

**EMC<sup>®</sup> Secure Remote Support Gateway**

Release 1.04

**Technical Description**

P/N 300-010-254

Rev A01

November 10, 2009

---

This technical description contains information on these topics:

◆ Introduction.....	2
◆ Gateway solution description.....	3
◆ Installation and configuration .....	5
◆ Security features of the Gateway solution .....	18
◆ Supported products and ports requirements .....	23
◆ Summary.....	25
◆ Glossary .....	26
◆ References .....	26

---

## Introduction

EMC® maintains a strong and highly visible 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 Gateway (ESRS) provides a secure, IP-based, distributed remote service support solution giving you command, control, and visibility of remote support access.

The Gateway solution expands and improves the EMC Secure Remote Support portfolio with these features:

- ◆ Consolidation — The Gateway solution 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 — The Gateway solution 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. Security features include:
  - Comprehensive digital security — Gateway security includes SSL (Secure Sockets Layer) data encryption, entity authentication (private digital certificates), and remote access user authentication verified through EMC network security.
  - Authorization controls — Policy controls allow 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 — Gateway establishes remote sessions using secure IP and application fixed and dynamic port assignment between source and target endpoints.
  - Auditing support — The Gateway Policy Manager logs all remote access connection, 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.

---

## Gateway solution description

This section includes a detailed description of the Gateway solution.

---

### Remote support rationale

The EMC remote support strategy delivers immediate response to product event reports such as error alerts to maximize your information infrastructure availability. When a support event occurs, EMC provides rapid remote support through two phases: first, through automated recognition and notification from your site (or from EMC, in the case of connectivity loss) to EMC, and second, through interpretation and response from EMC, in many cases pre-empting on-site service. This immediate and interactive remote support provides:

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

The Gateway solution augments the EMC secure remote support portfolio. In addition to the Gateway, this portfolio includes phone-based modems, WebEx, and email.

---

### Gateway security

The Gateway solution design acknowledges that the heart of any well-designed distributed system is security, and thus it incorporates the industry-recognized "3 A's": authentication, authorization and audit logging. The Gateway employs multiple security layers to ensure that you and EMC can use the system with confidence. From an applications architecture perspective, the Gateway is an asynchronous messaging system in which all communications are initiated from your site. All communications between the Gateway server and the EMC enterprise servers use the HTTPS protocol with end-to-end SSL tunneling with strong encryption.

Gateway uses a firewall-friendly, IP-based communication technology over SSL VPN gateway tunnels. Customer-controlled Gateway servers 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 a Gateway server at your site. Using industry standard SSL encryption over the Internet, and EMC-signed digital certificate authentication, your administrators need only enable outbound communication over SSL default port 443.

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

Gateway is comprised of 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.

Security features used in Gateway are as follows:

- ◆ TLS v1.0 tunneling with 3DES 168-bit data encryption
- ◆ Authenticated Gateway server digital certificate registration
- ◆ X.509 digital certificates generated
- ◆ Client authentication based on digital certificate at EMC
- ◆ EMC-issued RSA SecurID Authenticators register digital certificates
- ◆ Secure remote application path using IP and port-mapping
- ◆ Dynamic device-level customer authorization control using a Policy Manager
- ◆ EMC-issued SecurID for installation user authentication
- ◆ Logging of EMC-requested actions at customer site
- ◆ Access restricted to authenticated and authorized EMC personnel

---

## Gateway control

You control all EMC remote support access to the Gateway-managed products through the Gateway server and its associated Policy Manager software. Connections with EMC storage devices and EMC at the Gateway-managed site originate from, and are managed by, that site's Gateway servers and its Policy Manager.

The Policy Manager policies set by you control remote access via the Gateway for support events. The Policy Manager can be set to accept, ask for approval, or reject remote support connection requests.

At the processing core of the Gateway solution is a distributed Device Relationship Management enterprise suite which provides the mechanism for remote access activities from EMC Global Services.

---

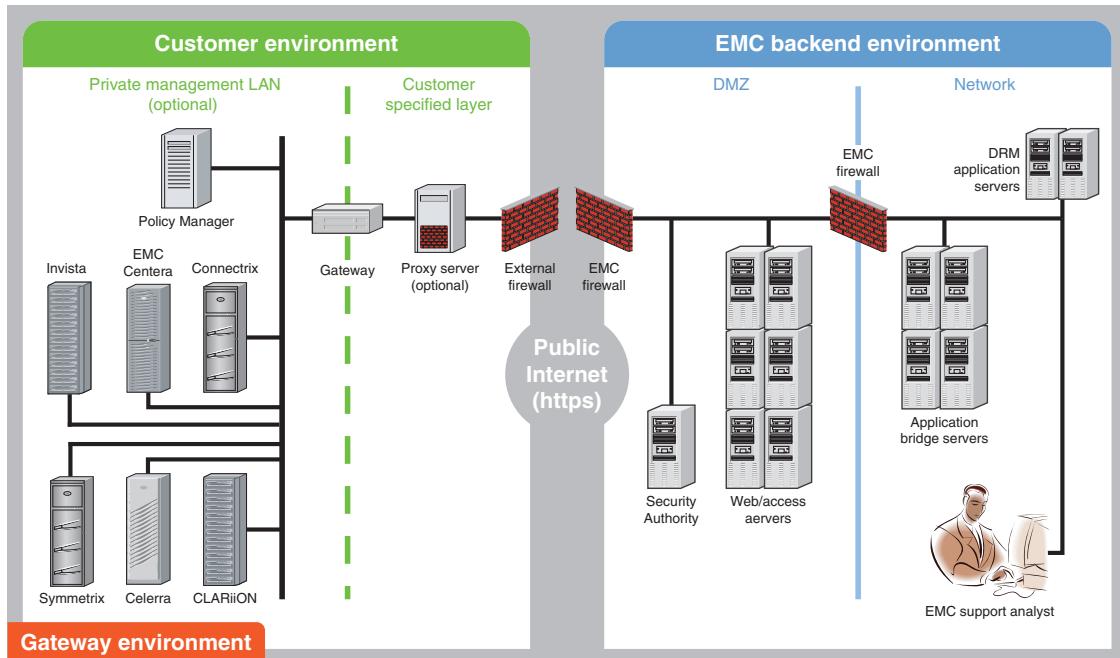
## Installation and configuration

This section provides details on architecture, installation, and configuration of the Gateway solution.

---

## Site architecture

The Gateway solution's application architecture consists of a secure, asynchronous messaging system designed to support the functions of secure encrypted file transfer, monitoring of device status, and remote execution of diagnostic activities. This distributed solution is designed to provide a scalable, fault-tolerant, and minimally intrusive extension to the customer's system support environment. [Figure 1 on page 6](#) provides a schematic display of the processing nodes and their interconnections.



GEN-000818

**Figure 1 Gateway solution schematic architecture**

The Gateway solution requires:

- ◆ A server for the Gateway software (two servers preferred for high availability)
- ◆ A server for the Policy Manager software

The Policy Manager software may be co-located on a non-high-availability Gateway server or on another application server (for example, a Navisphere Management station).

The customer manages administration and access to these servers and applications. The preferred configuration is to use two Gateway servers to create the high-availability (HA) configuration. Each Gateway pair is capable of handling 200 devices. One Policy Manager server can support up to three fully utilized Gateway server pairs.

**Note:** Once installed on your server, the Policy Manager application is inaccessible by third parties, including EMC.

Table 1 on page 7 indicates the minimum configuration of the required hardware and the application software EMC provides.

**Table 1 Gateway and Policy Manager server specifications**

Type	Requirements	EMC provided software	Notes
Gateway server	Processor—One or more processors, each 2.1 GHz or better. Memory - 512 MB RAM or more. (1 GB or more is recommended.) Comm - Two (dual) 10/100 Ethernet adapters (NIC cards). (1 GB preferred. You may prefer to use a third NIC card for data backups.) Storage - 500 MB available. (40 GB or larger storage device is recommended.) OS - Microsoft Windows Server 2003, SP1 or SP2. (32-bit or 64-bit).	Gateway server agent	Site-supplied server: Qty: Two required for HA configuration. Dedicated server required. Supports up to 200 devices.
Policy Manager server (optional)	Processor—One or more processors, each 750 MHz or better. Memory - 512 MB RAM or more. (1 GB is recommended.) Comm - 10/100 Ethernet adapter (NIC card). (1 GB preferred. You may prefer to use a second NIC card for data backups.) Storage - 1 GB available. (80 GB or larger storage device is recommended.) OS - Microsoft Windows Server 2003, SP1 or SP2. (32-bit or 64-bit).	Policy Manager	Optional, but strongly recommended. Site-supplied server. Supports up to three Gateway servers or pairs. (600 devices total)
Target devices	EMC information infrastructure products See <i>EMC Secure Remote Support Site Planning Guide</i>		You must provide required networking (or VLAN) from the target devices to the Gateway servers.

## Gateway server agent

The Gateway server agent is an HTTP handler. The agent functions as the communications broker between the Gateway-managed devices, the Policy Manager, and the EMC Device Relationship Manager (DRM). All messages are encoded using standard XML and SOAP application protocols. Agent message types include:

- ◆ Device state heartbeat polling
- ◆ Data file transfer
- ◆ Remote access session initiation
- ◆ User authentication requests
- ◆ Device management synchronization

The Gateway agent acts as a proxy, carrying information to and from the Gateway-managed devices. To maximize remote support

availability, EMC configures all Gateway agents to employ built-in failover to redundant EMC remote-support enterprise systems in the event that access to the primary site is unavailable. The Gateway agent can also queue session requests in the event of a temporary local network failure.

Network traffic can be configured to route from the Gateway through proxy servers to the Internet. Such configurations include support for auto-configuration, HTTP, and SOCKS proxy standards. The agent does not have its own user interface, and is run as a Windows service. All agent actions are logged to a local runtime file.

---

## Gateway to EMC communication

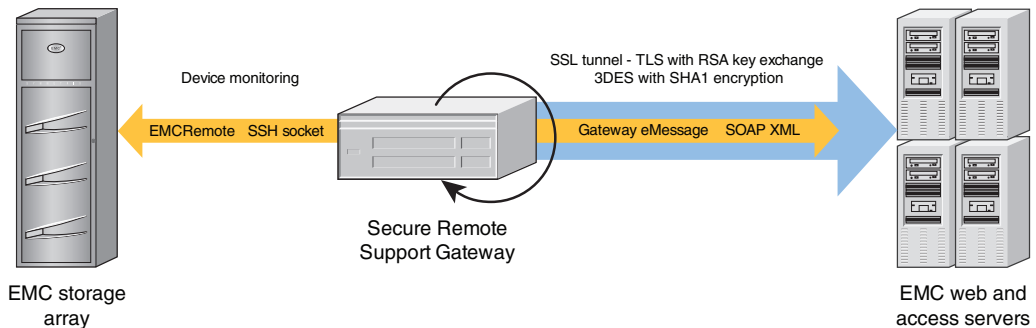
All communication between the customer's site and EMC is initiated at the customer's site by the Gateway server agent. Using industry standard SSL encryption over the Internet and EMC-signed digital certificate authentication, the Gateway creates a communication tunnel.

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

The Secure Remote Support Gateway uses the SSL tunnel to EMC to perform three different functions: Heartbeat polling, remote notification and remote access. Each relies on the SSL tunnel, but communication processes and protocols within the tunnel vary by function. Each is discussed in the following sections.

### Heartbeat polling

The Heartbeat is a regular communication, at 30-second intervals, from the Gateway to the EMC DRM. The heartbeat contains a small datagram that identifies the Gateway server and provides the EMC Support Center with status information on the health of the EMC storage devices and the Gateway server. EMC servers receive the data in XML format and respond using SOAP (the Simple Object Access Protocol) commands. Once this response is received, the Gateway terminates the connection. [Figure 2 on page 9](#) provides an illustration of the heartbeat communication paths.



GEN-000826

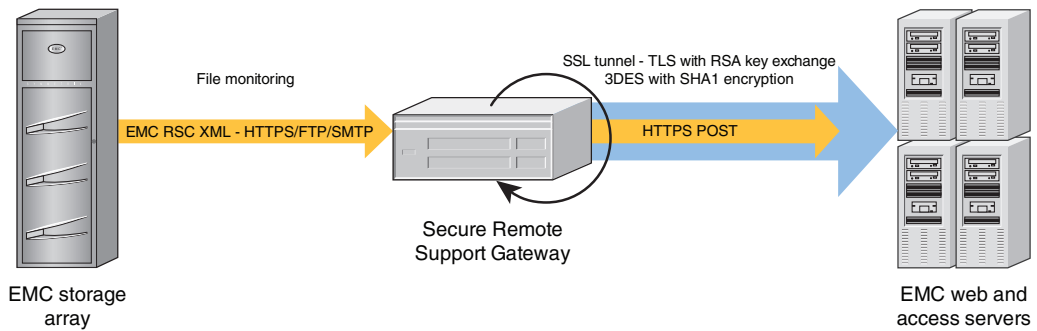
**Figure 2** Heartbeat communication

Once every 15 minutes the Gateway determines if each managed device is available for service by making a socket connection to the device and verifying that the service applications are responding. The information is recorded by the Gateway. If a change in status is detected, the Gateway notifies EMC over the next heartbeat. The heartbeat is a continuous service and EMC monitors the values sent and may automatically trigger service requests if a Gateway fails to send heartbeats or if the values contained in a heartbeat exceed certain limits.

### Remote notification

The Gateway also serves as a conduit for EMC products to send remote notification event files to EMC. EMC hardware platforms use remote notification for several different purposes. Errors, warning conditions, health reports, configuration data, and script execution statuses may be sent to EMC. [Figure 3 on page 10](#) 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 (or other services) on the devices to format the files and request a transfer to EMC. ConnectEMC uploads the file to the Secure Remote Support Gateway where it is received by one of three local transport protocols: HTTPS (if a device is qualified to send files using HTTPS), FTP, or SMTP. When an event file is received from a device, the Gateway compresses the file, opens the SSL tunnel to the EMC servers, and posts the data file to EMC. At EMC, the file is decompressed and forwarded to our DRM systems.



GEN-000828

**Figure 3 Remote notification communication**

Some EMC products take advantage of only the remote notification features of the Gateway. These products include:

- ◆ EMC ControlCenter<sup>®</sup>
- ◆ EMC OpenScale<sup>®</sup>

On the other hand, some products do not use the remote notification features of the Gateway, but do take advantage of the Gateway remote access features. These products send event files directly to EMC and include:

- ◆ EMC Centera<sup>®</sup>
- ◆ Cisco switches
- ◆ EMC RecoverPoint

Some products, depending on configuration, can send event files either through the Gateway or directly to EMC and include:

- ◆ EMC Celerra<sup>®</sup>
- ◆ EMC CLARiiON<sup>®</sup>
- ◆ EMC DLm
- ◆ EMC EDL

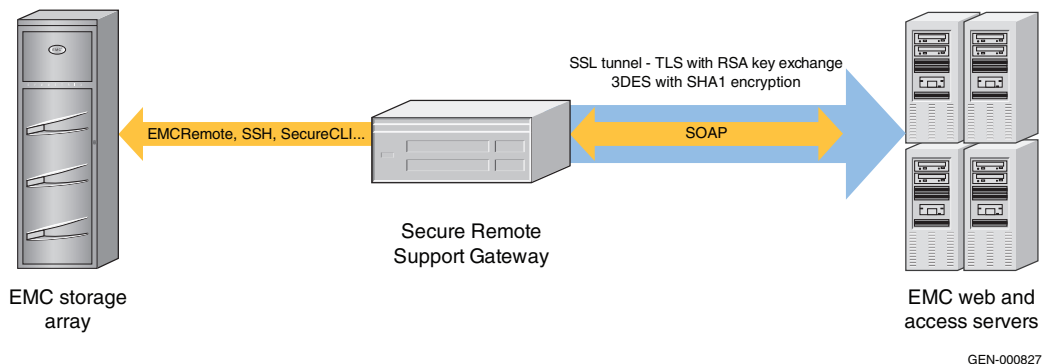
Brocade-B switches use just the Gateway remote access features and do not use a remote notification method.

### Remote access

To establish a remote access session, the Secure Remote Support Gateway uses asynchronous messaging to ensure that all communication is initiated from the customer's site. After being properly authenticated at EMC, a support professional makes a request to access a Gateway-managed device. The remote access session request includes a unique identifier for the user, the serial

number of the target device, and the remote application he or she wants to run on that device and may include the Service Request number. This request is queued at EMC until the Gateway that manages the device in question heartbeats home.

In response to the Heartbeat message, the EMC DRM sends a special status in the SOAP response. This response contains the request information as well as an address and an access server session to which the Gateway would connect. The Gateway uses its local repository to determine the local IP address of the end device, checks with the Policy Manager to see if the connection is permitted, and if approved, establishes a separate SSL connection to the access servers for the specific remote access session. This secure session allows IP traffic from the EMC internal service person to be routed through the Gateway to the end device. IP socket traffic received by the access server for this session is established, wrapped in a SOAP message, and sent to the Gateway. The Gateway un-wraps the SOAP object and forwards the traffic to the IP address of the end device for which the session was established. SOAP communication flows between the Gateway and the access server through this tunnel until it is terminated or times out after a period of inactivity. [Figure 4 on page 11](#) provides an illustration of the remote access communication paths.



**Figure 4 Remote access communication**

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

---

## Gateway server configuration

EMC recommends that your Gateway and Policy Manager servers be OS hardened prior to installation. The preparation and hardening of servers is your responsibility.

A Gateway server 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.

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

## VMware support

Secure Remote Support Gateway is qualified to run in a VMware virtual machine. VMware support allows customers to leverage their existing VMware infrastructure to benefit from the security features of the Gateway 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.

The following are the minimum requirements for VMware support:

- ◆ VMware ESX 2.5.2 or later
- ◆ 15 GB partition
- ◆ 2.2 GHz virtual CPU
- ◆ 512 MB memory allocated
- ◆ SMB modules optional
- ◆ VMotion functionality optional

---

**Note:** When running Peered HA Gateways on VMware, each Gateway must be located on different physical hardware.

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

---

## High-availability Gateway configuration

To enable maximum remote access availability, EMC recommends that you eliminate single point of failure by deploying a high-availability Gateway configuration which employs two Gateway servers.

Gateway servers in this configuration are active peers that manage the same set of devices without awareness of or contention with the other. There is no direct communication between the peer nodes. In the high-availability configuration the Policy Manager software cannot be co-located on a Gateway server and must be installed on a separate server. Gateway high-availability configurations are limited to two active nodes.

### Synchronization of Gateway peers

Gateway server device management is synchronized via the EMC enterprise servers during polling cycles so that changes to the configuration on one peer are automatically propagated to the other peer. When you add, remove, or edit devices on the managed devices list for either Gateway server in a high-availability configuration, the Deployment Utility sends a message through the Gateway agent to the DRM. The EMC DRM application looks up the serial number of the peer node and creates a transaction for the device information to be relayed to the peer node upon receipt of the next polling message. When the peer Gateway server receives the device management transaction information, it updates its Gateway agent's list of managed devices. If the peer Gateway server is currently not available during a synchronization attempt, the DRM application queues the transaction, and synchronization of the peers occurs upon the next successful poll message received from the previously unavailable Gateway server.

### High-availability installation

During your Gateway server installation, your EMC Global Services representative assigns a system name to the servers in the Gateway peer server pair. During the installation of the first Gateway server in the configuration (temporarily called the primary server), the Gateway installation program automatically assigns a base system name. This system name acts as the identification handle for all of the Gateway servers installed at your site.

This is the generic syntax of a generated base system name:

```
ESRS_SiteID_SiteName
```

For example:

```
ESRS_12345_ExampleCo
```

Since you may have multiple Gateway high-availability server pairs or Single Gateway HA-ready servers per site, your EMC Global Services representative uses an additional string value that uniquely identifies the high-availability pairs currently being installed. This string value becomes the subsystem name. In the previous example,

if you have one pair for managing only EMC Symmetrix® devices, and one pair for managing the heterogeneous storage arrays used to support manufacturing applications, the EMC® Global Services representative may use product-based subsystem names to uniquely identify each high-availability pair:

```
ESRS_12345_ExampleCo_Symm  
ESRS_12345_ExampleCo_Mfg
```

During the installation of the second Gateway server (temporarily called the secondary server), and during recovery from a hardware failure that requires re-installation of the Gateway application, the installation program provides a drop-down list of all the subsystem names at your site. Your EMC Global Services representative then selects the appropriate subsystem name previously assigned during the primary server installation. The installation program registers this information in the Gateway system's DRM database at EMC.

Once the two Gateway servers are synchronized by the DRM, they are peers and there is no longer a primary or secondary server.

## Deployment Utility

The Deployment Utility is a client-based application that is used to configure and manage the Gateway and identify EMC storage devices and switches. The term manage means that a device is monitored and can use the Gateway system to establish remote access connections. The Gateway agent proxies all Deployment Utility requests to the EMC DRM. The Gateway agent is the only application with which the utility communicates. The Gateway installation program automatically installs the Deployment Utility with the Gateway agent.

The Deployment Utility is a Java-based GUI application that authenticates with the Gateway agent upon startup. This secure protocol ensures that only the Deployment Utility can interface with the agent. Here is a listing of the configuration menu items available through the Deployment Utility:

- ◆ Base Configuration — Gateway model and serial number. The Gateway installation program automatically generates these values for you. *You should change these values only upon request from EMC Global Services.*
- ◆ EMC DRM Configuration — EMC primary and secondary DRM addresses, proxy server configuration, and SSL options. The Gateway installation program automatically generates these values and captures them. *You should change these values only upon request from EMC support personnel.*

- ◆ Policy Manager Configuration — DNS/IP address of Policy Manager server. The Gateway installation program automatically captures these values. *You should change these values only upon request from EMC support personnel.*
- ◆ Customer Location — Your organization name, address and contact information.
- ◆ Manage Devices — Allows you to view the list of currently managed devices. Any additions, edits or removals of devices must be performed by an EMC Global Services professional. One can use the Deployment Utility to manually add a single device or use the automated batch processing of Gateway Device Extract configuration files to add multiple devices at the same time.

Devices are usually deployed to the Gateway server that is physically located closer to the device. Management (monitoring, event notification, and remote access session management) is handled by that Gateway server, unless a problem occurs with that server. In this case, the peer server handles the activity.

### Gateway Extract Utility (GWExt)

To configure a device for management, the EMC Global Services representative on site must know the following for each managed device: serial number, EMC site identification number, product type, and an IP address that can be used to access the device. The Gateway Device Extract utility (**GWExt.exe**), when run on the EMC device, automates the collection of this information and transports it to the Gateway server. EMC supplies three versions of the **GWExt** utility with the Gateway server installer to support Windows, Linux and Solaris clients.

Your EMC Global Services professional copies the **GWExt** utility from the installation CD or the Gateway server to the managed device.

---

**Note:** The **GWExt** utility cannot be run on Cisco switches, Brocade-B switches, EDL, Centera, Invista<sup>®</sup> CPCs, or CLARiiON service processors. The **GWExt** utility can be run on CLARiiON Management Station.

---

When running the **GWExt** utility, the **GWExt** utility first requests the Gateway server IP address and EMC site identification number. It then extracts the serial number and local IP address from the target, creates a configuration file, and sends the file to the Gateway server.

The configuration files, for all devices that have used the **GWExt** utility, reside on the Gateway server until processed through the Deployment Utility's Managed Devices option.

### Information files

Beginning with ESRS Gateway release 1.03, any new products qualified for Gateway have a **GWExt** information file installed at time of production. This information file contains product information that the **GWExt** utility gathers and submits to the Gateway server for device registration, automating a large portion of the process.

### Target device management

Devices are added to the list of managed target devices (EMC storage products and select switches) in the Gateway system by using the Deployment Utility.

**Note:** Use of the Deployment Utility for device deployment, undeployment, and editing is restricted to authorized EMC Global Services personnel. Customers may use the Deployment Utility only to view configurations.

The managed device registration process is similar whether devices are manually added or added with the Gateway Extract Utility (GWExt) which enables batch processing of configuration files. Device registration requires the input of a serial number, IP address, model (product type), and site ID number.

When attempting to manage (or unmanage) a device EMC Global Services is prompted for their EMC-issued RSA SecurID Authenticator pass code. This information is then forwarded immediately to EMC servers for an authentication reply. No pass codes are kept on your Gateway server or in the EMC Gateway DRM database. All communications from the Deployment Utility are routed through the SSL tunnel to maximize data security.

EMC Global Services personnel must verify with your network administrators that the IP address of the target device is accessible from the Gateway server and is not translated (NAT'd). For example, the local IP address of a device is 144.10.10.3, and is only on your internal network. You are using NAT (or a NAT device) that maps the device IP (144.10.10.3) to IP 10.10.44.22 so that the device can be reached from within your DMZ. In this case, EMC must use the NAT IP address of 10.10.44.22 to reach the device, and in the Deployment Utility the IP address field must be changed to 10.10.44.22.

The final portion of the deployment process requires a validation that a device is successfully added to the configuration in the EMC DRM

system. The Deployment Utility 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 Deployment Utility catalogues the device under a UI tab labeled *unresolved*. This indicates that the device failed registration, and it needs to be reconciled with the serial number of the device on record with EMC Global Services. Until full reconciliation is achieved, the device is not accessible for remote support by the Gateway. The Deployment Utility is also used to edit the IP address of a device if it has been changed.

In the event you want to unmanage a device or otherwise no longer require it to be accessible, it can be removed from the list of managed devices by an authorized EMC Global Services representative through the device management menu within the Deployment Utility. This menu selection sends a message to the EMC DRM system to logically disassociate this serial number from your Gateway system.

## Security features of the Gateway solution

The section details the security features of the Gateway solution.

### Policy Manager

Using the Policy Manager, you control the authorization requirements for remote access connections, file transfers, service notification processes, diagnostic script executions, and other Gateway-related activities, as shown in [Figure 5 on page 18](#). The Policy Manager allows you to set authorization permissions for target devices or groups of target devices being managed by the Gateway system and provides these permissions to the Gateway system during polling by the Gateway server, and records all requests and actions in local log files. When a request arrives at the Gateway server for remote device access, the access is controlled by the Gateway enforcing the policy 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 Gateway agent 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 (provide authorization).

Action	Permission	Parameters	Access Right	Inheritance	Lock
Enable a Script	Default enable a script permission	Script name : *	Never Allow	Global	<input type="checkbox"/>
Register Script	Default register script permission	Script Name : *	Always Allow	Global	<input type="checkbox"/>
Disable a Script	Default disable a script permission	Script name : *	Always Allow	Global	<input type="checkbox"/>
Run Script	Default run script permission	Script Name : *	Always Allow	Global	<input type="checkbox"/>
UnSchedule a Script	Default permission for unscheduling a script	Script name : *	Never Allow	Global	<input type="checkbox"/>
Schedule a Script	Default permission for scheduling a script	Script name : *	Always Allow	Global	<input type="checkbox"/>
Stop Script	Default stop script permission	Script Name : *	Always Allow	Global	<input type="checkbox"/>
UnRegister Script	Default unregister script permission	Script Name : *	Always Allow	Global	<input type="checkbox"/>

Figure 5 Policy Management settings

When you set an authorization rule to Ask for Approval, the Policy Manager sends an email message to your designated address upon each action request, per transaction. This email message contains the action request itself and the user ID of the EMC<sup>®</sup> Global Services representative requesting permission to perform the action. You use the Policy Manager interface to accept or deny the requested action. [Figure 6 on page 19](#) provides an example.



**Figure 6** Pending request

As with agent and enterprise server communication behavior, the Policy Manager only responds to requests from the Gateway agent. Since the agent caches the Policy Manager's permission rules at startup, the agent must poll the Policy Manager for configuration updates. In this way, the agent captures any change to the Policy Manager rule set after its last polling cycle. Like the agent, 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.

The Policy Manager uses the Apache Jakarta 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 logs all remote support events. Remote access connections, diagnostic script executions, and support file transfer operations are stored in the audit log files. The Policy Manager also logs all authorization activity and policy changes. The audit log files can be viewed through the Policy Manager interface. All log files are controlled and managed by you to enable auditing of remote support connections executed by EMC. See [Figure 7 on page 20](#) for a sample audit log.

The screenshot shows the EMC Policy Manager interface. At the top, there is a navigation bar with 'Home', 'Policy', 'Pending Requests', 'Audit Log', and 'Configuration'. Below this, the page title is 'View audit log entries for Global group'. A text block explains that this is a list of audit log entries for the 'Global' group, including all audit messages generated by EMC Policy Manager and sent in messages from Agents defined in this group. Below the text is a table with the following columns: Group Name, User Name, Service Request, Date Message Posted, and Message. The table contains 15 rows of log entries, each detailing a specific action performed on a device, such as 'successfully processed Action: Remote Application: Remote Application Name-EMCRemote;'.

Group Name	User Name	Service Request	Date Message Posted	Message
ML2895000499-1	ginnes	2010780	Wed Nov 02 10:04:42 EST 2005	Device ML2895000499-1 successfully processed Action: Remote Application: Remote Application Name-CelerraMgr;
MCSN04975-5	ginnes	2010900	Wed Nov 02 10:04:22 EST 2005	Device MCSN04975-5 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
HK187401589-3	danicv	Unknown	Wed Nov 02 10:04:01 EST 2005	Device HK187401589-3 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
WRE000302000091-5	ginnes	2010510	Wed Nov 02 10:03:07 EST 2005	Device WRE000302000091-5 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
FOX06385907-3	ginnes	2011393	Wed Nov 02 10:02:38 EST 2005	Device FOX06385907-3 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
MCSN04975-5	ginnes	2010511	Wed Nov 02 10:02:18 EST 2005	Device MCSN04975-5 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
WRE000302000091-5	danicv	Unknown	Wed Nov 02 10:01:22 EST 2005	Device WRE000302000091-5 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
HK187401589-3	ginnes	2010487	Wed Nov 02 10:00:35 EST 2005	Device HK187401589-3 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
WRE000302000091-6	ginnes	2010506	Wed Nov 02 10:00:22 EST 2005	Device WRE000302000091-6 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
APM00034401489-6	danicv	Unknown	Wed Nov 02 10:00:04 EST 2005	Device APM00034401489-6 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
FOX06385907-3	ginnes	2010548	Wed Nov 02 09:59:51 EST 2005	Device FOX06385907-3 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;
MCSN04975-5	ginnes	2010471	Wed Nov 02 09:59:04 EST 2005	Device MCSN04975-5 successfully processed Action: Remote Application: Remote Application Name-EMCRemote;

Figure 7 Audit log sample

## Device control

The Gateway solution proactively monitors, alerts, and notifies the EMC Customer Support Center when the Gateway server or any Gateway-managed device fails to communicate back to EMC regularly. 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 Gateway device management system, and you can phase them in by product line. EMC provides applications to assist you in automating the addition of new devices to the Gateway management. All device management operations are logged and must be performed by authorized EMC Global Services professionals using EMC-issued RSA SecurID Authenticators.

## Digital Certificate Management

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

Digital Certificate Management (DCM) automates Gateway 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, DCM aids in programmatically generating and authenticating each certificate request, as well as issuing and installing each certificate on the Gateway.

The Gateway system DCM provides proof-of-identity of your Gateway server. This digital document binds the identity of the Gateway to a key pair that can be used to encrypt and authenticate communication back to EMC. Because of its role in creating these certificates, the EMC certificate authority is the central repository for the EMC Secure Remote Support Gateway key infrastructure.

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

The EMC Global Services professional requests a certificate by first authenticating himself or herself using an EMC-issued RSA SecurID Authenticator. Once authentication is complete, the Gateway installation program locally generates all the information required for the certificate on your Gateway server. It then enters the information on the certificate request, ensures accuracy and completeness of the information, and generates a random private key password with encryption. The installation program then submits the request, and after the certificate is issued, the installation program completes the certificate installation the Gateway server automatically.

---

## Device access control

The Gateway solution achieves remote application access to a server 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 access server and through a pull connection to the Gateway server. EMC never initiates a connection to your Gateway server or network. Your policies determine if and how a connection is established.

---

## Device configuration access control

Once your devices are configured for Gateway solution management, it is imperative that any changes to the configuration of the managed device are carefully controlled and monitored. For example, changing the configured IP address in the Gateway system or changing the IP address of the storage device disables EMC's ability to perform remote service on that device as well as the devices's call home capabilities. For this reason, the Gateway solution's Deployment Utility requires that only authorized EMC Global Services professionals are allowed to alter the configuration of a managed device. Each device modification, as well as the user ID of the EMC Global Services professional who performed the change, is tracked in the Policy Manager and EMC DRM audit logs.

---

## EMC enterprise access control

Several security features are incorporated into the EMC DRM system. The Gateway infrastructure is isolated from the rest of EMC's internal networks. EMC Global Services professionals must be logged into the EMC corporate network system to access the DRM system. Only authorized EMC personnel can access the DRM system, and only those employees that have authorization approval from EMC Global Services can use it.

In addition, only those EMC Global Services professionals that are approved to access your specific devices can initiate remote connection sessions with those devices.

## Supported products and ports requirements

The products supported for the EMC Secure Remote Support Gateway solution are listed in [Table 2 on page 23](#). The open port requirements for each product are listed in [Table 3 on page 24](#).

**Table 2 Products and application releases supported by ESRS**

Product	Environment/application releases
Brocade-B Switch	Brocade switches running Fabric OS 5.0.1b and later, with Fabric Manager 5.2.0b and later <sup>a</sup>
Celerra	NAS Code 5.4 or later
EMC Centera	EMC CentraStar® 2.4 or later <sup>a</sup>
Cisco Switch	3.1(3a), 3.1(2), 3.2(1a), 3.2(2c), 3.2 (3a) MDS 9000 running SAN-OS 3.3(1c), SAN-OS 3.3(2), NX-OS 4.1(1b) <sup>a</sup> , NX-OS 4.1 (3a)
CLARiiON	EMC FLARE® Operating Environment 2.17 or later EMC Navisphere® Manager 6.14 or later  <b>Note:</b> The AX-100/AX-150 are not supported as they do not support the required EMC CLARAlert®.  The AX4-5 series are supported if the Navisphere Full license (with CLARAlert) is purchased.
Invista	Invista 2.2 and above
EMC Connectrix® Manager and Connectrix M-series switches	Connectrix Manager 7.x with DialEMC 2.2.10 Connectrix Manager 8.x or later with ConnectEMC 1.x
Connectrix Manager and Connectrix M-series and B-series switches	M-series — Connectrix Manager 9.6.2 or later with ConnectEMC 1.x B-series — Connectrix Manager 6.0.0b or later
Connectrix Manager Data Center Edition and Connectrix M-series and B-series switches	M-series — CMDCE 10.1.1 or later with ConnectEMC 4.0.2 B-series — Running FOS 6.0.0b or later
EMC Disk Library for mainframe (DLm)	DLm4020, DLm4080 (release 1.2 and later), DLm120, DLm960
EMC Disk Library (EDL)	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 RecoverPoint	RPA 3.1 and later <sup>a</sup>
EMC Symmetrix 8000 Series	EMC Enginuity™ 5567 and 5568, with Service Processor Part Number <sup>b</sup> 090-000-064, 090-000-074, or 090-000-09x
EMC Symmetrix DMX™ Series	Enginuity 5670, 5671
Symmetrix DMX-3 Series	Enginuity 5771, 5772, 5773
Symmetrix DMX-4 Series	Enginuity 5772, 5773
EMC Symmetrix V-Max™ Series	Enginuity 5874

a. For remote support access only, not for callhome through ESRS Gateway.

b. These part numbers designate Service Processor running Windows NT SP6.

Table 3 Open port requirements for site network and device configuration

EMC product	Open port requirements	
<b>Gateway components</b>	<b>Outbound</b>	<b>Inbound</b>
EMC Gateway server	TCP 8090 (HTTP) and/or 8443 (HTTPS) (to Policy Manager) Device dependent ports (to devices) TCP 443 (to EMC)	HTTPS, Passive FTP, and SMTP (from target devices)
EMC Policy Manager	SMTP (to Email server)	TCP 8090 (HTTP) and/or 8443 (HTTPS) (from Gateway server)
<b>Target storage devices</b>	<b>Outbound to Gateway server (Service notification):</b>	<b>Inbound from Gateway server (Remote support)</b>
Celerra	HTTPS <sup>a</sup> , Passive FTP, SMTP	TCP 22, 23, 80, 443, and 8000
EMC Centra	SMTP <sup>b</sup>	TCP 22, 3218, and 3682
CLARiiON	HTTPS <sup>a,c</sup> , Passive FTP <sup>c</sup> , SMTP <sup>d</sup>	TCP 80 and 443 (or 2162 and 2163), 5414, 6389-6392, 9519, 13456, and 60020
Connectrix	HTTPS <sup>a</sup> , Passive FTP, SMTP	TCP 5414
DL3D	SMTP <sup>b</sup>	TCP 22
Disk Library for mainframe (DLm)	HTTPS <sup>a</sup> , Passive FTP, SMTP <sup>b</sup>	TCP 22, 80, 443, 8000
EDL	HTTPS <sup>a,c</sup> , Passive FTP <sup>c</sup> , SMTP <sup>d</sup>	TCP 22, 11576
Invista	(Element Manager) HTTPS <sup>a</sup> , Passive FTP, SMTP	(CPCs) TCP 80, 443, 2162, 2163, 5201, 5414
RecoverPoint	SMTP <sup>b</sup>	TCP 22
Brocade-B Switch	N/A	TCP 22 and 23
Cisco Switch	SMTP <sup>b</sup>	TCP 22 and 23
Symmetrix	HTTPS <sup>a</sup> , Passive FTP, SMTP	TCP 1300, 1400, 4444, 5414, 5555, 7000, 9519, 23003-23005

a. HTTPS available only if device is qualified to send files using HTTPS.

b. Via customer email server.

c. If in a centrally managed environment, via management server. Not supported in Distributed mode.

d. If in a centrally managed environment, via management server. If in Distributed mode, via SMTP to the Gateway or customer email server.

---

## Summary

The EMC Secure Remote Support Gateway, or Gateway, is the newest addition to the EMC Secure Remote Support portfolio and provides a increased security and functionality.

---

## Site architecture

You set up the Gateway solution at your site, with the assistance of EMC. The Gateway has the following capabilities:

- ◆ **Agent** — This SSL HTTPS handler is the broker that directs communication between your EMC-installed products and the EMC Customer Support Center, handling user authentication, service notification data file transfer, remote access session regulation, and device management—all the tasks required for remote support.
- ◆ **Configurations** — High-availability configurations require two Gateway servers to ensure that your system is, effectively, always available to handle remote support for all your EMC storage products.
- ◆ **Policy Manager** — This application lets you specify the access authorization criteria you want to use for remote access operations on each device or group of devices that you manage via the Gateway solution.
- ◆ **Deployment Utility** — This client-based application is used to configure the storage devices that the Gateway agent is to manage.

---

## Security features

The Gateway solution protects customer confidentiality and integrity through the industry-recognized "3 A's" for security—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 (DCM)** — DCM automates Gateway server 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 via EMC's strict centralized access controls.

---

## Glossary

<b>authenticate</b>	Confirm or deny identity of system user candidate.
<b>authorize</b>	Confirm or deny level of access or editing privileges for system user.
<b>device</b>	See target device.
<b>enterprise (servers)</b>	Gateway components located at EMC facilities supporting the customer site installations.
<b>event</b>	Error or otherwise notable activity reported from target device.
<b>Gateway</b>	(1) ESRS server at customer site. (2) Short name of EMC Secure Remote Support Gateway.
<b>RSA</b>	RSA Security, makers of security servers and SecurID Authenticators used in Gateway system authentication procedures.
<b>target device</b>	EMC information infrastructure product installed at a site. Gateway 1.03 includes, for example, Celerra, EMC Centera, CLARiiON, Connectrix, EMC Disk Library, Symmetrix devices, Brocade-B and Cisco switches, among others.

---

## References

1. *Security Protection in EMC Remote Support Services: Current Solutions*. EMC Corporation. September 2002.
2. *ICSA Labs Report of Findings for EMC: EMC Secure Remote Support Gateway*. ICSA (Mechanicsburg, PA). June 2006.

Additional EMC documentation may be available from the EMC Powerlink website:

<http://Powerlink.EMC.com>

Copyright © 2009 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the Technical Documentation and Advisories section on EMC Powerlink.

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

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