Dell EMC OpenManage Server Administrator Security Configuration Guide

September 2021
Rev. A00

DELL Technologies

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

1

Overview

Server Administrator provides a comprehensive one-to-one systems management solution in two ways: from an integrated web browser-based graphical user interface (GUI) and from a command line interface (CLI) through the operating system. Server Administrator enables system administrators to manage systems locally and remotely on a network. It enables system administrators to focus on managing their entire network by providing comprehensive one-to-one systems management. In the context of Server Administrator, a system refers to a stand-alone system, a system with attached network storage units in a separate chassis, or a modular system consisting of one or more server modules in a modular enclosure. Server Administrator provides information about:

- Systems that are operating properly and systems that have problems
- Systems that require remote recovery operations

Server Administrator provides easy-to-use management and administration of local and remote systems through a comprehensive set of integrated management services. Server Administrator is the sole installation on the system being managed and is accessible both locally and remotely from the Server Administrator home page. Remotely monitored systems may be accessed through dial-in, LAN, or wireless connections. Server Administrator ensures the security of its management connections through role-based access control (RBAC), authentication, and secure socket layer (SSL) encryption.

For information about installation, configuration, and usage of this software, see the documents mentioned in Document references.

Topics:

Legal disclaimer

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL 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. 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 or 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 contained in this document or materials 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 describes the security configurations for Server Administrator on all supported operating systems.

NOTE: The security details for the sub-systems that Server Administrator interacts with, namely the Integrated Dell Remote Access Controller (iDRAC) and Dell EMC system firmware (BIOS), are beyond the scope of this document.

Audience

This document is intended for individuals who are responsible for managing security on servers where Server Administrator is installed.

Document references

Server Administrator documents are available online at www.dell.com/openmanagemanuals.

Documents	Descriptions
Dell EMC Systems Software Support Matrix	Provides information about the various systems, the operating systems supported by these systems, and the components that can be installed on these systems.
Dell EMC OpenManage Server Administrator Release Notes	*Explains the new features and existing issues in the product.*
Dell EMC OpenManage Server Administrator Installation Guide	Provides instructions to help you install Dell EMC OpenManage Server Administrator.
Dell EMC OpenManage Management Station Software Installation Guide	Provides instructions on how to install DellEMC OpenManage management station software.
Dell EMC OpenManage SNMP Reference Guide	Provides the details of Simple Network Management Protocol (SNMP) and Management Information Base (MIB).
Dell EMC OpenManage Server Administrator CIM Reference Guide	Explains the Common Information Model (CIM) provider, which is an extension of the standard Management Object Format (MOF) file.
Dell EMC Messages Reference Guide	Lists the messages that are displayed in your Server Administrator home page Alert log or on your operating system's event viewer.
Dell EMC OpenManage Server Administrator Command Line Interface Guide	Explains the command line interface for Server Administrator.
Dell EMC OpenManage Server Administrator User's Guide	Provides an introduction about the product, supported operating systems, and browsers.

Security resources

1. Go to www.dell.com/support/security.
2. In the **Product Name** field, type OpenManage.
3. Select the required OpenManage version.

Reporting security vulnerabilities

Dell EMC takes reports of potential security vulnerabilities in the products seriously. If you discover a security vulnerability, you are encouraged to report it to Dell EMC immediately.

For more information on how to report a security issue to Dell EMC, see Dell Vulnerability Response Policy.

Follow us online

For more information on Dell products, see Security and Trust Center.

2

Security quick references

Topics:

Deployment models

Server Administrator does not explicitly have a deployment tool. Server Administrator can be installed securely through one of the following ways:

- OpenManage DVD (OMDVD)

  This is the physical disc which contains Server Administrator packages for all supported Operating systems

- Dell EMC support site—www.dell.com/support

  Server Administrator packages is available in the form of a Dell EMC Update Package (DUP) or GNU zip file. The integrity of the package can be verified with the checksum listed in the support web page.

- Dell Linux repository—supported for Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems

  The Dell EMC System Update (DSU) provides the linux repository for installing Server Administrator on supported Linux-based operating systems. Installations through DSU also imports Dell GPG keys for the packages so that Server Administrator packages downloaded from DSU are trusted.

- Dell VUM repository—supported for VMware ESXi

  Server Administrator vibs are available through the Dell VUM repository for supported ESXi operating systems.

Administrator/root privileges are required for users to install Server Administrator. For installations instructions for supported operating systems, see the Installation Guide for the corresponding supported operating system.

Security profiles

Server Administrator packages different components whose configurations are described in the following sections.

Webserver

- Server Administrator bundles the Apache Tomcat webserver that uses a self-signed certificate for HTTPS connections by default. To ensure system security, it is recommended that you generate a new X.509 certificate, reuse an existing X.509 certificate, or import a certificate chain from a Certification Authority (CA). To avoid encountering such warning messages about the certificate, the certificate used must be from a trusted CA. For more information about X.509 Certificate Management, see *Dell EMC OpenManage Server Administrator User's Guide* to import the CA signed certificate.
- The webserver supports SSL protocols TLSv1.2 and TLSv1.3. Using TLSv1.3 gives the maximum security for all the connections to web interface.
- The default port by which the web interface is made accessible is 1311. Change this port settings as per your organization security requirements.
- The key signing algorithm for the webserver supports SHA-256 and SHA-512. The default algorithm is SHA-256.
- The Apache Tomcat webserver uses the data encryption algorithm between the client and webserver for TLS web communications. For more information, see Cryptography. By default, the server administrator generates the keystore file on installation and at runtime the keystore password for the HTTPS connection is generated.
- The configuration of maximum connections for the webserver is not supported. It is recommended to have only one session for users with root/administrator privileges. The number of active sessions to the web interface is available through the Session Management page of Server Administrator.

- Session time-out configuration is available to set the web interface idle timeout duration. The default timeout is 30 minutes.

Role-based access

Role-based access is given to all local and domain users. Server Administrator grants different access rights based on the user's assigned group privileges by the operating system. The user privilege levels are User, Administrator, and Elevated Administrator.

User Privilege level	Access Type		Description
	View	Manage	
User	Yes	No	Can view most information.
Administrator	Yes	Yes	Can configure and perform shutdown actions, configure Auto Recovery actions in case a system has a nonresponsive operating system, and clear hardware, event and command logs. Administrators can also configure the system to send emails.
Elevated Administrator (Linux only)	Yes	Yes	Can view and manage information.

SNMP

Server Administrator supports the Simple Network Management Protocol (SNMP-a systems management standard-on all supported operating systems. SNMP versions v1 and v2c are supported by Server Administrator. SNMP versions v1 and v2c are supported by Server Administrator.

By default, the SNMP feature is disabled. This can be enabled through the installer. The default SNMP agent configuration usually includes a SNMP community, named as Public. For security reasons, you must rename the default SNMP community name.

Server Administrator uses the operating system configuration for SNMP. You can configure the SNMP agent to change the community name and to send traps to a management station. For information about the configuration of SNMP is documented in *Dell EMC OpenManage Server Administrator User's Guide.*

Remote enablement

Server Administrator features the distributed web server (DWS) which enables Server Administrator to remotely monitor and manage the systems (managed node) where Remote Enablement feature is installed. This feature requires generation of a server certificate for a https listener in Windows and WSMan in Linux or ESXi. The server certificate can be self-signed or a certificate from a trusted CA.

The managed system login screen displays an Ignore certificate warnings check box to support usage of self-signed certificate. You should use this option with discretion. It is recommended that you use it only in trusted Intranet environments.

The network connections and security between managed node and DWS is not the scope for the Server Administrator. System administrators shall ensure proper secure connections and connectivity between managed node and DWS.

The installation and configuration of remote enablement is available in the Installation guide, see *Dell EMC OpenManage Installation Guide—Linux* and *Dell EMC OpenManage Installation Guide—Windows*.

SELinux support

Security-Enhanced Linux (SELinux) is an optional security architecture that is integrated into the kernels of Red Hat Enterprise Linux operating systems. You can now install an optional SELinux security policy for Server Administrator. If the SELinux policy is set to **Permissive** mode, all attempted violations are logged by the kernel to audit log. If the policy is set to **Enforcing** mode, disallowed actions are prevented, and all attempted violations are logged by the kernel to audit log.

Installing the optional Server Administrator SELinux package with SELinux in **Enforcing** mode disallows any actions that are not defined in the policy by Server administrator services and facilitates system hardening. For more information about SELinux, see Using SELinux.

3

Product and subsystem security

Topics:

Security control maps

Server Administrator interfaces are described in the following figure. The interfaces are:

- Web interface through the Apache Tomcat webserver (HTTPS)
- Remote system monitoring through the mechanism of CIM-based providers and WSMan (HTTPS)
- Remote system monitoring through SNMP
- Command line utilities like omreport and omconfig that provide information of the system components managed by the Server Administrator
- Operating system and BMC or iDRAC communication through IPMI
- BIOS communication interface using System Management Driver (dcdbas in Windows)

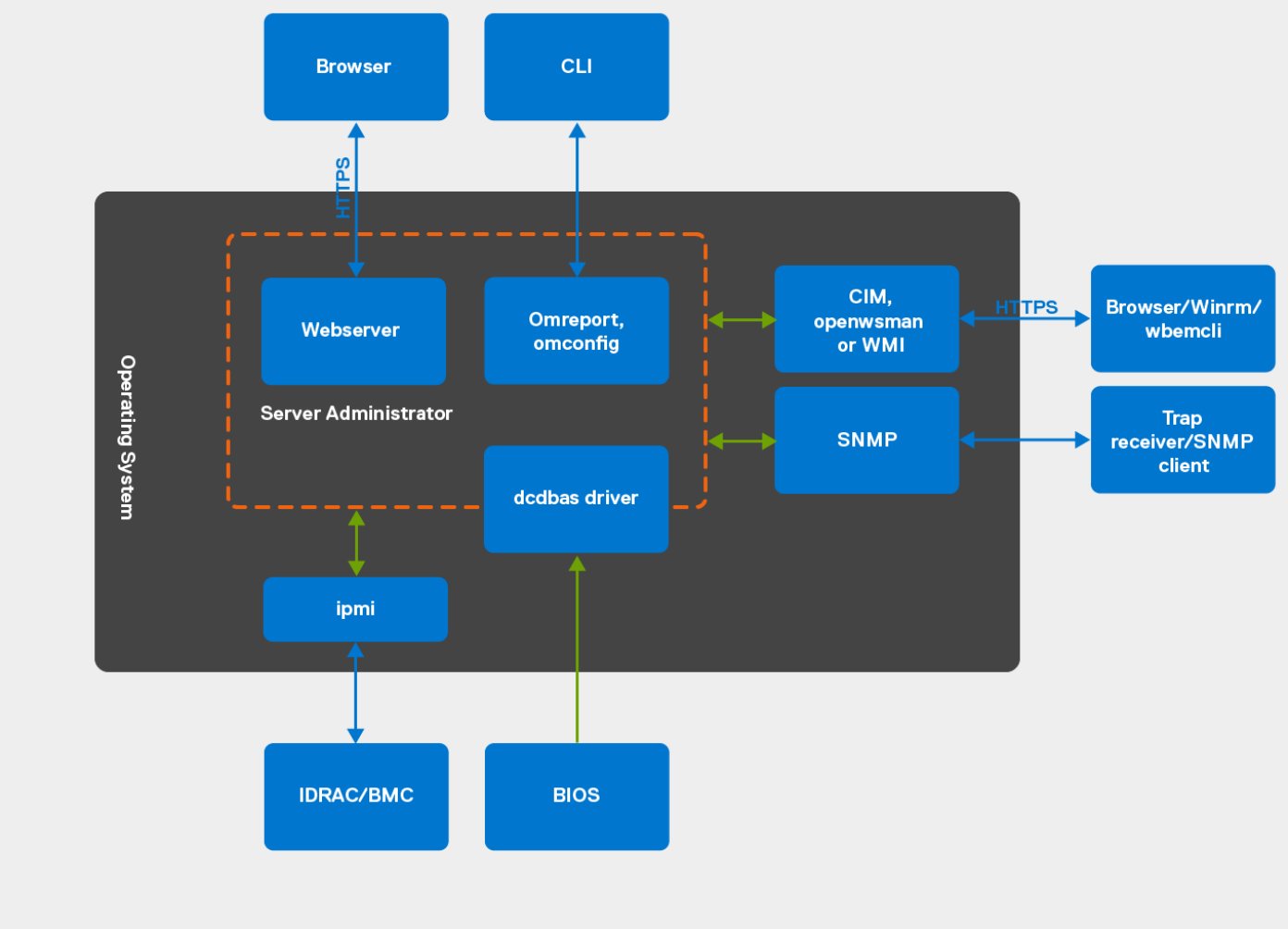

Figure 1. Server Administrator interfaces

Authentication

Server Administrator provides a login web interface for customers to provide user credentials. Server Administrator by default uses the operating system based or Active Directory based security configurations and there is no explicit user credentials management is supported by the product. As authentication is dependent on operating system, the login interface performs basic sanity checks on the input credentials.

Login security settings

Server Administrator does not support login security settings. The account lockout policy are dependent on the operating system configured policies. For any invalid attempt to login to Server Administrator's web interface, a generic error is displayed.

Authentication types and setup

The Server Administrator authentication scheme ensures that the correct access types are assigned to the correct user privileges. Additionally, when the command line interface (CLI) is invoked, the Server Administrator authentication scheme validates the context within which the current process is running. This authentication scheme ensures that all Server Administrator functions, whether accessed through the Server Administrator home page or CLI are authenticated.

Table 1. Authentication interfaces of supported operating systems

Supported operating system	Authentication interfaces
Windows	On supported Microsoft Windows operating systems, Server Administrator uses Integrated Windows Authentication (formerly called NTLM) to authenticate. This authentication system allows Server Administrator security in an overall security scheme for your network.
Linux	On supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server operating systems, Server Administrator uses various authentication methods based on the Pluggable Authentication Modules (PAM) library. Users can log in to Server Administrator either locally or remotely using different account management protocols, such as LDAP, NIS, Kerberos, and Winbind.
VMware ESXi	ESXi Server authenticates users accessing ESXi hosts using the vSphere/VI Client or Software Development Kit (SDK). The default installation of ESXi uses a local password database for authentication. ESXi authentication transactions with Server Administrator are also direct interactions with the vmware-hostd process. **NOTE:** On systems running VMware ESXi, Server Administrator does not support Active Directory (AD) domain user, when connecting from Server Administrator web server (DWS).

Unauthenticated interfaces

The login webpage for the web interface provides the following information which does not require user to login to the product.

- Link to Help that displays information about all the product features.
- Links to support webpage, product manuals.

User and credential management

Server Administrator by default uses the operating system based or Active Directory based security configurations and there is no explicit user credentials management is supported by the product.

Authorization

The authorization details for users configured on the system and configuring roles to those users are described.

General authorization settings

By default, all users can login to Server Administrator with the operating system privileges assigned to them. To protect access to your critical system components, assign a password to every user account that can access Server Administrator. Disable guest accounts for supported Windows operating systems to protect access to your critical system components. Consider renaming the guest accounts so that remote scripts cannot enable the accounts using the default guest account names. For more information, see *Dell EMC OpenManage Server Administrator User's Guide.*

Default authorizations

All local and domain users have read access to the product. Users with Administrator privileges have modification rights.

RBAC privileges

Role-Based Access Control (RBAC) manages security by determining the operations that can be executed by persons in particular roles. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. With RBAC, security administration corresponds closely to the organization structure. For user privilege access information, see Authentication types and setup. For information about creating users with different roles, see *Dell EMC OpenManage Server Administrator User's Guide.*

Configuring roles

In addition to the role assigned by operating systems, users in Linux-based operating system can be configured for addition privileges. This is achieved by editing the omarolemap file installed by the product. This modification can be done only by users with root privileges.

The following are the best practices to be considered while working with the omarolemap file:

- Do not delete the default entries in the omarolemap file.
- Do not change the omarolemap file permissions or file format.
- Do not use the loop back address for <Host_Name>. For example: localhost or 127.0.0.1.
- When the omarolemap file is copied from one machine to another machine, file permissions and the entries of the file needs to be rechecked.

For more information, see *Dell EMC OpenManage Server Administrator User's Guide.*

Network security

Server Administrator does not access any external URLs except for the update catalog from Dell for getting information about the latest version of the product. The catalog access is through https requests through the curl library.

Network exposure

The webserver supports both IPv4 and IPv6 interfaces. The webserver runs on port 1311 by default. These can be configured through the webserver preferences in order to meet the organization security requirements.

Communication security settings

For information, see Cryptography.

Firewall settings

For more information, see the Firewall configuration and FAQs sections in *Dell EMC OpenManage Server Administrator User's Guide.* and Installation Guides.

Data security

Server Administrator monitors and enumerates Server hardware and operating system related data and does not access any other data on the installed managed nodes. The product uses a proprietary data structure in memory to store the data about the monitored system components. This data is available to users as per the RBAC privileges using the CLI/UI or the WSMan/WMI and SNMP interfaces. No modification is possible by any users except for the configuration options available to the users with Administrator/root privileges.

Server Administrator only stores the software configuration data on the server. The software configuration data is available in plain text format with read-only access for all non-administrator accounts.

User credentials input through the login web interface of the product are not stored either temporarily or permanently on the server.

Cryptography

Server Administrator is accessed over a secure HTTPS connection using secure socket layer (SSL) technology to ensure and protect the identity of the system being managed. Java Secure Socket Extension (JSSE) is used by supported Microsoft Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server operating systems to protect the user credentials and other sensitive data that is transmitted over the socket connection when a user accesses the Server Administrator home page.

The webserver supports the following settings:

- SSL: TLS v1.2, TLS v1.3
- Ciphers suites:

  TLSv1.3:
  TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256,TLS_AES_128_CCM_8_SHA256,TLS_AES_128_CCM_SHA256

  TLSv1.2:
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- Encryption: SHA-256, SHA-512

Cryptographic configuration options

The SSL protocols, cipher suites, and encryption can be configured through the webserver preferences.

Certificate management

For more information about installing and managing the X.509 certificate for webserver, see the X.509 Certificate Management section in *Dell EMC OpenManage Server Administrator User's Guide.*

Auditing and logging

Server Administrator allows you to view and manage hardware, alert, and command logs. All users can access logs and print reports from either the Server Administrator web interface or from its command line interface. Users must be logged in with Administrator privileges to clear logs or must be logged in with Administrator or Power User privileges to email logs. Any invalid access through the Server Administrator is logged in the operating systems event log.

Logs

Server Administrator provides the following logs:

Hardware Log	There are two available hardware logs depending on your system - the Embedded System Management (ESM) log and the System Event Log (SEL). The ESM log and SEL are each a set of embedded instructions that can send hardware status messages to systems management software. Each component listed in the logs has a status indicator icon next to its name.
Alert Log	The Server Administrator generates events in response to changes in the status of sensors and other monitored parameters. These events are tracked in alert log.
Command Log	The Command log tracks all the commands issued by Server Administrator users.

Log management

Following actions can be performed on the logs from UI.

Table 2. User actions from the UI

Name	Description
Print	Prints a copy of the log to your default printer.
Export	Saves a text file containing the log data (with the values of each data field separated by a customizable delimiter) to a destination, you specify.
Email	Creates an email message that includes the log content as an attachment.
Clear Log	Erases all events from the log.
Save As	Saves the log content in a .zip file.
Refresh	Reloads the log content in the action window data area.

For Alert logs, SNMP traps can be configured based on different severity level (Informational, Warning, Critical).

Log protection

There is no explicit handling of log message with encryption.

Logging format

OMSA internally uses xml format for logs. Sample log entries are:

Feature Usage log:

```
<OMSA_GUI><featureCode>OMSASystemHealth</featureCode><action>read</action><trackTime>Wed
Jul 28 11:54:20 2021</trackTime>
```

Alert log:

```
<LogEntry><TimeStamp>1632306727</TimeStamp><DateTime>Wed Sep 20
16:02:07 2021</DateTime><ComputerName>WIN- XXXXXXXX
</ComputerName><Type>1</Type><ID>5354</ID><EnhMsgID>PSU0908</EnhMsgID><Link>help/hip/en/
msgguide/wwhelp/wwhimpl/common/html/wwhelp.htm?context=Messages_Guide&amp;topic=5354</
Link><UserInfo/><Source>Server Administrator</Source><Category>Instrumentation Service</
Category><Description>Severity: Critical, Category: System Health, MessageID: PSU0908,
Message: Power lost on power unit PS2 Status.</Description><Data/></LogEntry>

<LogEntry><TimeStamp>1632306727</TimeStamp><DateTime>Wed Sep 20
16:02:07 2021</DateTime><ComputerName>WIN- XXXXXXXX
</ComputerName><Type>4</Type><ID>5012</ID><EnhMsgID>SYS114</EnhMsgID><Link>help/hip/en/
msgguide/wwhelp/wwhimpl/common/html/wwhelp.htm?context=Messages_Guide&amp;topic=5012</
Link><UserInfo/><Source>Server Administrator</Source><Category>Instrumentation Service</
Category><Description>Severity: Informational, Category: System Health, MessageID:
SYS114, Message: The IPMI status for the interface: OS, Baseboard Management
Controller (BMC): present, Sensor Data Records (SDR): present, System Event
Log (SEL): present.</Description><Data/></LogEntry>
```

Command log: User login, logout, and failed user login format

```
<LogEntry><TimeStamp>1632295603</TimeStamp><DateTime>Wed Sep
20 12:56:43 2021</DateTime><ComputerName>WIN-
XXXXXXXX </ComputerName><Type>4</Type><ID>5301</ID><UserInfo>Administrator</
UserInfo><Source>CSDA</Source><Description><SMStatus>0</SMStatus><Parameter
name="priviliges" value="admin"/><Parameter name="ipaddr"
value="fe80:0:0:0:6de5:834e:2724:e936%13"/></Description><Data/></LogEntry>
```

```
<LogEntry><TimeStamp>1632295593</TimeStamp><DateTime>Wed Sep 20
12:56:33 2021</DateTime><ComputerName>WIN-XXXXXXXX</ComputerName><Type>4</Type><ID>5302</
ID><UserInfo>Administrator</UserInfo><Source>CSDA</Source><Description>User_Logged_out</
Description><Data/></LogEntry>

<LogEntry><TimeStamp>1632295598</TimeStamp><DateTime>Wed Sep
20 12:56:38 2021</DateTime><ComputerName>WIN-
XXXXXXXX </ComputerName><Type>1</Type><ID>5301</ID><UserInfo>Administrator</
UserInfo><Source>CSDA</Source><Description><SMStatus>-1</SMStatus><Parameter
name="priviliges" value="NONE"/><Parameter name="ipaddr"
value="fe80:0:0:0:6de5:834e:2724:e936%13"/></Description><Data/></LogEntry>
```

Serviceability

There is no explicit serviceability feature in Server Administrator.

Security updates and patching

Server Administrator does not have a mechanism of updating or patching the product by itself.

Product version information related to new releases are available in the About section of the product which can be accessed through the web interface or CLI.

To apply patches or upgrade the software to the latest version, see the installation guide.

Code and product authenticity and integrity

All packages and binaries of Server Administrator are signed with Dell digital signature (Dell Inc). The signature of vendor libraries that are shipped with Server Administrator are verified before integration into the software.

Authenticity and integrity verification

- Server Administrator's System Management Driver for supported Windows operating systems is signed by Microsoft (Microsoft Windows Hardware Compatibility Publisher) and Dell (Dell Inc).
- All windows binaries of the product can be verified by checking the signature of the file which is Dell signed (Dell Inc).
- Installations through DSU also imports Dell GPG keys for the packages, so that Server Administrator packages downloaded from DSU are trusted.
- For RHEL and SLES rpm packages, GPG key is provided in the webpack bundles and OMDVD, so that the authenticity of the packages can be verified.
- The Integrity of the product packages downloaded from Dell support site can be verified with the checksum provided alongside the product package downloads.
- Server Administrator vibs available from the Dell VUM repository are signed by VMware.

4

Miscellaneous configuration and management elements

Topics:

Customer modification and customization

Server Administrator installations can be modified after install to add or remove features as required. This is only available through Linux install script and Windows installer of the product on supporting operating systems.

5

Internal security information

Topics:

Embedded component usage

Table 3. List of third-party components

Third-party components	Version
Oracle Java Runtime Environment	11.0.11
Apache Tomcat	9.0.46
Libcurl	7.77.0
Libxml2	2.9.12
Openwsmandll.dll	2.2.3.9
OpenSSL (libssl)	1.1.1
Linux-PAM (Pluggable Authentication Modules for Linux) (libpam)	NA (built-in)
libxslt	1.1.34
xalan.jar	2.7.2
xerces.jar	2.12.1
commons-compress-1.19.jar	1.19

Internally discovered issues

For more information, see the Release Notes of the product.

6

Accessing support content from the Dell EMC support site

Access supporting content related to an array of systems management tools using direct links, going to the Dell EMC support site, or using a search engine.

- Direct links:
  - For Dell EMC Enterprise Systems Management and Dell EMC Remote Enterprise Systems Management—https://www.dell.com/esmmanuals
  - For Dell EMC Virtualization Solutions—www.dell.com/virtualizationsolutions
  - For Dell EMC OpenManage—https://www.dell.com/openmanagemanuals
  - For iDRAC—https://www.dell.com/idracmanuals
  - For Dell EMC OpenManage Connections Enterprise Systems Management—https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - For Dell EMC Serviceability Tools—https://www.dell.com/serviceabilitytools
- Dell EMC support site:
  1. Go to https://www.dell.com/support.
  2. Click **Browse all products**.
  3. From the **All products** page, click **Software**, and then click the required link.
  4. Click the required product and then click the required version.

Using search engines, type the name and version of the document in the search box.

7

Contacting Dell EMC

Topics:

- Getting help

Getting help

To get information related to the contents in this document, please contact Dell EMC support at www.dell.com/support.

To provide feedback on this documentation, email us at support@dell.com.