Getting Started

Dell Data Security Implementation Services

July 2024
Rev. A01

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Implementation Phases

The basic implementation process includes these phases:

- Perform Kick-off and Requirements Review
- Complete Preparation Checklist - Initial Implementation or Preparation Checklist - Upgrade/Migration
- Install or Upgrade/Migrate ***one*** of the following:
  - ***Security Management Server***
    - Centralized management of devices
    - A Windows-based application that runs on a physical or virtualized environment.
  - ***Security Management Server Virtual***
    - Centralized management of up to 3,500 devices
    - Runs in a virtualized environment

    For Dell Server installation/migration instructions, see *Security Management Server Installation and Migration Guide* or *Security Management Server Virtual Quick Start and Installation Guide.* To obtain these documents, see Dell Data Security Server documents.
- Configure Initial Policy
  - ***Security Management Server*** - see *Security Management Server Installation and Migration Guide*, *Administrative Tasks*, available on support.dell.com and *AdminHelp*, available from the Management Console
  - ***Security Management Server Virtual*** - see *Security Management Server Virtual Quick Start and Installation Guide*, *Management Console Administrative Tasks*, available on support.dell.com and *AdminHelp*, available from the Management Console
- Client Packaging

  For client requirements and software installation documents, select the applicable documents based on your deployment:
  - *Encryption Enterprise Basic Installation Guide* or *Encryption Enterprise Advanced Installation Guide*
  - *Endpoint Security Suite Enterprise Basic Installation Guide* or *Endpoint Security Suite Enterprise Advanced Installation Guide*
  - *Advanced Threat Prevention Administrator Guide*
  - *Encryption Personal Installation Guide*
  - *Encryption Enterprise for Mac Administrator Guide*
  - *Endpoint Security Suite Enterprise for Mac Administrator Guide*
  - To obtain these documents, refer to Dell Data Security client documents.
- Participate in Dell security administrator basic knowledge transfer
- Implement Best Practices
- Coordinate pilot or deployment support with Dell Client Services

2

Kick-off and Requirements Review

Before installation, it is important to understand your environment and the business and technical objectives of your project, to successfully implement Dell Data Security to meet these objectives. Ensure that you have a thorough understanding of your organization's overall data security requirements.

The following are some common key questions to help the Dell Client Services Team understand your environment and requirements:

1. What is your organization's type of business (health care, etc)?
2. What regulatory compliance requirements do you have (HIPAA/HITECH, PCI, etc.)?
3. What is the size of your organization (number of users, number of physical locations, etc.)?
4. What is the targeted number of endpoints for the deployment? Are there plans to expand beyond this number in the future?
5. Do users have local administrator privileges?
6. What data and devices do you need to manage and encrypt (local fixed disks, USB, etc.)?
7. What products are you considering deploying?
    - Encryption Enterprise
        - Encryption (DE entitlement) - Windows Encryption, Server Encryption, Encryption External Media, SED Management, Full Disk Encryption, BitLocker Manager, and Mac Encryption.
        - Encryption External Media
    - Endpoint Security Suite Enterprise
        - Advanced Threat Prevention - with or without optional Client Firewall and Web Protection (ATP entitlement)
        - Encryption (DE entitlement) - Windows Encryption, Server Encryption, Encryption External Media, SED Management, Full Disk Encryption, BitLocker Manager, and Mac Encryption.
        - Encryption External Media
8. What type of user connectivity does your organization support? Types might include the following:
    - Local LAN connectivity only
    - VPN-based and/or enterprise wireless users
    - Remote/disconnected users (users not connected to the network either directly or via VPN for extended periods of time)
    - Non-domain workstations
9. What data do you need to protect at the endpoint? What type of data do typical users have at the endpoint?
10. What user applications may contain sensitive information? What are the application file types?
11. How many domains do you have in your environment? How many are in-scope for encryption?
12. What operating systems and operating systems versions are targeted for encryption?
13. Do you have alternate boot partitions configured on your endpoints?
    a. Manufacturer Recovery Partition
    b. Dual-boot Workstations

Client Documents

For installation requirements, supported operating system versions, supported Self-Encrypting Drives, and instructions for the clients you plan to deploy, refer to the applicable documents, listed below.

Encryption Enterprise (Windows) - See the documents at: www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals.

- *Encryption Enterprise Advanced Installation Guide* - Installation guide with advanced switches and parameters for customized installations.
- *Dell Data Security Console User Guide* - Instructions for users.

Encryption Enterprise (Mac) - See the *Encryption Enterprise for Mac Administrator Guide* at www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. Includes installation and deployment instructions.

Endpoint Security Suite Enterprise (Windows) - See the documents at: www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Endpoint Security Suite Enterprise Advanced Installation Guide* - Installation guide with advanced switches and parameters for customized installations.
- *Endpoint Security Suite Enterprise Advanced Threat Prevention Quick Start Guide* - Instructions administration, including policy recommendations, threat identification and management, and troubleshooting.
- *Dell Data Security Console User Guide* - Instructions users.

Endpoint Security Suite Enterprise (Mac) - See the document at: www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Endpoint Security Suite Enterprise for Mac Administrator Guide* - Installation guide

For information on supported Self-Encrypting Drives, see https://www.dell.com/support/article/us/en/04/sln296720.

Server documents

For installation requirements, supported operating system versions, and configurations of the Dell Server you plan to deploy, refer to the applicable document below.

Security Management Server

- See the *Security Management Server Installation and Migration Guide* at

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  or

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

Security Management Server Virtual

- See the *Security Management Server Virtual Quick Start and Installation Guide* at

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  or

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

3

Preparation Checklist - Initial Implementation

Based on the Dell Server you deploy, use the appropriate checklist to ensure you have met all prerequisites before beginning to install Dell Encryption or Endpoint Security Suite Enterprise.

- Security Management Server checklist
- Security Management Server Virtual checklist

Security Management Server Initial Implementation Checklist

Proof of Concept environment cleanup is complete (if applicable)?

☐	The proof of concept database and application have been backed up and uninstalled (if using the same server) before the installation engagement with Dell. For more instruction on an uninstall, see https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us.
☐	Any production endpoints used during proof of concept testing have been decrypted or key bundles downloaded. For more information on the clients you plan to deploy, see Client Documents.

NOTE:

All new implementations must begin with a new database and fresh installation of the Encryption or Endpoint Security Suite Enterprise software. Dell Client Services will not perform a new implementation using a POC environment. Any endpoints encrypted during a POC will need to be either decrypted or rebuilt prior to the installation engagement with Dell.

Servers meet required hardware specifications?

☐	See Dell Security Management Server Architecture Design.

Servers meet required software specifications?

☐	Windows Server 2012 R2 (Standard or Datacenter), 2016 (Standard or Datacenter), Windows Server 2019 (Standard or Datacenter), or Windows Server 2022 (Standard or Datacenter) is installed. These operating systems can be installed on physical or virtual hardware.
☐	Windows Installer 4.0 or later is installed.
☐	.NET Framework 4.6.1 is installed.
☐	Microsoft SQL Native Client 2012 is installed, if using SQL Server 2012 or SQL Server 2016. If available, SQL Native Client 2014 may be used. **NOTE:** SQL Express is not supported with a production deployment of Security Management Server.
☐	Windows Firewall is disabled or configured to allow (inbound) ports 8000, 8050, 8081, 8888, 61613.
☐	Connectivity is available between Security Management Server and Active Directory (AD) over ports 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (inbound to AD).

☐	UAC is disabled before installation on Windows Server 2012 R2 when installing in C:\Program Files. The server must be rebooted for this change to take effect. (see Windows Control Panel > User Accounts). • Windows Server 2012 R2 - the installer disables UAC. • Windows Server 2016 R2 - the installer disables UAC. **NOTE:** UAC is no longer force-disabled unless a protected directory is specified for the install directory.

Service accounts successfully created?

☐	Service account with read-only access to AD (LDAP) - basic user/domain user account is sufficient.
☐	Service account must have local administrator rights to the Security Management Server application servers.
☐	To use Windows authentication for the database, a domain services account with system administrator rights. The user account must be in the format DOMAIN\Username and have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.
☐	To use SQL authentication, the SQL account used must have system administrator rights on the SQL Server. The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.

Software is downloaded?

Download from Dell Support website.

☐	Dell Data Security client software and Security Management Server downloads are located in the **Drivers & Downloads** folder at www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research or www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research or From the product page http://www.dell.com/support 1. Select **Drivers & Downloads**. 2. From the Operating system list, select the correct operating system for the product you are downloading. For example, to download Dell Enterprise Server, select **one of the Windows Server options.** 3. Under the applicable software title, select **Download File**.
☐	If you have purchased Encryption or Endpoint Security Suite Enterprise on-the-box, the software can be delivered to the target computer using Dell Digital Delivery.

OR

Download from Dell Data Security file transfer site (CFT)

☐	Software is located at https://ddpe.credant.com in the **SoftwareDownloads** folder.

Installation key and license file are available?

☐	The license key is included in the original email with FTP credentials - see Example Customer Notification Email. This key is also included in the download of the application from http://www.dell.com/support and https://ddpe.credant.com.

☐	The license file is an XML file located on the FTP site in the **Client Licenses** folder.

NOTE:

If you purchased your licenses on-the-box, no license file is necessary. The entitlement is automatically downloaded from Dell upon activation of any new Encryption Personal, Encryption Enterprise, or Endpoint Security Suite Enterprise client.

Database is created?

☐	(Optional) A new database is created on a supported server - see Requirements and Architecture in the *Security Management Server Installation and Migration Guide*. The Security Management Server installer creates a database during installation if one is not already created.
☐	The target database user has been given **db_owner** rights.

DNS alias created for Security Management Server and/or Policy Proxies with Split DNS for internal and external traffic?

It is recommended that you create DNS aliases, for scalability. This will allow you to add additional servers later or separate components of the application without requiring client update.

☐	DNS aliases are created, if desired. Suggested DNS aliases: • Security Management Server: dds.<domain.com> • Front end Server: dds-fe.<domain.com>

NOTE:

Split-DNS allows the user of the same DNS name internally and externally. This means that we could internally supply dds.<domain.com> as an internal c-name, and direct this to the Dell Security Management Server (back-end), and externally we could supply an a-record for dds.<domain.com> and forward the relevant ports (see Ports for Security Management Server) to the front-end server. We could leverage DNS round-robin or a load-balancer to distribute the load to the various front-ends (if multiple exist).

Plan for SSL Certificates?

☐	We have an internal Certificate Authority (CA) that can be used to sign certificates and is trusted by all workstations in the environment **or** we plan to purchase a signed certificate using a public Certificate Authority, such as VeriSign or Entrust. If using a public Certificate Authority, inform the Dell Client Services Engineer. The Certificate contains the Entire Chain of Trust (Root and Intermediate) with Public and Private Key Signatures.
☐	Subject Alternate Names (SANs) on Certificate Request match all DNS aliases given to every server being used for Dell Server installation. Does not apply to Wildcard or Self- Signed certificate requests.
☐	Certificate is generated to a .pfx format.

Change Control requirements identified and communicated to Dell?

☐	Submit any specific Change Control requirements for the installation of Encryption or Endpoint Security Suite Enterprise to Dell Client Services prior to the installation engagement. These requirements may include changes to the application server(s), database, and client workstations.

Test Hardware prepared?

☐	Prepare at least three computers with your corporate computer image to be used for testing. Dell recommends that you **not** use production computers for testing. Production computers should be used during a production pilot after encryption policies have been defined and tested using the Test Plan provided by Dell.

Security Management Server Virtual Initial Implementation Checklist

Proof of Concept environment cleanup is complete (if applicable)?

☐	The proof of concept database and application have been backed up and uninstalled (if using the same server) before the installation engagement with Dell. For more instruction on an uninstall, see https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us
☐	Any production endpoints used during proof of concept testing have been decrypted or key bundles downloaded. For more information on the clients you plan to deploy, see Client Documents.

NOTE:

All new implementations must begin with a new database and fresh installation of the Encryption or Endpoint Security Suite Enterprise software. Dell Client Services will not perform a new implementation using a POC environment. Any endpoints encrypted during a POC will need to be either decrypted or rebuilt prior to the installation engagement with Dell.

Service accounts successfully created?

☐	Service account with read-only access to AD (LDAP) - basic user/domain user account is sufficient.

Software is downloaded?

☐	Dell Data Security client software and Security Management Server downloads are located in the **Drivers & Downloads** folder at www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research or www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research or From the product page http://www.dell.com/support 1. Select **Drivers & Downloads**. 2. From the Operating system list, select the correct operating system for the product you are downloading. For example, to download Dell Enterprise Server, select **one of the Windows Server options.** 3. Under the applicable software title, select **Download File**.
☐	If you have purchased Encryption or Endpoint Security Suite Enterprise on-the-box, the software can be delivered to the target computer using Dell Digital Delivery.

License file(s) are available?

☐	The license file is an XML file located on the ddpe.credant.com site in the **Client Licenses** folder.

NOTE:

If you purchased your licenses on-the-box, no license file is necessary. The entitlement are automatically downloaded from Dell upon activation of any new Encryption or Endpoint Security Suite Enterprise client.

Servers meet required hardware specifications?

☐	See Security Management Server Virtual Architecture Design.

DNS alias created for Security Management Server Virtual and/or Policy Proxies with Split DNS for internal and external traffic?

It is recommended that you create DNS aliases, for scalability. This will allow you to add additional servers later or separate components of the application without requiring client update.

☐	DNS aliases are created, if desired. Suggested DNS aliases: • Security Management Server: dds.<domain.com> • Front end Server: dds-fe.<domain.com>

NOTE:

Split-DNS allows the user of the same DNS name internally and externally. This means that we could internally supply dds.<domain.com> as an internal c-name, and direct this to the Dell Security Management Server (back-end), and externally we could supply an a-record for dds.<domain.com> and forward the relevant ports (see Ports for Security Management Server Virtual) to the front-end server. We could leverage DNS round-robin or a load-balancer to distribute the load to the various front-ends (if multiple exist).

Plan for SSL Certificates?

☐	We have an internal Certificate Authority (CA) that can be used to sign certificates and is trusted by all workstations in the environment **or** we plan to purchase a signed certificate using a public Certificate Authority, such as VeriSign or Entrust. If using a public Certificate Authority, please inform the Dell Client Services Engineer.

Change Control requirements identified and communicated to Dell?

☐	Submit any specific Change Control requirements for the installation of Encryption or Endpoint Security Suite Enterprise to Dell Client Services prior to the installation engagement. These requirements may include changes to the application server(s), database, and client workstations.

Test Hardware prepared?

☐	Prepare at least three computers with your corporate computer image to be used for testing. Dell recommends that you **not** use production computers for testing. Production computers should be used during a production pilot after encryption policies have been defined and tested using the Test Plan provided by Dell.

4

Preparation Checklist - Upgrade/Migration

This checklist applies only to Security Management Server.

NOTE:

Update Security Management Server Virtual from the Basic Configuration menu in your Dell Server Terminal. For more information, see *Security Management Server Virtual Quick Start and Installation Guide*.

Use the following checklist to ensure you have met all prerequisites before beginning to upgrade Encryption or Endpoint Security Suite Enterprise.

Servers meet required software specifications?

☐	Windows Server 2012 R2 (Standard or Datacenter), Windows Server 2016 (Standard or Datacenter), Windows Server 2019 (Standard or Datacenter), or Windows Server 2022 (Standard or Datacenter) is installed. Alternatively, a virtualized environment can be installed. **NOTE:** Updating to Dell Server v11.0 or higher requires Windows Server 2019 or higher.
☐	Windows Installer 4.0 or later is installed.
☐	.NET Framework 4.6.1 is installed.
☐	Microsoft SQL Native Client 2012 is installed, if using SQL Server 2012 or SQL Server 2016. If available, SQL Native Client 2014 may be used. **NOTE:** SQL Express is not supported with Security Management Server.
☐	Windows Firewall is disabled or configured to allow (inbound) ports 8000, 8050, 8081, 8443, 8888, 61613.
☐	Connectivity is available between Security Management Server and Active Directory (AD) over ports 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (inbound to AD).
☐	UAC is disabled before installation on Windows Server 2012 R2 when installing in C:\Program Files. The server must be rebooted for this change to take effect. (see Windows Control Panel > User Accounts). • Windows Server 2012 R2 - the installer disables UAC. • Windows Server 2016 R2 - the installer disables UAC.

Service accounts successfully created?

☐	Service account with read-only access to AD (LDAP) - basic user/domain user account is sufficient.
☐	Service account must have local administrator rights to the Security Management Server application servers.
☐	To use Windows authentication for the database, a domain services account with system administrator rights. The user account must be in the format DOMAIN\Username and have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.
☐	To use SQL authentication, the SQL account used must have system administrator rights on the SQL Server. The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.

Database and all necessary files are backed up?

☐	The entire existing installation is backed up to an alternate location. The backup should include the SQL database, secretKeyStore, and configuration files.
☐	Ensure that these most critical files, which store information necessary to connect to the database, are backed up: <Installation folder>\Enterprise Edition\Compatibility Server\conf\server_config.xml <Installation folder>\Enterprise Edition\Compatibility Server\conf\secretKeyStore <Installation folder>\Enterprise Edition\Compatibility Server\conf\gkresource.xml

Installation key and license file are available?

☐	The license key is included in the original email with CFT credentials - see Example Customer Notification Email. This key is also included in the download of the application from http://www.dell.com/support and https://ddpe.credant.com.
☐	The license file is an XML file located on the CFT site under in the **Client Licenses** folder.

NOTE:

If you purchased your licenses on-the-box, no license file is necessary. The entitlement is automatically downloaded from Dell upon activation of any new Encryption or Endpoint Security Suite Enterprise client.

New and existing Dell Data Security software is downloaded?

Download from Dell Data Security file transfer site (CFT).

☐	Software is located at https://ddpe.credant.com in the **SoftwareDownloads** folder.
☐	If you purchased Encryption Enterprise or Endpoint Security Suite Enterprise on-the-box (OTB), the software is optionally fulfilled using Dell Digital Delivery. Alternatively, the software can be downloaded from www.dell.com/support or ddpe.credant.com respectively.

Have enough endpoint licenses?

Prior to upgrading, ensure that you have enough client licenses to cover all of the endpoints in your environment. If your installations currently exceed your license count, contact your Dell Sales Representative prior to upgrading or migrating. Dell Data Security performs license validation, and activations is prevented if no licenses are available.

☐	I have enough licenses to cover my environment.

Are DNS records documented?

☐	Validate that DNS records are documented and staged for update if hardware has been changed.

Plan for SSL Certificates?

☐	We have an internal Certificate Authority (CA) that can be used to sign certificates and is trusted by all workstations in the environment **or** we plan to purchase a signed certificate using a public Certificate Authority, such as VeriSign or Entrust. If using a public Certificate Authority, inform the Dell Client Services Engineer. The Certificate contains the Entire Chain of Trust (Root and Intermediate) with Public and Private Key Signatures.
☐	Subject Alternate Names (SANs) on Certificate Request match all DNS aliases given to every server being used for Dell Enterprise Server installation. Does not apply to Wildcard or Self Signed certificate requests.
☐	Certificate is generated to a .pfx format.

Change Control requirements identified and communicated to Dell?

☐	Submit any specific Change Control requirements for the installation of Encryption or Endpoint Security Suite Enterprise to Dell Client Services prior to the installation engagement. These requirements may include changes to the application server(s), database, and client workstations.

Test Hardware prepared?

☐	Prepare at least three computers with your corporate computer image to be used for testing. Dell recommends that you **not** use productions computers for testing. Production computers should be used during a production pilot after encryption policies have been defined and tested using the Test Plan provided by Dell.

5

Architecture

This section details architecture design recommendations for Dell Data Security implementation. Select the Dell Server you will deploy:

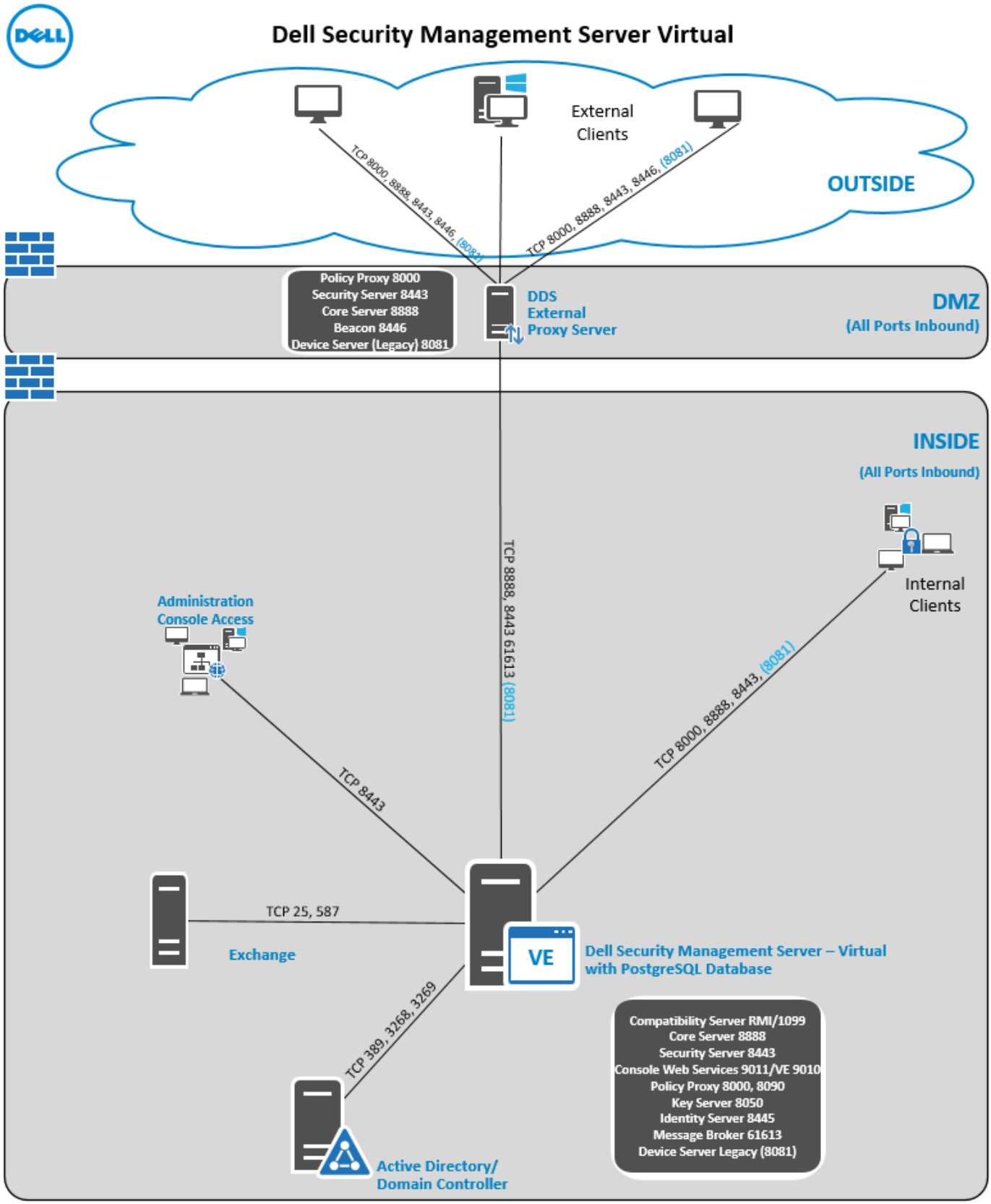
- Security Management Server Architecture Design
- Security Management Server Virtual Architecture Design

Security Management Server Virtual Architecture Design

The Encryption Enterprise and Endpoint Security Suite Enterprise solutions are highly scalable products, based on the number of endpoints targeted for encryption in your organization.

Architecture Components

Below is a basic deployment for the Dell Security Management Server Virtual.



Ports

The following table describes each component and its function.

Name	Default Port	Description
Access Group Service	TCP/ 8006	Manages various permissions and group access for various Dell Security products. **NOTE:** Port 8006 is not currently secured. Ensure this port is properly filtered through a firewall. This port is internal only.
Management Console	HTTPS/ 8443	Administration console and control center for the entire enterprise deployment.
Core Server	HTTPS/ 8887 (closed)	Manages policy flow, licenses, and registration for Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Prevention. Processes inventory data for use by the Management Console. Collects and stores authentication data. Controls role-based access.
Core Server HA (High Availability)	HTTPS/ 8888	A high-availability service that allows for increased security and performance of HTTPS connections with the Management Console, Preboot Authentication, SED Management, FDE, BitLocker Manager, Threat Protection, and Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Communicates with Policy Proxy; manages forensic key retrievals, activations of clients, and SED-PBA and Full Disk Encryption-PBA communication.
Compatibility Server	TCP/ 1099 (closed)	A service for managing the enterprise architecture. Collects and stores initial inventory data during activation and policy data during migrations. Processes data based on user groups. **NOTE:** Port 1099 should be filtered through a firewall. Dell suggests this port be internal only.
Message Broker Service	TCP/ 61616 (closed) and STOMP/ 61613 (closed or, if configured for DMZ,	Handles communication between services of the Dell Server. Stages policy information created by the Compatibility Server for Policy Proxy queuing. **NOTE:** Port 61616 should be filtered through a firewall. Dell recommends this port be internal only. **NOTE:** Port 61613 should only be opened to Security Management

Name	Default Port	Description
	61613 is open)	Servers configured in Front-End mode.
Identity Server	8445 (closed)	Handles domain authentication requests, including authentication for SED Management.
Forensic Server	HTTPS/ 8448	Allows administrators that have appropriate privileges to get encryption keys from the Management Console for use in data unlocks or decryption tasks. Required for Forensic API.
Inventory Server	8887	Processes the inventory queue.
Policy Proxy	TCP/ 8000	Provides a network-based communication path to deliver security policy updates and inventory updates. Required for Encryption Enterprise (Windows and Mac)
PostGres	TCP/ 5432	Local database used for eventing data. **NOTE:** Port 5432 should be filtered through a firewall. Dell recommends this port be internal only.
LDAP	389/636, 3268/3269 RPC - 135, 49125+	Port 389 - This port is used for requesting information from the local domain controller. LDAP requests sent to port 389 can be used to search for objects only within the global catalog's home domain. However, the requesting application can obtain all of the attributes for those objects. For example, a request to port 389 could be used to obtain a user's department. Port 3268 - This port is used for queries specifically targeted for the global catalog. LDAP requests sent to port 3268 can be used to search for objects in the entire forest. However, only the attributes marked for replication to the global catalog can be returned. For example, a user's department could not be returned using port 3268 since this attribute is not replicated to the global catalog.
Client Authentication	HTTPS/ 8449	Allows client servers to authenticate against Dell Server. Required for Server Encryption

Security Management Server Architecture Design

Encryption Enterprise and Endpoint Security Suite Enterprise solutions are highly scalable products, based on the number of endpoints that are targeted for encryption in your organization.

Architecture Components

Below are suggested hardware configurations that suit most environments.

Security Management Server

- Operating System: Windows Server 2012 R2 (Standard, Datacenter 64-bit), Windows Server 2016 (Standard, Datacenter 64-bit), Windows Server 2019 (Standard, Datacenter), Windows Server 2022 (Standard or Datacenter)
- Virtual or Physical Machine
- CPU: 4 Core(s)
- RAM: 16.00 GB
- Drive C: 30 GB available disk space for logs and application databases

NOTE: Up to 10 GB may be consumed for a local event database that is stored within PostgreSQL.

Proxy Server

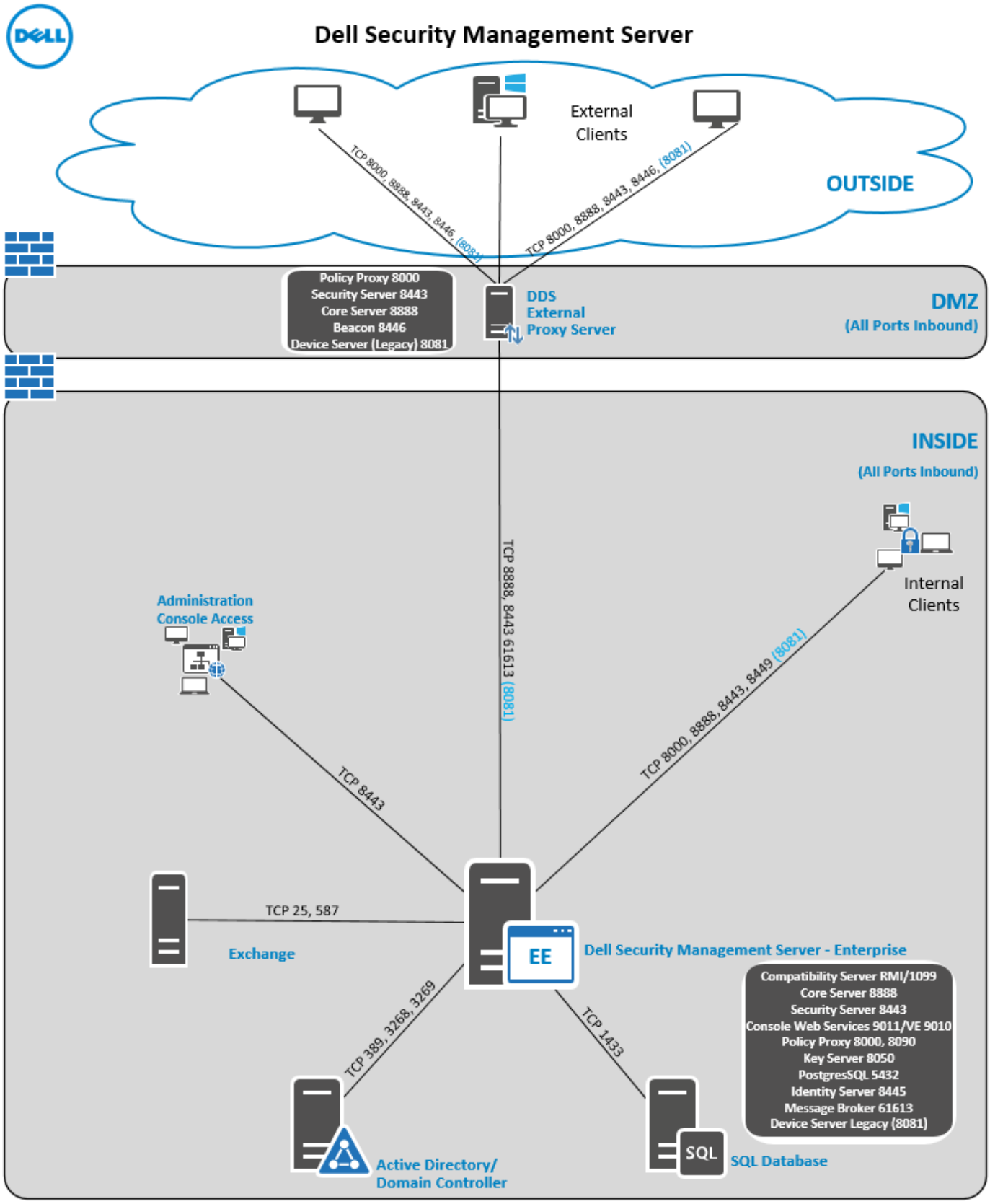
- Operating System: Windows Server 2012 R2 (Standard, Datacenter 64-bit), Windows Server 2016 (Standard, Datacenter 64-bit), Windows Server 2019 (Standard, Datacenter), Windows Server 2022 (Standard or Datacenter)
- Virtual/ or Machine
- CPU: 2 Core(s)
- RAM: 8.00 GB
- Drive C: 20 GB available disk space for logs

SQL Server Hardware Specs

- CPU: 4 Core(s)
- RAM: 24.00 GB
- Data Drive: 100 -150 GB of available disk space (This amount may vary based on environment.)
- Log Drive: 50 GB of available disk space (This amount may vary based on environment.).

NOTE: Dell Technologies recommends following SQL Server Best Practices, though the above information should cover most environments.

Below is a basic deployment for the Dell Security Management Server.



NOTE: If the organization has more than 20,000 endpoints, contact Dell ProSupport for assistance.

Ports

The following table describes each component and its function.

Name	Default Port	Description
ACL Service	TCP/ 8006	Manages various permissions and group access for various Dell Security products. **NOTE:** Port 8006 is not secured. Ensure that this port is properly filtered through a firewall. This port is internal only.
Management Console	HTTP(S)/ 8443	Administration console and control center for the entire enterprise deployment.
Core Server	HTTPS/ 8888	Manages policy flow, licenses, and registration for Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Prevention. Processes inventory data for use by the Management Console. Collects and stores authentication data. Controls role-based access.
Device Server	HTTPS/ 8081	Supports activations and password recovery. A component of the Security Management Server. Required for Encryption Enterprise (Windows and Mac)
Security Server	HTTPS/ 8443	Communicates with Policy Proxy; manages forensic key retrievals, activations of clients, SED-PBA and Full Disk Encryption-PBA communication, and Active Directory for authentication or reconciliation. This includes identity validation for authentication into the Management Console. Requires SQL database access.
Compatibility Server	TCP/ 1099	A service for managing the enterprise architecture. Collects and stores initial inventory data during activation and policy data during migrations. Processes data based on user groups. **NOTE:** Port 1099 should be filtered through a firewall. Dell Technologies recommends this port be internal only.
Message Broker Service	TCP/ 61616	Handles communication between services of the Dell Server.

Name	Default Port	Description
	and STOMP/ 61613	Stages policy information that the Compatibility Server creates for Policy Proxy queuing. Requires SQL database access. **NOTE:** Port 61616 should be filtered through a firewall. Dell Technologies recommends this port be internal only. **NOTE:** Only open port 61613 to Security Management Servers configured in Front-End mode.
Key Server	TCP/ 8050	Negotiates, authenticates, and encrypts a client connection using Kerberos APIs. Requires SQL database access to pull the key data.
Policy Proxy	TCP/ 8000	Provides a network-based communication path to deliver security policy updates and inventory updates.
PostGres	TCP/ 5432	Local database used for eventing data. **NOTE:** Port 5432 should be filtered through a firewall. Dell Technologies recommends this port be internal only.
LDAP	TCP/ 389/636 (local domain controller), 3268/3269 (global catalog) TCP/ 135/ 49125+ (RPC)	Port 389 - This port is used for requesting information from the local domain controller. LDAP requests sent to port 389 can be used to search for objects only within the home domain of the global catalog. However, the requesting application can obtain all the attributes for those objects. For example, a request to port 389 could be used to obtain a user's department. Port 3268 - This port is used for queries that are specifically targeted for the global catalog. LDAP requests sent to port 3268 can be used to search for objects in the entire forest. However, only the attributes marked for replication to the global catalog can be returned. For example, a user's department could not be returned using port 3268 since this attribute is not replicated to the global catalog.
Microsoft SQL Database	TCP/ 1433	The default SQL Server port is 1433, and client ports are assigned a random value 1024–5000.

Name	Default Port	Description
Client Authentication	HTTPS/ 8449	Allows client servers to authenticate with Dell Server. Required for Server Encryption.

6

SQL Server Best Practices

The following list explains SQL Server best practices, which should be implemented when Dell security is installed if not already implemented.

1. Ensure the NTFS block size where the data file and log file reside is 64 KB. SQL Server extents (basic unit of SQL storage) are 64 KB.

   For more information, search Microsoft's TechNet articles for "Understanding Pages and Extents."

2. As a general guideline, set the maximum amount of SQL Server memory to 80 percent of the installed memory.

   For more information, search Microsoft's TechNet articles for *Server Memory Server Configuration Options*.

   - Microsoft SQL Server 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3. Set -t1222 on the instance startup properties to ensure deadlock information is captured if one occurs.

   For more information, search Microsoft's TechNet articles for "Trace Flags (Transact-SQL)."

   - Microsoft SQL Server 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms188396.aspx

4. Ensure that all Indexes are covered by a weekly maintenance job to rebuild the indexes.

5. Validate that permissions and features are appropriate for the database leveraged by the Security Management Server. For more information, see KB article 124909.

7

Example Customer Notification Email

After you purchase Dell Data Security, you will receive an email from DellDataSecurity@Dell.com. Below is an example of the email, which will include your CFT credentials and License Key information.

Dell Data Security

Thank you for purchasing Dell Encryption Enterprise - Order %USER.CUSTOM2%

Dell Encryption offers a comprehensive data-centric encryption solution that secures data wherever it goes while enabling IT end-users to do more. Listed below are helpful links and information about the support services that are available to you.

Get your Software

Download your software and its accompanying documentation.

Download Now

Username:	%USER.LOGIN%
Password:	%USER.PASSWORD%
Required to change password:	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
License Key:	xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx

Explore our top knowledge base solutions for Dell Encryption Enterprise.

ProSupport for Software

- Online Support: www.dell.com/datasecuritysupport
- 1.877.459.7304, Option 1, X4310039 - U.S. & Canada Only
- Outside the U.S., click here for a list of numbers

Need Support? CHAT NOW! Click Here

You will need your software service tag to open a Support ticket. This is a seven digit alphanumeric code located above or also can be found on your asset.

Other Products and Services

- Explore our Products
- Subscribe to our Newsletter
- Search our Knowledge Base
- Deployment and Training Services - please contact your sales representative for options