

Dell Data Protection

Getting Started with Dell Data Protection v9.6



Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

© 2016 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Registered trademarks and trademarks used in the Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools, and Dell Data Protection | Secure Lifecycle suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecuriD® are registered trademarks of Dell EMC. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. This product uses parts of the 7-Zip program. The source code can be found at 7-zip.org/license.txt. Licensing is under the GNU LGPL license + unRAR restrictions (7-zip.org/license.txt).

Getting Started with Dell Data Protection

2017 - 02

Rev. A01

Contents

1 Implementation Phases.....	4
2 Kick-off and Requirements Review.....	5
Dell Data Protection client documents.....	6
Dell Data Protection Server documents.....	6
3 Preparation Checklist - Initial Implementation.....	8
Dell Enterprise Server initial implementation checklist.....	8
DDP Enterprise Server - VE initial implementation checklist.....	11
4 Preparation Checklist - Upgrade/Migration.....	13
5 Architecture.....	16
Dell Enterprise Server Architecture Design.....	16
Dell Enterprise Server Ports.....	21
DDP Enterprise Server - Virtual Edition Architecture Design.....	24
Virtual Edition Ports.....	24
6 Example Customer Notification Email.....	28



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:
 - **Dell Enterprise Server**
 - Centralized management of devices
 - Runs on a Microsoft Windows server
 - **DDP Enterprise Server - VE**
 - Centralized management of up to 3,500 devices
 - Runs in a virtualized environment

For more information about Dell Data Protection Servers, see *Enterprise Server Installation and Migration Guide* or *Virtual Edition Quick Start and Installation Guide*. To obtain these documents, refer to Dell Data Protection Server documents.

For instructions about client requirements and software installation, select the applicable documents based on your deployment:

- Enterprise Edition Basic Installation Guide or Enterprise Edition Advanced Installation Guide
- Endpoint Security Suite Basic Installation Guide or Endpoint Security Suite Advanced Installation Guide
- Endpoint Security Suite Enterprise Basic Installation Guide or Endpoint Security Suite Enterprise Advanced Installation Guide
- Personal Edition Installation Guide
- Security Tools Installation Guide
- Enterprise Edition for Mac Administrator Guide
- Endpoint Security Suite Enterprise for Mac Administrator Guide
- Secure Lifecycle User Guide
- Secure Lifecycle for Mac Administrator Guide
- Mobile Edition Administrator Guide

To obtain these documents, refer to [Dell Data Protection client documents](#).

- Configure Initial Policy
 - **Dell Enterprise Server** - see *Enterprise Server Installation and Migration Guide, Administrative Tasks*
 - **DDP Enterprise Server - VE** - see *Virtual Edition Quick Start and Installation Guide, Remote Management Console Administrative Tasks*
- Execute Test Plan
- Client Packaging
- Participate in Dell Data Protection Administrator basic knowledge transfer
- Implement Best Practices
- Coordinate Pilot or Deployment Support with Dell Client Services

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 Protection 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 end users have local admin 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?
 - Enterprise Edition
 - Encryption (DE entitlement) - Windows Encryption, Server Encryption, External Media Shield (EMS), SED Management, Advanced Authentication, BitLocker Manager (BLM), and Mac Encryption.
 - External Media Edition (EME entitlement)
 - Secure Lifecycle (CE entitlement)
 - Endpoint Security Suite
 - Threat Protection (TP entitlement)
 - Encryption (DE entitlement) - Windows Encryption, External Media Shield (EMS), SED Management, Advanced Authentication, BitLocker Manager (BLM), and Mac Encryption.
 - External Media Edition (EME entitlement)
 - Endpoint Security Suite Enterprise
 - Advanced Threat Protection (ATP entitlement)
 - Encryption (DE entitlement) - Windows Encryption, Server Encryption, External Media Shield (EMS), SED Management, Advanced Authentication, BitLocker Manager (BLM), and Mac Encryption.
 - External Media Edition (EME entitlement)
 - Secure Lifecycle (CE entitlement)
 - Mobile Edition (ME entitlement) for Android, iOS, and Windows Phone
- 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 OS versions are targeted for encryption?
- 13 Do you have alternate boot partitions configured on your endpoints?



- a Manufacturer Recovery Partition
- b Dual-boot Workstations

Dell Data Protection client documents

For installation requirements, supported OS versions and SEDs, and user instructions for the Dell Data Protection products you plan to deploy, refer to the applicable document(s), listed below.

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

- *Enterprise Edition Basic Installation Guide* - Installation guide for Enterprise Edition.
- *Enterprise Edition Advanced Installation Guide* - Installation guide for Enterprise Edition, with advanced switches and parameters for customized installations.
- *DDP Console User Guide* - Instructions for Advanced Authentication end users.
- *Secure Lifecycle User Guide* - Installation, activation, and operation instructions for Secure Lifecycle end users.

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

Endpoint Security Suite (Windows clients) - See the following documents at this address: www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/manuals.

- *Endpoint Security Suite Basic Installation Guide* - Installation guide for Endpoint Security Suite.
- *Endpoint Security Suite Advanced Installation Guide* - Installation guide for Endpoint Security Suite, with advanced switches and parameters for customized installations.
- *DDP Console User Guide* - Instructions for Endpoint Security Suite end users.

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

- *Endpoint Security Suite Enterprise Basic Installation Guide* - Installation guide for Endpoint Security Suite Enterprise.
- *Endpoint Security Suite Enterprise Advanced Installation Guide* - Installation guide for Endpoint Security Suite Enterprise, with advanced switches and parameters for customized installations.
- *DDP Console User Guide* - Instructions for Endpoint Security Suite Enterprise end users.

Endpoint Security Suite Enterprise (Mac clients) - See the following document at this address: 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 Endpoint Security Suite Enterprise for Mac.

Secure Lifecycle - See the following documents at this address: <http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-secure-lifecycle/manuals>

- *Secure Lifecycle User Guide* - Installation, activation, and operation instructions for Secure Lifecycle end users.
- *Secure Lifecycle for Mac Administrator Guide* - Installation and deployment instructions for Secure Lifecycle.

Mobile Edition for Android, iOS, and Windows Phone

- See the *Mobile Edition Administrator Guide* at www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. The *Administrator Guide* explains how to deploy Mobile Edition.

Dell Data Protection Server documents

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



Dell Enterprise Server

- See the *Enterprise 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/04/product-support/product/dell-dp-endpt-security-suite/manuals

or

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

or

<http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-secure-lifecycle/manuals>

DDP Enterprise Server - Virtual Edition

- See the *Virtual Edition Quick Start Guide 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/04/product-support/product/dell-dp-endpt-security-suite/manuals

or

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

or

<http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-secure-lifecycle/manuals>



Preparation Checklist - Initial Implementation

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

- [Dell Enterprise Server checklist](#)
- [DDP Enterprise Server - VE checklist](#)

Dell Enterprise 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.
- ☐ Any production endpoints used during Proof of Concept testing have been decrypted or key bundles downloaded.
- ☐ The Proof of Concept application has been removed from the environment.

NOTE:

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

Servers meet required hardware specifications?

- ☐ See [Dell Enterprise Server Architecture Design](#).

Servers meet required software specifications?

- ☐ Windows Server 2008 SP2 64-bit (Standard or Enterprise); 2008 R2 SP0-SP1 64-bit (Standard or Enterprise); 2012 R2 (Standard or Datacenter) is installed.
- ☐ Windows Installer 4.0 or later is installed.
- ☐ .NET Framework 4.5 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 Dell Enterprise Server.

- ☐ Windows Firewall is disabled or configured to allow (inbound) ports 80, 1099, 1433, 8000, 8050, 8081, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616.

- ❑ Connectivity is available between Dell Enterprise Server and Active Directory (AD) over ports 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (inbound to AD).
- ❑ UAC is disabled (see Windows Control Panel > User Accounts).
 - Windows Server 2008 SP2 64-bit/Windows Server 2008 R2 SP0-SP1 64-bit
 - Windows Server 2012 R2 - the installer disables UAC.
 - Windows Server 2012 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 Dell Enterprise 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 Protection client software and Dell Enterprise 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/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

or

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

or

www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-secure-lifecycle/research

To navigate to the folder from www.dell.com/support

- 1 Under **Browse for a product**, select **View Products** then **Software & Security** and **Endpoint Security Solutions**.
 - 2 Select **Dell Data Protection | Encryption**, **Dell Data Protection | Endpoint Security Suite**, or **Dell Data Protection | Endpoint Security Suite Enterprise**, or **Dell Data Protection | Secure Lifecycle** then **Drivers & downloads**.
 - 3 From the Operating system pull-down 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**.
 - 4 Under the applicable software title, select **Download File**.
- ❑ If you have purchased Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise on-the-box, the software can be downloaded from www.dell.com. On-the-box refers to software that is included with the factory computer image from Dell. Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise can be preinstalled at the factory on any Dell computer.

OR

Download from Dell Data Protection file transfer site (CFT)



- ❑ Software is located at <https://ddpe.credant.com> or <https://cft.credant.com> under the **SoftwareDownloads** folder.
- ❑ If you have purchased Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise on-the-box, the software can be downloaded from www.dell.com. On-the-box refers to software that is included with the factory computer image from Dell. Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise can be preinstalled at the factory on any Dell computer.

Installation key and license file are available?

- ❑ The license key is included in the original email with CFT credentials - see [Example Customer Notification Email](#).
- ❑ The license file is an XML file located on the CFT site under the **Client Licenses** folder.

NOTE:

If you purchased your licenses on-the-box, no license file is necessary. The entitlement will be automatically downloaded from Dell upon activation of any new Encryption, Endpoint Security Suite, 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 Enterprise Server Installation and Migration Guide. The Enterprise 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 Dell Enterprise 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:
 - Dell Enterprise Server: ddpe-es.<domain.com>
 - Front-End Server: ddpe-fe.<domain.com>

NOTE:

Split-DNS allows you use to use the same DNS name for both internal and external Front-End Services and is necessary in some cases. Split-DNS enables you to use a single address for your clients and provides flexibility when performing upgrades or scaling the solution later. A suggested CNAME for Front-End Servers when using Split-DNS is this: ddpe-fe.<domain.com>.

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. 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, Endpoint Security Suite, 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 live systems for testing. Live systems should be used during a production pilot after encryption policies have been defined and tested using the Test Plan provided by Dell.

DDP Enterprise Server - VE initial implementation checklist

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

- ❑ The Proof of Concept (POC) database and application have been backed up and uninstalled (if using the same server) before the installation engagement with Dell.
- ❑ Any production endpoints used during Proof of Concept testing have been decrypted or key bundles downloaded.
- ❑ The Proof of Concept application has been removed from the environment.

NOTE:

All new implementations must begin with a new database and installation of the Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise software. Dell Client Services will not perform a new implementation using a POC environment. Any endpoints encrypted during a Proof of Concept 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 Protection client software and Virtual Edition 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/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y
or
www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research
or
www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-secure-lifecycle/research

To navigate to the folder from www.dell.com/support

- 1 Under **Browse for a product**, select **View Products** then **Software & Security** and **Endpoint Security Solutions**.
- 2 Select **Dell Data Protection | Encryption**, **Dell Data Protection | Endpoint Security Suite**, or **Dell Data Protection | Endpoint Security Suite Enterprise**, or **Dell Data Protection | Secure Lifecycle** then **Drivers & downloads**.



- 3 From the Operating system pull-down list, select the correct operating system for the product you are downloading. For example, to download Virtual Edition, select **one of the VMware versions**.
 - 4 Under the applicable software title, select **Download File**.
- ☐ If you have purchased Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise on-the-box, the software can be downloaded from www.dell.com. On-the-box refers to software that is included with the factory computer image from Dell. Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise can be preinstalled at the factory on any Dell computer.

License file(s) are available?

- ☐ The license file is an XML file located on the CFT site under the **Client Licenses** folder.

NOTE:

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

Servers meet required hardware specifications?

- ☐ See [DDP Enterprise Server - Virtual Edition Architecture Design](#).

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, Endpoint Security Suite, 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 live systems for testing. Live systems should be used during a production pilot after encryption policies have been defined and tested using the Test Plan provided by Dell.

Preparation Checklist - Upgrade/Migration

This checklist applies only to Dell Enterprise Server.

NOTE:

Update DDP Enterprise Server - VE from the Basic Configuration menu in your VE Terminal. For more information, see ***Virtual Edition Quick Start and Installation Guide***.

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

Servers meet required software specifications?

- ☐ Windows Server 2008 SP2 64-bit (Standard or Enterprise); 2008 R2 SP0-SP1 64-bit (Standard or Enterprise); 2012 R2 (Standard or Datacenter) is installed.
- ☐ Windows Installer 4.0 or later is installed.
- ☐ .NET Framework 4.5 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 Dell Enterprise Server.

- ☐ Windows Firewall is disabled or configured to allow (inbound) ports 80, 1099, 1433, 8000, 8050, 8081, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616.
- ☐ Connectivity is available between Dell Enterprise Server and Active Directory (AD) over ports 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (inbound to AD).
- ☐ UAC is disabled (see Windows Control Panel > User Accounts).
 - Windows Server 2008 SP2 64-bit/Windows Server 2008 R2 SP0-SP1 64-bit
 - Windows Server 2012 R2 - the installer disables UAC.
 - Windows Server 2016 - 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 Dell Enterprise 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](#).
- ❑ The license file is an XML file located on the CFT site under the **Client Licenses** folder.

NOTE:

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

New and existing Dell Data Protection software is downloaded?

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

- ❑ Software is located at <https://ddpe.credant.com> or <https://cft.credant.com> under the **SoftwareDownloads** folder.
- ❑ If you have purchased Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise on-the-box, the software can be downloaded from www.dell.com. On-the-box refers to software that is included with the factory computer image from Dell. Encryption, Endpoint Security Suite, or Endpoint Security Suite Enterprise can be preinstalled at the factory on any Dell computer.

Have enough endpoint licenses?

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

- ❑ I have enough licenses to cover my environment.

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. 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, Endpoint Security Suite, 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 live systems for testing. Live systems should be used during a production pilot after encryption policies have been defined and tested using the Test Plan provided by Dell.



Architecture

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

- [Dell Enterprise Server](#)
- [DDP Enterprise Server - Virtual Edition](#)

Dell Enterprise Server Architecture Design

The Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise, and Secure Lifecycle solutions are highly scalable products, scaled on the size of your organization and the number of endpoints targeted for encryption. This section provides a set of guidelines for scaling the architecture for 5,000 to 60,000 endpoints.

NOTE: If the organization has more than 50,000 endpoints, please contact Dell ProSupport for assistance.

NOTE:

Each of the components listed in each section include the minimum hardware specifications, which are required to ensure optimal performance in most environments. Failing to allocate adequate resources to any of these components may result in performance degradation or functional problems with the application.

Up to 5,000 Endpoints

This architecture accommodates most small to medium size businesses ranging between 1 and 5,000 endpoints. All Dell Enterprise Server components can be installed on a single server. Optionally, a front-end server can be placed in the DMZ for publishing policies and/or activating endpoints over the Internet.

Architecture Components

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard or Enterprise Edition

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

Single-Server Configuration

16GB; 20GB or more free disk space (plus virtual paging space); Modern Quad-Core CPU (2 GHz+)

Server configuration when used with Front-End Server

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

Dell External Front-End Server

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard or Enterprise Edition

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

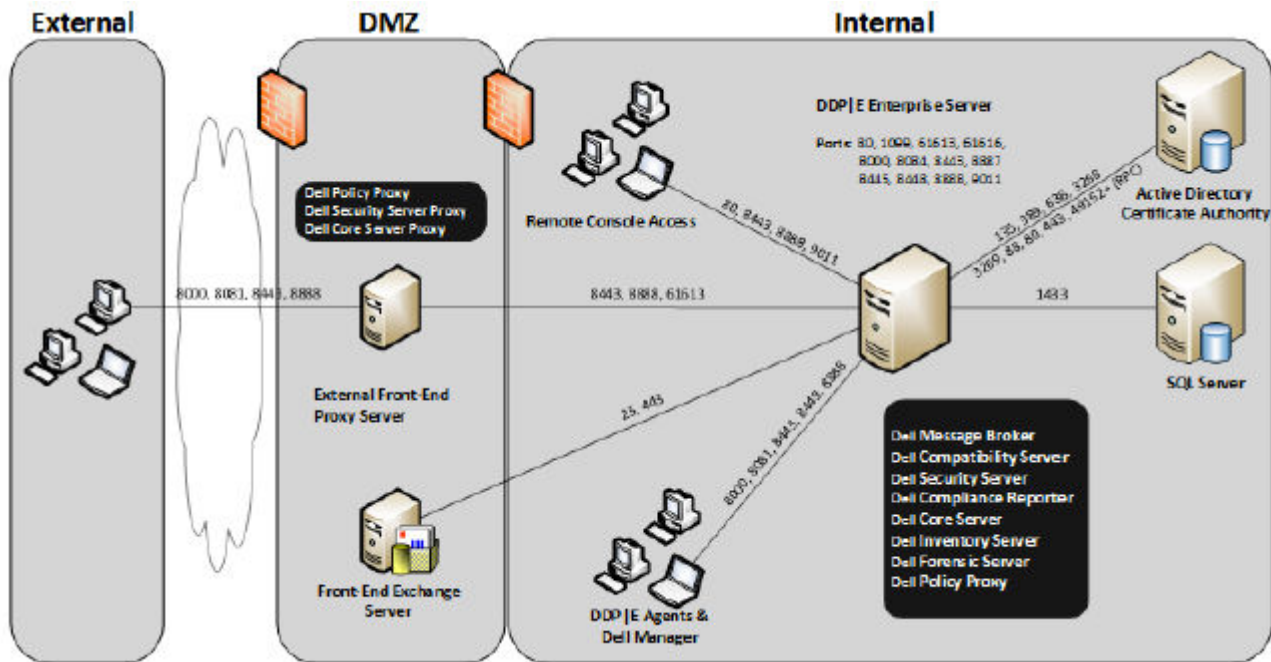
SQL Server

SQL Server 2008, SQL Server 2008 R2, and SQL Server 2008 SP4 (with KB3045311) Standard Edition / Enterprise Edition

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition



5,000 - 20,000 Endpoints

This architecture accommodates environments ranging between 5,000 and 20,000 endpoints. A front-end server is added to distribute the additional load and is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for publishing policies and/or activating endpoints over the Internet.

Architecture Components

Dell Enterprise Server

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

Dell Internal Front-End Server (1) and Dell External Front-End Server (1)

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard or Enterprise Edition

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition



8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

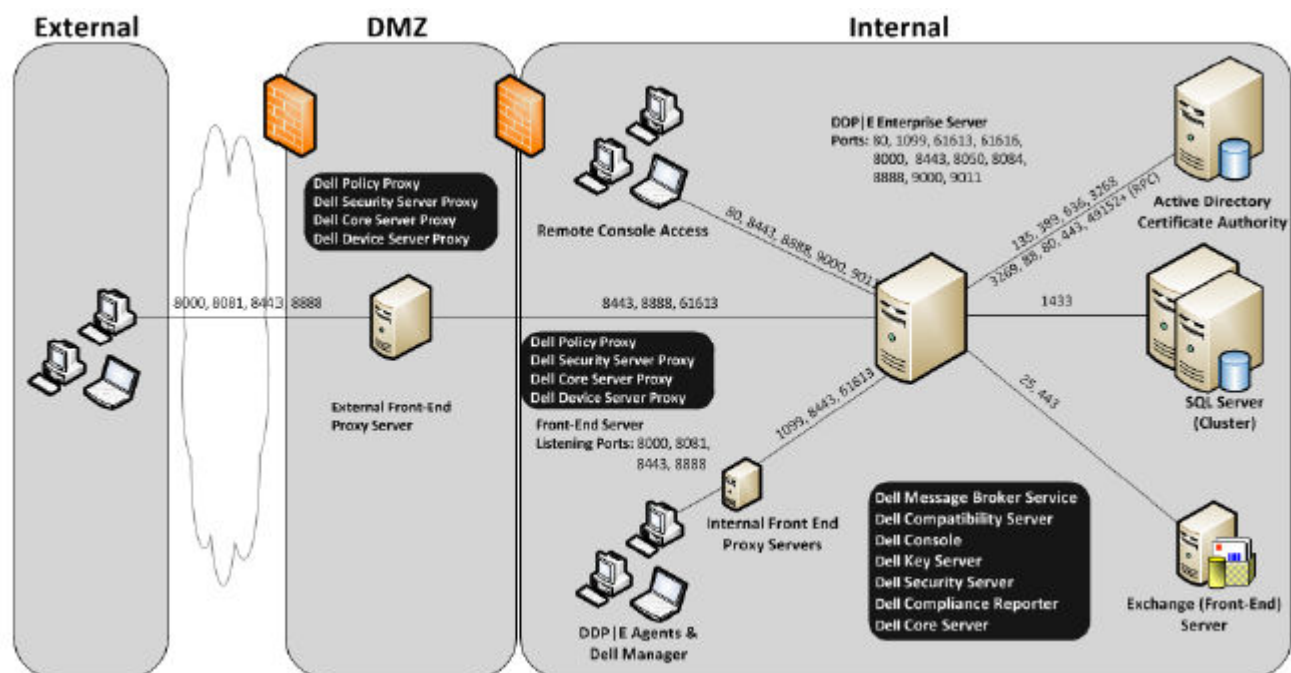
SQL Server

SQL Server 2008, SQL Server 2008 R2, and SQL Server 2008 SP4 (with KB3045311) Standard Edition / Enterprise Edition

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition



20,000 - 40,000 Endpoints

This architecture accommodates environments ranging between 20,000 and 40,000 endpoints. An additional front-end server is added to distribute the additional load. Each front-end server is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.

Architecture Components

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard or Enterprise Edition

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

Dell Internal Front-End Servers (2) and Dell External Front-End Server (1)

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard or Enterprise Edition

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

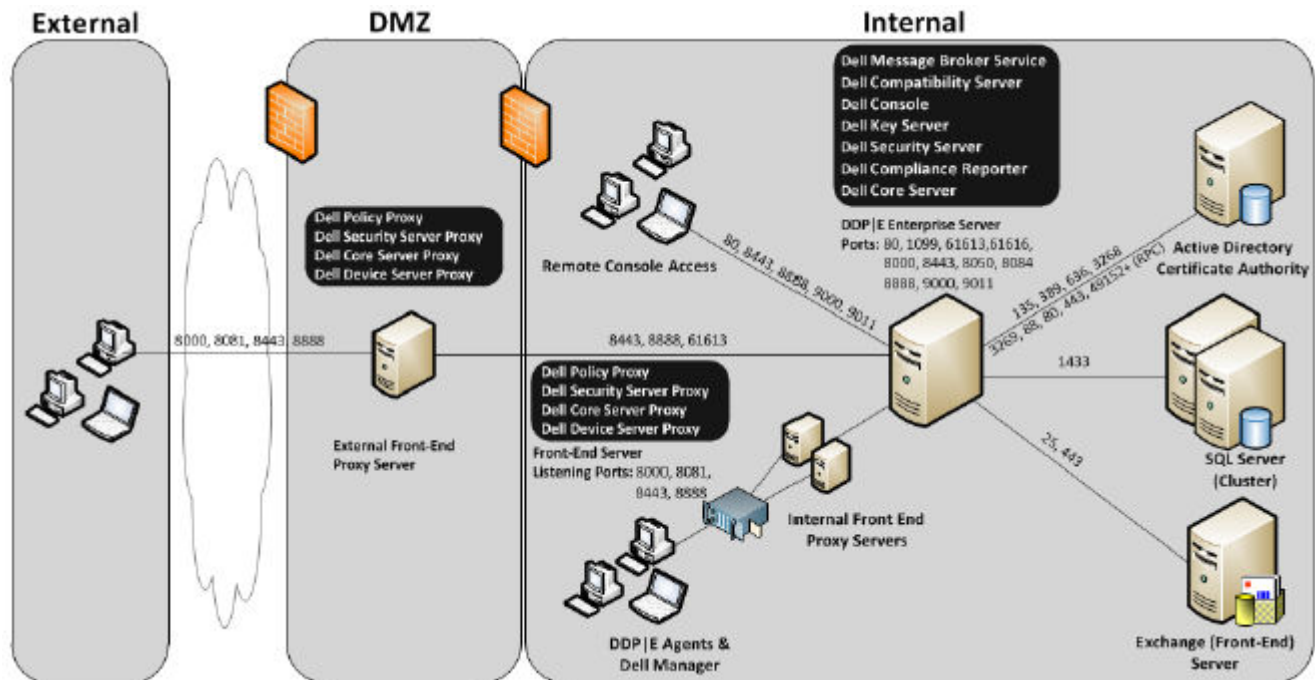
SQL Server

SQL Server 2008, SQL Server 2008 R2, and SQL Server 2008 SP4 (with KB3045311) Standard Edition / Enterprise Edition

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition



40,000 - 60,000 Endpoints

This architecture accommodates environments ranging between 40,000 and 60,000 endpoints. An additional front-end server is added to distribute the additional load. Each front-end server is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.

NOTE:

If the organization has more than 50,000 endpoints, please contact Dell ProSupport for assistance.

Architecture Components

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard or Enterprise Edition

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition



8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

Dell Internal Front-End Servers (2) and Dell External Front-End Server (1)

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard or Enterprise Edition

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

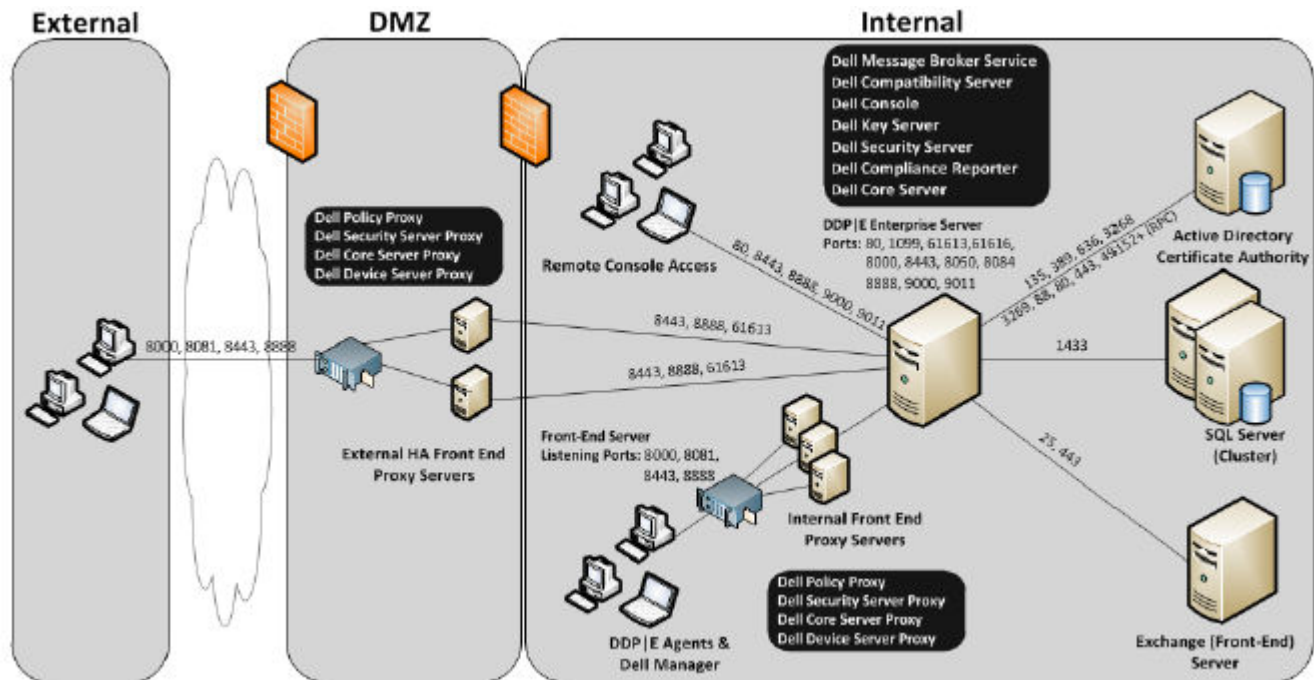
SQL Server

SQL Server 2008, SQL Server 2008 R2, and SQL Server 2008 SP4 (with KB3045311) Standard Edition / Enterprise Edition

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition



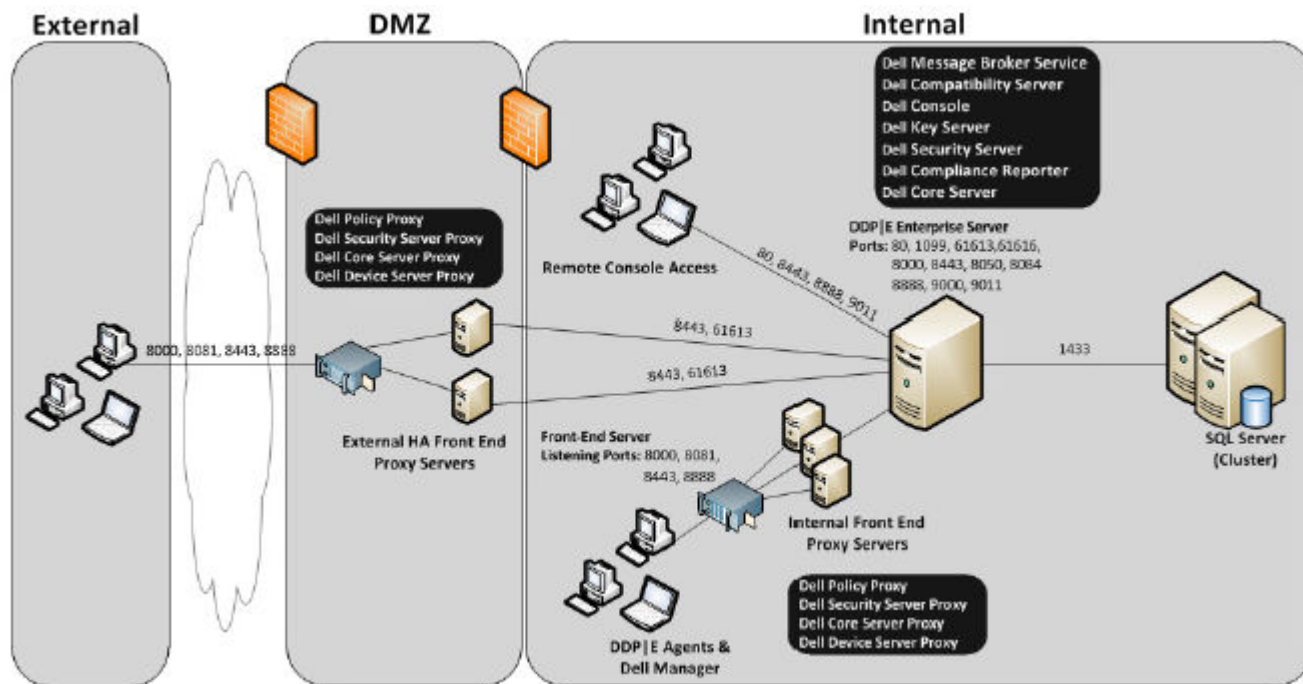
High Availability Considerations

This architecture depicts a highly available architecture supporting up to 60,000 endpoints. There are two Dell Enterprise Servers set up in an active/passive configuration. To failover to the second Dell Enterprise Server, stop the services on the primary node and point the DNS Alias (CNAME) to the second node. Start the services on the second node and launch the Remote Management Console to ensure the application is working properly. Services on the second (passive) node should be configured as "Manual" in order to prevent those services from accidentally starting during regular maintenance and patching.

An organization can also choose to have an SQL Cluster database server. In this configuration, the Dell Enterprise Server should be configured to use the cluster IP or hostname.

NOTE:
Database replication is not supported.

Client traffic is distributed across three internal front-end servers. Optionally, multiple front-end servers can also be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.



Virtualization

Dell Data Protection Application Servers

Disk speed on the hardware that hosts the virtual server, RAM allocation to the guest, and storage configuration may cause significant performance impact. The impact is most noticeable during activation, policy and inventory processing, and triage. Dell recommends reserving as much RAM as possible for the virtual host, and giving the virtual host priority in resource allocation. If performance is a concern, Dell recommends deploying to a non-virtual server environment.

SQL Server

In larger environments, it is highly recommended that the SQL Database server run on physical hardware and on a redundant system, such as a SQL Cluster, to ensure availability and data continuity. It is also recommended to perform daily full backups with transactional logging enabled to ensure that any newly generated keys through user/device activation are recoverable.

Database maintenance tasks should include rebuilding of all databases indexes and collecting statistics.

Dell Enterprise Server Ports

The following table describes each component and its function.

Name	Default Port	Description	Required For
Compliance Reporter	HTTP(S)/ 8084	Provides an extensive view of the environment for auditing and compliance reporting.	Reporting



Name	Default Port	Description	Required For
		A component of the Dell Enterprise Server.	
Remote Management Console	HTTP(S)/ 8443	Administration console and control center for the entire enterprise deployment.	All
		A component of the Dell Enterprise Server.	
Core Server	HTTPS/ 8888 and 9000	Manages policy flow, licenses, and registration for Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Protection. Processes inventory data for use by Compliance Reporter and the Remote Management Console. Collects and stores authentication data. Controls role-based access.	All
		A component of the Dell Enterprise Server.	
Device Server	HTTPS/ 8443	Supports activations and password recovery.	Enterprise Edition for Mac
		A component of the Dell Enterprise Server.	Enterprise Edition for Windows
	HTTPS/ 8081		CREDActivate
	(to Back End Dell Device Server		
Security Server	HTTPS/ 8443	Communicates with Policy Proxy; manages forensic key retrievals, activations of clients, Secure Lifecycle products, SED-PBA communication, and Active Directory for authentication or reconciliation, including identity validation for authentication into the Remote Management Console. Requires SQL database access.	All
		A component of the Dell Enterprise Server.	
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 in this service.	All
		A component of the Dell Enterprise Server.	
Message Broker Service	TCP/ 61616 and STOMP/ 61613	Handles communication between services of the Dell Enterprise Server. Stages policy information created by the Compatibility Server for policy proxy queuing. Requires SQL database access.	All
		A component of the Dell Enterprise Server.	
Identity Server	HTTPS/	Handles domain authentication requests, including authentication of the SED Manager.	All



Name	Default Port	Description	Required For
Key Server	8445	Requires an Active Directory account. Must be the account used to access SQL when Windows Authentication is used.	
		A component of the Dell Enterprise Server.	
	TCP/8050	Negotiates, authenticates, and encrypts a client connection using Kerberos APIs.	Dell Admin Utilities
		Requires SQL database access to pull the key data.	
Policy Proxy		A component of the Dell Enterprise Server.	
	TCP/8000	Provides a network-based communication path to deliver security policy updates and inventory updates.	Enterprise Edition for Mac Enterprise Edition for Windows
		A component of the Dell Enterprise Server.	Mobile Edition
LDAP	TCP/389/636 (local domain controller), 3268/3269 (global catalog)	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.	All
	TCP/135/49125+ (RPC)	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.	
Microsoft SQL Database	TCP/1433	The default SQL server port is 1433, and client ports are assigned a random value between 1024 and 5000.	All
Client Authentication	HTTPS/8449	Allows client servers to authenticate with Dell Enterprise Server.	Server Encryption (SE)
Email communication	25	Provides notifications of events.	Optional
EAS Device Manager		Enables over-the-air functionality. Installed on the Exchange Client Access Server.	Exchange ActiveSync Management of mobile devices.
EAS Mailbox Manager		The mailbox agent that is installed on the Exchange Mailbox Server.	Exchange ActiveSync Management of mobile devices.



DDP Enterprise Server - Virtual Edition Architecture Design

This architecture accommodates small to medium size businesses ranging between one and 3500 endpoints. Optionally, a front-end server can be placed in the DMZ for publishing policies and/or activating endpoints over the Internet.

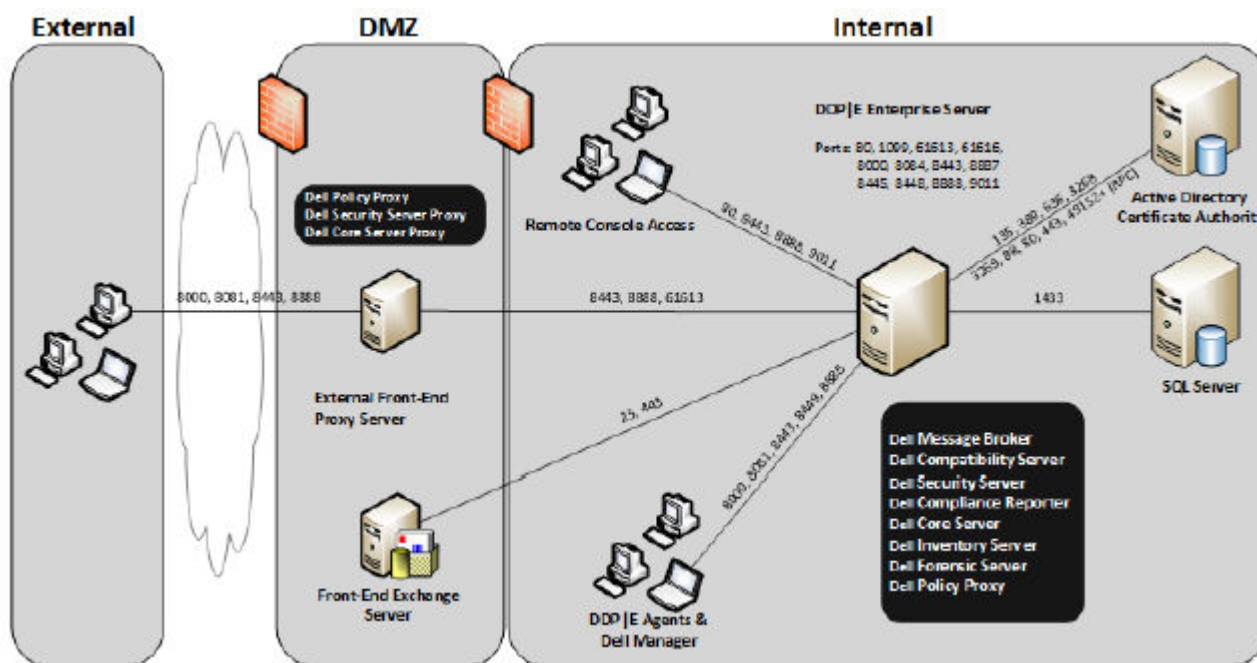
Hardware specifications

- DDP Enterprise Server - Virtual Edition (VE)
- VMware Workstation 11; VMware Workstation 12.5; VMware ESXi 5.5 or ESXi 6.0
- 4 GB RAM with VMware Workstation 11 or VMware Workstation 12.5; 8 GB RAM with ESXi 5.5 or ESXi 6.0
- 80 GB free disk space
- 2+ Ghz processor, Dual Core or greater

For more detailed requirements, see the *DDP Enterprise Server - Virtual Edition Quick Start Guide and Installation Guide*.

Dell External Front-End Server

- Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard or Enterprise Edition/Windows Server 2012 R2 - Standard or Datacenter Edition/Windows Server 2016 - Standard or Datacenter Edition
- 2 GB minimum dedicated RAM/4 GB dedicated RAM recommended
- 1.5 GB free disk space (plus virtual paging space)
- 2 GHz Core Duo or better



Virtual Edition Ports

The following table describes each component and its function.

Name	Default Port	Description	Required For
Compliance Reporter	HTTP(S)/ 8084	Provides an extensive view of the environment for auditing and compliance reporting. A component of the DDP Enterprise Server - VE.	Reporting
Remote Management Console		Administration console and control center for the entire enterprise deployment. A component of the DDP Enterprise Server - VE.	All
Core Server	HTTPS/ 8888	Manages policy flow, licenses, and registration for Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Protection. Processes inventory data for use by Compliance Reporter and the Remote Management Console. Collects and stores authentication data. Controls role-based access. A component of the DDP Enterprise Server - VE.	All
Core Server HA (High Availability)	HTTPS/ 8888	A high-availability service that allows for increased security and performance of HTTPS connections with the Remote Management Console, Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Protection. A component of the DDP Enterprise Server - VE.	All
Security Server	HTTPS/ 8443	Communicates with Policy Proxy; manages forensic key retrievals, activations of clients, Secure Lifecycle products, and SED-PBA communication. A component of the DDP Enterprise Server - VE.	All
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 in this service. A component of the DDP Enterprise Server - VE.	All
Message Broker Service	TCP/ 61616 and STOMP/	Handles communication between services of the DDP Enterprise Server - VE. Stages policy information created by the Compatibility Server for policy proxy queuing. A component of the DDP Enterprise Server - VE.	All



Name	Default Port	Description	Required For
	61613 (closed or, if configured for DMZ, 61613 is open)		
Identity Server	8445	Handles domain authentication requests, including authentication of the SED Manager. Requires an Active Directory account. A component of the DDP Enterprise Server - VE.	All
Forensic Server	HTTPS/ 8448	Allows administrators that have appropriate privileges to get encryption keys from the Remote Management Console for use in data unlocks or decryption tasks. A component of the DDP Enterprise Server - VE.	Forensic API
Inventory Server	8887	Processes the inventory queue. A component of the DDP Enterprise Server - VE.	All
Policy Proxy	TCP/ 8000/8090	Provides a network-based communication path to deliver security policy updates and inventory updates. A component of the DDP Enterprise Server - VE.	Enterprise Edition for Mac Enterprise Edition for Windows Mobile Edition
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.	All
Client Authentication	HTTPS/ 8449	Allows client servers to authenticate against DDP Enterprise Server - VE.	Server Encryption

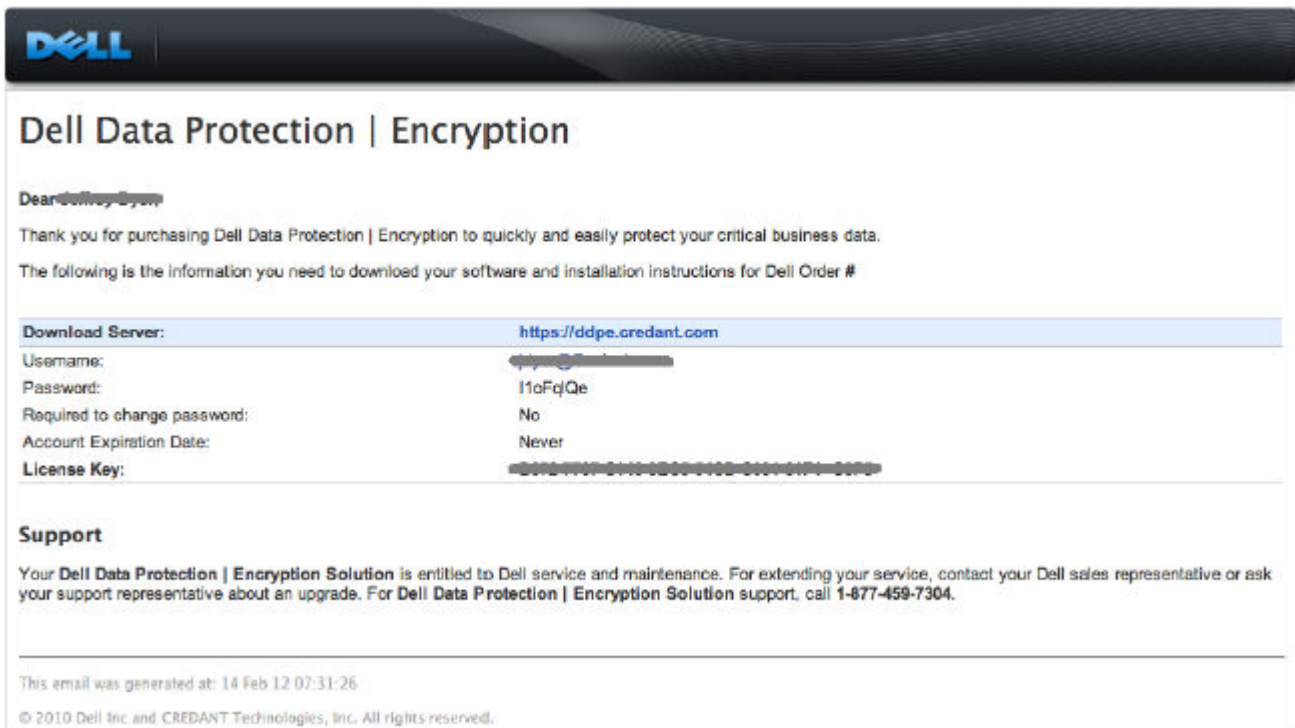


Name	Default Port	Description	Required For
EAS Device Manager		Enables over-the-air functionality. Installed on the Exchange Client Access Server.	Exchange ActiveSync Management of mobile devices.
EAS Mailbox Manager		The mailbox agent that is installed on the Exchange Mailbox Server.	Exchange ActiveSync Management of mobile devices.



Example Customer Notification Email

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



Below is an example of the Dell Data Protection | Endpoint Security Suite email.

