EMC® Secure Remote Support Gateway for Windows

Release 2.28

Operations Guide

REV 01

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

Published June, 2014

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

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

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

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

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

RSA is a registered trademark of RSA Security Inc.

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

Contents

Preface

Chapter 1 Introduction

Architecture 18
Customer site components 19
Communication to EMC 22
Responsibilities for the ESRS components 28
Customer 28
EMC Global Services 28
Configuration 29
Gateway Client server configuration 29
Configuration Tool... 33
Gateway Extract Utility 35
Digital Certificate Management 37
Device access control 38
Device configuration access control 38
EMC enterprise access control 39

Chapter 2 Gateway Client Server Preparation

Overview 42
Operating system configuration 42
Internet protocols (IPv4 and IPv6) 43
Microsoft .NET Framework 44
Internet Information Services (IIS) 45
IIS settings 46
Deploying IIS 6.0 in Windows 2003 48
Deploying IIS 7.0 in Windows 2008 R1 without IIS 7.5 FTP Add-in

61
Before starting the IIS 7.0 deployment 61
Temporarily reconfiguring the password policies............... 61
Creating the IIS user accounts and passwords..................... 64
Restoring the password policies.. 68
Installing IIS and the FTP service with IIS 6.0 Compatibility
Windows 2008 R1 without IIS 7.5 FTP add-in...................... 71
Installing the SMTP service.. 78
Configuring the SMTP server 85
Configuring the FTP server... 90
Restarting the FTP and SMTP services............................... 103
Creating required folders 104
Starting the FTP and SMTP services................................... 104
Enabling the Write permission for the FTP service 106
Configuring the Windows 2008 firewall settings...................... 110
Testing the Windows 2008 firewall 114
Testing FTP server functionality.. 114
Testing SMTP from another host... 116
How to configure OS (IIS, FTP and SMTP, and Windows Firewall
with Advanced Security) on Windows 2008 R2........................ 119
Create Users.. 119
Install IIS and FTP and add the SMTP Feature 128
FTP Configuration (IIS 7.5) for Windows 2008 R2............. 136
Create Directory Structure.. 143
Configure SMTP 156

Chapter 3 Configuration Tool

Configuration Tool overview 162
Installing and using the Configuration Tool............................. 163
Installing the Configuration Tool 163
If you are running Windows 2008.. 163
Using the Configuration Tool 166
Managing devices.. 168
Communicating through a proxy server............................ 175
Linking a Gateway Client to a Policy Manager 176
Disabling communication 179
Displaying the status of Services... 179
Displaying active remote sessions 180
Displaying the Configuration Tool log files 181
Uninstalling the Configuration Tool 182

Chapter 4 Server Maintenance

Power sequences 184
Time Zone settings 185
Service preparation for Gateway Client..................................... 186
Gateway Client server 186
Backup guidelines and procedures 188
Server image backup 188
Restoration procedures... 189
Server image backup restoration 189
Installation restoration 189

Appendix A Uninstalling Gateway Client 2.16 using Provisioning Tool 2.14

Uninstalling Gateway Client 2.16 using Provisioning Tool 2.14 192

Appendix B Patch installation

Patch installation instructions 194
Field Instructions.. 194
Process 197
Gateway Client Uninstallation... 208
2.16.00.06 and Above Uninstall Process............................... 208

Appendix C Troubleshooting

Troubleshooting unexpected service events............................... 214
Service malfunction 214
Service does not start up 214
Operating system or hardware failures 214
Troubleshooting ESRSHTTPS.. 215
Concepts 215
ESRSHTTPS service command line examples 216
ESRSHTTPS configuration command line examples 217

Index

Figures

Title Page

1 ESRS architecture 18
2 Heartbeat communication.... 23
3 Remote notification communication 24
4 Remote access communication.... 25
5 Windows Component Wizard 49
6 Files Needed dialog box 49
7 Messages tab 53
8 Drop directory 54
9 Command prompt.... 55
10 Default SMTP properties.... 56
11 Default SMTP message tab 56
12 E-mail server specification 57
13 Mail drop specification.... 58
14 E-mail server test 59
15 Sample e-mail.... 60
16 Local security policy 62
17 Complexity requirements 63
18 Disable the complexity requirements.... 63
19 Computer—Manage 64
20 Menu—Users 65
21 New User 65
22 Clear the checkbox 67
23 Select the checkboxes 68
24 Local security policy 69
25 Complexity requirements 70
26 Enable Local Security setting.... 70
27 Add Roles 72
28 Select Server Roles—Web Server (IIS).... 73
29 Add features.... 73
30 Web Server (IIS).... 74

31 Web Server (IIS) introduction 75
32 Select Role Services 76
33 Confirm Installation Selections 77
34 Installation Results 78
35 Server Manager 79
36 Select Features 80
37 Add Features Wizard 80
38 Select Features—checked 81
39 Confirm Installation Selections 82
40 Installation Progress 83
41 Installation Results 84
42 Server Manager status 85
43 IIS 6.0 Manager 86
44 Rename the folder 87
45 ESRS Gateway SMTP Server Properties 88
46 Rename the default domain 89
47 Drop directory example 90
48 Administrative Tools menu 91
49 FTP Site 92
50 Welcome screen 93
51 FTP Site Description 94
52 IP Address and Port Settings 95
53 FTP User Isolation 96
54 FTP Site Home Directory 96
55 FTP Site Access Permissions 97
56 FTP Server menu 98
57 FTP Site tab 99
58 Clear the Allow anonymous connections checkbox 100
59 Authentication option continue 100
60 FTP Server Properties—Home Directory 101
61 FTP Site messages example 102
62 FTP and SMTP services 103
63 Internet services restart 104
64 Starting the service from IIS 6.0 Manager 105
65 Starting the service from Services 106
66 Navigate to LocalUser Properties 107
67 Edit Users 108
68 Allow Write 109
69 Windows Firewall—Change settings 110
70 Add port 111
71 Name and Port number example 112
72 Inbound ESRS ports example 113
73 E-mail server test 117

74 E-mail server test 118
75 Client is not running 164
76 Configuration Tool properties 165
77 Run this program as an administrator 166
78 Configuration Tool screen header 167
79 Status tab 167
80 Managed Devices tab 169
81 Add New Device window 170
82 History 174
83 Proxy Servers tab 175
84 Policy Manager tab 177
85 Services tab 179
86 Remote Sessions tab 180
87 Logs tab 181
88 Event Viewer System and Security Log settings 187
89 Configuration Tool 197
90 Creating a Directory 198
91 Extracting the patch.zip 199
92 Extracting Upgrade Files 199
93 Files Successfully Unzipped 200
94 Files Extracted 201
95 Command Prompt 201
96 Command Prompt: Enter Executable 202
97 Command Prompt: Answer Y to Proceed 203
98 Connectivity Status 203
99 Managed Devices 204
100 Services Running 205
101 Review Logs 206

Tables

	Title	Page
1	Specifications for ESRS Gateway Client server	21
2	Product use of ESRS	25
3	Products supported by the Gateway Extract Utility (GWExt)	36
4	Gateway Client server standard configuration requirements	46
5	Valid Suffixes and Code Versions	170
6	Error Codes and where in the process they may occur	207

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 documentation set and is intended for use by device administrators.

Related documentation

Related documents include:

- *EMC Secure Remote Support Release Notes*
- *EMC Secure Remote Support Release Technical Description*
- *EMC Secure Remote Support Release Pre-Site Checklist*
- *EMC Secure Remote Support Release Site Planning Guide*
- *EMC Secure Remote Support Port Requirements*
- *EMC Secure Remote Support Customer Environment Check Tool for Windows Operations Guide*
- *EMC Secure Remote Support Gateway for Linux Operations Guide*
- *EMC Secure Remote Support Customer Environment Check Tool for Linux Operations Guide*
- *EMC Secure Remote Support Policy Manager Release 6.6 Operations Guide*

Conventions used in this guide

EMC uses the following conventions for notes and cautions.

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

CAUTION

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

EMC uses the following type style conventions in this guide:

Normal	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 Online Support Site (support.emc.com) (registration required) at:

```
http://support.emc.com
```

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

Your comments

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

```
techpubcomments@EMC.com
```

1

Introduction

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

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

- Architecture.. 18
- Responsibilities for the ESRS components 28
- Configuration 29

Architecture

The EMC® Secure Remote Support (ESRS) application architecture consists of a secure, asynchronous messaging system designed to support the functions of secure encrypted file transfer, monitoring of device status, and remote execution of diagnostic activities. This distributed solution is designed to provide a scalable, fault-tolerant, and minimally intrusive extension to the customer's system support environment. Figure 1 on page 18 illustrates the major processing components and their interconnections.

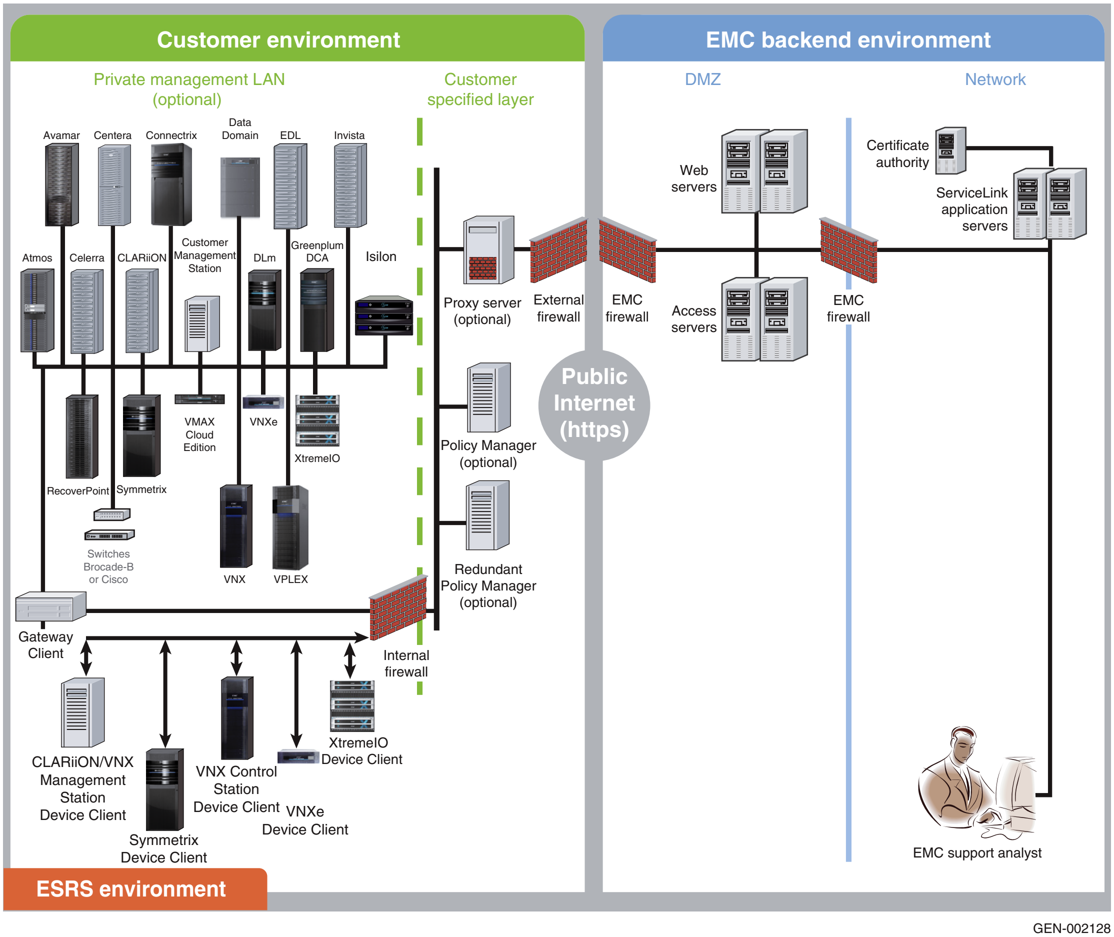


Figure 1 ESRS architecture

Customer site components

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

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

Gateway Clients

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

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

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

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

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

Table 1 on page 21 shows the minimum configuration of the required hardware and the application software.

Policy Manager

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

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

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

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

Proxy server

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

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

Table 1 on page 21 shows the minimum configuration of the required Gateway Client hardware and the application software.

Table 1 Specifications for ESRS Gateway Client server

Type	Requirements	EMC provided software	Notes
Gateway Client server	**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 recommended 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 (minimum) or Microsoft .NET Framework 3.5 is required. NOTE: Microsoft.NET Framework 4.0 is not compatible at this time. **Microsoft Visual C++ 2005 SP1 Runtime Library** **Operating System** — US English only supported, as follows: • Windows Server 2003 R1, 32-bit or 64-bit, SP1, SP2 or SP3 • Windows Server 2003 R2, 32-bit or 64-bit, SP1, SP2 or SP3 • Windows Server 2008 R1, 6.0, 32-bit or 64-bit, IIS 7.0, SP1 or SP2 (IIS 6 Compatibility) • Windows Server 2008 R1, 6.0, 32-bit or 64-bit, IIS 7.0, SP1 or SP2 w/ IIS 7.5 FTP Add-in • Windows Server 2008 Enterprise R1, 6.0, 32-bit or 64-bit, IIS 7.0, SP1 or SP2 (IIS 6 Compatibility) • Windows Server 2008 Datacenter R1, 6.0, 32-bit or 64-bit, IIS 7.0, SP1 or SP2 (IIS 6 Compatibility) • Windows Server 2008 R2, 6.1, 64-bit only, IIS 7.0/7.5, SP1 or SP2 • Windows Server 2008 R2 Enterprise 64-bit IIS 7.0/7.5, SP1 or SP2 • Windows Server 2008 R2 Datacenter 64-bit IIS 7.0/7.5, SP1 or SP2 • Windows Server 2012 R1 Foundation 64-bit IIS 8.0 • Windows Server 2012 R1 Standard 64-bit IIS 8.0 • Supported French OS (Windows 2008 R1 and R2), IIS requirements as above, with English language pack • Supported Japanese OS (Windows 2008 R1 and R2), IIS requirements as above, with English language pack • Hyper-V and VMware ESX 2.5.x or above running the following operating systems: – Windows Server 2008 Standard 32-bit – Windows Server 2008 Enterprise 32-bit – Windows Server 2008 Datacenter 32-bit – Windows Server 2008 R2 Standard 64-bit – Windows Server 2008 R2 Enterprise 64-bit – Windows Server 2008 R2 Datacenter 64-bit	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. **Note:** Support for ESRS Gateway on Windows 2003 will be deprecated in the near future. **Note:** Windows Server 2012 must be GUI mode to install the ESRS Gateway.

Communication to EMC

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

IMPORTANT

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

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

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

- Heartbeat polling
- Remote notification
- Remote access

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

Heartbeat polling

Heartbeat polling is described in the following sections:

- “To EMC by the Gateway Client” on page 22
- “To EMC devices managed by the Gateway Client” on page 23

To EMC by the Gateway Client

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

EMC servers receive the data in XML format and acknowledge the receipt of data using SOAP (Simple Object Access Protocol) commands. Once this response is received, the Gateway Client terminates the connection. Figure 2 on page 23 provides an illustration of the heartbeat communication paths.

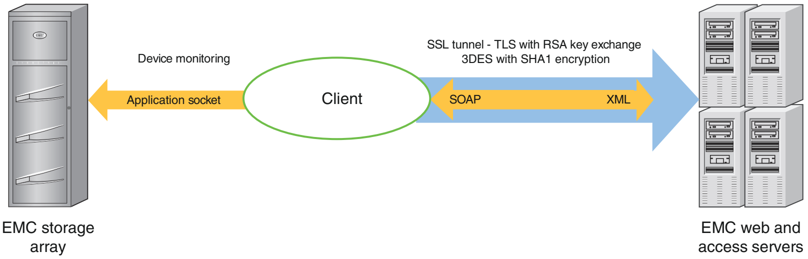

Device monitoring
Application socket
Client
SSL tunnel - TLS with RSA key exchange
3DES with SHA1 encryption
SOAP
XML
EMC storage array
EMC web and access servers

Figure 2 **Heartbeat communication**

To EMC devices managed by the Gateway Client

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

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

Remote notification (Connect Home)

The Gateway Clients also serve as a conduits for EMC products to send remote notification event files to EMC. EMC hardware platforms use remote notification for several different purposes. Errors, warning conditions, health reports, configuration data, and script execution statuses may be sent to EMC. Figure 3 on page 24 provides an illustration of the remote notification communication paths.

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

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

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

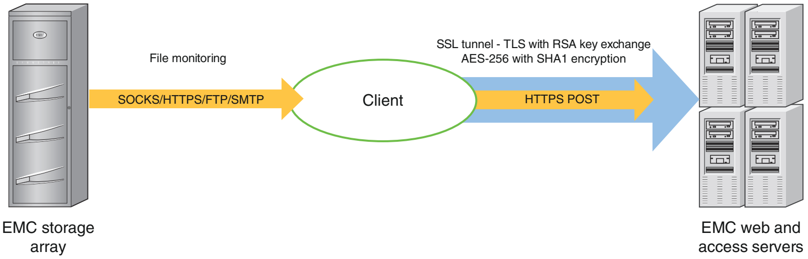

File monitoring
SOCKS/HTTPS/FTP/SMTP
Client
SSL tunnel - TLS with RSA key exchange
AES-256 with SHA1 encryption
HTTPS POST
EMC storage array
EMC web and access servers

Figure 3 **Remote notification communication**

Remote access

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

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

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

This secure session allows IP traffic from the EMC internal service person to be routed through the Gateway Client to the end device. IP socket traffic received by the Global Access Server for the session is established, wrapped in a SOAP message, and sent to the Gateway Client over the persisted SSL tunnel. The Gateway Client unwraps the SOAP object and forwards the traffic to the IP address and port of the end device for which the session was established. SOAP communication flows between the Gateway Client and the Global Access Server through this tunnel until it is terminated or times out after a period of inactivity. Figure 4 on page 25 provides an illustration of the remote access communication paths.

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

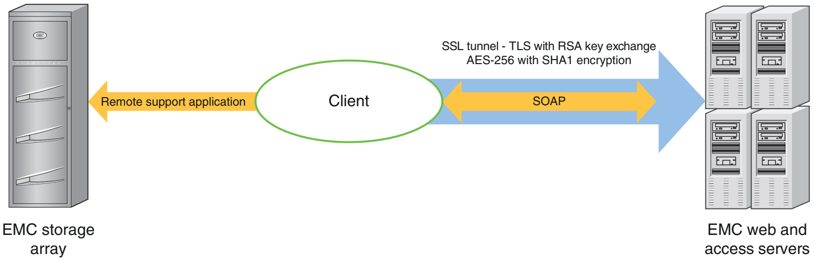

SSL tunnel - TLS with RSA key exchange
AES-256 with SHA1 encryption
Remote support application
Client
SOAP
EMC storage array
EMC web and access servers

Figure 4 **Remote access communication**

Table 2 on page 25 shows which EMC products use the remote notification and remote access features of ESRS.

Table 2 **Product use of ESRS (page 1 of 3)**

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

Table 2 Product use of ESRS (page 2 of 3)

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

Table 2 Product use of ESRS (page 3 of 3)

Product	Remote notification to EMC via ESRS	EMC remote access to device via ESRS
EMC VPLEX®	Yes	Yes
EMC XtremIO	Yes	Yes

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

b. Via CiscoFabric Manager or Cisco Data Center Network Manager

Responsibilities for the ESRS components

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

Customer

You are responsible for the following:

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

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

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

Note: Policy Manager software is customer installable.

EMC Global Services

EMC Global Services personnel are responsible for the following:

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

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

- Updating the Gateway Client and Policy Manager software

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

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

Configuration

This section provides details on the configuration of ESRS.

Gateway Client server configuration

A Gateway Client server can be implemented in one of several configurations to meet your network and security requirements. See Figure 1 on page 18 for a sample configuration.

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

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

Hyper-V/VMware support

ESRS is qualified to run on a Hyper-V/VMware virtual machine. VMware support allows customers to leverage their existing Hyper-V/VMware infrastructure to benefit from the security features of ESRS 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 Hyper-V/VMware support:

- VMware ESX 2.5.2 or later
- 15 GB partition
- 2.2 GHz virtual CPU
- 1 GB memory allocated minimum 2 GB preferred
- SMB modules optional
- VMotion functionality optional (not supported for the Gateway Client)
- Operating Systems are the same as for physical hardware

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.

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

Gateway Clients in the cluster. There is no direct communication between the Gateway Clients within the cluster.

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

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

Synchronization of Gateway Client clusters

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

Installing a High Availability Gateway Cluster

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

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

Note: The Cluster name is limited to 64 characters.

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

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

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

Configuration Tool

The Configuration Tool is an ESRS Client-based graphical user interface (GUI) application that is automatically installed upon successful completion of your Gateway Client installation. It is typically located at Start > Programs > ESRS > Config Tool.

The Configuration Tool is used to perform the following tasks:

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

Note: The term *manage* means that a device is monitored and can use the Gateway Client to establish remote access connections. The Gateway Client proxies all Configuration 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 should 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 Gateway 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 Gateway Client and the EMC enterprise.
- Policy Manager tab — Allows enabling or disabling communication between a Policy Manager and an Gateway Client and configuring Proxy Server for communication to the Policy Manager.

- Services tab — Displays the state (running, stopped, or disabled) and the startup type (automatic or manual) of the following services related to ESRS 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 Gateway Client activity.

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

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

Device management

The Configuration 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 Gateway Client. If Network Address Translation (NAT) is being used in the environment, the IP address used to deploy the device must be the NAT IP address, not the device's IP address. Let us say, for example, that the local IP address of a device is 192.168.0.100, and is only on your internal network. You are using NAT (or a NAT device) that maps the device IP (192.168.0.100) to IP 10.10.44.22 so that the device can be reached from within your DMZ. In this case, EMC must use the NAT IP address of 10.10.44.22 to reach the device, and in the Configuration 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 un-manage 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 Gateway Client.

Gateway Extract Utility

To configure a device for management by a Gateway Client, the EMC Global Services professional on site must know the following for each managed device: serial number, product type, and an IP address that the Gateway Client can use to communicate with the device. The Gateway Extract utility (GWExt), when run on the EMC device, can be used to automate the collection of this information and transport it to the Gateway Client. EMC supplies the GWExt utility with the Gateway Client installer. For a list of the products that the GWExt utility supports, see Table 3 on page 36.

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

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

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

Table 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	
Isilon	OneFS 7.1	
Symmetrix	Win32	
ViPR	LINUX openSUSE11.0	
VMAX Cloud Edition (CE)	Win 32	
VNX - Block	Win32	
VNX - File	Linux	NAS Code 7.x

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

Product supported by GWExt	Operating system	Additional notes
VNXe	SUSE Linux 11 64-bit	
VPLEX	SUSE Linux 10.2 32-bit	
XtremIO	CentOS 6.2 64-bit	

Digital Certificate Management

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

Digital Certificate Management automates Gateway Client digital certificate enrollment by taking advantage of EMC's existing network authentication systems, which use the RSA SecurID Authenticator and the EMC local certificate authority (CA). Working with EMC systems and data sources, Digital Certificate Management aids in programmatically generating and authenticating each certificate request, as well as issuing and installing each certificate on the Gateway Client.

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

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

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

The installation program then submits the request. After the certificate is issued, the installation program automatically completes the certificate installation on the Gateway Client.

IMPORTANT

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

Device access control

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

Device configuration access control

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

EMC enterprise access control

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

2

Gateway Client Server Preparation

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

- Overview 42
- Microsoft .NET Framework 44
- Internet Information Services (IIS) 45
- Deploying IIS 6.0 in Windows 2003.. 48
- Deploying IIS 7.0 in Windows 2008 R1 without IIS 7.5 FTP Add-in 61
- Configuring the Windows 2008 firewall settings 110
- Testing the Windows 2008 firewall.. 114
- How to configure OS (IIS, FTP and SMTP, and Windows Firewall with Advanced Security) on Windows 2008 R2 119

Overview

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

As part of the preparation, the following software applications are required. Additional requirements are described in "Operating system configuration" on page 42:

- **Microsoft Internet Information Services (IIS) —** The ESRS 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 21.
   - 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.
   - Harden server as required by your corporate standards.

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 with SP1 (minimum) or Microsoft .NET Framework 3.5. Instructions are included in "Microsoft .NET Framework" on page 44.

Note: Microsoft .NET Framework 2.0 is installed by default as part of Windows 2008 Operating System. Microsoft .NET4.0 is incompatible with the proper operation of Gateway Client and associated support applications. Microsoft Automatic Updates to .NET 4.0 may result in the Client and/or 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 45.

Note: This is the initial configuration of IIS and may require manual reconfiguration post Gateway Client installation.

4. Install the Microsoft Visual C++ 2005 SP1 Runtime Library.

Note: Microsoft Visual C++ 2005 SP1 Runtime Library is automatically on Windows 2008, any version.

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 (minimum) or Microsoft .NET Framework 3.5 is required for the 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)
- Microsoft .NET Framework 3.5

Note: Microsoft .NET Framework 2.0 is installed by default as part of Windows 2008 Operating System. Microsoft .NET Framework 4.0 is incompatible with the proper operation of Gateway Client and associated support applications. Microsoft Automatic Updates to .NET 4.0 may result in the Client and/or 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 46.
- Instructions for deploying IIS are provided in "Deploying IIS 6.0 in Windows 2003" on page 48.

IIS settings

Before installing the ESRS Gateway Client software, you must configure its server operating system with the IIS settings shown in Table 4 on page 46.

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).ESRS **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	C:\Inetpub\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	C:\Inetpub\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)

Table 4 Gateway Client server standard configuration requirements

Category	Variable	Value
	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 Gateway Client is installed per CSP2100* IIS MUST be reconfigured to point to <install_drive>:\EMC\ESRS\Gateway\work\ftproot\

c. Important: AFTER the Gateway 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
For customer environments that do NOT permit the use of FTP, the FTP service, Directories, or Users are not require to permit installation of the ESRS Gateway Client.

d. The Gateway Client does NOT support the use of Domain credentials for ftp users.

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 R1 without IIS 7.5 FTP Add-in" on page 61.)

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

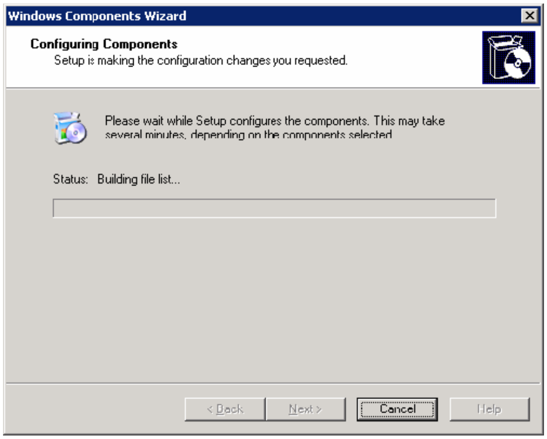
Installing and configuring IIS 6.0 in Windows 2003 SP1 (for IPV4 support)

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 49 appears.



Windows Components Wizard

Configuring Components

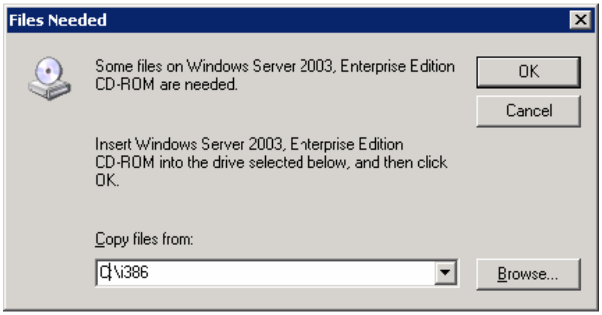
Setup is making the configuration changes you requested.

Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Building file list...

Figure 5 Windows Component Wizard

9. If you receive a **Files Needed** prompt as shown in Figure 6 on page 49, insert the required CD-ROM. Provide the path to the Windows Installation CD-ROM I386 directory or wherever your CD-ROM i386 is located.



Files Needed

Some files on Windows Server 2003, Enterprise Edition CD-ROM are needed.

Insert Windows Server 2003, Enterprise Edition CD-ROM into the drive selected below, and then click OK.

Copy files from: C:\i386

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 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 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 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

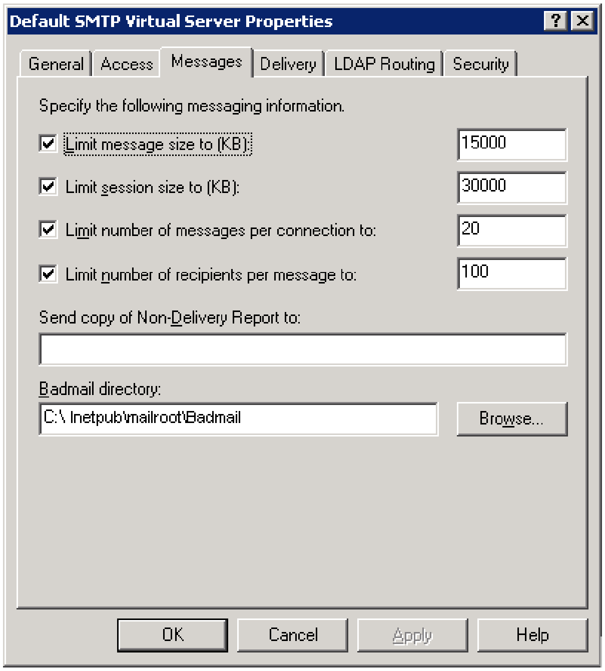
After completing your ESRS Gateway Client installation, change the path to the following:
`<install drive>:\EMC\ESRS\Gateway\work\mailroot\Badmail`

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 53.



Default SMTP Virtual Server Properties

Specify the following messaging information.

☑ Limit message size to (KB): 15000

☑ Limit session size to (KB): 30000

☑ Limit number of messages per connection to: 20

☑ Limit number of recipients per message to: 100

Send copy of Non-Delivery Report to:

Badmail directory: C:\ Inetpub\mailroot\Badmail

Figure 7 Messages tab

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

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

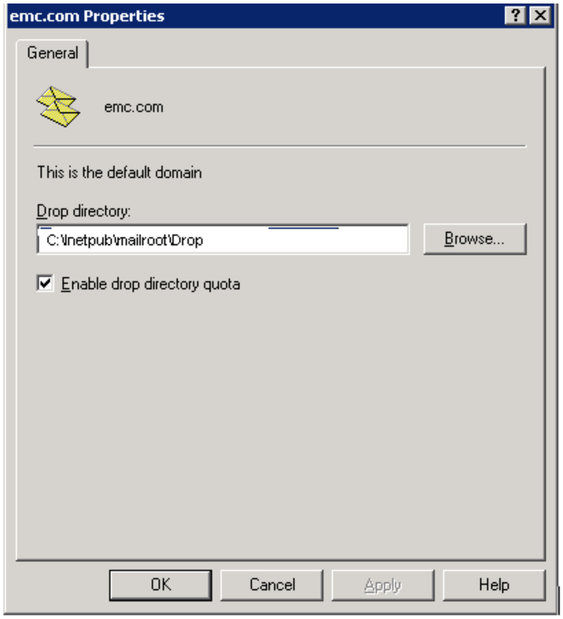
IMPORTANT

After completing your ESRS 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 54.



emc.com Properties

emc.com

This is the default domain

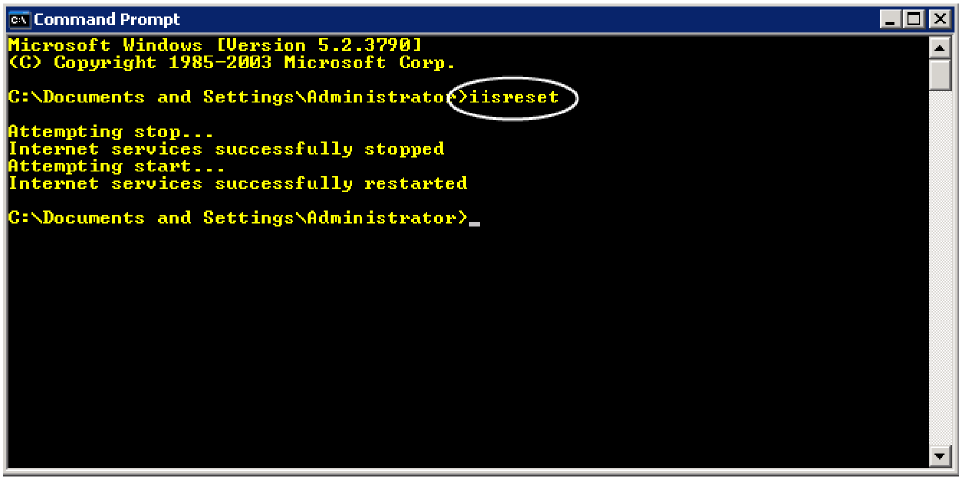
Drop directory: C:\Inetpub\mailroot\Drop

☑ Enable drop directory quota

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 55.



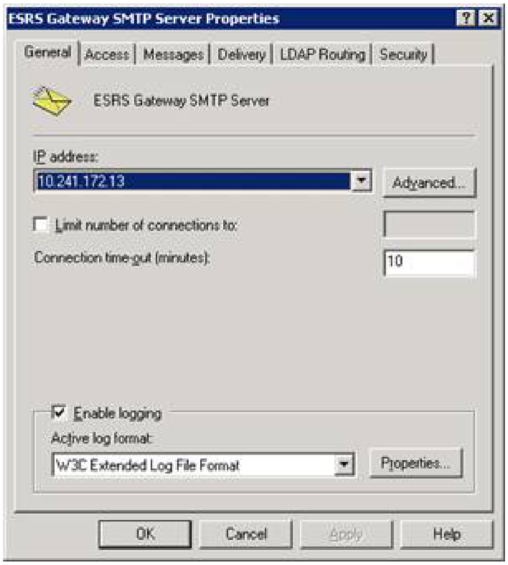
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>iisreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

C:\Documents and Settings\Administrator>_
```

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 56.



ESRS Gateway SMTP Server

IP address: 10.241.172.13

□ Limit number of connections to:

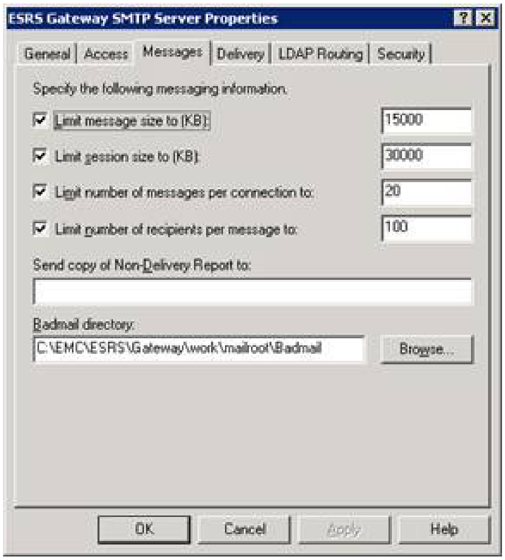
Connection time-out (minutes): 10

☑ Enable logging

Active log format: W3C Extended Log File Format

Figure 10 **Default SMTP properties**

2. Click **Messages** as shown in Figure 11 on page 56.



Specify the following messaging information.

☑ Limit message size to (KB): 15000

☑ Limit session size to (KB): 30000

☑ Limit number of messages per connection to: 20

☑ Limit number of recipients per message to: 100

Send copy of Non-Delivery Report to:

Badmail directory: C:\EMC\ESRS\Gateway\work\mailroot\Badmail

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 57.

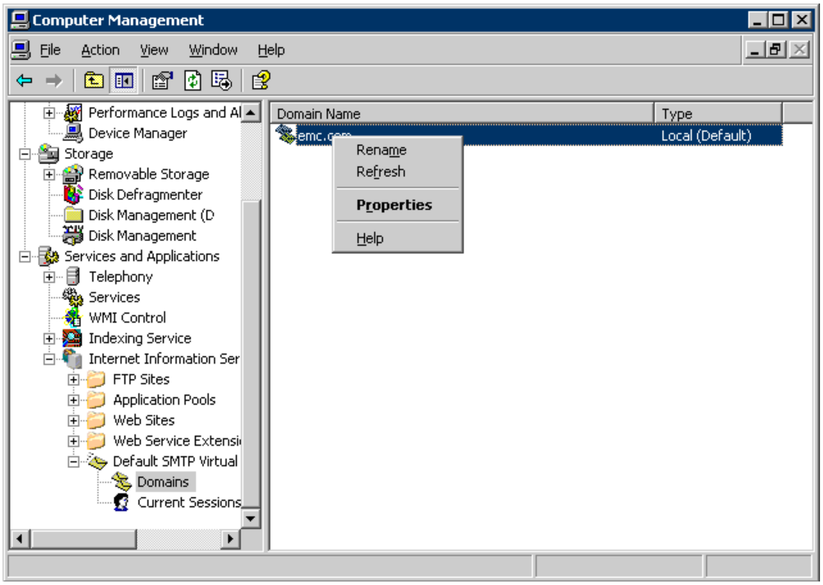
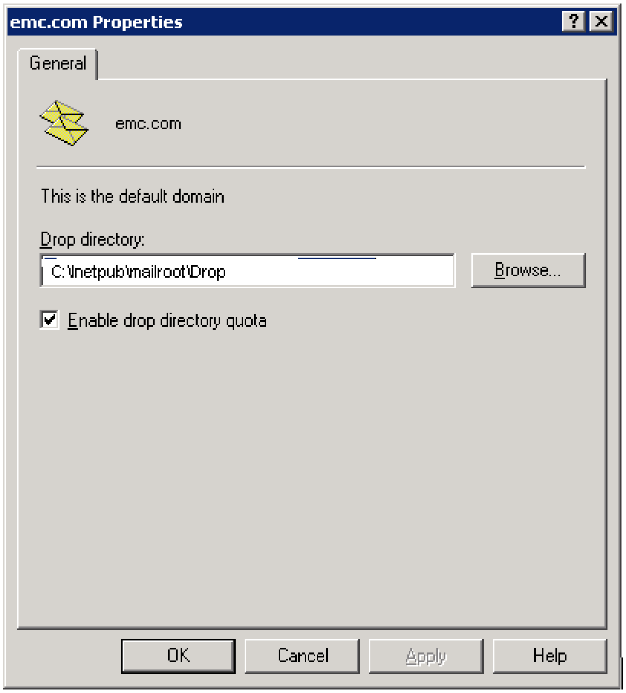


Figure 12 E-mail server specification

8. Point to the maildrop directory on the installation drive as shown in Figure 13 on page 58.



emc.com Properties

emc.com

This is the default domain

Drop directory: C:\Inetpub\mailroot\Drop

☑ Enable drop directory quota

Figure 13 Mail drop specification

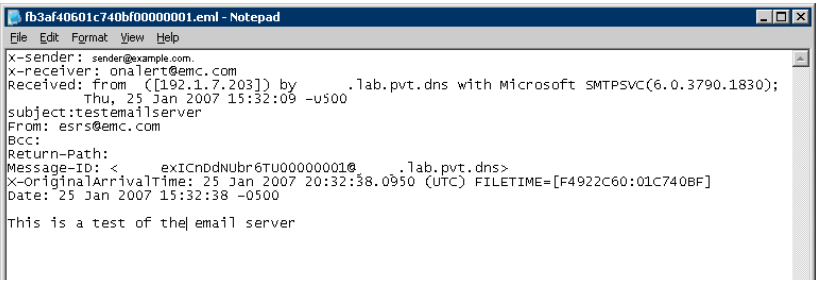
9. Test the mail server and verify that mail is in the proper directory, as shown in Figure 14 on page 59.

```
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 60.



```
x-sender: sender@example.com.
x-receiver: onalert@emc.com
Received: from  ([192.1.7.203]) by      .lab.pvt.dns with Microsoft SMTPSVC(6.0.3790.1830);
         Thu, 25 Jan 2007 15:32:09 -u500
subject:testemailserver
From: esrs@emc.com
Bcc:
Return-Path:
Message-ID: <     exICnDdNUbr6TU00000001@     .lab.pvt.dns>
X-OriginalArrivalTime: 25 Jan 2007 20:32:38.0950 (UTC) FILETIME=[F4922C60:01C740BF]
Date: 25 Jan 2007 15:32:38 -0500

This is a test of the email server
```

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 Gateway 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 that 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 R1 without IIS 7.5 FTP Add-in

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 48.)

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

Before starting the IIS 7.0 deployment

Before you install IIS:

- Install Windows 2008.

  Note: The current ESRS configuration supports Windows 2008 in a workgroup configuration. Ensure that Windows patches are up to date.

- 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 ESRS.

The next step is to reconfigure the password policies.

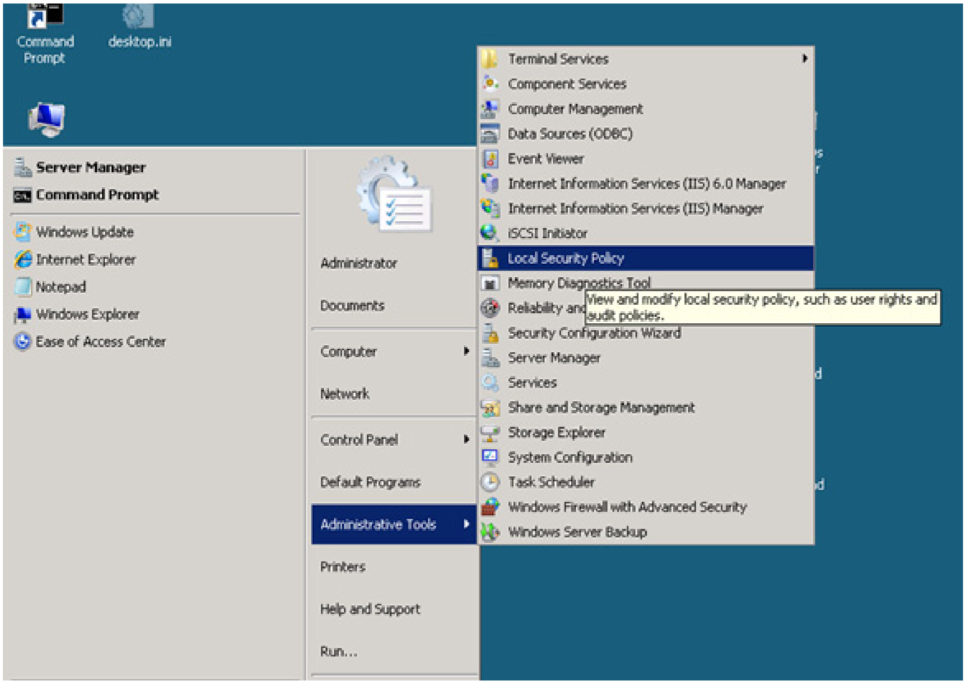
Temporarily reconfiguring the password policies

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.

Note: If the server is a member of a Windows Domain, Domain Policies may prohibit changing the Local Password Policies.

To reconfigure the password policies:

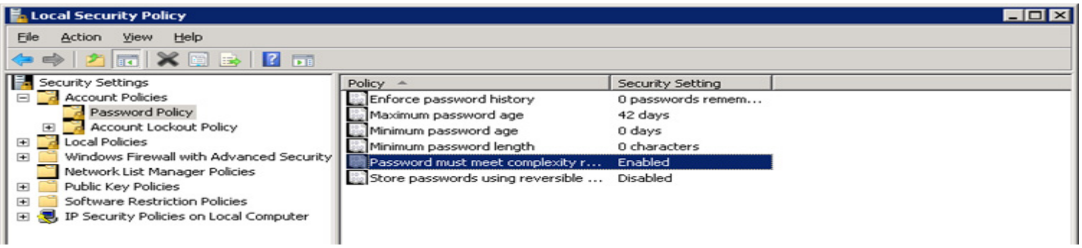
1. From the Windows 2008 **Start** menu, click **Administrative Tools**. The **Administrative Tools** menu appears, as shown in Figure 16 on page 62.



View and modify local security policy, such as user rights and audit policies.

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.

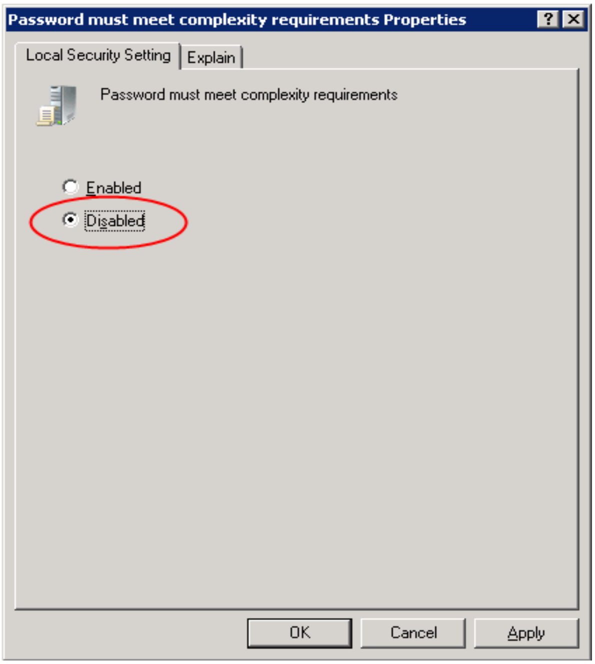


Security Settings
- Account Policies
  - Password Policy
  - Account Lockout Policy
- Local Policies
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- IP Security Policies on Local Computer

Policy	Security Setting
Enforce password history	0 passwords remem...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity r...	Enabled
Store passwords using reversible ...	Disabled

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 63.



Password must meet complexity requirements

○ Enabled

● Disabled

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 68.

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 64. The **Server Manager** window appears.

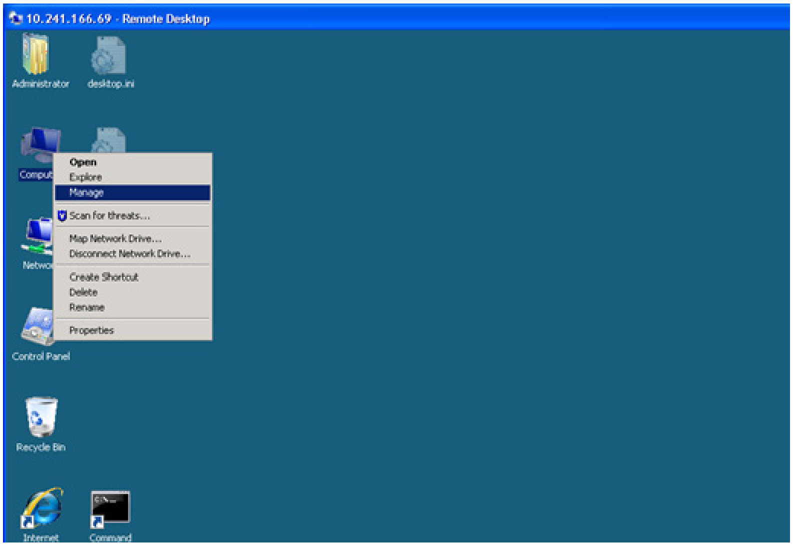
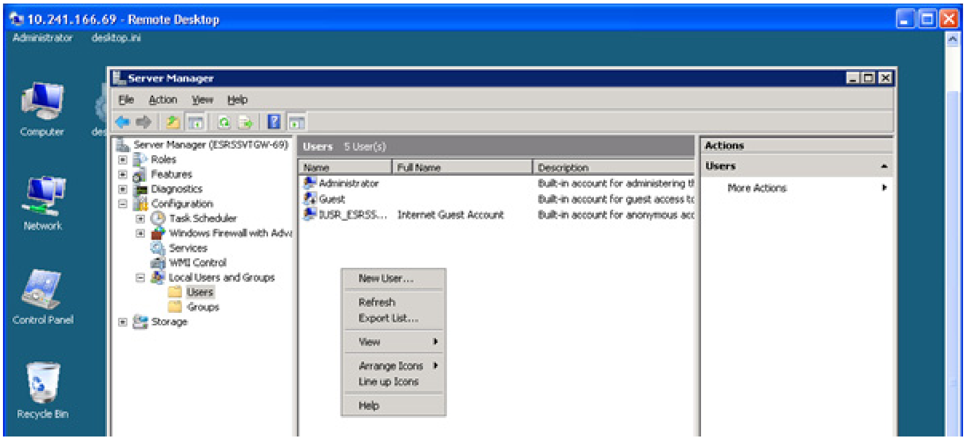


Figure 19 Computer—Manage

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.

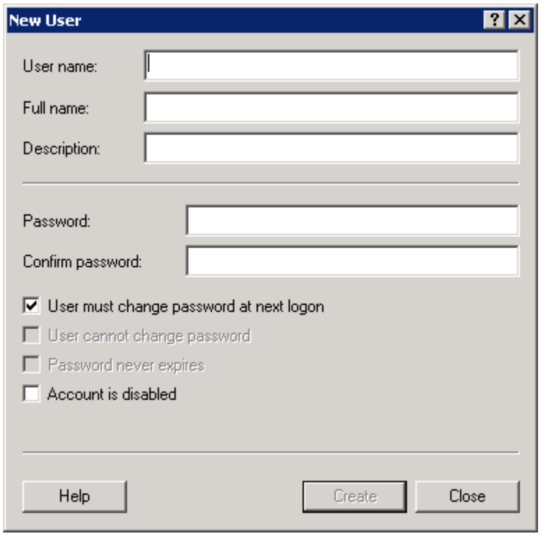
5. Right-click **Users**. A menu appears, as shown in Figure 20 on page 65.



Name	Full Name	Description
Administrator		Built-in account for administering th
Guest		Built-in account for guest access tc
IUSR_ESRSS...	Internet Guest Account	Built-in account for anonymous acc

Figure 20 Menu—Users

6. Click **New User**. The **New User** window appears, as shown in Figure 21 on page 65.



User name:

Full name:

Description:

Password:

Confirm password:

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

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**.

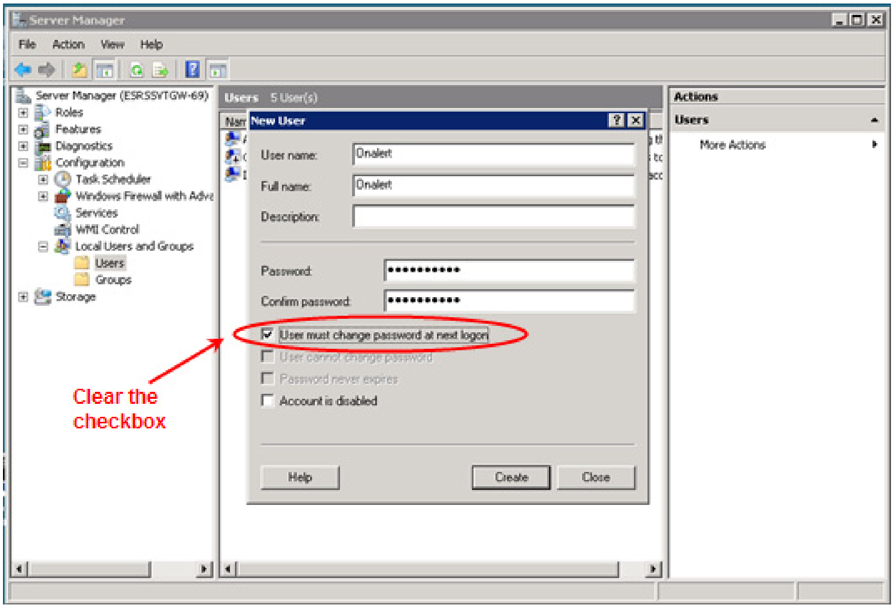
   - The **Full name** can be the same as the **User Name**.

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 46.

4. When you have entered the passwords, clear **User must change password at next logon**, as shown in Figure 22 on page 67.



User name: Onalert

Full name: Onalert

Description:

Password: •••••••••••

Confirm password: •••••••••••

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

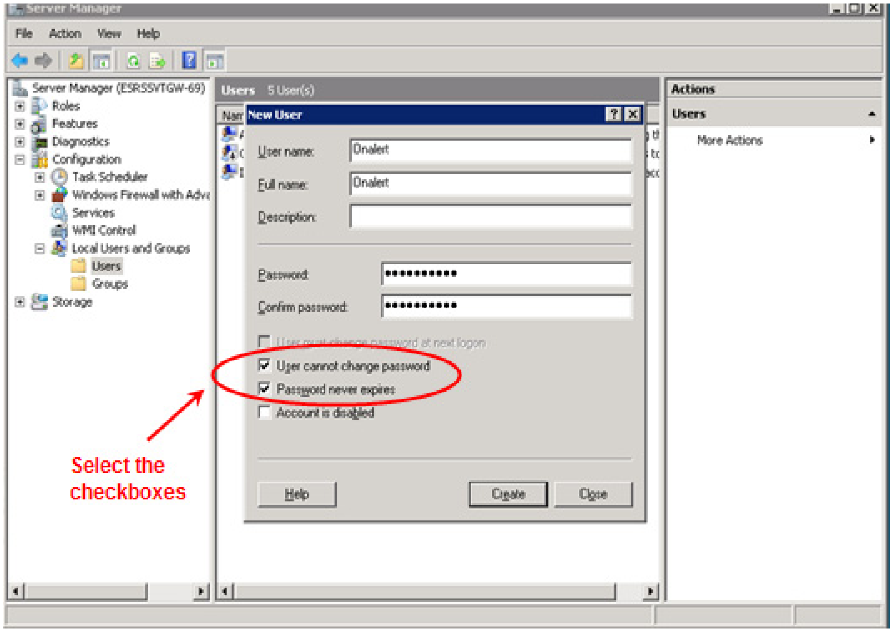
□ Account is disabled

Clear the checkbox

Figure 22 **Clear the checkbox**

5. Select the following checkboxes, as shown in Figure 23 on page 68:

   - **User cannot change password**
   - **Password never expires**



User name: Onalert

Full name: Onalert

Description:

Password: •••••••••••

Confirm password: •••••••••••

☐ User must change password at next logon

☑ User cannot change password

☑ Password never expires

☐ Account is disabled

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**.

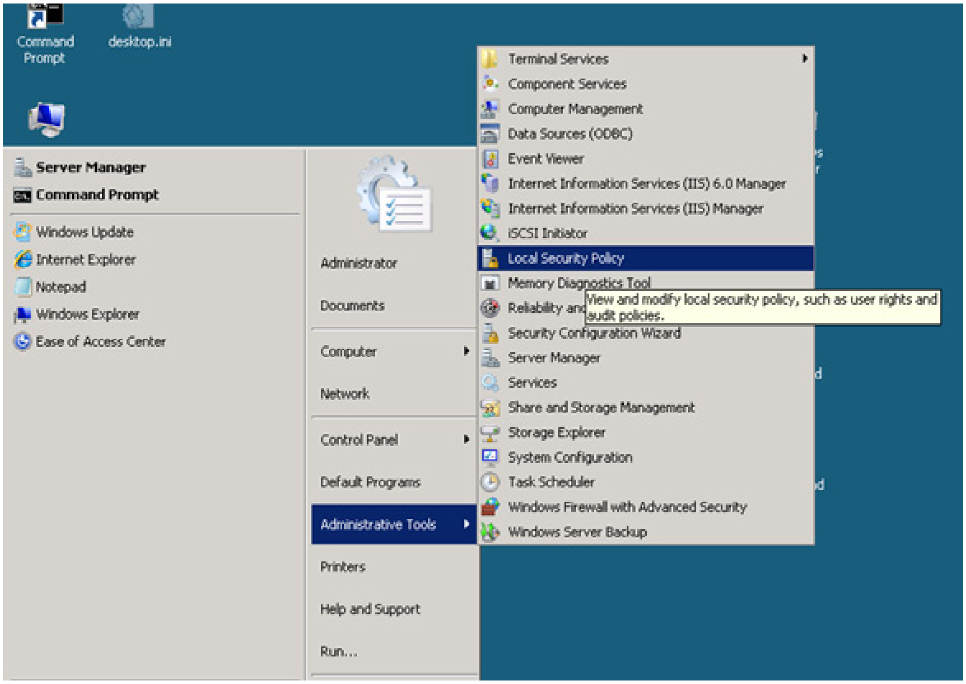
The next task is to restore the password policies.

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 69.



View and modify local security policy, such as user rights and audit policies.

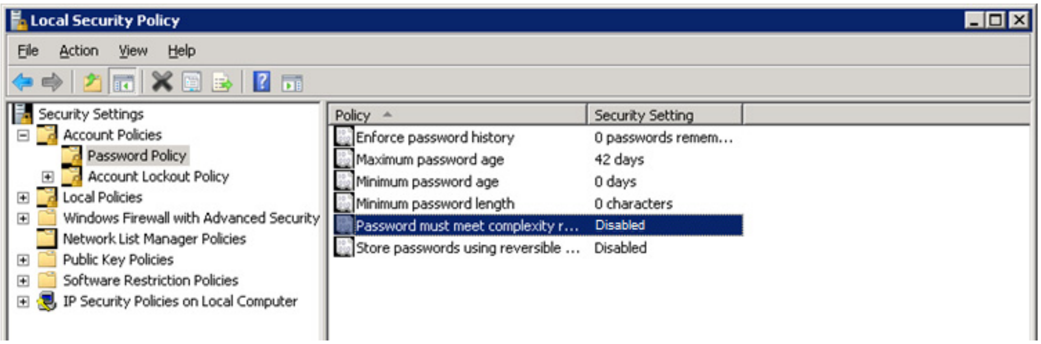
Figure 24 **Local security policy**

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.

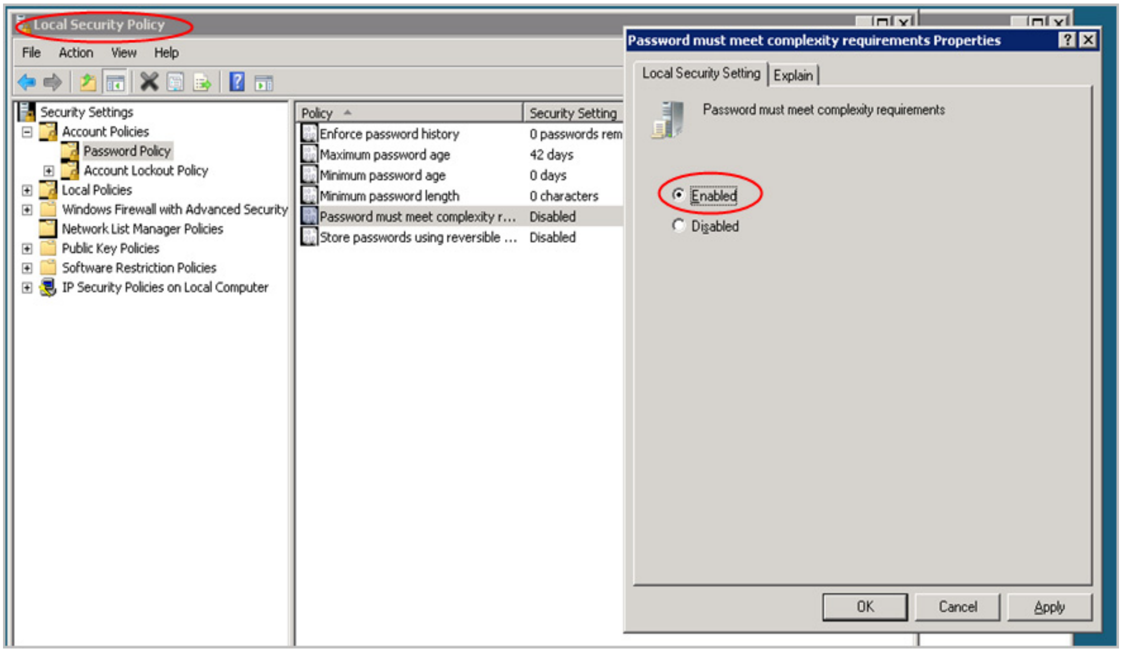
5. In the right pane, double-click **Password must meet complexity requirements**, as shown in Figure 25 on page 70.



Policy	Security Setting
Enforce password history	0 passwords remem…
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity r…	Disabled
Store passwords using reversible …	Disabled

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 70.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
IP Security Policies on Local Computer
Password must meet complexity requirements Properties
Local Security Setting
Explain
OK
Cancel
Apply

Policy	Security Setting
Enforce password history	0 passwords rem
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity r…	Disabled
Store passwords using reversible …	Disabled

Password must meet complexity requirements

● Enabled

○ Disabled

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 with IIS 6.0 Compatibility Windows 2008 R1 without IIS 7.5 FTP add-in

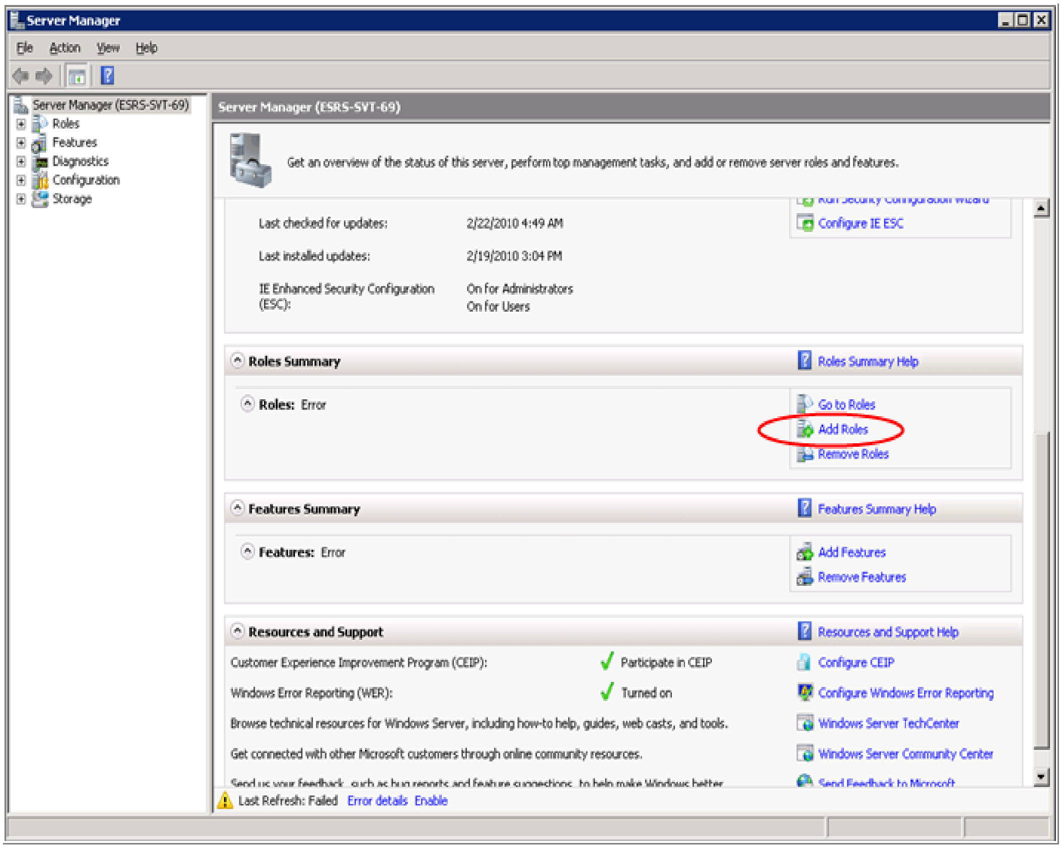
Now that you have created the IIS user accounts and reset the password policies, you can install IIS and the FTP service.

Beginning the IIS installation

To begin the IIS installation:

Note: The initial configuration of IIS is used to configure and verify that IIS is properly installed and is used by the Customer Environment Check Tool (CECT). The Provisioning Tool (PvT) will attempt to reconfigure IIS correctly as part of the Gateway Client install. The reconfiguration needs to verified after the Gateway Client 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.



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Last checked for updates: 2/22/2010 4:49 AM

Last installed updates: 2/19/2010 3:04 PM

IE Enhanced Security Configuration (ESC): On for Administrators
On for Users

Roles: Error

Features: Error

Customer Experience Improvement Program (CEIP): ✓ Participate in CEIP

Windows Error Reporting (WER): ✓ Turned on

Browse technical resources for Windows Server, including how-to help, guides, web casts, and tools.

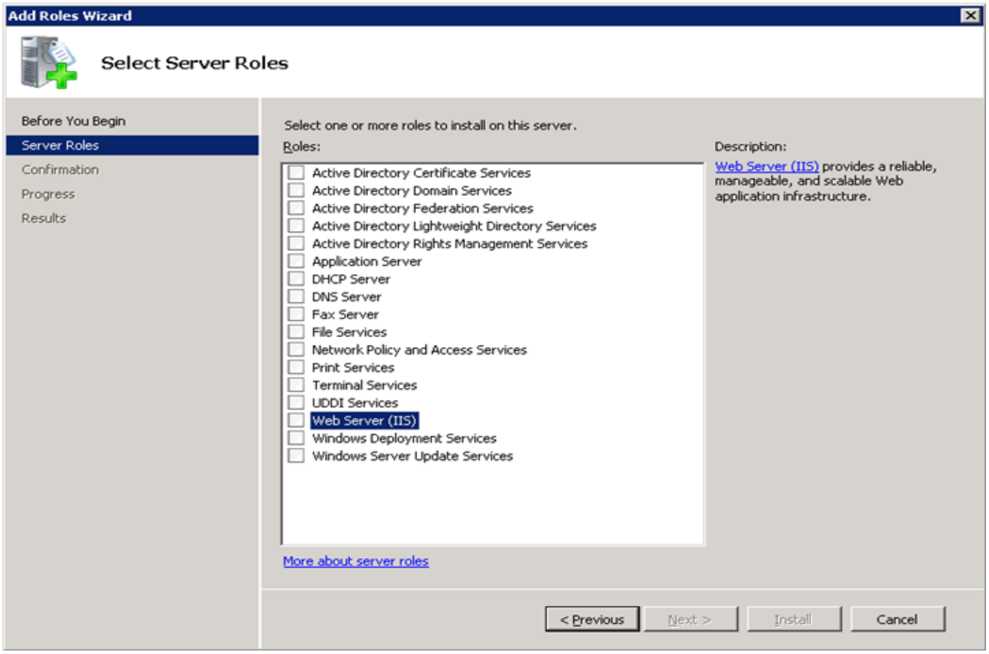
Get connected with other Microsoft customers through online community resources.

Send us your feedback, such as bug reports and feature suggestions, to help make Windows better.

Last Refresh: Failed

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.



Select Server Roles

Select one or more roles to install on this server.

Roles:

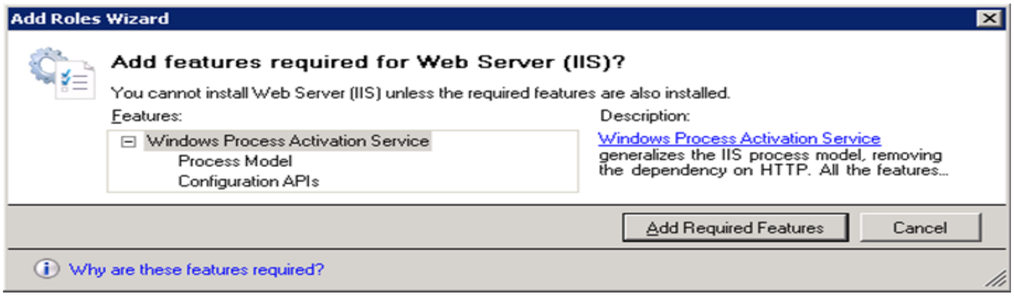
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

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 73.



Add features required for Web Server (IIS)?

You cannot install Web Server (IIS) unless the required features are also installed.

Features:

Windows Process Activation Service
- Process Model
- Configuration APIs

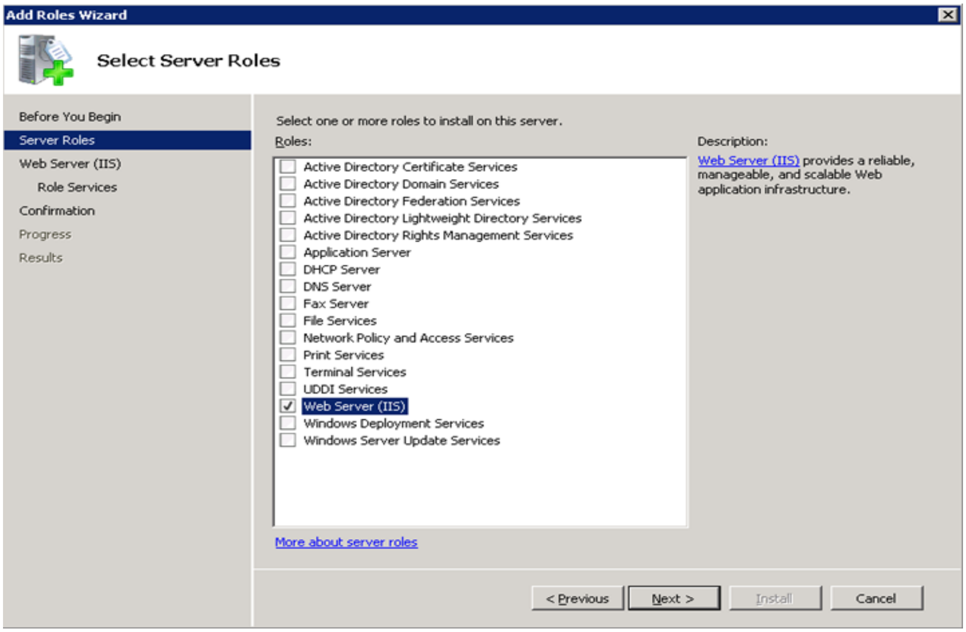
Description:

Windows Process Activation Service generalizes the IIS process model, removing the dependency on HTTP. All the features...

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.



Add Roles Wizard

Select Server Roles

Before You Begin
Server Roles
Web Server (IIS)
Role Services
Confirmation
Progress
Results

Select one or more roles to install on this server.

Roles:

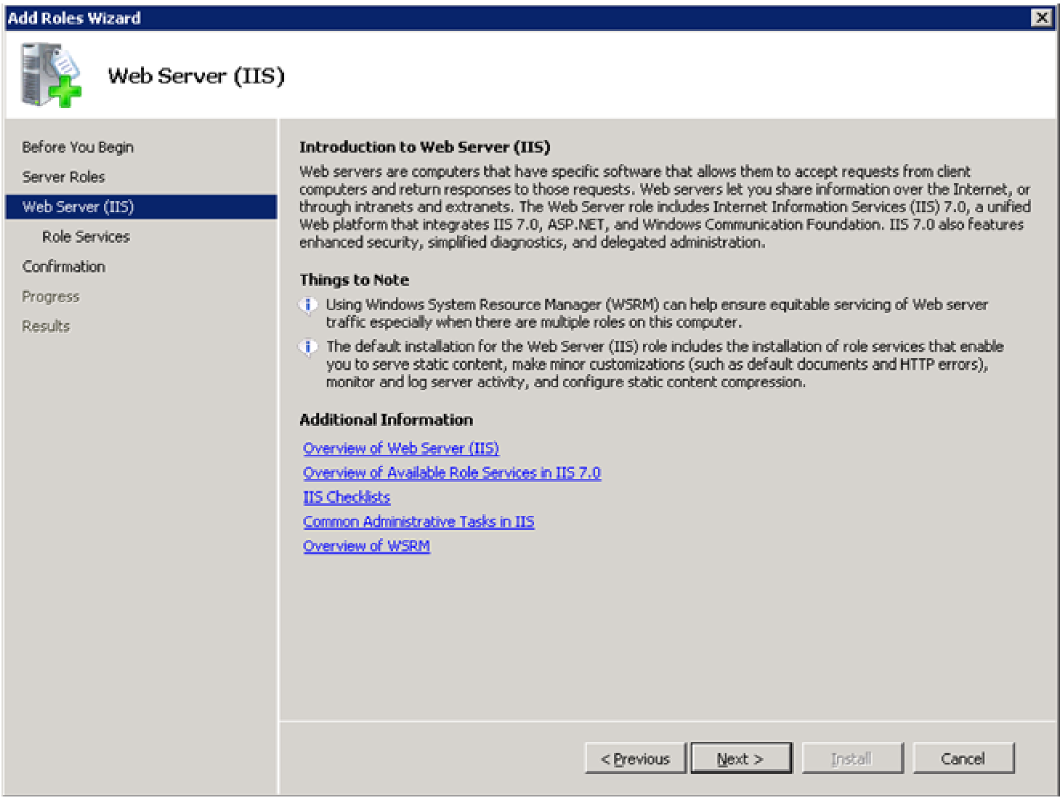
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

More about server roles

Figure 30 Web Server (IIS)

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



Introduction to Web Server (IIS)

Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.

Things to Note

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Additional Information

Overview of Web Server (IIS)
Overview of Available Role Services in IIS 7.0
IIS Checklists
Common Administrative Tasks in IIS
Overview of WSRM

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.

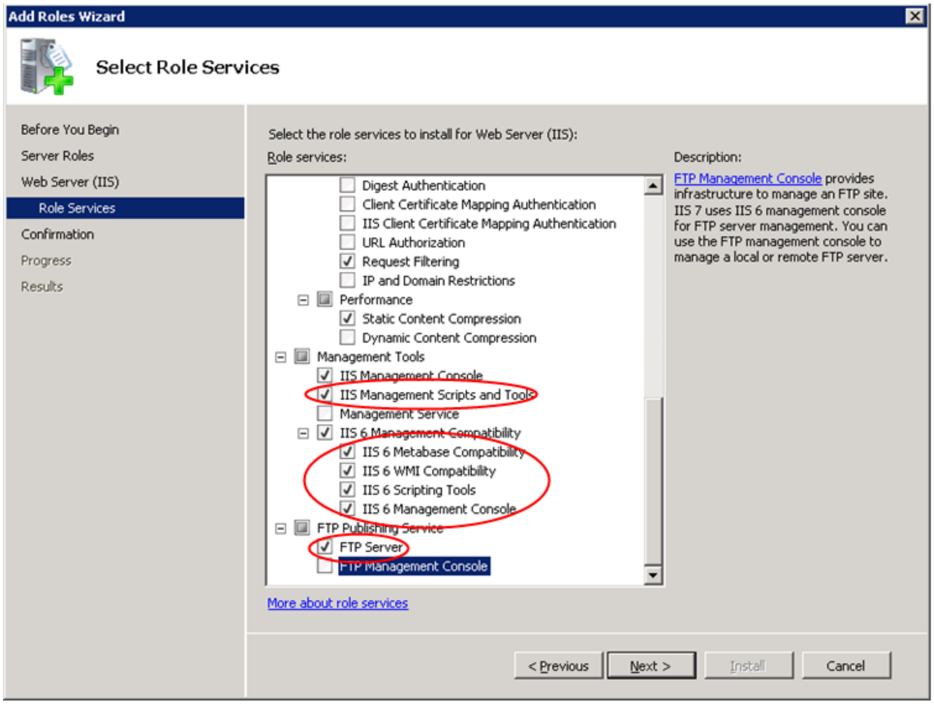
Your IIS installation is almost complete. Now you must install role services, including the FTP service.

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.



Add Roles Wizard

Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

☐ Digest Authentication
☐ Client Certificate Mapping Authentication
☐ IIS Client Certificate Mapping Authentication
☐ URL Authorization
☑ Request Filtering
☐ IP and Domain Restrictions
⊟ ▣ Performance
☑ Static Content Compression
☐ Dynamic Content Compression
⊟ ▣ Management Tools
☑ IIS Management Console
☑ IIS Management Scripts and Tools
☐ Management Service
⊟ ☑ IIS 6 Management Compatibility
☑ IIS 6 Metabase Compatibility
☑ IIS 6 WMI Compatibility
☑ IIS 6 Scripting Tools
☑ IIS 6 Management Console
⊟ ▣ FTP Publishing Service
☑ FTP Server
☐ FTP Management Console

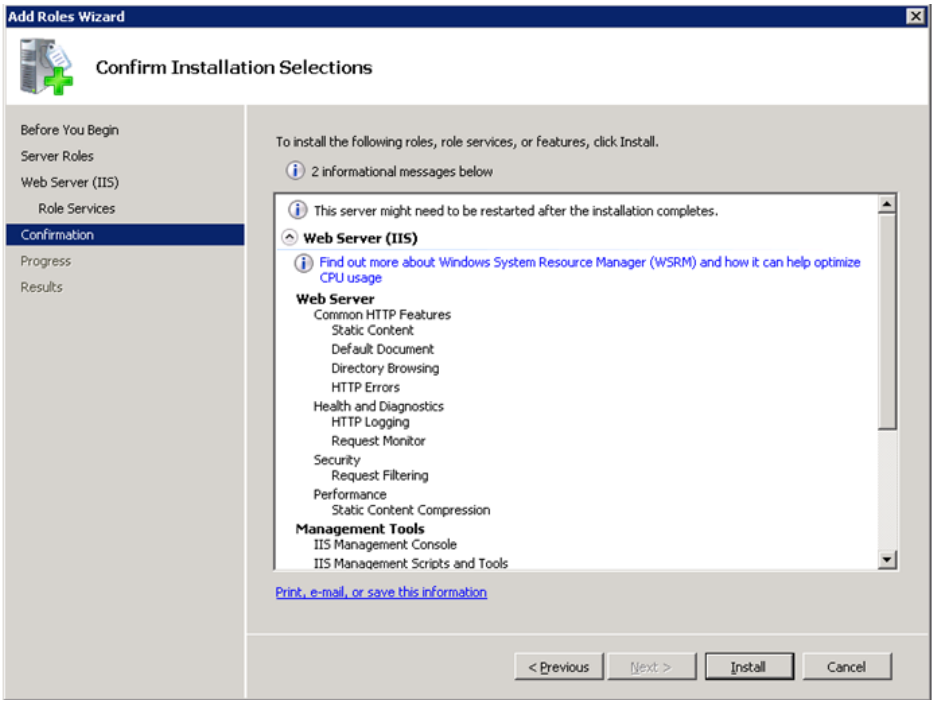
Description:

FTP Management Console provides infrastructure to manage an FTP site. IIS 7 uses IIS 6 management console for FTP server management. You can use the FTP management console to manage a local or remote FTP server.

More about role services

Figure 32 Select Role Services

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



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

Web Server (IIS)

Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

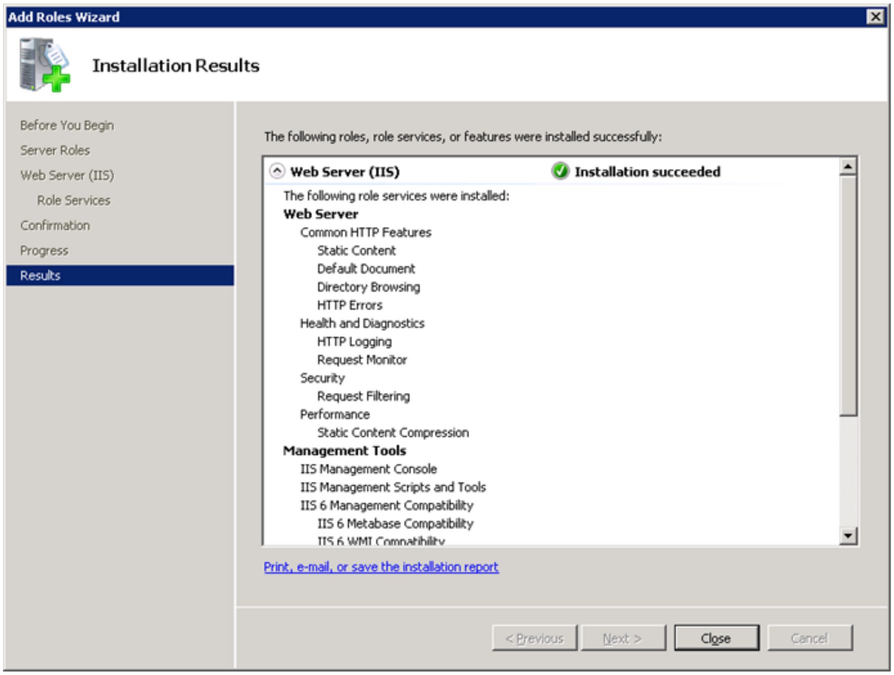
Web Server
Common HTTP Features
Static Content
Default Document
Directory Browsing
HTTP Errors
Health and Diagnostics
HTTP Logging
Request Monitor
Security
Request Filtering
Performance
Static Content Compression
Management Tools
IIS Management Console
IIS Management Scripts and Tools

Print, e-mail, or save this information

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.



Installation Results

The following roles, role services, or features were installed successfully:

Web Server (IIS) ✓ Installation succeeded

The following role services were installed:

Web Server

- Common HTTP Features
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
- Health and Diagnostics
  - HTTP Logging
  - Request Monitor
- Security
  - Request Filtering
- Performance
  - Static Content Compression

Management Tools

- IIS Management Console
- IIS Management Scripts and Tools
- IIS 6 Management Compatibility
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility

Print, e-mail, or save the installation report

Figure 34 **Installation Results**

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

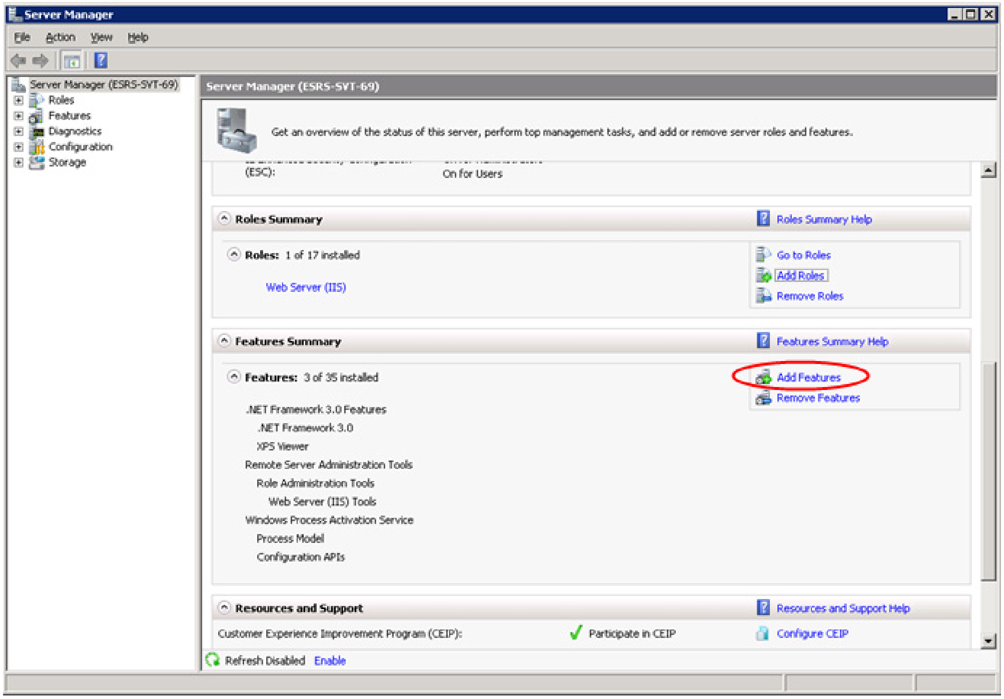
This completes the IIS installation and the FTP service installation. The next task is to install the SMTP service.

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.



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

(ESC): On for Users

Roles: 1 of 17 installed

Web Server (IIS)

Features: 3 of 35 installed

.NET Framework 3.0 Features
.NET Framework 3.0
XPS Viewer
Remote Server Administration Tools
Role Administration Tools
Web Server (IIS) Tools
Windows Process Activation Service
Process Model
Configuration APIs

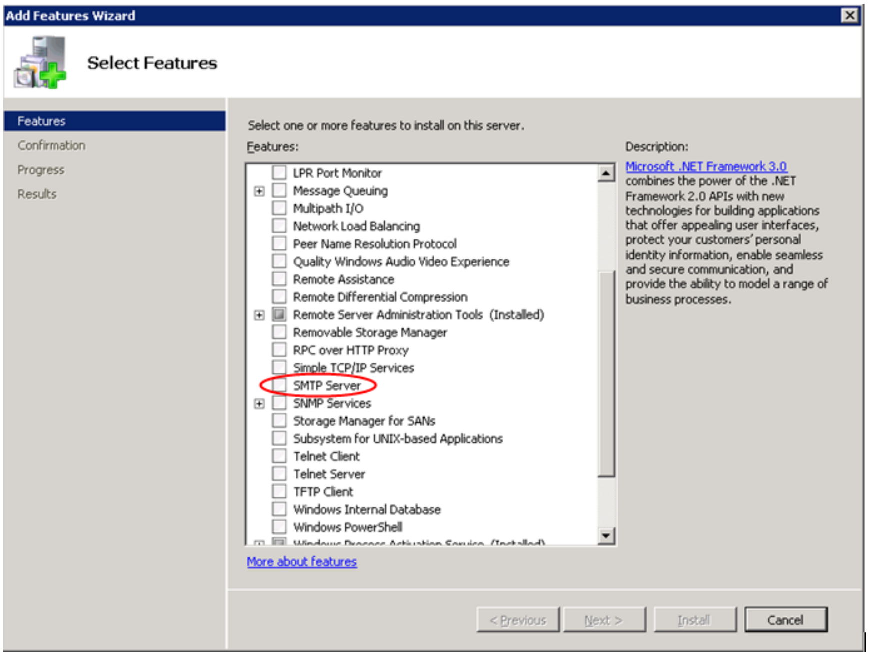
Customer Experience Improvement Program (CEIP): ✓ Participate in CEIP

Refresh Disabled Enable

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.



Add Features Wizard

Select Features

Features
Confirmation
Progress
Results

Select one or more features to install on this server.

Features:

- □ LPR Port Monitor
- ⊞ □ Message Queuing
- □ Multipath I/O
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ Remote Assistance
- □ Remote Differential Compression
- ⊞ ■ Remote Server Administration Tools (Installed)
- □ Removable Storage Manager
- □ RPC over HTTP Proxy
- □ Simple TCP/IP Services
- □ SMTP Server
- ⊞ □ SNMP Services
- □ Storage Manager for SANs
- □ Subsystem for UNIX-based Applications
- □ Telnet Client
- □ Telnet Server
- □ TFTP Client
- □ Windows Internal Database
- □ Windows PowerShell
- ⊞ ■ Windows Process Activation Service (Installed)

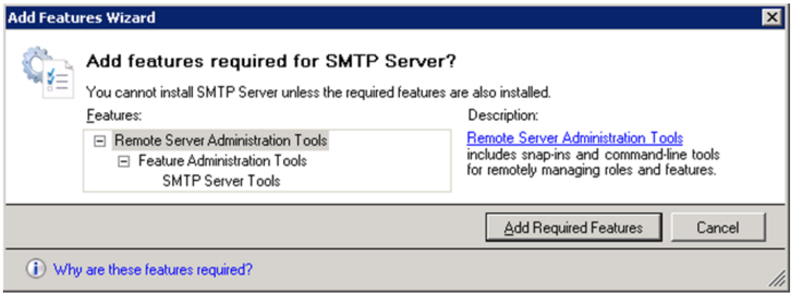
Description:

Microsoft .NET Framework 3.0 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

More about features

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.



Add Features Wizard

Add features required for SMTP Server?

You cannot install SMTP Server unless the required features are also installed.

Features:

- ⊟ Remote Server Administration Tools
  - ⊟ Feature Administration Tools
    - SMTP Server Tools

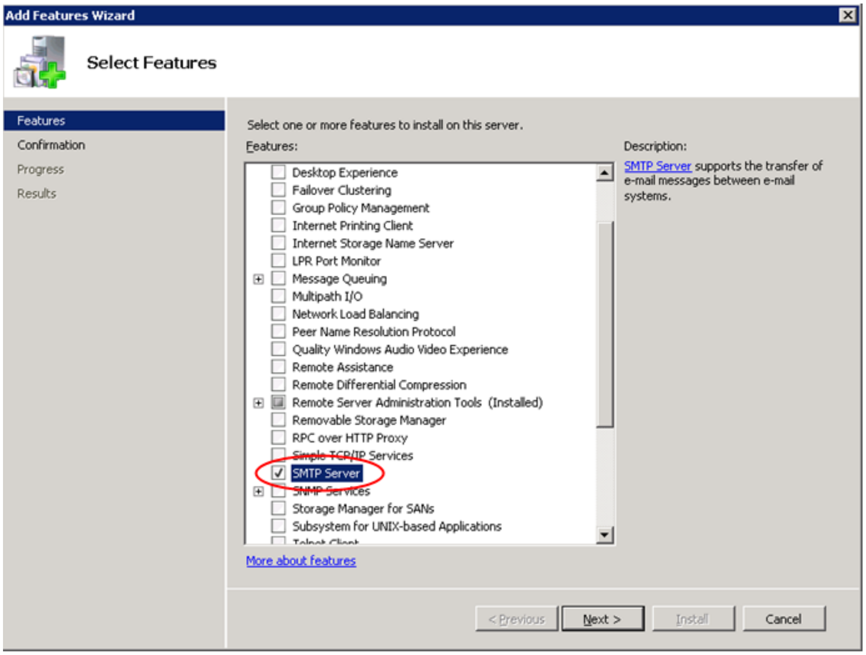
Description:

Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.

Why are these features required?

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.



Add Features Wizard

Select Features

Select one or more features to install on this server.

Features:

- □ Desktop Experience
- □ Failover Clustering
- □ Group Policy Management
- □ Internet Printing Client
- □ Internet Storage Name Server
- □ LPR Port Monitor
- ⊞ □ Message Queuing
- □ Multipath I/O
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- □ Remote Assistance
- □ Remote Differential Compression
- ⊞ ▣ Remote Server Administration Tools (Installed)
- □ Removable Storage Manager
- □ RPC over HTTP Proxy
- □ Simple TCP/IP Services
- ☑ SMTP Server
- ⊞ □ SNMP Services
- □ Storage Manager for SANs
- □ Subsystem for UNIX-based Applications
- □ Telnet Client

Description:

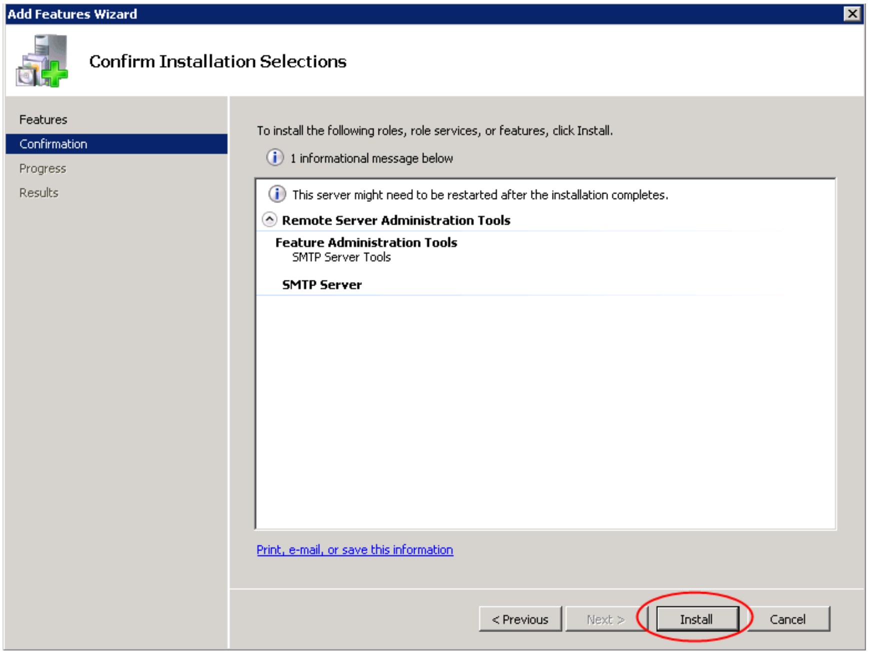
SMTP Server supports the transfer of e-mail messages between e-mail systems.

More about features

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.



To install the following roles, role services, or features, click Install.

1 informational message below

This server might need to be restarted after the installation completes.

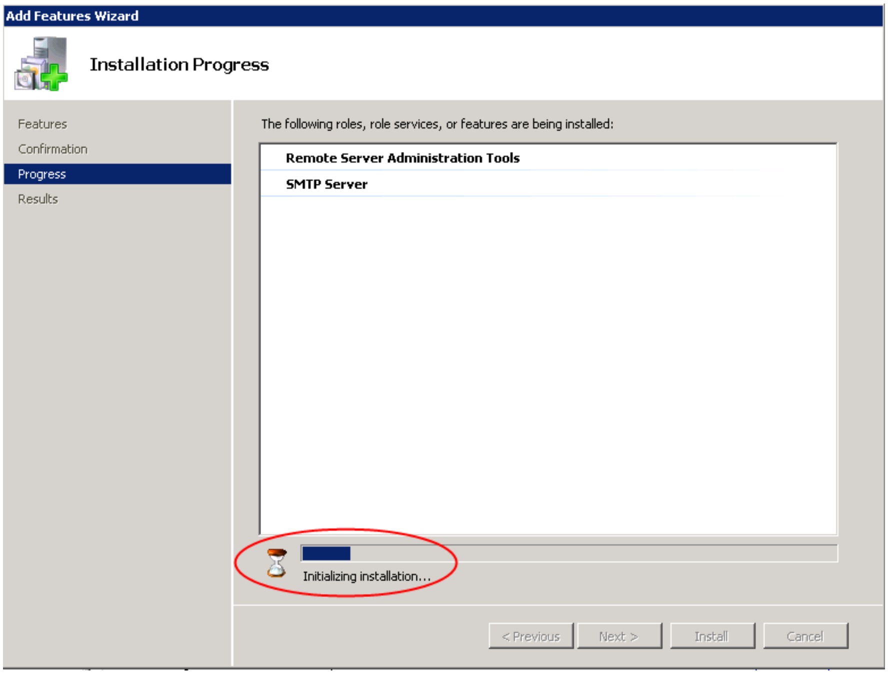
Remote Server Administration Tools

Feature Administration Tools
SMTP Server Tools

SMTP Server

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.



The following roles, role services, or features are being installed:

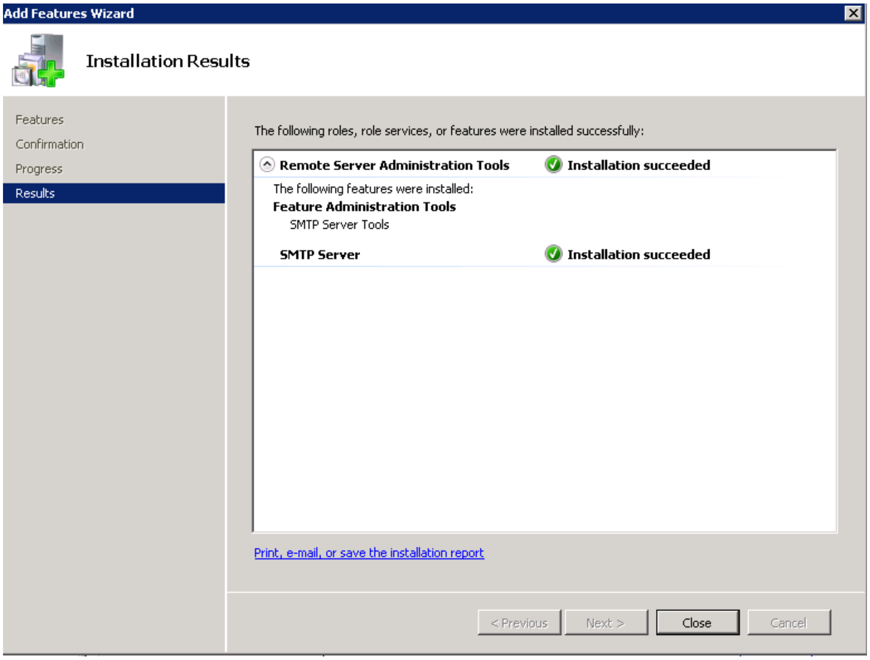
Remote Server Administration Tools

SMTP Server

Initializing installation...

Figure 40 **Installation Progress**

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



Add Features Wizard

Installation Results

The following roles, role services, or features were installed successfully:

Remote Server Administration Tools ✓ **Installation succeeded**

The following features were installed:
Feature Administration Tools
SMTP Server Tools

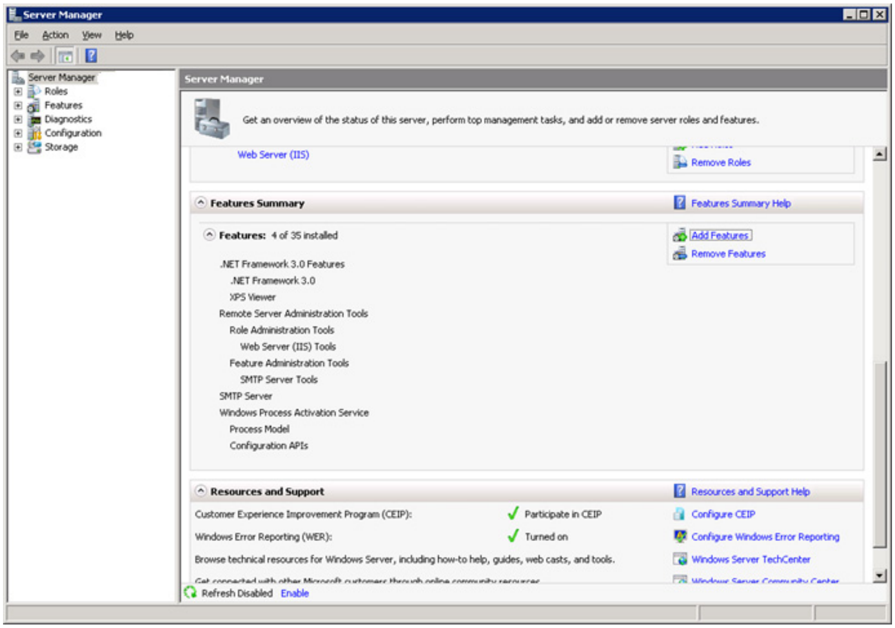
SMTP Server ✓ **Installation succeeded**

Print, e-mail, or save the installation report

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.



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Web Server (IIS) — Remove Roles

Features Summary — Features Summary Help

Features: 4 of 35 installed — Add Features, Remove Features

.NET Framework 3.0 Features
    .NET Framework 3.0
    XPS Viewer
Remote Server Administration Tools
    Role Administration Tools
        Web Server (IIS) Tools
    Feature Administration Tools
        SMTP Server Tools
SMTP Server
Windows Process Activation Service
    Process Model
    Configuration APIs

Resources and Support — Resources and Support Help

Customer Experience Improvement Program (CEIP): ✓ Participate in CEIP — Configure CEIP

Windows Error Reporting (WER): ✓ Turned on — Configure Windows Error Reporting

Browse technical resources for Windows Server, including how-to help, guides, web casts, and tools. — Windows Server TechCenter

Get connected with other Microsoft customers through online community resources — Windows Server Community Center

Refresh Disabled Enable

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

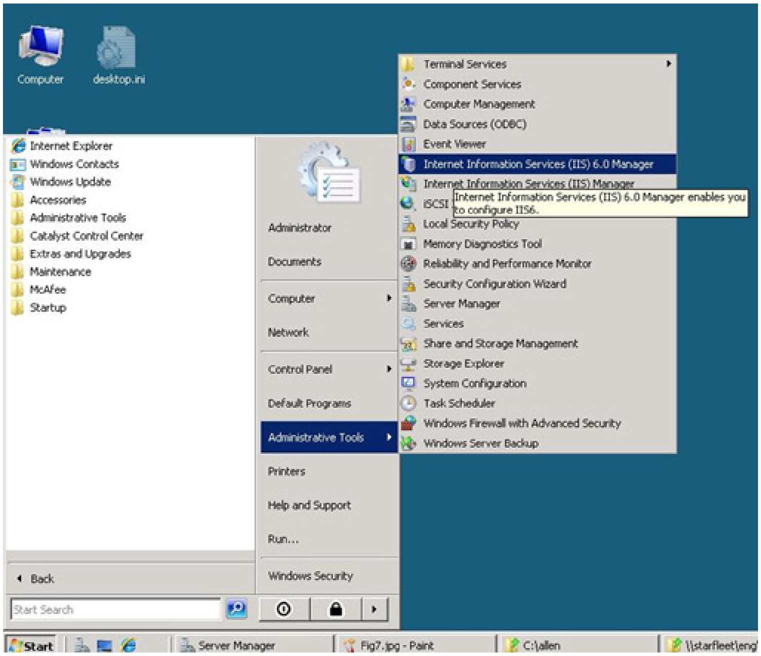
AFTER the Gateway Client is installed per CSP2100* IIS MUST be reconfigured to point to <install_drive>:\EMC\ESRS\Gateway\work\mailroot\Drop and <install_drive>:\EMC\ESRS\Gateway\work\mailroot\BadMail

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.



Internet Information Services (IIS) 6.0 Manager enables you to configure IIS6.

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.

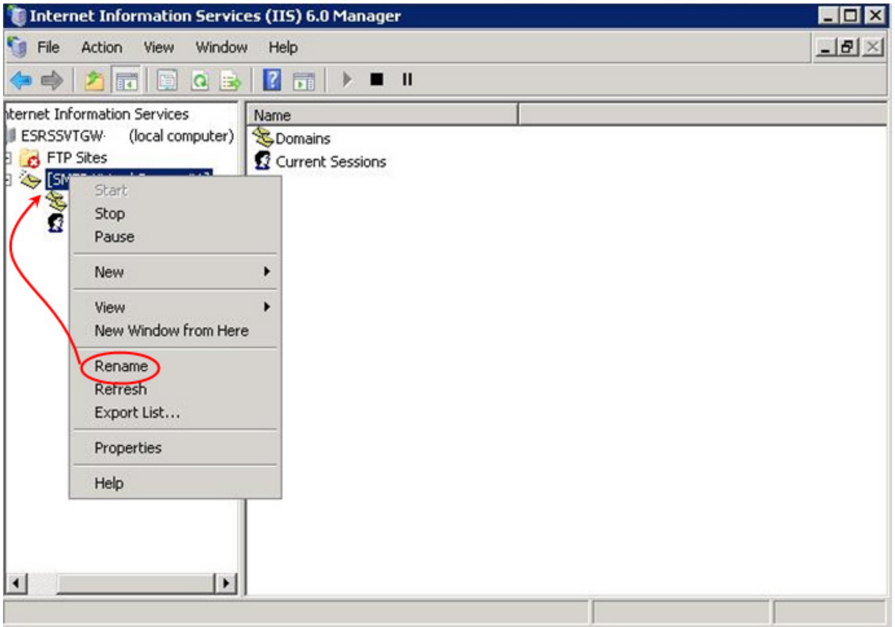


Figure 44 Rename the folder

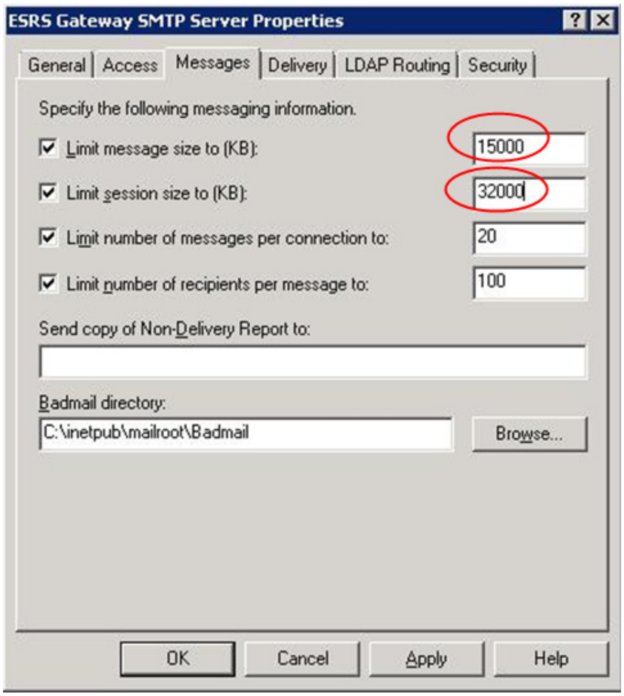
4. Right-click **ESRS Gateway SMTP Server** and select **Properties**. The **ESRS Gateway SMTP Server Properties** window appears.

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.



Specify the following messaging information.

☑ Limit message size to (KB): 15000

☑ Limit session size to (KB): 32000

☑ Limit number of messages per connection to: 20

☑ Limit number of recipients per message to: 100

Send copy of Non-Delivery Report to:

Badmail directory: C:\inetpub\mailroot\Badmail

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.

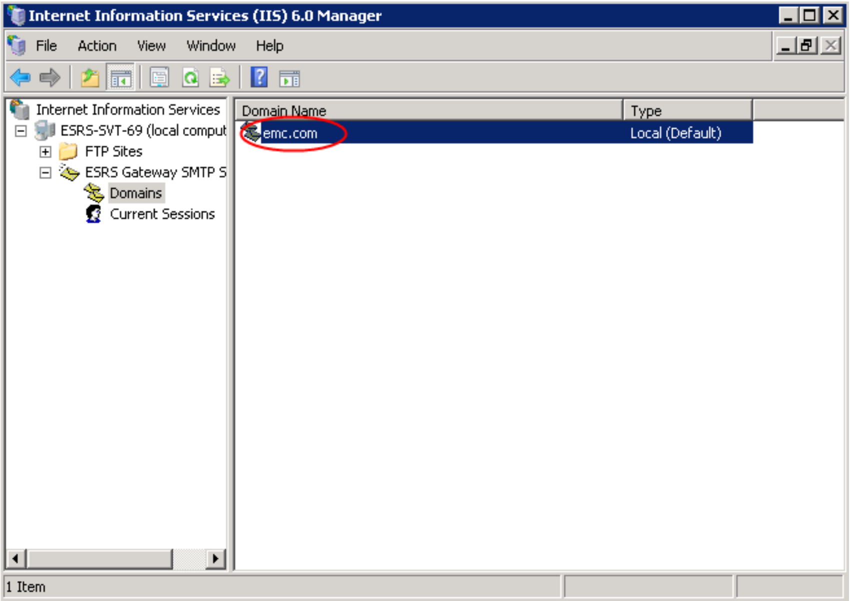
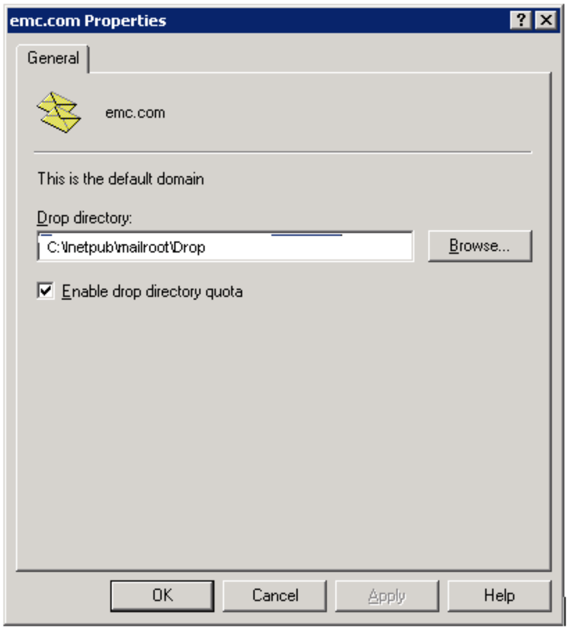

Internet Information Services (IIS) 6.0 Manager
File Action View Window Help
Internet Information Services
ESRS-SVT-69 (local comput
FTP Sites
ESRS Gateway SMTP S
Domains
Current Sessions
Domain Name
Type
emc.com
Local (Default)
1 Item

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.



emc.com Properties

General

emc.com

This is the default domain

Drop directory:

C:\Inetpub\mailroot\Drop

☑ Enable drop directory quota

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

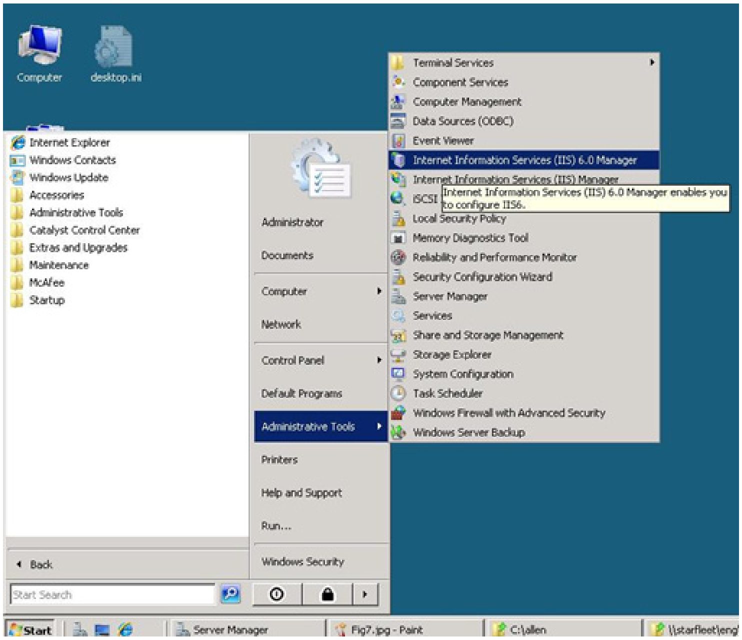
Beginning the FTP server configuration

To configure the FTP server:

IMPORTANT

AFTER the Gateway 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.



Internet Information Services (IIS) 6.0 Manager enables you to configure IIS6.

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.

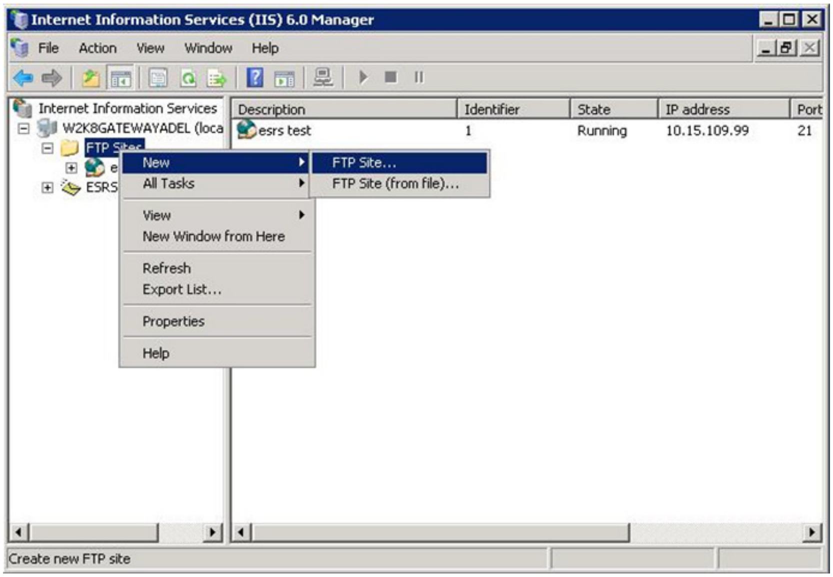
3. In the left pane of the **IIS 6.0 Manager** window, expand the folder structure so that the **FTP Sites** folder is visible.

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.

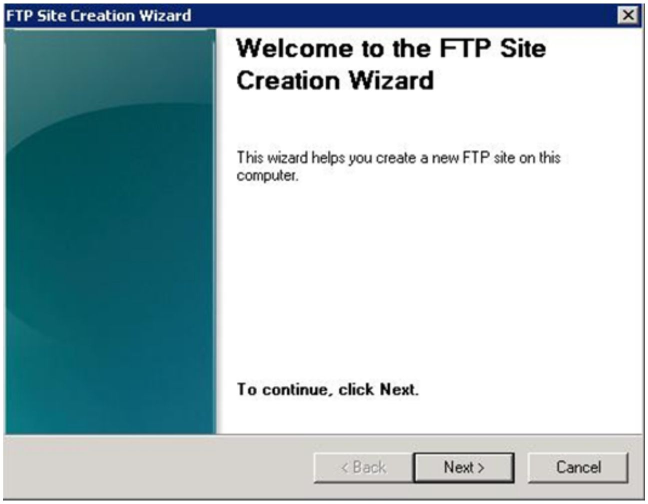
6. To create the new FTP site, right-click **FTP Sites**. The FTP Sites menu appears, as shown in Figure 49 on page 92.



Description	Identifier	State	IP address	Port
esrs test	1	Running	10.15.109.99	21

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.



FTP Site Creation Wizard

Welcome to the FTP Site Creation Wizard

This wizard helps you create a new FTP site on this computer.

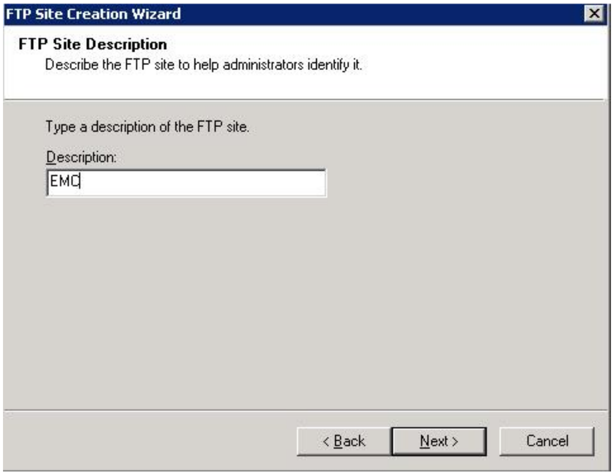
To continue, click Next.

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.


FTP Site Creation Wizard

FTP Site Description

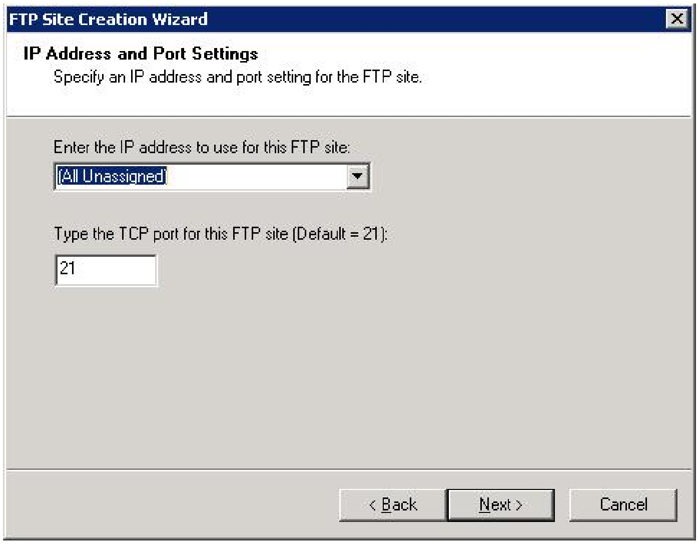
Describe the FTP site to help administrators identify it.

Type a description of the FTP site.

Description: EMC

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**.



FTP Site Creation Wizard

IP Address and Port Settings

Specify an IP address and port setting for the FTP site.

Enter the IP address to use for this FTP site:

(All Unassigned)

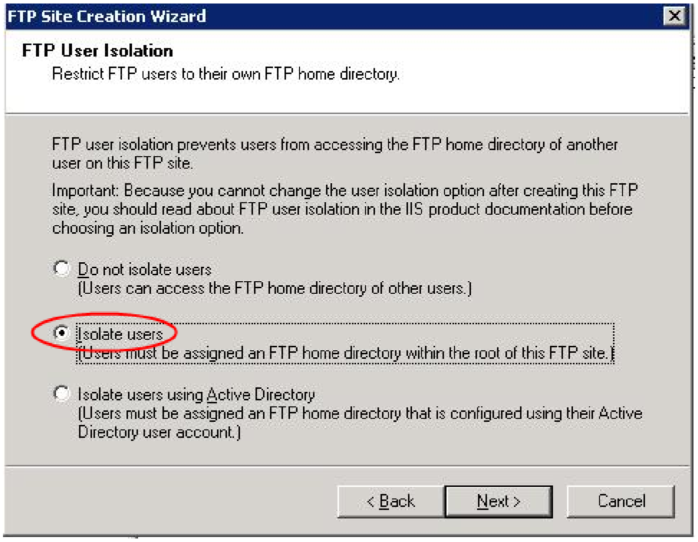
Type the TCP port for this FTP site (Default = 21):

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.



FTP Site Creation Wizard

FTP User Isolation

Restrict FTP users to their own FTP home directory.

FTP user isolation prevents users from accessing the FTP home directory of another user on this FTP site.

Important: Because you cannot change the user isolation option after creating this FTP site, you should read about FTP user isolation in the IIS product documentation before choosing an isolation option.

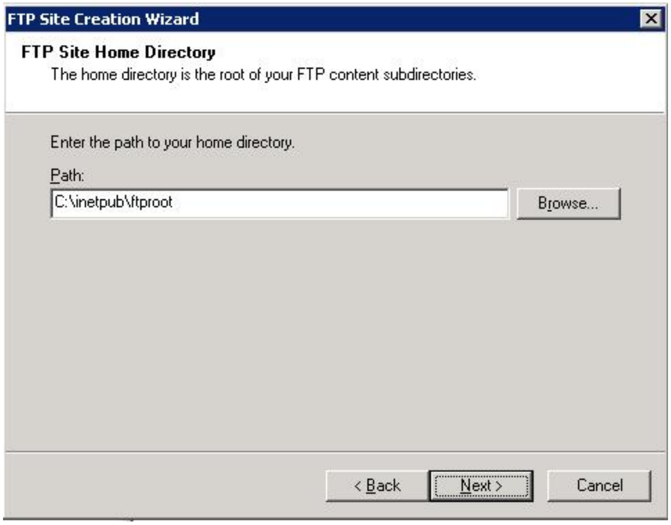
○ Do not isolate users
(Users can access the FTP home directory of other users.)

● Isolate users
(Users must be assigned an FTP home directory within the root of this FTP site.)

○ Isolate users using Active Directory
(Users must be assigned an FTP home directory that is configured using their Active Directory user account.)

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.



FTP Site Creation Wizard

FTP Site Home Directory

The home directory is the root of your FTP content subdirectories.

Enter the path to your home directory.

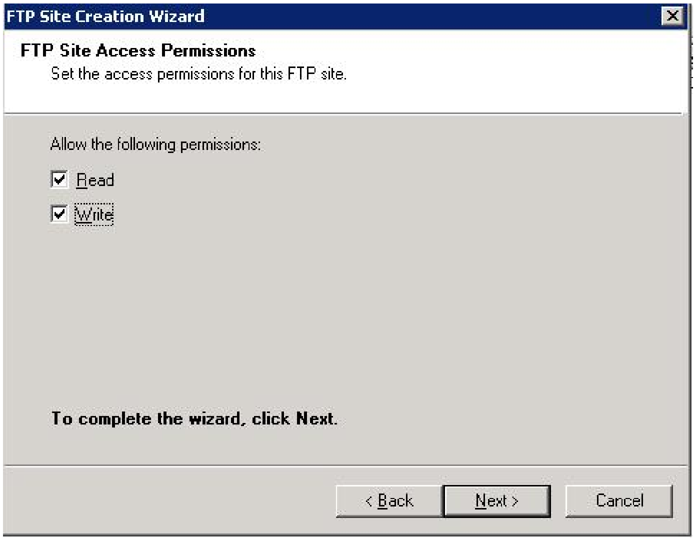
Path: C:\inetpub\ftproot

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**



FTP Site Creation Wizard

FTP Site Access Permissions

Set the access permissions for this FTP site.

Allow the following permissions:

☑ Read

☑ Write

To complete the wizard, click Next.

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**.

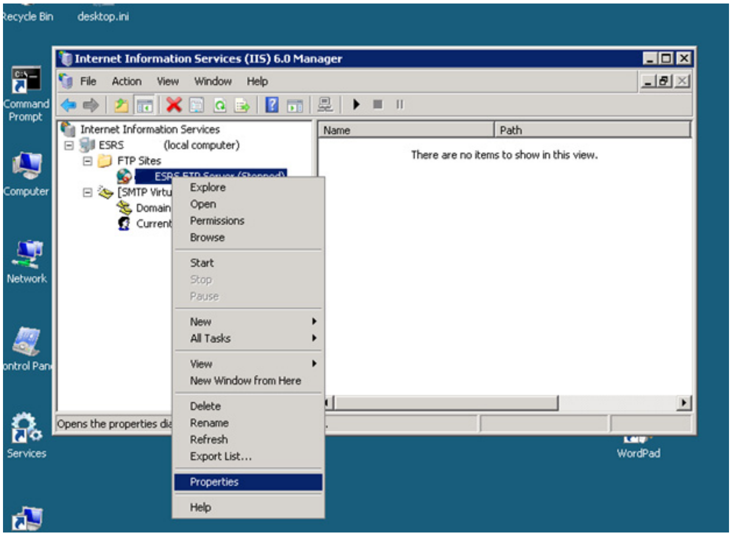
11. Click **Finish**.

    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.

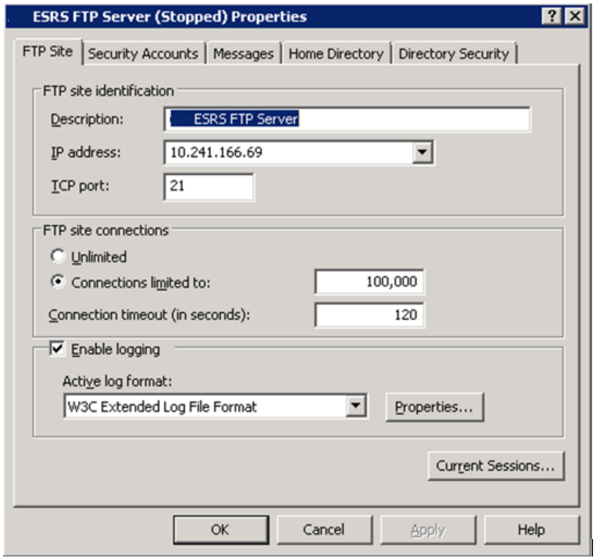


There are no items to show in this view.

Opens the properties di

Figure 56 **FTP Server menu**

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



ESRS FTP Server (Stopped) Properties

FTP site identification

Description: ESRS FTP Server

IP address: 10.241.166.69

TCP port: 21

FTP site connections

○ Unlimited

● Connections limited to: 100,000

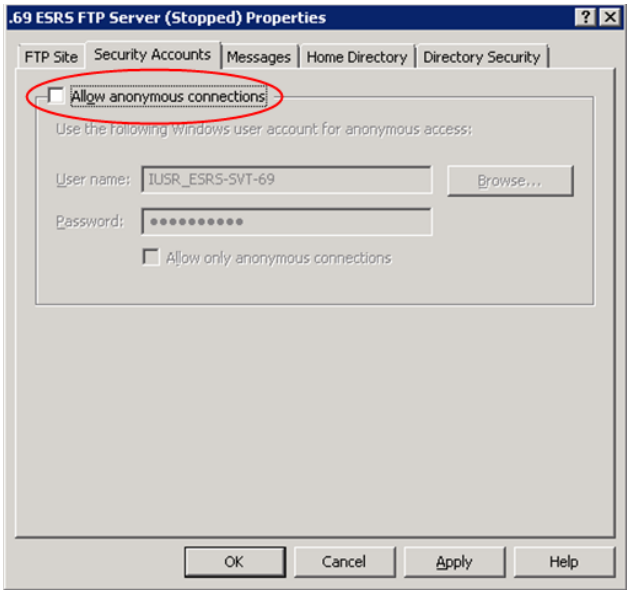
Connection timeout (in seconds): 120

☑ Enable logging

Active log format: W3C Extended Log File Format

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.



.69 ESRS FTP Server (Stopped) Properties

☐ Allow anonymous connections

Use the following Windows user account for anonymous access:

User name: IUSR_ESRS-SVT-69

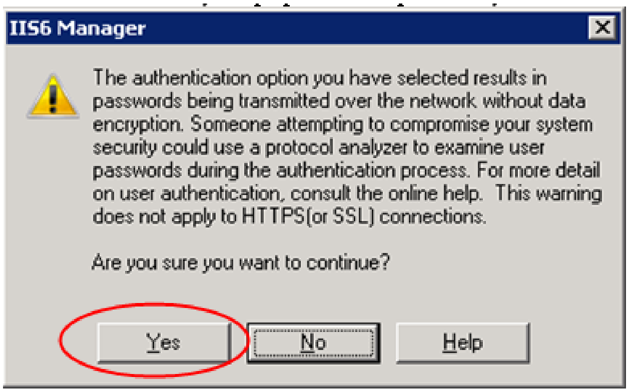
Password: ●●●●●●●●●●

☐ Allow only anonymous connections

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.



IIS6 Manager

The authentication option you have selected results in passwords being transmitted over the network without data encryption. Someone attempting to compromise your system security could use a protocol analyzer to examine user passwords during the authentication process. For more detail on user authentication, consult the online help. This warning does not apply to HTTPS(or SSL) connections.

Are you sure you want to continue?

Figure 59 Authentication option continue

9. In the **FTP Server Properties** window, click **Home Directory**. The **Home Directory** tab appears.

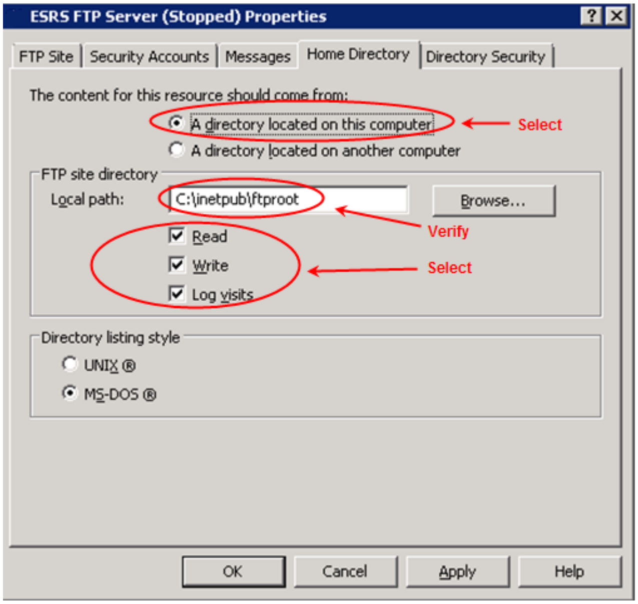
10. In the **Home Directory** tab, take the following steps, as shown in Figure 60 on page 101:

    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**



ESRS FTP Server (Stopped) Properties

The content for this resource should come from:

● A directory located on this computer ← Select

○ A directory located on another computer

FTP site directory

Local path: C:\inetpub\ftproot ← Verify

☑ Read

☑ Write

☑ Log visits ← Select

Directory listing style

○ UNIX ®

● MS-DOS ®

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.

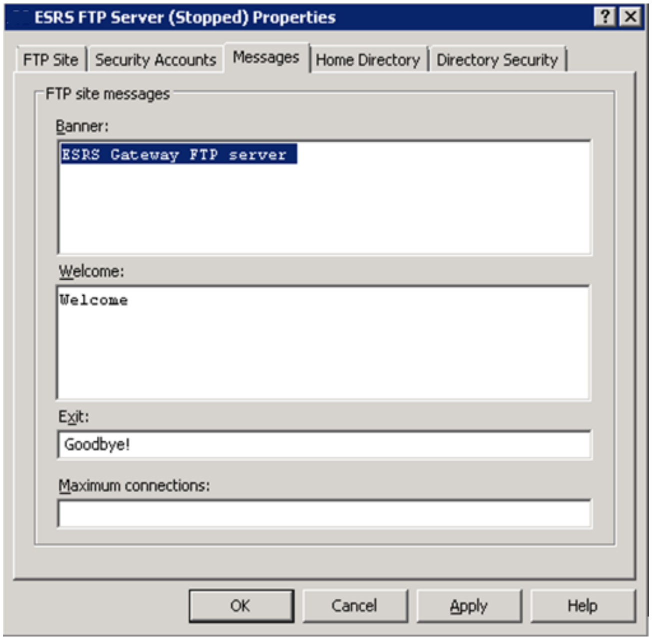
Creating optional site messages

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.



ESRS FTP Server (Stopped) Properties

Banner: ESRS Gateway FTP server

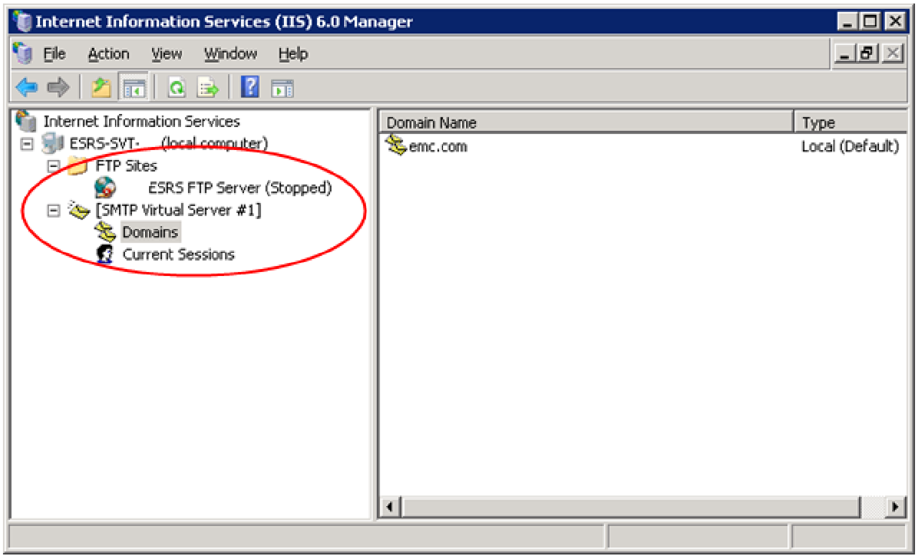
Welcome: Welcome

Exit: Goodbye!

Maximum connections:

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.


Internet Information Services (IIS) 6.0 Manager
File
Action
View
Window
Help
Internet Information Services
ESRS-SVT- (local computer)
FTP Sites
ESRS FTP Server (Stopped)
[SMTP Virtual Server #1]
Domains
Current Sessions

Domain Name	Type
emc.com	Local (Default)

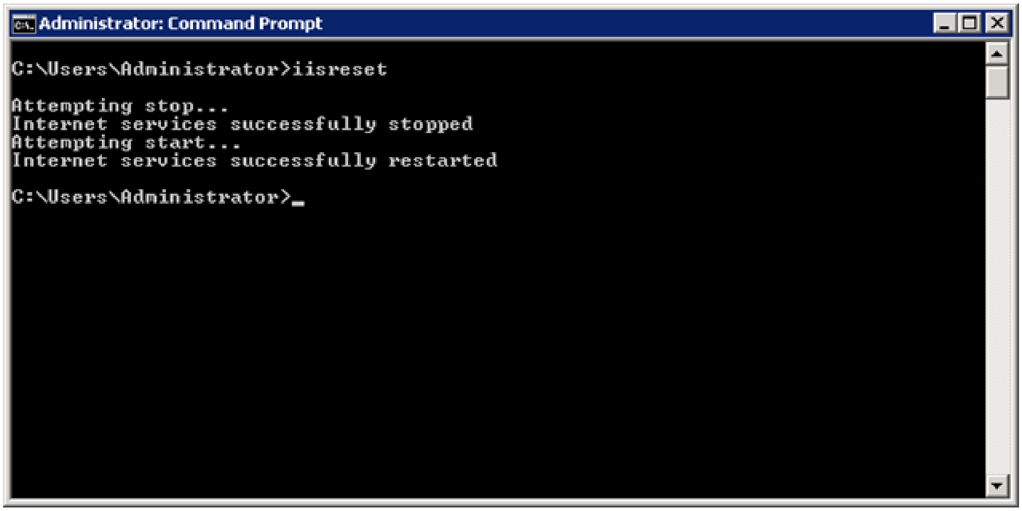
Figure 62 **FTP and SMTP services**

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.



```
C:\Users\Administrator>iisreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

C:\Users\Administrator>_
```

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:

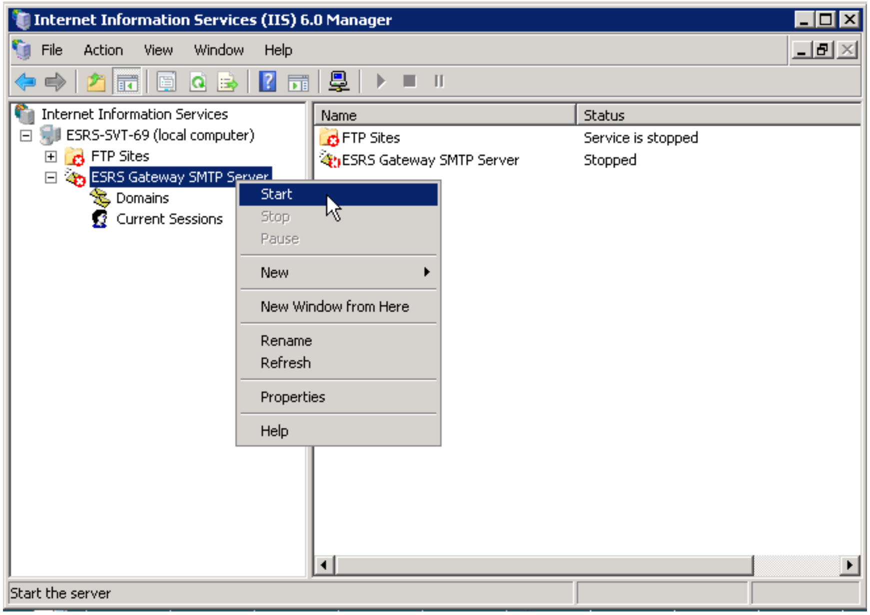
1. Click Windows **Start**, then **Administrative Tools** > **Internet Information Services (IIS) 6.0 Manager**.

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

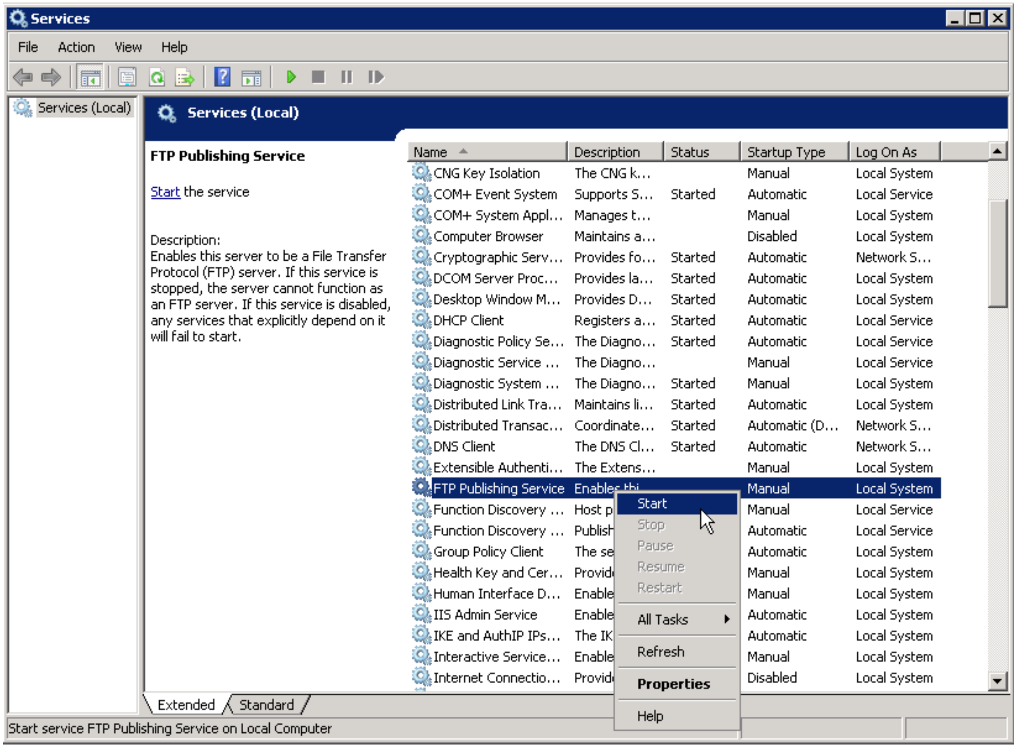
To start the service from the Services main window:

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.



Name	Status
FTP Sites	Service is stopped
ESRS Gateway SMTP Server	Stopped

Figure 64 Starting the service from IIS 6.0 Manager



FTP Publishing Service

Start the service

Description:
Enables this server to be a File Transfer Protocol (FTP) server. If this service is stopped, the server cannot function as an FTP server. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
CNG Key Isolation	The CNG k...		Manual	Local System
COM+ Event System	Supports S...	Started	Automatic	Local Service
COM+ System Appl...	Manages t...		Manual	Local System
Computer Browser	Maintains a...		Disabled	Local System
Cryptographic Serv...	Provides fo...	Started	Automatic	Network S...
DCOM Server Proc...	Provides la...	Started	Automatic	Local System
Desktop Window M...	Provides D...	Started	Automatic	Local System
DHCP Client	Registers a...	Started	Automatic	Local Service
Diagnostic Policy Se...	The Diagno...	Started	Automatic	Local Service
Diagnostic Service ...	The Diagno...		Manual	Local Service
Diagnostic System ...	The Diagno...	Started	Manual	Local System
Distributed Link Tra...	Maintains li...	Started	Automatic	Local System
Distributed Transac...	Coordinate...	Started	Automatic (D...	Network S...
DNS Client	The DNS Cl...	Started	Automatic	Network S...
Extensible Authenti...	The Extens...		Manual	Local System
FTP Publishing Service	Enables thi		Manual	Local System
Function Discovery ...	Host p		Manual	Local Service
Function Discovery ...	Publish		Automatic	Local Service
Group Policy Client	The se		Automatic	Local System
Health Key and Cer...	Provid		Manual	Local System
Human Interface D...	Enable		Manual	Local System
IIS Admin Service	Enable		Automatic	Local System
IKE and AuthIP IPs...	The IK		Automatic	Local System
Interactive Service...	Enable		Manual	Local System
Internet Connectio...	Provid		Disabled	Local System

Start service FTP Publishing Service on Local Computer

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.

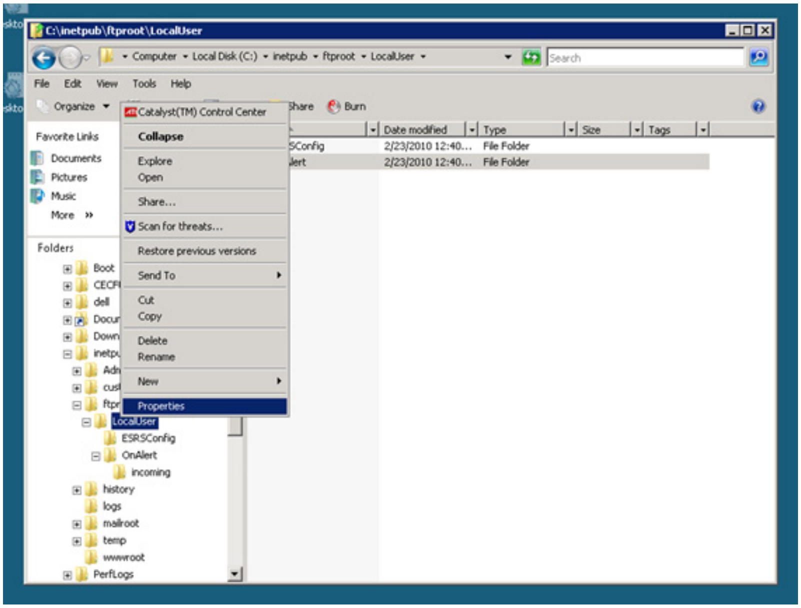
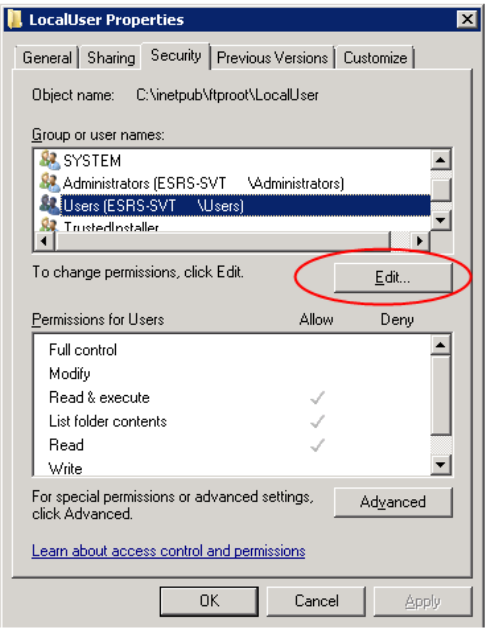


Figure 66 **Navigate to LocalUser Properties**

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.



LocalUser Properties

Object name: C:\inetpub\ftproot\LocalUser

Group or user names:

- SYSTEM
- Administrators (ESRS-SVT \Administrators)
- Users (ESRS-SVT \Users)
- TrustedInstaller

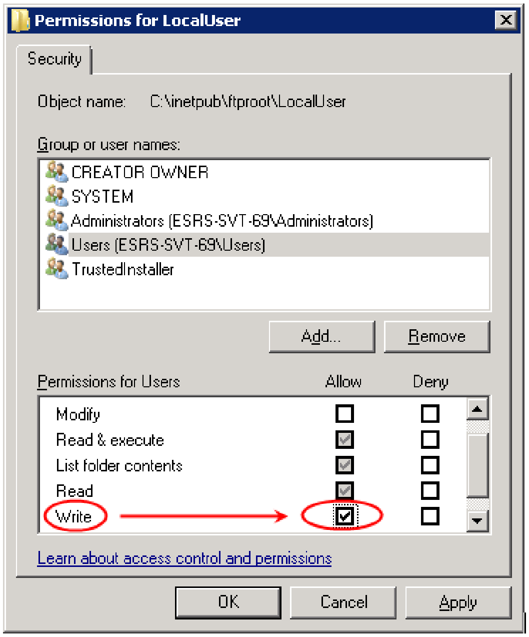
To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

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.



Object name: C:\inetpub\ftproot\LocalUser

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (ESRS-SVT-69\Administrators)
- Users (ESRS-SVT-69\Users)
- TrustedInstaller

Permissions for Users	Allow	Deny
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□
Write	☑	□

Learn about access control and permissions

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

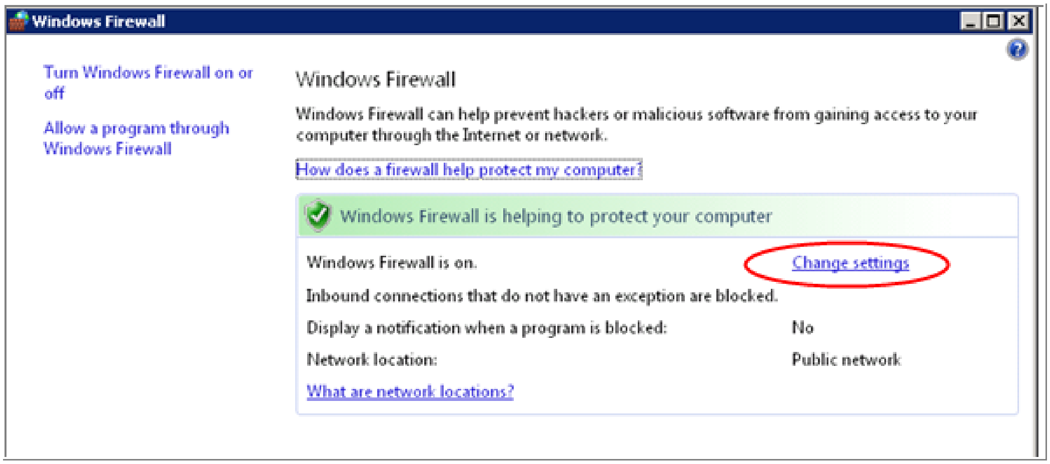
This section explains how to configure the Windows 2008 firewall settings.

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.


Windows Firewall
Turn Windows Firewall on or off
Allow a program through Windows Firewall
How does a firewall help protect my computer?
Change settings
What are network locations?

Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.

Windows Firewall is helping to protect your computer

Windows Firewall is on.

Inbound connections that do not have an exception are blocked.

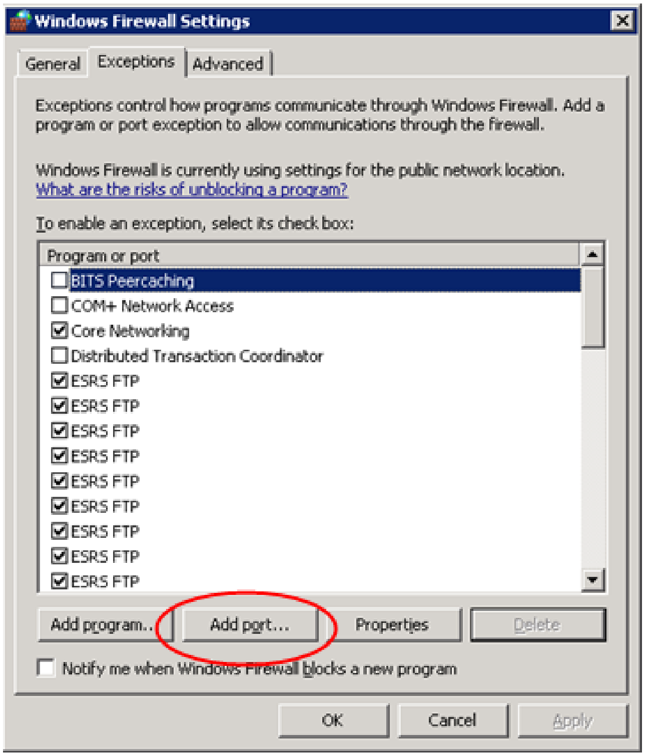
Display a notification when a program is blocked: No

Network location: Public network

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.



Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

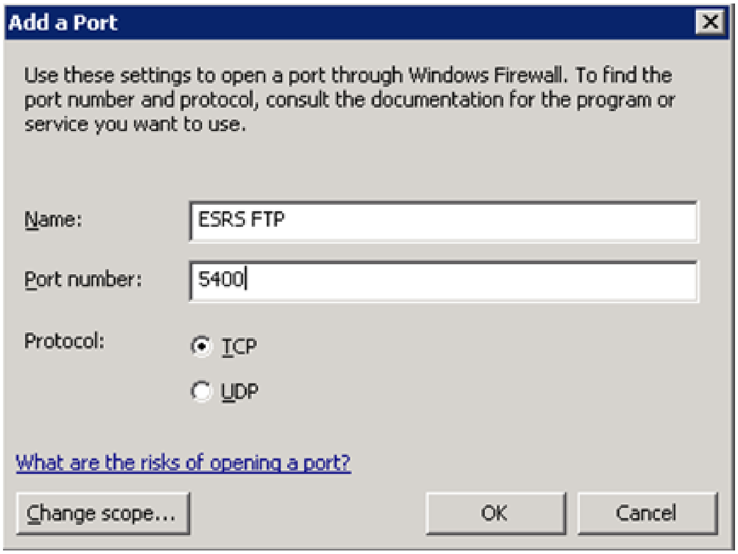
To enable an exception, select its check box:

Program or port
- □ BITS Peercaching
- □ COM+ Network Access
- ☑ Core Networking
- □ Distributed Transaction Coordinator
- ☑ ESRS FTP
- ☑ ESRS FTP
- ☑ ESRS FTP
- ☑ ESRS FTP
- ☑ ESRS FTP
- ☑ ESRS FTP
- ☑ ESRS FTP
- ☑ ESRS FTP
- ☑ ESRS FTP

□ Notify me when Windows Firewall blocks a new program

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.


Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: ESRS FTP

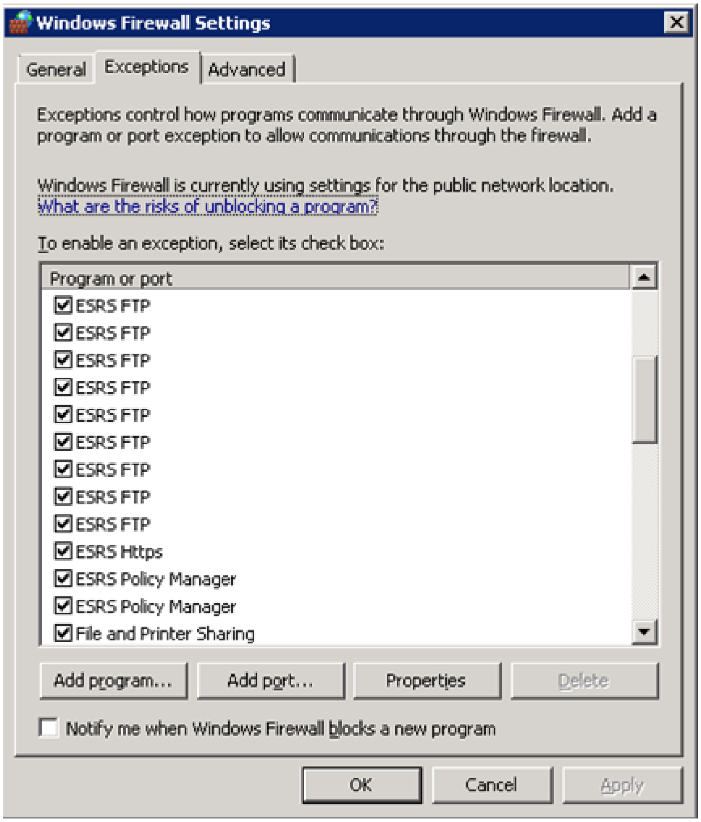
Port number: 5400

Protocol: ● TCP ○ UDP

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.



Windows Firewall Settings

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port
☑ ESRS FTP
☑ ESRS FTP
☑ ESRS FTP
☑ ESRS FTP
☑ ESRS FTP
☑ ESRS FTP
☑ ESRS FTP
☑ ESRS FTP
☑ ESRS FTP
☑ ESRS Https
☑ ESRS Policy Manager
☑ ESRS Policy Manager
☑ File and Printer Sharing

□ Notify me when Windows Firewall blocks a new program

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 Server 2008 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!
```

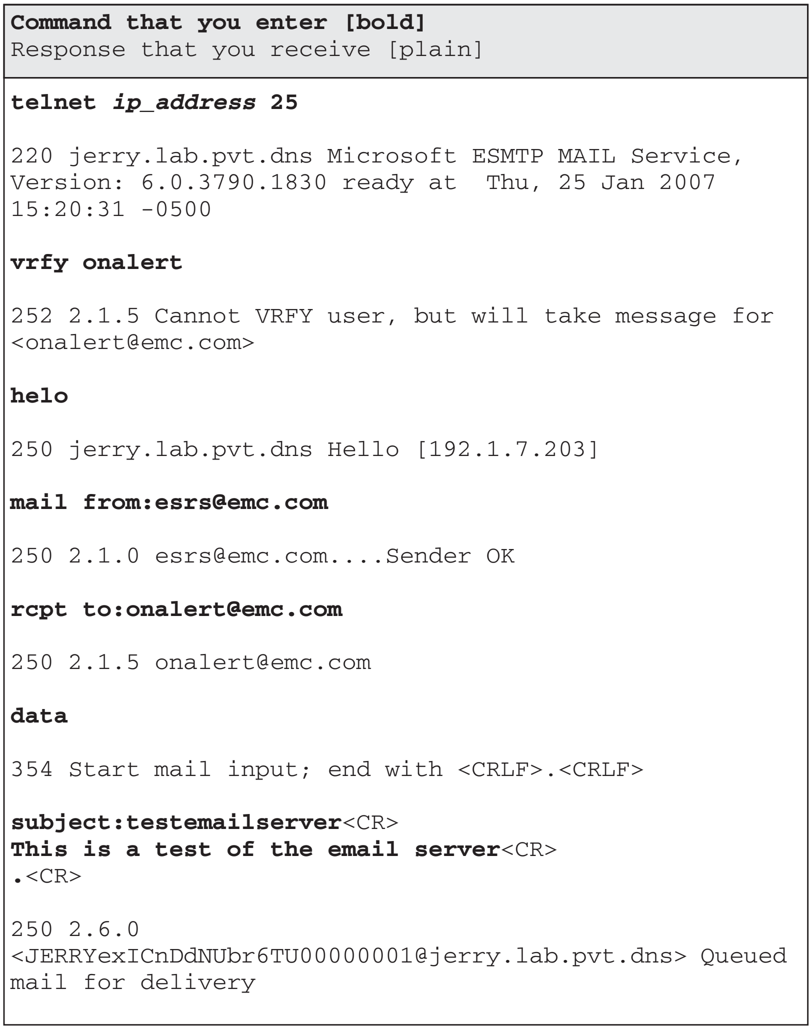
Testing SMTP from another host

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.



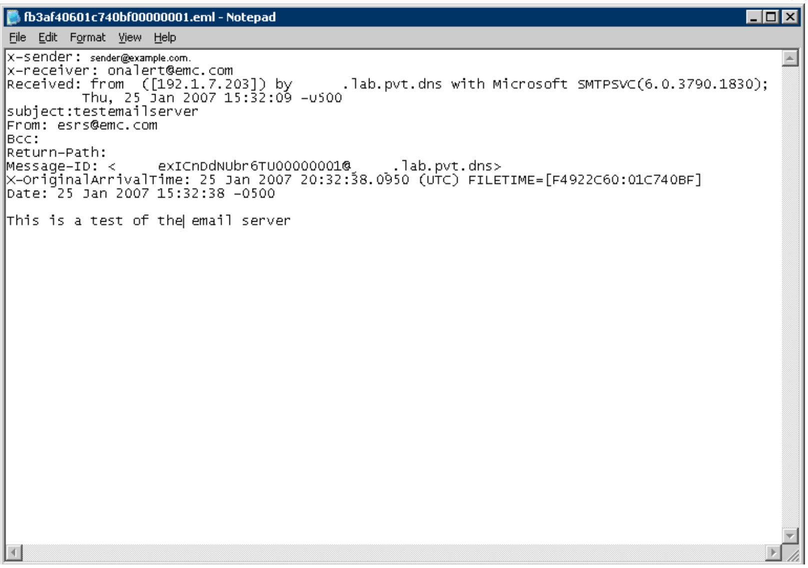
```
Command that you enter [bold]
Response that you receive [plain]

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.


fb3af40601c740bf00000001.eml - Notepad
File Edit Format View Help

```
x-sender: sender@example.com.
x-receiver: onalert@emc.com
Received: from  ([192.1.7.203]) by       .lab.pvt.dns with Microsoft SMTPSVC(6.0.3790.1830);
         Thu, 25 Jan 2007 15:32:09 -u500
subject:testemailserver
From: esrs@emc.com
Bcc:
Return-Path:
Message-ID: <     exICnDdNUbr6TU00000001@_     .lab.pvt.dns>
X-OriginalArrivalTime: 25 Jan 2007 20:32:38.0950 (UTC) FILETIME=[F4922C60:01C740BF]
Date: 25 Jan 2007 15:32:38 -0500

This is a test of the email server
```

Figure 74 **E-mail server test**

6. Close the email.
7. Delete the email from the directory.

This completes this test.

How to configure OS (IIS, FTP and SMTP, and Windows Firewall with Advanced Security) on Windows 2008 R2

This process will configure Windows 2008 R2 (IIS 7.5) or Windows 2008 R1 with IIS 7.5 FTP Add-in.

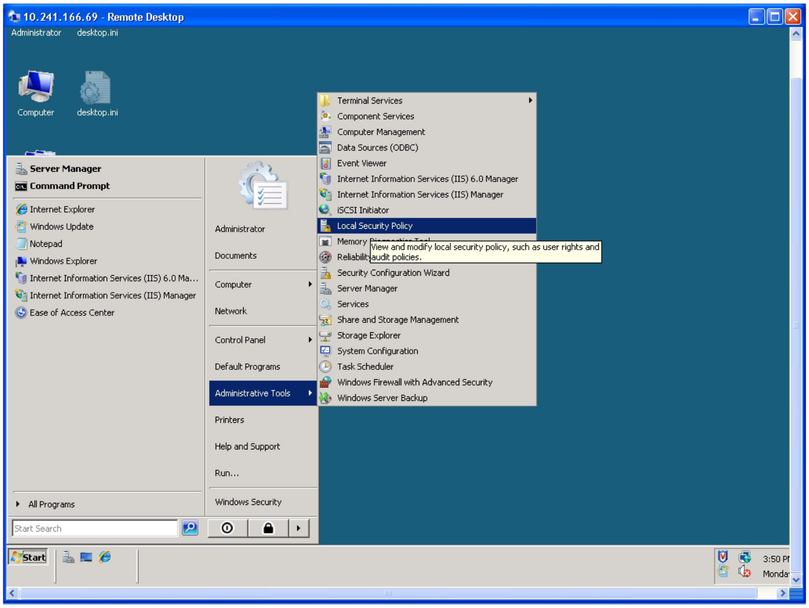
Create Users

1. Create ESRS user accounts and set passwords:

   a. Windows 2008 by default enforces complex password rules. The ESRS user accounts (Onalert & ESRSConfig) do NOT conform to the complex password requirements. In order to support Legacy devices that do not permit reconfiguration of ConnectEMC or SWDialer or have the default values hard coded you must reset Local Security Policy to not enforce password complexity rules during the creation of these Local Accounts. After the passwords have been set you can revert to the default Local Security Settings.

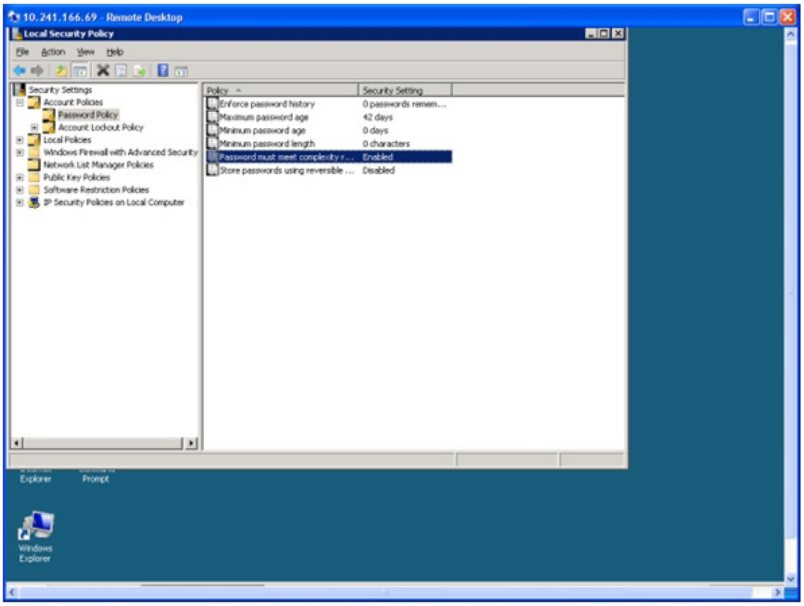
   Note: SDOU Policies may not permit this action if the Server is joined to a Domain.

   b. From the **Start** menu, point to **Administrative Tools** and click **Local Security Policy**.



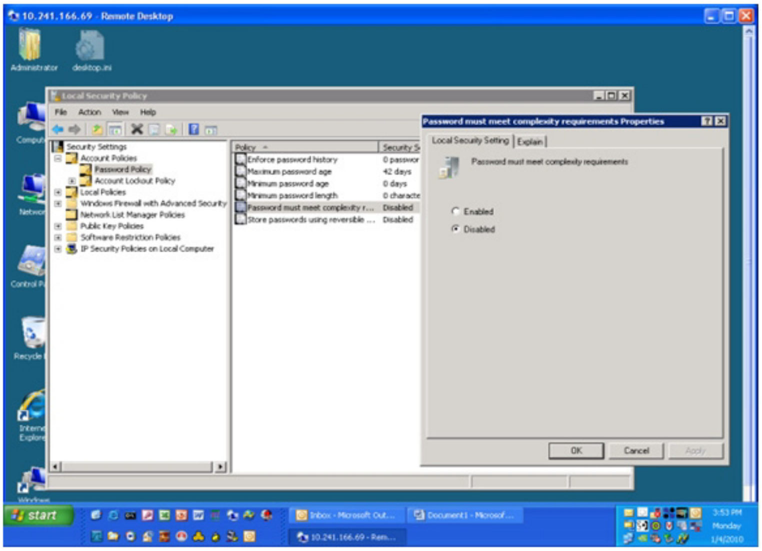
View and modify local security policy, such as user rights and audit policies.

c. Click **Account Policy** and then click **Password Policy**.



Policy	Security Setting
Enforce password history	0 passwords remem...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity r...	Enabled
Store passwords using reversible ...	Disabled

d. Select **Disable**. Click **Apply** then **OK**. Close the Local Security Setting box.



10.241.166.69 - Remote Desktop
Administrator
desktop.ini
Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
IP Security Policies on Local Computer
Password must meet complexity requirements Properties
Local Security Setting
Explain
OK
Cancel
Apply
start

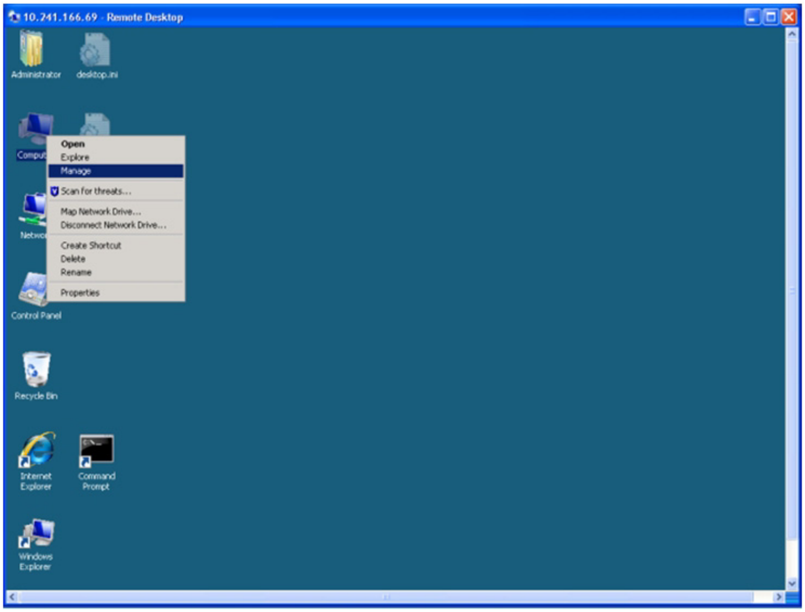
Policy	Security S
Enforce password history	0 passwor
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characte
Password must meet complexity r...	Disabled
Store passwords using reversible ...	Disabled

Password must meet complexity requirements

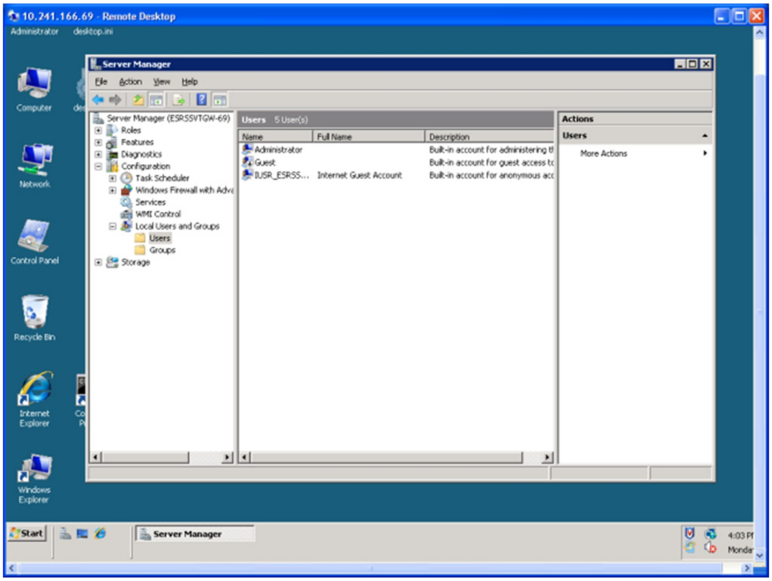
○ Enabled

● Disabled

e. Right-click on My Computer and select **Manage**.



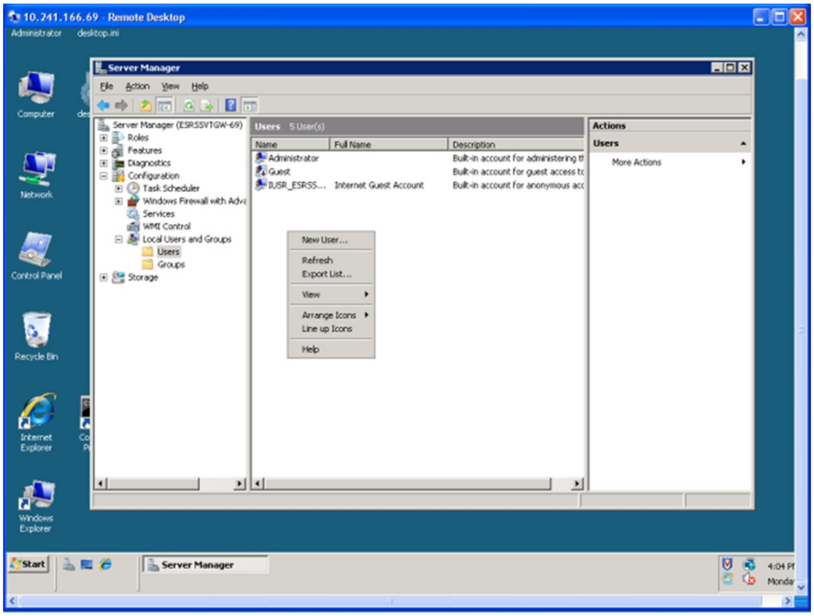
f. Expand the Configuration selection, and select **Local Users and Groups**. Click on the **Users** folder.



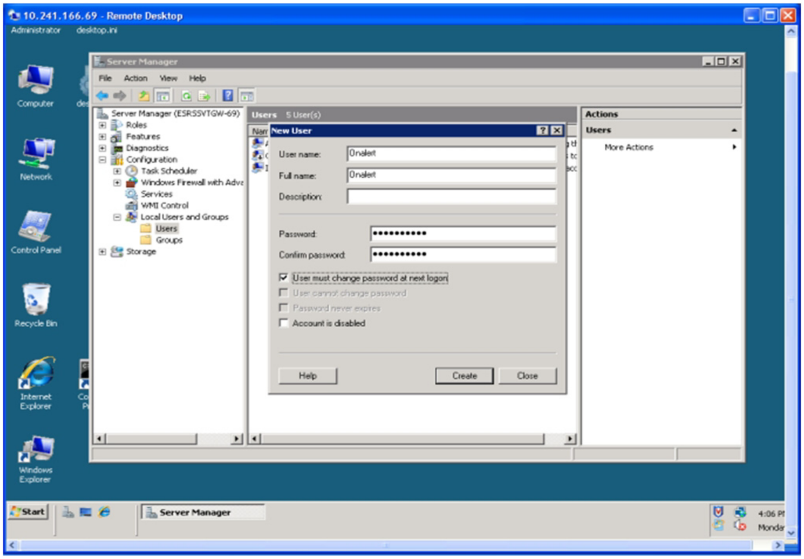
Users 5 User(s)

Name	Full Name	Description
Administrator		Built-in account for administering tl
Guest		Built-in account for guest access tc
IUSR_ESRSS...	Internet Guest Account	Built-in account for anonymous acc

g. Right click and create the **Onalert** and **ESRSConfig** users, and set the default passwords.



h. Uncheck **User must change password at next logon**.



User name: Onalert

Full name: Onalert

Description:

Password: •••••••••••

Confirm password: •••••••••••

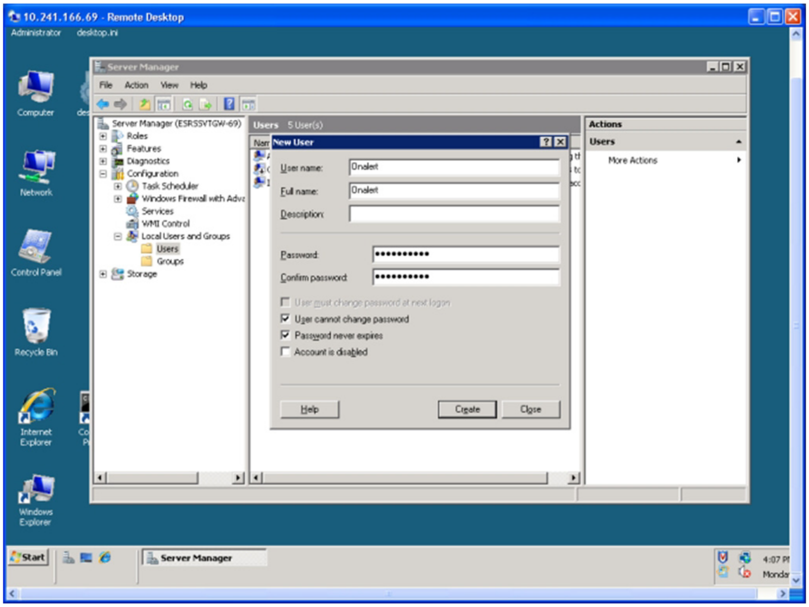
☑ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

i. Check **Password never expires** and **User can not change password**.



User name: Onalert

Full name: Onalert

Description:

Password: •••••••••••

Confirm password: •••••••••••

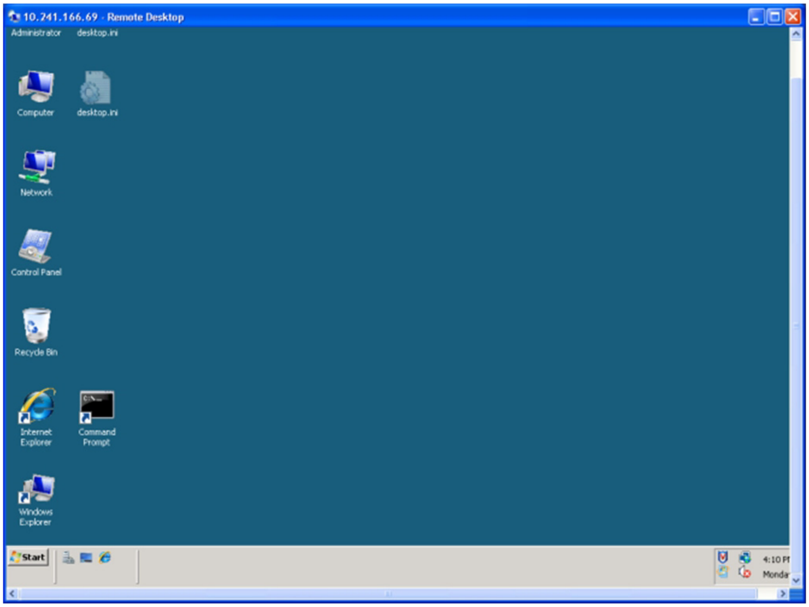
☐ User must change password at next logon

☑ User cannot change password

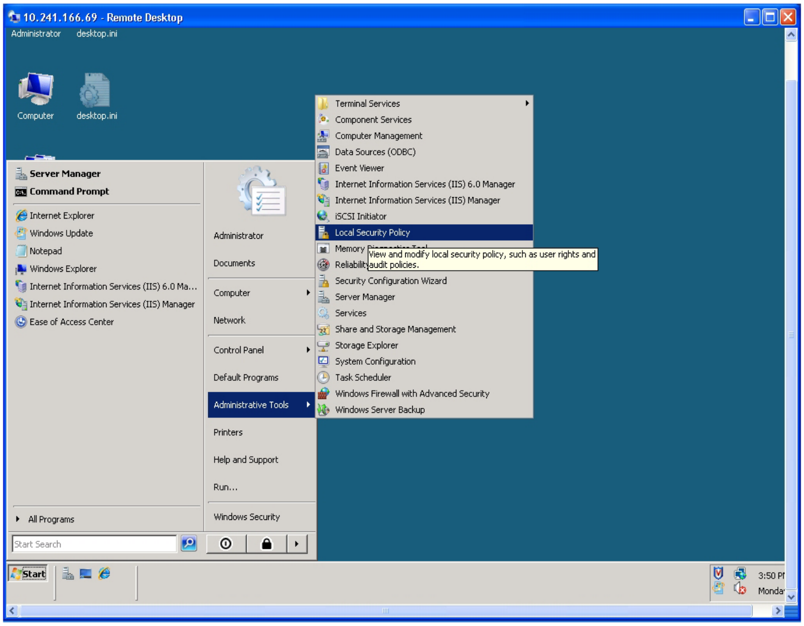
☑ Password never expires

☐ Account is disabled

j. Click **Close** and then close the Server Manager.

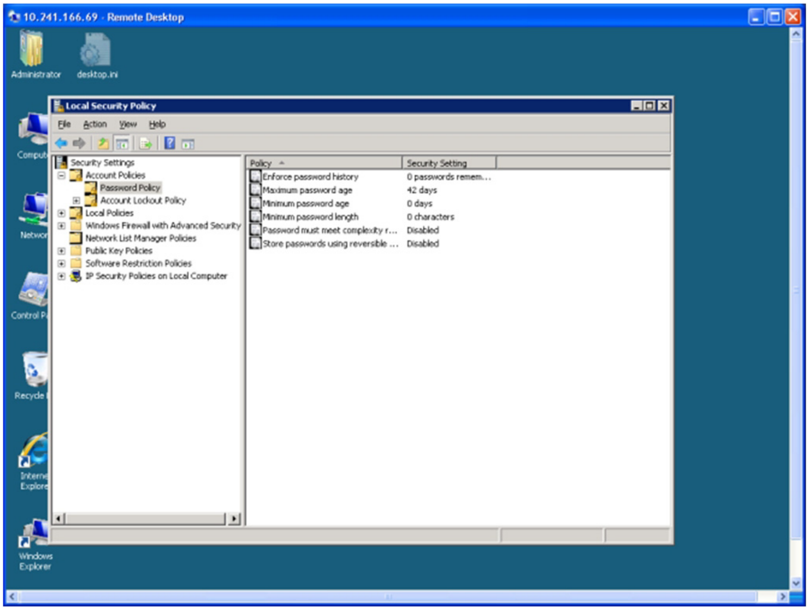


k. To Re-enable Default Complex Password Requirement, go to **Start > Administrative Tools > Local Security Policy.**



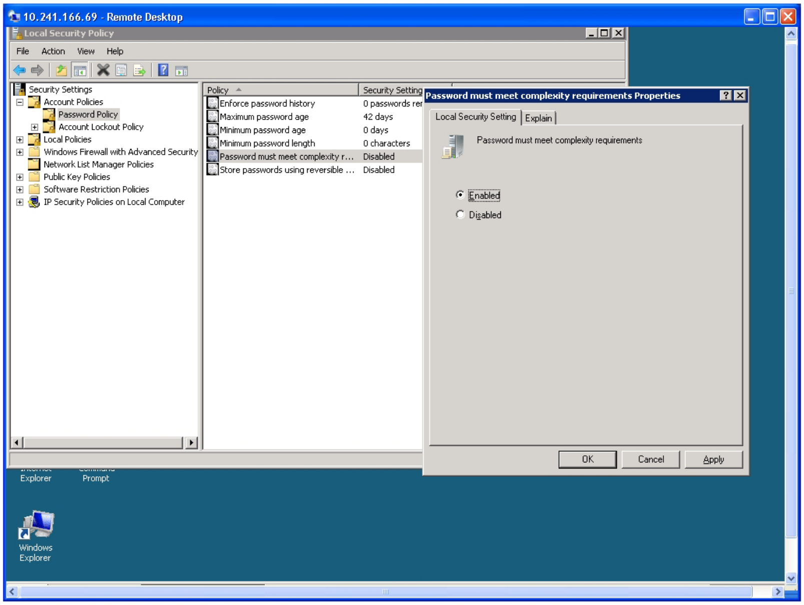
View and modify local security policy, such as user rights and audit policies.

2. Go to **Account Policy > Password Policy**.



Policy	Security Setting
Enforce password history	0 passwords remem...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity r...	Disabled
Store passwords using reversible ...	Disabled

3. Select **Password must meet complexity requirement**.



Policy	Security Setting
Enforce password history	0 passwords rer
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity r...	Disabled
Store passwords using reversible ...	Disabled

Password must meet complexity requirements Properties

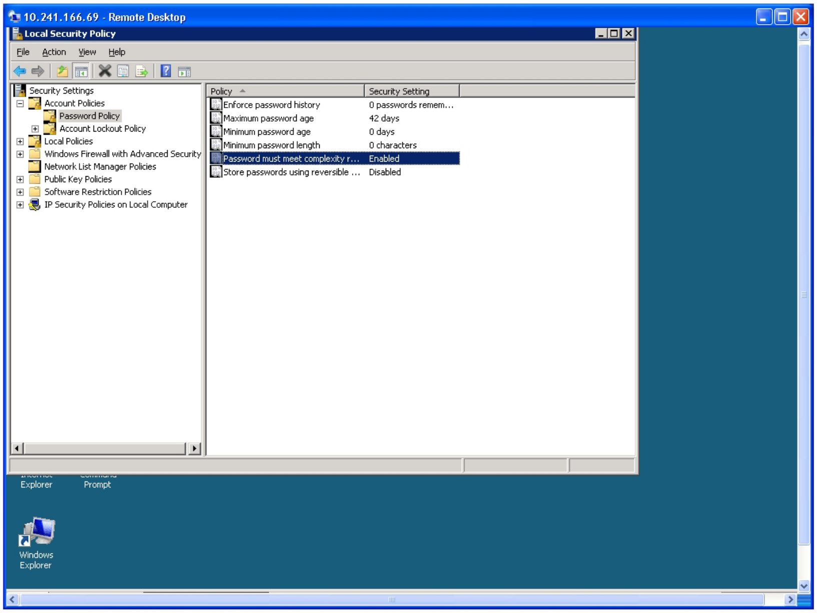
Password must meet complexity requirements

● Enabled

○ Disabled

4. Select **Enable**. Click **Apply** then **OK**.

5. Close the Local Security Setting box.



Policy	Security Setting
Enforce password history	0 passwords remem...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity r...	Enabled
Store passwords using reversible ...	Disabled

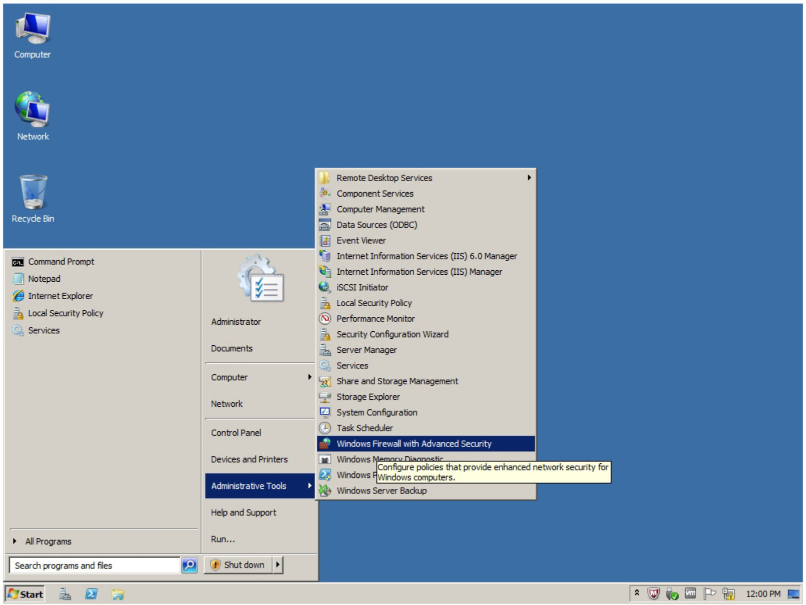
6. Configuration is complete.

Install IIS and FTP and add the SMTP Feature

This section describes how to install IIS and FTP, and add the SMTP feature.

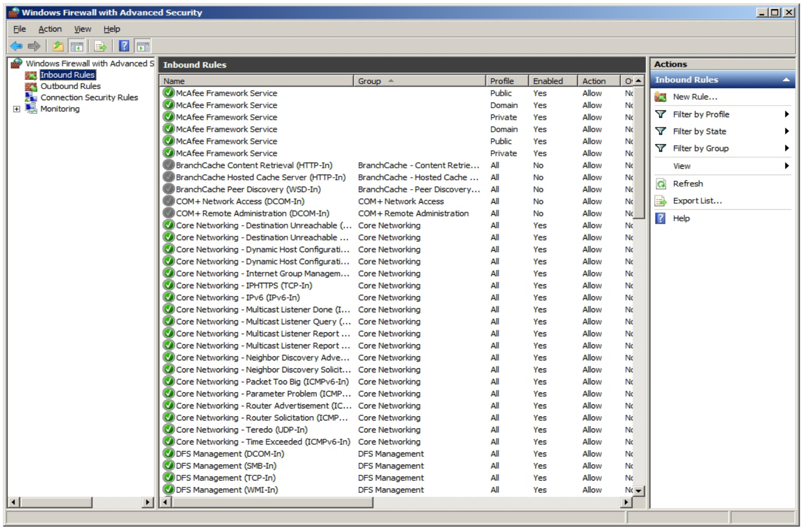
1. Configure Windows Firewall both inbound and outbound for ESRS Use (Including rules for Policy Manager if Collocated)

2. Open Windows Firewall with Advanced Security (Start\Administrative Tools\ Windows Firewall with Advanced Security)



Configure policies that provide enhanced network security for Windows computers.

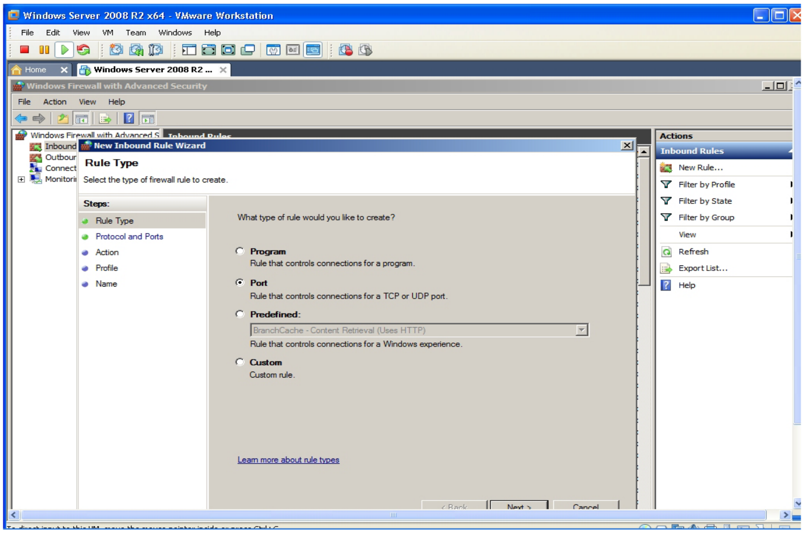
3. In the left pane, select **Inbound Rules**.



Inbound Rules

Name	Group	Profile	Enabled	Action	O
McAfee Framework Service		Public	Yes	Allow	Nc
McAfee Framework Service		Domain	Yes	Allow	Nc
McAfee Framework Service		Private	Yes	Allow	Nc
McAfee Framework Service		Domain	Yes	Allow	Nc
McAfee Framework Service		Public	Yes	Allow	Nc
McAfee Framework Service		Private	Yes	Allow	Nc
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retrie...	All	No	Allow	Nc
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache ...	All	No	Allow	Nc
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discovery...	All	No	Allow	Nc
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow	Nc
COM+ Remote Administration (DCOM-In)	COM+ Remote Administration	All	No	Allow	Nc
Core Networking - Destination Unreachable (...	Core Networking	All	Yes	Allow	Nc
Core Networking - Destination Unreachable ...	Core Networking	All	Yes	Allow	Nc
Core Networking - Dynamic Host Configurati...	Core Networking	All	Yes	Allow	Nc
Core Networking - Dynamic Host Configurati...	Core Networking	All	Yes	Allow	Nc
Core Networking - Internet Group Managem...	Core Networking	All	Yes	Allow	Nc
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	Nc
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	Nc
Core Networking - Multicast Listener Done (I...	Core Networking	All	Yes	Allow	Nc
Core Networking - Multicast Listener Query (...	Core Networking	All	Yes	Allow	Nc
Core Networking - Multicast Listener Report ...	Core Networking	All	Yes	Allow	Nc
Core Networking - Multicast Listener Report ...	Core Networking	All	Yes	Allow	Nc
Core Networking - Neighbor Discovery Adve...	Core Networking	All	Yes	Allow	Nc
Core Networking - Neighbor Discovery Solicit...	Core Networking	All	Yes	Allow	Nc
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes	Allow	Nc
Core Networking - Parameter Problem (ICMP...	Core Networking	All	Yes	Allow	Nc
Core Networking - Router Advertisement (IC...	Core Networking	All	Yes	Allow	Nc
Core Networking - Router Solicitation (ICMP...	Core Networking	All	Yes	Allow	Nc
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow	Nc
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes	Allow	Nc
DFS Management (DCOM-In)	DFS Management	All	Yes	Allow	Nc
DFS Management (SMB-In)	DFS Management	All	Yes	Allow	Nc
DFS Management (TCP-In)	DFS Management	All	Yes	Allow	Nc
DFS Management (WMI-In)	DFS Management	All	Yes	Allow	Nc

4. In the right pane, click **New Rule**, and when the window appears select **Port**.



Windows Server 2008 R2 x64 - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows Server 2008 R2 ...
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanced S
Inbound
Outbour
Connect
Monitori
Inbound Rules
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

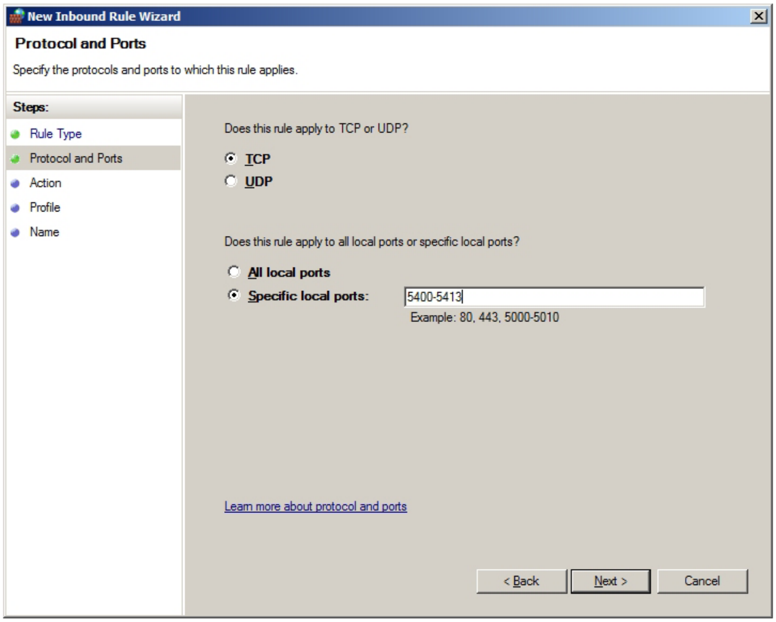
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Learn more about rule types

5. Click **Next**.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

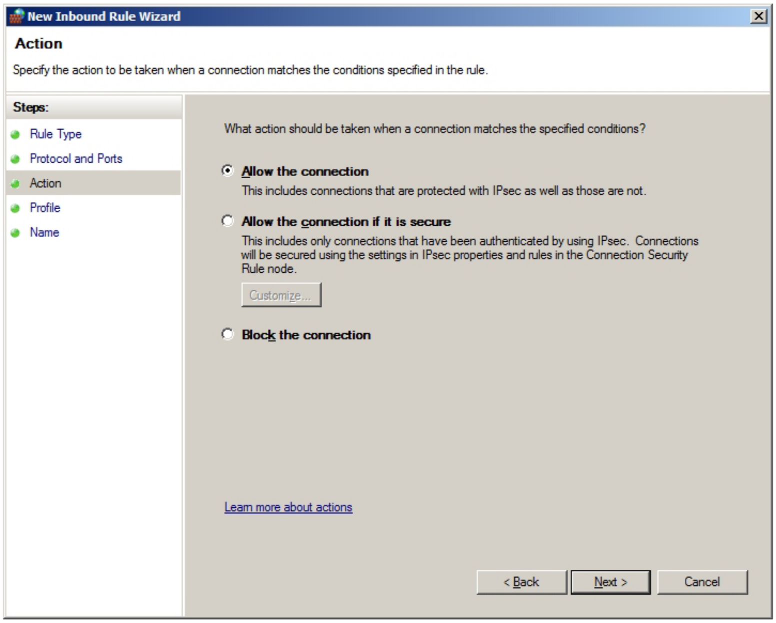
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 5400-5413

Example: 80, 443, 5000-5010

6. Fill in the Passive Port Range for ESRS FTP Gateway (5400-5413), and click **Next**.



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

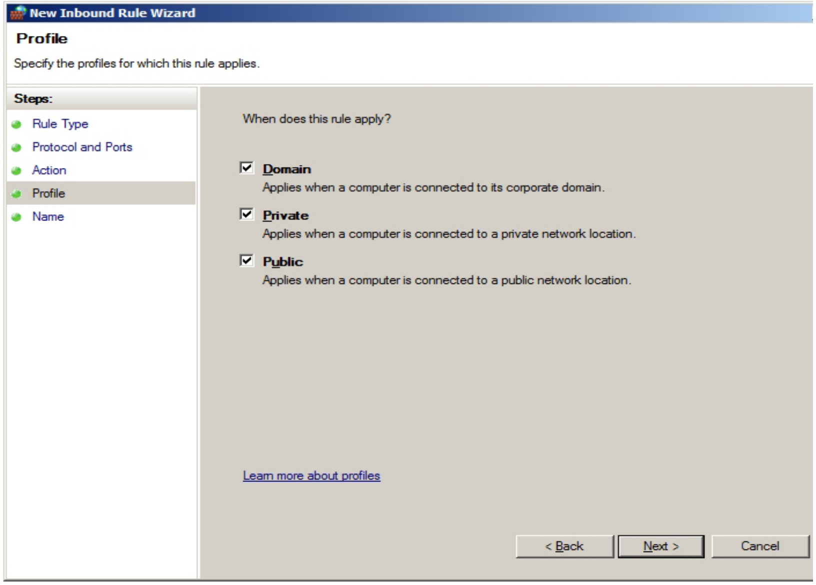
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

7. Select **Allow the connection if it is secure**, and click **Next**.



Profile

Specify the profiles for which this rule applies.

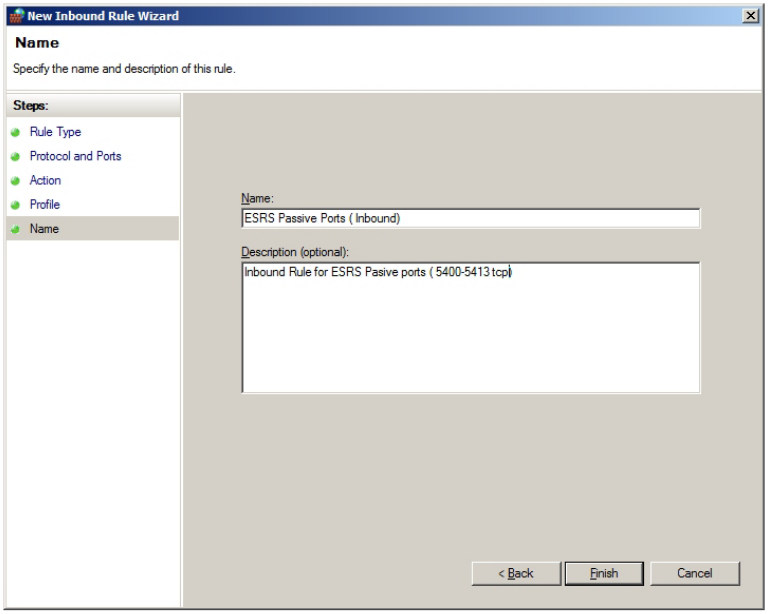
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

8. Accept the defaults, and click **Next**.



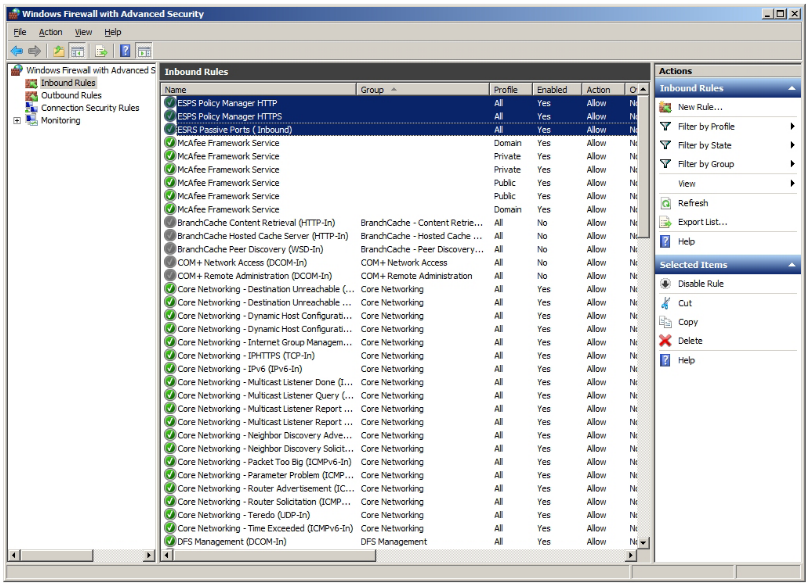
Name:
ESRS Passive Ports (Inbound)

Description (optional):
Inbound Rule for ESRS Pasive ports (5400-5413 tcp)

9. Fill in the description, and click **Finish**.

Note: Repeat this Inbound rules process for Policy Manager HTTP (port 8090 tcp) and Policy Manager HTTPS (port 8443 tcp) if Policy Manger is collocated.

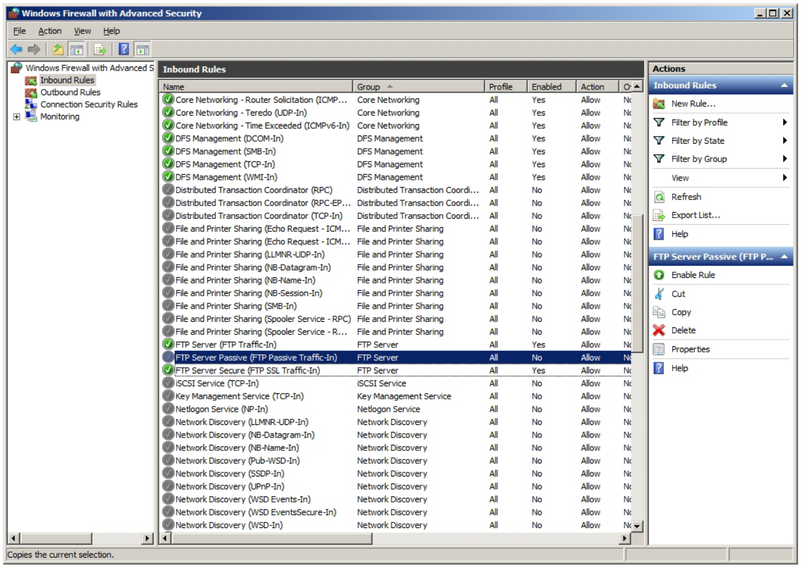
10. The inbound rules should look like the following:



Inbound Rules

Name	Group	Profile	Enabled	Action	O
ESPS Policy Manager HTTP		All	Yes	Allow	N
ESPS Policy Manager HTTPS		All	Yes	Allow	N
ESRS Passive Ports (Inbound)		All	Yes	Allow	N
McAfee Framework Service		Domain	Yes	Allow	N
McAfee Framework Service		Private	Yes	Allow	N
McAfee Framework Service		Private	Yes	Allow	N
McAfee Framework Service		Public	Yes	Allow	N
McAfee Framework Service		Public	Yes	Allow	N
McAfee Framework Service		Domain	Yes	Allow	N
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retrie...	All	No	Allow	N
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cache ...	All	No	Allow	N
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discovery...	All	No	Allow	N
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow	N
COM+ Remote Administration (DCOM-In)	COM+ Remote Administration	All	No	Allow	N
Core Networking - Destination Unreachable (...	Core Networking	All	Yes	Allow	N
Core Networking - Destination Unreachable ...	Core Networking	All	Yes	Allow	N
Core Networking - Dynamic Host Configurati...	Core Networking	All	Yes	Allow	N
Core Networking - Dynamic Host Configurati...	Core Networking	All	Yes	Allow	N
Core Networking - Internet Group Managem...	Core Networking	All	Yes	Allow	N
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	N
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	N
Core Networking - Multicast Listener Done (I...	Core Networking	All	Yes	Allow	N
Core Networking - Multicast Listener Query (...	Core Networking	All	Yes	Allow	N
Core Networking - Multicast Listener Report ...	Core Networking	All	Yes	Allow	N
Core Networking - Multicast Listener Report ...	Core Networking	All	Yes	Allow	N
Core Networking - Neighbor Discovery Adve...	Core Networking	All	Yes	Allow	N
Core Networking - Neighbor Discovery Solicit...	Core Networking	All	Yes	Allow	N
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes	Allow	N
Core Networking - Parameter Problem (ICMP...	Core Networking	All	Yes	Allow	N
Core Networking - Router Advertisement (IC...	Core Networking	All	Yes	Allow	N
Core Networking - Router Solicitation (ICMP...	Core Networking	All	Yes	Allow	N
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow	N
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes	Allow	N
DFS Management (DCOM-In)	DFS Management	All	Yes	Allow	N

11. In the Inbound rules, ***disable*** default **FTP Server Passive (FTP Passive Traffic-In)**.

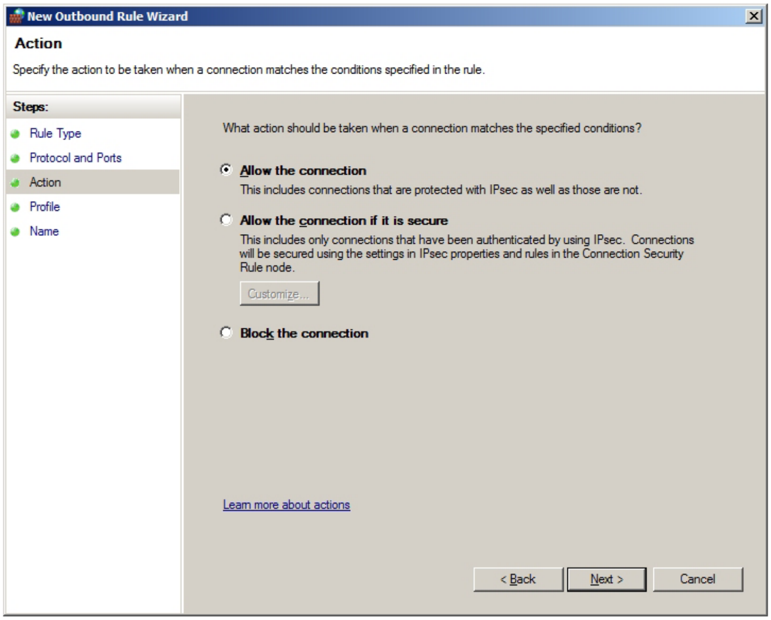


Inbound Rules

Name	Group	Profile	Enabled	Action	O
Core Networking - Router Solicitation (ICMP...	Core Networking	All	Yes	Allow	N
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow	N
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes	Allow	N
DFS Management (DCOM-In)	DFS Management	All	Yes	Allow	N
DFS Management (SMB-In)	DFS Management	All	Yes	Allow	N
DFS Management (TCP-In)	DFS Management	All	Yes	Allow	N
DFS Management (WMI-In)	DFS Management	All	Yes	Allow	N
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coordi...	All	No	Allow	N
Distributed Transaction Coordinator (RPC-EP...	Distributed Transaction Coordi...	All	No	Allow	N
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coordi...	All	No	Allow	N
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	All	No	Allow	N
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	All	No	Allow	N
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	Allow	N
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	No	Allow	N
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No	Allow	N
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	No	Allow	N
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No	Allow	N
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	No	Allow	N
File and Printer Sharing (Spooler Service - R...	File and Printer Sharing	All	No	Allow	N
FTP Server (FTP Traffic-In)	FTP Server	All	Yes	Allow	N
FTP Server Passive (FTP Passive Traffic-In)	FTP Server	All	No	Allow	N
FTP Server Secure (FTP SSL Traffic-In)	FTP Server	All	Yes	Allow	N
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow	N
Key Management Service (TCP-In)	Key Management Service	All	No	Allow	N
Netlogon Service (NP-In)	Netlogon Service	All	No	Allow	N
Network Discovery (LLMNR-UDP-In)	Network Discovery	All	No	Allow	N
Network Discovery (NB-Datagram-In)	Network Discovery	All	No	Allow	N
Network Discovery (NB-Name-In)	Network Discovery	All	No	Allow	N
Network Discovery (Pub-WSD-In)	Network Discovery	All	No	Allow	N
Network Discovery (SSDP-In)	Network Discovery	All	No	Allow	N
Network Discovery (UPnP-In)	Network Discovery	All	No	Allow	N
Network Discovery (WSD Events-In)	Network Discovery	All	No	Allow	N
Network Discovery (WSD EventsSecure-In)	Network Discovery	All	No	Allow	N
Network Discovery (WSD-In)	Network Discovery	All	No	Allow	N

Copies the current selection.

12. Create an Outbound Passive Ports rule for ESRS by selecting Outbound in the left panel and follow the same process as above using the Outbound Rules wizard. Make sure to set Connection as Allowed.



New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

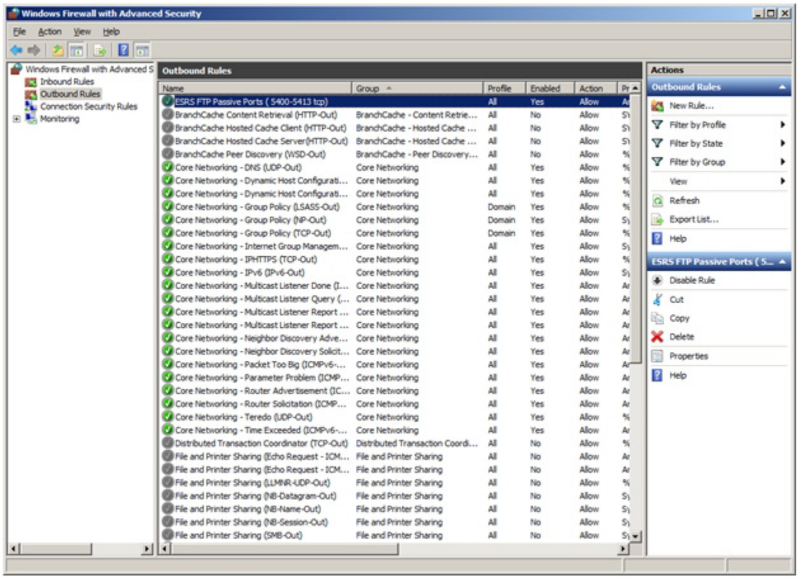
What action should be taken when a connection matches the specified conditions?

● Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

13. When completed, the Outbound rule should be as follows:



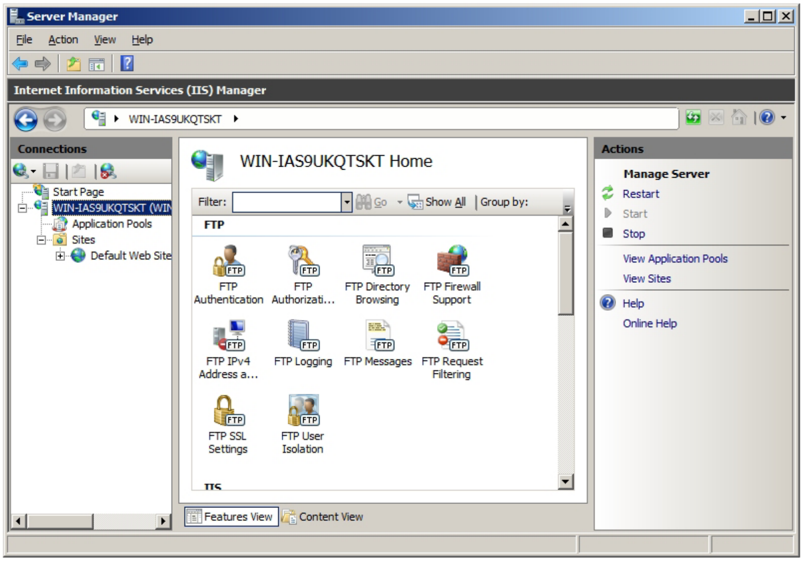
Name	Group	Profile	Enabled	Action	Pr
ESRS FTP Passive Ports (5400-5413 tcp)		All	Yes	Allow	Ar
BranchCache Content Retrieval (HTTP-Out)	BranchCache - Content Retrie...	All	No	Allow	Sy
BranchCache Hosted Cache Client (HTTP-Out)	BranchCache - Hosted Cache ...	All	No	Allow	Sy
BranchCache Hosted Cache Server(HTTP-Out)	BranchCache - Hosted Cache ...	All	No	Allow	Sy
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discovery...	All	No	Allow	%
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	%
Core Networking - Dynamic Host Configurati...	Core Networking	All	Yes	Allow	%
Core Networking - Dynamic Host Configurati...	Core Networking	All	Yes	Allow	%
Core Networking - Group Policy (LSASS-Out)	Core Networking	Domain	Yes	Allow	%
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	Sy
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	%
Core Networking - Internet Group Managem...	Core Networking	All	Yes	Allow	Sy
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	%
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	Sy
Core Networking - Multicast Listener Done (I...	Core Networking	All	Yes	Allow	Ar
Core Networking - Multicast Listener Query (...	Core Networking	All	Yes	Allow	Ar
Core Networking - Multicast Listener Report ...	Core Networking	All	Yes	Allow	Ar
Core Networking - Multicast Listener Report ...	Core Networking	All	Yes	Allow	Ar
Core Networking - Neighbor Discovery Adve...	Core Networking	All	Yes	Allow	Ar
Core Networking - Neighbor Discovery Solicit...	Core Networking	All	Yes	Allow	Ar
Core Networking - Packet Too Big (ICMPv6-...	Core Networking	All	Yes	Allow	Ar
Core Networking - Parameter Problem (ICMP...	Core Networking	All	Yes	Allow	Ar
Core Networking - Router Advertisement (IC...	Core Networking	All	Yes	Allow	Ar
Core Networking - Router Solicitation (ICMP...	Core Networking	All	Yes	Allow	Ar
Core Networking - Teredo (UDP-Out)	Core Networking	All	Yes	Allow	%
Core Networking - Time Exceeded (ICMPv6-...	Core Networking	All	Yes	Allow	Ar
Distributed Transaction Coordinator (TCP-Out)	Distributed Transaction Coordi...	All	No	Allow	%
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	All	No	Allow	Ar
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	All	No	Allow	Ar
File and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing	All	No	Allow	%
File and Printer Sharing (NB-Datagram-Out)	File and Printer Sharing	All	No	Allow	Sy
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing	All	No	Allow	Sy
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing	All	No	Allow	Sy
File and Printer Sharing (SMB-Out)	File and Printer Sharing	All	No	Allow	Sy

14. Close the Windows Firewall with Advanced Security window.

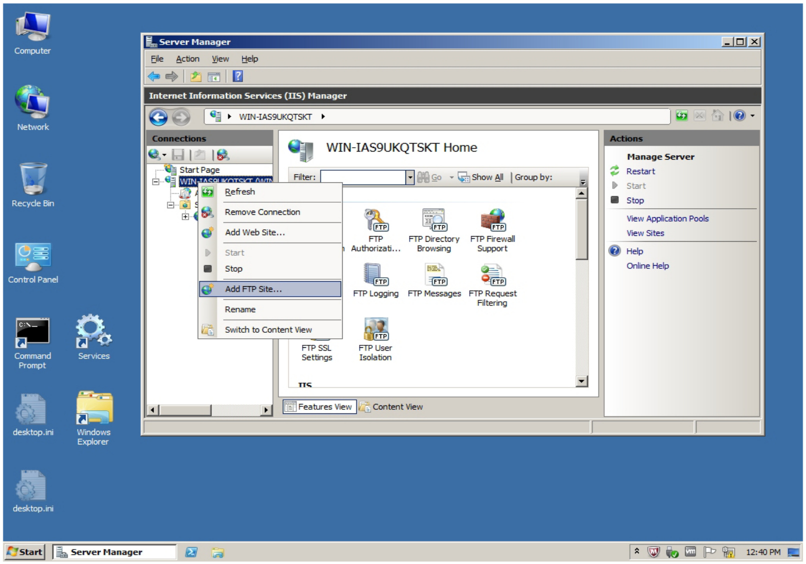
FTP Configuration (IIS 7.5) for Windows 2008 R2

To configure FTP (IIS 7.5) for Windows 2008 R2:

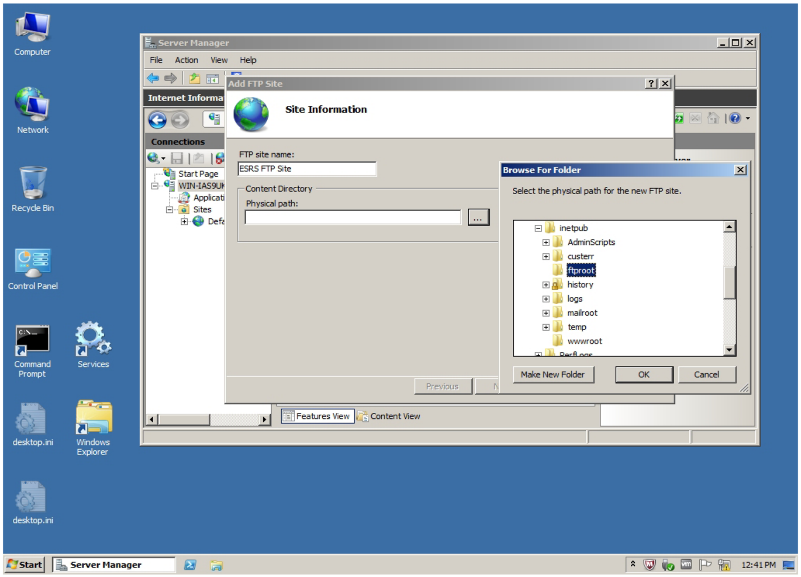
1. Open the Server Manager.



2. Right click and select **Add FTP Site.**



3. In the Add FTP Site box, type ESRS FTP Site.



Site Information

FTP site name: ESRS FTP Site

Content Directory

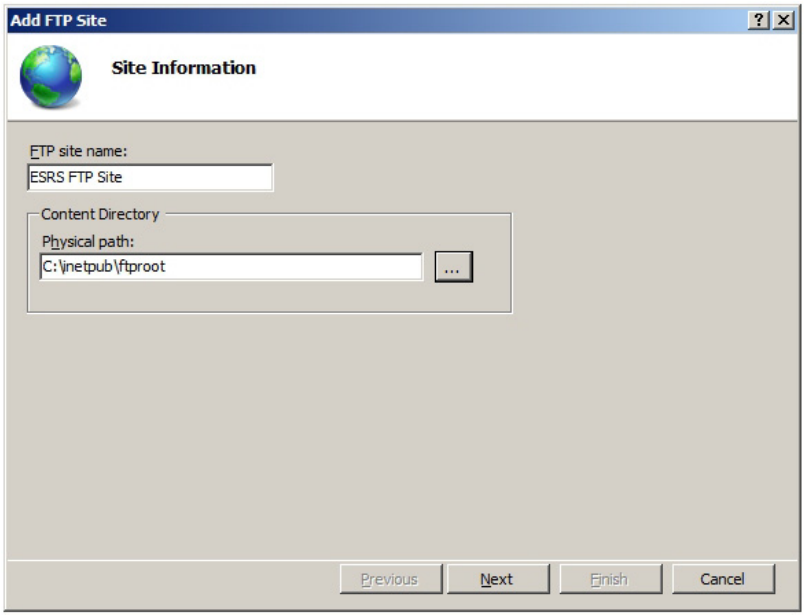
Physical path:

Browse For Folder

Select the physical path for the new FTP site.

- inetpub
  - AdminScripts
  - custerr
  - ftproot
  - history
  - logs
  - mailroot
  - temp
  - wwwroot
- PerfLogs

4. In the Physical Path field, click the browse button and select **C: \inetpub\ftproot**.

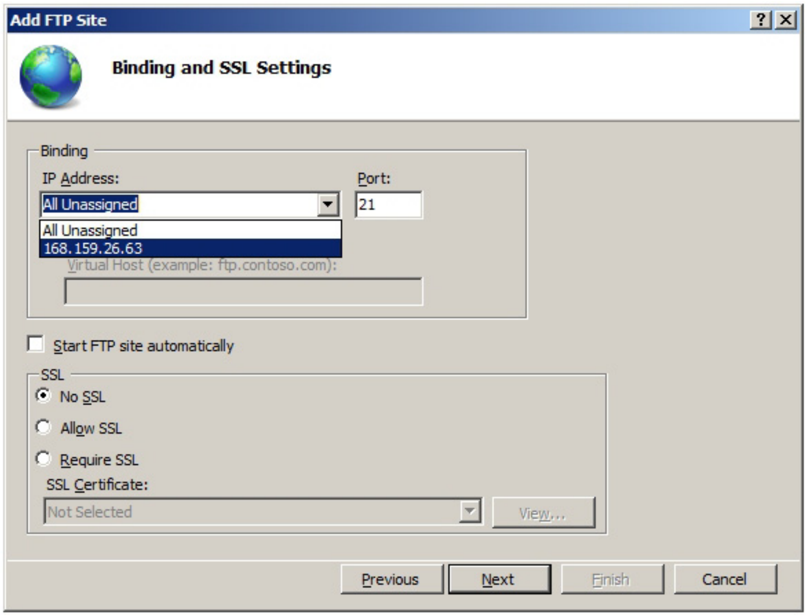


FTP site name: ESRS FTP Site

Content Directory

Physical path: C:\inetpub\ftproot

5. In the IP Address field, assign an IP address.



Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned

All Unassigned
168.159.26.63

Port: 21

Virtual Host (example: ftp.contoso.com):

□ Start FTP site automatically

SSL

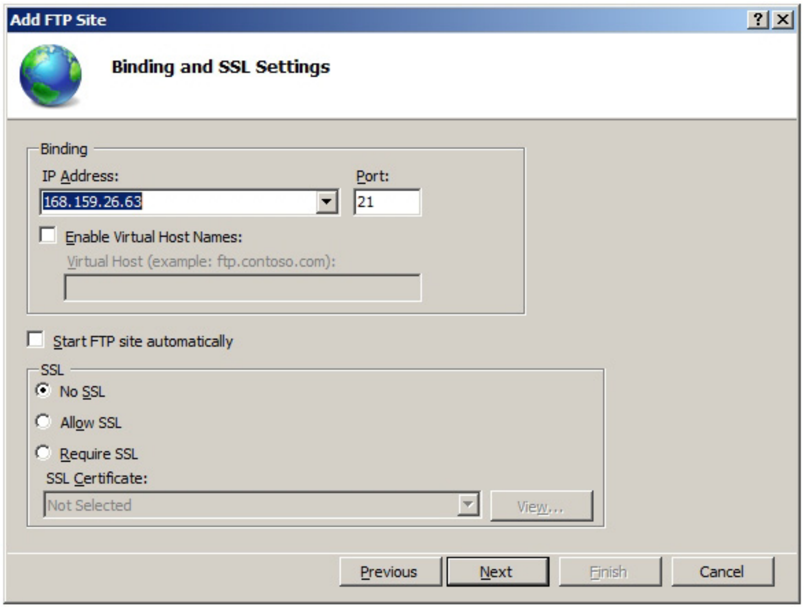
● No SSL

○ Allow SSL

○ Require SSL

SSL Certificate: Not Selected

6. Continue as follows:



Add FTP Site

Binding and SSL Settings

Binding

IP Address: 168.159.26.63

Port: 21

□ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

□ Start FTP site automatically

SSL

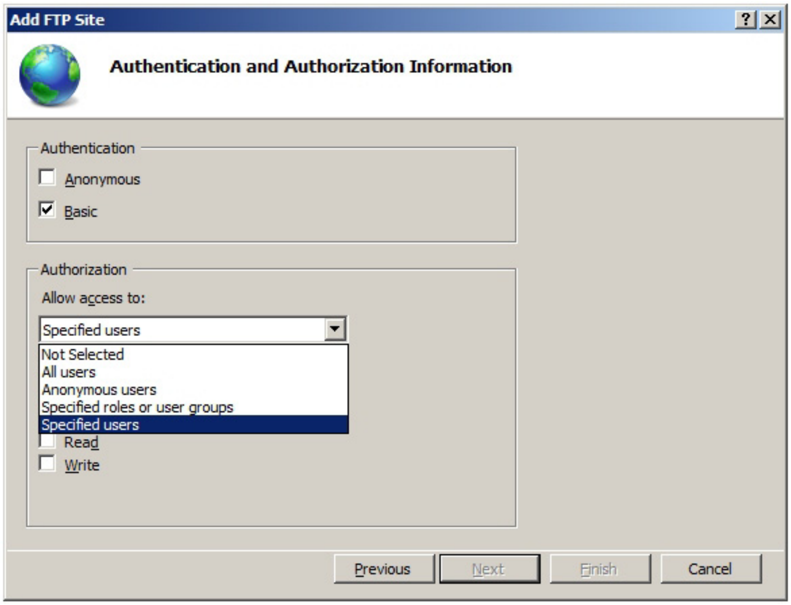
● No SSL

○ Allow SSL

○ Require SSL

SSL Certificate: Not Selected

7. Click **Next**.



Add FTP Site

Authentication and Authorization Information

Authentication

☐ Anonymous

☑ Basic

Authorization

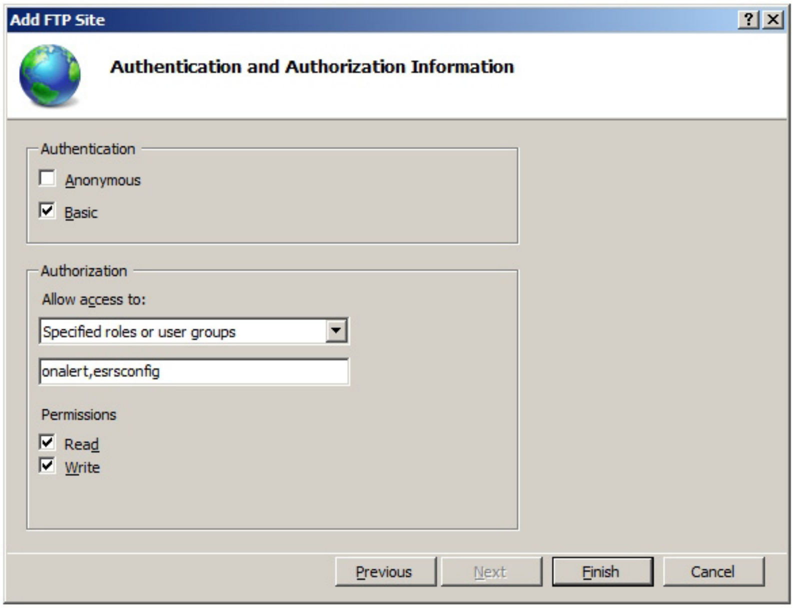
Allow access to:

Specified users

☐ Read

☐ Write

8. In the Authentication box, select **Basic**. Allow access to Specified users, and click **Next**.



Add FTP Site

Authentication and Authorization Information

Authentication

□ Anonymous

☑ Basic

Authorization

Allow access to:

Specified roles or user groups

onalert,esrsconfig

Permissions

☑ Read

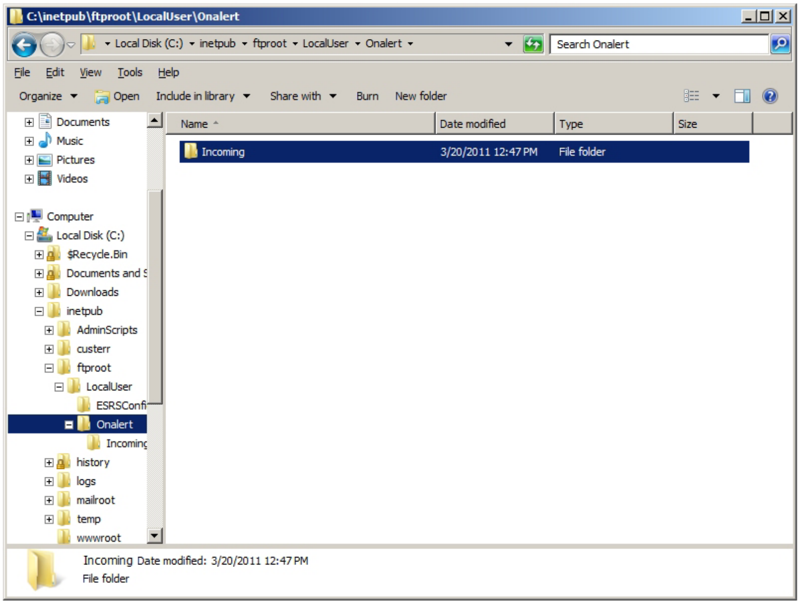
☑ Write

9. Select Specified roles or user groups, and add **onalert, esrsconfig**.
10. Click **Finish**. Configuration is complete.

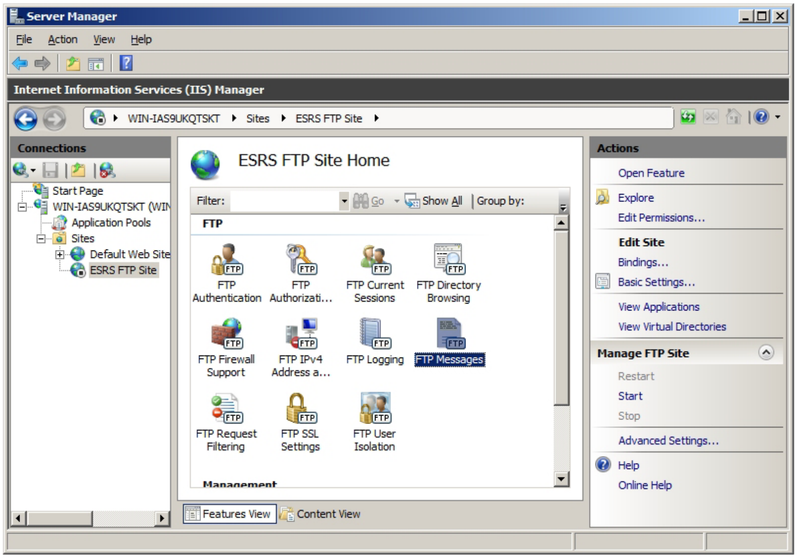
Create Directory Structure

To create the directory structure:

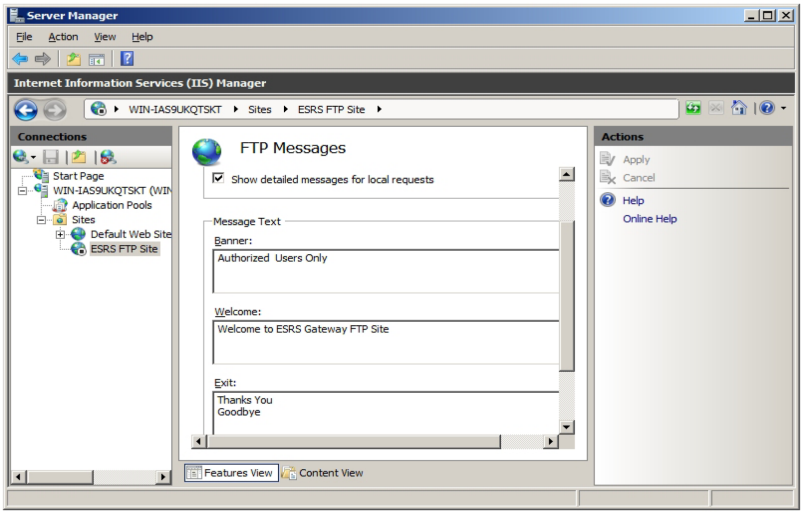
1. With Windows Explorer, create both:
   - C:\Inetpub\ftproot\localuser\Onalert\Incoming
   - C:\Inetpub\ftproot\localuser\ESRSConfig directories.



2. Continue as follows:



3. Click **FTP Messages**.



☑ Show detailed messages for local requests

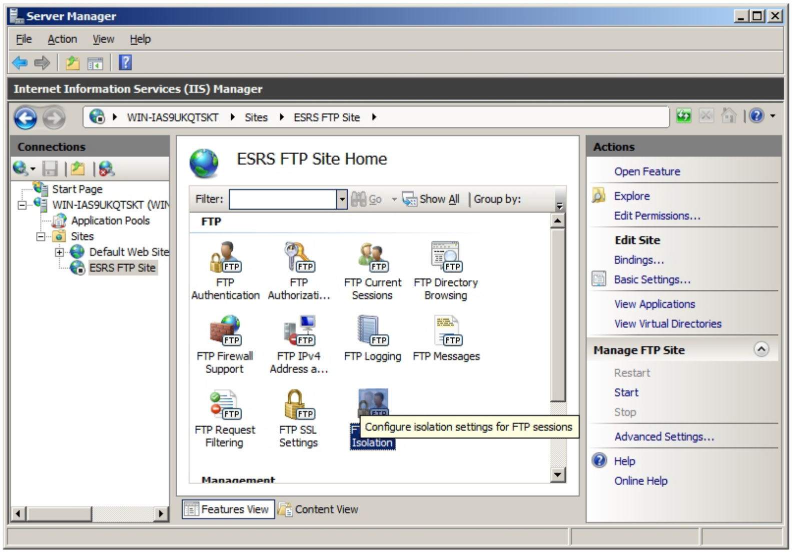
Message Text

Banner:
Authorized Users Only

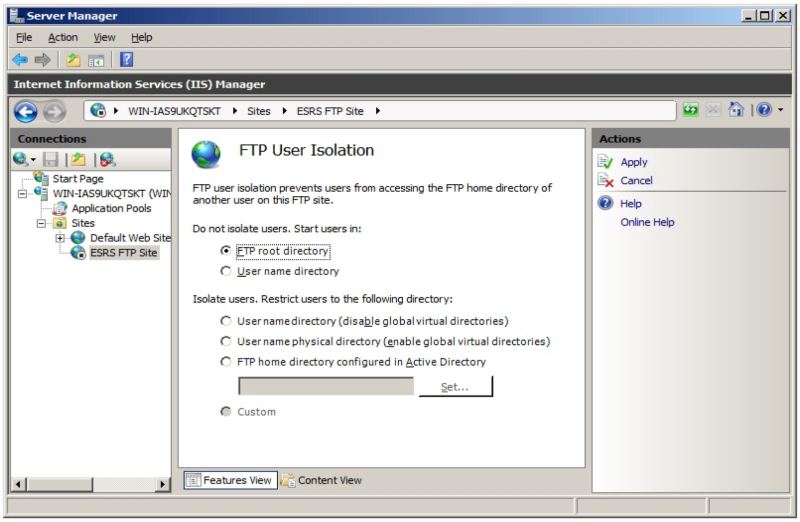
Welcome:
Welcome to ESRS Gateway FTP Site

Exit:
Thanks You
Goodbye

4. Go to the ESRS FTP Site Home:



5. Click **FTP User Isolation.**



FTP User Isolation

FTP user isolation prevents users from accessing the FTP home directory of another user on this FTP site.

Do not isolate users. Start users in:

- ● FTP root directory
- ○ User name directory

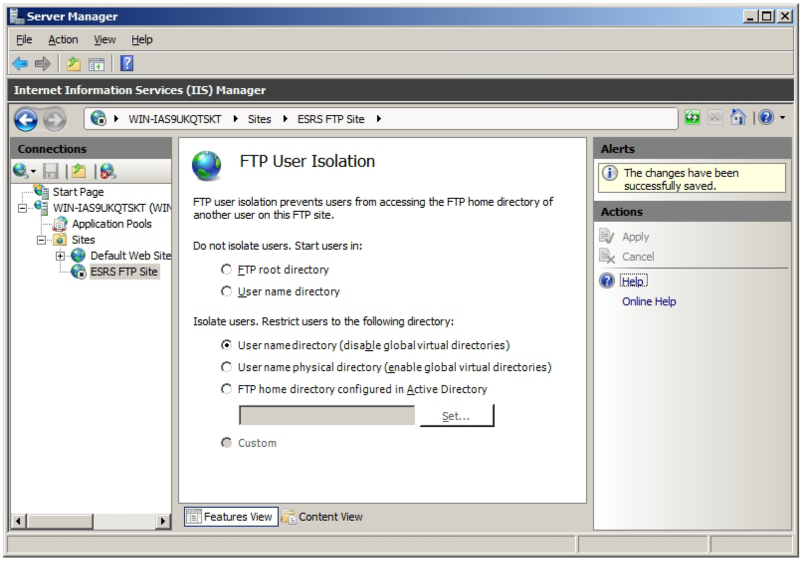
Isolate users. Restrict users to the following directory:

- ○ User name directory (disable global virtual directories)
- ○ User name physical directory (enable global virtual directories)
- ○ FTP home directory configured in Active Directory

Set...

- ○ Custom

6. Select **User name directory**.



The changes have been successfully saved.

FTP User Isolation

FTP user isolation prevents users from accessing the FTP home directory of another user on this FTP site.

Do not isolate users. Start users in:

- ○ FTP root directory
- ○ User name directory

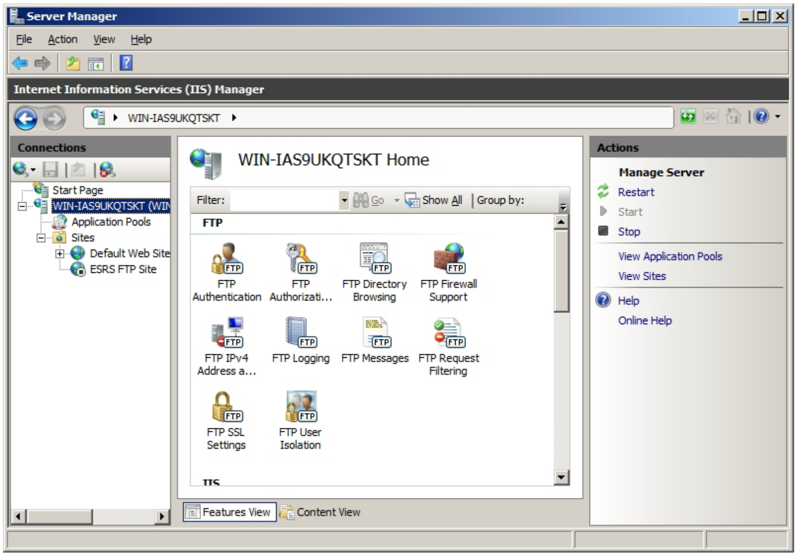
Isolate users. Restrict users to the following directory:

- ● User name directory (disable global virtual directories)
- ○ User name physical directory (enable global virtual directories)
- ○ FTP home directory configured in Active Directory

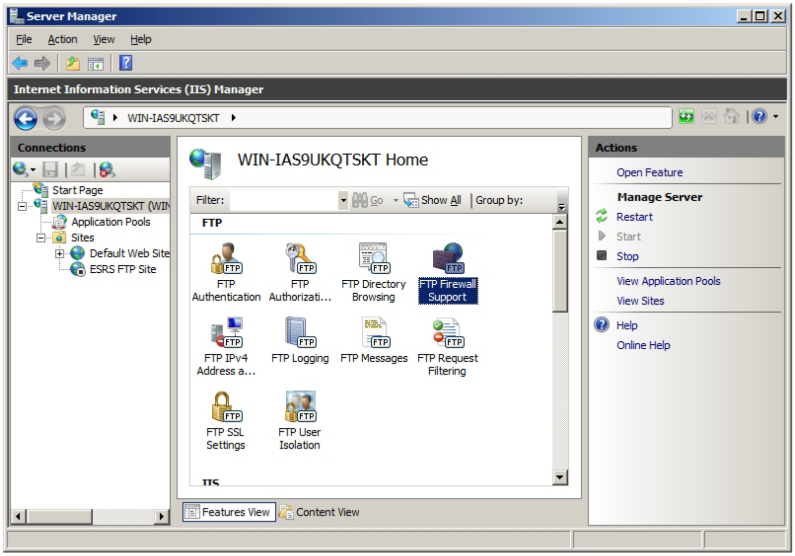
Set...

- ○ Custom

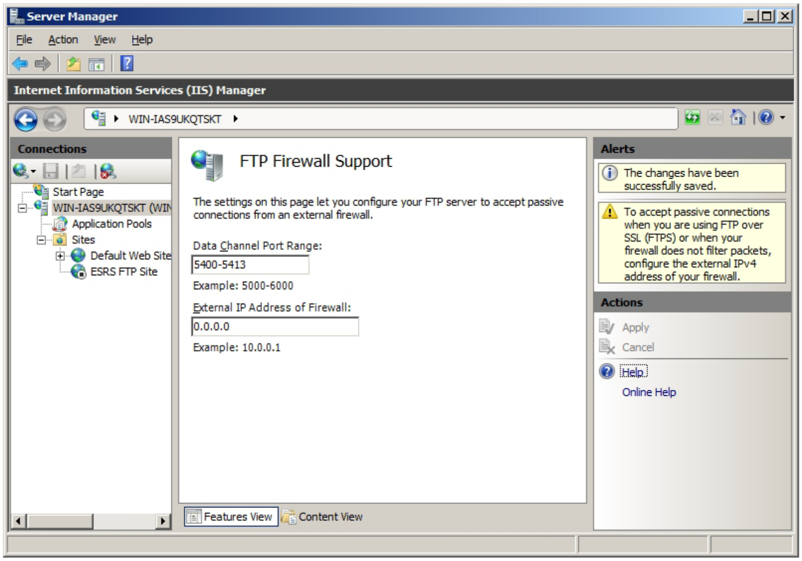
7. Go to the Server level.



8. Select **FTP Firewall Support**.



9. Set Passive port range (5400-5413) and external IP address 0.0.0.0 (this indicates any IP address).



FTP Firewall Support

The settings on this page let you configure your FTP server to accept passive connections from an external firewall.

Data Channel Port Range: 5400-5413

Example: 5000-6000

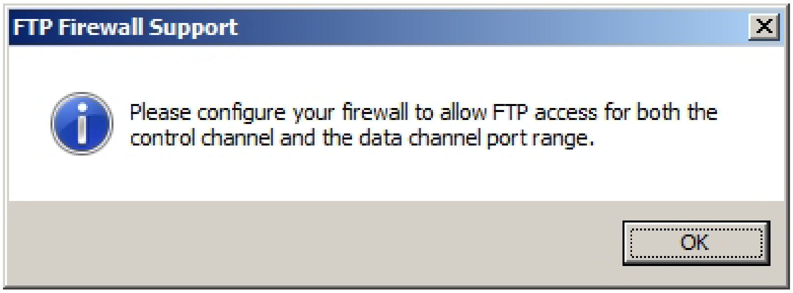
External IP Address of Firewall: 0.0.0.0

Example: 10.0.0.1

The changes have been successfully saved.

To accept passive connections when you are using FTP over SSL (FTPS) or when your firewall does not filter packets, configure the external IPv4 address of your firewall.

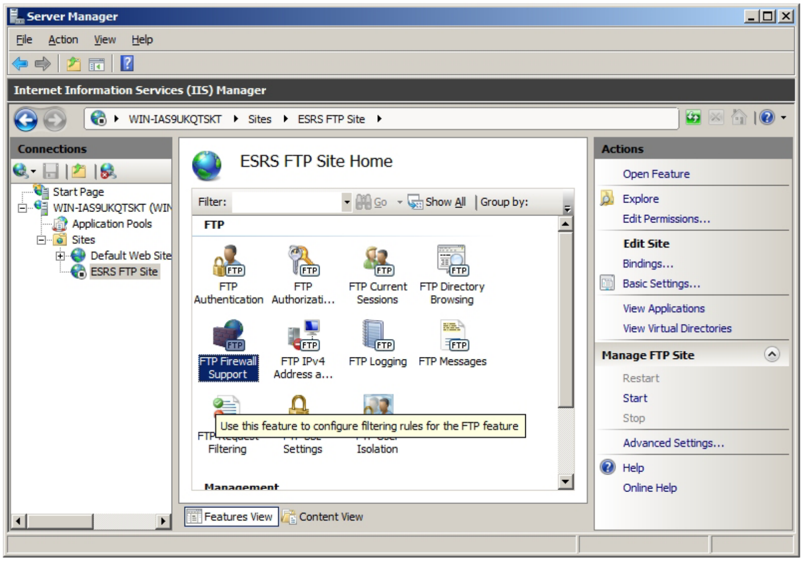
10. Click **Apply**. The FTP Firewall Support dialog appears.



Please configure your firewall to allow FTP access for both the control channel and the data channel port range.

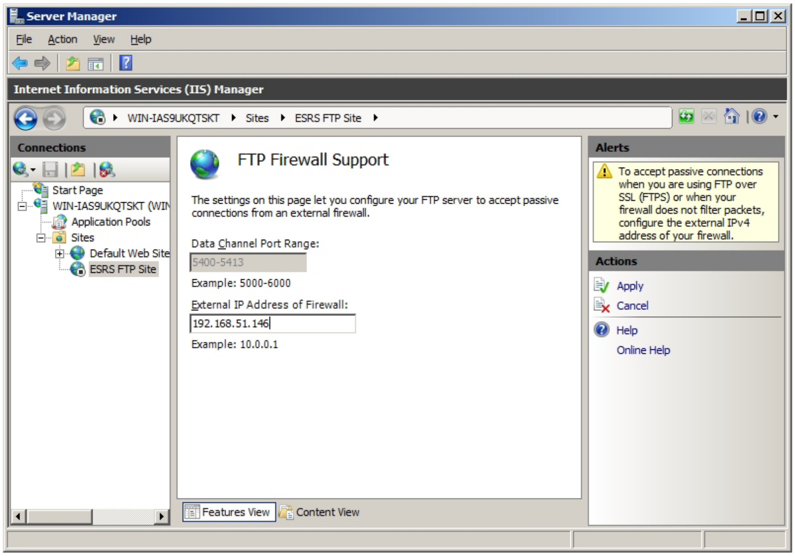
11. Click **OK** (this has been done previously).

12. Return to the FTP Site you created.



Use this feature to configure filtering rules for the FTP feature

13. Select **FTP Firewall Support**.



To accept passive connections when you are using FTP over SSL (FTPS) or when your firewall does not filter packets, configure the external IPv4 address of your firewall.

The settings on this page let you configure your FTP server to accept passive connections from an external firewall.

Data Channel Port Range: 5400-5413

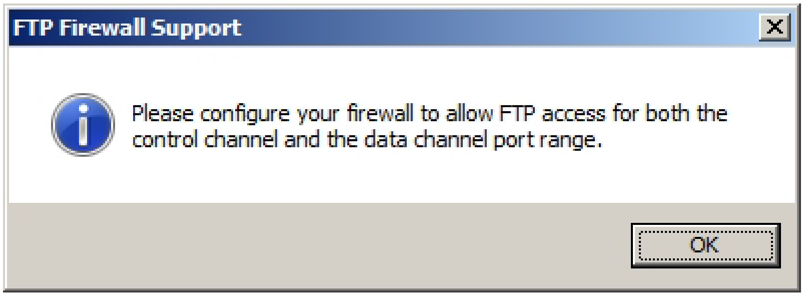
Example: 5000-6000

External IP Address of Firewall: 192.168.51.146

Example: 10.0.0.1

14. Enter the IP address of the Gateway Server. If multihomed, enter the “Internal IP address” of the Gateway Server.

15. Click **Apply**. The FTP Firewall Support dialog appears.

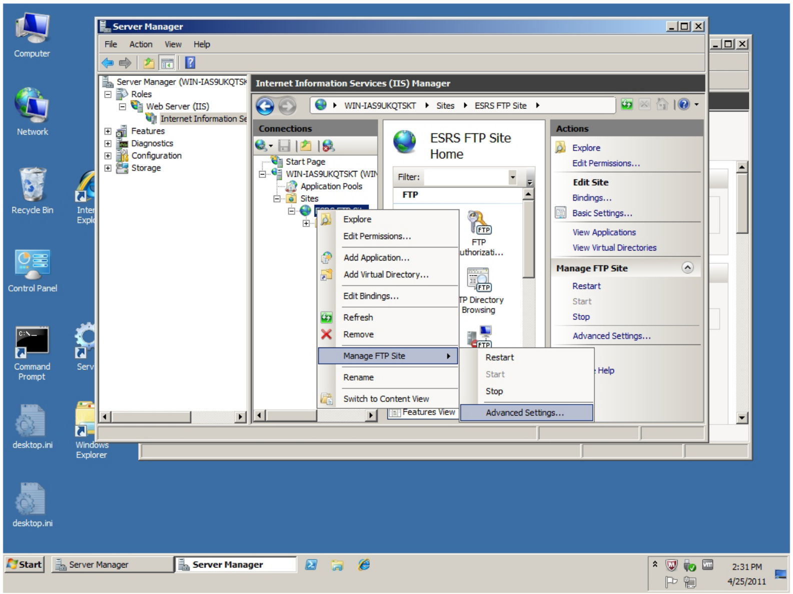


FTP Firewall Support

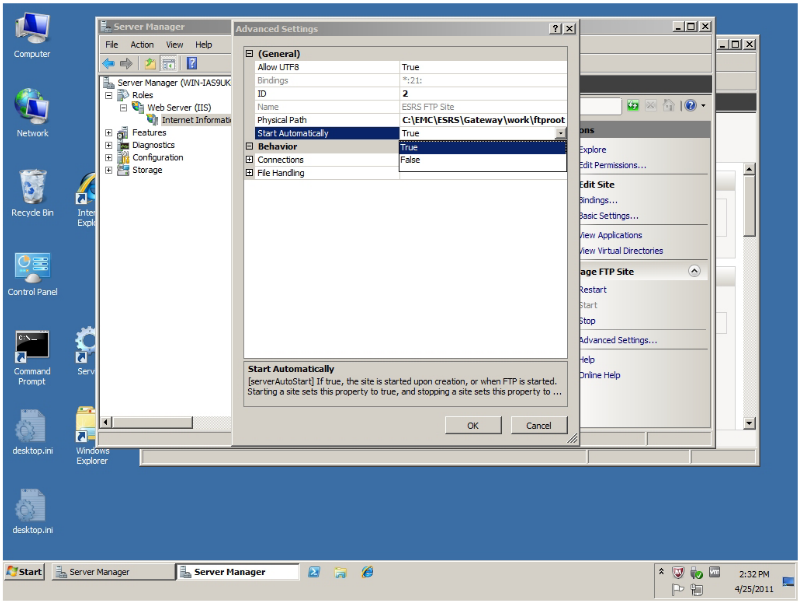
Please configure your firewall to allow FTP access for both the control channel and the data channel port range.

16. Click **OK** (this has been done previously).

17. Start the FTP site, and go to **Advanced Settings**.



18. At the Site Level. set the FTP site Auto Start to **True**.



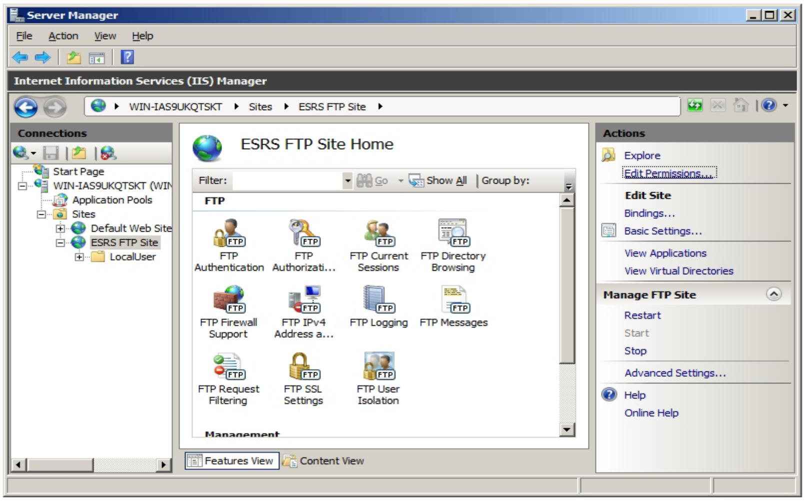
Advanced Settings

(General)	
Allow UTF8	True
Bindings	*:21:
ID	2
Name	ESRS FTP Site
Physical Path	C:\EMC\ESRS\Gateway\work\ftproot
Start Automatically	True
Behavior	
Connections	
File Handling	

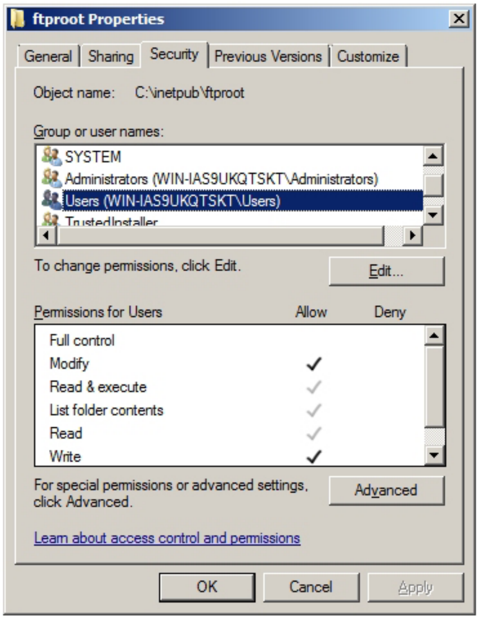
Start Automatically
[serverAutoStart] If true, the site is started upon creation, or when FTP is started. Starting a site sets this property to true, and stopping a site sets this property to …

19. Set the FTP site Start Automatically setting to **True**, and click **OK**.

20. On the left pane, click **ESRS FTP Site** to edit permissions for the FTP site.



21. On the right pane, click **Edit Permissions**.



Object name: C:\inetpub\ftproot

Group or user names:

- SYSTEM
- Administrators (WIN-IAS9UKQTSKT\Administrators)
- Users (WIN-IAS9UKQTSKT\Users)
- TrustedInstaller

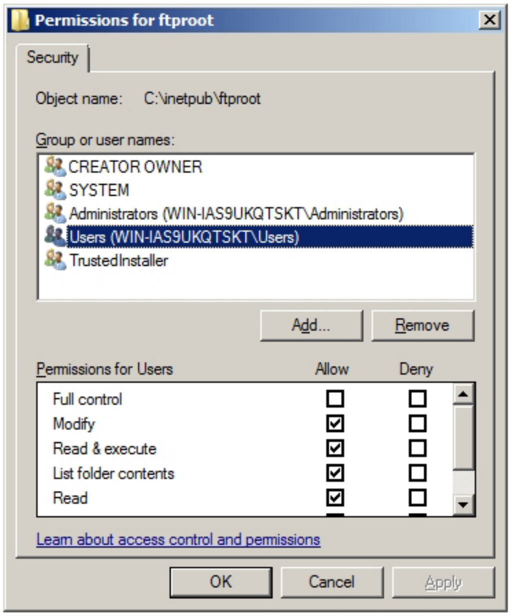
To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

22. Click **Edit**, then select **Users**.



Permissions for ftproot

Security

Object name: C:\inetpub\ftproot

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (WIN-IAS9UKQTSKT\Administrators)
- Users (WIN-IAS9UKQTSKT\Users)
- TrustedInstaller

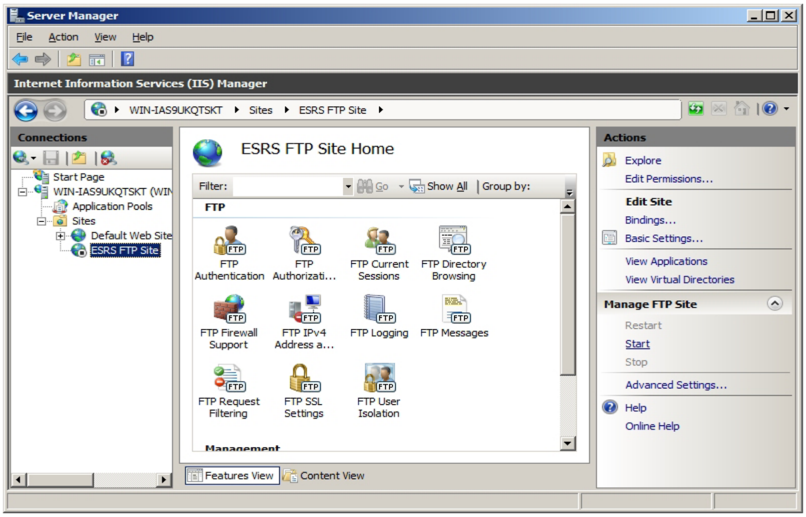
Add... Remove

Permissions for Users	Allow	Deny
Full control	□	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

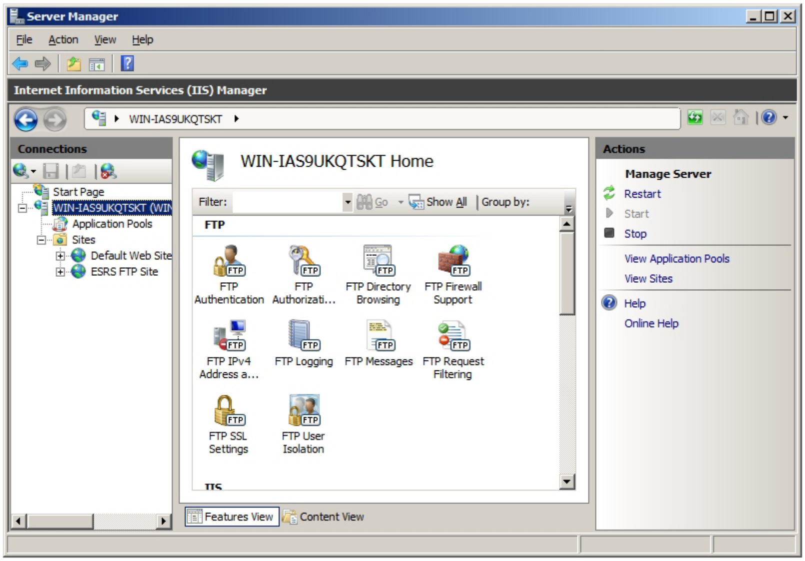
Learn about access control and permissions

OK Cancel Apply

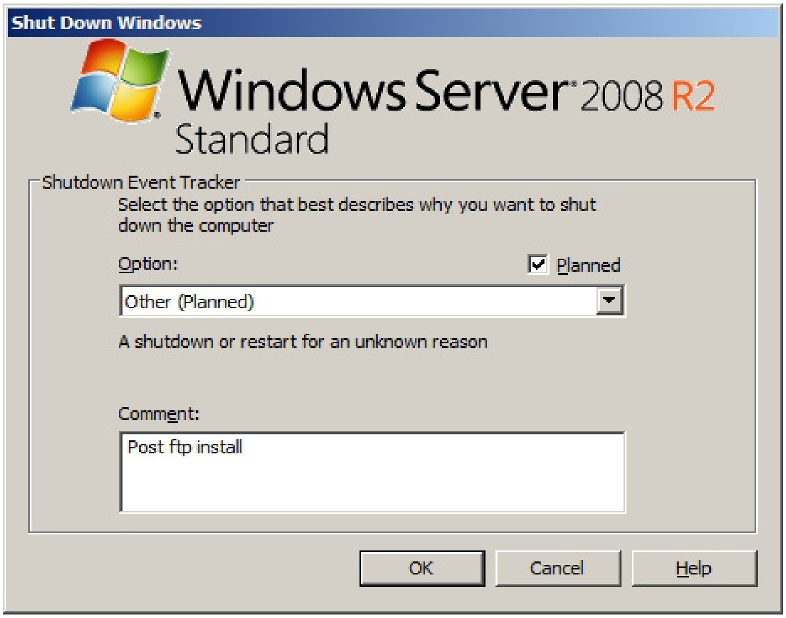
23. Click **Modify**, then **Apply** and **OK**.



24. Go to the Server Level, and restart the IIS service.



25. Reboot the server.



Shutdown Event Tracker

Select the option that best describes why you want to shut down the computer

Option: ☑ Planned

Other (Planned)

A shutdown or restart for an unknown reason

Comment:

Post ftp install

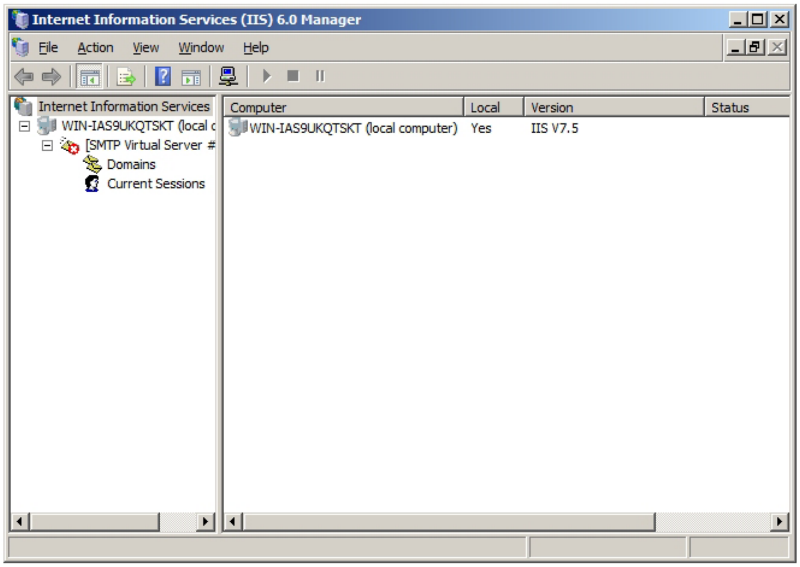
26. Test FTP Server for User Isolation (dir command) and passive port range

```
C:\Users\Administrator>ftp 192.168.51.146
Connected to 192.168.51.146.
220-Microsoft FTP Service
220 Authorized  Users Only
User (192.168.51.146:(none)): onalert
331 Password required for onalert.
Password:
230-Welcome to ESRS Gateway FTP Site
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-20-11  12:47PM       <DIR>          Incoming
226 Transfer complete.
ftp: 49 bytes received in 0.00Seconds
49000.00Kbytes/sec.
ftp> cd /
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-20-11  12:47PM       <DIR>          Incoming
226 Transfer complete.
ftp: 49 bytes received in 0.00Seconds
49000.00Kbytes/sec.
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,26).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,27).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,28).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,29).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,30).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,31).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,32).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,33).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,34).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,35).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,36).
ftp> quote pasv
```

```
227 Entering Passive Mode (192,168,51,146,21,37).
<<<<<<5413
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,24).
<<<<<< 5400
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,25).
ftp> quote pasv
227 Entering Passive Mode (192,168,51,146,21,26).
ftp> bye
221-Thanks You
221 Goodbye
```

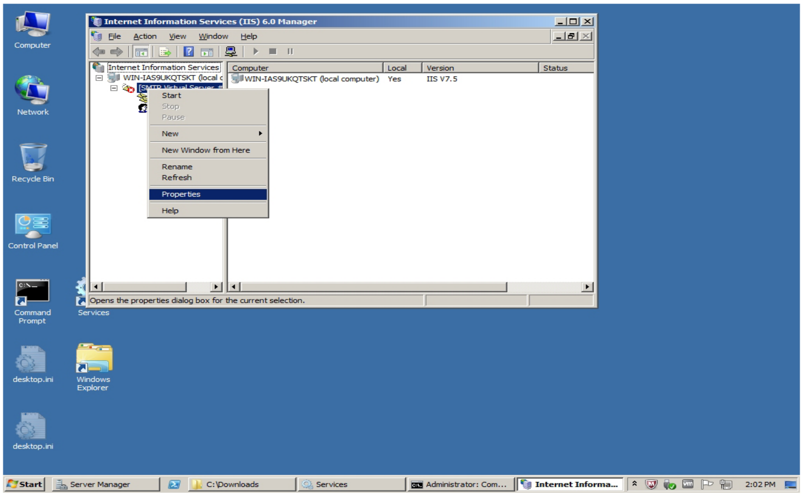
Configure SMTP

1. Open Internet Information Services (IIS) 6.0 Manager (Start\Administrative Tools\Internet Information Services (IIS) 6.0 Manager).

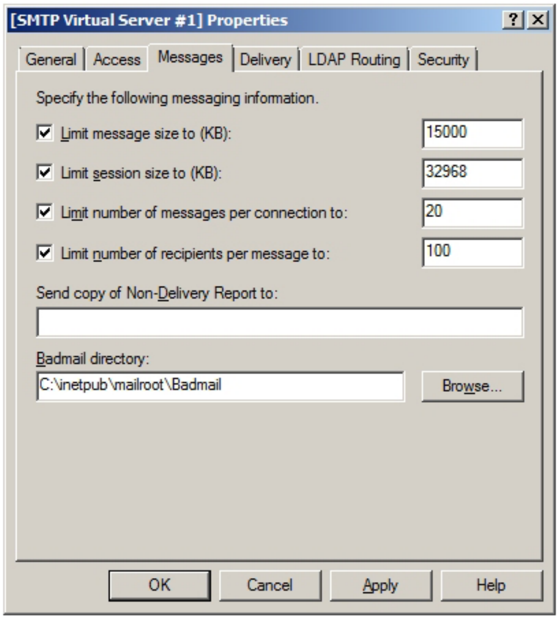


Computer	Local	Version	Status
WIN-IAS9UKQTSKT (local computer)	Yes	IIS V7.5	

2. Right click and select **Properties**.



3. Enter the following values, and click **Apply**.



[SMTP Virtual Server #1] Properties

General | Access | Messages | Delivery | LDAP Routing | Security

Specify the following messaging information.

☑ Limit message size to (KB): 15000

☑ Limit session size to (KB): 32968

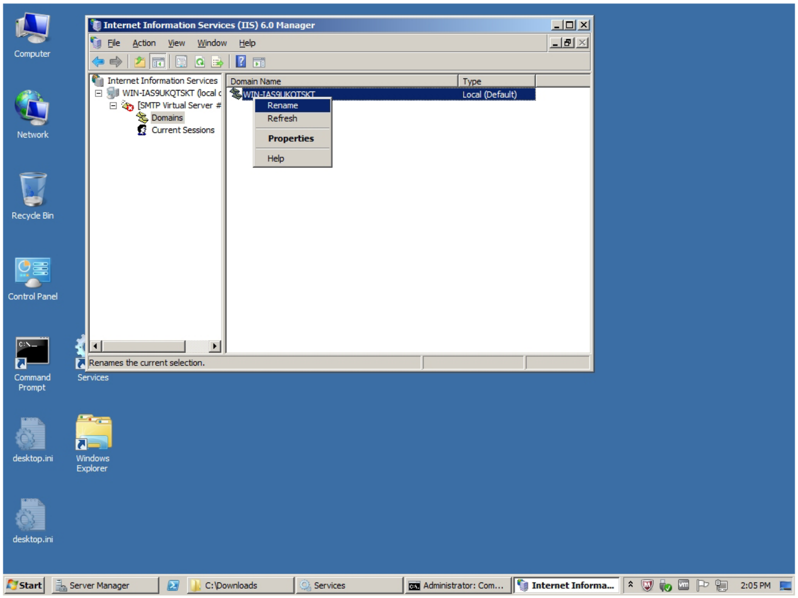
☑ Limit number of messages per connection to: 20

☑ Limit number of recipients per message to: 100

Send copy of Non-Delivery Report to:

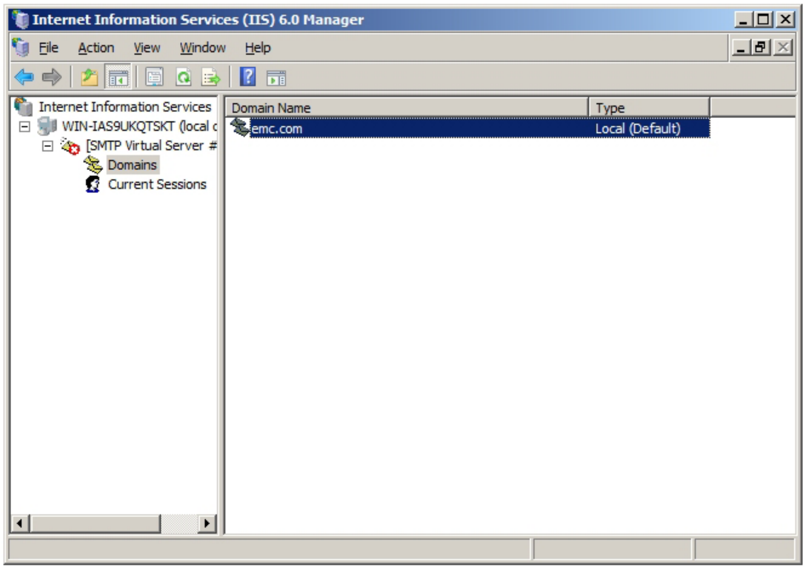
Badmail directory: C:\inetpub\mailroot\Badmail

4. In the left pane, click on **Domains**. In the right pane, click on the server and select **Rename**.



Renames the current selection.

5. Change the name to **emc.com**.


Internet Information Services (IIS) 6.0 Manager
File Action View Window Help
Internet Information Services
WIN-IAS9UKQTSKT (local c
[SMTP Virtual Server #
Domains
Current Sessions
Domain Name
Type

Domain Name	Type
emc.com	Local (Default)

6. SMTP configuration is complete.

3

Configuration Tool

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

This chapter includes the following topics:

- Configuration Tool overview 162
- Installing and using the Configuration Tool 163
- Uninstalling the Configuration Tool 182

Configuration Tool overview

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

The following sections explain 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.

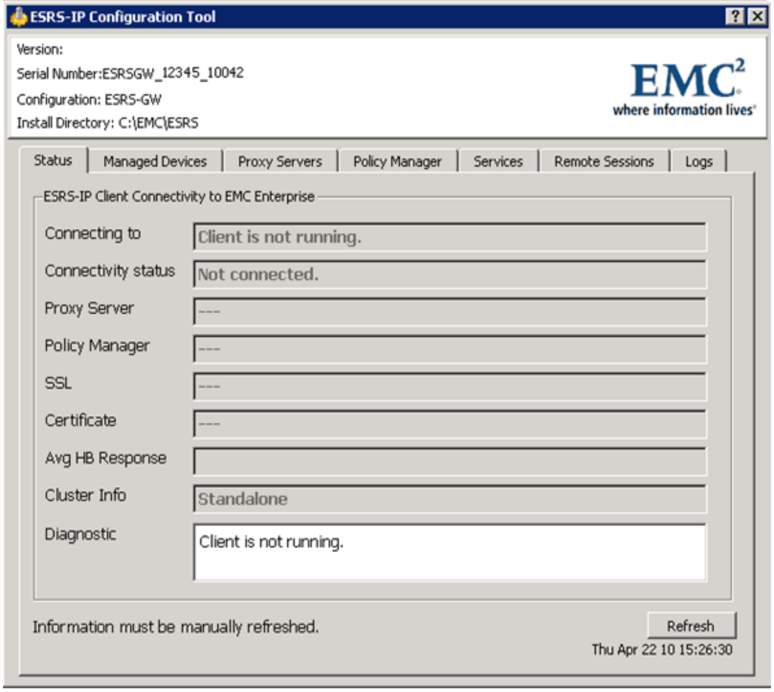
If you are running Windows 2008

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 75 on page 164.



Version:
Serial Number:ESRSGW_12345_10042
Configuration: ESRS-GW
Install Directory: C:\EMC\ESRS

ESRS-IP Client Connectivity to EMC Enterprise

Connecting to	Client is not running.
Connectivity status	Not connected.
Proxy Server	---
Policy Manager	---
SSL	---
Certificate	---
Avg HB Response	
Cluster Info	Standalone
Diagnostic	Client is not running.

Information must be manually refreshed.

Thu Apr 22 10 15:26:30

Figure 75 **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 76 on page 165.

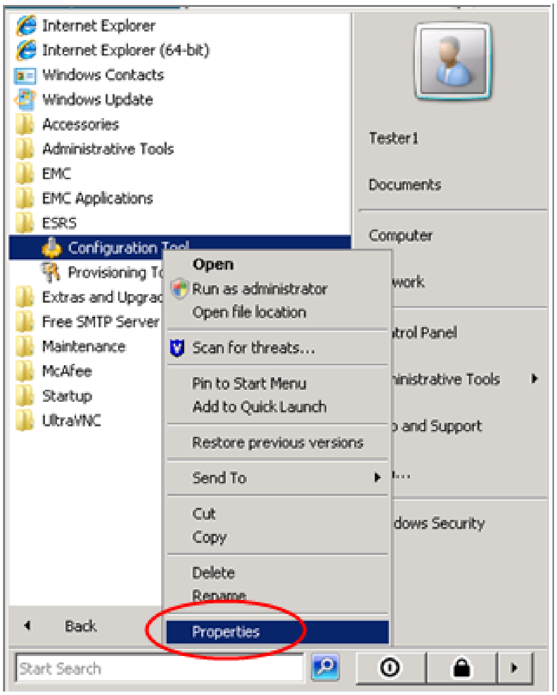
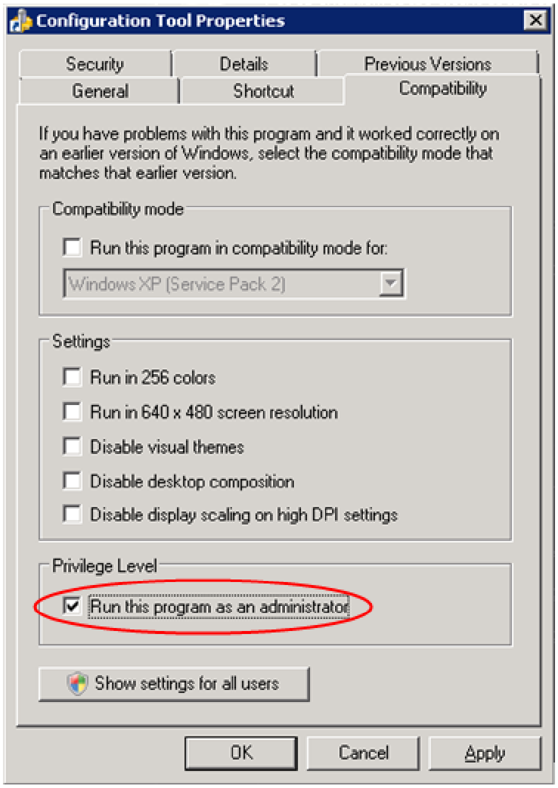


Figure 76 Configuration Tool properties

4. Click **Compatibility**, then select **Run this program as an administrator**, as shown in Figure 77 on page 166.



If you have problems with this program and it worked correctly on an earlier version of Windows, select the compatibility mode that matches that earlier version.

Compatibility mode

□ Run this program in compatibility mode for:

Windows XP (Service Pack 2)

Settings

□ Run in 256 colors

□ Run in 640 x 480 screen resolution

□ Disable visual themes

□ Disable desktop composition

□ Disable display scaling on high DPI settings

Privilege Level

☑ Run this program as an administrator

Show settings for all users

Figure 77 **Run this program as an administrator**

5. Click **OK**, then launch the Configuration Tool as described in "Using the Configuration Tool" on page 166.

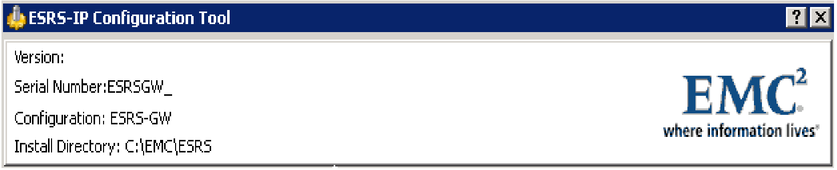
Now that you have enabled yourself to run Configuration Tool as an administrator, you will be able to view connectivity status as shown in Figure 79 on page 167.

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 Gateway Client device, the configuration of your device, and the install directory, as shown in Figure 78 on page 167.



Version:

Serial Number:ESRSGW_

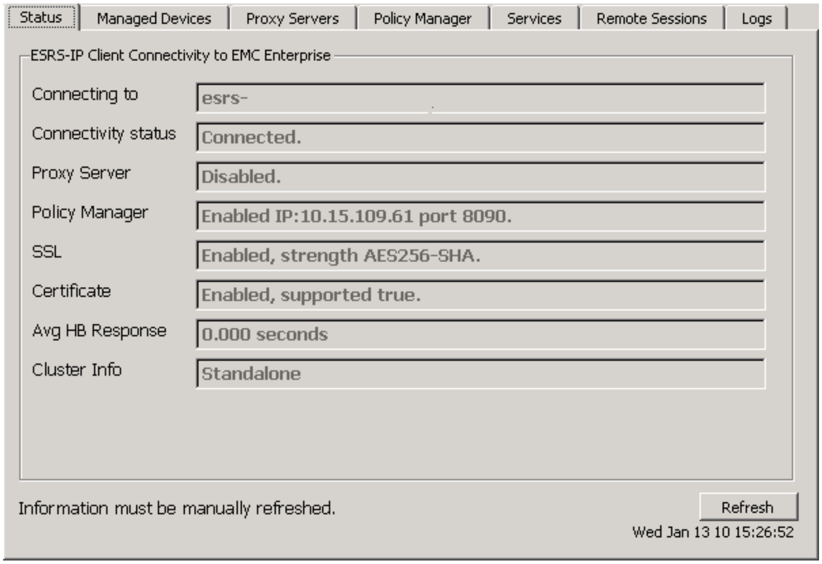
Configuration: ESRS-GW

Install Directory: C:\EMC\ESRS

Figure 78 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 Gateway Client and EMC, as shown in Figure 79 on page 167.



ESRS-IP Client Connectivity to EMC Enterprise

Connecting to	esrs-
Connectivity status	Connected.
Proxy Server	Disabled.
Policy Manager	Enabled IP:10.15.109.61 port 8090.
SSL	Enabled, strength AES256-SHA.
Certificate	Enabled, supported true.
Avg HB Response	0.000 seconds
Cluster Info	Standalone

Information must be manually refreshed.

Wed Jan 13 10 15:26:52

Figure 79 Status tab

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

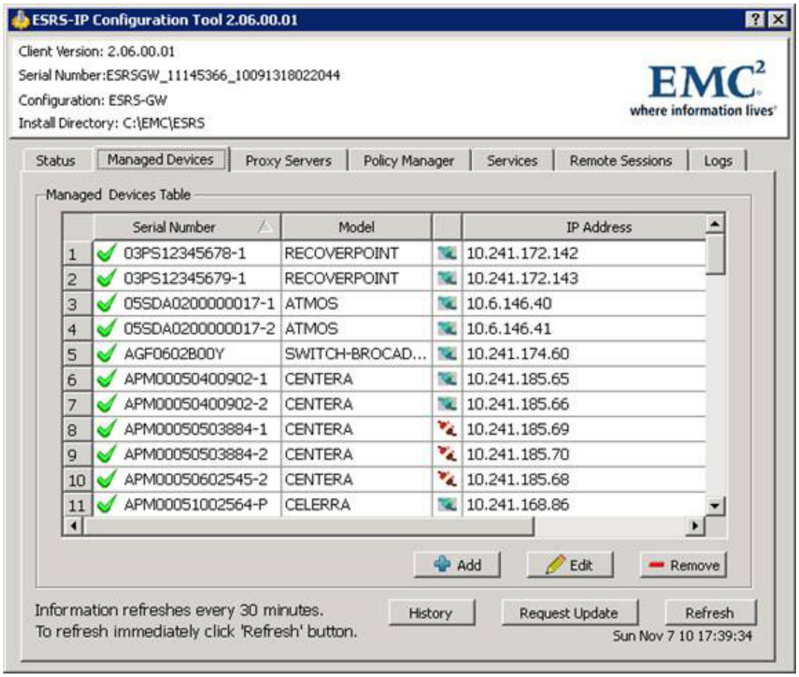
Note: To update the displayed information at any time, click **Refresh**. The screens will automatically update every 30 minutes.

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 80 on page 169.



ESRS-IP Configuration Tool 2.06.00.01

Client Version: 2.06.00.01
Serial Number:ESRSGW_11145366_10091318022044
Configuration: ESRS-GW
Install Directory: C:\EMC\ESRS

Managed Devices Table

		Serial Number	Model		IP Address
1	✓	03PS12345678-1	RECOVERPOINT		10.241.172.142
2	✓	03PS12345679-1	RECOVERPOINT		10.241.172.143
3	✓	05SDA0200000017-1	ATMOS		10.6.146.40
4	✓	05SDA0200000017-2	ATMOS		10.6.146.41
5	✓	AGF0602B00Y	SWITCH-BROCAD...		10.241.174.60
6	✓	APM00050400902-1	CENTERA		10.241.185.65
7	✓	APM00050400902-2	CENTERA		10.241.185.66
8	✓	APM00050503884-1	CENTERA		10.241.185.69
9	✓	APM00050503884-2	CENTERA		10.241.185.70
10	✓	APM00050602545-2	CENTERA		10.241.185.68
11	✓	APM00051002564-P	CELERRA		10.241.168.86

Information refreshes every 30 minutes.
To refresh immediately click 'Refresh' button.

Sun Nov 7 10 17:39:34

Figure 80 **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 81 on page 170.

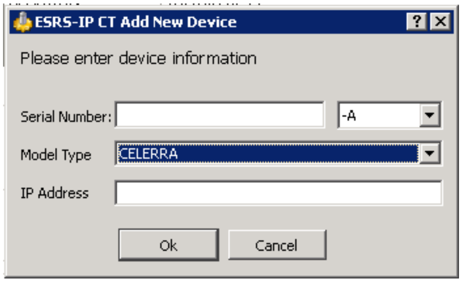


Figure 81 **Add New Device window**

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 product from the drop-down list)
   - IP Address

Table 5 on page 170 lists the valid suffixes and code versions for each product:

Table 5 **Valid Suffixes and Code Versions**

Product	Suffix	Explanation	ESRS Gateway Code Version
Atmos	1-16		2.08
Avamar	None		2.08
Beta1	1-32		2.04
Beta2	1-32		2.04
Celerra	P S A	Primary Control Station (CS0) Secondary Control Station (CS1) Control Station Alias	2.02
Centera	1-36		2.02
Clariion	A B	SP A&B	2.02
Connectrix	CM, CLI		2.02

Table 5 Valid Suffixes and Code Versions

Product	Suffix	Explanation	ESRS Gateway Code Version
Customer Management Station	1-32		2.24
Data Domain	None		2.14
DCA	B P		2.12
DL3D	1 2 3		2.02
DLm	P S A	Primary Control Station (CS0) Secondary Control Station (CS1) Control Station Alias	2.02
DLm3	1000, ACP1, ACP2, ACPA		2.16
DLm4	VTE1, VTE2, VTEA		2.24
EDL	Blank A B	Blank for engine SP A&B	2.02
Invista	A B		2.02
Isilon	None		2.24
RecoverPoint	1-16		2.02
Switch-Brocade-B	CM, CLI		2.02
Switch-Cisco	None		2.02
Symmetrix	None		2.02
ViPR	1 2 3		2.22
VMAX Cloud Edition (CE)	H1, H2, COL, AE, SE, VC, CECV	Host 1 (H1) Host 2 (H2) Collector (COL) Automation Engine (AE) Solutions Enabler (SE) vCenter (VC) ConnectEMC (CECV)	2.22
VNX	FileP, FileS, FileA, BlockA, BlockB	Primary Control Station (CS0) Secondary Control Station (CS1) Control Station Alias, IP Block (SP A&B)	2.08

Table 5 Valid Suffixes and Code Versions

Product	Suffix	Explanation	ESRS Gateway Code Version
VNXe	None		2.08
VPLEX	None		2.04
XtremIO	None		2.22

3. After entering the device information, 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 174.

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 174.

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

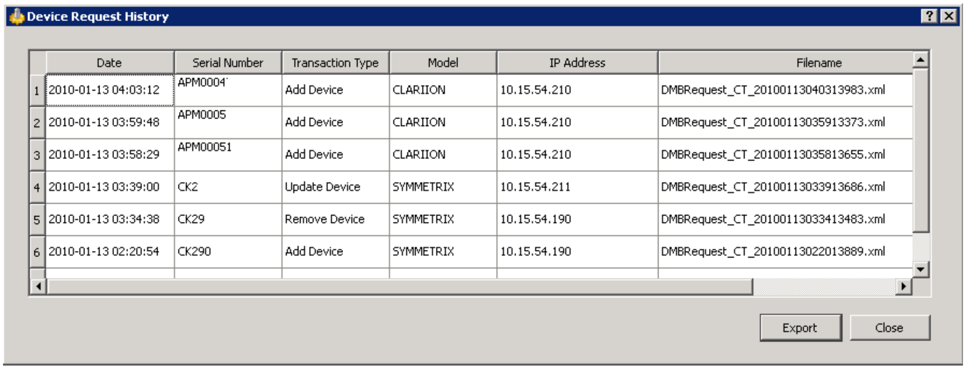
When you have completed all your manage, edit, or unmanage requests, click **Request Update**. Your change requests will be displayed for verification. Click **OK** to submit your requests to EMC for implementation.

When an authorized EMC Global Services professional has approved your requests via the EMC enterprise, the requested updates will be processed by the Gateway 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 82 on page 174.



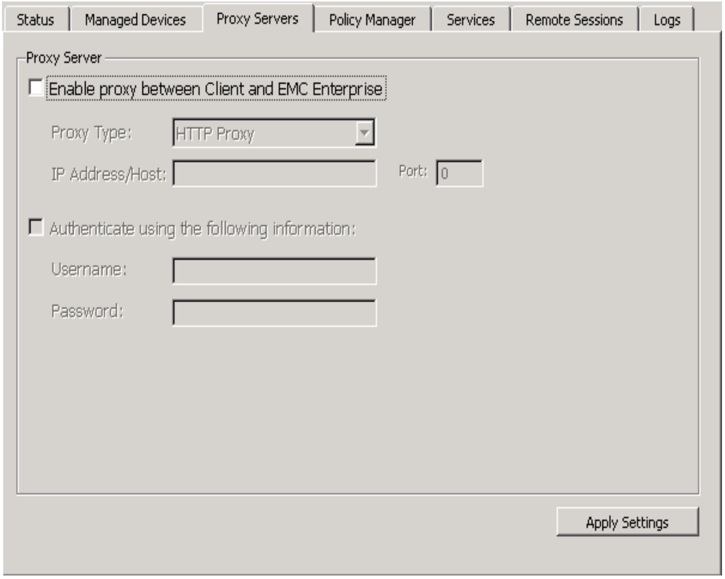
Device Request History

	Date	Serial Number	Transaction Type	Model	IP Address	Filename
1	2010-01-13 04:03:12	APM0004'	Add Device	CLARIION	10.15.54.210	DMBRequest_CT_20100113040313983.xml
2	2010-01-13 03:59:48	APM0005	Add Device	CLARIION	10.15.54.210	DMBRequest_CT_20100113035913373.xml
3	2010-01-13 03:58:29	APM00051	Add Device	CLARIION	10.15.54.210	DMBRequest_CT_20100113035813655.xml
4	2010-01-13 03:39:00	CK2	Update Device	SYMMETRIX	10.15.54.211	DMBRequest_CT_20100113033913686.xml
5	2010-01-13 03:34:38	CK29	Remove Device	SYMMETRIX	10.15.54.190	DMBRequest_CT_20100113033413483.xml
6	2010-01-13 02:20:54	CK290	Add Device	SYMMETRIX	10.15.54.190	DMBRequest_CT_20100113022013889.xml

Figure 82 History

Communicating through a proxy server

Gateway Clients can be configured to communicate directly through EMC or through an HTTPS or SOCKS proxy, as shown in Figure 83 on page 175.



☐ Enable proxy between Client and EMC Enterprise

Proxy Type: HTTP Proxy

IP Address/Host:

Port: 0

☐ Authenticate using the following information:

Username:

Password:

Figure 83 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 Gateway Client and the EMC Enterprise. If connectivity is not available, an error message will be returned.

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

Disabling proxy server communication

To disable communication through a proxy server:

1. Click the **Proxy Servers** tab in the Configuration Tool, as shown in Figure 83 on page 175.
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 Gateway Client and the EMC enterprise without the use of a proxy server. If connectivity is not available, an error message is returned.

Linking a Gateway Client to a Policy Manager

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

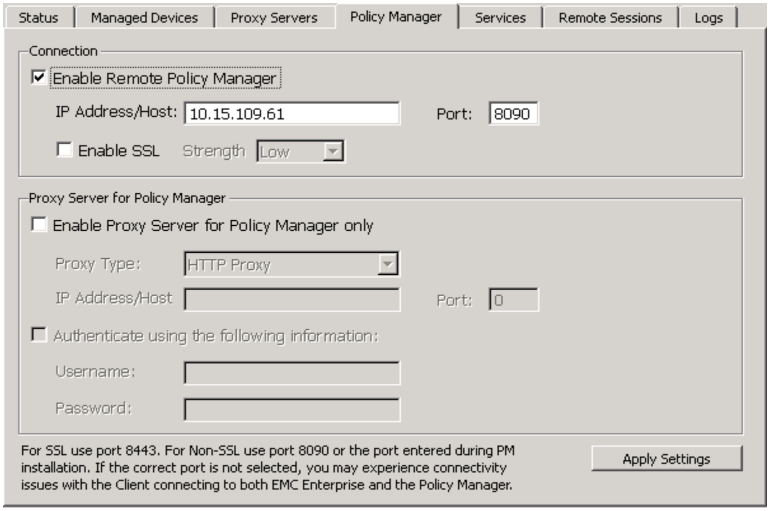
The following procedure explains how use the Configuration Tool to link a Gateway Client to a Policy Manager.

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 Gateway Client will lose connectivity to the Enterprise server. To avoid this problem, do not enable a Policy Manager unless the Gateway Client can connect to it.

To link a Gateway Client to a Policy Manager:

1. Check **Enable Remote Policy Manager** in the **Policy Manager** tab in the Configuration Tool, as shown in Figure 84 on page 177.



Connection

☑ Enable Remote Policy Manager

IP Address/Host: 10.15.109.61 Port: 8090

□ Enable SSL Strength Low

Proxy Server for Policy Manager

□ Enable Proxy Server for Policy Manager only

Proxy Type: HTTP Proxy

IP Address/Host Port: 0

□ Authenticate using the following information:

Username:

Password:

For SSL use port 8443. For Non-SSL use port 8090 or the port entered during PM installation. If the correct port is not selected, you may experience connectivity issues with the Client connecting to both EMC Enterprise and the Policy Manager.

Figure 84 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 Gateway 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 Gateway 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, refer to the *EMC Secure Remote Support Policy Manager Operations Guide*.

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 Gateway Client to Policy Manager communication only. It will not affect the communication between the Gateway Client and the EMC Enterprise.

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

   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 Gateway Client is now linked to the Policy Manager.

Disabling communication

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

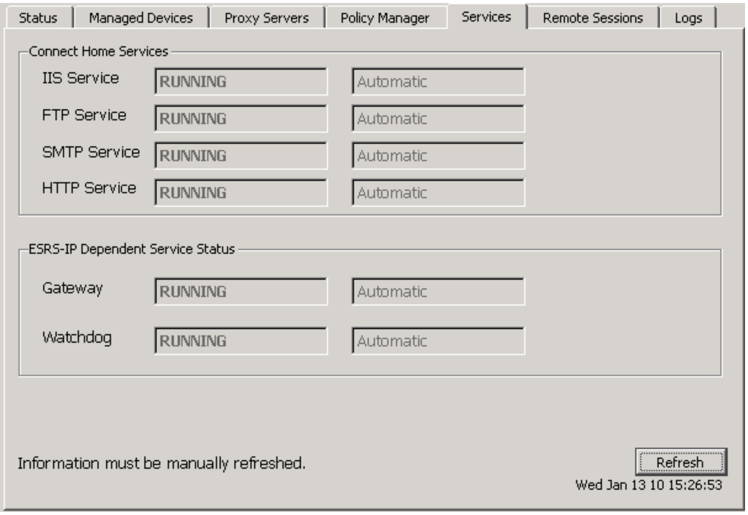
Note: Disabling communication with the Policy Manager will result in all permission settings for the Gateway Client being set to Always Allow.

Displaying the status of Services

To display the status of services related to ESRS and connect homes, select the Service tab in the Configuration Tool, as shown in Figure 85 on page 179. 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.



Connect Home Services

IIS Service	RUNNING	Automatic
FTP Service	RUNNING	Automatic
SMTP Service	RUNNING	Automatic
HTTP Service	RUNNING	Automatic

ESRS-IP Dependent Service Status

Gateway	RUNNING	Automatic
Watchdog	RUNNING	Automatic

Information must be manually refreshed.

Wed Jan 13 10 15:26:53

Figure 85 Services tab

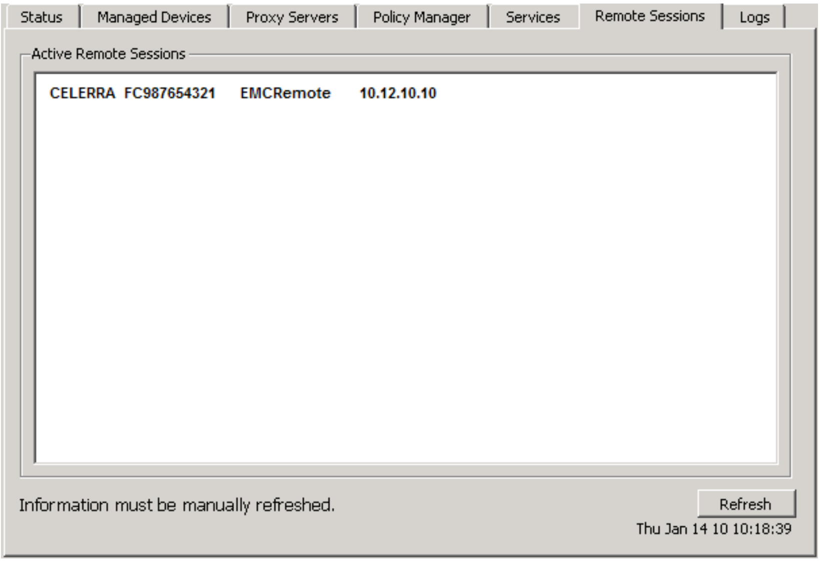
Displaying active remote sessions

To display all active remote sessions to a managed device through the Gateway Client, click the **Remote Sessions** tab in the Configuration Tool, as shown in Figure 86 on page 180. 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 Policy Manager to view and terminate remote sessions.



CELERRA FC987654321 EMCRemote 10.12.10.10

Information must be manually refreshed.

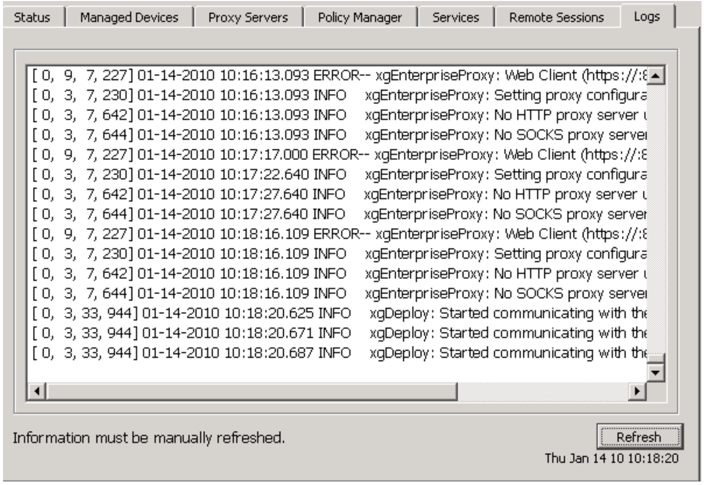
Thu Jan 14 10 10:18:39

Figure 86 **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 87 on page 181.

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



```
[ 0,  9,  7, 227] 01-14-2010 10:16:13.093 ERROR-- xgEnterpriseProxy: Web Client (https://:8
[ 0,  3,  7, 230] 01-14-2010 10:16:13.093 INFO    xgEnterpriseProxy: Setting proxy configura
[ 0,  3,  7, 642] 01-14-2010 10:16:13.093 INFO    xgEnterpriseProxy: No HTTP proxy server u
[ 0,  3,  7, 644] 01-14-2010 10:16:13.093 INFO    xgEnterpriseProxy: No SOCKS proxy server
[ 0,  9,  7, 227] 01-14-2010 10:17:17.000 ERROR-- xgEnterpriseProxy: Web Client (https://:8
[ 0,  3,  7, 230] 01-14-2010 10:17:22.640 INFO    xgEnterpriseProxy: Setting proxy configura
[ 0,  3,  7, 642] 01-14-2010 10:17:27.640 INFO    xgEnterpriseProxy: No HTTP proxy server u
[ 0,  3,  7, 644] 01-14-2010 10:17:27.640 INFO    xgEnterpriseProxy: No SOCKS proxy server
[ 0,  9,  7, 227] 01-14-2010 10:18:16.109 ERROR-- xgEnterpriseProxy: Web Client (https://:8
[ 0,  3,  7, 230] 01-14-2010 10:18:16.109 INFO    xgEnterpriseProxy: Setting proxy configura
[ 0,  3,  7, 642] 01-14-2010 10:18:16.109 INFO    xgEnterpriseProxy: No HTTP proxy server u
[ 0,  3,  7, 644] 01-14-2010 10:18:16.109 INFO    xgEnterpriseProxy: No SOCKS proxy server
[ 0,  3, 33, 944] 01-14-2010 10:18:20.625 INFO    xgDeploy: Started communicating with the
[ 0,  3, 33, 944] 01-14-2010 10:18:20.671 INFO    xgDeploy: Started communicating with the
[ 0,  3, 33, 944] 01-14-2010 10:18:20.687 INFO    xgDeploy: Started communicating with the
```

Information must be manually refreshed.

Thu Jan 14 10 10:18:20

Figure 87 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.

4

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 server. It is your responsibility to perform backups and ensure that the servers can be restored through the use of the backup data. Either image backup or data file backup is satisfactory.

Topics in this section include:

- Power sequences 184
- Time Zone settings 185
- Service preparation for Gateway Client 186
- Backup guidelines and procedures 188
- Restoration procedures 189

Power sequences

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

IMPORTANT

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

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

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

IMPORTANT

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

Time Zone settings

The 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

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

Gateway Client server

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

Logging preparation

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 88 on page 187:

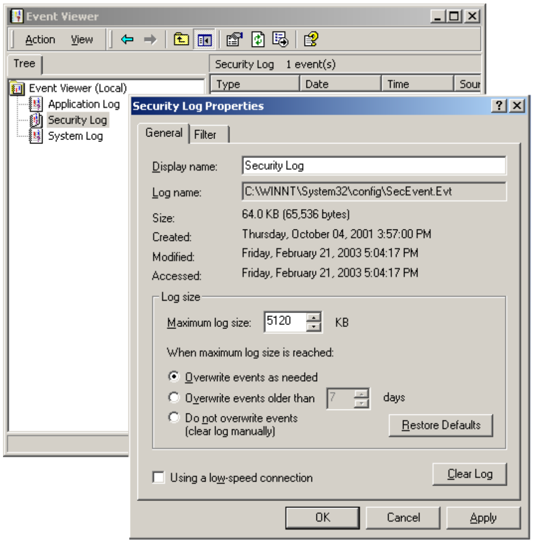
1. Select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Event Viewer**.
2. Right-click **System Log** and then select **Properties**.
3. Select option **Overwrite events as needed**, and click **OK** under the tab **General**.
4. Repeat step 2 and step 3 to set properties 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 Gateway Client will fail to function properly for callhome messages, and possibly for support connections. If the problem is severe enough, the server operating will stop functioning.

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



Display name: Security Log

Log name: C:\WINNT\System32\config\SecEvent.Evt

Size: 64.0 KB (65,536 bytes)

Created: Thursday, October 04, 2001 3:57:00 PM

Modified: Friday, February 21, 2003 5:04:17 PM

Accessed: Friday, February 21, 2003 5:04:17 PM

Maximum log size: 5120 KB

When maximum log size is reached:

● Overwrite events as needed

○ Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection

Figure 88 Event Viewer System and Security Log settings

Backup guidelines and procedures

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

Specific procedures depend on your:

- ESRS site architecture
- Backup software
- Existing procedures

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

Backup

1. **Gateway Client server image** — See "Server image backup" on page 188 for recommended Gateway server backup guidelines.

Restoration

2. **Gateway Client server** — See "Restoration procedures" on page 189 for recommended guidelines on restoring your server from image backup.

Server image backup

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

Initial setup

At installation time:

For each Gateway Client server:

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

Optionally, for each Gateway server:

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

Restoration procedures

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

Server image backup restoration

For a Gateway Client server:

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

Installation restoration

This section provides details on installation restoration.

For a Gateway Client server:

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

CAUTION

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

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

5

Uninstalling Gateway Client 2.16 using Provisioning Tool 2.14

This appendix describes how to uninstall the Gateway Client 2.16 with Provisioning Tool 2.14.

◆ Uninstalling Gateway Client 2.16 using Provisioning Tool 2.14 192

Uninstalling Gateway Client 2.16 using Provisioning Tool 2.14

The eLicensing proxy service has been introduced in Gateway release 2.16, and therefore uninstalling the Gateway Client 2.16 using the Provisioning Tool 2.14 will fail as it would not recognize this newly-added service. As a workaround, a separate uninstall utility is packaged with the Gateway Client 2.16.

Note: The Provisioning Tool (PvT) 2.14.xx.xx is not aware of the SRS Gateway Proxy Service which was added in the 2.16.XX.XX and above, so it does not stop the service and when the uninstall tries to delete the C:/EMC/ESRS/Gateway/Privoxy/logs/privoxy.log because the file it is open causing the uninstall to fail which forces a rollback.

The 2.16.XX.XX Gateway Code and/or patch includes a separate Uninstaller application, located in <install_drive>:\EMC\ESRS\Uninstall\Gateway\2.XX.XX.XX.

To uninstall:

1. Open Windows Explorer.
2. Navigate to the Gateway uninstaller directory:

   <install_drive>:\EMC\ESRS\Uninstall\Gateway\2.XX.XX.XX_
3. Double click the GatewayUninstaller.exe. This will launch a command window.
4. At the command prompt, type **Y** and press **Enter**.
5. The uninstaller will run and uninstall the Gateway Application and ALL its components.

Note: To view a detailed install log, see Primus emc287085, "Provisioning Tool Error: ESRS Gateway uninstallation fails after 2.16.xx.xx Patch installed OR fresh install with Provisioning a Tool 2.14.xx.xx or below." You can access this Primus at http://knowledgebase.emc.com

6

Patch installation

This appendix describes how to patch any version of ESRS Gateway Client only.

- Patch installation instructions 194

Patch installation instructions

Note: These instructions are for patching ANY version of ESRS Gateway Client ONLY. Patches for the ESRS Gateway Client are cumulative and do NOT require a stepped upgrade process. The version 2.08.04 patch was used for the example in the following process. The same process is to be followed for any ESRS Gateway Client Patch.

Note: Due to the use of User Access Control (UAC) in Windows Server 2008 (Any Version), you may be required to execute the patch in a Command Window opened in RunAsAdministrator Mode to successfully install the Gateway Patch.

Policy Manager update is NOT included in the patch and will require a new CD and has an entirely separate update process. The latest Policy Manager code is available on EMC Online Support Site (support.emc.com):

These instructions do NOT apply to ESRS Device Clients. Instructions and Processes for ESRS Device Clients will be the responsibility of the individual Product Groups.

Do NOT apply the ESRS Gateway Client Patches to ESRS Device Clients.

Field Instructions

All activities must be properly documented in the service request/case. Service requests/cases should only be closed upon either the completion of the activity or a properly documented customer refusal. No service request/case should be cancelled at any time without approval by EMC's FCO Specialist Ann St. Onge.

1. The patch will be located at the following link:

   ```
   http://www.cs.isus.emc.com/csweb2/EMC_Secure_Remote_S
   upport.htm
   ```

   You'll then go to **Software Patch Upgrades** then select "2.08.00.xx patch."

2. You will see the details of the 2.xXX.00.xx patch.
3. Read through the pertinent information.
4. Scroll to the bottom of the page and you will see the zip file.
5. Download the zip file to your memory stick.

6. Go to the customer site.
7. Create a directory named Patch-2.XX.00.xx under <install_drive>:\

   (the directory should be created on the drive that the Gateway Client is installed on)
8. Copy the patch zip file into this new directory.
9. Expand the zip file.
10. Review the installation instructions document.
11. Click twice on the executable file which will extract the patch and additional documentation.
12. Follow the patch installation instructions from this point onward.
13. You must install this patch on the Gateway(s). There is no patch to be applied to the Policy Manager in this release.

Note: The 2.0X.00.xx Patch is for ESRS 2.0X.XX.xx and above are for Gateway Clients only.

Note: The Gateway Client patches are NOT for CLARiiON / VNX; VNXe or Symmetrix Device Clients.

Note: Policy Manager update is NOT included in the patch and will require an new CD and has an entirely separate update process.

WARNING

It is imperative that when applying the 2.10 ESRS Gateway Client Patch that you MATCH the patch applied to the Operating System (Windows 2003 OR Windows 2008) that the ESRS Gateway Client is installed on. Failure to do so will result in the FTP services NOT being properly controlled by the ESRS Watchdog Service and may/will result in missed callhomes that can result in Data Unavailability / Data Loss situations

IMPORTANT

This version of the of the patch (regardless of version) will address the requirement of the Gateway to be able to trust the new Root Certificate from RSA. If patching from a lower level of code the

patch will upgrade the code and apply the fix for the certificate (i.e 2.06.04.00 patch to 2.10.xx.xx will apply the patch to upgrade the base Gateway code to 2.10.10.00 which includes the certificate fix. If applying the patch to the same level of code (i.e. currently 2.06.04.00, the base gateway code remain the same but code level will change from 2.06.04.00 to 2.06.10.00) to indicate that the certificate fix has been applied.

All patches listed below contain the Certificate Fix.

The new patches are as follows:

```
GatewayUpgrade-2.02.10.00.zip
GatewayUpgrade-2.04.12.00.zip
GatewayUpgrade-2.06.10.00.zip
GatewayUpgrade-2.08.10.00.zip

GatewayUpgrade-2.10.10.00-2k3-only.zip
GatewayUpgrade-Win2008-2.10.10.00.zip
GatewayUpgrade- 2.10.10.00-combined.zip

GatewayUpgrade-2.12.10.00-2k3-only.zip
GatewayUpgrade-Win2008-2.12.10.00.zip
GatewayUpgrade-2.12.10.00-combined.zip

GatewayUpgrade-2.14.00.02.-2k3-only.zip
GatewayUpgrade-Win2008-2.14.00.02.zip
GatewayUpgrade-2.14.00.02-combined.zip

GatewayUpgrade-2.16.00.06.-2k3-only.zip
GatewayUpgrade-Win2008-2.16.00.06.zip
GatewayUpgrade-2.16.00.06-combined.zip

GatewayUprade-ALL-Patches
```

WARNING

DO NOT USE OLDER VESIONS OF THE ESRS 2 PATCHES.

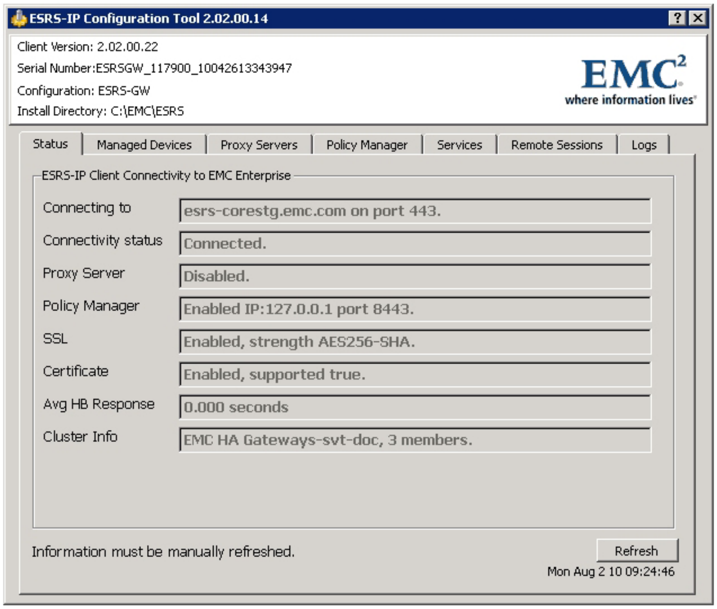
IMPORTANT

The 2.16.00.06 version of code adds an additional Service (SRS Gateway Proxy) to ESRS attempting to uninstall with a Provisioning Tool (PvT) with a version below 2.16.00.06 will fail and will rollback the uninstall. An additional tool has been added to the 2.16.00.06 Patch and Downloaded code to address this issue.

Please see Primus emc287085: Provisioning Tool Error: ESRS Gateway uninstall fails after 2.16.xx.xx patch installation OR fresh installation with Provisioning Tool 2.14.xx.xx or earlier

Process

1. Verify the current ESRS code version by launching the Configuration Tool (CT).



ESRS-IP Configuration Tool 2.02.00.14

Client Version: 2.02.00.22
Serial Number:ESRSGW_117900_10042613343947
Configuration: ESRS-GW
Install Directory: C:\EMC\ESRS

ESRS-IP Client Connectivity to EMC Enterprise

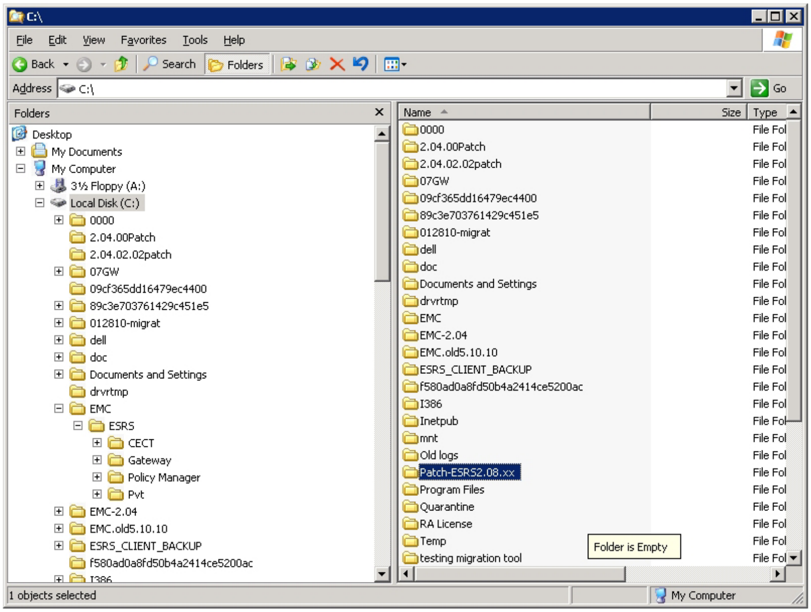
Connecting to	esrs-corestg.emc.com on port 443.
Connectivity status	Connected.
Proxy Server	Disabled.
Policy Manager	Enabled IP:127.0.0.1 port 8443.
SSL	Enabled, strength AES256-SHA.
Certificate	Enabled, supported true.
Avg HB Response	0.000 seconds
Cluster Info	EMC HA Gateways-svt-doc, 3 members.

Information must be manually refreshed.

Mon Aug 2 10 09:24:46

Figure 89 Configuration Tool

2. Create a directory in the Root of the drive where the Gateway Application is installed.



```
Desktop
  My Documents
  My Computer
    3½ Floppy (A:)
    Local Disk (C:)
      0000
      2.04.00Patch
      2.04.02.02patch
      07GW
      09cf365dd16479ec4400
      89c3e703761429c451e5
      012810-migrat
      dell
      doc
      Documents and Settings
      drvrtmp
      EMC
        ESRS
          CECT
          Gateway
          Policy Manager
          Pvt
      EMC-2.04
      EMC.old5.10.10
      ESRS_CLIENT_BACKUP
      f580ad0a8fd50b4a2414ce5200ac
      I386
```

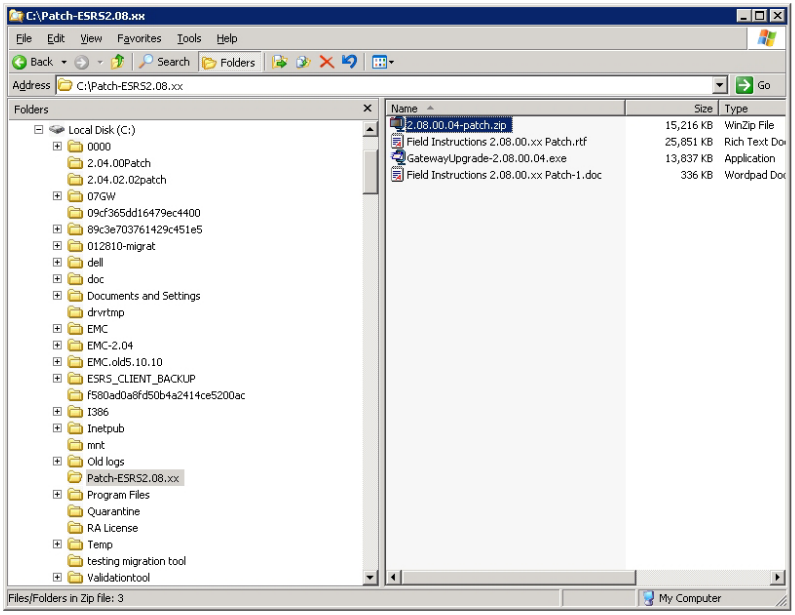
Name	Size	Type
0000		File Fol
2.04.00Patch		File Fol
2.04.02.02patch		File Fol
07GW		File Fol
09cf365dd16479ec4400		File Fol
89c3e703761429c451e5		File Fol
012810-migrat		File Fol
dell		File Fol
doc		File Fol
Documents and Settings		File Fol
drvrtmp		File Fol
EMC		File Fol
EMC-2.04		File Fol
EMC.old5.10.10		File Fol
ESRS_CLIENT_BACKUP		File Fol
f580ad0a8fd50b4a2414ce5200ac		File Fol
I386		File Fol
Inetpub		File Fol
mnt		File Fol
Old logs		File Fol
Patch-ESRS2.08.xx		File Fol
Program Files		File Fol
Quarantine		File Fol
RA License		File Fol
Temp		File Fol
testing migration tool		File Fol

Folder is Empty

1 objects selected

Figure 90 Creating a Directory

3. Copy the ESRS2.08.00.xx -patch.zip to that folder and extract.



C:\Patch-ESRS2.08.xx

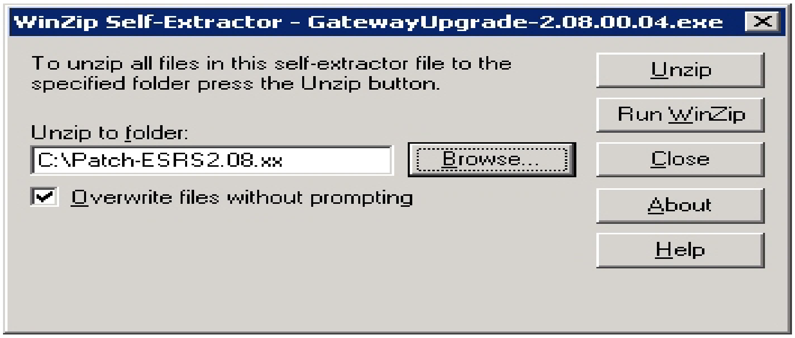
Address: C:\Patch-ESRS2.08.xx

Name	Size	Type
2.08.00.04-patch.zip	15,216 KB	WinZip File
Field Instructions 2.08.00.xx Patch.rtf	25,851 KB	Rich Text Do
GatewayUpgrade-2.08.00.04.exe	13,837 KB	Application
Field Instructions 2.08.00.xx Patch-1.doc	336 KB	Wordpad Do

Files/Folders in Zip file: 3

Figure 91 Extracting the patch.zip

4. Double click on the GatewayUpgrade-2.08.00.04.exe to extract upgrade files. The default path is the user's temporary directory. This should be redirected to the directory where the patch is located (C:\Patch-ESRS2.08.00.xx).



WinZip Self-Extractor - GatewayUpgrade-2.08.00.04.exe

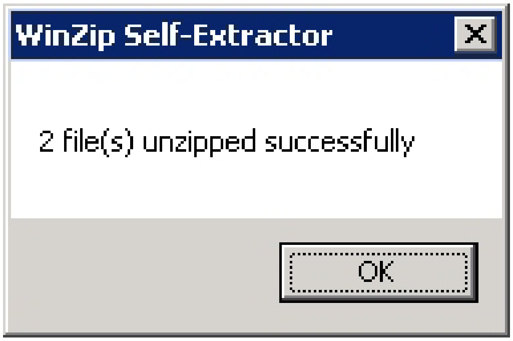
To unzip all files in this self-extractor file to the specified folder press the Unzip button.

Unzip to folder: C:\Patch-ESRS2.08.xx

☑ Overwrite files without prompting

Figure 92 Extracting Upgrade Files

A message appears that the files were unzipped successfully.



WinZip Self-Extractor

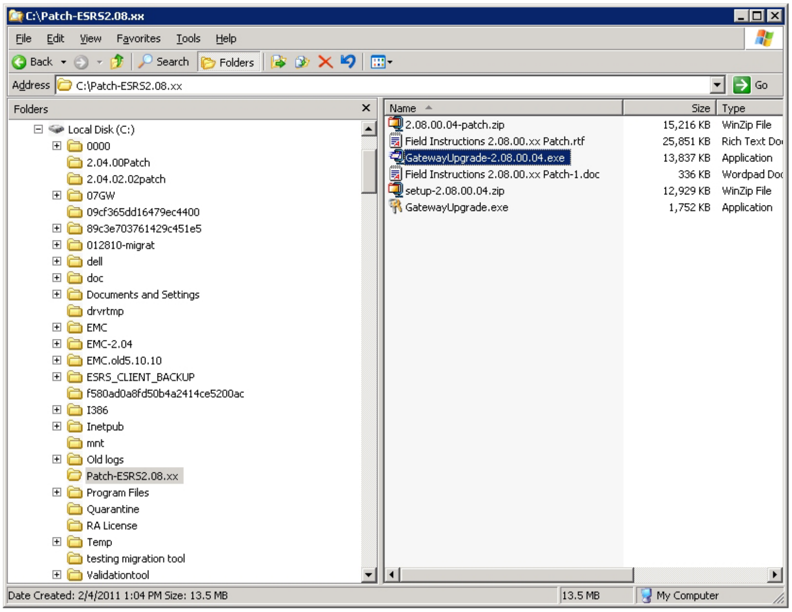
2 file(s) unzipped successfully

Figure 93 Files Successfully Unzipped

WARNING

It is imperative that when applying the 2.10 and above ESRS Gateway Client Patch that you MATCH the patch applied to the Operating System (Windows 2003 OR Windows 2008) that the ESRS Gateway Client is installed on. Failure to do so will result in the FTP services NOT being properly controlled by the ESRS Watchdog Service and may/will result in missed callhomes that can result in Data Unavailability / Data Loss situations.

5. Click **OK** and close the extractor. This will have extracted two additional files.



Address: C:\Patch-ESRS2.08.xx

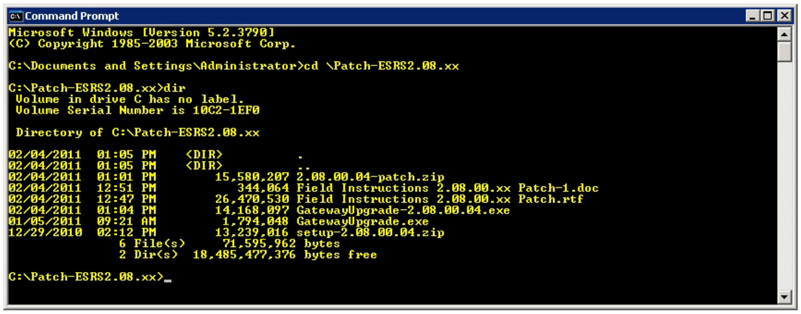
Local Disk (C:)
- 0000
- 2.04.00Patch
- 2.04.02.02patch
- 07GW
- 09cf365dd16479ec4400
- 89c3e703761429c451e5
- 012810-migrat
- dell
- doc
- Documents and Settings
- drvrtmp
- EMC
- EMC-2.04
- EMC.old5.10.10
- ESRS_CLIENT_BACKUP
- f580ad0a8fd50b4a2414ce5200ac
- I386
- Inetpub
- mnt
- Old logs
- Patch-ESRS2.08.xx
- Program Files
- Quarantine
- RA License
- Temp
- testing migration tool
- Validationtool

Name	Size	Type
2.08.00.04-patch.zip	15,216 KB	WinZip File
Field Instructions 2.08.00.xx Patch.rtf	25,851 KB	Rich Text Doc
GatewayUpgrade-2.08.00.04.exe	13,837 KB	Application
Field Instructions 2.08.00.xx Patch-1.doc	336 KB	Wordpad Doc
setup-2.08.00.04.zip	12,929 KB	WinZip File
GatewayUpgrade.exe	1,752 KB	Application

Date Created: 2/4/2011 1:04 PM Size: 13.5 MB 13.5 MB

Figure 94 **Files Extracted**

6. Open a command window and change to the directory that the patch is located (C:\Patch-ESRS2.08.00.xx).



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \Patch-ESRS2.08.xx

C:\Patch-ESRS2.08.xx>dir
 Volume in drive C has no label.
 Volume Serial Number is 10C2-1EF0

 Directory of C:\Patch-ESRS2.08.xx

02/04/2011  01:05 PM    <DIR>          .
02/04/2011  01:05 PM    <DIR>          ..
02/04/2011  01:01 PM        15,580,207 2.08.00.04-patch.zip
02/04/2011  12:51 PM           344,064 Field Instructions 2.08.00.xx Patch-1.doc
02/04/2011  12:47 PM        26,470,530 Field Instructions 2.08.00.xx Patch.rtf
02/04/2011  01:04 PM        14,168,097 GatewayUpgrade-2.08.00.04.exe
01/05/2011  09:21 AM         1,794,048 GatewayUpgrade.exe
12/29/2010  02:12 PM        13,239,016 setup-2.08.00.04.zip
               6 File(s)     71,595,962 bytes
               2 Dir(s)  18,485,477,376 bytes free

C:\Patch-ESRS2.08.xx>_
```

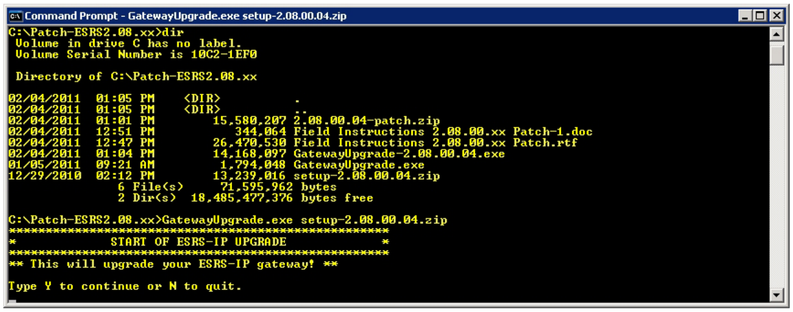
Figure 95 **Command Prompt**

Note: If you double click the GatewayUpgrade.exe in Windows Explorer it will “flash” a DOS box and will **NOT** install the patch. The patch **MUST** be run from a command window and must include the patch.zip to be applied.

The log will show the following:

```
Tue Jun 29 12:57:57 2010 ERROR
Invalid command. Use the following command:
GatewayUpgrade.exe <zip file>
Tue Jun 29 12:57:57 2010 ERROR
Tue Jun 29 12:57:57 2010 ERRORError code 1.
Tue Jun 29 12:57:57 2010 ERRORExiting setup.
```

7. At the command prompt enter the executable and the patch.zip to be applied and press **Enter** (GatewayUpgrade.exe setup-2.08.00.xx.zip).

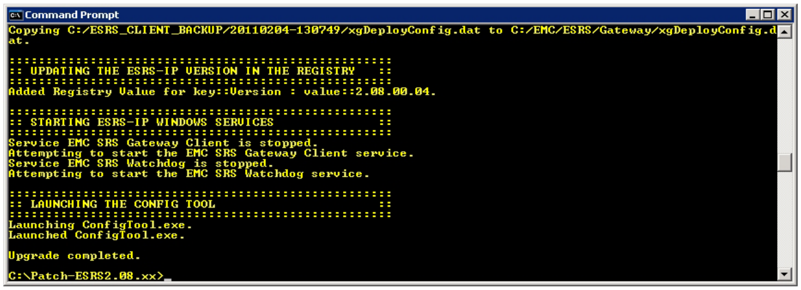


Command Prompt - GatewayUpgrade.exe setup-2.08.00.04.zip

```
C:\Patch-ESRS2.08.xx>dir
 Volume in drive C has no label.
 Volume Serial Number is 10C2-1EF0

 Directory of C:\Patch-ESRS2.08.xx

02/04/2011  01:05 PM    <DIR>          .
02/04/2011  01:05 PM    <DIR>          ..
02/04/2011  01:01 PM        15,580,207 2.08.00.04-patch.zip
02/04/2011  12:51 PM           344,064 Field Instructions 2.08.00.xx Patch-1.doc
02/04/2011  12:47 PM        26,470,530 Field Instructions 2.08.00.xx Patch.rtf
02/04/2011  01:04 PM        14,168,097 GatewayUpgrade-2.08.00.04.exe
01/05/2011  09:21 AM         1,794,048 GatewayUpgrade.exe
12/29/2010  02:12 PM        13,239,016 setup-2.08.00.04.zip
               6 File(s)     71,595,962 bytes
               2 Dir(s)  18,485,477,376 bytes free

C:\Patch-ESRS2.08.xx>GatewayUpgrade.exe setup-2.08.00.04.zip
****************************************************
*             START OF ESRS-IP UPGRADE             *
****************************************************
** This will upgrade your ESRS-IP gateway! **

Type Y to continue or N to quit.
```

Figure 96 **Command Prompt: Enter Executable**

8. Answer **Y** and press **Enter**. The patch process will proceed in the command window.

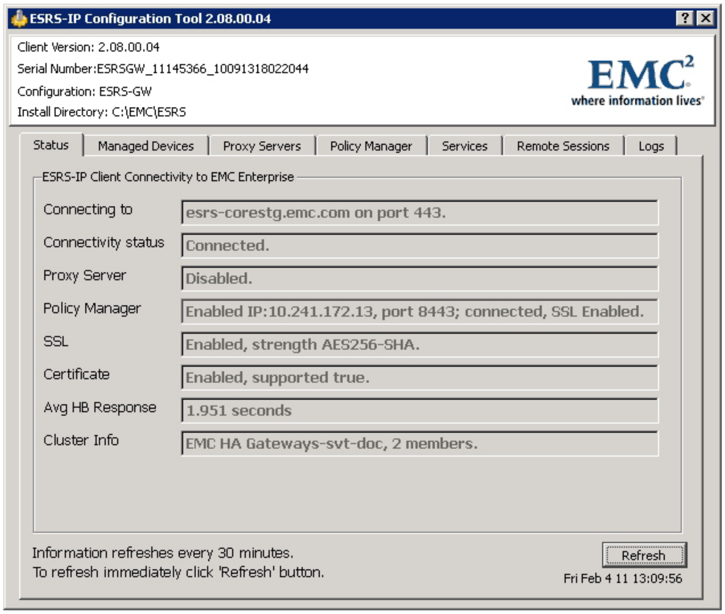


```
Copying C:/ESRS_CLIENT_BACKUP/20110204-130749/xgDeployConfig.dat to C:/EMC/ESRS/Gateway/xgDeployConfig.d
at.

::::::::::::::::::::::::::::::::::::::::::::::::::::
:: UPDATING THE ESRS-IP VERSION IN THE REGISTRY   ::
::::::::::::::::::::::::::::::::::::::::::::::::::::
Added Registry Value for key::Version : value::2.08.00.04.

::::::::::::::::::::::::::::::::::::::::::::::::::::
:: STARTING ESRS-IP WINDOWS SERVICES              ::
::::::::::::::::::::::::::::::::::::::::::::::::::::
Service EMC SRS Gateway Client is stopped.
Attempting to start the EMC SRS Gateway Client service.
Service EMC SRS Watchdog is stopped.
Attempting to start the EMC SRS Watchdog service.

::::::::::::::::::::::::::::::::::::::::::::::::::::
:: LAUNCHING THE CONFIG TOOL                      ::
::::::::::::::::::::::::::::::::::::::::::::::::::::
Launching ConfigTool.exe.
Launched ConfigTool.exe.

Upgrade completed.

C:\Patch-ESRS2.08.xx>_
```

Figure 97 Command Prompt: Answer Y to Proceed

9. The Configuration Tool (CT) will automatically launch. After the CT launches, close the command window.

10. Review the CT screens and check the connectivity status to EMC and Policy Manager. Refresh the screen if necessary.



Client Version: 2.08.00.04

Serial Number:ESRSGW_11145366_10091318022044

Configuration: ESRS-GW

Install Directory: C:\EMC\ESRS

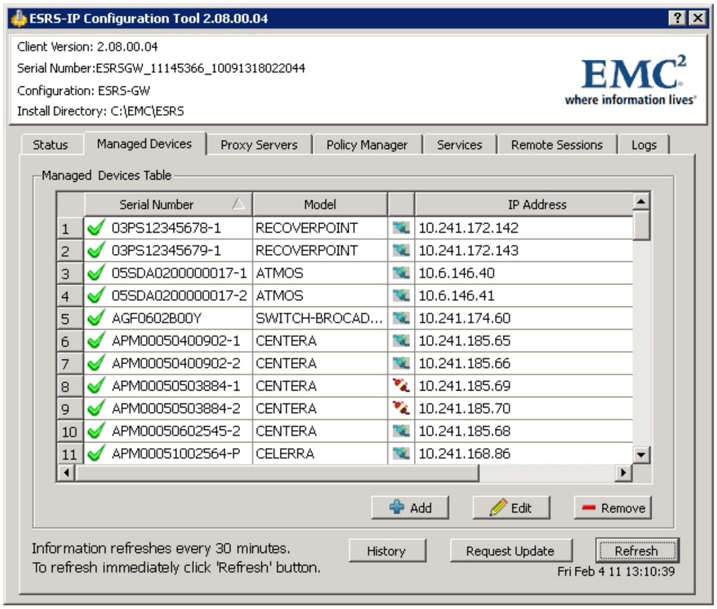
Connecting to	esrs-corestg.emc.com on port 443.
Connectivity status	Connected.
Proxy Server	Disabled.
Policy Manager	Enabled IP:10.241.172.13, port 8443; connected, SSL Enabled.
SSL	Enabled, strength AES256-SHA.
Certificate	Enabled, supported true.
Avg HB Response	1.951 seconds
Cluster Info	EMC HA Gateways-svt-doc, 2 members.

Information refreshes every 30 minutes.
To refresh immediately click 'Refresh' button.

Fri Feb 4 11 13:09:56

Figure 98 Connectivity Status

11. On the Managed Devices tab you will see your devices. Check connectivity. Refresh the screen if necessary.



ESRS-IP Configuration Tool 2.08.00.04

Client Version: 2.08.00.04
Serial Number:ESRSGW_11145366_10091318022044
Configuration: ESRS-GW
Install Directory: C:\EMC\ESRS

Managed Devices Table

	Serial Number	Model		IP Address
1	✓ 03PS12345678-1	RECOVERPOINT	●	10.241.172.142
2	✓ 03PS12345679-1	RECOVERPOINT	●	10.241.172.143
3	✓ 05SDA0200000017-1	ATMOS	●	10.6.146.40
4	✓ 05SDA0200000017-2	ATMOS	●	10.6.146.41
5	✓ AGF0602B00Y	SWITCH-BROCAD...	●	10.241.174.60
6	✓ APM00050400902-1	CENTERA	●	10.241.185.65
7	✓ APM00050400902-2	CENTERA	●	10.241.185.66
8	✓ APM00050503884-1	CENTERA	✗	10.241.185.69
9	✓ APM00050503884-2	CENTERA	✗	10.241.185.70
10	✓ APM00050602545-2	CENTERA	●	10.241.185.68
11	✓ APM00051002564-P	CELERRA	●	10.241.168.86

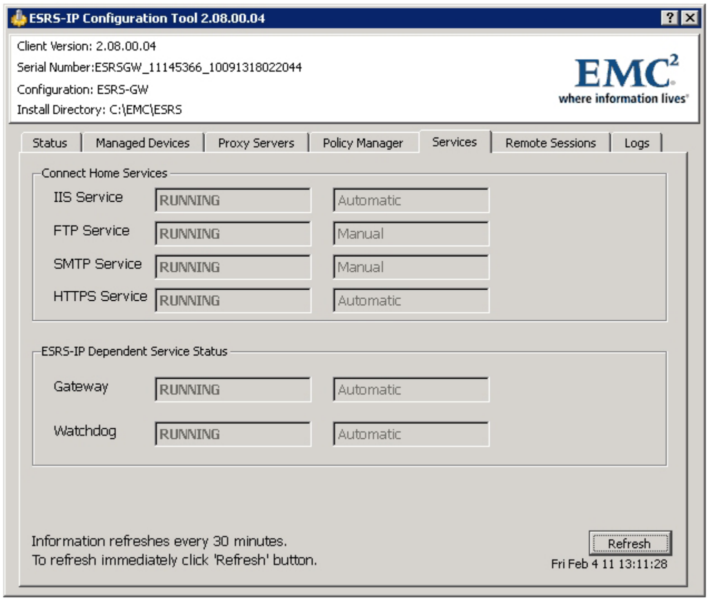
Information refreshes every 30 minutes.
To refresh immediately click 'Refresh' button.

Fri Feb 4 11 13:10:39

Figure 99 **Managed Devices**

12. Check other tabs on the Configuration Tool (CT) and confirm Status/Configuration is as expected. Refresh the screen if necessary.

13. On the Service tab, verify services are as expected. Refresh the screen if necessary.



Client Version: 2.08.00.04
Serial Number:ESRSGW_11145366_10091318022044
Configuration: ESRS-GW
Install Directory: C:\EMC\ESRS

Connect Home Services

IIS Service	RUNNING	Automatic
FTP Service	RUNNING	Manual
SMTP Service	RUNNING	Manual
HTTPS Service	RUNNING	Automatic

ESRS-IP Dependent Service Status

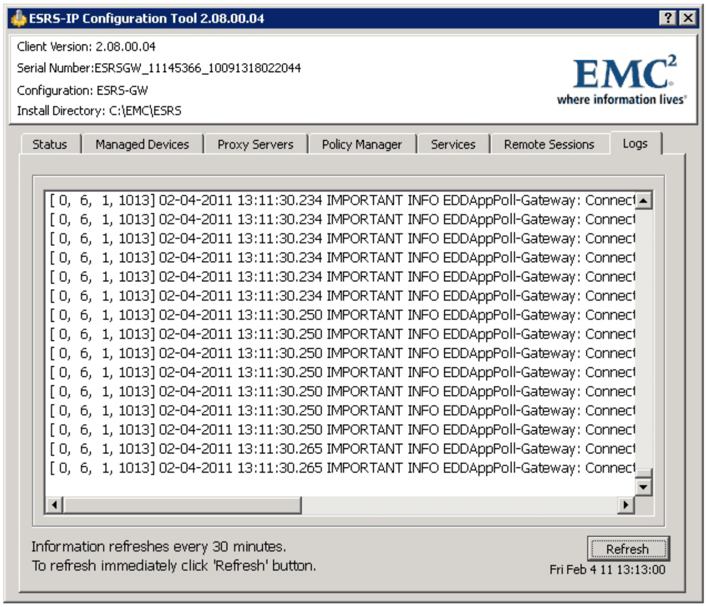
Gateway	RUNNING	Automatic
Watchdog	RUNNING	Automatic

Information refreshes every 30 minutes.
To refresh immediately click 'Refresh' button.

Fri Feb 4 11 13:11:28

Figure 100 Services Running

14. Also review the logs on the Log tab.



Client Version: 2.08.00.04
Serial Number:ESRSGW_11145366_10091318022044
Configuration: ESRS-GW
Install Directory: C:\EMC\ESRS

```
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.234 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.234 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.234 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.234 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.234 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.234 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.250 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.250 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.250 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.250 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.250 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.250 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.250 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.265 IMPORTANT INFO EDDAppPoll-Gateway: Connect
[ 0,  6,  1, 1013] 02-04-2011 13:11:30.265 IMPORTANT INFO EDDAppPoll-Gateway: Connect
```

Information refreshes every 30 minutes.
To refresh immediately click 'Refresh' button.

Fri Feb 4 11 13:13:00

Figure 101 **Review Logs**

15. You can also review the Upgrade Log (upgrade-YYYYMMDD-HHMMSS.log) in this case, upgrade-20101109-145831.log.

Note: During the upgrade the Gateway directory is backed up to the **C:\ESRS_CLIENT_BACKUP\20101109-145831** is the date- time/stamp of when the upgrade was performed. It is not removed after the upgrade has completed. If an issue occurs the Client can be recovered. If the patch is successful and you have limited disk space the backup of the Client can be removed manually if necessary.

Note: A complete log of the upgrade process is located in the directory from which the upgrade was executed.

If any upgrade issues occur the upgrade log **MUST** be included when requesting support the format of the file is upgrade-20101109-145831.log, where 20101109-145831 is the date/time stamp of when the upgrade was executed. Each upgrade attempt will have its own log. If multiple attempts have been made to upgrade a client, include all logs.

Table 6 Error Codes and where in the process they may occur

Step	Code	Error Scenario	Message
2	1	User enters invalid parameters into GatewayUpgrade.exe CLI	Invalid command. Use the following command: GatewayUpgrade.exe <zip file>
2	2	User enters a file name that does not exist into GatewayUpgrade.exe CLI	<file name> file does not exist.
4	3	User cancels upgrade process	User entered 'n'. User cancelled upgrade.
5	10	Missing Registry Entry	Options: • Client service name is null or empty. • Watchdog service name is null or empty. • HTTPS Listener service name is null or empty. • Current ESRS-IP Version is null or empty. • Base Path is null or empty. • Configuration Type is null or empty. • Gateway Config Path is null or empty.
6	4	Installation directory has insufficient disk space	Available space check failed.
7	5	Configuration type other than ESRS-GW is installed	"ESRS-IP configuration type check failed." "Configuration type <detected value> does not match ESRS-GW."
8	6	ESRS Client version does not equal 2.02	ESRS-IP version check failed. Current version of <detected value> does not match required version of 2.02.00.
8	6	ESRS Client 2.04 is installed	ESRS-IP version check failed. System is already at version 2.04.00.
9	7	User has insufficient rights	User does not have admin privilege.
12	8	Error occurred while applying patch. Upgrade Software must roll back to the original version.	Options: • Failure during stopping of services. Trying to roll back. • Failure during backing up client. Trying to roll back. • Failure during copying new files. Trying to roll back. • Failure during updating the registry. Trying to roll back.

Gateway Client Uninstallation

When uninstalling the Gateway Client, it is very important to complete all steps in the process. Devices that are managed by a single Gateway Client must be unmanaged, the Gateway Client must be set offline within ServiceLink and, if clustered, the Gateway should be unenrolled prior to uninstallation. Devices need not be undeployed if the Gateway is being uninstalled due to some failure provided another Gateway will be installed and clustered with the original Gateway. This will eliminate the possibility of unnecessary service requests being created.

If the devices are managed by other Gateway Clients in the cluster and you intend to continue to manage them within the cluster, do NOT undeploy the devices prior to uninstalling the Gateway Client.

The Provisioning Tool, which will be used to uninstall the Gateway Client, will remain.

To uninstall the Provisioning Tool, use Add/Remove programs. The Provisioning Tool cannot be uninstalled if the Gateway Client is still installed.

The 2.16.00.06 version of code adds an additional Service (SRS Gateway Proxy) to ESRS. This results in any attempt to uninstall the Gateway Client with a Provisioning Tool (PvT) version 2.14.XX.xx. or below will fail. The Provisioning Tool (PvT) will rollback the uninstall and restart all service relative to the ESRS Gateway. An additional tool has been added to the 2.16.00.06 Patch and Downloaded code to address this issue. Please see Primus emc287085: Provisioning Tool Error: ESRS Gateway uninstall fails after 2.16.xx.xx patch installation OR fresh installation with Provisioning Tool 2.14.xx.xx or earlier

2.16.00.06 and Above Uninstall Process

If ESRS Gateway Client was installed with the 2.16.00.06 PvT the uninstall process is the same as previous. If however the ESRS Gateway Client was patched from a lower level of code OR was a fresh install from the Provisioning Service (PvS) with a Provisioning Tool (PvT) version **2.14.XX.XX or BELOW** the alternate method using the standalone uninstaller application must be used

The 2.16.XX.XX Gateway Code and/or patch includes a separate Uninstaller application located in:

```
<install_drive>:\EMC\ESRS\Uninstall\Gateway\2.XX.XX.XX.
```

Note: Due to the use of User Access Control (UAC) in W2k8 (Any Version) you may be required to execute the Uninstaller in a Command Window opened in RunAsAdministrator Mode to successfully uninstall install the Gateway

To uninstall

1. Open Windows Explorer.
2. Navigate to the Gateway uninstaller directory

   ```
   <install_drive>:\EMC\ESRS\Uninstall\Gateway\2.XX.XX.X
   X  _)
   ```

3. Double click the GatewayUninstaller.exe.
4. This will Launch a command window.
5. At the command prompt type **Y** and press **Enter**.
6. The Uninstaller will run and uninstall the Gateway Application and ALL its components.

Excerpt of the uninstall log

```
****************************************************
Wed Feb 1 18:39:43 2012 INFO         START OF ESRS-IP
UNINSTALL
Wed Feb 1 18:39:43 2012 INFO
****************************************************
Wed Feb 1 18:41:21 2012 INFOUser entered 'y'.
Wed Feb 1 18:41:21 2012 INFOUser elected to proceed
with uninstall.
Wed Feb 1 18:41:21 2012 INFO
Wed Feb 1 18:41:21 2012 INFO
::::::::::::::::::::::::::::::::::::::::::::::::::::
Wed Feb 1 18:41:21 2012 INFOREADING VALUES FROM THE
REGISTRY
Wed Feb 1 18:41:21 2012 INFO
::::::::::::::::::::::::::::::::::::::::::::::::::::
Wed Feb 1 18:41:21 2012 INFOClient service name: EMC
SRS Gateway Client
Wed Feb 1 18:41:21 2012 INFOWatchdog service name: EMC
SRS Watchdog
Wed Feb 1 18:41:21 2012 INFOHTTPS Listener service
name: ESRSHTTPS
Wed Feb 1 18:41:21 2012 INFORegistry value does not
exist ProxyServiceName
Wed Feb 1 18:41:21 2012 ERRORPrivoxy service name is
null or empty.
Wed Feb 1 18:41:21 2012 INFO  Using default value of
EMC SRS Gateway Proxy.
```

```
Wed Feb 1 18:41:21 2012 INFOCurrent ESRS-IP Version:
2.16.00.06
Wed Feb 1 18:41:21 2012 INFOBase Path: C:\EMC\ESRS
Wed Feb 1 18:41:21 2012 INFOConfiguration Type:
ESRS-GW
Wed Feb 1 18:41:21 2012 INFOGateway Serial Number:
ESRSGW_11145366_11102714179045
Wed Feb 1 18:41:21 2012 INFOGateway Config Path:
C:\EMC\ESRS\Gateway
Wed Feb 1 18:41:21 2012 INFO
   ~
   ~
   ~

::::::::::::::::::::::::::::::::::::::::::::::::::::
Wed Feb 1 18:41:21 2012 INFOCREATING A BACKUP OF THE
CURRENT ESRS-IP FILES
Wed Feb 1 18:41:21 2012
INFO:::::::::::::::::::::::::::::::::::::::::::::::::
:::
Wed Feb 1 18:41:22 2012 INFOZip 5 pct completed.
Wed Feb 1 18:41:22 2012 INFOZip 10 pct completed.
Wed Feb 1 18:41:22 2012 INFOZip 15 pct completed.
Wed Feb 1 18:41:23 2012 INFOZip 20 pct completed.
Wed Feb 1 18:41:23 2012 INFOZip 25 pct completed.
Wed Feb 1 18:41:24 2012 INFOZip 30 pct completed.
~
~
~
Wed Feb 1 18:41:36 2012 INFOREMOVING BACKUP FOLDER
Wed Feb 1 18:41:36 2012
INFO:::::::::::::::::::::::::::::::::::::::::::::::::
:::
Wed Feb 1 18:41:36 2012 INFO
Wed Feb 1 18:41:36 2012 INFOUninstall completed.
Wed Feb 1 18:41:36 2012 INFO
Wed Feb 1 18:41:36 2012 INFO It is OK to delete the
C:/EMC/ESRS/Uninstall/Gateway/2.16.00.06 directory.
Wed Feb 1 18:41:36 2012 INFO
Wed Feb 1 18:41:36 2012 INFOPress the<Enter>key to exit
7.PressEnterat the Prompt and the Window will close
Uninstall is complete and the directory structure is
deleted
```

If there is a need to reinstall the Gateway, it is recommended that you upgrade the Provisioning Tool (PvT) before reinstalling the new Gateway. Acquire a copy of the latest Provisioning Tool (PvT) before uninstalling the existing Provisioning Tool (PvT) that is currently installed.

1. Uninstall the down rev version of the Provisioning Tool (PvT), as follows:
    - In Windows 2003, use the Control Panel\Add/Remove Programs to uninstall the PvT.
    - In Windows 2008, use the Control Panel\Programs and Features to uninstall the PvT.

Note: Gateway Device Client code must be uninstalled first. Uninstalling the Provisioning Tool (PvT) with a Gateway in Place will also uninstall the Gateway Client.

1. Install the new version of the Provisioning Tool (PvT) (in this case 2.16.00.06).
2. Install the new Gateway.

Note: This Solution may also be used if there are issues using the 2.16.xx.xx Provisioning Tool for uninstall of the Gateway.

Also see Primus emc239260, “Provisioning Tool Error: ESRS Gateway uninstall fails” for other possible solutions.

7

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 214
- Troubleshooting ESRSHTTPS.. 215

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 189.
- 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 189.

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 189.

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 Gateway 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 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.

Index

Symbols

.NET Framework 43, 44

A

access control
- device 38
- device configuration 38
- EMC Enterprise 39

architecture, ESRS 18
Atmos 25, 170
Avamar 25, 170

B

backup
- Gateway Client 188
- image 188
- procedure 188
- restoration 188

Brocade-B 26, 171

C

Celerra 25, 36, 170
Centera 25, 170
Cisco 26, 171
CLARiiON 25
Clariion 170
CLARiiON Management Station 36
Code version 170
Configuration Tool 33
- device management 34
- displaying log files 181
- displaying remote sessions 180
- displaying service status 179
- if running Windows 2008 163
- installing 33
- linking a Client to a Policy Manager 176
- menu items 33
- proxy server communication 175
- uninstalling 182
- viewing connectivity status 167

Connect homes 19
Connectrix 26, 36, 170
Customer Management Station 26, 171
customer responsibilities 28

D

Data Domain 26, 171
DCA 36, 171
device configuration access control 38
device management
- history 174
- managing or viewing devices 168
- synchronization 19

Digital Certificate Management 37
DL3D 26, 36, 171
DLm 26, 171
DLm3 171
DLm4 171

E

EDL 26, 36, 171
e-mail
- configuration and testing 55

EMC Global Services responsibilities 28
ESRS

- architecture 18
- Gateway Extract Utility 35

ESRSConfig user account 50
ESRSHTTPS listener service 215

F

firewall settings, Windows 2008 110
FTP
- server configuration 90
- service 71
- site messages 102

G

Gateway Client 42
- IIS 45
- IIS 6.0 deployment 48
- IIS 7.0 deployment 61
- IIS settings 46
- Internet protocols 43
- Microsoft .NET Framework 44
- operating system configuration 42
- required software applications 42
- server preparation 41
- Windows 2008 firewall settings 110

Gateway Extract Utility (GWExt) 35
Greenplum DCA 26

H

hardware failure 214
heartbeat polling 22
heartbeat, defined 22
High Availability Gateway Cluster 30
- configuration 30
- installing 31
- synchronization 31

HTTPS event notifications 215

I

IIS
- IIS 6.0 deployment 48
- IIS 7.0 deployment 61
- settings 46

image backup 188
Internet protocols 43
Invista 26, 171
Invista Element Manager 36
Isilon 26, 36, 171

M

managing devices 168
Microsoft .NET Framework 43, 44

O

OnAlert user account 50
operating system
- configuration 42
- failure 214

P

Policy Manager
- maintenance 185

power sequences 184
proxy server
- communication 176

R

RecoverPoint 26, 171
remote access 24
restoration procedures 189

S

server maintenance 183
service events, unexpected 214
service status 179
SMTP
- server configuration 85
- service 78

Suffix 170
Switch-Brocade-B 26, 171
Switch-Cisco 26, 171
Symmetrix 26, 36, 171

T

testing
- FTP server 114
- SMTP e-mail server 116
- Windows 2008 firewall 114

time zone 42, 185
troubleshooting
  ESRSHTTPS 215
  unexpected service events 214

U

user authentication 19

V

ViPR 26, 36, 171
VMAX Cloud Edition (CE) 26, 36, 171
VMware
  minimum requirements 30
  support 30
VNX 26, 36, 171
VNXe 26, 37, 172
VPLEX 27, 37, 172

X

XtremIO 27, 37, 172