either Max, High, Medium, Low, or Min. Selecting Max gives this group the highest weight for policy arbitration. Selecting Min gives this group the least weight for policy arbitration.
4. Click **Save**.
5. Click **Management > Commit**.
6. Enter a description of the change in the Comment field.
7. Click **Commit Policies**.

Assign or Modify Administrator Roles

From the Administrators page, you can view or modify existing Administrator privileges.

To view or modify existing Administrator privileges, follow these steps:

1. In the left pane, click **Populations > Administrators**.
2. Search or select the row that displays the Username of the appropriate Administrator to display User Detail.
3. View or modify administrator roles in the pane at the right.
4. Click **Save**.

Note: Dell recommends assigning Administrator Roles at the Group level rather than at the User level.

To view, assign, or modify Administrator Roles at the Group level, follow these steps:

1. In the left pane, click **Populations > User Groups**.
2. Search or select a Group Name, then the **Admin** tab.

   The User Group Detail page displays.
3. Select or deselect Administrator Roles assigned to the Group.
4. Click **Save**.

If you remove a Group that has Administrative privileges and later re-add the Group, it remains an Administrator Group.

To view, assign, or modify Administrator Roles at the User level, see User Admin.

Related topics:

Administrator Roles

User Admin

Delegate Administrator Roles

View Reconciliation Date

To view the date and time a User Group's or User's information was last reconciled with Active Directory, click the Details & Actions tab for the Group or User, and refer to Last Reconciled. For instructions, refer to View or Modify User Group Policies and Information and View or Modify User Policies and Information.

View Policy Proxy State

The Remote Management Console tracks the Policy Proxy's Policy Updating state.

1. In the left pane, click **Populations > Endpoints**.
2. Select an endpoint type, for example, **Workstation** or **Mobile Device**.
3. If you know the full Hostname of the endpoint, enter it into the Search field and click the **Search** icon.

   For Windows and Mac, enter the full Hostname of the endpoint if you know it. However, you may leave the field blank to display all Windows and Mac endpoints.

   For Mobile devices, optionally enter the user's email address.

   If you do not know the full Hostname or user email address, scroll through the list of available endpoints to locate the endpoint.
4. Click an endpoint in the list to display the Endpoint Detail.
5. Click the **Details & Actions** tab of the endpoint for which you want to view information.

Users

Users

Users are added through reconciliation. Reconciliation is the automated process the DDP Server uses to compare user data in the DDP Server database with user data in the enterprise directory server and update the DDP Server database when necessary.

Click a User Name to view details about the user. Click an arrow next to a User Name to view the Common Name, sAM Account Name, and User Principal Name.

Add a User to a Domain

1. In the left pane, click **Populations > Users**.
2. On the Users page, click **Add**.
3. In the Add Users by Domain dialog, select a domain from the pull-down list.
4. In the Full name field, enter the exact text for the user name or use the wildcard character (*). For best results, use non-wild card characters at the beginning of the filter (e.g., User* instead of *ser).
5. Select Common Name, Universal Principal Name, or sAMAccountName from the pull-down list.

   A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a Domain or Group but does not appear in the Domain or Group Members list in the Remote Management Console, ensure that all three names are properly defined for the user in the enterprise directory server.
6. Click **Search**. Depending on the size, this may take a few minutes to populate.

   If the query is too large, a dialog prompts you to revise the query.
7. Select users from the directory user list to add to the Domain. The user names are added to the field below the list.
8. Click **X** to remove the user name from the field or click **Add**.

Remove Users

In general, a user cannot be removed in the Remote Management Console. Instead, you must remove the user from Active Directory.

To remove a Dropbox for Business User, see Dropbox Management.

Find Users

1. In the left pane, click **Populations > Users**.
2. Do one of these:
    - Enter the user name or a filter in the Search field and click the search icon.

      Note: To search, you can enter Common Name, Universal Principal Name, or sAMAccountName. You can use the wildcard character (*) but it is not needed at the beginning or end of the text.

    - Scroll through the User Name list.
3. Click a link in the User Name column.

   The User Detail page opens, displaying the Security Policies tab.

Deactivate/Suspend Users

If the user you are deactivating is no longer associated with your organization, be sure to publish appropriate *Current Shield State* policy with a value other than *Activate*, and ensure that the policy commit is complete and successful prior to removing the user from your enterprise directory server. The user does not need to be in your enterprise directory server, but the Policy Proxy does need to deliver the policy to their device in order for it to take effect.

Best Practice - Deleting users from the enterprise directory server is not recommended. If a user leaves the organization, the account should be moved to a disabled group. With that said, if a deletion occurs, the user is simply marked "removed" in the VE Server, rather than deleted. The user will not display in the Remote Management Console, but their keys and other information are still available in the database.

1. In the left pane, click **Populations > Users**.
2. Click a User Name link or enter a filter to search for available users.

   Note: To Search, you can enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character (*) may be used but is not required at the beginning or end of the text.
3. On the **User Detail > Security Policies** tab under the Windows Encryption technology group, click the **Policy-Based Encryption** policy group.
4. Click **Show advanced settings**.
5. Change the *Current Shield State* policy to **Suspend**.
6. Click **Save**.
7. Commit Policies.

To reactivate a deactivated Windows user, follow the instructions in Reinstate Suspended Users.

Reinstate Suspended Users

To reinstate a suspended user, follow these steps:

1. In the left pane, click **Populations > Users**.
2. Click a User Name link or enter a filter to search for available users.

   Note: To Search, you can enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character (*) may be used but is not required at the beginning or end of the text.
3. On the **User Detail > Security Policies** tab under the Windows Encryption technology group, click the **Policy-Based Encryption** policy group.

4. Click **Show advanced settings**.
5. Change the *Current Shield State* policy to **Activate**.
6. Click **Save**.
7. Commit Policies.

   Repeat these steps for each type of device the user was suspended from.

8. To reinstate a suspended Windows Shield user, perform the preceding steps and then run WSDeactivate on the computer that was suspended for that particular user. WSDeactivate and its instructions are located in the Dell Data Protection installation media. When using WSDeactivate, existing local keys, credentials, and policy material are no longer accessible to the Shield, and all managed users are forced to reactivate upon their next log on.

View or Modify User Policies and Information

1. In the left pane, click **Populations > Users**.
2. Click a User Name or enter a filter to search for available users.

   Note: To Search, you can enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character (*) may be used but is not required at the beginning or end of the text.

   When you click a User Name, the User Detail page displays.

3. Click the tab that corresponds with the action you want to perform:

   Security Policies - To view or modify policies of the User, click **Security Policies**.

   Details & Actions - To view properties of the User, click **Details & Actions**. Viewable information includes:
   User Name: User Name (username@organization.com)
   Distinguished Name: CN=User Name, OU=Dallas, DC=Organization, DC=com
   Common Name: User Name
   User Principal Name: username@organization.com
   sAM Account Name: username
   User Type - possible values are *AD* or *local*
   Last Modified - Date/time stamp
   Last Reconciled - Date/time stamp

   Endpoints - To view or modify information for the User's endpoints, click **Endpoints**. For instructions on how to modify endpoint information, refer to View or Modify Endpoint Information.

   User Groups - To view the information for Groups the User belongs to, click **Groups**. A list displays of Groups the User belongs to. Click a User Group to view the Group's Security Policies, Details & Actions, Members, and Admin.

   Admin - To view, assign, or modify Administrator Roles assigned to the User, click **Admin**. Select or deselect Administrator Types to modify Administrator Roles assigned to the User.

4. If modified, click **Save**.

VDI User Policies

To manage policy for users in a VDI environment, create a Windows Domain group, associate domain users with that group, and then import the group into Dell Server. This allows Dell Server to manage the users and their policies.

Policy settings differ, based on whether persistent or non-persistent VDI is deployed in the environment. For an explanation of the differences between persistent and non-persistent VDI, see Persistent vs. Non-Persistent VDI.

Policy and Configuration Requirements for VDI Users

The policy requirements below are for VDI Users running Advanced Threat Prevention. The list includes only policies that are significant for VDI Users. VDI Endpoint Group policy settings must also meet certain requirements. See Policy and Configuration Requirements for VDI Endpoint Groups.

Note: Ensure that you turn off Advanced Threat Prevention Agent Auto Update. In the left pane of the Remote Management Console, select **Management > Services Management > Advanced Threats - Agent Auto Update**, then select **Off**.

Note: With Persistent VDI Groups, ensure that roaming user profiles are configured.

These policy and configuration settings for VDI Users must be configured before VDI client activation:

Technology	Category	Policy or Setting	Persistent VDI Group setting	Non-Persistent VDI Group setting
Windows Encryption	Policy-Based Encryption	Policy-Based Encryption	On	Off
Windows Encryption	Policy-Based Encryption	Encrypt Outlook Personal Folders	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Encrypt Temporary Files	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Encrypt Temporary Internet Files	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Encrypt User Profile Documents	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Secure Post-Encryption Cleanup	Single-pass Overwrite	Single-pass Overwrite
Windows Encryption	Policy-Based Encryption	Force Logoff/Reboot on Policy Updates	Selected	Not Selected
Removable Media Encryption	Windows Media Encryption	Windows Media Encryption	On	On
Removable Media Encryption	Windows Media Encryption	EMS Scan External Media	Not Selected	Not Selected

User Details & Actions

The User Details & Actions tab lists the properties of the selected user.

1. In the left pane, click **Populations > Users**.
2. Search or select a User Name, then the **Details & Actions** tab.

Details:

User Name - User Name (username@organization.com)

Distinguished Name - CN=User Name, OU=Dallas, DC=Organization, DC=com

Common Name - User Name

Universal Principal Name - username@organization.com

sAMAccountName - username

User Type - possible values are AD or local

Last Modified - Date/time stamp

Last Reconciled - Date/time stamp

User Endpoints

This page displays information about a user's endpoints, listed by platform type. Endpoint categories include Shielded, Mobile Device, and Cloud endpoints.

1. In the left pane, click **Populations > Users**.
2. Search or select a User Name, then the **Endpoints** tab.

Shielded

Platform - The platform type

Device Id - Value that uniquely identifies the target device

Last Successful Login - Date/timestamp, per endpoint

Last Unsuccessful Login - Date/timestamp, per endpoint

Last Gatekeeper Sync - Date/timestamp, per endpoint

Effective Policies - Click **view** for a simple layout view of the effective endpoint policies

Actions - Click **Recover** to proceed to the Recover Data page

Last Encryption Sweep Start - Date/timestamp, per user

Sweep End - Date/timestamp, per user

Encryption Failure - Click **view** for a simple list of files that could not be encrypted, per user

States (Date/timestamp, per endpoint):

Policy Updating

User Encryption Profile Updating

EMS Encryption Profile Updating

User Data Encryption On

Deactivation Pending

Suspension Pending

Suspended

Mobile Device

Platform - The platform type

Device Id - Value that uniquely identifies the target device

Effective Policies - Click **view** for a simple layout view of the effective endpoint policies

Cloud

Platform - The platform type

Device Id - Value that uniquely identifies the target device

User Groups

If the user belongs to a User Group, this page displays information about the group and provides a link to the group.

1. In the left pane, click **Populations > Users**.
2. Search or select a User Name, then the **Users Groups** tab.

User Group - Group to which the user belongs

Distinguished Name - CN=Group1, OU=Dallas, DC=Organization, DC=com

CN is the common name

OU is the organizational unit name

DC are domain components

Common Name - non-technical name of the user group

User Admin

This page allows you to assign, modify, or view Administrator roles for the user.

1. In the left pane, click **Populations > Users**.
2. Search or select a User Name, then the **Admin** tab.

Administrator Roles - Assign or modify roles for the user and click **Save**.

Inherited Group Roles - A read-only list of roles that the user inherited from a group. To modify the roles, click the **User Groups** tab for that user and select the Group Name.

Delegated Roles - Delegate Administrator rights to a User.

Related topics:

Administrator Roles

Assign or Modify Administrator Roles

Delegate Administrator Roles

View Reconciliation Date

To view the date and time a User Group's or User's information was last reconciled with Active Directory, click the Details & Actions tab for the Group or User, and refer to Last Reconciled. For instructions, refer to View or Modify User Group Policies and Information and View or Modify User Policies and Information.

View Policy Proxy State

The Remote Management Console tracks the Policy Proxy's Policy Updating state.

1. In the left pane, click **Populations > Endpoints**.
2. Select an endpoint type, for example, **Workstation** or **Mobile Device**.
3. If you know the full Hostname of the endpoint, enter it into the Search field and click the **Search** icon.

For Windows and Mac, enter the full Hostname of the endpoint if you know it. However, you may leave the field blank to display all Windows and Mac endpoints.

For Mobile devices, optionally enter the user's email address.

If you do not know the full Hostname or user email address, scroll through the list of available endpoints to locate the endpoint.

4. Click an endpoint in the list to display the Endpoint Detail.
5. Click the **Details & Actions** tab of the endpoint for which you want to view information.

Issue a User Decryption Policy

1. In the left pane, click **Populations > Users**.
2. Click a User Name link or search for a user and then click a link to display the User Detail.

   To Search, you can enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character (*) may be used but is not required at the beginning or end of the text.
3. On the **Security Policies** tab, click **Policy-Based Encryption**.
4. Set the value of *Policy-Based Encryption* to **Off**.
5. Click **Save**.
6. Commit Policies.

   Once this policy reaches the specified Shield, decryption begins.

Endpoint Groups

Endpoint Groups

On the Endpoint Groups page, you can add an endpoint group or search and select an endpoint group to View or Modify Endpoint Group Information.

Types of Endpoint Groups

System - Endpoint group maintained by Dell Server. System groups include Default Endpoint Group, Opt-In Endpoint Group, Persistent VDI Endpoint Group, and Non-Persistent VDI Endpoint Group. For more information about VDI Endpoint Groups, see VDI Endpoint Groups.

Rule-Defined - Dynamic endpoint group based on a Specification, or rule set, defined by the administrator.

Admin-Defined - Static endpoint group for which the administrator can select specific endpoints for inclusion. The group remains unchanged unless the administrator adds or removes an endpoint.

Add an Endpoint Group

Before you add the first Endpoint Group see Endpoint Groups Specification, which explains fields and expressions used in Group Specifications.

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click **Add**.
3. In the *Select the type of Endpoint Group* field, select **RULE-DEFINED Group** or **ADMIN-DEFINED Group**.
4. In the *Group Name* field, enter a name for the new endpoint group.
5. In the *Description* field, enter a description for the new endpoint group.

6. (For Rule-Defined Groups only) In the *Specification* field, enter the rule that describes the endpoint group. Specifications can be up to 4000 characters. Specifications are case insensitive.
7. Click **Preview** to view the endpoints to be included in the group.
8. Click **Add Group** to save the group definition.

Endpoint Groups Specification

To skip to instructions about how to add an endpoint, see Add Endpoint Groups.

At deployment time, all endpoints belong to a default endpoint group, which is generally sufficient for most deployments. This feature is used to assign policy to a specific group of endpoints. For instance, you may want to create an endpoint group based on the locale that the operating system sends up in inventory. Once that endpoint group is established, you could then apply a specific policy set to just the endpoints in your specified locale.

Conversely, creating an endpoint group based on a platform type would not be useful because policies are already grouped by platform.

Endpoint groups are created using a group specification. This specification allows you to define the endpoint characteristics used to add endpoints to a group. You cannot manually add endpoints to endpoint groups. The system, based on the characteristics in the endpoint group specification, automatically manages endpoints and endpoint group membership.

Endpoints can be members of many endpoint groups simultaneously, as there is no mutual exclusion requirement for endpoints in groups. All endpoints are included in the default endpoint group in addition to any defined endpoint groups that they may be a member of. This is similar to the way users are a member of the domain they are a part of, in addition to any security groups. Like the user group mapping, the endpoint group mapping creates a potential policy arbitration problem for endpoints. To resolve this problem, the default endpoint group has the lowest possible precedence, and cannot be altered. The endpoint groups that you create have medium precedence by default. For more information on group precedence, see Modify Group Precedence.

Endpoint Group Specification

The endpoint group specification is a domain specific language that allows you to define groups. The endpoint group specification consists of a set of operators and a set of data fields that these operators can be applied to. A group specification is a Boolean expression that is evaluated per endpoint to determine whether or not a endpoint is a member of a group.

The information obtained to assign endpoints to endpoint groups happens when inventory is received, not at activation time. If you set up endpoint groups, all endpoints will stay only in the default endpoint group until inventory is received.

Group specifications are created using the following fields and expressions. Multiple fields and operators can be used in a single group specification.

Field Name	Description
CATEGORY	Endpoint category: WINDOWS, MAC, SED Dell Data Protection | Mobile Edition is not available for use in the Endpoint Groups feature.
UID	Windows hostname
DISPLAYNAME	Fully qualified hostname
OSVERSION	Operating system version as reported in inventory. We recommend using other available fields, as discrepancies in operating system versions may reduce the usefulness of this field.

OS	Operating system name as reported in the endpoint's inventory
PROCESSOR	System processor information
SERIALNUMBER	Endpoint serial number
LOCALE	The current locale of the endpoint. This is typically only reported by Enterprise Edition for Windows.
WINCOMPUTERNAME	Fully qualified hostname
ASSETTAG	Asset tag of the computer manufacturer
PLUGINVERSION	Plugin version for Manager
CLOUDPRESENT	All Cloud clients
CLOUDINTERNAL	Internal Cloud clients
CLOUDEXTERNAL	External Cloud clients
SEDPRESENT	All SED clients
BITLOCKERPRESENT	TRUE/FALSE value for BitLocker Manager, indicating if BitLocker is enabled.
TOTALMEMORY	Total memory available on the system

Operators and Expressions

The basic operators are the binary operators that return a Boolean value.

Operator	Meaning
=	Boolean, Integer, and String equality operator
>, >=	Greater than, greater than or equal, integer operator
<, <=	Less than, less than or equal, integer operator
<>	Not equal, integer string operator
AND	Logical AND for Boolean expression
OR	Logical OR for Boolean expression
NOT	Logical NOT for Boolean expression

The logical operators follow the standard Boolean operator precedence (NOT, AND, OR). String fields have the following string operators that return Boolean values:

BEGINSWITH

ENDSWITH

CONTAINS

These operators can be used on the string fields:

```
UID BEGINSWITH "A1850502"
```

```
ASSETTAG CONTAINS "007"
```

String fields also have the following string operators that return substrings of the field:

LEFT(string,int)

RIGHT(string,int)

MID(string,int,int)

The substring operators can be used in the string operators that return Boolean values:

```
LEFT(DISPLAYNAME, 4 ) = "A185"
```

There is one additional string operator that returns an integer value that is the length of the string:

LEN(string)

This can be used in a Boolean expression:

```
LEN(DISPLAYNAME)<=10
```

Group specifications are created using the fields and expressions described in the previous sections. Multiple fields and operators can be used in a single group specification. For example, a group for WINDOWS devices, with a hostname that started with 'FOO' that also had Hardware Crypto Accelerator cards would be:

```
UID BEGINSWITH "A1850502" AND LEFT(DISPLAYNAME, 4 ) = "A185"

UID BEGINSWITH "A1850502" AND LEFT(DISPLAYNAME, 4 ) = "A185" AND LEN(UID) >= 20

UID BEGINSWITH "A1850502" AND LEFT(DISPLAYNAME, 4 ) = "A185" OR ( LEN(UID) >= 20
AND BITLOCKERPRESENT)
```

- Using the FQDN of the client computer to attach it to a device group can be done by keying on any commonality amongst the desired client computers. In the example below, we have a child domain of ORGANIZATION, called AMERS to represent a domain in America. Additionally we have a 2nd child domain EMEA representing non-American based clients.

  DISPLAYNAME ENDSWITH "AMERS.ORGANIZATION.COM"

  This group will contain all clients that are in the AMERS domain according to their FQDN.

  DISPLAYNAME ENDSWITH "EMEA.ORGANIZATION.COM"

  This group will contain all clients that are in the EMEA domain according to their FQDN

- If the hostname of the client computers contain several notations that indicate desired ways in which to create a group, those specific portions can be captured as long as their location is consistent.

  Looking at the hostname: A12345jdoe.AMER.ORGANIZATION.COM

  A denotes an asset, while the following 5 digits denotes the asset's assigned value. The user that was assigned the asset has their SAM account appended to the end.

  You can capture the assigned number of the asset, and that it is within a certain subsection of assets. This example shows how to look for assets that have a value less than 1000.

MID(DISPLAYNAME , 2, 5) < 1001

This example targets user's machines where their last name begins with 'r'.

MID(DISPLAYNAME , 8, 1) = "r"

- Example for Dell Data Protection | Cloud Edition:

  To display Cloud internal clients, add the specification "cloudpresent and cloudinternal".

  To display Cloud external clients, add the specification "cloudpresent and cloudexternal".

For instructions about how to add an endpoint, see Add Endpoint Groups.

Modify Group Precedence

Note: Precedence of VDI Endpoint Groups (Non-Persistent and Persistent) is set at **Max**. This level ***must*** remain at **Max** precedence. Ensure that policies for VDI Endpoint Groups are set according to Policy and Configuration Requirements for VDI Endpoint Groups.

The Group Precedence feature is used to determine policy arbitration for effective policies that include multiple groups. Group precedence creates a weight associated with the specific group it is assigned to, and that weight is used in policy arbitration for all policy overrides. Policy overrides are used from the group with higher precedence when two (or more) separate groups in a policy arbitration map have different precedence. Normal per-policy arbitration takes place when all groups in a policy arbitration map have the same precedence.

For a specific User Group or Endpoint Group to carry the highest weight, set the precedence to Max. Conversely, set the precedence to Min for the specific group to carry the lowest weight. The default value for User Groups is Min. The default value for Endpoint Groups is Medium.

To change Group Precedence:

1. In the left pane, click **Populations > Endpoint Groups** (or **User Groups**).
2. Select the appropriate group.
3. In the Precedence drop-down on the Securities Policies tab, select either Max, High, Medium, Low, or Min. Selecting Max gives this group the highest weight for policy arbitration. Selecting Min gives this group the least weight for policy arbitration.
4. Click **Save**.
5. Click **Management > Commit**.
6. Enter a description of the change in the Comment field.
7. Click **Commit Policies**.

View Endpoints in an Endpoint Group

This page displays the endpoints included in information for every user of the specified endpoint.

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click a Group Name link or enter a filter to search for available Groups.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.

   When you click a Group Name, the Endpoint Group Detail page displays.
3. If applicable, View or Modify Endpoint Information.

View or Modify Endpoint Group Policies and Information

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click a Group Name or enter a filter to search for available Endpoint Groups.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.

   When you click a Group Name, the Endpoint Group Detail page displays.
3. Click the tab that corresponds with the action you want to perform:

   Security Policies - To view or modify policies of the Group, click **Security Policies**.
   Note: Before modifying VDI Endpoint Group policies, see Policy Requirements for VDI Endpoint Groups.

   Details & Actions - To view properties of the Group, click **Details & Actions**. Viewable information includes:
   Group Name: Group1 (Domain\Group1)
   Description: The Description provided when the Group was added.
   (For Rule-Defined groups) Specification: The endpoint group specification that defines endpoints as members of the group.
   SED Device Control - The SED Unlock command for this endpoint group is carried out in the SED Device Control area. This command unlocks the PBA screen after it has been locked – either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

   Members - To view or modify the information of an Endpoint in the Group, click **Members**. The list of Endpoints in the Group displays. Click an Endpoint to view the Endpoint's Security Policies, Details & Actions, Users, Endpoint Groups, Threat Events, and Advanced Events.
4. If modified, click **Save**.

Endpoint Group Details & Actions

This page lists the properties of the selected Endpoint Group.

1. In the left pane, click **Populations > Endpoint Groups**.
2. Search or select a Group Name, then the **Details & Actions** tab.

Details:

Group Name of the endpoint group

A description of this endpoint group

The specification that was used to create this endpoint group (applies only to Rule-Defined groups)

SED Device Control

The SED Unlock command for this endpoint group is carried out in the SED Device Control area. This command unlocks the PBA screen after it has been locked – either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

Endpoint Group Members

This page lists the endpoints within an endpoint group. Information displays based on the group specification used to create the endpoint group.

1. In the left pane, click **Populations > Endpoint Groups**.
2. Search or select a Group Name, then the **Members** tab.

Category - WINDOWS, MAC, or SED (Mobile Edition is not available for the Endpoint Groups feature.)

Display Name - Hostname of the endpoint

Endpoints

Endpoints

On the Endpoints page, you can remove an endpoint or search and select an endpoint to View or Modify Endpoint Information.

Click a Hostname to view details about the endpoint. Click an arrow next to a Hostname to view the Category, Unique ID, and Processor.

Add Endpoints

An endpoint is added to inventory when a user who is in the Dell database activates the endpoint.

If the user is not found in the VE Server database, they will be located in Active Directory.

Remove Endpoints

Endpoint removal is permanent. Once an endpoint is removed, the action cannot be undone.

To remove an endpoint:

1. In the left pane, click **Populations > Endpoints**.
2. Select the appropriate endpoint type, for example, **Workstation** or **Mobile Device**.
3. Click a Hostname or Endpoint Serial Number in the list or enter a filter to search for available endpoints.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.

   For Windows and Mac, if you know the Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Windows and Mac endpoints.

   For Mobile devices, optionally enter the model name or user's email address.
4. Select a row to highlight it.
5. At the top left, click **Remove**.
6. Click **OK** to confirm that you want to remove the endpoint.

   Note: As another option, click an endpoint link and select the **Details & Actions** tab. Under Endpoint Detail, click **Remove**.

Find Endpoints

1. In the left pane, click **Populations > Endpoints**.
2. Select the appropriate endpoint type, for example, **Workstation** or **Mobile Device**.
3. Click a Hostname or Endpoint Serial Number in the list or enter a filter to search for available endpoints.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.

   For Windows and Mac, if you know the Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Windows and Mac endpoints.

   For Mobile devices, optionally enter the model name or user's email address.

View or Modify Endpoint Policies and Information

1. In the left pane, click **Populations > Endpoints**.
2. Select the appropriate endpoint type, for example, **Workstation** or **Mobile Device**.
3. Click a Hostname or Endpoint Serial Number in the list or enter a filter to search for available endpoints.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.

   For Windows and Mac, if you know the Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Windows and Mac endpoints.

   For Mobile devices, optionally enter the model name or user's email address.

   When you click a Hostname or Endpoint Serial Number, the Endpoint Detail page displays.
4. Click the tab that corresponds with the action you want to perform:

   Security Policies - To view or modify policies of the endpoint, click **Security Policies**.

   Details & Actions - To view properties of the endpoint, including Inventory Information, click **Details & Actions**. Viewable information includes hardware information, effective policies, inventory and protection status, threat protection and Advanced Threat Prevention detail, and SED Device Control commands.

   Users - To view a list of users who store and access data on the endpoint, click **Users**. These statistics of endpoint users may be available on the Endpoint Detail page: Login, Last Gatekeeper Sync, Effective Policies, and States. You can also recover data from this page.

   Endpoint Groups - To view a list of Endpoint Groups to which this endpoint belong, click Endpoint Groups. All endpoint belong to at least one endpoint group, the Default Endpoint Group.

   Threat Events - To view information about threat events on the endpoint, click **Threat Events**. The following information is displayed for events: Severity, Category (Malware, Web Filtering, Web Protection, and Firewall), Event ID, Event Description, User Name, and Received time stamp.

   Advanced Events - To view, export, quarantine, or waive unsafe files, click **Advanced Events**. Events are grouped by Status (Unsafe, Quarantined, or Abnormal), and the following information is displayed for events: File Name, File Paths, Score, Classification, First Found time stamp, Running, Auto Run, and Detected By.
6. If modified, click **Save**.

View Effective Policy

When you view Effective Policies, you are viewing the policies and settings that are enforced on an endpoint.

1. In the left pane, click **Populations > Endpoints**.
2. Select the appropriate endpoint type, for example, **Workstation** or **Mobile Device**.
3. Click a Hostname or Endpoint Serial Number in the list or enter a filter to search for available endpoints.

   Note: The wildcard character (*) may be used but is not required at the beginning or end of the text.

   For Windows and Mac, if you know the Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Windows and Mac endpoints.

   For Mobile devices, optionally enter the model name or user's email address.

   When you click a Hostname or Endpoint Serial Number, the Endpoint Detail page displays.

5. On the Endpoint Detail page, click the **Details & Actions** tab.
6. Under Manager Detail, click **View Effective Policies**.

Related topics:

Manage Security Policies

Endpoint Details & Actions

The Details & Actions page lists the details for the selected endpoint as well as commands, such as Remove Endpoint. Available details and commands vary, depending on the endpoint platform.

To access Endpoint Details & Actions, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a Hostname, then the **Details & Actions** tab.

Endpoint Detail

Command:

Click the **Remove** link to remove this endpoint.

Note: Endpoint removal is permanent. Once an endpoint is removed, the action cannot be undone.

Details:

Windows

Category - Windows

OS/OS Version - Example: Microsoft Windows 10 Enterprise

Processor

Serial Number - Manufacturer assigned serial number

Unique ID - Dell assigned unique identifier

Protected - Date and time stamp

Mac

Category - Mac

OS/OS Version - Example: Mac OS X 10.11.0

Processor

Serial Number - Manufacturer assigned serial number

Unique ID - Dell assigned unique identifier

Protected - Date and time stamp

Mobile Device

Category - Mobile Device

OS/OS Version - Example: Lollipop / 5.0

Model Name - Examples: Android or iPad

Serial Number - Manufacturer assigned serial number

Last Contact Time - Date and time stamp of last contact with DDP Server

State:

Discovered – device found

Blocked – block from Exchange access

Blocked Sub-States (on the Endpoint Detail page):

Blocked by Admin – (EAS only) blocked by administrative override using the Block Device command

Blocked by Policy – (EAS or iOS) subject to the Allow iOS Devices and Allow Non-iOS Devices policies.

Pending – iOS policy pending

Protected – policies implemented

Cloud

Category - Windows, iOS, or Android

OS/OS Version - Examples:

Windows 10

Android / 5.0

iPhone OS / 8.0

Model ID - Examples: iPhone6, or iPad3,4

Model Name (if available)

Phone ESN/IMEI (if available)

Processor (will display if the data is available)

Memory available and total (MBs) (will display if the data is available)

Battery remaining% (will display if the data is available)

Serial Number - Manufacturer assigned serial number

Unique ID - Dell assigned unique identifier

Actions - Hide or Remove Endpoint

Shield Detail

Commands:

To view the policies of the endpoint, click **View Effective Policies**.

Obtain the endpoint's recovery keys:

1. Click **Device Recovery Keys**.
2. Enter a Recovery Password and click **Download**.

The recovery bundle containing this endpoint's encryption keys is downloaded. You must remember the Recovery Password to access the recovery keys.

Detail:

Windows

Policy Proxy Group (typically CMGREMOTE)

Recovery ID of the specific endpoint

Version (core/edition)

Activation Method (typically Mandatory)

HCA Enabled: True or False

TPM Present: True or False

Edition: Dell or CREDANT

States:

- Policy Updating: Date and timestamp
- Device Encryption Updating: Date and timestamp
- Device Data Encryption On: Date and timestamp
- Sweep Started: Date and timestamp
- Sweep Completed: Date and timestamp
- Inventory Received: Date and timestamp
- Inventory Processed: Date and timestamp
- Manager Inventory Received: Date and timestamp
- Manager Inventory Processed: Date and timestamp
- Protected:
  - Protection Status Tab:
    - Disk Name
    - Capacity (storage)
    - Protection Status (Protected, Protecting, Unknown)
    - Interface type
    - Model number of the endpoint
  - GPE Tab:
    - GPE Available (True or False)
    - GPE Driver Version
    - GPE Functional (True or False)
    - GPE Lifecycle Remaining (number)
    - GPE Lifecycle Owner Remaining (number)
    - GPE Provisioned Status
  - TPM Tab:
    - TPM Present (True or False)
    - TPM Activated (True or False)

TPM Owned (True or False)

TPM Functional Status (True or False)

TPM Spec Version (version number)

HCA Tab:

HCA Functional Status

HCA Provision State

Preboot Present (True or False)

Preboot Set (True or False)

Actions: Effective policies on the specific endpoint and Recovery Keys for the specific endpoint

---

Mac

Policy Proxy Group (typically CMGREMOTE)

Recovery ID of the specific endpoint

Version (core/edition)

Activation Method (typically Mandatory)

Edition (Dell or Credant)

States:

Policy Updating: Date and timestamp

Device Encryption Updating: Date and timestamp

Device Data Encryption On: Date and timestamp

Sweep Started: Date and timestamp

Sweep Completed: Date and timestamp

Inventory Received: Date and timestamp

Inventory Processed: Date and timestamp

Protected:

Protection Status Tab:

Disk Name

Capacity (storage)

Protection Status (Protected, Protecting, Unknown)

Interface type

Model number of the endpoint

Actions: Effective policies on the specific endpoint and Recovery Keys for the specific endpoint

---

Manager Detail (Windows only)

Command:

Click **View Effective Policies** to go to the effective policy page for this endpoint.

States

The client gathers the following information via a Windows Management Instrumentation (WMI) call to the Operating System. It is updated with each inventory update.

Inventory Received - the date and time that the inventory was received by the Enterprise Server and placed in the queue.

Inventory Processed - the date and time that the inventory was picked up from the queue and processed (**Note**: If the Server is under load, the Processed and Received times may be different, but usually they will be the same.)

Agent Version - the version of Manager the endpoint is running.

Protected - Summarizes the protection status of the disk.

Protection Status

Disk - number of the disk

Partitions - number of partitions the disk has

Capacity - capacity of the disk

Protection Status - Protected or unprotected

Interface - Disk interface (Examples: IDE, SATA)

Model - Manufacturer name and model of the disk

Click the small black arrow on the left to expand the disk details to view information for each partition of the disk.

Logical Disk - The name of the logical disk.

ID - The identifying number of the logical disk.

Encryption % - The percentage of the partition that has been encrypted.

Capacity - The capacity of the partition.

Protection Status - Protection status for the partition: Protected, Unprotected, Locked

Providers

Agent - SED, Authentication Proxy, Preboot Authentication, Windows Authentication, HCA, BitLocker, TPM, Threat Protection, Advanced Threat Prevention

Plugin Functional Status (green check mark or red "x") - This indicates whether the Agent has been enabled via policy. To get more detail on whether each plugin is working as expected, look at Plugin State column.

Plugin State:

- BitLocker Plugin:

  Starting - Manager is starting up. Because this is a fairly quick process, it is unlikely an inventory update would capture this so you would probably never see this state in the Enterprise Server Console.

Disabled - Manager is disabled by policy and not enforcing any previously received policy.

Active - Manager is running normally and enforcing policies.

No Policy - Initial policy has not been received so the plugin is not actively enforcing any policy. This is only relevant the very first time you install the Manager client. Manager will not start a plugin until an initial policy is received from the VE Server, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from the VE Server, via the activation process, plugins are always started with the last policy the client is aware of.

OpSys Not Supported - Manager does not support this operating system. Manager is not actively enforcing policy related to this plugin, due to this plugin-specific exception.

- TPM Plugin:

Starting - Manager is starting up. Because this is a fairly quick process, it is unlikely an inventory update would capture this so you would probably never see this state in the Enterprise Server Console.

Disabled - Manager is disabled by policy and not enforcing any previously received policy.

Active - Manager is running normally and enforcing policies.

TPM Services Not Started – In the Enterprise Server Console this is listed as *TPM Base Services Failed*. It means something is preventing the TPM service from starting as expected. The Manager is not actively enforcing policy related to this plugin, due to this plugin-specific exception.

No TPM Device – The TPM device is not present or is not detectable in the indicated computer. The Manager is not actively enforcing policy related to this plugin, due to this plugin-specific exception.

No Policy - Initial policy has not been received so the plugin is not actively enforcing any policy. This is only relevant the very first time you install the Manager client. Manager will not start a plugin until an initial policy is received from the VE Server, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from the VE Server, via the activation process, plugins are always started with the last policy the client is aware of.

- SED Plugin:

Initialized - Manager is initialized waiting for delayed startup

Starting - Manager is starting up. Because this is a fairly quick process, it is unlikely an inventory update would capture this so you would probably never see this state in the Enterprise Server Console.

Disabled - Manager is disabled by policy and not enforcing any previously received policy.

Active - Manager is running normally and enforcing policies.

No Policy - Initial policy has not been received so the plugin is not actively enforcing any policy. This is only relevant the very first time you install the Manager client. Manager will not start a plugin until an initial policy is received from the VE Server, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from the VE Server, via the activation process, plugins are always started with the last policy the client is aware of.

Waiting For Escrow - Manager is waiting for keys to escrow

Waiting For Server Public Key - Manager is waiting for public key to proceed with activation

No Opal Drive Present - Manager did not detect an OPAL drive

Plugin Version - The version of the plugin, which is taken from the plugin's version information

Vendor version - The version of the underlying framework. For example, BitLocker is Microsoft's technology, therefore Vendor Version is Microsoft's version for BitLocker.

Threat Protection Detail (Windows only)

Scan Engine Version - Lists the version of the engine that performed the last scan.

DAT File Version - Lists the version of the DAT file.

Last Scan Started - Date/time stamp that the last scan was started.

Last Scan Completed - Date/time stamp that the last scan was completed.

Advanced Threat Prevention Detail

Device ID - Lists the identifier of the device as it pertains to Advanced Threat Prevention.

Agent Version - Lists the version of the agent.

Update Date - Date/time stamp that the agent was updated.

Provisioned Date - Date/time stamp that the client was provisioned.

Mobile Device Detail

For Mobile devices, once a device is discovered, commands are carried out on this page. Unlike policies and restrictions that are concerned with enforcement, commands are pushed to the device to enable an action.

Commands:

<table>
<tr><th>Command</th><th>Sent</th><th>Sender</th><th>Acknowledged</th><th>Error</th></tr>
<tr><td>Wipe Device – (shared iOS and EAS command) To permanently delete all media and data on the device and restore it to factory settings, iOS can remotely wipe iPhone and iPad. This is primarily to support a quick remote wipe operation.</td><td rowspan="3">Date and timestamp of when the command was sent.</td><td rowspan="3">Name of the sender that sent the command.</td><td>Date and timestamp of when the command was implemented on the endpoint.</td><td rowspan="3">Used for internal troubleshooting.</td></tr>
<tr><td>Block Device – (EAS only command) You can send an administrative override to the device to immediately block Exchange services. This command is independent of policy values. Date and timestamp of when the Policy Proxy sent the command to the endpoint.</td><td>Date and timestamp of when the command was implemented on the endpoint.</td></tr>
<tr><td>Allow Device – (EAS only command) This command reverses the Block Device command. Once a device is blocked by your administrative override, the only way to restore access to Exchange services is to invoke this command. This command is also independent of policy values. For example, if you have set the Allow Non-iOS Devices policy to False, invoking this command has no effect.</td><td>Date and timestamp of when the Policy Proxy sent the command to the endpoint.</td></tr>
</table>

Cloud Device Control

Cloud device commands apply to the selected endpoint and are carried out from the Cloud Device Control section of the device's endpoint page. Unlike policies, commands are pushed to the device to enable an action.

Commands:

Suspend - Suspends the endpoint device. It does not suspend the user account.

Unsuspend - Unsuspends the endpoint device.

SED Device Control (Windows only)

Current State of the Endpoint - Unlocked or Locked

Commands:

SED commands for a specific endpoint are carried out in the SED Device Control area. Each command has a priority ranking. A command with a higher priority rank cancels commands of lower priorities in the enforcement queue. For a list of command priority rankings, see Priority of Commands for Self-Encrypting Drives.

Lock - Locks the PBA screen and prevents any user from logging into the computer.

Unlock - Unlocks the PBA screen after it has been locked on this endpoint, either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

Remove Users - Removes all users from the PBA.

Bypass Login - Bypasses the PBA screen one time to allow a user into the computer without authenticating. The user will still need to login to Windows after PBA has been bypassed.

Wipe - The Wipe command functions as a "restore to factory state" for the SED drive. The Wipe command can be used to re-purpose a computer or, in an emergency situation, wipe the computer, making the data permanently unrecoverable. When the wipe command is consumed by the client, all history and details about this endpoint are removed from the EE/VE Server. Ensure that this is the desired behavior before invoking this command.

The SED Device Control Table

The table lists the commands most recently sent to the SED Device.

To sort the table, click a column header.

Endpoint Users

This page displays information for every user of the specified endpoint. The user information differs for each technology group or policy category.

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a Hostname, then the **Users** tab.

Shielded

User - Each user on the specific endpoint

Last Successful Login - Date/timestamp, per user

Last Unsuccessful Login - Date/timestamp, per user

Last Gatekeeper Sync - Date/timestamp, per user

Effective Policies - Click **view** for a simple layout view of the effective user policies

Actions - Click **Recover** to proceed to the Recover Data page

Last Encryption Sweep Start - Date/timestamp, per user

Sweep End - Date/timestamp, per user

Encryption Failure - Click **view** for a simple list of files that could not be encrypted, per user

States (Date/timestamp, per user):

Policy Updating

User Encryption Profile Updating

EMS Encryption Profile Updating

User Data Encryption On

EMS Data Encryption On

Deactivation Pending

Suspension Pending

Suspended

Cloud

User - Each user on the specific endpoint

Endpoint Groups

This page lists the Endpoint Groups to which an endpoint belongs.

Endpoint Group - Name of the group to which this endpoint belongs. All endpoints belong to at least one endpoint group, the Default Endpoint Group.

Description - Describes the group.

To view Endpoint Groups of an endpoint, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a Hostname, then the **Endpoint Groups** tab.

VDI Endpoint Groups

Upon activation, a VDI endpoint is added to the appropriate VDI Endpoint Group on Dell Server, and policies are sent to the endpoint. Persistent VDI Endpoint Groups and Non-Persistent VDI Endpoint Groups are System Endpoint Groups, which are maintained by Dell Server.

Policy settings differ, based on whether persistent or non-persistent VDI is deployed in the environment. For an explanation of the differences between persistent and non-persistent VDI, see Persistent vs. Non-Persistent VDI.

Policy and Configuration Requirements for VDI Endpoint Groups

The policy requirements below are for VDI endpoints running Advanced Threat Prevention. The list includes only policies that are significant for VDI endpoints. VDI User policy settings must also meet certain requirements. See Policy and Configuration Requirements for VDI Users.

Note: Ensure that you turn off Advanced Threat Prevention Agent Auto Update. In the left pane of the Remote Management Console, select **Management > Services Management > Advanced Threats - Agent Auto Update**, then select **Off**.

Note: With Persistent VDI Groups, ensure that roaming user profiles are configured.

These policy and configuration settings for VDI Endpoint Groups must be configured before VDI client activation:

Technology	Category	Policy or Setting	Persistent VDI Group setting	Non-Persistent VDI Group setting

Windows Encryption	Self-Encrypting Drive (SED)	Self-Encrypting Drive (SED)	Off	Off
Windows Encryption	Hardware Crypto Accelerator (HCA)	Hardware Crypto Accelerator (HCA)	Off	Off
Windows Encryption	Policy-Based Encryption	SDE Encryption Enabled	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Common Encrypted Folders	<retain default settings>	<retain default settings>
Windows Encryption	Policy-Based Encryption	Encrypt Windows Paging File	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Secure Windows Credentials	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Block Unmanaged Access to Domain Credentials	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Secure Windows Hibernation File	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Prevent Unsecured Hibernation	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Enable Software Auto Updates	Not Selected	Not Selected
Windows Encryption	BitLocker Encryption	BitLocker Encryption	Off	Off
Windows Encryption	Server Encryption	Server Encryption	Off	Off
Threat Prevention	Advanced Threat Protection	Advanced Threat Protection	On	On
Removable Media Encryption	Mac Media Encryption	Mac Media Encryption	Off	Off
Port Control	Windows Port Control	Port Control System	Disabled	Disabled

Endpoint Threat Events

This page lists information on threat events for the selected endpoint.

1. In the left pane, click **Populations > Endpoints > Workstation**.
2. Search or select a Hostname, then the **Threat Events** tab.

Threat Event Data

Severity - Severity of the threat, where Critical is the most dangerous threat to the endpoint, and Information is just a notification of an event that is unlikely to harm the endpoint. (Critical, Major, Minor, Warning, Information)

Category - Category of the threat. Upon identification, threats are sorted into these categories: Malware, Web Filtering, Web Protection, and Firewall.

Event ID - Unique number assigned to each threat event.

Description - Description of the last preventative action taken to handle the threat.

User Name - The domain\user name associated with the endpoint where the threat was identified.

Received - Date/timestamp when the last action was taken to handle a threat.

Navigate the Threat Event Data

To sort the data, click a column header.

Use the controls at the bottom of the page to:

- Advance to the top of the data.
- Go back one page.
- Go forward one page.
- Advance to the end of the data.
- Increase or reduce the items per page.
- View the range of items currently displayed.
- Refresh the data.

Endpoint Advanced Threats

This page allows you to view, export, quarantine, or waive unsafe files that trigger events on the selected endpoint.

An event is not necessarily a threat. An event is generated when a recognized file or program is quarantined, safe listed, or waived. Threats are a category of events that are newly detected as potentially unsafe files or programs and require guided remediation.

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a Hostname, then the **Advanced Events** tab.

List of Events

The list presents all files that have triggered events found on this device.

Columns

- Icon - An icon appears in this column, when available.
- Name - File triggering the event.
- File Paths - The location of the file on the device.
- Cylance Score - A score is assigned to each file that is deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.
- Status - Indicates whether the file has been quarantined or waived.
- Classification - Classification of the threat: High, Medium, or Low. For details, see Advanced Threat Protection Classifications.
- First Found - Date/timestamp that the file was first found.
- Running - Indicates whether the file that triggered the event is running or not.
- Auto Run - Indicates whether the file was set to automatically run upon startup.
- Detected By - Indicates whether the file was detected by Execution Control or by Memory Protection.

Configure the Threat List

Add or Remove Columns

Click an arrow next to any column header and select **Columns** to add columns to, or remove columns from, the table.

Filter on Column Data

To filter the list based on column data, click the down-arrow on any column to display the context menu, and select **Filter**.

The filter options vary, depending on the type of data in the column. For example, you may want to filter the list so that it shows only high priority threats.

Group by a Column

Drag a column header, such as Status, to the area directly above the column headers to group the data by Status. When you drag a column header, it turns green, indicating that the table can be grouped by that data. You can drag additional headers over the table to group the data even further.

For each group, a number appears in parentheses to indicate the total number of threats that share that group's attribute.

Commands:

Select the check box of next to a file name to perform an action on the file. To select all files, select the check box in the column heading row.

The **Export** button lets you export selected data to a .CSV file so that you can view the data in Excel or a similar application which has powerful sorting/organizing features.

After selecting the data you want to export, click **Export** to save the data in a .CSV file.

Click **Quarantine** to add the file to the Quarantine list.

Quarantining a file will prevent the file from being executed on this device.

Note: Quarantining a file will move the file from its original location to the Quarantine directory (C:\ProgramData\Cylance\Desktop\q).

Click **Waive** to allow the file to run on this device.

Note: Occasionally, a “good” file could be quarantined or reported. This could happen if the features of that file strongly resemble those of malicious files. Waiving or globally safe listing the file can be useful in these instances.

Exploit Attempts

This section lists the detection of attempts to exploit running processes, or malware that executes from within memory space.

A number displays the total number of events, followed by the number in each subcategory.

Checkbox - Select all events by selecting the check box in the column heading row, or select individual events. When you click a box, Quarantine and Waive are activated.

Added - Date and time when the exploit attempt was added.

Process Name - Name of the process identified as an exploit attempt.

Process ID - Unique number associated with the exploit attempt.

Type - Type of memory exploit: Exploitation, Process Injection, Escalation.

Action - Action taken to protect the system from the exploit attempt:

- Ignore - The agent will not take any action against identified memory violations.
- Alert - The agent will record the violation and list the incident on this page.
- Block - If an application attempts to call a memory violation process, the agent will block the process call. The application that made the call is allowed to continue to run.
- Terminate - If an application attempts to call a memory violation process, the agent will block the process call and will also terminate the application that made the call.

User Name - Name of the user who was logged in when the exploit attempt was identified.

Endpoint Advanced Threat Events

The Advanced Threat Events tab displays if the Advanced Threat Prevention service is provisioned and Advanced Threat Prevention is enabled on the endpoint.

The tab displays information about events for the endpoint based on information available in the Dell Data Protection Server.

To access the Enterprise Advanced Threats tab, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a Hostname, then the **Advanced Threat Events** tab.

Use the following filters to select content to display on the Advanced Threat Events tab:

Type - Threat Found, Threat Blocked, Threat Terminated, Memory Violation Blocked, Memory Violation Terminated, Memory Violation (Detected), Threat Removed, Threat Quarantined, Threat Waived, Threat Changed, Protection Status Changed.

Severity - Severity level of the event: Critical, Major, Minor, Warning, or Informational.

Timeframe (in days) - 1, 7, 14, 30, 60, 90

Columns - Allows you to select the following additional columns to display:

Host Name - The fully qualified name of the computer

Data - Details about the event

Created - Date and time that the event was captured

Machine Name - Name of the computer on which the threat event was detected

Path - Path to the file in which the threat was detected

Sha256 - The file's 256-character Secure Hash Algorithm can be compared with an expected result to indicate whether the file has been tampered with.

Score - The threat file's score, indicating the confidence level that the file is malware. The higher the number, the greater the confidence.

Server Encryption Clients

Suspend a Server Encryption Client

When you suspend a Server Encryption client, you suspend the user associated with the encryption client rather than an individual user who logs on to the endpoint.

To suspend a Server Encryption client:

1. In the left pane, click **Populations > Users**.
2. In the Search field, enter **SERVER-USER** and click the search icon.
3. Click the User Name of the appropriate user.
4. On the User Detail page, click the **Endpoints** tab.
5. Click the Device Id of the appropriate endpoint.
6. On the Endpoint Detail page, click the **Details & Action** tab.
7. In Server Device Control, click **Suspend**.

The Server Encryption client is suspended the next time the endpoint is rebooted.

To reinstate a suspended Server Encryption client, follow the instructions in Reinstate a Suspended Server Encryption Client.

Reinstate a Suspended Server Encryption Client

To reinstate a suspended Server Encryption client, follow these steps:

1. In the left pane, click **Populations > Users**.
2. In the Search field, enter **SERVER-USER** and click the search icon.
3. Click the User Name of the appropriate user.
4. On the User Detail page, click the **Endpoints** tab.
5. Click the Device Id of the appropriate endpoint.
6. On the Endpoint Detail page, click the **Details & Action** tab.
7. In Server Device Control, click **Reinstate**.

The Server Encryption client is reinstated the next time the endpoint is rebooted.

Commands for Self-Encrypting Drives

Priority of Commands for Self-Encrypting Drives

Each command for self-encrypting drives has a priority ranking. A command with a higher priority rank cancels commands of lower priorities in the enforcement queue.

Priority rankings (1 is highest):

1. Wipe
2. Lock
3. Remove Users
4. Unlock
5. Bypass

For example, a Wipe command cancels a Lock command that was previously queued to send to the endpoint.

Related topics:

Send Wipe Command to Self-Encrypting Drive

Lock a Self-Encrypting Drive

Remove Users from Endpoint with Self-Encrypting Drive

Unlock a Self-Encrypting Drive

Allow PBA Login Bypass

Allow PBA Login Bypass

You can allow users to bypass the Preboot Authentication (PBA) screen one time to allow a user into the computer without authenticating on an endpoint equipped with a self-encrypting drive.

To send the Bypass Login command, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the Workstation Endpoint Type.
3. If you know the full Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Workstation endpoints.
4. Click the search icon.

   An endpoint or list of endpoints displays, based on your search filter.
5. Click the Hostname of the endpoint on which to allow PBA login bypass.
6. Click the **Details & Actions** tab.
7. Under SED Device Control, click **Bypass Login**.
8. Click **Yes** to confirm that you want to send the Bypass Login command to the endpoint.

Unlock a Self-Encrypting Drive

You can unlock the PBA screen after it has been locked on this endpoint, either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

To send the Unlock command, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the **Workstation** endpoint type.
3. If you know the full Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Workstation endpoints.
4. Click the search icon.

   An endpoint or list of endpoints displays, based on your search filter.
5. Click the Hostname of the endpoint with the self-encrypting drive to unlock.
6. Click the **Details & Actions** tab.
7. Under SED Device Control, click **Unlock**.
8. Click **Yes** to confirm that you want to send the Unlock command to the endpoint.

Remove Users from Endpoint with Self-Encrypting Drive

To remove users from the PBA, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the **Workstation** endpoint type.
3. If you know the full Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Workstation endpoints.
4. Click the search icon.

   An endpoint or list of endpoints displays, based on your search filter.
5. Click the Hostname of the endpoint from which to remove users.
6. Click the **Details & Actions** tab.
7. Under SED Device Control, click **Remove Users**.
8. Click **Yes** to confirm that you want to send the Remove Users command to the endpoint.

Lock a Self-Encrypting Drive

To lock the PBA screen and prevent any user from logging onto the computer, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the Workstation Endpoint Type.
3. If you know the full Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Workstation endpoints.
4. Click the search icon.

   An endpoint or list of endpoints displays, based on your search filter.
5. Click the Hostname of the endpoint with the self-encrypting drive to lock.
6. Click the **Details & Actions** tab.
7. Under SED Device Control, click **Lock**.
8. Click **Yes** to confirm that you want to send the Lock command to the endpoint.

Send Wipe Command to Self-Encrypting Drive

WARNING: The Wipe command clears all data from the disk and cannot be undone.

The Wipe command functions as a “restore to factory state” for the SED drive. The Wipe command can be used to re-purpose a computer or, in an emergency situation, wipe the computer, making the data permanently unrecoverable. When the wipe command is consumed by the client, all history and details about this endpoint are removed from the EE/VE Server. Ensure that this is the desired behavior before invoking this command.

To send the Wipe command, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the Workstation Endpoint Type.
3. If you know the full Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Workstation endpoints.

4. Click the search icon.

   An endpoint or list of endpoints displays, based on your search filter.

5. Click the Hostname of the endpoint on which to wipe the self-encrypting drive.
6. Click the **Details & Actions** tab.
7. Under SED Device Control, click **Wipe**.
8. Click **Yes** to confirm that you want to send the Wipe command to the endpoint.

Administrators

Assign or Modify Administrator Roles

From the Administrators page, you can view or modify existing Administrator privileges.

To view or modify existing Administrator privileges, follow these steps:

1. In the left pane, click **Populations > Administrators**.
2. Search or select the row that displays the Username of the appropriate Administrator to display User Detail.
3. View or modify administrator roles in the pane at the right.
4. Click **Save**.

Note: Dell recommends assigning Administrator Roles at the Group level rather than at the User level.

To view, assign, or modify Administrator Roles at the Group level, follow these steps:

1. In the left pane, click **Populations > User Groups**.
2. Search or select a Group Name, then the **Admin** tab.

   The User Group Detail page displays.

3. Select or deselect Administrator Roles assigned to the Group.
4. Click **Save**.

If you remove a Group that has Administrative privileges and later re-add the Group, it remains an Administrator Group.

To view, assign, or modify Administrator Roles at the User level, see User Admin.

Related topics:

Administrator Roles

User Admin

Delegate Administrator Roles

Administrator Roles

Administrator login is integrated with Active Directory to simplify the process of managing Administrators and to allow you to leverage your existing user authentication infrastructure. Administrators are assigned roles that define what level of access each Administrator is allowed. For example, some Administrators may only be allowed to implement help desk assisted recovery while others have full access to edit security policies. You can assign Administrator roles to Active Directory groups so you can easily change the level of

Administrator access users have with a simple change to AD group membership. Non-domain users can be granted reporting-only access via Compliance Reporter.

There are 11 types of Administrators. Distributed administration is key to the secure administration of your environment. It allows you to divide roles appropriately among your Administrators and ensures the proper level of privileges are assigned to each Administrator. A single Administrator can have privileges of more than one Administrator type. However, it is recommended to have a maximum of one Super Administrator (an Administrator who has privileges of all Administrator types).

The following table shows the tasks each Administrator can perform in the Remote Management Console or Compliance Reporter Interface.

Task	Performed by Type of Administrator										
	Help Desk	System	Security	Log	Account	Forensic[1]	Policy[2]	Report	Report Owner	Report User	Super
Log in	•	•	•	•	•			•	•	•	•
Log out	•	•	•	•	•			•	•	•	•
View current system state	•	•	•		•						•
Search for Users, Groups, and Endpoints	•	•	•		•						•
Add Users and Groups		•	•								•
Browse Domains	•	•	•		•						•
Add and edit Domains		•	•								•
Upload licenses		•									•
Recover an endpoint - Authentication Failure	•		•								•
Remove an endpoint		•									•
Change VE Server Options		•	•								•
Suspend a User			•								•
Recover Data - authentication failure or reinstate suspended user	•	•	•		•						•
Deactivate a User			•								•
View policies			•								•
Modify policies			•								•
Commit policies			•								•
Issue commands			•								•

View audit events	•	•	•	•	•			•	•	•	•
Analyze logs		•		•							•
View Administrators					•						•
Create, change, and delete Administrator accounts					•						•
Delegate Administrator privileges					•						•
Download Recovery Key Bundle											•
Provision or recover the Advanced Threat Prevention service		•									•
Enroll for Advanced Threat Prevention auto updates		•									•
Set email notifications of Client Access Licenses, Threat Protection, and Advanced Threat Prevention Alerts		•	•								•
Manage Secure Lifecycle external users			•								•
Install/uninstall Compliance Reporter											•
Log in to Compliance Reporter								•	•	•	•
Manage report folders and modify/save Compliance Reporter Report Layouts								•			•
Access the Compliance Reporter Reports Window								•	•	•	•
Work with Compliance Reporter Report Views and generate reports								•	•	•	•
Access the Compliance Reporter Report Administrator Window								•			•
Create, manage, schedule, and make Compliance Reporter report layouts available to Report Users								•	•		•

Specify the data source for Compliance Reporter								•			•
Manage Compliance Reporter user privileges								•			•
Edit or delete a report that is set to run at a specified interval in the Compliance Reporter Scheduler								•			•
Schedule and rename a report that is set to run at a specified interval in the Compliance Reporter Scheduler								•	•		•
Enter or modify settings in Compliance Reporter Settings								•			•
Set up Compliance Reporter plug-ins								•			•
Open a Report, modify an online Report display, and rename a Report view in Compliance Reporter								•	•		•
Generate, export, store, print, and email a Report result in Compliance Reporter								•	•	•	•
Add, edit, and delete a Compliance Reporter Report folder								•	•		•

1 The Forensic Administrator role provides the rights to use the Forensic Administrator Tools via XAPI.

[2] The Policy Administrator role is reserved for future use.

Delegate Administrator Rights

Administrator rights for a User Group can be delegated to a User. The delegated Administrator and Users must be members of the User Group not only in Active Directory but in the VE Server database. Administrator rights are available to the delegated Administrator only if the delegated Administrator is a member of the User Group in the VE Server database. Delegated Administrator rights are effective only with regard to Users who are members of the User Group in the VE Server database.

Note: Only the Superadmin and Account Administrator can delegate Administrator rights.

To delegate Administrator rights, follow these steps:

1. In the left pane, click **Populations > User Groups**.

2. Search for the appropriate group.
3. Click the **Admin** tab.
4. Under Delegated Roles, click **Add**.
5. Search for and select the User to receive administrator rights, then click **Add**.

To remove delegated administrator rights, under Delegated Roles in User Group Detail, locate the User to remove as delegated administrator and click the red **X** next to the User name.

Compliance Reporter

Compliance Reporter has its own help system. When Compliance Reporter launches, click the Help link on the top menu.

To launch Compliance Reporter:

1. In the left pane of the Remote Management Console, click **Compliance Reporter**.
2. When Compliance Reporter launches, log in with superadmin credentials or reporting credentials.

View Audit Events (Geolocation)

Click **Audit Events** in the left pane of the Remote Management Console to view geographic map points of file events on computers and devices running Secure Lifecycle.

For a list of audit event types, see Secure Lifecycle and Audit Events.

For information about exporting audit events to a SIEM server, see Export Secure Lifecycle Audit Events to SIEM Server.

Map points are color coded to indicate the number of audit events in a location:

	Map point represents a single event
	Fewer than 10 events
	More than 10 events
	More than 100 events

Use the + and - icons in the upper left corner of the map to zoom in or out. Drag the map to view different areas of the map.

To view individual events for map points representing multiple events, use the + icon in the upper left corner to zoom in on the map point. Click an individual map point within the group of points to view the event.

Event Data

Event data displays below the map about the events represented on the map. Narrow the amount of data displayed by using the **+** icon in the upper left corner of the map to zoom in. Expand the amount of data displayed by using the **-** icon in the upper left corner of the map to zoom out.

Filter the event data with the following fields, which are immediately below the map:

Event Type - Secure Lifecycle Cloud Encryption, Protected Office, or Beacon

Timestamp - Event date and time

Device - Device type and identifier (hostname, serial number, IMEI/MEID, CDN)

User - User name in UPN format

File KeyID - GUID that identifies the key used to protect the file

File Name - File name with extension

Action - File action that triggered the event

Secure Lifecycle Action - Action taken by Secure Lifecycle, based on policy and the file action that triggered the event

Select columns to display from the drop-down **Columns** list.

Export Events to a SIEM/Syslog Server

Integrating with a SIEM/syslog server allows administrators to run customized analytics on threat and audit data within their environments. Dell Data Protection Server supports export of Advanced Threat Protection and Secure Lifecycle events.

For information about SIEM/syslog integration with Advanced Threat Protection, see Manage Advanced Threats - Options.htm.

For information about SIEM integration with Secure Lifecycle, see Export Secure Lifecycle Audit Events to SIEM Server.

Management

Commit Policies

To commit polices that have been modified and saved:

1. In the left pane of the Remote Management Console, click **Management > Commit**.
2. Enter a description of the change in the Comment field.

   Best practice: add a comment about the changes that are committed.
3. Click **Commit Policies**.

A policy publication/commit occurs when an administrator clicks **Commit Policies**. The following information displays:

Pending Policy Changes - The number of policy changes ready to commit.

Date Committed - Date and time the policies were committed.

Changed by - User name of the administrator who performed the policy commit.

Comment - Any comments that were added when the polices were committed.

Version - The number of policy saves since the last policy commit plus the previous Version.

Log Analyzer

Log Analyzer gives you the power to search logs by message priority level, date and time periods, and occurrences of usernames and hosts.

To view Remote Management Console logs:

1. In the left pane of the Remote Management Console, click **Management > Log Analyzer**.
2. Select a Category.

   The Categories are Admin Actions, Shield for Server Events, Advanced Threat Events, and System Logs.
3. To narrow the results, select from these optional filters:
   - Priority - Choose DEBUG, INFO, WARN, ERROR, or FATAL. FATAL returns fewest entries; DEBUG returns the greatest number of entries.
   - And more severe - Check this option to include all areas of greater severity than the Priority level you selected.
   - Date Range - Enter a Start Date and End Date to limit results to entries that occur between these dates. To insert dates into these fields, click the calendar icons to the right of the fields.
   - Time Range - If you entered a Date Range, you may further narrow the entries by entering a Start Time and End Time. To insert times into these fields, click the calendar icons to the right of the fields.
   - Username and Host - Enter a either a Username or Host or both.
4. Click **Search**.
5. To sort the results in ascending order by column, click the heading of the column you want to sort.

Recovery

Recover Data - EMS Authentication Failure

EMS encrypts data on removable storage, as defined by policy. There may be several different circumstances where access to EMS encrypted data needs to be regained. In general, these scenarios fall into two categories:

- The EMS password is lost or forgotten
- The EMS software or key material has been lost or corrupted on the device

Manual Authentication when EMS Password is Lost or Forgotten

If a user has lost or forgotten an EMS password, manual authentication is necessary.

1. The user will be prompted for their password. Since the password is not available, the user clicks **I forgot**.
2. The user is given another opportunity to try again. If the user clicks **Yes - I forgot**, the Manual Authentication window displays (or the Manual Authentication window will automatically display upon the set number of retries allowed).
3. The user is instructed to contact their Administrator and inform them that they need to manually recover EMS for Windows.
4. As a Dell Administrator, log in to the Remote Management Console.
5. In the left pane, click **Populations > Users**.
6. Enter a filter to search for the user. The wild card character is *. You can enter Common Name, Universal Principal Name, or sAMAccountName.
7. Click the search icon.

   A user or list of users displays, based on your search filter.
8. Locate the appropriate user and click the **Endpoints** tab.
9. Locate the appropriate *Shielded* Endpoint.
10. Under Actions, click the **Recover** link.

    The Recover Data page displays.

Tip: Numbers are red and letters are blue.

11. Ask the user for the **Shield ID** and verify that it is correct or enter it into the Shield ID field. Shield IDs do not contain the letters B, O, Q, and S.
12. Ask the user for the 8, 16, or 32-character **Endpoint Code** (not case sensitive) and enter it into the appropriate field. Endpoint Codes contain only the letters A-F.
13. Ask the user for the **Key ID** and enter it into the appropriate field (if your organization allows non-domain user activation, the Key ID is required.
14. Click **Generate Access Code**. The Restore User Access page displays the Directory User Alias associated with the Shield, along with an Access Code.
15. Confirm to your satisfaction that the request is coming from the Directory User Alias shown.

    This is especially important if recovering removable storage that may have been given to another user. Dell recommends that you set a help desk policy for how to handle requests from users other than those who originally copied the data.
16. Do **one** of the following:
    - To allow the user to access the endpoint, click **Activate**.
    - To **not** allow the user to access the endpoint, click **Cancel**.

17. If the requester is the device authorized user, ask the user to enter the Access Code (not case sensitive) on the endpoint and click **OK**. The Access Code policies of the user affect this process (for example, how many attempts the user has to enter the code correctly).
18. When the user successfully enters the Access Code, the Shield changes the *Current Shield State* policy to *Activate*, and the successfully entered Access Code is no longer valid. Instruct the user to click **OK** to close the dialog.
19. In the left pane, click **Management > Commit**.
20. Click **Commit Policies**.

Once manual authentication is successful, the user is directed to reset their password. Depending on how policies are set, one of the following three dialogs are displayed. The user enters a new password and confirms it, then clicks **OK** or **Cancel**.

Depending on policies set, the user may be prompted to type this password when using this removable storage in other computers.

If the policy is set to **block** all access to removable storage until authenticated/encrypted and the user clicks Cancel, they cannot access any files on this removable storage. If a user re-uses a password that has been used too recently, a dialog displays asking them to use a different password. If a password does not meet the criteria set by policy, a dialog displays, outlining the password criteria.	If the policy gives **read-access** to removable storage until authenticated/encrypted and the user clicks Cancel, they can read/delete existing files on this removable storage, but cannot edit/add files to this removable storage. If a user re-uses a password that has been used too recently, a dialog displays asking them to use a different password. If a password does not meet the criteria set by policy, a dialog displays, outlining the password criteria.	If the policy gives **full access** to removable storage until authenticated/encrypted and the user clicks Cancel, they have full access to unencrypted files on this removable storage, but cannot access encrypted files. If a user re-uses a password that has been used too recently, a dialog displays asking them to use a different password. If a password does not meet the criteria set by policy, a dialog displays, outlining the password criteria.

The user may now use the removable storage as usual.

If manual authentication is **not** successful, the device is disabled according to policy, as follows:

- The policy could be set to wait (cooldown) between unsuccessful manual authentication attempts.

  or

- The policy may be set to delete the encryption key material and prevent any access to encrypted files on this removable storage. In this case, the user will need to contact an Administrator again for instructions to re-enable access.

Restore Lost EMS Key Material

If encryption keys have been deleted on the removable storage (because of failed manual authentication, accidentally deleting a necessary file, a change in policy), the encrypted data will be inaccessible until an authorized user reinitializes the key material.

A dialog displays, notifying the user that key material is missing. Click **Yes** to use the self-healing feature of EMS or click No.

If the policy **blocks** all access to removable storage until encrypted and the user clicks No, they cannot access this removable storage.	If the policy gives **read-access** to removable storage until encrypted and the user clicks No, they have read-access to unencrypted data on this media, but no access to encrypted data.	If the policy gives **full access** to removable storage, whether or not encrypted and the user clicks No, they have full access to unencrypted data on this media. They cannot access encrypted data.

Occasionally, based on policies set, encryption keys cannot be reinitialized on the computer that the removable storage is inserted in. If policy permits, the user can insert the media into any Shielded computer where the original user is logged in, to reinitialize the encryption keys. If policy does not permit this, it must be inserted into the originally Shielding computer, with the originally Shielding user name.

On rare occasions, when key material is lost, the Shield cannot automatically locate the necessary information. Use the following process to recover encrypted data.

1. Attach the device to a Windows computer that is not running the Shield.
2. Copy all folders from the device onto the Windows computer.
3. Use WSScan to determine the DCID of the encrypted data.
4. Follow the process for recovering access to encrypted data on Windows computers. Use the DCID obtained from WSScan for the RecoveryID.

Recover Data - BitLocker Manager

See the *Recovery Guide* for the most up-to-date recovery instructions.

The latest *Recovery Guide* is available at http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/manuals.

SED Recovery

SED Authentication Failure

Use this procedure to recover access to a computer with an SED drive after an authentication failure.

1. In the left pane, click **Management > Recover Data**.
2. Click the **SED** tab.
3. Under Recover SED Endpoint, enter the Hostname of the computer.

   You can find the Hostname at **Populations > Endpoints**. If you know the full Hostname of the endpoint, enter it in the *Search* field. You can leave the field blank to display all Windows and Mac endpoints.
4. In the SED drop-down, select the correct self-encrypting drive.
5. Instruct the user to give you the Challenge Code. Enter the Challenge Code and click **Generate Response**.
6. A Response Code displays. Instruct the user to enter this code on their computer.

SED Endpoint Recovery

For instructions on how to recover an SED Endpoint, see the *Recovery Guide*. The latest *Recovery Guide* is available at any of these locations:

Encryption - http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/manuals

Threat Protection - Endpoint Security Suite - http://www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite/manuals

Advanced Threat Prevention - Endpoint Security Suite Enterprise - http://www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

Security Tools - http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-security-tools/manuals

Recover Endpoint

To download encryption keys of a managed or removed endpoint:

NOTE: Select **Include Removed Endpoints** to display endpoints that were previously removed.

1. In the left pane, click **Management > Recover Endpoint**.
2. Enter the Hostname and click **Search**.
3. Click **Recover** next to the endpoint.
4. Enter a password then click **Download**.
5. Copy the recovery file to the endpoint and run the file.

Windows Recovery

For Windows Recovery, follow the instructions in the *Recovery Guide.*

The latest *Recovery Guide* is available at these locations:

Encryption - http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/manuals

Threat Protection - Endpoint Security Suite - http://www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite/manuals

Advanced Threat Prevention - Endpoint Security Suite Enterprise - http://www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

SED Recovery

For information about SED authentication failure or SED endpoint recovery, see SED Recovery.

EMS Recovery

For information about recovering after EMS authentication failure, see EMS Authentication Failure.

Mac Recovery

See the *Enterprise Edition for Mac Administrator Guide* for the most up-to-date recovery instructions.

The latest *Enterprise Edition for Mac Administrator Guide* is available at http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/manuals.

License Management

License Management

To view usage of Client Access Licenses (CALs) that you own and upload new licenses, click **Management > License Management**.

Upload Client Access Licenses

You received CALs separately from the installation files, either at the initial purchase or later if you added additional CALs.

1. In the left pane of the Remote Management Console, click **Management > License Management**.
2. Under Upload Licenses, click **Choose File** to browse to the location of the saved CAL.

View or Add License Notifications

Through Notification Management, you can set up notifications of license usage or expiration.

In the left pane of the Remote Management Console, click **Management > Notification Management**.

Related topics:

CAL Information

Notification Management

CAL Information

When logging in to the Remote Management Console, if there is a problem with your CAL, an error message displays (typically, the error states that the VE Server has exceeded the maximum number of authorized Client Licenses). The next step is to review your CALs to ensure that your enterprise has the appropriate number of CALs to Client ratio (1-to-1 ratio).

If authorized CALs exceed 5% of that specific CAL total, new client activations for that specific product will be blocked until the license key is brought into compliance. No other client or VE Server functions will be impacted when a license key is in the over 105% state. Two separate warning messages are displayed, the first warning message is when the CAL reaches 100% of the authorized licenses, the second when the CAL count reaches or exceeds the 105% total.

For example:

- Authorized CAL for Shield for Windows: 5000 user licenses
- First warning message from VE Server and an email message is sent to the admin: CAL count reaches 5000
- Second warning message from VE Server and an email message is sent to the admin: CAL count reaches 5250

If a client has previously been activated and inventory records exist, then it will not be blocked from any re-activation. However, if the CAL authorized count is exceeded during this process, new activations will be blocked for the specific CAL that is in the over 105% state.

Licensing

1. License structure:
    a. Disk Encryption (DE) – Windows Agent (Shield), Server Encryption, External Media Shield (EMS), SED Management, Advanced Authentication, BitLocker Manager (BLM), and Mac Encryption.
    b. External Media Edition (EME)
    c. Secure Lifecycle (CE)
    d. Mobile Edition (ME)
    e. Threat Protection (TP)
    f. Advanced Threat Prevention (ATP)

2. Dell Digital Delivery of entitlements

License Management

Upload Licenses

Choose File

Client Licenses Owned

Alert	Type	Valid From	Valid To
	Secure Lifecycle	12/31/1752 6:00 PM	12/31/9999 5:59 PM
	Threat Protection	12/31/1752 6:00 PM	12/31/9999 5:59 PM
	Enterprise Edition	12/31/1752 6:00 PM	12/31/9999 5:59 PM
	BitLocker Manager	12/31/1752 6:00 PM	12/31/9999 5:59 PM
	Enterprise Edition	12/31/1752 6:00 PM	12/31/9999 5:59 PM

Client License Usage

Alert	Type	Total	Used
	Enterprise Edition	260	13
	Secure Lifecycle	260	1
	External Media Edition	520	0
	Mobile Edition	260	0
	BitLocker Manager	520	0
	Threat Protection	260	0
	Advanced Threat Protection	250	0

Entitlements

Type	Guid
Threat Protection	3471c5a4-3f94-4a95-ad23-953a81ba5e75
Enterprise Edition	3471c5a4-3f94-4a95-ad23-953a81ba5e75
BitLocker Manager	3471c5a4-3f94-4a95-ad23-953a81ba5e75
Mobile Edition	3471c5a4-3f94-4a95-ad23-953a81ba5e75
Threat Protection	b885e9fa-49c1-4dce-94a5-9e999296861b

Dropbox Management

To remotely remove a member from the Dropbox for Business team account, an administrator must be registered to perform this action. Registration requires linking the administrator's Dropbox for Business account with the EE/VE Server. Removing a Dropbox for Business team member remotely wipes the user account and associated data.

To register to remove Dropbox for Business users and their data:

1. In the left pane of the Remote Management Console, click **Management > Dropbox Management**.
2. Click **Register**.
3. If prompted to sign in to Dropbox to link with the DDP Server, enter your email address and password and click **Sign in**.
4. Click **Allow**.

When the Dropbox Management page is refreshed, the Administrator name displays.

Remove a Dropbox for Business User

A Dropbox for Business user is the only type of user that can be removed in the Remote Management Console. The Remote Wipe option is available only for enrolled Dropbox for Business team member accounts. If the Remote Wipe option does not display for a user account, the user has not enrolled a Dropbox for Business account.

Note: Before you Remote Wipe the account, back up any files or folders from the team member account that might be needed by the enterprise or other Dropbox for Business team members.

To remove a Dropbox for Business user account and associated data, follow these instructions:

1. In the left pane, click **Populations > Users**.
2. Enter the User Name or a filter to search for available users. The wild card character is *. For best results, include non-wild card characters at the beginning of the filter (e.g., User* instead of * ser). You can enter Common Name, Universal Principal Name, or sAMAccountName.
3. Click **Search**.
4. Select the appropriate user.
5. On the User Detail page, click the **Details & Actions** tab.
6. In the Command column, click **Remote Wipe**.
7. Click **Yes**.

In the Dropbox for Business Administrator Console, the user is removed from the list of Team Members. If necessary, refresh the list of Team Members. To view a list of removed users, click the **Removed Members** tab.

Advanced Threat Prevention Services Management

The Services Management Advanced Threats tab provides the following options:

Provision and Recover the Advanced Threat Prevention service - After the service is provisioned, clients are automatically provisioned with Advanced Threat Prevention. For more information, see Provision Advanced Threat Prevention Service.

Enroll to receive Advanced Threat Prevention agent auto updates - After enrollment, clients can automatically download and apply updates from the Advanced Threat Prevention server. For more information, see Enroll for Agent Auto Update.

Access the Services Management Advanced Threats tab from the left pane of the Remote Management Console, **Management > Services Management** and then click the **Advanced Threats** tab.

Product Notifications

You can enroll to receive notifications of product updates, recommended configuration changes, and relevant Knowledge Base articles.

Receive product notifications

To enroll to receive product notifications:

1. In the left pane of the Remote Management Console, click **Management > Services Management**.
2. Select the **Product Notifications** tab.
3. Click the **On** button, then click the **Save Preferences** button.

Stop receiving product notifications

To stop receiving product notifications:

1. In the left pane of the Remote Management Console, click **Management > Services Management**.
2. Select the **Product Notifications** tab.
3. Click the **Off** button, then click the **Save Preferences** button.

Alerts Management

Notification Management

The Notification Management page lets you manage email notifications.

To add an email notification:

1. In the left pane of the Remote Management Console, click **Management > Notification Management**.
2. Click the **Add** button and fill in the dialog:

   Email: Enter or select your email address.

   Notification Type: Select the type of alert you want to add.

   Priority Level: Select the priority levels of notifications.

   Email Frequency: Select how often you want to receive alerts of this type. (Default frequency is 24 hours.)

2. Press **Enter** when complete.

To edit an alert:

- Select the alert you want to change, click **Edit**, make the changes, and press **Enter**.

To delete an alert:

- Select the alert you want to delete, and click **Delete**.

Related topics:

License Management

Configure SMTP Settings

To receive DDP Enterprise Server - VE email notifications or to use Dell Data Protection | Cloud Edition, follow the steps in this section to configure SMTP settings. DDP Enterprise Server - VE email notifications inform recipients of DDP Enterprise Server - VE server status error states, password updates, availability of DDP Enterprise Server - VE updates, and client license issues.

It is a best practice to restart the services any time a settings change is made.

To configure SMTP settings, follow these steps:

1. From the Advanced Configuration menu, select **Email Notifications**.
2. In the Set up Email Notifications screen, to enable email alerts, press the Spacebar to enter an **X** in the Enable Email Alerts field.
3. Enter the SMTP Server fully qualified domain name.
4. Enter the SMTP Port.
5. In the From User field, enter the email account ID that will send email notifications.
6. In the Enter User field, enter an email account ID for access to change configured email notifications.
7. In the Password field, enter a password for access to change configured email notifications.
8. In the Mail IDs fields for VE Status, Password Updates, and Updates Availability, enter lists of recipients for each notification type.
9. Follow these conventions when listing recipients:

   Email address format is recipient@dell.com.

   Recipients are separated with commas or semicolons.
10. In the Service alert reminder field, to enable reminders, press the Spacebar to enter an X in the field then set the reminder interval in minutes.
11. A Service alert reminder is triggered when the reminder interval has passed after a notification is sent about a system health issue and the host or service remains in the same state.
12. In the Summary Report field, to enable reports of notifications, select the desired interval (Daily, Weekly, or Monthly) and then press the Spacebar to enter an **X** in the field.
13. Select **OK**.

External User Management

To allow or block Secure Lifecycle access for users who are not in the organization's domain:

1. In the left pane of the Remote Management Console, click **Management > External User Management**.
2. Click **Add**.
3. Select Registration Access Type:

   Blacklist - Blocks registration and file access for a user or a domain.

   Full Access List - Grants registration and file access for a user or domain. If the user or domain is also on the blacklist, no access is granted.
4. Enter either a domain to set access for the entire domain, or email address to set access only for a single user.
5. Click **Add**.

Change the Superadmin Password

1. In the masthead at the top of the screen, click the gear icon and select **Change superadmin password**.
2. Enter the Current Password.
3. Enter the New Password.

   The new password must be at least 6 characters, contain at least one capital letter and one of these characters: **~@#$%^*()|?!{}[]**.
4. Confirm the New Password.
5. Click **Update**.

Manage Policies

Manage Security Policies

You can apply security policies at the Enterprise, Domain, User Group, User, Endpoint Group, and Endpoint levels. The initial deployment of your Dell Data Protection Server has default policy settings that allow your enterprise to get started with Dell Data Protection, but you can customize the security and configuration settings. If you've migrated from an earlier version of Dell Data Protection Server, your policy settings have been migrated for you.

Security policies are grouped by technology. Click a Technology Group to view its policies and policy descriptions.

Windows Encryption
- Self-Encrypting Drive (SED)
- Hardware Crypto Accelerator (HCA)
- Policy-Based Encryption
- Bitlocker Encryption
- Server Encryption

Threat Prevention
- Advanced Threat Prevention
- Threat Protection
- Malware Protection
- Web Protection
- Client Firewall

Mac Encryption
- Dell Volume Encryption
- Mac Global Settings

Authentication
- Windows Authentication
- Microsoft Passport

Removable Media Encryption
- Windows Media Encryption
- Mac Media Encryption
- Media Encryption Settings

Port Control
- Windows Port Control
- Windows Device Control

Secure Lifecycle
- Cloud Encryption
- Protected Office Documents
- Mobile Client
- Settings

Mobile Protection
- Mobile Edition - EAS
- Mobile Edition - iOS

Global Settings
- Settings
- DDP Auto Updates
- Audit Control
- Mobile Audit Control

The following override information displays at the top of the Security Policies page:

Override count - the number of policy settings that are changed from their default settings.

Uncommitted overrides - the number of changes from default settings that are not yet committed.

NOTE: The Security Policies page for a population displays overrides to localizable policies in the browser language only.

Icons and their meanings:

The master switch for policies in the subgroup is On, which means the policy group is enabled. Policies in the group are sent to clients when policies are committed.

Policies in the subgroup are not enabled.

At least one default setting in the policy group has been overridden.

Group of policy settings that has no master switch.

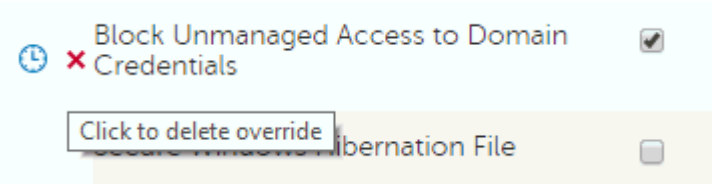
The policy change is not yet committed.

The policy value can be localized, in order for policies to display on the endpoint computer in a selected language. For more information, see Localize Policies Displayed on the Endpoint Computer and Localizable policies.

The default setting of a localizable policy is overridden.

A localizable policy change is not yet committed.

To remove a policy override, hover over the red flag next to the policy name. The red flag becomes a red X. Click the red **X** to revert to the default value.



Group precedence

You can Modify Group Precedence. Group precedence creates a weight associated with the specific group it is assigned to, and that weight is used in policy arbitration for all policy overrides.

Related topics:

View or Modify Enterprise-Level Policies

View or Modify Domain Policies and Information

View or Modify User Group Policies and Information

View or Modify User Policies and Information

View or Modify Endpoint Group Policies and Information

View or Modify Endpoint Policies and Information

Windows Encryption

A word about types of encryption: SDE is designed to encrypt the operating system and program files. In order to accomplish this purpose, SDE must be able to open its key while the operating system is booting without intervention of a password by the user. Its intent is to prevent alteration or offline attacks on the operating system by an attacker. SDE is not intended for user data. Common and User key encryption are intended for sensitive user data because they require a user password in order to unlock encryption keys.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Self-Encrypting Drive (SED)		
Self-Encrypting Drive (SED)	On	*On* *Off*

		Toggle On to activate the PBA. If toggled to OFF, the PBA will be deactivated. Ensure in both cases that the policy "Enable Plugin" is also set to selected.
SED Authentication Method	Password	*Password* *Smart Card* Select the type of authentication to use when logging in to the PBA.
Support Information Text	String Please contact your system administrator.	*String 0-512 characters* Text to display on the PBA support information screen. We recommend that you customize the message to include specific instructions about how to contact the Help Desk or Security Administrator. Not entering text in this field results in no support contact information being available for the user. Also note that text wrapping occurs at the word level, not the character level. For instance, if you have a single word that is more than approximately 50 characters in length, it will not wrap and no scroll bar will be present, therefore the text will be cut off.
PBA Title Text	0-17 characters	*0-17 characters* The text to display on the top of the PBA screens. Not entering text in this field results in no title being displayed. Text does not wrap, so entering more than 17 characters will result in the text being cut off.
Sync Users at PBA Activation	Not Selected	Enables full user synchronization during activation.
See advanced settings		
Policy	**Default Setting**	**Description**
Hardware Crypto Accelerator (HCA)		
Hardware Crypto Accelerator (HCA)	On	*On* *Off* Toggle to ON to enable HCA policies. If this policy is toggled to OFF, no HCA encryption takes place, regardless of other HCA policies. HCA can only be used on computers equipped with an HCA card. See Hardware Crypto Accelerator for terminology. More... If an endpoint computer comes equipped with an HCA card and you choose to enable HCA policies, all SDE policies are ignored. Likewise, if you enable

		SDE policies and later decide to enable HCA policies, SDE issues a decryption policy before HCA policies are implemented. HCA and SDE cannot coexist on the same computer.
Volumes Targeted for Encryption	All Fixed Volumes	All Fixed Volumes, System Volume Only Specify which volume(s) to target for encryption.
See advanced settings		
Policy	**Default Setting**	**Description**
Policy-Based Encryption		
Policy-Based Encryption	On	*On* *Off* Toggle to ON to enable all policy-based encryption policies. If this policy is toggled to OFF, no policy-based encryption takes place, regardless of other policy values. On means that all Policy-Based Encryption policies are enabled. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
Application Data Encryption Key	Common	Common, User, User Roaming Choose a key to indicate who should be able to access files encrypted by Application Data Encryption List, and where. More... Common if you want these files to be accessible to all managed users on the endpoint where they were created (the same level of access as Common Encrypted Folders), and encrypted with the Common Encryption Algorithm. User if you want these files to be accessible only to the user who created them, only on the endpoint where they were created (the same level of access as User Encrypted Folders), and encrypted with the User Encryption Algorithm. User Roaming if you want these files to be accessible only to the user who created them, on any Shielded Windows endpoint, and encrypted with the User Encryption Algorithm. Changes to this policy do not affect files already encrypted because of this policy.
SDE Encryption Enabled	Not Selected	This policy is the "master policy" for all other System Data Encryption (SDE) policies. If this policy is Not Selected, no SDE

		encryption takes place, regardless of other policy values. A Selected value means that all data not encrypted by other Intelligent Encryption policies will be encrypted per the SDE Encryption Rules policy. More... Changing the value of this policy requires a reboot. If an endpoint computer comes equipped with an HCA and you choose to enable HCA policies, all SDE policies are ignored. Likewise, if you enable SDE policies and later decide to enable HCA policies, SDE issues a decryption policy before HCA policies are implemented. HCA and SDE cannot coexist on the same computer.
SDE Encryption Rules	String F#:\ -^%ENV:SYSTEMDRIVE%\System Volume Information -^%ENV:SYSTEMROOT%\;dll.exe.sys.ocx.man.cat.manifest.policy -^%ENV:SYSTEMROOT%\System32 -^%ENV:SYSTEMROOT%\SysWow64 -^%ENV:SYSTEMROOT%\WinSxS -^%ENV:SYSTEMROOT%\Fonts -^3@%ENV:SYSTEMROOT%\SYSTEM32\cmd.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\autochk.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\winresume.exe;exe -^F#:\bootmgr -^F#:\boot	Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. See Encryption Rules for information. SDE Encryption Rules may be changed as appropriate for your environment. However, these defaults have been tested extensively. Removing these exclusions may result in Windows issues, particularly after applying patch updates. Contact Customer Support for guidance if you are unsure about changing the values.
Common Encrypted Folders	String %ENV:SYSTEMDRIVE%\;accdb.doc.docm.docx.mdb.pdf.ppam.pps.ppsm.ppsx .ppt.pptm.pptx.pub.puz.sldm.sldx.tif.tiff.vdx.vsd.vss.vst.vsx.vtx.xlam .xlm.xls.xlsb.xlsm.xlsx.xsf.zip.rar %ENV:USERPROFILE%\Desktop %ENV:USERPROFILE%\Download -^%ENV:SYSTEMDRIVE%\;dat.ini.xml.txt.log.db.lnk	String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters) A list of folders on endpoint drives to be encrypted or excluded from encryption, which can then be accessed by all managed users who have access to the endpoint. See Encryption Rules for information. More... The available drive letters are: #: Refers to all drives f#: Refers to all fixed (non-removable) drives r#: Refers to all removable drives **Important:** *Overriding directory protection can result in an unbootable computer and/or require reformatting drives.* If the same folder is specified in

		both this policy and the User Encrypted Folders policy, this policy prevails.
Policy-Based Encryption-User Experience		
Enable Software Auto Updates	Selected	*Selected* *Not Selected* Selected enables the client update agent to automatically check for updates. If this policy is Selected, the On Premise Update Staging Location policy must include the staging location.
On Premise Update Staging Location	String	The network location (UNC) where DDP Server stages update packages. This policy must have a value if the Enable Software Auto Updates policy is Selected.
See advanced settings		
Policy	**Default Setting**	**Description**
Bitlocker Encryption		
BitLocker Encryption	On	*On* *Off* Toggle to ON to enable BitLocker Manager policy settings. Toggling to OFF disables all BitLocker Manager policies, regardless of other policy values.
TPM Manager Enabled	Not Selected	*Selected* *Not Selected* Selected enables TPM management with BitLocker management. Not Selected disables **all** TPM management policies, *including* policies in the Operating System Volume Settings category.
Disable Sleep Mode	Selected	*Selected* *Not Selected* Selected disables sleep mode on the local computer. Changing this policy requires a reboot for the new value to take effect.
Encrypt System Drive	Turn On Encryption	*Do Not Manage* *Turn On Encryption* *Turn Off Encryption* Do Not Manage ignores the System Drive (typically the drive that the operating system is installed on). Turn On Encryption allows BitLocker to encrypt the System Drive. Turn Off Encryption causes Manager to decrypt any BitLocker encrypted

		system drives.
Encrypt Fixed Drives	Do Not Manage	*Do Not Manage* *Turn On Encryption* *Turn Off Encryption* This policy does not encrypt the system drive. To also encrypt the system drive, make sure that Encrypt System Drive Only is also Turn On Encryption. Do Not Manage ignores Fixed Drives. Turn On Encryption allows BitLocker to encrypt Fixed Drives. Turn Off Encryption causes Manager to decrypt any BitLocker encrypted fixed drives.
Encrypt Removable Drives	Do Not Manage	*Do Not Manage* *Turn On Encryption* *Turn Off Encryption* Do Not Manage ignores Removable Drives. Turn On Encryption allows BitLocker to encrypt Removable Drives. Turn Off Encryption causes Manager to decrypt any BitLocker encrypted removable drives.
Require Additional Authentication at System Startup	Selected	*Selected* *Not Selected* This policy allows for the configuration of BitLocker to require additional authentication each time the computer starts up and whether BitLocker can be used with or without a Trusted Platform module (TPM). More... This policy is the parent policy to: Allow BitLocker Encryption Without a Compatible TPM Configure TPM Startup Configure TPM Startup PIN Configure TPM Startup Key Configure TPM Startup Key and PIN
Allow BitLocker Encryption Without a Compatible TPM	Not Selected	*Selected* *Not Selected* Selected allows a computer without a compatible TPM to be allowed to use BitLocker encryption. In this mode, a USB drive is required for startup. When the key is inserted, access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable, the computer will require BitLocker recovery options for access. To use this policy, Require Additional Authentication at System Startup must be set to Selected.

Configure TPM Startup	Require	*Do Not Allow* *Require* *Allow* On computers with a compatible TPM, three types of authentication are supported. Only one of the following can be required: Configure TPM Startup PIN Configure TPM Startup Key Configure TPM Startup Key and PIN To use this policy, Require Additional Authentication at System Startup must be set to Selected.
Configure TPM Startup PIN	Allow	*Do Not Allow* *Require* *Allow* To use this policy, Require Additional Authentication at System Startup must be set to Selected. This type of authentication involves the entry of a 4-digit to 20-digit personal identification number (PIN).
Configure TPM Startup Key	Allow	*Do Not Allow* *Require* *Allow* To use this policy, Require Additional Authentication at System Startup must be set to Selected. This type of authentication involves insertion of a USB drive containing the startup key.
Configure TPM Startup Key and PIN	Allow	*Do Not Allow* *Require* *Allow* To use this policy, Require Additional Authentication at System Startup must be set to Selected. This type of authentication involves a 4-digit to 20-digit personal identification number (PIN) and a USB drive containing the startup key.
Encryption Method and Cipher Strength (OS Volumes)	XTS-AES-128	*AES-128* *AES-256* *XTS-AES-128 (Windows 10 Anniversary Edition and later)* *XTS-AES-256 (Windows 10 Anniversary Edition and later)* Algorithm and cipher strength used by BitLocker Drive Encryption for OS Volumes.

Encryption Method and Cipher Strength (Removable Volumes)	AES-128	*AES-128* *AES-256* *XTS-AES-128 (Windows 10 Anniversary Edition and later)* *XTS-AES-256 (Windows 10 Anniversary Edition and later)* Algorithm and cipher strength used by BitLocker Drive Encryption for Removable Volumes. To encrypt removable drives that will be used with older versions of Windows as well as with Windows 10 Anniversary Edition and later, use AES-128 or AES-256.
Encryption Method and Cipher Strength (Fixed Volumes)	XTS-AES-128	*AES-128* *AES-256* *XTS-AES-128 (Windows 10 Anniversary Edition and later)* *XTS-AES-256 (Windows 10 Anniversary Edition and later)* Algorithm and cipher strength used by BitLocker Drive Encryption for Fixed Volumes.
See advanced settings		
Policy	**Default Setting**	**Description**
Server Encryption		
Server Encryption	Off	*On* *Off* This policy enables or disables System Data Encryption (SDE) and Common Encryption on the client server. Toggle to ON to enable both System Data Encryption (SDE) and Common Encryption. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
Allow Software Server Encryption	Selected	*Selected* *Not Selected* Selected means that the Server allows client server endpoint activations at the Enterprise level. This policy may be set to Not Selected to block activations during initial Server setup and maintenance interruptions.
Server Maintenance Schedule	Not Selected	This policy is the "master policy" for all other Server Maintenance policies. If this policy is Not Selected, no Server Maintenance policies are enforced, regardless of other policy values. Selected allows a maintenance schedule to control application of policy that requires a reboot.

Server Maintenance Schedule Repeats	Weekly	*Daily, Weekly, Monthly, Quarterly, Annually* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, Monthly, Quarterly, and Annually. Daily: Runs the task every day at the specified Server Maintenance Schedule Start Time. Weekly: Runs the task weekly on the days specified in Server Maintenance Day of the Week. Monthly: Runs the task monthly on the specified Server Maintenance Day of the Month. Quarterly: Runs the task quarterly on the specified Server Maintenance Day of the Month. Annually: Runs the task annually on the specified Server Maintenance Day of the Month.
Port Control System	Disabled	Enable or Disable all Port Control System policies. If this policy is set to Disable, no Port Control System policies are applied, regardless of other Port Control System policies. **Note**: PCS policies require a reboot before the policy takes effect.
SDE Encryption Enabled	Not Selected	This policy is the "master policy" for all other System Data Encryption (SDE) policies. If this policy is Not Selected, no SDE encryption takes place, regardless of other policy values. A Selected value means that all data not encrypted by other Intelligent Encryption policies will be encrypted per the SDE Encryption Rules policy. More... Changing the value of this policy requires a reboot. If an endpoint computer comes equipped with an HCA and you choose to enable HCA policies, all SDE policies are ignored. Likewise, if you enable SDE policies and later decide to enable HCA policies, SDE issues a decryption policy before HCA policies are implemented. HCA and SDE cannot coexist on the same computer.
SDE Encryption Rules	String F#:\ -^%ENV:SYSTEMDRIVE%\System Volume Information -^%ENV:SYSTEMROOT%\;dll.exe.sys.ocx.man.cat.manifest.policy -^%ENV:SYSTEMROOT%\System32 -^%ENV:SYSTEMROOT%\SysWow64 -^%ENV:SYSTEMROOT%\WinSxS	Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. See Encryption Rules for information. SDE Encryption Rules may be changed as appropriate for your environment. However, these defaults have been tested

	-^%ENV:SYSTEMROOT%\Fonts ^3@%ENV:SYSTEMROOT%\SYSTEM32\;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\cmd.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\autochk.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\winresume.exe;exe -^F#:\bootmgr -^F#:\boot	extensively. Removing these exclusions may result in Windows issues, particularly after applying patch updates. Contact Customer Support for guidance if you are unsure about changing the values.
Encryption Enabled	Selected	This policy is the "master policy" for all Common Encryption policies. A cleared check box means that no Common Encryption takes place, regardless of other policy values. A checked box means that all Common Encryption policies are enabled. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
See advanced settings		

Variables

Some Windows policies support the following variables. A pathname can consist entirely of one or more of these variables, or can include one or more of these variables at any point.

To get directory locations that these CSIDL values resolve to, go to http://msdn.microsoft.com/en-us/library/bb762494.aspx. All names listed on the MSDN page are CSIDL_<name>.

Note: Some operating systems have different CSIDL values, such as Windows 7 having values that Windows XP does not.

%CSIDL:name%

- Includes any of the following Windows CSIDL constants:

  DESKTOP

  INTERNET

  PROGRAMS

  CONTROLS

  PRINTERS

  PERSONAL

  FAVORITES

  STARTUP

  RECENT

  SENDTO

  STARTMENU

  STARTMENU

  MYDOCUMENTS

  MYMUSIC

MYVIDEO

DESKTOPDIRECTORY

DRIVES

NETWORK

NETHOOD

FONTS

TEMPLATES

COMMON_STARTMENU

COMMON_PROGRAMS

COMMON_STARTUP

COMMON_DESKTOPDIRECTORY

APPDATA

PRINTHOOD

LOCAL_APPDATA

ALTSTARTUP

COMMON_ALTSTARTUP

COMMON_FAVORITES

INTERNET_CACHE

COOKIES

HISTORY

COMMON_APPDATA

WINDOWS

SYSTEM

PROGRAM_FILES

PROGRAMFILES

MYPICTURES

PROFILE

SYSTEMX86

PROGRAM_FILESX86

PROGRAMFILESX86

PROGRAM_FILES_COMMON

PROGRAM_FILES_COMMONX86

COMMON_TEMPLATES

COMMON_DOCUMENTS

COMMON_ADMINTOOLS

ADMINTOOLS

CONNECTIONS

COMMON_MUSIC

COMMON_PICTURES

COMMON_VIDEO

RESOURCES

PROFILES

%HKCU:regpath%

- Includes a numeric or text value stored in the registry for the Current User. If you specify a path but not an item, the Shield uses the default value

%HKLM:regpath%

- Includes a numeric or text value stored in the registry for the local computer. If you specify a path but not an item, the Shield uses the default value

%ENV:envname%

- Includes the value of a Windows local environment variable

%%

- Includes the % character

Windows Policies that Require Reboot

- SDE Encryption Enabled
- All PCS policies

Windows Policies that Require Logoff

- SDE Encryption Enabled

Advanced Windows Encryption

A word about types of encryption: SDE is designed to encrypt the operating system and program files. In order to accomplish this purpose, SDE must be able to open its key while the operating system is booting without intervention of a password by the user. Its intent is to prevent alteration or offline attacks on the operating system by an attacker. SDE is not intended for user data. Common and User key encryption are intended for sensitive user data because they require a user password in order to unlock encryption keys.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Self-Encrypting Drive (SED)		
Legal Notice Text	String 0-512 characters	*String 0-512 characters* Text to display before being allowed to log on to the device. For examp clicking OK, you agree to abide by the acceptable computer use policy Not entering text in this field results in no text or OK/Cancel buttons b

		displayed. Text wrapping occurs at the word level, not the character level. For in you have a single word that is more than approximately 50 characters i will not wrap and no scroll bar will be present, therefore the text will
Crypto Erase Password	String 0-100 characters	*String 0-100 characters* A word or code of up to 100 characters used as a fail-safe security mec Entering this word or code in the user name or password field during th authentication deletes the authentication tokens for all users and locks Afterward, only an administrator can forcibly unlock the device. Leave this field blank if you do not want to have a crypto erase passwo in case of emergency.
Self Help Questions (Pre-8.0 clients)	At least 3 selectable questions	Specify the questions that will be presented to Windows users during re questions setup. Separate each question by a carriage return. These qu be used if the Windows password is forgotten. At least 3 questions mus specified. What is the name of your first pet? Who was your first employer? What was the first concert you attended? What was the make of the first car you owned? What was the last name of your third grade teacher? In what city or town did your mother and father meet? In what city or town was your first job?
Initial Access Code	String 1-100 characters	*String 1-100 characters* This policy is used to log on to an endpoint computer when network ac unavailable. Meaning, access to the EE Server or VE Server and Active D (AD) are both unavailable. The Initial Access Code policy should only be absolutely necessary, it is not the recommended method to log in. Usin Access Code policy does not provide the same level of security as the u authentication method of logging in using User Name, Domain, and Pas The Initial Access Code can only be used one time, immediately after a The first domain login that occurs after the Initial Access Code is enter cached and the Initial Access Code entry field will not be displayed aga
Encryption Administrator Password	String	Computer-generated password used by server and client for recovery a internal processes. No end user or Administrator interaction is required If there is a list of passwords in the inherited value and none in local va the inherited list is added to the local list and the new password is put bottom of the list upon Save. If there is a list of passwords in the inherited value and a list in local va the new password is put at the bottom of the existing local value list u Clicking Reset has no effect on this policy. All values are maintained in NOTE: After a value is entered for this policy, it can never be deleted. value for this policy does not affect the Override Count.
Non-Cached User Login Attempts Allowed	50	*Any number* This policy does not come into play when connected to the network (th connection to AD), because authentication with AD is attempted. This policy only comes into play when the computer is not connected t network and an unknown user attempts to log in (meaning, a user that logged in to the computer before -- no credentials have been cached).
Cached User Login Attempts Allowed	10	*1-20 times* Number of times that a cached user can attempt to log in.
Self Help Question/Answer Attempts Allowed	3	*1-10 times* Number of times the user can attempt to enter the correct answer.

Enable One Step Logon	Selected	This policy simplifies the logon process when multi-factor authenticatio enabled at both preboot and Windows logon. If selected (or not configu authentication is required at preboot only, and users are automatically to Windows. If not selected, authentication may be required multiple t
Number of Shutdown/Restart Delays Allowed	5	*1-25 times* Number of times that a user is allowed to snooze/delay a shutdown/re being forced to shutdown/restart. TPM requires a reboot. SED requires a shutdown.
Length of Each Shutdown/Restart Delay	300 seconds	*300-30000 seconds* Number of seconds between each time the user is asked to shutdown/r TPM requires a reboot. SED requires a shutdown.
Length of Forced Shutdown/Restart Notice	60 seconds	*60-1800 seconds* When user has reached the maximum number of authorized shutdown/ snoozes/delays, this policy sets the number of seconds allowed before shutdown/restart. TPM requires a reboot. SED requires a shutdown.
Enable Plugin	Selected	The plugin must remain selected. To deactivate the PBA and disable SE Management, toggle the *Self-encrypting Drive* policy to OFF.
See basic settings		

Policy	Default Setting	Description
Hardware Crypto Accelerator (HCA)		
Allow User Approval of Secondary Drive Encryption	Not selected	Allows users to decide if additional drives are encrypted.
Encryption Algorithm	AES256	AES 256 or AES 128 Encryption algorithm used to encrypt data at the Enterprise, Endpoint Endpoints levels. Encryption algorithms in order of speed, fastest first, are AES 128, AES
Forensic Meta Data Available on HCA Encrypted Drive	Not Selected	When selected, forensics meta data is included on the drive to facilitat Meta data included: • Machine ID (MCID) of the current machine • Device ID (DCID/SCID) of the current Shield installation When not selected, forensics meta data is not included on the drive. More... Switching from not selected to selected will re-sweep, based on the HC to add forensics. This policy is intended to help forensic vendors find the GUIDs more ea automate the key retrieval for the Forensic Admin through our forensic library. If this policy is not selected, meaning the GUIDs are not includ drive, the forensic tool will just prompt the Forensic Admin for the ma the drive came from and the GUIDs will be retrieved that way. As alwa to retrieve the keys, you must provide a username and password that h authorized with the Forensic Admin privilege.

Encryption Administrator Password	String	Computer-generated password used by server and client for recovery a internal processes. No end user or Administrator interaction is required If there is a list of passwords in the inherited value and none in local va the inherited list is added to the local list and the new password is put bottom of the list upon Save. If there is a list of passwords in the inherited value and a list in local va the new password is put at the bottom of the existing local value list u Clicking Reset has no effect on this policy. All values are maintained in NOTE: After a value is entered for this policy, it can never be deleted. value for this policy does not affect the Override Count.
See basic settings		
Policy	**Default Setting**	**Description**
Policy-Based Encryption		
Encrypt with SDE when SED is detected	Not Selected	When Selected, this policy applies SDE encryption to self-encrypting dr this policy when SDE encryption is preferred instead of native SED encr
User Encrypted Folders	String	String - maximum of 100 entries of 500 characters each (up to a maxim characters) A list of folders on the endpoint hard drive to be encrypted with the Us Encryption Key or excluded from encryption. If the same folder is specified in this policy for multiple users of the sa endpoint, each file in that folder is encrypted for the first owner of the the policy takes effect, and can be decrypted only by that owner. More... Specify as for Common Encrypted Folders. This policy applies to all drives classified by Windows as Hard Disk Drive Computer). You cannot use this policy to encrypt drives or external me type displays as Removable Disk, use EMS Encrypt External Media instea
Application Data Encryption List	Exe List winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe winzip.exe winrar.exe onenote.exe onenotem.exe	String - maximum of 100 entries of 500 characters each We do not recommend adding explorer.exe or iexplorer.exe to the ADE unexpected or unintended results may occur. However, explorer.exe is the process used to create a new notepad file desktop using the right-click menu. Setting encryption by file extension the ADE list, provides more comprehensive coverage. Changes to this policy do not affect files already encrypted because of List process names of applications (without paths) whose new files you encrypted, separated by carriage returns. Do not use wildcards. More... You can also specify these process names (separated by commas) via th value HKLM\Software\Dell\CMGShield\ApplicationDataEncryptionList. The Shield encrypts all new files (not already being encrypted by Comm Encrypted Folders and User Encrypted Folders) on the current compute drives created by these application processes whenever they are owned currently-logged-on managed user. This may include files excluded fro encryption by Common Encrypted Folders and/or User Encrypted Folde The following folders and their subfolders are always excluded from en this policy: C:\Windows\system32 C:\Windows\Software Distribution C:\Windows\Security C:\System Volume Information\Program Files\Dell\(.dll.exe.sys.mac.ddp.wip.rty.nmd.inv) We strongly recommend not listing applications or installers that write critical files. Doing so could result in encryption of important system fi could make a Windows endpoint unbootable. Common process names:

		Outlook: outlook.exe Word: winword.exe FrontPage: frontpg.exe PowerPoint: powerpnt.exe Access: msaccess.exe WordPad: wordpad.exe Microsoft Paint: mspaint.exe Excel: excel.exe The following hard-coded system and installer process names are ignor specified in this policy (you can also add to this list via the registry valu HKLM\Software\Dell\CMGShield\EUWPrivilegedList): hotfix.exe, a Windows update process update.exe, a Windows update process setup.exe, a third-party installer process msiexec.exe, a third-party installer process wuauclt.exe, a Windows update process wmiprvse.exe, a Windows system process migrate.exe, a Windows update process unregmp2.exe, a Windows update process ikernel.exe, a third-party installer process wssetup.exe, the Windows Shield installer svchost.exe, a Windows system process
User Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt data at the individual user level. specify different values for different users of the same endpoint. Encryption algorithms in order of speed, fastest first, are AES 128, AES
SDE Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to for System Data Encryption. Encryption algorithms in order of speed, fastest first, are AES 128, AES
Common Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt data at the endpoint (all users) le System paging files are encrypted using AES 128. Encryption algorithms in order of speed, fastest first, are AES 128, AES
Encrypt Outlook Personal Folders	Selected	Encrypts Outlook Personal Folders (%csidl:local_appdata %\Microsoft\Outlook) with the User Data Encryption Key.
Encrypt Temporary Files	Selected	When this policy is selected, the paths listed in the environment variab and TMP are encrypted. TEMP and TMP for the OS are encrypted with t Encryption Key. TEMP and TMP for the User are encrypted with the Use Encryption Key. To reduce encryption sweep time, the Shield clears the contents of the TMP folders for initial encryption, as well as updates to this policy. How your organization uses a third-party application that requires the file s within the \temp directory to be preserved, you should prevent this de To disable temporary file deletion, create DeleteTempFiles (REG_DWO its value to 0 in the registry at HKLM\SOFTWARE\Dell\CMGShield.
Encrypt Temporary Internet Files	Not Selected	When this policy is selected, the path listed in the environment variabl CSIDL_INTERNET_CACHE is encrypted with the User Data Encryption Ke To reduce encryption sweep time, the Shield clears the contents of CSIDL_INTERNET_CACHE for initial encryption, as well as updates to th This policy is applicable when using Microsoft Internet Explorer only. F party web browsers such as Mozilla and Opera, an Administrator must c encryption policy that is specific to the storage location of the tempora files used by each browser.
Encrypt User	Selected	When this policy is selected, the following are encrypted:

Profile Documents		• The My Documents folder on Windows XP and the users profile (C:\Us on Window 7 with the User Data Encryption Key • \All Users\Shared Documents on Windows XP and \Users\Public on Wir the Common Encryption Key
Encrypt Windows Paging File	Selected	When this policy is selected, the Windows paging file is encrypted. A cl policy requires a reboot.
Managed Services		String - maximum of 100 entries of 500 characters each (up to a maxim characters) When a Service is managed by this policy, the Service is started only af is logged in and the Shield is unlocked. This policy also ensures that th managed by this policy is stopped before the Shield is locked during log policy can also prevent a user logoff if a Service is unresponsive. More... Syntax is one Service name per line. Spaces in the Service name are su Wildcards are not supported. Entries are not case-sensitive. For example, GoogleDesktop Manager is googledesktopmanager. The Service log on as setting has no bearing on whether or not the Shie control it. It does not matter if a user logs on with user credentials ver system. The startup type (Automatic or Manual) does not affect the ability of th control it. Automatic or Manual startup is acceptable. Managed Services will not be started if an unmanaged user logs on.
Secure Post-Encryption Cleanup	Single Pass Overwrite	No Overwrite, Single-pass Overwrite, Three-pass Overwrite, Seven-pass Once folders specified via other policies in this category have been enc policy determines what happens to the unencrypted residue of the orig • No Overwrite deletes it. This value yields the fastest encryption proc • Single-pass Overwrite overwrites it with random data. • Three-pass Overwrite overwrites it with a standard pattern of 1s and with its complement, and then with random data. • Seven-pass Overwrite overwrites it with a standard pattern of 1s and with its complement, and then with random data five times. This value most difficult to recover the original files from memory, and yields the secure encryption processing.
Secure Windows Credentials	Selected	When this policy is selected, the Windows Credentials will be secured b encrypting the entire registry with the exception of registry informatio for computer boot. The information required for computer boot includ HKLM/SYSTEM and all sub-keys. This policy value will be automatically set to Selected if SDE is enabled More... When a change to this policy is delivered, the Shield requires a reboot. this reboot, configure the following policies: Force Reboot on Update, Each Reboot Delay, and Number of Reboot Delays Allowed.
Block Unmanaged Access to Domain Credentials	Selected	This policy prevents unmanaged users and applications from accessing domain credentials when a user is logged in.
Secure Windows Hibernation File	Selected	When this policy is selected, the hibernation file will be encrypted only computer enters hibernation. The Shield will disengage protection whe computer comes out of hibernation, providing protection without impa or applications while the computer is in use.
Prevent Unsecured Hibernation	Selected	When this policy is selected, the Shield will not allow computer hiberna Shield is unable to encrypt the hibernation data.
Scan Workstation on Logon	Not selected	When this policy is selected, all current and previous encrypted folder Shielded computer's local hard drives are scanned each time a manage on, ensuring that all Common Encrypted Folders and User Encrypted Fo values are properly implemented. Uses Workstation Scan Priority.
Workstation Scan Priority	Normal	Highest, High, Normal, Low, Lowest Specifies the relative Windows priority of encrypted folder scanning. H Highest prioritize scanning speed over computer responsiveness, Low a

		prioritize computer responsiveness over scanning speed and favor othe intensive activities, and Normal balances the two. The Shield checks for a changed Workstation Scan Priority before proce next file. The scan priority levels are used in two different ways. 1. These values correspond with the values used by the Microso set thread execution priority. 2. The Shield uses these values to introduce a delay in the encr sweep after every single file is processed. The values translate to the following millisecond delay ranges encryption thread will sit idle and then return full control to t operating system: Highest=0 ms / Lowest=100 ms
User Data Encryption Key	Common	Common, User, User Roaming Choose a key to indicate who should be able to access files encrypted b following policies, and where: • User Encrypted Folders • Encrypt Outlook Personal folders • Encrypt Temporary Files (\Documents and Settings\username\Local Se only) • Encrypt Temporary Internet Files • Encrypt User Profile Documents (except \All Users\Documents or for V \All Users\Shared Documents) Select: • Common if you want User Encrypted Files/Folders to be accessible b managed users on the endpoint where they were created (the same lev as Common Encrypted Folders), and encrypted with the Common Encry Algorithm. More... The Common Encryption Algorithm controls the encryption algorithm fo Encrypted Folders and overrides any encryption algorithm selected, inc default User Encryption Algorithm. For example, if the Common Encryp Algorithm is set to AES 256, all Common and User Encrypted Files/Fold encrypted with the AES 256 algorithm. All other Shield encryption parameters can be selected to override defa settings. For example, if the Encrypt Temporary Files policy is set to Fa override this setting for any Managed User by setting this value to True Designated User Encrypted Folders will use Common Key, resulting in a users having the key to access any encrypted files stored in these folde permitted by security settings on the operating system. • User if you want these files to be accessible only to the user who cre only on the endpoint where they were created (the same level of acces Encrypted Folders), and encrypted with the User Encryption Algorithm. • User Roaming if you want these files to be accessible only to the user created them, on any Shielded Windows endpoint, and encrypted with Encryption Algorithm. If you elect to incorporate an encryption policy to encrypt entire disk p is recommended to use the default SDE encryption policy, rather than User. This ensures that any operating system files that are encrypted a accessible during states when the managed user is not logged in.
Policy Proxy Connections		String - maximum of 1500 characters List fully qualified Policy Proxy hostnames, or IP addresses, separated b returns. More... Once the Shield finds a valid entry, the remainder of the entries are ig Entries are processed in the following order: 1. GKConnections Override (this registry entry overrides all other entri 2. GKConnections (this registry entry is set automatically by the Shield the this policy) 3. GK

		This policy works in conjunction with the Policy Proxy Polling Interval p To override this policy and specify ports via the registry item HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CMGShield\GKConnectionsOverride. You cannot specify ports in this policy. The Shield communicates with Policy Proxies using the GKPORT specifi Shield installation (the default is 8000). If necessary, change that port via the registry item HKLM\Software\Microsoft\WindowsNT\Current Version\Winlogon\CMGShield\GKPort. Inherited values for this policy accumulate. In order for the Shield to connect to a Policy Proxy specified in this pol be in the same group as the Policy Proxy specified during Shield installa Because the Shield supports up to 255 users per endpoint, this policy is only at the Enterprise Policies level.
Policy Proxy Polling Interval	360	1-1440 minutes The interval that the Shield attempts to poll Policy Proxy for policy upd send inventory information to Policy Proxy. The Shield also attempts to poll Policy Proxy each time a user logs on.
Allow Activations	Selected	Precedence: Max, High, Medium, Low, Min When this policy is selected, the Server allows endpoint activations at Enterprise, Domain, User Group, or User levels. When this policy is not selected, for example, activations can be stagg blocked during initial Server setup and maintenance interruptions. For information, see Temporarily Block Activations.
Current Shield State	Activate	Activate, Suspend Activate is the normal state for a Shielded user. A user must be in this order to activate an endpoint. To require endpoint recovery before the user can access the endpoint, Suspend. When a user is suspended, encrypted data cannot be accessed. The use recovered by pushing down a new policy to unsuspend the user.
See basic settings		
Policy-Based Encryption - User Experience		
Enable Software Auto Updates	Not Selected	*Selected* *Not Selected* Selected enables the client update agent to automatically check for up Dell Data Protection software. If this policy is not selected, no DDP Aut take place, regardless of other policies. If this policy is set, the On Pre Update Staging Location must have a network location in its value.
On Premise Update Staging Location	String	*String* Network location (UNC) where DDP Server stages Dell Data Protection u packages. If a network location is not specified in this policy, the Enab Auto Updates policy should not be published.
Update Check Period	10080	*1-43200 minutes (30 days)* The period in minutes between checks for updates.
Number of Policy Update Delays Allowed	3	0-5000 If Force Logoff/Reboot on Policy Updates is Selected, a non-zero value user to delay the required logoff or reboot the specified number of tim zero to disable delays.
Force Logoff / Reboot on Policy Updates	Selected	Selected requires either a logoff or a reboot in order for key policy upd effect. Otherwise, these policy updates take effect whenever the next reboot occurs.

Policy Viewer Enabled	Not Selected	When Selected, the end-user can view their Windows Shield policies fr Shield icon.
Display Local Encryption Processing Control	Not Selected	When Selected, the user sees a menu option in the system tray icon th them to pause/resume encryption/decryption (depending on what the currently doing). **Important:** *Allowing a user to pause encryption could allow the user t the Shield from fully encrypting or decrypting data per policy.*
Suppress File Contention Notification	Selected	This policy controls whether users see notification pop-ups if an applic attempts to access a file while the Shield is processing it. More... If the Shield is processing a large file that an application needs, and th enabled, it may appear that the application is unresponsive or slow to no message indicating what the issue is). Care should be taken when u policy.
Number of Encryption Processing Delays Allowed	0	0-5000 A non-zero value allows the user to delay any encryption processing re the encryption policies you set, the specified number of times. Set to z disable delays.
Length of Each Encryption Processing Delay	5	5-40320 minutes If Number of Encryption Processing Delays Allowed has a non-zero valu policy to specify how often the Shield prompts the user to continue wi encryption processing or delay again. More... The Shield displays this prompt for five minutes each time. If the user respond to the prompt, encryption processing begins. The final delay p includes a countdown and progress bar, and it displays until the user re the final delay expires and encryption processing begins. Calculate the maximum possible delay as follows (a maximum delay wo the user responding to each delay prompt immediately prior to the 5-m mark): (Number of Encryption Processing Delays Allowed x Length of Each Enc Processing Delay) + (5 minutes x [Number of Encryption Processing Dela 1])
Length of Each Policy Update Delay	15	5-40320 minutes If Number of Policy Update Delays Allowed has a non-zero value, use th specify how often the Shield prompts the user to logoff/reboot or dela More... The Shield displays this prompt for five minutes each time. If the user respond to the prompt, the next delay begins. The final delay prompt i countdown and progress bar, and it displays until the user responds, or delay expires and the required logoff/reboot occurs. You can change the behavior of the user prompt to begin or delay encr prevent encryption processing following no user response to the promp To do this, set the registry key SnoozeBeforeSweep |(DWORD), stored i HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGSh non-zero value. Any non-zero value will change the default behavior to With no user interaction, encryption processing will be delayed up to t of configurable allowed delays. When the final delay expires, encryptio processing begins. Calculate the maximum possible delay as follows (a maximum delay wo the user never responding to a delay prompt, each of which displays fo minutes): (Number of Policy Update Delays Allowed x Length of Each Policy Upda (5 minutes x [Number of Policy Update Delays Allowed - 1])
Force Reboot on Update	Selected	When selected, the computer immediately reboots to allow processing encryption or updates related to device-based policy, such as System D Encryption (SDE).
Length of Each Reboot Delay	15	5-40320 minutes The number of minutes to delay when the user chooses to delay reboot

		based policy.
Number of Reboot Delays Allowed	3	0-5000 The number of times the user will be allowed to delay reboot for devic policy.
Allow Encryption Processing Only When Screen is Locked	Not Selected	Selected, Not Selected, User-Optional When Selected, there will be no encryption or decryption of data while actively working. The Shield will only process data when the screen is l User-Optional adds an option to the system tray icon allowing the user feature on or off. When Not Selected, encryption processing will occur any time, even wh is working. Enabling this option will significantly extend the amount of time it take complete encryption or decryption.
Hide Overlay Icons	Selected	When Selected, encryption overlay icons do not display on encrypted fi Explorer for all managed users on an endpoint.
See basic settings		
Policy	**Default Setting**	**Description**
Bitlocker Encryption		
Disable BitLocker on Self-Encrypting Drives	Selected	*Selected* *Not Selected* If Selected, BitLocker Manager will not start encryption on a volume th protected by an activated SED. For example, if this policy is Selected and both C: and D: are on one ph encrypting drive, and the PBA has been activated, then C: and D: will n for BitLocker even if System and Fixed drive encryption are turned on i BitLocker policies.
See basic settings		
Bitlocker Encryption - Fixed Data Volume Settings		
Configure the Use of Smart Cards on Fixed Data Drives	Allow	*Allow* *Disallow* *Require* This policy specifies whether smart cards can be used to authenticate a BitLocker fixed data drives. These settings are enforced when turning o BitLocker, not when unlocking a drive. BitLocker will allow unlocking a any of the protectors available on the drive.
Deny Write Access to Fixed Data Drives Not Protected by BitLocker	Enabled	*Enabled* *Disabled* *Enabled for Organizations* If the drive is protected by BitLocker, it will be mounted with read and access. If you disable or do not configure this policy setting, all fixed data driv computer will be mounted with read and write access.
Allow Access to BitLocker Protected Fixed Data Drives from Earlier Versions of Windows	Selected	*Selected* *Not Selected* When Enabled, fixed data drives with the FAT file system can be unlock computers running Windows Server 2008, , XP SP3 and their contents ca viewed. This policy does not apply to drives that are formatted with th system. Set this policy to Selected and the Do Not Install BitLocker to Go Reade formatted Fixed Drives policy to Not Selected to allow BitLocker to Go

		be installed on the fixed drive.
Do Not Install BitLocker to Go Reader on FAT Formatted Fixed Drives	Selected	*Selected* *Not Selected* If this policy is Not Selected, BitLocker to Go Reader will be installed o drive to enable users to unlock the drive on computers running Window 2008, , XP SP3 that do not have the BitLocker to Go Reader installed. Set this policy to Not Selected and the Allow Access to BitLocker Prote Data Drives from Earlier Versions of Windows policy to Not Selected to BitLocker to Go Reader to be installed on the fixed drive.
Configure Use of Passwords for Fixed Data Drives	Allow	*Allow* *Require* *Disallow* When set to Require, a connection to a domain controller is necessary the complexity of the password. When set to Allow, a connection to a controller will be attempted to validate complexity, but if no domain found, the password will still be accepted. When set to Do Not Allow, complexity validation will be done. To use this policy, Configure Use of Passwords for Fixed Data Drives mu Allow or Require.
Configure Password Complexity for Fixed Data Drives	Allow	*Do Not Allow* *Require* *Allow* When set to Require, a connection to a domain controller is necessary the complexity of the password. When set to Allow, a connection to a controller will be attempted to validate complexity, but if no domain found, the password will still be accepted. When set to Do Not Allow, complexity validation will be done. To use this policy, Configure Use of Passwords for Fixed Data Drives mu Allow or Require.
Minimum Password Length for Fixed Data Drives	8	*8 min* *20 max* Passwords must be at least 8 characters. To configure a greater minimu for the password enter the desired number of characters. To use this policy, Configure Use of Passwords for Fixed Data Drives mu Allow or Require.
Encryption Type for Fixed Data Drives	Full Encryption	*Allow User to Choose* *Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for Fixed Data Drives.
Choose How BitLocker-protected Fixed Drives Can be Recovered	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, ever value is Not Selected. This policy allows for the control of how BitLock fixed data drives are recovered in the absence of the required credent More... This policy is the parent policy to: Allow Data Recovery Agent for Protected Fixed Data Drives Config User Storage of BitLocker 48-digit Recovery Password Config User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard Save BitLocker Recovery Info to AD DS for Fixed Data Drives BitLocker Recovery Info to Store in AD DS Do Not Enable BitLocker Until Recovery Info is Stored in AD DS for Fixe Drives
Allow Data Recovery Agent for Protected	Selected	*Selected* *Not Selected*

Fixed Data Drives		When Selected, a data recovery agent is allowed for use with BitLocke fixed data drives. Before the agent can be used, it must be added from Key Policies in either the Group Policy Management Console or the Loc Policy Editor. When setting this policy to Selected, the Choose How BitLocker-protec Drives Can be Recovered policy must also be set to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Allow* *Require* *Do Not Allow* This policy determines if a user is allowed, required, or not allowed to 48-digit password. When setting this policy to Allow or Require, the Choose How BitLocke Fixed Drives Can be Recovered policy must also be set to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Allow* *Require* *Do Not Allow* This policy determines if a user is allowed, required, or not allowed to 256-bit recovery key. When setting this policy to Allow or Require, the Choose How BitLocke Fixed Drives Can be Recovered policy must also be set to Selected.
Omit Recovery Options from the BitLocker Setup Wizard	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options w BitLocker is enabled. Recovery options for the drive are determined by settings. When setting this policy to Not Selected, the Choose How BitLocker-pr Fixed Drives Can be Recovered policy must also be set to Selected.
Save BitLocker Recovery Information to AD DS for Fixed Data Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS fo drives. BitLocker recovery information is always saved in the Remote M Console. Enabling this policy additionally saves the information to AD. More... The appropriate schema extensions and access control settings on the be first configured before AD DS backup can succeed. When setting this policy to True, the Choose How BitLocker-protected Can be Recovered policy must also be set to True. Set this policy to True to use the policy BitLocker Recovery Informatio AD DS.
BitLocker Recovery Information to Store in AD DS	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key p storing the recovery password only in AD DS. The appropriate schema e and access control settings on the domain must be first configured bef this policy. The Choose How BitLocker-protected Fixed Drives Can be Recovered po be set to Selected to use this policy. To use this policy, Save BitLocker Recovery Information to AD DS for Fi Drives must be set to Selected.
Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Fixed Data Drives	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically stored in the Management Console, this policy additionally requires BitLocker drive e recovery information to be stored in AD DS. The appropriate schema ex and access control settings on the domain must be configured before u policy. More... This policy is used to prevent users from enabling BitLocker unless the connected to the domain and the backup of the BitLocker recovery inf AD DS has succeeded.

		The Choose How BitLocker-protected Fixed Drives Can be Recovered po be set to True to use this policy.
Configure Use of Hardware-Based Encryption for Fixed Data Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on fi drives.
Use Hardware-Based Encryption for Fixed Data Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption for fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fix Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Fixed Data Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on fixed data dr hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Fix Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Fixed Data Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for Bit hardware encryption on fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fix Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites Settings on Fixed Data Drives	String	String - 2.16.840.1.101.3.4.1.2; 2.16.840.1.101.3.4.1.42 Set specific Crypto Algorithms and Cipher Suites on fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fix Drives must be set to Selected.
See basic settings		
Bitlocker Encryption - Global Settings		
Default Folder Location to Save Recovery Password		Qualified path Important: This policy is not used by BitLocker Manager, because it doe prompt the user when saving recovery passwords. Microsoft defines this policy as: This setting provides the default path t displayed when the BitLocker drive encryption setup wizard prompts th enter the location of a folder to save the recovery password.
Encryption Method and Cipher Strength	AES 128 with Diffuser	*AES 128 with Diffuser* *AES 256 with Diffuser* *AES 128* *AES 256* This policy specifies the encryption method and cipher strength used fo drive encryption. Note that changing this policy has no effect if the dri encrypted or encryption is in progress.
Enable Organizational Unique Identifiers	Not Selected	*Selected* *Not Selected* This policy allows for the association of unique organizational identifie drive that is enabled with BitLocker. These identifiers are stored as the identification field and allowed identification field. The allowed identi field is used in combination with the Deny Write Access to Removable D Protected by BitLocker policy to help control the use of removable driv organization. This policy must be set to Selected to use the policies Set Organization Identifiers and Set Allowed Org Unique Identifiers.

Set Organizational Unique Identifiers		*Up to 260 characters* The identification field allows you to associate a unique organizational BitLocker-protected drives. This identifier is automatically added to ne BitLocker-protected drives and can be updated on existing BitLocker-p drives using the Manage-BDE command-line tool. An identification field for management of certificate-based data recovery agents on BitLocke drives and for potential updates to the BitLocker To Go Reader. BitLoc manage and update data recovery agents when the identification field matches the value configured in the identification field. In a similar ma BitLocker will only update BitLocker To Go Reader when the identificat the drive matches the value configured for the identification field. To use this policy, Enable Organizational Unique Identifiers must be se Selected.
Set Allowed Organizational Unique Identifiers		*Up to 260 characters* The allowed identification field is used in combination with the Deny W to Removable Drives Not Protected by BitLocker policy to help control removable drives in the organization. It is a comma separated list of id fields from your organization or other external organizations. To use this policy, Enable Organizational Unique Identifiers must be se Selected.
Prevent Memory Overwrite on Restart	Not Selected	*Selected* *Not Selected* Selected prevents memory from being overwritten on restart. Preventi overwrite may improve restart performance, but will increase the risk BitLocker secrets. When Not Selected, BitLocker secrets are removed f when the computer restarts.
Enable Smart Card Certificate Identifier	Not Selected	*Selected* *Not Selected* This policy allows or denies an object identifier to be specified for enh usage with a certificate. This policy must be set to Selected to use the policy Smart Card Certifi Identifier.
Smart Card Certificate Identifier	1.3.6.1.4.1.311.67.1.1	*1.3.6.1.4.1.311.67.1.1* This policy provides for an object identifier to be specified for enhance with a certificate. BitLocker can identify which certificates may be use authenticate a user certificate to a BitLocker drive by matching the ob identifier in the certificate with the object identifier that is defined by Use caution if changing the default value. To use this policy, Enable Smart Card Certificate Identifier must be set Selected.
See basic settings		
Bitlocker Encryption - Operating System Volume Settings		
Allow Enhanced PINs for Startup	Not Selected	*Selected* *Not Selected* Selected allows enhanced startup PINs to be used with BitLocker. Enhanced startup PINs permit the use of characters including uppercas lowercase letters, symbols, numbers, and spaces. This policy setting is when you turn on BitLocker.
Number of Characters Required in PIN	4	*4-20 digits* This policy configures the minimum length for a TPM startup PIN. The s must have a minimum length of 4 digits and can have a maximum of 20
Allow Network Unlock at Startup on Operating System Drives	Not Selected	*Selected* *Not Selected* This policy specifies if a user is allowed to use the Network Unlock at S feature on operating system drives.
Allow SecureBoot on Operating	Selected	*Selected* *Not Selected*

System Drives		This policy specifies if a user is allowed to use SecureBoot on operating drives.
Disallow Standard Users from Changing the PIN on Operating System Drives	Not Selected	*Selected* *Not Selected* This policy specifies if a standard user is allowed to change their PIN o system drives.
Enable Use of Preboot Keyboard Input on Slates	Not Selected	*Selected* *Not Selected* This policy specifies if a preboot keyboard input is enabled on Slates.
Reset Platform Validation Data After Recovery	Not Selected	*Selected* *Not Selected* This policy specifies if a preboot keyboard input is enabled on Slates.
Choose How BitLocker-protected Operating System Drives Can be Recovered	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, ever value is Not Selected. For the GPO, a Selected value allows you to spec BitLocker drives are recovered. More... This policy is the parent policy to: Allow Data Recovery Agent for Protected Operating System Drives Configure User Storage of BitLocker 48-digit Recovery Password Configure User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard Save BitLocker Recovery Info to AD DS for Operating System Drives BitLocker Recovery Information to Store in AD DS (Windows Server 2008 Do Not Enable BitLocker Until Recovery Information is Stored in AD DS Operating System Drives
Allow Data Recovery Agent for Protected Operating System Drives	Selected	*Selected* *Not Selected* The "Allow Certificate Based Data Recovery Agent" is used to specify w data recovery agent can be used with BitLocker operating system drive data recovery agent can be used, it must be added from the Public Key either the Group Policy Management Console or the Local Group Policy To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Do Not Allow* *Require* *Allow* This policy configures if a user is allowed, required, or not allowed to g 48-digit password. To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Do Not Allow* *Require* *Allow* This policy configures if a user is allowed, required or not allowed to g 256-bit recovery key. To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Omit Recovery Options from the BitLocker Setup Wizard	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options w BitLocker is enabled. Recovery options for the drive are determined by settings. To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.

Save BitLocker Recovery Information to AD DS for Operating System Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS fo system drives. Note that the appropriate schema extensions and access settings on the domain must be first configured before AD DS backup ca To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
BitLocker Recovery Information to Store in AD DS (Windows Server 2008 Only)	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key p storing the recovery password only in AD DS. The appropriate schema e and access control settings on the domain must be first configured befo this policy. This policy is applicable only to computers running Windows Server 200 To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Operating System Drives	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically stored in the Management Console, this policy additionally requires BitLocker drive e recovery information to be stored in AD DS. The appropriate schema ex and access control settings on the domain must be configured before u policy. This policy is used to prevent users from enabling BitLocker unless the connected to the domain and the backup of the BitLocker recovery info AD DS has succeeded. To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Configure Use of Hardware-Based Encryption for Operating System Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on op system drives.
Use Hardware-Based Encryption for Operating System Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption on operating system drive To use this policy, Configure Use of Hardware-Based Encryption for Ope System Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Operating System Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on operating sys if hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Ope System Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Operating System Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for Bit hardware encryption on operating system drives. To use this policy, Configure Use of Hardware-Based Encryption for Ope System Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites Settings on Operating System Drives	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	*String -* *2.16.840.1.101.3.4.1.2;* *2.16.840.1.101.3.4.1.42* Specific Crypto Algorithms and Cipher Suites allowed on operating syst To use this policy, Configure Use of Hardware-Based Encryption for Ope System Drives must be set to Selected.

Encryption Type for Operating System Drives	Full Encryption	*Allow User to Choose* *Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for operating system drives.
Configure Use of Passwords for Operating System Drives	Not Configured	*Enabled* *Disabled* *Not Configured* Configure password requirements for Operating System Drives.
Configure Password Complexity for Operating System Drives	Allow	*Allow* *Require* *Do Not Allow* When set to Require, a connection to a domain controller is necessary the complexity of the password. When set to Allow, a connection to a controller will be attempted to validate complexity, but if no domain found, the password will still be accepted. When set to Do Not Allow, complexity validation will be done. To use this policy, Configure Use of Passwords for Operating System Dr set to Enabled.
Minimum Password Length for Operating System Drives	8	*8-256* The default value is a password length of 8 characters. 8-256 character allowed. To use this policy, Configure Use of Passwords for Operating System Dr set to Enabled.
Require ASCII-Only Passwords for Operating System Drives	Not Selected	*Selected* *Not Selected* Require ASCII-only passwords for operating system drives to create stro passwords. To use this policy, Configure Use of Passwords for Operating System Dr set to Enabled.
Use Enhanced Boot Configuration Data Profile	Disabled	*Enabled* *Disabled* *Not Configured* Set this policy to Enable to allow the verification and exclusion of BCD
Verify Additional BCD Settings	String	*String* Specify the additional Boot Configuration settings. To use this policy, Use Enhanced Boot Configuration Data Profile must Enabled.
Exclude Additional BCD Settings	String	*String* Exclude specific Boot Configuration settings. To use this policy, Use Enhanced Boot Configuration Data Profile must Enabled.
Configure TPM Platform Validation Profile	Not Selected	*Selected* *Not Selected* Set to Selected to enable boot up TPM drive unlocking for Windows 7 a Server 2008 R2. Selected allows the configuration of how the TPM secu hardware secures the BitLocker encryption key. This policy does not ap computer does not have a compatible TPM or if BitLocker has already b on with TPM protection. This policy must be set to Selected to use the policy Configure Specific Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK more information.
Configure Specific TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off	This policy allows you to configure how the computer's TPM security ha secures the BitLocker encryption key. This policy setting does not appl computer does not have a compatible TPM or if BitLocker has already b on with TPM protection. This setting determines what values the TPM r when it validates early boot components before unlocking a drive on a running Windows 7 or Windows Server 2008 R2.

	PCR4,on PCR5,on PCR6,off PCR7,off PCR8,on PCR9,on PCR10,on PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off PCR22,off	More... If you enable this policy before turning on BitLocker, you can configure components that the TPM will validate before unlocking access to the E encrypted operating system drive. If any of these components change v BitLocker protection is in effect, the TPM will not release the encryptio unlock the drive and the computer will instead display the BitLocker re console and require that either the recovery password or recovery key to unlock the drive. If you disable or do not configure this policy, the TPM uses the default validation profile or the platform validation profile specified by the set platform validation profile consists of a set of Platform Configuration R (PCR) indices ranging from 0 to 23. The default platform validation pro the encryption key against changes to the Core Root of Trust of Measur (CRTM), BIOS, and Platform Extensions (PCR 0), the Option ROM Code (Master Boot Record (MBR) Code (PCR 4), the NTFS Boot Sector (PCR 8), Boot Block (PCR 9), the Boot Manager (PCR 10), and the BitLocker Acce (PCR 11). The descriptions of PCR settings for computers that use an Ex Firmware Interface (EFI) are different than the PCR settings described computers that use a standard BIOS. The BitLocker Drive Encryption De Guide on Microsoft TechNet contains a complete list of PCR settings fo and standard BIOS. **Warning:** Changing from the default platform validation profile affects and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depe inclusion or exclusion (respectively) of the PCRs. To use this policy, Configure TPM Platform Validation Profile must be s
Configure BIOS TPM Platform Validation Profile	Not Selected	Selected Not Selected Set to Selected to enable boot up BIOS TPM drive unlocking. Selected a configuration of how the BIOS TPM security hardware secures the BitLo encryption key. This policy does not apply if the computer does not hav compatible TPM or if BitLocker has already been turned on with TPM pr This policy must be set to Selected to use the policy Configure Specific Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK_ more information.
Configure Specific BIOS TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off PCR4,on PCR5,off PCR6,off PCR7,off PCR8,on PCR9,on PCR10,on PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off	This policy setting allows you to configure how the computer's TPM sec hardware secures the BitLocker encryption key. This setting determine values the TPM measures when it validates early boot components befo an operating system drive on a computer with BIOS configuration or wi firmware that has the Compatibility Support Module (CSM) enabled. If you enable this policy before turning on BitLocker, you can configure components that the TPM will validate before unlocking access to the E encrypted operating system drive. If any of these components change v BitLocker protection is in effect, the TPM will not release the encryptio unlock the drive and the computer will instead display the BitLocker re console and require that either the recovery password or recovery key to unlock the drive. To use this policy, Configure BIOS TPM Platform Validation Profile must Selected.

	PCR22,off	
Configure UEFI TPM Platform Validation Profile	Not Selected	*Selected* *Not Selected* Set to Selected to enable boot up UEFI TPM drive unlocking. Selected a configuration of how the UEFI TPM security hardware secures the BitLo encryption key. This policy does not apply if the computer does not ha compatible TPM or if BitLocker has already been turned on with TPM p This policy must be set to Selected to use the policy Configure Specific Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK for more information.
Configure Specific UEFI TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off PCR4,on PCR5,off PCR6,off PCR7,off PCR8,off PCR9,off PCR10,off PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off PCR22,off	This policy setting allows you to configure how the computer's TPM sec hardware secures the BitLocker encryption key. This setting determine values the TPM measures when it validates early boot components befo an operating system drive on a computer with native UEFI firmware co If you enable this policy before turning on BitLocker, you can configure components that the TPM will validate before unlocking access to the E encrypted operating system drive. If any of these components change v BitLocker protection is in effect, the TPM will not release the encryptio unlock the drive and the computer will instead display the BitLocker re console and require that either the recovery password or recovery key to unlock the drive. To use this policy, Configure UEFI TPM Platform Validation Profile must Selected.
See basic settings		
Bitlocker Encryption - Removable Storage Settings		
Allow User to Apply BitLocker Protection on Removable Drives	Selected	*Selected* *Not Selected* When Selected, users are permitted to run the BitLocker setup wizard removable data drive.
Allow User to Suspend and Decrypt BitLocker Protection on Removable Data Drives	Not Selected	*Selected* *Not Selected* When Selected, users are authorized to suspend and decrypt BitLocker on removable data drives.
Configure Use of Smart Cards on Removable Data Drives	Allow	*Allow* *Disallow* *Require* This policy specifies whether smart cards can be used to authenticate BitLocker removable data drives. These settings are enforced when tur BitLocker, not when unlocking a drive. BitLocker will allow unlocking a

		any of the protectors available on the drive.
Deny Write Access to Removable Drives Not Protected by BitLocker	Enabled	*Enabled* *Disabled* *Enabled for Organization* If this policy is enabled, all removable drives that are not BitLocker pro be mounted as read only. If this policy is disabled, all removable drives computer will be mounted with read and write access.
Allow Access to BitLocker Protected Removable Data Drives from Earlier Versions of Windows	Selected	*Selected* *Not Selected* When Selected, removable data drives with the FAT file system can be computers running Windows Server 2008, , or XP SP3 and their content viewed. This policy does not apply to drives that are formatted with th system.
Do Not Install BitLocker to Go Reader on FAT formatted Removable Drives	Selected	*Selected* *Not Selected* If this policy is Not Selected, removable data drives formatted with the system that are BitLocker protected cannot be unlocked on computers Windows Server 2008, , or XP SP3. Bitlockertogo.exe will not be install
Configure Use of Passwords for Removable Data Drives	Allow	*Allow* *Require* *Disallow* This policy specifies whether a password is required to unlock BitLocke data drives. These settings allow the use of a password, require the us password, or disallow the use of a password. This policy must be set to Allow or Require to use the Configure Passwo Complexity for Removable Data Drives and Minimum Password Length f Removable Data Drives polices.
Configure Password Complexity for Removable Data Drives	Allow	*Allow* *Require* *Disallow* When set to Require, a connection to a domain controller is necessary the complexity of the password. When set to Allow, a connection to a controller will be attempted to validate complexity, but if no domain found, the password will still be accepted. When set to Do Not Allow, complexity validation will be done. To use this policy, Configure Use of Passwords for Removable Data Driv set to Allow or Require.
Minimum Password Length for Removable Data Drives	8	*8-20 characters* Passwords must be at least 8 characters in length, with a maximum of characters. To use this policy, Configure Use of Passwords for Removable Data Driv set to Allow or Require.
Encryption Type for Removable Data Drives	Full Encryption	*Allow User to Choose* *Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for Removable Data Drives.
Choose How BitLocker-protected Removable Drives Can be Recovered	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, ever value is Not Selected. This policy allows for the control of how BitLock removable data drives are recovered in the absence of the required cre More... This policy is the parent policy to: Allow Data Recovery Agent for Protected Removable Data Drives Configure User Storage of BitLocker 48-digit Recovery Password Configure User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard for Removable

		Save BitLocker Recovery Information to AD DS for Removable Data Driv BitLocker Recovery Info to Store in AD DS for Removable Data Drives Do Not Enable BitLocker Until Recovery Info is Stored in AD DS for Rem
Allow Data Recovery Agent for Protected Removable Data Drives	Selected	*Selected* *Not Selected* When Selected, a data recovery agent is allowed for use with BitLocke removable data drives. Before the agent can be used, it must be added Public Key Policies in either the Group Policy Management Console or t Group Policy Editor. To use this policy, Choose How BitLocker-protected Removable Drives Recovered must be to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Allow* *Require* *Do Not Allow* This policy configures if a user is allowed, required, or not allowed to g 48-digit password. To use this policy, Choose How BitLocker-protected Removable Drives Recovered must be to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Allow* *Require* *Do Not Allow* This policy configures if a user is allowed, required, or not allowed to g 256-bit recovery key. To use this policy, Choose How BitLocker-protected Removable Drives Recovered must be to Selected.
Omit Recovery Options from the BitLocker Setup Wizard for Removable Media	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options w BitLocker is enabled. Recovery options for the drive are determined by settings. To use this policy, Choose How BitLocker-protected Removable Drives Recovered must be to Selected.
Save BitLocker Recovery Information to AD DS for Removable Data Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS fo data drives. The appropriate schema extensions and access control set domain must be first configured before AD DS backup can succeed. To use this policy, Choose How BitLocker-protected Removable Drives Recovered must be to Selected. Set this policy to Selected to use the policy BitLocker Recovery Informa Store in AD DS for Removable Data Drives.
BitLocker Recovery Information to Store in AD DS for Removable Data Drives	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key p storing the recovery password only in AD DS. The appropriate schema e and access control settings on the domain must be first configured befo this policy. To use this policy, Choose How BitLocker-protected Removable Drives Recovered must be to Selected. To use this policy, Save BitLocker Recovery Information to AD DS for Re Data Drives must be set to Selected.
Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Removable Data Drives	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically stored in the Management Console, this policy additionally requires BitLocker drive e recovery information to be stored in AD DS. Note that the appropriate extensions and access control settings on the domain must be configure using this policy. This policy is used to prevent users from enabling BitLocker unless the

		connected to the domain and the backup of the BitLocker recovery info AD DS has succeeded. To use this policy, Choose How BitLocker-protected Removable Drives Recovered must be to Selected.
Configure Use of Hardware-Based Encryption for Removable Data Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on re data drives.
Use Hardware-Based Encryption for Removable Data Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption on removable data drives To use this policy, Configure Use of Hardware-Based Encryption for Rer Data Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Removable Data Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on removable da hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Rer Data Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Removable Data Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for Bit hardware encryption. To use this policy, Configure Use of Hardware-Based Encryption for Rer Data Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites Settings on Removable Data Drives	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	*String -* *2.16.840.1.101.3.4.1.2;* *2.16.840.1.101.3.4.1.42* Specific Crypto Algorithms and Cipher Suites allowed. To use this policy, Configure Use of Hardware-Based Encryption for Rer Data Drives must be set to Selected.
See basic settings		
Policy	**Default Setting**	**Description**
Server Encryption		
Server Encryption	On	*On* *Off* This policy enables or disables System Data Encryption (SDE) and Comm Encryption on the client server. Toggle to ON to enable both System Data Encryption (SDE) and Commo Encryption. Changing the value of this policy triggers a new sweep to encrypt/decr
Allow Software Server Encryption	Selected	*Selected* *Not Selected* Selected means that the Server allows client server endpoint activation Enterprise level. This policy may be set to Not Selected to block activations during initia setup and maintenance interruptions.
Max Network Failed Attempts	3	*1-10* Number of successive failed attempts for the client server to connect t Server before the Encryption client locks the encryption keys.

Retry Interval to connect to DDP Server	5	*1-60 minutes* Time interval for the client server to attempt to connect to Dell Server
Retry if Authentication Fails Upon Network Failure	Selected	*Selected* *Not Selected* If Selected, the client server continues to attempt to contact Dell Serv first attempt fails due to a network failure.
Retry Interval Upon Network Failure	10	*10-60 minutes* The length of time between attempts to contact Dell Server if the first fails due to a network failure. The *Retry if Authentication Fails Upon N Failure* policy must be set to Selected for this policy to be enforced.
Server Maintenance Schedule	Not Selected	This policy is the "master policy" for all other Server Maintenance polic policy is Not Selected, no Server Maintenance policies are enforced, re other policy values. Selected allows a maintenance schedule to control application of polic requires a reboot.
Server Maintenance Schedule Repeats	Weekly	*Daily, Weekly, Monthly, Quarterly, Annually* The schedule configuration defines when the task should run. Schedule Daily, Weekly, Monthly, Quarterly, and Annually. Daily: Runs the task every day at the specified Server Maintenance Sch Time. Weekly: Runs the task weekly on the days specified in Server Maintena the Week. Monthly: Runs the task monthly on the specified Server Maintenance Da Month. Quarterly: Runs the task quarterly on the specified Server Maintenance Month. Annually: Runs the task annually on the specified Server Maintenance D Month.
Server Maintenance Schedule Start Time	21:00	String - format is [HH:mm]. Example: 11:59 PM The time the task should run.
Server Maintenance Day of the Week	Saturday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Server Maintenance Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
Infinite Suppress	Not Selected	When Selected, an automatic reboot is suppressed indefinitely.
Port Control System	Disabled	Enable or Disable all Port Control System policies. If this policy is set to Port Control System policies are applied, regardless of other Port Contr policies. **Note**: PCS policies require a reboot before the policy takes effect.
Port: Express Card Slot	Enabled	Enable, Disable, or Bypass ports exposed through the Express Card Slot
Port: USB	Enabled	Enable, Disable, or Bypass port access to external USB ports. **Note:** USB port-level blocking and HID class-level blocking is **only** hono can identify the computer chassis as a laptop/notebook form-factor. W the computer's BIOS for the identification of the chassis.
Port: eSATA	Enabled	Enable, Disable, or Bypass port access to external SATA ports.
Port: PCMCIA	Enabled	Enable, Disable, or Bypass port access to PCMCIA ports.
Port: Firewire (1394)	Enabled	Enable, Disable, or Bypass port access to external Firewire (1394) ports
Port: SD	Enabled	Enable, Disable, or Bypass port access to SD card ports.

Port: Memory Transfer Device (MTD)	Enabled	Enable, Disable, or Bypass access to Memory Transfer Device (MTD) por
Class: Storage	Enabled	PARENT to the next 3 policies. Set this policy to Enabled to use the nex Storage polices. Setting this policy to Disabled disables all 3 Subclass S policies - no matter what their value.
Subclass Storage: External Drive Control	Full Access	CHILD of Class: Storage. Class: Storage must be set to Enabled to use th This policy interacts with the Removable Storage - EMS Access to unShi policy. If you intend to have Full Access to media, also set this policy t to ensure that the media is not set to read only and the port is not bloc Full Access: External Drive port does not have read/write data restricti Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Subclass Storage: Optical Drive Control	UDF Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use th Full Access: Optical Drive port does not have read/write data restrictio UDF Only: Blocks all data writes that are not in the UDF format (CD/DV ISO burning). Read data is enabled. Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy. Universal Disk Format (UDF) is an implementation of the specification k ISO/IEC 13346 and ECMA-167 and is an open vendor-neutral file system computer data storage for a broad range of media. To encrypt data written to CD/DVD media: Set EMS Encrypt External Media = Selected, EMS Exclude CD/DVD Encry Selected, and Storage Class: Optical Drive Control = UDF Only.
Subclass Storage: Floppy Drive Control	Read Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use th Full Access: Floppy Drive port does not have read/write data restrictio Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Class: Windows Portable Device (WPD)	Disabled	PARENT to the next policy. Set this policy to Enabled to use the Subcla Portable Device (WPD): Storage policy. Setting this policy to Disabled c Subclass Windows Portable Device (WPD): Storage policy - no matter w value. Control access to all Windows Portable Devices.
Subclass Windows Portable Device (WPD): Storage	Full Access	CHILD of Class: Windows Portable Device (WPD) . Class: Windows Porta (WPD) must be set to Enabled to use this policy. Full Access: Port does not have read/write data restrictions applied. Read Only: Allows read capability. Write data is disabled. Blocked: Port is blocked from read/write capability.
Class: Human Interface Device (HID)	Enabled	Control access to all Human Interface Devices (keyboards, mice). **Note:** USB port-level blocking and HID class-level blocking is **only** hono can identify the computer chassis as a laptop/notebook form-factor. W the computer's BIOS for the identification of the chassis.
Class: Other	Enabled	Control access to all devices not covered by other Classes.
EMS Encrypt External Media	Not Selected	This policy is the "master policy" for all Removable Storage policies. A N value means that no encryption of removable storage takes place, rega other policy values. A Selected value means that all Removable Storage encryption policies enabled.
EMS Exclude CD/DVD	Not Selected	Not Selected encrypts CD/DVD devices.

Encryption		
EMS Access to unShielded Media	Read Only	*Block, Read Only, Full Access* Note that this policy interacts with the Port Control System - Storage C External Drive Control policy. If you intend to set this policy to Full Acc that Storage Class: External Drive Control is not set to Read Only or Blo More... When this policy is set to Block Access, you have no access to removab unless it is encrypted. Choosing either Read-Only or Full Access allows you to decide what ren storage to encrypt. If you choose not to encrypt removable storage and this policy is set to you have full read/write access to removable storage. If you choose not to encrypt removable storage and this policy is set to you can read or delete existing files on the unencrypted removable sto the Shield will not allow any files to be edited on, or added to, the ren storage.
EMS Encryption Algorithm	AES256	*AES 256, AES 128, 3DES* Encryption algorithm used to encrypt removable storage. Encryption algorithms in order of speed, fastest first, are AES 128, AES
EMS Automatic Authentication	Local	*Disabled, Enable Local, Enable Roaming* Local automatic authentication allows the Shielded media to be autom authenticated when inserted in the originally Shielding computer when of that media is logged in. When automatic authentication is disabled, always manually authenticate to access Shielded media. Disabling Roaming Authentication helps to prevent users from forgettin password when they take the media home or share it with a colleague. Roaming Authentication also promotes a sense of awareness from a sec perspective for users that the data being written to that media is prote
EMS Scan External Media	Not Selected	Selected allows EMS to scan removable storage every time removable s inserted. When this policy is Not Selected and the EMS Encrypt External Media po Selected, EMS only encrypts new and changed files. See EMS Encryption Rules if changing this policy to Selected. Do not en policy without applying EMS Encryption Rules also. More... A scan occurs at every insertion so that EMS can catch any files added t removable storage without authenticating. You can add files to the ren storage if you decline to authenticate, but you cannot access encrypte files added will not be encrypted in this case, so the next time you aut the removable media to work with encrypted data, EMS scans it and en files that may have been added without encryption.
EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable storag the endpoint is Shielded or not. More... When this policy is False, the user will be able to work with encrypted logged on to any Shielded endpoint, regardless of the Enterprise Server activated against. The user will not be able to work with encrypted da unShielded device.
EMS Device Whitelist		*String - Maximum of 150 devices with a maximum of 500 characters p PNPDeviceID. Maximum of 2048 total characters allowed. "Space" and " characters used count in the total characters used.* This policy allows the specification of removable storage devices to exc EMS encryption [using the removable storage device's Plug and Play dev identifier (PNPDeviceID)], thereby allowing users full access to the spe removable storage devices. More... This policy is available on an Enterprise, Domain, Group, and User leve local settings override inherited settings. If a user is in more than one g EMS Device Whitelist entries, across all Groups, apply.

Note: This policy is particularly useful when using removable storage d
provide hardware encryption. However, this policy should be used with
This policy does not check whether external media devices on this list
hardware encryption. Whitelisting removable storage devices which do
hardware encryption will not have enforced security and will not be pr

*For example, the Kingston® DataTraveler® Vault Privacy model enforc
encryption is enabled to use the device. However, the Kingston DataTr
model has an unsecured partition and a secured partition. Because it i
physical removable storage device with only one PNPDeviceID, the two
cannot be distinguished, meaning that whitelisting this particular rem
storage device would allow unencrypted data to leave the endpoint.*

*Additionally, if an removable storage device is protected by EMS and s
added to the EMS Device Whitelist policy, it remains encrypted and re
reformat of the removable storage device to remove encryption.*

The following is an example of a PNPDeviceID, which contains the man
identifier, product identifier, revision, and hardware serial number:

```
USBSTOR\DISK&VEN_KINGSTON
&PROD_DTVAULT_PRIVACY&
REV_104\07005B831A0004B4&0
```

To whitelist a removable storage device, provide a string value which r
portions of the device's PNPDeviceID. Multiple device PNPDeviceIDs are

For example, to whitelist all Kingston DataTraveler Vault Privacy mode
string:

```
PROD_DTVAULT_PRIVACY
```

To whitelist both models of Kingston DataTraveler, the Vault and Vault
models, input the string:

```
PROD_DTVAULT_PRIVACY;
PROD_DT_VAULT
```

Note that space characters are considered part of the substring to mat
PNPDeviceID. Using the previous PNPDeviceID as an example, a space b
after the semicolon would cause neither of the substrings to be matche
the space character is not part of the PNPDeviceID.

Instructions...

To find the PNPDeviceID for removable storage:

1. Insert the removable storage device into a Shielded compute
2. Open the EMSService.log in C:\Programdata\Dell\Dell
   Protection\Encryption\EMS.
3. Find PNPDeviceID=

   For example:
   14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDevice
   USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_04
   KJ&0
   VEN=Vendor; Green highlighted text is for the vendor
   excluded

   PROD=Product/Model Name; Adding text highlighted
   excludes all of Seagate's USB drives

   REV=Firmware Revision; Adding text highlighted gray
   excludes the specific model being used
   Serial number (in this example); Adding text highlight
   excludes just this device

OR

To find the PNPDeviceID for removable storage on Windows 7 or later:

1. Insert the removable storage device.
2. Open the Control Panel and go to Administrative Tools > Con
   Management.
3. Select the Hardware tab, select the drive, and click Pr

		4. A new windows displays. Select the Device Instance P Property drop-down menu. The PNPDeviceID is displayed in the Value field. *To find the PNPDeviceID for removable storage on Windows XP:* 1. Click Start > Run... 2. Type msinfo32 and click Enter. 3. When the System Information window displays, go to Compo A list of USB devices and their PNPDeviceIDs displays. **Available Delimeters:** Tabs Commas Semi colons Hex character 0x1E (Record separator character)
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.
EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in th
EMS Number of Characters. Required in Password	8	*1-40 characters* Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	Selected	Selected requires one or more numeric characters in the password.
EMS Password Attempts Allowed	3	*1-10* Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.
EMS Access and Device Code Length	16	*8, 16, 32* Number of characters access and device codes have. 32 characters is th secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	*1-10* Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	*Apply Cooldown, Wipe Encryption Keys* Action to take following unsuccessful Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the spe cooldown period (Cooldown Time Delay and Cooldown Time Increment • Wipe Encryption Keys to have the Shield delete the encryption keys o removable storage, making the encrypted data inaccessible until the ow the media to a Shielded computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	*String - 5-512 characters - Authentication Failed: Please contact your s administrator.* Message that displays when a user needs to contact you for an access c authentication failure). More... Message policies must have non-blank values.

		"Space" and "Enter" characters used to add lines between rows count as used. Messages over the 512 character limit are truncated on the clien We recommend that you customize the second sentence of the messag specific instructions about how to contact a Help Desk or Security Adm authentication failures.
EMS Cooldown Time Delay	30	*0-5000 seconds* Number of seconds the user must wait between the first and second ro access code entry attempts.
EMS Cooldown Time Increment	20	*0-5000 seconds* Incremental time to add to the previous cooldown time after each unsu round of access code entry attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	*String - 5-512 characters - You are not authorized to use this media. P contact your system administrator.* Message that displays following unsuccessful Access Code Attempts Allo More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as used. Messages over the 512 character limit are truncated on the clien We recommend that you customize the message to include specific ins about how to contact the Help Desk or Security Administrator.
EMS Encryption Rules	String	Encryption rules to be used to encrypt/not encrypt certain drives, dire folders. A total of 2048 characters are allowed. "Space" and "Enter" characters lines between rows count as characters used. Any rules exceeding the are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as USB, eSATA, etc. may require the use of both EMS and encryption rules the endpoint. This is necessary due to differences in how the Windows system handles storage devices based on interface type. To ensure encrypting an iPod via EMS does not make the device unusab following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories ab the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx encrypted in the directories excluded from encryption via the previous ^R#:\Calendars ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx .xlsx ^R#: \iPod_Control ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx

		Replacing these five rules with the following rule will force encryption pptx, doc, docx, xls, and xlsx files in any directory on the iPod, includi Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file type removable devices - not just an iPod. Use care when defining rules to e iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation iPod Mini 4gb second generation We do not recommend the use of the iPod Shuffle, as unexpected resul occur. As iPods change, this information could also change, so caution is advis allowing the use of iPods on EMS-enabled computers. Because folder names on iPods are dependent on the model of the iPod recommend creating an exclusion encryption policy which covers all fo across all iPod models.
EMS Block Access to UnShieldable Media	Selected	Block access to any removable storage that is less than 55 MB and thus insufficient storage capacity to host a Removable Media Shield (such as floppy disk). More... All access is blocked if Encrypt External Media and this policy are both Encrypt External Media is True, but this policy is False, data can be rea unShieldable removable storage, but write access to the media is block If Encrypt External Media is False, then this policy has no effect and ac unShieldable removable storage is not impacted.
SDE Encryption Enabled	Not Selected	This policy is the "master policy" for all other System Data Encryption (policies. If this policy is Not Selected, no SDE encryption takes place, r other policy values. A Selected value means that all data not encrypted by other Intelligen policies will be encrypted per the SDE Encryption Rules policy. More... Changing the value of this policy requires a reboot. If an endpoint computer comes equipped with an HCA and you choose t HCA policies, all SDE policies are ignored. Likewise, if you enable SDE p later decide to enable HCA policies, SDE issues a decryption policy befo policies are implemented. HCA and SDE cannot coexist on the same co
SDE Encryption Algorithm	AES256	*AES 256, AES 128, 3DES* Encryption algorithm used to for System Data Encryption. Encryption algorithms in order of speed, fastest first, are AES 128, AES
SDE Encryption Rules	String F#:\ -^%ENV:SYSTEMDRIVE%\System Volume Information -^%ENV:SYSTEMROOT%\;dll.exe.sys.ocx.man.cat.manifest.policy -^%ENV:SYSTEMROOT%\System32 -^%ENV:SYSTEMROOT%\SysWow64 -^%ENV:SYSTEMROOT%\WinSxS -^%ENV:SYSTEMROOT%\Fonts ^3@%ENV:SYSTEMROOT%\SYSTEM32\;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\cmd.exe;exe	Encryption rules to be used to encrypt/not encrypt certain drives, dire folders. See Encryption Rules for information. SDE Encryption Rules may be changed as appropriate for your environm However, these defaults have been tested extensively. Removing these may result in Windows issues, particularly after applying patch updates Contact Customer Support for guidance if you are unsure about changi values.

	-^3@%ENV:SYSTEMROOT%\SYSTEM32\autochk.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\winresume.exe;exe -^F#:\bootmgr -^F#:\boot	
Encryption Enabled	Selected	This policy is the "master policy" for all Common Encryption policies. A check box means that no Common Encryption takes place, regardless o policy values. A checked box means that all Common Encryption policies are enabled Changing the value of this policy triggers a new sweep to encrypt/decr
Common Encrypted Folders	String %ENV:SYSTEMDRIVE%\;accdb.doc.docm.docx.mdb.pdf.ppam.pps.ppsm.ppsx .ppt.pptm.pptx.pub.puz.sldm.sldx.tif.tiff.vdx.vsd.vss.vst.vsx.vtx.xlam .xlm.xls.xlsb.xlsm.xlsx.xsf.zip.rar %ENV:USERPROFILE%\Desktop %ENV:USERPROFILE%\Download -^%ENV:SYSTEMDRIVE%\;dat.ini.xml.txt.log.db.lnk	*String - maximum of 100 entries of 500 characters each (up to a maxin characters)* A list of folders on endpoint drives to be encrypted or excluded from e which can then be accessed by all managed users who have access to t See Encryption Rules for information. More... The available drive letters are: #: Refers to all drives f#: Refers to all fixed (non-removable) drives r#: Refers to all removable drives **Important:** *Overriding directory protection can result in an unbootable and/or require reformatting drives.*
Common Encryption Algorithm	AES256	*AES 256, AES 128, 3DES* Encryption algorithm used to encrypt data at the endpoint (all users) le System paging files are encrypted using AES 128. Encryption algorithms in order of speed, fastest first, are AES 128, AES
Application Data Encryption List	Exe List winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe winzip.exe winrar.exe onenote.exe onenotem.exe	*String - maximum of 100 entries of 500 characters each* We do not recommend adding explorer.exe or iexplorer.exe to the ADE unexpected or unintended results may occur. However, explorer.exe is the process used to create a new notepad file desktop using the right-click menu. Setting encryption by file extension the ADE list, provides more comprehensive coverage. Changes to this policy do not affect files already encrypted because of List process names of applications (without paths) whose new files you encrypted, separated by carriage returns. Do not use wildcards. More... The Shield encrypts all new files (not already being encrypted by Comm Encrypted Folders and User Encrypted Folders) on the current computer hard drives created by these application proc whenever they are owned by a currently- logged-on managed user. This may include files excluded from encrypt Common Encrypted Folders and/or User Encrypted Folders. The following folders and their subfolders are always excluded from en this policy: C:\Windows\system32 C:\Windows\Software Distribution C:\Windows\Security C:\System Volume Information\Program Files\Credant\(.dll.exe.sys.mac.ddp.wip.rty.nmd.inv) We strongly recommend not listing applications or installers that write critical files. Doing so could result in encryption of important system files, which could make a Windows e unbootable.

		Common process names: Outlook: outlook.exe Word: winword.exe FrontPage: frontpg.exe PowerPoint: powerpnt.exe Access: msaccess.exe WordPad: wordpad.exe Microsoft Paint: mspaint.exe Excel: excel.exe The following hard-coded system and installer process names are ignor specified in this policy (you can also add to this list via the registry value HKLM\Software\Dell\ CMGShield\EUWPrivilegedList): hotfix.exe, a Windows update process update.exe, a Windows update process setup.exe, a third-party installer process msiexec.exe, a third-party installer process wuauclt.exe, a Windows update process wmiprvse.exe, a Windows system process migrate.exe, a Windows update process unregmp2.exe, a Windows update process ikernel.exe, a third-party installer process wssetup.exe, the Windows Shield installer svchost.exe, a Windows system process
Encrypt Temporary Files	Not Selected	Selected encrypts the paths listed in the environment variables TEMP a TEMP and TMP for the OS are encrypted with the Common Encryption K To reduce encryption sweep time, the Shield clears the contents of the TMP folders for initial encryption, as well as updates to this policy. Hov your organization uses a third-party application that requires the file s within the \temp directory to be preserved, you should prevent this de To disable temporary file deletion, create DeleteTempFiles (REG_DWO its value to 0 in the registry at HKLM\SOFTWARE\Dell\CMGShield.
Encrypt User Profile Documents	Selected	Selected encrypts all shared files and public folders with the Common Key
Encrypt Windows Paging File	Selected	Selected encrypts the Windows paging file. A change to this policy requ reboot.
Managed Services	null	*String - maximum of 100 entries of 500 characters each (up to a maxim characters)* When a Service is managed by this policy, the Service is started only af is logged in and the Shield is unlocked. This policy also ensures that the managed by this policy is stopped before the Shield is locked during log policy can also prevent a user logoff if a Service is unresponsive. More... Syntax is one Service name per line. Spaces in the Service name are su Wildcards are not supported. Entries are not case-sensitive. For example, GoogleDesktop Manager is googledesktopmanager. The Service log on as setting has no bearing on whether or not the Shie control it. It does not matter if a user logs on with user credentials ver system. The startup type (Automatic or Manual) does not affect the ability of th control it. Automatic or Manual startup is acceptable. Managed Services will not be started if an unmanaged user logs on.

Secure Post-Encryption Cleanup	Single Pass Overwrite	*No Overwrite, Single-pass Overwrite, Three-pass Overwrite, Seven-pas* Once folders specified via other policies in this category have been enc policy determines what happens to the unencrypted residue of the orig • No Overwrite deletes it. This value yields the fastest encryption proc • Single-pass Overwrite overwrites it with random data. • Three-pass Overwrite overwrites it with a standard pattern of 1s and with its complement, and then with random data. • Seven-pass Overwrite overwrites it with a standard pattern of 1s and with its complement, and then with random data five times. This value most difficult to recover the original files from memory, and yields the secure encryption processing.
Secure Windows Credentials	Selected	The Windows Credentials will be secured by encrypting the entire regis exception of registry information required for computer boot. The info required for computer boot includes HKLM/SYSTEM and all sub-keys. This policy value will be automatically set to Selected if SDE is enabled When a change to this policy is delivered, the Shield requires a reboot. this reboot, configure the following policies: Force Reboot on Update, Each Reboot Delay, and Number of Reboot Delays Allowed.
Block Unmanaged Access to Domain Credentials	Selected	This policy prevents unmanaged applications from accessing the Windo credentials when a user is logged in.
Secure Windows Hibernation File	Not Selected	When enabled, the hibernation file will be encrypted only when the co enters hibernation. The Shield will disengage protection when the com out of hibernation, providing protection without impacting users or app while the computer is in use.
Prevent Unsecured Hibernation	Not Selected	When enabled, the Shield will not allow computer hibernation if the Sh unable to encrypt the hibernation data.
Workstation Scan Priority	Lowest	*Highest, High, Normal, Low, Lowest* Specifies the relative Windows priority of encrypted folder scanning. H Highest prioritize scanning speed over computer responsiveness, Low a prioritize computer responsiveness over scanning speed and favor othe intensive activities, and Normal balances the two. The Shield checks for a changed Workstation Scan Priority before proce next file. The scan priority levels are used in two different ways. 1. These values correspond with the values used by the Microso set thread execution priority. 2. The Shield uses these values to introduce a delay in the encr sweep after every single file is processed. The values translate to the following millisecond delay ranges encryption thread will sit idle and then return full control to t operating system: Highest=0 ms / Lowest=100 ms
Policy Proxy Connections	String	String - maximum of 1500 characters List fully qualified Policy Proxy hostnames, or IP addresses, separated returns. More... Once the Shield finds a valid entry, the remainder of the entries are ig Entries are processed in the following order: 1. GKConnections Override (this registry entry overrides all other entri 2. GKConnections (this registry entry is set automatically by the Shield the this policy) 3. GK This policy works in conjunction with the Policy Proxy Polling Interval p To override this policy and specify ports via the registry item HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CMGShield\GKConnectionsOverride.

		You cannot specify ports in this policy. The Shield communicates with Policy Proxies using the GKPORT specifi Shield installation (the default is 8000). If necessary, change that port via the registry item HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ CMGShield\GKPort. Inherited values for this policy accumulate. In order for the Shield to connect to a Policy Proxy specified in this pol be in the same group as the Policy Proxy specified during Shield install Because the Shield supports up to 255 users per endpoint, this policy is only at the Enterprise Policies level.
Policy Proxy Polling Interval	720	1-1440 minutes The interval that the Shield attempts to poll Policy Proxy for policy up send inventory information to Policy Proxy. The Shield also attempts to poll Policy Proxy each time a user logs on.
See basic settings		

Variables

Some Windows policies support the following variables. A pathname can consist entirely of one or more of these variables, or can include one or more of these variables at any point.

To get directory locations that these CSIDL values resolve to, go to http://msdn.microsoft.com/en-us/library/bb762494.aspx. All names listed on the MSDN page are CSIDL_<name>.

Note: Some operating systems have different CSIDL values, such as Windows 7 having values that Windows XP does not.

%CSIDL:name%

- Includes any of the following Windows CSIDL constants:

  DESKTOP

  INTERNET

  PROGRAMS

  CONTROLS

  PRINTERS

  PERSONAL

  FAVORITES

  STARTUP

  RECENT

  SENDTO

  STARTMENU

  STARTMENU

  MYDOCUMENTS

  MYMUSIC

  MYVIDEO

  DESKTOPDIRECTORY

DRIVES

NETWORK

NETHOOD

FONTS

TEMPLATES

COMMON_STARTMENU

COMMON_PROGRAMS

COMMON_STARTUP

COMMON_DESKTOPDIRECTORY

APPDATA

PRINTHOOD

LOCAL_APPDATA

ALTSTARTUP

COMMON_ALTSTARTUP

COMMON_FAVORITES

INTERNET_CACHE

COOKIES

HISTORY

COMMON_APPDATA

WINDOWS

SYSTEM

PROGRAM_FILES

PROGRAMFILES

MYPICTURES

PROFILE

SYSTEMX86

PROGRAM_FILESX86

PROGRAMFILESX86

PROGRAM_FILES_COMMON

PROGRAM_FILES_COMMONX86

COMMON_TEMPLATES

COMMON_DOCUMENTS

COMMON_ADMINTOOLS

ADMINTOOLS

CONNECTIONS

COMMON_MUSIC

COMMON_PICTURES

COMMON_VIDEO

RESOURCES

PROFILES

%HKCU:regpath%

- Includes a numeric or text value stored in the registry for the Current User. If you specify a path but not an item, the Shield uses the default value

%HKLM:regpath%

- Includes a numeric or text value stored in the registry for the local computer. If you specify a path but not an item, the Shield uses the default value

%ENV:envname%

- Includes the value of a Windows local environment variable

%%

- Includes the % character

Windows Policies that Require Reboot

- SDE Encryption Enabled
- Encrypt Windows Paging File
- Secure Windows Credentials
- All PCS policies

Windows Policies that Require Logoff

- SDE Encryption Enabled
- User state change to Suspended
- EMS Encrypt External Media
- EMS Scan External Media
- EMS Encryption Algorithm
- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Authentication

Authentication policies allow you to configure user experience and Windows authentication.

Policy descriptions also display in tooltips in the Remote Management Console.

Policy	Default Setting	Description

Windows Authentication		
Logon Authentication Policy for Administrators	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card One-Time Password
Logon Authentication Policy for Users	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card One-Time Password
See advanced settings		
Microsoft Passport		
Microsoft Passport	Off	*On* *Off* Toggle to On to enable Microsoft Passport. If this policy is toggled to Off, no Microsoft Passport policies are enabled. Microsoft Passport is supported only on computers running Windows 10.
Maximum NGC Authentication Attempts	3	*1-10 attempts* Number of chances the user has to authenticate with correct credentials.
Logon Authentication Method	PIN	Currently, logon authentication method is supported only with PIN.
PIN Length	8	*4-127 numeric characters* Minimum number of characters required in the PIN.

Advanced Authentication

Authentication policies allow you to configure user experience and Windows authentication.

Policy descriptions also display in tooltips in the Remote Management Console.

Policy	Default Setting	Description
Windows Authentication		
In-session Authentication Policy for Administrators	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card One-Time Password
In-session Authentication Policy for Users	Windows Password and None	The possible VALUES are:

		Windows Password None Fingerprints Contactless Card One-Time Password
Recovery Questions for Windows Authentication	At least 3 selectable questions	Specify the questions that will be presented to Windows users during recovery questions setup. Separate each question by a carriage return. These questions will be used if the Windows password is forgotten. At least 3 questions must be specified. What is your mother's maiden name? What was the name of the first school you attended? What is the name of your first pet? What is your father's middle name? What is your mother's middle name? Who was your first employer? Who was your first teacher? What city were you born in? What city was your mother born in? What city was your father born in? What was the first concert you attended? Who is your favorite TV show character? What was the name of your first stuffed animal? What was the make of the first car you owned? Where did you spend your honeymoon? Where did you meet your spouse? What is your oldest cousin's name? What is your oldest niece's name? What is your oldest nephew's name? What is your youngest child's nickname? What is your oldest child's nickname? What was the last name of your third grade teacher? In what city or town did your mother and father meet? In what city or town was your first job?
Allow Recovery Questions	Not Selected	*Selected* *Not Selected* Set to Selected to allow users to use recovery questions/answers to log on to Windows.

Log Events Level	Audit	*Errors* *Audit* *Details* Level of detail in Windows Event Logs. Determines whether events such as fingerprint registration and authentication attempts are logged in the Windows Event Log. Each higher level includes all previous levels. Events are logged on the computer where they occur. Normally, the Auditing level provides sufficient detail, covering all logon, authentication, fingerprint management, and user management events. The Details levels can fill the log file very quickly. Status events provide information about the state of several important systems on the computer. They are logged on configurable intervals and generally used when events are remotely collected.
False Accept Rate of Fingerprint	Medium High - 1 in 100,000	The False Accept Rate is the probability of receiving a false acceptance decision when comparing fingerprints scanned from different fingers. You can select one of the following FAR values: * Medium (1 in 10,000) * Medium High (1 in 100,000) * High (1 in 1,000,000) For example: if you select Medium High, on average, one false acceptance will occur when a fingerprint is compared against one hundred thousand fingerprints scanned from different fingers. The higher the setting, the lower the chance of receiving a false acceptance. However, at the High setting, the system may reject legitimate fingerprints. **NOTE**: The FAR is set on a per verification basis. When matching a fingerprint against fingerprints of multiple users (identification), the internally used FAR is automatically adjusted to maintain the same effective FAR as was selected for a single match.
Minimum Number of Fingerprints to Enroll	2	The minimum number of fingerprints required to be enrolled.
Maximum Number of Fingerprints to Enroll	10	The maximum number of fingerprints required to be enrolled.
Allow Users to Enroll Credentials	Selected	Set to Selected to allow users to enroll their own credentials without administrator involvement.
Allow Users to Modify Credentials	Selected	Set to Selected to allow users to modify their own credentials that have been previously set up or enrolled.
Reminder to Enroll Credentials (Admin)	In one day	Values for reminders: Disable Reminder At Next Logon In One Day In One Week Every Two Hours

Reminder to Enroll Credentials Expiration Date (Admin)	Now	The date (time is always 12 am) when authentication policy is going into full effect. Meaning, the client stops asking the local admin to enroll credentials and forces them to enroll before they can logon. The default is “now”.
Reminder to Enroll Credentials (User)	In one day	Values for reminders: Disable Reminder At Next Logon In One Day In One Week Every Two Hours
Reminder to Enroll Credentials Expiration Date (User)	Now	The date (time is always 12 am) when authentication policy is going into full effect. Meaning, the client stops asking the user to enroll credentials and forces them to enroll before they can logon. The default is “now”.
Action Upon Smart Card Removal	Lock Workstation	*No Action* *Lock Workstation* *Force Logoff* *Disconnect if on a Remote Desktop session* The action that occurs when a smart card is removed from the computer.
Allow One-Time Password for Recovery	Not Selected	*Selected* *Not Selected* This policy is the "master policy" for all other One-time Password policies. If this policy is Not Selected, the One-time Passwords feature is disabled on the endpoint. The user will not be able to use OTP to unlock the account, regardless of other OTP policy values. If Selected, the One-time Password Recovery feature is enabled and allows the user to use a paired mobile device to generate passwords for one-time use to unlock their account, if the account password is lost.
One-Time Password Length	6	*6, 8, or 10 characters* Specifies the minimum One-time Password length.
Maximum One-Time Password Authentication Attempts	3	*3-10* Number of times a One-time Password can be entered into a device.
Require Password for Mobile Apps	Selected	Set to Selected to require the One-time Password generation application to be password protected on the mobile device.
See basic settings		

Threat Prevention

Threat Prevention policies are available at the Enterprise, Endpoint Group, and Endpoint levels.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

See Advanced Threat Prevention Features by Operating System for information about support for Advanced Threat Prevention features on Windows and Mac operating systems

Policy	Default Setting	Description
Advanced Threat Prevention		
Advanced Threat Prevention	Off	*On* *Off* Toggle ON to enable Advanced Threat Prevention. If this policy is toggled to OFF, Advanced Threat Prevention is disabled, regardless of other policies.
File Actions		
File Action: Unsafe Executable Auto Quarantine with Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Unsafe executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices under a test policy in order to observe the behavior and ensure that no business-critical applications are blocked at execution.
File Action: Abnormal Executable Auto Quarantine with Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Abnormal executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices under a test policy in order to observe the behavior and ensure that no business-critical applications are blocked at execution.
Memory Actions		
Memory Action: Memory Protection Enabled	Not Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Memory policies. If this policy is Not Selected, no Memory Action policies are enforced, regardless of other policy values. NOTE: Before enabling Memory Protection, enable Compatibility Mode, to ensure applications function properly on the client computer. For instructions on how to enable Compatibility Mode, see Enable_Compatibility_Mode_for_Memory_Protection.htm. Compatibility Mode does not apply to Mac clients.
See **advanced settings**		

Policy	Default Setting	Description
Threat Protection		
Threat Protection	Off	*On* *Off* Toggle to ON to enable Threat Protection. If toggled to OFF, no Threat Protection policies will be applied. Threat Protection includes Malware Protection, Web Protection, and Client Firewall.
Action on Malicious Activity for Files and Folders	Block and Report	*Block Only* *Report Only* *Block and Report* Prevents users from modifying or deleting Threat Protection system files and folders and sets the action to

		take upon attempt. Block Only: Blocks activity but does not report to the Server. Report Only: Reports activity to the Server but does not block activity. Block and Report (default): Blocks and reports activity to the Server.
Action on Malicious Activity for Registry	Block and Report	*Block Only* *Report Only* *Block and Repor*t Prevents users from modifying or deleting Threat Protection registry keys and values and sets the action to take upon attempt. Block Only: Blocks activity but does not report to the Server. Report Only: Reports activity to the Server but does not block activity. Block and Report (default): Blocks and reports activity to the Server.
See advanced settings		
Policy	**Default Setting**	**Description**
Malware Protection		
Malware Protection	Off	*On* *Off* Toggle to ON to enable Malware Protection. If toggled to OFF, no Malware Protection policies will be applied. Malware Protection protects the critical operating system resources from changes made by malware or other unauthorized processes.
Exploit Protection	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Exploit Protection policies. If this policy is Not Selected, no Exploit Protection policies are enforced, regardless of other policy values. A Selected value means that Exploit Protection is enabled. Exploit Protection monitors for application vulnerabilities and keeps buffer overflow exploits from executing arbitrary code on the computer. This policy must be set to Selected to enable Exploit Protection. If this policy is Not Selected, no Exploit Prevention policies will be applied.
On-Access Protection	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other On-Access Protection policies. If this policy is Not Selected, no On-Access Protection policies are enforced, regardless of other policy values. A Selected value means that On-Access Protection is enabled. This policy must be set to Selected to enable On-Access Protection. If this policy is Not Selected, no On-Access Protection policies will be applied.
See advanced settings		

Policy	Default Setting	Description
Web Protection		
Web Protection	Off	*On* *Off* Toggle to ON to enable Web Protection. If toggled to OFF, no Web Protection policies will be applied.
Enforcement - Action to Apply to Sites Not Verified	Allow	*Block* *Allow* *Warn* Specifies the default action to apply to sites that have not been verified. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before continuing.
Enforcement - Enable File Scanning for File Downloads	Selected	*Selected* *Not Selected* A Selected value scans all files (including .zip files) before downloading. This option prevents users from accessing a downloaded file until Threat Protection marks the file as clean. Downloaded files are sent to Threat Protection for scanning. Threat Protection performs a Reputation Service lookup on the file. If a downloaded file is detected as a threat, Threat Protection takes action on the file and alerts the user.
Enable Secure Search	Not Selected	*Selected* *Not Selected* A Selected value enables Secure Search, automatically blocking malicious sites in search results based on safety rating.
Block Links to Risky Sites in Search Results	Not Selected	*Selected* *Not Selected* A Selected value prevents users from clicking links to risky sites in search results.
See advanced settings		
Policy	**Default Setting**	**Description**
Client Firewall		
Client Firewall	Off	*On* *Off* Toggle to ON to enable Client Firewall. If toggled to OFF, no Client Firewall Settings or Rules will be applied. Client firewall is a stateful firewall.
See advanced settings		

Advanced Threat Prevention

Threat Prevention policies are available at the Enterprise, Endpoint Group, and Endpoint levels.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

See Advanced Threat Prevention Features by Operating System for information about support for Advanced Threat Prevention features on Windows and Mac operating systems

Policy	Default Setting	Description
Advanced Threat Prevention		
Advanced Threat Prevention	Off	*On* *Off* Toggle ON to enable Advanced Threat Prevention. If this policy is toggled to OFF, Advanced Threat Prevention is disabled, regardless of other policies.
File Actions		
File Action: Unsafe Executable Auto Quarantine With Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Unsafe executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices under a test policy in order to observe the behavior and ensure that no business-critical applications are blocked at execution.
File Action: Unsafe Executable Auto Upload Enabled	Selected	*Selected* *Not Selected* If selected, any detected Unsafe file is automatically uploaded for a deeper analysis and additional details about the file.
File Action: Abnormal Executable Auto Quarantine With Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Abnormal executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices under a test policy in order to observe the behavior and ensure that no business-critical applications are blocked at execution.
File Action: Abnormal Executable Auto Upload Enabled	Selected	*Selected* *Not Selected* If selected, any detected Abnormal file is automatically uploaded for a deeper analysis and additional details about the file.
Allow Execution of Files in Exclude Folders	Not Selected	*Selected* *Not Selected* If selected, executable files are allowed to run, even though they are not in folders excluded in the Exclude Specific Folders policy.
Memory Actions		
Memory Action: Memory Protection Enabled	Not Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Memory Protection policies. If this policy is Not Selected, no Memory Action policies are enforced, regardless of other policy values. NOTE: Before enabling Memory Protection, enable Compatibility Mode, to ensure applications function properly on the client computer. For instructions on how to enable

		Compatibility Mode, see Enable Compatibility Mode for Memory Protection. Compatibility Mode does not apply to Mac clients.
Memory Action: Enable Exclude executable files	Selected	*Selected* *Not Selected* Allows specific process files to be excluded from Memory Protection. This policy must be selected, to use the policy Memory Action: Exclude executable files.
Memory Action: Exclude executable files	String \Windows\System32\CmgShieldService.exe \Windows\System32\EMSService.exe	String - Example: \folder\file.exe Excludes specific process files from Memory Protection. This allows the specified files to run or be installed on any device on which this policy is enforced. Enter the relative paths of the files to exclude.
Memory Action: Exploitation: Stack Pivot	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a stack pivot threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Exploitation: Stack Protect	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a stack protect threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Exploitation: Overwrite Code	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when an overwrite code threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts

		to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Exploitation: Scanner Memory Search	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a scanner memory search threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Exploitation: Malicious Payload	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a malicious payload is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote Allocation of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote memory allocation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote Mapping of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote attempt to map memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP

		Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote Write to Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote attempt to write to memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote Write PE to Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote attempt to write a portable executable to memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Process Injection: Remote Overwrite Code	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote overwrite code threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.

Memory Action: Process Injection: Remote Unmap of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote memory unmapping threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Process Injection: Remote Thread Creation	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote thread creation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote APC Scheduled	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote APC scheduled threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Process Injection: Remote DYLD Injection (Mac OS X only)	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote DYLD injection threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server.

		Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Windows clients.
Memory Action: Escalation: LSASS Read	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when an LSASS read threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Escalation: Zero Allocate	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a zero byte allocation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Protection Settings		
Execution Control: Prevent Service Shutdown from Device	Not Selected	*Selected* *Not Selected* If selected, the Advanced Threat Prevention service is protected from being shut down either manually or by another process.
Kill Unsafe Running Processes and Sub-Processes	Not Selected	*Selected* *Not Selected* If selected, processes and sub-processes are quarantined and terminated regardless of their state when a threat is detected (exe or dll). Although a process or sub-process is terminated, the command prompt window remains open. If a file has been determined to be Safe and allowed to run and then a threat model update occurs that results in the file being identified as unsafe, the process is automatically terminated. Dell recommends that you review threat model updates before Selecting this policy. For more information, see Threat Model Updates.
Execution Control: Background Threat	Run Once	*Disabled* *Run Recurring* *Run Once*

Detection		If set to Run Recurring or Run Once, a full-disk scan is run to detect and analyze any dormant threats on the disk. An upgrade to the Advanced Threat Prevention model triggers a full-disk scan.
Execution Control: Watch for New Files	Selected	*Selected* *Not Selected* If selected, any new or modified files are detected and analyzed for dormant threats. Dell recommends enabling this policy. However, If Auto Quarantine is enabled for all Unsafe or Abnormal files, all malicious files will be blocked at execution. Therefore, it is not necessary to enable this policy with Auto Quarantine mode unless you prefer to quarantine a file as it is added to a disk but before execution.
Execution Control: Set Maximum Archive File Size to Scan	150 MB	The default setting is 150 MB. Specifies the maximum size of archive (compressed) files, including .jar files to be scanned. Because scanning compressed files can negatively affect computer performance, Dell recommends setting Quick-Scan - Scan Archives and Full-Scan - Scan Archives policies to be used during off-work hours.
Enable Exclude Specific Folders (includes subfolders)	Selected	*Selected* *Not Selected* Allows specific folders to be excluded from Auto Quarantine and Auto Upload. This policy must be selected in order to use the policy, Exclude Specific Folders.
Execution Control: Exclude Specific Folders (includes subfolders)	String	*String* Folders specified in this policy are excluded from actions performed based on the policies, Background Threat Detection and Watch for New Files, when these features are enabled. This exclusion extends to subfolders of folders that are specified with this policy.
Application Control	Not Selected	*Selected* *Not Selected* If selected, specified devices are locked down, restricting any changes on a device after it is locked down. Only the applications that exist on a device before the lock-down occurs are allowed to execute on that device. Any new applications, as well as changes to the executables of existing applications, will be denied. The Advanced Threat Prevention agent updater is also disabled. When the Application Control policy is Selected, certain File Action, Memory Action, and Execution Control policies are automatically set. These policy settings may be changed after they are automatically set, without disabling Application Control. For a list of policies that are automatically set when the Application Control policy is Selected, see Policies Set by Application Control. To exclude specific folders from lock-down, specify the folders in the Application Control Allowed Folders policy. This policy does not apply to Mac clients.
Application Control Allowed Folders	Not Selected	*Selected* *Not Selected* Allows specific folders to be excluded from Application Control lock-down.
Enable Change Window	Not Selected	*Selected* *Not Selected* If selected, Application Control is temporarily disabled to allow, edit, and run new applications or perform updates. This includes updating the Advanced Threat Prevention agent. After performing the necessary changes, deselect Change Window. **Note:** Using Change Window retains any changes made to the

		Application Control settings. Deselecting Application Control and then back Selecting it resets the Application Control settings back to default. This policy does not apply to Mac clients.
Suppress Popup Notifications	Not Selected	*Selected* *Not Selected* If Selected, no popup notifications of Advanced Threat Prevention events display on the client computer.
Minimum Popup Notification Level	High	*High* *Medium* *Low* Severity level of events that result in popup notifications that display on the client computer. A setting of High allows only notifications of critical events to display. A setting of Low displays all on-screen notifications for all events. Listed below are individual examples of events that fall into the severity levels: High 1) Protection status has changed. (Protected means that the Advanced Threat Prevention service is running and protecting the computer and needs no user or administrator interaction.) 2) A threat is detected and policy is not set to automatically address the threat. Medium 1) Execution Control blocked a process from starting because it was detected as a threat. 2) A threat is detected that has an associated mitigation (for example, the threat was manually quarantined), so the process has been terminated. 3) A process was blocked or terminated due to a memory violation. 4) A memory violation was detected and no automatic mitigation policy is in effect for that violation type. Low 1) A file that was identified as a threat has been added to the Global Safe List or deleted from the file system. 2) A threat has been detected and automatically quarantined. 3) A file has been identified as a threat but waived on the computer. 4) The status of a current threat has changed (for example, Threat to Quarantined, Quarantined to Waived, or Waived to Quarantined).
Enable BIOS Assurance	Selected	*Selected* *Not Selected* If selected, BIOS integrity checks are performed on end user systems to validate that the BIOS has not been modified from the Dell factory version. A custom factory image cannot be used with this feature, as the BIOS has been modified. This feature is available only on Dell platforms. Platforms available with this feature include the newest release of select XPS, Latitude, Optiplex, Precision Workstations, and Venues. Speak to your Sales Associates for details or contact Dell ProSupport. This policy does not apply to Mac clients.
Script Control	Not Selected	*Selected* *Not Selected* If selected. Script Control protects devices by blocking malicious scripts from running. **Note:** Script Control is currently only available for PowerShell and Active Scripts. This policy does not apply to Mac clients.
Script Control Mode	Alert	*Alert* *Block*

		Alert (default) - Monitors scripts running in the environment. Recommended for initial deployment. **Block - Allow scripts to run only from specific folders. This should be used only after testing in Alert mode.** This policy does not apply to Mac clients.
Script Control Active Script	Alert	*Alert* *Block* Alert (default) - Monitors Active Scripts running in the environment. Recommended for initial deployment. **Block - Allow** Active Scripts **to run only from specific folders. This should be used only after testing in Alert mode.** This policy does not apply to Mac clients.
Script Control Macros	Alert	*Alert* *Block* Alert (default) - Monitors Office macros running in the environment. Recommended for initial deployment. **Block - Allow** Office macros **to run only from specific folders. This should be used only after testing in Alert mode.** **Note:** Starting with Office 2013, macros are disabled by default. Most of the time, users should not be required to enable macros to view the content of an Office document. Dell recommends enabling macros only for documents from trusted users. Otherwise, macros should always be disabled. This policy does not apply to Mac clients.
Script Control PowerShell	Alert	*Alert* *Block* Alert (default) - Monitors PowerShell scripts running in the environment. Recommended for initial deployment. **Block - Allow** PowerShell **scripts to run only from specific folders. This should be used only after testing in Alert mode.** This policy does not apply to Mac clients.
Script Control PowerShell Console	Allow	*Allow* *Block* Allow (default) - Allows the PowerShell console to be launched. Block - Blocks the PowerShell console from being launched. Provides additional security by protecting against the use of PowerShell one-liners. Note: If this policy is set to Block and you use a script that launches the PowerShell console, the script will fail. It is recommended that users change their scripts to invoke the PowerShell scripts, not the PowerShell console. This policy does not apply to Mac clients.
Enable Script Control Approve Scripts in Folders (and Subfolders)	Not Selected	*Selected* *Not Selected* Allows scripts stored in specific folders to be automatically approved to run. This policy must be selected in order to use the policy, Script Control Approve Scripts in Folders (and Subfolders). This policy does not apply to Mac clients.
Script Control Approve Scripts in Folders (and Subfolders)	String	*String* Folders specified in this policy are excluded from actions performed based on the Script Control policy. This exclusion extends to subfolders of folders that are specified with this policy. This policy does not apply to Mac clients.
Global Allow (available only in Disconnected mode)	String	*String* This policy will NOT be sent to the client if the Server does not detect a Disconnected mode install token. The token is prefixed with *DELLAG*.

		The value of this policy must include the entire contents of the policy.xml file. Copy and paste the contents of policy.xml into the policy editor and shown in this example.
Quarantine List (available only in Disconnected mode)	String	*String* This policy will NOT be sent to the client if the Server does not detect a Disconnected mode install token. The token is prefixed with *DELLAG*. The value of this policy includes a collection of hashes, represented by these JSON examples.
Safe List (available only in Disconnected mode)	String	*String* This policy will NOT be sent to the client if the Server does not detect a Disconnected mode install token. The token is prefixed with *DELLAG*. The value of this policy includes a collection of hashes, represented by these JSON examples.
Agent Logs		
Enable Auto-upload of Log Files	Not Selected	*Selected* *Not Selected* If selected, log files are automatically uploaded at 12:00 am or when their size reaches 100 MB.
See basic settings		

Policy	Default Setting	Description
Threat Protection		
Action on Malicious Activity for Processes	Block and Report	*Block Only* *Report Only* *Block and Report* Prevents users from stopping Threat Protection processes and sets the action to take upon attempt. Block Only: Blocks activity but does not report to the Server. Report Only: Reports activity to the Server but does not block activity. Block and Report (default): Blocks and reports activity to the Server.
Suppress Popup Notifications	Not Selected	*Selected or Not Selected* If Selected, no popup notifications of Threat Protection events display on the client computer.
Minimum Popup Notification	Major	*Critical, Major, Minor, Warning, Information* Severity level of popup notifications that display on the client computer. Information displays all on-screen notifications for all events.
Exclude Processes	String	String - Example: avtask.exe Excludes specific process files from Threat Protection scans. Enter the exact resource name of a process to exclude.
Log Files Location	<SYSTEM_DRIVE>:\ProgramData\DDP\Suite\Logs	String - File path Specifies the location for the log files. The default location is <SYSTEM_DRIVE>:\ProgramData\DDP\Suite\Logs.
Enable Activity Logging	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Threat Protection logging policies. If this policy is Not Selected, no Threat Protection logging takes place, regardless of other policy values.

		A Selected value enables Threat Protection logging.
Debug Logging for Malware Protection	Not Selected	*Selected* *Not Selected* A Selected value enables debug logging of Malware and Exploit Protection activity.
Debug Logging for Client Firewall	Not Selected	*Selected* *Not Selected* A Selected value enables verbose logging of Firewall activity.
Debug Logging for Web Protection	Not Selected	*Selected* *Not Selected* A Selected value enables verbose logging of Web Protection activity.
Client Update Schedule	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Client Scheduling policies. If this policy is Not Selected, no Client Scheduling takes place, regardless of other policy values. A Selected value enables the Client Scheduling options.
Client Update Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Client Update Schedule Start Time. Weekly: Runs the task weekly on the days specified in Client Update Day of the Week. Monthly: Runs the task monthly on the specified Client Update Day of the Month.
Client Update Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Client Update Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Client Update Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
See basic settings		
Policy	**Default Setting**	**Description**
Malware Protection		
Malware Protection	Off	*On* *Off* Toggle to ON to enable Malware Protection. If toggled to OFF, no Malware Protection policies will be applied. Malware Protection protects the critical operating system resources from changes made by malware or other unauthorized processes.

On-Access Max Seconds for Scan	45	*10 to 9999* Specifies the maximum number of seconds for each file scan. Limits each file scan to the specified number of seconds. If a scan exceeds the time limit, the scan stops and logs a message.
On-Access Scan Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.
On-Access Scan Processes on Enable	Not Selected	*Selected* *Not Selected* Rescans all processes that are currently in memory each time: - On-Access Scan is disabled and re-enabled. - The computer starts. When the on-access scanner is enabled, it always scans all processes when they are executed. Because some programs or executables start automatically when the computer starts, enabling this option can slow the computer and increase computer startup time.
On-Access Scan Trusted Installers	Not Selected	*Selected* *Not Selected* Scans MSI files or Windows Trusted Installer service files. Disable this option to improve the performance of large Microsoft application installers.
On-Access Scan When Copying Between Local Folders	Not Selected	*Selected* *Not Selected* Scans files whenever the user copies from one local folder to another. If disabled, only items in the destination folder are scanned. If enabled, items in both source and destination folders are scanned.
On-Access Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result

		in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.
On-Demand Protection - Full Scan	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other On-Demand Protection: Full Scan policies. If this policy is Not Selected, no On-Demand Protection: Full Scan policies are enforced, regardless of other policy values. A Selected value means that On-Demand Protection: Full Scan is enabled. This policy must be set to Selected to enable On-Demand Protection: Full Scan settings. If this policy is Not Selected, no On-Demand Protection: Full Scan policies will be applied. By default, every time Full Scan runs, it scans the following locations for threats: - the computer memory for installed rootkits, hidden processes, and other behavior that suggests malware is attempting to hide itself. This scan occurs before all other scans. - the memory of all running processes. - all drives and their subfolders on the computer. By default, the scanner scans all file types, regardless of extension.
Full-Scan Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.
Full-Scan Unwanted Programs	Selected	*Selected* *Not Selected* Enables the scanner to detect potentially unwanted programs. The scanner uses configured information to detect potentially unwanted programs.
Full-Scan Decode MIME Files	Not Selected	*Selected* *Not Selected* Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
Full-Scan - Scan Archives	Selected	*Selected* *Not Selected* Examines the contents of archive (compressed) files, including .jar files. Because scanning compressed files can negatively affect computer performance, Dell recommends using this option in scans during off-work hours.
Full-Scan Files Migrated to Storage	Not Selected	*Selected* *Not Selected* Scans files that remote storage manages. When the scanner encounters a file with migrated content, it restores the file to the local computer before scanning.

Full-Scan Program Threats	Selected	*Selected* *Not Selected* Detects executable files that have code that resembles malware.
Full-Scan Macro Threats	Selected	*Selected* *Not Selected* Detects unknown macro viruses.
Full-Scan - Scan Subfolders	Selected	*Selected* *Not Selected* Examines all subfolders of the specified folder.
Full-Scan Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next content file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.
Full-Scan Exclusions	String	String - Comma-separated list of parameters Specify files, folders, and drives to exclude from scanning. Comma separated list of parameters: <ExclusionType>,<ExclusionData>,<ExcludeSubfolders (only applies to FileOrFolder type)>

		Possible values: <FileOrFolder|FileType|ModifiedAge|AccessedAge|CreatedAge>,<PathToFileOrFolder|FileType|Age>,<true|false> Examples: FileOrFolder,C:\Users,false FileType,xml,false FileType,mp?,false ModifiedAge,120,true AccessedAge,150,false CreatedAge,300,true
Full-Scan Threat First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a threat is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Full-Scan Threat First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when a threat is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Full-Scan Exploit First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a potentially unwanted program is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Full-Scan Exploit First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when an unwanted program is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.

Full-Scan Use Scan Cache	Selected	*Selected* *Not Selected* A Selected value enables the scanner to use the existing clean scan results. A Selected value reduces duplicate scanning and improves performance.
Full-Scan System Utilization	Below Normal	*Low Priority* *Below Normal* *Normal* Enables the operating system to specify the amount of CPU time that the scanner receives during the scan. Each task runs independently, unaware of the limits for other tasks. Low Priority - Provides improved performance for other running applications. Select this option for computers with end user activity. Below Normal - Sets the computer utilization for the scan to the default. Normal - Enables the scan to complete faster. Select this option for computers that have large volumes and little end user activity.
Full-Scan - Scan on Battery Power	Not Selected	*Selected* *Not Selected* A Selected value allows the scan when the computer is using battery power. Not Selected postpones the scan until the computer is no longer using battery power.
Full-Scan Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Full-Scan Schedule Start Time. Weekly: Runs the task weekly on the days specified in Full-Scan Schedule Day of the Week. Monthly: Runs the task monthly on the specified Full-Scan Schedule Day of the Month.
Full-Scan Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Full-Scan Schedule Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Full-Scan Schedule Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
On-Demand Protection - Quick Scan	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other On-Demand Protection: Quick Scan policies. If this policy is Not Selected, no On-Demand Protection: Quick Scan policies are enforced, regardless of other policy values. A Selected value means that On-Demand Protection: Quick Scan is enabled. This policy must be set to Selected to enable On-Demand Protection: Quick Scan settings. If this policy is Not Selected, no On-Demand Protection: Quick Scan policies will be applied. By default, every time Quick Scan runs, it scans the following locations for threats: - the memory of all running processes - the files that the Windows Registry references

		- the contents of the Windows folder - the contents of the Temp folder By default, the scanner scans all file types, regardless of extension.
Quick-Scan Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.
Quick-Scan Unwanted Programs	Selected	*Selected* *Not Selected* Enables the scanner to detect potentially unwanted programs. The scanner uses configured information to detect potentially unwanted programs.
Quick-Scan Decode MIME Files	Not Selected	*Selected* *Not Selected* Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
Quick-Scan - Scan Archives	Selected	*Selected* *Not Selected* Examines the contents of archive (compressed) files, including .jar files. Because scanning compressed files can negatively affect computer performance, Dell recommends using this option in scans during off-work hours.
Quick-Scan Files Migrated to Storage	Not Selected	*Selected* *Not Selected* Scans files that remote storage manages. When the scanner encounters a file with migrated content, it restores the file to the local computer before scanning.
Quick-Scan Program Threats	Selected	*Selected* *Not Selected* Detects executable files that have code that resembles malware.
Quick-Scan Macro Threats	Selected	*Selected* *Not Selected* Detects unknown macro viruses.
Quick-Scan - Scan Subfolders	Selected	*Selected* *Not Selected* Examines all subfolders of the specified folder.
Quick-Scan Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next content file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average

		of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.
Quick-Scan Exclusions	String	String - Comma-separated list of parameters Specify files, folders, and drives to exclude from scanning. Comma separated list of parameters: <ExclusionType>,<ExclusionData>,<ExcludeSubfolders (only applies to FileOrFolder type)> Possible values: <FileOrFolder|FileType|ModifiedAge|AccessedAge|CreatedAge>,<PathToFileOrFolder|FileType|Age>,<true|false> Examples: FileOrFolder,C:\Users,false FileType,xml,false FileType,mp?,false ModifiedAge,120,true AccessedAge,150,false CreatedAge,300,true
Quick-Scan Threat First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a threat is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Quick-Scan Threat First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning*

		Specifies the action for the scanner to take when a threat is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Quick-Scan Exploit First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a potential exploit is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Quick-Scan Exploit First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when an exploit is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Quick-Scan Use Scan Cache	Selected	*Selected* *Not Selected* A Selected value enables the scanner to use the existing clean scan results. A Selected value reduces duplicate scanning and improves performance.
Quick-Scan System Utilization	Below Normal	*Low Priority* *Below Normal* *Normal* Enables the operating system to specify the amount of CPU time that the scanner receives during the scan. Each task runs independently, unaware of the limits for other tasks. Low Priority - Provides improved performance for other running applications. Select this option for computers with end user activity. Below Normal - Sets the computer utilization for the scan to the default. Normal - Enables the scan to complete faster. Select this option for computers that have large volumes and little end user activity.
Quick-Scan - Scan on Battery Power	Not Selected	*Selected* *Not Selected* A Selected value allows the scan when the computer is using battery power. Not Selected postpones the scan until the computer is no longer using battery power.
Quick-Scan Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Quick-Scan

		Schedule Start Time. Weekly: Runs the task weekly on the days specified in Quick-Scan Schedule Day of the Week. Monthly: Runs the task monthly on the specified Quick-Scan Schedule Day of the Month.
Quick-Scan Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Quick-Scan Schedule Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Quick-Scan Schedule Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
Access Protection	Selected	*Selected* *Not Selected* Access Protection prevents other computers from making a connection and creating or altering autorun (autorun.inf) files from CDs. The rule prevents spyware and adware distributed on CDs from being executed and will automatically block and report the issue.
Script Scan Protection	Selected	*Selected* *Not Selected* This policy enables scanning JavaScript and VBScript scripts to prevent unwanted scripts from executing. **Note:** If Script Scan Protection is disabled when Internet Explorer is launched, and then is enabled, it doesn't detect malicious scripts in that instance of Internet Explorer.
Source Sites for Update	Hyperlink	To modify the source sites your clients access for Malware Protection signature updates, click the **Source Sites for Updates** link. To modify the priority level or availability of an external source site, click either NAIHttp or NAIFtp, edit the necessary fields, and click **OK**. To designate an internal signature update server, see Designate a Threat Protection Signature Update Server. Designating a signature update server within your network allows client computers to obtain signature updates without accessing the Internet.
See basic settings		
Policy	**Default Setting**	**Description**
Web Protection		
Web Protection	Off	*On* *Off* Toggle to ON to enable Web Protection. If toggled to OFF, no Web Protection policies will be applied.
Enforcement - Enable HTML iFrames Support	Selected	*Selected* *Not Selected* A Selected value blocks access to malicious (Red) and warn (Yellow) sites that appear in an HTML iframe.
Enforcement - Block Sites by Default if Reputation Service Server is not Reachable	Not Selected	*Selected* *Not Selected* A Selected value blocks access to websites if Web Control cannot reach the Reputation Service server.

Enforcement - Block Phishing Pages for All Sites	Selected	*Selected* *Not Selected* A Selected value blocks all phishing pages, overriding content rating actions.
Enforcement - Specify Reputation Service Risk Level to Block	Very High	*Disable* *Very Low* *Low* *Medium* *High* *Very High* Specifies the Reputation Service risk level to block when the Threat Protection on-demand scan feature is not installed and enabled. Web Protection uses the risk level to calculate the score when retrieving the checksum reputation from the Reputation Service.
IP Exclusions for Web Protection	String	String - IP or IP Range Configures Web Protection not to rate or act on the specified private IP address range. The format is the IP address or IP address range.
Set Default Search Engine	Google	*Google* *Yahoo* *Bing* *Ask* Specifies the default search engine to use for supported browsers: Google, Yahoo, Bing, Ask.
Rating Action for Red Sites	Block	*Block* *Allow* *Warn* Specifies the action to apply to sites that are rated Red. Block: Prevents users from accessing the site and displays a message that the site is blocked. Block is the default for Red sites. Allow: Permits users to access the site. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. Green-rated sites and downloads are automatically allowed.
Rating Action for Yellow Sites	Warn	*Block* *Allow* *Warn* Specifies the action to apply to sites that are rated Yellow. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. Warn is the default for Yellow sites. Green-rated sites and downloads are automatically allowed.
Rating Action for Unrated Sites	Allow	*Block* *Allow* *Warn* Specifies the action to apply to sites that are Unrated. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site. Allow is the default for Unrated sites. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning

		before canceling or proceeding to the site. Green-rated sites and downloads are automatically allowed.
Rating Action for Red Downloads	Block	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are rated Red. Block: Prevents users from downloading the file and displays a message that the download is blocked. Block is the default for Red downloads. Allow: Permits users to proceed with the download. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download.
Rating Action for Yellow Downloads	Warn	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are rated Yellow. Block: Prevents users from downloading the file and displays a message that the download is blocked. Allow: Permits users to proceed with the download. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download. Warn is the default for Yellow sites.
Rating Action for Unrated Downloads	Allow	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are Unrated. Block: Prevents users from downloading the file and displays a message that the download is blocked. Allow: Permits users to proceed with the download. Allow is the default for Unrated downloads. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download.
See basic settings		
Policy	**Default Setting**	**Description**
Client Firewall		
Client Firewall	Off	*On* *Off* Toggle to ON to enable Client Firewall. If toggled to OFF, no Client Firewall Settings or Rules will be applied. Client firewall is a stateful firewall.
Settings and Rules		See Client Firewall Settings and Rules.
See basic settings		

Client Firewall Settings and Rules

In the Client Firewall policy, Settings and Rules, click **View/Edit**.

In the Settings window, you can set Client Firewall Options and Client Firewall Rules.

Return to Client Firewall Policies

Client Firewall Options

Setting	UI Control	Description
Protection Options		
Allow traffic for unsupported protocols	Check box	Allows all traffic that uses unsupported protocols. When disabled, all traffic using unsupported protocols is blocked.
Allow only outgoing traffic until firewall services have started	Check box	Allows outgoing traffic but no incoming traffic until the Firewall service starts. If this option disabled, Firewall allows all traffic before services are started.
Allow bridged traffic	Check box	Allows traffic with a local MAC address. The MAC address is an address in the list of VMs that Firewall supports, not the local system's MAC address. Use this option to allow traffic through a bridged environment with virtual machines.
Enable IP spoof protection	Check box	Blocks network traffic from non-local host IP addresses or from local processes that attempt to spoof their IP address.
Enable firewall intrusion alerts	Check box	Displays alerts automatically when Firewall detects a potential attack.
Setting	**UI Control**	**Description**
Tuning Options		
Enable Adaptive mode	Check box	Creates rules automatically to allow traffic. **NOTE:** Enable this option ***temporarily*** while tuning a deployment.
Log all blocked traffic to client activity log	Check box	*Enabled by default* Logs all blocked traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client.
Log all allowed traffic to client activity log	Check box	*Disabled by default* Logs all allowed traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client. N**OTE:** Enabling this option might negatively impact performance.
Setting	**UI Control**	**Description**
Network Reputation		

Incoming network - reputation threshold	Drop-down menu	*Medium Risk* *Unverified* *DO NOT USE* *High Risk* Specifies the rating threshold for blocking incoming or outgoing traffic from a network connection. Do not block - This site is a legitimate source or destination of content/traffic. Unverified - This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary. Medium Risk - This source/destination shows behavior that is considered suspicious. Any content/traffic from the site requires special scrutiny. High Risk - This source/destination sends or hosts potentially malicious content/traffic that is considered risky.
Outgoing network - reputation threshold	Drop-down menu	*Medium Risk* *Unverified* *DO NOT USE* *High Risk* Specifies the rating threshold for blocking incoming or outgoing traffic from a network connection. Do not block - This site is a legitimate source or destination of content/traffic. Unverified - This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary. Medium Risk - This source/destination shows behavior that is considered suspicious. Any content/traffic from the site requires special scrutiny. High Risk - This source/destination sends or hosts potentially malicious content/traffic that is considered risky.
Setting	**UI Control**	**Description**
Stateful Firewall		
Number of seconds (1-240) before TCP connections time out	Up/down number selector	Specifies the time, in seconds, that an unestablished TCP connection remains active if no more packets matching the connection are sent or received. The default number is 60; the valid range is 1–240.
Number of seconds (1-300) before UDP and ICMP echo virtual connections time out	Up/down number selector	Specifies the time, in seconds, that a UDP or ICMP Echo virtual connection remains active if no more packets matching the connection are sent or received. This option resets to its configured value every time a packet that matches the virtual connection is sent or received. The default number is 60; the valid range is 1–300.
Setting	**UI Control**	**Description**

DNS Blocking		
Domain name	Button/text input field	Defines domain names to block. When applied, this setting adds a rule near the top of the firewall rules that blocks connections to the IP addresses resolving to the domain names. Add - To add a domain name to block, click **Add**, then enter a domain name. You can use the * and ? wildcards. For example, *domain.com. Separate multiple domains with a comma (,) or a carriage return. Duplicate entries are automatically removed. Delete - To remove a domain name from the blocked list, select the domain name and click **Delete**.

Return to top

Client Firewall Rules

Client Firewall applies the rule at the top of the firewall rules list.

1. Client Firewall applies the rule at the top of the firewall rules list. If the traffic meets this rule's conditions, Client Firewall allows or blocks the traffic. It doesn't try to apply any other rules in the list.
2. If the traffic doesn't meet the first rule's conditions, Client Firewall continues to the next rule in the list until it finds a rule that the traffic matches.
3. If no rule matches, the firewall automatically blocks the traffic.

To modify Core Networking or Default Rules, expand either **Core Networking Rules** or **Default Rules**, select the rule to modify, and edit the desired settings, and click **OK**. The settings are described in the table below.

Alternatively, click one of the following buttons to perform the desired action:

Add Rule - Adds a firewall rule.

Duplicate - Creates a copy of the selected item.

Delete - Removes a selected firewall item.

Setting	UI Control	Description
Description		
Name	Text input field	Specifies the descriptive name of the item.
Status	Check box	Select **Enable rule** to make the rule active.

Actions	Radio button/Check box	*Allow* *Block* *Treat match as intrusion* *Log matching traffic* Allow - Allows traffic through the firewall if the item is matched. Block - Stops traffic from passing through the firewall if the item is matched. Treat match as intrusion - Treats traffic that matches the rule as an attack and generates an event that is sent to the Reputation Service. The *Block* action for the rule must be selected for an event to be generated. Log matching traffic - Preserves a record of matching traffic in the Firewall activity log on the Endpoint Security Client.
Direction	Drop-down menu	*In* *Out* *Either* In - Monitors incoming traffic. Out - Monitors outgoing traffic. Either - Monitors both incoming and outgoing traffic.
Notes	Text input field	Provides more information about the rule.
Setting	**UI Control**	**Description**
Networks		
Network protocol	Radio Button/Check box	*Any protocol* *IP protocol* *Non-IP protocol* Any protocol - Allows both IP and non-IP protocols. IP protocol - Excludes non-IP protocols. IPv4 protocol or IPv6 protocol. If neither check box is selected, any IP protocol applies. Both IPv4 and IPv6 can be selected. Non-IP protocol - Includes non-IP protocols only.
Connection types	Check box	*Wired* *Wireless* *Virtual* Indicates if one or all connection types apply. A Virtual connection type is an adapter presented by a VPN or a virtual machine application, such as VMware, rather than a physical adapter.
Specify Networks	Button/Drop-down menu/text input field	To add a network, click **Add**, then specify the following: *Name* - Specifies the network address name (required). *Type* - Select either Local Network or Remote Network. Click **Add**, then specify the following: *Network type* - Specifies the origin or destination of traffic. Select from the network types Single IP, Subnet, Local subnet, Range, or Fully qualified domain

		name *IP address* - Specifies the IP address to add to the network. Wildcards are valid.
Transport		
Transport protocol	Drop-down menu	Select the transport protocol from the drop-down menu.
Executables		
Name	String	The name that you use for the executable to add or edit.
File path	String	The file path to the executable.
File description	String	*Description of the executable.*

Fingerprint	String	*The MD5 hash of the process.*
Enable digital signature check	Check box	Enables or disables the digital signature check that guarantees code hasn't been altered or corrupted since it was signed with a cryptographic hash. If enabled, specify: Allow any signature — Allows files signed by any process signer. Signed by — Allows only files signed by the specified process signer.

Return to top

Return to Client Firewall Policies

Secure Lifecycle

Secure Lifecycle basic policies are available for these populations:

- Cloud Encryption policies - Enterprise, Endpoint Groups, and Endpoints
- Protected Office Documents - Enterprise (master switch)
- Mobile Client - Enterprise, Domain, User Groups, and User

An audit trail of file activity allows you to monitor security. See Secure Lifecycle and Audit Events.

Determine which Secure Lifecycle policy groups you want to enable for Windows and Mac:

Secure Lifecycle Policy Groups	Windows	Mac
Cloud Encryption is *On* Protected Office Documents is *Off*	Office and non-Office documents are protected as .xen files based on policies set. A virtual drive displays in the client's Windows Explorer.	Office and non-Office documents are protected as .xen files based on policies set.
Cloud Encryption is *Off* Protected Office Documents is *On*	Office documents are protected based on policies. For more information, see Set Security Policies to Protect Office Documents in Windows. No virtual drive is created. Non-Office documents are not impacted.	N/A
Both are *On*	Non-Office documents are protected as .xen files if in the virtual drive. A virtual drive displays in the client's Windows Explorer. Office documents have different levels of security based on policy. If protected, the Office document retains its extension in the cloud but unauthorized users cannot access it.	Non-Office documents are protected as .xen files. Office documents are protected based on Protected Office policies. For more information, see Set Security Policies to Protect Office Documents in Mac.

	Additional policies impact Office documents. For more information, see Set Security Policies to Protect Office Documents in Windows.	
Neither is *On*	Files are not protected. If opened, content displays in cleartext.	Files are not protected. If opened, content displays in cleartext.

The DDP Server automatically updates profiles of cloud storage providers. For more information, see Cloud Profile Update.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Cloud Encryption		
Cloud Encryption (Windows and Mac)	On	*On* *Off* Toggle *On* to enable Cloud Encryption policies. If this policy is *Off*, no Cloud protection takes place, regardless of other policies.
Enable In-App Feedback (Cloud) (Windows and Mac)	Not Selected	*Selected* *Not Selected* When selected, an end user can submit feedback and satisfaction ratings to Dell via a link within the client application to a web form.
Enable Access to Restricted File (Windows)	Not Selected	*Selected* *Not Selected* Applies only to Google Drive with Cloud Edition 2.0. *Selected* disables any Google Drive-created shortcuts to the web that Secure Lifecycle cannot encrypt.
Cloud Storage Protection Providers (Windows and Mac)	String Protect,Dropbox_V1 Protect,Box.net_V1 Protect,Chrome_V1* Protect,Firefox_V1* Protect,IE_V1* Protect,SkyDrive_V1 Allow,BoxInstaller_V1 Allow,SkyDriveInstaller_V1 Protect,Flash_V1* Protect,Java_V1* Allow,TrendMicroProxy_V1 Allow,DropboxInstaller_V1 Protect,OneDrive_For_Business_V1 Protect,Google_Drive_V1 Allow,OneDriveForBusinessInstaller_V1 Allow,GoogleDriveInstaller_V1 *For these profiles, ProtectionLevel settings must match.	*String* Profiles that Allow, Block, Protect, or Bypass these providers/connections. Protect: Allow the provider/connection, encrypt the files, and send audit events about file/folder activity. Block: Block all access to the provider/connection. Allow: Allow the provider/connection to pass through without encrypting, but audit file/folder activity. Bypass: Bypass the protection of the provider/connection without encrypting or auditing. When this value is set, the cloud storage provider folder does not display in the DDP|SL virtual drive on the client computer. The format is: ProtectionLevel,ProfileName. ProtectionLevel options: Allow, Protect, Block, Bypass The DDP Server automatically checks for updated profiles of Cloud storage providers supported with Secure Lifecycle. When available, updated profiles are sent to Secure Lifecycle clients after the administrator commits policy changes. When the Pending Policy Changes value in the Remote Management Console is automatically incremented although an administrator has not modified policy values, at least one updated profile is available. The polling interval for Cloud storage provider profile updates is daily at 12:30 a.m.

Dropbox Encrypt Personal Folders (Windows)	Selected	*Selected* *Not Selected* Selected encrypts personal cloud storage provider folders.
Dropbox Encrypt Personal Folders Message (Windows)	String You have added files to your Dropbox (Personal) folder. Do not add business files to your Dropbox (Personal) folder. The names of all files that you add to your Dropbox (Personal) folder are being logged and sent back to the Dell Data Protection Server.	*String* Message to display when Dropbox Encrypt Personal Folders is set to Not Selected. This message is customizable by the Administrator.
Help File Visible (Windows)	Selected	*Selected* *Not Selected* *Selected* allows the registration help file to be visible in the provider folder. More... *Not Selected* hides the help file, therefore, potential file sharers will not be redirected to the registration URL located at https://<yoursecurityserver>.<domain>.com:8443/cloudweb/register.
See advanced settings		

Policy	Default Setting	Description
Protected Office Documents		
Protected Office Documents (Windows and Mac) Note: Enabled only at the Enterprise level.	Off	*On* *Off* Toggle *On* to provide users with a menu option for protecting Office .docx, .xlsx, and .pptx documents. *On* also allows you to enable other Protected Office policies. If this policy is *Off*, no Office-protected formatting takes place, regardless of other policies.
See advanced settings		

Policy	Default Setting	Description
Mobile Client		
Secure Lifecycle Master Switch	Off	*Off* *Cloud Protection* *Protected Office Documents* *Both* Select one option or *Both* to use Secure Lifecycle with mobile clients. If this policy is *Off*, Secure Lifecycle is not enabled for mobile clients, regardless of other policies.
Dropbox	Allow and Audit	*Allow and Audit* *Allow and Protect* *Disallow* Sets the status for Dropbox usage and protection.
Box	Allow and Audit	*Allow and Audit* *Allow and Protect* *Disallow* Sets the status for Box usage and protection.
Google Drive	Allow and Audit	*Allow and Audit* *Allow and Protect*

		Disallow Sets the status for Google Drive usage and protection.
OneDrive	Allow and Audit	*Allow and Audit* *Allow and Protect* *Disallow* Sets the status for OneDrive usage and protection.
OneDrive for Business	Allow and Audit	*Allow and Audit* *Allow and Protect* *Disallow* Sets the status for OneDrive for Business usage and protection.
Apply Encryption to Root Data-Store Location	Selected	*Selected* *Not Selected* Selected encrypts personal cloud storage provider folders.
See advanced settings		

Policy	Default Setting	Description
Settings		
Allow Mac Secure Lifecycle Activation	Selected	*Selected* *Not Selected* *Not Selected* prevents Mac Secure Lifecycle clients from being activated.
Allow Mobile Secure Lifecycle Activation	Selected	*Selected* *Not Selected* *Not Selected* prevents Mobile iOS or Android Secure Lifecycle clients from being activated.

Advanced Secure Lifecycle

Advanced Secure Lifecycle policies are available for these populations:

- Cloud Encryption policies - Enterprise, Endpoint Groups, and Endpoints
- Protected Office Documents - Enterprise, Endpoint Groups, and Endpoints (The *Protected Office Documents* master policy, *Enable Callback Beacon*, and *Callback Beacon URL* policies are available at the Enterprise level only.)
- Mobile Client - Enterprise, Domain, User Groups, and User

See Secure Lifecycle policy groups to determine which policies to enable.

The DDP Server automatically updates profiles of cloud storage providers. For more information, see Cloud Profile Update.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Cloud Encryption		
Cloud Encryption (Windows and Mac)	On	*On* *Off* Toggle *On* to enable Cloud Encryption policies. If this policy is *Off*, no Cloud Encryption protection takes place,

		regardless of other policies.
Dropbox for Business Message (Windows)	String Dropbox for Business is enabled for your organization. If you also have a personal Dropbox account, please do not use it for business purposes. You must allow DDP|CE to access your Dropbox account. Click Next, then enter the credentials for your Dropbox for Business account.	*String* Message to display when Dropbox for Business is enabled for the organization. This message is customizable by the Administrator.
iOS Document Handling (Windows)	Disallow	*Allow* *Disallow* Use this policy to allow or disallow iOS clients to open documents with external applications.
Help File Name (Windows)	1. How to access secure files.html	*String* Name of the registration help file. The file name format is helpfilename.html.
Help File Contents (Windows)	HTML <![CDATA[<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> <head><title>How to Access Secure Files</title></head> <body> <table border="0"> <tr> <th> </th> <th> %PRODUCTNAME% </th> </tr> </table> <hr /> <br /

	%ProgramData%\WebEx	
Excluded Files (Windows)	String C3901A99-1A1B-55B4-AE11-891207B1D341.xen desktop.ini thumbs.db creddb.cef ~$* .~* ~*.tmp .DDPCE.attr *.lnk	*String* Files excluded from encryption, separated by carriage returns.
Server Polling Interval (Windows and Mac)	360 minutes	*1-1440 minutes* How often, in minutes, the client checks in with the EE/VE Server for updates. Default is 360 minutes (6 hours).
Software Update Server URL (Windows)		*String* Use this policy if software updates for users will be located at an alternate Server URL.
Obfuscate Filenames (Windows and Mac)	Extension only	*Extension only* *Guid* Select *Extension only* to display the actual filename with the ".xen" extension. Select *Guid* to display a scrambled filename with the ".xen" extension. When this policy is changed, Cloud Encryption maintains the previous option for any existing folders. Any new folders created will have the new policy applied. To use the new policy with the old files, cut and paste files to a new folder.
Folder Management Enabled (Windows)	Not Selected	*Selected* *Not Selected* *Selected* allows management of encryption on a folder-by-folder basis within the sync client folders. For example, if users uploaded files before installing Secure Lifecycle, you can provide temporary Folder Management rights to some users. To provide temporary Folder Management rights to a user: 1. Set this policy for the specific endpoint to **Selected**. 2. Instruct the user to manually turn on encryption for the pre-existing folder. The files will be encrypted when the files sync to the cloud. 3. After the folders are encrypted, set the *Folder Management Enabled* policy

		for the endpoint back to *Not Selected*.
See basic settings		
Policy	**Default Setting**	**Description**
Protected Office Documents		
Protected Office Documents (Basic - Windows and Mac) Note: Enabled only at the Enterprise level.	Off	*On* *Off* Toggle *On* to provide users with a menu option for protecting Office .docx, .xlsx, and .pptx documents. On also allows you to enable other Protected Office policies. If this policy is *Off*, no Office-protected formatting takes place, regardless of other policies.
Force Protected Files Only (Windows)	Not Selected	*Selected* *Not Selected* *Selected* forces users to save Office files as protected documents. It also enables a sweep on the clients' internal fixed drives to locate new Office files and change them to Protected mode. It disables the Share option (Office 2013 and 2016) and Save & Send option (Office 2010). If *Not Selected*, users have some options in determining whether to save a file as protected or unprotected.
Enable Time To Live and Embargo Control (Windows)	Not Selected	*Selected* *Not Selected* *Selected* allows users to specify dates for when protected Office files are accessible to external users.
Print Control (Windows)	Allowed	*Allowed* *Watermark* *Disabled* Controls the Print function of protected Office .docx, .pptx, and .xlsx documents: • Allowed - Print option is enabled for protected Office documents. • Watermark - Print option is enabled for protected Office documents but a watermark with the user's name, domain name, and computer ID displays on each page. Unprotected documents print without the watermark. • Disabled - Print option is disabled for protected Office documents. Users can print unprotected Office documents.

		Note: If **Force Protected Files Only** is *Not Selected*, the Print option is available for all unprotected Office documents.
Export Control (Windows)	Allowed	*Allowed* *Watermark* *Disabled* For Office 2013 and higher, controls the Export function of protected Office .docx, .pptx, and.xlsx documents: • Allowed - This varies based on whether **Force Protected Files Only** is *Selected*. For detailed information, see Set Security Policies to Protect Office Documents. • Watermark - Export is disabled. See Protected Export. • Disabled - Export is disabled for protected Office documents. Users can export unprotected Office documents. Note: For Office 2010, see Save and Send.
Office Protected Clip Board Unauthorized Text (Windows)	Pasting of protected data is not allowed on this computer. Please contact your administrator for assistance.	String to display when a user attempts to paste secure data from a protected document into an unprotected location.
Office Protected Document Tamper Prompt (Windows)	The file you have attempted to open appears to have been tampered with and can no longer be validated. Please contact the original author or your administrator.	String to display if a user encounters an Office-protected document that is identified as having been tampered with.
Offline Key Generation Escrow Reminder Delay (Windows)	3 days	*1-14 days. 3 days default.* Specifies the number of days the client will wait while not being able to escrow key material prior to warning the end user.
Offline Key Generation Escrow Reminder Text (Windows)	Dell Data Protection | Secure Lifecycle has not been able to contact the DDP Server for several days. Please ensure that you are connected to the network. If you are connected to the network, contact your Administrator.	String to display when the end user is warned that the client cannot escrow key material.
Office Protected Files Cover Page Notice (Windows and Mac)	String	Enterprise-defined text to be displayed on Office-protected cover pages. Maximum number of character is 4096. See Set Cover Page Policies. Note: If line breaks are entered as part of the text, they are automatically converted to spaces to ensure the text displays correctly in all Office applications.
Office Protected Files Cover Page Corporate Logo (Windows and Mac)	Browse button and Save Logo File button	Image to be displayed on the document cover page. See Set Cover Page Policies. Note: The logo image must be a .jpg of square dimensions with a maximum file size of 25 KB. If the image height and width dimensions are not equal, the displayed image is stretched.
Office Protected Files Cover Page DDP	https://server	DDP Server URL that will be displayed

Server URL (Windows and Mac)		on the cover page.
Enable Callback Beacon	Selected	Selected inserts a callback beacon into every protected Office file. To use the callback beacon, the following requirements must be met: • The beacon server must be installed as part of Front End Server/Proxy Mode installation. Port 8446 must be open. For more information, see the *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start Guide and Installation Guide*. • An administrator must have enrolled to receive Product Notifications. • The *Callback Beacon URL* policy is set.
Callback Beacon URL	String	Specifies the URL to be used when the callback beacon is inserted into Office-protected files. The URL must be externally available, hosted on an HTTP server that is installed as part of Front End Server/Proxy Mode installation. Port 8446 must be open. For more information, see the *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start Guide and Installation Guide*. The *Enable callback beacon* policy must be Selected.
See basic settings		
Policy	**Default Setting**	**Description**
Mobile Client		
Secure Lifecycle Geo Location Audit Data	Selected	*Selected* allows audit data to include geo-tracking location data.
Enable Callback Beacon	Selected	Selected inserts a callback beacon into every protected Office file. To use the callback beacon, the following requirements must be met: • The beacon server must be installed as part of Front End Server/Proxy Mode installation. Port 8446 must be open. For more information, see the *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start Guide and Installation Guide*. • An administrator must have enrolled to receive Product

		Notifications. • The *Callback Beacon URL* policy is set.
Callback Beacon URL	String	Specifies the URL to be used when the callback beacon is inserted into Office-protected files. The URL must be externally available, hosted on an HTTP server that is installed as part of Front End Server/Proxy Mode installation. Port 8446 must be open. For more information, see the *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start Guide and Installation Guide*. The *Enable callback beacon* policy must be Selected.
Server Polling Interval	360 minutes	*1-1440 minutes* How often, in minutes, the client checks in with the EE/VE Server for updates. Default is 360 minutes (6 hours).
Workspace Access		
Application pass code (PIN)	4	*4 or 6* Required number of characters for Workspace PIN.
Set maximum failed login attempts	8	*4 - 16* Define the number of PIN login failures. Then set the policy for action to take on the Workspace after the failed attempts.
Set action on maximum failed login attempts	Timeout for 1 minute	*Timeout for 1 minute* *Timeout for 5 minutes* *Lock Workspace* *Wipe Workspace Data* The action to take after the maximum failed login attempts are reached.
Set inactivity lock duration	5	*2, 5, 20, 30, or 60 minutes* Configure the amount of inactivity time that can elapse before the end user must re-enter a PIN.
Set copy/paste capabilities	Not Selected	*Selected* *Not Selected* *Selected* allows users to copy and paste outside of the workspace.
Allow Non-Genuine device OS	Not Selected	*Selected* *Not Selected* *Selected* allows a jailbroken iOS device or a rooted Android device.
Cover Page		
Office Protected Files Cover Page Acceptance Text	String	Enterprise-defined text to be displayed on Office-protected cover pages. See Set Cover Page Policies.
Office Protected Files Cover Page Corporate Logo	Browse button and Save Logo File button	Image to be displayed on the document cover page. See Set Cover Page Policies. Note: The logo image must be a .jpg of square dimensions with a maximum

		file size of 25 KB. If the image height and width dimensions are not equal, the displayed image is stretched.
Office Protected Files Cover Page DDP Server URL	https://server	DDP Server URL that will be displayed on the cover page.
Office Protected Document Tamper Prompt	The file being opened appears to have been tampered with and can no longer be validated. Please contact the original author or your administrator.	Text to be displayed if a user encounters an Office Protected Document that has been determined was tampered with.
Web Browser		
Set a default homepage	http://www.dell.com	Homepage default for the Workspace browser.
Pre-configure bookmarks		Pre-configure bookmarks.
See basic settings		

Set Cover Page Policies

You can set policies to customize a cover page for protected Office documents.

- Internal users - The cover page displays for the following:
    - Protected Office Documents policies have been enabled but the user has not yet installed or activated the Secure Lifecycle.
    - User opens a protected Office document from the cloud.
    - User downloads a protected Office document to a device that does not have Secure Lifecycle installed.
- Unauthorized users - The cover page displays, and the person cannot access the content.

To customize the cover page for protected Office documents, you can use these Advanced Secure Lifecycle policies:

- Office Protected Files Cover Page Notice
- Office Protected Files Cover Page Corporate Logo
- Office Protected Files Cover Page DDP Server URL

Removable Media Encryption

A note about Removable Storage policies: EMS for Mac policies are device-based policies. This is different behavior than EMS for Windows, which are user-based.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Windows Media Encryption		
Windows Media Encryption	Off	Toggle ON to enable Windows Removable Media Encryption policies. If this policy is toggled to OFF, no Windows Removable Media Encryption takes place, regardless of other policies.
EMS Scan External Media	Not Selected	Selected allows EMS to scan removable storage every time removable storage is

		inserted. When this policy is Not Selected and the EMS Encrypt External Media policy is Selected, EMS only encrypts new and changed files. More... A scan occurs at every insertion so that EMS can catch any files added to the removable storage without authenticating. You can add files to the removable storage if you decline to authenticate, but you cannot access encrypted data. The files added will not be encrypted in this case, so the next time you authenticate to the removable media to work with encrypted data, EMS scans it and encrypts any files that may have been added without encryption.
EMS Access to unShielded Media	Read Only	Block, Read Only, Full Access Note that this policy interacts with the Port Control System - Storage Class: External Drive Control policy. If you intend to set this policy to Full Access, ensure that Storage Class: External Drive Control is not set to Read Only or Blocked. More... When this policy is set to Block Access, you have no access to removable storage unless it is encrypted. Choosing either Read-Only or Full Access allows you to decide what removable storage to encrypt. If you choose not to encrypt removable storage and this policy is set to Full Access, you have full read/write access to removable storage. If you choose not to encrypt removable storage and this policy is set to Read-Only, you can read or delete existing files on the unencrypted removable storage, but the Shield will not allow any files to be edited on, or added to, the removable storage.
EMS Block Access to UnShieldable Media	Selected	Block access to any removable storage that is less than 55 MB and thus has insufficient storage capacity to host a Removable Media Shield (such as a 1.44MB floppy disk). More... All access is blocked if Encrypt External Media and this policy are both True. If Encrypt External Media is True, but this policy is False, data can be read from the unShieldable removable storage, but write access to the media is blocked. If Encrypt External Media is False, then this policy has no effect and access to unShieldable removable storage is not impacted.
See advanced settings		
Policy	**Default Setting**	**Description**
Mac Media Encryption		
Mac Media Encryption	Off	Toggle On to enable Mac Removable Media

		Encryption policies. If this policy is toggled to OFF, no Mac Removable Media Encryption takes place, regardless of other policies. HFS Plus is supported and must be enabled. For instructions to enable HFS Plus, see the Enterprise Edition for Mac Administrator Guide. Media containing Time Machine backups are not supported. However, media recognized by computers as Time Machine backup destinations are automatically whitelisted, to allow backups to continue. All other removable media with Time Machine backups are handled based on *EMS Access to unShielded Media* and *EMS Block Access to UnShieldable Media* policies.
EMS Scan External Media	Not Selected	Selected allows EMS to scan removable storage every time removable storage is inserted. When this policy is Not Selected and the EMS Encrypt External Media policy is Selected, EMS only encrypts new and changed files. More... A scan occurs at every insertion so that EMS can catch any files added to the removable storage without authenticating. You can add files to the removable storage if you decline to authenticate, but you cannot access encrypted data. The files added will not be encrypted in this case, so the next time you authenticate to the removable media to work with encrypted data, EMS scans it and encrypts any files that may have been added without encryption.
EMS Access to unShielded Media	Read Only	*Block, Read Only, Full Access* When this policy is set to Block Access, you have no access to removable storage unless it is encrypted. Choosing either Read-Only or Full Access allows you to decide what removable storage to encrypt. If you choose not to encrypt removable storage and this policy is set to Full Access, you have full read/write access to removable storage. If you choose not to encrypt removable storage and this policy is set to Read-Only, you cannot read or delete existing files on the unencrypted removable storage, but the Shield will not allow any files to be edited on, or added to, the removable storage unless it is encrypted.
EMS Block Access to UnShieldable Media	Selected	Block access to any removable storage that is less than 55 MB and thus has insufficient storage capacity to host a Removable Media Shield (such as a 1.44MB floppy disk). All access is blocked if Encrypt External Media and this policy are both True. If Encrypt External Media is True, but this policy is False, data can be read from the unShieldable removable storage, but write access to the media is blocked. If Encrypt External Media is False, then this policy has no effect and access to unShieldable removable storage is not

		impacted.
See advanced settings		
Policy	**Default Setting**	**Description**
Media Encryption Settings		
Event Retention		"security", "fail", "30" "security", "success", "30" "application", "error", "30" "application", "warn", "15" "application", "info", "5" "application", "debug", "5" Defines the amount of time (in days) that EMS, HCA, and PCS event types are maintained in the Server event log. Each event type is defined by category and level. You may set different retention times for each event level in each category. The "Security" category represents events related to user authentication, authorization, or encryption. This includes events for Shielding devices, updating security policies, or failed authentication attempts. "Security" events are further differentiated by a "fail" or "success" indicating the outcome of the event. The "Application" category (application type event, rather than a security type event) represents events related to general application actions. These events are further differentiated by a set of severity levels - "error", "warn", "info", and "debug". You should use longer retention times for more severe levels.

Removable Media Policies that Require Logoff

- EMS Encrypt External Media
- EMS Scan External Media
- EMS Encryption Algorithm
- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Advanced Removable Media Encryption

A note about Removable Storage policies: EMS for Mac policies are device-based policies. This is different behavior than EMS for Windows, which are user-based.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description

Windows Media Encryption		
Windows Media Encryption	Off	Toggle On to enable Windows Removable Media Encryption policies. If this policy is toggled to OFF, no Windows Removable Media Encryption takes place, regardless of other Removable Media Encryption policies.
EMS Exclude CD/DVD Encryption	Not Selected	**False encrypts CD/DVD devices.**
EMS Allow Read-access to unShielded Media (5.4.x Only)	Selected	This policy applies to 5.4.x Windows Shields only. More... If an end-user chooses not to encrypt media and this policy is set to True, they will be able to read or delete existing files on the unShielded media, but the Shield will not allow any files to be edited on or added to the removable storage unless it is Shielded.
EMS Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt removable storage. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
EMS Data Encryption Key	User Roaming	Common, User, User Roaming Choose a key to be used by the Shield to encrypt all data encrypted by the External Media Shield. More... You cannot save a policy where this policy has the same value as either User Data Encryption Key policy or Application Data Encryption Key policy, the error message *Policy Constraint Violation: The value for EMS Data Encryption Key conflicts with User Data Encryption Key and/or Application Data Encryption Key* will display.
EMS Automatic Authentication	Local	Disabled, Enable Local, Enable Roaming Local automatic authentication allows the Shielded media to be automatically authenticated when inserted in the originally Shielding computer when the owner of that media is logged in. When the User Roaming key is applied to EMS, Roaming Automatic Authentication allows Shielded media to be automatically authenticated when it is inserted in any Shielded computer the media owner is logged into. When automatic authentication is disabled, users must always manually authenticate to access Shielded media. Disabling Roaming Authentication helps to prevent users from forgetting their password when they take the media home or share it with a colleague. Disabling Roaming Authentication also promotes a sense of awareness from a security perspective for users that the data being written to that media is protected.
EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable storage whether the endpoint is Shielded or not. More... When this policy is False, the user will be able to work with encrypted data when logged on to any Shielded endpoint, regardless of the Enterprise Server the user activated against. The user will not be able to work with encrypted data using any unShielded device.
EMS Device Whitelist		String - Maximum of 300 devices with a maximum of 500 characters per PNPDeviceID. Maximum of 4096 total characters allowed. "Space" and "Enter" characters used count in the total characters used. This policy allows the specification of removable storage devices to exclude from EMS encryption [using the removable storage device's Plug and Play device identifier (PNPDeviceID)], thereby allowing users full access to the specified removable storage devices. More... This policy is available on an Enterprise, Domain, Group, and User level. Note that local settings override inherited settings. If a user is in more than one group, all EMS Device Whitelist entries, across all Groups, apply. Note: This policy is particularly useful when using removable storage

		devices which provide hardware encryption. However, this policy should be used with caution. This policy does not check whether external media devices on this list provide hardware encryption. Whitelisting removable storage devices which do not have hardware encryption will not have enforced security and will not be protected.
		
		For example, the Kingston® DataTraveler® Vault Privacy model enforces that encryption is enabled to use the device. However, the Kingston DataTraveler Vault model has an unsecured partition and a secured partition. Because it is the same physical removable storage device with only one PNPDeviceID, the two partitions cannot be distinguished, meaning that whitelisting this particular removable storage device would allow unencrypted data to leave the endpoint.
		
		Additionally, if an removable storage device is protected by EMS and subsequently added to the EMS Device Whitelist policy, it remains encrypted and requires a reformat of the removable storage device to remove encryption.
		
		The following is an example of a PNPDeviceID, which contains the manufacturer identifier, product identifier, revision, and hardware serial number:
		
		`USBSTOR\DISK&VEN_KINGSTON &PROD_DTVAULT_PRIVACY& REV_104\07005B831A0004B4&0`
		
		To whitelist a removable storage device, provide a string value which matches portions of the device's PNPDeviceID. Multiple device PNPDeviceIDs are allowed.
		
		For example, to whitelist all Kingston DataTraveler Vault Privacy models, input the string:
		
		`PROD_DTVAULT_PRIVACY`
		
		To whitelist both models of Kingston DataTraveler, the Vault and Vault Privacy models, input the string:
		
		`PROD_DTVAULT_PRIVACY; PROD_DT_VAULT`
		
		Note that space characters are considered part of the substring to match to a PNPDeviceID. Using the previous PNPDeviceID as an example, a space before and after the semicolon would cause neither of the substrings to be matched, because the space character is not part of the PNPDeviceID.
		
		Instructions...
		
		To find and edit the PNPDeviceID for removable storage:
		
		1. Insert the removable storage device into a Shielded computer.
		2. Open the EMSService.log in C:\Programdata\Dell\Dell Data Protection\Encryption\EMS.
		3. Find PNPDeviceID= and enter the applicable values, explained below.
		
		For example:
		14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0
		
		Specify the following:
		
		VEN=Vendor; Green highlighted text represents the vendor's devices to be excluded
		
		PROD=Product/Model Name; Blue highlighted text also excludes all of Seagate's USB drives; a value represented by green highlighted text must precede this value
		
		REV=Firmware Revision; Gray highlighted text also excludes the specific model being used; values represented by green and blue highlighted text must precede this value
		
		Serial number (in this example); Yellow highlighted text excludes only this device; values represented by green,

		blue, and gray highlighted text must precede this value OR *To find the PNPDeviceID for removable storage on Windows 7 or later:* 1. Insert the removable storage device. 2. Open the Control Panel and go to Administrative Tools > Computer Management. 3. Select the Hardware tab, select the drive, and click Properties. 4. A new windows displays. Select the Device Instance Path in the Property drop-down menu. The PNPDeviceID is displayed in the Value field. *To find the PNPDeviceID for removable storage on Windows XP:* 1. Click Start > Run... 2. Type msinfo32 and click Enter. 3. When the System Information window displays, go to Components > USB. A list of USB devices and their PNPDeviceIDs displays. **Available Delimeters:** Tabs Commas Semi colons Hex character 0x1E (Record separator character)
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.
EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters Required in Password	8	1-40 characters Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	Selected	Selected requires one or more numeric characters in the password.
EMS Password Attempts Allowed	3	1-10 Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.
EMS Access and Device Code Length	16	8, 16, 32 Number of characters access and device codes have. 32 characters is the most secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	1-10 Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	Apply Cooldown, Wipe Encryption Keys Action to take following unsuccessful Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the specified cooldown period (Cooldown Time Delay and Cooldown Time Increment policies) • Wipe Encryption Keys to have the Shield delete the encryption keys on the removable storage, making the encrypted data inaccessible until the owner takes the media to a Shielded computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	String - 5-512 characters - Authentication Failed: Please contact your system administrator. Message that displays when a user needs to contact you for an access

		code (after authentication failure). More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. We recommend that you customize the second sentence of the message to include specific instructions about how to contact a Help Desk or Security Administrator for authentication failures.
EMS Cooldown Time Delay	30	0-5000 seconds Number of seconds the user must wait between the first and second rounds of access code entry attempts.
EMS Cooldown Time Increment	20	0-5000 seconds Incremental time to add to the previous cooldown time after each unsuccessful round of access code entry attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	String - 5-512 characters - You are not authorized to use this media. Please contact your system administrator. Message that displays following unsuccessful Access Code Attempts Allowed. More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. We recommend that you customize the message to include specific instructions about how to contact the Help Desk or Security Administrator.
EMS Encryption Rules		Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. "Space" and "Enter" characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as Firewire, USB, eSATA, etc. may require the use of both EMS and encryption rules to encrypt the endpoint. This is necessary due to differences in how the Windows operating system handles storage devices based on interface type. To ensure encrypting an iPod via EMS does not make the device unusable, use the following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories above. Adding the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx files are encrypted in the directories excluded from encryption via the previous rules: ^R#:\Calendars ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx .xlsx ^R#: \iPod_Control ;ppt.doc

		.xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx Replacing these five rules with the following rule will force encryption of ppt, pptx, doc, docx, xls, and xlsx files in any directory on the iPod, including Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file types for all removable devices - not just an iPod. Use care when defining rules to exclude an iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation iPod Mini 4gb second generation We do not recommend the use of the iPod Shuffle, as unexpected results may occur. As iPods change, this information could also change, so caution is advised when allowing the use of iPods on EMS-enabled computers. Because folder names on iPods are dependent on the model of the iPod, we recommend creating an exclusion encryption policy which covers all folder names, across all iPod models.
See basic settings		
Mac Media Encryption		
Mac Media Encryption	Off	Toggle On to enable Mac Removable Media Encryption policies. If this policy is toggled to OFF, no Mac Removable Media Encryption takes place, regardless of other policies.
EMS Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt removable storage. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
EMS Data Encryption Key	User Roaming	Common, User, User Roaming ***Note that although Common is available, it is not implemented in this release.*** Choose a key to be used by the Shield to encrypt all data encrypted by the External Media Shield.
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.
EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters. Required in Password	8	1-40 characters Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	Selected	Selected requires one or more numeric characters in the password.
EMS Password Attempts Allowed	3	1-10 Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.

EMS Access and Device Code Length	16	8, 16, 32 Number of characters access and device codes have. 32 characters is the most secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	1-10 Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	Apply Cooldown, Wipe Encryption Keys Action to take following unsuccessful Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the specified cooldown period (Cooldown Time Delay and Cooldown Time Increment policies) • Wipe Encryption Keys to have the Shield delete the encryption keys on the removable storage, making the encrypted data inaccessible until the owner takes the media to a Shielded computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	String - 5-512 characters - Authentication Failed: Please contact your system administrator. Message that displays when a user needs to contact you for an access code (after authentication failure). More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. We recommend that you customize the second sentence of the message to include specific instructions about how to contact a Help Desk or Security Administrator for authentication failures.
EMS Cooldown Time Delay	30	0-5000 seconds Number of seconds the user must wait between the first and second rounds of access code entry attempts.
EMS Cooldown Time Increment	20	0-5000 seconds Incremental time to add to the previous cooldown time after each unsuccessful round of access code entry attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	String - 5-512 characters - You are not authorized to use this media. Please contact your system administrator. Message that displays following unsuccessful Access Code Attempts Allowed. More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. We recommend that you customize the message to include specific instructions about how to contact the Help Desk or Security Administrator.
EMS Encryption Rules		Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. "Space" and "Enter" characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as Firewire, USB, eSATA, etc. may require the use of both EMS and encryption rules to encrypt the endpoint. This is necessary due to differences in how the Windows operating system handles storage devices based on interface type. To ensure encrypting an iPod via EMS does not make the device

		unusable, use the following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories above. Adding the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx files are encrypted in the directories excluded from encryption via the previous rules: ^R#:\Calendars ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx .xlsx ^R#: \iPod_Control ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx Replacing these five rules with the following rule will force encryption of ppt, pptx, doc, docx, xls, and xlsx files in any directory on the iPod, including Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file types for all removable devices - not just an iPod. Use care when defining rules to exclude an iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation iPod Mini 4gb second generation We do not recommend the use of the iPod Shuffle, as unexpected results may occur. As iPods change, this information could also change, so caution is advised when allowing the use of iPods on EMS-enabled computers. Because folder names on iPods are dependent on the model of the iPod, we recommend creating an exclusion encryption policy which covers all folder names, across all iPod models.
EMS Automatic Authentication	Local	Disabled, Enable Local, Enable Roaming Local automatic authentication allows the Shielded media to be automatically authenticated when inserted in the originally Shielding computer when the owner of that media is logged in. When the User Roaming key is applied to EMS, Roaming Automatic Authentication allows Shielded media to be automatically authenticated when it is inserted in any Shielded computer the media owner is logged into. When automatic authentication is disabled, users must always manually authenticate to access Shielded media. Disabling Roaming Authentication helps to prevent users from forgetting their password when they take the media home or share it with a colleague. Disabling Roaming Authentication also promotes a sense of awareness from a security perspective for users that the data being written to that media is protected.

EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable storage whether the endpoint is Shielded or not. When this policy is False, the user will be able to work with encrypted data when logged on to any Shielded endpoint, regardless of the Server the user activated against. The user will not be able to work with encrypted data using any unShielded endpoint.
EMS Device Whitelist		String - Maximum of 150 devices with a maximum of 500 characters per PNPDeviceID. Maximum of 2048 total characters allowed. "Space" and "Enter" characters used count in the total characters used. This policy allows the specification of removable storage devices to exclude from EMS encryption [using the removable storage device's Plug and Play device identifier (PNPDeviceID)], thereby allowing users full access to the specified removable storage devices. More... This policy is available on an Enterprise, Domain, Group, and Endpoint level. Note that local settings override inherited settings. If a device is in more than one group, all EMS Device Whitelist entries, across all Groups, apply. Note: This policy is particularly useful when using removable storage devices which provide hardware encryption. However, this policy should be used with caution. This policy does not check whether external media devices on this list provide hardware encryption. Whitelisting removable storage devices which do not have hardware encryption will not have enforced security and will not be protected. Additionally, if a removable storage device is protected by EMS and subsequently added to the EMS Device Whitelist policy, it remains encrypted and requires a reformat of the removable storage device to remove encryption. Instructions... 1. Insert USB removable media. 2. Open System Profiler. 3. Under Hardware, select the USB device and find the Product ID and Vendor ID, as follows: Capacity:2.06 GB (2,055,019,008 bytes) Removable Media:Yes Detachable Drive:Yes BSD Name:disk2 **Product ID:0x5406** **Vendor ID:0x0781 (SanDisk Corporation)** Version: 0.10 Serial Number:0000188C36725BC8 Speed:Up to 480 Mb/sec Manufacturer:SanDisk Location ID:0x24100000 Current Available (mA):500 Current Required (mA):200 Partition Map Type:MBR (Master Boot Record) S.M.A.R.T. status:Not Supported 4. The following Whitelist Rules can be used: USBVendorName=abc USBVendorNum=0x02 USBVendorNum=2,USBProductNum=3 USBVendorNum=2,USBProdName=abc For this example, in the Enterprise Server, add the following key/pair string to the EMS Device Whitelist policy, as shown below: "USBVendorNum=0x0781,USBProductNum=0x05406"

		(including quotes) 5. When satisfied with the EMS Device Whitelist rules, save and commit the policy.
See basic settings		

Removable Media Policies that Require Logoff

- EMS Encrypt External Media
- EMS Scan External Media
- EMS Encryption Algorithm
- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Mobile Protection

Mobile Protection Policies apply to iOS, EAS, and Androids.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Mobile Edition - EAS		
Require Passcode on Device	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines whether the user is forced to set a PIN. Simply setting this value (and not others) forces the user to enter a passcode, without imposing a length or quality.
Inactivity Period for Device Lock	60 minutes	*0-60 minutes* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the number of minutes for which the device can be idle (without user input) before it gets locked by the system. Once this limit is reached, the device is locked and the passcode must be entered.
Require Device Encryption	Not Selected	*Selected* *Not Selected* When Selected the device must be encrypted or it will be blocked.
See advanced settings		
Policy	Default Setting	Description

Mobile Edition - iOS		
Require Passcode on Device	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines whether the user is forced to set a PIN. Simply setting this value (and not others) forces the user to enter a passcode, without imposing a length or quality.
Allow iOS Devices	Not Selected	*Selected or Not Selected* When Selected, allows all iOS devices to have Exchange access.
Allow Non-iOS Devices	Not Selected	*Selected or Not Selected* When Selected, allows all non-iOS devices to have Exchange access.
Block iOS Prior To Enrollment	Selected	*Selected or Not Selected* When Not Selected, iOS Exchange access is blocked until device has completed the initial iOS enrollment process. The device will be in a Discovered state until enrolled.
See advanced settings		
See advanced settings		

Advanced Mobile Protection

Mobile Protection Policies apply to iOS, EAS, and Androids.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Mobile Edition - EAS		
Allow Simple Characters in Passcode	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines whether a simple passcode is allowed. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA). Setting this value to Not Selected is synonymous to setting Minimum Complex Characters in Passcode to 1. During testing, we observed that some Android devices ignored this policy.
Minimum Complex Characters in Passcode	1	*0-4 characters* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in

		the Exchange ActiveSync policy category, and vice-versa. Specifies the minimum number of complex characters that a passcode must contain. A complex character is a character other than a number or a letter, such as &%$#.
Maximum Passcode Age	30 days	*0-365 days. 30 days default.* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the number of days for which the passcode can remain unchanged. After this number of days, the user is forced to change the passcode before the device is unlocked. Set to 0 to require the passcode to be changed each time the device is unlocked (not recommended). **NOTE:** We have seen in testing that setting this value to 1 causes the device to request a new passcode every minute.
Number of Unique Passcodes Before Reuse	0	*0-50 passcodes* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines the number of unique new passcodes that have to be associated with a user account before an old passcode can be reused. Set to 0 to disable; set to 1 to disallow reusing the current passcode.
Minimum Passcode Length	4	*0-18 characters* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the minimum password length if passcode is enabled. This parameter is independent of the Minimum Complex Characters in Passcode policy.
Require Alphanumeric Characters in Passcode	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies whether the user must enter alphabetic characters (abcd), or if numbers are sufficient.
Number of Failed Passcode Attempts Before Device Wipe	16	*4-16 failed passcode attempts* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies how many times an incorrect password can be entered before the mobile device performs a wipe of all data.

Allow Camera	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. When Not Selected, the Camera is disabled and its icon is removed from the Home screen.
Allow Browser	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. When Not Selected, the web browser application is disabled and its icon removed from the Home screen.
Encrypt Storage Card	Not Selected	*Selected* *Not Selected* When Selected the device's storage card must be encrypted or it will be blocked.
See basic settings		
Policy	**Default Setting**	**Description**
Mobile Edition - iOS		
Allow Simple Characters in Passcode	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines whether a simple passcode is allowed. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA). Setting this value to Not Selected is synonymous to setting Minimum Complex Characters in Passcode to 1. During testing, we observed that some Android devices ignored this policy.
Require Alphanumeric Characters in Passcode	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies whether the user must enter alphabetic characters (abcd), or if numbers are sufficient.
Minimum Passcode Length	4	*0-18 characters* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and

		vice-versa. Specifies the minimum password length if passcode is enabled. This parameter is independent of the Minimum Complex Characters in Passcode policy.
Minimum Complex Characters in Passcode	1	*0-4 characters* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the minimum number of complex characters that a passcode must contain. A complex character is a character other than a number or a letter, such as &%$#.
Maximum Passcode Age	30 days	*0-365 days. 30 days default.* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the number of days for which the passcode can remain unchanged. After this number of days, the user is forced to change the passcode before the device is unlocked. Set to 0 to require the passcode to be changed each time the device is unlocked (not recommended). **NOTE:** We have seen in testing that setting this value to 1 causes the device to request a new passcode every minute.
Inactivity Period for Device Lock	60 minutes	*0-60 minutes* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the number of minutes for which the device can be idle (without user input) before it gets locked by the system. Once this limit is reached, the device is locked and the passcode must be entered.
Number of Unique Passcodes Before Reuse	0	*0-50 passcodes* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines the number of unique new passcodes that have to be associated with a user account before an old passcode can be reused. Set to 0 to disable; set to 1 to disallow reusing the current passcode.
Grace Period for Device Lock	0	*0-240 minutes* The maximum grace period, in minutes, to unlock the phone without entering passcode. The default is 0, no grace period, which requires a passcode immediately.
Number of Failed Passcode Attempts Before Device Wipe	16	*4-16 failed passcode attempts* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in

		the Exchange ActiveSync policy category, and vice-versa. Specifies how many times an incorrect password can be entered before the mobile device performs a wipe of all data.
Allow Removal Passcode	Not Selected	*Selected* *Not Selected* Set to Selected if there is a removal passcode.
Disallow Payload Removal	Not Selected	*Selected* *Not Selected* If present and set to Selected, the user cannot delete the profile (unless the profile has a removal password and the user provides it). If locked in this way, the profile can be replaced be a new version only if the profile identifier matches and the profile is signed by the same authority.
Removal Password Value	1-32 characters	*1-32 characters* Specifies the removal password for the profile.
Allow Browser	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. When Not Selected, the web browser application is disabled and its icon removed from the Home screen.
Allow YouTube	Selected	*Selected* *Not Selected* When Not Selected, the YouTube application is disabled and its icon is removed from the Home screen.
Allow Camera	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. When Not Selected, the Camera is disabled and its icon is removed from the Home screen.
Allow iTunes	Selected	*Selected* *Not Selected* When Not Selected, the iTunes Music Store is disabled and its icon is removed from the Home screen. Users cannot preview, purchase, or download content.
Allow Installing Apps	Selected	*Selected* *Not Selected* When Not Selected, the App Store is disabled and its icon is removed from the Home screen. Users are unable to install or update their applications.
Allow Explicit Content	Not Selected	*Selected* *Not Selected*

		When Not Selected, explicit music or video content purchased from the iTunes Store is hidden. Explicit content is marked as such by content providers, such as record labels, when sold through the iTunes Store.
Allow Screen Capture	Selected	*Selected* *Not Selected* When Not Selected, users are unable to save a screenshot of the display.
Allow Assistant	Selected	*Selected* *Not Selected* When Not Selected, disables Siri.
Force iTunes Password	Selected	*Selected* *Not Selected* When Selected, forces user to enter their iTunes password for each transaction.
Allow Untrusted HTTPS Certs	Not Selected	*Selected* *Not Selected* When Not Selected, automatically rejects untrusted HTTPS certificates without prompting the user.
Allow iCloud Backup	Not Selected	*Selected* *Not Selected* When Selected, the device is permitted to back up to and restore from iCloud.
Allow iCloud Document Sync and Key-Value Sync	Not Selected	*Selected* *Not Selected* When Selected, the device allows document synchronization to iCloud and allows sync data between apps running on different iOS and OS X devices to iCloud.
Allow iCloud Photo Stream	Not Selected	*Selected* *Not Selected* When Selected, iCloud automatically pushes (via Wi-Fi) a copy of any photo taken on or imported to an iOS device, to the user's other iOS devices, iPhoto or Aperture on a Mac, Pictures Library on a PC, and Apple TV.
Web Clip URL		The URL that the Web Clip should open when clicked. The URL must begin with HTTP or HTTPS or it will not work.
Web Clip Label		*Label must not exceed 32 characters.* The name of the Web Clip as displayed on the Home screen.
Allow Web Clip Removal	Not Selected	*Selected* *Not Selected* *If Not Selected, the user cannot remove the Web Clip, but it will be removed if the profile is deleted.*
See basic settings		

Mac Encryption

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Dell Volume Encryption		
Dell Volume Encryption	On	*On* *Off* Toggle ON to enable Dell Volume Encryption policies. If this policy is toggled to OFF, no Dell Volume Encryption takes place, regardless of other policies.
Encrypt Using FileVault for Mac	Off	*On* *Off* Toggle ON to enable FileVault to encrypt all volumes including System Volumes and Fusion Drives.
Workstation Scan Priority	Normal	*Highest, High, Normal, Low, Lowest* Specifies the relative priority of encrypted folder scanning. High and Highest prioritize scanning speed over computer responsiveness, Low and Lowest prioritize computer responsiveness over scanning speed and favor other resource-intensive activities, and Normal balances the two. The Shield checks for a changed Workstation Scan Priority before processing the next file. NOTE: This policy applies to Dell Encryption, not FileVault encryption.
See advanced settings		

Policy	Default Setting	Description
Mac Global Settings		
Volumes Targeted for Encryption	All Fixed Volumes	*System Volume Only* *All Fixed Volumes* The System Volume Only setting secures only the currently running system volume.
Policy Proxy Connections		*String - maximum of 1500 characters* List fully qualified Policy Proxy hostnames, or IP addresses, separated by carriage returns. More... Once the Shield finds a valid entry, the remainder of the entries are ignored. Entries are processed in the following order: 1. GKConnections Override (this registry entry overrides all other entries) 2. GKConnections (this registry entry is set automatically by the Shield, based on the this policy) 3. GK This policy works in conjunction with the Policy Proxy Polling Interval policy. You cannot specify ports in this policy. The Shield communicates with Policy Proxies using the GKPORT specified during Shield installation (the default is 8000).

		Inherited values for this policy accumulate. In order for the Shield to connect to a Policy Proxy specified in this policy, it must be in the same group as the Policy Proxy specified during Shield installation. Because the Shield supports up to 255 users per endpoint, this policy is available only at the Enterprise Policies level.
Policy Proxy Polling Interval	360	*1-1440 minutes* The interval that the Shield attempts to poll Policy Proxy for policy updates, and send inventory information to Policy Proxy. Setting the Policy Proxy Polling Interval below 60 minutes is not recommended, due to potential degradation of performance. The Shield also attempts to poll Policy Proxy each time a user logs on.
Force Restart on Policy Updates	Selected	If this policy is set to Selected, the Shield will force a computer restart after the specified delay upon receiving a policy update requiring a restart. The delay is specified by the *Length of Each Restart Delay* and *Number of Restart Delays Allowed* policies. If this policy is set to Not Selected, the Shield will neither force nor prompt for a restart. The policy requiring the restart will take effect the next time the user restarts their computer.
Length of Each Restart Delay	15	If *Force Restart on Policy Updates* is set to Selected, this value is the number of minutes the user can delay the restart before another restart prompt is displayed. If *Force Restart on Policy Updates* is set to Not Selected, this policy is ignored. More... The Shield displays the restart prompt for five minutes each time. If the user does not respond to the prompt, the dialog is dismissed and next delay begins. If the five-minute timer expires and no restart delays remain, the computer will restart immediately. **Tip:** Calculate the maximum possible delay as follows (a maximum delay would involve the user responding to each delay prompt immediately prior to the 5-minute mark): (Number of Reboot Delays Allowed x Length of Each Reboot Delay) + (5 minutes x [Number of Reboot Delays Allowed + 1]).
Number of Restart Delays Allowed	3	If *Force Restart on Policy Update* is set to Selected, this value is the number of times the user can delay the restart. If this policy is set to "0", the Shield will prompt the user to restart immediately and will force the restart if the user does not acknowledge the prompt within five minutes. If *Force Restart on Policy Updates* is set to Not Selected, this policy is ignored.

Advanced Mac Encryption

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Dell Volume Encryption		
Dell Volume Encryption	On	*On* *Off* Toggle ON to enable Dell Volume Encryption policies. If this policy is toggled to OFF, no Dell Volume Encryption takes place, regardless of other policies.
Encryption Algorithm	AES256	*AES 256, AES 128* Encryption algorithm used to encrypt data at the endpoint (all users) level. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256. NOTE: This policy applies to Dell Encryption, not FileVault encryption.
See basic settings		

Port Control

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Windows Port Control		
Port Control System	Disabled	Enable or Disable all Port Control System policies. If this policy is set to Disable, no Port Control System policies are applied, regardless of other Port Control System policies. **Note**: PCS policies require a reboot before the policy takes effect.
Port: Express Card Slot	Enabled	Enable, Disable, or Bypass ports exposed through the Express Card Slot.
Port: USB	Enabled	Enable, Disable, or Bypass port access to external USB ports. **Note:** USB port-level blocking and HID class-level blocking is **only** honored if we can identify the computer chassis as a laptop/notebook form-factor. We rely on the computer's BIOS for the identification of the chassis.
Port: eSATA	Enabled	Enable, Disable, or Bypass port access to external SATA ports.
See advanced settings		
Windows Device Control		
Class: Storage	Enabled	PARENT to the next 3 policies. Set this policy to Enabled to use the next 3 Subclass Storage

		polices. Setting this policy to Disabled disables all 3 Subclass Storage policies - no matter what their value.
Class: Windows Portable Device (WPD)	Disabled	PARENT to the next policy. Set this policy to Enabled to use the Subclass Windows Portable Device (WPD): Storage policy. Setting this policy to Disabled disables the Subclass Windows Portable Device (WPD): Storage policy - no matter what its value. Control access to all Windows Portable Devices.
Subclass Windows Portable Device (WPD): Storage	Full Access	CHILD of Class: Windows Portable Device (WPD) . Class: Windows Portable Device (WPD) must be set to Enabled to use this policy. Full Access: Port does not have read/write data restrictions applied. Read Only: Allows read capability. Write data is disabled. Blocked: Port is blocked from read/write capability.
Class: Human Interface Device (HID)	Enabled	Control access to all Human Interface Devices (keyboards, mice). **Note:** USB port-level blocking and HID class-level blocking is **only** honored if we can identify the computer chassis as a laptop/notebook form-factor. We rely on the computer's BIOS for the identification of the chassis.
See advanced settings		

Advanced Port Control

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Windows Port Control		
Subclass Storage: External Drive Control	Full Access	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. This policy interacts with the Removable Storage - EMS Access to unShielded Media policy. If you intend to have Full Access to media, also set this policy to Full Access to ensure that the media is not set to read only and the port is not blocked. Full Access: External Drive port does not have read/write data restrictions applied Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Subclass Storage: Optical Drive Control	UDF Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. Full Access: Optical Drive port does not have

		read/write data restrictions applied UDF Only: Blocks all data writes that are not in the UDF format (CD/DVD burning, ISO burning). Read data is enabled. Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy. Universal Disk Format (UDF) is an implementation of the specification known as ISO/IEC 13346 and ECMA-167 and is an open vendor-neutral file system for computer data storage for a broad range of media. To encrypt data written to CD/DVD media: Set EMS Encrypt External Media = True, EMS Exclude CD/DVD Encryption = False, and Storage Class: Optical Drive Control = UDF Only.
Subclass Storage: Floppy Drive Control	Read Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. Full Access: Floppy Drive port does not have read/write data restrictions applied Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Port: PCMCIA	Enabled	Enable, Disable, or Bypass port access to PCMCIA ports.
Port: Firewire (1394)	Enabled	Enable, Disable, or Bypass port access to external Firewire (1394) ports.
Port: SD	Enabled	Enable, Disable, or Bypass port access to SD card ports.
Port: Memory Transfer Device (MTD)	Enabled	Enable, Disable, or Bypass access to Memory Transfer Device (MTD) ports.
See basic settings		
Windows Device Control		
Class: Other	Enabled	Control access to all devices not covered by other Classes.
See basic settings		

Global Settings

Global Settings policies are available at the Enterprise, Endpoint Groups, and Endpoints levels. All Global Settings policies are endpoint-based, meaning the policies follow the endpoint, not the user.

Audit Control policies are available at the Enterprise, Endpoint Groups, Endpoints, User Groups, and Users levels.

Policy descriptions also display in tooltips in the Remote Management Console.

Policy	Default	Description

Settings		
Device Lease Period	30	Defines the period of inactivity (in days) before a Shielded endpoint is automatically removed from the list of managed clients. The inactivity period is based on the number of days since the EE Server or VE Server last received inventory information from the Shielded endpoint. Once removed, the endpoint will no longer be included in reports, statistics, and other administrative views. If the Shielded endpoint communicates with the EE Server or VE Server after the inactivity period has expired, the endpoint will be returned to the list of actively-managed clients. **Note:** The EE Server or VE Server will always keep encryption keys in escrow, even for removed endpoints. This ensures recoverability of encrypted data through various workflows, such as Shield re-activation and forensic analysis.
Enable In-App Feedback	Not selected	When selected, an end user can submit feedback and satisfaction ratings to Dell via a link within the client application to a web form.
Server Polling Interval	360 minutes	*1-1440 minutes* How often in minutes the SED client attempts to contact the DDP Server for updates.
DDP Auto Updates		
Enable Software Auto Updates	Not Selected	*Selected* *Not Selected* Selected enables the client update agent to automatically check for updates to Dell Data Protection software. If this policy is not selected, no DDP Auto Updates take place, regardless of other policies. If this policy is set, the On Premise Update Staging Location must have a network location in its value.
On Premise Update Staging Location	String	*String* Network location (UNC) where DDP Server stages Dell Data Protection update packages. If a network location is not specified in this policy, the Enable Software Auto Updates policy should not be published.
Update Check Period	10080	*1-43200 minutes (30 days)* The period in minutes between checks for updates.
Audit Control		
Secure Lifecycle Audit Data Enabled	Selected	*Selected* *Not Selected* Selected enables Audit Control policies. If this policy is not selected, no Audit Control takes place, regardless of other policies. It also enables the collection of audit data from Secure Lifecycle clients.

Secure Lifecycle Geo Location Audit Data	Selected	*Selected* *Not Selected* Selected includes geo tracking location data in audit data.
Client Retention Period	30 days	*0-365 days. 30 days default.* Specifies the number of days that the client will hold on to audit data without transmission.
Mobile Audit Control		
Secure Lifecycle Audit Data Enabled	Selected	*Selected* *Not Selected* Selected enables Audit Control policies. If this policy is not selected, no Audit Control takes place, regardless of other policies. It also enables the collection of audit data from Secure Lifecycle clients.
Secure Lifecycle Geo Location Audit Data	Selected	*Selected* *Not Selected* Selected includes geo tracking location data in audit data.

Referenced Topics

Advanced Threat Events tab fields and filters

The Advanced Threat Events tab displays information about events for the entire enterprise based on information available in the Dell Data Protection Server.

The tab displays if the Advanced Threat Prevention service is provisioned and licenses are available.

To access the Enterprise Advanced Threats tab, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threat Events** tab.

Use the following filters to select content to display on the Advanced Threat Events tab:

Type - Threat Found, Threat Blocked, Threat Terminated, Memory Violation Blocked, Memory Violation Terminated, Memory Violation (Detected), Threat Removed, Threat Quarantined, Threat Waived, Threat Changed, Protection Status Changed.

Severity - Severity level of the event: Critical, Major, Minor, Warning, or Informational.

Timeframe (in days) - 1, 7, 14, 30, 60, 90

Columns - Allows you to select the following additional columns to display:

Host Name - The fully qualified name of the computer

Data - Details about the event

Created - Date and time that the event was captured

Machine Name - Name of the computer on which the threat event was detected

Path - Path to the file in which the threat was detected

Sha256 - The file's 256-character Secure Hash Algorithm can be compared with an expected result to indicate whether the file has been tampered with.

Score - The threat file's score, indicating the confidence level that the file is malware. The higher the number, the greater the confidence.

Temporarily Block Activations

The *Allow Activations* policy is set to Selected/On to automatically allow Enterprise Edition for Windows activations, by default. To stagger activations, or to prevent activations during initial DDP Server setup or maintenance interruptions, activations can be blocked at the Enterprise, Domain, User Group, or User levels. Other platforms do not require this policy to be changed.

To temporarily block activations, follow these steps:

1. As a Dell Administrator, log in to the Remote Management Console.
2. In the left pane, click **Populations > Enterprise** or **Domains** or **User Groups** or **Users**.
3. If applicable, search or select a Domain, User Group, or User Name from the list that displays, then click the **Security Policies** tab.
4. Under Windows Encryption, click **Policy-Based Encryption**.
5. Click **Show advanced settings**.
6. Clear the check box next to Allow Activations and then click **Save**.
7. In the left pane, click **Management > Commit**.

8. Enter a comment for the change and then click **Commit Policies**.

Cloud Profile Update

The DDP Server automatically checks for updated profiles of Cloud storage providers supported with Dell Data Protection | Cloud Edition. When available, updated profiles are sent to Cloud Edition clients after the administrator commits policy changes. When the Pending Policy Changes value in the Remote Management Console is automatically incremented although an administrator has not modified policy values, at least one updated profile is available.

The polling interval for Cloud storage provider profile updates is daily at 12:30 a.m.

Set the Server Connection Retry Interval

To set the interval at which the SED client will attempt to contact the VE Server when the Server is unavailable to communicate with the SED client, set the following value on the client computer:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DellMgmtAgent\Parameters

CommErrorSleepSecs (DWORD Value)=300

This value is the number of seconds the SED client waits to attempt to contact the Server if the Server is unavailable to communicate with the SED client. The default is 300 seconds (5 minutes).

Advanced Threat Prevention Classifications

The Advanced Threat Prevention Classifications pane shows a heat map of threats. The color indicates the priority classification of the threat. The size of the box indicates the relative number of endpoints that have a particular threat. This classification helps administrators determine which threats and devices to address first. Click a threat to view threat and device details.

Threat classifications include the following:

Malware

- Trojan
- Downloader

Potentially Unwanted Programs (PUP)

- Adware
- Hacking Tool
- Portable Application

Remove System Data Encryption (SDE)

To completely decrypt SDE encrypted files, apply the following policies:

SDE Encryption Enabled = False

Encrypt Windows Paging File = False

Secure Windows Credentials = False

Designate a Threat Protection Signature Update Server

Both an HTTP and FTP signature update server are pre-configured with your DDP Server installation. You can also, optionally, designate an internal signature update server or servers within your network.

Designating a signature update server within your network allows client computers to obtain signature updates without accessing the Internet. Rather than individual clients contacting an external update server,

they contact your internal update server, which maintains current signatures through contact with the external signature update server.

To designate a signature update server, follow these steps:

1. As an administrator on the server that will be the internal update server, run the appropriate command:

   VSSETUP_86.EXE /SetRelayServerEnable=1
   or
   VSSETUP_64.EXE /SetRelayServerEnable=1

2. Restart the internal update server.
3. In the DDP Server Remote Management Console, navigate to **Populations > Enterprise** and select **Malware Protection** on the Security Policies tab.
4. In Malware Protection advanced settings, click **Source Sites for Updates**.
5. Click **Add**.
6. Enter a Name for the internal update server.
7. To enable connections to the internal update server, select **Enabled**. To enable later, clear the Enabled check box.
8. In the Order field, set the sequence in which clients will contact the internal update server in relation to other update servers. Dell recommends that you set the Order for internal update servers to precede the Order for external update servers.
9. Select the type of repository or path to the update server: HTTP repository, FTP repository, UNC path, or Local path.
10. Enter the URL or path to the internal update server.
11. Complete the remaining fields in the form, and click **OK**.
12. Repeat these steps to designate additional internal update servers.

To revert an internal update server to non-update server status, enter the appropriate command:

VSSETUP_86.EXE /SetRelayServerEnable=0
or
VSSETUP_64.EXE /SetRelayServerEnable=0

Disconnected Mode Policy Examples

Examples for Global Allow, Quarantine List, and Safe List policies are shown below.

Global Allow policy example

```
<?xml version="1.0" encoding="utf-8"?>

<disconnected_policy>

  <policy_name>Default</policy_name>

  <policy_company>Acme</policy_company>

  <policy_company_id>uxSYabW9P2nMbGLzuqJhvT9Y</policy_company_id>

  <policy_utctimestamp>Date(-62135596800000+0000)</policy_utctimestamp>


  <filetype_actions>
```

```
    <suspicious_files file_type="executable" actions="7" />
    <threat_files file_type="executable" actions="7" />
  </filetype_actions>
  <memoryviolation_actions>
    <memory_violation violation_type="stackpivot" action="Alert" />
    <memory_violation violation_type="stackprotect" action="Block" />
    <memory_violation violation_type="stackpivot" action="Terminate" />
    <memory_violation violation_type="overwritecode" action="None" />
    <memory_violation violation_type="outofprocessallocation" action="Scuba" />
    <memory_violation violation_type="outofprocessmap" action="Alert" />
    <memory_violation violation_type="outofprocesswrite" action="Block" />
    <memory_violation violation_type="outofprocesswritepe" action="Terminate" />
    <memory_violation violation_type="outofprocessoverwritecode" action="None" />
    <memory_violation violation_type="outofprocessunmapmemory" action="Alert" />
    <memory_violation violation_type="outofprocesscreatethread" action="Alert" />
    <memory_violation violation_type="outofprocessapc" action="Alert" />
    <memory_violation violation_type="lsassread" action="Alert" />
    <memory_exclusion_list>
      <path>temp\files\exe1.exe</path>
      <path>stuff\folder\exe2.exe</path>
    </memory_exclusion_list>
  </memoryviolation_actions>

  <appcontrol>
<changewindow_enabled>0</changewindow_enabled>
<lockdown lockdown_type="executionfromexternaldrives" action="deny" />
<lockdown lockdown_type="pechange" action="deny" />
  </appcontrol>

  <policy>
    <option name="auto_blocking" value="0" />
    <option name="auto_uploading" value="1" />
    <option name="threat_report_limit" value="500" />
    <option name="low_confidence_threshold" value="-600" />
```

```
    <option name="full_disc_scan" value="0" />
    <option name="watch_for_new_files" value="0" />
    <option name="memory_exploit_detection" value="0" />
    <option name="trust_files_in_scan_exception_list" value="0" />
    <scan_exception_list>
      <path>C:\temp</path>
      <path>C:\stuff</path>
    </scan_exception_list>
  </policy>


  <exclusion_list>
<checksum>3fdc391ef0e200af3e4c206e785e1de0</checksum>
<error_rate>1E-05</error_rate>
<size>509</size>
<exclusionlisthash>XjxtEUkQvOFIxTZof+f6Jb149fhxFbOHUzc3S/5Hif6zqeiZrvOaM9QvGruM1un
/uiOGeMwiNB3lLCBD9PtwbgaYUpiz8Ne88wOmKhnerXo5TJRy+4HzPWDotDXSz+d5AHP74zbbHfH7m47KG
9bFAsPa4KNhFLqSOD3g/AI7ZCWLL/IOFyWcFMTLLkeLRycDIyZpzf8QDskQVsAt8Ub1h2UGY4BGgKwCQfY
z9J/yJWuF1XGy9A7rMAHzYdqh0B5s4Y2iB2jrdlHuGSxtNPu9gTuMldfxEBgcXq7XUWxuJUTbo1Fv2jsCH
Ypd/hg1d+3SkNbI9qykHmK9gnCH2r7IHPlK5zvR9Y1eVxTshl6JoxQMDD+M0VkrL3tHqlS1mJi9NI979dd
8GiYnAqtkFsMg+FhOT2PkVkBSzLgkCF+rHWoeDdo+MVX79X9XjJqT1kRwSM2p30IPi4g+NH6X/YPs6Fz7w
b95jMx6ILX/L7pHGOdM0fSeSfwO/XIOyk5FhogOJqY86SkJs437CS7+pW+nz82lXuFqNP4pZaG2xf2iepT
Do89dAMQJGWEoCnlR1z0lPI8782TLLRm5OKytCrhUMut+P28K8LuPOTdTgSCnf2uVrcecQTz/BZOyqX5B6
vy7g1P2H0HmEV1uVfhWMjABRoSK+aI5VXd5qNRaY4zfn0w5Z6LOiIYDtvESgkLuw0bzHrsf5ADKEkwv9Ig
09DxhDYzLdJlZp/DNMsnJGtvntZ/cezXbGtzJuGSFq7lem5L00cavDQ3vRo3GlfettwN2CT9Z2MssLJhwe
TS8utTabMBFfIsM8dx3sdN26lAsx9rDyR7fLn4BJ2WnMXv8FRoTZJ3oXxOQFUsCM1Rnhw7ottTaLEiPf7R
d4jdxbsErBnK1CYfyYAePaD6ycle1h6bYMyWxUUD2ZqyVBiu3La/4MKalmI9V2IzEsYObxp9RRXkY3HcTz
PHk5e8Zp+YbPQAr88RNpC277sCRiBWYlb00OH/hx5yc61rae/pzrGjusBT53KaiG6mlLpvRYrqDQ7fW0cp
Fa2eC1czQ+o8LN/gNVT7FtFhKgd8pnQW00CidxeSULfzRk6TS9rLCgXBDtRyK1fRrkkOCrHZU/YvC2BXaW
VAx60giDsKxBUYQsgXQbaGwPG279ChdwnjWlVMWCqdvOoGEBMDApjbkqqkwgHJpkCJIF4zOTChpVfM17Pf
Kw/uycxoqMzpdb+AOQnTX+MzRm9BkTN9T9aFh+CRleDqc/xhP59RBUUT3GAP+rk3789EQXdUVp9tC7hmXT
jjg85jWSEe6IcGE5RY7NQXdXZGJScLmyiUVq+0lZjO3xkAUZ5eq0lUJo5KYaneGeYQFe7VzSmyzPMao6YP
fpnRxOuLvMANIhKf9q0zL1IPgJfVTwU9AHoLcUE2ztor3bdrRnZ3+e5HqZkEpHtMGruMjiP4ZLmA7tJNhj
63KspEEKJfCSkXGw74+cepc6J5ThPJWNd33IZmgcwqE27/sXxsb5xzYFgfBUZmr12KnU7JMbg95bZTatxN
8PtIQS2NTdnyXK/f7j7i74FQZXNksONgfyEelFDOTlqlI7SLKw1uffUEk2QGv54bUQANLhbAvLbLR1b6v3
52rw3ANgECdQbqXcvKE/jYKUzHSW3qqIPcPnrguYVoJuydKNiJVmoaqPLJ3LC6m7+PdGBuqEdVo+MK/PMJ
dTVb47zW1RSYX0t9SJ/4xWEBybUMsHXRZTux6nlca5qCxHDiHb50I677Bi+Y0YLddza7iA7z4mPTRmqEX6
jEo5ZorZ4kcTIbNHj77p4kzouYDg3s+o+9KvoxcI0iw8MAOtKrRVZTN24jjSUAETJ66rb3JdzcfJJeb7w4
QVOUckL2kfyaS4ASp80fzpOxJl3hSLw2bnR2n0WukMhj3kWvY+GeXDBfGzHfDGeLV0pF/+hQTPR/XWuOSs
nH1wUeJEXS3al6lyhcRCS7XbVPt+85NYGuk2ntf6zmST/v6a3E2exxerUDAmHfCK/0VQKrqlYec1hkH1Sb
vCQ==</exclusionlisthash>
<exclusionlisthash_secondary>rT7UrQItY0RfpDEVEDwSXdiGq3fUgEJ9OpQMEUEacRRy1OFAS2W51
m9f3hbzrOA7lvoiKZLy9/h0koV2d5vyIj+xC275ucwOvqhKpKPQH8mfcD3vT498DuteV0i1Tmzq/WFLlhd
qK75CF8ys17UVZZabbExD2s9W49gUft5W9UozOW5K1mC9V5E79YCf83s0wra6qrZqENI98WNpD9UbyN1UQ
N72g5mQligT8ViuoEMagB6JQaTI8CgCLe6NK8DFvuykGOYVtLfKCtmCqt0eg1Im0oFxLiVrouovcCdNpfz
WOXflQSEVEbVeqfPxEuTrHRWZBzFxOYLrT86tSsH8ll+XC3uFjN7uI/HB8daE3saFPmIAZUC9sq3rMU8Ro
y9+iRw3lebL0P51RTSHxC9Mz8xr85gt3m4MyqSO8mNNBxIzwxeUCishz8A17VB5ai/R5Hy17zMTwIXU2x5
Pcnpd2UqyeLQbXWpnkeRpl7f0rdwBM0FDCpZqExnFYQswvOb8kPnruC0/iIgx/zNSFeuFlT8dSbCZNvgh0
7Ohh4sl0v9U9Ir7nBe9ZreDgdZMdZ1wCTqXBk/yxJB74+95uRYasNznVAG2yD1IIwtWNvygHrmw5sZgk09
7K2quTOHjDp0thnhaSGdOK5pF2TFEm8zegjewP65pR5Jdys1lvKquzbx3NZ3LtR0XyVIMBzcF9NDLP8v4U
```

kwaKg9EL73o2yPjqgDVwt9AhXlh4VdSEv5M+JRfo+EguQB9I/DleTbWUGAEMMn1cADZj9yY0fB/SEsDVAW
iLbiP/PYcUXz6g4Cv2uF9jk2Tn7KEbvuFWfIlnq2+z/qUNUH0Uj44jgqswv6G/q5VfbW5dM0MtTGmZd5jE
8PNy3R/uygm4ZoTvnOUu93FIC8dpmVjlsyii9XhM8XN/YX9om5wXAJ9CuTgRWbuUK4lvW9ROiEokQRFu76
Y8OTEvx6kpCEFgAVZlhbfe0fmGo+CD1wI+dg0tze2BN7jk/ItXgiPKp/+/fLoH3HR8mZSWX8bW8uRpBgqo
3xq57tpP9JxcyPQetG9fungtlBjzAd53Frro8XYXbzOd71honuEsFYv4T03ojU8w7a9EBbJ7SvRfDDi27m
T/YmZNr3Y39FRlT7qQ44Ng5cjgp9etwVIego1xpfBXECF2PxOuA/S7u06QakK+Ngkl+bFw5MBbG/NLHALb
kV+jbL6NKmUMWHYO4ruPzSoUYE84f9V0WFBZpWMxnx/j/ZZZMwv8+p8kF3dAR9SjK38coPVCnLCJ8uDJPo
LDXS79u+pfQbsqgdPL+dwDeQAlIhHzjpNlpM5UeHYGUiwHFbOr8GTdq2GSEacfW510uv1dNeIk1wo2a2zl
cBMH0V57f3/aVi0ZDtDKL5N1TO81xSPa6/hck4RGjIRInr632OmMh/dtx+40q7c8269KQSnXvpaVS8kyf2
GvLMHCWurEg+NyCB0N5+UonnC+0i9KialfIByLBuPCNQppds0mkjhbCmJqPtCxgLaJVYop2qddzsry9PFW
97tDEJcUilrQc7a5NTFWExc4a8LLpT+dtXNxEvZAg2VSsffawcZ894um6Gw55IBRmLHeyso0Y3zBWOGq5G
3KA31fFyk9OAfxgdwIkHA6jB9nSRzi/ea7HSRUHNRfp26Bc0/c4K/dDDA23NdTOT14AIuU+3d822EH9l/M
cuVa1FAK1gzPwcOrL8lT3x9vrRJwUOCw0EamqgAzQNrE3tIbPsVuOhevtZhjm+NDzRZcxuk4Tu38Tojo5H
2xCucaEWdYxz0CKzCch/vH8FIpr0J9s1Jbl0Ac1m+frnuUZImePkSXdmvkX4SpD4hoCy0L1F4eVGMniFfj
fCIhQyBwphCoqGKo1wP7WOQA/9fDZc7z0vka2u6Uz3Sy/ekJHZ0yI7OzP4nAzTq7bnBQR2KCXgLaUP2mq0
VjyFS9zPmsxloHU8fjs2kDP4jH2e+qXSAJwQ0112Y+9mEvdktSkAJq24c5HSO4F80p1Ae8YhpuAECKXqCC
+P0YiksNToTGA==</exclusionlisthash_secondary>

  </exclusion_list>

</disconnected_policy>

Quarantine List and Safe List policy example

The following sample Quarantine List and Safe List policy can be set at the Enterprise- and Endpoint-levels:

```
{code}

"airgap_policy": {

"file_lists" : [

{

"file_list_type": "quarantine",

"files": ["0A5F695900F1FC75070BB8B7C7A55B5BCFAAD6FE",

"525E7A55B5BCB6B16F25B5DD6CE11DFC6DD0B4E6"]

},

{

"file_list_type": "safe",

"files": ["0A5F695900F1FC75070BB8B7C7A55B5BCFAAD6FE",

"525E7A55B5BCB6B16F25B5DD6CE11DFC6DD0B4E6"]

},

{

"file_list_type": "quarantine_command",

"files": ["0A5F695900F1FC75070BB8B7C7A55B5BCFAAD6FE",

"525E7A55B5BCB6B16F25B5DD6CE11DFC6DD0B4E6"]

},

{
```

```
"file_list_type": "waive_command",
"files": ["0A5F695900F1FC75070BB8B7C7A55B5BCFAAD6FE",
"525E7A55B5BCB6B16F25B5DD6CE11DFC6DD0B4E6"]
}
],
"exclusion_list" : {
"checksum": "3fdc391ef0e200af3e4c206e785e1de0",
"error_rate": 1E-05,
"exclusionlisthash": "Xj..CQ==",
"exclusionlisthash_secondary": "rT..A==",
"size": 0
}
},
{code}
```


Enable Compatibility Mode for Memory Protection

Compatibility Mode allows applications to run on the client computer while Memory Protection or Memory Protection and Script Control policies are enabled. Compatibility Mode is enabled through a registry setting or a command on the client computer. Compatibility Mode does not apply to Mac clients.

To enable Compatibility Mode with a registry setting:

1. In the Remote Management Console, disable the Memory Protection Enabled policy. If the Script Control policy is enabled, disable it.
2. Save the policy changes, and Commit Policies.
3. Using the Registry Editor on the client computer, go to HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
4. Right-click **Desktop**, click **Permissions**, then take ownership and grant yourself Full Control.
5. Right-click **Desktop**, then select **New > Binary Value**.
6. For the name, type *CompatibilityMode*.
7. Open the registry setting and change the value to *01*.
8. Click **OK**, then close Registry Editor.
9. In the Remote Management Console, enable the Memory Protection Enabled policy. If the Script Control policy was enabled, enable it.
10. Save the policy changes, and Commit Policies.

To add the registry setting with a command:

1. In the Remote Management Console, disable the Memory Protection Enabled policy. If the Script Control policy is enabled, disable it.
2. Save the policy changes, and Commit Policies.
3. Select one command line option to run on the client computer:

   (For one computer) Psexec:
   psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v CompatibilityMode /t REG_BINARY /d 01

   (For multiple computers) Invoke-Command cmdlet:
   $servers = "testComp1","testComp2","textComp3"
   $credential = Get-Credential -Credential {UserName}\administrator
   Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item -Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value 01}
4. In the Remote Management Console, enable the Memory Protection Enabled policy. If the Script Control policy was enabled, enable it.
5. Save the policy changes, and Commit Policies.

Encryption Rules

Important: *Before you begin, you must understand directory protection, as well as when and how to override directories and file types. If you do not completely understand the information included in this section, as well as the encryption settings that currently exist on your environment, do not attempt to override protected directories.*

Do not encrypt files with the extension tmp. Encrypting .tmp files may result in an unbootable computer and/or require reformatting drives.

Protected Directories

The Shield has several directories that are, by default, protected from encryption. The level of protection varies from folder to folder. If a folder is protected, then the only way to encrypt data within that directory is to use the override modifier described in Modifiers – What they are and what they do.

There are four levels (categories) of protection that directories and files can have: 0, 1, 2, and 3. Category 3 is the most protected level.

The following directories have Category 0 exclusions (including subfolders unless specified):

NOTE: All exclusions may not apply in all environments.

%SYSTEMDRIVE% (no subfolders)

Profile directory ("C:\Documents and Settings" in XP and "C:\Users" in Win7)

%SYSTEMROOT%

Default user profile ("C:\Documents and Settings\Default User" in XP and "C:\Users\Default" in Win7)

CSIDL_PROGRAM_FILES

CSIDL_PROGRAM_FILESX86

%SYSTEMROOT%\Driver Cache\i386

<Windows File Protection> ([HKLM\Software\Microsoft\Windows NT\CurrentVersion] SourcePath:REG_SZ)

%SYSTEMDRIVE%\I386

CSIDL_COMMON_APPDATA

%SYSTEMROOT%\temp\WgaErrLog.txt

F#:\boot

CSIDL_COMMON_APPDATA\Credant

CSIDL_COMMON_APPDATA\Dell\Dell Data Protection

CSIDL_COMMON_APPDATA\CmgAdmin.log

F#:\bootmgr

%SYSTEMROOT%\SysWOW64

CSIDL_COMMON_APPDATA\Microsoft\Windows\Caches

CSIDL_PROGRAM_FILES\Symantec

CSIDL_PROGRAM_FILESX86\Symantec

CSIDL_PROGRAM_FILES_COMMON\Symantec

CSIDL_PROGRAM_FILES_COMMONX86\Symantec

CSIDL_COMMON_APPDATA\Symantec

CSIDL_PROGRAM_FILES\McAfee

CSIDL_PROGRAM_FILESX86\McAfee

CSIDL_PROGRAM_FILES_COMMON\McAfee

CSIDL_PROGRAM_FILES_COMMONX86\McAfee

CSIDL_COMMON_APPDATA\McAfee

CSIDL_PROGRAM_FILES\Trend Micro

CSIDL_PROGRAM_FILESX86\Trend Micro

CSIDL_COMMON_APPDATA\Trend Micro

CSIDL_PROGRAM_FILES\Microsoft Security Client

CSIDL_PROGRAM_FILESX86\Microsoft Security Client

CSIDL_COMMON_APPDATA\Microsoft Security Client

CSIDL_PROGRAM_FILES\Sophos

CSIDL_PROGRAM_FILESX86\Sophos

CSIDL_COMMON_APPDATA\Sophos

CSIDL_PROGRAM_FILES\Kaspersky

CSIDL_PROGRAM_FILESX86\Kaspersky

CSIDL_COMMON_APPDATA\Kaspersky

CSIDL_PROGRAM_FILES\Kaspersky Lab

CSIDL_PROGRAM_FILESX86\Kaspersky Lab

CSIDL_COMMON_APPDATA\Kaspersky Lab

%SYSTEMROOT%\Config.MSI

%SYSTEMROOT%\$Windows.~BT

F#:\.xen

%ProgramFiles%\Dell\Dell Data Protection\Encryption\Local Console.exe

%SystemDrive%\Program Files\WindowsApps

%SystemRoot%\SystemApps

%SystemRoot%\InfusedApps

The following directories have Category 1 exclusions:

%SYSTEMROOT%\System32\.tmp

The following directories have Category 2 exclusions:

%SYSTEMROOT%\System32

F#:\System Volume Information

%SYSTEMROOT%\SoftwareDistribution

%SYSTEMROOT%\Security

The following directories have Category 3 exclusions:

<Shield install directory>\.dll.exe.sys.mac.ddp.tbp.wip.rty.nmd.inv.config.sdf.installstate

%SYSTEMROOT%\system32\drivers\CmgHiber.dat

Modifiers - What they are and what they do

The ^ character is the “Override” command. It causes the listed policy to override protected directories. It may be followed by a “2” or a “3”, indicating the level of the override.

The **@** character is the “At” command. It will cause the listed policy to be applied at the specified folder location only (subdirectories of that folder will not be subject to that policy).

The **-** is the “Not” command. It will cause the listed policy to be an exclusion policy instead of an inclusion policy.

Using the Override Modifier

The Override Modifier can be used to allow for inclusion or exclusion in cases where there is a higher level of protection. The following are the different override levels supported:

^ Category 1 Override

^2 Category 2 Override

^3 Category 3 Override

Encrypting/Not Encrypting Extensions

In order to include or exclude filename extensions using encryption rules, use the following within your rules:

- After specifying your directory location, use a semi-colon (;) before listing your extensions.
- After specifying your directory location, you **do not need** to list a trailing backslash (\).
- The period is used as a delineator. It is not meant to be used as "dot-extension." However, you can precede the first extension with a period.
- The **Override** command (^) can be used with extensions.
- The **At** command (@)can be used with extensions.
- The **Not** command (-) can be used with extensions.
- You can make any combination of the modifiers with an extension inclusion or exclusion.

Examples of extension inclusions/exclusion

C:\;doc.xls.ppt.docx.xlsx.pptx

> **What this does:** On the C: drive, this encrypts all doc, docx, xls, xlsx, ppt, and pptx files that do not exist within any protected directory.

^C:\;txt

> **What this does:** On the C: drive, this encrypts all txt files that are not in a directory that has protection of Category 1 or better.

-C:\;bat.exe.dll

> **What this does:** On the C: drive, this causes all files with the extension bat, exe, and dll to not be encrypted.

Encrypting/Not Encrypting Directories

In order to include or exclude directories using encryption rules, use the following within your rules:

- After specifying your directory location, you **do not need** to list a trailing backslash (\).
- If you list a directory for inclusion, every file contained within that directory will be encrypted.
- The **Override** command (^) can be used with folders only when specifying an exclusion policy.
- The **At** command (@) can be used with folders.
- The **Not** command (-) can be used with folders.
- You can make any combination of the supported modifiers for folders. If the **Override** command (^) is used, the statement can only be an exclusion statement.

Examples of folder inclusion/exclusion

C:\CustomApplication\DataStore

> **What this does:** On the C: drive, this causes every file within the directory of \CustomApplication\DataStore to be encrypted.

-C:\Documents and Settings\All Users

> **What this does:** On the C: drive, this applies a Category 0 level of protection to the directory of \Documents and Settings\All Users.

-^2C:\CustomApplication\dll

> **What this does:** On the C: drive, this applies a Category 2 level of protection to the directory of \CustomApplication\dll.

Sub-directories and Precedence of Directives

Encryption rules may be listed in any order. If more than one rule applies to a given folder or file, then the following general rules determine which one prevails:

1. The rule with the more specific path prevails.
2. If the rules have equal paths, specified extensions prevail.
3. If the rules both specify extensions, exclusion overrides inclusion.

Example of sub-directories

C:

-C:\MyApplicationFolder

> **What this does:** (1st statement is an inclusion, 2nd statement is an exclusion) On the C: drive, encrypt all files in folders at the root level and below, **except** for files residing in the protected directories and any files residing in "MyApplicationFolder".

Example 1 of competing directives:

C:

-C:\MyApplicationFolder

^C:\;doc.xls.ppt.docx.xlsx.pptx

> **What this does:** (1st statement is an inclusion, 2nd statement is an exclusion, 3rd statement is an inclusion) On the C: drive, encrypt all files in folders at the root level and below, **except** for files residing in the protected directories and files residing in "MyApplicationFolder". However, override and encrypt files with the extension doc, docx, xls, xlsx, ppt, and pptx in the protected directories **and** in the folder "MyApplicationFolder".

Example 2 of competing directives:

C:

-C:\MyApplicationFolder

^C:\;doc.xls.ppt.docx.xlsx.pptx

-^C:\MyApplicationFolder;doc.xls.ppt.docx.xlsx.pptx

> **What this does:** (1st statement is an inclusion, 2nd statement is an exclusion, 3rd statement is an inclusion, 4th statement is an exclusion) On the drive of C:, encrypt all files in folders at the root level and below, **except** for files residing in the protected directories and files residing in "MyApplicationFolder". However, override and encrypt files with the extension doc, docx, xls, xlsx, ppt, and pptx in the protected directories, **but not** in the folder "MyApplicationFolder".

Example 3 of competing directives:

C:

-C:\MyApplicationFolder

^C:\;doc.xls.ppt.docx.xlsx.pptx

-^C:\MyApplicationFolder;doc.xls.ppt.docx.xlsx.pptx

-^C:\MyApplicationFolder\Templates

What this does: (1st statement is an inclusion, 2nd statement is an exclusion, 3rd statement is an inclusion, 4th statement is an exclusion, 5th statement is an exclusion) On the C: drive, encrypt all files in folders at the root level and below, **except** for files residing in the protected directories and files residing in "MyApplicationFolder". However, override and encrypt files with the extension doc, docx, xls, xlsx, ppt, and pptx in the protected directories, **but not** in the folder "MyApplicationFolder". Additionally, the folder "MyApplicationFolder\Templates" gains a category 2 protection causing no data to be encrypted there, since the inclusion statements are less than or equal to category 2.

Environment Variables, KNOWNFOLDERID constants, and CSIDL

Using encryption rules, you can make use of environment variables, KNOWNFOLDERID constants (Windows 7 and later), and CSIDL values (pre-Windows 7 computers) in addition to specifying your policy folder locations as absolute paths. In order to use variables in your encryption rules, follow these formatting rules:

- Before and after the use of the variable, use a percent sign (**%**).
- For environment variables, you must use "**ENV:**" preceding the variable name, all contained within the percent signs.
- For KNOWNFOLDERID constants, you must use "**FOLDERID_**" preceding the variable name. Percent signs are not used.
- For CSIDL variables, you must use "**CSIDL:**" preceding the variable name, all contained within the percent signs.
- Ensure that your variable contains a trailing backslash if you plan on appending another directory after the use of the variable.
- Variables can be used in both folder and extension inclusion or exclusion rules.

The following environment variables are supported:

All locally defined environment variables

The following KNOWNFOLDERID values are supported:

RoamingAppData

Cookies

Desktop

Favorites

InternetCache

LocalAppData

Music

Pictures

Documents

Programs

Recent

SendTo

StartMenu

Startup

Templates

The following CSIDL variables are supported:

APPDATA

COOKIES

DESKTOPDIRECTORY

FAVORITES

INTERNET_CACHE

LOCAL_APPDATA

MYMUSIC

MYPICTURES

PERSONAL

PROGRAMS

RECENT

SENDTO

STARTMENU

STARTUP

TEMPLATES

Some examples of variables used in folder and extension policy:

%ENV:SYSTEMDRIVE%\CustomApplication

What this does: This lists the folder \CustomApplication\ for encryption on the default drive where Windows is installed.

-%ENV:USERPROFILE%\Desktop

What this does: This lists the user who is logged in to have their desktop obtain a category 0 protection.

Application Data Encryption (ADE)

ADE encrypts any file written by a protected application, using a category 2 override. This means that any directory that has a category 2 protection or better, or any location that has specific extensions protected with category 2 or better, will cause ADE to not encrypt those files.

For example, ADE will not encrypt any files written into /Windows/System32 folder, because this directory has a default protection of category 2.

Example Policies for Common/User Key Encryption

The following set of encryption rules encrypts most of the drive, including standard Microsoft Office-type documents in the Documents and Settings folders. This policy set should only be used for Common Encryption (not User Encryption, EMS, or SDE). This is considered a strong policy set, and will typically require some adjustments for local conditions and requirements.

%ENV:SYSTEMDRIVE%

^%ENV:USERPROFILE%\;<insert standard office extensions here >

FOLDERID_Documents or **%CSIDL:PERSONAL%** (pre-Windows 7)

%ENV:USERPROFILE%\Desktop

^%ENV:USERPROFILE%\;mp3.mp4.mpeg.avi.wmv.wav

-^%ENV:USERPROFILE%\Desktop\;<system file extensions to exclude>

-%ENV:SYSTEMDRIVE%\;<system file extensions to exclude>

-%ENV:SYSTEMDRIVE%\config.msi

What this does:

Encrypts all of C:\, except for protected directories

Encrypts standard Microsoft Office documents across the drive, except for protected directories, although it will encrypt them in the USERPROFILE directory.

Encrypts all of My Documents

Encrypts all of the Desktop, except for any selected excluded extensions

Excludes common system files from encryption

Excludes all encryption from C:\config.msi directory, due to MSI upgrade migration issues

All paths are dynamic based on environment variables

System Data Encryption (SDE)

SDE is an intelligent file-based encryption method where the encryption key is auto-authenticated during the volume mount process. A unique SDE Key is generated for each volume that is targeted for encryption by SDE. This allows the SDE Key to be used to encrypt data that would not otherwise be possible with the Common or User Keys due to time-based availability of the keys.

Due to the difference in how the SDE Key can be used, there are several caveats to be aware of when considering use of this feature.

- The built-in exclusions covered in protected directories do not apply to SDE. By design, SDE excludes portions of the operating system that are necessary for booting and updating.
- If a file is targeted for encryption by any key other than SDE in addition to SDE, then SDE will not encrypt the file.
- All encryption rules apply when writing SDE policies.

Policies for SDE Encryption

The following is the default SDE policy. **Any changes to this policy should be considered carefully.**

The following directories have Category 1 exclusions (including subfolders unless specified):

%SystemRoot%\system32\ntoskrnl.exe

%SystemRoot%\system32\ntkrnlpa.exe

%SystemRoot%\system32\ntkrnlmp.exe

%SystemRoot%\system32\hal.dll

%SystemRoot%\system32\halacpi.dll

%SystemRoot%\system32\halmacpi.dll

%SystemRoot%\system32\winload.exe

%SystemRoot%\system32\kdcom.dll

%SystemRoot%\system32\kd.dll

%SystemRoot%\system32\kdnet.dll

%SystemRoot%\system32\kd1394.dll

%SystemRoot%\system32\kdusb.dll

%SystemRoot%\system32\kdstub.dll

%SystemRoot%\system32\mcupdate_AuthenticAMD.dll

%SystemRoot%\WinSxS*\mcupdate_AuthenticAMD.dll

%SystemRoot%\WinSxS*\mcupdate_GenuineIntel.dll

%SystemRoot%\system32\mcupdate_GenuineIntel.dll

%SystemRoot%\system32\winload.exe

%SystemRoot%\system32\PSHED.dll

%SystemRoot%\system32\BOOTVID.dll

%SystemRoot%\system32\CLFS.SYS

%SystemRoot%\system32\CI.dll

%SystemRoot%\system32\sethc.exe

%SystemRoot%\system32\utilman.exe

%SystemRoot%\system32\narrator.exe

%SystemRoot%\system32\magnify.exe

%SystemRoot%\system32\osk.exe

%SystemRoot%\system32\csrss.exe

%SystemRoot%\system32\hvloader.exe

%SystemRoot%\system32\hvix64.exe

%SystemRoot%\system32\hvax64.exe

%ProgramFiles%\Dell\Dell Data Protection\Encryption\Local Console.exe

%SystemRoot%\boot

%SystemRoot%\prefetch

%SystemRoot%\system32\Boot

%SystemRoot%\Config.MSI

%SystemRoot%\system32\drivers

%SystemDrive%\Windows.old\Windows\WinSxS

%SystemRoot%\fonts

%SystemDrive%\boot

%SystemDrive%\boot\bcd.log

%SystemDrive%\boot\bcd.log1

%SystemDrive%\boot\bcd.log2

%SystemDrive%\boot\bcd

%SystemDrive%\boot\bootstat.dat

%SystemDrive%\boot\memtest.exe

%SystemRoot%\inf

%SystemRoot%\System Volume Information

%SystemRoot%\system32\CodeIntegrity\bootcat.cache

%SystemRoot%\system32\CodeIntegrity\driver.stl

%SystemRoot%\ ;dll.exe.sys.ocx.man.cat.manifest.policy

%SystemRoot%\system32

%SystemRoot%\WinSxS

%SystemRoot%\fonts

%SystemRoot%\WinSxS\pending.xml

%SystemRoot%\WinSxS\Temp

%SystemRoot%\servicing\packages

%SystemRoot%\SoftwareDistribution\Download

%SystemDrive%\Program Files\Symantec

%SystemDrive%\Program Files (x86)\Symantec

%SystemDrive%\Program Files\Common Files\Symantec Shared

%SystemDrive%\Program Files (x86)\Common Files\Symantec Shared

%SystemDrive%\ProgramData\Symantec

%AllUsersProfile%\Symantec

%SystemDrive%\Program Files\PGP Corporation

%SystemDrive%\PGPWDE00

%SystemDrive%\PGPWDE01

%SystemDrive%\PGPWDE02

%SystemDrive%\PGPWDE03

%SystemDrive%\SafeBoot.fs

%SystemDrive%\SafeBoot.rsv

%SystemDrive%\SafeBoot.csv

%SystemDrive%\Program Files\McAfee

%SystemDrive%\Program Files\Common Files\McAfee

%SystemDrive%\Program Files\McAfee

%SystemDrive%\Program Files (x86)\Common Files\McAfee

%SystemDrive%\Program Files (x86)\McAfee

%ProgramData%\McAfee\Common Framework

%AllUsersProfile%\McAfee\Common Framework

%SystemDrive%\Program Files\Trend Micro

%SystemDrive%\Program Files (x86)\Trend Micro

%AllUsersProfile%\Trend Micro

%SystemDrive%\Program Files\Microsoft Security Client

%SystemDrive%\Program Files (x86)\Microsoft Security Client

%AllUsersProfile%\Microsoft Security Client

%SystemDrive%\Program Files\Sophos

%SystemDrive%\Program Files (x86)\Sophos

%AllUsersProfile%\Sophos

%SystemDrive%\Program Files\Kaspersky

%SystemDrive%\Program Files (x86)\Kaspersky

%AllUsersProfile%\Kaspersky

%SystemDrive%\Program Files\Kaspersky Lab

%SystemDrive%\Program Files (x86)\Kaspersky Lab

%AllUsersProfile%\Kaspersky Lab

%ProgramData%\Microsoft\Windows\Caches

%SystemDrive%\$Windows.~BT

%SystemRoot%\system32\.tmp

%SystemDrive%\Program Files\WindowsApps

%SystemRoot%\SystemApps

%SystemRoot%\InfusedApps

The following directories have Category 3 exclusions (including subfolders unless specified):

F#:\System Volume Information\MountPointManagerRemoteDatabase

F#:\.xen

%SystemRoot%\<path>\.NLS.FON (coded – path queried from the registry [HKLM\SYSTEM\CurrentControlSet

\Control\Nls\CodePage] and [HKLM\SYSTEM\CurrentControlSet\Control\Nls\Language])

%APPDATA%\Roaming\Wave Systems Corp\DocMgr

%APPDATA%\Roaming\McAfee

%APPDATA%\Credant\.log

%APPDATA%\Dell\Dell Data Protection\.log

%APPDATA%\CmgAdmin.log

The following directories have Category 3 exclusions (no subfolders):

%SystemDrive%\AUTOEXEC.BAT

%SystemDrive%\BOOT.INI

%SystemDrive%\BOOTMGR

%SystemDrive%\BOOTNXT

%SystemDrive%\BOOTSECT.BAK

%SystemDrive%\CONFIG.SYS

%SystemDrive%\IO.SYS

%SystemDrive%\MSDOS.SYS

%SystemDrive%\NTDETECT.COM

%SystemDrive%\NTLDR

%SystemDrive%\install.log

%SystemDrive%\pagefile.sys

%SystemDrive%\hiberfil.sys

%SystemDrive%\boot.bmp

%SystemDrive%\CMG3301d.DAT

%SystemDrive%\credsed.dat

%SystemDrive%\credsed.log

%SystemRoot%\bootstat.dat

%SystemDrive%\credsde.boo

%SystemRoot%\fonts\vgaoem.fon

%SystemRoot%\AppPatch\drvmain.sdb

%SystemRoot%\system32\config\.evt.ftl.regtrans-ms.blf

%SystemRoot%\system32\config\system

%SystemRoot%\system32\config\system.log

%SystemRoot%\system32\config\system.log1

%SystemRoot%\system32\config\system.log2

%SystemRoot%\system32\config\system.alt

%SystemRoot%\system32\config\system.sav

%SystemRoot%\system32\config\SYSTEM.CB1

%SystemRoot%\system32\config\SYSTEM.CB2

%SystemRoot%\system32\config\SYSTEM.CB3

%SystemRoot%\system32\config\SYSTEM.CBT

%SystemRoot%\system32\config\CREDSDE.BAD

%SystemRoot%\system32\winload.exe

%SystemRoot%\system32\winresume.exe

%SystemRoot%\system32\winlogon.exe

%SystemRoot%\system32\autochk.exe

%SystemRoot%\system32\apisetschema.dll

%SystemRoot%\system32\catroot*\windows-legacy-whql.cat

%SystemRoot%\WinSxS*\drvmain.sdb

Notes

Protection of SystemRoot

The protection of the SystemRoot directory is specified so that only the root itself is protected, meaning that the sub-directories of the SystemRoot do not inherit this protection. This would be the equivalent of using the following policy:

-@C:

External Media Shield (EMS)

EMS operates off its own set of encryption rules independent of what Common Encryption, User Encryption, or SDE uses. User/Common Encryption policies will only be applied to fixed disks. If an endpoint is determined to be removable storage, then EMS policy will be applied.

What Happens When Policies Tie

- When an exclusion and inclusion statement both apply to a given directory or file, the exclusion policy prevails.
- If you apply a Common encryption policy and User encryption policy specifically to the same file or location, the file or location will be Common Key encrypted.
- If you apply a Common encryption policy and an SDE encryption policy specifically to the same file or location, the file or location will be Common Key encrypted.
- If you apply a user encryption policy and an SDE encryption policy specifically to the same file or location, the file or location will be User Key encrypted.

See Sub-directories and Precedence of Directives for more information.

Generic Drive Statements

Instead of having to specify each drive in an inclusion or exclusion rule by its drive letter assignment, you may use a generic rule to target either All Fixed Drives or all Removable Drives.

Fixed Drive Usage: Replace the drive letter with F#.

Example: F#:\ instead of C:\ or D:\

The Fixed Drive rule can only be used within a Common Encrypted Folder policy, User Encrypted Folder policy, and/or SDE policy.

Removable Drive Usage: Replace the drive letter with R#.

Example: R#:\ instead of F:\ or H:\

The Removable Drive rule can only be used within an EMS Encryption Rules policy.

Enroll for Advanced Threat Prevention Agent Auto Updates

You can enroll to receive Advanced Threat Prevention agent auto updates. Enrolling to receive agent auto updates allows clients to automatically download and apply updates from the Advanced Threat Prevention server. Updates are released monthly.

Receive agent auto updates

To enroll to receive agent auto updates:

1. In the left pane of the Remote Management Console, click **Management > Services Management**.
2. On the **Advanced Threats** tab, under Agent Auto Update, click the **On** button then click the **Save Preferences** button.

Stop receiving agent auto updates

To stop receiving agent auto updates:

1. In the left pane of the Remote Management Console, click **Management > Services Management**.
2. On the **Advanced Threats** tab, under Agent Auto Update, click the **Off** button, then click the **Save Preferences** button.

Export Secure Lifecycle Audit Events to a SIEM Server

Dell Data Protection Server can be configured to forward Secure Lifecycle audit events to a SIEM server.

Audit event forwarding has been validated on splunk>enterprise (local installation) with the universal forwarder.

To enable audit event forwarding:

1. Install and configure a SIEM server and a forwarder; establish the connection between them; and enable receiving.

   For setup instructions, refer to documentation provided by your SIEM vendor.

2. Enable audit event logging on the Dell Data Protection Server. To enable logging, in the Security Server applications.properties file, set the **auditdb.events.export.enabled** property to **true**:

   auditdb.events.export.enabled=true

   The applications.properties file is located in the following folders:

   Dell Enterprise Server - <install directory>\Dell\Enterprise Edition\Security Server\conf

   VE - /opt/dell/server/security-server/conf

3. On the SIEM forwarder, specify the location of the audit event log file on DDP Server.

   Dell Enterprise Server - <install directory>\Dell\Enterprise Edition\Security Server\logs\siem

   VE - <hostname>/opt/dell/server/security-server/logs/siem/

The following audit event logging settings may be configured in the Security Server applications.properties file:

auditdb.cleanup.cron=0 0 0/2 * * ? - Interval at which the DDP Server polls the audit event database and writes changes to the log file. Default, 2 hours.

auditdb.size.percentage=0.95 - Percentage of the maximum size of the audit database the log file can consume. Default, 95 percent.

auditdb.max.size.gb= - Maximum size of the audit event log file.

auditdb.events.export.enabled=false - Enable or disable audit event logging into the audit-export.log file. Default, false.

auditdb.events.export.location=${app.home}/logs/siem/audit-export.log - Location of the audit event log file.

Localizable Policies

Localizable policies are indicated with this icon:

Available languages:

English	Korean
French	Brazilian Portuguese
German	Portuguese
Italian	Spanish
Japanese	

For instructions about localizing policies, see Localize policies.

The following policies can be displayed in a selected language on the endpoint computer:

Enterprise Level

Technology Group	Policy
Windows Encryption > Self-Encrypting Drive (SED)	Support Information Text
	PBA Title Text
	Legal Notice Text
	Self Help Questions (Pre-8.0 clients)
Windows Encryption > Policy-Based Encryption	Common Encrypted Folders
	User Encrypted Folders
	OS Update Encryption Rules
	Application Data Encryption List
	Managed Services
Windows Encryption > BitLocker Encryption	Default Folder Location to Save Recovery Password
Authentication > Windows Authentication	Recovery Questions for Windows Authentication (Checkbox selections)
Removable Media Encryption > Windows Media Encryption	EMS Device Whitelist

	EMS Access Code Required Message
	EMS Access Code Failed Message
Cloud Encryption > Cloud Protection	Help File Name
	Help File Contents
	Excluded Folders
	Excluded Files

Users Level

Technology Group	Policy
Windows Encryption > Policy-Based Encryption	User Encrypted Folders
	Application Data Encryption List
	Managed Services
Removable Media Encryption > Windows Media Encryption	EMS Device Whitelist
	EMS Access Code Required Message
	EMS Access Code Failed Message

Endpoints Level

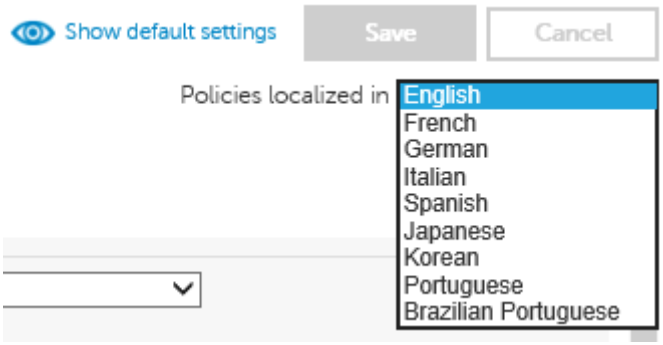
Technology Group	Policy
Windows Encryption > Self-Encrypting Drive (SED)	Support Information Text
	PBA Title Text
	Legal Notice Text
	Self Help Questions (Pre-8.0 clients)
Windows Encryption > Policy-Based Encryption	Common Encrypted Folders
	OS Update Encryption Rules
Windows Encryption > BitLocker Encryption	Default Folder Location to Save Recovery Password
Cloud Encryption > Cloud Protection	Help File Name
	Help File Contents
	Excluded Folders
	Excluded Files

Localize Policies Displayed on the Endpoint Computer

Localizable policies are indicated with this icon:

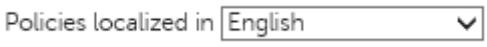
To localize policies that are displayed on the endpoint computer, follow these steps:

1. In the left pane, expand **Populations** and select a population.
2. Click the **Security Policies** tab.
3. Select the technology group, such as Windows Encryption, or policy group, such as Policy-Based Encryption, to modify.
4. Select a language for localizable policies from the drop-down list at the top right of the screen.



5. Enter text that is in the language you selected for localizable policies. Navigate the populations and technology groups as necessary to localize all desired policies for that language.
6. Click **Save**.
7. To update policies in a different language, select the language from the drop-down list, enter localized text for all desired policies, and click **Save**.

   Save policy changes before selecting another language in the drop-down list. A different language cannot be selected until policy changes are saved.
8. When finished, select the desired language. Any changes made to localizable policies will be made in the language that displays.



NOTE: The Security Policies page for a population displays overrides to localizable policies in the browser language only.

Log In

To perform a given administrative procedure, an Administrator must first log in to the Remote Management Console using an appropriate Dell Administrator account.

The DDP Server installs with a default Super Administrator user name (superadmin) and password (changeit) that you can use to add additional Dell Administrator accounts.

1. Open Internet Explorer and type **http://server.domain.com:8443/webui/login**.
2. If you are logging in for the first time, in the *Username:* field, enter **superadmin**. In the *Password:* field, enter **changeit**.

   If you are not logging in for the first time, in the *Username:* field, enter your **Username** in one of the formats listed below. In the *Password:* field, enter **<your_case-sensitive_password>**.

   user@domain.com (preferred format)

   sAMAccountName, such as jsmith

<domain>\<username> - You must specify your domain name as an alias to use this format. For more information, refer to Add Domains.

If you are not logging in for the first time, in the *Username:* field, enter your **Username** in one of the formats listed below. In the *Password:* field, enter **<your_case-sensitive_password>**.

3. Click **Sign in**.

To log out, see Log Out.

Log Out

Note: If you are an Account Administrator and make changes to your own account, you must log out and log back in to see the results.

- Click the gear icon in the top right corner of the Remote Management Console and select **Log out** from the drop-down menu.

Manage Enterprise Advanced Threats - Agents

After an Advanced Threat Prevention client is installed on an endpoint computer, it is recognized by the EE Server/VE Server as an agent.

Agents Table Data, Explained

- Name - The name of the agent on the endpoint computer.
- State - State of the agent, online or offline.
- Offline Date - If applicable, the date on which the agent went offline.
- Files Analyzed - Number of files analyzed on the endpoint computer.
- Unsafe - Number of files deemed Unsafe on the device. An unsafe file has characteristics that greatly resemble malware.
- Quarantined - Number of files Quarantined on the device.
- Waived - Number of Waived files on the device.
- Abnormal - Number of Quarantined files on the device.
- Exploit Attempts - Number of exploit attempts on the device.

Commands

To export details about an agent or remove an agent from the list, click the appropriate button:

Export - Creates and downloads a CSV file that contains device information (Name, State, Policy, etc.).

Remove - Removes selected agents from the Agent Table. This does not uninstall the agent from the device.

Manage Enterprise Advanced Threats - Certificate

The Certificate tab allows you to upload a certificate for the purpose of safelisting it.

To upload a certificate, follow these steps:

1. Navigate to **Populations > Enterprise > Advanced Threats tab > Certificate tab**.
2. Click **Browse**.
3. Select a certificate and click **Open**.

4. Click **Upload Certificate**.
5. At the *Upload Successful* dialog, click **OK**.

For instructions about how to safelist a certificate, see Manage Enterprise Advanced Threats - Global List.

Manage Enterprise Advanced Threats - Cylance Score and Threat Model Updates

A Cylance score is assigned to each file that is deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.

Threat Model Updates

The predictive threat model used to protect devices receives periodic updates to improve detection rates.

Two columns on the Protection page in the Remote Management Console show how a new threat model affects your organization. Display and compare the Production Status and New Status columns to see which files on devices might be impacted by a model change.

To view the Production Status and New Status columns:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threats** tab.
3. Click the **Protection** tab.
4. Click the down-arrow on a column header in the table.
5. Hover over **Columns**.
6. Select the **Production Status** and **New Status** columns.

Production Status - Displays the current model status (Safe, Abnormal or Unsafe) for the file.

New Status - Displays the model status for the file in the new model.

For example, a file that was considered Safe in the current model might change to Unsafe in the new model. If your organization needs that file, you can add it to the Safe list. A file that has never been seen or score by the current model might be considered Unsafe by the new model. If your organization needs that file, you can add it to the Safe list.

Only files found on device in your organization and that have a change in its Cylance Score are displayed. Some files might have a Score change but still remain within its current Status. For example, if the Cylance Score for a file goes from 10 to 20, the file status may remain Abnormal and the file will appear in the updated model list (if this file exists on devices in your organization).

The information for the model comparison comes from the database, not your devices. So no re-analysis is done for the model comparison. However, when a new model is available and the proper Agent is installed, a re-analysis is done on your organization and any model changes are applied.

Compare Current Model with New Model

You can now review differences between the current model and the new model.

The two scenarios you should be aware of are:

Production Status = Safe, New Status = Abnormal or Unsafe

- Your Organization considers the file as Safe
- Your Organization has Abnormal and/or Unsafe set to Auto-Quarantine

Production Status = Null (not seen or scored), New Status = Abnormal or Unsafe

- Your Organization considers the file as Safe
- Your Organization has Abnormal and/or Unsafe set to Auto-Quarantine

In the above scenarios, the recommendation is to Safelist the files you want to allow in your organization.

Identify Classifications

To identify classifications that could impact your organization, Dell recommends the following approach:

1. Apply a filter to the New Status column to display all Unsafe, Abnormal, and Quarantined files.
2. Apply a filter to the Production Status column to display all Safe files.
3. Apply a filter to the Classification column to only show Trusted - Local threats.
   Trusted - Local files have been analyzed by Cylance and found to be safe. Safelist these items after review. If you have a lot of files in the filtered list, you may need to prioritize using more attributes. For example, add a filter to the Detected By column to review threats found by Execution Control. These were convicted when a user attempted to execute an application and need more urgent attention than dormant files convicted by Background Threat Detection or File Watcher.

Manage Enterprise Advanced Threats - Global List

The Global Quarantine, Safe, and Unassigned tables provide a view of files in list as well as options to perform actions on these files.

Global Quarantine

Global Quarantine lists files that are permanently quarantined from all devices.

Add a file to the global quarantine list

Add the selected file to the Global Quarantine list to prevent it from being run on any device in the organization. Adding a file to Quarantine removes it from lists of Unsafe or Unassigned files.

1. Select **Global Quarantine (n)**.
2. Select a threat.
3. Click **Add File**.
4. Enter a reason that this file should be global quarantined and click **Yes**.

Manually Add File to the Global Quarantine list

1. Select **Global Quarantine (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be quarantined.
7. Click **Submit**.

Remove a file from the global quarantine list

Remove the selected file from the Global Quarantine list to allow it to run on any device in the organization.

1. Select **Global Quarantine (n)**.

2. Select a file.
3. Click **Remove from List**.

Safelist a file from the global quarantine list

Safelist the selected file from the Global Quarantine list to allow it to run on any device in the organization.

1. Select **Global Quarantine (n)**.
2. Select a file.
3. Click **Safe**.

Safe

Safelisted files and certificates are permanently treated as safe across all devices. Any certificate that is safelisted will be a known safe certificate for the Advanced Threat Prevention tenant.

Add a file to the safe list

Safelisting a file allows that file to run on any device across the entire organization.

Note: Occasionally, a “good” file may be reported as unsafe (this could happen if the features of that file strongly resemble those of malicious files). Waiving or safelisting the file can be useful in these instances.

1. Select **Safe (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be safelisted.
7. Click **Submit**.

Remove a file from the safe list

1. Select **Safe (n)**.
2. Select **Files (n)**.
3. Select the file you want to remove from the safe list.
4. Click **Remove from List**.

Add a certificate to the safe list

Safelisting a certificate allows access to that certificate, as needed, across the entire organization.

1. Select **Safe (n)**.
2. Select **Certificates (n)**.
3. Select the certificate you want to list as safe.
4. Click **Add Certificate**.
5. Select the category that fits the certificate.

6. Enter a reason why the certificate should be listed as safe, and click **Submit**.

Note: You must upload a certificate in order for it to be available to safelist. For more information, see **Manage Enterprise Advanced Threats - Certificate.**

Remove a certificate from the safe list

1. Select **Safe (n)**.
2. Select **Certificates (n)**.
3. Select the certificate you want to remove from the safe list.
4. Click **Remove from List**.

Unassigned

Unassigned files can be added to the global quarantine or safe list.

Add an unassigned file to the global quarantine list

Add the selected file to the Global Quarantine list to prevent it from being run on any device in the organization. Adding a file to Quarantine removes it from lists of Unsafe or Unassigned files.

1. Select **Unassigned (n)**.
2. Select a file.
3. Click **Global Quarantine**.
4. Enter a reason that this file should be global quarantined and click **Yes**.

Manually Add File to the Global Quarantine list

1. Select **Unassigned (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be quarantined.
7. Click **Submit**.

Add an unassigned file to the safe list

Safelisting a file allows that file to run on any device across the entire organization.

1. Select **Unassigned (n)**.
2. Select a file.
3. Click **Safe**.
4. Select the category that fits the file.
5. Enter a reason why the file should be listed as safe, and click **Yes**.

Note: Occasionally, a “good” file may be reported as unsafe (this could happen if the features of that file strongly resemble those of malicious files). Waiving or safelisting the file can be useful in these instances.

Manually Add File to the Safe list

1. Select **Unassigned (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be safelisted.
7. Click **Submit**.

Add the selected file to the Global Quarantine list to prevent it from being run on any device in the organization. Adding a file to Quarantine removes it from lists of Unsafe or Unassigned files.

1. Select **Global Quarantine (n)**.
2. Select a threat.
3. Click **Add File**
4. Enter a reason that this file should be global quarantined and click **Yes**.

Manually Add File to the Global Quarantine list

1. Select **Global Quarantine (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be quarantined.
7. Click **Submit**.

Manage Enterprise Advanced Threats - Options

The Options tab allows you to integrate with Security Information Event Management (SIEM) software using the Syslog feature as well as export Advanced Threat data. SIEM software allows administrators to run customized analytics on threat data within their environments. Software options include Splunk, available to Splunkbase users at https://splunkbase.splunk.com/app/3233.

Syslog events are persisted at the same time Agent events are persisted to the Cylance server. For more information about supported event types, see Syslog Event Types.

To integrate with SIEM, select **Syslog/SIEM** on the **Options** tab, and complete the form that displays. For a list of syslog server IP addresses to allow, see Syslog IP Addresses.

With SIEM integration, to export data about threats, select **Threat Data Report** on the **Options** tab. For instructions and a description of exportable data, see Threat Data Report.

Manage Enterprise Advanced Threats - Protection

The Protection tab provides information about files and scripts that are potentially harmful.

Threats

The table lists all events found across the organization. An event may also be a threat but is not necessarily so.

View additional information about a specific threat either by clicking on the threat name link to view details displayed on a new page or by clicking anywhere in the row of the threat to view details at the bottom of the page.

To view additional threat information in the table, click the drop-down arrow on a column header to select and add columns. Columns display metadata about the file, such as Classifications, Cylance Score (confidence level), AV Industry conviction (links to VirusTotal.com for comparison with other vendors), Date first found, Data last found, SHA256, MD5, File information (author, description, version), and Signature details.

Filter Events Table Data

Click the **Threat Filters** dropdown list at the upper right side of the table to view data about events by Priority, Status: Last 24 Hours, and Status: Total.

The number of events occurring in each subcategory are shown in parentheses.

Priority: Unsafe - Select a priority to view only events that match the selected priority. High, Medium, or Low.

Status: Last 24 Hours - Select a status to view only events that have had changes to this status in the last 24 hours.

Status: Total - Select a status to only events with that status.

The predictive threat model used to protect devices receives periodic updates to improve detection rates. To understand differences in how a new threat model affects information about files in your organization, see Threat Model Updates.

Commands

Select a threat to act on it. On this page, you can do the following to the selected threat data:

Export **-** Export threat data to a CSV file.

Select the rows you want to export, and then click **Export.**

Open the file with Microsoft Excel or similar application, which allows you to sort and organize the data.

Global Quarantine **-** Add a file to the global quarantine list. The threat is permanently quarantined from all devices.

Add the selected file to the Global Quarantine list to prevent it from being run on any device in the organization. Adding a file to Quarantine removes it from lists of Unsafe files.

1. Select a threat.
2. Click **Global Quarantine**.
3. Enter a reason that this file should be global quarantined and click **Yes**.

Safe - Add a file to the safe list. The file is permanently treated as safe across all devices.

1. Select the file you want to list as safe.
2. Click **Safe**.
3. Select the category that fits the file.
4. Enter a reason why the file should be listed as safe, and click **Yes**.

Note: Occasionally, a "good" file may be reported as unsafe (this could happen if the features of that file strongly resemble those of malicious files). Waiving or safelisting the file can be useful in these instances.

Edit Global List - Add or remove files from the global quarantine list.

1. Click **Edit Global List**.
2. Select the items you want to change.
3. Select **Safe** to add the selected items to the safelist, or select **Remove from list** to remove the selected files from the Global Quarantine list.

Manually Add File to the Global Quarantine list

1. Click **Edit Global List**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be quarantined.
7. Click **Submit**.

View Threat Details - Click a threat name to display details of the threat details on a new page. Click anywhere in the threat's row to display the same threat details on the left side of this page, under the table.

File Details

Details: [*file name*]

At the bottom of the page, this section displays details about the file that triggered an event. To display this information, select the row that displays the file name in the Advanced Events table.

Click the filename next to Details: to display the same information about the event on a new web page.

Overview

The overview box contains summary information about the file.

Threat Indicators

Threat Indicators are observations about a file that has been analyzed.

These indicators help administrators understand the reason for a file's classification and provide insight into its attributes and behavior. Threat Indicators are grouped into categories.

Devices

In the Devices pane, the administrator can view a list of devices that have unsafe or abnormal files and quarantine or waive them.

The device list can be filtered by file state: Unsafe, Quarantined, Waived, or Abnormal.

Waiving a file will allow that file to run on the device.

Detailed Threat Data

If the file has been uploaded for analysis, the Detailed Threat Data pane may display a comprehensive summary of the static and dynamic characteristics of the file including additional file metadata, file

structure details, and dynamic behaviors such as files dropped, registry keys created or modified, and URLs with which it attempted to communicate.

Note: If no results display in the Detailed Threat Data pane, the file has not yet been uploaded for analysis. Debug logging may provide information about why the file was not uploaded.

Script Control Table

The table lists details about Active and PowerShell scripts that have been blocked or have triggered an alert and the affected devices.

Columns display the File name, Interpreter (PowerShell or ActiveScript), Last found, Drive type (such as internal hard drive), SHA256, Number of devices on which the script is found, and Number of occurrences that were blocked or triggered alerts.

To filter column data, click the filter icon on a column header and select values to include or exclude.

Persistent vs. Non-Persistent VDI

Persistent and Non-Persistent VDI endpoints differ in the following ways:

Persistent VDI	Non-Persistent VDI
Persistent endpoints may exist for many days to years.	Non-persistent endpoints usually exist only for a few days or weeks.
Persistent endpoints retain the configurations that are set for the VM, until the VM clone pool is removed and rebuilt.	Non-persistent endpoints revert to baseline settings after a user logs off.
A persistent endpoint is dedicated to a single user.	After reverting to baseline settings,a non-persistent endpoint is available for another user.

Policies Set by Application Control

The following policies are set when the Advanced Threat Prevention policy, Application Control, is selected.

Policy	Setting When Application Control policy is Selected
File Action: Unsafe Executable Auto Quarantine With Executable Control Enabled	Selected
File Action: Abnormal Executable Auto Quarantine With Executable Control Enabled	Selected
Memory Action: Memory Protection Enabled	Selected
Memory Action: Exploitation: Stack Pivot	Terminate
Memory Action: Exploitation: Stack Protect	Terminate
Memory Action: Exploitation: Overwrite Code	Terminate

Memory Action: Exploitation: Scanner Memory Search	Terminate
Memory Action: Process Injection: Remote Allocation of Memory	Terminate
Memory Action: Process Injection: Remote Mapping of Memory	Terminate
Memory Action: Process Injection: Remote Write to Memory	Terminate
Memory Action: Process Injection: Remote Write PE to Memory	Terminate
Memory Action: Process Injection: Remote Overwrite Code	Terminate
Memory Action: Process Injection: Remote Unmap of Memory	Terminate
Memory Action: Process Injection: Remote Thread Creation	Terminate
Memory Action: Process Injection: Remote APC Scheduled	Terminate
Memory Action: Process Injection: Remote DYLD Injection (Mac OS X only)	Terminate
Memory Action: Escalation: LSASS Read	Terminate
Memory Action: Escalation: Zero Allocate	Terminate
Execution Control: Watch for New Files	Selected

Advanced Authentication

Authentication policies allow you to configure user experience and Windows authentication.

Policy descriptions also display in tooltips in the Remote Management Console.

Policy	Default Setting	Description
Windows Authentication		
In-session Authentication Policy for Administrators	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card One-Time Password
In-session Authentication Policy for Users	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card One-Time Password
Recovery Questions for Windows Authentication	At least 3 selectable questions	Specify the questions that will be presented to Windows users during recovery questions setup. Separate each question by a carriage return. These questions will be used if the Windows password is forgotten. At least 3 questions must be specified. What is your mother's maiden name? What was the name of the first school you attended? What is the name of your first pet? What is your father's middle name? What is your mother's middle name?

		Who was your first employer? Who was your first teacher? What city were you born in? What city was your mother born in? What city was your father born in? What was the first concert you attended? Who is your favorite TV show character? What was the name of your first stuffed animal? What was the make of the first car you owned? Where did you spend your honeymoon? Where did you meet your spouse? What is your oldest cousin's name? What is your oldest niece's name? What is your oldest nephew's name? What is your youngest child's nickname? What is your oldest child's nickname? What was the last name of your third grade teacher? In what city or town did your mother and father meet? In what city or town was your first job?
Allow Recovery Questions	Not Selected	*Selected* *Not Selected* Set to Selected to allow users to use recovery questions/answers to log on to Windows.
Log Events Level	Audit	*Errors* *Audit* *Details* Level of detail in Windows Event Logs. Determines whether events such as fingerprint registration and authentication attempts are logged in the Windows Event Log. Each higher level includes all previous levels. Events are logged on the computer where they occur. Normally, the Auditing level provides sufficient detail, covering all logon, authentication, fingerprint management, and user management events. The Details levels can fill the log file very quickly. Status events provide information about the state of several important systems on the computer. They are logged on configurable intervals and generally used when events are remotely collected.

False Accept Rate of Fingerprint	Medium High - 1 in 100,000	The False Accept Rate is the probability of receiving a false acceptance decision when comparing fingerprints scanned from different fingers. You can select one of the following FAR values: * Medium (1 in 10,000) * Medium High (1 in 100,000) * High (1 in 1,000,000) For example: if you select Medium High, on average, one false acceptance will occur when a fingerprint is compared against one hundred thousand fingerprints scanned from different fingers. The higher the setting, the lower the chance of receiving a false acceptance. However, at the High setting, the system may reject legitimate fingerprints. **NOTE**: The FAR is set on a per verification basis. When matching a fingerprint against fingerprints of multiple users (identification), the internally used FAR is automatically adjusted to maintain the same effective FAR as was selected for a single match.
Minimum Number of Fingerprints to Enroll	2	The minimum number of fingerprints required to be enrolled.
Maximum Number of Fingerprints to Enroll	10	The maximum number of fingerprints required to be enrolled.
Allow Users to Enroll Credentials	Selected	Set to Selected to allow users to enroll their own credentials without administrator involvement.
Allow Users to Modify Credentials	Selected	Set to Selected to allow users to modify their own credentials that have been previously set up or enrolled.
Reminder to Enroll Credentials (Admin)	In one day	Values for reminders: Disable Reminder At Next Logon In One Day In One Week Every Two Hours
Reminder to Enroll Credentials Expiration Date (Admin)	Now	The date (time is always 12 am) when authentication policy is going into full effect. Meaning, the client stops asking the local admin to enroll credentials and forces them to enroll before they can logon. The default is “now”.
Reminder to Enroll Credentials (User)	In one day	Values for reminders: Disable Reminder At Next Logon In One Day In One Week Every Two Hours
Reminder to Enroll Credentials Expiration Date (User)	Now	The date (time is always 12 am) when authentication policy is going into full effect. Meaning, the client stops asking the user to enroll credentials and forces them to enroll before they can logon. The default is “now”.

Action Upon Smart Card Removal	Lock Workstation	*No Action* *Lock Workstation* *Force Logoff* *Disconnect if on a Remote Desktop session* The action that occurs when a smart card is removed from the computer.
Allow One-Time Password for Recovery	Not Selected	*Selected* *Not Selected* This policy is the "master policy" for all other One-time Password policies. If this policy is Not Selected, the One-time Passwords feature is disabled on the endpoint. The user will not be able to use OTP to unlock the account, regardless of other OTP policy values. If Selected, the One-time Password Recovery feature is enabled and allows the user to use a paired mobile device to generate passwords for one-time use to unlock their account, if the account password is lost.
One-Time Password Length	6	*6, 8, or 10 characters* Specifies the minimum One-time Password length.
Maximum One-Time Password Authentication Attempts	3	*3-10* Number of times a One-time Password can be entered into a device.
Require Password for Mobile Apps	Selected	Set to Selected to require the One-time Password generation application to be password protected on the mobile device.
See basic settings		

Advanced Mac Encryption

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Dell Volume Encryption		
Dell Volume Encryption	On	*On* *Off* Toggle ON to enable Dell Volume Encryption policies. If this policy is toggled to OFF, no Dell Volume Encryption takes place, regardless of other policies.
Encryption Algorithm	AES256	*AES 256, AES 128* Encryption algorithm used to encrypt data at the endpoint (all users) level. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256. NOTE: This policy applies to Dell Encryption, not FileVault encryption.
See basic settings		

Advanced Mobile Protection

Mobile Protection Policies apply to iOS, EAS, and Androids.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Mobile Edition - EAS		
Allow Simple Characters in Passcode	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines whether a simple passcode is allowed. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA). Setting this value to Not Selected is synonymous to setting Minimum Complex Characters in Passcode to 1. During testing, we observed that some Android devices ignored this policy.
Minimum Complex Characters in Passcode	1	*0-4 characters* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the minimum number of complex characters that a passcode must contain. A complex character is a character other than a number or a letter, such as &%$#.
Maximum Passcode Age	30 days	*0-365 days. 30 days default.* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the number of days for which the passcode can remain unchanged. After this number of days, the user is forced to change the passcode before the device is unlocked. Set to 0 to require the passcode to be changed each time the device is unlocked (not recommended). **NOTE:** We have seen in testing that setting this value to 1 causes the device to request a new passcode every minute.
Number of Unique Passcodes Before Reuse	0	*0-50 passcodes* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines the number of unique new passcodes that have to be associated with a user account before an old passcode can be reused. Set to 0 to disable; set to 1 to disallow reusing the current passcode.

Minimum Passcode Length	4	*0-18 characters* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the minimum password length if passcode is enabled. This parameter is independent of the Minimum Complex Characters in Passcode policy.
Require Alphanumeric Characters in Passcode	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies whether the user must enter alphabetic characters (abcd), or if numbers are sufficient.
Number of Failed Passcode Attempts Before Device Wipe	16	*4-16 failed passcode attempts* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies how many times an incorrect password can be entered before the mobile device performs a wipe of all data.
Allow Camera	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. When Not Selected, the Camera is disabled and its icon is removed from the Home screen.
Allow Browser	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. When Not Selected, the web browser application is disabled and its icon removed from the Home screen.
Encrypt Storage Card	Not Selected	*Selected* *Not Selected* When Selected the device's storage card must be encrypted or it will be blocked.
See basic settings		
Policy	**Default Setting**	**Description**
Mobile Edition - iOS		
Allow Simple Characters in Passcode	Selected	*Selected*

		Not Selected This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines whether a simple passcode is allowed. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA). Setting this value to Not Selected is synonymous to setting Minimum Complex Characters in Passcode to 1. During testing, we observed that some Android devices ignored this policy.
Require Alphanumeric Characters in Passcode	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies whether the user must enter alphabetic characters (abcd), or if numbers are sufficient.
Minimum Passcode Length	4	*0-18 characters* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the minimum password length if passcode is enabled. This parameter is independent of the Minimum Complex Characters in Passcode policy.
Minimum Complex Characters in Passcode	1	*0-4 characters* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the minimum number of complex characters that a passcode must contain. A complex character is a character other than a number or a letter, such as &%$#.
Maximum Passcode Age	30 days	*0-365 days. 30 days default.* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the number of days for which the passcode can remain unchanged. After this number of days, the user is forced to change the passcode before the device is unlocked. Set to 0 to require the passcode to be changed each time the device is unlocked (not recommended). **NOTE:** We have seen in testing that setting this value to 1 causes the device to request a new passcode every minute.
Inactivity Period for Device Lock	60 minutes	*0-60 minutes* This policy is an iOS policy and an Exchange

		ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies the number of minutes for which the device can be idle (without user input) before it gets locked by the system. Once this limit is reached, the device is locked and the passcode must be entered.
Number of Unique Passcodes Before Reuse	0	*0-50 passcodes* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Determines the number of unique new passcodes that have to be associated with a user account before an old passcode can be reused. Set to 0 to disable; set to 1 to disallow reusing the current passcode.
Grace Period for Device Lock	0	*0-240 minutes* The maximum grace period, in minutes, to unlock the phone without entering passcode. The default is 0, no grace period, which requires a passcode immediately.
Number of Failed Passcode Attempts Before Device Wipe	16	*4-16 failed passcode attempts* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. Specifies how many times an incorrect password can be entered before the mobile device performs a wipe of all data.
Allow Removal Passcode	Not Selected	*Selected* *Not Selected* Set to Selected if there is a removal passcode.
Disallow Payload Removal	Not Selected	*Selected* *Not Selected* If present and set to Selected, the user cannot delete the profile (unless the profile has a removal password and the user provides it). If locked in this way, the profile can be replaced be a new version only if the profile identifier matches and the profile is signed by the same authority.
Removal Password Value	1-32 characters	*1-32 characters* Specifies the removal password for the profile.
Allow Browser	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. When Not Selected, the web browser application is disabled and its icon removed from the Home screen.
Allow YouTube	Selected	*Selected*

		Not Selected When Not Selected, the YouTube application is disabled and its icon is removed from the Home screen.
Allow Camera	Selected	*Selected* *Not Selected* This policy is an iOS policy and an Exchange ActiveSync policy. Setting the policy in the iOS policy category also changes the value in the Exchange ActiveSync policy category, and vice-versa. When Not Selected, the Camera is disabled and its icon is removed from the Home screen.
Allow iTunes	Selected	*Selected* *Not Selected* When Not Selected, the iTunes Music Store is disabled and its icon is removed from the Home screen. Users cannot preview, purchase, or download content.
Allow Installing Apps	Selected	*Selected* *Not Selected* When Not Selected, the App Store is disabled and its icon is removed from the Home screen. Users are unable to install or update their applications.
Allow Explicit Content	Not Selected	*Selected* *Not Selected* When Not Selected, explicit music or video content purchased from the iTunes Store is hidden. Explicit content is marked as such by content providers, such as record labels, when sold through the iTunes Store.
Allow Screen Capture	Selected	*Selected* *Not Selected* When Not Selected, users are unable to save a screenshot of the display.
Allow Assistant	Selected	*Selected* *Not Selected* When Not Selected, disables Siri.
Force iTunes Password	Selected	*Selected* *Not Selected* When Selected, forces user to enter their iTunes password for each transaction.
Allow Untrusted HTTPS Certs	Not Selected	*Selected* *Not Selected* When Not Selected, automatically rejects untrusted HTTPS certificates without prompting the user.
Allow iCloud Backup	Not Selected	*Selected* *Not Selected* When Selected, the device is permitted to back up to and restore from iCloud.
Allow iCloud Document Sync and Key-Value Sync	Not Selected	*Selected* *Not Selected* When Selected, the device allows document synchronization to iCloud and allows sync data between apps running on different iOS and OS X devices to iCloud.

Allow iCloud Photo Stream	Not Selected	*Selected* *Not Selected* When Selected, iCloud automatically pushes (via Wi-Fi) a copy of any photo taken on or imported to an iOS device, to the user's other iOS devices, iPhoto or Aperture on a Mac, Pictures Library on a PC, and Apple TV.
Web Clip URL		The URL that the Web Clip should open when clicked. The URL must begin with HTTP or HTTPS or it will not work.
Web Clip Label		*Label must not exceed 32 characters.* The name of the Web Clip as displayed on the Home screen.
Allow Web Clip Removal	Not Selected	*Selected* *Not Selected* *If Not Selected, the user cannot remove the Web Clip, but it will be removed if the profile is deleted.*
See basic settings		

Advanced Port Control

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Windows Port Control		
Subclass Storage: External Drive Control	Full Access	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. This policy interacts with the Removable Storage - EMS Access to unShielded Media policy. If you intend to have Full Access to media, also set this policy to Full Access to ensure that the media is not set to read only and the port is not blocked. Full Access: External Drive port does not have read/write data restrictions applied Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Subclass Storage: Optical Drive Control	UDF Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. Full Access: Optical Drive port does not have read/write data restrictions applied UDF Only: Blocks all data writes that are not in the UDF format (CD/DVD burning, ISO burning). Read data is enabled. Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.

		Universal Disk Format (UDF) is an implementation of the specification known as ISO/IEC 13346 and ECMA-167 and is an open vendor-neutral file system for computer data storage for a broad range of media. To encrypt data written to CD/DVD media: Set EMS Encrypt External Media = True, EMS Exclude CD/DVD Encryption = False, and Storage Class: Optical Drive Control = UDF Only.
Subclass Storage: Floppy Drive Control	Read Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. Full Access: Floppy Drive port does not have read/write data restrictions applied Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Port: PCMCIA	Enabled	Enable, Disable, or Bypass port access to PCMCIA ports.
Port: Firewire (1394)	Enabled	Enable, Disable, or Bypass port access to external Firewire (1394) ports.
Port: SD	Enabled	Enable, Disable, or Bypass port access to SD card ports.
Port: Memory Transfer Device (MTD)	Enabled	Enable, Disable, or Bypass access to Memory Transfer Device (MTD) ports.
See basic settings		
Windows Device Control		
Class: Other	Enabled	Control access to all devices not covered by other Classes.
See basic settings		

Advanced Removable Media Encryption

A note about Removable Storage policies: EMS for Mac policies are device-based policies. This is different behavior than EMS for Windows, which are user-based.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Windows Media Encryption		
Windows Media Encryption	Off	Toggle On to enable Windows Removable Media Encryption policies. If this policy is toggled to OFF, no Windows Removable Media Encryption takes place, regardless of other Removable Media Encryption policies.
EMS Exclude CD/DVD Encryption	Not Selected	**False encrypts CD/DVD devices.**
EMS Allow Read-access to unShielded Media (5.4.x Only)	Selected	This policy applies to 5.4.x Windows Shields only. More... If an end-user chooses not to encrypt media and this policy is set to True, they will be able to read or delete existing files on the

		unShielded media, but the Shield will not allow any files to be edited on or added to the removable storage unless it is Shielded.
EMS Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt removable storage. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
EMS Data Encryption Key	User Roaming	Common, User, User Roaming Choose a key to be used by the Shield to encrypt all data encrypted by the External Media Shield. More... You cannot save a policy where this policy has the same value as either User Data Encryption Key policy or Application Data Encryption Key policy, the error message *Policy Constraint Violation: The value for EMS Data Encryption Key conflicts with User Data Encryption Key and/or Application Data Encryption Key* will display.
EMS Automatic Authentication	Local	Disabled, Enable Local, Enable Roaming Local automatic authentication allows the Shielded media to be automatically authenticated when inserted in the originally Shielding computer when the owner of that media is logged in. When the User Roaming key is applied to EMS, Roaming Automatic Authentication allows Shielded media to be automatically authenticated when it is inserted in any Shielded computer the media owner is logged into. When automatic authentication is disabled, users must always manually authenticate to access Shielded media. Disabling Roaming Authentication helps to prevent users from forgetting their password when they take the media home or share it with a colleague. Disabling Roaming Authentication also promotes a sense of awareness from a security perspective for users that the data being written to that media is protected.
EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable storage whether the endpoint is Shielded or not. More... When this policy is False, the user will be able to work with encrypted data when logged on to any Shielded endpoint, regardless of the Enterprise Server the user activated against. The user will not be able to work with encrypted data using any unShielded device.
EMS Device Whitelist		String - Maximum of 300 devices with a maximum of 500 characters per PNPDeviceID. Maximum of 4096 total characters allowed. "Space" and "Enter" characters used count in the total characters used. This policy allows the specification of removable storage devices to exclude from EMS encryption [using the removable storage device's Plug and Play device identifier (PNPDeviceID)], thereby allowing users full access to the specified removable storage devices. More... This policy is available on an Enterprise, Domain, Group, and User level. Note that local settings override inherited settings. If a user is in more than one group, all EMS Device Whitelist entries, across all Groups, apply. Note: This policy is particularly useful when using removable storage devices which provide hardware encryption. However, this policy should be used with caution. This policy does not check whether external media devices on this list provide hardware encryption. Whitelisting removable storage devices which do not have hardware encryption will not have enforced security and will not be protected. *For example, the Kingston® DataTraveler® Vault Privacy model enforces that encryption is enabled to use the device. However, the Kingston DataTraveler Vault model has an unsecured partition and a secured partition. Because it is the same physical removable storage device with only one PNPDeviceID, the two partitions cannot be distinguished, meaning that whitelisting this particular removable storage device would allow unencrypted data to leave the endpoint.* *Additionally, if an removable storage device is protected by EMS and*

		subsequently added to the EMS Device Whitelist policy, it remains encrypted and requires a reformat of the removable storage device to remove encryption.
		
		The following is an example of a PNPDeviceID, which contains the manufacturer identifier, product identifier, revision, and hardware serial number:
		
		`USBSTOR\DISK&VEN_KINGSTON &PROD_DTVAULT_PRIVACY& REV_104\07005B831A0004B4&0`
		
		To whitelist a removable storage device, provide a string value which matches portions of the device's PNPDeviceID. Multiple device PNPDeviceIDs are allowed.
		
		For example, to whitelist all Kingston DataTraveler Vault Privacy models, input the string:
		
		`PROD_DTVAULT_PRIVACY`
		
		To whitelist both models of Kingston DataTraveler, the Vault and Vault Privacy models, input the string:
		
		`PROD_DTVAULT_PRIVACY; PROD_DT_VAULT`
		
		Note that space characters are considered part of the substring to match to a PNPDeviceID. Using the previous PNPDeviceID as an example, a space before and after the semicolon would cause neither of the substrings to be matched, because the space character is not part of the PNPDeviceID.
		
		Instructions...
		
		To find and edit the PNPDeviceID for removable storage:
		
		1. Insert the removable storage device into a Shielded computer.
		2. Open the EMSService.log in C:\Programdata\Dell\Dell Data Protection\Encryption\EMS.
		3. Find PNPDeviceID= and enter the applicable values, explained below.
		
		For example:
		14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0
		
		Specify the following:
		
		VEN=Vendor; Green highlighted text represents the vendor's devices to be excluded
		
		PROD=Product/Model Name; Blue highlighted text also excludes all of Seagate's USB drives; a value represented by green highlighted text must precede this value
		
		REV=Firmware Revision; Gray highlighted text also excludes the specific model being used; values represented by green and blue highlighted text must precede this value
		
		Serial number (in this example); Yellow highlighted text excludes only this device; values represented by green, blue, and gray highlighted text must precede this value
		
		OR
		
		To find the PNPDeviceID for removable storage on Windows 7 or later:
		
		1. Insert the removable storage device.
		2. Open the Control Panel and go to Administrative Tools > Computer Management.
		3. Select the Hardware tab, select the drive, and click Properties.
		4. A new windows displays. Select the Device Instance Path in the Property drop-down menu.

		The PNPDeviceID is displayed in the Value field. *To find the PNPDeviceID for removable storage on Windows XP:* 1. Click Start > Run... 2. Type msinfo32 and click Enter. 3. When the System Information window displays, go to Components > USB. A list of USB devices and their PNPDeviceIDs displays. **Available Delimeters:** Tabs Commas Semi colons Hex character 0x1E (Record separator character)
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.
EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters Required in Password	8	1-40 characters Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	Selected	Selected requires one or more numeric characters in the password.
EMS Password Attempts Allowed	3	1-10 Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.
EMS Access and Device Code Length	16	8, 16, 32 Number of characters access and device codes have. 32 characters is the most secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	1-10 Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	Apply Cooldown, Wipe Encryption Keys Action to take following unsuccessful Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the specified cooldown period (Cooldown Time Delay and Cooldown Time Increment policies) • Wipe Encryption Keys to have the Shield delete the encryption keys on the removable storage, making the encrypted data inaccessible until the owner takes the media to a Shielded computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	String - 5-512 characters - Authentication Failed: Please contact your system administrator. Message that displays when a user needs to contact you for an access code (after authentication failure). More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. We recommend that you customize the second sentence of the message to include specific instructions about how to contact a Help Desk or Security Administrator for authentication failures.
EMS Cooldown Time Delay	30	0-5000 seconds

		Number of seconds the user must wait between the first and second rounds of access code entry attempts.
EMS Cooldown Time Increment	20	0-5000 seconds Incremental time to add to the previous cooldown time after each unsuccessful round of access code entry attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	String - 5-512 characters - You are not authorized to use this media. Please contact your system administrator. Message that displays following unsuccessful Access Code Attempts Allowed. More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. We recommend that you customize the message to include specific instructions about how to contact the Help Desk or Security Administrator.
EMS Encryption Rules		Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. "Space" and "Enter" characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as Firewire, USB, eSATA, etc. may require the use of both EMS and encryption rules to encrypt the endpoint. This is necessary due to differences in how the Windows operating system handles storage devices based on interface type. To ensure encrypting an iPod via EMS does not make the device unusable, use the following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories above. Adding the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx files are encrypted in the directories excluded from encryption via the previous rules: ^R#:\Calendars ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx .xlsx ^R#: \iPod_Control ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx Replacing these five rules with the following rule will force encryption of ppt, pptx, doc, docx, xls, and xlsx files in any directory on the iPod,

		including Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file types for all removable devices - not just an iPod. Use care when defining rules to exclude an iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation iPod Mini 4gb second generation We do not recommend the use of the iPod Shuffle, as unexpected results may occur. As iPods change, this information could also change, so caution is advised when allowing the use of iPods on EMS-enabled computers. Because folder names on iPods are dependent on the model of the iPod, we recommend creating an exclusion encryption policy which covers all folder names, across all iPod models.
See basic settings		
Mac Media Encryption		
Mac Media Encryption	Off	Toggle On to enable Mac Removable Media Encryption policies. If this policy is toggled to OFF, no Mac Removable Media Encryption takes place, regardless of other policies.
EMS Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt removable storage. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
EMS Data Encryption Key	User Roaming	Common, User, User Roaming ***Note that although Common is available, it is not implemented in this release.*** Choose a key to be used by the Shield to encrypt all data encrypted by the External Media Shield.
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.
EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters. Required in Password	8	1-40 characters Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	Selected	Selected requires one or more numeric characters in the password.
EMS Password Attempts Allowed	3	1-10 Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.
EMS Access and Device Code Length	16	8, 16, 32 Number of characters access and device codes have. 32 characters is the most secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	1-10 Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	Apply Cooldown, Wipe Encryption Keys Action to take following unsuccessful Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the specified cooldown period (Cooldown Time Delay and Cooldown Time

		Increment policies) • Wipe Encryption Keys to have the Shield delete the encryption keys on the removable storage, making the encrypted data inaccessible until the owner takes the media to a Shielded computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	String - 5-512 characters - Authentication Failed: Please contact your system administrator. Message that displays when a user needs to contact you for an access code (after authentication failure). More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. We recommend that you customize the second sentence of the message to include specific instructions about how to contact a Help Desk or Security Administrator for authentication failures.
EMS Cooldown Time Delay	30	0-5000 seconds Number of seconds the user must wait between the first and second rounds of access code entry attempts.
EMS Cooldown Time Increment	20	0-5000 seconds Incremental time to add to the previous cooldown time after each unsuccessful round of access code entry attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	String - 5-512 characters - You are not authorized to use this media. Please contact your system administrator. Message that displays following unsuccessful Access Code Attempts Allowed. More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. We recommend that you customize the message to include specific instructions about how to contact the Help Desk or Security Administrator.
EMS Encryption Rules		Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. "Space" and "Enter" characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as Firewire, USB, eSATA, etc. may require the use of both EMS and encryption rules to encrypt the endpoint. This is necessary due to differences in how the Windows operating system handles storage devices based on interface type. To ensure encrypting an iPod via EMS does not make the device unusable, use the following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories above. Adding the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx files are encrypted in the directories excluded from encryption via the previous rules: ^R#:\Calendars ;ppt.doc

		.xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx .xlsx ^R#: \iPod_Control ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx Replacing these five rules with the following rule will force encryption of ppt, pptx, doc, docx, xls, and xlsx files in any directory on the iPod, including Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file types for all removable devices - not just an iPod. Use care when defining rules to exclude an iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation iPod Mini 4gb second generation We do not recommend the use of the iPod Shuffle, as unexpected results may occur. As iPods change, this information could also change, so caution is advised when allowing the use of iPods on EMS-enabled computers. Because folder names on iPods are dependent on the model of the iPod, we recommend creating an exclusion encryption policy which covers all folder names, across all iPod models.
EMS Automatic Authentication	Local	Disabled, Enable Local, Enable Roaming Local automatic authentication allows the Shielded media to be automatically authenticated when inserted in the originally Shielding computer when the owner of that media is logged in. When the User Roaming key is applied to EMS, Roaming Automatic Authentication allows Shielded media to be automatically authenticated when it is inserted in any Shielded computer the media owner is logged into. When automatic authentication is disabled, users must always manually authenticate to access Shielded media. Disabling Roaming Authentication helps to prevent users from forgetting their password when they take the media home or share it with a colleague. Disabling Roaming Authentication also promotes a sense of awareness from a security perspective for users that the data being written to that media is protected.
EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable storage whether the endpoint is Shielded or not. When this policy is False, the user will be able to work with encrypted data when logged on to any Shielded endpoint, regardless of the Server the user activated against. The user will not be able to work with encrypted data using any unShielded endpoint.
EMS Device Whitelist		String - Maximum of 150 devices with a maximum of 500 characters per PNPDeviceID. Maximum of 2048 total characters allowed. "Space" and "Enter" characters used count in the total characters used. This policy allows the specification of removable storage devices to exclude from EMS encryption [using the removable storage device's Plug and Play device identifier (PNPDeviceID)], thereby allowing users

		full access to the specified removable storage devices. More... This policy is available on an Enterprise, Domain, Group, and Endpoint level. Note that local settings override inherited settings. If a device is in more than one group, all EMS Device Whitelist entries, across all Groups, apply. Note: This policy is particularly useful when using removable storage devices which provide hardware encryption. However, this policy should be used with caution. This policy does not check whether external media devices on this list provide hardware encryption. Whitelisting removable storage devices which do not have hardware encryption will not have enforced security and will not be protected. Additionally, if a removable storage device is protected by EMS and subsequently added to the EMS Device Whitelist policy, it remains encrypted and requires a reformat of the removable storage device to remove encryption. Instructions... 1. Insert USB removable media. 2. Open System Profiler. 3. Under Hardware, select the USB device and find the Product ID and Vendor ID, as follows: Capacity:2.06 GB (2,055,019,008 bytes) Removable Media:Yes Detachable Drive:Yes BSD Name:disk2 **Product ID:0x5406** **Vendor ID:0x0781 (SanDisk Corporation)** Version: 0.10 Serial Number:0000188C36725BC8 Speed:Up to 480 Mb/sec Manufacturer:SanDisk Location ID:0x24100000 Current Available (mA):500 Current Required (mA):200 Partition Map Type:MBR (Master Boot Record) S.M.A.R.T. status:Not Supported 4. The following Whitelist Rules can be used: USBVendorName=abc USBVendorNum=0x02 USBVendorNum=2,USBProductNum=3 USBVendorNum=2,USBProdName=abc For this example, in the Enterprise Server, add the following key/pair string to the EMS Device Whitelist policy, as shown below: "USBVendorNum=0x0781,USBProductNum=0x05406" (including quotes) 5. When satisfied with the EMS Device Whitelist rules, save and commit the policy.
See basic settings		

Removable Media Policies that Require Logoff

- EMS Encrypt External Media
- EMS Scan External Media
- EMS Encryption Algorithm

- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Advanced Secure Lifecycle

Advanced Secure Lifecycle policies are available for these populations:

- Cloud Encryption policies - Enterprise, Endpoint Groups, and Endpoints
- Protected Office Documents - Enterprise, Endpoint Groups, and Endpoints (The *Protected Office Documents* master policy, *Enable Callback Beacon*, and *Callback Beacon URL* policies are available at the Enterprise level only.)
- Mobile Client - Enterprise, Domain, User Groups, and User

See Secure Lifecycle policy groups to determine which policies to enable.

The DDP Server automatically updates profiles of cloud storage providers. For more information, see Cloud Profile Update.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Cloud Encryption		
Cloud Encryption (Windows and Mac)	On	*On* *Off* Toggle *On* to enable Cloud Encryption policies. If this policy is *Off*, no Cloud Encryption protection takes place, regardless of other policies.
Dropbox for Business Message (Windows)	String Dropbox for Business is enabled for your organization. If you also have a personal Dropbox account, please do not use it for business purposes. You must allow DDP|CE to access your Dropbox account. Click Next, then enter the credentials for your Dropbox for Business account.	*String* Message to display when Dropbox for Business is enabled for the organization. This message is customizable by the Administrator.
iOS Document Handling (Windows)	Disallow	*Allow* *Disallow* Use this policy to allow or disallow iOS clients to open documents with external applications.
Help File Name (Windows)	1. How to access secure files.html	*String* Name of the registration help file. The file name format is helpfilename.html.
Help File Contents (Windows)	HTML <![CDATA[<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> <head><title>How to Access Secure Files</title></head> <body> <table border="0">	HTML for the registration help file. HTML validation is not performed. The files in this folder have been secured using Secure Lifecycle. To view files in this folder you need to register with the owner of the files. %PRODUCTNAME% and %ACTIVATIONURL% are both replaced by the Windows client based on the activation URL dynamically. The html can be modified to suit your environment.

	<tr> <th> </th> <th> %PRODUCTNAME% </th> </tr> </table> <hr /> <br /

		Encryption maintains the previous option for any existing folders. Any new folders created will have the new policy applied. To use the new policy with the old files, cut and paste files to a new folder.
Folder Management Enabled (Windows)	Not Selected	*Selected* *Not Selected* *Selected* allows management of encryption on a folder-by-folder basis within the sync client folders. For example, if users uploaded files before installing Secure Lifecycle, you can provide temporary Folder Management rights to some users. To provide temporary Folder Management rights to a user: 1. Set this policy for the specific endpoint to **Selected**. 2. Instruct the user to manually turn on encryption for the pre-existing folder. The files will be encrypted when the files sync to the cloud. 3. After the folders are encrypted, set the *Folder Management Enabled* policy for the endpoint back to *Not Selected*.
See basic settings		

Policy	Default Setting	Description
Protected Office Documents		
Protected Office Documents (Basic - Windows and Mac) Note: Enabled only at the Enterprise level.	Off	*On* *Off* Toggle *On* to provide users with a menu option for protecting Office .docx, .xlsx, and .pptx documents. On also allows you to enable other Protected Office policies. If this policy is *Off*, no Office-protected formatting takes place, regardless of other policies.
Force Protected Files Only (Windows)	Not Selected	*Selected* *Not Selected* *Selected* forces users to save Office files as protected documents. It also enables a sweep on the clients' internal fixed drives to locate new Office files and change them to Protected mode. It disables the Share option (Office 2013 and 2016) and Save & Send option (Office 2010). If *Not Selected*, users have some options in determining whether to save a file as protected or unprotected.
Enable Time To Live and Embargo Control (Windows)	Not Selected	*Selected* *Not Selected* *Selected* allows users to specify dates for when protected Office files are

		accessible to external users.
Print Control (Windows)	Allowed	*Allowed* *Watermark* *Disabled* Controls the Print function of protected Office .docx, .pptx, and .xlsx documents: • Allowed - Print option is enabled for protected Office documents. • Watermark - Print option is enabled for protected Office documents but a watermark with the user's name, domain name, and computer ID displays on each page. Unprotected documents print without the watermark. • Disabled - Print option is disabled for protected Office documents. Users can print unprotected Office documents. Note: If **Force Protected Files Only** is *Not Selected*, the Print option is available for all unprotected Office documents.
Export Control (Windows)	Allowed	*Allowed* *Watermark* *Disabled* For Office 2013 and higher, controls the Export function of protected Office .docx, .pptx, and.xlsx documents: • Allowed - This varies based on whether **Force Protected Files Only** is *Selected*. For detailed information, see Set Security Policies to Protect Office Documents. • Watermark - Export is disabled. See Protected Export. • Disabled - Export is disabled for protected Office documents. Users can export unprotected Office documents. Note: For Office 2010, see Save and Send.
Office Protected Clip Board Unauthorized Text (Windows)	Pasting of protected data is not allowed on this computer. Please contact your administrator for assistance.	String to display when a user attempts to paste secure data from a protected document into an unprotected location.
Office Protected Document Tamper Prompt (Windows)	The file you have attempted to open appears to have been tampered with and can no longer be validated. Please contact the original author or your administrator.	String to display if a user encounters an Office-protected document that is identified as having been tampered with.
Offline Key Generation Escrow Reminder Delay	3 days	*1-14 days. 3 days default.* Specifies the number of days the client

(Windows)		will wait while not being able to escrow key material prior to warning the end user.
Offline Key Generation Escrow Reminder Text (Windows)	Dell Data Protection | Secure Lifecycle has not been able to contact the DDP Server for several days. Please ensure that you are connected to the network. If you are connected to the network, contact your Administrator.	String to display when the end user is warned that the client cannot escrow key material.
Office Protected Files Cover Page Notice (Windows and Mac)	String	Enterprise-defined text to be displayed on Office-protected cover pages. Maximum number of character is 4096. See Set Cover Page Policies. Note: If line breaks are entered as part of the text, they are automatically converted to spaces to ensure the text displays correctly in all Office applications.
Office Protected Files Cover Page Corporate Logo (Windows and Mac)	Browse button and Save Logo File button	Image to be displayed on the document cover page. See Set Cover Page Policies. Note: The logo image must be a .jpg of square dimensions with a maximum file size of 25 KB. If the image height and width dimensions are not equal, the displayed image is stretched.
Office Protected Files Cover Page DDP Server URL (Windows and Mac)	https://server	DDP Server URL that will be displayed on the cover page.
Enable Callback Beacon	Selected	Selected inserts a callback beacon into every protected Office file. To use the callback beacon, the following requirements must be met: • The beacon server must be installed as part of Front End Server/Proxy Mode installation. Port 8446 must be open. For more information, see the *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start Guide and Installation Guide*. • An administrator must have enrolled to receive Product Notifications. • The *Callback Beacon URL* policy is set.
Callback Beacon URL	String	Specifies the URL to be used when the callback beacon is inserted into Office-protected files. The URL must be externally available, hosted on an HTTP server that is installed as part of Front End Server/Proxy Mode installation. Port 8446 must be open. For more information, see the *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start Guide and Installation Guide*. The *Enable callback beacon* policy must be Selected.
See basic settings		

Policy	Default Setting	Description
Mobile Client		
Secure Lifecycle Geo Location Audit Data	Selected	*Selected* allows audit data to include geo-tracking location data.
Enable Callback Beacon	Selected	Selected inserts a callback beacon into every protected Office file. To use the callback beacon, the following requirements must be met: • The beacon server must be installed as part of Front End Server/Proxy Mode installation. Port 8446 must be open. For more information, see the *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start Guide and Installation Guide*. • An administrator must have enrolled to receive Product Notifications. • The *Callback Beacon URL* policy is set.
Callback Beacon URL	String	Specifies the URL to be used when the callback beacon is inserted into Office-protected files. The URL must be externally available, hosted on an HTTP server that is installed as part of Front End Server/Proxy Mode installation. Port 8446 must be open. For more information, see the *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start Guide and Installation Guide*. The *Enable callback beacon* policy must be Selected.
Server Polling Interval	360 minutes	*1-1440 minutes* How often, in minutes, the client checks in with the EE/VE Server for updates. Default is 360 minutes (6 hours).
Workspace Access		
Application pass code (PIN)	4	*4 or 6* Required number of characters for Workspace PIN.
Set maximum failed login attempts	8	*4 - 16* Define the number of PIN login failures. Then set the policy for action to take on the Workspace after the failed attempts.
Set action on maximum failed login attempts	Timeout for 1 minute	*Timeout for 1 minute* *Timeout for 5 minutes* *Lock Workspace* *Wipe Workspace Data* The action to take after the maximum

		failed login attempts are reached.
Set inactivity lock duration	5	*2, 5, 20, 30, or 60 minutes* Configure the amount of inactivity time that can elapse before the end user must re-enter a PIN.
Set copy/paste capabilities	Not Selected	*Selected* *Not Selected* *Selected* allows users to copy and paste outside of the workspace.
Allow Non-Genuine device OS	Not Selected	*Selected* *Not Selected* *Selected* allows a jailbroken iOS device or a rooted Android device.
Cover Page		
Office Protected Files Cover Page Acceptance Text	String	Enterprise-defined text to be displayed on Office-protected cover pages. See Set Cover Page Policies.
Office Protected Files Cover Page Corporate Logo	Browse button and Save Logo File button	Image to be displayed on the document cover page. See Set Cover Page Policies. Note: The logo image must be a .jpg of square dimensions with a maximum file size of 25 KB. If the image height and width dimensions are not equal, the displayed image is stretched.
Office Protected Files Cover Page DDP Server URL	https://server	DDP Server URL that will be displayed on the cover page.
Office Protected Document Tamper Prompt	The file being opened appears to have been tampered with and can no longer be validated. Please contact the original author or your administrator.	Text to be displayed if a user encounters an Office Protected Document that has been determined was tampered with.
Web Browser		
Set a default homepage	http://www.dell.com	Homepage default for the Workspace browser.
Pre-configure bookmarks		Pre-configure bookmarks.
See basic settings		

Set Cover Page Policies

You can set policies to customize a cover page for protected Office documents.

- Internal users - The cover page displays for the following:
  - Protected Office Documents policies have been enabled but the user has not yet installed or activated the Secure Lifecycle.
  - User opens a protected Office document from the cloud.
  - User downloads a protected Office document to a device that does not have Secure Lifecycle installed.
- Unauthorized users - The cover page displays, and the person cannot access the content.

To customize the cover page for protected Office documents, you can use these Advanced Secure Lifecycle policies:

- Office Protected Files Cover Page Notice

- Office Protected Files Cover Page Corporate Logo
- Office Protected Files Cover Page DDP Server URL

Advanced Windows Encryption

A word about types of encryption: SDE is designed to encrypt the operating system and program files. In order to accomplish this purpose, SDE must be able to open its key while the operating system is booting without intervention of a password by the user. Its intent is to prevent alteration or offline attacks on the operating system by an attacker. SDE is not intended for user data. Common and User key encryption are intended for sensitive user data because they require a user password in order to unlock encryption keys.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Self-Encrypting Drive (SED)		
Legal Notice Text	String 0-512 characters	*String 0-512 characters* Text to display before being allowed to log on to the device. For examp clicking OK, you agree to abide by the acceptable computer use policy Not entering text in this field results in no text or OK/Cancel buttons b displayed. Text wrapping occurs at the word level, not the character level. For in you have a single word that is more than approximately 50 characters i will not wrap and no scroll bar will be present, therefore the text will
Crypto Erase Password	String 0-100 characters	*String 0-100 characters* A word or code of up to 100 characters used as a fail-safe security mec Entering this word or code in the user name or password field during th authentication deletes the authentication tokens for all users and locks Afterward, only an administrator can forcibly unlock the device. Leave this field blank if you do not want to have a crypto erase passwo in case of emergency.
Self Help Questions (Pre-8.0 clients)	At least 3 selectable questions	Specify the questions that will be presented to Windows users during re questions setup. Separate each question by a carriage return. These qu be used if the Windows password is forgotten. At least 3 questions mus specified. What is the name of your first pet? Who was your first employer? What was the first concert you attended? What was the make of the first car you owned? What was the last name of your third grade teacher? In what city or town did your mother and father meet? In what city or town was your first job?
Initial Access Code	String 1-100 characters	*String 1-100 characters* This policy is used to log on to an endpoint computer when network ac unavailable. Meaning, access to the EE Server or VE Server and Active D (AD) are both unavailable. The Initial Access Code policy should only be absolutely necessary, it is not the recommended method to log in. Usin Access Code policy does not provide the same level of security as the u authentication method of logging in using User Name, Domain, and Pas The Initial Access Code can only be used one time, immediately after a The first domain login that occurs after the Initial Access Code is enter cached and the Initial Access Code entry field will not be displayed aga

Encryption Administrator Password	String	Computer-generated password used by server and client for recovery a internal processes. No end user or Administrator interaction is required If there is a list of passwords in the inherited value and none in local va the inherited list is added to the local list and the new password is put bottom of the list upon Save. If there is a list of passwords in the inherited value and a list in local va the new password is put at the bottom of the existing local value list u Clicking Reset has no effect on this policy. All values are maintained in NOTE: After a value is entered for this policy, it can never be deleted. value for this policy does not affect the Override Count.
Non-Cached User Login Attempts Allowed	50	*Any number* This policy does not come into play when connected to the network (th connection to AD), because authentication with AD is attempted. This policy only comes into play when the computer is not connected t network and an unknown user attempts to log in (meaning, a user that logged in to the computer before -- no credentials have been cached).
Cached User Login Attempts Allowed	10	*1-20 times* Number of times that a cached user can attempt to log in.
Self Help Question/Answer Attempts Allowed	3	*1-10 times* Number of times the user can attempt to enter the correct answer.
Enable One Step Logon	Selected	This policy simplifies the logon process when multi-factor authenticatio enabled at both preboot and Windows logon. If selected (or not configu authentication is required at preboot only, and users are automatically to Windows. If not selected, authentication may be required multiple t
Number of Shutdown/Restart Delays Allowed	5	*1-25 times* Number of times that a user is allowed to snooze/delay a shutdown/re being forced to shutdown/restart. TPM requires a reboot. SED requires a shutdown.
Length of Each Shutdown/Restart Delay	300 seconds	*300-30000 seconds* Number of seconds between each time the user is asked to shutdown/r TPM requires a reboot. SED requires a shutdown.
Length of Forced Shutdown/Restart Notice	60 seconds	*60-1800 seconds* When user has reached the maximum number of authorized shutdown/ snoozes/delays, this policy sets the number of seconds allowed before shutdown/restart. TPM requires a reboot. SED requires a shutdown.
Enable Plugin	Selected	The plugin must remain selected. To deactivate the PBA and disable SE Management, toggle the *Self-encrypting Drive* policy to OFF.
See basic settings		

Policy	Default Setting	Description

Hardware Crypto Accelerator (HCA)		
Allow User Approval of Secondary Drive Encryption	Not selected	Allows users to decide if additional drives are encrypted.
Encryption Algorithm	AES256	AES 256 or AES 128 Encryption algorithm used to encrypt data at the Enterprise, Endpoint Endpoints levels. Encryption algorithms in order of speed, fastest first, are AES 128, AES
Forensic Meta Data Available on HCA Encrypted Drive	Not Selected	When selected, forensics meta data is included on the drive to facilitat Meta data included: • Machine ID (MCID) of the current machine • Device ID (DCID/SCID) of the current Shield installation When not selected, forensics meta data is not included on the drive. More... Switching from not selected to selected will re-sweep, based on the HC to add forensics. This policy is intended to help forensic vendors find the GUIDs more ea automate the key retrieval for the Forensic Admin through our forensic library. If this policy is not selected, meaning the GUIDs are not includ drive, the forensic tool will just prompt the Forensic Admin for the ma the drive came from and the GUIDs will be retrieved that way. As alwa to retrieve the keys, you must provide a username and password that h authorized with the Forensic Admin privilege.
Encryption Administrator Password	String	Computer-generated password used by server and client for recovery a internal processes. No end user or Administrator interaction is required If there is a list of passwords in the inherited value and none in local va the inherited list is added to the local list and the new password is put bottom of the list upon Save. If there is a list of passwords in the inherited value and a list in local va the new password is put at the bottom of the existing local value list u Clicking Reset has no effect on this policy. All values are maintained in NOTE: After a value is entered for this policy, it can never be deleted. value for this policy does not affect the Override Count.
See basic settings		

Policy	Default Setting	Description
Policy-Based Encryption		
Encrypt with SDE when SED is detected	Not Selected	When Selected, this policy applies SDE encryption to self-encrypting dr this policy when SDE encryption is preferred instead of native SED encr
User Encrypted Folders	String	String - maximum of 100 entries of 500 characters each (up to a maxim characters) A list of folders on the endpoint hard drive to be encrypted with the Us Encryption Key or excluded from encryption. If the same folder is specified in this policy for multiple users of the sa endpoint, each file in that folder is encrypted for the first owner of the the policy takes effect, and can be decrypted only by that owner. More... Specify as for Common Encrypted Folders. This policy applies to all drives classified by Windows as Hard Disk Drive Computer). You cannot use this policy to encrypt drives or external me type displays as Removable Disk, use EMS Encrypt External Media instea

Application Data Encryption List	Exe List winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe winzip.exe winrar.exe onenote.exe onenotem.exe	String - maximum of 100 entries of 500 characters each We do not recommend adding explorer.exe or iexplorer.exe to the ADE unexpected or unintended results may occur. However, explorer.exe is the process used to create a new notepad file desktop using the right-click menu. Setting encryption by file extension the ADE list, provides more comprehensive coverage. Changes to this policy do not affect files already encrypted because of List process names of applications (without paths) whose new files you encrypted, separated by carriage returns. Do not use wildcards. More... You can also specify these process names (separated by commas) via th value HKLM\Software\Dell\CMGShield\ApplicationDataEncryptionList. The Shield encrypts all new files (not already being encrypted by Comm Encrypted Folders and User Encrypted Folders) on the current compute drives created by these application processes whenever they are owne currently-logged-on managed user. This may include files excluded fro encryption by Common Encrypted Folders and/or User Encrypted Folde The following folders and their subfolders are always excluded from en this policy: C:\Windows\system32 C:\Windows\Software Distribution C:\Windows\Security C:\System Volume Information\Program Files\Dell\(.dll.exe.sys.mac.ddp.wip.rty.nmd.inv) We strongly recommend not listing applications or installers that write critical files. Doing so could result in encryption of important system fi could make a Windows endpoint unbootable. Common process names: Outlook: outlook.exe Word: winword.exe FrontPage: frontpg.exe PowerPoint: powerpnt.exe Access: msaccess.exe WordPad: wordpad.exe Microsoft Paint: mspaint.exe Excel: excel.exe The following hard-coded system and installer process names are ignor specified in this policy (you can also add to this list via the registry val HKLM\Software\Dell\CMGShield\EUWPrivilegedList): hotfix.exe, a Windows update process update.exe, a Windows update process setup.exe, a third-party installer process msiexec.exe, a third-party installer process wuauclt.exe, a Windows update process wmiprvse.exe, a Windows system process migrate.exe, a Windows update process unregmp2.exe, a Windows update process ikernel.exe, a third-party installer process wssetup.exe, the Windows Shield installer svchost.exe, a Windows system process
User Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt data at the individual user level. specify different values for different users of the same endpoint. Encryption algorithms in order of speed, fastest first, are AES 128, AES
SDE Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to for System Data Encryption.

		Encryption algorithms in order of speed, fastest first, are AES 128, AES
Common Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt data at the endpoint (all users) le System paging files are encrypted using AES 128. Encryption algorithms in order of speed, fastest first, are AES 128, AES
Encrypt Outlook Personal Folders	Selected	Encrypts Outlook Personal Folders (%csidl:local_appdata %\Microsoft\Outlook) with the User Data Encryption Key.
Encrypt Temporary Files	Selected	When this policy is selected, the paths listed in the environment variab and TMP are encrypted. TEMP and TMP for the OS are encrypted with t Encryption Key. TEMP and TMP for the User are encrypted with the Use Encryption Key. To reduce encryption sweep time, the Shield clears the contents of the TMP folders for initial encryption, as well as updates to this policy. How your organization uses a third-party application that requires the file s within the \temp directory to be preserved, you should prevent this de To disable temporary file deletion, create DeleteTempFiles (REG_DWO its value to 0 in the registry at HKLM\SOFTWARE\Dell\CMGShield.
Encrypt Temporary Internet Files	Not Selected	When this policy is selected, the path listed in the environment variabl CSIDL_INTERNET_CACHE is encrypted with the User Data Encryption Ke To reduce encryption sweep time, the Shield clears the contents of CSIDL_INTERNET_CACHE for initial encryption, as well as updates to th This policy is applicable when using Microsoft Internet Explorer only. Fo party web browsers such as Mozilla and Opera, an Administrator must c encryption policy that is specific to the storage location of the tempora files used by each browser.
Encrypt User Profile Documents	Selected	When this policy is selected, the following are encrypted: • The My Documents folder on Windows XP and the users profile (C:\Us on Window 7 with the User Data Encryption Key • \All Users\Shared Documents on Windows XP and \Users\Public on Win the Common Encryption Key
Encrypt Windows Paging File	Selected	When this policy is selected, the Windows paging file is encrypted. A cl policy requires a reboot.
Managed Services		String - maximum of 100 entries of 500 characters each (up to a maxim characters) When a Service is managed by this policy, the Service is started only af is logged in and the Shield is unlocked. This policy also ensures that the managed by this policy is stopped before the Shield is locked during log policy can also prevent a user logoff if a Service is unresponsive. More… Syntax is one Service name per line. Spaces in the Service name are su Wildcards are not supported. Entries are not case-sensitive. For example, GoogleDesktop Manager is googledesktopmanager. The Service log on as setting has no bearing on whether or not the Shie control it. It does not matter if a user logs on with user credentials ver system. The startup type (Automatic or Manual) does not affect the ability of th control it. Automatic or Manual startup is acceptable. Managed Services will not be started if an unmanaged user logs on.
Secure Post-Encryption Cleanup	Single Pass Overwrite	No Overwrite, Single-pass Overwrite, Three-pass Overwrite, Seven-pass Once folders specified via other policies in this category have been enc policy determines what happens to the unencrypted residue of the orig • No Overwrite deletes it. This value yields the fastest encryption proc • Single-pass Overwrite overwrites it with random data. • Three-pass Overwrite overwrites it with a standard pattern of 1s and with its complement, and then with random data. • Seven-pass Overwrite overwrites it with a standard pattern of 1s and with its complement, and then with random data five times. This value

		most difficult to recover the original files from memory, and yields the secure encryption processing.
Secure Windows Credentials	Selected	When this policy is selected, the Windows Credentials will be secured b encrypting the entire registry with the exception of registry informatio for computer boot. The information required for computer boot includ HKLM/SYSTEM and all sub-keys. This policy value will be automatically set to Selected if SDE is enabled More... When a change to this policy is delivered, the Shield requires a reboot. this reboot, configure the following policies: Force Reboot on Update, Each Reboot Delay, and Number of Reboot Delays Allowed.
Block Unmanaged Access to Domain Credentials	Selected	This policy prevents unmanaged users and applications from accessing domain credentials when a user is logged in.
Secure Windows Hibernation File	Selected	When this policy is selected, the hibernation file will be encrypted onl computer enters hibernation. The Shield will disengage protection whe computer comes out of hibernation, providing protection without impa or applications while the computer is in use.
Prevent Unsecured Hibernation	Selected	When this policy is selected, the Shield will not allow computer hiberna Shield is unable to encrypt the hibernation data.
Scan Workstation on Logon	Not selected	When this policy is selected, all current and previous encrypted folder Shielded computer's local hard drives are scanned each time a manage on, ensuring that all Common Encrypted Folders and User Encrypted Fo values are properly implemented. Uses Workstation Scan Priority.
Workstation Scan Priority	Normal	Highest, High, Normal, Low, Lowest Specifies the relative Windows priority of encrypted folder scanning. H Highest prioritize scanning speed over computer responsiveness, Low a prioritize computer responsiveness over scanning speed and favor othe intensive activities, and Normal balances the two. The Shield checks for a changed Workstation Scan Priority before proce next file. The scan priority levels are used in two different ways. 1. These values correspond with the values used by the Microso set thread execution priority. 2. The Shield uses these values to introduce a delay in the encr sweep after every single file is processed. The values translate to the following millisecond delay ranges encryption thread will sit idle and then return full control to t operating system: Highest=0 ms / Lowest=100 ms
User Data Encryption Key	Common	Common, User, User Roaming Choose a key to indicate who should be able to access files encrypted b following policies, and where: • User Encrypted Folders • Encrypt Outlook Personal folders • Encrypt Temporary Files (\Documents and Settings\username\Local Se only) • Encrypt Temporary Internet Files • Encrypt User Profile Documents (except \All Users\Documents or for V \All Users\Shared Documents) Select: • Common if you want User Encrypted Files/Folders to be accessible b managed users on the endpoint where they were created (the same lev as Common Encrypted Folders), and encrypted with the Common Encry Algorithm. More... The Common Encryption Algorithm controls the encryption algorithm fo Encrypted Folders and overrides any encryption algorithm selected, inc default User Encryption Algorithm. For example, if the Common Encryp

		Algorithm is set to AES 256, all Common and User Encrypted Files/Fold encrypted with the AES 256 algorithm. All other Shield encryption parameters can be selected to override def settings. For example, if the Encrypt Temporary Files policy is set to F override this setting for any Managed User by setting this value to True Designated User Encrypted Folders will use Common Key, resulting in a users having the key to access any encrypted files stored in these folde permitted by security settings on the operating system. • User if you want these files to be accessible only to the user who cre only on the endpoint where they were created (the same level of acce Encrypted Folders), and encrypted with the User Encryption Algorithm. • User Roaming if you want these files to be accessible only to the use created them, on any Shielded Windows endpoint, and encrypted with Encryption Algorithm. If you elect to incorporate an encryption policy to encrypt entire disk p is recommended to use the default SDE encryption policy, rather than User. This ensures that any operating system files that are encrypted a accessible during states when the managed user is not logged in.
Policy Proxy Connections		String - maximum of 1500 characters List fully qualified Policy Proxy hostnames, or IP addresses, separated returns. More... Once the Shield finds a valid entry, the remainder of the entries are ig Entries are processed in the following order: 1. GKConnections Override (this registry entry overrides all other entri 2. GKConnections (this registry entry is set automatically by the Shield the this policy) 3. GK This policy works in conjunction with the Policy Proxy Polling Interval p To override this policy and specify ports via the registry item HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CMGShield\GKConnectionsOverride. You cannot specify ports in this policy. The Shield communicates with Policy Proxies using the GKPORT specifi Shield installation (the default is 8000). If necessary, change that port via the registry item HKLM\Software\Microsoft\WindowsNT\Current Version\Winlogon\CMGShield\GKPort. Inherited values for this policy accumulate. In order for the Shield to connect to a Policy Proxy specified in this pol be in the same group as the Policy Proxy specified during Shield installa Because the Shield supports up to 255 users per endpoint, this policy is only at the Enterprise Policies level.
Policy Proxy Polling Interval	360	1-1440 minutes The interval that the Shield attempts to poll Policy Proxy for policy up send inventory information to Policy Proxy. The Shield also attempts to poll Policy Proxy each time a user logs on.
Allow Activations	Selected	Precedence: Max, High, Medium, Low, Min When this policy is selected, the Server allows endpoint activations at Enterprise, Domain, User Group, or User levels. When this policy is not selected, for example, activations can be stagg blocked during initial Server setup and maintenance interruptions. For information, see Temporarily Block Activations.
Current Shield State	Activate	Activate, Suspend Activate is the normal state for a Shielded user. A user must be in this order to activate an endpoint. To require endpoint recovery before the user can access the endpoint, Suspend.

		When a user is suspended, encrypted data cannot be accessed. The use recovered by pushing down a new policy to unsuspend the user.
See basic settings		
Policy-Based Encryption - User Experience		
Enable Software Auto Updates	Not Selected	*Selected* *Not Selected* Selected enables the client update agent to automatically check for up Dell Data Protection software. If this policy is not selected, no DDP Aut take place, regardless of other policies. If this policy is set, the On Pre Update Staging Location must have a network location in its value.
On Premise Update Staging Location	String	*String* Network location (UNC) where DDP Server stages Dell Data Protection u packages. If a network location is not specified in this policy, the Enab Auto Updates policy should not be published.
Update Check Period	10080	*1-43200 minutes (30 days)* The period in minutes between checks for updates.
Number of Policy Update Delays Allowed	3	0-5000 If Force Logoff/Reboot on Policy Updates is Selected, a non-zero value user to delay the required logoff or reboot the specified number of tim zero to disable delays.
Force Logoff / Reboot on Policy Updates	Selected	Selected requires either a logoff or a reboot in order for key policy upd effect. Otherwise, these policy updates take effect whenever the next reboot occurs.
Policy Viewer Enabled	Not Selected	When Selected, the end-user can view their Windows Shield policies fr Shield icon.
Display Local Encryption Processing Control	Not Selected	When Selected, the user sees a menu option in the system tray icon tha them to pause/resume encryption/decryption (depending on what the currently doing). **Important:** *Allowing a user to pause encryption could allow the user t the Shield from fully encrypting or decrypting data per policy.*
Suppress File Contention Notification	Selected	This policy controls whether users see notification pop-ups if an applic attempts to access a file while the Shield is processing it. More... If the Shield is processing a large file that an application needs, and th enabled, it may appear that the application is unresponsive or slow to no message indicating what the issue is). Care should be taken when us policy.
Number of Encryption Processing Delays Allowed	0	0-5000 A non-zero value allows the user to delay any encryption processing re the encryption policies you set, the specified number of times. Set to z disable delays.
Length of Each Encryption Processing Delay	5	5-40320 minutes If Number of Encryption Processing Delays Allowed has a non-zero valu policy to specify how often the Shield prompts the user to continue wi encryption processing or delay again. More... The Shield displays this prompt for five minutes each time. If the user respond to the prompt, encryption processing begins. The final delay p includes a countdown and progress bar, and it displays until the user re the final delay expires and encryption processing begins. Calculate the maximum possible delay as follows (a maximum delay wo the user responding to each delay prompt immediately prior to the 5-m mark): (Number of Encryption Processing Delays Allowed x Length of Each Enc Processing Delay) + (5 minutes x [Number of Encryption Processing Dela

		1])
Length of Each Policy Update Delay	15	5-40320 minutes If Number of Policy Update Delays Allowed has a non-zero value, use th specify how often the Shield prompts the user to logoff/reboot or dela More… The Shield displays this prompt for five minutes each time. If the user respond to the prompt, the next delay begins. The final delay prompt i countdown and progress bar, and it displays until the user responds, or delay expires and the required logoff/reboot occurs. You can change the behavior of the user prompt to begin or delay encr prevent encryption processing following no user response to the promp To do this, set the registry key SnoozeBeforeSweep |(DWORD), stored i HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGSh non-zero value. Any non-zero value will change the default behavior to With no user interaction, encryption processing will be delayed up to t of configurable allowed delays. When the final delay expires, encryptio processing begins. Calculate the maximum possible delay as follows (a maximum delay wo the user never responding to a delay prompt, each of which displays fo minutes): (Number of Policy Update Delays Allowed x Length of Each Policy Upda (5 minutes x [Number of Policy Update Delays Allowed - 1])
Force Reboot on Update	Selected	When selected, the computer immediately reboots to allow processing encryption or updates related to device-based policy, such as System D Encryption (SDE).
Length of Each Reboot Delay	15	5-40320 minutes The number of minutes to delay when the user chooses to delay reboot based policy.
Number of Reboot Delays Allowed	3	0-5000 The number of times the user will be allowed to delay reboot for devic policy.
Allow Encryption Processing Only When Screen is Locked	Not Selected	Selected, Not Selected, User-Optional When Selected, there will be no encryption or decryption of data while actively working. The Shield will only process data when the screen is l User-Optional adds an option to the system tray icon allowing the user feature on or off. When Not Selected, encryption processing will occur any time, even wh is working. Enabling this option will significantly extend the amount of time it take complete encryption or decryption.
Hide Overlay Icons	Selected	When Selected, encryption overlay icons do not display on encrypted fi Explorer for all managed users on an endpoint.
See basic settings		

Policy	Default Setting	Description
Bitlocker Encryption		
Disable BitLocker on Self-Encrypting Drives	Selected	*Selected* *Not Selected* If Selected, BitLocker Manager will not start encryption on a volume th protected by an activated SED. For example, if this policy is Selected and both C: and D: are on one ph encrypting drive, and the PBA has been activated, then C: and D: will n for BitLocker even if System and Fixed drive encryption are turned on i BitLocker policies.

See basic settings		
Bitlocker Encryption - Fixed Data Volume Settings		
Configure the Use of Smart Cards on Fixed Data Drives	Allow	*Allow* *Disallow* *Require* This policy specifies whether smart cards can be used to authenticate a BitLocker fixed data drives. These settings are enforced when turning o BitLocker, not when unlocking a drive. BitLocker will allow unlocking a any of the protectors available on the drive.
Deny Write Access to Fixed Data Drives Not Protected by BitLocker	Enabled	*Enabled* *Disabled* *Enabled for Organizations* If the drive is protected by BitLocker, it will be mounted with read and access. If you disable or do not configure this policy setting, all fixed data driv computer will be mounted with read and write access.
Allow Access to BitLocker Protected Fixed Data Drives from Earlier Versions of Windows	Selected	*Selected* *Not Selected* When Enabled, fixed data drives with the FAT file system can be unlock computers running Windows Server 2008, , XP SP3 and their contents ca viewed. This policy does not apply to drives that are formatted with th system. Set this policy to Selected and the Do Not Install BitLocker to Go Reade formatted Fixed Drives policy to Not Selected to allow BitLocker to Go be installed on the fixed drive.
Do Not Install BitLocker to Go Reader on FAT Formatted Fixed Drives	Selected	*Selected* *Not Selected* If this policy is Not Selected, BitLocker to Go Reader will be installed o drive to enable users to unlock the drive on computers running Window 2008, , XP SP3 that do not have the BitLocker to Go Reader installed. Set this policy to Not Selected and the Allow Access to BitLocker Prote Data Drives from Earlier Versions of Windows policy to Not Selected to BitLocker to Go Reader to be installed on the fixed drive.
Configure Use of Passwords for Fixed Data Drives	Allow	*Allow* *Require* *Disallow* When set to Require, a connection to a domain controller is necessary the complexity of the password. When set to Allow, a connection to a controller will be attempted to validate complexity, but if no domain c found, the password will still be accepted. When set to Do Not Allow, n complexity validation will be done. To use this policy, Configure Use of Passwords for Fixed Data Drives mu Allow or Require.
Configure Password Complexity for Fixed Data Drives	Allow	*Do Not Allow* *Require* *Allow* When set to Require, a connection to a domain controller is necessary the complexity of the password. When set to Allow, a connection to a controller will be attempted to validate complexity, but if no domain c found, the password will still be accepted. When set to Do Not Allow, n complexity validation will be done. To use this policy, Configure Use of Passwords for Fixed Data Drives mu Allow or Require.
Minimum Password Length for Fixed Data Drives	8	*8 min* *20 max* Passwords must be at least 8 characters. To configure a greater minimu for the password enter the desired number of characters.

		To use this policy, Configure Use of Passwords for Fixed Data Drives mu Allow or Require.
Encryption Type for Fixed Data Drives	Full Encryption	*Allow User to Choose* *Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for Fixed Data Drives.
Choose How BitLocker-protected Fixed Drives Can be Recovered	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, ever value is Not Selected. This policy allows for the control of how BitLocke fixed data drives are recovered in the absence of the required credent More... This policy is the parent policy to: Allow Data Recovery Agent for Protected Fixed Data Drives Config User Storage of BitLocker 48-digit Recovery Password Config User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard Save BitLocker Recovery Info to AD DS for Fixed Data Drives BitLocker Recovery Info to Store in AD DS Do Not Enable BitLocker Until Recovery Info is Stored in AD DS for Fixed Drives
Allow Data Recovery Agent for Protected Fixed Data Drives	Selected	*Selected* *Not Selected* When Selected, a data recovery agent is allowed for use with BitLocke fixed data drives. Before the agent can be used, it must be added from Key Policies in either the Group Policy Management Console or the Loc Policy Editor. When setting this policy to Selected, the Choose How BitLocker-protec Drives Can be Recovered policy must also be set to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Allow* *Require* *Do Not Allow* This policy determines if a user is allowed, required, or not allowed to 48-digit password. When setting this policy to Allow or Require, the Choose How BitLocke Fixed Drives Can be Recovered policy must also be set to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Allow* *Require* *Do Not Allow* This policy determines if a user is allowed, required, or not allowed to 256-bit recovery key. When setting this policy to Allow or Require, the Choose How BitLocke Fixed Drives Can be Recovered policy must also be set to Selected.
Omit Recovery Options from the BitLocker Setup Wizard	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options w BitLocker is enabled. Recovery options for the drive are determined by settings. When setting this policy to Not Selected, the Choose How BitLocker-pr Fixed Drives Can be Recovered policy must also be set to Selected.
Save BitLocker Recovery Information to AD DS for Fixed Data Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS fo drives. BitLocker recovery information is always saved in the Remote M Console. Enabling this policy additionally saves the information to AD. More...

		The appropriate schema extensions and access control settings on the be first configured before AD DS backup can succeed. When setting this policy to True, the Choose How BitLocker-protected Can be Recovered policy must also be set to True. Set this policy to True to use the policy BitLocker Recovery Information AD DS.
BitLocker Recovery Information to Store in AD DS	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key p storing the recovery password only in AD DS. The appropriate schema e and access control settings on the domain must be first configured bef this policy. The Choose How BitLocker-protected Fixed Drives Can be Recovered po be set to Selected to use this policy. To use this policy, Save BitLocker Recovery Information to AD DS for Fi Drives must be set to Selected.
Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Fixed Data Drives	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically stored in the Management Console, this policy additionally requires BitLocker drive e recovery information to be stored in AD DS. The appropriate schema ex and access control settings on the domain must be configured before u policy. More... This policy is used to prevent users from enabling BitLocker unless the connected to the domain and the backup of the BitLocker recovery inf AD DS has succeeded. The Choose How BitLocker-protected Fixed Drives Can be Recovered po be set to True to use this policy.
Configure Use of Hardware-Based Encryption for Fixed Data Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on fi drives.
Use Hardware-Based Encryption for Fixed Data Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption for fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fix Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Fixed Data Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on fixed data dr hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Fix Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Fixed Data Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for Bit hardware encryption on fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fix Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites Settings on Fixed Data Drives	String	String - 2.16.840.1.101.3.4.1.2; 2.16.840.1.101.3.4.1.42 Set specific Crypto Algorithms and Cipher Suites on fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fix Drives must be set to Selected.

See basic settings		
Bitlocker Encryption - Global Settings		
Default Folder Location to Save Recovery Password		Qualified path Important: This policy is not used by BitLocker Manager, because it doe prompt the user when saving recovery passwords. Microsoft defines this policy as: This setting provides the default path displayed when the BitLocker drive encryption setup wizard prompts th enter the location of a folder to save the recovery password.
Encryption Method and Cipher Strength	AES 128 with Diffuser	*AES 128 with Diffuser* *AES 256 with Diffuser* *AES 128* *AES 256* This policy specifies the encryption method and cipher strength used fo drive encryption. Note that changing this policy has no effect if the dri encrypted or encryption is in progress.
Enable Organizational Unique Identifiers	Not Selected	*Selected* *Not Selected* This policy allows for the association of unique organizational identifie drive that is enabled with BitLocker. These identifiers are stored as the identification field and allowed identification field. The allowed identi field is used in combination with the Deny Write Access to Removable D Protected by BitLocker policy to help control the use of removable driv organization. This policy must be set to Selected to use the policies Set Organization Identifiers and Set Allowed Org Unique Identifiers.
Set Organizational Unique Identifiers		*Up to 260 characters* The identification field allows you to associate a unique organizational BitLocker-protected drives. This identifier is automatically added to ne BitLocker-protected drives and can be updated on existing BitLocker-p drives using the Manage-BDE command-line tool. An identification field for management of certificate-based data recovery agents on BitLocke drives and for potential updates to the BitLocker To Go Reader. BitLoc manage and update data recovery agents when the identification field matches the value configured in the identification field. In a similar ma BitLocker will only update BitLocker To Go Reader when the identificat the drive matches the value configured for the identification field. To use this policy, Enable Organizational Unique Identifiers must be se Selected.
Set Allowed Organizational Unique Identifiers		*Up to 260 characters* The allowed identification field is used in combination with the Deny W to Removable Drives Not Protected by BitLocker policy to help control removable drives in the organization. It is a comma separated list of id fields from your organization or other external organizations. To use this policy, Enable Organizational Unique Identifiers must be se Selected.
Prevent Memory Overwrite on Restart	Not Selected	*Selected* *Not Selected* Selected prevents memory from being overwritten on restart. Preventi overwrite may improve restart performance, but will increase the risk BitLocker secrets. When Not Selected, BitLocker secrets are removed f when the computer restarts.
Enable Smart Card Certificate Identifier	Not Selected	*Selected* *Not Selected* This policy allows or denies an object identifier to be specified for enh usage with a certificate. This policy must be set to Selected to use the policy Smart Card Certifi Identifier.
Smart Card Certificate	1.3.6.1.4.1.311.67.1.1	*1.3.6.1.4.1.311.67.1.1*

Identifier		This policy provides for an object identifier to be specified for enhance with a certificate. BitLocker can identify which certificates may be use authenticate a user certificate to a BitLocker drive by matching the ob identifier in the certificate with the object identifier that is defined by Use caution if changing the default value. To use this policy, Enable Smart Card Certificate Identifier must be set Selected.
See basic settings		
Bitlocker Encryption - Operating System Volume Settings		
Allow Enhanced PINs for Startup	Not Selected	*Selected* *Not Selected* Selected allows enhanced startup PINs to be used with BitLocker. Enhanced startup PINs permit the use of characters including uppercas lowercase letters, symbols, numbers, and spaces. This policy setting is when you turn on BitLocker.
Number of Characters Required in PIN	4	*4-20 digits* This policy configures the minimum length for a TPM startup PIN. The s must have a minimum length of 4 digits and can have a maximum of 20
Allow Network Unlock at Startup on Operating System Drives	Not Selected	*Selected* *Not Selected* This policy specifies if a user is allowed to use the Network Unlock at S feature on operating system drives.
Allow SecureBoot on Operating System Drives	Selected	*Selected* *Not Selected* This policy specifies if a user is allowed to use SecureBoot on operating drives.
Disallow Standard Users from Changing the PIN on Operating System Drives	Not Selected	*Selected* *Not Selected* This policy specifies if a standard user is allowed to change their PIN or system drives.
Enable Use of Preboot Keyboard Input on Slates	Not Selected	*Selected* *Not Selected* This policy specifies if a preboot keyboard input is enabled on Slates.
Reset Platform Validation Data After Recovery	Not Selected	*Selected* *Not Selected* This policy specifies if a preboot keyboard input is enabled on Slates.
Choose How BitLocker-protected Operating System Drives Can be Recovered	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, ever value is Not Selected. For the GPO, a Selected value allows you to spec BitLocker drives are recovered. More... This policy is the parent policy to: Allow Data Recovery Agent for Protected Operating System Drives Configure User Storage of BitLocker 48-digit Recovery Password Configure User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard Save BitLocker Recovery Info to AD DS for Operating System Drives BitLocker Recovery Information to Store in AD DS (Windows Server 2008 Do Not Enable BitLocker Until Recovery Information is Stored in AD DS Operating System Drives
Allow Data Recovery Agent for Protected	Selected	*Selected* *Not Selected*

Operating System Drives		The "Allow Certificate Based Data Recovery Agent" is used to specify wh data recovery agent can be used with BitLocker operating system drive data recovery agent can be used, it must be added from the Public Key either the Group Policy Management Console or the Local Group Policy To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Do Not Allow* *Require* *Allow* This policy configures if a user is allowed, required, or not allowed to g 48-digit password. To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Do Not Allow* *Require* *Allow* This policy configures if a user is allowed, required or not allowed to g 256-bit recovery key. To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Omit Recovery Options from the BitLocker Setup Wizard	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options w BitLocker is enabled. Recovery options for the drive are determined by settings. To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Save BitLocker Recovery Information to AD DS for Operating System Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS fo system drives. Note that the appropriate schema extensions and access settings on the domain must be first configured before AD DS backup ca To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
BitLocker Recovery Information to Store in AD DS (Windows Server 2008 Only)	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key p storing the recovery password only in AD DS. The appropriate schema e and access control settings on the domain must be first configured befo this policy. This policy is applicable only to computers running Windows Server 200 To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Operating System Drives	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically stored in the Management Console, this policy additionally requires BitLocker drive e recovery information to be stored in AD DS. The appropriate schema ex and access control settings on the domain must be configured before u policy. This policy is used to prevent users from enabling BitLocker unless the connected to the domain and the backup of the BitLocker recovery info AD DS has succeeded. To use this policy, Choose How BitLocker-protected Operating System D be Recovered must be set to Selected.
Configure Use of Hardware-Based Encryption for Operating System Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on op

		system drives.
Use Hardware-Based Encryption for Operating System Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption on operating system drive To use this policy, Configure Use of Hardware-Based Encryption for Ope System Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Operating System Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on operating sys if hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Ope System Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Operating System Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for Bit hardware encryption on operating system drives. To use this policy, Configure Use of Hardware-Based Encryption for Ope System Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites Settings on Operating System Drives	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	*String -* *2.16.840.1.101.3.4.1.2;* *2.16.840.1.101.3.4.1.42* Specific Crypto Algorithms and Cipher Suites allowed on operating syst To use this policy, Configure Use of Hardware-Based Encryption for Ope System Drives must be set to Selected.
Encryption Type for Operating System Drives	Full Encryption	*Allow User to Choose* *Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for operating system drives.
Configure Use of Passwords for Operating System Drives	Not Configured	*Enabled* *Disabled* *Not Configured* Configure password requirements for Operating System Drives.
Configure Password Complexity for Operating System Drives	Allow	*Allow* *Require* *Do Not Allow* When set to Require, a connection to a domain controller is necessary the complexity of the password. When set to Allow, a connection to a controller will be attempted to validate complexity, but if no domain found, the password will still be accepted. When set to Do Not Allow, complexity validation will be done. To use this policy, Configure Use of Passwords for Operating System Dr set to Enabled.
Minimum Password Length for Operating System Drives	8	*8-256* The default value is a password length of 8 characters. 8-256 character allowed. To use this policy, Configure Use of Passwords for Operating System Dr set to Enabled.
Require ASCII-Only Passwords for Operating System Drives	Not Selected	*Selected* *Not Selected* Require ASCII-only passwords for operating system drives to create stro passwords. To use this policy, Configure Use of Passwords for Operating System Dr set to Enabled.
Use Enhanced Boot	Disabled	*Enabled* *Disabled*

Configuration Data Profile		*Not Configured* Set this policy to Enable to allow the verification and exclusion of BCD
Verify Additional BCD Settings	String	*String* Specify the additional Boot Configuration settings. To use this policy, Use Enhanced Boot Configuration Data Profile must Enabled.
Exclude Additional BCD Settings	String	*String* Exclude specific Boot Configuration settings. To use this policy, Use Enhanced Boot Configuration Data Profile must Enabled.
Configure TPM Platform Validation Profile	Not Selected	*Selected* *Not Selected* Set to Selected to enable boot up TPM drive unlocking for Windows 7 a Server 2008 R2. Selected allows the configuration of how the TPM secu hardware secures the BitLocker encryption key. This policy does not ap computer does not have a compatible TPM or if BitLocker has already b on with TPM protection. This policy must be set to Selected to use the policy Configure Specific Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK more information.
Configure Specific TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off PCR4,on PCR5,on PCR6,off PCR7,off PCR8,on PCR9,on PCR10,on PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off PCR22,off	This policy allows you to configure how the computer's TPM security ha secures the BitLocker encryption key. This policy setting does not appl computer does not have a compatible TPM or if BitLocker has already b on with TPM protection. This setting determines what values the TPM r when it validates early boot components before unlocking a drive on a running Windows 7 or Windows Server 2008 R2. More... If you enable this policy before turning on BitLocker, you can configure components that the TPM will validate before unlocking access to the E encrypted operating system drive. If any of these components change v BitLocker protection is in effect, the TPM will not release the encrypti unlock the drive and the computer will instead display the BitLocker re console and require that either the recovery password or recovery key to unlock the drive. If you disable or do not configure this policy, the TPM uses the default validation profile or the platform validation profile specified by the se platform validation profile consists of a set of Platform Configuration R (PCR) indices ranging from 0 to 23. The default platform validation pro the encryption key against changes to the Core Root of Trust of Measur (CRTM), BIOS, and Platform Extensions (PCR 0), the Option ROM Code (Master Boot Record (MBR) Code (PCR 4), the NTFS Boot Sector (PCR 8), Boot Block (PCR 9), the Boot Manager (PCR 10), and the BitLocker Acce (PCR 11). The descriptions of PCR settings for computers that use an Ex Firmware Interface (EFI) are different than the PCR settings described computers that use a standard BIOS. The BitLocker Drive Encryption De Guide on Microsoft TechNet contains a complete list of PCR settings fo and standard BIOS. **Warning:** Changing from the default platform validation profile affects and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depe inclusion or exclusion (respectively) of the PCRs. To use this policy, Configure TPM Platform Validation Profile must be s
Configure BIOS TPM Platform Validation Profile	Not Selected	Selected Not Selected Set to Selected to enable boot up BIOS TPM drive unlocking. Selected a configuration of how the BIOS TPM security hardware secures the BitLo encryption key. This policy does not apply if the computer does not ha compatible TPM or if BitLocker has already been turned on with TPM p This policy must be set to Selected to use the policy Configure Specific Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK

		more information.
Configure Specific BIOS TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off PCR4,on PCR5,off PCR6,off PCR7,off PCR8,on PCR9,on PCR10,on PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off PCR22,off	This policy setting allows you to configure how the computer's TPM sec hardware secures the BitLocker encryption key. This setting determine values the TPM measures when it validates early boot components befo an operating system drive on a computer with BIOS configuration or wi firmware that has the Compatibility Support Module (CSM) enabled. If you enable this policy before turning on BitLocker, you can configure components that the TPM will validate before unlocking access to the E encrypted operating system drive. If any of these components change v BitLocker protection is in effect, the TPM will not release the encrypti unlock the drive and the computer will instead display the BitLocker re console and require that either the recovery password or recovery key to unlock the drive. To use this policy, Configure BIOS TPM Platform Validation Profile must Selected.
Configure UEFI TPM Platform Validation Profile	Not Selected	*Selected* *Not Selected* Set to Selected to enable boot up UEFI TPM drive unlocking. Selected a configuration of how the UEFI TPM security hardware secures the BitLo encryption key. This policy does not apply if the computer does not ha compatible TPM or if BitLocker has already been turned on with TPM p This policy must be set to Selected to use the policy Configure Specific Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK_ for more information.
Configure Specific UEFI TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off PCR4,on PCR5,off PCR6,off PCR7,off PCR8,off PCR9,off PCR10,off PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off	This policy setting allows you to configure how the computer's TPM sec hardware secures the BitLocker encryption key. This setting determine values the TPM measures when it validates early boot components befo an operating system drive on a computer with native UEFI firmware co If you enable this policy before turning on BitLocker, you can configure components that the TPM will validate before unlocking access to the E encrypted operating system drive. If any of these components change v BitLocker protection is in effect, the TPM will not release the encrypti unlock the drive and the computer will instead display the BitLocker re console and require that either the recovery password or recovery key to unlock the drive. To use this policy, Configure UEFI TPM Platform Validation Profile must Selected.

	PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off PCR22,off	
See basic settings		
Bitlocker Encryption - Removable Storage Settings		
Allow User to Apply BitLocker Protection on Removable Drives	Selected	*Selected* *Not Selected* When Selected, users are permitted to run the BitLocker setup wizard removable data drive.
Allow User to Suspend and Decrypt BitLocker Protection on Removable Data Drives	Not Selected	*Selected* *Not Selected* When Selected, users are authorized to suspend and decrypt BitLocker on removable data drives.
Configure Use of Smart Cards on Removable Data Drives	Allow	*Allow* *Disallow* *Require* This policy specifies whether smart cards can be used to authenticate BitLocker removable data drives. These settings are enforced when tur BitLocker, not when unlocking a drive. BitLocker will allow unlocking a any of the protectors available on the drive.
Deny Write Access to Removable Drives Not Protected by BitLocker	Enabled	*Enabled* *Disabled* *Enabled for Organization* If this policy is enabled, all removable drives that are not BitLocker pro be mounted as read only. If this policy is disabled, all removable drives computer will be mounted with read and write access.
Allow Access to BitLocker Protected Removable Data Drives from Earlier Versions of Windows	Selected	*Selected* *Not Selected* When Selected, removable data drives with the FAT file system can be computers running Windows Server 2008, , or XP SP3 and their content viewed. This policy does not apply to drives that are formatted with th system.
Do Not Install BitLocker to Go Reader on FAT formatted Removable Drives	Selected	*Selected* *Not Selected* If this policy is Not Selected, removable data drives formatted with the system that are BitLocker protected cannot be unlocked on computers Windows Server 2008, , or XP SP3. Bitlockertogo.exe will not be install
Configure Use of Passwords for Removable Data Drives	Allow	*Allow* *Require* *Disallow* This policy specifies whether a password is required to unlock BitLocke data drives. These settings allow the use of a password, require the us password, or disallow the use of a password. This policy must be set to Allow or Require to use the Configure Passwo Complexity for Removable Data Drives and Minimum Password Length f Removable Data Drives polices.
Configure Password Complexity for Removable Data Drives	Allow	*Allow* *Require* *Disallow* When set to Require, a connection to a domain controller is necessary the complexity of the password. When set to Allow, a connection to a

		controller will be attempted to validate complexity, but if no domain c found, the password will still be accepted. When set to Do Not Allow, r complexity validation will be done. To use this policy, Configure Use of Passwords for Removable Data Driv set to Allow or Require.
Minimum Password Length for Removable Data Drives	8	*8-20 characters* Passwords must be at least 8 characters in length, with a maximum of characters. To use this policy, Configure Use of Passwords for Removable Data Driv set to Allow or Require.
Encryption Type for Removable Data Drives	Full Encryption	*Allow User to Choose* *Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for Removable Data Drives.
Choose How BitLocker-protected Removable Drives Can be Recovered	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, ever value is Not Selected. This policy allows for the control of how BitLock removable data drives are recovered in the absence of the required cre More... This policy is the parent policy to: Allow Data Recovery Agent for Protected Removable Data Drives Configure User Storage of BitLocker 48-digit Recovery Password Configure User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard for Removable Save BitLocker Recovery Information to AD DS for Removable Data Driv BitLocker Recovery Info to Store in AD DS for Removable Data Drives Do Not Enable BitLocker Until Recovery Info is Stored in AD DS for Rem
Allow Data Recovery Agent for Protected Removable Data Drives	Selected	*Selected* *Not Selected* When Selected, a data recovery agent is allowed for use with BitLocker removable data drives. Before the agent can be used, it must be added Public Key Policies in either the Group Policy Management Console or t Group Policy Editor. To use this policy, Choose How BitLocker-protected Removable Drives C Recovered must be to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Allow* *Require* *Do Not Allow* This policy configures if a user is allowed, required, or not allowed to g 48-digit password. To use this policy, Choose How BitLocker-protected Removable Drives C Recovered must be to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Allow* *Require* *Do Not Allow* This policy configures if a user is allowed, required, or not allowed to g 256-bit recovery key. To use this policy, Choose How BitLocker-protected Removable Drives C Recovered must be to Selected.
Omit Recovery Options from the BitLocker Setup Wizard for Removable Media	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options w BitLocker is enabled. Recovery options for the drive are determined by settings. To use this policy, Choose How BitLocker-protected Removable Drives C Recovered must be to Selected.

Save BitLocker Recovery Information to AD DS for Removable Data Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS fo data drives. The appropriate schema extensions and access control set domain must be first configured before AD DS backup can succeed. To use this policy, Choose How BitLocker-protected Removable Drives C Recovered must be to Selected. Set this policy to Selected to use the policy BitLocker Recovery Informa Store in AD DS for Removable Data Drives.
BitLocker Recovery Information to Store in AD DS for Removable Data Drives	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key p storing the recovery password only in AD DS. The appropriate schema e and access control settings on the domain must be first configured befo this policy. To use this policy, Choose How BitLocker-protected Removable Drives C Recovered must be to Selected. To use this policy, Save BitLocker Recovery Information to AD DS for Re Data Drives must be set to Selected.
Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Removable Data Drives	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically stored in the Management Console, this policy additionally requires BitLocker drive e recovery information to be stored in AD DS. Note that the appropriate extensions and access control settings on the domain must be configure using this policy. This policy is used to prevent users from enabling BitLocker unless the connected to the domain and the backup of the BitLocker recovery info AD DS has succeeded. To use this policy, Choose How BitLocker-protected Removable Drives C Recovered must be to Selected.
Configure Use of Hardware-Based Encryption for Removable Data Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on re data drives.
Use Hardware-Based Encryption for Removable Data Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption on removable data drives To use this policy, Configure Use of Hardware-Based Encryption for Rem Data Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Removable Data Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on removable da hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Rem Data Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Removable Data Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for Bit hardware encryption. To use this policy, Configure Use of Hardware-Based Encryption for Rem Data Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	*String -* *2.16.840.1.101.3.4.1.2;* *2.16.840.1.101.3.4.1.42*

Settings on Removable Data Drives		Specific Crypto Algorithms and Cipher Suites allowed. To use this policy, Configure Use of Hardware-Based Encryption for Rem Data Drives must be set to Selected.
See basic settings		
Policy	**Default Setting**	**Description**
Server Encryption		
Server Encryption	On	*On* *Off* This policy enables or disables System Data Encryption (SDE) and Comm Encryption on the client server. Toggle to ON to enable both System Data Encryption (SDE) and Commo Encryption. Changing the value of this policy triggers a new sweep to encrypt/decr
Allow Software Server Encryption	Selected	*Selected* *Not Selected* Selected means that the Server allows client server endpoint activation Enterprise level. This policy may be set to Not Selected to block activations during initia setup and maintenance interruptions.
Max Network Failed Attempts	3	*1-10* Number of successive failed attempts for the client server to connect t Server before the Encryption client locks the encryption keys.
Retry Interval to connect to DDP Server	5	*1-60 minutes* Time interval for the client server to attempt to connect to Dell Server
Retry if Authentication Fails Upon Network Failure	Selected	*Selected* *Not Selected* If Selected, the client server continues to attempt to contact Dell Serv first attempt fails due to a network failure.
Retry Interval Upon Network Failure	10	*10-60 minutes* The length of time between attempts to contact Dell Server if the first fails due to a network failure. The *Retry if Authentication Fails Upon N Failure* policy must be set to Selected for this policy to be enforced.
Server Maintenance Schedule	Not Selected	This policy is the "master policy" for all other Server Maintenance polic policy is Not Selected, no Server Maintenance policies are enforced, re other policy values. Selected allows a maintenance schedule to control application of polic requires a reboot.
Server Maintenance Schedule Repeats	Weekly	*Daily, Weekly, Monthly, Quarterly, Annually* The schedule configuration defines when the task should run. Schedule Daily, Weekly, Monthly, Quarterly, and Annually. Daily: Runs the task every day at the specified Server Maintenance Sch Time. Weekly: Runs the task weekly on the days specified in Server Maintena the Week. Monthly: Runs the task monthly on the specified Server Maintenance Da Month. Quarterly: Runs the task quarterly on the specified Server Maintenance Month. Annually: Runs the task annually on the specified Server Maintenance D Month.
Server Maintenance	21:00	String - format is [HH:mm]. Example: 11:59 PM

Schedule Start Time		The time the task should run.
Server Maintenance Day of the Week	Saturday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Server Maintenance Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
Infinite Suppress	Not Selected	When Selected, an automatic reboot is suppressed indefinitely.
Port Control System	Disabled	Enable or Disable all Port Control System policies. If this policy is set to Port Control System policies are applied, regardless of other Port Contr policies. **Note**: PCS policies require a reboot before the policy takes effect.
Port: Express Card Slot	Enabled	Enable, Disable, or Bypass ports exposed through the Express Card Slot
Port: USB	Enabled	Enable, Disable, or Bypass port access to external USB ports. **Note:** USB port-level blocking and HID class-level blocking is **only** hono can identify the computer chassis as a laptop/notebook form-factor. W the computer's BIOS for the identification of the chassis.
Port: eSATA	Enabled	Enable, Disable, or Bypass port access to external SATA ports.
Port: PCMCIA	Enabled	Enable, Disable, or Bypass port access to PCMCIA ports.
Port: Firewire (1394)	Enabled	Enable, Disable, or Bypass port access to external Firewire (1394) ports
Port: SD	Enabled	Enable, Disable, or Bypass port access to SD card ports.
Port: Memory Transfer Device (MTD)	Enabled	Enable, Disable, or Bypass access to Memory Transfer Device (MTD) por
Class: Storage	Enabled	PARENT to the next 3 policies. Set this policy to Enabled to use the nex Storage polices. Setting this policy to Disabled disables all 3 Subclass S policies - no matter what their value.
Subclass Storage: External Drive Control	Full Access	CHILD of Class: Storage. Class: Storage must be set to Enabled to use th This policy interacts with the Removable Storage - EMS Access to unShi policy. If you intend to have Full Access to media, also set this policy t to ensure that the media is not set to read only and the port is not bloc Full Access: External Drive port does not have read/write data restricti Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Subclass Storage: Optical Drive Control	UDF Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use th Full Access: Optical Drive port does not have read/write data restrictio UDF Only: Blocks all data writes that are not in the UDF format (CD/DV ISO burning). Read data is enabled. Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy. Universal Disk Format (UDF) is an implementation of the specification k ISO/IEC 13346 and ECMA-167 and is an open vendor-neutral file system computer data storage for a broad range of media. To encrypt data written to CD/DVD media: Set EMS Encrypt External Media = Selected, EMS Exclude CD/DVD Encry Selected, and Storage Class: Optical Drive Control = UDF Only.
Subclass Storage: Floppy Drive Control	Read Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use th Full Access: Floppy Drive port does not have read/write data restrictio

		Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Class: Windows Portable Device (WPD)	Disabled	PARENT to the next policy. Set this policy to Enabled to use the Subcla Portable Device (WPD): Storage policy. Setting this policy to Disabled o Subclass Windows Portable Device (WPD): Storage policy - no matter w value. Control access to all Windows Portable Devices.
Subclass Windows Portable Device (WPD): Storage	Full Access	CHILD of Class: Windows Portable Device (WPD) . Class: Windows Porta (WPD) must be set to Enabled to use this policy. Full Access: Port does not have read/write data restrictions applied. Read Only: Allows read capability. Write data is disabled. Blocked: Port is blocked from read/write capability.
Class: Human Interface Device (HID)	Enabled	Control access to all Human Interface Devices (keyboards, mice). **Note:** USB port-level blocking and HID class-level blocking is **only** hono can identify the computer chassis as a laptop/notebook form-factor. W the computer's BIOS for the identification of the chassis.
Class: Other	Enabled	Control access to all devices not covered by other Classes.
EMS Encrypt External Media	Not Selected	This policy is the "master policy" for all Removable Storage policies. A value means that no encryption of removable storage takes place, rega other policy values. A Selected value means that all Removable Storage encryption policies enabled.
EMS Exclude CD/DVD Encryption	Not Selected	Not Selected encrypts CD/DVD devices.
EMS Access to unShielded Media	Read Only	*Block, Read Only, Full Access* Note that this policy interacts with the Port Control System - Storage C External Drive Control policy. If you intend to set this policy to Full Acc that Storage Class: External Drive Control is not set to Read Only or Blo More... When this policy is set to Block Access, you have no access to removab unless it is encrypted. Choosing either Read-Only or Full Access allows you to decide what ren storage to encrypt. If you choose not to encrypt removable storage and this policy is set to you have full read/write access to removable storage. If you choose not to encrypt removable storage and this policy is set to you can read or delete existing files on the unencrypted removable sto the Shield will not allow any files to be edited on, or added to, the ren storage.
EMS Encryption Algorithm	AES256	*AES 256, AES 128, 3DES* Encryption algorithm used to encrypt removable storage. Encryption algorithms in order of speed, fastest first, are AES 128, AES
EMS Automatic Authentication	Local	*Disabled, Enable Local, Enable Roaming* Local automatic authentication allows the Shielded media to be autom authenticated when inserted in the originally Shielding computer when of that media is logged in. When automatic authentication is disabled, always manually authenticate to access Shielded media. Disabling Roaming Authentication helps to prevent users from forgettin password when they take the media home or share it with a colleague. Roaming Authentication also promotes a sense of awareness from a sec perspective for users that the data being written to that media is prote
EMS Scan External Media	Not Selected	Selected allows EMS to scan removable storage every time removable s inserted. When this policy is Not Selected and the EMS Encrypt External Media po

		Selected, EMS only encrypts new and changed files. See EMS Encryption Rules if changing this policy to Selected. Do not en policy without applying EMS Encryption Rules also. More... A scan occurs at every insertion so that EMS can catch any files added removable storage without authenticating. You can add files to the rem storage if you decline to authenticate, but you cannot access encrypte files added will not be encrypted in this case, so the next time you aut the removable media to work with encrypted data, EMS scans it and en files that may have been added without encryption.
EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable storag the endpoint is Shielded or not. More... When this policy is False, the user will be able to work with encrypted logged on to any Shielded endpoint, regardless of the Enterprise Server activated against. The user will not be able to work with encrypted da unShielded device.

EMS Device Whitelist		*String - Maximum of 150 devices with a maximum of 500 characters p PNPDeviceID. Maximum of 2048 total characters allowed. "Space" and " characters used count in the total characters used.*
		This policy allows the specification of removable storage devices to ex EMS encryption [using the removable storage device's Plug and Play dev identifier (PNPDeviceID)], thereby allowing users full access to the spe removable storage devices.
		More...
		This policy is available on an Enterprise, Domain, Group, and User leve local settings override inherited settings. If a user is in more than one EMS Device Whitelist entries, across all Groups, apply.
		Note: This policy is particularly useful when using removable storage d provide hardware encryption. However, this policy should be used with This policy does not check whether external media devices on this list hardware encryption. Whitelisting removable storage devices which do hardware encryption will not have enforced security and will not be pr
		For example, the Kingston® DataTraveler® Vault Privacy model enforc encryption is enabled to use the device. However, the Kingston DataTr model has an unsecured partition and a secured partition. Because it i physical removable storage device with only one PNPDeviceID, the two cannot be distinguished, meaning that whitelisting this particular rem storage device would allow unencrypted data to leave the endpoint.
		Additionally, if an removable storage device is protected by EMS and s added to the EMS Device Whitelist policy, it remains encrypted and re reformat of the removable storage device to remove encryption.
		The following is an example of a PNPDeviceID, which contains the man identifier, product identifier, revision, and hardware serial number:
		`USBSTOR\DISK&VEN_KINGSTON &PROD_DTVAULT_PRIVACY& REV_104\07005B831A0004B4&0`
		To whitelist a removable storage device, provide a string value which r portions of the device's PNPDeviceID. Multiple device PNPDeviceIDs are
		For example, to whitelist all Kingston DataTraveler Vault Privacy mode string:
		`PROD_DTVAULT_PRIVACY`
		To whitelist both models of Kingston DataTraveler, the Vault and Vault models, input the string:
		`PROD_DTVAULT_PRIVACY; PROD_DT_VAULT`
		Note that space characters are considered part of the substring to mat PNPDeviceID. Using the previous PNPDeviceID as an example, a space b after the semicolon would cause neither of the substrings to be matche the space character is not part of the PNPDeviceID.
		Instructions...

		To find the PNPDeviceID for removable storage: 1. Insert the removable storage device into a Shielded compute 2. Open the EMSService.log in C:\Programdata\Dell\Dell Protection\Encryption\EMS. 3. Find PNPDeviceID= For example: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDevicel USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_04 KJ&0 VEN=Vendor; Green highlighted text is for the vendor excluded PROD=Product/Model Name; Adding text highlighted excludes all of Seagate's USB drives REV=Firmware Revision; Adding text highlighted gray excludes the specific model being used Serial number (in this example); Adding text highlight excludes just this device OR *To find the PNPDeviceID for removable storage on Windows 7 or later:* 1. Insert the removable storage device. 2. Open the Control Panel and go to Administrative Tools > Cor Management. 3. Select the Hardware tab, select the drive, and click Pr 4. A new windows displays. Select the Device Instance P Property drop-down menu. The PNPDeviceID is displayed in the Value field. *To find the PNPDeviceID for removable storage on Windows XP:* 1. Click Start > Run... 2. Type msinfo32 and click Enter. 3. When the System Information window displays, go to Compo A list of USB devices and their PNPDeviceIDs displays. **Available Delimeters:** Tabs Commas Semi colons Hex character 0x1E (Record separator character)
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.
EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in th
EMS Number of Characters. Required in Password	8	*1-40 characters* Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	Selected	Selected requires one or more numeric characters in the password.

EMS Password Attempts Allowed	3	*1-10* Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.
EMS Access and Device Code Length	16	*8, 16, 32* Number of characters access and device codes have. 32 characters is th secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	*1-10* Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	*Apply Cooldown, Wipe Encryption Keys* Action to take following unsuccessful Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the spe cooldown period (Cooldown Time Delay and Cooldown Time Increment • Wipe Encryption Keys to have the Shield delete the encryption keys o removable storage, making the encrypted data inaccessible until the ow the media to a Shielded computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	*String - 5-512 characters - Authentication Failed: Please contact your s administrator.* Message that displays when a user needs to contact you for an access c authentication failure). More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as used. Messages over the 512 character limit are truncated on the clien We recommend that you customize the second sentence of the messag specific instructions about how to contact a Help Desk or Security Adm authentication failures.
EMS Cooldown Time Delay	30	*0-5000 seconds* Number of seconds the user must wait between the first and second ro access code entry attempts.
EMS Cooldown Time Increment	20	*0-5000 seconds* Incremental time to add to the previous cooldown time after each unsu round of access code entry attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	*String - 5-512 characters - You are not authorized to use this media. P contact your system administrator.* Message that displays following unsuccessful Access Code Attempts Allo More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as used. Messages over the 512 character limit are truncated on the clien We recommend that you customize the message to include specific ins about how to contact the Help Desk or Security Administrator.
EMS Encryption Rules	String	Encryption rules to be used to encrypt/not encrypt certain drives, dire folders. A total of 2048 characters are allowed. "Space" and "Enter" characters u lines between rows count as characters used. Any rules exceeding the 2 are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as USB, eSATA, etc. may require the use of both EMS and encryption rules the endpoint. This is necessary due to differences in how the Windows system handles storage devices based on interface type.

		To ensure encrypting an iPod via EMS does not make the device unusab following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories ab the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx encrypted in the directories excluded from encryption via the previous ^R#:\Calendars ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx .xlsx ^R#: \iPod_Control ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx Replacing these five rules with the following rule will force encryption pptx, doc, docx, xls, and xlsx files in any directory on the iPod, includi Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file type removable devices - not just an iPod. Use care when defining rules to e iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation iPod Mini 4gb second generation We do not recommend the use of the iPod Shuffle, as unexpected resul occur. As iPods change, this information could also change, so caution is advis allowing the use of iPods on EMS-enabled computers. Because folder names on iPods are dependent on the model of the iPod recommend creating an exclusion encryption policy which covers all fo across all iPod models.
EMS Block Access to UnShieldable Media	Selected	Block access to any removable storage that is less than 55 MB and thus insufficient storage capacity to host a Removable Media Shield (such as floppy disk). More... All access is blocked if Encrypt External Media and this policy are both Encrypt External Media is True, but this policy is False, data can be rea unShieldable removable storage, but write access to the media is block If Encrypt External Media is False, then this policy has no effect and ac unShieldable removable storage is not impacted.
SDE Encryption Enabled	Not Selected	This policy is the "master policy" for all other System Data Encryption (policies. If this policy is Not Selected, no SDE encryption takes place, r other policy values. A Selected value means that all data not encrypted by other Intelligen

		policies will be encrypted per the SDE Encryption Rules policy. More... Changing the value of this policy requires a reboot. If an endpoint computer comes equipped with an HCA and you choose t HCA policies, all SDE policies are ignored. Likewise, if you enable SDE p later decide to enable HCA policies, SDE issues a decryption policy befo policies are implemented. HCA and SDE cannot coexist on the same co
SDE Encryption Algorithm	AES256	*AES 256, AES 128, 3DES* Encryption algorithm used to for System Data Encryption. Encryption algorithms in order of speed, fastest first, are AES 128, AES
SDE Encryption Rules	String F#:\ -^%ENV:SYSTEMDRIVE%\System Volume Information -^%ENV:SYSTEMROOT%\;dll.exe.sys.ocx.man.cat.manifest.policy -^%ENV:SYSTEMROOT%\System32 -^%ENV:SYSTEMROOT%\SysWow64 -^%ENV:SYSTEMROOT%\WinSxS -^%ENV:SYSTEMROOT%\Fonts ^3@%ENV:SYSTEMROOT%\SYSTEM32\;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\cmd.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\autochk.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\winresume.exe;exe -^F#:\bootmgr -^F#:\boot	Encryption rules to be used to encrypt/not encrypt certain drives, dire folders. See Encryption Rules for information. SDE Encryption Rules may be changed as appropriate for your environm However, these defaults have been tested extensively. Removing these may result in Windows issues, particularly after applying patch updates Contact Customer Support for guidance if you are unsure about changi values.
Encryption Enabled	Selected	This policy is the "master policy" for all Common Encryption policies. A check box means that no Common Encryption takes place, regardless o policy values. A checked box means that all Common Encryption policies are enabled Changing the value of this policy triggers a new sweep to encrypt/decr
Common Encrypted Folders	String %ENV:SYSTEMDRIVE%\;accdb.doc.docm.docx.mdb.pdf.ppam.pps.ppsm.ppsx .ppt.pptm.pptx.pub.puz.sldm.sldx.tif.tiff.vdx.vsd.vss.vst.vsx.vtx.xlam .xlm.xls.xlsb.xlsm.xlsx.xsf.zip.rar %ENV:USERPROFILE%\Desktop %ENV:USERPROFILE%\Download -^%ENV:SYSTEMDRIVE%\;dat.ini.xml.txt.log.db.lnk	*String - maximum of 100 entries of 500 characters each (up to a maxim characters)* A list of folders on endpoint drives to be encrypted or excluded from e which can then be accessed by all managed users who have access to t See Encryption Rules for information. More... The available drive letters are: #: Refers to all drives f#: Refers to all fixed (non-removable) drives r#: Refers to all removable drives **Important:** *Overriding directory protection can result in an unbootable and/or require reformatting drives.*
Common Encryption Algorithm	AES256	*AES 256, AES 128, 3DES* Encryption algorithm used to encrypt data at the endpoint (all users) le System paging files are encrypted using AES 128. Encryption algorithms in order of speed, fastest first, are AES 128, AES
Application Data Encryption List	Exe List winword.exe excel.exe	*String - maximum of 100 entries of 500 characters each* We do not recommend adding explorer.exe or iexplorer.exe to the ADE

	powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe winzip.exe winrar.exe onenote.exe onenotem.exe	unexpected or unintended results may occur. However, explorer.exe is the process used to create a new notepad file desktop using the right-click menu. Setting encryption by file extension the ADE list, provides more comprehensive coverage. Changes to this policy do not affect files already encrypted because of List process names of applications (without paths) whose new files you encrypted, separated by carriage returns. Do not use wildcards. More... The Shield encrypts all new files (not already being encrypted by Comm Encrypted Folders and User Encrypted Folders) on the current computer hard drives created by these application proc whenever they are owned by a currently- logged-on managed user. This may include files excluded from encrypt Common Encrypted Folders and/or User Encrypted Folders. The following folders and their subfolders are always excluded from en this policy: C:\Windows\system32 C:\Windows\Software Distribution C:\Windows\Security C:\System Volume Information\Program Files\Credant\(.dll.exe.sys.mac.ddp.wip.rty.nmd.inv) We strongly recommend not listing applications or installers that write critical files. Doing so could result in encryption of important system files, which could make a Windows e unbootable. Common process names: Outlook: outlook.exe Word: winword.exe FrontPage: frontpg.exe PowerPoint: powerpnt.exe Access: msaccess.exe WordPad: wordpad.exe Microsoft Paint: mspaint.exe Excel: excel.exe The following hard-coded system and installer process names are ignor specified in this policy (you can also add to this list via the registry value HKLM\Software\Dell\ CMGShield\EUWPrivilegedList): hotfix.exe, a Windows update process update.exe, a Windows update process setup.exe, a third-party installer process msiexec.exe, a third-party installer process wuauclt.exe, a Windows update process wmiprvse.exe, a Windows system process migrate.exe, a Windows update process unregmp2.exe, a Windows update process ikernel.exe, a third-party installer process wssetup.exe, the Windows Shield installer svchost.exe, a Windows system process
Encrypt Temporary Files	Not Selected	Selected encrypts the paths listed in the environment variables TEMP a TEMP and TMP for the OS are encrypted with the Common Encryption K To reduce encryption sweep time, the Shield clears the contents of the TMP folders for initial encryption, as well as updates to this policy. Ho your organization uses a third-party application that requires the file s

		within the \temp directory to be preserved, you should prevent this de To disable temporary file deletion, create DeleteTempFiles (REG_DWO its value to 0 in the registry at HKLM\SOFTWARE\Dell\CMGShield.
Encrypt User Profile Documents	Selected	Selected encrypts all shared files and public folders with the Common Key
Encrypt Windows Paging File	Selected	Selected encrypts the Windows paging file. A change to this policy requ reboot.
Managed Services	null	*String - maximum of 100 entries of 500 characters each (up to a maxim characters)* When a Service is managed by this policy, the Service is started only af is logged in and the Shield is unlocked. This policy also ensures that the managed by this policy is stopped before the Shield is locked during log policy can also prevent a user logoff if a Service is unresponsive. More... Syntax is one Service name per line. Spaces in the Service name are su Wildcards are not supported. Entries are not case-sensitive. For example, GoogleDesktop Manager is googledesktopmanager. The Service log on as setting has no bearing on whether or not the Shie control it. It does not matter if a user logs on with user credentials ver system. The startup type (Automatic or Manual) does not affect the ability of th control it. Automatic or Manual startup is acceptable. Managed Services will not be started if an unmanaged user logs on.
Secure Post-Encryption Cleanup	Single Pass Overwrite	*No Overwrite, Single-pass Overwrite, Three-pass Overwrite, Seven-pas* Once folders specified via other policies in this category have been enc policy determines what happens to the unencrypted residue of the orig • No Overwrite deletes it. This value yields the fastest encryption proc • Single-pass Overwrite overwrites it with random data. • Three-pass Overwrite overwrites it with a standard pattern of 1s and with its complement, and then with random data. • Seven-pass Overwrite overwrites it with a standard pattern of 1s and with its complement, and then with random data five times. This value most difficult to recover the original files from memory, and yields the secure encryption processing.
Secure Windows Credentials	Selected	The Windows Credentials will be secured by encrypting the entire regis exception of registry information required for computer boot. The info required for computer boot includes HKLM/SYSTEM and all sub-keys. This policy value will be automatically set to Selected if SDE is enabled When a change to this policy is delivered, the Shield requires a reboot. this reboot, configure the following policies: Force Reboot on Update, Each Reboot Delay, and Number of Reboot Delays Allowed.
Block Unmanaged Access to Domain Credentials	Selected	This policy prevents unmanaged applications from accessing the Windo credentials when a user is logged in.
Secure Windows Hibernation File	Not Selected	When enabled, the hibernation file will be encrypted only when the co enters hibernation. The Shield will disengage protection when the com out of hibernation, providing protection without impacting users or app while the computer is in use.
Prevent Unsecured Hibernation	Not Selected	When enabled, the Shield will not allow computer hibernation if the Sh unable to encrypt the hibernation data.
Workstation Scan Priority	Lowest	*Highest, High, Normal, Low, Lowest* Specifies the relative Windows priority of encrypted folder scanning. H Highest prioritize scanning speed over computer responsiveness, Low a prioritize computer responsiveness over scanning speed and favor othe intensive activities, and Normal balances the two.

		The Shield checks for a changed Workstation Scan Priority before proce next file. The scan priority levels are used in two different ways. 1. These values correspond with the values used by the Microso set thread execution priority. 2. The Shield uses these values to introduce a delay in the encr sweep after every single file is processed. The values translate to the following millisecond delay ranges encryption thread will sit idle and then return full control to t operating system: Highest=0 ms / Lowest=100 ms
Policy Proxy Connections	String	String - maximum of 1500 characters List fully qualified Policy Proxy hostnames, or IP addresses, separated returns. More... Once the Shield finds a valid entry, the remainder of the entries are ig Entries are processed in the following order: 1. GKConnections Override (this registry entry overrides all other entri 2. GKConnections (this registry entry is set automatically by the Shield the this policy) 3. GK This policy works in conjunction with the Policy Proxy Polling Interval p To override this policy and specify ports via the registry item HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CMGShield\GKConnectionsOverride. You cannot specify ports in this policy. The Shield communicates with Policy Proxies using the GKPORT specifi Shield installation (the default is 8000). If necessary, change that port via the registry item HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\ CMGShield\GKPort. Inherited values for this policy accumulate. In order for the Shield to connect to a Policy Proxy specified in this pol be in the same group as the Policy Proxy specified during Shield install Because the Shield supports up to 255 users per endpoint, this policy is only at the Enterprise Policies level.
Policy Proxy Polling Interval	720	1-1440 minutes The interval that the Shield attempts to poll Policy Proxy for policy up send inventory information to Policy Proxy. The Shield also attempts to poll Policy Proxy each time a user logs on.
See basic settings		

Variables

Some Windows policies support the following variables. A pathname can consist entirely of one or more of these variables, or can include one or more of these variables at any point.

To get directory locations that these CSIDL values resolve to, go to http://msdn.microsoft.com/en-us/library/bb762494.aspx. All names listed on the MSDN page are CSIDL_<name>.

Note: Some operating systems have different CSIDL values, such as Windows 7 having values that Windows XP does not.

%CSIDL:name%

- Includes any of the following Windows CSIDL constants:

DESKTOP

INTERNET

PROGRAMS

CONTROLS

PRINTERS

PERSONAL

FAVORITES

STARTUP

RECENT

SENDTO

STARTMENU

STARTMENU

MYDOCUMENTS

MYMUSIC

MYVIDEO

DESKTOPDIRECTORY

DRIVES

NETWORK

NETHOOD

FONTS

TEMPLATES

COMMON_STARTMENU

COMMON_PROGRAMS

COMMON_STARTUP

COMMON_DESKTOPDIRECTORY

APPDATA

PRINTHOOD

LOCAL_APPDATA

ALTSTARTUP

COMMON_ALTSTARTUP

COMMON_FAVORITES

INTERNET_CACHE

COOKIES

HISTORY

COMMON_APPDATA

WINDOWS

SYSTEM

PROGRAM_FILES

PROGRAMFILES

MYPICTURES

PROFILE

SYSTEMX86

PROGRAM_FILESX86

PROGRAMFILESX86

PROGRAM_FILES_COMMON

PROGRAM_FILES_COMMONX86

COMMON_TEMPLATES

COMMON_DOCUMENTS

COMMON_ADMINTOOLS

ADMINTOOLS

CONNECTIONS

COMMON_MUSIC

COMMON_PICTURES

COMMON_VIDEO

RESOURCES

PROFILES

%HKCU:regpath%

- Includes a numeric or text value stored in the registry for the Current User. If you specify a path but not an item, the Shield uses the default value

%HKLM:regpath%

- Includes a numeric or text value stored in the registry for the local computer. If you specify a path but not an item, the Shield uses the default value

%ENV:envname%

- Includes the value of a Windows local environment variable

%%

- Includes the % character

Windows Policies that Require Reboot

- SDE Encryption Enabled

- Encrypt Windows Paging File
- Secure Windows Credentials
- All PCS policies

Windows Policies that Require Logoff

- SDE Encryption Enabled
- User state change to Suspended
- EMS Encrypt External Media
- EMS Scan External Media
- EMS Encryption Algorithm
- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Advanced Threat Prevention

Threat Prevention policies are available at the Enterprise, Endpoint Group, and Endpoint levels.

Policy descriptions also display in tooltips in the Remote Management Console. In this table, master policies are in bold font.

See Advanced Threat Prevention Features by Operating System for information about support for Advanced Threat Prevention features on Windows and Mac operating systems

Policy	Default Setting	Description
Advanced Threat Prevention		
Advanced Threat Prevention	Off	*On* *Off* Toggle ON to enable Advanced Threat Prevention. If this policy is toggled to OFF, Advanced Threat Prevention is disabled, regardless of other policies.
File Actions		
File Action: Unsafe Executable Auto Quarantine With Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Unsafe executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices under a test policy in order to observe the behavior and ensure that no business-critical applications are blocked at execution.
File Action: Unsafe Executable Auto Upload Enabled	Selected	*Selected* *Not Selected* If selected, any detected Unsafe file is automatically uploaded for a deeper analysis and additional details about the file.
File Action: Abnormal Executable Auto Quarantine With Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Abnormal executable files are automatically quarantined or blocked to prevent their execution.

		Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices under a test policy in order to observe the behavior and ensure that no business-critical applications are blocked at execution.
File Action: Abnormal Executable Auto Upload Enabled	Selected	*Selected* *Not Selected* If selected, any detected Abnormal file is automatically uploaded for a deeper analysis and additional details about the file.
Allow Execution of Files in Exclude Folders	Not Selected	*Selected* *Not Selected* If selected, executable files are allowed to run, even though they are not in folders excluded in the Exclude Specific Folders policy.
Memory Actions		
Memory Action: Memory Protection Enabled	Not Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Memory Protection policies. If this policy is Not Selected, no Memory Action policies are enforced, regardless of other policy values. NOTE: Before enabling Memory Protection, enable Compatibility Mode, to ensure applications function properly on the client computer. For instructions on how to enable Compatibility Mode, see Enable Compatibility Mode for Memory Protection. Compatibility Mode does not apply to Mac clients.
Memory Action: Enable Exclude executable files	Selected	*Selected* *Not Selected* Allows specific process files to be excluded from Memory Protection. This policy must be selected, to use the policy Memory Action: Exclude executable files.
Memory Action: Exclude executable files	String \Windows\System32\CmgShieldService.exe \Windows\System32\EMSService.exe	String - Example: \folder\file.exe Excludes specific process files from Memory Protection. This allows the specified files to run or be installed on any device on which this policy is enforced. Enter the relative paths of the files to exclude.
Memory Action: Exploitation: Stack Pivot	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a stack pivot threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Exploitation: Stack Protect	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a stack protect threat is detected.

		Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Exploitation: Overwrite Code	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when an overwrite code threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Exploitation: Scanner Memory Search	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a scanner memory search threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Exploitation: Malicious Payload	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a malicious payload is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.

Memory Action: Process Injection: Remote Allocation of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote memory allocation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote Mapping of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote attempt to map memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote Write to Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote attempt to write to memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote Write PE to Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote attempt to write a portable executable to memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run.

		Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Process Injection: Remote Overwrite Code	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote overwrite code threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Process Injection: Remote Unmap of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote memory unmapping threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Process Injection: Remote Thread Creation	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote thread creation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call.
Memory Action: Process Injection: Remote APC Scheduled	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote APC scheduled threat is detected.

		Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Process Injection: Remote DYLD Injection (Mac OS X only)	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a remote DYLD injection threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Windows clients.
Memory Action: Escalation: LSASS Read	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when an LSASS read threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the application that made the call. This policy does not apply to Mac clients.
Memory Action: Escalation: Zero Allocate	Alert	*Ignore* *Alert* *Block* *Terminate* Specifies the action to take when a zero byte allocation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the DDP Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and also terminate the

		application that made the call.
Protection Settings		
Execution Control: Prevent Service Shutdown from Device	Not Selected	*Selected* *Not Selected* If selected, the Advanced Threat Prevention service is protected from being shut down either manually or by another process.
Kill Unsafe Running Processes and Sub-Processes	Not Selected	*Selected* *Not Selected* If selected, processes and sub-processes are quarantined and terminated regardless of their state when a threat is detected (exe or dll). Although a process or sub-process is terminated, the command prompt window remains open. If a file has been determined to be Safe and allowed to run and then a threat model update occurs that results in the file being identified as unsafe, the process is automatically terminated. Dell recommends that you review threat model updates before Selecting this policy. For more information, see Threat Model Updates.
Execution Control: Background Threat Detection	Run Once	*Disabled* *Run Recurring* *Run Once* If set to Run Recurring or Run Once, a full-disk scan is run to detect and analyze any dormant threats on the disk. An upgrade to the Advanced Threat Prevention model triggers a full-disk scan.
Execution Control: Watch for New Files	Selected	*Selected* *Not Selected* If selected, any new or modified files are detected and analyzed for dormant threats. Dell recommends enabling this policy. However, If Auto Quarantine is enabled for all Unsafe or Abnormal files, all malicious files will be blocked at execution. Therefore, it is not necessary to enable this policy with Auto Quarantine mode unless you prefer to quarantine a file as it is added to a disk but before execution.
Execution Control: Set Maximum Archive File Size to Scan	150 MB	The default setting is 150 MB. Specifies the maximum size of archive (compressed) files, including .jar files to be scanned. Because scanning compressed files can negatively affect computer performance, Dell recommends setting Quick-Scan - Scan Archives and Full-Scan - Scan Archives policies to be used during off-work hours.
Enable Exclude Specific Folders (includes subfolders)	Selected	*Selected* *Not Selected* Allows specific folders to be excluded from Auto Quarantine and Auto Upload. This policy must be selected in order to use the policy, Exclude Specific Folders.
Execution Control: Exclude Specific Folders (includes subfolders)	String	*String* Folders specified in this policy are excluded from actions performed based on the policies, Background Threat

		Detection and Watch for New Files, when these features are enabled. This exclusion extends to subfolders of folders that are specified with this policy.
Application Control	Not Selected	*Selected* *Not Selected* If selected, specified devices are locked down, restricting any changes on a device after it is locked down. Only the applications that exist on a device before the lock-down occurs are allowed to execute on that device. Any new applications, as well as changes to the executables of existing applications, will be denied. The Advanced Threat Prevention agent updater is also disabled. When the Application Control policy is Selected, certain File Action, Memory Action, and Execution Control policies are automatically set. These policy settings may be changed after they are automatically set, without disabling Application Control. For a list of policies that are automatically set when the Application Control policy is Selected, see Policies Set by Application Control. To exclude specific folders from lock-down, specify the folders in the Application Control Allowed Folders policy. This policy does not apply to Mac clients.
Application Control Allowed Folders	Not Selected	*Selected* *Not Selected* Allows specific folders to be excluded from Application Control lock-down.
Enable Change Window	Not Selected	*Selected* *Not Selected* If selected, Application Control is temporarily disabled to allow, edit, and run new applications or perform updates. This includes updating the Advanced Threat Prevention agent. After performing the necessary changes, deselect Change Window. **Note:** Using Change Window retains any changes made to the Application Control settings. Deselecting Application Control and then back Selecting it resets the Application Control settings back to default. This policy does not apply to Mac clients.
Suppress Popup Notifications	Not Selected	*Selected* *Not Selected* If Selected, no popup notifications of Advanced Threat Prevention events display on the client computer.
Minimum Popup Notification Level	High	*High* *Medium* *Low* Severity level of events that result in popup notifications that display on the client computer. A setting of High allows only notifications of critical events to display. A setting of Low displays all on-screen notifications for all events. Listed below are individual examples of events that fall into the severity levels: High 1) Protection status has changed. (Protected means that the Advanced Threat Prevention service is running and protecting the computer and needs no user or administrator interaction.) 2) A threat is detected and policy is not set to automatically address the threat. Medium 1) Execution Control blocked a process from starting because it was detected as a threat. 2) A threat is detected that has an associated mitigation (for example, the threat was manually quarantined), so the process has been terminated. 3) A process was blocked or terminated due to a memory

		violation. 4) A memory violation was detected and no automatic mitigation policy is in effect for that violation type. Low 1) A file that was identified as a threat has been added to the Global Safe List or deleted from the file system. 2) A threat has been detected and automatically quarantined. 3) A file has been identified as a threat but waived on the computer. 4) The status of a current threat has changed (for example, Threat to Quarantined, Quarantined to Waived, or Waived to Quarantined).
Enable BIOS Assurance	Selected	*Selected* *Not Selected* If selected, BIOS integrity checks are performed on end user systems to validate that the BIOS has not been modified from the Dell factory version. A custom factory image cannot be used with this feature, as the BIOS has been modified. This feature is available only on Dell platforms. Platforms available with this feature include the newest release of select XPS, Latitude, Optiplex, Precision Workstations, and Venues. Speak to your Sales Associates for details or contact Dell ProSupport. This policy does not apply to Mac clients.
Script Control	Not Selected	*Selected* *Not Selected* If selected. Script Control protects devices by blocking malicious scripts from running. **Note:** Script Control is currently only available for PowerShell and Active Scripts. This policy does not apply to Mac clients.
Script Control Mode	Alert	*Alert* *Block* Alert (default) - Monitors scripts running in the environment. Recommended for initial deployment. **Block - Allow scripts to run only from specific folders. This should be used only after testing in Alert mode.** This policy does not apply to Mac clients.
Script Control Active Script	Alert	*Alert* *Block* Alert (default) - Monitors Active Scripts running in the environment. Recommended for initial deployment. **Block - Allow** Active Scripts **to run only from specific folders. This should be used only after testing in Alert mode.** This policy does not apply to Mac clients.
Script Control Macros	Alert	*Alert* *Block* Alert (default) - Monitors Office macros running in the environment. Recommended for initial deployment. **Block - Allow** Office macros **to run only from specific folders. This should be used only after testing in Alert mode.** **Note:** Starting with Office 2013, macros are disabled by default. Most of the time, users should not be required to enable macros to view the content of an Office document. Dell recommends enabling macros only for documents from trusted users. Otherwise, macros should always be disabled. This policy does not apply to Mac clients.
Script Control PowerShell	Alert	*Alert* *Block* Alert (default) - Monitors PowerShell scripts running in the environment. Recommended for initial deployment.

		Block - Allow PowerShell **scripts to run only from specific folders. This should be used only after testing in Alert mode.** This policy does not apply to Mac clients.
Script Control PowerShell Console	Allow	*Allow* *Block* Allow (default) - Allows the PowerShell console to be launched. Block - Blocks the PowerShell console from being launched. Provides additional security by protecting against the use of PowerShell one-liners. Note: If this policy is set to Block and you use a script that launches the PowerShell console, the script will fail. It is recommended that users change their scripts to invoke the PowerShell scripts, not the PowerShell console. This policy does not apply to Mac clients.
Enable Script Control Approve Scripts in Folders (and Subfolders)	Not Selected	*Selected* *Not Selected* Allows scripts stored in specific folders to be automatically approved to run. This policy must be selected in order to use the policy, Script Control Approve Scripts in Folders (and Subfolders). This policy does not apply to Mac clients.
Script Control Approve Scripts in Folders (and Subfolders)	String	*String* Folders specified in this policy are excluded from actions performed based on the Script Control policy. This exclusion extends to subfolders of folders that are specified with this policy. This policy does not apply to Mac clients.
Global Allow (available only in Disconnected mode)	String	*String* This policy will NOT be sent to the client if the Server does not detect a Disconnected mode install token. The token is prefixed with *DELLAG*. The value of this policy must include the entire contents of the policy.xml file. Copy and paste the contents of policy.xml into the policy editor and shown in this example.
Quarantine List (available only in Disconnected mode)	String	*String* This policy will NOT be sent to the client if the Server does not detect a Disconnected mode install token. The token is prefixed with *DELLAG*. The value of this policy includes a collection of hashes, represented by these JSON examples.
Safe List (available only in Disconnected mode)	String	*String* This policy will NOT be sent to the client if the Server does not detect a Disconnected mode install token. The token is prefixed with *DELLAG*. The value of this policy includes a collection of hashes, represented by these JSON examples.
Agent Logs		
Enable Auto-upload of Log Files	Not Selected	*Selected* *Not Selected* If selected, log files are automatically uploaded at 12:00 am or when their size reaches 100 MB.
See basic settings		

Policy	Default Setting	Description
Threat Protection		

Action on Malicious Activity for Processes	Block and Report	*Block Only* *Report Only* *Block and Repor*t Prevents users from stopping Threat Protection processes and sets the action to take upon attempt. Block Only: Blocks activity but does not report to the Server. Report Only: Reports activity to the Server but does not block activity. Block and Report (default): Blocks and reports activity to the Server.
Suppress Popup Notifications	Not Selected	*Selected or Not Selected* If Selected, no popup notifications of Threat Protection events display on the client computer.
Minimum Popup Notification	Major	*Critical, Major, Minor, Warning, Information* Severity level of popup notifications that display on the client computer. Information displays all on-screen notifications for all events.
Exclude Processes	String	String - Example: avtask.exe Excludes specific process files from Threat Protection scans. Enter the exact resource name of a process to exclude.
Log Files Location	<SYSTEM_DRIVE>:\ProgramData\DDP\Suite\Logs	String - File path Specifies the location for the log files. The default location is <SYSTEM_DRIVE>:\ProgramData\DDP\Suite\Logs.
Enable Activity Logging	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Threat Protection logging policies. If this policy is Not Selected, no Threat Protection logging takes place, regardless of other policy values. A Selected value enables Threat Protection logging.
Debug Logging for Malware Protection	Not Selected	*Selected* *Not Selected* A Selected value enables debug logging of Malware and Exploit Protection activity.
Debug Logging for Client Firewall	Not Selected	*Selected* *Not Selected* A Selected value enables verbose logging of Firewall activity.
Debug Logging for Web Protection	Not Selected	*Selected* *Not Selected* A Selected value enables verbose logging of Web Protection activity.
Client Update Schedule	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Client Scheduling policies. If this policy is Not Selected, no Client Scheduling takes place, regardless of other policy values. A Selected value enables the Client Scheduling options.
Client Update Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Client Update Schedule Start Time. Weekly: Runs the task weekly on the days specified in Client

		Update Day of the Week. Monthly: Runs the task monthly on the specified Client Update Day of the Month.
Client Update Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Client Update Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Client Update Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
See basic settings		
Policy	**Default Setting**	**Description**
Malware Protection		
Malware Protection	Off	*On* *Off* Toggle to ON to enable Malware Protection. If toggled to OFF, no Malware Protection policies will be applied. Malware Protection protects the critical operating system resources from changes made by malware or other unauthorized processes.
On-Access Max Seconds for Scan	45	*10 to 9999* Specifies the maximum number of seconds for each file scan. Limits each file scan to the specified number of seconds. If a scan exceeds the time limit, the scan stops and logs a message.
On-Access Scan Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.
On-Access Scan Processes on Enable	Not Selected	*Selected* *Not Selected* Rescans all processes that are currently in memory each time: - On-Access Scan is disabled and re-enabled. - The computer starts. When the on-access scanner is enabled, it always scans all processes when they are executed. Because some programs or executables start automatically when the computer starts, enabling this option can slow the computer and increase computer startup time.
On-Access Scan Trusted Installers	Not Selected	*Selected* *Not Selected* Scans MSI files or Windows Trusted Installer service files. Disable this option to improve the performance of large Microsoft application installers.
On-Access Scan When Copying Between Local Folders	Not Selected	*Selected* *Not Selected* Scans files whenever the user copies from one local folder to another. If disabled, only items in the destination folder are scanned. If enabled, items in both source and destination folders are scanned.

On-Access Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.
On-Demand Protection - Full Scan	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other On-Demand Protection: Full Scan policies. If this policy is Not Selected, no On-Demand Protection: Full Scan policies are enforced, regardless of other policy values. A Selected value means that On-Demand Protection: Full Scan is enabled. This policy must be set to Selected to enable On-Demand Protection: Full Scan settings. If this policy is Not Selected, no On-Demand Protection: Full Scan policies will be applied. By default, every time Full Scan runs, it scans the following locations for threats: - the computer memory for installed rootkits, hidden processes, and other behavior that suggests malware is attempting to hide itself. This scan occurs before all other scans. - the memory of all running processes. - all drives and their subfolders on the computer.

		By default, the scanner scans all file types, regardless of extension.
Full-Scan Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.
Full-Scan Unwanted Programs	Selected	*Selected* *Not Selected* Enables the scanner to detect potentially unwanted programs. The scanner uses configured information to detect potentially unwanted programs.
Full-Scan Decode MIME Files	Not Selected	*Selected* *Not Selected* Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
Full-Scan - Scan Archives	Selected	*Selected* *Not Selected* Examines the contents of archive (compressed) files, including .jar files. Because scanning compressed files can negatively affect computer performance, Dell recommends using this option in scans during off-work hours.
Full-Scan Files Migrated to Storage	Not Selected	*Selected* *Not Selected* Scans files that remote storage manages. When the scanner encounters a file with migrated content, it restores the file to the local computer before scanning.
Full-Scan Program Threats	Selected	*Selected* *Not Selected* Detects executable files that have code that resembles malware.
Full-Scan Macro Threats	Selected	*Selected* *Not Selected* Detects unknown macro viruses.
Full-Scan - Scan Subfolders	Selected	*Selected* *Not Selected* Examines all subfolders of the specified folder.
Full-Scan Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next content file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security

		footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.
Full-Scan Exclusions	String	String - Comma-separated list of parameters Specify files, folders, and drives to exclude from scanning. Comma separated list of parameters: <ExclusionType>,<ExclusionData>,<ExcludeSubfolders (only applies to FileOrFolder type)> Possible values: <FileOrFolder|FileType|ModifiedAge|AccessedAge|CreatedAge>,<PathToFileOrFolder|FileType|Age>,<true|false> Examples: FileOrFolder,C:\Users,false FileType,xml,false FileType,mp?,false ModifiedAge,120,true AccessedAge,150,false CreatedAge,300,true
Full-Scan Threat First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a threat is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Full-Scan Threat First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when a threat is detected if the first action fails. Clean files - Removes the threat from the detected file, if

		possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Full-Scan Exploit First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a potentially unwanted program is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Full-Scan Exploit First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when an unwanted program is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Full-Scan Use Scan Cache	Selected	*Selected* *Not Selected* A Selected value enables the scanner to use the existing clean scan results. A Selected value reduces duplicate scanning and improves performance.
Full-Scan System Utilization	Below Normal	*Low Priority* *Below Normal* *Normal* Enables the operating system to specify the amount of CPU time that the scanner receives during the scan. Each task runs independently, unaware of the limits for other tasks. Low Priority - Provides improved performance for other running applications. Select this option for computers with end user activity. Below Normal - Sets the computer utilization for the scan to the default. Normal - Enables the scan to complete faster. Select this option for computers that have large volumes and little end user activity.
Full-Scan - Scan on Battery Power	Not Selected	*Selected* *Not Selected* A Selected value allows the scan when the computer is using battery power. Not Selected postpones the scan until the computer is no longer using battery power.
Full-Scan Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Full-Scan Schedule Start Time. Weekly: Runs the task weekly on the days specified in Full-

		Scan Schedule Day of the Week. Monthly: Runs the task monthly on the specified Full-Scan Schedule Day of the Month.
Full-Scan Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Full-Scan Schedule Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Full-Scan Schedule Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
On-Demand Protection - Quick Scan	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other On-Demand Protection: Quick Scan policies. If this policy is Not Selected, no On-Demand Protection: Quick Scan policies are enforced, regardless of other policy values. A Selected value means that On-Demand Protection: Quick Scan is enabled. This policy must be set to Selected to enable On-Demand Protection: Quick Scan settings. If this policy is Not Selected, no On-Demand Protection: Quick Scan policies will be applied. By default, every time Quick Scan runs, it scans the following locations for threats: - the memory of all running processes - the files that the Windows Registry references - the contents of the Windows folder - the contents of the Temp folder By default, the scanner scans all file types, regardless of extension.
Quick-Scan Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.
Quick-Scan Unwanted Programs	Selected	*Selected* *Not Selected* Enables the scanner to detect potentially unwanted programs. The scanner uses configured information to detect potentially unwanted programs.
Quick-Scan Decode MIME Files	Not Selected	*Selected* *Not Selected* Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
Quick-Scan - Scan Archives	Selected	*Selected* *Not Selected* Examines the contents of archive (compressed) files, including .jar files. Because scanning compressed files can negatively affect computer performance, Dell recommends using this option in scans during off-work hours.
Quick-Scan Files Migrated to Storage	Not Selected	*Selected* *Not Selected* Scans files that remote storage manages. When the scanner encounters a file with migrated content, it restores the file to the local computer before scanning.

Quick-Scan Program Threats	Selected	*Selected* *Not Selected* Detects executable files that have code that resembles malware.
Quick-Scan Macro Threats	Selected	*Selected* *Not Selected* Detects unknown macro viruses.
Quick-Scan - Scan Subfolders	Selected	*Selected* *Not Selected* Examines all subfolders of the specified folder.
Quick-Scan Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next content file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.
Quick-Scan Exclusions	String	String - Comma-separated list of parameters Specify files, folders, and drives to exclude from scanning. Comma separated list of parameters: <ExclusionType>,<ExclusionData>,<ExcludeSubfolders (only applies to FileOrFolder type)>

		Possible values: <FileOrFolder|FileType|ModifiedAge|AccessedAge|CreatedAge>,<PathToFileOrFolder|FileType|Age>,<true|false> Examples: FileOrFolder,C:\Users,false FileType,xml,false FileType,mp?,false ModifiedAge,120,true AccessedAge,150,false CreatedAge,300,true
Quick-Scan Threat First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a threat is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Quick-Scan Threat First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when a threat is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Quick-Scan Exploit First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a potential exploit is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Quick-Scan Exploit First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when an exploit is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.

Quick-Scan Use Scan Cache	Selected	*Selected* *Not Selected* A Selected value enables the scanner to use the existing clean scan results. A Selected value reduces duplicate scanning and improves performance.
Quick-Scan System Utilization	Below Normal	*Low Priority* *Below Normal* *Normal* Enables the operating system to specify the amount of CPU time that the scanner receives during the scan. Each task runs independently, unaware of the limits for other tasks. Low Priority - Provides improved performance for other running applications. Select this option for computers with end user activity. Below Normal - Sets the computer utilization for the scan to the default. Normal - Enables the scan to complete faster. Select this option for computers that have large volumes and little end user activity.
Quick-Scan - Scan on Battery Power	Not Selected	*Selected* *Not Selected* A Selected value allows the scan when the computer is using battery power. Not Selected postpones the scan until the computer is no longer using battery power.
Quick-Scan Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Quick-Scan Schedule Start Time. Weekly: Runs the task weekly on the days specified in Quick-Scan Schedule Day of the Week. Monthly: Runs the task monthly on the specified Quick-Scan Schedule Day of the Month.
Quick-Scan Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Quick-Scan Schedule Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Quick-Scan Schedule Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
Access Protection	Selected	*Selected* *Not Selected* Access Protection prevents other computers from making a connection and creating or altering autorun (autorun.inf) files from CDs. The rule prevents spyware and adware distributed on CDs from being executed and will automatically block and report the issue.
Script Scan Protection	Selected	*Selected* *Not Selected* This policy enables scanning JavaScript and VBScript scripts to prevent unwanted scripts from executing. **Note:** If Script Scan Protection is disabled when Internet Explorer is launched, and then is enabled, it doesn't detect malicious scripts in that instance of Internet Explorer.
Source Sites for Update	Hyperlink	To modify the source sites your clients access for Malware

		Protection signature updates, click the **Source Sites for Updates** link. To modify the priority level or availability of an external source site, click either NAIHttp or NAIFtp, edit the necessary fields, and click **OK**. To designate an internal signature update server, see Designate a Threat Protection Signature Update Server. Designating a signature update server within your network allows client computers to obtain signature updates without accessing the Internet.
See basic settings		
Policy	**Default Setting**	**Description**
Web Protection		
Web Protection	Off	*On* *Off* Toggle to ON to enable Web Protection. If toggled to OFF, no Web Protection policies will be applied.
Enforcement - Enable HTML iFrames Support	Selected	*Selected* *Not Selected* A Selected value blocks access to malicious (Red) and warn (Yellow) sites that appear in an HTML iframe.
Enforcement - Block Sites by Default if Reputation Service Server is not Reachable	Not Selected	*Selected* *Not Selected* A Selected value blocks access to websites if Web Control cannot reach the Reputation Service server.
Enforcement - Block Phishing Pages for All Sites	Selected	*Selected* *Not Selected* A Selected value blocks all phishing pages, overriding content rating actions.
Enforcement - Specify Reputation Service Risk Level to Block	Very High	*Disable* *Very Low* *Low* *Medium* *High* *Very High* Specifies the Reputation Service risk level to block when the Threat Protection on-demand scan feature is not installed and enabled. Web Protection uses the risk level to calculate the score when retrieving the checksum reputation from the Reputation Service.
IP Exclusions for Web Protection	String	String - IP or IP Range Configures Web Protection not to rate or act on the specified private IP address range. The format is the IP address or IP address range.
Set Default Search Engine	Google	*Google* *Yahoo* *Bing* *Ask* Specifies the default search engine to use for supported browsers: Google, Yahoo, Bing, Ask.
Rating Action for Red Sites	Block	*Block* *Allow* *Warn* Specifies the action to apply to sites that are rated Red. Block: Prevents users from accessing the site and displays a message that the site is blocked. Block is the default for Red

		sites. Allow: Permits users to access the site. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. Green-rated sites and downloads are automatically allowed.
Rating Action for Yellow Sites	Warn	*Block* *Allow* *Warn* Specifies the action to apply to sites that are rated Yellow. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. Warn is the default for Yellow sites. Green-rated sites and downloads are automatically allowed.
Rating Action for Unrated Sites	Allow	*Block* *Allow* *Warn* Specifies the action to apply to sites that are Unrated. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site. Allow is the default for Unrated sites. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. Green-rated sites and downloads are automatically allowed.
Rating Action for Red Downloads	Block	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are rated Red. Block: Prevents users from downloading the file and displays a message that the download is blocked. Block is the default for Red downloads. Allow: Permits users to proceed with the download. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download.
Rating Action for Yellow Downloads	Warn	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are rated Yellow. Block: Prevents users from downloading the file and displays a message that the download is blocked. Allow: Permits users to proceed with the download. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download. Warn is the default for Yellow sites.
Rating Action for Unrated Downloads	Allow	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are Unrated.

		Block: Prevents users from downloading the file and displays a message that the download is blocked. Allow: Permits users to proceed with the download. Allow is the default for Unrated downloads. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download.
See basic settings		
Policy	**Default Setting**	**Description**
Client Firewall		
Client Firewall	Off	*On* *Off* Toggle to ON to enable Client Firewall. If toggled to OFF, no Client Firewall Settings or Rules will be applied. Client firewall is a stateful firewall.
Settings and Rules		See Client Firewall Settings and Rules.
See basic settings		

Client Firewall Settings and Rules

In the Client Firewall policy, Settings and Rules, click **View/Edit**.

In the Settings window, you can set Client Firewall Options and Client Firewall Rules.

Return to Client Firewall Policies

Client Firewall Options

Setting	UI Control	Description
Protection Options		
Allow traffic for unsupported protocols	Check box	Allows all traffic that uses unsupported protocols. When disabled, all traffic using unsupported protocols is blocked.
Allow only outgoing traffic until firewall services have started	Check box	Allows outgoing traffic but no incoming traffic until the Firewall service starts. If this option disabled, Firewall allows all traffic before services are started.
Allow bridged traffic	Check box	Allows traffic with a local MAC address. The MAC address is an address in the list of VMs that Firewall supports, not the local system's MAC address. Use this option to allow traffic through a bridged environment with virtual machines.
Enable IP spoof protection	Check box	Blocks network traffic from non-local host IP addresses or from local processes that attempt to spoof their IP address.
Enable firewall intrusion alerts	Check box	Displays alerts automatically when Firewall detects a potential attack.

Setting	UI Control	Description
Tuning Options		
Enable Adaptive mode	Check box	Creates rules automatically to allow traffic. **NOTE:** Enable this option ***temporarily*** while tuning a deployment.
Log all blocked traffic to client activity log	Check box	*Enabled by default* Logs all blocked traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client.
Log all allowed traffic to client activity log	Check box	*Disabled by default* Logs all allowed traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client. N**OTE:** Enabling this option might negatively impact performance.
Setting	**UI Control**	**Description**
Network Reputation		
Incoming network - reputation threshold	Drop-down menu	*Medium Risk* *Unverified* *DO NOT USE* *High Risk* Specifies the rating threshold for blocking incoming or outgoing traffic from a network connection. Do not block - This site is a legitimate source or destination of content/traffic. Unverified - This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary. Medium Risk - This source/destination shows behavior that is considered suspicious. Any content/traffic from the site requires special scrutiny. High Risk - This source/destination sends or hosts potentially malicious content/traffic that is considered risky.
Outgoing network - reputation threshold	Drop-down menu	*Medium Risk* *Unverified* *DO NOT USE* *High Risk* Specifies the rating threshold for blocking incoming or outgoing traffic from a network connection. Do not block - This site is a legitimate source or destination of content/traffic. Unverified - This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary. Medium Risk - This source/destination shows behavior that is considered suspicious. Any content/traffic from the site requires special

		scrutiny. High Risk - This source/destination sends or hosts potentially malicious content/traffic that is considered risky.
Setting	**UI Control**	**Description**
Stateful Firewall		
Number of seconds (1-240) before TCP connections time out	Up/down number selector	Specifies the time, in seconds, that an unestablished TCP connection remains active if no more packets matching the connection are sent or received. The default number is 60; the valid range is 1–240.
Number of seconds (1-300) before UDP and ICMP echo virtual connections time out	Up/down number selector	Specifies the time, in seconds, that a UDP or ICMP Echo virtual connection remains active if no more packets matching the connection are sent or received. This option resets to its configured value every time a packet that matches the virtual connection is sent or received. The default number is 60; the valid range is 1–300.
Setting	**UI Control**	**Description**
DNS Blocking		
Domain name	Button/text input field	Defines domain names to block. When applied, this setting adds a rule near the top of the firewall rules that blocks connections to the IP addresses resolving to the domain names. Add - To add a domain name to block, click **Add**, then enter a domain name. You can use the * and ? wildcards. For example, *domain.com. Separate multiple domains with a comma (,) or a carriage return. Duplicate entries are automatically removed. Delete - To remove a domain name from the blocked list, select the domain name and click **Delete**.

Return to top

Client Firewall Rules

Client Firewall applies the rule at the top of the firewall rules list.

1. Client Firewall applies the rule at the top of the firewall rules list. If the traffic meets this rule's conditions, Client Firewall allows or blocks the traffic. It doesn't try to apply any other rules in the list.
2. If the traffic doesn't meet the first rule's conditions, Client Firewall continues to the next rule in the list until it finds a rule that the traffic matches.
3. If no rule matches, the firewall automatically blocks the traffic.

To modify Core Networking or Default Rules, expand either **Core Networking Rules** or **Default Rules**, select the rule to modify, and edit the desired settings, and click **OK**. The settings are described in the table below.

Alternatively, click one of the following buttons to perform the desired action:

Add Rule - Adds a firewall rule.

Duplicate - Creates a copy of the selected item.

Delete - Removes a selected firewall item.

Setting	UI Control	Description
Description		
Name	Text input field	Specifies the descriptive name of the item.
Status	Check box	Select **Enable rule** to make the rule active.
Actions	Radio button/Check box	*Allow* *Block* *Treat match as intrusion* *Log matching traffic* Allow - Allows traffic through the firewall if the item is matched. Block - Stops traffic from passing through the firewall if the item is matched. Treat match as intrusion - Treats traffic that matches the rule as an attack and generates an event that is sent to the Reputation Service. The *Block* action for the rule must be selected for an event to be generated. Log matching traffic - Preserves a record of matching traffic in the Firewall activity log on the Endpoint Security Client.
Direction	Drop-down menu	*In* *Out* *Either* In - Monitors incoming traffic. Out - Monitors outgoing traffic. Either - Monitors both incoming and outgoing traffic.
Notes	Text input field	Provides more information about the rule.
Setting	UI Control	Description
Networks		

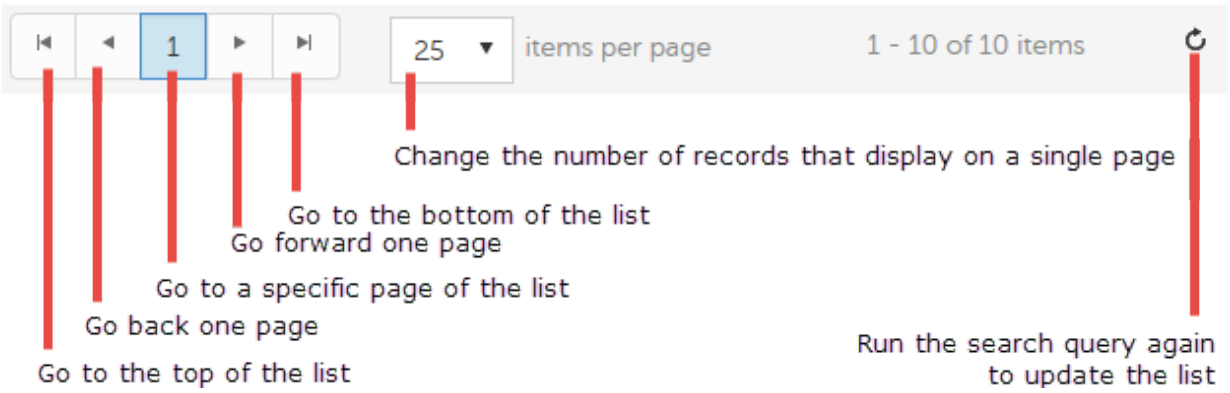
Network protocol	Radio Button/Check box	*Any protocol* *IP protocol* *Non-IP protocol* Any protocol - Allows both IP and non-IP protocols. IP protocol - Excludes non-IP protocols. IPv4 protocol or IPv6 protocol. If neither check box is selected, any IP protocol applies. Both IPv4 and IPv6 can be selected. Non-IP protocol - Includes non-IP protocols only.
Connection types	Check box	*Wired* *Wireless* *Virtual* Indicates if one or all connection types apply. A Virtual connection type is an adapter presented by a VPN or a virtual machine application, such as VMware, rather than a physical adapter.
Specify Networks	Button/Drop-down menu/text input field	To add a network, click **Add**, then specify the following: *Name* - Specifies the network address name (required). *Type* - Select either Local Network or Remote Network. Click **Add**, then specify the following: *Network type* - Specifies the origin or destination of traffic. Select from the network types Single IP, Subnet, Local subnet, Range, or Fully qualified domain name *IP address* - Specifies the IP address to add to the network. Wildcards are valid.
Transport		
Transport protocol	Drop-down menu	Select the transport protocol from the drop-down menu.
Executables		
Name	String	The name that you use for the executable to add or edit.

File path	String	The file path to the executable.
File description	String	*Description of the executable.*
Fingerprint	String	*The MD5 hash of the process.*
Enable digital signature check	Check box	Enables or disables the digital signature check that guarantees code hasn't been altered or corrupted since it was signed with a cryptographic hash. If enabled, specify: Allow any signature — Allows files signed by any process signer. Signed by — Allows only files signed by the specified process signer.

Return to top

Return to Client Firewall Policies

Navigate the list using these controls.



Notifications List

The Notifications list contains all of the notifications within the DDP system that you, as report administrator or report user, are entitled to see.

The **green percentage number** indicates the percentage of endpoints on this platform that are protected.

The **red percentage number** indicates the percentage of endpoints on this platform that are NOT protected.

N/A means that there are no endpoints on this platform in the organization.

Select a notification to remove from the list, and click **Dismiss**. Remove a notification only if necessary. It is removed for all users.

The Type drop-down list lets you select the notification type or types you want to see, and hides the notification types that are not selected.

Types include:

Update - News of upcoming product updates.

Config - News about configuration changes.

Knowledge Base - Summary of, and link, to a knowledge base article with in-depth technical information such as work-arounds and configuration tricks.

Announcement - News of upcoming releases and new products.

License - Alerts when your volume license is low, or when your CAL is has been exceeded.

After selecting one or more types, click in the neutral space above the list to apply the selections.

Select **Clear selected items** to reset the selections in this drop-down list.

The Priority drop-down list lets you select the priority level of notifications to list, and hides the notifications of unselected priority levels.

Priorities include Critical, High, Medium, and Low. These priority levels are relative to one another only within a type of notification.

Note: Notification priority levels are not related to any other priority levels elsewhere on the Dashboard.

After selecting one or more priority levels, click in the neutral space above the drop-down list to apply your selections.

Select **Clear selected items** to reset the selections in this drop down list. All notifications will display (unless filtered elsewhere).

The **Priority** drop-down lets you select one or more priority levels of notifications to include in the list. Notifications with all other priority levels remain hidden.

Enter a word or phrase to search for notifications with matching text, and click the search icon.

To clear the search criterion and display all notifications, click the X that displays next to the text you entered in the Search field.

The Advanced Threat Prevention Classifications section of the Dashboard shows a heat map of threats. The larger the block, the more threats of this kind have been found on endpoints in the organization.

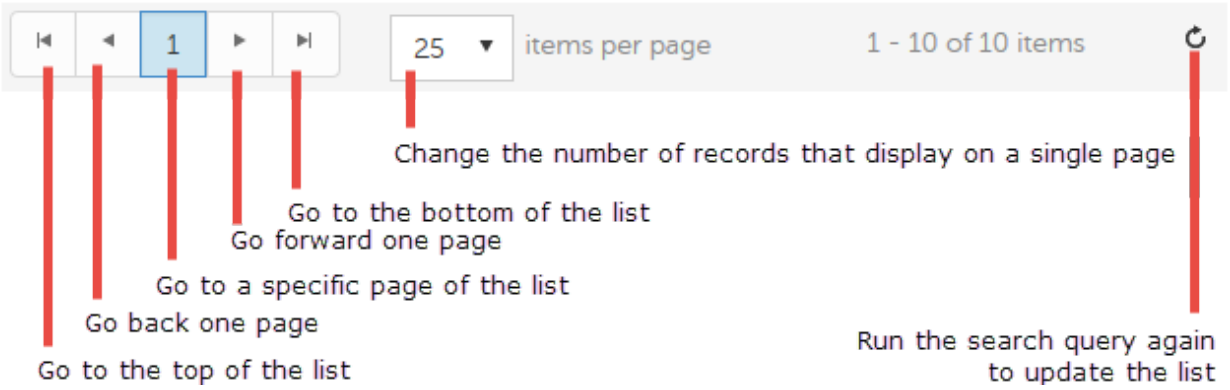
Click one of the indicators to hide the data on the chart; click a second time to re-include the data.

Click to view a detailed list of endpoints matching your selection.

Click a platform to view an Endpoint Operating System report of endpoints running on that platform.

Click **ALL** to view a summary report for all platforms.

Heat map of threats. Click a threat to see details about the selected threat.



Number of protected endpoints on each platform. The bottom number represents all protected endpoints.

Click a number to view a list of the protected endpoints.

Number of unprotected endpoints on each platform. The bottom number represents the total number of unprotected endpoints.

Click a number to display a list of the unprotected endpoints.

The green bar graphically indicates the percentage of endpoints on this platform that are protected.

The red bar graphically indicates the percentage of endpoints on this platform that are not protected.

A gray bar indicates that no endpoints are running on this platform.

Hover over the green in the pie chart to view the number of protected endpoints in the organization.

Hover over the red pie slice to view the number of unprotected endpoints.

Click a value to display a list of threats in the selected category.

The time frame is selectable, in days: 1, 7, 14, 30, 60, and 90.

Adjust the time frame for which to display threats.

Click a platform to view a list of endpoints running on that platform.

Click **ALL** to display a list of all protected endpoints, regardless of platform.

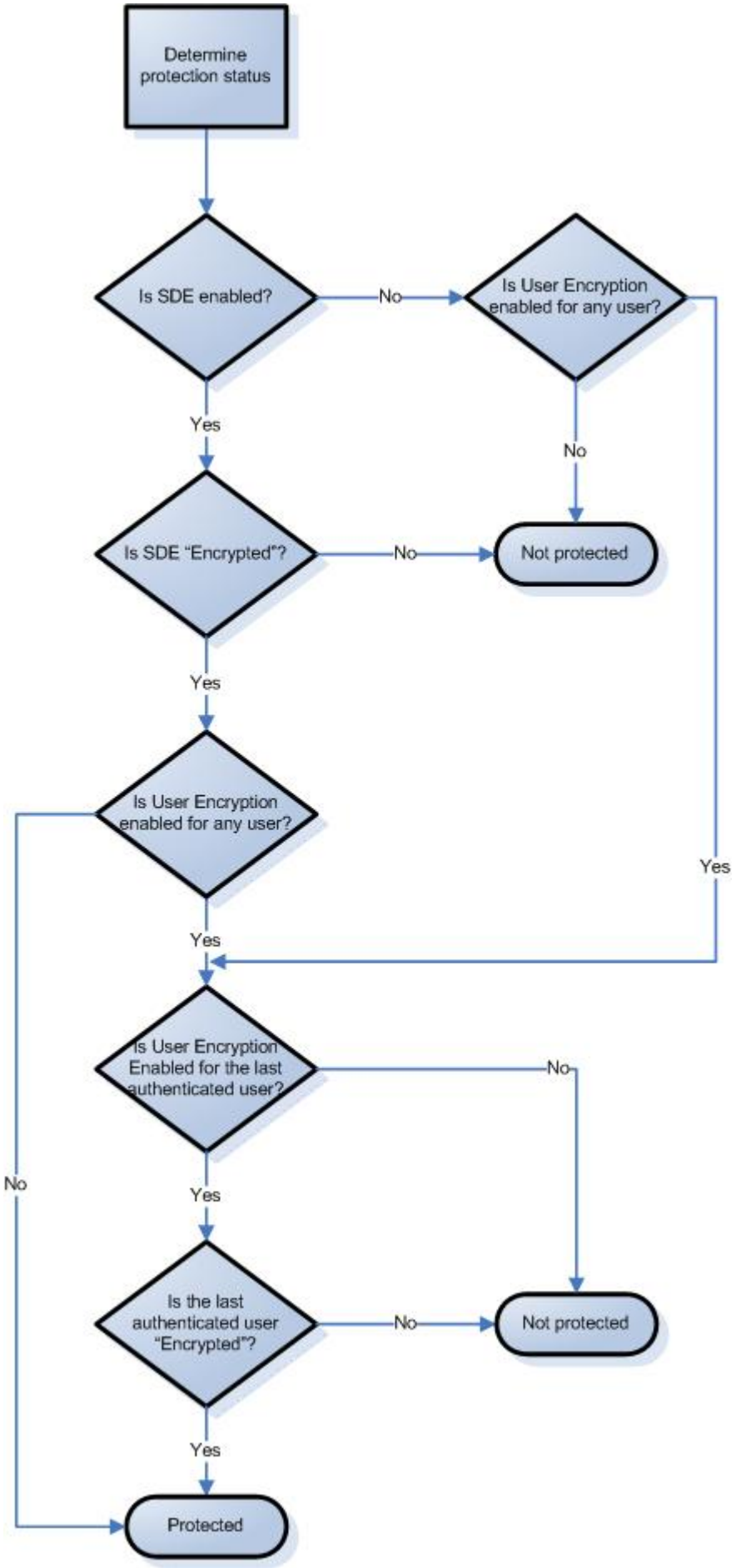
Click a number to view a list of endpoints running on that platform.

Click the bottom number to list all endpoints, regardless of platform.

The **Type** drop-down lets you select one or more types of notifications to include in the list. Notifications of the remaining types are hidden.

Protected

The protection status of a Windows workstation is derived from the current encryption policies and encryption states of the Encryption client users, as well as the current device encryption policy and state of the endpoint.


Determine protection status
Is SDE enabled?
No
Is User Encryption enabled for any user?
Yes
No
Is SDE "Encrypted"?
No
Not protected
Yes
Is User Encryption enabled for any user?
Yes
Yes
Is User Encryption Enabled for the last authenticated user?
No
No
Yes
Is the last authenticated user "Encrypted"?
No
Not protected
Yes
Protected

Provision Advanced Threat Prevention Service

The Advanced Threat Prevention service is provisioned and recovered, if necessary, through the Services Management Advanced Threats tab. Only the System Administrator can provision and recover the service.

After provisioning is complete, the Services Management page displays the contact information of the administrator who provisioned the service and a button, **Back Up Certificate**. To back up the certificate, click **Back Up Certificate** then select **Download Existing Certificate**. Save the certificate to a secure location separate from the server running EE/VE Server.

Provision service

To provision the Advanced Threat Prevention service:

1. In the left pane of the Remote Management Console, click **Management > Services Management**.
2. Select the **Advanced Threats** tab.
3. Click **Setup Advanced Threat Prevention Service**.
4. Follow the guided setup and complete necessary fields in the Service Setup dialogs.

   Regional provisioning to support geographical data centers is available for these regions: NA (North America), EU (EMEA), and AU (APAC).

   Dell recommends that you download and back up the Advanced Threat Prevention certificate in a safe location. The certificate will be required if at a future time service recovery is necessary. The guided setup prompts you to download and back up the certificate.

Clients are automatically provisioned with Advanced Threat Prevention.

After provisioning is complete, the **Setup** link no longer displays.

Recover service

You will need your backed up certificate to recover the Advanced Threat Prevention service.

1. In the left pane of the Remote Management Console, click **Management > Services Management**.
2. Click **Recover Advanced Threat Prevention Service**.
3. Follow the guided service recovery dialogs and upload the Advanced Threat Prevention certificate when prompted.

Remove HCA-Based Encryption

To remove hardware-based encryption, issue a policy of Hardware Crypto Accelerator (HCA) = False.

Secure Lifecycle Audit Events

In the Remote Management Console, Secure Lifecycle audit event logs maintain an audit trail of file activity for Windows, Mac, and mobile devices. By alternating between a map visualization and multiple filter options, you can access audit data in various ways, from a global overview to specific geolocations or audit data on a specific file or a specific user. This audit data offers the potential to visually identify data security breaches or preliminary security risks.

To view audit events in the Remote Management Console, select **Reporting > Audit Events**. The Audit Events page contains the map visualization and columns for filtering.

Map visualization

If you enable the Secure Lifecycle *Geo Location Audit Data* policy and have the operating system's geolocation API, audit events that are sent to the Dell Server include the geolocation data (latitude and longitude) of each device. A map visualization of the enterprise's audit events can identify device locations

that might indicate significant location changes or unexpected/questionable locations for devices within an enterprise. The system checks geolocation periodically, not each time an event is recorded.

If the policy for geolocation is disabled, no geolocation data is contained in the audit events that are sent to the Dell Server.

The map displays the following:

- Marker cluster - A numeric value represents audit events within a similar area. Hover over the marker cluster to view an outline of the determined area. Click a marker cluster to zoom to the audit event markers within that cluster. Continue to click on marker clusters until you see blue markers.
- Blue marker - Represents the location of a single audit event.
    - Click a marker and it can list the Device, File, User, and Timestamp for that marker's audit event.
    - The audit event can be a combination of the device and user that caused the audit event, for example: One device or user accessed one file. Multiple devices or users accessed one file and the timestamp indicates the user who last accessed the file. One user accessed numerous files.
- Mapping points of interest and points visible - If you scroll to the bottom right of the columns, the total number of items in the column displays. The map displays only files that have geolocation data (latitude and longitude). If a column lists 1000 files, but some lack geolocation data, the map displays only the points with geolocation data.
    - For performance purposes, the map limits the display to the first 2000 audit events that have latitude/longitude points in the table. It also varies depending on the filters you set.
    - If you drill in on the marker cluster, the map lists the total points of interest and the visible points.

  Note: Files that lack geolocation data and display only in the columns still provide some information for auditing.
- *Show only visible* check box - If you click a marker cluster, the map displays only the area for that cluster but the columns list all audit events in the original query. On the lower right of the map, click this check box and the columns list only the audit events for those visible map points. As you continue to drill down, the columns list only the events for the visible map points. Clear the check box to return to the global view.

Columns and filters

The columns provide options for multiple filters. For a description, see Options in the Columns dropdown.

- Default columns display based on the type of audit report, for example:
    - Moniker - Some audit events are specific to cloud encryption and .xen files; others to protected Office documents.
    - Timestamp
- More - If you set filters and create a query, you can select the filter options in More to modify the query.
- Search field - Use a wildcard to search on .docx, .pptx, or .xlsx.
- Search icons in the columns - If you click the Search icon next to an item in the Device, User, File Name, or KeyID columns, it copies the cell content to the Search field and executes a search on that content. You can then select Action or IP address to do additional filtering.

- If you clear all column check boxes, audit events are listed for all endpoints and all users.

Options in the Columns dropdown

Audit Event - Column options	Description
Moniker	Category of the audit event: • Cloud Encryption (In the log file, this displays as sl_xen_file) • Protected Office (In the log file, this displays as sl_protected_file) • Beacon - A device that did not have Secure Lifecycle tried to access a file. These audit events may have limited data (the location of where the file was accessed), but it may not have the name of the user of device.
Device	The location or IP address of the device where the event occurred.
User	User associated with the event.
Timestamp	Date and time when the event occurred. 1, 7, 14, 30, 60, 90 days.
Column options related to geolocation: Geo Type Latitude Longitude	Geolocation for Secure Lifecycle audit events identifies a device's latitude and longitude based on each operating system's APIs. The data visualization is based on those coordinates rather than a street address. Usually, the map visualization displays the location of the device. If a user accesses the computer remotely and neither GPS or WiFi is available, the map visualization may display the location based on the remote computer's VPN IP address.
Column options related to payload data: File KeyID File Path File Name File Size	Data for an audit event's moniker or parameters. Parameters may differ for each audit event but are the same within the event. For example, the data may differ for sl_xen_file and sl_protected_file, but the data for each Cloud Encryption .xen file event is the same.
Column options related to Embargo: From To	From - The time that an external user can start viewing a protected file. To - The time that an external user can no longer view a protected file.
Client Type	Indicates whether the client is internal or external
Cloud Name	The .xen file name (if a policy creates a GUID, you can see the filename here)
Action	The action associated with the payload file.
Cloud Action	If a service acts on a .xen file, the Cloud Action column lists the reason. See Cloud Encryption audit events.
SL Action	If a service acts on a protected Office file, for example, modifying or deleting a file, the SL (Secure Lifecycle) column lists the reason. See Protected Office Document audit events.
Process	Migration of Cloud Encryption events.
Column options related to folder management: Folder Path Folder Protection	If the *Folder Management Enabled* policy in Secure Lifecycle > Cloud Encryption is enabled for an endpoint, a user can select the Secure Lifecycle icon in the endpoint's system tray, select Manage Folders, and manually protect or unprotect a sync client folder. This audit event allows you to monitor overrides to protected folders and investigate if files that need to be encrypted are now decrypted.

Examples of Map Visualization and Column Filters

You can alternate between drilling in at the map level and drilling in at the filter and Search level. Here are some examples.

- Endpoint or endpoint group - If geolocation is enabled, the map displays the location of the events for each endpoint's .xen and protected Office files. If the map indicates protected files in an unexpected location, you can use the audit data to identify who modified the file. If several users

modified the file, you can filter the Timestamp column to determine the last person who modified it.

- User - You can audit a users' file activities. For example, in Columns, if you select **Action**, the protected Office files for that column can list *Created* or *Modified*. If you also select **SL (Secure Lifecycle) Action**, the column lists the reason for a user modifying files, such as *Updated* or *Swept*. For information on Action and SL Action, see Options in the Columns dropdown, Cloud Encryption audit events, and Protected Office Document audit events.

Example of drilling in at the map level

1. In the global view, drill in to a marker cluster and select a blue marker.
2. Select the *Show only visible* check box for the columns to list only the files for that audit event.
3. Click a quick search icon next to a Device, User, File Name, or KeyID.
4. If you click a User quick search, you can then click a File Name quick search icon and the map zooms in to the location of the user when the file was accessed.
5. Clear the Search field and press **Enter** to return to the global map view.

Cloud Encryption audit events

This table lists audit events that occur for files or folders stored in the cloud sync client folders. Events may differ slightly for Windows, Mac, and mobile devices.

Types of audit events	Description	Windows	Mac	Mobile device
Create	In the cloud sync client folder, Secure Lifecycle encrypted a file, creating a .xen file.	•	•	•
Decrypt	Secure Lifecycle decrypted a .xen file.	•	•	•
Deleted	A user deleted a .xen file from the cloud sync folder.	•	•	•
Folder override	If the *Folder Management Enabled* policy in Secure Lifecycle > Cloud Encryption is enabled for an endpoint, a user can select the Secure Lifecycle icon in the endpoint's system tray, select Manage Folders, and manually protect or unprotect a sync client folder. This audit event allows an administrator to monitor any overrides to protected folders and determine if files that need to be encrypted have been decrypted.	•		
.NET information	Attempts by a user or device to open an application or browser, but the attempt was blocked. Attempts to proxy through, but the address was blocked.	•		
Upload	Lists the folder path and whether the folder was protected.	•	•	

Protected Office Document audit events

This table lists audit events that apply to Office documents:

- For Windows, audit events apply to Opt-in or Force Protected modes.
- Mac and Mobile have Opt-in mode only.

Types of audit events	Description	Windows	Mac	Mobile device
Create	**Opt-in mode** - logs an event when a user selects Save As Protected and an Office document is protected. **Force-Protected mode** - logs events when Secure Lifecycle performs a sweep and creates protected Office documents.	•	•	•

Open	A user opened a protected Office document.	•	•	•
Sweep	For Windows, when Force Protected is set to On, provides data on files that were swept and converted from unprotected to protected Office.	•		
Updated	Summary of the number of times a file was changed since the last audit data transmission.	•	•	•
Watermark	User printed a file or exported a file with a watermark.	•	•	
Detected tampering	Tampering was detected in the .xen file portion of a protected Office document. This audit event alerts you to the tampering, but the .xen file cannot be repaired.	•	•	•
Repaired tampering	Tampering was detected in the wrapper of the protected Office document, which contains the cover page that opens in the cloud or on a device that does not have Secure Lifecycle. Secure Lifecycle repaired the wrapper or cover page.	•	•	•

Return to Secure Lifecycle policies.

Set Policies to Protect Office Documents in Mac

For enhanced security on Office documents (.docx, .xlsx, or .pptx), you can implement Secure Lifecycle's Protected Office mode. Protected Office documents are uploaded to the cloud, not as .xen files, but with their file extensions (.docx, .xlsx, or .pptx). However, the Office documents are encrypted. If opened or downloaded to a device that does not have Secure Lifecycle installed, only a cover page displays with instructions on how to obtain validated access. An authorized user can obtain installation or activation information from the enterprise. An unauthorized user cannot access the protected data.

Set Protected Office Document Policies

To set Protected-mode policies on Office documents for internal users:

1. Log in to the Remote Management Console.
2. In **Populations > Enterprise**, under the **Secure Lifecycle** technology group, click the **Protected Office Documents** policy group.
3. Toggle the *Protected Office Documents* policy to **On**.
5. **Note:** The *Force Protected files only* policy is not available for Mac.
4. At the *Enterprise* level, under **Secure Lifecycle**, click **Settings**.
5. Ensure the **Allow Mac Secure Lifecycle Activation** check box is selected.
6. Set additional Protected Office policies at the **Enterprise**, **Endpoint Groups**, or **Endpoints** levels.

   Note: For Endpoint Groups or Endpoints, click an option to access the Detail page's Security Policies tab.
7. To view protected Office documents in mobile devices, see Set Policies to Protect Office Documents in Mobile Devices.

Return to Secure Lifecycle.

Set Policies to Protect Office Documents in Mobile Devices

For enhanced security on Office documents (.docx, .xlsx, or .pptx), you can implement Secure Lifecycle's Protected Office mode. Protected Office documents are uploaded to the cloud, not as .xen files, but with their file extensions (.docx, .xlsx, or .pptx). However, the Office documents are encrypted.

Set Protected Office Document Policies

To set Protected-mode policies on Office documents:

1. Log in to the Remote Management Console.
2. In **Populations > Enterprise**, under the **Secure Lifecycle** technology group, click the **Protected Office Documents** policy group.
3. Toggle the *Protected Office Documents* policy to **On**.
5. **Note:** The *Force Protected files only* policy is not available for mobile.
4. At the *Enterprise* level, under **Secure Lifecycle**, click **Settings**.
5. Ensure the **Allow Mobile Secure Lifecycle Activation** check box is selected.
6. Set additional Protected Office policies at the **Enterprise**, **Domains**, **User Groups**, or **Users** levels.

   Note: For Domains, User Groups, or Users, click an option to access the Detail page's Security Policies tab.

Set Policies to Protect Office Documents in Windows

For enhanced security on Office documents (.docx, .xlsx, or .pptx), you can implement Secure Lifecycle's Protected Office mode for internal users. If an unauthorized user tries to access a protected file, the file remains encrypted, for example when the file is:

- Attached in an email
- Moved in a browser - if the user selects *Move* in a cloud sync client
- Moved in File Explorer
- Stored on removable media

Set Policies for Protected Office Documents

To set Protected-mode policies on Office documents for internal users:

1. Log in to the Remote Management Console.
2. In **Populations > Enterprise**, under the **Secure Lifecycle** technology group, click the **Protected Office Documents** policy group.
3. Determine the level of security for Office documents:

   5.

   - **Opt-in mode** (allows users the option to choose which Office documents to protect): Toggle the *Protected Office Documents* policy to **On**.
   - **Force-Protected mode** (ensures protection of all Office documents):
     - At the Enterprise level, toggle the *Protected Office Documents* policy to **On**.
     - At the Enterprise, Endpoint Groups, or Endpoints level, click **Show advanced settings** and select the *Force Protected files only* check box.

   Note: For Endpoint Groups or Endpoints, click an option to access the Detail page's Security Policies tab.
4. Set additional *Protected Office Documents* policies based on security requirements for Office documents, for example, Print, Export, and Embargo.
5. To view protected Office documents in mobile devices, see Set Policies to Protect Office Documents in Mobile Devices.

Determine Impact on Windows Users for Opt-in or Force Protected Modes

When you set *Protected Office Documents* policies and the client is activated, the *File* menu for Office documents displays additional options and enables/disables some options.

Dell recommends that you test policy updates on a test group of endpoints before applying them on a large scale.

This table provides an overview of the security impact on the Office File menu options for internal users based on which policies you activate:

- **Protected Office Documents** (Opt-in mode - user has the option to choose which Office documents to protect. Both Save As and Protected Save As are enabled).
- **Protected Office Documents** and **Force Protected files only** (Force-Protected mode - higher security) - The *Force Protected* policy enables a sweep on the clients' internal fixed drives to locate unprotected Office files and change them to Protected mode. It disables Save As, the Share option (Office 2013 and 2016), and Save & Send option (Office 2010). It enables Protected Save As.

  For Secure Lifecycle to sweep the Office documents, the user must log in and be connected to the network. The sweep acquires keys from the server for ten unprotected Office files at a time. If fewer than ten unprotected Office files require keys, the sweep waits 30 seconds for more files but then requests the keys.

  Note: Sweep ignores network file share, optical, and removable drives.

  Note: On the DDP|SL virtual drive, if the user right-clicks to create an Office document, it is saved as a .xen file. The user must manually access the File menu option and save the document as **Protected.** The Office document retains its extension in the cloud but is encrypted.

  Note: For Office-protected documents, users cannot use macro-enabled documents.

File menu option for Office documents	Policy for Opt-in mode: Protected Office Documents		Policies for Force-Protected mode: Protected Office Documents Force Protected files only
	Protected Office documents	**Unprotected Office documents**	**All Office documents**
Open	Files open as usual.	Files open as usual.	Unprotected documents open in read-only mode. See **Save** and **Protected Save As**.
Save	User clicks **Save**: the file is protected. If the file is in read-only mode, the *Save As* window opens. The only option in the *Save as type* field is *Protected (Documents, Presentation, or Workbook)*. User opens and saves a .xen file - the only option in the *Save as type* field is *Protected*. The .xen file is removed from the cloud.	User clicks **Save**: the file is saved but not in protected mode. *Save as type* field - If this is the first time to save the file, the *Save As* window opens and this field has the standard list of options.	User clicks **Save**: the file is protected. If the file is in read-only mode, the *Save As* window opens. The only option in the *Save as type* field is *Protected (Documents, Presentation, or Workbook)*. User opens and saves a .xen file - the only option in the *Save as type* field is *Protected*. The .xen file is removed from the cloud.
Save As	Enabled for user - saves as unprotected	Enabled for user- saves as unprotected	Disabled for user - the only option is **Protected Save As**.
Protected Save As	Enabled for user *Save as type* field - the only option is *Protected (Documents, Presentation,* or *Workbook)*.	Enabled for user *Save as type* field - the only option is *Protected (Documents, Presentation,* or *Workbook)*.	Enabled for user *Save as type* field - the only option is *Protected (Documents, Presentation,* or *Workbook)*.

This table provides an overview of additional Protected Office policy settings and what displays in the Office File menu.

File menu option for Office documents	Policy enabled (some protection options for user): Protected Office Documents		Policies enabled (higher security): Protected Office Documents Force Protected files only
	Protected Office documents	**Unprotected Office documents**	**With Force Protected enabled, the user is forced to save any Office document as Protected.**
Print	For Office-protected documents, the Print_Control policy determines how this function behaves.	Enabled for user	For Office-protected documents, the Print_Control **policy** determines how this function behaves.
Export (Office 2013 and higher)	**Office** 2013/2016 and ***Export Control*** **policy**: • **Allowed:** Enabled for user • **Watermark:** Export is disabled. See Protected Export. • **Disabled:** Disabled for user	Enabled for user	**Office** 2013/2016 and ***Export Control*** **policy**: • **Allowed:** Export option is enabled for user. However, with Force Protected enabled and a higher level of security, Dell recommends setting this policy to **Watermark** or **Disabled**. With Allowed, users can save as another file type, which could leave a document unprotected. • **Watermark:** Export is disabled. See Protected Export. • **Disabled:** Disabled for user
Protected Export (Office 2013 and higher) This option displays in the File menu only if the *Export Control* policy is set to Watermark.	**Office** 2013/2016 and ***Export Control*** **policy**: • **Watermark:** The user can export only to a PDF, but a watermark with their name, domain name, and computer ID displays on each page. **Note:** Export is disabled for user.	N/A	**Office** 2013/2016 and ***Export Control*** **policy**: • **Watermark:** The user can export only to a PDF, but a watermark with their name, domain name, and computer ID displays on each page. **Note:** Export is disabled for the user.
Save and Send (Office 2010) (Instead of Export)	Enabled for user	Enabled for user	Disabled for user Note: To export to a PDF, the user can use the Print menu (if Print Control policy is set to Allowed) to print to a PDF.
Share (Office 2013 and higher)	Enabled for user	Enabled for user	Disabled for user

This table provides an overview of Protected Office policy settings and other menu options.

File menu option for	Policy enabled (some protection options for user):	Policies enabled (higher security):

Office documents	Protected Office Documents		Protected Office Documents Force Protected files only
	Protected Office documents	Unprotected Office documents	With Force Protected enabled, the user is forced to save any Office document as Protected.
Copy/Paste (*Office Protected Clip Board* policy)	Copy/Paste only to a protected Office document.	Copy/Paste unprotected content as usual.	Copy/Paste only to a protected Office document.

Enable Both Cloud Encryption and Protected Office Documents

If you enable both policy groups, Protected Office documents differ from non-Office documents in some areas:

- If the *Cloud Storage Protection Providers* policy is set to *Allow* and does not encrypt non-Office files, protected Office documents still maintain any protection status.
- If the Excluded Folders policy excludes a particular folder from encryption, protected Office documents still maintain any protection status if copied to those folders.

Return to Secure Lifecycle.

Suspend Users

Suspending a user is effective (suspended users cannot authenticate with their devices) but reversible, whereas deactivating a user (depending on the device and the policy value you choose) can go as far as deleting all secure data on the device and uninstalling the Shield. You might want to suspend a user who is taking a sabbatical, or who is on involuntary leave pending review.

You can also suspend a group by making the same policy change at the group level. If you do this, be aware that if any of the users in the group have a local setting of Active for this policy (which would happen if any users have previously been suspended and reinstated), that local setting overrides the inherited group setting. When a policy setting is critical for a given user, we recommend that you set it locally in order to be certain of the outcome.

To suspend a user, follow the steps below. Note that reinstating a suspended Windows Shield user requires the use of WSDeactivate, which is obtained from Customer Support. We recommend that you obtain this utility from Customer Support near the same time that you suspend the user, so that reinstatement can be performed promptly if needed.

1. In the left pane, click **Populations > Users**.
2. In the Search field, either enter the user's name or enter a filter to search for the user. The wild card character is *. You can enter Common Name, Universal Principal Name, or sAMAccountName.
3. Click a User Name.
4. On the **Security Policies** tab under the Windows Encryption technology group, select the **Policy-Based Encryption** policy group.
5. Expand the user's *Shield Permissions* polices.
6. In the Local Value, change the *Current Shield State* policy to *Suspend*.
7. Click **Save**.
8. In the left pane, click **Actions > Commit Policies**.
9. Click **Apply Changes**.

Repeat these steps for each type of device the user should be suspended from.

Syslog Event Types

Following are event types that are supported with the Syslog/SIEM Advanced Threats option.

Application Control

This option is only visible to users who have the Application Control feature enabled. Application Control events represent actions occurring when the device is in Application Control mode. Selecting this option will send a message to the Syslog server whenever an attempt is made to modify or copy an executable file, or when an attempt is made to execute a file from an external device or network location.

Example Message for Deny PE File Change:

```
CylancePROTECT: Event Type: AppControl, Event Name: pechange, Device Name: WIN-
7entSh64, IP Address: (192.168.119.128), Action: PEFileChange, Action Type: Deny,
File Path: C:\Users\admin\AppData\Local\Temp\MyInstaller.exe, SHA256:
04D4DC02D96673ECA9050FE7201044FDB380E3CFE0D727E93DB35A709B45EDAA
```

Example Message for Deny Execution from External Drive:

```
CylancePROTECT: Event Type: AppControl, Event Name: executionfromexternaldrives,
Device Name: WIN-7entSh64, IP Address: (192.168.119.128), Action: PEFileChange,
Action Type: Allow, File Path: \\shared1\psexec.exe, SHA256:
F8DBABDFA03068130C277CE49C60E35C029FF29D9E3C74C362521F3FB02670D5
```

Devices

Select this option to send device events to the Syslog server.

- When a new device is registered, two messages for this event are received: Registration and SystemSecurity.

  Example Message for Device Registered Event:

  ```
  Event Type: Device, Event Name: Registration, Device Name: WIN-55NATVQHBUU

  Event Type: Device, Event Name: SystemSecurity, Device Name: WIN-
  55NATVQHBUU, Agent Version: 1.1.1270.58, IP Address: (10.3.0.154), MAC Address:
  (005056881877), Logged On Users: (WIN-55NATVQHBUU\Administrator), OS: Microsoft
  Windows Server 2008 R2 Standard Service Pack 1 x64 6.1.7601
  ```

- When a device is removed.

  Example Message for Device Removed Event:

  ```
  Event Type: Device, Event Name: Device Removed, Device Names: (
  ), User: (
  )
  ```

- When a device's policy or logging level has changed.

Example Message for Device Updated Event:

```
Event Type: Device, Event Name: Device Updated, Device Message:
Renamed: 'WIN-55NATVQHBUU' to 'WIN-2008R2-IRV1'; Policy Changed: 'Default' to
'IRVPolicy1';
```

Memory Protection

Selecting this option will log any Memory Exploit Attempts that might be considered an attack from any of the Tenant's devices to the Syslog server.

There are four types of Memory Exploit actions:

- **None:** Allowed because no policy has been defined for this violation.
- **Allowed:** Allowed by policy.
- **Blocked:** Blocked from running by policy.
- **Terminated:** Process has been terminated.

Example Message of Memory Protection Event:

```
Cyl CylancePROTECT: Event Type: ExploitAttempt, Event Name: blocked, Device Name:
WIN-7entSh64, IP Address: (192.168.119.128), Action: Blocked, Process ID: 3804,
Process Name: C:\AttackTest64.exe, User Name: admin, Violation Type: LSASS Read
```

Script Control

Selecting this option will log any newly found scripts that have been blocked or have triggered an alert to the Syslog server.

Syslog Script Control events contain the following properties:

- **Alert:** The script is allowed to run. A script control event is sent to the DDP Server.
- **Block:** The script is not allowed to run. A script control event is sent to the DDP Server.

Example Message of Script Control

```
CylancePROTECT - - - Event Type: ScriptControl, Event Name: Blocked, Device Name:
Fake_Device, File Path: d:\windows\system32\windowspowershell\v2.1\newlyMade.vbs,
Interpreter: active, Interpreter Version: 6.1.7600.16385 (win7_rtm.090713-1255)
```

Threats

Select this option to log any newly found threats or changes observed for any existing threat, to the Syslog server. Changes include a threat being Removed, Quarantined, Waived, or Executed.

There are five types of Threat Events:

- **threat_found**: A new threat has been found in an Unsafe status.
- **threat_removed**: An existing threat has been Removed.
- **threat_quarantined**: A new threat has been found in the Quarantine status.

- **threat_waived**: A new threat has been found in the Waived status.
- **threat_changed**: The behavior of an existing threat has changed (examples: Score, Quarantine Status, Running Status).

  Example Message of Threat Event:

```
Event Type: Threat, Event Name: threat_found, Device Name:
1, IP Address: (), File Name: virusshare_00fbc4cc4b42774b50a9f71074b79bd9,
Path: c:\ruby\host_automation\test\data\test_files\, SHA256:
1EBF3B8A61A7E0023AAB3B0CB24938536A1D87BCE1FCC6442E137FB2A7DD510B, Status: Unsafe,
Cylance Score: 100, Found Date: 6/1/2015 10:57:42 PM, File Type: Executable, Is
Running: False, Auto Run: False, Detected By: FileWatcher
```

Threat Classifications

Hundreds of threats are classified each day as either Malware or Potentially Unwanted Programs (PUPs). If this option is selected, you subscribe to be notified when these events occur.

Example Message of Threat Classification:

```
Event Type: ThreatClassification, Event Name: ResearchSaved, Threat
Class: Malware, Threat Subclass: Worm, SHA256:
1218493137321C1D1F897B0C25BEF17CDD0BE9C99B84B4DD8B51EAC8F9794F65
```

SIEM (Security Information and Event Management)

Specifies the type of Syslog server or SIEM that events are to be sent to.

Protocol

This must match what is configured on your Syslog server. The choices are UDP or TCP. UDP is generally not recommended as it does not guarantee message delivery. Dell recommends TCP (default).

TLS/SSL

Only available if the Protocol specified is TCP. TLS/SSL ensures the Syslog message is encrypted in transit from Advanced Threat Prevention to the Syslog server. Dell encourages customers to select this option. Ensure that the Syslog server is configured to listen for TLS/SSL messages.

IP/Domain

Specifies the IP address or fully-qualified domain name of the Syslog server that the customer has setup. Consult with your internal network experts to ensure firewall and domain settings are properly configured.

Port

Specifies the port number on the devices that the Syslog server listens for messages. It must be a number between 1 and 65535. Typical values are: 512 for UDP, 1235 or 1468 for TCP, and 6514 for Secured TCP (example: TCP with TLS/SSL enabled).

Severity

Specifies the severity of the messages that should display in the Syslog server. This is a subjective field, and it may set to whatever level preferred. The value of severity does not change the messages that are forwarded to Syslog.

Facility

Specifies what type of application is logging the message. The default is Internal (or Syslog). This is used to categorize the messages when they are received by the Syslog server.

Testing the Connection

Click Test Connection to test the IP/Domain, Port and Protocol settings. If valid values are entered, after a couple of moments, a success confirmation displays.

Syslog IP Addresses

Syslog server IP addresses to allow, by region:

US (includes my.cylance.com and my-vs2.cylance.com):

52.2.154.63

52.20.244.157

52.71.59.248

52.72.144.44

54.88.241.49

AU (my-au.cylance.com):

52.63.15.218

52.65.4.232

EU (my-vs0-euc1.cylance.com and my-vs1-euc1.cylance.com):

52.28.219.170

52.29.102.181

52.29.213.11

Note: This IP Address should remain static.

For the latest IP addresses for Syslog messages, contact Dell ProSupport.

Threat Protection Policy Overview

Threat Protection policies are divided into the following categories:

- Client Options
- Client Firewall
- Malware Protection
- Web Protection

For more information about Threat Protection policies, see Windows Threat Protection.

Client Options Policies

When you set the *Threat Protection* master policy to True, you can then set policies for these client options:

- Actions to take when malicious activity is identified (Block, Report, Block and Report)

Policies allow you to set the action to take when users attempt to modify or delete Threat Protection system files, registry keys, and processes. The default setting for these policies is Block and Report: *Action on Malicious Activity for Files and Folders*, *Action on Malicious Activity for Registry*, and *Action on Malicious Activity for Processes*.

- Exclusion of specified processes from Threat Protection scans
- Logging locations and debug/verbose logging of certain activities

  Activity logging is enabled by default. Debug logging is disabled by default.

- Client update scheduling

  Client updates ensure that client computers are always protected from the latest threats through content files that include definitions of threats such as viruses and spyware, that are used to detect threats. The *Client Update Schedule* policy is set to True (Enabled) by default. The *Client Update Schedule Repeats* policy, which determines the frequency of client updates, is set to Daily by default.

Client Firewall Policies

The Client Firewall is a stateful firewall that checks all incoming and outgoing traffic against its list of rules. If the traffic matches all criteria in a rule, the Client Firewall acts according to the rule, blocking or allowing traffic through the firewall.

Configurable options and rules define how the Client Firewall works. When the master policy, *Client Firewall*, is set to **True** (default), you can select **View/Edit** in the *Settings and Rules* policy to view or configure an extensive set of Client Firewall options and rules.

Client Firewall options

Options include which subsets of traffic to block or allow and logging settings, as well as timeout parameters for TCP, UDP, and ICMP connections.

Client Firewall rules

Client firewall rules define specific handling of network traffic. Each rule provides a set of conditions that traffic must meet and an action to allow or block that traffic. When Client Firewall finds traffic that matches a rule's conditions, it performs the associated action.

Client Firewall uses precedence to apply rules and applies the rule at the top of the firewall rules list.

1. If the traffic meets the conditions of the rule at the top of the list, Client Firewall allows or blocks the traffic. It does not try to apply any other rules in the list.
2. If the traffic does not meet the first rule's conditions, Client Firewall continues to the next rule in the list until it finds a rule that the traffic matches.
3. If no rule matches, the firewall automatically blocks the traffic.

For a list of Client Firewall rules and their descriptions, see Client Firewall Settings and Rules.

Malware Protection Policies

Malware Protection checks for viruses, spyware, unwanted programs, and other threats by scanning items on the client computer. When you set the master policy, *Malware Protection*, to True, you can then set additional policies.

Types of Malware Protection

The following policies represent the different types of scans included in malware protection:

On-Access Protection – When a user accesses files, folders, and programs, the on-access scanner intercepts the operation and scans the item. Default: True (Enabled).

On-Demand Protection - Full Scan – Based on a schedule set in policy, the on-demand scanner runs a thorough check of all areas of the computer. Default: True (Enabled).

By default, every time Full Scan runs, it scans the following for threats:

- Computer memory for installed rootkits, hidden processes, and other behavior that suggests malware is attempting to hide itself. This scan occurs before all other scans.
- Memory of all running processes.
- All drives on the computer and their subfolders.

By default, the scanner scans all file types, regardless of extension.

On-Demand Protection - Quick Scan – Based on a schedule set in policy, the on-demand scanner runs a quick check of areas of the computer that are most susceptible to threats. Default: True (Enabled).

By default, every time Quick Scan runs, it scans the following for threats:

- Memory of all running processes.
- Files that the Windows Registry references.
- Contents of the Windows folder.
- Contents of the Temp folder.

By default, the scanner scans all file types, regardless of extension.

Access Protection – Prevents other computers from making a connection and creating or altering autorun (autorun.inf) files from CDs. The rule prevents spyware and adware distributed on CDs from being executed and automatically blocks and reports such issues. Default: True (Enabled).

Exploit Protection – Monitors for application vulnerabilities and keeps buffer overflow exploits from executing arbitrary code on the computer. Default: True (Enabled).

Script Scan Protection – Enables scanning JavaScript and VBScript scripts to prevent unwanted scripts from executing. Default: True (Enabled).

Configurable Actions - After Threat is Detected

Actions taken if a threat, unwanted program, or exploit is detected are controlled by policy and include the following:

Full-Scan Threat First Response - Specifies the first action for the scanner to take when a threat is detected. Default: Clean file.

Full-Scan Threat First Response Fails - Specifies the action for the scanner to take when a threat is detected if the first action fails. Default: Delete file.

Full-Scan Unwanted Program First Response - Specifies the first action for the scanner to take when a potentially unwanted program is detected. Default: Clean file.

Full-Scan Unwanted Program First Response Fails - Specifies the action for the scanner to take when an unwanted program is detected if the first action fails. Default: Delete file.

Quick-Scan Threat First Response - Specifies the first action for the scanner to take when a threat is detected. Default: Clean file.

Quick-Scan Threat First Response Fails - Specifies the action for the scanner to take when a threat is detected if the first action fails. Default: Delete file.

Quick-Scan Exploit First Response - Specifies the first action for the scanner to take when a potential exploit is detected. Default: Clean file.

Quick-Scan Exploit First Response Fails - Specifies the action for the scanner to take when an exploit is detected if the first action fails. Default: Delete file.

Reputation Service Sensitivity policies

When the *Full-Scan Reputation Service Sensitivity* or *Quick-Scan Reputation Service Sensitivity* policies are enabled, samples are submitted to the Reputation Service lab to determine if they are malware. The sensitivity level is used when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results.

The following values can be set:

Disable - Samples are not submitted to the Reputation Service lab.

Very Low - A detection is made available to Threat Protection when the Reputation Service lab publishes it instead of waiting for the next file update. Average of 10-15 queries per day, per computer.

Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10-15 queries per day, per computer.

Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. This setting is the minimum recommendation for laptops or desktops and servers. Average of 20-25 queries per day, per computer.

High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20-25 queries per day, per computer.

Very High - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20-25 queries per day, per computer.

Web Protection Policies

Web Protection monitors web browsing and downloads to identify threats and enforce action set by policy when a threat is detected, based on ratings for websites. When you set the master policy, *Web Protection*, to **True**, you can set other policies for Web Protection.

The Web Protection feature is supported with Internet Explorer.

The Reputation Service analyzes each website and assigns a color-coded safety rating based on test results. The color indicates the level of safety for the site:

Red – Malicious

Yellow – Potentially malicious

Green - Safe

Through the following policies, you can assign actions to implement when a user accesses a website or attempts a download, based on website ratings:

Rating Action for Red Sites - Specifies the action to apply to sites that are rated Red. Default: Block.

Rating Action for Yellow Sites - Specifies the action to apply to sites that are rated Yellow. Default: Warn.

Rating Action for Unrated Sites - Specifies the action to apply to sites that are Unrated. Default: Allow.

Rating Action for Red Downloads - Specifies the action to apply to file downloads that are rated Red. Default: Block.

Rating Action for Yellow Downloads - Specifies the action to apply to file downloads that are rated Yellow. Default: Warn.

Rating Action for Unrated Downloads - Specifies the action to apply to file downloads that are Unrated. Default: Allow.

Configurable actions for website access or download attempts include the following:

Block – Prevents users from accessing the site or downloading a file from the site. A message is displayed.

Allow – Permits users to access the site or proceed with the download.

Warn – Displays a warning to notify users of potential dangers associated with the site or download file. Users must dismiss the warning before ending the web session or proceeding with the download.

To exclude a private IP address or range of addresses from Web Protection content rating actions, specify the IP address or IP address range in the *IP Exclusions for Web Protection* policy.

To block all phishing pages, without regard to policy values that control content rating actions, set the *Enforcement - Block Phishing Pages for All Sites* policy to True.

Threat Data Report

Select **Threat Data Report** on the **Options** tab to enable threat data export to .csv files.

The following types of data are available for export:

Threats - Lists all threats discovered in your organization. This information includes File Name and File Status (Unsafe, Abnormal, Waived, and Quarantined).

Devices - Lists all devices in your organization that have an Agent installed. This information includes Device Name, OS Version, Agent Version, and Policy applied.

Events - Lists all events related to the Threat Events Graph on the Dashboard for the last 30 days. This information includes File Hash, Device Name, File Path, and the Date the event occurred.

Indicators - Lists each threat and the associated threat characteristics.

Cleared - Lists all files that have been cleared in your organization. This information includes files that were Waived, added to the Safe List, or deleted from the quarantine folder on a device.

Export Data

To access the exported data:

1. Select **Generate token.**
2. Copy the URL of the desired data and paste it into a web browser address field.
3. In the URL, replace [Token] with the generated token displayed in the **Token** field.

To disable access to the exported data, select **Delete** or **regenerate** to invalidate the current token. After regenerating a token, provide it to persons who should have continued access to the exported data.

Upload Client Access Licenses

You received CALs separately from the installation files, either at the initial purchase or later if you added additional CALs.

1. In the left pane of the Remote Management Console, click **Management > License Management**.
2. Under Upload Licenses, click **Choose File** to browse to the location of the saved CAL.

Related topics:

CAL Information

License Management