

# Dell EMC PowerProtect Data Manager Software: Deployment Best Practice

## Abstract

This white paper explains Power Protect Data Manager deployment best practices. It discusses on pre and post deployment requirements and best practices

July 2019

## Revisions

Date	Description
July 2019	Initial release

## Acknowledgements

This paper was produced by the following:

Author: Sonali Dwivedi

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [7/25/2019] [Technical White Paper] [Document ID]

# Table of Contents

- Executive summary .....4
- Audience.....4
- PowerProtect Software Overview.....5
- 1 PowerProtect Software Deployment Considerations .....6
  - 1.1 Pre-Installation Tasks .....6
    - 1.1.1 Planning VMware vCenter .....6
    - 1.1.2 Planning Data Domain.....7
    - 1.1.3 Planning Networking.....7
    - 1.1.4 Preparing Application Hosts .....8
- 2 Post Installation Tasks .....9
  - 2.1 Login Screen.....9
  - 2.2 License .....9
  - 2.3 Authentication .....10
  - 2.4 System Settings.....11
  - 2.5 Email and SMTP setup .....11
  - 2.6 Login and Getting Started.....12
  - 2.7 Adding Data Domain .....13
  - 2.8 Verification .....14
- Conclusion.....15
- References .....15

## Executive summary

Data protection has become an integral and essential part of any successful business. The need to provide a powerful, scalable and yet simple disaster and operational recovery solution is at all-time high.

IT teams are also looking for a solution that is scalable, easy and efficient to implement and handle the workload of their small and mid-size environment. To meet the Mid-Market industry demands Dell EMC has come up with a new offering called Power Protect Software.

Some key differentiators for PowerProtect are:

- Software defined backup appliance with built-in deduplication for data protection, replication, and reuse.
- Self-service for data owners combined with central IT governance.
- SaaS-based management, compliance, and predictive analytics.
- Multidimensional with scale-up and scale-out flexibility and all flash performance.
- Microservices architecture for ease of deployment, scaling and upgrading.
- Multi cloud that is optimized with built-in cloud tiering and cloud disaster recovery.

In this whitepaper we will focus on the Data Protection Software only deployment requirements and best practices.

## Audience

This white paper is intended for customers, partners, and employees who want to better understand, evaluate, and explore deployment requirements and best practice of Power Protect Software. Familiarity with Power Protect Software and Data Domain is required.

# PowerProtect Software Overview

PowerProtect Data Manager integrates multiple data protection products within the Dell EMC Data Protection portfolio to enable data protection as a service. PowerProtect Data Manager enables new data paths with provisioning, automation, and scheduling that enable a data protection team to embed protection engines into the infrastructure for high-performance backup and recovery.

PowerProtect Data Manager integrates multiple data protection products within the Dell EMC Data Protection portfolio to enable data protection as a Service. PowerProtect Data Manager enables new data paths with provisioning, automation, and scheduling that enable a data protection team to embed protection engines into the infrastructure for high-performance backup and recovery.

There are several integrated services that comprise the PowerProtect Data Manager solution:

- Protection Storage Services:
  - Data Domain—Hardware
  - Data Domain Operating System (DDOS)
  - Data Domain Management Center (DDMC)
  - Data Domain Virtual Edition (DDVE)
- The following data paths:
  - Application Direct for Enterprise Applications, or Application Direct
  - VM Direct vProxy

PowerProtect Data Manager Software Appliance is easy to install and configure. You can deploy the PowerProtect Data Manager Open Virtual Appliance (OVA) by using one of the following methods:

- Manually deploying the OVA to a vCenter server—Use this method to deploy the OVA to a stand-alone or cluster host, while logged into the vCenter server. Supports configuring the network settings during the deployment.
- Manually deploying the OVA to an ESXi host—Use this method to deploy the OVA while logged in to an ESXi host. Use the VM console to configure the network settings after the deployment completes..

After the PowerProtect Software OVA deployment and setup is complete then we will get access to all other services and components of the software.

# 1 PowerProtect Software Deployment Considerations

## 1.1 Pre-Installation Tasks

### 1.1.1 Planning VMware vCenter

- Planning the environment for deploying PowerProtect Data Manager plays a vital role. It is necessary to facilitate adequate resources to achieve optimal performance of the PowerProtect Data Manager.
- The minimum resource requirements to deploy a PowerProtect Data Manager in vSphere 6.0 and above are:
  - 10 CPU cores
  - 18 GB RAM
  - 700 GB Storage (one 100 GB disk and one 500 GB disk)
- Requirements for Application Aware backups on virtual machines are:
  - vSphere version 6.5 and later
  - VMware ESXi server version 6.5 and later
  - VMware Tools version 10.1 and later
- The vProxies or Protection Engines are designed to meet the workload requirements, based on the number of virtual machines to be backed up. Each external vProxy supports 24 virtual machines and four streams per virtual machine (96 streams per vProxy).
- Also, based on the number of virtual machines to be backed up, you can use embedded or external Protection Engines. The table below lists the considerations for embedded and external Protection Engines.



Embedded Protection Engine	External Protection Engine
<ul style="list-style-type: none"><li>• For small scale environments</li><li>• Does not require concurrent backups</li><li>• Hotadd transport mode is not required</li></ul>	<ul style="list-style-type: none"><li>• For large-scale environments</li><li>• Requires a large amount of data movement</li><li>• Requires concurrent data protection operations</li><li>• Supports up to 10000 virtual machines</li></ul>

#### Best Practices:



- Create a dedicated PowerProtect vCenter user, and avoid using the vCenter administrator
- Install VMware Tools on each virtual machine
- Use Hotadd transport mode for faster backups and restores and less exposure to network routing, firewall, and, SSL certificate issues
- Avoid deploying virtual machines with IDE virtual disks

## 1.1.2 Planning Data Domain

- The licenses for DDBOOST and AppDirect are built in. Microsoft SQL and
- Oracle can write to Data Domain directly.
- Other Licenses: Retention lock (optional) and Replication license (optional)
- Data Domain OS 6.1 requires Data Domain Management Center (DDMC).
- Data Domain OS 6.1.2 and above can be discovered directly by PowerProtect
- Data Manager.
- The supported DDVE version is 4.0.
- If you are adding Data Domain to PowerProtect Data Manager directly through PowerProtect Data Manager Infrastructure >Storage:
- DDOS 6.1.2 or higher: DD990, DD4500, DD7200, DD9500, DD6300, DD6800, DD9300, DD9800, DD3300
- If you are adding Data Domain to PowerProtect Data Manager through Data Domain Management Center (DDMC): DDMC 6.1.0.x, 6.1.x with DDOS 6.1.x and higher



**Best Practice:** Create a dedicated PowerProtect Data Domain BOOST user and avoid using sysadmin account for Data Domain discovery.

## 1.1.3 Planning Networking

### IP and DNS requirements

- Unique IP address must be allocated to the PowerProtect Data Manager .
- If customer is using External Protection engine (VM Proxy) that will also require one IP address.
- It is mandatory to sync PowerProtect Data Manager with NTP server.
- DNS server and default gateway servers should also be specified during install.

## Firewall and Port Requirements

PowerProtect Data Manager is a single node in a virtual appliance that uses the Linux SLES 12 firewall to protect and limit external access to the appliance.

PowerProtect Data Manager uses a direct socket connection to communicate and move data internally and across the network to the required service with minimal overhead

- The firewall rule needs to be for bi-directional, outbound, or inbound.
- The following TCP ports must be opened on firewall:
  - Port 443 between the administrator's desktop and PowerProtect.
  - TCP port 7000 between SQL and Oracle servers and PowerProtect appliance.
  - TCP port 3009 between PowerProtect appliance and Data Domain.
  - TCP port 111,2049,2052 should be open between Data Domain and vProxy and Application Hosts.

---

Note: For detailed information on complete port requirements please refer to PowerProtect Data Manager Security Configuration Guide.

---



### Best Practices:

- Verify all components have network connectivity to each other
- Configure forward and reverse lookup addresses

## 1.1.4 Preparing Application Hosts

- The application hosts and PowerProtect Data Manager must be synced to an NTP server.
- Dell EMC recommends pre-installing the supported application agents:
  - Oracle RMAN agent
  - DD Boost for Microsoft Application agent
  - DD Boost File System agent version (Linux and Windows)
- TCP port 7000 between SQL and Oracle servers and PowerProtect appliance.





## 2 Post Installation Tasks

- Once PowerProtect Data Manager OVA is successfully deployed and VM is powered ON, the PowerProtect UI can be accessed by entering the IP address or FQDN configured during the deployment  
→[https://appliance\\_hostname](https://appliance_hostname)
- Next step is to configure the basic settings for the PowerProtect Data Manager. Currently, Google Chrome is the only supported browser.

---

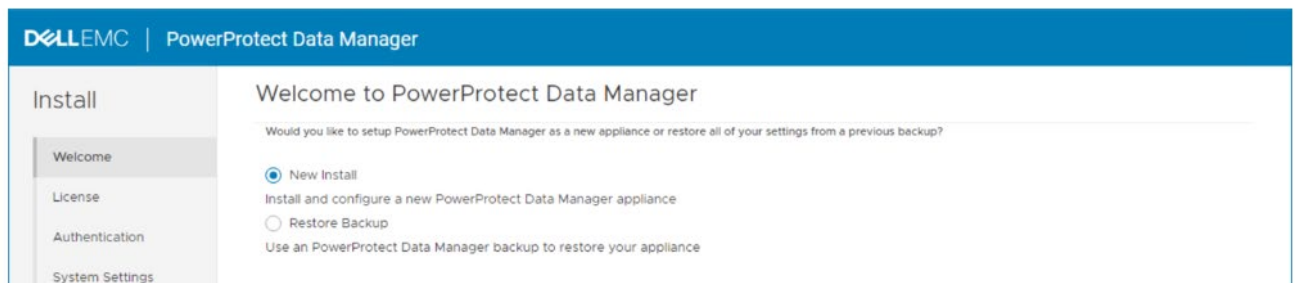
Note: To get more details and step by step instruction please refer to PowerProtect Data Manager Deployment Guide.

---

### 2.1 Login Screen

The Welcome screen is displayed when the PowerProtect UI is accessed for the first time after deploying the OVF template. There are two options available on this screen: New Install and Restore Backup.

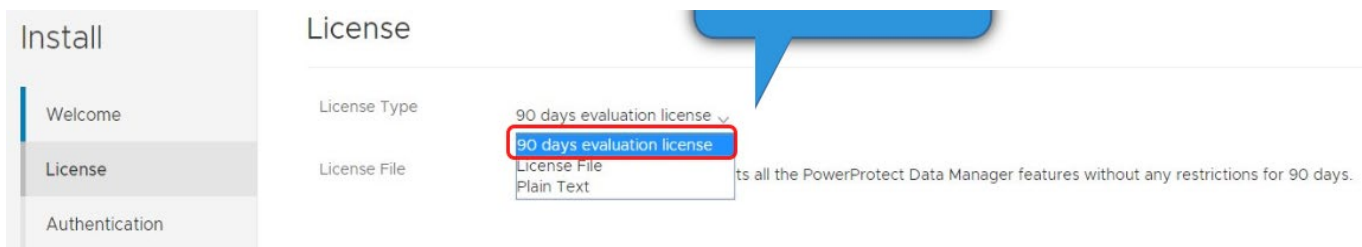
- New Install -If you are installing the device first time then select New Install.
- Restore Backup – This option is used when PowerProtect Data Manager appliance needs to be restored from backup.



### 2.2 License

PowerProtect Software has two types of license -trial license (valid for 90 days) and Front-end protected capacity by terabyte.

You can obtain the .xml license file from the Dell EMC license management website. To obtain the license file, you must have the License Authorization Code (LAC), which Modifying the System Settings was emailed from Dell EMC. If you have not received the LAC, contact your customer support representative.




---

**Note:** To use Secure Remote Services you must apply a valid PowerProtect Data Manager license.

---

## 2.3 Authentication

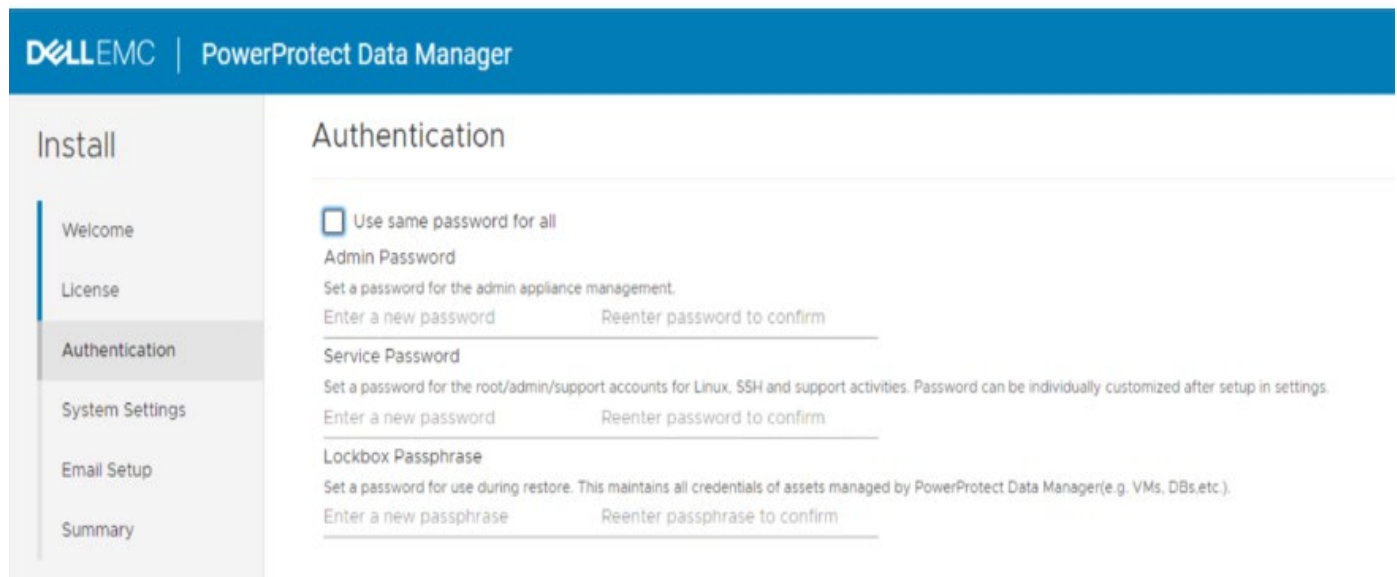
The authentication screen allows the admin to set an authentication password for various users with different roles.

- Admin password is used to login to PowerProtect Data Manager management console.
- Service password is used to login to ssh for support activities.
- Lockbox password is used during restore operations.
- The use same password for all checkbox can be selected to set the same password for admin, service and lockbox accounts but this is not the best practice.

---

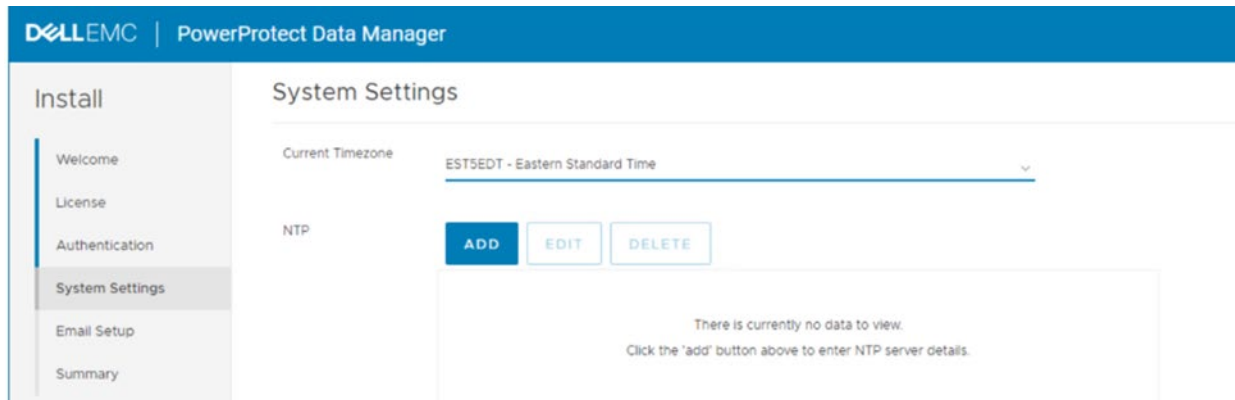
**Note:** It is strongly advised to save all the passwords securely for later use.

---



## 2.4 System Settings

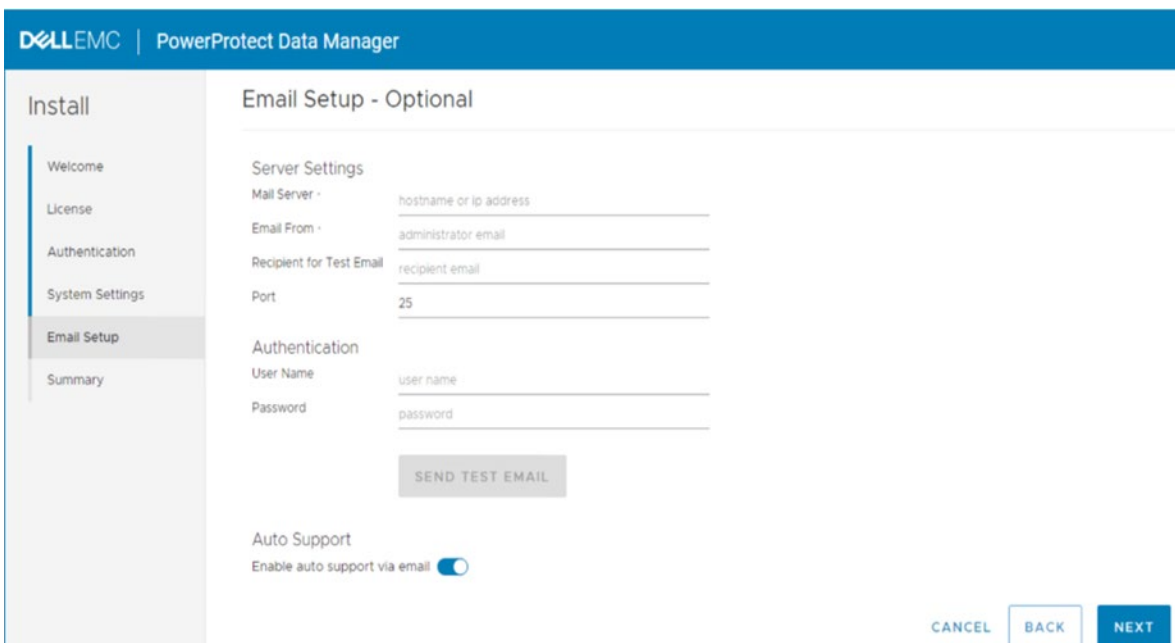
The system settings screen allows the user to add the NTP server. Dell EMC recommends that users should always add a NTP server and sync the PowerProtect Data Manager with it.



The screenshot shows the 'System Settings' page in the Dell EMC PowerProtect Data Manager interface. On the left, a sidebar menu under 'Install' includes 'Welcome', 'License', 'Authentication', 'System Settings' (highlighted), 'Email Setup', and 'Summary'. The main content area is titled 'System Settings' and features a 'Current Timezone' dropdown set to 'ESTSEDT - Eastern Standard Time'. Below this, an 'NTP' section contains 'ADD', 'EDIT', and 'DELETE' buttons. A message states: 'There is currently no data to view. Click the 'add' button above to enter NTP server details.'

## 2.5 Email and SMTP setup

Email setup is an optional step. The SMTP server can be configured to receive the PowerProtect Data Manager alerts on the specified email.

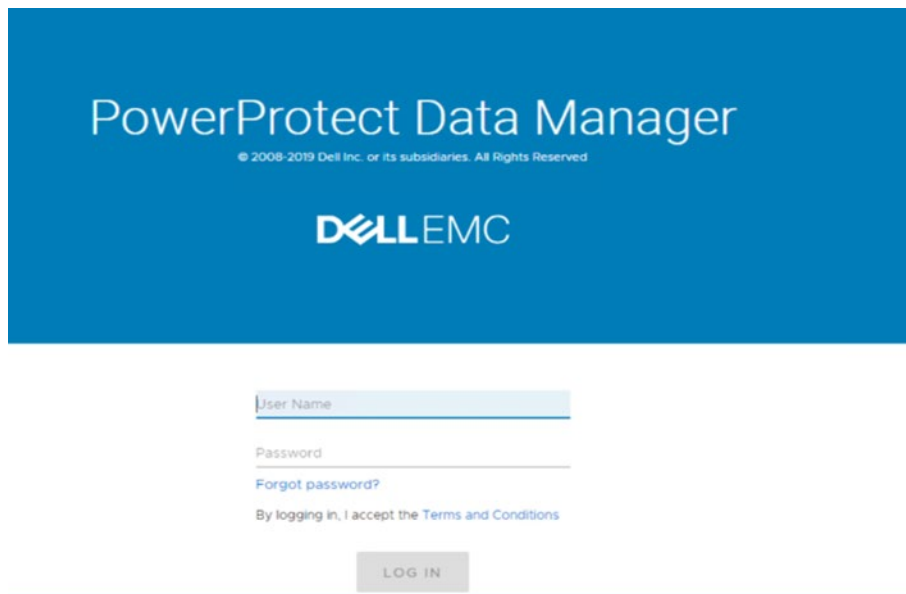


The screenshot shows the 'Email Setup - Optional' page in the Dell EMC PowerProtect Data Manager interface. The sidebar menu is identical to the previous screen, with 'Email Setup' highlighted. The main content area is titled 'Email Setup - Optional' and includes 'Server Settings' and 'Authentication' sections. The 'Server Settings' section has fields for 'Mail Server' (hostname or ip address), 'Email From' (administrator email), 'Recipient for Test Email' (recipient email), and 'Port' (25). The 'Authentication' section has fields for 'User Name' (user name) and 'Password' (password). A 'SEND TEST EMAIL' button is located below these fields. At the bottom, there is an 'Auto Support' section with the text 'Enable auto support via email' and a toggle switch that is currently turned on. Navigation buttons 'CANCEL', 'BACK', and 'NEXT' are at the bottom right.

## 2.6 Login and Getting Started

Once the user clicks the DONE button on the summary screen, the PowerProtect Data Manager applies all the configured settings, and the login screen appears after the setup is complete.

The user can login to the PowerProtect Data Manager using the credentials specified in the authentication step. The default login User Name is admin.



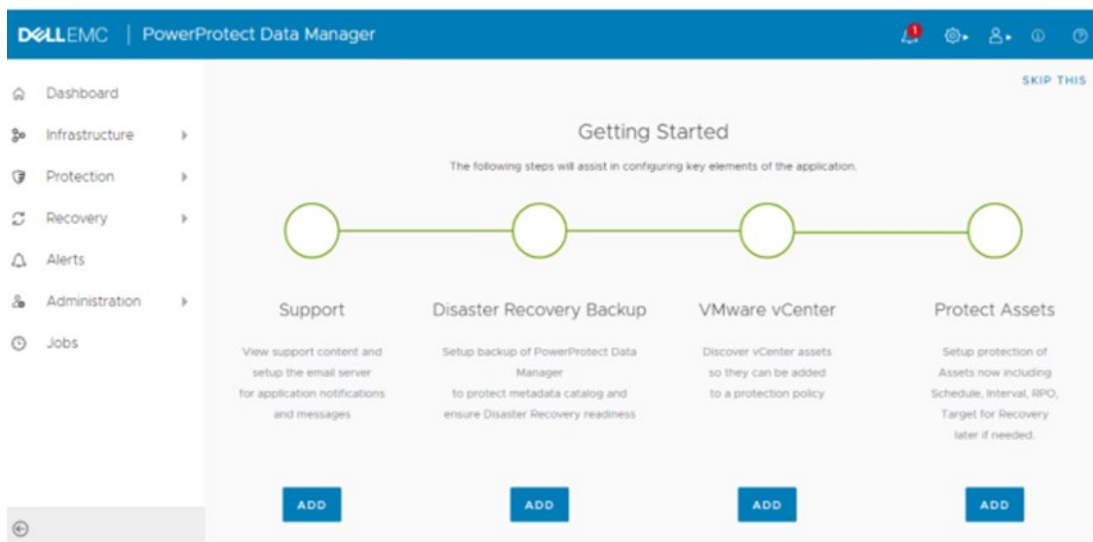
After login you will get “Getting Started” screen. PowerProtect Data Manager navigates back to Get Started until you exit Getting Started. To exit Getting Started, click **Skip This**.

Getting Started can be accessed anytime through System Settings > Getting Started.

There are four navigation options from the Getting Started screen, which are:

- Support - links to the Secure Remote Services (ESRS) configuration page.
- Disaster Recovery Backup - links to the backup configuration workflow.
- VMware vCenter - links to the workflow to add vCenter as asset sources.
- Protect Assets - links to the Protection Life Cycle workflow for all asset types.

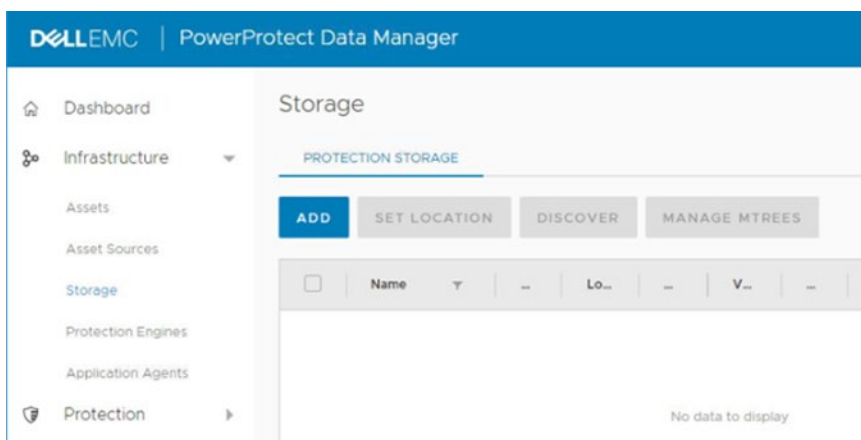
**NOTE:** For more information on the workflows refer to the *PowerProtect Deployment Guide*



## 2.7 Adding Data Domain

Last step before we can start configuring backup is adding a protection storage target that is configured to store the backup data. You can accomplish this by adding a Data Domain system to the PowerProtect environment.

- From the left navigation pane, select Infrastructure > Storage > PROTECTION STORAGE tab > ADD
- Based on the Data Domain operating system version number, select either a Data Domain System or a Data Domain Management Center to add.
- Specify a name and the FQDN for the Data Domain system (or Data Domain Management Center).
- Specify the Data Domain system login credentials. Save the credentials information and click SAVE again to complete the configuration step.



### Add Storage

Enter the connection information and credentials to access the storage system.

☐ Data Domain System
 ☒ Data Domain Management Center
 ☐ PowerProtect System

Name: DDMC  
 Address: ddmc.emc.edu  
 Port: 3009

**ADD CREDENTIALS** ▾

Credential Name: DDMC\_Credential  
 User Name: sysadmin  
 Password: \*\*\*\*\*

**SAVE**

## 2.8 Verification

Verify that the Data Domain system has been added to the PowerProtect Data Manager successfully.

- The Data Domain system should be discovered and added to PowerProtect Data Manager in a few minutes.
- The Data Domain system should be listed under Infrastructure > Storage > PROTECTION STORAGE tab.

The screenshot shows the Dell EMC PowerProtect Data Manager interface. The left sidebar contains navigation links: Dashboard, Infrastructure (selected), Assets, Asset Sources, Storage, Protection Engines, Application Agents, and Protection. The main content area is titled 'Storage' and has the 'PROTECTION STORAGE' tab selected. Below the tab are four buttons: ADD, SET LOCATION, DISCOVER, and MANAGE MTREES. A table displays the discovered storage system:

	Name	Type	Model	Version
<input checked="" type="checkbox"/>	ddve.emc.edu	Data Domain	DD VE Version 3.1	6.1.0.1-560300

You are ready now to start configuring the backups, please refer to *PowerProtect Administration Guide* for more configuring VM, File System and Application backups along with other management activities.

## Conclusion

This paper provided information on Power Protect Data Manager Software deployment pre and post installation requirements and best practices.

## References

The following documents were used in writing this whitepaper. All documents are available on <https://support.emc.com>

PowerProtect Data Manager Administration and User Guide 19.1

PowerProtect Data Manager Deployment Guide 19.1

PowerProtect Data Manager Security Configuration Guide 19.1

Data Domain Operating System 6.2 Administration Guide

Data Domain Operating System 6.1 Administration Guide