Secure Remote Services Requirements and Configuration

Version 5.x

Secure Remote Services Requirements and Configuration

P/N 302-002-573 Rev 07

June 2019

DELL EMC

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

CONTENTS

Preface 5

Chapter 1 Introduction 7
Benefits of ESRS 8
About remote service options 8
Operational description 10

Chapter 2 Requirements and Configuration 13
Prerequisites for ESRS 14
Requirements for Integrated ESRS 14
Requirements for Centralized ESRS 14
Dell EMC Online Support Full-access account 15
How to configure ESRS 16

Chapter 3 Configure Remote Support using Unisphere 19
Configure remote support 20
Configure Integrated ESRS (physical deployments only) 21

Chapter 4 Configure Remote Support using CLI 25
Overview of configuring Remote Support using the CLI 26
Configure or change support and proxy server settings 26
Configure or change the system contact information 28
Configure or change support credentials 29
Configure Centralized ESRS with the Unisphere CLI 29
Enable or change Centralized ESRS 29
Check Centralized ESRS network connection 30
Test Centralized ESRS 31
Configure Integrated ESRS with the Unisphere CLI 31
Check support credential readiness for integrated ESRS 32
Enable or change Integrated ESRS 32
Check Integrated ESRS network connection 33
Request access code for Integrated ESRS 33
Validate access code for Integrated ESRS 34
Test Integrated ESRS 34
Configure or change Policy Manager and proxy server settings 35

Chapter 5 Troubleshooting 37
ESRS cannot be enabled 38
Using RSA credentials to configure ESRS 39
ESRS reported a connection issue 39

Additional resources

As part of an improvement effort, revisions of the software and hardware are periodically released. 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 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.

Troubleshooting

For information about products, software updates, licensing, and service, go to 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 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 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

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 8
- About remote service options 8
- Operational description 10

Benefits of ESRS

The embedded ESRS feature in Unity deployments provides a highly secure, remote connection between your Unity environment and Dell 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 Dell EMC environment through the MyService360 dashboard.
- Remote delivery of Dell EMC's service and support.
- CloudIQ, a 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

Three remote service options are available by which to send storage system information to the Support Center for remote troubleshooting:

- Centralized ESRS
- Integrated ESRS (physical deployments only) with one of the following types of remote service connectivity options:
  - Outbound/Inbound
  - Outbound only

A fourth option, Disabled, is available but not recommended. If you select this option, the Support Center 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.

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 Support Center servers and an off-array ESRS Gateway. The ESRS Gateway is the single point of entry and exit for all IP-based ESRS 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 (optional) and proxy servers (optional), and the Support Center. 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. You can configure a Primary and a Secondary Gateway for ESRS for high availability in the event that one of the gateways is inaccessible. Both gateways must reside on the same cluster to minimize disruption if one gateway fails over to the other.

For more information about ESRS Gateway and Policy Manager, go to the ESRS 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. Also, ensure that port 443 is open (outbound) for network traffic.

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, you set up the storage system to use a secure connection between itself and the Support Center. You can select one of the following remote service connectivity options for Integrated ESRS:

- Outbound/Inbound, which is the default, from the storage system to the Support Center and from the Support Center to the storage system for remote access using https.
- Outbound only from the storage system to the Support Center using https.

When you select the Outbound/Inbound option, the storage system sets up a secure connection between itself and the Support Center. This option enables remote service connectivity capabilities for remote transfer to and remote transfer from the Support Center with the storage system. Configure the connection from the storage system to a Policy Manager (optional) and any associated proxy servers (optional) through either Unisphere or the CLI.

When you select the Outbound only option, the storage system sets up a secure connection between itself and the Support Center. This option enables remote service connectivity capability for remote transfer to the Support Center from the storage system.

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

1. Specify valid support credentials, otherwise, you cannot perform an ESRS readiness check or configure ESRS.
2. Run a readiness check (optional, but highly recommended).
3. If you skipped the readiness check, accept the license agreement for the feature.
4. Run the network check.
   Note: Several ports need to be allowed by your firewall/network setting for the network check and ESRS functionality. Ports 443 and 8443 are required for outbound connections while ports 80 and 443 are required for inbound connections. Also, if the settings that appear for the global proxy server need to be changed, edit the settings then run the network check.
5. For Outbound/Inbound remote service connectivity, you must specify the required customer contact data for the storage system if it has not been specified. This step is not applicable to Outbound only remote service connectivity.
6. Request an access code for verification through email (an extra level of authentication) and submit the access code for validation to continue the ESRS enabling process.
7. Check the status of the system's ESRS connection to the Support Center.
8. For Outbound/Inbound remote service connectivity, configure the Policy Manager (if an additional layer of security is required). The Policy Manager requires port 8090 (default) or the customer-specified port to be open for outgoing traffic. If it is configured to use SSL, port 8443 must be open.
9. Specify whether to send data to CloudIQ.

When Outbound only is the current ESRS configuration on the storage system, you can modify the proxy server information, if applicable, and change the remote service connectivity option to Outbound/Inbound. Changing the remote service connectivity option to Outbound/Inbound also

requires you to specify the customer contact data for the storage system if it has not been specified and, if required, to configure the Policy Manager.

When Outbound/Inbound is the current ESRS configuration on the storage system, you can modify the proxy server information, if applicable, and the contact and system information. However, you cannot change the remote service connectivity option from Outbound/Inbound to Outbound only, that change is not supported.

Operational description

The ESRS feature provides an IP-based connection that enables 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 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 Support can use the solution with confidence:

- All notifications 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 the Support Center are bilaterally authenticated using RSA® digital certificates
- Only authorized 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, which is only applicable to Integrated ESRS with Outbound/Inbound connectivity, enables you to grant or restrict Support 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, change the settings for the global proxy server, set up a Policy Manager (physical deployments only), 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 (applicable to Integrated ESRS with Outbound/Inbound connectivity) 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 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.

Centralized ESRS allows you to configure both a Primary gateway and a Secondary gateway to allow for high availability (HA) within the VE cluster on the network. If the primary gateway goes down, the Unity system will automatically fail over to the secondary gateway on the network for ESRS and Cloud IQ connectivity. Configuration of the primary gateway is mandatory, while configuration of the secondary gateway is optional.

Note: Once the Primary and Secondary gateway have been configured for Centralized ESRS, you cannot change the primary gateway to the secondary gateway. In order to do this, you must disable and then reenable Centralized ESRS with the appropriate gateway order.

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 Support Center back-end systems. If the proxy server is not available, ESRS attempts to bypass the proxy server and communicate directly to the Support Center back-end 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:

- Prerequisites for ESRS 14
- Requirements for Integrated ESRS 14
- Requirements for Centralized ESRS 14
- Dell EMC Online Support Full-access account 15
- How to configure ESRS 16

Prerequisites 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 Support Center (https://support.emc.com/) over the Internet using HTTPS (for non-proxy environments).
- Online Support Full-access account (requires specific credentials that are associated with the site ID, which is associated with the system serial number).
  Note: If there is a problem with your Online Support account, Support personnel can help you configure ESRS using their RSA credentials.
- Do not use dynamic IP addresses (DHCP) for any components of the ESRS Gateway servers, Policy Manager servers, or managed devices.
- Network traffic over port 443 is required for ESRS functionality and 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 those 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) to the Support Center. 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 your ESRS implementation will include a Policy Manager for more control over remote access to the storage system, you must indicate this when you configure the ESRS feature.
  Note: A Policy Manager is applicable only to Integrated ESRS with Outbound/Inbound connectivity.
- 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. Also, network traffic over port 443 is required for ESRS functionality.
- 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.

Dell EMC Online Support Full-access account

Configuring ESRS on a storage system requires an active Full-access account on the Dell 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.

During the ESRS readiness check, you may receive a message that your Support Credentials are not associated with a customer account. This may indicate that you need to upgrade from a Limited-access (Lite) account to a Full-access account. Refer to the steps below for more information on upgrading to a Full-access account. Otherwise, you may need to contact your service provider for issues with Support Credential registration.

Note: Full-access support is only provided to customers that have direct Online Support.

Creating an initial Online Support account

When you create an initial 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 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 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 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 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 Online Support web site, you must provide the following information:

Required Information	Description
Relationship with Dell EMC	Indicate whether your organization is a partner, supplier, or customer of Dell 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 Online Support system.

After you activate Full-access support privileges for your 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 by using any of the following means:

- 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**).
- ESRS—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 support credentials (user name and password associated with an active Online Support account with Full-access privileges) before you can configure ESRS.

- ESRS—Type of ESRS, Centralized or Integrated (Outbound/Inbound or Outbound only), 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.
- Network check (optional, settings only appear for Integrated ESRS)—Validates network readiness for ESRS configuration and, if applicable, used to edit the global proxy server information:
  - Protocol: Protocol used to communicate with a proxy server used for the communication channel. The available options are HTTP on port 3128 (default port) and SOCKS (the protocol default) on port 1080 (default port).
    Note: Selecting either SOCKS or HTTP automatically adds the associated default port to the proxy sever address. If necessary, a different port can be specified through Unisphere, or UEMCLI or REST commands.
  - Proxy server address: Network address to associate with the global proxy server traffic.
    Note: Changing the protocol selection after specifying an IP address automatically changes the appended port to the default for the protocol unless a port other than the default has been specified either through UEMCLI or REST commands.
  - Credentials: User name and password of an account used to access the proxy server system.
- Contact and System Location information (settings only appear for Integrated ESRS Outbound/Inbound)—Information that can be edited and that Support will use to respond to your support issues.

- Email verification—Request for access code and subsequent authentication of email address.
- Policy manager information (optional, settings only appear for Integrated ESRS Outbound/Inbound)—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, settings only appear for Integrated ESRS Outbound/Inbound)—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.
- Send data to CloudIQ (The check box appears for Integrated ESRS only and is selected (enabled) by default. Clear the check box to disable sending data to CloudIQ (not recommended).)—CloudIQ is a software-as-a-service cloud management dashboard used to provide intelligent analytics about performance, capacity, and configuration for health-based reporting and remediation.

  Note: CloudIQ is enabled by default when Centralized ESRS is enabled. To disable or re-enable CloudIQ for Centralized ESRS, in Unisphere, go to **Settings** > **Support Configuration** > **CloudIQ**.

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 Outbound/Inbound 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 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 20
- Configure Integrated ESRS (physical deployments only) 21

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.

About this task

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 **Support Credentials** to specify your support credentials, Username, and Password. Otherwise, go to the next step.

   If you do not specify valid Support Credentials, you cannot view support contract information, or navigate to Online Support product pages.
3. Select **EMC Secure Remote Services**.

   It is recommended to run a readiness check before configuring ESRS to determine whether ESRS can be configured. To bypass the readiness check, simply click **Configure** and go to step 6.
4. Click **Readiness Check**.
5. In **ESRS Readiness Check**, select the ESRS option you prefer to use.

Option	Description
Integrated (physical deployments only)	Before the readiness check runs, the ESRS end user license agreement (ESRS EULA) must be accepted. After the license agreement is accepted, click **Next** to run the check. **Note:** After the license agreement is accepted, it does not appear again.
Centralized	Before the readiness check runs, the minimal required software version of the gateway server appears and the Gateway Network Address must be supplied. After the Gateway Network Address is typed, click **Next** to run the check.

   After the readiness check runs, one of the following occurs:

   - If no errors are found, a green circle with a check mark and a success message appears. Either click **Configure ESRS** and go to step 6 to continue configuring ESRS or click **Close** to return to **Settings** for ESRS and continue with the configuration at a later time.
   - If errors appear, either resolve any issues and click **Check Again** to ensure ESRS can be configured or click **Close** and resolve issues at a later time.
6. In **Configure ESRS**, specify the appropriate ESRS option information.

Option	Description
Centralized—Monitor with a Centralized ESRS configuration	a. Specify the **Primary Gateway Network Address** of the ESRS Gateway server that is used to connect to the EMC enterprise and

Option	Description
	ensure that port 9443 is open between the Gateway server and the storage system. **Note:** RSA credentials can be used for Primary Gateway configurations without a customer support account. This allows the configuration of Centralized ESRS while support account credentials are being created and validated on the backend. b. Optionally enter a **Secondary Gateway Network Address** for ESRS High Availability (HA). The second gateway must be configured in the same ESRS HA cluster as the **Primary Gateway Network Address**. **Note:** If RSA credentials were used for the primary gateway, they must also be provided to complete the configuration of a secondary gateway. **Note:** CloudIQ is enabled by default when Centralized ESRS is enabled. To disable or re-enable CloudIQ for Centralized ESRS, in Unisphere, go to **Settings** > **Support Configuration** > **CloudIQ**.
Integrated—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. You can select whether to have Outgoing only or Outbound/Inbound connectivity with your remote service provider and whether to send data to CloudIQ. Use of the Policy Manager and proxy servers is optional and only applicable when you select Integrated ESRS with Outbound/Inbound connectivity. Once selected, you can configure a Policy Manager and Proxy Server settings. **Note:** (The ESRS EULA does not appear after it is accepted as part of the readiness check process.)
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 the EMC enterprise 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.

Note: If the Status remains 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.

About this task

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.

   Note: If the license agreement was accepted during running of the Readiness check before you configure ESRS, the license agreement does not appear again.

2. Run a Network check. If a proxy server has been configured for the storage system, you can make changes, if necessary, by clicking the pencil icon beside **Connect Through a Proxy Server** and filling in the appropriate information in the dialog box that appears.

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

   When you submit the Network Check page and the server details have been entered, network tests are performed to check connectivity between the device and the core node. If you selected Integrated ESRS with Outbound/Inbound connectivity, the back-end Global Access Servers (GAS) are also included in the network tests. The network connectivity from ESRS to all the required back-end servers is checked. If the tests are unsuccessful, which means the device is unable to connect to some or all of the back-end 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 the back-end servers. All tests must be successful. You are responsible for resolution of proxy server and firewall issues that impact connectivity to the ESRS infrastructure.

3. Verify the Customer Contact Data information. (This verification only appears and is applicable when you have selected Integrated ESRS with Outbound/Inbound connectivity.)

   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. Support will use this information to respond to your support issues.

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.

      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 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 or a problem with the support account setup, Support personnel can select **Alternative for Support personnel only** and enter their RSA credentials, in which case the email verification process is skipped.

      If RSA support credentials are used, second pop-up window will display requiring Support personnel to re-enter the RSA support credentials.

5. (Optional, only applicable when you have selected Integrated ESRS.) If your storage system will use a Policy Manager to set authorization permissions, select **Policy Manager** and fill in the appropriate information for the Policy Manager. 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. If you will not be using a Policy Manager, go to step 6.

   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.

6. The **Send data to CloudIQ** check box is selected (enabled) by default. Clear the check box to disable sending data to CloudIQ (not recommended).

   CloudIQ can be enabled or disabled after completing ESRS configuration from **Settings** > **Support Configuration** > **CloudIQ**.

   Once ESRS is successfully configured, the relevant certificates are installed, ESRS is provisioned and registered on the Support Center, and the **Results** page appears.

7. 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**

Note: If the Status appears to remain as Transitioning and does not change after 20 minutes (the time it should take to test connectivity), contact 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.

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

- For Integrated ESRS with Outbound only connectivity:
  - If a proxy server has been configured for the storage system, you can make changes, if necessary, by clicking the pencil icon beside **Connect Through a Proxy Server** and filling in the appropriate information in the dialog box that appears.
  - You can change the ESRS type to either Integrated (Outbound/Inbound) or Centralized and specify the applicable information.
- For Integrated ESRS with Outbound/Inbound connectivity:
  - If a proxy server has been configured for the storage system, you can make changes, if necessary, by clicking the pencil icon beside **Connect Through a Proxy Server** and filling in the appropriate information in the dialog box that appears.
  - The **Verify Contact Information and System Location** information panel in the ESRS wizard is enabled with an edit option (pencil icon) beside both **Contact Information** and **System information**. System information can be updated with the exception of the Site ID number.
  - You can change the ESRS type from Integrated (Outbound/Inbound) to Centralized and specify the applicable information.

    Note: Once Integrated ESRS is configured for Inbound/Outbound connectivity, it cannot be changed back to Outbound-only connectivity.

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:

- Overview of configuring Remote Support using the CLI 26
- Configure or change support and proxy server settings 26
- Configure or change the system contact information 28
- Configure or change support credentials 29
- Configure Centralized ESRS with the Unisphere CLI 29
- Configure Integrated ESRS with the Unisphere CLI 31
- Configure or change Policy Manager and proxy server settings 35

Overview of configuring Remote Support using the CLI

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

Before you begin

This topic provides an overview of the chronological steps required for configuring ESRS using the CLI. Refer to the subsequent sections of this chapter for the detailed command usage and examples for each of these steps.

Procedure

1. Optionally, configure the use of a proxy server with the `/sys/support/config set` command.
2. Set the Customer Contact Data Information using the `/sys/info set` command.
3. Set your support account credentials using the `sys/support/account set` command.
4. Enable and configure the type of ESRS you want to use:
    a. For Centralized ESRS:
        a. Enable ESRS and configure settings using the `/sys/support/esrsc set` command.
        b. Check the network connectivity from the primary or secondary Centralized ESRS gateway to the Dell EMC servers using the `/sys/support/esrsc checkNetwork` command.
        c. After Centralized ESRS is enabled, test the configuration by sending a test Call Home to Dell EMC using the `/sys/support/esrsc test`command.

    b. For Integrated ESRS:
        a. Check that the support account associated with your system is configured and ready for ESRS connectivity using the `/sys/support/esrsi checkSupportAccountReadiness` command.
        b. Check the network connectivity from the Integrated ESRS client to the Dell EMC servers using the `/sys/support/esrsi checkNetwork` command.
        c. Enable ESRS and configure settings using the `/sys/support/esrsi set` command. This command allows you to accept the EULA and select the type of Integrated ESRS--one-way or two-way.
        d. Optionally request an access code to be sent to the email account user using the `/sys/support/esrsi requestAccessCode` command.
        Note: The access code is for additional verification purposes and expires after 30 minutes.
        e. If you requested an access code, validate the access code you received using the `/sys/support/esrsi validateAccessCode -accessCode` command.
        f. Test the ESRS configuration using the `/sys/support/esrsi test`command.
5. Optionally, configure the Policy Manager and policy proxy server attributes using the `/sys/support/esrsi/policymgr set` command.

Configure or change support and proxy server settings

Change support configuration attributes.

Format

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

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.
-autoUpdateContracts	Specify whether the system automatically updates its service contracts list once a week. Valid values are: • yes • no **Note:** Values are case-sensitive.
-enableCloudMgmt	Specify whether sending data to CloudIQ is enabled on the system. Valid values are: • yes • no **Note:** Values are case-sensitive.

Example

The following command specifies the support services proxy server parameters:

```
uemcli /sys/support/config set -supportProxyAddr 10.0.0.1 -supportProxyPort 8080
-supportProxyUser user1 -supportProxyPasswd password123 -supportProxyProtocol
http
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Configure or change the system contact information

Enter or change the system and contact information attributes.

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.
-contactLastName	Specify the new contact last name for the system.

Example

The following command changes the following system information:

- Contact first name
- Contact last name
- Contact email
- Contact phone
- System location
- Contact mobile phone

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/info set -
contactFirstName Zach -contactLastName Arnold -contactEmail
something@someemail.com -contactPhone 1233456789 -location here -
contactMobilePhone 987654321
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection
Operation completed successfully.
```

Configure or change support credentials

Configure or change the support account credential attributes associated with your system.

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

The following command specifies the new password of the support account:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/account set -user
user1 -passwd Password123
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Configure Centralized ESRS with the Unisphere CLI

The following sections describe how to configure and test Centralized ESRS using the CLI.

Enable or change Centralized ESRS

Enable or change the Centralized ESRS configuration.

Format

```
/sys/support/esrsc set -enable { yes | no } [ -address <value> ] [ -port
<value>] [-secondAddress <value>] [-secondPort <value>]
```

Action qualifiers

Qualifier	Description
-enable	Specifies whether to enable or disable Centralized ESRS. Valid values are: • yes • no **Note:** If ESRS is disabled, other parameters cannot be changed.
-address	Specifies the IP address of the Centralized ESRS VE server to which to be connected.

Qualifier	Description
-port	Specifies the port number to be used to connect to the centralized ESRS.
-secondAddress	Specify the network name or IP address of the secondary Centralized ESRS VE server.
-secondPort	Specify the port number to be used to connect to the primary Centralized ESRS VE server. **Note:** The secondary gateway should be in the same cluster as the primary gateway.

Example 1

The following command specifies the Centralized ESRS parameters:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc set -enable
yes -address 10.10.22.22
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Example 2

The following example configures Centralized ESRS VE with a secondary gateway for high availability.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc set -enable
yes -address 10.10.22.22 -secondAddress 10.10.22.32
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Check Centralized ESRS network connection

Check Centralized ESRS network connectivity before configuring ESRS.

Check the network connectivity from Centralized ESRS to the Dell EMC servers. If there is any failure, Centralized ESRS cannot be enabled.

Format

```
/sys/support/esrsc checkNetwork -address <value> [-port <value>]
```

Action qualifier

Qualifier	Description
-address	Type the IP address of Centralized ESRS VE.
-port	Type the port number used for Centralized ESRS VE.

Example

This example shows when the network connectivity check for Centralized ESRS fails.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc
checkNetwork -address 10.100.10.7
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation failed. Error code: 0x6400be8

The centralized ESRS network connectivity check failed. Please check your
firewall configuration and whether the centralized ESRS server is operating
normally. (Error Code:0x6400be8)
```

Test Centralized ESRS

Once Centralized ESRS is already configured, you can use this command to test the connection between your system and the ESRS database. While the `checkNetwork` command will check your local network connectivity, this `test` command will check the connection back to Dell EMC.

Format

```
/sys/support/esrsc test
```

Example 1

The following example shows the results of running this command when Centralized ESRS is not yet configured.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc test
```

```
Operation failed. Error code: 0x6400c06
 Not supported since Centralized Secure Remote Support is not enabled. (Error
Code:0x6400c06)
```

Example 2

The following example shows when this command is run successfully.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsc test
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Note: A successful operation indicates that the test was executed successfully, not that the connection itself was successful. In other words, it indicates a Call Home was sent, but does not indicate whether it was received by the ESRS server. To check the status of the actual test, log into Service 360 to view recent Service Requests (SRs). If the call home was received by the ESRS server, the connection test will appear as an automatically-closed Call Home SR.

Configure Integrated ESRS with the Unisphere CLI

The following sections describe how to configure and test Integrated ESRS using the CLI.

Check support credential readiness for integrated ESRS

Before configuring ESRS, check that the support account credentials configured for your system are properly registered in the Online Support database.

Format

```
/sys/support/esrsi checkSupportAccountReadiness
```

Example

The following example shows that the command run successfully, where support credentials are properly configured.

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi checkSupportAccountReadiness

```
Storage system address: 10.0.0.1
Storage system port: 443
HTPS connection

Operation completed successfully.
```

Enable or change Integrated ESRS

Enable or change the Integrated ESRS configuration.

Format

```
/sys/support/esrsi set {-enable {yes|no}|-acceptEula yes|-type {oneWay|twoWay}}
```

Action qualifiers

Qualifier	Description
`-enable`	Specifies whether to enable or re-enable, or disable the ESRS. Valid values are: • `yes` • `no` **Note:** If ESRS is disabled, other parameters cannot be changed.
`-acceptEula`	Specifies whether to accept the end user license. Valid value is: • `yes` **Note:** If ESRS EULA is not accepted, nothing can be configured for the Integrated ESRS.
`-type`	Specifies which type of Integrated ESRS to use. Valid values are: • `oneWay` (Outbound only) • `twoWay` (Outbound/Inbound) (default)

Example

The following command enables Integrated ESRS, accepts the EULA, and sets the type of Integrated ESRS:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi set -enable yes -acceptEula yes -type oneWay

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Check Integrated ESRS network connection

Check the network connectivity from the Integrated ESRS client to the EMC servers. If there is any failure, the Integrated ESRS cannot be enabled.

Format

```
/sys/support/esrsi checkNetwork
```

Example

The following command displays the network connectivity for Integrated ESRS:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi checkNetwork

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation failed. Error code: 0x6400bc8
 Remote Support cannot be enabled at this time, because the system cannot
contact some required EMC servers:
esrghoprd02.emc.com:443/8443,esrghoprd03.emc.com:8443/443. Please refer to
online help for this error code to resolve the issue. (Error Code:0x6400bc8)
```

Request access code for Integrated ESRS

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

Format

```
/sys/support/esrsi requestAccessCode
```

Example

The following command sends a request for an access code as part of the email verification process for Integrated ESRS:

uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi requestAccessCode

```
Storage system address: 10.0.0.1
Storage system port: 443
HTPS connection

1:     Recipient email address = sxxxxxxxxxx@mail.com
```

Validate access code for Integrated ESRS

Validate the access code for Integrated ESRS that was received by email to the email account user. The received access code will only be valid for 30 minutes.

Format

```
/sys/support/esrsi validateAccessCode -accessCode <value>
```

Example

The following command displays the response to validating the access code part of the email verification process:

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi
validateAccessCode -accessCode 76507252
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTPS connection

Operation completed successfully.
```

Test Integrated ESRS

Once Integrated ESRS is already configured, you can use this command to test the connection between your system and the ESRS database. While the `checkNetwork` command will check your local network connectivity, this `test` command will check the connection back to Dell EMC.

Format

```
/sys/support/esrsi test
```

Example 1

The following example shows the results of running this command when Integrated ESRS is not yet configured.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi test
```

```
Operation failed. Error code: 0x6400bad
 Not supported since Integrated Secure Remote Support is not enabled. (Error
Code:0x6400bad)
```

Example 2

The following example shows when this command can be executed successfully.

```
uemcli -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi test
```

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

Note: A successful operation indicates that the test was executed successfully, not that the connection itself was successful. In other words, it indicates a Call Home was sent, but does not indicate whether it was received by the ESRS server. To check the status of the actual test, log into Service 360 to view recent Service Requests (SRs). If the call home was

received by the ESRS server, the connection test will appear as an automatically-closed Call Home SR.

Configure or change Policy Manager and proxy server settings

Configure or change the Policy Manager and 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` • `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 -d 10.0.0.1 -u Local/joe -p MyPassword456! /sys/support/esrsi/policymgr set -enable no

```
Storage system address: 10.0.0.1
Storage system port: 443
HTTPS connection

Operation completed successfully.
```

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 *Dell 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 38
- ESRS reported a connection issue 39

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 Online Support. • 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 Online Support (https://Support.EMC.com). If you have not already registered your storage system, please register now. If you are still unable to access the site, 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 Support systems for each location within your organization where EMC products have been installed.	Verify your Site ID number is on Online Support: 1. Log in to Online Support 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. **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

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

Probable Cause	Recommended Action
	the site ID that is associated with the system.

Using RSA credentials to configure ESRS

There are some cases where your customer support credentials have not been completely set up or validated on the backend support servers. In 4.x releases, this prevented configuration of ESRS. While on site or through a remote conference call, support personnel can enter their RSA credentials to bypass the requirement of a fully configured customer support account.

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 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. • Verify that the appropriate firewall hosts and ports (443 and 8443) are open to EMC.

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

Probable Cause	Recommended Action
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.