



EMC® Secure Remote Support Gateway for Linux

Release 2.24

Operations Guide

REV 02

EMC Corporation

Corporate Headquarters:

Hopkinton, MA 01748-9103

1-508-435-1000

www.EMC.com

Copyright © 2005-2013 EMC Corporation. All rights reserved.

Published September, 2013

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.” 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 EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

RSA is a registered trademark of RSA Security Inc.

For the most up-to-date regulatory document for your product line, go to the Document/Whitepaper Library on the EMC Online Support Site (support.emc.com).

Preface

Chapter 1

Introduction

Architecture	16
Customer site components	17
Communication to EMC	20
Responsibilities for the ESRS components	25
Customer	25
EMC Global Services	25
Configuration	26
Gateway Client server configuration	26
Configuration CLI Commands	30
Gateway Extract Utility	33
Digital Certificate Management	34
Device access control	36
Device configuration access control	36
EMC enterprise access control	36

Chapter 2

Gateway Client Server Preparation

Overview	38
Configure Operating System (Red Hat Enterprise Linux 6.2 (32-bit))	39
Configure Network and firewall	39
Activate the Ethernet Port	47
Create Users and Set Passwords	48
Install vsftpd for FTP and Email	49
Install vsftpd	49

Install postfix.....	51
Create directories and install CECT and Provisioning Tool (PvT) .	52
Post ESRS Client install and configure permissions and firewall for vsftpd and Postfix.....	58
Verify status of Gateway and services.....	66
To configure the Gateway to use a Proxy server, edit the configuration, or remove the Proxy Server.....	69
Manage Devices	71

Chapter 3 Configuration CLI Commands

Configuration CLI Commands overview	78
Installing the Configuration CLI Commands.....	79
Installing the Configuration CLI Commands.....	79
Using the Configuration CLI Commands.....	79
gateway_status command options.....	79
Viewing connectivity status	79
manage_device command options	81
manage_device error codes.....	82
Managing devices.....	83
Communicating through a proxy server.....	86
Linking a Gateway Client to a Policy Manager	87
Disabling communication	89
Displaying the status of Services.....	90
Displaying active remote sessions	91
Displaying the log files	92

Chapter 4 Server Maintenance

Power sequences.....	94
Time Zone settings.....	95
Service preparation for Gateway Client	96
Gateway Client server.....	96
Backup guidelines and procedures.....	98
Server image backup.....	98
Restoration procedures	99
Server image backup restoration.....	99
Installation restoration.....	99

Appendix A Troubleshooting

Troubleshooting unexpected Gateway service events	102
Service malfunction.....	102
Service does not start up.....	102

Checking status and starting Gateway services	102
Cause of start up problem.....	103
Operating system or hardware failures	103
Troubleshooting ESRSHTTPS listener service	103
Concepts	103
Configuring the ESRSHTTPS listener	103
HTTPS listener paths	104
Files created	104
ESRSHTTPS listener service command line options.....	105
ESRSHTTPS configuration	107
esrshttps_config.xml file parameters	107

Index

	Title	Page
1	ESRS architecture	16
2	Heartbeat communication.....	21
3	Remote notification communication	22
4	Remote access communication.....	23
5	Firewall Configuration	40
6	Disable Firewall.....	41
7	Network Configuration.....	42
8	Device Configuration.....	42
9	Select A Device	43
10	Network Configuration.....	43
11	DNS Configuration	44
12	DNS Configuration	44
13	Saving Device and DNS Configuration	45
14	Quit Red Hat Setup Utility	46
15	Adding Users and Setting Passwords.....	48
16	Installing vsftpd.....	50
17	Verifying vsftpd service	50
18	Installing postfix.....	51
19	Verifying postfix service.....	51
20	Creating Gateway install directories	52
21	Copying .tar file and verifying.....	52
22	Running tar -xvf	52
23	Changing to PvT directory.....	52
24	Copying tar.gz to PVT directory and running tar -xvf.....	53
25	provision_agent command syntax.....	54
26	Running provision_agent command with arguments.....	55
27	gateway_status command syntax.....	55
28	Viewing Gateway Status	56
29	Viewing Gateway service information.....	56
30	Viewing active service information	56

31	Running gateway_status command with all arguments	57
32	Running setsebool for vsftpd	58
33	Modifying selinux for Postfix.....	58
34	Installing audit2allow.....	63
35	Staging the change to Postfix	64
36	Creating the selinux module	64
37	Making policy package active	64
38	Installing semodule.....	65
39	Verifying semodule install.....	65
40	Verifying Gateway and service status	66
41	config_policy_manager.sh command syntax.....	67
42	Running the config_policy_manager.sh command with arguments	68
43	Checking the Policy Manager configuration.....	68
44	Viewing Gateway status information	68
45	config_agent_proxy.sh command syntax	69
46	Configuring Gateway to use a Proxy server	69
47	Verifying proxy server status.....	70
48	Viewing Gateway status information	70
49	manage_device command syntax.....	71
50	Running manage_device --add-device	74
51	Viewing list of managed devices	75
52	gateway_status command options	79
53	Viewing Gateway connectivity status.....	80
54	manage_device command options	81
55	manage_device --list command.....	83
56	Adding a managed device.....	84
57	manage_device --modify-device command.....	85
58	manage_device --remove-device command	85
59	manage_device --show-history command	86
60	config_agent_proxy.sh command.....	87
61	config_agent_proxy.sh --remove-proxy command.....	87
62	config_policy_manager.sh command	88
63	config_policy_manager.sh --remove command	89
64	gateway_status --service-status command.....	90
65	gateway_status --remote-sessions command.....	91
66	cat xGate.log command.....	92
67	esrshttps_config.xml file	107

	Title	Page
1	Specifications for ESRS Gateway Client server.....	19
2	Product use of ESRS.....	23
3	Configuration items	31
4	Products supported by the Gateway Extract Utility (GWExt)	34
5	Valid Suffixes and Code Versions.....	72
6	manage_device error codes	82

As part of an effort to improve and enhance the performance and capabilities of its product line, EMC from time to time releases revisions of its hardware and software. Therefore, some functions described in this guide may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this guide, contact your EMC representative.

Audience

This guide is a part of the EMC Secure Remote Support documentation set and is intended for use by device administrators.

Related documentation

Related documents include:

- ◆ *EMC Secure Remote Support Release Notes*
- ◆ *EMC Secure Remote Support Technical Description*
- ◆ *EMC Secure Remote Support Pre-Site Checklist*
- ◆ *EMC Secure Remote Support Site Planning Guide*
- ◆ *EMC Secure Remote Support Port Requirements*
- ◆ *EMC Secure Remote Support Gateway for Windows Operations Guide*
- ◆ *EMC Secure Remote Support Customer Environment Check Tool for Windows Operations Guide*
- ◆ *EMC Secure Remote Support Customer Environment Check Tool for Linux Operations Guide*
- ◆ *EMC Secure Remote Support Policy Manager Release 2.02.1-xxx Operations Guide*

Conventions used in this guide

EMC uses the following conventions for notes and cautions.

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



CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

EMC uses the following type style conventions in this guide:

Normal	<p>In running text:</p> <ul style="list-style-type: none"> Interface elements (for example, button names, dialog box names) outside of procedures Items that user selects outside of procedures Java classes and interface names Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, menu names, utilities Pathnames, URLs, filenames, directory names, computer names, links, groups, service keys, file systems, environment variables (for example, command line and text), notifications
Bold	<ul style="list-style-type: none"> User actions (what the user clicks, presses, or selects) Interface elements (button names, dialog box names) Names of keys, commands, programs, scripts, applications, utilities, processes, notifications, system calls, services, applications, and utilities in text
<i>Italic</i>	<ul style="list-style-type: none"> Book titles New terms in text Emphasis in text
Courier	<ul style="list-style-type: none"> Prompts System output Filenames Pathnames URLs Syntax when shown in command line or other examples
Courier, bold	<ul style="list-style-type: none"> User entry Options in command-line syntax
<i>Courier italic</i>	<ul style="list-style-type: none"> Arguments in examples of command-line syntax Variables in examples of screen or file output Variables in pathnames
<>	Angle brackets for parameter values (variables) supplied by user.
[]	Square brackets for optional values.
	Vertical bar symbol for alternate selections. The bar means or.

... Ellipsis for nonessential information omitted from the example.

Where to get help

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

Product Information—For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Online Support Site (registration required) at:

<http://support.emc.com>

Technical support—For technical support, click Support on the EMC Online Support Site. To open a service request through the EMC Online Support Site, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a support agreement or to answer any questions about your account.

Your comments

Your comments and suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your comments and suggestions to:

techpubcomments@EMC.com

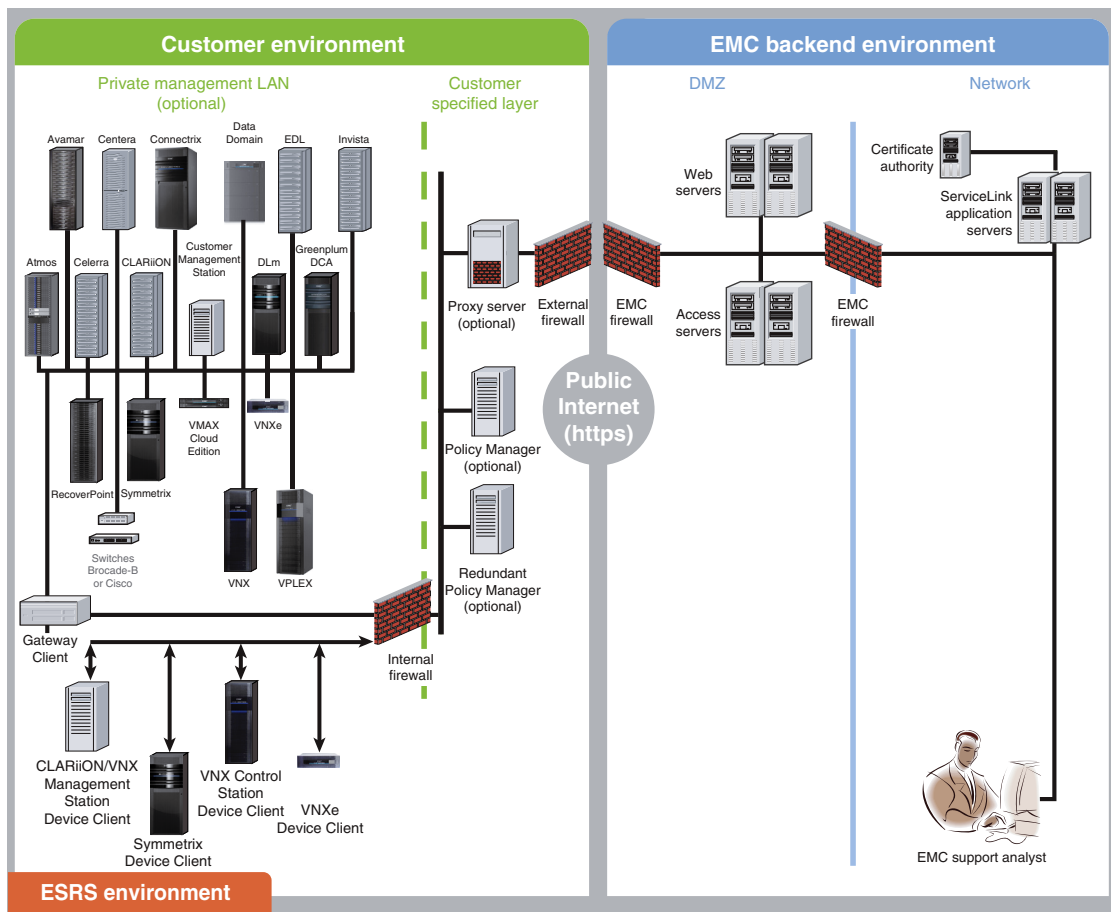
You should become familiar with the *EMC Secure Remote Support Site Planning Guide*. It is important to understand system requirements and configurations before you execute any administrative tasks.

This chapter introduces the EMC Secure Remote Support Gateway for Linux Client. Topics include:

- ◆ [Architecture..... 16](#)
- ◆ [Responsibilities for the ESRS components 25](#)
- ◆ [Configuration 26](#)

Architecture

The EMC® Secure Remote Support (ESRS) application architecture consists of a secure, asynchronous messaging system designed to support the functions of secure encrypted file transfer, monitoring of device status, and remote execution of diagnostic activities. This distributed solution is designed to provide a scalable, fault-tolerant, and minimally intrusive extension to the customer's system support environment. Figure 1 on page 16 illustrates the major processing components and their interconnections.



GEN-002128

Figure 1 ESRS architecture

Customer site components

ESRS requires the following software and hardware at the customer site:

Gateway Client(s) — This ESRS software component is installed on a customer-supplied dedicated server or Hyper-V/VMware instance. It can also be installed on multiple servers. The servers act as the single point of entry and exit for all IP-based remote support activities and most EMC connect home notifications.

Embedded ESRS Device clients: This ESRS software component is integrated on some EMC Products and utilizes the same technology as the ESRS Gateway Client. If the Embedded ESRS Device Client is utilized, the device is not managed by an ESRS Gateway Client. The Embedded ESRS Device Client can also use the same or a different Policy Manager as an ESRS Gateway Client and enforces the policy, and audits just like an ESRS Gateway Client but only on that specific device.

Policy Manager — This ESRS 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 ESRS Clients, and access to and administration actions performed on the Policy Manager.

Gateway Clients

The ESRS Gateway Client is the remote support solution application that is installed on one or more customer-supplied dedicated servers. The Gateway Client(s) become the single point of entry and exit for all IP-based EMC remote support activities for the devices associated with that particular Gateway or Gateway Cluster.

The Gateway Clients function as communication brokers between the managed devices, the Policy Manager, and the EMC enterprise. The Gateway Clients are HTTPS handlers and all messages are encoded using standard XML and SOAP application protocols. Gateway Client message types include:

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

Each Gateway Client acts as a proxy, carrying information to and from managed devices or to a Policy Manager. Gateway Clients can also queue session requests in the event of a temporary local network failure.

The Gateway Clients do not have their own user interface, and are run as Linux services. All Gateway Client actions are logged to a local rolling runtime log file.

[Table 1 on page 19](#) shows the minimum configuration of the required hardware and the application software.

Policy Manager

The Policy Manager allows you to set permissions for devices that are being managed by the Gateway Clients. The Gateway Client polls the Policy Manager every 2 minutes and receives the current policies, which it then are cached locally. (Because of this polling time interval, policy updates may take up to 2 minutes before being applied.)

During the periodic poll, the Gateway Client posts all requests and actions that have occurred which are then written to local log files and the Policy Manager database. When a remote access request arrives at the Gateway Client for device access, the access is controlled by the Gateway Client enforcing the policy set by the Policy Manager.

The Policy Manager software may be on another application server (for example, an EMC Navisphere® Management station) or co-located on a non-high-availability Gateway Client server (recommended for test purposes only).

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

Proxy server

Network traffic can be configured to route from the Gateway Clients through proxy servers to the Internet. Such configurations include support for auto-configuration, HTTP, and SOCKS proxy standards.

Note: When a customer configuration requires proxy communication between the Gateway Client and the Policy Manager or between the Gateway Client and the EMC Enterprise, if the Gateway Client cannot connect to either the Policy Manager or to the EMC Enterprise through the proxy communication path, it will continue to attempt to connect multiple times. After a couple of minutes, if the Gateway Client is unable to connect using the proxy connection path, it will then attempt a direction connection

(disregarding the proxy path). If the Gateway Client successfully makes a direct connection, no error message will appear to notify the customer or EMC that there is a problem with the proxy communication path.

Table 1 on page 19 shows the minimum configuration of the required Gateway Client hardware and the application software.

Table 1 Specifications for ESRS Gateway Client server

Type	Requirements	EMC provided software	Notes
Gateway Client server	<p>Processor — One or more processors, each 2.2 GHz minimum, must be SSE2 supported (required for FIPS compliance)</p> <p>Free Memory — Minimum 1 GB RAM, preferred 2 GB RAM. (If the Gateway Client and Policy Manager are on the same server, the recommended minimum RAM is 3 GB.)</p> <p>Network Interface Cards (NIC) — Two 10/100 Ethernet adapters (NIC cards) are recommended (1 Gb preferred). You may choose to use a third NIC card for data backups.</p> <p>Free Disk Space — Minimum 1 GB available for installation. (A 40 GB or larger storage device is recommended.)</p> <p>Operating System — US English only supported, as follows:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 6.2 (32-bit) • CentOS release 6.4, 32-bit • Hyper-V and VMware ESX 2.5.x or above running the following operating systems in a virtual machine <ul style="list-style-type: none"> – Red Hat Enterprise Linux 6.2 (32-bit) – CentOS release 6.4, 32-bit 	Gateway Client	<p>The Gateway Client requires a site-supplied dedicated server.</p> <p>Two servers are required for a High Availability configuration.</p> <p>One Gateway Client server can support up to 250 devices.</p>

Communication to EMC

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



IMPORTANT

Port 8443 is not required for functionality, however without this port being opened, there will be a significant decrease in remote support performance, which will directly impact time to resolve issues on the end devices.

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

The Gateway Clients use the SSL tunnel to EMC to perform the following functions:

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

Each 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 EMC by the Gateway Client” on page 20](#)
- ◆ [“To EMC devices managed by the Gateway Client” on page 21](#)

To EMC by the Gateway Client

The *heartbeat* is a regular outbound communication, at a default interval of 30 seconds, from the Gateway Clients to the EMC enterprise. Each heartbeat contains a small datagram that identifies

the Gateway Client and provides the EMC enterprise with status information on the connectivity health of the EMC storage devices and the Gateway Client.

EMC servers receive the data in XML format and acknowledge the receipt of data using SOAP (Simple Object Access Protocol) commands. Once this response is received, the Gateway Client terminates the connection. [Figure 2 on page 21](#) provides an illustration of the heartbeat communication paths.

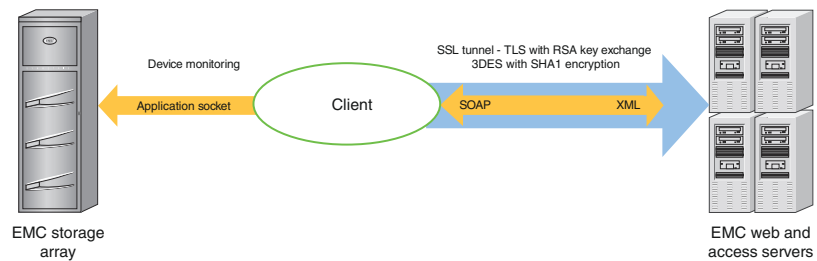


Figure 2 Heartbeat communication

To EMC devices managed by the Gateway Client

Once every 60 minutes the Gateway Client determines if each managed device is available for service by making a socket connection to the device on one or more support application ports and verifying that the service application(s) are responding. If a change in status is detected, the Gateway Client notifies EMC over the next heartbeat.

The heartbeat is a continuous service. EMC monitors the values sent and may automatically trigger service requests if an Gateway Client fails to send heartbeats, or if the values contained in a heartbeat exceed certain limits.

Remote notification (Connect Home)

The Gateway Clients also serve as a conduits for EMC products to send remote notification event files to EMC. EMC hardware platforms use remote notification for several different purposes. Errors, warning conditions, health reports, configuration data, and script execution statuses may be sent to EMC. [Figure 3 on page 22](#) provides an illustration of the remote notification communication paths.

When an alert condition occurs, the storage system generates an event message file and passes it to the ConnectEMC service on the device to format the files and request a transfer to EMC. ConnectEMC

uploads the file to the Gateway Client where it is received by one of the following local transport protocols:

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

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

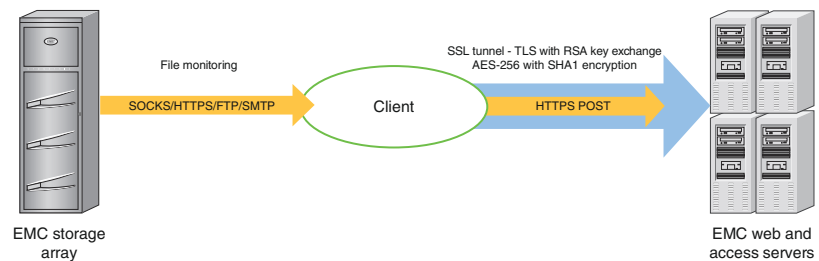


Figure 3 Remote notification communication

Remote access

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

After being properly authenticated at EMC, an 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. This request is queued at EMC until an Gateway Client that manages the device in question sends a heartbeat to EMC.

In response to the Heartbeat XML message, the 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 the Gateway Client would use to connect. The Gateway Client 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 connection to the Global Access Server for the specific remote access session.

This secure session allows IP traffic from the EMC internal service person to be routed through the Gateway Client to the end device. IP socket traffic received by the Global Access Server for the session is established, wrapped in a SOAP message, and sent to the Gateway Client over the persisted SSL tunnel. The Gateway Client 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 the Gateway Client and the Global Access Server through this tunnel until it is terminated or times out after a period of inactivity. [Figure 4 on page 23](#) provides an illustration of the remote access communication paths.

As the result of an application remote access session request, the Gateway Client forwards traffic only to the specific ports at the IP address associated with the registered serial number of the EMC device at the time of deployment.

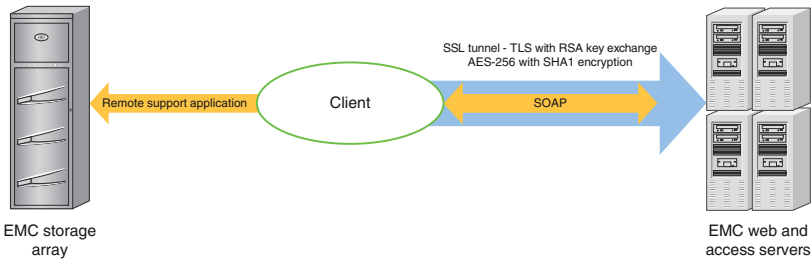


Figure 4 Remote access communication

[Table 2 on page 23](#) shows which EMC products use the remote notification and remote access features of ESRS.

Table 2 Product use of ESRS (page 1 of 2)

Product	Remote notification to EMC via ESRS	EMC remote access to device via ESRS
EMC Atmos®	Yes	Yes
EMC Avamar®	Yes	Yes
EMC Celerra®	Yes	Yes
EMC Centera®	Device does not send Connect Homes via the Gateway Client	Yes
EMC CLARiiON®	Yes	Yes

Table 2 Product use of ESRS (page 2 of 2)

Product	Remote notification to EMC via ESRS	EMC remote access to device via ESRS
EMC Connectrix®	Yes	Yes
Customer Management Station	Device does not send Connect Homes via the Gateway Client	Yes
Data Domain	Device does not send Connect Homes via the Gateway Client	Yes
DL3D	Device does not send Connect Homes via the Gateway Client	Yes
DLm	Yes	Yes
EDL	Yes	Yes
EMC Greenplum DCA®	Yes	Yes
EMC Invista®	Yes	Yes
RecoverPoint	Yes	Yes
Switch-Brocade-B	Yes ^a	Yes
Switch-Cisco	Yes ^b	Yes
EMC Symmetrix®	Yes	Yes
EMC VMAX® Cloud Edition (CE)	Yes	Yes
EMC VNX®	Yes	Yes
EMC VNXe®	Yes	Yes
EMC VPLEX®	Yes	Yes

a. Via Connectrix Manager, Connectrix Manager Data Center Edition, or Connectrix Manager Converged Network Edition

b. Via CiscoFabric Manager or Cisco Data Center Network Manager

Responsibilities for the ESRS components

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

Customer

You are responsible for the following:

- ◆ Installing, configuring, and maintaining the following hardware and software components:
 - Gateway Client server hardware and operating system
 - Policy Manager server hardware and operating system
 - Antivirus and other applicable security software
- ◆ Providing continuing maintenance to hardware and operating systems, including security updates
- ◆ Monitor and maintain 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 Gateway Client and Policy Manager servers, including the SSL certificate(s) if applicable
- ◆ Configuring, administering, and updating policies and accounts on the Policy Manager

Note: For more information on the Operations and configuration of the Policy Manager, refer to the *EMC Secure Remote Support Policy Manager Operations Guide*.

Note: Customers can download ESRS Gateway Client Patches from the EMC Online Support Site (support.emc.com) and install them at their convenience. All ESRS Gateway Client patches are cumulative.

Note: Policy Manager software is customer installable.

EMC Global Services

EMC Global Services personnel are responsible for the following:

- ◆ Installing the ESRS software:
 - Gateway Client server software
 - Policy Manager software (customers may install this software)
- ◆ Configuring and deploying the EMC devices managed through ESRS
- ◆ Configuring ESRS High Availability Clusters
- ◆ Approval of the Deployment, Removal or Edits of Deployed Devices in ServiceLink

Note: Note: If connect home is already set up, customer may use the If connect home is already set up, customer may use the Configuration CLI Commands to process device deployment requests.

- ◆ Updating the Gateway Client and Policy Manager software

Note: Maintenance of the operating system on the Gateway Client and Policy Manager servers, including updates, upgrades, and antivirus protection, is a customer responsibility.

Note: Customers can download ESRS Gateway Client Patches from the EMC Online Support Site (support.emc.com) and install them at their convenience. All ESRS Gateway Client patches are cumulative. Customers can also Update or Migrate to newer versions of Policy Manager.

Configuration

This section provides details on the configuration of ESRS.

Gateway Client server configuration

A Gateway Client server can be implemented in one of several configurations to meet your network and security requirements. Refer to [Figure 1 on page 16](#) for a sample configuration.

EMC recommends that your Gateway Client and Policy Manager servers be OS hardened prior to installation. The preparation and hardening of servers is *your* responsibility and must not interfere with the Gateway Client, Policy Manager, or Utilities functionality or operation.

There are no technical restrictions on the network location of the Gateway Client server, other than its connectivity to your devices and Policy Manager as well as to the EMC enterprise. EMC strongly recommends the use of a firewall to block network ports not required by ESRS.

VMware/Hyper-V requirements

VMware servers must be version ESX 2.52 and later.

Minimum requirements:

- ◆ 15 GB partition
- ◆ 2.2 GHz virtual CPU
- ◆ 512 MB memory allocated (2 GB recommended, 3GB preferred)

Note: EMC strongly recommends that virtual hosts meet the same hardware and OS recommendations as for physical hardware so as to minimize performance issues.

Optional components:

- ◆ SMB modules
- ◆ VMotion functionality (for Policy Manager only, and cannot be used for the ESRS Client due to RSA LockBox Technology)

Note: The customer MUST be aware the over provisioning of the underlying VMware ESX/Hyper-V infrastructure may have significant negative impact on the operation and functionality of ESRS.

VMware/Hyper-V examples

Scenario 1

Two physical ESX servers with three VMware partitions—two on the first server and one on the second server. The first server hosts a Gateway Client and the Policy Manager. The second server hosts another Gateway Client. This enables you to put applications on the same server that normally would not be co-located.

Scenario 2

Three or more physical servers in an existing VMware environment. You install two or more Gateway Clients and Policy Manager on any of the existing physical servers, independent of physical location.

High Availability Gateway Cluster configuration

To enable maximum remote access availability, EMC recommends deployment of a High Availability Gateway Cluster configuration to eliminate single point of failure. A Gateway Cluster refers to the relationship created between two or more Gateway Clients.

Gateway Client servers, in a High Availability configuration, are active peers. Each Gateway Client in the cluster manages the same set of devices without awareness of, or contention with, the other Gateway Clients in the cluster. There is no direct communication between the Gateway Clients within the cluster.

If Gateways that are to be Clustered to create an HA environment are installed in separated sites with different Party/SiteID's, the Party/SiteID of those additional Gateways must be added to the cluster to permit the Gateways to be enumerated and joined to the existing cluster.

In the High Availability configuration, the Policy Manager software cannot be co-located on a Gateway Client server. It must be installed on a separate server.

Synchronization of Gateway Client clusters

Gateway Client cluster device management is synchronized by the EMC enterprise servers during polling cycles so that changes to the configuration on one Gateway Client in the cluster are automatically propagated to the other. When there is an addition, removal, or edit of a device on the managed devices list for any Gateway Client in a High Availability Gateway Cluster configuration, the EMC enterprise sends a synchronization message to all clustered Gateway Clients. When the other Gateway Client(s) in the cluster receives the device management transaction information, it updates its list of managed devices maintained on the Gateway Client. If that Gateway Client is currently not available during a synchronization attempt, the EMC enterprise queues the transaction. Synchronization of the Gateway Cluster occurs upon the next successful poll message received from the previously unavailable Gateway Client.

Installing a High Availability Gateway Cluster

To implement a High Availability Gateway Cluster configuration, your EMC Global Services professional will create the cluster relationship from the Device Management utility that is part of the EMC enterprise application (ServiceLink).

When a cluster is created, a cluster name must be assigned. The default name is the organization name followed by the words *HA Gateways*. Other names can be assigned, but no two clusters can have the same name.

Note: The Cluster name is limited to 64 characters.

The High Availability Gateway Cluster will take on the devices managed by the *first* Gateway Client enrolled into the cluster. When additional Gateway Clients are added to the cluster, they will begin managing the cluster's devices.

Note: The first Gateway Client used to create a High Availability Gateway Cluster may have managed devices. Any additional Gateway Clients enrolled in a High Availability Gateway Cluster must not be managing *any* devices at the time of enrollment. An error message will result if the additional Gateway Clients are managing devices. The managed devices must be un-managed before the Gateway Client can be enrolled, and then may be re-deployed after the Client is joined to the Cluster.

Note: If Gateways that are to be Clustered to create an HA environment are installed in separated sites with different Party/SiteID's, the Party/SiteID of those additional Gateways must be added to the cluster to permit the Gateways to be enumerated and joined to the existing cluster.

Configuration CLI Commands

The Configuration CLI Commands are automatically installed upon successful completion of your Gateway Client installation. The commands are typically located at:

`/opt/emc/esrs2/Gateway`

The Configuration CLI Commands are used to perform the following tasks:

- ◆ Configure the Gateway Client and Policy Manager
- ◆ Process management requests for EMC storage devices and switches to be managed by the Gateway Client

Note: The term *manage* means that a device is monitored and can use the Gateway Client to establish remote access connections. The Gateway Client proxies all Configuration CLI Commands management requests to the EMC enterprise for approval by EMC Global Services.

Connect home capability through the Gateway Client is configured at the device and should be in place (if applicable) before the Configuration CLI Commands are used to make device deployment requests.

Configuration items Table 3, “Configuration items,” describes the available configuration CLI commands.

Table 3 Configuration items

Configuration item	Description
<code>./gateway status - - agent status</code>	Displays status information about the connection between the Gateway Client and EMC, including connectivity status, proxy server and Policy Manager enablement, and other status results.
<code>./manage_device</code>	<p>Enables viewing of managed devices. Enables entry of requests to add new devices, make changes to managed devices, and remove currently managed devices.</p> <hr/> <p>Note: Customers may use the Configuration CLI Commands to make requests to add, edit, or remove a device. However, approval by an EMC Global Services professional is required before these changes will take place.</p> <hr/>
<code>./config_agent_proxy.sh</code>	Allows enabling or disabling of a proxy between an Gateway Client and the EMC enterprise.
<code>./config_policy_manager.sh</code>	Allows enabling or disabling communication between a Policy Manager and a Gateway Client and configuring Proxy Server for communication to the Policy Manager.
<code>./gateway_status -- service-status</code>	<p>Displays the state (running, stopped, or disabled) and the startup type (automatic or manual) of the following services related to ESRS and connect homes:</p> <ul style="list-style-type: none"> • FTP • SMTP • HTTP • Gateway • Watchdog
<code>./gateway_status --remote-session</code>	Displays all active remote sessions to the managed devices.
<code>./xGate.log</code>	Displays the log file for the Gateway Client activity. All transaction and configuration activity is logged to xGate.log.

Monitoring and event notification are handled by the Gateway Client. If a problem occurs with an Gateway Client and a High

Availability Gateway Cluster has been implemented, another Gateway Client within the cluster will handle these activities.

In a High Availability Gateway Cluster, remote access session management is handled by the first Gateway Client to send a heartbeat to the EMC enterprise and receive the remote access request.

Device management

The Configuration CLI Commands enable you to request the addition or removal of a managed device. You can also use the Configuration CLI Commands to change the IP address of a managed device. Further details are provided in [Chapter 4, “Server Maintenance.”](#)

The Configuration CLI Commands are automatically installed upon successful completion of your Gateway Client installation. The application is typically found at the following location:

```
/opt/emc/esrs/Gateway
```

Adding a device

To add a device, you use the **manage_device -- add-device** command with the following parameters:

- ◆ EMC device serial number
- ◆ Model (product type)
- ◆ IP address

After you submit a device management request, it must be approved by an authorized EMC Global Services professional via the EMC enterprise.

Note: EMC Global Services personnel must verify with your network administrators that the IP address of the managed device is accessible from the Gateway Client. If Network Address Translation (NAT) is being used in the environment, the IP address used to deploy the device must be the NAT IP address, not the device’s IP address. Let us say, for example, that the local IP address of a device is 192.168.0.100, and is only on your internal network. You are using NAT (or a NAT device) that maps the device IP (192.168.0.100) to IP 10.10.44.22 so that the device can be reached from within your DMZ. In this case, EMC must use the NAT IP address of 10.10.44.22 to reach the device, and in the Configuration CLI Commands when managing the device, the IP address utilized must be 10.10.44.22.

Changing a device’s IP address

You can use the Configuration CLI Commands to request a change to a managed device’s IP address. Your request will be sent to the EMC

enterprise for approval by an authorized EMC Global Services professional.

Note: If you will be submitting device management, removal, or edit requests via the Configuration CLI Commands, be sure to inform your EMC Global Services professional so that the necessary approvals can be made via the EMC enterprise.

Unmanaging a device

If you want to un-manage a device, you use the **manage_device --remove-device** command to request the device's removal from the list of managed devices. Your request will be sent to the EMC enterprise for approval by an EMC Global Services professional. When approved, the serial number of the device will be disassociated from your Gateway Client.

Gateway Extract Utility

To configure a device for management by a Gateway Client, the EMC Global Services professional on site must know the following for each managed device: serial number, product type, and an IP address that the Gateway Client can use to communicate with the device. The Gateway Extract utility (GWExt), when run on the EMC device, can be used to automate the collection of this information and transport it to the Gateway Client. EMC supplies the GWExt utility with the Gateway Client installer. For a list of the products that the GWExt utility supports, see [Table 4 on page 34](#).

Your EMC Global Services professional copies the GWExt utility from the Gateway Client server to the device that is to be managed.

The GWExt utility requests the Gateway Client server IP address. It then extracts the serial number and local IP address from the managed device, creates a configuration file, and sends the file to the Gateway Client via HTTPS by default. The Gateway Client then uploads the file to the EMC enterprise.

Certain products qualified for ESRS have a GWExt information file installed at time of production. This information file contains product information that the GWExt utility gathers and submits to the

Gateway Client for device registration, automating a large portion of the process.

Table 4 Products supported by the Gateway Extract Utility (GWExt)

Product supported by GWExt	Operating system	Additional notes
Celerra	Red Hat Enterprise Linux 5	NAS Code 6.0
Celerra	Red Hat Enterprise Linux 4	NAS Code 5.6
CLARiiON Management Station	Win32	
Connectrix	Win32	
EMC Disk Library (EDL)	SUSE Linux 9.3 32-bit	v3.0 - v3.2
EMC Disk Library 3D (DL3D)	SUSE Linux 10.2 32-bit	v3.3, v4.0
Greenplum Data Computing Appliance (DCA)	Red Hat Enterprise Linux 5	v5.5
Invista Element Manager	Win32	
Symmetrix	Win32	
VMAX Cloud Edition (CE)	Win32	
VNX - Block	Win32	
VNX - File	Linux	NAS Code 7.x
VNXe	SUSE Linux 11 64-bit	
VPLEX	SUSE Linux 10.2 32-bit	

Digital Certificate Management

During the site Gateway Client installation, digital certificates are installed on the Gateway Client. This procedure can only be performed by EMC Global Services professionals using EMC-issued RSA SecurID Authenticators. All certificate usage is protected by unique password encryption. Any message received by the Gateway Client, whether pre- or post-registration, requires entity-validation authentication.

Digital Certificate Management automates Gateway Client digital certificate enrollment by taking advantage of EMC's existing network authentication systems, which use the RSA SecurID Authenticator and the EMC local certificate authority (CA). Working with 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 Gateway Client.

ESRS Digital Certificate Management provides proof-of-identity of your Gateway Client. This digital document binds the identity of the Gateway Client to a key pair that can be used to encrypt and authenticate communication back to EMC. Because of its role in creating these certificates, the EMC certificate authority is the central repository for the ESRS key infrastructure.

The CA requires full authentication of a certificate requester before it issues the requested certificate to the Gateway Client. Not only must the CA verify that the information contained in the certificate request be accurate, it must also verify that the EMC Global Services professional making the request is authenticated, and that this person belongs to an EMC Global Services group that is allowed to request a certificate for the customer site at which the Gateway Client certificate is to be installed.

The EMC Global Services professional requests a certificate by first authenticating himself or herself using an EMC-issued RSA SecurID Authenticator. Once authentication is complete, the Gateway Client installation program locally gathers all the information required for requesting certificates. It also generates a certificate request, a private key, and a random password for the private key. The Gateway Client 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. After the certificate is issued, the installation program automatically completes the certificate installation on the Gateway Client.



IMPORTANT

Due to EMC's use of RSA Lockbox technology, a certificate cannot be copied and used on another machine. Changing the host name, joining to a Linux Domain, or changing the MAC addresses will cause the Lockbox to fail and may result in having to reinstall the Gateway Client.

Device access control

ESRS achieves remote application access to a process running on an EMC storage 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 connections are initiated by an EMC Global Services request at the EMC Global Access Server and through a pull connection by the Gateway Client. EMC never initiates a connection to your Gateway Client or network. Your policies as set in the ESRS Policy Manager determine if and how a connection is established.

Device configuration access control

Once your devices are configured for ESRS management, you must carefully control and monitor any changes to the configuration of the managed device. For example, changing the configured IP address in ESRS or changing the IP address of the storage device disables EMC's ability to perform remote service on that device as well as the device's connect home capabilities. For this reason, ESRS requires that only authorized EMC Global Services professionals are allowed to approve the change for a managed device. Each device modification, as well as the user ID of the EMC Global Services professional who approved the change, is tracked in the EMC enterprise audit logs.

EMC enterprise access control

Several security features are incorporated into the EMC enterprise. For access, EMC Global Services professionals must be logged into the EMC corporate network and must connect to the ESRS Enterprise Application using RSA SecurID® two-factor authentication technology. Only authorized EMC personnel can access the EMC enterprise.

Gateway Client Server Preparation

This chapter provides information you will need to prepare the Gateway Client server for installing the ESRS software. Topics include:

- ◆ Overview 38
- ◆ Configure Operating System (Red Hat Enterprise Linux 6.2 (32-bit) 39
- ◆ Activate the Ethernet Port..... 47
- ◆ Create Users and Set Passwords 48
- ◆ Install vsftpd for FTP and Email..... 49
- ◆ Create directories and install CECT and Provisioning Tool (PvT) .. 52
- ◆ Post ESRS Client install and configure permissions and firewall for vsftpd and Postfix 58
- ◆ Verify status of Gateway and services 66
- ◆ To configure the Gateway to use a Proxy server, edit the configuration, or remove the Proxy Server 69
- ◆ Manage Devices 71

Overview

Before you install ESRS, you must prepare the Gateway Client server operating system to receive notification from your managed devices after they are deployed.

As part of the preparation, the following software applications are required:

- ◆ **FTP server (vsftpd)** — ESRS uses vsftpd to receive notification files sent through the FTP transport to the Gateway Client. You must install vsftpd before installing the Gateway Client.
- ◆ **SMTP server (postfix)** — ESRS uses postfix to receive notification files sent through the SMTP transport to the Gateway Client. You must install postfix before installing the Gateway Client.
- ◆ **HTTPS Listener (esrshttps)** — EMC will install the esrshttps listener as part of the Gateway Client software installation. The HTTPS Listener is used when the ConnectEMC service sends device notifications over the HTTPS transport to the Gateway Client.

Configure Operating System (Red Hat Enterprise Linux 6.2 (32-bit))

Configure Network and firewall

Use the setup command and the resulting menu process to configure the following items:

- ◆ Firewall
 - ◆ IP address
 - ◆ Broadcast address
 - ◆ Netmask
 - ◆ default Gateway
 - ◆ DNS
1. To run the Red Hat configuration tools, type:

```
[root@localhost ~]# setup
```
 2. The Red Hat Setup Utility appears. You can use the Firewall Configuration tool to disable the firewall, OR configure per the Ports document. Refer to the *EMC Secure Remote Support Port Requirements*.

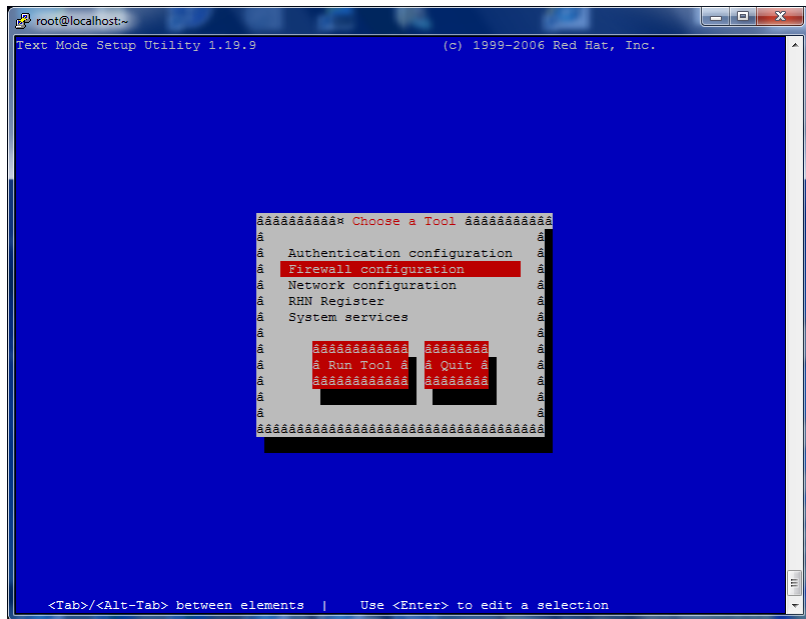


Figure 5 Firewall Configuration

3. Select **Firewall configuration**, then **Run Tool**. The Firewall Configuration tool appears. If the firewall is enabled, you need to disable it or configure it to pass the necessary traffic for the listener services per the *EMC Secure Remote Support Port Requirements* inbound to the Gateway.

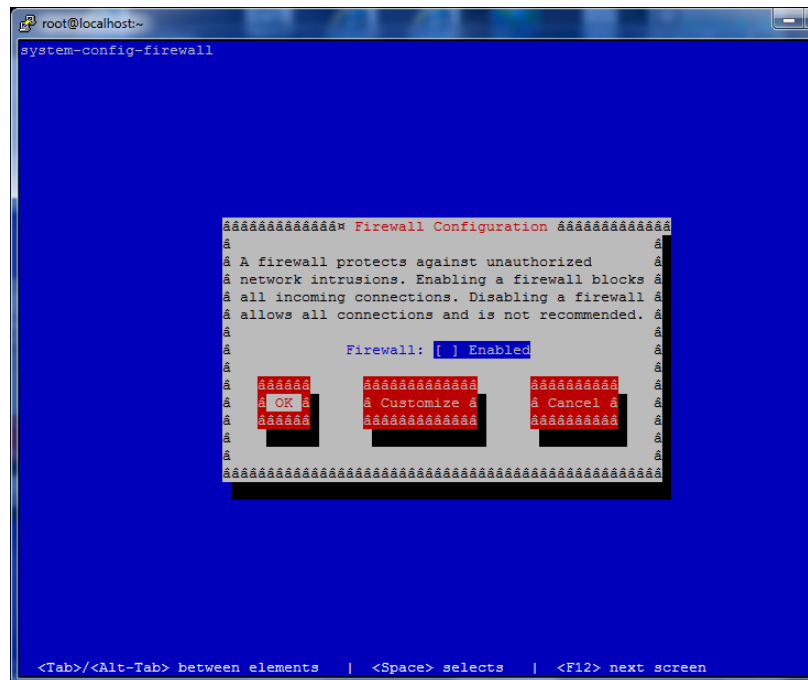


Figure 6 Disable Firewall

4. If the Firewall is enabled, use the space bar to remove the selection for **Enabled**, and select **OK** or configure it to pass the necessary traffic for the listener services per the *EMC Secure Remote Support Port Requirements* inbound to the Gateway.

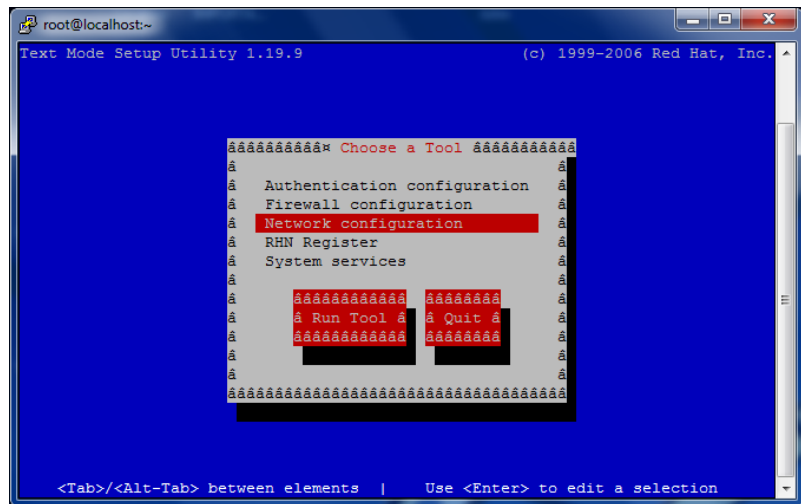


Figure 7 Network Configuration

5. Select **Network configuration**, and select **Run Tool**.

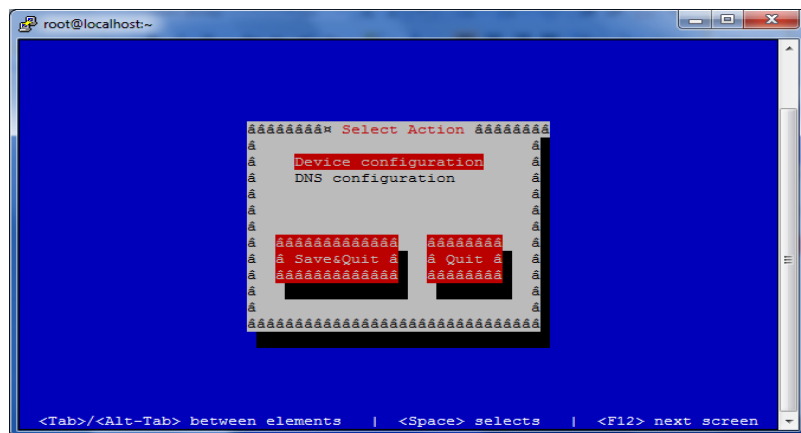


Figure 8 Device Configuration

6. Select **Device configuration**. The Select A Device screen appears.

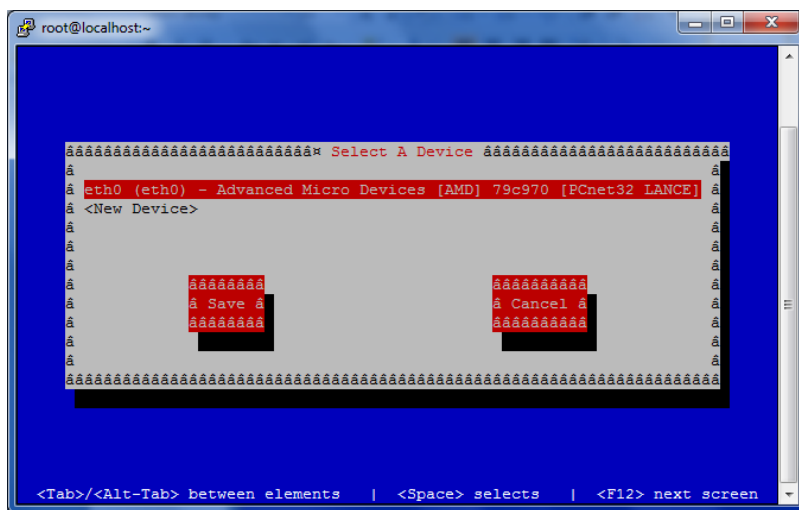


Figure 9 Select A Device

7. Select the device, and press **Enter**. The Network Configuration screen appears.

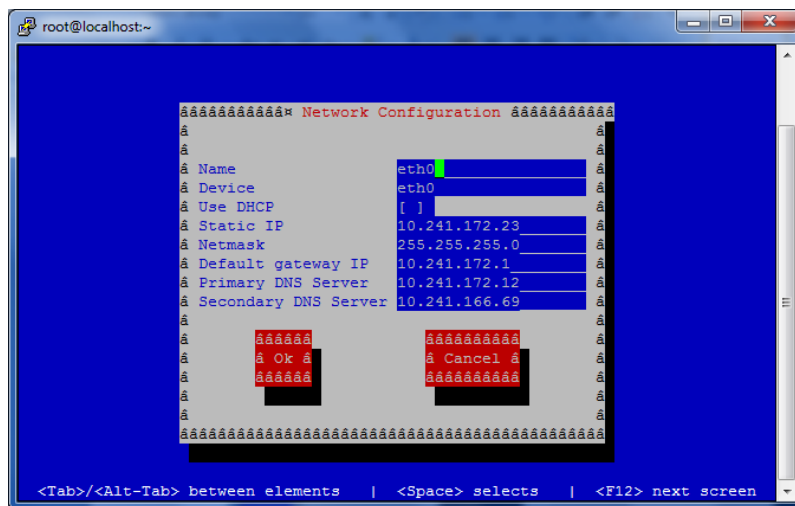


Figure 10 Network Configuration

8. To accept Network configuration changes, select **OK**. The Device and DNS configuration screen appears.

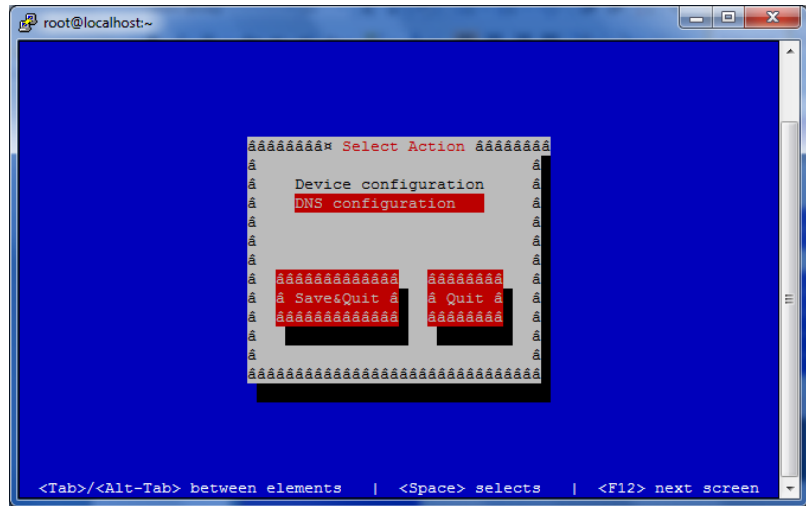


Figure 11 DNS Configuration

9. Select **DNS configuration**.

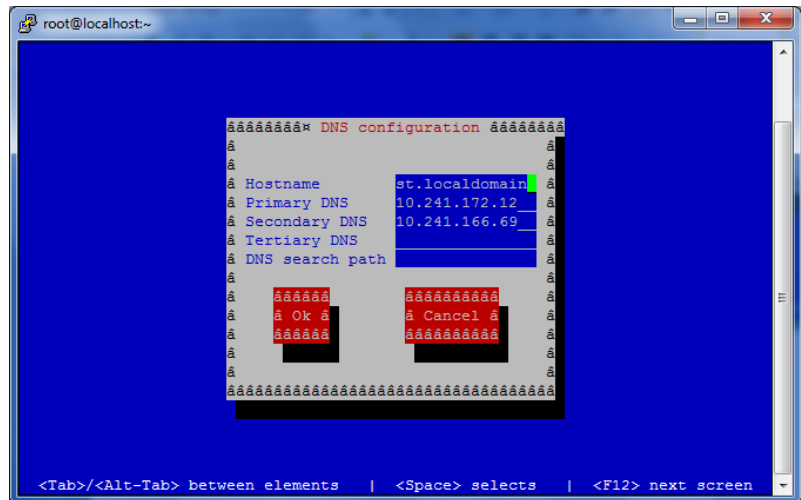


Figure 12 DNS Configuration

10. To accept DNS configuration changes, select **OK**. The Device and DNS configuration screen appears.

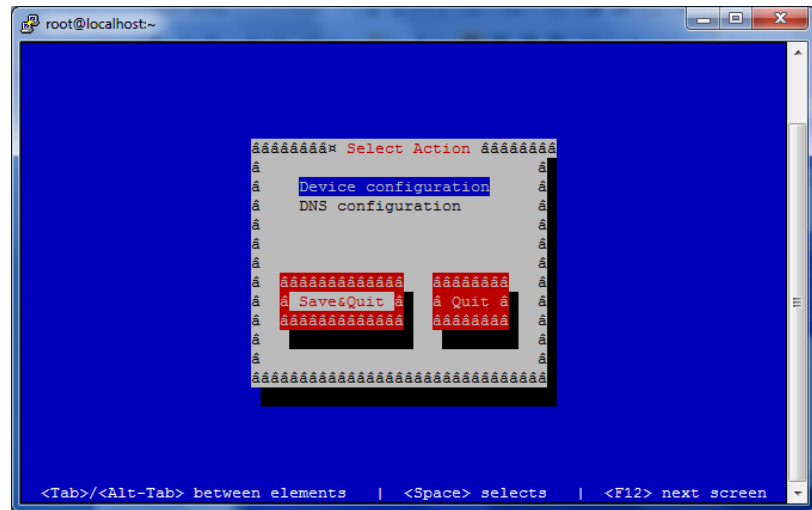


Figure 13 Saving Device and DNS Configuration

11. Select **Save&Quit**. The Red Hat Setup Utility main screen appears.
12. DNS configuration screen appears.

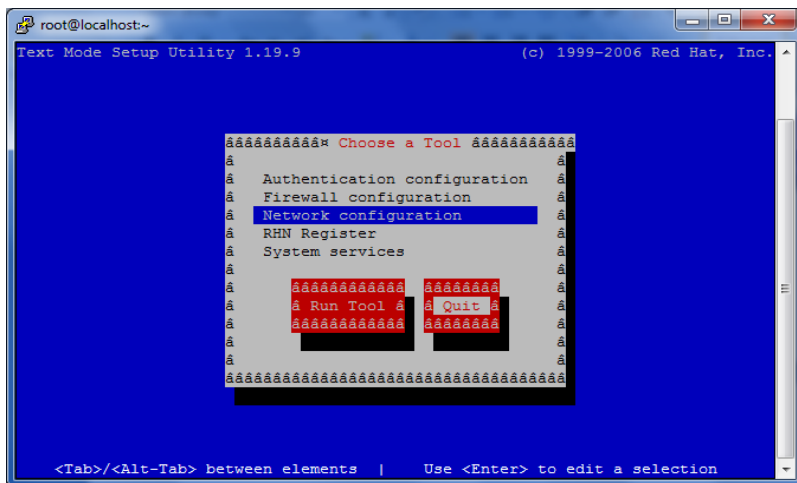


Figure 14 Quit Red Hat Setup Utility

13. Select **Quit**, and press **Enter**.

Activate the Ethernet Port

You need to bring the Ethernet port up and active, as follows:

1. Type:

```
/sbin/ifup eth{x}
```
2. This command will permit you to shell in to the server over the network.

Note: Refer to Red Hat Enterprise Linux (RHEL) documentation on starting SSHD server; it may not be started by default. You will not be able to use a shell without this server being started.

Create Users and Set Passwords

You need to create users and set passwords, as follows:

- The Password for **onalert** and **ONALERT** users is **EMCCONNECT**.
 - The Password for **emailalert** and **emailalertesg** can be anything you want as these accounts are to permit the receipt of email connect homes.
 - The Password for **esrsconfig** is **esrsconfig**.
1. Log in to the server as root or as a user and su.
 2. Add users and set passwords as shown in the following example:

```
[root@localhost ~]# /usr/sbin/useradd onalert
[root@localhost ~]# /usr/sbin/useradd ONALERT
[root@localhost ~]# /usr/sbin/useradd esrsconfig
[root@localhost ~]# /usr/sbin/useradd emailalert
[root@localhost ~]# /usr/sbin/useradd emailalertesg
[root@localhost ~]# /usr/bin/passwd onalert
Changing password for user onalert.
New password:
passwd: all authentication tokens updated
successfully.
[root@localhost ~]# /usr/bin/passwd ONALERT
Changing password for user ONALERT.
New password:
passwd: all authentication tokens updated
successfully.
[root@localhost ~]# /usr/bin/passwd esrsconfig
Changing password for user esrsconfig.
New password:
passwd: all authentication tokens updated
successfully.
[root@localhost ~]# /usr/bin/passwd emailalert
Changing password for user emailalert.
New password:
passwd: all authentication tokens updated
successfully.
[root@localhost ~]# /usr/bin/passwd emailalertesg
Changing password for user emailalertesg.
New password:
passwd: all authentication tokens updated
successfully.
[root@localhost ~]# ls
emailalert emailalertesg esrsconfig onalert ONALERT
```

Figure 15 Adding Users and Setting Passwords

Install vsftpd for FTP and Email

Note: The process below requires that the RHEL server be registered with Red Hat. FTP (vsftpd AND postfix will be reconfigured by the Gateways (Provisioning Tool) process. NO configuration is needed at this time.

Install vsftpd

1. To install vsftpd, run:

```
[root@localhost ~]# yum install vsftpd
Loaded plugins: product-id, rhnplugin, security,
subscription-manager
Updating certificate-based repositories.
rhel-i386-server-6
1.8 kB      00:00
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package vsftpd.i686 0:2.2.2-11.el6 will be
installed
--> Finished Dependency Resolution
```

Dependencies Resolved

```
=====
=====
Package      Arch      Version      Repository
Size
=====
Installing:
  vsftpd      i686      2.2.2-11.el6
rhel-i386-server-6      157 k
```

Transaction Summary

```
=====
=====
Install      1 Package(s)
```

Total download size: 157 k

Installed size: 0

Is this ok [y/N]: y

Downloading Packages:

vsftpd-2.2.2-11.el6.i686.rpm

```
| 157 kB      00:00
```

warning: rpmts_HdrFromFdno: Header V3 RSA/SHA256

Signature, key ID fd431d51: NOKEY

Retrieving key from

file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

```

Importing GPG key 0xFD431D51:
  Userid : Red Hat, Inc. (release key 2)
<security@redhat.com>
  Package:
redhat-release-server-6Server-6.2.0.3.el6.i686
(@anaconda-RedHatEnterpriseLinux-201111171035.i386/6.
2)
  From   : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
Importing GPG key 0x2FA658E0:
  Userid : Red Hat, Inc. (auxiliary key)
<security@redhat.com>
  Package:
redhat-release-server-6Server-6.2.0.3.el6.i686
(@anaconda-RedHatEnterpriseLinux-201111171035.i386/6.
2)
  From   : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : vsftpd-2.2.2-11.el6.i686
1/1
Installed products updated.

Installed:
  vsftpd.i686 0:2.2.2-11.el6

Complete!

```

Figure 16 **Installing vsftpd**

2. Verify service is running by typing:

```

cd /etc/init.d/
service vsftpd status

```

Figure 17 **Verifying vsftpd service**

Install postfix

1. To install postfix, run:

```
[root@localhost ~]# yum install postfix
Loaded plugins: product-id, rhnplugin, security,
subscription-manager
Updating certificate-based repositories.
Setting up Install Process
Package 2:postfix-2.6.6-2.2.el6_1.i686 already
installed and latest version
Nothing to do
```

Figure 18 **Installing postfix**

2. Verify service is running by typing:

```
cd /etc/init.d/
service vsftpd status
```

Figure 19 **Verifying postfix service**

Create directories and install CECT and Provisioning Tool (PvT)

This section describes how to create directories and install the Customer Environment Check Tool (CECE) and Provisioning Tool (PvT).

1. To create directories, run:

```
[root@localhost home]# cd /opt/
[root@localhost opt]# mkdir emc
[root@localhost opt]# mkdir emc/esrs2
[root@localhost opt]# mkdir emc/esrs2/PvT
[root@localhost opt]# cd emc/esrs2
```

Figure 20 Creating Gateway install directories

2. Copy the CECT-2.24.00.06.tar (or later) to the /opt/emc/esrs2 directory, and verify:

```
[root@localhost esrs2]# ls
CECT  CECT-2.24.00.06.tar  PvT
```

Figure 21 Copying .tar file and verifying

3. To install the CECT, run:

```
[root@localhost esrs2]# tar -xvf CECT-2.24.00.06.tar
CECT/
CECT/license.pdf
CECT/LICENSE.txt
CECT/CECT
CECT/CECT.sh
CECT/config.xml
[root@localhost esrs2]# ls -l
total 4592
drwxr-xr-x. 2 root root    4096 Dec 26 11:48 CECT
-rw-r--r--. 1 root root 4689920 Dec 26 16:04
CECT-2.24.00.06.tar
drwxr-xr-x. 2 root root    4096 Jan 14 10:54 PvT
```

Figure 22 Running tar -xvf

4. To change to the PvT directory, run:

```
[root@localhost esrs2]# cd PvT
```

Figure 23 Changing to PvT directory

5. Copy the esrs-pvt-2.24.00.06.tar.gz to the PvT directory and untar it:

```
[root@localhost PvT]# tar -xvf esrs-pvt-2.24.00.06.tar.gz
configuration.xml
provision_agent
[root@localhost PvT]# ls -l
total 14376
-rw-r--r--. 1 root root      150 Jan 10 09:13 configuration.xml
-rw-r--r--. 1 root root 7362560 Jan 10 21:07
esrs-pvt-2.24.00.06.tar.gz
-rwxr-xr-x. 1 root root 7351475 Jan 10 09:13 provision_agent
[root@localhost esrs2]# ls -l
total 4592
drwxr-xr-x. 2 root root      4096 Dec 26 11:48 CECT
-rw-r--r--. 1 root root 4689920 Dec 26 16:04 CECT-2.24.00.06.tar
drwxr-xr-x. 2 root root      4096 Jan 14 10:54 PvT
[root@localhost esrs2]# cd CECT
[root@localhost CECT]#
```

Figure 24 Copying tar.gz to PVT directory and running tar -xvf

6. The ESRS Code and Tools are now on the Linux Server. Proceed by executing the Provisioning Tool with the necessary arguments. This must be performed by EMC personnel with RSA SecurID.
7. Change to the directory in which you installed the Provisioning Tool (PvT), and run the following to view the syntax for the provision_agent command:

```
[root@localhost PvT]# ./provision_agent --help
Usage: provision_agent [args]
--user-name      User Name
--emc-user       If user is CE
--reprovision    To reprovision the Serial number(Not
applicable for Linux Gateway)
--http --socks   Use either of them to set the Proxy Type
--proxy-host     Proxy IP or Host address.Used only with
either --http or --socks else its ignored
--proxy-port     Proxy port number.Used only with either
--http or --socks else its ignored
--proxy-user     Proxy user Name.Used only with either
--http or --socks else its ignored
--install-dir    Install Directory path
--site-id       Site Id (applicable only for a gateway)
--reprovision    To reprovision the Serial number (not
applicable for gateway)
--uninstall      Uninstall agent(applicable only for a
gateway)
--help          To list the agent proxy help details
```

```

Example:
Install gateway agent: provision_agent --user-name
<name> --emc-user --site-id <siteid>
Install DC agent: provision_agent --user-name <name>
--emc-user --reprovision
Install gateway agent with proxy: provision_agent
--user-name <name> --emc-user --site-id <siteid>
--http --proxy-host proxy.abc.com --proxy-port 3128

```

Figure 25 provision_agent command syntax

8. To run the provision_agent command with arguments, run:

```

[root@localhost PvT]# ./provision_agent --user-name
smithj --emc-user --site-id 11145366 --install-dir
/opt/emc/esrs2/
Please enter user password:
Device Name : ESRS-GW
User has Administration rights Passed.
ESRS Client is not installed on this system Passed.
FTP service is installed Passed.
SMTPService is installed Passed.
HTTPSService is not installed Passed.
HTTPS port 443 is in use Passed.
Application requires 100MB of free disk space Passed.
Disk Space 12536 MB is available.
User does have write permission Passed.
Verifying is ESRS2 Service is running...
ESRS2 client services are not running. -9
User Type : emcorasp
User Name : smithj
Logging In...

User Name : smithj
Login Successful
Authorizing...

EMC Authorization Successful
Downloading Software...
OS details
Linux
Red Hat Enterprise Linux Server release 6.2 (Santiago)
i686
Interface name: lo
IP Address: 127.0.0.1
IP Address: 0:0:0:0:0:0:1
Interface name: eth0
IP Address: 10.241.172.23
IP Address: FE80:0:0:0:20C:29FF:FE0D:51B7
cache size : 2048 KB
cache size : 2048 KB
cache size : 2048 KB

```

```

cache size      : 2048 KB
Finished downloading...
Software bundle downloaded from server

Installing software...
Gateway Model
Opening EmcDeployConfig.so...

Loading symbol ...
Closing library...
0

Software installed successfully.

```

Figure 26 Running `provision_agent` command with arguments

9. To verify Gateway status, run the following command to view the syntax of the `gateway_status` command:

```

[root@localhost Gateway]# ./gateway_status --help
Usage : gateway_status [args]

--agent-status  To display agent status information.
--remote-session  To display Active Remote Sessions.
--service-status  To display ESRS related Service
information.
--help          To list the gateway status help details
Example:
To display agent info: gateway_status --agent-status
To display all info: gateway_status --agent-status
--remote-session --service-status

```

Figure 27 `gateway_status` command syntax

10. To view Gateway status information, run:

```

[root@localhost Gateway]# ./gateway_status
--agent-status

ESRS-IP Client Connectivity to EMC Enterprise

Client Version: 2.24.00.06
Serial Number: ESRSGW_11145366_13011508374403
Install Directory: /opt/emc/esrs2/
Connecting To: esrs-corestg.emc.com on port 443
Connection Status: Connected
Proxy Server: Disabled
Policy Manager: Disabled.
SSL: Enabled, strength 168
Certificate: Enabled, supported true
Avg HB Response: 1.022 seconds

```

Cluster Info: Standalone

Figure 28 Viewing Gateway Status

11. To view Gateway service information, run:

```
[root@localhost Gateway]# ./gateway_status
--service-status
```

Connect Home Services

```
FTP Service:      Running
SMTP Service:     Running
HTTPS Service:    Running
```

ESRS-IP Dependent Service Status

```
Gateway:          Running
Watchdog:         Running
```

ESRS-IP Gateway as Proxy Service Status

```
Proxy Service:    Running
```

Figure 29 Viewing Gateway service information

12. To view active remote sessions:

```
[root@localhost Gateway]# ./gateway_status
--remote-session
```

Active Remote Sessions

Remote Sessions:

Figure 30 Viewing active service information

13. To run the gateway_status command with all arguments:

```
[root@localhost Gateway]# ./gateway_status
--agent-status --service-status --remote-session
```

ESRS-IP Client Connectivity to EMC Enterprise

```
Client Version: 2.24.00.06
Serial Number:  ESRSGW_11145366_13011508374403
Install Directory: /opt/emc/esrs2/
Connecting To:  esrs-corestg.emc.com on port 443
Connection Status: Connected
Proxy Server: Disabled
Policy Manager: Disabled.
```



```
SSL: Enabled, strength 168
Certificate: Enabled, supported true
Avg HB Response: 1.022 seconds
Cluster Info: Standalone

Active Remote Sessions

Remote Sessions:

Connect Home Services

FTP Service:      Running
SMTP Service:     Running
HTTPS Service:    Running

ESRS-IP Dependent Service Status

Gateway:          Running
Watchdog:         Running

ESRS-IP Gateway as Proxy Service Status

Proxy Service:    Running
[root@localhost Gateway]#
```

Figure 31 Running gateway_status command with all arguments



IMPORTANT

The following procedures **MUST** be performed **AFTER** the Gateway Client is installed. Connect home **MUST** be tested on all listener services (FTP, SMTP, ESRSHHTTPS) and verified on ServiceLink that the files are received. Failure to do so will result in missed connect homes that may result in Data Unavailable or Data Loss.

Post ESRS Client install and configure permissions and firewall for vsftpd and Postfix

1. For vsftpd, run:

Note: setsebool is an OS utility that changes the value of a given item.

```
[root@localhost Gateway]#
[root@localhost Gateway]# setsebool -P ftp_home_dir on
[root@localhost Gateway]# setsebool -P
allow_ftp_full_access on
[root@localhost Gateway]#
```

Figure 32 Running setsebool for vsftpd



IMPORTANT

Before proceeding further AND for the following process to be successful, send 1 or 2 emails to the Gateway from a device. This is necessary to permit the postfix and the process below to proceed and be successful configure postfix (email) to set permissions and reconfigure POSTFIX to use the Gateway/work directly as the root for the mail service.

2. For POSTFIX, you need to modify selinux to allow Postfix to write to /opt/esrs/emc/Gateway/...

Note: selinux is an OS based access control system.

```
Set selinux to permissive
vi /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of
#                 enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
restart server
```

Figure 33 Modifying selinux for Postfix

3. To install audit2allow, run:

```
[root@localhost ~]# yum install policycoreutils-python
Loaded plugins: product-id, rhnplugin, security,
subscription-manager
Updating certificate-based repositories.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package policycoreutils-python.i686
0:2.0.83-19.24.el6 will be installed
--> Processing Dependency: policycoreutils =
2.0.83-19.24.el6 for package: polic
ycoreutils-python-2.0.83-19.24.el6.i686
--> Processing Dependency: libsemanage-python >=
2.0.43-4 for package: policycor
eutils-python-2.0.83-19.24.el6.i686
--> Processing Dependency: audit-libs-python >=
1.4.2-1 for package: policycoreu
tils-python-2.0.83-19.24.el6.i686
--> Processing Dependency: setools-libs-python for
package: policycoreutils-pyth
on-2.0.83-19.24.el6.i686
--> Processing Dependency: libselinux-python for
package: policycoreutils-python
-2.0.83-19.24.el6.i686
--> Running transaction check
---> Package audit-libs-python.i686 0:2.2-2.el6 will
be installed
--> Processing Dependency: audit-libs = 2.2-2.el6 for
package: audit-libs-python
-2.2-2.el6.i686
---> Package libselinux-python.i686 0:2.0.94-5.3.el6
will be installed
--> Processing Dependency: libselinux = 2.0.94-5.3.el6
for package: libselinux-p
ython-2.0.94-5.3.el6.i686
---> Package libsemanage-python.i686 0:2.0.43-4.1.el6
will be installed
---> Package policycoreutils.i686 0:2.0.83-19.18.el6
will be updated
---> Package policycoreutils.i686 0:2.0.83-19.24.el6
will be an update
---> Package setools-libs-python.i686 0:3.3.7-4.el6
will be installed
--> Processing Dependency: setools-libs = 3.3.7-4.el6
for package: setools-libs-
python-3.3.7-4.el6.i686
--> Processing Dependency: libsefs.so.4(VERS_4.0) for
package: setools-libs-pyth
on-3.3.7-4.el6.i686
```

```

--> Processing Dependency: libsefs.so.4 for package:
setools-libs-python-3.3.7-4
.el6.i686
--> Processing Dependency: libseaudit.so.4(VERS_4.2)
for package: setools-libs-p
ython-3.3.7-4.el6.i686
--> Processing Dependency: libseaudit.so.4(VERS_4.1)
for package: setools-libs-p
ython-3.3.7-4.el6.i686
--> Processing Dependency: libseaudit.so.4 for
package: setools-libs-python-3.3.
7-4.el6.i686
--> Processing Dependency: libqpol.so.1(VERS_1.4) for
package: setools-libs-pyth
on-3.3.7-4.el6.i686
--> Processing Dependency: libqpol.so.1(VERS_1.3) for
package: setools-libs-pyth
on-3.3.7-4.el6.i686
--> Processing Dependency: libqpol.so.1(VERS_1.2) for
package: setools-libs-pyth
on-3.3.7-4.el6.i686
--> Processing Dependency: libqpol.so.1 for package:
setools-libs-python-3.3.7-4
.el6.i686
--> Processing Dependency: libpoldiff.so.1(VERS_1.3)
for package: setools-libs-p
ython-3.3.7-4.el6.i686
--> Processing Dependency: libpoldiff.so.1(VERS_1.2)
for package: setools-libs-p
ython-3.3.7-4.el6.i686
--> Processing Dependency: libpoldiff.so.1 for
package: setools-libs-python-3.3.
7-4.el6.i686
--> Processing Dependency: libapol.so.4(VERS_4.1) for
package: setools-libs-pyth
on-3.3.7-4.el6.i686
--> Processing Dependency: libapol.so.4(VERS_4.0) for
package: setools-libs-pyth
on-3.3.7-4.el6.i686
--> Processing Dependency: libapol.so.4 for package:
setools-libs-python-3.3.7-4
.el6.i686
--> Running transaction check
---> Package audit-libs.i686 0:2.1.3-3.el6 will be
updated
--> Processing Dependency: audit-libs = 2.1.3-3.el6 for
package: audit-2.1.3-3.e
l6.i686
---> Package audit-libs.i686 0:2.2-2.el6 will be an
update
---> Package libselinux.i686 0:2.0.94-5.2.el6 will be
updated

```

```
--> Processing Dependency: libselinux = 2.0.94-5.2.el6
for package: libselinux-u
tils-2.0.94-5.2.el6.i686
---> Package libselinux.i686 0:2.0.94-5.3.el6 will be
an update
---> Package setools-libs.i686 0:3.3.7-4.el6 will be
installed
--> Running transaction check
---> Package audit.i686 0:2.1.3-3.el6 will be updated
---> Package audit.i686 0:2.2-2.el6 will be an update
---> Package libselinux-utils.i686 0:2.0.94-5.2.el6
will be updated
---> Package libselinux-utils.i686 0:2.0.94-5.3.el6
will be an update
--> Finished Dependency Resolution
```

Dependencies Resolved

```
=====
=====
Package                Arch Version      Repository
Size
=====
=====
Installing:
polycoreutils-python   i686   2.0.83-19.24.el6
rhel-i386-server-6     338 k
Installing for dependencies:
audit-libs-python      i686   2.2-2.el6
rhel-i386-server-6     57 k
libselinux-python      i686   2.0.94-5.3.el6
rhel-i386-server-6     199 k
libsemanage-python     i686   2.0.43-4.1.el6
rhel-i386-server-6     80 k
setools-libs           i686   3.3.7-4.el6
rhel-i386-server-6     400 k
setools-libs-python    i686   3.3.7-4.el6
rhel-i386-server-6     210 k
Updating for dependencies:
audit                  i686   2.2-2.el6
rhel-i386-server-6     225 k
audit-libs            i686   2.2-2.el6
rhel-i386-server-6     60 k
libselinux            i686   2.0.94-5.3.el6
rhel-i386-server-6     108 k
libselinux-utils      i686   2.0.94-5.3.el6
rhel-i386-server-6     81 k
polycoreutils         i686   2.0.83-19.24.el6
rhel-i386-server-6     671 k
```

Transaction Summary

```

=====
=====
Install          6 Package(s)
Upgrade         5 Package(s)

Total download size: 2.4 M
Is this ok [y/N]: y
Downloading Packages:
(1/11): audit-2.2-2.el6.i686.rpm
| 225 kB      00:00
(2/11): audit-libs-2.2-2.el6.i686.rpm
| 60 kB       00:00
(3/11): audit-libs-python-2.2-2.el6.i686.rpm
| 57 kB       00:00
(4/11): libselinux-2.0.94-5.3.el6.i686.rpm
| 108 kB      00:00
(5/11): libselinux-python-2.0.94-5.3.el6.i686.rpm
| 199 kB      00:00
(6/11): libselinux-utils-2.0.94-5.3.el6.i686.rpm
| 81 kB       00:00
(7/11): libsemanage-python-2.0.43-4.1.el6.i686.rpm
| 80 kB       00:00
(8/11): policycoreutils-2.0.83-19.24.el6.i686.rpm
| 671 kB      00:00
(9/11):
policycoreutils-python-2.0.83-19.24.el6.i686.rpm
| 338 kB      00:00
(10/11): setools-libs-3.3.7-4.el6.i686.rpm
| 400 kB      00:00
(11/11): setools-libs-python-3.3.7-4.el6.i686.rpm
| 210 kB      00:00
-----
-----
Total
85 kB/s | 2.4 MB      00:28
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Updating : libselinux-2.0.94-5.3.el6.i686
1/16
Updating : audit-libs-2.2-2.el6.i686
2/16
Installing: audit-libs-python-2.2-2.el6.i686
3/16
Installing: libselinux-python-2.0.94-5.3.el6.i686
4/16
Updating : libselinux-utils-2.0.94-5.3.el6.i686
5/16
Updating : policycoreutils-2.0.83-19.24.el6.i686
6/16

```

```

Installing: setools-libs-3.3.7-4.el6.i686
7/16
Installing: setools-libs-python-3.3.7-4.el6.i686
8/16
Installing: libsemanage-python-2.0.43-4.1.el6.i686
9/16
Installing :
policycoreutils-python-2.0.83-19.24.el6.i686
10/16
Updating : audit-2.2-2.el6.i686
11/16
Cleanup : policycoreutils-2.0.83-19.18.el6.i686
12/16
Cleanup : libselinux-utils-2.0.94-5.2.el6.i686
13/16
Cleanup : audit-2.1.3-3.el6.i686
14/16
Cleanup : audit-libs-2.1.3-3.el6.i686
15/16
Cleanup : libselinux-2.0.94-5.2.el6.i686
16/16
Installed products updated.

Installed:
  policycoreutils-python.i686 0:2.0.83-19.24.el6

Dependency Installed:
  audit-libs-python.i686 0:2.2-2.el6
  libselinux-python.i686 0:2.0.94-5.3.el6
  libsemanage-python.i686 0:2.0.43-4.1.el6
  setools-libs.i686 0:3.3.7-4.el6
  setools-libs-python.i686 0:3.3.7-4.el6

Dependency Updated:
  audit.i686 0:2.2-2.el6          audit-libs.i686
0:2.2-2.el6          libselinux.i686
0:2.0.94-5.3.el6
  libselinux-utils.i686 0:2.0.94-5.3.el6
  policycoreutils.i686 0:2.0.83-19.24.el6

Complete!

```

Figure 34 **Installing audit2allow**

4. To stage the change to Postfix, run:

```
[root@localhost audit]# cd /opt/emc/esrs2
[root@localhost esrs2]# grep local_t
/var/log/audit/audit.log | audit2allow -m postfixlocal
> postfixlocal.te
```

Figure 35 Staging the change to Postfix

5. To create the selinux module, run:

```
[root@localhost esrs2]# cat postfixlocal.te

module postfixlocal 1.0;

require {
    type postfix_local_t;
    type usr_t;
    class capability chown;
    class dir { write remove_name add_name };
    class file { write create unlink setattr append
};
}

#===== postfix_local_t =====
allow postfix_local_t self:capability chown;
#!!!! The source type 'postfix_local_t' can write to a
'dir' of the following types:
# var_run_t, user_home_t, dovecot_spool_t,
mailman_data_t, tmp_t, user_home_dir_t,
postfix_local_tmp_t, nfs_t, mail_spool_t

allow postfix_local_t usr_t:dir { write remove_name
add_name };
allow postfix_local_t usr_t:file { write create unlink
append setattr };
```

Figure 36 Creating the selinux module

6. Run:

```
[root@localhost esrs2]# grep local_t
/var/log/audit/audit.log | audit2allow -M postfixlocal

***** IMPORTANT *****
To make this policy package active, run:
semodule -i postfixlocal.pp
```

Figure 37 Making policy package active

7. To install the semodule, run:

```
[root@localhost esrs2]# semodule -i postfixlocal.pp
```

Note: audit2allow generates rules from logs.

Figure 38 **Installing semodule**

8. To verify that it installed, run:

Note: semodule manages OS policy modules

```
[root@localhost esrs2]# semodule -l |grep post
postfix 1.11.0
postfixlocal 1.0
postgresql 1.12.1
postgrey 1.7.0
[root@localhost esrs2]#reboot now
```

The Linux server WILL reboot

!! IMPORTANT !!

Test all callhome protocols and verify that the Gateway receives the callhome and that they are present on ServiceLink.

Figure 39 **Verifying semodule install**

Verify status of Gateway and services

1. To verify the status of the Gateway and services, run:

```
[root@localhost Gateway]# ./gateway_status
--agent-status
ESRS-IP Client Connectivity to EMC Enterprise

Client Version: 2.24.00.06
Serial Number: ESRSGW_11145366_13011508374403
Install Directory: /opt/emc/esrs2/
Connecting To: esrs-corestg.emc.com on port 443
Connection Status: Connected
Proxy Server: Disabled
Policy Manager: Disabled.
SSL: Enabled, strength 168
Certificate: Enabled, supported true
Avg HB Response: 2.613 seconds
Cluster Info: SERVICE, 3 members.
[root@localhost Gateway]#
[root@localhost Gateway]# ./gateway_status
--service-status

Connect Home Services

FTP Service:      Running
SMTP Service:    Running
HTTPS Service:   Running

ESRS-IP Dependent Service Status

Gateway:          Running
Watchdog:         Running

ESRS-IP Gateway as Proxy Service Status

Proxy Service:   Running
[root@localhost Gateway]#
```

Figure 40 Verifying Gateway and service status

2. To configure the Gateway to use a Policy Manager, edit the configuration, or remove the Policy Manager, use the `config_policy_manager.sh` command. To view the syntax of the `config_policy_manager.sh` command, run:

```
[root@localhost Gateway]# ./config_policy_manager.sh
--help

Usage: config_policy_manager [args]
```

```

--add          adds the agent policy manager
configuration
--remove       removes the policy manager configuration
--secure       if specified, use HTTPS protocol to
access the server
--host         the IP address of the policy manager host
--port         the port to use to access the policy
manager
--add-proxy    adds the proxy configuration
--remove-proxy removes the proxy configuration
--http --socks use either of them to set the Proxy Type
--proxy-host   the IP or Host address.
--proxy-port   proxy port number.
--proxy-user   proxy user Name.
--list         To list the agent policy manager details
--help         To list the agent proxy help details
Example:
Add a policy manager: config_policy_manager --add
--secure --host pm.abc.com
Add a proxy server: config_policy_manager --add-proxy
--http --proxy-host policy.abc.com

```

Note: If the proxy server has a username (--proxy-user) you will be prompted for the password after executing the command. The password is not stored in the history.

Figure 41 `config_policy_manager.sh` command syntax

3. Run the `config_policy_manager.sh` command with arguments as follows:

```

[root@localhost Gateway]# ./config_policy_manager.sh
--add --secure --host 10.241.172.13 --port 8443

```

```

Checking Policy Manager Connectivity...
Connected
Error : 0 Agent PM changes successful

```

Note: An Error code of 0 as above means successful; any other result (alpha or numeric) indicates some failure to complete successfully.

```

[root@localhost Gateway]# ./config_policy_manager.sh
--list
Policy Server
  Enabled: true
  Host: 10.241.172.13
  Port: 8443
  SSL Enabled: true
  SSL Strength: 128-bit

```

```
Proxy Server
  Enabled: false
[root@localhost Gateway]#
```

Figure 42 Running the `config_policy_manager.sh` command with arguments

4. To check Policy Manager configuration, run:

```
[root@localhost Gateway]# ./config_policy_manager.sh
--list
Policy Server
  Enabled: true
  Host: 10.241.172.13
  Port: 8443
  SSL Enabled: true
  SSL Strength: 128-bit
Proxy Server
  Enabled: false
[root@localhost Gateway]#
```

Figure 43 Checking the Policy Manager configuration

5. To view Gateway status information, run:

```
[root@localhost Gateway]# ./gateway_status
--agent-status
ESRS-IP Client Connectivity to EMC Enterprise

Client Version: 2.24.00.06
Serial Number: ESRSGW_11145366_13011508374403
Install Directory: /opt/emc/esrs2/
Connecting To: esrs-corestg.emc.com on port 443
Connection Status: Connected
Proxy Server: Disabled
Policy Manager: Enabled IP:10.241.172.13, port 8443;
connected, SSL Enabled
SSL: Enabled, strength 168
Certificate: Enabled, supported true
Avg HB Response: 0.000 seconds
Cluster Info: SERVICE, 3 members.
```

Figure 44 Viewing Gateway status information

To configure the Gateway to use a Proxy server, edit the configuration, or remove the Proxy Server

1. To view syntax for the `config_agent_proxy.sh` command, run:

```
[root@localhost Gateway]# ./config_agent_proxy.sh
--help
Usage : config_agent_proxy [args]

--add-proxy      To add the agent proxy configuration
--remove-proxy   To remove the proxy configuration
--http --socks   Use either of them to set the Proxy Type
--proxy-host     Proxy IP or Host address.
--proxy-port     Proxy port number.
--proxy-user     Proxy user Name.
--list          To list the agent proxy details
--help          To list the agent proxy help details
Example:
Add a proxy: config_agent_proxy --add-proxy --http
--proxy-host proxy.abc.com --proxy-port 3128
Remove a proxy server: config_agent_proxy
--remove-proxy
```

Note: If the proxy server has a username (`--proxy-user`) you will be prompted for the password after executing the command. The password is not stored in the history.

Figure 45 `config_agent_proxy.sh` command syntax

2. To configure the Gateway to use a Proxy server, run:

```
[root@localhost Gateway]# ./config_agent_proxy.sh
--add-proxy --http --proxy-host 10.241.172.13
--proxy-port 8118

Checking Proxy Connectivity... Host : 10.241.172.13
Port: 8118
ApplyProxyChangesToAgent successful.
AGENT PATH :/opt/emc/esrs2/Gateway
Privoxy user.action not modified.
Updating Privoxy config file Successful.
Error : 0 Agent Proxy configuration Successful.
```

Note: An Error code of 0 as above means successful; any other result (alpha or numeric) indicates some failure to complete successfully.

Figure 46 Configuring Gateway to use a Proxy server

3. To verify status of proxy server configuration, run:

```
[root@localhost Gateway]# ./config_agent_proxy.sh
--list
```

```
DRMProxy Server
  Enabled: true
  Proxy Type: HTTP
  Host: 10.241.172.13
  Port: 8118
  User name:
Error : 0 Agent Proxy configuration Successful.
```

Note: An Error code of 0 as above means successful; any other result (alpha or numeric) indicates some failure to complete successfully.

Figure 47 Verifying proxy server status

4. To view Gateway status information with proxy server configuration. run:

```
[root@localhost Gateway]# ./gateway_status
--agent-status
```

```
ESRS-IP Client Connectivity to EMC Enterprise
```

```
Client Version: 2.24.00.06
Serial Number: ESRSGW_11145366_13011508374403
Install Directory: /opt/emc/esrs2/
Connecting To: esrs-corestg.emc.com on port 443
Connection Status: Connected
Proxy Server: Enabled, HTTP IP:10.241.172.13 port 8118,
Connectivity Status: Online
Policy Manager: Enabled IP:10.241.172.13, port 8443;
connected, SSL Enabled
SSL: Enabled, strength 168
Certificate: Enabled, supported true
Avg HB Response: 3.690 seconds
Cluster Info: SERVICE, 3 members.
[root@localhost Gateway]#
```

Figure 48 Viewing Gateway status information

Manage Devices

1. To view the syntax for the `manage_device` command, run:

```
[root@localhost Gateway]# ./manage_device --help
Usage : manage_device [args]

--add-device      Adds a device to be managed
--modify-device   Modifies the IP address of an already
managed device
--remove-device   Removes a managed device
--model           Model of the managed device
--host            IP address of the device
--serialnumber    Serial number of the device with the
suffix
--list            To list the managed devices
--list-models     To list valid models
--show-history    To display device management history
--help           To list the help details
```

Example:

```
Add a device: ./manage_device --add-device --model
VNX-GWC --host 1.2.3.4 --serialnumber ABC123-BLOCKA
Modify a device: ./manage_device --modify-device
--model VNX-GWC --host 5.6.7.8 --serialnumber
ABC123-BLOCKA
Remove a device: ./manage_device --remove-device
--model VNX-GWC --host 1.2.3.4 --serialnumber
ABC123-BLOCKA
```

Figure 49 `manage_device` command syntax

2. To add all Device Types that are deployable on a Gateway, refer to [Table 5 on page 72](#), then run the `manage_device --add-device` command. Enter the following information:
 - Model Type
 - IP Address
 - Serial Number
 - Suffix, if applicable

Note: Serial number and Device type (model) are case sensitive. The serial number for Customer Management Station is auto-generated as shown in the examples on [Figure 50 on page 74](#) and [Figure 51 on page 75](#).

Table 5 on page 72 lists the valid product, suffixes, and code versions for each product:

Table 5 Valid Suffixes and Code Versions

Product	Suffix	Explanation	ESRS Gateway Code Version
Atmos	1-16		2.08
Avamar	None		2.08
Beta1	1-32		2.04
Beta2	1-32		2.04
Celerra	P S A	Primary Control Station (CS0) Secondary Control Station (CS1) Control Station Alias	2.02
Centera	1-36		2.02
CLARiiON	A B	SP A&B	2.02
Connectrix	CM, CLI		2.02
Customer Management Station	1-32		2.24
Data Domain	None		2.14
DCA	B P		2.12
DL3D	1 2 3		2.02
DLm	P S A	Primary Control Station (CS0) Secondary Control Station (CS1) Control Station Alias	2.02
DLm3	1000, ACP1, ACP2, ACPA		2.16
DLm4	VTE1, VTE2, VTEA		2.24
EDL	Blank A B	Blank for engine SP A&B	2.02
Invista	A B		2.02
RecoverPoint	1-16		2.02
Switch-Brocade-B	CM, CLI		2.02
Switch-Cisco	None		2.02

Table 5 Valid Suffixes and Code Versions

Product	Suffix	Explanation	ESRS Gateway Code Version
Symmetrix	None		2.02
VNX	FileP, FileS, FileA, BlockA, BlockB	Primary Control Station (CS0) Secondary Control Station (CS1) Control Station Alias, IP Block (SP A&B)	2.08
VMAX Cloud Edition (CE)	H1, H2, COL, AE, SE, VC, CECV	Host 1 (H1) Host 2 (H2) Collector (COL) Automation Engine (AE) Solutions Enabler (SE) vCenter (VC) ConnectEMC (CECV)	2.22
VNXe	None		2.08
VPLEX	None		2.04

For example:

```
./manage_device --add-device --model VNX-GW --host
10.241.216.233 --serialnumber FNM00104600113 --suffix
-BLOCKA
./manage_device --add-device --model RECOVERPOINT-GW
--host 10.241.172.143 --serialnumber 03PS12345678
--suffix -1
./manage_device --add-device --model Symmetrix-GW
--host 10.5.25.40 --serialnumber HK184502989
./manage_device --add-device --model VNX-GW --host
10.241.216.230 --serialnumber APM00112304752 --suffix
-FILEP
./manage_device --add-device --model Atmos-GW --host
10.5.25.40 --serialnumber 05DA0300000081 --suffix -1
./manage_device --add-device --model Avamar-GW --host
10.241.216.230 --serialnumber 13153569740024E855DC72
./manage_device --add-device --model Celerra-GW --host
10.241.216.230 --serialnumber APM00051002565 --suffix
-P
./manage_device --add-device --model Centera-GW --host
10.241.216.230 --serialnumber APM00031700200 --suffix
-1
./manage_device --add-device --model Datadomain-GW
--host 10.241.216.230 --serialnumber 5FP4112002
```

```

./manage_device --add-device --model DCA-GW --host
10.241.216.230 --serialnumber FNM00103500347 -suffix
-P
./manage_device --add-device --model DLM3-GW --host
10.241.216.230 --serialnumber APM00113501268 -suffix
-ACP-1
./manage_device --add-device --model
Switch-Brocade-B-GW --host 10.5.25.40 --serialnumber
BRCDN000015159
./manage_device --add-device --model Switch-Cisco-GW
--host 10.241.216.230 --serialnumber FOX102100BD
./manage_device --add-device --model VPLEX-GW --host
10.241.216.230 --serialnumber VS1CSE000003
./manage_device --add-device --model VNXe-GW --host
10.241.216.230 --serialnumber FNM00101100292
./manage_device --add-device --model Celerra-GW --host
10.241.216.230 --serialnumber 1F41509024 -suffix -P
./manage_device --add-device --model INVISTA-GW --host
10.241.216.230 --serialnumber 1F41509024 -suffix -A
./manage_device --add-device --model CustManageSta-GW
--host 10.241.216.230 -suffix -1

```

Figure 50 Running `manage_device --add-device`

3. To view the list of managed devices, run:

```

[root@localhost Gateway]# ./manage_device --list
Serial Number      Model              Status    IP Address
HK100080200042-A   CLARiion-GW       online
10.241.166.136
HK100080200042-B   CLARiion-GW       offline
10.15.54.210
APM00092504983-S   DLM-GW            online
10.241.208.183
APM00050503884-2   Centera-GW        offline
10.241.185.70
DEV10000000106-B   Invista-GW        offline
10.15.54.210
APM000906001517-1  Centera-GW        online
10.241.185.51
APM00090601520-1   Centera-GW        offline
10.241.185.53
APM00064304871     EDL-Engine-GW     online
10.241.166.184
05SDA0200000017-1  ATMOS-GW          online
10.6.146.41
APM00084902090-B   EDL-Engine-GW     online
10.241.216.100
FNM00093800021     VPLEX-GW          online
10.241.165.60
APM00080601397-1   DL3D-GW           offline
10.241.166.26

```

```

APM00084902090-A      EDL-Engine-GW      online
10.241.216.99
FCNHH050500031-P      Celerra-GW        online
10.241.168.84
APM00090601517-3      Centera-GW        offline
10.241.185.127
03PS12345678-1        RecoverPoint-GW   online
10.241.172.142
FNM00110300428        VNXe-GW           online
10.241.168.200
APM00110100565-P      DCA-GW            online
10.241.164.253
APM00105101002-P      DCA-GW            offline
10.5.214.28
1298999529842B2B4989C0AVAMAR-GW      offline
10.241.218.241
HK190309998           Symmetrix-GW      offline
10.241.216.81
1300986969842B2B498535AVAMAR-GW      offline
10.241.218.243
FNM00103200198-BLOCKAVNX-GW            online
10.6.12.95
CF2A5101500919-BLOCKAVNX-GW            offline
10.6.36.6
CF2A5101500919-BLOCKBVNX-GW            online
10.6.12.96
ALT11075000025-1      ATMOS-GW          online
10.241.218.89
HK195700133           Symmetrix-GW      online
10.15.54.211
ESRS2EDL1-A           CLARiion-GW       offline
10.15.69.60
FNM00104600112-BLOCKAVNX-GW            online
10.241.216.230
FNM00104600112-BLOCKBVNX-GW            online
10.241.216.231
MC51003826R           Connectrix-GW     offline 1.2.3.4
WCAKA072100825-1      RecoverPoint-GW   online
10.241.172.130
APM00114002265        VMAXCE-GW         online
10.241.168.24
ESRSGW_10174_130611234926_MSTA-1 CustManageSta-GW
online 10.241.216.230
[root@localhost Gateway]#

```

Figure 51 Viewing list of managed devices

Configuration CLI Commands

The Configuration CLI Commands are used to view Gateway Client status, manage devices for a Gateway Client, and perform other tasks related to your ESRS configuration.

This chapter includes the following topics:

- ◆ Configuration CLI Commands overview 78
- ◆ Installing the Configuration CLI Commands 79
- ◆ Using the Configuration CLI Commands 79

Configuration CLI Commands overview

The ESRS Configuration CLI Commands are used to manage Gateway Client devices and view and modify settings related to managed devices and related services.

Most of the Configuration CLI Commands are designed for access and use by authorized ESRS users. Some configuration activities, such as your device deployment requests or changes must be authorized by an EMC Global Services professional before they take effect.

The Configuration CLI Commands are used to:

- ◆ View connectivity status between the Gateway Client and EMC
- ◆ View connectivity status between the Gateway Client and Policy Manager
- ◆ View connectivity status between the Gateway Client and Managed Devices
- ◆ Initiate device deployment requests
- ◆ Initiate device removal requests
- ◆ Process managed device update requests
- ◆ Process managed device update requests
- ◆ View history of Deployment / UnDeployment or edit requests of devices
- ◆ Configure or change the Gateway Client for Proxy server
- ◆ Set up communication between the Policy Manager and the Gateway Client
- ◆ Configure or change the Gateway Client for Proxy server for the Policy Manager (if needed)
- ◆ View status of Watchdog, ESRS Gateway Client and Listener Services
- ◆ View only of active Remote Access Connection thru the ESRS Gateway Client
- ◆ View ESRS Gateway Client log

The following sections explain how to install and use the Configuration CLI Commands.

Installing the Configuration CLI Commands

Installing the Configuration CLI Commands

When you install a Gateway Client using the Provisioning Tool, the Configuration CLI Commands will automatically install on your Gateway Client.

Using the Configuration CLI Commands

Using the Configuration CLI Commands, you can:

- ◆ Check ESRS Gateway Client status (gateway_status)
- ◆ Manage Devices (manage_device)
- ◆ Proxy services (config_agent_proxy.sh)
- ◆ Policy Manager services (config_policy_manager)
- ◆ Remote Sessions (gateway_status)

gateway_status command options

The following options are available with the gateway_status command:

```
[root@localhost Gateway]# ./gateway_status --help
Usage : gateway_status [args]

--agent-status    To display agent status information.
--remote-session  To display Active Remote Sessions.
--service-status  To display ESRS related Service
information.
--help           To list the gateway status help details
```

Example:

```
To display agent info: gateway_status --agent-status
To display all info: gateway_status --agent-status
--remote-session --service-status
```

Figure 52 gateway_status command options

Viewing connectivity status

To view connectivity status, run the gateway_status command, as follows:

```
[root@185rhel62d Gateway]# ./gateway_status
--agent-status
```

```

ESRS-IP Client Connectivity to EMC Enterprise
Client Version: 2.24.00.06
Serial Number: ESRSGW_11145366_13011009472687
Install Directory: /opt/emc/esrs2/
Connecting To: esrs-corestg.emc.com on port 443
Connection Status: Connected
Proxy Server: Disabled
Policy Manager: Enabled IP:10.15.109.153, port 8443;
HTTP Proxy IP:10.15.109.95, port 3128; connected, SSL
Enabled
SSL: Enabled, strength 168
Certificate: Enabled, supported true
Avg HB Response: 0.357 seconds
Cluster Info: Standalone

```

Figure 53 Viewing Gateway connectivity status

The connectivity information in the `gateway_status` command is automatically populated when you run the Configuration CLI Commands.

Note: To update the status information, run the command again.

The `gateway_status` command displays the following information:

Connecting To — Displays the Domain Name System (DNS) name of the EMC enterprise

Connection Status — Displays Gateway Client connectivity to the EMC Enterprise. One of the following values is shown:

Connected — The Gateway Client is successfully connected to the EMC enterprise.

Not Connected — The Gateway Client service is running but is unable to connect to the EMC enterprise.

Not Running — The Gateway Client service is stopped and is not trying to connect to the EMC enterprise.

Proxy Server — Indicates whether a proxy server is enabled.

Policy Manager — Indicates whether Policy Manager is enabled (includes IP Address, Port, and Proxy, if enabled).

Proxy IP — Includes IP Address and Port, if enabled

SSL — Indicates whether Secure Socket Layer (SSL) communication is enabled to EMC.

Certificate — Indicates whether a digital certificate is enabled.

Average HB Response Time — Displays the average heartbeat (HB) response time from the Gateway Client to the EMC enterprise.

Diagnostic — Displays the reason that the Gateway Client is not connected to the EMC enterprise (only displays if Connectivity Status is Not Connected).

Cluster Info — If the Gateway Client is part of a High Availability Gateway Cluster, the Cluster Identifier will be displayed along with the number of Gateway Clients within the cluster. If the Gateway Client is *not* part of a High Availability Gateway Cluster, the words Stand Alone will be displayed.

manage_device command options

The following options are available with the `manage_device` command:

```
[root@LinuxGW Gateway]# ./manage_device --help
Usage : manage_device [args]

--add-device      Adds a device to be managed
--modify-device   Modifies the IP address of an already
managed device
--remove-device   Removes a managed device
--model           Model of the managed device
--host            IP address of the device
--serialnumber    Serial number of the device with the
suffix
--list            To list the managed devices
--list-models     To list valid models
--show-history    To display device management history
--help           To list the help details
```

Example:

```
Add a device: ./manage_device --add-device --model
VNX-GWC --host 1.2.3.4 --serialnumber ABC123-BLOCKA
Modify a device: ./manage_device --modify-device --model
VNX-GWC --host 5.6.7.8 --serialnumber ABC123-BLOCKA
Remove a device: ./manage_device --remove-device --model
VNX-GWC --host 1.2.3.4 --serialnumber ABC123-BLOCKA
```

Figure 54 **manage_device command options**

You can choose the following actions from the `manage_device` command:

add-device — Add a new device to be managed.

- modify-device** — Change the IP address of a managed device.
- remove_device** — Remove (unmanage) a device that is currently managed.
- history** — View history of all requests that have not yet been approved by an authorized EMC Global Services professional.
- model** — Model of the managed device
- host** — IP address of the device
- serialnumber** — Serial number of the device with the suffix
- list** — To list the managed devices
- list-models** — To list valid models
- show-history** — To display device management history

**manage_device
error codes**

Table 6 on page 82 describes error codes that may occur when running the manage_device command:

Table 6 manage_device error codes

Error code	Description
0	Everything is ok
1	The model is missing
2	The host is missing
3	The serial number is missing
4	The suffix is missing
5	User did not supply a command
6	User supplied too many commands
7	Could not load DeviceModels.xml
8	Could not load DeviceConnectivity.xml
9	Invalid model
10	Invalid suffix
11	Could not connect to device
12	Could not find an existing device

Table 6 **manage_device error codes**

Error code	Description
13	Device already exists
14	Gateway/Device Client service not running
14	Failed to connect to the Gateway/Device Client

Managing devices

To manage or view devices, run the `manage_device --list` command as follows:

```
[root@LinuxGW Gateway]# ./manage_device --list
Serial Number      Model              Status    IP
Address
FNM00104600112-BLOCKBVNX-GW      online
10.241.216.231
FNM00104600112-BLOCKAVNX-GW      online
10.241.216.230
APM00113910434      VNXXe-GW          online
10.241.168.35
HK192699998         Symmetrix-GW      online
168.159.16.12
APM00084902090-A    EDL-Engine-GW     online
10.241.216.99
APM00084902090-B    EDL-Engine-GW     online
10.241.216.100
FOX110905RG         Switch-Cisco-GW   online
10.241.174.190
SSI2480506          Switch-Cisco-GW   online
10.241.174.158
XK00401             Connectrix-GW     online
10.241.174.38
QV060000109         Switch-Brocade-B-GW online
10.241.174.63
AGF0602B00Y         Switch-Brocade-B-GW online
10.241.174.60
HK187490033         Symmetrix-GW      online
10.243.184.116
HK194900732         Symmetrix-GW      online
10.243.112.108
HK190103799         Symmetrix-GW      online
10.243.186.178
ESRSGW_10174_130611234926_MSTA-1  CustManageSta-GW
online      10.241.216.230
```

Figure 55 **manage_device --list command**

Adding a managed device

To add a managed device, run the `manage_device` command as in the following example:

```
./manage_device --add-device --model CENTERA --host
10.241.185.59 --serialnumber APM00205030103-2
```

```
Error: 0
```

Note: An Error code of 0 as above means successful; any other result (alpha or numeric) indicates some failure to complete successfully.

Figure 56 Adding a managed device

1. Enter the following device information:

- Model Type
- IP Address
- Serial Number
- Suffix, if applicable

Note: Refer to [Table 5, “Valid Suffixes and Code Versions,”](#) on page 72 for the list of valid suffixes and code versions for each product.

2. After entering the device information, the Configuration CLI Commands will run a connectivity test. An error message will appear if the connectivity test fails.

Note: The added device needs to be approved by EMC and may not be available immediately. The device goes into pending approval state in ServiceLink, and will not appear as a managed device until approved in ServiceLink.

3. The update will not take effect until it has been approved by an authorized EMC Global Services professional via the EMC enterprise.

Note: The ESRS Portal is located at the following url: esrs.emc.com.

4. Once the request has been approved via the EMC enterprise, and the synchronization process completes, you can view the device by running:

```
manage_device --list
```

Note: Please allow sufficient time for the approval and synchronization process to occur.

Modifying the IP address of a managed device

To modify the IP address of a managed device:

1. To modify the IP address of a managed device, run:

```
[root@LinuxGW Gateway]# ./manage_device
--modify-device --model Symmetrix-GW --host
168.159.16.12 --serialnumber HK192699998
```

Figure 57 **manage_device --modify-device command**

2. When you send the revised IP address to EMC, the update will not take effect until it has been approved by an authorized EMC Global Services professional.
3. When prompted, confirm the device you wish to edit. The previous IP address will be displayed until the edit has been approved by an authorized EMC Global Services professional via the EMC enterprise.
4. Once the request has been approved via the EMC enterprise, and the synchronization process completes, then run the **manage_device -- list** command to view the newly added device. Please allow sufficient time for the approval and synchronization process to occur, then perform the list command.

Unmanaging a device

To unmanage a managed device:

1. To unmanage a managed device, run:

```
[root@LinuxGW Gateway]# ./manage_device
--remove-device --model Symmetrix-GW --host
168.159.16.12 --serialnumber HK192699998
```

Figure 58 **manage_device --remove-device command**

2. The update will not take effect until it has been approved by an authorized EMC Global Service professional via the EMC enterprise. The device will remain listed as a managed device until the removal has been approved.

- Once the request has been approved via the EMC enterprise, and the synchronization process completes, run the list command to see if it has been removed. Please allow sufficient time for the approval and synchronization process to occur.

Submitting Managed Devices requests for approval

Your manage, edit, or unmanage requests will be submitted to EMC for implementation. When an authorized EMC Global Services professional has approved your requests via the EMC enterprise, the requested updates will be processed by the Gateway Client. The device information will be listed by running the list command. Any devices that have been removed will no longer be listed.

Note: Once you have submitted your requests for approval, they will no longer be listed in the Configuration CLI Commands until they have been approved by an authorized EMC Global Services professional via the EMC enterprise. The processed requests will not be listed until they have been approved and the associated synchronization process has completed.

Viewing history

To view transaction and configuration history, run:

```
[root@LinuxGW Gateway]# ./manage_device
--show-history
SerialNumber      Model              IPAddress
TransactionDate  TransactionType    FileName
FNM00104600112-BLOCKAVNX-GW  10.241.216.230
2013-01-10 12:21:18    Add Device        User Input
FNM00104600112-BLOCKBVNX-GW  10.241.216.231
2013-01-10 12:21:25    Add Device        User Input
APM00113910434      VNXe-GW           10.241.168.35
2013-01-10 12:22:05    Add Device        User Input
HK192699998         SYMMETRIX-GW      168.159.16.12
2013-01-10 12:22:53    Add Device        User Input
HK192699998         SYMMETRIX-GW      168.159.16.12
2013-01-10 13:39:27    Update Device     User Input
XK00401             CONNECTRIX-GW     10.241.174.38
2013-01-10 13:41:11    Add Device        User Input
FOX110905RG         SWITCH-CISCO-GW   10.241.174.190
2013-01-10 13:42:00    Add Device        User Input
```

Figure 59

manage_device --show-history command

Communicating through a proxy server

Gateway Clients can be configured to communicate directly through EMC or through an HTTPS or SOCKS proxy.

Enabling proxy server communication

To enable communication through a proxy server:

1. To enable proxy between the Client and EMC Enterprise, run:

```
config_agent_proxy.sh --add-proxy --http --proxy-host
proxy.abc.com --proxy-port 3128
```

Figure 60 **config_agent_proxy.sh command**

2. Provide the following proxy information as parameters to the command:

- Proxy Type
- IPS Address or DNS Name
- Port
- Username (if required)
- Password (if required)

The Configuration CLI Commands will use the proxy information you provided to verify connectivity between the Gateway Client and the EMC Enterprise. If connectivity is not available, an error message will be returned.

Note: You must provide a username and password if you are using a SOCKS proxy.

Disabling proxy server communication

To disable communication through a proxy server:

3. To disable proxy between Client and EMC Enterprise.

```
config_agent_proxy.sh --remove-proxy
```

Figure 61 **config_agent_proxy.sh --remove-proxy command**

The command will verify that there is direct connectivity between the Gateway Client and the EMC enterprise without the use of a proxy server. If connectivity is not available, an error message is returned.

Linking a Gateway Client to a Policy Manager

Linking a Gateway Client to a Policy Manager ensures that policy enforcement and auditing are enabled for the Gateway Client. For more information about using a Policy Manager, refer to the *EMC Secure Remote Support Policy Manager Operations Guide*.

The following procedure explains how use the Configuration CLI Commands to link a Gateway Client to a Policy Manager.

To link a Gateway Client to a Policy Manager:

1. To link a Gateway Client to a Policy Manager, run:

```
[root@185rhel62d Gateway]# ./config_policy_manager.sh
--add --secure --medium --host 10.15.109.153 --port
8443
Checking Policy Manager Connectivity...
Connected
Error : 0 Agent PM changes successful
```

Note: An Error code of 0 as above means successful; any other result (alpha or numeric) indicates some failure to complete successfully.

Figure 62 `config_policy_manager.sh` command

2. Provide the following Policy Manager information as parameters to the command:

- **host** (IP Address)
- **port**

Note: If you are utilizing SSL, you *must* enter port 8443. If you are not utilizing SSL, you must enter port 8090 or the port that you specified during installation. If the port and SSL combination is incorrect, the Gateway Client will not be able to communicate with the Policy Manager and EMC.

- **secure** (use HTTPS) along with an option to select cipher strength
- **low**, **medium**, or **high** (cipher strength) enables you to choose the cipher that will be used in communication between the Gateway Client computer and the Policy Manager:
 - For an AES 128-bit cipher, use **low** or **medium**.
 - For an AES 256-bit cipher or a 3DES 168-bit cipher, use **high**. The Policy Manager will apply the highest strength cipher that it supports.

Note: The highest strength cipher that Policy Manager currently supports is the 3DES 168-bit cipher. However, the Policy Manager can be configured to use the AES 256-bit cipher. For more information, refer to the *EMC Secure Remote Support Policy Manager Operations Guide*.

- **add-proxy.** If applicable, provide Proxy Server for Policy Manager only with the following parameters:
 - **http** or **socks.** The proxy will be used for Gateway Client to Policy Manager communication only. It will not affect the communication between the Gateway Client and the EMC Enterprise.

Note: If the Gateway Client cannot connect to the Policy Manager using the proxy you entered, it will attempt to connect without using the proxy server.

- **proxy-host,** provide with the IP address.
- **proxy-port,** provide with the port number.
- **proxy-user.** If applicable, provide with user name and password.

Note: You must provide a username and password if you are using a SOCKS proxy.

3. Running the command links the Gateway Client to the Policy Manager.
4. You can verify the connection by running the **config_policy_manager.sh --list** command.

Disabling communication

To disable communication between a Gateway Client and a Policy Manager, run the following command:

```
[root@185rhel62d Gateway]# ./config_policy_manager.sh
--remove
Error : 0 Agent PM changes successful
```

Note: An Error code of 0 as above means successful; any other result (alpha or numeric) indicates some failure to complete successfully.

Figure 63 **config_policy_manager.sh --remove** command

Note: Disabling communication with the Policy Manager will result in all permission settings for the Gateway Client being set to Always Allow.

Displaying the status of Services

To check the status of services related to ESRS and connect homes, run the following command.

```
[root@185rhel62d Gateway]# ./gateway_status
--service-status

Connect Home Services

FTP Service:      Running
SMTP Service:     Running
HTTPS Service:    Running

ESRS-IP Dependent Service Status

Gateway:          Running
Watchdog:         Running

ESRS-IP Gateway as Proxy Service Status

Proxy Service:    Running
```

Figure 64 **gateway_status --service-status command**

Each service is listed along with its current state (Running or Disabled).

Displaying active remote sessions

To display all active remote sessions to a managed device through the Gateway Client, run the following command:

```
[root@LinuxGW Gateway]# ./gateway_status
--remote-session

Active Remote Sessions

Remote Sessions:
  Symmetrix-GW HK187490033 RemotelyAnywhere
10.243.184.116
```

Figure 65 `gateway_status --remote-sessions` command

You will see a list of active remote sessions that includes the following data:

- ◆ Product type
- ◆ Serial number
- ◆ Remote Application name
- ◆ IP address

Note: You cannot terminate active sessions with this command. However, you can use the ESRS Policy Manager to view and terminate remote sessions.

Displaying the log files

To display the xGate log that shows configuration and transaction activity:

1. Change to the `/opt/emc/esrs2/Gateway` folder.
2. Run the following command:

```
cat xGate.log
```

Figure 66 `cat xGate.log` command

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

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

Topics in this section include:

◆ Power sequences	94
◆ Time Zone settings	95
◆ Service preparation for Gateway Client	96
◆ Backup guidelines and procedures	98
◆ Restoration procedures	99

Power sequences

EMC's customers routinely perform maintenance tasks that include powering down and powering up their data centers based on scheduled timeframes. While these powerdown/powerup sequences are defined by the customers' internal processes, the presence of the EMC Secure Remote Support Gateway in customer environments can affect the sequence in which powerdown/powerup actions are carried out.



IMPORTANT

Improper shutdown procedures generate service requests. Be sure to notify your EMC Customer Engineer of any shutdown plans to avoid unnecessary service calls.

Typically, the order in which powerdown sequences take place is as follows:

1. Hosts — So that the data has a chance to destage to disk and be captured.
2. Arrays — To allow destaging time for any pending writes to get to the disks for storage last.
3. Networking devices — After all data has been transported to the arrays.
4. Gateway Clients and Policy Manager servers.



IMPORTANT

EMC recommends that the ESRS Gateway Client server(s) and Policy Manager servers be the last devices powered down and the first devices powered up after maintenance is complete. This will enable support level access to the EMC end devices at all stages in the power up/ power down sequence.

Time Zone settings

The server Time Zone must be set to the correct time zone for the location of Gateway Client and Policy Manager servers.

Having the server Time Zone set to a setting other than the local time zone may adversely affect remote support tool performance.

Note: When changing the time zone on existing server installations, you must reboot the Gateway Client server after changing the setting.

Service preparation for Gateway Client

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

Gateway Client server

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

Logging preparation

The Gateway client 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 following configuration file. By default the Gateway client keeps up to 5 old files before cycling them, and this number can also be set as shown in the following conf file:

```
../Gateway/ESRS/xgLogFile.xml
```

Run the following command

```
[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.



CAUTION

If the server disk becomes full, the Gateway Client will fail to function properly for callhome messages, and possibly for support connections. If the problem is severe enough, the server operating will stop functioning.

It is the customer's responsibility to monitor and manage disk utilization on *both* the Gateway Client and Policy Manager servers.

Backup guidelines and procedures

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

Specific procedures depend on your:

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

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

Backup 1. **Gateway Client server image** — Refer to [“Server image backup” on page 98](#) for recommended Gateway server backup guidelines.

Restoration 2. **Gateway Client server** — Refer to [“Restoration procedures” on page 99](#) for recommended guidelines on restoring your server from image backup.

Server image backup

Image backup is the preferred method for backing up a Gateway Client server and data.

Initial setup

At installation time:

For each Gateway Client server:

1. Perform all needed installation stages—**hardening, ESRS software installation, configuration, deployment**—first.
2. Using your company’s approved procedure, create an image of the drive containing the installation root directory.

Optionally, for each Gateway server:

To provide a more complete configuration and data match to your server, periodically create a new drive image.

Restoration procedures

Restoration procedures will differ depending on the method of backup you are using.

Server image backup restoration

For a Gateway Client server:

Restore the disk drive by copying a backup image to that drive (use the most recent backup prior to the incident causing the problem).

Installation restoration

This section provides details on installation restoration.

For a Gateway Client server:

Reinstall the server software with the assistance of your EMC Global Services specialist or the EMC Global Services help desk.



CAUTION

If the server disk becomes full, the Gateway Client will fail to function properly for callhome messages might fail for support connections. If the problem is severe enough, the server operating system will stop functioning.

It is the customer's responsibility to monitor and manage disk utilization on the Gateway servers.

This appendix provides information about troubleshooting unexpected Gateway service events. It also explains how to troubleshoot the ESRSHTTPS listener, and describes how to perform configuration tasks such as install, remove, start, stop, and check status of the ESRS listener service.

- ◆ Troubleshooting unexpected Gateway service events..... 102
- ◆ Checking status and starting Gateway services 102
- ◆ Troubleshooting ESRSHTTPS listener service 103
- ◆ ESRSHTTPS listener service command line options 105
- ◆ ESRSHTTPS configuration 107

Troubleshooting unexpected Gateway service events

This section provides information about troubleshooting unexpected service events in the Gateway Client.

Service malfunction

If the Gateway Client service appears to malfunction, try to reboot and restart the service.

Service does not start up

If the Gateway Client service fails to manually start up from the Services window, refer to [“Checking status and starting Gateway services” on page 102](#).

Checking status and starting Gateway services

You can use the following command line scripts to check Gateway status and to start Gateway services:

Checking Gateway client service status

To check the Gateway client service status:

```
[root@185rhel62d ESRS]# service esrs2client status
Checking for service ESRS2 Client: xGate (pid 4369) is
running...
```

Starting the Gateway client service if not running already

To start the Gateway client service if not running already:

```
[root@185rhel62d ESRS]# service esrs2client start
Starting ESRS2 client:
OK ]
```

Checking the Gateway watchdog service status

To check the Gateway watchdog service status:

```
[root@185rhel62d ESRS]# service esrs2watchdog status
Checking for service ESRS2 Watchdog: xWatchDog (pid
4447) is running...
```

Starting the Gateway watchdog service

To start the Gateway watchdog service if not running already:

```
[root@185rhel62d ESRS]# service esrs2watchdog start
Starting ESRS2 Watchdog: xWatchDog running as daemon
process. [ OK ]
```

Cause of start up problem

A start up problem might be caused by files that have been inadvertently deleted or moved, as follows:

1. Examine the Gateway log file to confirm missing-file errors.
2. Attempt restoration from image backup. You may have to reinstall if image backup is not available. See [“Restoration procedures” on page 99](#).

Operating system or hardware failures

If a server failure clearly occurs at a more basic level than the Gateway Client service, you may want to perform a reinstallation, as described in [“Restoration procedures” on page 99](#).

Troubleshooting ESRSHTTPS listener service

The ESRSHTTPS listener service is used to accept the HTTPS event notifications from a ConnectEMC client application running on an EMC device. This section provides details on performing configuration tasks to troubleshoot the ESRSHTTPS listener.

Concepts

ESRSHTTPS registers to receive HTTPS requests for particular URLs, to receive HTTPS notifications, and to send HTTPS responses. The ESRSHTTPS includes SSL support so applications can also exchange data over secure HTTPS connections. It is also designed to work with I/O completion ports.

The ESRSHTTPS service is automatically installed and configured when you install an Gateway Client. However, you can also configure the ESRSHTTPS service from a command line as described in the following sections.

Configuring the ESRSHTTPS listener

ESRSHTTPS listener is installed as part of the Gateway installation, in the following Gateway folder:

```
./Gateway/ESRSHTTPS
```

[“ESRSHTTPS listener service command line options” on page 105](#) describes the command line options to install, remove, start, stop, and check status of the ESRS listener service.

HTTPS listener paths

The ESRS HTTPS listener service uses the following relative paths for storing files it receives from ConnectEMC or the ESRS Gateway Extract Utility (GWExt):

- ◆ For files coming from the ConnectEMC service, the relative path is `./Gateway/work/httpsroot/incoming`
- ◆ For files coming from GWExt, the relative path is `./Gateway/work/dmb/request`

Files created

The following files exist after configuring and starting the ESRSHTTPS listener:

- ◆ **esrshttps_config.xml**
- ◆ **esrshttps.log**

ESRSHTTPS listener service command line options

The following command line scripts will provide the options to install, build, start, stop, and check status of the ESRS listener service.

Installing ESRSHTTPS listener service

To install the ESRSHTTPS listener service:

1. Extract esrshttps.tar to the install folder:

```
tar -xvf esrshttps.tar
```

2. Build esrshttps binary from the install directory:

Run 'make' or 'gmake'

3. Add esrshttps listener service to Linux service:

```
cp esrs2httpslistener script to /etc/init.d
```

Note: If necessary modify the above script to reflect the correct location of esrshttps listener installation directory

4. Change the privileges of this script to be readable and executable:

```
chmod 775 esrs2httpslistener
```

5. Change the privileges of start & shutdown scripts to be readable and executable:

```
chmod 775 startup.sh shutdown.sh
```

Removing ESRSHTTPS listener service

To remove the ESRSHTTPS listener service:

1. Stop esrs2httpslistener listener service:

```
service esrs2httpslistener stop
```

2. Delete esrs2httpslistener listener service from init.d dir:

```
cd /etc/init.d
rm esrs2httpslistener
```

3. Delete the esrshttps listener install directory:

```
cd ../ESRSHTTPS (install dir)
rm -r ../ESRSHTTPS
```

Starting ESRSHTTPS listener service

To start the ESRSHTTPS listener service:

```
[root@185rhel62d ESRSHTTPS]# ./startup.sh
esrshttps service is starting
done starting esrshttps service
```

Stopping ESRSHTTPS listener service

To stop the ESRSHTTPS listener service:

```
[root@185rhel62d ESRSHTTPS]# ./shutdown.sh
esrshttps service is shutting down
done shutting down esrshttps service
```

Checking ESRSHTTPS listener service status

Linux service to check the status of ESRSHTTPS listener service:

```
[root@185rhel62d ESRSHTTPS]# service
esrs2httpslistener status
esrshttps (pid 9663 9556 8644 8064) is running...
```

Checking stop of ESRSHTTPS listener service

Linux service to check the stop of ESRSHTTPS listener service:

```
[root@185rhel62d ESRSHTTPS]# service
esrs2httpslistener stop
log location is: /var/log/esrshttps_serv/shutdown
[ OK ]
```

Checking start of ESRSHTTPS listener service

Linux service to check the start of ESRSHTTPS listener service:

```
[root@185rhel62d ESRSHTTPS]# service
esrs2httpslistener start
Starting ESRS2 HTTPS listener: ESRS2 HTTPS listener
already running: 9760
```

ESRSHTTPS configuration

The following configuration file sets the parameters for the ESRSHHTTPS listener:

```
../Gateway/ESRSHTTPS/esrshttps_config.xml

<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <sectionGroup name="applicationSettings"
type="System.Configuration.ApplicationSettingsGroup,
System, Version
=2.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089">
      <section name="esrshttp.Properties.Settings"
type="System.Configuration.ClientSettingsSection,
System, Version=2.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089"
requirePermission="false" />
    </sectionGroup>
  </configSections>
  <connectionStrings />
  <Settings>
    <IPAddress>0.0.0.0</IPAddress>
    <Port>443</Port>
    <VirtualPath>incoming</VirtualPath>
    <RootDir>/opt/emc/esrs2</RootDir>
    <LogFileMaxSize>1024000</LogFileMaxSize>
    <LogFileNumArchives>20</LogFileNumArchives>
  </Settings>
</configuration>
```

Figure 67 esrshttps_config.xml file

esrshttps_config.xml file parameters

The following describes the parameters in the esrshttps_config.xml file:

ipaddress — Takes IP parameter as a string specifying the IP address to be added to the **esrshttps_config.xml** file.

port — Takes port parameter as a string specifying the port number to be added to the **esrshttps_config.xml** file.

rootdir — Takes rootdir parameter as a string specifying the rootdir to be added to the **esrshttps_config.xml** file. A root directory is the base directory to which the ESRSHTTPS listener is allowed access. The ESRSHTTPS listener will be allowed to create files from this directory.

LogFileMaxSize — The maximum size of the log file. The default is 1024000.

LogFileNumArchives — The maximum number of log files to retain before deleting the oldest file.

A

- access control
 - device 36
 - device configuration 36
 - EMC Enterprise 36
- architecture, ESRS 16
- Atmos 23, 72
- audit2allow 63, 65
- Avamar 23, 72

B

- backup
 - Gateway Client 98
 - image 98
 - procedure 98
 - restoration 98
- Broadcast address 39
- Brocade-B 24, 72

C

- Celerra 23, 34, 72
- Centera 23, 72
- Cisco 24, 72
- CLARiiON 23, 72
- CLARiiON Management Station 34
- config_agent_proxy.sh 69, 70
- config_policy_manager.sh 66, 67, 68
- Configuration CLI Commands
 - installing 30
- Configuration Tool 30
 - device management 32
 - linking a Client to a Policy Manager 87

- proxy server communication 86
- viewing connectivity status 79
- Connect homes 17
- Connectrix 24, 34, 72
- Customer Management Station 24, 72
- customer responsibilities 25

D

- Data Domain 24, 72
- DCA 34, 72
- default Gateway 39
- Device Configuration 42
- device configuration access control 36
- device management
 - managing or viewing devices 83
 - synchronization 17
- Digital Certificate Management 34
- Disable Firewall 41
- DL3D 24, 34, 72
- DLm 24, 72
- DLm3 72
- DLm4 72
- DNS 39
- DNS Configuration 44

E

- EDL 24, 34, 72
- EMC Global Services responsibilities 25
- ESRS
 - architecture 16
 - Gateway Extract Utility 33
- esrshttps 38
- ESRSHTTPS listener service 103

- check status 106
- checking start 106
- checking status 106
- checking stop 106
- command line options 105
- configuration file 107
- installing 105
- removing 105
- starting 106
- stopping 106
- ESRSHTTPS listener service
 - troubleshooting 103
- esrshttps_config.xml 104
 - parameters 107, 108
- esrshttps.log 104
- Ethernet Port 47

F

- Firewall 39
- Firewall configuration 40

G

- Gateway Client 38
 - required software applications 38
 - server preparation 37
- Gateway client service
 - checking status 102
 - starting 102
 - troubleshooting 102
- Gateway Extract Utility (GWExt) 33
- Gateway watchdog service
 - checking status 102
 - starting 102
- gateway_status 55, 56, 57, 66, 68, 70
- Greenplum DCA 24

H

- hardware failure 103
- heartbeat polling 20
- heartbeat, defined 20
- High Availability Gateway Cluster 27
 - configuration 27
 - installing 28
 - synchronization 28
- HTTPS event notifications 103

- Hyper-V
 - requirements 27

I

- image backup 98
- Invista 24, 72
- Invista Element Manager 34
- IP address 39

M

- manage_device 71
- managed devices
 - list 75
- managing devices 83

N

- Netmask 39
- Network Configuration 42, 43

O

- operating system
 - failure 103

P

- Passwords 48
- Policy Manager
 - maintenance 95
- Postfix 38, 51, 58, 64
- power sequences 94
- provision_agent 55
- proxy server
 - communication 87

R

- RecoverPoint 24, 72
- Red Hat Enterprise Linux 6.2 (32-bit) 39
- Red Hat Setup Utility 39, 40, 41, 43, 44, 45, 46
- remote access 22
- restoration procedures 99

S

- Select A Device 43
- selinux 58

semodule 64, 65
server maintenance 93
service events, unexpected 102
setsebool 58
Suffixes 72
Switch-Brocade-B 24, 72
Switch-Cisco 24, 72
Symmetrix 24, 34, 73

T

tar -xvf 52
time zone 95
troubleshooting
 ESRSHTTPS 103
 unexpected service events 102

U

user authentication 17
Users 48

V

VMAX Cloud Edition (CE) 24, 34, 73
VMware
 requirements 27
VNX 24, 34, 73
VNXe 24, 34, 73
VPLEX 24, 34, 73
vsftpd 38, 49, 50, 58

