EMC Unity™ Family

EMC Unity™ All Flash, EMC Unity™ Hybrid, EMC UnityVSA™

Version 4.1

Secure Remote Services Requirements and Configuration

P/N 302-002-573 REV 02

EMC²

CONTENTS

CONTENTS

Additional resources

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features. Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Where to get help
Support, product, and licensing information can be obtained as follows:

Product information
For product and feature documentation or release notes, go to Unity Technical Documentation at: www.emc.com/en-us/documentation/unity-family.htm. You can also access this page from the Unity product family page at: www.emc.com/en-us/storage/unity.htm. In the **Why EMC Unity Storage** section, click **Unity Product Resources** > **Technical Documentation**.

Troubleshooting
For information about EMC products, software updates, licensing, and service, go to EMC Online Support (registration required) at: https://Support.EMC.com. After logging in, locate the appropriate **Support by Product** page.

Technical support
For technical support and service requests, go to EMC Online Support at: https://Support.EMC.com. After logging in, locate **Create a service request**. To open a service request, you must have a valid support agreement. Contact your EMC Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

Special notice conventions used in this document
EMC uses the following conventions for special notices:

⚠ **DANGER**

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠**WARNING**

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠ **CAUTION**

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Addresses practices not related to personal injury.

Note

Presents information that is important, but not hazard-related.

CHAPTER 1

Introduction

This chapter introduces you to the EMC Secure Remote Services (ESRS) feature.

Topics include:

Benefits of ESRS

The embedded ESRS feature in Unity deployments provides a highly secure, remote connection between your EMC Unity environment and EMC. A connection that, once made, can unlock a wide range of benefits and services like:

- Automated health checks.
- 24x7 predictive wellness monitoring.
- Remote issue analysis and diagnosis.
- An enhanced Online Support experience with actionable, real-time data-driven insight into your global EMC environment through the MyService360 dashboard.
- Remote delivery of EMC's service and support.
- CloudIQ, a free software-as-a-service cloud management dashboard that provides intelligent analytics about performance, capacity, and configuration for health-based reporting and remediation. ESRS must be enabled on your storage system to send data to CloudIQ.

About remote service options

Two remote service options are available by which to send storage system information to EMC for remote troubleshooting:

- Centralized EMC Secure Remote Services
- Integrated EMC Secure Remote Services (physical deployments only)

A third option, to not enable remote services, is available but not recommended. If you select this option, EMC will not receive notifications about issues with the storage system. You may need to collect system information manually to assist support representatives with troubleshooting and resolving problems with the storage system.

Note

Before you can configure ESRS, you must specify valid support credentials and contact information.

Centralized ESRS

Centralized ESRS runs on a gateway server. When you select this option, your storage system is added to other storage systems in an ESRS cluster. The cluster resides behind a single common (centralized) secure connection between EMC servers and an off-array ESRS Gateway. The ESRS Gateway is the single point of entry and exit for all IP-based EMC remote support activities for the storage systems associated with the gateway.

The ESRS Gateway is a remote support solution application that is installed on one or more customer-supplied dedicated servers. The ESRS Gateway functions as a communication broker between the associated storage systems, Policy Manager and proxy servers (optional), and the EMC enterprise. Connections to the Policy Manager and associated proxy servers are configured through the ESRS Gateway interface along with add (register), modify, delete (unregister), and querying status capabilities that ESRS clients can use to register with the ESRS Gateway.

For more information about ESRS Gateway and Policy Manager, go to the EMC Secure Remote Services product page on Online Support (https:// Support.EMC.com).

To configure your storage system to use Centralized ESRS, you only need to provide the IP address of the ESRS Gateway and ensure that port 9443 is open between the gateway and the storage system.

Note

Storage systems can only be added to the ESRS Gateway from Unisphere. If the storage system is added from the gateway server, it will appear to be connected, but will not successfully send system information.

Integrated ESRS (physical deployments only)

Note

This feature may not be available in your implementation.

Integrated ESRS runs directly on the storage system. When you select this option, the storage system sets up a secure connection between itself and EMC Global Access Servers. This option enables remote connectivity for dial in and dial out capabilities with this storage system. The connection from this storage system to a Policy Manager and any associated proxy servers (optional) must be configured through either Unisphere or the CLI.

To configure the storage system to use Integrated ESRS, you must:

1. Accept the license agreement for the feature.

2. Verify contact and system location information.

3. Configure a proxy server (if required by your IT administrator).

4. Open ports 443 and 8443 outbound to *.emc.com on the storage system. Refer to *KB 335386* for more information on the IP addresses used by ESRS.

5. Request an access code for verification through email (an extra level of authentication).

6. Confirm the site ID information for the storage system.

7. Check the status of the system's ESRS connection to EMC.

8. Configure the Policy Manager (if an additional layer of security is required). The Policy Manager requires port 8090 to be open for outgoing traffic. If it is configured to use SSL, port 8443 must be open.

Operational description

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

Note

It is strongly recommended that you enable the ESRS feature to accelerate problem diagnosis, perform troubleshooting, and help speed time to resolution. If you do not enable ESRS, you may need to collect system information manually to assist EMC Support with troubleshooting and resolving problems with your storage system. ESRS must be enabled on the system for data to be sent to CloudIQ.

ESRS and security

ESRS employs multiple security layers throughout each step in the remote connectivity process to ensure that you and EMC can use the solution with confidence:

- All notifications to EMC originate from your site—never from an outside source—and are kept secure through the use of Advanced Encryption Standard (AES)-256 bit encryption

- IP-based architecture integrates with your existing infrastructure and maintains the security of your environment

- Communications between your site and EMC are bilaterally authenticated using RSA® digital certificates

- Only authorized EMC Customer Service professionals verified via two-factor authentication can download the digital certificates needed to view a notification from your site

- The optional ESRS v3 Policy Manager application enables you to grant or restrict EMC access based on your own unique guidelines and requirements, and includes a detailed audit log

ESRS management

You can manage ESRS using Unisphere, UEMCLI, or the REST API. You can enable or disable the service, set up a proxy server or Policy Manager (physical deployments only), or both, and provide your Full-access support account credentials which are necessary for ESRS to work.

The storage system itself does not implement any policies. If you require more control over remote access to your storage system, you can use a Policy Manager to set authorization permissions. The Policy Manager software component can be 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 by whom, what, and when access to your storage system occurs. For more information about the Policy Manager, go to the Online Support website (https://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.

The integrated ESRS feature (physical deployments only) is embedded in the operating environment (OE) of the storage system as a managed service. This feature may not be available in your implementation. The integrated implementation includes the High Availability (HA) feature, which provides monitoring of ESRS and is responsible for failing it over from the primary storage processor (SP) to the backup SP should the primary SP fail. HA is responsible for restarting ESRS if it fails. The OE is responsible for persisting the configuration and certificates that are needed for ESRS to work.

ESRS is supported in full service mode (both SPs are in service mode). If you have already enabled ESRS, the system functions as configured. If you have not enabled ESRS, you can temporarily enable it. In this latter situation, the configuration will not persist once your storage system has recovered to normal operation.

ESRS communication

Access to a DNS server is required for ESRS to work.

By default, ESRS attempts to use a configured proxy server to communicate with EMC backend systems. If the proxy server is not available, ESRS attempts to bypass the proxy server and communicate directly to the EMC backend systems.

CHAPTER 2

Requirements and Configuration

This chapter describes the requirements for the ESRS feature and provides an operational description of the feature. The chapter also describes the processes to provision the feature.

Topics include:

Requirements for ESRS

As prerequisites for enabling ESRS on the storage system, you must have the following:

- Operating environment (OE) version 4.0 or later.

- At least one DNS server must be configured on the storage system.

- Unrestricted access to backend EMC Global Access Servers (GAS) over the Internet using HTTPS (for non-proxy environments). For more information, see *KB 335386*.

- EMC Online Support Full-access account (requires specific credentials that are associated with the site ID, which is associated with the system serial number).

- Do not use dynamic IP addresses (DHCP) for any components of the ESRS Gateway servers, Policy Manager servers, or managed devices.

- Network traffic over ports 80 and 443 is not required for ESRS functionally, but is required for remote support personnel to perform many break/fix tasks using ESRS.

- SSL checking, certificate verification, and certificate proxying are not permitted for ESRS network traffic.

> **NOTICE**

If you use DHCP to assign IP addresses to any ESRS components (ESRS Gateway servers, Policy Manager servers, or managed devices), they must have static IP addresses. Leases for the IP addresses that EMC devices use cannot be set to expire. It is recommended that you assign static IP addresses to those devices you plan to have managed by ESRS.

Requirements for Integrated ESRS

The following requirements are related to the Integrated ESRS implementation only:

- Network traffic (HTTPS) must be permitted on ports 443 and 8443 (outbound only) for the required backend EMC Global Access Servers. Failure to open port 8443 results in significant performance impact (30–45 percent). Failure to open both ports may result in a delay in resolving issues with the end device.

- If the ESRS implementation includes a proxy server to connect to the Internet, you must indicate this when you configure the ESRS feature.

- If the ESRS implementation includes a Policy Manager for more control over remote access to the storage system, you must indicate this when you configure the ESRS feature.

- If the ESRS implementation includes a proxy server for the storage system to connect to a Policy Manager, you must indicate this when you configure the ESRS feature.

Requirements for Centralized ESRS

The following requirement is related to the Centralized ESRS implementation only:

- Network traffic (HTTPS) must be permitted on port 9443 between the Unity system and the ESRS Gateway server.

- The ESRS gateway server operating environment must be version 3.12.00.04 or later.

> **NOTICE**
>
> Never manually add or remove a Unity system from an ESRS Gateway server. Only add or remove a storage system from a gateway server with the Unisphere ESRS configuration wizard.

Note

The configuration will fail if the ESRS Gateway server is not associated with the Site ID for the Unity system. For more information, see *KB 488483*. If the Unity system is listed under the wrong site ID, refer to *KB 489840* for information on how to change the site ID that is associated with the system.

EMC Online Support Full-access account

Configuring ESRS on a storage system requires an active Full-access account on the EMC Online Support website. This account associates specific credentials with a particular organization and email domain. When you configure ESRS on the storage system, you must specify these credentials (a user name password pair) to enable the ESRS communication channel for the system.

Note

Full-access support is only provided to customers that are EMC Supported (not supported by a Service Enabled Partner).

Creating an initial EMC Online Support account

When you create an initial EMC Online Support account, your account may have Limited-access privileges and may not be associated with a company profile. Unless your company has an established profile with EMC Online Support, the account is created with an email address, user name and password, but without company affiliation. When you create the account, you receive a confirmation email message containing a validation link. You can click the link, log into the EMC Online Support website, activate your account, and if established as a Limited-access (or "Lite") account, you can (optionally) request an upgrade to Full-access privileges.

Note

Limited-access account privileges are sufficient for registering and licensing storage systems. However, you cannot configure ESRS for a storage system based on an account that has only Limited-access privileges.

Upgrading to Full Access privileges

If your EMC Online Support account is initially activated as a Limited-access account, you can provide additional information in a request for Full-access privileges.

If your organization already has a company profile within the EMC Online Support website, you may be asked to select your site ID (location) from among those provided, upon which you will be associated to your company and will be able to configure ESRS on your storage system.

To request a new customer profile on the EMC Online Support web site, you must provide the following information:

Required Information	Description
Relationship with EMC	Indicate whether your organization is a partner, supplier, or customer of EMC products.
Site ID (Location)	Select an existing Site ID (if one has already been created for your organization) or select your organization from a database of organization profiles.

Note

The email address associated with the initial Limited-access account becomes the business email domain associated with the new customer profile.

If you provided company information when validating your Limited-access account, your request will be processed within 24-48 hours. At that time, you will receive a confirmation email confirming the account status change to Full-access privileges. The email contains a validation link that you click in order to log in and activate Full-access support privileges on the EMC Online Support system.

After you activate Full-access support privileges for your EMC Online Support, you can use the account credentials to configure the ESRS feature on your storage systems associated with your organization.

How to configure ESRS

In Unisphere, you can configure remote support for a storage system in several ways:

- Initial Configuration Wizard - Wizard for configuring global storage system settings which runs when you first access the system with Unisphere.

- Overview - Service page for the storage system that you can access from Unisphere (**System** > **Service** > **Overview**).

- EMC Secure Remote Services - An ESRS settings page that you can access from Unisphere (**Settings** > **Support Configuration**).

- UEMCLI - Command line interface that includes commands you can run on a system through a prompt from a Microsoft Windows or UNIX/Linux host to configure ESRS settings. For information about ESRS related CLI commands, see the *Unisphere Command Line Interface User Guide*.

- Unisphere Management REST API server - Application interface that can receive REST API requests to configure ESRS settings. For information related to the Unisphere Management REST API, see the *Unisphere Management REST API Programmers Guide*.

To determine the status of the ESRS feature, in Unisphere, go to **System** > **Service** > **Overview**. ESRS is enabled when a check mark appears within a green circle under **EMC Secure Remote Services**.

When enabling the ESRS feature on a storage system, configure the following settings:

Note

You must specify valid EMC support credentials (user name and password associated with an active Online Support account with Full-access privileges) and contact information before you can configure EMC Secure Remote Services.

- EMC Secure Remote Services - Type of ESRS, Centralized or Integrated, that the storage system will use. Although you can disable ESRS, it is not recommended.
- License Agreement (Integrated ESRS only) - The ESRS End User License Agreement (EULA) must be accepted in order to configure and use the Integrated ESRS.
- Contact and System Location information - Information that the EMC enterprise will use to respond to your support issues. The Email Address must be valid. The length of System Location, First and Last Name, Email Address, Phone Number, Address 1, Address 2, City, and State should be no more than 64. The text length of the Postal Code should be no more than 12.
- Proxy server information (optional, Integrated ESRS only) - Proxy server information for the ESRS communication channel:
    - Protocol: Protocol used to communicate with a proxy server used for the ESRS communication channel. The available options are HTTP on port 3128 and SOCKS (the default) on port 1080.

        Note

        Selecting either SOCKS or HTTP automatically adds the associated port to the proxy sever address if you do not specify the port.

    - Proxy server address: Network address and port number to associate with proxy server traffic.
    - Credentials: User name and password of an account used to access the proxy server system.
- Policy manager information (optional, Integrated ESRS only) - Policy manager information for the ESRS communication channel:
    - Protocol: Protocol used to communicate with a policy manager system used for the ESRS communication channel.
    - Proxy server address: Network address and port number to associate with policy server traffic.
- Policy manager proxy server information (optional, Integrated ESRS only) - When a policy manager is in use, proxy server used by the ESRS policy manager:
    - Protocol: Protocol used to communicate with a proxy server used by the policy manager.
    - Proxy server address: Network address and port number to associate with proxy server used by policy server.
    - Credentials: User name and password of an account used to access the proxy server used by the policy manager.

Proxy Server (Integrated ESRS only)

The proxy server settings for the system should have already been configured as part of the system initial configuration. Verify these settings while configuring an integrated ESRS implementation and make any necessary changes.

Policy Manager (Integrated ESRS only)

If your storage system will use a Policy Manager to set authorization permissions, you must indicate this when you configure the ESRS. If the Policy Manager will use a

proxy server to connect to your storage system, you must also indicate this when you configure the ESRS. If the Policy Manager's proxy server requires authentication (SOCKS is supported only with 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.

For more information about the Policy Manager, refer to the *Secure Remote Services Policy Manager Operations Guide* on the EMC Online Support website (https://Support.EMC.com).

CHAPTER 3

Configure Remote Support using Unisphere

This chapter describes the processes to provision the ESRS feature using the Unisphere interface.

Topics include:

Configure remote support

Before you begin

If your IT environment requires the storage system to connect through a proxy server, verify that the proxy server is configured before continuing by reviewing the **Settings** > **Support Configuration** > **Proxy Server** page.

To configure remote support using Unisphere, do the following:

Procedure

1. Select the **Settings** icon, and then select **Support Configuration**.
2. If your support credentials are not already specified, select **EMC Support Credentials** to specify your support credentials, Username, and Password. Otherwise, go to the next step.

   If you do not specify valid EMC Support Credentials, you cannot configure ESRS, view support contract information, or navigate to Online Support product pages.

3. If your contact information is not already specified, select **Contact Information** to specify the contact information that the EMC enterprise will use to respond to your support issues. Otherwise, go to the next step.

   The Email Address must be valid. The text length of System Location, First and Last Name, Email Address, Phone Number, Address 1, Address 2, City, and State should be no more than 64. The text length of Zip Code should be no more than 12.

4. Select **EMC Secure Remote Services** to specify which ESRS option you prefer to use.

Option	Description
Monitor with a Centralized ESRS configuration	Specify the Network Address of the ESRS Gateway server that is used to connect to the EMC enterprise and ensure that port 9443 is open between the Gateway server and the storage system.
Monitor with this storage system's integrated ESRS client (physical deployments only)	This feature may not be available in your implementation. You must go through the Configure ESRS process and accept the ESRS EULA and verify your contact and site location information. Use of the Policy Manager and proxy servers is optional. Once selected, you can configure a Policy Manager and Proxy Server settings.
Do not enable remote services	Not enabling remote services is not recommended. Enabling Remote Services accelerates problem diagnosis and helps speed time to resolution.

After you finish

Always test connectivity after configuring ESRS. This process checks that the connection is working and causes EMC to recognize the system and update its status from Unknown. Click **Test** in one of the following locations:

- **Dashboard** > **System** > **Service** under **EMC Secure Remote Services**

- **Settings** > **Support Configuration** > **EMC Secure Remote Services**

If you need to change (re-provision) the ESRS configuration information, select **Change**. The **Configure ESRS** wizard appears in which you can make changes. The **Verify Contact Information and System Location** information panel in the ESRS wizard is enabled with an edit option (pencil icon) beside **System information**. System information can be updated with the exception of the Site ID number.

Note

If the Status appears to remain as Transitioning and does not change after several minutes (the time it should take to test connectivity), contact Online Support.

Configure Integrated ESRS (physical deployments only)

Before you begin

Integrated has been selected in **EMC Secure Remote Services** and the **Configure ESRS** wizard appears.

To complete configuring Integrated ESRS, do the following:

Procedure

1. Accept the ESRS End User License Agreement (EULA).

   The ESRS EULA must be accepted in order to configure and use the Integrated ESRS.

2. Verify the Customer Contact Data information.

   To add or change Customer Contact Data information, click the pencil icon beside **Contact Information** and fill in the appropriate information in the dialog box that appears. This information is required to proceed with the ESRS configuration. Ensure that this information is accurate. The EMC enterprise will use this information to respond to your support issues.

3. Review the proxy server settings and make any necessary changes.

   Note

   Changes made on this page apply to the global proxy settings for the storage system.

   When you submit the Proxy Server page and the server details have been entered, network tests are performed to check connectivity between the device, the core node, and the EMC Global Access Servers (GAS). The network connectivity from ESRS to all the required EMC servers is checked. If the tests are unsuccessful, which means the device is unable to connect to some or all of the backend servers, the results are displayed at the top of the wizard page. If this is the case, verify that the appropriate firewall hosts and ports (443 and 8443) are open to EMC. All tests must be successful. You are responsible for resolution of proxy server and firewall issues that impact connectivity to the EMC ESRS infrastructure.

4. Go through the email verification process.

   This step adds an extra level of authentication and helps to ensure that you are the correct user and authorized to enable ESRS on the storage system.

   a. Select **Send access code** to initiate a request for an access code from EMC.

The generated access code is an 8-digit PIN code and is valid for 30 minutes from the time it is generated. You must complete the wizard within that period. If you select **Send access code** again at any time during the 30 minute period for this procedure, the previous code is automatically invalidated, and you must use the most current code.

An access code is subsequently sent from EMC to the email address associated with the support credentials of the support account. A message appears at the top of the page informing you to check your email.

b. In the **Access code** field, type the access code that you received by email.

If you encounter problems with this email verification process, EMC support personnel can select **Support Authentication** and use their RSA credentials, in which case the email verification process is skipped.

5. Confirm the site ID of the storage system.

   - If you need to change the site ID, select **Change Site ID**. In the **Change the site ID** dialog box that appears, the first item selected is, by default, the local associated site ID. Select the appropriate site ID from the list that appears. If the Unity system is listed under the wrong site ID, refer to *KB 489840* for more information.

   - If the site ID for the storage system cannot be found, select **Choose Site ID**. Select the appropriate site ID from the list that appears. If a site ID is not available or the correct site ID is not listed, you must notify your local field representative to request one. If a partner is doing the installation, the partner must submit the request to either the Install Base Group or to their field representative. The configuration will fail if the correct site ID is not provided. Inform user to quit the ESRS configuration until they have a valid site ID for the Unity system.

   Once ESRS is successfully configured, the EMC certificates are installed, ESRS is provisioned and registered on the EMC Enterprise, and the **Results** page appears.

6. If your storage system will use a Policy Manager to set authorization permissions, select **Configure Policy Manager** and fill the appropriate information for the Policy Manager; otherwise, go to step 8.

   The **Policy Manager** dialog box appears. If you are using Policy Manager, it must be installed and operational. It is recommended that the SSL strength be High.

7. If the Policy Manager will use a Proxy Server, select **Use Proxy Server for Policy Manager** and fill the appropriate information for the Proxy Server; otherwise, go to step 8.

8. Check the **Overview** panel on the **Service** page (**Dashboard** > **System** > **Service**) to see the status of the ESRS connection.

After you finish

Always test connectivity after configuring ESRS. This process checks that the connection is working and causes EMC to recognize the system and update its status from Unknown. Click **Test** in one of the following locations:

- **Dashboard** > **System** > **Service** under **EMC Secure Remote Services**

- **Settings** > **Support Configuration** > **EMC Secure Remote Services**

If you need to change (re-provision) the ESRS configuration information, select **Change**. The **Configure ESRS** wizard appears in which you can make changes. The

Verify Contact Information and System Location information panel in the ESRS wizard is enabled with an edit option (pencil icon) beside **System information**. System information can be updated with the exception of the Site ID number.

Note

If the Status appears to remain as Transitioning and does not change after several minutes (the time it should take to test connectivity), contact EMC Support.

Note

The Policy Manager can be configured or changed after configuring ESRS by clicking **Edit** on the **Settings** > **Support Configuration** > **EMC Secure Remote Services** page.

CHAPTER 4

Configure Remote Support using CLI

This chapter describes the processes to provision the ESRS feature using the UEMCLI. For full documentation of these and related commands, see the *Unisphere Command Line Interface User Guide*.

Topics include:

Configuring Remote Support using the CLI

Users have the option to provision Integrated ESRS with the UEMCLI.

Procedure

1. Set the support credentials:

   Format:
   ```
   /sys/support/account set -user <value> {-passwd <value> |
   -passwdSecure}
   ```

   Action qualifiers:

Qualifier	Description
-user	Specify the user name of the support account.
-passwd	Specify the new password of the support account.
-passwdSecure	Specifies the password in secure mode - the user will be prompted to input the password.

   Example:
   ```
   uemcli -u Local/joe -p MyPassword456! -sslPolicy accept /sys/
   support/account set -user user1 -passwd Password123
   ```

2. Accept the ESRS End User License Agreement (EULA):

   Format:
   ```
   /sys/support/esrsi set -acceptEula yes
   ```

   Example:
   ```
   uemcli -u Local/joe -p MyPassword456! -sslPolicy accept /sys/
   support/esrsi set -acceptEula yes
   ```

3. Set the Customer Contact Data information:

   Format:
   ```
   /sys/info set [-location <value>] [-contactFirstName
   <value>] [-contactLastName <value>] [-contactEmail
   <value>] [-contactPhone <value>] [-contactMobilePhone
   <value>]
   ```

   Action qualifiers:

Qualifier	Description
-location	Specify an updated location name.
-contactEmail	Specify the new contact email address for the system.
-contactPhone	Specify the new contact phone number for the system.
-contactMobilePhone	Specify the new contact mobile phone number for the system.
-contactFirstName	Specify the new contact first name for the system.

Qualifier	Description
`-contactLastName`	Specify the new contact last name for the system.

Example:
```
uemcli -u Local/joe -p MyPassword456! -sslPolicy accept /sys/
info set -contactFirstName Zach -contactLastName Arnold -
contactEmail something@someemail.com -contactPhone 1233456789 -
location here -contactMobilePhone 987654321
```

4. Optionally, configure the use of a proxy server:

Format:
```
/sys/support/config set [-enableSupportProxy {yes | no }]
[-supportProxyPort <value>] [-supportProxyUser <value> {-
supportProxyPasswd <value> |-supportProxyPasswdSecure}] [-
supportProxyProtocol {http | socks}]
```

Action qualifiers:

Qualifier	Description
`-enableSupportProxy`	Specifies whether to enable or disable the proxy server. Valid values are: • `yes` • `no`
`-supportProxyAddr`	Specify the name or IP address of the support services proxy server.
`-supportProxyPort`	Specify the port of the support services proxy server.
`-supportProxyUser`	Specify the user name of an account on the support services proxy server.
`-supportProxyPasswd`	Specify the password for the support services proxy server account.
`-supportProxyPasswdSecure`	Specifies the password in secure mode - the user is prompted to input the password.
`-supportProxyProtocol`	Specify the protocol used for communications with the support proxy server. Valid values are: • `http` • `socks` **Note** Values are case-sensitive.

Example:
```
uemcli -u <adminUser> -p <password> -sslPolicy accept /sys/
support/config set -supportProxyAddr 10.0.0.1 -supportProxyPort
```

```
8080 -supportProxyUser user1 -supportProxyPasswd password123 –
supportProxyProtocol http
```

5. Check the network connectivity from the Integrated ESRS client to the EMC servers:

   Format:
   ```
   /sys/support/esrsi checkNetwork
   ```

   Example:
   ```
   uemcli -u Local/joe -p MyPassword456! -sslPolicy accept /sys/
   support/esrsi checkNetwork
   ```

6. Request an access code for Integrated ESRS. This access code is emailed to the email account user. The access code is only valid for 30 minutes.

   Format:
   ```
   /sys/support/esrsi requestAccessCode
   ```

   Example:
   ```
   uemcli -u Local/joe -p MyPassword456! -sslPolicy accept /sys/
   support/esrsi requestAccessCode
   ```

7. Validate access code and review site information:

   Format:
   ```
   /sys/support/esrsi/site show -accessCode <value>
   ```

   Action qualifiers:

Qualifier	Description
-accessCode	Specifies the access code that was received by email from the IT service base.
	Note
	The access code must be provided in the command to execute this command.

   Example:
   ```
   uemcli -u Local/joe -p MyPassword456! /sys/support/esrsi/site
   show -accessCode 2216789 -detail
   ```

8. Select site ID and enable Integrated ESRS:

   Format:
   ```
   /sys/support/esrsi set -enable { yes | no } [ -siteId
   <value> ]
   ```

   Action qualifiers:

Qualifier	Description
-enable	Specifies whether to enable or disable the ESRS. Valid values are:
	• yes
	• no

Qualifier	Description
	Note If ESRS is disabled, other parameters cannot be changed.
-siteId	EMC id of site where the system is located. **Note** Use the **Request access code** action to get an access code sent to the registered email address.

Example:
```
uemcli -u Local/joe -p MyPassword456! -sslPolicy accept /sys/
support/esrsi set -enable yes -siteId 234
```

9. Optionally, configure the Policy Manager and policy proxy server attributes:

Format:
```
/sys/support/esrsi/policymgr set [ -enable { yes | no } ]
[ -address <value> ] [ -port <value> ] [ -protocol { http
| https } ] [ sslStrength { high | medium | low } ] [ -
enableProxy { yes | no } ] [ -proxyAddr <value> ] [ -
proxyPort <value> ] [ -proxyUser <value> { -proxyPasswd
<value> | -proxyPasswdSecure } ] [ -proxyProtocol { http |
socks } ]
```

Action qualifiers:

Qualifier	Description
-enable	Specifies whether to enable or disable the ESRS policy manager. Valid values are: • yes • no **Note** If the ESRS policy Manager is disabled, other policy manager parameters cannot be changed.
-address	Specifies the policy manager address to be configured for Integrated ESRS.
-port	Specifies the policy manager server port number to be configured for Integrated ESRS.
-protocol	Specifies the protocol to be used by the policy manager server.
-sslStrength	Specifies the ESRS Policy Manager SSL strength (applicable only when the protocol is HTTPS). Valid values are: • high

Qualifier	Description
	• medium • low
-enableProxy	Specifies to enable the policy manager proxy. Valid values are: • yes • no --- **Note** If the ESRS Policy Manager is disabled, other policy manager proxy server parameters cannot be changed.
-proxyAddr	Specifies the policy proxy server address.
-proxyPort	Specifies the policy proxy port number.
-proxyUser	Specifies the user name of the account on the policy manager proxy server.
-proxyPasswd	Specifies the password of the account on the policy manager proxy server.
-proxyProtocol	Specifies the protocol to be used by the policy manager proxy server.

Example:

```
uemcli -u Local/joe -p MyPassword456! -sslPolicy accept /sys/
support/esrsi/policymgr set -enable yes -address 10.0.0.2 -port
8080 -protocol http -sslStrength high -enableProxy yes -
proxyAddr 10.0.0.3 -proxyPort 8080 -proxyUser user2 -
proxyPasswdSecure -proxyProtocol http
```

CHAPTER 5

Troubleshooting

The service command `svc_esrs_ve` allows the user to perform basic tasks on ESRS VE, such as checking the status of the service and network or cleaning up the configuration. For more information, refer to the *EMC Unity™ Service Commands Technical Notes* document.

This chapter provides information about the probable causes of problems that you may encounter when enabling and running the ESRS feature and the recommended actions to take to resolve them.

Topics include:

ESRS cannot be enabled

When the ESRS feature cannot be enabled, review the following possible causes and actions you can take to resolve the problem.

Table 1 ESRS feature cannot be enabled problem resolution

Probable Cause	Recommended Action
You may have provided invalid login credentials or you have not upgraded to a Full-access support account. It can take up to 48 hours for your initial account with Full-access support credentials to be activated.	Check for the following: • The credentials you have specified match the credentials that were used to register the storage system on the EMC support website. • Your account information has been upgraded to a Full-access support account (registered user with access to the site where the installed storage system resides). **Note** You can determine whether your credentials are valid by logging in to the EMC Online Support website (https://Support.EMC.com). If you have not already registered your storage system, please register now. If you are still unable to access the website, send an email to support@emc.com
You may have provided valid login credentials but the credentials are not associated with your Site ID where the storage system is located. A Site ID is created in EMC support systems for each location within your organization where EMC products have been installed.	Verify your Site ID number is on the EMC Online Support website: 1. Log in to the EMC Online Support website with your credentials. 2. Select **Service Center**. 3. On the Service Center page, below the Sites and Contracts area, click **Administer a Site**. 4. Ensure that the site where the storage system is installed is listed in the My Sites area.

Table 1 ESRS feature cannot be enabled problem resolution (continued)

Probable Cause	Recommended Action
	Note You can also search for a site and add it to the My Sites list. If a site ID is not available or the correct site ID is not listed, you must notify your local field representative to request one. If a partner is doing the installation, the partner must submit the request to either the Install Base Group or to their field representative. If the Unity system is listed under the wrong site ID, refer to *KB 489840* for information on how to change the site ID that is associated with the system.

ESRS reported a connection issue

When the ESRS feature has become disconnected, review the following possible causes and actions you can take to resolve the problem.

Table 2 ESRS feature in disconnected state problem resolution

Probable Cause	Recommended Action
The Domain Name System (DNS) server is not running or does not exist.	Do the following: 1. Ensure that the DNS server set in Unisphere is entered correctly. 2. Enable SSH, log in as Service, and use the ping command to ensure that the storage system can ping the DNS server IP address. 3. Use the **Nslookup** tool on one of the ESRS hostnames to ensure that the DNS server can properly resolve it. If it cannot, or the DNS server cannot be pinged, contact your network administrator.
A Policy Manager is configured but is not reachable.	Check that the Policy Manager is online. From Unisphere, go to **Settings** > **Support Configuration** > **EMC Secure Remote Service** and verify that the Policy Manager protocol, port, and network name/IP address settings are configured correctly.
The ESRS connection is functional, but you cannot establish remote sessions. It is likely that the EMC Global Access Server (GAS) is not reachable. GAS servers are used for remote sessions only.	Do the following: • If the connection includes a customer proxy server, ensure the proxy server is reachable.

Table 2 ESRS feature in disconnected state problem resolution (continued)

Probable Cause	Recommended Action
	• Verify that the appropriate firewall hosts and ports (443 and 8443) are open to EMC.
A system configured with the ESRS centralized implementation has problems with HTTP keep-alive and does not appear to be connected.	Confirm that port 9443 is open to allow REST API calls from the storage system to the ESRS Gateway.