# Dell EMC System Update version 1.9.2.0

## Security Configuration Guide

July 2021
Rev. A00

## Notes, cautions, and warnings

**NOTE:** A NOTE indicates important information that helps you make better use of your product.

**CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

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

# Contents

**Figures** ..... **4**

**Tables** ..... **5**

**Chapter 1: PREFACE** ..... **6**
Terms used in this document ..... 7

**Chapter 2: Deployment models** ..... **8**
Security profiles ..... 8

**Chapter 3: Product and Subsystem Security** ..... **9**
Security controls map ..... 9
Authentication ..... 9
Access control ..... 9
Login security settings ..... 10
Failed login behavior ..... 10
Remote connection security ..... 10
User and credential management ..... 10
Network security ..... 10
Network exposure ..... 10
Outbound ports ..... 10
Inbound ports ..... 11
Data security ..... 11
Auditing and logging ..... 11
Serviceability ..... 11
Product code integrity ..... 12

**Chapter 4: Miscellaneous Configuration and Management** ..... **13**
Dell EMC System Update licensing ..... 13
Protect authenticity and integrity ..... 13
Manage backup and restore in Dell EMC System Update ..... 13

# Figures

1 Security Controls Map..... 9

# Tables

1 Revision History....6
2 Terms used in this document....7
3 Outbound ports....10
4 Inbound ports....11

# 1

# PREFACE

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 System Update (DSU).

## Audience

This document is intended for individuals who are responsible for managing security for Dell EMC System Update.

## Revision History

The following table presents the revision history of this document.

**Table 1. Revision History**

| Revision | Date | Description |
|---|---|---|
| A00 | July 2021 | Initial release of the Dell EMC System Update 1.9.2.0 Security Guideline Document. |
| A00 | March 2021 | Initial release of the Dell EMC System Update 1.9.1.0 Security Guideline Document. |

# Document References

In addition to this guide, you can access the other guides available at **dell.com/support** . Since DSU supports an Update to the Server through iDRAC, see Integrated Dell Remote Access Controller User's Guide for any configuration-related queries. For the information about supported PowerEdge Servers, see Dell EMC Systems Management - OpenManage Software Support Matrix. Go to support site, click product support -> Dell EMC system Update to access the following documents:

- Dell EMC System Update Version 1.9 User's Guide
- Dell System Update 1.9 Release Notes

You can find the technical artifacts including white papers at **dell.com/support**

# Security resources

- Dell Security Advisories (DSA) **dell.com/support/security**
- Support knowledge base (KB) articles at **dell.com/support/kbdoc/en-us/000130590/dell-emc-system-update-dsu**

# 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 |
|---|---|
| DSU | Dell EMC System Update |
| DUP | Dell EMC Update Package |
| iDRAC | Integrated Dell Remote Access Controller |
| WMI | Windows Management Instrumentation |
| SSH | Secure Shell |

# 2

# Deployment models

You can deploy Dell EMC System Update on Microsoft Windows Server or Linux operating system through Dell Update Package (DUP) on supported Dell EMC PowerEdge servers. Dell EMC System Update supports online or offline method to deploy on the selected operating system through Dell Update Package. For more information on the deployment of Dell System Update, see Dell EMC System Update User's Guide at **dell.com/support**

**Topics:**


- Security profiles


## Security profiles

Dell EMC System Update has a default security profile for secure HTTP or HTTPS access with self-signed certificate during installations. It is recommended to replace the Certificate Authority (CA) signed certificates for a better security environment.

3

# Product and Subsystem Security

**Topics:**

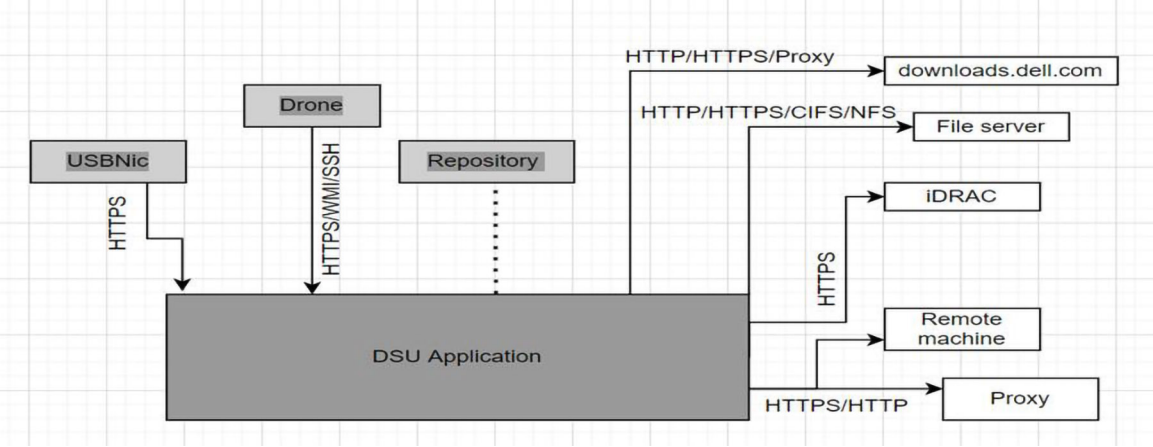

- Security controls map
- Authentication
- Login security settings
- User and credential management
- Network security
- Data security
- Auditing and logging
- Serviceability
- Product code integrity


## Security controls map

Dell EMC System Update is a script optimized update deployment tool that is used to apply Dell EMC updates such as applications, firmware, and drivers for Linux and Microsoft Windows operating systems. Using DSU, identifies the available updates, select the relevant updates, and deploy the updates on a single system or multiple systems through operating systems or integrated Dell Remote Access Controller(iDRAC) or iDRAC passthrough(connection to the iDRAC through redfish API to get relevant firmware update and deploy. System Credentials (share location credentials) used for repository or system (remote server) access are not stored within DSU.

The following figure displays the DSU security controls map:

**Figure 1. Security Controls Map**




## Authentication

### Access control

Dell EMC System Update allows only administrator console and root privilege console account to perform the operation.

# Login security settings

## Failed login behavior

DellEMC System Update (DSU) populate failed login message on console for wrong credential. For more information about failed login behavior of DSU, see the Dell EMC System Update User's Guide at **dell.com/support**

## Remote connection security

Dell EMC System Update uses open source library for remote connection using SSH and WMI and it does not log the credentials mentioned for connections.

# User and credential management

Dell EMC System Update supports HTTPS and HTTP connections.

# Network security

Dell System Update uses a pre-configured firewall to enhance security by restricting inbound and outbound network traffic to the TCP and UDP ports. The tables in this section lists the inbound and outbound ports that Dell System Update uses.

## Network exposure

Dell System Update uses inbound and outbound ports when communicating with remote systems.

## Outbound ports

Outbound ports can be used by Dell System Update when connecting to a remote system..

The ports that are listed in the following table are the Dell System Update outbound ports.

**Table 3. Outbound ports**

| Port number | Layer 4 Protocol | Service |
|---|---|---|
| 7 | TCP, UDP | ECHO |
| 22 | TCP | SSH |
| 25 | TCP | SMTP |
| 53 | UDP, TCP | DNS |
| 67,68 | TCP | DHCP |
| 80 | TCP | HTTP |
| 88 | TCP, UDP | Kerberos |
| 111 | TCP, UDP | ONC RPC |
| 123 | TCP, UDP | NTP |
| 161-163 | TCP, UDP | SNMP |
| 389 | TCP, UDP | LDAP |
| 443 | TCP | HTTPS |

**Table 3. Outbound ports (continued)**

| Port number | Layer 4 Protocol | Service |
|---|---|---|
| 448 | TCP | Data Protection Search Admin REST API |
| 464 | TCP, UDP | Kerberos |
| 514 | TCP, UDP | rsh |
| 587 | TCP | SMTP |
| 636 | TCP, UDP | LDAPS |
| 902 | TCP | VMware ESXi |
| 2049 | TCP, UDP | NFS |
| 2052 | TCP, UDP | mountd, clearvisn |
| 3009 | TCP | Data Domain REST API |

## Inbound ports

The inbound ports that are available to be used by a remote system when connecting to Dell System Update remote.

The ports that are listed in the following table are the Dell System Update inbound ports.

**Table 4. Inbound ports**

| Port number | Layer 4 Protocol | Service |
|---|---|---|
| 22 | TCP | SSH |
| 80 | TCP | HTTP |
| 443 | TCP | HTTPS |
| 135 | TCP | WMI |

# Data security

DSU does not store any data in databases also from input dependencies libraries. DSU uses certificates for secure HTTP access (HTTPS). By default, DSU installs GPG keys and uses the self-signed certificate for the HTTPS secure transactions. For better security, it is recommended to use the Certificate Authority (CA) signed or custom certificates.

# Auditing and logging

DSU administration console generate all the relevant logs in default location or user provided location. DSU supports Log file retention , compression and file rollover. Log file sizes are defined to 5 MB limit. A descriptive and clear log messages are provided. For more information about Troubleshooting, Log files, see the Dell EMC System Update 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 Dell EMC System Update for service personnel. If the troubleshooting bundle is not sufficient, the personnel can enable the root user to collect more information.

Ensure that you install security patches and other updates when they are available, including the Dell EMC System Update.

# Product code integrity

The Dell EMC System Update software installer is signed by Dell. It is recommended that you verify the authenticity of the Dell EMC System Update installer signature.

# 4

# Miscellaneous Configuration and Management

**Topics:**


- Dell EMC System Update licensing
- Protect authenticity and integrity
- Manage backup and restore in Dell EMC System Update


## Dell EMC System Update licensing

DSU has open source approvals for the internal dependencies and gets installed with the application on the box. It can also be find at **opensource.dell.com/releases/DSU/** For more information about licensing of Dell EMC System Update, see the *Dell EMC System Update User's Guide* available at **dell.com/support**

**NOTE:**

Any active license can be used for Dell EMC System Update 1.9.1.0 versions. Licenses used from previous instances of Dell EMC System Update or downloaded again from the Digital Locker can be used for current instances of Dell EMC System Update.

## Protect authenticity and integrity

To ensure product integrity, the Dell EMC System Update installation and update components are signed.

To ensure communication integrity, it is recommended to use CA-signed certificate.

## Manage backup and restore in Dell EMC System Update

For information about backup and restore, see the Dell EMC System Update User's Guide available at **https://www.dell.com/support/home/?app=knowledgebase**