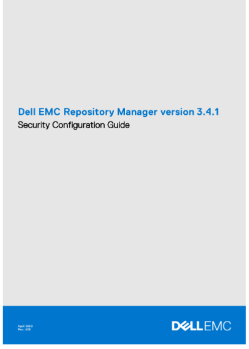
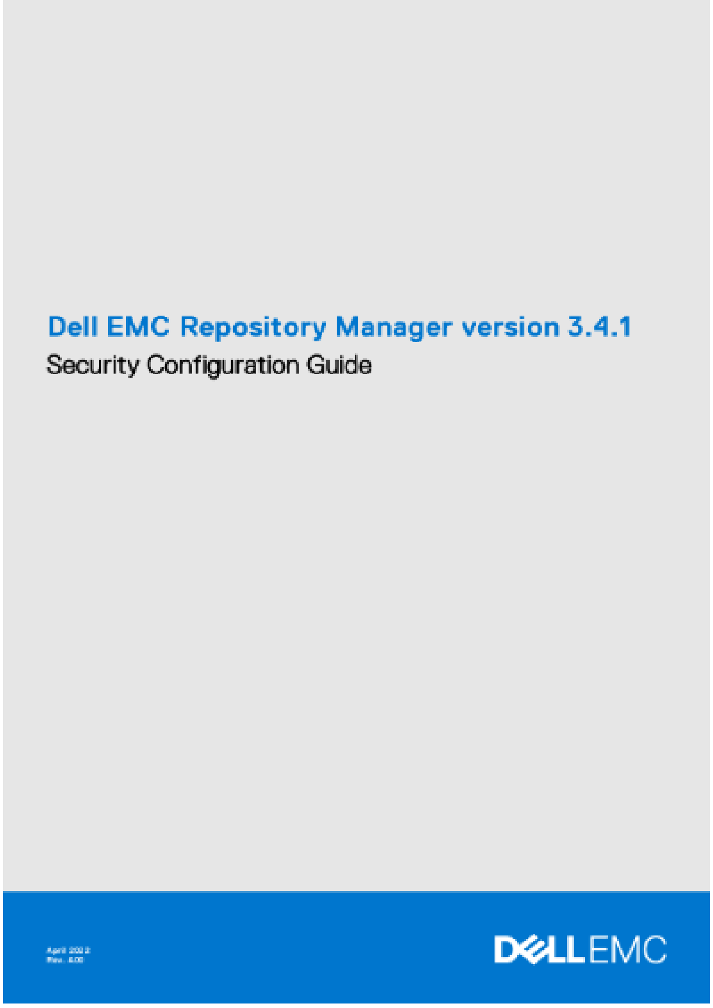


Dell EMC Repository Manager version 3.4.1
Security Configuration Guide

DELLEMC Repository Manager version 3.4.1 User Guide

Home » DELLEMC » DELLEMC Repository Manager version 3.4.1 User Guide

DELLEMC Repository Manager version 3.4.1 User Guide



Dell EMC Repository Manager version 3.4.1
Security Configuration Guide

April 2022
Rev. A00

Contents

Introduction

ⓘ	**NOTE:** A NOTE indicates important information that helps you make better use of your product
△	**CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.
⚠	**WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.
Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document. This document was accurate at publication time. To ensure that you are using the latest version of this document, go to https://www.dell.com/support.

Legacy disclaimers

The information in the publication is provided as-is. Dell Technologies makes no representations or warranties of any kind regarding the information in the publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages.
The Security Configuration Guide intends to be a reference. The guidance is provided based on a diverse set of installed systems and may not represent the actual risk/guidance to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. All aspects of this Security Configuration Guide are subject to change without notice and on a case-by-case basis. Your use of the information that is contained in this document or materials that are linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

Scope of the document

This document includes information about security features and capabilities of Dell EMC Repository Manager (DRM).

Audience

This document is intended for individuals who are responsible for managing security for Dell EMC Repository Manager.

Revision History

The following table presents the revision history of this document.

Table 1. Revision History

Revision	Date	Description
A00	April 2022	Initial release of the Dell EMC Repository Manager 3.4.1 Security Guideline Document

Document References

In addition to this guide, you can access the other guides available at dell.com/support. Dell EMC Repository Manager supports creating artifacts to update services for Dell systems using Dell System Update, Bootable ISO, and Server Update Utility Update. For configuration related information, see DSU, Bootable ISO and SUU User's Guide. For more information, see Dell EMC Repository Manager Software Support Matrix. Go to support site, click product support -> Dell EMC Repository
Manager to access the following documents:

- Dell EMC Repository Manager Version 3.4.1 User's Guide
- Dell EMC Repository Manager Version 3.4.1 Release Notes
- Dell EMC Repository Manager Software Support Matrix

Security resources

- Dell Security Advisories (DSA) dell.com/support/security
- Support knowledge base (KB) articles at https://www.dell.com/support/kbdoc/en-us/000177083/support-for-dellemc-repository-manager-drm

Getting help

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document.
This document was accurate at publication time. To ensure that you are using the latest version of this document, go to **dell.com/support**

Reporting security vulnerabilities

Dell EMC takes reports of potential security vulnerabilities in our products very seriously. If you discover a security vulnerability, you are encouraged to report it to Dell EMC immediately. For the latest on how to report a security issue to Dell, please see the Dell Vulnerability Response Policy on the Dell.com site.
Topics:

- Terms used in this document

Terms used in this document

Table 2. Terms used in this document

Terminology	Description
DRM	Dell EMC Repository Manager
DUP	Dell EMC Update Package
SUU	Server Update Utility
DSU	Dell EMC System Update
iDRAC	Integrated Dell Remote Access Controller
OMEnt	Open Manage Enterprise
OMIVV	Open Manage Integration for VMWare V Center
OMIMSSC	Open Manage Integration for Microsoft System Center

Deployment models

Dell EMC Repository Manager can be installed on the supported Microsoft Windows and Linux operating systems to generate the artifacts that can be used to deploy and upgrade the system. For more information about the installation, see Dell EMC Repository Manager User's Guide and Quick Installation Guide at dell.com/support.
Topics:

- Security profiles

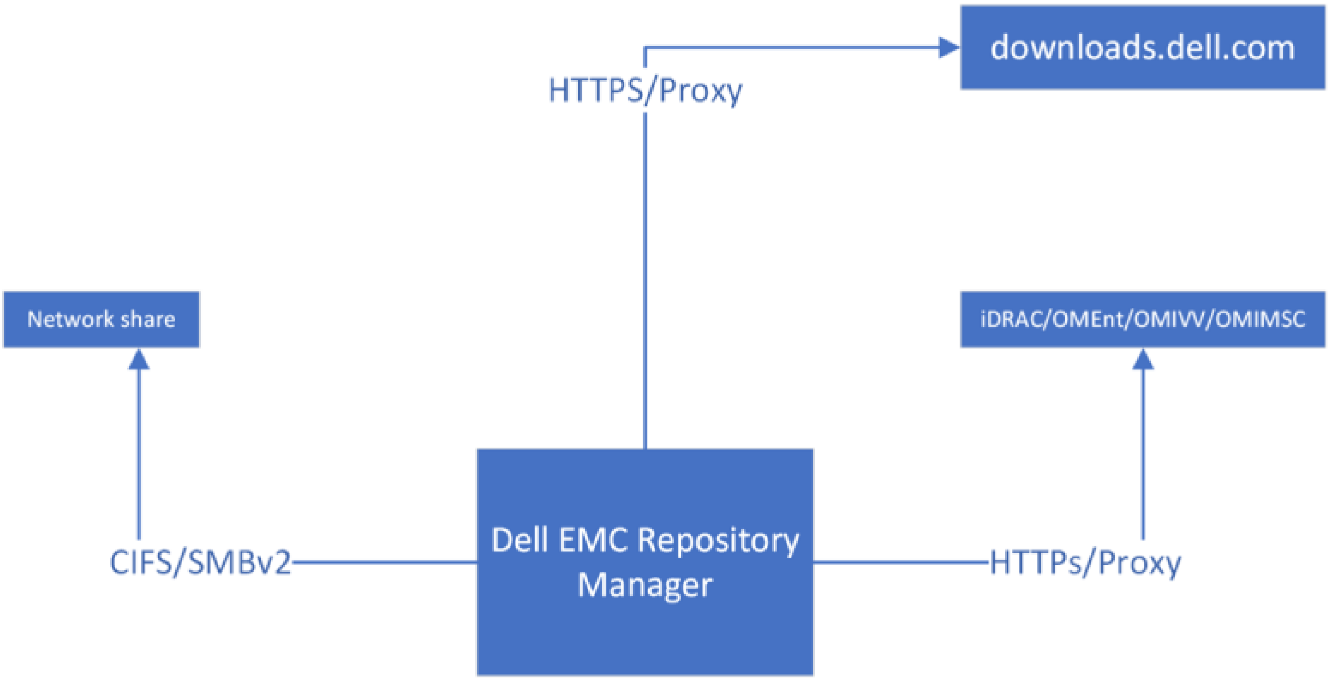
Security profiles

DRM has a default security profile for secure HTTPS access with a self-signed certificate during installations. The downloaded artifacts such as DUPs, catalogs, and plugins are signed by Dell.

Product and subsystem security

Security controls map

The Dell EMC Repository Manager (DRM) is an application within the Dell OpenManage portfolio that allows IT Administrators to manage system updates.
Dell Repository Manager provides a searchable interface that is used to create custom software collections, which are known as bundles and repositories of Dell Update Packages (DUPs).
These bundles and repositories allow for the deployment of multiple firmware updates at once.
The DRM User Interface (UI) interacts with the DRM service through HTTPs protocol.
Dell EMC Repository Manager (DRM) interacts with downloads.dell.com to download the DUPs, Catalogs, and other artifacts such as plugins and DRM updates through HTTPs protocol. DRM interacts with various consoles such as iDRAC and OME to collect inventory information over the HTTPs protocol.
This protocol is the only supported way to connect to the various consoles. Also, DRM interacts with any network or file share through CIFS or SMBv2 protocols.
The following figure displays the DRM security controls map:
Figure 1. Security Controls Map
As the diagram depicts, DRM interacts with downloads.dell.com through HTTPS protocol and with the network share through the CIFS/SMBv2.



Authentication

Access control

Dell EMC Repository Manager functions as a service which requires minimum privileges for Windows (Windows services) and Linux users (read or write access to drmusers) on a system to run and perform all the operations.

Login security settings

Remote connection security

DRM uses open-source library for remote connection using CIFS/SMBv2 and does not log the credentials mentioned for connections.

User and credential management

Dell EMC Repository Manager stores all the user credentials in a database with an encrypted format.
The database is password protected that user provides during the installation. |
The password can be modified by an administrator or a user with the administrative privileges. All the traffic between the
User interface (UI) and the service are managed using HTTPs.

Password Complexity

DRM Database password must contain at least eight characters that has at least one character each in upper case, lower case, integer, and special character.

Network security

DRM supports only HTTPs connection to connect downloads.dell.com, and then download the catalogs, DUPs, and plugins.
These artifacts are signed by Dell.
DRM performs SHA 256 hash verification and PGP sign verification for all the downloaded artifacts.

Network exposure
DRM can only be accessed within the system and cannot be reached by any other system over the network

Outbound ports

Outbound ports are used by Dell EMC Repository Manager Update when connecting to a remote system.
The table below lists the DRM outbound ports.

Table 3. Outbound ports

Port number	Layer 4 Protocol	Service
80	TCP	HTTP
139 or 445	TCP	SMB/CIFS

Table 3. Outbound ports (continued)

Port number	Layer 4 Protocol	Service
443	TCP	HTTPs

Data security

DRM stores all sensitive information, such as passwords, in databases in an encrypted format. DRM uses certificates for secure HTTP access (HTTPS).
DRM installs a java store and uses a self-signed certificate to secure HTTPS transactions.
DRM database is protected by a password that is provided by the user during the installation phase.
This password is stored in an encrypted format in a file that is locked using another layer of password.
The password that locks the file is generated randomly and varies according to various system parameters.

Auditing and logging

DRM creates log and stores in the working directory. The log files size between 1 MB to 10 MB. For more information about
Troubleshooting, or Log files, see the Dell EMC Repository Manager User's Guide available at **dell.com/support.**

Serviceability

The support website **https://www.dell.com/support** provides access to licensing information, product documentation, advisories, downloads, and troubleshooting information.
This information helps you to resolve a product issue before you contact support team.
Special login is not required to enable DRM for service personnel.
Ensure that you install security patches and other updates when available, including the Dell Repository Manager updates.

Product code integrity

The Dell EMC Repository Manager installer is signed by Dell. It is recommended that you verify the authenticity of the Dell EMC Repository Manager installer signature.

Miscellaneous configuration and management

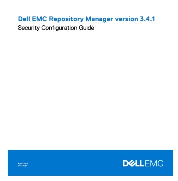
Dell EMC Repository Manager licensing

DRM has open-source approval for internal dependencies and is installed with the application on the box. It can also be found at https://opensource.dell.com/releases/drm/. For more information about licensing of Dell EMC Repository Manager, see the Dell EMC Repository Manager User's Guide available at **dell.com/support.**

Protect authenticity and integrity

To ensure the integrity of product, the installation and update of components for Dell EMC Repository Manager are signed.

Documents / Resources

 Dell EMC Repository Manager version 3.4.1 Security Configuration Guide	**DELLEMC Repository Manager version 3.4.1** [pdf] User Guide Repository Manager version 3.4.1, Manager version 3.4.1, version 3.4.1