

**Dell Security Center v10.2.7
AdminHelp**

Table of Contents

Welcome	1
About Online Help	1
Attributions & Copyrights.....	1
Get Started.....	23
Get Started with Dell Data Security.....	23
Log In	23
Log Out	23
Dashboard.....	23
Navigate Dell Security Center.....	25
Management Console.....	25
Dashboard.....	25
Populations.....	25
Reporting.....	25
Management	25
Masthead Icons	25
Dashboard.....	26
Dashboard	26
Notifications List.....	27
Notification Types	27
Priority Levels	28
Protection Status	28
Protection History.....	28
Inventory History	28
Summary Statistics.....	28
Endpoint OS Report.....	29
Platform Report	29
Populations.....	29
Populations	29
Enterprise.....	30
View or Modify Enterprise Policies.....	30
Domains.....	30
Domain	30

Users..... 31

 Add Azure AD Users 31

User Groups 31

 Add a User Group..... 31

User Groups..... 32

 User Groups 32

 Add a User Group..... 32

 Remove User Groups 33

 Find User Groups 33

 View or Modify User Group Policies and Information 33

 User Group Details & Actions 34

 User Group Members 34

 Add Users to the Group 34

 Remove Users from the Group 34

 User Group Admin 35

 Edit Group Priority 35

 Edit Endpoint Group Priority 35

 Edit User Group Priority 36

 Assign or Modify Administrator Roles..... 37

 View Reconciliation Date 37

Users 37

 Remove Users 37

 Find Users 37

 View or Modify User Policies and Information 38

 User Details & Actions..... 38

 User Endpoints 39

 User Groups 39

 User Admin..... 39

 View Reconciliation Date 40

Endpoint Groups..... 40

 Endpoint Groups..... 40

 Types of Endpoint Groups..... 40

 Add an Endpoint Group..... 40

 Remove an Endpoint Group 41

Modify an Endpoint Group	41
Endpoint Groups Specification	41
Endpoint Group Specification	41
Operators and Expressions	42
Working with Complex Queries	43
Examples	43
Edit Group Priority	44
Edit Endpoint Group Priority	44
Edit User Group Priority	45
View Endpoints in an Endpoint Group	45
View or Modify Endpoint Group Policies and Information	45
Endpoint Group Details & Actions	46
Endpoint Group Members	46
Add Endpoints to an Admin-Defined Endpoint Group	46
Remove Endpoints from an Admin-Defined Endpoint Group	47
Endpoints	47
Endpoints	47
Add Endpoint to Group	47
Remove Endpoints	48
View or Modify Endpoint Policies and Information	48
View Effective Policy	49
Endpoint Details & Actions	49
Plugins	49
Plugins & Agents	50
Endpoint Detail	51
Plugin Manager Detail	52
Protected Status	52
Endpoint Users	52
Data Guardian	53
Administrators	53
Assign or Modify Administrator Roles	53
Administrator Roles	53
Delegate Administrator Rights	55
Reporting	55

Manage Reports.....	55
Manage Reports.....	55
View or Modify an Existing Report.....	56
Create a New Report	56
View Report.....	56
Query using Search and More... to filter.....	57
Export File	58
Data Guardian Audit Events.....	58
Map visualization.....	58
Audit Event Options and Filters	59
Options in the Columns Menu	60
Protected Office Document or Basic File Protection audit events (Windows, Mac, mobile, web portal, CASB)	61
Examples of Map Visualization and Column Filters.....	66
Example of drilling in at the map level	66
Get Started with Data Guardian Audit Events.....	66
Audit Protected Office Documents	66
Audit Cloud Encryption (Mac or mobile)	68
Default Monikers and Columns.....	68
EU General Data Protection Regulation (GDPR)	68
View Audit Events (Geolocation).....	68
Event Data.....	69
Management	70
Commit Policies	70
Log Analyzer.....	70
Subscriptions.....	71
Subscriptions	71
View Total Seats Used	71
Reclaim Subscription Licenses.....	71
Subscriptions Information	71
Subscriptions.....	72
Services Management	72
Events Management - Export Audit Events to a SIEM Server	72
Enable Data Guardian Access Groups.....	73

Notification Management.....	73
Notification Management.....	73
Product Notifications.....	74
Receive product notifications.....	74
External User Management.....	74
Registration Access.....	74
Key Request.....	74
Key Revocation.....	75
Data Guardian Management.....	75
Registration Access.....	75
Key Request.....	76
Key Revocation.....	76
Key Management.....	77
Downloads.....	77
Endpoint Software.....	77
Configuration.....	78
CASB Management.....	78
Manage Policies.....	79
Manage Security Policies.....	79
Localize Policies Displayed on the Endpoint Computer.....	80
Localizable Policies.....	81
Data Guardian.....	82
Overview of Data Guardian Features and Policies.....	82
Protect data in use, in motion, or at rest.....	82
Control data.....	82
Monitor data.....	83
Policies.....	83
Data Guardian.....	83
Advanced Data Guardian.....	87
Set Cover Page Policies.....	95
Configure Basic File Protection Policies.....	96
Supported applications and file types.....	96
Additional applications and file types.....	97
Configure policy for Basic File Protection.....	97

Configure policy to exclude folders for Basic File Protection (Windows and Mac)	99
Unsupported applications and file types	100
Remove a file type	100
Use the Recovery Tool	100
Plan for factors in configuration	100
To add a Universal Windows Platform (UWP) application	101
Use Data Guardian in Opt-in Mode (Windows or Mac)	101
Set opt-in policies for internal users	101
Determine file types to protect	101
File menu options for protected Office documents in Opt-in mode - Windows	103
Configure Access Groups	104
Legacy policies for Data Guardian	104
Use Data Guardian in Force-Protected Mode (Windows or Mac)	104
Set Force-Protected policies for internal users	105
Determine file types to protect	105
File menu options for protected Office documents in Force-Protected mode	106
Configure Access Groups	107
Legacy policies for Data Guardian	107
Legacy Policies for Data Guardian's Opt-in Mode	107
Windows: Additional Office menu options for Data Guardian v2.7 and earlier	107
Windows: Additional Office menu options on Windows for Data Guardian v2.7 and earlier	108
Windows: Additional policies	108
Legacy Policies for Data Guardian's Force-Protected Mode	108
Windows: Additional Office menu options for Data Guardian v2.7 and earlier	108
Windows: Additional Office menu options on Windows for Data Guardian v2.7 and earlier	109
Windows: Additional policies	109
Set Policies to Protect Documents in Mobile Devices	109
Set Protected Office Document Policies	110
Set Policies to Protect Documents on the Web Portal	110
Set Protected Office Document Policies	110
Configure Content Based Protection for Data Guardian's Opt-in mode	110
Modify a Content-Based Rule	111
Content-Based Rule Name and Priority	112
Actions	112

Dell Security Center v10.2.7 AdminHelp

Rules	113
Elements	113
Add an Enterprise-Specific Rule Name or Tag Element	114
Create a Rule Name.....	114
Create an Element.....	114
View Audit Event Reports.....	115
Set TITUS classification (Opt-in mode).....	115
Configure TITUS to encrypt files.....	115
Configure TITUS to encrypt macro-enabled documents.....	116
Use Data Guardian with Cloud Encryption.....	116
Windows 2.3 and earlier or Mac 2.8 and earlier	116
Enable Both Cloud Encryption and Protected Office Documents (Windows 2.3 and earlier)	117
Configure Access Groups.....	117
Set up Access Groups	118
Enterprise does not yet have Data Guardian	118
Enterprise has Data Guardian Installed	119
Configure Access Groups	120
Disable Auto access for swept files (Windows and Mac)	120
Global Settings	121
Advanced Global Settings.....	123

Welcome

About Online Help

Version: **10.1.1906**

Attributions & Copyrights

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

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

The software described 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:

- o The conditions indicated in the above permission notice are met;
- o 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) Technologie. 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 3rd 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 is 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 is 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>.

Copyright 2009 RestSharp

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

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>.

The MIT License (MIT)

Copyright (c) 2007 James Newton-King

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.

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>.

CXIX. Portions of this product make use of the Mono and the Mono runtime, under MIT, BSD, and Apache licenses. You may obtain a copy of the licenses at <http://www.mono-project.com/docs/faq/licensing/>.

Copyright 2018 Microsoft

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.

Copyright 2018 Microsoft

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, 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.
3. Neither the name of the copyright holder 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 COPYRIGHT HOLDER 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.

Copyright 2018 Microsoft

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License

You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

CXX. Portions of this product make use of the Mono .NET assemblies under MIT and BSD licenses. You may obtain a copy of the licenses at <https://mit-license.org/> and <https://opensource.org/licenses/BSD-3-Clause>.

The MIT License (MIT)

Copyright © 2018 Microsoft

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.

The BSD License

Copyright 2018 Microsoft

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, 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.
3. Neither the name of the copyright holder 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 COPYRIGHT HOLDER 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.

CXXI. Portions of this product make use of mkbundle in Mono under GNU LESSER GENERAL PUBLIC LICENSE v3. You may obtain a copy of the license at <https://www.gnu.org/licenses/lgpl.txt>.

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<https://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.

0. 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.

The "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.

CXXII. Portions of this product make use of minizip, memcheck.h, freebsd-dwarf.h, freebsd-elf_common.h, freebsd-elf64.h, freebsd-elf32.h, bsearch.c, w32file-unix-glob.c, and w32file-unix-glob.h in Mono under BSD license. You may obtain a copy of the license at <https://opensource.org/licenses/BSD-3-Clause>.

The BSD License

Copyright 2018 Microsoft

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, 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.
3. Neither the name of the copyright holder 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 COPYRIGHT HOLDER 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.

CXXIII. Portions of this product make use of RabbitMQ.Client in Mono under dual license in Apache v2 and Mozilla Public License 1.1. You may obtain a copy of the licenses at <http://www.apache.org/licenses/LICENSE-2.0> and <https://www.mozilla.org/MPL/>.

License Information:

Copyright (c) 1999 - 2017 Dell Inc. All rights reserved.

This software and associated documentation (if any) is furnished under a license and may only be used or copied in accordance with the terms of the license.

Dell elects to use only the Apache license for any software where a choice of Apache v2, and Mozilla Public License 1.1 license versions are made available with the language indicating that Apache v2, and Mozilla Public License 1.1 "or any later version may be used, or where a choice of which version of the Apache v2, and Mozilla Public License 1.1" is applied is unspecified.

CXXIV. Portions of this product make use of Compat.ICSharpCode.SharpZipLib and ICSharpCode.SharpZipLib in Mono under GNU LESSER GENERAL PUBLIC LICENSE v3. You may obtain a copy of the license at <https://www.gnu.org/licenses/lgpl.txt>, although the full text is available below.

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<https://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.

The "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.

2. 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.

3. 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.

4. 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.

5. 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.)

6. 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.

7. 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.

Classpath is distributed under the terms of the GNU General Public License with the following clarification and special exception.

Linking this library statically or dynamically with other modules is making a combined work based on this library. Thus, the terms and conditions of the GNU General Public License cover the whole combination.

As a special exception, the copyright holders of this library give you permission to link this library with independent modules to produce an executable, regardless of the license terms of these independent modules, and to copy and distribute the resulting executable under terms of your choice, provided that you also meet, for each linked independent module, the terms and conditions of the license of that module. An independent module is a module which is not derived from or based on this library. If you modify this library, you may extend this exception to your version of the library, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

As such, it can be used to run, create and distribute a large class of applications and applets. When GNU Classpath is used unmodified as the core class library for a virtual machine, compiler for the java language, or for a program written in the java programming language it does not affect the licensing for distributing those programs directly.

Source code for this component can be found at <http://opensource.dell.com>.

CXXV. Portions of this product make use of TimeZoneInfo.Android.cs in Mono under Apache License, Version 2.0. You may obtain a copy of the license at <http://www.apache.org/licenses/LICENSE-2.0>

Copyright 2018 Microsoft

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS,

WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

CXXVI. Portions of Advanced Threat Prevention are licensed under GNU LESSER GENERAL PUBLIC LICENSE v3. You may obtain a copy of the license at <https://www.gnu.org/licenses/lgpl.txt> or request information at www.cylance.com.

Get Started

Get Started with Dell Data Security

- Once your environment has been configured in the Server Configuration Tool, ensure that Dell services are .
- [Log in](#) to the Management Console.
- Manage [Subscriptions](#)
- Add [Azure AD Users](#)
- 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 Data Guardian.

Log In

To perform a given administrative procedure, an administrator must first log in to the Management Console using an appropriate Dell administrator account.

1. Open a supported browser and type **<https://<console.dellsecuritycenter.com>/webui/<tenant>>**.
2. Click **Log in with Azure AD** and log in with Azure user credentials.

To log out, see [Log Out](#).

Log Out

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 Management Console and select **Log out** from the menu.

Dashboard

The dashboard displays an overview of status information for the organization. Access more detailed information directly from the dashboard by clicking its statistics, graphs, and chart legends.

In the top right, select the **Widgets** menu to add or remove the following widgets:

- Notifications
- Protection Status
- Protection History
- Inventory History
- Summary Statistics

The images below reflect what may be seen in the dashboard, depending on widgets enabled.

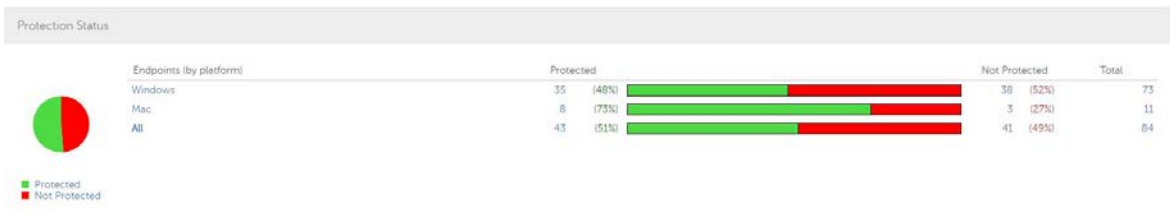
Click an area below to view a description of the detail accessible by clicking the same area in the dashboard.

Notifications

Dismiss Type: All Priority: All Search

Summary	Priority	Type	Date
Client License pool has been exceeded	Critical	Subscription	8/15/18 2:34 PM
Client License pool has been exceeded	Critical	Subscription	8/15/18 2:34 PM
Client License pool has been exceeded	Critical	Subscription	8/15/18 2:44 PM
Client License pool has been exceeded	Critical	Subscription	8/15/18 2:44 PM
Client License pool has been exceeded	Critical	Subscription	8/10/18 8:18 AM
Client License pool has been exceeded	Critical	Subscription	8/10/18 8:18 AM
Client License pool has been exceeded	Critical	Subscription	8/8/18 2:09 PM
Client License pool has been exceeded	Critical	Subscription	8/8/18 2:09 PM

Items per page: 25



Summary Statistics

Details		Endpoints (by platform)	
User Groups	2	Windows	9
Endpoint Groups	4	Mac	0
AD Users	28	All	9
Endpoints	9		
Protected	8		
Not-Protected	1		
Managers	10		
Modified Policies	0		

Navigate Dell Security Center

Management Console

The Management Console is the central control center that allows administrators to monitor the state of endpoints, policy enforcement, and protection across the enterprise.

The Management Console features security and configuration settings that are applied through policy to groups called Populations.

For increased security, administrator duties are separated 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 Management Console has the following features.

- Centralized management of diverse mobile devices
- Role-based mobile security policy creation and management
- Separation of administrative duties
- Automatic distribution of security policies
- Device inventory
- Searchable, ODBC-compliant system logs
- Trusted paths for communication between components
- Unique encryption key generation and automatic secure encryption key escrow
- Centralized compliance auditing and reporting

The menu pane allows access to the following functions.

Dashboard

The Management Console opens to the dashboard. The dashboard provides graphs and statistics on endpoints 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, security policies can be applied at the Enterprise, User Group, User, Endpoint Group, and Endpoint levels. See [Populations](#). See [Manage Security Policies](#).

Reporting

Reporting menu items provide reports on the protection state of the environment and endpoints, deployment issues that require action, and devices within the network. Create and manage reports with the [Manage Reports](#) tool. This menu allows you to collect, view, and export [audit events](#) to a SIEM server.

Management

Commit policies, manage subscriptions, services, alerts, and Data Guardian 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 - View information about Dell Security Center, get Dell ProSupport contact information, and log out.
- (3) Question mark icon - Open a help topic that explains the current screen in the Management Console.

Dashboard

Dashboard

The dashboard displays an overview of status information for the organization. Access more detailed information directly from the dashboard by clicking its statistics, graphs, and chart legends.

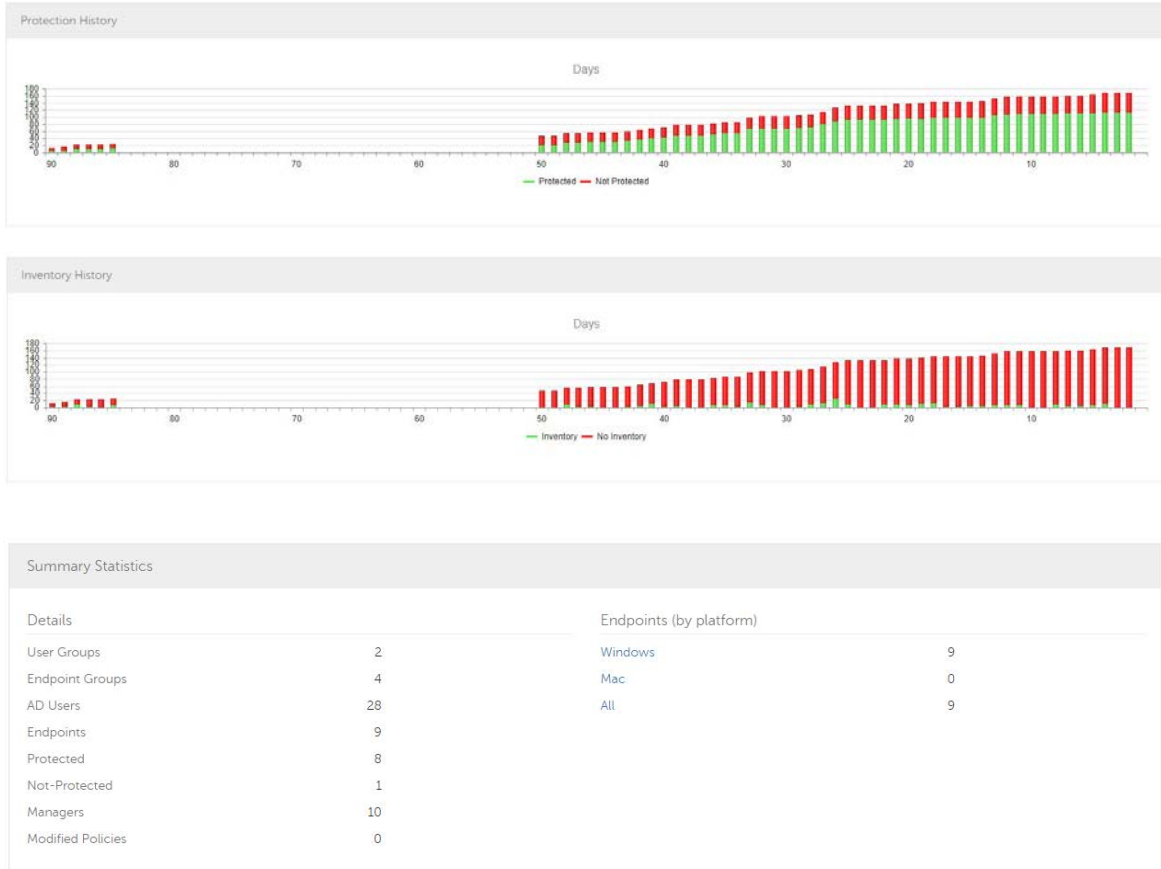
In the top right, select the **Widgets** menu to add or remove the following widgets:

- Notifications
- Protection Status
- Protection History
- Inventory History
- Summary Statistics

The images below reflect what may be seen in the dashboard, depending on widgets enabled.

Click an area below to view a description of the detail accessible by clicking the same area in the dashboard.





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

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.

Subscription - Alerts about subscriptions.

Announcement - News of upcoming releases and new products.

DDP Server Exceptions - A communication issue is impacting delivery of the following notifications: 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 list.

Priority Levels

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.

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 list to apply selections.

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

Protection Status

In the Protection Status section of the dashboard, view endpoint status by platform: Windows, Mac, 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 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.

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 Dell Security Center and the total number that have not sent inventory.

Summary Statistics

Summary Statistics provides a breakdown of the following:

- User groups
- Endpoint groups
- AD users

- Endpoints
- Protected
- Not protected
- 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
- 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

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 or Mac

Count - Number of endpoints or devices [Platform Report](#) for that platform

Shielded - Number of encrypted endpoints for that platform

Unshielded - Number of endpoints for that platform that are not encrypted

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 and select a Population. For example, **Populations > Enterprise**.

Tabs available on each Populations page provide information, allow you to edit details 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	Endpoint Groups	Endpoints	User Group
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.

The tabs available for an administrator may vary, depending on the role.

Enterprise

View or Modify Enterprise Policies

To view or modify Enterprise 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 Data Guardian, or policy group, such as Cloud Encryption, to view or modify.

Domains

Domain

Get more detailed information about the Domain.

In the left pane, click **Populations > Domains** to view Domain Details.

Details displayed on the Domain page:

- Domain Name
- Tenant Name
- Tenant Proper Name
- Setup Admin

Users

Users are added through reconciliation. Reconciliation is the automated process used to compare user data in the Dell Security Center with Azure. When a user attempts to log in or activate on an endpoint, the user credentials are verified with Azure and then added to their designated group.

In the left pane, click **Populations > Users** and then click a user name, to view details about the user. Click the arrow next to a User Name to view the Common Name, sAM Account Name, and User Principal Name.

Add Azure AD Users

1. In the left pane, click **Populations > Users**.
2. On the Users page, click **Add Azure AD Users**.
3. In the Add Users by Domain dialog, select a domain from the pull-down list.
4. In *Full name*, enter the exact text for the user name or use the wildcard character (*).
5. Select Common Name, Universal Principal Name, or sAMAccountName from the list.

A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user.

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 or click **Add**.

User Groups

Add a user group, [edit User Group priority](#), 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. Select the type of User Group from the list: **AzureAD** or **ADMIN-DEFINED User Group**

Note: If adding user groups for Access Groups, see [Set up Access Groups](#).

4. Select a domain from the list.
5. For Active Directory User Groups, follow these steps:
 - a. Enter the exact text for the group name or by first letter.

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

- d. Click **Add**.
6. For ADMIN-DEFINED User Groups, follow these steps:
 - a. Enter the exact text for the group name or use the wildcard character (*).
 - b. Enter a description for the group.
 - c. Click **Add Group**.

Notes:

Universal security groups are only supported for domains that connect through the Global Catalog port.

Nested groups are not supported.

User Groups

User Groups

Add a user group, [edit User Group priority](#), 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. Select the type of User Group from the list: **AzureAD** or **ADMIN-DEFINED User Group**
- Note:** If adding user groups for Access Groups, see [Set up Access Groups](#).
4. Select a domain from the list.
 5. For Active Directory User Groups, follow these steps:
 - a. Enter the exact text for the group name or by first letter.
 - b. Click **Search**. Depending on the size, this may take a few minutes to populate.
 - c. 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.

 - d. Click **Add**.
 6. For ADMIN-DEFINED User Groups, follow these steps:
 - a. Enter the exact text for the group name or use the wildcard character (*).
 - b. Enter a description for the group.
 - c. Click **Add Group**.

Notes:

Universal security groups are only supported for domains that connect through the Global Catalog port.

Nested groups are not supported.

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. The wildcard character (*) is supported.
3. Select a row to highlight it.
4. At the top, click **Delete**.

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. The wildcard character (*) is supported.
3. Click **Search**.

A Group or list of Groups displays, based on the 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 the User Group Detail page. The wildcard character (*) is supported.

Click a group name to display the User Group Detail page.

3. Click the tab that corresponds with the action 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:
- Last Modified in Directory - date and time stamp
- Last Reconciled - date and time stamp

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 Dell Security Center.

Details:

Group Name - 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.

Access Groups Enabled - Access Group is configured for a user group when selected.

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 click the numeral in the **Members column**.

Add Users to the Group

1. On the **Members** tab, click **Add Users to Group**.
2. Search or select a user, then select the check box to the left of the user name.
3. Click **Add Selected Users to Group**.

OR

Select **Upload Multiple User from File**, then click **Browse** to select a CSV file and click **Upload**.

Valid CSV requirements:

- The file must be in valid CSV format and contain a maximum of 999 endpoints.
- The first column must contain valid fully qualified host names. All columns except the first column are ignored.
- Only activated endpoints are added to the group.

Remove Users from the Group

1. In User Group Detail, search or select a user, then select the check box to the left of the user name.
2. Click **Remove Users from Group**.
3. Click **OK**.

Users can also be removed from the ADMIN DEFINED Groups.

User Group Admin

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](#)

Edit Group Priority

The Group priority feature is used to determine policy precedence for effective policies that affect multiple groups. Group priority creates a weight associated with the specific group it is assigned to, and that weight is used to determine which policy setting is applied to an endpoint that is a member of more than one Endpoint Group when policy settings differ between those groups. Policy overrides are used from the group with higher priority when two (or more) separate groups have different priority levels.

Edit Endpoint Group Priority

Endpoint Group Priority can be changed only for Rule-Defined, Admin-Defined, and Active Directory Groups. System-Defined Group priority cannot be modified. In general, the Endpoint Group at the top of the list of Endpoint Groups has highest priority. The Endpoint Group at the bottom of the list has lowest priority.

User Defined Endpoint Groups

+ Add
🗑 Delete
↕ Edit Priority
Group Type: All
Search

Priority	Group Name	Members	Overrides	Group Type	Description
1	Server-Test	0	0	Active Directory	this is a test
2	Accounting Group	0	4	Admin Defined	Accounting Department
3	g group	0	0	Admin Defined	g group desc
4		1	2	Rule Defined	a group

⏪
⏩
1
25 items per page
 1 - 21 of 21 items

System Defined Endpoint Groups

Group Name	Members	Overrides	Group Type	Description
Persistent VDI Endpoint Group	0		System Defined	Persistent VDI Endpoint Group
Non-Persistent VDI Endpoint Group	0		System Defined	Non-Persistent VDI Endpoint Group
Default Endpoint Group	4		System Defined	This group contains all endpoints, including endpoints that are defined in other endpoint groups.
Opt-In Endpoint Group	0		System Defined	This group contains all opt-in endpoints, including endpoints that are defined in other endpoint groups.

Precedence Ranking

The System Defined Non-Persistent VDI Endpoint Group has the highest priority level, followed by the Persistent VDI Endpoint Group.

Order of priority:

1. Non-Persistent VDI Endpoint Group
2. Persistent VDI Endpoint Group
3. Highest ranked Active Directory/Rule-Defined/Admin-Defined Endpoint Group
4. Second and subsequent highest ranked Active Directory/Rule-Defined/Admin-Defined Endpoint Groups
5. Opt-in Endpoint Group
6. Default Endpoint Group

To change Active Directory/Rule-Defined/Admin-Defined Endpoint Group priority:

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click **Edit Priority**.
3. Select the row of the appropriate group and drag it to the location in the list of Endpoint Groups that reflects its new priority level.
4. Click **Save**.

Edit User Group Priority

The user group at the top of the list has highest priority. The user group at the bottom of the list has lowest priority.

User Groups

+ Add
🗑 Delete
↕ Edit Priority
Group Type: All
Search

Priority	Group Name	Members	Group Type	Description	Last Modified	Last Reconciled
1	...	3	Admin Defined	An Admin-Defined User Group		
2	...	0	Admin Defined	Accounting group North Texas.		
3	...	5	Admin Defined	B group description		
4	...	0	Active Directory		3/23/15 1:36 PM	6/13/17 1:12 PM
5	...	7	Admin Defined	group		
6	...	7	Admin Defined	desc		
7	...	6	Active Directory		6/7/17 3:44 PM	6/13/17 1:12 PM
8	...	5	Active Directory		5/26/17 2:09 PM	6/13/17 1:12 PM
9	...	1	Active Directory		3/15/17 2:11 PM	6/13/17 1:12 PM
10	...	1	Active Directory		3/26/15 1:56 PM	6/13/17 1:12 PM

1
25 items per page
 1 - 10 of 10 items

To edit User Group priority:

1. In the left pane, click **Populations > User Groups**.
2. Click **Edit Priority**.
3. Select the row of the appropriate group and drag it to the location in the list of Endpoint Groups that reflects its new priority level.
4. Click **Save**.

Assign or Modify Administrator Roles

View or modify existing administrator privileges.

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

Dell recommends assigning administrator roles at the Group level rather than at the User level.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a group name, then the **Admin** tab.
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](#)

[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](#).

Users

Remove Users

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

Find Users

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

- Enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character is supported.
 - 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.

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. The wildcard character (*) is supported.

Click a user name to display the User Detail page.

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

Security Policies - Click to view or modify policies of the user.

Details & Actions - Click to view properties of the user. Viewable information includes:

User Name: (username@organization.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 - Click to view or modify information for the User's endpoints. For instructions on how to modify endpoint information, refer to [View or Modify Endpoint Information](#).

User Groups - Click **Groups** to view information for groups for which the user belongs. Click a user group to view the group's Security Policies, Details & Actions, Members, and Admin.

Admin - Click to view, assign, or modify administrator roles assigned to the user. Select or deselect administrator types to modify administrator roles assigned to the user.

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

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 - (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

Email - User email address

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 Shield, Mobile Device, and Cloud.

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

PBE

Data Guardian

Device ID - Value that uniquely identifies the target device

Activated - Date/time stamp, per endpoint

Updated - Date/time stamp, per endpoint

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 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](#).

Endpoint Groups

Endpoint Groups

On the Endpoint Groups page, you can [add](#) or [remove](#) an Endpoint Group, [edit Endpoint Group priority](#), or search and select an Endpoint Group to [view or modify Endpoint Group information](#).

Types of Endpoint Groups

System - Endpoint Group maintained by Dell Security Center. System groups include Default Endpoint Group, Opt-In Endpoint Group

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. For more information, see [Add Endpoints to an Admin-Defined Endpoint Group](#) or [Remove Endpoints from an Admin-Defined Endpoint Group](#).

Active Directory Group - Endpoint group for which the administrator can select a group from Active Directory for inclusion. The Active Directory group scope must be Global, and type must be Security. At least one endpoint in the Active Directory group must be running a Dell Data Security product and be managed by Dell Security Center.

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 *Select the type of Endpoint Group*, select **RULE-DEFINED Group**, **ADMIN-DEFINED Group**, or **Active Directory Group**.
4. In *Group Name*, enter a name for the new Endpoint Group.
5. In *Description*, enter a description for the new Endpoint Group.
6. (For Rule-Defined Groups only) In *Specification*, enter the rule that describes the Endpoint Group. Specifications can be up to 20,000 characters and are case insensitive.

(For Active Directory Groups only) In *Choose AD Group*, enter the beginning characters of an Active Directory group name (Example: Accounting), and select the desired group.

7. (For Rule-Defined and Active Directory Groups only) Click **Preview** to view the endpoints to be included in the group.
8. Click **Add Group** to save the group definition.
9. After the group is added, modify the group priority if necessary.

Remove an Endpoint Group

1. In the left pane, click **Populations > Endpoint Groups**.
2. Select the group to remove.
3. Click **Delete**, then click **OK**.

Modify an Endpoint Group

1. In the left pane, click **Populations > Endpoint Groups**.
2. Select the group to modify.
3. Click the **Details & Actions** tab.
4. Click **Modify**.
5. Make changes as desired.
6. Click **Update Group**.

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
UID	Windows hostname
DISPLAYNAME	Fully qualified hostname
OSVERSION	Operating system version as reported in inventory. Dell recommends 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.
WINCOMPUTERNAME	Fully qualified hostname
ASSETTAG	Asset tag of the computer manufacturer
PLUGINVERSION	Plugin version for Manager
MEMBEROFGROUP	Active Directory group name
MEMBEROFDOMAIN	Active Directory domain name
CLOUDPRESENT	All Dell Data Guardian clients
CLOUDINTERNAL	Internal Data Guardian clients
CLOUDEXTERNAL	External Data Guardian clients

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
```

Rule Specifications in the Management Console allows users to combine rules to filter a unique set of devices. For queries that contain multiple options, isolate sub-rules in parenthesis to ensure they are run separately before they are combined with the larger specification.

This query selects all devices with an operating system named Windows 10 Pro or Windows 10 Ent and DESKTOP in the hostname:

```
OS CONTAINS "Windows 10 Pro" OR OS CONTAINS "Windows 10 Ent" AND UID  
CONTAINS "DESKTOP"
```

This query selects any device containing Windows 10 Pro and only devices with the hostname containing DESKTOP that running an operating system with the name containing Windows 10 Ent:

```
OS CONTAINS "Windows 10 Pro" OR (OS CONTAINS "Windows 10 Ent" AND UID  
CONTAINS "DESKTOP")
```

- Data Guardian:

To display Data Guardian internal clients, add the specification "cloudpresent and clouinternal".

To display Data Guardian external clients, add the specification "cloudpresent and clouexternal".

For instructions about how to add an endpoint, see [Add Endpoint Groups](#).

Edit Group Priority

The Group priority feature is used to determine policy precedence for effective policies that affect multiple groups. Group priority creates a weight associated with the specific group it is assigned to, and that weight is used to determine which policy setting is applied to an endpoint that is a member of more than one Endpoint Group when policy settings differ between those groups. Policy overrides are used from the group with higher priority when two (or more) separate groups have different priority levels.

Edit Endpoint Group Priority

Endpoint Group Priority can be changed only for Rule-Defined, Admin-Defined, and Active Directory Groups. System-Defined Group priority cannot be modified. In general, the Endpoint Group at the top of the list of Endpoint Groups has highest priority. The Endpoint Group at the bottom of the list has lowest priority.

User Defined Endpoint Groups

+ Add 🗑 Delete ↕ Edit Priority
Group Type: All Search

Priority	Group Name	Members	Overrides	Group Type	Description
1	Server-Test	0	0	Active Directory	this is a test
2	Accounting Group	0	4	Admin Defined	Accounting Department
3	g group	0	0	Admin Defined	g group desc
4	a group	1	2	Rule Defined	a group

◀ 1 ▶ 25 items per page 1 - 21 of 21 items

System Defined Endpoint Groups

Group Name	Members	Overrides	Group Type	Description
Persistent VDI Endpoint Group	0		System Defined	Persistent VDI Endpoint Group
Non-Persistent VDI Endpoint Group	0		System Defined	Non-Persistent VDI Endpoint Group
Default Endpoint Group	4		System Defined	This group contains all endpoints, including endpoints that are defined in other endpoint groups.
Opt-In Endpoint Group	0		System Defined	This group contains all opt-in endpoints, including endpoints that are defined in other endpoint groups.

Precedence Ranking

The System Defined Non-Persistent VDI Endpoint Group has the highest priority level, followed by the Persistent VDI Endpoint Group.

Order of priority:

1. Non-Persistent VDI Endpoint Group
2. Persistent VDI Endpoint Group
3. Highest ranked Active Directory/Rule-Defined/Admin-Defined Endpoint Group
4. Second and subsequent highest ranked Active Directory/Rule-Defined/Admin-Defined Endpoint Groups
5. Opt-in Endpoint Group
6. Default Endpoint Group

To change Active Directory/Rule-Defined/Admin-Defined Endpoint Group priority:

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click **Edit Priority**.
3. Select the row of the appropriate group and drag it to the location in the list of Endpoint Groups that reflects its new priority level.
4. Click **Save**.

Edit User Group Priority

The user group at the top of the list has highest priority. The user group at the bottom of the list has lowest priority.

User Groups

[+](#) Add [-](#) Delete [↕](#) Edit Priority Group Type: All

Priority	Group Name	Members	Group Type	Description	Last Modified	Last Reconciled
1	Group 1	3	Admin Defined	An Admin-Defined User Group		
2	Accounting Group	0	Admin Defined	Accounting group North Texas.		
3	Group 3	5	Admin Defined	B group description		
4	Group 4	0	Active Directory		3/23/15 1:36 PM	6/13/17 1:12 PM
5	Group 5	7	Admin Defined	group		
6	Group 6	7	Admin Defined	desc		
7	Group 7	6	Active Directory		6/7/17 3:44 PM	6/13/17 1:12 PM
8	Group 8	5	Active Directory		5/26/17 2:09 PM	6/13/17 1:12 PM
9	Group 9	1	Active Directory		3/15/17 2:11 PM	6/13/17 1:12 PM
10	Group 10	1	Active Directory		3/26/15 1:56 PM	6/13/17 1:12 PM

25 items per page 1 - 10 of 10 items

To edit User Group priority:

1. In the left pane, click **Populations > User Groups**.
2. Click **Edit Priority**.
3. Select the row of the appropriate group and drag it to the location in the list of Endpoint Groups that reflects its new priority level.
4. Click **Save**.

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. The wildcard character (*) is supported.

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. The wildcard character (*) is supported.

When you click a Group Name, the Endpoint Group Detail page displays.

3. Click the tab that corresponds with the action 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

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.

Members - To view or modify the information of an endpoint in the group, click **Members**. Click an endpoint to view the endpoint's Security Policies, Details & Actions, Users, and Endpoint Groups.

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)

Active Directory Group (applies only to Active Directory Groups)

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, iOS, or Android

Hostname - Endpoint hostname

OS/Version - Endpoint operating system and version

Add Endpoints to an Admin-Defined Endpoint Group

1. In the left pane, click **Populations > Endpoint Groups**.
2. Select the group to which to add endpoints.
3. Click the **Members** tab.

4. Select **Add Endpoints to Group**, then search for specific endpoints or select endpoints in the list, and click **Add Selected Endpoints to Group**.

OR

Select **Upload Multiple Endpoints from File**, then click **Browse** to select a CSV file and click **Upload**.

Valid CSV requirements:

- The file must be in valid CSV format and contain a maximum of 999 endpoints.
- The first column must contain valid fully qualified hostnames. All columns except the first column are ignored.
- Only activated endpoints are added to the group.

Remove Endpoints from an Admin-Defined Endpoint Group

1. In the left pane, click **Populations > Endpoint Groups**.
2. Select the group in which to add endpoints.
3. Click the **Members** tab.
4. Search for specific endpoints or select endpoints in the list. To select more than one endpoint, press **Shift** and select the endpoints.
5. Click the red **X** in the right column for each endpoint, or select the endpoints and click **Remove Endpoints from Group**.

Endpoints

Endpoints

On the Endpoints page, you can [add an endpoint to a group](#), [remove an endpoint](#), or search and select an endpoint to [View or Modify Endpoint Information](#). You can also quickly view the following summary information about each endpoint:

*Hostname - Endpoint hostname.

*OS/Version - Operating system and version running on the endpoint (Example: Microsoft Windows 10 Enterprise).

*Category - Category of endpoint (Example: Windows or Mac).

*[Protected](#) - A green check displays if the endpoint is protected. If the endpoint is not protected, the column is blank.

*Serial Number - Manufacturer assigned serial number.

Manager - Manager/Agent version.

Data Guardian - Data Guardian version.

Hardware ID - A unique identifier sent to the server from the client.

* Click the column header to sort by column label.

Click a hostname to view additional details about the endpoint. Click an arrow at the left of a hostname to view the Category, Unique ID, and Processor.

Add Endpoint to Group

To add an endpoint to an Endpoint Group:

1. In the left pane, click **Populations > Endpoints**.
2. Select the check box next to a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

For Windows and Mac, if you know the endpoint hostname, enter it in *Search*. Leave the field blank to display all Windows and Mac endpoints.

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

3. At the top left, click **Add Endpoints to Group**.

An endpoint is added to inventory when a user activates the endpoint.

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 the box next to a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

For Windows and Mac, if you know the hostname of the endpoint, enter it in *Search*. 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. At the top left, click **Remove**.
5. Click **OK** to confirm removal of the endpoint.

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

View or Modify Endpoint Policies and Information

1. In the left pane, click **Populations > Endpoints**.
2. Select the appropriate endpoint type.
3. Click a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

For Windows and Mac, if you know the endpoint hostname, enter it in *Search*. Leave the field blank to display all Windows and Mac endpoints.

Click a hostname or endpoint serial number to display the Endpoint Detail page.

4. Click the tab that corresponds with the action to perform:

Security Policies - Click **Security Policies** to view or modify policies of the endpoint.

Details & Actions - Click **Details & Actions** to view properties of the endpoint, including Inventory Information. Viewable information includes hardware information, effective policies, inventory and protection status, and plugin details.

Plugins - Click **Plugins** view a list of plugins and agents to which this endpoint are plugged into. Viewable information includes status, state, version, and vendor version.

Users - Click **Users** to view a list of users who store and access data on the endpoint. These statistics of 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 - Click **Endpoint Groups** to view a list of Endpoint Groups to which this endpoint belongs. All endpoint belong to at least one endpoint group, the Default Endpoint Group.

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. Click a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

For Windows and Mac, if you know the endpoint hostname, enter it in *Search*. Leave the field blank to display all Windows and Mac endpoints.

Click a hostname or endpoint serial number to display the Endpoint Detail page.

3. On the Endpoint Detail page, click the **Details & Actions** tab.
4. Under *Plugin 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.

[Plugins](#)

Plugins

The Plugins & Agents page lists the plugin details for the selected endpoint.

To access Plugins & Agents, follow these steps:

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

Plugins & Agents

Agent - SED, FDE, Authentication Proxy, Preboot Authentication, Windows Authentication, BitLocker, TPM

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 - Encryption Management Agent/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 Management Console.

Disabled - Encryption Management Agent/Manager is disabled by policy and not enforcing any previously received policy.

Active - Encryption Management Agent/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 Encryption Management Agent/Manager client. Encryption Management Agent/Manager does not start a plugin until an initial policy is received from the Dell Security Center, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from the Dell Security Center, via the activation process, plugins are always started with the last policy the client is aware of.

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

- TPM Plugin:

Starting - Encryption Management Agent/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 Management Console.

Disabled - Encryption Management Agent/Manager is disabled by policy and not enforcing any previously received policy.

Active - Encryption Management Agent/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. Encryption Management Agent/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 Encryption Management Agent/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 does not start a plugin until an initial policy is received from Dell Security Center, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from Dell Security Center, via the activation process, plugins are always started with the last policy the client is aware of.

- SED Plugin:

Initialized - Encryption Management Agent/Manager is initialized waiting for delayed startup

Starting - Encryption Management Agent/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 Management Console.

Disabled - Encryption Management Agent/Manager is disabled by policy and not enforcing any previously received policy.

Active - Encryption Management Agent/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 Encryption Management Agent/Manager client. Encryption Management Agent/Manager does not start a plugin until an initial policy is received from Dell Security Center, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from Dell Security Center, via the activation process, plugins are always started with the last policy the client is aware of.

Waiting For Escrow - Encryption Management Agent/Manager is waiting for keys to escrow

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

No Opal Drive Present - Encryption Management Agent/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.

Endpoint Detail

Commands:

Remove - Endpoint is removed.

Recover - Provides instructions for endpoint recovery.

Endpoint Removal is not permanent. If an endpoint checks back in after it was removed, it re-appears in the Management Console.

Details:

[Windows](#)

Category - Windows

OS/Version - Example: Microsoft Windows 10 Enterprise

Processor

Serial Number - Manufacturer assigned serial number

Host ID - Endpoint identifier

Unique ID - Dell assigned unique identifier

Hardware ID - A unique identifier sent to the server from the client.

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

Host ID - Endpoint identifier

Unique ID - Dell assigned unique identifier

Hardware ID - A unique identifier sent to the server from the client.

Protected - Date and time stamp

Plugin Manager Detail

Command:

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

Version-Version of Data Guardian the endpoint is running.

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

Inventory Processed - the date and time that the inventory was picked up from the queue and processed.

Protected - the date and time that the device was protected.

Protected Status

Protected status is indicated if any of the following criteria are met:

- Data Guardian is installed and enabled.

To check Protected Status of an endpoint:

1. In the left pane, click **Populations > Endpoints**.
2. Click a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

For Windows and Mac, if you know the endpoint hostname, enter it in the *Search* field. Leave the field blank to display all Windows and Mac endpoints.

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

Click a hostname or endpoint serial number to display the Endpoint Detail page.

3. A green check mark displays in the Protected column if any of the criteria for Protected status are met.

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.

Data Guardian

User - Each user on the specific endpoint

Activated - Date/time stamp, per user

Update - Date/time stamp, per user

Administrators

Assign or Modify Administrator Roles

View or modify existing administrator privileges.

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

Dell recommends assigning administrator roles at the Group level rather than at the User level.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a group name, then the **Admin** tab.
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](#)

[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. 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.

There are 10 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.

The following table shows the tasks each administrator can perform in the Management Console.

Task	Performed by Type of Administrator							
	Help Desk	System	Security	Log	Account	Forensic ¹	Policy ²	Report
Log in	•	•	•	•	•			•
Log out	•	•	•	•	•			•
View current system state	•	•	•		•			
Search for Users, Groups, and Endpoints	•	•	•		•			
Add Users and Groups		•	•		•			
Remove an endpoint		•						
Change Dell Security Center Options		•	•					
Suspend a User			•					
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 Data Guardian		•	•					
Manage Data		•	•					

Guardian external users								
Manage Data Guardian external user key requests		•	•					
Revoke Data Guardian keys		•	•					

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 Dell Security Center.

Administrator rights are available to the delegated administrator only if the delegated administrator is a member of the user group in Dell Security Center. Delegated administrator rights are effective only with regard to Users who are members of the user group in Dell Security Center.

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.

Reporting

Manage Reports

Manage Reports

In the left pane, click **Reporting > Manage Reports**. For compliance and monitoring purposes, you can:

- [Manage reports](#)
- [View or modify an existing report](#)
- [Create a new report](#)

The Manage Reports page has:

- **New Report** - See [Create a new report](#).
- **Report Type** - Select **All** (default) or specific report types to display in the Name column. **Clear selected items** to undo selections. See [Report Type](#).

Note: Policy-based reports are not an option.

- **Grouping** - Group by **Report Type**, **Author**, **Private**, or **None** (default).
- **Columns** - Select which columns to display on the Manage Reports page, such as Name, Description, Report Type, Author. Also:
 - **Private - True** indicates only the owner of the report can access it.
 - Report Administrator - can view all public and private reports.
 - Other Administrators - can view private reports they created and all public reports.
 - **Created** - Date the report was created.
 - **Modified** - Date the report was modified.
- **Search** - Hover to view columns for performing a search, then enter specific text for those columns. Use * for a wildcard. For additional filtering to provide a detailed search on a specific report, see [Use Search and More to filter](#).

View or Modify an Existing Report

On the Manage Reports page, select a report from the Name column to view an instance of that report. The owner can make the report private or public. See [View Report](#).

Create a New Report

On the Manage Reports page, click **Create New Report** and select an option. An instance of that report opens to customize the information to display. See [View Report](#).

View Report

On the Manage Reports page, select an option in **Create New Report** or click an existing report in the **Name** column.

- New report - An administrator can select **Save As**. Save, Rename, and Delete options are activated, and the report is saved to the Manage Reports page. The owner can make the report private or public. You can create:
 - Single reports
 - Report templates - Determine frequent report content that you will generate. Select Column and Grouping options that are common to all those reports and save it as a template. See [View or modify an existing report](#).
- Existing report:
 - To filter a report, perform a query using **Search** and **More**.
 - Owner of a report - Can view their private reports and all public ones. Only the Owner or a Report administrator can modify or rename the report.
 - Report administrator - Can view all private and public reports. Can modify or rename public and private reports.
 - Public reports - Any administrator can select **Save As** to modify a copy of the report.

Grouping, Columns, and More differ for each report type. Some Column and Grouping options are selected by default.

- **Columns** allows customized options to display. After you select options, you can drag and resequence to avoid scrolling. The resequenced columns return to the default when you close the report.
- **Grouping** allows you to sort the column options you selected.
- Hover over *Search* to view suggested columns for performing a search, then enter specific text. Suggested column options differ for each report type. Use (*) as a wildcard.

For a description of each report's Column and Grouping options, click a link below.

Report Type	Description and link
Device Detail	Provides reports based on Windows, Mac, iOS, and Android device details. See Endpoint Details & Actions .
Notifications	Customize a report of news, alerts, and events or email notifications. See Notifications .
Log Analyzer	Customize a report of policy modifications or logs based on message priority level, date and time periods, and occurrences of usernames and hosts. See Log Analyzer .
Audit Event	Provides reports on the audit trail of file activity for Windows, Mac, mobile devices, and the web client. Data Guardian and Audit Events Get Started with Data Guardian Audit Events
Operational Logs	Provides reports from the SaaS around the day-to-day operation within the Dell Security Center.

Query using Search and More... to filter

Search performs a text-only quick search across multiple fields and may return numerous results.

- Hover to view columns that apply to this search, then enter specific text for those columns.
- Use * for a wildcard.

To filter and narrow the search with *More...* :

- Select **More...** and select a check box. Check boxes differ for each report type. Select one or multiple check boxes to narrow the search.
- An additional field displays for that check box option where you can either enter text to search on that column or select from a list of enumerators or a data type for that column.

Query example for Log Analyzer report

1. In Columns, select options. From menu options such as, **Priority** and **Category** select enumerators. **Created** allows you to filter by date.
2. Enter text in *Search* to perform a quick search on *Username* and *Message*.
3. For additional filtering, select **More....** and then select **Username**, **Message**, or both. Additional text fields allow you to limit the text search specifically to that column.

Query example for Data Guardian and Audit Events report

With Data Guardian, you can set specify policies and the *Protected Office* and *Beacon* Monikers to identify protected Office files in an unexpected location or a non-Data Guardian Device that tries to access a protected Office document. See [Protected Office Document or Basic File Protection audit events](#) or [Map visualization](#).

Export File

Export to Excel or a .csv file.

Data Guardian Audit Events

Data Guardian audit event logs maintain an audit trail of file activity for Windows, Mac, mobile devices, and the web portal. 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, select **Reporting > Audit Events**. The Audit Events page contains the map visualization and columns for filtering. For tips on getting started, see [Get Started with Data Guardian Audit Events](#).

Map visualization

In **Populations > Enterprise > Global Settings**, if you enable the *Data Guardian Geo Location Audit Data* policy and have the operating system's geolocation API, audit events that are sent to the Dell Security Center include the geolocation data (latitude and longitude) of each device. A map visualization of audit events can identify device locations that might indicate significant location changes or unexpected/questionable locations for devices within an organization. The geolocation is checked periodically, not each time an event is recorded. See [Examples of Map Visualization and Column Filters](#).

If the policy for geolocation is disabled, no geolocation data is contained in the audit events.

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 marker clusters until blue markers.
- **Blue marker** - Represents the location of a single audit event.
 - Click a marker to 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 time stamp indicates the user who last accessed the file. One user accessed numerous files.
- **Mapping points of interest and points visible** - Scroll to the bottom right of the columns to display the total number of items in the column. 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, 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.
 - Drill into a marker cluster to list the total points of interest and 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 only displays the area for that cluster, but the columns list all audit events in the original query. Select the check box on the lower right for the columns to only list audit events for those visible map points. As you continue to drill down, the columns only list the events for the visible map points. Clear the check box to return to the global view.

Audit Event Options and Filters

Use these options to determine the type and amount of audit event data to display.


- **Moniker** - By default, information displays for all monikers. Select one or more check boxes to display specific monikers. Click **Clear selected items** to display all.
 - Cloud Encryption - applies to:
 - Cloud Encryption (Mac, mobile and web portal; Windows Data Guardian v2.3 and earlier)
 - [Cloud Access Security Broker](#) (CASB) (web portal 2.9 and higher)
 - Basic File Protection (web portal 2.9 and higher with CASB, when a .xen file event is created)
 - Protected Office (Windows, Mac, mobile, and web portal) - also applies to [Cloud Access Security Broker](#)
 - [System](#) - Populates the user logged into or logged out of the device that has Data Guardian installed.
 - [Content Based Protection](#) - previously *Data Classification* (Windows)
 - [Protected Email](#) (Windows) - Relates to files other than protected Office documents.
 - [Share](#) (Windows) - Lists events when a user shares one or more files or attaches an encrypted file to an email.
 - [Beacon](#) - (protected Office documents) Indicates a device without Data Guardian installed that tried to access a protected file. These audit events may have limited data. For example, the location where the file was accessed but without the name of the user of the device.
- **Time stamp** - Select the amount of past time for audit events to display - 1, 7, 14, 30, 60, or 90 days.
- **More** - If you set filters and create a query, you can select the filter options in *More* to modify the query. As you select an option, it displays as a menu. Some actions apply to Windows, Mac, and mobile devices. Some are specific to one or more.
 - **Action** - The default is **All**. Select one or more check boxes to display specific actions associated with the payload file. See [Action](#) and the tables below for details and to determine the operating system.
 - **Cloud Action** - The default is **All**. Select one or more check boxes to display the reason for an Action. See [Cloud Encryption audit events](#) and the tables below for details and to determine the operating system.
 - **Data Guardian Action** - The default is **All**. Select one or more check boxes to display the reason for an Action. See

[Protected Office Document or Basic File Protection audit events](#) and the tables below for details and to determine the operating system.

- **Net Action - (Windows and Data Guardian v2.7 and earlier)**
- **Grouping** - Allows you to select one option. The default is **None**. For example:
 - **Moniker** - Groups by moniker if you have more than one selected.
 - **Device or User** - Allows you to determine the activity of specific devices or users.
 - **File Name, File Path or File Key ID** - With device and user columns added, allows you to see which users or devices accessed a file.
- **Columns** - Filter the amount of data by selecting one or multiple columns to display. If you clear all column check boxes, audit events are listed for all endpoints and all users. Some filters apply to all monikers and some to specific monikers. For a description of column filters, see [Options in the Columns menu](#).
- **Search** - Hover to view columns for performing a search (device, user, file name, and file key ID), then enter specific text for those columns. Use a wildcard (*) to search on .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, or .pdf.
- **Export File** - Export to Excel or a .csv file.

Options in the Columns Menu

Options can apply to all monikers or to a specific moniker. Policies must be enabled for audit data to display.

Search icons in the columns - If you click  next to an item in the device, user, file name, or key ID columns, it copies the cell content to *Search* and executes a search on that content. You can then select Action or IP address to do additional filtering.

Column options for all audit events

Audit Event - Column options	Description
Moniker - Select one or more.	Category of the audit event: <ul style="list-style-type: none"> • Cloud Encryption (mobile and web portal; Windows Data Guardian v2.3 and earlier; Mac; web portal for CASB; Basic File Protection) • Protected Office (Windows, Mac, mobile, web portal, CASB) • System (protected Office documents and Windows) • Content Based Protection - previously <i>Data Classification</i> (Windows) • Protected Email (Windows) • Share (Windows) • Beacon (protected Office documents)
Device	The hostname of the device where the event occurred.
User	User associated with the event. Typically, this is the email address of the activated user. See also Logged In User .
Logged In User	For manual activations or external users, the login name and email address used to activate may differ. If you do not recognize the user name, open the log files to view the logged-in user name. <ul style="list-style-type: none"> • In the log file for Protected Office, information displays as sl_protected_file. • In the log file for Cloud Encryption, information displays as sl_xen_file. Applies to Mac or mobile. Also applies to Windows Data Guardian v2.3 and earlier.
Timestamp	Date and time when the event occurred.
Created	Date and time when the entry was created. View this if a delay occurs.
Column options related to payload data:	Data for an audit event's moniker or parameters.

File Name	To search for a specific file, use the file key ID.
File Path	Note: When both .xen and protected Office files exist in Mac or mobile or Windows (v2.3 and earlier), 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.
File Key ID	
File Size	Note: For web portal and CASB, no File Path exists.
Client Type	Indicates whether the client is internal or external. For Windows and Mac, the only option is internal.
Action	The action associated with the payload file. See Protected Office Document or Basic File Protection audit events . For Mac or mobile, see also Cloud Encryption audit events .
Version	For internal Dell use only.
Client	For internal Dell use only. (Windows and Mac)

Column options for Protected Office only

Audit Event - Column options	Description
Data Guardian Action	If a service acts on a protected Office file, for example, modifying or deleting a file, the Data Guardian Action column lists the reason. See Protected Office Document or Basic File Protection audit events .
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.
See also Column options for all audit events .	

Protected Office Document or Basic File Protection audit events (Windows, Mac, mobile, web portal, CASB)

This table lists audit events that apply to Office documents or other files entered in Basic File Protection:

- For Windows and Mac, audit events apply to Opt-in or Force Protected modes.
- Mobile has Opt-in mode only.
- Protected Office document audit events do not contain the Cloud Name or Cloud Action events since protected Office documents can move to a cloud storage provider outside of the bounds of Data Guardian. Those display for XEN audit events under [Cloud Encryption](#).
- Basic File Protection events for Windows (excluding any .xen file extensions)

Actions for audit events	Data Guardian Action and Description	Windows	Mac	Mobile device	Web portal	CASB
Created	New 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 Data Guardian performs a sweep and creates protected Office documents.	•	•	•	•	•
Accessed	Open A user opened a protected Office document.	•	•	•	•	•
Modified	Swept For Windows, when Force Protected is enabled, provides data about files	•	•			

	that were swept and converted from unprotected to protected Office.					
Modified	Updated Summary of the number of times a file was changed since the last audit data transmission.	•	•	•	•	
Modified (Data Guardian v2.7 and earlier)	Watermarked User printed a file or exported a file with a watermark.	•	•			
Accessed (Windows only with Data Guardian v2.7 and earlier)	Block Copy Indicates a file where a user tried to copy from a protected Office document to an unprotected file and was blocked.	•				
Accessed (Windows only with Data Guardian v2.7 and earlier)	Blocked Print Indicates a file where a user tried to print a protected Office document and was blocked.	•				
Accessed	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. For the web portal, tampering is detected on protected Office documents but not .xen files.	•	•	•	•	
Modified	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 Data Guardian installed. Data Guardian repaired the wrapper or cover page.	•	•	•	•	
Attempt Access	Request Access An external user requested a key for a file to which they do not have access or the access time has expired. Audit data includes user account, time stamp, filename, key ID, and geolocation if enabled by policy.	•	•	•		
Modified	Unprotected: A Mac user unprotected a protected Office file or a Basic File Protected one-time decrypt. Windows - Opt-in mode only, for example, a protected Office document is open and the user selects Save As and unprotects it.	• (Opt-in mode)	•			
Deleted (Mac only)	Deleted The user deleted a .xen file from the cloud sync folder.		•			
Accessed (Mobile only)	Geo Blocked A user outside the geofence tried to access a protected document, and the attempt was blocked.			•		

Open (Windows only)	Used with Email Action .	•				
Sent (Windows only)	Used with Email Action .	•				
Reply (Windows only)	Used with Email Action .	•				
Forward (Windows only)	Used with Email Action .	•				

Column options for System (protected Office documents and Windows)

The following actions relate to the computer, so they have no corresponding Data Guardian action.

Note: The grey options apply to Windows and Data Guardian v2.7 and earlier.

Audit Event - Column options	Description
Login	If a user logged in and did a fast user switch, for example, logged in and then rebooted.
Logout	User logged out of a session.
Blocked PrintScreen (Windows only and Data Guardian v2.7 and earlier)	Indicates a file where a user tried to capture a screen while a protected Office document was open and is blocked.
Blocked Process (Windows only and Data Guardian v2.7 and earlier)	When policy blocks a specified process executable, indicates a file where a user tried to run that process executable.
Process Name (Windows only and Data Guardian v2.7 and earlier)	The name of the process that was blocked, for example, Snipping Tool.
Process Disposition (Windows only and Data Guardian v2.7 and earlier)	Indicates whether the process has exited or has been terminated.

Column options for Beacon only (protected Office documents)

Audit Event - Column options	Description
Column options related to geolocation: IP Address Routable Geo Type Latitude Longitude	IP Address - When a Beacon event comes in and the Beacon server can determine the location of the event, it lists the IP address. Routable - True or False <ul style="list-style-type: none"> • If True, geolocation data exists for that IP address and identifies the device's latitude and longitude based on each operating system's APIs. Note: If the Routable column lists True, but no geolocation data displays, an error occurred. • If False, the IP address is non-routable. Latitude and longitude - The data visualization is based on these 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. The column lists the coordinates as plus (+) or minus (-), correlating to North, South, East, or West. Geo Type - Typically, this is Point. Geolocation for audit events is supported on Windows 8.1 and higher

Column options for Cloud Encryption only (mobile and web portal; Windows Data Guardian v2.3 and earlier; Mac)

Greyed out options indicate earlier versions of Windows and Mac Data Guardian. See also [Column options for all audit events](#).

Audit Event - Column options	Description
Provider	Cloud storage provider. (Used for earlier versions.)
Cloud Name	Cloud storage provider name. See also File Name .
Cloud Action	If a service acts on a .xen file, the Cloud Action column lists the reason. See Cloud Encryption audit events .
Process Application	Process - Migration of Cloud Encryption events. A system event from the client performs an action on the .xen file. Application - <i>App</i> indicates this is part of the Cloud Encryption application.
Column options related to folder management (Windows only with Data Guardian v2.3 and earlier): Folder Path Folder Protection	If the <i>Folder Management Enabled</i> policy in Data Guardian > Cloud Encryption is enabled for an endpoint, a user can select the Data Guardian icon in the endpoint's notification area, select Manage Folders, and manually protect or unprotect a sync client folder. Typically, this policy is enabled for a manager on a temporary basis. This audit event allows you to monitor overrides to protected folders and investigate if files that need to be encrypted are now decrypted.

Cloud Encryption audit events (mobile and web portal; Windows Data Guardian v2.3 and earlier; Mac)

This table lists audit events that occur for files or folders stored in the cloud sync client folders. Events may differ slightly for Mac and mobile devices. Greyed out options indicate earlier versions of Windows and Mac Data Guardian.

Actions for audit events	Cloud Action and Description	Windows 2.7 and earlier	Mac	Mobile device	Web portal	CASB
Created	Encrypt A new .xen file has been uploaded and encrypted.	•	•	•	•	•
Modified	Encrypt An existing .xen file has been modified in the cloud and encrypted.	•	•	•	•	
Unprotected	Decrypt Data Guardian decrypted a .xen file.	•	•	•	•	
Deleted	Deleted A user deleted a .xen file from the cloud sync folder or cloud storage provider.	•	•	•	•	
Accessed	Decrypt A user accessed a .xen file, and Data Guardian decrypted it.					•
N/A	Upload (Windows 2.7 and earlier; Mac) Lists the folder path and whether the folder was protected.	•	•			

Column options for Cloud Access Security Broker (CASB) (web portal v2.9 and higher)

If an enterprise uses Data Guardian with Netskope, a Cloud Access Security Broker (CASB), to monitor cloud storage providers, you must select these monikers to run a report:

- Protected Office
- Cloud Encryption

The Device column lists *CASB*.

For actions, see the CASB column in [Protected Office Document or Basic File Protection audit events](#) and [Cloud Encryption audit events](#).

See also [Column options for all audit events](#).

Column options for Content Based Protection only (Windows)

Content Based Protection applies to Windows' Opt-in mode.

Policies: *Protected Office Documents, Content Based Protection, Content Based Protection Rules*. To include emails that must comply with a Content Based Protection rule, also enable *Email Encryption via Outlook*.

For a report, select from these column options.

Audit Event - Column options	Description
Content Rule	The content rule category, such as Public, Internal Use, or Restricted.
Content Rule File	The name of the file that was audited or encrypted based on a content rule.
Content Rule Path	The location of the file.
Content Rule Action	Based on the content rule selected, these actions can display: <ul style="list-style-type: none"> • Audit - If a rule in the Categories list has a priority of two and higher, audit events are created. • Encrypt - If the Encrypt check box is selected for a rule in the Categories list, the file was encrypted based on the rules set. <i>Public</i> rule has no actions.
Content Rule Triggers	The rules that cause the actions to occur.

Column options for Protected Email only (Windows)

Audit Event - Column options	Description
Email Keyid	The Key ID used to protect the email .
Email Subject	Subject line from the email.
Email From	The email address of the person who sent the email.
Email To	Email addresses of recipients.
Email Cc	Email addresses of those copied.
Email Bcc	Email addresses of those blind-copied.
Email Attachment	Names of attachments added to the email.
Email Action	What the user did with the action. In Protected Office Document or Basic File Protection audit events , see Opened, Sent, Reply, and Forwarded.

Column options for Share only (Windows)

In [Column options for all audit events](#), see User, Logged in User, Client Type, Action. You can also select File, Email, Group, and Status.

Actions for Share are listed here.




Actions for Share audit	Description	Windows
-------------------------	-------------	---------

events		
Add	A protected file or email was shared with a user or a group. This applies to pre-share.	●
Remove	Data Guardian Access to a protected file or email has been revoked from a user or a group.	●
Request	A user had to request access to a protected file or email because they did not have access.	●

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. For example:

- **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 time stamp 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 **Data Guardian Action**, the column lists the reason for a user modifying files, such as *Updated* or *Swept*. For information on Action and Data Guardian Action, see [Options in the Columns menu](#), [Cloud Encryption audit events](#), and [Protected Office Document or Basic File Protection audit events](#).

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  next to a device, user, file name, or key ID.
For example, click  next to a user name, then click  next to a file name to zoom to the map location of the specified user when a specified file was accessed.
4. Clear *Search* and press **Enter** to return to the global map view.

Return to [Data Guardian](#) policies.

Get Started with Data Guardian Audit Events

Before you begin, navigate to **Populations > Global > Settings** and select the *Data Guardian Audit Data Enabled* policy for these policy groups:

- **Audit Control Policies** (for Windows or Mac)
- **Web Portal Audit Policies**
- **Mobile Audit Control Policies**


In the **Dell Security Center > Reporting > Audit Events**, use these examples to get started.

For detailed information about column options, see [Data Guardian and Audit Events](#).

Audit Protected Office Documents

To audit protected Office documents only:

1. In *Moniker*, select **Protected Office**.
2. In *More*, select **Action** and **Data Guardian Action**.
3. In *Columns*, select **Device**, **User**, **Timestamp**, **File Name**, and **File KeyID**.
4. Optionally, in *Grouping*, select one item like **Device** or **User** to sort.
5. Select **Export File > Excel** or **CSV** to view the data for the *Action* and *Data Guardian Action* columns. For more information, see Protected_Office_Document_audit_events. Optionally, you can export the audit events to a SIEM server.
6. To identify issues, return to the Dell Security Center, click **Data Guardian Action**, and select:
 - **Block Copy** (for Windows) - indicates a Windows user tried to copy from a protected Office document and was blocked.
 - **Geo Blocked** (for Mobile) - indicates a mobile user outside a geofence tried to access a protected document and the attempt was blocked.

If these options display in the Data Guardian Action column, click  next to that user or device. In **Data Guardian Action**, click **Clear selected items** and view all the actions by that user or device to determine a potential issue. For more information, see [Protected Office Document audit events](#).

7. To identify issues, select **Data Guardian Action** and select the following:
 - Detected tampering
 - Repaired tampering

If these options display, determine any potential issues.

8. For Windows, in **Moniker**, select **System**. In **Action**, select **Login** and **Logout** to identify a user who logged into the device that has Data Guardian installed.
9. Analyze the data in the Dell Security Center or select **Export File > Excel** or **CSV** where you can sort the data. Optionally, you can export the audit events to a SIEM server.

Audit events related to external users

In addition to the steps above:

1. In *Columns*, select:
 - **Client Type** - to indicate internal or external users.
 - **From** and **To** - to audit embargo and external users.
 - **Request Access** - an external user requested access to encryption keys from an internal user.
2. Analyze the data in the Dell Security Center or select **Export File > Excel** or **CSV** where you can sort the data. Optionally, you can export the audit events to a SIEM server.

Map visualization


You can use this to identify protected Office files in an unexpected location or a non-Data Guardian Device that tries to access a protected Office document.



For map data to display, you must enable policy. See **Global > Settings** and select the *Data Guardian Geo Location Audit Data* policy from one or more of these:

- **Audit Control Policies**
- **Web Portal Audit Policies**
- **Mobile Audit Control Policies**

For Beacon events, see the advanced settings for **Data Guardian** and select the *Enable Callback Beacon* policy from one or more of these policy groups:

- **Protected Office**
- **Mobile Client**
- **Web Portal**

1. In **Moniker**, select **Protected Office** and **Beacon**.
2. In the global map view, drill in to a marker cluster in an unexpected location and select a blue marker.
3. Select the *Show only visible* check box for the columns to list only the files for that audit event.
4. Click  next to a Device, User, File Name, or File KeyID.

For example, click  next to a user name, then click  next to a file name to zoom to the map location of the specified user when a specified file was accessed.

5. Analyze the data in the Dell Security Center or click **Export File > Excel** or **CSV** where you can sort the data. Optionally, you can export the audit events to a SIEM server.
6. Clear *Search* and press **Enter** to return to the global map view.

Audit Cloud Encryption (Mac or mobile)

To audit protected .xen files only:

1. In *Moniker*, select **Cloud Encryption**.
2. In *More*, select **Action** and **Cloud Action**.
3. Initially, in *Columns*, select Device, User, Timestamp, File KeyID, Provider, Action, and Cloud Action.

Default Monikers and Columns

If you leave the defaults, all monikers and columns display. Select one item from Grouping to sort monikers or column options. Select options to minimize the data that displays.

EU General Data Protection Regulation (GDPR)

For privacy laws in Europe, you can disable audit events. See **Enterprise > Global Settings > Settings > Web Portal Audit Policies**.





View Audit Events (Geolocation)

Click **Audit Events** in the left pane to view geographic map points of file events on computers and devices running Data Guardian.

For a list of audit event types, see [Data Guardian and Audit Events](#).

For information about exporting audit events to a SIEM server, see [Export 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 - Data Guardian 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 Key ID - GUID that identifies the key used to protect the file

File Name - File name with extension

Action - File action that triggered the event

Data Guardian Action - Action taken by Data Guardian, based on policy and the file action that triggered the event

Select columns to display from the **Columns** list.

Management

Commit Policies

Uncommitted policies display in a badge icon in the top left of the Management Console. Click the badge icon to navigate to **Management > Commit**.

To commit policies that have been modified and saved:

1. In the left pane, click **Management > Commit**.
2. In Comment, enter a description of the change.
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 policies 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 or export logs:

1. In the left pane, click **Management > Log Analyzer**.
2. Select a Category.
 - The Categories are Admin Actions, System logs, Policy, and Full Access List.
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 - Select 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, 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 to sort.
 6. To export the results to an Excel or CSV file, pull down the **Export File** list and select **Excel** or **CSV**.
- Exported files can hold up to 100,000 records.

Subscriptions

Subscriptions

To view usage of Subscription Licenses that you own and reclaim subscription licenses, click **Management > Subscriptions**.

View Total Seats Used

1. In the left pane, click **Management > Subscriptions**.
2. Select the **Seats Used** tab.

Reclaim Subscription Licenses

1. In the left pane, click **Management > Subscriptions**.
2. Select the **Reclaim Seats** tab.

Related topics:

[Subscriptions Information](#)

Subscriptions Information

Upon log in to the Management Console, if there is a problem with your subscription, an error message displays (typically, the error states that your license usage has exceeded the number of subscriptions purchased). The next step is follow instructions on how to reclaim licenses or add subscriptions to your account.

If authorized license exceeds the current subscription, new client activations for that specific product is blocked until the license key is brought into compliance. No other client or Dell Security Center functions is impacted when a license key is in the over 105% state. Two separate warning messages are displayed, the first warning message is when the subscription reaches 99% of the authorized licenses, the second when the subscription count reaches or exceeds the 105% total.

For example:

- Authorized subscription for Dell Guardian: 5000 user licenses
- First warning message from Dell Security Center and an email message is sent to the administrator: License count reaches 5000
- Second warning message from Dell Security Center and an email message is sent to the administrator: License count reaches 5250

If a client has previously been activated and inventory records exist, then it is not blocked from any re-activation. However, if the subscription authorized count is exceeded during this process, new activations are blocked for the specific license that is in the over 105% state.

Subscriptions

1. Subscription structure:
 - a. Dell Data Guardian
2. Dell Digital Delivery of entitlements

Subscriptions

Alert	Type	Used	Total
OK	Data Guardian	41	25002

Subscriptions

Hostname	Platform	Manager Inventory Received +	Manager Inventory Processed
[Redacted]	Windows	6/20/18 4:13 PM	6/20/18 4:13 PM
[Redacted]	Windows	6/29/18 4:58 PM	6/29/18 4:58 PM
[Redacted]	Windows	7/6/18 12:48 PM	7/6/18 12:48 PM
[Redacted]	Windows	7/18/18 10:59 PM	7/18/18 10:59 PM
[Redacted]	Windows	7/23/18 1:50 PM	7/23/18 1:50 PM
[Redacted]	Windows	7/23/18 4:08 PM	7/23/18 4:08 PM
[Redacted]	Mac	7/23/18 4:14 PM	7/23/18 4:14 PM
[Redacted]	Windows	7/25/18 10:51 AM	7/25/18 10:51 AM
[Redacted]	Mac	7/30/18 9:04 AM	7/30/18 9:04 AM
[Redacted]	Windows	8/2/18 3:42 PM	8/2/18 3:42 PM
[Redacted]	iOS	8/2/18 3:42 PM	8/2/18 3:42 PM
[Redacted]	Android	8/2/18 3:42 PM	8/2/18 3:42 PM
[Redacted]	Windows	8/3/18 3:17 PM	8/3/18 3:17 PM
[Redacted]	Windows	8/3/18 3:35 PM	8/3/18 3:35 PM
[Redacted]	Mac	8/3/18 3:43 PM	8/3/18 3:43 PM
[Redacted]	Mac	8/6/18 2:23 PM	8/6/18 2:23 PM
[Redacted]	Windows	8/21/18 2:04 AM	8/21/18 2:04 AM
[Redacted]	iOS	8/23/18 5:22 AM	8/23/18 5:22 AM
[Redacted]	iOS	8/23/18 7:47 AM	8/23/18 7:47 AM
[Redacted]	iOS	8/23/18 10:20 AM	8/23/18 10:20 AM

Services Management

Events Management - Export Audit Events to a SIEM Server

To export audit events to a syslog server or to a local file:

1. In the left pane, click **Management > Services Management**.
2. Select the **Events Management** tab.

3. Select the appropriate option(s):
Export to Syslog lets you specify the syslog server to which to export the file. If TCP protocol is not selected, select it.
4. Click the **Save Preferences** button.

Enable Data Guardian Access Groups

You can allow access to selected user groups to collaborate on encrypted data by updating Access Groups preferences. Users outside that group cannot access or view the data unless the owner of the file grants access. See [Configure Access Groups](#).

Note: Access Groups were initially named Circle of Trust. The Management Console is in the process of updating the user interface.

To enable Access Groups:

1. In the left pane, navigate to **Management > Services Management**.
2. Select the **Data Guardian** tab.
3. For Access Groups, click **On**.
Important: Currently, if you enable Access Groups, you cannot disable it.
3. Click **Save Preferences**. A check box displays.
4. Optionally, if you are implementing a transitional period for an initial implementation, click the *Auto access for swept files* check box. When the transitional period is complete, clear the check box.
5. Click **Save Preferences**.
6. Continue with [Configure Access Groups](#).

Notification Management

Notification Management

The Notification Management page lets you manage email notifications.

To add an email notification:

1. In the left pane, click **Management > Notification Management**.
2. Click **Add** and enter the following information:
Email: Enter or select your email address.
[Notification Type](#): Select the type of alert to add.
[Priority Level](#): Select the priority levels of notifications.
Email Frequency: Select how often alerts of this type. The default frequency is 24 hours.
3. Click **Add** when complete.

To edit an alert:

- Select the alert to change, click **Edit**, make the changes, and press **Enter**.

To delete an alert:

- Select the alert to delete, and click **Delete**.

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, click **Management > Notification Management**.
2. Select the **Configure Notifications** tab.


External User Management

Registration Access

To allow or block Data Guardian access for users who are not in the organization's domain:

1. In the left pane, click **Management > Data Guardian Management**.
2. Select the **Registration Access** tab.
3. Click **Add**.
4. 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.
5. Enter either a domain to set access for the entire domain, or email address to set access only for a single user.
6. Click **Add**.

External users can also be added to the blacklist from the Audit Events page, if the user is associated with an audit event:

1. In the left pane, click **Reporting > Audit Events**.
2. In the user column, click  to the right of the user name to add to the blacklist.

Key Request

Data Guardian external users can request a key from an internal user to access a protected Office document. Key requests are shown on the Key Request Management page until the internal user approves or denies the request. After 48 hours, key requests are removed from the list. At that time, external users can request access again.

If the internal user is not available or has left the enterprise, an administrator can use this page to approve or deny requests.

Columns include:

- User - external user making the request

- File Name
- Request Date
- Request Expiration
- File Owner - internal user
- Approve/Deny

To approve or deny a request:

1. In the left pane, click **Management > Data Guardian Management**.
2. Select the **Key Request** tab.
3. Search for specific requests or select requests in the list.

To select multiple requests to approve or deny, press **Ctrl** and then select the requests.

To select multiple sequential requests, select the first request and then press **Shift** and select the last request in the sequential list.

4. Click **Approve** or **Deny**.

To approve or deny a single request, click approve  or deny  icon at the right end of the request.

Key Revocation

The administrator can revoke access to files, at both the user level and the file level.

To revoke access:

1. In the left pane, click **Management > Data Guardian Management**.
2. Select the **Key Revocation** tab.
3. Select the user or file from which to revoke files.
4. Click **Revoke Keys**.

Data Guardian Management

Registration Access

To allow or block Data Guardian access for users who are not in the organization's domain:

1. In the left pane, click **Management > Data Guardian Management**.
2. Select the **Registration Access** tab.
3. Click **Add**.
4. 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.

5. Enter either a domain to set access for the entire domain, or email address to set access only for a single user.

6. Click **Add**.

External users can also be added to the blacklist from the Audit Events page, if the user is associated with an audit event:

1. In the left pane, click **Reporting > Audit Events**.
2. In the user column, click  to the right of the user name to add to the blacklist.

Key Request

Data Guardian external users can request a key from an internal user to access a protected Office document. Key requests are shown on the Key Request Management page until the internal user approves or denies the request. After 48 hours, key requests are removed from the list. At that time, external users can request access again.

If the internal user is not available or has left the enterprise, an administrator can use this page to approve or deny requests.

Columns include:

- User - external user making the request
- File Name
- Request Date
- Request Expiration
- File Owner - internal user
- Approve/Deny

To approve or deny a request:

1. In the left pane, click **Management > Data Guardian Management**.
2. Select the **Key Request** tab.
3. Search for specific requests or select requests in the list.

To select multiple requests to approve or deny, press **Ctrl** and then select the requests.

To select multiple sequential requests, select the first request and then press **Shift** and select the last request in the sequential list.

4. Click **Approve** or **Deny**.

To approve or deny a single request, click approve  or deny  icon at the right end of the request.

Key Revocation

The administrator can revoke access to files, at both the user level and the file level.

To revoke access:

1. In the left pane, click **Management > Data Guardian Management**.
2. Select the **Key Revocation** tab.
3. Select the user or file from which to revoke files.

4. Click **Revoke Keys**.

Key Management

The administrator can manage key ownership.

The keyid is available here:

- **Reporting > Audit Events > Columns > File KeyID**. See [Options in the Columns menu](#).
- On the client side, a user can right-click a protected file to see the KeyID.

To find/change the owner for a key:

1. In the left pane, navigate to **Management > Data Guardian Management**.
2. Select the **Key Management** tab.
3. Enter the keyid and click **Find Owner**. The owner displays in the **Current Owner** field.
4. In the **New Owner** field, enter the email address of the new owner and click **Change Owner**.

To change ownership for all keys:

1. In the left pane, navigate to **Management > Data Guardian Management**.
2. Select the **Key Management** tab.
3. Select **Change Ownership for ALL keys**.
4. Enter the email address of the current owner.
5. Enter the email address of the new owner.
6. Click **Change Owner**.

If changing ownership for all keys, a table, *Key Changes in Progress*, displays at the bottom during the transfer. When complete, this content is removed. The [Log Analyzer](#) displays a log of the entries in the *Transfer of keys* column that have changed ownership.

Downloads

Endpoint Software

To download the latest version of Dell Data Guardian:

1. In the left pane, click **Management > Downloads**.
2. Select the **Endpoint Software** tab.
3. Choose from the following:
 - **Navigate to Download** (for Windows or Mac)
 - **Download on the App Store** (for iOS)
 - **Get it on Google Play** (for Android)

The **Download** tab is only available if the user has been assigned a security and a system administrator role.

Configuration

To activate endpoints with the Dell Security Center, an Installation ID may be required:

1. In the left pane, click **Management > Downloads**.
2. Select the **Configuration** tab.
3. Copy the **Installation ID**.

The **Download** tab is only available if the user has been assigned a security and a system administrator role.

CASB Management

Dell Security Center can link with Netskope. If a Netskope tenant is linked to Dell Security Center:

- The Management Console includes a link to Netskope's console labeled *CASB Management*.
- Administrators can access Netskope's console and select policies to invoke Data Guardian encryption with cloud storage providers.

To access the Netskope console:

1. Navigate to **Management > CASB Management**.

Manage Policies

Manage Security Policies

You can apply security policies at the Enterprise, Domain, User Group, User, and Endpoint Group levels. Default policy settings allow your enterprise to get started with Dell security, but you should customize the security and configuration settings.

Security policies are grouped by technology. Click a technology group to view its policies and policy descriptions.

<u>Data Guardian</u>	<u>Global Settings</u>
<u>Cloud Encryption</u>	<u>Settings</u>
<u>Protected Office Documents</u>	
<u>Content Based Protection</u>	
<u>Mobile Client</u>	
<u>Web Portal</u>	
<u>Settings</u>	








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.

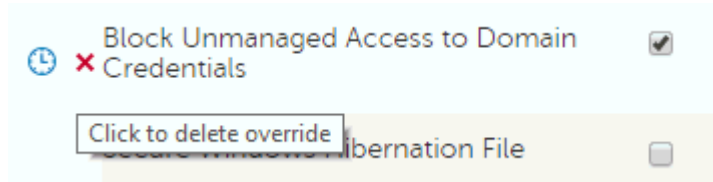
NOTE: The Security Policies page for a population displays overrides to localizable policies in the browser language only.

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, so that policies on the endpoint computer display 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 User Group Policies and Information](#)

[View or Modify User Policies and Information](#)

[View or Modify Endpoint Group Policies and Information](#)

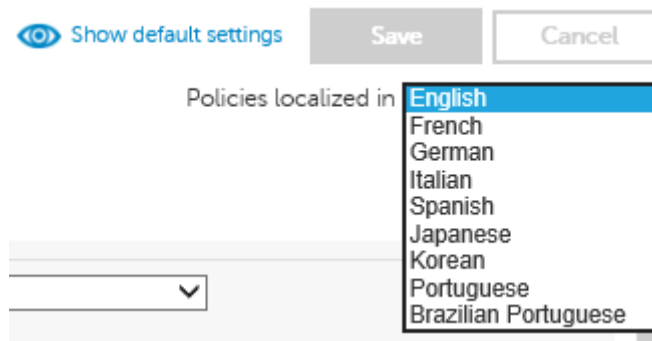
[View or Modify Endpoint Policies and Information](#)

Localize Policies Displayed on the Endpoint Computer

[Localizable policies](#) are indicated by: 

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 Data Guardian or a policy group, such as *Classification*, to modify.
4. Select a language for localizable policies from the 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 list, enter localized text for all desired policies, and click **Save**.


Save policy changes before selecting another language in the 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 are made in the language that displays.

Policies localized in

NOTE: The Security Policies page for a population displays overrides to localizable policies in the browser language only.

Localizable Policies

Localizable policies are indicated with by 

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
Data Guardian > Cloud Encryption	Help File Name
	Help File Contents
	Excluded Folders
	Excluded Files
Data Guardian > Protected Office	Office Protected Clip Board Unauthorized Text

Documents

Office Protected Document Tamper Prompt

Offline Key Generation Escrow Reminder Text

Office Protected Files Cover Page Notice

Data Guardian > Mobile Client > Cover Page

Office Protected Files Cover Page Acceptance Text

Office Protected Document Tamper Prompt

Data Guardian > Web Portal

Office Protected Files Cover Page EULA

Data Guardian

Overview of Data Guardian Features and Policies

This topic provides a brief overview of the Data Guardian key features and policies.

Protect data in use, in motion, or at rest

The following are some of the key Data Guardian features that allow you to protect data:

- [Basic File Protection](#) - allows an enterprise to sweep users' computers and encrypt a large number of file types (non-Office). Encrypted files are logged and audited.
- **Office document protection** - allows an enterprise to encrypt Office documents and PDFs for [Windows or Mac with opt-in mode](#), [Windows or Mac with Force-protected mode](#), [mobile devices](#), and a [Data Guardian web portal](#).

In addition, Windows and opt-in mode have:

- [Content Based Protection](#) - Based on content rules, a sweep of users' computers encrypts files that contain specified content like account numbers or Social Security Numbers.
- [TITUS classification](#)
- [Cloud Encryption](#)
- [Access Groups](#) - Administrators can specify groups and only those users can view the encrypted files.

Control data

Determine who can access data and revoke access if needed:

- [Registration Access](#)
- [Key Request](#)
- [Key Revocation](#)
- [Key Management](#)

- [Web Portal](#)

Monitor data

To detect potential security risks, monitor audit events and create reports to identify who uses the data and how it is used.

- [Data Guardian and Audit Events](#)
- [Get Started with Data Guardian Audit Events](#)
- [View Audit Events \(Geolocation\)](#)
- Export Events to SIEM Server
- [Manage Reports](#)
- [View Report](#)
- [Add Schedule](#)

Policies

To set policies for these features, see:

- [Data Guardian](#) - basic policies
- [Advanced Data Guardian](#)

Data Guardian

Data Guardian provides the following:

- Data on the device and data-in-motion is encrypted. To decrypt and view the content, users must have Data Guardian installed on the client. Users can access protected files on Windows, Mac, mobile devices, and a web portal.
- An audit trail of file activity allows you to monitor security. See [Data Guardian and Audit Events](#).

Data Guardian basic policies are available for these populations:

- [Cloud Encryption](#) (Mac; v2.3 and earlier for Windows) - Enterprise, Endpoint Groups, and Endpoints
- [Protected Office Documents](#) - Enterprise (master switch)
- [Content Based Encryption](#) - previously *Classification* - Enterprise (master switch)
- [Mobile Client](#) - Enterprise, Domain, User Groups, and User
- [Web Portal](#) - Enterprise, Domain, User Groups, and User
 - Node level policies are only available at the Enterprise level and require a node restart.
 - Lock Account is only available at the User level.

Policy descriptions also display in tooltips in the Dell Security Center. In this table, master policies are in bold font.

Policy	Default Setting	Description
--------	-----------------	-------------

<p>Cloud Encryption This technology allows for files to be automatically encrypted prior to being uploaded to supported public clouds; this maintains ownership/control of all data encryption keys. The supported public cloud providers are Dropbox, Dropbox for Business, Box, OneDrive, OneDrive for Business, and Google Drive.</p>		
<p>Cloud Encryption (Mac; 2.3 and earlier for Windows)</p>	<p>Off</p>	<p><i>On</i> <i>Off</i> Toggle <i>On</i> to enable Cloud Encryption policies. If this policy is <i>Off</i>, no Cloud protection takes place, regardless of other policies.</p>
<p>Enable Access to Restricted File (Windows - v2.3 and earlier)</p>	<p>Not Selected</p>	<p><i>Selected</i> <i>Not Selected</i> Applies only to Google Drive. <i>Selected</i> disables any Google Drive-created shortcuts to the web that Data Guardian cannot encrypt.</p>
<p>Enable In-App Feedback (Cloud) (Mac; v2.3 and earlier for Windows)</p>	<p>Not Selected</p>	<p><i>Selected</i> <i>Not Selected</i> When selected, an end user can submit feedback and satisfaction ratings to Dell via a link within the client application to a web form.</p>
<p>Cloud Storage Protection Providers (Mac; v2.3 and earlier for Windows)</p>	<p>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.</p>	<p><i>String</i> 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. The format is: ProtectionLevel,ProfileName. ProtectionLevel options: Allow, Protect, Block, Bypass Dell Security Center automatically checks for updated profiles of Cloud storage providers supported with Data Guardian. When available, updated profiles are sent to Data Guardian clients after the administrator commits policy changes. When the Pending Policy Changes value in the 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.</p>
<p>Dropbox Encrypt Personal Folders (Windows- v2.3 and earlier)</p>	<p>Selected</p>	<p><i>Selected</i> <i>Not Selected</i> Selected encrypts personal cloud storage provider folders.</p>
<p>Dropbox Encrypt Personal Folders Message (Windows- v2.3 and earlier)</p>	<p>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 Dell Security Center .</p>	<p><i>String</i> Message to display when Dropbox Encrypt Personal Folders is set to Not Selected. This message is customizable by the Administrator.</p>
<p>Help File Visible (Windows- v2.3 and earlier)</p>	<p>Selected</p>	<p><i>Selected</i> <i>Not Selected</i> Selected allows the registration help file to be visible in the provider folder. More... <i>Not Selected</i> hides the help file, therefore, potential file sharers does not be redirected to the registration URL located at https://console.<Domain</p>

		Name>/cloudweb/register.
See advanced settings		
Policy	Default Setting	Description
Protected Office Documents This technology allows for Office documents (Excel, PowerPoint, and Word) to be encrypted at the file level. Encryption travels with the file wherever it goes, inside or outside the network.		
Protected Office Documents (Windows and Mac)	On	<i>On</i> <i>Off</i> Toggle <i>On</i> to provide users with a menu option for protecting Office documents (.docx, .xlsx, .pptx, .docm, .xlsm, .pptm, and .pdf). <i>On</i> also allows you to enable other Protected Office policies. If this policy is <i>Off</i> , no Office-protected formatting takes place, regardless of other policies. This policy is available at the Enterprise level.
Basic File Protection (Windows and Mac)	Not Selected	Selected Not Selected When selected, the Basic File Protection Feature is enabled. This feature allows for the key-per-file encryption of line of business files that are not covered within Microsoft Office.
Basic File Protection Configuration (Windows and Mac)	String	String Specifies which process and which extensions are included in Basic File Protection. For Windows, specifies which process and which extensions are included in Basic File Protection. For Mac and mobile devices, these encrypted files are read-only. These encrypted files can be uploaded to the web portal. The following are examples to follow for specific format inclusions: Notepad.exe:txt.csv Wordpad.exe:txt.rtf Word.exe:txt.rtf Note: Basic File Protection Configuration is supported in Data Guardian v1.6 and later. See Configure Basic File Protection Policies .
Block Print Screen (Windows- 2.7 and earlier)	Selected	<i>Selected</i> disables the user's ability to take screen captures via the Windows Print Screen capability while a protected office document is open. Note: To block this option, Data Guardian must be installed and run on the operating system, not a VM or Remote Desktop.
File Icon Overlay (Windows)	Selected	An overlay icon for Windows that indicates a file is protected by Data Guardian.
See advanced settings		
Policy	Default Setting	Description
Content Based Protection This technology allows for files to be encrypted based on selected rule category level.		
Content Based Protection (previously <i>Classification</i>) (Windows)	Off	<i>On</i> <i>Off</i> Toggle <i>On</i> to provide users with a menu option for protecting files based on content rules. If this policy is <i>Off</i> , files are not automatically protected based on content rules.

		See Column options for Content Based Protection only Windows.
Content Based Protection Rules (previously <i>Data Classification Rules</i>) (Windows)	test (default) Public Internal Use Restricted	Selected Not Selected When selected, the selected content rule applies for encrypting files.
Policy	Default Setting	Description
Mobile Client This technology allows mobile phones and tablets access to encrypted content on supported public clouds, including Dropbox, Box, Google Drive, OneDrive, and OneDrive for Business.		
Data Guardian	Off	Off Cloud Protection Office Protected Documents <i>Both</i> Select one option or <i>Both</i> to use Data Guardian with mobile clients. If this policy is <i>Off</i> , Data Guardian 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	<i>Selected</i> <i>Not Selected</i> Selected encrypts personal cloud storage provider folders.
Basic File Protection	Not Selected	Selected Not Selected When selected, the Basic File Protection Feature is enabled.
Basic File Protection Configuration	String	String Specifies which process and which extensions are included in Basic File Protection. For mobile, copy and paste the processes and extensions from the Windows Basic File Protection policy. For Mac and mobile devices, these encrypted files are read-only. See Basic File Configuration for Mobile .
Geo-Fencing		
Enable Geo-Fencing	Not Selected	<i>Selected</i> <i>Not Selected</i> Selected allows only users in the region selected in the <i>Geo-</i>

		<i>Fencing Location</i> policy to access files.
Geo-Fencing Location	US and Canada	<i>US</i> <i>Canada</i> <i>US and Canada</i> Sets the location in which users can access files. The <i>Enable Geo-Fencing</i> policy must be Selected.
See advanced settings		
Policy	Default Setting	Description
Web Portal The Web Portal is a web-based client for creating and editing documents protected by Data Guardian.		
Edit Permission	Selected	<i>Selected</i> <i>Not Selected</i> Selected allows users to edit files within the web client.
External User Edit Permission	Not Selected	<i>Selected</i> <i>Not Selected</i> Selected allows external users to edit files within the web client.
Main Title Image (Enterprise only)	Choose File button	Image or logo to display on the login page. The 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. On a single node with Dell Security Center, you can select a different one for each tenant.
Masthead (Enterprise only)	Choose File button	Image to display as the masthead on the login page. The image must be a .png file, 26x26 pixels. On a single node with Dell Security Center, you can select a different one for each tenant.
Access Agreement (Enterprise only)	String	Agreement text to be displayed for users to accept before they are allowed to log in. On a single node with Dell Security Center, you can select a different one for each tenant.
See advanced settings		
Policy	Default Setting	Description
Settings This technology enables/disables Data Guardian Mac and Data Guardian Mobile access.		
Allow Mac Data Guardian Activation	Selected	<i>Selected</i> <i>Not Selected</i> <i>Not Selected</i> prevents Mac Data Guardian clients from being activated.
Allow Mobile Data Guardian Activation	Selected	<i>Selected</i> <i>Not Selected</i> <i>Not Selected</i> prevents Mobile Data Guardian clients from being activated.

Advanced Data Guardian

Advanced Data Guardian policies are available for these populations:

- [Cloud Encryption](#) (Mac; v2.3 and earlier for Windows) - 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
- [Web Portal](#):
 - Node level policies are only available at the Enterprise level and require a node restart.
 - Lock Account is only available at the User level.

See [Data Guardian policy groups](#) to determine which policies to enable.

Policy descriptions also display in tooltips in the Dell Security Center. In this table, master policies are in bold font.

Policy	Default Setting	Description
Cloud Encryption This technology allows for files to be automatically encrypted prior to being uploaded to supported public clouds; this maintains ownership/control of all data encryption keys. The supported public cloud providers are Dropbox, Dropbox for Business, Box, SkyDrive, OneDrive for Business, and Google Drive.		
Cloud Encryption (Mac; v2.3 and earlier for Windows)	Off	<i>On</i> <i>Off</i> Toggle <i>On</i> to enable Cloud Encryption policies. If this policy is <i>Off</i> , no Cloud Encryption protection takes place, regardless of other policies.
iOS Document Handling (Windows)	Disallow	<i>Allow</i> <i>Disallow</i> 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 <?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> <style type="text/css">P { text-align: center }</style> </head> <body> <h3>%PRODUCTNAME%</h3> <hr /> <p> The files in this folder have been secured using %PRODUCTNAME%. 	HTML for the registration help file. HTML validation is not performed. The files in this folder have been secured using Data Guardian. 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.

Dell Security Center v10.2.7 AdminHelp

	<p>To view the files in the folder, you need to register with the owner of the files.

 <a >click="" a><br="" here="" href="%ACTIVATIONURL%web/register" register<="" to=""> </p> </body> </html></p>	
Excluded Folders (Windows)	<p>String %windir% %SystemDrive%\\$recycle.bin %ProgramFiles% %SystemDrive%\users*\appdata %ProgramFiles(x86)% %ProgramData%\WebEx</p>	<p>String Folders excluded from encryption, separated by carriage returns. A "!" before the variable means to exclude exactly that directory. Folders without the "!" are partial matches, so everything that starts with the path is excluded.</p>
Excluded Files (Windows)	<p>String C3901A99-1A1B-55B4-AE11-891207B1D341.xen desktop.ini thumbs.db creddb.cef ~\$* ~* ~*.tmp .DDPCE.attr *.lnk</p>	<p>String Files excluded from encryption, separated by carriage returns.</p>
Server Polling Interval (Windows and Mac)	360 minutes	<p>1-1440 minutes How often, in minutes, the client checks in with Dell Security Center for updates. Default is 360 minutes (6 hours).</p>
Software Update Server URL (Windows)		<p>String Use this policy if software updates for users is located at an alternate Server URL.</p>
Obfuscate Filenames (Mac; v2.3 and earlier for Windows)	Extension only	<p>Extension only Select <i>Extension only</i> to display the actual filename with the ".xen" extension.</p>
Folder Management Enabled (Windows- v2.3 and earlier)	Not Selected	<p>Not available for v2.8 and higher. Selected Not Selected <i>Selected</i> allows management of encryption on a folder-by-folder basis within the sync client folders. For example, if users uploaded files before installing Data Guardian, you can provide temporary Folder Management rights to some users. To provide temporary Folder Management rights to a user:</p> <ol style="list-style-type: none"> 1. Set this policy for the specific endpoint to Selected. 2. Instruct the user to manually turn on encryption for the pre-existing folder.

		<p>The files are encrypted when the files sync to the cloud.</p> <p>3. After the folders are encrypted, set the <i>Folder Management Enabled</i> policy for the endpoint back to <i>Not Selected</i>.</p>
See basic settings		
Policy	Default Setting	Description
<p>Protected Office Documents This technology allows for Office documents (Excel, PowerPoint, and Word) to be encrypted at the file level. Encryption travels with the file wherever it goes, inside or outside the network.</p>		
Protected Office Documents (Basic - Windows and Mac)	Off	<p><i>On</i> <i>Off</i></p> <p>Toggle <i>On</i> to provide users with a menu option for protecting Office documents (.docx, .xlsx, .pptx, .docm, .xlsm, .pptm, and .pdf). <i>On</i> also allows you to enable other Protected Office policies. If this policy is <i>Off</i>, no Office-protected formatting takes place, regardless of other policies.</p> <p>This policy is available at the Enterprise level.</p>
Folder Exclusions for Basic File Protection (Windows and Mac)	String	<p>String</p> <p>Listing of folder paths that are excluded from Basic File Protection.</p> <p>See Configure policy to exclude folders.</p>
Protected Office Document Process Protection (Windows - 2.7 and earlier)	String	<p>String</p> <p>Specifies which process and which extensions to block while a Protected Office Document is open. The following are examples to follow for specific format inclusions: SnippingTool.exe mspaint.exe</p>
Force Protected Files Only (Windows)	Not Selected	<p><i>Selected</i> <i>Not Selected</i></p> <p><i>Selected</i> 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.</p> <p>If <i>Not Selected</i>, users have some options in determining whether to save a file as protected or unprotected.</p>

Dell Security Center v10.2.7 AdminHelp

<p>Enable Time To Live and Embargo Control (Windows)</p>	<p style="text-align: center;">Not Selected</p>	<p><i>Selected</i> <i>Not Selected</i> Selected allows users to specify dates for when protected Office files are accessible to external users.</p>
<p>Print Control (Mac; Windows- v2.7 and earlier)</p>	<p style="text-align: center;">Allowed</p>	<p><i>Allowed</i> <i>Watermark</i> <i>Disabled</i> Controls the Print function of protected Office documents (.docx, .xlsx, .pptx, .docm, .xslm, .pptm, and .pdf):</p> <ul style="list-style-type: none"> ● 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 enabled. However, if the user clicks Print for a protected Office document or when a protected Office document is open in Acrobat Reader DC, a toaster states that Print is not allowed. In addition, the attempt to print is an audit event. Users can always print unprotected Office documents. <p>If Force Protected Files Only is <i>Not Selected</i>, the Print option is available for all unprotected Office documents.</p>
<p>Export Control (Windows - v2.7 and earlier)</p>	<p style="text-align: center;">Allowed</p>	<p><i>Allowed</i> <i>Watermark</i> <i>Disabled</i> For Office 2013 and higher, controls the Export function of protected Office documents (.docx, .xlsx, .pptx, .docm, .xslm, .pptm, and .pdf):</p> <ul style="list-style-type: none"> ● Allowed - This varies based on whether Force Protected Files Only is <i>Selected</i>. 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.
<p>Protected Office Clip Board Unauthorized Text (Windows - 2.7 and earlier)</p>	<p>Pasting of protected data is not allowed on this computer. Please contact your administrator for assistance.</p>	<p>String to display when a user attempts to paste secure data from a protected document into an unprotected location.</p>
<p>Protected Office Document Tamper Prompt (Windows)</p>	<p>The file has been tampered with. Contact the author or your administrator.</p>	<p>String to display if a user encounters an Office-protected document that is identified as having been tampered with.</p>

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)	Data Guardian has not been able to contact Dell Security Center 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.
Protected Office Documents Cover Page Notice (Windows and Mac)	String	Enterprise-defined text to be displayed on Office-protected cover pages. Maximum number of characters is 4096. See Set Cover Page Policies . 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. For Dell Security Center, if you have multiple tenants, you can customize this policy for each tenant.
Protected Office Documents 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 . 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. For Dell Security Center, if you have multiple tenants, you can customize this policy for each tenant.
Enable Callback Beacon	Not Selected	Selected inserts a callback beacon into every protected Office file. To use the callback beacon, the following requirements must be met: <ul style="list-style-type: none"> An administrator must have enrolled to receive Product Notifications.
Hidden Audit Trail within Protected Office Document (Windows and Mac)	Selected	Enables a hidden watermark audit trail within a Protected Office Document. For information on decrypting protected documents to view audit data, see Data Guardian in the <i>Recovery Guide</i> . See also web client and Mobile .
On Screen Watermark (Windows - 2.7 and earlier)	Not Selected	<i>Selected</i> <i>Not Selected</i> <i>Selected</i> displays a watermark on the client computer screen when any protected Office file is open.
Encrypt based on Titus Classification (Windows and Opt-in mode)	Not Selected	<i>Selected</i> <i>Not Selected</i> <i>Selected</i> causes the supported files to be converted into Protected Office Documents if a Titus classification is specified.
Titus Classification Encryption Mapping (Windows and Opt-in mode)	String	Requires "Encrypted based on Titus Classification" to be enabled. This policies specifies which classifications, when selected, will have files classified as such automatically converted to Protected Office Documents. Each Classification is separated by a carriage return, semi-colon, or comma. Example: Restricted Classified

		This policy is supported as of Data Guardian v1.6 and later. See Set TITUS classification .
Allow File Exclusions	Not Selected	<i>Selected</i> <i>Not Selected</i> <i>Selected</i> allows internal users to place files within an Unprotected Documents folder where no data is protected. This applies only when <i>Force Protected Files Only</i> is selected.
Email Encryption via Outlook	Selected	<i>Selected</i> <i>Not Selected</i> <i>Selected</i> allows users to send emails as Protected by Data Guardian.
See basic settings		
Policy	Default Setting	Description
Mobile Client This technology allows mobile phones and tablets access to encrypted content on supported public clouds, including Dropbox, Box, Google Drive, OneDrive, and OneDrive for Business.		
Enable Callback Beacon	Not Selected	Selected inserts a callback beacon into every protected Office file. To use the callback beacon, the following requirements must be met: <ul style="list-style-type: none"> An administrator must have enrolled to receive Product Notifications.
Hidden Audit Trail within Protected Office Document	Selected	Enables a hidden watermark audit trail within a Protected Office Document. For information on decrypting protected documents to view audit data, see Data Guardian in the <i>Recovery Guide</i> . See also Windows and Mac and web client .
On Screen Watermark	Not Selected	<i>Selected</i> <i>Not Selected</i> <i>Selected</i> displays a watermark on the mobile client screen when any protected Office file is open.
Server Polling Interval	360 minutes	<i>1-1440 minutes</i> How often, in minutes, the client checks in with the Data Guardian for updates. Default is 360 minutes (6 hours).
Workspace Access		
Application pass code (PIN)	4	<i>4 or 6</i> Required number of characters for Workspace PIN.
Set maximum failed login attempts	8	<i>4 - 16</i> 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	<i>Timeout for 1 minute</i> <i>Timeout for 5 minutes</i> <i>Lock Workspace</i> <i>Wipe Workspace Data</i> 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	<i>Selected</i> <i>Not Selected</i> <i>Selected</i> allows users to copy and paste outside of the workspace.
Allow Non-Genuine device OS	Not Selected	<i>Selected</i> <i>Not Selected</i> <i>Selected</i> allows a jailbroken iOS device or a rooted Android device.
Cover Page		
Protected Office Documents Cover Page Notice	String	Enterprise-defined text to be displayed on Office-protected cover pages. See Set Cover Page Policies . For Dell Security Center, if you have multiple tenants, you can customize this policy for each tenant.
Protected Office Documents 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 . 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. For Dell Security Center, if you have multiple tenants, you can customize this policy for each tenant.
Protected Office Documents Cover Page Dell Server URL	String	Dell Security Center URL that is displayed on the cover page. Note: With mobile, for the URL to work with all file types, it must have http or https prepended.
Protected Office 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		
Policy	Default Setting	Description
Web Portal The Web Portal is a web-based client for creating and editing documents protected by Data Guardian.		
Protected Office Documents Cover Page Notice	String	Text to be displayed on Protected Office Documents Cover Page. The text in this policy is translatable. For Dell Security Center, if you have multiple tenants, you can customize this policy for each tenant.

Dell Security Center v10.2.7 AdminHelp

Protected Office Documents Cover Page Corporate Logo	Choose File button	Corporate logo to display on the document cover page. The 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. For Dell Security Center, if you have multiple tenants, you can customize this policy for each tenant.
Protected Office Documents Cover Page Dell Server URL	String	Dell Security Center URL that is displayed on the Cover Page.
Enable Callback Beacon	Not Selected	Selected inserts a callback beacon into every protected Office file. To use the callback beacon, the following requirements must be met: <ul style="list-style-type: none"> An administrator must have enrolled to receive Product Notifications.
Hidden Audit Trail within Protected Office Document	Selected	Enables a hidden watermark audit trail within a Protected Office Document. For information on decrypting protected documents to view audit data, see the Data Guardian in the <i>Recovery Guide</i> . See also Windows and Mac and Mobile .
On Screen Watermark	Not Selected	<i>Selected</i> <i>Not Selected</i> <i>Selected</i> displays a watermark on the mobile client screen when any protected Office file is open.
Basic File Protection	Not Selected	Selected Not Selected When selected, the Basic File Protection Feature is enabled. This feature allows for the key-per-file encryption of line of business files that are not covered within Microsoft Office.
Basic File Protection Configuration	String	String Specifies which process and which extensions are included in Basic File Protection. For Windows, specifies which process and which extensions are included in Basic File Protection. For Mac and mobile devices, these encrypted files are read-only. These encrypted files can be uploaded to the web portal. The following are examples to follow for specific format inclusions: Notepad.exe:txt.csv Wordpad.exe:txt.rtf Word.exe:txt.rtf Note: Basic File Protection Configuration is supported in Data Guardian v1.6 and later. See Configure Basic File Protection Policies .
See basic settings		

Set Cover Page Policies

For Windows, Mac, mobile, and web portal, you can set policies to customize a cover page for protected Office documents.

- Internal users for all platforms and external users for mobile and web portal - The cover page displays for the following:

- *Protected Office Documents* policies have been enabled, but the user has not yet installed or activated Data Guardian.
- User opens a protected Office document or .pdf from the cloud.
- User downloads a protected Office document or .pdf to a device that does not have Data Guardian 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 Data Guardian](#) policies:

- Protected Office Documents Cover Page Notice
- Protected Office Documents Cover Page Corporate Logo

See also, Data Guardian Management > [Web Portal](#) to add a URL to access the web portal.

Note: If a hosted Dell Security Center has multi-tenants:

- You can customize the notice policy and corporate logo policy for each tenant
- A unique installation ID also displays on the cover page

Configure Basic File Protection Policies

With Data Guardian v1.6 and higher, you can configure a large number of file extensions (non-Office) to encrypt and identify the applications to open them. This policy applies at the Enterprise level.

For Windows and Mac, a sweep of users' computers encrypts those configured file types. For Windows, Mac

This topic includes:

- [Supported applications and file types](#)
- [Additional applications and file types](#)
- [Configure policy for Basic File Protection](#)
- [Configure policy to exclude folders](#) (Windows and Mac)
- [Unsupported applications and file types](#)
- [Use the Recovery Tool](#)

Supported applications and file types

This table lists applications and file types that Dell has certified.

Supported applications	Supported file extensions	Description
<p>Dell has certified these applications:</p> <ul style="list-style-type: none"> • Notepad • Wordpad • Visio • MSPaint <p>Add these applications if you want them to open the supported file extensions. For an example, see</p>	<p>.bmp .csv .gif .jif .jpe .jpg .jpeg .png</p>	<p>In the policy configuration field, enter the application, followed by applicable file extensions. As a best practice, only add the essential file extensions to prevent performance issues.</p> <p>.tmp extension Be aware that if you add a .tmp extension, all Temp files are encrypted. Use only if necessary.</p>

NoRename. <ul style="list-style-type: none"> Word (winword) Excel PowerPoint 	.tmp .rtf .tif .tiff .txt .vsdx	
These applications are partially supported: <ul style="list-style-type: none"> Microsoft.Photos.exe (Windows 10) 	.bmp	See .bmp file.
	This file extension is partially supported: .odt	Currently, when opened with Wordpad, a protected .odt file may not save new content.
Add these applications if required by another application: <ul style="list-style-type: none"> Sihost Code Writer Runtime Broker 	Add applicable extensions from above.	Here are examples: RuntimeBroker.exe:png.rtf.txt.bmp CodeWriter.exe:rtf.txt

Additional applications and file types

Many applications and file types should work. However, Dell has not certified all. In addition, enterprise-created applications and file types may work.

You can add other applications and file types, but as a best practice, configure them in a test environment before deploying to your enterprise.

If you test frequently used or essential applications and would like Dell to confirm that and add them to the Supported list or if issues arise, contact Dell support.

Configure policy for Basic File Protection

Overview

With Data Guardian v1.6 and higher, you can configure applications and file types, such as .txt or .png, in addition to Office documents. This policy applies at the Enterprise level. A sweep of users' computers encrypts those configured file types.

Policy	Description for Force Protected	Version availability
Before you enable Basic File Protection (optional but important): <i>Enterprise > Data Guardian > Protected Office Documents > advanced:</i> Folder Exclusions for Basic File Protection > string	You may want to allow users to exclude existing files with that file extension from an encryption sweep, for example: <ul style="list-style-type: none"> To prevent files needed by the system from being encrypted To create a folder where users can place files of that type that do not require security or encrypting Windows and Mac: See Configure policy to exclude folders. Note: You must inform users to create this folder and place existing files there <i>before</i> you enable Basic File Protection.	Windows Mac v1.6 and higher
<i>Enterprise > Data Guardian > Protected Office Documents:</i> Protected Office Documents > On Basic File Protection > check box selected Basic File Protection Configuration > string	Windows and Mac For more information, see Configure Basic File Protection Policies. For Mac, it protects files in the Home folder. Windows and Mac - audit events <ul style="list-style-type: none"> For compliance and monitoring purposes, creates audit events. 	Windows Mac v1.6 and higher
<i>Enterprise > Data Guardian > Protected Office Documents > advanced:</i> Allow File Exclusions > check box selected	Users must remove files from the Unprotected Documents folder for these file types to be swept and encrypted. An <i>Unprotected Documents</i> folder is added to the root of each computer's <i>Documents</i> folder. When users place a Basic File Protection file in that folder, Data Guardian automatically decrypts it.	Windows Mac

To configure additional file types to be encrypted:

1. In the left pane, click *Populations > Enterprise*, enable the **Protected Office Documents** policy.
2. In the *Data Guardian > Windows* technology group, enable the **Basic File Protection** policy.

Note: This policy applies to the Enterprise population only. Also, if you enable *Allow File Exclusions*, users must remove files from the Unprotected Documents folder for these file types to be swept and encrypted.

3. In Windows technology group's *Basic File Protection Configuration* policy field, enter an application that you want to be encrypted, followed by a colon, for example:

notepad.exe:

4. After the colon, add the file extensions that is encrypted and any processes needed to support that application. Here are some sample configuration strings that Dell has certified. Only add essential extensions to prevent performance issues.

wordpad.exe:rtf.odt.txt.png.jpg.csv.bmp

notepad.exe:txt.csv

visio.exe:vsdv.png.jpg.jpeg.jpe.jfif.gif.tif.tiff.bmp

mspaint.exe:png.jpg.jpeg.jpe.jfif.gif.tif.tiff.bmp

sihost.exe:png.jpg.jpeg.jpe.jfif.gif.tif.tiff.rtf.txt.bmp

microsoft.photos.exe:png.jpg.jpeg.jpe.jfif.gif.tif.tiff.bmp

5. For Mobile, copy the extensions from the Windows policy to the **Enterprise > Mobile Client > Basic File Protection Configuration** policy. The file extensions in the Mobile policy must match Windows.

Basic File Protection policy and operating systems

- **Windows and Mac:** When the policy is enabled, these files are swept and Data Guardian encrypts all local files with those extensions. Files encrypted with Basic File Protection can only be viewed and edited using the application associated with the file extension. Mac requires Force-Protected mode.
- **Web Portal:** If the *Edit Permission* policy is enabled for web portal, users can edit them.

Some folders are excluded from Windows' Basic File Protection sweep and files are not encrypted:

- AppData
- Some System folders
- Folders that relate to protected Office documents, such as the Secure Documents folder

6. If applicable, add these workflows to the policy lists:

- **NoRename** - add this for Office applications to ensure that if users open them, they can only save them as an Office file, not as a Basic File Protection file. Here are some examples:

winword.exe:NoRename.odt.txt.png.jpg.csv.rtf.jpeg.jpe.jfif.gif.tif.tiff.bmp

excel.exe:NoRename.png.jpg.csv.jpeg.jpe.jfif.gif.tif.tiff.bmp

powerpnt.exe:NoRename.png.jpg.jpeg.jpe.jfif.gif.tif.tiff.bmp

Note: Do not add Office file extensions to this policy configuration.

- **NoNetwork** – if users go to a network and files hang when users close them, add this to the application to prevent network save.
8. Before deploying Basic File Protection to the enterprise, be sure to test applications and file extensions in a test environment to ensure that the intended file types remain encrypted. Also, you can download procmon (process monitor) to determine file types that might create an issue for that application.
 9. Inform users:
 - Which applications and file types your enterprise encrypts
 - Which operating systems can be used and whether files are read only or can be edited
 - Files sent to external users or to devices that do not have Data Guardian installed

Configure policy to exclude folders for Basic File Protection (Windows and Mac)

After you enter file types, like .txt or .png, in the *Basic File Protection Configuration* policy field, a sweep will encrypt those files on the client computers.

You may want to exclude some of those file types, for example:

- To prevent files needed by the system from being encrypted
- To create a folder where users can place files of that type that do not require encrypting

In the *Folder Exclusions for Basic File Protection* policy, enter the path for a folder on client computers to exclude files from a Basic File Protection sweep.

Note: You cannot exclude the *Secure Documents* folder.

Windows example

Enter the string in one of these formats based on type:

- C:\Program Files, System, or a subfolder in those paths - for files needed by the system
- Variables with a %VALUE% format
- KNOWNFOLDERID - for Windows-specified known-folder ID mappings. For example, enter a string for a uniquely named folder like *My Excluded Basic File Types* and then tell users to create that folder in their User Profile. Here are examples of supported formats for Known Folder ID mappings:
 - GUID with dashes:
D0384E7D-BAC3-4797-8F14-CBA229B392B5
 - GUID without dashes:
D0384E7DBAC347978F14CBA229B392B5
 - GUID with dashes and curly brackets:
{D0384E7D-BAC3-4797-8F14-CBA229B392B5}

If the computer has more than one user, only the current logged-in user can place files in that folder and have them excluded from the sweep. Any files that another user has placed in that folder will be swept and encrypted.

Mac example

Enter the string in this format:

- Variable with a \$VALUE format, for example, \$HOME/Documents or \$HOME/Hidden

Note: For Force-protected mode, a sweep occurs in the /Users folder.

Inform users of the impact or usability

If you define a unique folder name in the *Folder Exclusions for Basic File Protection* policy so that users can store files of a specific type that should not be encrypted, the policy does not create that folder on the client computers. You must inform users of the folder name and the need to create it.

Users can add subfolders and create names. The content of subfolders is also excluded.

Note: If that folder already has files that are encrypted with *Basic File Protection*, those files are not decrypted.

Unsupported applications and file types

- Do not add these Office file extensions to the Basic File Configuration policy: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf. Basic File Protection does not scan these during a sweep.
- PhotosApp.exe (Windows 8.1)

Remove a file type

If you modify the *Folder Exclusions for Basic File Protection* policy to remove a file type, those encrypted files on the client computer are decrypted.

However, if the computer has more than one user, only the current logged-in user has files decrypted. If the logged in user logs out and a second user logs in, the sweep starts again but decrypts only the files of the second logged-in user.

Use the Recovery Tool

For more information, see the *Recovery Tool* document > *Data Guardian*.

Plan for factors in configuration

You can modify Data Guardian to encrypt additional file types. However, to ensure protection, be aware of the following factors.

File extension type or environment	Issue	Options or Solution
<p>Cloud Encryption enabled (Windows 2.7 and earlier)</p> <p>Windows 8.1 - 10 and higher</p> <p>Universal Windows Platform (UWP) application added to <i>Basic File Protection Configuration</i> policy (See below for steps to add a UWP application.)</p>	<p>In the <i>Basic File Protection Configuration</i> policy, if you add any UWP application and the processes that support the app, all UWP applications are enabled to read these encrypted file types.</p> <p>Edge is a UWP application. File extensions added to the policy, such as .txt or .png, are encrypted. However, if users use Edge to upload these encrypted files to a cloud storage provider, the file is decrypted.</p>	<p>Options to avoid Edge decrypting files on upload:</p> <ul style="list-style-type: none"> • Do not add UWP apps to the configuration field. <p>or</p> <ul style="list-style-type: none"> • If you add a UWP application, block Edge through GPO or ensure that it is not installed on computers. • Consider which UWP applications you want users to have encrypted. However, test all UWP applications before deploying Basic File Protection to the enterprise to ensure that the intended file types remain encrypted.
<p>These applications are supported and can open a .bmp file:</p>	<p>.bmp files require additional configuration in the <i>Basic File Protection Configuration</i> policy.</p>	<p>Here is an example: microsoft.photos.exe:bmp</p>

<ul style="list-style-type: none"> • Microsoft.Photos.exe (Windows 10) • Windows Photo Viewer (Windows 8.1) <p>This UWP application, is not supported and will not open a .bmp file:</p> <ul style="list-style-type: none"> • PhotosApp.exe (Windows 8.1) 		DllHost.exe:bmp sihost.exe:bmp RuntimeBroker.exe:bmp
---	--	--

To add a Universal Windows Platform (UWP) application

1. In the *Basic File Protection Configuration* policy, enter the UWP application name.
2. Also enter the following process names:
 - RuntimeBroker.exe
 - sihost.exe

Note: For Windows 8, if you want to add **Photo Previewer** as a UWP application to the *Basic File Protection Configuration* policy, you must also add the **DLLHost.exe** process.

3. To add the file extensions that each .exe will encrypt, follow the examples in the policy.

Use Data Guardian in Opt-in Mode (Windows or Mac)

With opt-in mode, users have some options in protecting Office documents. Other features, like Content Based Protection (previously Data Classification) and TITUS classification, involve a sweep.

When you enable encryption for these files in Windows or Mac, you can also set policies for users to view the encrypted files in mobile devices or the web portal. See [Set Policies to Protect Office Documents in Mobile Devices](#) or [Set Policies to Protect Documents on the web client](#).

- [Set opt-in policies for internal users](#)
- [Determine file types to protect](#)
- [File menu options](#)
- [Configure Access Groups](#)
- [Legacy policies for Data Guardian](#)

Set opt-in policies for internal users

To set opt-in policies for Office and other file types:

1. Log in to the **Dell Security Center**.
2. In **Populations > Enterprise**, in the *Data Guardian* technology group, click the **Protected Office Documents** policy group.
3. Set *Protected Office Documents* to **On**.

Note: You must enable the policy if you want to use any of the policies in the **Protected Office Documents** policy group.

4. Set additional policies based on security requirements.

Return to [list](#)

Determine file types to protect

For Windows and Mac, users have the option to determine which Office files, .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, or .pdf, to protect.

This table lists policies required for enabling protected Office documents in Opt-in mode.

If the *Protected Office Documents* policy is *Off*, no Office-protected formatting takes place, regardless of other policies.

Policy	Description for Opt-in mode	Version availability
<p>Windows and Mac Enterprise > Data Guardian > Protected Office Documents: Protected Office Documents > On</p> <p>Mac Enterprise > Data Guardian > Protected Office Documents > Settings: Allow Mac Data Guardian Activation > check box selected</p>	<p>Windows and Mac - options for encrypting a file:</p> <ul style="list-style-type: none"> Applies to the Enterprise population. A Secure Documents folder is added to the root of each client's Documents folder. Office files added to that folder are encrypted. When users right-click an Office file, a <i>Protect</i> menu option displays. <p>Windows -additional option for encrypting a file:</p> <ul style="list-style-type: none"> File menu for Office documents has a <i>Protected Save As</i> option. See File menu options. <p>Windows and Mac - audit events</p> <ul style="list-style-type: none"> For compliance and monitoring purposes, creates audit events. 	Windows Mac

Protected Office Documents - additional policies

If your enterprise enables encryption for protected Office documents and PDFs, you can select these additional policies.

Policy	Description	Version availability
<p>Cover page for protected Office documents Data Guardian > Protected Office Documents > advanced:</p> <ul style="list-style-type: none"> Protected Office Documents Cover Page Notice Protected Office Documents Cover Page Corporate Logo 	See Set Cover Page Policies .	Windows Mac
<p>Additional policies for Windows and Mac: Data Guardian > Protected Office Documents > advanced:</p> <ul style="list-style-type: none"> Protected Office Document Tamper Prompt Hidden Audit Trail within Protected Office Document 	<p>Tampering</p> <ul style="list-style-type: none"> For compliance and monitoring purposes, creates audit events. 	Windows Mac
<p>Additional policies for Windows: Data Guardian > Protected Office Documents: Data Guardian > Protected Office Documents > advanced:</p> <ul style="list-style-type: none"> File Icon Overlay Enable Time To Live and Embargo Control Offline Key Generation Escrow Reminder Delay Offline Key Generation Escrow Reminder Text 		Windows
Content Based Protection policies for	Enforce encryption on sensitive data based on content and a set of rules.	Windows

<p>Windows in Opt-in mode: <i>Data Guardian > Content Based Protection:</i></p> <ul style="list-style-type: none"> ● Content Based Protection (previously Data Classification) ● Content Based Protection Rules 	<p>Content-based rules can be set at the Enterprise, Endpoint Groups, or Endpoints populations. See Configure Content Based Protection for Data Guardian's Opt-in mode.</p> <p>Windows</p> <ul style="list-style-type: none"> ● For compliance and monitoring purposes, creates audit events. 	
<p>Callback Beacon policies: <i>Data Guardian > Protected Office Documents > advanced:</i></p> <ul style="list-style-type: none"> ● Enable Callback Beacon 	<p>Inserts a callback beacon into every protected Office file.</p> <p>Windows and Mac - audit events</p> <ul style="list-style-type: none"> ● For compliance and monitoring purposes, creates audit events. 	<p>Windows Mac</p>
<p>TITUS Classification policies for Windows: <i>Data Guardian > Protected Office Documents > advanced:</i></p> <ul style="list-style-type: none"> ● Encrypt based on Titus Classification ● Titus Classification Encryption Mapping 	<p>Provides another way for users to protect Office documents and PDFs. When you configure a TITUS classification for Data Guardian, users can right-click a file and select that TITUS classification to have the Office file or PDF encrypted. See Set TITUS classification (Opt-in mode).</p>	<p>Windows v1.6 and higher</p>
<p>Outlook email policies Windows in Opt-in mode: <i>Data Guardian > Protected Office Documents > advanced:</i></p> <ul style="list-style-type: none"> ● Email Encryption via Outlook 	<p>A allows users to send emails as Protected by Data Guardian.</p> <p>Windows</p> <ul style="list-style-type: none"> ● For compliance and monitoring purposes, creates audit events. 	<p>Windows v2.0.1 and higher</p>

Basic File Protection

With Data Guardian v1.6 and higher, you can configure applications and file types, such as .txt or .png, in addition to Office documents. This policy applies at the Enterprise level. A sweep of users' computers encrypts those configured file types.

Policy	Description for Opt-in	Version availability
<p><i>Enterprise > Data Guardian > Protected Office Documents:</i> Protected Office Documents > On</p> <p>Basic File Protection > check box selected Basic File Protection Configuration > string</p>	<p>Windows and Mac Applies to the Enterprise population. For more information, see Configure Basic File Protection Policies.</p> <p>For Mac, it protects files in Home folder.</p> <p>Windows and Mac - audit events</p> <ul style="list-style-type: none"> ● For compliance and monitoring purposes, creates audit events. 	<p>Windows Mac v1.6 and higher</p>
<p>Before you enable Basic File Protection (optional but important): <i>Enterprise > Data Guardian > Protected Office Documents > advanced:</i> Folder Exclusions for Basic File Protection > string</p>	<p>You may want to allow users to exclude existing files with that file extension from an encryption sweep, for example:</p> <ul style="list-style-type: none"> ● To prevent files needed by the system from being encrypted ● To create a folder where users can place files of that type that do not require security or encrypting <p>Windows and Mac: See Configure policy to exclude folders. Note: You must inform users to create this folder and place existing files there <i>before</i> you enable Basic File Protection.</p>	<p>Windows Mac v1.6 and higher</p>

Return to [list](#)

File menu options for protected Office documents in Opt-in mode - Windows

For Office-protected documents, Data Guardian adds a *Protected Save As* option to the File menu list. This table also lists the behavior of other File menu options.

File menu option for Office documents	Policy for Opt-in mode: Protected Office Documents	
	Protected Office documents	Unprotected Office documents
Open	Files open as usual.	Files open as usual.
Save	User clicks Save on an existing protected file: The file is saved as protected If the file is in read-only mode, the <i>Save As</i> window opens. The only option in the <i>Save as type</i> field is <i>Protected (Documents, Presentation, or Workbook)</i> . User opens and saves a .xen file - the only option in the <i>Save as type</i> field is <i>Protected</i> . The .xen file is removed from the cloud.	User clicks Save on an existing unprotected file: The file is saved as unprotected <i>Save as type</i> field - If this is the first time to save the file, the <i>Save As</i> window opens and this field has the standard list of options.
Save As	Enabled for user - saves as unprotected	Enabled for user - saves as unprotected
Protected Save As	Enabled for user <i>Save as type</i> field - the only option is <i>Protected (Documents, Presentation, or Workbook or PDF)</i> .	Enabled for user <i>Save as type</i> field - the only option is <i>Protected (Documents, Presentation, or Workbook or PDF)</i> .

Configure Access Groups

Data Guardian's *Access Groups* (formerly *Circle of Trust*) enhance security by creating user groups that can collaborate on encrypted data. Users outside a group cannot access or view the data unless the owner of the file grants access. Access Groups can include internal and external users. You can use *Access Groups* with Windows, Mac, mobile, and web portal.

To plan for and implement this feature, see [Configure Access Groups](#).

Return to [list](#)

Legacy policies for Data Guardian

For Windows and Data Guardian v2.4 and higher or Mac Data Guardian v2.9 and higher, Cloud Encryption protection has been disabled to prevent compatibility issues with newer functions of cloud service providers. If your enterprise has earlier versions, see [Use Data Guardian with Cloud Encryption](#).

For Data Guardian v2.8 and higher, some Data Loss Prevention (DLP) features focus on Data Guardian's mobile clients and web portal. These policies no longer apply to Data Guardian v2.8 and higher.

Legacy Data Guardian policies	Legacy Advanced Data Guardian policies
Block Print Screen	Print Control Export Control Protected Office Document Process Protection Protected Office Clip Board Unauthorized Text On Screen Watermark

For Data Guardian v2.7 and earlier, see [Legacy Policies for Data Guardian's Opt-in Mode](#).

Return to [list](#)

Return to [Data Guardian](#).

Use Data Guardian in Force-Protected Mode (Windows or Mac)

Data Guardian's Force-Protected mode provides a higher level of security than Opt-in mode.

When you enable encryption for these files in Windows or Mac, you can also set policies for users to view the encrypted files in mobile devices or the web portal. See [Set Policies to Protect Office Documents in Mobile Devices](#) or [Set Policies to Protect Documents on the web client](#).

Set Force-Protected policies for internal users

To set Force-Protected policies for Office and other file types:

1. Log in to the **Dell Security Center**.
2. In **Populations > Enterprise**, in the *Data Guardian* technology group, click the **Protected Office Documents** policy group.
3. Set *Protected Office Documents* to **On**.

Note: You must enable the policy if you want to use any of the policies in the **Protected Office Documents** policy group.

4. At the Enterprise, Endpoint Groups, or Endpoints level, click **Show advanced settings** and select the *Force Protected Files Only* check box.
5. For Mac, in the *Data Guardian* technology group, click **Settings** and ensure the *Allow Mac Data Guardian Activation* check box is selected.
6. Based on security requirements, set additional policies at the *Enterprise, Endpoint Groups, or Endpoints* levels.

For Endpoint Groups or Endpoints, click an option to access the Detail page's Security Policies tab.

Determine file types to protect

For Windows and Mac, a sweep of users' computers encrypts all .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, or .pdf documents to ensure protection.

This table lists policies required for enabling protected Office documents in Opt-in mode.

If the *Protected Office Documents* policy is *Off*, no Office-protected formatting takes place, regardless of other policies.

Policy	Description for Force Protected	Version availability
<p><i>Enterprise > Data Guardian > Protected Office Documents:</i></p> <p>Protected Office Documents > On</p> <p><i>Enterprise, Endpoint Groups, or Endpoints > Data Guardian > Protected Office Documents > advanced:</i></p> <p>Force Protected Files Only > check box selected</p> <p>For Mac:</p> <p><i>Enterprise > Data Guardian > Protected Office Documents > Settings:</i></p> <p>Allow Mac Data Guardian Activation > check box selected</p>	<p>A sweep of users' computers encrypts all Office documents.</p> <p>Windows</p> <p>On Windows, for Data Guardian to sweep the Office documents, the user must log in and be connected to the network. Sweep ignores network file share, optical, and removable drives..</p> <p>Mac</p> <p>Mac protects files in the <i>Home</i> folder.</p> <p>Windows and Mac - audit events</p> <ul style="list-style-type: none"> • For compliance and monitoring purposes, creates audit events. 	<p>Windows</p> <p>Mac</p>

Protected Office Documents - additional policies for Force-Protected mode

If your enterprise enables encryption for protected Office documents and PDFs, you can select these additional policies.

Policy	Description for Force Protected	Version availability
Enterprise > Data Guardian > Protected Office Documents > advanced: Allow File Exclusions > check box selected	Windows and Mac For internal users, an <i>Unprotected Documents</i> folder is added to the root of each computer's <i>Documents</i> folder. When users place an Office document in that folder, Data Guardian automatically decrypts it.	Windows Mac
Cover page for Protected Office Documents Enterprise > Data Guardian > Protected Office Documents > advanced: <ul style="list-style-type: none"> Protected Office Documents Cover Page Notice Protected Office Documents Cover Page Corporate Logo 	See Set Cover Page Policies .	Windows Mac
Additional policies for Windows and Mac : Data Guardian > Protected Office Documents > advanced: <ul style="list-style-type: none"> Protected Office Document Tamper Prompt Hidden Audit Trail within Protected Office Document 	Tampering <ul style="list-style-type: none"> For compliance and monitoring purposes, creates audit events. 	Windows Mac
Additional policies for Windows : Data Guardian > Protected Office Documents: <ul style="list-style-type: none"> File Icon Overlay Data Guardian > Protected Office Documents > advanced: <ul style="list-style-type: none"> Enable Time To Live and Embargo Control Offline Key Generation Escrow Reminder Delay Offline Key Generation Escrow Reminder Text 		Windows
Callback Beacon policies: Data Guardian > Protected Office Documents > advanced: <ul style="list-style-type: none"> Enable Callback Beacon 	Inserts a callback beacon into every protected Office file. Windows and Mac - audit events <ul style="list-style-type: none"> For compliance and monitoring purposes, creates audit events. 	Windows Mac

File menu options for protected Office documents in Force-Protected mode

These options display for Force-Protecte mode in Windows.

File menu option for Office documents	Policies for Force-Protected mode: Protected Office Documents Force Protected files only
Open	Users can select Open for an unprotected document in these locations. The document opens in Edit mode. <ul style="list-style-type: none"> Excluded folder if you enable that policy. <i>Unprotected Documents</i> folder at the root of each computer's <i>Documents</i> folder if you enable that policy.
Save	User clicks Save : the file is protected.

	If the file is in read-only mode, the <i>Save As</i> window opens. The only option in the <i>Save as type</i> field is <i>Protected (Documents, Presentation, or Workbook)</i> . User opens and saves a .xen file - the only option in the <i>Save as type</i> field is <i>Protected</i> . The .xen file is removed from the cloud.
Save As	Windows: Data Guardian saves the file as unprotected but if the file is in a local folder, it gets swept and encrypted..

Configure Access Groups

Data Guardian's *Access Groups* (formerly *Circle of Trust*) enhance security by creating user groups that can collaborate on encrypted data. Users outside a group cannot access or view the data unless the owner of the file grants access. Access Groups can include internal and external users. You can use *Access Groups* with Windows, Mac, mobile, and web portal.

To plan for and implement this feature, see [Configure Access Groups](#).

Legacy policies for Data Guardian

For Windows and Data Guardian v2.4 and higher or Mac Data Guardian v2.9 and higher, Cloud Encryption protection has been disabled to prevent compatibility issues with newer functions of cloud service providers. If your enterprise has earlier versions, see [Use Data Guardian with Cloud Encryption](#).

For Data Guardian v2.8 and higher, some Data Loss Prevention (DLP) features focus on Data Guardian's mobile clients and web portal. These policies no longer apply to Data Guardian v2.8 and higher.

Legacy Data Guardian policies	Legacy Advanced Data Guardian policies
Block Print Screen	Print Control Export Control Protected Office Document Process Protection Protected Office Clip Board Unauthorized Text On Screen Watermark

For Data Guardian v2.7 and earlier, see [Legacy Policies for Data Guardian's Forcde-Protected Mode](#).

Return to [Data Guardian](#).

Legacy Policies for Data Guardian's Opt-in Mode

For Data Guardian v2.8 and higher, some Data Loss Prevention (DLP) features focus on Data Guardian's mobile clients and web portal.

For Data Guardian v2.7 and earlier, you can use these policies and features.

Windows: Additional Office menu options for Data Guardian v2.7 and earlier

For Data Guardian v2.7 and earlier, this table provides an overview of additional Protected Office policy settings and what displays in the Office *File* menu. These do not apply to Data Guardian v2.8 and higher.

File menu option for Office documents	Policy enabled (some protection options for user): Protected Office Documents	
	Protected Office documents	Unprotected Office documents
Print	Enabled for user For Office-protected documents, the Print Control policy determines how this function behaves.	Enabled for user

Export (Office 2013 and higher)	Office 2013/2016 and <i>Export Control</i> policy: <ul style="list-style-type: none"> • Allowed: Enabled for user • Watermark: Export is disabled. See Protected Export. • Disabled: Disabled for user 	Enabled for user
Protected Export (Office 2013 and higher) This option displays in the File menu only if the <i>Export Control</i> policy is set to Watermark.	Office 2013/2016 and <i>Export Control</i> policy: <ul style="list-style-type: none"> • 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
Share (Office 2013 and higher)	Disabled for protected Office documents Enabled for unprotected documents	Enabled for user

Windows: Additional Office menu options on Windows for Data Guardian v2.7 and earlier

For Data Guardian v2.7 and earlier, this table lists other menu options for Office. These do not apply to Data Guardian v2.8 and higher.

File menu option for Office documents	Policy enabled (some protection options for user): Protected Office Documents	
	Protected Office documents	Unprotected Office documents
Copy/Paste (Office Protected Clipboard policy)	Copy/Paste only to a protected Office document or protected .pdf. However, no unprotected PDFs can be open in Adobe Acrobat Reader DC.	Copy/Paste unprotected content as usual.
Screen Sketch (previously Snipping Tool)	Windows 10 RS5 and higher - In the Protected Office Document Process Protected policy enter this .exe to block this app since users could capture images of protected documents or content. Note: This policy cannot block the Action Center tile that directly launches the screen-clipping Windows feature.	
Protected Office Document Process Protection - example: Snipping Tool	Windows 10 RS4 and earlier - In the Protected Office Document Process Protected policy enter SnippingTool.exe to block it. Windows 10 RS5 and higher	

Windows: Additional policies

Block Print Screen - For Windows and protected Office documents, disables the user's ability to take screen captures via the Windows Print Screen capability while a protected office document is open.

Return to [Data Guardian](#).

Legacy Policies for Data Guardian's Force-Protected Mode

For Data Guardian v2.8 and higher, some Data Loss Prevention (DLP) features focus on Data Guardian's mobile clients and web portal.

For Data Guardian v2.7 and earlier, you can use these policies and features.

Windows: Additional Office menu options for Data Guardian v2.7 and earlier

For Data Guardian v2.7 and earlier, this table provides an overview of additional Protected Office policy settings and what displays in the Office File menu. These do not apply to Data Guardian v2.8 and higher.

With Force Protected enabled, the user is forced to save any Office document as Protected.

File menu option for Office documents	Policies enabled (higher security): Protected Office Documents Force Protected files only	Version availability
Print	Enabled for user For Office-protected documents, the Print Control policy determines how this function behaves.	v2.7 and earlier
Export (Office 2013 and higher)	Office 2013/2016 and <i>Export Control</i> policy: <ul style="list-style-type: none"> 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 	v2.7 and earlier
Protected Export (Office 2013 and higher) This option displays in the File menu only if the <i>Export Control</i> policy is set to Watermark.	Office 2013/2016 and <i>Export Control</i> policy: <ul style="list-style-type: none"> 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	v2.7 and earlier
Share (Office 2013 and higher)	Disabled for user	v2.7 and earlier

Windows: Additional Office menu options on Windows for Data Guardian v2.7 and earlier

For Data Guardian v2.7 and earlier, this table lists other menu options for Office. These do not apply to Data Guardian v2.8 and higher.

With Force Protected enabled, the user is forced to save any Office document as Protected.

File menu option for Office documents	Policies enabled (higher security): Protected Office Documents Force Protected files only	Version availability
Copy/Paste (Office Protected Clipboard policy)	Copy/Paste only to a protected Office document or protected .pdf. However, no unprotected PDFs can be open in Adobe Acrobat Reader DC.	v2.7 and earlier
Protected Office Document Process Protection - example: Snipping Tool	With Force Protected enabled, if you block the PrtScr button, this may also block the ability for users to print screens with touch screen or tablets.	v2.7 and earlier

Windows: Additional policies

Block Print Screen - For Windows and protected Office documents, disables the user's ability to take screen captures via the Windows Print Screen capability while a protected office document is open.

Set Policies to Protect Documents in Mobile Devices

For enhanced security on Office documents (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, or .pdf), you can implement Data Guardian's Protected Office mode. Protected Office documents are uploaded to the cloud, not as .xen files, but with their file extensions (for example, .docx or .pdf). However, the Office documents are encrypted.

Basic File Protection policies allow you to configure additional file extensions to be encrypted. Copy the extensions from the Windows policy to the mobile's *Basic File Protection Configuration* policy. Users can open, edit, and save encrypted files.

Set Protected Office Document Policies

To set Protected-mode policies on Office documents:

1. Log in to the **Dell Security Center**.
2. In **Populations > Enterprise**, in the *Data Guardian* technology group, click the **Protected Office Documents** policy group.
3. Toggle the *Protected Office Documents* policy to **On**.

The *Force Protected files only* policy is not available for mobile.

4. In the *Data Guardian* technology group, click **Settings**.
5. Ensure the *Allow Mobile Data Guardian Activation* check box is selected.
6. Set additional Protected Office policies at the *Enterprise, User Groups*, or *Users* levels.

For user groups, or users, click an option to access the Detail page's Security Policies tab.

Set Policies to Protect Documents on the Web Portal

For enhanced security on Office documents (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, or .pdf), you can implement Data Guardian's Protected Office mode for internal users.

Users can open a protected .pdf file with Adobe Acrobat Reader DC or Microsoft Word.

If additional file extensions are set through the *Basic File Protection Configuration* policy on a Windows client, users can upload those encrypted files on the web portal. If an editing policy is enabled, users can edit them.

With OneDrive for Business, users can connect to the cloud storage provider to download files directly from the cloud to the web portal.

Set Protected Office Document Policies

To set Protected-mode policies on Office documents:

1. Log in to the **Dell Security Center**.
2. In **Populations > Enterprise**, in the *Data Guardian* technology group, click the **Protected Office Documents** policy group.
3. Toggle the *Protected Office Documents* policy to **On**.
4. In the [Web Portal](#) policy group or [Global Settings](#), set additional policies at the *Enterprise, User Groups*, or *Users* levels. Some policies are set at the Enterprise (node level) only.

For user groups, or users, click an option to access the Detail page's Security Policies tab.

Configure Content Based Protection for Data Guardian's Opt-in mode

In Windows for Office documents and PDFs, use the *Content Based Protection Rules* policy to set rules that enforce encryption on sensitive data. Data Guardian sweeps users' computers when you set the rules and if you modify the rules.

Note: Users also have the option to right-click a file that has been analyzed by Content Based Protection and select **Protect File**.

You can set content-based rules at the Enterprise, Endpoint Groups, or Endpoints populations. Dell recommends that IT best practices are followed during the deployment. This includes, but is not limited to, controlled test environments for initial tests and staggered deployments to users.

Initially, in *Actions*, do not select the *Encrypt* check box for any rule. View the audit event reports to see the amount of data returned and the number of endpoints affected. Then modify your rules. To store a large amount of data, see [Export Dell Data Guardian Audit Events to SIEM a Server](#).

To configure the *Content Based Protection Rules* policy:

1. In the **Data Guardian** technology group, set these policies to **On**:
 - **Protected Office Documents**
 - **Content Based Protection** (previously *Classification*)
2. Click **Edit Rules**. Edit and delete icons display for each rule category. An *Elements* button displays at the bottom.
3. Configure the rule name, priority, rules, elements, and actions:
 - [Modify a Content-Based Rule](#)
 - [Content-Based Rule Name and Priority](#)
 - [View Audit Event Reports](#)
4. Each time you add or modify a rule, you must click **Save** beneath the *Content Based Protection Rules* policy.

Note: If you navigate away from this page without clicking Save at the bottom, your changes are not saved.
5. When finished, click **Save** in the upper-right and commit the policy.

The sweep for Content Based Protection does not include folders for your cloud storage provider. Also, if a file is already encrypted, the sweep does not rescan it to protect it based on the content rule.

Modify a Content-Based Rule

The *Content Based Protection Rules* policy allows you to modify:

- [Content-Based Rule Name and Priority](#) - The policy lists sample rule names in the Categories list with default priorities that you can modify:
 - *Restricted* - priority 3, the highest
 - *Internal Use* - priority 2
 - *Public* - priority 1, the lowest. The lowest priority displays (*default*) after the rule name, and no rules or actions apply.
- Important:** Optionally, you can delete the rules in the Categories list, but the policy requires a minimum number. See [Delete](#).
- [Actions](#):

- **Encrypt** - If you select the **Encrypt** check box for a non-default rule in the Categories list, the system encrypts the files. In addition, [Reports](#) can list which files were encrypted based on content rules. If you select Encrypt and the system sweeps an endpoint and encrypts, the files remain encrypted.
- **Audit** - By default when the **Content Based Protection** policy is enabled, the Audit action applies to all files. You can view these in [Audit Events](#) and [Reports](#). The report displays the first 2000 audit events. Before deploying, you can configure the rules without selecting the Encrypt option and then generate an audit report to determine the impact on endpoints and then further modify the rules.
- **Rules** - For configured rules, the system will sweep and detect them when a user saves the file. If the *Encrypt* check box is selected, the system encrypts the files.
- **Elements** - Options for configuring a rule, such as Credit Card number, US Name, Social Security Number, or Tags.

Content-Based Rule Name and Priority

To modify:

1. See [Configuration overview](#).
2. Select a non-default rule name in the Categories list, and click the **Edit** icon.
3. Optionally, modify the rule name.
4. Modify the priority:
 - The Priority label lists the range of numbers based on your number of rules in the Categories list.
 - The largest number is the highest priority.
 - By default, *Public* is set to **1**, the lowest priority. Whichever rule is set to priority **1** is listed with the *(default)* label and has no Encrypt option and no rules to modify. If you configure rules for a name with a higher priority but then change the priority to **1**, those rules are ignored.
5. To remove a rule name, select one and click the **Delete** icon (**X**). The range of priorities will also decrease.

Important: The policy requires a minimum number of rule names in the Categories lists.

- For files to be encrypted, this policy requires a minimum of two rule names and one *Encrypt* check box selected.
 - For the policy to function and create audit events, this policy requires a minimum of one rule name in the Categories list.
6. In *Edit Rule*, click **Save**.
 7. Below the *Content Based Protection Rules* policy, click **Save**.

[Return to top](#)

Actions

To modify:

1. See [Configuration overview](#).
2. Click the icon to expand a non-default rule name.

3. Select the **Encrypt** check box if you want the audit report to display files that have met the criteria for encryption.
4. Below the *Content Based Protection Rules* policy, click **Save**.

[Return to top](#)

Rules

To modify:

1. See [Configuration overview](#).
2. Click the icon to expand a non-default rule name in the Categories list.
3. Click **+** to add a rule.
3. In the Rule field that displays, select one or more check boxes for that rule and modify the number if needed. Incremented numbers mean that a file must contain that element, such as U.S. Address or Social Security Number, the specified number of times or higher in order to encrypt the file. For example, if your file lists a *sample* U.S. Address, you may not want the file to be encrypted. Therefore, you could set this number to 2 for an encryption.
4. Click **+** to add and configure more rules for that rule name. Rules are or'd together.
5. Below the *Content Based Protection Rules* policy, click **Save**.

[Return to top](#)

Elements

To view Elements:

1. See [Configuration overview](#).
2. Select a non-default rule name in the Categories list.
3. Click the **Elements** button at the bottom.
4. On the Elements window, select an element.
5. Do not modify the Content Identifier or Content Type.
6. See the table below.
7. When finished with the Elements window, click **Save**.
8. Below the *Content Based Protection Rules* policy, click **Save**.

For elements that you can modify, if you use them in multiple rule names be aware that future changes impact all rule names that use that element.

Content Based Protection Elements	Description
Predefined Elements: <ul style="list-style-type: none"> • Credit Card • Email (IPv4 and IPv6 IP addresses are recognized.) • IP Address • Social Security Number • US Address • US Date 	Do not modify these elements, except for US Name. For US Name, use these fields: First Names, Last Names, Common Words. You cannot delete these elements.

<ul style="list-style-type: none"> • US Name • US Phone Number 	
Keywords elements	In the Keywords field, type any key words that you want the system to recognize when encrypting files for that rule name. The format is [object Object]. Click Save . Click X to delete. See Add an Enterprise-Specific Rule Name or Tag Element .
Tags elements <i>Public, Internal Use, Confidential, Restricted</i>	Select the tag element that corresponds to the rule name, for example, with the <i>Restricted</i> rule name, select Restricted Tag . In the Tag field, a default tag displays. The system recognizes that tag when encrypting content based on that rule. For Tag elements, do not enter content in the <i>Regex</i> field. Click X to delete. Note: If end users want to use the Tag option in Office documents to trigger a content rule, inform them of the content in the Tag field. End users must match the case. See Add an Enterprise-Specific Rule Name or Tag Element .
Custom Regex element	The best practice is not to modify the Regex for predefined elements or Tag elements. Use the Custom Regex element or create a new Regex element. See Add an Enterprise-Specific Rule Name or Tag Element .

9. When finished with the Elements window, click **Save**.

10. Below the *Content Based Protection Rules* policy, click **Save**.

[Return to top](#)

Add an Enterprise-Specific Rule Name or Tag Element

Create a Rule Name

You can create an additional rule or modify the names of existing ones.

To create a new rule name:

1. See [Configuration overview](#).
2. In the *Content Based Protection Rules* policy, click the add icon (+) next to *Categories*.
3. In the Add Rule window, enter a name for the rule.
4. Enter a priority. A number displays to indicate the range of rules in your list. See [Content-Based Rule Name and Priority](#).
5. Click **Add**.
6. Below the *Content Based Protection Rules* policy, click **Save**.

Create an Element

To create an element:

1. See [Configuration overview](#).
2. In the *Elements* window, click the add icon (+) next to *Elements*.
3. In the Content Identifier field, enter a unique identifier.
4. Select a Content Type.

Note: Select the KeywordContent for any Keywords elements; the FileTagMetadataContent for any Tag elements, and the CustomRegexContent for any Regex elements.

5. Click **Add**.

6. Below the *Content Based Protection Rules* policy, click **Save**.
7. Modify the [Element](#) when it displays in the Element window.

After you create an element, you can add it as a new [rule](#).

For Regex, the best practice is to create a new element with a Content Identifier such as MyEnterprise Custom Regex or Custom Regex for Internal Use. Any Custom Regex would use the Content Type Custom Regex. However, do not use Custom Regex for predefined or Tags elements.

Note: Content Based Protection uses the .NET regex engine.

[Return to top](#)

View Audit Event Reports

Any documents that are impacted by Content Based Protection rules can display in [Audit Events](#) and [Reports](#). If you select the Encrypt check box in policy, the report can also display which files were encrypted based on these rules.

You can set filters on the columns to view the essential data in the report.

[Return to top](#)

Set TITUS classification (Opt-in mode)

For Data Guardian 1.6 and later, you can use the *Titus Classification Encryption Mapping* policy to set one or more TITUS classifications to encrypt unprotected Office documents (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, or .pdf) for Windows.

TITUS classification in a Data Guardian environment with Opt-in mode provides another way for users to protect Office documents. When a user right-clicks and selects a TITUS classification that you have configured, Data Guardian converts it to a protected Office document.

Currently, TITUS classification applies only to Office documents and PDFs, not additional file extensions set in the *Basic File Protection* policy.

In the policy, you can also add keywords.

Configure TITUS to encrypt files

TITUS server

The TITUS server administrator must set the TITUS Classification levels on the TITUS server.

Here are some examples.

TITUS Classification level	TITUS Classification Encryption mapping policy - formatting
Public	t_class_1
Internal	t_class_2
Confidential	t_class_3
Restricted	t_class_4

For more information, see the *TITUS Administration Guide*.

Dell Security Center

Configure the policy on the Dell Security Center:

1. From the TITUS server administrator, obtain the format for each TITUS classification level.

2. In the *Dell Security Center* > *Protected Office Documents* policy group, enable these policies:
 - *Protected Office Documents*
 - *Advanced: Encrypt based on Titus Classification*

Do not select the *Force Protected Files Only* policy.

3. In the *Titus Classification Encryption Mapping* policy field, enter the formatting. For example, for Data Guardian to encrypt a **Restricted** TITUS classification, enter **Set classification to t_class_4**.
4. Separate each classification by a carriage return, semi-colon, or comma, for example, t_class_1, t_class_2.
5. Optionally, obtain keywords for sensitive data from the TITUS administrator. For example, TITUS can scan a document for sensitive data, like Social Security Numbers. If you enter a keyword for that in this policy field and TITUS detects it, that document is protected as Restricted regardless of which TITUS option the user selects. For more information, see *Actions* in the *TITUS Administration Guide*.

Configure TITUS to encrypt macro-enabled documents

To use TITUS classification with Data Guardian and macro-enabled documents (.docm, .pptm, .xlsm) requires additional configuration.

1. In the TITUS Administration Console, select the **Configurations** tab.
2. Select the current enabled configuration from the list and click **Edit**.
3. In the left pane, click **Adapters**.
4. In the Adapter column, click **OPC Document Properties**.
5. Click **Edit**.
6. In the *OPC Document Properties* view > *Additional File Extensions* field, add **.docm, .pptm, .xlsm**.
7. Click **Save**.

Use Data Guardian with Cloud Encryption

Data Guardian with Cloud Encryption with:

- Mobile
- Web portal

Dell Security Center automatically updates profiles of cloud storage providers. For more information, see *Cloud Profile Update*.

For Windows 2.4 and higher or Mac 2.9 and higher, Data Guardian's Cloud Encryption protection has been disabled to prevent compatibility issues with newer functions of cloud service providers. To view .xen files already protected with Cloud Encryption, use Data Guardian's Mobile app or web portal.

Windows 2.3 and earlier or Mac 2.8 and earlier

Determine which Data Guardian policy groups you want to enable:

Data Guardian Policy Groups	Windows	Mac
-----------------------------	---------	-----

Protected Office Documents is <i>On</i> Cloud Encryption is <i>Off</i>	Office documents are protected based on policies. No DDG VDisk virtual drive is created. Non-Office documents are not impacted. If <i>Force Protected Files Only</i> is selected, an <i>Unprotected</i> folder is added to the root of the user's Documents folder.	N/A
Cloud Encryption is <i>On</i> Protected Office Documents is <i>Off</i>	Office and non-Office documents are protected as .xen files based on policies set. A DDG VDisk virtual drive displays in the client's Windows Explorer.	Office and non-Office documents are protected as .xen files based on policies set.
Both are <i>On</i>	Non-Office documents are protected as .xen files if in the DDG VDisk virtual drive. A DDG VDisk 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. Additional policies impact Office documents.	Non-Office documents are protected as .xen files. Office documents are protected based on Protected Office policies.
Neither is <i>On</i>	Files are not protected. If opened, content displays in cleartext.	Files are not protected. If opened, content displays in cleartext.

Enable Both Cloud Encryption and Protected Office Documents (Windows 2.3 and earlier)

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.

Configure Access Groups

Data Guardian's *Access Groups* (formerly *Circle of Trust*) enhance security by creating user groups that can collaborate on encrypted data. Users outside a group cannot access or view the data unless the owner of the file grants access. Access Groups can include internal and external users. You can use *Access Groups* with Windows, Mac, mobile, and web portal.

Data Guardian encrypted files:

- Internal users within an access group have access to encrypted data.
- Internal users outside an access group or external users do not have access but can request access.

Important: Currently, if you enable *Access Groups* in the Management Console, you cannot disable it.

To configure access groups, complete the following:

- [Set up Access Groups](#)
- Determine whether the enterprise already has Data Guardian installed. Implementation will be easier if you have a brief transition period where you allow users with shared files to prepare a plan for shared files. Do one of these:
 - [Enterprise does not yet have Data Guardian](#) - Transition time differs based on Force-Protected or Opt-in mode. Instruct users to process shared files.

- [Enterprise has Data Guardian Installed](#) - Instruct users to process shared, encrypted files.
- [Configure Access Groups](#)
- [Disable Auto access for swept files](#)

Set up Access Groups

Analyze which users to include within each access group based on which users need to share or collaborate on documents. You can create groups before or after enabling *Access Groups* in the Management Console.

To set up groups, see [Add a User Group](#).

For *Access Groups*, you can configure the following:

- Import existing AD groups, for example, an accounting or legal group that shares files.
- Select *ADMIN-DEFINED User Groups* for cross-functional teams of managed users and any external users that share or collaborate on files.

Note: When defining new groups, be sure to use descriptive names. On the client side, users will be selecting some of these groups.

- After you add the user group, you can select that group, select the *Details and Action* tab, and enable *Access Groups* for a single group or a combination of groups.

Also consider the following:

- Develop a plan for adding and removing users from a group if internal users join or leave the enterprise.
- As a best practice, stagger deployment of *Access Groups* to user groups.

Note: Access groups should be specific groups within the enterprise, not the entire enterprise.

[Return to top](#)

Enterprise does not yet have Data Guardian

If you do not yet have Data Guardian installed, develop a plan for implementing access groups and creating a smooth transition for users who have shared files.

Determine a transitional time range for deployment

Initially, enable *Access Groups* and *Auto access for swept files* for a transitional period. This should be a brief time but long enough for user files to be swept. In the transitional period, allow enough time for the following:

- Determine or estimate the quantity of documents that users have. Allow enough time for Data Guardian to sweep unprotected files. A sweep occurs with the following:
 - If you enable Force-Protected mode (Office documents and PDFs) or Basic File Protection (additional file types), all those unprotected files are swept.
 - Opt-in mode - A sweep only occurs for Content Based Protection (Windows only), TITUS Classification (Windows only), or Basic File Protection (additional file types).
- Users must log in to their computers while *Access Groups* and *Auto access for swept files* are enabled. Be sure to allow for users who are out of the office or on vacation.

Instruct users to process shared files

Inform internal users who will be in their access group and allow them to process shared files to ensure a smooth transition. Inform them that this effort will minimize their having to request access to shared files later.

- After *Access Groups* is enabled, a sweep occurs for Windows and Mac files. See [Disable Auto access for swept files](#). If files are shared by multiple users, the first computer to be swept gives ownership of any shared files to the owner of that computer, not the original author.
 - All internal users within the same access group will have access to the file.
 - If the original author of the file is not in the access group with the user whose computer was first swept, the author must request access or request that the administrator [change ownership of the file](#).
 - External users' unprotected shared files are not swept.
- If Auto access will be temporarily enabled, instruct users that any internal user outside their access group who has a copy of the file has permanent access to the key. In some cases, the key cannot be revoked later. See [Disable Auto access for swept files](#).

Note: After Auto access is disabled, for those outside an access group, the internal user can grant access or users outside the access group can request access if they receive an encrypted file. You can revoke the key access in the Management Console if needed.

[Return to top](#)

Enterprise has Data Guardian Installed

If you have Data Guardian installed, develop a plan for implementing access groups and creating a smooth transition for users who have shared files.

Determine a transitional time range for deployment

Initially, enable *Access Groups* and *Auto access for swept files* for a transitional period. This should be a brief time but owners of a protected, shared file should plan for any impact to that file.

Instruct users to process shared files

Inform internal users who will be in their access group and allow them to process shared files to ensure a smooth transition.

- During the Auto-access transitional period, all internal users within the same access group have access to the shared, protected files.
- If Auto access will be temporarily enabled, instruct users that any internal user outside their access group who has a copy of the file and opens it has permanent access to the key. In some cases, the key cannot be revoked later. See [Disable Auto access for swept files](#).
- If a user does not open a file and auto access is disabled, they lose access.
- If an internal user already granted access to an external user, the external user will not lose access.
- When a file is created after *Access Groups* is enabled, all users within that access group have access to the file.
 - If a user is removed from the access group, the user no longer has access to the files.
 - If the owner of the file is removed from the access group, others who shared access still have access.

For detailed information on the impact, see [Disable Auto access for swept files](#).

[Return to top](#)

Configure Access Groups

IT best practices should be followed during deployment. This includes, but is not limited to, controlled test environments for initial tests, and staggered deployments to users.

1. [Enable Data Guardian Access Groups](#) and, optionally, *Auto access for swept files*.

Important: Currently, if you enable Access Groups, you cannot disable it.

2. If you have not yet created user groups for this feature, see [Add a User Group](#).
3. In User Groups, select a group.
4. On User Group Detail, select the **Details and Action** tab.
5. Click the check box for *Access Group Enabled*.

Note: You can also modify the group members, remove the group, or clear the *Access Group* check box.

With Access Groups enabled, the *Protected File Access* screen allows internal users to select one or more access groups or add an individual when sharing a protected file. External users who own a document can share it with individual users but not access groups. This is available on Windows, Mac, mobile, and web portal. For more information, see the *Data Guardian User Guide*.

[Return to top](#)

Disable Auto access for swept files (Windows and Mac)

If you have a transitional period, when it is complete, clear the *Auto access for swept files* check box.

Be aware of the following for an enterprise that already had Data Guardian installed on Windows or Mac.

Internal users in access groups

	Pre-existing encrypted files created before <i>Access Groups</i>	New files created after were enabled
Force-protected mode		
Force-protected mode - files that Data Guardian swept <ul style="list-style-type: none"> • Force-Protected sweep (Office documents, PDFs) • Basic File Protection sweep (additional file types) 	Internal users within the access group do not have automatic access. <ul style="list-style-type: none"> • Owner of the file can grant protected access. • Users with a protected file can request access. In the Management Console, if needed, you can revoke key access that has been granted. <p>Note: During the transitional period when <i>Auto access for swept files</i> was enabled, if a user within the access group opened the file, that user has permanent access, and you cannot revoke key access.</p>	Internal users within the access group have protected files. <ul style="list-style-type: none"> • If someone is removed from access. • If the owner of a file leaves the organization, the file still have access.
Opt-in mode		
Opt-in mode - files that Data Guardian swept <ul style="list-style-type: none"> • Secure documents folder sweep • Basic File Protection sweep (additional file types) • TITUS classification (Windows) 	Same as above.	Same as above.

<ul style="list-style-type: none"> Content Based Protection (Windows) 		
<p>Opt-in mode files protected through:</p> <ul style="list-style-type: none"> Protected Save As Right-click protect Basic File Protection - direct save Protected messages 	<p>Internal users within the access group do not have automatic access.</p> <ul style="list-style-type: none"> Owner of the file can grant protected access. Users with a protected file can request access. <p>In the Management Console, if needed, you can revoke key access that has been granted.</p>	Same as above.

Internal users not in the access group and external users

	Files created before <i>Access Groups</i> were enabled	New files created after were enabled
Force-protected mode		
<p>Force-protected mode - files that Data Guardian swept</p> <ul style="list-style-type: none"> Force-Protected sweep (Office documents, PDFs) Basic File Protection sweep (additional file types) <p>Note: Sweeping only applies to internal users. External users' computers are not swept.</p>	<p>Internal users outside the access group and external users do not have automatic access.</p> <ul style="list-style-type: none"> Owner of the file can grant protected access. Users with a protected file can request access. <p>In the Management Console, if needed, you can revoke key access that has been granted.</p> <p>Note: During the transitional period when <i>Auto access for swept files</i> was enabled, if a user within the access group opened the file, that user has permanent access, and you cannot revoke key access.</p>	<p>Internal users outside the access group do not have automatic access.</p> <ul style="list-style-type: none"> Owner of the file can grant protected access. Users with a new protected file can request access. <p>In the Management Console, if needed, you can revoke key access that has been granted.</p> <p>Note: During the transitional period when <i>Auto access for swept files</i> was enabled, if a user within the access group opened the file, that user has permanent access, and you cannot revoke key access.</p>
Opt-in mode		
<p>Opt-in mode - files that Data Guardian swept</p> <ul style="list-style-type: none"> Secure documents folder sweep Basic File Protection sweep (additional file types) TITUS classification (Windows) Content Based Protection (Windows) <p>Note: Sweeping only applies to internal users. External users' computers are not swept.</p>	<p>Internal users outside the access group and external users: Same as above.</p>	<p>Internal users outside the access group do not have automatic access. Same as above.</p>
<p>Opt-in mode files protected through:</p> <ul style="list-style-type: none"> Protected Save As Right-click protect Basic File Protection - direct save Protected messages 	<p>Internal users outside the access group and external users: Same as above.</p>	<p>Internal users outside the access group do not have automatic access. Same as above.</p> <p>However, if the owner of the new file is not a member of the new user group, other members still have access. New members of the group, or users who were not members of Guardian after the group was created, must request access of the file.</p>

Change the owner of a file

After enabling *Access Groups*, if another user was designated as the owner of a shared, encrypted document, you can change the owner. See [Key Management](#).

[Return to top](#)

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 Management Console.

Policy	Default	Description
Settings This technology allows control over general settings such as polling intervals, support dialogs, in-app feedback, auto updates, data auditing, and client retention periods.		
Audit Control Policies		
Data Guardian Audit Data Enabled	Selected	<i>Selected</i> <i>Not Selected</i> 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 Data Guardian clients.
Data Guardian Geo Location Audit Data	Selected	<i>Selected</i> <i>Not Selected</i> Selected includes geo tracking location data in audit data. For Windows, this policy is supported on v8.1 and higher.
Client Retention Period	30	<i>1-365 days. 30 days default.</i> Specifies the number of days that the client will hold on to audit data without transmission.
Client Retention Storage	512	<i>Megabytes of storage space</i> Specifies the maximum storage space used by the client for audit data without transmission.
Web Portal Audit Control Policies		
Data Guardian Audit Data Enabled	Selected	<i>Selected</i> <i>Not Selected</i> Selected enables Web Portal Audit 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 Data Guardian clients.
Data Guardian Geo Location Audit Data	Selected	<i>Selected</i> <i>Not Selected</i> Selected includes geo tracking location data in audit data. For Windows, this policy is supported on v8.1 and higher.
Mobile Audit Control		
Data Guardian Audit Data Enabled	Selected	<i>Selected</i> <i>Not Selected</i> 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 Data Guardian clients.
See advanced settings		

Advanced 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 Management Console.

Policy	Default	Description
Settings This technology allows control over general settings such as polling intervals, support dialogs, in-app feedback, auto updates, data auditing, and client retention periods.		
Mobile Audit Control		
Data Guardian Geo Location Audit Data	Selected	<i>Selected</i> <i>Not Selected</i> Selected includes geo tracking location data in audit data.
See basic settings		