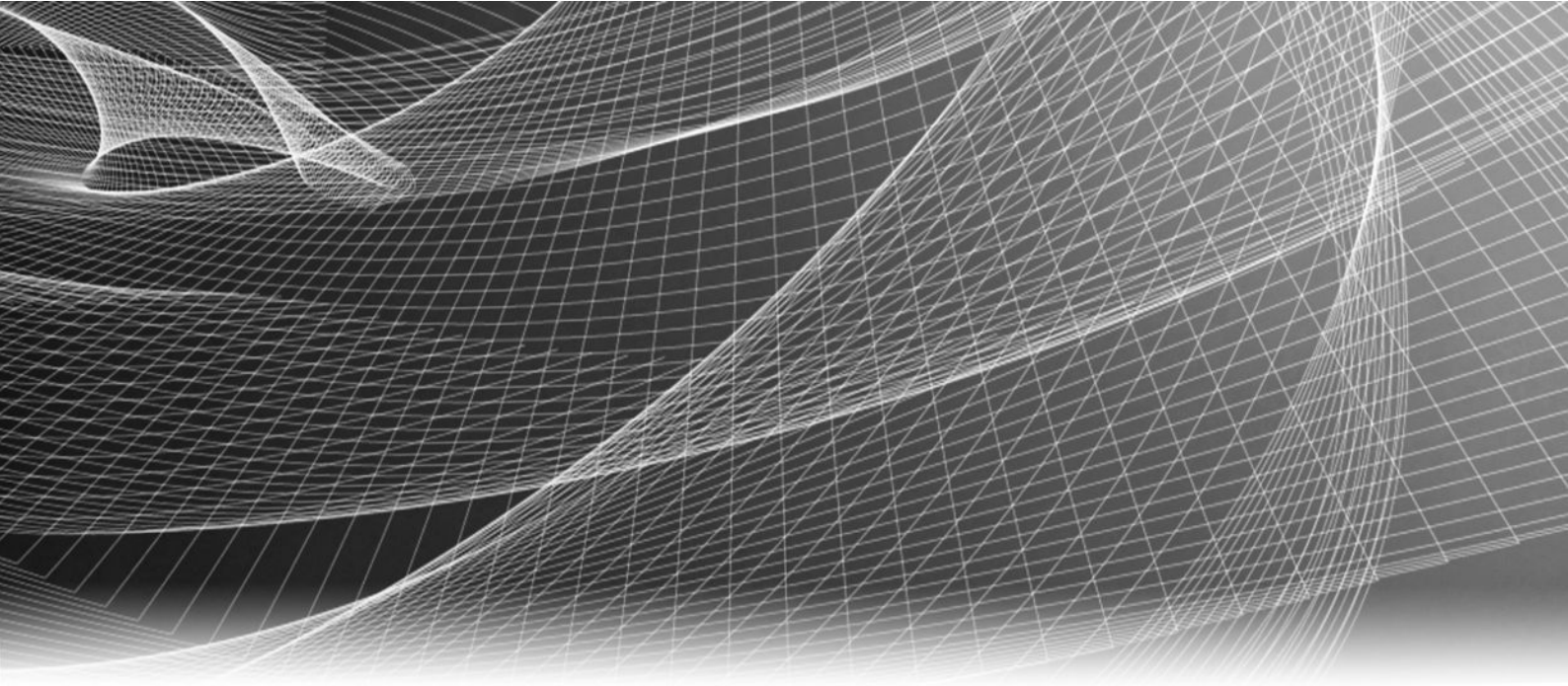


EMC® VNX® Series

Version VNX1, VNX2

EMC Secure Remote Support for VNX

300-014-340 REV 03

EMC²

Published July, 2014

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

FIGURES

CHAPTER 1

Introduction

This chapter introduces you to the EMC Secure Remote Support (ESRS) embedded device client on a control station and the ESRS embedded device client on a storage processor features, which are for single systems. It also introduces you to the ESRS IP Client for VNX and VNX gateway installations, which require a server in addition to the storage system and can be used for multiple systems.

Major topics include:

ESRS embedded device client on a control station overview

The ESRS embedded device client software is packaged into the VNX® operating environment (OE) for file/unified systems and resides on the control station. This feature provides your authorized EMC® service provider with remote access capabilities to your VNX file/unified system using a secure and encrypted tunnel. For outbound access, the VNX management IP network must allow outbound and inbound HTTPS traffic. The secure tunnel that ESRS establishes between the VNX device and authorized systems on the EMC network can also be used to transfer files out to the VNX system or transfer files back to EMC's network.

For more information concerning this feature, see ESRS device client on control station feature on page 11.

ESRS embedded device client on a storage processor overview

The ESRS embedded device client software is packaged into the VNX OE for block systems and resides on the storage processors. This feature provides your authorized EMC service provider with remote access capabilities to your VNX block system using a secure and encrypted tunnel. For outbound access, the VNX management IP network must allow outbound and inbound HTTPS traffic. The secure tunnel that ESRS establishes between the VNX device and authorized systems on the EMC network can also be used to transfer files out to the VNX system or transfer files back to EMC's network. For more information concerning this feature, see ESRS device client on storage processor feature on page 17.

ESRS IP Client for VNX overview

You install the ESRS IP Client for VNX software on an external monitor station (a host or virtual machine). This software monitors the operation of your EMC VNX or legacy CLARiiON® systems for error events and automatically notifies your service provider and provides a path to securely connect to your monitored VNX or legacy systems.

For more information concerning ESRS IP Client for VNX, see ESRS IP Client for VNX feature on page 23.

VNX gateway installations

An ESRS Gateway configuration supports a wide range of EMC products, and is appropriate for a customer environment with a heterogeneous mix of EMC products. Only trained EMC or EMC partner personnel should install and configure a VNX gateway system configuration. This includes the setup of remote connectivity to contact EMC Customer Service or a third-party service provider for problem resolution assistance.

Note

ESRS embedded device client on control station (included with OE for file version 7.1.56.x or later) and ESRS IP Gateway 2.0 or later (version 2.22 as a minimum is required for later model VNX gateway systems) is supported as a remote connectivity and callhome solution for a VG2/VG8 gateway configuration; ESRS Gateway 1.x is not supported.

For additional information on ESRS IP Gateway, go to the EMC Online Support website (Support.EMC.com)

CHAPTER 2

ESRS device client on control station feature

This chapter describes the requirements for the ESRS embedded device client on control station software and provides an operational description of the feature. The chapter also describes the processes to provision the feature and to re-provision the feature.

Major topics include:

ESRS embedded device client on control station requirements

The ESRS embedded device client on control station feature requires the following:

- VNX operating environment (OE) for VNX version 7.1.56.x or later.
- At least one DNS server must be configured on your VNX before you set up the ESRS communication channel and provision the feature; otherwise, the feature will not work.
- Unrestricted access to *.emc.com over the Internet using HTTPS (for non-proxy environments).
- EMC online support account.

Note

Provisioning or re-provisioning the ESRS device client on a control station in a VNX file/unified system requires an active account on the EMC Online Support website. This account associates specific credentials with a particular organization and email domain. When you provision or re-provision the ESRS device client on a control station in a VNX file/unified system, you must specify these credentials (a user name password pair) to set up the ESRS communication channel for the system.

The following requirements are dependent on your ESRS device client on a control station implementation:

- If your ESRS implementation will include a proxy server to connect to the Internet, you must indicate this when you provision the ESRS feature.
- If your ESRS implementation will include a Policy Manager for more control over remote access to your VNX system, you must indicate this when you provision the ESRS feature.
- If your ESRS implementation will include a proxy server for your VNX to connect to a Policy Manager, you must indicate this when you provision the ESRS feature.

ESRS embedded device client operational description

The ESRS embedded device client on control station feature provides an IP-based connection that enables EMC Support to receive error files and alerts from your VNX file/unified system, and to perform remote troubleshooting resulting in a fast and efficient time to resolution.

Note

EMC strongly recommends that you provision the ESRS device client on control station feature and select it as the primary transport mechanism for Connect Home notifications. These actions will help to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. If you do not provision ESRS, you may need to collect system information manually to assist EMC Support with troubleshooting and resolving problems with the VNX file/unified system.

The ESRS device client on control station feature offers a secure architecture from end to end, including the following features:

- EMC issues X.509 digital certificates to authenticate the ESRS device client on control station to EMC.

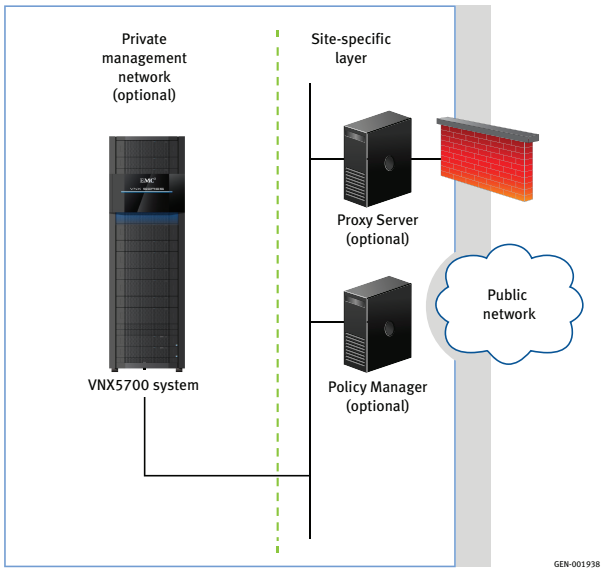
- EMC professionals are authenticated using two unique factors.
- All EMC service professionals have a unique username that is logged with all their actions.
- All communication originates from the control station. The ESRS device client on control station does not accept unsolicited connections from EMC or the Internet.
- All communications between EMC and the ESRS device client on control station includes the latest security practices and encryption technologies, including certificate libraries based on RSA Lockbox technology, and Advanced Encryption Standard (AES) 256-bit encryption.
- Those who implement the ESRS device client on control station solution can further control remote access by using the Policy Manager. The Policy Manager gives full control of how EMC interacts with VNX systems. SSL is available between the ESRS device client on control station and the Policy Manager.

ESRS device client on control station management

You can initially setup the ESRS device client on control station feature using the VNX Installation Assistant (VIA). When using VIA, it is important to have all information for setup at the time of installation/initialization. You can manage the ESRS device client on control station feature using Unisphere®. You can provision or re-provision the service, set up a proxy server or Policy Manager, or both. You must provide your support account credentials to provision or re-provision the ESRS device client on a control station.

The VNX file/unified system itself does not implement any policies. If you require more control over remote access to your VNX file/unified system, you can use a Policy Manager to set authorization permissions. The Policy Manager software component can be installed on a customer-supplied server (see ESRS device client feature customer-side network topology example on page 13). It controls remote access to your devices, maintains an audit log of remote connections, and supports file transfer operations. You can control by whom, what, and when access to your VNX file/unified system occurs. For additional information about the Policy Manager, go to the EMC Online Support website (Support.EMC.com). After logging in, locate the applicable Support by Product page and search for the link to the specific ESRS product technical documentation.

Figure 1 ESRS device client feature customer-side network topology example



ESRS device client on control station communication

Access to a DNS server is required for the ESRS device client on control station feature to work. You should set the ESRS device client on control station feature to be the primary (default) method used by ConnectEMC to communicate with EMC backend systems.

Provision ESRS embedded device client on control station

Note

As a prerequisite for you to provision the ESRS device client on control station feature in your VNX file/unified system, you must have an existing EMC Online Support account. Also, at least one DNS server must be configured on your VNX before you set up the ESRS communication channel and provision the feature; otherwise, the feature will not work.

You or your EMC service provider can provision the ESRS device client on the control station through either the VNX Initialization Assistant (VIA, for fresh installs) or Unisphere. To provision the feature requires either you to provide your EMC Online Support account credentials (username and password) or your EMC service provider to provide their SecurID credentials.

To provision the ESRS device client on control station feature in Unisphere, you must be logged in to the control station as User root and Scope Local. Select your system and from the task list, under **Service Tasks**, select **Manage ESRS for File**.

Note

For a VNX with two control stations, in Unisphere a dialog box for selecting the target control station (Primary or Standby) appears first. The Primary control station will be selected by default. If necessary, you can change the selection and click **Continue** to navigate to the Manage ESRS page for the corresponding control station. Also, as an alternate method to access the ESRS parameters, under **Service Tasks**, you can select **Manage Connect Home for File** and click **Manage ESRS Settings** in the **ESRS Priority** field. This link navigates directly to the Manage ESRS page for the primary Control Station. To manage the ESRS on a standby control station, you must select **Manage ESRS for File** from the task list under **Service Tasks**.

When provisioning the ESRS device client on the control station, you can provision an optional Proxy Server or a Policy Manager, or both. Once you have provisioned the feature, you should ensure that the primary transport mechanism for Connect Home notifications is set to **ESRS**. You can do this by selecting your system and from the task list, under **Service Tasks**, select **Manage Connect Home for File**. After you configure your Connect Home settings, you should test them using **Test** on the **Manage Connect Home** page.

For detailed instructions and more information about provisioning the ESRS device client on control station feature and testing the transport mechanisms for Connect Home notifications, see the Unisphere online help.

Proxy Server

If the VNX file/unified system will use a proxy server to connect to the Internet, you must indicate this when you configure the ESRS. You must provide the following information for the proxy server:

- Protocol (HTTPS or SOCKS)
- IP address
- Port number

If the proxy server requires authentication, you must also indicate this during the ESRS configuration and supply login credentials for the proxy server. You must supply both a username and password for authentication.

If you install a proxy server on a non-standard port, you will need to enter a port number to use the proxy server. If the port is not specified, the system defaults to the appropriate standard port for the given proxy type, port 3128 for the HTTP protocol or port 1080 for the SOCKS protocol.

Policy Manager

If the VNX file/unified system will use a Policy Manager to set authorization permissions, you must indicate this when you configure the ESRS. You must provide the following information for the Policy Manager:

- Indicate whether the connection to the Policy Manager needs to be secure (SSL will be used in the connection to the Policy Manager); otherwise, SSH is used in the connection to the Policy Manager.
- IP address
- Port number

If the Policy Manager will use a proxy server to connect to the VNX file/unified system, you must indicate this when you configure the ESRS. You must provide the following information for the Policy Manager's proxy server:

- Protocol (HTTPS or SOCKS)
- IP address
- Port number

If the Policy Manager's proxy server requires authentication, you must also indicate this during the ESRS configuration and supply login credentials for the proxy server. You must supply both a username and password for authentication.

While you configure the policy manager, you have the option to change the default port if you choose to use a non-secure transport. In this case, you will need to enter a port number for the policy manager proxy server. If you do not specify the port, then a default proxy server port is used. The system defaults to the appropriate standard port for the given protocol, port 3128 for the HTTP protocol or port 1080 for the SOCKS protocol. The default ports for the Policy Manager are 8443 for secure communication or 8090 if not secure.

Add storage processor to RemotelyAnywhere IP address filter tables

When you provision ESRS embedded device client on CS you must also add the internal storage processor (SP) IP addresses to the RemotelyAnywhere filter tables on the SPs.

Procedure

1. Enter the SP A or SP B IP address or hostname in a supported browser address field and append the setup page path to the IP address or hostname, for example, `http://IP address/setup` or `http://hostname/setup`.

   The SP setup login page opens.
2. Enter the system Unisphere administrator access username and password.

   The SP setup page opens.
3. Scroll down to **Set RemotelyAnywhere Access Restriction** and click the name panel to open the page.

Note

System security must be enabled and configured before you can access the **Set RemotelyAnywhere Access Restriction IP** address filter table.

The **IP Filter Configuration for RemotelyAnywhere** page opens.

4. Enter the control station IP addresses in the following list to the filters that apply to the connected storage system input table.
   - Primary control station CS0:
     - 128.221.252.100 (eth0)
     - 128.221.253.100 (eth1)
   - Secondary control station CS1 (if applicable):
     - 128.221.252.101 (eth0)
     - 128.221.253.101 (eth1)
5. Click **Apply Settings**.

Note

The following text message should appear:

```
RemotelyAnywhere IP Filter request was successful.
```

The **RemotelyAnywhere IP Filter Configuration - Apply** page opens.

6. Click **Back**.

   The main setup page appears.
7. Click the **Logout** and close the browser.

Re-provision ESRS embedded device client on the control station

You may need to re-provision the ESRS device client on the control station feature for any of the following reasons:

- To add or remove a Proxy Server or change existing Proxy Server settings
- To add or remove a Policy Manager or associated Proxy Server or change existing Policy Manager settings, including settings for an associated Proxy Server

Note

As a prerequisite for you to re-provision the ESRS embedded device client on the control station in your VNX file/unified system, you must have already provisioned the ESRS feature. Also, to re-provision the ESRS device client on control station feature in Unisphere, you must be logged in to the control station as User root and Scope Local. See Provision ESRS embedded device client on control station on page 14 for information.

Upgrade ESRS embedded device client on control station

The ESRS embedded device client on control station feature is packaged into the VNX file/unified software image. Upgrade of the device client or associated features will only be delivered as part of a full VNX file/unified system software upgrade.

CHAPTER 3

ESRS device client on storage processor feature

This chapter describes the requirements for the ESRS embedded device client on storage processor software and provides an operational description of the feature. The chapter also describes the processes to provision the feature and to re-provision the feature.

Major topics include:

ESRS embedded device client on storage processor requirements

The ESRS embedded device client on storage processor feature requires the following:

- VNX operating environment (OE) for block versions 5.32 that are later than version 5.32.000.5.209 and block versions 5.33 that are later than 5.33.000.5.051.
- At least one DNS server must be configured on your VNX before you set up the ESRS communication channel and provision the feature; otherwise, the feature will not work.
- Unrestricted access to *.emc.com over the Internet using HTTPS (for non-proxy environments).
- EMC online support account

Note

Provisioning or re-provisioning the ESRS device client on a storage processor in a VNX block system requires an active account on the EMC Online Support website. This account associates specific credentials with a particular organization and email domain. When you provision or re-provision the ESRS device client on a storage processor in a VNX block system, you must specify these credentials (a user name password pair) to set up the ESRS communication channel for the system.

The following requirements are dependent on your ESRS device client on a storage processor implementation:

- If your ESRS implementation will include a proxy server to connect to the Internet, you must indicate this when you provision the ESRS feature.
- If your ESRS implementation will include a Policy Manager for more control over remote access to your VNX system, you can indicate this when you either provision or re-provision the ESRS feature.
- If your ESRS implementation will include a proxy server for your VNX to connect to a Policy Manager, you can indicate this when you either provision or re-provision the ESRS feature.

ESRS embedded device client on storage processor operational description

The ESRS embedded device client on storage processor feature provides an IP-based connection that enables EMC Support to receive error files and alerts from your VNX block system, and to perform remote troubleshooting resulting in a fast and efficient time to resolution.

NOTICE

After successfully initializing your system, EMC strongly recommends that you provision the ESRS device client on storage processor feature and select it as the primary transport mechanism for ConnectEMC notifications. These actions will help to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. If you do not provision ESRS, you may need to collect system information manually to assist EMC Support with troubleshooting and resolving problems with the VNX block system.

The ESRS device client on storage processor feature offers a secure architecture from end to end, including the following features:

- EMC issues X.509 digital certificates to authenticate the ESRS device client on storage processor to EMC.
- EMC professionals are authenticated using two unique factors.
- All EMC service professionals have a unique username that is logged with all their actions.
- All communication originates from the storage processor. The ESRS device client on storage processor does not accept unsolicited connections from EMC or the Internet.
- All communications between EMC and the ESRS device client on storage processor includes the latest security practices and encryption technologies, including certificate libraries based on RSA Lockbox technology, and Advanced Encryption Standard (AES) 256-bit encryption.
- Those who implement the ESRS device client on storage processor solution can further control remote access by using the Policy Manager. The Policy Manager gives full control of how EMC interacts with VNX systems. SSL is available between the ESRS device client on storage processor and the Policy Manager.

ESRS device client on storage processor management

You can manage the ESRS device client on storage processor feature using Unisphere®. You can provision or re-provision the service, set up a proxy server or Policy Manager, or both. You must provide your support account credentials to provision or re-provision the ESRS device client on a storage processor.

The VNX block system itself does not implement any policies. If you require more control over remote access to your VNX block system, you can use a Policy Manager to set authorization permissions. The Policy Manager software component can be installed on a customer-supplied server (see ESRS device client feature customer-side network topology example on page 13). It controls remote access to your devices, maintains an audit log of remote connections, and supports file transfer operations. You can control by whom, what, and when access to your VNX block system occurs. For additional information about the Policy Manager, go to the EMC Online Support website (https://support.emc.com/Products/). After logging in, locate the applicable Support by Product page and search for the link to the specific ESRS product technical documentation.

ESRS device client on storage processor communication

Access to a DNS server is required for the ESRS device client on storage processor feature to work. You should set the ESRS device client on storage processor feature to be the primary (default) method used by ConnectEMC to communicate with EMC backend systems.

Provision ESRS embedded device client on storage processor

NOTICE

As a prerequisite for you to provision the ESRS device client on storage processor feature in your VNX block system, you must have an existing EMC Online Support account. Also, at least one DNS server must be configured on your VNX before you set up the ESRS communication channel and provision the feature; otherwise, the feature will not work.

You or your EMC service provider can provision the ESRS device client on the storage processor through Unisphere. To provision the feature requires either you to provide your EMC Online Support account credentials (username and password) or your EMC service provider to provide their SecurID credentials.

To provision the ESRS device client on storage processor feature in Unisphere, you must be logged in to the storage processor as User administrator. Select your system and from the task list, under **Service Tasks**, select **Manage ESRS**.

Note

When provisioning the ESRS device client on the storage processor, you can provision an optional Proxy Server or a Policy Manager, or both. Once you have provisioned the feature, you should ensure that the primary transport mechanism for ConnectEMC notifications is set to ESRS. You can do this by selecting your system and from the task list, under **Service Tasks**, select **Manage ConnectEMC**. For detailed instructions and more information about provisioning the ESRS device client on storage processor feature, see the Unisphere online help.

Proxy Server

If the VNX block system will use a proxy server to connect to the Internet, you must indicate this when you configure the ESRS. You must provide the following information for the proxy server:

- Protocol (HTTPS or SOCKS)
- IP address
- Port number

If the proxy server requires authentication, you must also indicate this during the ESRS configuration and supply login credentials for the proxy server. You must supply both a username and password for authentication.

If you install a proxy server on a non-standard port, you will need to enter a port number to use the proxy server. If the port is not specified, the system defaults to the appropriate standard port for the given proxy type, port 3128 for the HTTP protocol or port 1080 for the SOCKS protocol.

Policy Manager

If the VNX block system will use a Policy Manager to set authorization permissions, you must indicate this when you configure the ESRS. You must provide the following information for the Policy Manager:

- Indicate whether the connection to the Policy Manager needs to be secure (SSL will be used in the connection to the Policy Manager); otherwise, SSH is used in the connection to the Policy Manager.
- IP address
- Port number

If the Policy Manager will use a proxy server to connect to the VNX block system, you must indicate this when you configure the ESRS. You must provide the following information for the Policy Manager's proxy server:

- Protocol (HTTPS or SOCKS)
- IP address
- Port number

If the Policy Manager's proxy server requires authentication, you must also indicate this during the ESRS configuration and supply login credentials for the proxy server. You must supply both a username and password for authentication.

While you configure a policy manager, you have the option to change the default port if you choose to use a non-secure transport. In this case, you will need to enter a port number for the policy manager proxy server. If you do not specify the port, then a default proxy server port is used. The system defaults to the appropriate standard port for the given protocol, port 3128 for the HTTP protocol or port 1080 for the SOCKS protocol. The

default ports for the Policy Manager are 8443 for secure communication or 8090 if not secure.

Re-provision ESRS embedded device client on the storage processor

You may need to re-provision the ESRS device client on the storage processor feature for any of the following reasons:

- To add or remove a Proxy Server or change existing Proxy Server settings
- To add or remove a Policy Manager or associated Proxy Server or change existing Policy Manager settings, including settings for an associated Proxy Server

Note

As a prerequisite for you to re-provision the ESRS embedded device client on the storage processor in your VNX block system, you must have already provisioned the ESRS feature. Also, to re-provision the ESRS device client on storage processor feature in Unisphere, you must be logged in to the storage processor as User administrator. See Provision ESRS embedded device client on storage processor on page 19 for information.

Upgrade ESRS embedded device client on storage processor

The ESRS embedded device client on storage processor feature is packaged into the VNX OE for block. Upgrade of the device client or associated features will only be delivered as part of a VNX OE for block software upgrade.

Capture array configuration data settings

VNX OE for block versions later than 5.32.000.5.209 and earlier than 5.33 provide a mechanism in Unisphere to manage the scheduling of capturing your VNX Block system configuration data. The resultant file will be sent through ConnectEMC to EMC backend systems. You must be logged in to Unisphere with Administrator privileges to use this feature.

To manage the schedule to capture your VNX Block system configuration data, select your system and from the task list, under **Service Tasks**, select **Capture Configuration Data**. The following is a list of the actions that you can take:

Note

EMC recommends using the default settings, especially the setting for the time of day to start the capture of your VNX Block system configuration data and the settings for those days on which to capture your VNX Block system configuration data.

- Enable or disable the related fields and controls.
- Select the frequency, in weeks to capture your VNX Block system configuration data.
- Schedule the time of day to start the capture of your VNX Block system configuration data.
- Select those days on which to capture your VNX Block system configuration data.
- Select to immediately capture your VNX Block system configuration data and send the resulting file through ConnectEMC to EMC backend systems.

CHAPTER 4

ESRS IP Client for VNX feature

This chapter describes the requirements for installing the ESRS IP Client for VNX software. It explains how to access and download the ESRS IP Client UI-based installer wizard from the EMC Online Support website. It describes how to run the installation wizard that is used to download and use ESRS IP Client Management Utility to manage all the ESRS IP Client software components. These components are required so you can:

- Set up a centralized monitoring environment for your VNX or legacy systems
- Specify control stations running on each version of VNX or legacy systems that can connect to the monitor station and send ConnectHome notifications to your service provider.

After completing the installation or upgrade of your ESRS IP Client software on the monitor station, what you do next depends on the type of systems that have been added to your ESRS IP Client configuration.

Major topics include:

ESRS IP Client requirements

Note

Refer to the *EMC Serviceability Release Notes* for the latest ESRS IP Client environment and systems requirements.

The version of ESRS IP Client software must be at or later than the version of the management software bundled with the VNX Operating Environment (OE) running on each VNX for block or legacy system that is being monitored. Also, legacy Celerra® systems are not supported by ESRS IP Client; only VNX for file/unified is supported. ESRS IP Client installation requires:

- **Monitor station**: The monitor station must be a host or virtual machine with one or more CPUs at a minimum speed of 2.2 GHz, must be SSE and/or SSE2 supported, have a total physical memory size of 2 GB or greater and 1 GB of hard disk space, must be running a supported Windows operating system, have the .NET Framework version 2.0 installed, and use JRE revision 6.0 update 29 or later for 32-bit system (JRE for 32-bit system is also required for 64-bit Windows). The monitor station cannot be a client (host connected to storage-system data ports), and the monitored systems must be able to connect to it over your network. Also, the ESRS IP Client for VNX and the Unisphere Server for Windows cannot coexist on the same server. A pre-installation check in the ESRS IP Client for VNX prevents installation of the ESRS IP Client for VNX on a system that already has the Unisphere Server installed on it. For more information about the monitor station, refer to the *Setting Up a Unisphere Management Station for the VNX Series* document.

  Note

  For the latest list of supported Windows operating systems, refer to the *EMC Serviceability Release Notes*.

  - **If you do not have an existing monitor station** — You can create a monitor station by installing ESRS IP Client on a Windows host.
  - **If you have an existing monitor station running CLARalert (precursor to ESRS IP Client for VNX)** — You can upgrade to the ESRS IP Client on the monitor station.
  - **If you have an existing monitor station running event monitor** — You can install the ESRS IP Client on the monitor station.
- **Fixed or static IP address**: The monitor station must have a fixed or static IP address. If dynamic host control protocol (DHCP) is used, you must configure a reserved IP address. The ESRS IP Client wizard automatically detects and configures the ESRS IP Client with the IP address for the monitor station, which is required for the ESRS IP Client installation.
- **Open TCP Ports from the monitor station to your service provider**: The monitor station uses the following TCP ports to connect to your service provider:
  - TCP port 443 (for HTTPS, outbound)
  - TCP port 8443 (for HTTPS, outbound); not required for functionality, however without this port being opened there will be a significant decrease in remote support performance.
- **Open TCP Ports from the monitor station to your storage systems**: The monitor station uses the following TCP ports to connect to the storage systems:
  - TCP port 80 (for HTTP, inbound/outbound)

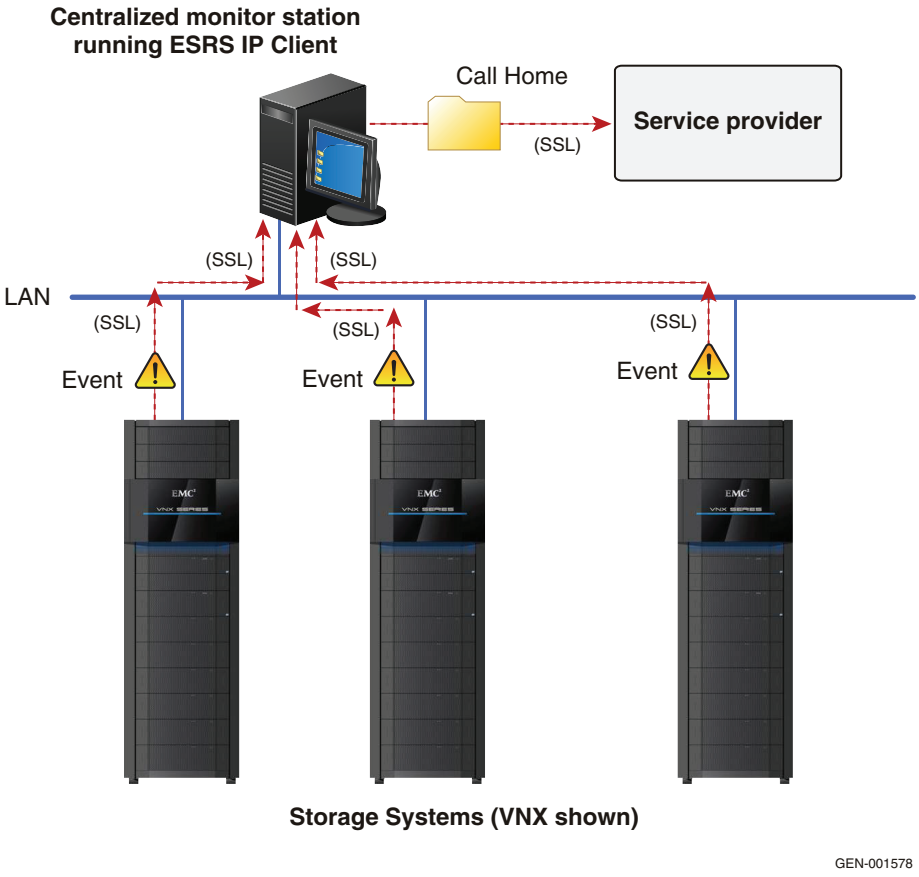
- TCP port 443 (for HTTPS, inbound/outbound)
- TCP port 25 (for the SMTP server, outbound)
- TCP port 6389 (for the Unisphere Host Agent, inbound/outbound)
- TCP port 5414 (for the EMCRemote Client, outbound)
- TCP port 9519 (for RemotelyAnywhere on VNX OE for block or legacy systems, outbound)
- TCP port 6391, 6392, and 60020 (for the Remote Diagnostic Agent, outbound)
- TCP port 22 (for the CLI with SSH)
- TCP port 13456 (for KTCONS)
- TCP port 22 and 9519 (for RemoteKtrace)
- TCP port 80, 443, 2162, 2163, and 8000 (for Unisphere Service Manager, Unisphere, and Navisphere® Secure CLI)

- **Proxy server:** If the monitor station connects to the Internet through a proxy server, you must indicate this during the ESRS IP Client installation and provide the IP address, port, and protocol (HTTPS or SOCKS) for the proxy server. If the proxy server requires authentication (SOCKS is supported only with authentication), you must also indicate this during installation and supply login credentials for the proxy server. You must supply both a username and password for authentication.
- **EMC Online Support account:** You must have an existing EMC Online Support account. You are required to log in to the EMC Online Support website at http://Support.EMC.com and supply your valid storage-system serial number before you can download and install the ESRS IP Client software.
- **Registered monitoring site:** The monitoring site must be registered on EMC Online Support. During the ESRS IP Client installation, you must specify contact information that includes the name, email address and phone number of a person to contact at the monitoring site.

New installation

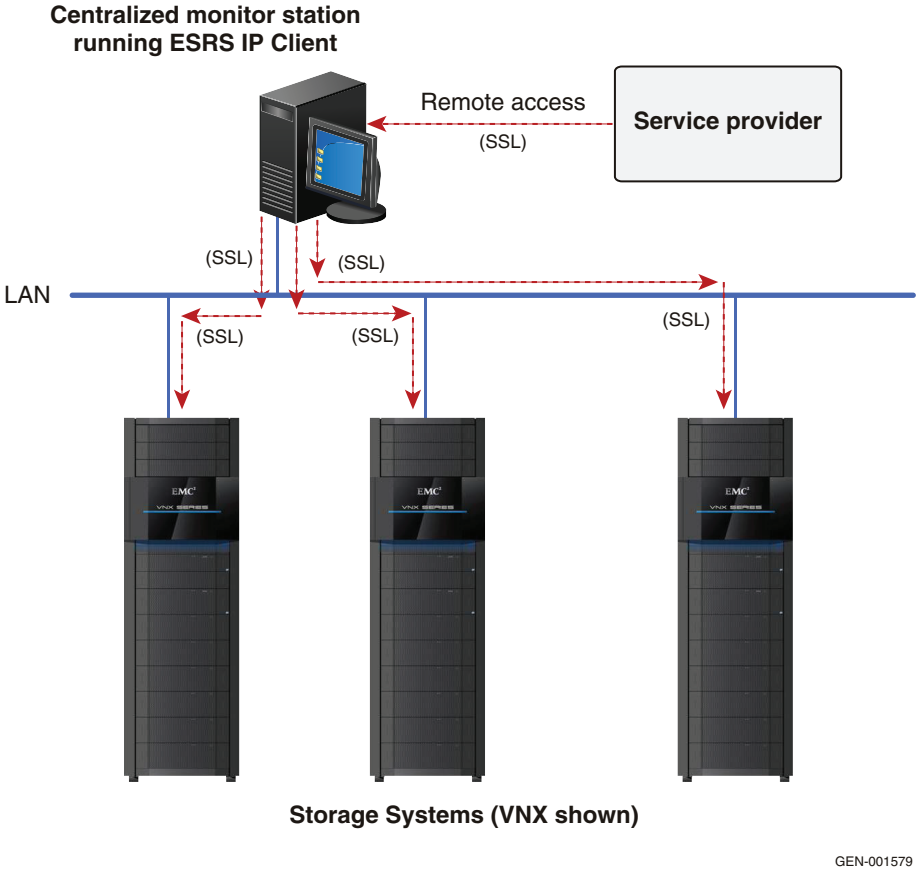
For a new ESRS IP Client installation, the installation wizard automatically installs a communication infrastructure that supports secure inbound/outbound communication (SSL) as the primary communication method with your service provider. This communication infrastructure notifies your service provider of events (Call Home feature, see Figure 2 on page 26).

Figure 2 ESRS IP Client communication infrastructure - Call Home example



This same communication infrastructure is used to send ConnectHome data from your specified VNX device(s) (the associated control station(s) that are connected to the monitor station) or legacy systems to your service provider and to provide your service provider with remote access to your VNX devices or legacy systems (see Figure 3 on page 27).

Figure 3 ESRS IP Client communication infrastructure - Remote access example



Note

The default authorization permission for remote access to your VNX or legacy systems is set to always allow. If you require more control over remote access to your VNX or legacy systems, you can use a Policy Manager to set authorization permissions. The Policy Manager software component is installed on a customer-supplied server. It controls remote access to your devices, maintains an audit log of remote connections, and supports file transfer operations. You can control who, what, and when, and even why access to your system has occurred. For additional information on Policy Manager, go to the EMC Online Support website (Support.EMC.com). After logging in, locate the applicable Support by Product page and the link for the specific product technical documentation.

Before the ESRS IP Client software installation starts, you need to configure the proxy settings if the server uses a proxy server to connect to the Internet. Also, you are required to enter the credentials to log in and provide the Customer Contact Information as communication methods.

When the ESRS IP Client software installation completes, you need to launch the ESRS IP Client Management Utility to add new system(s) to be monitored. You enter the IP address of a system to access it. Once you log into the system, the ESRS IP Client Management Utility will obtain a list of all the systems in the same domain. You can add one or more discovered systems to be monitored by selecting them in Add System dialog. The application will ignore the system(s) that are already being monitored. It will also designate an Storage Processor that is running on the latest VNX OE for block as the Host Agent portal system if there is no existing portal system. If the version of the VNX OE for

block of the existing portal system is older than the VNX OE for block of the newly added system, the portal system will be migrated to the new SP automatically.

The ESRS IP Client Management Utility application allows you to configure and manage the systems you added through the following operations:

- **Add System**. Add a system to be monitored.
- **Save Changes**. Save the changes you made to systems being monitored.
- **Cancel Changes**. Drop the changes you made to the systems being monitored.
- **Configure Local Email**. Specify an email address of a designated local user.
- **Configuration Capture Settings**. Capture the configuration data of selected system(s) and send it to EMC periodically.
- **Capture Configuration Now**. Capture the real-time configuration data of selected system(s) manually.
- **Remove System**. Remove the selected system(s) from the list of systems being monitored.
- **Send Test Alert**. Send out an email alert for the purpose of testing.

Upgrade

Only ESRS IP client upgrades within versions 1.3.x.x or later are supported.

Upgrades from previous ESRS IP Client or CLARalert versions (1.0.x.x, 1.1.x.x, or 1.2.x.x to 1.3.x.x) are not supported. For these previous versions, record the IP addresses of the system(s) that are currently being monitored, uninstall the current software and reboot the client, install this version and then re-add the systems.

Note

You can uninstall the ESRS IP Client for VNX, by selecting **Add/Remove Programs** from the Windows control panel. If AHA or UDoctor have been installed, they should be uninstalled.

During the installation, you will need:

- Internet access
- An EMC Online Support (Powerlink) account
- The serial number of one system installed at the customer site and associated with the user's Powerlink account
- The name of the customer site
- Internet proxy settings, if required
- SMTP server name, if backup email will be configured
- Record the systems that are being monitored by this configuration:
  - Start the ESRS Configuration Tool GUI and select the **Managed Devices** tab and execute the **Refresh** button. Record the systems serial numbers and IP addresses that will be re-added to the new installation. (**Program Files** › **ESRS** › **Configuration Tool**).

Note

There is also a Configuration Tool text file that contains the monitored systems data. First execute the Refresh button from the Managed Devices tab. Navigate to Program Files\EMC\ESRS IP Client\Gateway directory. Open the EsrsConfigTool text file and scroll to the end of the file. All monitored systems are recorded in this file after the refresh.

- CLARiiON and VNX for Block systems: record the address of SPA
- VNX for File systems: record the address of the Control Station

Note

This version of the ESRS IP Client will not block the user from installing over an existing version, but EMC does not recommend doing so.

After the ESRS IP Client installation, launch the Management Utility to add or remove systems. The software will automatically create a portal system and configure your centralized monitoring environment for VNX and CLARiiON storage systems. You can add VNX for Block and CLARiiON storage systems to your centralized monitoring environment using Unisphere/Navisphere Manager. See the EMC Unisphere/Navisphere Manager online help for more information.

Installation on a Windows 7 or Windows Server 2008 host with the Windows firewall enabled requires you to open TCP/IP port 6389 inbound/outbound for "C:\Program Files (x86)\EMC\HostAgent\HostAgent.exe" to allow the Unisphere Host Agent to function properly. This must be done before you install the ESRS IP Client. If the port is blocked, the installation will fail because the client will not be able to communicate with the target storage systems.

Verify HTTPS connectivity during pre-installation

The ESRS IP Client installer wizard verifies the following IP address names for HTTPS connectivity during pre-installation:

EMC Registration:

- https://esrs.emc.com
- https://esrs.emc.com:443

ESRS Core (for gateway pings):

- https://esrs-core.emc.com:80
- https://esrs-core.emc.com:443

Global access server:

- https://esrgweprd01.emc.com:443
- https://esrgweprd02.emc.com:443
- https://esrgweprd03.emc.com:443
- https://esrghoprd01.emc.com:443
- https://esrghoprd02.emc.com:443
- https://esrghoprd03.emc.com:443
- https://esrgckprd01.emc.com:443
- https://esrgckprd02.emc.com:443

- https://esrgckprd03.emc.com:443
- https://esrgscprd01.emc.com:443
- https://esrgscprd02.emc.com:443
- https://esrgscprd03.emc.com:443
- https://esrgspprd01.emc.com:443
- https://esrgspprd02.emc.com:443
- https://esrgspprd03.emc.com:443

HTTPS connectivity is required for the ESRS core and ESRS UI IP address names and at least four of the global access server IP address names. EMC recommends that all the global access server IP address names listed above should be accessible for HTTPS connectivity.

Installation wizard

Note

The installation wizard will prompt you to select an installation mode for ESRS IP Client. This document describes the customer installation mode only. It is the recommended installation mode and is supported for customers performing a new ESRS IP Client installation or upgrade.

The installation wizard guides you through the ESRS IP Client installation process. You can use the wizard for a new ESRS IP Client installation, or to upgrade an existing 6.22 or later CLARalert or ESRS IP Client for CLARiiON environment. An EMC service provider or EMC authorized partner must perform upgrades to an existing CLARalert environment that is running a CLARalert version earlier than 6.22.

Download and install ESRS IP Client software

You can access and download the ESRS IP Client UI-based installer wizard from the EMC Online Support website. Use the wizard to download and configure all the ESRS IP Client software components required to set up a centralized monitoring environment for your VNX and legacy systems.

Before you begin

Do not install the ESRS IP client for VNX on an ESRS gateway server.

Before installing the ESRS IP client for VNX on a Windows 7 host with the Windows firewall enabled, ensure TCP/IP port 6389 is open. TCP/IP port 6389 must be open to allow the Unisphere Host Agent to function properly. If TCP/IP port 6389 is blocked, the installation will fail because the client will not be able to communicate with the target storage systems. The HostAgent.exe is located at **`C:\Program Files\EMC\HostAgent\HostAgent.exe`** for 32 bit Windows versions and **`C:\Program Files (x86)\EMC\HostAgent\HostAgent.exe`** for 64 bit Windows versions.

Also, the ESRS IP Client for VNX and the Unisphere Server for Windows cannot coexist on the same server. A pre-installation check in the ESRS IP Client for VNX will prevent installation of the ESRS IP Client for VNX on a system that already has the Unisphere Server installed on it. If this is the case, uninstall the Unisphere Server before installing the ESRS IP Client for VNX. The ESRS IP Client for VNX uses the presence of the registry key **`HKEY_LOCAL_MACHINE\Software\EMC\ManagementServer`** to determine if the Unisphere Server is installed. If that key is not removed by the Unisphere Server uninstaller, it can prevent the ESRS IP Client for VNX from being installed. You can delete

the key from the registry by using `regedit` command and then you should be able to install the ESRS IP Client for VNX.

From the monitor station:

Procedure

1. Go to the EMC Online Support website at http://Support.EMC.com and locate the Download page and the link to download the ESRS IP Client for VNX software.
2. Select **Download ESRS IP Client** and save the software to your monitor station.
3. In the folder where you saved the ESRS IP Client, double-click the ESRS IP Client executable file or if necessary, right-click the file and select **Run as** to run the installation wizard using a different user's credentials.
4. Follow the steps in the wizard to complete the installation.

Note

For VNX OE for block and legacy systems that are deployed in this ESRS IP Client configuration, you must add the monitor station IP address to the RemotelyAnywhere filter tables of those systems. See Add monitor station to RemotelyAnywhere IP address filter tables on page 31 for detailed information.

Results

For a list of the IP address names verified for HTTPS connectivity during the pre-installation checks, see Verify HTTPS connectivity during pre-installation on page 29. Also, the ESRS IP Client software installation generates four log files. Two of these log files (`esrsagent_installer.log` and `esrsipclient_installer.log`) are located under the user's home directory in the `EMC\ESRSIPClient` folder. The other two logs, `esrs_rscapi.log`, and `esrs_jema.log`, are located in the directory where the ESRS IP Client is installed. The `esrs_rscapi.log` log is created for VNX for block registrations only. The `esrs_jema.log` log is created for VNX for file registrations only.

Add monitor station to RemotelyAnywhere IP address filter tables

Note

Perform this procedure for VNX OE for block and legacy systems in this ESRS IP Client configuration.

By default, this feature adds an always-on, additional layer of security that restricts the use of remote service tools to the system's service ports. Administrators and security administrators can extend remote service tool access to a system's management ports by entering the IP addresses of the attached, trusted service clients.

Note

For IPv6 configurations, temporary private addresses are disabled on the system by default. EMC strongly recommends that you also disable them on the client system.

Procedure

1. Enter the SP A or SP B IP address or hostname in a supported browser address field and append the setup page path to the IP address or hostname, for example, `http://IP address/setup` or `http://hostname/setup`.

   The SP setup login page opens.

2. Enter the system Navisphere Manager or Unisphere administrator access username and password.

   The SP setup page opens.

3. Scroll down to **Set RemotelyAnywhere Access Restriction** and click the name panel to open the page.

   Note

   System security must be enabled and configured before you can access the **Set RemotelyAnywhere Access Restriction IP** address filter table.

   The **IP Filter Configuration for RemotelyAnywhere** page opens.

4. Verify that your monitor station IP address is entered in the IP address filter tables.
5. Enter your monitor station IP address in the **Filters that apply to all storage systems in the domain** input table.

   Note

   You can enter up to 16 RemotelyAnywhere (RA) client addresses into the input tables. At this time you cannot enter address ranges or complete subnets into the input tables. Entering RA client addresses into the **Connected storage system only** input table does not propagate those addresses to VNX OE for block and legacy systems in the domain. Use the **Connected storage system only** input table if you do not want to propagate the data to other systems in the domain.

   Using the **Filters that apply to all storage systems in the domain** input table will propagate the RA client address you entered to VNX OE for block and legacy systems in the domain.

6. Click **Apply Setting**.

   Note

   Updating the IP filter tables will reset any existing RA connections.

   The **RemotelyAnywhere IP Filter Configuration - Confirmation** page opens.

7. Click **Apply Settings**.

   Note

   The following text message should appear:

   ```
   RemotelyAnywhere IP Filter request was successful.
   ```

   The **RemotelyAnywhere IP Filter Configuration - Apply** page opens.

8. Click **Back**.

   The main setup page appears.

9. Click **Logout** and close the browser.
10. If you entered the monitor station IP address in the **Connected storage system only** filter table, repeat these steps for VNX OE for block and legacy systems in the domain of this ESRS IP Client configuration.

Change HTTPS communications security

When you initially set up a configuration with VNX for file/unified systems, the HTTPS connection between the ConnectHome feature on a control station and the ESRS HTTPS Listener service that is installed on the monitor station uses a default HTTPS configuration. Once the ConnectHome feature and the ESRS HTTPS Listener service are installed and configured using the default HTTPS configuration and the connection is working, you should provide the ESRS HTTPS Listener service with an X.509 certificate that is specific to the system hosting the service. This action strengthens the security of the HTTPS connection and allows the server identity to be verified by any ConnectHome client. For specific instructions and additional information, go to the EMC Online Support website and locate the applicable Support by Product page and the link for the specific product technical documentation (*Managing the SSL Certificate for the ESRS HTTPS Listener Service*).

Make changes using Unisphere UI

Use the Unisphere UI to do the following:

- Add VNX for block and legacy systems to or remove them from your centralized monitoring environment.
- View the properties of the Call Home templates and assign additional Call Home templates to VNX for block or legacy systems.
- Manage ConnectHome information for a VNX for file/unified system.
- View events for a monitored VNX for block or file/unified or a legacy system.

For more information about using Unisphere, see the Unisphere help, which is in the Unisphere UI or go to the EMC Online Support website and locate the applicable Support by Product page and the link for the specific product technical documentation required. The website has the most recent version.