# Dell PowerProtect Data Manager Appliance Configuration Best Practices

July 2023

H19361.2

White Paper

Abstract

This white paper discusses PowerProtect Data Manager Appliance deployment, planning, and implementation practices for customers, partners, and Dell employees. It describes best practices for the efficient deployment and configuration of the appliance.

## Copyright

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

# Contents

# Executive summary

## Overview

Successful businesses recognize the importance of data protection. Demand is increasing for data protection solutions that are powerful, scalable, and easy to use. Scalability, ease of use, and efficiency are among the top priorities for business and IT teams today.

In response to market demands for next-generation data management software platforms and integrated appliances, Dell Technologies introduces Dell PowerProtect Data Manager Appliance. The appliance helps organizations transform IT faster while being confident that their data is secure and available for business operations.

PowerProtect Data Manager Appliance is an integrated solution that offers industry-leading deduplication, data protection, and multicloud capabilities. Powering the appliance is the Dell PowerEdge R740xd2 server, which offers flexible capacity and performance resources to address data-intensive workloads, ensuring the highest levels of application availability, security, and performance. The appliance also employs Role Based Access Control (RBAC), providing an additional layer of security.

With PowerProtect Data Manager Appliance, your data is always available, secure, and storage optimized.

## Audience

The information in this paper is intended for customers who are responsible for planning, implementing, administering, or auditing security controls in environments that contain PowerProtect Data Manager Appliance solutions. The primary audience is Customer Service and remote Professional Services engineers.

## Revisions

| Date | Part number/ revision | Description |
|---|---|---|
| November 2022 | H19361 | Initial release |
| April 2023 | H19361.1 | Revised for Data Manager Appliance DM5500 5.13.0.0:<br>• Updated introduction (appliance features), hardware composition (SAS card), download filename, screenshots, resources<br>• Added sections about physical network separation and appliance reconfiguration<br>• Updated documentation references |
| July 2023 | H19361.2 | Revised for Data Manager Appliance DM5500  5.14.0.0:<br>• R3 new feature details |

## We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

**Author:** Sandeep Rajagopal
**Contributors**: Scott DeFlaminio, Sonali Verma

**Note**: For links to other documentation for this topic, see the PowerProtect Data Manager Appliance Info Hub.

# Introduction

PowerProtect Data Manager Appliance is an integrated solution that offers deduplication and data protection capabilities. PowerProtect Data Manager Appliance supports a large ecosystem of traditional and modern workloads. These workloads include replication, instant access, instant restore, search, monitoring and reporting, cloud readiness, disaster recovery, and long-term retention to the cloud.

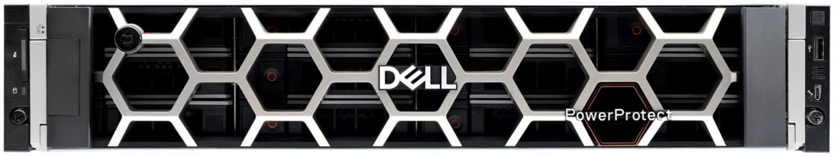


**Figure 1. PowerProtect Data Manager Appliance**

PowerProtect Data Manager Appliance provides the following features:

- **Integrated customer experience**—PowerProtect Data Manager Appliance simplifies the steps needed to configure the appliance. Going beyond simplified appliance configuration, the appliance offers an end-to-end integrated UI experience by delivering unified management, alert, and native reporting capabilities.
- **Simplified appliance networking**—PowerProtect Data Manager Appliance requires only three public IP addresses on the customer's network for configuration. One IP address is required to carry management traffic, and two IP addresses are required to handle data traffic for workloads protected by the appliance.

  In addition, the appliance supports multiple networks to load-balance the management and data traffic network channels.
- **Identity and Access Management (IAM)**—PowerProtect Data Manager Appliance uses IAM to provide centralized authentication, authorization, single sign-on, and user management capabilities. IAM offers a unified appliance login experience and enhanced security by using Role Based Access Control (RBAC).
- **Multi-factor authentication (MFA)—**MFA is an authentication method that requires the user to provide two or more verification factors to gain access to a system. PowerProtect Data Manager Appliance adds layers of security beyond usernames and passwords by using MFA with Google Authenticator and Microsoft Authenticator, preventing unauthorized access to the system. MFA is disabled by default. When MFA is enabled, the PowerProtect Data Manager Appliance UI prompts you for a verification code, also known as a time-based one-time password (TOTP), after you sign in with your username and password. As a result, your appliance and data are protected from unauthorized access.
- **Active Directory support**—Active Directory is Microsoft's proprietary directory service that enables administrators to manage permissions and access to network resources.

  PowerProtect Data Manager Appliance uses secure Active Directory as an external identity provider for users and groups. When mapped to Active Directory, users in the group can exercise their respective privileges on the appliance based on the role assigned.

- **Physical network separation**—PowerProtect Data Manager Appliance allows customers to physically separate networks based on their needs. This separation is possible through the use of the appliance's additional PCIe slot for these distinct networks. Use cases for distinct networks include backup, replication, long-term retention, and Data Domain Cloud Disaster Recovery.
- **Cyber Recovery**—The Cyber Recovery solution protects mission-critical business data and technology configurations from ransomware and other threats by maintaining them in a secure, air-gapped "vault" that is physically isolated from an unsecure system or network.
  - The Cyber Recovery solution enables access to the Cyber Recovery vault only long enough to replicate data from the production system. At all other times, the Cyber Recovery vault is secured and off the network.
  - Once the data is secured in the vault, CyberSense identifies suspicious activity through its machine learning technology and allows for recovery of known good data and resumption of normal business operations.
- **Retention Lock Compliance**—Retention Lock Compliance allows you to meet the strictest data permanence requirements of regulatory standards.
  - Any data that is locked cannot be overwritten, modified, or deleted for a user-defined retention period or until Indefinite Retention Hold, if being used, is disabled.
  - Retention Lock Compliance requires a security officer user to be present (or created, if not existing), a security officer authorization policy to be enabled using the security officer, and an iDRAC read-only user to be present (or configured, if not existing).
  - Retention Lock Compliance must be enabled on the system level and storage unit level before it can be enabled on the policy level:
    - After enabling the retention lock on the system level, a storage unit with retention lock mode must be created.
    - Then, the policy must be set up using the retention-locked storage unit, with retention lock enabled on the policy level.

    The backups taken using the retention lock enabled policy will then have their copies locked to ensure that data integrity is maintained.
- **Replication to external Dell PowerProtect DD/DDVE system**—DM5500 requires backups to be written to the local appliance storage. However, customers will want to be able to replicate those backups to traditional Data Domain platforms—either to reuse existing systems or support multiple DM5500s replicating into a single larger target.
  - The external PowerProtect DD/DDVE could serve as a centralized remote data center with larger capacity and hold data for longer retention time.
  - The external PowerProtect DD/DDVE can either be on-premises or at the remote site.

  - DD Boost file-replication encryption should be enabled on both the DM5500 and external PowerProtect DD/DDVE.

  **Note**: On DM5500, DD Boost file-replication encryption is enabled, by default, unless the configuration has been changed.

  Before configuring the replication policy, the file-replication encryption must be enabled on the target, and the external PowerProtect DD/DDVE must be added as a replication target on DM5500 through the DM5500 UI .

  **Note**: On PowerProtect DD systems with DDOS versions earlier than 7.10, both the replication encryption and authentication modes must match the appliance (source) default setting, which is encryption enabled and authentication mode set to two-way. This match between the appliance and replication target system is necessary for replication to function as expected.

- **Appliance reconfiguration**—With PowerProtect Data Manager Appliance, customers can modify configuration parameters—such as the default management and data networks, and DNS, NTP, time zone, and location settings—post deployment without affecting data integrity.
- **Audit logging—**PowerProtect Data Manager Appliance enables customers to conduct audit logging to ensure that the system is secure. Audit logging is the process of documenting activity within or across systems to assist with meeting standards and debugging security issues.
- **SAS card inclusion**—Beginning with version 5.13.0.0 of the PowerProtect Data Manager Appliance, the factory includes a SAS HBA card in PCIe slot 5 to allow storage expansion beyond 96 TB for future releases.
- **Perpetual licensing model**—PowerProtect Data Manager Appliance adopts a perpetual licensing model with backend capacity utilization. The system is preconfigured with a default storage capacity license of 12 TB. To increase the storage capacity, you must apply for additional capacity licenses, which are available in 12 TB increments to a maximum of 96 TB.
- **Support for proven and modernized workloads**—PowerProtect Data Manager Appliance offers differentiated VMware protection. It uses the transparent snapshots data mover (TSDM) framework while still upholding the core values of data protection, data availability, deduplication, operational agility, self-service, and IT governance. The appliance supports various traditional workloads, including file systems, SQL, SAP HANA, Oracle, and modern cloud-native Kubernetes workloads.

PowerProtect Data Manager Appliance provides an efficient and comprehensive data protection solution for your modernized workloads with a simplified user interface that is easy to navigate. It streamlines the data protection process and reduces the number of steps required for creation of backups, replication, recovery, expansion, and upgrades. The appliance addresses the issue of copy sprawling, so that monitoring, managing, and analyzing copies of data are no longer tedious tasks.

PowerProtect Data Manager Appliance provides centralized governance that helps mitigate risk and assures compliance of service-level agreements (SLAs) and service-level objectives (SLOs) through simple protection workflows.

PowerProtect Data Manager Appliance enables automated discovery and onboarding of:

- Filesystems
- Databases
- Virtual machines
- Kubernetes clusters
- NAS

- **Multicloud-optimized**—Multicloud continues to be the path forward in today’s era of massive growth and distribution of data for our customers. Data protection offerings are being enhanced to enable various cloud providers as consumers embark on this path.

  The multicloud-optimized PowerProtect Data Manager Appliance offers a solution for effective long-term retention and disaster recovery of customer data.

- **Storage-optimized and performance-optimized**—In today's world, the cost and efficiency of a solution are important considerations for most businesses. Customers are always looking for solutions that enable cost-effective and efficient use of storage infrastructure and resources.

  PowerProtect Data Manager Appliance delivers deduplication and compression using gzfast as the default algorithm for optimal storage consolidation across the system. The system also uses a hardware-assisted compression card that allows for the highest compression of incoming data without sacrificing performance.

- **Improved Data Invulnerability Architecture (DIA) using protection pools**—PowerProtect Data Manager Appliance uses DIA to ensure safe and reliable data storage. By performing a full-featured end-to-end verification of incoming data, fault avoidance, and containment, the DIA architecture ensures that customers can retrieve their data with confidence. It also protects against failures of both hardware and software that might result in data loss.

  In addition, the system uses a new software-defined RAID technology in the form of protection pools. A protection pool is a patented technology of Dell Technologies. It enables linear scaling of capacity and eliminates the need for separate spare drives, dedicated cloud tier storage, or overprovisioning disks. Protection pools ensure that the services have direct access to the underlying storage without any intervention from the hardware layer. The technology provides better control of storage consolidation, fault avoidance, and self-healing capabilities for the appliance.

# PowerProtect Data Manager Appliance hardware composition

PowerProtect Data Manager Appliance is powered by the Dell PowerEdge R740xd2 server. It provides resiliency of the data protection service, ensuring the highest levels of application availability.

PowerProtect Data Manger Appliance is a 2U server with two drives bays. Each drive bay has 12 drives for a total of 24 drives. Other components include:

- 2 x 5218R 20-core, 2.1 GHz Cascade Lake Intel CPUs
- 384 GB RAM or 12 x 32 GB DIMMs
- 20 x 12 TB hard drives
  - 2 for internal storage, 6+2 base for protection storage, 10 expansions
  - 12 TB to 96 TB usable at capacity in 2U (cloud tier @ 2:1)
- 2 x 1 TB (960 GB) SSD for operating system/boot
- 1 x 1.92 TB, 1 x 3.84 TB cache SSD (metadata cache, IA/IR)
- Mirrored IDSDM 16 GB SD cards for boot recovery
- Hardware-assisted compression card
- 10 GbE/25 GbE networking
- 12 Gbps SAS card (Dell HBA 355e-s)

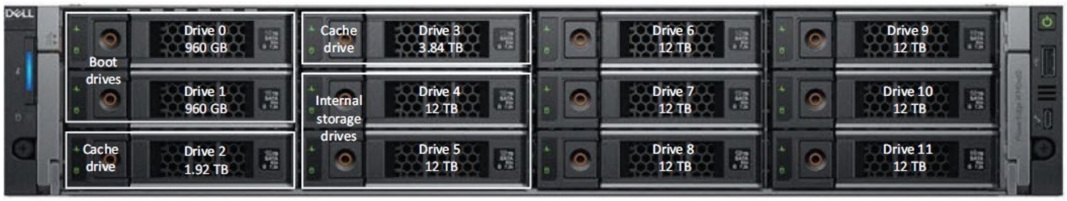


**Figure 2. Front disk layout (drive bay 1)**

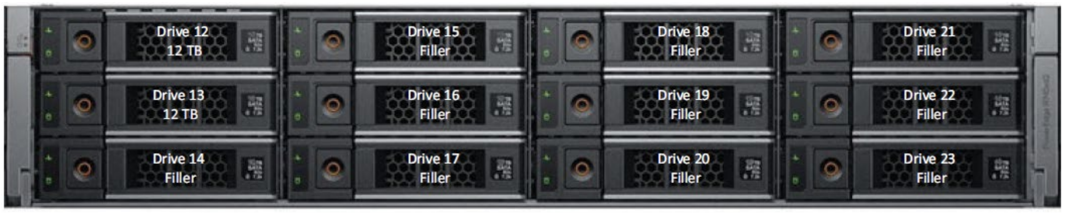


**Figure 3. Middle disk layout (drive bay 2)**

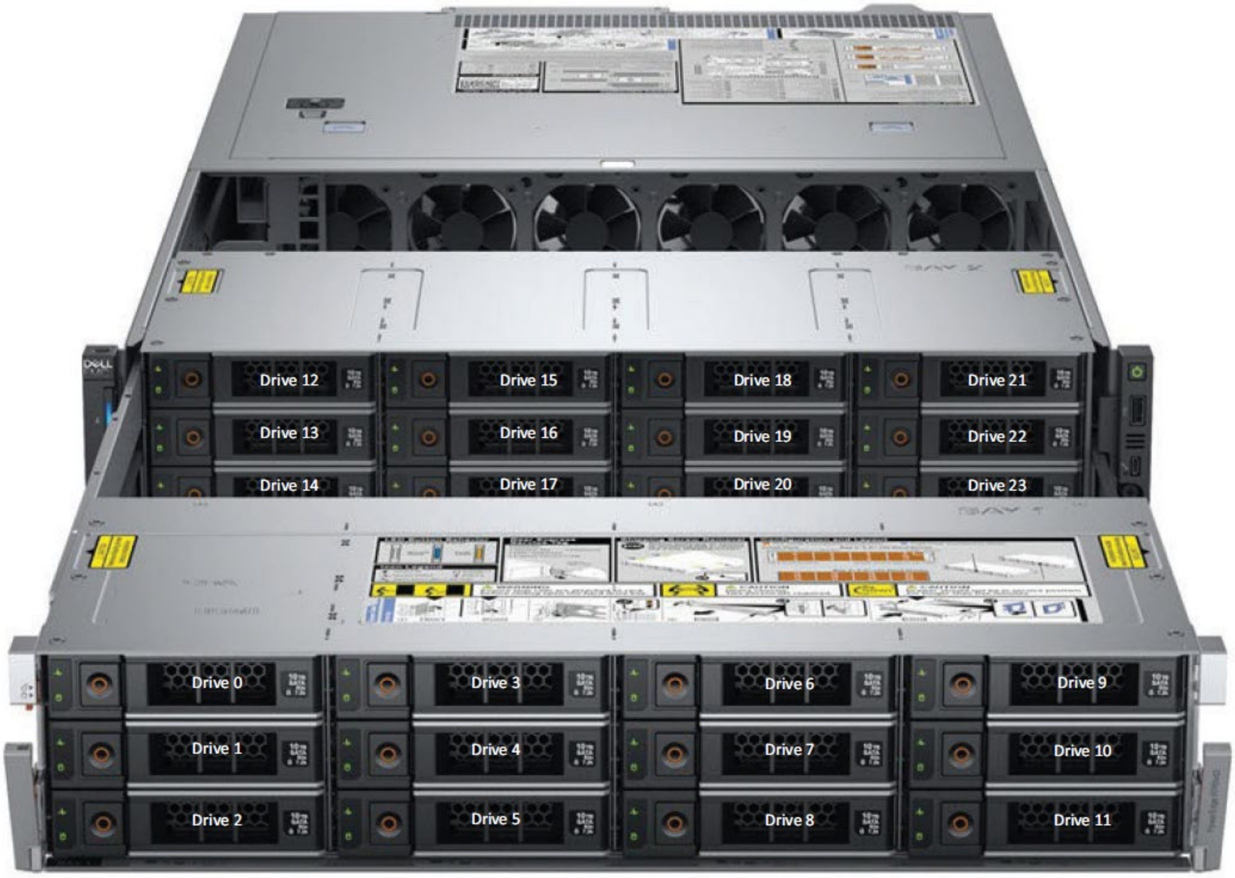


**Figure 4. View of drive bay extended**

**Note**: Customers can order the system based on usable capacity of 24 TB or 96 TB. The drive bays are populated depending on the order type. For example, if the customer orders a system with 24 TB capacity, slots 0 to 13 are populated; a system with 96 TB capacity has both drive bays fully populated.

A system with 24 TB configuration is shipped with only one SSD (1.92 TB) used for the cache tier; slot 3 is empty.

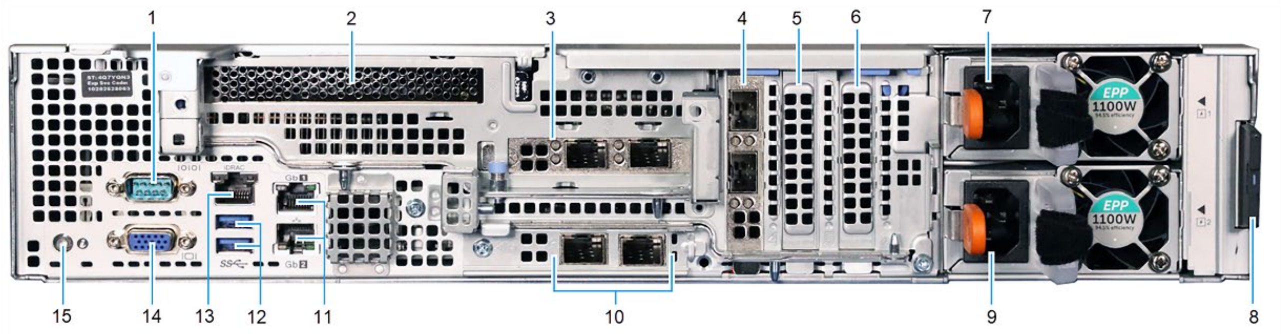


**Figure 5. Rear view of PowerProtect Data Manager Appliance**

The following table describes the back panel features of PowerProtect Data Manager Appliance:

**Table 1. PowerProtect Data Manager Appliance back panel**

| Figure 5 callout | Description |
|---|---|
| 1 | Serial port |
| 2 | Intel hardware-assisted compression (QAT) card (PCIe slot 2) |
| 3 | Dual or quad port HBA (PCIe slot 3)<br>Can be configured to run as two 10/25 GbE SFP28 ports, two 10 GbE SFP+ ports, or four 10 GBT ports |
| 4 | Dual or quad port HBA (PCIe slot 4)<br>Can be configured to run as two 10/25 GbE SFP28 ports, two 10 GbE SFP+ ports, or four 10 GBT ports |
| 5 | Dual-port HBA (2 x SAS 12 Gbps) (PCIe slot 5) |
| 6 | Filler (unused) PCIe expansion card (PCIe slot 6) |
| 7 | Power supply unit (PSU 1)<br>PSU 1 can be 1100 W or 1600 W but must be the same wattage as PSU 2. |
| 8 | Information tag with the DM5500 Serial Number (PSNT)<br>The pull-out information tag contains a white label with the 14-character DM5500 serial number. The complete serial number (PSNT) plus a prefix of dm@ is the initial default password for the PowerProtect Data Manager Appliance UI. |
| 9 | Power supply unit (PSU 2)<br>PSU 2 can be 1100 W or 1600 W but must be the same wattage as PSU 1. |
| 10 | LAN on motherboard (LOM) Ethernet port (2) (PCIe slot 1)<br>Can be configured to run as 10/25 GbE SFP28, 10 GbE SFP+, or 10 GBT |
| 11 | Ethernet port (Gb1); service port used for initial DM5500 login<br>You can use this Gb1 port or the Gb2 port for the initial DM5500 login. |
| 12 | USB 3.0 port (2) |
| 13 | iDRAC9 dedicated network port |
| 14 | VGA port |
| 15 | System identification button |

**Note**: For information about hardware and software requirements for installation and the procedure to rack and stack the appliance, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Installation Guide*.

# Licensing of PowerProtect Data Manager Appliance

As previously noted, PowerProtect Data Manager Appliance is equipped with a default storage capacity license of 12 TB. To increase the storage capacity, you must apply additional capacity licenses. Licenses are available in 12 TB increments to a maximum of 96 TB.

The Dell Electronic Licensing Management System (ELMS) issues the license for the requested capacity. You can also upload the license file manually through the UI, or the appliance can automatically fetch the license from ELMS. The required appliance capacity is enabled once the license is applied successfully.

**Note:** The default capacity license of 12 TB is valid for 90 days, as noted by warnings in the appliance UI. For information about license activation, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Administration Guide*.

# Cabling and network ports requirements

## Prerequisite

To successfully connect and power on PowerProtect Data Manager Appliance, first ensure that the appliance is installed in the rack.

**Note:** For information about hardware and software requirements for installation and the procedure to rack and stack the appliance, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Installation Guide*.

## Connect power cables

Ensure that the rack that contains PowerProtect Data Manager Appliance contains two PDUs connected to different power sources for redundancy.

Redundant power sources allow one AC source to fail or be serviced without affecting appliance operation. On PowerProtect Data Manager Appliance, connect PSU 0 to one AC source and PSU 1 to the other AC source.

**Note**: We are only connecting the power cables to the appliance. To power on the appliance, see Installation overview.

## Connect iDRAC cable

Integrated Dell Remote Access Controller (iDRAC) provides an out-of-band method for remote management. iDRAC is optional but highly recommended.

iDRAC allows you to:

- Power the appliance on and off for required maintenance activities.
- Enable Dell Support to gather detailed information about the state of the hardware.

**Note**: iDRAC uses a 1GBASE-T Ethernet connection. The 1 GbE management switch to which the Category 5 or 6 iDRAC cable connects must have RJ45 connections.

## Connect network cables

This section describes onsite networking, switch, and cabling requirements and considerations for successfully configuring PowerProtect Data Manager Appliance.

Dell Technologies recommends having five network cables.

**Note**: Network card types cannot be mixed and matched (optical and copper). Similarly, the network speeds cannot be mixed and matched.

**Table 2. Physical network port type on PowerProtect Data Manager Appliance**

| Type of switch recommended (customer network) | NIC type on the appliance | Transceiver | Speed | Cable required |
|---|---|---|---|---|
| 1 Gb RJ45 | 1GBASE-T Ethernet | Not applicable | 1 Gb | Category 5e or Category 6 |
| 25 Gb SFP28 | SFP28 (optical) | SPF28 duplex LC/ DAC | 25 Gb | LC to LC with SR optical GBICs or copper Twinax DAC cables |
| 10 Gb SFP+ | SFP+ (optical) | SFP+ duplex LC/ DAC | 10 Gb | LC to LC with SR optical GBICs or copper Twinax DAC cables |
| 1 Gb or 10 Gb RJ45 | SFP+ (optical) | SFP RJ45 | 1 Gb | UTP with RJ45 (Category 5e or Category 6) |
| 1 Gb or 10 Gb RJ45 | 10GBASE-T (RJ45) | Not applicable | 1 Gb or 10 Gb (depending on switch) | UTP/STP with RJ45 (Category 6a or Category 7) |

As part of the standard installation, the appliance uses four ports. Two ports are used for load balancing of management traffic, and two ports are used for data traffic/uplinks to the customer's network switch.

To achieve improved reliability and fault tolerance for the management interface, connect port 1 of LOM PCIe slot 1 and port 1 of PCIe slot 4 to different network switches at the customer site. Similarly, to achieve better performance and reliability for the data traffic, connect port 2 of LOM PCIe slot 1 and port 2 of PCIe slot 4 to different network switches at the customer site:

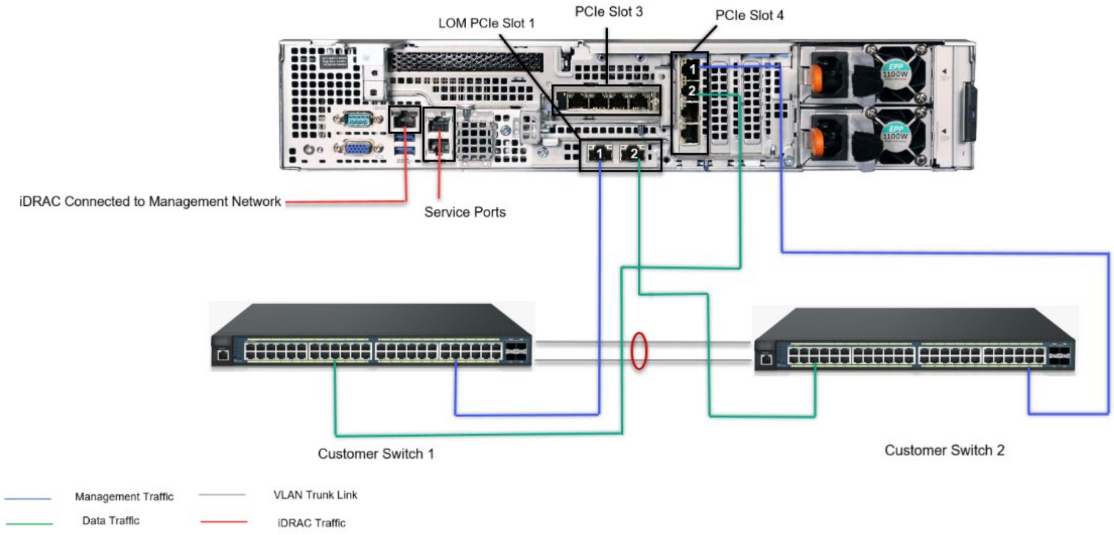


**Figure 6. Recommended network settings for PowerProtect Data Manager Appliance**

**Note**: A copper-based appliance has four physical network cards (NICs) on PCIe slot 4. When setting up the initial connection, always connect ports 1 and 2 (top to bottom) on the appliance.

The following table shows the combinations of NIC ports available on PowerProtect Data Manager Appliance. The number of available ports depends on the customer's choice of appliance, with a maximum of six optical ports and ten copper ports available for consumption.

**Table 3. NIC combinations on PowerProtect Data Manager Appliance**

| LOM (PCIe slot 1) | NIC (PCIe slot 3) | NIC (PCIe slot 4) | Number of NIC ports |
|---|---|---|---|
| 2 x 10/25GbE SFP28 | 2 x 10/25 GbE SFP28 | 2 x 10/25 GbE SFP28 | 6 x 10/25 GbE SFP28 |
| 2 x 10 GbE SFP+ | 2 x 10 GbE SFP+ | 2 x 10 GbE SFP+ | 6 x 10 GbE SFP+ |
| 2 x 10 GBT | 4 x 10 GBT | 4 x 10 GBT | 10 x 10 GBT |

Note the following networking considerations for the appliance at the customer site:

- For redundancy and fault tolerance, configure the appliance with two switches.
- You must turn off Cisco port security on the customer uplink ports.
- Uplinks to the customer's switch can support separation with multiple VLANs. The appliance can be configured to support up to 80 VLANs (with trunk mode).

**Note**: The initial configuration of the appliance supports a single VLAN. After initial configuration, VLANs can be added to the appliance through the PowerProtect Data Manager Appliance UI.

- The appliance can be configured successfully with the switch ports as access (untagged) or trunked (tagged) ports. However, trunk mode is recommended.

| Switch port configuration | External network VLAN ID |
|---|---|
| Tagged (trunk mode) (recommended) | VLAN ID that corresponds to customer network |
| Untagged (access mode) | 0 |

## Physical network separation

Uplinks are physical network interface links that connect a machine to the network. An uplink enables a machine to join a network, operate as a member of the network, and communicate with other machines on the network. An uplink transports network traffic from a machine to the network with which it is associated and then routes the traffic back to the machine.

Benefits of using uplink groups include:

- **Load balancing**: If an uplink group consists of a set of uplinks, load balancing algorithms ensure that the network packets that are going through the uplink group are evenly distributed across the uplinks in the uplink group.
- **Failover**: If an uplink in an uplink group fails or breaks, network traffic is sent through other uplinks in the uplink group.

Uplinks are used to physically separate network data. This separation is possible through the use of the appliance's additional PCIe slot (slot 3 or 4, based on the appliance type) for these distinct networks.

PowerProtect Data Manager Appliance has uplinks that provide connectivity to the users' network. Manage these uplinks through the uplink group mechanism. Apply different load balancing and failover algorithms to the uplink group.

**Note**: A PowerProtect Data Manager Appliance uplink group can have one or two uplinks.

**Note:** Physical network separation is a post-deployment activity. For information about how to configure network separation, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Administration Guide*.

## Network connectivity

PowerProtect Data Manager Appliance has simplified networking requirements, which is one of its key differentiating factors. Configuring the appliance using only two public interfaces is possible, however, using three is recommended.

The following table details the number of IP addresses that are required for various components of PowerProtect Data Manager Appliance.

**Table 4. IP address requirements**

| Required number of IP addresses | Component | DNS entry | Remarks |
|---|---|---|---|
| 1 | iDRAC (optional but recommended) | No | We recommend that you configure the iDRAC network on a subnet and switch separate from the management and data network. |
| 1 | Management traffic | Yes | A separate subnet or the same subnet as the data network can be configured. |
| 1 | Data traffic 1 | No | A separate subnet or the same subnet as the management network can be configured. |
| 1 | Data traffic 2 (optional but recommended) | No | A separate subnet or the same subnet as the management network can be configured. |

# Installation overview

## Power on the appliance

### Prerequisites

Before you can power on the appliance, ensure that:

- The appliance is installed in the rack.
- The power cables are connected.
- The appliance is cabled to the switches.
- iDRAC cables are connected to the appliance.

### Powering on the appliance

Power on the appliance by pressing the power button on the front right corner.

When the appliance is powered on, the power icon on the button lights up green ⏻, and the LED displays a solid blue line.

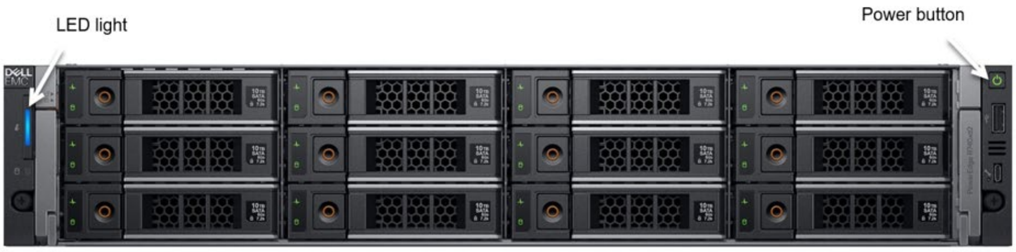


**Figure 7. Powering on PowerProtect Data Manager Appliance**

## Assign static IP address to the management workstation

The management workstation helps you to configure PowerProtect Data Manager Appliance on the customer's network.

Connect the management workstation and assign the static IP address as follows:

1. Connect the management workstation to the service port on the back of the appliance using a Category 5 or Category 6 cable.

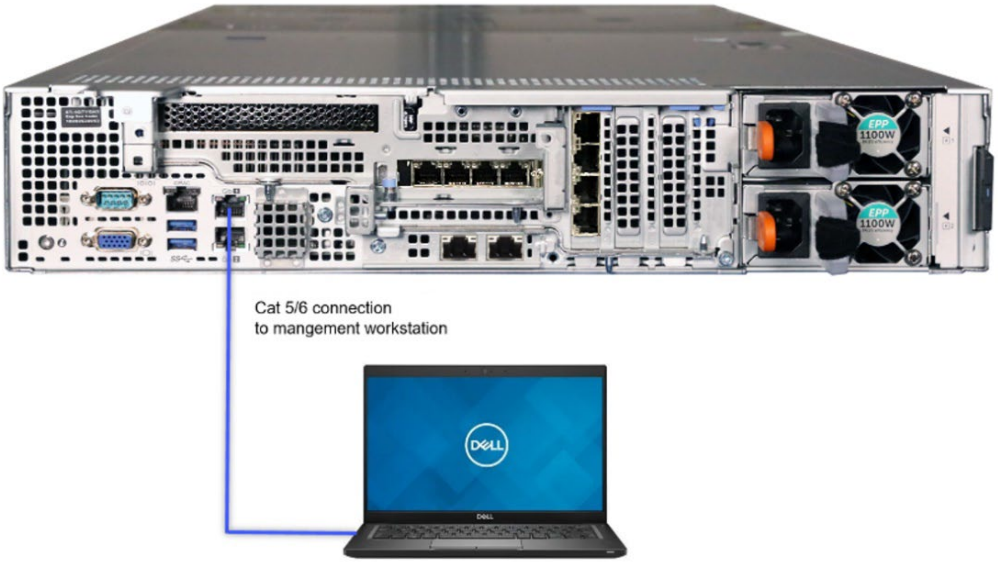
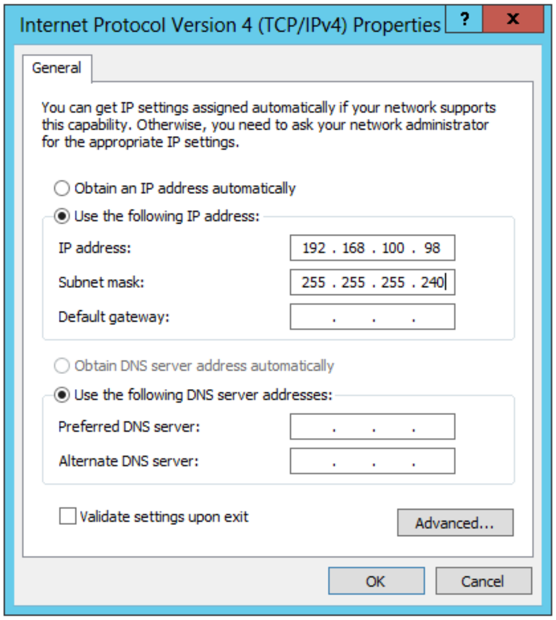


**Figure 8. Management workstation connection**

2. Assign the static IP address of 192.168.100.98 to the management workstation and the subnet mask of 255.255.255.240 for the Ethernet interface that is connected to the appliance.

   A default gateway is not required.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 100 . 98

Subnet mask: 255 . 255 . 255 . 240

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

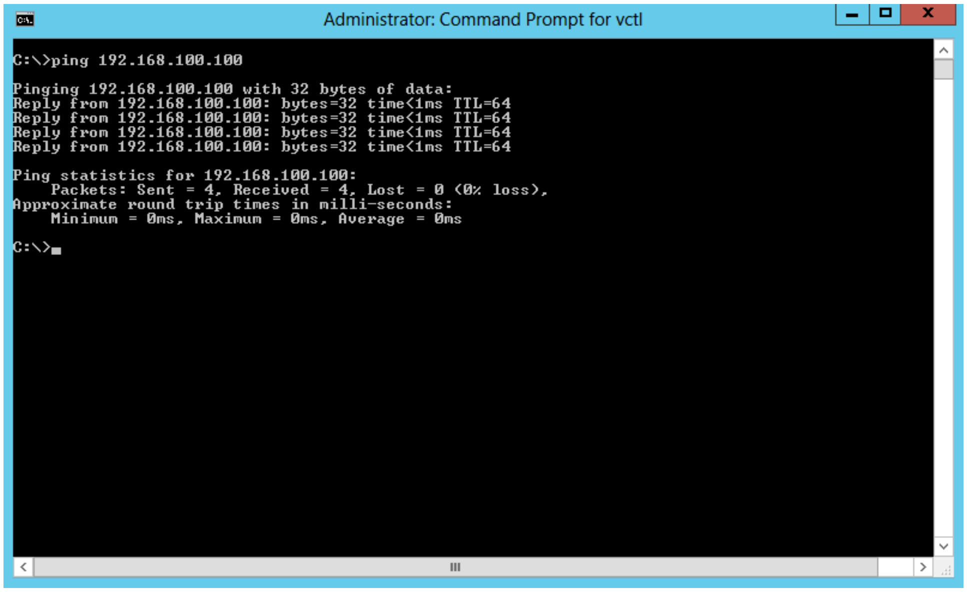
**Figure 9. Management workstation Ethernet settings**

---

**Note**: For information about how to assign a static IP address for Windows and Mac operating systems, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Installation Guide*.

---

3. Open the command prompt on the management workstation and ping the 192.168.100.100 management IP address of the appliance to verify that you can reach it.



```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:
Reply from 192.168.100.100: bytes=32 time<1ms TTL=64
Reply from 192.168.100.100: bytes=32 time<1ms TTL=64
Reply from 192.168.100.100: bytes=32 time<1ms TTL=64
Reply from 192.168.100.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

**Figure 10. Command prompt on management workstation**

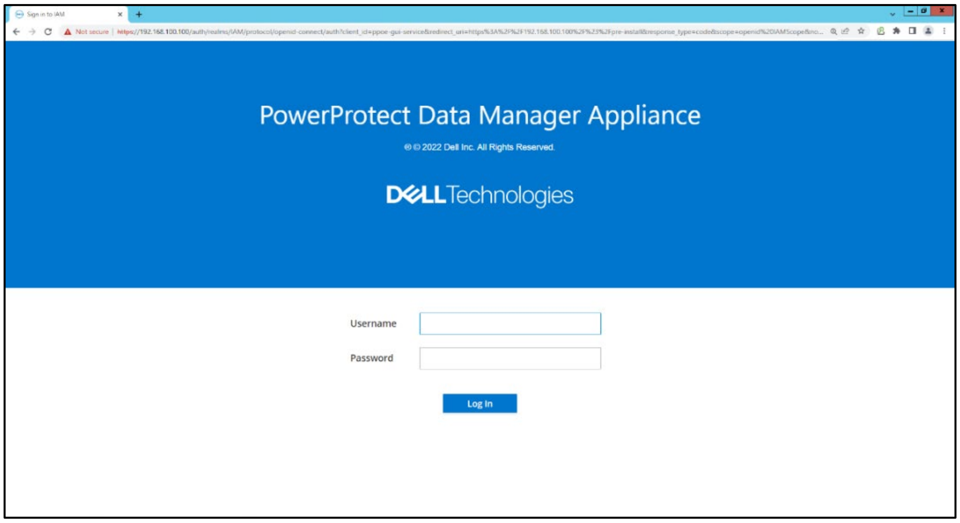
## Configure the appliance

Configure the appliance as follows:

1. Log in to the PowerProtect Data Manager Appliance configuration UI by entering the following URL in your browser's address bar:

   `https://192.168.100.100`

   The PowerProtect Data Manager Appliance configuration UI is displayed.


Sign in to IAM
Not secure
https://192.168.100.100/auth/realms/IAM/protocol/openid-connect/auth?client_id=ppoe-gui-service&redirect_uri=https%3A%2F%2F192.168.100.100%2F%23%2Fpre-install&response_type=code&scope=openid%20IAMScope&no...

PowerProtect Data Manager Appliance

®© 2022 Dell Inc. All Rights Reserved.

DELL Technologies
Username
Password
Log In

**Figure 11. PowerProtect Data Manager Appliance configuration UI**

2. In the configuration UI, log in using the administrator credentials, where the password is `dm@` followed by the appliance serial number (PSNT).

   **Note**: The PSNT is on the pull-out information tag on the back of the server, to the right of the PSUs.

   For example, if the PSNT is DPDIH220124121, the password would be `dm@DPDIH220124121`.

3. Click **Login**.

4. On the **Create Secure Credentials** page, perform the following actions:

   a. In the **Current Password field**, enter the appliance serial number (PSNT) with the prefix `dm@`.

   By default, the **New Admin Username** field is set to **admin**.

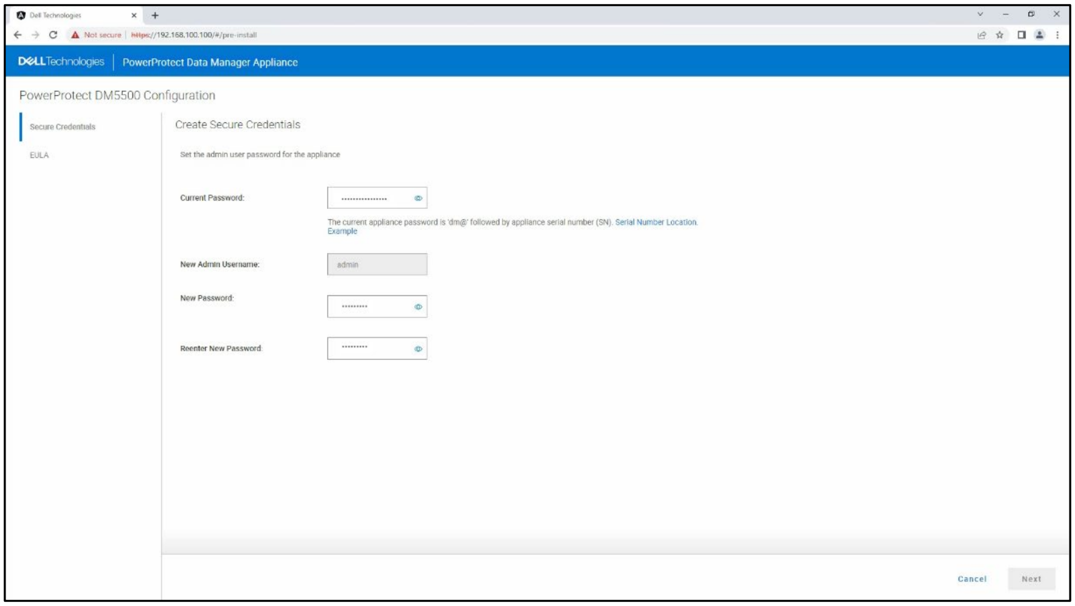
   b. In the **New Password** and **Reenter New Password** fields, specify a new admin user password.

   After deployment, use the updated password to log in to PowerProtect Data Manager Appliance.

   Ensure that the password meets the following requirements:

   - Minimum of nine characters and a maximum of 16 characters
   - At least one numeric character (0-9)
   - At least one uppercase character (A-Z)
   - At least one lowercase character (a-z)
   - At least one special character from the following list of acceptable characters:

     !@#$%^&*()<>?



PowerProtect DM5500 Configuration

Create Secure Credentials

Set the admin user password for the appliance

Current Password: ················

The current appliance password is 'dm@' followed by appliance serial number (SN). Serial Number Location. Example

New Admin Username: admin

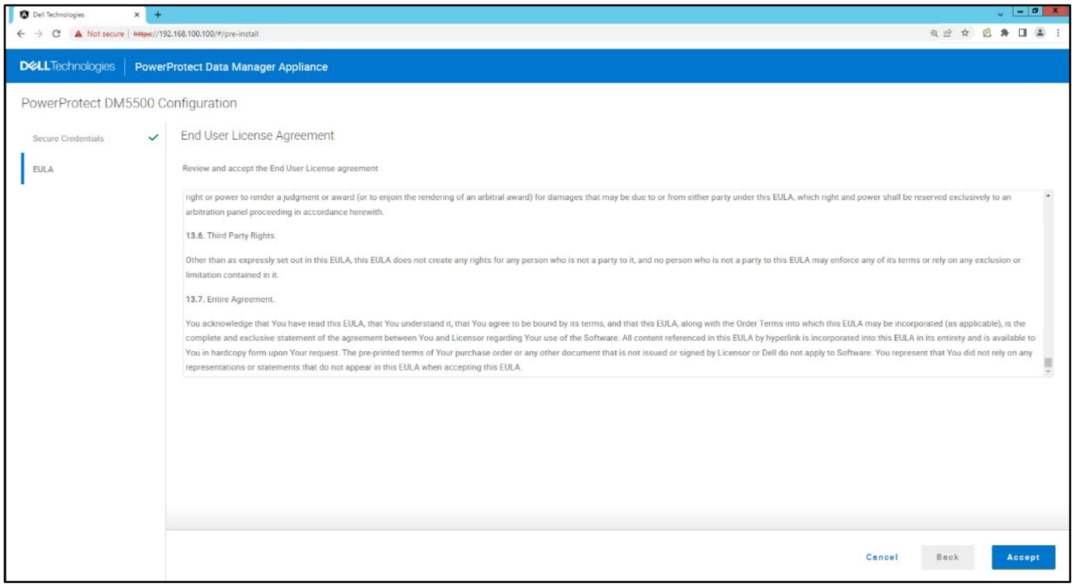
New Password: ·········

Reenter New Password: ·········

**Figure 12. PowerProtect Data Manager Appliance credentials**

5. Click **Next**.

   The End User License Agreement is displayed.



Dell Technologies
Not secure | https://192.168.100.100/#/pre-install
DELLTechnologies | PowerProtect Data Manager Appliance

PowerProtect DM5500 Configuration

Secure Credentials ✓
EULA

End User License Agreement

Review and accept the End User License agreement

right or power to render a judgment or award (or to enjoin the rendering of an arbitral award) for damages that may be due to or from either party under this EULA, which right and power shall be reserved exclusively to an arbitration panel proceeding in accordance herewith.

13.6. Third Party Rights.

Other than as expressly set out in this EULA, this EULA does not create any rights for any person who is not a party to it, and no person who is not a party to this EULA may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.7. Entire Agreement.

You acknowledge that You have read this EULA, that You understand it, that You agree to be bound by its terms, and that this EULA, along with the Order Terms into which this EULA may be incorporated (as applicable), is the complete and exclusive statement of the agreement between You and Licensor regarding Your use of the Software. All content referenced in this EULA by hyperlink is incorporated into this EULA in its entirety and is available to You in hardcopy form upon Your request. The pre-printed terms of Your purchase order or any other document that is not issued or signed by Licensor or Dell do not apply to Software. You represent that You did not rely on any representations or statements that do not appear in this EULA when accepting this EULA.

**Figure 13. PowerProtect Data Manager Appliance End User License Agreement**

6. Review the license agreement and click **Accept**.

   The **Network** page is displayed.

7. On the **Network** page, in the **Network** section, perform the following actions:

   a. In the **Management IP** field, specify an IP address.

   b. In the **Management FQDN** field, specify a FQDN name for the management interface.

   c. In the **Management Domain name** field, specify a domain name for the management FQDN.

   d. In the **Data IP 1** field, specify an IP address.

   e. (Optional) In the **Data IP 2** field, specify an IP address.

8. In the **Management VLAN** section, perform the following actions:

   a. In **the Management VLAN ID** field, specify a numerical VLAN ID.

      If the switch port is tagged (trunk mode), provide the correct VLAN ID that corresponds to the customer network. If the switch port is untagged (access mode), use VLAN 0. However, trunk mode is recommended.

   b. In the **Management subnet mask** field, specify a subnet mask.

   c. In the **Management Gateway** field, specify a gateway IP address.

      In the **MTU field**, the maximum transition units (MTU) value is set to 1500.

   d. In the **Bonding options** list, the port bonding configuration is set to **Active-Active** so that all ports actively load balance the internal network traffic. Active/active bonding does not require any corresponding switch-side settings.

9. In the **Data VLAN** section, perform the following actions:

   a. Select the separate **Data Network checkbox option** if you want the data network to be different than the management network. When this checkbox is selected, the **Data VLAN ID, Data subnet mask, Data Gateway** fields are unpopulated, and the user can key in the corresponding values.

   b. In the **Data VLAN ID** field, specify a numerical VLAN ID.

   **Note**: If the switch port is tagged (trunk mode), provide the correct VLAN ID that corresponds to the customer network. If the switch port is untagged (access mode), use VLAN 0. However, trunk mode is recommended.

   c. In the **Data subnet mask** field, specify a subnet mask.

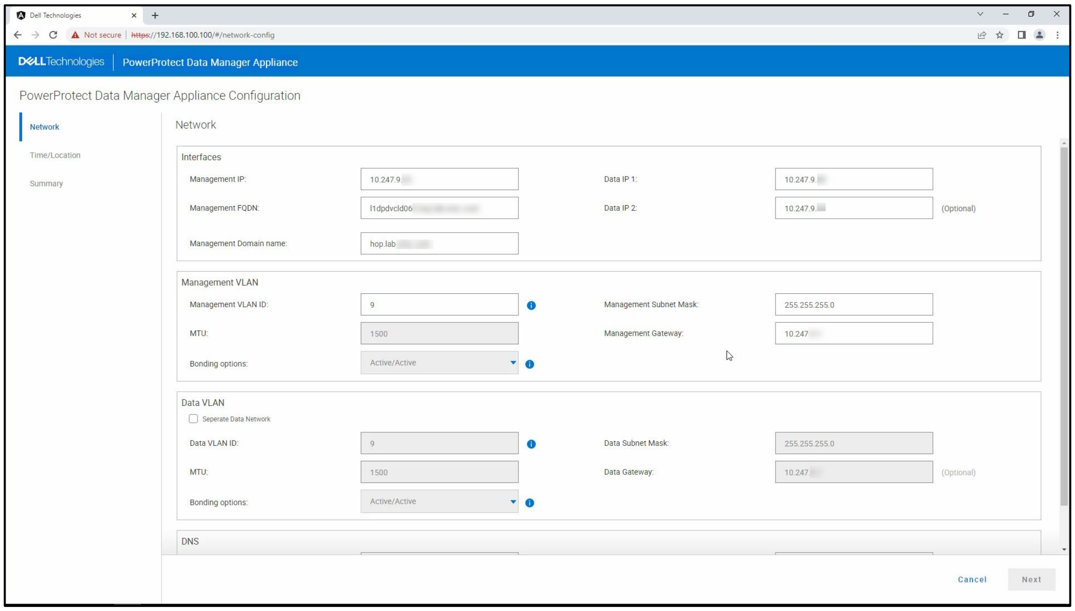
   d. In the **Data Gateway field**, specify a gateway IP address.

   e. In the **MTU field**, the maximum transition units (MTU) value is set to 1500.

   f. In the **Bonding options** list, the port bonding configuration is set to **Active-Active** so that all ports actively load-balance the internal network traffic. Active/active bonding does not require any corresponding switch-side configuration.

10. In the **Primary DNS Server** field, specify a DNS server IP address.

11. In the **Secondary DNS Server** field, optionally specify a second DNS server IP address.



PowerProtect Data Manager Appliance Configuration

Network

Interfaces

Management IP: 10.247.9.[redacted]
Data IP 1: 10.247.9.[redacted]
Management FQDN: l1dpdvcld06[redacted]
Data IP 2: 10.247.9.[redacted] (Optional)
Management Domain name: hop.lab[redacted]

Management VLAN

Management VLAN ID: 9
Management Subnet Mask: 255.255.255.0
MTU: 1500
Management Gateway: 10.247[redacted]
Bonding options: Active/Active

Data VLAN

□ Seperate Data Network
Data VLAN ID: 9
Data Subnet Mask: 255.255.255.0
MTU: 1500
Data Gateway: 10.247.[redacted] (Optional)
Bonding options: Active/Active

DNS

Figure 14. PowerProtect Data Manager Appliance network configuration

12. Click **Next**.

    The **Time/Location** page is displayed.

13. On the **Time/Location** page, perform the following actions:

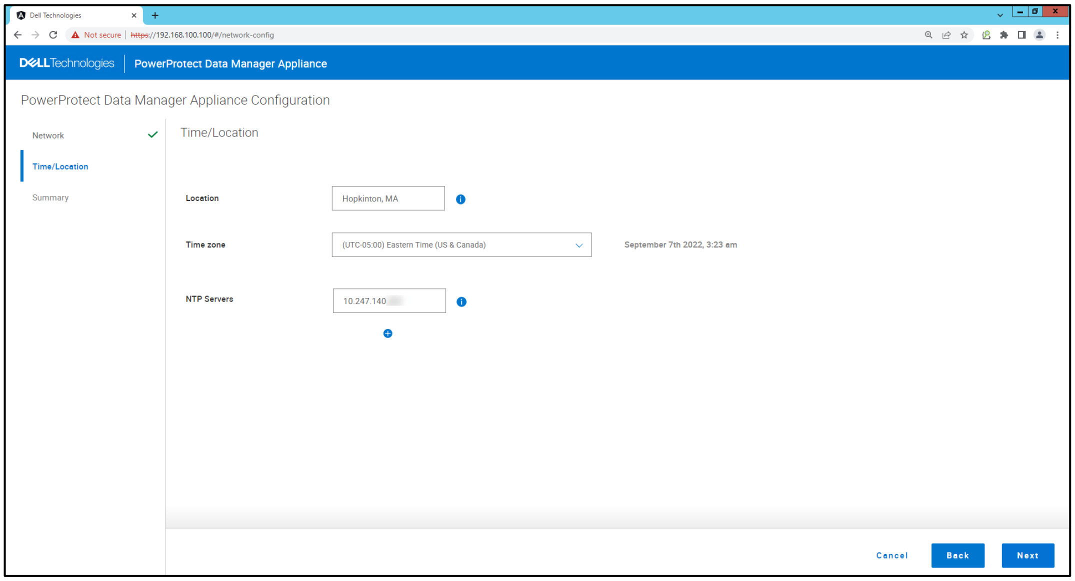
    a. From the **Time zone** list, select the time zone where the system exists.

b. In the **NTP Servers** field, specify the NTP server IP address.

c. (Optional) Click **+** to add a secondary NTP server.

d. Click **Next**.

The **Summary** page is displayed.



Dell Technologies
Not secure | https://192.168.100.100/#/network-config
DØLLTechnologies | PowerProtect Data Manager Appliance

PowerProtect Data Manager Appliance Configuration

Network ✓
Time/Location
Summary

Time/Location

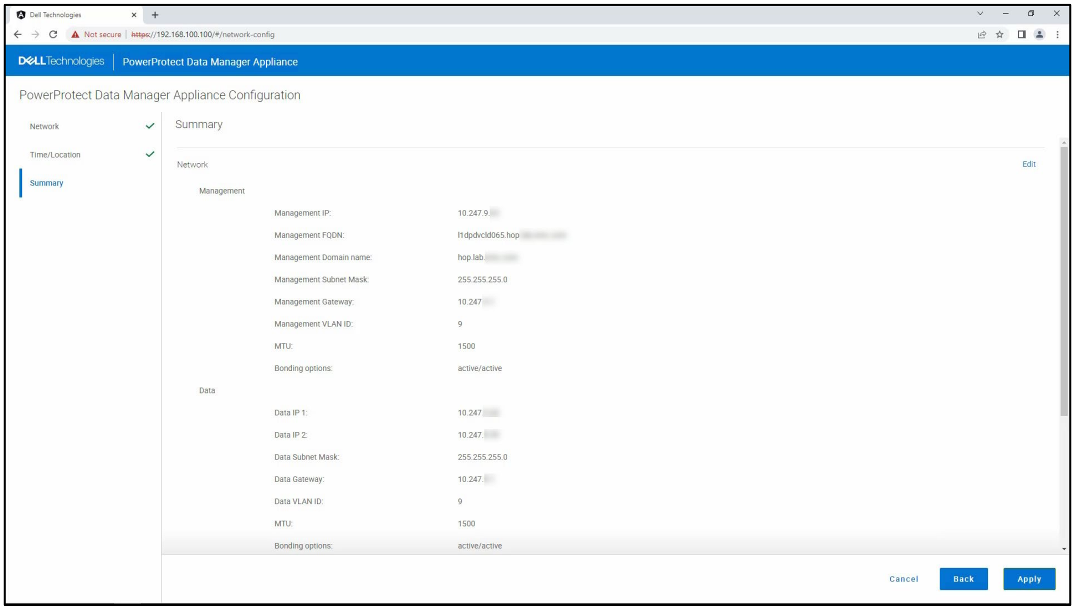
Location: Hopkinton, MA

Time zone: (UTC-05:00) Eastern Time (US & Canada)   September 7th 2022, 3:23 am

NTP Servers: 10.247.140[redacted]

**Figure 15. PowerProtect Data Manager Appliance time and location**

14. On the **Summary** page, click **Apply** to initiate the deployment process.



Dell Technologies
Not secure | https://192.168.100.100/#/network-config
DØLLTechnologies | PowerProtect Data Manager Appliance

PowerProtect Data Manager Appliance Configuration

Network ✓
Time/Location ✓
Summary

Summary

Network

Management

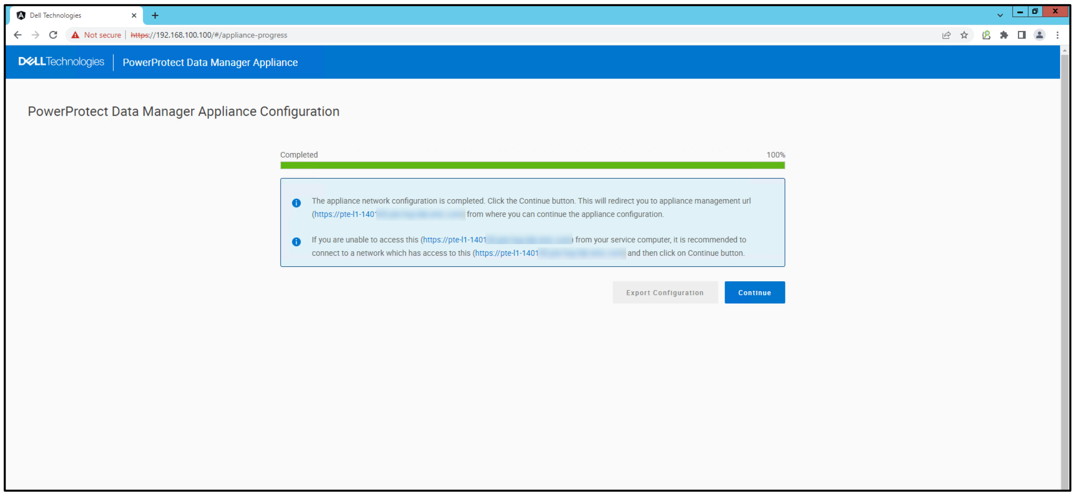
| | |
|---|---|
| Management IP: | 10.247.9.[redacted] |
| Management FQDN: | l1dpdvcld065.hop[redacted] |
| Management Domain name: | hop.lab.[redacted] |
| Management Subnet Mask: | 255.255.255.0 |
| Management Gateway: | 10.247[redacted] |
| Management VLAN ID: | 9 |
| MTU: | 1500 |
| Bonding options: | active/active |

Data

| | |
|---|---|
| Data IP 1: | 10.247[redacted] |
| Data IP 2: | 10.247.[redacted] |
| Data Subnet Mask: | 255.255.255.0 |
| Data Gateway: | 10.247.[redacted] |
| Data VLAN ID: | 9 |
| MTU: | 1500 |
| Bonding options: | active/active |

**Figure 16. PowerProtect Data Manager Appliance Summary page**

The appliance displays a progress bar showing the status of the configuration.


Dell Technologies
Not secure | https://192.168.100.100/#/appliance-progress
DELL Technologies | PowerProtect Data Manager Appliance
Completed
100%
Export Configuration
Continue

PowerProtect Data Manager Appliance Configuration

The appliance network configuration is completed. Click the Continue button. This will redirect you to appliance management url (https://pte-l1-140[redacted] from where you can continue the appliance configuration.

If you are unable to access this (https://pte-l1-1401[redacted]) from your service computer, it is recommended to connect to a network which has access to this (https://pte-l1-1401[redacted] and then click on Continue button.

**Figure 17. PowerProtect Data Manager Appliance Is successfully deployed**

15. When the appliance is successfully deployed and configured, click **Continue**.

    The PowerProtect Data Manager Appliance login page is displayed.

## Replication

The PowerProtect Data Manager Appliance system protection service enables the protection of the system’s persistent data from catastrophic loss by creating a series of server DR backups. PowerProtect Data Manager Appliance supports only replication to another PowerProtect Data Manager Appliance. From a system recovery perspective, only one target system can be configured or added. From a PLC perspective, the appliance supports various topologies, as outlined in Quick recovery.

**Note**: Create a separate PLC for each asset to optimize replication topologies (Fan-in, Fan-out) at an asset level.

### System recovery

System recovery creates point-in-time snapshots of the PowerProtect Data Manager Appliance server in protection storage. During a DR activity, recover the server from protection storage and then restore protected assets.

#### *Supported topologies*

Currently, only one backup target and one replication target are supported at a time (1:1).

**Note:** When you specify a new PowerProtect Data Manager Appliance as the target, you override the existing selection.

### Quick recovery

Quick recovery makes a remote PowerProtect Data Manager Appliance replication destination aware of replicated backups and enables the recovery view. During a DR activity, you can restore assets from these replicated backups at the destination without recovering the source server.

### *Supported topologies*

- Uni-directional,  replicating one way from source to destination
- Bi-directional, replicating both ways from source to destination
- Fan-in, replicating many source systems to one destination system
- Fan-out, replicating from one source system to many destination systems

The following figure shows the bi-directional replication topology:

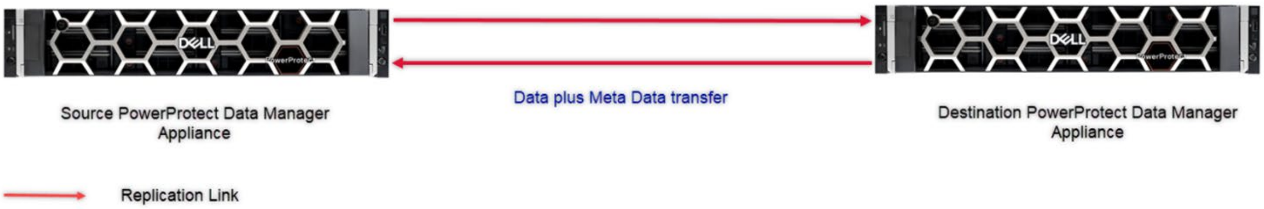

Source PowerProtect Data Manager Appliance
Data plus Meta Data transfer
Destination PowerProtect Data Manager Appliance
Replication Link

**Figure 18. Bi-directional replication topology of PowerProtect Data Manager Appliance**

## Cloud disaster recovery

Cloud DR enables you to restore to a DR site in a supported public cloud environment. During a DR activity, restore virtual machines to a cloud DR server and recover those workloads in the cloud.

### *Supported cloud computing services*

- Amazon Web Services (AWS) S3
- Microsoft Azure Storage

### *Supported topologies*

Currently, only one cloud DR site can be configured with PowerProtect Data Manager Appliance (1:1).

**Note:** For more information about server DR and configuration, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Administration Guide*.

## Appliance reconfiguration

Today's customers are changing production setup configurations for various reasons. These reasons include running low on IP addresses for a given subnet, management hostname updates, and DNS updates, among others. It is imperative for any product to be able to seamlessly transition between system configurations without affecting data integrity.

In PowerProtect Data Manager Appliance, customers can modify configuration parameters (such as the default management and data networks, DNS, NTP, time zone, and location settings) post-deployment without affecting data integrity.

Before changing configuration settings, consider the following guidance:

- To change the appliance management and data network settings, we recommend that the user be connected to the appliance private network on 192.168.100.100 through the service laptop,

- If no existing protection policies, VM proxies, or agents are configured with the existing network parameters, the customer can modify the appliance management and data network.
- If existing protection policies, VM proxies, or agents are configured with the existing network parameters, the customer must reach out to Dell Customer Support.

**Note:** The user does not need to be linked to the private network to change DNS settings, location, time zone, or NTP settings. Because DNS and NTP settings are nondestructive activities, they can be changed through the appliance management IP address.

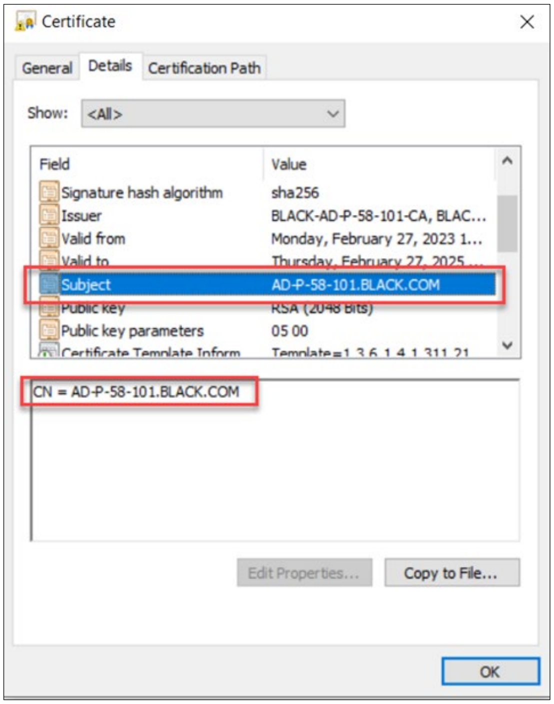
**Note:** For information about how to perform a system reconfiguration, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Administration Guide*.

## Active Directory

PowerProtect Data Manager Appliance leverages secured Active Directory as an external identity provider for users and groups. When mapped, users in the group can exercise their privileges on the appliance based on the assigned role.

The following requirements and recommendations apply:

- Usernames and passwords must exist for all LDAP users.
- The certificate issued by the Active Directory server should contain the FQDN name or the IP address of the Active Directory server.



Show: <All>

| Field | Value |
|---|---|
| Signature hash algorithm | sha256 |
| Issuer | BLACK-AD-P-58-101-CA, BLAC... |
| Valid from | Monday, February 27, 2023 1... |
| Valid to | Thursday, February 27, 2025 ... |
| Subject | AD-P-58-101.BLACK.COM |
| Public key | RSA (2048 Bits) |
| Public key parameters | 05 00 |
| Certificate Template Inform | Template=1.3.6.1.4.1.311.21 |

CN = AD-P-58-101.BLACK.COM

**Figure 19. Certificate issued with Active Directory FQDN name in the Subject field**

- All Active Directory users must have the UID number defined in their profile for seamless access across the appliance UI.

**Note**: Mapping the Protected Users group from Windows Active Directory is not supported. If you add a mapping for this group, its members cannot log in to Data Manager Appliance.

**Note**: For information about how to integrate Active Directory with Data Manager, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Security Configuration Guide*.

## Multi-factor authentication

Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a system.

PowerProtect Data Manager Appliance leverages knowledge and possession factors to achieve MFA capabilities:

- Knowledge factor reflects the user's well-known username and password as defined.
- Possession factor is a smartphone capable of generating tokens (TOTP) through Google Authenticator.

When using MFA:

- Verify that the user is conscious of the well-known password assigned to the user’s profile.
- Verify that the smartphone device can generate a time-based one-time password (TOTP) using Google Authenticator.

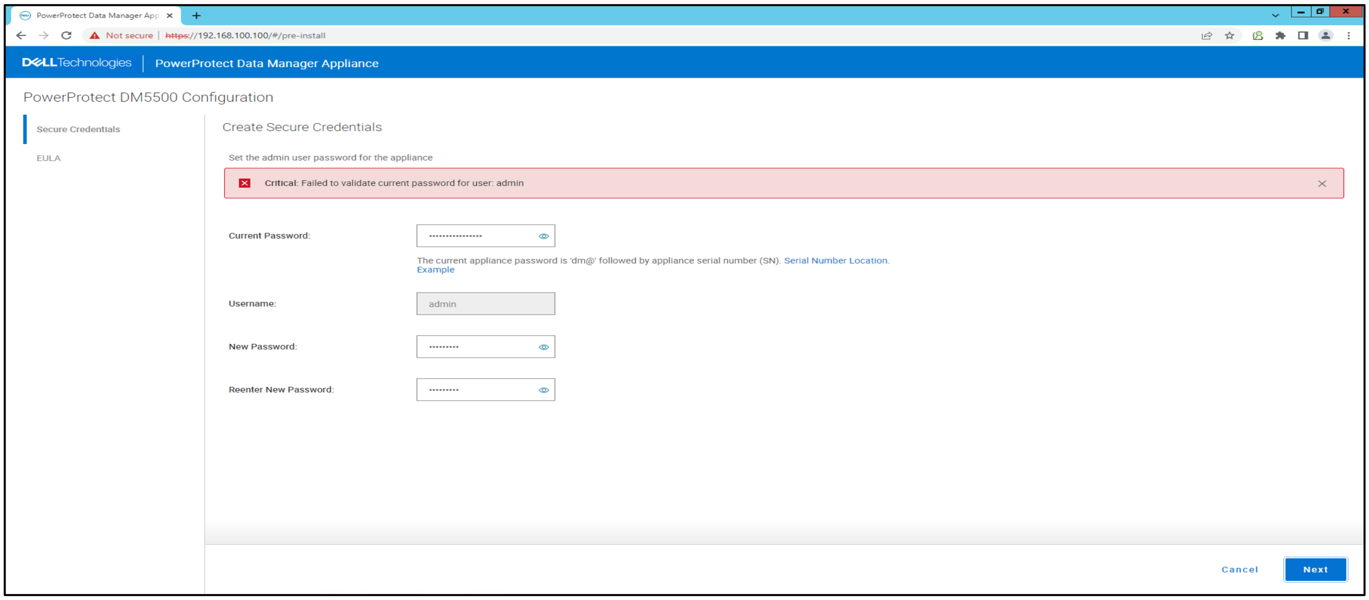
**Note**: For information about how to enable MFA on Data Manager, see the *PowerProtect Data Manager Appliance DM5500 5.14.0.0 Security Configuration Guide*.

## Troubleshooting

This section provides a list of potential causes and resolutions for error messages that are related to PowerProtect Data Manager deployment.

### Invalid PSNT number

When the user enters an incorrect password during appliance deployment, the following error message is displayed:


PowerProtect Data Manager App
Not secure
https://192.168.100.100/#/pre-install
DELLTechnologies
PowerProtect Data Manager Appliance
Secure Credentials
EULA
Cancel
Next

PowerProtect DM5500 Configuration

Create Secure Credentials

Set the admin user password for the appliance

Critical: Failed to validate current password for user: admin

Current Password: ••••••••••••••••••

The current appliance password is 'dm@' followed by appliance serial number (SN). Serial Number Location. Example

Username: admin

New Password: •••••••••

Reenter New Password: •••••••••

**Figure 20. Invalid PNST number**

To resolve this issue:

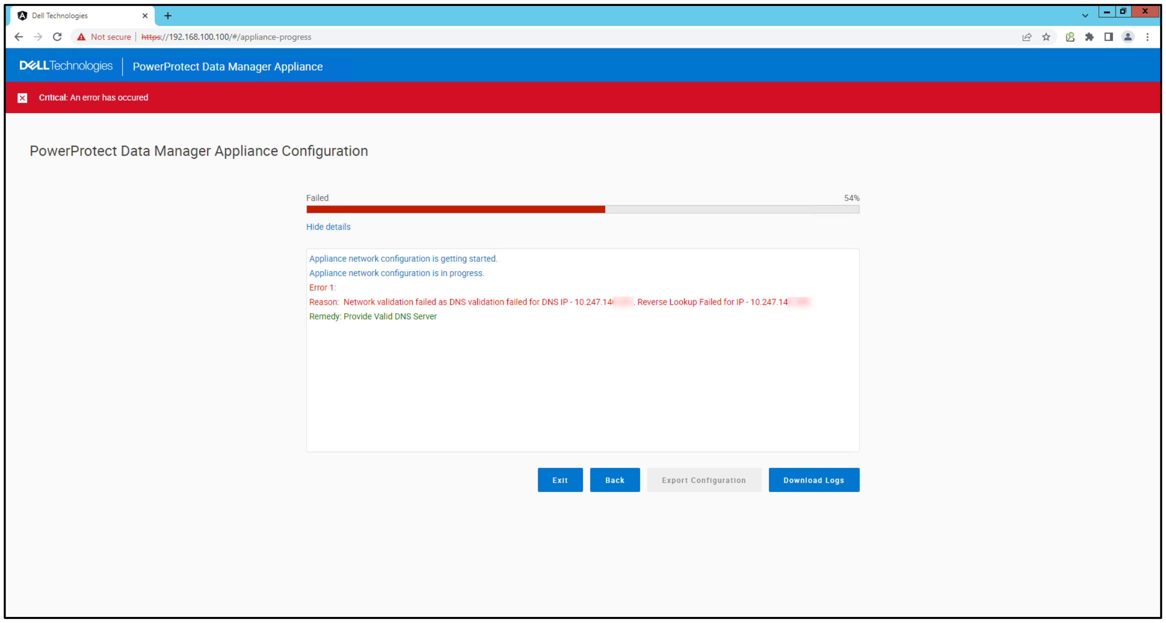
1. Log out of the web browser.
2. Log back into the PowerProtect Data Manager Appliance configuration UI.
3. Enter the correct password.

   The password is the complete appliance serial number (PSNT) with a prefix of `dm@`. For example, if the PSNT is DPDIH220124121, the password would be `dm@DPDIH220124121`.
4. Click **Next** to proceed with the deployment.

## Network validation failed for DNS <*DNS IP*>, and reverse lookup failed for <*IP*>

When a DNS entry is missing for the management interface, the following error message is displayed.

**Note**: DNS entry is mandatory for the management interface of the appliance. If the DNS entries are missing, the deployment fails.


Dell Technologies
Not secure | https://192.168.100.100/#/appliance-progress
DELLTechnologies | PowerProtect Data Manager Appliance

Critical: An error has occured

PowerProtect Data Manager Appliance Configuration

Failed 54%

```
Appliance network configuration is getting started.
Appliance network configuration is in progress.
Error 1:
Reason:  Network validation failed as DNS validation failed for DNS IP - 10.247.14[redacted]. Reverse Lookup Failed for IP - 10.247.14[redacted]
Remedy: Provide Valid DNS Server
```

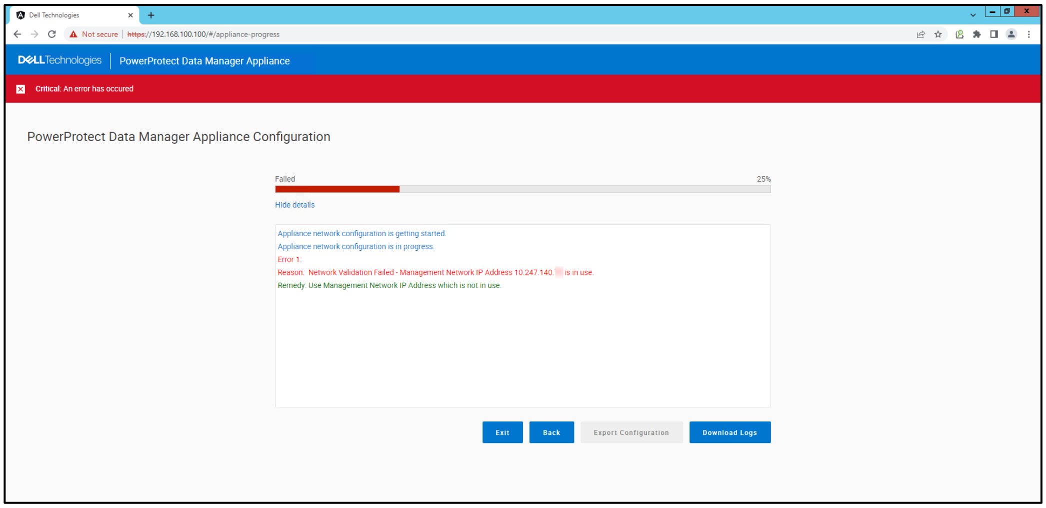
**Figure 21. Network validation error for management interface**

To resolve this issue:

1. Determine if a DNS entry exists for the management interface.
2. If a DNS entry for the management interface does not exist, add an entry in DNS for both forward and reverse lookup for the management interface.
3. Go back to the **Network** page and validate the configuration again by clicking **Back**.
4. On the **Summary** page, click **Apply** to rerun the deployment.

## Network validation failed—management network IP address <IP> is in use

When the user enters an IP address that is assigned or already in use as the management interface for the application, the following error message is displayed:


Dell Technologies
Not secure | https://192.168.100.100/#/appliance-progress
DELL Technologies | PowerProtect Data Manager Appliance

Critical: An error has occured

PowerProtect Data Manager Appliance Configuration

Failed 25%

```
Appliance network configuration is getting started.
Appliance network configuration is in progress.
Error 1:
Reason:  Network Validation Failed - Management Network IP Address 10.247.140.[redacted] is in use.
Remedy: Use Management Network IP Address which is not in use.
```

Exit
Back
Export Configuration
Download Logs

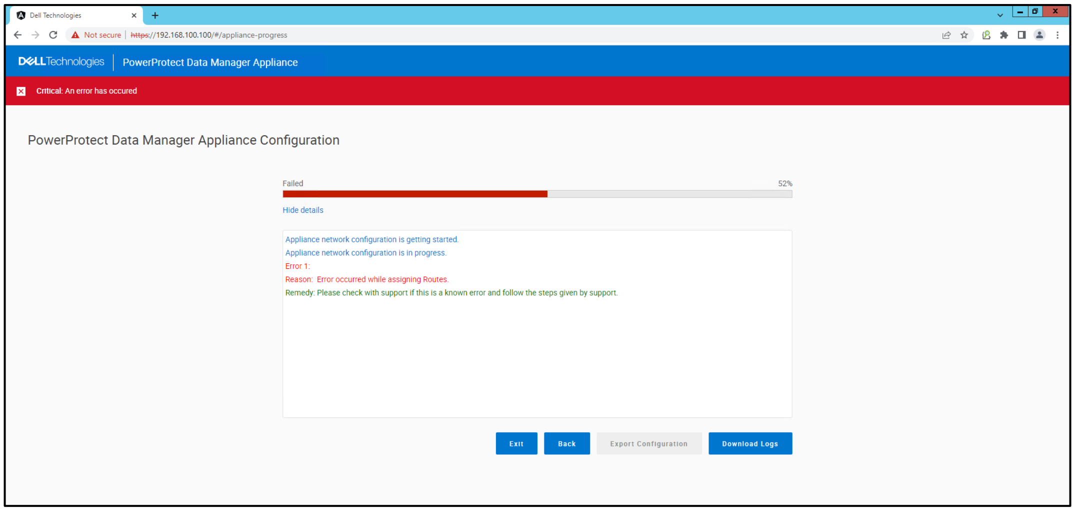
**Figure 22. Network validation error when management interface is in use**

To resolve this issue:

1. Determine whether the assigned IP address is already in use.
2. If the IP address is in use, assign an unused IP address to the management interface.
3. Go back to the **Network** page and click **Back** to rectify the configuration.
4. On the **Summary** page, click **Apply** to rerun the deployment.

## Error occurred while assigning routes

Whenever the user enters an incorrect VLAN ID, the firewall configuration restricts the communication, or cannot connect to the management network gateway, and the following error message is displayed:


Dell Technologies
Not secure | https://192.168.100.100/#/appliance-progress
DELL Technologies | PowerProtect Data Manager Appliance

Critical: An error has occured

PowerProtect Data Manager Appliance Configuration

Failed 52%

```
Appliance network configuration is getting started.
Appliance network configuration is in progress.
Error 1:
Reason:  Error occurred while assigning Routes.
Remedy: Please check with support if this is a known error and follow the steps given by support.
```

Exit
Back
Export Configuration
Download Logs

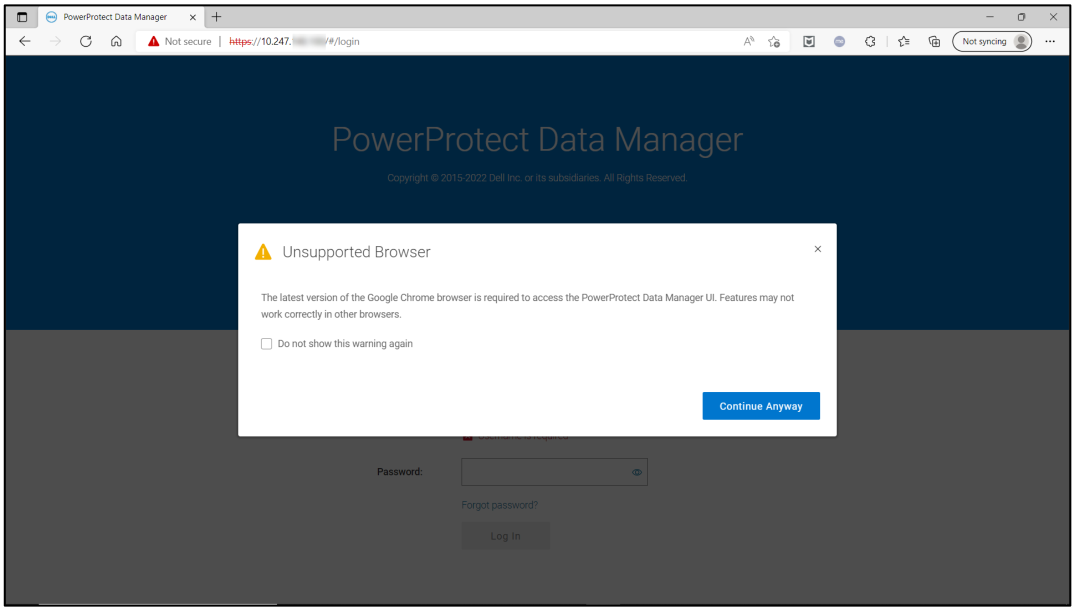
**Figure 23. Network validation error when incorrect VLAN ID is entered**

To resolve this issue:

1. Determine if the switch is configured in access mode or trunked mode.
   - If it is in access mode, enter the VLAN ID as 0.
   - If it is in trunked mode, enter the correct VLAN ID.
2. If the switch configuration is correct, ensure that you can reach the management gateway from the service laptop.
3. Determine if the firewall on the customer network is restricting the connection.
4. Return to the **Network** page and click **Back** to rectify the configuration.
5. On the **Summary** page, click **Apply** to rerun the deployment.

## Unsupported web browser

When the user launches the PowerProtect Data Manager Appliance UI from an unsupported web browser, the following warning message is displayed:



Unsupported Browser

The latest version of the Google Chrome browser is required to access the PowerProtect Data Manager UI. Features may not work correctly in other browsers.

□ Do not show this warning again

PowerProtect Data Manager
Not secure
~~https~~://10.247.[redacted]/#/login
Not syncing
PowerProtect Data Manager
Copyright © 2015-2022 Dell Inc. or its subsidiaries. All Rights Reserved.
Continue Anyway
Password:
Forgot password?
Log In

**Figure 24. Unsupported browser**

The **Unsupported Browser** message is a warning; the user can continue to use the web browser, but the functionality of the appliance will be limited. Using an unsupported web browser can pose a security risk.

Google Chrome is the preferred web browser for managing PowerProtect Data Manager Appliance.

To resolve this issue, launch the PowerProtect Data Manager Appliance UI using Google Chrome.

# Upgrading PowerProtect Data Manager Appliance

## Introduction

This section describes the procedure to upgrade the PowerProtect Data Manager Appliance. The software, firmware, and infrastructure components are updated in the appliance upgrade.

## Upgrade prerequisites

Ensure that the upgrade binary `dmas-upgrade-5.14.0.0-x.pkg` has been downloaded from Dell Support and is available on your computer for upload.

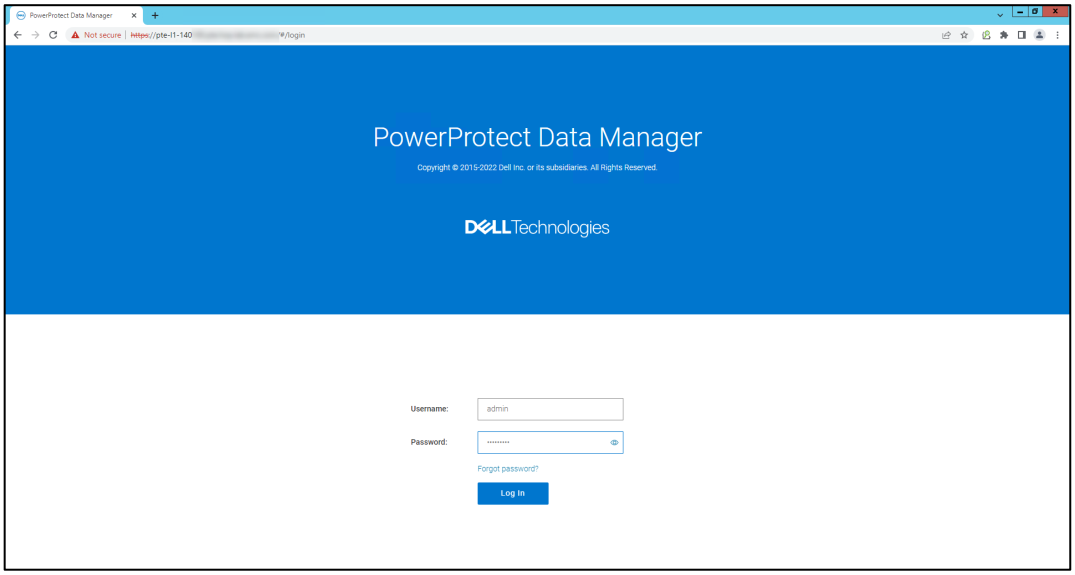
## Upgrade procedure

To upgrade PowerProtect Data Manager Appliance to its latest version, follow these steps:

1. Using the IAM credentials, log in to the PowerProtect Data Manager Appliance UI:

   `https://<PowerProtect Data Manager Appliance UI>`

2. Click **Login**.



~~https~~://pte-l1-140[redacted]/#/login

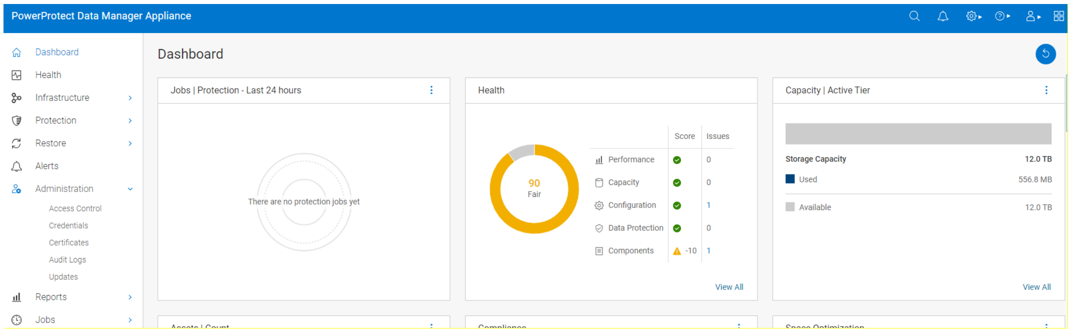
Copyright © 2015-2022 Dell Inc. or its subsidiaries. All Rights Reserved.

Username: admin

Password: ········

**Figure 25. PowerProtect Data Manager Appliance UI**

3. Go to **Administration**, and click **Updates**.



There are no protection jobs yet

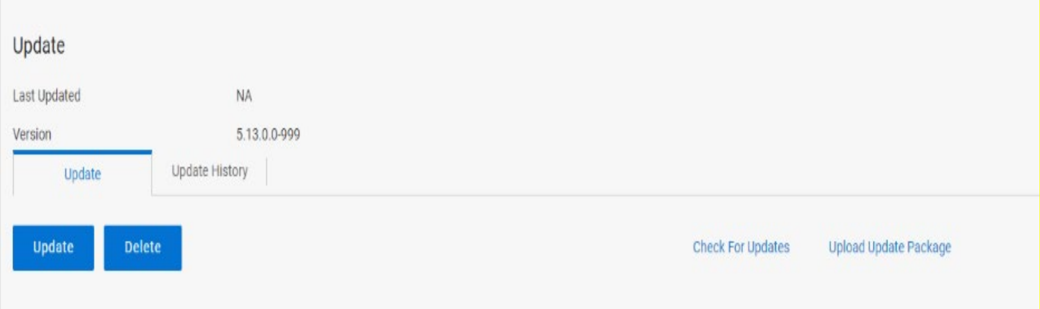
| | Score | Issues |
|---|---|---|
| Performance | ✓ | 0 |
| Capacity | ✓ | 0 |
| Configuration | ✓ | 1 |
| Data Protection | ✓ | 0 |
| Components | ⚠ -10 | 1 |

| | |
|---|---|
| Storage Capacity | 12.0 TB |
| Used | 556.8 MB |
| Available | 12.0 TB |

**Figure 26. PowerProtect Data Manger Appliance Administration**

The **PowerProtect Data Manager Appliance Update** page is displayed.

4. Click **Upload Update Package.**

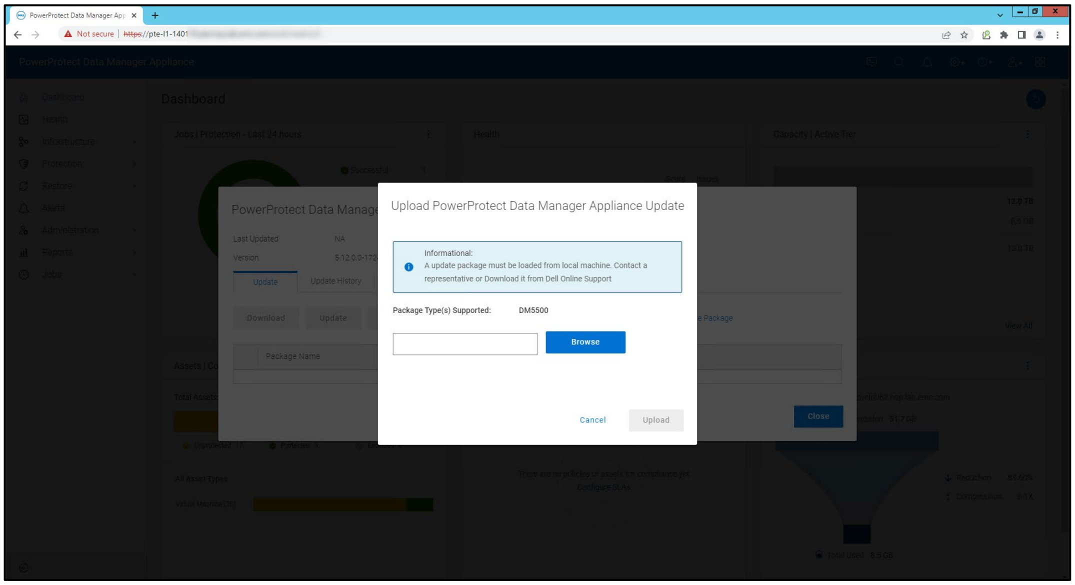

Update

Last Updated NA

Version 5.13.0.0-999

**Figure 27. PowerProtect Data Manger Appliance Update page**

The **Upload PowerProtect Manager Appliance Update** dialog box is displayed, allowing you to browse and upload a previously downloaded package.


Upload PowerProtect Data Manager Appliance Update

Informational:
A update package must be loaded from local machine. Contact a representative or Download it from Dell Online Support

Package Type(s) Supported: DM5500

**Figure 28. PowerProtect Data Manger Appliance Update page**

5. Click **Browse** and select the previously downloaded upgrade package (see Upgrade prerequisites).

---

**Note**: The upgrade package has a file extension .pkg. Select an appropriate file extension. The selected file is displayed in the field, and the **Upload** button is enabled.

---

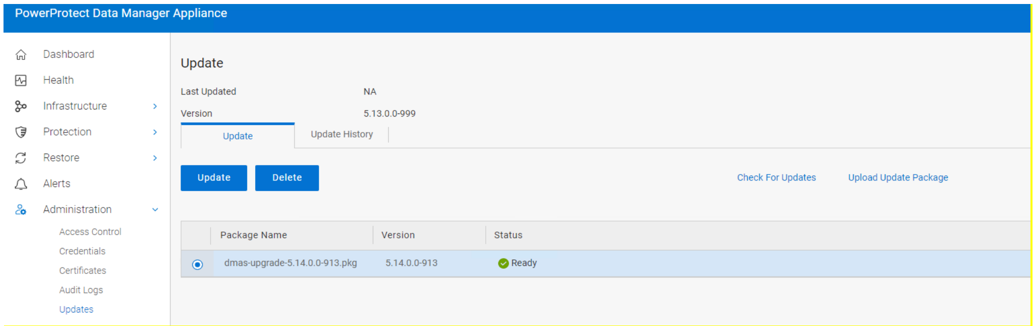
6. Click the **Upload** option.

   Once the package is uploaded, the **Close** button is enabled.

7. Click **Close**.

   The package is now added to the list.

8. Verify that the update package status is **Ready**, as shown in the following figure:



Update

Last Updated NA

Version 5.13.0.0-999

| | Package Name | Version | Status |
|---|---|---|---|
| ● | dmas-upgrade-5.14.0.0-913.pkg | 5.14.0.0-913 | ✓ Ready |

**Figure 29. PowerProtect Data Manager Appliance update package status**

9. Select the radio button next to the package name.

   The **Update** and **Delete** buttons are enabled.

10. Click **Update**.

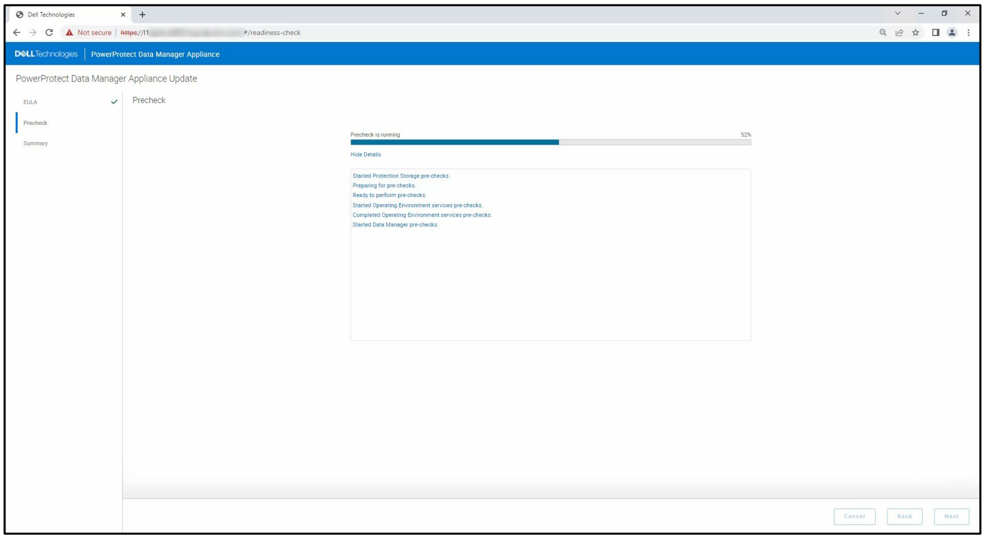
    The browser is redirected to a new URL.

11. Log in to the appliance using IAM credentials.

    The End User License Agreement is displayed.

12. Review the license agreement and click **Accept**.

    The **Precheck** page is displayed. The prechecks are triggered by default, and the progress is displayed. You can view detailed status messages of the prechecks being performed by clicking the **Show Details** link.



PowerProtect Data Manager Appliance Update

Precheck

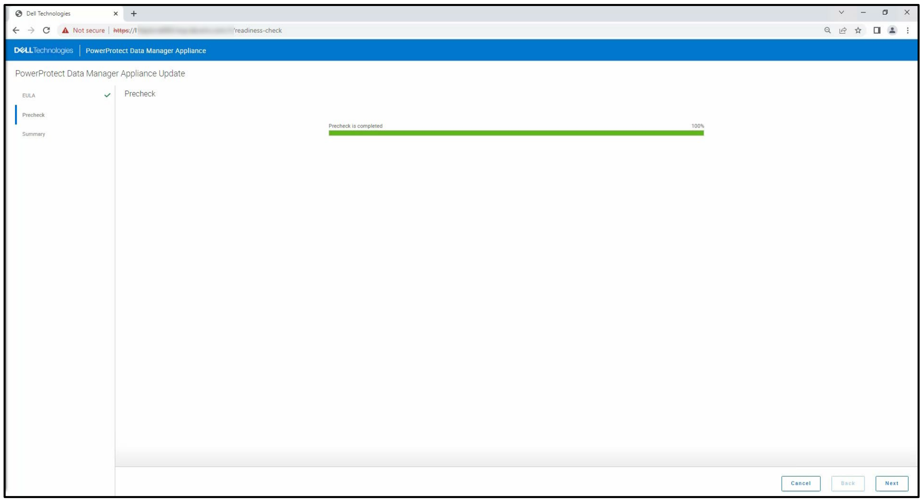
Precheck is running 52%

Started Protection Storage pre-checks.
Preparing for pre-checks.
Ready to perform pre-checks.
Started Operating Environment services pre-checks.
Completed Operating Environment services pre-checks.
Started Data Manager pre-checks.

**Figure 30. PowerProtect Data Manager Appliance precheck progress**

13. When the precheck is completed, click **Next** to continue.

    The **Summary** page is displayed.


Dell Technologies
Not secure | https://[redacted]/readiness-check
DELL Technologies | PowerProtect Data Manager Appliance
EULA ✓
Precheck
Summary
Cancel
Back
Next

PowerProtect Data Manager Appliance Update

Precheck

Precheck is completed 100%

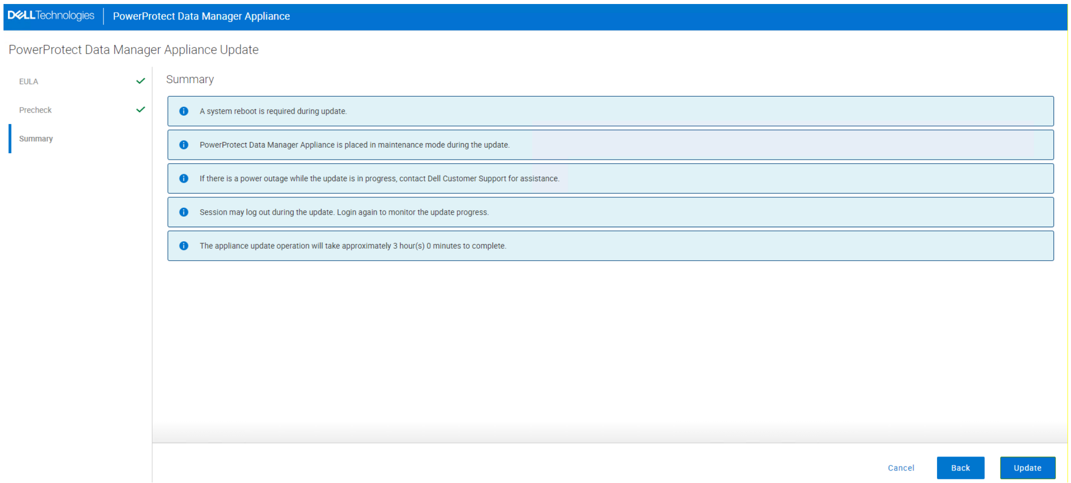
Figure 31. **PowerProtect Data Manager Appliance precheck completed**

14. On the **Summary** page, click **Update** to initiate the upgrade process.

---

**Note**: During upgrade, PowerProtect Data Manager Appliance is placed in maintenance mode.

---



PowerProtect Data Manager Appliance Update

Summary

- A system reboot is required during update.
- PowerProtect Data Manager Appliance is placed in maintenance mode during the update.
- If there is a power outage while the update is in progress, contact Dell Customer Support for assistance.
- Session may log out during the update. Login again to monitor the update progress.
- The appliance update operation will take approximately 3 hour(s) 0 minutes to complete.

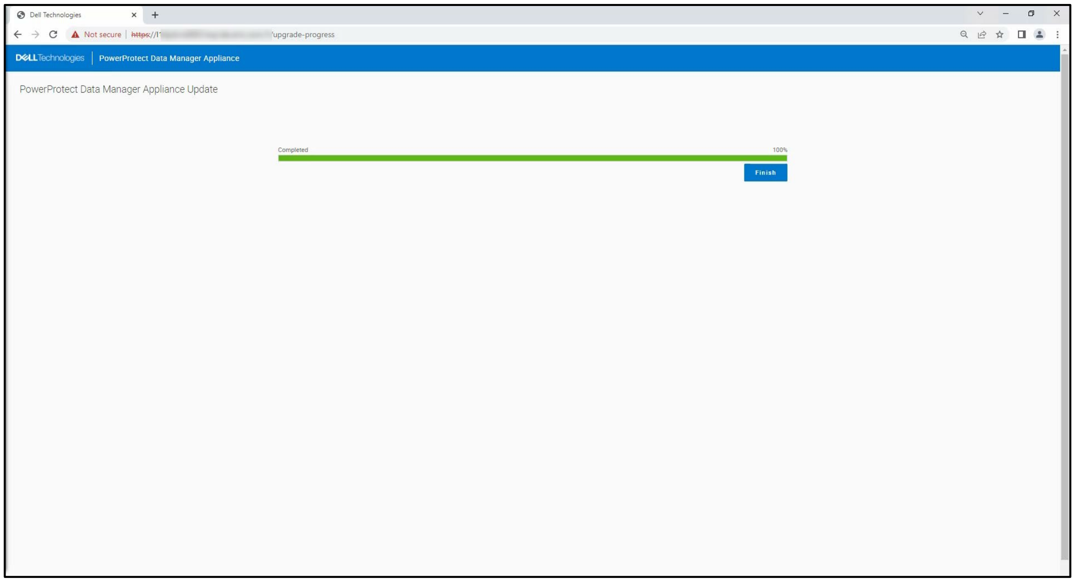
Figure 32. **PowerProtect Data Manager Appliance upgrade Summary page**

On the appliance update page, you can monitor the progress of the upgrade by clicking the **Show Details** link.

When the upgrade is completed, the **Finish** button is displayed.

15. Click **Finish**.
16. Click **Close**.

The update is complete.

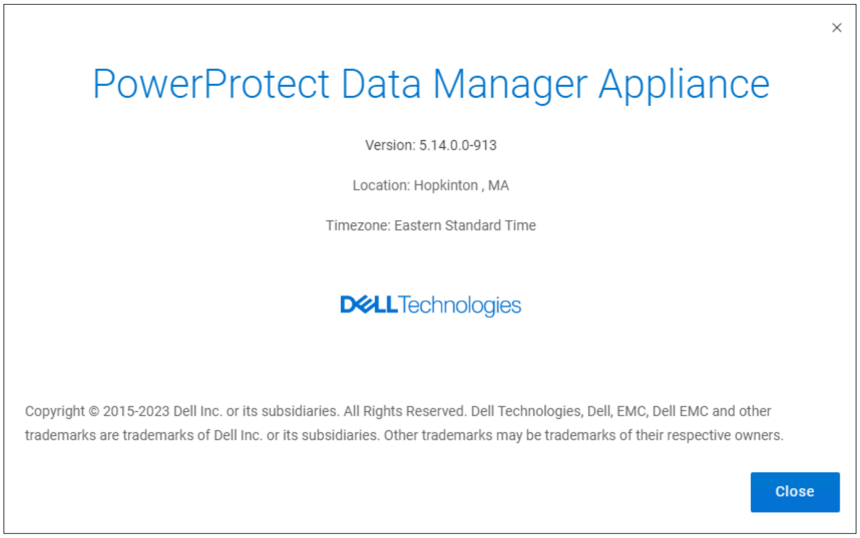


Dell Technologies
Not secure | ~~https~~://[redacted]/upgrade-progress
DELL Technologies | PowerProtect Data Manager Appliance
Finish

PowerProtect Data Manager Appliance Update

Completed 100%

Figure 33. PowerProtect Data Manager Appliance has been upgraded successfully



PowerProtect Data Manager Appliance

Version: 5.14.0.0-913

Location: Hopkinton , MA

Timezone: Eastern Standard Time

Copyright © 2015-2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Figure 34. PowerProtect Data Manager Appliance is upgraded to the latest version

# Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

The Data Protection Info Hub provide expertise to ensure customer success with Dell Technologies data protection products.

The PowerProtect Data Manager Appliance DM5500 5.14.0.0 documentation set includes the following documents:

- Release Notes
- Installation Guide
- Security Configuration Guide
- Networking Guide
- Resiliency Guide
- Software Compatibility Guide
- Field Services Guide
- Customer Replaceable Unit Guide
- Administration and User Guide