

Secure Remote Services

Release 3.38

Operations Guide

REV 01

Copyright © 2019 Dell EMC Corporation. All rights reserved. Published in the USA.

Published August 2019

Dell EMC 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 EMC Corporation 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 EMC software described in this publication requires an applicable software license.

Dell EMC, EMC², and the Dell and EMC logos are registered trademarks or trademarks of Dell EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to Dell EMC Online Support (<https://support.emc.com>).

CONTENTS

Preface	
Chapter 1	Introduction
	Overview..... 10
	Customer site components..... 10
	Communication to Dell EMC 12
	Digital Certificate Management 15
	Device access control..... 16
	Device configuration access control 16
	Dell EMC enterprise access control..... 16
	Responsibilities for SRS components 16
Chapter 2	SRS Web UI Configuration
	Accessing SRS Version 3 via Web UI 20
	Using the Dashboard 23
	Devices - Manage Devices 29
	Configuration 37
	Audit..... 57
	Logs..... 60
	Logging out..... 62
	Changing the password using the Web UI..... 63
	Exporting to CSV Managed Devices 67
Chapter 3	Server Maintenance
	Service preparation for SRSv3 70
	Backup guidelines and procedures 71
Chapter 4	Virtual Lifecycle Management - Updating
	Overview..... 74
	Update checks 74
	Downloading and applying updates 75
	Upgrading Docker 77
Chapter 5	Troubleshooting
	Resetting the Web UI administrator user password 80
	Service commands and debugging..... 82
	Provisioning Logs 84
	Unzipping files using WinZip 85
Appendix A	SRS Migration Process
	SRS Migration Tool version 3.xx..... 88
	Precondition prior to migration process initiation 89
	Assumptions..... 90
	Procedure for migrating devices from source to target gateway 91
	SRS Export Import Migration Tool (Version 3.xx) for Windows 94

	Backend migration process	113
Appendix B	Network Configuration Using YaST	
	Procedure	122
Appendix C	IP Addresses used by SRS	
	Key information.....	130
	Article access.....	130
Appendix D	Dell EMC Customer Environment Check Tool for SRS v3.x	
	Customer Environment Check Tool overview	132
	Required CECT test resolution	132
	Installation	134
	Operation	134
Appendix E	SRS Version 3 CLI Utility	
	Overview.....	164
	Installing SRSv3 CLI utility.....	164
	Using SRSv3 CLI utility	164

PREFACE

As part of an effort to improve its product lines, Dell 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 Dell EMC technical support professional if a product does not function properly or does not function as described in this document.

Note: EMC Secure Remote Services (ESRS) has been rebranded to Secure Remote Services (SRS).

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

Purpose

This guide is part of the Secure Remote Services (SRS) Release 3.38 documentation set, and is intended for use by customers and prospective customers.

Readers of this guide are expected to be familiar with the following topics:

- ◆ Local network administration
- ◆ Internet protocols
- ◆ Dell EMC storage system characteristics and administration

Related documentation

The following Dell EMC publications provide additional information:

- ◆ *Secure Remote Services Release Notes*
- ◆ *Secure Remote Services Technical Description*
- ◆ *Secure Remote Services Pre-Site Checklist*
- ◆ *Secure Remote Services Site Planning Guide*
- ◆ *Secure Remote Services Port Requirements*
- ◆ *Secure Remote Services Installation Guide*
- ◆ *Secure Remote Services Operations Guide*
- ◆ *Secure Remote Services Policy Manager Operations Guide*
- ◆ *SRS Policy Manager 6.8 Installation Guide - Standard Windows*
- ◆ *SRS Policy Manager 6.8 Installation Guide - Integrated AD (Windows)*

Documentation conventions

Dell EMC uses the following conventions for special notices:



DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.



WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.



CAUTION, used with the safety alert symbol, indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.



NOTICE is used to address practices not related to personal injury.

Note: A note presents information that is important, but not hazard-related.

Typographical conventions

Dell EMC uses the following type style conventions in this document:

Bold	Use 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)
<i>Italic</i>	Use for full titles of publications referenced in text and for variables in body text.
Monospace	Use for: <ul style="list-style-type: none"> • System output, such as an error message or script • System code • Pathnames, file names, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Use for variables.
Monospace bold	Use 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

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

Product information — For documentation, release notes, software updates, or information about Dell EMC products, go to Dell EMC Online Support at:

<https://support.emc.com>

Technical support — Go to Dell EMC Online Support and click Service Center. You will see several options for contacting Dell EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your Dell 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

You should become familiar with the Secure Remote Services Site Planning Guide. It is important to understand the system requirements and configurations before you execute any administrative tasks.

This chapter introduces the Secure Remote Services v3.38 (SRS v3.38) that is the virtual edition of SRS. Topics include:

- ◆ Overview 10
- ◆ Customer site components 10
- ◆ Communication to Dell EMC 12
- ◆ Digital Certificate Management 15
- ◆ Device access control 16
- ◆ Responsibilities for SRS components 16

Overview

Secure Remote Services, also known as SRS, is a two-way remote connection between Dell EMC Customer Service and your Dell EMC products that enables remote monitoring, diagnosis, and repair. SRS assures availability and optimization of your Dell EMC infrastructure, and is a key component of Dell EMC's industry leading Customer Service. The connection is secure, high speed, and operates 24x7. Note that SRS v3.38 is the virtual edition of SRS.

SRS is included in all Enhanced and Premium warranties and maintenance agreements at no additional cost.

Dell EMC solution benefits

The following describes the solution benefits of SRS to Dell EMC:

- ◆ Eliminates dependency on product/OS
- ◆ Reduces time to market from 6-9 months to 2-4 months through faster availability of product on boards
- ◆ Represents a prebuilt software solution that is packaged, updated, and maintained as a unit
- ◆ Simplifies software development, distribution, deployment, and management
- ◆ Provides prebuilt and configured, off the shelf operating system, and preinstalled SRS software that allows setup and configuration of the software, with final configuration at the time of deployment

Customer site components

SRSv3 requires the following software/hardware options at the customer site:

- ◆ **SRS Virtual Edition(s)** — This SRS Virtual Edition OS and software component are installed on a customer-supplied Enterprise VMware or Hyper-V instance. It can be installed on multiple virtual instances either as a standalone instance or as SRS VE High Availability clusters. The servers act as the single point of entry and exit for all IP-based remote service activities and most Dell EMC Connect Home notifications.
- ◆ **SRS Docker Edition** — SRS can be installed on a Linux host using the Docker Engine. Before installing SRS on a Linux host, the following must already be installed:
 - Docker supported Linux distribution (x64 bit)
 - Docker Engine (Docker runtime)

Using the binary installer, SRS can be installed on the Linux distributions that support Docker. For a list of Linux distributions that are supported by Docker and for Docker installation instructions, refer to the following address:

<https://docs.docker.com/engine/installation>

Note: Cloud platform support for the SRS Docker Edition is best effort. Passive FTP is not supported with SRS DE

The following component is optional but highly recommended:

Policy Manager — This SRS software component is installed on a customer-supplied server or servers. It can be configured to control remote access to your devices and maintain an audit log of remote connections, file transfers Connect Homes by the SRS Clients, and access to and administration actions performed on the Policy Manager.

SRSv3 servers

SRS is the remote service solution application that is installed on one or more customer-supplied dedicated servers. SRS becomes the single point of entry and exit for all IP-based Dell EMC remote service activities for the devices associated with that particular SRS Virtual Edition or SRS Virtual Edition Cluster.

SRS functions as a communication broker between the managed devices, the Policy Manager, and the Dell EMC enterprise. SRS is an HTTPS handler. All messages are encoded using standard XML and SOAP application protocols. SRS message types include the following:

- ◆ Device state heartbeat polling
- ◆ Connect Homes
- ◆ Remote access session initiation
- ◆ User authentication requests
- ◆ Device management synchronization

Each SRS Virtual Edition acts as a proxy, carrying information to and from managed devices or to a Policy Manager. SRS Virtual Editions can also queue and forward Connect Home requests via FTPS and/or SMTP (if properly configured) in the event of a temporary SRS channel failure.

Each SRS Virtual Edition has its own web user interface, which runs as a Linux service on the underlying OpenSUSE operating system. All SRS Virtual Edition actions are logged to a local rolling runtime log file.

Policy Manager

The Policy Manager allows you to set permissions for devices that are being managed by SRS. SRS polls the Policy Manager every 2 minutes and receives the current policies, which are then cached locally in memory and to disk. Due to this polling time interval, policy updates may take up to 2 minutes before being applied.

During the periodic poll, SRS posts all audit requests and actions that have occurred to the Policy Manager. These events are written to the Policy Manager database and the local log files. These audits can also be streamed to a customer's syslog server. When a remote access request arrives at SRS for device access, the access is controlled by SRS enforcing the policy set by the Policy Manager.

SRS Virtual Edition is supported with any version of Policy Manager 2.02.1-xxx or Policy Manager 6.6 or later. A redundant Policy Manager is only supported on Policy Manager 2.02.1-xxx.

Note: Once installed on your server, the Policy Manager application is inaccessible by third parties, including Dell EMC. For more information about the operations and configuration of the Policy Manager, refer to the *Secure Remote Services Policy Manager Operations Guide*.

Proxy server

Network traffic can be configured to route from SRS through proxy servers to the Internet. SRS supports basic authentication for HTTP and SOCKS proxy servers, with or without credentials based on the proxy setup; however, the customer is responsible for all proxy server configuration.

Note: If user accounts are required, they should be service accounts that do not have expiring passwords.

IMPORTANT

To ensure communication integrity, proxy servers and devices external to your DMZ must not perform any method of SSL checking on outbound or inbound traffic for SRS. SSL checking will cause connectivity loss to Dell EMC. If SSL checking is performed on outbound communications by customer firewalls, proxies, web traffic filtering appliances or applications, web traffic shaping/load balancing, certificate verification or proxying, or Intrusion Detection Services (IDS), there will be loss connectivity to Dell EMC.

Note: When a customer configuration requires proxy communication between SRS and the Policy Manager or between SRS and Dell EMC Enterprise, and if SRS cannot connect to either through the proxy communication path, then it will attempt to connect multiple times. If the SRS successfully establishes a direct connection, then no error message appears to notify the customer or Dell EMC that there is a problem with the proxy communication path.

Communication to Dell EMC

All outbound communication between the customer's site and Dell EMC is initiated from the customer's site by the SRS server(s) over port 443 and 8443. Using industry standard Secure Sockets Layer (SSL) encryption over the Internet and a Dell EMC-signed digital certificate for authentication, the SRS creates a secure communication tunnel.

IMPORTANT

Port 8443 is not required for functionality. However, unless you open this port, you may experience a significant decrease in remote support performance, which will directly impact the time necessary to resolve issues on the end devices.

SRS uses industry-accepted bilateral authentication for the Dell EMC servers and SRS. Each SRS has a unique digital certificate that is verified by Dell EMC whenever an SRS makes a connection attempt. SRS then verifies the Dell EMC server certificate. Only when the mutual SSL authentication passes does SRS transmit messages to Dell EMC, securing the connection against spoofing and man-in-the-middle attacks.

SRS uses the SSL tunnel to Dell EMC to perform the following functions:

- ◆ Heartbeat polling
- ◆ Remote notification
- ◆ Remote access

Each SRS relies on the SSL tunnel, but communication processes and protocols within the tunnel vary by function. Each function is discussed in the following sections.

Heartbeat polling

Heartbeat polling is described in the following sections:

- ◆ [“To Dell EMC by SRS” on page 13](#)
- ◆ [“To Dell EMC devices managed by SRS” on page 13](#)

To Dell EMC by SRS

The *heartbeat* is a polling that occurs every 30 seconds, from SRS to the Dell EMC enterprise. Each heartbeat contains a small datagram that identifies SRS and provides the Dell EMC enterprise with status information on the connectivity and health of the Dell EMC storage devices and the SRS.

Dell EMC ServiceLink receives the data in a Simple Object Access Protocol (SOAP) message. Once this response is acknowledged, the SRS terminates the connection.

Monitoring and event notification are handled by SRS. If a problem occurs with an SRS server and a High Availability SRS Cluster has been implemented, then another SRS within the cluster handles these activities. In a High Availability SRS Cluster, remote access session management is handled by the first SRS to send a heartbeat to the Dell EMC enterprise and to receive the remote access request.

Note: SRS v3.x can only be clustered to other SRS v3.x. They can not be clustered to existing SRS 2.XX or Embedded SRS Device Clients.

To Dell EMC devices managed by SRS

Once every 60 minutes SRS polls each managed device to determine if primary support application(s) are available by making a socket connection to the device on one or more of the primary support application ports and by then verifying that the service applications are responding. If a change in status is detected, then SRS notifies Dell EMC over the next heartbeat.

Remote notification (Connect Home)

SRS also serves as a conduit for Dell EMC products to send remote notification event files to Dell EMC. Dell EMC products send remote notifications for several different purposes. Errors, warning conditions, health reports, configuration data, and script execution statuses may be sent to Dell EMC. [Figure 1 on page 14](#) provides an illustration of the remote notification communication paths.

When an alert condition occurs, the Dell EMC product generates an event message file and passes it to the ConnectEMC service on the device to format the files and request a transfer to Dell EMC. ConnectEMC uploads the file to SRS where it is received by one of the following local transport protocols:

- ◆ HTTPS, if a device is qualified to send files using HTTPS
- ◆ SMTP
- ◆ Passive FTP
- ◆ REST

When an event file is received, SRS compresses the file, opens the SSL tunnel to the Dell EMC servers, and posts the data file to Dell EMC. At Dell EMC, the file is decompressed and forwarded to the Customer Relationship Management (CRM) systems.

Note: The connection in [Figure 1 on page 14](#) is to SRS. SRS forwards the Connect Home file through the SRS tunnel. If the tunnel is unavailable, then SRS can failover to FTPS or to the customer's SMTP server to Dell EMC, if it is configured.

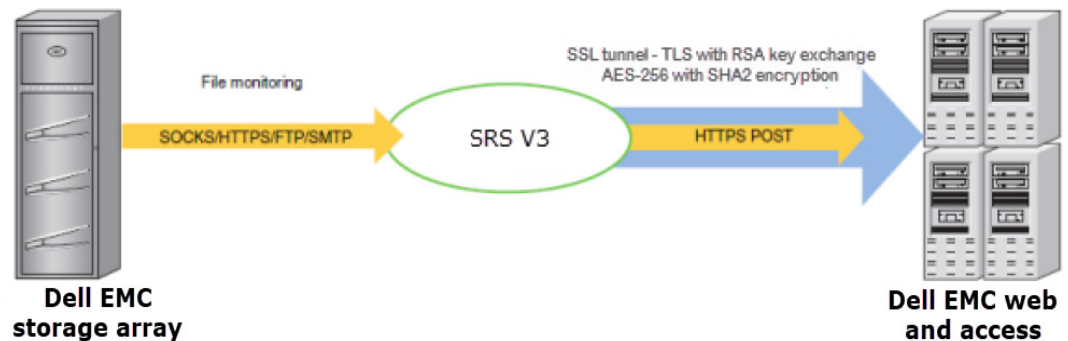


Figure 1 Remote notification communication

Remote access

To establish a Dell EMC Global Services remote access session to a customer's device, SRS uses asynchronous messaging to ensure that all communication is initiated outbound from SRS at the customer's site.

After being properly authenticated at Dell EMC, a Dell EMC Global Services professional makes a request to access a managed device. The remote access session request includes a unique identifier for the user, the serial number of the managed device, and the remote application he or she will use to access the device. It may include the Service Request number and or additional notes. This request is queued at Dell EMC until an SRS that manages the device in question sends a heartbeat to Dell EMC.

In response to the Heartbeat, the Dell EMC enterprise sends a special status in the SOAP response. This response contains the request information as well as the address of the Global Access Server and a unique session ID, which SRS would use to establish the connection. SRS uses its local repository to determine the local IP address of the end device, checks the Policy Manager permissions to see if the connection is permitted, and if approved, establishes a separate persistent SSL tunnel to the Global Access Server for the specific remote access session.

This secure session allows IP traffic from the Dell EMC internal service person to be routed through SRS to the end device. IP socket traffic received by the Global Access Server when the session is established, is wrapped in a SOAP message, and sent to SRS over the SSL tunnel. SRS unwraps the SOAP object and forwards the traffic to the IP address and port of the end device for which the session was established. SOAP communication flows between SRS and the Global Access Server through this tunnel until it is terminated or times out after a period of inactivity. [Figure 2 on page 15](#) provides an illustration of the remote access communication paths.

As a result of an application remote access session request, SRS forwards traffic **only** to the specific IP address and ports that are associated with the registered serial number of the Dell EMC device at the time of deployment.

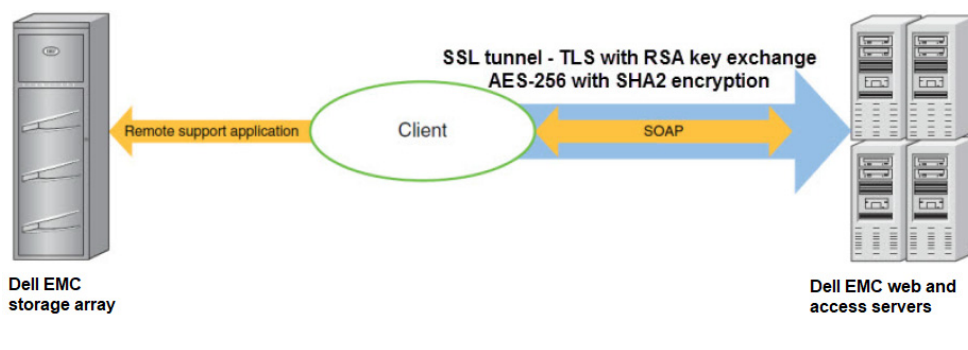


Figure 2 Remote access communication

Digital Certificate Management

During the SRS installation, digital certificates are installed on the SRSv3. All certificate usage is protected by unique password encryption. Any message received by the SRSv3, whether pre- or post-registration, requires entity-validation authentication.

Digital Certificate Management automates SRS digital certificate enrollment by taking advantage of Dell EMC's existing network authentication systems, which use the RSA SecurID Authenticator and the Dell EMC's private certificate authority (CA). Working with Dell EMC systems and data sources, Digital Certificate Management aids in programmatically generating and authenticating each certificate request, as well as issuing and installing each certificate on the SRSv3.

The SRS Digital Certificate provides proof-of-identity for your SRSv3. This digital document binds the identity of the SRS server to a key pair that is used to encrypt and authenticate communication back to Dell EMC. Because of its role in creating these certificates, the Dell EMC Certificate Authority is the central repository for the Secure Remote Services key infrastructure.

Before the certificate authority issues a certificate for the SRSv3, it requires full authentication of a certificate requester by verifying that the Dell EMC Global Services professional making the request is properly authenticated using the Dell EMC RSA SecurID, and belongs to a Dell EMC Global Services group that is permitted to request a certificate for the customer site or by a customer with a valid Dell EMC support account. The certificate authority then verifies that the information contained in the certificate request is accurate and generates the Certificate and returns the certificate to the requestor. The process is as follows:

Once authentication is completed by the customer, Dell EMC personnel, or partner, the SRSv3 installation program gathers all the information required for requesting certificates and generates a certificate request, a private key, and a random password for the private key. The SRSv3 installation program then writes the certificate request information to a request file, ensuring accuracy and completeness of the information.

The installation program then submits the request over a TLS tunnel. After the certificate is issued and returned over the TLS tunnel the installation program automatically installs the certificate to the SRS server.

Note: Due to Dell EMC's use of RSA Lockbox technology, a certificate cannot be copied and used on another machine.

Device access control

SRSv3 achieves remote application access to a process running on a Dell EMC device by using a strict IP and application port-mapping process. You have complete control over which ports and IP addresses are opened on your internal firewall to allow connectivity. The remote access session connection is initiated by a Dell EMC Global Services Professional request that results in a session being staged on a Dell EMC Global Access Server. After the SRSv3 and Policy Manager evaluate the request, the session is established through a pull connection by the SRSv3. Dell EMC never initiates (pushes) a connection to your SRSv3 or network. Your policies determine if and how a connection is established.

Device configuration access control

Once your devices are configured for SRS management, you must ensure that the configuration of the managed devices are carefully controlled and monitored. For example, changing the configured IP address of the SRSv3 will disable the storage device connect home capabilities; or changing the IP address of the storage device will disable Dell EMC's ability to perform remote service on that device. After changes to the SRSv3 or devices configuration are made, these changes **MUST** be reconfigured on the other affected portions of the Solution. Each device modification is tracked in the Policy Manager and the Dell EMC enterprise audit logs.

Note: For REST devices, you will need to read the product documentation on how to update the SRSv3 IP information.

Dell EMC enterprise access control

Several robust security features are incorporated into the Dell EMC enterprise. To access the SRS Enterprise Solution, Dell EMC Global Services professionals or authorized service providers must log in using RSA SecurID two-factor authentication technology. Only authorized Dell EMC personnel or authorized service providers can access the Dell EMC's SRS Enterprise Solution.

Responsibilities for SRS components

The following sections describe the installation, configuration, operation, and maintenance responsibilities of Dell EMC customers and Dell EMC Global Services.

Note: Some products are customer deployable. Please reference the product installation documentation for that information.

Customer

You are responsible for the following:

- ◆ Installing, configuring, and maintaining the following hardware and software components:

- SRS Virtual Edition hardware and virtual host environment for the customer's environment
- Policy Manager server hardware and operating system
- Antivirus and other applicable security software in the customer environment
- ◆ Providing continuous maintenance to the ESX server that hosts the SRS Virtual Edition and the operating systems, including security updates
- ◆ Monitoring and maintaining sufficient disk space
- ◆ Preparing and configuring the network, proxy server, and firewall
- ◆ Backing up and restoring your file systems
- ◆ Maintaining physical security of the hardware
- ◆ Protecting all files on the SRS and the Policy Manager servers, including the SSL certificate(s) if applicable
- ◆ Configuring, administering, and updating policies and accounts on the Policy Manager
- ◆ Maintenance of the Policy Manager servers, including updates, upgrades, and anti-virus protection, is the customer's responsibility. For the SRSv3 Virtual Appliance, updates supplied by Dell EMC must be applied by the customer via the Update tab in the GUI. Dell EMC does not recommend updating the virtual machine using any other method. Customers can install anti-virus protection, however, Dell EMC cannot guarantee that it will be compatible with the V3 software package.

Note: Policy Manager software is customer installable. For more information on the operation and configuration of the Policy Manager, refer to the *Secure Remote Services Policy Manager Operations Guide*.

Note: SRSv3 solutions are not supported for VMware VMotion. VMotion actions can corrupt the RSA Lockbox, which will require a full SRS re-install to recover.

Customer or Dell EMC Global Services

Dell EMC Global Services personnel or customers are responsible for installing the SRS software.

The same is true of the Policy Manager software (customers may install this software) and of the following tasks:

- ◆ Configuring and deploying the Dell EMC devices managed by SRS
- ◆ Updating the SRS and Policy Manager software

Dell EMC Global Services

Dell EMC Global Services are responsible for the following:

- ◆ Configuring SRS Virtual Edition High Availability Clusters must be done by Dell EMC Global Services.
- ◆ Approving the Deployment, Removal, or Revisions of Deployed Devices in ServiceLink

CHAPTER 2

SRS Web UI Configuration

The Web UI configurations are used to view the SRS Version 3 (SRSv3) status, manage the devices for SRSv3, and perform other tasks related to your SRSv3 configuration.

This chapter includes the following topics:

- ◆ [Accessing SRS Version 3 via Web UI.....](#) 20
- ◆ [Using the Dashboard.....](#) 23
- ◆ [Devices - Manage Devices](#) 29
- ◆ [Configuration](#) 37
- ◆ [Audit.....](#) 57
- ◆ [Logs.....](#) 60
- ◆ [Logging out.....](#) 62
- ◆ [Changing the password using the Web UI](#) 63
- ◆ [Exporting to CSV Managed Devices.....](#) 67

Accessing SRS Version 3 via Web UI

Requirements

The following conditions must be met before you can access SRS Version 3 (SRSv3):

- ◆ SRSv3 Appliance setup and customer environment setup (root password, network settings, date and time) completed
- ◆ Web UI Session has not expired during configuration
- ◆ SRSv3 Web UI is supported on Internet Explorer 9 or later, Google Chrome, or Mozilla Firefox browsers.

Logging on and initial setup

After the SRS first boot is set up, you can access SRS through the Web UI as follows:

1. Launch the browser and use `https://<ip of the SRS WebUI>:9443`. The SRS home page displays, as shown in [Figure 3 on page 20](#).

Note: The IP address has been configured by the user during the first boot. The first boot log files record the user's activity during first boot. The log files are cumulative.

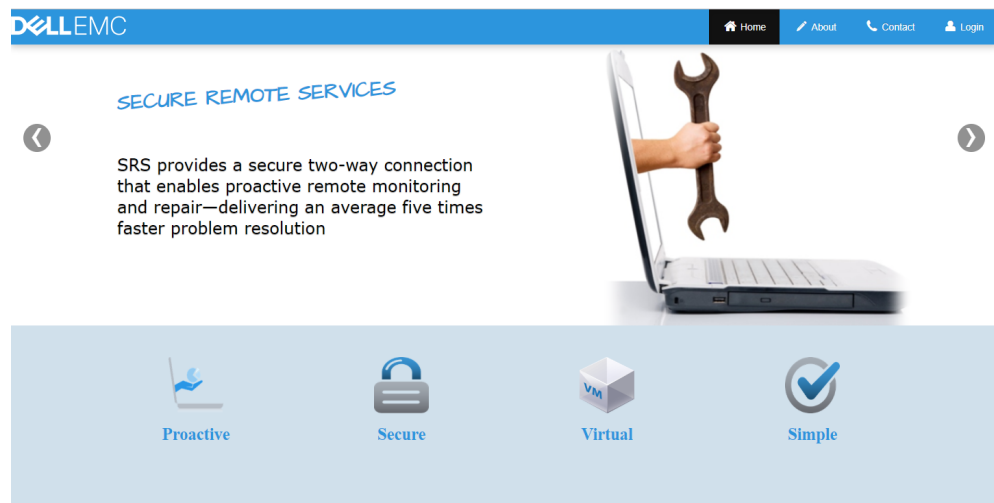


Figure 3 SRS Web UI home page

Note: English is the only language supported on the Web UI.

- In the SRS home page, click **Login**, as shown in [Figure 4 on page 21](#). The Login page appears.

Figure 4 Login page

- In the Login page, log in to SRS using the Admin credentials created during the first boot and the initial configuration/setup of the SRS, and then click **Login**. The SRS dashboard appears.

Login attempts

After provisioning SRS, when you logon to the SRS Web UI, and if the login attempt was unsuccessful, it will display the number of attempts at the bottom of the page. See [Figure 5](#) for example. The maximum attempt allowed is five for local host and three for LDAP.

Figure 5 Login Failed

If you have admin privileges, you can reset the administration password by selecting **admin > Change Password** on the SRS Web UI. This procedure can be found in the [“Changing the password using the Web UI” on page 63](#).

Note that you may have to wait at least 15 minutes before logging back in, and then refresh the page.

Using the Dashboard

The Dashboard is the home page of the SRS Web UI, which displays information related to SRS. You can use the dashboard to verify the status of SRS and all services. Information includes serial number and current version of SRS, SRS health status, and the health status of all the services related to SRS.

The Dashboard displays after first boot, when you log in as Admin. The following tabs display on the Dashboard:

- ◆ System Status
- ◆ Remote Sessions
- ◆ Active MFT Sessions
- ◆ Active Remote Scripts
- ◆ Connect Homes
- ◆ Alerts
- ◆ Service Status
- ◆ Update

A brief description of each tab is provided in the following sections.

System Status tab

The System Status, as shown in [Figure 6 on page 23](#), displays all the information entered in the system. It gives the basic and necessary information for SRS, for example, the connectivity status and the environment to which SRS is pointing.

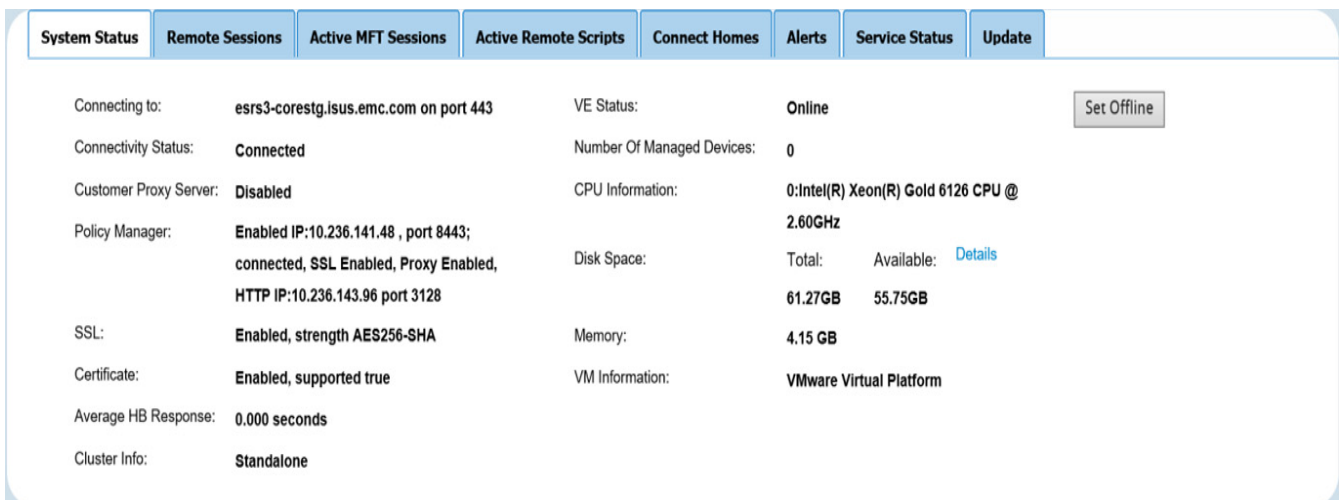


Figure 6 Dashboard - System Status

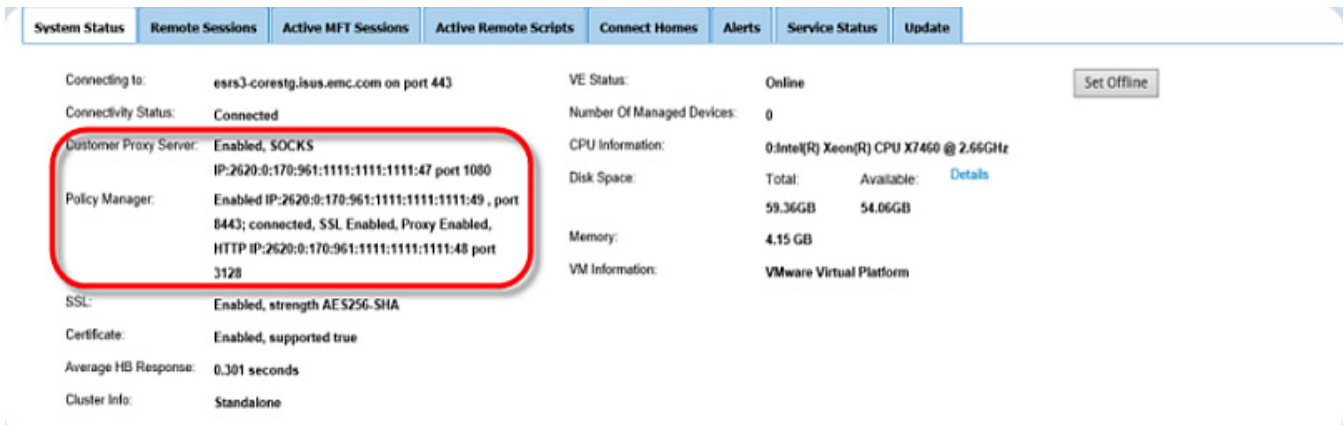


Figure 7 Dashboard - System Status tab using IPV6 connection

Remote Sessions tab

The Remote Sessions tab displays all of the active remote sessions for the devices that are being managed by the SRSv3. [Figure 8 on page 24](#) shows a record of the Dell EMC Remote application launched from the Symmetrix-GW.

System Status	Remote Sessions	Active MFT Sessions	Active Remote Scripts	Connect Homes	Alerts	Service Status	Update
Started At	Model	Serial Number	Device IP	Application Name	Port	User	Duration (mins)
2017-10-07 05:40:19	VNX-GW	FNM00130702660-CS0	10.241.166.223	CLIViaSSH	2022,22	1003358	0.6

Figure 8 Dashboard - Remote Sessions for IPV4

System Status	Remote Sessions	Active MFT Sessions	Active Remote Scripts	Connect Homes	Alerts	Service Status	Update
Started At	Model	Serial Number	Device IP	Application Name	Port	User	Duration (mins)
2018-03-04 09:38:33	Beta1-GW	BETA1DELL10	2620:0:170:961:1111:1111:1111:44	CLIViaSSH	22	1110275	0.9

Figure 9 Dashboard - Remote Sessions for IPV6

Active MFT Sessions tab

This tab displays the details of files being transferred from the products to Dell EMC using the SRS Managed File Transfer (MFT) process.

If there are stale session records, then the **Clear** button becomes enabled. This may occur when performing upgrades, where the user may see an error message stating that the sessions should be removed.

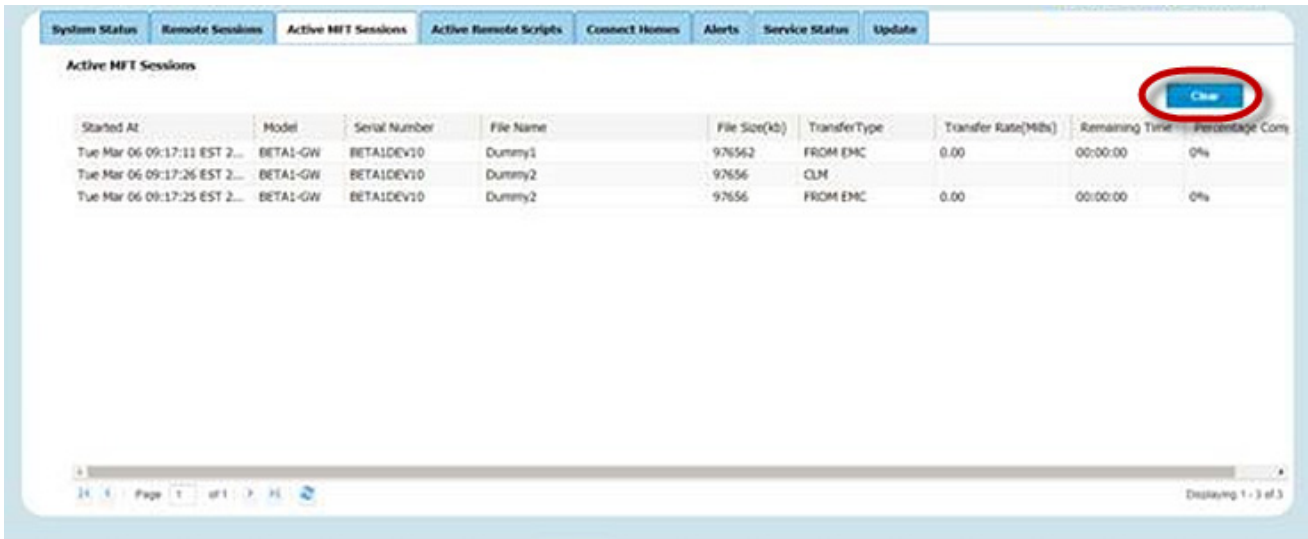


Figure 10 Dashboard - Active MFT Sessions

When the user clicks the **Clear** button, a pop-up window displays, prompting the user to confirm. If the user clicks **OK**, then the records will be cleared.

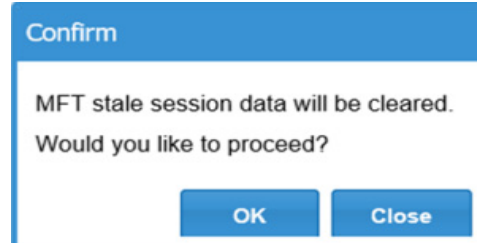


Figure 11 Confirmation box for clearing stale MFT sessions

This tab displays the details of files being transferred from the products to Dell EMC using the SRS Managed File Transfer (MFT) remote scripting capability.

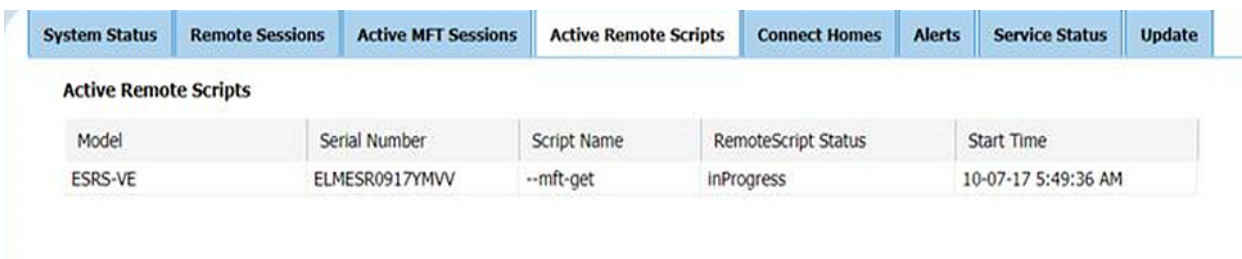


Figure 12 Dashboard - Active Remote Scripts

Connect Homes tab

The **Connect Homes** tab displays the total file count, the oldest file age, as well as all of the files that are present in the poll directory of SRS that have yet to upload to Service Link. [Figure 13 on page 26](#) shows six records, indicating that those files are present in the poll directory of the SRS host.

System Status	Remote Sessions	Active MFT Sessions	Active Remote Scripts	Connect Homes	Alerts	Service Status	Update
---------------	-----------------	---------------------	-----------------------	---------------	--------	----------------	--------

Total File Count: 6 Oldest File Age: 0 mins (Click on each record to get additional details.)

Started At	File Name	File Size (kb)	Age (mins)
10/07/17 05:54 AM	/opt/connectemc/poll/RSC_ELMAPP1017NRRH_100717_055457757.xml	2	0
10/07/17 05:54 AM	/opt/connectemc/poll/RSC_ELMAPP1017NRRH_100717_055456068.xml	2	0
10/07/17 05:54 AM	/opt/connectemc/poll/RSC_ELMAPP1017NRRH_100717_055457757.cec	2	0
10/07/17 05:54 AM	/opt/connectemc/poll/RSC_ELMAPP1017NRRH_100717_055457757.xml.gzip	0	0
10/07/17 05:54 AM	/opt/connectemc/poll/RSC_ELMAPP1017NRRH_100717_055452646.xml	2	0
10/07/17 05:54 AM	/opt/connectemc/poll/RSC_ELMAPP1017NRRH_100717_055459482.xml	2	0

Page 1 of 1

Figure 13 Dashboard - Connect Homes

Alerts tab

When there is a change in SRS, any events that need user attention are displayed on this page, for example, proxy server disabled, Policy Manager has changed, or connectivity issues.

In the **Alerts** tab, all of the alerts for this particular SRSv3 are displayed with options to **Acknowledge** and **Acknowledge All** alerts. You can click each record to get additional details.

System Status	Remote Sessions	Active MFT Sessions	Active Remote Scripts	Connect Homes	Alerts	Service Status	Update
---------------	-----------------	---------------------	-----------------------	---------------	--------	----------------	--------

☐ Acknowledge ☐ Acknowledge All (Click on each record to get additional details.)

<input type="checkbox"/> Date	Service Name	Caller ID	Caller IP	Action	Status
<input type="checkbox"/> 03/04/2018 09:38:33 AM	Agent Service	1110275	127.0.0.1	Remote Session Monitoring	0
<input type="checkbox"/> 03/03/2018 02:54:13 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	201
<input type="checkbox"/> 03/02/2018 01:49:36 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	201
<input type="checkbox"/> 03/02/2018 01:49:20 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	201
<input type="checkbox"/> 03/02/2018 01:09:11 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	201
<input type="checkbox"/> 03/02/2018 01:08:26 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	201
<input type="checkbox"/> 03/02/2018 01:06:31 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	201
<input type="checkbox"/> 02/28/2018 09:23:59 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	201
<input type="checkbox"/> 02/28/2018 09:19:38 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	201
<input type="checkbox"/> 02/28/2018 09:09:08 AM	esrsconnectivityreport	Internal Caller	2620:0:170:961:20...	Add Device	500

Page 1 of 2

Displaying 1 - 10 of 18

Figure 14 Dashboard - Alerts for IPV6

Service Status tab

In the **Service Status** tab, the status of each service related to SRSv3 is displayed.

- ◆ Green circle indicates that the service is running
- ◆ Red circle indicates that the service has stopped or is not working.

You can also check the banner to verify the health status of the system, as shown in [Figure 15 on page 27](#).

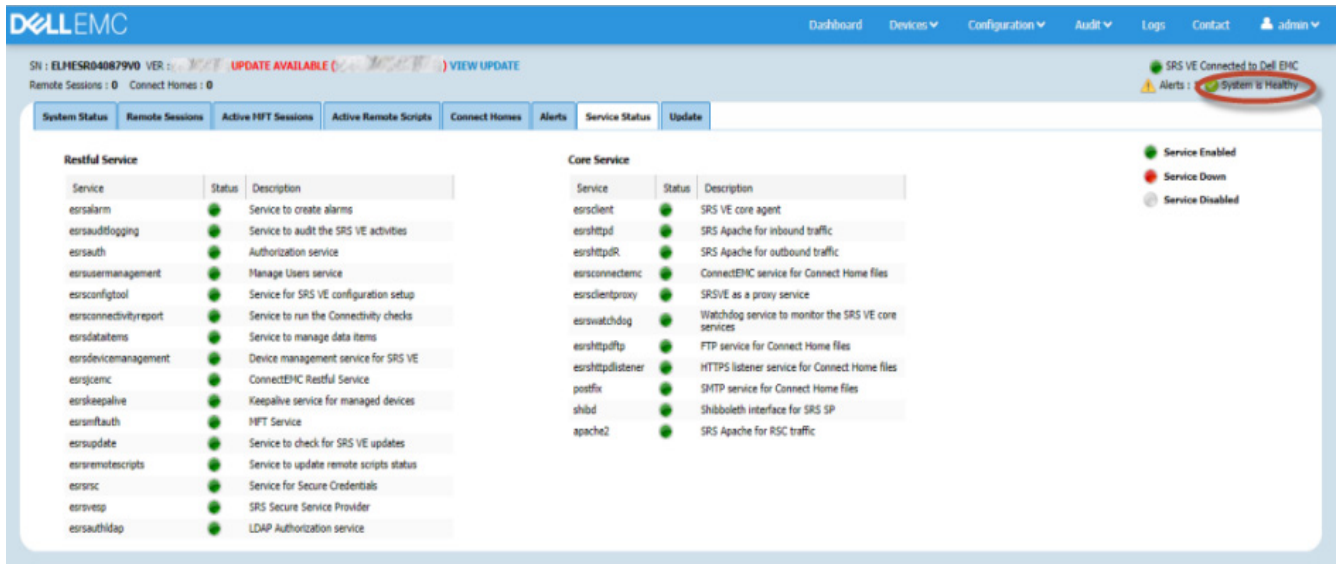


Figure 15 Dashboard - Service Status tab

Update tab

The **Update** tab provides the following:

- ◆ Information on the current version of SRS
- ◆ Latest updates available from the SRS backend
- ◆ Summary of previously downloaded updates with release notes

See [Figure 16 on page 27](#) for example.

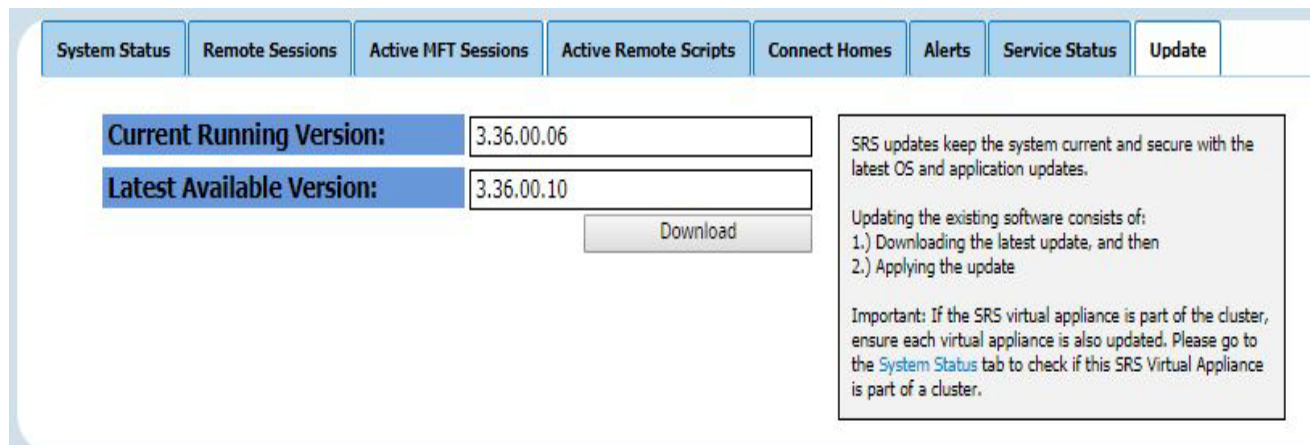


Figure 16 Update tab

Taking SRS offline

Note: This feature is only available for SRS version 3.12 or higher. For more information, visit the Dell EMC Community Update.

This section explains how to take your machine offline and make it a standalone for down time/planned maintenance purposes.

On the Dashboard page, the **VE Status** should be displaying **Online**, as highlighted in [Figure 17](#).

To set it to offline, you can click the **Set Offline** button, as shown in [Figure 17](#). This updates ServiceLink to offline. Note that all devices under the gateway will be marked offline.

This feature is only available in the ServiceLink 6.8 infrastructure.

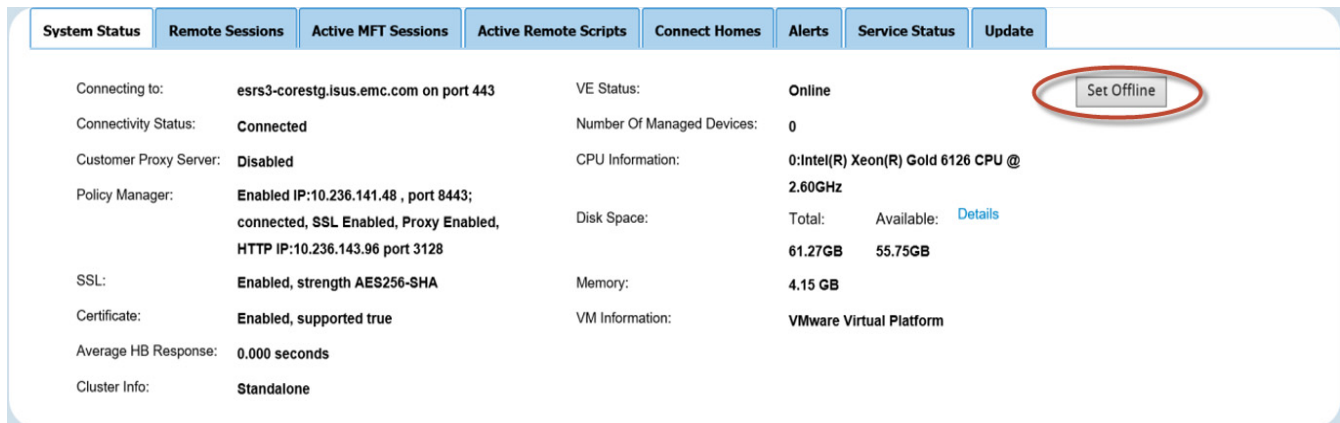


Figure 17 Selecting Set Offline

Setting each device offline

Setting the devices offline for maintenance or downtime will prevent the SRSv3 server from sending Connect Homes generated by those devices that are offline. If you set the SRSv3 server offline, all Connect Homes from any devices being managed will not connect home through the SRSv3 until it is back online.

Note: If the device status is shown as missing on the Manage Device page, then this functionality is disabled.

To set a particular device as offline, go to **Devices > Manage Device**, and then select the applicable **Set Offline** button, as shown in [Figure 18](#).

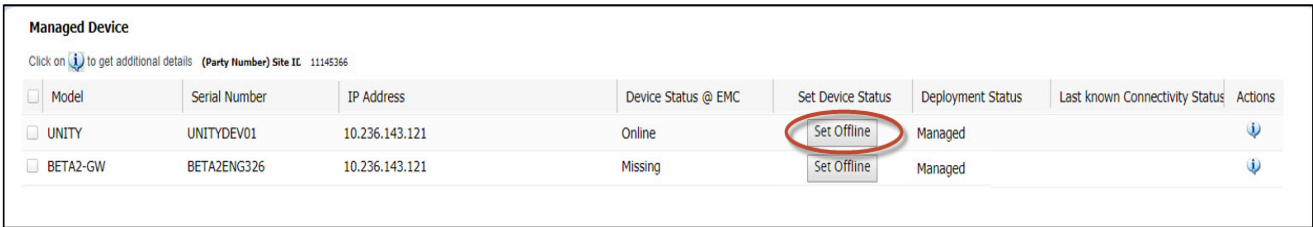


Figure 18 Setting a device Offline

To set the devices back online, click the **Set Online** button next to the corresponding device.

Devices - Manage Devices

Users can add, edit, and remove devices using the **Manage Device** option, which is displayed under the **Device** tab, as shown in [Figure 19 on page 29](#). The Manage Device page also displays the last known connectivity status for the devices, as well as additional information such as on demand real time socket connection details.

⚠ CAUTION

For REST enabled devices, consult the product documentation on SRS deployment instructions. REST enabled products need to be added, updated, and removed from the product and not from the SRS Web UI.

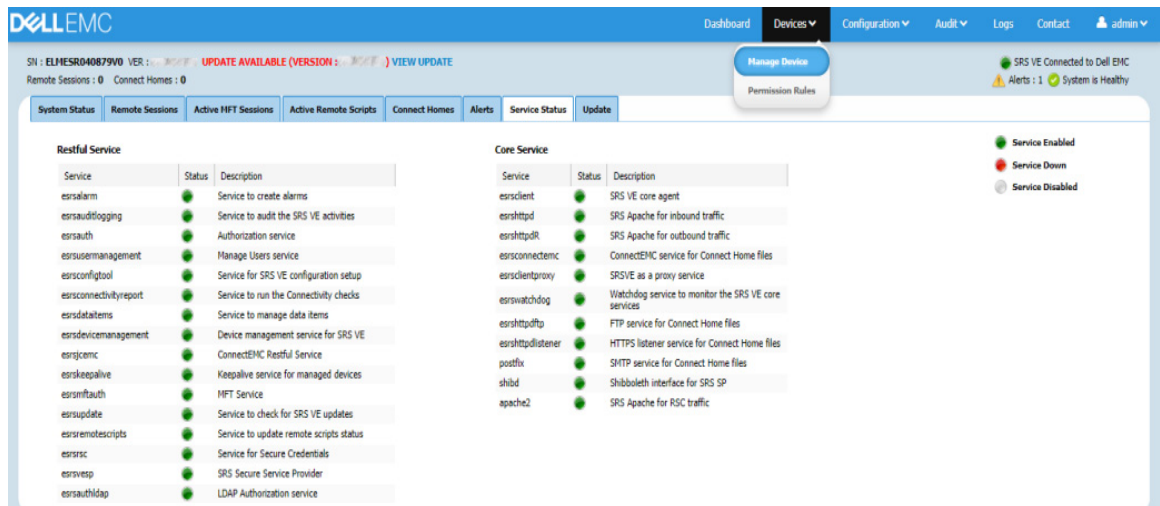


Figure 19 Selecting Devices > Manage Devices

Once you are on this page, you can follow the steps in the following sections to manage the devices.

Adding devices

To add a device to the SRS system:

1. In the Manage Device page, click **Add**, as shown in [Figure 20 on page 29](#). The **SRS Manage Device** window appears.

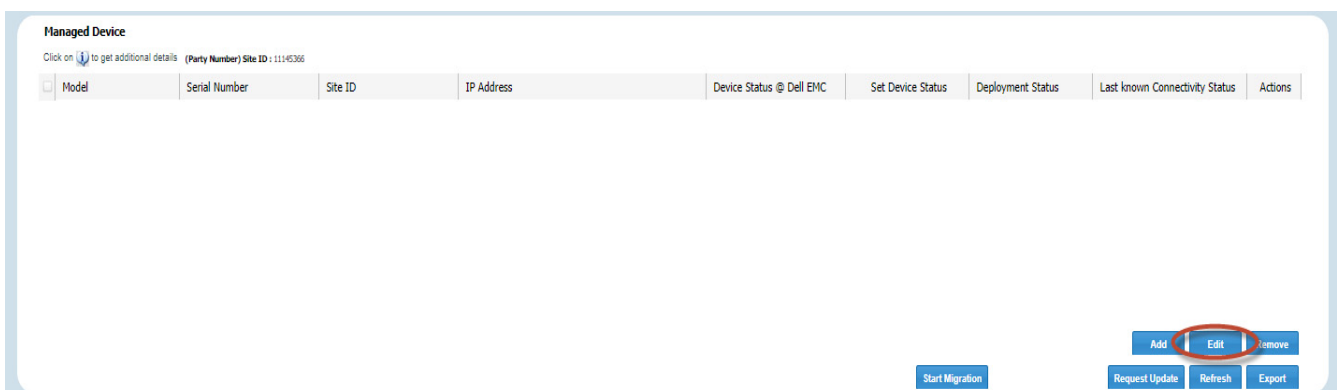


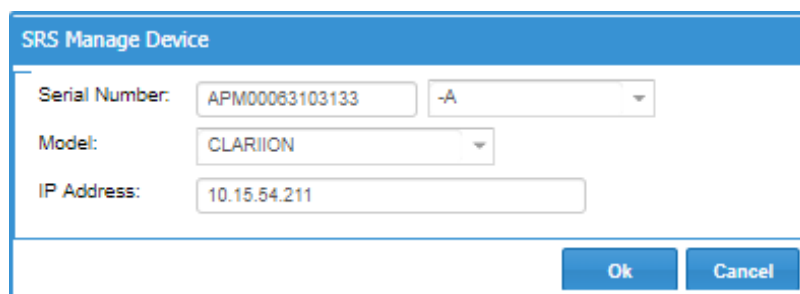
Figure 20 Adding a device

2. In the **SRS Manage Device** window, input the following information, as shown in [Figure 21 on page 30](#):

- Serial number
- If applicable, the suffix for the serial number

Note: This only applies to serial numbers with multiple nodes deployed to SRS, for example, serial number APM00063103133-B, as shown in [Figure 21 on page 30](#). The Secure Remote Services Release 3.xx Site Planning Guide.pdf has information on suffixes.

- Model
- IP address

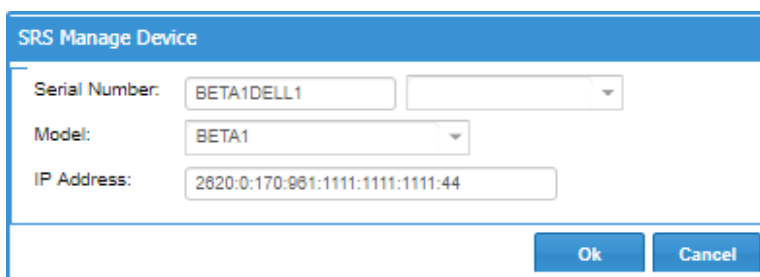


The SRS Manage Device window shows the following configuration for IPv4:

- Serial Number: APM00063103133
- Suffix: -A
- Model: CLARIION
- IP Address: 10.15.54.211

Buttons: Ok, Cancel

Figure 21 Entering device to be added for IPV4



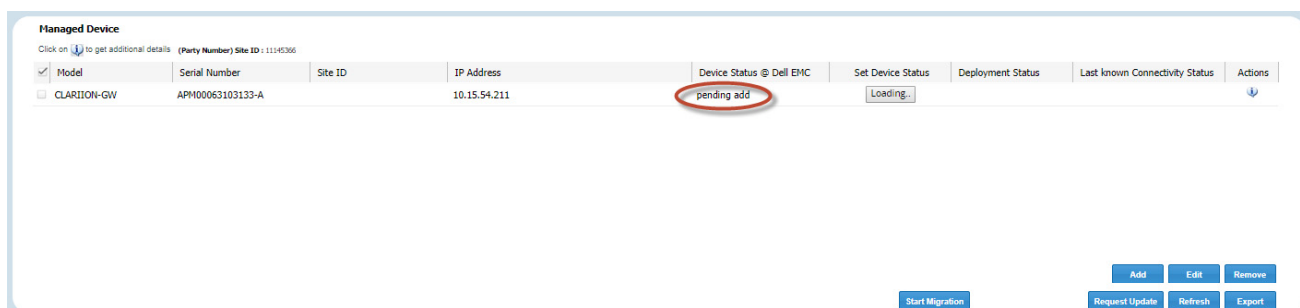
The SRS Manage Device window shows the following configuration for IPv6:

- Serial Number: BETA1DELL1
- Suffix: (empty)
- Model: BETA1
- IP Address: 2620:0:170:961:1111:1111:1111:44

Buttons: Ok, Cancel

Figure 22 Entering device to be added for IPV6

3. Click **Ok**. A pending status appears in the Manage Device list, as shown in [Figure 23 on page 30](#).



Model	Serial Number	Site ID	IP Address	Device Status @ Dell EMC	Set Device Status	Deployment Status	Last known Connectivity Status	Actions
<input checked="" type="checkbox"/> CLARIION-GW	APM00063103133-A		10.15.54.211	pending add	Loading...			

Buttons: Add, Edit, Remove, Start Migration, Request Update, Refresh, Export

Figure 23 Pending add

- Click **Request Update**. A message window appears, as shown in [Figure 24 on page 31](#).

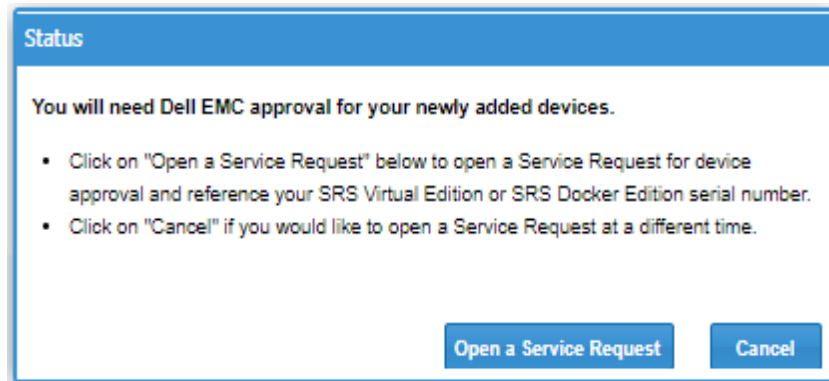


Figure 24 Message box

- In the message window, click **Open a Service Request**. The window closes.
- Contact Dell EMC to notify them that the device has been added and requires Dell EMC personnel to go to ServiceLink directly to approve the request.

Note: The device will not be listed and managed until the request has been approved and the sync has occurred on Dell EMC ServiceLink. Approval can only be done by Dell EMC personnel who have access to ServiceLink.

- Once the request is approved by Dell EMC, click the **Refresh** button or restart your WebUI.

Editing IP addresses of devices

To edit the IP address of a device:

- In the Manage Device page, check the device to be edited, and then click **Edit**. The **SRS Manage Device** window appears.
- In the **SRS Manage Device** window, edit the IP address, and then click **Ok**. A pending status appears in the Manage Device list.
- Click **Request Update**. A message window appears.
- In the message window, click **OK**. The window closes.
- Contact Dell EMC to notify them that the device has been modified and requires Dell EMC personnel to go to ServiceLink directly to approve the request.

Note: The edit will not take effect until the request has been approved and the sync has occurred on Dell EMC ServiceLink.

- Once it is approved in ServiceLink, click the **Refresh** button to update the status.
- To check the status of *Pending Add*, contact your local Account Service Representative. The device maintains the *Pending Add* status until it gets approved. There is no time limit.

Removing devices

To remove a device from the SRS system:

- In the Manage Device page, select the device to be removed, and then click **Remove**. A confirmation window appears.

2. Click **Ok**. A pending status appears in the Manage Device list.
3. Click **Request Update**. A message window appears.
4. In the message window, click **OK**. The window closes.
5. Contact Dell EMC to notify them that the device has been modified and requires Dell EMC personnel to go to ServiceLink directly to approve the request.

Note: The device will still be managed until the request has been approved and the sync has occurred on Dell EMC ServiceLink.

6. Once it is approved in ServiceLink, click the **Refresh** button and the device will no longer appear in the list.

Migrating devices

Note: Only authorized persons with a Dell EMC SecureID can migrate. Partners must be a Primary Dispatch Resource (PDR) for both SRS v2.x and SRS v3.0x.

This procedure allows you to transfer (via the SRSv3 Web UI) deployed devices from existing Windows and Linux gateways to SRSv3, after the installation of SRSv3.

To migrate devices:

1. In the Manage Device page, click the **Start Migration** button. The **SRS Migrate Gateway** window appears.

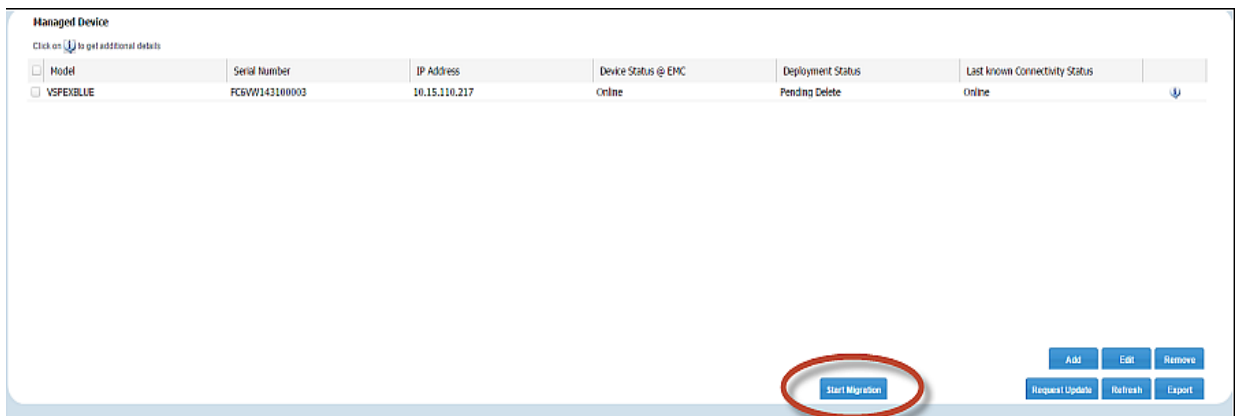
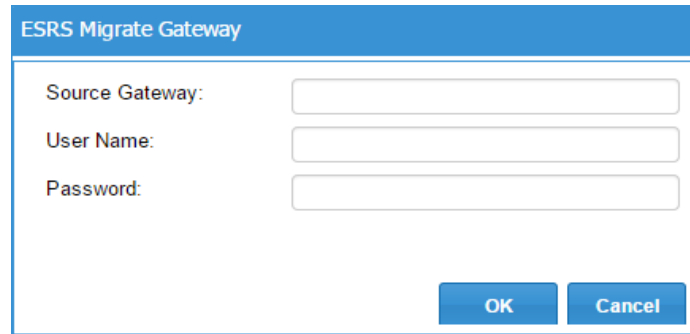


Figure 25 Start Migration

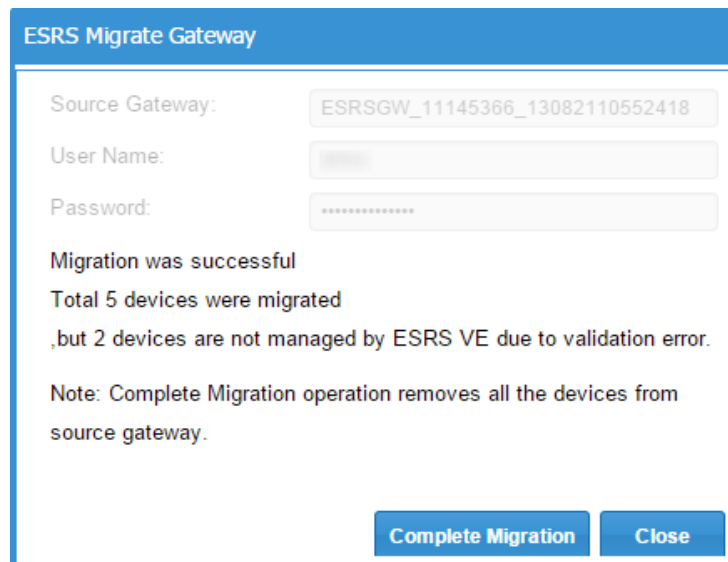
2. In the pop-up window, enter the following information:
 - Source Gateway (Serial Number)
 - User Name
 - Password



The dialog box titled "ESRS Migrate Gateway" contains three input fields: "Source Gateway:", "User Name:", and "Password:". At the bottom right, there are two buttons: "OK" and "Cancel".

Figure 26 Entering details

3. Click **OK**. If you were successful, then a Migration was successful message appears.



The dialog box titled "ESRS Migrate Gateway" displays the following information:

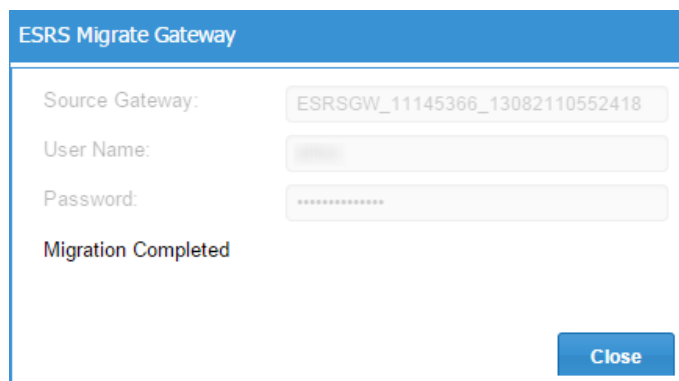
- Source Gateway: ESRSGW_11145366_13082110552418
- User Name: [redacted]
- Password: [redacted]
- Migration was successful
- Total 5 devices were migrated
- ,but 2 devices are not managed by ESRS VE due to validation error.
- Note: Complete Migration operation removes all the devices from source gateway.

At the bottom right, there are two buttons: "Complete Migration" and "Close".

Figure 27 Migration successful

4. Verify that all devices are migrated as expected by comparing the devices between the source gateway and the target SRS.

- Click **Complete Migration**. If you were successful, then a Migration Completed message displays and the devices are no longer managed by the source gateway.



The screenshot shows a dialog box titled "ESRS Migrate Gateway". It contains three input fields: "Source Gateway:" with the value "ESRSGW_11145366_13082110552418", "User Name:" with a blurred value, and "Password:" with a masked value "*****". Below these fields, the text "Migration Completed" is displayed in red. A blue "Close" button is located at the bottom right of the dialog.

Figure 28 Migration completed

- Click **Close**. The Manage Device page appears.
- Go to ServiceLink and navigate to the Source Gateway Managed Devices page (DMB page).
- To remove all devices associated with the legacy gateway, click **Remove All** button. A pop-up window displays a confirmation message.
- Click **OK**. The pop-up window closes and no devices are managed by the source gateway.
- When all of the devices are unmanaged on the source gateway, then the Customer Engineer (CE) manually sets the gateway status to offline in ServiceLink.

Note: CE must check the status of the devices before setting the gateway offline. Even if some of the devices were not removed, the migration process is still considered complete or successful. If this is the case, then the customer must manually undeploy the devices from the source gateway to complete the migration.

Actions column

Additional data is displayed when you click the bubble under the Actions column.

Additional data includes the following managed device details:

- ◆ Device Model
- ◆ Device Serial Number
- ◆ Device IP Address
- ◆ Connected State
- ◆ Validation Status

Permissions Rule

Permissions are set by the customer in the SRS Web UI. Note that MFT for Isilon is not considered full MFT and therefore is not handled as such in the SRS WebUI. Note the following as well regarding permissions in the SRS WebUI:

- ◆ If any rules are not set, the check box is not selected.
- ◆ Permissions can be allowed or denied.
- ◆ If a device is bidirectional that means it can support both From Dell EMC and To Dell EMC.

To set permissions:

1. Go to **Devices > Permission Rules**.
2. Select the check box for the desired permission, as shown in [Figure 29](#). By default, all three options (MFT From Dell EMC [GET], MFT To Dell EMC [PUSH], Remote Scripting) are selected.

<input type="checkbox"/>	Model	Serial Number	IP Address	Deployed Status	Rules			Updated By	Last Updated Date
					MFT From EMC	MFT To EMC	Remote Scripting		
<input type="checkbox"/>	ESRS-VE	ELMESR0218R6TQ	-	-	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	BETA1-GW	BETA1DELL10	2620:0:170:961:1111:1111:1111:44	Managed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	BETA1-GW	BETA1DELL1	2620:0:170:961:1111:1111:1111:44	Managed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	ISILON-GW	ISILONTEST05	2620:0:170:961:1111:1111:1111:41	Managed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	SWITCH-BROCA...	BRW2539J09-CLI	10.236.143.121	Validation Error	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Page 1 of 1

Displaying 1 - 5 of 5

Figure 29 Permission Rules page with IPV4 and IPV6 addresses

3. If applicable, select Remote Scripting to allow the user to run the script remotely.
4. Click **Save**.
5. The system may prompt the customer to enter the customer's support zone credentials, that is, the same credentials used in provisioning. If this is the case, then enter the credentials and click **Login**, as shown in [Figure 30](#). Changes are updated on the Manage Device page.

Note: Credentials are only requested once per session, if the user has not logged out.

UserName:

Password:

Figure 30 Entering user credentials

6. If you are not asked for credentials, then a confirmation box appears, as shown in [Figure 31](#). Click **OK**. Changes are saved on the Manage Device page.

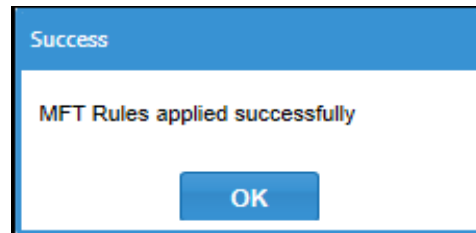


Figure 31 Confirmation box

Configuration

You can configure the following features to SRSv3 after provisioning.

- ◆ Email Configuration
- ◆ Policy Manager
- ◆ Proxy Server
- ◆ Connect Home
- ◆ Network Check
- ◆ Customer Contact
- ◆ VMware Tools
- ◆ LDAP Configuration

These features can be found listed under the **Configurations** tab present in the menu bar of the WEBUI.

The step-by-step procedure of enabling and disabling the above features are explained in the following sections.

E-mail configuration

1. The **Email Configuration** is the first option listed under the **Configurations** tab. Select **Email Configuration**, and the email configuration page appears.
2. In the Email Configuration page, you must provide valid data for all of the fields in order to receive the notification emails.
 - Enable onSuccess Notification checkbox is indicated on the SRS Web UI to enable sending notifications to the email address listed on the Email Configuration screen, during provisioning as well as post provisioning.
 - If onSuccess is checked and you have configured the ConnectEMC Configurations, then the emails are triggered to the contacts list for successful Connect Home events; However, notifications for failed ConnectEMC sessions will occur whether notifications are turned on or off.

E-mail Configuration

☒ Enable onSuccess Notification

☒ Enable Device Connection Notification

Email Server *: mailhub.lss.emc.com

Port *: 25

Sender Email *: esrssupport@emc.cor

Notification Email *: scott.jones@nordstror

Add Email

Notification settings

- To send notification e-mails and Connect Home files (if enabled), provide e-mail server and its port details in the E-mail Server and Port text boxes.
- Provide an email address in the **Sender Email** section which can be used as FROM address in the email notifications.
- Provide an email address in the **Notification Email** section which will be used as recipients for any critical failure event notifications and for successful events (if configured).
- Use Test option to send a test E-mail.

Test **Apply Settings**

Figure 32 Email Configuration

- Enable Device Connection Notification: SRS sends the customer an email notification whenever Dell EMC personnel connects to a device. This must be selected as an option.

Note: To configure more than one email ID in the notification email, click on the **Add Email** button.

3. When the email configurations are configured, click the **Test** button to validate the details provided in the Email Configuration page.

Note: Always click **Test** before clicking **Apply Settings**.

For correct details verification, a success pop-up message appears, and a test e-mail is sent to the mail IDs configured in the Email Configuration page.

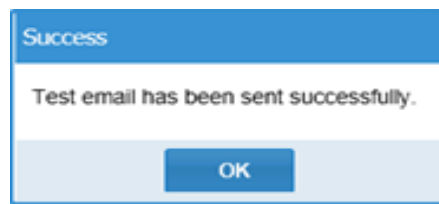


Figure 33 Success pop-up message

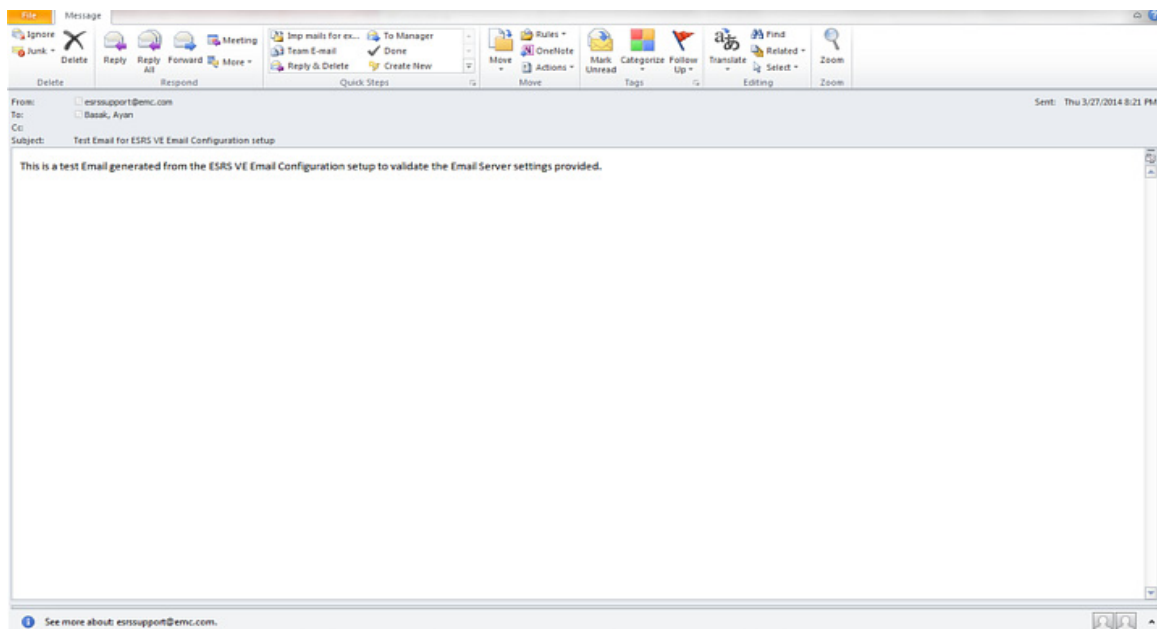


Figure 34 Sample of test e-mail received by the listed participants

Click **Apply settings** once the configuration is validated in order to apply the configuration changes to SRS.

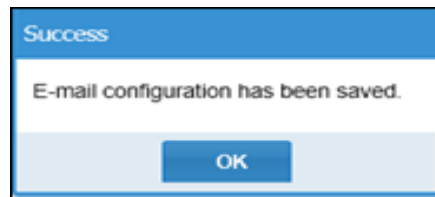


Figure 35 Saving email configuration

Policy Manager

The Policy Manager configuration is the second option listed under the **Configuration** tab. By selecting the policy configuration option, you are redirected to the Policy Configuration page.

Note: The below do not apply to eVE in Unity/CloudIQ Collector.

- ◆ The user can configure Policy Manager 6.9 with these options:
 - Non-SSL
 - SSL
 - SSL with Agent authentication
- ◆ **Enable Agent Authentication for Policy Manager** option is added - By enabling this option, the user can send the authentication request. Agent authentication is available only for SSL. Once the user selects this option, they are required to enter the following details:
 - User Name - Policy Manager admin user name
 - Password - Policy Manager admin password
 - Policy Manager Port - Policy Manager user port
 - Agent PassKey - Passkey provided during installation (encrypted in UI)
 - Configure - User can send authentication request using this option

Note: Enable agent authentication is available only if the user enters the port number 8445.

DELL EMC SRS Virtual Edition 3.36.00.10 admin

☐ **Enable Agent Authentication For Policy Manager (6.9)**

PM User Name: PM Password:

PM Port: Agent Pass Key:

Configure

CUSTOMER PROXY SERVER FOR POLICY MANAGER

☐ **Enable Proxy Server for Policy Manager only**

☐ HTTP ☐ SOCKS

IP Address:

Port:

☐ **Authenticate using the following information**

User Name:

Password:

Policy Manager

- Enter Policy Manager details and optional proxy configuration for Policy Manager.
- Agent Communication to PM 6.9 is restricted to configured ports.
- For SSL, use port 8443. For non-SSL, use port 8090 or the port entered during Policy Manager Installation. For SSL with agent authentication, use port 8445.
- If the correct port is not selected, you may experience connectivity issues

Submit & Go to Connect Home

Figure 36 Agent authentication during provisioning

Connection

☐ **Enable Remote Policy Manager**

IP Address/Host:

Port: Enable SSL: ☐ Strength:

☐ **Enable Agent Authentication for policy manager**

PM UserName:

PM Password:

PM Login Port: Agent PassKey:

Configure

Customer Proxy Server

☐ **Enable Proxy Server for Policy Manager only**

Proxy Type:

IP Address/Host: Port:

☐ **Authenticate using following information**

User Name:

Password:

Policy Manager

- Enter Policy Manager details and optional proxy configuration for Policy Manager.
- Agent Communication to PM 6.9 is restricted to configured ports.
- For SSL, use port 8443. For non-SSL, use port 8090 or the port entered during Policy Manager Installation. For SSL with agent authentication, use port 8445.
- If the correct port is not selected, you may experience connectivity issues with the client connecting to both DELL EMC Enterprise and Policy Manager.
- If the correct agent details are not entered you will experience connectivity issues.
- Login to the Policy Manager actively once before configuring the PM with agent authentication in VE.
- Use **Test** option to check the connectivity to Policy Manager from SRS VE.

Figure 37 Agent authentication after provisioning

Proxy Server

SRS can be configured with proxy from the Proxy Server Configuration page.

Specifically, you can configure the following types of proxy:

- ◆ HTTP with authentication
- ◆ HTTP without authentication
- ◆ SOCKS with authentication
- ◆ SOCKS without authentication

Accessing proxy configuration

To access proxy configuration, go to **Configuration > Proxy Server**. The Proxy Configuration page appears.

Enabling proxy between client and Dell EMC

To enable or edit the current proxy server settings between SRS Client and Dell EMC Enterprise:

1. Select the **Enable Proxy between Client and Dell EMC Enterprise** checkbox, as shown in [Figure 38 on page 41](#).

Figure 38 Enabling proxy check box

2. In the Proxy Type menu, select the desired proxy type.
3. In the IP Address/Host field, enter your desired IP address.
4. In the Port field, enter your port information.

Note: If your Proxy is not set up with credentials, then you do not have to select the **Authenticate using following information** checkbox.

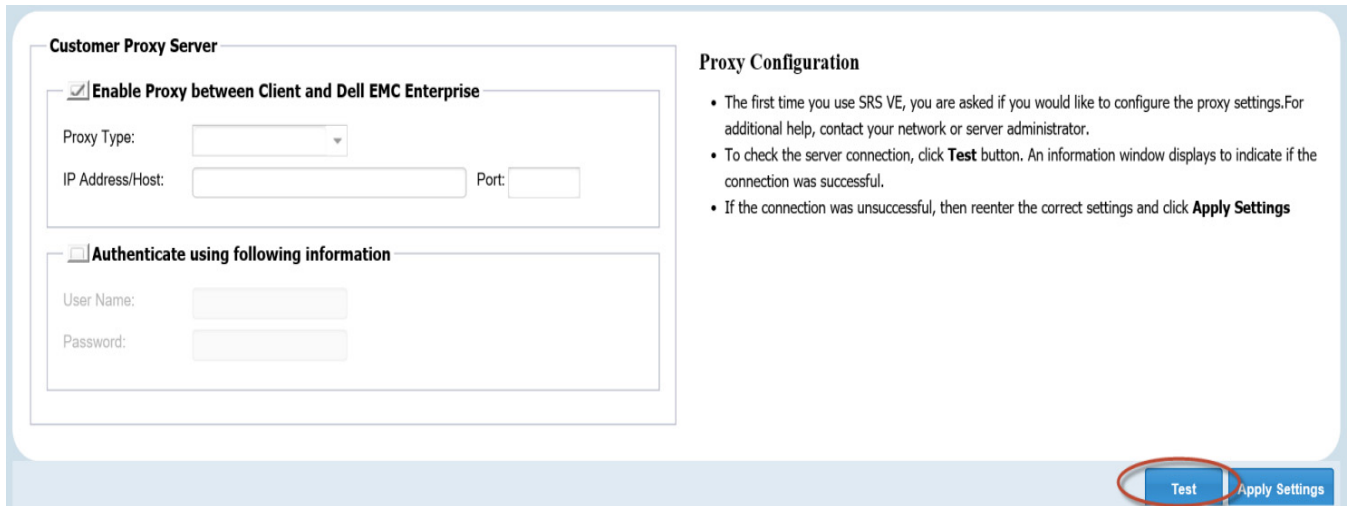
Testing server connection

To test the server connection:

IMPORTANT

Always test connectivity before clicking the Apply Settings button.

1. Click the **Test** button, as shown in [Figure 39 on page 42](#).



The screenshot shows the SRS Web UI Configuration page. On the left, under the heading "Customer Proxy Server", there is a checkbox labeled "Enable Proxy between Client and Dell EMC Enterprise" which is checked. Below this, there are input fields for "Proxy Type:" (a dropdown menu), "IP Address/Host:" (a text box), and "Port:" (a text box). Below these fields is a section titled "Authenticate using following information" with input fields for "User Name:" and "Password:". On the right side of the page, under the heading "Proxy Configuration", there is a list of instructions: "The first time you use SRS VE, you are asked if you would like to configure the proxy settings. For additional help, contact your network or server administrator.", "To check the server connection, click **Test** button. An information window displays to indicate if the connection was successful.", and "If the connection was unsuccessful, then reenter the correct settings and click **Apply Settings**". At the bottom right of the page, there are two buttons: "Test" and "Apply Settings". The "Test" button is circled in red.

Figure 39 Selecting Test

2. If you connected successfully, then a success test message appears, as shown in [Figure 40 on page 42](#). Click **OK**.

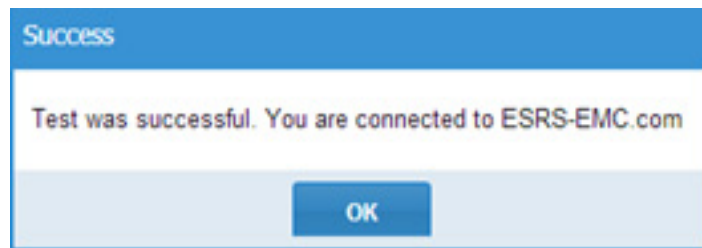


Figure 40 Success message

3. If unsuccessful, then reenter the correct settings in the Customer Proxy Server section and retest.

4. When the test is successful, click **Apply Settings**, as shown in [Figure 41 on page 43](#). A confirmation message appears.

Customer Proxy Server

☒ **Enable Proxy between Client and Dell EMC Enterprise**

Proxy Type:

IP Address/Host: Port:

☐ **Authenticate using following information**

User Name:

Password:

Proxy Configuration

- The first time you use SRS VE, you are asked if you would like to configure the proxy settings. For additional help, contact your network or server administrator.
- To check the server connection, click **Test** button. An information window displays to indicate if the connection was successful.
- If the connection was unsuccessful, then reenter the correct settings and click **Apply Settings**

Test **Apply Settings**

Figure 41 Clicking Apply Settings

5. In the confirmation message window, click **OK**, as shown in [Figure 42 on page 43](#). The window closes.

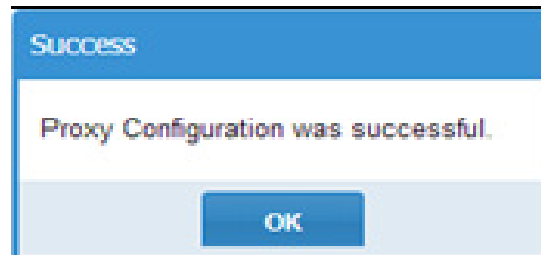


Figure 42 Clicking OK

Connect Home

The Connect Home page allows you to enable and test Connect Home failover to alternative paths. [Figure 43 on page 43](#) shows you how to access Connect Home.

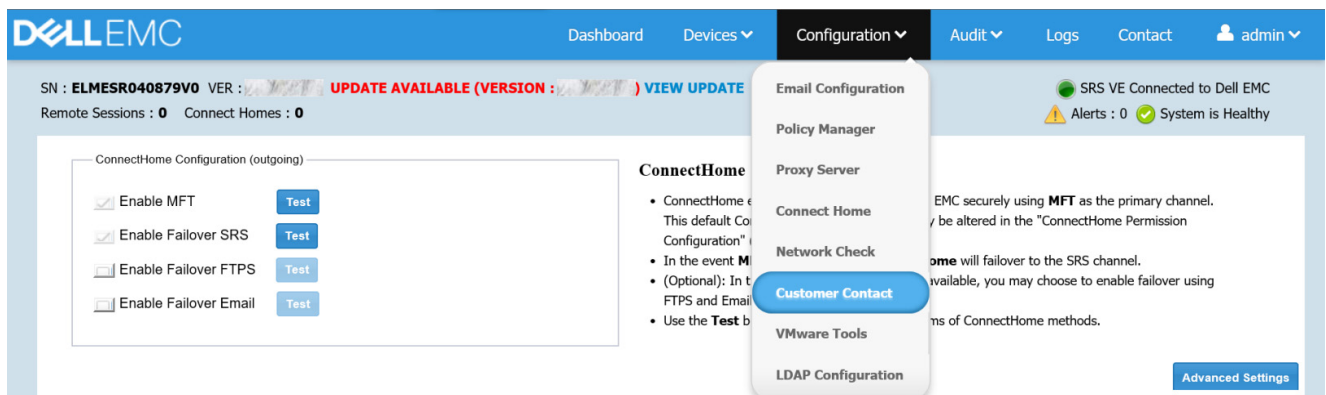


Figure 43 Accessing Connect Home

To enable Connect Home failover:

1. Select or deselect the Connect Home connection(s). The **Test** button becomes enabled and a success message appears, as shown in [Figure 44 on page 44](#).

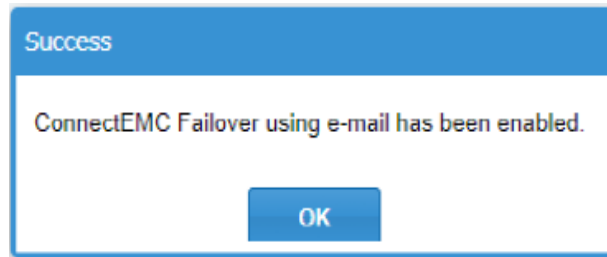


Figure 44 Success message for enabling failover using FTPS

2. Click **OK** and the success message window closes.
3. Click the corresponding **Test** button to test the connection to Dell EMC. If you are successful, a message appears, as shown in [on page 45](#).

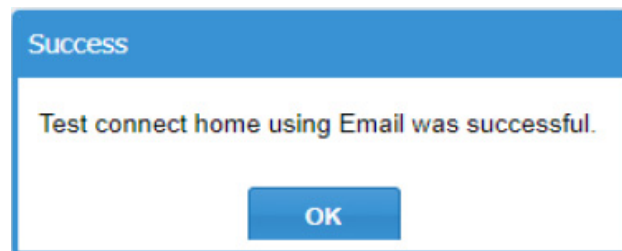


Figure 45 Testing Connect Home

4. Click **OK** to close the message box.

ConnectHome Notification configuration tab

For customers that utilize the Rest API for device to SRSv3 communications, they have the ability to receive files that are generated from the SRSv3 monitored device. However, and depending on configuration options, the customer may not receive the email. For example, in the Advanced Settings of the Connect Home Notification configuration tab, if the Device Model is **Default** and **Include Call Home Data** is selected, then the customer will receive the file.

ConnectHome Notification configuration

Device Model*:

Notification Email*: [Add Email](#)

Enable onSuccess Notification: ☒

Include Call Home Data: ☒

Email Format:

Email Subject:

Description:

[Apply Settings](#)

ConnectHome Notification

- By Selecting Include Call Home Data will send the event file XML that is generated to the customer.
- Only REST enabled products can leverage this feature and Non REST enabled products continue using the ConnectEMC app on the product for this feature.
- The **Default** settings for the Connect Home Email Notification is inherited from the Email Configuration section, any modifications to the Email Configuration settings will override the Connect Home Email notification settings.

Figure 46 Selecting Include Cal Home Data

If the Device Model is **Default** and **Include Call Home Data** is *not* selected but it is selected under the specific model type, then the file will **not** be received.

ConnectHome Listener configuration tab

On the ConnectHome Listener configuration tab, you can disable and enable any or all of the legacy call home services (HTTPS/FTP/Email (SMTP)) through the WebUI.

Note: You can only disable/enable each call home service one at a time. If you disable a call home service, then ensure that none of your devices use that method for call home or it will be impacted.

To disable:

1. Go to **Configuration > Connect Home**. The Connect Home Configuration page displays.

ConnectHome Configuration (outgoing)

☒ Enable MFT [Test](#)

☒ Enable Failover SRS [Test](#)

☐ Enable Failover FTPS [Test](#)

☐ Enable Failover Email [Test](#)

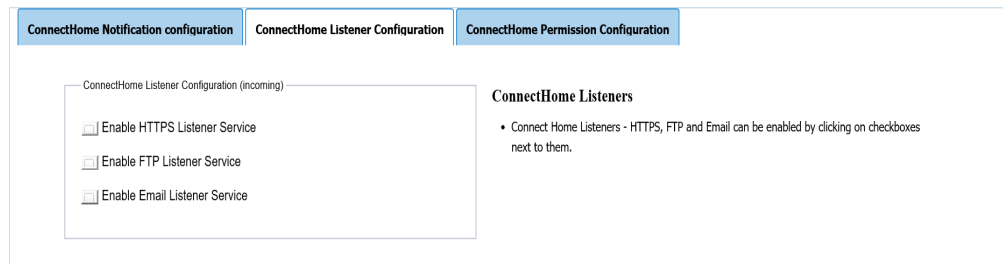
ConnectHome

- ConnectHome event information is sent to Dell EMC securely using **MFT** as the primary channel. This default ConnectHome mechanism can only be altered in the "ConnectHome Permission Configuration" (NOT Recommended).
- In the event **MFT** is not available, **Connect Home** will failover to the SRS channel.
- (Optional): In the event **MFT** and **SRS** are unavailable, you may choose to enable failover using FTPS and Email.
- Use the **Test** buttons available to check all forms of ConnectHome methods.

[Advanced Settings](#)

Figure 47 Connect Home Configuration page

2. Click **Advanced Settings**, and then select the **ConnectHome Listener Configuration** tab.



The image shows the 'ConnectHome Listener Configuration' page. It has three tabs: 'ConnectHome Notification configuration', 'ConnectHome Listener Configuration' (selected), and 'ConnectHome Permission Configuration'. Under the selected tab, there is a section titled 'ConnectHome Listener Configuration (incoming)' containing three checkboxes: 'Enable HTTPS Listener Service', 'Enable FTP Listener Service', and 'Enable Email Listener Service'. To the right, under the heading 'ConnectHome Listeners', there is a bullet point stating: 'Connect Home Listeners - HTTPS, FTP and Email can be enabled by clicking on checkboxes next to them.'

Figure 48 ConnectHome Listener Configuration page

3. Click on the applicable check box for HTTPS, FTP, or Email to disable any of the legacy call home services. A Success message box displays.

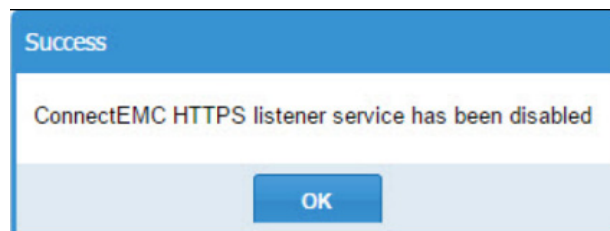


Figure 49 Success message box for disabling

4. Click **OK**. The message box closes and your selection is unchecked on the ConnectHome Listeners page.

To re-enable:

1. If you are not already in the ConnectHome Listeners page, then follow steps 1-2 above, and then select the applicable check box. The following Success message dialog box displays.

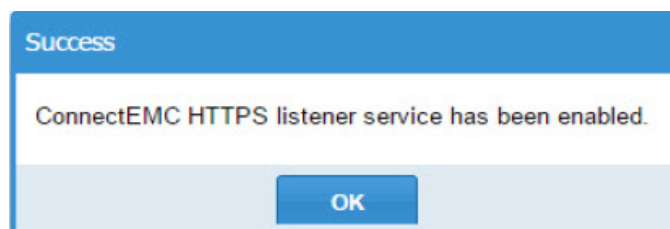


Figure 50 Success message box for enabling

2. Click **OK**. The message box closes and your selection is checked on the ConnectHome Listeners page.

Note: If the email configuration was skipped during provisioning or incorrect email information was entered, then the Connect Home email configuration is not enabled and a red warning message appears stating to validate the email configuration. Also, if the user has an invalid configuration, then Enable fail over email is unchecked and disabled.

ConnectHome Permission configuration tab

Once you are on this tab, note the following:

- ◆ **Disable Connect Home** check box displays. By default, the check box should not be selected.

ConnectHome Permission Configuration

☐ Disable Connect Home

ConnectHome Permission

- By enabling the **checkbox** ConnectHome will be disabled and the ConnectHome event information for managed devices as well as SRS will NOT be sent to Dell EMC using MFT and SRS as the primary and secondary channels. This is not a recommended configuration.
- Failover ConnectHome mechanisms will be utilized based on the options selected. If you disable ConnectHome and NO failovers are selected, ConnectHomes will not be sent back to Dell EMC.

Figure 51 ConnectHome Permission Configuration tab

- ◆ If you select the check box, then a pop-up message window opens with the following content, and the option to select **OK** or **Cancel**:

Are you sure you wish to disable this feature? By disabling this, none of the SRS managed devices will be able to send ConnectHomes back to Dell EMC

By disabling this, none of the SRS managed devices will be able to send ConnectHomes back to Dell EMC

Are you sure you wish to disable this feature?

OK Cancel

Figure 52 Confirmation message

- If you click **OK**, then the Success message displays, as shown in [Figure 53](#). Clicking **OK** again will close the Success message box.

Success

Permissions applied successfully.

OK

Figure 53 Success message

- If you click the **Cancel** button, then no changes are applied.
- ◆ Failover ConnectHome mechanisms will be utilized based on the options selected. If you disable ConnectHome and **no** failovers are selected, then ConnectHomes will **not** be sent back to Dell EMC.

MFT as the primary channel to transfer files

Managed File Transfer (MFT) is the default and primary channel for the Connect Home files. In the event MFT is not available, Connect Home will failover to the SRS channel.

On the Connect Home page, MFT is enabled with a grayed-out check box by default, as shown in [Figure 54](#).

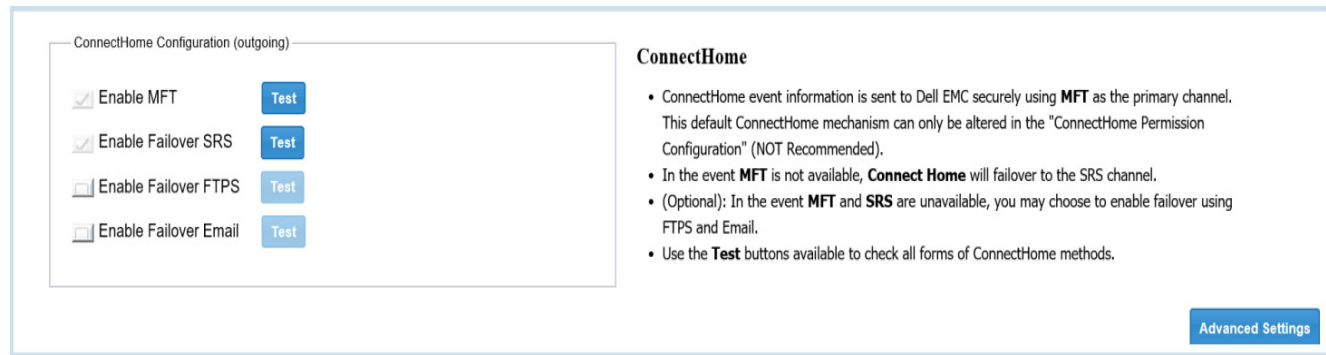


Figure 54 MFT enabled by default

Note the following:

- ConnectHome event information is sent to Dell EMC securely using MFT as the primary channel.
- (Optional): In the event MFT and SRS are unavailable, you may choose to enable failover using FTPS and Email.
- Use the test buttons available to check all forms of ConnectHome methods.

Network Check

The Network Check page provides the ability to check the network connectivity from SRS to all of the required Dell EMC servers.

IMPORTANT

You cannot provision until you complete the network tests.

To test the network:

- Click the **Run Test** button, as shown in [Figure 55 on page 48](#).

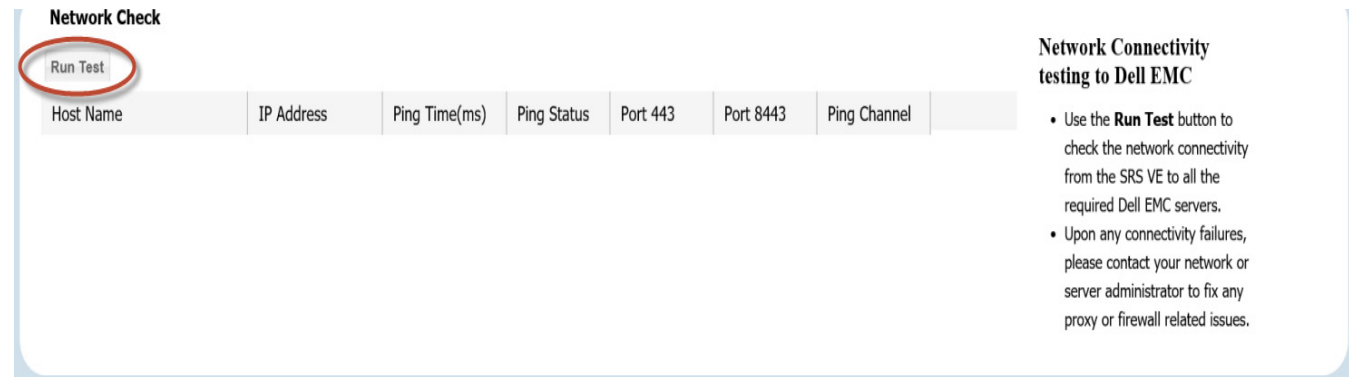


Figure 55 Network Check

After the Run Test is completed, the status of the hosts in the Dell EMC infrastructure is shown. Healthy connectivity is indicated by a green circle, as shown in [Figure 56 on page 49](#). Failed connections are indicated with red circles.

Network Check						
Run Test						
Host Name	IP Address	Ping Time(ms)	Ping Status	Port 443	Port 8443	Ping Channel
EMC Enterprise Servers						
esrs3stg.isus.emc.com	10.105.130.236	176			NA	Proxy not enabled
esrs3-corestg.isus.emc.com	10.105.130.237	82			NA	Proxy not enabled
EMC Global Access Servers						
esr3gdustg01-dbi.isus.emc....	10.105.21.66	132				Proxy not enabled
esr3gdustg02-dbi.isus.emc....	10.105.21.67	145				Proxy not enabled
esr3gdustg03-dbi.isus.emc....	10.105.21.68	0				Proxy not enabled

Network Connectivity testing to Dell EMC

- Use the **Run Test** button to check the network connectivity from the SRS VE to all the required Dell EMC servers.
- Upon any connectivity failures, please contact your network or server administrator to fix any proxy or firewall related issues.

Figure 56 Network Check Status

2. If there are any red circles, then you must investigate and correct any connectivity issues.

Customer Contact

The Customer Contact page provides the ability to add or edit contact information at any time.

To add or edit customer contact information:

1. Navigate to the **Configuration** tab and click on the **Customer Contact** link, as shown in [Figure 57 on page 49](#). The system retrieves the most current contact details from ServiceLink.

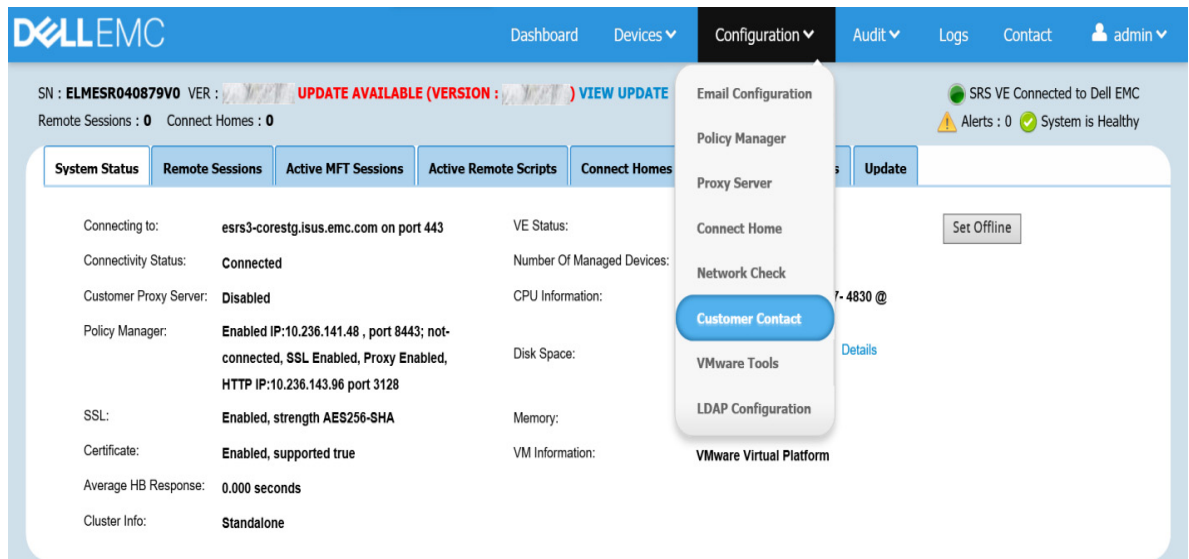


Figure 57 Accessing Configuration > Customer Contact

The following fields are required and are indicated by an asterisk, as shown in [Figure 58 on page 50](#):

- First Name
- Last Name
- Email
- Phone
- Company
- Dell EMC Contact

The screenshot displays the 'Customer Contact' page with two main sections: 'Primary Contact' and 'Technical Contact'. Each section contains a form with fields for First Name*, Last Name*, Email*, Phone*, Title, Company*, Dell EMC Contact, and Mobile. The 'Primary Contact' section has pre-filled values: First Name: Dell, Last Name: EMC, Email: catherine.aillon@dell.com, Phone: 111, Company: Dell. To the right of each form is a list of bullet points explaining the contact information's use. At the bottom right, there are 'Refresh' and 'Submit' buttons.

Primary Contact

- The information provided in this section will be used as customer contact by Dell EMC for the SRS VE.
- User can contact Dell EMC at later stage to update the primary contact information for the SRS VE.
- Dell EMC will reach Primary contact first regarding any SRS VE queries.

Technical Contact

- The information provided in this section will be used as customer contact by Dell EMC for the SRS VE.
- This is an optional step. User can contact Dell EMC at later stage to provide or update the Technical contact information for the SRS VE.
- Dell EMC will reach Technical contact regarding any SRS VE queries, if Primary contact is not available.

Refresh Submit

Figure 58 Customer Contact page

2. Add or edit the desired information.

Note: An asterisk indicates required information.

3. Click **Submit**. A pop-up window displays a success message, as shown in [Figure 59 on page 50](#).

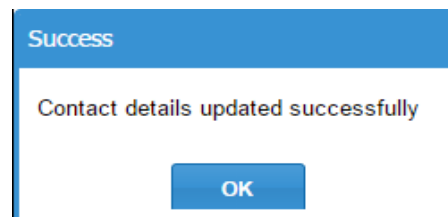


Figure 59 Success pop-up window

4. Click **OK**. The pop-up window closes and the newly updated information appears on the Customer Contact page.
5. Click the **Refresh** button to update ServiceLink with the edited information. Also, you can click the **Refresh** button at any time to retrieve the most updated information on ServiceLink.

VMware Tools

Note: This option is **not** available for Hyper-V or SRS Docker Edition (SRS DE).

VM Tools Support is enabled by default on the VMware-based image.

To enable/disable VMware Tools:

1. Navigate to the SRSv3 Web UI -> **Configuration** -> **VMware Tools**, as shown in [Figure 60](#).

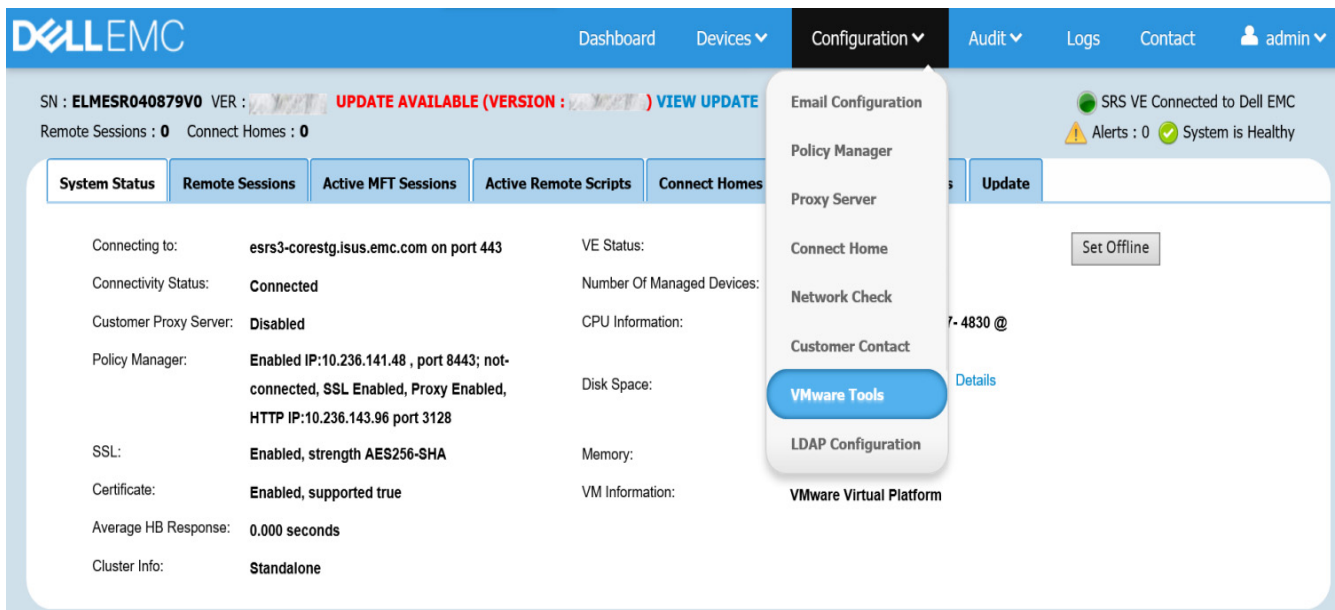


Figure 60 Selecting VMware Tools

2. Select **Enable** or **Disable**, and then click **Apply**, as shown in [Figure 61](#).

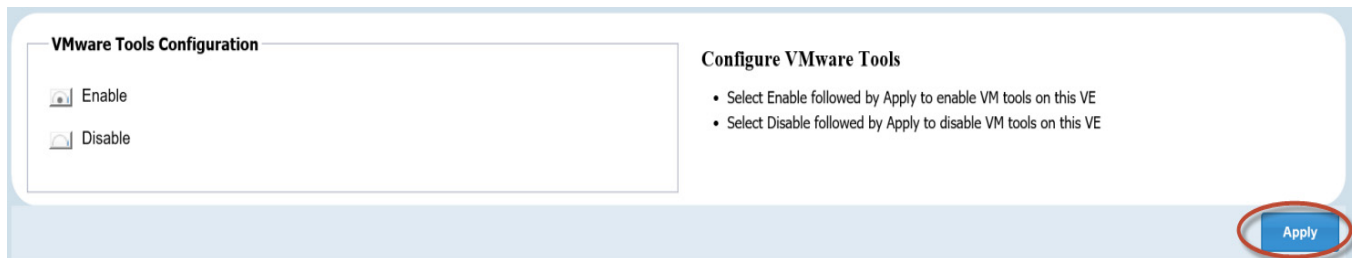


Figure 61 Enable/Disable VMware Tools

LDAP Configuration

After provisioning the VE, LDAP can be configured later as listed in Configuration menu.

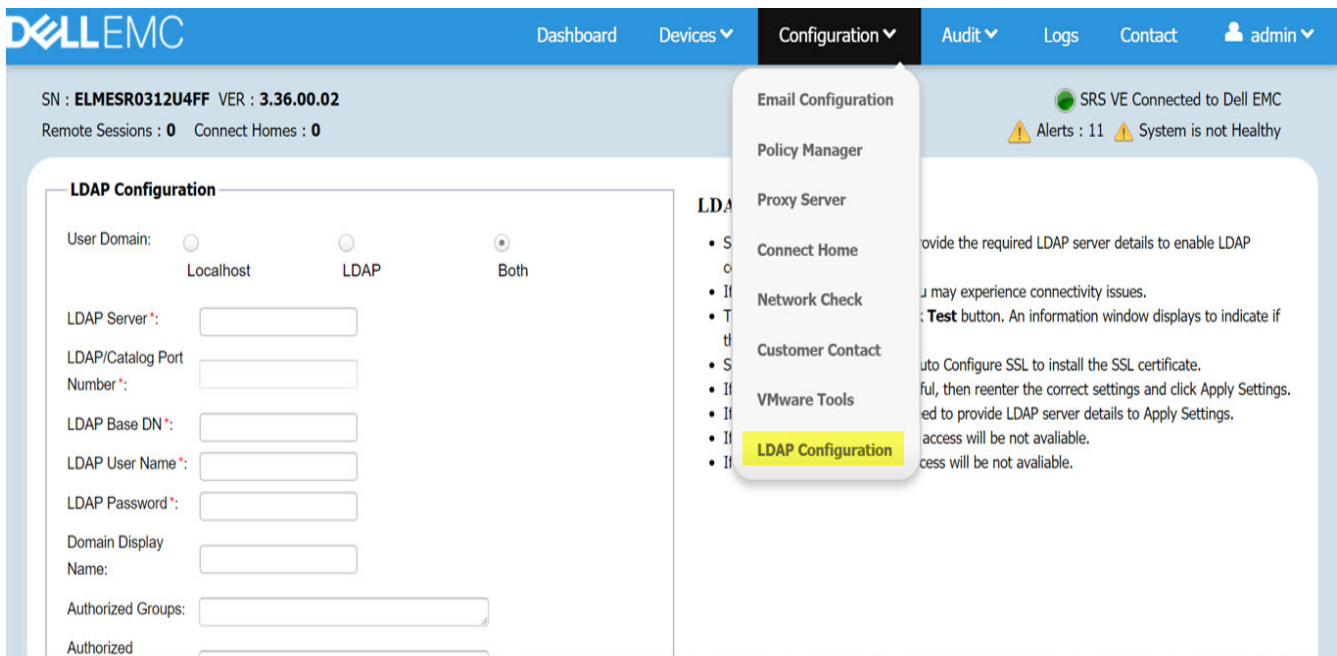


Figure 62 Selecting LDAP Configuration

- ◆ User Domain:
 - Localhost - Select this option to enable only Localhost login
 - LDAP - Select this option to enable only LDAP login
 - Both - Select this option to enable both Localhost and LDAP login
- ◆ LDAP Server - Customer LDAP server URL
- ◆ LDAP/Catalog Port Number - LDAP's port number or Catalog server port number
- ◆ LDAP Base DN - LDAP Base DN
- ◆ LDAP User Name - LDAP username with admin read permissions. Individual or group(s) users are allowed access to Web UI.
- ◆ LDAP Password - LDAP password
- ◆ Domain Display Name - Enter the domain name to be displayed on login
- ◆ Authorized Groups - Add the user group names separated by commas
- ◆ Authorized Individuals - Add the individual users separated by commas
- ◆ Enable SSL - If the user wants to enable the SSL certificate, then check this option. SSL will be configured successfully when **Auto Configure SSL** is selected.
- ◆ Test - User clicks on **Test** to check whether the connection is successful
- ◆ Apply Settings - User clicks on **Apply Settings** to configure the LDAP login

NOTICE

When changes are made to the LDAP configuration, the user must logout of SRS and log back in for the changes to be applied.

The screenshot shows the 'LDAP Configuration' page in the Dell EMC SRS Web UI. The page has a blue header with navigation links: Dashboard, Devices, Configuration, Audit, Logs, Contact, and a user profile for 'admin'. Below the header, there's a status bar showing 'SN : ELMESR0312U4FF VER : 3.36.00.02', 'Remote Sessions : 0', and 'Connect Homes : 1'. On the right, it says 'SRS VE Connected to Dell EMC' with a green status icon and 'Alerts : 10 System is not Healthy' with a yellow warning icon.

The main content area is titled 'LDAP Configuration' and contains two panels. The left panel has radio buttons for 'Localhost', 'LDAP', and 'Both'. Below these are input fields for 'LDAP Server', 'LDAP/Catalog Port Number', 'LDAP Base DN', 'LDAP User Name', 'LDAP Password', 'Domain Display Name', 'Authorized Groups', and 'Authorized Individuals'. There's also an 'Enable SSL' checkbox and an 'Auto Configure SSL' button. The right panel contains a list of instructions for LDAP configuration, including selecting the LDAP/BOTH option, checking port settings, testing the connection, enabling SSL, and applying settings. At the bottom right of the page are 'Test' and 'Apply Settings' buttons.

Figure 63 LDAP Configuration page

If the user configures both local host and LDAP, then after provisioning, they will see the Login page below:

Note: If the user logs in to LDAP with invalid credentials, after 3 invalid attempts, then the user's domain account will be locked.

The screenshot shows the 'Login' page in the SRS Web UI. The page has a light gray background. On the left, there's a 'Login' form with a blue header. Below the header is a light blue box with a note: 'The default user name for Local domain is admin (unless it was changed during VE setup)'. The form has three input fields: 'Domain' (a dropdown menu showing 'LDAP-corp'), 'User Name' (containing '@domain not required'), and 'Password' (empty). At the bottom of the form are two buttons: 'Login' (blue) and 'Cancel' (gray). On the right side of the page, there's a 'Login' section with a 'Note:' and instructions for Local and LDAP domains. The 'Note:' says 'For Local domain, please provide the administrator credentials that was set during the VE setup'. The instructions for LDAP say 'For LDAP domain, please provide your system/LDAP credentials'.

Figure 64 LDAP Domain Login Page

The user can check the service status of the LDAP Authorization service **esrsauthldap** in the dashboard below.

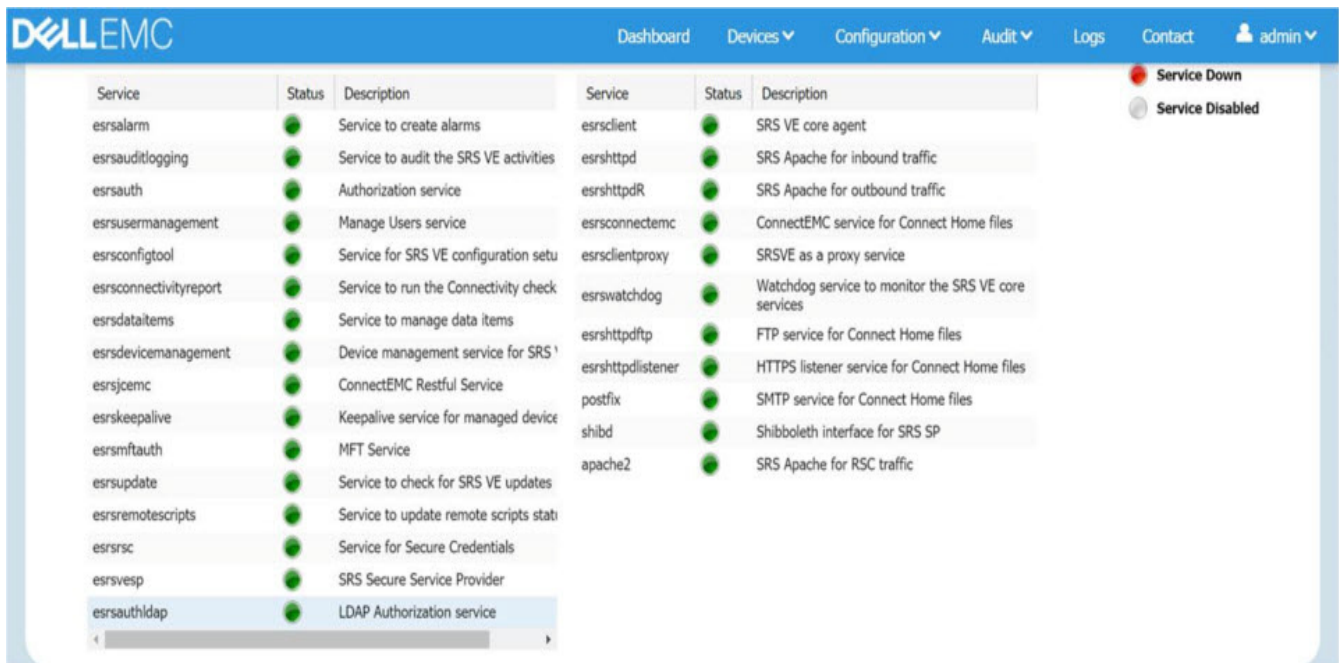


Figure 65 LDAP Authorization Service

Requirements not in scope

- ◆ This feature is not applicable for VE version 3.36.00.10 and below
- ◆ LDAP configuration is not applicable for other roles except admin
- ◆ eVE is out of scope
- ◆ Ability to define LDAP search at root levels (e.g. corp.emc.com) versus having to specify a specific OU)

LDAP User Management

The **LDAP User Management** tab is added to maintain the LDAP users/groups. The user can search and add individual users and groups to the LDAP configuration using this tab.

On this tab, the users will see the existing LDAP Users and LDAP Groups with the following details:

- ◆ **LDAP Users:**
 - Email Address
 - User ID
 - First Name
 - Last Name
- ◆ **LDAP Group:**
 - Email Address

- Group ID
- Group Name

The screenshot displays the 'LDAP User Management' tab. At the top, there are search filters: 'Ldap Users' (a dropdown), 'Email ID' (a dropdown), 'Starts with' (a dropdown), and a search input field with the placeholder 'Type 4 characters for auto search'. Below these are 'Add', 'Remove', and 'Save Changes' buttons. The main content area is divided into two sections: 'LDAP Users' and 'LDAP Group'. The 'LDAP Users' section contains a table with the following data:

Email Address	User ID	First Name	Last Name
abhishek.kumar20@emc.com	kumara240	Abhishek	Kumar
sidhartha.sahu@emc.com	sahus14	Sidhartha Sekhar	Sahu
abhi_choksi@deli.com	abhi_choksi	Abhishek	Choksi

The 'LDAP Group' section contains a table with the following data:

Email Address	Group ID	Group Name
vengadirects@emc.com	Venga Directs	

At the bottom of the interface, there is an 'Email' dropdown, a 'Browse' button, an 'Import' button, a 'Download Sample' button, and an 'Export' button.

Figure 66 LDAP User Management tab

Adding or removing new user/group

To add a new user or group:

1. Select either **Ldap Users** or **Group Users** from the drop-down list.
2. Select the search criteria, based on which field the search has to be done.
 - If **Ldap Users** is selected, then the search can be done on the Email ID and User ID fields.
 - If **Group Users** is selected, then the search can be done on Group Email and Group ID fields.
3. Select either **Starts with**, **Contains**, or **Ends with**.
4. Enter a minimum of 4 characters for auto search.
5. Click **Add** to add the selected user or group from the search result.
6. Click **Save Changes**.

Note: Any modifications done to the user/group list will be saved only after clicking on this option. The message "Please click on Save Changes to apply the changes" will be displayed at the top of the page if any changes are made to the list.

7. To remove a user or group, follow the steps above but click **Remove** instead of **Add**.

Importing user/group

To add more users, instead of searching and adding the users one by one, you can enter all the user/group details in a CSV file (MS Excel) and then use the Import option in SRS to add all the users at once.

To import user/group:

1. Under **LDAP Group** section, select either **Email** or **ID**. User email and group email addresses can be added in the same file as well as user ID and group ID can be added in the same file.
2. Select a file using the **Browse** option. The **Import** button becomes enabled.
3. Click **Import**. All the valid users/groups will be added to the respective tables and the incorrect values will be downloaded in MS Excel so that user will be aware of users/groups not added.

Exporting user

Selected users and groups can be exported to CSV file format by using the respective drop-down list and clicking **Export**. An MS Excel spreadsheet will be downloaded for users to open and view.

If no users or groups are selected, by default all users and groups will be exported.

Requirements not in scope

The following requirements are not in scope for this release:

- ◆ This feature is not applicable for VE version 3.36 and below
- ◆ LDAP configuration is not applicable for other roles except admin
- ◆ eVE is out of scope

Audit

Audit information is available for Virtual Edition Audit (VE Audit), Connect Home Audit, and MFT Audit on the SRS Web UI.

Within the VE Audit, Connect Home Audit, and MFT Audit, you have the ability to search the audit log and to export it as an MS Excel file, as shown in [Figure 67 on page 57](#).

The screenshot shows the 'VE Audit' interface. At the top, there is a search filter section with fields for 'From Date', 'To Date', 'Service Name', 'Caller ID', 'Caller IP', 'Action', and 'Status'. A red circle highlights these search fields. Below the search fields is a table with the following columns: Date, Service Name, Caller ID, Caller IP, Action, and Status. The table contains 10 rows of audit data. At the bottom right, there is an 'Export' button, also highlighted with a red circle. The bottom of the interface shows pagination information: 'Page 1 of 100' and 'Displaying 1-10 of 104'.

Date	Service Name	Caller ID	Caller IP	Action	Status
02/18/2015 09:29:40 AM	esrskreepalive	admin	10.105.34.133	Banner Details	200
02/18/2015 05:24:49 PM	esrjpcmc	Internal Caller	10.105.34.133	Download Logs	200
02/18/2015 05:24:49 PM	esrjpcmc	Internal Caller	10.105.34.133	Download Logs	200
02/18/2015 05:24:35 PM	esrjpcmc	admin	10.105.34.133	Get Log Tree	200
02/18/2015 09:29:40 AM	esrconnectivityreport	admin	10.105.34.133	Service Status	200
02/18/2015 09:29:40 AM	esrconnectivityreport	admin	10.105.34.133	Service Status	200
02/18/2015 11:25:15 AM	esrconfigtool	admin	10.105.34.133	Get Registration	200
02/18/2015 09:29:40 AM	esrconfigtool	admin	127.0.0.1	Get Agent Connectivity	200
02/18/2015 09:29:40 AM	esrconfigtool	admin	10.105.34.133	Agent Status	200
02/18/2015 09:29:40 AM	esrconfigtool	admin	10.105.34.133	Agent Status	200

Figure 67 Search and export capability

Archived audit data will be stored for one month and then gets deleted on the first day of the new month.

VE Audit

This section of Audit records the entire audit information regarding all of the activities done on SRS.

To access VE Audit, select **Audit > VE Audit**.

You can specify the filters in the text box for the following columns (as shown in [Figure 68 on page 58](#)):

- ◆ From Date
- ◆ To Date
- ◆ Service Name
- ◆ Caller ID
- ◆ Caller IP
- ◆ Action
- ◆ Status

VE Audit

From Date: To Date: Service Name: Caller ID:

Caller IP: Action: Status: [Filter](#)

Click on each record to get additional details.

Date	Service Name	Caller ID	Caller IP	Action	Status
02/19/2015 02:05:40 PM	esrsmftauth	admin	10.239.21.27	MFT UI File Audit upload	200
02/19/2015 02:05:09 PM	esrsmftauth	admin	10.239.21.27	MFT UI File Audit upload	200
02/19/2015 02:04:49 PM	esrsjcmc	admin	10.239.21.27	Call Home History	200
02/19/2015 02:03:40 PM	esrsjcmc	admin	10.239.21.27	Call Home History	200
02/19/2015 02:03:40 PM	esrsjcmc	admin	10.239.21.27	Call Home History	200
02/19/2015 02:03:36 PM	esrsjcmc	admin	10.239.21.27	Call Home History	200
02/19/2015 02:03:36 PM	esrsjcmc	admin	10.239.21.27	Call Home History	200
02/19/2015 02:03:31 PM	esrsjcmc	admin	10.239.21.27	Call Home History	200
02/19/2015 02:03:31 PM	esrsjcmc	admin	10.239.21.27	Call Home History	200
02/19/2015 01:18:13 PM	esrsjcmc	Internal Caller	10.239.21.27	Download Connecthome Audit	200

[Export](#)

Figure 68 SRSv3 Audit with IPV4 addresses

VE Audit

From Date: To Date: Service Name: Caller ID:

Caller IP: Action: Status: [Filter](#)

Click on each record to get additional details.

Date	Service Name	Caller ID	Caller IP	Action	Status
2018-02-28 4:51:16	esrconfigtool	admin	2620:0:170:961:1111:1111:1111:49	Get Device List and Rules	200
2018-02-28 4:50:53	esrsauth	admin	2620:0:170:961:1111:1111:1111:49	Agent Status	200
2018-02-28 4:50:52	esrsauth	admin	2620:0:170:961:1111:1111:1111:49	Get Managed Device List	200
2018-02-28 4:50:52	esrsauth	admin	2620:0:170:961:1111:1111:1111:49	Get Device Model	200
2018-02-28 4:50:51	esrsauth	admin	2620:0:170:961:1111:1111:1111:49	add site id	200
2018-02-28 4:50:44	esrsauth	admin	2620:0:170:961:1111:1111:1111:49	Get Proxy Configuration	200
2018-02-28 4:50:37	esrsauth	admin	2620:0:170:961:1111:1111:1111:49	Agent Status	200
2018-02-28 4:50:37	esrsauth	admin	2620:0:170:961:1111:1111:1111:49	Get Policy Mgr Details	200
2018-02-28 4:48:35	esrsauth	admin	2620:0:170:961:1111:1111:1111:49	get Asset Status	200
2018-02-28 4:48:35	esrsdevicemanagement	admin	2620:0:170:961:1111:1111:1111:49	Banner Details	200

[Export](#)

Figure 69 SRSv3 Audit with IPV6 addresses

Table 1 on page 58 displays some common status codes.

Table 1 Add Device Response Structure

Status Code	Description
200, 201	Request approved by Service Link
500	Failure

Connect Home Audit

This section of Audit records the entire audit information regarding the Connect Home activities on SRS.

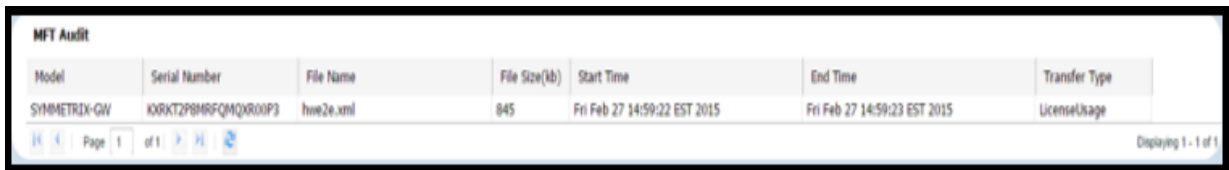
To access Connect Home Audit, go to **Audit > Connect Home Audit**.

You can specify the filters in the text box for the following columns:

- ◆ From Date
- ◆ To Date
- ◆ File Name
- ◆ Transport Type
- ◆ Notification Type
- ◆ Result
- ◆ Success
- ◆ Failure

MFT Audits

This section of Audit records the entire audit information regarding the MFT activities on SRS. [Figure 70 on page 59](#) displays an example of the **MFT Audit** tab.



Model	Serial Number	File Name	File Size(kb)	Start Time	End Time	Transfer Type
SYMMETRIX-GW	XXRKT2P8MRFMQXR00P3	hmc2e.xml	845	Fri Feb 27 14:59:22 EST 2015	Fri Feb 27 14:59:23 EST 2015	LicenseUsage

Figure 70 MFT Audit Logs

Logs

The **Logs** section in the SRS Web UI has the following logs, as shown in [Figure 71 on page 60](#):

- ◆ ConnectEMC
- ◆ SRS REST Services
- ◆ SRS Agent
- ◆ Apache



Figure 71 Download Logs

Each of the log folders has all of the related log files present in it. You can download any one of these log files.

You can click on the plus icon (+) or double-click each folder to see the log files, as shown in [Figure 72 on page 61](#).

You can also click on any log file to start the download process.



Figure 72 Expanding the log folders

Logging out

To log out of the Admin, select **Admin > Logout**, as shown in [Figure 73 on page 62](#). The SRS home page appears, as shown in [Figure 74 on page 62](#).



Figure 73 Logging out of Admin

Logging out of the application returns you to the SRS home page. Further access requires you to log back in using the **Login** option in the top navigation bar, as shown in [Figure 74 on page 62](#).

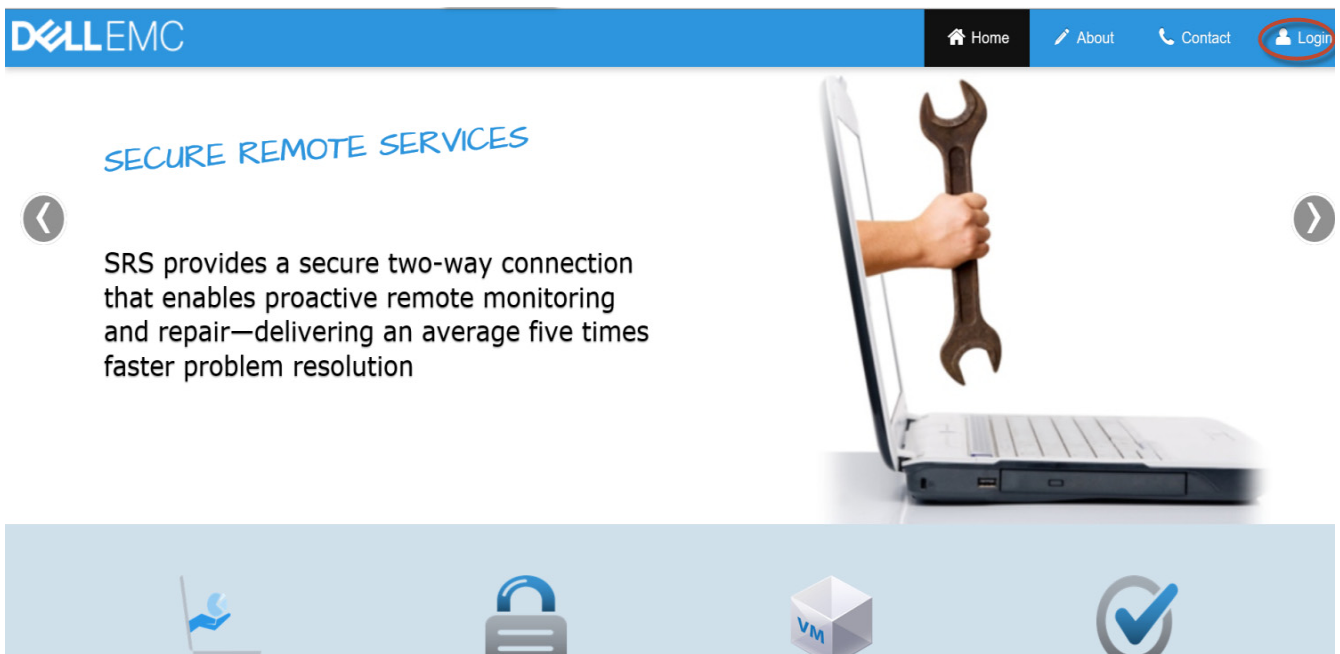


Figure 74 SRSv3 home page

Changing the password using the Web UI

This section details how to change your existing password through the Web UI when you already know your current password. Note that you must log in as Admin to perform this task; you will not be able to perform this task if you log in as root.

Changing the password

To change the password, the Admin user performs the following steps:

1. Log on to the SRS v3.0x Web UI page.
2. Select the **admin** tab.
3. Click **Change Password**. The Change Password page displays with the following password specifications:

Note: All special characters **except** single and double quotes are permitted in the password.

- Be 8 or more characters in length, with a maximum of 16 characters.
- Contain at least one numeric character.
- Contain at least one uppercase and one lowercase character.
- Contain at least one special character such as ~ ! @ # \$ % ^ & * () - _ = + [] { } ; < > .
- Use a password that does not match the previous password.
- Do **not** use special characters ' (single quote) and " (double quotes) as part of the password.

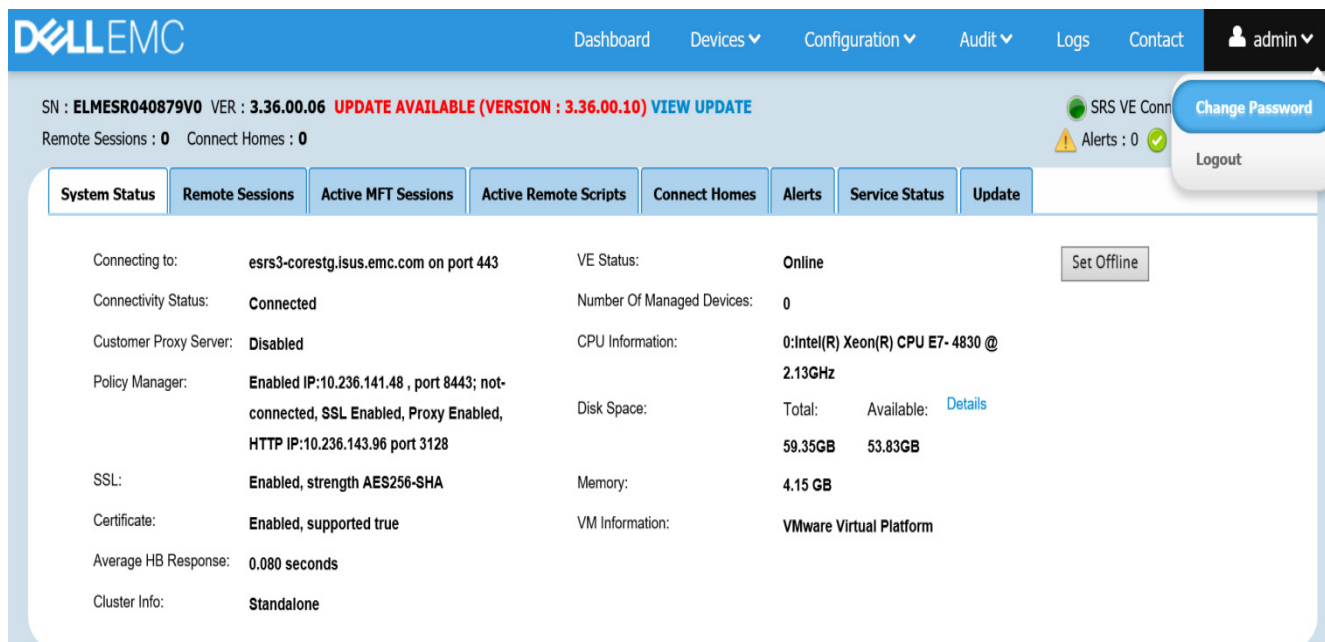


Figure 75 Selecting *Change Password*

4. In the Change Password page, in the appropriate text boxes, type the current password, the new password, and then confirm the new password.

5. Click **Submit**. If the password meets the required specifications, then a success message appears.
6. In the success message window, click **Ok**. The window closes.

Setting password expiration date

Admin account users can set the password expiration date in the Admin tab of the SRSv3 Web UI. There is an option to set a time, in days, for the Admin account password to expire.

The system will send a warning message if the password is about to expire. It will also prompt the user to change the password upon login if the password has expired.

To change the password expiration date:

Note: By default, passwords will never expire and the change password setting is set to "0" (forever).

1. Navigate to the SRSv3 Web UI-> **admin** -> **Change Password**, as shown in [Figure 76](#). The Change Password page appears.

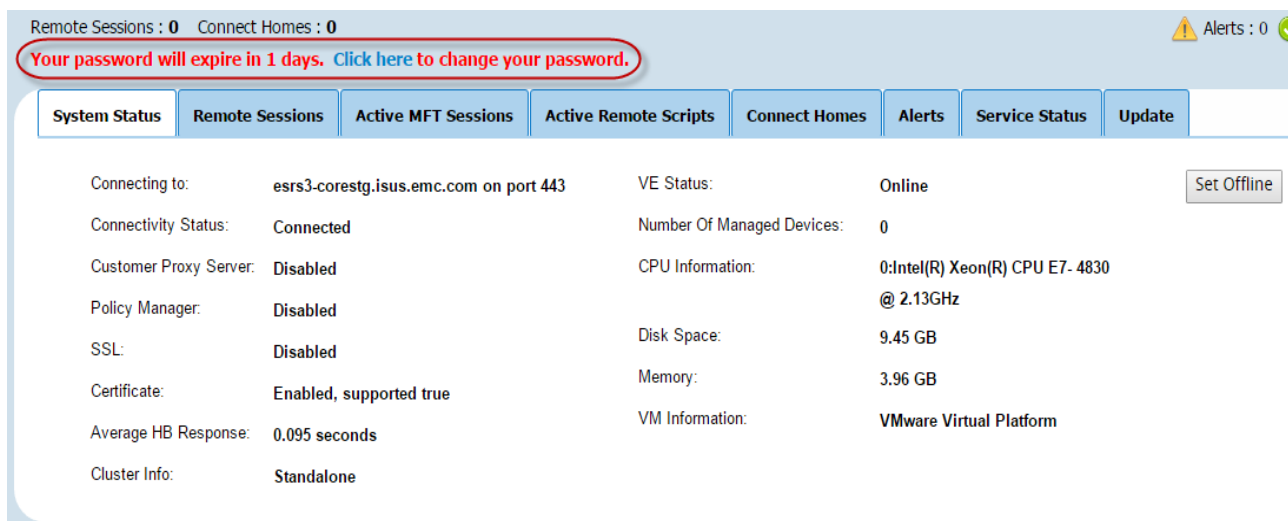


Figure 76 Select *Change Password*

2. In the Change Password page, enter the required information, indicated by a red asterisk, as shown in [Figure 77](#).

Note: Admin users will be able to enter a value for how many days will pass before the user needs to reset the password. The available date range is “0-365”. A value of “0” will designate that the password will never expire.

Change Password

User Name:

Current Password *:

New Password *:

Confirm New Password *:

Password Expiry (in days) *:

Password Specification

- Be 8 or more characters in length, with a maximum of 16 characters.
- Contain at least one numeric character.
- Contain at least one uppercase and one lowercase character.
- Contain at least one special character such as ` ~ ! @ # \$ % ^ & * () - _ = + [] { } ; < >
- Do NOT use Special characters / ? : , . | \ ' and " as part of the password.
- Use a password that does not match the previous password.
- New password needs to be set to update the password expiry.
- Valid Password Expiry range is 0-365 days, with 0 being never expire.

Submit

Figure 77 Change Password page

3. When you are done entering the required information, click **Submit**. A confirmation message appears, as shown in [Figure 78](#).

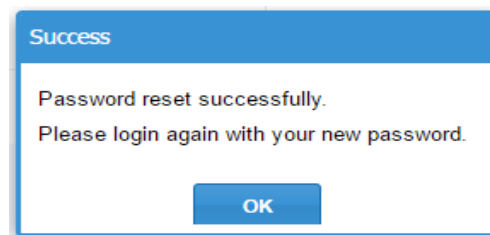


Figure 78 Password reset successfully message

4. Click **OK**. The message box closes and the SRS home page opens.
5. On the SRS home page, log on again with your new password. This takes you back to the main Admin page.

Note: A text field banner comes up each time the user logs in for the last 10 days before the password will need to change, as shown in [Figure 79](#). You can use the [Click here](#) link in the text field banner to change your password.

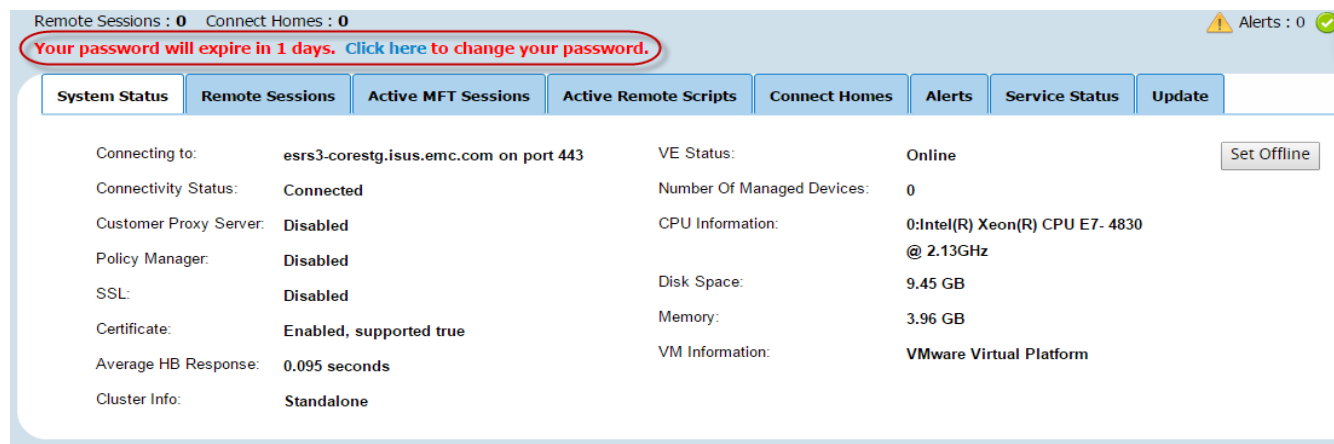


Figure 79 Password notification banner

6. If the password has expired, there will be a different text banner stating “Password is expired. Please change your password”. You will be directed to the change password page, as shown in [Figure 80](#). You can follow the same steps to change the password expiration date.

The screenshot shows the 'Change Password' page. On the left, there's a form with the following fields: 'User Name' (pre-filled with 'admin'), 'Current Password *', 'New Password *', 'Confirm New Password *', and 'Password Expiry (in days) *' (set to 0). On the right, under the heading 'Password Specification', there's a list of requirements:

- Be 8 or more characters in length, with a maximum of 16 characters.
- Contain at least one numeric character.
- Contain at least one uppercase and one lowercase character.
- Contain at least one special character such as `~!@#\$%^&*()-_+=[]{};<>`
- Do NOT use Special characters / ? : , . | \ ' and " as part of the password.
- Use a password that does not match the previous password.
- New password needs to be set to update the password expiry.
- Valid Password Expiry range is 0-365 days, with 0 being never expire.

A blue 'Submit' button is located at the bottom right of the page.

Figure 80 Change Password page

Exporting to CSV Managed Devices

Note: This section only applies to Admin users. To use the command line version of this tool, see the Appendix.

Using the Configuration tool, you can export the managed devices to a CSV formatted file that would contain the device type, serial number, and IP address.

Procedure

To export the managed devices:

1. Navigate to the Web UI Manage Device page.
2. To export all managed devices in CSV file format, click the **Export** button.

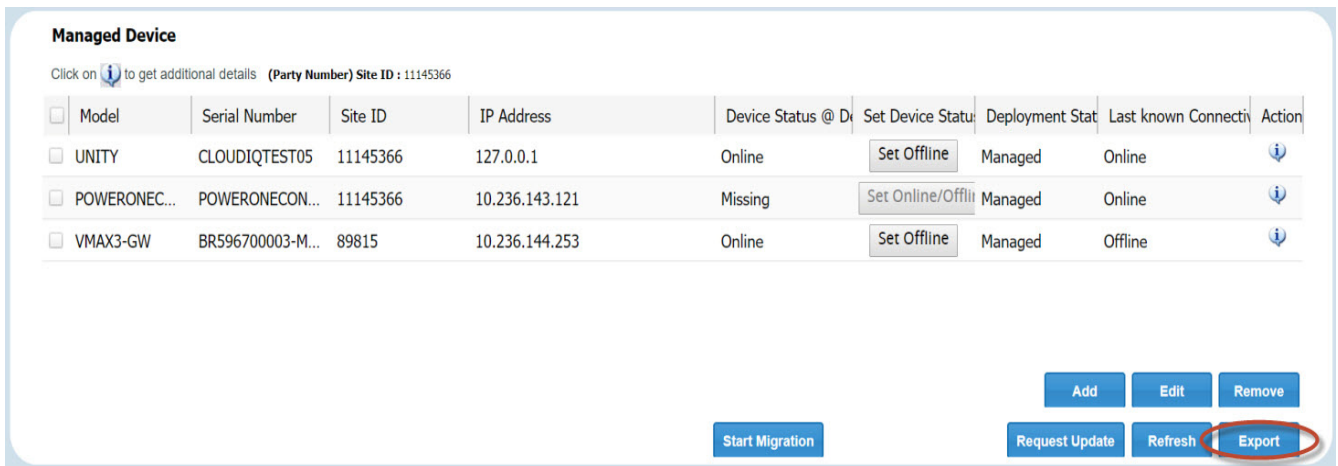


Figure 81 Manage Device page

The CSV formatted file complies with the following naming convention:

ManageDeviceListYearMonthDateTimeStamp

For example, a file exported on June 24, 2014 at 2:33:06 p.m. will be:

ManageDeviceList20140624023306

The CSV formatted file contains, at a minimum, the following information:

- Device Type
- Serial Number
- IP Address

Note: The CSV formatted file will not export the managed devices that have the following status: Pending Approval, Add, Pending Add, Edit, Pending Edit, and Remove.

Once the user clicks **Export**, the data is exported to an Excel spreadsheet, as shown in [Figure 82](#), where the user can sort, copy, paste, etc.

Model	Serial Number	IP Address	Device Status @ EMC	Deployment Status	Last Known Connectivity Status
BETA1-GW	BETA1DEV1-11	10.236.143.121	Online	Managed	Online

Figure 82 Excel spreadsheet

CHAPTER 3

Server Maintenance

This section includes a variety of server maintenance procedures, including backup procedures.

Dell EMC strongly recommends that you back up your data on the SRS server. It is your responsibility to perform backups and to ensure that the servers can be restored through the use of the backup data. Either an image backup or a data file backup is satisfactory.

Topics in this section include:

- ◆ [Service preparation for SRSv3.....](#) 70
- ◆ [Backup guidelines and procedures](#) 71

Service preparation for SRSv3

This section describes steps that need to be taken prior to performing maintenance procedures on the SRS server.

SRSv3 server

Follow the procedures in this section before performing maintenance on the SRS server.

Logging preparation

SRS regularly cycles (or rotates) log files by removing the oldest ones from your system and creating new log files. These log files get rotated based on the file size, which is set to 5 MB by default and can be modified to a different size in the xgLogFile.xml configuration file. By default SRS keeps up to 5 old files before cycling them, and this number can also be set as shown in the xgLogFile.xml config file.

1. Navigate to the xgLogFile.xml directory.

```
cd ../Gateway/ESRS
```

2. Run the following command:

Note: This step **must** be formed by logging in to the OS Shell of the SRS with an SSH Client such as PuTTY.

```
[root@185rhel62d ESRS]# more xgLogFile.xml
<?xml version="1.0" standalone="yes"?>
<PersistedData moduleName="xgLogFile" TerseType="1">
  <i>2</i>
  <PointerList>
    <EFileSpec>
      <s>"KernelLog"</s>
      <s>"</s>
      <s>"EKernel<!--E42:Event.Sequence-->.log"</s>
      <i>5242880</i> // size of log file
      <i>5</i> // number of log files to keep
      <i>0</i>
      <i>1</i>
      <i>1</i>
      <i>0</i>
      <s>"</s>
    </EFileSpec>
  </PointerList>
</PersistedData>
```

Note: You or your system administrator may decide that other adjustments should be made. For example, the maximum log size should be increased if overwriting is not allowed by corporate policy.

Backup guidelines and procedures

You must prepare backup procedures to protect SRS servers in case of hardware failure, software failure, or data corruption.

Specific procedures depend on your:

- ◆ SRSv3 site architecture
- ◆ Backup software
- ◆ Existing procedures

and possibly other conditions. Consult your system and network administrators.

CHAPTER 4

Virtual Lifecycle Management - Updating

This chapter provides information about updating SRS software. Topics include:

- ◆ Overview 74
- ◆ Update checks 74
- ◆ Downloading and applying updates 75
- ◆ Upgrading Docker 77

Overview

Software updates and enhancements must be provided for the continuous support of SRS. The Virtual Lifecycle Management (VLM) helps to provide updates and new releases via a patch for product support for the customers.

Update checks

Whenever the SRS v3 of version 3.xx is connected, the SRS v3.xx will automatically check with the Dell EMC back office daily to see if there is a new SRS v3.xx version available for updating. If the SRS v3.xx fails to check for the update on a specific day, the next check will happen on the next day at the specific time.

When a new version of SRS v3.xx is available for download, the SRS v3.xx sends an email notification to the customer's email address provided in the 'Notification Email(s)' field shown in [Figure 83, "Email Configuration Tab."](#)

The screenshot shows the 'Email Configuration' tab within a three-step process: Registration, Provisioning, and Configuration. The 'Email Configuration' section contains the following fields and options:

- Email Server:** mailhub.lss.emc.com
- Port:** 25
- Sender Email:** esrs_support@emc.com
- Notification Email(s):** shashikala.j@emc.com (This field is circled in red in the original image)
- ☒ Enable onSuccess Notification
- ☒ Enable Device Connection Notification
- Notification settings:**
 - To send notification e-mails and Connect Home files (if enabled), provide e-mail server and its port details in the E-mail Server and Port text boxes.
 - Provide an email address in the **Sender Email** section which can be used as FROM address in the email notifications.
 - Provide an email address in the **Notification Email** section which will be used as recipients for any critical failure event notifications and for successful events (if configured).
 - Use Test option to send a test E-mail
- Test** button
- Submit & Go to Policy Manager** button

Figure 83 Email Configuration Tab

The text UPDATE AVAILABLE (VERSION #) along with the link VIEW UPDATE is displayed next to the Serial Number and Version information in the banner at the top of the SRS v3.xx Dashboard as shown in [Figure 84 on page 75](#).

The screenshot shows the SRS v3.xx Dashboard. At the top, the banner displays the Serial Number (SN: ELMESR040879V0) and Version (VER: 3.36.00.06). A red banner indicates "UPDATE AVAILABLE (VERSION: 3.36.00.10)" with a "VIEW UPDATE" link circled in red. The dashboard includes tabs for System Status, Remote Sessions, Active MFT Sessions, Active Remote Scripts, Connect Homes, Alerts, Service Status, and Update. The System Status tab is active, showing various system metrics and a "Set Offline" button.

Connecting to:	esrs3-corestg.isus.emc.com on port 443	VE Status:	Online	Set Offline
Connectivity Status:	Connected	Number Of Managed Devices:	0	
Customer Proxy Server:	Disabled	CPU Information:	0: Intel(R) Xeon(R) CPU E7- 4830 @ 2.13GHz	
Policy Manager:	Enabled IP:10.236.141.48 , port 8443; not-connected, SSL Enabled, Proxy Enabled, HTTP IP:10.236.143.96 port 3128	Disk Space:	Total: 59.35GB Available: 53.82GB	Details
SSL:	Enabled, strength AES256-SHA	Memory:	4.15 GB	
Certificate:	Enabled, supported true	VM Information:	VMware Virtual Platform	
Average HB Response:	0.081 seconds			
Cluster Info:	Standalone			

Figure 84 Update Available Notice on the SRS v3.xx Dashboard

Downloading and applying updates

Follow these steps to download and apply updates:

1. When you log on to the SRS Web UI, the dashboard will show a message that a new version is available for update.
2. Navigate to the Update tab. The current running version and the latest available version appears on the Update tab, as shown in [Figure 85 on page 75](#).

The screenshot shows the SRS v3.xx Dashboard with the "Update" tab selected. It displays the "Current Running Version" (3.36.00.06) and the "Latest Available Version" (3.36.00.10). A "Download" button is visible. A text box on the right explains that SRS updates keep the system current and secure with the latest OS and application updates, and lists the steps for updating: 1.) Downloading the latest update, and then 2.) Applying the update.

Current Running Version:	3.36.00.06
Latest Available Version:	3.36.00.10

[Download](#)

SRS updates keep the system current and secure with the latest OS and application updates.

Updating the existing software consists of:

- 1.) Downloading the latest update, and then
- 2.) Applying the update

Figure 85 Update tab

3. Click **Download** to start the download process of the patch.
4. Leave the Web UI idle for around 20 minutes, while the download process is in progress.
5. Log on again to the Web UI and navigate to the Update page and validate that the patch is downloaded.

6. Click **Apply** to run and apply the patch for the upgrade, as shown in [Figure 86 on page 76](#). Status pop-up window appears.

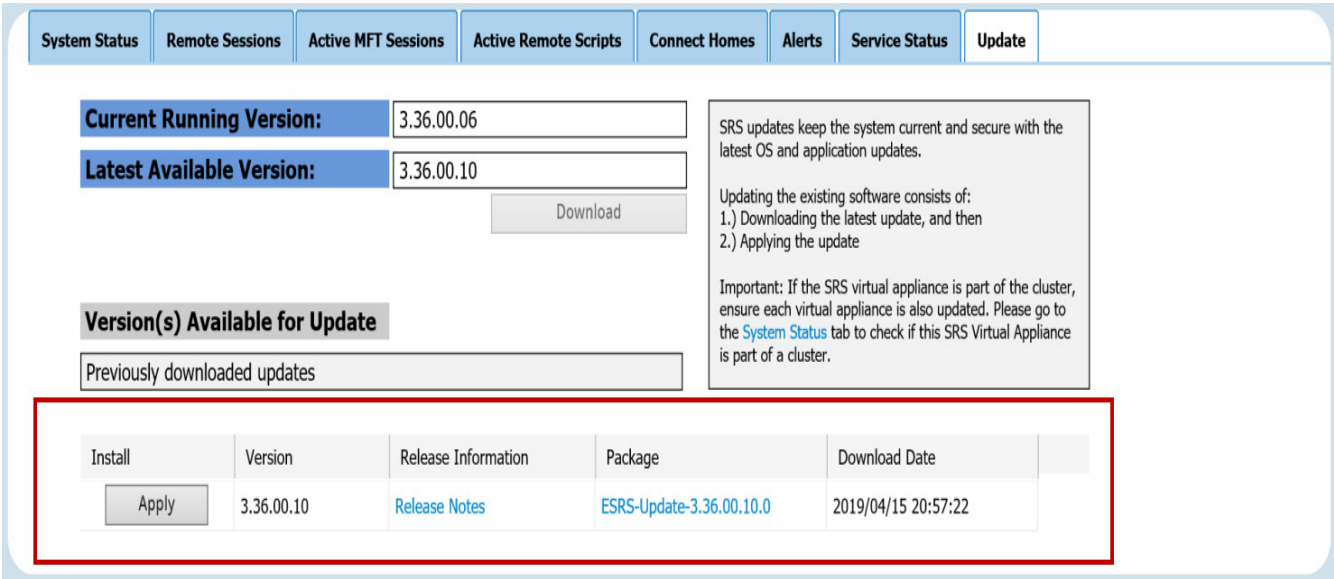


Figure 86 Clicking *Apply*

7. In the status pop-up window, click **Yes, Apply Update**, as shown in [Figure 87 on page 76](#).

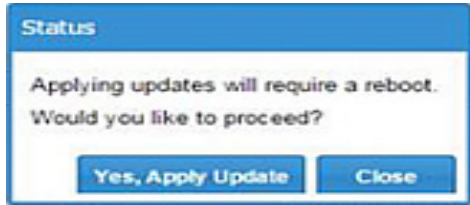


Figure 87 Applying Update

While applying updates, the following pop-up status message appears:

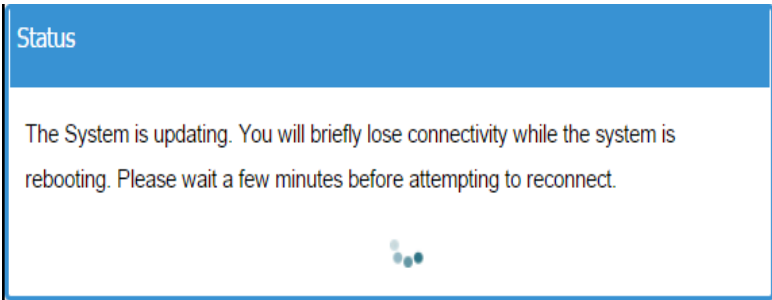


Figure 88 Pop-up status message

8. After applying the patch, SRS reboots after some time. An Update in Progress status bar on the Web UI initially appears, as shown in [Figure 89 on page 77](#), but later it will only show the static content as it cannot communicate to SRS once the SRS reboot process had started.

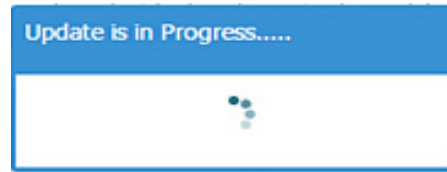


Figure 89 Update in progress

9. Wait for approximately 20 minutes, and then log on again to the Web UI once the SRS is rebooted.
10. Validate if the version has changed, as shown in [Figure 90 on page 77](#).

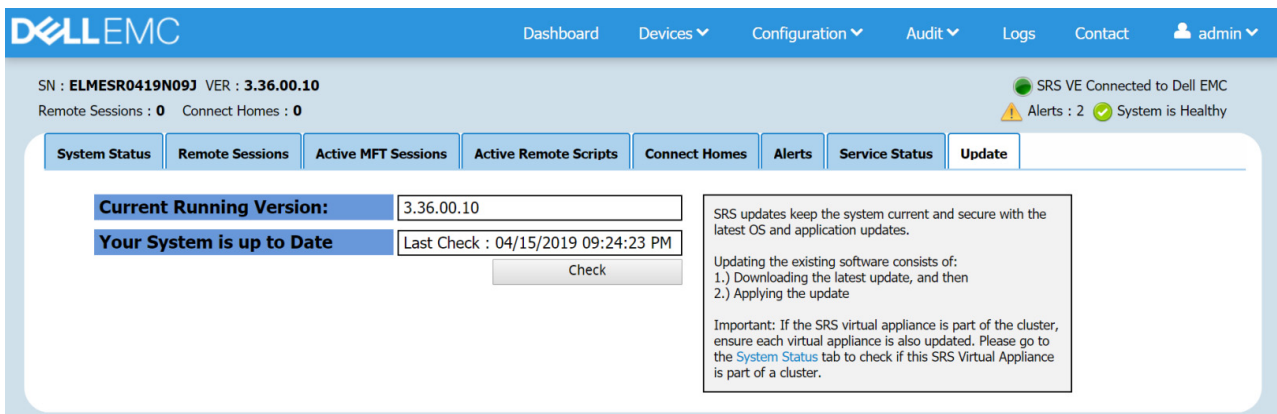


Figure 90 Validating update

Upgrading Docker

To upgrade SRS DE:

1. Download the latest SRS Docker Edition (SRS DE) for Linux on Dell EMC Online Support and copy to the Linux server running Docker:

<https://support.Dell EMC.com>

2. To change the permission of the installer, use the following chmod command example:

```
chmod +x ESRsde-3.xx.00.01.bin
```

3. Execute the upgrade using the following command example:

```
./ESRsde-3.xx.00.01.bin --upgrade
```

The command will check the following prerequisites, and proceed with the upgrade:

- Disk space availability, must be at least 64 GB

- Docker runtime
 - Ports 21, 25, 443, 9443, and 8118 are free
 - IP address is valid
4. Follow the instructions on the prompt to complete the upgrade.

During the upgrade, the installer will request a password to be set for the root account of SRS.

Note: This is **not** the root account of the host.

CHAPTER 5

Troubleshooting

This chapter provides information about troubleshooting unexpected SRS service events. Topics include:

- ◆ [Resetting the Web UI administrator user password](#) 80
- ◆ [Service commands and debugging](#) 82
- ◆ [Unzipping files using WinZip.....](#) 85

Resetting the Web UI administrator user password

Prerequisite

You must have **root** console access to the SRSv3 in order to reset the Web UI admin password.

Procedure

To reset the Web UI administrator password:

1. Log in to the VM console where the SRSv3 is installed, using your root credentials, or connect with an SSH client.
2. Navigate to the directory: `cd /opt/ESRS/webuimgmt-util`.
3. Execute the script `./passwordAdmin.sh`. You are prompted to reset the password for the Web UI admin user.

Note: The script auto detects the Web UI administrator user name, whether you use the default user name of admin or have selected a different user name for the Web UI.

4. Type the new password.

Note: Password reset will fail if the new password is not compliant with the password policy. For password requirements, refer to the [“Password specifications” on page 81](#).

5. Reenter the new password. The text “confirm the new password to be set for the user admin” appears, as shown in [Figure 91 on page 80](#).

```
esrsveP226:/opt/esrs/webuimgmt-util # pwd
/opt/esrs/webuimgmt-util
esrsveP226:/opt/esrs/webuimgmt-util # ./passwordAdmin.sh

*****
*****Password Reset Util*****
*****
-----Password Specifications-----
1. Be 8 or more characters in length, with a maximum of 16 characters
2. Contain at least one numeric character
3. Contain at least one uppercase and one lowercase character
4. Contain at least one special character such as ` ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } ; <
5. Do not use special characters [ ? : , . | \ ] and [ ] as part of the password
-----
Provide the password to be set for the user admin:Testpassword@123
Confirm the new password to be set for the user admin:Testpassword@123
Password has been successfully reset for the user admin
esrsveP226:/opt/esrs/webuimgmt-util #
```

Figure 91 Confirming the new password

6. At the prompt, reenter the password. If you are successful, then a success message appears. If instead you receive an error message, then check your password specifications and reenter your new password.

After successfully changing the password, the root user will be able to log in to the SRS Web UI with the new password.

Password specifications

IMPORTANT

Do not use special characters ' (single quote) and " (double quotes) as part of the password, as shown in the command/script example in [Figure 92 on page 81](#).

Password specifications **must**:

- ◆ Be 8 or more characters in length, with a maximum of 16 characters.
- ◆ Contain at least one numeric character.
- ◆ Contain at least one uppercase and one lowercase character.
- ◆ Contain at least one special character such as ' ~ ! @ # \$ % ^ & * () - _ = + [] { } ; < > .
- ◆ Represents a password that does not match the previous password.
- ◆ **Does Not** use special characters / ? : , . | \ ' and " .

```
esrsveP226:/opt/esrs/webuimgmt-util # pwd
/opt/esrs/webuimgmt-util
esrsveP226:/opt/esrs/webuimgmt-util # ./passwordAdmin.sh

*****
*****Password Reset Util*****
*****
-----Password Specifications-----
1. Be 8 or more characters in length, with a maximum of 16 characters
2. Contain at least one numeric character
3. Contain at least one uppercase and one lowercase character
4. Contain at least one special character such as ` ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } ; < >
5. Do not use special characters / ? : , . | \ ' and " as part of the password
-----
*****
*****

Provide the password to be set for the user admin:Testpassword@123

Confirm the new password to be set for the user admin:Testpassword@123

Password has been successfully reset for the user admin
esrsveP226:/opt/esrs/webuimgmt-util #
```

Figure 92 Password reset

Service commands and debugging

Syntax to stop and start status check for core services

Table 2 on page 82 summarizes the syntaxes to use when performing stop and start status checks of the core services.

Table 2 Syntax Description and Command

To check the status of the service	<code>service <servicename> status</code>
To stop the service	<code>service <servicename> stop</code>
To start the service	<code>service <servicename> start</code>
To restart the service	<code>service <servicename> restart</code>

```
esrssecurity:/opt/esrs/gateway # service esrsclient status
Checking for service ESRS Client: running
esrssecurity:/opt/esrs/gateway # service esrsclient stop
Shutting down ESRS Client: done
esrssecurity:/opt/esrs/gateway # service esrsclient start
Starting ESRS client: done
esrssecurity:/opt/esrs/gateway # service esrsclient restart
Shutting down ESRS Client: done
Starting ESRS client: done
esrssecurity:/opt/esrs/gateway # service esrsclient status
Checking for service ESRS Client: running
esrssecurity:/opt/esrs/gateway #
```

Figure 93 Status check examples

Core service names

The core service names used are:

- ◆ ESRSclient
- ◆ ESRShttpd
- ◆ ESRShttpdR
- ◆ ESRSconnectEMC
- ◆ ESRSclientproxy
- ◆ ESRSwatchdog
- ◆ ESRShttpdftp
- ◆ ESRShttpdlistener
- ◆ postfix

The status of the core services can be found in the Web UI as well, as shown in [Figure 94 on page 83](#).

Service	Status	Description
esrsalarm	Service Enabled	Service to create alarms
esrsauditlogging	Service Enabled	Service to audit the SRS VE
esrsauth	Service Enabled	Authorization service
esrsusermanagement	Service Enabled	Manage Users service
esrsconfigtool	Service Enabled	Service for SRS VE configural
esrsconnectivityreport	Service Enabled	Service to run the Connectivi
esrsdataitems	Service Enabled	Service to manage data item
esrsdevicemanagement	Service Enabled	Device management service
esrsjcmcm	Service Enabled	ConnectEMC Restful Service
esrskeepalive	Service Enabled	Keepalive service for manage

Service	Status	Description
esrsclient	Service Enabled	SRS VE core agent
esrshttd	Service Enabled	SRS Apache for inbound traffic
esrshttdR	Service Enabled	SRS Apache for outbound traffic
esrsconnectemc	Service Enabled	ConnectEMC service for Connect Home fil
esrsclientproxy	Service Enabled	SRSVE as a proxy service
esrs watchdog	Service Enabled	Watchdog service to monitor the SRS VE services
esrshttdftp	Service Enabled	FTP service for Connect Home files
esrshttdlistener	Service Enabled	HTTPS listener service for Connect Home
postfix	Service Enabled	SMTP service for Connect Home files
chihvi	Service Enabled	Chihhvlath interface for SRS SD

Figure 94 Core service status in the Web UI

Steps to enable logging

IMPORTANT

Once you complete the trouble shooting, disable the debug logging to avoid any disk space issues.

GW logs

To enable debug logs for the SRS:

1. To enable debug logs for SRSv3, edit the `xgEnterpriseProxy.xml` file in the `/opt/ESRS/gateway` directory by changing an element value from '0' to '1'. This element is shown below in **boldface**.

```
<?xml version="1.0" standalone="yes"?>
<PersistedData TerseType="1">
  <i>12</i>
  <s>"#URL_1#"</s>
  <s>"eMessage"</s>
  <i>443</i>
  .....
  .....
  .....
  .....
  <i>300</i>
  <i>1</i>
  <i>1</i>
  <s>"Enterprise"</s>
  <s>"AES256-SHA:DES-CBC3-SHA"</s>
</PersistedData>
```

2. Restart the `ESRSclient` service (**service ESRSclient restart**) `xGate.log`. Debugging information will be written to the `/opt/ESRS/gateway` directory.

To disable the debug: revert the changes and restart the `ESRSclient` service.

Remote session logs

To enable remote session logs for the SRS:

1. Edit the `xgRCon.xml` file (found in the `/opt/ESRS/gateway/ESRS` directory) by inserting the element highlighted below in **bold**.

```
<?xml version="1.0" standalone="yes"?>
<PersistedData moduleName="RCon" TerseType="1">
```

```
<Debug>true</Debug>
</PersistedData>
```

2. Restart the ESRSclient service. A new remote session log will be written to the `/opt/ESRS/gateway` directory.

To disable the remote session logs: revert the changes; restart the ESRSclient service; and delete the remote session logs.

Privoxy logs

To enable the privoxy logging, edit the `Privoxy` config file in the `/opt/ESRS/gateway/privoxy` directory as follows:

At the end of the section **3.1. debug**, by default the debug options are commented, as shown below. Uncomment those options to enable debugging.

```
debug 1 # Log the destination for each request Privoxy let through.
See also debug 1024.
debug 1024 # Actions that are applied to all sites and maybe overruled
later on.
debug 4096 # Startup banner and warnings
debug 8192 # Non-fatal errors
```

The `privoxy.log` will be written to the `/var/log/ESRS/privoxy/` directory.

To disable the privoxy logging, revert the changes.

Provisioning Logs

The provisioning logs can be downloaded from the **logs** tab under the Provisioning folder, when the provisioning is successful and the Web UI is accessible.

In the case of a provisioning failure, these logs (`provisioning.log`) can be accessed from the OS directly on the SRS box at:

`/var/log/ESRS/provisioning/`

Unzipping files using WinZip

Once your zip file is open, follow the following procedure so that your import will be successful:

1. Open WinZip (You can also use 7-Zip or WinRAR).
2. Select **Options**, as shown in [Figure 95 on page 85](#).

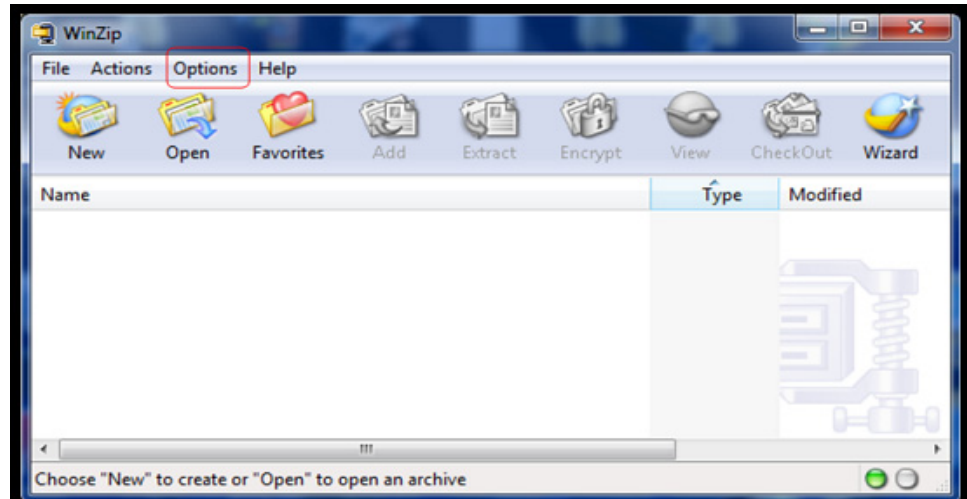


Figure 95 Selecting Options

3. Select **Configuration**, and then the **Miscellaneous** tab, as shown in [Figure 96 on page 85](#).

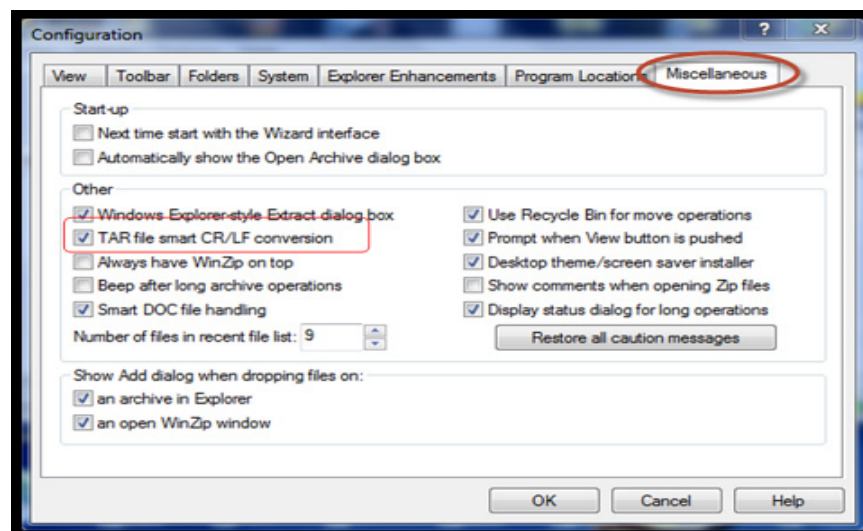


Figure 96 Selecting Miscellaneous tab

4. Clear the **TAR file smart CR/LF conversion** checkbox, and then click **OK**, as shown in [Figure 97 on page 86](#). The box will remain unchecked until it is selected again, or WinZip is reinstalled.

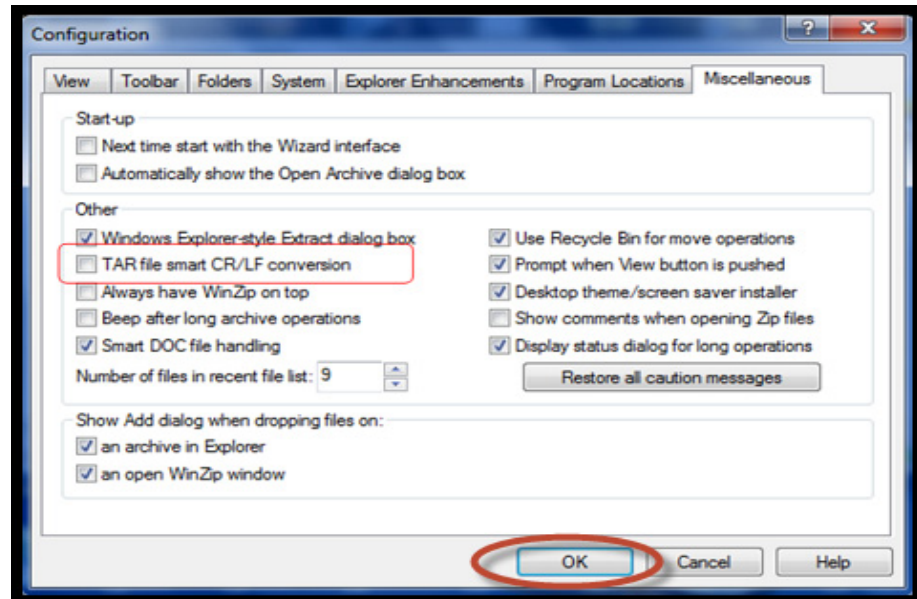


Figure 97 Clearing the TAR file smart CR/LF conversion checkbox

5. Unzip and import the data.

APPENDIX A

SRS Migration Process

This appendix describes the manual process to migrate devices from the SRS 2.xx version to the SRS 3.xx version.

- ◆ SRS Migration Tool version 3.xx 88
- ◆ Precondition prior to migration process initiation 89
- ◆ Assumptions 90
- ◆ Procedure for migrating devices from source to target gateway 91
- ◆ SRS Export Import Migration Tool (Version 3.xx) for Windows. 94
- ◆ Backend migration process..... 113

SRS Migration Tool version 3.xx

The SRS Migration Tool (Migration Tool) is a wizard-based application, used to export the managed devices from SRS 2.xx so that they can be migrated to SRS 3.xx. The Migration Tool runs on the Source Windows Gateway host, which reads the Gateway configuration file, exports device information, and generates an XML file. The devices are then deployed to a new SRS2 Gateway or SRSv3 by copying this XML file to any of the following:

- ◆ **SRS2 Gateways:**

Windows OS: <install_drive>;\EMC\ESRS\Gateway\work\dmb\request

- ◆ **SRS2 Gateways on Linux:** /opt/EMC/ESRS2/Gateway/work/dmb/request

- ◆ **SRSv3:**

(opt/ESRSve/gateway/work/dmb/request) on the destination on an SRSv3.

This process requires a manual approval and a Sync Now to be deployed to the Gateway/Gateway Cluster or SRS/SRS Cluster. Prior to approval, any validation errors must be resolved.

If the migration of devices needs to be done from a Linux Gateway, then you need to manually copy the `xgDeployConfig.xml` file in the Source SRS Gateway installation directory (/opt/Dell EMC/ESRS/Gateway) to a Windows host. The user executes the Migration Tool and points it to the location of the `xgDeployConfig.xml` file copied from the Linux SRS2 Gateway. You then copy the generated XML file to any of the following:

- ◆ **SRS2 Gateways:**

Windows OS: <install_drive>;\EMC\ESRS\Gateway\work\dmb\request

- ◆ **SRS2 Gateways on Linux:** /opt/EMC/ESRS2/Gateway/work/dmb/request

- ◆ **SRSv3:**

(opt/ESRSve/gateway/work/dmb/request) on the destination on an SRSv3.

As stated previously, the process requires manual approval and a Sync Now for deployment to the Gateway/Gateway Cluster or SRS/SRS Cluster. Prior to approval, any validation errors must be resolved.

Note: Avoid using multiple ServiceLink browsers or tabs while performing migration.

Precondition prior to migration process initiation

Before you begin the migration process initiation, follow these steps:

1. Ensure that the source SRS is installed and has managed devices.
2. Ensure that SRS is provisioned and has connectivity with Dell EMC.
3. On a Windows host, you can execute the Migration Tool directly by clicking the Migration Tool executable.
4. On a Linux host, you have to manually copy `xgDeployConfig.xml` from the Source Gateway host to any Windows host to execute the Migration Tool.
5. Ensure that .Net Framework 2.0 or later is installed on the Gateway host or another Windows host where the Migration Tool will be running.

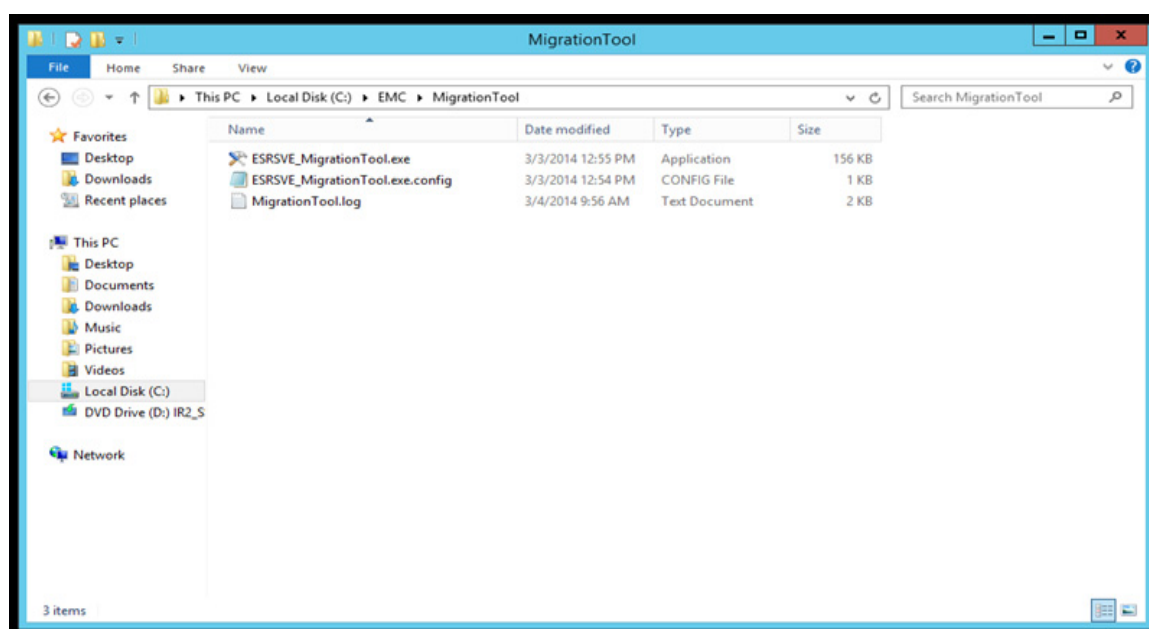


Figure 98 Installing Migration Tool

6. Ensure that the following entry exists in the `ESRSVE_MigrationTool.exe.config` file to execute the Migration Tool on .Net Framework versions later than 3.5.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0"/>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>
```

Note: If the following error displays while executing the Migration Tool, then the required version of the .Net Framework for the Migration Tool needs to be manually installed or the appropriate ESRSVE Migration Tool.exe.config file is missing.

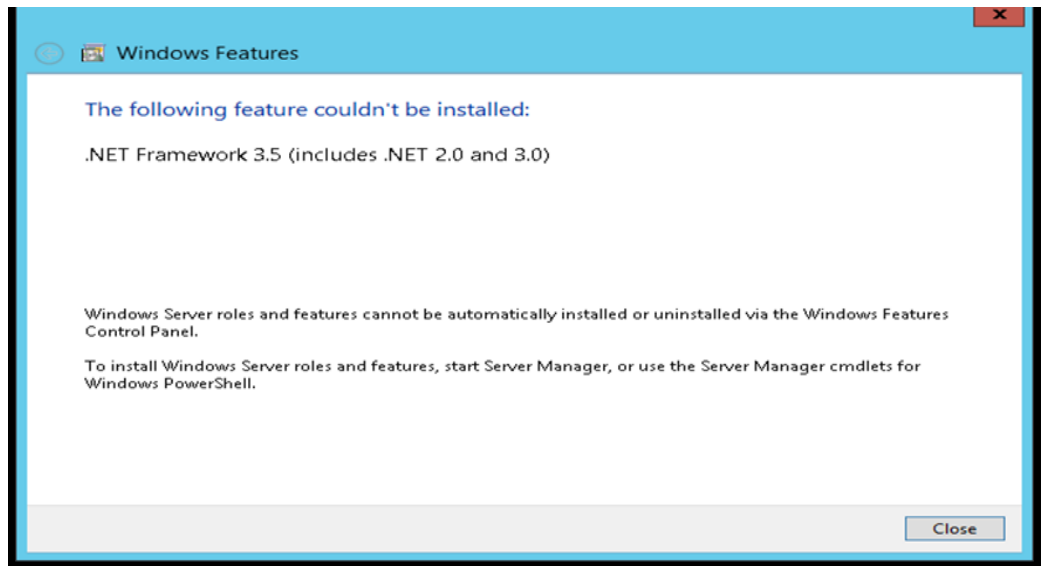


Figure 99 Unable to install Windows Features error message

7. Right-click on the `ESRSVE_MigrationTool.exe` and select **Run as Administrator** mode on Windows 2008 and later.
8. To avoid any Site ID validation errors, ensure that all Site IDs are populated on the SRS Agent.

Assumptions

The assumptions are as follows:

- ◆ Partial migration of devices is not supported through the Migration Tool.
- ◆ The source gateway from where the Migration Tool should be run needs to manage at least one device.
- ◆ Migration on a High Availability gateway or a Cluster gateway to an SRS target gateway remains the same.
- ◆ For migration of a High Availability gateway, all device management validation errors, user authentication, and authorization errors for standalone gateway migration remain the same.
- ◆ To migrate the devices from a source HA gateway Cluster to an SRS target gateway or an SRS gateway cluster, you only need to perform migration on one gateway in a cluster.
- ◆ Running the migration process on one gateway within a cluster migrates all of the devices to the target gateway.
- ◆ Site ID issues will be resolved by manually adding the site ID to the SRS or the SRS Cluster in ServiceLink.

Procedure for migrating devices from source to target gateway

1. Copy the Migration Tool executable to a directory on the Gateway or the intermediate host.
2. Right-click on the executable and select **Run As Administrator**. The Migration Tool wizard appears, as shown in [Figure 100 on page 91](#).



Figure 100 Migration Tool wizard

3. On the Migration Tool wizard, click **Next**. The Migration Tool wizard displays the Source and Destination Directory information, as shown in [Figure 101 on page 92](#). Note the following:
 - The Source Directory is the path of the SRS installation directory or intermediate host.
 - The Destination Directory is the directory where the Migration Tool stores the migration output file (which is a DMB Request file).

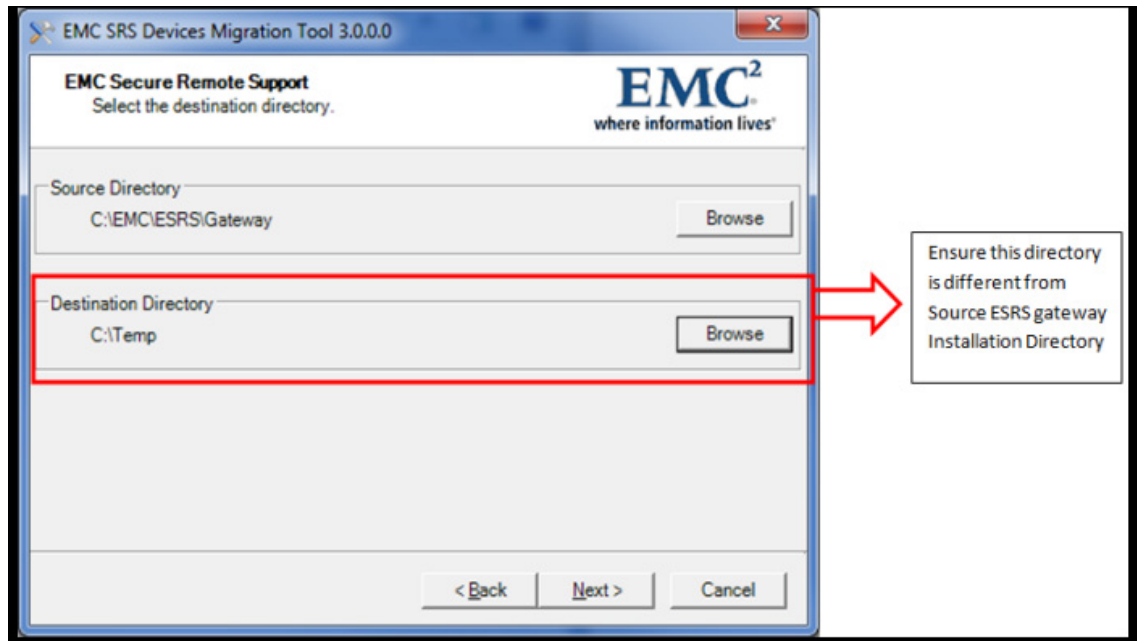


Figure 101 Selecting Destination Directory

4. Click **Next**. Once the migration process starts, a progress bar indicates the status of the migration, as shown in [Figure 102 on page 92](#).

Note: The SRS Migration Tool, its files, and the `xgDeployConfig.xml` should all be in the same directory on the host.

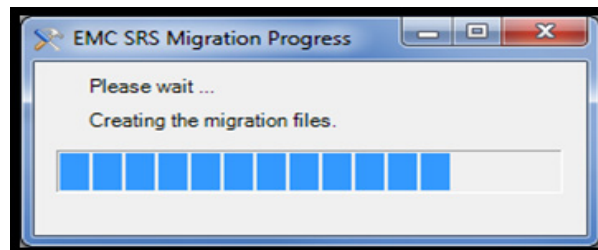


Figure 102 Dell EMC SRS Migration Progress Bar

After completion of the migration process, a summary page appears, as shown in [Figure 103 on page 93](#). This page details the devices managed by the Source Gateway.

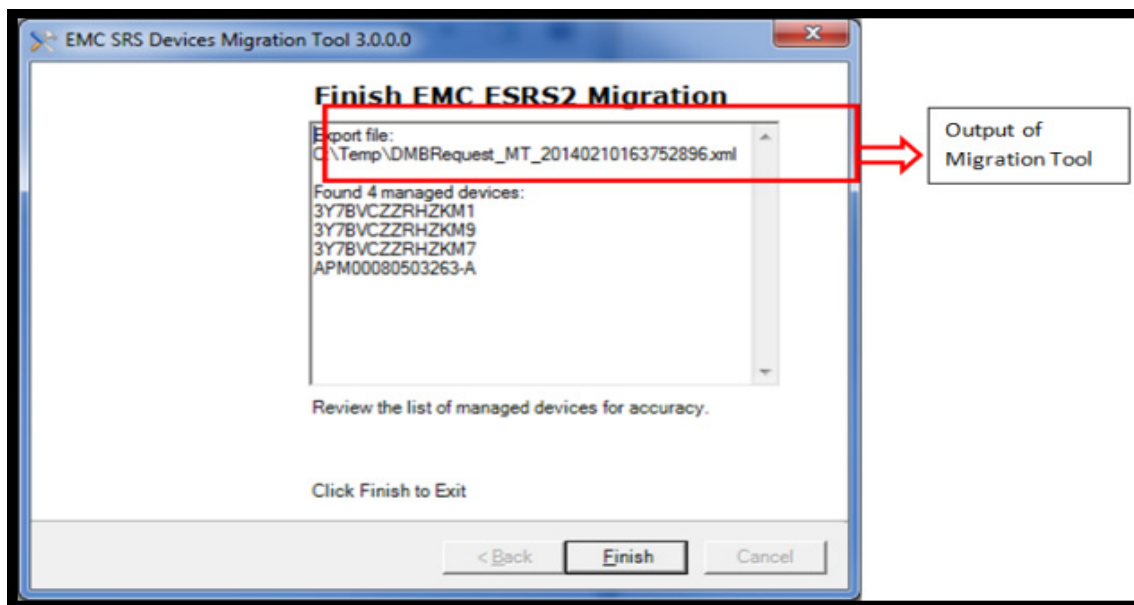


Figure 103 Summary page

A DMB Request XML file is saved under the destination directory, as shown in [Figure 104 on page 93](#).

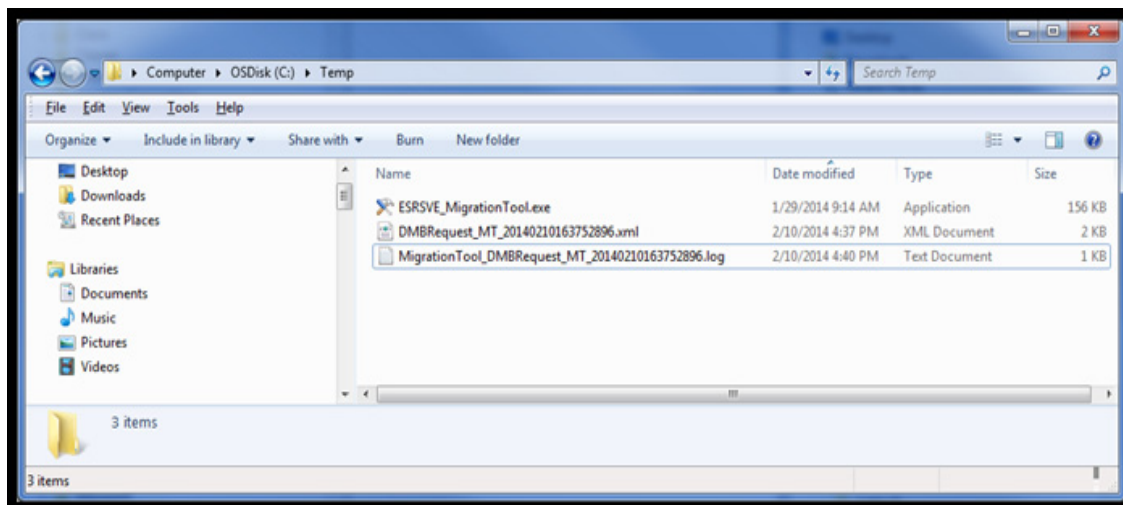


Figure 104 Example of DMB Request xml file in destination directory

5. Manually copy the DMB Request file from the Source gateway (or intermediate host) to the SRS target gateway DMB directory (for example, the /opt/ESRSve/gateway/work/dmb/request directory on the SRS host).
6. Once the DMB sync process (Forced Sync or Automated Sync) with ServiceLink is complete, navigate to ServiceLink and verify that all devices are listed on the Target Gateway DMB page.

Note: Avoid using multiple ServiceLink browsers or tabs while performing migration.

7. Correct any validation errors.

Note: The status of the devices will be **UnManaged** until the devices are manually approved.

8. Click **Approve All**, and then click **Sync Now**.
9. Validate that the devices are managed and have good connectivity.
10. Navigate to the Source Gateway and manually remove all the devices that have been migrated.

Note: All validation errors corresponding to Device Management remain the same when the devices are migrated from either the Standalone Gateway to the SRS Target Gateway or from the High Availability Gateway to SRS.

11. Once verification is complete and the devices have been removed from the existing gateway, set the gateway or gateways (if clustered) offline in ServiceLink (since you have to manually decommission or uninstall the existing gateway).

SRS Export Import Migration Tool (Version 3.xx) for Windows

The SRS Export Import Migration Tool is a standalone tool that can be used to export the deployed devices on a Gateway/Gateway cluster in a CSV file format that a customer may use for device tracking or other use as they may desire. Also, the tool can export the deployed devices to an XML format, as well as migrate devices between SRS 2 Gateways or SRS 2 Gateways and SRS v3.0x.

The Import function permits the generation of DMB_Request files from a CSV formatted file, provided certain information is supplied in the file that will enable bulk deployment of devices to a Gateway or SRS v3.xx without having to manually enter the information through the Configuration Tool or ServiceLink. Copy the resulting file output to one of the following:

- ◆ **SRS2 Gateways:**

Windows OS : <install_drive>;\EMC\ESRS\Gateway\work\dmb\request

- ◆ **SRS2 Gateways on Linux:**

/opt/Dell EMC/ESRS2/Gateway/work/dmb/request

- ◆ **SRSv3:**

(opt/ESRSve/gateway/work/dmb/request) on the destination on an SRSv3.

This process requires manual approval and a Sync Now for deployment to the Gateway/Gateway Cluster or SRS/SRS Cluster. Prior to approval, any validation errors must be resolved.

The devices will NOT be listed in the Configuration Tool or on the SRS **Devices > Managed > Device** tab until they have been approved in ServiceLink by Dell EMC Authorized Personnel.

Procedure

1. Acquire a copy of the bulkimportexport-3.xx.xx.zip file from support.Dell EMC.com.

2. Navigate to the location where SRS is installed (default path <install_drive>:\EMC\ESRS\), as shown in [Figure 105 on page 95](#).

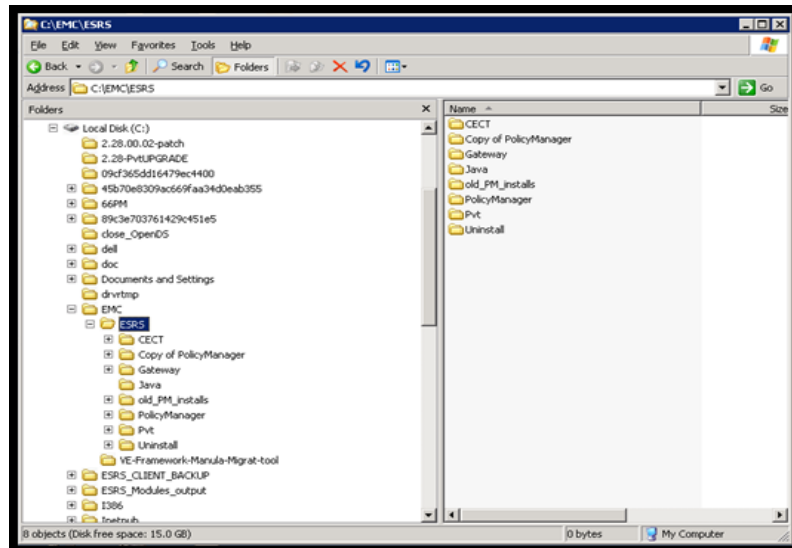


Figure 105 Navigating to SRS

3. Create a directory for the tool, as shown in [Figure 106 on page 95](#).

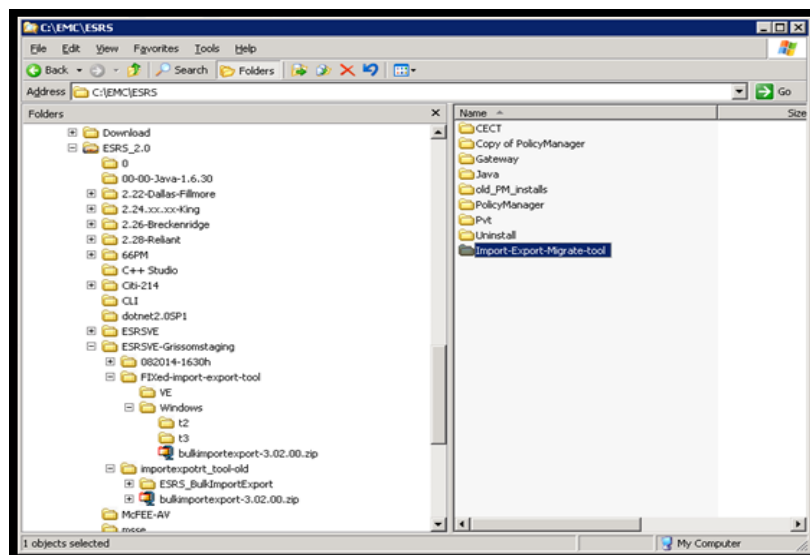


Figure 106 Creating a directory

- Copy the downloaded file to the directory and uncompress it, as shown in [Figure 107](#) on page 96.

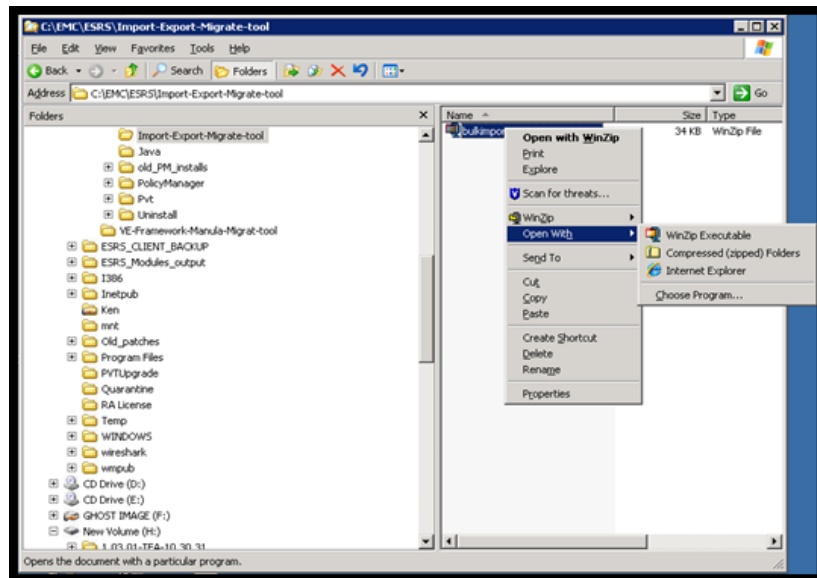


Figure 107 Uncompressing a file

- Right-click the program and select **Run As Administrator**, as shown in [Figure 108](#) on page 96. A screen appears that explains what the tool can do.

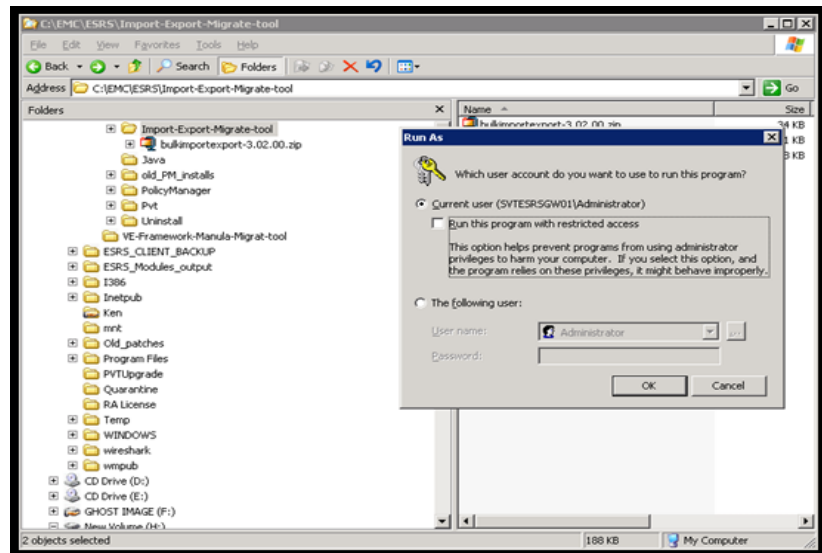


Figure 108 Running as administrator

6. Click **Next**, as shown in [Figure 109](#) on page 97.

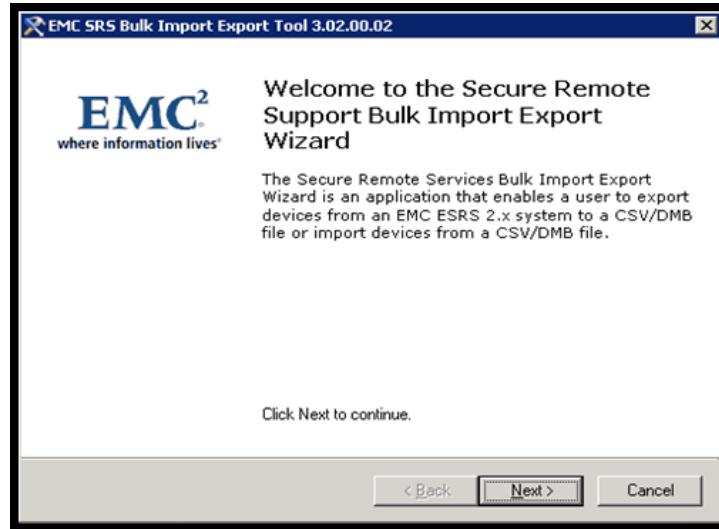


Figure 109 Clicking Next

Note: This tool may also be used to manually migrate between Gateways and to migrate to the SRS 3.0X.XX.XX.

7. Select the operation you wish to perform.
- This option permits the export of all of the currently deployed devices on the SRS2 Gateway to a DMB Request file (XML format) that may be used to redeploy the devices to another Gateway or to the SRS in order to perform a manual migration. You may also use this export file as you desire in your environment.

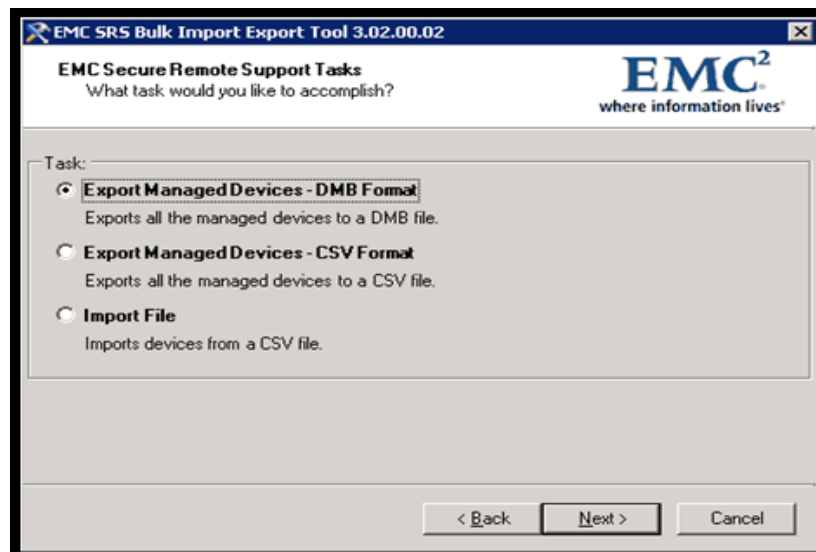


Figure 110 Exporting Managed Devices - DMB Format

The application will attempt to locate the location of the gateway install. If it cannot find it, you can browse for it. The output file will be written to the directory in which the application is executed. You can direct it to another location by using the **Browse** button, as shown in [Figure 111 on page 98](#).

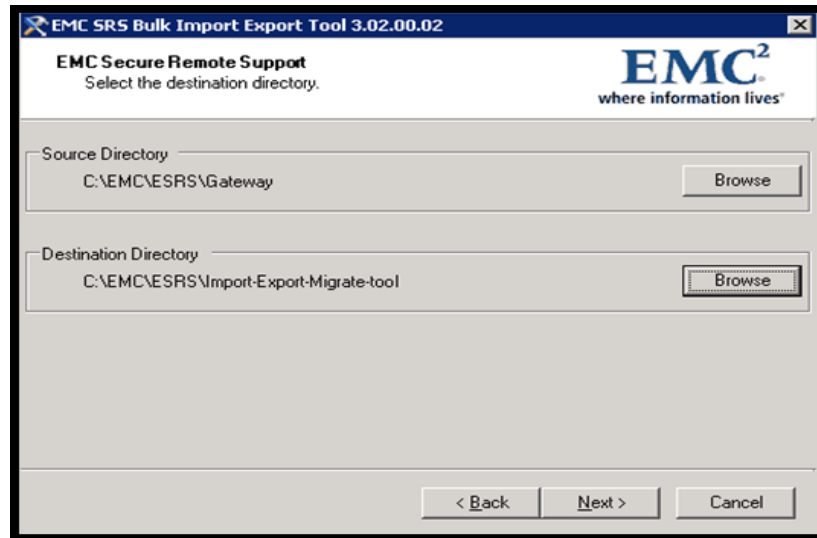


Figure 111 Using the Browse button

The application runs, generates a file, and then provides a summary.

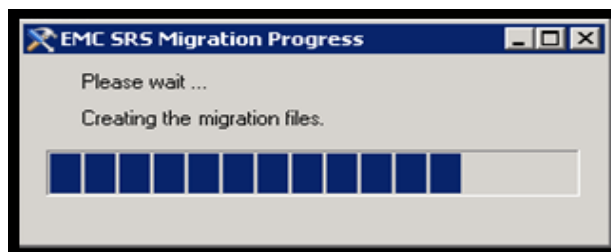


Figure 112 Creating the migration files

When the process is complete, click **Finish**.

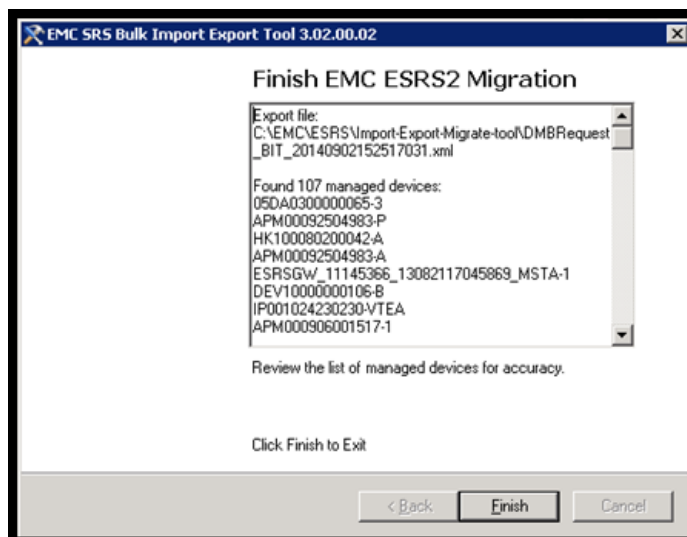


Figure 113 Clicking Finish

A runtime log is generated, as shown in [Figure 114 on page 99](#).

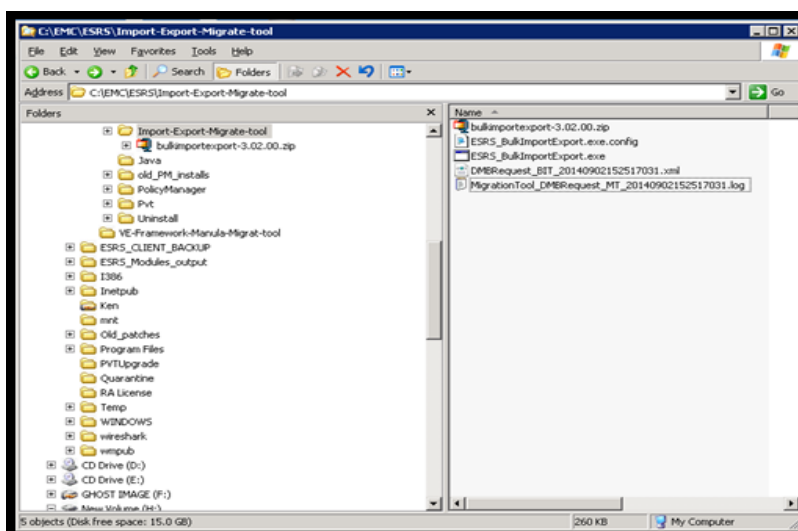


Figure 114 Runtime log

Sample of file content: (truncated)

```
<?xml version="1.0"?>
<deviceManagementRequest schemaVersion="1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.emc.com/ESRS/deviceManagement
deviceManagementRequest.xsd"
xmlns="http://www.emc.com/ESRS/deviceManagement">
  <requestTimestamp>2014-09-02T15:25:16.828</requestTimestamp>
  <requestTool>BIT</requestTool>

  <sourceSerialNumber>ESRSGW_11145366_13082117045869</sourceSerialNum
ber>
  <sourceModel>ESRS-GW</sourceModel>
```

```

<managementRequest>
  <operation>Manage</operation>
  <device>
    <modelName>ATMOS-GW</modelName>
    <serialNumber>05DA0300000065-3</serialNumber>
    <ipAddress>10.241.218.79</ipAddress>
  </device>
</managementRequest>
<managementRequest>
  <operation>Manage</operation>
  <device>
    <modelName>DLm-GW</modelName>
    <serialNumber>APM00092504983-P</serialNumber>
    <ipAddress>10.241.208.182</ipAddress>
  </device>
</managementRequest>
<managementRequest>
  <operation>Manage</operation>
  <device>
    <modelName>CLARIION-GW</modelName>
    <serialNumber>HK100080200042-A</serialNumber>
    <ipAddress>10.15.54.210</ipAddress>
  </device>
</managementRequest>
<managementRequest>
  <operation>Manage</operation>
  <device>
    <modelName>DLm-GW</modelName>
    <serialNumber>APM00092504983-A</serialNumber>
    <ipAddress>10.241.208.181</ipAddress>
  </device>
</managementRequest>
~
~
~
~

```

- b. This option permits the export of all of the currently deployed devices on the SRS2 Gateway to a CSV file format that you may use as you desire in your environment. The CSV formatted file can also be used as a source file for this application or for the command line tool that is embedded on the SRS versions 3.02.XX.XX and later.

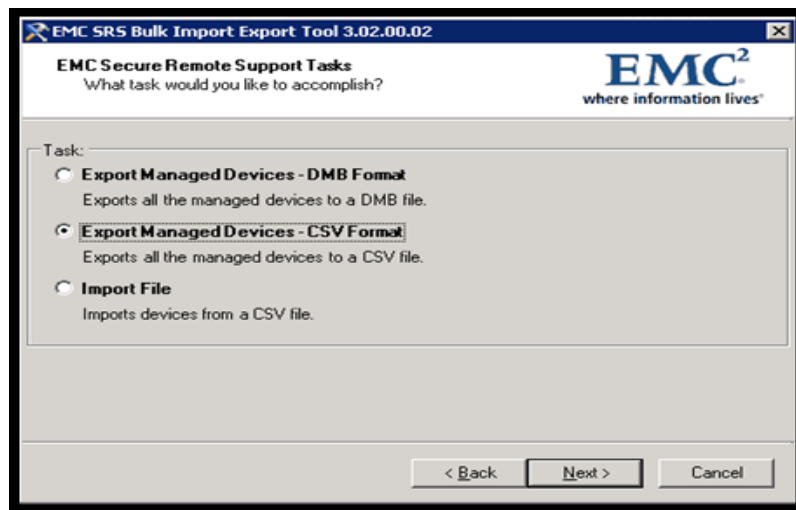


Figure 115 Export Managed Devices - CSV Format

The application will attempt to find the location of the gateway install. If it cannot find it, you can browse for it. The output file will be written to the directory in which the application is executed. You can direct it to another location by using the Browse button, and then clicking **Next**, as shown in [Figure 116 on page 101](#).

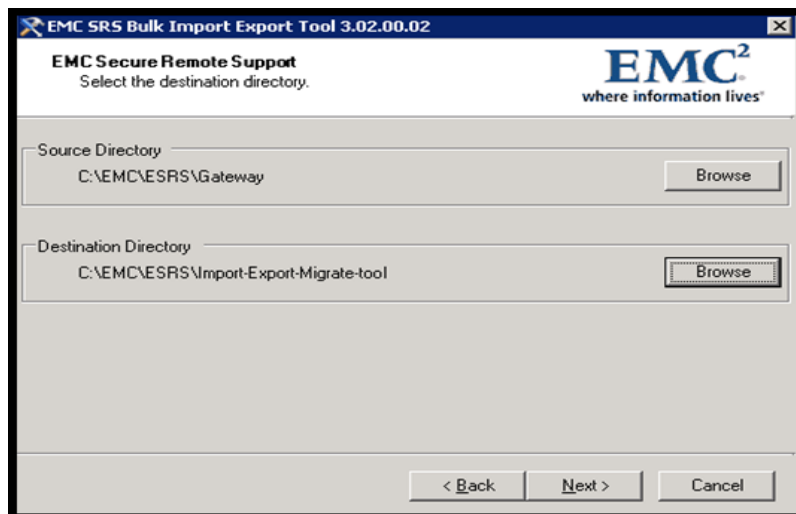


Figure 116 Selecting destination directory

The application runs, generates a file, and then provides a summary.

When it completes, click **Finish**. A runtime log is generated, as shown in [Figure 117 on page 102](#).

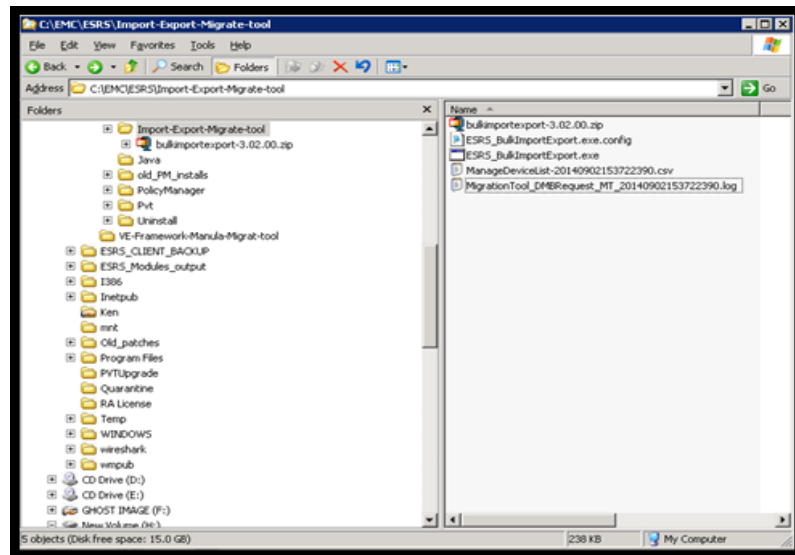


Figure 117 Run time log

- c. This option, as shown in [Figure 118 on page 103](#), permits the import of a CSV formatted file to generate as a DMB Request file (XML format) that can be used on the SRS2 Gateway or the SRSv3 as a DMB Request file (XML format). It can then be used to do a bulk deploy of devices to an SRS2 Gateway or to the SRSv3. You may now copy this file to any of the following:
 - **SRS2 Gateways:**
Windows OS:
`<install_drive>;\EMC\ESRS\Gateway\work\dmb\request`
 - **SRS2 Gateways on Linux:**
`/opt/EMC/ESRS2/Gateway/work/dmb/request`
 - **SRSv3:**
(`opt/ESRSve/gateway/work/dmb/request`) on the destination on an SRSv3.

This process requires manual approval and a Sync Now for deployment to the Gateway/Gateway Cluster or the SRS/SRS Cluster. Prior to approval, any validation errors must be resolved.

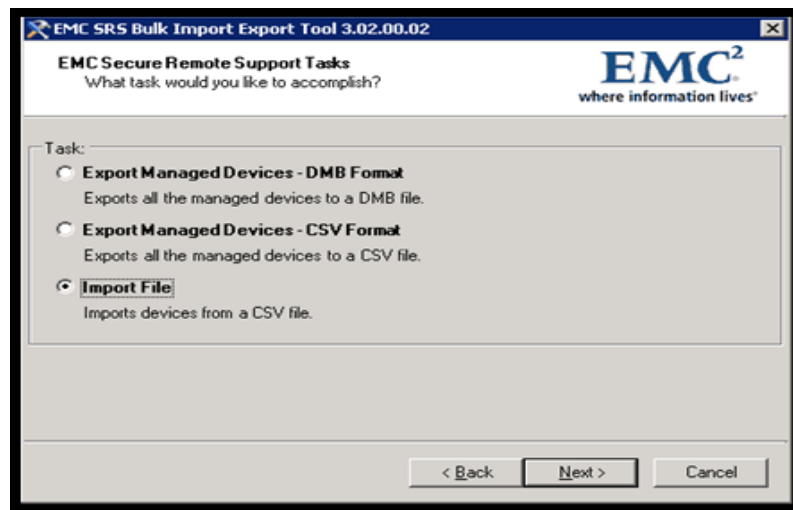


Figure 118 Import File

The CSV formatted file must contain the following information in the following format/order:

SRS Model,Serial Number,IP Address

Example:

```
Model,Serial Number,IP Address
ATMOS-GW,05DA0300000065-3,10.241.218.79
CLARIION-GW,HK100080200042-A,10.15.54.210
DLm-GW,APM00092504983-A,10.241.208.181
DLm-GW,APM00092504983-P,10.241.208.182
~
~
~
```

Note: You must append "-GW" to the Dell EMC Model of the product and you must separate the fields using a comma. Also, if the serial number is listed more than once, then you must append it with the appropriate suffix for that model.

Browse to select the source file, as shown in [Figure 119 on page 104](#) and [Figure 120 on page 104](#).

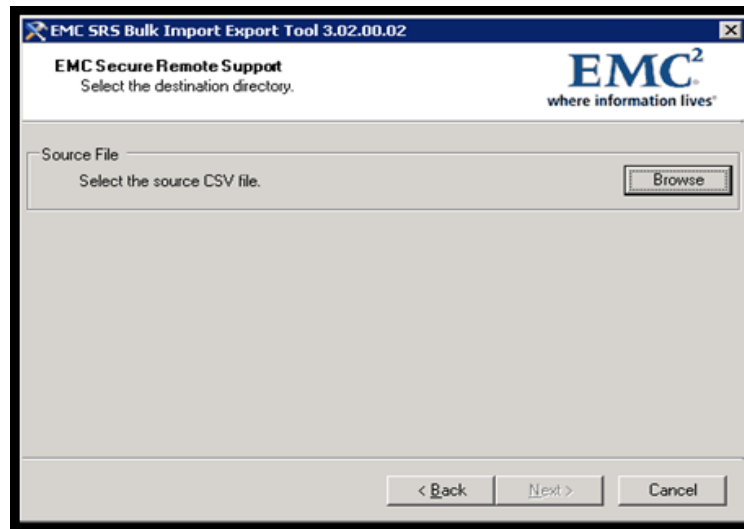


Figure 119 Using browse to select the source file

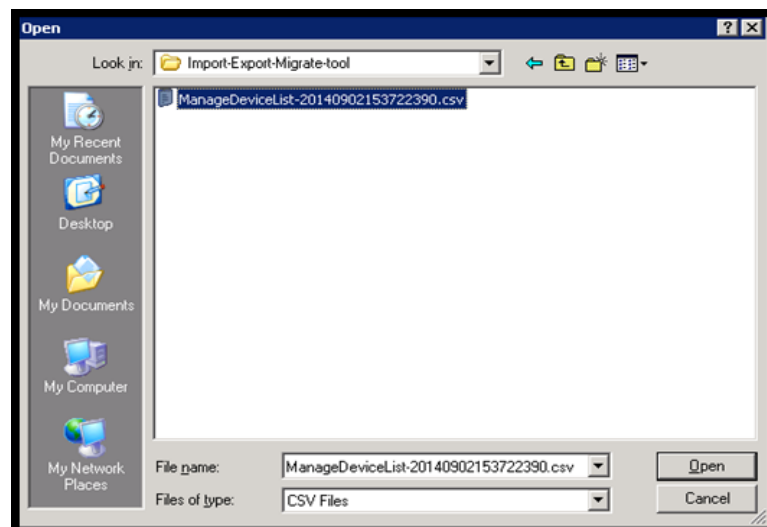


Figure 120 Selecting the source file

Browse to select the destination directory, and then click **Next**.

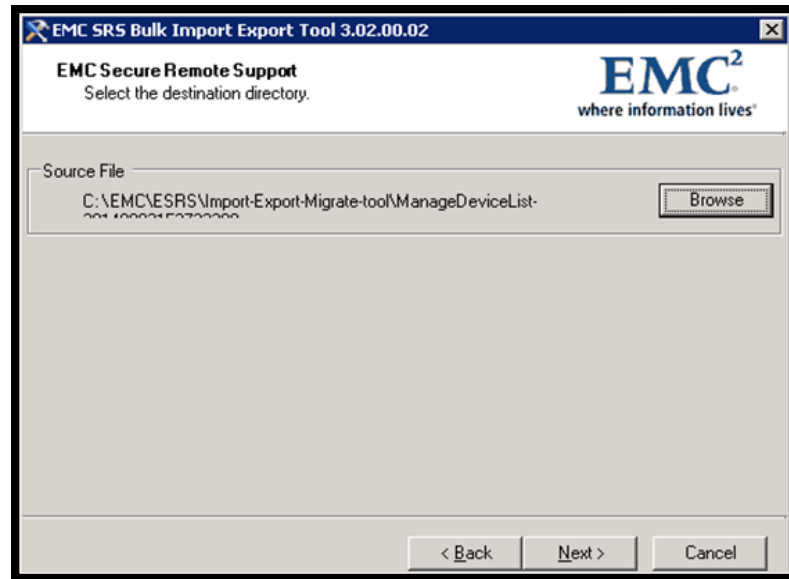


Figure 121 Selecting destination directory

The application runs and generates the DMB Request file, a Summary, and a Log file.

When the execution completes, click **Finish**.

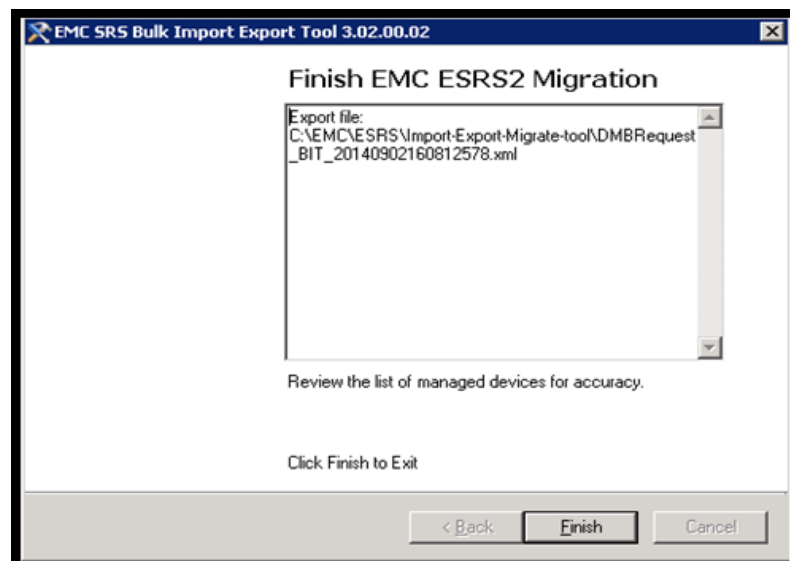


Figure 122 Finish Dell EMC SRS2 Migration

The log file appears.

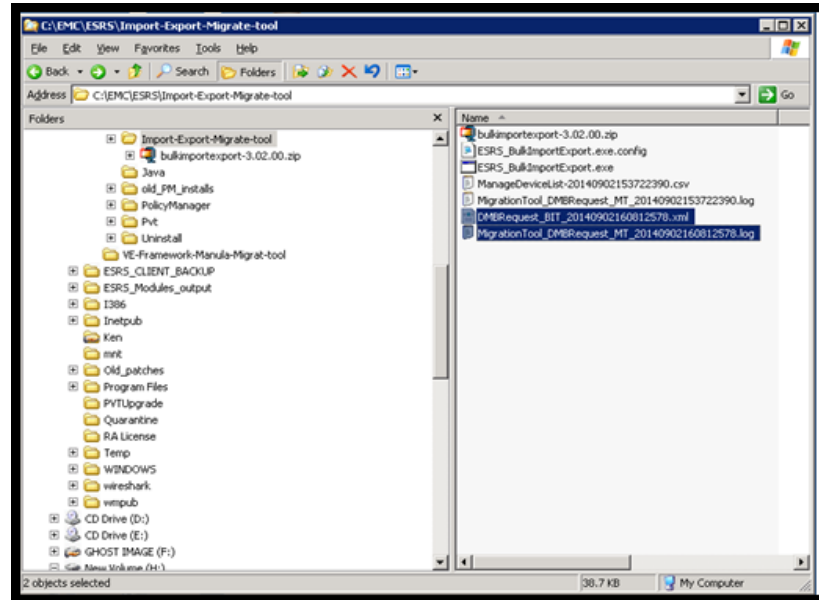


Figure 123 Log files

Sample of file contents: (Truncated)

```
<?xml version="1.0"?>
<deviceManagementRequest schemaVersion="1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.emc.com/ESRS/deviceManagement
deviceManagementRequest.xsd"
xmlns="http://www.emc.com/ESRS/deviceManagement">
  <requestTimestamp>2014-09-02T16:08:11.937</requestTimestamp>
  <requestTool>BIT</requestTool>

  <sourceSerialNumber>ESRSGW_11145366_13082117045869</sourceSerialNum
ber>
  <sourceModel>ESRS-GW</sourceModel>
  <managementRequest>
    <operation>Manage</operation>
    <device>
      <modelName>ATMOS-GW</modelName>
      <serialNumber>05DA0300000065-3</serialNumber>
      <ipAddress>10.241.218.79</ipAddress>
    </device>
  </managementRequest>
  <managementRequest>
    <operation>Manage</operation>
    <device>
      <modelName>DLm-GW</modelName>
      <serialNumber>APM00092504983-P</serialNumber>
      <ipAddress>10.241.208.182</ipAddress>
    </device>
  </managementRequest>
  <managementRequest>
    <operation>Manage</operation>
    <device>
      <modelName>CLARIION-GW</modelName>
      <serialNumber>HK100080200042-A</serialNumber>
      <ipAddress>10.15.54.210</ipAddress>
    </device>
  </managementRequest>
```

```
</managementRequest>
~
~
~
~
```

You may now copy this file to any of the following:

– **SRS2 Gateways:**

Windows OS:

```
<install_drive>;\EMC\ESRS\Gateway\work\dmb\request
```

– **SRS2 Gateways on Linux:**

```
/opt/EMC/ESRS2/Gateway/work/dmb/request
```

– **SRSv3:**

(opt/ESRSve/gateway/work/dmb/request) on the destination on an SRS.

This process requires manual approval and a Sync Now for deployment to the Gateway/Gateway Cluster or the SRS/SRS Cluster. Prior to approval, any validation errors must be resolved.

For Linux SRS Gateways

1. Copy the /opt/EMC/ESRS2/Gateway/xgDeployConfig.xml from the Linux Gateway to a directory where the Import Export Migration Tool is installed.

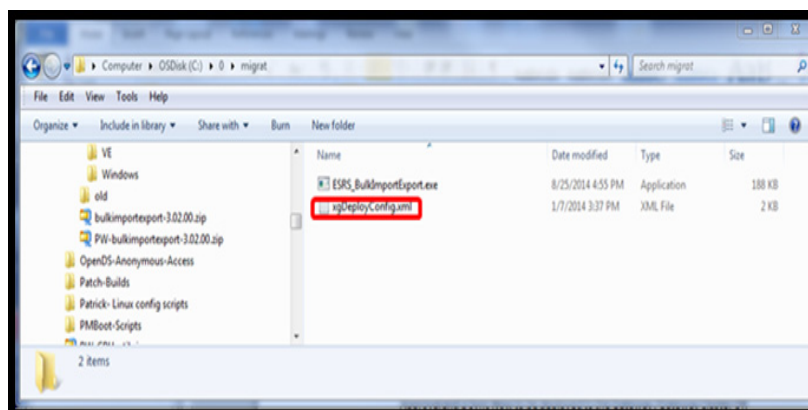


Figure 124 Copying file

2. Execute the ESRS_BulkImportExport.exe application and point it to the location of where the xgDeployConfig.xml file is located. You can use the same processes as detailed above.

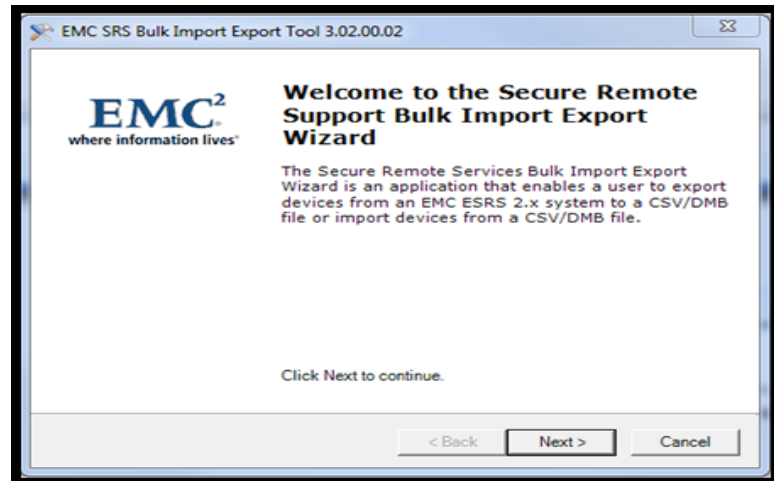


Figure 125 Secure Remote Support Bulk Import Export Wizard

3. Select the appropriate export option (DMB format for use for migrations or CSV format for customer use.)

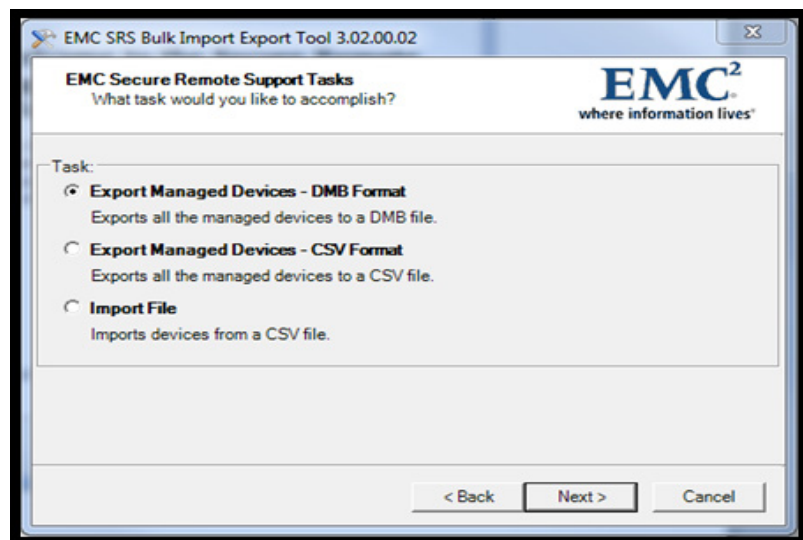


Figure 126 Selecting Export feature

4. Browse to the location of the `xgDeployConfig.xml` file from the Linux SRS2 Gateway.

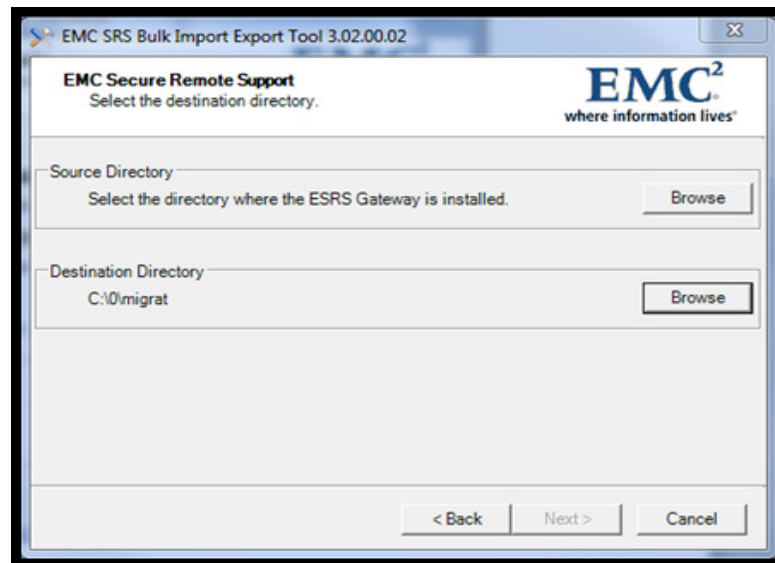


Figure 127 Browsing to the location of the file

You can also define an alternate path for where the exported file will be written using the same method as for the file location.

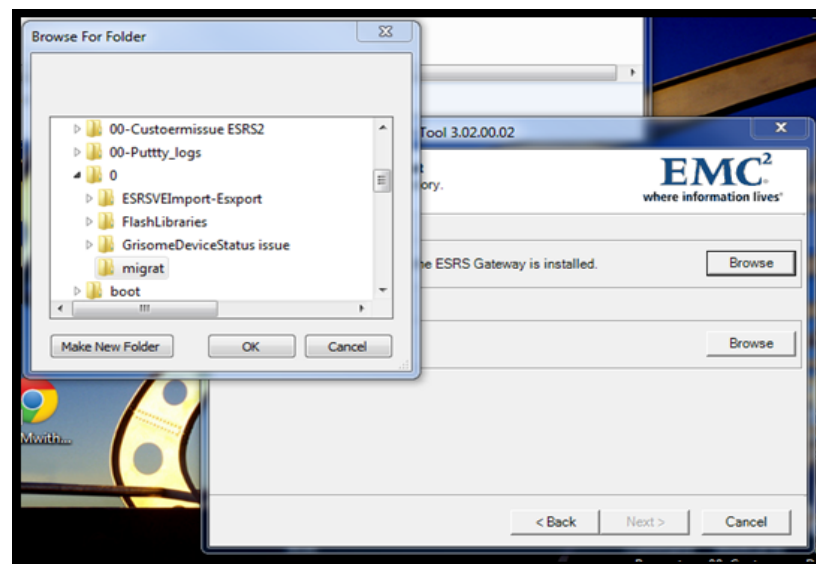


Figure 128 Defining an alternate path

5. Click **Next** to perform the export.

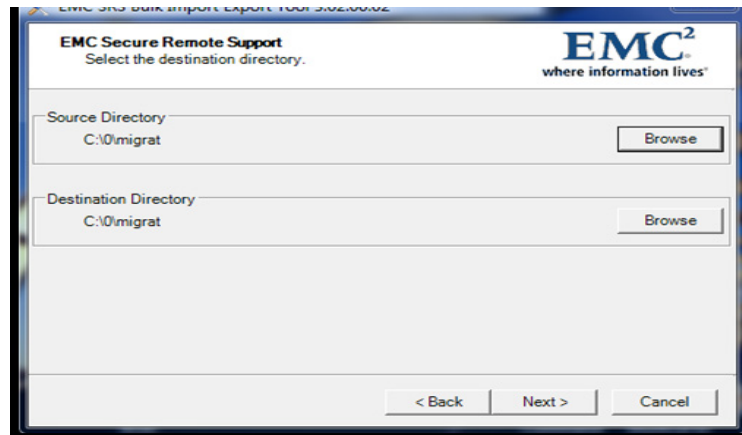


Figure 129 Selecting Next

6. When the migration completes, click **Finish**.

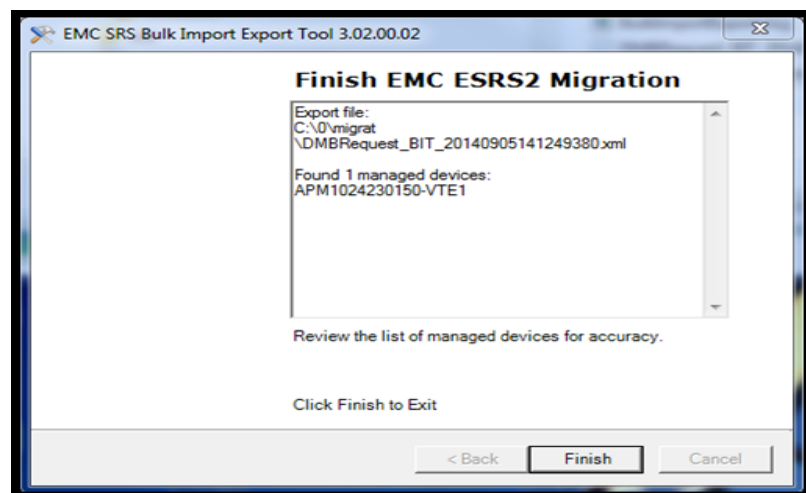


Figure 130 Selecting Finish

The directory now contains the export file (DMB Request or CSV formatted file) and the log for this execution of the tool.

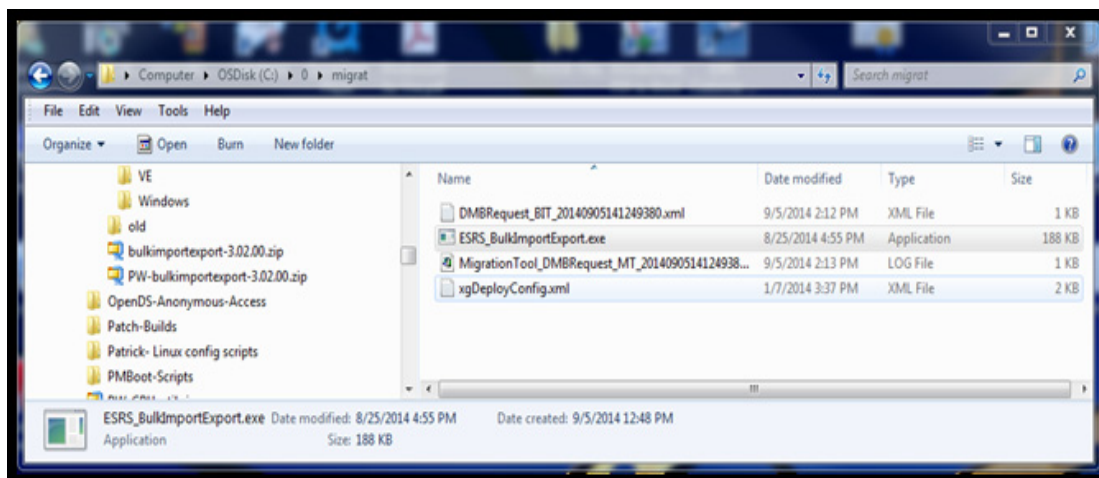


Figure 131 Export file directory

Note: The exported file will be located in the directory defined in step 4.

Bulk Import Export Tool embedded in SRS 3.02.XX.XX and above

Procedure 1. Log in to the SRS shell with an SSH client.

```
===== PuTTY log 2014.09.05 15:44:49
=====
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Wed Sep 3 16:11:33 2014 from jpcsnikijl2c.corp.emc.com
```

2. Change to the /opt/esrsve/utilities/bulkimportexport directory.

```
# cd /opt
grissomu2-103:/opt # ls
ADG connectemc connectemcVE esrs esrsve httpd httpdR httpdftp
httpdlistener lb vmware
grissomu2-103:/opt # cd esrsve/
grissomu2-103:/opt/esrsve # ls
alarm configtool deviceutility sysmon
vfabric-config
auditlogging connectivityreport gateway usermanagement
webcontent
auth cst jcemc utilities
webuimgmt-util
bin dataitems keepalive uuid
cect devicemanagement provisioning vappconfig
grissomu2-103:/opt/esrsve # cd utilities/
grissomu2-103:/opt/esrsve/utilities # ls
```

```
bulkimportexport
grissomu2-103:/opt/esrsve/utilities # cd bulkimportexport/
grissomu2-103:/opt/esrsve/utilities/bulkimportexport # ls
bulk_import_export.sh bulkimportexporttool.jar
```

3. Execute the ./bulk_import_export.sh application.

```
grissomu2-103:/opt/esrsve/utilities/bulkimportexport # ./
./bulk_import_export.sh --help
usage:
./bulk_import_export.sh [operation] [export-type] [filename]
options:
-e, --export
-i, --import
-t, --type
-f, --file
Examples:
./bulk_import_export.sh --export --type dmb --file /tmp/esrs.xml
./bulk_import_export.sh --export --type csv --file /tmp/esrs.csv
./bulk_import_export.sh --import --file /tmp/esrs.csv
```

4. To export the deployed devices, execute the following command. Specify the function (export or import), the type (DMB for a DMB Request file that can be moved to another SRS gateway to deploy the devices or CSV formatted file to use as you wish, it can also be used as a source file to import devices to another SRS gateway), and the complete file name with its extension. If you wish to place the file in another location, then you must supply the complete path and file name. If no path is specified, then the file will be written to the local directory.

Type DMB_Request

```
grissomu2-103:/opt/esrsve/utilities/bulkimportexport #
./bulk_import_export.sh --export --type dmb --file
DMB_request-09-05.xml
Export was successful.
```

Type .csv

```
./bulk_import_export.sh --export --type csv --file
exportt-09-05.csv
Export was successful
```

```
grissomu2-103:/opt/esrsve/utilities/bulkimportexport # ls -ailh
total 60K
868378 drwxr-xr-x 2 root root 4.0K Sep  5 16:00 .
852068 drwxr-xr-x 3 root root 4.0K Aug 28 08:07 ..
869294 -rw-r--r-- 1 root root 182 Sep  5 15:42
BulkImportExport_20140905154205.log
869295 -rw-r--r-- 1 root root 230 Sep  5 15:43
BulkImportExport_20140905154322.log
869296 -rw-r--r-- 1 root root 403 Sep  5 15:44
BulkImportExport_20140905154403.log
869298 -rw-r--r-- 1 root root 441 Sep  5 16:00
BulkImportExport_20140905160013.log
869297 -rw-r--r-- 1 root root 768 Sep  5 15:44 DMB_request-09-05.xml
868520 -rwxr-xr-x 1 root root 181 Aug 28 10:18 bulk_import_export.sh
868521 -rwxr-xr-x 1 root root 24K Aug 28 10:18
bulkimportexporttool.jar
869299 -rw-r--r-- 1 root root 130 Sep  5 16:00 exportt-09-05.csv
```

```
grissomuat2-103:/opt/esrsve/utilities/bulkimportexport #
```

5. To Import a CSV formatted file to the SRS:

```
./bulk_import_export.sh --import --file exportt-09-05.csv
Import was successful.
grissomuat2-103:/opt/esrsve/utilities/bulkimportexport # exit
logout
```

6. Each time the tool is run, a runtime log is generated:

```
grissomuat2-103:/opt/esrsve/utilities/bulkimportexport # ls -aailh
total 72K
868378 drwxr-xr-x 2 root root 4.0K Sep  5 16:14 .
852068 drwxr-xr-x 3 root root 4.0K Aug 28 08:07 ..
869294 -rw-r--r-- 1 root root 182 Sep  5 15:42
BulkImportExport_20140905154205.log
869295 -rw-r--r-- 1 root root 230 Sep  5 15:43
BulkImportExport_20140905154322.log
869296 -rw-r--r-- 1 root root 403 Sep  5 15:44
BulkImportExport_20140905154403.log
869298 -rw-r--r-- 1 root root 441 Sep  5 16:00
BulkImportExport_20140905160013.log
869300 -rw-r--r-- 1 root root 390 Sep  5 16:13
BulkImportExport_20140905161341.log
869302 -rw-r--r-- 1 root root 2.0K Sep  5 16:13
BulkImportExport_20140905161358.log
869301 -rw-r--r-- 1 root root 2.0K Sep  5 16:14
BulkImportExport_20140905161432.log
869297 -rw-r--r-- 1 root root 768 Sep  5 15:44 DMB_request-09-05.xml
868520 -rwxr-xr-x 1 root root 181 Aug 28 10:18 bulk_import_export.sh
868521 -rwxr-xr-x 1 root root 24K Aug 28 10:18
bulkimportexporttool.jar
869299 -rw-r--r-- 1 root root 130 Sep  5 16:00 exportt-09-05.csv
grissomuat2-103:/opt/esrsve/utilities/bulkimportexport #
```

7. When the processes finishes, log out of SRS:

```
grissomuat2-103:/opt/esrsve/utilities/bulkimportexport # exit
logout
```

Backend migration process

This section describes the backend migration from a regular SRS to an SRSv3.

Note: This section only applies to ServiceLink users.

1. The first step is to determine the source gateway or virtual edition serial number. You can determine this information from the Gateway Configuration Tool or the SRS GUI Dashboard, but for the backend migration, you can determine all necessary information from the SRS Portal or ServiceLink (ESRS.EMC.com), as shown in [Figure 132 on page 114](#).

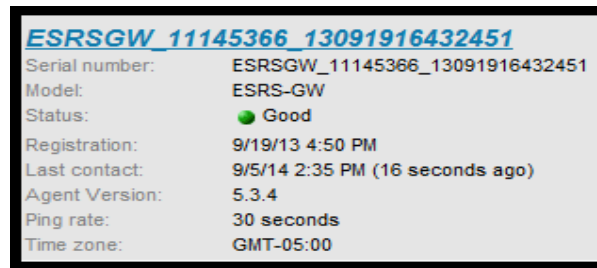


Figure 132 Example of source gateway serial number on ServiceLink

- Once you have determined the gateway or virtual edition serial number, select **Manage Devices**, as shown in [Figure 133 on page 114](#). You can then review the current managed device configuration, as shown in [Figure 134 on page 114](#). Note any existing errors or validation issues.

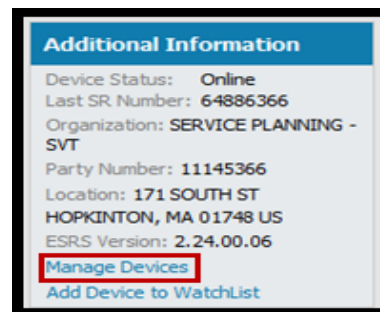


Figure 133 Selecting Manage Devices

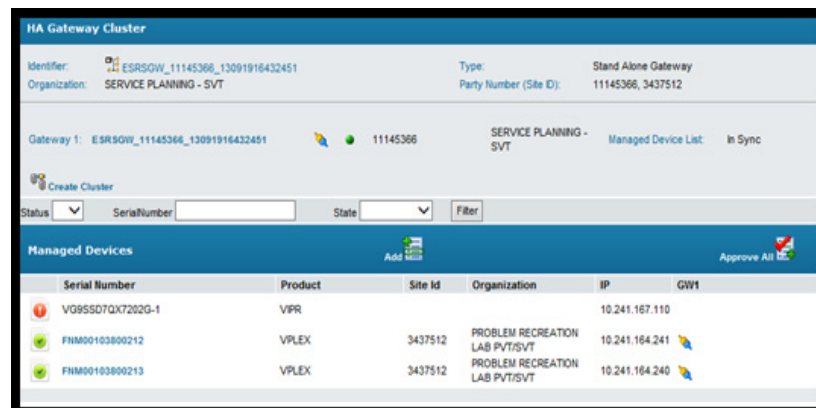


Figure 134 Managed Device List

3. Note the serial number of the virtual edition server, as shown in [Figure 135 on page 115](#). This is the server to which you will be migrating Managed Devices.



Figure 135 Virtual edition serial number

4. From the SRS Portal serial number page, click **Manage Devices**, as shown in [Figure 136 on page 115](#).

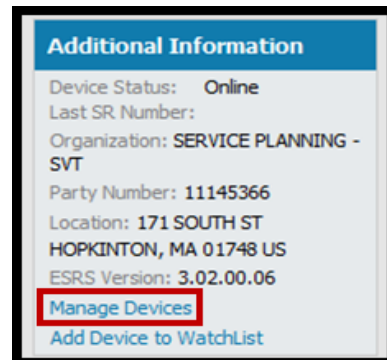


Figure 136 Manage Devices

5. Click **Migrate Gateway**, as shown in [Figure 137 on page 115](#).

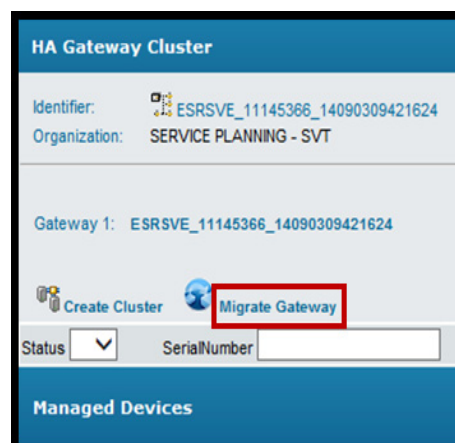


Figure 137 Selecting Migrate Gateway

6. In the Migrate Gateway dialog box, type your existing Gateway serial number, and then click **Migrate**, as shown in [Figure 138 on page 116](#). The output that you receive will be based on the number of managed devices. This process will also pick up and migrate any existing errors.

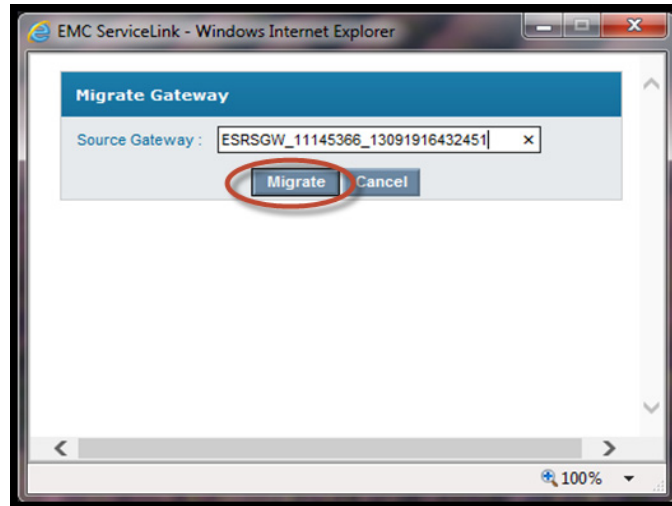


Figure 138 Migrate Gateway dialog box

7. When the process is complete, click **Done** to close the dialog box, as shown in [Figure 139 on page 116](#).

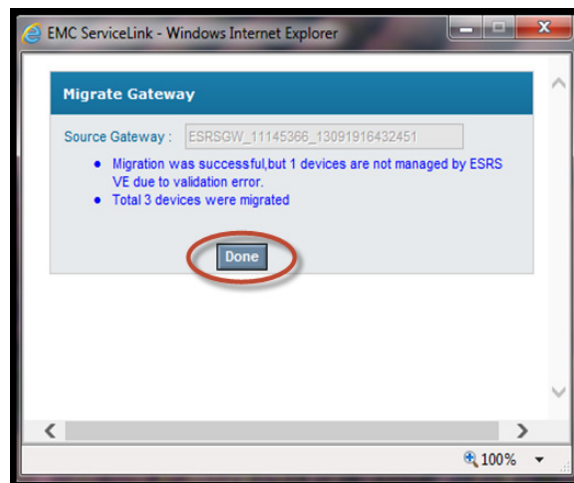


Figure 139 Clicking Done

IMPORTANT

You must manually resolve any validation errors on the SRS Deployment in order for the migration to complete.

8. When the migration process is complete, you may have to wait a brief period while the sync process occurs, or you can select the **Sync Now** button on SRS to force an immediate sync process to occur, as shown in [Figure 140 on page 117](#).

Once the Sync process has occurred, devices are ready for standard SRS activities such as Remote Device Access as well as Call Home Configuration and Testing.

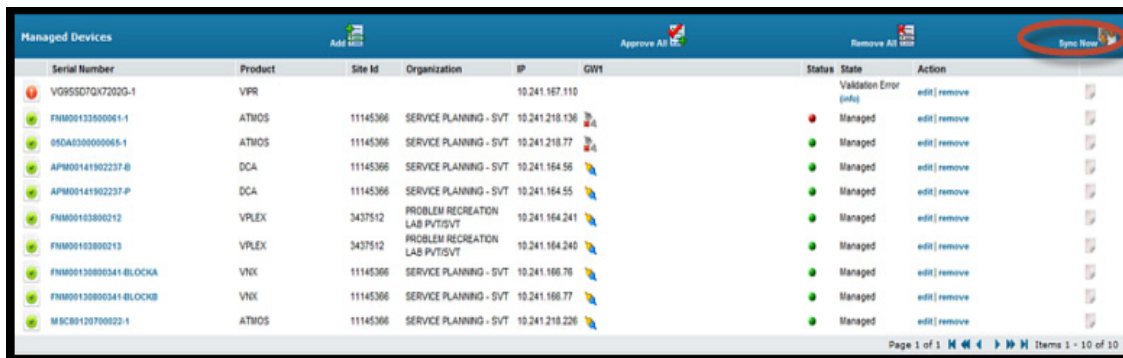


Figure 140 Selecting Sync Now

On the SRS Web UI, you can see that the devices are managed.

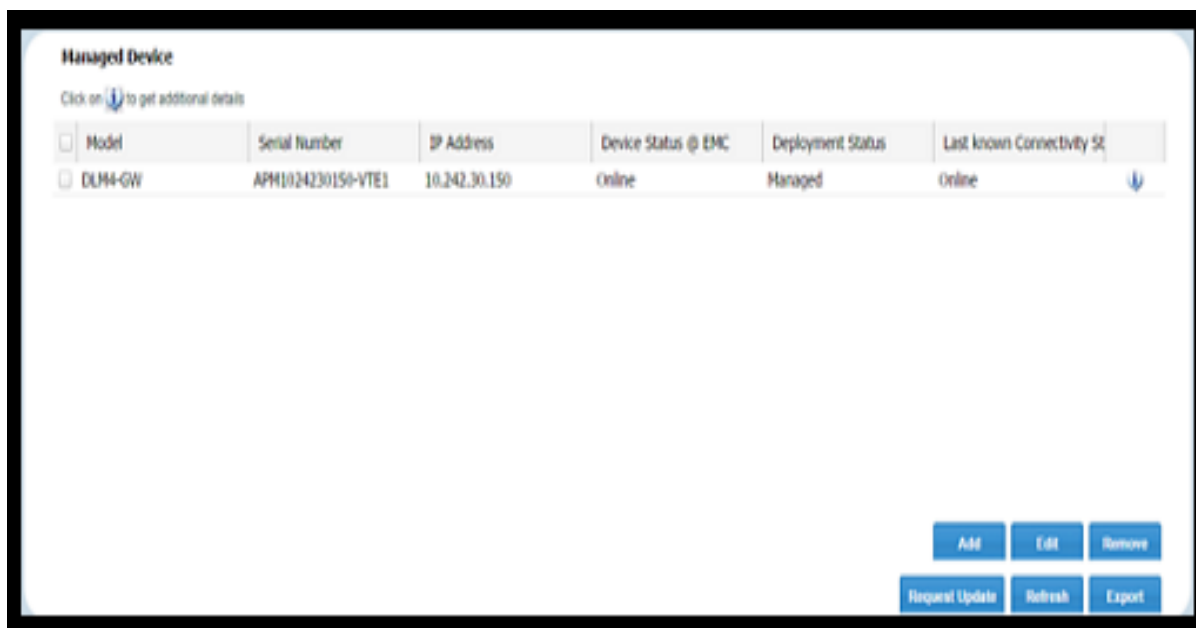


Figure 141 Viewing deployment status

- Go to the Managed Devices page for the SRS2 Gateway or one of the gateways in a Gateway Cluster that was used as the source for the migration.

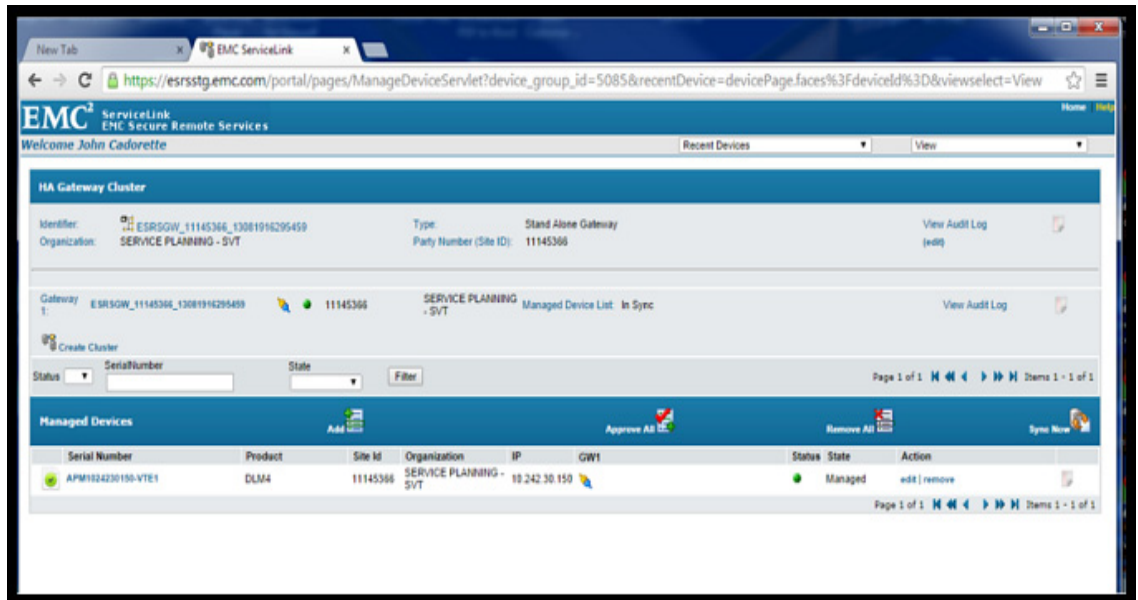


Figure 142 Managed Devices page

- Remove all of the managed devices by clicking the **Remove All** button. A confirmation dialog box appears.

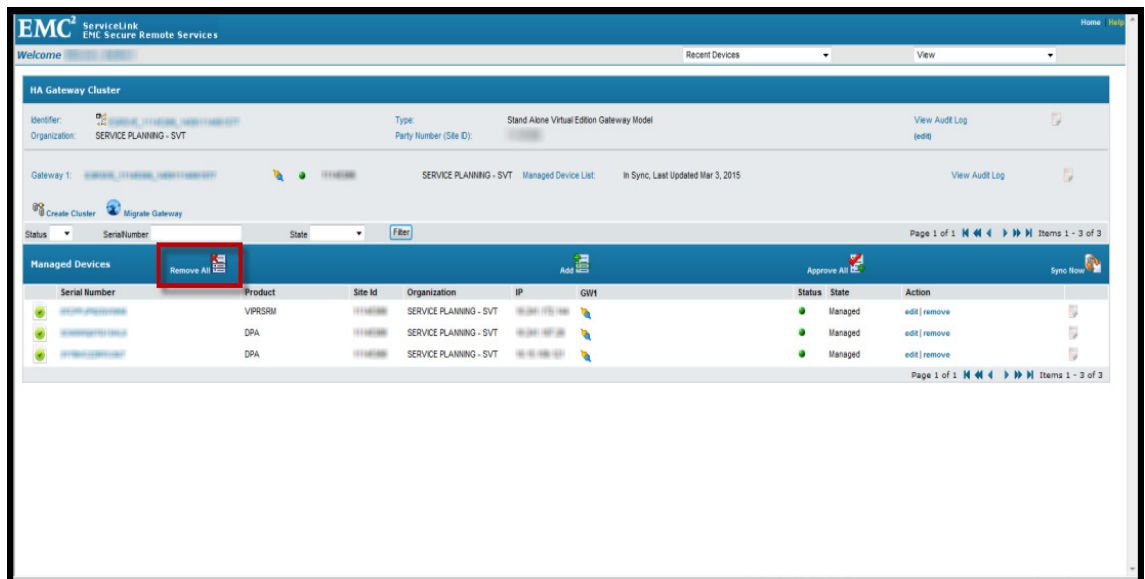


Figure 143 Selecting Remove All button

11. In the confirmation dialog box, click OK.

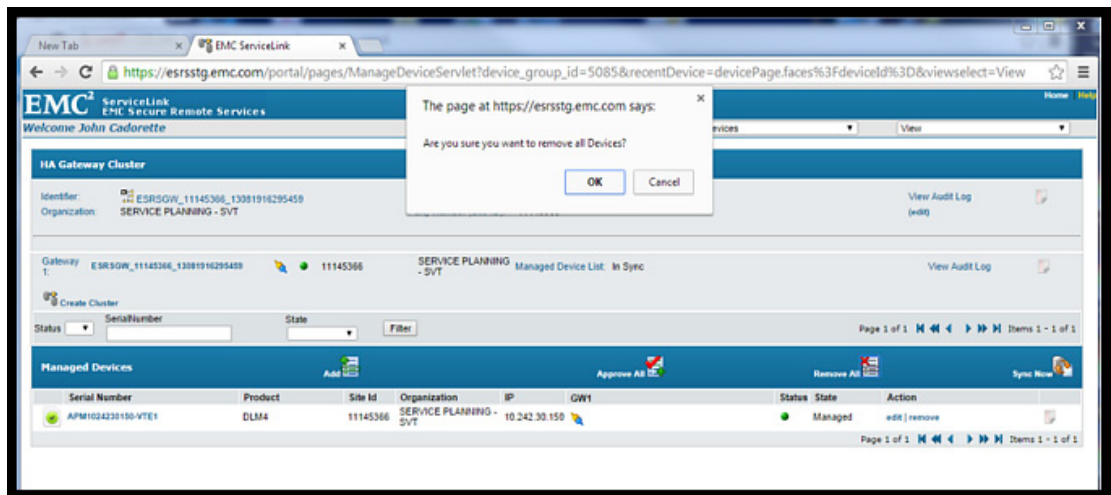


Figure 144 Confirming deletion

The status of the managed devices changes to Pending Delete.

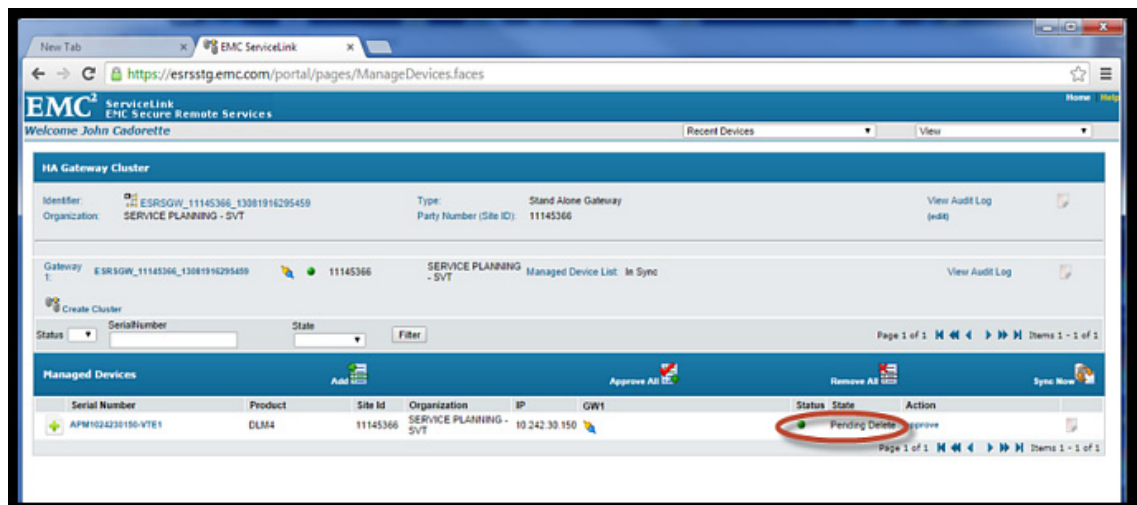


Figure 145 Pending Delete

12. Click the **Approve All** button, and then click **Sync Now**.

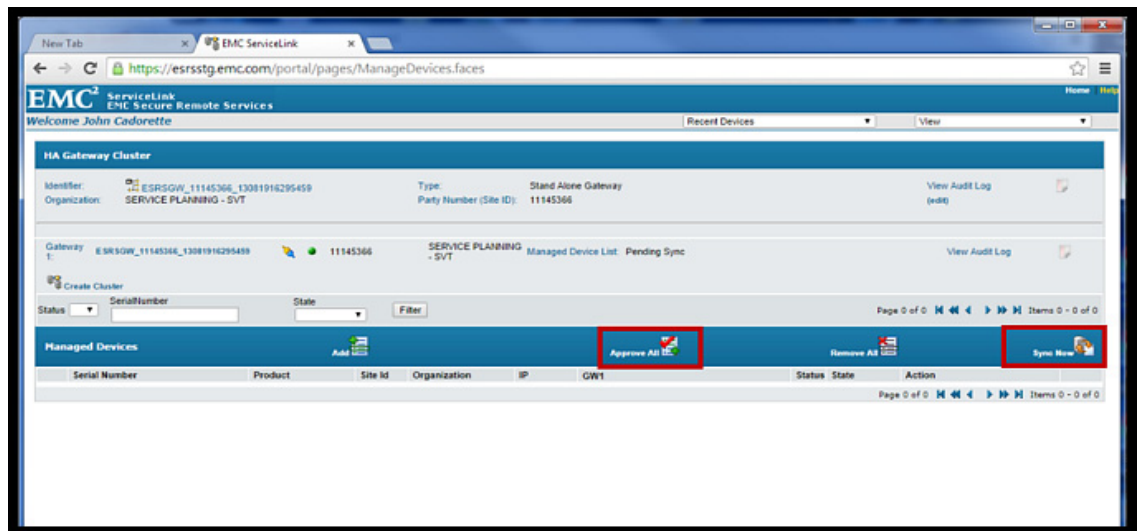


Figure 146 Selecting Approve All and Sync Now

13. Once the device removal and sync are complete, go to the Gateway Page and set the Gateway Offline. If this is an SRS2 Gateway Cluster, you also need to set any peer gateways in the Cluster offline as well.
14. If SRS 3.xx is NOT using the same IP address as the source gateway, then all of the migrated devices MUST be reconfigured to the SRS IP Address for Connect Home. Once this is completed, you can uninstall the gateway code and power-off or reprovision the host(s).

APPENDIX B

Network Configuration Using YaST

This appendix describes how to implement a network configuration using YaST for the SRS Release 3.xx.

- ◆ Procedure 122

Procedure

To implement network configuration using YaST:

Note: Requires shell or console access to the shell of the SRS.

1. From an ssh session or a console session of the SRS shell, log in using the root credentials established during the first boot configuration of the install process, as shown in [Figure 147 on page 122](#).

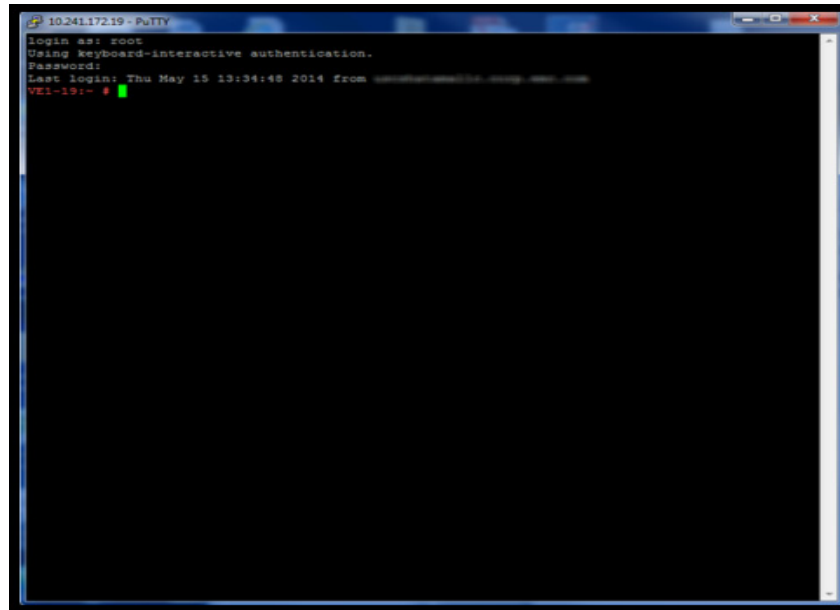


Figure 147 Logging in as root

2. At the prompt, type **yast2**, and then press **Enter**. The YaST2 user interface appears, as shown in [Figure 148 on page 122](#).

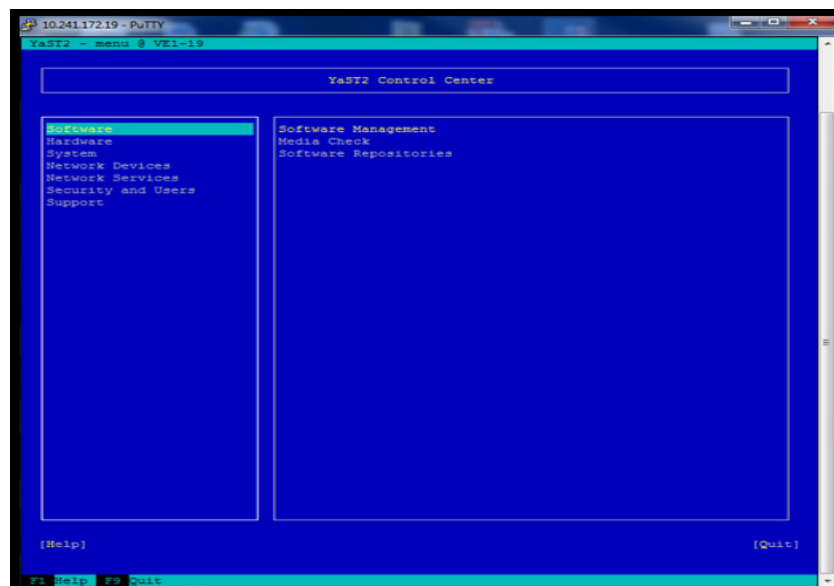


Figure 148 User interface

3. Select **Network Devices**, as shown in [Figure 149 on page 123](#).

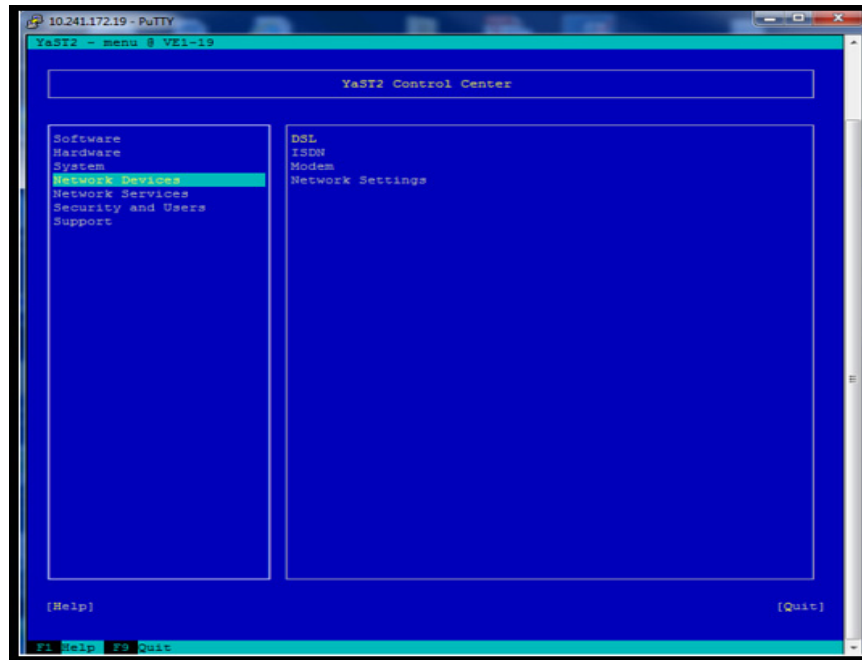


Figure 149 Selecting Network Devices

4. Use the **Tab** key to navigate to the right-side pane, and then select **Network Settings**, as shown in [Figure 150 on page 123](#).

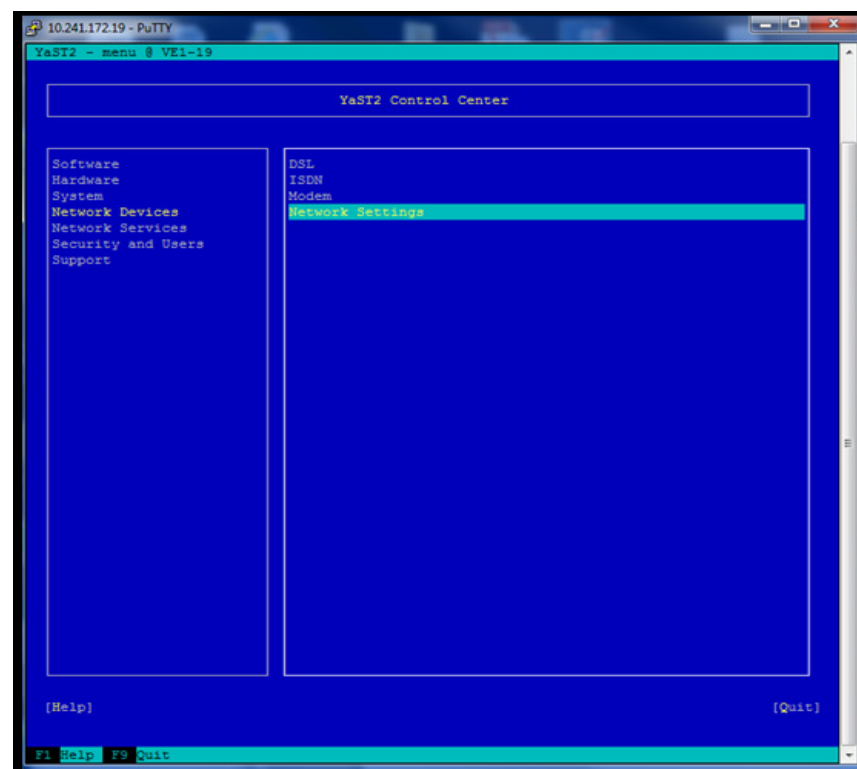


Figure 150 Selecting Network Settings

5. Press **Enter**. The Network Settings screen appears, as shown in [Figure 151 on page 124](#).

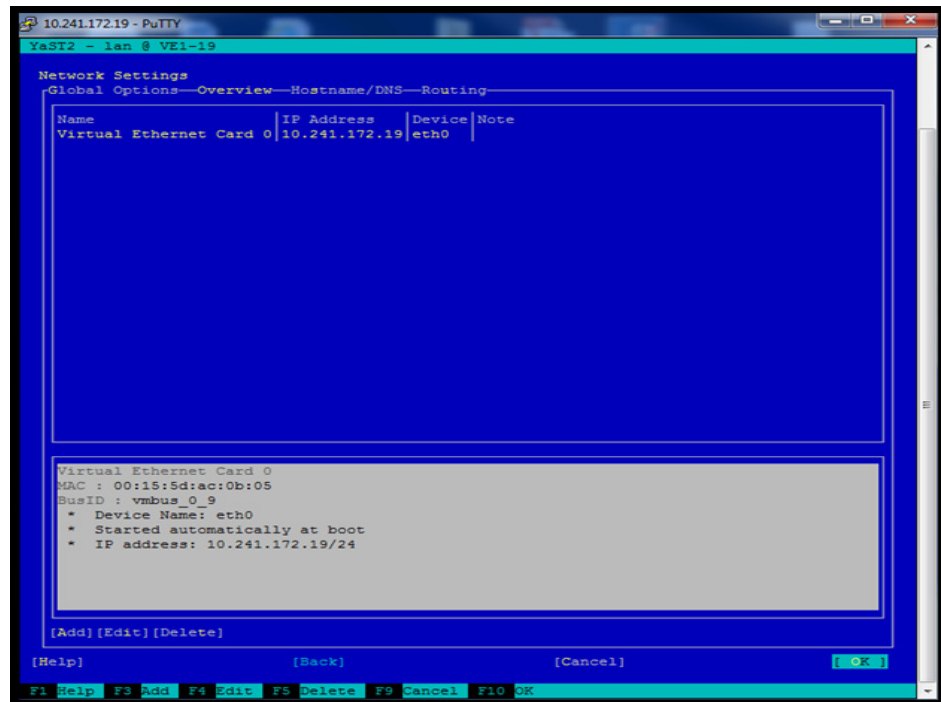


Figure 151 Network Settings screen

6. In the Network Settings screen, you can perform the following:
 - a. Edit the IP address or host name (as shown in [Figure 152 on page 124](#)) by using the **Tab** key, **Alt-I**, or **F4**. When done, use **Tab**, **Alt-N**, or **F10** for Next.

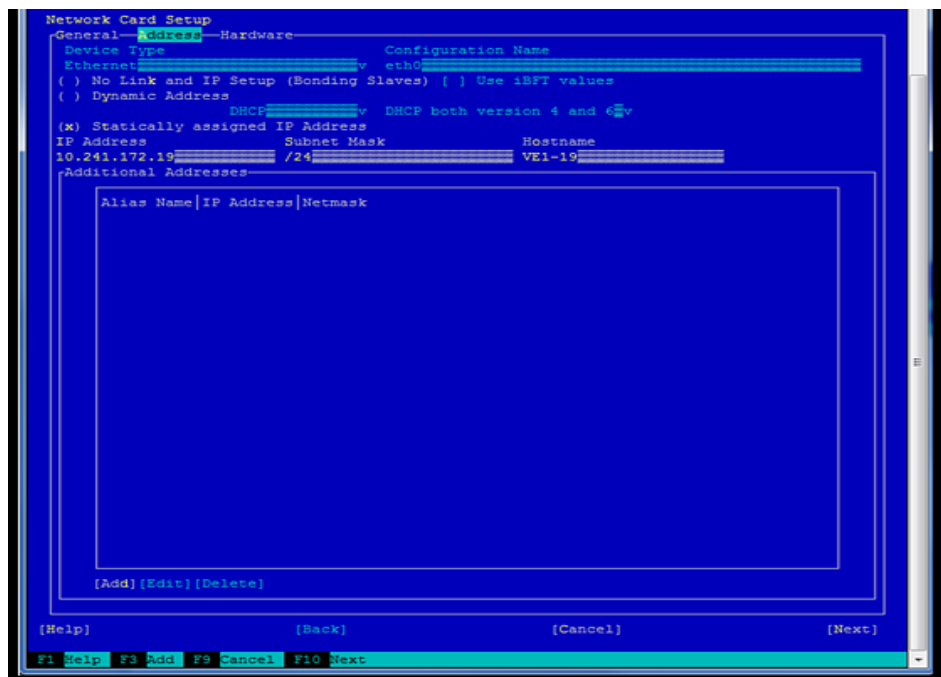


Figure 152 Network Card Setup screen

- b. Edit the DNS configuration using **Alt-S**, as shown in [Figure 153 on page 125](#). If editing is complete, then use **Tab**, **Alt-O**, or **F10** for **OK**. All edits to the network configuration will be written to the system configuration.

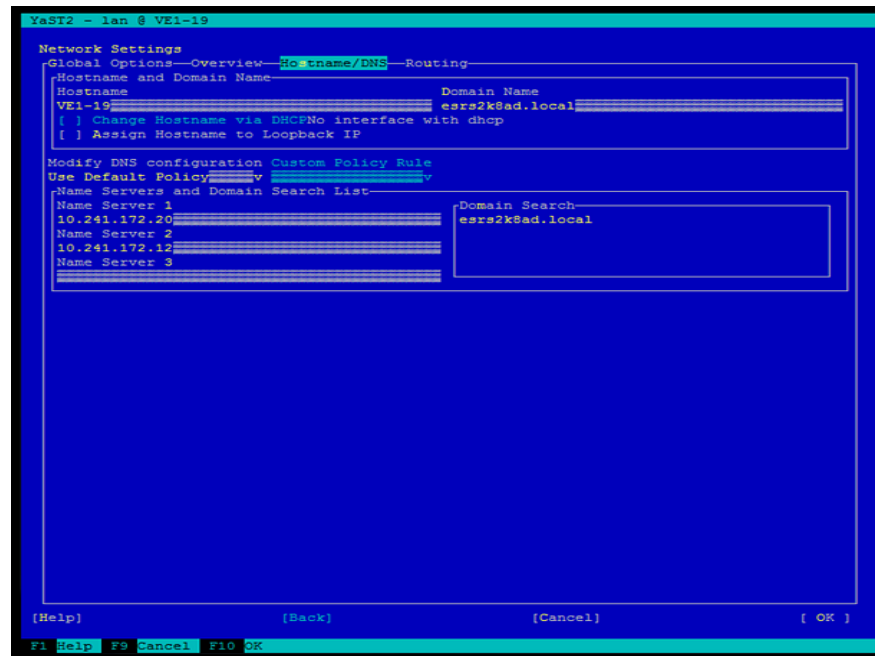


Figure 153 Changing DNS configuration

- c. Edit the default route/gateway using **Alt-U**, as shown in [Figure 154 on page 125](#). When editing is complete, use **Tab**, **Alt-O**, or **F10** for **OK**. All edits to the network configuration are written to the system configuration and the network services become activated, as shown in [Figure 155 on page 126](#).

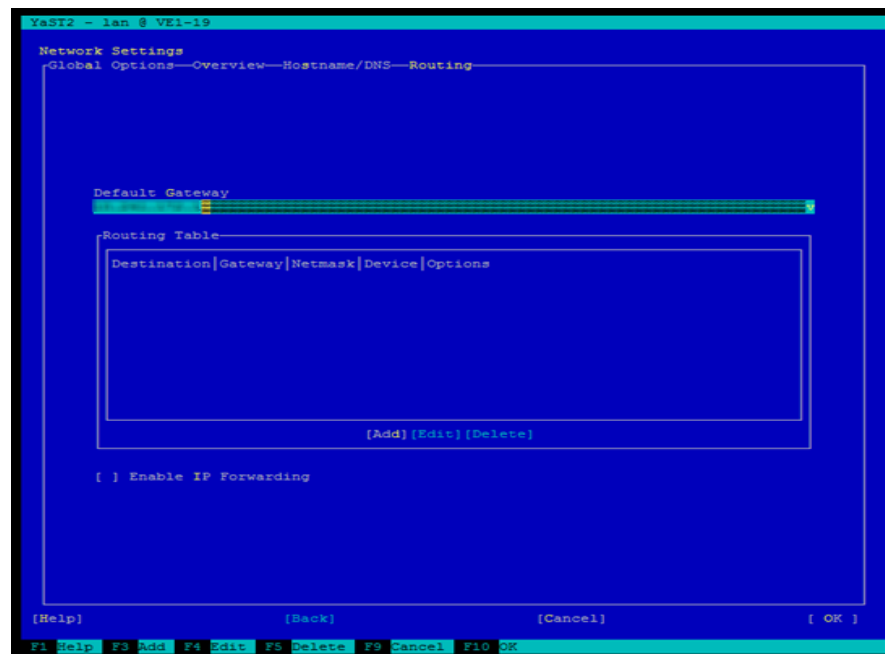


Figure 154 Editing the default gateway

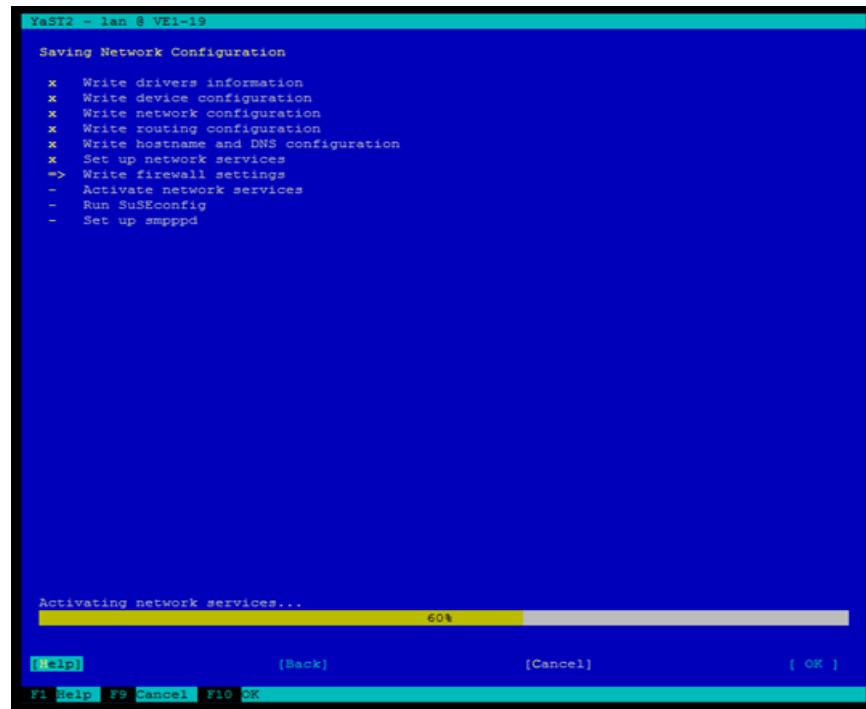


Figure 155 Saving network configuration

7. If you need to set the date and time, then select **System** on the left-side pane, tab to the right-side pane, select **Date and Time** as shown in [Figure 156 on page 126](#), and then press **Enter**. The Clock and Time Zone screen appears.

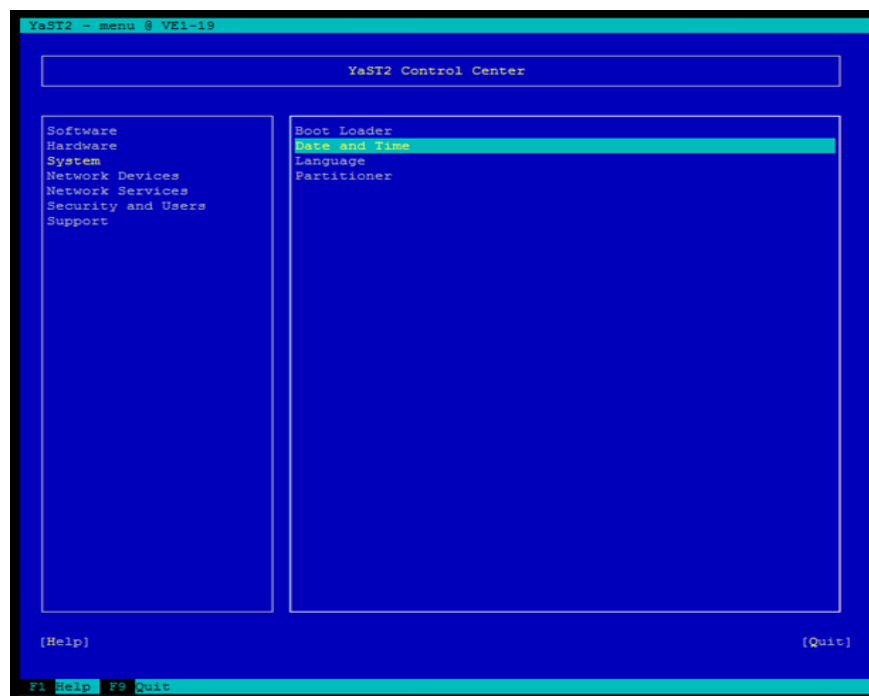


Figure 156 Setting date and time

8. In the Clock and Time Zone screen, make the desired changes, as shown in [Figure 157 on page 127](#). When you are done, use **Tab**, **Alt-O**, or **F10** for **OK**. This step takes you to the original page of the YaST2 Tool, as shown in [Figure 158 on page 127](#).

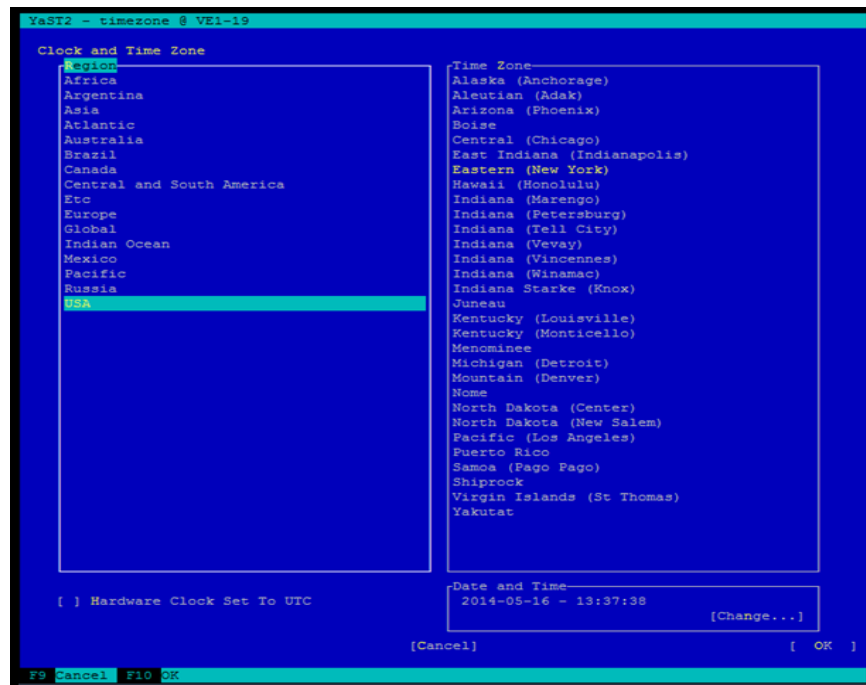


Figure 157 Clock and Time Zone screen

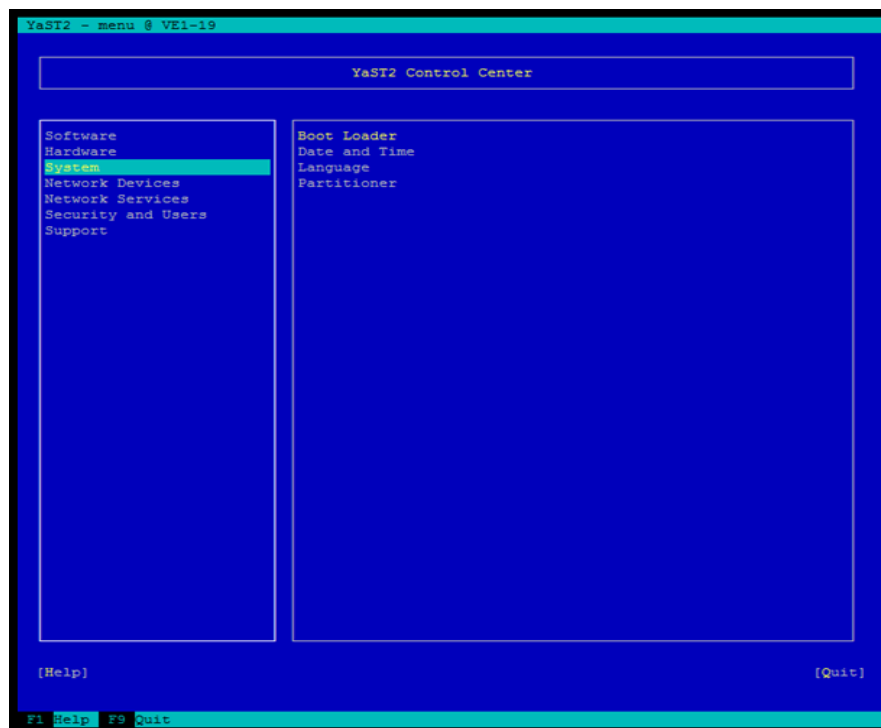


Figure 158 YaST2 Control Center

9. Use **Tab**, **Alt-Q**, or **F9** to **Quit**. You return to the command prompt.
10. Test the network connectivity using the normal tools process (Ping, dig, etc.).

APPENDIX C

IP Addresses used by SRS

This appendix lists the article that provides the IP addresses used by the Secure Remote Services Virtual Edition.

- ◆ [Key information](#) 130
- ◆ [Article access](#) 130

Key information

Article Number: 0000494729

Version: 1

ID: EMC238467

Domain: EMC1

Solution Class: 3.X Compatibility

Note: Always check [support . emc . com](https://support.emc.com) for the latest version of this article as it may have been updated.

Article access

The following is a Primus(R) eServer solution.

Article Title: What IP addresses are used by the EMC Secure Remote Services IP Solution?

This is from KB article 494729. To access this article, go to:

<https://support.emc.com/kb/494729>

APPENDIX D

Dell EMC Customer Environment Check Tool for SRS v3.x

This appendix describes how to obtain, install, and operate the Customer Environment Check Tool (CECT) for the SRSv3 (SRS v3.xx). The CECT for SRS verifies that a candidate server meets the hardware, software, and network configuration requirements for successful SRS software installation.

This appendix contains the following topics:

- ◆ [Customer Environment Check Tool overview](#) 132
- ◆ [Required CECT test resolution](#) 132
- ◆ [Installation](#) 134
- ◆ [Operation](#) 134

Customer Environment Check Tool overview

SRSv3 has specific requirements for hardware, software, and network configurations. If the customer's environment does not meet one or more of the requirements listed in Table 6, then various problems may occur during and after the SRSv3 software installation.

The Customer Environment Check Tool (CECT) for SRSv3 is provided as part of the SRS software base image.

The CECT tests the customer's environment to determine if it meets all of the configuration requirements necessary for successful SRS software installation.

When you run the CECT for the SRSv3 virtual host operating system, the CECT performs a series of automated system requirement tests on the server. Each test verifies the server's compliance with a specific system requirement. CECT then assigns a Passed or Failed status to each test result.

The CECT is also used to test connectivity from the SRSv3 server to the managed or prospective devices, and to confirm that the devices are reachable on all of the ports necessary for Dell EMC to be able to properly support the devices. The connectivity tests for devices should be run before installing the SRSv3 to ensure that the network environment has been properly configured.

Each time you run a new series of tests, CECT creates a new report file and stores all the test results in that file. You can then use the CECT application, Notepad, or WordPad to view the report files for all of the test series that you have run on a server.

Note: You must install and run the CECT application on every gateway client server. You must verify that each server passes the required CECT tests prior to your SRSv3 installation date.

Note: Some ports may fail the connectivity test. This is due to the existence of secondary connections, and does not affect the overall test result.

Note: You must supply a copy of the test results to your Dell EMC Global Services professional before the SRSv3 software installation is performed.

Required CECT test resolution

The CECT checks that your SRSv3 server and environment meet specific requirements. The CECT requirements are a subset of the complete requirements of the SRS servers.

To successfully run the SRSv3 software installation program, each target server must pass the tests required for its server type, as specified in the following table.

Note: If any required tests show a Failed status, you must resolve those failures prior to your SRS installation date.

Table 3 CECT test failure resolution

Test Name	Notes
Gateway Environment Tests	Required tests must pass on SRSv3 server.
Memory	Required: At least 4 GB RAM.
Comm	Required: One (dual) 10/100 Ethernet adapters (NIC cards), 1 Gb preferred.
Free Disk Space	Required: At least 60 GB
Processor Speed	Required: At least 2.2 GHz total speed per processor (one or more processors).
	Note: CPU must support SSE2 Instruction Set.
Network Connectivity Tests	Required tests must pass on SRSv3 server. Required: SRS server must pass either or both the HTTPS or the TCP/IP connection tests to proceed with SRS software installation. The Dell EMC Registration Authority Connect and Dell EMC Secure Remote Support Connect tests can be performed using either the HTTPS protocol or a simple TCP / IP connection to the Dell EMC application servers.
Dell EMC Registration Authority Connect	Required: SRSv3 server can connect to Dell EMC servers over TCP port 443.
Dell EMC Secure Remote Support Connect	
Dell EMC Registration Authority Connect HTTPS	HTTPS tests may fail for any of several reasons - for example, time-out and proxy configuration / authorization errors. You can test connections by using a local Web browser to open the URLs provided in the detailed test results.
System Applications Tests	Required tests must pass on SRSv3 server.
Simple Mail Transport Protocol	Required: SMTP enabled on SRSv3 server and configured. Optional: FTP enabled on SRSv3 server and configured as specified in the SRSv3 Server Preparation section in the Secure Remote Services for SRSv3 Operations Guide.
File Transfer Service	Optional: FTP enabled on SRSv3 server and configured as specified in the SRSv3 Server Preparation section in the Secure Remote Services for SRSv3 Operations Guide.

Installation

The Customer Environment Check Tool for SRSv3 is part of the base image that is installed and is available in the command shell of the virtual host for use after the first boot process is completed. No installation is needed; however, you must accept the License Agreement on the first use of the tool.

Operation

CECT provides a suite of tests that you can run on a candidate SRSv3 server in order to verify that the target server meets the hardware, software, and network configuration requirements for a successful installation of the SRSv3 software.

To run a series of tests using the CECT application:

1. Launch the CECT application.
2. Accept the End User License Agreement.
3. Enter your customer site and contact information.
4. Select the tests you want to run.
5. Execute the test run.
6. View the test results from the log file in the server Logs directory.

Launching the Customer Environment Check Tool (CECT)

Note: If you are in the CECT directory, you must precede the command with a ./ or if in another directory, provide the full path to the CECT executable. You must also read and accept the license agreement in order to be able to use the tool. Also, remember that all SRSv3 commands and arguments are case sensitive.

1. Launch the CECT application (from the attached log file, edit as needed):

```
[root@localhost CECT]# ./CECT.sh
```

End user's license agreement appears as follows:

```
End User License Agreement
1 - Display the license
2 - Accept the license
3 - Do not accept the license
Select an option to edit: 1
EMC Secure Remote Support (ESRS) Software License
Agreement
```

```
IMPORTANT    PLEASE READ CAREFULLY
```

```
This EMC Secure Remote Support Software contains
computer programs and other proprietary material and
information, the use of which is subject to and
expressly conditioned upon acceptance of this EMC
Secure Remote Support Software License Agreement.
This EMC Secure Remote Support Software License
Agreement (the Agreement) is a legal agreement between
EMC Corporation, with a principal office at 176 South
Street, Hopkinton, MA 01748 USA ("EMC"), and you and
the organization on whose behalf you are accessing this
Agreement and Software (the Licensee), and governs
Licensee's access to, downloading of, and use of any
and all components, associated media, printed
materials,
11.9 Force Majeure Neither party shall be liable under
this Agreement because of a failure or delay in
```

performing its obligations hereunder on account of any force majeure event, such as strikes, riots, insurrection, terrorism, fires, natural disasters, acts of God, war, governmental action, or any other cause which is beyond the reasonable control of such party.

2. Accept the license agreement as follows:

```
End User License Agreement
1 - Display the license
2 - Accept the license
3 - Do not accept the license
Select an option to edit: 2
EMC SRS CECT 2.26.00.06
```

3. Fill in the required customer contact information, indicated by an asterisk (*), beginning with **Customer Name**. The following is an example:

```
Fill in the customer contact information
Checking customer information
**Missing required customer information.**
Site Information
1 - *Customer Name:
2 - Address:
3 - City:
4 - State:
5 - Country:
6 - *Contact name (First, Last):
7 - Department:
8 - Phone:
9 - *Email:
* Required
Select an option to edit: 1
Customer Name: EMC Corporation
```

4. Fill in **Contact Name** (First, Last) as shown below:

```
Site Information
1 - *Customer Name: EMC Corp
2 - Address:
3 - City:
4 - State:
5 - Country:
6 - *Contact name (First, Last):
7 - Department:
8 - Phone:
9 - *Email:
* Required
Select an option to edit: 6
Contact Name: John Smith
```

5. Fill in the **Email** address as follows:

```
Site Information
1 - *Customer Name: EMC Corp
2 - Address:
3 - City:
4 - State:
5 - Country:
6 - *Contact name (First, Last): John Cadorette
7 - Department:
8 - Phone:
9 - *Email:
* Required
```

```
Select an option to edit: 9
Email: john.smith@emc.com
```

6. Save the data to continue. The following serves as an example:

```
Site Information
1 - *Customer Name: EMC Corp
2 - Address:
3 - City:
4 - State:
5 - Country:
6 - *Contact name (First, Last): John Cadorette
7 - Department:
8 - Phone:
9 - *Email: john.cadorete@emc.com
10 - Save data and return to the previous menu
* Required
Select an option to edit: 10
```

Selecting tests to be run

After you have entered your site and contact information in the Site Information screen, you are ready to select the specific tests to be performed during the test run.

To select CECT tests to be run:

1. From the main CECT application screen, select option 2. The following serves as an example:

```
[root@localhost CECT]# ./CECT
EMC SRS CECT 2.26.00.06

Checking customer information
Required customer information found

Main Menu
1 - Display/Edit Customer Info
2 - Gateway Tests Menu
3 - Display Log Files
4 - Display the license
5 - Exit
Select an option: 2
```

2. Select option 2. The Gateway Tests Menu appears, as shown in [Figure 159 on page 136](#).

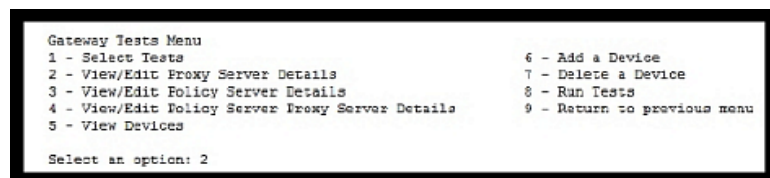


Figure 159 Gateway Tests Menu

3. To select the CECT tests, select option 1. The SRS Server Environment Tests screen appears, as shown in [Figure 160 on page 137](#).

```

SRS Server Environment Tests
1 - Memory
2 - Free Disk Space
3 - Processor Speed
4 - Processor SSE2 Instruction Set
5 - Operating System Version
6 - Network Interface Card
7 - Required Local User Accounts
8 - Select All Environment Tests

Network Connectivity Tests
9 - SRS Client Provisioning Connection (HTTPS)
10 - SRS Core Connection (HTTPS)
11 - SRS Client Provisioning Connection (TCP)
12 - SRS Core Connection (TCP)
13 - SRS Remote Access Connection (HTTPS)
14 - SRS Remote Access Connection (TCP 443)
15 - SRS Remote Access Connection (TCP 8443)
16 - SRS to Policy Server Connection
17 - Device Application and Port Connection Test
18 - Select All Network Connectivity Tests

Linux Service/Daemon Tests
19 - File Transfer Protocol
20 - Simple Mail Transport Protocol
21 - SRS Gateway and Device Client
22 - SRS Watchdog
23 - SRS HTTPS Listener
24 - Select All Service/Daemon Tests

25 - Return to previous menu

Separate multiple tests with a comma
Select an option: █

```

Figure 160 SRS Server Environment Tests

4. Decide which tests you want to include in this test run. The Server Environment Tests screen lets you select options from the following test groups:
 - **SRS Server Environment Tests** — Verifies that the Gateway Client server hardware meets the minimum requirements and verifies that the correct operating system is installed on the server.
 - **Network Connectivity Tests** — Verifies that all required network connections have been configured properly, so that communications are enabled between the ESRS server and EMC and between the ESRS and Policy Manager servers. The CECT Network Connectivity Tests were updated to ensure that all HTTPS and TCP tests are run against the ESRS production environment as well as the Disaster Recovery service at EMC.
 - **SRS Service/Daemon Tests** — Verifies that the Gateway Client server has FTP and SMTP services enabled and configured properly; has the required directory structure in place on the installation root drive; has the required user accounts configured properly; and has the proper ports open for communication with each application installed on each of its managed devices.
5. To select multiple tests, separate the tests with a comma.
6. To run all tests, enter **8, 18, 24**.

Note: If you select all tests prior to installing the gateway and/or Policy Manager, some tests will fail. These failures are actually false failures as the prerequisites were not met.

For example:

- If you are using a Policy Manager, then it must be installed and the information must be configured in the CECT for the test to pass successfully.
- If you are using a Proxy server, then information about the Proxy server also needs to be entered in the CECT before the tests are run.
- These configuration steps must be performed in the Gateway Tests Menu using options 2, 3, 4, 6, and 7.

7. Return to the Gateway Tests Menu, as shown in [Figure 161 on page 138](#), and select option 8 to run the tests you selected.

Note: Selection 1 must be done before selection 8.

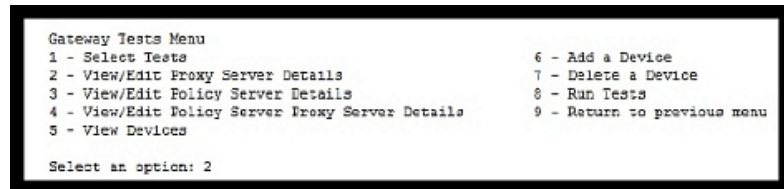


Figure 161 Gateway Tests Menu - Running Tests

8. The test results from your current test are automatically saved to a CECT test log file located in the Gateway CECT/Logs directory. Refer to [“Viewing test result log files” on page 138](#) for more details.

Viewing test result log files

You can view the current or previous CECT test log files. To view the log file from your current CECT test:

1. Change to the **opt/emc/esrs/Logs/CECT/Logs** directory.
2. Locate the most current test based on the date stamp of the filename. For example, **CECT_EMCCorporation_20130117093501.log**.
3. Use standard SRS edit tools commands (view, vi, cat, and so forth) to view the output logs.

For example:

```

[root@localhost Logs]# view "CECT_EMCCorporation_20130117101807.log"
10/17/2013 10:20:26 AMEMC Secure Remote Support Gateway Check
Verification
Tests
10/17/2013 10:20:26 AM
10/17/2013 10:20:26 AMRun Date: 10/17/2013 10:20:26 AM
10/17/2013 10:20:26 AMCECT Version: 2.26.00.06
10/17/2013 10:20:26 AMUser Name: root
10/17/2013 10:20:26 AMMachine Name: localhost.localdomain
10/17/2013 10:20:26 AMOS Version: Red Hat Enterprise ESRS Server
release 6.2
(Santiago) Red Hat Enterprise ESRS Server release 6.2 (Santiago)
10/17/2013 10:20:26 AMShell: /bin/bash
10/17/2013 10:20:26 AMCurrent Directory: /opt/emc/esrs2/CECT
10/17/2013 10:20:26 AM
*****
*****
10/17/2013 10:20:26 AMSite and Customer Contact Information:
10/17/2013 10:20:26 AM
10/17/2013 10:20:26 AMCustomer Name: EMC Corp
10/17/2013 10:20:26 AMAddress:
10/17/2013 10:20:26 AMCity:
10/17/2013 10:20:26 AMState:
10/17/2013 10:20:26 AMCountry:
10/17/2013 10:20:26 AMContact Name: John Smith
10/17/2013 10:20:26 AMDepartment:
10/17/2013 10:20:26 AMPhone:
10/17/2013 10:20:26 AMEmail: john.smith@emc.com
  
```

- ```

10/17/2013 10:20:26 AM

10/17/2013 10:20:26 AMGateway Test Results
10/17/2013 10:20:26 AM

10/17/2013 10:20:26 AM

10/17/2013 10:20:26 AM

10/17/2013 10:20:26 AM
10/17/2013 10:20:26 AMTEST NAME : EMC SRS Policy Manager Pre
Installation
Connect Test.STATUS : Failed
10/17/2013 10:20:26 AM
@
"CECT EMC Corp_20131017101807.log" [readonly] 76L, 4679C

```
4. View the CECT test results in the log file. You can scroll down to view more results.
  5. You can then open and view the other log files from your current or previous test runs.

## Run log example

The following example provides additional content that you need to update the command line section.

```

===== PuTTY log 2014.08.29 11:15:12 =====
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 27 17:06:00 2014 from usxxcadorjllc.corp.emc.com

2k12-V-Grissom-103:~ # cd opt
-bash: cd: opt: No such file or directory
2k12-V-Grissom-103:~ # cd /opt
2k12-V-Grissom-103:/opt # ls
ADG connectemc connectemcVE esrs esrsve httpd httpdR httpdftp httpdlistener lb vmware
2k12-V-Grissom-103:/opt # cd esrsve
2k12-V-Grissom-103:/opt/esrsve # ls
alarm configtool deviceutility sysmon vfabric-config
auditlogging connectivityreport gateway usermanagement webcontent
auth cst jcemc utilities webuimgmt-util
bin dataitems keepalive uuid
cect devicemanagement provisioning vappconfig
2k12-V-Grissom-103:/opt/esrsve # cd cect
2k12-V-Grissom-103:/opt/esrsve/cect # ls -ailh
total 4.7M
49233 drwxr-xr-x 2 root root 4.0K Aug 20 02:57 .
49158 drwxr-xr-x 25 esrsve esrsve 4.0K Aug 27 16:47 ..
49578 -rwxr-xr-x 1 root root 4.3M Aug 20 05:06 CECT
49579 -rwxr-xr-x 1 root root 78 Aug 20 05:06 CECT.sh
49580 -rw-r--r-- 1 root root 19K Aug 20 05:06 LICENSE.txt
49581 -rw-r--r-- 1 root root 25K Aug 20 05:06 config.xml
49582 -rw-r--r-- 1 root root 321K Aug 20 05:06 license.pdf
2k12-V-Grissom-103:/opt/esrsve/cect # ./CECT.sh

End User License Agreement
1 - Display the license
2 - Accept the license
3 - Do not accept the license
Select an option to edit: 2

```

```

```

Please read the license before accepting it.

\*\*\*\*\*

End User License Agreement

- 1 - Display the license
- 2 - Accept the license
- 3 - Do not accept the license

Select an option to edit: 1

EMC Customer Environment Check Tool Software License Agreement

IMPORTANT PLEASE READ CAREFULLY

This EMC Customer Environment Check Tool contains computer programs and other proprietary material and information, the use of which is subject to and expressly conditioned upon acceptance of this EMC Customer Environment Check Tool Software License Agreement. This EMC Customer Environment Check Tool License Agreement (the "Agreement") is a legal agreement between EMC Corporation, with a principal office at 176 South Street, Hopkinton, MA 01748 USA ("EMC"), and you and the organization on whose behalf you are accessing this Agreement and Software (the "Licensee"), and governs Licensee's access to, downloading of, and use of any and all components, associated media, printed materials, documentation, and programming accessed via the EMC software (the "Software"). This Agreement also applies to any subsequent versions of the Software made available by EMC (at EMC's sole discretion) and downloaded, installed or used by Licensee.

By clicking on the "Agree" or similar button or check box set forth below, or by downloading, installing, or using the Software, or authorizing any other person to do so, you are representing to EMC that (i) you are authorized to legally bind the Licensee, and (ii) you are agreeing on behalf of the Licensee that the terms of this Agreement shall govern the relationship of the parties with regard to the Software.

If you do not have authority to agree to the terms of this Agreement, or do not accept the terms of this Agreement, click on the "Cancel", "Reject" or other similar button below and/or immediately cease any further attempt to install, download or use this Software for any purpose, and remove any partial or full copies made from this Software. In such event, no access to, or authorization to download or use the Software, is granted by EMC.

EMC and Licensee enter into this Agreement and this Agreement shall become effective on the date on which Licensee clicks on the "Agree" button described above or downloads, installs or uses the Software, whichever occurs first (the "Effective Date").

NOW, THEREFORE, in consideration of the premises and obligations contained herein, it is agreed as follows:

## 1.0 DEFINITIONS

1.1 "Affiliate" means a legal entity that is controlled by, controls or is under common "control" of EMC. "Control" means more than 50% of the voting power or ownership interests.

Press the <enter> key to continue

1.2 "Equipment" means the Licensee owned storage devices, systems, central processing units ("CPU") or management station equipment that the Software was designated to operate on or with.

1.3 "Confidential Information" means the Software and any and all information or materials provided by one party to the other which are in tangible form and labeled "confidential" or the like, or, if disclosed orally, are identified as being confidential at the time of disclosure and are followed up within two (2) weeks in a tangible form that is appropriately labeled, but shall not include information or materials that (i) were, on the Effective Date, generally known to the public; or (ii) become generally known to the public after the Effective Date other than as a result of the act or omission of the receiving party; or (iii) the receiving party lawfully received from a third party without that third party's breach of agreement or obligation of trust; or (iv) are independently developed by the receiving party without use of or reference to disclosing party's Confidential Information; or (v) were rightfully in the receiving party's possession without an obligation of confidentiality prior to receipt from the disclosing party.

## 2.0 PURPOSE AND CONFIDENTIALITY

2.1 Licensee shall use the Software solely for Licensee's internal business purposes and in accordance with EMC's instructions and documentation.



2.2 Licensee may use the Software on each item of applicable Equipment for the sole purpose described in Section 2.1 above and in a manner consistent with this Agreement.

2.3 The receiving party shall protect the other's Confidential Information for three (3) years after receipt thereof by means of the same standard of care as used by the receiving party to protect its own information of a similar nature and importance, and no less than reasonable care, except with respect to the Software which shall remain EMC Confidential Information until one of the exceptions specified in Section 1.2 above applies. The receiving party shall use Confidential Information only to fulfill its obligations or to exercise its rights hereunder, and shall disclose Confidential Information only to those persons in its organization who have a need to know such Confidential Information in the performance of their duties in connection herewith and who are bound by a written agreement to protect the confidentiality of such Confidential Information. The receiving party will promptly report to the disclosing party any actual or suspected breach hereof. Notwithstanding the foregoing, (a) EMC may disclose Confidential Information to an Affiliate for the purpose of fulfilling its obligations or exercising its rights hereunder as long as such Affiliate complies with the foregoing; and (b) either party may disclose Confidential Information if required by law provided the receiving party has given the disclosing party prompt notice prior to any such disclosure so that the disclosing party will have an opportunity to defend, limit or protect against such disclosure.

### 3.0 LICENSE TERMS

3.1 Subject to Licensee's compliance with the terms of this Agreement, EMC grants Licensee a personal, non-exclusive, non-transferable, and non-sublicensable license during the Term (as defined below) to download and use the Software solely on or in connection with the Equipment for which it was licensed. Such license commences on the Effective Date and shall terminate upon termination by EMC or Licensee in accordance with the terms and conditions specified in Section 7.0 (Termination) below ("Term"). Notwithstanding anything to the contrary, Licensee shall not, without EMC's prior written consent, use Software in a service bureau capacity, or copy, provide, disclose or otherwise make available Software in any form to anyone other than (i) Licensee's employees who shall use Software solely for Licensee's internal business purposes in a manner consistent with this Agreement, or (ii) the authorized EMC Velocity Services Implement partner selected by Licensee to install the applicable EMC products at the approved installation site who is only authorized to install the Software on the Equipment solely for Licensee's internal business purposes and in a manner consistent with this Agreement. Such employees described in sub-section 3.1(i) above and partner described in sub-section 3.1(ii) above are collectively referred to this Agreement as "License Personnel". Licensee shall be fully responsible to EMC for the compliance of License Personnel with the terms and conditions of this Agreement.

Press the <enter> key to continue

3.2 Software is licensed only. No title to, or ownership of, the Software is transferred to Licensee. Licensee shall reproduce and include copyright and other proprietary notices on and in any copies, including but not limited to partial, physical or electronic copies, of the Software. Neither Licensee nor Licensee personnel shall modify, decrypt, enhance, supplement, create derivative works from, reverse assemble, reverse engineer, reverse compile or otherwise reduce to human readable form the Software without EMC's prior written consent. All rights not expressly granted to Licensee hereunder are reserved by EMC.

### 4.0 DELIVERY AND INSTALLATION

4.1 Delivery of the Software is only by download from the applicable EMC website (where available), EMC provided media, or other EMC approved method.

4.2 EMC shall, as reasonably necessary, provide Licensee with information needed to initially download, install and use the Software.

### 5.0 SOFTWARE REFRESH

5.1 Licensee understands the importance of using only the latest, most current version of the Software and that changes and updates periodically occur. Licensee is solely responsible to return to the applicable EMC website and download the then current version of the Software. Licensee acknowledges and agrees that EMC is under no obligation to provide Licensee with any notification(s) concerning the availability of the latest, most current version of the Software.

5.2 Should Licensee experience problems using the Software, Licensee may contact EMC at the number or email address shown on the applicable EMC website for assistance

Press the <enter> key to continue

## 6.0 AUDIT RIGHTS

6.1 EMC (including its independent auditors) shall have the right to audit Licensee's usage of Software to confirm compliance with the agreed terms. Such audit is subject to reasonable advance notice by EMC and shall not unreasonably interfere with Licensee's business activities. Licensee will provide EMC with the support required to perform such audit and will, without prejudice to other rights of EMC, address any non-compliant situations identified by the audit. EMC, in its sole discretion, shall have the right to terminate this Agreement and/or the licenses granted hereunder in the event that such audit reveals that Licensee violated the terms of this Agreement or in the event that Licensee fails to promptly remediate any non-compliance with the terms of this Agreement as directed by EMC.

## 7.0 TERMINATION

7.1 If Licensee fails to perform any of its covenants, obligations or responsibilities under this Agreement, Licensee shall be in breach of this Agreement, and EMC shall, in addition to any other rights or remedies which may be available to EMC under this Agreement, at law or in equity, have the right, in EMC's sole discretion, to terminate this Agreement (and any or all related license(s) granted to Licensee) by providing written notice to Licensee, with such termination to be effective immediately. Additionally, either EMC or Licensee may terminate this Agreement for its convenience by providing at least thirty (30) days' prior written notice to the other party. Upon termination for any reason, Licensee shall cease all use and return or certify destruction of Software (including copies) to EMC. Any provision that by its nature or context is intended to survive any termination or expiration, including but not limited to provisions relating to confidentiality and liability, shall so survive.

## 8.0 NO WARRANTY

8.1 EMC (INCLUDING IT SUPPLIERS) PROVIDES ALL SOFTWARE HEREUNDER ON AN "AS IS", "WHERE IS" BASIS. EMC (INCLUDING ITS SUPPLIERS) MAKES NO OTHER EXPRESS WARRANTIES, WRITTEN OR ORAL, AND ALL OTHER WARRANTIES OF EVERY TYPE AND NATURE, WHETHER EXPRESS OR IMPLIED, ARE SPECIFICALLY EXCLUDED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ANY WARRANTY ARISING BY STATUTE, OPERATION OF LAW, COURSE OF DEALING OR PERFORMANCE, OR USAGE OF TRADE.

8.2 No representation or other affirmation of fact, including but not limited to, statements regarding capacity, suitability for use or performance of Software, whether made by EMC employees or otherwise, shall be deemed to be a warranty for any purpose or give rise to any liability of EMC whatsoever unless contained in this Agreement.

8.3 LICENSEE ACKNOWLEDGES AND AGREES THAT THE PROVISIONS OF SECTIONS 8.0, 9.0 AND 10.0 RESPECTIVELY REFLECT AN ALLOCATION OF RISK BETWEEN THE PARTIES THAT IS A MATERIAL INDUCEMENT FOR EMC PERFORMING UNDER THIS AGREEMENT AND THAT THESE DISCLAIMERS AND LIMITATIONS ARE FAIR AND REASONABLE UNDER THE CIRCUMSTANCES, AND LICENSEE HEREBY IRREVOCABLY AND PERPETUALLY WAIVES ANY CLAIMS OR CAUSES OF ACTION TO THE CONTRARY.

Press the <enter> key to continue

## 9.0 NO INDEMNIFICATION

9.1 EMC shall have no liability to Licensee for any action (and all related prior claims) brought by or against Licensee alleging that Licensee's use or other disposition of any Software infringes any patent, copyright, trade secret or other intellectual property right. In event of such an action, EMC retains the right to terminate this Agreement and take possession of the Software.

9.2 THIS SECTION 9.0 STATES EMC'S ENTIRE LIABILITY WITH RESPECT TO ALLEGED INFRINGEMENTS OF INTELLECTUAL PROPERTY RIGHTS BY THE SOFTWARE OR ANY PART OF THEM OR BY ITS OPERATION.

## 10.0 LIMITATION OF LIABILITY

10.1 EMC'S AND ITS SUPPLIER'S TOTAL LIABILITY AND LICENSEE'S SOLE AND EXCLUSIVE REMEDY FOR A CLAIM OF DAMAGE TO REAL OR TANGIBLE PERSONAL PROPERTY OR ANY OTHER CLAIM WHATSOEVER, INCLUDING BUT NOT LIMITED TO CLAIMS BASED ON CONTRACT, WARRANTY, NEGLIGENCE OR STRICT LIABILITY IN TORT, THAT ARISES OUT OF OR IN CONNECTION WITH THIS AGREEMENT, THE SOFTWARE OR ANY SERVICES PROVIDED HEREUNDER, SHALL BE LIMITED TO PROVEN DIRECT DAMAGES CAUSED BY EMC'S SOLE NEGLIGENCE IN AN AMOUNT NOT TO EXCEED US\$5,000.00.

10.2 IN NO EVENT SHALL EMC OR ITS SUPPLIERS BE LIABLE FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS, REVENUES, DATA AND/OR USE) EVEN IF ADVISED OF THE POSSIBILITY THEREOF. NEITHER PARTY SHALL BRING ANY CLAIM ARISING OUT OF THIS AGREEMENT, THE SOFTWARE OR ANY SERVICES PROVIDED HEREUNDER MORE THAN EIGHTEEN (18) MONTHS AFTER SUCH CLAIM HAS ACCRUED.

10.3 IF LICENSEE USES SOFTWARE FOR ANY PURPOSE EXCEPT AS STATED HEREIN OR AS OTHERWISE MUTUALLY AGREED IN WRITING, EMC SHALL HAVE NO LIABILITY WHATSOEVER FOR ANY DAMAGES RESULTING FROM SUCH USE INCLUDING, WITHOUT LIMITATION, DAMAGES TO ANY SYSTEMS, EQUIPMENT (AS DEFINED ABOVE) LICENSEE'S ENVIRONMENT, DATA, OR FINANCIAL LOSSES.

Press the <enter> key to continue

#### 11.0 GENERAL

11.1 Assignment Licensee shall not assign any right or interest hereunder nor delegate any work or other obligation to be performed hereunder without EMC's prior written consent. Without limiting the foregoing, EMC may terminate this Agreement immediately upon notice to Licensee if Licensee, without the prior written consent of EMC, merges, is acquired or otherwise undergoes a change of control. Any action in violation of the foregoing shall be void.

11.2 Entire Agreement - This Agreement (i) is the complete statement of the agreement of the parties with regard to the subject matter hereof and shall supersede all prior oral or written communications and agreements between the parties with regard to the subject matter hereof; and (ii) may be modified only by a writing signed by both parties.

11.3 Compliance with Export Control Laws Software and the technology included therein provided under this Agreement are subject to governmental restrictions on (i) exports from the U.S.; (ii) exports from other countries in which such Software and technology included therein may be produced or located; (iii) disclosures of technology to foreign persons; (iv) exports from abroad of derivative products thereof; and (v) the importation and/or use of such Software and technology included therein outside of the United States or other countries (collectively, "Export Laws"). Licensee shall comply with all Export Laws and EMC export policies to the extent such policies are made available to Licensee by EMC. Licensee shall obtain all necessary governmental permits, licenses and clearances at its sole expenses. Licensee represents that it is not a Restricted Person as defined by Export Laws. Diversion contrary to U.S. law or other Export Laws is expressly prohibited. This Agreement shall be void and Licensee shall have no rights with respect to the Software if the foregoing representation is or becomes false.

11.4 Governing Law - This Agreement shall be governed by the laws of the Commonwealth of Massachusetts, excluding its conflict of law rules. Licensee agrees that the courts of the Commonwealth of Massachusetts shall be exclusively competent to rule on disputes arising out of or in connection with this Agreement. The U. N. Convention on Contracts for the International Sale of Goods shall not apply.

11.5 Notices Any notices required or permitted hereunder shall be in writing, and shall be deemed given when delivered (i) in person, (ii) by overnight courier, upon written confirmation of receipt, (iii) by certified or registered mail, with proof of delivery, (iv) by facsimile transmission with confirmation of receipt, or (v) by email, with confirmation of receipt (except for routine business communications issued by EMC, which shall not require confirmation from Licensee). In the case of EMC, notices shall be sent to the following address, facsimile number or email address or at such other address, facsimile number or email address as provided by EMC to Licensee in writing: EMC Corporation 176 South Street, Hopkinton, MA 01748. Fax for legal notices: 508.293.7780. Email for legal notices: legalnotices@emc.com. In the case of Licensee, notices shall be sent to the address, facsimile number or email address provided by Licensee as part of the registration process or on file in EMC records, or such other address, facsimile number or email as provided by Licensee to EMC in writing. The parties agree that this Agreement has been written in the English language, that the English language version shall govern and that all notices shall be in the English language.

11.6No Waiver No waiver shall be deemed a waiver of (i) any prior or subsequent default hereunder; or (ii) any remedy that may be available hereunder.

11.7Independent Contractors - The parties are independent contractors for all purposes under this Agreement. Nothing contained herein shall be deemed to constitute either party as an agent or representative of the other party, or both parties as joint venturers or partners for any purpose. Neither party shall be responsible for the acts or omissions of the other party, and neither party will have authority to speak for, represent or obligate the other party in any way. Press the <enter> key to continue

11.8Separability - If any provision of this Agreement shall be held illegal or unenforceable, such provision shall be deemed separable from, and shall in no way affect or impair the validity or enforceability of, the remaining provisions.

11.9 Force Majeure Neither party shall be liable under this Agreement because of a failure or delay in performing its obligations hereunder on account of any force majeure event, such as strikes, riots, insurrection, terrorism, fires, natural disasters, acts of God, war, governmental action, or any other cause which is beyond the reasonable control of such party.

#### End User License Agreement

1 - Display the license  
2 - Accept the license  
3 - Do not accept the license  
Select an option to edit: 2  
EMC SRS CECT 3.04

#### Checking customer information

\*\*Missing required customer information.\*\*

#### Site Information

1 - \*Customer Name:  
2 - Address:  
3 - City:  
4 - State:  
5 - Country:  
6 - \*Contact name (First, Last):  
7 - Department:  
8 - Phone:  
9 - \*Email:  
\* Required  
Select an option to edit: 1  
Customer Name: John Cadorette

#### Site Information

1 - \*Customer Name: John Cadorette  
2 - Address:  
3 - City:  
4 - State:  
5 - Country:  
6 - \*Contact name (First, Last):  
7 - Department:  
8 - Phone:  
9 - \*Email:  
\* Required  
Select an option to edit: 6  
Contact Name: John, Cadorette

#### Site Information

1 - \*Customer Name: John Cadorette  
2 - Address:  
3 - City:  
4 - State:

5 - Country:  
 6 - \*Contact name (First, Last): john  
 7 - Department:  
 8 - Phone:  
 9 - \*Email:  
 \* Required  
 Select an option to edit: 9  
 Email: john.cadorette@emc.com

#### Site Information

1 - \*Customer Name: John Cadorette  
 2 - Address:  
 3 - City:  
 4 - State:  
 5 - Country:  
 6 - \*Contact name (First, Last): John, Cadorette  
 7 - Department:  
 8 - Phone:  
 9 - \*Email: john.cadorette@emc.com  
 10 - Save data and return to the previous menu  
 \* Required  
 Select an option to edit: 10

#### Main Menu

1 - Display/Edit Customer Info  
 2 - Gateway Tests Menu  
 3 - Display Log Files  
 4 - Display the license  
 5 - Exit  
 Select an option: 2

#### Gateway Tests Menu

1 - Select Tests6 - Add a Device  
 2 - View/Edit Proxy Server Details7 - Delete a Device  
 3 - View/Edit Policy Server Details8 - Run Tests  
 4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu  
 5 - View Devices

Select an option: 1

#### SRS Server Environment Tests

1 - Memory5 - Operating System Version  
 2 - Free Disk Space6 - Network Interface Card  
 3 - Processor Speed7 - Required Local User Accounts  
 4 - Processor SSE2 Instruction Set8 - Select All Environment Tests

#### Network Connectivity Tests

9 - SRS Client Provisioning Connection (HTTPS)14 - SRS Remote Access Connection (TCP 443)  
 10 - SRS Core Connection (HTTPS)15 - SRS Remote Access Connection (TCP 8443)  
 11 - SRS Client Provisioning Connection (TCP)16 - SRS to Policy Server Connection  
 12 - SRS Core Connection (TCP)17 - Device Application and Port Connection Test  
 13 - SRS Remote Access Connection (HTTPS)18 - Select All Network Connectivity Tests

#### Linux Service/Daemon Tests

19 - File Transfer Protocol22 - SRS Watchdog  
 20 - Simple Mail Transport Protocol23 - SRS HTTPS Listener  
 21 - SRS Gateway and Device Client24 - Select All Service/Daemon Tests

25 - Return to previous menu

Separate multiple tests with a comma

Select an option: 8,16,24

1: / (59000M)  
 2: /dev (2000M)  
 3: /dev/shm (2000M)  
 4: /run (2000M)

```
5: / (59000M)
Select an option: 1
Input FTP daemon name (default esrshttpdfp):
Input SMTP daemon name (default postfix):
```

**\*\*Make sure the Policy Server details have been entered and are correct.\*\***

```
Gateway Tests Menu
1 - Select Tests6 - Add a Device
2 - View/Edit Proxy Server Details7 - Delete a Device
3 - View/Edit Policy Server Details8 - Run Tests
4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu
5 - View Devices
```

```
Select an option: 8
EMC Secure Remote Support Gateway Check Verification Tests
```

```
Run Date: 08/29/2014 11:15:53 AM
CECT Version: 3.04
User Name: root
Machine Name: 2k12-V-Grissom-103
OS Version: SUSE Linux Enterprise Server 11 (x86_64) VERSION = 11 PATCHLEVEL = 3 1.1.5
Shell: /bin/bash
Current Directory: /opt/esrsve/cect
```

\*\*\*\*\*  
Site and Customer Contact Information:

```
Customer Name: John Cadorette
Address:
City:
State:
Country:
Contact Name: John, Cadorette
Department:
Phone:
Email: john.cadorette@emc.com
```

\*\*\*\*\*  
Gateway Test Results  
\*\*\*\*\*

TEST NAME : EMC SRS system memory >= 1 GB STATUS : Passed

\*\*\*\*\*  
Test Notes: Secure Remote Server RAM Test Success.  
Test Notes: Minimum required value = 1 GB. Current Value = 3.95371 GB  
\*\*\*\*\*

TEST NAME : EMC SRS free disk space >= 1GB STATUS : Passed

\*\*\*\*\*  
Test Notes: Secure Remote Server Free Disk Space Test Success.  
Test Notes: Minimum required value = 1 GB. Current value = 59 GB  
\*\*\*\*\*

TEST NAME : EMC SRS CPU speed >= 2.2 GHZ STATUS : Passed

\*\*\*\*\*  
Test Notes: Secure Remote Server CPU Speed Test Success.  
Test Notes: Minimum required value = 2.2 GHZ. Current Value per processor = 1861.91 GHZ, Number  
of Processors = 1  
\*\*\*\*\*

TEST NAME : EMC SRS CPU SSE2 instruction set test. STATUS : Passed

\*\*\*\*\*

Test Notes: Gateway Server CPU SSE2 Instruction Set Test Success.

Test Notes: CPU is SSE2 compliant.

\*\*\*\*\*

TEST NAME : EMC SRS OS version requirement check. STATUS : Passed

\*\*\*\*\*

Test Notes: SUSE Linux Enterprise Server 11 (x86\_64) VERSION = 11 PATCHLEVEL = 3 1.1.5 is a valid operating system.

\*\*\*\*\*

TEST NAME : EMC SRS test for network interface device. STATUS : Passed

\*\*\*\*\*

Test Notes: Server network interface device check is installed and operational.

Test Notes: Name=eth0, Is Up=1, Is Running=2, MAC Address=00:15:5D:AE:6E:08

\*\*\*\*\*

TEST NAME : EMC SRS required user accounts test. STATUS : Passed

\*\*\*\*\*

Test Notes: Secure Remote Server User Account Check Success.

Test Notes: Account Name = onalert Password Expires = 0. Password Changeable = 0. Account Expires = 0.

Test Notes: Secure Remote Server User Account Check Success.

Test Notes: Account Name = esrsconfig Password Expires = 0. Password Changeable = 0. Account Expires = 0.

\*\*\*\*\*

TEST NAME : EMC SRS Policy Manager Pre Installation Connect Test. STATUS : Failed

\*\*\*\*\*

Test Notes: EMC SRS Policy Manager Pre Installation Connect Test. Test Failed.

Test Notes: You have requested a connection test to the Policy Server which is NOT installed.

Test Notes: This is a PM pre-installation connection test. Please supply the IP address and port of the Policy Server.

\*\*\*\*\*

TEST NAME : EMC SRS FTP service test. STATUS : Passed

\*\*\*\*\*

Test Notes: Secure Remote Server Linux Service esrshttpdfp Test is Success.

Test Notes: esrshttpdfp Service Status = Installed, State = Running

\*\*\*\*\*

TEST NAME : EMC SRS SMTP service test. STATUS : Passed

\*\*\*\*\*

Test Notes: Secure Remote Server Linux Service postfix Test is Success.

Test Notes: postfix Service Status = Installed, State = Running

\*\*\*\*\*

TEST NAME : EMC SRS Gateway agent service test. STATUS : Passed

\*\*\*\*\*

Test Notes: Secure Remote Server Linux Service esrsclient Test is Success.

Test Notes: esrsclient Service Status = Installed, State = Running

\*\*\*\*\*

TEST NAME : EMC SRS Watchdog service test. STATUS : Passed

\*\*\*\*\*

Test Notes: Secure Remote Server Linux Service esrswatchdog Test is Success.

Test Notes: esrswatchdog Service Status = Installed, State = Running

\*\*\*\*\*

TEST NAME : EMC SRS HTTPS Listener service test.      STATUS : Passed

```

Test Notes: Secure Remote Server Linux Service esrshttpdlistener Test is Success.
Test Notes: esrshttpdlistener Service Status = Installed, State = Running

```

Total tests run: 13  
Successul count: 12  
Failed count: 1

Gateway Tests Menu

- 1 - Select Tests6 - Add a Device
- 2 - View/Edit Proxy Server Details7 - Delete a Device
- 3 - View/Edit Policy Server Details8 - Run Tests
- 4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu
- 5 - View Devices

Select an option: 9

Main Menu

- 1 - Display/Edit Customer Info
- 2 - Gateway Tests Menu
- 3 - Display Log Files
- 4 - Display the license
- 5 - Exit

Select an option: 3

Log files found: 1

- 1 - CECT\_John Cadorette\_20140829111326.log

Select an option: 5

Invalid option

Select an option:

Invalid option

Select an option: 5

Invalid option

Select an option: 3

Invalid option

Select an option: 9

Invalid option

Select an option: 3

Invalid option

Select an option: 1

08/29/2014 11:15:53 AMEMC Secure Remote Support Gateway Check Verification Tests

08/29/2014 11:15:53 AM

08/29/2014 11:15:53 AMRun Date: 08/29/2014 11:15:53 AM

08/29/2014 11:15:53 AMCECT Version: 3.04

08/29/2014 11:15:53 AMUser Name: root

08/29/2014 11:15:53 AMMachine Name: 2k12-V-Grissom-103

08/29/2014 11:15:53 AMOS Version: SUSE Linux Enterprise Server 11 (x86\_64) VERSION = 11  
PATCHLEVEL = 3 1.1.5

08/29/2014 11:15:53 AMShell: /bin/bash

08/29/2014 11:15:53 AMCurrent Directory: /opt/esrsve/cect

08/29/2014 11:15:53

AM\*\*\*\*\*

08/29/2014 11:15:53 AMSite and Customer Contact Information:

08/29/2014 11:15:53 AM

08/29/2014 11:15:53 AMCustomer Name: John Cadorette

08/29/2014 11:15:53 AMAddress:

08/29/2014 11:15:53 AMCity:

Press the <enter> key to continue

08/29/2014 11:15:53 AMState:

08/29/2014 11:15:53 AMCountry:

08/29/2014 11:15:53 AMContact Name: John, Cadorette

08/29/2014 11:15:53 AMDepartment:



```

08/29/2014 11:15:53 AMPhone:
08/29/2014 11:15:53 AMEmail: john.cadorete@emc.com
08/29/2014 11:15:53
AM*****
08/29/2014 11:15:53 AMGateway Test Results
08/29/2014 11:15:53
AM*****
08/29/2014 11:15:53
AM*****
08/29/2014 11:15:53 AM
08/29/2014 11:15:53 AMTEST NAME : EMC SRS system memory >= 1 GB STATUS : Passed
08/29/2014 11:15:53 AM
08/29/2014 11:15:53
AM*****
08/29/2014 11:15:53 AMTest Notes: Secure Remote Server RAM Test Success.
Press the <enter> key to continue

08/29/2014 11:15:53 AMTest Notes: Minimum required value = 1 GB. Current Value = 3.95371 GB
08/29/2014 11:15:53
AM*****
08/29/2014 11:15:53 AM
08/29/2014 11:15:53 AMTEST NAME : EMC SRS free disk space >= 1GB STATUS : Passed
08/29/2014 11:15:53 AM
08/29/2014 11:15:53
AM*****
08/29/2014 11:15:53 AMTest Notes: Secure Remote Server Free Disk Space Test Success.
08/29/2014 11:15:53 AMTest Notes: Minimum required value = 1 GB. Current value = 59 GB
08/29/2014 11:15:53
AM*****
08/29/2014 11:15:53 AM
08/29/2014 11:15:53 AMTEST NAME : EMC SRS CPU speed >= 2.2 GHZ STATUS : Passed
08/29/2014 11:15:53 AM
08/29/2014 11:15:53
AM*****
08/29/2014 11:15:53 AMTest Notes: Secure Remote Server CPU Speed Test Success.
08/29/2014 11:15:53 AMTest Notes: Minimum required value = 2.2 GHZ. Current Value per processor
= 1861.91 GHZ, Number of Processors = 1
Press the <enter> key to continue

08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AM
08/29/2014 11:15:54 AMTEST NAME : EMC SRS CPU SSE2 instruction set test. STATUS : Passed
08/29/2014 11:15:54 AM
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AMTest Notes: Gateway Server CPU SSE2 Instruction Set Test Success.
08/29/2014 11:15:54 AMTest Notes: CPU is SSE2 compliant.
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AM
08/29/2014 11:15:54 AMTEST NAME : EMC SRS OS version requirement check. STATUS : Passed
08/29/2014 11:15:54 AM
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AMTest Notes: SUSE Linux Enterprise Server 11 (x86_64) VERSION = 11
PATCHLEVEL = 3 1.1.5 is a valid operating system.
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AM
Press the <enter> key to continue

08/29/2014 11:15:54 AMTEST NAME : EMC SRS test for network interface device. STATUS : Passed
08/29/2014 11:15:54 AM
08/29/2014 11:15:54
AM*****

```

```

08/29/2014 11:15:54 AMTest Notes: Server network interface device check is installed and
operational.
08/29/2014 11:15:54 AMTest Notes: Name=eth0, Is Up=1, Is Running=2, MAC
Address=00:15:5D:AE:6E:08
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AM
08/29/2014 11:15:54 AMTEST NAME : EMC SRS required user accounts test. STATUS : Passed
08/29/2014 11:15:54 AM
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AMTest Notes: Secure Remote Server User Account Check Success.
08/29/2014 11:15:54 AMTest Notes: Account Name = onalert Password Expires = 0. Password
Changeable = 0. Account Expires = 0.
08/29/2014 11:15:54 AMTest Notes: Secure Remote Server User Account Check Success.
08/29/2014 11:15:54 AMTest Notes: Account Name = esrsconfig Password Expires = 0. Password
Changeable = 0. Account Expires = 0.
08/29/2014 11:15:54
AM*****
Press the <enter> key to continue

08/29/2014 11:15:54 AM
08/29/2014 11:15:54 AMTEST NAME : EMC SRS Policy Manager Pre Installation Connect Test. STATUS
: Failed
08/29/2014 11:15:54 AM
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AMTest Notes: EMC SRS Policy Manager Pre Installation Connect Test. Test
Failed.
08/29/2014 11:15:54 AMTest Notes: You have requested a connection test to the Policy Server
which is NOT installed.
08/29/2014 11:15:54 AMTest Notes: This is a PM pre-installation connection test. Please supply
the IP address and port of the Policy Server.
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AM
08/29/2014 11:15:54 AMTEST NAME : EMC SRS FTP service test. STATUS : Passed
08/29/2014 11:15:54 AM
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AMTest Notes: Secure Remote Server Linux Service esrshttpdfstp Test is
Success.
08/29/2014 11:15:54 AMTest Notes: esrshttpdfstp Service Status = Installed, State = Running
08/29/2014 11:15:54
AM*****
Press the <enter> key to continue

08/29/2014 11:15:54 AM
08/29/2014 11:15:54 AMTEST NAME : EMC SRS SMTP service test. STATUS : Passed
08/29/2014 11:15:54 AM
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AMTest Notes: Secure Remote Server Linux Service postfix Test is Success.
08/29/2014 11:15:54 AMTest Notes: postfix Service Status = Installed, State = Running
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AM
08/29/2014 11:15:54 AMTEST NAME : EMC SRS Gateway agent service test. STATUS : Passed
08/29/2014 11:15:54 AM
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AMTest Notes: Secure Remote Server Linux Service esrsclient Test is Success.
08/29/2014 11:15:54 AMTest Notes: esrsclient Service Status = Installed, State = Running
08/29/2014 11:15:54
AM*****
08/29/2014 11:15:54 AM

```

Press the <enter> key to continue

08/29/2014 11:15:54 AMTEST NAME : EMC SRS Watchdog service test. STATUS : Passed

08/29/2014 11:15:54 AM

08/29/2014 11:15:54

AM\*\*\*\*\*

08/29/2014 11:15:54 AMTest Notes: Secure Remote Server Linux Service esrswatchdog Test is Success.

08/29/2014 11:15:54 AMTest Notes: esrswatchdog Service Status = Installed, State = Running

08/29/2014 11:15:54

AM\*\*\*\*\*

08/29/2014 11:15:54 AM

08/29/2014 11:15:54 AMTEST NAME : EMC SRS HTTPS Listener service test. STATUS : Passed

08/29/2014 11:15:54 AM

08/29/2014 11:15:54

AM\*\*\*\*\*

08/29/2014 11:15:54 AMTest Notes: Secure Remote Server Linux Service esrshttpdlistener Test is Success.

08/29/2014 11:15:54 AMTest Notes: esrshttpdlistener Service Status = Installed, State = Running

08/29/2014 11:15:54

AM\*\*\*\*\*

08/29/2014 11:15:54 AM

08/29/2014 11:15:54 AMTotal tests run: 13

Press the <enter> key to continue

08/29/2014 11:15:54 AMSuccessful count: 12

08/29/2014 11:15:54 AMFailed count: 1

Main Menu

1 - Display/Edit Customer Info

2 - Gateway Tests Menu

3 - Display Log Files

4 - Display the license

5 - Exit

Select an option: 5

2k12-V-Grissom-103:/opt/esrsve/cect #

2k12-V-Grissom-103:/opt/esrsve/cect # ./CECT.sh

EMC SRS CECT 3.04

Checking customer information

Required customer information found

Main Menu

1 - Display/Edit Customer Info

2 - Gateway Tests Menu

3 - Display Log Files

4 - Display the license

5 - Exit

Select an option: 2

Gateway Tests Menu

1 - Select Tests6 - Add a Device

2 - View/Edit Proxy Server Details7 - Delete a Device

3 - View/Edit Policy Server Details8 - Run Tests

4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu

5 - View Devices

Select an option: 4

Please enter the Policy Server values before entering in the Policy Server Proxy values.

Gateway Tests Menu

1 - Select Tests6 - Add a Device

2 - View/Edit Proxy Server Details7 - Delete a Device

3 - View/Edit Policy Server Details8 - Run Tests

4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu  
5 - View Devices

Select an option: 3

Policy Server

1 - Currently Installed: False  
2 - IP Address:  
3 - Listening Port: 8090  
4 - Configured to use SSL: False  
5 - Policy Server co-located to on SRS Server: False  
6 - Clear values  
7 - Save data and return to the previous menu

Select an option to edit: 1

Policy Server Currently Installed

1 - Yes  
2 - No

Select an option: 1

Policy Server

1 - Currently Installed: True  
2 - \*IP Address:  
3 - \*Listening Port: 8090  
4 - Configured to use SSL: False  
5 - Policy Server co-located to on SRS Server: False  
6 - Clear values  
\* Required

Select an option to edit: 2

IP Address: 10.241.172.25

Policy Server

1 - Currently Installed: True  
2 - \*IP Address: 10.241.172.25  
3 - \*Listening Port: 8090  
4 - Configured to use SSL: False  
5 - Policy Server co-located to on SRS Server: False  
6 - Clear values  
7 - Save data and return to the previous menu  
\* Required

Select an option to edit: 3

Listening Port: 8443

Policy Server

1 - Currently Installed: True  
2 - \*IP Address: 10.241.172.25  
3 - \*Listening Port: 8443  
4 - Configured to use SSL: False  
5 - Policy Server co-located to on SRS Server: False  
6 - Clear values  
7 - Save data and return to the previous menu  
\* Required

Select an option to edit: 4

Policy Server Using SSL?

1 - Yes  
2 - No

Select an option: 1

Policy Server

1 - Currently Installed: True  
2 - \*IP Address: 10.241.172.25  
3 - \*Listening Port: 8443  
4 - Configured to use SSL: True  
5 - Policy Server co-located to on SRS Server: False  
6 - Clear values  
7 - Save data and return to the previous menu  
\* Required

Select an option to edit: 5  
 Policy Server co-located on SRS Server?  
 1 - Yes  
 2 - No  
 Select an option: 2

Policy Server  
 1 - Currently Installed: True  
 2 - \*IP Address: 10.241.172.25  
 3 - \*Listening Port: 8443  
 4 - Configured to use SSL: True  
 5 - Policy Server co-located to on SRS Server: False  
 6 - Clear values  
 7 - Save data and return to the previous menu  
 \* Required  
 Select an option to edit: 7

Gateway Tests Menu  
 1 - Select Tests6 - Add a Device  
 2 - View/Edit Proxy Server Details7 - Delete a Device  
 3 - View/Edit Policy Server Details8 - Run Tests  
 4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu  
 5 - View Devices

Select an option: 1

SRS Server Environment Tests  
 1 - Memory5 - Operating System Version  
 2 - Free Disk Space6 - Network Interface Card  
 3 - Processor Speed7 - Required Local User Accounts  
 4 - Processor SSE2 Instruction Set8 - Select All Environment Tests

Network Connectivity Tests  
 9 - SRS Client Provisioning Connection (HTTPS)14 - SRS Remote Access Connection (TCP 443)  
 10 - SRS Core Connection (HTTPS)15 - SRS Remote Access Connection (TCP 8443)  
 11 - SRS Client Provisioning Connection (TCP)16 - SRS to Policy Server Connection  
 12 - SRS Core Connection (TCP)17 - Device Application and Port Connection Test  
 13 - SRS Remote Access Connection (HTTPS)18 - Select All Network Connectivity Tests

Linux Service/Daemon Tests  
 19 - File Transfer Protocol22 - SRS Watchdog  
 20 - Simple Mail Transport Protocol23 - SRS HTTPS Listener  
 21 - SRS Gateway and Device Client24 - Select All Service/Daemon Tests  
 25 - Return to previous menu

Separate multiple tests with a comma  
 Select an option: 25

Gateway Tests Menu  
 1 - Select Tests6 - Add a Device  
 2 - View/Edit Proxy Server Details7 - Delete a Device  
 3 - View/Edit Policy Server Details8 - Run Tests  
 4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu  
 5 - View Devices

Select an option: 8  
 Error - no tests were selected. Please select at least one test to be run.

Gateway Tests Menu  
 1 - Select Tests6 - Add a Device  
 2 - View/Edit Proxy Server Details7 - Delete a Device  
 3 - View/Edit Policy Server Details8 - Run Tests  
 4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu  
 5 - View Devices

Select an option: 1

SRS Server Environment Tests

- 1 - Memory
- 5 - Operating System Version
- 2 - Free Disk Space
- 6 - Network Interface Card
- 3 - Processor Speed
- 7 - Required Local User Accounts
- 4 - Processor SSE2 Instruction Set
- 8 - Select All Environment Tests

Network Connectivity Tests

- 9 - SRS Client Provisioning Connection (HTTPS)
- 14 - SRS Remote Access Connection (TCP 443)
- 10 - SRS Core Connection (HTTPS)
- 15 - SRS Remote Access Connection (TCP 8443)
- 11 - SRS Client Provisioning Connection (TCP)
- 16 - SRS to Policy Server Connection
- 12 - SRS Core Connection (TCP)
- 17 - Device Application and Port Connection Test
- 13 - SRS Remote Access Connection (HTTPS)
- 18 - Select All Network Connectivity Tests

Linux Service/Daemon Tests

- 19 - File Transfer Protocol
- 22 - SRS Watchdog
- 20 - Simple Mail Transport Protocol
- 23 - SRS HTTPS Listener
- 21 - SRS Gateway and Device Client
- 24 - Select All Service/Daemon Tests

25 - Return to previous menu

Separate multiple tests with a comma

Select an option: 8

- 1: / (59000M)
- 2: /dev (2000M)
- 3: /dev/shm (2000M)
- 4: /run (2000M)
- 5: / (59000M)

Select an option: 1

Gateway Tests Menu

- 1 - Select Tests
- 6 - Add a Device
- 2 - View/Edit Proxy Server Details
- 7 - Delete a Device
- 3 - View/Edit Policy Server Details
- 8 - Run Tests
- 4 - View/Edit Policy Server Proxy Server Details
- 9 - Return to previous menu
- 5 - View Devices

Select an option: 8

EMC Secure Remote Support Gateway Check Verification Tests

Run Date: 08/29/2014 11:24:26 AM

CECT Version: 3.04

User Name: root

Machine Name: 2k12-V-Grissom-103

OS Version: SUSE Linux Enterprise Server 11 (x86\_64) VERSION = 11 PATCHLEVEL = 3 1.1.5

Shell: /bin/bash

Current Directory: /opt/esrsve/cect

\*\*\*\*\*

Site and Customer Contact Information:

Customer Name: John Cadorette

Address:

City:

State:

Country:

Contact Name: John, Cadorette

Department:

Phone:

Email: john.cadorette@emc.com

\*\*\*\*\*

Gateway Test Results

\*\*\*\*\*

TEST NAME : EMC SRS system memory >= 1 GB STATUS : Passed

```

Test Notes: Secure Remote Server RAM Test Success.
Test Notes: Minimum required value = 1 GB. Current Value = 3.95371 GB

```

TEST NAME : EMC SRS free disk space >= 1GB STATUS : Passed

```

Test Notes: Secure Remote Server Free Disk Space Test Success.
Test Notes: Minimum required value = 1 GB. Current value = 59 GB

```

TEST NAME : EMC SRS CPU speed >= 2.2 GHZ STATUS : Passed

```

Test Notes: Secure Remote Server CPU Speed Test Success.
Test Notes: Minimum required value = 2.2 GHZ. Current Value per processor = 1861.91 GHZ, Number
of Processors = 1

```

TEST NAME : EMC SRS CPU SSE2 instruction set test. STATUS : Passed

```

Test Notes: Gateway Server CPU SSE2 Instruction Set Test Success.
Test Notes: CPU is SSE2 compliant.

```

TEST NAME : EMC SRS OS version requirement check. STATUS : Passed

```

Test Notes: SUSE Linux Enterprise Server 11 (x86_64) VERSION = 11 PATCHLEVEL = 3 1.1.5 is a
valid operating system.

```

TEST NAME : EMC SRS test for network interface device. STATUS : Passed

```

Test Notes: Server network interface device check is installed and operational.
Test Notes: Name=eth0, Is Up=1, Is Running=2, MAC Address=00:15:5D:AE:6E:08

```

TEST NAME : EMC SRS required user accounts test. STATUS : Passed

```

Test Notes: Secure Remote Server User Account Check Success.
Test Notes: Account Name = onalert Password Expires = 0. Password Changeable = 0. Account Expires
= 0.
Test Notes: Secure Remote Server User Account Check Success.
Test Notes: Account Name = esrsconfig Password Expires = 0. Password Changeable = 0. Account
Expires = 0.

```

Total tests run: 7  
Successful count: 7  
Failed count: 0

#### Gateway Tests Menu

- 1 - Select Tests6 - Add a Device
- 2 - View/Edit Proxy Server Details7 - Delete a Device
- 3 - View/Edit Policy Server Details8 - Run Tests
- 4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu
- 5 - View Devices

Select an option: 3

Policy Server

1 - Currently Installed: True  
2 - \*IP Address: 10.241.172.25  
3 - \*Listening Port: 8443  
4 - Configured to use SSL: True  
5 - Policy Server co-located to on SRS Server: False  
6 - Clear values  
7 - Save data and return to the previous menu  
\* Required  
Select an option to edit: 7

Gateway Tests Menu

1 - Select Tests6 - Add a Device  
2 - View/Edit Proxy Server Details7 - Delete a Device  
3 - View/Edit Policy Server Details8 - Run Tests  
4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu  
5 - View Devices

Select an option: 1

SRS Server Environment Tests

1 - Memory5 - Operating System Version  
2 - Free Disk Space6 - Network Interface Card  
3 - Processor Speed7 - Required Local User Accounts  
4 - Processor SSE2 Instruction Set8 - Select All Environment Tests

Network Connectivity Tests

9 - SRS Client Provisioning Connection (HTTPS)14 - SRS Remote Access Connection (TCP 443)  
10 - SRS Core Connection (HTTPS)15 - SRS Remote Access Connection (TCP 8443)  
11 - SRS Client Provisioning Connection (TCP)16 - SRS to Policy Server Connection  
12 - SRS Core Connection (TCP)17 - Device Application and Port Connection Test  
13 - SRS Remote Access Connection (HTTPS)18 - Select All Network Connectivity Tests

Linux Service/Daemon Tests

19 - File Transfer Protocol22 - SRS Watchdog  
20 - Simple Mail Transport Protocol23 - SRS HTTPS Listener  
21 - SRS Gateway and Device Client24 - Select All Service/Daemon Tests

25 - Return to previous menu

Separate multiple tests with a comma

Select an option: 16

**\*\*Make sure the Policy Server details have been entered and are correct.\*\***

Gateway Tests Menu

1 - Select Tests6 - Add a Device  
2 - View/Edit Proxy Server Details7 - Delete a Device  
3 - View/Edit Policy Server Details8 - Run Tests  
4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu  
5 - View Devices

Select an option: 8

EMC Secure Remote Support Gateway Check Verification Tests

Run Date: 08/29/2014 11:26:04 AM

CECT Version: 3.04

User Name: root

Machine Name: 2k12-V-Grissom-103

OS Version: SUSE Linux Enterprise Server 11 (x86\_64) VERSION = 11 PATCHLEVEL = 3 1.1.5

Shell: /bin/bash

Current Directory: /opt/esrsve/cect

\*\*\*\*\*

Site and Customer Contact Information:

Customer Name: John Cadorette



Address:  
 City:  
 State:  
 Country:  
 Contact Name: John, Cadorette  
 Department:  
 Phone:  
 Email: john.cadorette@emc.com

\*\*\*\*\*  
 Gateway Test Results  
 \*\*\*\*\*

TEST NAME : EMC SRS system memory >= 1 GB      STATUS : Passed

\*\*\*\*\*  
 Test Notes: Secure Remote Server RAM Test Success.  
 Test Notes: Minimum required value = 1 GB. Current Value = 3.95371 GB  
 \*\*\*\*\*

TEST NAME : EMC SRS free disk space >= 1GB      STATUS : Passed

\*\*\*\*\*  
 Test Notes: Secure Remote Server Free Disk Space Test Success.  
 Test Notes: Minimum required value = 1 GB. Current value = 59 GB  
 \*\*\*\*\*

TEST NAME : EMC SRS CPU speed >= 2.2 GHZ      STATUS : Passed

\*\*\*\*\*  
 Test Notes: Secure Remote Server CPU Speed Test Success.  
 Test Notes: Minimum required value = 2.2 GHZ. Current Value per processor = 1861.91 GHZ, Number  
 of Processors = 1  
 \*\*\*\*\*

TEST NAME : EMC SRS CPU SSE2 instruction set test.      STATUS : Passed

\*\*\*\*\*  
 Test Notes: Gateway Server CPU SSE2 Instruction Set Test Success.  
 Test Notes: CPU is SSE2 compliant.  
 \*\*\*\*\*

TEST NAME : EMC SRS OS version requirement check.      STATUS : Passed

\*\*\*\*\*  
 Test Notes: SUSE Linux Enterprise Server 11 (x86\_64) VERSION = 11 PATCHLEVEL = 3 1.1.5 is a  
 valid operating system.  
 \*\*\*\*\*

TEST NAME : EMC SRS test for network interface device.      STATUS : Passed

\*\*\*\*\*  
 Test Notes: Server network interface device check is installed and operational.  
 Test Notes: Name=eth0, Is Up=1, Is Running=2, MAC Address=00:15:5D:AE:6E:08  
 \*\*\*\*\*

TEST NAME : EMC SRS required user accounts test.      STATUS : Passed

\*\*\*\*\*  
 Test Notes: Secure Remote Server User Account Check Success.  
 Test Notes: Account Name = onalert Password Expires = 0. Password Changeable = 0. Account Expires  
 = 0.  
 Test Notes: Secure Remote Server User Account Check Success.  
 Test Notes: Account Name = esrsconfig Password Expires = 0. Password Changeable = 0. Account  
 Expires = 0.  
 Trying to connect to https://10.241.172.25:8443/actions/index

Trying to connect to https://10.241.172.25:8443/aps/index.html

\*\*\*\*\*

TEST NAME : EMC SRS Policy Manager Post Installation Connect Test. STATUS : Passed

\*\*\*\*\*

Test Notes: EMC SRS Policy Manager Post Installation Connect Test. TCP Connection Test - OK.

Test Notes: Successful socket connection to address 10.241.172.25 on port = 8443

Test Notes: EMC SRS Policy Manager Post Installation Connect Test. Success.

Test Notes: Connection made using URL address: https://10.241.172.25:8443/actions/index

Test Notes: HTTPS response status: No error

Test Notes: HTTPS response status: 0

Test Notes: EMC SRS Policy Manager Post Installation Connect Test. TCP Connection Test - OK.

Test Notes: Successful socket connection to address 10.241.172.25 on port = 8443

Test Notes: EMC SRS Policy Manager Post Installation Connect Test. Success.

Test Notes: Connection made using URL address: https://10.241.172.25:8443/aps/index.html

Test Notes: HTTPS response status: No error

Test Notes: HTTPS response status: 0

\*\*\*\*\*

Total tests run: 8

Successful count: 8

Failed count: 0

Gateway Tests Menu

1 - Select Tests6 - Add a Device

2 - View/Edit Proxy Server Details7 - Delete a Device

3 - View/Edit Policy Server Details8 - Run Tests

4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu

5 - View Devices

Select an option: 9

Main Menu

1 - Display/Edit Customer Info

2 - Gateway Tests Menu

3 - Display Log Files

4 - Display the license

5 - Exit

Select an option: 2

Gateway Tests Menu

1 - Select Tests6 - Add a Device

2 - View/Edit Proxy Server Details7 - Delete a Device

3 - View/Edit Policy Server Details8 - Run Tests

4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu

5 - View Devices

Select an option: 1

SRS Server Environment Tests

1 - Memory5 - Operating System Version

2 - Free Disk Space6 - Network Interface Card

3 - Processor Speed7 - Required Local User Accounts

4 - Processor SSE2 Instruction Set8 - Select All Environment Tests

Network Connectivity Tests

9 - SRS Client Provisioning Connection (HTTPS)14 - SRS Remote Access Connection (TCP 443)

10 - SRS Core Connection (HTTPS)15 - SRS Remote Access Connection (TCP 8443)

11 - SRS Client Provisioning Connection (TCP)16 - SRS to Policy Server Connection

12 - SRS Core Connection (TCP)17 - Device Application and Port Connection Test

13 - SRS Remote Access Connection (HTTPS)18 - Select All Network Connectivity Tests

Linux Service/Daemon Tests

19 - File Transfer Protocol22 - SRS Watchdog

20 - Simple Mail Transport Protocol23 - SRS HTTPS Listener

21 - SRS Gateway and Device Client 24 - Select All Service/Daemon Tests

25 - Return to previous menu

Separate multiple tests with a comma

Select an option: 16

**\*\*Make sure the Policy Server details have been entered and are correct.\*\***

Gateway Tests Menu

1 - Select Tests 6 - Add a Device  
 2 - View/Edit Proxy Server Details 7 - Delete a Device  
 3 - View/Edit Policy Server Details 8 - Run Tests  
 4 - View/Edit Policy Server Proxy Server Details 9 - Return to previous menu  
 5 - View Devices

Select an option: 8

EMC Secure Remote Support Gateway Check Verification Tests

Run Date: 08/29/2014 11:27:02 AM

CECT Version: 3.04

User Name: root

Machine Name: 2k12-V-Grissom-103

OS Version: SUSE Linux Enterprise Server 11 (x86\_64) VERSION = 11 PATCHLEVEL = 3 1.1.5

Shell: /bin/bash

Current Directory: /opt/esrsve/cect

\*\*\*\*\*

Site and Customer Contact Information:

Customer Name: John Cadorette

Address:

City:

State:

Country:

Contact Name: John, Cadorette

Department:

Phone:

Email: john.cadorette@emc.com

\*\*\*\*\*

Gateway Test Results

\*\*\*\*\*

\*\*\*\*\*

TEST NAME : EMC SRS system memory >= 1 GB STATUS : Passed

\*\*\*\*\*

Test Notes: Secure Remote Server RAM Test Success.

Test Notes: Minimum required value = 1 GB. Current Value = 3.95371 GB

\*\*\*\*\*

TEST NAME : EMC SRS free disk space >= 1GB STATUS : Passed

\*\*\*\*\*

Test Notes: Secure Remote Server Free Disk Space Test Success.

Test Notes: Minimum required value = 1 GB. Current value = 59 GB

\*\*\*\*\*

TEST NAME : EMC SRS CPU speed >= 2.2 GHZ STATUS : Passed

\*\*\*\*\*

Test Notes: Secure Remote Server CPU Speed Test Success.

Test Notes: Minimum required value = 2.2 GHZ. Current Value per processor = 1861.91 GHZ, Number of Processors = 1

\*\*\*\*\*

TEST NAME : EMC SRS CPU SSE2 instruction set test. STATUS : Passed

```

Test Notes: Gateway Server CPU SSE2 Instruction Set Test Success.
Test Notes: CPU is SSE2 compliant.

```

TEST NAME : EMC SRS OS version requirement check. STATUS : Passed

```

Test Notes: SUSE Linux Enterprise Server 11 (x86_64) VERSION = 11 PATCHLEVEL = 3 1.1.5 is a
valid operating system.

```

TEST NAME : EMC SRS test for network interface device. STATUS : Passed

```

Test Notes: Server network interface device check is installed and operational.
Test Notes: Name=eth0, Is Up=1, Is Running=2, MAC Address=00:15:5D:AE:6E:08

```

TEST NAME : EMC SRS required user accounts test. STATUS : Passed

```

Test Notes: Secure Remote Server User Account Check Success.
Test Notes: Account Name = onalert Password Expires = 0. Password Changeable = 0. Account Expires
= 0.
Test Notes: Secure Remote Server User Account Check Success.
Test Notes: Account Name = esrsconfig Password Expires = 0. Password Changeable = 0. Account
Expires = 0.
Trying to connect to https://10.241.172.25:8443/actions/index
Trying to connect to https://10.241.172.25:8443/aps/index.html

```

TEST NAME : EMC SRS Policy Manager Post Installation Connect Test. STATUS : Passed

```

Test Notes: EMC SRS Policy Manager Post Installation Connect Test. TCP Connection Test - OK.
Test Notes: Successful socket connection to address 10.241.172.25 on port = 8443
Test Notes: EMC SRS Policy Manager Post Installation Connect Test. Success.
Test Notes: Connection made using URL address: https://10.241.172.25:8443/actions/index
Test Notes: HTTPS response status: No error
Test Notes: HTTPS response status: 0
Test Notes: EMC SRS Policy Manager Post Installation Connect Test. TCP Connection Test - OK.
Test Notes: Successful socket connection to address 10.241.172.25 on port = 8443
Test Notes: EMC SRS Policy Manager Post Installation Connect Test. Success.
Test Notes: Connection made using URL address: https://10.241.172.25:8443/aps/index.html
Test Notes: HTTPS response status: No error
Test Notes: HTTPS response status: 0

```

Total tests run: 8  
Successful count: 8  
Failed count: 0

#### Gateway Tests Menu

- 1 - Select Tests6 - Add a Device
- 2 - View/Edit Proxy Server Details7 - Delete a Device
- 3 - View/Edit Policy Server Details8 - Run Tests
- 4 - View/Edit Policy Server Proxy Server Details9 - Return to previous menu
- 5 - View Devices

Select an option: 9

#### Main Menu

- 1 - Display/Edit Customer Info
- 2 - Gateway Tests Menu

```
3 - Display Log Files
4 - Display the license
5 - Exit
Select an option: 5
2k12-V-Grissom-103:/opt/esrsve/cect # exit
logout
```



# APPENDIX E

## SRS Version 3 CLI Utility

This appendix describes the SRS Version 3 (SRSv3) CLI utility, which is used to view SRS agent status, SRSv3 deployed devices, and significant SRSv3 services' status. It is also used to add or view proxy configurations and to perform other tasks in relation to the SRS configuration.

This appendix contains the following topics:

- ◆ [Overview.....](#) 164
- ◆ [Installing SRSv3 CLI utility.....](#) 164
- ◆ [Using SRSv3 CLI utility.....](#) 164

## Overview

SRSv3 CLI utility is a tool used to view SRS agent status, view important VE services' status, display active remote sessions, view deployed devices, configure proxy configuration, and perform other related services.

SRSv3 webUI credentials are required for all of the SRSv3 CLI utility operations. Various operations that can be performed using the SRSv3 CLI utility are listed as follows:

- ◆ Display agent status
- ◆ Display active remote sessions
- ◆ Display important SRS services' status
- ◆ List the devices managed by the SRSv3
- ◆ Manage (add, delete, or view) Policy Manager configuration
- ◆ Manage (add, delete, or view) proxy configuration

## Installing SRSv3 CLI utility

SRSv3 CLI utility is a built-in utility and included with the SRSv3 image.

## Using SRSv3 CLI utility

To use the SRSv3 CLI utility:

1. Open up the SRSv3 console using PuTTY or similar ssh tool.
2. Change to the utility directory:

```
/opt/ESRS/utilities/commandlineutil
```

---

**Note:** The SRSv3 CLI utility is named ESRS-VE-CLI-Util.sh. Running the script with -help argument shows all the operations available.

---

3. You can run the script with -help parameter to know the options.

```
./ESRS-VE-CLI-Util.sh --help
```

The following is a list of valid commands for the ESRS-VE-CLI-Util.sh script.



**Table 4** List of valid commands for the ESRS-VE-CLI-Util.sh script

| Sl no. | Commands               | Description                                                                                                                                                                                  |
|--------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | --agent-status         | Displays status information about:<br>The connection between the Gateway Client and EMC,<br>Statuses of proxy server and Policy Manager<br>Connectivity status and other status information. |
| 2      | --remote-session       | Shows all active remote sessions to the managed devices                                                                                                                                      |
| 3      | --service-status       | Displays important ESRS services state (Running/Stopped)                                                                                                                                     |
| 4      | --device-list          | Displays list of devices                                                                                                                                                                     |
| 5      | --view-policymanager   | Shows policy manager details                                                                                                                                                                 |
| 6      | --add-policymanager    | Adds agent policy manager in interactive way                                                                                                                                                 |
| 7      | --remove-policymanager | Removes policy manager configuration                                                                                                                                                         |
| 8      | --view-proxy           | Shows proxy server configuration                                                                                                                                                             |
| 9      | --add-proxy            | Adds agent proxy server configuration                                                                                                                                                        |
| 10     | --remove-proxy         | Removes agent proxy configuration                                                                                                                                                            |
| 11     | --help                 | Shows available options                                                                                                                                                                      |
| 13     | --quit                 | To exit the script                                                                                                                                                                           |

**Note:** Running script without any parameter will start the utility and prompt for SRSv3 WebUI username and password.

