EMC® Secure Remote Support IP Solution

Release 2.08

Site Planning Guide

P/N 300-012-317
REV A01

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Published February, 2011

Contents

Chapter 3 Configurations

Chapter 4 Preparing for Site Installation

Appendix A Pre-Site Checklist Example

Figures

Tables

Preface

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, please contact your EMC representative.

Audience

This guide is part of the EMC Secure Remote Support IP Solution release 2.0 documentation set, and is intended for use by customers and prospective customers.

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

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

Related documentation

See the following documents for related information:

- *EMC Secure Remote Support IP Solution Technical Description*
- *EMC Secure Remote Support IP Solution Pre-Site Checklist*
- *EMC Secure Remote Support IP Solution Operations Guide*
- *EMC Secure Remote Support IP Solution Port Requirements*
- *EMC Secure Remote Support IP Solution Release Notes*

Conventions used in this guide

EMC uses the following conventions for notes, cautions, warnings, and danger notices.

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.

IMPORTANT

An important notice contains information essential to operation of the software.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, utilities • URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, notifications
Bold	Used in running (nonprocedural) text for: • Names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system call, man pages Used in procedures for: • Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) • What user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis (for example a new term) • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text

Courier bold	Used for: • Specific user input (such as commands)
Courier italic	Used in procedures for: • Variables on command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces indicate content that you must specify (that is, x or y or z)
...	Ellipses indicate nonessential information omitted from the example

Where to get help

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

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

http://Powerlink.EMC.com

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

Your comments

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

techpubcomments@EMC.com

1 Overview

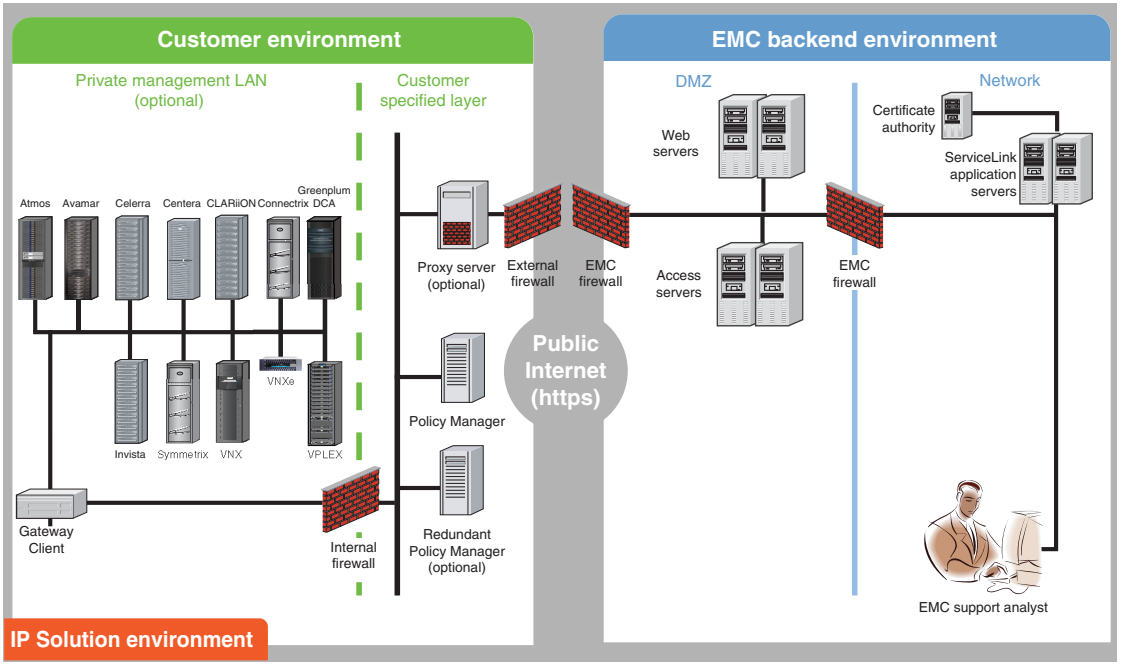
This chapter introduces the EMC Secure Remote Support IP Solution so that you can begin to make decisions about the configuration that will best fit your requirements and environment.

It also provides an overview of the process for working with EMC Global Services to prepare your site for your ESRS IP implementation. Topics include:

About the ESRS IP Solution

The EMC® Secure Remote Support IP Solution (ESRS IP) is an IP-based automated connect home and remote support solution enhanced by a comprehensive security system. ESRS IP creates both a unified architecture and a common point of access for remote support activities performed on your EMC products. For an illustration of the ESRS IP communication paths, see Figure 1 on page 16.

Note: *EMC Secure Remote Support IP Solution Technical Description* (available on the EMC Powerlink® website) provides details on how your site ESRS IP architecture performs and communicates with the EMC enterprise.



GEN-001688

Figure 1 ESRS IP Solution

What is new

The EMC Secure Remote Support IP Solution builds upon previous releases by providing many new features for remote notification and support.

Terminology

The ESRS IP Solution is a new version of the product known as ESRS Gateway. The ESRS IP Solution component that was formerly called Gateway is now called Gateway Client.

Redundant Policy Manager option

The ESRS IP Solution provides the option to install a redundant Policy Manager. If the primary Policy Manager becomes unavailable, the redundant Policy Manager is used to resume operations. Both Policy Managers enforce the same policies. Manual failover is required.

Application installation

A Provisioning Tool is provided on a CD. The tool is used to initiate the installation process and download the most recent versions of the ESRS IP Client application from EMC.

Deployment and configuration

The ESRS IP Solution provides a Configuration Tool that is used after software installation for various activities including:

- Viewing connectivity status between the ESRS IP Client and EMC
- Viewing connectivity status between the ESRS IP Client and Policy Manager
- Viewing connectivity status between the ESRS IP Client and Managed Devices
- Initiating device deployment requests
- Initiating device removal requests
- Processing managed device update requests
- Configuring or changing the ESRS IP Client for Proxy server
- Processing managed device update requests
- Configuring or changing the ESRS IP Client for Proxy server
- Setting up communication between the Policy Manager and the ESRS IP Client
- Configuring or changing the ESRS IP Client for Proxy server for the Policy Manager (if needed)
- Viewing status of Listener Services

Security enhancements

The ESRS IP Solution provides the enhanced security practices and encryption technologies, including:

- Certificate libraries based on RSA Lockbox Technology
- Advanced Encryption Standard (AES) 256-bit encryption between the Gateway Client and EMC
- Configurable security between ESRS IP Solution components

ESRS IP components

ESRS IP adds the following components at your site:

- **Gateway Client(s)** — This ESRS IP software component is installed on a customer-supplied dedicated server or 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 callhome notifications.**
- **Policy Manager** — This ESRS IP software component is installed on a customer-supplied server or servers. It is configured to control remote access to your devices and maintain an audit log of remote connections.

Requirements for ESRS IP customers

ESRS IP Solution customers must provide the following:

- An IP network with Internet connectivity
- The capability to add Gateway Client servers and Policy Manager servers to your network
- Network connectivity between the servers and EMC devices to be managed by ESRS IP
- Internet connectivity to EMC's ESRS infrastructure by using outbound port 443 and 8443
- Network connectivity between ESRS IP Client and Policy Manager

For additional requirements, see "Responsibilities for the ESRS IP components" on page 21.

Supported devices

Table 1 on page 19 lists the EMC storage device models and environments supported by ESRS IP.

If you need to upgrade one or more of your EMC devices so that they are compatible with ESRS IP, you must contact EMC Global Services and schedule the device upgrades to occur *before* you have those devices added to your ESRS IP managed device list.

Once the devices have been upgraded, you can have them added to the managed device list during or after the ESRS IP installation. Upgrades to EMC products may be billed separately from the ESRS IP installation.

Note: Upgrades to service processors or device code are *not* included as part of the ESRS IP implementation.

Table 1 Product and application releases supported by ESRS IP Clients

Product	Environment/application releases
EMC Atmos®	Atmos 1.4 or later
EMC Avamar®	Avamar 6.0 or later
Fabric Manager managing Brocade B-series switches	Brocade B-series switches running Fabric OS 5.0.1b through 6.1.0x only, with Fabric Manager 5.2.0b or later [a d e g]
EMC Celerra®	NAS Code 5.4 or later
EMC Centera®	CentraStar® 2.4 or later [a]
Cisco switches	MDS 9000 Family switches that are running SAN-OS 3.3(2) or later and NX-OS 4.1(1b) or later. [a] Nexus 5000 Family switches that are running NX-OS 4.1(3)N1(1) or later. [b h]
EMC CLARiiON® CX, CX3, CX4, and AX4-5 Series storage systems *(distributed or Enterprise environments)*	FLARE® Operating Environment 2.19 or later Navisphere® Manager 6.19 or later **Note**: The AX-100/AX-150 are not supported as they do not support the required CLARalert. The AX4-5 series are supported only if the Navisphere Full license (with CLARalert) is purchased and installed on the storage system.
EMC Connectrix® Manager (CM) managing Connectrix M-series switches	Connectrix Manager 7.x with DialEMC 2.2.10, or Connectrix Manager 8.x or later with ConnectEMC 1.x
Connectrix Manager (CM) managing Connectrix M-series and B-series switches	Connectrix Manager 9.6.2 or later with ConnectEMC 1.x [e]
Connectrix Manager Data Center Edition (CMDCE) managing Connectrix M-series and B-series switches	Connectrix Manager Data Center Edition 10.1.1 or later with ConnectEMC 4.0.2 [f]
EMC Disk Library for mainframe (DLm)	DLm4020, DLm4080, release 1.2 and later

Table 1 Product and application releases supported by ESRS IP Clients

Product	Environment/application releases
EMC Disk Library (EDL)	DL-5100 and 5200 series DL-4000 series — DL-4100, DL-4106, DL-4200, DL-4206, DL-4400A/B, DL-4406A/B DL-700 series — DL-710, DL-720, DL-740 DL-310 DL3D 1500, 3000, 4000 — release 1.01 and later
EMC Greenplum® Data Computing Appliance (DCA)	Greenplum 4.0
EMC Invista®	Invista 2.2 or later
EMC RecoverPoint	RPA 3.1 and later [a]
EMC Symmetrix® 8000 Series	Enginuity™ 5567 and 5568 with Service Processor Part Number [c] 090-000-064, 090-000-074, or 090-000-09*x*
Symmetrix DMX™ Series	Enginuity 5670, 5671
Symmetrix DMX-3 Series	Enginuity 5771, 5772, 5773
Symmetrix DMX-4 Series	Enginuity 5772, 5773
Symmetrix VMax™ Series	Enginuity 5874, 5875
EMC VNX®	VNX Operating Environment (OE) for Block 05.31.000.5.006 or greater VNX Operating Environment (OE) for File 7.0.12.0 or greater
EMC VNXe®	VNXe 2.0.x
EMC VPLEX™	GeoSynchrony 4.0.0.00.00.11 or later

a. For remote support access only, not for connect home through ESRS IP.
b. For remote support access only. Connect home is not supported at this time.
c. These part numbers designate Service Processor that is running Windows NT SP6.
d. Fabric Manager does not support FOS 6.1.1 or higher. CM or CMDCE is required. Please refer to the appropriate FOS Release Notes.
e. CM does not support FOS 6.3.x or higher. cmdce is required. Please refer to the appropriate FOS Release Notes.
f. CMDCE is required to support FOS 6.3.x or higher. Please refer to the appropriate fos Release Notes
g. Callhome via CM, CMDCE, or ECC, otherwise no callhome through ESRS IP Client.
h. Callhome via Cisco Fabric Manager or ECC, otherwise no callhome through ESRS IP Client.

Responsibilities for the ESRS IP components

This section defines who is responsible for various ESRS IP tasks including installation, configuration, operation, and maintenance.

Customer

The EMC customer is responsible for the following tasks:

- Maintaining internet connectivity
- Preparing and configuring the network, proxy server, and firewall
- Preparing the servers for installation. This includes:
  - Preparing the Gateway Client server hardware and operating system
  - Preparing the Policy Manager server hardware and operating system
  - Placing the Gateway Client and Policy Manager servers on the IP network
  - Maintaining Network Connectivity between Gateway Client and EMC
  - Maintaining Network Connectivity between Gateway Client and Managed Devices
  - Maintaining Network Connectivity between Gateway Client and Policy Manager
  - Maintain OS patches / updates for Gateway and Policy Manager servers
  - Installing and maintaining antivirus and other applicable security software on the servers
  - Configuring, administering, and updating policy management activities, policies, and accounts on the Policy Manager
  - Backing up and restoring file systems
  - Providing continuing maintenance, including security and operating system updates and upgrades on the Gateway Client and Policy Manager servers
  - Providing physical security of all hardware
  - Protecting all files on the servers, including the SSL certificate, if applicable

EMC Global Services

EMC Global Services personnel are responsible for the following tasks:

- Installing the ESRS IP Gateway Client software and Policy Manager software
- Configuring and deploying EMC product managed devices
- Updating the ESRS IP Client and Policy Manager software

Site planning process

The EMC Secure Remote Support IP Solution requires customer-provided and EMC-provided components and actions. Your network, storage system, and security administration personnel must work closely with your EMC Global Services representatives to prepare your site for ESRS IP software installation.

This guide provides detailed instructions for completing each step in the customer site planning process. You should plan your solution deployment on a schedule that you have coordinated with your EMC Global Services professional.

Coordination with EMC

This is a recommended schedule of preparation coordination meetings and activities with EMC and your internal network, storage, and security teams:

- Your teams should meet with EMC Sales and EMC Global Services to receive an ESRS IP review and get answers to your initial questions.
- You should host an onsite meeting for EMC Global Services and your teams to finalize and record your ESRS IP system configuration.
- Your teams should meet with EMC Global Services to finalize the solution deployment schedule and details.

For additional details about these meetings, see Chapter 4, "Preparing for Site Installation."

2

Component Requirements

This chapter describes the requirements for the ESRS IP Clients, server hardware, and software that you must supply as part of the total configuration. Topics include:

Basics

To properly support the ESRS IP configuration you choose, EMC recommends that you become familiar with the requirements of each software and hardware component. This chapter provides the requirements of each component.

IMPORTANT

Be sure to read Chapter 3, "Configurations," to define your configuration type and determine if you will need additional servers.

Server types

Depending on your chosen configuration, you must supply:

- At least one Gateway Client server (two or more servers are required for a High Availability configuration). Servers can be dedicated or virtual.
- A Policy Manager server, which can be dedicated, virtual, or co-located with a Gateway Client server.

Note: Detail on virtual servers are provided in "VMware support for servers" on page 29.

For detailed server requirements, refer to the tables in "Server requirements" on page 25.

To verify that your servers meet the hardware and software requirements of the ESRS IP Solution, you must obtain a copy of the Customer Environment Check Tool (CECT) from your EMC Global Services professional or download from Powerlink. Install and run the tool on each server before installation of the Gateway Client and Policy Manager software on the servers. The *EMC Secure Remote Support IP Solutions Operations Guide* provides instructions on how to use the CECT.

Server requirements

Servers must meet the hardware and operating system requirements listed in Table 2 on page 25 through Table 5 on page 28.

Table 2 Gateway Client server requirements

Hardware	Software	Notes
Processor — One or more processors, minimum 2.2 GHz, must support SSE2 instruction set (required for FIPS compliance) **Free Memory** — Minimum 1 GB of RAM, preferred 2 GB of RAM **Comm** — Minimum single 10/100 Ethernet adapter (may require dual 10/100 Ethernet depending on customer network configuration and environment), preferred Gigabit Ethernet adapters, optional additional NIC for data backups **Free Disk Space** — Minimum 1GB available for installation (preferably on a storage device of 40 GB or larger for operation) **VMware server**[a] **Note:** Contact EMC Global Services if your configuration does not meet the minimum hardware requirements.	**Operating system** — One of the following (US English only supported): • Windows Server 2003 R1 or R2, 5.2, 32-bit, SP 1 or 2 • Windows Server 2003 R2, 5.2, 64-bit, SP 1 or 2 • Windows Server 2008, R1, 6.0, 32-bit or 64-bit, IIS 7.0, SP1 or SP2 • Windows Server 2008, R2, 6.1, 64-bit, IIS 7.0, SP1 **Microsoft .NET Framework** Version 2.0 with SP1 or greater. NOTE: .NET Framework 3.5 and 4.0 are not compatible at this time. **Microsoft Visual C++ 2005 SP1 Runtime Library installed** **Microsoft Internet Information Services (IIS) installed on system drive** **IIS FTP and SMTP services enabled and configured** as specified in Table 3 on page 26 **EMC OnAlert™ and ESRSConfig user accounts created and configured** as specified in Table 3 on page 26 **Remote Desktop installed**[b]	Topology, see Chapter 3, "Configurations": • Two servers are required for a High Availability configuration. • The ESRS IP software must reside on a dedicated server. You may harden the Windows OS to meet network security requirements, as long as the hardened servers: • Meet ESRS IP OS requirements (at left). • Meet network configuration requirements. See "Network requirements" on page 30. • Do not inhibit normal ESRS IP installation or operation.

a. For more information, see "VMware support for servers" on page 29.
b. If EMC needs to remotely access a desktop to verify ESRS IP configuration or to troubleshoot, EMC will contact you for a WebEx session and ask you to establish a Remote Desktop session to the Gateway or Policy Manager.

Note: If co-locating the Gateway Client and Policy Manager on the same server, the minimum RAM should be 3 GB with a minimum of 3 GB disk space.

Table 3 Gateway Client server standard configuration requirements

Category		Variable	Value
Internet Information Services (IIS)		Startup type	Manual
		State	Started
Note: The following settings describe the FTP services and directory structure required for Gateway Client server installation. Once the server has been installed, the FTP or SMTP *services* may be disabled (one or the other, but not both). However, the FTP directory *structure* must remain in place.			
Default FTP Site > Properties			
	FTP Site	Description	**ESRS Gateway FTP Site**
		IP address	Local IP <Internal>
		TCP port	21
	Security Accounts	Allow anonymous connections	**No (unchecked)**
	Home Directory	Local path	<install_drive>:\EMC\ESRS\Gateway\work\ftproot
		Read	Yes (checked)
		Write	Yes (checked)
		Log visits	Yes (checked)
		User Isolation	Yes
Default SMTP Virtual Server > Properties			
		Description	**ESRS Gateway SMTP Site**
		Domain	**emc.com**
		Drop directory	<install_drive>:\EMC\ESRS\Gateway\work\mailroot\Drop
		Email message	maximum size of 15 MB
Local Users and Groups > New User			
		Default User Group	Yes
	New User (1)	Username	**OnAlert**
		Password	**EMCCONNECT** *(case-sensitive)*
		User must change password at next logon	No (unchecked)
		Password never expires	Yes (checked)
	New User (2)	Username	**ESRSConfig**
		Password	**esrsconfig** *(case-sensitive)*
		User must change password at next logon	No (unchecked)
		Password never expires	Yes (checked)
New directory			<install_drive>:\EMC\ESRS\Gateway\work\mailroot\Badmail
Note: <install_drive>:\EMC\ESRS\Gateway\work\ftproot; <install_drive>:\EMC\ESRS\Gateway\work\mailroot\Drop; and <install_drive>:\EMC\ESRS\Gateway\work\mailroot\BadMail are configured in IIS **after** Gateway software is installed			

Table 4 Policy Manager server requirements

Hardware	Software	Notes
Processor — One or more processors, each 2.1 GHz or better **Free memory** — Minimum 2 GB RAM, preferred 3 GB RAM **Comm** — Minimum single 10/100 Ethernet adapter (may require dual 10/100 Ethernet adapters depending on customer network configuration and environment), preferred one Gigabit Ethernet adapter, optional additional NIC for data backups **Free Disk Space** — Minimum 2 GB available (preferably on a storage device of 80 GB or larger) **VMware server**	**Operating system** — One of the following: (US English only supported) • Windows XP, SP2 or later • Windows Server 2003 • Windows Vista • Windows Server 2008, 6.0, 32-bit or 64-bit (R1 only), SP1 or 2, NOTE: Windows Server 2008 R2 is not supported **Microsoft .NET Framework** Version 2.0 with SP1 or greater is required if you are using the Customer Environment Check Tool (CECT) to validate that the PM server is setup correctly to install the PM software. NOTE: .NET Framework 3.5 and 4.0 are not compatible at this time. **Microsoft Windows Task Scheduler running and unrestricted** **Remote Desktop installed** [b]	Topology, see Chapter 3, "Configurations": • Policy Manager use is optional, but strongly recommended. • In an HA configuration, two dedicated servers required for ESRS IP software and one server for Policy Manager You may harden Windows OS to meet network security requirements, as long as the hardened servers: • Meet ESRS IP OS requirements (at left). • Meet Network configuration requirements. See "Network requirements" on page 30. Do not inhibit normal ESRS IP installation or operation. Policy Manager software may reside on a shared server. However, there are some restrictions; contact your EMC Global Services representative with questions. Following are two examples: • Policy Manager cannot be on same server as EMC ControlCenter. • There may be conflicts if the Policy Manager resides on a server with an application that uses the Tomcat web server, or with any applications that use port 8090 or 8443.
Notes: Disk space will be consumed due to audit logging. Ensure that adequate disk space is maintained. Contact EMC Global Services if your configuration does not meet the minimum hardware requirements. Failure to maintain sufficient disk space may result in the Policy Manager becoming unavailable and/or in the corruption of the Policy Manager database, which could impact remote support and callhome notifications.		

Table 5 Co-located Gateway Client and Policy Manager server (for test only)

Hardware	Software	Notes
Processor — One or more processors, minimum 2.2 GHz, must support SSE2 instruction set (required for FIPS compliance) **Free memory** — 3 GB RAM **Comm** — Minimum single 10/100 Ethernet adapter (may require dual 10/100 Ethernet adapters depending on customer network configuration and environment), preferred dual Gigabit Ethernet adapters, optional additional NIC for data backups **Free disk space** — Minimum 3 GB available (preferably on a storage device of 80 GB or larger) **VMware server**	**Operating system** — One of the following: (US English only supported) • Windows Server 2003 R2, 5.2, 32 bit • Windows Server 2003, 5.2, 32 bit • Windows Server 2003, 5.2, 64 bit • Windows Server 2008, 6.0, 32-bit or 64-bit, IIS 7.0, (R1 only) SP1 or 2, NOTE: Windows Server 2008 R2 is not supported **Microsoft .NET Framework** Version 2.0 with SP1 or greater. NOTE: .NET Framework 3.5 and 4.0 are not compatible at this time. **Microsoft Visual C++ 2005 SP1 Runtime Library** **Microsoft Internet Information Services (IIS) installed on system drive** **IIS FTP and SMTP services enabled and configured** as specified in Table 3 on page 26 **EMC OnAlert and ESRSConfig user accounts created and configured** as specified in Table 3 on page 26 **Windows Task Scheduler running and unrestricted** **Remote Desktop installed** [b]	Topology, see Chapter 3, "Configurations": • Server dedication to only the ESRS IP software plus the Policy Manager software is required. You may harden Windows OS to meet network security requirements, as long as the hardened servers: • Meet ESRS IP OS requirements (at left). • Meet Network configuration requirements. See "Network requirements" on page 30. • Do not inhibit normal ESRS IP installation or operation. Policy Manager software may reside on a shared server. However, there are some restrictions—contact your EMC Global Services representative with questions. Following are two examples: • Policy Manager cannot be on the same server as EMC ControlCenter. • There may be conflicts if the Policy Manager resides on a server with an application that uses the TomCat web server, or with any applications that use port 8090 or 8443.
Notes: Disk space will be consumed due to audit logging. Ensure that adequate disk space is maintained. Contact EMC Global Services if your configuration does not meet the minimum hardware requirements. Failure to maintain sufficient disk space may result in the Policy Manager becoming unavailable and/or in the corruption of the Policy Manager database, which could impact remote support and callhome notifications.		

VMware support for servers

The EMC Secure Remote Support IP Solution is qualified to run on a VMware virtual machine. VMware support enables you to use your existing VMware infrastructure to benefit from the security features of the Gateway Client without adding hardware. VMware VMotion functionality also allows the Policy Manager, when installed in a virtual machine, to be moved from one physical server to another with no impact to remote support.

IMPORTANT

When running clustered HA Gateway Clients on VMware, each Gateway Client must be located on different physical hardware.

Do not place VMware images or storage files on EMC devices managed by the Gateway Client.

Installation of the VM instance and operating system are the customer's responsibility.

VMware 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)

Optional components:

- SMB modules
- VMotion functionality

VMware 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.

Network requirements

Before the EMC Secure Remote Support IP Solution goes online, you must ensure your network meets the following requirements:

- Port Address Translation (PAT) cannot be used for the IP addresses of any EMC devices managed by the ESRS IP Solution.
- Dynamic IP addresses (DHCP) should not be used for any components of the ESRS IP Solution Gateway Client servers, Policy Manager servers, or managed devices.

  Note: If you use DHCP to assign IP addresses to any IP Solution components (Gateway Client servers, Policy Manager, or managed devices), they must have "permanent reservation" IP addresses. Leases for the IP addresses that EMC devices use cannot be set to expire. EMC recommends that you assign static IP addresses to those devices you plan to have managed by the ESRS IP Solution.

- Routes must exist from each of your managed devices to each of your ESRS IP Clients.
- The Policy Manager must be reachable by all ESRS IP Clients.

Enabling communication to EMC

All communication between the EMC devices at your site and EMC Global Services is initiated by, and occurs through, a ESRS IP Client at your site over the outbound default port 443 and/or 8443. Your firewall administrators must open port 443 and 8443 *outbound* to enable communication between EMC and the ESRS IP Clients.

IMPORTANT

To maintain communication integrity, proxy servers and devices external to your DMZ must not perform any method of SSL checking on outbound IP traffic.

Enabling proxy server for ESRS IP Client traffic to EMC

The ESRS IP Solution supports the use of a proxy server for routing outbound Internet traffic from the ESRS IP Clients to EMC.

If you use a proxy server for outbound Internet traffic, you must make sure the proxy server:

- Can communicate with the ESRS IP Clients over an agreed-upon port.
- Can communicate with EMC, outbound, over SSL port 443 and 8443.

IMPORTANT

To maintain communication integrity, proxy servers and devices external to your DMZ must not perform any method of SSL checking on outbound IP traffic.

The following proxy servers have been tested for use with the ESRS IP Solution. Note that configuration and operation are your responsibility.

- Linux Squid (supported in Red Hat 6.1 and 6.2)
- Apache HTTP Server release 1.1 and later (contains mod_proxy module)
- Microsoft ISA
- Netscape iPlanet Proxy Server release 3.6
- DeleGate 7_9_3

The ESRS IP Solution supports the following protocols for use with a proxy server:

- HTTP Proxy releases 1.0 and 1.1 (Username/Password is optional. If a username is provided s password is required)
- SOCKS releases 4 and 5 (requires username and password authentication)

Communication between Policy Manager and ESRS IP Clients

The Policy Manager application *only* responds to communication requests from the ESRS IP Clients.

At startup, the ESRS IP Client queries the Policy Manager and caches the permission rules. It must then periodically poll the Policy Manager for configuration updates and audit logging.

The Policy Manager is an HTTP listener. You must configure the Policy Manager and ESRS IP Client to use an agreed-upon port and protocol. EMC recommends that you use the port 8090 for standard HTTP, or port 8443 for SSL-enabled HTTPS. If necessary, you can specify a different port during the Policy Manager and ESRS IP Client installations.

Note: If you are running Policy Manager in a Windows Server 2008 environment, you must configure the Windows firewall to permit traffic to the Policy Manager on both ports 8090 (default) and 8443. The firewall is closed by default and must be specifically configured to permit the Policy Manager traffic.

Communication between the ESRS IP Clients and devices

There are two connection requirements between the ESRS IP Client and your managed devices:

- The first is the communication between the ESRS IP Client and your managed devices for **remote access** connections. The ESRS IP Client secures remote access connections to your EMC devices by using a session-based IP port-mapped solution.
- The second communication requirement is between your managed devices and the ESRS IP Client for connect home messages. For those devices that use the ESRS IP Client to forward connect home transfers, the transfer is sent through a secure encrypted data tunnel to EMC, with an audit of the transfer is kept on the Policy Manager.

Gateway Client

To enable communication between your Gateway Client and your devices, you must configure your internal firewalls to allow traffic over the specific ports shown in Table 6 on page 34 and Table 7 on page 35. These tables identify the installation site network firewall configuration open-port requirements for the EMC Secure Remote Support IP Solution. The protocol/port number and direction are identified relative to EMC Gateway Client servers and storage devices. Figure 2 on page 33 provides a representation of the connections between devices, the Gateway Client, and EMC.

Note: Some ports used by the Gateway Client servers and devices may be registered for use by other parties, or may not be registered by EMC. EMC is addressing these registration issues. In the meantime, be aware that all ports listed for use by Gateway Client servers and devices will be in use by the EMC applications listed.

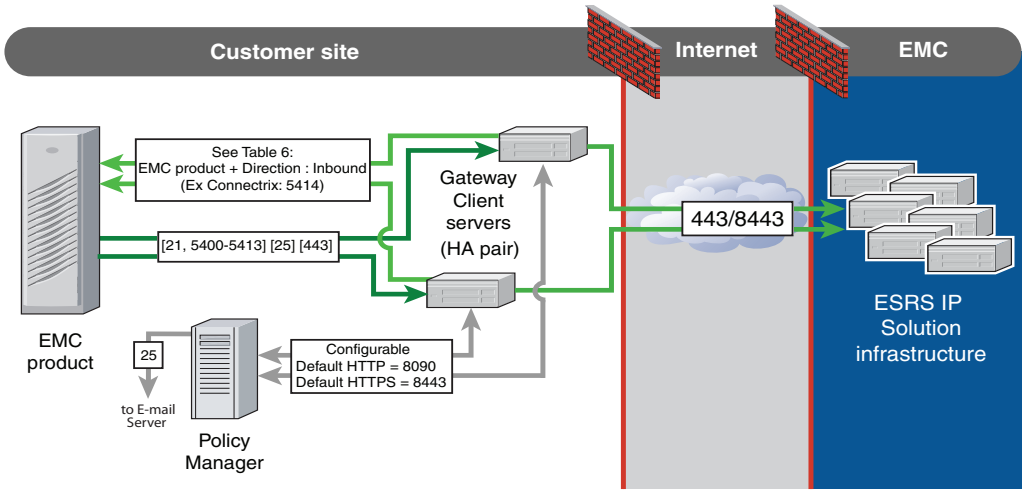


Figure 2 **Port diagram Gateway Client**

Port Requirements

Table 6 on page 34 lists the port requirements for the Gateway Client and Policy Manager servers. Table 7 on page 35 lists the port requirements for devices.

Table 6 Port requirements for Gateway Client and Policy Manager servers

EMC product	TCP port *or* Protocol	Notes for port settings	Direction open	Source *-or-* Destination	Application name	Communication (network traffic) type	*Performed by authorized EMC Global Services personnel: Support objective (frequency)*
Gateway Client	HTTPS 443		Outbound	to EMC	Client service	Service notification, setup, all traffic except remote support	N/A
	HTTPS **443** and **8443**		Outbound	to EMC Global Access Servers (GAS)	Client service	Remote support	N/A
	HTTPS **443**	Use of HTTPS for service notifications inbound is dependent on the version of ConnectEMC used by the managed device. Refer to product documentation.	Inbound	from **Managed device** (EMC product)	ESRSHTTP	Service notification from device	N/A
	Passive FTP ports: **21**, 5400–5413	During the ESRS-IP installer execution, the value for Passive Port Range in IIS FTP is set to **21** and **5400** through **5413**. This range indicates the data channel ports available for response to PASV commands. See RFC 959 for passive FTP definition. These ports are used for passive mode FTP of call home messages as well as for the GWExt loading and output. GWExt uses HTTPS by default but can be configured to use HTTP.			Microsoft IIS FTP		
	SMTP **25**				Microsoft IIS SMTP		
	IMPORTANT: When opening ports for devices in Table 7, also open the same ports on the **Gateway Client server**, identified as "Inbound from Gateway Client server"		Outbound	to **Managed device**	Client service	Remote support for device	N/A
	HTTP (configurable) Default = **8090**		Outbound	to Policy Manager	Client service	Policy query	N/A
	HTTPS 8443						
Policy Manager	HTTP (configurable) Default = **8090**		Inbound	from Client (and customer browser)	Policy Manager service	Policy query (and policy management by customer)	N/A
	HTTPS 8443						
	SMTP 25		Outbound	to email server		Action request	

Table 7 Port requirements for devices managed by Gateway Client (page 1 of 4)

EMC product	TCP port *or* Protocol	Notes for port settings	Direction open	Source *-or-* Destination	Application name	Communication (network traffic) type	*Performed by authorized EMC Global Services personnel: Support objective (frequency)*
Atmos®	HTTPS[a]		Outbound	to Customer SMTP server	ConnectEMC	Service notification	NA
	Passive FTP						
	SMTP						
	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Administration (occasional)
	443				SecureWebUI		Troubleshooting (frequent)
Avamar®	HTTPS[a]		Outbound	to Customer SMTP server	ConnectEMC	Service notification	NA
	Passive FTP						
	SMTP						
	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Administration (occasional)
	443				AVInstaller		Troubleshooting (frequent)
	80,443				Enterprise Manager		
Celerra®	HTTPS[a]		Outbound	to Gateway Client	ConnectEMC	Service notification	**Note:** NAS code 5.5.30.x and earlier supports only FTP; NAS code 5.5.31.x supports both FTP and SMTP for callhome by using the Gateway Client.
	Passive FTP						
	SMTP						
	All of: **80**, **443**, and **8000**		Inbound	from Gateway Client	Celerra Manager (Web UI)	Remote support	Administration (occasional)
	22				CLI (via SSH)		Troubleshooting (frequent)
	23	This telnet port should be enabled ***only*** if SSH (port **22**) cannot be used.			Telnet		Troubleshooting (rare) Use *only* if CLI cannot be used
EMC Centera®	SMTP		Outbound	to Customer SMTP server	ConnectEMC	Service notification	N/A
	Both **3218** and **3682**			from Gateway Client	EMC Centera Viewer	Remote support	Diagnostics (frequent)
	22				CLI (via SSH)		Troubleshooting (frequent)

Table 7 Port requirements for devices managed by Gateway Client (page 2 of 4)

EMC product	TCP port *or* Protocol	Notes for port settings	Direction open	Source *-or-* Destination	Application name	Communi-cation (network traffic) type	*Performed by authorized EMC Global Services personnel: Support objective (frequency)*
CLARiiON® and CLARiiON portion of EDL	HTTPS[a]	Service notification for CLARiiON and EDL is supported only on centrally managed devices via a management server. Distributed CLARiiON devices (including EDL) use Gateway Client or Customer email server (SMTP) for service notifications.	Outbound	to Gateway Client	ConnectEMC	Service notification	N/A
	Passive FTP[b]						
	SMTP[c]				ConnectEMC, Navisphere® SP Agent		
	13456 22 (to run pling)		Inbound	from Gateway Client	KTCONS	Remote support	Troubleshooting (occasional)
	Both **80** and **443**, or optionally (depending on configuration), both **2162** and **2163**	For more information, refer to CLARiiON documentation.			Navisphere Manager; also allows Navisphere SecureCLI		Administration (frequent) Troubleshooting (frequent)
	9519				RemotelyAnywhere		
	5414				EMCRemote		
	All of: **6389**, **6390**, **6391**, and **6392**				Navisphere CLI		
	60020				Remote Diagnostic Agent		Diagnostics (occasional)
Navisphere Manage-ment Station	HTTPS[a]		Outbound	to Gateway Client	ConnectEMC	Service notification	N/A
	Passive FTP[b]						
	SMTP[c]				ConnectEMC, Navisphere SP Agent		
Connectrix® *switch family*	HTTPS[a]		Outbound	to Gateway Client	ConnectEMC or DialEMC	Service notification	N/A
	Passive FTP[b]						
	SMTP[c]						
	5414		Inbound	from Gateway Client	EMCRemote	Remote support	Troubleshooting (frequent)
DL3D Engine	SMTP[c]		Outbound	to Customer SMTP server	CentOS	Service notification	N/A
	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Troubleshooting (frequent)
	443		Inbound		Secure Web UI		
DLm	HTTPS[a]		Outbound	to Gateway Client	ConnectEMC	Service notification	N/A
	Passive FTP[b]						
	SMTP[c]						
	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Troubleshooting (frequent)
	80, 443, 8000				Celerra Manager		

Table 7 Port requirements for devices managed by Gateway Client (page 3 of 4)

EMC product	TCP port *or* Protocol	Notes for port settings	Direction open	Source *-or-* Destination	Application name	Communi-cation (network traffic) type	*Performed by authorized EMC Global Services personnel: Support objective (frequency)*
EDL Engine (except DL3D)	HTTPS[a]	Service notification for EDL is supported only on centrally managed devices via a management server. Distributed CLARiiON devices (including EDL) use Gateway Client or Customer email server (SMTP) for service notifications.	Outbound	to Gateway Client	ConnectEMC	Service notification	N/A
	Passive FTP[b]						
	SMTP[c]						
	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Troubleshooting (frequent)
	11576				EDL Mgt Console		
Greenplum Data Computing Appliance (DCA)®	HTTPS[a]		Outbound	to Customer SMTP server	ConnectEMC	Service notification	NA
	Passive FTP						
	SMTP						
	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Administration (occasional)
							Troubleshooting (frequent)
Invista® Element Manager	HTTPS[a]		Outbound	to Gateway Client	ConnectEMC	Service notification	N/A
	Passive FTP[b]						
	SMTP[c]						
Invista CPCs	5414		Inbound	from Gateway Client	EMCRemote	Remote support	Troubleshooting (frequent)
	All of: 80, 443, 2162, and 2163				Invista Element Manager and InvistaSecCLI		
	5201				ClassicCLI		
Recover-Point	SMTP[c]		Outbound	to Customer SMTP server		Service notification	N/A
	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Troubleshooting (frequent)
Switch–Brocade-B	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Troubleshooting (frequent)
	23	This telnet port should be enabled *only* if SSH (port 22) cannot be used.			Telnet		Troubleshooting (rare) Use *only* if CLI cannot be used
Switch–Cisco	SMTP[c]		Outbound	to Customer SMTP server			N/A
	22	SSH must be enabled and configured.	Inbound	from Gateway Client	CLI (via SSH)	Remote support	Troubleshooting (frequent)
	23	This telnet port should be enabled *only* if SSH (port 22) cannot be used.			Telnet		Troubleshooting (rare) Use *only* if CLI cannot be used
Symmetrix®	HTTPS[a]		Outbound	to Gateway Client	ConnectEMC or DialEMC	Service notification	N/A
	Passive FTP[b]						
	SMTP[c]						
	9519		Inbound	from Gateway Client	RemotelyAnywhere	Remote support	Troubleshooting (frequent)
	5414				EMCRemote		
	All of: **1300**, **1400**, **4444**, **5555**, **7000**, **23003**, **23004**, and **23005**				SGBD/Swuch/ Chat Server/ Remote Browser/ InlineCS		Advanced troubleshooting (by EMC Symmetrix Engineering) (rare)

Table 7 Port requirements for devices managed by Gateway Client (page 4 of 4)

EMC product	TCP port *or* Protocol	Notes for port settings	Direction open	Source *-or-* Destination	Application name	Communi-cation (network traffic) type	*Performed by authorized EMC Global Services personnel: Support objective (frequency)*
VNX®	HTTPS[a]		Outbound	to Gateway Client	ConnectEMC	Service notification	N/A
	Passive FTP[b]						
	SMTP[c]						
	13456		Inbound	from Gateway Client	KTCONS	Remote support	Troubleshooting (occasional)
	22, 9519				RemoteKTrace		Administration (frequent)
							Troubleshooting (frequent)
	9519				Remotely-Anywhere		
	22				CLI (via SSH)		
	80, 443, 2162, 2163, 8000				Unisphere/USM/ Navisphere SecureCLI		
	6391,6392, 60020				Remote Diagnostic Agent		Diagnostics (occasional)
VNXe®	HTTPS[a]		Outbound	to Customer SMTP server	ConnectEMC	Service notification	NA
	Passive FTP						
	SMTP						
	22		Inbound	from Gateway Client	CLI (via SSH)	Remote support	Administration (occasional)
	80 and 443				Unisphere		Troubleshooting (frequent)
VPLEX	SMTP		Outbound	to Gateway Client	ConnectEMC	Service notification	N/A
					CLI (via SSH)		
	443		Inbound	from Gateway Client	Invista Element Manager	Remote support	Troubleshooting (frequent)
	22				CLI (via SSH)		Advanced troubleshooting (by EMC Symmetrix Engineering) (rare)

a. Use of HTTPS for service notifications is dependent on the version of ConnectEMC used by the managed device. Refer to product documentation. The default port for HTTPS is 443.

b. During the ESRS-IP installer execution, the value for Passive Port Range in IIS FTP is set to 21 and 5400 through 5413. This range indicates the data channel ports available for response to PASV commands. See RFC 959 for passive FTP definition. These ports are used for passive mode FTP of call home messages as well as for the GWExt loading and output.

c. The protocol SMTP is assigned the service port 25, used for Outbound Service Notification to Gateway Client or email server.

3

Configurations

This chapter describes the ESRS IP configurations supported by EMC and provides recommendations for choosing a configuration and topology for your site. Topics include:

Introduction

EMC recommends specific EMC Secure Remote Support IP Solution component configurations. EMC supports, but does not recommend, certain other configurations. Both types of configurations are discussed in this chapter.

Note: In addition to the specifications described in the following sections, there are limits on the quantity of devices that can be safely managed on each server. There is a limit of 250 devices per Gateway Client server (each CLARiiON counts as two devices) and 750 devices per Policy Manager. Table 8 on page 42 provides detailed examples of device and server limits.

There are two main software components of ESRS IP that reside at a your site: the ***ESRS IP Client*** and the ***Policy Manager***.

ESRS IP Client

The ESRS IP Client is the application installed on a dedicated customer-provided server or VMware instance (or multiple servers/ESX servers for a High Availability Gateway Cluster configuration)

Policy Manager

The Policy Manager application may reside on its own server/VM instance, or may be co-located on an existing server (with dependencies). The Policy Manager may also be configured on multiple servers for redundancy.

Device limits

The Gateway Client and Policy Manager components of ESRS IP have the following device limits to help ensure reliable performance.

Gateway Client: The recommended device limit for each Gateway Client or Clustered High Availability Gateway Client is 250 devices. The device limit was developed by using remote session performance data and historical statistics about the number of remote sessions and devices in the field. By limiting the number of devices that can be deployed on a Gateway Client, remote servicing of equipment can be continued during periods when there might be numerous remote connections due to several concurrent problems.

Note: There is currently no software block that will stop the deployment of more than 250 devices. However, exceeding this recommended limit may cause an unacceptable level of throughput for remote connections during periods of peak usage. This can result in poor remote application performance, the inability to service some devices and/or the being unable to process and forward device callhomes in a timely manner. The performance and behavior of the Policy Manager may also be significantly impacted.

Policy Manager: The recommended device limit for each Policy Manager is 750 devices. This limit enables the Policy Manager to retain spare bandwidth that may be needed during times of high activity.

Note: Manager at risk of database corruption during periods of high activity. Database failure / corruption which could result in the loss auditing of remote session approvals, connect home file uploads, configuration changes and Policy Manager access audits. Policy Manager database corruption may also result in the loss of Policy Manager configuration and have significant impact on EMC's ability to provide remote support.

IMPORTANT

Exceeding the maximum device limits may cause performance degradation, resulting in remote access support limitations and a loss of connect home capabilities. Policy Manager Database failure / corruption which could result in the loss auditing of remote session approvals, connect home file uploads, configuration changes and Policy Manager access audits. Policy Manager database corruption may also result in the loss of Policy Manager configuration and have significant impact on EMC's ability to provide remote support.

Table 8 Gateway Client configuration examples for maximum devices

	Configuration	Maximum devices	Policy Manager	Total servers
Site 1	Clustered HA servers group 1	250	Server No. 1 (servicing 6 Gateway Clients, 750 devices)	7
	Clustered HA servers group 2	250		
	Clustered HA servers group 3	250		
	Clustered HA servers group 4	250	Server No. 2 (servicing 6 Gateway Clients, 750 devices)	7
	Clustered HA servers group 5	250		
	Clustered HA servers group 6	250		
	Total maximum devices	1500		14
Site 2	Single Gateway Client server 1	250	Server No. 1 (servicing 3 Gateway Clients, 750 devices)	4
	Single Gateway Client server 2	250		
	Single Gateway Client server 3	250		
	Single Gateway Client server 4	250	Server No. 2 (servicing 3 Gateway Clients, 750 devices)	4
	Single Gateway Client server 5	250		
	Single Gateway Client server 6	250		
	Total maximum devices	1500		8
Site 3[a]	Single Client server 1 / co-located PM	250	(Co-located on Gateway Client 1, servicing 3 Gateway Clients, 750 devices)	3
	Single Gateway Client server 2	250		
	Single Gateway Client server 3	250		
	Single Client server 4 / co-located PM	250	(Co-located on Gateway Client 4, servicing 3 Gateway Clients, 750 devices)	3
	Single Gateway Client server 5	250		
	Single Gateway Client server 6	250		
	Total maximum devices	1500		6

a. The Site 3 example is not a recommended configuration, but may be used as a test configuration.

Recommended ESRS IP configurations

EMC has three recommended configurations for ESRS IP:

- High Availability Gateway Cluster and Policy Manager (Standalone or Redundant) (preferred configuration)
- Single Gateway Client Server and Policy Manager (Standalone or Redundant)
- Single Gateway Client Server with co-located Policy Manager (recommended for testing only)

The following section describes these recommended configurations.

High Availability Gateway Cluster and Policy Manager

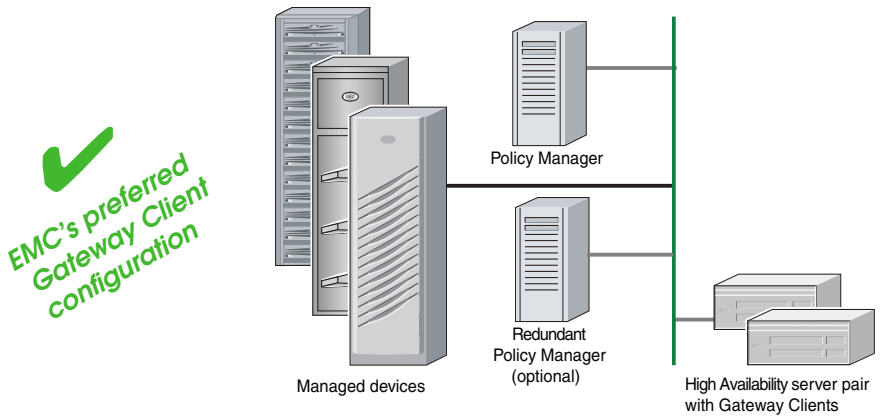


Figure 3 Clustered HA Gateway Client servers and Policy Manager

EMC's preferred configuration for ESRS IP is the **High Availability Gateway Cluster and Policy Manager** configuration shown in Figure 3 on page 43.

Once the cluster relationship is established, devices may be deployed on any of the clustered Gateway servers and are managed by *all* Gateway servers in the High Availability solution. Each server serves as a peer for the other servers in the cluster relationship. Each server monitors all devices, and any of the clustered servers can provide remote support access and/or connect home activity.

The Policy Manager provides auditing of connect homes and script execution on the ESRS IP Client. The Policy Manager also provides auditing and access control to managed devices. A Redundant Policy Manager is optional but highly recommended. It will enable you to manually fail over your backup Policy Manager database in the event that your primary Policy Manager becomes unavailable.

If you implement the High Availability Cluster and Policy Manager configuration, the Policy Manager will not be impacted by failure of the Gateway server hardware.

The **High Availability Gateway Cluster and Policy Manager** configuration has the following characteristics:

- **Number of required servers:** 3 (minimum), or 3 VMware instances on separate servers (provided that the minimum hardware requirements are met)
- **Pros**:
  - The Policy Manager provides auditing and access control for the solution.
  - The cluster configuration provides connect home and remote support connection redundancy.
  - In the event of a server hardware failure, the cluster configuration allows for easy recovery of the failed ESRS IP Client.
- **Con**: Multiple servers or VMware instances are required.

Single Gateway Client and Policy Manager

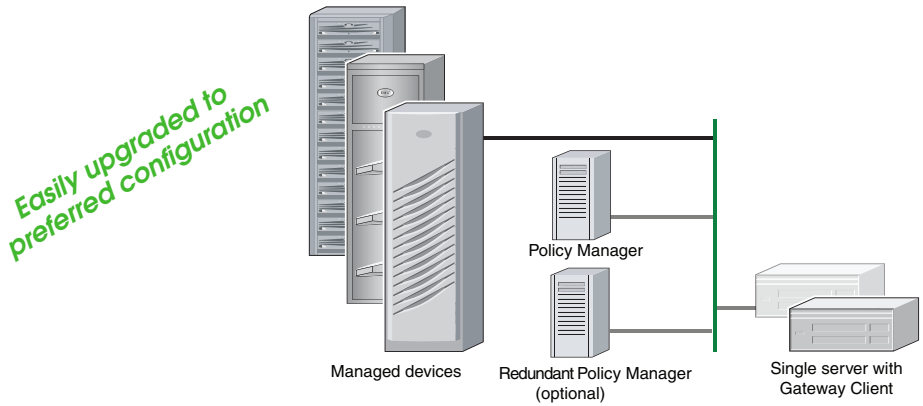


Figure 4 **Single Gateway Client server and Policy Manager**

The **Single Gateway Client and Policy Manager** configuration shown in Figure 4 on page 45 is designed for customers who initially want to utilize a single Gateway server with a separate Policy Manager server.

Note: This configuration does not provide High Availability. It does, however, provide an upgrade path to a High Availability configuration.

The **Single Gateway Client and Policy Manager** configuration has the following characteristics:

- **Number of required servers:** 2
- **Pro**: Ease of upgrade from this configuration to a High Availability Gateway Cluster configuration (the preferred configuration)
- **Con**: Single point of failure for the server, which can negatively impact connect home and remote access

If you upgrade from the single Gateway Client configuration to the High Availability Gateway Cluster configuration, upgrade tasks will include installation of the new servers and ESRS IP Client software. The new servers must be clustered to the original server and pointed to the same Policy Manager. Devices are then configured to utilize the other servers in the cluster for connect home failover.

Single Gateway Client server with co-located Policy Manager

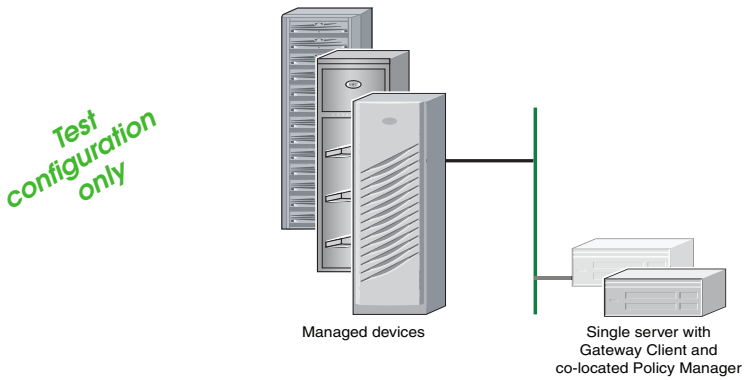


Figure 5 Single Gateway Client server with co-located Policy Manager

The configuration shown in Figure 5 on page 46 is sometimes used for initial certification (or testing) of the ESRS IP Solution.

IMPORTANT

This configuration does not provide High Availability, and is not a supported configuration for production environments.

The **Single Gateway Client server with co-located Policy Manager** configuration has the following characteristics:

- **Number of servers:** 1
- **Pro**: Only one server is required.
- **Con**: The single-server configuration is a single point of failure. This configuration should be used for test purposes only.

The tasks required to upgrade to a High Availability configuration would include: installation of a separate Policy Manager server, migration of current policies to the new Policy Manager, and establishment of the High Availability Gateway Cluster. The new Gateway Client server must be clustered to the original server, and both Gateway Clients must be pointed to the new standalone Policy Manager.

Note: Minimum recommended memory for Gateway with Collocated Policy Manager is 3 GB.

Other supported configurations

EMC recommends one of the three configurations described in "Recommended ESRS IP configurations" on page 43. However, EMC also supports the following configurations:

- High Availability Gateway Client servers without Policy Manager
- Single Gateway Client server without Policy Manager

This section provides details on these other supported configurations.

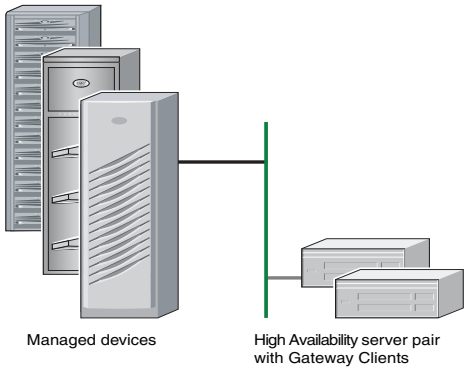


Figure 6 High Availability Gateway Client servers without Policy Manager

High Availability Gateway Client servers without Policy Manager

The **High Availability Gateway Client servers without Policy Manager** configuration shown in Figure 6 on page 47 is supported by EMC. The configuration has the following characteristics:

- **Number of servers:** 2
- **Pros**:
  - This configuration can be upgraded to a High Availability Gateway Cluster with standalone Policy Manager (preferred configuration).
  - This configuration provides connect home and remote support connection redundancy.

- This configuration allows for easy recovery of the failed server In the event of a server hardware failure.

◆ **Con**:

No Policy Manager (therefore no access control or auditing).

If you decide to upgrade from this configuration to a configuration that includes a Policy Manager, installation and configuration will be required. Both Gateway Client servers must be pointed to the new Policy Manager.

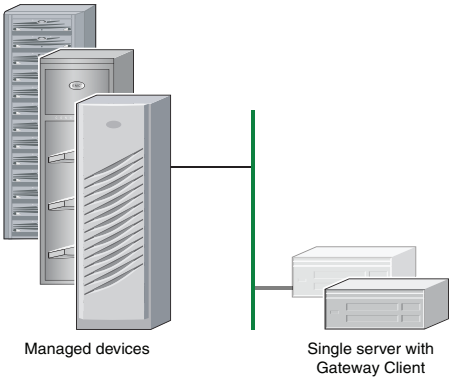


Figure 7 Single Gateway Client server without Policy Manager

Single Gateway Client server without Policy Manager

The **Single Gateway Client server without Policy Manager** configuration shown in Figure 7 on page 48 is supported by EMC.

The configuration has the following characteristics:

◆ **Number of servers:** 1

◆ **Pro**:

- This configuration can be upgraded to a recommended configuration.

◆ **Cons**:

- No Policy Manager (therefore no access control or auditing)
- Single point of failure for the Gateway Client server

If you decide to upgrade from this configuration to a configuration that includes a High Availability Gateway Cluster and a Policy

Manager, upgrade tasks will include installation and configuration of the Policy Manager, installation of the new Gateway Client, and establishment of the High Availability Gateway Cluster. The new Gateway Client server must be clustered to the original Gateway Client server, and both Gateway Client servers must be pointed to the new standalone Policy Manager.

Topology and network considerations

Follow the recommendations and other information in this section when you are making decisions about your site topology.

Determining the quantity of Gateway Clients and Policy Managers

The quantity of independent ESRS IP Client solutions you install is determined by the total number of devices that you want to monitor.

There is a maximum number of monitored devices that can be managed by a single Gateway Client server (or HA clustered servers) and each Policy Manager:

- A single Gateway Client server (or a server in a High Availability cluster) can manage a maximum of 250 devices.
- A single Policy Manager can manage a maximum of 750 monitored devices.

Note: Each CLARiiON device serial number is deployed as two devices.

Thus, for *each* 250 or fewer monitored devices (where each CLARiiON counts as two devices), install one Gateway Client server (or multiple clustered servers), and one Policy Manager per three Gateway Client servers (or three sets of clustered servers). Examples are shown in Table 8 on page 42.

Installing a separate Policy Manager server

EMC recommends that you install the Policy Manager on a separate dedicated server on your internal production network.

This is recommended for the following reasons:

- **Easier access to the Policy Manager server**
  You will be able to quickly log in to the Policy Manager server to respond to a remote access request or make changes to your device access or authorization rules.
- **Increased network security for the Policy Manager**
  The Policy Manager is designed to be inaccessible to all third parties, including EMC. If you install the Policy Manager on a separate server inside your internal network, there is virtually no way for any third party to gain access to the server application.

Note: If you want to install a single Gateway Client server in your DMZ, you may co-locate the Policy Manager on this server. This configuration is recommended for testing purposes only, and is not recommended for production purposes. If you decide to use this configuration, you must ensure that the Policy Manager has bidirectional access to your internal network so that it can provide email notification and permit access to the Policy Manager application.

Protecting the Gateway Client server

There are no specific technical restrictions on the location of Gateway Client servers within the network. However, you should do the following:

- Provide firewall protection for your Gateway Client server.
- Block all network ports that are not required by the ESRS IP Solution.

Note: See Table 6 on page 34 to identify the ports that should be opened.

Using proxy servers

The ESRS IP Solution supports the use of a proxy server for routing outbound Internet traffic from the ESRS IP Client to EMC. A list of tested proxy servers, protocols, and network configuration requirements is provided in "Enabling proxy server for ESRS IP Client traffic to EMC" on page 31.

When EMC installs your ESRS IP Solution software, your EMC Global Services professional will configure the Clients to route all outbound Internet traffic to the proxy server and to use only the port that you specify to send data to the proxy server. The proxy server must direct the Client transactions through the external firewall over port 443.

You are responsible for all proxy server configuration, rules, and troubleshooting needs resulting from ESRS IP Solution preparation and installation.

IMPORTANT

To ensure communication integrity, proxy servers and devices external to your DMZ must not perform any method of SSL checking on outbound or inbound IP traffic.

Topology configurations

There are several options for locating the Gateway Clients and Policy Manager. This section provides details on several configurations.

The following topology diagrams represent a configuration of a High Availability Gateway Client with a Policy Manager.

The recommended Gateway Client configuration is shown in Figure 8 on page 52. The Gateway Client is located on a private management LAN (or VLAN), and the Policy Manager is located on the production network.

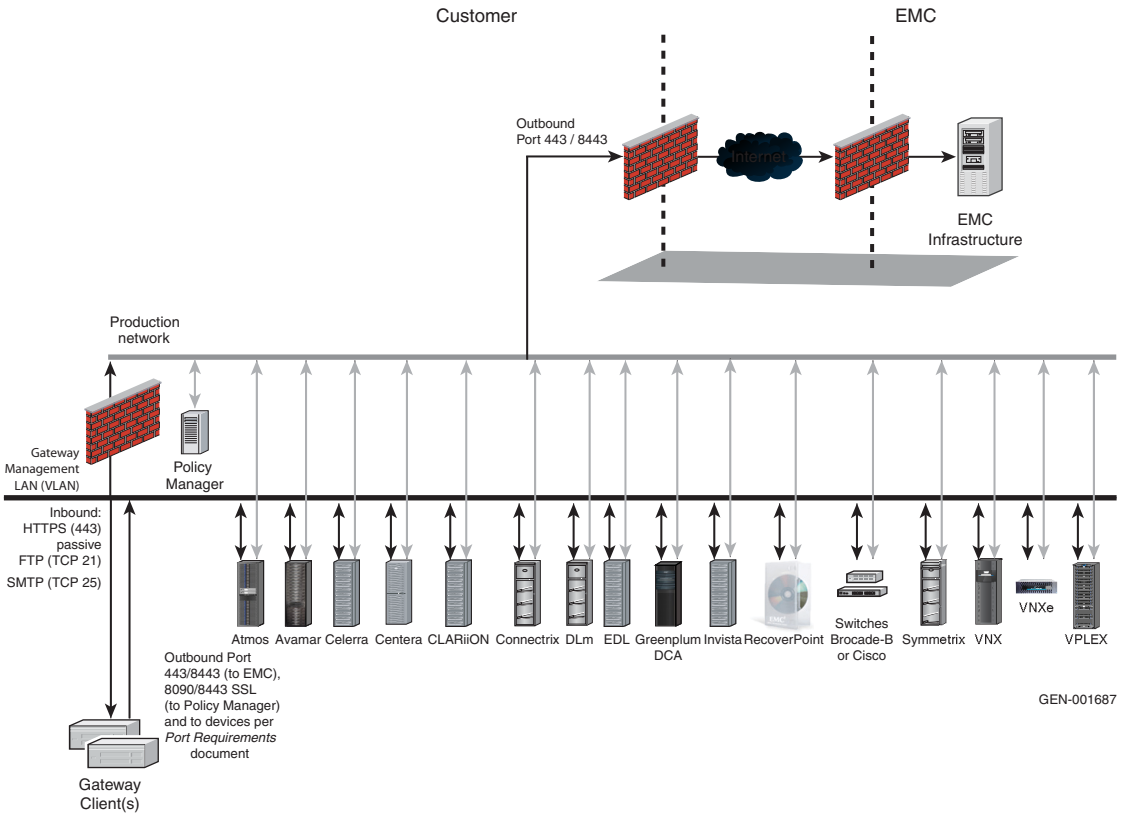


Figure 8 Gateway Client / Management LAN configuration

Another configuration is shown in Figure 9 on page 53. In this configuration, the Gateway Client and Policy Manager are both located on your production LAN.

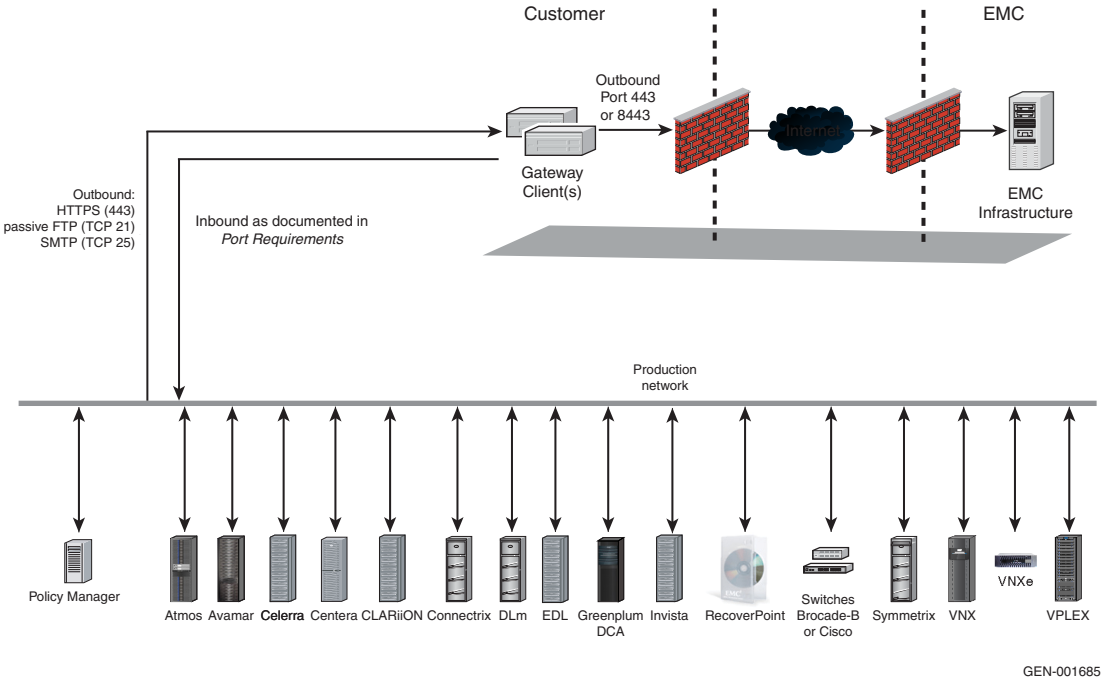


Figure 9 Gateway Client / Production network configuration

In Figure 10 on page 54, the Gateway Client server is located in your DMZ, while the Policy Manager is located on your production network.

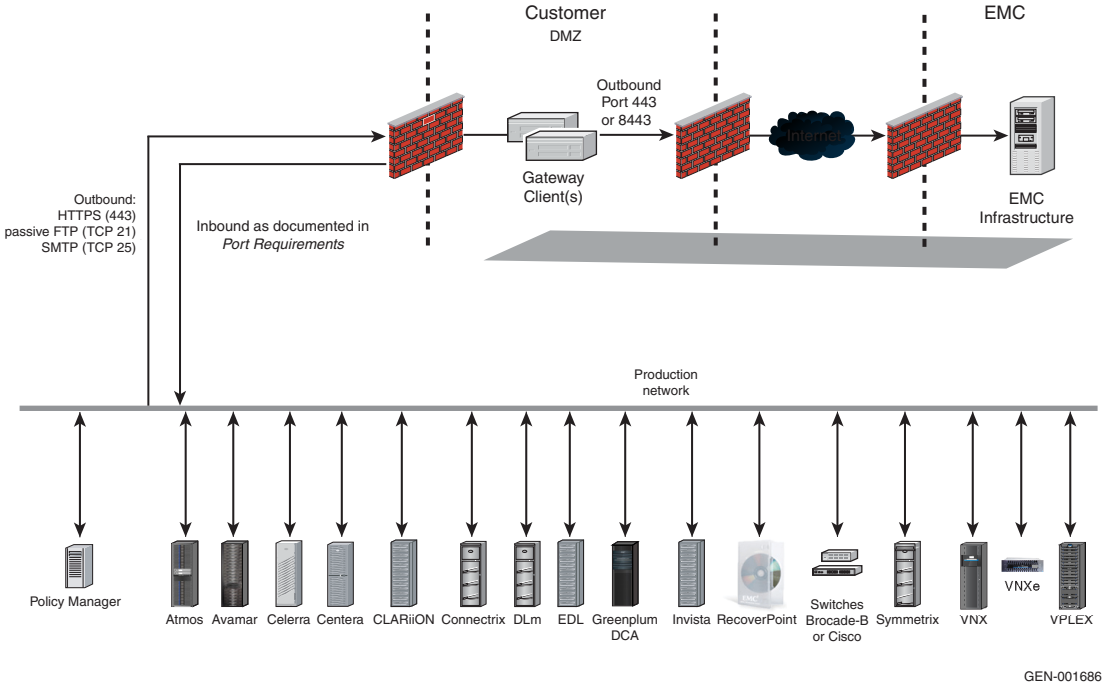


Figure 10 Gateway Client / DMZ configuration

About the Policy Manager

The Policy Manager is the ESRS IP Solution component that determines, for each access request, whether the request should be granted, denied, or forwarded elsewhere for a decision. The Policy Manager also creates and maintains audit logs for your site. These logs tell you which activities have occurred, when they occurred, and who performed them. If a service request is supplied as part of an access request, the Policy Manager will display the service request in the Notification email and in the audit of the request and approval or denial of the request.

Although a Policy Manager may be installed at any time, EMC recommends that it be installed at the time of the Gateway Client installation. The ESRS IP Configuration Tool is used to establish the relationship between the Policy Manager and the Gateway Client. The two are not automatically linked.

IMPORTANT

Installation of a Policy Manager is *highly recommended*. Without a Policy Manager, your ESRS IP Solution site will not have access control or audit logging, and access will be "Always Allow."

Redundant Policy Manager

For additional protection, EMC highly recommends installation of a Redundant Policy Manager. This will enable you to continue policy management operations if your Policy Manager becomes unavailable. If this occurs you would manually fail over to the Redundant Policy Manager.

Note: If you install a Redundant Policy Manager, you must set up an automated backup process for your Policy Manager database so that it can be restored onto the Redundant Policy Manager. Local Policy Manager Database backup is configured during Policy Manager installation.

Policy Manager authorization settings

There are three levels of authorization for remote access activity. The ESRS IP Solution monitors activities and responds according to the authorization settings:

- **Always Allow** — Use this setting if you want to always allow remote access for the activity.

- **Never Allow** — Use this setting if you want to always deny remote access for the activity.
- **Ask for Approval** — Use this setting if you want to require manual approval of remote access requests for the activity. Approval is performed by using the Policy Manager's web-based user interface.

Policy Manager failure

If the Policy Manager fails, certain default conditions apply. Some of these default conditions can be overridden. This section explains the default response and how to override the default response if desired.

Default response

If a Policy Manager server failure or communication failure occurs, policies are cached on the Gateway Client. The following default conditions will apply:

- An **Always Allow** or **Never Allow** policy setting will allow or deny the applicable activity request, just as the Policy Manager would have done.
- An **Ask for Approval** setting will time out, since the Policy Manager is not available to request and transmit approval. This will effectively deny the activity request.

Overriding the default response

If remote access is required after a Policy Manager failure (when the setting is **Ask for Approval**), you may grant access by using the ESRS IP Configuration Tool to disable the Policy Manager connection on the Gateway Client(s).

The illustration in Figure 11 on page 56 provides a view within the Configuration Tool on the Gateway Client. To remove Policy Manager requirements, clear the Enable Remote Policy Manager checkbox and save the new setting by clicking Apply Settings.

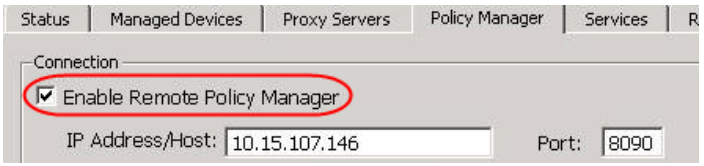


Figure 11 **Configuration Tool: Removing Policy Manager requirements**

Clearing the Enable Remote Policy Manager checkbox causes Client policies to revert to **Always Allow**. This procedure also flushes any previously cached policy settings and audits.

Audit entries remain cached on the ESRS IP Client if the following conditions are met:

- If no changes have been made to the ESRS IP Solution configuration by the Configuration Tool
- If the ESRS IP Client service has not been restarted
- If the ESRS IP Client server has not been rebooted

If these conditions are met, the cached audit entries will be appended to the active audit log when the Policy Manager becomes available.

About not using a Policy Manager

If you do not use a Policy Manager, or if the Policy Manager is not actively configured with ESRS IP Clients, the ESRS IP Solution approves all remote access requests and does not provide any access control audit logging.

About High Availability Gateway Clusters

To ensure maximum remote support uptime for your site, EMC strongly recommends that you prepare a minimum of two servers on which EMC Global Services can install an ESRS IP Gateway Client for configuration as High Availability Cluster.

Each Gateway Client server in the High Availability cluster should be running the same version of the Gateway Client software. For example, if one of the Gateway Clients is running release 2.04 code, all of the other Gateway Clients in the cluster should also run release 2.04 code. This will ensure that all of the Gateway Clients in the cluster are able to communicate with all of the device types qualified in that code release.

IMPORTANT

A High Availability Gateway Cluster implementation provides multiple-server "active/active" server support. It does *not* perform an automated server failover. See details in this section.

Note: Each Gateway Client server must have Windows Terminal Services Remote Desktop enabled so that EMC Global Services can provide support if necessary.

A High Availability Gateway Cluster server configuration requires a minimum of two dedicated servers. These servers actively and simultaneously monitor devices on their shared managed device list. They also share the handling of remote access session requests and connect home requests based on the configuration of the managed devices.

With a High Availability implementation, your Gateway Client servers implement an "active/active" solution, which eliminates the single-point-of-failure characteristic of a single-server configuration. The servers synchronize their managed device configuration information by relaying device list modifications to one another through the EMC ServiceLink application servers.

Devices are usually deployed to the Gateway Client server that is physically located closer to the device. Monitoring and event notification are performed by that Gateway Client, unless a problem occurs with that server. In that case, another server in the Gateway cluster performs the activity. Remote access session management is

performed by the first device in the Gateway cluster that sends a heartbeat and responds to the access request.

CAUTION

CLARiiON and EDL devices in a distributed environment do not have High Availability functionality for callhome event notification. These devices use a non-resilient email client for sending a single message directly to EMC or the Gateway. If the message fails to reach EMC or the Gateway for any reason, no other notification attempts are made.

High Availability Gateway Cluster clients do not have failover

A High Availability Gateway Cluster provides operational redundancy, ensuring that at least one of the servers is always operational. The High Availability cluster also provides backup capacity, which is operational in advance of any failure.

However, it is important to understand that the ESRS IP Solution does not implement *failover* behavior.

If a server fails in a High Availability Gateway Cluster

If a Gateway Client server fails, the other Gateway Client servers in the cluster *already have* full responsibility. Also, when device-to-Gateway Client ratios are properly configured, the other servers have the capacity for all device monitoring, event notification, and remote access session management.

When the failed server comes back online, all ESRS IP Clients once again simultaneously monitor devices and share the handling of connect home and remote access session requests.

Failover behavior at the EMC device level

Failover of connect home is initiated at an EMC storage device

When appropriately configured, EMC device connect home applications supports clustered High Availability servers as defined by the Product implementation of ConnectEMC. When an EMC device supported by ESRS recognizes that connect home calls can not be received by the Gateways Client, it switches its connect home destination from its primary Gateway Client to an alternate.

Note: There is no failover for connect home messages by Gateway Client servers in Distributed CLARiiON environments. Only one message is sent by the EMC device. If the message fails for any reason, no attempt is made to resend the message.

About Single Gateway Client configurations

EMC provides you with the option of configuring a single Gateway Client server.

However, when you choose a single Gateway Client configuration:

- You do *not* have High Availability protection. If the server fails, remote connection is not possible.
- If a server or connection fails, EMC will not be notified of exception events on devices. As a result, EMC will not be able to provide remote support in a timely manner.

4

Preparing for Site Installation

This chapter describes how you should work with your assigned EMC Global Services professionals to prepare your sites for installation of the ESRS IP Solution.

The chapter includes the following sections:

Additional information for specific information of Network; Operation System and ESRS IP Solution application configuration are defined in the *EMC Secure Remote Support IP Solution Operations Guide*. Conslutation as to specifics may require contacting ESRS Customer Support.

Overview

This section provides information about site installation.

Coordination with EMC

Because the EMC Secure Remote Support IP Solution has both customer site components and EMC site components, your network, storage system, and security administration personnel must work closely with your EMC Global Services representatives to prepare your site for ESRS IP software installation.

As part of the software installation process, your EMC team may initiate multiple planning meetings with you to ensure that your onsite software installation is as fast and seamless as possible. You should also hold internal meetings to discuss your site configuration planning and documentation requirements.

For example, planning meetings could include the following meetings:

- An implementation kickoff meeting with your team and EMC Global Services and EMC Sales. This meeting would include a review of the ESRS IP Solution.
- A site configuration planning and documentation meeting with your network, storage, and security administration teams and EMC Global Services
- A final site installation planning and scheduling meeting with your network, storage, and security administration teams and EMC Global Services

For additional details, see "EMC coordination schedule" on page 63.

Preparation work

In conjunction with your meetings with EMC, you should plan and execute the required preparation work. For more information on these requirements, refer to the following sections:

- "Installing and configuring servers" on page 67
- "Configuring your network" on page 67

EMC coordination schedule

Before installation of your ESRS IP Solution, you must provide EMC Global Services with the following information for configuring your ESRS IP software:

- Contact information for the people who will prepare your site for installation and support your hardware and software
- Specifications for the servers on which you plan to install the ESRS IP Client and Policy Manager applications
- Specifications for the number and types of devices to be managed by the Solution
- Specifications for the network configuration, network security policies, and Internet protocols that determine how devices, Gateway Client and Policy Manager servers, and EMC's ServiceLink servers communicate with one another within the ESRS IP Solution

Note: A Pre-site Checklist is available from your EMC Global Services representative or may be downloaded from PowerLink. The checklist will help you track and report the progress of your site preparation for the ESRS IP Solution.

Kickoff meeting

One of the first steps for a successful ESRS IP Solution implementation is a review and implementation kickoff meeting with EMC Sales, EMC Global Services, or both.

At this meeting, you will:

1. **Review topology options** — The EMC team will provide an overview of the ESRS IP solution. You and the EMC team will discuss the possible site configuration options and review the necessary site requirements for your chosen configuration.
2. **Determine physical locations and resources** — You and the EMC team will identify physical locations for installing the Gateway Client and Policy Manager servers. You will identify the network, storage, and security personnel responsible for:
   - Preparing your site for installation

- Troubleshooting the customer-supplied hardware and software during installation
- Maintaining the customer-supplied hardware and software after installation

Note: EMC Global Services is not responsible for troubleshooting or resolving customer operating system or network issues. EMC Global Services is also not responsible for performing server operating system installation and configuration.

3. **Obtain EMC documentation and tools** — EMC Global Services will provide you with the following documentation and tools:
   - EMC Secure Remote Support IP Solutions Technical Description
   - *EMC Secure Remote Support IP Solutions Site Planning Guide*
   - EMC Secure Remote Support IP Solutions Operations Guide
   - *EMC Secure Remote Support IP Solutions Pre-Site Checklist* (to be completed with EMC Global Service assistance)
   - Customer Environment Check Tool (CECT)

These documents and tools are also available for download from PowerLink.

Action items

EMC will order your ESRS IP Solution kit — After a successful kickoff meeting, EMC Sales personnel will place an order for the ESRS IP Solution kit (Model # ESRS-GW-200, Part # 953-002-303).

Note: If you are installing a High Availability Gateway Cluster, and the Gateway Client servers are at different sites, a separate kit must be ordered for each site (one kit per Site ID).

Begin your internal prep work — At this point, you should hold meetings with your network, storage system, and security administration teams. Review and be prepared to discuss the following items so that your team will be ready to make configuration decisions:

1. Review the following documents, as well as any additional information that EMC provides during the kickoff meeting:
   - *EMC Secure Remote Support IP Solution Site Planning Guide*

- *EMC Secure Remote Support IP Solution Technical Description*
- *EMC Secure Remote Support IP Solution Operations Guide*

2. Decide which EMC devices that you want EMC to support remotely via ESRS IP. Chapter 1, "Overview," provides information on the device models that are available for support by the ESRS IP Solution.
3. Decide which ESRS IP site configuration option that you want to implement. Chapter 3, "Configurations," provides information to help you make this decision.
4. Decide how you want to configure your network to accommodate the ESRS IP Solution components. Chapter 3, "Configurations," provides information to help you make this decision.
5. Assign a resource to record the specifications of each component in your ESRS IP site configuration. Record the information in the *EMC Secure Remote Support IP Solutions Pre-Site Checklist* that you obtain from your EMC Global Services professional.

   This editable checklist will help you record information about whichever of the following components apply to your configuration:

   - Gateway Client server
   - Policy Manager server
   - Managed devices
   - Proxy server
   - Email server for Policy Manager
   - Network information for the connections between components

   Note: Chapter 2, "Component Requirements," provides information on the minimum requirements for each customer-supplied component of the ESRS IP solution.

6. Prepare a block diagram that depicts the planned server and device network configuration.

Configuration planning and documentation meeting

This will be the second meeting between your network, storage system, and security administration teams and EMC Global Services representatives. At this meeting, you will take the following actions:

1. **Review site plans** — You and your EMC Global Services representative will review and discuss your site configuration plans. You will use your completed *EMC Secure Remote Support IP Solutions Pre-Site Checklist* and block diagram as references.
2. **Create a prep-work schedule** — Your network, storage system, and security administration personnel will schedule the onsite pre-installation work that your teams must perform when setting up the Gateway Client or Policy Manager servers. You should also review with EMC a schedule for the onsite time required for EMC to perform any other changes required before the upcoming ESRS IP solution installation.
3. **Schedule device upgrades (if needed)** — You should inform EMC Global Services whether any EMC device upgrades are needed to make them compatible with the ESRS IP solution.

Note: Any upgrades that must be performed on storage devices in order to make them compatible with the ESRS IP solution are not part of the ESRS IP deployment process.

Action items

Implement site configuration — Your network, storage system, and security administration teams should now implement the server and network preparation work that they scheduled during the second meeting with EMC Global Services, as detailed in the following sections.

Run initial site tests — EMC Global Services will provide you with the Customer Environment Check Tool utility (CECT). You must install this utility on each target Gateway Client and Policy Manager server. The utility verifies that your hardware, operating system, and network connectivity configurations meet the ESRS IP solution requirements for connectivity to EMC and to the devices to be managed. Any adjustments must be documented within the pre-site checklist.

Provide the output of the Customer Environment Check Tool (CECT) and the documents for the previous page (completed Presite Check

List and network diagram) to the EMC Global Services Representative for review.

Installing and configuring servers

Before the ESRS IP software is installed, you must install and configure the required operating system on your Gateway Client and Policy Manager servers. The *EMC Secure Remote Support IP Solutions Operations Guide* provides more information for a standard "C:" drive installation and for an operating system installation on a drive other than the standard.

Customer Environment Check Tool

EMC Global Services will provide you with the Customer Environment Check Tool utility (CECT), which tests your target Gateway Client servers and Policy Manager servers to verify that they meet hardware, operating system, and network configuration requirements.

The *EMC Secure Remote Support IP Solutions Operations Guide* provides instructions for installing and running CECT.

Testing configuration

When you have finished configuring the operating system on the servers, you must run tests to make sure the servers are configured properly, and that the Internet Information Services (IIS) FTP and SMTP services are running normally on the Gateway Client servers.

Run **CECT** on all servers and ensure that each server passes all required tests before the ESRS IP installation date. **CECT** provides output logs which must be supplied to EMC Global Services.

Note: CECT requires that Microsoft .NET Framework 2.0 w/ SP1 or higher (or a newer version that is backward compatible with 2.0. Note that the .NET 3.5 and 4.0 are not compatible at this time. Microsoft Visual C++ 2005 SP1 Runtime library is also required on the Gateway Client server.

Preparing network connections

Before EMC Global Services installs the ESRS IP software, you must ensure that your Client servers can communicate with EMC, with your Policy Manager server, and with your managed devices,. The **Customer Environment Check Tool** (CECT) has the capability to test and verify connectivity to EMC, the Policy Manager server, and with your devices to be managed by the ESRS IP client.

Configuring your network

To configure your network to support ESRS IP, take the following steps:

1. Ensure that your servers have unique IP addresses for all interfaces. Adhere to the following restrictions:

Note: All unused interfaces should be disabled.

- You must not use Port Address Translation. The Gateway Client servers, as well as all EMC devices to be managed through the Gateway Client, have services that listen for connection requests.These services will not work if Port Address Translation is employed.
- You must not use Dynamic IP (DHCP) addresses for any ESRS IP component, whether they be Gateway Client servers, Policy Manager servers, or managed devices.
- If you use DHCP to assign IP addresses to any Solution components (Gateway Client servers, Policy Manager servers, or managed devices), they must have "permanent reservation" IP addresses. Leases for any IP addresses that EMC devices are using must not expire. It is best to assign static IP addresses to those devices you plan to manage using the ESRS IP Solution.

2. Enable communication from each of your managed devices through your internal firewall to your Gateway Client servers over the required port connections.

Note: EMC is not and will not be responsible for the configuration of Firewalls and or Router/Switch Access Control Lists (ACLs).

3. Follow these proxy server guidelines:
   - **If you are *not* using a proxy server for outbound Internet traffic:**
     Enable your ESRS IP Clients to communicate with the Internet through your external firewalls over ports 443 and 8443.
   - **If you *are* using a proxy server for outbound Internet traffic:**
     Enable your ESRS IP Clients to route all outbound traffic to the proxy server over the port required by your proxy server. The proxy server then needs to be able to connect outbound through the firewall over ports 443 and 8443.

   Note: Neither the proxy server nor the firewall should do SSL checking. The customer is responsible for configuring Proxy Server.

4. Check that you have no existing constraints on your network that could interfere with communication between the following:

- Gateway Client servers and Policy Manager servers
- Gateway Client servers and EMC
- Gateway Client servers and your managed devices

To ensure connectivity, use the port lists in Table 6 on page 34 and Table 7 on page 35. These tables show which ports need to be open for ESRS IP network traffic.

Testing network connections and port functionality

You must test all required connectivity between the following pairs:

- Gateway Client servers and EMC
- Gateway Client servers and your outbound proxy server (if any)
- Your outbound proxy server (if you use one) and EMC
- Gateway Client server and Policy Manager server (if applicable)
- Gateway Client servers and managed devices

EMC requires that you test all of these connections *before* the Installation Planning and Scheduling meeting. You should take to that meeting a list of any problems or failures that you have encountered.

Use the Customer Environment Check Tool (CECT) on each target Gateway Client server and Policy Manager server to verify that all required network connections are functioning properly. CECT will be run before doing any installation work in order to identify potential issues. It also should be run after installation is completed to ensure that the ESRS IP Client Solution is functioning properly.

Installation planning and scheduling meeting

An installation and planning meeting should be the final meeting between customer network, storage, and security administration teams and EMC Global Services. At this meeting you should take the following actions:

1. **Review the Pre-site Checklist** — Your network, storage, and security administration teams should review your finalized pre-site checklist with EMC Global Services. The checklist must be complete and accurate since it will be used by EMC Global Services to perform ESRS IP installation. For an example of the checklist, see Appendix C, "Pre-Site Checklist Example."
2. **Discuss and resolve problems** — Using your notes from network tests, as well as the output logs provided by the Customer Environment Check Tool (CECT), your team should discuss with EMC Global Services any problems that must be resolved before

scheduling the ESRS IP installation.

Note that EMC Global Services is not responsible for:

- Troubleshooting or resolving customer operating system or network issues
- Performing server operating system installation and configuration
- Configuring proxy servers or firewalls

3. **Schedule the installation** — Work with EMC Global Services to schedule your ESRS IP installation date.
4. **Run CECT again —** EMC recommends that you run the Customer Environment Check Tool (CECT) one more time just before your installation date. This will help determine if any changes have occurred to your environment between your initial site preparation work and the installation date.

A

Pre-Site Checklist Example

This appendix is adapted from *EMC Secure Remote Support IP Solution Pre-Site Checklist*. The Pre-site Checklist is designed to help EMC and customer personnel successfully coordinate the installation and maintenance of the ESRS IP Solution at customer sites.

You need to complete your own checklist in coordination with your EMC Global Services professional. Topics in this appendix include:

Contact information

Site information

Length of engagement	Installation date	Completion date

Site function	Site name	Site ID	Locations
Primary			
Secondary *(if applicable)*			

Site contacts

Contacts	Company	Role	Phone numbers	Email

Gateway Client / Policy Manager server details

Type	Sales order number	Serial number	Version	Location	Install drive/path
Primary Gateway Client					
Additional Gateway Client					
Additional Gateway Client					
Primary Policy Manager					
Additional Policy Manager					

ESRS managed devices

EMC products (managed devices)	Serial number	Location	Connect Home method	IP address	Date deployed

EMC products (managed devices)	Serial number	Location	Connect Home method	IP address	Date deployed

Environment specifications

Network

Proxy server IP address/port *(optional)*	
Proxy server username *(optional)*	
Proxy server password *(optional)*	
Network Address Translation (NAT) IP?	
Are ports 443 and 8443 open?	
Customer IP address ranges and customer subnet masks (device LANs)	
Client Server IP address (Internal/External)	
Is DHCP disabled?	
Is ESRS IP Client server in a DMZ?	
Is Client server inside customer network, and is customer using a proxy forwarder?	
Type of proxy server: Auto/HTTP/SOCKS	
Address (domain name or IP) of email server	
Admin email address	
Notification email address	

Gateway Client server

Equipment name	
Type	
Dual NIC cards available?	
IP address (1) / used for	
IP address (2) / used for	
Administrator rights	
Username	
Password	

Policy Manager server

Processor size, memory, drive size, free	
Dual NIC cards available?	
IP address / DNS name (1) used for	
IP address / DNS name (2) used for	
Windows Task Scheduler: Running unrestricted (so that Policy Manager backups	
Is port 8090 or 8443 open? Non-default port?	
Enable SSL communication with Client	

Checklist for installation visit readiness

Use this checklist with the **Customer Environment Check Tool** (described in *EMC Secure Remote Support IP Solution Operations Guide*).

Readiness item	References	OK?	Exception / notes
ESRS IP Software Kit (Model: ESRS-GW-200; Part:953-002-303)			
Has the software kit been ordered? (A kit is needed for each site if a High Availability Gateway Cluster is being installed at multiple sites.)			
Gateway Client servers are built and ready			
Supported operating system installed			
Windows Time Zone set to local time zone			
Internet Explorer 6.0+ installed			
.NET Framework Version 2.0 SP1 or greater installed (.NET Framework 3.5 and 4.0 are not compatible)			
Microsoft Visual C++ 2005 SP 1 Runtime library			
IIS installed and configured			
Server allows for user account notification			
Server attached to network in DMZ/other			
Network personnel verifies that server can route to internal devices (internal Gateway			
Network personnel verifies that server can route to Internet (internal Gateway Client)			
The **Customer Environment Check Tool** has been run and tests pass, otherwise note exceptions and follow-up plan for All Gateway and Policy Manager servers			
Policy Manager server is built and ready			
Supported operating system installed			
Windows Time Zone set to local time zone			
Internet Explorer 6.0+ installed			
.NET Framework Version 2.0 SP1 or greater installed is required to run the Customer Environment Check Tool (CECT) (.NET Framework 3.5 and 4.0 are not compatible)			
Server is on the appropriate network			

Readiness item	References	OK?	Exception / notes
Network personnel verifies that server can route to default ESRS IP Client			
The **Customer Environment Check Tool** has been run and tests pass, otherwise note exceptions and follow-up plan			
EMC database			
All managed devices are in EMC database with a status of “installed”			
IP Solution Site ID and P/N (953-001-994) in EMC database, with a status of “installed”			
Customer network and security external			
External IP Solution/firewalls allow 443 outbound (Site A and B)			
No SSL checking is performed on outbound communications on customer			
Internal IP Solution/firewalls opened up all appropriate ports for remote access connectivity *(Site A)*			
Atmos ports open			
Avamar ports open			
Celerra ports open			
EMC Centera ports open			
CLARiiON ports open			
Connectrix ports open			
Connection Home / FTP (passive ports open) Inbound to Gateway Client			
DLm ports open			
EDL ports open			
Greenplum DCA ports open			
Invista ports open			
RecoverPoint port open			
Switch-Brocade-B ports open			
Switch-Cisco ports open			
Symmetrix ports open			
VNX ports open			
VNXe ports open			
VPLEX ports open			
Internal IP Solutions/firewalls opened up all appropriate ports for remote access connectivity *(Site B)*			
Atmos ports open			
Avamar ports open			

Readiness item	References	OK?	Exception / notes
Celerra ports open			
EMC Centera ports open			
CLARiiON ports open			
Connectrix ports open			
Connection Home / FTP (passive ports open) Inbound to Gateway Client			
DLm ports open			
EDL ports open			
Greenplum DCA ports open			
Invista ports open			
RecoverPoint port open			
Switch-Brocade-B ports open			
Switch-Cisco ports open			
Symmetrix ports open			
VNX ports open			
VNXe ports open			
VPLEX ports open			
Device readiness complete *(Site A)*			
Atmos devices addressed			
Atmos devices physically connected to network			
Atmos devices updated for network			
Problems / failures of above noted			
Avamar devices addressed			
Avamar devices physically connected to network			
Avamar devices updated for network			
Problems / failures of above noted			
Celerra devices addressed			
Celerra devices physically connected to network			
Celerra devices updated for network			
Problems / failures of above noted			
EMC Centera devices addressed			
EMC Centera devices physically connected to network			
EMC Centera devices updated for network			
Problems / failures of above noted			
CLARiiON devices addressed			

Readiness item	References	OK?	Exception / notes
CLARiiON devices physically connected to network			
CLARiiON devices updated for network			
Problems / failures of above noted			
Connectrix devices addressed			
Connectrix devices physically connected to network			
Connectrix devices updated for network			
Problems / failures of above noted			
DLm devices addressed			
DLm devices physically connected to network			
DLm devices updated for network			
Problems / failures of above noted			
EDL devices addressed			
EDL devices physically connected to network			
EDL devices updated for network			
Problems / failures of above noted			
Greenplum DCA devices addressed			
Greenplum DCA devices physically connected to network			
Greenplum DCA devices updated for network			
Problems / failures of above noted			
Invista devices addressed			
Invista devices physically connected to network			
Invista devices updated for network			
Problems / failures of above noted			
RecoverPoint devices addressed			
RecoverPoint devices physically connected to network			
RecoverPoint devices updated for network			
Problems / failures of above noted			
Switch-Brocade-B devices addressed			
Switch-Brocade-B devices physically connected to network			
Switch-Brocade-B devices updated for network			

Readiness item	References	OK?	Exception / notes
Problems / failures of above noted			
Switch-Cisco devices addressed			
Switch-Cisco devices physically connected to network			
Switch-Cisco devices updated for network			
Problems / failures of above noted			
Symmetrix devices addressed			
Symmetrix devices physically connected to network			
Symmetrix devices updated for network			
Problems / failures of above noted			
VNX devices addressed			
VNX devices physically connected to network			
VNX devices updated for network			
Problems / failures of above noted			
VNXe devices addressed			
VNXe devices physically connected to network			
VNXe devices updated for network			
Problems / failures of above noted			
VPLEX devices addressed			
VPLEX devices physically connected to network			
VPLEX devices updated for network			
Problems / failures of above noted			
Device readiness complete *(Site B)*			
Atmos devices addressed			
Atmos devices physically connected to network			
Atmos devices updated for network			
Problems / failures of above noted			
Avamar devices addressed			
Avamar devices physically connected to network			
Avamar devices updated for network			
Problems / failures of above noted			
Celerra devices addressed			
Celerra devices physically connected to network			

Readiness item	References	OK?	Exception / notes
Celerra devices updated for network			
Problems / failures of above noted			
EMC Centera devices addressed			
EMC Centera devices physically connected to network			
EMC Centera devices updated for network			
Problems / failures of above noted			
CLARiiON devices addressed			
CLARiiON devices physically connected to network			
CLARiiON devices updated for network			
Problems / failures of above noted			
Connectrix devices addressed			
Connectrix devices physically connected to network			
Connectrix devices updated for network			
Problems / failures of above noted			
DLm devices addressed			
DLm devices physically connected to network			
DLm devices updated for network			
Problems / failures of above noted			
EDL devices addressed			
EDL devices physically connected to network			
EDL devices updated for network			
Problems / failures of above noted			
Greenplum DCA devices addressed			
Greenplum DCA devices physically connected to network			
Greenplum DCA devices updated for network			
Problems / failures of above noted			
Invista devices addressed			
Invista devices physically connected to network			
Invista devices updated for network			
Problems / failures of above noted			
RecoverPoint devices addressed			

Readiness item	References	OK?	Exception / notes
RecoverPoint devices physically connected to network			
RecoverPoint devices updated for network			
Problems / failures of above noted			
Switch-Brocade-B devices addressed			
Switch-Brocade-B devices physically connected to network			
Switch-Brocade-B devices updated for network			
Problems / failures of above noted			
Switch-Cisco devices addressed			
Switch-Cisco devices physically connected to network			
Switch-Cisco devices updated for network			
Problems / failures of above noted			
Symmetrix devices addressed			
Symmetrix devices physically connected to network			
Symmetrix devices updated for network			
Problems / failures of above noted			
VNX devices addressed			
VNX devices physically connected to network			
VNX devices updated for network			
Problems / failures of above noted			
VNXe devices addressed			
VNXe devices physically connected to network			
VNXe devices updated for network			
Problems / failures of above noted			
VPLEX devices addressed			
VPLEX devices physically connected to network			
VPLEX devices updated for network			
Problems / failures of above noted			
All items above have been checked and completed			
Exeptions have been reviewed			

Ports opened for Gateway Client operation

Product	Application	Port
Atmos		
Avamar		
Celerra		
EMC Centera		
CLARiiON		
Connectrix Manager		
DLm		

Product	Application	Port
EDL		
Greenplum DCA		
Invista		
RecoverPoint		
Switch-Brocade-B		
Switch-Cisco		

Product	Application	Port
Symmetrix		
VNX		
VNXe		
VPLEX		
Gateway		
Policy Manager		

Glossary

This glossary contains terms related to remote support and the ESRS IP Solution.

A

access See *Remote Access*.

C

connect home Connecting from a remote site to EMC's support network.

Client See *Gateway Client*.

Customer Environment Check Tool (CECT) A utility that verifies that a candidate server meets the hardware, software, and network configuration requirements for a successful Gateway Client and Policy Manager software installation.

D

DMZ Demilitarized zone — Device used to secure an internal network from unauthorized external access.

Dynamic IP address An address that is assigned by the access device by which the user's host connects over a dialup telephone line or by a set-top box for an IP over cable network.

E

EMC Powerlink Web-based document archive that is accessible and configurable for EMC customers and internal EMC users.

ESRS IP Solution The EMC Secure Remote Support IP Solution (ESRS IP), installed on a Gateway Client server, provides automated connect home and remote support activities through an IP-based solution enhanced by a comprehensive security system.

F

failover The capability to switch over automatically to a standby server upon the failure or abnormal termination of the previously active server. Failover happens without human intervention and generally without warning.

firewall A hardware or software device that is configured to permit, deny, or proxy data through a computer network which has different levels of trust.

FTP File Transfer Protocol — Used to transfer data from one computer to another, over the Internet or through a network.

G

Gateway Client An ESRS IP Solution software component that is installed on a customer-supplied dedicated server (or servers) or VMware instance. The servers act as the single point of entry and exit for all IP-based EMC remote notification and remote support activity.

I

IIS Microsoft Windows Internet Information Services lockdown tool — Functions by turning off unnecessary features, thereby reducing areas available to attackers.

P

Policy Manager An ESRS IP Solution software component that is installed on a customer-supplied server or servers. It enables customizable control of remote access to customer devices and maintains an audit log of remote connections.

proxy server A server (a computer system or an application program) which services the request of its clients by forwarding request to other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server provides the resource by connecting to the specified server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the servers's response, and sometimes it may serve the request without contacting the specified server.

R

remote access Communication with a processing device from a remote location through a data link.

S

Secure Sockets Layer (SSL) port A port that uses cryptographic protocols to provide secure Internet communications for data transfers.

SMTP Simple Mail Transfer Protocol — The de facto standard for email transmissions across the Internet.

T

topology Network configuration, including firewalls, servers, devices, and ports used for communication between all devices.

Index

V