EMC® Secure Remote Support IP Solution

Release 2.08

Operations Guide

P/N 300-012-319
REV A02

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

Published March, 2011

Contents

Figures

Tables

Preface

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

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

Audience

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

Related documentation

Related documents include:

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

Conventions used in this guide

EMC uses the following conventions for notes and cautions.

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

CAUTION

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

EMC uses the following type style conventions in this guide:

Normal	In running text: • Interface elements (for example, button names, dialog box names) outside of procedures • Items that user selects outside of procedures • Java classes and interface names • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, menu names, utilities • Pathnames, URLs, filenames, directory names, computer names, links, groups, service keys, file systems, environment variables (for example, command line and text), notifications
Bold	• User actions (what the user clicks, presses, or selects) • Interface elements (button names, dialog box names) • Names of keys, commands, programs, scripts, applications, utilities, processes, notifications, system calls, services, applications, and utilities in text
Italic	• Book titles • New terms in text • Emphasis in text
`Courier`	• Prompts • System output • Filenames • Pathnames • URLs • Syntax when shown in command line or other examples
`Courier, bold`	• User entry • Options in command-line syntax
`Courier italic`	• Arguments in examples of command-line syntax • Variables in examples of screen or file output • Variables in pathnames
<>	Angle brackets for parameter values (variables) supplied by user.
[]	Square brackets for optional values.
|	Vertical bar symbol for alternate selections. The bar means or.
...	Ellipsis for nonessential information omitted from the example.

Where to get help

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

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

`http://Powerlink.EMC.com`

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

Your comments

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

`techpubcomments@EMC.com`

PART 1

Preinstallation

Before you install the ESRS IP software on your servers, you should be familiar with the components. There are tasks you must perform, as described in the following chapters.

Chapter 1, "Introduction"

Provides an introduction to the EMC Secure Remote Support IP Solution architecture and its components.

Chapter 2, "Gateway Client Server Preparation"

Provides steps necessary to prepare the Gateway Client server prior to ESRS IP software installation.

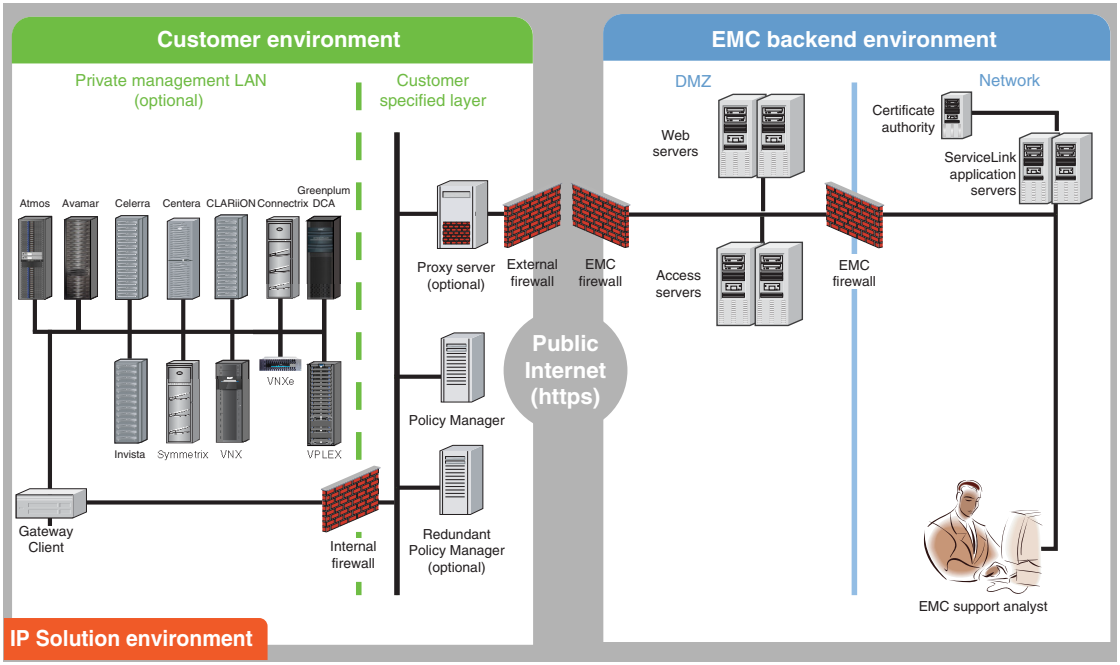
1 Introduction

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

This chapter introduces the EMC Secure Remote Support IP Solution. Topics include:

Architecture

The EMC® Secure Remote Support IP Solution (ESRS IP) 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 24 illustrates the major processing components and their interconnections.



GEN-001688

Figure 1 ESRS IP architecture

Customer site components

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

- ESRS IP Client software residing on a dedicated server (for a High Availability configuration, two or more servers are required)
- ESRS IP Policy Manager software residing on a Policy Manager server

Gateway Clients

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

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

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

Each ESRS IP Client acts as a proxy, carrying information to and from managed devices or to a Policy Manager. 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 rolling runtime log file.

Policy Manager

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

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

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

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

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.

Note: When a customer configuration requires proxy communication between the ESRS IP Client and the Policy Manager or between the ESRS IP Client and the EMC Enterprise, if the ESRS IP Client cannot connect to either the Policy Manager or to the EMC Enterprise through the proxy communication path, it will continue to attempt to connect multiple times. After a couple of minutes, if the ESRS IP Client is unable to connect using the proxy connection path, it will then attempt a direction connection (disregarding the proxy path). If the ESRS IP Client successfully makes a direct connection, no error message will appear to notify the customer or EMC that there is a problem with the proxy communication path.

Table 1 on page 27 shows the minimum configuration of the required hardware and the application software.

Table 1 Specifications for ESRS IP Client server and Policy Manager server

Type	Requirements	EMC provided software	Notes
Gateway Client server	**Processor** — One or more processors, each 2.2 GHz minimum, must be SSE and/or SSE2 supported (required for FIPS compliance) **Free Memory** — Minimum 1 GB 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. NOTE: .NET Framework 3.5 and 4.0 are not compatible at this time. **Microsoft Visual C++ 2005 SP1 Runtime Library** **Operating System** — US English only supported, as follows: • Windows Server 2003 R1 or R2, 5.2, 32-bit, SP 1 or 2 • Windows Server 2003 R2, 5.2, 64-bit, SP 1 or 2 • Windows Server 2008, R1, 6.0, 32-bit or 64-bit, IIS 7.0, SP1 or SP2 • Windows Server 2008, R2, 6.1, 64-bit, IIS 7.0, SP1	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 2.1GHz or better. **Free Memory**—Minimum 2 GB RAM, preferred 3 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 2 GB available (preferably on a storage device of 80 GB 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 System** — US English only supported, as follows: • 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 Gateway Client servers See *EMC Secure Remote Support IP Solution Site Planning Guide*		

Communication to EMC

All outbound communication between the customer's site and EMC is initiated from the customer's site by the ESRS IP Clients over port 443 and 8443. Using industry standard Secure Sockets Layer (SSL) encryption over the Internet and an EMC-signed digital certificate for authentication, the 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 a 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 relies on the SSL tunnel, but communication processes and protocols within the tunnel vary by function. Each function is discussed in the following sections.

Heartbeat polling

Heartbeat polling is described in the following sections:

- "To EMC by the ESRS IP Client" on page 28
- "To EMC devices managed by the ESRS IP Client" on page 29

To EMC by the ESRS IP Client

The *heartbeat* is a regular outbound 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 enterprise with status information on the connectivity 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. Once this response is received, the ESRS IP Client

terminates the connection. Figure 2 on page 29 provides an illustration of the heartbeat communication paths.

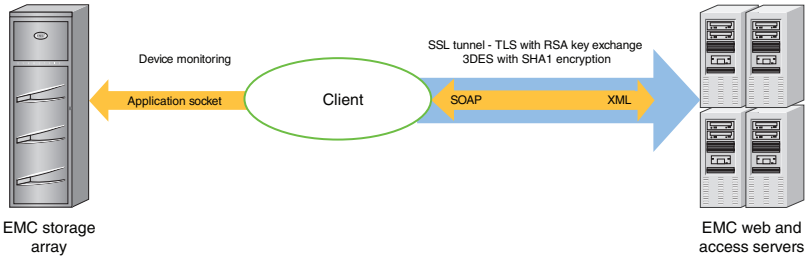


Figure 2 Heartbeat communication

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 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 also serve as a conduits for EMC products to send remote notification event files to EMC. EMC hardware platforms use remote notification for several different purposes. Errors, warning conditions, health reports, configuration data, and script execution statuses may be sent to EMC. Figure 3 on page 30 provides an illustration of the remote notification communication paths.

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

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

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

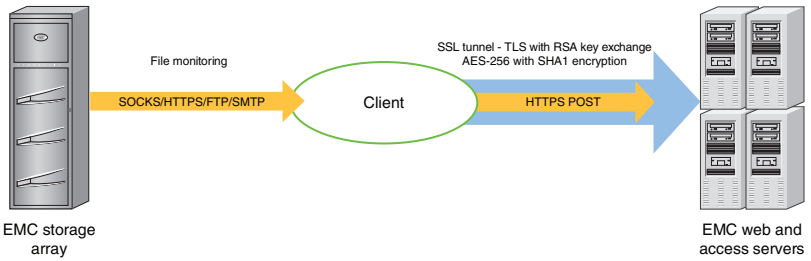


Figure 3 **Remote notification communication**

Remote access

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

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

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

This secure session allows IP traffic from the EMC internal service person to be routed through the ESRS IP Client to the end 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 31 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 only to the specific ports at the IP address associated with the registered serial number of the EMC device at the time of deployment.

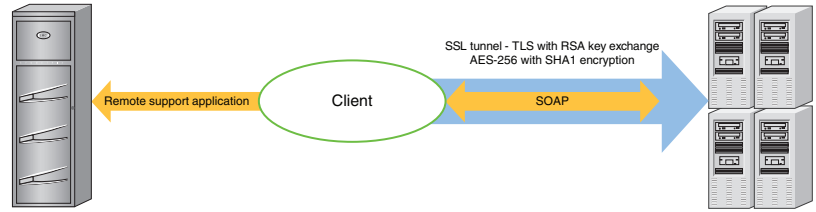


Figure 4 **Remote access communication**

Table 2 on page 31 shows which EMC products 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 via ESRS IP	EMC remote access to device via ESRS IP
EMC Atmos®	Device does not send Connect Homes via the ESRS IP Client	Yes
EMC Avamar®	Yes	Yes
EMC Celerra®	Yes	Yes
EMC Centera®	Device does not send Connect Homes via 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 via ESRS IP	EMC remote access to device via ESRS IP
DL3D	Device does not send Connect Homes via the ESRS IP Client	Yes
DLm	Yes	Yes
EDL	Yes	Yes
EMC Invista®	Yes	Yes
EMC Greenplum DCA®	Yes	Yes
RecoverPoint	Yes	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. Via Connectrix Manager; ECC or approved third-party application

b. Via Cisco Fabric Manager; ECC or approved third-party application

Responsibilities for the ESRS IP components

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

Customer

You are responsible for the following:

- Installing, configuring, and maintaining the following hardware and software components:
  - Gateway Client server hardware and operating system
  - Policy Manager server hardware and operating system
  - Antivirus and other applicable security software
- Providing continuing maintenance to hardware and operating systems, including security updates
- Preparing and configuring the network, proxy server, and firewall
- Backing up and restoring your file systems
- Maintaining physical security of the hardware
- Protecting all files on the Gateway Client and Policy Manager servers, including the SSL certificate if applicable
- Configuring, administering, and updating policies and accounts on the Policy Manager

EMC Global Services

EMC Global Services personnel are responsible for the following:

- Installing the ESRS IP solution software:
  - Gateway Client server software
  - Policy Manager software (customers may install this software)
- Configuring and deploying the EMC devices managed through the ESRS IP solution

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

- Updating the ESRS IP Client and Policy Manager software

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

Configuration

This section provides details on the configuration of the ESRS IP Solution.

ESRS IP Client server configuration

A Gateway Client server can be implemented in one of several configurations to meet your network and security requirements. See Figure 1 on page 24 for a sample configuration.

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

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

VMware support

ESRS IP is qualified to run on a VMware virtual machine. VMware support allows customers to leverage their existing VMware infrastructure to benefit from the security features of ESRS IP without adding hardware. VMware VMotion functionality also allows the Policy Manager, when installed on 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
- 1 GB memory allocated
- SMB modules optional
- VMotion functionality optional

Note:
When running clustered High Availability Gateway Client servers on VMware, each Gateway Client must be located on different physical hardware.

Do not place VMware images or storage files on EMC devices managed by 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 configuration to eliminate single point of failure. A Gateway Cluster refers to the relationship created between two or more Gateway Clients.

Gateway Client servers, in a High Availability configuration, are active peers. Each Gateway Client in the cluster manages the same set of devices without awareness of, or contention with, the other 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 cluster device management is synchronized by the EMC enterprise servers during polling cycles so that changes to the configuration on one Gateway Client in the cluster are automatically propagated to the other. When there is an addition, removal, or edit of a device on the managed devices list for any Gateway Client in a High Availability Gateway Cluster configuration, the EMC enterprise sends a synchronization message to all clustered Gateway Clients. When the other Gateway Client(s) in the cluster receives the device management transaction information, it updates its list of managed devices. If that Gateway Client is currently not available during a synchronization attempt, the EMC enterprise queues the transaction. Synchronization of the Gateway Cluster occurs upon the next successful poll message received from the previously unavailable Gateway Client.

Installing a High Availability Gateway Cluster

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

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 automatically installed upon successful completion of your ESRS IP Client installation. It is typically located at Start > Programs > ESRS > Config Tool.

The Configuration Tool is used to perform the following tasks:

- Configure the ESRS IP Client and Policy Manager
- Process management requests for 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. The ESRS IP Client proxies all Configuration Tool management requests to the EMC enterprise for approval by EMC Global Services.

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

Menu items

The following list describes the configuration menu items available through tabs in the Configuration Tool. Note that these pages do not refresh dynamically—you must manually refresh the page:

- Status tab — Displays status information about the connection between the ESRS IP Client and EMC, including connectivity status, proxy server and Policy Manager enablement, and other status results.
- 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 by an EMC Global Services professional is required before these changes will take place.

- Proxy Servers tab — Allows enabling or disabling of a proxy between an ESRS IP Client and the EMC enterprise.
- Policy Manager tab — Allows enabling or disabling communication between a Policy Manager and an ESRS IP Client.

- Services tab — Displays the state (running, stopped, 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 managed devices.
- Log tab — Displays the log file for the ESRS IP Client activity.

Monitoring and event notification are handled by the ESRS IP Client. If a problem occurs with an ESRS IP Client and a High Availability Gateway Cluster has been implemented, another Gateway Client within the cluster will handle these activities.

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

Device management

The Configuration Tool enables you to request the addition or removal of a managed device. You can also use the Configuration Tool to change the IP address of a managed device.

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

```
Start > Programs > ESRS > Configuration Tool
```

Adding a device

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

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

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

Note: EMC Global Services personnel must verify with your network administrators that the IP address of the managed device is accessible from the 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 us say, for example, that the local IP address of a device is 192.168.0.100, and is only on your internal network. You are using NAT (or a NAT device) that maps the device IP (192.168.0.100) to IP 10.10.44.22 so that the device can be reached from within your DMZ. In this case, EMC must use the NAT IP address of 10.10.44.22 to reach the device, and in the Configuration Tool when managing the device, the IP address utilized must be 10.10.44.22.

Changing a device's IP address

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

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

Unmanaging a device

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

ESRS IP Client installer. For a list of the products that the GWExt utility supports, see Table 3 on page 40.

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

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

Certain products qualified for ESRS 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.

Table 3 Products supported by the Gateway Extract Utility (GWExt)

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

Digital Certificate Management

During the site 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 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 ESRS IP key infrastructure.

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

The EMC Global Services professional requests a certificate by first authenticating himself or herself using an EMC-issued RSA SecurID Authenticator. Once authentication is complete, the ESRS IP Client installation program locally gathers all the information required for requesting certificates. It also generates a certificate request, a private key, and a random password for the private key. The 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. After the certificate is issued, the installation program automatically completes the certificate installation 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 by the ESRS IP Client. EMC never initiates a connection to your ESRS IP Client or network. Your policies as set in the ESRS IP Policy Manager determine if and how a connection is established.

Device configuration access control

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

EMC enterprise access control

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

2

Gateway Client Server Preparation

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

Overview

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

As part of the preparation, the following software applications are required. Additional requirements are described in "Operating system configuration" on page 44:

- **Microsoft Internet Information Services (IIS) —** The ESRS IP service uses IIS to receive notification files sent through the FTP or SMTP transports to the Gateway Client. You must install the following IIS components:
  - Admin Scripts (part of Common Files installed as part of the IIS install)
  - FTP
  - SMTP

  This chapter discusses related tasks, including setting up the FTP and SMTP servers on the system drive.
- **HTTPS Listener—esrshttps.exe** — EMC will install this as part of the Gateway Client software installation. The HTTPS Listener is used when the ConnectEMC service sends device notifications over the HTTPS transport to the Gateway Client.

Operating system configuration

To create the required operating system configuration, start by performing the following steps for each intended server:

1. Install the Windows operating system and any applicable updates:
   - Install one of the supported operating systems shown in Table 1 on page 27.
   - Install and configure any device drivers required by the OS and the hardware.
   - Apply any service packs and security fixes that are required by your corporate policies, including antivirus software.
   - Set the Windows time zone to the correct time zone for your Gateway Client server's physical location.

Note: Remote support tool performance may be adversely affected if the Windows time zone is not set correctly.

2. Load **Microsoft .NET Framework** version 2.0 SP1 (or a newer version that is backwards compatible with 2.0). Instructions are included in "Microsoft .NET Framework" on page 46.

Note: NET3.5 and .NET4.0 are incompatible with the proper operation of ESRS IP Client and associated support applications. hat may result the Client and Applications to stop functioning or fail to perform as designed.

3. Install, configure, and test **Microsoft IIS** according to the instructions in "Internet Information Services (IIS)" on page 47.
4. Install the Microsoft Visual C++ 2005 SP1 Runtime Library.
5. When the configuration is complete, run the Customer Environment Check Tool (CECT) to verify the system configuration and connectivity to EMC managed devices. Refer to Chapter 3, "Customer Environment Check Tool."

Internet protocols (IPv4 and IPv6)

You *must* use Internet protocol v4 (IPv4) for communication from the Gateway Client to EMC.

However, you may use IPv4 *or* IPv6 for the following connection types:

- Communication from the Gateway Client to EMC devices for remote access purposes
- Communication from the Gateway Client to the Policy Manager for access control

Note: Windows 2003/Windows 2008 connect home listeners on the ESRS Gateway (FTP, SMTP, HTTPS) do *not* support IPv6 due to a limitation in Windows 2003 Internet Information Services (IIS).

Microsoft .NET Framework

Microsoft .NET Framework is required for full functionality of the Gateway Client server and its utilities.

Note: The .NET Framework runs as a 32-bit application.

Version 2.0 SP1 (or a newer version that is backward compatible with 2.0) is required for CECT and the Gateway Client server application.

You can download and install the Microsoft .NET Framework from the Microsoft Download Center website. You will need one of the following:

- Microsoft .NET Framework 2.0 Service Pack 1 (x86)
- Microsoft .NET Framework 2.0 Service Pack 1 (x64)

Note: .NET3.5 and .NET4.0 are incompatible with the proper operation of ESRS IP Client and associated support applications. That may result the Client And Applications to stop functioning or fail to perform as designed.

Internet Information Services (IIS)

This section provides the required Internet Information Services (IIS) settings and explains how to deploy IIS:

- The required IIS settings are provided in "IIS settings" on page 48.
- Instructions for deploying IIS are provided in "Deploying IIS 6.0 in Windows 2003" on page 49.

IIS settings

Before installing the ESRS IP Gateway Client software, you must configure its server operating system with the IIS settings shown in Table 4 on page 48.

Table 4 Gateway Client server standard configuration requirements

Category		Variable	Value
Internet Information Services (IIS)		Startup type	Manual
		State	Started
Note: The following settings describe the FTP services and directory structure required for Gateway Client server installation. Once the server has been installed, the FTP or SMTP *service* may be disabled (one or the other, but not both).			
Default FTP Site [a] **> Properties**			
	FTP Site	Description	ESRS Gateway FTP Site
		IP address	Local/Internal IP
		Port	21
	Security Accounts	Allow anonymous connections	No (unchecked)
	Home Directory	Local path	<install drive>:\EMC\ESRS\Gateway\work\ftproot [b]
		Read	Yes (checked)
		Write	Yes (checked)
		Log visits	Yes (checked)
		User Isolation	Yes
Default SMTP Virtual Server > Properties			
		Description	ESRS Gateway SMTP Site
		Domain	emc.com
		Default mail directory	<install drive>:\EMC\ESRS\Gateway\work\mailroot\Drop [c]
		E-mail message	Maximum size of 15 MB
Local Users and Groups > New User		Default User Group	Yes
Note: if set to lockout, test after 5 minutes.	New User (1)	Username	onalert
		Password	EMCCONNECT *(case sensitive)*
		Password cannot be changed	Yes (checked)
		Password does not expire	Yes (checked)
	New User (2)	Username	esrsconfig
		Password	esrsconfig *(case sensitive)*
		Password cannot changed	Yes (checked)
		Password does not expire	Yes (checked)
Create directory			<install drive>:\EMC\ESRS\Gateway\work\mailroot\Badmail [c]

a. These settings describe the FTP services and directory structure required for Gateway Client server installation. Once the server has been installed, these FTP services may be disabled.

b. Important: AFTER the ESRS IP Client is installed per CSP2100* IIS MUST be reconfigured to point to <install_drive>:\EMC\ESRS\Gateway\work\ftproot\

c. Important: AFTER the ESRS IP Client is installed per CSP2100* IIS MUST be reconfigured to point to <install_drive>:\EMC\ESRS\Gateway\work\mailroot\Drop and <install_drive>:\EMC\ESRS\Gateway\work\mailroot\BadMail

Deploying IIS 6.0 in Windows 2003

The following section explains how to install and configure Internet Information Services (IIS) V6.0 in Windows 2003. It also explains how to enable FTP and SMTP services on the system drive.

(For instructions on deploying IIS in Windows 2008, refer to "Deploying IIS 7.0 in Windows 2008" on page 62.)

Note: You must install IIS *before* you install the ESRS IP Gateway Client.

Installing and configuring IIS 6.0 in Windows 2003 SP1 (for IPV4 support)

To install IIS 6.0 in a Windows 2003 SP1 environment (for IPV4 support):

1. Open the **Control Panel**, and from there open **Add or Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. Select **Application Server** and click **Details**.
4. Select **Internet Information Services (IIS)** and click **Details**.
5. Select:
   - **File Transfer Protocol (FTP)**
   - **SMTP Service**

   Leave the **Common Files** and **Internet Information Services Manager** checkboxes selected.
6. Click **OK** to exit the **Internet Information Services (IIS)** setup.
7. Click **OK** to exit the **Application Server** setup.
8. Click **Next** at the **Windows Components** page.

The window in Figure 5 on page 50 appears.

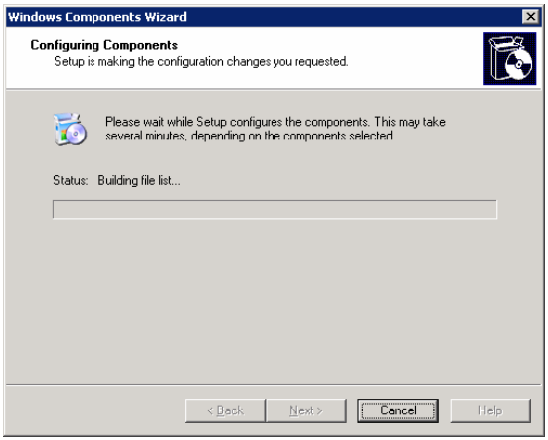


Figure 5 **Windows Component Wizard**

9. If you receive a **Files Needed** prompt as shown in Figure 6 on page 50, insert the required CD-ROM. Provide the path to the Windows Installation CD-ROM I386 directory or wherever your CD-ROM i386 is located.

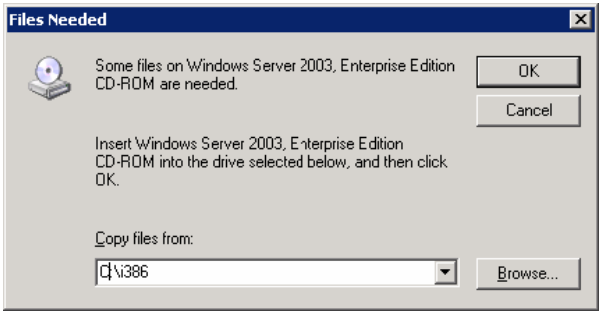


Figure 6 **Files Needed dialog box**

10. Click **Finish**. IIS installs Common Files and FTP and SMTP services in the OS system drive.

Configuring IIS user accounts

This section explains how to configure the operating system for the following IIS user accounts:

- EMC OnAlert™
- ESRSConfig

OnAlert user account setup

To set up OnAlert user accounts, follow these steps:

1. Right-click **My Computer** on the desktop, and select **Manage** from the pop-up menu.
2. Double-click **Local Users and Groups**.
3. Right-click **Users** and select **New User** from the pop-up menu.
4. Type **OnAlert** in the **User Name** field.
5. Type **EMCCONNECT** (case sensitive) in the **Password** field.
6. Type **EMCCONNECT** (case sensitive) in the **Confirm Password** field.
7. Clear the **User must change password at next logon** checkbox.
8. Select the **Password Never Expires** checkbox.
9. Select **User cannot change password**.
10. Click **Create**.

ESRSConfig user account setup

Use this procedure to set up ESRSConfig user accounts:

1. Right-click **Users** and select **New User** from the pop-up menu.
2. Type **ESRSConfig** in the **User Name** field.
3. Type **esrsconfig** (case-sensitive) in the **Password** field.
4. Type **esrsconfig** (case-sensitive) in the **Confirm Password** field.
5. Deselect the **User must change password at next logon** checkbox.
6. Select the **Password Never Expires** checkbox.
7. Select **User cannot change password**.
8. Click **Create**, and then click **Close**.
9. Exit the Computer Management application.

Configuring the FTP server

To configure the FTP server:

1. Open the Internet Information Services (IIS) Manager: **Start** > **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**
2. In the left pane of the **Internet Information Services (IIS) Manager** window, highlight **Default FTP Site**.
3. Right-click **Default FTP Site**, select **Delete** from the pop-up menu, and click **Yes** to confirm the deletion.
4. Right-click **FTP Sites** and select **New FTP Site** from the pop-up menu.
5. Click **Next** at the **Welcome** screen.
6. Type the description **ESRS Gateway FTP**, and click **Next**.
7. Type the IP address that is being used for the FTP server.

   Note: On a Multihomed Server the IP address is the *internal* IP address that connects to the devices.

   (Do not change the default TCP port 21.) Click **Next**.
8. Select **Isolate users**, and click **Next**.
9. Browse to the following location:

   `C:\Inetpub\ftproot\`

IMPORTANT

After completing your ESRS IP Gateway Client installation, change the path to the following:
`<install drive>:\EMC\ESRS\Gateway\work\ftproot`

10. Click **OK**, then click **Next**.
11. Select the **Read** and **Write** checkboxes, and click **Next**.
12. Click **Finish**.
13. In the Internet Information Services (IIS) Manager, right-click the FTP site **ESRS Gateway FTP** and select **Properties** from the pop-up menu.
14. Click **Security Accounts** and clear **Allow anonymous connections**.
15. At the alert, **continue anyway?**, click **Yes**.

16. Click **Messages**.
17. In the **Welcome** field, type a welcome message.

    For example:
    `Welcome to the name_of_your_FTP_server FTP server.`
18. In the **Exit** field, type an exit message.

    For example:
    `You are leaving the name_of_your_FTP_server FTP server. Goodbye!`
19. Click **Home Directory**.
20. Enter the following path in the **Local Path** field:

    `C:\Inetpub\ftproot\`

IMPORTANT

After completing your ESRS IP Gateway Client installation, change the path to the following:
`<install drive>:\EMC\ESRS\Gateway\work\ftproot`

21. Select the **Read**, **Write**, and **Log** visits checkboxes.
22. Click **OK** to exit.

Configuring the SMTP server

To configure the SMTP server:

1. From Windows Explorer, open the following directory:

   `C:\Inetpub\mailroot\`

IMPORTANT

After completing your ESRS IP Gateway Client installation, change the path to the following:
`<install drive>:\EMC\ESRS\Gateway\work\mailroot`

2. Create the following subdirectory:

   `C:\Inetpub\mailroot\Badmail`

IMPORTANT

After completing your ESRS IP Gateway Client installation, change the path to the following:
`<install drive>:\EMC\ESRS\Gateway\work\mailroot\Badmail`

3. In the left pane of the **Internet Information Services (IIS) Manager** window, right-click **Default SMTP Virtual Server**, and select **Rename** from the pop-up menu.
4. Type the new SMTP virtual server name **ESRS Gateway SMTP Server**.
5. Select **Properties**.
6. Select the **Messages** tab, as shown in Figure 7 on page 54.

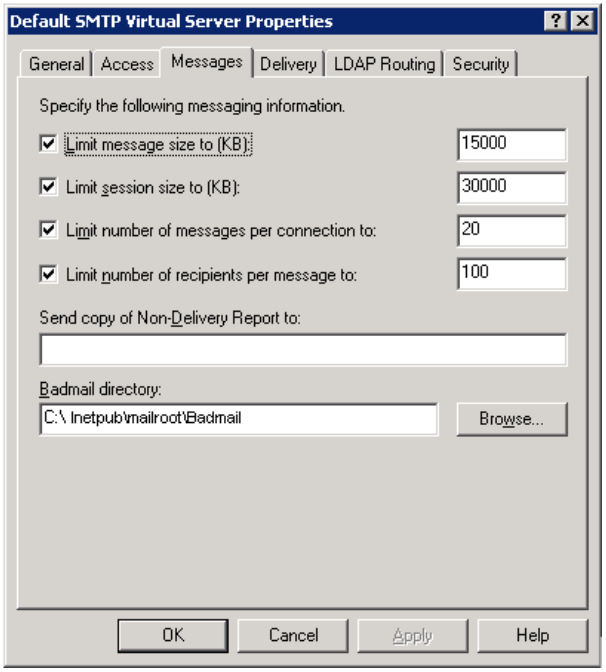


Figure 7 **Messages tab**

7. In the **Badmail directory** field, browse to the following directory:

```
C:\Inetpub\mailroot\Badmail
```

IMPORTANT

After completing your ESRS IP Gateway Client installation, you must change the path to the following:

`<install drive>:\EMC\ESRS\Gateway\work\mailroot\Badmail`

8. In the **Limit Message Size to (KB)** field, type **15000**.

9. In the **Limit Session Size to (KB)** field, type **30000**.
10. Click **OK** to save.
11. Double-click **ESRS Gateway SMTP Server**.
12. Double-click **Domains**.
13. On the right side of the **Domains** window, highlight the domain name.
14. Right-click the domain name and select **Rename** from the pop-up menu.
15. Type the name **emc.com**, and click **Done**.
16. Right-click **emc.com** and set the Drop directory path to the location of the CDrop directory located under the Gateway install, as shown in Figure 8 on page 55.

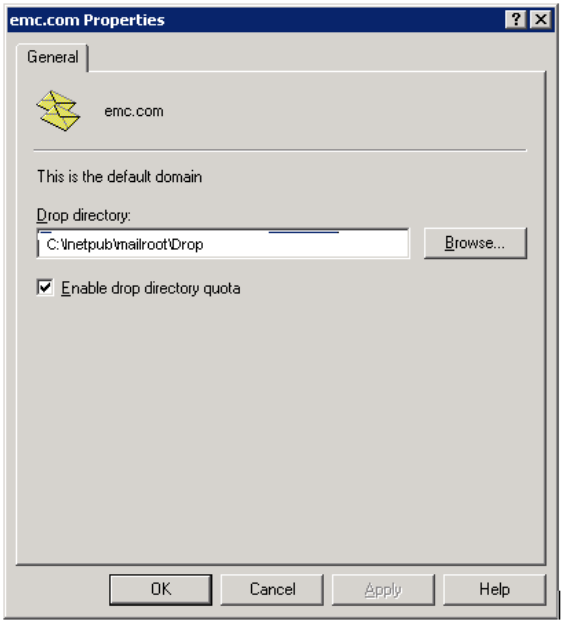


Figure 8 **Drop directory**

17. Click **Apply**.
18. Click **OK**.

19. Open a command window and type **iisreset**, as shown in Figure 9 on page 56.

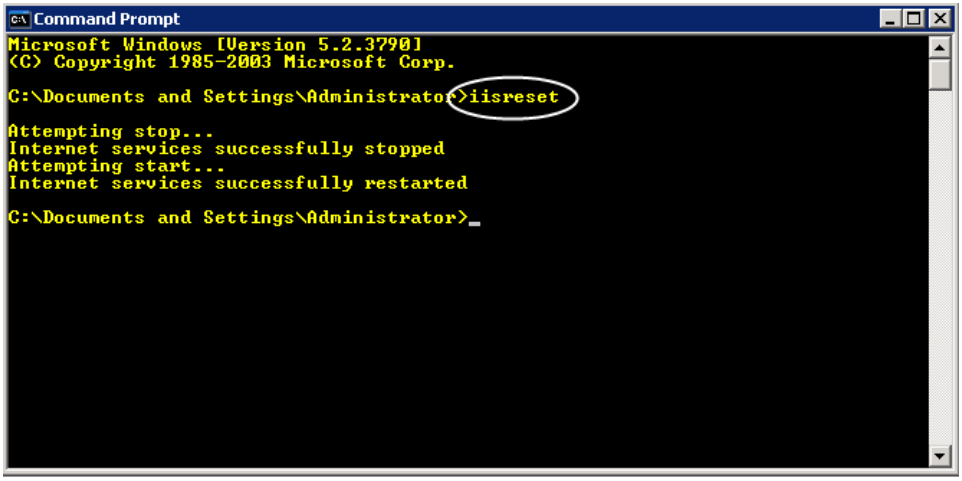


Figure 9 **Command prompt**

Configuring and testing e-mail

The following procedure explains how to set the message size limit and session size limit. It also explains how to test the e-mail server and verify that mail is in the proper directory:

1. In the left pane of the **Internet Information Services (IIS) Manager** window, right-click **ESRS Gateway SMTP Server** and select **Properties**, as shown in Figure 10 on page 57.

Figure 10 Default SMTP properties

2. Click **Messages** as shown in Figure 11 on page 57.

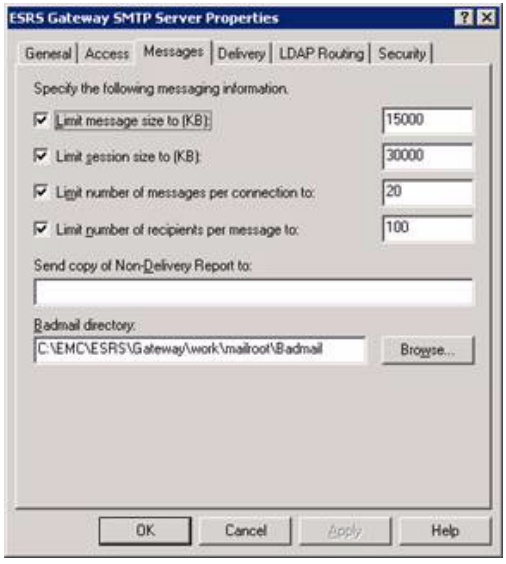


Figure 11 Default SMTP message tab

3. Change the Limit message size to **15000**.

4. Change the Limit session size to **30000**.
5. Click **OK**.
6. In the left pane of the **Internet Information Services (IIS) Manager** window, click **Domain** under Default SMTP Virtual Server.
7. Right-click **emc.com** and select **Properties** as shown in Figure 12 on page 58.

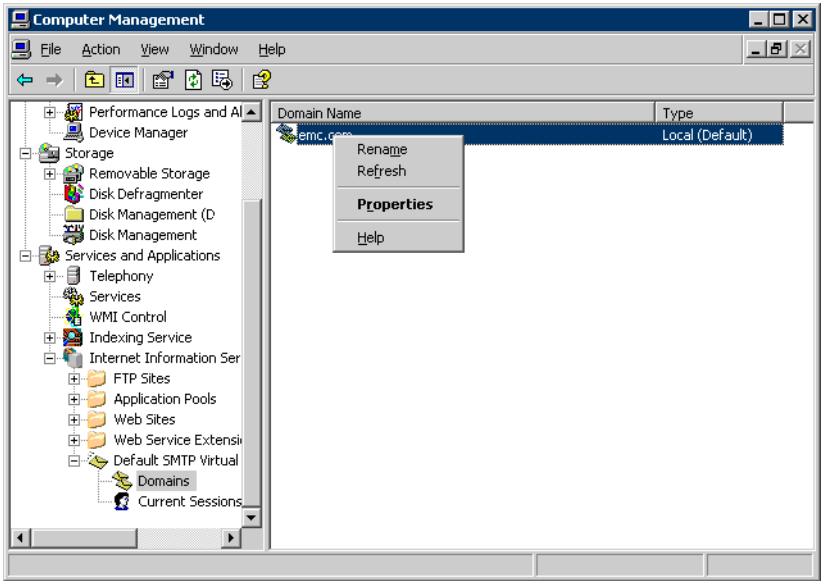


Figure 12 E-mail server specification

8. Point to the maildrop directory on the installation drive as shown in Figure 13 on page 59.

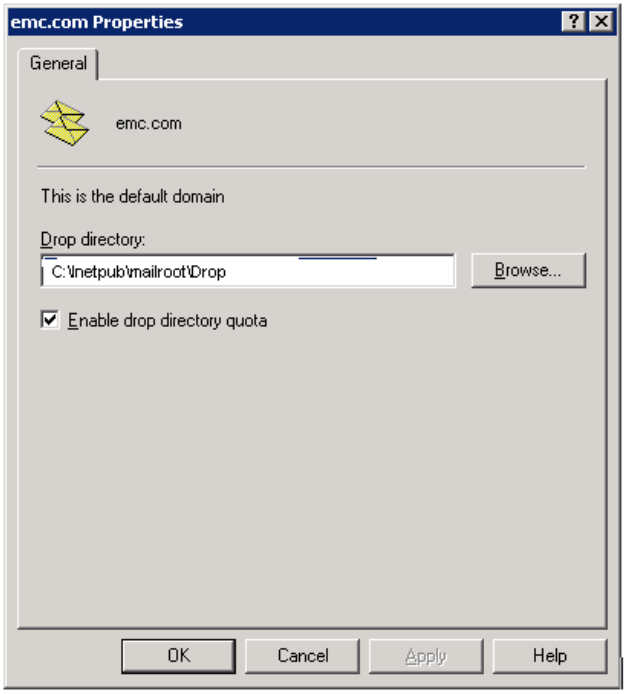


Figure 13 Mail drop specification

9. Test the mail server and verify that mail is in the proper directory, as shown in Figure 14 on page 60.

```
Command that you enter [bold]
Response that you receive [plain]

telnet ip_address 25

220 jerry.lab.pvt.dns Microsoft ESMTP MAIL Service,
Version: 6.0.3790.1830 ready at  Thu, 25 Jan 2007
15:20:31 -0500

vrfy onalert

252 2.1.5 Cannot VRFY user, but will take message for
<onalert@emc.com>

helo

250 jerry.lab.pvt.dns Hello [192.1.7.203]

mail from:esrs@emc.com

250 2.1.0 esrs@emc.com....Sender OK

rcpt to:onalert@emc.com

250 2.1.5 onalert@emc.com

data

354 Start mail input; end with <CRLF>.<CRLF>

subject:testemailserver<CR>
This is a test of the email server<CR>
.<CR>

250 2.6.0
<JERRYexICnDdNUbr6TU00000001@jerry.lab.pvt.dns> Queued
mail for delivery
```

Figure 14 E-mail server test

10. Return to the \\inetpub\mailroot\drop directory.
11. Right-click one of the listed mail messages.
12. Open the mail using Notepad.

    You should see contents similar to those shown in Figure 15 on page 61.

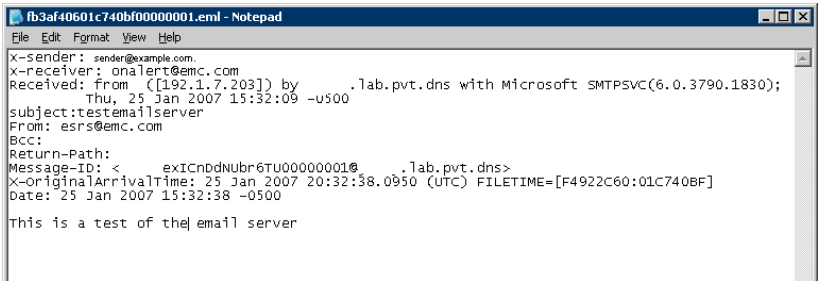


Figure 15 **Sample e-mail**

13. Close and delete all e-mail from the directory.

When the IIS configuration is complete

This completes the installation and configuration of the base operating system. Verify the following:

IMPORTANT

Post ESRS IP Client install verify that the IIS configuration has been reconfigured to reflect the <install_drive>:\EMC\ESRS\Gateway\work\ftproot\ and <install_drive>:\EMC\ESRS\Gateway\work\mailroot\ directory paths as required. If the Provisioning Tool (PvT) / installer has failed to do so manually reconfigure these paths to assure tat Callhomes will be received in the correct directory for forwarding to the Enterprise.

- All devices should be properly installed and functioning. All software should be properly installed and functioning, including the appropriate service pack and patches.
- Your operating system should be hardened according to your specifications.

Next, run the Customer Environment Check Tool (CECT) to verify the system configuration and connectivity to EMC managed devices.

For instructions, refer to Chapter 3, "Customer Environment Check Tool."

Deploying IIS 7.0 in Windows 2008

The following section explains how to install and configure Internet Information Services (IIS) V7.0 in Windows 2008 (for IPv4 support). It also explains how to enable FTP and SMTP services on the system drive.

(For instructions on deploying IIS in Windows 2003, refer to "Deploying IIS 6.0 in Windows 2003" on page 49.)

Note: You must install IIS *before* you install the ESRS IP Gateway Client.

Before starting the IIS 7.0 deployment

Before you install IIS:

- Install Windows 2008.

  Note: The current ESRS IP configuration supports Windows 2008 in a workgroup configuration. It does not support Windows 2008 in a domain configuration.

- Ensure that Windows patches are up to date.
- Install antivirus software.
- Harden the operating system as needed, but ensure that this will not interfere with the functioning of the ESRS IP Solution.

The next step is to reconfigure the password policies.

Temporarily reconfiguring the password policies

Before you can install the necessary IIS user accounts (OnAlert and ESRSConfig), you must temporarily reconfigure the password policies. After you create the user accounts, you will restore them to their original configuration to ensure proper password compliance for additional users.

To reconfigure the password policies:

1. From the Windows 2008 **Start** menu, click **Administrative Tools**. The **Administrative Tools** menu appears, as shown in Figure 16 on page 63.

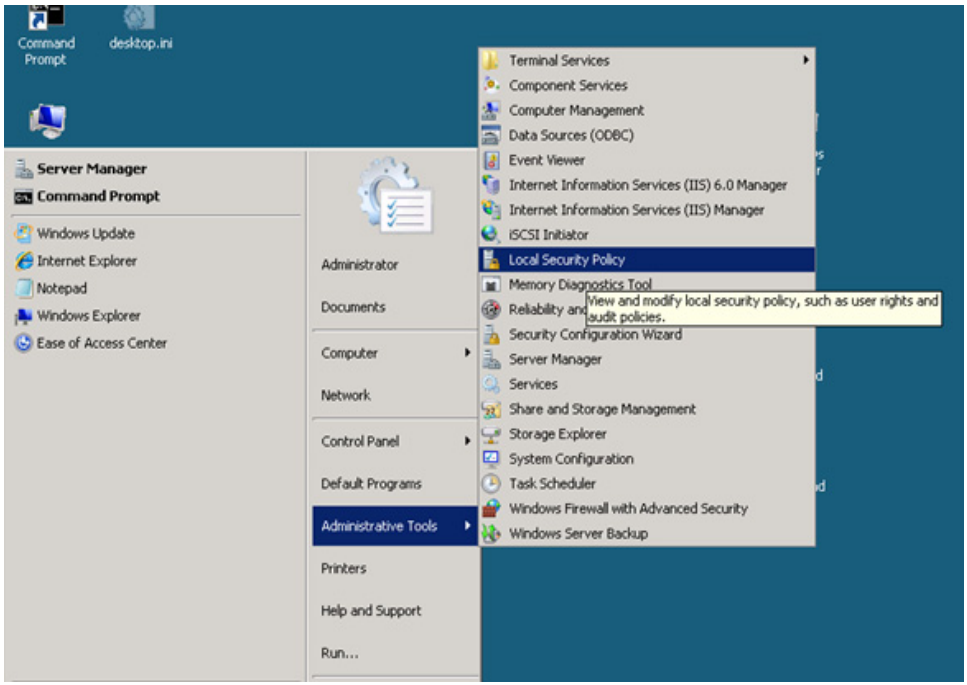


Figure 16 **Local security policy**

2. From the **Administrative Tools** menu, click **Local Security Policy**. The **Local Security Policy** window appears.
3. In the left pane, expand the **Account Policies** folder.
4. Click **Password Policy.** Password policy options will appear in the right pane.
5. In the right pane, double-click **Password must meet complexity requirements**, as shown in Figure 17 on page 63.

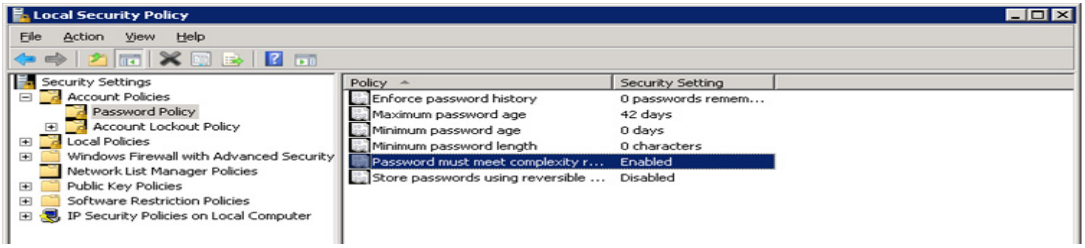


Figure 17 **Complexity requirements**

6. In the **Properties** window, select **Disabled** to disable Password must meet complexity requirements, as shown in Figure 18 on page 64.

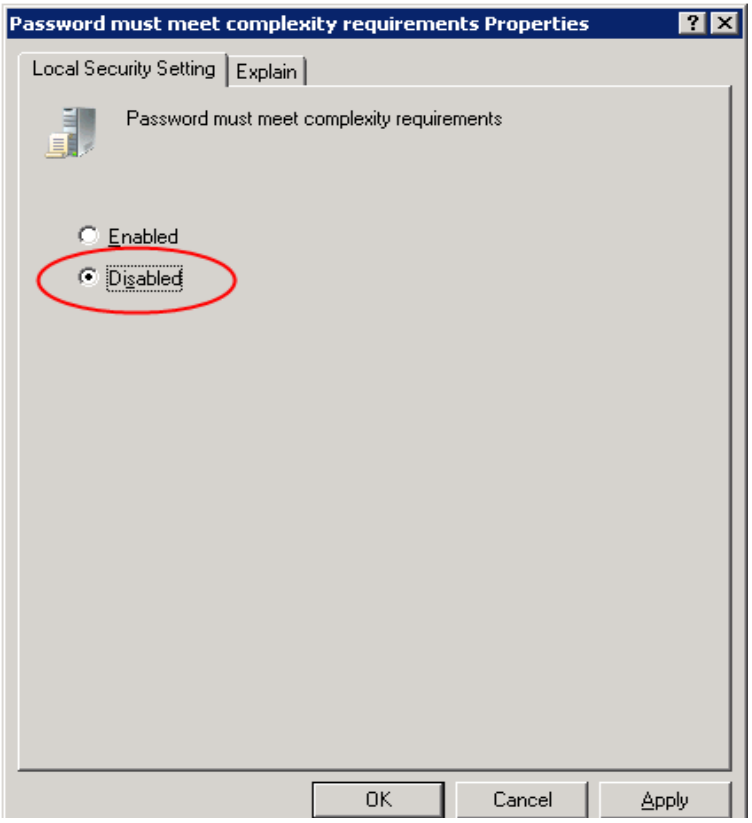


Figure 18 **Disable the complexity requirements**

7. Click **OK** to save your selection.
8. Minimize the **Local Security Policy** window.

You will now be able to create the IIS OnAlert and ESRSConfig user accounts and passwords as described in the following section.

Creating the IIS user accounts and passwords

This section explains how to create the required IIS user accounts and assign their passwords. The required IIS user accounts are:

- OnAlert
- ESRSConfig

IMPORTANT

After you create the IIS user accounts OnAlert and ESRSConfig, you must return to the Local Security Policy window to re-enable Password must meet complexity requirements, as shown in "Restoring the password policies" on page 69.

To create the OnAlert and ESRSConfig user accounts and assign their passwords:

1. From the Windows **Start** menu, right-click **Computer**. The **Computer** menu appears.
2. From the **Computer** menu, click **Manage**, as shown in Figure 19 on page 65. The **Server Manager** window appears.

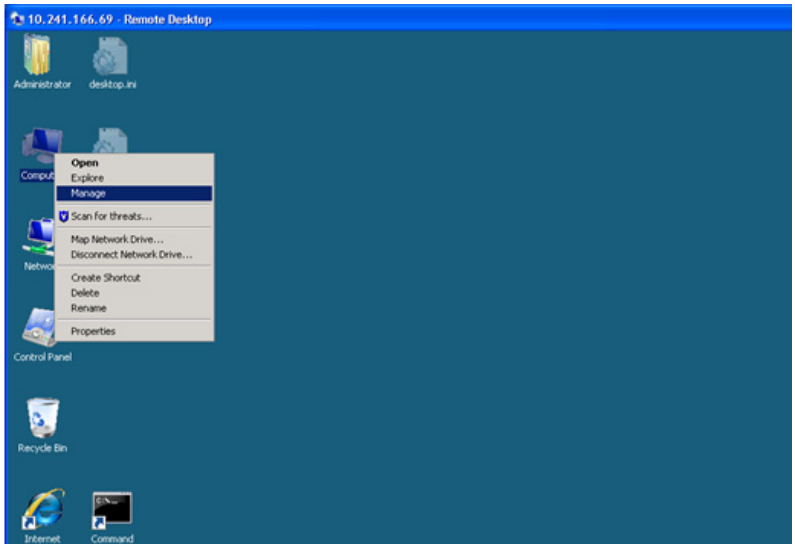


Figure 19 Computer—Manage

3. From the left pane of the **Server Manager** window, expand **Configuration**.
4. Expand **Local Users and Groups.** Two options are visible: Users and Groups.
5. Right-click **Users**. A menu appears, as shown in Figure 20 on page 66.

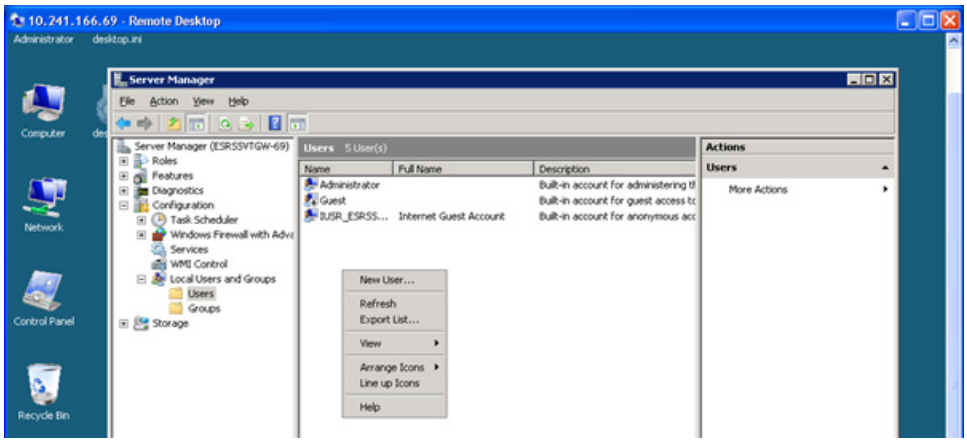


Figure 20 **Menu—Users**

6. Click **New User**. The **New User** window appears, as shown in Figure 21 on page 66.

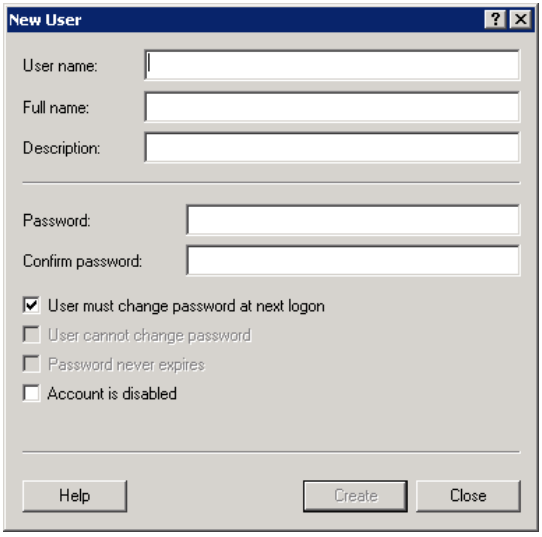


Figure 21 **New User**

Entering the information

Now you are ready to enter the OnAlert and ESRSConfig user account information. For *each* of those accounts, open a **New User** window and perform the following actions:

1. Type the **User name** and **Full name**.
   - For **User name**, you must type **onalert**.

     Note: After you complete these steps to create the username **onalert**, you must repeat these steps to create the username **esrsconfig**.

   - The **Full name** can be the same as the **User Name**.
2. Enter a **Description** (optional).
3. Type the ESRS-specified password in the **Password:** and **Confirm password:** fields.

   Note: You must use specified passwords for the OnAlert and ESRSConfig user accounts. These passwords, which are case-sensitive, are shown in Table 4 on page 48.

4. When you have entered the passwords, clear **User must change password at next logon**, as shown in Figure 22 on page 68.

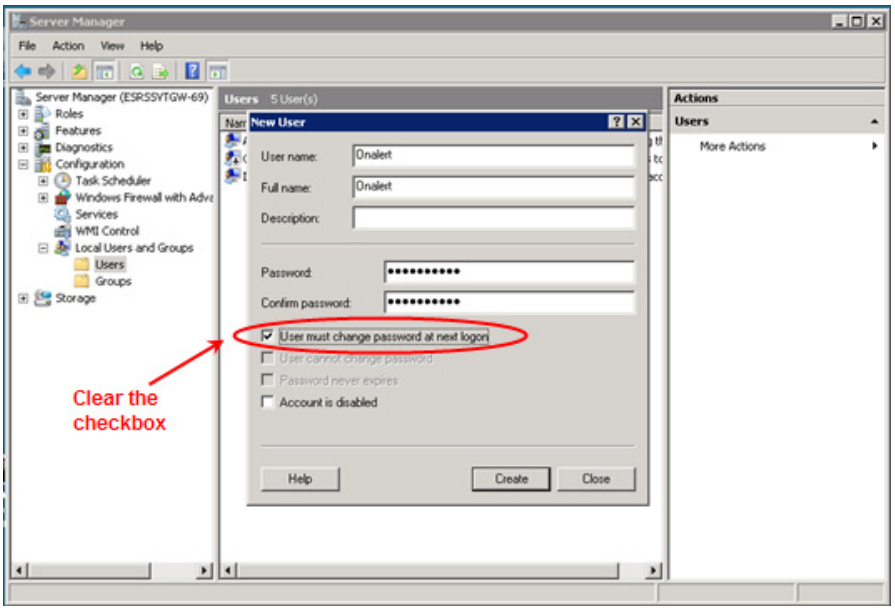


Figure 22 **Clear the checkbox**

5. Select the following checkboxes, as shown in Figure 23 on page 69:
   - **User cannot change password**
   - **Password never expires**

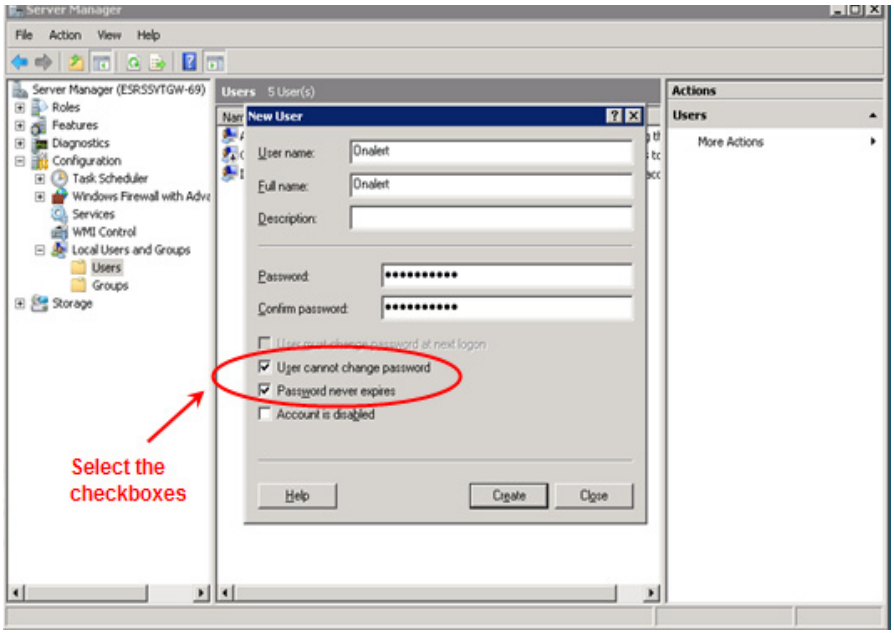


Figure 23 **Select the checkboxes**

6. Click **Create**.
7. Repeat steps 1–6 to create the username **esrsconfig**.
8. Close the **New User** window.
9. Close the **Server Manager** window by selecting **File** > **Exit**.

This completes the user account creation process. Make sure you have created two user accounts: one for **OnAlert** and one for **ESRSConfig**.

The next task is to restore the password policies.

Restoring the password policies

Now that you have created the IIS user accounts, you must restore the password policies to their original configuration. This will ensure proper password compliance for any additional users.

To restore the password policies to their original configuration:

1. From the Windows 2008 **Start** menu, click **Administrative Tools**. The **Administrative Tools** menu appears, as shown in Figure 24 on page 70.

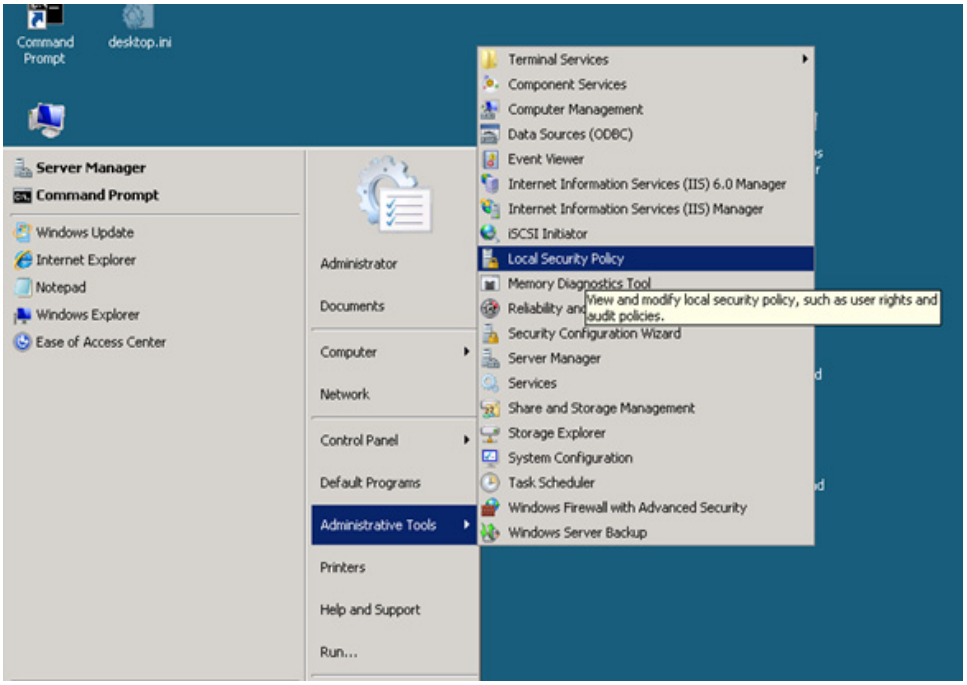


Figure 24 **Local security policy**

2. From the **Administrative Tools** menu, click **Local Security Policy**. The **Local Security Policy** window appears.
3. In the left pane, expand the **Account Policies** folder.
4. Click **Password Policy.** Password policy options will appear in the right pane.
5. In the right pane, double-click **Password must meet complexity requirements**, as shown in Figure 25 on page 71.

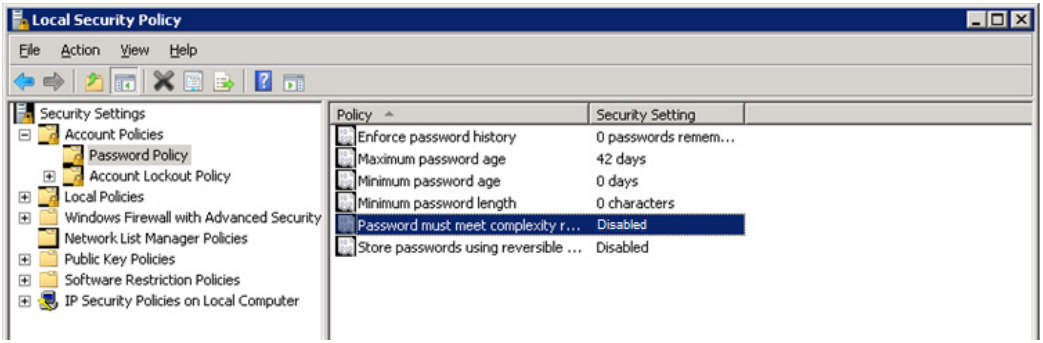


Figure 25 **Complexity requirements**

6. In the **Properties** window, click **Enabled** to enable Password must meet complexity requirements, as shown in Figure 26 on page 71.

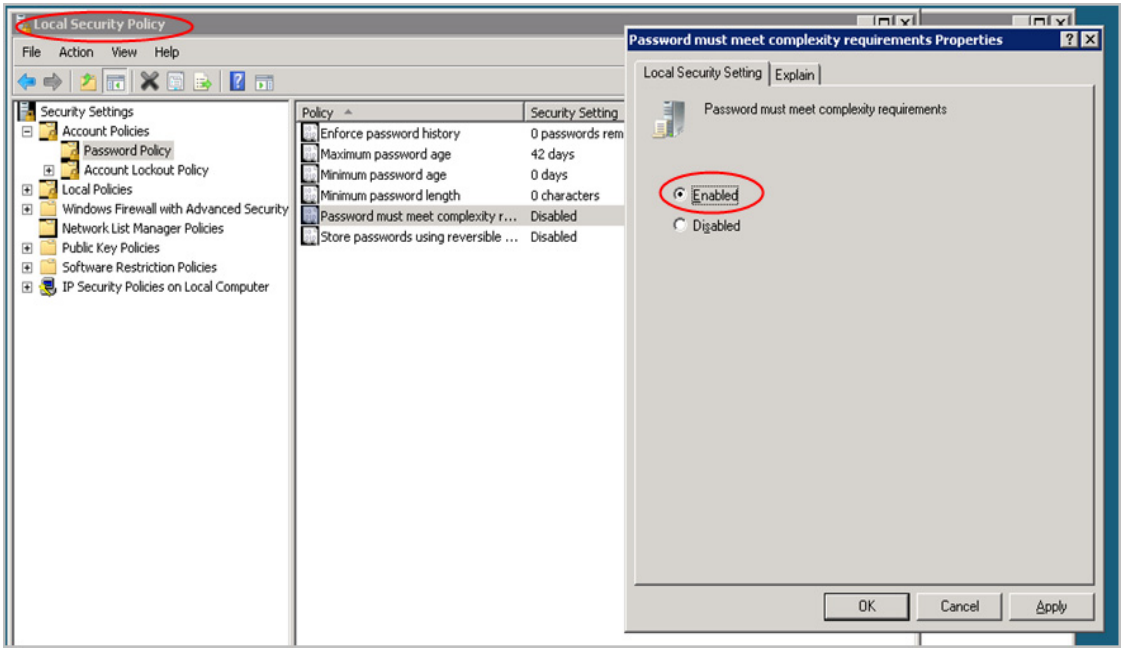


Figure 26 **Enable Local Security setting**

7. Click **OK** to save your selection.
8. Select **File** > **Exit** to close the **Local Security Policy** window.

Your password policies have been restored to their original configuration.

Installing IIS and the FTP service

Now that you have created the IIS user accounts and reset the password policies, you can install IIS and the FTP service.

Beginning the IIS installation

To begin the IIS installation:

1. From the **Start** menu, select **Server Manager**.
2. From the **Roles Summary** section of the **Server Manager** menu, click **Add Roles**, as shown in Figure 27 on page 72.

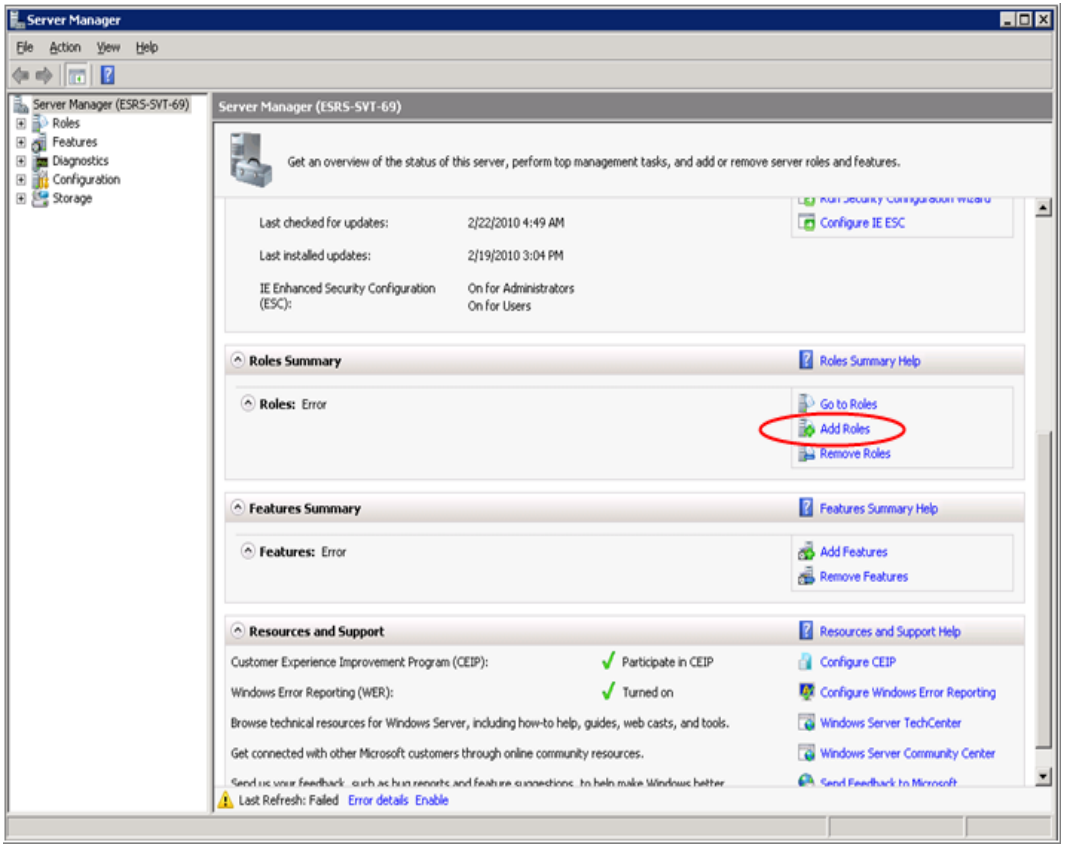


Figure 27 Add Roles

3. One of the following **Add Roles Wizard** windows will appear, depending on whether this is the first time you have added a role:
   - **Before You Begin** window
   - **Select Server Roles** window
4. If the **Before You Begin** window appears:
   a. Read the information in the window.
   b. (Optional) Select **Skip this page by default**.
   c. Click **Next**. The **Select Server Roles** window appears.
5. In the **Select Server Roles** window, select **Web Server (IIS)**, as shown in Figure 28 on page 73.

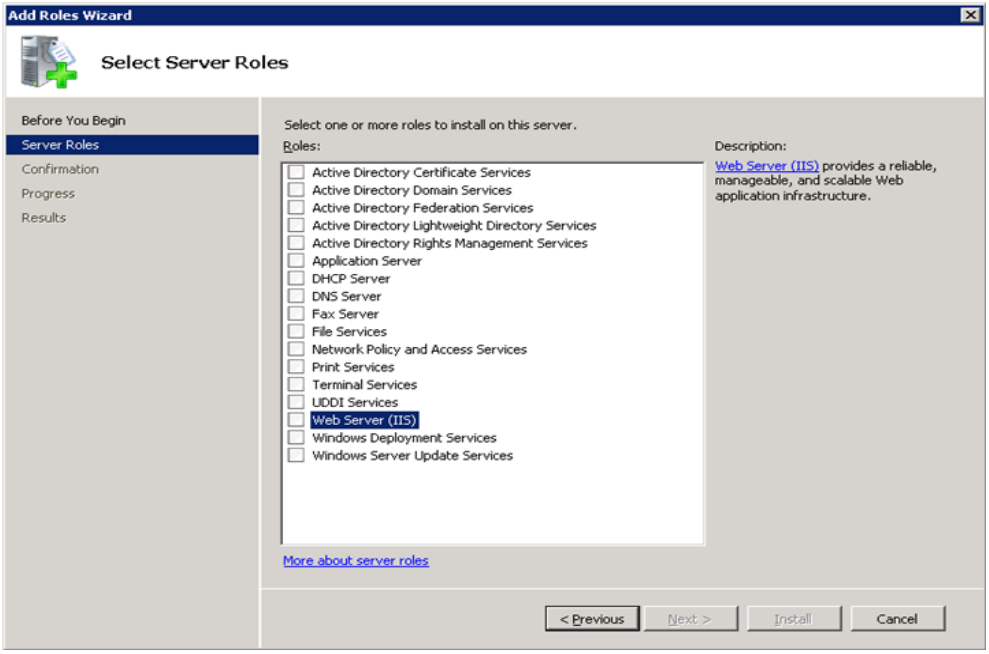


Figure 28 **Select Server Roles—Web Server (IIS)**

6. Click **Next**. The **Add features required for Web Server (IIS)?** window appears, as shown in Figure 29 on page 74.

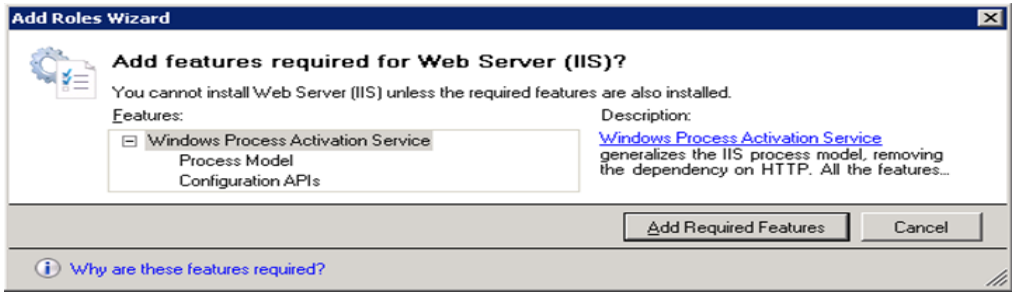


Figure 29 **Add features**

7. Click **Add Required Features**. The **Select Server Roles** window appears.
8. Ensure that **Web Server (IIS)** is selected, as shown in Figure 30 on page 74.

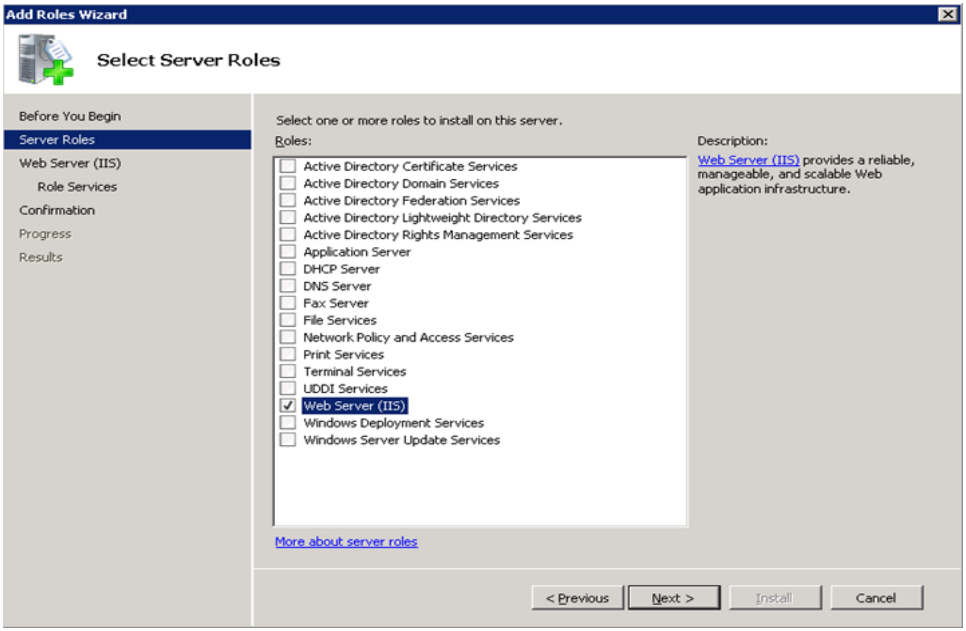


Figure 30 **Web Server (IIS)**

9. Click **Next**. The **Web Server (IIS) introduction** window appears, as shown in Figure 31 on page 75.

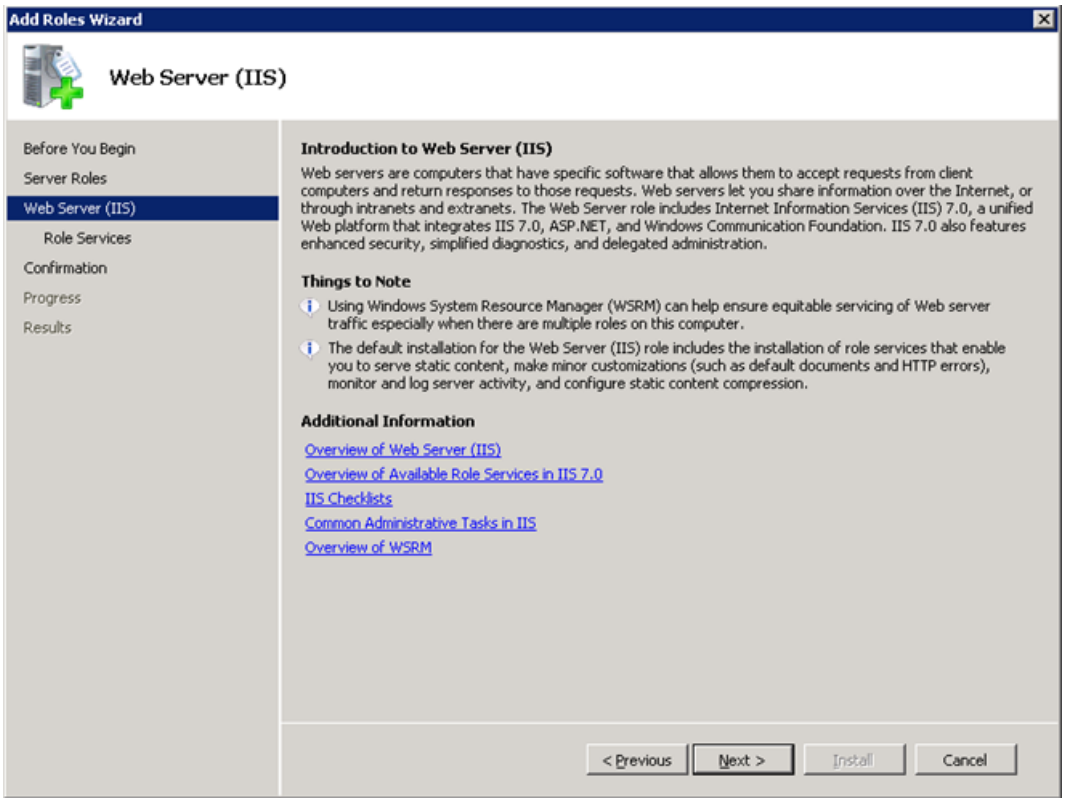


Figure 31 **Web Server (IIS) introduction**

10. Read the information in the **Web Server (IIS) introduction** window and click **Next**. The **Select Role Services** window appears, as shown in Figure 32 on page 76.

Your IIS installation is almost complete. Now you must install role services, including the FTP service.

Installing the FTP service

Take the following steps to install role services, including the FTP service:

1. From the **Select Role Services** window, maintain all of the default selections and select the following additional choices, as shown in Figure 32 on page 76:
   - Select **IIS Management Scripts and Tools** from within the **Management Tools** category.

- Select *all* of the options within the **IIS 6 Management Compatibility** category.
- Select **FTP Server** from within the **FTP Publishing Service** category.

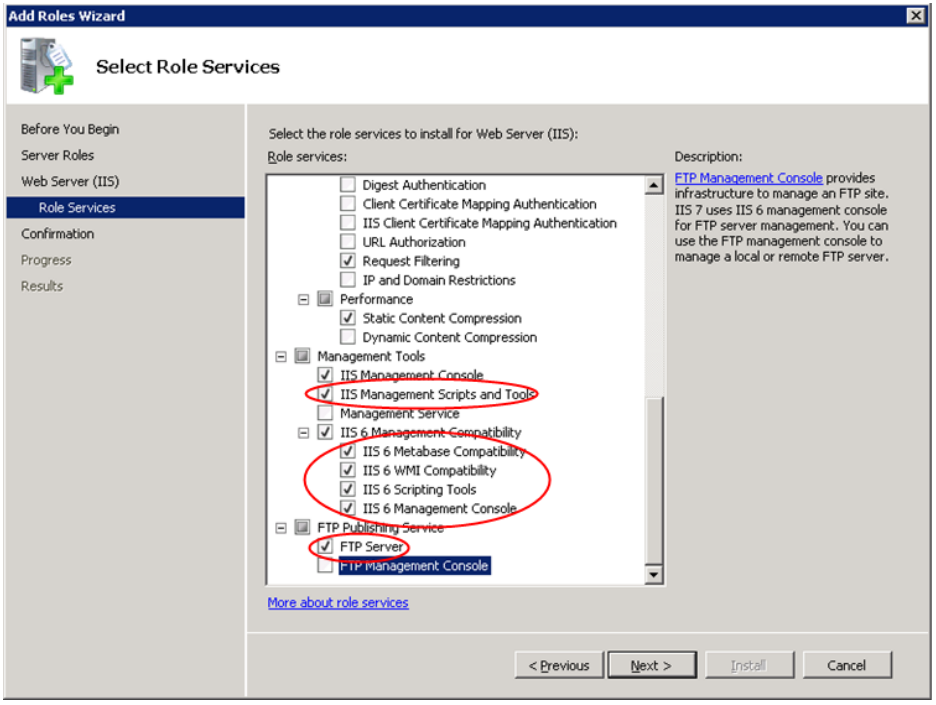


Figure 32 Select Role Services

2. Click **Next**. The **Confirm Installation Selections** window appears, as shown in Figure 33 on page 77.

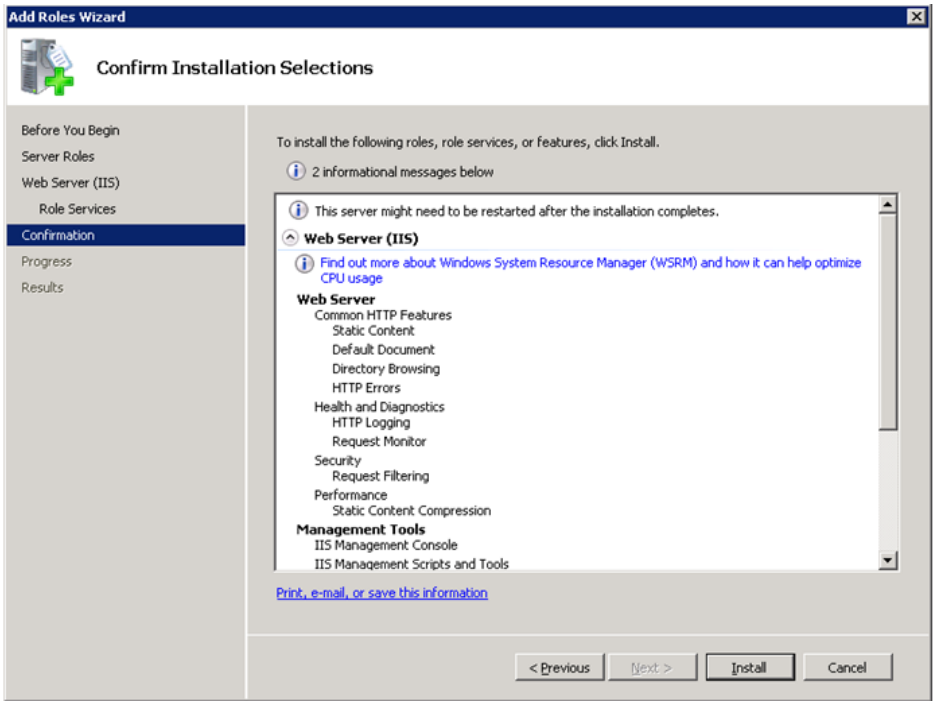


Figure 33 **Confirm Installation Selections**

3. Click **Install**. The **Installation Progress** window appears. A progress bar displays the progress of your installation.
4. If the installation is successful, the **Installation Results** window appears with the message **Installation succeeded**, as shown in Figure 34 on page 78.

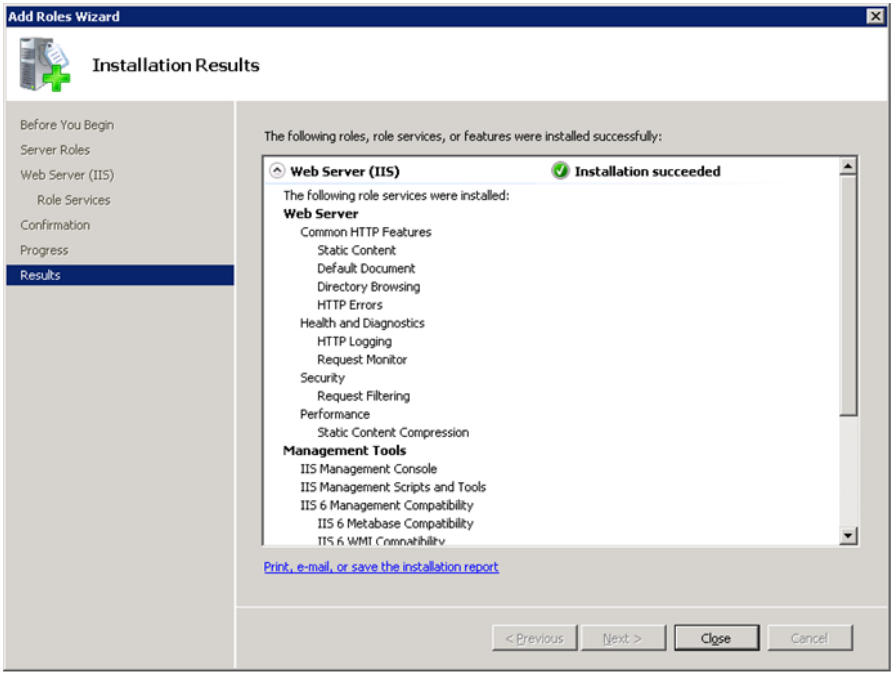


Figure 34 **Installation Results**

5. Review the installation results and click **Close.**

This completes the IIS installation and the FTP service installation. The next task is to install the SMTP service.

Installing the SMTP service

You install the SMTP service from the Server Manager as an SMTP *feature*.

If the Server Manager window is not open:

1. From the main Windows screen, click **Start**.
2. Right-click **Computer**.
3. Click **Manage**. The **Server Manager** window appears, as shown in Figure 35 on page 79.

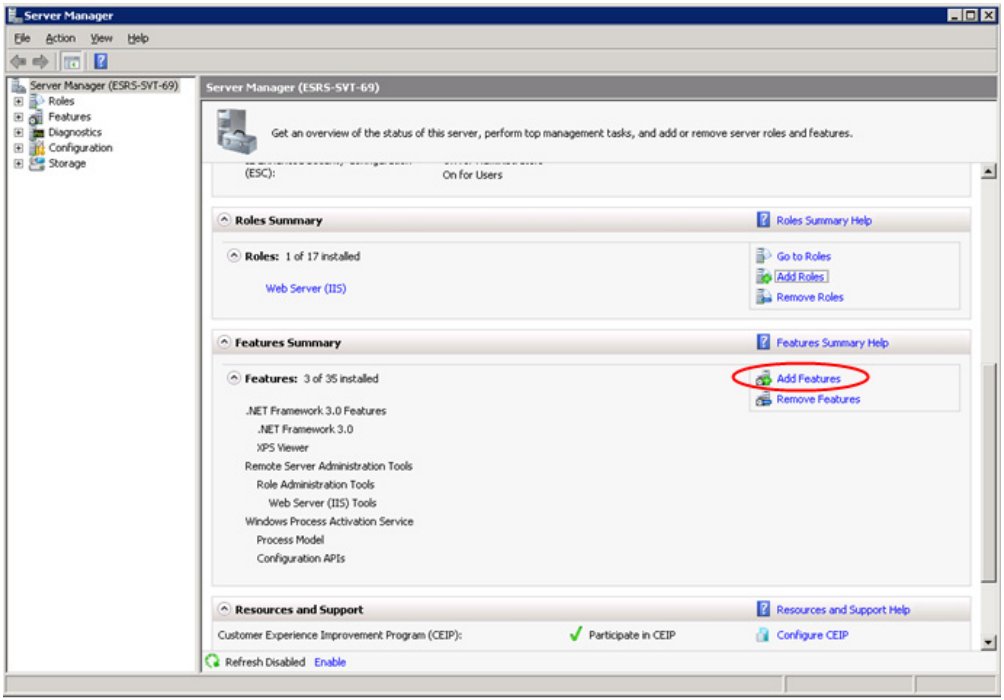


Figure 35 **Server Manager**

To install SMTP:

1. In the **Feature Summary** section of Server Manager, select **Add Features.** The **Select Features** window appears, as shown in Figure 36 on page 80.

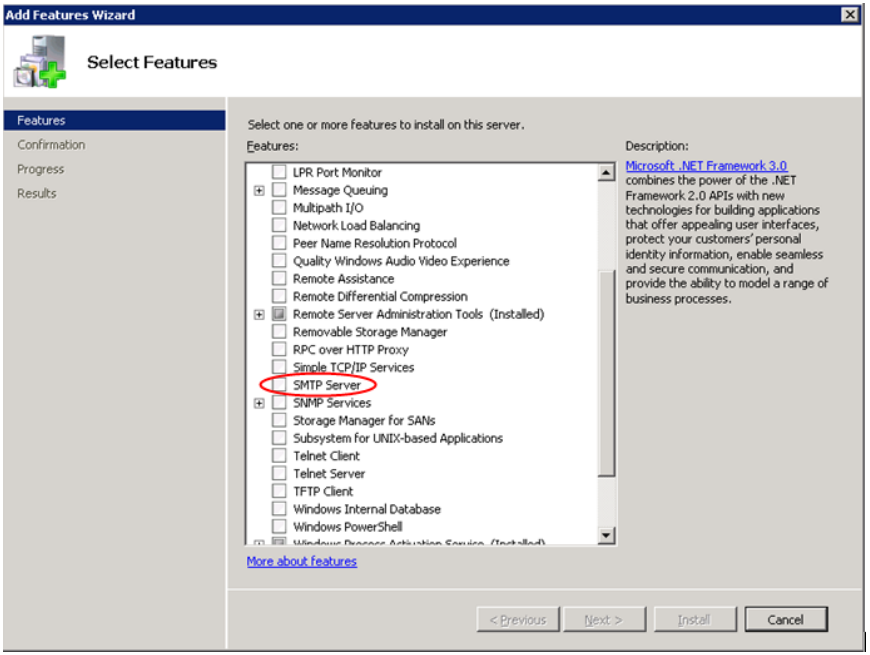


Figure 36 Select Features

2. Scroll down in the **Select Features** window and select **SMTP Server**. The **Add Features Wizard** appears, as shown in Figure 37 on page 80.

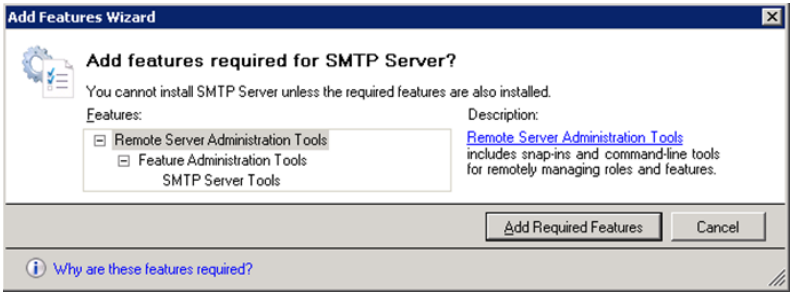


Figure 37 Add Features Wizard

3. In the **Add Features Wizard**, click **Add Required Features**. The **Select Features** window appears, as shown in Figure 38 on page 81.

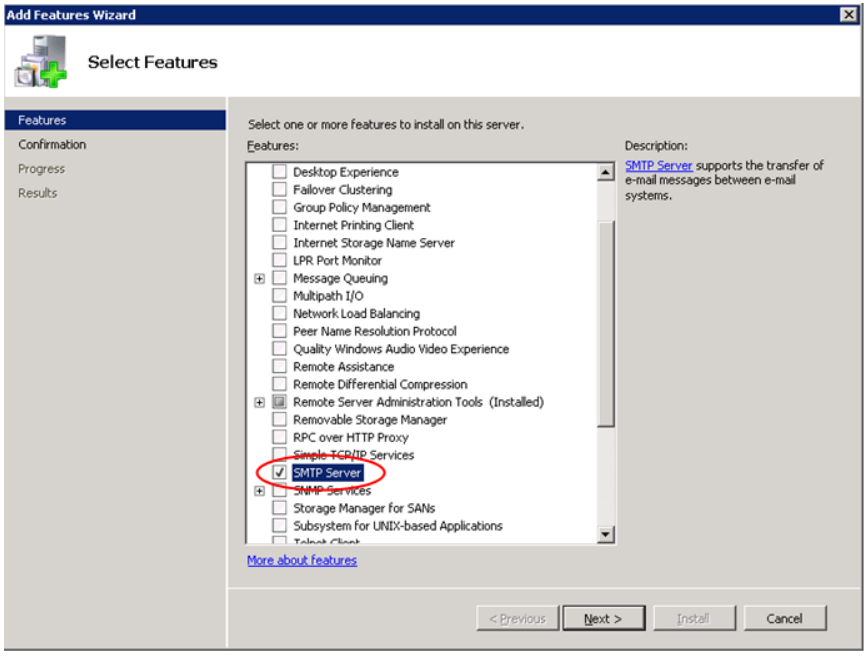


Figure 38 **Select Features—checked**

4. In the **Select Features** window, click **Next**. The **Confirm Installation Selections** window appears.
5. From the **Confirm Installation Selections** window, click **Install**, as shown in Figure 39 on page 82.

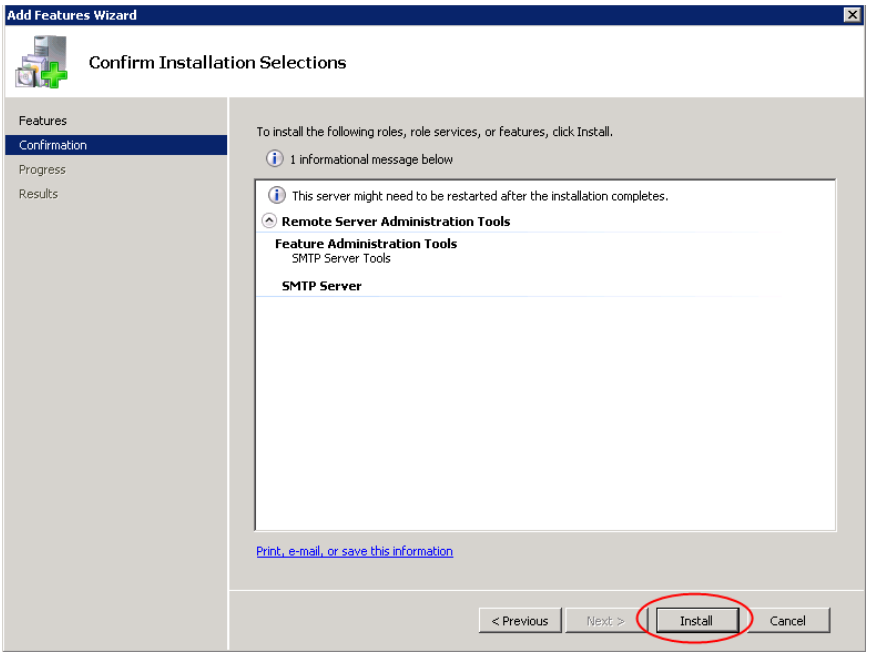


Figure 39 Confirm Installation Selections

After you click **Install,** a progress bar shows the progress of the installation, as shown in Figure 40 on page 83.

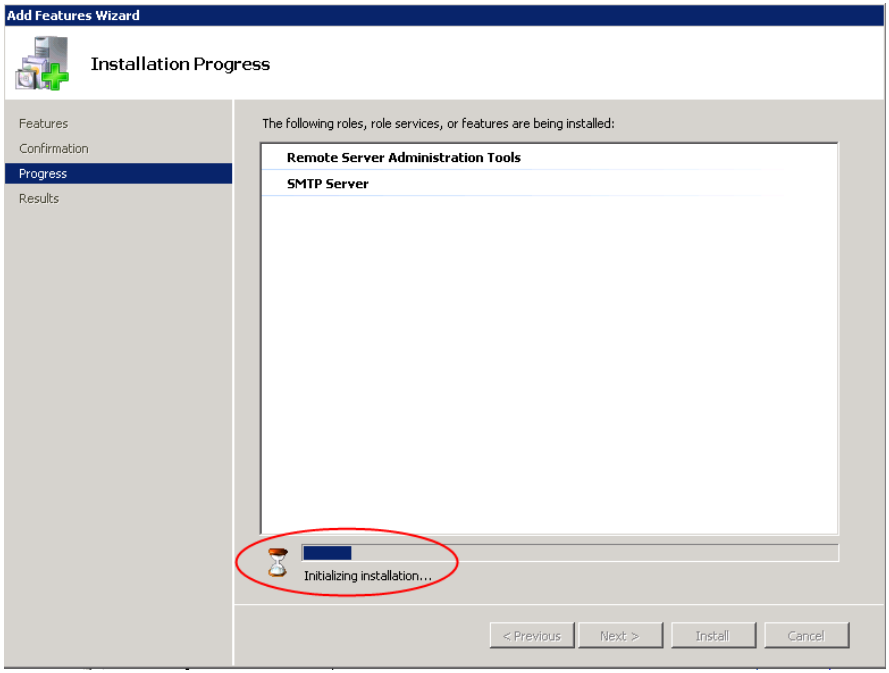


Figure 40 Installation Progress

When the installation is complete, the **Installation Results** window appears, as shown in Figure 41 on page 84.

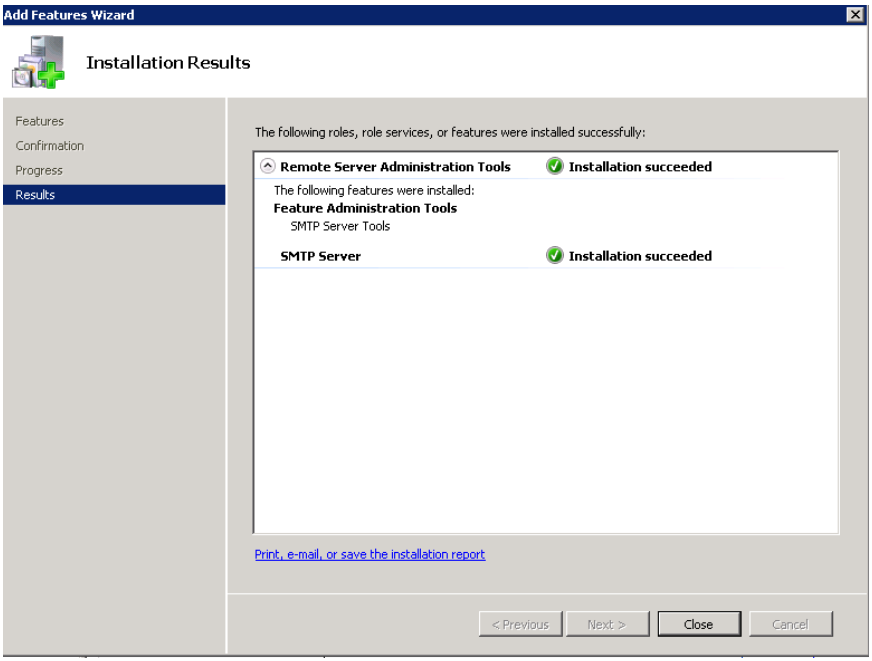


Figure 41 Installation Results

6. From the **Installation Results** window, click **Close**.

   The **Server Manager** window appears, providing an overview of your server status and current roles and features, as shown in Figure 42 on page 85.

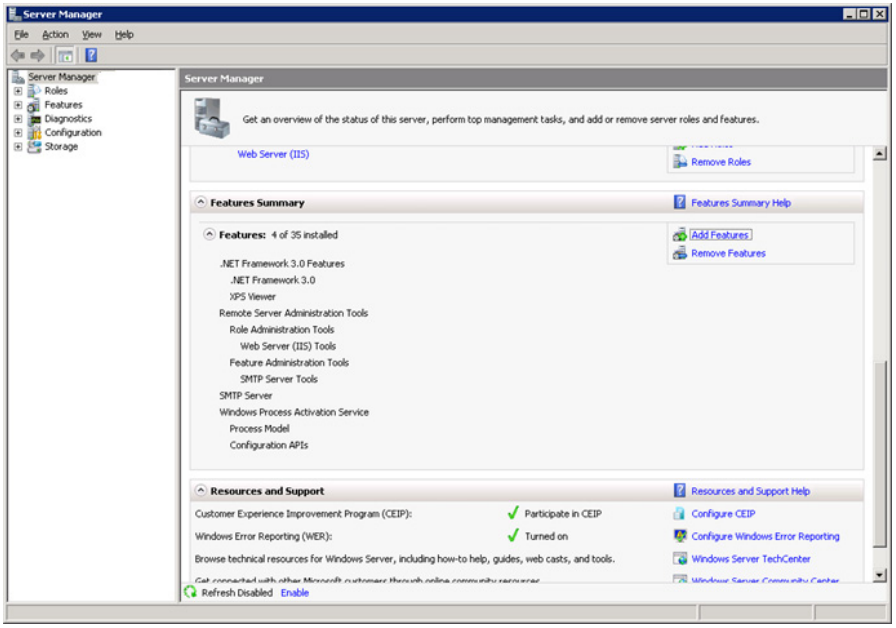


Figure 42 **Server Manager status**

This completes the steps for the SMTP server installation. The next tasks are to configure the SMTP server and the FTP server. The following sections explain how to do this.

Configuring the SMTP server

This section explains how to configure SMTP parameters, including server name, message and session size, domain name, and drop directory.

IMPORTANT

AFTER the ESRS IP Client is installed per CSP2100* IIS MUST be reconfigured to point to <install_drive>:\EMC\ESRS\Gateway\work\mailroot\Drop and <install_drive>:\EMC\ESRS\Gateway\work\mailroot\BadMail

To configure the SMTP server:

1. From the Windows **Start** menu, select **Administrative Tools**. The **Administrative Tools** menu appears.

2. From the **Administrative Tools** menu, select **Internet Information Services (IIS) 6.0 Manager**, as shown in Figure 43 on page 86. The **IIS 6.0 Manager** window appears.

Note: IIS 7.0 uses IIS 6.0 interfaces for SMTP and FTP configuration.

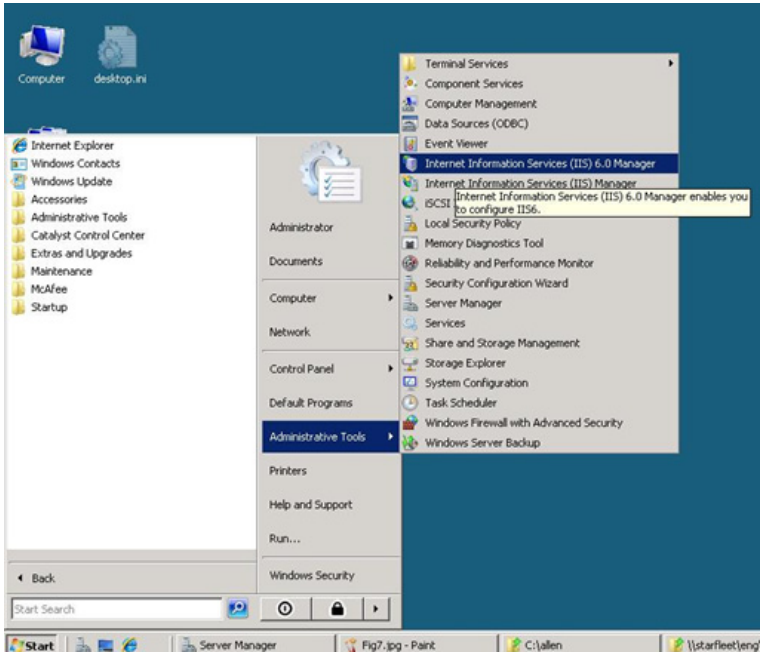


Figure 43 IIS 6.0 Manager

3. Rename **[SMTP Virtual Server]** to **ESRS Gateway SMTP Server**, as shown in Figure 44 on page 87. Do not enclose the new folder name in brackets.

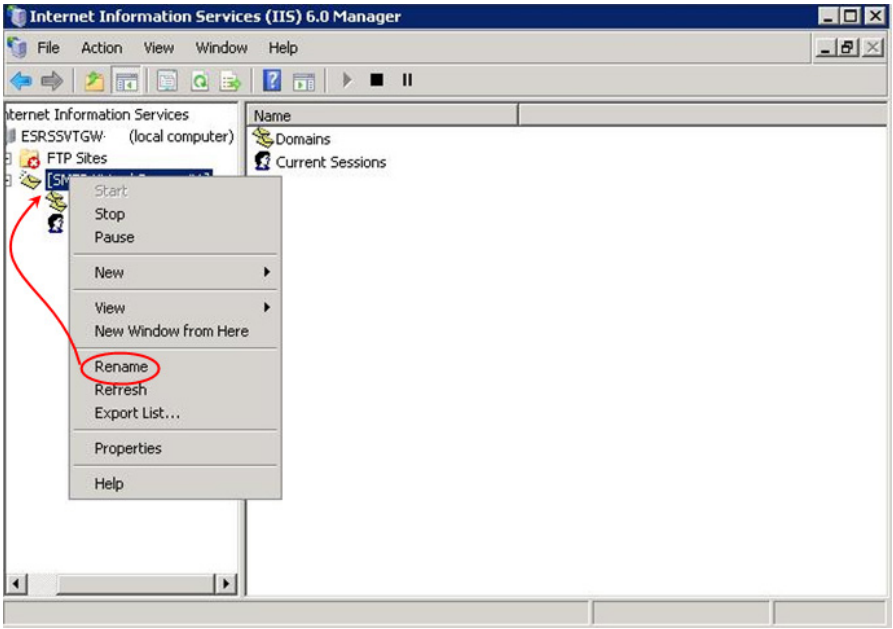


Figure 44 **Rename the folder**

4. Right-click **ESRS Gateway SMTP Server** and select **Properties**. The **ESRS Gateway SMTP Server Properties** window appears.
5. In the **ESRS Gateway SMTP Server Properties** window, click **Messages**.
6. In the **Messages** tab, set the following parameters, as shown in Figure 45 on page 88:
   - Set the **message size limit** to 15000.
   - Set the **session size limit** to 32000.
7. Click **OK** to save the parameters.

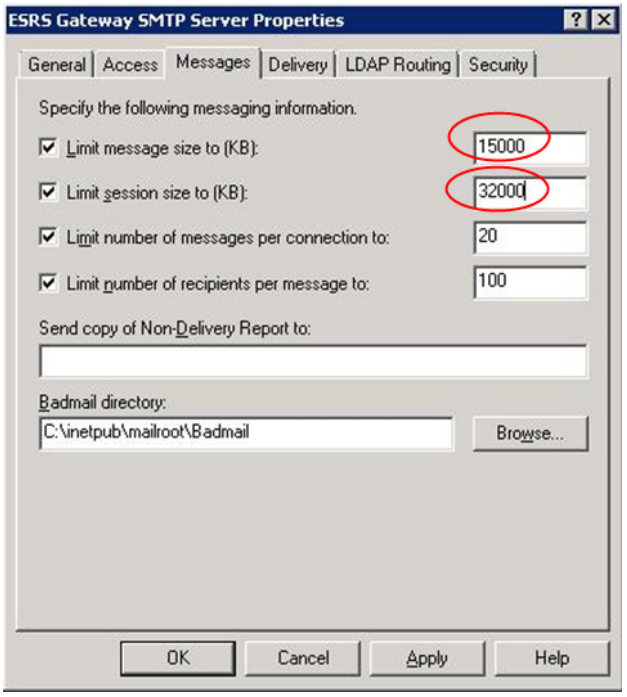


Figure 45 **ESRS Gateway SMTP Server Properties**

8. In the left pane of the IIS 6.0 Manager window, expand the **ESRS Gateway SMTP Server** folder.
9. Click **Domains**. The default domain appears in the right-hand pane.
10. Right-click the default domain and select **Rename**.
11. Rename the default domain to **emc.com**, as shown in Figure 46 on page 89.

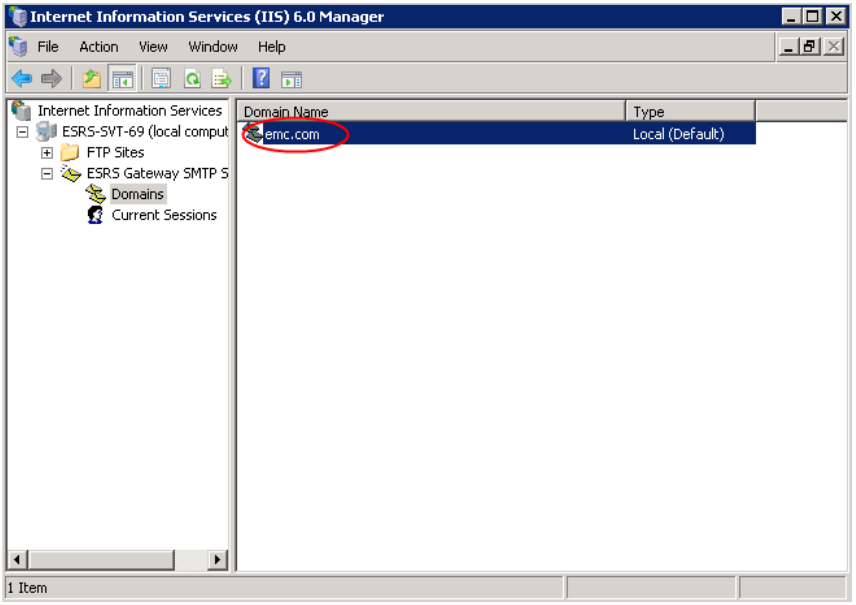


Figure 46 **Rename the default domain**

12. Right-click **emc.com** and select **Properties**. The Properties window appears.
13. Modify the install directory (Drop directory) to correspond to your ESRS installation. For an example, see Figure 47 on page 90.

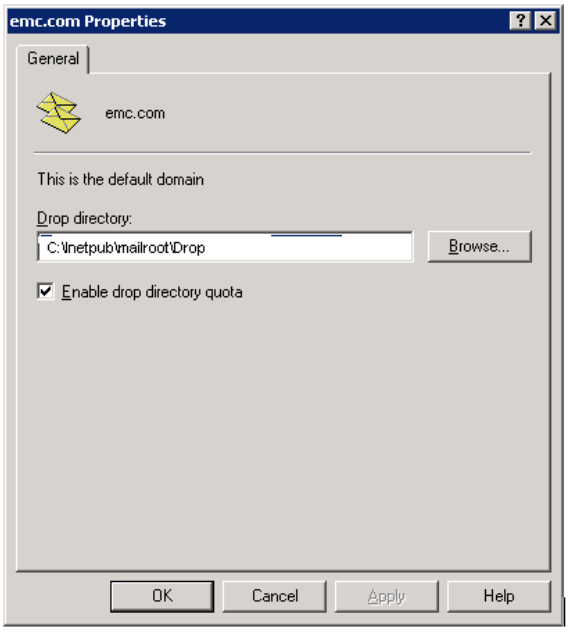


Figure 47 **Drop directory example**

14. Click **OK** to save.

This completes the configuration of the SMTP server. The following section explains how to configure the FTP server.

Configuring the FTP server

This section explains how to configure the FTP (IPv4) server. The procedure is provided here in the following groups of steps:

- "Beginning the FTP server configuration" on page 91
- "Using the FTP Site Creation Wizard" on page 93
- "Continuing the FTP configuration" on page 98
- "Creating optional site messages" on page 102

Beginning the FTP server configuration

To configure the FTP server:

IMPORTANT

AFTER the ESRS IP Client is installed per CSP2100* IIS MUST be reconfigured to point to <install_drive>:\EMC\ESRS\Gateway\work\ftproot

1. From the **Start** menu, select **Administrative Tools**. The **Administrative Tools** menu appears, as shown in Figure 48 on page 91.

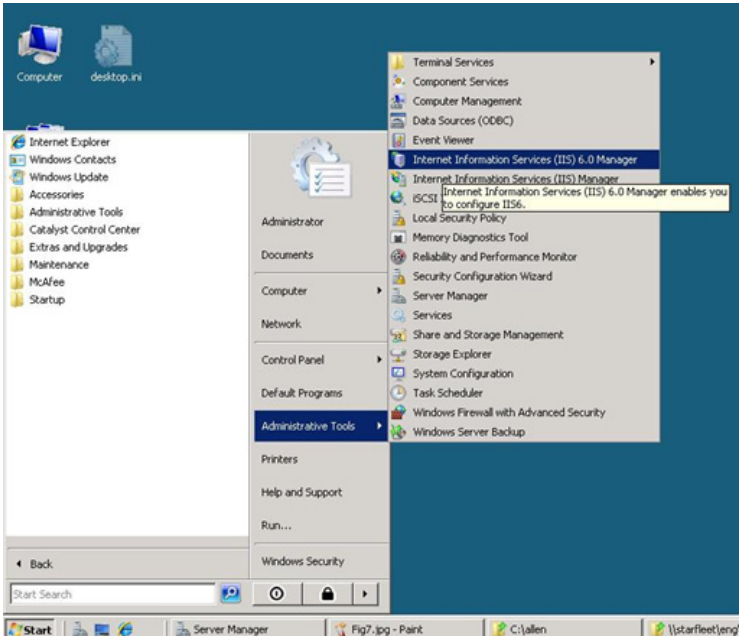


Figure 48 **Administrative Tools menu**

2. From the **Administrative Tools** menu, select **Internet Information Services (IIS) 6.0 Manager**. The **IIS 6.0 Manager** window appears.

Note: IIS 7.0 uses IIS 6.0 interfaces for SMTP and FTP configuration.

3. In the left pane of the **IIS 6.0 Manager** window, expand the folder structure so that the **FTP Sites** folder is visible.
4. Expand the **FTP Sites** folder so that **Default FTP Site** is visible.
5. Right-click **Default FTP Site** and select **Delete**. Confirm the deletion of the file if prompted.

Note: Deleting the default FTP site is an important step. You must delete the default FTP site *before* you create the new FTP site.

6. To create the new FTP site, right-click **FTP Sites**. The FTP Sites menu appears, as shown in Figure 49 on page 92.

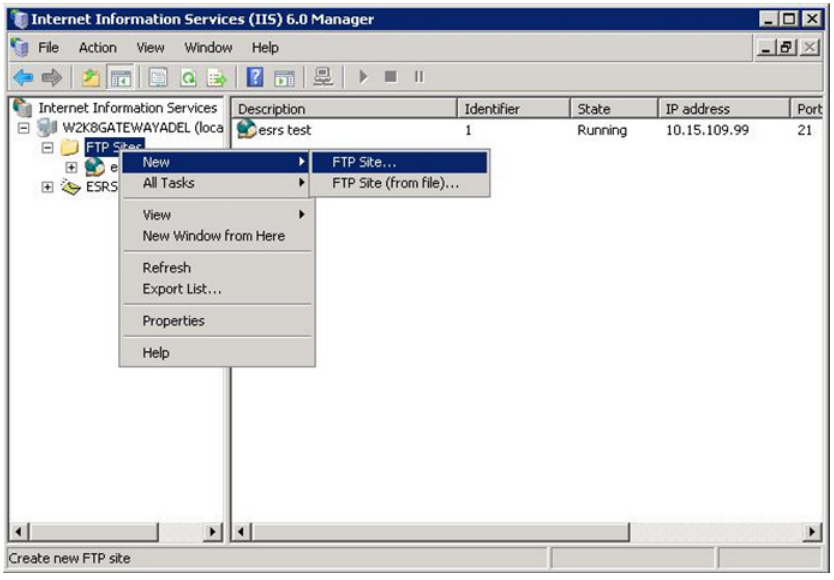


Figure 49 FTP Site

7. Click **New**, then click **FTP Site**. The welcome screen for the **FTP Site Creation Wizard** appears, as shown in Figure 50 on page 93.

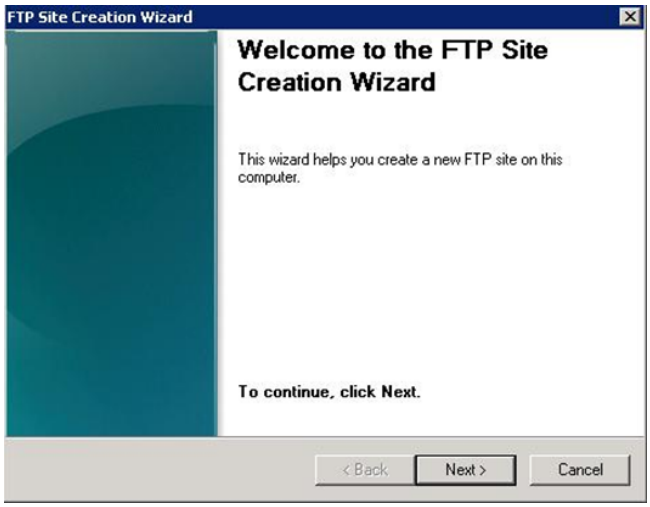


Figure 50 **Welcome screen**

Using the FTP Site Creation Wizard

The previous section, "Beginning the FTP server configuration" on page 91, explained how to invoke the FTP Site Creation Wizard. The following steps explain how to use the wizard to configure an FTP server:

1. From the **FTP Site Creation Wizard** screen, click **Next**. The **FTP Site Description** window appears.
2. In the **FTP Site Description** window, type **EMC** in the **Description**: field, as shown in Figure 51 on page 94.

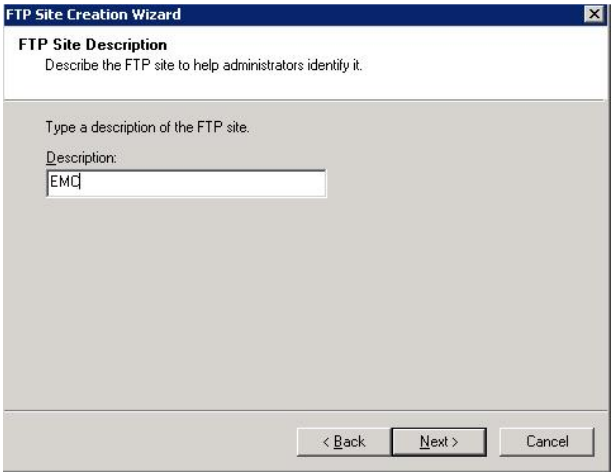


Figure 51 FTP Site Description

3. Click **Next**. The **IP Address and Port Settings** window appears.
4. In the **IP Address and Port Settings** window, enter the following values as shown in Figure 52 on page 95:
   - In the **IP address** field, select **[All Unassigned]** in the drop-down list.
   - In the **TCP port** field, type **21**.

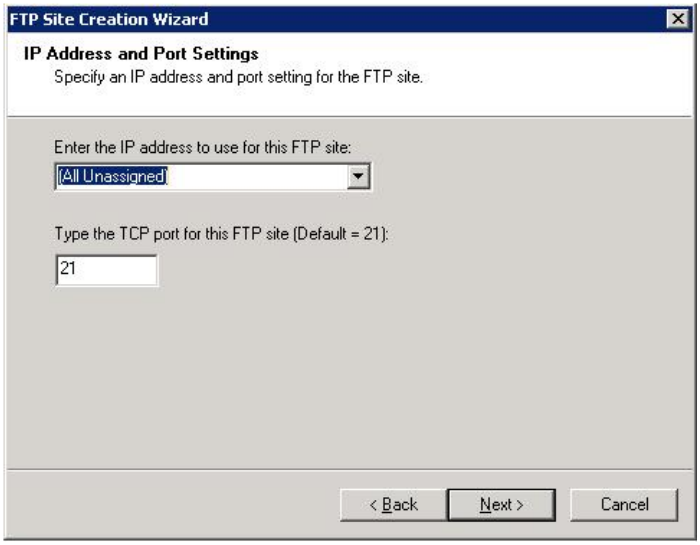


Figure 52 **IP Address and Port Settings**

5. Click **Next**. The **FTP User Isolation window** appears.
6. In the **FTP User Isolation** window, select **Isolate users** and click **Next**, as shown in Figure 53 on page 96. The **FTP Site Home Directory** window appears.

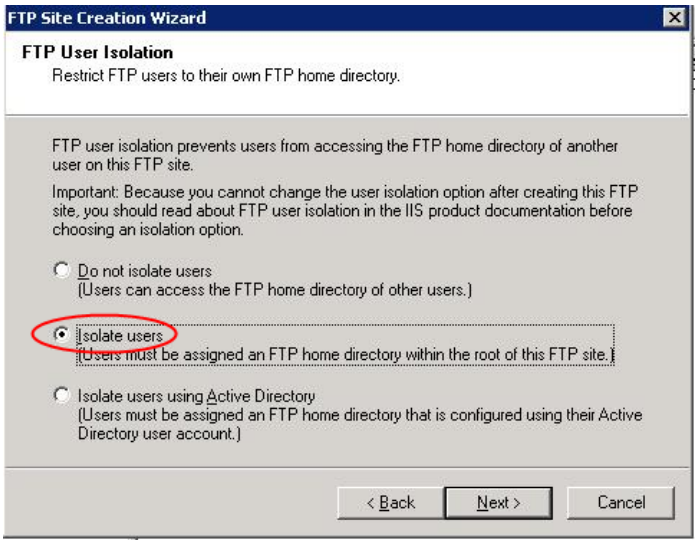


Figure 53 FTP User Isolation

7. In the **FTP Site Home Directory** window, browse to the following path: `C:\inetpub\ftproot`, as shown in Figure 54 on page 96.

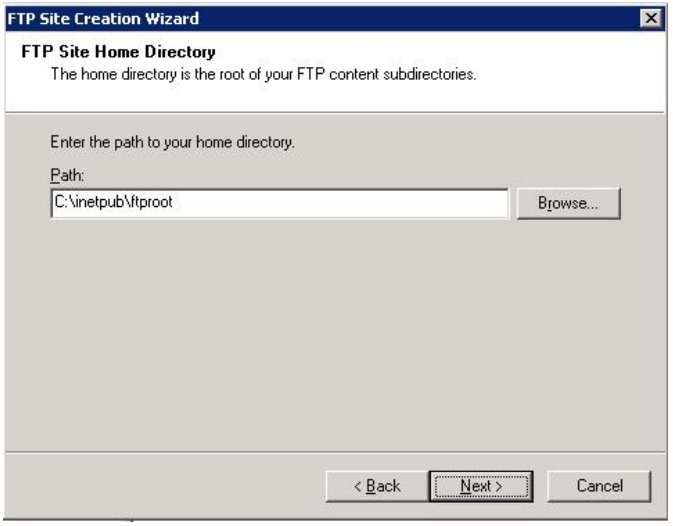


Figure 54 FTP Site Home Directory

8. When you have entered the path, click **Next**. The **FTP Site Access Permissions** window appears.
9. In the **FTP Site Access Permissions** window, select the following permissions, as shown in Figure 55 on page 97:
   - **Read**
   - **Write**

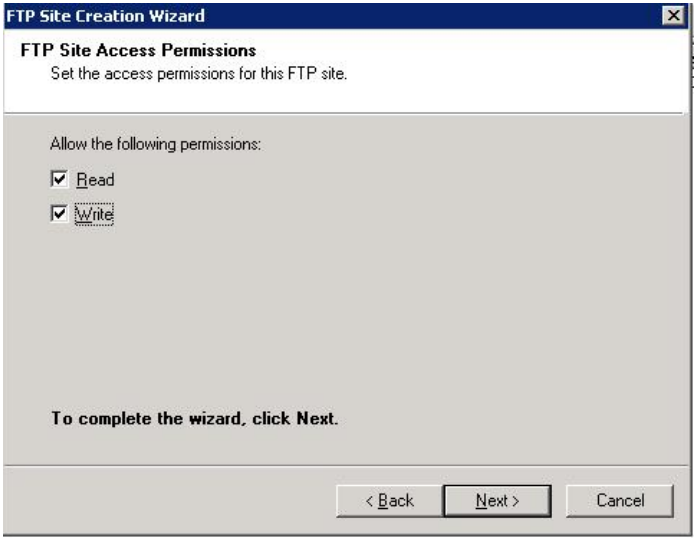


Figure 55 **FTP Site Access Permissions**

10. After you select the Site Access Permissions, click **Next**. The following window appears: **You have successfully completed the FTP Site Creation Wizard**.
11. Click **Finish**.

    This completes the initial FTP server setup. However, there are some additional steps you must take, as described in "Continuing the FTP configuration" on page 98.

Continuing the FTP configuration

Now that you have completed the steps within the FTP Site Creation wizard, you must take the following steps to continue the FTP configuration.

1. From the left pane of the **Internet Information Services (IIS) 6.0 Manager** window, expand the directory structure.
2. From the left-pane directory, right-click **EMC**, which is the name of the FTP server that you created in the previous steps.
3. Select **Properties** from the menu, as shown in Figure 56 on page 98.

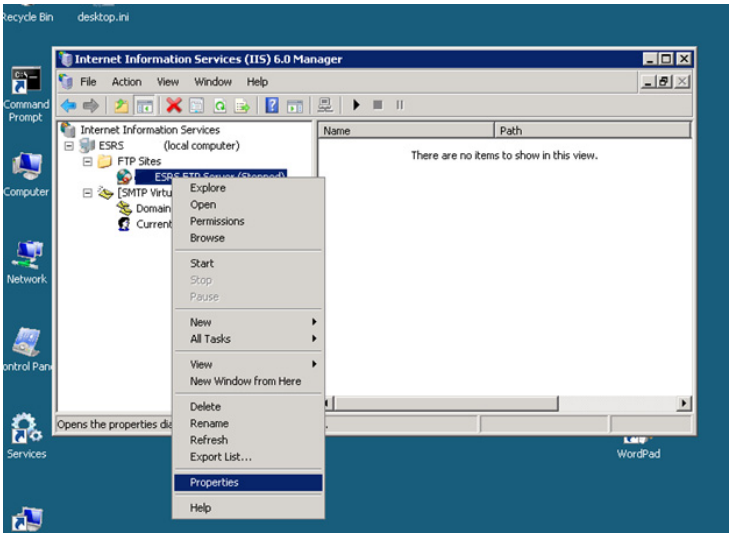


Figure 56 **FTP Server menu**

The **FTP Server Properties** window appears, as shown in Figure 57 on page 99.

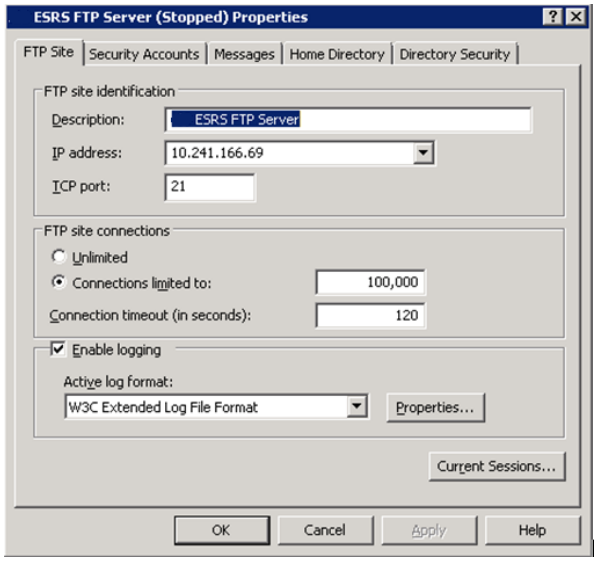


Figure 57 **FTP Site tab**

4. On the FTP site tab assure an IP address is selected (on a multihomed server this should be the internal network IP address.
5. Click **Security Accounts**. The **Security Accounts** tab appears.
6. Clear **Allow anonymous connections**, as shown in Figure 58 on page 100.

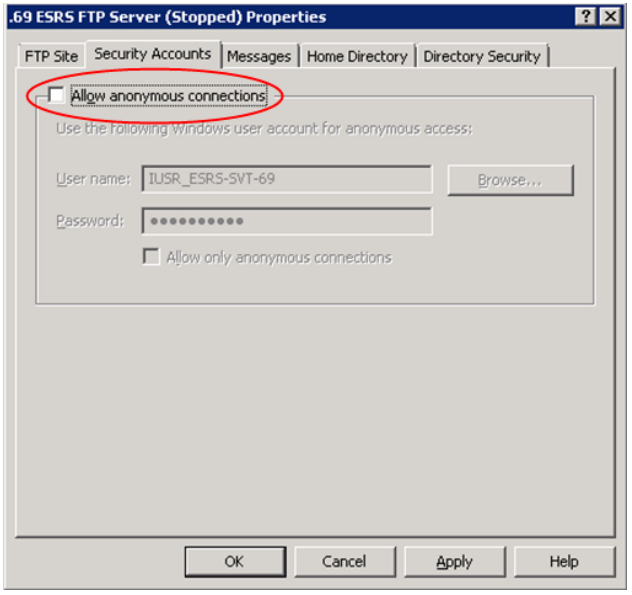


Figure 58 **Clear the Allow anonymous connections checkbox**

7. Click **OK**. An IIS 6 Manager message window appears.
8. In response to the question **Are you sure you want to continue?**, click **Yes**, as shown in Figure 59 on page 100.

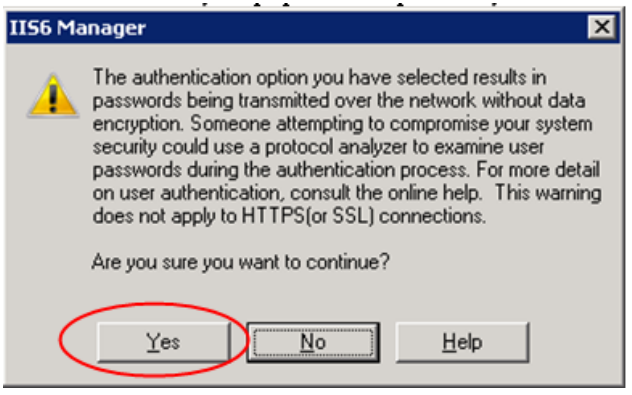


Figure 59 **Authentication option continue**

9. In the **FTP Server Properties** window, click **Home Directory**. The **Home Directory** tab appears.
10. In the **Home Directory** tab, take the following steps, as shown in Figure 60 on page 101:
    a. Verify that the following checkbox is selected: **A directory located on this computer**
    b. In the **FTP site directory** section, verify that the path in **Local path** is correct.
    c. In the **FTP site directory** section, verify that the following checkboxes are selected:
       – **Read**
       – **Write**
       – **Log visits**

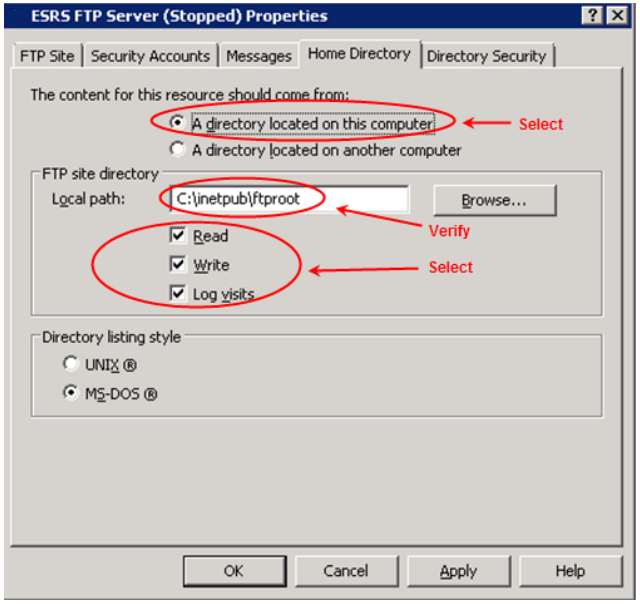


Figure 60 **FTP Server Properties—Home Directory**

11. (Optional) If you want to create site messages, such as welcome and exit messages, follow the instructions in "Creating optional site messages" on page 102.
12. Click **OK** to save your selections.

This completes most of the required FTP configuration steps. You can choose to create FTP site messages, as described in "Creating optional site messages" on page 102.

Creating optional site messages

Take the following steps if you want to create optional FTP site messages, as shown in Figure 61 on page 102.

To create the optional FTP site messages:

1. In the **FTP Server Properties** window, click **Messages**. The **Messages** tab appears.
2. In the **Messages** tab, type messages in the **Banner**, **Welcome**, and **Exit** fields.
3. Click **OK** to save your messages.

For additional information about the Messages tab, click the question mark icon at the top right corner of the Server Properties window, and then click within one of the FTP site message fields.

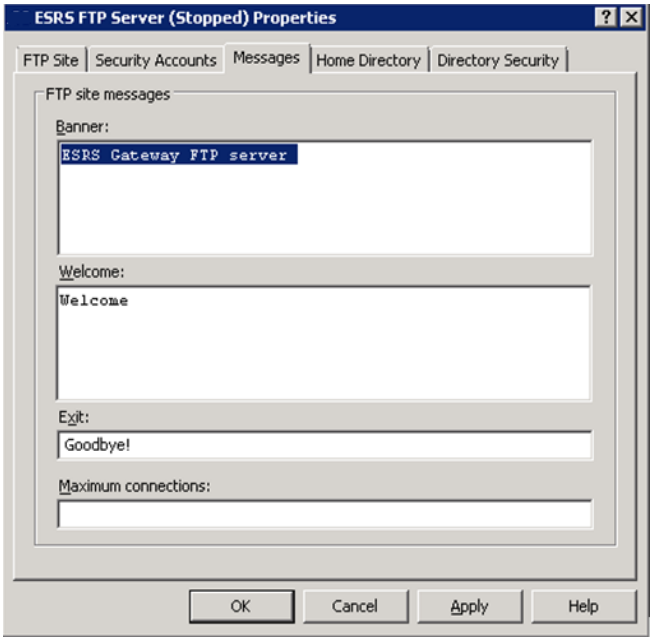


Figure 61 FTP Site messages example

This completes the configuration of your FTP server. Your FTP and SMTP services should look similar to those shown in Figure 62 on page 103.

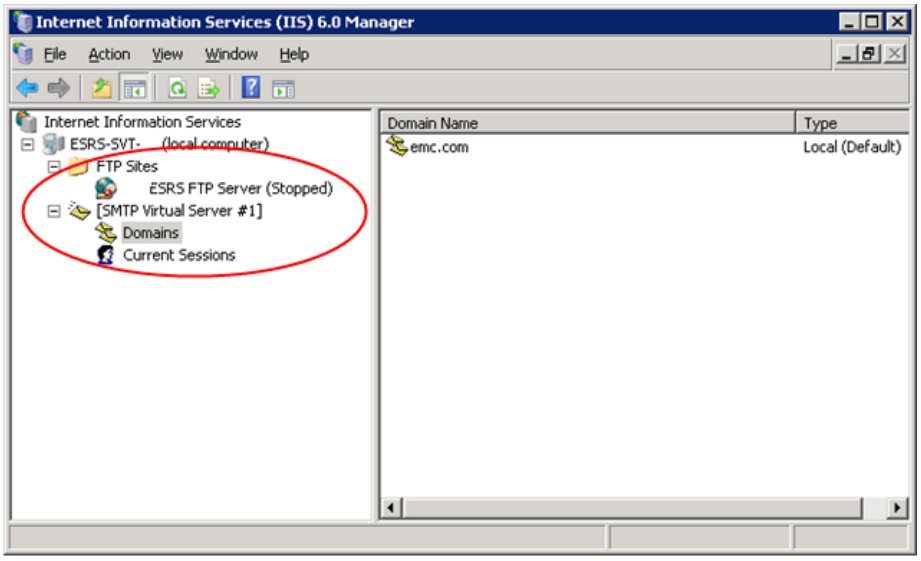


Figure 62 **FTP and SMTP services**

Restarting the FTP and SMTP services

You must execute the following command to restart the SMTP and FTP services so that your configuration will take effect:

1. Open a command prompt.
2. Execute the command **iisreset**, as shown in "Internet services restart" on page 104.

The FTP and SMTP services will restart.

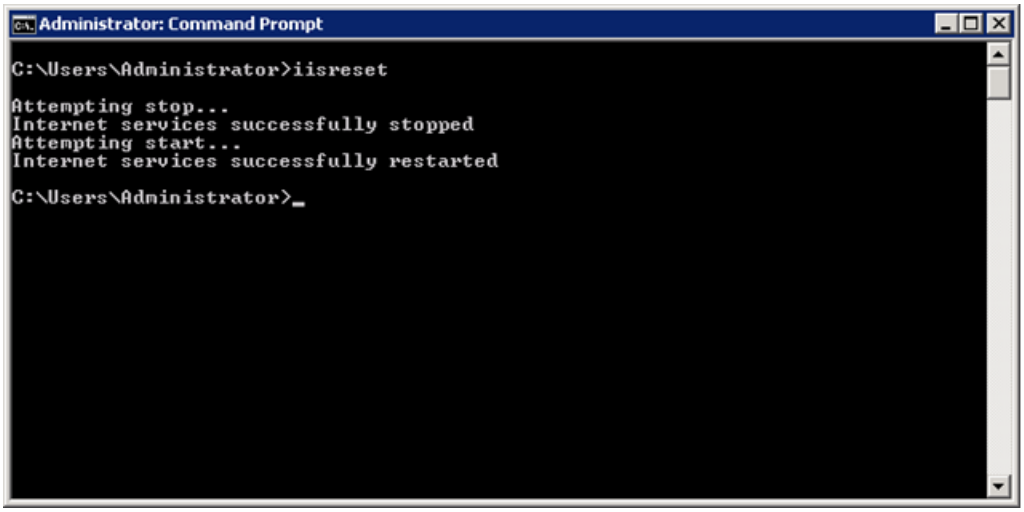


Figure 63 **Internet services restart**

Creating required folders

After you configure and restart the FTP and SMTP services, you must create three new folders.

To create the required folders:

1. Navigate to `C:\Inetpub\ftproot`.
2. Create the following new folders:
   - LocalUser\ESRSConfig
   - LocalUser\OnAlert
   - LocalUser\OnAlert\incoming

You must now start the FTP and SMTP services as described in the following procedure.

Starting the FTP and SMTP services

The FTP and SMTP services are set to manual start mode by default. You can start the services in either of the following two ways.

Starting the service from the IIS 6.0 Manager window

To start the service from the IIS 6.0 Manager window:

1. Click Windows **Start**, then **Administrative Tools** > **Internet Information Services (IIS) 6.0 Manager**.

2. Right-click the FTP or STMP service that you want to start.
3. Click **Start** to start the service, as shown in Figure 64 on page 105.

Starting the service from the Services main window

To start the service from the Services main window:

1. Click Windows **Start**, then **Administrative Tools** > **Services**.
2. Right-click the FTP or STMP service that you want to start.
3. Click **Start** to start the service, as shown in Figure 65 on page 106.

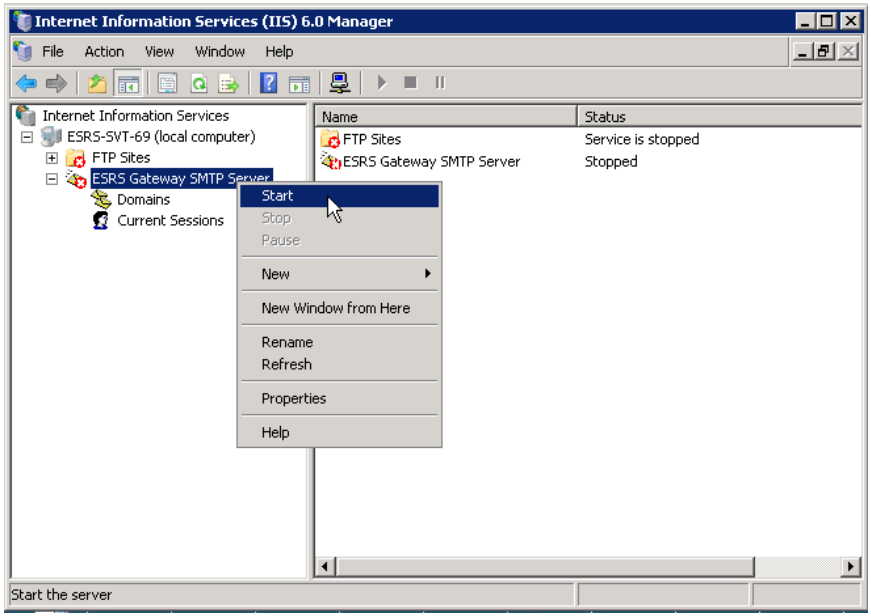


Figure 64 Starting the service from IIS 6.0 Manager

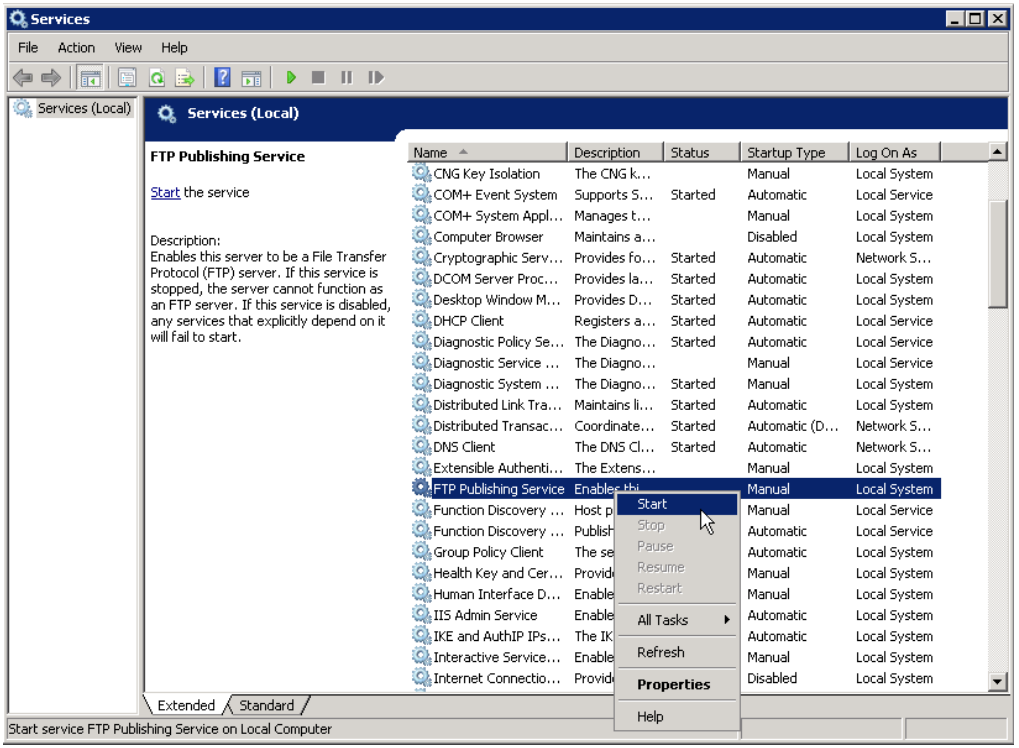


Figure 65 **Starting the service from Services**

Enabling the Write permission for the FTP service

Because Microsoft Windows does not set the permissions correctly on the folders in C:\Inetpub\ftproot\LocalUser, you *must* enable the Write permission at the LocalUser directory level.

To enable the Write permission at the LocalUser directory level:

1. Right-click the **Start** menu and select **Explore**. The Windows Explorer menu opens.
2. Navigate to the following directory:

   `C:\Inetpub\ftproot\LocalUser`

3. Right-click the **LocalUser** directory and select **Properties**, as shown in Figure 66 on page 107. The **LocalUser Properties** window appears.

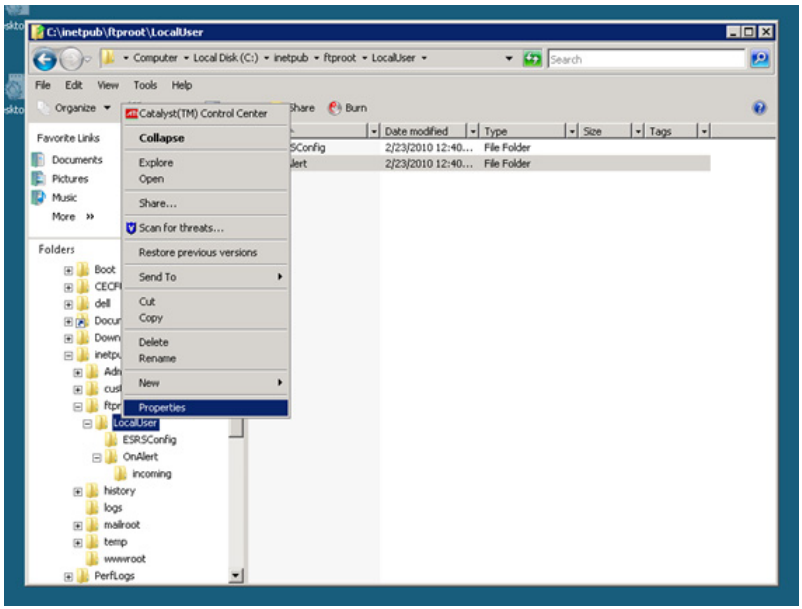


Figure 66 **Navigate to LocalUser Properties**

4. From the **LocalUser Properties** window, click the **Security** tab.
5. In the **Security** Tab, select **Users** in the **Group or user names** section.
6. Click **Edit**, as shown in Figure 67 on page 108. The **Security** tab in the **Permissions for LocalUser** window appears.

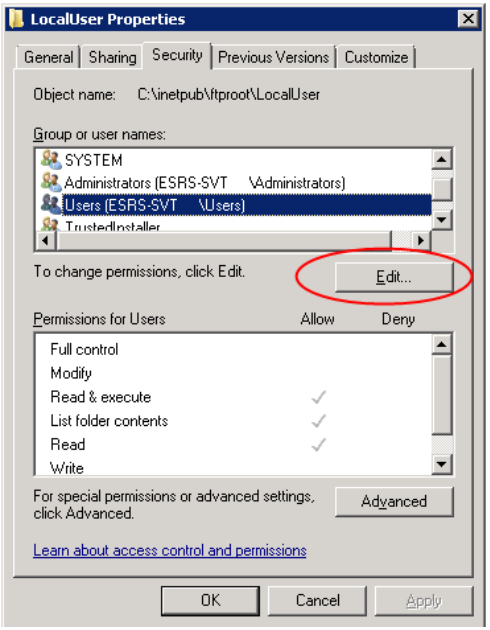


Figure 67 Edit Users

7. In the **Permissions for Users** area of the **Security** tab:
   a. Navigate to the **Allow** column.
   b. Select **Write**, as shown in Figure 68 on page 109.
   c. Click **OK** to save your selection.

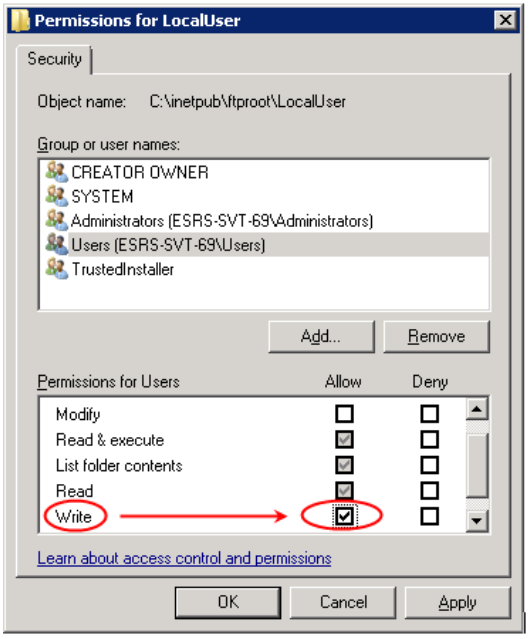


Figure 68 Allow Write

This completes the enablement of the Write permission for the FTP service.

In order to permit incoming communications to the Gateway Server, you must now configure the firewall settings as discussed in "Configuring the Windows 2008 firewall settings" on page 110.

Configuring the Windows 2008 firewall settings

This section explains how to configure the Windows 2008 firewall settings.

If you are running Windows 2008, you *must* configure the Windows Firewall settings to permit incoming communications. Do this by adding the following ports within the Windows Firewall settings:

- Passive FTP ports (ports 5400-5413)
- ESRShttps (port 443)
- ESRS Policy Manager, if installed (ports 8090 and 8443)

To add the required ports:

1. Click **`Start`** > **`Control Panel`** > **`Windows Firewall`**. The **Windows Firewall** window appears.
2. From the **Windows Firewall** window, click **Change Settings**, as shown in Figure 69 on page 110. The **Windows Firewall Settings** window appears.

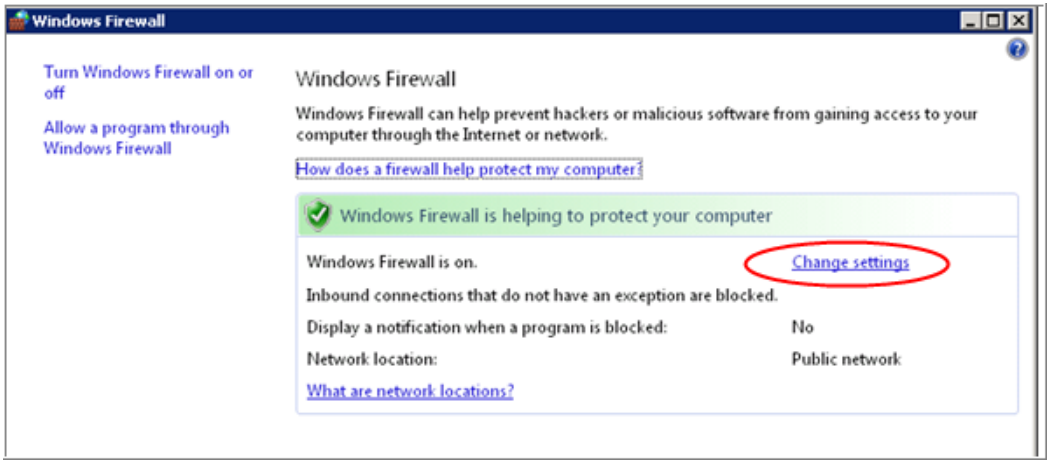


Figure 69 **Windows Firewall—Change settings**

3. From the **Windows Firewall Settings** window, click **Exceptions.** The **Exceptions** tab appears.

4. In the **Exceptions** tab, click **Add Port**, as shown in Figure 70 on page 111. The **Add a Port** window appears.

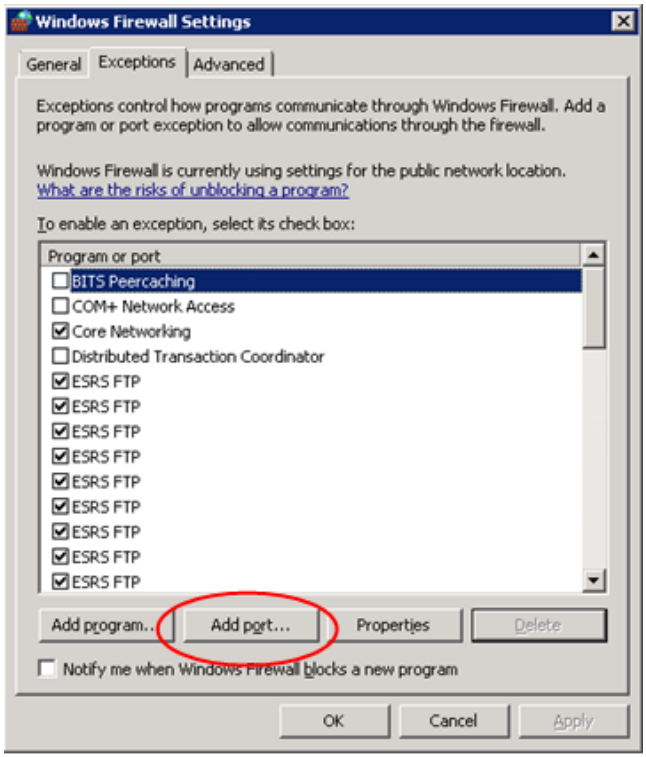


Figure 70 **Add port**

5. In the **Add a Port** window, type the applicable name and port number in the **Name** and **Port Number** fields, and click **OK**. An example is shown in Figure 71 on page 112.

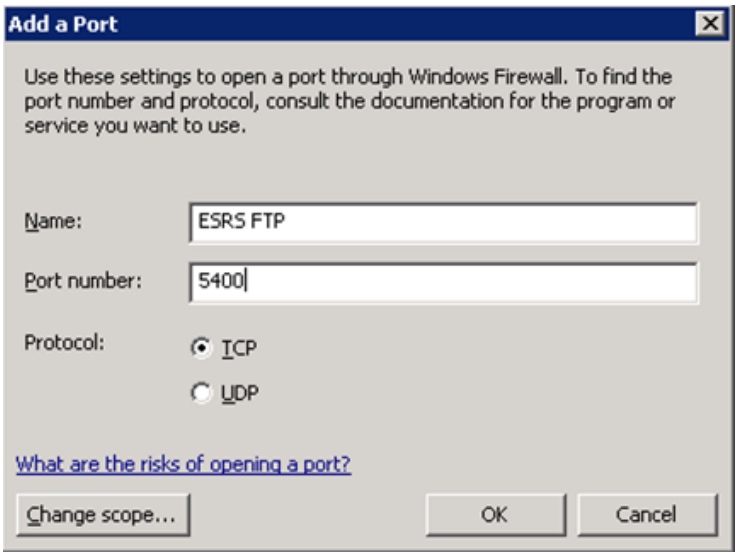


Figure 71 **Name and Port number example**

6. Repeat this procedure to add the following ESRS ports:
   - Passive FTP ports (ports 5400-5413)
   - ESRShttps (port 443)
   - ESRS Policy Manager, if installed (ports 8090 and 8443)

For an example of a Windows Firewall Settings window that shows many enabled ESRS FTP ports, refer to Figure 72 on page 113.

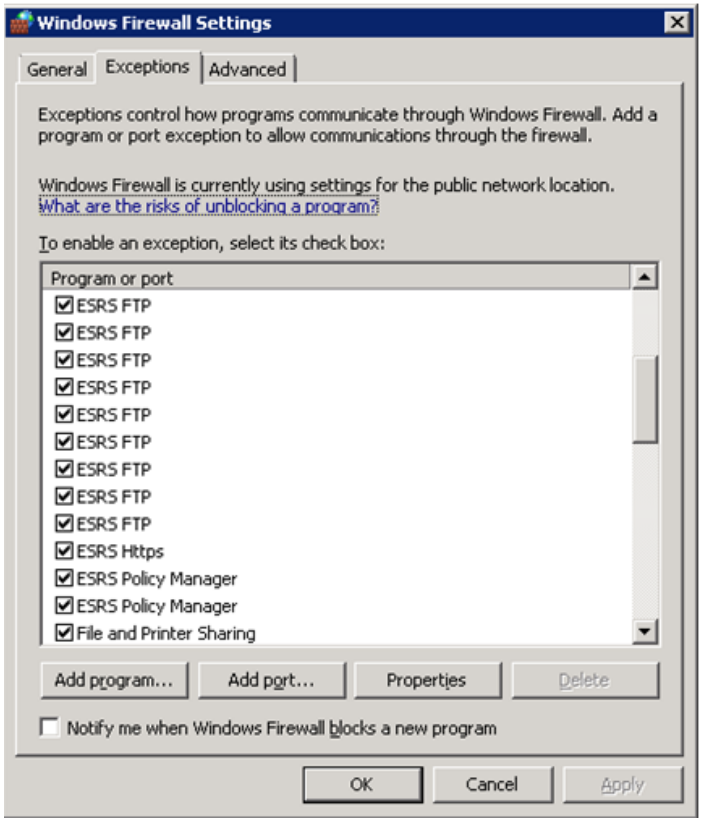


Figure 72 **Inbound ESRS ports example**

Testing the Windows 2008 firewall

After you configure the firewall settings as explained in "Configuring the Windows 2008 firewall settings" on page 110, perform the following tests to check connectivity and functionality:

1. If you have already installed the Gateway Client software, stop the Gateway and Watchdog services.
2. Ensure that the FTP and SMTP services are running.
3. Run the following tests:
   - Test that a device can connect home by FTP, as described in "Testing FTP server functionality" on page 114.
   - Test that a device can connect home via SMTP, as described in "Testing SMTP from another host" on page 116.
   - From a different host, test connectivity to the Policy Manager if it is installed on a Windows 2008 server with a browser.
4. After you have finished testing, restart the Watchdog service. The Watchdog service will automatically start the Gateway Service. It will also restart the FTP and SMTP services.
5. Proceed with the Gateway Client installation. If a Policy Manager is installed, you must then configure Windows Firewall to permit inbound traffic on ports 8090 and 8443.

Testing FTP server functionality

The following steps explain how to test that the FTP server is functioning correctly.

1. Open a command window and FTP to the server's IP address.
2. Log in using the OnAlert credentials.
3. Verify that user isolation is configured correctly, as described in "Configuring the FTP server" on page 90.
4. Verify that anonymous connections are not allowed. The correct configuration is described in "Configuring the FTP server" on page 90.
5. Verify that you can write a file to the incoming directory:

```
C:\Users\Administrator\Documents>ftp 10.241.166.69
Connected to 10.241.166.69.
220-Microsoft FTP Service
```

```
220 ESRS Gateway FTP server
User (10.241.166.69:(none)): Onalert
331 Password required for Onalert.
Password:
230-Welcome
230 User Onalert logged in.  <<< log on test
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
02-23-10  12:40PM       <DIR>          incoming
226 Transfer complete.
ftp: 49 bytes received in 0.00Seconds 49000.00Kbytes/sec.
ftp> cd /<<<< Test for User Isolation and No Anonymous
connections.
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
02-23-10  12:40PM       <DIR>          incoming
<<< Did not go above user's directory
226 Transfer complete.
ftp: 49 bytes received in 0.00Seconds 49000.00Kbytes/sec.
ftp> quote pasv   << Check passive ports.
227 Entering Passive Mode (10,241,166,69,192,254).
<<<<<The passive port is 49406. This will be changed
during code install.
ftp> cd incoming
250 CWD command successful.
ftp> pwd
257 "/incoming" is current directory.
ftp> !dir
 Volume in drive C has no label.
 Volume Serial Number is 5AD2-9404

 Directory of C:\Users\Administrator\Documents

02/23/2010  12:53 PM    <DIR>          .
02/23/2010  12:53 PM    <DIR>          ..
02/23/2010  12:53 PM                18 test.txt
               1 File(s)             18 bytes
               2 Dir(s)  29,164,433,408 bytes free
ftp> mput te*
mput test.txt? y
200 PORT command successful.
150 Opening ASCII mode data connection for test.txt.
226 Transfer complete.
ftp: 18 bytes sent in 0.00Seconds 18000.00Kbytes/sec.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
02-23-10  01:23PM                   18 test.txt
226 Transfer complete.
```

```
ftp: 49 bytes received in 0.00Seconds 49000.00Kbytes/sec.
ftp> bye
221  Goodbye!
```

Testing SMTP from another host

The following instructions explain how to test SMTP from another host.

Note: Windows 2008 does not have a Telnet client.

To test SMTP from another host:

1. Enter test commands as shown in the example in Figure 73 on page 117.

Command that you enter [bold]
Response that you receive [plain]

```
telnet ip_address 25

220 jerry.lab.pvt.dns Microsoft ESMTP MAIL Service,
Version: 6.0.3790.1830 ready at  Thu, 25 Jan 2007
15:20:31 -0500

vrfy onalert

252 2.1.5 Cannot VRFY user, but will take message for
<onalert@emc.com>

helo

250 jerry.lab.pvt.dns Hello [192.1.7.203]

mail from:esrs@emc.com

250 2.1.0 esrs@emc.com....Sender OK

rcpt to:onalert@emc.com

250 2.1.5 onalert@emc.com

data

354 Start mail input; end with <CRLF>.<CRLF>

subject:testemailserver<CR>
This is a test of the email server<CR>
.<CR>

250 2.6.0
<JERRYexICnDdNUbr6TU00000001@jerry.lab.pvt.dns> Queued
mail for delivery
```

Figure 73 **E-mail server test**

2. Return to the directory:

   ```
   C:\Inetpub\mailroot\drop
   ```

3. Right-click a message file in the directory.
4. Select **Open with** > **Notepad**. The e-mail message opens.
5. Review the e-mail message, as shown in Figure 74 on page 118.

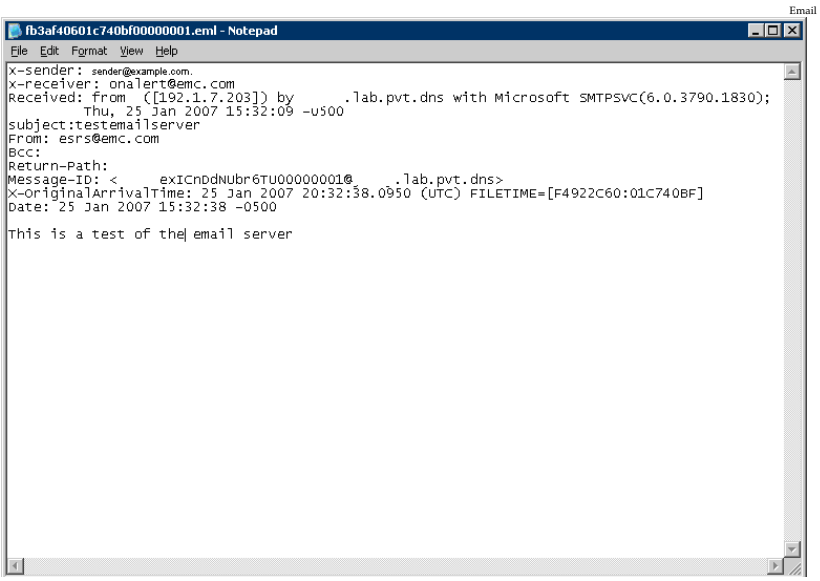


Figure 74 E-mail server test

6. Close the e-mail.
7. Delete the e-mail from the directory.

This completes this test.

PART 2

Management Tools

The ESRS IP Solution includes management tools to help you install and manage the solution components.

Chapter 3, "Customer Environment Check Tool"

This chapter describes how to run the Customer Environment Check Tool (CECT) to verify that your systems are ready for installation of the ESRS IP software.

Chapter 4, "Configuration Tool"

This chapter describes how to use the Configuration Tool to view Gateway Client status, manage devices for a Gateway Client, and perform other tasks related to the configuration of your ESRS IP solution.

3 Customer Environment Check Tool

This chapter provides instructions on installing and running the Customer Environment Check Tool (CECT). The CECT verifies that a candidate server meets the hardware, software, and network configuration requirements for successful Gateway Client and Policy Manager software installation.

Topics in this chapter include:

Customer Environment Check Tool overview

The ESRS IP solution has specific requirements for the hardware, software, and network configurations of the customer-supplied Gateway Client and Policy Manager servers. If a Gateway Client or Policy Manager server does not meet one or more of the requirements listed in Table 5 on page 123, various problems may occur during and after ESRS IP software installation.

The Customer Environment Check Tool (CECT) is provided on the ESRS IP Solution CD (model number ESRS-GW-200). The CECT tool tests candidate Gateway Client and Policy Manager servers to verify that each server meets all the configuration requirements necessary for successful ESRS IP software installation.

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

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

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

Note: You must install and run the CECT application on every Gateway Client and Policy Manager server. You must verify that each server passes the required CECT tests *before* your ESRS IP installation date.

Note: The Microsoft .NET Framework 2.0 (or a newer version that is backward compatible with 2.0) must be installed and functioning for CECT to function correctly.

.NET3.5 and .NET4.0 are incompatible with the proper operation of ESRS IP Client and associated support applications. That may result the Client and Applications to stop functioning or fail to perform as designed.

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

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

Required CECT test resolution

Note: To Use Customer Environment Check Tool on Windows 2008 it may be necessary to "Run As Administrator" to have the tool perform properly.

The CECT checks that your Gateway Client server and Policy Manager server and their environments meet specific requirements. The CECT requirements are a subset of the complete requirements of the Gateway Client and Policy Manager servers.

To successfully run the Gateway Client and Policy Manager software installation program, each target server *must* pass the tests required for its server type, as specified in Table 5 on page 123. If any required tests show a **Failed** status, you must resolve those failures *before* your ESRS IP installation date.

Note: If the Client and Policy Manager are to be co-located on a single server, the target server must pass the required tests for *both* server types.

Table 5 CECT test failure resolution (page 1 of 3)

Test name	Notes
Gateway Environment Tests	*Required tests must pass on Gateway Client server*
Memory	*Required*: At least 1 GB RAM NOTE: If Collocating Policy Manager with ESRS IP Client, 3 GB of memory is recommended.
Comm	*Required*: Two (dual) 10/100 Ethernet adapters (NIC cards), 1 Gb preferred
Free Disk Space	*Required:* At least 1 GB
Processor Speed	*Required:* Each processor at least 2.2 GHz total speed (one or more processors). NOTE: CPU must support SSE2.Instruction Set.

Table 5 CECT test failure resolution (page 2 of 3)

Test name	Notes
Operating System	*Required (US English only supported):* • Windows Server 2003 R2, 5.2, 32 bit • Windows Server 2003, 5.2, 32 bit or 64 bit • Windows Server 2008, 6.0, 32 bit or 64 bit (R1 only)
Drive	*Required:* Designated drive available
Policy Mgr Environment Tests	*Required tests must pass on Policy Manager server*
Memory	*Required:* At least 2 GB RAM Minimum single 10/100 Ethernet adapter, preferred Gigabit Ethernet adapters, optional additional NIC for data backups
Comm	*Required:* 10/100 Ethernet adapter (NIC card), 1 Gb preferred
Free Disk Space	*Required:* At least 2 GB
Processor Speed	*Required:* Each processor at least 2.1 GHz total speed (one or more processors)
Operating System	*Required (US English only supported):* • Windows Vista • Windows XP, SP2 or later • Windows Server 2003
Network Connectivity Tests	*Required tests must pass on Gateway Client server* **Note:** The EMC Registration Authority Connect and EMC Secure Remote Support Connect tests can be performed using either the HTTPS protocol or a simple TCP / IP connection to the EMC application servers. *Required:* Gateway Client server *must* pass both TCP / IP connection tests to proceed with Gateway Client software installation.
EMC Registration Authority Connect EMC Secure Remote Support Connect	*Required:* Gateway Client server can connect to EMC servers over TCP port 443.
EMC Registration Authority Connect HTTPS EMC Secure Remote Support Connect HTTPS	HTTPS tests may fail for any of several reasons — for example, time-out and proxy configuration / authorization errors. You can test connections by using a local web browser to open the URLs provided in the detailed test results.
System Applications Tests	*Required tests must pass on Gateway Client server*
IIS Administration Service	*Required:* IIS installed on Gateway Client server
File Transfer Service	*Optional:* FTP enabled on Gateway Client server and configured as specified in *"Gateway Client Server Preparation" on page 43*
Simple Mail Transport Protocol	*Required*: SMTP enabled on Gateway Client server and configured as specified in *"Gateway Client Server Preparation" on page 43*

Table 5 CECT test failure resolution (page 3 of 3)

Test name	Notes
Required Local User Accounts	*Required:* OnAlert and ESRSConfig user accounts created on Gateway Client server and configured as specified in "IIS settings" on page 48
IIS and ESRS Installation Drive Check	*Required:* IIS and Gateway Client software installed on the same local drive **Note:** If EMC has not yet installed the Gateway Client software, this test has a Failed status. However, the detailed test results state that the failure is a warning, and identify the drive on which EMC should install the Gateway Client software.
Device Application Port Connection Test	*Required:* Internal firewall rules must be updated to allow communication between the Gateway Client server and each of its managed devices, using the required ports for each remote support application, as specified in *EMC Secure Remote Support IP Solution Port Requirements*. **Note:** CECT tests the required port connections only for the devices and applications that you specify in the Configuration Parameters screen shown in Figure 85 on page 136. You should test the port connections for every application on every device that you want to manage through the ESRS IP system. **Note:** For devices not yet on the network, this test has a Failed status. For those devices, you should manually check the firewall rules to ensure that communication is allowed between the Gateway Client server and each device, using the required ports for each remote support application, as specified in *EMC Secure Remote Support IP Solution Port Requirements*.

Installation

To install CECT:

1. On the targeted Gateway Client or Policy Manager server, run **CECT.msi** from the ESRS IP Provisioning Tool CD. The CECT Setup Wizard appears, as shown in Figure 75 on page 126.

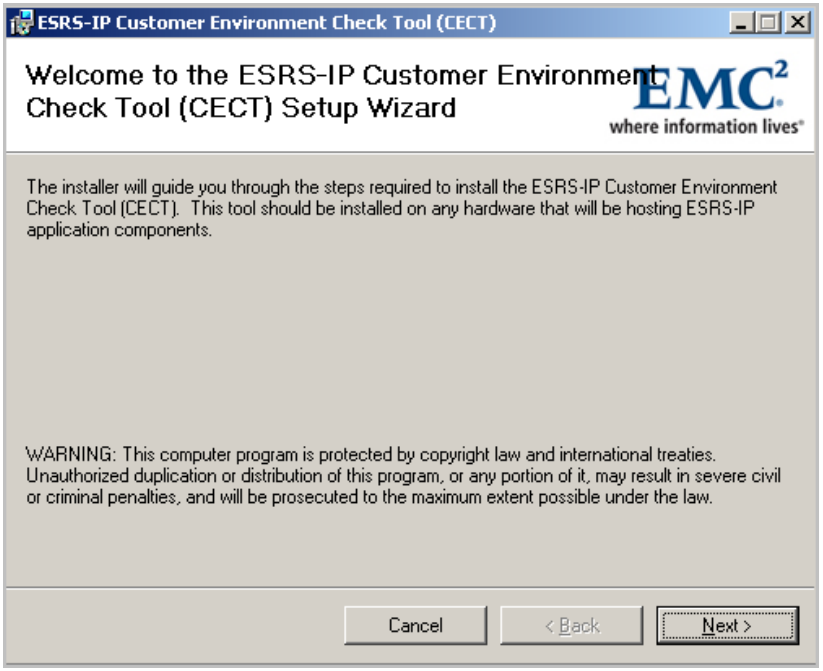


Figure 75 Setup wizard

2. Click **Next.** The **Installation Folder** screen appears, as shown in Figure 76 on page 127.

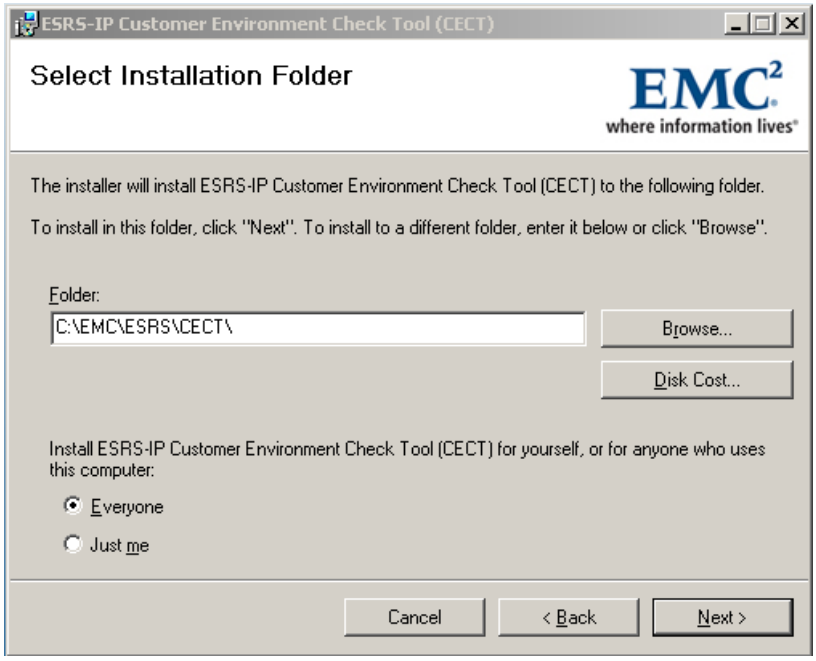


Figure 76 Installation folder

3. Select an installation directory and click **Next**. (The default directory is C:\EMC\ESRS\CECT\). The **License Agreement** screen appears.
4. Accept the license agreement and click **Next**. The CECT install screen appears, as shown in Figure 77 on page 128. Wait while the check tool installs.

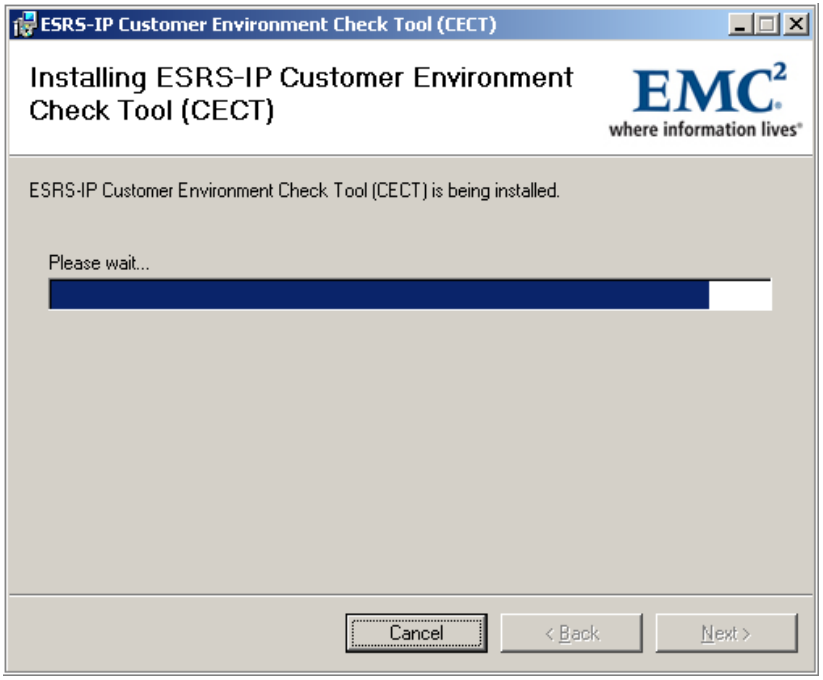


Figure 77 **Install screen**

5. When you see the Installation Complete notification, click **Close**, as shown in Figure 78 on page 129. The CECT application is now in the folder you specified. A shortcut to the application is on your desktop.

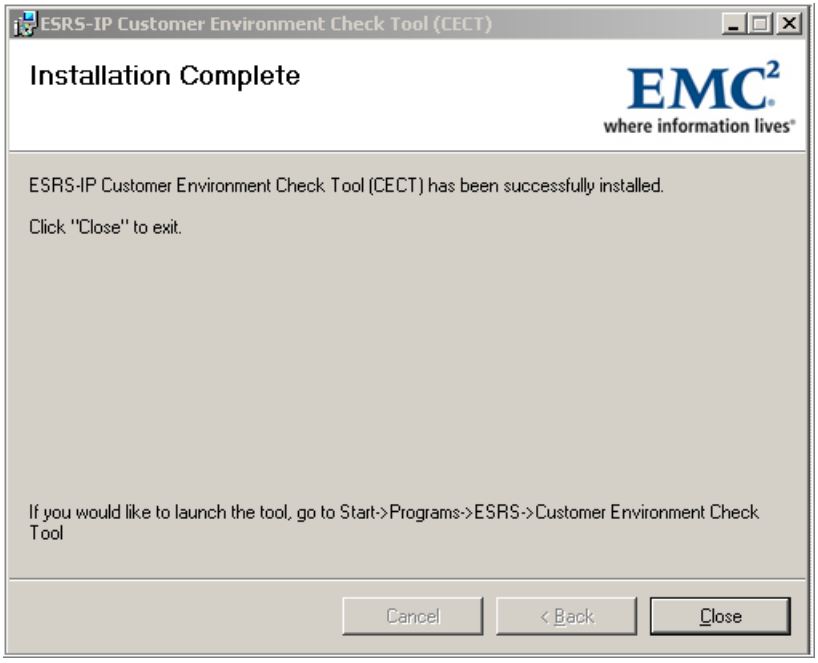


Figure 78 Installation complete

Operation

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

There are tests specific to Gateway Client servers and to Policy Manager servers:

- If you plan to run the Gateway Client and Policy Manager applications on the same server, you should run all available tests on that server.
- If you plan to run the Gateway Client and Policy Manager applications on separate servers, you should run the Gateway Client-related tests only on the Gateway Client server, and you should run the Policy Manager tests only on the Policy Manager server.

To run a series of tests using the CECT application:

1. Launch the CECT application.

Note: To Use Customer Environment Check Tool on Windows 2008 it may be necessary to "Run As Administrator" to have the tool perform properly.

2. Enter your customer site and contact information.
3. Select the tests you want to run.
4. Set the configuration parameters for each test.
5. Execute the test run.
6. View the test results.
7. Save the test results to a log file in the CECT directory.
8. Exit the CECT application.

The following sections provide additional details about these steps.

Launching the application

To launch the CECT application:

1. Click the CECT Desktop Icon, or run **Start** > **Programs** > **EMC** > **ESRS** > **Customer Environment Check Tool**. The welcome screen appears, as shown in Figure 79 on page 131.

Note: If you have not yet installed Microsoft .NET Framework 2.0 (or a newer version that is backward compatible with 2.0), you will be prompted to install it at this point.

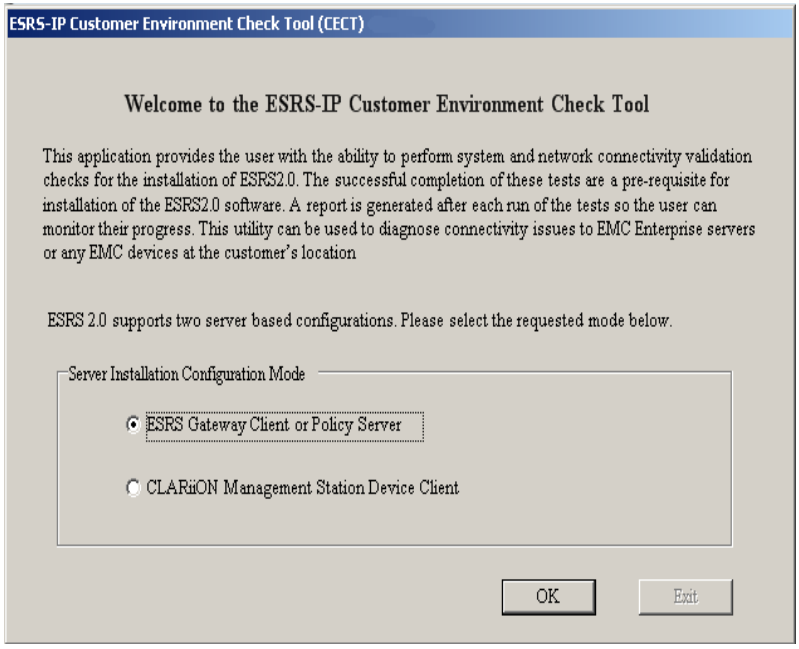


Figure 79 **Welcome screen**

2. Select a server installation configuration mode and click **OK**. The main CECT application screen appears, as shown in Figure 80 on page 132. The screen will appear as a blank screen at this point.

Note: The configuration mode selection will only be available the first time you open the CECT tool. After you make the selection, you can only change it by uninstalling and reinstalling the CECT application.

The Device Client configuration mode might not be applicable, depending on your version of ESRS IP. Your EMC Global Services professional can provide additional information.

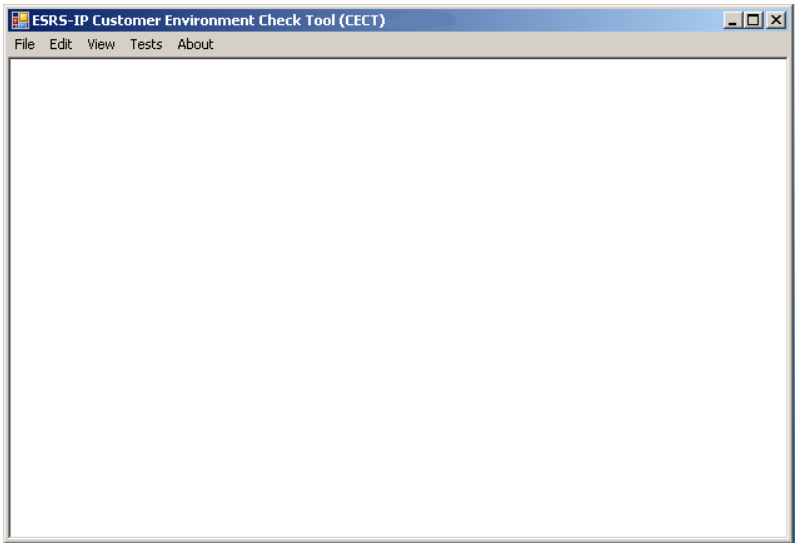


Figure 80 **Main CECT application screen**

3. If you have not yet entered site information for this device, select **Edit** from the top menu and click **Gateway Customer Info**, as shown in Figure 81 on page 132.

Gat

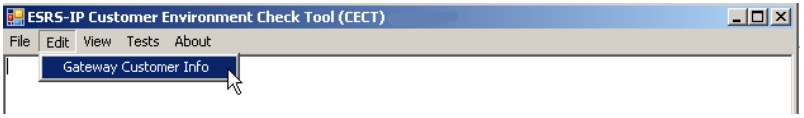


Figure 81 **Gateway customer info**

4. The Site Information screen appears, as shown in Figure 82 on page 133.

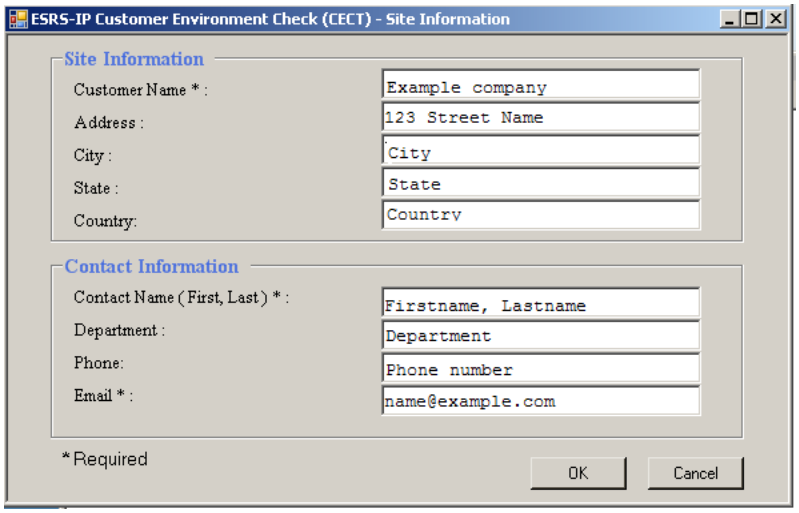


Figure 82 **Site information**

5. Enter the site information, including the fields marked as required fields, and click **OK**.

Selecting tests to be run

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

1. From the main CECT application screen, select **Tests** from the menu bar.
2. Click **ESRS IP Customer Environment Check**, as shown in Figure 83 on page 133. The Server Environment Tests screen appears. This screen enables you to choose the tests you wish to run, as described in "Selecting tests to be run" on page 133.

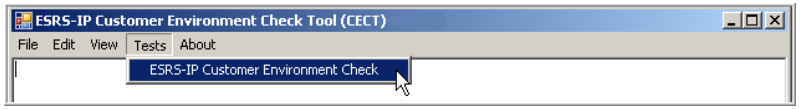


Figure 83 **Tests screen**

3. Review the Server Environment Tests screen as shown in "Server Environment Tests" on page 134.

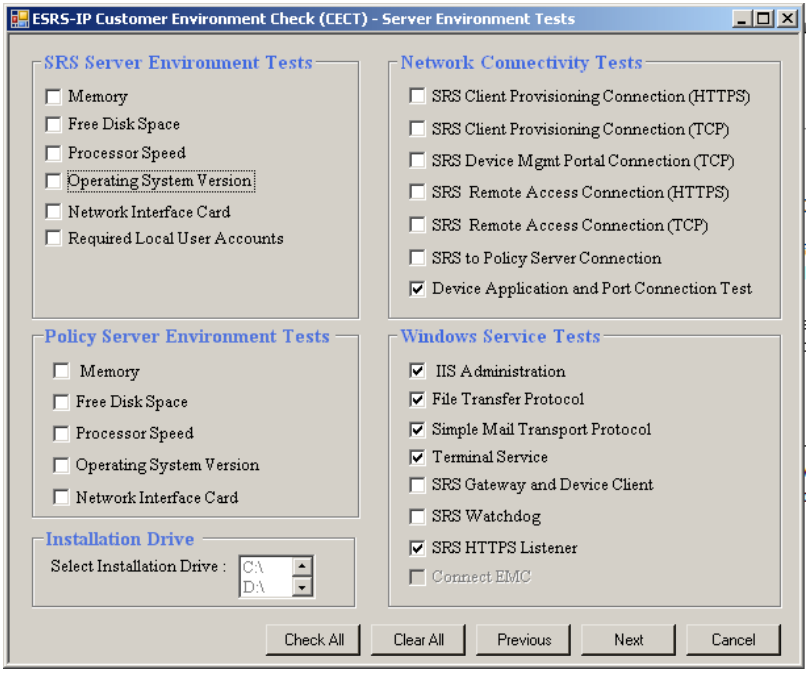


Figure 84 Server Environment Tests

4. Decide which tests you want to include in this test run. The Server Environment Tests screen lets you select options from any of the following test groups:

   - **SRS Server Environment Tests** — Verifies that the Gateway Client server hardware meets the minimum requirements and verifies that the correct operating system is installed on the server.
   - **Policy Server Environment Tests** — Verifies that the Policy Manager server hardware meets the minimum requirements and verifies that the correct operating system is installed on the server.

- **Network Connectivity Tests** — Verifies that all required network connections have been configured properly, so that communications are enabled between the Gateway Client server and EMC and between the Gateway Client and Policy Manager servers.
- **Windows Service Tests** — Verifies that the Gateway Client server has Microsoft IIS installed, has FTP and SMTP services enabled and configured properly, has the required directory structure in place on the installation root drive, has the required user accounts configured properly, and has the proper ports open for communication with each application installed on each of its managed devices.

Different tests are designed to run on each type of server, as follows:

- **Co-located Gateway and Policy Manager** — You should run *all* available tests.

  Note: If you select at least one test option in *each* of the SRS Server and Policy Server test groups, the CECT application assumes that the Gateway Client and Policy Manager servers are to be co-located. (CECT only tests the server on which it is installed.)

- **Gateway Only** — You should run all available tests *except* the tests for the Policy Manager.
- **Policy Manager Only** — You should run *only* the tests in the **Policy Server Environment Tests** group.

5. Using the checkboxes in the Server Environment Tests screen shown in Figure 84 on page 134, choose the tests you want to run on this server.
6. Click **Next**. Depending on which tests you selected, the Configuration Parameters screen or Test Results screen appears.
   - If the Configuration Parameters screen appears, refer to "Setting test configuration parameters" on page 136 for instructions for entering the parameters.
   - If the Test Results screen appears, refer to "Executing the test run" on page 140 for instructions on running tests and viewing test results.

Setting test configuration parameters

If you selected any tests that require additional parameters, the Configuration Parameters screen appears, as shown in Figure 85 on page 136.

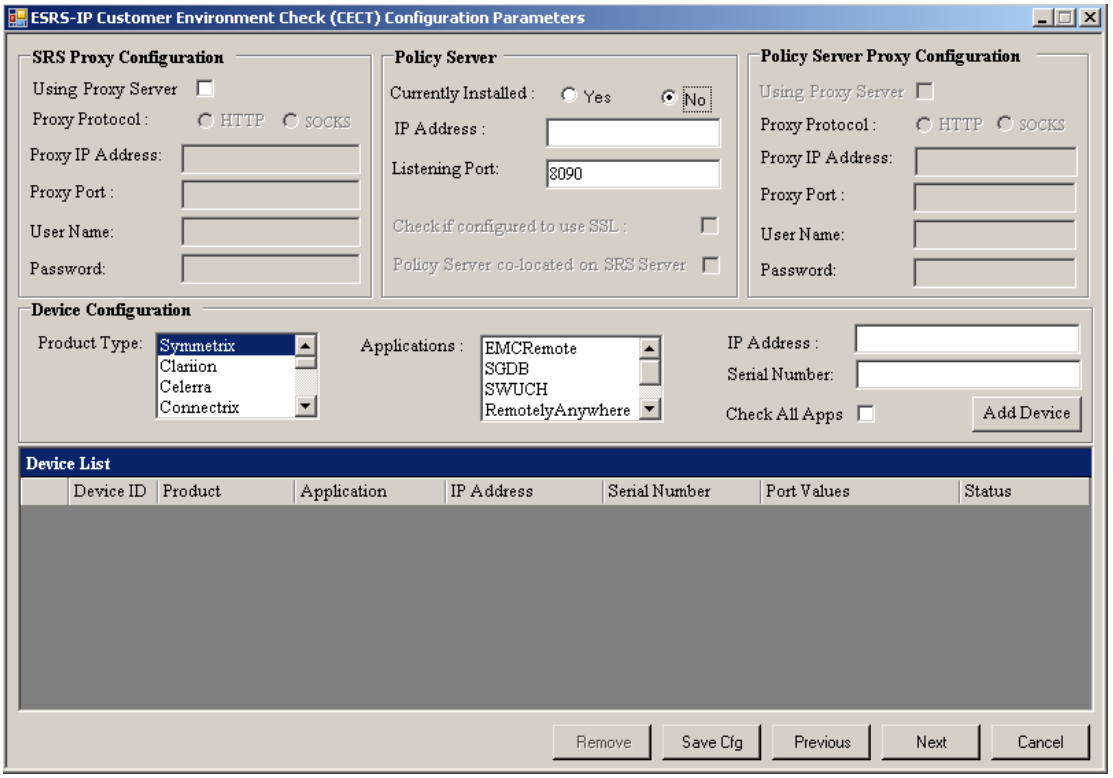


Figure 85 **Configuration Parameters**

To return to the Server Environment Tests screen and choose different test options, click **Previous**.

To set the parameters for the tests you selected, enter the information required to perform the selected tests, as follows:

1. In the **SRS Proxy Configuration** area of the screen:
   a. If a proxy server routes outbound Internet traffic from the Gateway Client server, select the **Using Proxy Server** checkbox.

b. If the SRS proxy server information fields are active, complete the following information:

- **Proxy Protocol** — Select HTTP or SOCKS
- **Proxy IP Address** — Proxy server IP address
- **Proxy Port** — Port over which proxy server communicates with Gateway Client server
- **User Name** — Username for an authorized proxy server user account (Required for SOCKS Proxy)
- **Password** — Password for previously-named proxy server user account (Required for SOCKS Proxy) (valid characters *do not* include %, &, <, and >)

Note: If the password field is not filled in, you will receive a warning message. You may continue with the test.

---

2. In the **Policy Server** area of the screen:

   a. In the **IP Address** field, enter the Policy Manager server's IP address.

   b. If the Policy Manager is not yet installed on this server, select **No** to answer the **Policy Mgr currently installed:** question.

Note: If you select **No** and you selected **SRS to Policy Server Connection** in the Server Environment Tests window (see **Figure 84 on page 134**), you will be required to supply the IP address of the intended Policy Manager server.

---

   c. If the Policy Manager *is* installed, select **Yes** to answer the **Policy Mgr currently installed:** question. If applicable, select the **Check if configured to use SSL:** checkbox. Select the **Policy Server co-located on SRS Server** checkbox if you have installed co-located Gateway Client and Policy Manager servers on this machine.

3. In the **Policy Server Proxy Configuration** area of the screen:

   a. If a proxy server routes outbound Internet traffic from the Policy Server, select the **Using Proxy Server** checkbox.

   b. If the SRS proxy server information fields are active, complete the following information:

- **Proxy Protocol** — Select HTTP or SOCKS

- **Proxy IP Address** — Proxy server IP address
- **Proxy Port** — Port over which proxy server communicates with the Policy Manager server
- **User Name** — Username for an authorized proxy server user account (Required for SOCKS Proxy)
- **Password** — Password for previously-named proxy server user account (Required for SOCKS Proxy) (valid characters **do not** include %, &, <, and >)

Note: If the password field is not filled in, you will receive a warning message. You may continue with the test.

4. In the **Device Configuration** area of the Configuration Parameters screen, take the following steps for each device if you are running CECT on a Gateway Client server in the DMZ *and* you want to ensure that the internal firewall rules allow network connections between the Gateway Client server and the managed EMC devices, using the required application-specific ports:

   a. Click to select the **Product Type** from the scrolling list. **Symmetrix** is selected by default.

   Note: To test a Symmetrix for connectivity, it must already be on the network and configured to use the ESRS IP Gateway Client.

   b. Click to select the **Application**s to be tested on the device. (Press and hold the **Ctrl** key and click to select multiple applications.)

   c. Enter the device's **IP** address. You cannot use the DNS name.

   d. Enter the device's **Serial Number**.

   e. Click **Check All Apps** if applicable.

   f. Click **Add Device** to add the device to the Device List at the bottom of the screen.

   To *remove* a device from the **Device List**:

   a. Click the box to the left of a **Device ID** to select the row. (You can also press and hold the **Ctrl** key and click to select multiple rows.)

   b. Click **Remove**.

5. If you have added any devices to the **Device List**, click **Save Cfg**.

   CECT creates one test record for each application selected. If an application requires more than one port, CECT tests the ports for that application one at a time until either one port fails (causing the application test to fail) or all ports pass (causing the application test to pass).

6. When you have completed all available fields in the **SRS Proxy Configuration**, **Policy Server,** and **Policy Server Proxy Configuration** areas, and you have added all the devices that you want to test to the **Device List**, click **Next**.

   The Test Results screen appears, as shown in Figure 86 on page 139.

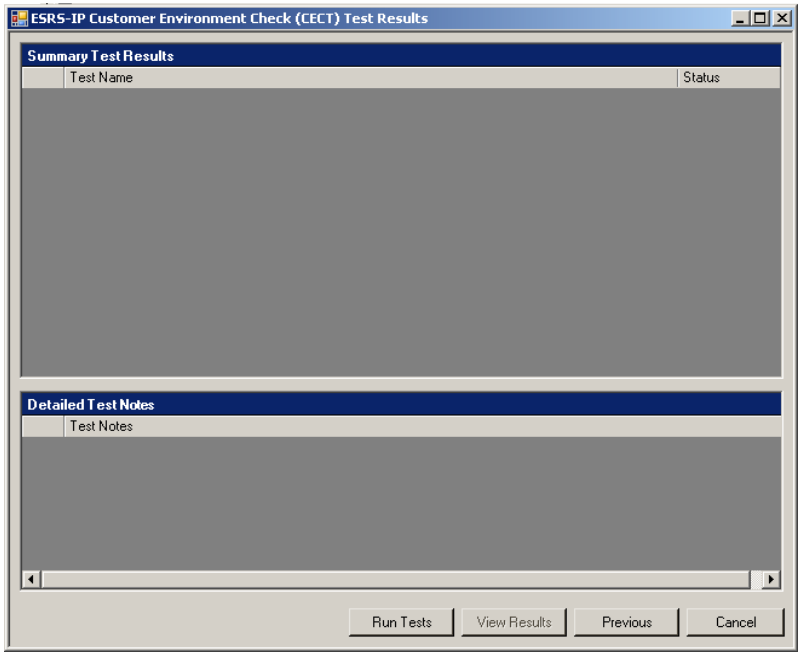


Figure 86 CECT Test Results screen before test run execution

Executing the test run

Once you have selected the tests you want to run and configured the parameters for those tests if necessary, the Test Results screen appears, as shown in Figure 86 on page 139.

To return to the Configuration Parameters screen shown in Figure 85 on page 136 and reset your Policy Server, Proxy Configuration, and Device information, click **Previous**.

To return to the Server Environment Tests screen shown in Figure 84 on page 134 and select a different set of tests for this run, click **Previous** twice – first on the Test Results screen and then on the Configuration Parameters screen.

To use the Test Results screen to execute the test run and view results:

1. Click **Run Tests**.
2. CECT runs all selected tests, one at a time. As each test runs, the name of that test appears beneath a test progress bar in the middle of the application window. As each test completes, its progress bar disappears, and the progress bar for the next test appears instead.

Note: If you have selected many devices or applications to be tested, the test run may take some time. Please be patient.

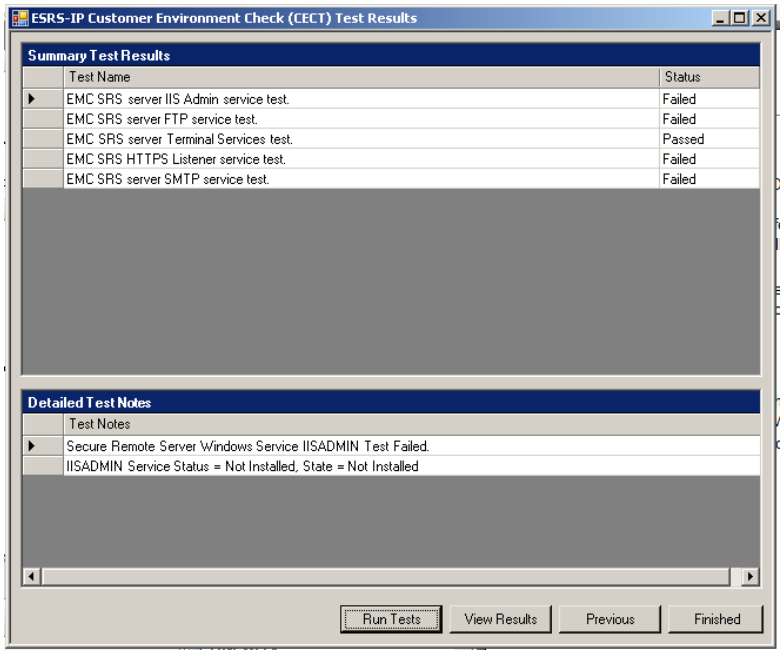


Figure 87 **CECT Test Results screen after test execution**

3. When the tests are complete, the basic status of each test (**Passed** or **Failed**) appears in the **Summary Test Results** pane. The detailed results of each test appear in the **Detailed Test Notes** pane. Figure 87 on page 141 shows some sample test results.

Viewing test results

This section describes how to view test results and test result log files.

Test results

When the test names and results appear in the Test Results screen as shown in Figure 87 on page 141, you can view each test result in detail. You can also use a text editor such as Notepad to view test results from the file system.

To view the detailed results of any test:

1. From the **Test Results** screen, select the desired test status (**Passed** or **Failed**) in the **Summary Test Results** pane. The selected test is marked by an arrow in the far-left column in the pane.

2. The **Detailed Test Notes** pane shows the following results for the selected test:
   - The system configuration values obtained from the test
   - If the test status is **Failed**, available information about why the test failed
3. When you have finished reviewing the test results, click **Finished**.

   The Test Results window closes, but the main application window remains, as shown in Figure 80 on page 132.

Test result log files

You can view the following CECT test log files:

- Log file from your current test
- Log files from your current test and previous tests

To view the log file from your current CECT test:

1. In the Test Results screen, click **View Results**. The log file for your current test appears, as shown in Figure 88 on page 143.
2. To search within the log file for specific text string values, use the **View**, **Find** menu option.
3. When you finish viewing the log file, use the **File, Close** menu option to close the log file and leave the CECT application running.

Note: The log file from your current test is automatically saved in the Gateway Test Logs area.

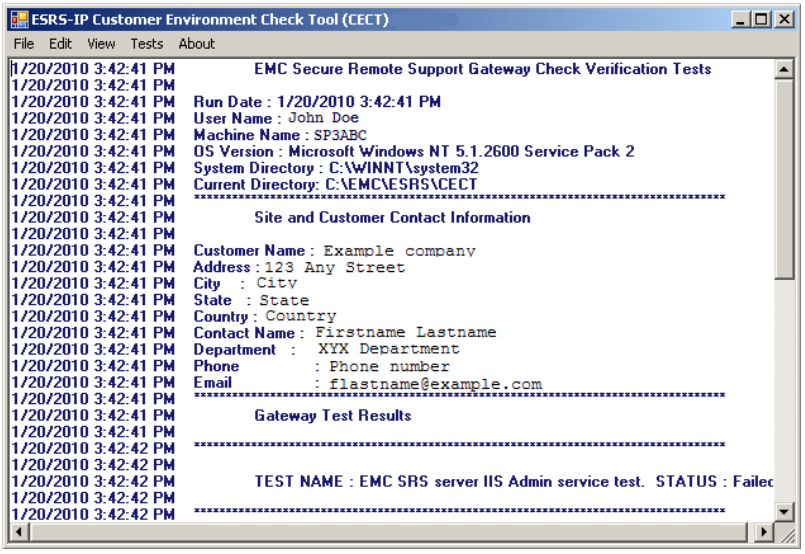


Figure 88 **Current test log file**

To view the log files from your current and previous CECT tests:

1. From the menu bar of either your current test log window or the main CECT application window, select **View** > **Gateway Test Logs**.

   The **Test Results Logs** navigation window appears, as shown in Figure 89 on page 144.

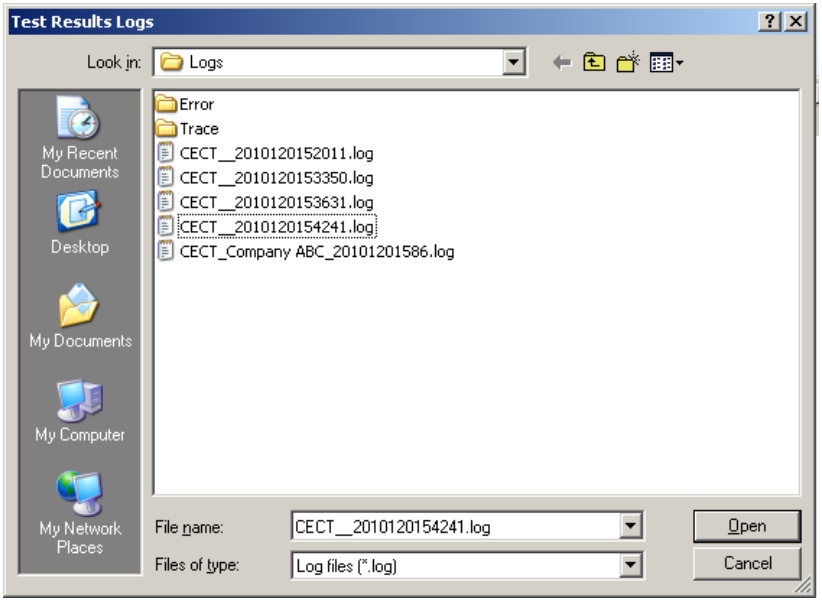


Figure 89 **CECT Test Results Logs navigation window**

2. In the **Files of type**: drop-down list box, select **Log files (*.log)**.

   The **Test Results Logs** window displays the log files for every CECT test series that you have completed on this server.

3. Select the log file for the test results you want to view and click **Open**.

   The **Test Results Logs** window closes, and the contents of the log file that you selected appear in the main CECT application window, as shown in Figure 90 on page 145.

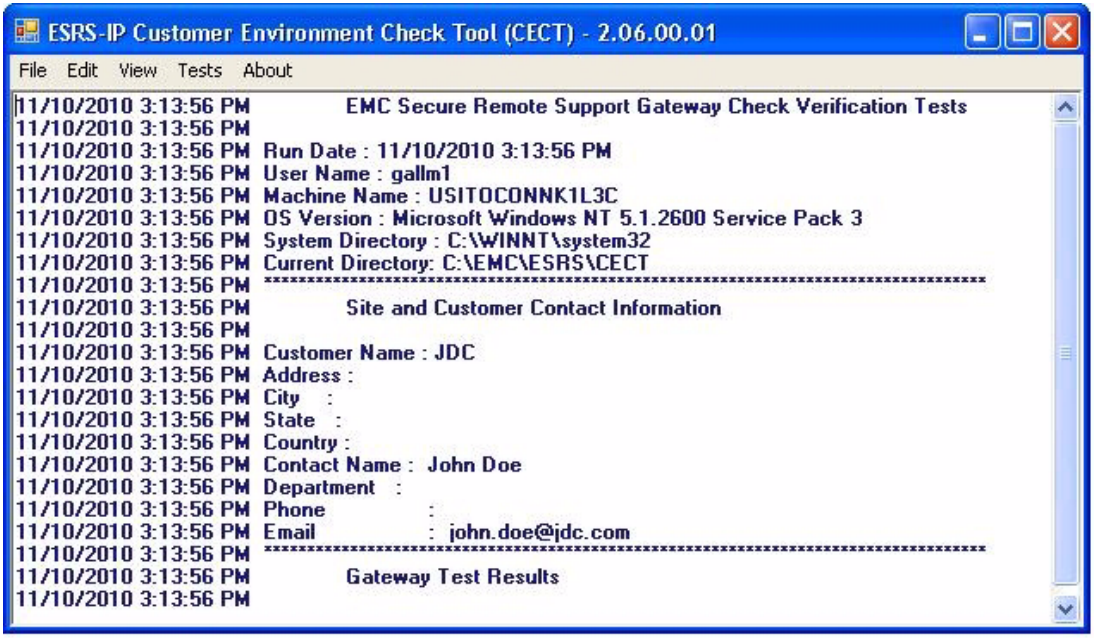


Figure 90 **Sample CECT Test Results log file contents**

4. Use the **View**, **Find** option in main application window to search within the log file for specific text string values.
5. When you have finished viewing the log file, use the **File, Close** menu option to close the log file and leave the CECT application running.

Once you close the log file containing your test results, you can use the **View, Gateway Test Logs** menu option to reopen the **Test Results Logs** navigation window (shown in Figure 89 on page 144). You can then open and view the other log files from your test run.

CECT application log files

This section explains how to troubleshoot the CECT application by viewing runtime error and program execution log files.

Runtime error logs

To see the CECT application's runtime error messages:

1. In the **Test Results Logs** navigation window (accessed from the **View** option of the main CECT application window), open the Error directory.
2. In the **Files of type**: drop-down list box, select **Error files (*.err)**.

   The **Test Results Logs** window displays the application's runtime error files for every CECT test series that you have completed on this server.
3. Select the error file for your test run and click **Open**.

   The **Test Results Logs** window closes, and the contents of the error file that you selected appear in the main CECT application window.

Program execution logs

To see the CECT application's program execution logs:

1. In the **Test Results Logs** navigation window, open the Trace directory.
2. In the **Files of type**: drop-down list box, select **Trace files (*.trace)**.

   The **Test Results Logs** window displays the application's program execution logs for every CECT test series that you have completed on this server.
3. Select the trace file for your test run and click **Open**.

   The **Test Results Logs** window closes, and the contents of the trace file that you selected appear in the main CECT application window.

Saving Test Results and exiting the application

When you have finished viewing all of your log files in the main application window, you can do any of the following:

- Close the log file, using the **File** > **Close** menu option, and use the main application window to start another test run or view another file.
- Save the log file in the current display window to a new filename, using the **File** > **Save As** menu option to open a standard Windows **Save As** dialog box.
- Exit the application, using the **File** > **Exit** menu option or the **X** button in the upper-right corner of the window to close the application window.

Version information

Use the main CECT application screen shown in Figure 80 on page 132 to get version and copyright information. From the main CECT application screen, select **About**.

4

Configuration Tool

The Configuration Tool is used to view Gateway Client status, manage devices for a Gateway Client, and perform other tasks related to the configuration of your ESRS IP solution.

This chapter includes the following topics:

Configuration Tool overview

The ESRS IP Configuration Tool is used to manage ESRS IP Client devices and view and modify settings related to managed devices and related services.

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

The Configuration Tool is used to:

- View various ESRS IP Client statuses, including connectivity status, Policy Manager enablement, and cluster status
- View the managed devices for an ESRS IP Client
- Create device deployment, change, and removal requests
- Configure a proxy server
- Configure an ESRS IP Client to use a Policy Manager
- View the status of ESRS IP services and connect home services
- View active remote support sessions
- View logs of ESRS IP Client activities

The following section explains how to install and use the Configuration Tool.

Installing and using the Configuration Tool

Installing the Configuration Tool

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

If you are running Windows 2008

If you are running Windows 2008, you must set the Configuration Tool to run the program as an administrator. You only need to do this once. The following steps explain how to set the Configuration Tool.

Note: If you do not set the Configuration Tool to run the program as an administrator, and you log in as a local user, the Configuration Tool connection status will display the following message when you launch the tool:

```
Client is not running
```

This only applies if you are running on Windows 2008. For an example, see Figure 91 on page 152.

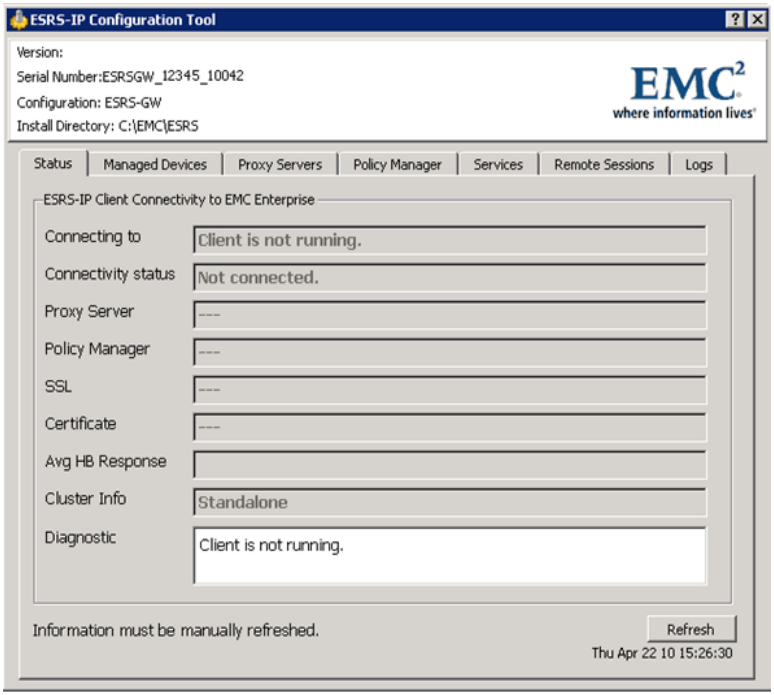


Figure 91 **Client is not running**

To set the Configuration Tool to run the program as an administrator, follow these instructions (required on Windows 2008 only):

1. From your Windows 2008 desktop, click **Start**, then click **All Programs**. The programs menu appears.
2. Expand the **ESRS** folder so that **Configuration Tool** is visible.

3. Right-click **Configuration Tool** and select **Properties**, as shown in Figure 92 on page 153.

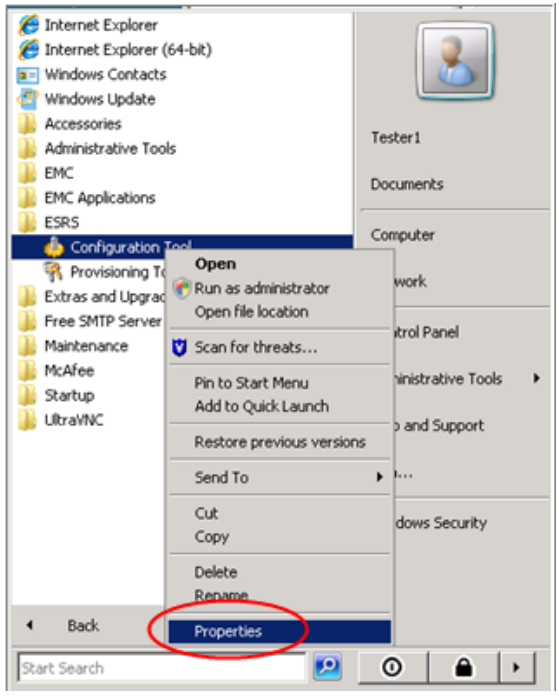


Figure 92 **Configuration Tool properties**

4. Click **Compatibility**, then select **Run this program as an administrator**, as shown in Figure 93 on page 154.

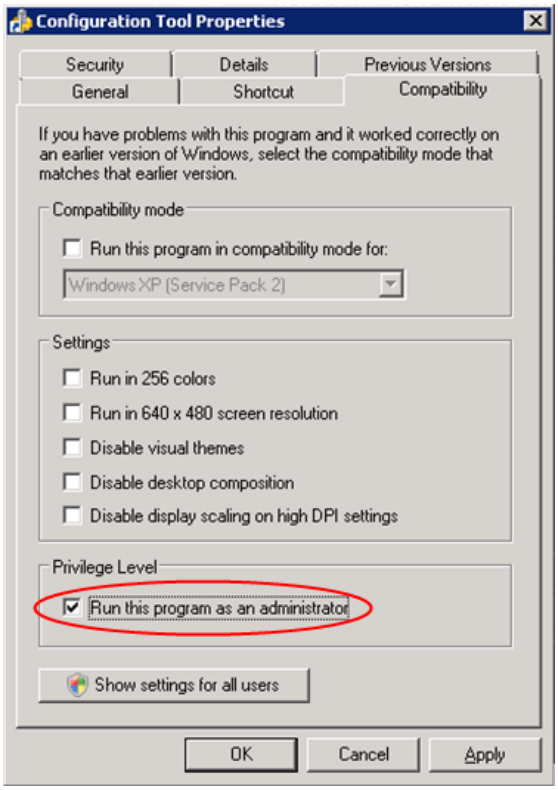


Figure 93 **Run this program as an administrator**

5. Click **OK**, then launch the Configuration Tool as described in "Using the Configuration Tool" on page 154.

Now that you have enabled yourself to run Configuration Tool as an administrator, you will be able to view connectivity status as shown in Figure 95 on page 155.

Using the Configuration Tool

To use the Configuration Tool, initiate it from the Start Menu:

```
Start Menu\Programs\ESRS\Configuration Tool
```

The Configuration Tool screen appears. The screen header displays the ESRS version, the serial number of your ESRS IP Client device,

the configuration of your device, and the install directory, as shown in Figure 94 on page 155.

Figure 94 **Configuration Tool screen header**

Viewing connectivity status

To view connectivity status, click the **Status** tab in the Configuration Tool. The Status tab displays connectivity information between the ESRS IP Client and EMC, as shown in Figure 95 on page 155.

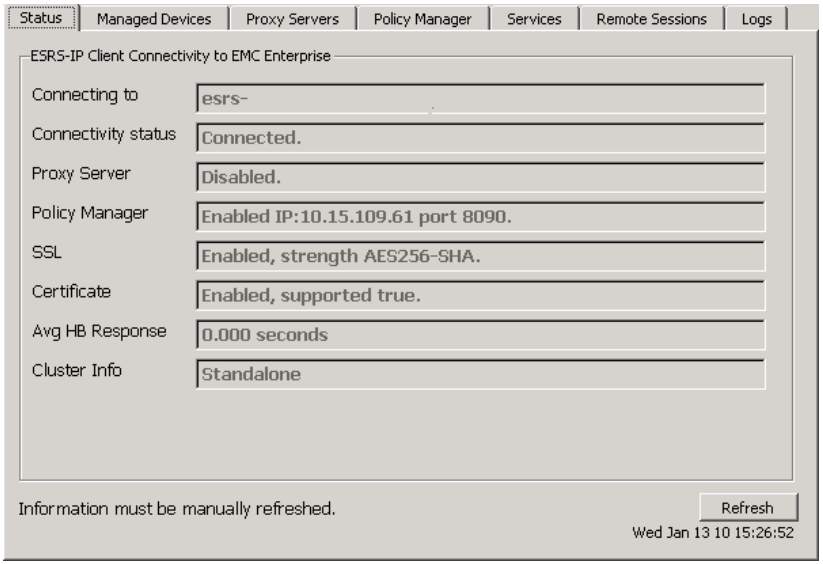


Figure 95 **Status tab**

The connectivity information in the Status tab is automatically populated when you run the Configuration Tool.

Note: To update the displayed information at any time, click **Refresh**.

The Status tab displays the following information:

- **Connecting To**: Displays the Domain Name System (DNS) name of the EMC enterprise
- **Connectivity Status**: Displays Gateway Client connectivity to the EMC Enterprise. One of the following values is shown:
  - **Connected**: The Gateway Client is successfully connected to the EMC enterprise.
  - **Not Connected**: The Gateway Client service is running but is unable to connect to the EMC enterprise.
  - **Not Running**: The Gateway Client service is stopped and is not trying to connect to the EMC enterprise.
- **Proxy Server**: Indicates whether a proxy server is enabled (includes IP Address and Port, if enabled).
- **Policy Manager**: Indicates whether Policy Manager is enabled (includes IP Address, Port, and Proxy, if enabled).
- **SSL**: Indicates whether Secure Socket Layer (SSL) communication is enabled to EMC.
- **Certificate**: Indicates whether a digital certificate is enabled.
- **Average HB Response Time**: Displays the average heartbeat (HB) response time from the Gateway Client to the EMC enterprise.
- **Diagnostic**: Displays the reason that the Gateway Client is not connected to the EMC enterprise (only displays if Connectivity Status is Not Connected).
- **Cluster Info**: If the Gateway Client is part of a High Availability Gateway Cluster, the Cluster Identifier will be displayed along with the number of Gateway Clients within the cluster. If the Gateway Client is *not* part of a High Availability Gateway Cluster, the words Stand Alone will be displayed.

Managing devices

To manage or view devices, click the **Managed Devices** tab in the Configuration Tool. The tab displays the serial number, model, and IP address of each device that is currently managed by the Gateway Client, as show in Figure 96 on page 157.

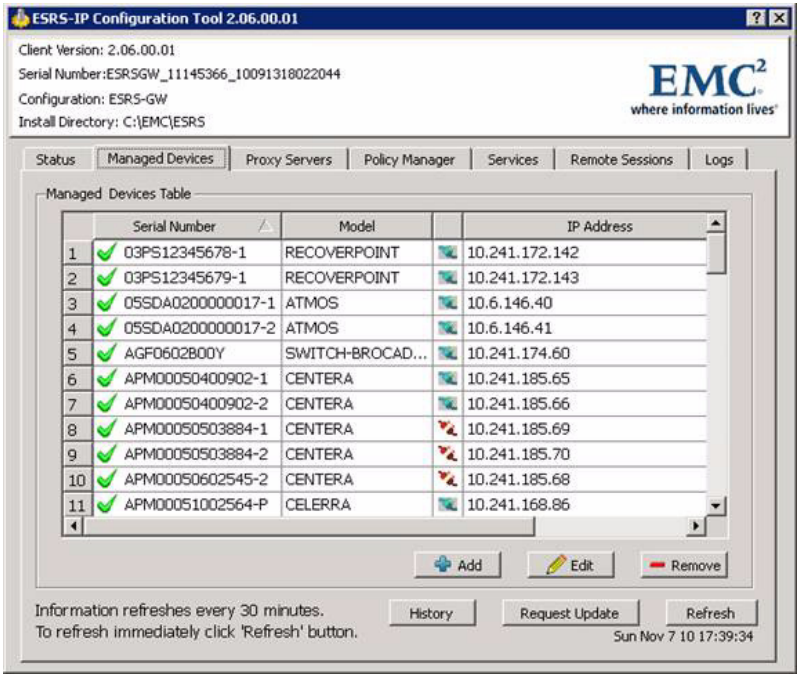


Figure 96 **Managed Devices tab**

You can choose the following actions from the Managed Devices tab:

- **Add**: Add a new device to be managed.
- **Edit**: Change the IP address of a managed device.
- **Remove**: Remove (unmanage) a device that is currently managed.
- **History**: View history of all requests that have not yet been approved by an authorized EMC Global Services professional.
- **Request Update**: Submit your pending requests to EMC for approval.
- **Refresh**: View the most current information.

Adding a managed device

To add a managed device:

1. Click **Add**. The Add New Device window displays, as shown in Figure 97 on page 158.
2. Enter the following device information:
   - Serial Number

- Suffix, if applicable (the options displayed in the drop-down list are dependent on the selected model type)
- Model Type (select a model type from the drop-down list)
- IP Address

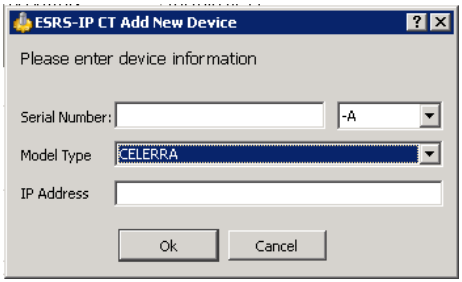


Figure 97 Add New Device window

3. Click **OK.**
4. The Configuration Tool will run a connectivity test. An error message will appear if the connectivity test fails. However, you can still elect to manage the device.

   Once the information has been entered, the device will be marked with a plus sign .The device will continue to display the plus sign until you click Request Update, at which time the request will disappear.
5. To send the Add New Device request to EMC, click **Request Update**.
6. When prompted, confirm the device you wish to add. The update will not take effect until it has been approved by an authorized EMC Global Services professional via the EMC enterprise.

   Note: After you confirm the device, your request will no longer be visible in the tab. To view the request, click **History** as described in "Viewing history" on page 160.
7. Once the request has been approved via the EMC enterprise, and the synchronization process completes, refresh your screen to see the newly added device. Please allow sufficient time for the approval and synchronization process to occur, then refresh.

Editing the IP address of a managed device

To edit the IP address of a managed device:

1. Select the device from the **Managed Devices** tab.
2. Click **Edit**.
3. Edit the displayed address.
4. Click **OK**.
5. If the Configuration Tool is unable to access the device, or if the selected IP address is being used for another device, a warning message appears. If you want to continue with the edit, click **Yes** when prompted.
6. When prompted, click **OK** to set the device edit. A pencil icon appears next to the device you have edited. 
7. To send the revised IP address to EMC, click **Request Update** on the **Managed Devices** tab. The update will not take effect until it has been approved by an authorized EMC Global Services professional.
8. When prompted, confirm the device you wish to edit. The previous IP address will be displayed until the edit has been approved by an authorized EMC Global Services professional via the EMC enterprise.

   Note: After you confirm the device, your request will no longer be visible in the tab. To view the request, click **History** as described in "Viewing history" on page 160.

9. Once the request has been approved via the EMC enterprise, and the synchronization process completes, refresh your screen to see the newly added device. Please allow sufficient time for the approval and synchronization process to occur, then perform the refresh.

Unmanaging a device

To unmanage a managed device:

1. Select the device from the **Managed Devices** tab.
2. Click **Remove**.
3. When prompted to confirm your request, click **OK**. The device will be marked with a minus sign until you send the Remove request to EMC or change the device back to being a managed device.

4. To send the request to EMC, click **Request Update** at the bottom of the **Managed Devices** tab.
5. When prompted, confirm the device or devices you wish to unmanage. The update will not take effect until it has been approved by an authorized EMC Global Service professional via the EMC enterprise. The device will remain listed as a managed device until the removal has been approved.
6. Once the request has been approved via the EMC enterprise, and the synchronization process completes, refresh your screen to display current information. Please allow sufficient time for the approval and synchronization process to occur.

Submitting Managed Devices requests for approval

When you have completed all your manage, edit, or unmanage requests, click **Request Update**. Your change requests will be displayed for verification. Click **OK** to submit your requests to EMC for implementation.

When an authorized EMC Global Services professional has approved your requests via the EMC enterprise, the requested updates will be processed by the ESRS IP Client. The device information will be visible in the Configuration Tool. Any devices that have been removed will no longer be visible in the Managed Devices tab.

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

Viewing history

To display history of all requested changes for a device, click the device name in the Managed Devices tab. Then click **History**. The device history appears as shown in Figure 98 on page 161.

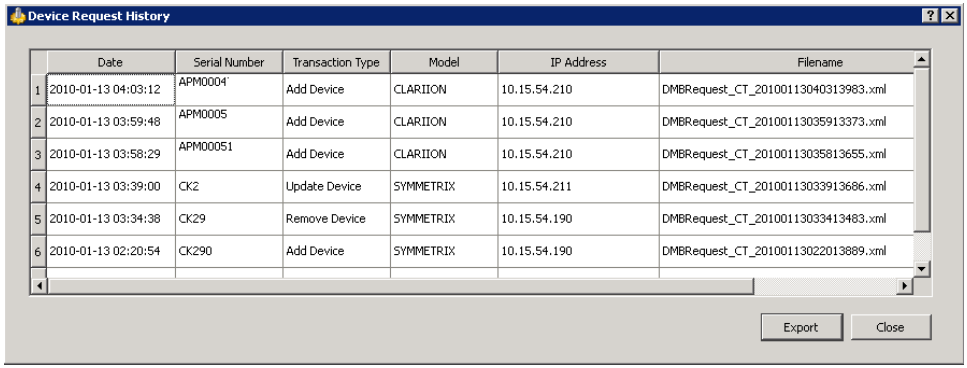


Figure 98 **History**

Communicating through a proxy server

ESRS IP Clients can be configured to communicate directly through EMC or through an HTTPS or SOCKS proxy, as shown in Figure 99 on page 161.

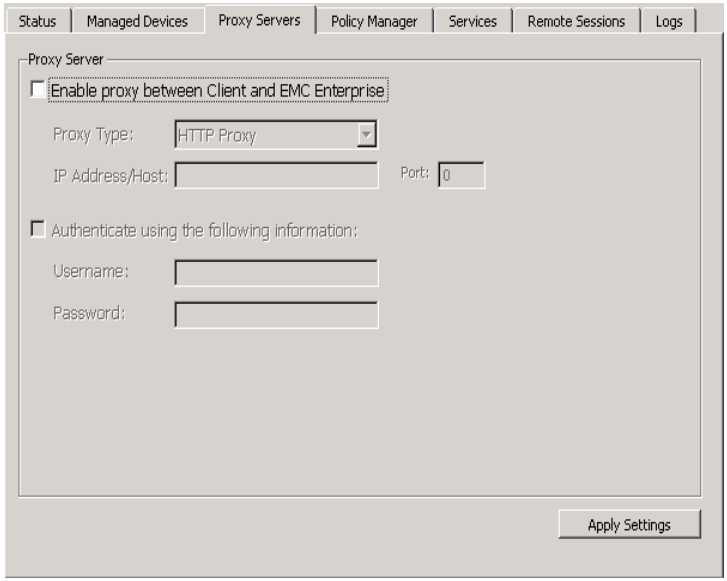


Figure 99 **Proxy Servers tab**

Enabling proxy server communication

To enable communication through a proxy server:

1. Click the **Proxy Servers** tab in the Configuration Tool.
2. Check **Enable proxy between Client and EMC Enterprise**.
3. Enter the following proxy information:
   - Proxy Type
   - IPS Address or DNS Name
   - Port
   - Username (if required)
   - Password (if required)
4. Click **Apply Settings**.

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

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

Disabling proxy server communication

To disable communication through a proxy server:

1. Click the **Proxy Servers** tab in the Configuration Tool, as shown in Figure 99 on page 161.
2. Remove the check from **Enable proxy between Client and EMC Enterprise**.
3. Click **Apply Settings.**

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

Linking an ESRS IP Client to a Policy Manager

Linking an ESRS IP Client to a Policy Manager ensures that policy enforcement and auditing are enabled for the ESRS IP Client. For more information about using a Policy Manager, see "Policy Management" on page 169.

The following procedure explains how use the Configuration Tool to link a ESRS IP Client to a Policy Manager.

CAUTION

The Configuration Tool checks connectivity to the IP address and port that you specify in the following procedure. If the tool is unable to reach the Policy Manager, a warning message will appear. If you ignore the warning message and continue to enable the Policy Manager, the ESRS IP Client will lose connectivity to the Enterprise server. To avoid this problem, do not enable a Policy Manager unless the ESRS IP Client can connect to it.

To link an ESRS IP Client to a Policy Manager:

1. Check **Enable Remote Policy Manager** in the **Policy Manager** tab in the Configuration Tool, as shown in Figure 100 on page 163.

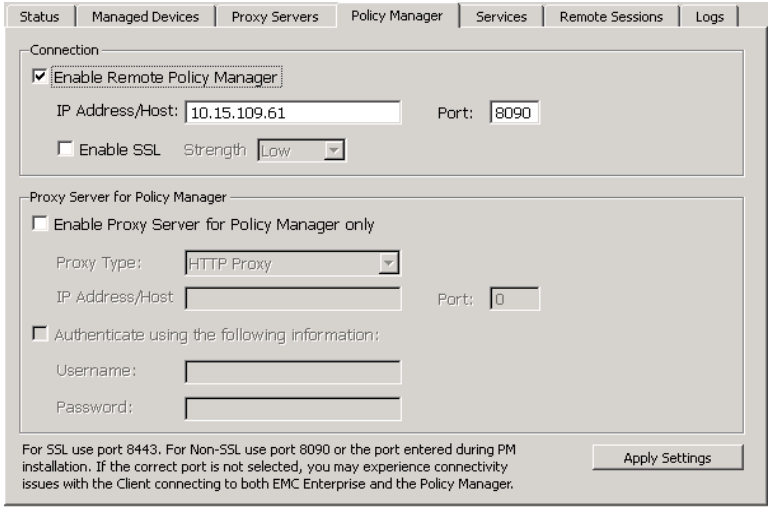


Figure 100 Policy Manager tab

2. Enter the following Policy Manager information:
   - IP Address/Host
   - Port

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

3. Select **Enable SSL** if applicable.
4. If you selected **Enable SSL**, select one of the following choices from the **Strength** drop-down list: Low, Medium, or High. This option enables you to choose the cipher that will be used in communication between the ESRS IP Client computer and the Policy Manager:
   - For an AES 128-bit cipher, select **Low** or **Medium**.
   - For an AES 256-bit cipher or a 3DES 168-bit cipher, select **High**. The Policy Manager will apply the highest strength cipher that it supports.

   Note: The highest strength cipher that Policy Manager currently supports is the 3DES 168-bit cipher. However, the Policy Manager can be configured to use the AES 256-bit cipher. For more information, see Appendix A, "Changing Security Parameters of the Policy Manager SSL Certificate,"and Appendix B, "Enabling SSL communication between the ESRS IP Client and Policy Manager."
5. If applicable, select **Enable Proxy Server for Policy Manager only** and take the following steps:
   a. Select a **Proxy Type** (HTTP or SOCKS) from the pull-down menu. The proxy will be used for ESRS IP Client to Policy Manager communication only. It will not affect the communication between the ESRS IP Client and the EMC Enterprise.

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

   b. In the **IP Address/Host** field, enter the IP address.
   c. In the **Port** field, enter the port number.
6. If applicable, select **Authenticate using the following information** and enter the **User name** and **Password**.

   Note: You must provide a username and password if you are using a SOCKS proxy.
7. Click **Apply Settings**.

The ESRS IP Client is now linked to the Policy Manager.

Disabling communication

To disable communication between an ESRS IP Client and a Policy Manager, remove the check from the Enable Remote Policy Server box.

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

Displaying the status of Services

To display the status of services related to ESRS IP and connect homes, select the Service tab in the Configuration Tool, as shown in Figure 101 on page 165. Each service is listed along with its current state (running or disabled) and its startup type (automatic or manual).

The Service screen is read-only. The Configuration Tool cannot be used to make any changes to the services.

Note: To refresh the data, click **Refresh**. It is not refreshed automatically.

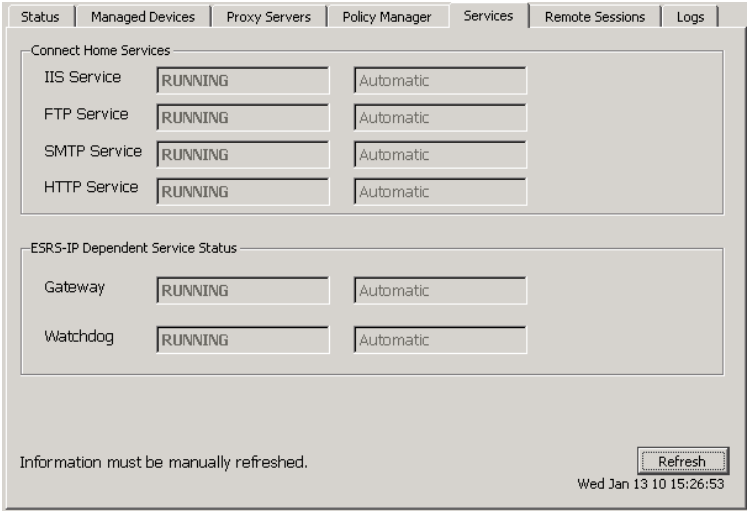


Figure 101 Services tab

Displaying active remote sessions

To display all active remote sessions to a managed device through the ESRS IP Client, click the **Remote Sessions** tab in the Configuration Tool, as shown in Figure 102 on page 166. You will see a list of active remote sessions that includes the following data:

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

Note: To refresh the data, click **Refresh**. It is refreshed automatically every 30 minutes.

The information you see is read-only. You cannot terminate active sessions from this display. However, you can use the ESRS IP Policy Manager to view and terminate remote sessions.

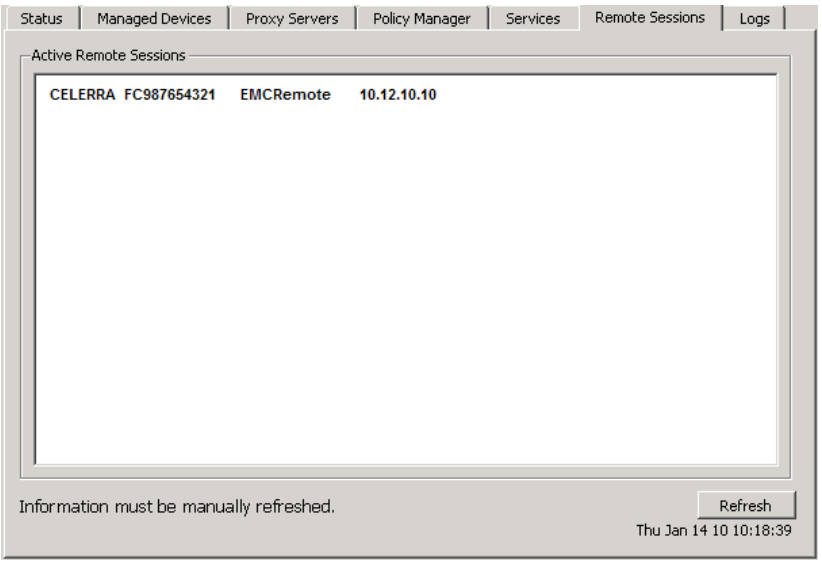


Figure 102 Remote Sessions tab

Displaying the Configuration Tool log files

To display the xGate log that shows activity performed within the Configuration Tool, click the **Logs** tab, as shown in Figure 103 on page 167.

Note: The data in the Logs tab is not automatically refreshed. To refresh the data, click Refresh.

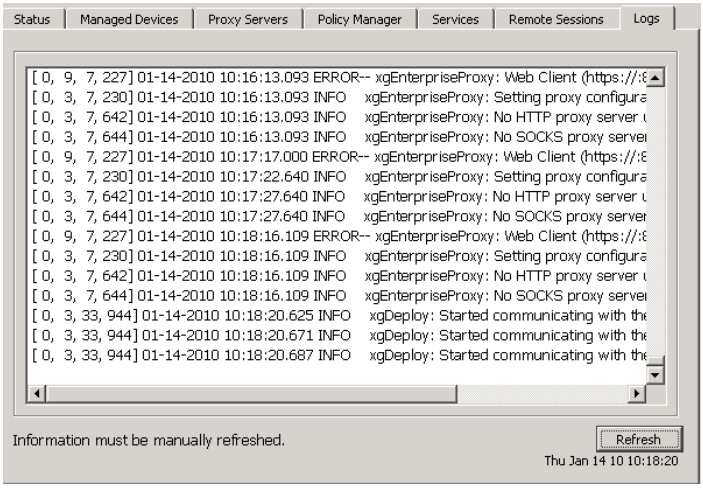


Figure 103 Logs tab

Uninstalling the Configuration Tool

The Configuration Tool is automatically uninstalled when a Gateway Client is uninstalled. For information on uninstalling a Gateway Client, contact your EMC Global Services professional.

PART 3

Policy Management

The Policy Manager enforces the rules for customer-controlled ESRS IP site access and activity.

Chapter 5, "Policy Manager Administration"

Provides policy administrators with instructions for setting up Policy Manager user accounts.

Chapter 6, "Policy Manager Configuration and Operation"

Provides explanations and procedures for policy configuration and storage array access control.

5

Policy Manager Administration

This chapter presents the initial Policy Manager configuration procedures, including web server administration. Topics include:

Startup/shutdown

Upon Policy Manager server startup, its web server automatically starts as a Windows service.

Note: To open the Policy Manager application, see "Logging in to the Policy Manager home page" on page 186.

You can manually start or stop the Policy Manager from the Windows Services item as follows:

1. Open the **Control Panel** in Windows.
2. Open **Administrative Tools**.
3. Open **Services**.
4. Select **ESRS IP Policy Manager** as shown in Figure 104 on page 172.

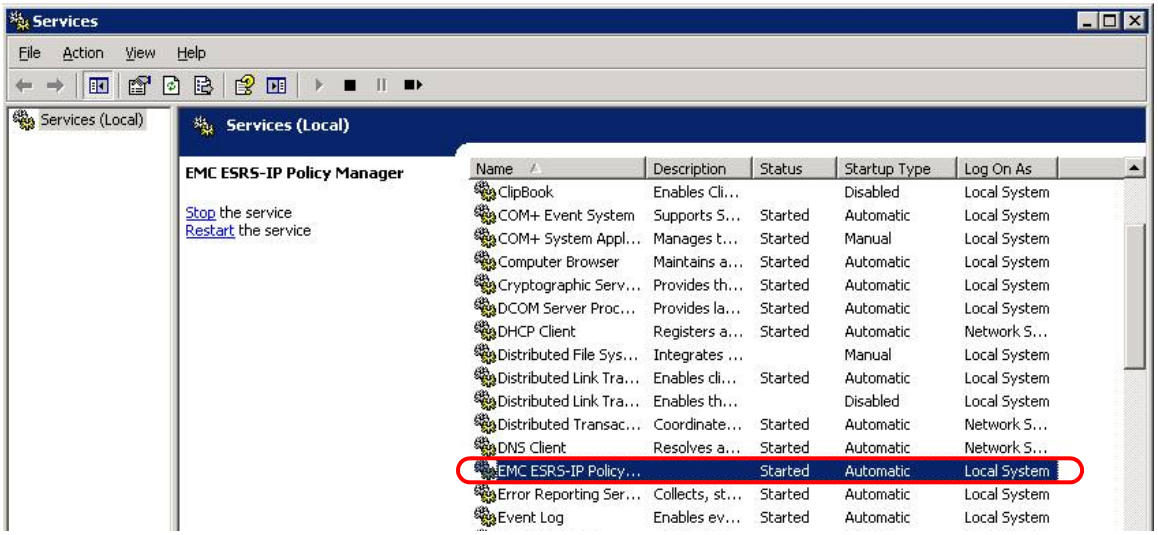


Figure 104 Services listing

5. Click **Stop** to stop the service, as shown in Figure 105 on page 173.

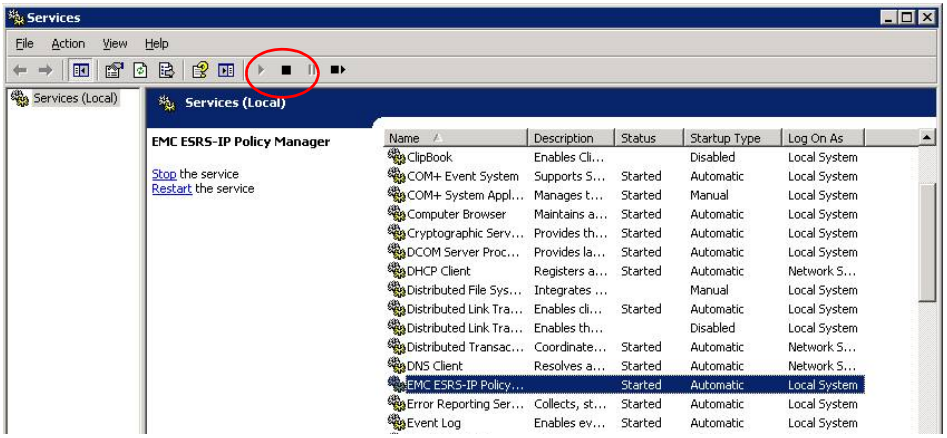


Figure 105 Stopping the service

6. Click **Start** to restart the Policy Manager service, as shown in Figure 106 on page 173.

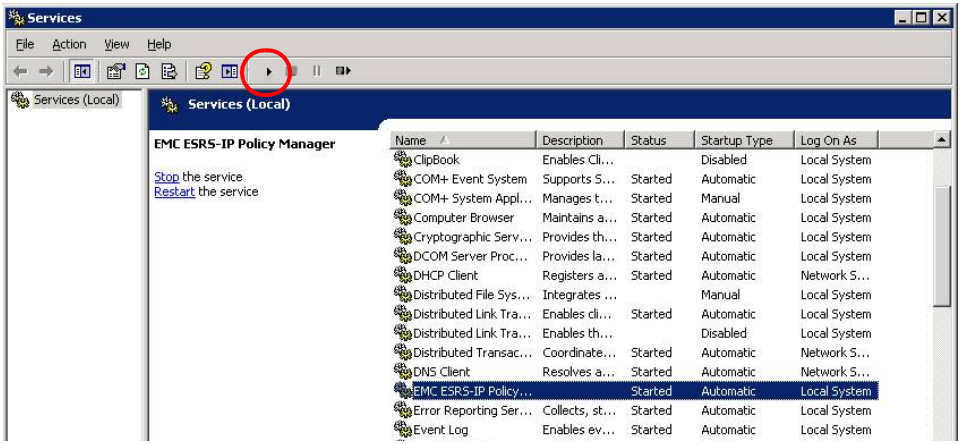


Figure 106 Starting the service

7. Wait 10 seconds after starting the service to permit the Policy Manager to stabilize.

Modifying the login banner

You can change the text that displays in the disclaimer section of the Policy Manager login screen. To change the text:

1. Browse to the following directory location:

```
C:\EMC\ESRS\Policy Manager\Tomcat5\webapps\applications\apm\templates
```

2. Use a text editing program such as Notepad to edit the file disclaimer.html.
3. Save the file without changing the filename.

Policy Manager user accounts

This section provides details about users and user accounts. You assign privileges to the components of the Policy Manager application by configuring *profiles*, *roles*, and *users*. To configure profiles, roles, and users, you use the Administration component of the Policy Manager application. When you first log in as the administrator, all of the appropriate pages are available to you.

Note: To add users, roles, and profiles, you must be an administrator of the directory server associated with Policy Manager, because adding users in the Policy Manager application adds them to your directory server. Whether you are using the internal directory server or an external directory server, be sure you know the administrator login and password for the directory server.

Although you can create profiles, roles, and users in any order, you may want to create profiles first, then roles, and finally users. You can always return to the created profiles, roles, and users and edit their definitions later. Note that you cannot rename these elements; you must delete them and create new ones. The rest of this section explains how to create a profile, a role, and a user. To learn about editing them, refer to the online help for the Policy Manager application.

Creating a profile

Profiles control the privileges within the application and are assigned to roles or users.

To create a profile, you must have View and Add/Edit privileges to the Administration component. If you are logged in as the administrator of your directory server, you have those privileges.

To create a profile, follow these steps:

1. Click the **Administration** tab.
2. From the **New** menu, select **Profile**. The **Create profile** page appears as shown in Figure 107 on page 176.

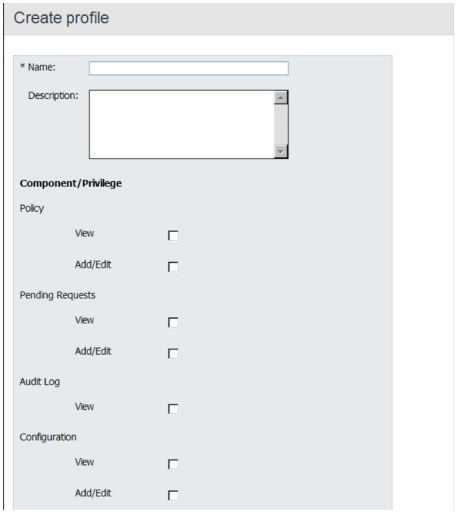


Figure 107 Create profile page

3. In the **Name** field, type a unique identifier for the profile, using up to 50 characters with no spaces, punctuation, or special characters. You may want to use the names of the components. For example, you might type AuditLog, Policy, PolicyView, or PendingRequests.

   Note: If you use spaces, punctuation, or any special characters, the system will return an error message when you click **Next**.

4. In the **Description** field, type a brief description of the profile. For example, if you are assigning both the View and Add/Edit privileges for a component, type the names of the privileges here. They are NOT shown in the View and remove profiles page, unless you type them here. The Description field is optional.
5. Under **Component / Privilege**, select the checkbox for each privilege that you want to assign to the profile. Scroll as needed to find the Administration and Remote (Sessions) privileges.
6. When you have completed these steps, click **Submit** to save the new profile. To discard the profile, click **Cancel**.

The View and remove profiles page appears when you exit the Create profile page. If you created the profile, the name and description appear in the View and remove profiles page. Notice the Delete link in the Actions column. You can click this link to remove the related profile.

7. Repeat these steps for each profile that you require.

Tips:

If you want both Add/Edit (or End) and View privileges for a component, select the checkbox for Add/Edit. The View privilege is automatically selected and that checkbox becomes unavailable.

Because you will group profiles together to create roles, you may want to keep the profile set as simple as possible. For example, create one profile for each component that has both View and Add/Edit privileges.

If you want certain users to have View but not Add/Edit to a component, create a View-only profile for that component. For example, the user who will monitor Pending Requests may want to view the Policy for a device group before accepting or denying a request. You can create one profile called PolicyView with only the View privilege, and a PendingRequests profile with both View and Add/Edit privileges. When you create a RequestManager role, you can assign both profiles to the role.

Creating a role

Roles are equivalent to groups. Roles and groups contain users. Profiles are assigned to roles. Roles control user access based on the profile(s) assigned to the role. This facilitates Policy Manager management.

To create a role, you must have View and Add/Edit privileges to the Administration component.

If you are logged in as the administrator of your directory server, you have these privileges. To create a role, follow these steps:

1. Click the **Administration** tab.
2. From the **New** menu, select **Role**. The **Create role** page appears as shown in Figure 108 on page 178.

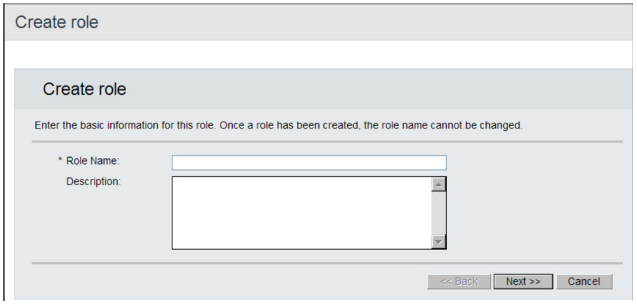


Figure 108 **Create role page**

3. In the **Role Name** field, type a unique identifier for the role, using up to 50 characters with no spaces, punctuation, or special characters. **Role Name** is a required field.

   Note: If you use spaces, punctuation, or any special characters, the system will return an error message when you click **Next**.

4. In the **Description** field, type a brief explanation of the role, using up to 200 characters.
5. Click **Next** to display the Assign profiles to role page as shown in Figure 109 on page 178.

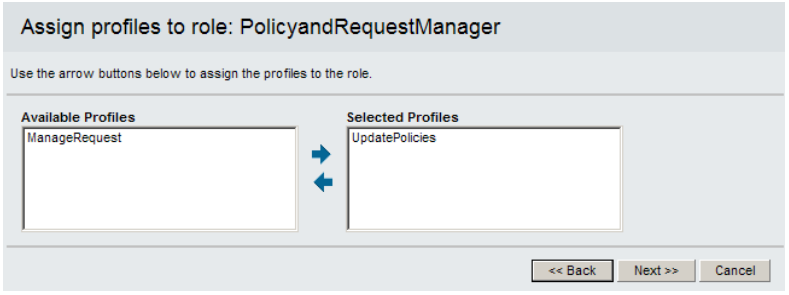


Figure 109 **Assign profiles to role**

6. In the **Available Profiles** list, select the profiles that you want to assign to this role and click the right arrow to move them to the Selected Profiles list. To select more than one profile at a time, press the SHIFT or CTRL key while you click each name. If you decide not to use a profile, select it in the Selected Profiles list and then click the left arrow to move it back to the Available Profiles list.

7. When you have completed your profile selections, click **Next**.
8. The **Assign users to role page** appears. Assuming that you have not configured any users yet, click **Next** again. The **Confirm role details** page appears.
9. Review the information in this last page, and click one of the following options:
   - **Finish** to create the role.
   - **Back** to make a change. Click this button until the appropriate page is displayed. Make your changes, return to this page, and click Finish.
   - **Cancel** to exit without creating the role.
10. Repeat these steps for each role that you want to create. You will assign users to the roles while creating the users.

Tip for selecting the profiles:

Consider the privileges that you want the user who will be assigned this role to have. For example, if the user will monitor and respond to Pending Requests from the ESRS IP Clients, the user must have View and Add/Edit privileges to the Pending Requests component. In addition, you may want to assign the View privilege to the Policy component so that the user can check the policy of a device group before accepting or denying a request. You may also want to give the View privilege to the Audit Log so the user can view messages from the devices.

Creating a user

Now that you have created the profiles and roles, you are ready to create the users and assign them the roles that will give them the privileges they need to do their jobs. To create users, you need the View and Add/Edit privileges to the Administration tab. You also need the login name and password of the administrator for the directory server that you are using with Policy Manager.

To create a user, follow these steps:

1. Select the **Administration** tab.
2. From the **New** menu, select **User**. The Create user page appears as shown in Figure 111 on page 180, *unless* this is your first access during your current login session with Policy Manager. If this is your first access, the Authentication Required dialog box appears, as shown in Figure 110 on page 180.

Figure 110 Authentication Required

3. If the Authentication Required dialog box appears, enter the User name of the administrator of your directory server. For the OpenDS server installed with Policy Manager, type **admin**. If you use a different directory server, it may require a different user name.
4. Type the Password for the administrator of your directory server. For the OpenDS server installed with Policy Manager, type **admin**. If you use a different directory server, it may require a different password.
5. Click **Submit** to send these credentials to the directory server. If the authentication is successful, you can start to enter the information for the new user in the Create user page shown in Figure 111 on page 180.

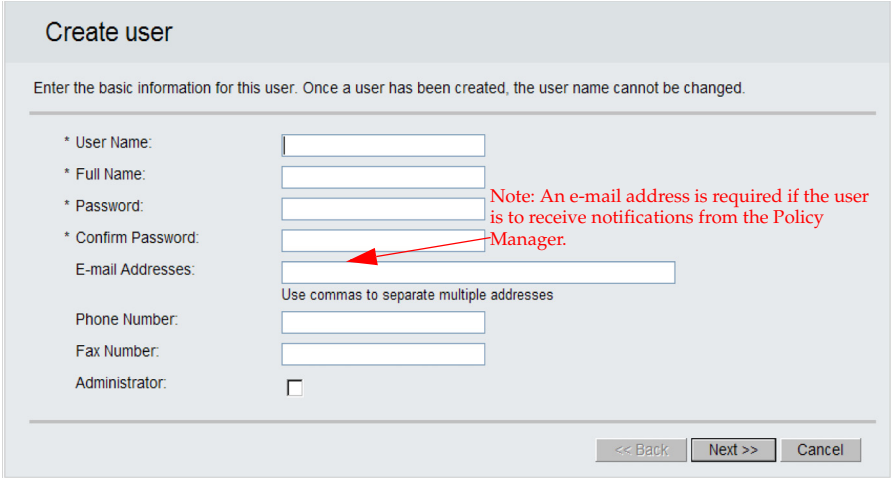


Figure 111 Create user page

6. In the **User Name** field, type a unique identifier for the user, using up to 50 alphanumeric characters with no spaces, punctuation, or special characters. Keep in mind that you cannot change this user name once the user has been created.

   Note: If you use spaces, punctuation, or any special characters, the system will return an error message when you click **Next**.

7. In the **Full Name** field, type the first and last names of the user. You may use up to 50 alphanumeric characters, a period, and spaces.

8. In the **Password** and **Confirm Password** fields, type the initial password for the user. Passwords must be at least six characters long and can be up to 50 characters long. This field accepts alphanumeric characters, spaces, and punctuation characters. For security reasons it is preferable to create passwords that include lowercase letters, uppercase letters, numerals, and punctuation characters.

9. If you want the user to be able to receive e-mail notifications from Policy Manager regarding device groups that have been assigned to the user, type the E-mail Address for the user. If more than one address is needed, separate the addresses with a comma. Be sure to use a comma as a separator, not a semicolon. Use the following e-mail address format: username@company.com.

   Note: In order for the user to receive these e-mail notifications, you must also configure the notification e-mail settings as described in "Configuring e-mail notifications" on page 231.

10. If desired, type the Phone Number and Fax Number for the user. These fields accept numerals and hyphens.

11. If the user is an administrator of Policy Manager and the local directory server, select the Administrator checkbox. When you select this option, the Assign roles to user page does not apply and does not appear. The user has all privileges to all components of the Policy Manager application.

12. Click **Next**. If you selected the Administrator checkbox, the Confirm user details page appears as shown in Figure 113 on page 182. In this case, skip the next two steps and continue with

step 15. If you did NOT select the Administrator checkbox, the Assign roles to user page appears. Figure 112 on page 182 shows this page with two roles already selected.

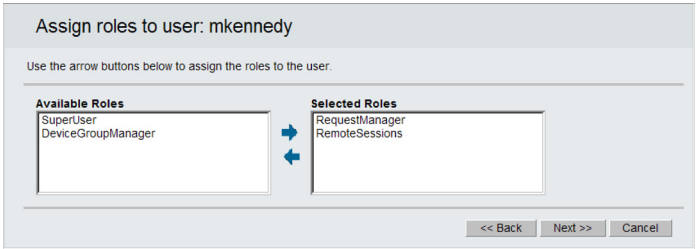


Figure 112 Assign roles to users page

13. In the **Available Roles** list, select the roles that you want to assign to this user and click the right arrow to move them to the Selected Roles list. To select more than one role at a time, press the **SHIFT** or **CTRL** key while you click each name with the mouse. If you decide not to use a profile, select it in the Selected Roles list and then click the left arrow to move it back to the Available Roles list.
14. When ready, click **Next**. The **Confirm user details** page appears as shown in Figure 113 on page 182.

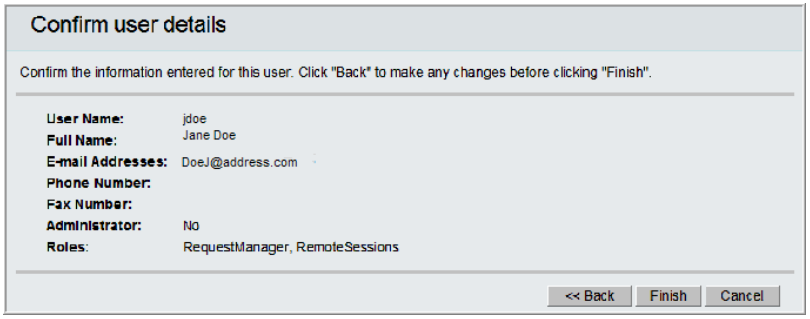


Figure 113 Confirm user details page

15. Review the information shown and click one of the following buttons:
    - **Finish** to create the role.
    - **Back** to make a change. Click this button until the appropriate page is displayed. Make your changes, return to this page, and click Finish.
    - **Cancel** to exit without creating the role.
16. Repeat these steps for each user that you want to create.

LDAP authentication

You can configure Policy Server to use either your internal directory server or an external LDAP directory server for user authentication.

During Policy Manager installation, you choose whether to have the installation program install and configure your local directory server (OpenDS) or an external LDAP directory server. If you choose to install an external LDAP directory server, you indicate whether you want to use Sun ONE LDAP or OpenDS LDAP, and then provide the configuration information to the installation program.

For information about installing and configuring an external LDAP directory server, refer to "External LDAP integration" on page 288.

Note: The ESRS IP Solution does not currently support Microsoft Active Directory.

6

Policy Manager Configuration and Operation

This chapter presents the main policy management interface for the Policy Manager. Topics include:

Introduction

This section explains how to log in to Policy Manager, how to change the Policy Manager date format, and how to enable Policy Manager support for Internet Explorer 8 (IE8).

Logging in to the Policy Manager home page

Once your Policy Manager system administrator has assigned you a username and password, log in to the Policy Manager application as follows:

1. Open a web browser. Type the Policy Manager server's IP address or domain name and the port number that the web server uses (8090, or 8443 for SSL, or the alternate port number designated at installation) in the following URL:

   `http://HostName(FQDN)_or_IPAddr:PortNumber/`

   For example:

   `http://server1.customer.com:8090/`

   Another example:

   `https://10.241.172.13:8443/`

   Note: If your installation uses Secure Sockets Layer (SSL), you must use https as shown in the previous example.

   If you open the web browser on the Policy Manager server itself, you can type:

   `http://localhost:port_number/`

   For example:

   `http://localhost:8090/`

   The Policy Manager login screen appears as shown in Figure 114 on page 187.

   Note: "Modifying the login banner" on page 174 describes how to configure the disclaimer section of the login screen.

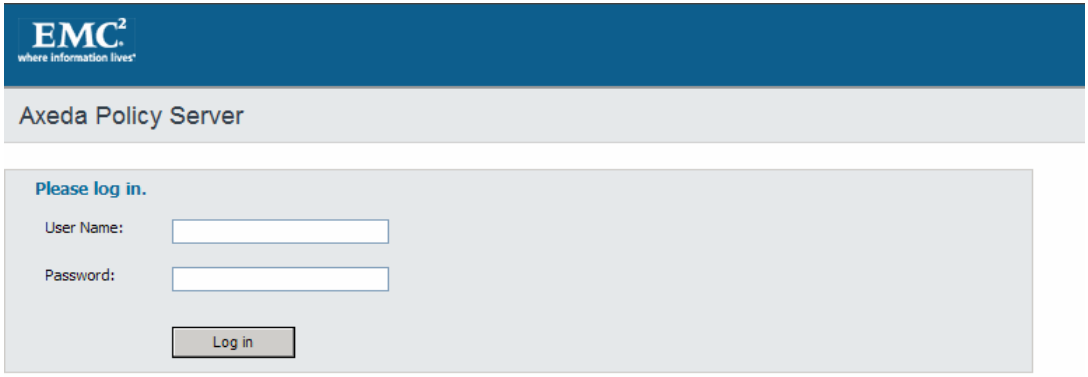


Figure 114 Policy Manager login screen

2. Type the username and password given to you by your system administrator and click **Log in**.

   The Policy Manager home page appears, with links to the roles-based, user-accessible features of the Policy Manager application, as shown in Figure 115 on page 187.

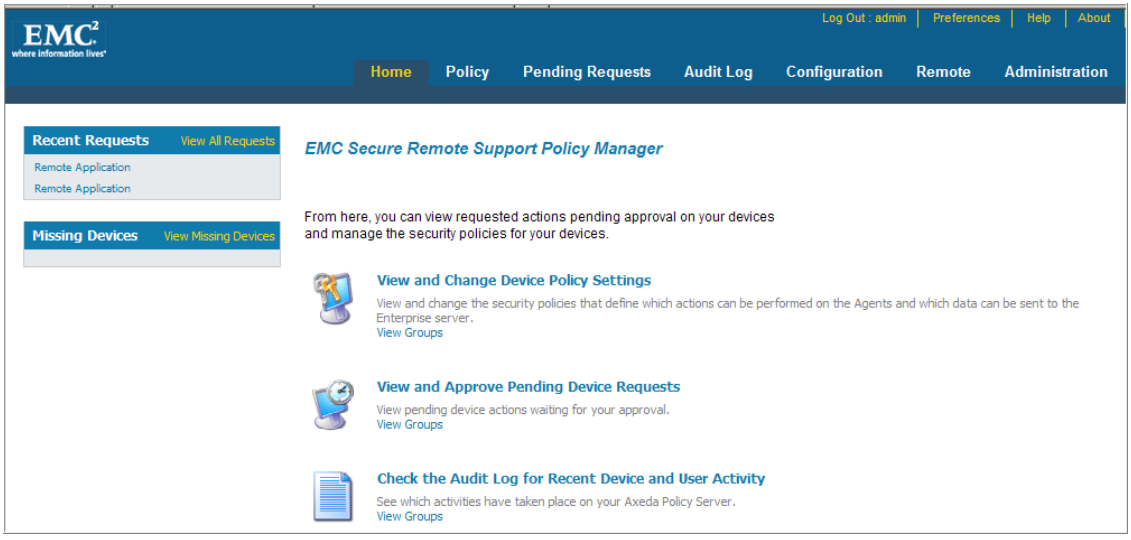


Figure 115 Policy Manager home page

3. Access the main Policy Manager features by clicking the following tabs:
   - **Policy** — View or change the policy settings, as described in "Policy settings" on page 189. This is where you initially set or modify the policy settings for the Global group.
   - **Pending Requests** — Review and edit currently active transactions, as described in "Pending requests" on page 220.
   - **Audit Log** — Review completed transactions, as described in "Remote sessions" on page 236.
   - **Configuration** — Configure device groups (a single set of policies applies to all devices in a group), as described in "Configuration" on page 229.

Changing the Policy Manager date format

You can choose either of the following date formats for Policy Manager: MM/DD/YY or DD/MM/YY. The default format is MM/DD/YY.

To change the date format:

1. Click **Preferences** at the top of the Policy Manager home page as shown in Figure 115 on page 187. The User Preferences screen appears.
2. In the User Preferences screen, select a date format from the **Date Format** drop-down list box.
3. Click **Submit** to save your date format preference.

Enabling support for Internet Explorer 8

Windows Internet Explorer 8 (IE8) is not automatically supported by the Policy Manager. You can enable support by editing your compatibility view settings within IE8.

To enable Policy Manager support for IE8:

1. From the Command Bar in IE8, select **Tools.**
2. Select **Compatibility View Settings**.
3. In the **Address** box, enter the website URL for Policy Manager.
4. Click **Add**.
5. Click **Close** to save your compatibility setting.

Policy settings

ESRS IP Policy Manager has policy settings at the following levels:

- Global
- Group
- Device

Policy settings for each of these levels are discussed in the following sections.

Global policy settings

Global policy settings are the top, or parent, level settings. This section describes how to view the Global settings, and explains *permissions*, *actions*, and other policy settings.

To view the Global policy settings:

1. Log in to the Policy Manager home page, following the procedure in "Logging in to the Policy Manager home page" on page 186.
2. Click **Policy** to view settings for the top-level Global group.

   Figure 116 on page 190 shows the Global group page.

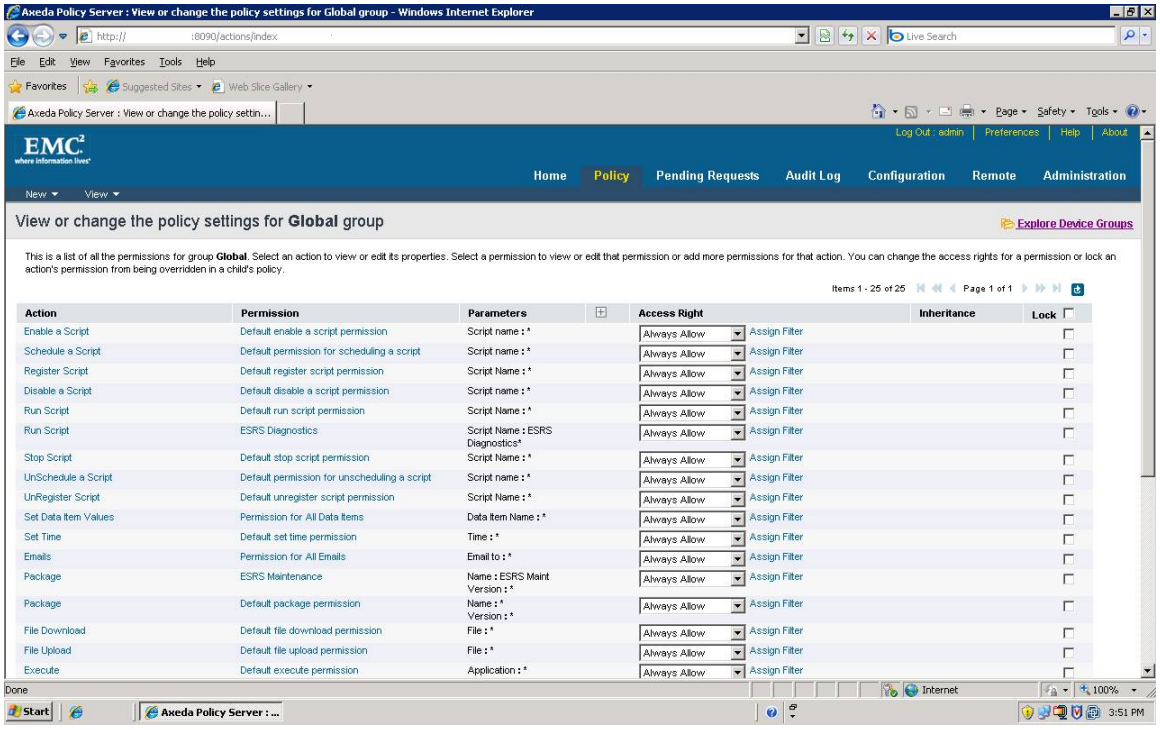


Figure 116 Global policy settings

In the Global settings page you will see six fields that represent the policy record for each *permission*. A permission is an *action* with defined *parameters*. The permission also has an *access right* setting that

tells you whether it is allowed for that group. Table 6 on page 191 provides an explanation and example of the policy settings.

Table 6 Policy settings

Action	Permission	Parameters	Access right	Inheritance	Lock
Behavior regulated by Policy Manager	Specific version of an action	Defines a general *action* through the use of specified limits (*permission*)	Allows or denies permission: The *value* of the permission	Shows source level of access right, at or above current level	Can lock access right for lower levels
Listed in Table 7 on page 191 and Table 13 on page 280 **Example**	See Table 14 on page 283		See Table 8 on page 201		
Remote Application	Celerra Remote Access Application - CelerraMgr	Remote Application Name: CelerraMgr	Always Allow [can choose from menu]	Celerra	[optional]

Note: Scrolling the policy settings window shows all line-item global action/permission records. Although a number of actions are available to the ESRS IP solution, only a subset are currently used in the Policy Manager (the grayed out text are the actions currently not used). The actions are listed in Table 7 on page 191.

Table 7 Actions (Global group default set)

Enable a Script	Set Time	Restart Client
Register Script	Package	Execute
Disable a Script	Alarms	Remote Application
Run Script	Events	Remote Terminal
UnSchedule a Script	Data Item Values	Enable a Timer
Schedule a Script	Emails	Remove a Timer
Stop Script	Modify Ping Update Rate	Disable a Timer
UnRegister Script	File Download	Create a Timer
Set Data Item Values	File Upload	Stop Remote Session

Note: You cannot modify the grayed out values.

Group policy settings

At the level beneath Global is a ***group*** for each device type (for example, CLARiiON devices; Symmetrix devices). Each group has its own set of rules. Global permission and access right defaults are inherited by the device type groups.

To view the device groups, select the **Explore Device Groups** link at the upper right of the page.

The Select a Device Group window appears as shown in Figure 117 on page 192. The window shows the hierarchy of preset groups as well as the devices registered with the Policy Manager.

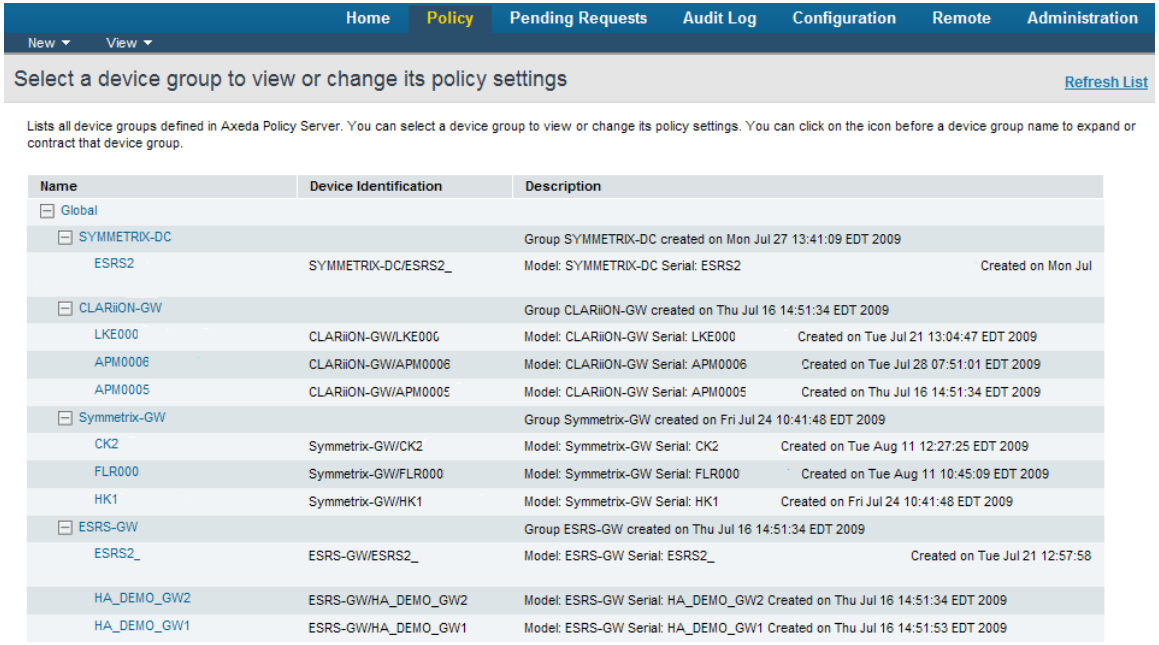


Figure 117 Group policy settings

Configure group policy settings

To configure group policy settings:

1. Log in to the Policy Manager home page, following the procedure in "Logging in to the Policy Manager home page" on page 186.

2. Navigate to the correct policy settings page by clicking the **Policy** tab, then the **Explore Device Groups** link, and then a group (name) link.

   This opens the policy settings page for the selected group.

3. For each desired action/permission line item, select the desired access right in the policy settings page. Your choices are:

   - **Always Allow**
   - **Ask for Approval**
   - **Never Allow**

4. Click **Done** at the bottom of the page, and click **OK** on the **Update this policy?** dialog box.

5. Repeat step 2 on page 193 through step 4 on page 193 for other groups desired.

Group hierarchy: Preset groups

Each policy group is designated by a line item that links to further information for each group. Your Policy Manager installation includes a default set of second-level groups:

```
Atmos-GW
Celerra-GW
Centera-GW
CLARiiON-GW
CLARiiON-GWM
Connectrix-GW
DL3D-GW
DLm-GW
EDL-Engine-GW
Invista-GW
RecoverPoint-GW
Switch-Brocade-B-GW
Switch-Cisco-GW
Symmetrix-GW
VPLEX-GW
```

The abbreviations in the policy group list have the following meanings:

- GW—managed by Gateway
- GWM—managed by a CLARiiON Management Station

Note: You cannot alter the group names.

The following group is also found under the Name column:

```
ESRS-GW
   ESRS_Site_ID_ …
```

The ESRS-GW group represents the Gateway Client, and contains policy that you may want to edit as you would with the EMC product devices.

From the top level, the default structure of policy settings groups reflects device types (EMC product families) and particular devices:

Global [the top-level group]

Device Type [the group identified by product name]

Device [the group identified by product serial number]

To see the policy settings for a particular group, locate the group in the hierarchy and click its name to open the corresponding policy settings page.

Device policy settings

At the level beneath Group is *device*. Each device can have its own set of rules. The device inherits device permission defaults and access right defaults from its higher-level group.

Device type settings page

If you select a product from the *group* hierarchy, you see policy settings for that product, which are also the default settings for specific product devices (the next lower level).

Actions listed at the global level will be the same as those listed at the individual product level.

Device settings page

From the group hierarchy, select the group for a particular device. The device is represented below the device type name by a serial number—for example, ML12345678900.

You now see policy settings for that device only. Some may be inherited from the global settings, some from the device group settings (for example, the Celerra device group), and some may be specific to that device.

Remote Support Application permissions

CAUTION

The current implementation of Policy Manager controls all remote applications for a specific device or device group under a single permission inherited from the Global permission "Remote Application." If you decide you want to control each remote support application individually, you *must* create *all* support applications associated with the specific device and set the permissions individually. Any application that is not defined will not be available for use, which may impact EMC's ability to properly support the device in question.

If the definitions are created at the Group level, they will propagate to all the devices within the group. If they are defined at the Device level, they will only apply to that specific device. Individual remote applications should not be defined at the Global level.

A decision to control each remote support application individually should not be taken lightly, as it can greatly complicate Policy Manager configuration and management and may impact the ability to upgrade to future releases of the product.

Overview

An EMC Global Services professional may need to use a remote support tool to provide remote support to a device. The Policy Manager defaults to Always Allow for each EMC product remote support application. If you wish to change a particular remote support application to Ask for Approval or Never Allow, you must create a remote application permission for that application, and then you must change the access right.

Note: If the Remote Application permissions functionality is used to set permissions for something other than remote applications, the ESRS IP Solution may stop functioning as designed. This may have a negative impact on EMC device connect home and connect in capabilities.

Creating a Remote Application permission

To create a remote application permission:

1. Navigate to the **Policy** tab and select the global group, product group, or individual device for which you are setting the permission. (Depending on the screen you are viewing, you first might need to click **Explore Device Groups**.)
2. In the Action column, click **Remote Application.** The Remote Application action screen appears as shown in Figure 118 on page 196.

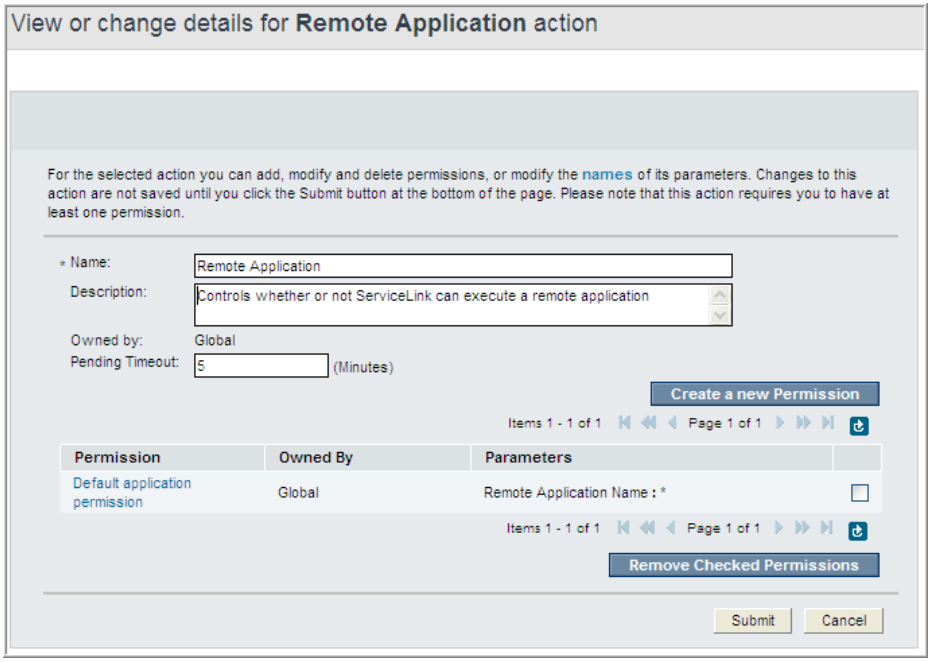


Figure 118 Remote Application action

3. Click **Create a New Permission**. The Permission screen appears.
4. Enter a Permission Name and Description as shown in "Add a new permission" on page 197.

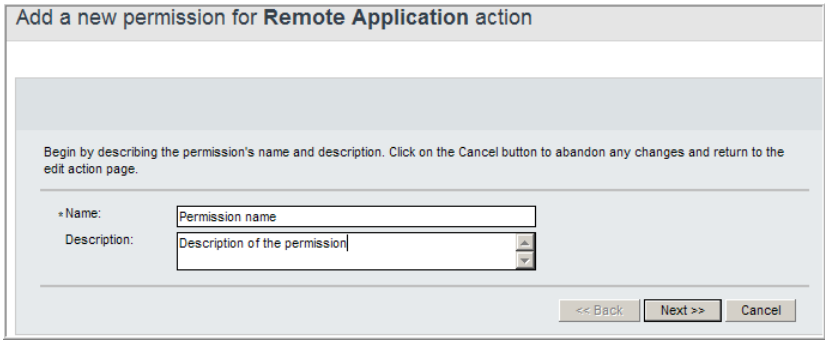


Figure 119 **Add a new permission**

5. Click **Next**. The Remote Application action screen appears.
6. Enter the Remote Application Name as shown in Figure 120 on page 197.

Note: In order for the Remote Application to execute successfully, you must enter the Remote Application Name *exactly* as defined within EMC's enterprise servers (including upper and lower case letters as required). For example, the RemotelyAnywhere application name must be entered with upper case R, upper case A, and no spaces. For a listing of the correct syntax for each EMC remote application, see "Required syntax" on page 285.

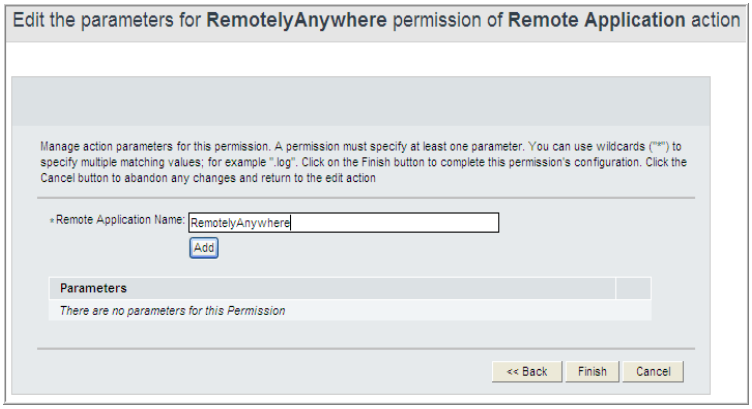


Figure 120 **Remote Application name**

7. Click **Add**. The Remote Application Name that you entered appear in the Parameters window, as shown in Figure 121 on page 198.

Figure 121 Parameters window

8. Click **Finish** if you are satisfied with your entry. The View or change details screen appears, as shown in Figure 122 on page 198.

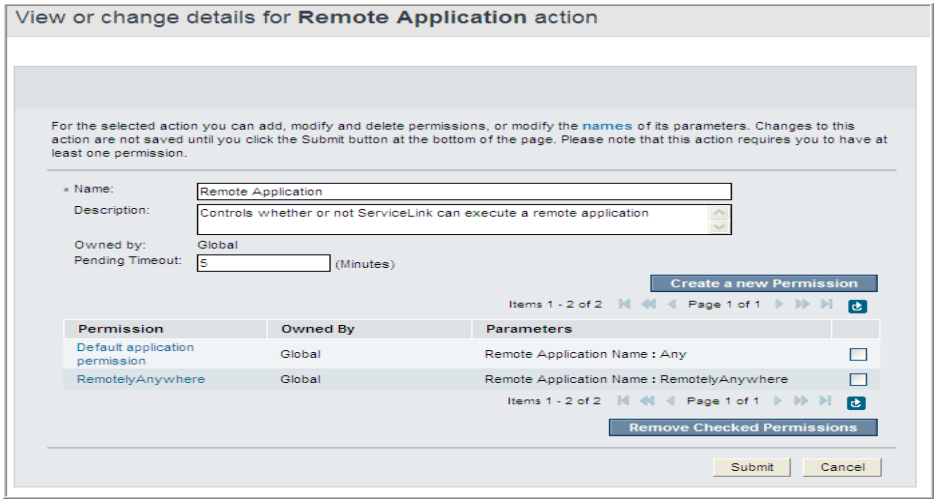


Figure 122 View or change Permission details

9. Click **Submit** if you are satisfied with your entry. The permission you created is now listed separately.

Your next step is to set the access right as desired, remembering that the default setting is Always Allow. For general information about

access rights, including a description of each access right, see "Access rights" on page 200. For information on setting an access right, see "Set access rights" on page 217.

Access rights

Policy settings are embodied in *access rights*. Each permission has an access right that specifies whether it can be executed.

Default settings

The policy for each new device registering with the Policy Manager is inherited from the device type. Device type policy is preset by EMC, but some of the policies can be edited.

Associated access rights

Policy for a particular group consists of a set of permissions (action-parameter combination). Each permission has one of the following associated access rights:

- **Always Allow**
- **Ask for Approval**
- **Never Allow**

IMPORTANT

Do not change the Set Data Items policy, which is set to Always Allow. That policy is applied to remote access server information that is updated and passed every 30 days. The information update is used to provide optimal connectivity to the end device. If you set the Set Data Items policy to Never Allow, or if you set the policy to Ask for Approval and the request is denied, the end device might not have the most current information.

The access right options are described in detail in Table 8 on page 201.

Table 8 Access right descriptions

Name	Description
Always Allow	The ESRS IP Client can execute these permissions without asking for approval or sending the action information to Policy Manager (the ESRS IP Client does log an entry in the Policy Manager audit log). To see which actions of Always Allow rights were performed on a device, refer to the device's log file.
Ask for Approval	The ESRS IP Client forwards the action and its parameters to Policy Manager for approval. When Policy Manager receives the action, it sends an e-mail to the address specified for the device's policy and then stores the action request in the Pending Requests queue. The action request remain shown in the Pending Request page until it is approve or denied, or it times out. (If timed out, the action is denied and needs to be requested again, if desired, and a message is logged to the Policy Manager audit log.) If approved or denied, the action request is removed from the Pending Requests page. A message regarding the approval or denial is logged to the Policy Manager audit log. Policy Manager sends its response (accept or deny) to the ESRS IP Client. If the action request was approved, the device processes the action.
Never Allow	The ESRS IP Client does not execute these permissions and sends information for these requests to Policy Manager only when Never Allow actions are requested from the ESRS IP Client. To see which device-initiated actions of Never Allow rights were denied on a device, refer to the device's log file.

Locked policies

The Policy Manager contains eight locked policies that are not visible from the Policy Manager user interface. The access rights for these locked policies are set to **Always Allow**. In order for the ESRS IP Solution to function correctly, the access rights for these policies may not be changed.

The following list describes each locked policy:

- **Data Item Values** — This policy controls sending data item values to the Enterprise server. The data item values are required for EMC to monitor device connectivity.
- **Package: ESRS Sync** — This policy controls sending synchronization messages to the ESRS IP Client. They are required for device deployment, device edits and device removals.
- **File Upload: Connect Home Files** — This policy controls files uploaded to the EMC Enterprise from the ESRS IP Client. These file uploads are necessary to send health status messages from EMC devices to the EMC Enterprise.

- **File Download: ESRS Device Registration** — This policy controls files downloaded from the Enterprise server to the ESRS IP Client. The files are required for device registration.
- **Events** — This policy controls sending EMC device event notifications from the ESRS IP Client to the EMC Enterprise.
- **Alarms** — This policy controls sending alarms from the ESRS IP Client to the EMC Enterprise. These alarm notifications provide the EMC Enterprise with notification if there are Gateway Client or EMC Device connectivity issues.
- **Modify Ping Update Rate** — This policy controls the ability to edit the frequency at which the ESRS IP Client server sends status messages to the Enterprise server. The messages are necessary for monitoring of the ESRS IP Client and all managed devices.
- **Restart Agent** — This policy controls the ability to restart the ESRS IP Client services from the EMC Enterprise.

Filters

A *filter* is a set of restrictions for a permission. You can create a filter and assign it to one or more permissions in the same policy or in different policies. You must have Add/Edit permission to the Policy component of the application to create, edit, delete, or assign filters to permissions.

Note: When you add or edit a filter, it is very important that you thoroughly test the filter. This will ensure that you do not negatively impact the solution and that the filter functions as expected.

IMPORTANT

Do not modify the SYR filter for access, which is set to Always Allow. Changing this setting may negatively affect ESRS support. For more information on the SYR filter, see "Adding an SYR filter at the device level" on page 213.

Default permission filter

Every permission has a default filter that cannot be removed. The default filter is an access right that can be set to Always Allow, Ask for Approval, or Never Allow. A default filter has no name, expression, or time window. If the permission has multiple filters, the default filter is always the last one in the list. When the ESRS IP Client evaluates the filters for a permission, if no user-defined filter in the list is a match, then the ESRS IP Client evaluates the default filter, which always matches.

Additional filters

Adding filters to permissions enables you to:

- Maintain a static list of permissions, each with a default access right
- Explicitly allow a user access to an action but deny access to everyone else by default
- Explicitly deny a user access to an action but by default ask for approval for everyone else
- Create a time window (for example, a window called *Maintenance Window*) to allow or ask for approval when users access the device during the Maintenance Window, and deny at any other time
- Assign multiple filters to a permission to set up a complex set of allow, ask, deny rules. For example, the filter list for a permission such as Access SSH Remote Session could read:

1. Always allow userId="123456" from 1 PM - 3 PM on Saturdays and Sundays.
2. Ask for approval when a particular Partner user requests an action on a device.
3. Always allow everyone during Maintenance Window.
4. Deny in every other case.

Assigning filter names and access rights

When you create filters, you must assign the filter a name that is unique in the Policy Manager database, and you must assign an access right to the filter (Always Allow, Ask for Approval, or Never Allow). If you want to restrict a permission to specific EMC Global Services users at certain times, you can add expressions, which can consist of variables, values, and operators:

- For operators, you can use the equals sign (=) and the AND operator.
- For variables, you can specify the userId and the domain name of the Enterprise server (enterpriseId) from which the ESRS IP Client received the action request. (The userId is the user's EMC backend log in ID.) Values for variables can contain the asterisk (*) wildcard character to represent zero or more characters.

Notes about expressions:

- Grouping and other Boolean operators, such as OR and NOT, are not supported.
- In general, expressions are case insensitive. For example, you can enter and or AND for this Boolean operator; the results are the same. However, the variable names must be entered as follows: *userId* and *enterpriseId* (uppercase I, lowercase all other letters).
- When they evaluate expressions, the ESRS IP Clients parse and check the syntax. Policy Manager does NOT check expression syntax.
- For examples of expressions, refer to the online help for the Policy Manager application.

Restricting access to specific time periods

To restrict access to a certain period of time, you define a Time Window for the filter. You can choose a fixed time period or one of two recurring time periods. The Time Window options follow:

- (Blank) — This option specifies NO time period. If you previously added a Time Window and need to remove it, select this option.

- One Time — This option allows the action for a single time period. This time period can span days, weeks, or months. When you select this option, you must select a Start Date and Start Time as well as an End Date and End Time:
  - For the date fields, click the calendar icon and select the date. If you manually enter a date, you must use the following format to avoid unexpected results: mm/dd/yy.
  - For the time fields, use the format HH:MM AM or PM. For example, between 10:00 AM on 10/4/2010 and 9:00 AM on 10/6/2010.
- Weekly Recurrence — This recurring option allows the action on specified days of the week, during specified hours. For example, between 5:00 PM and 8:00 PM every Monday and Wednesday, or every Tuesday and Thursday from 4:00 AM to 8:00 AM.
- Weekly Range — This recurring option allows the action during a specified range of days of the week. The period begins at the Start Time on the Start Day of the week. The time period ends at the End Time on the End Day of the week. For example, between 5:00 PM on Friday and 9:00 AM on Monday.

Viewing details for default and assigned filters

After you have defined your own filters and assigned them to one or more permissions, the Access Right column for those permissions shows the default filter. It also contains the details for the assigned filters.

The column to the left of the default filter shows an Expand icon (+) that you can click to display the details of all filters assigned to a permission. The filters appear in the order in which the ESRS IP Client will evaluate them, from first to last, with the default filter shown last.

Keep in mind that, when other filters are assigned, they are evaluated in the order in which they appear here and the default filter is always evaluated last. For details on how the ESRS IP Clients evaluate filters, see "Filter evaluation" on page 206.

For each permission that has at least one filter assigned to it, you will see the following icon to the right of the Assign Filter link: This icon is for informational purposes only. Click the Expand icon ( ) to view details about the filter(s) assigned to the permission.

Figure 123 on page 206 shows an example of a custom permission, Execute Notepad, to which two filters have been applied. The Access Right column has been expanded to show you the filter details.

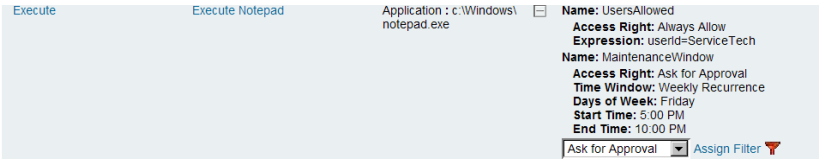


Figure 123 Custom permission

If the permission inherited filters from the parent device group or if another filter was applied directly to this permission for this device group, you will receive a warning when you click the Assign Filter link. This warning tells you that you will lose all other applied filters by following this link. If only the default filter is shown for the permission, then you will not see this warning. The default filter is always preserved.

If the Access Right field is disabled, the permission is locked at a higher level. The name of the parent device group where the permission is locked appears in the Inheritance column.

Online help

For more information about creating, editing, deleting, and assigning filters, refer to the online help for the Policy Manager application.

Filter evaluation

Filters are evaluated in the order in which they appear or in which you enter them, from first to last. There is an implicit OR operator between filters. Evaluation stops when a filter in the list is matched. A filter match means that the ESRS IP Client was able to match both the expression and the time attribute of the filter to an incoming user request.

You can view and change the filter order from the Policy page for a device group. To learn how, refer to the online help for the Policy Manager application.

Notes about Filter Evaluation:

- A Time Window is not associated with any particular time zone. When evaluating the filter, the ESRS IP Client uses its system clock. For more details, refer to the topic “Evaluation of filters in different time zones” in the online help for the Policy Manager application.
- An implicit AND operator exists between the filter’s expression and time window. When an ESRS IP Client evaluates a filter, both the associated expression AND the Time Window must match before the filter is considered a match and the requested action is allowed. In other words, a filter is only a match if the attributes of

the incoming user (userId and enterpriseId) match the filter's expression AND the user is requesting the action within the Time Window associated with the filter.

- When a filter has no explicit expression or Time Window, the filter has no restrictions with regard to the user making the request or the time of the request. A filter with an empty expression matches all users and a filter with an empty time window matches at all times.

Creating, adding, and removing filters

The following sections explain how to do the following:

- Create new filters
- Add filters that have already been created
- Remove filters

Creating a new filter for a specific user

To create a new filter for a specific user:

1. Log in to the Policy Manager and navigate to the **Policy** tab (this is the home page by default).
2. Click **Assign Filter** next to the applicable policy.
3. Click **Create a new filter**.
4. Provide the following criteria as shown in Figure 124 on page 208:
   - Name (required field)
   - Description
   - Access Right (required field)
   - Expression
   - Time Window

Note: When you create an expression, you must use the correct case for variable names (for example, *userId*, not *UserID*). You must enclose the value for *userId* in double quotes (for example, "000000").

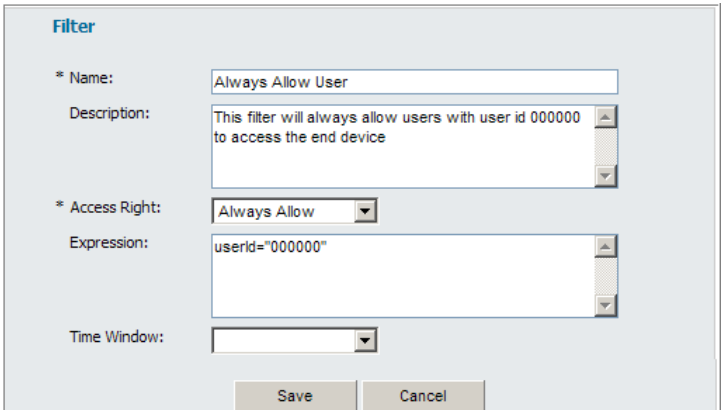


Figure 124 Entering the filter criteria

5. Click **Save**
6. In the **Selected Filters** list, verify the filter you created and its order in the list of filters. Then click **Save Changes** as shown in Figure 125 on page 208.

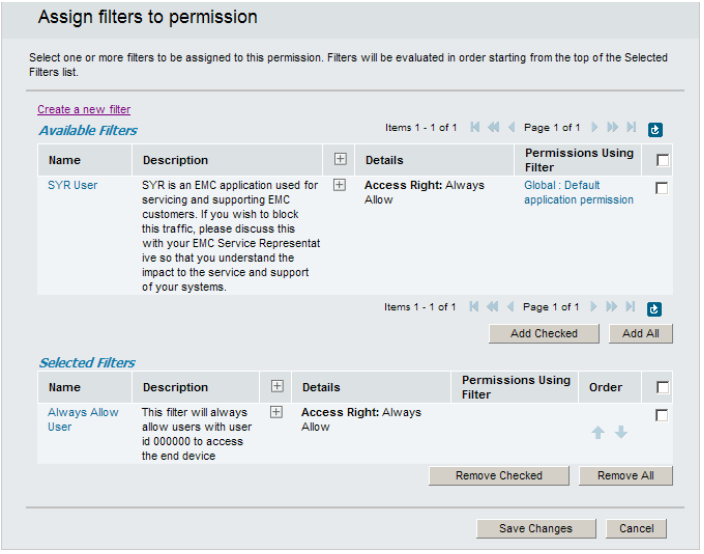


Figure 125 Verifying the created filter and saving changes

Defining a time window for a new filter

To restrict access to a certain period of time, define a time window for the filter. You can choose a fixed time period or one of two recurring time periods. For more information about the time window options, refer to the descriptions on page 204.

To define a time window for a new filter:

1. Begin creating a new filter as described in "Creating a new filter for a specific user" on page 207.
2. Select one of the following Time Window options as shown in Figure 126 on page 210:
   - **(Blank) -- This option specifies NO time period.**
   - **One Time**
   - **Weekly Recurrence**
   - **Weekly Range**
3. For all options except the **(Blank)** option, select the applicable day, date, and time options.

Note: The One Time option requires that you enter a Start Date and End Date. To change the date format from the default mm/dd/yy format to the dd/mm/yy format, click **Preferences** near the top right of your screen, and then modify **Date Format**.

If you choose the Weekly Recurrence option and want to select multiple days of the week, press **Ctrl** while clicking the days you want to select.

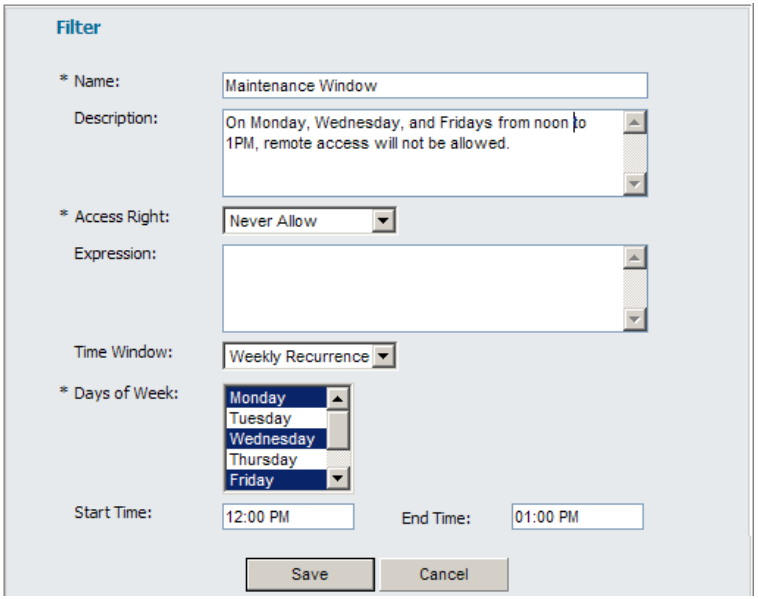


Figure 126 Selecting a time window

4. Click **Save**.
5. In the **Selected Filters** list, verify the Filter and Order, then click **Save Changes** as shown in Figure 127 on page 211.

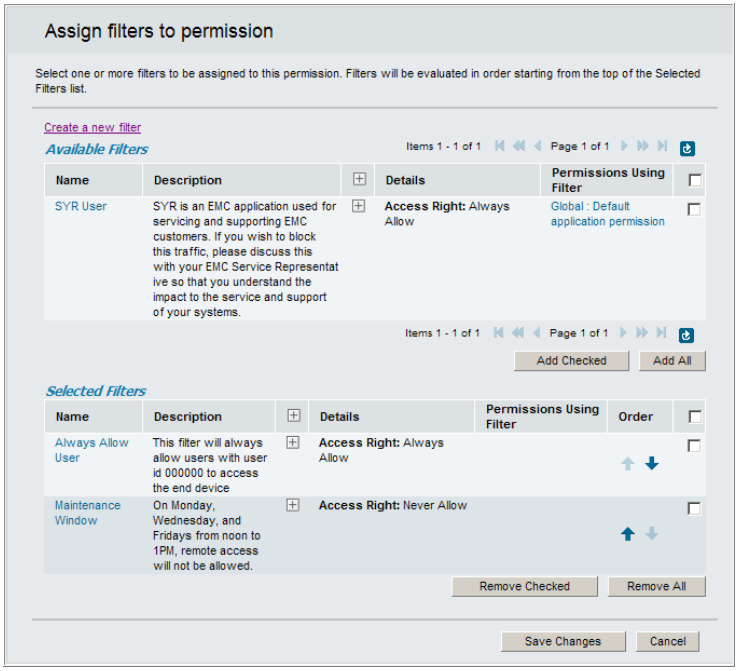


Figure 127 Verifying the created filter and saving changes

Adding an existing filter

To add an existing filter:

1. Log in to the Policy Manager and navigate to the **Policy** tab (this is the home page by default).
2. Click **Assign Filter** next to the applicable policy.
3. Select an existing filter from the **Available Filters** list by checking the appropriate checkbox.
4. Click **Add Checked** as shown in Figure 128 on page 212.

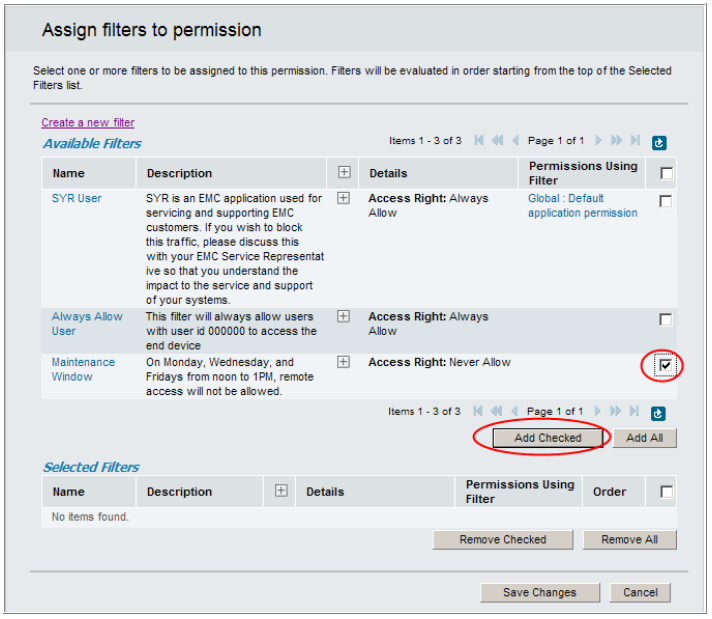


Figure 128 Adding an existing filter

5. Verify the added filter and filter order. Use the up and down arrows to change the order if necessary, and click **Save Changes** as shown in Figure 129 on page 213.

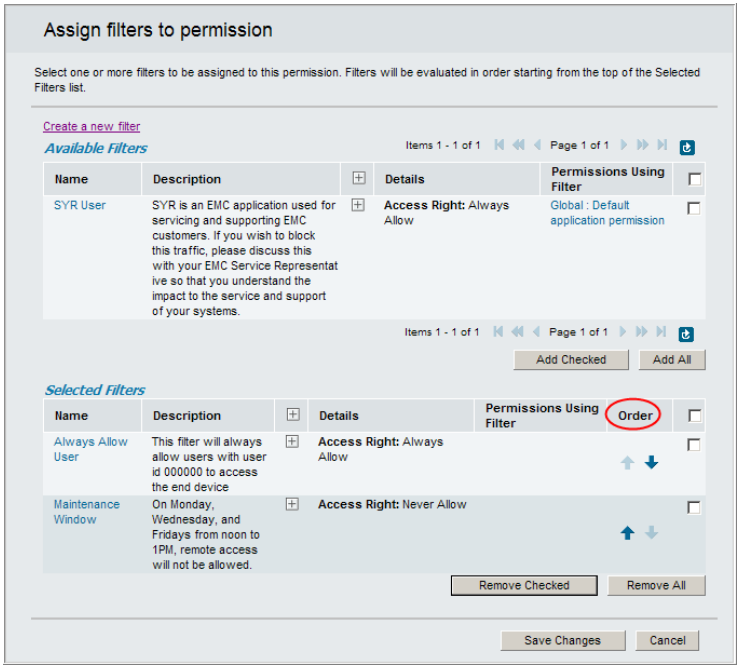


Figure 129 **Verifying the added filter and order and saving changes**

Adding an SYR filter at the device level

SYR is an EMC systems reporting mechanism used for problem resolution and proactive maintenance. It can automatically process system errors and alerts that systems send to EMC, and then apply proactive business rules processing to notify EMC support personnel.

SYR can also access devices remotely to perform diagnostics, download configuration data, health reports and other support-related data, and make software updates.

When Policy Manager is installed, an SYR filter is applied at the global and product levels. You have the option to add the SYR filter at the device level.

Follow these steps to add the SYR filter at the device level:

1. Log in to the Policy Manager and navigate to the **Policy** tab (this is the home page by default).
2. Click **Explore Device Groups**.
3. Click a device serial number. The policies for that device appear.

4. Locate the Remote Application policy and click **Assign Filter** for that policy. The **Assign filters to permission** window appears.
5. In the **Available Filters** list, select the existing **SYR User** filter and click **Add Checked** as shown in Figure 130 on page 214.

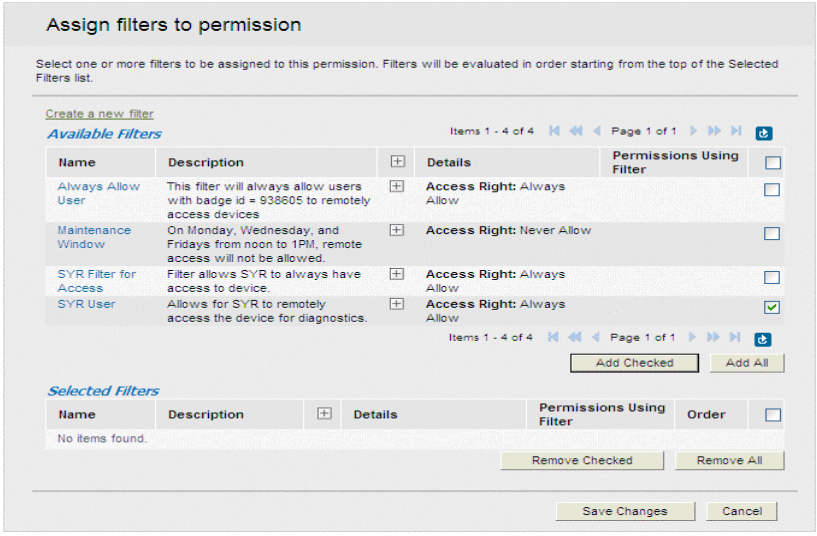


Figure 130 Selecting the SYR User filter

6. In the **Selected Filters** list, click **Save Changes** as shown in Figure 131 on page 215.

IMPORTANT

Do not modify the SYR filter for access, which is set to Always Allow. Changing this setting may negatively affect ESRS support.

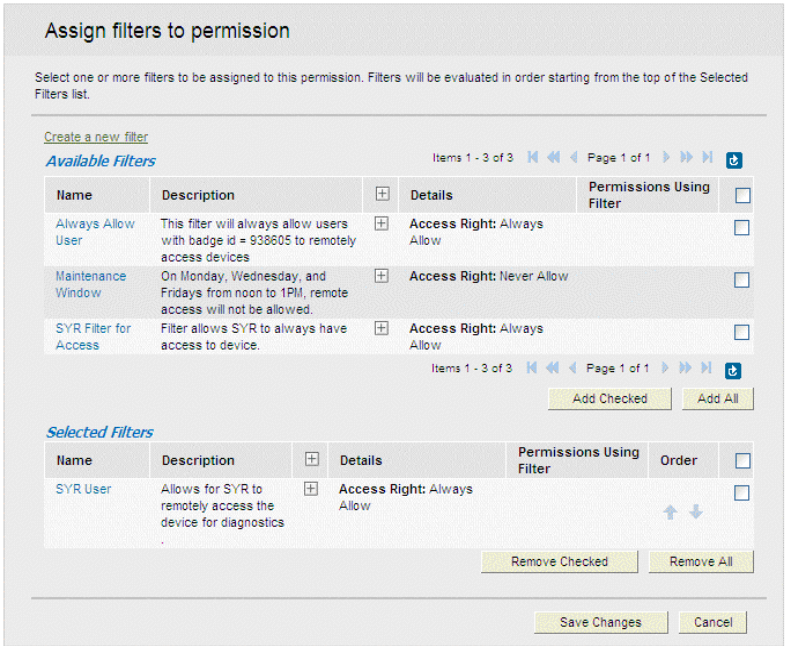


Figure 131 Saving changes

7. Check the Remote Application policy to verify the filter you have set, as shown in Figure 132 on page 215.

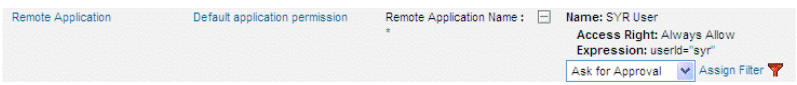


Figure 132 Verifying the SYR filter

Removing a filter

To remove a filter:

1. Log in to the Policy Manager and navigate to the **Policy** tab (this is the home page by default).
2. Click **Assign Filter** next to the applicable policy.
3. Select a filter to remove from the **Selected Filters** list by checking the appropriate checkbox.
4. Click **Remove Checked** as shown in Figure 133 on page 216. To remove all filters, click **Remove All**.

Figure 133 Removing a filter

5. Verify that the filter has been removed from the **Selected Filters** list and click **Save Changes** as shown in Figure 134 on page 216.

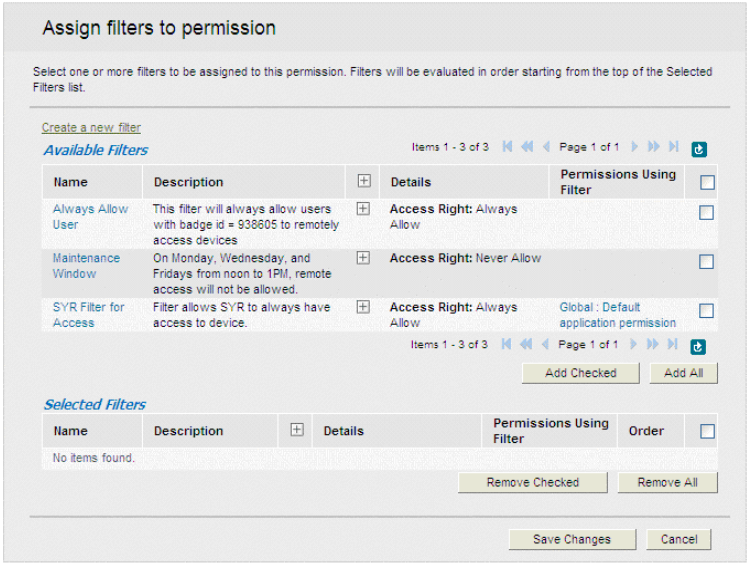


Figure 134 Verifying the removed filter and saving changes

Access right settings

This section describes parent/child permissions and settings.

Set access rights

Set (or reset) an access right by choosing from the list box menu provided for the particular permission, as shown in Figure 135 on page 217 for **Default package permission**.

Figure 135 Setting an access right

You can set all access rights for a group to a single value by using the checkbox **Set All Permissions** at the bottom left side of the page. For example, **Set All Permissions: Never Allow** can be used in emergencies to block all requests, as shown in Figure 136 on page 217.

Figure 136 Set All Permissions

At the far right of each (unlocked) permission line item is the **Lock** checkbox (Figure 137 on page 217) allowing you to lock that permission. Selecting this box prevents the corresponding access right in any child group from being changed.

Figure 137 Access right lock

If an access right is locked in a parent group, then for any child group this right appears as uneditable text (no list box menu) and cannot be reset. The first three access rights listed in Figure 138 on page 218 are locked by a parent group.

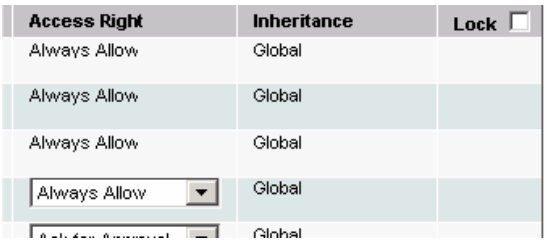


Figure 138 Locked and unlocked access rights

Lock permission for child

Lock

You can force the inheritance of a permission's access rights from a parent group or device to its child by *locking* the parent permission. Access rights that are locked in a parent's policy appear as plain text, rather than a list box, in the child's V**iew or change the policy settings** page.

To Lock Permission of Child — Navigate to the **View or change the policy settings** page under the **Configuration** tab. For each permission that you want to lock, select the **Lock** checkbox for the related permissions.

To Unlock a Permission — Navigate to the next parent (or higher) policy in which that permission is locked. If the parent permission has a selected **Lock** checkbox, clear it and click **Done**. If you do not find a checkbox on that permission at all, navigate to the next higher parent until you do, clear it and click **Done**.

Reset all permissions to match parent's values

Reset to Parent's Policy

You can force the policy of a child group or device to match that of its parent, by clicking the **Reset to Parent's Policy** button in the child's View or change the policy settings page.

Reset all permissions to a single value

Set All Permissions

You can force the access rights for all permissions in the current policy to the same setting. In the lower left corner of a View or change the policy settings page:

1. Choose the desired access right.
2. Select **Set All Permissions** for a selected group.
3. Click **Done.**

Reverse *Set All Permissions*

You can reverse the *Set All Permissions* action. This is useful if you want to prevent the ESRS IP Client from performing any actions for a period of time, for example, while the device is in maintenance mode or you are troubleshooting a problem. When the devices for that policy are ready to resume normal policy management:

1. Clear the **Set All Permissions** checkbox for that policy. The checkbox is shown in Figure 139 on page 219.
2. Click **Done**.

The Access Right column shows the previously defined access rights for all permissions in that policy.

Figure 139 Set All Permissions Access Rights

Pending requests

During operation, the Policy Manager runs without manual intervention until an Ask for Approval permission is activated. These activations are called *requests*.

About requests

If an Ask for Approval policy is in place, an ESRS IP Client-managed device sends a request to the ESRS IP Client for approval to perform a requested action. The ESRS IP Client then sends a message to the Policy Manager that it needs to get its approval and waits for the Policy Manager's response.

When the Policy Manager receives the request, it sends an e-mail notification, such as the message in Figure 149 on page 234, to the individual defined for that device's policy (or device group's policy), and then queues it for approval.

If the responsible individual does not accept the request within the period specified for that permission, the Policy Manager removes the action from the Pending Request queue and posts an entry to its audit log (see example message in Figure 142 on page 226). The device is sent a denied request due to time-out message. When a time-out occurs, a new request may be submitted.

Pending requests are shown in the Policy Manager's Pending Requests tab, View all pending single or container[1] requests for <*selected*> group. The tab displays a list of all pending requests for a group. You can accept or deny a single action request, or a container of pending action requests, or all actions shown.

1. A container is a grouping of requests containing multiple sub actions.

Accept/deny pending requests

This section provides details on how to accept or deny requests for the Ask for Approval setting. Figure 140 on page 222 shows the details for the following steps:

1. Click **Pending Requests.** The **View all pending single or container requests for <***selected***> group** page appears.

   You can view all requests pending for all groups, for a selected group, or for a selected device.

2. From the line item's list box menu at right, choose **Accept** or **Deny** for any number of selected actions, or all actions shown.

   You can also click the applicable button above the list box menu to **Set all to Accept, Set all to Deny, or Reset All**.

3. Click **Submit** to apply all changes made to this page.

The Policy Manager notifies the ESRS IP Client of all accepted or denied actions. The ESRS IP Client then performs the accepted actions.

View request details

View details, and accept or deny pending request

You can view more information for a single permission before accepting or denying it. You cannot view more information on a container, which can contain multiple permissions. Click the name of the permission from the Name column in the View Pending Requests page, as shown in Figure 140 on page 222.

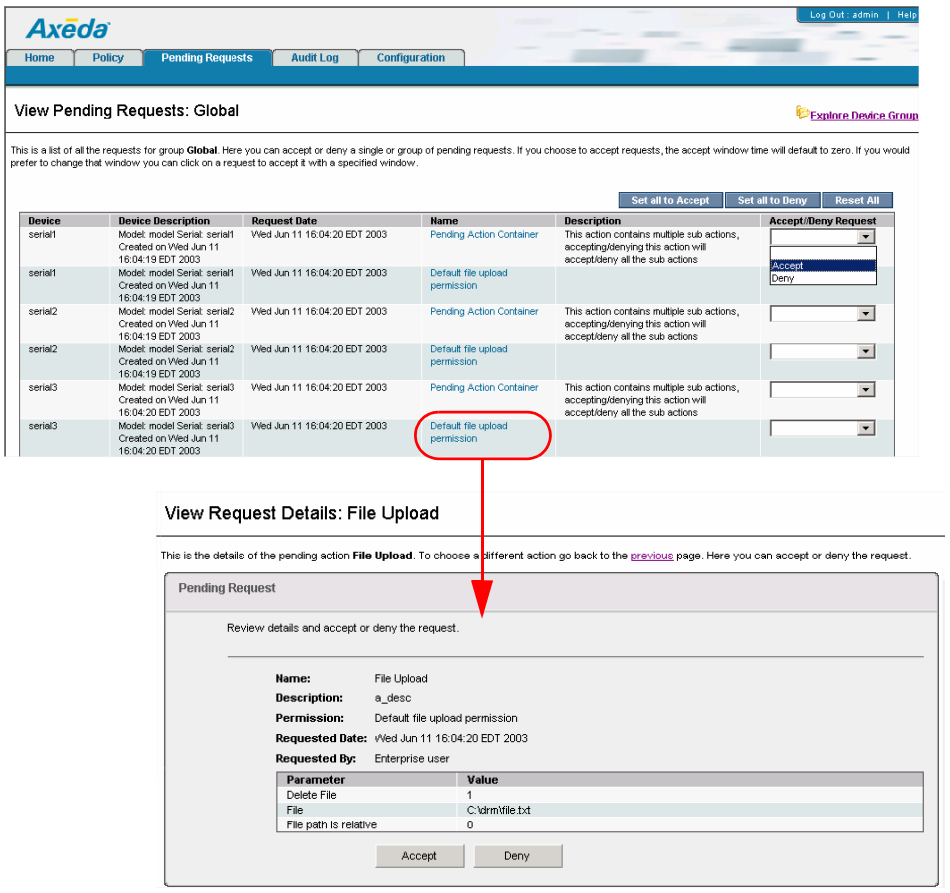


Figure 140 View Pending Requests and View Request Details

The View Request Details page appears showing further details about the action, including the time the action request was received by the ESRS IP Client. This detail page is shown in Figure 140 on page 222.

Pending time-out

When a request is made for a permission with an access right set to Ask for Approval, a response must be received within a configured period of time called the Pending Time-out setting. If the responsible individual does not accept the request within the time-out period specified for that permission, the request expires. The Pending Time-out setting is an action parameter (Permissions of the same action have the same Pending Time-out). As part of the action configuration, you can specify a length of time (minutes) for a permission request to be granted.

Note: Changing the setting at a device level is not recommended, because it changes the global policy setting for all devices and will impact EMC support of those devices.

To change the time-out setting:

1. Click **Policy**.
2. Click the name of the desired action. The **View or change details for <*name*> action** page appears.
3. Type the desired value into **Pending Time-out** field.
4. Click **Submit** to record new setting and return to settings page.

When a device sends a request to the Policy Manager, the user specified for the policy has a limited amount of time to permit the ESRS IP Client to perform the action. This amount of time is defined as the Pending Time-out period.

Note: If EMC is attempting a remote connection and you have your remote access settings set to Ask for Approval, but no one responds to the e-mail within the time-out period (5 minutes by default), the request is denied. This may prevent service on your devices from occurring within a reasonable time.

Audit log

The audit log displays the activity generated by the Policy Manager and the ESRS IP Client during a 365-day log rollover period. Through the Policy Manager you can view global log entries (up to 1000 lines) or only those entries for a selected group or a selected device.

About log messages

Logs contain user interaction activity records for the ESRS IP Client and Policy Manager.

The View audit log entries for device group: Global page shows audit log entries generated during the current rollover period. Logs from previous rollover periods (and logs larger than 1000 lines) are viewable within the file system, using a text editor such as Notepad.

Audit log entries are stored on the Policy Manager server. Each day a file is created. All the audit log messages generated by the Policy Manager for that day are saved to the file. By default, the daily files are created with the following syntax:

`APM_Audit_yyyy_mm_dd.txt`

where yyyy is the current four-digit year, mm is the current month, and dd is the current day.

Note: There are no limits on how large these files can grow or how many files are stored on disk. Be sure to keep track of disk use and space, and archive the files as needed.

Failure to maintain sufficient free disk space will result in Policy Manager failure and corruption of the Policy Manager database. This may result in the need for an uninstallation and reinstallation of the Policy Manager application.

Audit log

To view the audit log, click the **Audit Log** tab. The View audit log entries for device group: Global page appears, as shown in Figure 141 on page 225.

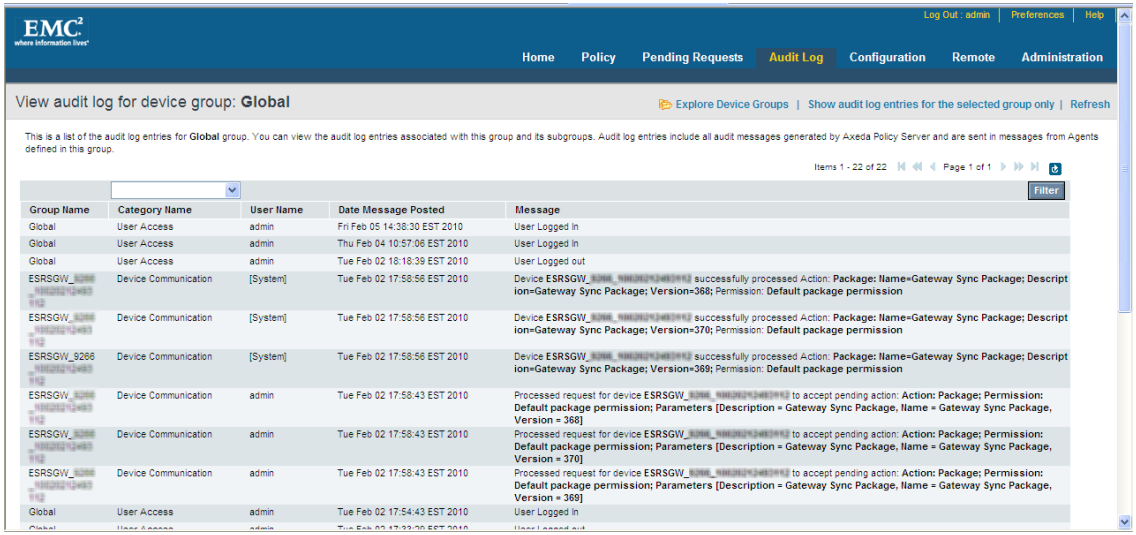


Figure 141 Audit log (Global)

Recorded parameters

Audit logs record the following types of parameters for log display:

- **Group Name**: The relevant policy level
- **Category Name**: The name of the audit message category. Categories include:
  - User Access
  - Device Communication
  - Remote Access
  - Administration
  - Configuration
- **User name**:
  - The remote user prompting policy response
  - The local user modifying policy
  - The device processing an action
- **Date Message Posted**: Time stamp
- **Message**: Description of policy management action performed:
  - Type of action taken (nonbold text)

- Parameters of action (bold text)

Message examples are shown in Figure 142 on page 226.

Figure 142 Audit log message example

Specifying the audit log scope

To see audit logs for only certain groups, you can select logs for:

- Any group
- Group (only) *-or-* group + all child groups

Note: Callhome activities are only shown on the Gateway instance of the Policy Manager.

Activity of one device type

To see a log—for example—of Symmetrix-related activity, you look at Symmetrix-level activity as well as the activity for specific devices:

1. From any Audit Log view, click **Explore Device Groups**.

   You see the group hierarchy.

2. Click **Symmetrix**.

   This takes you to an audit log view, but now only entries for groups named Symmetrix and groups with Symmetrix serial numbers are shown. See the upper left of the two screens in Figure 143 on page 227.

3. From the Audit Log: Symmetrix view, click **Show audit log entries for the selected group only**.

   You see that the Group Name column on the left now shows only Symmetrix entries. The link you selected has toggled to **Show all audit log entries for the selected group and subgroups**. (Click that link if you want to return to the all-Symmetrix view.) See the lower right of two screens in Figure 143 on page 227.

Specific device-only activity

To see a log of only specific device activity, follow these steps to return to the group hierarchy:

1. From any Audit Log view, click **Explore Device Groups**.
2. Click any serial number.

Note: If you leave the audit log to select another tab, such as Policy or Configuration, and you later return to the Audit Log tab, you will see the previous log view.

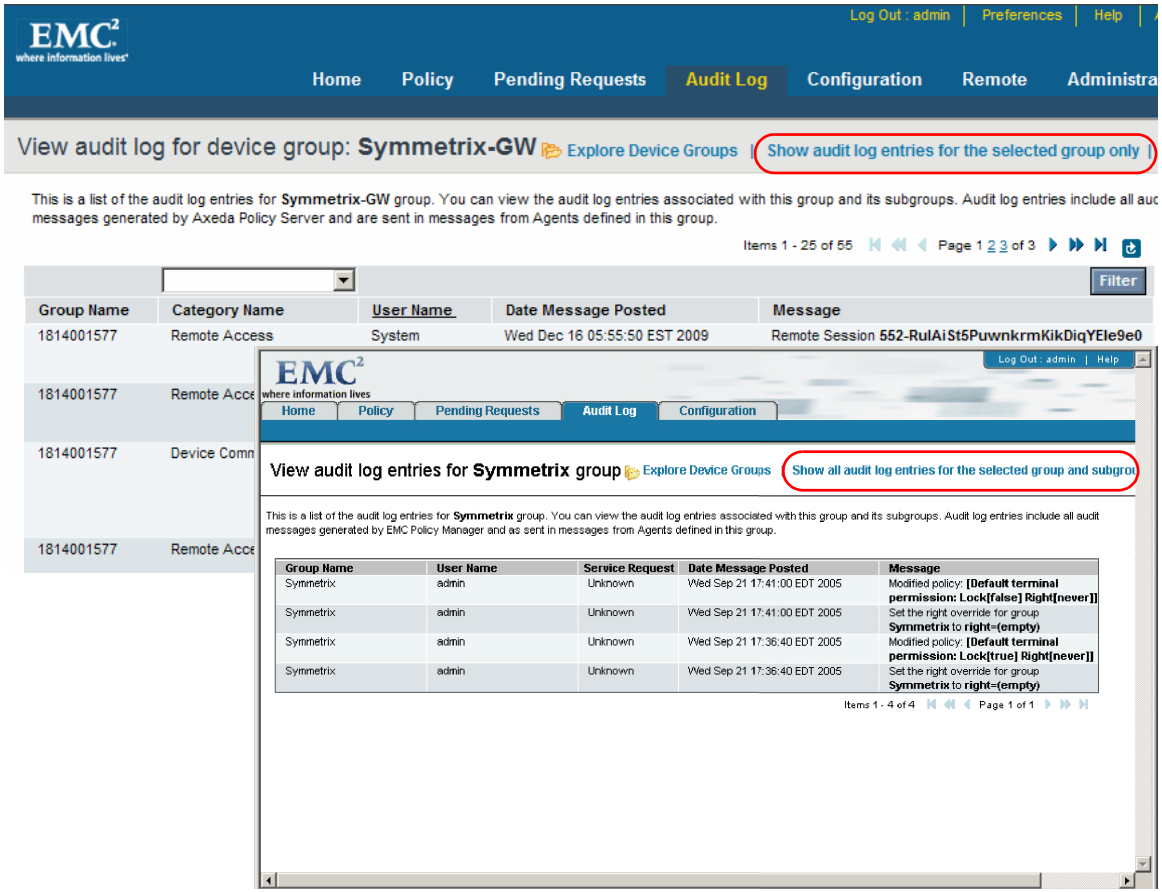


Figure 143 Symmetrix group audit logs

Audit log recording

All Policy Manager activities, and some ESRS IP Client activities, are recorded in the audit log.

Policy Manager

All Policy Manager activity is recorded in the audit log.

ESRS IP Client

The following ESRS IP Client activities are recorded in the audit log:

- ESRS IP Client registers with the Policy Manager.
- ESRS IP Client sends a request to perform an action with a permission access right of for example.
- ESRS IP Client performs an action defined for a permission access right of **Always**. The message sent to the Policy Manager audit log includes the name of the user who performed the action, the action performed, and the success or failure of executing the action.
- ESRS IP Client denies an action defined for a permission access right of Never Allow. The message sent to the Policy Manager audit log includes username of the person who attempted the action, information about the rejected action (specific to the type of action), and the policy permission that caused the action to be rejected.
- ESRS IP Client sends a Remote Session Disconnect message.

Audit log configuration

For information on configuring the audit log, see "Configuring the audit log" on page 229.

Configuration

Policy Manager provides a number of options for configuring policy information. These options include:

- Viewing device group configurations
- Configuring the audit log
- Viewing missing devices
- Configuring e-mail notifications

Viewing device groups

Clicking the Configuration tab in Policy Manager displays the Select a device group to view its configuration page as shown in Figure 144 on page 229.

The page displays a list of all of the device groups currently defined in Policy Manager.

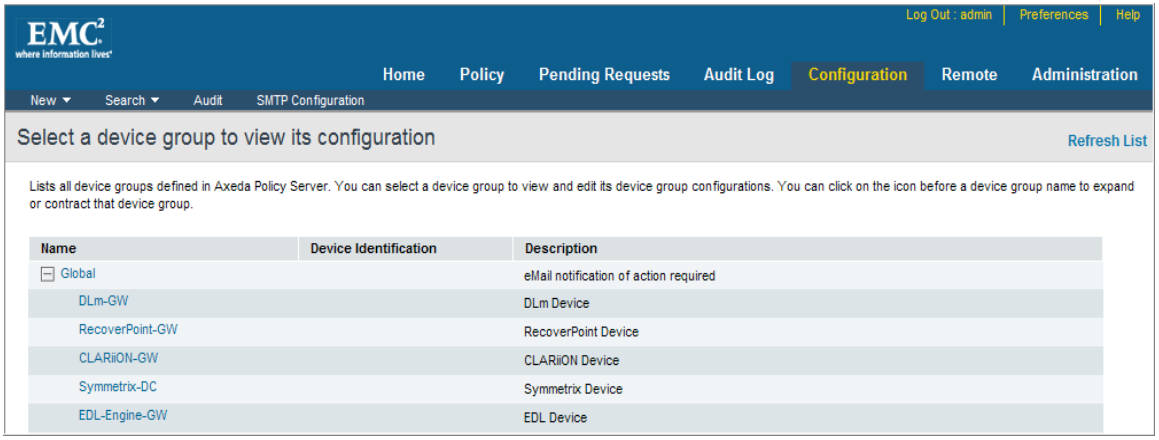


Figure 144 Configuration tab—Select a device group

Configuring the audit log

The Configure Audit Category screen enables you to select which audit categories are displayed in the audit log. You can also specify the number of days that log files are saved on the server before they are automatically deleted. The available audit categories are:

- Administration
- Remote Access

- Device Communication
- Configuration
- User Access

To select categories to display in the audit log, and to specify the number of days to maintain log files:

1. Click **Audit** from the Configuration tab. The Configure Audit Category appears as shown in Figure 145 on page 230.
2. Specify a number of days in **Delete audit log after _days**.
3. Click a checkbox next to **Category Name** to enable or disable audit logs for that category.
4. Click **Done** to save your changes
5. When prompted with Update this configuration?, click **OK** to commit your changes or **Cancel** to discard them.

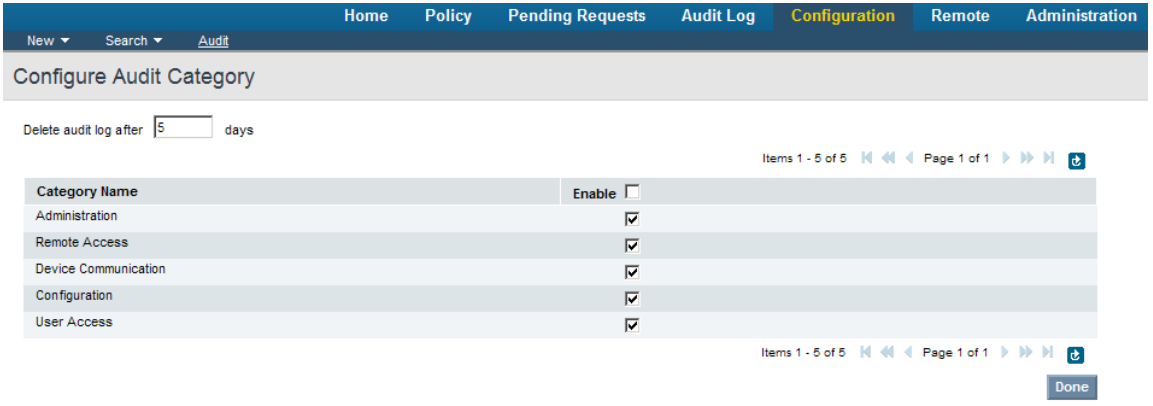


Figure 145 Configure audit category

Viewing missing devices

If a device is offline or not connected to the ESRS IP Client, it may be enforcing an outdated policy. This could mean that the device is allowing actions that should be set to Never Allow or Ask for Permission, or denying actions that it should be allowing.

To determine if a device is offline to the ESRS IP Client, click **Search** from the Configuration tab, then click **Missing Devices**. The **View and remove missing devices page** appears as shown in Figure 146 on page 231. Any devices shown in this page have missed their last contact (ping) with the Gateway and are now considered offline.

Figure 146 Configuration: View and remove missing devices

Before you request that a device be removed from the Policy Manager, make sure that you know the true status of the device:

- Any devices for which you request removal must be undeployed by EMC Global Services.
- If you accidentally request the removal of a device still in production, it will reregister when placed back online.
- Any devices on the missing list that have an unknown status must be investigated. Contact EMC Global Services for assistance.

E-mail notifications

When an EMC Global Services professional requests a remote support session, if an access right is set to Ask for Approval, the ESRS IP Client sends an action request to the Policy Manager for approval. The Policy Manager then sends an e-mail notification to the individuals, group aliases, or roles specified in the notification configuration.

Configuring e-mail notifications

Notifications are specified for each device group, and can also be specified for individual devices. Each notification specified for a group is sent with a message based on that group's standard form.

The Global group notification message template is configured during installation.

Note: If you make no changes to any notification settings, all e-mail is delivered with the same message form. To add an e-mail address, edit the notification form as described in the following procedure.

To modify the notification format for a group (and its children) or for an individual device:

1. Click **Configuration** (from any Policy Manager page).

   A group hierarchy appears, similar to that shown in Figure 147 on page 232.

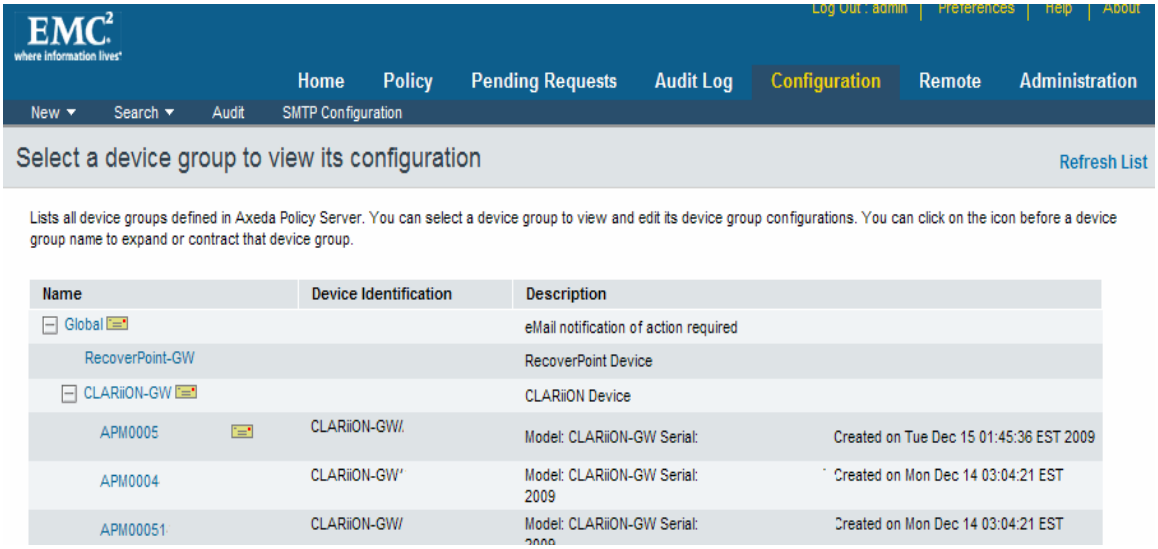


Figure 147 Configuration tab

Notice that the Global group has an envelope icon associated with it, as does a CLARiiON group and an individual CLARiiON device within the CLARiiON group. The envelope icons are colored *yellow*, indicating that the original contents of the notification form have been overwritten. In the case of the Global group, the form was originally blank and then filled in with the default notification message and recipient during the Policy Manager installation.

In the case of the groups and individual devices that are beneath the Global group in the hierarchy, they inherit the contents of their parent group. In Figure 147 on page 232, the CLARiiON group and one of its individual devices show a yellow envelope icon because the original contents of their notification forms have been overwritten.

2. From the hierarchy, click the name of a device group or individual device.

The notification form opens for editing. The form might display blank fields—if so, you may have to copy contents from the global notification if you want to use the same addresses, subject, and body text. The notification fields and settings for the Global group are shown in Figure 148 on page 233. The full default Body is shown in Figure 149 on page 234.

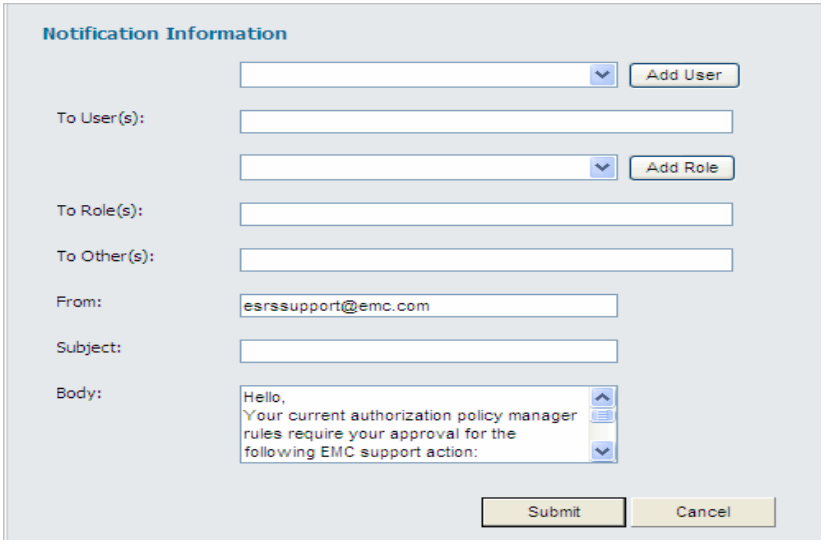


Figure 148 Global group notification settings

```
Hello,
Your current authorization policy manager rules require your approval for
the following EMC support action:
 Date: <$TMST>
 Action: <$ACTN>
 Description: <$ACTD>
 Device Model:<$A_MN>
 Device Serial Number:<$A_SN>
 EMC Username:<$USRN>

Please click the URL link listed below to approve or deny this request.
http://000.000.000.000:8090/actions/request/show_requests

This email was automatically generated by the EMC Secure Remote Support
Policy Manager in  response to the following permission settings:
 Model : <$A_MN>
 Permission Name: <$PR_N>
 Permission Description: <$PR_D>
 Permission Detail Setting : <$PRDT>

Please note that details of the action request can be viewed in the Policy
Manager Audit Log web  pages. Please use your browser to log into the
Policy Manager server to approve or deny this request.

Thank You,
EMC Customer Service
```

Link to access authorization page

Figure 149 Default notification e-mail body

3. Fill in the notification information, then click **Submit** to save your settings and return to the group hierarchy window. The following table describes each field in the Notification Information section of the Configuration window.

To User(s)	Select one or more users from the drop-down list.
To Role(s)	Select one or more roles from the drop-down list.
To Other(s)	Enter an e-mail address or multiple e-mail addresses separated by commas.

From	Enter an e-mail address. **Note:** The From address may need to be a registered user of your e-mail server for the notification feature to operate correctly.
Subject	Enter any text. You may include any substitution parameters identified in Table 9 on page 235.
Body	Enter any text. You may include any substitution parameters identified in Table 9 on page 235, or a link to server.

Default notification form

Table 9 Substitution parameters for notifications

Tag	Description
<$A_MN>	Gateway server model number
<$A_SN>	Gateway server serial number
<$A_GN>	Gateway server associated group name
<$A_GD>	Gateway server associated group description
<$ACTN>	Action name
<$ACTD>	Action description
<$PR_N>	Permission name
<$PR_D>	Permission description
<$PRDT>	Permission details (parameter names and values)
<$SMSG>	SOAP message
<$TMST>	Timestamp when action was forwarded from Client
<$USRN>	Username

During Policy Manager installation, a default notification Body field for the Global group is created, as shown in Figure 149 on page 234. This field contains a line with the web address of the Policy Manager access authorization page. Several substitution parameters, shown in Table 9 on page 235, are also used.

When a request is sent using the embedded web address, the policy administrator receiving the e-mail has direct access to the Policy Manager interface to approve or deny the request.

Remote sessions

You can use the Remote (Sessions) window of Policy Manager to view the status of all remote sessions for devices managed by Policy Manager. This window also enables you to end remote sessions.

To use these features of Policy Manager, you need View and End privileges to the Remote (Sessions) tab. When you select the Remote tab in the application, the View and end remote sessions window appears, as shown in Figure 150 on page 236.

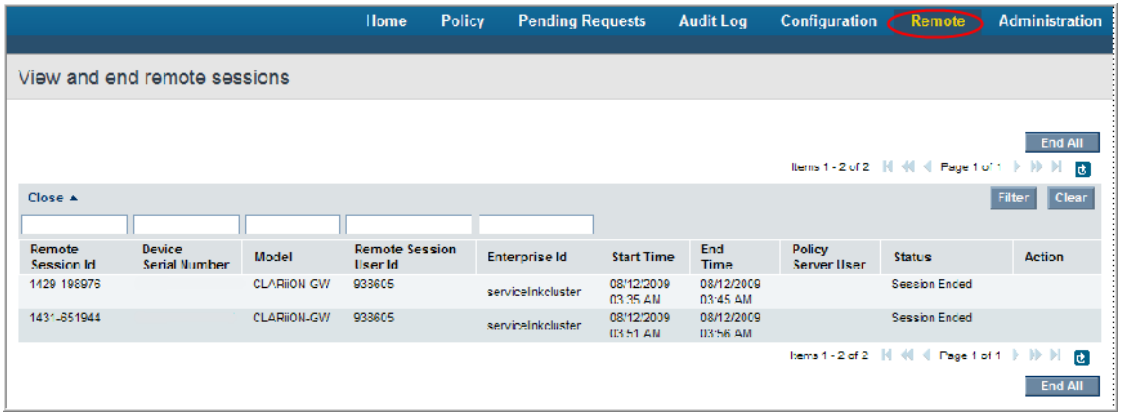


Figure 150 View and end remote sessions window

To access the View and end remote sessions window, use its search facility, and end remote sessions, you must be logged in as a user with role privileges to the Remote (Sessions) component. If you cannot see the Remote tab in the application, you do not have privileges to the component. Contact your Policy Manager administrator if you require access to the component.

You can search for and view the following types of remote sessions from the View and end remote sessions window:

- Currently pending (waiting for approval from Policy Manager)
- Active
- Inactive
- Ended

The Policy Manager displays sessions for the number of hours configured in the Policy Manager configuration file. For example, if

the setting is 24 hours, this page displays remote sessions for the previous 24-hour period.

Remote tab

The information for remote sessions is displayed in a table that is accessed from the Remote tab, as shown in Figure 150 on page 236. The table may take up multiple pages. You can sort the table by clicking the column heading for any of the table columns. The table provides a filter option. For more information, see "Filter feature" on page 238.

This table in the Remote tab displays the following information for each remote session:

- **Remote Session ID** — The identifier assigned to the remote session by the Enterprise server that established the session. For example, ASD-456-908 or BBD-231-008.
- **Device Serial Number/Model** — The model and serial identifiers for the device as they exist in the Policy Manager database. The device must be registered with Policy Manager and its ESRS IP Client must be actively contacting Policy Manager concerning remote sessions to appear in this table. If you also have privileges to the Policy component (View and Add/Edit), the Device Serial Number and Model entries in the table are shown as links. To view the policy for the device group to which the device model belongs, click the link in the Model column; to view the policy for the device group to which the device serial number belongs, click the link in the Device Serial Number column.
- **Remote Session User Id** — The login name of the user who established the remote session through the Enterprise server. For example, Jane Doe.
- **Remote Session Enterprise Id** — The host URL for the Enterprise server that established the remote session. For example, CGEnterprise.acme.com.
- **Start Time** — The date and time that the ESRS IP Client connected to the remote session.
- **End Time** — If applicable, the date and time that the ESRS IP Client disconnected the remote session. If a user ended the remote session from this page (by clicking End in the Action column), then this field is updated once the ESRS IP Client running on the device notifies Policy Manager that the End action was carried out.

- **Policy Manager User** — If applicable, the login name of the Policy Manager user who ended the session.
- **Status** — The current status of the remote session. Possible entries in this column include:
  - Pending approval
  - Session started
  - Session ended
  - Waiting to end session
  - Session denied
  - Missing device.

  Note: The Status field cannot be updated when an ESRS IP Client is missing from Policy Manager. Policy Manager will change the status to Missing device when the ESRS IP Client misses three contacts (pings). For example, if the ESRS IP Client is configured to contact Policy Manager for new policies every 30 minutes, and if the ESRS IP Client misses three of those contacts in a row, Policy Manager changes the status to Missing device.

- **Action** — For a remote session in progress, this column displays the End link. You must have the End privilege to see this link. For more information about ending remote sessions, refer to "Terminating a remote session" on page 239.

Filter feature

You can filter the list of remote sessions displayed based on the Remote Session ID, Device Model and Serial identifiers, the Remote Session user, and the Remote Session Enterprise server ID.

To filter the table information, use the filters at the top of the following columns:

- **Remote Session Id** — Type a specific session identifier (Id) that you want to find or use the wildcard character (*) to find all sessions that have similar identifiers. For example, type ASD* to find all remote sessions where the ID begins with ASD.
- **Device Serial Number and Model** — To view remote sessions for a particular Model, type the model name or number in the filter box above the Model column. To narrow the list to a specific device, type the serial number of the device in the box above the Device Serial Number column.

- **Remote Session User Id / Remote Session Enterprise Id** — Type the User Id and the Enterprise Id to display only those remote sessions started by the user you specify from the Enterprise server you specify. For example, type Sarah in the User Id box and remote.acme.com in the Enterprise Id box to find all sessions started by user Sarah from the Enterprise server for which the hostname is remote and the domain is acme.com.

After you specify your filter criteria, click the Filter button. When the table refreshes, only those remote sessions that match your filter criteria are displayed in the table.

If you want to filter the table by different criteria, click Clear to remove the current entries in the filter boxes. Then specify new information in the boxes and click Filter again.

To sort the information, click any of the column headings. To reverse the sort order, click the column heading a second time.

Terminating a remote session

To terminate a remote session, follow these steps:

1. Log in to the Policy Manager using an account with View/Edit privileges.
2. Click **Remote**.
3. Search for the session to terminate, using:
   - Remote session ID
   - Device serial number
   - Model
   - Remote session User Id
   - Enterprise Id
4. End the session as follows:
   a. To end a session that displays a Session Started status, click **End** in the **Action** column as shown in Figure 151 on page 240.
   b. To end all active remote sessions, click **End All**.

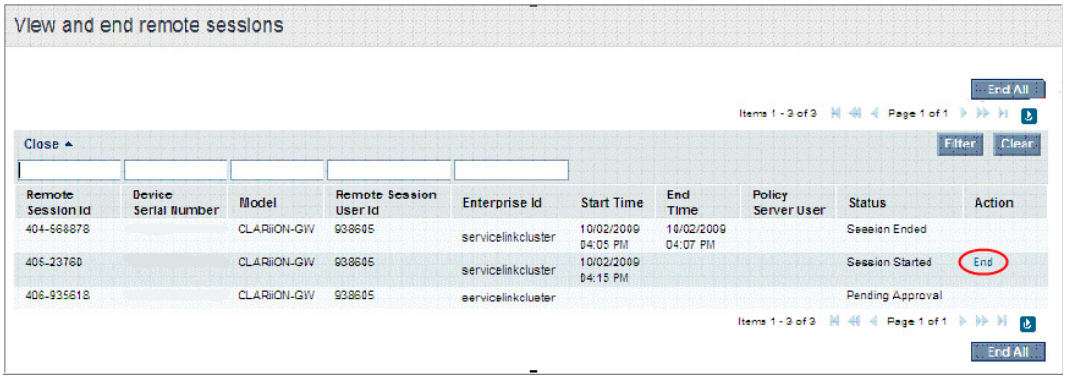


Figure 151 **Terminating a remote session**

5. Read the caution message that appears, as shown in Figure 152 on page 240. If you are sure that you want to terminate the remote session, click **OK**.

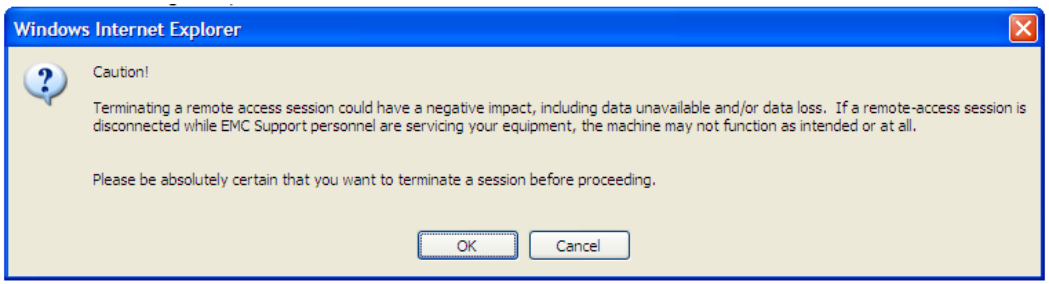


Figure 152 **Caution message**

6. If you clicked **OK** in the caution message window, the status of the remote session changes to **Session Ended**.

Note: The action of terminating a session is recorded in the audit logs of the Policy Manager and the EMC enterprise.

PART 4

Maintenance

This section describes required and recommended customer site operations for the ESRS IP Solution.

Chapter 7, "Server Maintenance"

ESRS IP Client and Policy Manager server backup and other maintenance setup procedures are described here.

7

Server Maintenance

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

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

Topics in this section include:

Power sequences

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

IMPORTANT

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

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

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

IMPORTANT

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

Time Zone settings

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

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

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

Service preparation for Gateway Client and Policy Manager

This section describes steps that need to be taken prior to performing maintenance procedures on the Gateway Client and Policy Manager servers.

Gateway Client server

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

Logging preparation

Overwrite Events turned on

To prevent the Event Viewer log from locking and failing to record:

- Starting/stopping services
- Logging in
- Installing/uninstalling applications

in the Windows Event Viewer, set the Event Viewer log to overwrite as needed, for both system logs and security logs, as shown in Figure 153 on page 247:

1. Select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Event Viewer**.
2. Right-click **System Log** and then select **Properties**.
3. Select option **Overwrite events as needed**, and click **OK** under the tab **General**.
4. Repeat step 2 and step 3 to set properties for **Security Logs**.

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

CAUTION

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

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

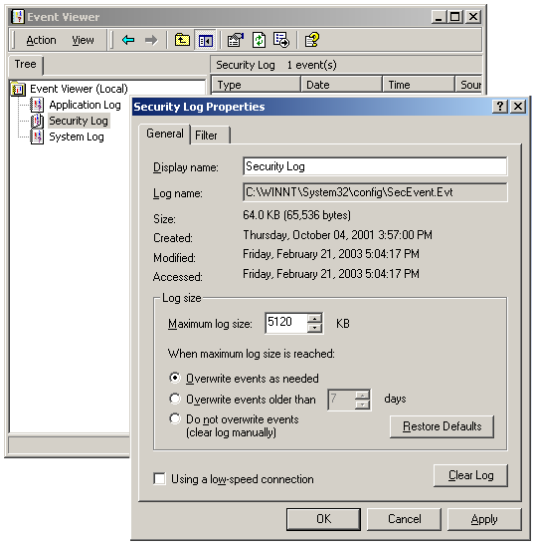


Figure 153 Event Viewer System and Security Log settings

Policy Manager server

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

Backup preparation

Windows Task Scheduler turned on

For automated daily backups of the Policy Manager database to occur, the Windows Task Scheduler must be running and unrestricted, allowing new tasks to be added.

Your company's IT security policies determine if this has been set up on your server at the time the Policy Manager was installed by EMC.

Disk space for log files

Your Policy Manager server should be set up with a minimum of 2GB available disk space. Monitor your log file usage and plan your archiving policy accordingly.

CAUTION

If the system runs out of disk space for log files, the Policy Manager database will be corrupted and will require reinstallation.

To maintain flat audit logs and conserve disk space, compress audit logs and copy them to a repository. Audit logs typically compress by greater than 85%.

Policy Manager database management

The Policy Manager database is located at:

```
[install drive]:\EMC\ESRS\Policy Manager\hsqldb
```

Figure 154 on page 248 shows an example of a database location.

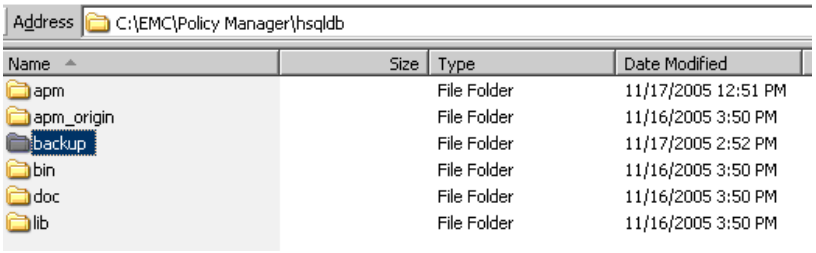


Figure 154 Policy Manager database location

It is configured to run as in-process (or in standalone) mode.

For example, in a default installation the database is located in the following directory:

```
C:\EMC\ESRS\Policy Manager\hsqldb\apm
```

Component files

The data for each database consists of five files in the same directory, apm. The file extensions are *.properties, *.script, *.data, *.backup, and *.log. All these files are essential and thus should never be deleted or allowed to become corrupted.

These files are identified in Table 10 on page 248.

Table 10 Policy Manager database files

File	Description
apm.backup	Zipped backup of the last known consistent state of the data file
apm.data	Data for cached tables
apm.log	Recent changes within the database
apm.properties	General settings for the database
apm.scripts	Definition of tables and other database objects, plus data for noncached tables

Mode

The default mode for the hsqldb is the In_Process mode (Standalone Mode).

Backup and restore scripts

The component files of the database are backed up together. The following scripts are contained in hsqldb\lib:

- apmbackup.vbs
- apmrestore.vbs

The scripts are described in Table 11 on page 249.

Table 11 Backup/Restore scripts

File	Description
apmbackup.vbs	This script backs up the [*install_drive*]:\EMC\Policy Manager\ESRS\hsqldb\apm folder. This must be installed in [*install_drive*]:\EMC\ESRS\Policy Manager\hsqldb\lib. If backup was selected during installation, the script runs daily at 3:00 a.m., copying the apm folder to [*install_drive*]:\EMC\ESRS\Policy Manager\hsqldb\backup. It maintains 31 days history of the apm database.
apmrestore.vbs	Simple GUI script to help restore the desired backup image to [*install_drive*]:\EMC\Policy Manager\hsqldb\apm. This script must be installed in [*install_drive*]:\EMC\ESRS\Policy Manager\hsqldb\lib. You must stop the Policy Manager service before you do a database restore. The original[install drive]:\EMC\ESRS\Policy Manager\hsqldb\apm is moved to [*install_drive*]:\EMC\ESRS\Policy Manager\hsqldb\apm_dateoftherestore

A view of the hsqldb\lib directory is shown in Figure 155 on page 250.

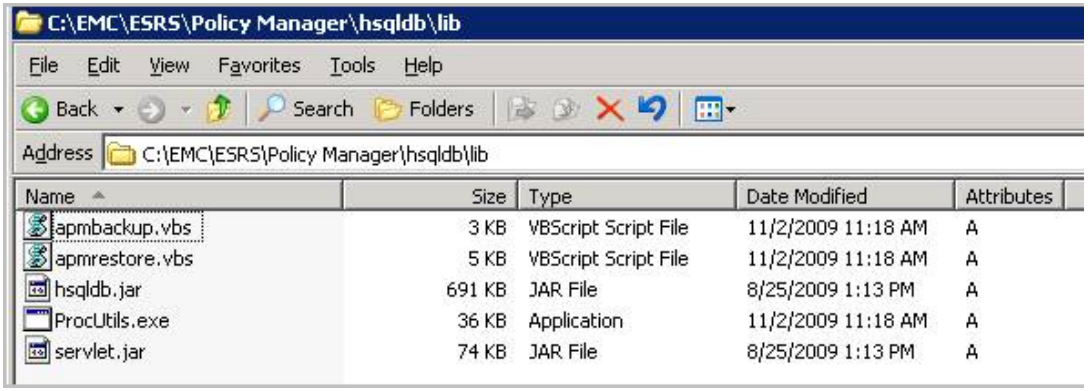


Figure 155 Location of Policy Manager scripts

Numbered directories and an index are accumulated in the backup directory. The directory numbering starts at 0 the day after The ESRS IP Gateway is installed. An example is shown in Figure 156 on page 250. After 31 backups have occurred (0-30), the directories are reused and the previous backup in each directory is overwritten.

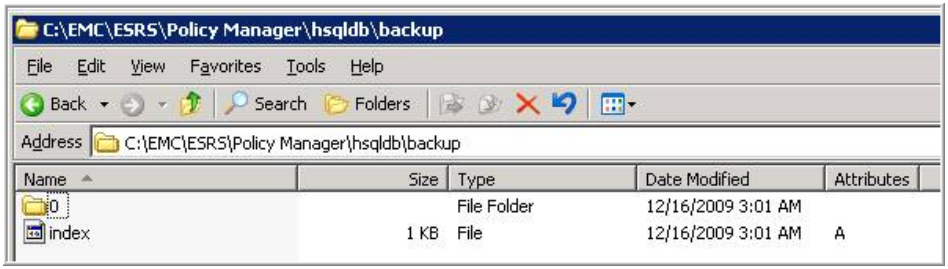


Figure 156 Policy Manager backup directory

Enabling logging to an external Syslog server

To enable Syslog integration (logging to an external Syslog server), you must modify the following files that are shipped with the Policy Manager installer:

- `Custom.properties`
- `log4j.properties`

Note: After you modify the files, you must restart the Policy Manager services.

The following section explains how to modify the files to enable logging to an external Syslog server.

Modifying the Custom.properties file

To modify the Custom.properties file:

1. Navigate to the following folder:

```
[install drive]:\EMC\ESRS\Policy Manager\Tomcat5\common\classes
```

2. Copy the Custom.properties file to another location before editing. Do not add any additional spaces or punctuation.
3. Open Custom.properties.
4. In the following line within Custom.properties, change **false** to **true**:

```
com.axeda.apm.server.enable-syuslog-audit=false
```

5. Save the file Custom.properties.

Modifying the log4j.properties file

To modify the log4j.properties file, do the following:

1. Navigate to the following folder:

```
[install drive]:\EMC\ESRS\Policy Manager\Tomcat5\common\classes
```

2. Copy the log4j.properties file to another location before editing. Do not add any additional spaces or punctuation.
3. Open log4j.properties. The file contains a configuration block that is specific to the Syslog configuration.

4. Uncomment specific lines in the configuration block, as directed in the example shown in Figure 157 on page 252.

```
## ############################################################
## Define an appender called "SYSLOG", which outputs log messages to a
## Unix-style Syslog server.
##
## log4j.appender.SYSLOG.SyslogHost=hostname_or_IP_address[:port_number_if_not_514]
##
## Uncomment settings below to activate capability for logging audit messages to a Syslog
Server.
#

## Uncomment the following line to enable Audit messages to be output to the SYSLOG
# log4j.logger.com.axeda.esrs=INFO, SYSLOG

## Uncomment the following lines, and edit per your specific Syslog instance
# log4j.appender.SYSLOG=org.apache.log4j.net.SyslogAppender
# log4j.appender.SYSLOG.layout=org.apache.log4j.PatternLayout
# log4j.appender.SYSLOG.layout.ConversionPattern=%d{ISO8601}: %m%n
# log4j.appender.SYSLOG.SyslogHost=localhost
# log4j.appender.SYSLOG.Facility=LOCAL0
# log4j.appender.SYSLOG.FacilityPrinting=false
```

Figure 157 Policy Manager syslog example

5. Edit the parameters within the lines you uncommented, based on your specific Syslog requirements. You must configure the following parameters within the block:
   - **Sysloghost**: Replace localhost with the hostname or IP address where the syslog server will be listening.
   - **Facility**: Replace LOCAL0 with the facility or log level of the messages that will be posted to the Syslog server.
6. Save the log4j.properties file.

Note: You can customize the log4j.properties file using an external script, or you can replace the file with another copy of log4j.properties.

IMPORTANT

You must restart the Policy Manager services after modifying the Custom.properties and log4j.properties files.

Backup guidelines and procedures

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

Specific procedures depend on your:

- ESRS IP site architecture
- Backup software
- Existing procedures

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

Backup

1. **Gateway Client or Policy Manager server image** — See "Server image backup" on page 253 for recommended Gateway and Policy Manager server backup guidelines.
2. **Policy Manager database** — See "Policy Manager database automated backup" on page 254 for the recommended Policy Manager database backup procedure.

Restoration

3. **Gateway Client or Policy Manager server** — See "Restoration procedures" on page 256 for recommended guidelines on restoring your server from image backup and, if applicable, the Policy Manager database.

Server image backup

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

Initial setup

At installation time:

For each Gateway Client and Policy Manager server:

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

Additionally, for each Policy Manager server:

Set up the Policy Manager database for daily (or other periodic) automated database backup: If your EMC Global Services professional has not done so already, perform the procedure outlined in "Policy Manager database automated backup" on page 254.

Note that the Policy Manager database includes Audit Log files as well as configuration settings.

Regular maintenance

For the Policy Manager server:

Database backup should occur automatically if automation has been set up, described in "Policy Manager database automated backup" on page 254.

Optionally, for each Gateway and Policy Manager server:

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

Policy Manager database automated backup

An automated backup of your Policy Manager database may already be activated, based on your discussions with your EMC Global Services professional.

Whether or not the automated backup is currently activated, you may examine and possibly customize the script provided with your Policy Manager, and then activate it with the Windows Task Scheduler.

To configure and activate your backup tasks:

1. Check whether there is a backup task already scheduled by first, in Windows, opening **Start** > **Settings** > **Control Panel** > **Scheduled Tasks**:
   a. If the automated backup has been activated by your EMC Global Services professional, you find the scheduled task **apmbackup** listed. In this case your backup has been configured and activated—you are done.
   b. However, if you are unsure of the location of the backup path, or if you want to change that path, you can also perform step 2 and then exit.
   c. If there is no existing backup task, you first edit the backup script to specify the backup path, and then schedule the backup task—continue with the next step.

2. Edit the backup script:

Note: Unless you edit the script file to provide a pathname, the backup is created in the root directory of the Policy Manager application.

   a. Decide where you want to put your backup files—preferably, on a different server or network share to ensure against complete loss of the server. Identify the absolute pathname or the pathname relative to the database location (inside [*install_drive*]:\EMC\Policy Manager\hsqldb\apm).

   b. Navigate to:

```
[install_drive]:\EMC\ESRS\Policy Manager\hsqldb\lib\
```

   c. Make a backup copy of apmbackup.vbs.

   d. Right-click **apmbackup.vbs**, select **Open with**, and select **Notepad**.

Note: There are three instances of the text **backup** in this script file, indicating (by default) the relative location of the backup directory.

   e. Substitute the pathname string inside quotes (default: **...\backup**) with your preferred path for creating a backup directory. Recheck your edits before saving and closing this file.

3. Specify and schedule the backup task:

   a. From the Scheduled Tasks window in step 1, double-click **Add Scheduled Task** to open the task creation wizard.

   b. In the next window, select the script (task) to run by choosing **Browse.**

   c. To see the available scripts, navigate to:

```
[install drive]:\EMC\ESRS\Policy Manager\hsqldb\lib
```

   d. Select **apmbackup.vbs**

   e. Select **Daily**, and click **Next**.

   f. Specify the activation time of day, frequency, and start date, and click **Next**.

   g. Type the domain, \, and username, and type and confirm the password, and click **Next**. Click **Confirm** on the next window.

Restoration procedures

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

Note: The Policy Manager service must be stopped before performing a restoration.

Server image backup restoration

For a Gateway Client or Policy Manager server:

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

Additionally, for a Policy Manager server:

Policy Manager database files are stored for up to 30 days. After 30 days, the most recent backup file overwrites the oldest backup file. Backup images are numbered 0 through 30, and are created by the automated Policy Manager backup script starting on the day after the Policy Manager install is completed.

For example, as shown in Figure 158 on page 257, the Policy Manager was installed on 3/06/08. The first backup was made to folder 0 on 3/07/08. On each successive day a new folder was created and the backup was written to that directory (the backup for 3/08/08 was written to folder 1; the backup for 3/09/08 was written to folder 2, and so on). The 31st backup occurred on 4/05/08 and was written to folder 30. On 4/06/08 the backup was written to folder 0, *replacing* the original backup *files* that were written on 3/07/08. The date on the folder did not change, but the date on the backup files inside the folder changed. (This backup process occurs every morning at 3 a.m. and is handled by the Windows Scheduler Application.)

Restore the Policy Manager database with files that are more recent than those on the drive image, but that precede the incident that caused you to perform a restoration.

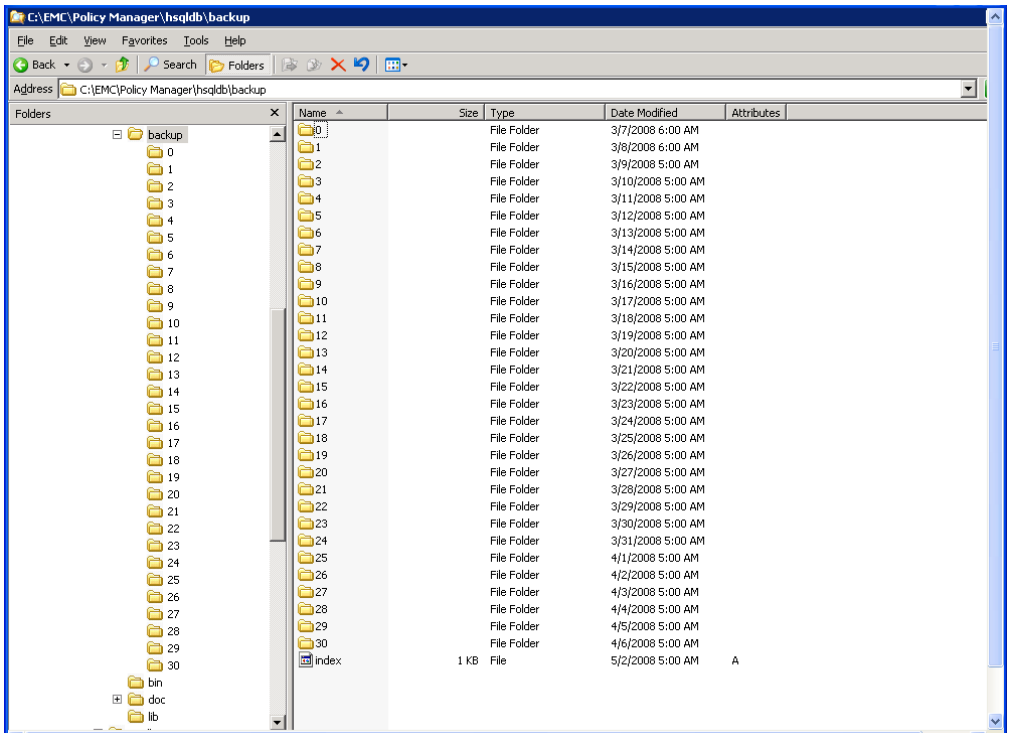


Figure 158 Backup folder

To restore a backup image:

1. Stop the Policy Manager service as described in "Startup/shutdown" on page 172.
2. Navigate to the following location as shown in Figure 159 on page 258:

   `[install_drive]:\EMC\Policy Manager\hsqldb\lib`

3. Double-click the script named **apmrestore.vbs**.

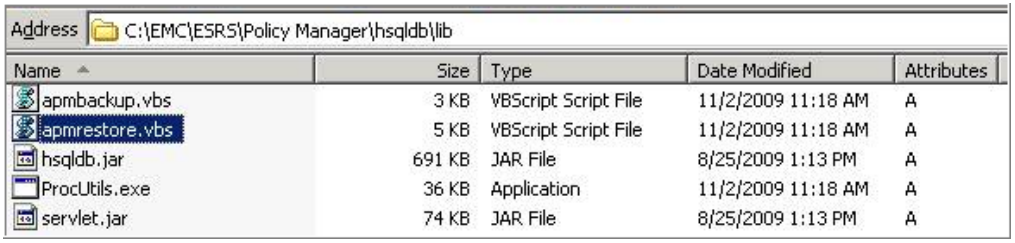


Figure 159 Location of apmrestore.vbs script

4. You are prompted about which backup image you want to restore, similar to that shown in Figure 160 on page 258. To restore the Policy Manager database, you must have located the backup for the date from which you wish to restore. This is done by looking through the directories of the backups to locate the file with the proper date. Make note of the folder name (0 through 30).

Note: The date listed for each folder is the date the folder was created. It is not necessarily the date the actual backup files were written.

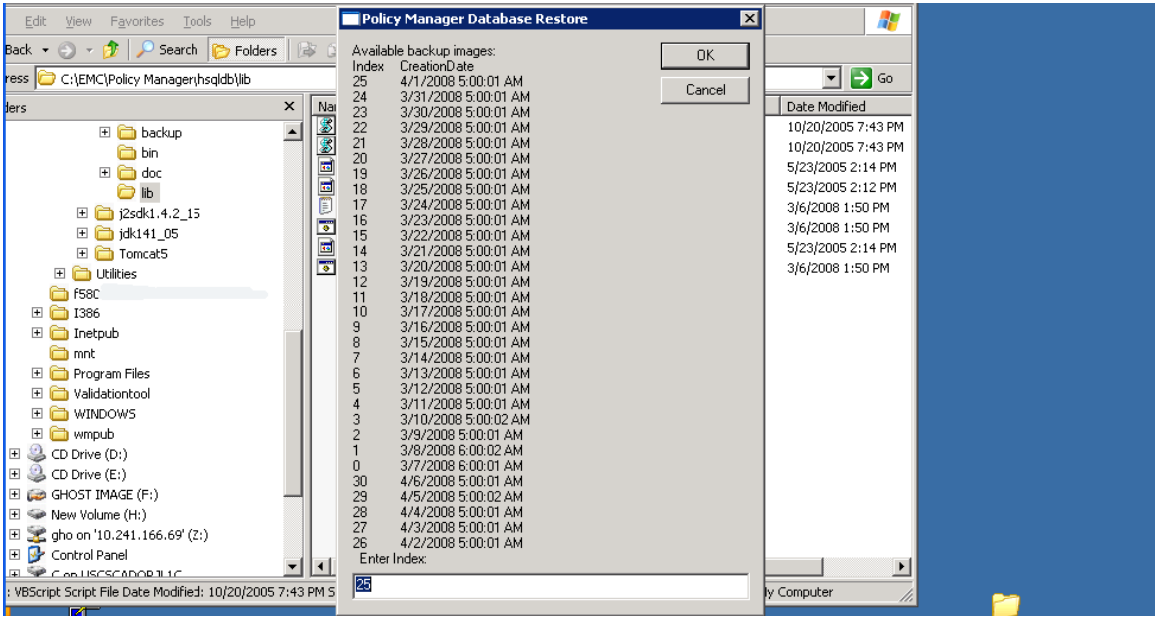


Figure 160 Restore prompt

5. Type the proper backup folder number and click **OK**.
6. You are now prompted with a confirmation. Click **OK**.

   The script completes the restoration.
7. Restart the Policy Manager service as described in "Startup/shutdown" on page 172.

Note: Audits that occur after the date of the restore date are *not* displayed in the audit history of the Policy Manager web interface. Any new audits are appended to the database as they occur. Even though the audits are not displayed in the web interface, they are viewable through the file system, located in the <*install_drive*>:\EMC\ESRS\Policy Manager\Audit directory.

Installation restoration

This section provides details on installation restoration.

IMPORTANT

If you need to restore a Policy Manager, start with a clean installation only if you have a recent database backup on a separate drive. Reinstall only the same software release version as that of the database backup.

For a Gateway or Policy Manager server:

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

Additionally, for a Policy Manager server:

Restore Policy Manager database files from a database backup located on a separate drive by using apmrestore.vbs as shown in step 1 on page 257 through step 6 on page 259 in the previous section.

CAUTION

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

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

Redundant Policy Manager

Note: Failover to a Redundant Policy Manager is a manual process and cannot be automated. The Redundant Policy Manager is a warm spare and is not active until the process below for manual failover is completed. If the Primary Policy Manager is un available and the Redundant Policy manager has not been activated there may be significant impact on the ESRS IP Solution's usability.

For additional protection, EMC recommends that you install a Redundant Policy Manager. This will enable you to continue policy management operations if your original Policy Manager becomes unavailable. A Redundant Policy Manager enforces the same policies as the original Policy Manager. It is recommended that the Redundant Policy Manager be installed and fully configured on a separate server prior to the need to fail over. This will significantly reduce the impact of the if Primary Policy Manager Becomes unavailable for whatever reason (hardware failure , network unavailability, or application failure)

You can uninstall and install a Policy Manager on the original server the Policy Manager was installed and use the restore process to recover the original Policy Manager and User databases however a backup of the databases must exist prior to the need to recover the Policy Manager in this manner

EMC is not responsible for the configuration of Redundant Policy Manager(s) above and beyond the basic install of the Policy Manager(s).

Due to the uniqueness each customer's environment (Corporate / IT Policies, network environments,etc) the customer is responsible for configuring automatic backups of the Policy Manager and local user databases to the Redundant Policy Manager(s), the editing of the scripts to perform these functions, configuration of the Scheduled Tasks, and verification of proper operation of the configuration for backup and failover to and/or back of the Redundant Policy Manager(s).

The instructions below are provided as an example of a configuration that has been tested does work. As each customers environment is different these procedures may need to be modified to meet the current conditions

Note: If the original Policy Manager becomes unavailable, you must manually fail over to the Redundant Policy Manager if located on another server.

Best Practices

Best practice dictates that for Redundant Policy Manager to be effective and reduce the impact of the Primary (active) Policy Manager becoming unavailable a number of manual configuration steps MUST be performed PRIOR to the need to use the Redundant Policy Manager. It should also be noted that if the Databases for the Primary Policy Manager are corrupt or damaged full recovery may not be possible.

Note: If the Primary Policy Manager is unavailable a backup of the Policy Manager Database and Local Policy Manager Users Database must be available to be restored to the Redundant Policy Manager or to recover the Primary Policy Manger

1. Redundant Policy Manager (non Primary) should be installed and fully functional before it is needed. Customizations for use of a customer external syslogger; integration with Windows AD or external LDAP for user authentication, remote backup to and from other Policy servers or any other features should fully configured and verified prior to the need to utilize the Redundant Policy Manager.
2. In addition to the Scheduled Task created during the install of the Policy Manager to backup the Policy Manager database locally at 3AM, separate Scheduled Task(s) on the Primary Policy Manager must be configured to back up both the Policy Manager and the Policy Manager Local Users Database to a location (Mapped Drive and Path) on the Redundant Policy Manager. The apmbackup.vbs scripts must be edited for this to function properly. If using the Local Users database (OPenDS) scripts should created and scheduled to backup the Local Users database both locally and to the redundant Policy Manager. This is especially important if the customer has created local users other that the default user account (admin)
3. To reduce the loss of audits, Policy changes and or changes to the Policy Manager User Database (OpenDS), within the Policy Manager, backups can be scheduled to some value less than 24 hours. The scheduled task can scheduled to run more frequently but be aware this will affect the number of days backups

available for restore of Redundant Policy Manager.(the apmbackup.vbs script will maintain 31 instances (0-30)of backups automatically.

a. This value can be changed by editing the index values in the remote apmbackup.vbs script. It should be noted that an increase in the number of backups maintained may have significant impact on free disk space especially in large active environments. Disk space management is the customer's responsibility and is not addressed or controlled by the Policy Manager processes.

4. It should be noted that frequent backups may also impact the availability of the Primary Policy Manager as the Policy Manager Service must be stopped as part of the backup process. Depending on the sizes of the PM databases and network latency the Primary(active) Policy Manager may become unavailable for a period of time. Large active environments and network latency can / will affect the length of time the Policy Manager will be unavailable during backup operations. The customer should balance this impact against the risk of not capturing all the audits and policy changes against the loss of immediate availability.
5. The flat audit files are not copied between the Primary Policy Manager and the Redundant Policy Manager – if so desired the customer may develop a script of their own to provide this capability.(an example of this functionality is NOT provided)
6. Each basic Policy Manager is configured independently of the other any customizations (streaming to a syslog server ; LDAP / Active Directory integration; etc) must be performed on each server as required
7. If not using Active Directory or LDAP for user authentication the Policy Manager Local Users Database must be manually backed up and restored as needed. There is no native automated / scripted method of doing this that is supported by EMC (examples provided)
8. Fail over to the Redundant Policy Manager is a manual process and is NOT automatic
9. The backup and failover processes should be tested after configuration to assure the behavior is as expected

10. If there is a desire to be able to fail back to the original Primary Policy Manager after it has become available this is also a manual process and is not automated. The same constrains as above apply. This requires that the process for Remote backup are also configured on the Redundant Policy Manager to the Primary Policy Manager. The fail back process from Redundant Policy Manager to the Primary Policy Manager is the same as failing over from the Primary Policy Manager to the Redundant Policy Manager with the exception that immediately prior to fail back you would trigger the Scheduled Tasks backup jobs to have the most recent versions of the Policy Manager and user databases available for the restore.

Failing over to the Redundant Policy Manager

This section explains how to manually fail over to a Redundant Policy Manager if you have a problem with your original Policy Manager server.

Note: If you install a Redundant Policy Manager, you must set up an automated backup process for your original Policy Manager database so that it can be restored onto the Redundant Policy Manager if needed. For information on setting up an automated backup process for your original Policy Manager database, see"Policy Manager database automated backup" on page 254. For information on performing a backup restoration, see "Server image backup restoration" on page 256.

Restoring to the same server

To restore a Redundant Policy Manager that has been installed on the *same* server as the original Policy Manager:

1. Partially uninstall the original Policy Manager.
2. Install Policy Manager. During installation, do *not* overwrite the backup files when prompted.
3. Run the Restore script (apmrestore.vbs) described in "Backup and restore scripts" on page 249.
4. Select the backup folder from the primary Policy Manager.

Restoring to a different server

To restore a Redundant Policy Manager that has been installed on a *different* server than the original Policy Manager:

1. Install Policy Manager if it has not already been installed.
2. Copy the backup files from the primary Policy Manager.

3. Save the backup files that were created during the installation to the backup folder in the Redundant Policy Manager.
4. Run the Restore script (apmrestore.vbs) described in "Backup and restore scripts" on page 249, selecting the backup folder that you created.

PART 5

Appendixes

This section provides detailed site maintenance reference information.

Appendix A, “Changing Security Parameters of the Policy Manager SSL Certificate”

This appendix explains how to change the security parameters of the Policy Manager Secure Sockets Layer (SSL) certificate to create a more secure certificate.

Appendix B, “Enabling SSL communication between the ESRS IP Client and Policy Manager”

This appendix explains how to enable SSL communication between the ESRS IP Client and the Policy Manager.

Appendix C, “Default Policy Values”

This appendix provides information about Policy Manager default permissions, access rights, and remote application names.

Appendix D, “LDAP integration”

This appendix provides details about Policy Manager integration with LDAP.

Appendix E, “Troubleshooting”

This appendix provides information about troubleshooting unexpected service events. It also explains how to perform configuration tasks to identify failures of the ESRSHTTPS listener.

A

Changing Security Parameters of the Policy Manager SSL Certificate

This appendix explains how to change the security parameters of the Policy Manager Secure Sockets Layer (SSL) certificate to create a more secure certificate. This work must be performed by an EMC Global Services professional.

The appendix contains the following topic:

Making an SSL certificate more secure

This section explains how to create a Policy Manager Secure Sockets Layer (SSL) certificate that is more secure than the default certificate. This is done by changing the security parameters of the certificate.

Note: Changing the security parameters must be done by an EMC Global Services professional.

Changing the security parameters

The following procedure shows an example of how to create an SSL certificate:

1. Ensure that Java Runtime Environment (JRE), version 1.6 or greater, is installed on the ESRS IP Policy Manager. JRE is available from the following website:

   http://java.sun.com

2. Open a command prompt and proceed to the following directory containing the Java key tool:

   ```
   C:\>cd "Program Files\Java\jdk1.6.0_14\bin"
   ```

3. To create a keystore, run the following command. The command will create a keystore with name **PMIdentityStore.jks** and a self-signed certificate to use for SSL communication:

   ```
   >keytool -genkey -alias tomcat -keyalg RSA -keysize
   2048 -dname
   "CN=HostName,OU=EMC,O=ESRS,L=Westborough,S=MA,C=US"
   -validity 1095 -keypass PMStorePass1234 -keystore
   PMIdentityStore.jks -storepass PMStorePass1234
   ```

   Note: The variable **HostName** is the fully qualified name of the Policy Manager host system.

For additional information about SSL certificates (an Identity Keystore File) for Apache Tomcat, refer to the following website:

http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html

B

Enabling SSL communication between the ESRS IP Client and Policy Manager

This appendix explains how to enable Secure Sockets Layer (SSL) communication between the ESRS IP Client and the Policy Manager. This work must be performed by an EMC Global Services professional.

The topics in this appendix include:

Policy Manager configuration for SSL

This section explains how to change the Policy Manager configuration to support Secure Sockets Layer (SSL) communication.

Note: The configuration change must be performed by an EMC Global Services professional.

Enabling SSL on a Policy Manager

Use the following procedure to enable SSL on a Policy Manager:

1. Stop the Policy Manager service.
2. Ensure that you have created an Identity Keystore File (`PMIdentityStore.jks`) as described in "Making an SSL certificate more secure" on page 270.
3. Copy PMIdentityStore.jks to the following directory:

   `<install_root>\EMC\Policy Manager\Tomcat5\bin`

4. Locate the following file:

   `<install_root>\EMC\Policy Manager\Tomcat5\conf\server.xml`

5. Make a copy of the server.xml file and rename it to server.xml.orig.
6. Open the server.xml file using a text editor such as Notepad.

7. Locate and delete all the text between and including the <!-SSL and --> tags in the section inside the <Service name="Catalina"> element as shown in bold text:

```
  <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
  <!-- Start SSL -->
  <Connector port="8443" maxHttpHeaderSize="8192"
     maxThreads="5000" minSpareThreads="25" maxSpareThreads="75"
     enableLookups="false" disableUploadTimeout="true"
     acceptCount="1500" scheme="https" secure="true"
     clientAuth="false" keystoreFile="C:\EMC\ESRS\Policy Manager/apsserver.jks"
     keystorePass="tomcat" sslProtocol="TLS" />
<!-- End SSL -->
```

8. Add a new <Connector> element inside the <Service name="Catalina"> element as shown in bold text:

```
  <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
  <!-- Start SSL -->
  <Connector port="8443" maxHttpHeaderSize="8192"
     maxThreads="5000" minSpareThreads="25" maxSpareThreads="75"
     enableLookups="false" disableUploadTimeout="true"
     acceptCount="1500" scheme="https" secure="true"
     clientAuth="false" sslProtocol="TLS" keystorePass="PMStorePass1234"
     keystoreFile="C:/EMC/ESRS/PolicyManager/Tomcat5/bin/PMIdentityStore.jks"/>
  <!-- End SSL -->
```

9. Save the file with the updated configuration.

For the keystore attributes and descriptions, see Table 12 on page 274.

Table 12 Keystore attributes

Attribute	Description
keystoreFile	Add this attribute if the keystore file you created is not in the default location Tomcat uses (a file named .keystore in the user home directory under which Tomcat is running). You can specify an absolute pathname, or a relative pathname that is resolved against the $CATALINA_BASE environment variable.
keystorePass	Add this element if you used a keystore (and Certificate) password other than the default keystore password (changeit).
keystoreType	Add this element if using a keystore type other than JKS.
keyAlias	Add this element if you have more than one key in the KeyStore. If the element is not present, the first key read in the KeyStore is used.

Enabling the Policy Manager application to use SSL for all communications

Use the following procedure to enable the Policy Manager to use SSL for all communications:

1. Locate the following file:

<*install_root*>\EMC\ESRS\Policy Manager\Tomcat5\webapps\applications\apm\WEB-INF\web.xml

2. Create a copy of web.xml and rename it to web.xml.orig.
3. Open web.xml using a text editor such as Notepad.
4. Find the <security-constraint> with any web-resource-name and modify a portion of it to include the <user-data-constraint> element as shown in the following bold text.

```
<web-app>
......
......
<security-constraint>
   <web-resource-collection>
   <web-resource-name>anything</web-resource-name>
   ......
   </web-resource-collection>
   ......
   <user-data-constraint>
   <transport-guarantee>CONFIDENTIAL</transport-guarantee>
   </user-data-constraint>
   ......
</security-constraint>
......
</web-app>
```

5. Add a new <security-constraint> element inside the <web-app> element as shown in the following bold text.

```
  <web-app>
  ......
  ......
  <security-constraint>
     <web-resource-collection>
     <web-resource-name>Message Servlet</web-resource-name>
     <url-pattern>/message</url-pattern>
     </web-resource-collection>
     <user-data-constraint>
     <transport-guarantee>CONFIDENTIAL</transport-guarantee>
     </user-data-constraint>
     </security-constraint>
</web-app>
```

6. Save the file with the updated configuration.
7. Restart the Policy Manager service.

Gateway Client configuration for SSL

This section explains how to change the Gateway Client configuration to support SSL communication:

1. Locate the following file:

   `<install_root>\EMC\ESRS\Gateway\xgAPMProxy.xml`

2. Create a copy of xgAPMProxy.xml and rename it to xgAPMProxy.xml.orig.
3. Open xgAPMProxy.xml using a text editor such as Notepad.
4. Add the following <Encryption> element inside the <APMProxyConfig> element as shown in bold text:

```
<APMProxyConfig>
......
......
      <Encryption>
      <Bits>128</Bits>
      <Validate>false</Validate>
      </Encryption>
</APMProxyConfig>
```

Note: The value of the Bits element denotes the strength (in bits) of the SSL certificate used in the Policy Manager.

5. Save the file with the updated configuration and restart the Gateway service.
6. Launch the ESRS IP Configuration Tool on the Gateway Client from **Start** > **Programs** > **ESRS** > **Configuration Tool**.
7. From the Configuration Tool, click the **Policy Manager** tab.

8. In the Connection area of the Policy Manager tab, reset the cache by updating the following fields with the specified values:
   - **Port** = 8443 (or the value specified for SSL port in server.xml)
   - **Enable SSL** = Checked
   - **Strength** = High
   - **IP Address/Host** = Host Name of the Policy Manager
9. Click **Apply Settings** to update your changes to the Gateway Client, as shown in Figure 161 on page 278.

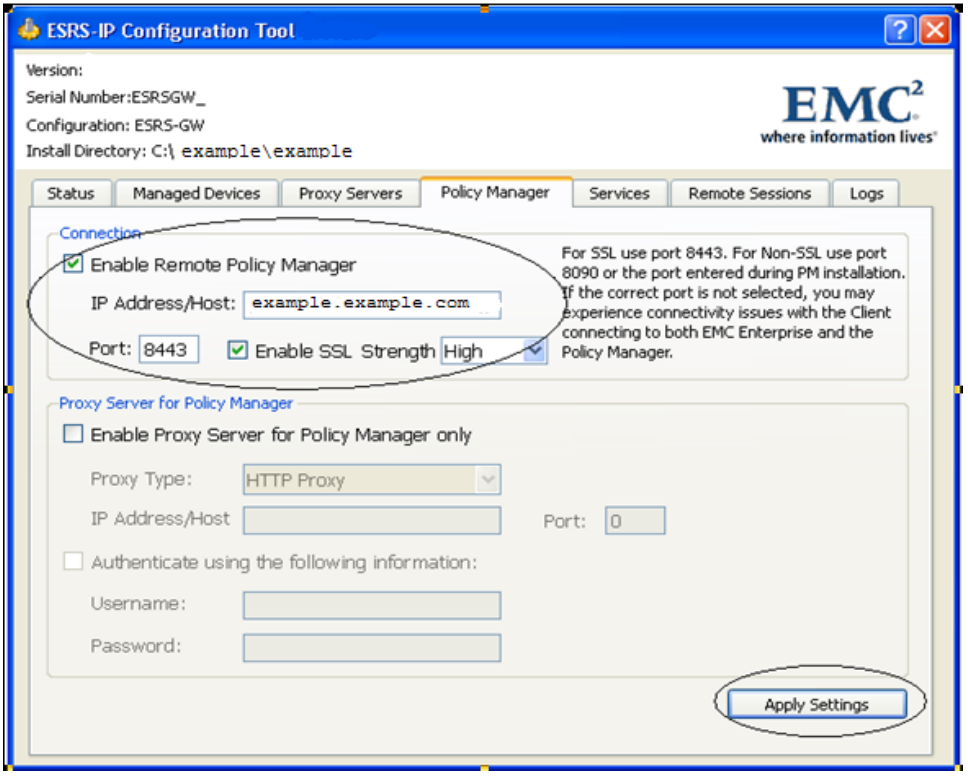


Figure 161 Configuration Tool—Connection settings

C

Default Policy Values

This appendix provides additional details on Policy Manager actions and Policy Manager default permissions and access rights. It also provides the correct remote application names for setting permissions for remote applications. It includes the following sections:

Policy Manager actions

Descriptions of the available ESRS IP Policy Manager actions are provided in Table 13 on page 280.

You see all Actions defined for a particular group when you examine that group's policy settings. (For example, see Figure 116 on page 190.)

Table 13 Actions defined by ESRS IP solution (page 1 of 2)

Action	Used by	Description
Register Script	Gateway Device only	Determines whether or not the ESRS IP Client can register a script on the device as requested, or needs to receive approval for the permission first. Permission parameters: name of the script to register.
Run Script	Gateway Device only	Determines whether or not the ESRS IP Client can run a script, or needs to receive approval for the permission first. Permission parameters: name of the script to run.
Schedule a Script	Gateway Device only	Determines whether or not the ESRS IP Client can schedule a script for operation on the device as requested, or needs to receive approval for the permission first. This action has no specific parameters.
Set Data Item Values	All except Gateway Device	Controls whether or not the ESRS IP Client can write values to its data items as requested, or needs to receive approval for the permission first. This action has no specific parameters.
Package	Gateway Device only (Can be modified)	Determines whether or not the ESRS IP Client accepts a package, or needs to receive approval for the permission first. Permission parameters: Name and version number of the package to execute on the device. All contents of a package are included in the permission. (Packages are handled differently than other permissions; check with EMC Global Services.)
Data Item Values	All except Gateway Device	Determines whether or not the ESRS IP Client can send data item values, or needs to receive approval for the permission first. (This does not affect data item values sent as the result of a Write Data Item action, configured in a logic schema.) For this release, only one permission can be set for all data items, meaning all data items are included in the action.
File Download	Gateway Device only (Can be modified)	Determines whether or not the ESRS IP Client can accept files downloaded to it from the DRM, or needs to receive approval for the permission first. Permission parameters: Fully-qualified path of the file(s) to download to the device. The name(s) of the file(s) and path(s) may be explicit (for example, "c:\error.log" or include wildcards (for example, "c:*.log" or "c:*.*").

Table 13 Actions defined by ESRS IP solution (page 2 of 2)

Action	Used by	Description
File Upload	Gateway Device only	Determines whether or not the ESRS IP Client can upload files to the DRM (whether an DRM-based request or ESRS IP Client-initiated process), or needs to receive approval for the permission first. Permission parameters: Fully-qualified path of the file(s) to upload to the DRM. The pathname on the device can be explicit or relative (which the ESRS IP Client interprets to be the root of the ESRS IP Client installation). File names can be explicit (for example, “error.log” or include wildcards (for example, “*.log” or “*.*”). Gateway defines File Upload permissions for connect home device configuration, FTP, and SMTP.
Restart Client	Gateway Device only (Can be modified)	Determines whether or not the ESRS IP Client can restart itself as requested, or needs to receive approval for the permission first. This action has no specific parameters.
Remote Application	A different set of instances is used by each device model	Determines whether the ESRS IP Client can start a remote application session as requested, or needs to receive approval for the permission first. Although applications are in general Always Allow access, permissions for specific applications are set at “Always Allow.” Permission Parameters: name of the remote application interface. For additional information, see “Remote Application names” on page 284.

Default permissions and access rights

The default Policy Manager installation provides global default permissions and access rights. It also provides device group default permissions and access rights.

Global and device groups have the following similarities:

- They have the same default permissions.
- They have the same default access right, which is Always Allow.

The default permissions and access rights are shown in Table 14 on page 283.

Note: When a new device registers with the Gateway for the Policy Manager, it copies the default settings for its particular device group.

CAUTION

If you change any Access Rights for Remote Application actions, change them *only* at the device group level or device level.

To avoid unexpected system behavior, do not edit the global permissions without assistance from EMC Global Services.

Table 14 Global and Device Group default permissions

Action	Permission	Parameters	Access Right
Enable a Script	Default enable a script permission	Script name: *	Always Allow
Schedule a Script	Default permission for scheduling a script	Script name: *	Always Allow
Register Script	Default register script permission	Script Name: *	Always Allow
Disable a Script	Default disable a script permission	Script name: *	Always Allow
Run Script	Default run script permission	Script Name: *	Always Allow
Run Script	ESRS Diagnostics	Script Name: ESRS Diagnostics*	Always Allow
Stop Script	Default stop script permission	Script Name: *	Always Allow
UnSchedule a Script	Default permission for unscheduling a script	Script name: *	Always Allow
UnRegister Script	Default unregister script permission	Script Name: *	Always Allow
Set Data Item Values	Permission for All Data Items	Data Item Name: *	Always Allow
Set Time	Default set time permission	Time: *	Always Allow
Emails	Permission for All Emails	Email to: *	Always Allow
Package	ESRS Maintenance	ESRS Maint*	Always Allow
Package	Default package permission	Name: * Version: *	Always Allow
File Download	Default file download permission	File: *	Always Allow
File Upload	Default file upload permission	File: *	Always Allow
Execute	Default execute permission	Application: *	Always Allow
Gateway Provisioning	Default Gateway provisioning permission	Action:*	Always Allow
Remove a Timer	Default remove timer permission	Timer name: *	Always Allow
Disable a Timer	Default disable timer permission	Timer name: *	Always Allow
Enable a Timer	Default enable timer permission	Timer name: *	Always Allow
Create a Timer	Default create timer permission	Timer name: *	Always Allow
Stop Remote Application	Default stop remote application	sessionid:*	Always Allow
Remote Terminal	Default terminal permission	Remote Interface Name: *	Always Allow
Remote Application	Default application permission	Remote Application Name: *	Always Allow

Remote Application names

CAUTION

The current implementation of Policy Manager controls all remote applications for a specific device or device group under a single permission inherited from the Global permission "Remote Application." If you decide you want to control each remote support application individually, you *must* create *all* support applications associated with the specific device and set the permissions individually. Any application that is not defined will not be available for use, which may impact EMC's ability to properly support the device in question.

If the definitions are created at the Group level, they will propagate to all the devices within the group. If they are defined at the Device level, they will only apply to that specific device. Individual remote applications should not be defined at the Global level.

A decision to control each remote support application individually should not be taken lightly, as it can greatly complicate Policy Manager configuration and management and may impact the ability to upgrade to future releases of the product.

Overview

When you set up Remote Application access in Policy Manager for a particular device type, you must use a specific Remote Application name with a specified spelling, capitalization, and word spacing.

For example, if you are setting up the CLIviaSSH remote application for a Celerra device, you must enter the remote application name in *exactly* that way: CLIviaSSH, with no spaces and the correct combination of upper case and lower case letters.

Required syntax

For the required syntax for each remote application, see Table 15 on page 285.

Table 15 Required syntax for Remote Application name (page 1 of 2)

Device type	Remote application
Atmos	CLIViaSSH
	SecureWebUI
Avamar	CLIViaSSH
	AVInstaller
	Enterprise Manager
CLARiiON	KTCONS
	Navisphere Manager
	NaviSecCLI
	RemotelyAnywhere
	EMCRemote
	NaviCli
	RemoteKtrace
	Remote Diagnostic Agent
Celerra	CLIviaSSH
	Celerra Manager
	Telnet
Connectrix- McData	EMCRemote
Centera	Centera Viewer
	CLIviaSSH
Greenplum DCA	CLIviaSSH
Invista	InvistaElement Manager
	Invista CLI
	EMCRemote
EDL Engine	EDL Management Console
	CLIviaSSH
	SecureWebUI
DLm	CLIviaSSH
	Celerra Manager
	Telnet
DL3D	CLIviaSSH
	EDL Management Console
	SecWebUI
RecoverPoint	CLIviaSSH
Switch Brocade	Telnet
	CLIviaSSH
	EMCRemote

Table 15 Required syntax for Remote Application name (page 2 of 2)

Device type	Remote application
Switch- Cisco	Telnet
	CLIviaSSH
Symmetrix	EMCRemote
	SGBD
	Swuch
	Remote Browser
	RemotelyAnywhere
	InlineCS
VNX	KTCONS
	RemoteKtrace
	RemotelyAnywhere
	CLIViaSSH
	Unisphere
	USM
	Navisphere SecureCLI
	Remote Diagnostic Agent
VNXe	CLIViaSSH
	Unisphere
VPLEX	ElementManager
	CLIViaSSH

D

LDAP integration

This appendix contains information about configuring Policy Manager to use the following external directory servers:

Note: Integration with Windows Active Directory is not currently supported, It will be supported in a future release.

External LDAP integration

This section provides information about configuring the following external LDAP directory servers:

- Sun ONE LDAP external directory server
- OpenDS LDAP external directory server

IMPORTANT

External LDAP directory servers are *not supported* by EMC Global Services. The following procedures are provided for general guidance only. If you choose to use an external LDAP server, you must engage your technical and security teams for LDAP configuration and support.

Sun ONE LDAP

To use an existing Sun ONE LDAP directory server to authenticate ESRS IP Policy Manager users, you must first perform the following tasks:

- Set up the groups required for ESRS IP Policy Manager in that directory server. Although you can set up the groups after installing Policy Manager, consider setting them up beforehand.
- Collect the information about the Sun ONE directory server that you will need when you run the ESRS IP Policy Manager installation program.

The following sections explain how to perform these tasks.

Note: These instructions are provided for the collection of LDAP configuration information to be used during installation of the ESRS IP Policy Manager. The same information is required to implement OpenDS LDAP with the Policy Manager.

Configuring groups and users

To configure your Sun ONE LDAP directory server for the ESRS IP Policy Manager, you must create the following groups:

APSAdmins group — The users that you define in the APSAdmins group will be able to log in to Policy Manager, configure additional users, and access all of the Policy Manager components.

APSUsers group — The users that you define in this group will be able to log in to the ESRS IP application. The specific tasks that users

can perform within the application are determined by the roles that you assign to them and the profiles you assign to those roles.

APSLdapAdmins group — The users that you define in this group are authorized to change user information and passwords, using the Administration tab within Policy Manager.

To configure the LDAP groups and users, follow these steps:

1. Log in to the LDAP directory server as an administrator capable of creating groups and users.
2. Create the following groups (Groups organization unit / ou) in the directory server database:
   - APSAdmins
   - APSUsers
   - APSLdapAdmins
3. Make the APSAdmins group a member of the APSLdapAdmins group.
4. Create the following user types (People organization unit / ou) in the directory server database:
   - An Admin user who is a member of the APSAdmins and APSUsers groups.
   - A non-Admin user who is a member of the APSUsers group or of a subgroup of the APSUsers group. A non-Admin user should not be a member of APSLdapAdmins, but should have access to an account defined in the APSLdapAdmins group.
5. Create users in the People organization. For example, a user in the **ldap.siroe.com** domain might have the following DN (LDAP distinguished name):

   ```
   cn=Barbara Jones, ou=Engineering, dc=siroe, dc=com
   ```

   Provide the following information for each user:

   - First Name and Last Name.
   - Common Name (cn). This is the name that the directory server will use to address the user on login.
   - User ID (UID). This name should uniquely identify the person or object defined by the entry.
   - Password to associate with the user. Confirm by retyping the password.

- (Optional) E-mail address. Required if you want to permit Policy Manager to send notification e-mails to the user.
- (Optional) Phone number and fax number.

6. When you have added users to the People organization, add them to the applicable ESRS IP Policy Manager groups.

Keep the following in mind:

- Users in the APSAdmins group must also be members of the APSUsers group.

  Note: To be an administrator, a user must belong directly to the APSAdmins group. You cannot give administrator privileges to an entire group by placing the group in the APSAdmins group.

- Non-administrative users who need to modify the LDAP user configuration (password, for example) will require access to an account defined in the APSLdapAdmins group.
- Users who are defined only in the APSLdapAdmins group and not in the APSUsers group will not be able to access the ESRS IP Policy Manager application.

Note: You should configure only one account in the APSLdapAdmins group. You should then provide that account information to all non-Admin users who need to be able to modify LDAP user settings from within the User Preferences of the ESRS IP Policy Manager application. Users who are members of the APSAdmins group, but do not have access to the APSLdapAdmins user account, will not be able to modify LDAP users and groups.

Finding information for configuring security

The installation program for the ESRS IP Policy Manager automatically sets the appropriate properties for the Sun ONE LDAP directory server, as long as you can provide certain information while running the installation program.

The following section explains where to locate the required information for configuring security.

Note: This section assumes that a Sun ONE LDAP directory server is already installed and that you have access to the Sun Java System Server Console application.

Displaying your current directory server information

To find the necessary information for configuring security:

1. Start the Sun Java System Server Console application (**startconsole.exe**).
2. In the **Servers and Applications** tab, expand the node that shows the name of your directory server machine. Using the machine name, **ldapServer.axeda.com**, expand the node as follows:

   ```
   ldapServer.axeda.com > Server Group > Directory Server
   ```

3. When the information about your directory server appears in the right pane, click **Open**.
4. Click the **Directory** tab to display it.

The next step is to locate the information for the Directory Server Principal (DN and Password).

Locating the Directory Server Principal information

To locate the information for the Directory Server Principal (DN and Password):

1. In the left pane of the **Directory** tab of the Sun ONE directory server application, select **o=NetscapeRoot>TopologyManagement>Administrators**
2. In the right pane of the **Directory** tab, right-click the **username, admin**, and select **Edit** with Generic Editor. The Generic Editor dialog box appears, showing the full name assigned to the administrator at the top.

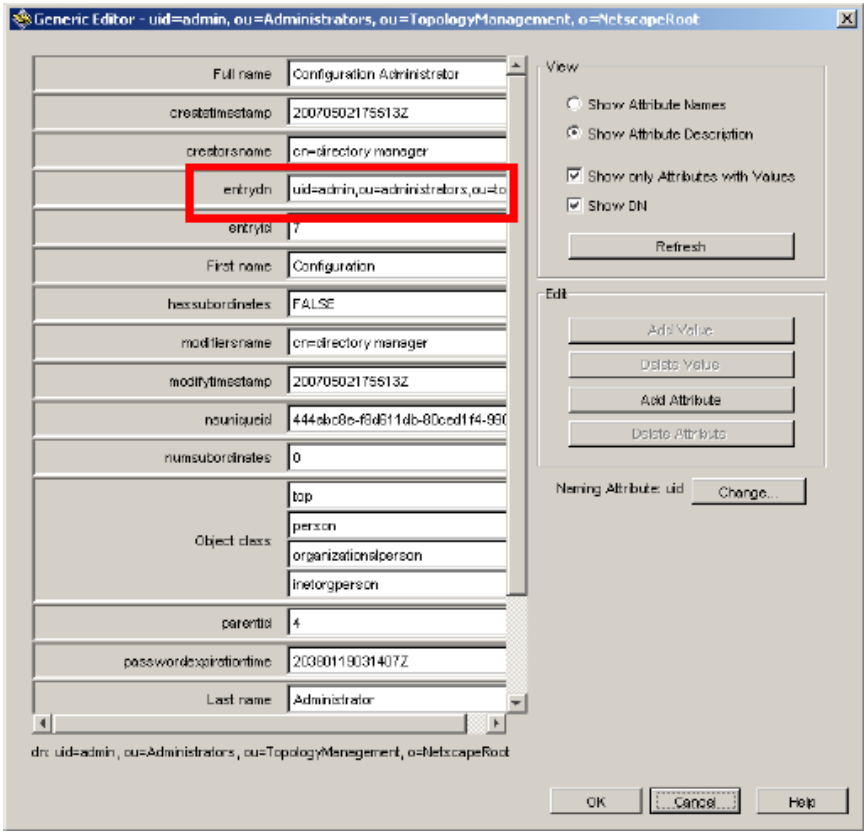


Figure 162 Generic editor—Administrator

3. Locate the entrydn property, as shown in Figure 162 on page 292, and copy its content to an empty text file (such as a Notepad file). Using the example shown, you would copy the following information from this field:

```
uid=admin,ou=administrators,ou=topologymanagement,o=netscaperoot
```

4. Click **Cancel** to exit the Generic Editor dialog box.

The next step is to locate the information for the User Base DN.

Locating the User Base DN information

To locate the information for the User Base DN:

1. In the left pane of the Directory tab, click **dc=axeda,dc=com** to display its components in the right pane.
2. In the right pane of the **Directory** tab, right-click **People**, and select **Edit with Generic Editor. The** Generic Editor dialog box for the selected organization (People) appears, as shown in Figure 163 on page 293.

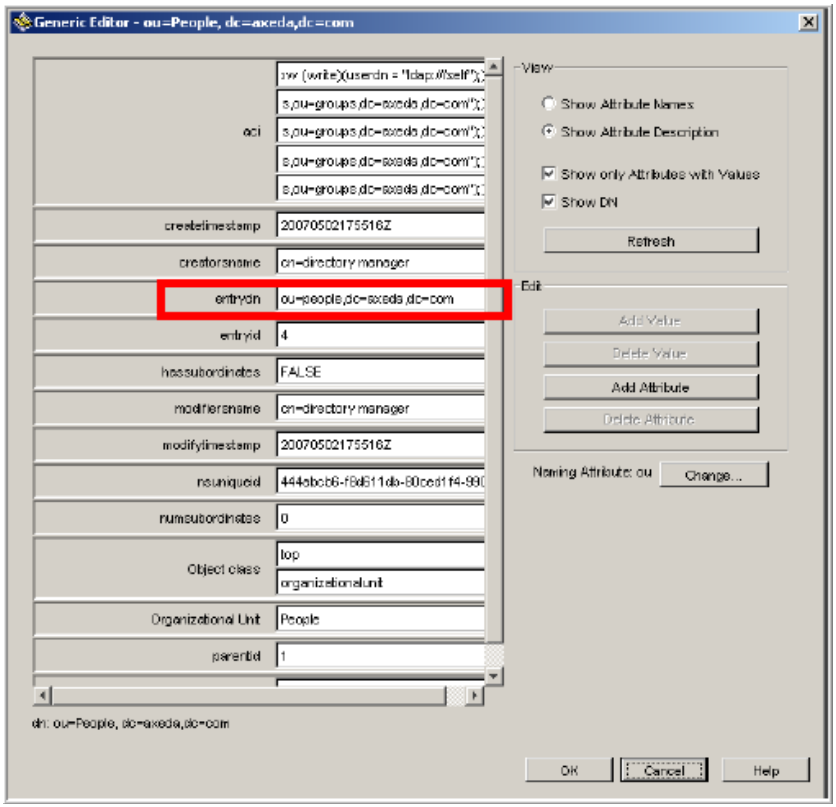


Figure 163 Generic editor—People

3. Copy the information in the **entrydn** field and paste it in your Notepad file. In this example shown in Figure 163 on page 293, the information is **ou=people,dc=axeda,dc=com**. Use this information to configure the **UserBaseDN** field when you run the installation program for the ESRS IP Policy Manager.

4. Click **Cancel** to exit the dialog box.

The next step is to locate the Group Base DN information.

Locating the Group Base DN information

To locate the information for the Group Base DN:

1. If necessary, in the left pane of the **Directory** tab, click **dc=axeda,dc=com** to display its components again in the right pane.
2. In the right pane, right-click **Groups**, and select **Edit with Generic Editor**. The Generic Editor dialog box for the selected organization (Groups) appears.

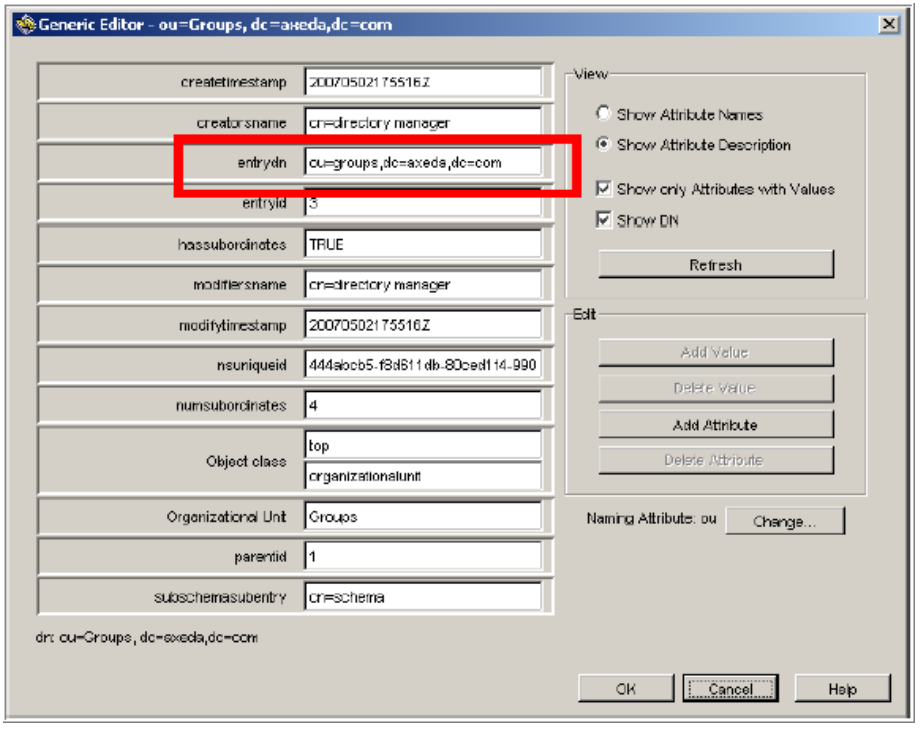


Figure 164 Generic editor—Groups

3. The information you need to copy and paste into the Notepad file is in the **entrydn** field, as shown in Figure 164 on page 294. Using the example shown here, you would copy:

   ou=groups,dc=axeda,dc=com

   Use this information to configure the Group Base DN in the installation program for the ESRS IP Policy Manager.

Configuring users and groups

To configure users and groups for the Policy Manager, follow these steps:

1. If it is not running, start the Sun Java System Server Console application (*startconsole.exe*).
2. In the **Servers and Applications** tab, expand the node that shows the name of your directory server machine. Using the machine name, **ldapServer.axeda.com**, expand the node as follows:

   ldapServer.axeda.com > **Server Group** > **Directory Server**
3. When the information about your Directory Server appears in the right pane, click **Open**.
4. Click the **Directory** tab to display it.
5. In the left pane of the **Directory** tab, click the node, **dc=axeda,dc=com**.
6. In the right pane, right-click the **Groups** organization, and select **New** > **User or New** > **Groups** to add each required user or group for Policy Manager. Follow the instructions in the section to ensure that you create all the required users and groups.

Changing the port value for the LDAP directory server

To change the port value for the LDAP directory server:

1. Start the Sun Java System Server Console application (*startconsole.exe*).
2. In the **Servers and Applications** tab, expand the node that shows the name of your directory server machine. Using the machine name, **ldapServer.axeda.com**, expand the node as follows: **ldapServer.axeda.com** > **Server Group** > **Directory Server**
3. When the information about your directory server appears in the right pane, click **Open**.
4. Click the **Configuration** tab to display it.

5. In the right pane of the Configuration tab, click the **Network** tab. An example of the tab is shown in Figure 165 on page 296.

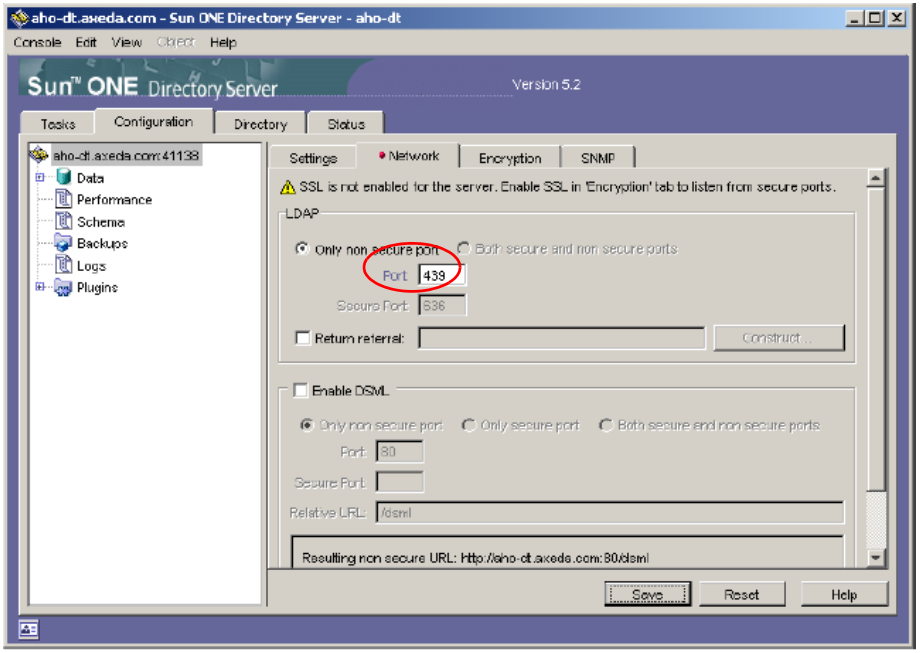


Figure 165 Configuration and Network tabs

6. In the **Network** tab, change the current port number to **389**.
7. Click **Save**. The Confirmation screen shown in Figure 166 on page 297 appears. You do not need to write down the steps shown on the Confirmation screen because they are repeated in the following procedure steps.

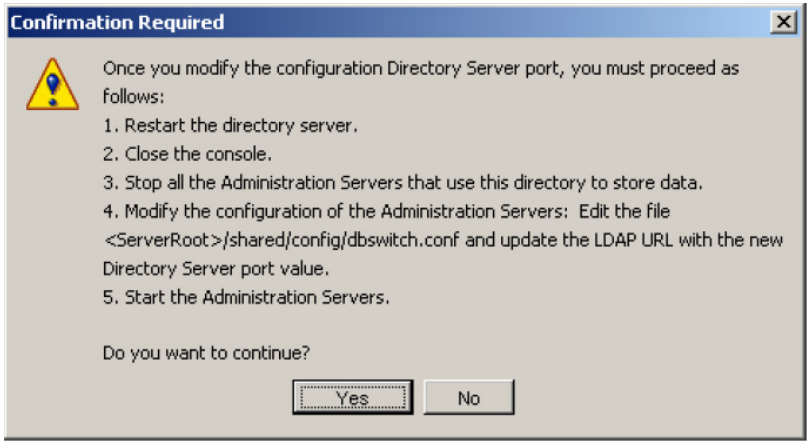


Figure 166 **Confirmation screen**

8. Click **Yes** to continue, or **No** to cancel the change of the port number. If you select **Yes**, a warning message appears as shown in Figure 167 on page 297.

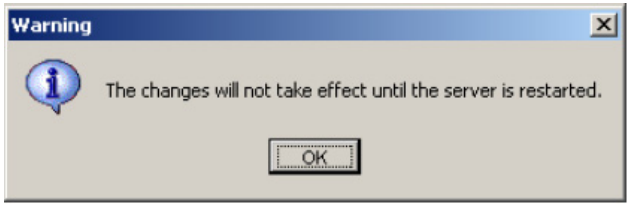


Figure 167 **Warning message**

9. As instructed in the Confirmation prompt, complete the change by taking the following steps:
   a. Restart the Directory Server.
   b. Close the Console application.
   c. Stop the Policy Manager server that uses the directory to store data.

d. For each Policy Manager server, edit the file PolicyManager.properties (located in the directory <installation_dir>/tomcat5/common/classes/) and update the LDAP information with the new directory server port value.

e. Start the Policy Manager server.

Enabling SSL encryption for the LDAP directory server

This section explains how to set up the Sun ONE LDAP directory server to support SSL for use with the ESRS IP Policy Manager.

Note: If you are switching from non-SSL to SSL for communications with the ESRS IP Policy Manager, ensure that your LDAP server is working properly with Policy Manager before making the change.

Starting the Sun ONE directory server

To start the Sun ONE directory server:

1. Open the Sun ONE Server Console.
2. Expand the Tree View for the desired domain (that is, the LDAP server) until the **Directory Server** item is displayed.
3. Right-click **Directory Server** and select **Open** from the context menu.
4. Select the **Tasks** tab.
5. Click **Manage Certificates** to open the Manage Certificates dialog box:
   - If you are entering this area for the first time, the system prompts you to set a server password. Remember this password, as you will need it for all future access to certificates or server restarts.
   - If you have a server password, enter it now. The following procedures assume that you are running the Console application for your Sun ONE directory server.

Generating a certificate request

To generate a certificate request:

1. Select the **Server Certs** tab.
2. Click **Request…** to start the Certificate Request Wizard.
3. On the Introduction page of the wizard, click **Next**. This page is the first of four pages (1 of 4).

4. Enter the information on the Requestor Information page (2 of 4).

   Note: The "Server name" is the name of the machine that is running the LDAP server, as it appears in the Tree View of the Sun ONE Console application.

5. To display the Token Password page (3 of 4), click **Next**.
6. Type the server password, and click **Next** to display the last page (4 of 4).
7. Click **Copy to Clipboard**.
8. Open Notepad, and from the **Edit** menu, select **Paste**.
9. If the file contains any blank lines, remove them.
10. Save the file as **sunone.cert**, and close Notepad.
11. Click **Done** to close the Certificate Request Wizard.
12. Send the *sunone.cert* file to your certificate authority (CA) to retrieve a server certificate. Alternately, if using OpenSSL to generate the certificate, refer to the Axeda procedure, "*To generate your own Sun ONE certificate*."

Installing the server certificate in Sun ONE

To install the server certificate in Sun ONE:

1. Return to the Manage Certificates dialog box. For instructions on how to display the dialog box, see "Starting the Sun ONE directory server" on page 298.
2. To start the Certificate Install Wizard, click **Install….**
3. In the Certificate Location page (1 of 4), select the option, **in this local file:**.
4. Click **Browse** and then locate and select the server certificate returned by your certificate authority (CA).
5. Back in the Certificate Location page, click **Next**.
6. In the Certificate Information page (2 of 4), review the certificate information to ensure that it is correct.
7. Click **Next** to display the Certificate Type page (3 of 4).
8. To keep the certificate name server-cert, click **Next**.

9. Enter the Token password and click **Done**. The Token password is the password mentioned in "Starting the Sun ONE directory server" on page 298.
10. Click the **Server Certs** tab, and verify that the certificate name server-cert appears in the list.
11. Click **Done** to return to the main Directory Server page.

Enabling SLDAP in Sun ONE

To enable SLDAP in Sun ONE:

1. Select the **Configuration** tab to display the Directory Server configuration.
2. Edit the **Encrypted Port** if desired (the default port is 636 and it is recommended that you use this value).
3. On the Configuration page, click the **Encryption** tab.
4. Select the **Enable SSL** checkbox for this server.
5. Select the **Use this cipher family: RSA** checkbox.
6. Ensure that the setting for **Security Device** is **internal (software)**.
7. Ensure the **Certificate** listed is the one you just installed, server-cert.
8. Select the option, **Do not allow client authentication**.
9. Click **Save**.
10. Select the **Tasks** tab to display the list of available tasks for the Directory Server.
11. Click **Restart**.
12. When prompted, type the server password to start the directory server. The server password is the password mentioned in "Starting the Sun ONE directory server" on page 298.

OpenDS LDAP

To implement OpenDS LDAP with ESRS IP Policy Manager, you need to collect the same LDAP configuration information described in "Sun ONE LDAP" on page 288. Refer to that section for instructions.

E

Troubleshooting

This appendix provides information about troubleshooting unexpected service events. It also explains how to perform configuration tasks to help troubleshoot the ESRSHTTPS listener:

Troubleshooting unexpected service events

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

Service malfunction

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

Service does not start up

If the Gateway Client or Policy Manager service fails to manually start up from the Services window, it might be caused by one of the following problems:

- Files that have been inadvertently deleted or moved:
  1. Examine the server log file to confirm missing-file errors.
  2. Attempt restoration from image backup. You may have to reinstall if image backup is not available. See "Restoration procedures" on page 256.
- Virus damage:
  1. Run a virus scanner program and attempt a virus repair if needed.
  2. If a virus repair is not successful, you may need to reinstall, as described in "Restoration procedures" on page 256.

Operating system or hardware failures

If a server failure clearly occurs at a more basic level than the Gateway Client or Policy Manager service, you may want to perform a reinstallation, as described in "Restoration procedures" on page 256.

Troubleshooting ESRSHTTPS

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

Concepts

ESRSHTTPS registers to receive HTTPS requests for particular URLs, receive HTTPS notifications, and send HTTPS responses. The ESRSHTTPS includes SSL support so applications can also exchange data over secure HTTPS connections without depending on IIS. It is also designed to work with I/O completion ports.

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

Configuring the ESRSHTTPS listener

You can use the executable to configure ESRSHTTPS listener in any of the following ways:

- Install and remove ESRSHTTPS listener Windows service without the need to use the Microsoft Installer tool **installutil.exe**.
- Start and stop the ESRSHTTPS listener.
- Automatically install the ESRSHTTPS listener common server certificate.
- Configure **esrshttps.exe** with IP address, port, rootdir, and scheme.

Virtual paths

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

- For files coming from the ConnectEMC service, the virtual path is `Gateway\work\httproot\incoming`
- For files coming from GWExt, the virtual path is `Gateway\work\dmb\request`

Files created

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

- **esrshttps.exe.config**
- **esrshttps.log**

ESRSHTTPS service command line examples

The following sections provide examples of using **esrshttps.exe** command line options to configure and control the ESRSHTTPS service.

Install the ESRSHTTPS service

```
esrshttps.exe -install
```

After running the command, **esrshttps.exe** displays the following text on the screen to confirm that the command completed without an error (error code 0):

```
Begin "esrshttps" Service Install.
esrshttps installed successfully.
End  "esrshttps" Service Install.
```

Remove the ESRSHTTPS service

```
esrshttps.exe -remove
```

After running the command, **esrshttps.exe** displays the following text on the screen to confirm the command completed without an error (error code 0):

```
Begin "esrshttps" Service Remove...
Current service  esrshttps status: Running
Try to stop service esrshttps
status: StopPending
status: Stopped
Service stopped  esrshttps status: Stopped
esrshttp removed successfully.
End "esrshttps" Service Remove.
```

Start the ESRSHTTPS service

```
esrshttps.exe -start
```

After running the command, **esrshttps.exe** displays the following text on the screen to confirm the command completed without an error (error code 0):

```
Begin "esrshttps" Service Install.
esrshttps installed successfully.
End  "esrshttps"  Service Install.
```

Stop the ESRSHTTPS service

```
esrshttps.exe -stop
```

After running the command, **esrshttps.exe** displays the following text on the screen to confirm the command completed without an error (error code 0):

```
Begin "esrshttps" Service Stop...
Current service  esrshttps status: Running
Try to stop service esrshttps
status: StopPending
status: Stopped
Service stopped  esrshttps status: Stopped
End "esrshttps" Service Stop.
```

ESRSHTTPS configuration command line examples

You may enter some or all of the following parameters in a single command line:

```
esrshttps.exe -ipaddress=HOST_IPADDRESS

ersrhttps.exe -port=PORT

ersrhttps.exe -rootdir=ROOT_DIR

ersrhttps.exe -scheme=[https|http]

ersrhttps.exe -config
```

ESRSHTTPS syntax

ESRSHTTPS uses the following syntax:

```
esrshttps.exe {-install | -remove | -stop | -start  |
-config} [-ipaddress=Ip] [-port=Port] [-rootdir=rootdir]
[-scheme-=scheme]
```

Parameters

Action commands are: **-install, -remove, -start, -stop, and -config**.

Action commands

-install

To install **esrshttps.exe** service manually

-remove

To uninstall **esrshttps.exe** service manually

-start

To start **esrshttps.ex**e service manually

-stop

To stop **esrshttps.exe** service manually

-config

To launch the **esrshttps.exe** graphical user interface for the configuration of **esrshttps.exe.config**

Setting commands are: **-ipaddress, -port, -rootdir, and -scheme**

Setting commands

esrshttps action=*parameter*

-ipaddress=*IP*

The **-ipaddress** action takes IP parameter as a string specifying the IP address to be added to the **esrshttps.exe.config** file.

-port=*Port*

The **-port** action takes port parameter as a string specifying the port number to be added to the **esrshttps.exe.config** file.

-rootdir=*rootdir*

The **-rootdir=** action takes rootdir parameter as a string specifying the rootdir to be added to the **esrshttps.exe.config** file. A root directory is the base directory to which the ESRSHTTPS listener is allowed access. The ESRSHTTPS listener will be allowed to create files from this directory.

[**-scheme**-=*scheme*]

The **-scheme** action takes scheme parameter as a string specifying the IP address to be added to the **esrshttps.exe.config** file. A URI Scheme is the top level of the Uniform Resource Identifier naming structure. All URIs are formed with a scheme name. The executable **esrshttps.exe** supports https and http schemes.

F

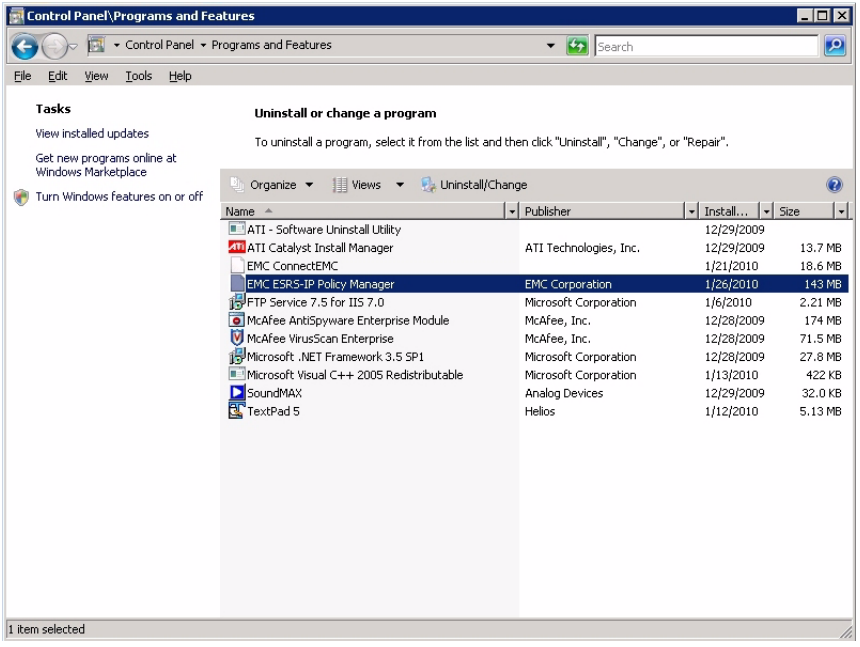
Uninstalling the Policy Manager Fully from a Windows 2008 Server

This appendix describes how to fully unistall the Policy Manager from a Windows 2008 Server.

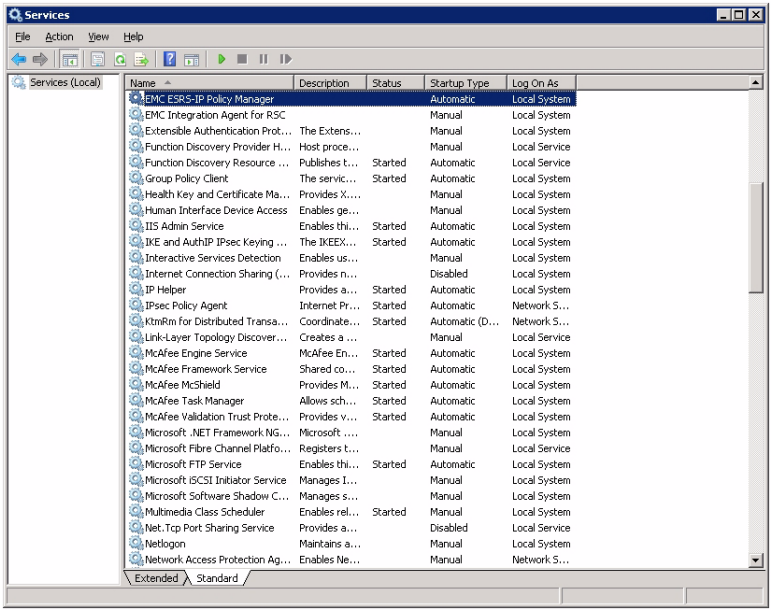
Uninstalling the Service from the Control Panel

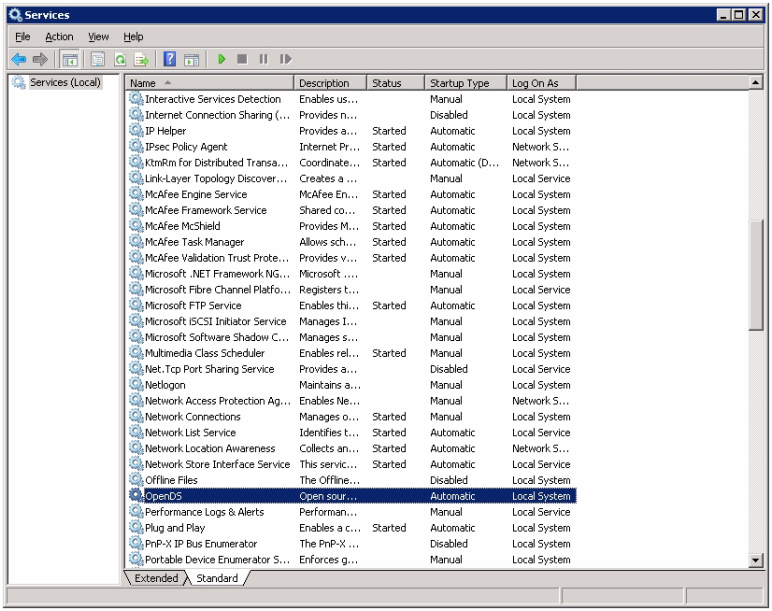
This section explains how to uninstall the Policy Manager through the Control Panel.

1. Go to the Control Panel\Programs and Features applet.



2. Select EMC SRS-IP Policy Manager, and click **Uninstall/Change** to complete the uninstall.
3. If you check the Services.msc you will see that the two services (EMC SRS-IP Policy Manager and OpenDS) are not removed.


Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
EMC ESRS-IP Policy Manager Automatic Local System
EMC Integration Agent for RSC Manual Local System
Extensible Authentication Prot... The Extens... Manual Local System
Function Discovery Provider H... Host proce... Manual Local Service
Function Discovery Resource ... Publishes t... Started Automatic Local Service
Group Policy Client The servic... Started Automatic Local System
Health Key and Certificate Ma... Provides X.... Manual Local System
Human Interface Device Access Enables ge... Manual Local System
IIS Admin Service Enables thi... Started Automatic Local System
IKE and AuthIP IPsec Keying ... The IKEEX... Started Automatic Local System
Interactive Services Detection Enables us... Manual Local System
Internet Connection Sharing (... Provides n... Disabled Local System
IP Helper Provides a... Started Automatic Local System
IPsec Policy Agent Internet Pr... Started Automatic Network S...
KtmRm for Distributed Transa... Coordinate... Started Automatic (D... Network S...
Link-Layer Topology Discover... Creates a ... Manual Local Service
McAfee Engine Service McAfee En... Started Automatic Local System
McAfee Framework Service Shared co... Started Automatic Local System
McAfee McShield Provides M... Started Automatic Local System
McAfee Task Manager Allows sch... Started Automatic Local System
McAfee Validation Trust Prote... Provides v... Started Automatic Local System
Microsoft .NET Framework NG... Microsoft .... Manual Local System
Microsoft Fibre Channel Platfo... Registers t... Manual Local Service
Microsoft FTP Service Enables thi... Started Automatic Local System
Microsoft iSCSI Initiator Service Manages I... Manual Local System
Microsoft Software Shadow C... Manages s... Manual Local System
Multimedia Class Scheduler Enables rel... Started Manual Local System
Net.Tcp Port Sharing Service Provides a... Disabled Local Service
Netlogon Maintains a... Manual Local System
Network Access Protection Ag... Enables Ne... Manual Network S...
Extended Standard


Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Interactive Services Detection Enables us... Manual Local System
Internet Connection Sharing (... Provides n... Disabled Local System
IP Helper Provides a... Started Automatic Local System
IPsec Policy Agent Internet Pr... Started Automatic Network S...
KtmRm for Distributed Transa... Coordinate... Started Automatic (D... Network S...
Link-Layer Topology Discover... Creates a ... Manual Local Service
McAfee Engine Service McAfee En... Started Automatic Local System
McAfee Framework Service Shared co... Started Automatic Local System
McAfee McShield Provides M... Started Automatic Local System
McAfee Task Manager Allows sch... Started Automatic Local System
McAfee Validation Trust Prote... Provides v... Started Automatic Local System
Microsoft .NET Framework NG... Microsoft .... Manual Local System
Microsoft Fibre Channel Platfo... Registers t... Manual Local Service
Microsoft FTP Service Enables thi... Started Automatic Local System
Microsoft iSCSI Initiator Service Manages I... Manual Local System
Microsoft Software Shadow C... Manages s... Manual Local System
Multimedia Class Scheduler Enables rel... Started Manual Local System
Net.Tcp Port Sharing Service Provides a... Disabled Local Service
Netlogon Maintains a... Manual Local System
Network Access Protection Ag... Enables Ne... Manual Network S...
Network Connections Manages o... Started Manual Local System
Network List Service Identifies t... Started Automatic Local Service
Network Location Awareness Collects an... Started Automatic Network S...
Network Store Interface Service This servic... Started Automatic Local Service
Offline Files The Offline... Disabled Local System
OpenDS Open sour... Automatic Local System
Performance Logs & Alerts Performan... Manual Local Service
Plug and Play Enables a c... Started Automatic Local System
PnP-X IP Bus Enumerator The PnP-X ... Disabled Local System
Portable Device Enumerator S... Enforces g... Manual Local System
Extended Standard

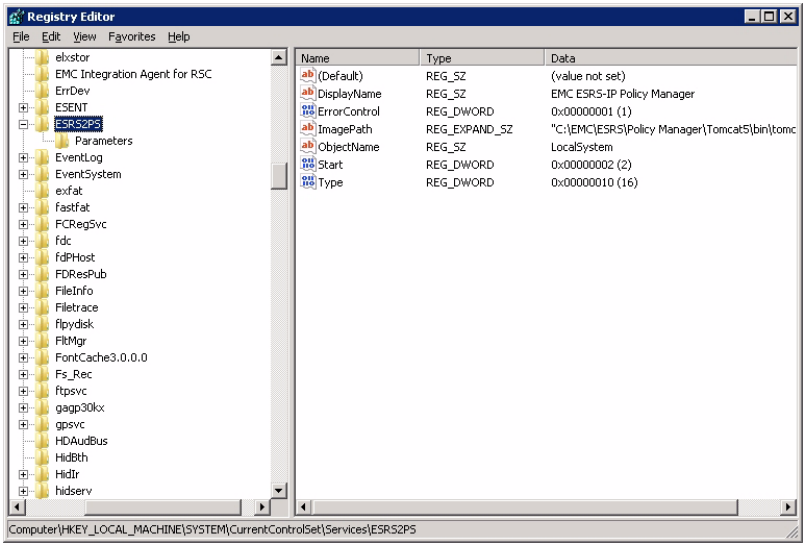
Editing the Registry to Remove the Services

After the uninstaller has completed, edit the Registry to remove the EMC SRS-IP Policy Manager service and OpenDS service.

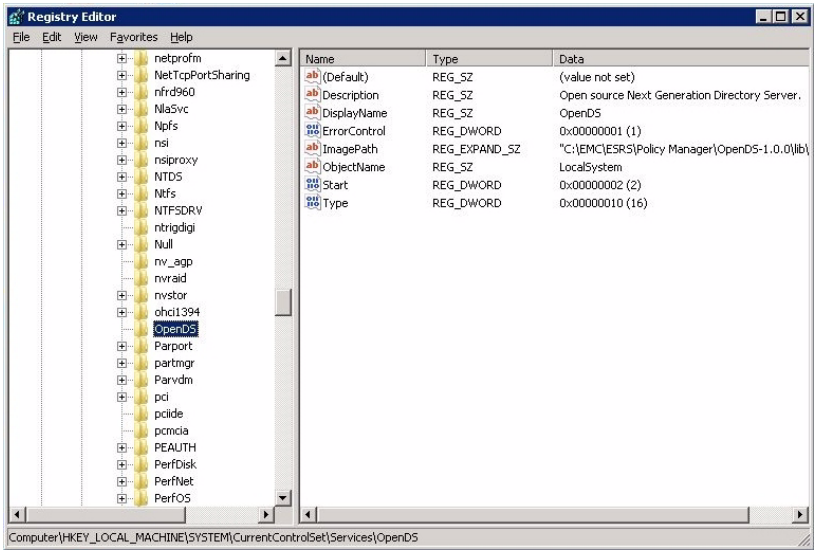
CAUTION

Exercise extreme caution when changing or deleting registry entries. A mistake can render you computer inoperative. Always back up the registry BEFORE editing.

1. From the Start menu, click **Run**.
2. Type regedit, and click **OK**.
3. In the registry editor, open HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Services -> ESRS2PS key.



4. Right click on the key, and click **Delete** to delete the entire key.
5. In the registry editor, open HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> Services -> OpenDS key.



6. Right click on the key, and click **Delete** to delete the entire key.
7. Reboot the server and log back in.
8. Using Windows Explorer, delete the entire <install_drive>:\EMC\ESRS\Policy Manager folder.
9. If you wish to maintain the Audit history, copy or move the <install_drive>:\EMC\ESRS\Policy Manager\Audit folder or its contents to another location.

Index

R

S

T

U

V

W