

# Site Recovery Manager Security

Site Recovery Manager 6.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-001875-01

**vmware**<sup>®</sup>

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2008–2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Contents

|  |          |
|--|----------|
| About VMware Site Recovery Manager Security              | 5        |
| Updated Information                                      | 7        |
| <b>1 Site Recovery Manager Security Reference</b>        | <b>9</b> |
| Site Recovery Manager Services                           | 10       |
| Site Recovery Manager Network Ports                      | 10       |
| Site Recovery Manager Configuration Files                | 11       |
| Site Recovery Manager Certificates and Keys              | 11       |
| Site Recovery Manager License and EULA Files             | 12       |
| Site Recovery Manager Log Files                          | 12       |
| Site Recovery Manager Accounts                           | 13       |
| Site Recovery Manager Security Updates and Patches       | 14       |
| Best Practices For Securing Site Recovery Manager Server | 14       |
| Index  | 15       |



# About VMware Site Recovery Manager Security

---

*Site Recovery Manager Security* provides a concise reference to the security features of Site Recovery Manager.

To help you protect your Site Recovery Manager installation, this guide describes security features built into Site Recovery Manager and the measures that you can take to safeguard it from attack.

- External interfaces, ports, and services that are necessary for the proper operation of Site Recovery Manager
- Configuration options and settings that have security implications
- Location of log files and their purpose
- Required system accounts
- Information on obtaining the latest security patches

## Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of Site Recovery Manager.



# Updated Information

---

*Site Recovery Manager Security* is updated with each release of the product or when necessary.

This table provides the update history of *Site Recovery Manager Security*.

| <b>Revision</b> | <b>Description</b>  |
|-----------------|---|
| EN-001875-01    | Replaced "federated" with "Enhanced Linked Mode" in " <a href="#">Site Recovery Manager Accounts</a> ," on page 13. |
| EN-001875-00    | Initial release.  |



# Site Recovery Manager Security Reference

---

# 1

Use the Security Reference to learn about the security features of your Site Recovery Manager installation and the measures that you can take to safeguard your environment from attack.

- [Site Recovery Manager Services](#) on page 10  
The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.
- [Site Recovery Manager Network Ports](#) on page 10  
Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.
- [Site Recovery Manager Configuration Files](#) on page 11  
Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.
- [Site Recovery Manager Certificates and Keys](#) on page 11  
Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.
- [Site Recovery Manager License and EULA Files](#) on page 12  
The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.
- [Site Recovery Manager Log Files](#) on page 12  
Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.
- [Site Recovery Manager Accounts](#) on page 13  
Site Recovery Manager uses Single Sign-On (SSO) certificates to access the Site Recovery Manager Server.
- [Site Recovery Manager Security Updates and Patches](#) on page 14  
You can apply Site Recovery Manager security updates and patches as they are made available by VMware. You can apply security updates and patches of the host operating system as they are made available by the vendors of the host operating system.
- [Best Practices For Securing Site Recovery Manager Server](#) on page 14  
Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

## Site Recovery Manager Services

The operation of Site Recovery Manager depends on several services that run on the Site Recovery Manager Server host machine.

**Table 1-1.** Services that Site Recovery Manager Requires

| Service Name   | Startup Time                                   | Description  |
|--|--|--|
| VMware vCenter<br>Site Recovery Manager Server               | Automatic                                      | Provides the core Site Recovery Manager functions.                           |
| VMware vCenter<br>Site Recovery Manager<br>Embedded Database | Automatic, if you use the<br>embedded database | The vPostgres server for the<br>Site Recovery Manager embedded database.     |
| Server   | Automatic                                      | Windows service that supports file sharing over<br>the network.              |
| Workstation  | Automatic                                      | Windows service that creates and maintains<br>connections to remote servers. |
| Protected Storage  | Automatic                                      | Windows services that store sensitive data.                                  |

## Site Recovery Manager Network Ports

Site Recovery Manager uses network ports, which you can configure, to communicate with clients and other servers. You must ensure that firewalls do not block the ports that Site Recovery Manager uses.

Site Recovery Manager Server receives all incoming traffic on one network port. The default port is 9086. If you configure Site Recovery Manager to use an embedded database, the Site Recovery Manager embedded database receives the localhost network traffic on the local loopback interface. The default port is 5678.

You can select other ports for Site Recovery Manager and embedded database traffic during the installation process if the default ports are blocked or other applications use them. You must configure network policies to enable traffic on the incoming port. For information about the ports that you can change after installation, see the *Modify a Site Recovery Manager Server Installation* topic in the *Site Recovery Manager Installation and Configuration* documentation.

Site Recovery Manager Server communicates with Platform Services Controller, vCenter Server, ESXi hosts, and Arrays at the local site. You must verify that the network firewall policies enable the traffic to network ports of all components at the local site. For the list of the default ports that all VMware products use, see <http://kb.vmware.com/kb/1012382>.

The connection between the local and the remote site of a Site Recovery Manager pair must be private such as VPN. The local Site Recovery Manager Server communicates with Site Recovery Manager Server, Platform Services Controller, and vCenter Server on the remote site, and your network provider must ensure the appropriate network policies to enable the traffic.

For a list of all the ports that must be open for Site Recovery Manager, see <http://kb.vmware.com/kb/2119329>.

## Site Recovery Manager Configuration Files

Some Site Recovery Manager configuration files contain settings that might affect the security of your environment. Improper settings can also impact the proper functioning of your Site Recovery Manager environment.

**Table 1-2.** Site Recovery Manager Configuration Files

| File or Directory Location  | Description  |
|---|--|
| <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml                  | <p>Defines system configuration of Site Recovery Manager Server.</p> <p><b>NOTE</b> Do not move, or delete the configuration file. You can safely change the system settings of a Site Recovery Manager instance by using the <b>Advanced Settings</b> tab on the <b>Manage</b> page in the vSphere Web Client user interface.</p> |
| <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager Embedded Database\bin\vmw_vpg_config\ | <p>Contains embedded database configuration files.</p> <p><b>NOTE</b> Do not modify, move, or delete the configuration file.</p>   |
| <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager\config\extension.xml                  | <p>Defines configuration of Site Recovery Manager Server Extension. The <i>extension.xml</i> file contains definitions of default user roles and their privileges.</p> <p><b>NOTE</b> Do not modify, move, or delete the configuration file.</p>   |

## Site Recovery Manager Certificates and Keys

Site Recovery Manager uses TLS certificates and private keys to protect network communication and securely establish authentication with other servers.

| CA certificate or private key or both   | Location and Description  |
|---|---|
| TLS certificate and key for Site Recovery Manager Server endpoint                           | <p>Windows Certificate Store and in the <i>installation_folder</i>\VMware\VMware vCenter Site Recovery Manager\bin\SRM_Server_IP_addressca.p12 file.</p> <p>Site Recovery Manager generates the certificate if you do not provide a custom certificate during the installation.</p> |
| TLS certificate and key for solution user created during Site Recovery Manager installation | <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager\bin\SRM_Server_IP_addresssu.p12 file.   |

| CA certificate or private key or both                               | Location and Description   |
|---|--|
| TLS certificate and key for solution user on the remote site        | <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager\bin\extension-s.p12 file or \VMware\VMware vCenter Site Recovery Manager\bin\extension-p.p12 file.<br>Site Recovery Manager creates the files during the pairing process.  |
| CA certificate for Site Recovery Manager Server and TLS certificate | <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager\bin\SRM_Server_IP_addressca.p7b file.<br>Site Recovery Manager generates the certificate if you do not provide a custom certificate during the installation.<br>You can import the certificate into a client trust keystore to allow users to implicitly trust the Site Recovery Manager Server certificate. |

**IMPORTANT** Configure access control lists to restrict the access to the .p12 files as appropriate for your environment.

**NOTE** Do not modify, delete, or move the .p12 files.

**NOTE** Do not extract or share private key information to protect your Site Recovery Manager instance.

For more information about the Site Recovery Manager authentication mechanisms, see the *Site Recovery Manager Authentication* topic in the *Site Recovery Manager Installation and Configuration Guide*.

## Site Recovery Manager License and EULA Files

The Site Recovery Manager license and EULA files are located on the Site Recovery Manager Server host machine.

**Table 1-3.** Site Recovery Manager License and EULA Files

| File or Directory   | Description  |
|---|--|
| <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager\en\   | Directory containing the Site Recovery Manager End-user license agreement files. |
| <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager\en\open_source_license.txt                      | Site Recovery Manager Open Source License file.                                  |
| <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager\en\open_source_license_vix.txt                  | Virtual Infrastructure Extension API Open Source License file.                   |
| <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager Embedded Database\share\EULA-en.doc             | Site Recovery Manager Embedded Database End-user license agreement file.         |
| <i>installation_folder</i> \VMware\VMware vCenter Site Recovery Manager Embedded Database\share\open_source_license.txt | Site Recovery Manager Embedded Database Open Source License file.                |

## Site Recovery Manager Log Files

Site Recovery Manager records operational information into the log files. The logs files do not contain sensitive information such as private keys and passwords.

Site Recovery Manager stores the system log files in the C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs directory. The latest messages from Site Recovery Manager Server are placed in the *vmware-dr-number.log* file.

If you restart Site Recovery Manager Server or the current file must exceed the set file size limit, Site Recovery Manager archives the current log file and creates a new log file.

To change the log file directory, enter a custom directory name in the directory XML element in the *installation\_directory\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml* configuration file. You can also change the log level of each component by updating the logLevel XML element in the *vmware-dr.xml* file. The default level of all components is verbose.

---

**IMPORTANT** Configure access control lists to restrict the access to the log files.

---

**Table 1-4.** Log Levels

| Level   | Description   |
|---------|---|
| error   | Displays only error log entries                                       |
| info    | Displays information, error, and warning log entries                  |
| trivia  | Displays information, error, warning, verbose, and trivia log entries |
| verbose | Displays information, error, warning, and verbose log entries         |
| warning | Displays warning and error log entries                                |

Site Recovery Manager supports the following components.

- App
- Replication
- Recovery
- Storage
- StorageProvider
- Vdb
- Persistence
- SoapAdapter

The *vmware-dr-number.log* file contains security messages concerning the authentication process and connections with the remote side.

## Site Recovery Manager Accounts

Site Recovery Manager uses Single Sign-On (SSO) certificates to access the Site Recovery Manager Server.

### User Accounts

The privileges of the vCenter Server administrator grant administration access to Site Recovery Manager in the default configuration. You must use the administrator credentials when you try to log in to Site Recovery Manager for the first time after the installation.

If you have administrator credentials, you can grant access to Site Recovery Manager to other users by using the vSphere Web Client.

For more information about Site Recovery Manager roles, privileges, and permissions, see the *Site Recovery Manager Privileges, Roles, and Permissions* in the *Site Recovery Manager Administration* documentation.

### Solution User Account

Site Recovery Manager creates a `solution` user during the installation and uses it during the authentication with vCenter Server. The `solution` user is unique for each Site Recovery Manager instance and is for internal use by Site Recovery Manager, vCenter Server, and Platform Services Controller.

Site Recovery Manager creates an additional `solution` user on each remote site during the pairing process of sites that do not use Enhanced Linked Mode. Site Recovery Manager uses the `solution` user to perform necessary operations on the remote site.

---

**NOTE** You must not delete and modify the roles and privileges associated with the `solution` user accounts.

---

For more information about the `solution` users and authentication between the local and remote site, see the *Site Recovery Manager Authentication* topic in the *Site Recovery Manager Installation and Configuration* documentation.

## Site Recovery Manager Security Updates and Patches

You can apply Site Recovery Manager security updates and patches as they are made available by VMware. You can apply security updates and patches of the host operating system as they are made available by the vendors of the host operating system.

### Site Recovery Manager Host Operating System Versions

For information about the supported host operating systems for Site Recovery Manager Server, see the *Compatibility Matrixes for Site Recovery Manager 6.1* at <https://www.vmware.com/support/srm/srm-compat-matrix-6-1.html>.

### Applying Site Recovery Manager Patches and Security Updates

You apply Site Recovery Manager security patches and updates by performing an in-place upgrade of your existing Site Recovery Manager installation. For information about upgrading Site Recovery Manager, see [In-Place Upgrade of Site Recovery Manager Server](#) in *Site Recovery Manager Installation and Configuration*.

## Best Practices For Securing Site Recovery Manager Server

Best practices for securing Site Recovery Manager Server can protect your environment from possible security problems.

The secure operation of Site Recovery Manager depends on the proper configuration and maintenance of the Site Recovery Manager Server operating system.

- Run Site Recovery Manager only on a supported host operating system, database, and hardware. If Site Recovery Manager is not running on a supported host operating system, Site Recovery Manager might not run properly.
- Apply the latest operating system updates and patches to protect the host operating system from malicious attacks. Apply the latest Site Recovery Manager updates and patches to address any known issues with Site Recovery Manager.
- Ensure the integrity of your Site Recovery Manager deployment when you run Site Recovery Manager as a VM. See the *Virtual Machine Security Best Practices* topic in the *vSphere Security* documentation.
- Limit installation of software and disable services that Site Recovery Manager does not use, to free resources and to decrease the possibilities for server attacks. Unneeded software and services consume CPU, storage, memory, and bandwidth resources and increase the chance of server attacks.
- Allow only administrators to access the server. To limit the number of accounts that an attacker can use, limit the number of accounts that can access the server.
- Check the network ports that Site Recovery Manager uses and configure a firewall to protect your server.
- Separate the Site Recovery Manager management network traffic from workload traffic to protect management servers from attacks.

# Index

## A

accounts 13

## B

best practices 14

## C

certificate, location 11

configuration files, locations 11

## D

default ports 10

## E

EULA 12

## I

intended audience 5

## L

license 12

log files 12

## N

network ports 10

## S

securing SRM 14

security

    certificate 11

    configuration files 11

    keystore 11

    reference 9

    updates and patches 14

services 10

Site Recovery Manager, security reference 5

SRM services 10

system log 12

## U

updated information 7

users 13

