Dell DL1300 Appliance Deployment Guide



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.

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

© **2016 Dell Inc. All rights reserved.** This product is protected by U.S. and international copyright and intellectual property laws. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2016 - 09

Rev. A02

Contents

1 Introducing your Dell DL1300	6
Dell DL1300 core technologies	6
Live Recovery	6
Universal Recovery	6
True Global Deduplication	7
Encryption	7
Dell DL1300 data protection features	7
Dell DL1300 Core	7
Dell DL1300 Smart Agent	
Snapshot process	
Replication — disaster recovery site or service provider	
Recovery	9
Recovery-as-a-Service	9
Virtualization and cloud	9
Dell DL1300 deployment architecture	
Other information you may need	
2 Installing your Dell DL1300	
Introduction	
Available configurations	
Installation overview	
Installation prerequisites	
Network requirements	
Recommended network infrastructure	
Setting up the hardware	
Installing the DL1300 appliance in a rack	
Using the system without a rack	
Cabling the appliance	
Connecting the Cable Management Arm (Optional)	
Turning on the DL1300 Appliance	
Initial software setup	
AppAssure Appliance Configuration Wizard	
DL Appliance Configuration Wizard	
Recovery and Update Utility	
Rapid Appliance Self Recovery	
Creating the RASR USB key	
Executing RASR	

3 Configuring your Dell DL1300	26
Configuration overview	
Configuring browsers to remotely access the DL1300 Core Console	26
Configuring browser settings in Internet Explorer and Chrome	26
Configuring browser settings in Firefox	27
Accessing the DL1300 Core Console	27
Updating trusted sites in Internet Explorer	27
Managing licenses	27
Updating or changing a license	29
Adding a license	
Contacting the Dell Data Protection Rapid Recovery License Portal server	31
Encrypting agent snapshot data	31
Configuring an Email server and Email notification template	32
4 Preparing to protect your servers	34
Overview	34
Installing agents on clients	
Deploying the agent software when protecting an agent	
Installing the Rapid Recovery Agent software on Windows machines	35
Deploying the Rapid Recovery Agent software to one or more machines	37
About installing the Agent software on Linux machines	40
Location of Linux Agent files	42
Agent dependencies	42
Installing the Rapid Recovery Agent software on Debian or Ubuntu	
Installing the Rapid Recovery Agent software on SUSE Linux Enterprise Server	44
Installing the agent on Red Hat Enterprise Linux and CentOS	44
Installing the Agent software on offline Linux machines	
Installing the Agent software on Windows Server Core Edition machines	
Configuring the Rapid Recovery Agent on a Linux machine	
Protecting a machine	48
Checking network connectivity	51
Checking the firewall settings	51
Checking DNS resolution	52
Teaming network adapters	52
Adjusting the number of streams	53
5 Common use cases	54
Protecting machines	54
Snapshots	54
Dell DL1300 Smart Agents	54
Deploying Smart Agents	

Configuring protection jobs	55
Protecting a machine	56
Recovering data	
Recovering directories or files	
Restoring volumes	
Bare Metal Recovery	60
Prerequisites for performing a Bare Metal Restore for a Windows machine	60
Roadmap for performing a Bare Metal Restore for a Windows machine	60
Replicating recovery points	61
Setting up your environment	61
Steps for configuring replication	62
Using virtual standby	63
Performing a one-time Hyper-V export	63
Performing a continuous (virtual standby) Hyper-V export	64
Managing recovery points	65
Archiving data	66
Archiving to a cloud	68
6 Getting help	69
Finding documentation and software updates	
Documentation	69
Software updates	
Contacting Dell	69
Documentation feedback	69

1

Introducing your Dell DL1300

Your Dell DL1300 combines backup and replication into a unified data protection product. It provides reliable application data recovery from your backups to protect virtual machines and physical machines. Your appliance is capable of handling up to terabytes of data with built-in global deduplication, compression, encryption, and replication to specific private or public cloud infrastructure. Server applications and data can be recovered in minutes for data retention and compliance purposes.

Your DL1300 supports multi-hypervisor environments on VMware vSphere, Oracle VirtualBox and Microsoft Hyper-V private and public clouds.

Dell DL1300 core technologies

Your appliance combines the following technologies:

- Live Recovery
- Universal Recovery
- True Global Deduplication
- Encryption

Live Recovery

Live Recovery is instant recovery technology for VMs or servers. It gives you near-continuous access to data volumes on virtual or physical servers.

DL1300 backup and replication technology records concurrent snapshots of multiple VMs or servers, providing near instantaneous data and system protection. You can resume the use of the server by mounting the recovery point without waiting for a full restore to production storage.

Universal Recovery

Universal Recovery provides unlimited machine restoration flexibility. You can restore your backups from physical systems to VMs, VMs to VMs, VMs to physical systems, or physical systems to physical systems, and carry out bare metal restores to dissimilar hardware.

Universal Recovery technology also accelerates cross-platform moves among virtual machines. For example, moving from VMware to Hyper-V or Hyper-V to VMware. It builds in application-level, item-level, and object-level recovery (individual files, folders, email, calendar items, databases, and applications).

True Global Deduplication

True Global Deduplication eliminates redundant or duplicate data by performing incremental block-level backups of the machines.

The typical disk layout of a server consists of the operating system, application, and data. In most environments, the administrators often use a common version of the server and desktop operating system across multiple systems for effective deployment and management. When backup is performed at the block-level across multiple machines, it provides a more granular view of what is in the backup and what is not, irrespective of the source. This data includes the operating system, the applications, and the application data across the environment.



Figure 1. Diagram of True Global Deduplication

Encryption

Your DL1300 provides encryption to protect backups and data-at-rest from unauthorized access and use, ensuring data privacy. The data can be accessed and decrypted using the encryption key. Encryption is performed inline on snapshot data, at line speeds without impacting performance.

Dell DL1300 data protection features

Dell DL1300 Core

The Core is the central component of the DL1300 deployment architecture. The Core stores and manages machine backups and provides services for backup, recovery, retention, replication, archival, and management. The Core is a self-contained network, addressable computer that runs a 64-bit version of Microsoft Windows Server 2012 R2 Foundation and Standard operating systems. The appliance performs target-based inline compression, encryption, and data deduplication of the data received from the agent. The Core then stores the snapshot backups in the repository, which resides on the appliance. Cores are paired for replication.

The repository resides on internal storage within the Core. The Core is managed by accessing the following URL from a JavaScript enabled web browser: https://CORENAME:8006/apprecovery/admin.

Dell DL1300 Smart Agent

The Smart Agent is installed on the core-protected machine. The Smart Agent tracks the changed blocks on the disk volume and then snaps an image of the changed blocks at a predefined interval of protection. The incremental block-level snapshots' forever approach prevents repeated copying of the same data from the protected machine to the Core.

After the agent is configured, it uses smart technology to track the changed blocks on the protected disk volumes. When the snapshot is ready, it is rapidly transferred to the Core using intelligent multi-threaded, socket-based connections.

Snapshot process

Your DL1300 protection process begins when a base image is transferred from a protected machine to the Core. In this phase, full copy of the machine is transported across the network under normal operation, followed by incremental snapshots forever. The DL1300 Agent for Windows uses Microsoft Volume Shadow copy Service (VSS) to freeze and quiesce application data to disk to capture a file-system-consistent and an application-consistent backup. When a snapshot is created, the VSS writer on the target server prevents content from being written to the disk. During the process of halting of writing content to disk, all disk I/O operations are queued and resume only after the snapshot is complete, while the operations in progress will be completed and all open files will be closed. The process of creating a shadow copy does not significantly affect the performance of the production system.

Your DL1300 uses Microsoft VSS because it has built-in support for all Windows internal technologies such as NTFS, Registry, Active Directory, to flush data to disk before the snapshot. Additionally, other enterprise applications, such as Microsoft Exchange and SQL, use VSS Writer plug-ins to get notified when a snapshot is being prepared and when they have to flush their used database pages to disk to bring the database to a consistent transactional state. The captured data is rapidly transferred and stored on the Core.

Replication — disaster recovery site or service provider

Replication is the process of copying recovery points from an Rapid Recovery core and transmitting them to another Rapid Recovery core in a separate location for disaster recovery. The process requires a paired source-target relationship between two or more cores.

The source core copies the recovery points of selected protected machines, and then asynchronously and continually transmits the incremental snapshot data to the target core at a remote disaster recovery site. You can configure outbound replication to a company-owned data center or remote disaster recovery site (that is, a "self-managed" target core). Or, you can configure outbound replication to a third-party managed service provider (MSP) or cloud provider that hosts off-site backup and disaster recovery services. When replicating to a third-party target core, you can use built-in work flows that let you request connections and receive automatic feedback notifications.

Replication is managed on a per-protected-machine basis. Any machine (or all machines) protected or replicated on a source core can be configured to replicate to a target core.

Replication is self-optimizing with a unique Read-Match-Write (RMW) algorithm that is tightly coupled with deduplication. With RMW replication, the source and target replication service matches keys before transferring data and then replicates only the compressed, encrypted, deduplicated data across the WAN, resulting in a 10x reduction in bandwidth requirements.

Replication begins with seeding: the initial transfer of deduplicated base images and incremental snapshots of the protected machines, which can add up to hundreds or thousands of gigabytes of data. Initial replication can be seeded to the target core using external media. This is typically useful for large sets of data or sites with slow links. The data in the seeding archive is compressed, encrypted and deduplicated. If the total size of the archive is larger than the space available on the removable media, the archive can span across multiple devices based on the available space on the media. During the seeding process, the incremental recovery points replicate to the target site. After the target core consumes the seeding archive, the newly replicated incremental recovery points automatically synchronize.

Recovery

Recovery can be performed in the local site or the replicated remote site. After the deployment is in steady state with local protection and optional replication, the DL1300 Core allows you to perform recovery using Verified Recovery, Universal Recovery, or Live Recovery.

Recovery-as-a-Service

Managed Service Providers (MSPs) can fully leverage DL1300 as a platform for delivering Recovery As A Service (RaaS). RaaS facilitates complete recovery-in-the-cloud by replicating customers' physical and virtual servers. The service provider's cloud are used as virtual machines to support recovery testing or actual recovery operations. Customers wanting to perform recovery-in-the-cloud can configure replication on their protected machines on the local cores to an Rapid Recovery service provider. In the event of a disaster, the MSPs can instantly spin-up virtual machines for the customer.

The DL1300 is not multi-tenant. The MSPs can use the DL1300 at multiple sites and create a multi-tenant environment at their end.

Virtualization and cloud

The DL1300 Core is cloud-ready, which allows you to leverage the compute capacity of the cloud for recovery and archive.

DL1300 can export any protected or replicated machine to licensed versions of VMware or Hyper-V. With continuous exports, the virtual machine is incrementally updated after every snapshot. The incremental updates are fast and provide standby-clones that are ready to be powered up with a click of a button. The supported virtual machine exports are:

- VMware Workstation or Server on a folder
- Direct export to a Vsphere or VMware ESXi host
- Export to Oracle VirtualBox
- Microsoft Hyper-V Server on Windows Server 2008 (x64)
- Microsoft Hyper-V Server on Windows Server 2008 R2
- Microsoft Hyper-V Server on Windows Server 2012 R2

You can now archive your repository data to the cloud using platforms such as Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage, or other OpenStack-based cloud services.

Dell DL1300 deployment architecture

Your DL1300 deployment architecture consists of local and remote components. The remote components may be optional for those environments that do not require leveraging a disaster recovery

site or a managed service provider for off-site recovery. A basic local deployment consists of a backup server called the Core and one or more protected machines known as the agents. The off-site component is enabled using replication that provides full recovery capabilities in the disaster recovery site. The DL1300 Core uses base images and incremental snapshots to compile recovery points of protected agents.

Also, DL1300 is application-aware because it can detect the presence of Microsoft Exchange and SQL and their respective databases and log files. Backups are performed by using application-aware block-level snapshots. DL1300 performs log truncation of the protected Microsoft Exchange server.

The following diagram depicts a simple DL1300 deployment. DL1300 Agents are installed on machines such as a file server, email server, database server, or virtual machines are connected to and protected by a single DL1300 Core, which consists of the central repository. The Dell software License Portal manages license subscriptions, groups and users for the agents and cores in your environment. The License Portal allows users to log in, activate accounts, download software, and deploy agents and cores per your license for your environment.



Figure 2. Dell DL1300 Deployment Architecture

You can also deploy multiple DL1300 Cores as shown in the following diagram. A central console manages multiple cores.



Figure 3. DL1300 Multi-Core Deployment Architecture

Other information you may need

NOTE: For all Dell OpenManage documents, go to Dell.com/openmanagemanuals.

l) l)

IJ

NOTE: Always check for updates on **Dell.com/support/home** and read the updates first because they often supersede information in other documents.

NOTE: For any documentation related to Dell OpenManage Server Administrator, see **Dell.com/ openmanage/manuals**.

Your product documentation includes:

Getting Started Guide	Provides an overview of setting up your system, and technical specifications. This document is shipped with your system.
System Placemat	Provides information on how to set up the hardware and install the software on your appliance.
Owner's Manual	Provides information about system features and describes how to troubleshoot the system and install or replace system components.
Deployment Guide	Provides information on hardware deployment and the initial deployment of the appliance.
User's Guide	Provides information about configuring and managing the system.
Release Notes	Provides product information and additional information on the Dell DL1300 Appliance.
Interoperability Guide	Provides information on supported software and hardware for your appliance as well as usage considerations, recommendations, and rules.
OpenManage Server Administrator User's Guide	Provides information about using Dell OpenManage Server Administrator to manage your system.

Installing your Dell DL1300

Introduction

The DL Backup to Disk Appliance allows:

- Faster backups, as well as quicker recovery scenarios over conventional tape devices and backup methodologies
- Optional deduplication capability
- Continuous data protection for data center and remote office servers
- Quick and easy deployment experience that reduces the time required to begin protecting critical data

Available configurations

The DL appliance comes in the following configurations:

Table 1. Available configurations

Capacity	Hardware Configuration
2 TB	Four 4 TB HDDs with 2 TB usable repository space
3 TB with 2 VMs	Four 4 TB HDDs with 3 TB usable repository space and adjustable VM space
4 TB with 2 VMs	Four 4 TB HDDs with 4 TB usable repository space and adjustable VM space

Each configuration includes the following hardware and software:

- Dell DL1300 system
- Dell PowerEdge RAID Controllers (PERC)
- Dell AppAssure software

Installation overview

The DL1300 installation involves installing the AppAssure Core and AppAssure 5 Agent services on the systems that have to be protected. If additional cores are set up then AppAssure 5 Central Management Console Services must be installed.

To install the DL1300 follow these steps:

1. Obtain the permanent license key. From the Core Console, you can manage your DL1300 licenses directly, change the license key, and contact the license server. You can also access the Dell AppAssure License Portal from the Licensing page in the Core Console.

NOTE: The appliance is configured and shipped with a 30 day temporary software license.

- 2. Review installation prerequisites.
- 3. Setting up the hardware.
- 4. Setting up the initial software (AppAssure Appliance Configuration Wizard).
- 5. Installing the Core Management Console.

Installation prerequisites

Network requirements

Your Appliance requires the following network environment:

- Active network with available Ethernet cables and connections
- A static IP address and DNS server IP address, if not provided by the Dynamic Host Configuration
 Protocol (DHCP)
- User name and password with administrator privileges

Recommended network infrastructure

Dell recommends organizations to use switches of 1 GbE or above along with AppAssure for efficient performance.

Setting up the hardware

The appliance ships with a single DL1300 system. Before setting up the appliance hardware, see the *Getting Started Guide* for your system that shipped with the appliance. Unpack and set up the DL1300 Appliance hardware.



NOTE: The software is pre-installed on the appliance. Any media included with the system must be used only in the event of a system recovery.

To set up the DL1300 hardware:

- **1.** Rack and cable the DL1300 system.
- 2. Turn on the DL1300 system.

Installing the DL1300 appliance in a rack

If your system includes a rail kit, locate the *Rack Installation Instructions* supplied with the rack kit. Follow the instructions to install the rails and the DL1300 in the rack.

Using the system without a rack

You can use the system without the server rack. When you are using the system without a rack, ensure that you follow these guidelines:

• The system must be placed on a solid, stable surface that supports the entire system.



NOTE: The system must not be placed vertically.

• Do not place the system on the floor.

- Do not place anything on top of the system. The top panel may deflect under the weight and cause damage to the system.
- Ensure adequate space around the system for proper ventilation.
- Ensure that the system is installed under the recommended temperature conditions as stated in the Technical Specification Environmental Section of *Dell DL1300 Appliance Owner's Manual* at **Dell.com/support/home**.

CAUTION: Failure to follow these guidelines may result in damage to the system or physical injury.



Figure 4. Using the System Without a Rack

Cabling the appliance

Locate the *Dell DL1300 Appliance Getting Started Guide* that is shipped with the appliance and follow the instructions to attach the keyboard, mouse, monitor, power, and network cables to the DL1300 system.

Connecting the Cable Management Arm (Optional)

If the appliance includes a Cable Management Arm (CMA), locate the CMA *Installation Instructions* that shipped with the CMA kit and follow the instructions to install the CMA.

Turning on the DL1300 Appliance

After cabling the appliance, turn on your system.



NOTE: It is recommended that you connect the appliance to an uninterrupted power supply (UPS) for maximum reliability and availability. For more information, see the *Dell DL1300 Getting Started Guide* at **Dell.com/support/manuals**.

Initial software setup

When you turn on the appliance for the first time, and change the system password, the **AppAssure Appliance Configuration wizard** starts automatically.

1. After you turn on the system, choose your operating system language from the Windows language options.

The Microsoft End User License Agreement (EULA) is displayed on the Settings page.

To accept the EULA, click I accept button.
 A page to change the administrator password is displayed.

- 3. Click **OK** on the message that prompts you to change the administrator password.
- Enter and confirm the new password.
 A message prompts you confirming that the password is changed.
- Click OK. After entering the password, Press Ctrl+Alt+Delete to Sign in screen is displayed.
- Log on using the changed administrator password.
 The Select the language for Appliance screen is displayed.
- 7. Select the language for your appliance from the list of supported languages. The **EULA** screen is displayed.
- 8. To accept the EULA, click Accept EULA button.

NOTE: You can run the AppAssure Appliance Configuration Wizard further only if you accept the EULA. Otherwise, the appliance will log you off immediately.

The AppAssure Appliance Configuration wizard welcome screen is displayed.



NOTE: The **AppAssure Appliance Configuration wizard** may take up to 30 seconds to display on the system console.

AppAssure Appliance Configuration Wizard

CAUTION: Make sure you complete all the steps of AppAssure Appliance Configuration Wizard before performing any other task or change any settings on the Appliance. Do not make any changes through the Control Panel, use Microsoft Windows Update, update AppAssure software or install licenses, until the wizard is complete. The Windows update service is disabled temporarily during the configuration process. Exiting the AppAssure Appliance Configuration Wizard before it is complete may cause errors in system operation.

The **AppAssure Appliance Configuration wizard** guides you through the following steps to configure the software on the appliance:

- Configuring the network Interface
- <u>Configuring host name and domain settings</u>
- <u>Configuring SNMP settings</u>

On completing the installation using the wizard, the Core Console launches automatically.

Configuring the network interface

To configure the available network interfaces:

- 1. On the AppAssure Appliance Configuration Wizard Welcome screen, click Next. The network interfaces page displays the available connected network interfaces.
- 2. Select the network interfaces that you want to configure.
 - **NOTE:** The **AppAssure Appliance Configuration wizard** configures network interfaces as individual ports (non-teamed). To improve ingest performance, you can create a larger ingest channel by teaming NICs. However, this must be done after the initial configuration of the appliance.
- 3. If required, connect additional network interfaces and click Refresh.

The additional connected network interfaces are displayed.

4. Click Next.

The Configure selected network interface page is displayed.

 Select the appropriate internet protocol for the selected interface. You can choose IPv4 or IPv6.

The network details are displayed depending on the internet protocol you select.

- 6. To assign the internet protocol details, do one of the following:
 - To assign the selected internet protocol details automatically, select **Obtain an IPV4 address** automatically.
 - To assign the network connection manually, select **Use the following IPv4 address** and enter the following details:
 - IPv4 Address or IPv6 Address
 - Subnet mask for IPv4 and Subnet prefix length for IPv6
 - Default Gateway
- 7. To assign the DNS server details, do one of the following:
 - To assign the DNS server address automatically, select Obtain DNS server address automatically.
 - To assign the DNS server manually, select **Use the following DNS server address** and enter the following details:
 - Preferred DNS sever
 - Alternate DNS server
- 8. Click Next.

The Configure hostname and domain setting page is displayed.

For information on NIC teaming, see Teaming Network Adapters.

Configuring host name and domain settings

You must assign a host name for the appliance. It is recommended that you change the host name before starting backups. By default, the host name is the system name that the operating system assigns.

IJ

NOTE: If you plan to change the host name, it is recommended that you change the host name at this stage. Changing the host name after completing the **AppAssure Appliance Configuration wizard** requires you to perform several steps.

To configure the host name and domain settings:

- 1. On the **Configure host name and domain setting** page, in **New host name** text box enter an appropriate host name.
- 2. If you do not want to connect your appliance to a domain, select **No** in **Do you want this appliance to join a domain?**



NOTE: If your DL1300 is installed with Microsoft Windows Server 2012 Foundation edition, the option to join a domain will be disabled.

By default, **Yes** is selected.

- 3. If you want to connect your appliance to a domain, enter the following details:
 - Domain name
 - Domain user name

NOTE: The domain user must have local administrative rights.

Domain user password

4. Click Next.

NOTE: Changing the host name or the domain requires restarting the machine. After restarting, U the AppAssure Appliance Configuration wizard is launched automatically. If the appliance is connected to a domain, after restarting the machine, you must log in as a domain user with administrative privileges on the appliance.

The **Configure SNMP Settings** page is displayed.

Configuring SNMP settings

Simple Network Management Protocol (SNMP) is a commonly used network management protocol that allows SNMP-compatible management functions such as device discovery, monitoring, and event generation. SNMP provides network management of the TCP/IP protocol.

To configure SNMP alerts for the appliance:

1. On the **Configure SNMP Settings** page, select **Configure SNMP on this appliance**.



NOTE: Deselect **Configure SNMP on this appliance** if you do not want to set up SNMP details and alerts on the appliance and skip to step 6.

- 2. In Communities, enter one or more SNMP community names. Use commas to separate multiple community names.
- 3. In Accept SNMP packets from these hosts, enter the names of hosts with which the appliance can communicate.

Separate the host names with commas, or leave it blank to allow communication with all hosts.

4. To configure SNMP alerts, enter the Community Name and the Trap destinations for the SNMP alerts and click Add.

Repeat this step to add more SNMP addresses.

- 5. To remove a configured SNMP address, in Configured SNMP addresses, select the appropriate SNMP address and click Remove.
- 6. Click Next.

The Thank You page is displayed.

- 7. To complete the configuration, click Next.
- 8. Click Exit on the Configuration Complete page.

The Core console opens on your default web browser.

DL Appliance Configuration Wizard



NOTE: You see the DL Appliance Configuration Wizard only when you upgrade your appliance using the latest RUU.

CAUTION: Make sure you complete all the steps of DL Appliance Configuration Wizard before performing any other task or change any settings on the Appliance. Do not make any changes through the Control Panel, use Microsoft Windows Update, update Rapid Recovery software or install licenses, until the wizard is complete. The Windows update service is disabled temporarily during the configuration process. Exiting the DL Appliance Configuration Wizard before it is complete may cause errors in system operation.

The DL Appliance Configuration wizard guides you through the following steps to configure the software on the appliance:

- <u>Configuring the network Interface</u>
- Registration and Host settings

- Alerts and Monitoring
- <u>Access and Management</u>
- <u>Configuring Windows backup</u>
- <u>Storage provisioning</u>
- <u>Configuring Retention policy and update options</u>

NOTE: After you complete the Appliance configuration, you can either skip the wizard or continue performing **Machine protection**, **Replication**, **Virtual Machine Exports/Standby**. If you choose to skip the wizard, the Core Console launches automatically and you can perform machine protection, replication, and virtual machine Exports at the later stages.

For more information on performing machine protection, replication, and virtual machine Exports see *Rapid Recovery on DL Appliances User's Guide* at **www.dell.com/support/home**.

Configuring the network interface

To configure the available network interfaces:

- On the DL Appliance Configuration Wizard Welcome screen, click Next. The License Agreement page is displayed.
- To accept the agreement, click I accept license agreement, and then click Next. The Network Settings page displays the available connected network interfaces.
- **3.** If necessary, connect extra network interfaces and click **Refresh**. The additional connected network interfaces are displayed.
- **4.** Select the appropriate network interfaces that are suitable for your environment. You have the following options: IPV4 and IPV6.

The network details are displayed depending on the internet protocol you select.

- 5. To enable IPV4, select Enable an IPv4 interface.
 - a. To assign the internet protocol details for IPV4 interface, do one of the following:
 - To assign the selected internet protocol details automatically, select **Obtain an IPV4 address** automatically.
 - To assign the network connection manually, select **Set manually IPV4 address** and enter the following details:
 - IPv4 Address
 - Subnet mask
 - Default Gateway
- 6. To enable IPV6, select Enable an IPv6 interface
 - a. To assign the internet protocol details for IPV6 interface, do one of the following:
 - To assign the selected internet protocol details automatically, select **Obtain an IPV6 address** automatically.
 - To assign the network connection manually, select **Set manually IPV6 address** and enter the following details:
 - IPv6 Address
 - Subnet prefix length
 - Default Gateway
- 7. To enable NIC teaming, select Enable NIC teaming.

For information on NIC teaming, see Teaming Network Adapters.

8. Click Next.

The **Registration** page is displayed.

Registration and Host settings

Register your appliance with the appropriate license key to avail the features accordingly. It is recommended that you change the host name before starting backups. By default, the host name is the system name that the operating system assigns.



NOTE: If you want to change the host name, it is recommended that you change the host name at this stage. Changing the host name after completing the DL Appliance Configuration wizard requires you to perform several steps.

- 1. On the **Registration** page, you must select one of the options below:
 - **Register now** To register your appliance with the purchased license. Enter the following details: license number in the License number text box and the valid email address in the Email address text box
 - Use trial license To register your appliance with the trial license. The trial license expires in 30 days. To continue using the product without interruption, register your appliance within that period.
- 2. Click next.

The Host Settings page is displayed.

- **3.** By default, the Host name of your appliance is displayed in the Host Name box. To change the host name of your appliance, enter appropriate name in the **Host Name** text box.
- **4.** If you want to join your appliance to a domain, select **Join this system to a domain** check box and specify the following information:

Otherwise, go to step 5.

NOTE: Joining to a domain is not possible on Windows Server 2012 R2 Foundation Edition. In this case the **Join this system to a domain** check box is disabled).

Text box	Description
Domain Address	Address of the domain to which you want to add your system
Domain Administrator	Domain Administrator
Password	Password

5. Click Next.

The Alerts and Monitoring page is displayed.

Alerts and Monitoring

To enable alerts for both hardware and software changes you have two options — SNMP and SMTP. Simple Network Management Protocol (SNMP) is a commonly used network management protocol that allows SNMP-compatible management functions such as device discovery, monitoring, and event generation. SNMP provides network management of the TCP/IP protocol. You can use Simple Network Management Protocol (SNMP) or Simple Mail Transfer Protocol (SMTP) to set alerts and monitoring for your appliance.

To receive notifications, configure the options here:



NOTE: It is recommended that you configure alerts. You also have the option to skip configuring alerts, to skip configuring alerts go to step 3.

- 1. You have the following options to enable alerts:
 - To enable system SNMP alerts, select Enable system SNMP alerts.
 - 1. In SNMP Community, enter one or more SNMP community names. Use commas to separate multiple community names.
 - 2. In SNMP Trap destinations, enter trap destinations and click Add.
 - To enable software SNMP alerts, select **Enable software SNMP alerts** option.
 - 1. In SNMP Community, enter one or more SNMP community names. Use commas to separate multiple community names.
 - 2. In SNMP Trap destinations, enter trap destinations and click Add.
- 2. To set software alerts through email, select Notify via email option and enter the valid email address.
- 3. Click Next.

The Access and Management page is displayed.

Access and Management

To access and manage your appliance, you must configure Access and Management settings. To configure the access and management settings of your appliance:

- **1.** On the **Access and Management** page, select or deselect the following options to access and manage your appliance through the following:
 - Enable Remote Desktop
 - Enable Windows Firewall
 - Enable IE Enhanced Security
 - Enable Windows Updates
 - Use Proxy Server
- 2. If you select Use Proxy Server, enter the proxy address in the Proxy address text box and port number in the Port text box.
- 3. NOTE: If you want to set the access and management setting to default options, click **Reset to Default** button.

Click Next.

The Appliance Configuration Backup Options page is displayed.

Configuring Windows backup

U

NOTE: All DL flavors, except DL 1000 support Windows backup feature.

Appliance configuration backup options allows you to set the frequency at which your appliance configuration is backed up. Windows backup data helps in recovering your appliance configuration settings from any of the states before failure.

1. On the **Appliance Configuration Backup Options**, select **Perform Appliance configuration backup**. You have the following options: Daily, Weekly, and Monthly.

2. To set the frequency for Windows backup, select one of the options:

Option	Description
Daily	Backs your configuration settings daily beginning at 12:01 AM

Option	Description
Weekly	Backs your configuration settings every week beginning every Sunday at 12:01 AM
Monthly	Backs your configuration settings every month beginning every Sunday at 12:01 AM

3. Click Next.

The Storage Provisioning page is displayed.

Storage provisioning

Your appliance allows you to provision its internal storage to create Virtual disks (VDs) to host repositories and Virtual Standby, archives or other purposes.

1. On the **Storage Provisioning page**, select the following configuration options for your storage. The Repository Name is displayed as **Repository 1** by default.

NOTE: The size of the repository depends on the license applied during registration of your appliance.

- If you had applied trial license while registering your appliance there is no restriction in the repository size.
- If you had applied purchased license while registering your appliance, the size of the repository corresponds to the model. For example: In DL 1300 2 TB Appliance, repository of size 2 TB is created. You have an option to expand the repository from the **Provisioning** page, by applying the expansion license, for more information see *Rapid Recovery 6.0.1 on DL Appliance User's Guide* at **Dell.com/support/home**.
- If you had applied the purchased expansion license, the size of the repository corresponds to the applied license. For example: In DL1300 2 TB appliance, if the purchased expansion license (1 TB) is applied during registration, the repository of size 3 TB is created.
- 2. Select Allocate a portion of your storage for Virtual Standby, archives, or other purposes.
- **3.** Allocate the percentage of storage space that is available after creating the repository by using the slider. You can also use Size box to specify the exact size.

A virtual disk of specified capacity for hosting virtual standby VMs, archives, other purpose is created.

4. Click Next.

The initial repository is created and the VDs for hosting VMs or other purposes are created.

The Retention Policy page is displayed.

Configuring Retention policy and update options

Retention policies enforce the periods of time in which backups are stored on short-term (fast and expensive) media. Sometimes certain business and technical requirements mandate extended retention of these backups, but use of fast storage is cost prohibitive. In your appliance, retention policies can be customized to specify the length of time a backup recovery point is maintained. As the age of the recovery points approaches the end of their retention period, the recovery points age out and are removed from the retention pool.

NOTE: If the retention policy license restriction is default, the retention policy cannot be configured to set the retention time period greater than six months. If you try to do so, you see an error message.

1. The following options let you define the length of time the backup snapshots of protected machines are stored and modify the rollup process of merging and deleting old backups. The **Retention Policy** page displays the following options:

Text Box	Description
Keep all recovery points for n [retention time period]	Specifies the retention period for the recovery points.
	Enter a number to represent the retention period and then select the time period. The default is 3 days.
	You can choose from: Days, Weeks, Months, or Years
and then keep one recovery point per hour for n [retention time period]	Provides a more granular level of retention. It is used as a building block with the primary setting to further define how long recovery points are maintained.
	Enter a number to represent the retention period and then select the time period. The default is 2 days.
	You can choose from: Days, Weeks, Months, or Years
and then keep one recovery point per day	Provides a more granular level of retention. It is used as a building block to further define how long recovery points are maintained.
for n [retention time period]	Enter a number to represent the retention period and then select the time period. The default is 4 days.
	You can choose from: Days, Weeks, Months, or Years
and then keep one recovery point per week for n [retention time period]	Provides a more granular level of retention. It is used as a building block to further define how long recovery points are maintained.
	Enter a number to represent the retention period and then select the time period. The default is 3 weeks.
	You can choose from: Weeks, Months, or Years
and then keep one recovery point per month for n [retention time period]	Provides a more granular level of retention. It is used as a building block to further define how long recovery points are maintained.
	Enter a number to represent the retention period and then select the time period. The default is 2 months.
	You can choose from: Months or Years
and then keep one recovery point per year	Enter a number to represent the retention period and then select the time period.
for n [retention time period]	You can choose from: Years

Table 2. Schedule options for default retention policy
--

2. Click Next.

The **Update Options** page is displayed.

3. To check for appliance software update, select **Check for appliance software update** option.

If an update exists, it is downloaded and installed upon completion of the wizard.

- **4.** To enable Rapid Recovery Core updates, select **Enable Rapid Recovery Core updates** and then select one of the options below:
 - Notify about updates, but don not install them automatically
 - Automatically install updates
- 5. Click Finish

The appliance settings are applied.

Recovery and Update Utility

The Recovery and Update Utility (RUU) is an all-in-one installer to recover and update DL Appliances (DL1000, DL1300, DL4000 and DL4300) software. It includes the Rapid Recovery Core software and appliance-specific components.

RUU consists of updated versions of the Windows Server Roles and Features, .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator and Rapid Recovery Core Software. In addition, the Recovery and Update Utility also updates the Rapid Appliance Self Recovery (RASR) content.



NOTE: If you are currently using any of the AppAssure Core versions, Rapid Recovery Core version 6.0.2.144 or earlier, RUU forces an update to the most recent version available in the Payload. It is not possible to skip the update and this update is not revertible. If you do not want to upgrade the Core software, do not run the RUU.

To install the most recent version of the RUU:

- 1. Go to the License Portal under the Downloads section or go to **support.dell.com** and download the RUU installer.
- 2. To start the RUU process, run launchRUU.exe file in the RUU package.



Rapid Appliance Self Recovery

Rapid Appliance Self Recovery (RASR) is a bare metal restore process that quickly restores your Appliance to an operating state.

RASR offers two recovery options:

- Restore factory settings
- Recover your appliance to a state just before failure (OS, configurations, and settings are recovered)

Creating the RASR USB key

To create a RASR USB key:

- **1.** Navigate to the **Appliance** tab.
- 2. Using the left pane navigation, select Appliance \rightarrow Backup. Create RASR USB Drive window is displayed.

NOTE: Insert a 16 GB or larger USB key before attempting to create the RASR key.

3. After inserting a 16 GB or larger USB key, click on **Create RASR USB Drive now**. A **Prerequisite Check** message is displayed.

After the prerequisites are checked, **Create the RASR USB Drive** window displays the minimum size required to create the USB drive and **List of Possible target paths**.

4. Select the target and click Create.

A warning dialog box is displayed.

5. Click Yes.

6.

The RASR USB Drive key is created.

NOTE: Make sure to use the Windows Eject Drive function to prepare the USB key for removal. Otherwise, the content in the USB key may be damaged and the USB key doesn't work as expected.

Remove the RASR USB key created for each DL Appliance, label, and store for future use.

Executing RASR

NOTE: Dell recommends you to create a RASR USB key after you have set up the appliance. To create RASR USB key, see <u>Creating the RASR USB Key</u> section.

NOTE: Ensure that you have the latest RUU available and reachable on your appliance.



IJ

NOTE: To perform system recovery using RASR, see *Recovering a Dell*TM *DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR)* document at **Dell.com/support/home**.

To perform a factory reset:

- **1.** Insert the RASR USB key created.
- 2. Restart the appliance and select Boot Manager (F11).
- 3. In the Boot Manager Main Menu, select One-shot BIOS Boot Menu.
- 4. In the Boot Manager Boot Menu, select the attached USB drive.
- 5. Select your keyboard layout.
- 6. Click Troubleshoot \rightarrow Rapid Appliance Self Recovery.
- 7. Select the target operating system (OS).

RASR is launched and **welcome** screen is displayed.

8. Click Next.

The **Prerequisites** check screen is displayed.

NOTE: Ensure all the hardware and other prerequisites are checked before performing the RASR.

9. Click Next.

The Recovery Mode Selection screen is displayed with three options:

- System Recovery
- Windows Recovery Wizard
- Factory Reset
- **10.** Select the **Factory Reset** option.

This option will recover the operating system disk from the factory image.

11. Click Next.

The following warning message is displayed in a dialog box: This operation will recover the operating system. All OS disk data will be overwritten.

12. Click Yes.

The operating system disk starts restoring back to factory reset.

- 13. The RASR Completed page is displayed on completion of the recovery process. Click Finish.
- 14. Boot the system after restore.
- **15. NOTE:** Continue further only if you see the **AppAssure Appliance Configuration Wizard**, otherwise go to **Step 17**.

Wait for AppAssure Appliance Configuration Wizard to load, you need to close it. Close the wizard using the Windows Task Manager.

- **16.** Run **launchRUU.exe** file in the RUU package. Follow the instructions and select the option to continue with RUU installation and complete the RUU installation.
- **17.** The **DL Appliance Configuration Wizard launches** and will guide you through the rest of the restore process.

Your appliance operates normally now.

Configuring your Dell DL1300

Configuration overview

Configuration includes tasks such as configuring browsers to remotely access the DL1300 Core Console, managing licenses, and setting up alerts and notifications. After you complete the configuration of the Core, you can then protect agents and perform recovery.



NOTE: While using the DL1300 Backup To Disk Appliance, it is recommended that you use the **Appliance** tab to configure the Core.

Configuring browsers to remotely access the DL1300 Core Console

Before you can successfully access the Core Console from a remote machine, you must modify your browser's settings. The following procedures detail how to modify Internet Explorer, Google Chrome, and Mozilla Firefox browser settings.



NOTE: To modify browser settings, you must be logged on to the machine with administrator privileges.



NOTE: Because Chrome uses Internet Explorer settings, you must make the changes for Chrome using Internet Explorer.



NOTE: Ensure that the Internet Explorer Enhanced Security Configuration is turned on when you access the Core Web Console either locally or remotely. To turn on the Internet Explorer Enhanced Security Configuration, open **Server Manager** \rightarrow **Local Server** \rightarrow **IE Enhanced Security Configuration** option is displayed, ensure that it is **On**.

Configuring browser settings in Internet Explorer and Chrome

To configure browser settings in Internet Explorer and Chrome:

- 1. From the Internet Options screen, select the Security tab.
- 2. Click Trusted Sites and then click Sites.
- **3.** Deselect the option **Require server verification (https:) for all sites in the zone**, and then add http://<hostname or IP Address of the Appliance server hosting the AppAssure 5 Core> to **Trusted Sites**.
- 4. Click Close, select Trusted Sites, and then click Custom Level.
- 5. Scroll to Miscellaneous -> Display Mixed Content and select Enable.
- 6. Scroll to the bottom of the screen to User Authentication → Logon, and then select Automatic logon with current user name and password.
- 7. Click OK, and then select the Advanced tab.
- 8. Scroll to Multimedia and select Play animations in webpages.
- 9. Scroll to Security, check Enable Integrated Windows Authentication, and then click OK.

Configuring browser settings in Firefox

To modify browser settings in Firefox:

- 1. In the Firefox address bar, type **about:config**, and then click **I'll be careful**, **I promise** if prompted.
- Search for the term ntlm.
 The search should return at least three results.
- **3.** Double-click **network.automatic-ntlm-auth.trusted-uris** and enter the following setting as appropriate for your machine:
 - For local machines, enter the host name.
 - For remote machines, enter the host name or IP address separated by a comma of the appliance system hosting the Core; for example, *IP Address, host name*.
- 4. Restart Firefox.

Accessing the DL1300 Core Console

Ensure that you update trusted sites as discussed in the topic <u>Updating Trusted Sites In Internet Explorer</u>, and configure your browsers as discussed in the topic <u>Configuring browsers to remotely access the</u> <u>DL1300 Core Console</u>. After you update trusted sites in Internet Explorer, and configure your browsers, perform one of the following to access the Core Console:

- Log on locally to your Core server, and then double-click the Core Console icon.
- Type one of the following URLs in your web browser:
 - https://<yourCoreServerName>:8006/apprecovery/admin/core
 - https://<yourCoreServerIPaddress>:8006/apprecovery/admin/core

Updating trusted sites in Internet Explorer

To update the trusted sites in Internet Explorer:

- 1. Open Internet Explorer.
- 2. If the File, Edit View, and other menus are not displayed, press <F10>.
- 3. Click the Tools menu, and select Internet Options.
- 4. In the Internet Options window, click the Security tab.
- 5. Click Trusted Sites and then click Sites.
- 6. In Add this website to the zone, enter https://[Display Name], using the new name you provided for the Display Name.
- 7. Click Add.
- 8. In Add this website to the zone, enter about:blank.
- 9. Click Add.
- 10. Click Close and then OK.

Managing licenses

Many Rapid Recovery Core users start with a trial license, which has limited capabilities. A trial license is valid for 14 days, and can be extended one time by the group administrator to a 28-day license. Once the

trial period expires, the Rapid Recovery Core stops taking snapshots until you obtain and register a valid non-trial license.



NOTE: For information about entering license key or file information (for example, to update or change a trial license to a valid long-term license), see <u>Updating or changing a license</u>.

Licenses are validated using license files or license keys.

License files are text files that end with the **.lic** file extension. Examples of license files include the following:

- License files can appear as nine characters in length, consisting of three groups of Arabic numbers, each separated by a hyphen; for example, 123-456-789.lic.
- Software-based licenses can appear in the format Software-<Group name>.lic, with the group named after the customer name or account; for example, Software-YourCompany.lic.
- Dell appliance licenses can appear in the format <Appliance Series>-<Group name>.lic, with the group named after customer name account; for example, DL4X00 Series-YourCompany.lic.

License keys are 30 characters in length, consisting of six groups of English alphanumeric characters, each separated by a hyphen. For example, a sample license key format is ABC12-DEF3G-H45IJ-6K78L-9MN10-OPQ11.

Rapid Recovery lets you manage licenses or contact the license server directly from the Core Console by

selecting **Licensing**. (Settings) from the icon bar and clicking **Licensing**.

The Licensing settings include the following information:

License Details:

- Change License. Lets you change an existing license associated with the Core by uploading a license file or entering a license key.
- Add License. This option is available only for Dell backup appliances and lets you upload a license file or entering a license key.
- Z License Portal Group. This option opens the license portal for group management.
- License type. Types of licenses include Trial, Subscription, or Enterprise. For more information, see the topic About Dell Data Protection | Rapid Recovery License Portal Software License Types in the Dell Data Protection | Rapid Recovery License Portal User Guide.
- License status. Indicates the status of the license. An active status ensures snapshots can continue as scheduled. If the license is blocked, or expired, or if the Core has not been able to communicate with the Dell Data Protection | Rapid Recovery License Portal past the grace period, snapshots are paused until the license status is corrected.

License Constraints:

• Maximum snapshots per day. Indicates the number of backups that are limited by the specific license.

License Pool:

• **Pool size**. The license pool is the number of non-trial licenses available to allocate across groups and subgroups in the Dell Data Protection | Rapid Recovery License Portal. The size of the pool determines how many licenses can be allocated. For more information, see the topic "Understanding License Pools" in the *Dell Data Protection* | *Rapid Recovery License Portal User Guide*.

- **Protected by this Core**. Indicates the number of machines from the license pool that are protected by this core.
- **Total protected in group**. Indicates the total number of machines protected within the same license group as this Core.

License Server. These settings apply to standard (phone home) licenses. These settings are not applicable for appliances and other non-phone-home licenses:

- License server address. Displays an active URL for the license server associated with this Core.
- Last response from the licensing server. Indicates whether the last attempted communication with the license server portal was successful.
- Last contact with licensing server. Displays the date and time of the last successful contact with the licensing server.
- Next attempt to contact the licensing server. Indicates the next scheduled date and time to attempt communication with the licensing server.
- **Contact Now**. This button contacts the license server on demand. Use this option after making changes to your license configuration, to register changes immediately rather than waiting for the next scheduled attempt.

For more information on licenses, see the *Dell Data Protection* | *Rapid Recovery License Portal User Guide*.

For more information on adding or changing a license key or file, see Updating or changing a license.

For more information on contacting the license portal server, see <u>Contacting the Dell Data Protection</u> <u>Rapid Recovery License Portal server</u>

Updating or changing a license

After you upgrade or purchase a long-term Rapid Recovery license, you receive by email either a license file or a license key.

Complete the steps in this procedure to upgrade your trial license or change your existing license, and associate it with the Rapid Recovery Core Console.



NOTE: Users of Dell backup appliances can also add licenses to the Core if necessary. For more information, see <u>Adding a license</u>.

For information about obtaining a license key, or for details about using the license portal to download software, register appliances, manage license subscriptions and license groups, and generate license portal reports, see the *Dell Data Protection* | *Rapid Recovery License Portal User Guide*.

If you just installed a new Core, and are being asked to choose a license file or key, skip to Step 5.

- 1. Navigate to the Rapid Recovery Core Console.
- 2. On the icon bar, click (Settings).
- **3.** Scroll down on the right side of the **Settings** page until you can see the Licensing heading. The Core settings for licensing appear.
- 4. To update or change the existing license associated with your Core, at the top of the License Details

core settings area, click **Change License**.

The **Change License** dialog box appears.

- 5. To enter a license key or upload a license file, do one of the following:
 - If you want to *manually enter* the license key, in the Change License dialog box, type the key carefully, and then click **Continue**.
 The dialog box closes and the license file you selected is authenticated, and that license is

The dialog box closes, and the license file you selected is authenticated, and that license is associated with your Core.

- b. If you want to upload a license file, in the Change License dialog box, click Choose File.
 In the File Upload dialog box, navigate through the file system and locate the new license file you want to use. For example, locate Software-YourCompany.lic.
- c. Click the license file, and then click **Open**.
 The File Upload dialog box closes. The selected license file appears in the Change License dialog box.
- d. In the **Change License** dialog box, click **Continue**.

The dialog box closes, and the license file you selected is authenticated, and that license is associated with your Core.

- **6.** Scroll down on the right side of the Settings page until you can see the License Server heading. The Licensing core settings appear.
- 7. In the License Server area, click **Contact Now**.

Once the license is applied to the license server, any associated protected machines automatically update with the new license.

Adding a license

Dell backup appliance owners can add one or more licenses to the Rapid Recovery Core Console.

Once you have upgraded or purchased your Rapid Recovery license, you receive by email either a license file or a license key.

You can also update or change an existing license on the Core Console. For more information, see <u>Updating or changing a license</u>.



NOTE: Only Dell backup appliance users see the Add Appliance button.



NOTE: For information about obtaining a license key, see the *Dell Data Protection* | *Rapid Recovery License Portal User Guide*.

- 1. Navigate to the Rapid Recovery Core Console.
- 2. On the icon bar, click (Settings).
- **3.** Scroll down on the right side of the Settings page until you can see the Licensing heading. The Core settings for licensing appear.
- **4.** To add a license and associate it with your Core, at the top of the License Details core settings area, click **Add License. In** the **Add License** dialog box, do one of the following:
 - a. If you want to *manually enter* the license key, in the Change License dialog box, type the key carefully, and then click **Continue**.

The dialog box closes, and the license file you selected is authenticated, and that license is associated with your Core.

b. If you want to upload a license file, in the Change License dialog box, click Choose File.

In the **File Upload** dialog box, navigate through the file system and locate the new license file you want to use. For example, locate <code>Software-YourCompany.lic</code>.

- c. Click the license file, and then click **Open**.
 The File Upload dialog box closes. The selected license file appears in the Change License dialog box.
- In the Change License dialog box, click Continue.
 The dialog box closes, and the license file you selected is authenticated, and that license is associated with your Core.
- **5.** Scroll down on the right side of the Settings page until you can see the License Server heading. The Licensing core settings appear.
- 6. In the License Server area, click Contact Now.

Once the license is applied to the license server, any associated protected machines automatically update with the new license.

Contacting the Dell Data Protection | Rapid Recovery License Portal server

The Rapid Recovery Core Console frequently contacts the portal server to remain current with any changes made in the Dell Data Protection | Rapid Recovery License Portal.

For non-trial licenses, the Rapid Recovery Core contacts the license portal once every hour. If the Core cannot reach the license portal after a 10-day grace period, the Core stops taking snapshots.

Typically, communication with the license portal server occurs automatically at designated intervals; however, you can initiate communication on-demand.

Complete the steps in this procedure to contact the license portal server.

- 1. Navigate to the Rapid Recovery Core Console.
- 2. On the icon bar, click **Settings**, and then scroll down on the right side of the **Settings** page until you can see the License Server heading.
- **3.** From the License Server area, click **Contact Now**.

Encrypting agent snapshot data

The Core can encrypt agent snapshot data within the repository. Instead of encrypting the entire repository, DL1300 allows you to specify an encryption key during the protection of an agent in a repository which allows the key to be reused for different agents.

To encrypt agent snapshot data:

- **1.** From the Core, click **Configuration** \rightarrow **Manage** \rightarrow **Security**.
- 2. Click Actions, and then click Add Encryption Key.
 - The **Create Encryption Key** page id displayed.
- **3.** Complete the following information:

Field	Description
Name	Enter a name for the encryption key.
Comment	Enter a comment for the encryption key. It is used to provide extra details about the encryption key.

Field	Description
Passphrase	Enter a passphrase. It is used to control access.
Confirm Passphrase	Re-enter the passphrase. It is used to confirm the passphrase entry.

NOTE: It is recommended that you record the encryption passphrase, as losing the passphrase makes the data inaccessible. For more information, see Managing Security chapter in the *Dell DL1300 Appliance User's Guide*.

Configuring an Email server and Email notification template

If you want to receive email notifications about events, configure an email server and an email notification template.



NOTE: You must also configure notification group settings, including enabling the **Notify by email** option, before email alert messages are sent. For more information on specifying events to receive email alerts, see Configuring Notification Groups For System Events in the *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.

To configure an email server and email notification template:

- 1. From the Core, select the **Configuration** tab.
- 2. From the Manage option, click Events.
- In the Email SMTP Settings pane, click Change.
 The Edit Email Notification Configuration dialog box is displayed.
- 4. Select Enable Email Notifications, and then enter details for the email server described as follows:

Text Box	Description
SMTP Server	Enter the name of the email server to be used by the email notification template. The naming convention includes the host name, domain, and suffix; for example, smtp.gmail.com .
Port	Enter a port number. It is used to identify the port for the email server; for example, the port 587 for Gmail. The default is 25.
Timeout (seconds)	To specify how long to try a connection before timing out, enter an integer value. It is used to establish the time in seconds when trying to connect to the email server before a time-out occurs. The default is 30 seconds.
TLS	Select this option if the mail server uses a secure connection such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL).
Username	Enter a user name for the email server.
Password	Enter a password for accessing the email server.

Text Box	Description
From	Enter a return email address. It is used to specify the return email address for the email notification template; for example, noreply@localhost.com .
Email Subject	Enter a subject for the email template. It is used to define the subject of the email notification template; for example, <hostname> - <level> <name>.</name></level></hostname>
Email	Enter information for the body of the template that describes the event, when it occurred, and the severity.

- 5. Click Send Test Email and review the results.
- 6. After you are satisfied with the results of the tests, click **OK**.

Preparing to protect your servers

Overview

To protect your data using DL 1300, you need to add the workstations and servers for protection in the Core Console; for example, your Exchange server, SQL Server, your Linux server, and so on.

In the Core Console, you can identify the machine on which an Agent is installed and specify which volumes, for example, a Microsoft Windows Storage Space, to protect. You can define the schedules for protection, add additional security measures such as encryption, and much more. For more information on how to access the Core Console to protect workstations and servers, see <u>Protecting a machine</u>.

Installing agents on clients

Each client that is backed up by the AppAssure appliance must have the AppAssure agent installed. The AppAssure Core console enables you to deploy agents to machines. Deploying agents to machines requires pre-configuring settings to select a single type of agent to push to clients. This method works well if all clients are running the same operating system. However, if there are different versions of operating systems, you may find it easier to install the agents on the machines.

You can also deploy the Agent software to the agent machine during the process of protecting a machine. This option is available for machines that do not already have the Agent software installed. For more information on deploying the Agent software while protecting a machine, see the *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.

Deploying the agent software when protecting an agent

You can download and deploy agents during the process of adding an agent for protection.

U

NOTE: This procedure is not required if you have already installed the Agent software on a machine that you want to protect.

If the Agent software is not installed prior to protecting a machine, you will not be able to select specific volumes for protection as part of this wizard. In this case, by default, all volumes on the agent machine will be included for protection.

Rapid Recovery supports the protection and recovery of machines configured with EISA partitions. Support is also extended to Windows 8 and 8.1, and Windows 2012 and 2012 R2 machines that use Windows Recovery Environment (Windows RE).

- **1.** Do one of the following:
 - If you are starting from the Protect Machine Wizard, proceed to Step 2...
 - If you are starting from the Rapid Recovery Core Console, from the button bar, click **Protect**.

The Protect Machine Wizard appears.

- 2. On the **Welcome** page, select the appropriate installation options:
 - If you do not need to define a repository or establish encryption, select Typical.
 - If you need to create a repository, or define a different repository for backups for the selected machine, or if you want to establish encryption using the wizard, select **Advanced (show optional steps)**.
 - Optionally, if you do not wish to see the **Welcome** page for the Protect Machine Wizard in the future, select the option **Skip this Welcome page the next time the wizard opens**.
- 3. When you are satisfied with your choices on the Welcome page, then click Next.

The **Connection** page appears.

4. On the **Connection** page, enter the information about the machine to which you want to connect as described in the following table, and then click **Next**.

Text Box	Description
Host	The host name or IP address of the machine that you want to protect.
Port	The port number on which the Rapid Recovery Core communicates with the Agent on the machine. The default port number is 8006.
User name	The user name used to connect to this machine; for example, Administrator (or, if the machine is in a domain, [domain name]\Administrator).
Password	The password used to connect to this machine.

Table 3. Machine connection settings

If the **Install Agent** page appears next in the Protect Machine Wizard, that means that Rapid Recovery does not detect the Rapid Recovery Agent on the machine and will install the current version of the software.

5. **NOTE:** The Agent software must be installed on the machine you want to protect, and that machine must be restarted, before it can back up to the Core. To have the installer reboot the protected machine, select the option **After installation, restart the machine automatically** (recommended) before clicking Next.

Click Next.

Installing the Rapid Recovery Agent software on Windows machines

Deploy the Rapid Recovery Agent installer file to the machine you want to protect using one of the methods described in the topic "Installing the Rapid Recovery Agent software" in the *Dell Data Protection* | *Rapid Recovery 6.0 Installation and Upgrade Guide.* Then launch the installer program as described below to install or upgrade the software on each Windows machine you want to protect in the Rapid Recovery Core.



NOTE: You must run the installer with local administrator privileges.

1. From the machine you want to protect, double-click on the executable Rapid Recovery Agent installer file to start the installer.

Depending on the configuration of your machine, the User Account Control window or the Open File - Security Warning window could appear.

2. If prompted for permission, confirm that you want to run the installer and make changes to the system.

- **3.** If .NET components are missing or need to be upgraded, accept the prompts to download and install the framework.
- 4. In the language field, select the appropriate language and then click **OK**.
- 5. Choose from one of the following:
 - If this is the first time the Rapid Recovery Agent software is being installed on this machine, the installer prepares the installation, and then the Rapid Recovery Agent Installation Wizard appears. Proceed to Step 6.
 - If this machine has an earlier version of the AppAssure Agent or Rapid Recovery Agent software installed, you will see a message asking if you want to upgrade to the current version.
 - 1. Click Yes.

The Rapid Recovery Agent Installation Wizard appears, showing the **Progress** page of the wizard. The application downloads to the destination folder, with progress displayed in the progress bar. When finished, the wizard automatically advances to the **Completed** page.

- 2. Skip to Step 12.
- 6. In the Rapid Recovery Agent Installation Wizard, on the **Welcome** page, click **Next** to continue with the installation.

The License Agreement page appears.

7. On the License Agreement page, click I accept the terms in the license agreement, and then click Next.

The **Prerequisites** page appears.

- 8. The Rapid Recovery Agent Installer verifies the existence of the prerequisite files.
 - If the prerequisite files exist, a message appears indicating that all prerequisites are installed on the machine.
 - If the prerequisite files do not exist, the Rapid Recovery Agent Installer identifies which files are needed and displays the results accordingly; for example, CRT 2013 (x64) ENU (distributable code for Microsoft Visual Studio[®]), or Microsoft System CLR Types for SQL Server 2008 R2 (x64). Click Install Prerequisites.
- 9. When the installation of the prerequisite files is completed, click Next.

The Installation Options page appears.

- **10.** On the **Installation Options** page, review the installation options. If necessary, modify them as described below.
 - In the **Destination Folder** text field, review the destination folder for the installation. If you want to change the location, do the following:
 - Click the folder icon.
 - In the Browse to Destination Folder dialog box, select a new location.
 - Click OK.
 - In the **Port Number** text field, enter a port number to use for communication between the Agent software on the protected machine and the Rapid Recovery Core.



NOTE: The default value is 8006. If you change the port number, be sure to make note of it in the event that you need to adjust configuration settings at a later time.

- Select Allow Agent to automatically send diagnostic and usage information to Dell Inc. to send diagnostic and usage information to Dell. If you do not want to send this information, clear this option.
- 11. Once you are satisfied with the installation options, click Install.

The **Progress** page appears, and includes a status bar that lets you monitor the progress of the installation.

When the installation is complete, the **Completed** page appears. Skip to Step 12. .

- **12.** On the **Completed** page, if you see a message indicating that the system must be restarted before the installation takes effect, perform one of the following steps:
 - To restart now, select Yes, I want to restart my computer now.
 - To restart later, clear the Yes, I want to restart my computer now option.
- **13.** On the **Completed** page, click **Finish**.

The installer wizard closes, and the Agent installation is complete.

Deploying the Rapid Recovery Agent software to one or more machines

You can simplify the task of deploying the Rapid Recovery Agent software to one or more Windows machines by using the Deploy Agent Software Wizard.



NOTE: In the past, this feature was referred to as "bulk deploy."

When you use the Deploy Agent Software Wizard, Rapid Recovery can automatically detect machines on a host and let you select the machines to which you want to deploy. For machines on domains or hosts other than Active Directory or vCenter or ESX(i), you can manually connect to individual machines by using their IP addresses and the appropriate credentials. You can also push upgrades of the software to machines that the local Rapid Recovery Core already protects.

From within the Core Console, you can complete any of the following tasks:

- Deploying to machines on an Active Directory domain
- Deploying to machines on a VMware vCenter/ESX(i) virtual host

NOTE: Dell recommends limiting the number of machines to which you deploy simultaneously to 50 or fewer, to preclude experiencing resource constraints that may cause the deploy operation to fail.

Installing Microsoft Windows agents at the client

To install the agents:

- **1.** Verify that the client has the Microsoft .NET 4 framework installed:
 - a. On the client, start the Windows Server Manager.
 - b. Click Configuration \rightarrow Services.
 - c. Ensure that Microsoft .NET Framework appears in the list of services. If it is not installed, you can get a copy from **microsoft.com**.
- 2. Install the agent:
 - a. On the AppAssure appliance, share the directory **C:\install\AppAssure** to the client(s) you plan to back up.
 - b. On the client system, map a drive to C:\install\AppAssure on the AppAssure appliance.
 - c. On the client system, open the **C:\install\AppAssure** directory and double-click the correct agent for the client system to begin the installation.

Deploying to machines on an Active Directory domain

Use this procedure to simultaneously deploy the Rapid Recovery Agent software to one or more machines on an Active Directory domain.

Before you begin this procedure, have the domain information and logon credentials for the Active Directory server on hand.

1. On the Rapid Recovery Core Console, click the **Protect** drop-down menu, and then click **Deploy Agent Software**.

The Deploy Agent Software Wizard opens.

- 2. On the Connection page of the wizard, from the Source drop-down list, select Active Directory.
- 3. Enter the domain information and logon credentials as described in the following table.

Table 4. Domain information and credentials

Text Box	Description
Host	The host name or IP address of the Active Directory domain.
User name	The user name used to connect to the domain; for example, Administrator or, if the machine is in a domain, [domain name]\Administrator).
Password	The secure password used to connect to the domain.

- 4. Click Next.
- 5. On the **Machines** page, select the machines to which you want to deploy the Rapid Recovery Agent software.
- 6. Optionally, to automatically restart the protected machines after the Agent is installed, select After Agent installation, restart the machines automatically (Recommended).

7. Click Finish.

The system automatically verifies each machine that you selected.

If Rapid Recovery detects any concerns during automatic verification, the wizard progresses to a Warnings page, where you can clear machines from selection and manually verify the selected machines. If the machines you added pass the automatic verification, they appear on the Deploy Agent to Machines pane.

8. If the Warning page appeared and you are still satisfied with your selections, click Finish again.

The Rapid Recovery Agent software deploys to the specified machines. The machines are not yet protected. To protect machines, see the topic "Protecting multiple machines on the Active Directory domain" in the *Rapid Recovery 6.0 on DL Appliances User's Guide*.

Deploying to machines on a VMware vCenter/ESX(i) virtual host

Use this procedure to simultaneously deploy the Rapid Recovery Agent software to one or more machines on a VMware vCenter/ESX(i) virtual host.

Before starting this procedure, you must have the following information:

- Logon credentials for the VMware vCenter/ESX(i) virtual host.
- Host location.
- Logon credentials for each machine you want to protect.

- NOTE: All virtual machines must have VMware Tools installed; otherwise, Rapid Recovery cannot IJ detect the host name of the virtual machine to which to deploy. In lieu of the host name, Rapid Recovery uses the virtual machine name, which may cause issues if the host name is different from the virtual machine name.
- 1. On the Rapid Recovery Core Console, click the **Protect** drop-down menu, and then click **Deploy** Agent Software.

The Deploy Agent Software Wizard opens.

- 2. On the Connection page of the wizard, from the Source drop-down list, select vCenter / ESX(i).
- 3. Enter the host information and logon credentials as described in the following table.

Table 5. vCenter/ESX(i) connection settings

Text Box	Description
Host	The name or IP address of the VMware vCenter Server/ESX(i) virtual host.
Port	The port used to connect to the virtual host. The default setting is 443.
User name	The user name used to connect to the virtual host; for example, Administrator or, if the machine is in a domain, [domain name]\Administrator.
Password	The secure password used to connect to this virtual host.

- 4. Click Next
- 5. On the **Machines** page of the wizard, select one of the following options from the drop-down menu:
 - Hosts and Clusters
 - VMs and Templates
- 6. Expand the list of machines, and then select the VMs to which you want to deploy the software. A notification appears if Rapid Recovery detects that a machine is offline or that VMware Tools are not installed.
- 7. If you want to restart the machines automatically after deployment, select After Agent installation, restart the machines automatically (Recommended).
- 8. Click Next.

Rapid Recovery automatically verifies each machine you selected.

9. On the Adjustments page of the wizard, enter the credentials for each machine in the following format: hostname::username::password.



NOTE: Enter one machine on each line.

10. Click Finish.

The system automatically verifies each machine that you selected.

If Rapid Recovery detects any concerns during automatic verification, the wizard progresses to a Warnings page, where you can clear machines from selection and manually verify the selected machines. If the machines you added pass the automatic verification, they appear on the Deploy Agent to Machines pane.

11. If the Warning page appeared and you are still satisfied with your selections, click **Finish** again.

The Rapid Recovery Agent software deploys to the specified machines.

About installing the Agent software on Linux machines

When installing the Agent software on Linux machines that you want to protect, use the following guidance. After installation is complete, configure the Agent as described in the topic "Configuring the Rapid Recovery Agent on a Linux machine" in the *Dell Data Protection* | *Rapid Recovery 6.0 Installation and Upgrade Guide*.

CAUTION: After configuring the newly installed Agent software on a Linux machine, restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.

The method for installing and removing the Agent software on Linux machines has changed. As of release 6.0.1, the following factors apply:

• One set of instructions applies to installations of Agent on a Linux machine with current access to the Internet. This is referred to as online installation. Instead of using shell scripts, package managers are used to install or remove the Rapid Recovery software from a repository referenced on the local Linux machine.



NOTE: The repository is used for staging of files for the relevant package managers. This repository is not related to the Rapid Recovery repository.

 If installing Agent on a Linux machine with no access to the Internet (such as an air-gapped or secured standalone machine), this is referred to as offline installation. For this process, you must first download an installation package from a Linux machine with Internet access, and then move those installation files to the secured computer for installation.

Because the various supported Linux distributions use different package managers for online installation, the procedure for installing, upgrading, or removing Agent on any supported Linux OS depends on the package manager used. The package managers, and the Linux distributions they support, are described in the following table.

Package Manager	Linux Distribution
yum	Linux distributions based on Red Hat Enterprise Linux (RHEL), including RHEL, CentOS, and Oracle Linux.
zypper	SUSE Linux Enterprise Server (SLES) versions 11, 12
apt	Linux distributions based on Debian, including Debian 7 or 8, and Ubuntu 12.04 and later

Table 6. Package managers and the Linux distributions they support

As a one-time setup step for each Linux machine, you must configure your local software repository to point to the location where the package manager obtains Dell Rapid Recovery installation files.



NOTE: This process is represented by steps 1 through 4 in each of the installation procedures. When upgrading future editions of the Rapid Recovery Agent on a Linux machine with the repository configured, you will not need to perform these steps.

After you configure a software repository on your Linux machine, the package manager is able to retrieve and install the packages needed for installation or removal of Rapid Recovery Agent software and related components, such as aamount (now called local mount), aavdisk (now called rapidrecovery-vdisk), and

Mono (an open source, Ecma standard-compliant, .NET Framework-compatible tool set used for porting the Agent software to Linux platforms).

For each package manager, you can run the appropriate command at the command line to determine if it is configured to download Rapid Recovery packages. These commands are listed in the following table.

Package Manager	Command to list configured repositories
yum	yum replolist
zypper	zypper repos
apt	ls /etc/apt/sources.list.d

Table 7. Command to show package manager repository configuration

Previous versions of the AppAssure Agent software must be completely removed from a Linux machine before installing the Rapid Recovery Agent version and protecting the Linux machine using the Rapid Recovery Core. This is true for online or offline installations. Removing AppAssure Agent employs the use of shell scripts. The uninstall instructions differ, depending on the Linux distribution you are using. For more information on uninstalling AppAssure Agent from a Linux machine, see the topic "Uninstalling the AppAssure Agent software from a Linux machine" in the *Dell Data Protection* | *Rapid Recovery 6.0 Installation and Upgrade Guide*.

Ű

NOTE: Removal of the new Rapid Recovery Agent software uses the package manager for each distribution. Therefore, if uninstalling a version of Rapid Recovery Agent, see the appropriate procedure under the topic see the topic "Uninstalling the AppAssure Agent software from a Linux machine" in the *Dell Data Protection* | *Rapid Recovery 6.0 Installation and Upgrade Guide*.

If installing Rapid Recovery Agent on a Linux machine that has never had AppAssure Agent installed, determine the appropriate package manager from the preceding table. Then follow the appropriate installation procedure.

After configuring the newly installed Agent software on a Linux machine, you must restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.

Thus, the installation process when upgrading from AppAssure to Rapid Recovery involves:

- Removing the AppAssure Agent software (not required for first-time installations)
- Determine the relevant package manager for your Linux distribution
- Follow the procedure for installing Rapid Recovery Agent on the Linux machine, including configuring the software repository (steps 1 through 4 of the installation procedure)
- Run the configuration utility to set port, configure users, add firewall exclusions, install the kernel module, and start the Agent service.
- Restart the Linux machine

The instructions for installing the Agent software on a Linux machine differ slightly depending on the Linux distribution you are using. For more information about preparing for and installing the Agent software for a Linux machine connected to the Internet, see the appropriate topic. You can choose from the following sections:

- Installing the Rapid Recovery Agent software on Debian or Ubuntu
- Installing the Rapid Recovery Agent software on SUSE Linux Enterprise Server

For more information about preparing for and installing the Agent software for a Linux machine that is not connected to the Internet, see the topic:

Installing the Agent software on offline Linux machines

Before you begin installation of Agent software, see the topics: Downloading the Linux distribution, About security, Location of Linux Agent files, Agent dependencies, Linux scripting information in the *Dell Data Protection* | *Rapid Recovery 6.0 Installation and Upgrade Guide*.

Location of Linux Agent files

There are several files required to support the Rapid Recovery Agent software on a Linux machine. For all supported Linux distributions, these files are located in the following directories:

- mono: /opt/apprecovery/mono
- agent: /opt/apprecovery/agent
 local mount:
- /opt/apprecovery/local mount
- rapidrecovery-vdisk and aavdctl: /usr/bin/aavdisk
- configuration files for rapidrecovery-vdisk: /etc/apprecovery/aavdisk.conf
- wrappers for agent and local_mount /usr/bin/agent

/usr/bin/local_mount

• autorun scripts for agent and rapidrecovery-vdisk:

/etc/init.d/rapidrecovery-agent

/etc/init.d/rapidrecovery-vdisk

Agent dependencies

The following dependencies are required and are installed as part of the Agent installer package:

- For Debian and Ubuntu:
 - The rapidrecovery-agent requires:

```
dkms, gcc, make, linux-headers-`uname-r`
libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3
```

- The rapidrecovery-mono requires:
 libc6 (>=2.7-18)
- For Red Hat Enterprise Linux, CentOS, and Oracle Linux:

```
- The nbd-dkms requires
```

```
dkms, gcc, make, kernel-headers-'uname-r' kernel-devel-'uname-r'
```

- The rapidrecovery-agent requires:

```
dkms, gcc, make, kernel-headers-'uname-r' kernel-devel-'uname-r', nbd-dkms, libblkid, pam, pcre
```

The rapidrecovery-mono requires:
 glibc >=2.11

- For SUSE Linux Enterprise Server:
 - The nbd-dkms requires:
 - dkms, gcc, make, kernel-syms
 - The rapidrecovery-agent requires:
 - dkms, kernel-syms, gcc, make, libblkid1, pam, pcre
 - The rapidrecovery-mono requires: glibc >= 2.11

Installing the Rapid Recovery Agent software on Debian or Ubuntu

The Rapid Recovery Agent .deb file is an archive containing repository information specific to the apt package manager. Complete the following steps to install the Rapid Recovery Agent on Debian or Ubuntu machines for an online installation.



NOTE: This procedure applies to a Linux machine that is connected to the internet. For offline installation of Rapid Recovery Agent on any Linux machine, see <u>Installing the Agent software on offline Linux machines</u>.

- 1. Open a terminal session with root access.
- 2. Determine your present working directory by entering PWD and pressing Enter. For example, assume your directory is /home/rapidrecovery/.
- **3.** Download the appropriate Rapid Recovery Agent .deb installation file from the License Portal at <u>https://licenseportal.com</u> to your present working directory.

For more information about the license portal, see the *Dell Data Protection* | *Rapid Recovery License Portal User Guide*.

4. To establish a persistent connection between your Linux machine and the remote Dell repository in which Rapid Recovery software and components are stored, type the following command:

dpkg -i <.deb installation file you downloaded>

For example, if the installer file is named rapidrecovery-repo-6.0.2.999.deb in the directory **/home/** rapidrecovery/, type the following command, and then press **Enter**:

dpkg -i rapidrecovery-repo-6.0.2.999.deb

Any missing packages or files required by the Agent will be downloaded from the remote repository and installed automatically as part of the script.

NOTE: For more information on dependencies for installing on a Linux machine, see <u>Agent</u> dependencies.

5. Install the Rapid Recovery Agent by invoking the apt package manager, updating the repository manager. Type the following command, and then press **Enter**:

apt-get update

6. Instruct the package manager to install the Rapid Recovery Agent software. Type the following command, and then press **Enter**:

apt-get install rapidrecovery-agent

7. The package manager prepares to install all dependent files. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

The Rapid Recovery Agent files are installed.

Installing the Rapid Recovery Agent software on SUSE Linux Enterprise Server

The Rapid Recovery Agent .rpm file is an archive containing repository information for SUSE Linux Enterprise Server (SLES) . This distribution uses the zypper package manager. Complete the following steps to install the Rapid Recovery Agent on SLES.



NOTE: This procedure applies to a Linux machine that is connected to the internet. For offline installation of Rapid Recovery Agent on any Linux machine, see <u>Installing the Agent software on offline Linux machines</u>.

- **1.** Open a terminal session with root access.
- 2. Determine your present working directory by entering PWD and pressing Enter. For example, assume your directory is /home/rapidrecovery/.
- Download the appropriate Rapid Recovery Agent .rpm installation file from the License Portal at https://licenseportal.com to your present working directory.

For more information about the license portal, see the *Dell Data Protection* | *Rapid Recovery License Portal User Guide*.

4. To establish a persistent connection between your Linux machine and the remote Dell repository in which Rapid Recovery software and components are stored, type the following command:

rpm -ivh <.rpm installation file you downloaded>

For example, if the installer file is named rapidrecovery-repo-6.0.2.999.rpm in the directory **/home/ rapidrecovery/**, type the following command, and then press **Enter**:

rpm -ivh rapidrecovery-repo-6.0.2.999.rpm

Any missing packages or files required by the Agent will be downloaded from the remote repository and installed automatically as part of the script.

NOTE: For more information on dependencies for installing on a Linux machine, see <u>Agent</u> <u>dependencies</u>.

5. Install the Rapid Recovery Agent by invoking the zypper package manager, updating the repository manager. Type the following command, and then press **Enter**:

apt-get update

6. Instruct the package manager to install the Rapid Recovery Agent software. Type the following command, and then press **Enter**:

apt-get install rapidrecovery-agent

7. The package manager prepares to install all dependent files. If prompted to confirm installation of unsigned files, enter **y** and then press **Enter**.

The Rapid Recovery Agent files are installed.

Installing the agent on Red Hat Enterprise Linux and CentOS



NOTE: Before performing these steps, ensure that you have downloaded the Red Hat or CentOS installer package to the **/home/system directory**. The following steps are the same for both 32-bit and 64-bit environments.

To install an agent on Red Hat Enterprise Linux and CentOS:

- 1. Open a terminal session with root access.
- 2. To make the Agent installer executable, type the following command:

chmod +x appassure-installer rhel amd64 5.x.x.xxxx.sh and then press <Enter>.



NOTE: For 32-bit environments, the installer is named appassureinstaller rhel i386 5.x.x.xxxx.sh.

The file becomes executable.

3. To extract and install the Agent, type the following command:

/appassure-installer rhel amd64 5.x.x.xxxx.sh and then press <Enter>.

The Linux agent begins its extraction and installation process. Any missing packages or files required by the agent is downloaded and installed automatically as part of the script.

For information on the files required by the Agent, see Agent dependencies.

After the installer completes, the Agent will be running on your machine. For more information on protecting this machine with the Core, see the topic 'Protecting Workstations and Servers' in the Rapid Recovery 6.0 on DL Appliances User's Guide at Dell.com/support/home.

Installing the Agent software on offline Linux machines

This task requires access to an online Linux machine, removable storage media, and access to the final offline Linux machine. If AppAssure Agent is installed on the offline Linux machine, you must first uninstall it before installing Rapid Recovery Agent. For more information, see "Uninstalling the AppAssure Agent software from a Linux machine" section in Dell Data Protection | Rapid Recovery Installation and Upgrade Guide.

When installing the Agent software on Linux machines that do not have access to the Internet, follow this procedure. After installation is complete, configure the Agent as described in the topic Configuring the Rapid Recovery Agent on a Linux machine.

NOTE: If installing on multiple Linux distributions, perform this procedure once for each distribution. U

1. From a Linux machine with access to the Internet, open a terminal window and type the following command:

wget http://s3.amazonaws.com/repolinux/6.0.2/packages-downloader.sh

The shell script downloads to your current directory.

2. Run the shell script by executing the following command: bash packages-downloader.sh

The script executes and prompts you to select a specific Linux distribution and architecture.

3. Type the index of the installation package you want and press Enter. For example, to obtain an installation package for Red Hat Enterprise Linux 7, enter 3 and press Enter.

The appropriate installer is extracted into the ~/rapidrecovery.packages/ directory.



4. Copy the packages for Rapid Recovery Agent to removable media. The specific location of your removable media can differ based on Linux distribution. Type the following command and then press Enter:

cp -R ~/rapidrecovery.packages/ <your removable media>

For example, if using a removable USB drive that is mounted to location /media/USB-drive-1, type the following command and then press **Enter**:

```
cp -R ~/rapidrecovery.packages /media/USB-drive-1
```

All the necessary files are copied to the removable medium.

- 5. Take the removable medium to the offline Linux machine and mount the drive.
- **6.** Copy the data from the mounted device to your home directory or other desired location. For example, type the following command and then press **Enter**:

```
cp -R /media/USB-drive-1 ~/rapidrecovery.packages
```

- 7. Change to the Rapid Recovery directory. For example, type the following command and then press **Enter**:
 - cd ~/rapidrecovery.packages
- 8. Run the installation of Agent with root privileges. This command differs based on Linux distribution.
 - For Red Hat, SLES, Oracle, and CentOS, type the following command and then press **Enter**: sudo rpm -i *.rpm
 - For Debian and Ubuntu, type the following command and then press Enter: sudo dpkg -i *.deb

The local package manager runs the installation of Rapid Recovery Agent.

After installation is complete, configure the Agent as described in the topic <u>Configuring the Rapid</u> <u>Recovery Agent on a Linux machine</u>.

CAUTION: After configuring the newly installed Agent software on a Linux machine, you must restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.

Installing the Agent software on Windows Server Core Edition machines

Complete the steps in the following procedure to install the Agent software on a Windows Server Core machine.



NOTE: The following procedure installs the Agent software in console mode. To install in silent mode instead, append /silent to the installer file name on the command line. For example, Agent-X64-6.X.X.xxxxx.exe /silent.

- 1. Download the Rapid Recovery Agent installer file from the Dell Data Protection | Rapid Recovery License Portal or from the Rapid Recovery Core.
- **2.** From a command prompt, navigate to the directory containing the Rapid Recovery Agent installer file and enter the installer file name to begin the installation:

Agent-X64-6.x.x.xxxx.exe

The installation program installs the Agent software and displays progress in the console. Upon completion, new installations trigger an automatic restart of the machine, whereas Agent upgrades may not require a machine restart.

Configuring the Rapid Recovery Agent on a Linux machine

Run the Rapid Recovery Configuration utility after installing Rapid Recovery Agent software on a Linux machine. This compiles and installs the kernel module on the Linux machine you want to protect in your Core.

The configuration utility offers several configuration options, and provides hints in the numbered steps of the instructions when it detects your specific configuration information.

Complete the steps below to configure the Rapid Recovery Agent software on any Linux machine. Some configuration options differ based on the Linux distribution you are installing.

- 1. Open a terminal session with root access.
- 2. Launch the configuration utility by typing the following command, and then press Enter:

sudo /usr/bin/rapidrecovery-config

The configuration utility starts. This lists several configuration options, each with an index number to enter for the appropriate configuration step.

3. Configure the port for this protected machine by typing the following command, and then press Enter. The default port is 8006.

1 <agent_port>

For example, if using the default port, type the command:

1 8006

4. Configure users available for protection, by typing the following command, and then press Enter:

```
1 <user_names_separated_by_comma>
```

For example, if using usernames michael, administrator, and test_user1, type the command:

- 2 michael,administrator,test_user1
- **5.** Configure firewall rules to select a firewall configuration manager. This establishes firewall exceptions for the port designated in step 1.

If the utility detects one or more firewall configuration managers (such as lokkit or firewalld), each is listed in the utility in line 3. Select the appropriate configuration manager and enter it, starting with the command number (3), and then press Enter:

3 <firewall configuration>

For example, if using firewalld, type the command:

3 firewalld

6. Query the list of compatible kernel modules from the utility by entering the command number, and then press Enter:

4

A sub-shell returns all kernel modules compatible for installation. For example, the following could be returned:

```
Searching for all available for installation kernels.
This might take a while, depending on the Internet connection speed.
Kernels compatible for module installation:
0 - linux-image-3.16.0.23-generic
1 - linux-image-3.16.0.31-generic
2 - linux-image-3.16.0.33-generic
3 - linux-image-3.16.0.34-generic
Input indices of the kernel modules you wish to install, delimited by
space; use 'all' to install into all supported kernels, or 'q' to quit.
```

7. Configure the appropriate Rapid Recovery kernel module.

For example, to enter kernel modules for 3.16.0-23 and 3.16.0-34, enter 1 4 and press Enter.

To enter all kernel modules, enter all and press Enter.

8. After configuring the newly installed Agent software, restart the machine. Restarting ensures that the proper kernel driver version is used to protect your machine.

After completing this process, the local repository has been configured on this Linux machine. The Agent software is installed and the kernel module is loaded.

Your next step is to protect the machine on the Rapid Recovery Core.

Protecting a machine

If you have already installed the Rapid Recovery Agent software on the machine you want to protect, but have not restarted it yet, restart the machine now.

This topic describes how to start protecting the data on a single machine that you specify using the Protect Machine Wizard.

When you add protection, you need to define connection information such as the IP address and port, and provide credentials for the machine you want to protect. Optionally, you can provide a display name to appear in the Core Console instead of the IP address. If you change this, you will not see the IP address for the protected machine when you view details in the Core Console. You will also define the protection schedule for the machine.

The workflow of the protection wizard may differ slightly based on your environment. For example, if the Rapid Recovery Agent software is installed on the machine you want to protect, you will not be prompted to install it from the wizard. Likewise, if a repository already exists on the Core, you will not be prompted to create one.

- **1.** Do one of the following:
 - If you are starting from the Protect Machine Wizard, proceed to Step 2.
 - If you are starting from the Rapid Recovery Core Console, from the button bar, click Protect.

The Protect Machine Wizard appears.

- 2. On the **Welcome** page, select the appropriate installation options:
 - If you do not need to define a repository or establish encryption, select Typical.
 - If you need to create a repository, or define a different repository for backups for the selected machine, or if you want to establish encryption using the wizard, select **Advanced (show optional steps)**.
 - Optionally, if you do not wish to see the **Welcome** page for the Protect Machine Wizard in the future, select the option **Skip this Welcome page the next time the wizard opens**.
- **3.** When you are satisfied with your choices on the Welcome page, then click **Next**. The **Connection** page appears.
- 4. On the **Connection** page, enter the information about the machine to which you want to connect as described in the following table, and then click **Next**.

Table 8. Machine connection settings

Text Box	Description
Host	The host name or IP address of the machine that you want to protect.
Port	The port number on which the Rapid Recovery Core communicates with the Agent on the machine. The default port number is 8006.
User name	The user name used to connect to this machine; for example, Administrator (or, if the machine is in a domain, [domain name]\Administrator).
Password	The password used to connect to this machine.

If the **Install Agent** page appears next in the Protect Machine Wizard, that means that Rapid Recovery does not detect the Rapid Recovery Agent on the machine and will install the current version of the software. Go to Step 7.

If the **Upgrade Agent** page appears next in the wizard, that means that an older version of the Agent software exists on the machine you want to protect.



NOTE: The Agent software must be installed on the machine you want to protect, and that machine must be restarted, before it can back up to the Core. To have the installer reboot the protected machine, select the option **After installation, restart the machine automatically** (recommended) before clicking Next.

- 5. On the Upgrade Agent page, do one of the following:
 - To deploy the new version of the Agent software (matching the version for the Rapid Recovery Core), select **Upgrade the Agent to the latest version of the software**.
 - To continue protecting the machine without updating the Agent software version, clear the option **Upgrade the Agent to the latest version of the software**.
- 6. Click Next.
- 7. Optionally, on the **Protection** page, if you want a name other than the IP address to display in the Rapid Recovery Core console for this protected machine, then in the **Display Name** field, type a name in the dialog box.

You can enter up to 64 characters. Do not use the special characters described in the topic "Prohibited characters" in the *Rapid Recovery on DL Appliances User's Guide*. Additionally, do not begin the display name with any of the character combinations described in the topic prohibited phrases in the *Rapid Recovery on DL Appliances User's Guide*.

- 8. Select the appropriate protection schedule as described below:
 - To use the default protection schedule, in the Schedule Settings option, select **Default protection**.

With a default protection schedule, the Core will take snapshots of all volumes on the protected machine once every hour. To change the protection settings at any time after you close the wizard, including choosing which volumes to protect, go to the Summary page for the specific protected machine.

- To define a different protection schedule, in the Schedule Settings option, select **Custom protection**.
- 9. Proceed with your configuration as follows:
 - If you selected a Typical configuration for the Protect Machine Wizard and specified default protection, then click **Finish** to confirm your choices, close the wizard, and protect the machine you specified.

The first time protection is added for a machine, a base image (that is, a snapshot of all the data in the protected volumes) will transfer to the repository on the Rapid Recovery Core following the schedule you defined, unless you specified to initially pause protection.

- If you selected a Typical configuration for the Protect Machine Wizard and specified custom protection, then click Next to set up a custom protection schedule. For details on defining a custom protection schedule, see "Creating custom protection schedules" section in the Rapid Recovery 6.0 on DL Appliances User's Guide. .
- If you selected Advanced configuration for the Protect Machine Wizard, and default protection. then click **Next** and proceed to Step 14 o see repository and encryption options.
- If you selected Advanced configuration for the Protect Machine Wizard and specified custom protection, then click **Next** and proceed to Step 11 to choose which volumes to protect.
- 10. On the Protection Volumes page, select which volumes you want to protect. If any volumes are listed that you do not want to include in protection, click in the Check column to clear the selection. Then click Next.



NOTE: Typically, it is good practice to protect, at minimum, the System Reserved volume and the volume with the operating system (typically the C drive).

11. On the Protection Schedule page, define a custom protection schedule and then click Next. For details on defining a custom protection schedule, see "Creating custom protection schedules" section in the Rapid Recovery 6.0 on DL Appliances User's Guide.

If you already have repository information configured, and you selected the Advanced option in Step 1, then the Encryption page appears. Proceed to Step 13.

12. Optionally, on the **Encryption** page, to enable encryption, select **Enable Encryption**. Encryption key fields appear on the **Encryption** page.



NOTE: If you enable encryption, it will be applied to data for all protected volumes for this machine.

You can change encryption settings later from the Rapid Recovery Core Console. For more information about encryption, see the topic "Understanding encryption keys" in the Rapid Recovery 6.0 on DL Appliances User's Guide at www.dell.com/support/home.

CAUTION: Rapid Recovery uses AES 256-bit encryption in the Cipher Block Chaining (CBC) mode with 256-bit keys. While using encryption is optional, Dell highly recommends that you establish an encryption key, and that you protect the passphrase you define. Store the passphrase in a secure location as it is critical for data recovery. Without a passphrase, data recovery is not possible.

- **13.** On the **Encryption** page, select one of the following options:
 - If you want to encrypt this protected machine using an encryption key that is already defined on this Rapid Recovery Core, select Encrypt data using an existing Encryption key, and then select the appropriate key from the drop-down menu. Proceed to the next step.
 - If you want to add a new encryption key to the Core and apply that key to this protected machine, then enter the information as described in the following table. Table 9. Encryption key settings

Text Box	Description
Name	Enter a name for the encryption key.
	Encryption key names must contain between 1 and 130 alphanumeric characters. You may not include special characters such as the back slash, forward slash, pipe, colon, asterisk, quotation mark, question mark, open or

Text Box	Description
	close brackets, ampersand or hash. This information appears in the Description field when viewing encryption keys from the Core Console.
Description	Enter a comment for the encryption key.
	This information appears in the Description field when viewing encryption keys from the Core Console.
Passphrase	Enter the passphrase used to control access.
	Best practice is to avoid special characters listed above.
	Record the passphrase in a secure location. Dell Support cannot recover a passphrase. Once you create an encryption key and apply it to one or more protected machines, you cannot recover data if you lose the passphrase.
Confirm Passphrase	Re-enter the passphrase you just entered.

14. Click Finish to save and apply your settings.

The first time protection is added for a machine, a base image (that is, a snapshot of all the data in the protected volumes) will transfer to the repository on the Rapid Recovery Core following the schedule you defined, unless you specified to initially pause protection.

- **15.** If you receive an error message, the appliance cannot connect to the machine to back it up. To resolve the issue:
 - a. Check Network Connectivity.
 - b. Check the Firewall Settings.
 - c. Verify Rapid Recovery Services and RPC are running.
 - d. Verify Domain Name Service Lookups (if applicable).

Checking network connectivity

To check network connectivity:

- 1. On the client system to which you are trying to connect, open a command line interface.
- 2. Run the command **ipconfig** and note the IP address of the client.
- 3. Open a command line interface on the appliance.
- 4. Run the command ping <IP address of client>.
- 5. Depending on the result, do one of the following:
 - If the client does not reply to the ping, verify the server's connectivity and network settings.
 - If the client replies, check that the firewall settings allow the DL1300 components to run.

Checking the firewall settings

If the client is connected properly to the network, but cannot be seen by the Core console, check the firewall to ensure that necessary inbound and outbound communications are allowed.

To check the firewall settings on the Core and any clients that it backs up:

- **1.** On the DL1300 appliance, click **Start** \rightarrow **Control Panel.**
- 2. In the Control Panel, click System and Security, under Windows Firewall click Check firewall status.
- 3. Click Advanced Settings.
- 4. In the Windows Firewall with Advanced Security screen, click Inbound Rules.

- 5. Ensure the Core and ports display Yes in the Enabled column.
- 6. If the rule is not enabled, right-click on Core and select **Enable Rule**.
- 7. Click Outbound Rules and verify the same for Core.

Checking DNS resolution

If the machine you are trying to back up uses DNS, verify that DNS forward and reverse lookups are correct.

To ensure that the reverse lookups are correct:

- 1. On the appliance, go to C:\Windows\system32\drivers\etc hosts.
- 2. Enter the IP address of each client that backs up to DL1300.

Teaming network adapters

By default, the network adapters (NICs) on the DL1300 Appliance are not bonded, which affects the performance of the system. It is recommended that you team the NICs to a single interface. Teaming the NICs require:

- Reinstalling the Broadcom Advanced Control Suite
- Creating the NIC team

Reinstalling Broadcom Advanced Configuration Suite

To reinstall Broadcom Advanced Configuration Suite:

- Go to C:\Install\BroadcomAdvanced and double-click setup. The InstallShield Wizard is displayed.
- 2. Click Next.
- 3. Click Modify, Add, or Remove.

The **Custom Setup** window is displayed.

- 4. Click CIM Provider, and then select This feature will be installed on local hard drive.
- 5. Click BASP, and then select This feature will be installed on local hard drive.
- 6. Click Next.
- 7. Click Install.
- 8. Click Finish.

Creating the NIC team

NOTE: It is recommended to **not** use the native teaming interface in Windows 2012 Server. The teaming algorithm is optimized for outbound, not inbound, traffic. It offers poor performance with a backup workload, even with more network ports in the team.

To create NIC teaming:

1. Go to Start \rightarrow Search \rightarrow Broadcom Advanced Control Suite.

NOTE: When using Broadcom Advanced Control Suite, only select the Broadcom network cards.

- 2. In the Broadcom Advanced Control Suite, select Teams \rightarrow Go to Team View.
- **3.** In the **Hosts list** on the left side, right-click on the host name of the DL1300 appliance and select **Create Team**.

The Broadcom Teaming Wizard window is displayed.

- 4. Click Next.
- 5. Enter a name for the team and click **Next**.
- 6. Select the Team Type and click Next.
- 7. Select an adapter you want to be part of the team, and click Add.
- 8. Repeat these steps for all other adapters that are a part of the team.
- 9. When all adapters are selected for the team, click Next.
- 10. Select a standby NIC if you want a NIC that can be used as the default, if the team fails.
- 11. Select whether to configure LiveLink, and then click Next.
- 12. Select Skip Manage VLAN and click Next.
- 13. Select Commit changes to system and click Finish.
- 14. Click Yes when warned that the network connection is interrupted.



NOTE: Building of the NIC team may take approximately five minutes.

Adjusting the number of streams

By default, Rapid Recovery is configured to allow three concurrent streams to the appliance. It is recommended that the number of streams is set between 10 and 15 for optimal performance. To change the number of concurrent streams:

- 1. Select the Configuration tab and then click Settings.
- 2. Select change in Transfer Queue.
- 3. Change Maximum Concurrent Transfers to a number between 10 and 15 for optimal performance, but if the performance seems unsatisfactory, try tuning it manually.

Common use cases

This section provides the most common use cases for the DL1300 and provides a high-level overview of the information and procedures required for each scenario. Where required, references to additional information is provided.

Protecting machines

The AppAssure backup and replication technology provides advanced protection of VMs or servers while enabling flexible application and data recovery. When a machine is protected, full and incremental snapshots of data are captured and stored in the core's repository. The AppAssure protection process leverages two key technologies – Snapshots and the Dell DL1300 Smart Agent that are described below.

Snapshots

The AppAssure Agent for Windows uses Microsoft Volume Shadow copy Service (VSS) to freeze and quiesce application data to disk to capture a file-system-consistent and an application-consistent backup. When a snapshot is created, the VSS, writer on the target server prevents content from being written to the disk. During the process of halting of writing content to disk, all disk I/O operations are queued and resume only after the snapshot is complete, while the operations already in flight will be completed and all open files will be closed. For more information, see topic <u>Snapshot Process</u>.

Dell DL1300 Smart Agents

The Smart Agent is installed on the machines that are protected by the DL1300 Core. The Smart Agent tracks the changed blocks on the disk volume and then snaps an image of the changed blocks at a predefined interval of protection. The incremental block-level snapshots' forever approach prevents repeated copying of the same data from the protected machine to the Core. When the snapshot is ready, it is rapidly transferred to the Core using intelligent multi-threaded, socket-based connections. For more information, see the topic <u>Dell DL1300 Smart Agent</u>.

Deploying Smart Agents

You must install the AppAssure Agent Installer on every machine in your environment protected by the DL1300 Core.



NOTE: These procedures are a summary. For detailed information, or specific instructions for Linux Agents, refer to the *Dell DL1300 Appliance User's Guide*.

Step 1: Obtaining the Agent Software

Smart Agent software can be obtained by following one of the following methods:

- Download from the AppAssure Core Log into the Core Console and download the software to the agent machine. Select **Downloads** from the **Tools** tab, and then download the web installer for the Agent component.
- Download from the AppAssure License Portal If you have registered your software in the Dell Software License Portal, you can log into the License Portal and download the software to the agent machine.
- Deploy the Agent Software when protecting a machine You can deploy the Agent software to the machine you want to protect using the Protect a Machine Wizard.
- Use the Bulk Deploy feature If the Core is installed, you can deploy the Agent software to multiple machines using the **Bulk deploy** feature, accessed from the **Tools** tab of the Core Console.

Step 2: Install the Agent Software

Launch the installer program as described below to install the software on each machine you want to protect in the Core. To install the Agent software on Windows machines:

- **1.** From the machine you want to protect, double-click the Agent installer file.
- 2. On the Welcome page, click Next to continue with the installation.
- 3. On the License Agreement page, click I accept the terms in the license agreement, and click Next.

NOTE: The Agent Installer verifies the existence of the prerequisite files. If the prerequisite files Ø do not exist, the Agent Installer identifies which files are needed and displays the results accordingly; for example, Microsoft System CLR Types for SQL Server 2008 R2 (x64).

- 4. Click Install Prerequisites.
- 5. When the installation of the prerequisite files is completed, click **Next**.
- 6. On the Installation Options page, review the installation options. If necessary, modify them as described below:
 - a. In the Destination Folder text field, review the destination folder for the installation. If you want to change the location, do the following:
 - Click the folder icon
 - In the Browse to Destination dialog box, select a new location. Click OK.
 - b. In the **Port Number** text field, enter a port number to use for communication between the agent and the Core.



NOTE: The default value is 8006. If you change the port number, make a note of it in the event that you need to adjust configuration settings at a later time.

- 7. Check for the installation options, click Install. When the installation is complete, the Completed page is displayed.
- 8. Select one of the following options, and then click Finish: Yes, I want to restart my computer now. No, I will restart my computer later.



NOTE: You must restart your system before using the Agent software.

Configuring protection jobs

When you add protection, you need to define connection information such as the IP address and port, and provide credentials for the machine you want to protect. Optionally, you can provide a display name to appear in the Core Console instead of the IP address. You will also define the protection schedule for the machine



NOTE: These procedures are a summary. For more detailed information, refer to the *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.

Protecting a machine

This topic describes how to start protecting the data on a machine that you specify.



NOTE: The machine must have the AppAssure Agent software installed in order to be protected. You can choose to install the Agent software prior to this procedure, or you can deploy the software to the agent as you define protection in the **Connection** dialog box. To install the agent software during the process of protecting a machine, see topic 'Deploying The Agent Software When Protecting An Agent' in *Dell DL1300 Appliance User's Guide*.

When you add protection, you must specify the name or IP address of the machine to protect and the volumes on that machine to protect as well as define the protection schedule for each volume.

To protect multiple machines at the same time, see topic 'Protecting Multiple Machines' in *Dell DL1300 Appliance User's Guide*.

To protect a machine:

- **1.** Reboot the machine on which the AppAssure Agent software is installed, if you haven't already done so.
- From the Core Console on the core machine, click Protect → Protect Machine on the button bar. The Protect Machine Wizard is displayed.
- 3. On the **Welcome** page, select the appropriate installation options:
 - If you do not need to define a repository or establish encryption, select **Typical**.
 - If you do not wish to see the **Welcome** page for the **Protect Machine Wizard** in the future, select the **Skip this Welcome page the next time the wizard opens** option.
- 4. Click Next.
- 5. On the **Connection** page, enter the information about the machine to which you want to connect as described in the following table.

Text Box	Description
Host	The host name or IP address of the machine that you want to protect.
Port	The port number on which the AppAssure Core communicates with the agent on the machine. The default port number is 8006.
Username	The user name used to connect to this machine; for example, administrator.
Password	The password used to connect to this machine.

- 6. Click Next. If the Protection page appears next in the Protect Machine Wizard, skip to Step 7.
 - **NOTE:** If the **Install Agent** page appears next in the **Protect Machine Wizard**, this indicates that the Agent software is not yet on installed on the designated machine. Click **Next** to install the Agent software. The Agent software must be installed on the machine you want to protect, and that be restarted, before it can back up to the Core. To have the installer reboot the agent machine, select the **After installation, restart the machine automatically (recommended)** option before clicking **Next**.
- 7. The host name or IP address you specified in the **Connect** dialog box appears in this text field. Optionally, enter a new name for the machine to be displayed in the Core Console.
- 8. Select the appropriate protection schedule:

- To use the default protection schedule, in the **Schedule Settings** option, select **Default protection (3 hour snapshots of all volumes)**. With a default protection schedule, the Core will take snapshots of the agent machine once every 3 hours. Snapshots of the agent machine can be taken once every hour (minimum). To change the protection settings at any time after you close the wizard, including choosing which volumes to protect, go to the Summary tab for the specific agent machine.
- To define a different protection schedule, in the **Schedule Settings** option, select **Custom protection**.
- **9.** Select one of the following:
 - If you selected a Typical configuration from the **Protect Machine Wizard** and specified default protection, then click **Finish** to confirm your choices, close the wizard, and protect the machine you specified.
 - The first time protection is added for a machine, a base image (that is, a snapshot of all the data in the protected volumes) will transfer to the repository on the Core following the schedule you defined, unless you specified to initially pause protection.
 - If you selected a Typical configuration for the Protect Machine Wizard and specified custom
 protection, then click Next to set up a custom protection schedule. For details on defining a
 custom protection schedule, see Creating Custom Protection Schedules.
 - If you selected Advanced configuration for the **Protect Machine Wizard**, and default protection, then click **Next** and proceed to Step 12 to see repository and encryption options.
 - If you selected Advanced configuration for the **Protect Machine Wizard** and specified custom protection, then click **Next** and proceed to Step 10 to choose which volumes to protect.
- **10.** On the **Protection Volumes** page, select the volumes on the agent machine that you want to protect. If any volumes are listed that you do not want to include in protection, click in the Check column to clear the selection. Then click **Next**.

NOTE: It is recommended to protect the System Reserved volume and the volume with the operating system (typically the C drive).

- 11. On the Protection Schedule page, define a custom protection schedule.
- 12. On the Repository page, select Use an existing repository.
- 13. Click Next.

The Encryption page is displayed.

14. Optionally, to enable encryption, select Enable Encryption.

Encryption key fields appear on the Encryption page.

U

NOTE: If you enable encryption, it will be applied to data for all protected volumes for this agent machine. You can change the settings later from the Configuration tab in the AppAssure 5 Core Console.

CAUTION: AppAssure uses AES 256-bit encryption in the Cipher Block Chaining (CBC) mode with 256-bit keys. While using encryption is optional, Dell highly recommends that you establish an encryption key, and that you protect the passphrase you define. Store the passphrase in a secure location as it is critical for data recovery. Without a passphrase, data recovery is not possible.

15. Enter the information as described in the following table to add an encryption key for the Core.

Text Box	Description
Name	Enter a name for the encryption key.
Description	Enter a description to provide additional details for the encryption key.
Passphrase	Enter the passphrase used to control access.

Text Box Description

ConfirmRe-enter the passphrase you just entered.Passphrase

16. Click Finish to save and apply your settings.

The first time protection is added for a machine, a base image (that is, a snapshot of all the data in the protected volumes) will transfer to the repository on the AppAssure Core following the schedule you defined, unless you specified to initially pause protection.

Recovering data

With the DL1300, data is protected on both Windows and Linux machines. Protected machine backups are saved to the Core as recovery points that can be used to restore your data. Entire volumes can be restored replaced from a recovery point to the destination machines. To restore data from recovery points any one of the following methods can be performed:

- Recovery of files and folders
- Recovery of data volumes, using Live Recovery
- Bare metal restore, using Universal Recovery

Recovering directories or files

You can use Windows Explorer to copy and paste directories and files from a mounted recovery point to any Windows machine. This can be helpful when you want to distribute only a portion of a recovery point to your users. When you copy directories and files, the access permissions of the user who is performing the copy operation are used and applied to the pasted directories and files. To restore a directory or file using Windows Explorer:

- **1.** Mount the recovery point that contains the data you want to restore. For more information, see Mounting A Recovery Point For A Windows Machine topic in the *Dell DL1300 Appliance User's Guide*.
- 2. In Windows Explorer, navigate to the mounted recovery point and select the directories and files that you want to restore. Right-click and select **Copy**.
- **3.** In Windows Explorer, navigate to the machine location to where you want to restore the data. Rightclick and select **Paste**.

Restoring volumes

From the Core Console, you can restore entire volumes from a recovery point of a non-system volume, replacing the volumes on the destination machine.



NOTE: The procedure below is a simplified overview of the restore process. For detailed information or procedures on additional restore options, see topic 'Restoring Volumes from a Recovery Point' in the *Dell DL1300 Appliance User's Guide*.

To restore volumes from a recovery point:

1. In the Core Console, click the **Restore** tab.

The Restore Machine Wizard is displayed.

2. From the **Protected Machines** page, select the protected machine for which you want to restore data, and then click **Next**.



NOTE: The protected machine must have the Agent software installed and must have recovery points from which you will perform the restore operation.

The **Recovery Points** page is displayed.

3. From the list of recovery points, search for the snapshot you want to restore to the agent machine.

NOTE: If required, use the navigation buttons at the bottom of the page to display additional Ø recovery points. Or if you want to limit the amount of recovery points showing in the Recovery Points page of the wizard, you can filter by volumes (if defined) or by creation date of the recovery point.

4. Click any recovery point to select it, and then click Next.

The **Destination** page is displayed.

- On the **Destination** page, choose the machine to which you want to restore data as follows: 5
 - If you want to restore data from the selected recovery point to the same agent machine (for example, Machine1), and if the volumes you want to restore do not include the system volume, then select Recover to a protected machine (only non-system volumes), verify that the destination machine (Machine1) is selected, and then click **Next**. The Volume Mapping page appears. Proceed to Step 6.
 - If you want to restore data from the selected recovery point to a different protected machine (for example, to replace the contents of Machine2 with data from Machine1), then select Recover to a protected machine (only non-system volumes), select the destination machine (for example, Machine2) from the list, and then click Next. The Volume Mapping page appears. Proceed to Step 6.
 - If you want to restore from a recovery point to a system volume (for example, the C drive of the agent machine named Machine1), you must perform a BMR.
- On the Volume Mapping page, for each volume in the recovery point that you want to restore, select 6. the appropriate destination volume. If you do not want to restore a volume, in the Destination Volumes column, select **Do not restore**.
- 7. Select **Show advanced options** and then do the following:
 - For restoring to Windows machines, if you want to use Live Recovery, select Live Recovery. Using the Live Recovery instant recovery technology in AppAssure 5, you can instantly recover or restore data to your physical machines or to virtual machines from stored recovery points of Windows machines, which includes Microsoft Windows Storage Spaces. Live Recovery is not available for Linux machines.
 - If you want to force dismount, select Force Dismount. If you do not force a dismount before restoring data, the restore may fail with a volume in use error.

The agent machine, when started from the boot CD, displays the Universal Recovery Console (URC) interface. This environment is used to restore the system drive or selected volumes directly from the Core. Note the IP address and authentication key credentials in the URC, which refresh each time you start from the boot CD.

- 8. If the volumes you want to restore contain SOL or Microsoft Exchange databases, on the **Dismount** Databases page, you are prompted to dismount them. Optionally, if you want to remount these databases after the restore is complete, select Automatically remount all databases after the recovery point is restored. Click Finish.
- 9. Click OK to confirm the status message that the restore process has started.
- **10.** To monitor the progress of your restore action, on the Core Console, click **Events**.

Bare Metal Recovery

AppAssure provides the ability to perform a bare metal restore (BMR) for your Windows or Linux machines. BMR is a process that restores the full software configuration for a specific system. It uses the term "bare metal" because the restore operation recovers not only the data from the server, but also reformats the hard drive and reinstalls the operating system and all software applications. To perform a BMR, you specify a recovery point from a protected machine, and roll back to the designated physical or virtual machine. Other circumstances in which you may choose to perform a bare metal restore include hardware upgrade or server replacement.

Performing a BMR is possible for physical or virtual machines. As an added benefit, AppAssure allows you to perform a BMR whether the hardware is similar or dissimilar.

Prerequisites for performing a Bare Metal Restore for a Windows machine

Before you can begin the process of performing a bare metal restore for a Windows machine, you must ensure that the following conditions and criteria exist:

- **Backups of the machine you want to restore** You must have a functioning AppAssure Core containing recovery points of the protected server you want to restore.
- Hardware to restore (new or old, similar or dissimilar) The target machine must meet the installation requirements for an agent.
- Image media and software You must have a blank CD or DVD and disk burning software, or software to create an ISO image. If managing machines remotely using virtual network computing software such as UltraVNC, then you must have VNC Viewer.
- Compatible storage drivers and network adapter drivers If restoring to dissimilar hardware, then you must have Windows 7 PE (32-bit) compatible storage drivers and network adapter drivers for the target machine, including RAID, AHCI, and chipset drivers for the target operating system, as appropriate.
- Storage space and partitions, as appropriate Ensure that there is enough space on the hard drive to create destination partitions on the target machine to contain the source volumes. Any destination partition should be at least as large as the original source partition.
- Compatible partitions Windows 8 and Windows Server 2012 operating systems that are booted from FAT32 EFI partitions are available for protection or recovery, as well as are Resilient File System (ReFS) volumes. UEFI partitions are treated as simple FAT32 volumes. Incremental transfers are fully supported and protected. AppAssure 5 provides support of UEFI systems for BMR including automatic partitioning GPT disks.

Roadmap for performing a Bare Metal Restore for a Windows machine

NOTE: Following are basic steps used in the Bare Metal Restore (BMR) process. For detailed information on each step, see the *Dell DL1300 Appliance User's Guide*.

To perform a BMR for a Windows machine:

- 1. Create a boot CD.
- 2. Burn the image to disk.
- **3.** Boot the target server from the boot CD.
- 4. Connect to the recovery disk.

- 5. Map the volumes.
- **6.** Initiate the recovery.
- 7. Monitor the progress.

Replicating recovery points

Replication is the process of copying recovery points and transmitting them to a secondary location for the purpose of disaster recovery. The process requires a paired source-target relationship between two cores. The source core copies the recovery points of the protected agents and then asynchronously and continuously transmits them to a target core at a remote disaster recovery site. The off-site location can be a company-owned data center (self-managed core) or a third-party managed service provider's (MSP's) location or cloud environment. When replicating to a MSP, you can use built-in work flows that let you request connections and receive automatic feedback notifications. Possible scenarios for replication include:

- **Replication to a Local Location** The target core is located in a local data center or on-site location, and replication is maintained at all times. In this configuration, the loss of the Core would not prevent a recovery.
- **Replication to an Off-site Location** The target core is located at an off-site disaster recovery facility for recovery in the event of a loss.
- **Mutual Replication** Two data centers in two different locations each contain a core and are protecting agents and serving as the off-site disaster recovery backup for each other. In this scenario, each core replicates the agents to the Core that is located in the other data center.
- Hosted and Cloud Replication— AppAssure MSP partners maintain multiple target cores in a data center or a public cloud. On each of these cores, the MSP partner lets one or more of their customers replicate recovery points from a source core on the customer's site to the MSP's target core for a fee.

Setting up your environment

If the bandwidth between the source core and the target core cannot accommodate the transfer of stored recovery points, replication begins with seeding the target core with base images and recovery points from the selected servers protected on the source core. The seeding process can be performed at any time, as part of the initial transfer of data to serve as the foundation for regularly scheduled replication, or in the case of re-instating replication for a previously replicated machine whose replication had been paused or deleted. In this case, the Build RP Chain option would let you copy not-yet replicated recovery points to a seed drive.

When preparing for replication, you should consider the following factors:

- **Change Rate**—The change rate is the rate at which the amount of protected data is accumulated. The rate depends on the amount of data that change on protected volumes and the protection interval of the volumes. If a set of blocks change on the volume, reducing the protection interval reduces the change rate.
- **Bandwidth** The bandwidth is the available transfer speed between the source core and the target core. It is crucial that the bandwidth be greater than the change rate for replication to keep up with the recovery points created by the snapshots. Due to the amount of data transmitted from core to core, multiple parallel streams may be required to perform at wire speeds up to the speed of a 1 GB Ethernet connection.

NOTE: Bandwidth specified by the ISP is the total available bandwidth. The outgoing bandwidth is shared by all devices on the network. Make sure that there is enough free bandwidth for replication to accommodate the change rate.

Number of Agents— It is important to consider the number of agents protected per source core and how many you plan to replicate to the target. DL1300 lets you perform replication on a per-protected server basis, so you can choose to replicate certain servers. If all protected servers must be replicated, this drastically affects the change rate, particularly if the bandwidth between the source and target cores is insufficient for the amount and size of the recovery points being replicated.

Depending on your network configuration, replication can be a time-consuming process.

The Maximum Change Rate for WAN Connection Types is shown in the table below with examples of the necessary bandwidth per gigabyte for a reasonable change rate.

Broadband	Bandwidth	Max Change Rate
DSL	768 Kbps and up	330 MB per hour
Cable	1 Mbps and up	429 MB per hour
Τ1	1.5 Mbps and up	644 MB per hour
Fiber	20 Mbps and up	8.38 GB per hour

Table 10. Maximum Change Rate for WAN Connection Types

For optimum results, you should adhere to the recommendations listed in the table above. If a link fails during data transfer, replication resumes from the previous failure point of the transfer once link functionality is restored.

Steps for configuring replication

NOTE: The information below is presented as a high-level overview of the steps required to perform Ø replication. For complete procedures, go to the Dell DL1300 Appliance User's Guide at dell.com/ support/home.

To replicate data using AppAssure, you must configure the source and target cores for replication. After you configure replication, you can then replicate agent data, monitor and manage replication, and perform recovery. Performing replication in AppAssure involves performing the following operations:

- Configure self-managed replication For more information on replicating to a self-managed target core, see topic 'Replicating to a Self-Managed Target Core' in the Dell DL1300 Appliance User's Guide at Dell.com/support/home.
- **Configure third-party replication** For more information on replicating to a third-party target core, see topic 'Process of Replicating to a Third-Party Target Core' in the Dell DL1300 Appliance User's Guide at **Dell.com/support/home**.
- **Replicate an existing agent** For more information on replicating an agent that is already protected by the source core, see topic 'Adding a Machine to Existing Replication' in the Dell DL1300 Appliance User's Guide at Dell.com/support/home.
- **Consume the seed drive** For more information on consuming seed drive data on the target core, see topic 'Consuming the Seed Drive on a Target Core' in the Dell DL1300 Appliance User's Guide at Dell.com/support/home.

- Set the replication priority for an agent— For more information on prioritizing the replication of agents, see topic 'Setting Replication Priority for an Agent' in the *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.
- Set a replication schedule for an agent— For more information on setting a replication schedule, see topic 'Scheduling Replication' in the *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.
- Monitor replication as needed— For more information on monitoring replication, see topic 'Monitoring Replication' in the *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.
- Manage replication settings as needed— For more information on managing replication settings, see topic 'Managing Replication Settings' in the *Dell DL1300 Appliance User's Guide* at **Dell.com/support/** home.
- Recover replicated data in the event of disaster or data loss— For more information on recovering replicated data, see topic 'Recovering Replicated Data' in the *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.

Using virtual standby

AppAssure supports both a one-time export and continuous export (to support virtual standby) of Windows backup information to a virtual machine. Exporting your data to a virtual standby machine provides you with a high availability copy of the data. If a protected machine goes down, you can boot up the virtual machine to perform recovery.

When you export to a virtual machine, all of the backup data from a recovery point as well as the parameters defined for the protection schedule for your machine will be exported. You can also create a "virtual standby" by having protected data continuously exported from your protected machine to a virtual machine.

NOTE: Only the 3 TB with 2 VMs and 4 TB with 2 VMs configuration of DL1300 supports the onetime export and continuous export on virtual standby VMs.

Performing a one-time Hyper-V export

To perform a one-time Hyper-V export:

- 1. In the Core Console, navigate to the machine you want to export.
- 2. On the Summary tab, click Actions \rightarrow Export \rightarrow One-time. The Export Wizard displays on the Protected Machines page.
- 3. Select a machine for export, and then click Next.
- 4. On the **Recovery Points** page, select the recovery point that you want to export, and then click **Next**.

Defining one-time settings for performing a Hyper-V export

To define one-time settings for performing a Hyper-V export:

- 1. From the Hyper-V dialog box, click **Use local machine** to perform the Hyper-V export to a local machine with the Hyper-V role assigned.
- 2. Click the **Remote host** option to indicate that the Hyper-V server is located on a remote machine. If you selected the Remote host option, enter the parameters for the remote host described as follows:

Text Box	Description
Host Name	Enter an IP address or host name for the Hyper-V server. It represents the IP address or host name of the remote Hyper-V server.
Port	Enter a port number for the machine. It represents the port through which the Core communicates with this machine.
User Name	Enter the user name for the user with administrative privileges for the workstation with the Hyper-V server. It is used to specify the logon credentials for the virtual machine.
Password	Enter the password for the user account with administrative privileges on the workstation with Hyper-V server. It is used to specify the logon credentials for the virtual machine.

- 3. Click Next.
- 4. On the Virtual Machines Options page in the VM Machine Location text box, enter the path or location for the virtual machine. For example, D:\export. The VM location must have sufficient space to hold the VM metadata and virtual drives needed for the virtual machine.
- 5. Enter the name for the virtual machine in the Virtual Machine Name text box.

The name that you enter appears in the list of virtual machines in the Hyper-V Manager console.

- 6. Click one of the following:
 - Use the same amount of RAM as the source machine to identify that the RAM use is identical between the virtual and source machines.
 - Use a specific amount of RAM to specify how much memory the virtual machine has after the export; for example, 4096 MB. (recommended)
- 7. To specify the disk format, next to **Disk Format**, click one of the following:
 - VHDX
 - VHD

NOTE: Hyper-V Export supports VHDX disk formats if the target machine is running Windows 8 (Windows Server 2012) or higher. If the VHDX is not supported for your environment, the option is disabled.

- 8. On the Volumes page, select the volume(s) to export. For the virtual machine to be an effective backup of the protected machine include the protected machine's boot drive. Example. C:\. Your selected volumes should be no larger than 2040 GB for VHD. If the selected volumes are larger than 2040 GB, and the VHD format is selected, you will receive an error.
- 9. On the Summary page, click Finish to complete the wizard and to start the export.

Performing a continuous (virtual standby) Hyper-V export



NOTE: Only the DL1300 3 TB with 2 VMs and 4 TB with 2 VMs configurations support the one-time export and continuous export on virtual standby VMs.

To perform a continuous (virtual standby) Hyper-V export:

- 1. In the Core Console, on the Virtual Standby tab, click Add to launch the Export Wizard. On the Protected Machines page of the Export Wizard.
- 2. Select the machine you want to export and then click Next.
- 3. On the Summary tab, click Export \rightarrow Virtual Standby.
- **4.** From the Hyper-V dialog box, click **Use local machine** to perform the Hyper-V export to a local machine with the Hyper-V role assigned.

5. Click the **Remote host** option to indicate that the Hyper-V server is located on a remote machine. If you selected the Remote host option, enter the parameters for the remote host described as follows:

Text Box	Description
Host Name	Enter an IP address or host name for the Hyper-V server. It represents the IP address or host name of the remote Hyper-V server.
Port	Enter a port number for the machine. It represents the port through which the Core communicates with this machine.
User Name	Enter the user name for the user with administrative privileges for the workstation with the Hyper-V server. It is used to specify the logon credentials for the virtual machine.
Password	Enter the password for the user account with administrative privileges on the workstation with Hyper-V server. It is used to specify the logon credentials for the virtual machine.

- 6. On the Virtual Machines Options page in the VM Machine Location text box, enter the path or location for the virtual machine. For example, D:\export. The VM location must have sufficient space to hold the VM metadata and virtual drives needed for the virtual machine.
- 7. Enter the name for the virtual machine in the Virtual Machine Name text box.

The name that you enter appears in the list of virtual machines in the Hyper-V Manager console.

- 8. Click one of the following:
 - Use the same amount of RAM as the source machine to identify that the RAM use is identical between the virtual and source machines.
 - Use a specific amount of RAM to specify how much memory the virtual machine has after the export; for example, 4096 MB (recommended).
- 9. To specify the Generation, click one of the following:
 - Generation 1 (recommended)
 - Generation 2
- 10. To specify the disk format, next to Disk Format, click one of the following:
 - VHDX (Default)
 - VHD

NOTE: Hyper-V Export supports VHDX disk formats if the target machine is running Windows 8 (Windows Server 2012) or higher. If the VHDX is not supported for your environment, the option is disabled. On the Network Adapters page, select the virtual adapter to be connected to a switch.

- 11. On the Volumes page, select the volume(s) to export. For the virtual machine to be an effective backup of the protected machine include the protected machine's boot drive. Example, C:\. Your selected volumes should be no larger than 2040 GB for VHD. If the selected volumes are larger than 2040 GB, and the VHD format is selected, you will receive an error.
- 12. On the Summary page, click Finish to complete the wizard and to start the export.



NOTE: You can monitor the status and progress of the export by viewing the Virtual Standby or **Events** tab

Managing recovery points

Periodic backup snapshots of all the protected servers accumulate on the Core over time. The retention policies are used to retain backup snapshots for longer periods of time and to help with management of

these backup snapshots. The retention policy is enforced by a nightly rollup process that helps in aging and deleting old backups.

Archiving data

Retention policies enforce the periods for which backups are stored on short-term (fast and expensive) media. Sometimes certain business and technical requirements mandate extended retention of these backups, but use of fast storage is cost prohibitive. Therefore, this requirement creates a need for long-term (slow and cheap) storage. Businesses often use long-term storage for archiving both compliance and noncompliance data. The archive feature in AppAssure is used to support the extended retention for compliance and noncompliance data. It is also used to seed replication data to a remote replica core.

Creating an archive

To create an archive:

1. In the Core Console, click **Tools** \rightarrow **Archive** \rightarrow **Create**.

The Add Archive Wizard dialog box appears.

- 2. On the Create page of the Add Archive Wizard, select one of the following options from the Location Type drop-down list:
 - Local
 - Network
 - Cloud
- **3.** Enter the details for the archive as described in the following table based on the location type you selected in Step 3.

Option	Text Box	Description
Local	Output location	Enter the location for the output. It is used to define the location path where you want the archive to reside; for example, d:\work\archive.
Network	Output location	Enter the location for the output. It is used to define the location path where you want the archive to reside; for example, \\servername \sharename.
	User Name	Enter a user name. It is used to establish logon credentials for the network share.
	Password	Enter a password for the network path. It is used to establish logon credentials for the network share.
Cloud	Account	Select an account from the drop-down list.

Table 11. Creating an archive

Option	Text Box	Description
		NOTE: To select a cloud account, you must first add it to the Core Console. See topic 'Adding A Cloud Account' in <i>Dell DL1300</i> <i>Appliance User's Guide</i> .
	Container	Select a container associated with your account from the drop-down menu.
	Folder Name	Enter a name for the folder in which the archived data is to be saved. The default name is AppAssure-5-Archive-[DATE CREATED]-[TIME CREATED]

4. Click Next.

5. On the Machines page of the wizard, select which protected machine or machines contains the recovery points you want to archive.

6. Click Next.

7. On the **Options** page, enter the information described in the following table.

Text Box	Description
Maximum Size	Large archives of data can be divided into multiple segments. Select the maximum amount of space you want to reserve for creating the archive by doing one of the following:
	 Select Entire Target to reserve all available space in the path provided on the destination provided in Step 4. (for example, if the location is D:\work \archive, all of the available space on the D: drive is reserved).
	• Select the blank text box, use the up and down arrows to enter an amount, and then select a unit of measurement from the drop-down list to customize the maximum space you want to reserve.
	NOTE: Amazon cloud archives are automatically divided into 50 GB segments. Windows Azure cloud archives are automatically divided into 200 GB segments.
Recycle action	Select one of the following recycle action options:
	• Do not reuse : Does not overwrite or clear any existing archived data from the location. If the location is not empty, the archive write fails.
	• Replace this Core : Overwrites any pre-existing archived data pertaining to this core but leaves the data for other cores intact.
	 Erase Completely: Clears all archived data from the directory before writing the new archive.
	 Incremental: Lets you add recovery points to an existing archive. It compares recovery points to avoid duplicating data that already exists in the archive.

Text Box	Description
Comment	Enter any additional information that is necessary to capture for the archive. The comment will be displayed if you import the archive later.
Use compatible format	Select this option to archive your data in a format that is compatible with previous versions of cores.
	NOTE: The new format offers better performance; however it is not compatible with older cores.

- 8. Click Next.
- **9.** On the Date Range page, enter the Start Date and Expiration Date of the recovery points to be archived.
 - To enter a time, click on the time shown (default, 8:00 AM) to reveal the slide bars for selecting hours and minutes.
 - To enter a date, click the text box to reveal the calendar, and then click on the preferred day.

10. Click Finish.

Archiving to a cloud

You can archive your data to a cloud by uploading it to a variety of cloud providers directly from the Core Console. Compatible clouds include Windows Azure, Amazon, Rackspace, and any OpenStack-based provider.

To export an archive to a cloud:

- Add your cloud account to the Core Console. For more information see topic, 'Adding A Cloud Account' in *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.
- Archive your data and export it to your cloud account. For more information see topic, 'Creating An Archive' in *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.
- Retrieve archived data by importing it from the cloud location. For more information see topic, 'Importing An Archive' in *Dell DL1300 Appliance User's Guide* at **Dell.com/support/home**.

Getting help

Finding documentation and software updates

Direct links to AppAssure and DL1300 Appliance documentation and software updates are available from the Core Console.

Documentation

To access the link for documentation:

- 1. On the Core Console, click the **Appliance** tab.
- 2. From the left pane, navigate **Appliance** \rightarrow **Documentation** link.

Software updates

To access the link for software updates:

- 1. On the Core Console, click the **Appliance** tab.
- 2. From the left pane, navigate Appliance \rightarrow Software Updates link.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer-service issues, go to **software.dell.com/support**.

Documentation feedback

Click the **Feedback** link in any of the Dell documentation pages, fill out the form, and click **Submit** to send your feedback.