EMC²

TECHNICAL NOTES

EMC® Secure Remote Support IP Solution

Release 2.08

Technical Description

P/N 300-012-315
Rev A01

February 28, 2011

This technical description contains information on the following topics:

Introduction

EMC maintains a strong commitment to protecting your information infrastructure through the 24x7 availability of remote technical support resources and automated secure remote support solutions. The EMC® Secure Remote Support IP Solution (ESRS IP) provides a secure, IP-based, distributed remote service support solution that provides command, control, and visibility of remote support access.

ESRS IP expands and improves the EMC Secure Remote Support portfolio with the following features:

- Consolidation — ESRS IP consolidates access points for EMC support by providing a uniform, standards-based architecture for remote access across EMC product lines. The benefits include reduced costs through the elimination of modems and modem lines, controlled authorization of access for remote support events, and consolidated logging of remote access for audit review.
- Security — ESRS IP fulfills requirements for authentication, authorization and auditing with a secure, highly scalable, fault-tolerant solution. This IP-based, firewall-friendly remote access architecture initiates all connections from your site.

  The ESRS IP security features include:

  - Comprehensive digital security — ESRS IP security includes SSL data encryption, TLS v1.0 tunneling with Advanced Encryption Standard (AES) 256-bit data encryption, entity authentication (private digital certificates), and remote access user authentication verified through EMC network security.
  - Authorization controls — Policy controls enable customized authorization to accept, deny, or require dynamic approval for connections to your EMC information infrastructure at the support application and device level.
  - Secure remote access session tunnels — ESRS IP establishes remote sessions using secure IP and application port assignment between source and target endpoints.
  - Auditing support — ESRS IP Policy Manager logs all remote access connections, all remote access connection termination, diagnostic script executions, and support file transfer operations. All log files are controlled and managed by you to enable auditing of remote support activities executed by EMC.

Description

This section provides a detailed description of the ESRS IP Solution.

Remote support benefits

The EMC remote support strategy delivers immediate response to product event reports such as error alerts, which can greatly increase the availability of your information infrastructure. When a support event occurs, EMC provides rapid remote support through two phases: first, through automated recognition and notification from your site to EMC (or recognition by EMC, in the case of connectivity loss), and second, through interpretation and response from EMC. In many cases this support can eliminate the need for an on-site support visit.

EMC's immediate and interactive remote support provides:

- Improved service levels
- Increased protection of information
- Simplification of complex environments
- Reduced risk
- Improved time-to-repair

The ESRS IP Solution augments the EMC secure remote support portfolio, which includes phone-based modems, WebEx, and e-mail.

Solution security

ESRS IP design acknowledges that the heart of any well-designed distributed system is security, and thus it incorporates the industry-recognized "3 As": authentication, authorization, and audit logging. ESRS IP employs multiple security layers to ensure that you and EMC can use the system with confidence.

From an applications architecture perspective, ESRS IP is an asynchronous messaging system in which all communications are initiated from your site. All communications between ESRS IP at your site and the EMC enterprise servers use the HTTPS protocol with end-to-end SSL tunneling with strong encryption.

ESRS IP uses a firewall-friendly, IP-based communication technology over SSL VPN gateway tunnels. Customer-controlled ESRS IP Clients negotiate the secure exchange of information between storage

management devices behind your internal firewall and the EMC Customer Support Center. All communication between your site and EMC is initiated by an ESRS IP Client at your site. Using industry standard Secure Sockets Layer (SSL) encryption over the Internet, and EMC-signed digital certificate authentication, your administrators need only enable outbound communication over SSL default ports 443 and 8443.

ESRS IP is designed to be scalable and fault-tolerant, and to provide you with the authentication, authorization, and audit logging control you require to meet your security needs and to support your environment. ESRS IP remote access to your EMC storage devices is secured using a session-based IP port-mapping solution. Service notification file transfers from the managed devices are always brokered through the ESRS IP Client to ensure secure encryption and audit logging.

The ESRS IP Solution comprises a suite of software products that securely link your EMC storage devices to the EMC Global Services support application systems. This distributed system provides you with the commands and controls to authorize and log EMC support actions such as remote access connections, file transfers, diagnostic script executions, and system updates.

The following security features are used in ESRS IP:

- TLS v1.0 tunneling with Advanced Encryption Standard (AES) 256-bit data encryption
- Bilateral authentication of digital certificate registration
- X.509 digital certificates generation
- ESRS IP Client authentication based on digital certificate at EMC
- EMC-issued RSA SecurID Authenticators for digital certificate registration
- EMC-issued RSA SecurID for user authentication
- Secure remote application path using IP and port-mapping
- Dynamic device-level customer authorization control using a Policy Manager
- Logging of EMC-requested actions at the customer site
- Access is restricted to authenticated and authorized EMC personnel

ESRS IP Control

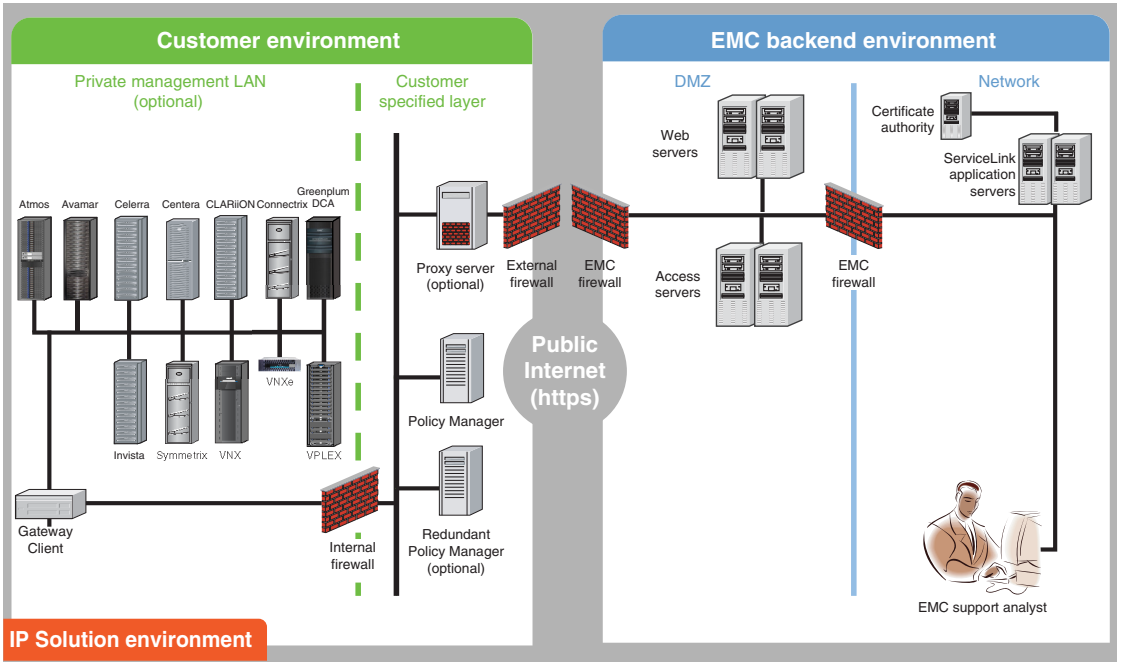
You control all EMC remote support access to the ESRS IP-managed products through the ESRS IP Client and its associated Policy Manager software. Connections with EMC storage devices and EMC at the ESRS IP-managed site originate from, and are managed, by the ESRS IP Client (or Clients) and the Policy Manager.

You set the policies of the ESRS IP Policy Manager, which controls ESRS IP remote access for support events. The Policy Manager can be set to accept, ask for approval of, or deny remote support connection requests.

At EMC, a distributed EMC enterprise suite is the processing core of ESRS IP. The EMC enterprise provides the mechanism for remote access activities from EMC Global Services.

Architecture

The ESRS IP application architecture is a secure, asynchronous messaging system designed to support the functions of secure encrypted file transfer, monitoring of device status, and remote execution of diagnostic activities. This distributed solution is designed to provide a scalable, fault-tolerant, and minimally intrusive extension to your system support environment. Figure 1 on page 6 illustrates the processing components and their interconnections.



GEN-001688

Figure 1 ESRS IP Solution architecture

Customer site components

ESRS IP requires the following components at the customer site:

- ESRS IP Client software residing on a dedicated server (two or more servers are preferred for high availability)
- ESRS IP Policy Manager software residing on a Policy Manager server

ESRS IP Client

The ESRS IP Gateway Client is the remote support solution application that is installed on a customer-supplied dedicated server, or servers.

The ESRS IP Clients function as communications brokers between the managed devices, the Policy Manager, and the EMC enterprise. All communication with EMC initiates from the ESRS IP Client on port 443 or 8443 outbound. The ESRS IP Clients are HTTP handlers. All messages are encoded using standard XML and SOAP application protocols. ESRS IP Client message types include:

- Device state heartbeat polling
- Data file transfer (connect homes)
- User authentication requests
- Device management synchronization

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

The ESRS IP Clients do not have their own user interface, and are run as Windows services. All ESRS IP Client actions are logged to a local runtime file.

Policy Manager

The Policy Manager enables you to set permissions for devices being managed by the ESRS IP Clients. The ESRS IP Client polls the Policy Manager, receives the current policies, and caches them locally. During the periodic poll, the ESRS IP Client posts all requests and actions that have occurred. These are then written to local log files and the Policy Manager database. When the ESRS IP Client retrieves a remote access request from the EMC enterprise, the access is controlled by the ESRS IP Client, which enforces the policy set by the Policy Manager.

The Policy Manager software may be on a standalone server (preferred method), on another application server (for example, a

Navisphere Management Station), or co-located on a non-high-availability Gateway Client server (recommended for test purposes only).

Proxy server

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

Table 1 on page 9 shows the minimum configuration of the required hardware and the application software that EMC provides.

Table 1 ESRS IP Client and Policy Manager specifications

Type	Requirements	EMC provided software	Notes
Gateway Client server	**Processor** — One or more processors, each 2.1 GHz or better. **Free Memory** — Minimum 1 GB of RAM, preferred 2 GB RAM.(If the Gateway Client and Policy Manager are on the same server, the minimum RAM is 3 GB.) **Network Interface Cards (NIC)** — Two 10/100 Ethernet adapters (NIC cards) are recommended (1 Gb preferred). You may choose to use a third NIC card for data backups. **Free Disk Space** — Minimum 1 GB available for installation. (A 40 GB or larger storage device is recommended.) **Microsoft .NET Framework** Version 2.0 with SP1 or greater. .NET Framework 3.5 and 4.0 are not compatible at this time. **Microsoft Visual C++ 2005 SP1 Runtime Library** **Operating Systems** — any of the following (U.S. English only): • Windows Server 2003 R1 or R2, 5.2, 32-bit, SP1 or SP2 • Windows Server 2003 R2, 5.2, 64-bit, SP1 or SP2 • 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	Gateway Client	The Gateway Client requires a site-supplied dedicated server. Two servers are required for a High Availability configuration. One Gateway Client server can support up to 250 devices.
Policy Manager server (optional)	**Processor** — One or more processors, each 2.1 GHz or better. **Free memory** — Minimum 2 GB of RAM. (If the Gateway Client and Policy Manager are on the same server, the minimum RAM is 3 GB.) **Network Interface Cards (NIC)** — Two 10/100 Ethernet adapters (NIC cards) are recommended (1 Gb preferred). You may choose to use a third NIC card for data backups. **Free Disk Space** — Minimum 2 GB available (preferably on a storage device of 80GB or larger) **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. **Operating Systems** — any of the following (U.S. English only): • Windows XP, SP2 or later • Windows Server 2003 • Windows Vista • Windows 7 • 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	Policy Manager	A Policy Manager is optional, but highly recommended. Policy Manager requires a site-supplied server. Policy Manager supports up to three Gateway Client servers or pairs. One Policy Manager server can support up to 750 devices.
Managed devices	**EMC information infrastructure products** — You must provide required networking (or VLAN) from the managed devices to the ESRS IP Client servers. See *EMC Secure Remote Support IP Solution Site Planning Guide*		

Communication to EMC

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

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

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

- Heartbeat polling
- Remote notification
- Remote access

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

Heartbeat polling

Heartbeat polling is described in the following sections:

- Heartbeat to EMC by the ESRS IP Client
- Heartbeat to EMC devices managed by the ESRS IP Client

Heartbeat to EMC by the ESRS IP Client

The Heartbeat is a regular communication, at a default interval of 30 seconds, from the ESRS IP Clients to the EMC enterprise. Each heartbeat contains a small datagram that identifies the ESRS IP Client and provides the EMC Support Center with status information on the health of the EMC storage devices and the ESRS IP Client.

EMC servers receive the data in XML format and acknowledge the receipt of data using SOAP (Simple Object Access Protocol) commands. The ESRS IP Client terminates the connection once it receives the acknowledgement response.

Figure 2 on page 11 provides an illustration of the heartbeat communication paths.

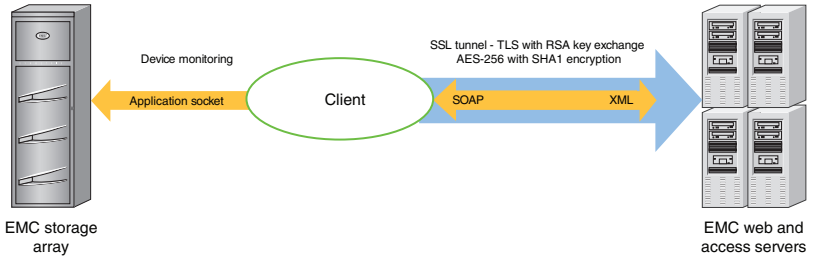


Figure 2 Heartbeat communication

Heartbeat to EMC devices managed by the ESRS IP Client

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

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

Remote notification (Connect Home)

The ESRS IP Clients serve as a conduits for EMC products to send remote notification event files to EMC. EMC hardware platforms use remote notification for several purposes. Errors, warning conditions, health reports, configuration data, and script execution statuses may be sent to EMC. Figure 3 on page 12 provides an illustration of the remote notification communication paths.

When an alert condition occurs, the storage system generates an event message file and passes it to the ConnectEMC service on the device to format the file and request a transfer to EMC. ConnectEMC uploads the file to the ESRS IP Client, where it is received by one of the following local listener services on the ESRS IP Client:

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

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

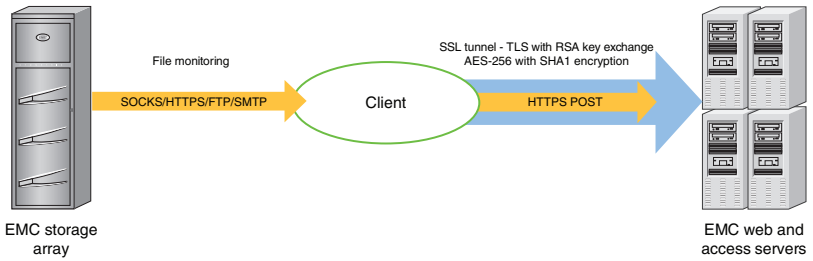


Figure 3 **Remote notification communication**

Remote access

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

After being properly authenticated at EMC, an EMC Global Services professional makes a request to access a managed device. The remote access session request includes a unique identifier for the user, the serial number of the managed device, the name of the remote application to be run on the managed device, and the service request number if available. The remote access request is queued at EMC until the ESRS IP Client that manages the device in question sends a heartbeat to EMC and retrieves the work request.

In response to the Heartbeat XML message, the EMC enterprise sends a special status in the SOAP response. This response contains the request information as well as the address of the Global Access Server and a unique session ID that the ESRS IP Client would use to connect. The ESRS IP Client uses its local repository to determine the local IP address of the managed device. It then checks with the Policy Manager to see if the connection is permitted. If the connection is permitted, the ESRS IP Client establishes a separate persistent SSL connection to the Global Access Server for the specific remote access session.

This secure session enables IP traffic from the EMC Global Services professional to be routed through the ESRS IP Client to the managed device. IP socket traffic received by the Global Access Server for this session is established, wrapped in a message, and sent to the ESRS IP Client. The ESRS IP Client unwraps the SOAP object and forwards

the traffic to the IP address and port of the end device for which the session was established. SOAP communication flows between the ESRS IP Client and the Global Access Server through this tunnel until it is terminated or times out after a period of inactivity. Figure 4 on page 13 provides an illustration of the remote access communication paths.

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

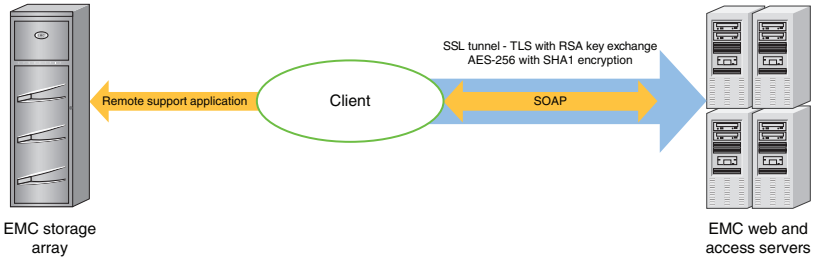


Figure 4 Remote access communication

Table 2 on page 13 shows the products that use the remote notification and remote access features of ESRS IP.

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

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

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

Product	Remote notification to EMC through ESRS IP	EMC remote access to device through ESRS IP
EMC DL3D	Device does not send Connect Homes through the ESRS IP Client	Yes
EMC DLm	Yes	Yes
EMC EDL	Yes	Yes
EMC Greenplum® Data Computing Appliance (DCA)	Yes	Yes
EMC Invista®	Yes	Yes
EMC RecoverPoint	Device does not send Connect Homes through the ESRS IP Client	Yes
Switch-Brocade-B	Yes[a]	Yes
Switch-Cisco	Yes[b]	Yes
EMC Symmetrix®	Yes	Yes
EMC VNX®	Yes	Yes
EMC VNXe®	Yes	Yes
EMC VPLEX™	Yes	Yes

a. By Connectrix Manager; ECC or approved third-party application.
b. By Cisco Fabric Manager; ECC or approved third-party application.

Configuration

This section provides details on the configurations of ESRS IP.

Server Client configuration

ESRS IP Client servers can be implemented in one of several configurations to meet your network and security requirements. See Figure 1 on page 6 for a sample configuration.

EMC recommends that the operating systems of your ESRS IP Client and Policy Manager servers be hardened before installing the ESRS IP Client and Policy Manager software. The preparation and hardening of servers is your responsibility.

There are no technical restrictions on the network location of the Gateway Client server. It must connect to your devices, to Policy Manager, and to the EMC enterprise. EMC strongly recommends that you use a firewall to block network ports not required by ESRS IP.

VMware support

ESRS IP is qualified to run on a VMware virtual machine. VMware support enables customers to leverage their existing VMware infrastructure to benefit from the security features of ESRS IP without adding hardware. VMware VMotion functionality also enables the Policy Manager, when installed in a virtual machine, to be moved from one physical server to another with no impact to remote support.

Note: The ESRS IP client cannot be moved withVMware VMotion due to RSA Lockbox restrictions.

The minimum requirements for VMware support are as follows:

- VMware ESX 2.5.2 or later
- 15 GB partition
- 2.2 GHz virtual CPU
- 512 MB memory allocated minimum (1 GB recommended, 2-3 GB preferred
- SMB modules optional

If you are run ESRS IP on a VMware virtual machine:

- When running Peered HA Gateway Client servers on VMWare, each client must be located on different physical hardware.
- Do not place VMware images or storage files on EMC devices managed by ESRS IP.
- Installation and configuration of the VM instance and operating system are the customer's responsibility.

High Availability Gateway Cluster configuration

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

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

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

Synchronization of Gateway Client clusters

Gateway Client server device management is synchronized by the EMC enterprise servers during polling cycles so that changes to the configuration on one Gateway Client in the cluster are automatically propagated to the other. When there is an addition, removal, or edit of a device on the managed devices list for any Gateway Client in a High Availability Gateway Cluster configuration, the EMC enterprise sends a synchronization message to all clustered Gateway clients.

When the other Gateway Client(s) in the cluster receives the device management transaction information, it updates its list of managed devices. If that Gateway Client is not currently available during a synchronization attempt, the EMC enterprise queues the transaction. Synchronization of the Gateway Cluster occurs upon the next successful poll message received from the previously unavailable Gateway Client.

Installing a High Availability Gateway Cluster

To implement a High Availability Gateway Cluster configuration, your EMC Global Services professional will create the cluster relationship from within the EMC enterprise.

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

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

Note: The first Gateway Client used to create a High Availability Gateway Cluster may have managed devices. Any additional Gateway Clients enrolled in a High Availability Gateway Cluster must not be managing devices at the time of enrollment. An error message will result if the additional Gateway Clients are managing devices. The managed devices must be unmanaged before they can be enrolled.

Configuration Tool

The Configuration Tool is an ESRS IP Client-based Graphical User Interface (GUI) application that is used to perform the following tasks:

- Configure and manage the ESRS IP Clients and Policy Manager
- Identify EMC storage devices and switches to be managed by the ESRS IP Client.

Note: The term *manage* means that a device is monitored and can use the ESRS IP Client to establish remote access connections. Connect home capability through the Gateway Client is configured at the device and should be in place (if applicable) before the Configuration Tool is used to make device deployment requests. Failure to do so may result in missed callhomes unless and alternate method is used for callhome.

The following list describes the configuration menu items available through tabs in the Configuration Tool. Note that these pages do refresh dynamically every 30 minutes —you must manually refresh the page for more frequent updates:

- Status tab — Displays status information about the connection between the ESRS IP Client and EMC, including connectivity status, proxy server enabled; Policy Manager enablement, connectivity status, and type; and other application statuses.

- Managed Devices tab — Enables viewing of managed devices. Enables entry of requests to add new devices, make changes to managed devices, and remove currently managed devices.

  Note: Customers may use the Configuration Tool to make requests to add, edit, or remove a device. However, approval within the EMC enterprise by an EMC Global Services professional is required before these changes will take place. Please ensure that the appropriate communication occurs with your EMC representative.

- Proxy Servers tab — Provides the ability to enable or disable a proxy between an ESRS IP Client and the EMC enterprise. *You should only change these values if requested by EMC support personnel.*
- Policy Manager tab — Provides the ability to enable or disable communication between a Policy Manager and an ESRS IP Client.
- Services tab — Displays the state (running or disabled) and the startup type (automatic or manual) of the following services related to ESRS IP and Connect Homes:
  - IIS
  - FTP
  - SMTP
  - HTTP
  - Gateway
  - Watchdog
- Remote Sessions tab — Displays all active remote sessions to the ESRS IP Client and managed devices.
- Log tab — Displays the log file for the Configuration Tool activity.

Devices managed on an ESRS IP Gateway Client will automatically be deployed to all other Gateway Clients in a Cluster Event notifications are handled by the configuration of the end device and will use the ESRS IP Client for which it is configured, if a problem occurs with that Client, the end device fails over the notification to an alternate ESRS IP Client in the High Availability Gateway Cluster. Remote access session management is handled by the Gateway Client whose heartbeat first retrieves the access request.

Device management

The Configuration Tool enables you to request the addition or removal of a managed device.

Adding a device

To add a device, you must enter the following data in the Managed Devices tab of the Configuration Tool:

- Serial number
- Model (product type)
- IP address

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

Note: EMC Global Services personnel must verify with your network administrators that the IP address of the managed device is accessible from the ESRS IP Client. If Network Address Translation (NAT) is being used in the environment, the IP address used to deploy the device must be the NAT IP address, not the device's IP address. Let's say, for example, that the local IP address of a device is 192.168.0.100, and is only on your internal network. To continue the example, let's say that you are using NAT (or a NAT device) that maps the device IP (192.168.0.100) to IP 10.10.44.22 so that the device can be reached from within your DMZ. In this case, EMC must use the IP address of 10.10.44.22 to reach the device, and in the Configuration Tool the IP address field must be changed to 10.10.44.22.

Once the device deployment has been approved by the EMC enterprise and the synchronization process is complete, the Configuration Tool adds the matched device to the current managed device list and makes the device available for remote access. If the serial number or Party ID for a newly integrated device does not match the EMC Global Services registered device lists for your site, the Configuration Tool records the device status as *pending*.

Changing a device's IP address

You can use the Configuration Tool to request a change to a device's IP address. Your request will be sent to the EMC enterprise for approval by an authorized EMC Global Services professional.

Unmanaging a device

If you want to unmanage a device, you can use the Configuration Tool to request the device's removal from the list of managed devices. Your request will be sent to the EMC enterprise for approval by an EMC Global Services professional. When approved, the serial number of the device will be disassociated from your ESRS IP Client.

Gateway Extract Utility

To configure a device for management by a ESRS IP Client, the EMC Global Services professional on site must know the following for each managed device: serial number, product type, and an IP address that the ESRS IP Client can use to communicate with the device. The Gateway Extract Utility (**GWExt**), when run on the EMC device, can be used to automate the collection of this information and transport it to the ESRS IP Client. EMC supplies the **GWExt** utility with the ESRS IP Client installer.

Your EMC Global Services professional copies the **GWExt** utility from the ESRS IP Client server to the managed device.

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

Certain products qualified for ESRS IP have a **GWExt** information file installed at time of production. This information file contains product information that the **GWExt** utility gathers and submits to the ESRS IP Client for device registration, automating a large portion of the process.

Security features

This section details the security features of ESRS IP.

Policy Manager

Using the Policy Manager, you control the authorization requirements for remote access connections, diagnostic script executions, and other ESRS IP Client-related activities, as shown in Figure 5 on page 21. The Policy Manager enables you to set access permissions for devices being managed by the ESRS IP Clients. The ESRS IP Client regularly polls Policy Manager for changes to the permissions and caches the permissions locally on the ESRS IP Client. All requests and actions are recorded in the Policy Manager database and local audit log files. When a request for remote access or any other action arrives at the ESRS IP Client enforces the policy received from the Policy Manager.

Policy Manager permissions can be assigned in a hierarchical system, establishing policies based on model and product groups. If required, you can override group-level permissions down to the individual device level.

The Policy Manager provides three options for assigning policy manager rule permissions for every action that the ESRS IP Client can perform on a device or group of devices:

- Always Allow — You always allow the action.
- Never Allow — You always deny the action.
- Ask for Approval — You must approve the request by providing authorization.

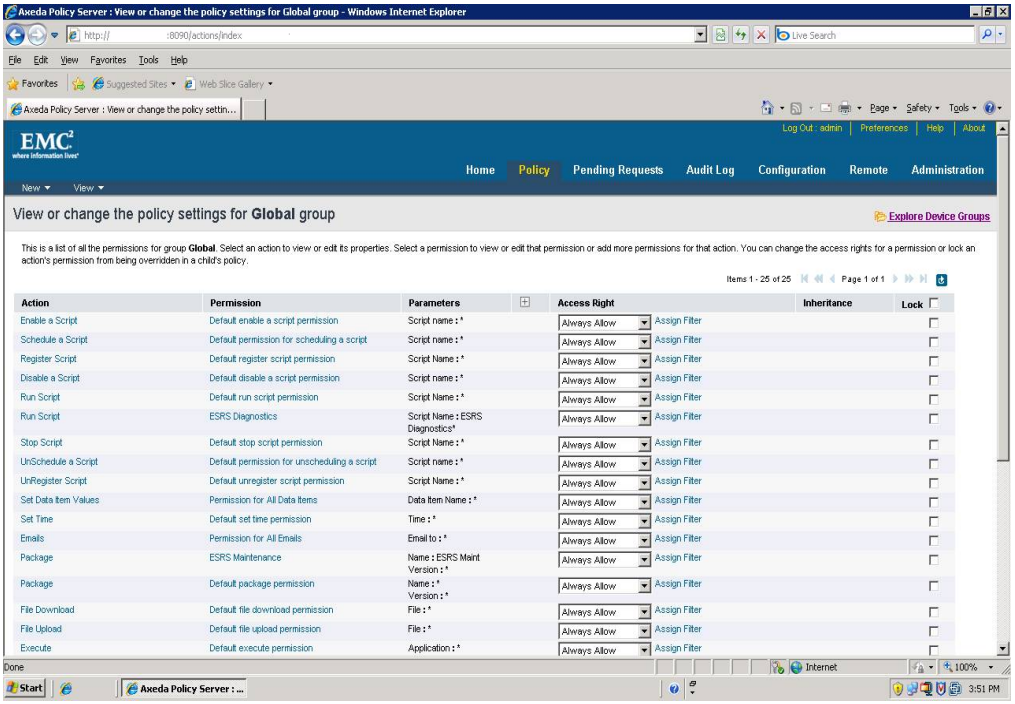


Figure 5 Policy Management settings

When you set an authorization rule to Ask for Approval, the Policy Manager sends an e-mail message to your designated address upon each action request, per transaction. This e-mail message contains the action request itself and the user ID of the EMC Global Services representative.

The e-mail message requests your permission to perform the action. You use the Policy Manager interface to accept or deny the requested action. You also have the option of creating filters to set further restrictions on authorization and actions.

As with ESRS IP Client and EMC enterprise communication behavior, the Policy Manager only responds to requests from the ESRS IP Client. Since the ESRS IP Client caches the Policy Manager's permission rules at startup, the ESRS IP Client must poll the Policy Manager for configuration updates. In this way, the ESRS IP Client captures any change to the Policy Manager rule set after its last polling cycle. Like the ESRS IP Client, the Policy Manager is an HTTP listener, which must be configured to receive messages on an agreed-upon port. The default port is 8090, but if necessary, you can specify a different port during your Policy Manager installation. For HTTPS access to the Policy Manager, you must use port 8443 and cannot change it.

Customers have the option of installing a second Policy Manager application on a separate server, allowing a redundant management system. Failover is manual.

The Policy Manager uses the Apache Tomcat engine and a 100 percent compliant local JDBC relational database to provide a secure web-based user interface for permission management.

Logging

The Policy Manager records all remote support events, remote access connections, diagnostic script executions, and support file transfer operations are stored in the Policy Manager database and flat text audit log files. The Policy Manager also audits access to the Policy Manager, policy changes, all authorization or denial of access activity. The audits are viewed through the Policy Manager interface and cannot be edited. The audits are also streamed to local flat text files which can be read w/ any text editor and are not tamper proof. Audit logs can also be configured to stream to a syslog server in your environment. See Figure 6 on page 23 for a Policy Manager interface example.

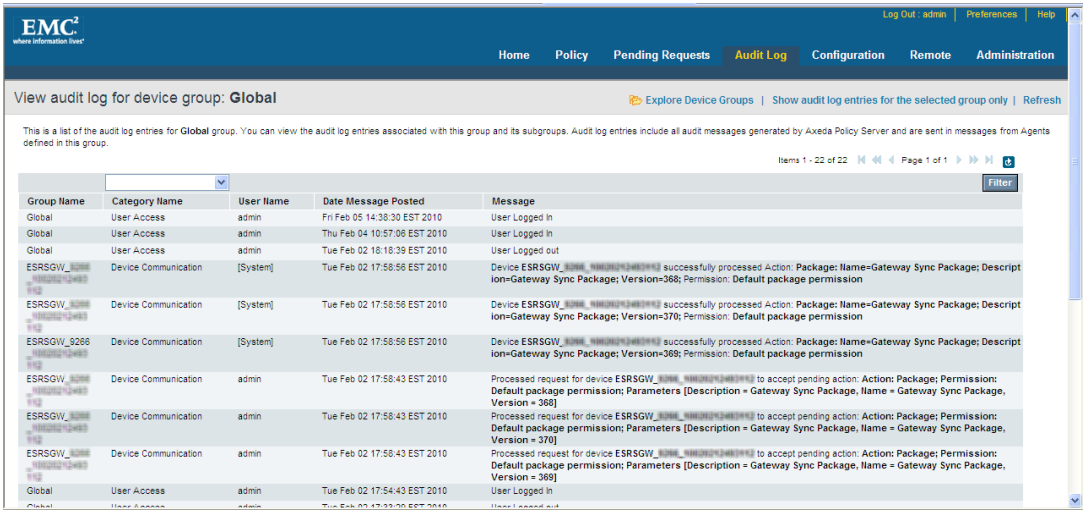


Figure 6 **Audit log example**

Device control

ESRS IP proactively monitors, alerts, and notifies EMC Global Services when the ESRS IP Client or any managed device fails to regularly communicate back to EMC. EMC alerts you of potential failures or issues that may affect EMC's ability to provide timely support. As an EMC customer, you are in complete control over which devices are included in your ESRS IP Client device management system, and you can phase them in by product line. EMC provides applications to help you automate the addition of new devices for management by the ESRS IP Client. All device management operations are logged and must be performed from the EMC enterprise by authorized EMC Global Services professionals.

Digital Certificate Management

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

Digital Certificate Management automates ESRS IP Client digital certificate enrollment by taking advantage of EMC's existing network

authentication systems, which use the RSA SecurID Authenticator and the EMC local certificate authority (CA). Working with EMC systems and data sources, Digital Certificate Management aids in programmatically generating and authenticating each certificate request, as well as issuing and installing each certificate on the ESRS IP Client.

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

Before the certificate authority issues a certificate for the ESRS IP Client, it requires full authentication of a certificate requester by verifying that the EMC Global Services professional making the request is Properly authenticated using the EMC RSA SecurID, and belongs to an EMC Global Services group that is permitted to request a certificate for the customer site. The certificate authority then verifies that the information contained in the certificate request is accurate generates the Certificate and returns the certificate to the requestor. The process is as follows:

The EMC Global Services professional requests a certificate by first authenticating himself or herself using an EMC-issued RSA SecurID Authenticator. Once authentication is complete, the ESRS IP Client installation program gathers all the information required for requesting certificates and generates a certificate request, a private key, and a random password for the private key. The ESRS IP Client installation program then writes the certificate request information to a request file, ensuring accuracy and completeness of the information.

The installation program then submits the request over an SSL tunnel. After the certificate is issued and returned over the SSL tunnel the installation program automatically installs the certificate on the ESRS IP Client.

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

Device access control

ESRS IP achieves remote application access to a process running on an EMC storage device by using a strict IP and application

port-mapping process. You have complete control over which ports and IP addresses are opened on your internal firewall to allow connectivity. The remote access session connections are initiated by an EMC Global Services request at the EMC Global Access Server and through a pull connection to the ESRS IP Client. EMC never initiates a connection to your ESRS IP Client or network. Your policies determine if and how a connection is established.

Device configuration access control

Once your devices are configured for ESRS IP management, you must ensure that the configuration of the managed devices are carefully controlled and monitored. For example, changing the configured IP address in ESRS IP or changing the IP address of the storage device disables the device's connect home capabilities and EMC's ability to perform remote service on that device. Each device modification is tracked in the Policy Manager and the EMC enterprise audit logs.

EMC enterprise access control

Several robust security features are incorporated into the EMC enterprise. To access the EMC enterprise, EMC Global Services professionals or authorized service providers must be logged into the EMC corporate network system or must connect using RSA SecurID two-factor authentication technology. Only authorized EMC personnel or authorized service providers can access the EMC enterprise.

Supported products

The products supported by ESRS IP are listed in Table 3 on page 26.

Table 3 Product and application releases supported by ESRS IP Clients (page 1 of 2)

Product	Environment/application releases
Atmos	Atmos 1.4 or later
Avamar	Avamar 6.0 or later
Celerra	NAS Code 5.4 or later
EMC Centera	CentraStar® 2.4 or later[a]
CLARiiON CX, CX3, CX4, and AX4-5 Series storage systems (distributed or Enterprise environments)	EMC FLARE® Operating Environment 2.19 or later EMC Navisphere® Manager 6.19 or later The AX-100/AX-150 are not supported as they do not support the required CLARalert. **Note:** The AX4-5 series are supported only if the Navisphere Full license (with CLARalert) is purchased and installed on the storage system.
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[b]
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[c]
Disk Library for mainframe (DLm)	DLm4020, DLm4080, release 1.2 and later
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
Greenplum Data Computing Appliance (DCA)	Greenplum 4.0
Invista	Invista 2.2 or later
RecoverPoint	RPA 3.1 and late r[a]
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 b d]
Cisco Switches	• MDS 9000 Family switches running SAN-OS 3.3(2) or later and NX-OS 4.1(1b) or later[a] • Nexus 5000 Family switches running NX-OS 4.1(3)N1(1) or later[e]

Table 3 Product and application releases supported by ESRS IP Clients (page 2 of 2)

Product	Environment/application releases
Symmetrix 8000 Series	EMC Enginuity™ 5567 and 5568, with Service Processor Part Number [f] 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
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
VNXe	VNXe 2.0.x
VPLEX	GeoSynchrony 4.0.0.00.00.11 or later

a. For remote support access only, not for connect home through ESRS IP.
b. CM does not support FOS 6.3.x or higher. CMDCE is required. Please refer to the appropriate FOS Release Notes.
c. CMDCE is required to support FOS 6.3x or higher. Please refer to the appropriate FOS Release Notes.
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. For remote access only. Connect home is not supported at this time.
f. These part numbers designate Service Processor running Windows NT SP6.

Port requirements

The open port requirements for each product are listed in Table 4 on page 28.

Table 4 Open port requirements for site network and device configuration (page 1 of 2)

EMC product	Open port requirements	
ESRS IP components	**Outbound**	**Inbound**
Gateway Client server	• TCP 8090 (HTTP) and/or 8443 (HTTPS) (to Policy Manager) • Device dependent ports (to devices) • TCP 443 (to EMC enterprise) • TCP 443 (HTTPS) and/or 8443 (SSL) to EMC Remote Support	HTTPS, Passive FTP, and SMTP (from managed devices)
Policy Manager	SMTP (to e-mail server)	TCP 8090 (HTTP) and/or 8443 (HTTPS) (from Gateway Client server)
Managed storage devices	**Outbound to Gateway Client server (Service notification)**	**Inbound from Gateway Client server (Remote support)**
Atmos	HTTPS, Passive FTP, SMTP	TCP 22, 80, 443
Avamar	HTTPS, Passive FTP, SMTP	TCP 22, 80, 443
Celerra	HTTPS, Passive FTP, SMTP	TCP 22, 23, 80, 443, and 8000
EMC Centera	SMTP	TCP 22, 3218, and 3682
CLARiiON	HTTPS, Passive FTP, SMTP	TCP 80 and 443 (or 2162 and 2163), 5414, 6389-6392, 9519, 13456, and 60020
Connectrix	HTTPS, Passive FTP, SMTP	TCP 5414
DL3D	SMTP	TCP 22, 443
Disk Library for mainframe (DLm)	HTTPS, Passive FTP, SMTP	TCP 22, 80, 443, 8000
EDL	HTTPS, Passive FTP, SMTP	TCP 22, 11576
GreenplumData Computing Appliance (DCA)	HTTPS, Passive FTP, SMTP	TCP 22
Invista	(Element Manager) HTTPS, Passive FTP, SMTP	(CPCs) TCP 80, 443, 2162, 2163, 5201, 5414

Table 4 Open port requirements for site network and device configuration (page 2 of 2)

EMC product	Open port requirements	
RecoverPoint	SMTP	TCP 22
Switch - Brocade-B	N/A	TCP 22 and 23
Switch - Cisco	SMTP	TCP 22 and 23
Symmetrix	HTTPS, Passive FTP, SMTP	TCP 1300, 1400, 4444, 5414, 5555, 7000, 9519, 23003-23005
VNX	HTTPS, Passive FTP, SMTP	TCP 22,80, 443, 2162, 2163, 6391, 6392, 8000,9519,13456,60020
VNXe	HTTPS, Passive FTP, SMTP	TCP 22, 80, 443
VPLEX	SMTP	TCP 22, 443

a. HTTPS available only if device is qualified to send files using HTTPS.
b. SMTP by customer e-mail server.
c. Passive FTP if in a centrally managed environment, by management server.
d. If in Distributed mode, by SMTP to the Gateway Client or customer e-mail server.

Summary

The EMC Secure Remote Support IP Solution (ESRS IP) provides increased security and functionality to the EMC Secure Remote Support portfolio.

Site architecture

You set up ESRS IP at your site, with the assistance of EMC Global Service professionals. ESRS IP has the following capabilities:

- **ESRS IP Client** — This SSL HTTPS handler is the broker that directs communication between your EMC-installed products and EMC Global Services, handling user authentication, service notification data file transfer, remote access session regulation, and device management—all the tasks required for remote support.
- **Configurations** —You can choose from a variety of configurations. If you choose a High Availability Gateway Cluster server configuration, you will use two or more Gateway Client servers to eliminate single point of failure and help ensure that your system is available for remote support of your EMC products.

- **Policy Manager** — This application lets you specify the access authorization criteria for remote access operations on each device or group of devices that you manage using ESRS IP.
- **Configuration Tool** — This application is used to configure the storage devices that are managed by the ESRS IP Client. The tool is installed as a component of the ESRS IP Client.

Security features

ESRS IP protects customer confidentiality and integrity through the industry-recognized "3 A" security practices—authentication, authorization, and audit logging—with full customer control over remote communications and policy management: All connections are initiated from your site:

- **Device Control** — Your EMC devices are protected with 24 x 7 heartbeat monitoring and rapid alert response to system events.
- **Policy Management** — You can specify authorization rules within a wide range of possible configurations and behaviors.
- **Digital Certificate Management** — Digital Certificate Management automates ESRS IP Client digital certificate enrollment by taking advantage of EMC's existing authentication system.
- **Access Control** — You have complete control over the configuration and management of EMC's strict IP and port-mapping secure connection solution. EMC Global Services professionals are granted access to your system only under your approval, in addition to their required authorization using EMC's strict centralized access controls.

Glossary

authenticate Confirm or deny the identity of a system user candidate.

authorize Confirm or deny the level of access or editing privileges for a system user.

Client The ESRS IP remote support solution application that acts as the single point of entry and exit for all IP-based EMC remote support activity.

demilitarized zone (DMZ) A computer or subnetwork that sits between a trusted internal network, such as a corporate private Local Area Network (LAN), and an untrusted external network, such as the public Internet.

device See managed device.

EMC enterprise The EMC ESRS IP back-end infrastructure, which includes a Graphical User Interface used by authorized EMC Global Services professionals.

event An error or otherwise notable activity reported from the managed device.

managed device An EMC information infrastructure product (such as Celerra, EMC Centera, CLARiiON, Symmetrix) installed at a customer site and "managed" by an ESRS IP Client as part of an ESRS IP Solution.

Network Address Translation (NAT) An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

RSA RSA, the Security Division of EMC, makers of security servers and SecurID Authenticators used in ESRS IP authentication procedures.

References

Security Protection in EMC Remote Support Services: *Current Solutions*. EMC Corporation. September 2002.

Additional EMC documentation is available from the EMC Powerlink® website:

http://Powerlink.EMC.com