ScaleIO®

Version 2.0.1.x

Security Configuration Guide

302-003-671

REV 02

EMC²

Copyright © 2017 Dell Inc. or its subsidiaries. All rights reserved.

Published March 2017

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

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. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

Tables **5**

Preface **7**

Chapter 1 **Introduction** **9**
Overview....10

Chapter 2 **Access Control Settings** **11**
General.... 12
User authentication....13
Default accounts.... 13
Authentication configuration....14
Non-disruptive SNMP upgrade issues.... 14
User authorization....15
Login banner.... 16
Component access control....16
Component authentication....16
Component authorization.... 17

Chapter 3 **Log Settings** **19**
Log description....20
Log management and retrieval....22

Chapter 4 **Communication Security Settings** **25**
Port usage....26
Network encryption....27

Chapter 5 **Data Security Settings** **31**
Data integrity....32

Chapter 6 **Known Issues** **33**
Known Issues....34

TABLES

1 Default accounts.....13
2 Local and LDAP User roles and permissions.....15
3 Log files.....20
4 Port usage.....26

Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions 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 on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Related documentation

The release notes for your version includes the latest information for your product.

The following EMC publication sets provide information about your ScaleIO or ScaleIO Ready Node product:

- ScaleIO software (downloadable as ScaleIO Software <version> Documentation set)
- ScaleIO Ready Node with AMS (downloadable as ScaleIO Ready Node with AMS Documentation set)
- ScaleIO Ready Node no AMS (downloadable as ScaleIO Ready Node no AMS Documentation set)
- VxRack Node 100 Series (downloadable as VxRack Node 100 Series Documentation set)

You can download the release notes, the document sets, and other related documentation from EMC Online Support.

Typographical conventions

EMC uses the following type style conventions in this document:

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values

|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support

Go to EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.

CHAPTER 1

Introduction

This guide provides an overview of the security settings available in ScaleIO to ensure secure operation of the product.

- Overview 10

Overview

This topic provides an overview of the product's security features.

Security settings are divided into the following categories:

- *Access Control Settings* describes the settings available to limit access by end-user or external product components.
- *Log Settings* describes settings related to the logging of events.
- *Communication Security Settings* describes settings related to security for the product's network communications.
- *Data Security Settings* describes settings available to ensure protection of the data handled by the product.

CHAPTER 2

Access Control Settings

This section describes the access control settings used to protect resources against unauthorized access. Topics include:

- General 12
- User authentication 13
- Component access control 16

General

This topic describes access control settings supported by the system.

- User roles and passwords are needed to access the MDM. User roles with different access permissions can be assigned to users. Both local and LDAP authentication are supported. For more information, see the chapter "Security and User Management" in the *ScaleIO User Guide*.
- Limited MDM access mode—a system can be configured to allow read-only access to the MDM by remote clients. In this mode, only local users connecting to the MDM using the IP address 127.0.0.1 have full configuration privileges.
- Restricted SDC mode—a system can be configured to only allow "approved" SDCs to connect to the MDM.
- Access to the ScaleIO Gateway requires defining a dedicated user. This user may either be a local user or an LDAP user. For more information, see the *ScaleIO User Guide*, or *ScaleIO User Roles and LDAP Usage Technical Notes*.
- Access to the Installation Manager (IM) requires a user name and password. The user to be used is the ScaleIO Gateway user.
- Access to the REST gateway requires a password.
- REST authenticates user access, using the *gatewayAdminPassword* and*mdmPassword* (for more information, see the appendix "REST API Reference" in the *ScaleIO User Guide*).
- SSL authentication of internal components to the MDM—allows secure authentication of ScaleIO SDS components to the MDM using a Public and Private Key (Key-Pair) associated with a certificate. The trust is established when adding the SDS, and reconnecting will require reauthentication.
- Secure connectivity with external components—allows external components to authenticate the MDM with a certificate and authenticate back to the MDM with a user name and password. After authentication, communication between the MDM and external components is performed using TLS (Transport Layer Security) protocols. External components include: IM client, CLI client, GUI client, vSphere plug-in, and ScaleIO Gateway. The same method is used between the IM client and LIAs.
- IM/Gateway access to the LIA may be restricted to predefined IP addresses, by configuring the list of trusted IP addresses in the file:
  - Windows: `C:\Program Files\emc\scaleio\LIA\cfg\conf.txt`
  - Linux: `/opt/emc/scaleio/lia/cfg/conf.txt`
- A manually generated public-private key pair can be used to perform SSH key authentication, instead of passwords, between the ScaleIO Gateway and ScaleIO system servers.
- An RSA LockBox is used to store MDM credentials on the ScaleIO Gateway. These credentials are required for authentication purposes by the SNMP trap sender and ESRS.
- SNMP—the SNMP trap sender can be enabled or disabled using one of the methods listed below. The feature is disabled by default. For detailed information, see the appendix "SNMP Trap Support, Configuring SNMP properties after deployment" in the *ScaleIO User Guide*.
  - During deployment (on Linux and Windows only)

  - Configuring the `gatewayUser.properties` file located on the ScaleIO Gateway.
  - Using the REST API
- REST feature enabler—access to the REST gateway can be blocked by configuring the `gatewayUser.properties` file located on the ScaleIO Gateway. The feature is enabled by default. For detailed information, see the appendix "REST API Reference, Configuring the Gateway by editing the user properties file", in the *ScaleIO User Guide*.

Note

OpenSSL 64-bit v1.0.1 or higher is required for secure authentication. In Linux, this version of OpenSSL is only supported in CentOS and RHEL 6.5 or higher.

User authentication

This section describes the user authentication settings that control the process of verifying an identity claimed by a user for accessing the product.

Default accounts

This topic provides details about the system's default accounts.

Table 1 Default accounts

User Account	Password	Description
Installation Manager (IM) admin user	Password is created by the admin at the beginning of the installation process	Lets the user issue installation commands in the IM web client. The IM has a default admin user. For more information, see "Preparing the Installation Manager and the Gateway" in the *ScaleIO Deployment Guide*.
SVM root user	Password is set in the plug-in	The account provides full administrator privileges to all configuration and monitoring activities via the vSphere plugin.
MDM admin	Admin	The MDM has only one default account (“admin”) with a default password (“admin”). The password must be reset at first login, using the command `scli --login --username admin --password admin scli --set_password --old_password admin --new_password <NEW_PASSWORD>`. For more information, search for "Creating the MDM cluster" in the *ScaleIO Deployment Guide*. This account is a Super User, and provides full administrator privileges to all configuration and monitoring activities via the CLI and the GUI.

Authentication configuration

This topic describes local password requirements.

Note

For LDAP users, the requirements are defined by the authenticating server according to the organization's user policy.

User authentication is initially configured during ScaleIO installation, and users can be added and removed later, using the ScaleIO CLI (and only by a privileged user). The MDM and LIA passwords must meet the following criteria:

- Include at least 3 of the following 4 groups: [a-z], [A-Z], [0-9], special characters (!@#$ ...)
- Contain between 6 and 31 characters
- No white spaces

Note

The ESXi 6 password policy has the following additional requirements:

- Passwords must contain characters from at least three character classes.
- Passwords containing characters from three character classes must be at least seven characters long.
- Passwords containing characters from all four character classes must be at least seven characters long.

An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used.

For more information, see the chapter "Security and User Management" in the *ScaleIO User Guide*.

Note

ESXi 6 security policy is disabled.

Non-disruptive SNMP upgrade issues

The SNMP trap sender's credentials are handled differently in ScaleIO v1.32 and v2.0. This needs to be taken into account during or after the upgrade process.

If a version 1.32 ScaleIO Gateway is configured as an SNMP trap sender, it is configured with SNMP MDM credentials. When upgrading to version 2.0, the SNMP MDM credentials will be uploaded to the lockbox, and will be erased from the old gatewayUser.properties configuration file. The update is performed using the SNMP MDM password as a phrase, which may be considered as not meeting the ultimate security guidelines (the same text is used for both the MDM password value and the phrase for Lockbox secrets). However, it is a value which should be confidential, and is known to the user.

To harden the password, one of the following procedures can be performed:

- After upgrading the ScaleIO Gateway, change the Lockbox phrase using SioGWTool

- During the ScaleIO Gateway upgrade, provide the LOCKBOXPHRASE env variable as part of the upgrade command.

Examples:

- *Windows:* `>> msiexec /i EMC-ScaleIO-gateway-2.0-4000.0-x64.msi /L*v GW_install.log LOCKBOXPHRASE=user_phrase`
- *Linux:* `>>LOCKBOXPHRASE=user_phrase rpm -Uvh EMC-ScaleIO-gateway-2.0-4000.0.x86_64.rpm`

User authorization

This topic describes the user authorization settings that control the rights or permissions that are granted to a user to access a resource managed by the product. Local users and LDAP users are supported by the system.

When users are added to the MDM, user role definitions must be assigned to them.

Note

Local authentication can be disabled on the Installation Manager/ScaleIO Gateway. For more information, see the chapter "Security and User Management," in the *ScaleIO User Guide*.

Table 2 Local and LDAP User roles and permissions

User role	Query		Configure parameters		Configure user credentials	
	Local	LDAP	Local	LDAP	Local	LDAP
Monitor	Yes	Yes	No	No	No	
Configurator	Yes	Not Applicable	Yes (an aggregation of both Frontend and Backed Configurator)	Not applicable	No	Not applicable
Backend Configurator	Yes	No	Yes Backend operations only (Protection Domains, Storage Pools, Fault Sets, SDSs, Devices, other system settings)		No	No
Frontend Configurator	Yes	No	Yes Frontend operations only (Volumes, SDCs, Snapshots)		No	No
Administrator	Yes	No	Yes	No	May configure Configurator and Monitor users	
Security Roles	No	No	No	No	May define Administrator users and control LDAP	
Super User (only one Super User is allowed per system, and it must be a local user)	Yes	Not applicable	Yes	Not applicable	Yes	Not applicable

For more information, see the chapter "Security and User Management," in the *ScaleIO User Guide*.

Login banner

A login banner can be configured for both GUI and CLI users.

A login banner is a text file that is displayed upon login to the system. It can be used to communicate messages or to obtain user consent to real-time monitoring of information and retrieval of stored files. When the login banner is set up, it appears during the system login process before the login credential prompts. The login banner displays differently in the GUI and in the CLI interfaces:

- GUI—When logging in, the login banner is displayed, and must be approved.
- CLI—When logging in, the user is prompted to press any key, after which the banner is displayed. To continue, the banner must be approved.

If a login banner is not required, the feature can be disabled. For more information about configuring these banners, refer to your system's *User Guide*.

Component access control

This section describes component access control. Component access control settings define control over access to the product by external and internal systems or components.

Component authentication

The system provides secure connectivity between internal and external components.

Secure connectivity with internal system components

The SSL authentication feature allows secure authentication of ScaleIO SDS components using a Public and Private Key (Key-Pair) associated with a certificate. The feature works as follows:

- When an SDS is added to the ScaleIO system (for example, using the `--add_sds command`), it generates its own CSR.
- The MDM acts as the Certificate Authority, and signs the certificates, using its credentials.
- Every time that a component reconnects to the system, authentication occurs. If the challenge fails, that component will not be able to connect to the ScaleIO system.
- If necessary, or if a malfunction occurs, this feature provides a secure protected manner in which to disable secure authentication.

Secure connectivity with external components

This feature allows external components to authenticate the MDM with a certificate and authenticate back to the MDM with a user name and password. After authentication, communication between the MDM and external components is performed using TLS (Transport Layer Security) protocols. Secure communication with the MDM is authenticated by the following components:

- CLI client
- ScaleIO Gateway
- GUI client

- IM client
- vSphere plug-in

Once added in the trust point, all communications will require authentication, followed by communications over TLS. The same method is employed between the IM and all LIAs.

On the ScaleIO Gateway, setting the *security.bypass_certificate_check* property in the gateway properties file to **`true`** will result in the gateway blindly trusting the certificates of the hosts to which it is trying to connect. Typically, the gateway connects to the MDM or to LIA. This setting affects REST and IM connections, because they are all included in the gateway. The default setting of this property is **`false`**.

Any actions relating to the acceptance of certificates will still add the certificates to the trust store file (`truststore.jks`) for future use, when this property is set to **`false`**. Such actions are:

- MDM certificate and LIA certificate approval during installation with the IM
- The REST request `trustHostCertificate`

Note

IM/Gateway access to the LIA may be restricted to predefined IP addresses, by configuring the list of trusted IP addresses in the file: Windows: `C:\Program Files\emc\scaleio\LIA\cfg\conf.txt`; Linux: `/opt/emc/scaleio/lia/cfg/conf.txt`

SSH

A manually generated public-private key pair can be used to perform SSH key authentication, instead of passwords, between the ScaleIO Gateway and ScaleIO system servers.

Note

Whenever Apache Tomcat is shut down normally and restarted, or when an application reload is triggered, the standard Manager implementation will attempt to serialize all currently active sessions to a disk file located via the pathname (by default SESSIONS.SER) attribute. All such saved sessions will then be deserialized and activated (assuming they have not expired in the mean time) when the application reload is completed. To remove saved sessions after a ScaleIO Gateway restart, delete the following file: `/opt/emc/scaleio/gateway/work/Catalina/localhost/_/SESSIONS.ser`

Component authorization

This topic describes the configurable LIA parameters for component authorization.

All the configurable parameters of LIA are included in the file `/opt/emc/scaleio/lia/cfg/conf.txt`. The list includes:

lia_token, *lia_enable_install*, *lia_enable_uninstall*, *lia_enable_configure*, and *lia_enable_fetch_logs*.

CHAPTER 3

Log Settings

This section describes the logs collected by ScaleIO. A log is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results. Topics include:

- Log description 20
- Log management and retrieval 22

Log description

This topic describes the logs collected by the system.

Note

ScaleIO uses Apache Tomcat, which has its own set of standard logs. For more information about Tomcat logs, refer to Apache Tomcat documentation.

Table 3 Log files

Component	Location
MDM log The logs do not contain any user data (as the user data do not pass through the MDM) The logs may contain the MDM's user names (but never passwords), IP addresses, MDM configuration commands, events etc.	Linux: `/opt/emc/scaleio/mdm/logs` Windows: `c:\Program Files\emc\scaleio\mdm\logs`
REST logs	<gateway installed folder>\logs For example: Windows—`c:\Program Files\emc\scaleio\gateway\logs` Linux—`/opt/emc/scaleio/gateway/logs` The following logs are available: • `scaleio.log` • `scaleio-trace.log` • `operations.log` • `localhost_access_log.log` • `audit.log` • `api_operations.log`

Installation Manager logs	<gateway installed folder>\logs
	For example:
	• Windows:
	  ▪ `c:\Program Files\emc\scaleio\gateway\logs`
	• Linux:
	  ▪ `/opt/emc/scaleio/gateway/logs`
	The following logs are available:
	• `scaleio.log`
	• `scaleio-trace.log`
	• `operations.log`

Table 3 Log files (continued)

Component	Location
	• `localhost_access_log.log`
LIA logs	Windows: • `C:\Program Files\emc\scaleio\lia\logs` Linux: • `/opt/emc/scaleio/lia/logs`
Tomcat logs	Windows: • `C:\Program Files\EMC\ScaleIO\Gateway\logs\tomcat.log` Linux: • `/opt/emc/scaleio/gateway/logs`
GUI logs	Windows: • `%AppData%\EMC\ScaleIO\logs` Linux: • `%AppData%\EMC\ScaleIO\logs`
vSphere web plug-in	
Plug-in: Deployment log:	Windows: • `c:\Windows\System32\config\systemprofile\AppDdata\Roaming\VMware\scaleio\deployment.log` Linux: • `/opt/.vmware/scaleio/deployment.log`
Plug-in: Rollback Log:	Windows: • `c:\Windows\System32\config\systemprofile\AppData\Roaming\VMware\scaleio\rollback.log` Linux: • `/opt/.vmware/scaleio/rollback.log`
Plug-in: Network Creation Log:	Windows: • `c:\Windows\System32\config\systemprofile\AppData\Roaming\VMware\scaleio\networkCreation.log` Linux: • `/opt/.vmware/scaleio/networkCreation.log`
vSphere Virgo Log:	Windows:

Table 3 Log files (continued)

Component	Location
	• `c:\ProgramData\Vmware\vSphere Web Client \serviceability \logsvsphere_client_virgo.log` Linux: • `/storage/log/vmware/vsphere-client/logs/ vsphere_client_virgo.log`

Log management and retrieval

This topic describes the ways in which logs can be managed and retrieved.

- Log roll-over (REST):
  - In the configuration of the log's behavior (`logback.xml`—see below), each log is defined to be no greater than 10 MB. Once it reaches this size, a new log file is created. Once the maximum (10) is reached, the oldest log is overwritten (roll-over). The log files are: `name_xxx.log, name_xxx.1.log.zip, … name_xxx.10.log.zip`.
- Configuration of an external Syslog server:
  - During ScaleIO installation, you can use the Installation Manager web client to configure Syslog event reporting. You can also configure these features after installation, using the CLI. For more information, see the appendix "System Events and Alerts" in the *ScaleIO User Guide* for CLI commands, and the topic "Installing with the web client" in the *ScaleIO Installation Guide*.
- Configuration of logging levels:
  - GUI—Logging levels can be modified. For more information, see the topic "Customizing System Preferences" in the chapter "Using the Graphical User Interface", in the *ScaleIO User Guide*.
  - REST Gateway—The log can be configured by editing the file: `<gateway installation folder>\webapps\ROOT\WEB-INF\classes \logback.xml`
  - Installation Manager—The log can be configured by editing the file: `<gateway installation folder>\webapps\ROOT\WEB-INF\classes \logback.xml`
- vSphere Web Client logging
  - To enable debug logging for the vSphere Web Client service:

    Note

    Take a backup of the `serviceability.xml` file before modifying it.

    1. Stop the vSphere Web Client service.
    2. Navigate to the configuration folder:
       - For vCenter Server 5.5—`C:\Program Files\VMware \Infrastructure\vSphereWebClient\Server\configuration`

- For vCenter Server 5.1—`C:\Program Files\VMware\Infrastructure\vSphereWebClient\Server\config`
- For vCenter Server 5.0—`C:\Program Files\VMware\Infrastructure\vSphere Web Client\DMServer\config`
- For vCenter Server Virtual Appliance 5.0—`/usr/lib/vmware-vsphere-client/server/configuration`
- For vCenter Server Virtual Appliance 5.1—`/usr/lib/vmware-vsphere-client/server/config`
- For vCenter Server Virtual Appliance 5.5—`/usr/lib/vmware-vsphere-client/server/configuration`

3. Open the `serviceability.xml` file using a text editor.

Note

Take a backup of the `serviceability.xml` file before modifying it.

4. Edit the root level logging parameter by replacing the default INFO with DEBUG. For example, change the `serviceability.xml` default configuration from:

```
<root level="INFO">
<appender-ref ref="SIFTED_LOG_FILE"></appender-ref>
<appender-ref ref="LOG_FILE"></appender-ref>
</root>
```

to:

```
<root level="DEBUG">
<appender-ref ref="SIFTED_LOG_FILE"></appender-ref>
<appender-ref ref="LOG_FILE"></appender-ref>
</root>
```

5. To add a logging section for ScaleIO plugin, create a section to increase logging to Debug levels:

```
<logger level="DEBUG" additivity="false" name="com.emc">
<appender-ref ref="SIFTED_LOG_FILE" />
<appender-ref ref="Log_FILE" />
</logger>
```

6. Save and close the file.
7. Start the vSphere Web Client service. Additional logs will be written to the `C:\ProgramData\VMware\vSphere Web Client\Logs` folder

- ESRS feature (EMC Secure Remote Support)—ESRS support enables secure, high-speed, 24x7, remote connection between EMC and customer installations, including:
  - Remote monitoring
  - Remote diagnosis and repair
  - Daily sending of logs, alerts, and ScaleIO topology configured after system deployment. For more information, see "Configuring ESRS connection properties" in the *ScaleIO Deployment Guide*.

- Viewing events locally—Use the `showevents.py` command, using filter switches to control the severity of alerts. For more information, see the appendix "System Events and Alerts" in the *ScaleIO User Guide*.
- Configuration for external log management tools like envision—NA
- Configuration of time synchronization with an external source (e.g. via NTP, Windows Time Service, etc.)—NA
- Get Info—Get Info allows you to assemble a ZIP file of system logs for troubleshooting. You can run this function from a local node for its own logs, or by using the Installation Manager to assemble logs from all MDM and SDS nodes in the system. For more information, see "Performing the Get Info operation" in the *ScaleIO Deployment Guide*.

CHAPTER 4

Communication Security Settings

This section describes the ScaleIO system's security settings. Communication security settings enable the establishment of secure communication channels between the product components, as well as between product components and external systems or components. Topics include:

- Port usage 26
- Network encryption 27

Port usage

This topic describes the port usage in ScaleIO.

The following table describes the ports used:

Table 4 Port usage

Component	Service	Protocol	Port	Description
Installation Manager	Installation Manager	REST over HTTPS	443 (default)	Used to perform installations using the Installation Manager. This port on the ScaleIO Gateway web server can be changed to a non-standard port by modifying the file `{gateway installation directory} /conf/catalina.properties`. Change the two instances of *port="443"* to another valid and non-occupied port of your choice and restart the ScaleIO Gateway service/daemon.
REST	scaleio-gateway	REST over HTTPS	443 (secure, default) 80 (non-secured http port, default)	To be used by clients wishing to query a ScaleIO cluster or perform operations on it.
MDM	MDM	Protobuf over TCP	6611, 9011 (defaults)	Used to provision a ScaleIO system, or to query it
SDS	SDS	Proprietary protocol over TCP	7072 (default)	SDCs connect through this port for data communication and the MDM for meta-data communication. For cases where multiple SDSs are installed on the same physical server, use ports 7072+x, where x is the index of the SDS.
LIA	LIA	Protobuf over TCP	9099 (default)	IM connects to the LIA to perform installation related operations
SNMP	SNMP	SNMP v2 over UDP	162 (default)	SNMP traps for system alerts are sent to a trap receiver via this port. The ScaleIO gateway sends messages to: snmp.traps_receiver_ip on the port snmp.port
SDBG for MDM (Manager)			25620	These ports are used by ScaleIO internal debugging tools to extract live information from the system for debugging purposes.

Table 4 Port usage (continued)

Component	Service	Protocol	Port	Description
SDBG for MDM (Tie-Breaker)			25600	
SDBG for SDS			25640	
SDBG for Multi-SDS			2564x	These ports are used by ScaleIO internal debugging tools to extract live information from the system for debugging purposes. For cases where multiple SDSs are installed on the same physical server, use ports 2564+x, where x is the index of the SDS.

Network encryption

This topic explains how network encryption is performed by the system.

The IM client, CLI client, GUI client, vSphere plug-in, and ScaleIO (REST) Gateway use TLSv1—after authentication, communication between the MDM and external components is performed using TLSv1 (Transport Layer Security) protocols. External components include: IM client, CLI client, GUI client, vSphere plug-in, and ScaleIO Gateway. The same method is used between the IM client and LIAs. For more information, see the chapter "Security and User Management" in the *ScaleIO User Guide*.

REST Gateway certificate validation—the OpenStack ScaleIO driver communicates with the ScaleIO REST Gateway through https, (over TLSv1). By default, the driver ignores verification of the REST Gateway's TLSv1 certificate, but it can verify the certificate if the following configuration parameters are defined:

- `verify_server_certificate`—set to *True*, if the server's certificate must be verified, and to *False* if no verification is required.
- `server_certificate_path`—If the parameter *verify_server_certificate* is set to *True*, specify the location of the `.pem` file containing the server's certificate.

For instructions for generating a self-signed certificate using Keytool, see the section "Generating a self-signed certificate using the keytool utility" in the *ScaleIO Installation Guide*.

The following encryption methods are approved for use with your system:

- MDM-External components:
  - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
  - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
  - ECDH-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AESGCM(256) Mac=AEAD
  - ECDH-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AESGCM(256) Mac=AEAD

  - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
  - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
  - ECDH-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AESGCM(128) Mac=AEAD
  - ECDH-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AESGCM(128) Mac=AEAD
  - DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
  - DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
  - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
  - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
  - ECDH-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AES(256) Mac=SHA384
  - ECDH-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AES(256) Mac=SHA384
  - DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
  - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
  - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
  - ECDH-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AES(128) Mac=SHA256
  - ECDH-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=AES(128) Mac=SHA256
  - DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
  - AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
  - AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
  - AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
  - AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
- Gateway components other than MDM (IM, REST):
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
  - TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256

Note

In order to use CURL on RHEL6 with ScaleIO Gateway v2.0.0.3 and higher, upgrade the NSS package to 3.21.0. (use the YUM update command).

CHAPTER 5

Data Security Settings

This section describes the data security settings used to define the controls that prevent permanently stored data from being disclosed in an unauthorized manner. Topics include:

- Data integrity 32

Data integrity

This section describes the integrity of data.

Data erasure is implemented using the hardware's data erasure tools.

CHAPTER 6

Known Issues

This chapter describes known security issues and workarounds. Topics include:

- Known Issues 34

Known Issues

This topic contains known security issues and workarounds.

Issue:

EMC ScaleIO versions prior to 2.0.1.1 may be vulnerable to the following vulnerabilities:

- Privilege escalation vulnerability
  A low-privileged local attacker may be able to modify the kernel memory in the SCINI driver, and may achieve code execution to escalate privileges to root on ScaleIO Data Client (SDC) servers.
- Denial-of-service vulnerability via IOCTL calls
  A low-privileged local attacker may cause a denial-of-service by generating a kernel panic in the SCINI driver using IOCTL calls, which may render the ScaleIO Data Client (SDC) server unavailable until the next restart.
- Denial-of-service through configuration API
  Incorrect permissions on the SCINI driver may allow a low-privileged local attacker to modify the configuration and render the ScaleIO Data Client (SDC) server unavailable.

Resolution:

ScaleIO version 2.0.1.1 contains resolutions to these vulnerabilities. Therefore, EMC recommends a system upgrade at the earliest possible opportunity. For those who are unable to upgrade, EMC recommends changing the access permission to 600. On each SDC, execute the SHELL command:

```
chmod 600 /dev/scini
```

Note

- This command should be executed "as-is" (Do not add anything else to the command).
- This command should be executed after every reload of the SDC, or after every restart.
- Once EMC ScaleIO is upgraded to version 2.0.1.1, there is no need to use this workaround.

Issue:

After upgrading the Operating System, the System Stable Values (SSVs) that Lockbox uses to fingerprint the system it is part of might change. In other words, the Lockbox may not be present or may lose content after the OS upgrade.

Resolution:

To update or reconfigure the Lockbox:

1. Open Lockbox with the password that was used to create it.
2. Reconfigure the Lockbox.

Note

If the Lockbox is not present, re-create the Lockbox using the command:

```
/opt/emc/scaleio/gateway/bin/SioGWTool.sh --set_ldap_properties --
server_url ldap://<LDAP SERVER IP> --base_dn "<BASE_DN>" --group_name
"<GROUP NAME>" --create_default_lockbox
```

LDAPS users must use: `ldaps:// <LDAP SERVER IP>`

instead of `ldap://` in the example above.