



Citi Architecture and Technology Engineering

EMC Secure Remote Support v2.28

GDSE-07006-SG

Solutions Guide

Version 2.2

Version Control

Version	Date	Author	Reviewed	Comments
1.0	30-July-07	Kevin Hobaugh	SAN Stakeholders	Added CM on SOE, CX and Centera
1.1	15-Oct-07	Kevin Hobaugh	SAN Stakeholders	Modified Section 8.4.2 for CM and Centera device group settings.
1.2	9-Nov-07	Kevin Hobaugh	SAN Stakeholders	Modified ESRS SMTP configuration
1.3	28-Feb-08	Kevin Hobaugh	Global Stakeholders	Patched ESRS Gateway with version 1.01.03/1.01.05 to provide support for EMC Cisco MDS Switches
1.4	7-Mar-08	Kevin Hobaugh	Global Stakeholders	- Added VMware Support Statement - Added section for a "Redundant Policy Manager Server"
1.5	18-Mar-08	Kevin Hobaugh	Global Stakeholders	RFC - Minor Modifications -Secondary (Standby) Policy Manager. -Added installation responsibility -CEP ports
1.6	26-Mar-08	Kevin Hobaugh	Global Stakeholders	- Added Section 7.4 required Gateway directories and files - Modified Section 7.6 Added FTP config and Local Acct - Modified Gateway install steps - Added Post install steps

Version	Date	Author	Reviewed	Comments
				- Added Appendix for ESRS SG Release Notes (Details)
1.7	12-Dec-08	Kevin Hobaugh	Gary Johnson	Peer Review Patched ESRS Gateway with version 1.01.07/1.01.09 to provide support for - EDL (EMC Disk Lib) - LDAP Integration w/Policy Manager
1.8	12-Dec-08	Kevin Hobaugh	Global Stakeholders	RFC – Patched ESRS Gateway with version 1.01.07/1.01.09 to provide support for - EDL (EMC Disk Lib) - LDAP Integration w/Policy Manager - Password Encryption
1.8	09-Jan-09	Kevin Hobaugh	Global Stakeholders	Production Release <i>No changes since RFC</i>
1.9	16-Feb-09	Kevin Hobaugh	SAN Stakeholder	Production: Minor update Added Section: 9.8 Functional IDs
1.91	15-Apr-09	Kevin Hobaugh	GDSE / SAN Stakeholders	Peer/RFC - -Changed policies for EMC remote access to “Always Allow”. -Removed need for Policy Manager -Added Remote Access Procedure for Operations.
1.92	24-Apr-09	Kevin Hobaugh	SAN Stakeholders	Production: -Added Section 8, High Level Installation Steps

Version	Date	Author	Reviewed	Comments
				-Added Section 10, Steps to “Disable Policy Manager”
1.93	09-Sep-09	Kevin Hobaugh	GDSE	Peer Review – Patched ESRS Gateway with version 1.02.00 to provide support for V-MAX storage array
1.94	16-Sep-09	Kevin Hobaugh	SAN Stakeholders	RFC – Patched ESRS Gateway with version 1.02.00 to provide support for V-MAX storage array
1.95	02-Oct-09	Kevin Hobaugh	SAN Stakeholders	Production- Patched ESRS Gateway with version 1.02.00 to provide support for V-MAX storage array
1.96	06-Aug-10	Kevin Hobaugh	SAN Stakeholders	Production- Added Appendix J: Disabling EMC Remote Access to Celerra and EDL
1.97	05-Dec-12	Kevin Hobaugh	CSBE	Peer Review/RFC -ESRS v2.14 Patch (Data Domain and VNX Support) -Adding ability for ESRS to listen on SMTP port 25
2.0	11-Dec-12	Kevin Hobaugh	SAN Stakeholders	Production: -ESRS v2.14 Patch (Data Domain and VNX Support) -Adding ability for ESRS to listen on SMTP port 25

Version	Date	Author	Reviewed	Comments
2.1	18-Dec-13	Kevin Hobaugh	Global SAN Stakeholders	RFC/RFP *ESRS v2.24 on W2K8 R2 *Required for VNX2 support
2.11	09-Mar-15	Kevin Hobaugh	CSBE	Peer Review ESRS 2.28 Upgrade patch for VMAX3 support.
2.2	20-Mar-15	Kevin Hobaugh	Global SAN Stakeholders	RFC ESRS 2.28 Upgrade patch for VMAX3 support.
2.2	1-April-15	Kevin Hobaugh	Global SAN Stakeholders	RFP ESRS 2.28 Upgrade patch for VMAX3 support.

Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, CITIGROUP and the Umbrella Device are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

Contact

Please address any comments or questions regarding the information contained in this document via email to the “*CATE Storage and Backup Engineering” distribution list.

Latest Versions

It is recommended that the latest version of the document be used from the [CATE - Storage and Backup Engineering](#) website. Newer versions may include expanded scope, or comments on issues discovered after deployment.

Table of Contents

1. INTRODUCTION.....	10
1.1. GATEWAY SERVER	10
1.2. ESRS SOLUTION ARCHITECTURE.....	11
2. PREREQUISITES.....	12
2.1. EMC CHECKLIST QUESTIONNAIRE	12
2.1.1. <i>Required</i>	12
2.2. FIREWALL RULE CHANGES.....	12
2.3. GATEWAY SERVER REQUIREMENTS.....	12
2.3.1. <i>Software (Windows 2008)</i>	12
2.3.2. <i>Hardware</i>	13
2.4. VMWARE ESX SUPPORT STATEMENT.....	13
2.5. IIS 7.5 AND SMTP INSTALLATION.....	13
3. HIGH LEVEL ESRS INSTALLATION PROCESS ON WINDOWS 2008....	21
3.1. ESRS V2.24 FOR WINDOWS 2008	21
3.2. ESRS V2.28 PATCH	21
4. ESRS DETAILED INSTALLATION STEPS ON WINDOWS 2008	21
4.1. ESRS V2.24 PACKAGE INSTALLATION	22
4.2. GATEWAY SERVER INSTALLATION.....	22
4.2.1. <i>PVT (Provisioning Tool) Installation</i>	22
4.2.1. <i>Gateway Installation via PVT</i>	27
5. CONFIGURE ESRS FOR SMTP (POST ESRS INSTALL)	33
5.1. SMTP CONFIGURATION.....	35
6. POST ESRS MIGRATION INSTALLATION STEPS	41
7. AUDITING.....	41
8. HIGH AVAILABILITY GATEWAY CLUSTER CONFIGURATION	41
8.1. GATEWAY CLUSTER SYNCHRONIZATION.....	42
8.2. SINGLE OR HA GATEWAY SAN DEVICE LIMITS.....	43
9. CONFIGURATION TOOL.....	43
9.1. VIEW CONNECTIVITY STATUS.....	44
9.2. MANAGE DEVICES	44
9.2.1. ADD, EDIT, OR REMOVE DEVICES FROM ESRS.....	45
9.3. PROXY SERVERS.....	48
9.4. STATUS OF IP SERVICES	49
9.5. ACTIVE REMOTE SESSIONS	50
9.6. CONFIGURATION TOOL LOGS	50
10. DEVICE DEPLOYMENT.....	51

10.1.	SYMM / DMX / V-MAX.....	51
10.1.1.	Prerequisites.....	51
10.1.2.	Installation.....	51
10.2.	CONNECTRIX MANAGER SERVER NON-SOE (CSP)	52
10.2.1.	Prerequisites.....	52
10.2.2.	Installation.....	52
10.3.	CONNECTRIX MANAGER SERVER ON SOE (CSP)	52
10.3.1.	Prerequisites.....	52
10.3.2.	Installation.....	52
10.4.	CLARIION	53
10.4.1.	Prerequisites.....	53
10.4.2.	Installation.....	53
10.5.	VNX.....	53
10.6.	CENTERA	53
10.6.1.	Prerequisites.....	53
10.6.2.	Installation.....	54
10.7.	CISCO MDS SWITCH (EMC SUPPLIED ONLY)	54
10.7.1.	Prerequisites.....	54
10.7.2.	Installation.....	54
10.8.	EDL (EMC DISK LIBRARY).....	54
10.8.1.	Prerequisites.....	54
10.8.2.	Installation.....	54
10.9.	DATA DOMAIN.....	55
10.9.1.	Prerequisites.....	55
10.9.2.	Installation.....	55
10.10.	EMC CELERRA NAS	55
10.10.1.	Prerequisites.....	55
10.10.2.	Installation.....	56
11.	APPENDIX A: REFERENCES AND RELATED DOCUMENTS.....	57
12.	APPENDIX B: EMC ALERT NOTIFICATION (HOW IT WORKS).....	58
13.	APPENDIX C: EMC REMOTE ACCESS (HOW IT WORKS).....	59
14.	APPENDIX D: USE OF PROXY SERVER	60
15.	APPENDIX E: ARCHITECTURE APPROVALS.....	60
16.	APPENDIX F: CEP FIREWALL PORT REQUIREMENTS.....	60
16.1.	SYMMETRIX / DMX / V-MAX	60
16.2.	CONNECTRIX MANAGER SERVER (SOE - CITI SERVER)	61
16.3.	CONNECTRIX MANAGER SERVER (NON SOE – EMC SERVER).....	61
16.4.	CLARIION/VNX	61
16.5.	EDL ENGINE (EMC DISK LIBRARY)	61
16.6.	CENTERA	61
16.7.	CISCO MDS SWITCHES (EMC SUPPLIED).....	62
16.8.	CELERRA NAS	62

17.	APPENDIX G: SUPPORTED STORAGE DEVICES	63
17.1.	AVAMAR	63
17.2.	SYMMETRIX / DMX / V-MAX	63
17.3.	CONNECTRIX MANAGER SERVER	63
17.4.	CLARIION	63
17.5.	EDL ENGINE (EMC DISK LIBRARY)	63
17.6.	CENTERA	63
17.7.	CISCO MDS SWITCHES	63
17.8.	CELERRA NAS	64
17.9.	VNX	64
17.10.	DATA DOMAIN	64
18.	APPENDIX I: EMC REMOTE ACCESS PROCEDURE	64
19.	APPENDIX J: DISABLING EMC REMOTE ACCESS TO CELERRA AND	
EDL	67	
19.1.	DISABLE ACCESS TO CELERRA AND EDL	67
19.2.	DISABLING NEWLY ADDED DEVICES	67
20.	APPENDIX K: HOW EMC HANDLES MISSING DEVICES	69
21.	APPENDIX L: ISSUES	70
21.1.	CONFIGURATION TOOL – CLIENT NOT RUNNING	70
22.	APPENDIX M: ESRS PATCHES	71
22.1.	ESRS V2.28 PATCH	71
23.	APPENDIX N: REVISION HISTORY	75

1. Introduction

EMC's Secure Remote Support Gateway product provides a secure, IP-based, distributed remote service support solution giving Citigroup control and visibility of remote support access.

Simplicity – The Gateway solution consolidates access points for EMC support by providing a uniform, standards-based architecture for remote access across EMC product lines. The benefits include the elimination of modems and modem lines, WWDS/CitiVPN/DialVPN connections, management of safeword tokens, Storage Operations controlled authorization of access for remote support events, and consolidated logging of remote access for audit review.

Improved Availability – Because the Gateway solution is built and supported by EMC, problems can be resolved faster because a single vendor will now own all the pieces. Also because fewer components are involved the risk of remote access malfunction from mis-configuration of a component is reduced.

Security – The Gateway solution fulfills CISS requirements for authentication, authorization and auditing.

- TLS v1.0 tunneling with Advanced Encryption Standard (AES) 256-bit SHA-1 data encryption
- Bilateral authentication of digital certificate registration
- X.509 digital certificates generation
- ESRS IP Client authentication based on digital certificate at EMC
- EMC-issued RSA SecurID Authenticators for digital certificate registration
- EMC-issued RSA SecurID for user authentication Secure remote application path using IP and port-mapping
- Access is restricted to authenticated and authorized EMC personnel

The Gateway solution has been reviewed and approved by Remote Access Engineering as well as Third Party Working Group (C3PAR).

1.1. Gateway Server

A Citi-supplied, dedicated server or pair of servers acts as the single point of entry and exit for all IP-based EMC remote support activity. The ESRS Gateway Client functions as communications brokers between the managed devices and the EMC Enterprise. All communication with EMC initiates from the ESRS Gateway Client on port 443 outbound. The ESRS Gateway Clients are HTTP handlers. All messages are encoded using standard XML and SOAP application protocols. ESRS Gateway Client message types include:

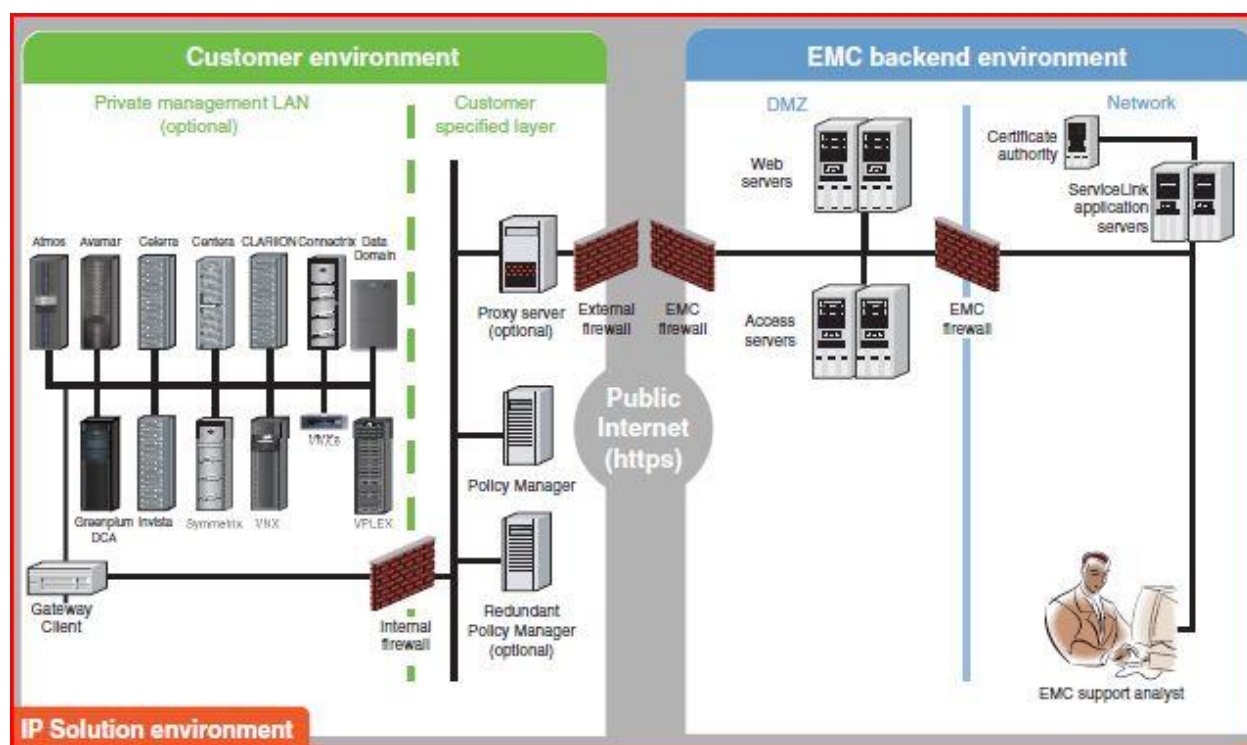
- Device state “heartbeat” polling

- Data file transfer
- User authentication requests
- Device management synchronization

The ESRS gateway will reside on the Citi Global Distributed Network (GDN). Via the Gateway, status and alert notifications are sent out to EMC through a tunneled connection inside an HTTPS session via Citi HTTP/HTTPS Proxy server. EMC remote access activity (troubleshooting / maintenance) comes back through the tunneled connection initiated from Citi.

1.2. ESRS Solution Architecture

The ESRS Gateway Client application architecture is a secure, asynchronous messaging system designed to support the functions of secure encrypted file transfer, monitoring of device status, and remote execution of diagnostic activities. This distributed solution is designed to provide a scalable, fault-tolerant, and minimally intrusive extension to your system support environment.



2. Prerequisites

2.1. EMC Checklist Questionnaire

Complete the “Gateway Pre-Site Checklist” (P/N 300-002-771) document. It can be obtained from the CSBE [ESRS](#) website or EMC Customer Service. This document will assist EMC and Citi personnel install EMC Secure Remote Support.

Engage EMC Customer Service (Customer Engineer) early in the planning process.

2.1.1. Required

- Site Information (Name, Site ID)
- Storage products and serial numbers
- Citi Proxy Server IP address (obtain from *CATE Network – Perimeter)
- Storage IP address ranges, subnet masks and gateway IP

2.2. Firewall Rule Changes

1. A Firewall Request for the new ESRS IP addresses will be needed for storage devices residing behind a firewall (CEP).
2. Engage EMC CE for assistance with the ESRS installation portion. There are steps only EMC can execute.
3. Post installation: On all the Symm products, an EMC CE will need to be engaged to modify ConnectEMC to point to the new ESRS GW IP addresses. Also, any left over Connectrix Mgr applications will need to have their ConnectEMC modified.

2.3. Gateway Server Requirements

2.3.1. Software (Windows 2008)

- Windows Server 2008 R2 Standard x64 Edition SP1
- IIS 7.5 TPM Packages in this order:
 - (1) **CITI_WIN_x64_IIS_Installation_01**
 - (2) **CITI_WIN_x64_IISBaseSecSetting_01**
 - (3) **CITI_WIN_x64_IIS_HFPackage_01**
 - IIS can be installed on the D:\drive
 - Configure IIS (Instructions in the IIS 7.5 Installation section)
 - After ESRS is installed, configure SMTP Server in IIS
 - **Note:** If you already have storage devices and they are configured to send alerts to the Gateway via port 3325, then add port 25 to the ESRS SMTP server. ESRS will listen on

both port 3325 and port 25. Any new arrays can be configured to use ESRS GW on port 25.

See Section 9: Device Deployment for more information on adding devices.

- .NET Framework 3.5 or greater (Required prior to installing ESRS)
- Microsoft Visual C++ 2005 SP1 Runtime Library

2.3.2. Hardware

- Processor: 2.5 GHz or greater (Dual preferred)
- Memory: 2 GB RAM minimum (3 GB recommended)
- Communication: 10/100 NIC (1 GB preferred by EMC)
- Storage: 1GB available for installation (40 GB or larger recommended)
- Network: Gateway should reside on the Global Data Network (GDN) with access to the EMC devices residing behind a firewall, Citigroup Extranet Platform (CEP). See [Section 14](#) for required firewall ports
- EMC does not recommend running the Gateway server on a shared server. **Note:** To reduce the cost of implementation at Citigroup, CSBE has tested and certified the Gateway server to run on servers running SANScreen server
- VMWare: ESX 2.5.2 or later, Minimum 15 GB partition size; 2.2GHz virtual CPU; 1 GB memory (2 GB recommended, 2-3 GB preferred)

2.4. VMware ESX Support Statement

EMC supports EMC Secure Remote Support Gateway on VMware ESX Server.

Note: The ESRS Gateway client cannot be moved with VMware VMotion due to RSA Lockbox restrictions.

CSBE does not recommend installing ESRS on ESX servers which reside on EMC storage or are SAN attached. Reasoning: If the EMC storage or the SAN were to go down, then ESRS would not function and EMC would be unable to receive alerts or connect remotely to provide support. For this reason, CSBE recommends that ESRS be installed on ESX running on NAS storage where available.

2.5. IIS 7.5 and SMTP Installation

Install the IIS TPM packages as instructed below on each ESRS Gateway Server before installing the ESRS Gateway software. IIS can be installed on the D:\drive. The installation will require adding the SMTP server.

1. Install the IIS 7.5 TPM Packages

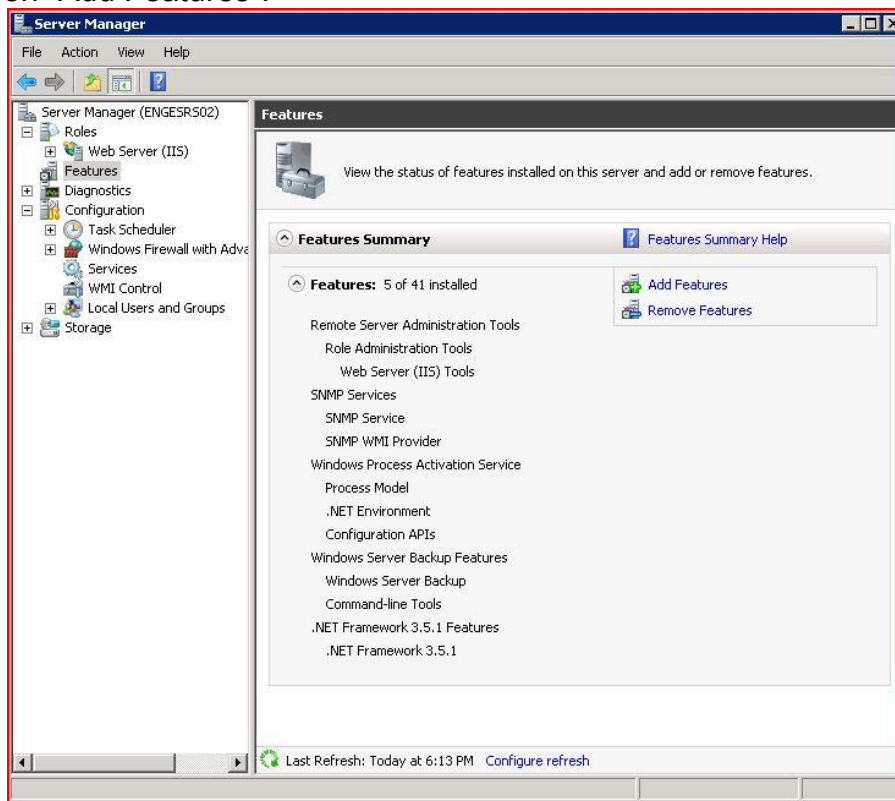
On the new W2k8 server, install the following IIS 7.5 TPM packages in this order. The server will reboot after each package is installed (BE PATIENT).

- A. CITI_WIN_x64_IIS_Installation_01**
- B. CITI_WIN_x64_IISBaseSecuSetting_01**
- C. CITI_WIN_x64_IIS_HFPackage_01**

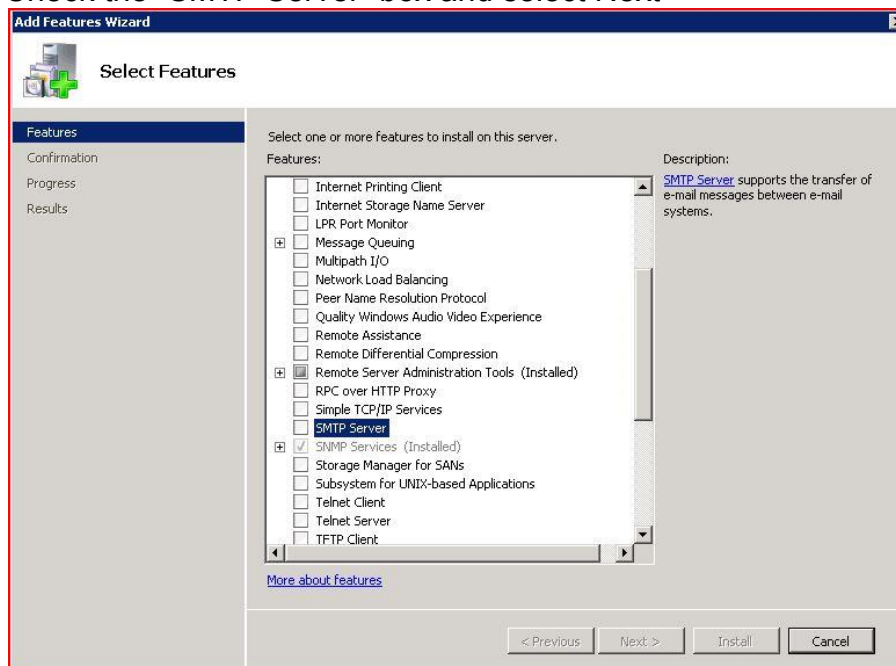
2. Configure IIS with SMTP Server

IIS 7.5 doesn't come with a built-in SMTP Server like IIS 6.0; it has to be added in.

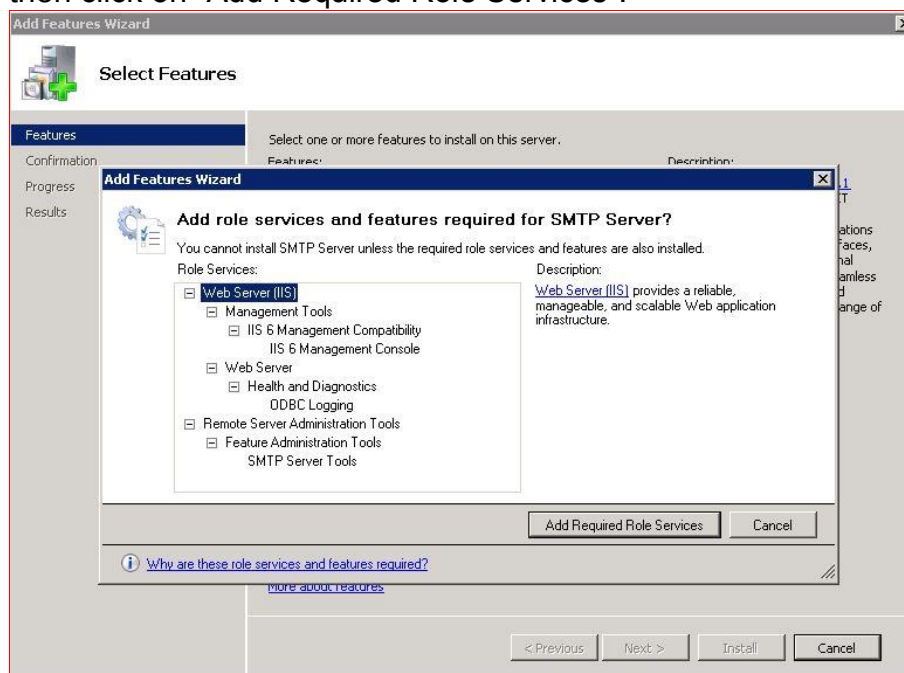
- A. Launch Server Manager by clicking Start / Administrative Tools / Server Manager. From the left pane, click on "Features". From the right pane, click on "Add Features".



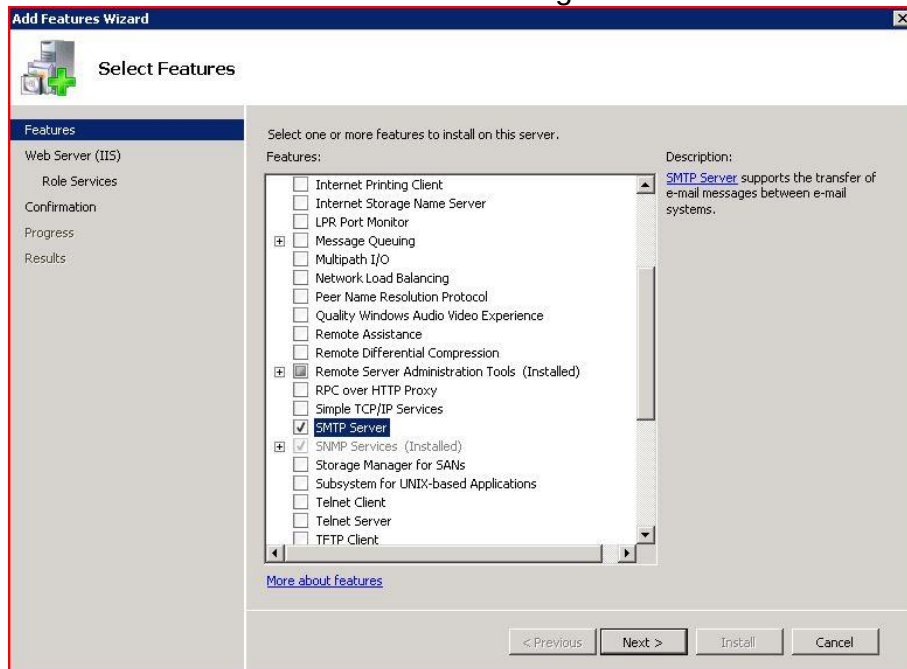
B. Check the “SMTP Server” box and select Next



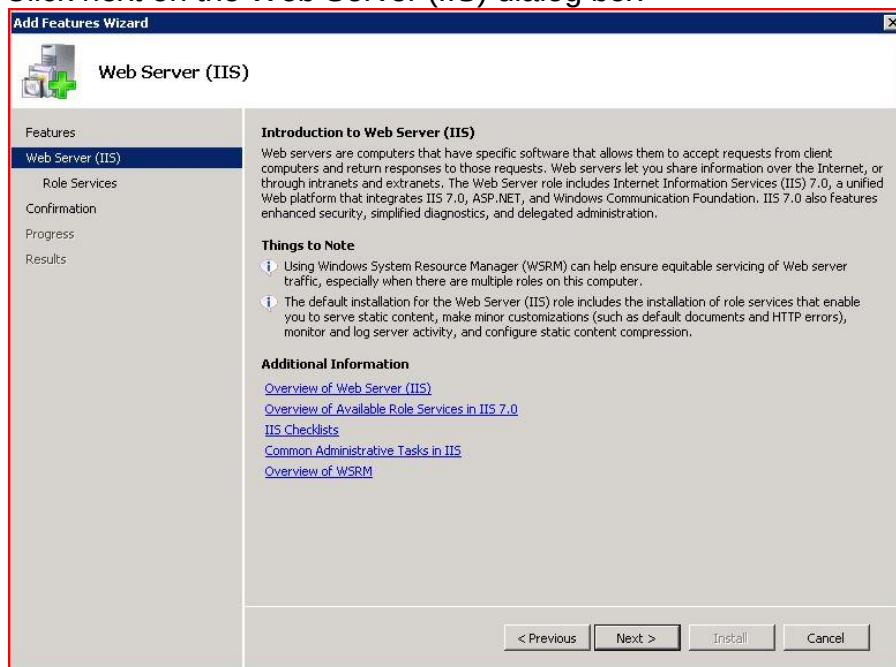
C. SMTP requires additional Role Services. Expand the plus sign to view them, then click on “Add Required Role Services”.



Click Next on the Select Features dialog box.

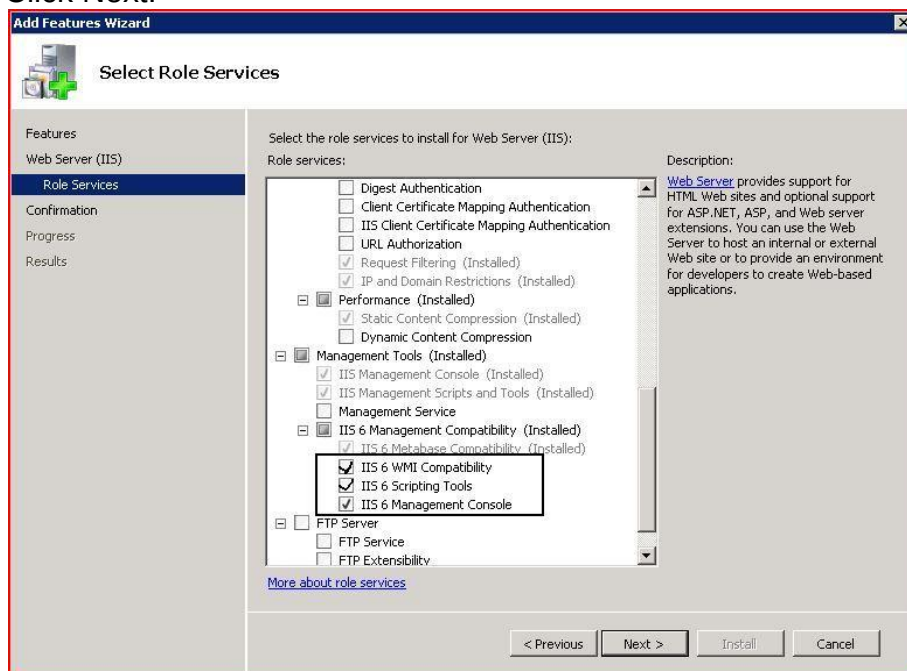


D. Click next on the Web Server (IIS) dialog box

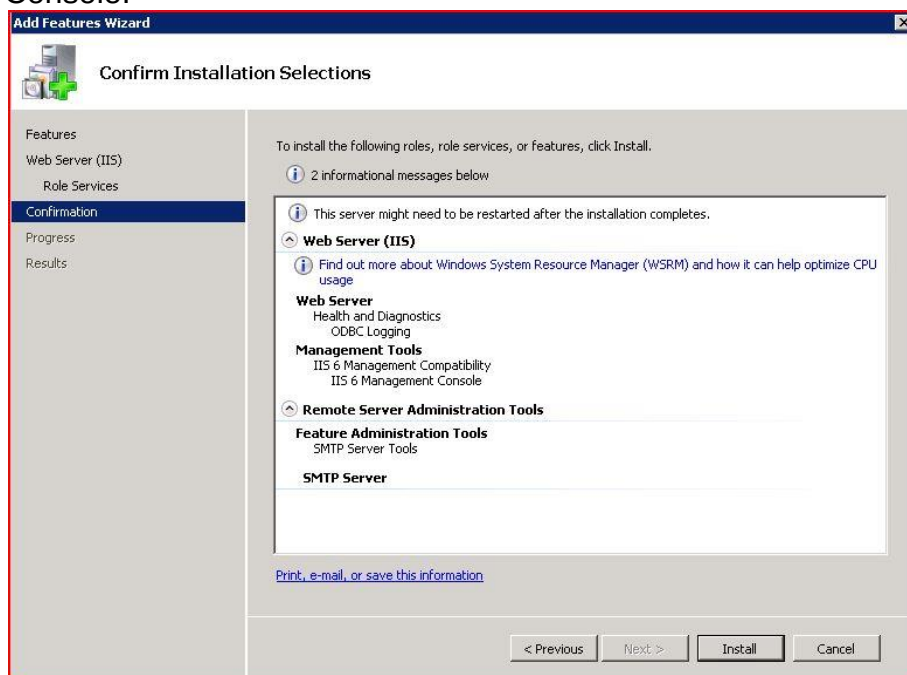


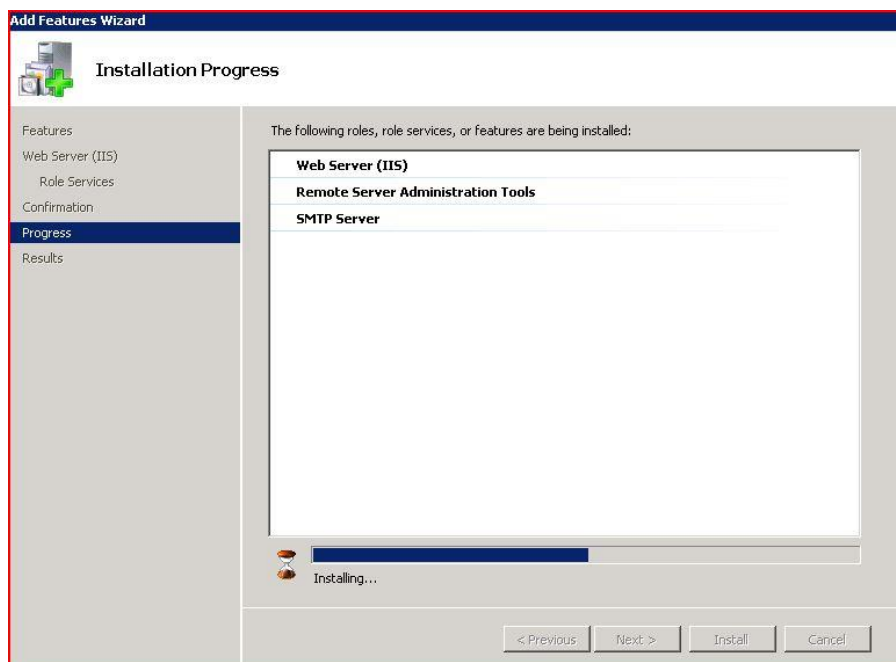
- E. Since IIS 7.5 doesn't come with SMTP, SMTP has to be managed by the IIS 6.0 management Console.

Under Role Services, scroll down to Management Tools/IIS 6 Management Compatibility. Check the boxes below if they are not already checked. Click Next.

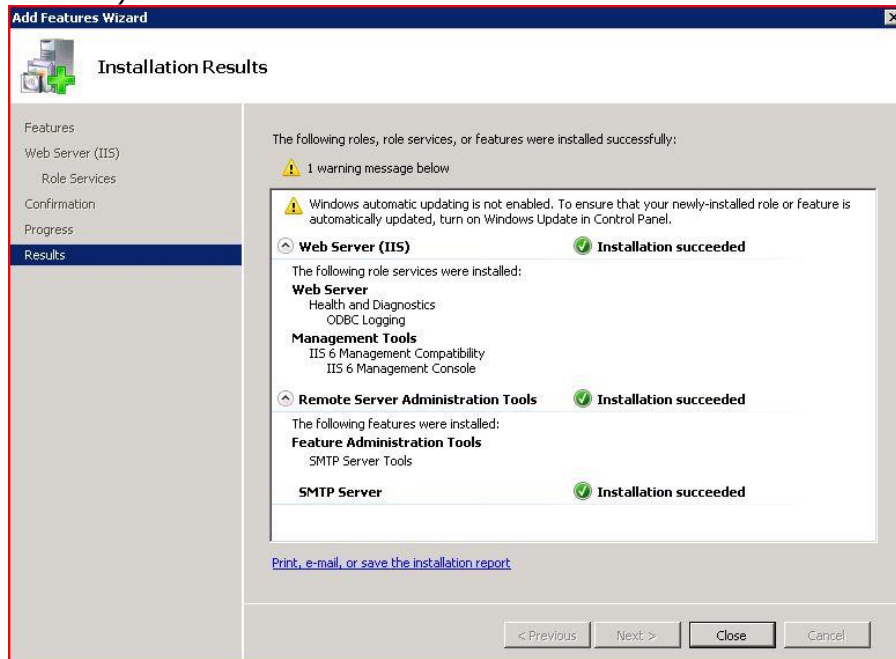


- F. Click Install to complete adding in SMTP and the IIS 6.0 Management Console.

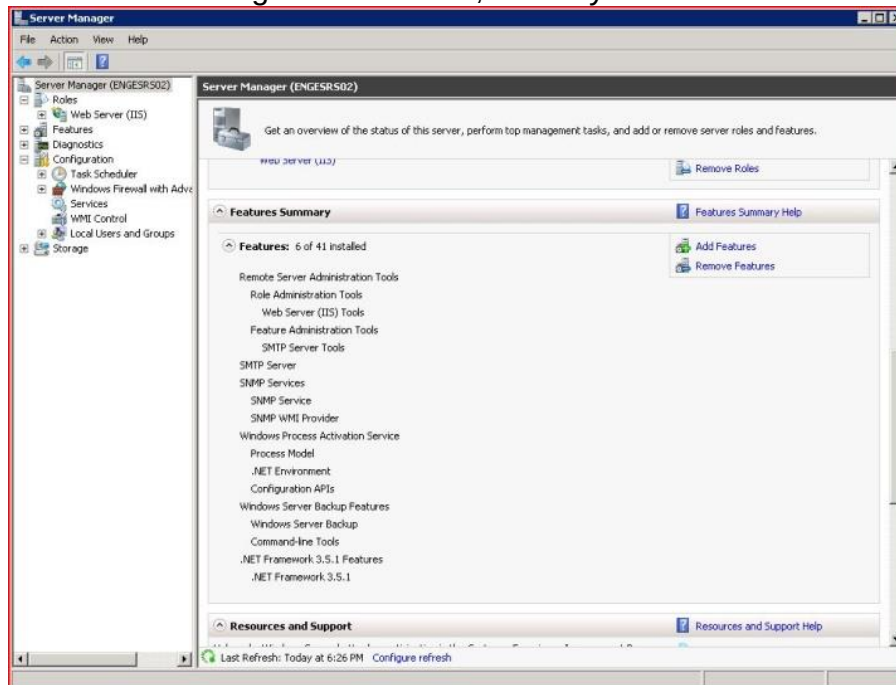




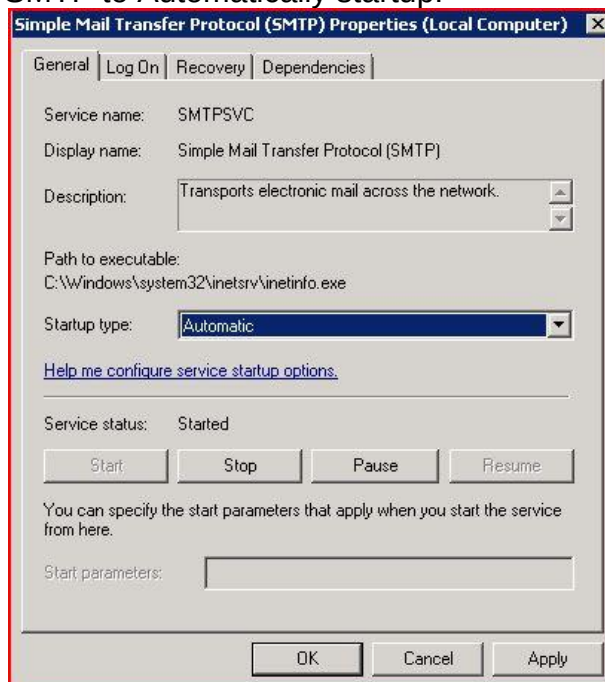
G. Installation complete, click Close (warning that Automatic Updates is not enabled).



H. Scroll down through the Features, to verify added features.



I. The SMTP service is set to Manual startup, by default. Open Services and set SMTP to Automatically startup.



- J. To create shortcuts on the desktop for IIS 6.0 Manager and the IIS 7.5 Manager, select Start / Administrative Tools, right click on IIS 6.0 Manager and IIS 7.5 Manager and send them to the desktop. Use the IIS 6.0 icon to manage the SMTP configuration.



ESRS Gateway is ready for installation.

3. High Level ESRS Installation Process on Windows 2008

To assist in determining what needs to be done, this section was added to give a high level of the steps you need to perform after the prerequisites are met.

Note: Engage EMC CE for assistance. There are steps only EMC can execute.

3.1. ESRS v2.24 for Windows 2008

Installation of ESRS is allowed on a D:\ drive.

1. From the Old Primary GW, document the current ESRS settings. Launch the “Configuration Tool” and document Site ID, Proxy address, port (should be 8080) and storage devices and their IP addresses.
2. From the New Primary GW (W2K8) with IIS7.5 installed and configured, install ESRS v2.24 W2k8 software via TPM package **CITI_WIN_2K8_SecureRemoteSupport_224_01** on the new W2k8 Primary GW server. The package will install the installation files into C:\ESRS_v2.24). With an EMC CE available, follow the instructions in the ESRS v2.24 Installation section.
3. EMC CE will add the New Primary GW to the cluster and sync it with the Old Primary GW.
4. Configure IIS SMTP.
5. Install the ESRS v2.24 on the New Secondary GW (W2K8) and sync it with the New Primary GW.
6. Configure IIS SMTP.
7. Modify Symmetrix products ConnectEMC to point to new ESRS GW IP addresses. Coordinate with EMC. An EMC CE will perform this task.
8. When ready, Before de-installing and powering off the Old GW servers (Windows 2003 Server), EMC CE will have to break the cluster relationship and take the Old GW's offline, then you can perform a clean uninstall using the PVT Tool.

3.2. ESRS v2.28 Patch

After installing and configuring ESRS v2.24, install the ESRS v2.28 Patch. Details are in [“Section 22: Appendix M”](#). If ESRS v2.24 is already installed and configured, proceed to Section 22 and install the v2.28 patch.

4. ESRS Detailed Installation Steps on Windows 2008

Installation of EMC Secure Remote Support is an interactive process and requires EMC assistance. During the install process there is Secure FOB information that EMC will have to enter to complete the installation.

ESRS v2.24 is in TPM package **CITI_WIN_2K8_SecureRemoteSupport_224_01**. The package will install the files required to perform the installation of ESRS IP Client v2.10.

4.1. ESRS v2.24 package installation

On the new W2k8 server, install the ESRS v2.24 package from TPM package

CITI_WIN_2K8_SecureRemoteSupport_224_01

The package will install the files required to perform the installation of ESRS v2.24 into directory **C:\ESRS_v2.24**.

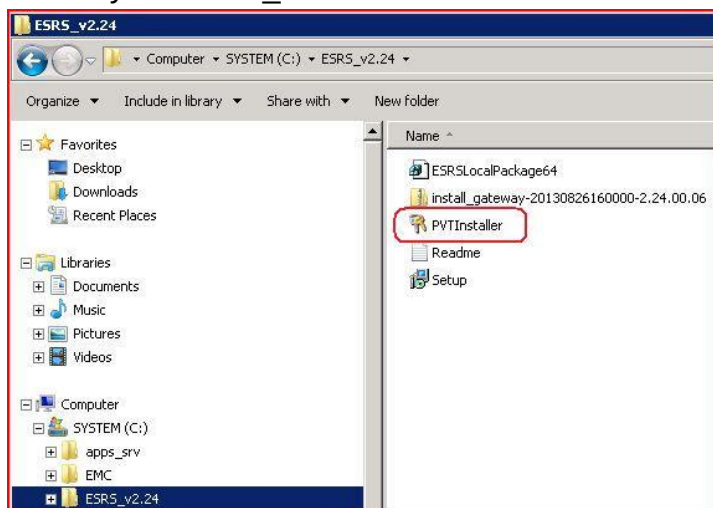
4.2. Gateway Server Installation

*The Gateway installation is performed by a **Citi SA and EMC**. During the installation there will be places where Citi will need to provide input and other places where EMC will provide input. The next sections list the points of interest.*

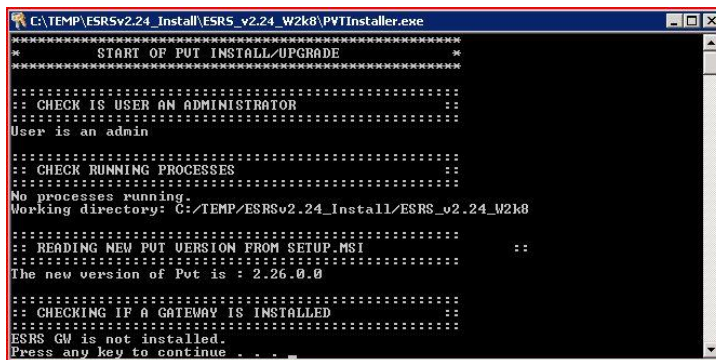
NOTE: With ESRS v2, EMC utilizes a **Provisioning Tool** to install the Gateway.

4.2.1. PVT (Provisioning Tool) Installation

1. Install the Provisioning Tool using the **PVTInstaller** (Run as Administrator) in the directory C:\ESRS_v2.24.



2. Installation script begins. Hit any key to continue.

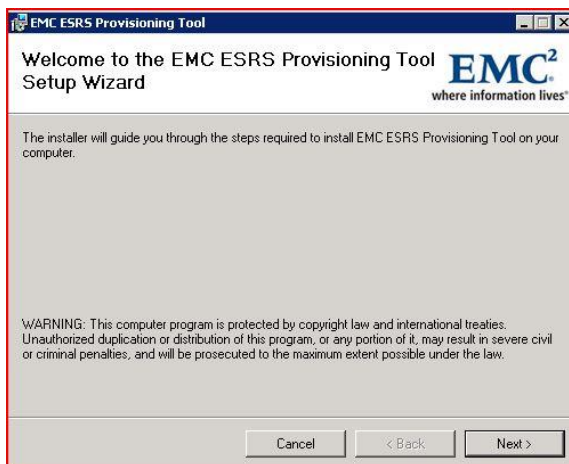


```

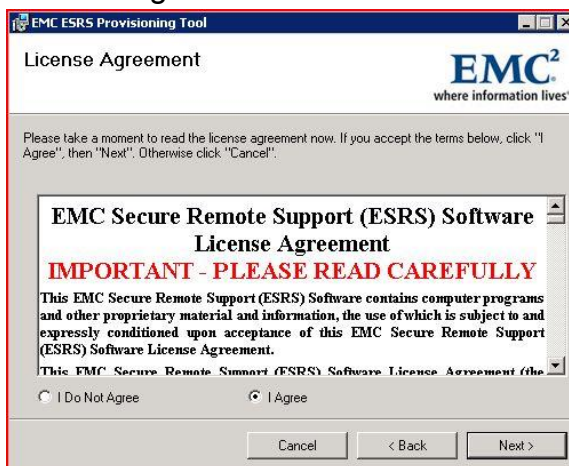
C:\TEMP\ESRSv2.24_Install\ESRS_v2.24_W2k8\PVTInstaller.exe
=====
START OF PVT INSTALL/UPGRADE
=====
:: CHECK IS USED AN ADMINISTRATOR
::
User is an admin
::
:: CHECK RUNNING PROCESSES
::
No processes running.
Working directory: C:\TEMP\ESRSv2.24_Install\ESRS_v2.24_W2k8
::
:: READING NEW PVT VERSION FROM SETUP.MSI
::
The new version of Pvt is : 2.26.0.0
::
:: CHECKING IF A GATEWAY IS INSTALLED
::
ESRS GW is not installed.
Press any key to continue . . .

```

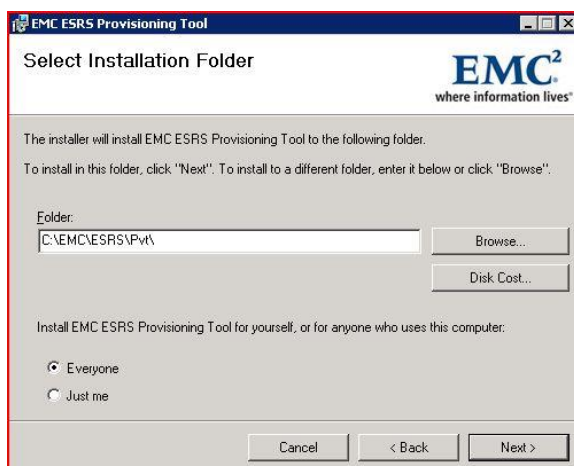
3. To continue with the PVT installation, click Next.



4. Select "I Agree" and click Next.



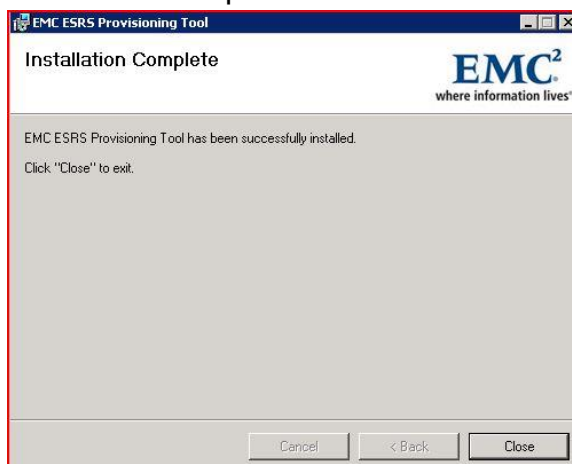
5. Choose your installation drive (D:\ drive is allowed) and click Next.



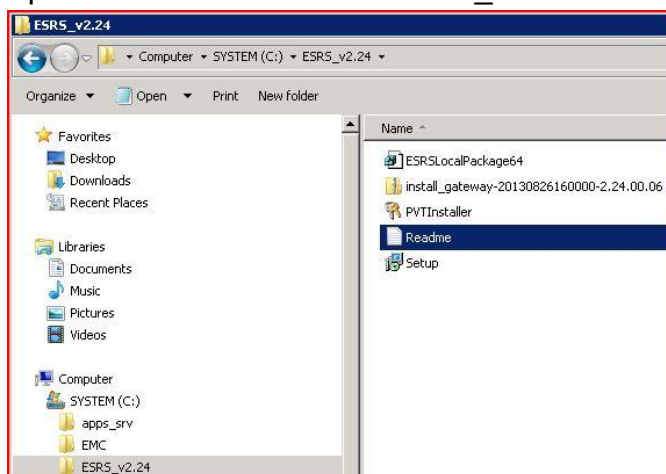
6. Confirm installation and click Next.



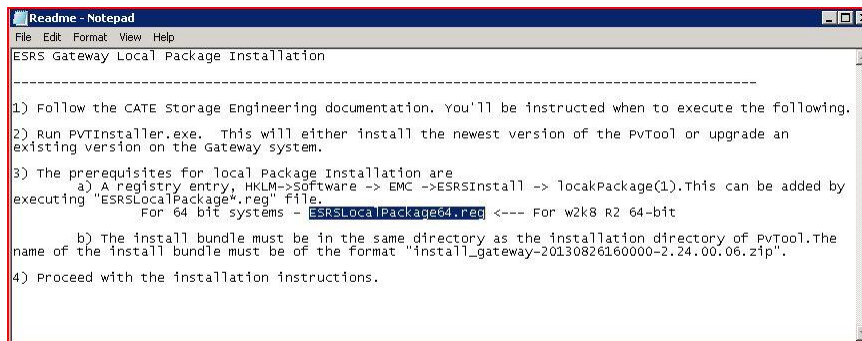
7. Installation complete. Click Close



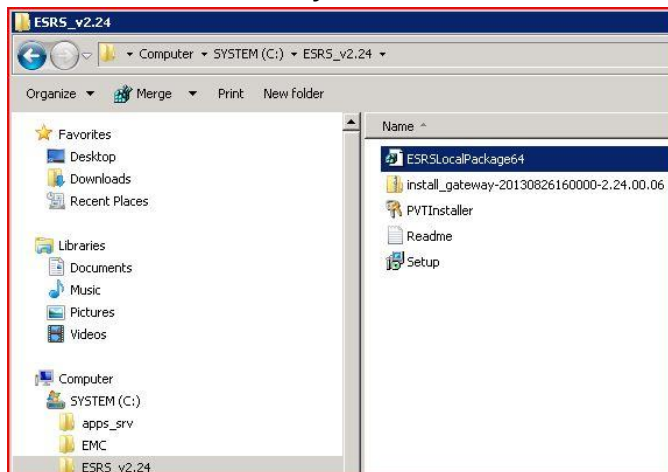
8. Open the Readme from C:\ESRS_v2.24.



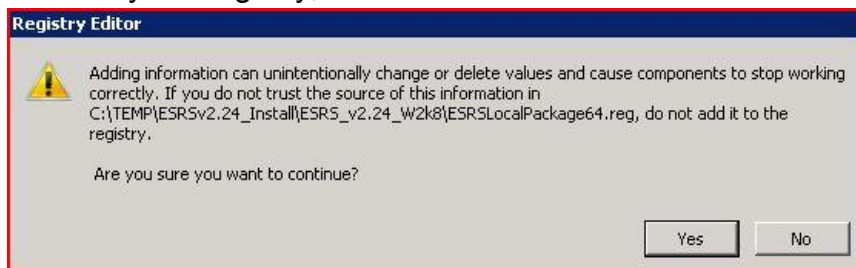
9. Review the Readme text document



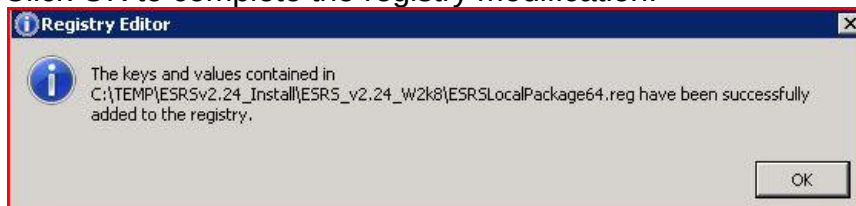
10. Double click the 64-bit registry file, (**ESRSLocalPackage64.reg**) to make the entry in the registry that will force the Provisioning Tool (PVT) to use version 2.x from our local directory.



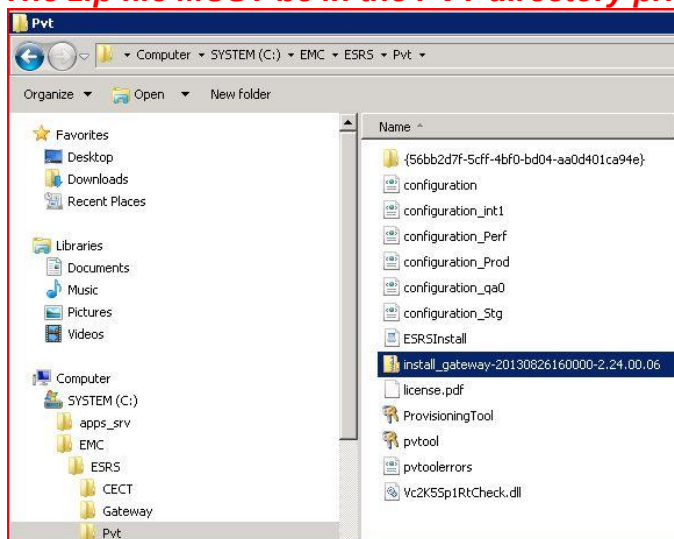
11. To modify the registry, click "Yes".



Click OK to complete the registry modification.



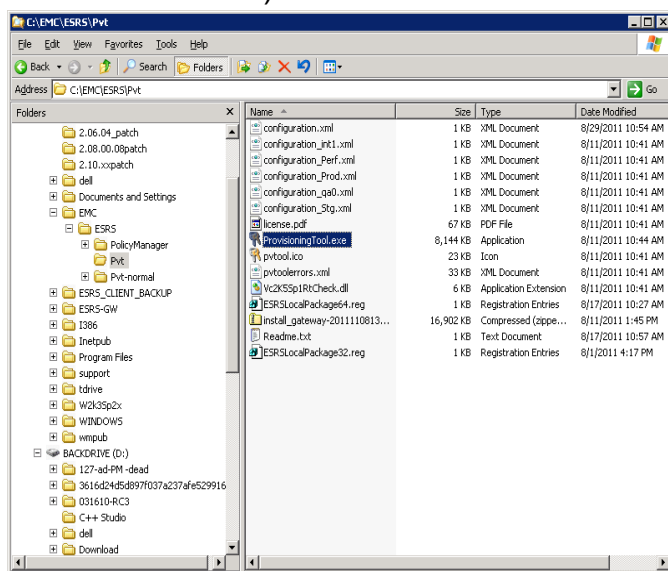
12. Copy the gateway zip file: **install_gateway-20130826160000-2.24.00.06.zip** from directory C:\ESRS_v2.24 to the PVT directory (*installdrive:\EMC\ESRS\Pvt*).
The zip file MUST be in the PVT directory prior to ESRS GW installation.



4.2.1. Gateway Installation via PVT

ESRS is installed using the PVT Tool (Provisioning Tool)

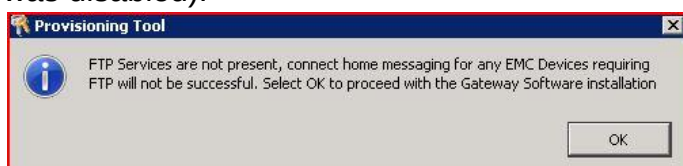
1. From *installdrive:\EMC\ESRS\Pvt*, launch the Provisioning Tool and proceed with the install. NOTE: Due to MS UAC, the Provisioning Tool MUST be run as Administrator. (Right click on the Provisioning Tool executable and select “**Run as administrator**”).



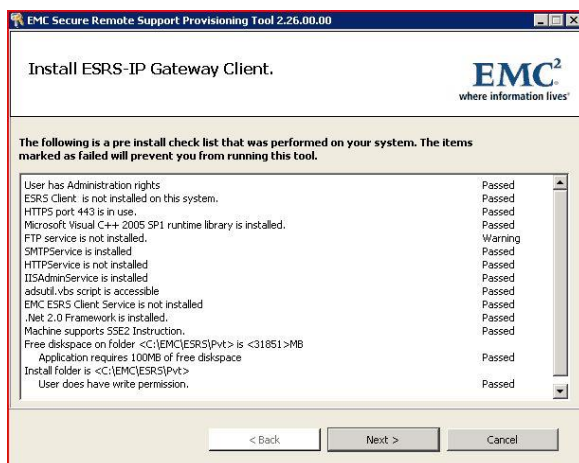
2. To begin the installation, click Next



3. FTP is not allowed from Citi. Click OK (Same as prior ESRS installation, FTP was disabled).



4. Pre installation checklist. Review and click Next



5. Fill in Proxy information.

Proxy: Yes

Proxy Type: HTTP

IP/DNS: webproxy.wlb2.nam.nsroot.net or whatever proxy you use in production

Port Number: 8080

The screenshot shows the 'Customer Proxy Configuration' window of the EMC Secure Remote Support Provisioning Tool. The window title is 'EMC Secure Remote Support Provisioning Tool 2.26.00.00'. The EMC logo is in the top right corner. The main text says: 'If you are not using a proxy server configuration, please click Next to continue.' Below this, there are radio buttons for 'Do you want to use a proxy server to connect to EMC?'. The 'Yes' option is selected. Under 'Select a proxy server type', the 'HTTP' radio button is selected. The 'Enter proxy server parameters' section contains two text boxes: 'IP Address / DNS Name' with the value 'webproxy.wlb2.nam.nsroot.net' and 'Port Number' with the value '8080'. There is a checkbox for 'Proxy server authentication required?' which is unchecked. Below this are text boxes for 'Username' and 'Password'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

6. Enter EMC SecurID credentials (*EMC CE completes this information*)

The screenshot shows the 'Login Credentials to Permit Software Download' window of the EMC Secure Remote Support Provisioning Tool. The window title is 'EMC Secure Remote Support Provisioning Tool 2.26.00.00'. The EMC logo is in the top right corner. The main text says: 'Enter your EMC SecurID username and passcode (pin + token code).' Below this are two text boxes: 'Username' and 'Passcode'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

7. Enter the Site ID where the Gateway will be installed and click Next

The screenshot shows the 'Verify CSI Party Number/Site-ID' window of the EMC Secure Remote Support Provisioning Tool. The window title is 'EMC Secure Remote Support Provisioning Tool 2.26.00.00'. The EMC logo is in the top right corner. The main text says: 'Enter the Customer Party Number/Site-ID for the physical location of the ESRS Client server.' Below this is a text box labeled 'Party Number/Site-ID'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

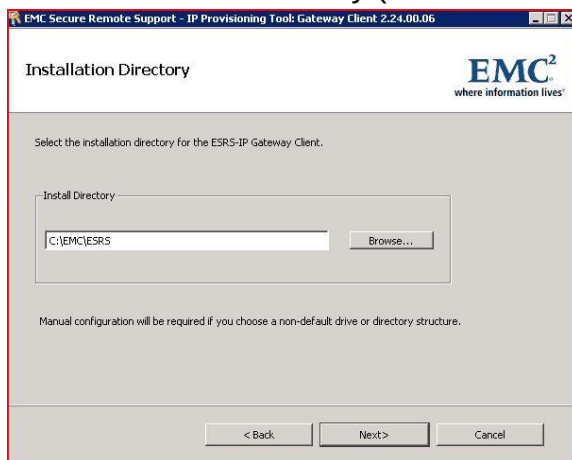
8. The Provisioning Tool contacts EMC Enterprise and verifies the site is eligible for the Gateway install and retrieves the serial number to be used by this Gateway (not displayed).

The screenshot shows the 'Validate Site Information' window of the EMC Secure Remote Support Provisioning Tool 2.26.00.00. The window has a title bar with the application name and version. Below the title bar is the EMC logo and the tagline 'where information lives'. The main content area contains instructions: 'Validate that the site information is correct. If correct, click Next. If the Party Number/Site-ID is incorrect, click "Back" and verify the Site-ID. If the returned customer information is incorrect, please contact EMC.' Below this is a section titled 'Customer Information' with several text input fields: 'Party Number/Site-ID' (containing '4109954'), 'Customer Name' (containing 'Citigroup - Warren'), 'Address' (containing '283 KING GEORGE RD BLDG A FL 3'), 'City' (containing 'WARREN'), 'State/Province' (containing 'NJ'), and 'Country' (containing 'US'). At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

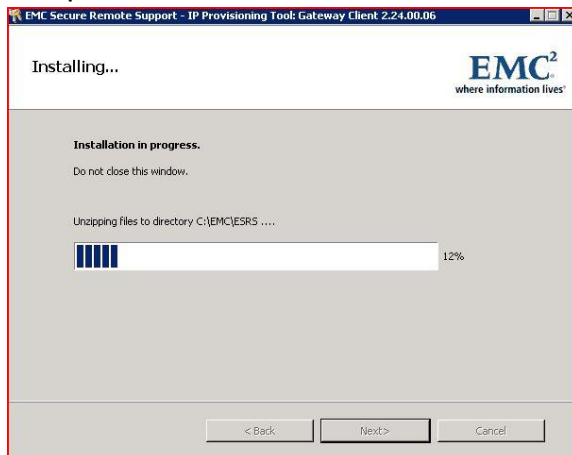
9. The Provision Tool runs a Pre Installation Check. Since this is fresh install, no previous version will be found. Click Next.

The screenshot shows the 'PreInstallation Check' window of the EMC Secure Remote Support - IP Provisioning Tool: Gateway Client 2.24.00.06. The window has a title bar with the application name and version. Below the title bar is the EMC logo and the tagline 'where information lives'. The main content area contains a text box with the following text: 'ESRSClient PreInstallation Check Summary' followed by a line of dots and 'No Previous ESRSClient Installation Found.' At the bottom of the window are three buttons: '< Back', 'Next>', and 'Cancel'.

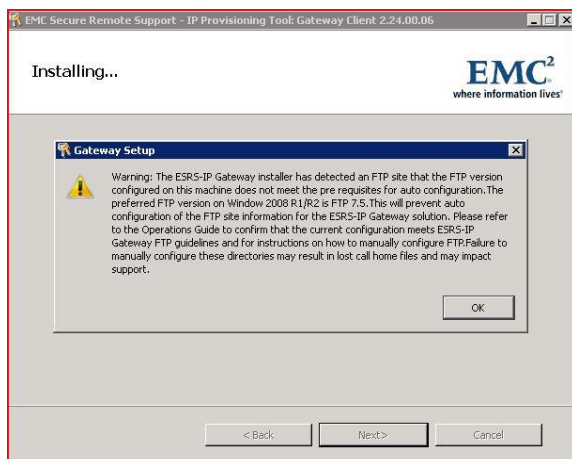
10. Select the install directory (Drive C:\ or D:\)



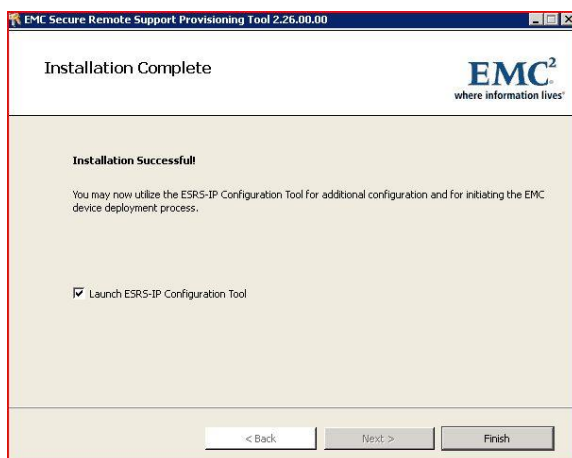
11. Unzips local bundle and installs the files in the designated directory.



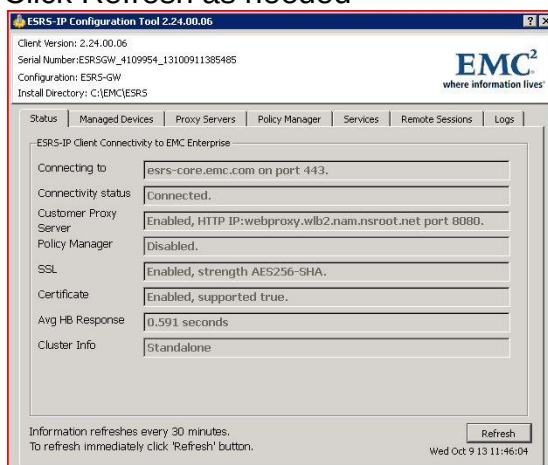
12. The installation warns that FTP is not detected. This is ok. Click OK.



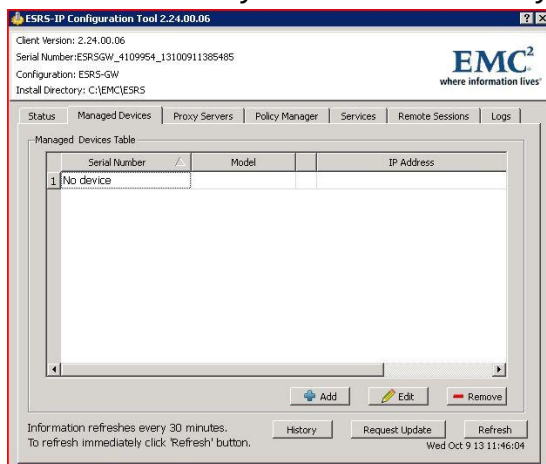
13. The installation completes. Check the box to “Launch the Configuration Tool”. Click Finish.



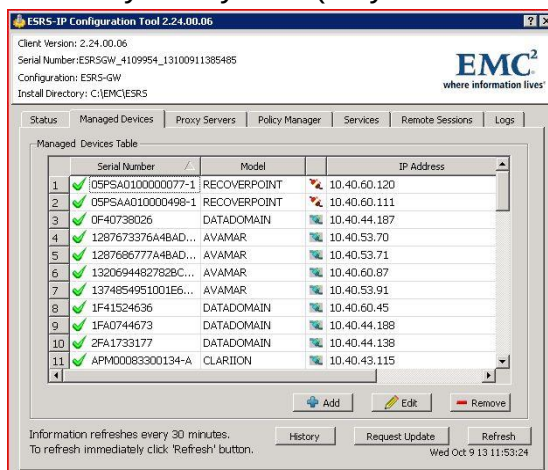
14. The Configuration Tool is launched. Verify that you have a connection to EMC Enterprise. Click Refresh as needed



15. Click on the “Managed Devices” tab. You will see “No device” until EMC adds this new Gateway to the cluster and syncs it with one of the old Gateways.



16. After they are synced (may take several minutes), all of the devices will show up.



17. Repeat this procedure for the second Gateway Server on Windows 2008

5. Configure ESRS for SMTP (Post ESRS install)

When ESRS was initially deployed at Citi, there was a particular Citi business that would not allow an SMTP service to listen on port 25, unless it was a Citi Mail Server. That business unit is no longer part of Citi. That allows us to add port 25 to our ESRS IIS SMTP configuration.

The significance of this is that several products couldn't be modified to send to SMTP 3325, so they had to be sent to a Citi Mail server port 25. There have been some instances of dropped messages and EMC wouldn't be aware of it. If there were dropped messages going through ESRS, EMC would be alerted.

Products that can be changed to point to the ESRS Gateway address for port 25:

- Clariion and Celerra
- New Symmetrix arrays will be configured to for ESRS on port 25
- New EDL arrays will be configured to for ESRS on port 25

Products requiring no change

- Existing Symmetrix arrays will continue to use ESRS on port 3325
- Existing EDL arrays will continue to use ESRS on port 3325
- Existing McData switch will continue to use ESRS on port 3325

Products that will continue to use the Citi Mail server

- Centera and Avamar send health check reports. They must continue to use Citi Mail server to allow distribution of the health check reports.
- Data Domain does not support call home via the ESRS GW
- Cisco switches (via DCNM)

Storage Device	Current CallHome Notification	Future CallHome Notification	Action Required
CLARiiON	Citi Mail Server port 25	ESRS GW port 25	Change devices to point to the ESRS GW Servers
Celerra/VNX	Citi Mail Server port 25	ESRS GW port 25	Change devices to point to the ESRS GW Servers
Cisco (via DCNM)	Citi Mail Server port 25	No change, continue with current configuration (Non-ESRS). For the DL's to get the daily reports, notifications have to be sent via Citi Mail Servers.	None
Centera	Citi Mail Server port 25. Device sends daily health reports via email to EMC and Citi Distribution Lists	No change, continue with current configuration (Non-ESRS). For the DL's to get the daily health reports, notifications have to be sent via Citi Mail Servers.	None
Avamar	Citi Mail Server port 25. Device sends daily health reports via email to EMC and Citi Distribution Lists	No change, continue with current configuration (Non-ESRS). For the DL's to get the daily health reports, notifications have to be sent via Citi Mail Servers.	None
Data Domain	CallHome not currently supported via ESRS	EMC is getting a target date for CallHome support via ESRS	TBD
Symmetrix	ESRS GW over port 3325	ESRS GW port 3325 and port 25	None. Existing arrays will continue to use ESRS GW's over port 3325. New arrays will be configured to use ESRS GW over port 25
EDL	ESRS GW over port 3325	ESRS GW port 3325 and port 25	None. Existing arrays will continue to use ESRS GW's over port 3325. New arrays will be configured to use ESRS GW over port 25

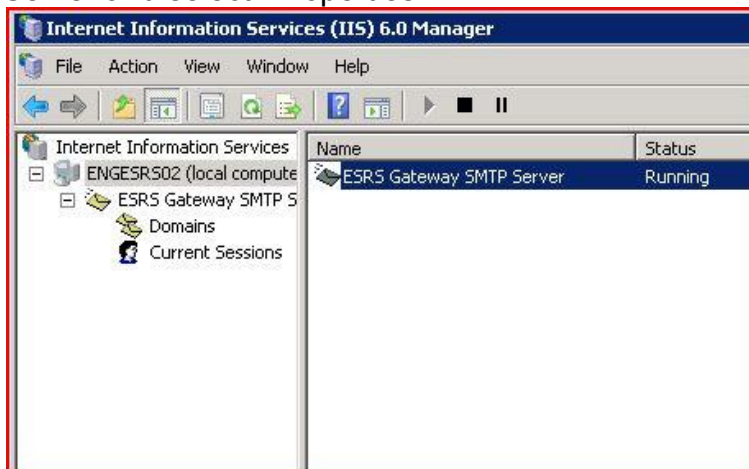
Note: See [Section 9](#) or the individual products Solution Guide for modifying storage products to use ESRS SMTP port 25

5.1. SMTP Configuration

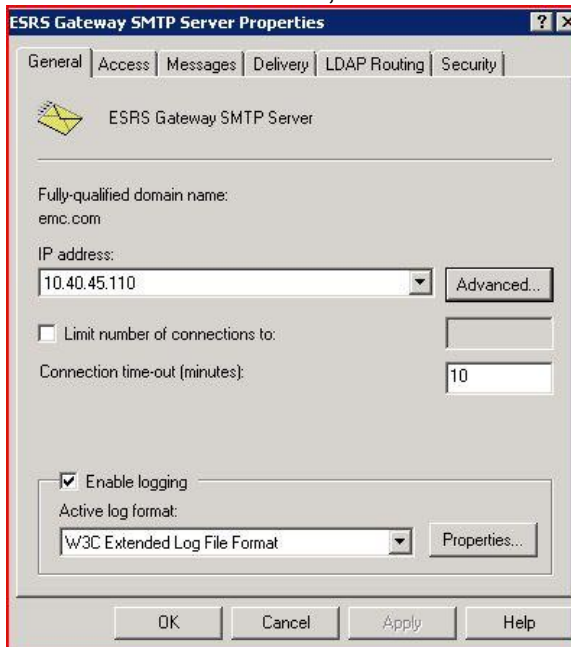
NOTE: The SMTP server can be configured to listen on the default port (25) for newly added storage devices and on port (3325) for older storage devices previously configured to use that port.

Configure the SMTP server as follows:

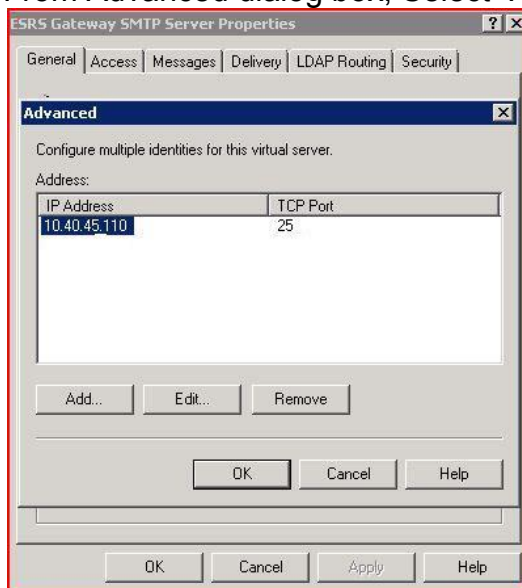
1. From the IIS 6.0 Management console, right click on the ESRS Gateway SMTP Server and select “Properties”



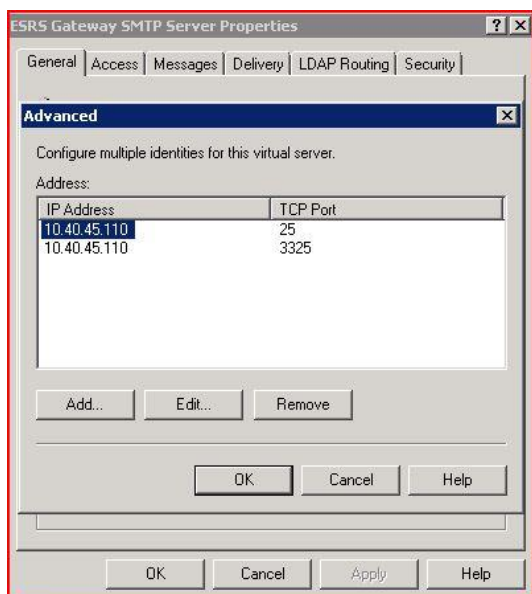
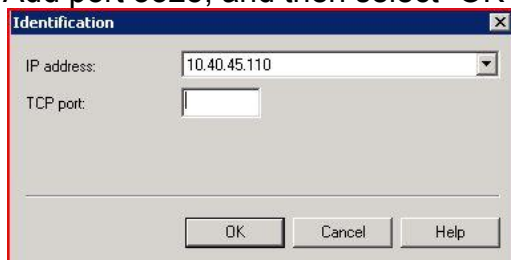
2. From the “General” tab, select “Advanced”.



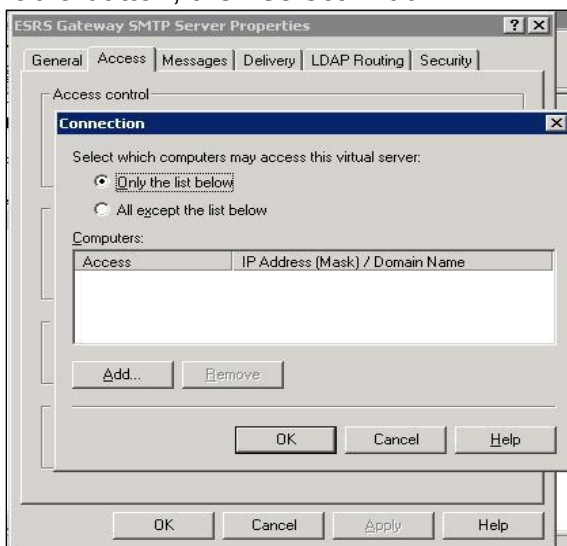
From Advanced dialog box, Select “Add”.



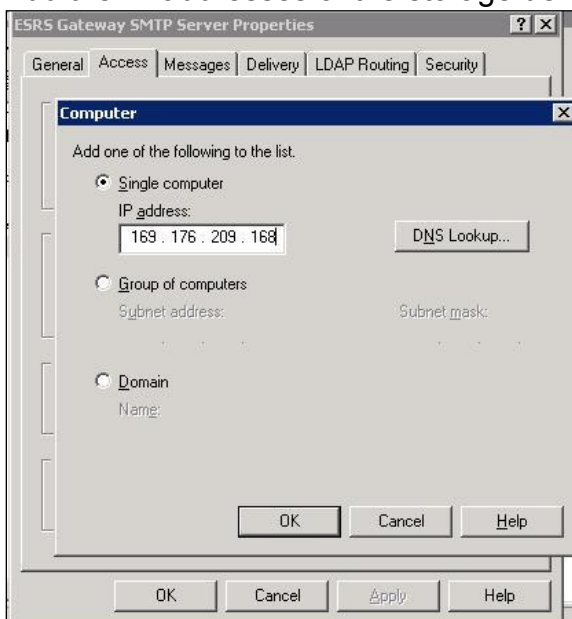
3. Add port 3325, and then select “OK”.



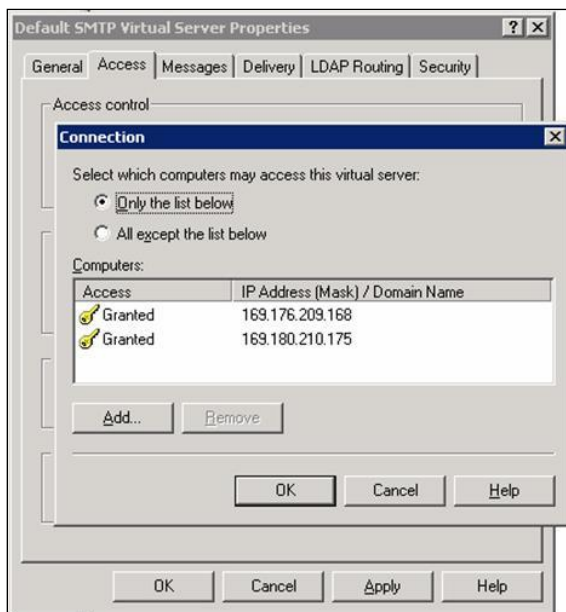
4. Select the “Access” tab and select “Connection”, select the “Only the list below” radio button, then select “Add”.



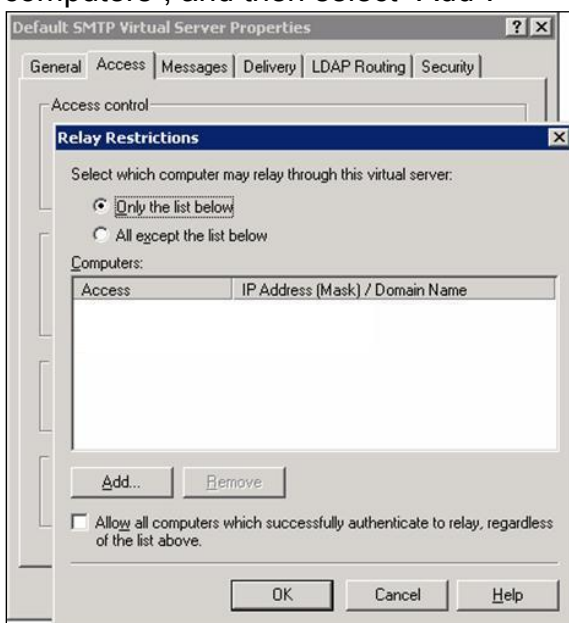
Add the IP addresses of the storage devices and select “OK”



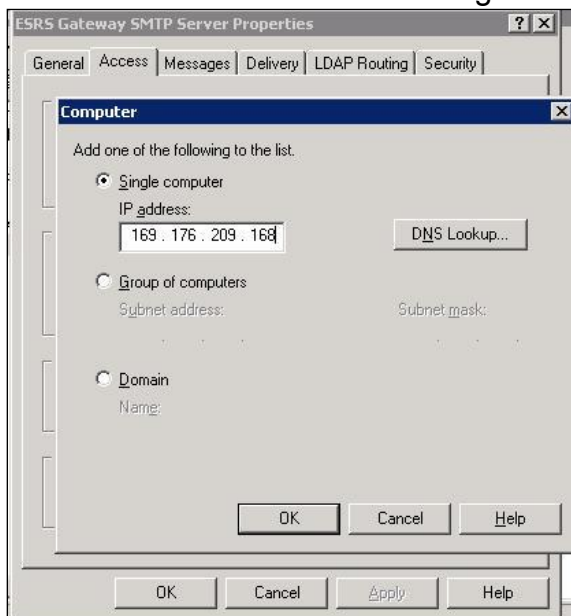
Select “OK”



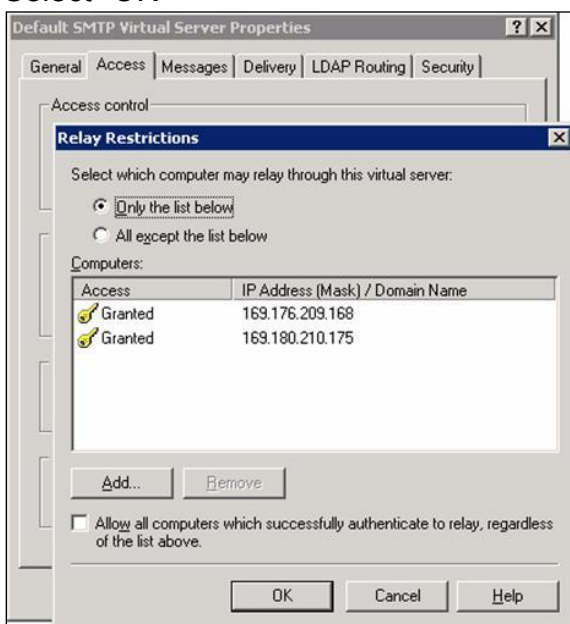
5. Select “Relay”, select “Only the list below” radio button, deselect “Allow all computers”, and then select “Add”.



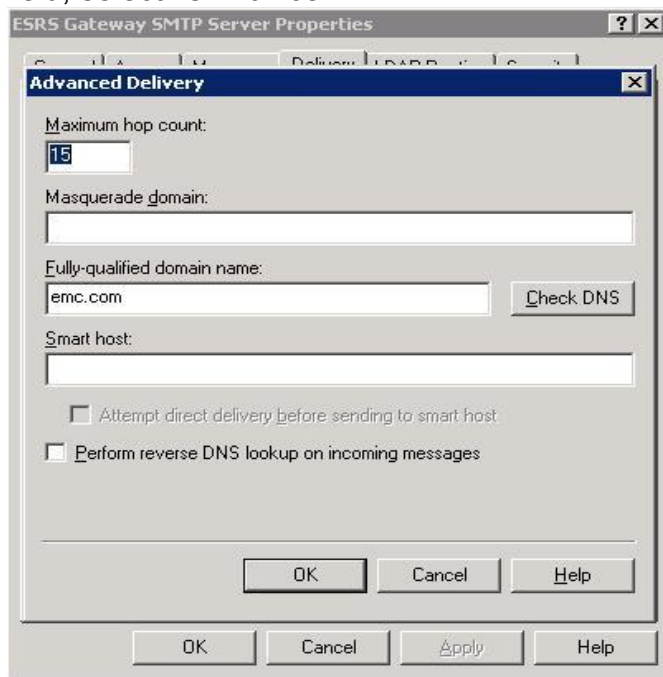
Add the IP addresses of the storage devices and select “OK”



Select “OK”



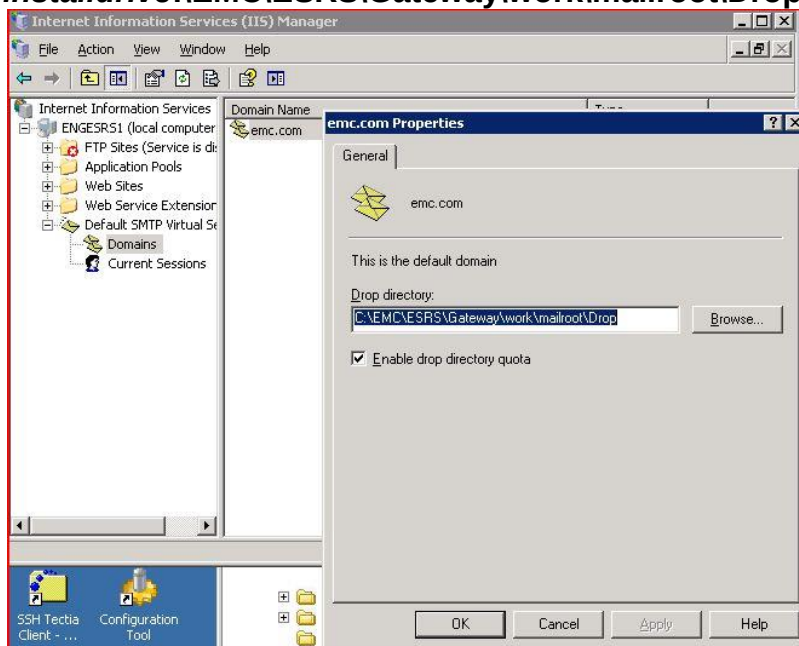
6. Select the “Delivery” tab and select “Advanced”, enter “emc.com” in the FDQN field, select “OK” twice.



7. From the IIS 6.0 Management Console, select “Domains” under the “ESRS Gateway SMTP Server”. Right click on the domain name “emc.com”. Click Properties.

Change the “Drop directory” to the following location:

installdrive:\EMC\ESRS\Gateway\work\mailroot\Drop



6. Post ESRS Migration Installation Steps

This section is used when migrating from ESRS on Windows 2003 to ESRS on Windows 2008

1. On all Symm products, EMC CE needs to modify ConnectEMC to point to the new ESRS Gateway server IP addresses.
2. Once satisfied with the new ESRS Gateways, the old ESRS Gateways on Windows 2003 can be uninstalled. **BUT**, before de-installing and powering off the Old Gateways, an EMC CE will have to set the Old Gateways offline (at EMC). **This step is critical**, if the gateways are not taken offline, a Missing Gateway service request will be created at EMC.
3. After EMC has taken the old ESRS Gateways on Windows 2003 offline, **ESRS should be uninstalled using the PVT Tool**.

7. Auditing

ESRS doesn't have any Audit Logs to monitor. The ESRS Gateway server is a "pass-through" to the EMC supported storage devices. All storage devices generate detailed audit logs of all logins and actions performed by EMC personnel. These logs are captured and stored within SEMS Arcsight Repository.

8. High Availability Gateway Cluster Configuration

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

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

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

If a Gateway Client server fails, the other Gateway Client server in the cluster already has full responsibility.

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

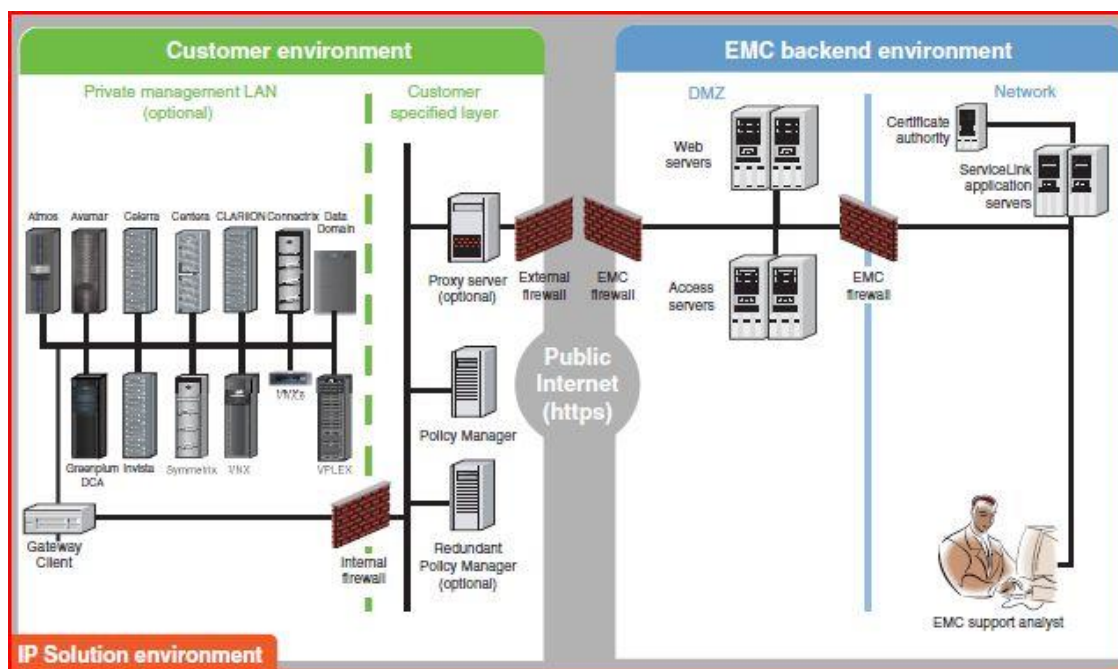
8.1. Gateway Cluster Synchronization

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

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

To implement a High Availability Gateway Cluster configuration, your EMC Global Services professional will create the cluster relationship from within the EMC Enterprise. When a cluster is created, a cluster name must be assigned. The default name is the organization name followed by the words “HA Gateways.” Other names can be assigned, but no two clusters can have the same name.

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



8.2. Single or HA Gateway SAN Device Limits

The Gateway Client of ESRS has the following device limits to help ensure reliable performance.

The recommended device limit for each Gateway Client or Clustered High Availability Gateway Client is **250 devices**.

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

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

9. Configuration Tool

The **ESRS Configuration Tool** is used to manage ESRS Client (Gateway) 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 various ESRS Client statuses, including connectivity status, Policy Manager enablement, and cluster status
- View the managed devices for an ESRS Client
- Create device deployment, change, and removal requests
- Configure a proxy server
- View the status of ESRS IP services and connect home services
- View active remote support sessions
- View logs of ESRS IP Client activities

9.1. View Connectivity Status

To view connectivity status, click the **Status** tab in the Configuration Tool. The Status tab displays connectivity information between the ESRS IP Client and EMC.

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

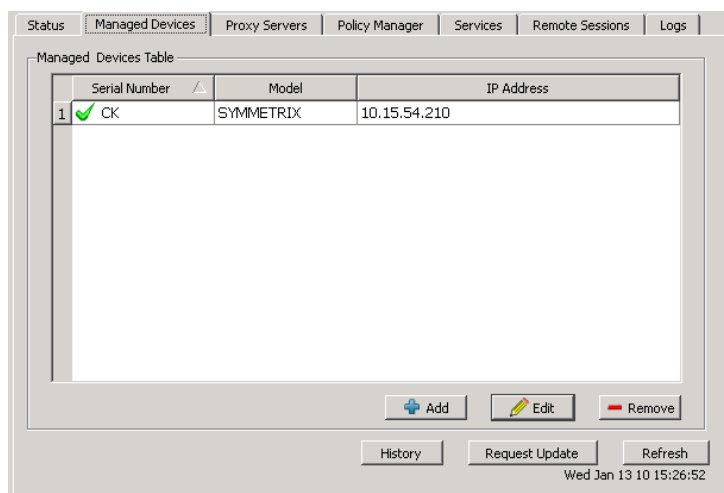
Information must be manually refreshed.

Refresh

Wed Jan 13 10 15:26:52

9.2. Manage 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.



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.

9.2.1. Add, Edit, or Remove Devices from ESRS

To add a managed device:

1. Click **Add**. The Add New Device window displays.

ESRS-IP CT Add New Device

Please enter device information

Serial Number: -A

Model Type:

IP Address:

Ok Cancel

2. Enter the following device information and click **OK**.
 - Serial Number
 - Suffix, if applicable (the options displayed in the drop-down list are dependent on the selected model type)
 - Model Type (select a model type from the drop-down list)

- IP Address
3. 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.

4. To send the Add New Device request to EMC, click **Request Update**.
5. 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** tab.

6. 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.

To edit the IP address of a managed device:

1. Select the device from the **Managed Devices** tab.
2. Click **Edit**. The Edit Device window displays.



3. Edit the displayed address and click **OK**.
4. 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.

5. When prompted, click **OK** to set the device edit. A pencil icon appears next to the device you have edited.
6. 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.
7. 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**.

8. 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.

To unmanage a managed device:

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

Submitting Managed Devices requests for approval:

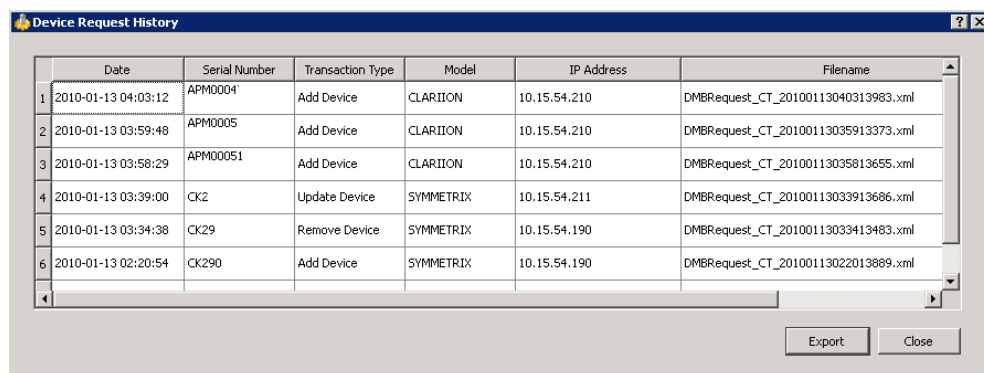
When you have completed all your manage, edit, or unmanage requests, click **Request Update**. Your change requests will be displayed for verification. Click **OK** to submit your requests to EMC for implementation.

When an authorized EMC Global Services professional has approved your requests via the EMC enterprise, the requested updates will be processed by the ESRS Gateway. 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 screenshot shows a window titled "Device Request History" with a table containing the following data:

	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 03:59:46	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

At the bottom right of the window are "Export" and "Close" buttons.

9.3. Proxy Servers

ESRS Clients can be configured to communicate directly through an HTTPS or SOCKS proxy. Set Proxy to: **webproxy.wlb2.nam.nsroot.net**

The screenshot shows the 'Proxy Servers' tab in the EMC Configuration Tool. The 'Proxy Server' section is active, showing the following settings:

- ☒ Enable proxy between Client and EMC Enterprise
- Proxy Type: HTTP Proxy (selected from a dropdown)
- IP Address/Host: webproxy.ssmb.com
- Port: 8080
- ☐ Authenticate using the following information:
 - Username: (empty text box)
 - Password: (empty text box)

An 'Apply Settings' button is located at the bottom right of the configuration area.

9.4. Status of IP Services

To display the status of services related to ESRS IP and connect homes, select the **Service** tab in the Configuration Tool. 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.

At Citi, the FTP will be stopped and disabled.

The screenshot shows the 'Services' tab in the EMC Configuration Tool. It displays the status of various services, categorized into 'Connect Home Services' and 'ESRS-IP Dependent Service Status'.

Service Name	Current State	Startup Type
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.

Refresh button

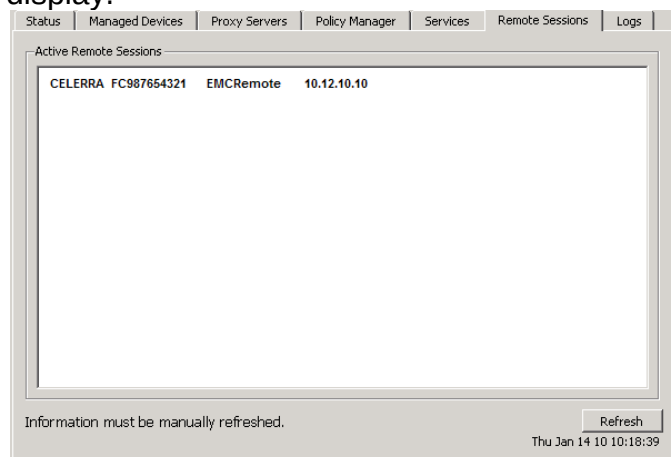
Wed Jan 13 10 15:26:53

9.5. Active Remote Sessions

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

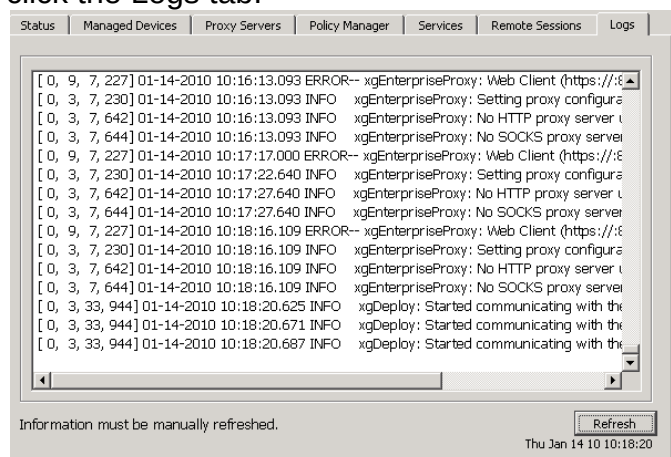
- Product type
- Serial number
- Remote Application name
- IP address

Note: To refresh the data, click **Refresh**. It is not refreshed automatically. The information you see is read-only. You cannot terminate active sessions from this display.



9.6. Configuration Tool Logs

To display the xGate log that shows activity performed within the Configuration Tool, click the **Logs** tab.



10. Device Deployment

Storage device verification and deployment is a joint effort between Citi Storage Personnel and EMC. Devices are added to ESRS via the **Configuration Tool** covered in the previous section. The following sections give you idea of what is required for devices to be added via the Configuration Tool.

By default, ESRS GW mail server listens on port 25. Originally, ESRS was configured to listen on port 3325 only. If your data center ESRS GW is configured to listen on port 3325, you can add port 25 to the configuration (described in a previous section). Leave the devices alone that are currently sending to ports 3325. Any new devices can be configured to send to ESRS GW on the standard port (25).

Prior to configuring devices, verify what SMTP port(s) the ESRS GW is listening on.

10.1. Symm / DMX / V-MAX

10.1.1. Prerequisites

- Open required CEP firewall ports (See [Appendix F](#))
- ESRS Gateway is installed
- ConnectEMC 2.12.02 or later (**SMTP 25**)
- ConnectEMC 4.0.2 or later (**HTTPS** support on V-MAX)

NOTE: CSBE recommends that V-MAX be configured to use SMTP until HTTPS is supported on other platforms.

- Storage Service Processor (SP) must have a routable IP address within the CEP
- Storage Service Processor must be on EMC supported list
- Enginuity support – see [Appendix G: Supported Storage Devices](#)
- ESRS Gateway IP addresses

10.1.2. Installation

- **EMC** will initiate a SP Utility program that will certify the SP configuration
- **EMC** will run the “SymmESRSsetup.exe” program
 - Checks configuration
 - Prompts for IP address, Subnet mask, Gateway IP and ESRS Gateway IP
 - Prompts for Call Home configuration (**select SMTP only**)
 - Set SP PrivateWire firewall rules for ESRS Gateway
 - Configure DialEMC for ESRS Gateway IP addresses (**SMTP 25**).
- **EMC** will need to verify that the PrivateWire firewall is configured correctly to allow ESRS Gateway traffic to and from the SP.

- **EMC** will manually deploy the Storage array on the Gateway Server, using the Deployment Utility (installed during ESRS installation)
- **EMC** will configure and test Call Home via the ESRS High Availability Gateway (Primary and Secondary)

10.2. Connectrix Manager Server Non-SOE (CSP)

10.2.1. Prerequisites

- Open required CEP firewall ports (See [Appendix F](#))
- ESRS Gateway is installed
- Must have a routable IP address within the CEP
- EMCRemote 4.02 or later
- ConnectEMC 2.12.02 or later (**SMTP 3325**)
- Connectrix 1U Server
- Connectrix Manager 9.1.1 or later

10.2.2. Installation

- **EMC** will configure ConnectEMC to add two new Email connections (port 3325) for each High Availability Gateway (Primary and Secondary Gateway). **EMC** will need to manually configure ConnectEMC to use **SMTP 3325**. ConnectEMC uses *ConnectEMC_config.xml* file located in
- **EMC** will manually deploy the switch environment on the Gateway Server, using the Deployment Utility (installed during ESRS installation)
- **EMC** will configure Connectrix Manager to email alert notifications

10.3. Connectrix Manager Server on SOE (CSP)

10.3.1. Prerequisites

- ESRS Gateway is installed
- EMCRemote 4.02 or later
- ConnectEMC 2.12.02 or later (**SMTP 3325**)
- Connectrix Manager 8.7.1 or later

10.3.2. Installation

- The **Citi SA and EMC** will need to manually configure ConnectEMC to use **SMTP 3325**. ConnectEMC uses *ConnectEMC_config.xml* file located in
- **EMC** will manually deploy the switch environment on the Gateway Server, using the Deployment Utility (installed during ESRS installation)

- **Storage Operations** will configure Connectrix Manager to email alert notifications

10.4. Clariion

10.4.1. Prerequisites

- Open required CEP firewall ports (See [Appendix F](#))
- Must have a routable IP address within the CEP
- ESRS Gateway is installed
- Note: EMC recommends ClarAlert to be installed on the Navisphere Management station. In CSBE testing, the ClarAlert install, removed the certified version of Navi Agent and installed a newer version, un-certified by CSBE. Due to this issue, the email home setup will be completed on the array.
- Configure CallHome on the array to send to the ESRS GW (Primary and secondary) on port 25 (default).

10.4.2. Installation

- **EMC** will manually deploy the Clariion array on the Gateway Server, using the Deployment Utility (installed during ESRS installation)
- **EMC** will configure the Clariion Array mail home to send email alerts to the Primary and Secondary ESRS Gateway IP addresses on port 25 (default).

10.5. VNX

- Configure VNX the same way Clariion's are configured.

10.6. Centera

10.6.1. Prerequisites

- Open required CEP firewall ports (See [Appendix F](#))
- CentraStar 2.4 and later
- Site ID and Centera Cluster Serial Number (obtained from Centera Viewer CLI command: *show config service*)
- IP address of one (or more) of the Centera access nodes (obtained from Centera Viewer CLI command: *show ip list*)
- The Centera must be fully configured and properly emailing Health Reports and Alerts (to a **Citi SMTP mail** server)
- Unlock the Centera Nodes (nodes will remain unlocked after installation and remote access)

10.6.2. Installation

- **EMC** will manually deploy the Centera on the Gateway Server, using the Deployment Utility (installed during ESRS installation)

10.7. Cisco MDS Switch (EMC supplied only)

10.7.1. Prerequisites

- Cisco switches reside on the GRN network. No CEP. No firewall ports to configure.
- Routable IP addresses of Cisco MDS switches
- ESRS Gateway is installed
- Cisco switches configured to send mail to emcsupport@emc.com via ESRS GW Server. Configuration is accomplished via Cisco DCNM Performance Manager web portal.

10.7.2. Installation

- **EMC** will manually deploy the Cisco switches on the Gateway Server, using the Deployment Utility (installed during ESRS installation)

10.8. EDL (EMC Disk Library)

10.8.1. Prerequisites

- EDL Engines reside on the GRN network. No CEP. No firewall ports to configure.
- Routable IP addresses of EDL Engines
- ESRS Gateway is installed
- EDL Management Console 3.1 installed on a Citi SOE server (see the *EDL Solutions Guide* for instructions)
- Tectia software (**SFTP**) installed and configured on EDL Management Console (see the *EDL Solutions Guide* for instructions)
- **EMC SFTP ID and Password** on the EDL Management Console for SFTP from the EDL Engines to the EDL Management Console

10.8.2. Installation

- **EMC** will manually deploy the EDL array on the Gateway Server, using the Deployment Utility (installed during ESRS installation)
- **EMC and an SA** will install and configure ConnectEMC (2.12.04 or later) on the EDL Management Console
 - Add two new Email connections for each High Availability Gateway (Primary and Secondary Gateway). Use the default **SMTP port 25**.

- **SA** will give **EMC SFTP ID** rights to the entire ConnectEMC folder on the EDL Management Console server
 - Rights: Modify, Read & Execute, List Folder Contents, Read, and Write
- **EMC** will install a patch on the EDL Engines (**Update-dl154913**), enabling SFTP

Note: Update-dl154913 must be installed prior to SP04. If the DL is running 3.1 SP05 or higher, the DL must be rolled back to SP04
- **EMC** will enable error forwarding on the EDL Engines. EDL Engines will **SFTP** the alerts to the “ConnectEMC/Poll” directory on the EDL Management Console. ConnectEMC will monitor this directory and forward any alerts to the ESRS Gateway. EMC will need:
 - IP address of the SFTP Server (EDL Management Console server)
 - EMC SFTP ID and Password to connect to SFTP server
 - Use port 22 (SFTP – Secure FTP)

10.9. Data Domain

10.9.1. Prerequisites

- Data Domain resides on the GRN network. No CEP. No firewall ports to configure.
- Routable IP address
- ESRS Gateway is installed
- Celerra Control Station configured to send mail to emcsupport@emc.com via **Citi SMTP mail** server (default “Citi Call-Home to EMC” configuration)

10.9.2. Installation

- **EMC** will manually deploy the EMC Celerra NAS array on the Gateway Server, using the Deployment Utility (installed during ESRS installation)
- **EMC** will install and configure ConnectEMC (2.0 or later) on the Celerra Control Station
 - Configure the Celerra mail home to send email alerts to a Primary and Secondary **Citi SMTP** server IP addresses (**SMTP port 25**)

10.10. EMC Celerra NAS

10.10.1. Prerequisites

- Celerra NAS resides on the GRN network. No CEP. No firewall ports to configure.
- Routable IP address
- ESRS Gateway is installed

- Celerra Control Station configured to send mail to emcsupport@emc.com via **ESRS Gateway's SMTP mail** server (default "Citi Call-Home to EMC" configuration)

10.10.2. Installation

- **EMC** will manually deploy the EMC Celerra NAS array on the Gateway Server, using the Deployment Utility (installed during ESRS installation)
- **EMC** will install and configure ConnectEMC (2.0 or later) on the Celerra Control Station
 - Configure the Celerra mail home to send email alerts to a Primary and Secondary ESRS Gateway server IP addresses (**SMTP port 25**)

11. Appendix A: References and Related Documents

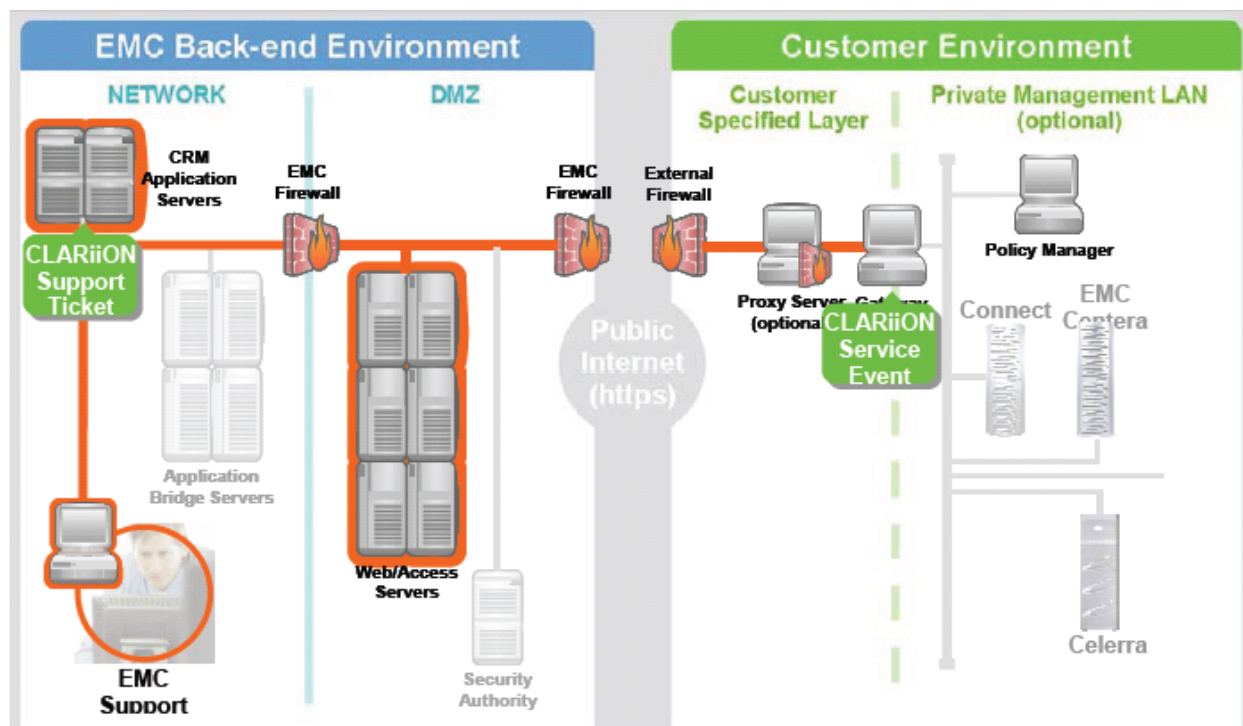
Document	Location
EMC Secure Remote Support – Release Notes	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/services/ESRS/07006-rn.pdf
Connectrix Manager 9.1.1 Release Notes	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/McDataFC/07022-rn.pdf
McData Switch Solutions Guide	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/McDataFC/04046-sg.pdf
CSBE Symmetrix website	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/symmetrix.aspx
CSBE Cisco MDS Switch website	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/ciscomds.aspx
CSBE Centera website	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/centera.aspx
CSBE Celerra website	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/celerra.aspx
CSBE Clariion website	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/clariion.aspx
CSBE EDL website	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/emcdisklib.aspx
CATE Storage and Backup Engineering Website	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/default.aspx
eTrust Audit Storage Monitoring - Solution Guide	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/services/eTrustAudit/08001-sg.pdf
C3PAR Website	http://www.citigroup.net/informationsecurityservices/tpaswg/index.htm

12. Appendix B: EMC Alert Notification (How it works)

Diagnostic information related to events on EMC storage devices is sent back to the EMC Customer Support Center. You can choose not to allow remote access to a particular device while still benefiting from the Gateway solution's secure encrypted email file transfer back to EMC.

EMC Customer Service will configure EMC storage devices as stated in the [Configuration Tool](#) section. When an exception event occurs, the data is sent to EMC Customer Service for review via the devices configured transport method (Email). For those devices that support ConnectEMC, their alerts will be sent to EMC via the ESRS Gateway SMTP server. For those that won't be using ConnectEMC (Centera, Cisco and Clariion), their alerts will be sent to a Citi SMTP server. ConnectEMC configuration files on your target devices are updated to route event files to your Gateway server. The Gateway server is configured to monitor specific directories for filename signatures that match a specific mask. By default the polling cycle is 30 seconds.

When the Gateway server receives a file from a device, the Gateway agent compresses and encrypts the file and issues an SSL request (via a Citi Proxy Server) to the EMC enterprise servers, carrying the data file as a payload. The request is digitally authenticated and forwarded to the EMC enterprise servers for processing. All Gateway-to-EMC communication is digitally authenticated.

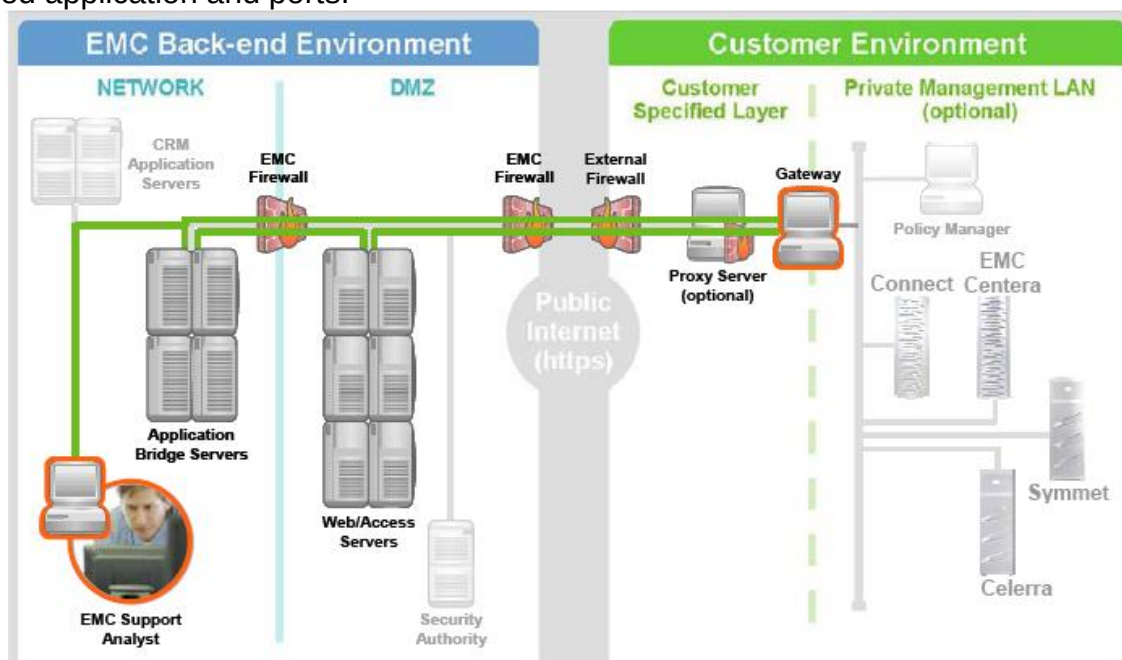


13. Appendix C: EMC Remote Access (How it works)

Remote access may occur in response to a notification message from an EMC storage device, in the event that an error occurs on that system. If the device that reports the error is a Gateway-managed device, an EMC Customer Service professional submits a request to conduct a remote access session to the target device. In the remote access session request, the EMC Customer Service professional specifies both the serial number of the target device and the remote application he/she wants to run on that device. A unique session identification number is assigned to the request, which is stored in the EMC enterprise database.

Every 30 seconds the Gateway agent posts a polling message containing status information about all managed EMC devices, primarily to identify which systems it is able to contact at that time. An EMC enterprise application first authenticates the Gateway certificate and then checks the system for any pending work items. When the enterprise application finds a remote access session request, it sends this request to the Gateway agent. The agent reads the request and attempts to initiate a session for the given target IP address and port back to the enterprise server system. At the same time, the EMC enterprise system initiates a parallel process that establishes a secure connection and waits for the connection request from the agent.

Again, the EMC enterprise system authenticates the agent's digital certificate and the session ID with source and target addresses is validated for those addresses. Then the connection is established and the remote access application can be invoked. With this remote access system, the secure remote access connection is actually established on the DRM servers and not on the Gateway server. The remote access session is restricted to EMC Customer Service professionals, who are able to perform actions only on the target device and only using the pre-defined application and ports.



14. Appendix D: Use of Proxy Server

The EMC Secure Remote Support Gateway solution supports the use of a proxy server for routing outbound Internet traffic from the Gateway servers to EMC. During the installation of the Gateway software, the EMC Customer Engineer configures the Gateway to route all outbound Internet traffic to the proxy server. The proxy server will then direct the Gateway transactions through the external firewall. All communication between our EMC storage devices and EMC is initiated by the Gateway server at the Citi site over SSL via our Citi Proxy server.

15. Appendix E: Architecture Approvals

This architected infrastructure for EMC Secure Remote Support has received approvals from:

- Global Distributed Storage Engineering
- Global Network Engineering (Remote Access)
- Proxy Server Infrastructure (Network Perimeter Solutions)
- 3PASWG (3rd Party Access Support Working Group)/C3PAR
 The C3PAR Business Users (Storage Operations) are responsible for managing relationship information in the C3PAR application.
- CATE BISO and North America BISO

16. Appendix F: CEP Firewall Port Requirements

If any of these devices reside on the GRN network (Corporate Network), the firewall rules are not necessary. They would reside on the same Citi corporate network as the Gateway Server.

16.1. Symmetrix / DMX / V-MAX

Source IP	Destination IP	Protocol	Port	Traffic Description
Gateway Server	Symm / DMX / V-MAX	TCP	5414	EMCRemote
		TCP	9519	Remotely Anywhere
		TCP	1300, 1400, 4444, 5555, 23003, 23004 and 23005	SGBD – Symm GNU Debug – Advanced troubleshooting by EMC Symm Engineering
		TCP	7000	Remote File and Log Browser –

Symm / DMX / V-MAX	Gateway Server	TCP	3325 or 25 depending on ESRS config	Troubleshooting SMTP – Connect Home
--------------------	----------------	-----	-------------------------------------	--

16.2. Connectrix Manager Server (SOE - Citi Server)

Connectrix Manager Server running on a Citi SOE server will reside on the GRN network and won't require any ports to be opened in the CEP firewall.

16.3. Connectrix Manager Server (non SOE – EMC Server)

Source IP	Destination IP	Protocol	Port	Traffic Description
Gateway Server	Connectrix SP	TCP	5414	EMCRemote
Connectrix SP	Gateway Server	TCP	3325 or 25 depending on ESRS config	SMTP – Connect Home

16.4. Clariion/VNX

Source IP	Destination IP	Protocol	Port	Traffic Description
Gateway Server	Clariion SP	TCP	60020	Remote Diagnostic Agent
		TCP	13456	Ktcons – Troubleshooting
		TCP	80, 443, 2162, 2163	Navisphere Mgr/Navisphere SecureCLI
Clariion SP	ESRS Gateway Server	TCP	25	SMTP – Connect Home

16.5. EDL Engine (EMC Disk Library)

EDL Engines reside on the GRN network and don't require any ports to be opened in the CEP firewall.

Source IP	Destination IP	Protocol	Port	Traffic Description
N/A	N/A			

16.6. Centera

Source IP	Destination IP	Protocol	Port	Traffic Description
Gateway Server	Centera	TCP	3218, 3682	Centera Viewer
		TCP	22	CLI via SSH

Centera	Citi SMTP servers	TCP	25	SMTP – Connect Home
---------	-------------------	-----	----	---------------------

16.7. Cisco MDS Switches (EMC Supplied)

Cisco switches reside on the GRN network and don't require any ports to be opened in the CEP firewall.

Source IP	Destination IP	Protocol	Port	Traffic Description
N/A	N/A			

16.8. Celerra NAS

Celerra devices reside on the GRN network and don't require any ports to be opened in the CEP firewall.

Source IP	Destination IP	Protocol	Port	Traffic Description
N/A	N/A			

17. Appendix G: Supported Storage Devices

17.1. Avamar

Model	Environment
Avamar	6.0 or later

17.2. Symmetrix / DMX / V-Max

Model	Environment
Symmetrix® 8000 Series	Enginuity 5567 and 5568 with Service Processor Part Numbers: 090-000-064, 090-000-074, and 090-000-09x
Symmetrix DMX™ Series	Enginuity 5670, 5671
Symmetrix DMX-3 Series	Enginuity 5771, 5772, 5773
Symmetrix DMX-4 Series	Enginuity 5772, 5773
Symmetrix V-MAX Series	Enginuity 5874

17.3. Connectrix Manager Server

Model	Environment
Connectrix® Connectrix Manager	8.7.1 and later

17.4. Clariion

Model	Environment
CLARiiON® Navisphere® Manager	6.19 and later
Flare	2.19 and later
AX-100/AX-150	Not supported as they do not support ClarAlert

17.5. EDL Engine (EMC Disk Library)

Model	Environment
DL-4000 series DL-700 series DL-310	See the EDL Solutions Guide for specific models supported by Citi.

17.6. Centera

Model	Environment
Centera™	CentraStar® 2.4 and later

17.7. Cisco MDS Switches

Model	Environment
Cisco Switch	NX-OS 4.1(1b) or later Requires Fabric Mgr or DCNM

17.8. Celerra NAS

Model	Environment
Celerra	NAS Code 5.4 or later

17.9. VNX

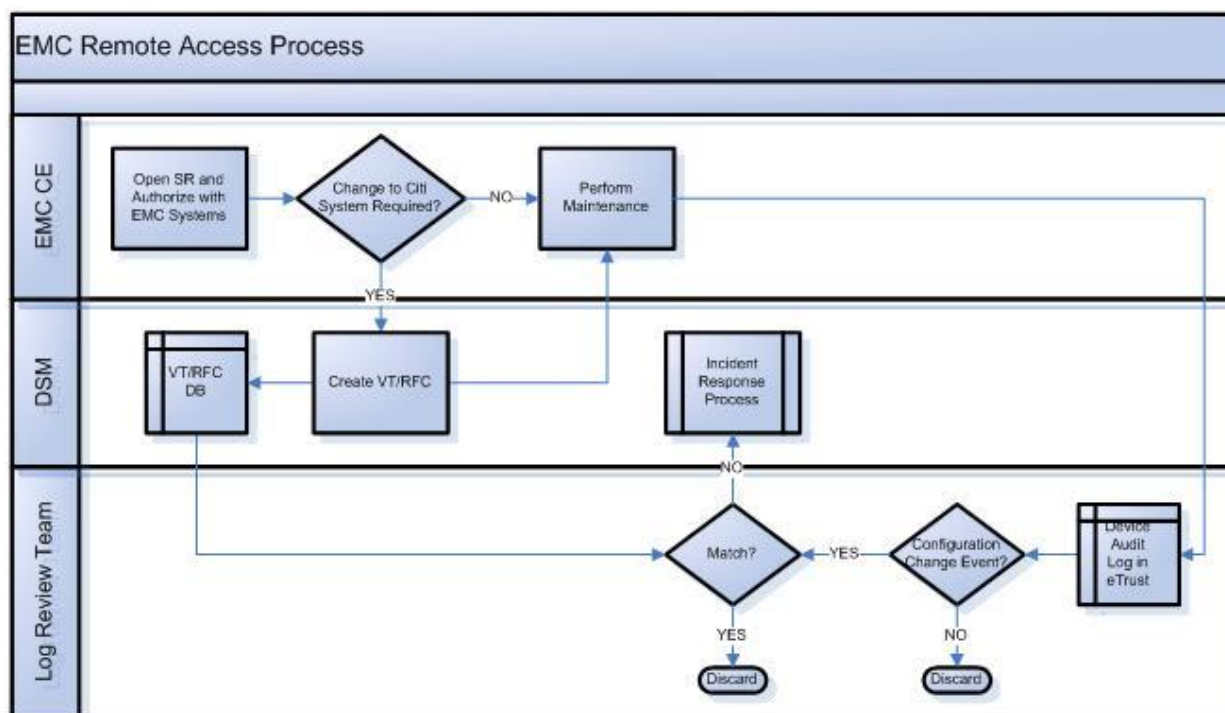
Model	Environment
VNX	VNX OE for Block 05.31.000.5.006 or greater VNX OE for File 7.0.12.0 or greater

17.10. Data Domain

Model	Environment
Data Domain	DD OS version 4.8 or higher

18. Appendix I: EMC Remote Access Procedure

EMC provides break fix support for EMC storage devices within Citi. A combination of onsite and offsite EMC personnel delivers this service. Storage devices send alerts to EMC support center and EMC logs in remotely in response to identify and fix the issue. EMC also logs in without a matching alert periodically for preventative maintenance. EMC Secure Remote Gateway Server (ESRS) is the technology that sends alerts to EMC and permits EMC to log on to Citi storage devices. ESRS always initiates connections from inside the Citi network guaranteeing that only specific EMC support personnel are able to log in to Citi devices. EMC also has an elaborate process and technology to control access to Citi devices. EMC gets access to the maintenance interface of the device; they do not have any access to Citi business data stored on the device. All storage devices generate detailed audit logs of all actions performed by EMC personnel. These logs are captured and forward to SEMS ArcSight for auditing purposes.



1. EMC Customer Engineer (CE) will authorize access to Citi devices from EMC Service Request (SR) process
2. CE will determine if servicing the device would require changes to be made on the device
3. If changes are to be made CE will call on-call Distributed Storage Management (DSM) person and ask him/her to open a virtual ticket (VT) or Request for Change (RFC) determined by the nature of the change. If it is off-hours, CE can proceed with the maintenance and contact DSM for VT/RFC next business day. DSM person will note the actual date and time the maintenance was performed in the VT/RFC record so that the event can be reconciled by the Log Review Team
4. If CE does not require making a change but only monitor status or generate diagnostic reports, there is no need to involve DSM to open VT/RFC

The following table outlines which storage devices allow EMC support to make changes:

Storage Device	Changes Allowed (R/W)	Changes Not Allowed (Read Only)
Symmetrix / DMX	Y	
CLARiiON	Y	
Centera	Y	
EMC Disk Library	Y	
Celerra	Y	

Cisco Switches		Y
Connectrix Manager		Y

5. The Log Review Team will scan the audit log for the device on which maintenance was performed periodically. This log is stored in the SEMS ArcSight audit repository. The team will filter out monitoring/diagnostic report type of activity by using a criteria provided by CATE Storage and Backup Engineering. The remaining events will be reconciled against VT/RFC repositories by matching the date and time. Instead of matching individual commands, the team will match all commands issued by EMC within one hour of the noted date and time in the VT/RFC record
6. Any unmatched items will be flagged to DSM management per an Incident Response Process PCM which will be developed by DSM. This process would involve working with EMC to identify the source of unauthorized access

19. Appendix J: Disabling EMC Remote Access to Celerra and EDL

CSBE has determined that EMC is able to SSH from a Celerra or EDL device. This is a risk (“Leapfrogging”). If they are able to SSH to another device, they might gain access to Internal Citi information. CSBE is providing a procedure to disable EMC remote access to these devices. This procedure will remain in place until EMC enhances these products with the ability to be configured to block outbound connections.

CSBE recommends that If EMC needs to access these devices; they will host a WebEx session, inviting Citi support personnel. Citi confidential or restricted data should NOT be shared with the vendor during the session.

Note: Alerts will continue as normal to EMC.

19.1. Disable Access to Celerra and EDL

Access to these devices will be disabled and remain disabled until EMC fixes the gap in their product.

1. From one of the Gateway servers, rename:

C:\EMC\Gateway\ESRS\Celerra to C:\EMC\Gateway\ESRS\Celerra_no_access
(Substitute EDL-Engine)
2. From the same Gateway server, stop the “EMC SRS Gateway” service. Stopping this service will also cause the “EMC Secure Remote Service Https Listener” service to stop. Click refresh to make sure it is also stopped. If the Https Listener does not stop, manually stop it.
3. From the same Gateway, restart the “EMC SRS Gateway” service. The “EMC Secure Remote Service Https Listener” service will automatically start. Click refresh until it is also started. If the Https Listener does not start, manually start it.
4. Repeat steps 1 – 3 on the second Gateway server

19.2. Disabling Newly Added Devices

If EMC adds a new Celerra or EDL, they will deploy the device in ESRS. With the device folders renamed to “xxxxx_no_access”, ESRS will add the device under a device folder (ie: Celerra). To disable these newly added devices, you’ll need to follow these steps.

1. From one of the Gateway servers, copy the newly added device folder to the "xxxxx_no_access" folder.

Example (a new Celerra was installed and deployed):

Copy C:\EMC\Gateway\ESRS\Celerra\APM0008339999-1 to
C:\EMC\Gateway\ESRS\Celerra_no_access

2. Delete C:\EMC\Gateway\ESRS\Celerra
3. From the same Gateway server, stop the "EMC SRS Gateway" service.
Stopping this service will also cause the "EMC Secure Remote Service Https Listener" service to stop. Click refresh to make sure it is also stopped. If the Https Listener does not stop, manually stop it.
4. From the same Gateway, restart the "EMC SRS Gateway" service. The "EMC Secure Remote Service Https Listener" service will automatically start. Click refresh until it is also started. If the Https Listener does not start, manually start it.
5. Repeat steps 1 – 4 on the second Gateway server

20. Appendix K: How EMC Handles Missing Devices

A “heartbeat” signal from the Gateway server to EMC's Device Relationship Manager (DRM) server occurs every 30 seconds. The heartbeat contains a small datagram identifying the Gateway server and provides status information on the health of the Gateway, IP connection, and EMC storage systems. When the DRM doesn't receive the information, it labels the device as “missing”.

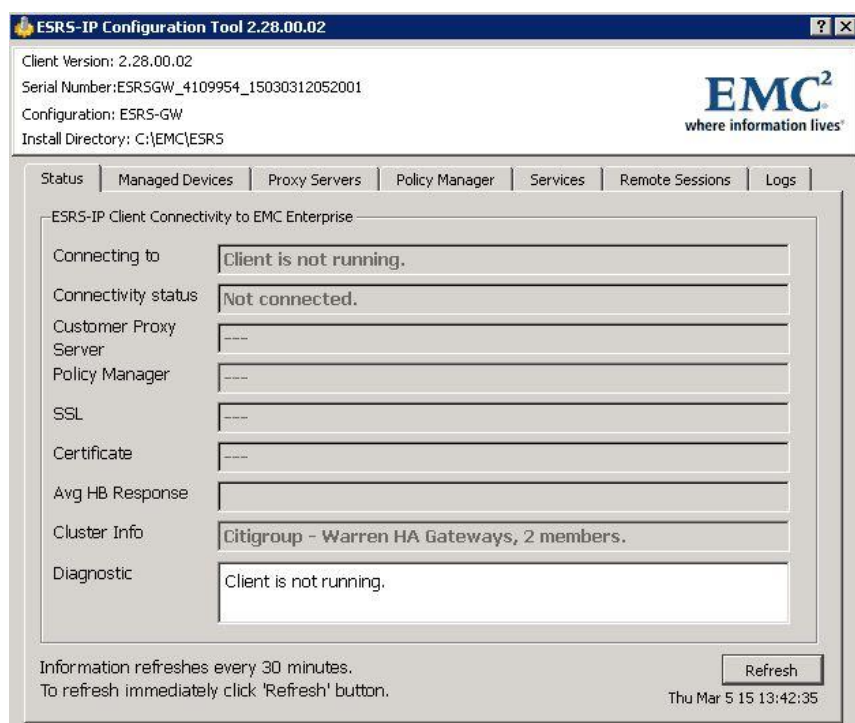
The following occurs at EMC when a storage device is found to be “missing”:

- The device is seen in EMC's Device Relationship Manager (DRM) server as missing
- A “service request/case” is generated as a severity 2 containing the pertinent information about the problem
- The DRM audit log is updated showing the case was created
- An alarm is generated in the DRM system
- An email is also generated and sent to the "service request/case support" email list.
- The case is researched and an EMC Customer Engineer is dispatched, if necessary.

21. Appendix L: Issues

21.1. Configuration Tool – Client Not Running

The Configuration Tool must be set to “Run as Administrator”. If this is not done, the Configuration Tool will display that the **Gateway Client is not running**.

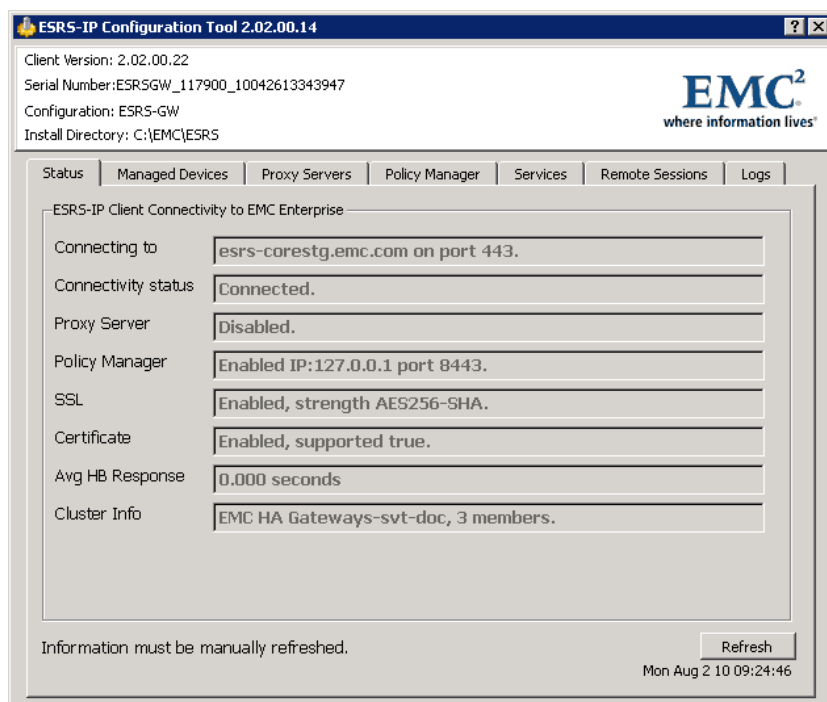


22. Appendix M: ESRS Patches

22.1. ESRS v2.28 Patch

Note: These instructions are for patching ESRS Gateway Client version 2.24.

- 1) From one of the GW Clients, verify current ESRS IP code version of by launching the Configuration Tool (CT).



- 2) On one of the ESRS Gateway servers, install the ESRS v2.28 package from TPM package **CITI_WIN_EMCSecureRemoteSupport_228_00**. The package will install the upgrade files into directory **C:\ESRS_v2.28_Upgrade**.
- 3) Stop the ESRS Services prior to applying the patch.



- 4) Open a command window (“run as administrator”) and change to the directory that the patch is located, **C:\ESRS_v2.28_Upgrade**.

```

Administrator: Command Prompt

C:\ESRS_v2.28_Upgrade>dir
Volume in drive C is SYSTEM
Volume Serial Number is F6AD-BCB9

Directory of C:\ESRS_v2.28_Upgrade

03/06/2015  11:03 AM    <DIR>          .
03/06/2015  11:03 AM    <DIR>          ..
06/24/2014  11:38 AM             2,121,728 GatewayUpgrade.exe
05/08/2014  10:43 AM             14,823,108 setup.zip
               2 File(s)          16,944,836 bytes
               2 Dir(s)          33,617,760,256 bytes free

C:\ESRS_v2.28_Upgrade>_

```

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.

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

```

Administrator: Command Prompt - GatewayUpgrade.exe setup.zip

C:\ESRS2.28>dir
Volume in drive C is SYSTEM
Volume Serial Number is 48FA-92DB

Directory of C:\ESRS2.28

11/10/2014  10:49 AM    <DIR>          .
11/10/2014  10:49 AM    <DIR>          ..
10/20/2014  02:54 PM             15,885,926 GatewayUpgrade-Win2008-2.28.00.02.exe
06/24/2014  11:38 AM             2,121,728 GatewayUpgrade.exe
05/08/2014  10:43 AM             14,823,108 setup.zip
11/10/2014  10:47 AM                234 upgrade-20141110-104732.log
11/10/2014  10:48 AM                234 upgrade-20141110-104804.log
11/10/2014  10:50 AM                482 upgrade-20141110-104936.log
               6 File(s)          32,831,712 bytes
               2 Dir(s)          30,388,547,584 bytes free

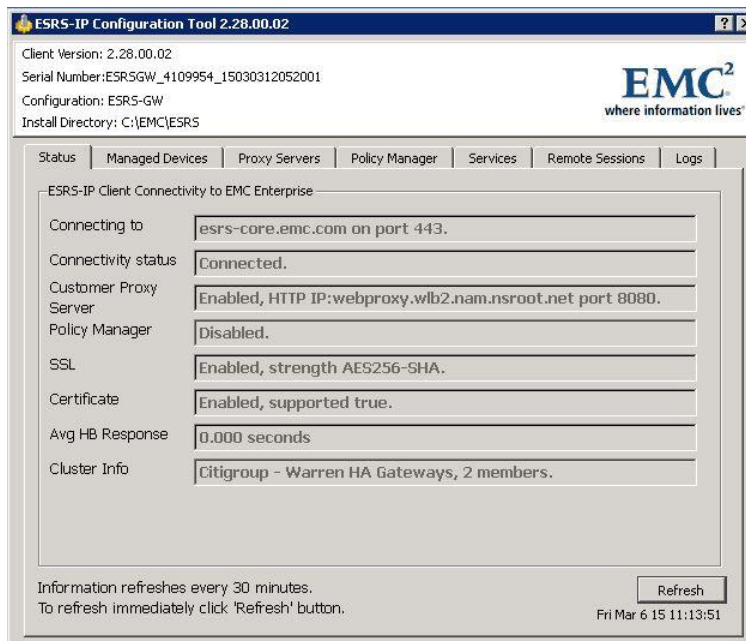
C:\ESRS2.28>GatewayUpgrade.exe setup.zip
*****
*          START OF ESRS-IP UPGRADE          *
*****
** This will upgrade your ESRS-IP gateway! **

Type Y to continue or N to quit.
_

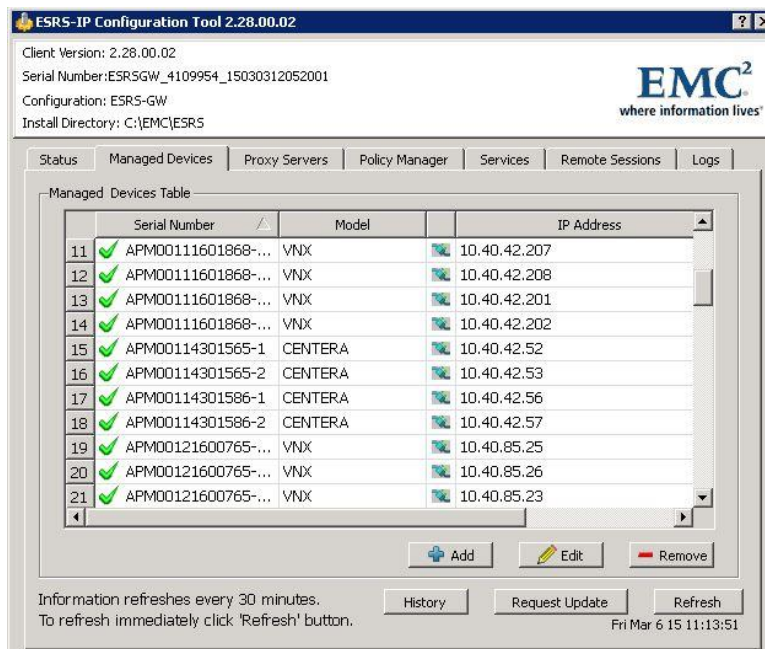
```

- 6) Answer “Y” and press Enter. The patch process will proceed in the command Window. These ESRS services will be restarted.
- 7) The Configuration Tool (CT) will automatically launch. After the CT launches, close the command window.

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

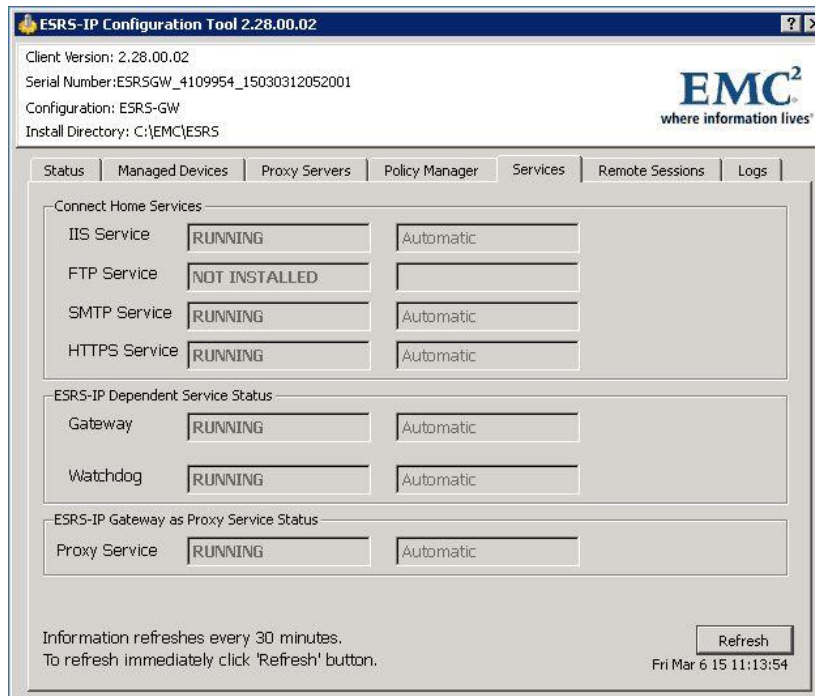


- 8) On the Managed Devices tab you will see your devices. Check connectivity. Refresh the screen if necessary.



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

10) On the Service tab verify services are as expected. Refresh the screen if necessary.



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

12) Repeat process on the other ESR IP GW Client.

23. Appendix N: Revision History

1.0 - Date: 30-Jul-07

- Initial release of EMC Secure Remote Support. Included Connectrix Manager on SOE, Clariion and Centera support

1.1 - Date: 15-Oct-07

- Modified the device group policy settings for Connectrix Manager and Centera in Section 9.2.2

1.2 - Date: 9-Nov-07

Modified the SMTP configuration in Section 7.5.3

- Changed ESRS to use TCP port 3325 instead of port 25
- Added SMTP configuration steps to lockdown ESRS SMTP mail server to allow only specific SAN device IP addresses to communicate with it

1.3 - Date: 28-Feb-07

- Added Section 19 for patching ESRS Gateway with version 1.01.03/1.01.05 to provide support for EMC Cisco MDS Switches

1.4 - Date: 7-Mar-08

- Added section 7.4 VMware Support Statement
- Modified the Policy Manager installation, section 8.3, adding a workaround for the lack of a “Redundant Policy Manager Server”. Provided a backup and restore procedure

1.5 – Date: 18-Mar-08

- Modified section 8.3: Redundant Policy Manager changed to Secondary (Standby) Policy Manager. Added the use of a NAS CIFS drive to be shared between the Primary and Secondary Policy Manager.
- In each of the installation/configuration sections, added who is the responsible party for installation.
- Modified Section 17 CEP Ports, removed ping (echo-request) from all SAN devices

1.6 – Date: 26-Mar-08

- Added Section 7.4, detailing required ESRS Gateway directories and the Gateway Check Utility. Pre Gateway installation requirements
- Modified Section 7.6, added FTP directories required for installation of ESRS
- Modified Section 7.6, added information on creating Local Accounts on Gateway Server
- Added Appendix for ESRS SG release details (this section).
- Added Section 8.6 Post Installation steps. Removal of the Local Accounts, FTP and the FTP directories
- Modified the installation steps in Section 8.4.2. Added comments on how to correct a possible “file not found” condition.
- Added Policy Manager HA solution diagram in Section 8.3.
- Modified Section 9.1 – Policy Manager Configuration

The **APMAdmin** role does not work correctly. Users given this role are unable to manage the TomCat web server. Users that require admin of the TomCat web server should be given the **admin** role. EMC has been notified about this issue.

- The following entries were removed from the [Version Control](#) Table:

Version	Date	Author	Reviewed	Comments
0.1	10-May-2007	Kevin Hobaugh	GDSE	Peer Review
0.2	11-May-07	Kevin Hobaugh	SAN Stakeholders	Phase I RFC

1.7 / 1.8 – Date: 12-Dec-08

- Reorganized Section 8 for better clarity
- Added Section 8.6, Securing the Policy Manager. Configuration steps to lock down Policy Manager access from the SOE server where it is installed.
- Added Section 8.7, Deployment Utility Configuration
- Modified Section 9.1, user roles modified. Admin role used for “ID management” and APMUsers used for “Policy Management”
- Added 9.1.1, LDAPS Support
- Added Section 9.2.2.6, policy settings for EDL (EMC Disk Library)
- Modified Section 9.3, modified the body of text in the “Vendor Access Request Notification” email
- Added Section 11.7, prerequisites and deployment parameters for EDL
- Added Section 18.4, added EDL to the list of storage devices
- Added Section 19.3, instructions for installing ESRS patch 1.01.07
- Added Section 19.4, instructions for installing ESRS patch 1.01.09
- Modified links to point to new GDSE Sharepoint website

1.8 – Date: 09-Jan-09

- No changes since RFC, see previous revision notes (above) for changes

1.9 – Date: 16-Feb-09

- Added Section 9.8 – Functional ID for Policy Manager “Admin” account

1.91 – Date: 15-Apr-09 (Peer/RFC)

- Modified Section 6 – Changed strategy on the use of Policy Manager. Policy Manager no longer required (BISO approved). Included reasons and benefits.
- Removed Section 7.2 – Policy Manager Requirements

- Modified Section 8 – Removed requirement for Policy Manager installation. If already installed, the Policy Manager service should be disabled. Removed Policy Manager backup and restore process.
- Modified Section 8.2 – Deployment Utility Configuration. Uncheck the box for enabling Policy Manager
- Modified Section 9 – Policy Manager section renamed to Disable Policy Manager. Removed sections on Vendor Access Requests, Auditing ESRS logs, and Functional IDs.
- Added Section 21 – EMC Remote Access Procedure
- Added Section 23 - Issue with Gateway Service not staying active. Add ESRS programs to the DEP (Data Execution Prevention) exclusion list

1.92 – Date: 17-Apr-09 (RFC)

- Added Section 8 – High Level ESRS Installation Steps
- Modified Section 10 – Disable Policy Manager. Added steps to remove UserID's from Policy Manager

1.94 – Date: 16-Sep-09 (Peer/RFC)

- Modified Section 13.1 – V-MAX deployment
- Added Section 13.8 – Celerra deployment
- Modified Section 19.1 – V-MAX firewall ports
- Added Section 19.8 – Celerra firewall ports
- Modified Section 20.1 – V-MAX supported devices
- Added Section 20.7 – Celerra supported devices
- Added Section 21.3 Patch 1.02.00 installation instructions

1.95 – Date: 02-Oct-09 (Production)

- Modified Section 21 – Removed references to “out of date” patches 1.01.03/1.02.05.
- Modified Section 21 – Added table of ESRS upgrade paths
- Added Section 24.2 – Issue EMC204925 ESRS Gateway fails to send call-home alerts after installing ESRS 1.02.00 Patch.

1.96 – Date: 06-Aug-10 (Production)

- Inserted Section 23 Appendix J – Celerra and EDL Remote Access Procedure. Procedure will disable EMC remote access. When needed, Citi will re-enable access for the duration of the connection.

1.97 – Date: 30-Nov-12 (RFC)

- Removed references to Policy Manager, since it is no longer a requirement.
- Removed requirement for FTP to be installed for the duration of the installation
- Modified Section 2.4.2 – IIS SMTP Configuration. The IIS outbound TCP port is now used for notifications being sent to EMC. Notifications from ESRS are sent over the secure SSL connection over port 443. Step f has been marked out.

- Added Section 6: Install ESRS v2.14 on Windows 2008 R2
- Added Section 7: Configure ESRS to listen on SMTP port 25
- Added Section 8: ESRS Configuration Tool
- Modified Section 19: Removed references to out dated patches

2.1 – Date: 18-Dec-13 (RFC/RFP)

- Modified Sections 2-6: ESRS Prerequisites, Installation and Configuration.
- Removed Section H for patches

2.2 – Date: 09-Mar-15 (RFC) / 01-Apr-15 (RFP)

- Inserted Section 22 Appendix M: ESRS Patches (ESRS V2.28 Patch)
- Added Section 3.2 ESRS v2.28 Patch: Updated the ESRS installation process to include installing the v2.28 patch.