DELL Technologies

DELL UNITY IMPLEMENTATION AND ADMINISTRATION

MODULE 1

PARTICIPANT GUIDE

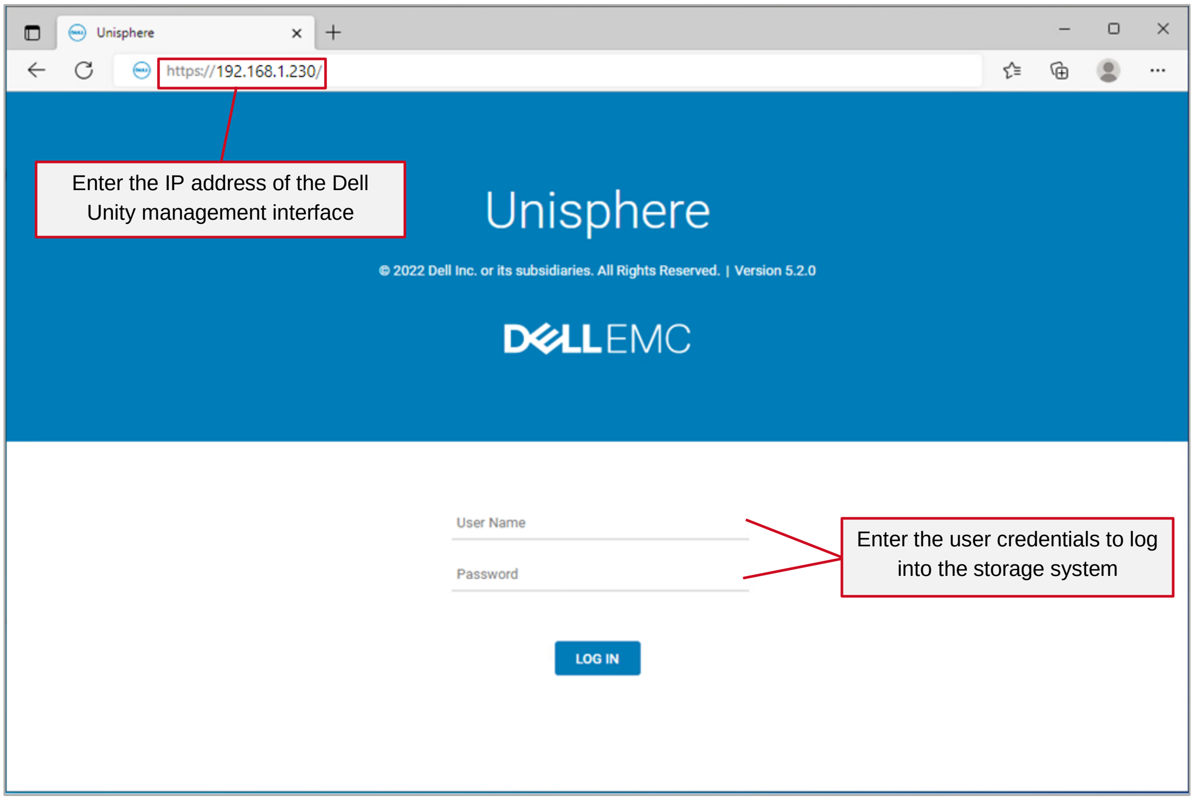
Table of Contents

System Administration

User Interfaces and Access Control

Administrative User Interfaces - Unisphere

Overview


Unisphere
https://192.168.1.230/
Unisphere
© 2022 Dell Inc. or its subsidiaries. All Rights Reserved. | Version 5.2.0
DELL EMC
User Name
Password
LOG IN

Enter the IP address of the Dell Unity management interface

Enter the user credentials to log into the storage system

Unisphere login

The Unisphere user interface is a web-based software that is built on the HTML5 technology with support on a wide range of browsers[1].

Unisphere enables the configuration, and management of a single Dell Unity storage system (physical models or UnityVSA) from one single interface.

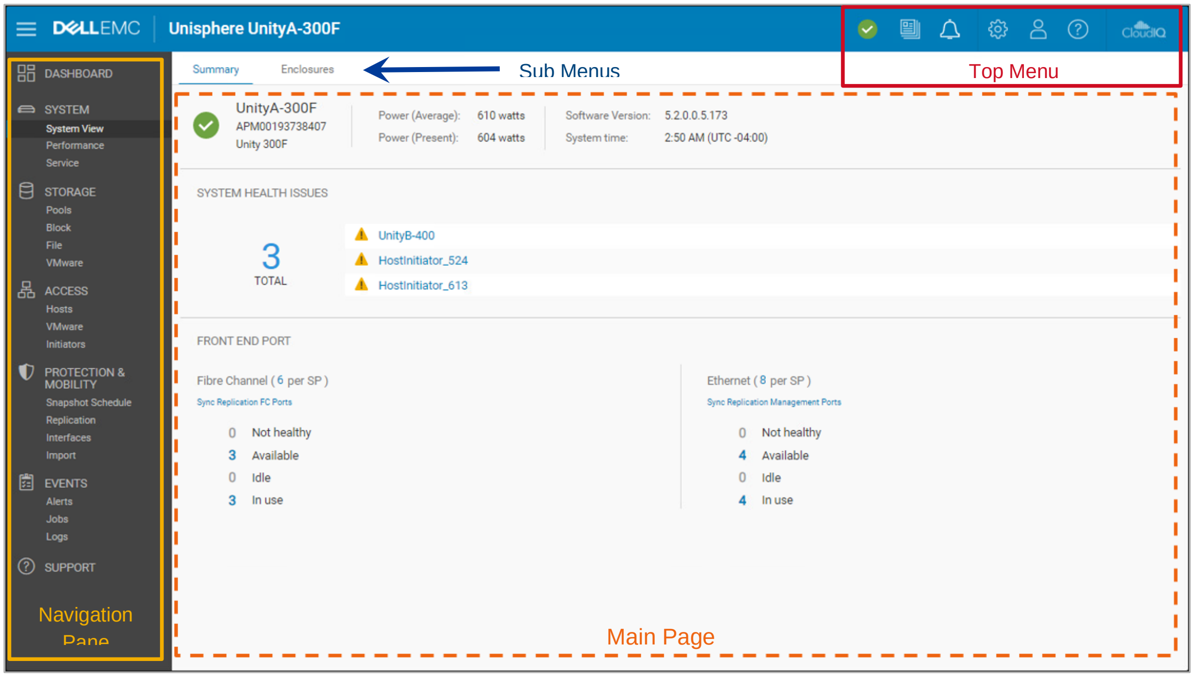
[1] The supported browsers are: Google Chrome v33 or later, Microsoft Edge, Mozilla Firefox v28 or later, and Apple Safari v6 or later.

The interface provides an overall view of what is happening in the environment plus an intuitive way to manage the storage array.

Launch Unisphere by entering the IP address of the storage system management port in the URL address of a supported web browser.

Provide the user and password to log into the system.

Interface Navigation



UnityA-300F
APM00193738407
Unity 300F

Power (Average): 610 watts
Power (Present): 604 watts

Software Version: 5.2.0.0.5.173
System time: 2:50 AM (UTC -04:00)

SYSTEM HEALTH ISSUES

3 TOTAL

- UnityB-400
- HostInitiator_524
- HostInitiator_613

FRONT END PORT

Fibre Channel (6 per SP)
Sync Replication FC Ports

0	Not healthy
3	Available
0	Idle
3	In use

Ethernet (8 per SP)
Sync Replication Management Ports

0	Not healthy
4	Available
0	Idle
4	In use

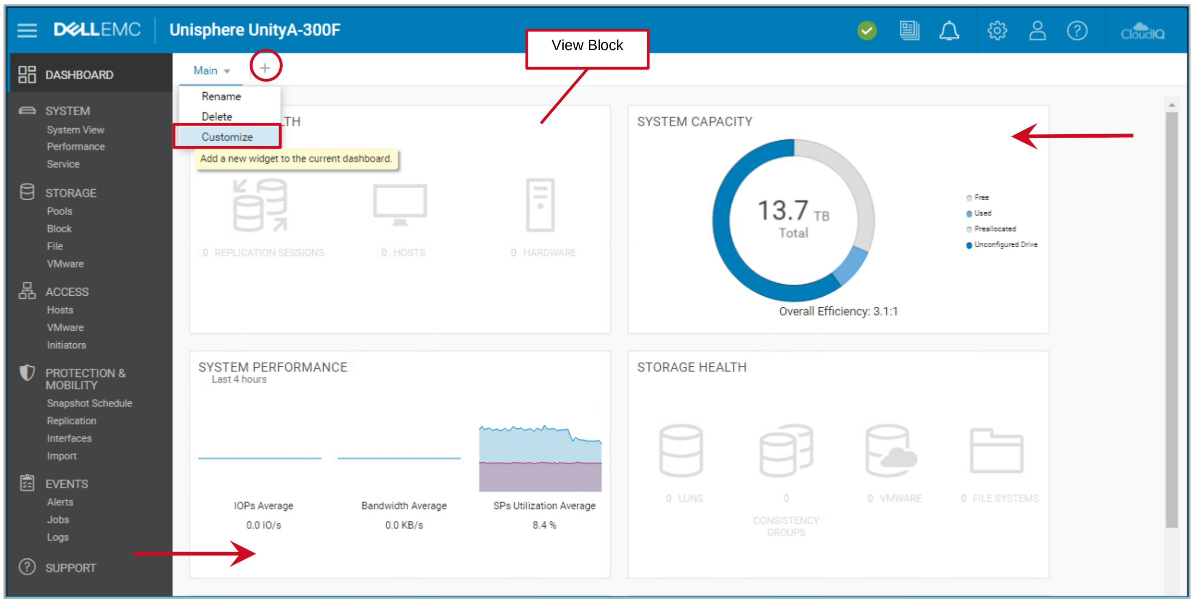
Unisphere interface showing the System View content page

The Unisphere interface has four main areas which are used for navigation and visualization of the content:

- The **Navigation Pane** has the Unisphere options for storage provisioning, host access, data protection and mobility, system operation monitoring, and support.
- The **Main Page** is where the pertinent information about options from the navigation pane and a particular submenu is displayed. The page also shows the available actions that can be performed for the selected object.

- The **Top Menu** has links for system alarms, job notifications, help menu, the Unisphere preferences, global system settings, and the CloudIQ.
- The **Sub Menus** provide various tabs, links, and more options for the selected item from the navigation pane.

Dashboard



Add a new widget to the current dashboard.

View Block

Unisphere Dashboard with menu and submenu options, and view blocks

The Unisphere main dashboard provides a quick view of the system health and storage health status.

A storage administrator can configure new dashboards by selecting **Add** and providing a name.

The customized dashboards can be renamed and deleted using the dashboard submenu.

Dashboard view blocks provide a summary of system storage usage, system alerts, and storage resources health status. The view blocks can be added to a dashboard, renamed or removed.

To add view blocks, open the selected dashboard submenu and select Customize.

Administrative User Interfaces - Unisphere CLI or UEMCLI

Overview

The Unisphere CLI or UEMCLI enables a storage administrator to script some of the most commonly performed tasks in the Dell Unity storage system.

Unisphere CLI enables you to run commands on a Dell Unity storage system from a host with the Unisphere CLI client installed.

- Unisphere CLI supports provisioning and management of network block and file-based storage.
- The Unisphere CLI client can be downloaded from the online support website and installed on a Microsoft Windows or UNIX/Linux computer.

The application is intended for advanced users who want to use commands in scripts for automating routine tasks.

The routine tasks include:

- Configuring and monitoring the system
- Managing users
- Provisioning storage
- Protecting data
- Controlling host access to storage

Command Syntax

The command syntax begins with the executable uemcli, using switches and qualifiers as described here.

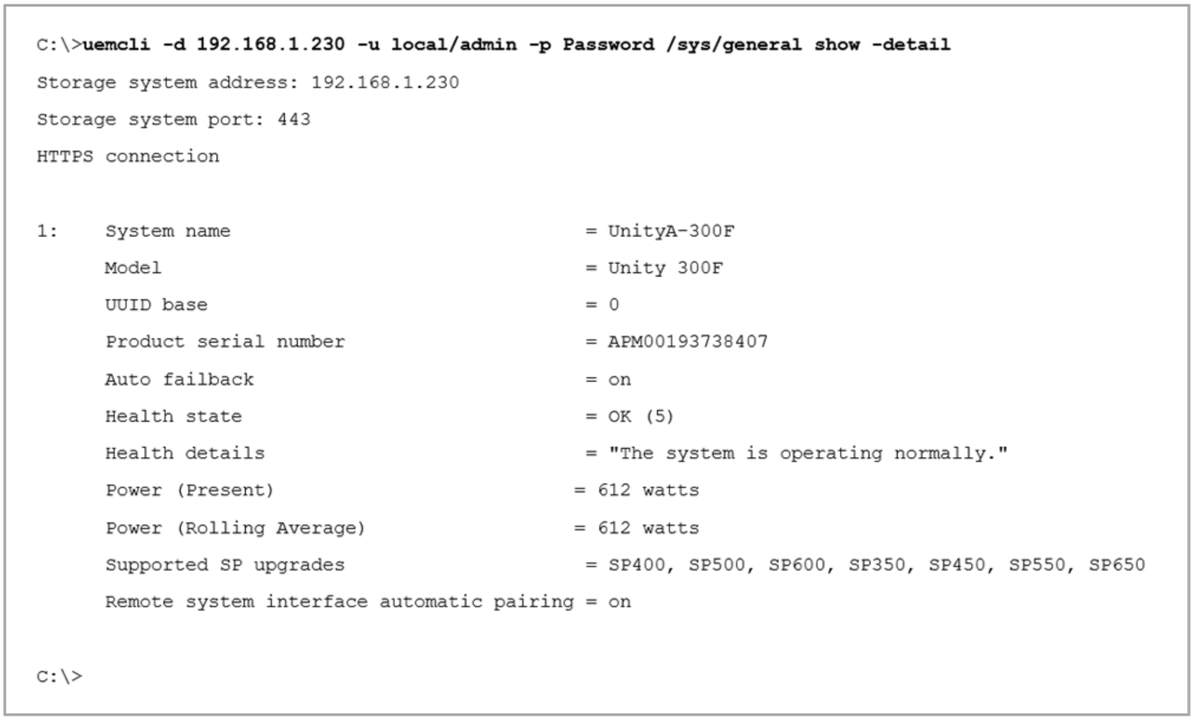
```
uemcli [<switches>] <object path> [<object qualifier>]
<action> [<action qualifiers>]
```

Where:

- **Switches:** Used to access a system, upload files to the system, and manage security certificates.

- **Object:** Type of object on which to perform an action, such as a user, host, LDAP setting.
- **Object qualifier**: Unique identifiers for objects in the system. The format is `–<identifier> <value>`.
- **Action**: Operations that are performed on an object or object type. Examples of actions are **`create`** and ***`set`***.
- **Action qualifier**: Parameters specific to actions. Examples of action qualifiers are `-passwd` and `-role`.

Example



```
C:\>uemcli -d 192.168.1.230 -u local/admin -p Password /sys/general show -detail
Storage system address: 192.168.1.230
Storage system port: 443
HTTPS connection

1:    System name                              = UnityA-300F
      Model                                    = Unity 300F
      UUID base                                = 0
      Product serial number                    = APM00193738407
      Auto failback                            = on
      Health state                             = OK (5)
      Health details                           = "The system is operating normally."
      Power (Present)                         = 612 watts
      Power (Rolling Average)                 = 612 watts
      Supported SP upgrades                    = SP400, SP500, SP600, SP350, SP450, SP550, SP650
      Remote system interface automatic pairing = on

C:\>
```

Example of an UEMCLI command output

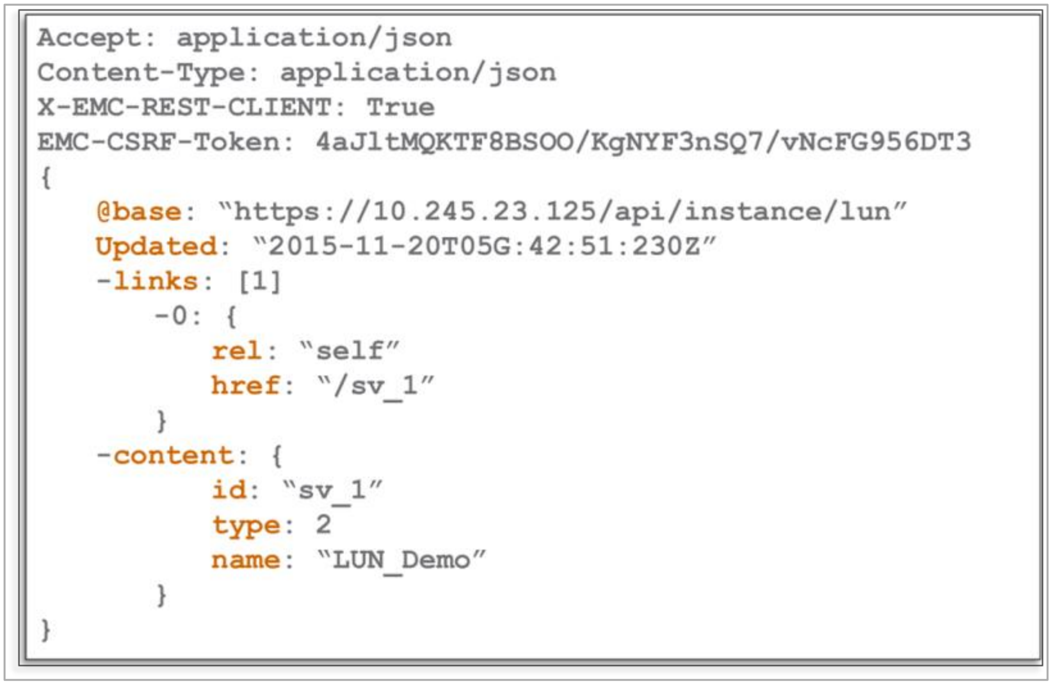
In the example, the Unisphere CLI command displays the general settings for a physical Unity storage system.

- Access a Dell Unity 300F system using the management port with IP address 192.168.1.230.
  - The first time a Unity system is accessed the command displays the system certificate. (Not shown here.)

  - The storage administrator has the choice to accept it only for the session or accept and store it for all sessions.
- Log into the system with the provided local admin user credentials.
- Retrieves the array's general settings and outputs its details on the screen.

Administrative User Interfaces - REST API

REST API is a set of resources, operations, and attributes that interact with the Unisphere management functionality.



```
Accept: application/json
Content-Type: application/json
X-EMC-REST-CLIENT: True
EMC-CSRF-Token: 4aJ1tMQKTF8BSOO/KgNYF3nSQ7/vNcFG956DT3
{
   @base: “https://10.245.23.125/api/instance/lun”
   Updated: “2015-11-20T05G:42:51:230Z”
   -links: [1]
      -0: {
         rel: “self”
         href: “/sv_1”
      }
   -content: {
         id: “sv_1”
         type: 2
         name: “LUN_Demo”
      }
}
```

Example of REST API script

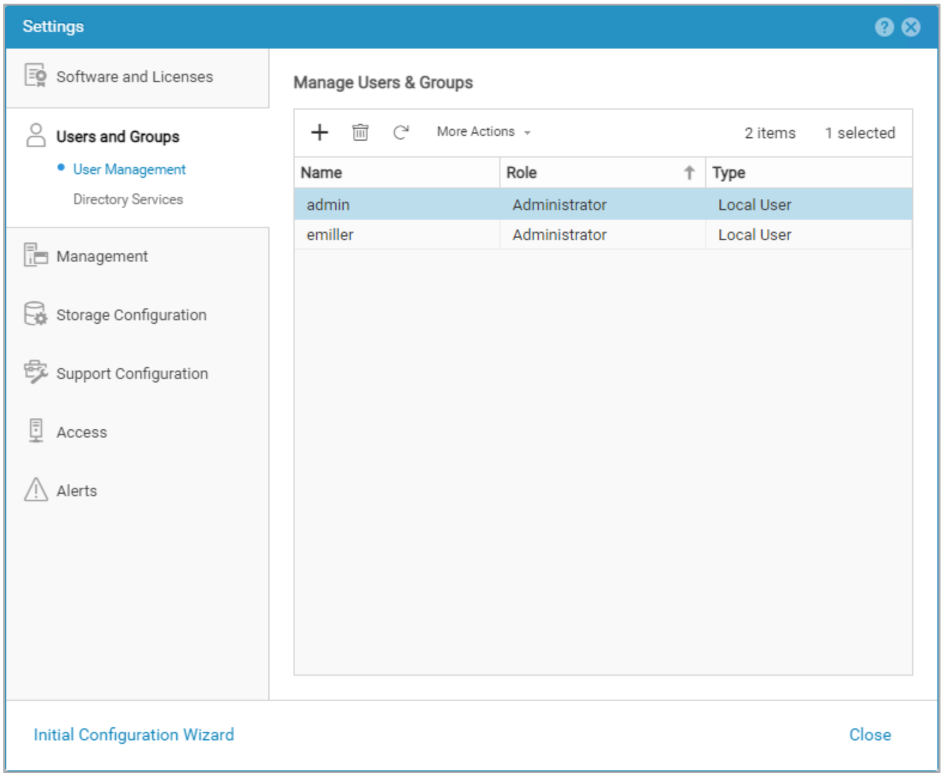
A storage administrator can perform some automated routines on the array using web browsers, and programming and scripting languages.

Deep Dive: For more details, read the **Unisphere Management REST API Programmer’s Guide** available on the online support website.

Access Control - User Authentication

There are two user authentication scopes for Dell Unity storage systems: **Local User Accounts** or **Domain-mapped User Accounts**.

Local User Account



Name	Role	Type
admin	Administrator	Local User
emiller	Administrator	Local User

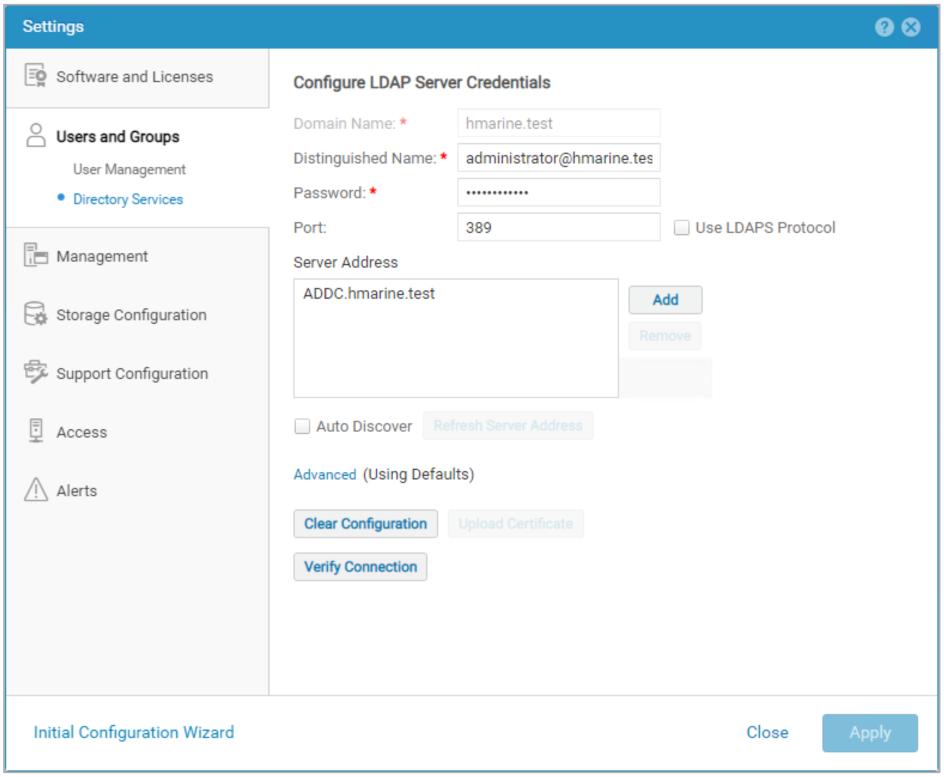
Local Users Management in Unisphere

Storage administrator can create local user accounts through the **User Management** section of the Unisphere UI Settings window.

These user accounts are associated with distinct roles. Each account provide a user name and password authentication only for the system on which they were created.

User accounts do not enable the management of multiple systems unless identical credentials are created on each system.

LDAP



Configure LDAP Server Credentials

Domain Name: * hmarine.test

Distinguished Name: * administrator@hmarine.tes

Password: * ••••••••••••

Port: 389 □ Use LDAPS Protocol

Server Address

ADDC.hmarine.test

□ Auto Discover

Advanced (Using Defaults)

Configuration of LDAP Server access In Unisphere Settings

With the domain-mapped user accounts method, access to a Lightweight Directory Access Protocol (LDAP) domain must be configured in the Directory Services.

Once the configuration is set, a storage administrator can create LDAP users or LDAP Groups in the **User Management** section of the Unisphere Settings window.

These accounts use the user name and password that is specified on an LDAP domain server. Integrating the system into an existing LDAP environment provides a way to control user and user group access to the system through Unisphere CLI or Unisphere.

The concept of a storage domain does not exist for Dell Unity systems. There is no Global authentication scope.

The user authentication and system management operations are performed over the network using industry standard protocols.

- Secure Socket Layer (SSL)
- Secure Shell (SSH)

Access Control - Default User Accounts

Dell Unity storage systems have factory default **management** and **service** user accounts. Use these accounts when initially accessing and configuring Unity.

These accounts can access both Unisphere and Unisphere CLI interfaces but have distinct privileges of operations they can perform.

During the initial configuration process, it is mandatory to change the passwords for the default admin and service accounts.

Account Type	Username	Password	Privileges
Management	admin	Password123#	Perform management and monitoring tasks that are associated with the storage system and its storage resources. Depending on the role type, these accounts have administrator privileges for resetting default passwords, configuring system settings, creating user accounts, and allocating storage.
Service	service	service	Perform specialized service operations such as collecting system service information, restarting management software, resetting the system to factory defaults, and so on. You cannot create or delete storage system service accounts. You can reset the service account password from Unisphere.

Tip: You can reset the storage system factory default account passwords by pressing the password reset button on the storage system chassis. Read the **Unisphere Online Help** and the **Hardware Information Guide** for more information.

Access Control - Role-Based Administration

For environments with more than one person managing the Unity system, multiple unique administrative accounts can be created.

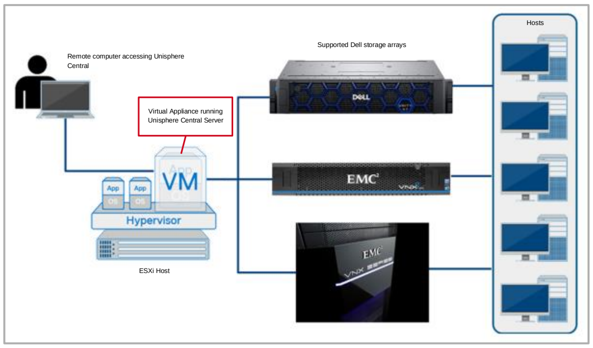
- Different roles can be defined for those accounts to distribute administrative tasks between users.
- Unisphere accounts combine a unique user name and password with a specific role for each identity.
- The specified role determines the types of actions that the user can perform after login.

This table describes each of the supported Dell Unity management user roles.

Management Role	Allowed Operations
Administrator (default)	Full administrative privileges for storage configuration and operations. • Perform the system initial configuration, edit system settings, and manage user accounts. • Create, modify, and delete storage resources, and upgrade system software.
Storage Administrator	View the storage system data, edit the Unisphere settings, use the Unisphere tools, and create, modify, and delete storage resources.
Security Administrator	Operator privileges for storage operations plus full security privileges for managing the Dell Unity user accounts.
Operator	View Unisphere system and storage status information.
VM Administrator	View and monitor basic storage components of the Dell Unity storage system through vCenter with VASA.

Centralized Management - Unisphere Central

Overview


Hosts
Supported Dell storage arrays
Remote computer accessing Unisphere Central
Virtual Appliance running Unisphere Central Server
VM
App
OS
Hypervisor
ESXi Host
DELL
EMC²
VNX
EMC
VNX

Unisphere Central theory of operations

Storage administrators can monitor Dell Unity systems (physical models and UnityVSA) using **Unisphere Central**.

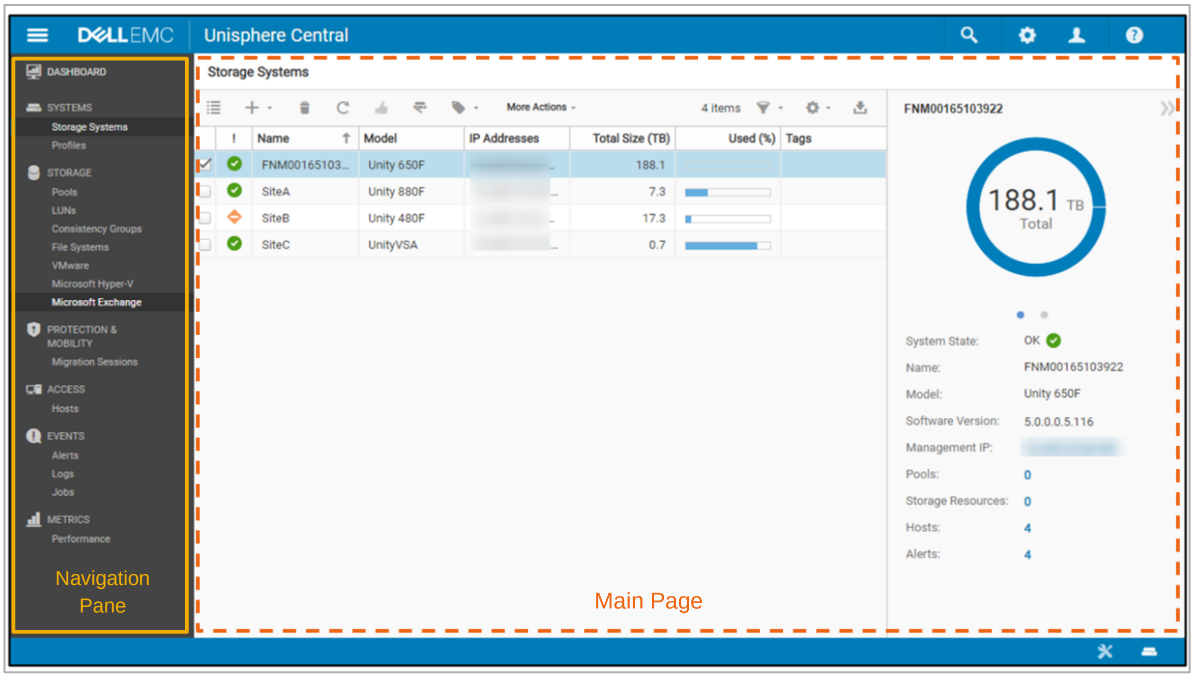
Unisphere Central is a centralized application that enables administrators to remotely monitor the status, activity, and resources of multiple storage systems that reside on a common network.

The Unisphere Central server is a vApp deployed on a VMware environment from an OVF template downloaded from the support web site.

- When deploying the OVF template, you can assign an IP address for the Unisphere Central server.
- This operation can be performed within vCenter or in the console of the VM on an ESXi host.

Storage administrators can remotely access the application from a client host, and check their storage environment.

Interface Navigation



Storage Systems

	!	Name	Model	IP Addresses	Total Size (TB)	Used (%)	Tags
☑	✓	FNM00165103...	Unity 650F	[redacted]	188.1		
□	✓	SiteA	Unity 880F	[redacted]	7.3		
□	◆	SiteB	Unity 480F	[redacted]	17.3		
□	✓	SiteC	UnityVSA	[redacted]	0.7		

FNM00165103922

System State: OK ✓
Name: FNM00165103922
Model: Unity 650F
Software Version: 5.0.0.0.5.116
Management IP: [redacted]
Pools: 0
Storage Resources: 0
Hosts: 4
Alerts: 4

Unisphere Central interface showing all the monitored Unity systems

Administrators use a single interface to rapidly access the systems that need attention or maintenance.

- Unisphere Central server obtains aggregated status, alerts and host details from the monitored systems.
- The server also collects performance and capacity metrics, and storage usage information.

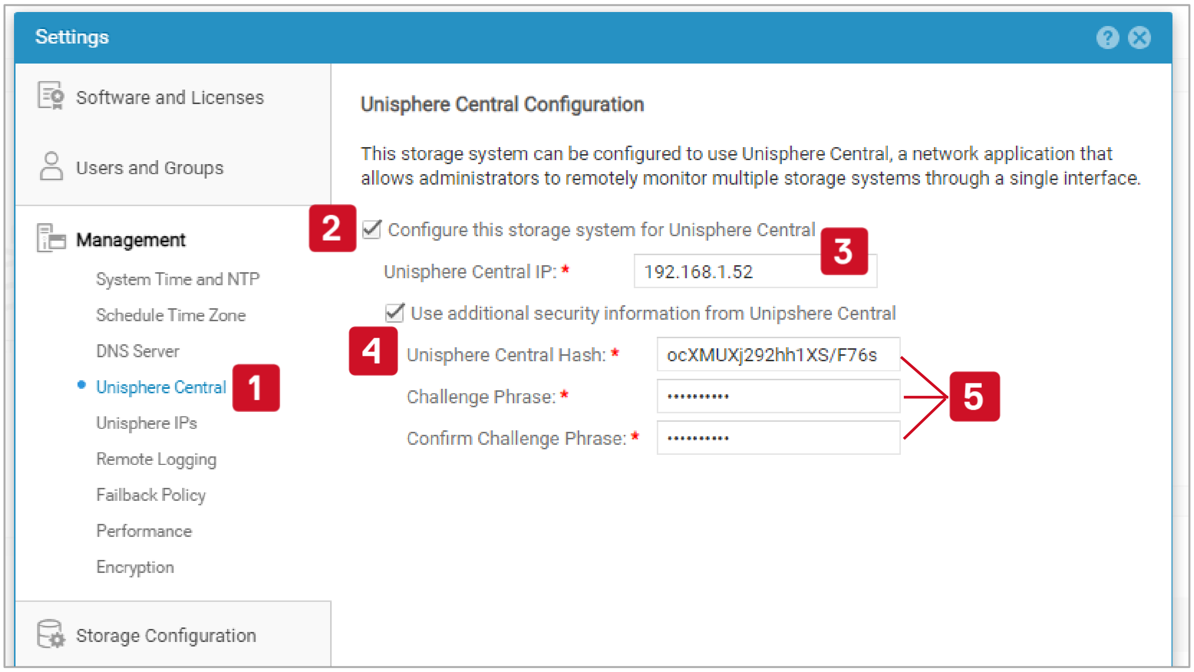
The **Navigation Pane** on the left has the Unisphere Central options for filtering and displaying information about the monitored storage systems.

The application displays all information for options selected from the navigation pane on the **Main Page**. In the example, the **Systems** page shows the storage systems the instance of Unisphere Central monitors.

The Unisphere Central user interface is built on the HTML5 technology with support on a wide range of browsers[2].

Configuration

To start monitoring a Dell Unity system, the storage administrator must configure the storage array to communicate with Unisphere Central.



Unisphere Central Configuration

This storage system can be configured to use Unisphere Central, a network application that allows administrators to remotely monitor multiple storage systems through a single interface.

☑ Configure this storage system for Unisphere Central

Unisphere Central IP: * 192.168.1.52

☑ Use additional security information from Unipshere Central

Unisphere Central Hash: * ocXMUXj292hh1XS/F76s

Challenge Phrase: * ••••••••••

Confirm Challenge Phrase: * ••••••••••

Unisphere Settings steps to enable system monitoring through Unisphere Central

[2] The compatible web browsers are: Google Chrome v33 or later, Microsoft Edge, Mozilla Firefox v28 or later, and Apple Safari v6 or later.

Open the Unisphere **Settings** window, and then go to the **Management** section.

1. Select **Unisphere Central**.
2. Select **Configure this storage system for Unisphere Central**.
3. Enter the IP address of the Unisphere Central server.
   - If the security policy on the Unisphere Central server was set to manual, no further configuration is necessary.
4. Select the **Use additional security information from Unisphere Central** if the security policy on the server is set to Automatic.
   - Then retrieve the security information from the server.
5. Enter the security information configured in the Unisphere Central server, and click **Apply** to save the changes

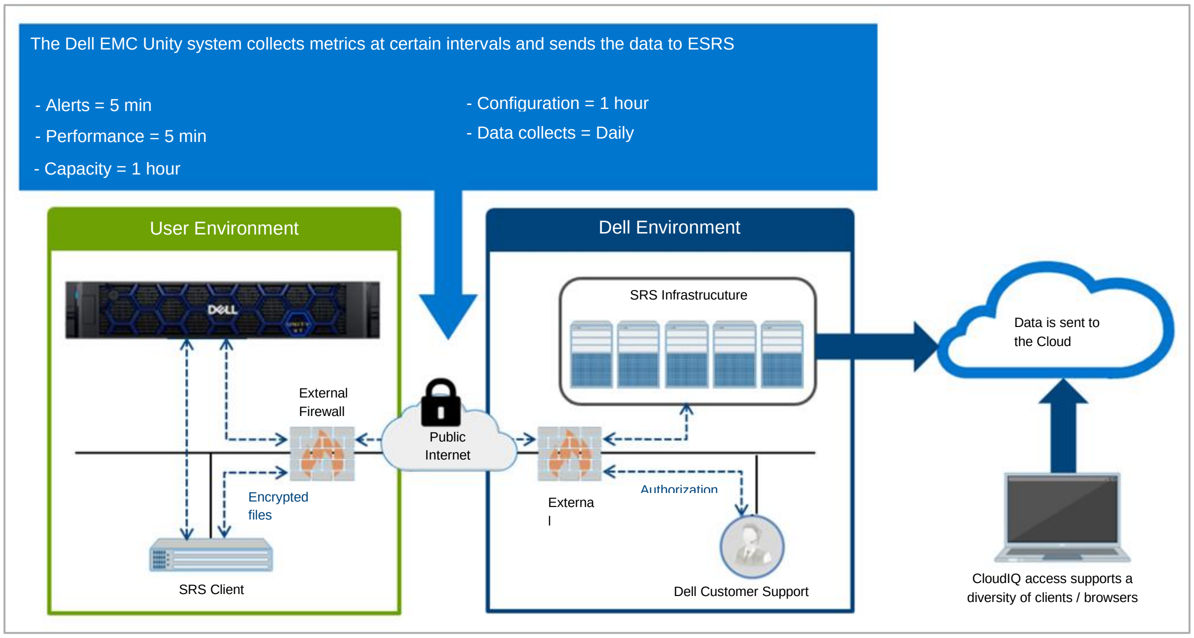
   a. Type the Unisphere Central **Certificate Hash**.

   b. Type and confirm the eight characters long **Challenge Phrase**.

Deep Dive: For more information, read the latest white paper on Unisphere Central available in the product support site.

Centralized Management - CloudIQ

Overview



CloudIQ theory of operations

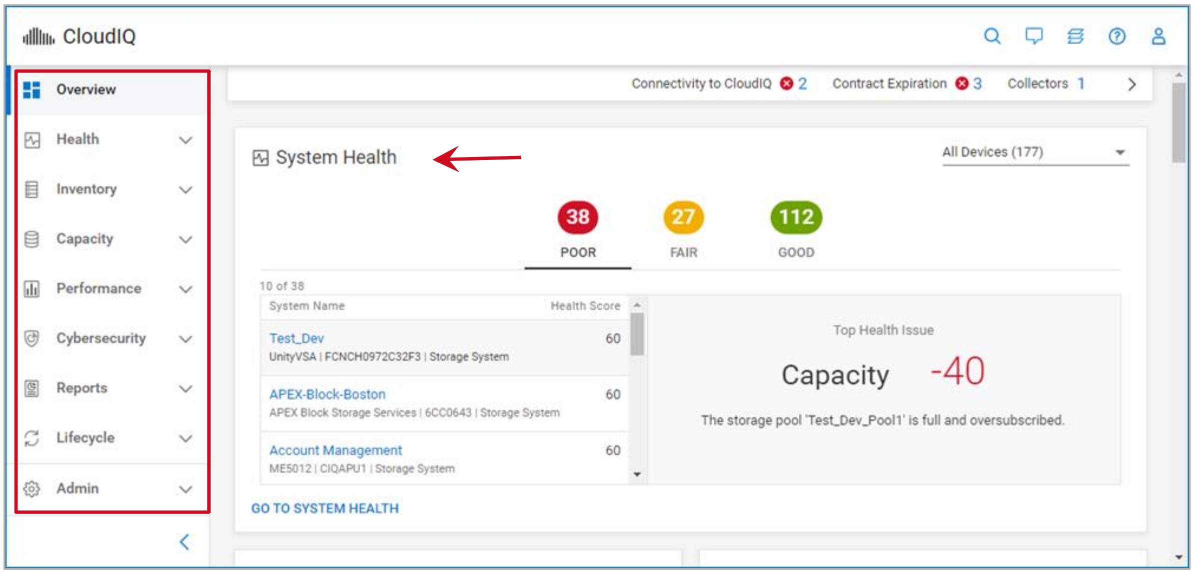
CloudIQ is a Cloud-based Software-as-a-Service (SaaS) solution used to monitor and service Dell Unity systems.

- CloudIQ is a Dell-hosted service that uses data collected by the Secure Connect Gateway.
  - **Secure Connect Gateway** also known as Secure Remote Services (SRS) is a secure, bi-directional connection between the Dell products in user environments and the Dell Support infrastructure.
  - Configured Unity storage systems collect several metrics at various predetermined time intervals and send the information to the SRS infrastructure.
- The CloudIQ functionality is embedded into the Dell Unity OE code and is free of cost requiring no license.

Administrators can monitor supported systems and perform basic service actions.

- The feature enables the access to near real-time analytics from anywhere at any time.
- The CloudIQ interface is accessible using a web browser from any location.

Interface Navigation



10 of 38

System Name	Health Score
Test_Dev UnityVSA | FCNCH0972C32F3 | Storage System	60
APEX-Block-Boston APEX Block Storage Services | 6CC0643 | Storage System	60
Account Management ME5012 | CIQAPU1 | Storage System	60

Top Health Issue

Capacity -40

The storage pool 'Test_Dev_Pool1' is full and oversubscribed.

CloudIQ Interface Overview page

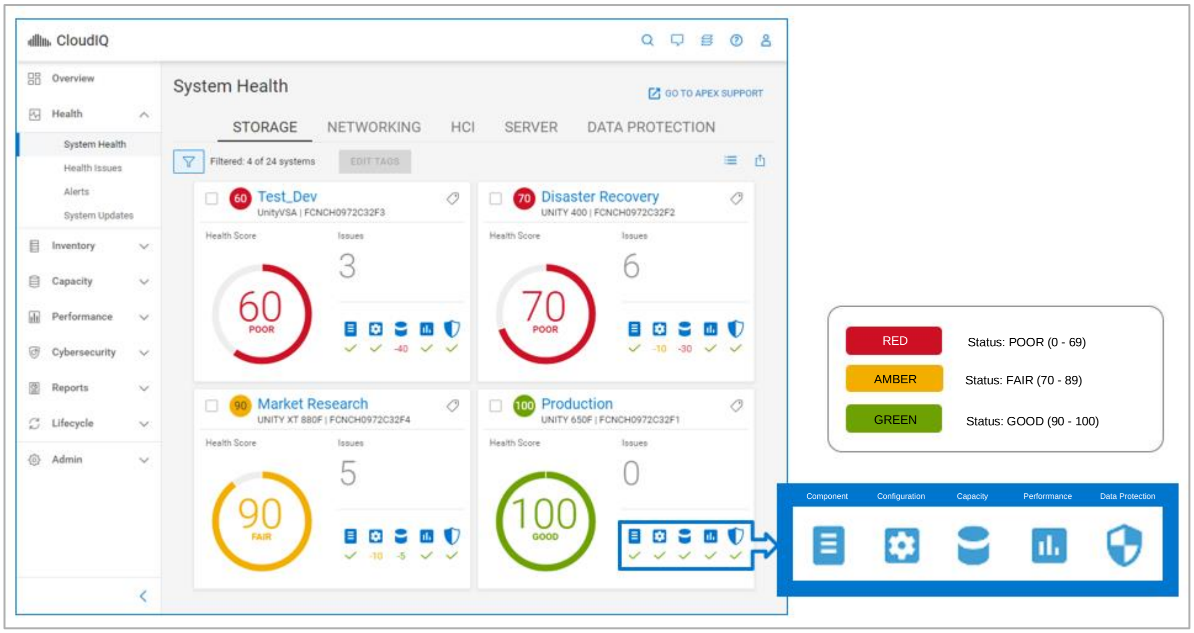
Navigation through the CloudIQ interface is done by selecting a menu option on the left pane. The selected information is displayed on the right pane.

CloudIQ provides dashboard views of all connected systems, displaying key information such as performance and capacity trending and predictions.

The Overview page widgets provide storage administrators with a quick check of the overall systems.

- Default widgets include system health scores, cybersecurity risks, system alerts, capacity approaching full, reclaimable storage, performance impacts, and systems needing updates.
- The System Health widget provides a summary of the health scores of all the monitored systems.

System Health



System Health page with filtered view of the monitored Unity systems

The System Health page is broken into Storage, Networking, HCI, Service and Data Protection systems categories.

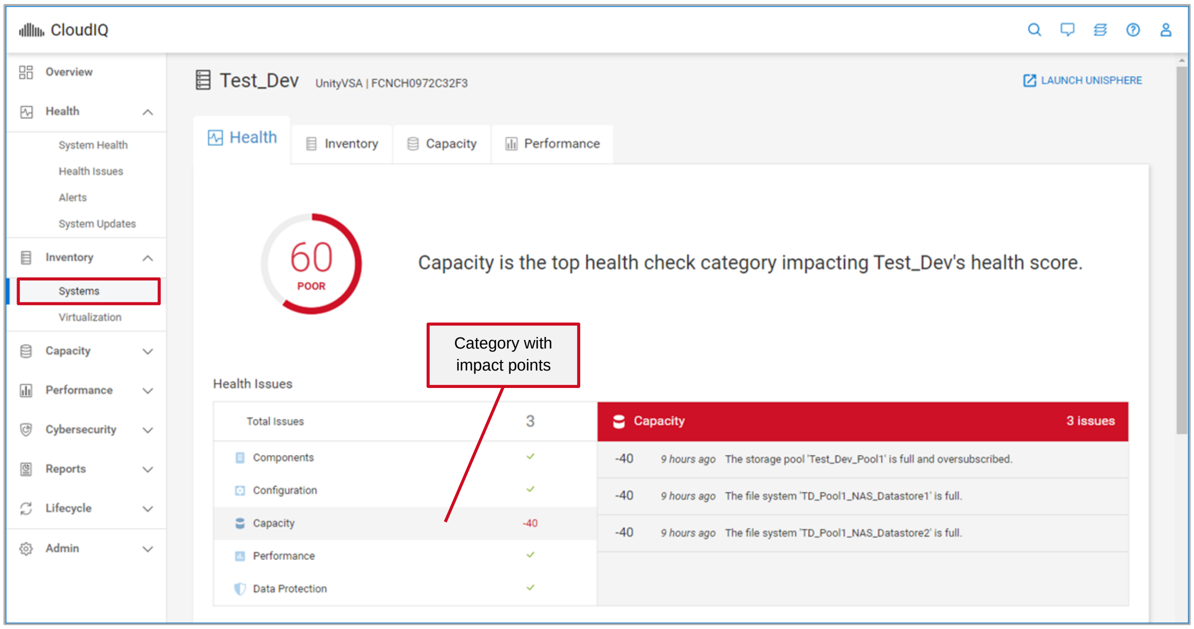
The page uses the proactive health score feature to display the health of a single or aggregated systems in the format of:

- A score that is shown as a number.
  - Systems are given a score with 100 being the top score and 0 being the lowest.
- A color that is associated with the score.

CloudIQ services running in the background collect data on each of the five categories: components, configuration, capacity, performance, and data protection.

- A set of rules is used to determine the impact point of these core factors on the system.
- The total score is based on the number of impact points across the five categories.

Individual System



Test_Dev UnityVSA | FCNCH0972C32F3

Capacity is the top health check category impacting Test_Dev's health score.

Category with impact points

Health Issues

Total Issues	3
Components	✓
Configuration	✓
Capacity	-40
Performance	✓
Data Protection	✓

Capacity 3 issues

-40	*9 hours ago*	The storage pool 'Test_Dev_Pool1' is full and oversubscribed.
-40	*9 hours ago*	The file system 'TD_Pool1_NAS_Datastore1' is full.
-40	*9 hours ago*	The file system 'TD_Pool1_NAS_Datastore2' is full.

CloudIQ individual system summary view

Selecting an individual system from the **System Health** view opens a summary page with key system information divided into tabs: health, configuration, capacity, and performance.

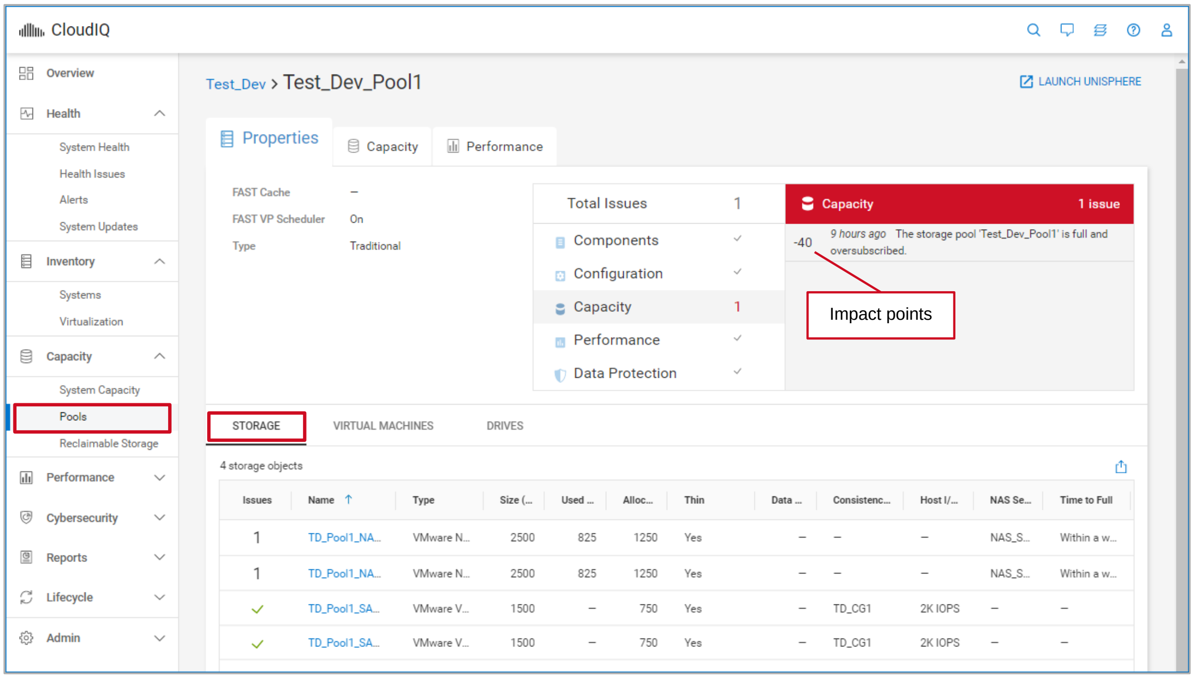
The summary landing page is the **Health** tab showing the system health score and the total of issues that are found in each category.

From the Health tab, additional information about the cause can be retrieved by selecting the affected category.

In this example, the Unity system **Test_Dev** is selected and the Health tab shows a **score of 60** (status = **poor**).

- The **RED** color is used to identify the system status and category with impact points that are causing the condition.
- The problem is at the storage **capacity** level. There are three issues reported: three storage pools are full.

Storage Pool



FAST Cache	–
FAST VP Scheduler	On
Type	Traditional

Total Issues	1
Components	✓
Configuration	✓
Capacity	1
Performance	✓
Data Protection	✓

Capacity 1 issue

-40 *9 hours ago* The storage pool 'Test_Dev_Pool1' is full and oversubscribed.

4 storage objects

Issues	Name ↑	Type	Size (...	Used ...	Alloc...	Thin	Data ...	Consistenc...	Host I/...	NAS Se...	Time to Full
1	TD_Pool1_NA...	VMware N...	2500	825	1250	Yes	–	–	–	NAS_S...	Within a w...
1	TD_Pool1_NA...	VMware N...	2500	825	1250	Yes	–	–	–	NAS_S...	Within a w...
✓	TD_Pool1_SA...	VMware V...	1500	–	750	Yes	–	TD_CG1	2K IOPS	–	–
✓	TD_Pool1_SA...	VMware V...	1500	–	750	Yes	–	TD_CG1	2K IOPS	–	–

CloudIQ pool properties page

To view a details about the pools provisioned by the monitored system:

- Select the **Pools** option under the **Capacity** section.
- Select the pool from the list and the Properties page for the individual resource is displayed.

The **Properties** page shows detailed information including the system health status at the capacity level, with the score impact points and the number of issues.

The **Capacity** tab displays the used and free capacity in the pool, and the time to reach a full state.

The **Performance** tab enables a storage administrator to view the top performance storage objects

The **STORAGE** tab on the bottom of the page shows storage objects that are created from the pool.

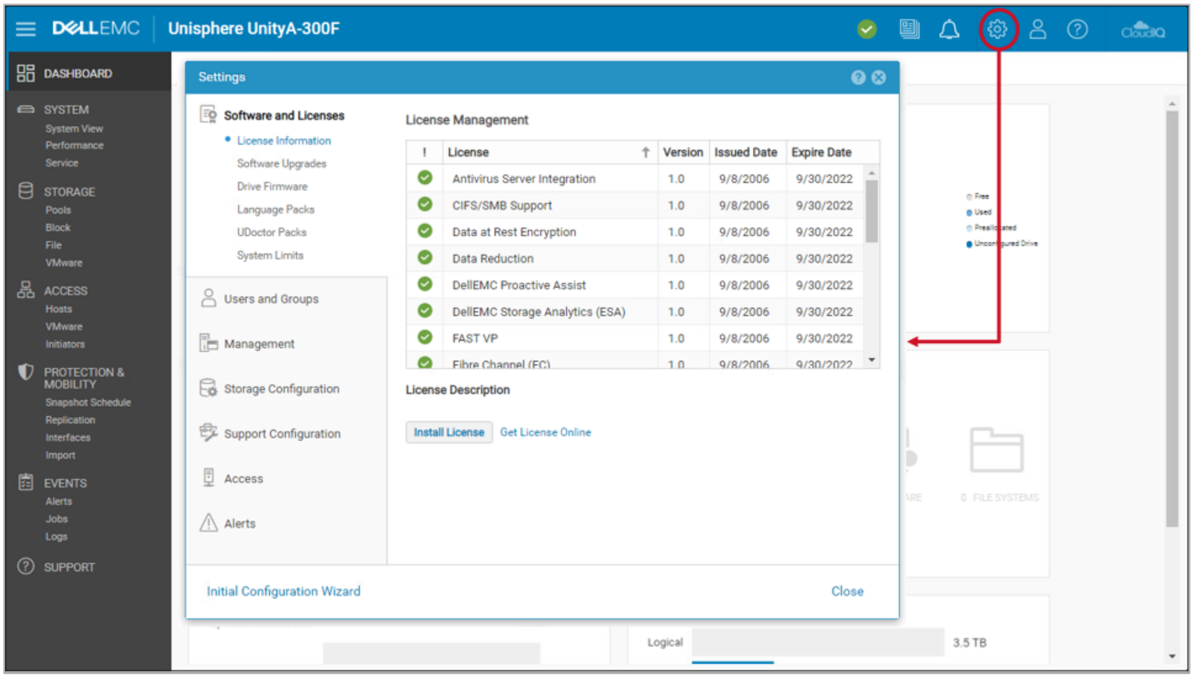
The **VIRTUAL MACHINES** tab shows information about the VMs using the provisioned storage resource.

The **DRIVES** tab shows the number of drives, drive types, and capacity that is used to create the storage pool.

Basic System Settings

Unisphere Settings

From the Unisphere **Settings** window, a storage administrator can configure the global settings and parameters for a Dell Unity system.



License Management

!	License	Version	Issued Date	Expire Date
✓	Antivirus Server Integration	1.0	9/8/2006	9/30/2022
✓	CIFS/SMB Support	1.0	9/8/2006	9/30/2022
✓	Data at Rest Encryption	1.0	9/8/2006	9/30/2022
✓	Data Reduction	1.0	9/8/2006	9/30/2022
✓	DellEMC Proactive Assist	1.0	9/8/2006	9/30/2022
✓	DellEMC Storage Analytics (ESA)	1.0	9/8/2006	9/30/2022
✓	FAST VP	1.0	9/8/2006	9/30/2022
✓	Fibre Channel (FC)	1.0	9/8/2006	9/30/2022

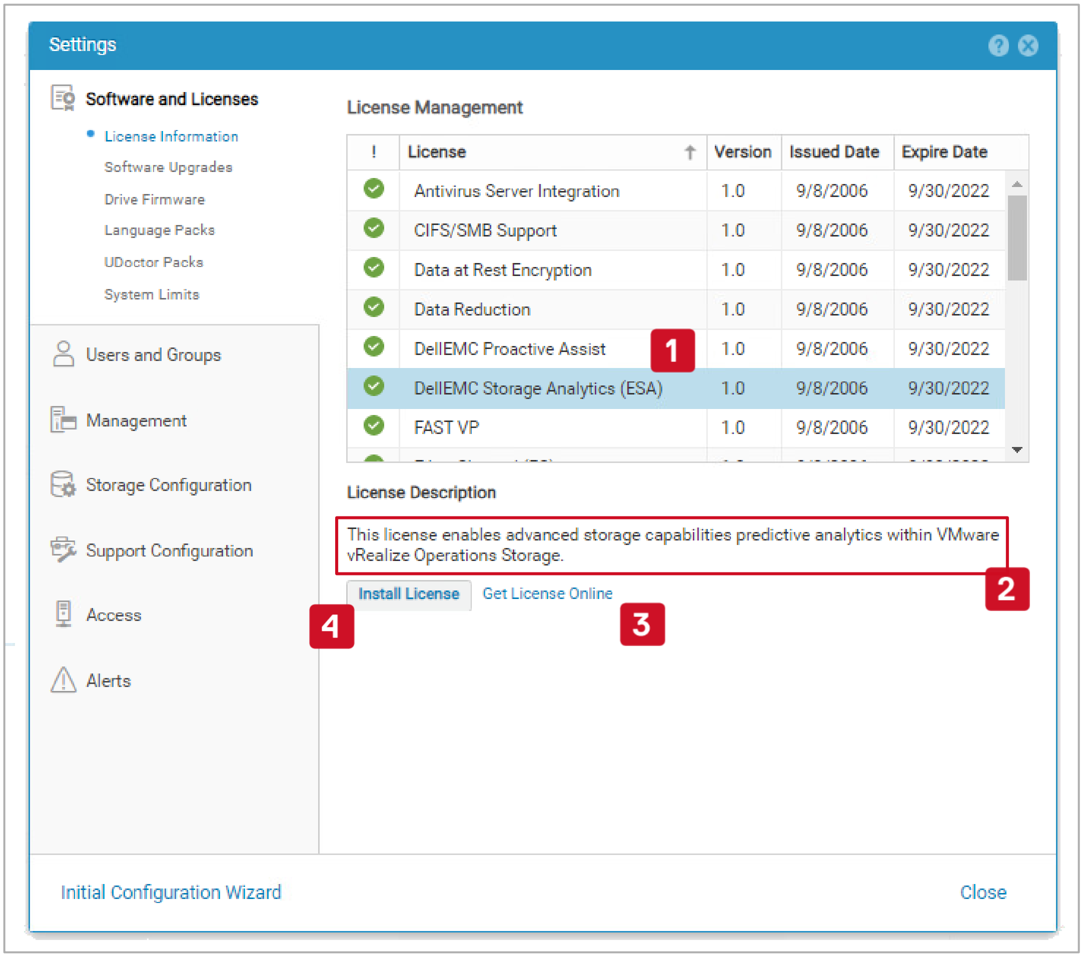
License Description

Unisphere Settings window

Open the **Settings** configuration window by selecting its icon from the top menu. Supported operations include:

- Monitor installed licenses.
- Manage users and groups that can access the system.
- Configure the network environment.
- Enable centralized management.
- Enable logging of system events to a remote log server.
- Start and pause FAST suite feature operations.
- Register support credentials, and enable Secure Remote Services.
- Create IP routes.
- Enable CHAP authentication for the iSCSI operations.
- Configure email and SNMP alerts.

Configure Unisphere Basic Settings - Licenses



License Management

!	License	Version	Issued Date	Expire Date
✓	Antivirus Server Integration	1.0	9/8/2006	9/30/2022
✓	CIFS/SMB Support	1.0	9/8/2006	9/30/2022
✓	Data at Rest Encryption	1.0	9/8/2006	9/30/2022
✓	Data Reduction	1.0	9/8/2006	9/30/2022
✓	DellEMC Proactive Assist	1.0	9/8/2006	9/30/2022
✓	DellEMC Storage Analytics (ESA)	1.0	9/8/2006	9/30/2022
✓	FAST VP	1.0	9/8/2006	9/30/2022

License Description

This license enables advanced storage capabilities predictive analytics within VMware vRealize Operations Storage.

Unisphere Settings Licenses Information

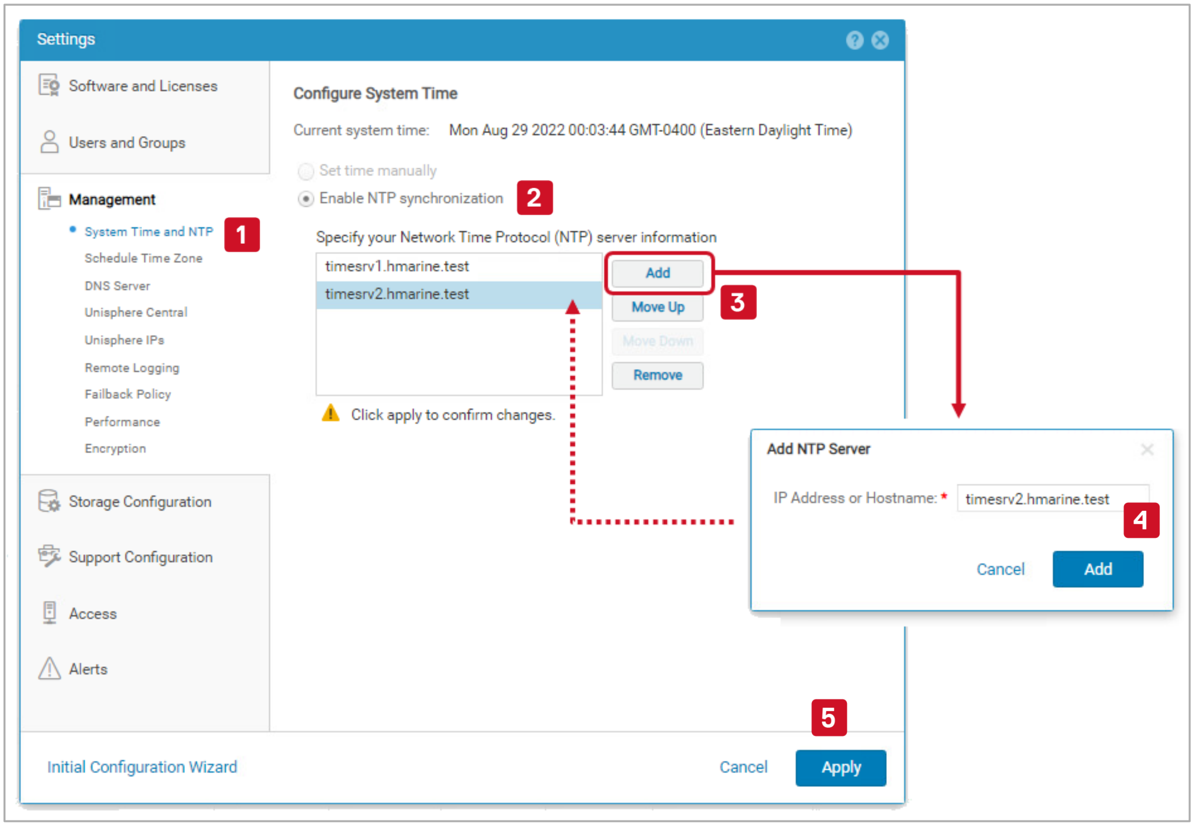
The first screen of the Settings window is the **License Information** page.

1. Select a feature license from the list.
2. A description of the feature is displayed.
3. To obtain a product license, select **Get License Online**.
   - Access the product page on the support site and download the license file.
   - Transfer the license file to a computer with access to the storage system.
4. To unlock the Dell Unity features, select **Install License**.

Basic System Settings

- Review and accept the software license and management agreement.
- Locate and upload the product license file from the local computer with access to the storage system.

Configure Unisphere Basic Settings - System Time



Configure System Time

Current system time: Mon Aug 29 2022 00:03:44 GMT-0400 (Eastern Daylight Time)

○ Set time manually

● Enable NTP synchronization

Specify your Network Time Protocol (NTP) server information

timesrv1.hmarine.test

timesrv2.hmarine.test

Click apply to confirm changes.

Add NTP Server

IP Address or Hostname: * timesrv2.hmarine.test

Unisphere Settings System Time and NTP

The Dell Unity platform supports two methods for configuring the storage system time:

- Manual setup
- Network Time Protocol (NTP) synchronization

To configure Unity to synchronize its time with NTP servers:

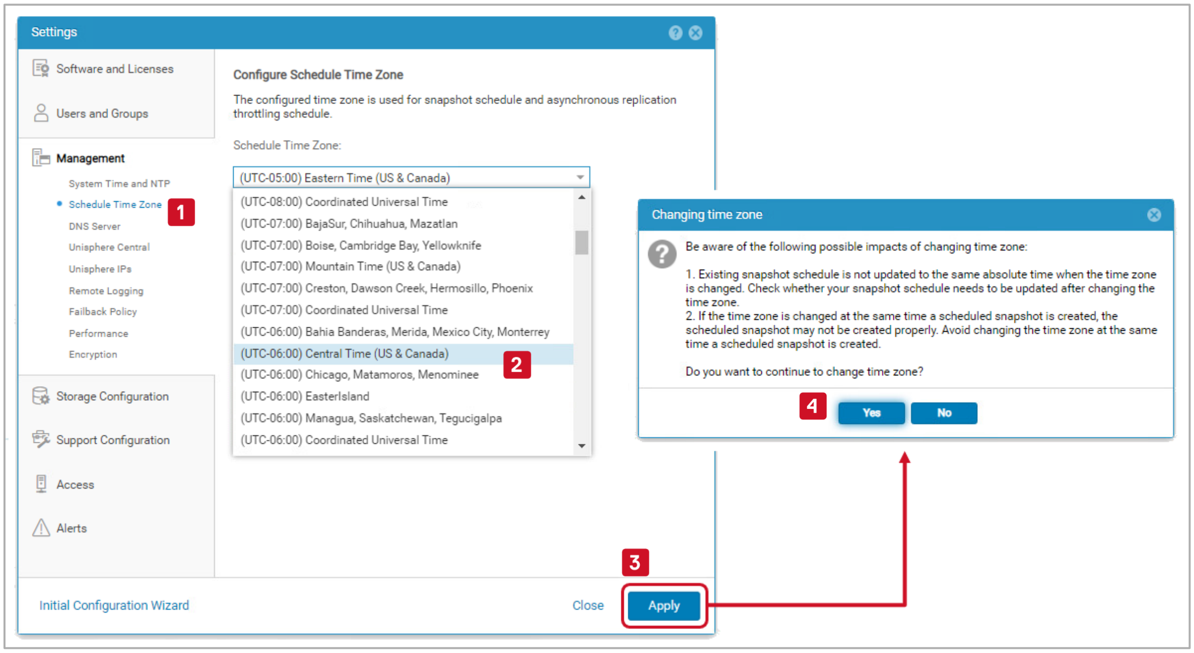
1. Select the **System Time and NTP** option under the Management section.
2. Check the **Enable NTP synchronization** radio button.
3. Then select **Add** to launch the Add NTP Server window.

4. Enter the IP address or the name of an NTP server and select **Add** on the dialog box.
5. The NTP server is added to the list. Select **Apply** to save the changes.

Configure Unisphere Basic Settings - Schedule Time Zone

The Dell Unity platform supports a time zone configuration for snapshot schedules and asynchronous replication throttling.

- The schedule time zone applies to system defined and user created snapshot schedules.



Configure Schedule Time Zone

The configured time zone is used for snapshot schedule and asynchronous replication throttling schedule.

Schedule Time Zone: (UTC-05:00) Eastern Time (US & Canada)

(UTC-08:00) Coordinated Universal Time
(UTC-07:00) BajaSur, Chihuahua, Mazatlan
(UTC-07:00) Boise, Cambridge Bay, Yellowknife
(UTC-07:00) Mountain Time (US & Canada)
(UTC-07:00) Creston, Dawson Creek, Hermosillo, Phoenix
(UTC-07:00) Coordinated Universal Time
(UTC-06:00) Bahia Banderas, Merida, Mexico City, Monterrey
(UTC-06:00) Central Time (US & Canada)
(UTC-06:00) Chicago, Matamoros, Menominee
(UTC-06:00) EasterIsland
(UTC-06:00) Managua, Saskatchewan, Tegucigalpa
(UTC-06:00) Coordinated Universal Time

Changing time zone

Be aware of the following possible impacts of changing time zone:

1. Existing snapshot schedule is not updated to the same absolute time when the time zone is changed. Check whether your snapshot schedule needs to be updated after changing the time zone.
2. If the time zone is changed at the same time a scheduled snapshot is created, the scheduled snapshot may not be created properly. Avoid changing the time zone at the same time a scheduled snapshot is created.

Do you want to continue to change time zone?

Unisphere Settings Schedule Time Zone

To configure a local time zone:

1. Select **Management >Schedule Time Zone**.
2. Open the drop-down list and select the time zone that matches your location.

- The selected schedule time zone reflects the Universal Time Coordinated (UTC)[3] adjusted by an offset for the local time zone.

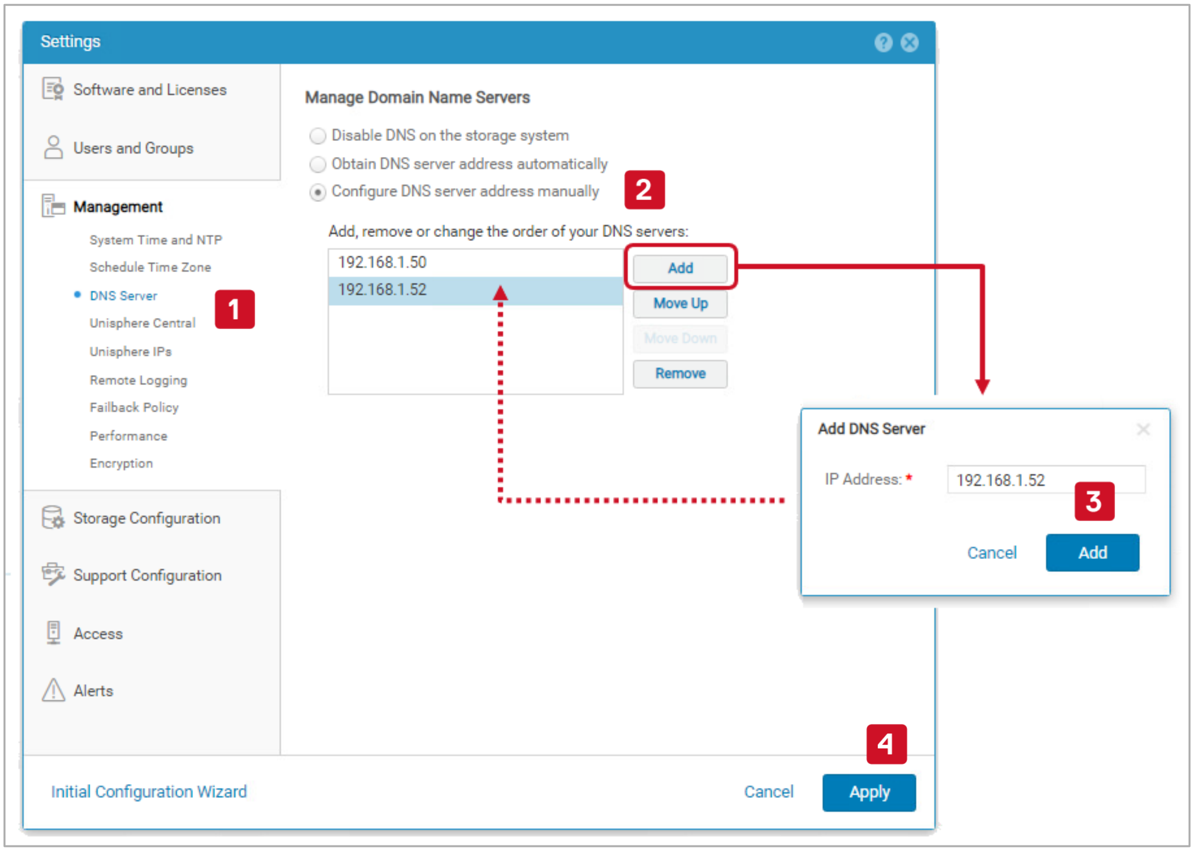
3. Select **Apply**. A disclaimer message is displayed with a warning about the impact of the change.
4. Select **Yes** to confirm the time zone change. The new schedule time zone is set for the system.

> **Important**: Existing snapshot schedules are not updated to the same absolute time when the time zone is changed. After changing the Schedule Time Zone, you must check whether your snapshot schedule must be updated.

[3] Unity systems use the Universal Time Coordinated (UTC) for time zone setting (operating system, logs, FAST VP, and so on).

Configure Unisphere Basic Settings - Domain Name Servers

Some Dell Unity features rely on network name resolution configuration to work. For example, Unisphere alert settings.



Manage Domain Name Servers

○ Disable DNS on the storage system
○ Obtain DNS server address automatically
● Configure DNS server address manually

Add, remove or change the order of your DNS servers:

192.168.1.50
192.168.1.52

IP Address: * 192.168.1.52

Unisphere Settings DNS Server

To manually add the network address of DNS servers the storage system uses for name resolution:

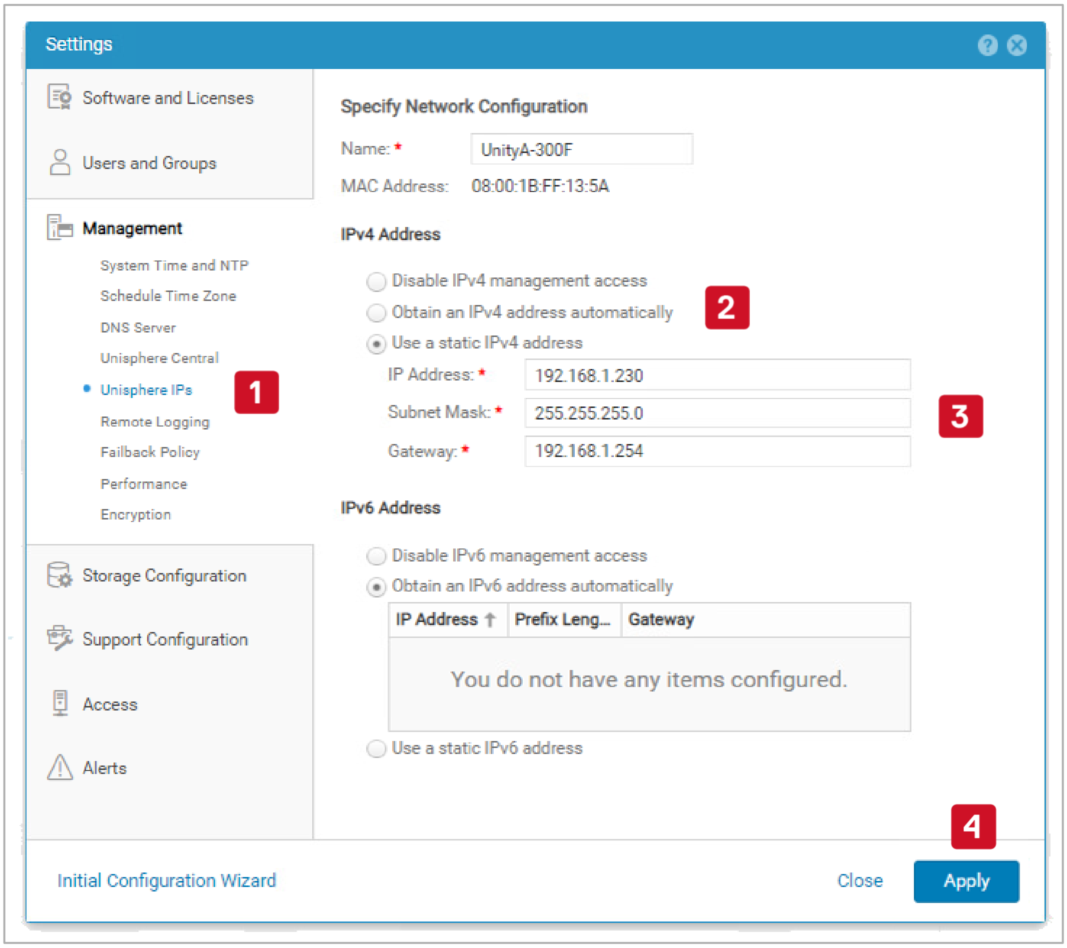
1. Select the **DNS Server** option under the Management section.
2. Select **Configure DNS server address manually**.
3. To open the Add DNS Server configuration window, select **Add**.
4. Enter the IP address of the DNS server and select **Add**.
5. The DNS server entry is added to the list. Select **Apply** to submit and save the changes.

If running Unity on a network which includes DHCP and DNS servers, the system can automatically retrieve one or more IP addresses of DNS servers.

- Select the **Obtain DNS servers address automatically** on the Manage Domain Name Servers page.

Configure Unisphere Basic Settings - Management Port Network Address

Administrators can view and modify the hostname, and the network addresses assigned to the Dell Unity storage system.



Specify Network Configuration

Name: * UnityA-300F

MAC Address: 08:00:1B:FF:13:5A

IPv4 Address

○ Disable IPv4 management access
○ Obtain an IPv4 address automatically
● Use a static IPv4 address

IP Address: * 192.168.1.230

Subnet Mask: * 255.255.255.0

Gateway: * 192.168.1.254

IPv6 Address

○ Disable IPv6 management access
● Obtain an IPv6 address automatically

IP Address ↑	Prefix Leng...	Gateway
You do not have any items configured.		

○ Use a static IPv6 address

Unisphere Settings Unity network address

The storage system supports both IPv4 and IPv6 addresses. Each IP version has radio buttons to disable the configuration and select the dynamic or static configuration.

- If running the storage system on a dynamic network, the management IP address can be assigned automatically by selecting the proper radio button.
- If enabling ESRS support for the Unity system, then Dell Technologies recommends that a static IP address is assigned to the storage system.

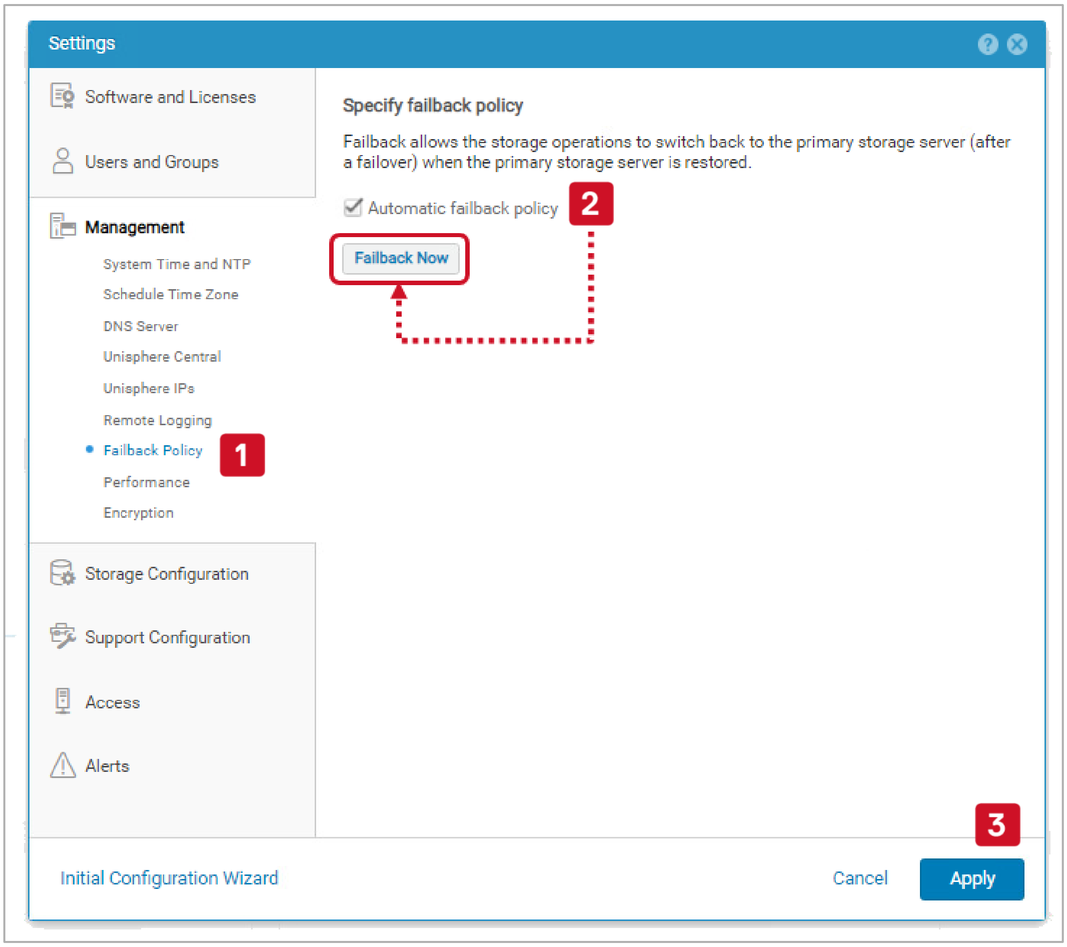
To view or modify the network configuration of the Unity system management port:

1. Expand the Management section and select the **Unisphere IPs** option.
2. To manually configure a IPv4 network address, select the **Use a static IPv4 address**. (Default option.)
3. Enter or modify the network address configuration: IP address, Subnet Mask, Gateway.
4. Select **Apply** to submit and save the changes.

If running the storage system on a dynamic network, the management IP address can be assigned automatically by selecting the proper radio button.

If enabling ESRS support for the Unity system, then Dell Technologies recommends that a static IP address is assigned to the storage system.

Configure Unisphere Basic Settings - Failback Policy



Specify failback policy

Failback allows the storage operations to switch back to the primary storage server (after a failover) when the primary storage server is restored.

☑ Automatic failback policy

Unisphere Settings failback policy

In Dell EMC Unity XT systems with dual SPs, when one of them has a problem or is rebooting, the NAS servers that are hosted on the SP fail over to the other SP.

Failback to the recovered SP can be automatic or manual depending on the failback policy set on the storage system.

To view or modify the failback policy of the Unity system:

1. Select the **Failback Policy** option under the Management section.
2. Disable, or enable the **automatic failback policy** (the default is enabled).

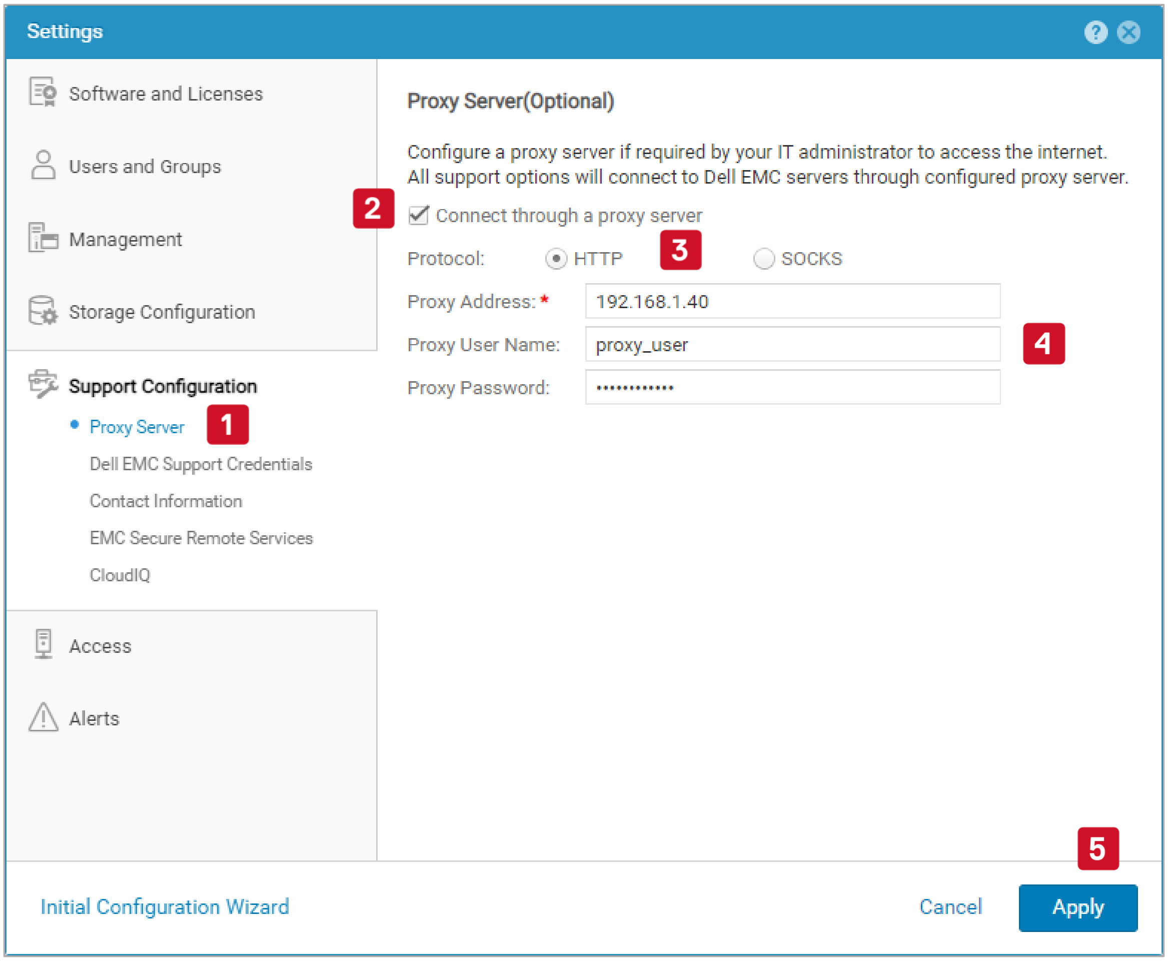
  - When the option is disabled, you can manually fail back all NAS servers, by selecting **Failback Now**.

3. Select **Apply** to submit and save the changes. The Failback Policy is set for the storage system.

Support Configuration

Configure Support Settings - Proxy Server

Proxy server configuration enables the exchange of service information for the Dell Unity systems that cannot connect to the Internet directly.



Proxy Server(Optional)

Configure a proxy server if required by your IT administrator to access the internet.
All support options will connect to Dell EMC servers through configured proxy server.

☑ Connect through a proxy server

Protocol: ● HTTP ○ SOCKS

Proxy Address: * 192.168.1.40

Proxy User Name: proxy_user

Proxy Password: ••••••••••••

Unisphere Settings Proxy Server Configuration

To configure the Proxy Server settings, the user must open the Settings window and perform the following:

1. Expand the Support Configuration section, and select **Proxy Server**.
2. The **Connect through a proxy server** checkbox must be selected.
3. Select the communication protocol: HTTP[4] or SOCKS[5].
4. Enter the IP address of the Proxy Server, and the credentials (username and password) if the protocol requires user authentication.
    - The SOCKS protocol requires user authentication.
5. Select **Apply** to save the changes.

After configured, the storage administrator performs the following service tasks using the proxy server connection:

- Configure and save support credentials.
- Configure Secure Connect Gateway.
- Display the support contract status for the storage system.
- Receive notifications about support contract expiration, technical advisories for known issues, software and firmware upgrade availability, and the Language pack update availability.

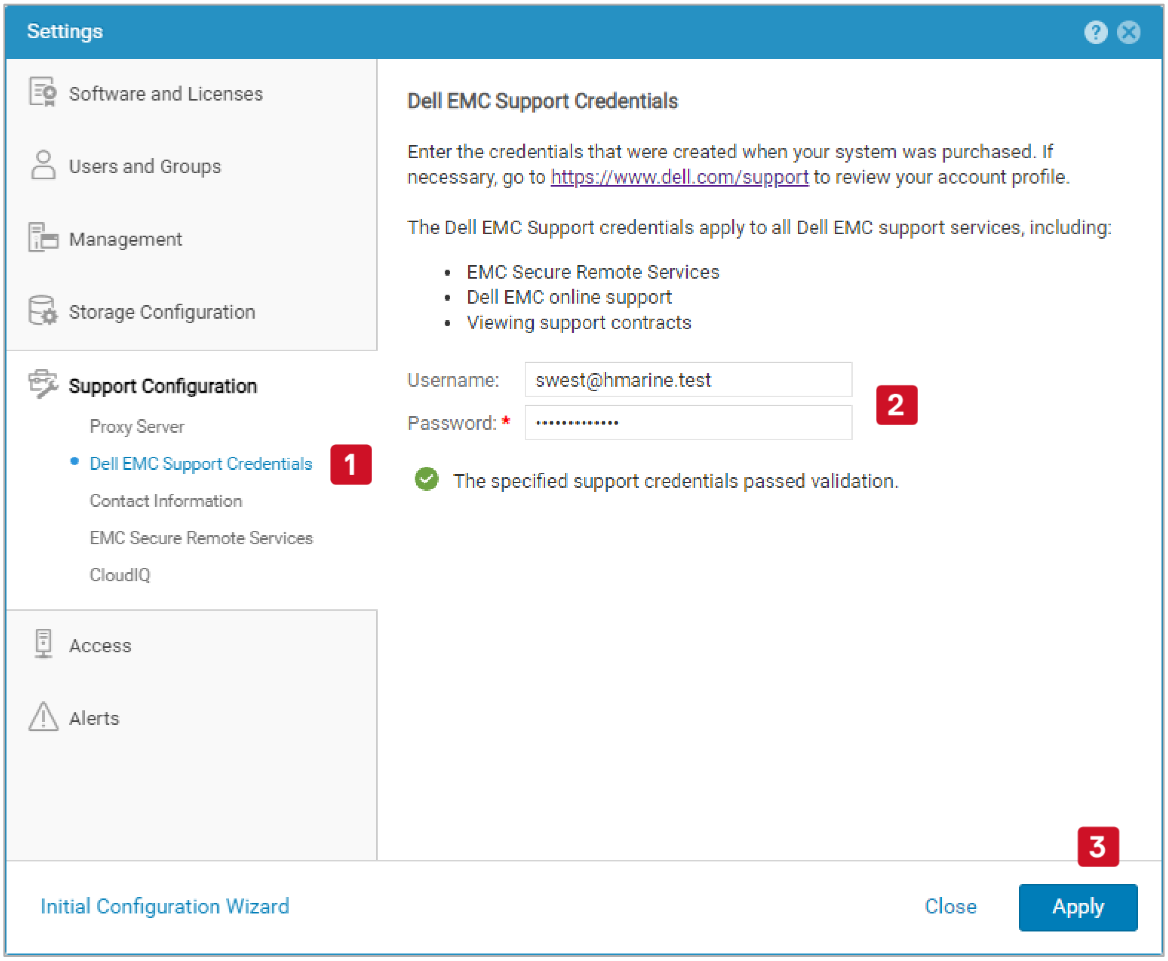
[4] The HTTP (nonsecure) protocol supports all service tasks including upgrade notifications. This option uses port 3128 by default.

[5] The SOCKS (secure) protocol should be selected for IT environments where HTTP is not allowed. This option uses port 1080 by default and does not support the delivery of notifications for technical advisories, software, and firmware upgrades.

Configure Support Settings - Dell Support Credentials

Support credentials are used to retrieve the customer current support contract information and keep it updated automatically.

- The data provides access to all the options to which the client is entitled on the Unisphere Support page.



Dell EMC Support Credentials

Enter the credentials that were created when your system was purchased. If necessary, go to https://www.dell.com/support to review your account profile.

The Dell EMC Support credentials apply to all Dell EMC support services, including:

- EMC Secure Remote Services
- Dell EMC online support
- Viewing support contracts

Username: swest@hmarine.test

Password: * •••••••••••••

✓ The specified support credentials passed validation.

Unisphere Settings Dell support credentials configuration

To configure the support credentials, the user must open the Settings page and perform the following:

1. Expand the Support Configuration section, and select the **Dell EMC Support Credentials** option.

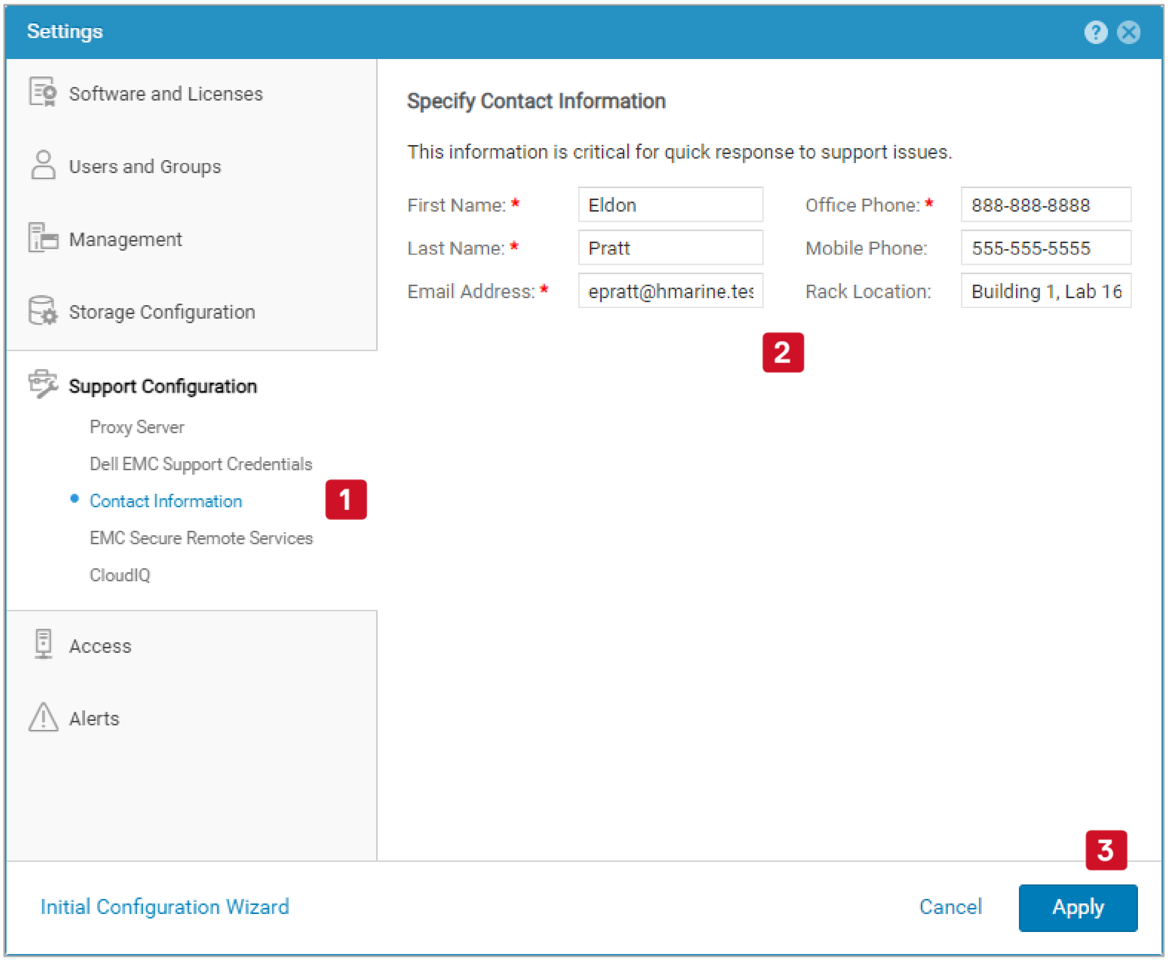
2. Then enter the username and password on the proper fields. The filled out credentials must be associated with a support account.
3. Select **Apply** to commit the changes.

Support credentials are required to configure Secure Connect Gateway.

- The service provides Dell support the direct access to the storage system (through HTTPS or SSH).
- Dell Support personnel can perform troubleshooting on the storage system and resolve issues more quickly.

Configure Support Settings - Contact Information

Up-to-date contact information ensures that Dell support has the most accurate information for contacting the user in response to an issue.



Specify Contact Information

This information is critical for quick response to support issues.

First Name: * Eldon

Last Name: * Pratt

Email Address: * epratt@hmarine.tes

Office Phone: * 888-888-8888

Mobile Phone: 555-555-5555

Rack Location: Building 1, Lab 16

Unisphere Settings contact information configuration

To configure the contact information, perform the following:

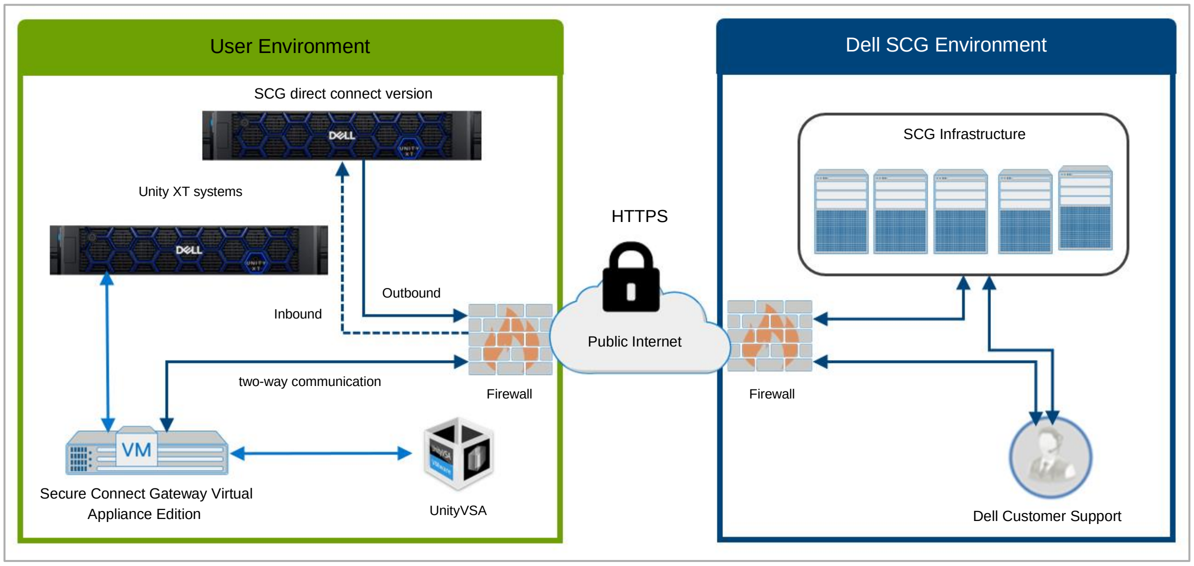
1. Expand the Support Configuration section, and select **Contact Information**.
2. Then type the contact information details on the proper fields.
3. Select **Apply** to commit the changes.

Tip: The user receives system alert reminders to update the contact information every six months.

Secure Connect Gateway (SCG)

Overview

Secure Connect Gateway is a Dell Technologies Services solution which consolidates the capabilities of the SupportAssist Enterprise (SAE) and Secure Remote Services (SRS) connectivity platforms. The solution provides a secure, bi-directional connection between the Dell products in user environments and the Dell Support infrastructure.



Secure Connect Gateway architecture

Benefits:

- Dell support can remotely monitor configured systems by receiving system-generated alerts.
- Support personnel can connect into the customer environment for remote diagnosis and repair activities.
- Provides a high-bandwidth connection for large file transfers.
- Enables proactive Service Request (SR) generation and usage license reporting.
- The service operates on a 24x7 basis.

Secure Connect Gateway is implemented as stand-alone virtual appliance and as a direct connect (integrated) version for selected Dell hardware.

Deployment Options

Secure Connect Gateway options available with the Dell Unity platform include an embedded version and the Secure Connect Gateway virtual appliance edition.

The embedded version provides direct connectivity integrated into the Dell Unity XT storage system.

- The Secure Connect Gateway software is embedded into the Dell Unity XT operating environment (OE)[6] as a managed service.
- The embedded version uses an on-array Docker container which enables only the physical system to communicate with Support Center.
- The storage administrator can configure one way (outbound) or two way (outbound/inbound) communication.

The Secure Connect Gateway Virtual Application Edition is a centralized gateway version that is installed as an off-array virtual machine.

- Secure Connect Gateway virtual appliance servers can be configured in a cluster for service resiliency.
- Dell Unity XT or Unity VSA systems are added to the Secure Connect Gateway cluster.
- The storage administrator provides the IP address of the primary and secondary Secure Connect Gateway servers.
- A single secure connection (two-way communication) is established between the Support Center servers and the off-array Secure Connect Gateway.

[6] The Dell EMC Unity OE is responsible for persisting the configuration and the certificates that are needed for Secure Connect Gateway to work.

Communication

There are two remote service connectivity options for the Integrated Secure Connect Gateway version:

- **Outbound/Inbound (default)**
  - This option enables remote service connectivity capabilities for remote transfer to and from the Support Center, with the Dell Unity XT system.
  - Ports 443 and 8443 are required for outbound connections.
  - Two-way Secure Connect Gateway is the recommended configuration.
- **Outbound only**
  - This option enables remote service connectivity capability for remote transfer to the Support Center from the Dell Unity XT system.
  - Ports 443 and 8443 must be opened for outbound connections.
  - One-Way Secure Connect Gateway is available for users who have security concerns but still want to take advantage of CloudIQ.

For the Centralized version, the administrator must ensure that port 9443 is open between the SCG virtual appliance server and the Unity system.

- For outbound network traffic, the port 443 must be open.

Comparison

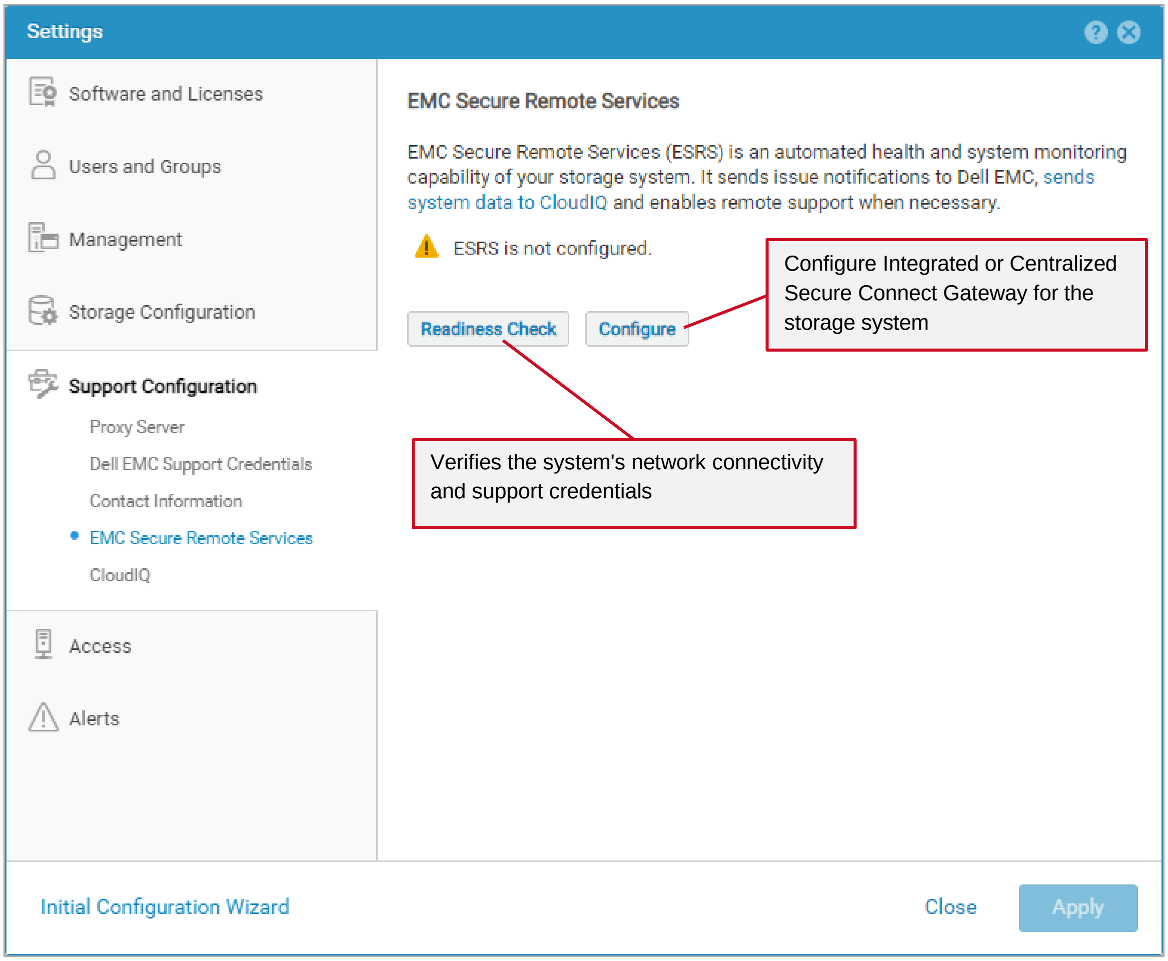
The table shows a comparison of the two deployment options.

Name	Centralized (Virtual Appliance Edition)	Integrated (Embedded)
Feature set	Same	Same
Number of devices	Multiple	1
Use of external VM is required.	Yes	No
Management interface	Native	Unisphere

Internet connectivity is required.	Gateway only	Every system
Ports used for Inbound Traffic	9443	80
Ports used for Outbound Traffic	443	443 and 8443

Configure Support Settings - Secure Connect Gateway

Storage administrators can view the status and enable Secure Connect Gateway from the **Secure Remote Services** page of the Unisphere settings.



EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is an automated health and system monitoring capability of your storage system. It sends issue notifications to Dell EMC, sends system data to CloudIQ and enables remote support when necessary.

⚠ ESRS is not configured.

Configure Integrated or Centralized Secure Connect Gateway for the storage system

Verifies the system's network connectivity and support credentials

Unisphere Settings Secure Connect Gateway configuration

To verify the Secure Connect Gateway configuration, expand the Support Configuration section, and select **EMC Secure Remote Services**.

- Run a **readiness check**, to verify if the system is properly set for configuring the Secure Connect Gateway. Running this operation is optional, but highly recommended.
- Select **Configure** to launch the **Configure Secure Connect Gateway** wizard. As discussed before, the remote service options available to send storage

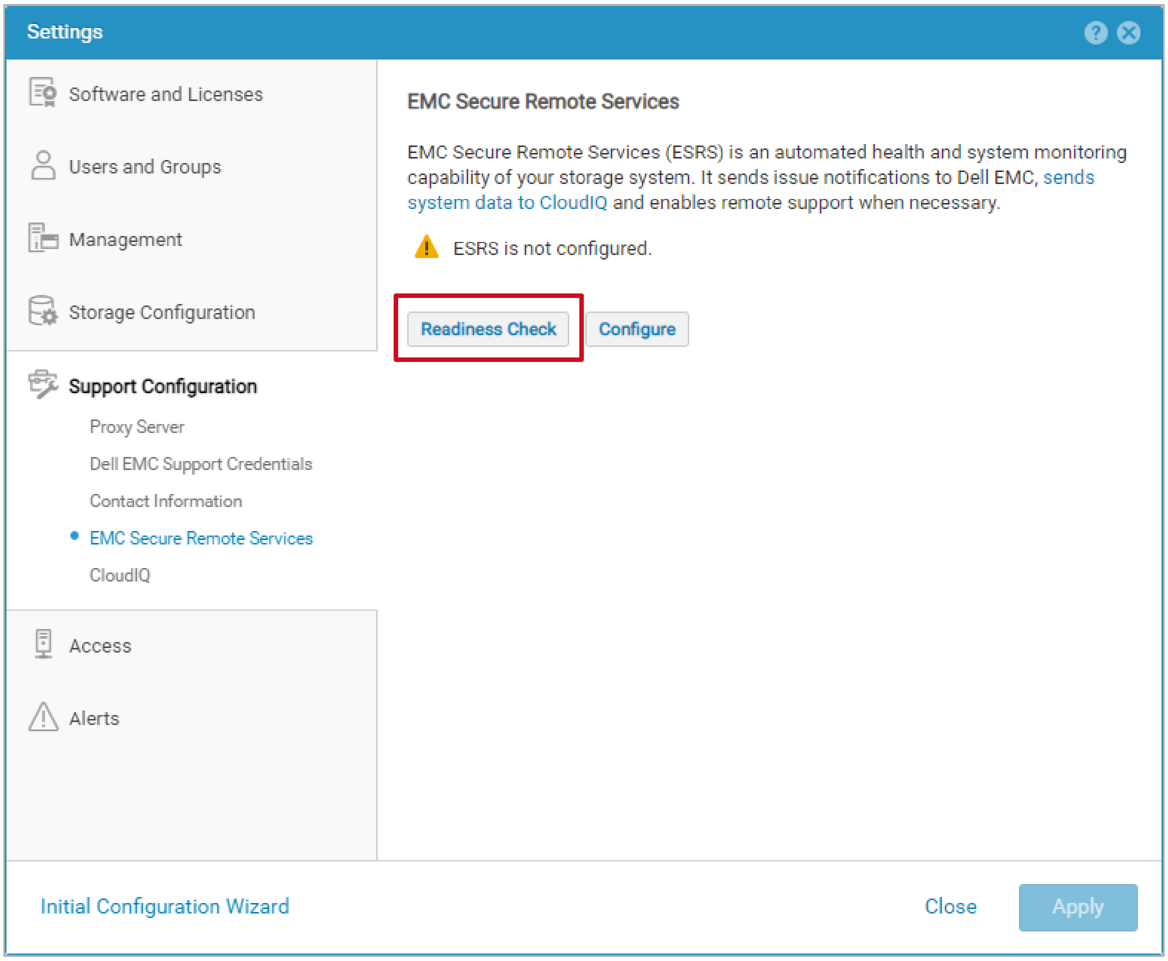
systems information to the Support Center for remote troubleshooting are Integrated Secure Remote Services and Centralized Secure Connect.

For proper functionality:

- At least one DNS server must be configured on the storage system.
- The storage system must have unrestricted access to Support Center over the Internet using HTTPS (for nonproxy environments).
- Online support full-access account is required.
  - User contact information and specific credentials that are associated with the site ID, which is associated with the system serial number.
  - If there is a problem with the user Online Support account, support personnel can help with the configuration using their RSA credentials.

Secure Connect Gateway - Readiness Check

Readiness Check



EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is an automated health and system monitoring capability of your storage system. It sends issue notifications to Dell EMC, sends system data to CloudIQ and enables remote support when necessary.

⚠ ESRS is not configured.

Unisphere Settings Secure Connect Gateway configuration

To verify if the storage system is ready for Secure Remote Services configuration, select the **Readiness Check** option on the Secure Remote Services page.

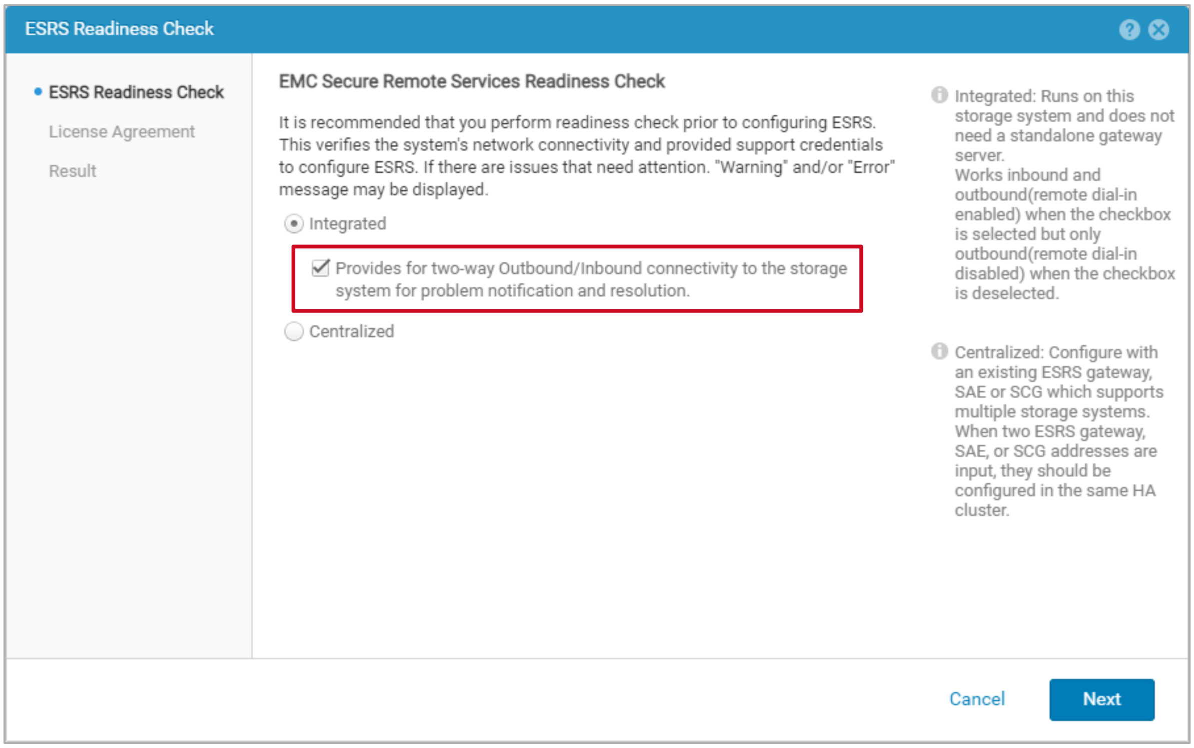
Dell Technologies recommends that you perform readiness check before configuring Secure Remote Services. The check verifies the system network connectivity and if the provided support credentials to configure Secure Remote Services are valid.

In the Secure Connect Gateway Readiness Check window, select the Secure Connect Gateway deployment option to configure

Integrated

To verify if the Unity XT storage system is ready for an Integrated Secure Connect Gateway deployment, select **Integrated**.

- Select the check box to configure two-way or uncheck it for one-way communication, and advance the step.



ESRS Readiness Check

- ESRS Readiness Check
- License Agreement
- Result

EMC Secure Remote Services Readiness Check

It is recommended that you perform readiness check prior to configuring ESRS. This verifies the system's network connectivity and provided support credentials to configure ESRS. If there are issues that need attention. "Warning" and/or "Error" message may be displayed.

● Integrated

☑ Provides for two-way Outbound/Inbound connectivity to the storage system for problem notification and resolution.

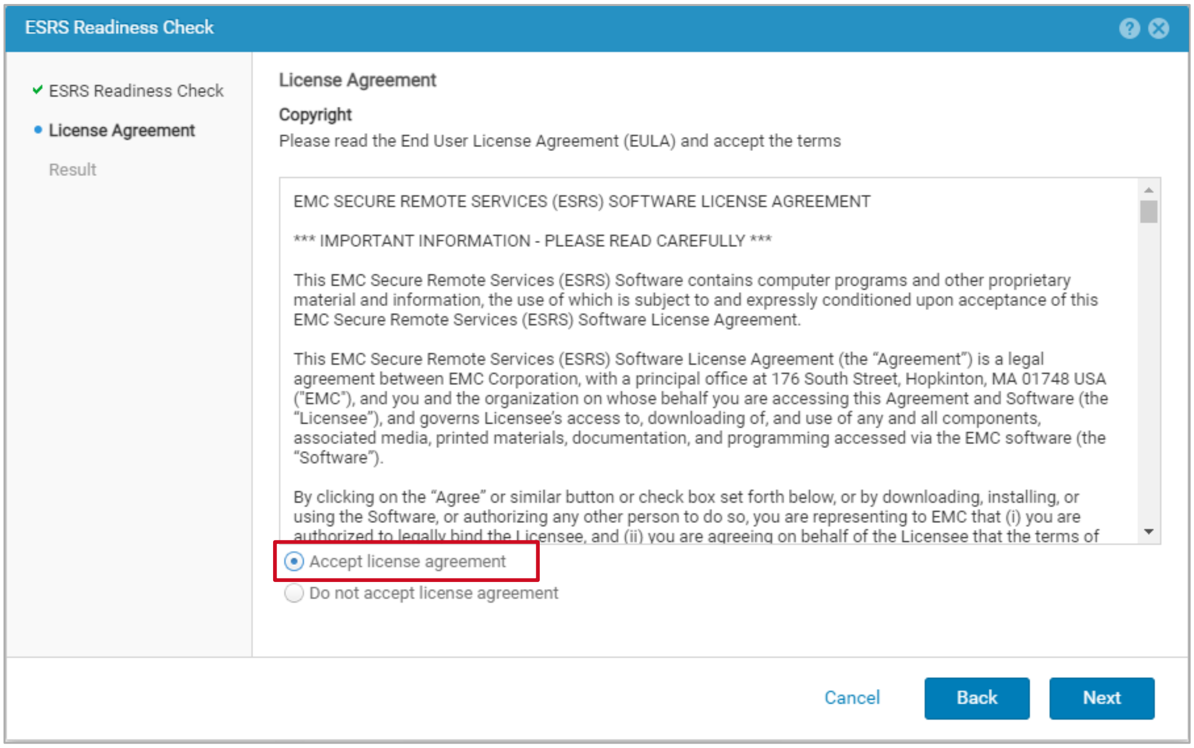
○ Centralized

Integrated: Runs on this storage system and does not need a standalone gateway server. Works inbound and outbound(remote dial-in enabled) when the checkbox is selected but only outbound(remote dial-in disabled) when the checkbox is deselected.

Centralized: Configure with an existing ESRS gateway, SAE or SCG which supports multiple storage systems. When two ESRS gateway, SAE, or SCG addresses are input, they should be configured in the same HA cluster.

ESRS Readiness Check window with integrated option selected

- Before the readiness check runs, the end user license agreement (EULA) must be accepted. Select **Accept license agreement**, and advance to the next step.



ESRS Readiness Check

✓ ESRS Readiness Check
• License Agreement
Result

License Agreement

Copyright

Please read the End User License Agreement (EULA) and accept the terms

EMC SECURE REMOTE SERVICES (ESRS) SOFTWARE LICENSE AGREEMENT

*** IMPORTANT INFORMATION - PLEASE READ CAREFULLY ***

This EMC Secure Remote Services (ESRS) Software contains computer programs and other proprietary material and information, the use of which is subject to and expressly conditioned upon acceptance of this EMC Secure Remote Services (ESRS) Software License Agreement.

This EMC Secure Remote Services (ESRS) Software License Agreement (the "Agreement") is a legal agreement between EMC Corporation, with a principal office at 176 South Street, Hopkinton, MA 01748 USA ("EMC"), and you and the organization on whose behalf you are accessing this Agreement and Software (the "Licensee"), and governs Licensee's access to, downloading of, and use of any and all components, associated media, printed materials, documentation, and programming accessed via the EMC software (the "Software").

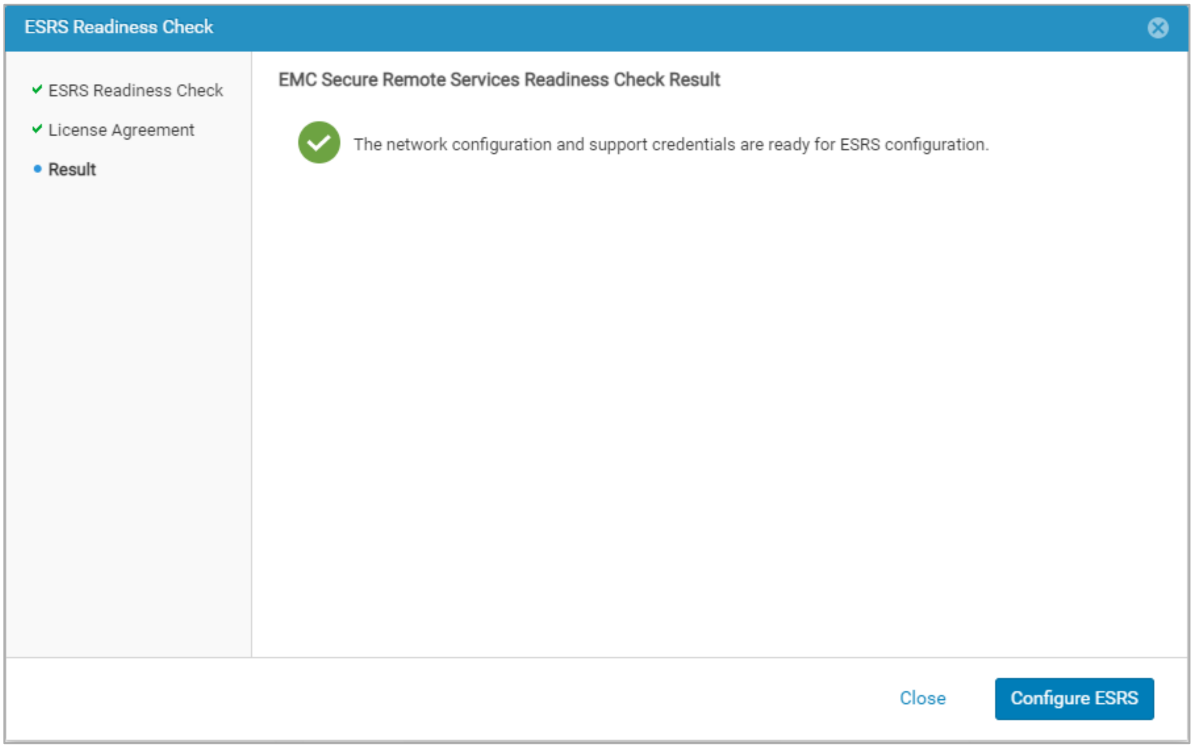
By clicking on the "Agree" or similar button or check box set forth below, or by downloading, installing, or using the Software, or authorizing any other person to do so, you are representing to EMC that (i) you are authorized to legally bind the Licensee, and (ii) you are agreeing on behalf of the Licensee that the terms of

● Accept license agreement

○ Do not accept license agreement

ESRS Readiness Check window with license agreement step

- After the readiness check runs, a results page is displayed.
  - If no errors are found, a successful message is displayed and you can select **Configure ESRS** to close the check and advance to the configuration.
  - However, If errors are displayed, a **Check Again** button is displayed and you must resolve the issues before running the new check.



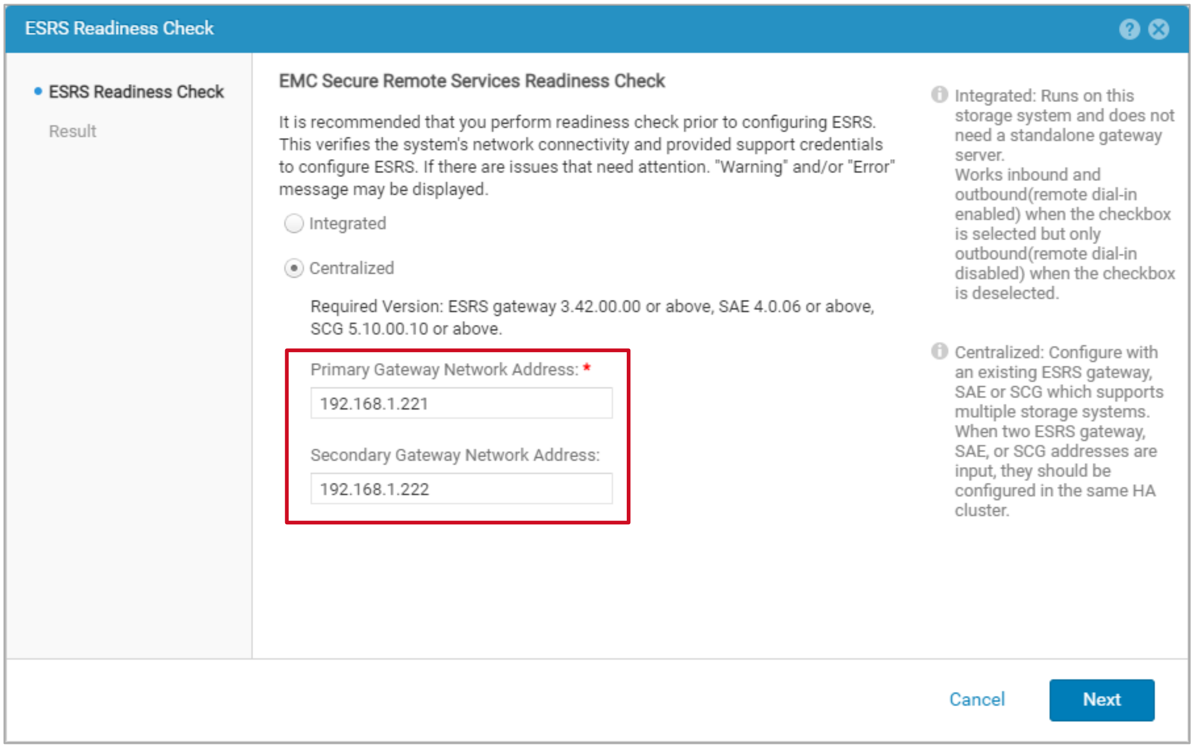
EMC Secure Remote Services Readiness Check Result

✓ The network configuration and support credentials are ready for ESRS configuration.

ESRS Readiness Check window showing the results of the readiness check

Centralized

After selecting the centralized option, enter the network address of the primary and secondary Secure Connect Gateway servers.



EMC Secure Remote Services Readiness Check

It is recommended that you perform readiness check prior to configuring ESRS. This verifies the system's network connectivity and provided support credentials to configure ESRS. If there are issues that need attention. "Warning" and/or "Error" message may be displayed.

○ Integrated

● Centralized

Required Version: ESRS gateway 3.42.00.00 or above, SAE 4.0.06 or above, SCG 5.10.00.10 or above.

Primary Gateway Network Address: * 192.168.1.221

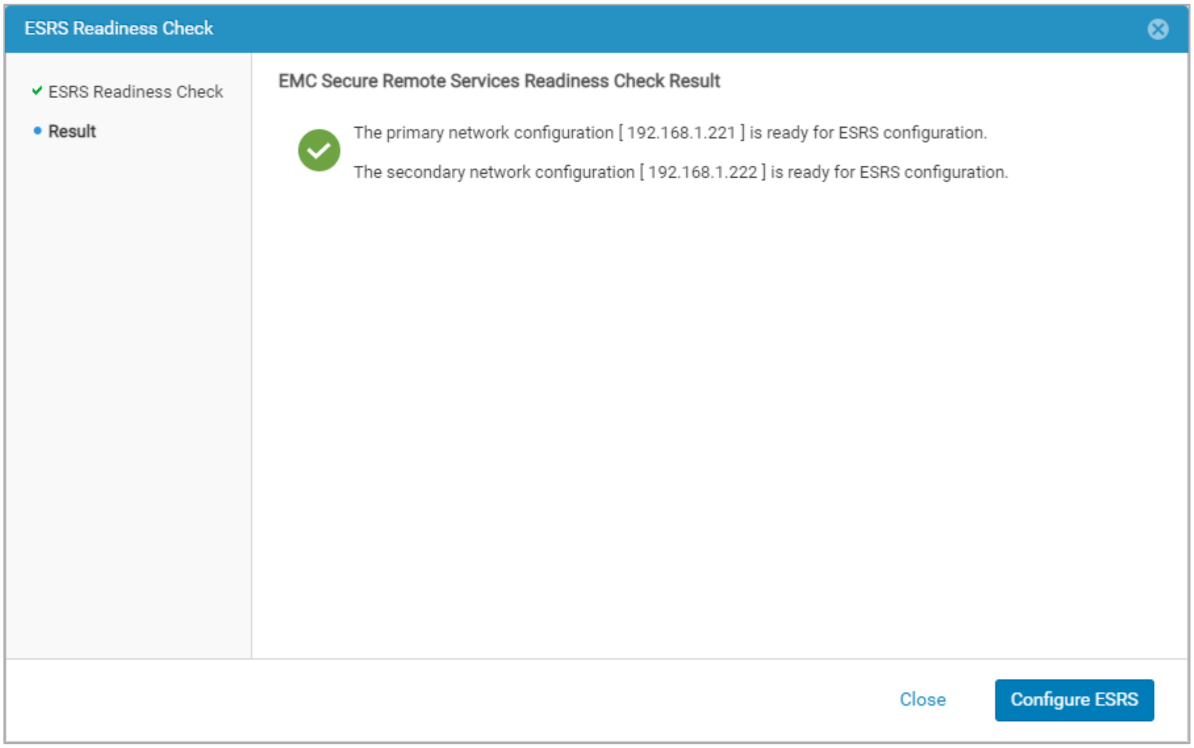
Secondary Gateway Network Address: 192.168.1.222

Integrated: Runs on this storage system and does not need a standalone gateway server. Works inbound and outbound(remote dial-in enabled) when the checkbox is selected but only outbound(remote dial-in disabled) when the checkbox is deselected.

Centralized: Configure with an existing ESRS gateway, SAE or SCG which supports multiple storage systems. When two ESRS gateway, SAE, or SCG addresses are input, they should be configured in the same HA cluster.

ESRS Readiness Check window with centralized option selected

- After the readiness check runs, a results page is displayed.
  - If no errors are found, a successful message is displayed and you can select **Configure ESRS** to close the check and advance to the configuration.
  - However, If errors are displayed, a **Check Again** button is displayed and you must resolve the issues before running the new check.



EMC Secure Remote Services Readiness Check Result

✓ The primary network configuration [192.168.1.221] is ready for ESRS configuration.

The secondary network configuration [192.168.1.222] is ready for ESRS configuration.

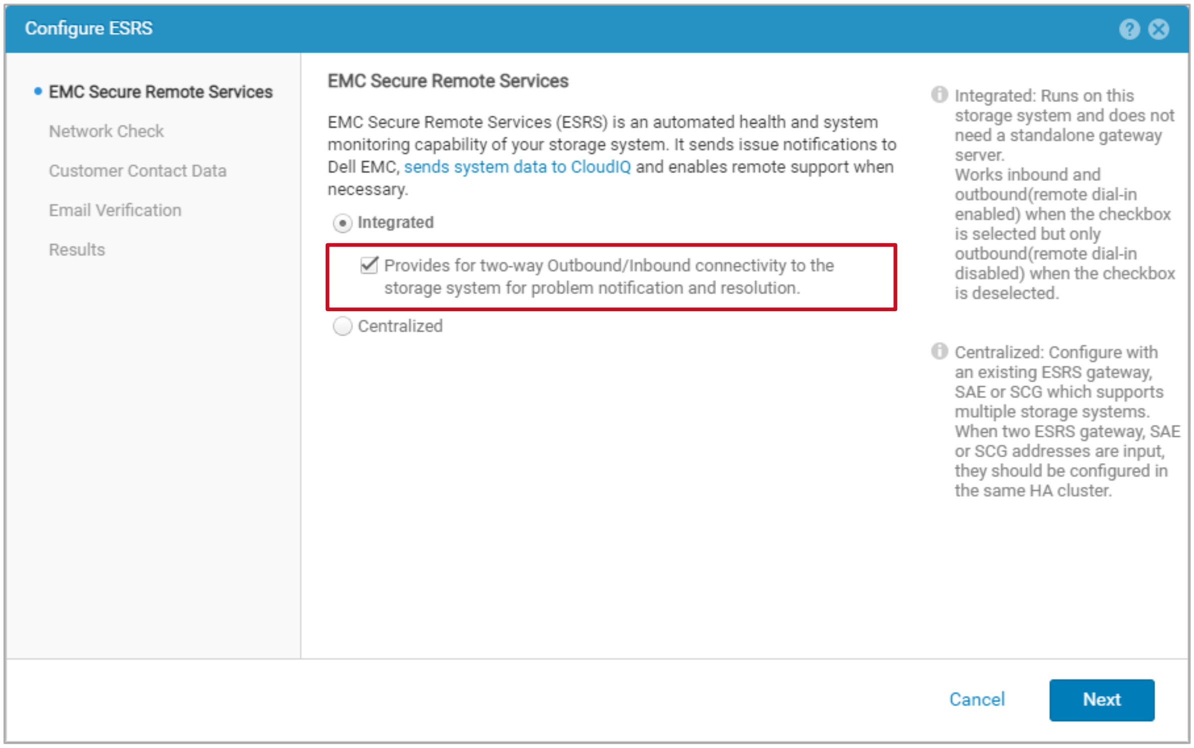
ESRS Readiness Check window showing the results of the readiness check

Secure Connect Gateway Configuration - Integrated

Integrated SCG

To configure Integrated Secure Connect Gateway on the storage system, the user must select **Integrated** on the Secure Remote Services page.

- Select the check box to configure two-way or uncheck it for one-way communication, and advance the step.



Configure ESRS

EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is an automated health and system monitoring capability of your storage system. It sends issue notifications to Dell EMC, sends system data to CloudIQ and enables remote support when necessary.

● Integrated

☑ Provides for two-way Outbound/Inbound connectivity to the storage system for problem notification and resolution.

○ Centralized

Integrated: Runs on this storage system and does not need a standalone gateway server.
Works inbound and outbound(remote dial-in enabled) when the checkbox is selected but only outbound(remote dial-in disabled) when the checkbox is deselected.

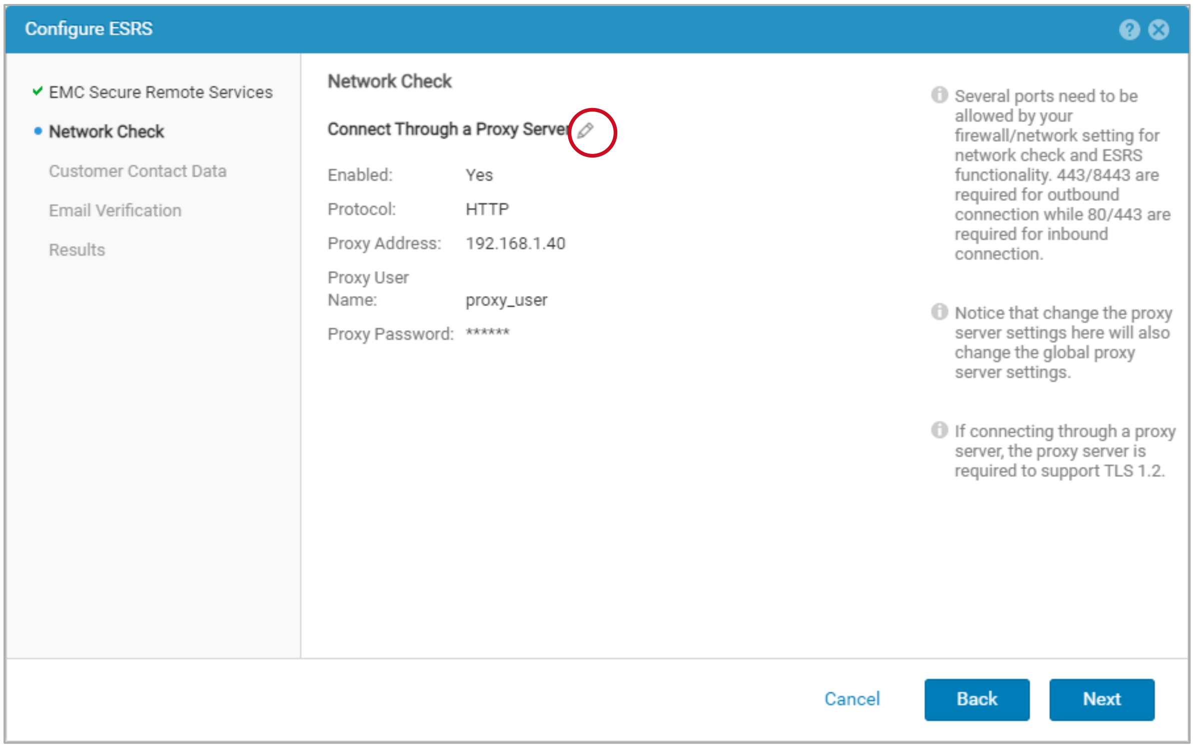
Centralized: Configure with an existing ESRS gateway, SAE or SCG which supports multiple storage systems. When two ESRS gateway, SAE or SCG addresses are input, they should be configured in the same HA cluster.

Configure ESRS wizard window with integrated option selected

Network Check

If a proxy server has been configured for the storage system, the server information is displayed on this page.

- To add a proxy server or modify the configuration select the **pencil** icon beside the **Connect Through a Proxy Server** option.



Network Check

Connect Through a Proxy Server

Enabled: Yes

Protocol: HTTP

Proxy Address: 192.168.1.40

Proxy User Name: proxy_user

Proxy Password: ******

Several ports need to be allowed by your firewall/network setting for network check and ESRS functionality. 443/8443 are required for outbound connection while 80/443 are required for inbound connection.

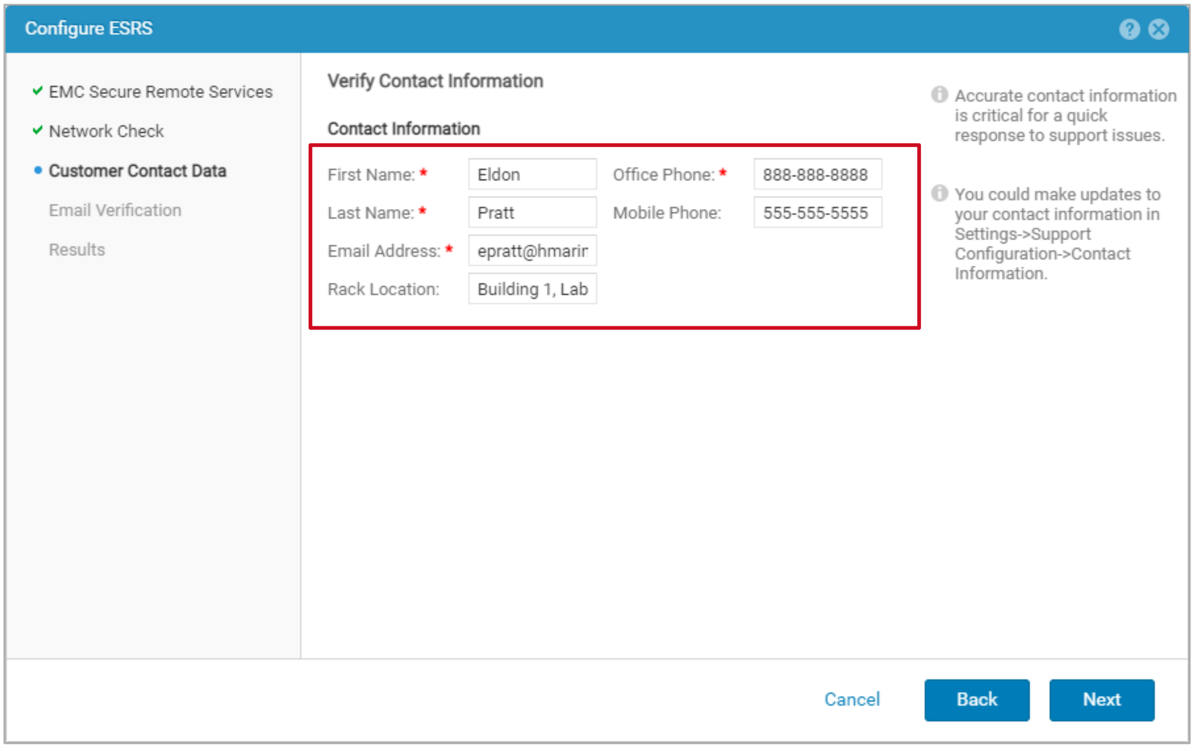
Notice that change the proxy server settings here will also change the global proxy server settings.

If connecting through a proxy server, the proxy server is required to support TLS 1.2.

Configure ESRS wizard window showing the proxy configuration determined by the network check.

Contact Information

Verify the customer contact data information and make any edits if required. Select **NEXT** to advance the step.



Configure ESRS

✓ EMC Secure Remote Services
✓ Network Check
● Customer Contact Data
Email Verification
Results

Verify Contact Information

Contact Information

First Name: *	Eldon	Office Phone: *	888-888-8888
Last Name: *	Pratt	Mobile Phone:	555-555-5555
Email Address: *	epratt@hmarir		
Rack Location:	Building 1, Lab		

Accurate contact information is critical for a quick response to support issues.

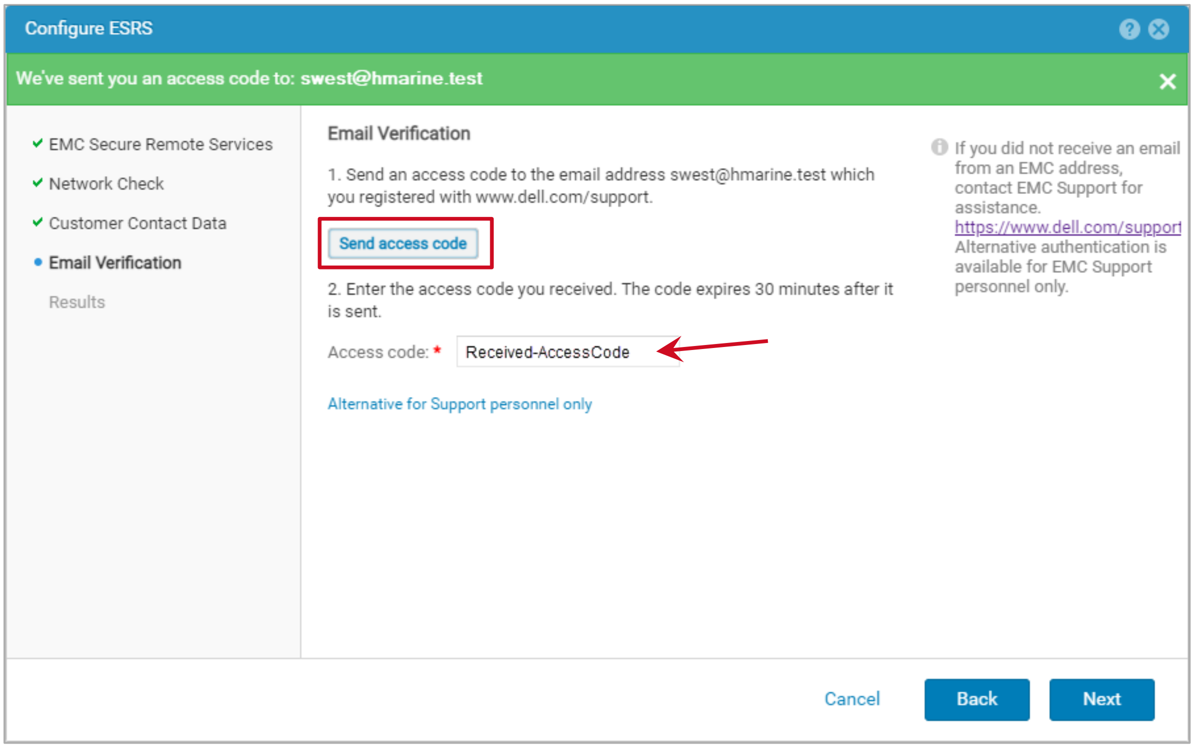
You could make updates to your contact information in Settings->Support Configuration->Contact Information.

Configure ESRS wizard window showing the contact data information

Email Verification

In the email verification process, select the **Send access code** to start a request for an access code.

- This option is unavailable if valid support credentials are not configured.



We've sent you an access code to: swest@hmarine.test

Email Verification

1. Send an access code to the email address swest@hmarine.test which you registered with www.dell.com/support.

2. Enter the access code you received. The code expires 30 minutes after it is sent.

Access code: * Received-AccessCode

If you did not receive an email from an EMC address, contact EMC Support for assistance. https://www.dell.com/support Alternative authentication is available for EMC Support personnel only.

Configure ESRS wizard with Email verification

A message is sent to the contact email with a generated 8-digit PIN access code which is valid for 30 minutes from the generated time.

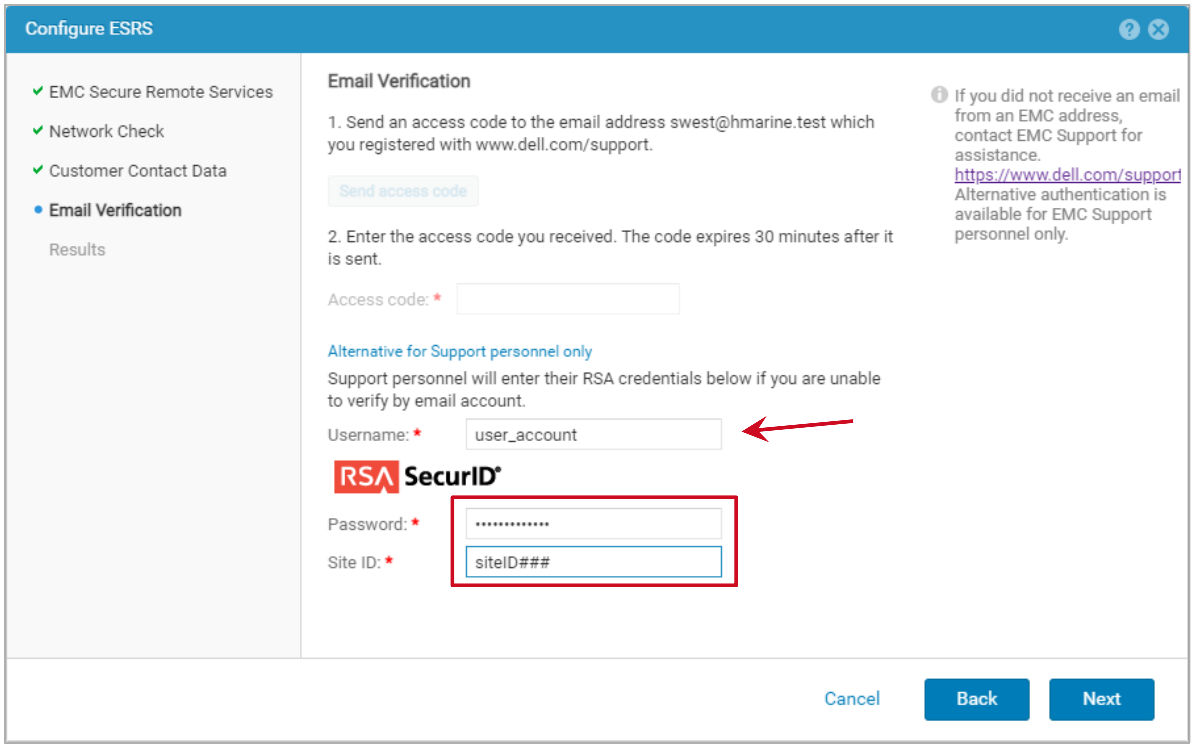
This code must be entered in the **Access code** field.

Select **Next** to advance the step.

RSA Credentials

If there is a problem with the user Online Support account, Dell support can help with the configuration by selecting the **Alternative for Support Personnel only**.

And then enter the RSA credentials and site ID on the proper fields to browse the Secure Connect Gateway configuration. Select **Next** to continue.



Configure ESRS

Email Verification

1. Send an access code to the email address swest@hmarine.test which you registered with www.dell.com/support.

2. Enter the access code you received. The code expires 30 minutes after it is sent.

Access code: *

Alternative for Support personnel only

Support personnel will enter their RSA credentials below if you are unable to verify by email account.

Username: * user_account

Password: * •••••••••••••

Site ID: * siteID###

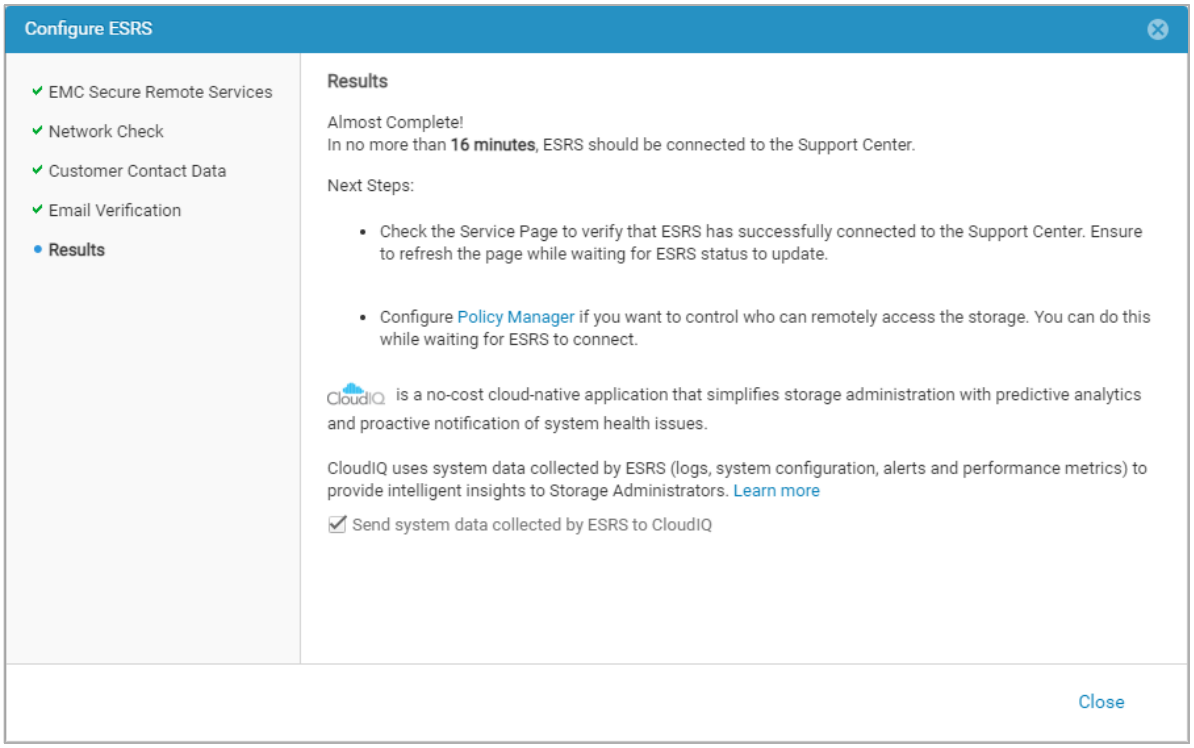
If you did not receive an email from an EMC address, contact EMC Support for assistance. https://www.dell.com/support Alternative authentication is available for EMC Support personnel only.

Configure ESRS wizard customer account validation using RSA credentials

The system starts initializing the Secure Connect Gateway. The Support Personnel RSA credentials are requested once again to finish the configuration. A new token code must be entered (only if the Alternative for Support personnel was invoked).

Results

The results page notifies that Secure Connect Gateway should be connected to the Support Center in 15 minutes. The user can monitor the status of the Secure Connect Gateway connectivity on the Service page, and configure Policy Manager while waiting for Secure Connect Gateway to connect.



Results

Almost Complete!
In no more than **16 minutes**, ESRS should be connected to the Support Center.

Next Steps:

- Check the Service Page to verify that ESRS has successfully connected to the Support Center. Ensure to refresh the page while waiting for ESRS status to update.
- Configure Policy Manager if you want to control who can remotely access the storage. You can do this while waiting for ESRS to connect.

CloudIQ is a no-cost cloud-native application that simplifies storage administration with predictive analytics and proactive notification of system health issues.

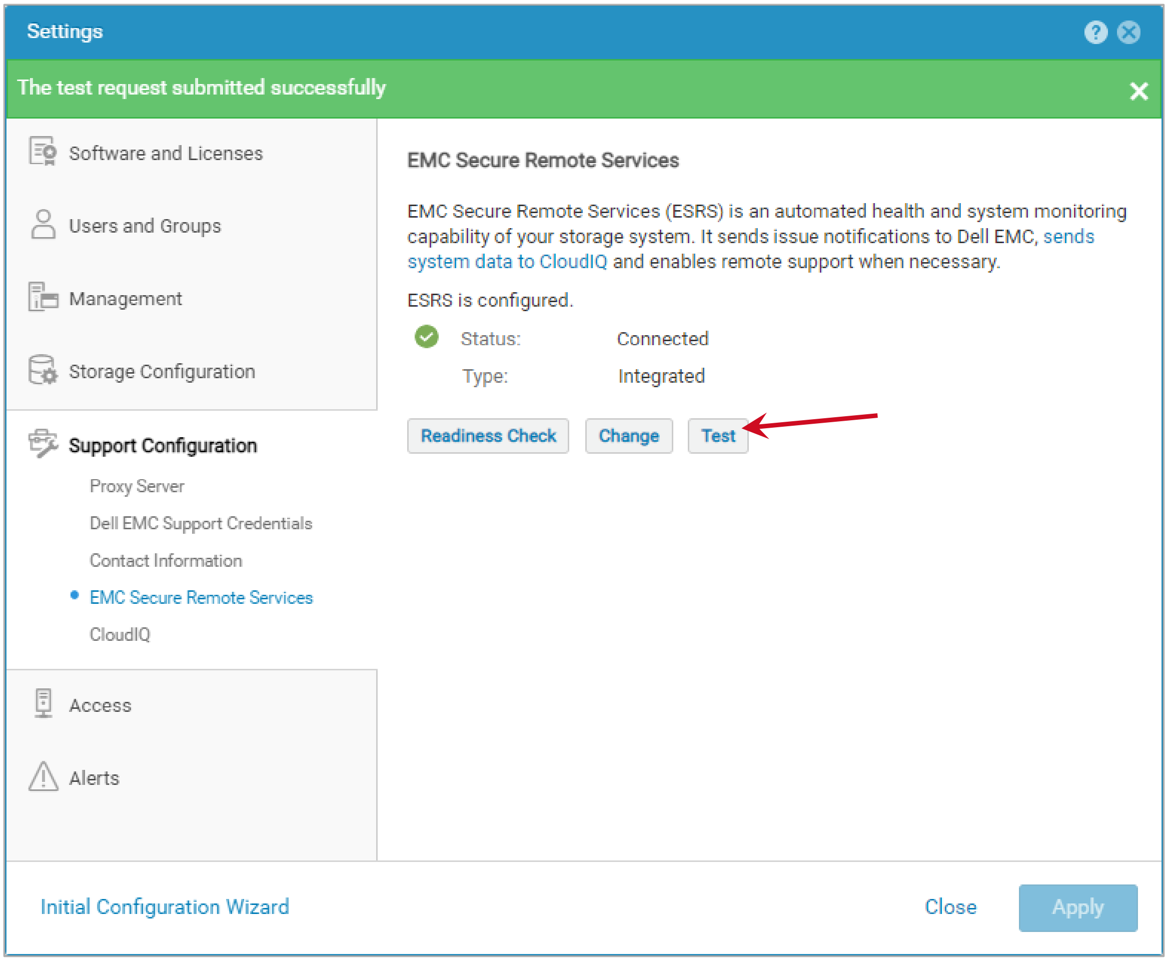
CloudIQ uses system data collected by ESRS (logs, system configuration, alerts and performance metrics) to provide intelligent insights to Storage Administrators. Learn more

☑ Send system data collected by ESRS to CloudIQ

Configure ESRS wizard results page

SCG Configured

The Secure Remote Services page show the status of the connection and which type of Secure Connect Gateway configuration is saved to the system.



The test request submitted successfully

EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is an automated health and system monitoring capability of your storage system. It sends issue notifications to Dell EMC, sends system data to CloudIQ and enables remote support when necessary.

ESRS is configured.

Status: Connected

Type: Integrated

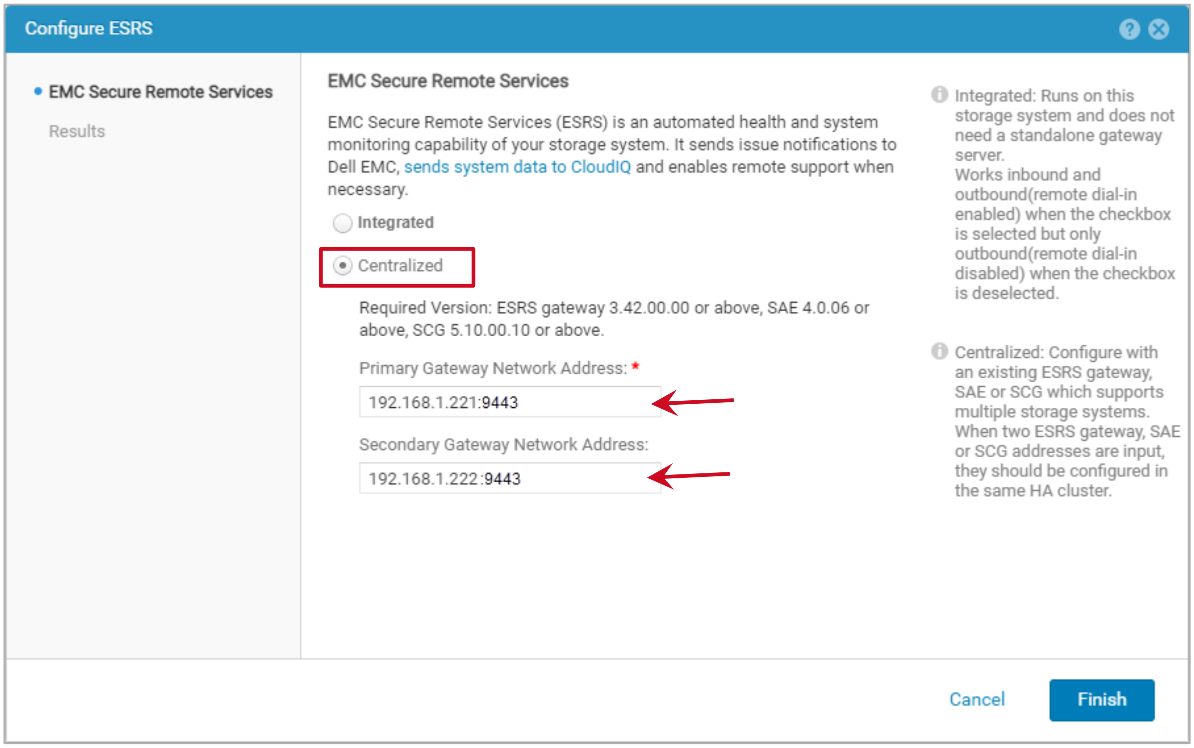
Unisphere Settings Secure Connect Gateway configuration

Secure Connect Gateway Configuration - Centralized

Centralized SCG

Select the **Centralized** option in the Secure Remote Services page.

- If the Secure Connect Gateway End User License Agreement (EULA) was not yet accepted the license would be the next step.



EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is an automated health and system monitoring capability of your storage system. It sends issue notifications to Dell EMC, sends system data to CloudIQ and enables remote support when necessary.

○ Integrated

● Centralized

Required Version: ESRS gateway 3.42.00.00 or above, SAE 4.0.06 or above, SCG 5.10.00.10 or above.

Primary Gateway Network Address: *
192.168.1.221:9443

Secondary Gateway Network Address:
192.168.1.222:9443

Integrated: Runs on this storage system and does not need a standalone gateway server.
Works inbound and outbound(remote dial-in enabled) when the checkbox is selected but only outbound(remote dial-in disabled) when the checkbox is deselected.

Centralized: Configure with an existing ESRS gateway, SAE or SCG which supports multiple storage systems. When two ESRS gateway, SAE or SCG addresses are input, they should be configured in the same HA cluster.

Configure ESRS wizard window with Centralized option selected

Specify the Primary gateway network address of the Secure Connect Gateway virtual appliance server that is used to connect to the Dell Enterprise.

- Ensure that the port 9443 is open between the server and the storage system.

RSA credentials can be used for Primary Gateway configuration without a Customer Support account.

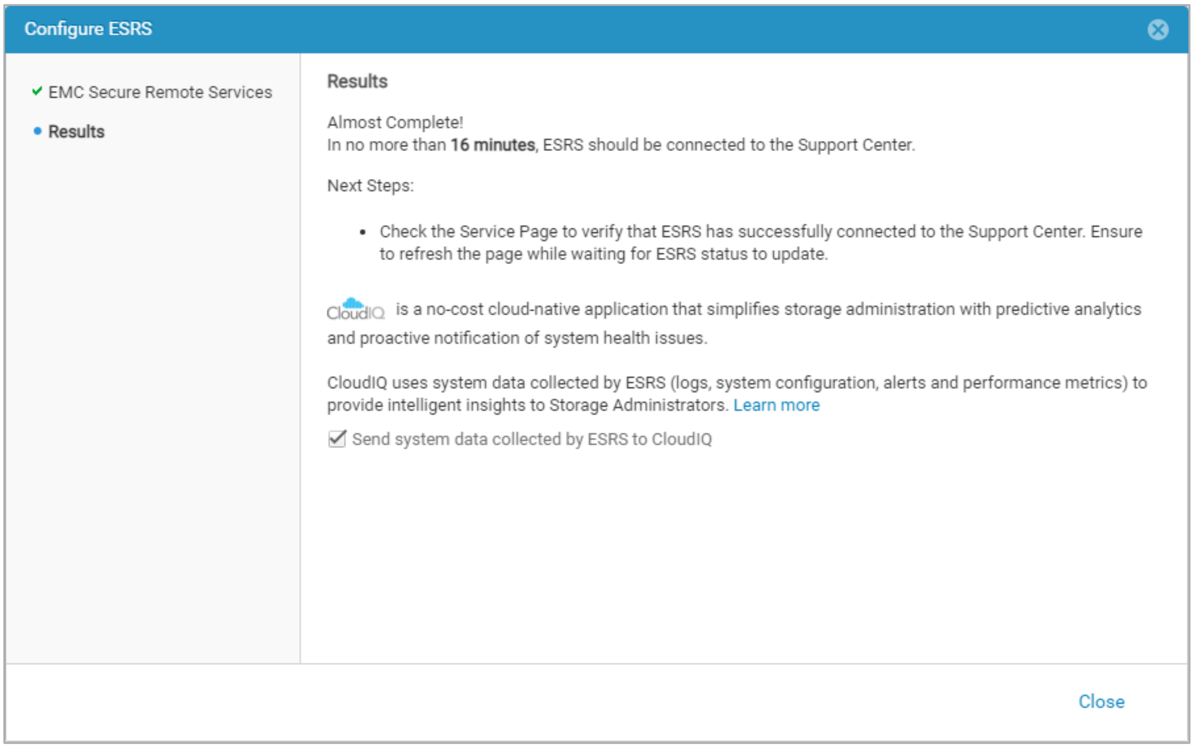
- This alternative enables the Secure Connect Gateway configuration while support account credentials are being created and validated on the backend.

- If a Secondary Gateway network address was also entered in the configuration, then the RSA credentials are required one more time.
- The RSA credentials that were used for the primary gateway must be also provided to complete the configuration of the second gateway.

After you click **Next**,the system starts initializing Secure Connect Gateway.

Results

The results page notifies that Secure Connect Gateway should be connected to the Support Center in 16 minutes. The user can monitor the status of the Secure Connect Gateway connectivity on the Service page.



Results

Almost Complete!
In no more than **16 minutes**, ESRS should be connected to the Support Center.

Next Steps:

- Check the Service Page to verify that ESRS has successfully connected to the Support Center. Ensure to refresh the page while waiting for ESRS status to update.

CloudIQ is a no-cost cloud-native application that simplifies storage administration with predictive analytics and proactive notification of system health issues.

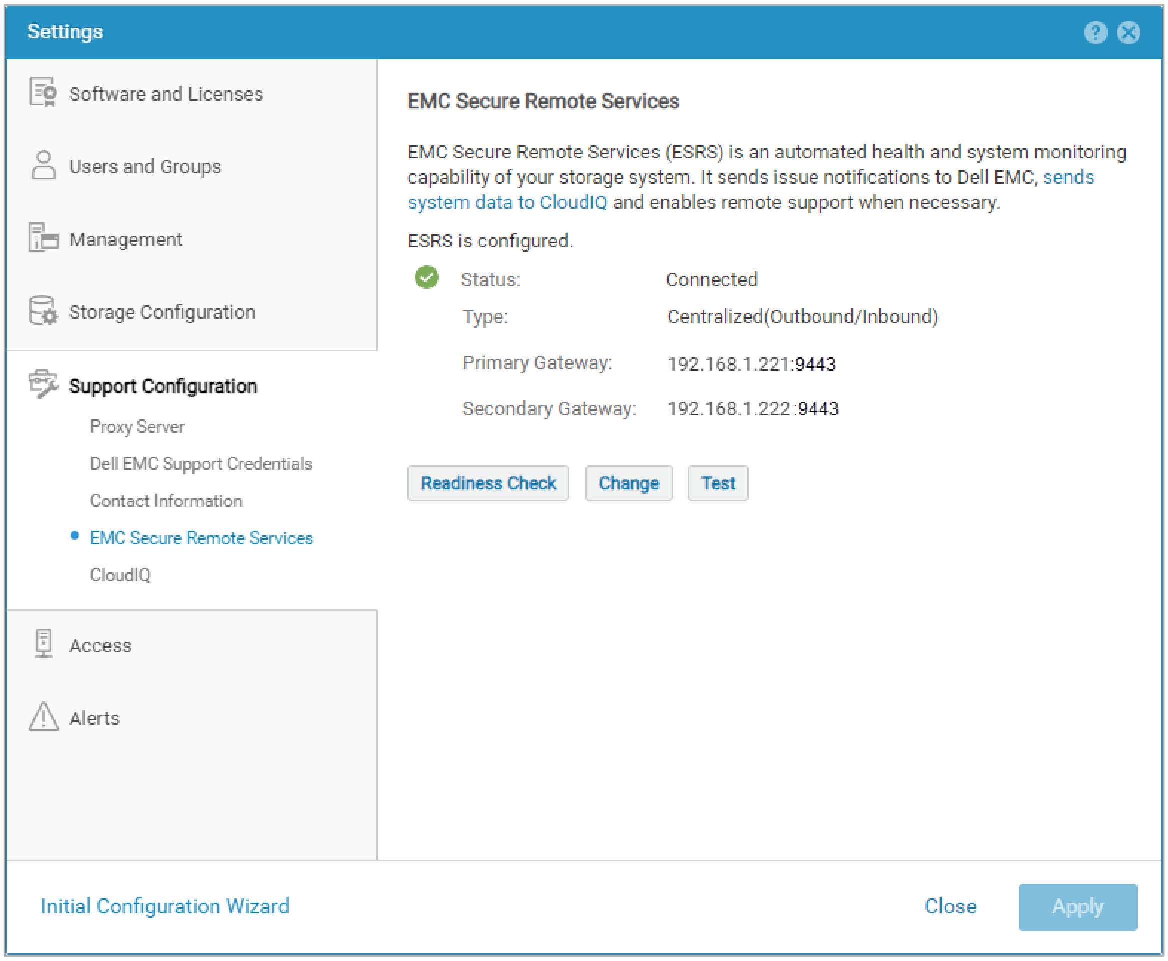
CloudIQ uses system data collected by ESRS (logs, system configuration, alerts and performance metrics) to provide intelligent insights to Storage Administrators. Learn more

☑ Send system data collected by ESRS to CloudIQ

Configure ESRS wizard results page

SCG Configured

The Secure Remote Services page show the status of the connection and which type of Secure Connect Gateway configuration is saved to the system.



EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is an automated health and system monitoring capability of your storage system. It sends issue notifications to Dell EMC, sends system data to CloudIQ and enables remote support when necessary.

ESRS is configured.

Status:	Connected
Type:	Centralized(Outbound/Inbound)
Primary Gateway:	192.168.1.221:9443
Secondary Gateway:	192.168.1.222:9443

Unisphere Settings Secure Connect Gateway configuration

Activity: Unisphere Tour

During this lab, you will:

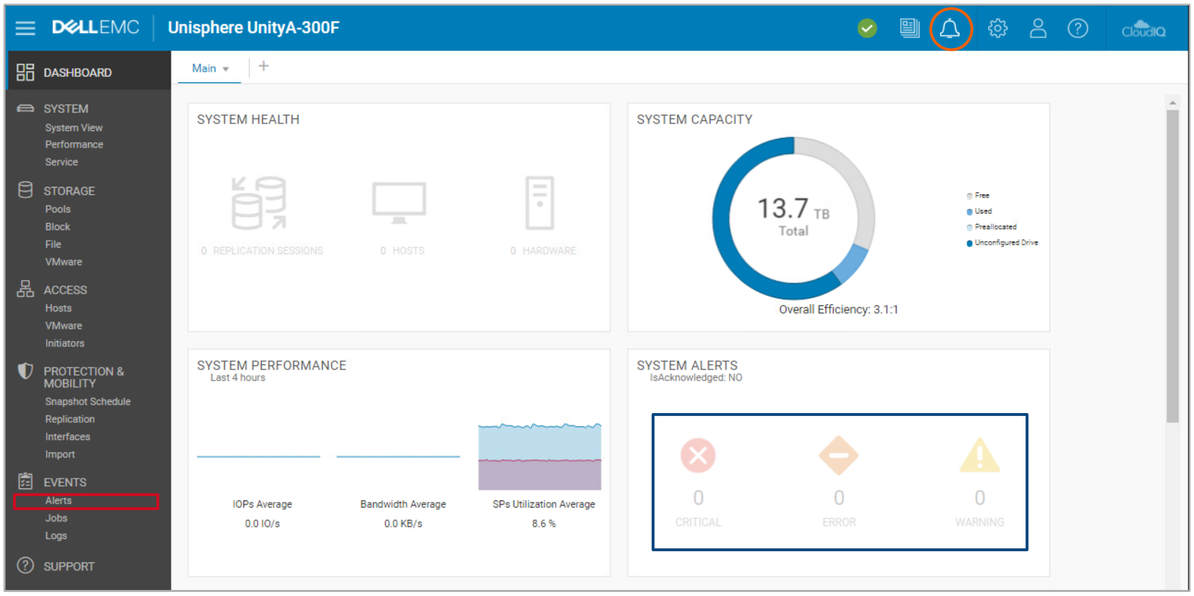
- Explore the Unisphere UI dashboard, preferences, and help options.
- View the system components and check storage system health.
- View the system settings page, and explore the sections.
- Create a user account with an associated role.

Unisphere Alerts and Events Monitoring

Unisphere Alerts and Events Monitoring

Unisphere System Alerts

Alerts are usually events that require attention from the system administrator. Some alerts indicate that there is a problem with the Dell Unity system. For example, you might receive an alert telling you that a disk has faulted, or that the storage system is running out of space.



Unisphere UI with dashboard view and the three methods used for alerts monitoring

Alerts are registered to the **System Alerts** page in Unisphere. Access the page using one of three methods

- Select the link on the top menu bar.
- Select the option on the navigation pane.
- Select notification icons on the dashboard view block.

The view block on the dashboard shows an icon with the number of alerts for each recorded severity category.

- The link on these icons opens the Alerts page, showing the records filtered by the selected **severity level**.

System Alerts Severity Levels

System alerts with their severity levels are recorded on the **System Alerts** page. Logging levels are not configurable.

The table provides an explanation about the alert severity levels from least to most severe.

Icon	Label	Indicates
ℹ	Information	An event has occurred that does not impact system functions. No action is required.
ℹ	Notice	An event has occurred that does not impact system functions. No action is required.
⚠	Warning	An error has occurred that the user should be aware of but does not have a significant impact on the system. For example, a component is working, but its performance may not be optimum.
⛔	Error	An error has occurred that has a minor impact on the system and should be remedied—no need to fix immediately. For example, a component is failing and some or all its functions may be degraded or not working.
✖	Critical	An error has occurred that has a significant impact on the system and should be remedied immediately. For example, a component is missing or has failed and recovery may not be possible.

Tip: Two of these severity levels are identified by the same icon and refer to events that require no user intervention: Information and Notice. **Information** alerts report the status of a system component or changes to a storage resource condition. **Notice** alerts normally report the status of a system process that is triggered by service commands.

System Alerts States

There are multiple ways to review the health of a Dell Unity system. In the Unisphere UI, the storage administrator can review the **System Health** view block on the dashboard, and the **System View** page. The user can also check the Alerts page for resolved issues.

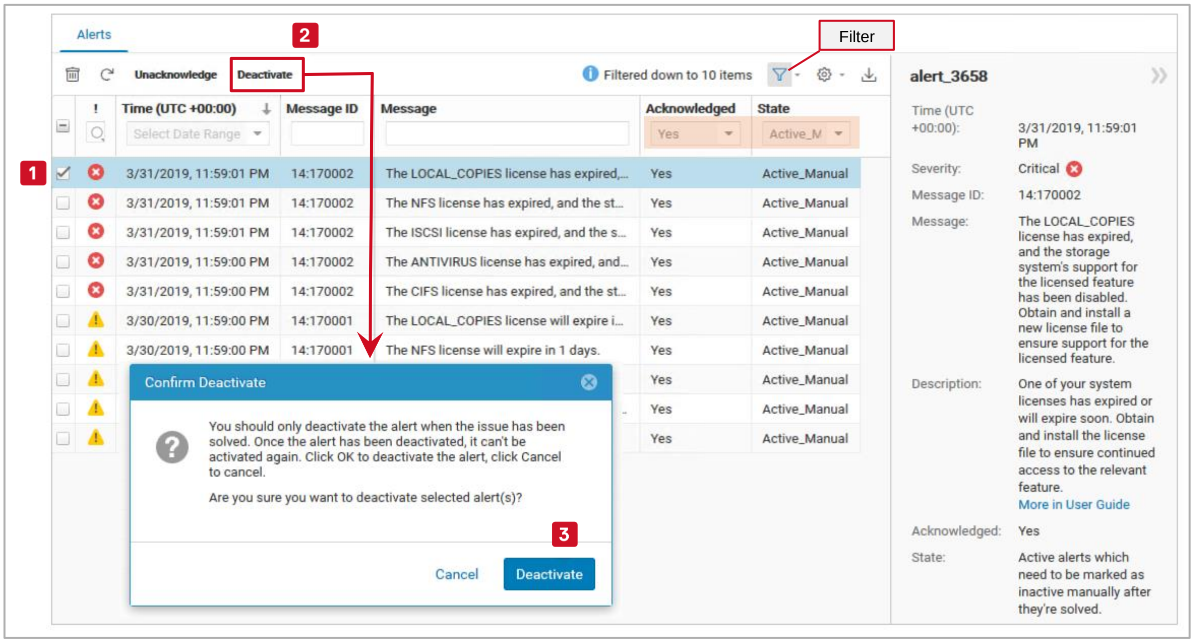
The Alerts page shows the event log with all alerts that have occurred in the system.

- Alert states are used to help the user determine which records are current, and which records are resolved.
- An alert state changes when the software OE is upgraded, the error condition is resolved, and the alert is repeating.

Alert State	Description
Active_Manual	Status when the alert is active and must be manually cleared. The alert is still Active, and a user must deactivate the alert to mark it Inactive once the condition is solved.
Active_Auto	Status when the alert is active but will be automatically cleared when the issue is resolved. The alert is still Active and will be marked Inactive automatically once the condition is cleared.
Inactive	Status when the alert is no longer active because it has been resolved. The alert condition has been resolved.
Updating	Status when the alert is transitioning between the other states: Active_Auto to Inactive, Active_Manual to Inactive.

Manage Alerts

The System Alerts page in Unisphere is accessed by selecting **Alerts** on the navigation pane under the Events section.



	!	Time (UTC +00:00)	Message ID	Message	Acknowledged	State
		Select Date Range			Yes	Active_M
☑	⊗	3/31/2019, 11:59:01 PM	14:170002	The LOCAL_COPIES license has expired,...	Yes	Active_Manual
□	⊗	3/31/2019, 11:59:01 PM	14:170002	The NFS license has expired, and the st...	Yes	Active_Manual
□	⊗	3/31/2019, 11:59:01 PM	14:170002	The ISCSI license has expired, and the s...	Yes	Active_Manual
□	⊗	3/31/2019, 11:59:00 PM	14:170002	The ANTIVIRUS license has expired, and...	Yes	Active_Manual
□	⊗	3/31/2019, 11:59:00 PM	14:170002	The CIFS license has expired, and the st...	Yes	Active_Manual
□	⚠	3/30/2019, 11:59:00 PM	14:170001	The LOCAL_COPIES license will expire i...	Yes	Active_Manual
□	⚠	3/30/2019, 11:59:00 PM	14:170001	The NFS license will expire in 1 days.	Yes	Active_Manual
□	⚠				Yes	Active_Manual
□	⚠				Yes	Active_Manual
□	⚠				Yes	Active_Manual

Confirm Deactivate

You should only deactivate the alert when the issue has been solved. Once the alert has been deactivated, it can't be activated again. Click OK to deactivate the alert, click Cancel to cancel.

Are you sure you want to deactivate selected alert(s)?

alert_3658

Time (UTC +00:00):	3/31/2019, 11:59:01 PM
Severity:	Critical ⊗
Message ID:	14:170002
Message:	The LOCAL_COPIES license has expired, and the storage system's support for the licensed feature has been disabled. Obtain and install a new license file to ensure support for the licensed feature.
Description:	One of your system licenses has expired or will expire soon. Obtain and install the license file to ensure continued access to the relevant feature. More in User Guide
Acknowledged:	Yes
State:	Active alerts which need to be marked as inactive manually after they're solved.

Unisphere System alerts page

In Unisphere, the Alerts page is automatically filtered by default to show only the records in Active and Updating states. Records in an Inactive state are hidden.

In the example, the records were also filtered to show only the log entries already acknowledged by the user.

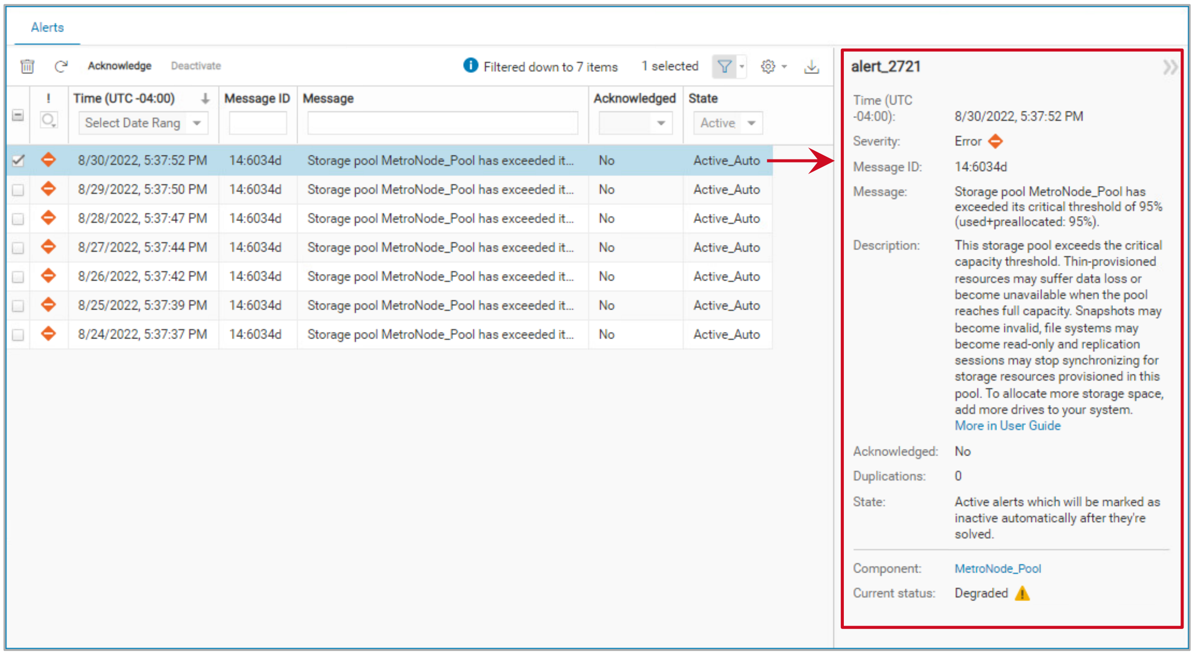
Active_Manual alerts must be manually deactivated by an Administrator. To deactivate an alert in Unisphere:

1. Select an alert that is in an **Active_Manual**state.
2. Select the **Deactivate** button.
3. A Confirm Deactivate dialog box is shown. Select **Deactivate** to continue

The dialog box is closed, and the record entry is marked as inactive. Because of the page filtering, the record entry is not displayed in the list of entries.

View Alerts Details

To view detailed information about a system alert, select the alert from the list of records of the **Alerts** Page.



	!	Time (UTC -04:00)	Message ID	Message	Acknowledged	State
☑	◆	8/30/2022, 5:37:52 PM	14:6034d	Storage pool MetroNode_Pool has exceeded it...	No	Active_Auto
□	◆	8/29/2022, 5:37:50 PM	14:6034d	Storage pool MetroNode_Pool has exceeded it...	No	Active_Auto
□	◆	8/28/2022, 5:37:47 PM	14:6034d	Storage pool MetroNode_Pool has exceeded it...	No	Active_Auto
□	◆	8/27/2022, 5:37:44 PM	14:6034d	Storage pool MetroNode_Pool has exceeded it...	No	Active_Auto
□	◆	8/26/2022, 5:37:42 PM	14:6034d	Storage pool MetroNode_Pool has exceeded it...	No	Active_Auto
□	◆	8/25/2022, 5:37:39 PM	14:6034d	Storage pool MetroNode_Pool has exceeded it...	No	Active_Auto
□	◆	8/24/2022, 5:37:37 PM	14:6034d	Storage pool MetroNode_Pool has exceeded it...	No	Active_Auto

alert_2721

Time (UTC -04:00):	8/30/2022, 5:37:52 PM
Severity:	Error ◆
Message ID:	14:6034d
Message:	Storage pool MetroNode_Pool has exceeded its critical threshold of 95% (used+preallocated: 95%).
Description:	This storage pool exceeds the critical capacity threshold. Thin-provisioned resources may suffer data loss or become unavailable when the pool reaches full capacity. Snapshots may become invalid, file systems may become read-only and replication sessions may stop synchronizing for storage resources provisioned in this pool. To allocate more storage space, add more drives to your system. More in User Guide
Acknowledged:	No
Duplications:	0
State:	Active alerts which will be marked as inactive automatically after they're solved.
Component:	MetroNode_Pool
Current status:	Degraded ⚠

Unisphere Alerts page with details of a selected alert

Details about the selected alert record are displayed in the right pane. The information includes:

- Time the event was logged.
- Severity level
- Alert message
- Description of the event
- Acknowledgement flag
- Component affected by the event
- Status of the component

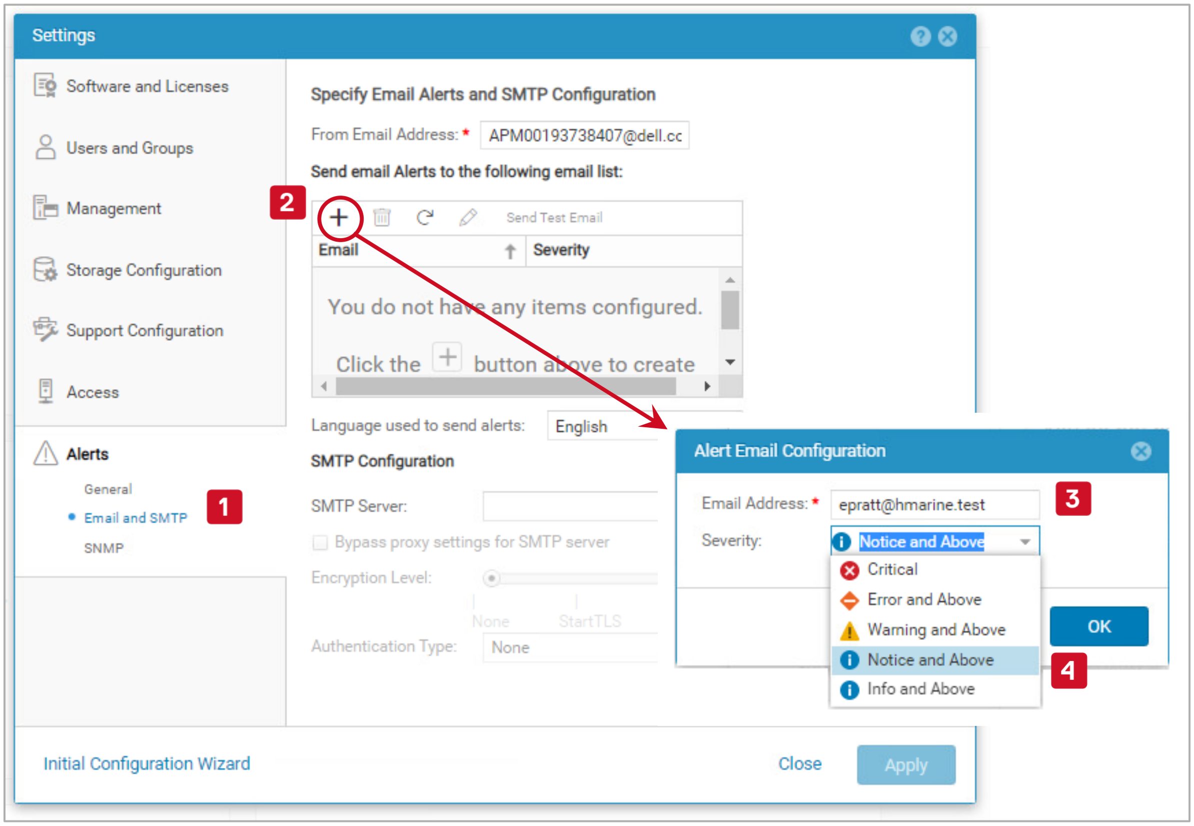
The example shows the details about theAlert_2721. Observe that the current status of the alert is **Degraded**, and the state is **Active_Auto.** The alert will transition to Inactive once the issue is resolved.

Unisphere can be configured to send the system administrator alert notifications. These notifications are sent through an email or through an SNMP message.

Configure Alert Notifications - Email

Email Address

A system administrator can configure Unisphere to send alert notifications in an email. Email alerts are used only for internal communication. No service requests are created based on the configured email alerts. Only the configuration of Secure Connect Gateway provides interaction with Dell support.



Specify Email Alerts and SMTP Configuration

From Email Address: * APM00193738407@dell.cc

Send email Alerts to the following email list:

You do not have any items configured.

Click the + button above to create

Language used to send alerts: English

Alert Email Configuration

Email Address: * epratt@hmarine.test

Severity: Notice and Above

Unisphere Settings Alerts section Email and SMTP

In Unisphere, open the **Settings** configuration window and expand the **Alerts** section:

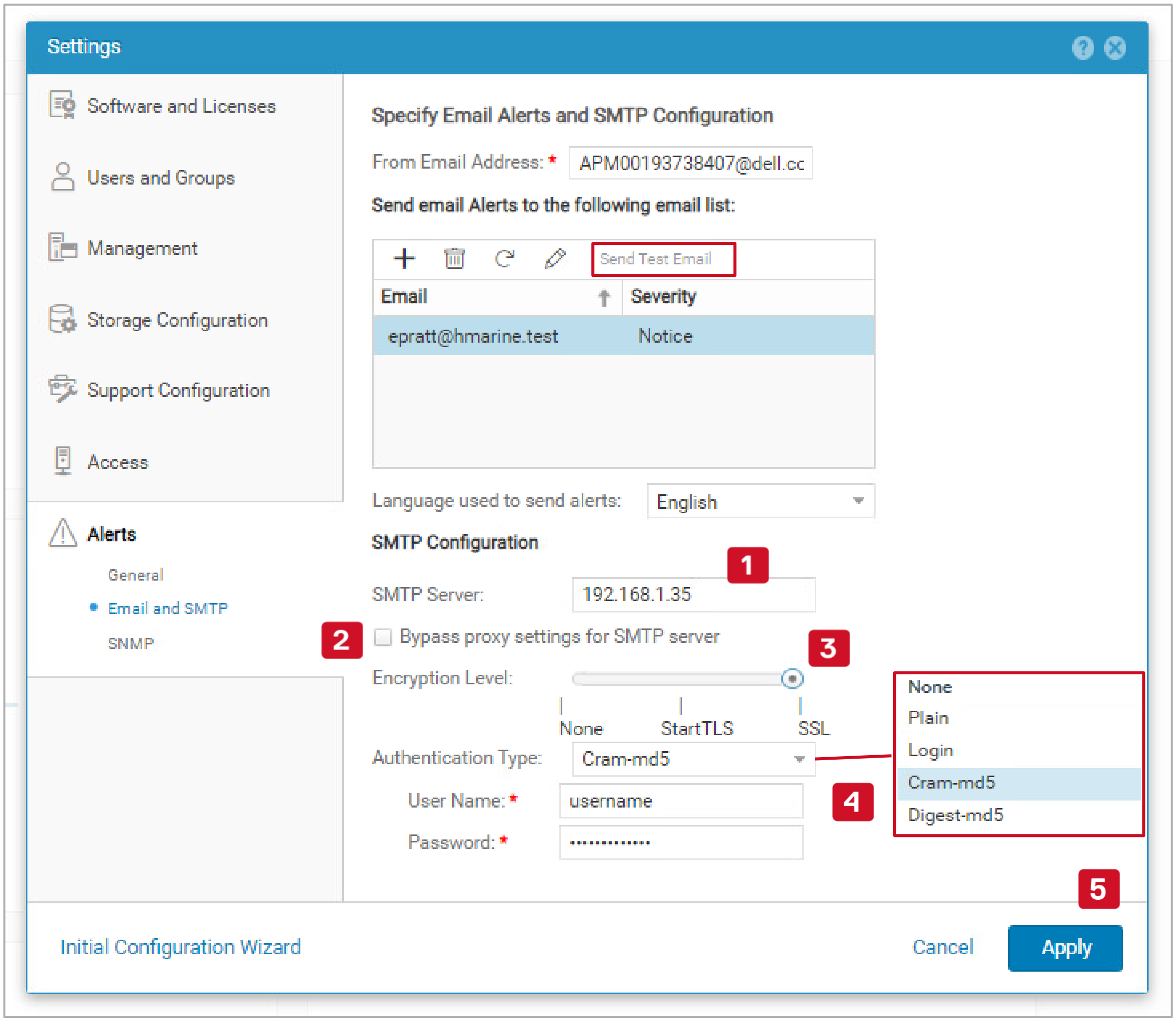
1. Select **Email and SMTP**, under the **Alerts** section.
2. On the **Specify Email Alerts and SMTP configuration**, click the **Add** icon.

3. The **Alert Email Configuration** window opens - enter the email that is supposed to receive the notification messages.
4. Select the severity level from the drop-down list, then select **OK** to save the configuration.

   - The dialog box closes, and the new email is displayed in the list of email messages.

The example shows the configuration of the email address **epratt@hmarine.test** as a recipient for notifications about issues with **Notice** and above severity levels.

SMTP Configuration



Specify Email Alerts and SMTP Configuration

From Email Address: * APM00193738407@dell.cc

Send email Alerts to the following email list:

Email	Severity
epratt@hmarine.test	Notice

Language used to send alerts: English

SMTP Configuration

SMTP Server: 192.168.1.35

☐ Bypass proxy settings for SMTP server

Encryption Level: None StartTLS SSL

Authentication Type: Cram-md5

User Name: * username

Password: * •••••••••••••

Unisphere Settings Alerts section Email and SMTP

On the **SMTP Configuration** section:

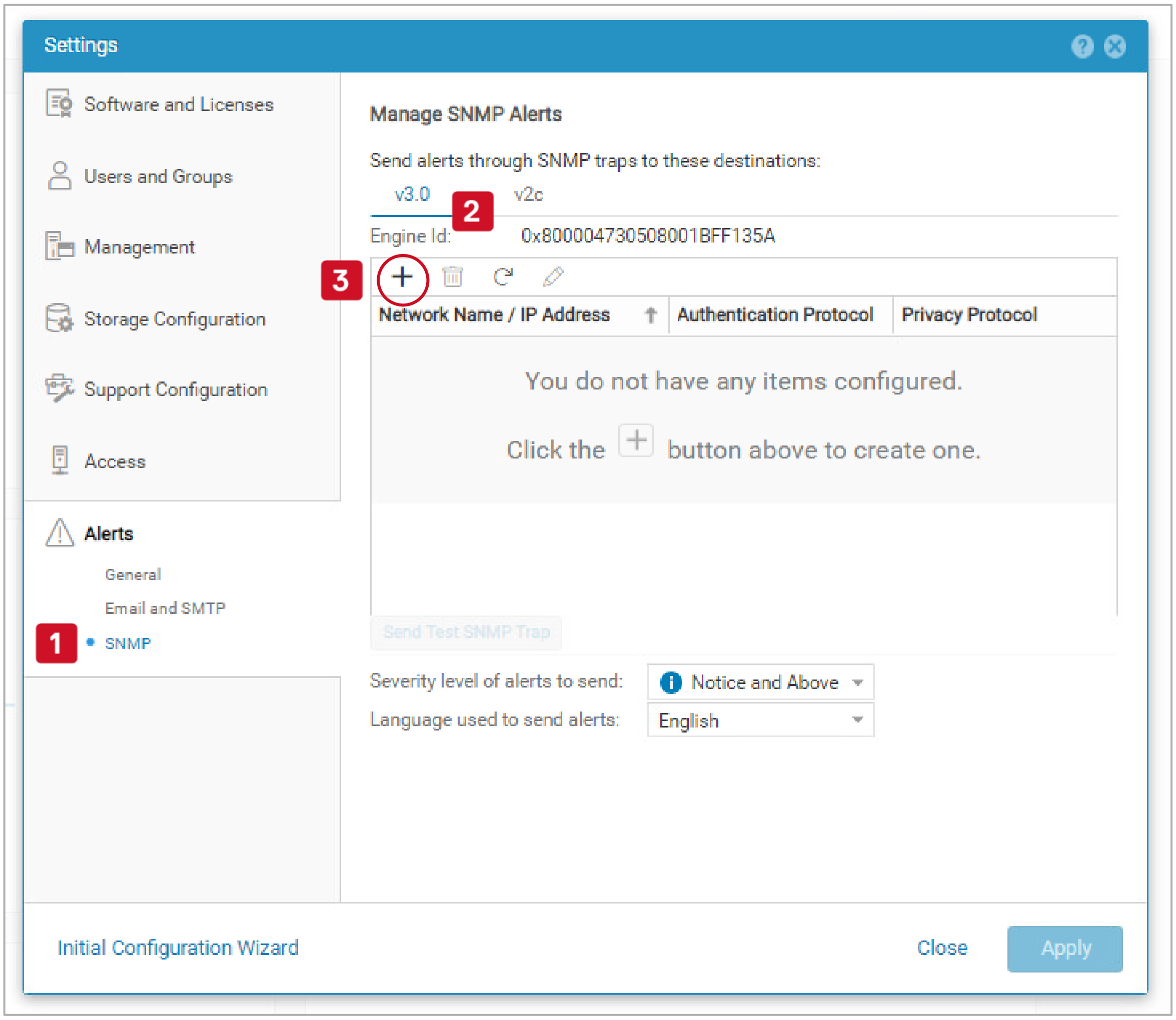
1. Type the **IP address** of the Simple Mail Transfer Protocol (SMTP) server that is used to send email messages.
2. Optionally, bypass the global proxy server settings that are typically used for SMTP email messages by checking the appropriate box.
3. Select the **Encryption Level** (SSL method) for the email server.
4. Specify the **Authentication Type**, and enter the authentication credentials.
5. Select **Apply** to commit the changes.

    - Optionally select **Send Test Email** to verify that the SMTP server and destination email addresses are valid.
    - The Send Test Email button is only available after changes to the email configuration.

Configure Alert Notifications - SNMP

SNMP Target

A system administrator can configure Unisphere to send alert notifications through a Simple Network Management Protocol (SNMP) message - known as a trap.



Manage SNMP Alerts

Send alerts through SNMP traps to these destinations:

Engine Id: 0x800004730508001BFF135A

You do not have any items configured.

Click the + button above to create one.

Severity level of alerts to send: Notice and Above

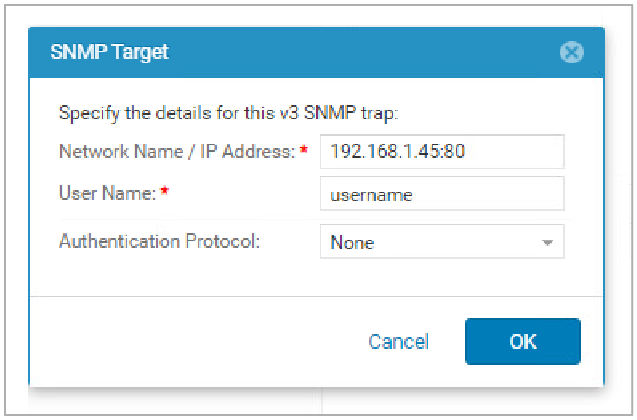
Language used to send alerts: English

Unisphere Settings Alerts section SNMP

Configure the SNMP trap destination targets in Unisphere:

1. From the **Settings** window, select **SNMP** from the Alerts section.
2. On the the **Manage SNMP Alerts** page, select the SNMP version.
   - Dell Unity supports SNMP **v2c** and SNMP **v3.0**.

3. Select **+ (Add)**. The SNMP target window opens
4. Enter the **network name** or **IP address**.



SNMP Target

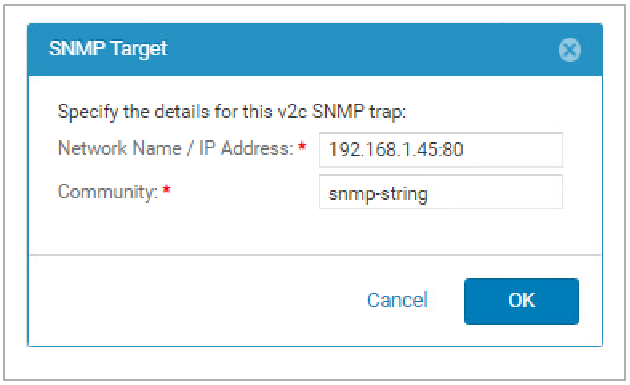
Specify the details for this v3 SNMP trap:

Network Name / IP Address: * 192.168.1.45:80

User Name: * username

Authentication Protocol: None

- For SNMP v2.c, specify a community.



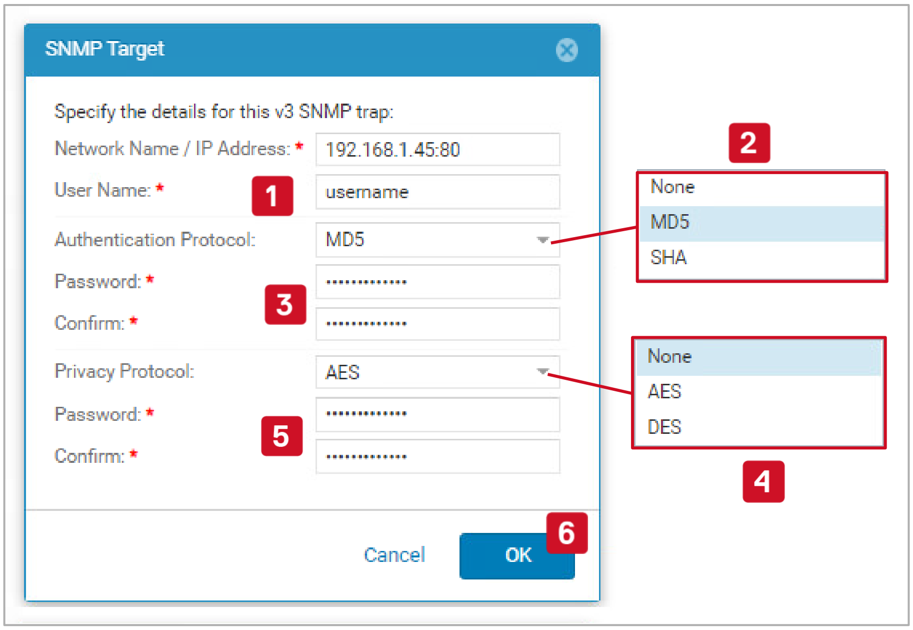
SNMP Target

Specify the details for this v2c SNMP trap:

Network Name / IP Address: * 192.168.1.45:80

Community: * snmp-string

SNMP v3.0



SNMP Target

Specify the details for this v3 SNMP trap:

Network Name / IP Address: * 192.168.1.45:80

User Name: * username

Authentication Protocol: MD5

Password: * •••••••••••••

Confirm: * •••••••••••••

Privacy Protocol: AES

Password: * •••••••••••••

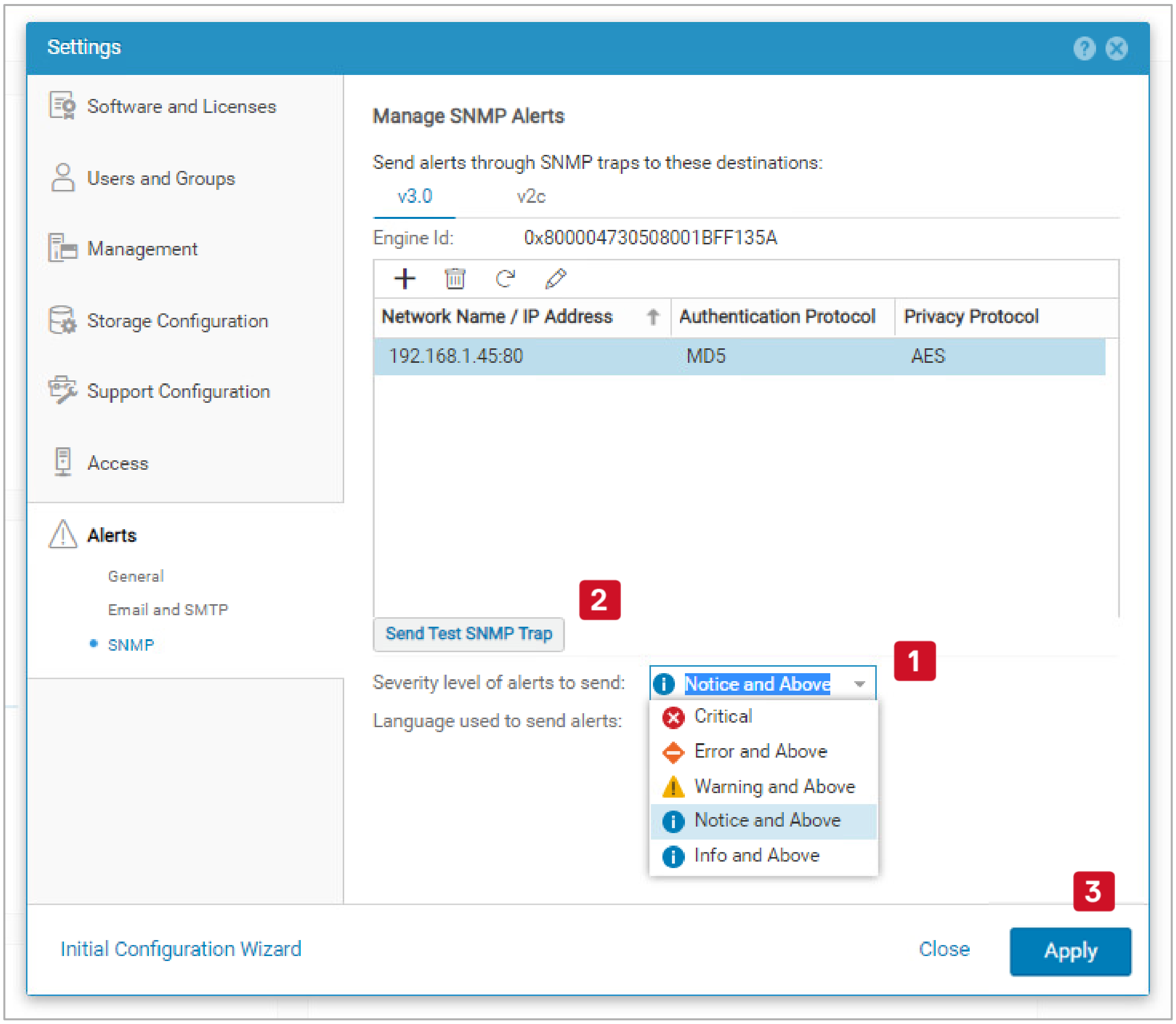
Confirm: * •••••••••••••

Configuration of a v3 SNMP trap

For the configuration of version 3.0 SNMP traps:

1. Type the user name to authenticate to the SNMP manager.
2. Select the authentication protocol for the traps from the drop-down: MD5, SHA, or none.
3. For the MD5 and SHA selections, type and confirm the password.
4. Select the privacy protocol (AES, DES, or none).
    - You can only specify the privacy protocol that is used to encode trap messages when you edit an existing destination.
5. If required, type and confirm the password.
6. Select **OK** To save the SNMP target. The new entry is displayed in the list.

Severity Level



Manage SNMP Alerts

Send alerts through SNMP traps to these destinations:

v3.0 v2c

Engine Id: 0x800004730508001BFF135A

Network Name / IP Address	Authentication Protocol	Privacy Protocol
192.168.1.45:80	MD5	AES

Severity level of alerts to send: Notice and Above

Language used to send alerts:

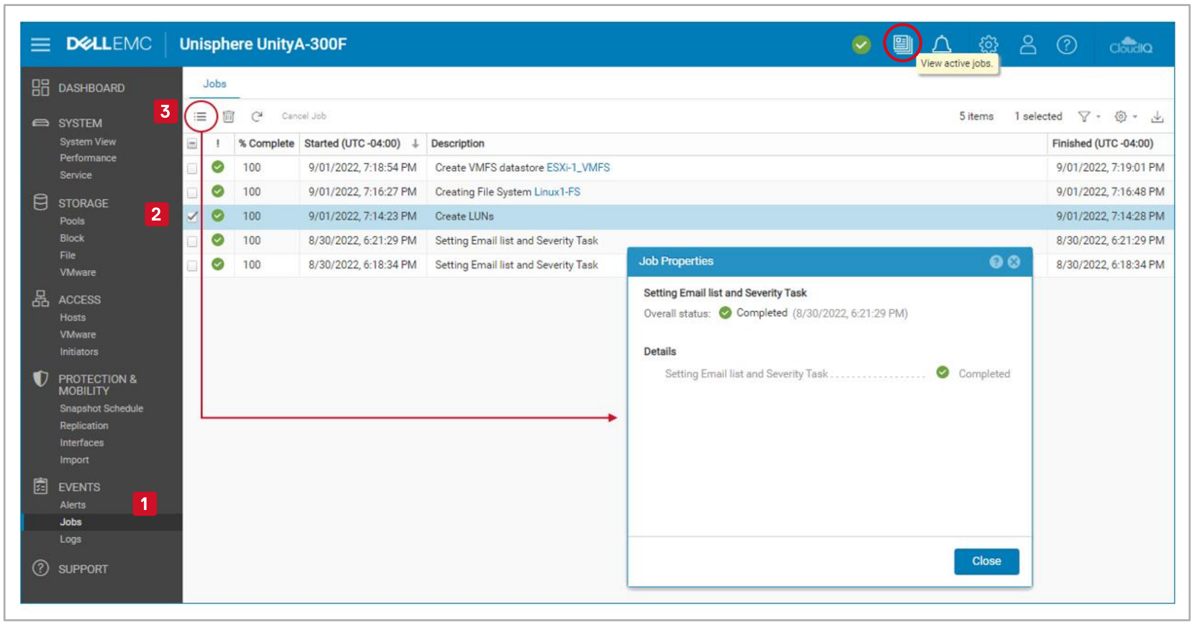
Unisphere Settings Alerts section SNMP

Configure the severity level of the alert notifications:

1. Select from the drop-down list the severity level for the alert notifications.
2. Click **Send Test SNMP Trap** to verify that the SNMP configuration is valid.
3. Select **Apply** button to commit the changes.

System Jobs Monitoring

Storage administrator can view information about all jobs, including the ones that are active, complete, or failed. From the Jobs page the administrator can also delete a completed or failed job, and cancel an active job (queued or running).



☐	!	% Complete	Started (UTC -04:00)	Description	Finished (UTC -04:00)
☐	✓	100	9/01/2022, 7:18:54 PM	Create VMFS datastore ESXi-1_VMFS	9/01/2022, 7:19:01 PM
☐	✓	100	9/01/2022, 7:16:27 PM	Creating File System Linux1-FS	9/01/2022, 7:16:48 PM
☑	✓	100	9/01/2022, 7:14:23 PM	Create LUNs	9/01/2022, 7:14:28 PM
☐	✓	100	8/30/2022, 6:21:29 PM	Setting Email list and Severity Task	8/30/2022, 6:21:29 PM
☐	✓	100	8/30/2022, 6:18:34 PM	Setting Email list and Severity Task	8/30/2022, 6:18:34 PM

Job Properties

Setting Email list and Severity Task

Overall status: ✓ Completed (8/30/2022, 6:21:29 PM)

Details

Setting Email list and Severity Task .... ✓ Completed

Unisphere Jobs page

To view and manage the active and completed jobs in Unisphere:

1. Select **Jobs**, under Events.
2. To view the properties of a job, select it from the list.
3. Select the **Details** icon.

Select the Jobs icon on the top menu to quickly view the jobs in progress.

- The Jobs icon also helps determine the number of active jobs: queued or running.
- The system polls for active jobs every 10 seconds and updates the count.

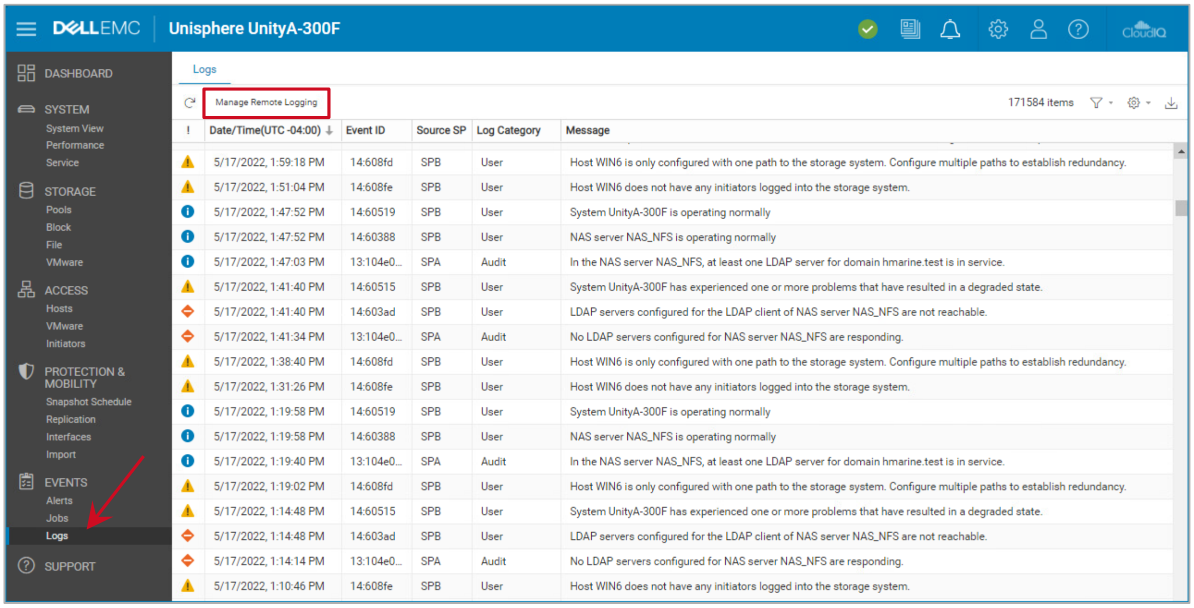
When a job is complete, a notification similar to system alerts is displayed on the screen. The user can select the notification message to access the Jobs page.

Inactive jobs older than seven days are automatically deleted from the list. Only the most recent 256 jobs are listed. Inactive jobs have a status of completed or failed.

System Logs Monitoring

Administrators can also view information about the Dell Unity system logged events by selecting **Logs**, under Events.

- Unisphere immediately displays real time changes to the storage system.
- By default, the logged events are sorted by the time the event was posted, from most recent to earlier.



!	Date/Time(UTC -04:00) ↓	Event ID	Source SP	Log Category	Message
⚠	5/17/2022, 1:59:18 PM	14:608fd	SPB	User	Host WIN6 is only configured with one path to the storage system. Configure multiple paths to establish redundancy.
⚠	5/17/2022, 1:51:04 PM	14:608fe	SPB	User	Host WIN6 does not have any initiators logged into the storage system.
ℹ	5/17/2022, 1:47:52 PM	14:60519	SPB	User	System UnityA-300F is operating normally
ℹ	5/17/2022, 1:47:52 PM	14:60388	SPB	User	NAS server NAS_NFS is operating normally
ℹ	5/17/2022, 1:47:03 PM	13:104e0...	SPA	Audit	In the NAS server NAS_NFS, at least one LDAP server for domain hmarine.test is in service.
⚠	5/17/2022, 1:41:40 PM	14:60515	SPB	User	System UnityA-300F has experienced one or more problems that have resulted in a degraded state.
⊖	5/17/2022, 1:41:40 PM	14:603ad	SPB	User	LDAP servers configured for the LDAP client of NAS server NAS_NFS are not reachable.
⊖	5/17/2022, 1:41:34 PM	13:104e0...	SPA	Audit	No LDAP servers configured for NAS server NAS_NFS are responding.
⚠	5/17/2022, 1:38:40 PM	14:608fd	SPB	User	Host WIN6 is only configured with one path to the storage system. Configure multiple paths to establish redundancy.
⚠	5/17/2022, 1:31:26 PM	14:608fe	SPB	User	Host WIN6 does not have any initiators logged into the storage system.
ℹ	5/17/2022, 1:19:58 PM	14:60519	SPB	User	System UnityA-300F is operating normally
ℹ	5/17/2022, 1:19:58 PM	14:60388	SPB	User	NAS server NAS_NFS is operating normally
ℹ	5/17/2022, 1:19:40 PM	13:104e0...	SPA	Audit	In the NAS server NAS_NFS, at least one LDAP server for domain hmarine.test is in service.
⚠	5/17/2022, 1:19:02 PM	14:608fd	SPB	User	Host WIN6 is only configured with one path to the storage system. Configure multiple paths to establish redundancy.
⚠	5/17/2022, 1:14:48 PM	14:60515	SPB	User	System UnityA-300F has experienced one or more problems that have resulted in a degraded state.
⊖	5/17/2022, 1:14:48 PM	14:603ad	SPB	User	LDAP servers configured for the LDAP client of NAS server NAS_NFS are not reachable.
⊖	5/17/2022, 1:14:14 PM	13:104e0...	SPA	Audit	No LDAP servers configured for NAS server NAS_NFS are responding.
⚠	5/17/2022, 1:10:46 PM	14:608fe	SPB	User	Host WIN6 does not have any initiators logged into the storage system.

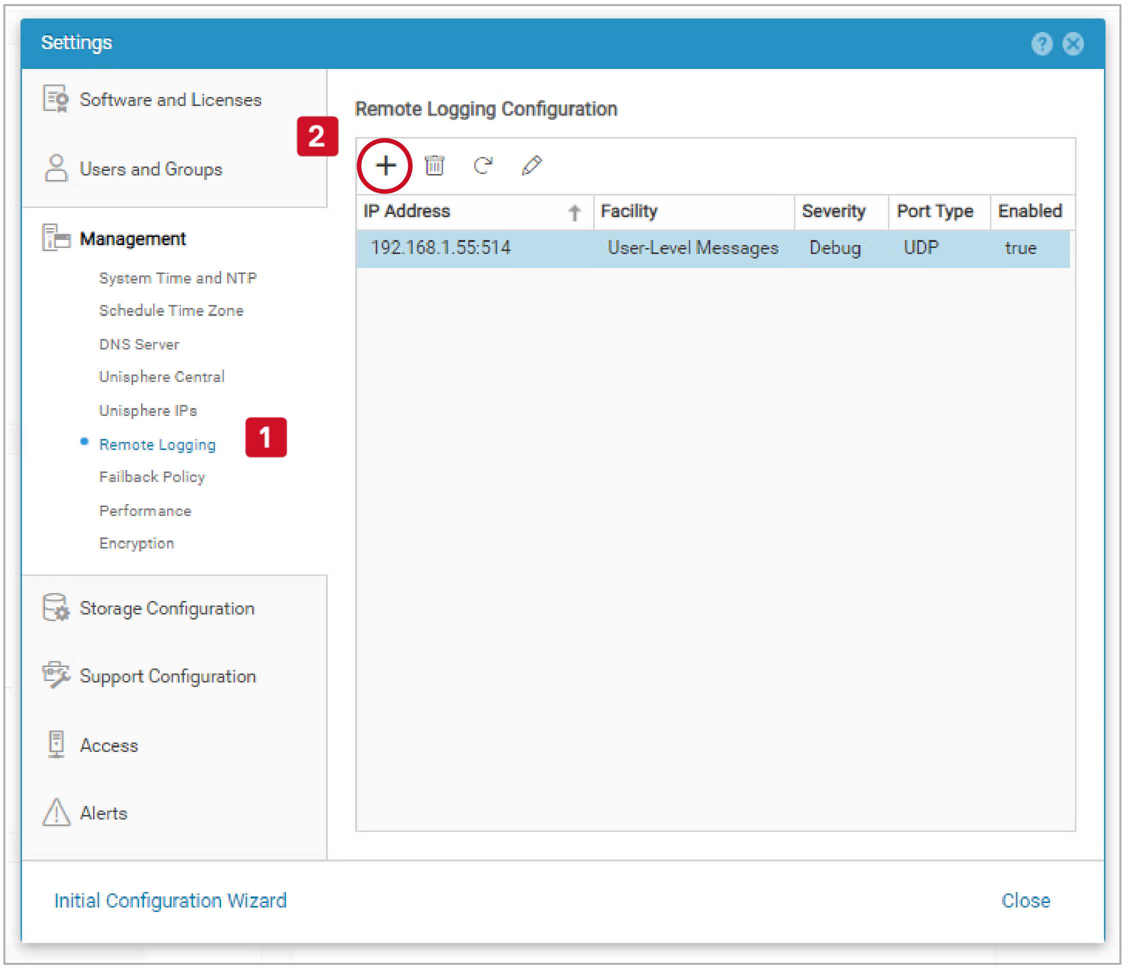
Unisphere Logs page

The storage administrator can also customize the view and sort, filter, and export the data. The event log list can be sorted by Date/Time: ascending or descending.

A link to the **Remote Logging** page in the Unisphere Settings window enables the administrator to configure the logging of user/audit messages to a remote host.

Add Remote Logging Configuration

Remote Logging



IP Address	Facility	Severity	Port Type	Enabled
192.168.1.55:514	User-Level Messages	Debug	UDP	true

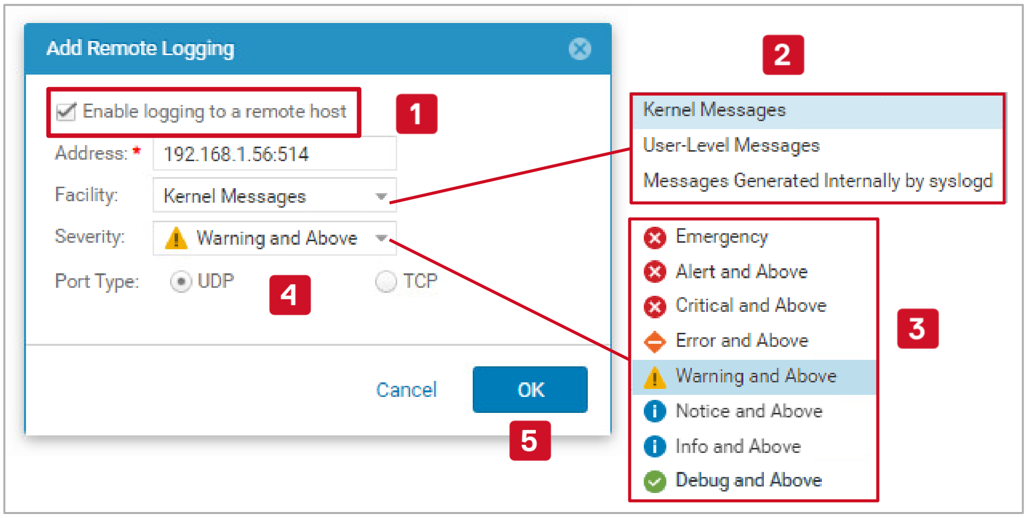
Unisphere Settings Remote Logging Configuration

The Remote Logging setting enables a Dell Unity system to log user/audit messages to a remote host. A remote host running syslog must be configured to receive logging messages from the storage system before the user can enable this feature in Unisphere.

To view and add a new remote logging configuration for another remote host, perform the following steps:

1. Open the Unisphere Settings window, and select **Remote Logging** under the Management section.
2. Select the **Add** icon. (Only a maximum of five remote logging configurations are supported. If five configurations are already configured, the Add icon is disabled.)
    - The Add Remote Logging window opens

Add Configuration



Add Remote Logging

☑ Enable logging to a remote host

Address: * 192.168.1.56:514

Facility: Kernel Messages

Severity: Warning and Above

Port Type: ● UDP ○ TCP

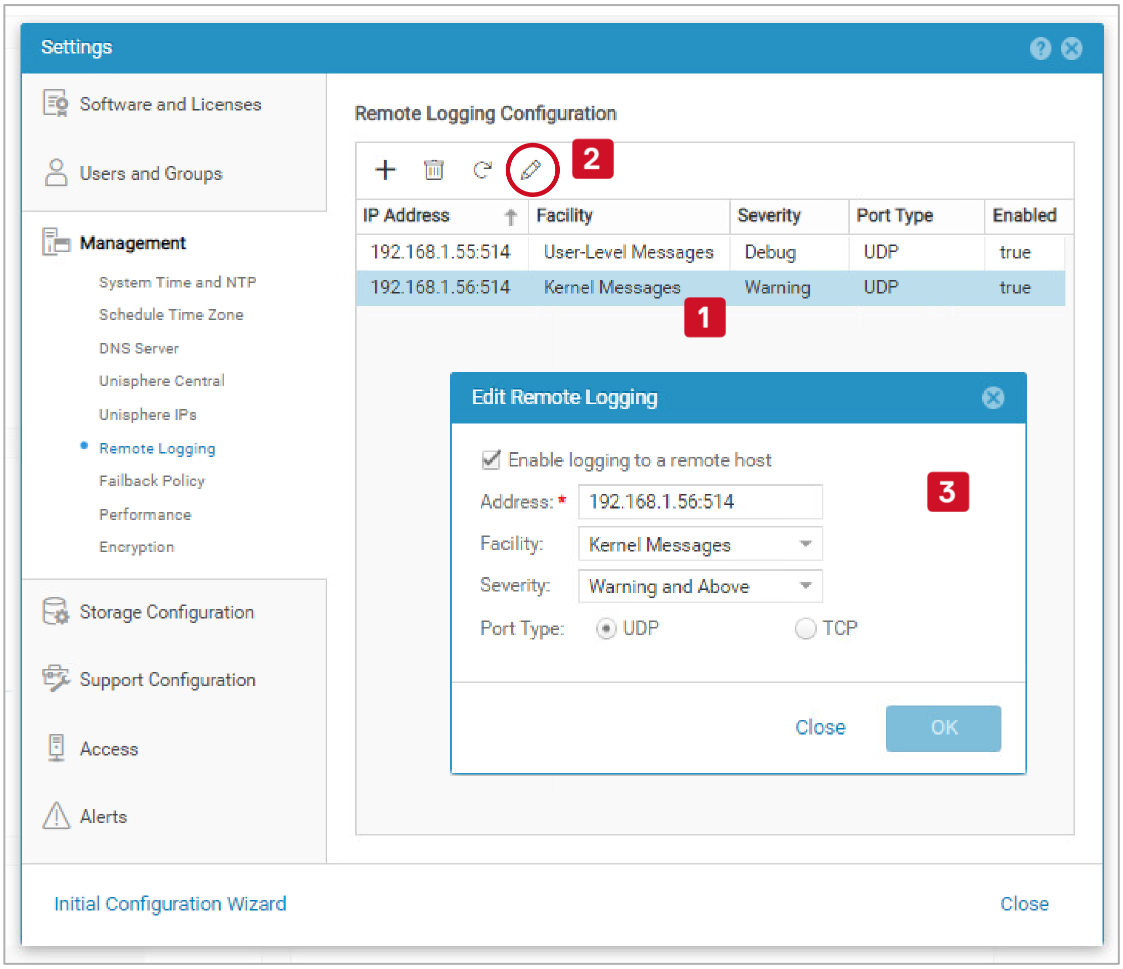
Add Remote Logging configuration window

1. Check the **Enable logging to a remote host** check box.
    - Specify the network address of the new host that receives the log data (include port 514 in the address).
2. Select the component that generates the log messages to record.
3. Select the severity level of the log entries that are sent to the remote host.
    - The severity levels are displayed in descending order in the related drop-down list.

4. Then select the protocol used to transfer log information (UDP or TCP).
5. Select **OK** to save the configuration.

> **Tip:** In many scenarios, a root or administrator account on the receiving computer can configure the remote syslog server to receive log information from the storage system. The configuration is set by editing the *syslog-ng.conf* file on the remote computer. For more information about setting up and running a remote syslog server, read the remote computer operating system documentation.

Edit Remote Logging Configuration



IP Address	Facility	Severity	Port Type	Enabled
192.168.1.55:514	User-Level Messages	Debug	UDP	true
192.168.1.56:514	Kernel Messages	Warning	UDP	true

☑ Enable logging to a remote host

Address: * 192.168.1.56:514

Facility: Kernel Messages

Severity: Warning and Above

Port Type: ● UDP ○ TCP

Unisphere Settings Remote Logging Configuration

To view or modify a Remote Logging configuration, perform the following:

1. Select a remote logging configuration.
   - You can edit the settings for remote logging to the first remote host (record entry with no network address) or an existing configuration.
2. Select the **Edit** icon.
3. Make any necessary changes, then select OK to save the configuration:
   - Unselect **Enable logging to a remote host** to disable remote logging.
   - Change the network address of the host that receives the log data (include port 514 in the address).

- Change the component that generates the log messages to be recorded.
    - **Kernel Messages** - Messages that are generated by the operating system kernel. These messages are specified with the facility code 0 (keyword kern).
    - **User-Level Messages** - This type of messages are the default option. Messages that are generated by random user processes. These messages are specified with the facility code 1 (keyword user).
    - **Messages Generated Internally by syslogd** - Messages that are generated internally by the system logging utility—syslogd. These messages are specified with the facility code 5 (keyword syslog).
- Change the severity level of the log entries sent to the remote host.
- Change the protocol used to transfer log information: *UDP* or *TCP*.

System Administration Key Points

1. **User Interfaces and Access Control**
    a. Configuration and management of the Dell Unity family of storage systems is performed using three interfaces: Unisphere, UEMCLI and REST API.
    b. Access to Dell Unity XT systems is granted to defined and configured user accounts (local or LDAP). The user accounts are role based.
    c. Dell Unity XT systems can be monitored through the Unisphere Central and CloudIQ applications.
2. **Basic System Settings**
    a. Dell EMC XT system global settings and parameters such as System time and DNS can be configured from Unisphere Settings.
    b. The Unisphere Settings window also provides options to configure the time zone for snapshot schedules and asynchronous replication throttling.
    c. The Dell Unity XT management port network address, and the failback policy can be configured from the Unisphere Settings.
3. **Support Configuration**
    a. A Proxy server can be configured to exchange service information for Dell Unity XT systems that cannot connect to the internet directly.
    b. Support credentials are used to retrieve the customer current support contract information and keep it updated automatically.
    c. Contact information ensures that Dell support has the most accurate information for contacting the user in response to an issue.
    d. Storage administrators can view the status and enable the Secure Connect Gateway (Secure Remote Services) feature from the Support Configuration section of Unisphere settings.
        - There are two Secure Connect Gateway deployment options available for the Dell Unity family of storage systems: centralized and integrated.
        - There are two remote service connectivity options for Integrated Secure Connect Gateway: Outbound/Inboud or Outbound only.
4. **Unisphere Alerts and Event Monitoring**

a. Unisphere alerts are usually events that require attention from the system administrator.

b. The alerts severity levels are categorized as **Information**, **Notice**, **Warning**, **Error**, and **Critical**.

c. There are four states for alerts: **Active_Manual**, **Active_Auto**, **Inactive**, and **Updating**.

d. Alert details provide **time** of the event, **severity level**, alert **message**, **description** of the event, **acknowledge flag**, **component affected** by the event, and **status of the component**.

e. Unisphere can be configured to send the system administrator alert notifications via email or though an SNMP trap.

f. Users can monitor when jobs are **active**, **complete**, or **failed**. The jobs page shows the number of active jobs: queued or running. The system polls for active jobs every 10 seconds and updates the active jobs count.

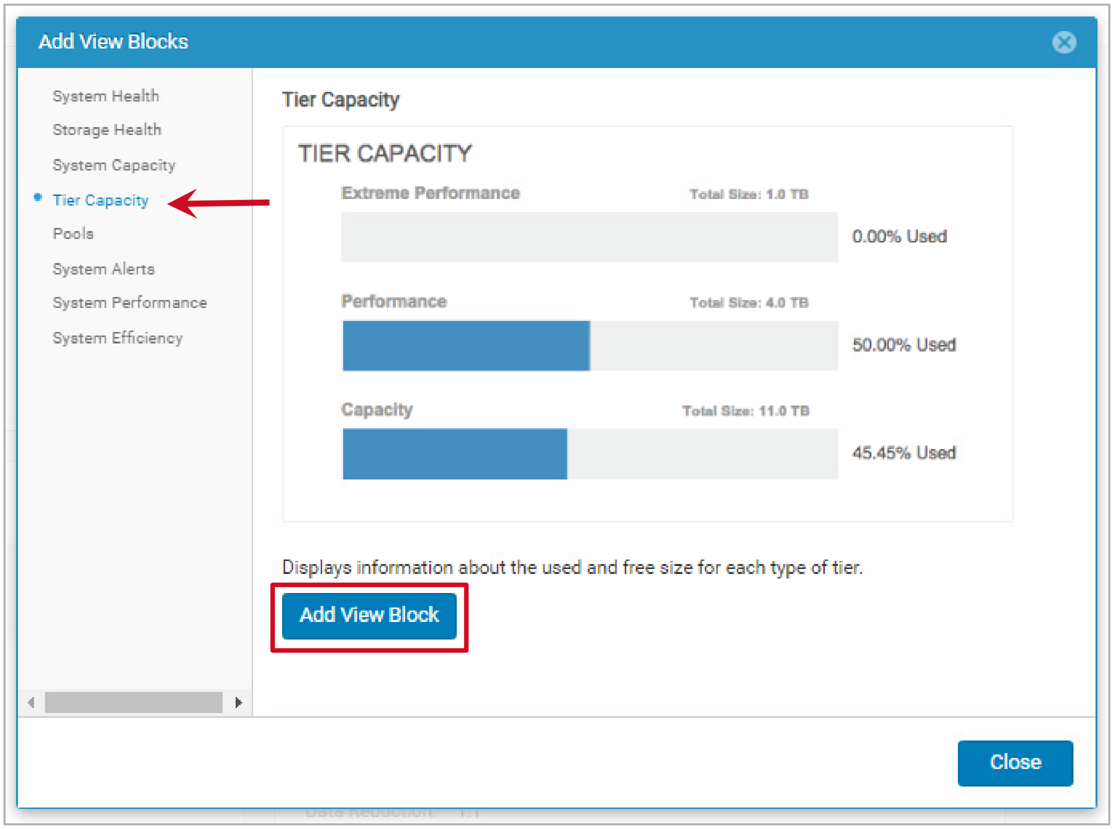
g. Unisphere can be configured to send log message entries of a determined severity level to a remote server.

For more information, see the **Dell Unity: Unisphere Overview**, **Secure Remote Support (SRS) Requirements and Configuration** on the Dell Technologies Support site.

Appendix

Adding View Blocks

Select a widget (view block) on the left pane then select **Add View Block**.



Displays information about the used and free size for each type of tier.

Health Score Categories

The CloudIQ Health Score engine breaks down into five categories each of which is monitored and contributes to the overall health of the system. For each category, CloudIQ runs a check against a known set of rules and makes a determination if a particular resource has issues.

The score can help a storage administrator spot where the most severe health issues are, based on the five core factors (health categories). The area with the highest risk to the system's health hurts its score until actions are taken towards remediation.

These categories are not customer configurable but built into the CloudIQ software.

Icon	Category	Types of Health Checks
☰	Component (system health)	Components with issues, OE/Firmware compliance issues
⚙	Configuration	Hosts - non-HA, drive issues: Faults subject to use (hot spare, RAID 6, RAID 5)
🛢	Capacity	Pools reaching full capacity
📊	Performance	Processor utilization, SP balance
🛡	Data Protection	RPOs not being met, last snap not taken.

Network Time Protocol (NTP) Synchronization

With the NTP synchronization method, the Unity storage system connects to an NTP server and synchronize the system clock with other applications and services on the network.

- Time synchronization is key for the Microsoft Windows environments for both client and server systems.
- Time synchronization is necessary to join a NAS server to the Active Directory domain, to enable SMB and multiprotocol access.
- Microsoft Windows environments typically use NTP service that is configured in one or more Domain Controllers.

Warning: If the storage system clock is not synchronized to the same source as the host system clock, some applications do not operate correctly.