Dell EMC Unity™ Family

Dell EMC Unity All Flash, Unity Hybrid, UnityVSA

Version 4.5

Security Configuration Guide

P/N 302-002-564 REV 08

DELL EMC

Published January 2019

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

CONTENTS

Additional resources

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

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

Product information
For product and feature documentation or release notes, go to Unity Technical Documentation at: www.emc.com/en-us/documentation/unity-family.htm.

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

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

Special notice conventions used in this document

DANGER

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

WARNING

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

CAUTION

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

NOTICE

Addresses practices not related to personal injury.

Note

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

CHAPTER 1

Introduction

This chapter briefly describes a variety of security features implemented on the storage system.

Topics include:

Overview

The storage system uses a variety of security features to control user and network access, monitor system access and use, and support the transmission of storage data. This document describes available security features.

This document is intended for administrators responsible for storage system configuration and operation.

The guide approaches security settings within the categories shown in Table 1 on page 10:

Table 1 Security settings categories

Security category	Description
Access control	Limiting access by end-user or by other entities to protect hardware, software, or specific product features.
Logs	Managing the logging of events.
Communication security	Securing product network communications.
Data security	Providing protection for product data.
Serviceability	Maintaining control of product service operations performed by the manufacturer or its service partners.
Alert system	Managing the alerts and notifications generated for security-related events.
Other security settings	Security settings that do not fall in one of the previous sections, such as physical security.

Related features and functionality information

Specific information related to the features and functionality described in this document is included in the following for Unity:

- *Unisphere Command Line Interface User Guide*
- Unisphere Online Help
- *SMI-S Provider Programmer's Guide*
- *Service Commands Technical Notes*
- *Secure Remote Services Requirements and Configuration*

The complete set of EMC customer publications is available on the EMC Online Support website at http://Support.EMC.com. After logging in to the website, click the **Support by Product** page, to locate information for the specific feature required.

CHAPTER 2

Access Control

This chapter describes a variety of access control features implemented on the storage system.

Topics include:

Storage system factory default management and service accounts

The storage system comes with factory default user account settings to use when initially accessing and configuring the storage system. See Table 2 on page 12.

Table 2 Factory default user account settings

Account type	Username	Password	Privileges
Management (Unisphere)	admin	Password123#	Administrator privileges for resetting default passwords, configure system settings, create user accounts, and allocate storage.
Service	service	service	Perform service operations.

Note

During the initial configuration process, you are required to change the default password for the Management and Service accounts.

Storage system account management

Table 3 on page 12 illustrates the ways in which you can manage the storage system accounts.

Table 3 Account management methods

Account roles	Description
Management: • Adminstrator • Storage Administrator • Security Administrator • Operator • VM Administrator	After the storage system initial system configuration process is complete, you can manage the storage system users and groups (either local accounts, LDAP accounts, or both) from Unisphere or the Unisphere CLI. • For local accounts, you can add a new user, delete a selected user, change the user's role, and reset (change) user password. • For an LDAP user, you can add an LDAP user, delete a selected user, and change the user's role. • For an LDAP group, you can add an LDAP group, delete a selected group, and change the group's role.
Service	You cannot create or delete storage system service accounts. You can reset the service account password from Unisphere. Under

Table 3 Account management methods (continued)

Account roles	Description
	System, select **Service** > **Service Tasks** > **Change Service Password** function.

Note

You can reset the storage system factory default account passwords by pressing the password reset button on the storage system chassis. The *Unisphere Online Help* provides more information.

Unisphere

Authentication for access to Unisphere is performed based on the credentials of the user (local or LDAP) account. User accounts are created and subsequently managed through the **User Management** selection under **Settings** > **Users and Groups** in Unisphere. The authorizations that apply to Unisphere depend on the role associated with the user account.

Before a user can download the Unisphere UI content to a management workstation, the user must provide credentials for authentication and establish a session on the storage system. When the user specifies the network address of the storage system as the URL in a web browser, the user will be presented with a login page from which the user can select to authenticate either as a local user or through an LDAP directory server. The credentials that the user provides will be authenticated and, upon successful authentication, a UI management session will be created on the storage system. Subsequently, the Unisphere UI will be downloaded and instantiated on the user's management workstation. The user then will be able to monitor and manage the storage system within the capabilities of the role assigned to the user.

LDAP

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory services running on TCP/IP networks. LDAP provides central management of authentication and identity and group information used for authorization on the storage system. 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.

After you configure LDAP settings for the system, you can manage users and user groups, within the context of an established LDAP directory structure. For instance, you can assign access roles (Administrator, Storage Administrator, Security Administrator, Operator, VM administrator) to the LDAP user or groups. The role applied will determine the level of authorization the user or group will have in administering the storage system. The system uses the LDAP settings only for facilitating control of access to Unisphere CLI and Unisphere, not for access to storage resources.

Session rules

Unisphere sessions have the following characteristics:

- Expiration term of one hour
- Session timeout is not configurable
- Session IDs are generated during authentication and used for the duration of each session

Username and Password usage

Unisphere account user names must meet these requirements, as shown in #GUID-BBF9609A-0138-47C9-9507-1AB0AF8DB285/GUID-72D5D132-AB83-4C7E-B3E1-1D38AB85B467 on page 14.

Table 4 Unisphere account username requirements

Restriction	Username requirement
Minimum number of alphanumeric characters	1
Maximum number of alphanumeric characters	64
Supported special characters	. (dot)

Unisphere account passwords must meet these requirements, as shown in Table 5 on page 14.

Table 5 Unisphere account password requirements

Restriction	Password requirement
Minimum number of characters	8
Minimum number of uppercase characters	1
Minimum number of lowercase characters	1
Minimum number of numeric characters	1
Minimum number of special characters • Supported special characters include: ▪ !,@#$%^*_~?	1
Maximum number of characters	40

Note

You can change account passwords from Unisphere by selecting **Settings** and, under **Users and Groups**, select **User Management** > **More Actions** > **Reset Password**. When changing a password, you cannot reuse any of the last three passwords. The *Unisphere Online Help* provides more information.

NOTICE

In STIG mode, the password size must be at least 15 characters. STIG mode also sets additional requirements for password count, period, and expiration status. User accounts that were created prior to STIG mode being enabled are not impacted unless the password is modified. For more information related to STIG mode, see Manage STIG mode (physical deployments only) on page 78.

Authorization

Table 6 on page 15 shows the roles you can assign to the storage system local users and the privileges associated with these roles. In addition, you can assign these roles to LDAP users and groups.

Table 6 Local user roles and privileges

Task	Operator	Storage administrator	Security administrator	Administrator	VM administrator
Change own local login password	x	x	x	x	
Add, delete, or modify hosts				x	
Create storage		x		x	
Delete storage		x		x	
Add storage objects, such as LUNs, shares, and storage groups to a storage resource		x		x	
View storage configuration and status	x	x	x	x	
View Unisphere user accounts		x	x	x	
Add, delete, modify, lock or unlock Unisphere user accounts			x	x	
View current software or license status	x	x	x	x	
Perform software or license upgrade				x	
Perform initial configuration				x	
Modify NAS server configuration				x	
Modify system settings				x	
Modify network settings				x	
Change management interface language	x	x	x	x	
View log and alert information	x	x	x	x	
View encryption status	x	x	x	x	
Perform encryption keystore, auditlog, checksum backup		x	x	x	
Modify FIPS 140-2 mode			x	x	
Modify STIG mode			x	x	
Establish VASA connections between vCenter and the storage system				x	x

In the case of the VM Administrator role, once connection is established between the vCenter and the storage system, a vCenter user will be able to view the subset of the storage configuration and status which is relevant to that vCenter and its ESXi servers. The vCenter user can view only that information which is allowed through the vCenter access control mechanisms.

Note

You can change account roles in Unisphere by selecting **Settings** and, under **Users and Groups**, select **User Management** > **More Actions** > **Change Role**. The *Unisphere Online Help* provides more information.

NAT
NAT is not supported for local login through Unisphere to the storage system.

Unisphere command line interface (CLI)

The Unisphere CLI provides a command line interface for the same functionality available through Unisphere.

Running the Unisphere CLI requires special storage system command line software. You can download this software from the product page for your storage system on EMC Online Support (https://support.emc.com).

Session rules
The Unisphere CLI client does not support sessions. You must use command line syntax to specify the account username and password with each command that you issue.

You can use the Unisphere CLI `-saveuser` command to save the access credentials (username and password) for a specific account to a file in the secure lockbox that resides locally on the host on which Unisphere CLI is installed. The stored data is only available on the host where it was saved and to the user who saved it. After you save the access credentials, the CLI automatically applies them to the specified storage system destination and port each time you run a command.

Password usage
Authentication to the Unisphere CLI is performed in accordance with management accounts created and managed through Unisphere. The same permissions that apply to Unisphere apply to specific commands depending on the role associated with the current login account.

Saved settings
You can save the following settings on the host on which you run Unisphere CLI:

- User access credentials, including your username and password, for each system you access.
- SSL certificates imported from the system.
- Information about default system to access through Unisphere CLI, including the system name or IP address and the system port number.

Unisphere CLI saves the settings to a secure lockbox that resides locally on the host on which Unisphere CLI is installed. The stored data is only available on the host where it was saved and to the user who saved it. The lockbox resides in the following locations:

- On Windows Server 2003 (XP): `C:\Documents and Settings\$<user_name>\Local Settings\ApplicationData\.emc\uemcli\cert`
- On Windows 7, Windows 8, and Windows 10: `C:\Users\${user_name}\AppData\Local\.emc\uemcli\cert`
- On UNIX/Linux: `<home_directory>/.emc/uemcli/cert`

Locate the files config.xml and config.key. If you uninstall Unisphere CLI, these directories and files are not deleted, giving you the option of retaining them. If these files are no longer needed, consider deleting them.

Storage system service SSH interface

The storage system SSH service interface when enabled provides a command line interface for performing related and overlapping functionality to that which is available

from the Unisphere Service page (under **System** select **Service** > **Service Tasks** > **Enable SSH**).

The service account enables users to perform the following functions:

- Perform specialized storage system service commands for monitoring and troubleshooting storage system settings and operations.
- Operate only a limited set of commands that are assigned as a member of a non-privileged Linux user account in restricted shell mode. This account does not have access to proprietary system files, configuration files, or user or customer data.

To learn more about using service commands, see the technical notes document, *Service Commands*.

The storage system SSH service interface setting is persistent across system reboots, failovers, and in both Service Mode and Normal Mode. Therefore, enabling the storage system SSH service interface will keep the interface enabled until it is explicitly disabled from the Unisphere Service page (under **System** select **Service** > **Service Tasks** > **Disable SSH**).

For maximum system security, it is recommended to leave the storage system SSH service interface disabled at all times unless it is specifically needed to perform service operations on the storage system. After performing the necessary service operations, disable the SSH interface to ensure that the system remains secure.

Sessions

The storage system SSH service interface sessions are maintained according to the settings established by the SSH client. Session characteristics are determined by the SSH client configuration settings.

Password usage

The service account is an account that service personnel can use to perform basic Linux commands.

The default password for the storage system service interface is service. When you perform initial configuration for the storage system, you must change the default service password. Password restrictions are the same as those that apply to Unisphere management accounts (see Username and Password usage on page 14). For information on the storage system service command, `svc_service_password`, used to manage the password settings for the storage system service account, see the technical notes document, *Service Commands*.

Authorization

As shown in Table 7 on page 17, authorization for the service account is defined in two ways.

Table 7 Service account authorization definitions

Authorization type	Description
Linux file system permissions	File system permissions define most of the tasks that the service account can and cannot perform on the storage system. For example, most Linux tools and utilities that modify system operation in any way require superuser account privileges. Since the service account does not have such access rights, the service account cannot use Linux tools and utilities to which it does not have execute permissions and cannot edit configuration files that require root access to read or modify, or both.

Table 7 Service account authorization definitions (continued)

Authorization type	Description
Access control lists (ACLs)	The ACL mechanism on the storage system uses a list of very specific rules to explicitly grant or deny access to system resources by the service account. These rules specify service account permissions to other areas of the storage system that are not otherwise defined by standard Linux file system permissions.

Storage system service commands

A set of problem diagnostic, system configuration, and system recovery commands are installed on the storage system's operating environment (OE). These commands provide an in-depth level of information and a lower level of system control than is available through Unisphere. The technical notes document, *Service Commands*, describes these commands and their common use cases.

Storage system SP Ethernet service port and IPMItool

Your storage system provides console access over an Ethernet service port that is on each SP. This access requires the use of the IPMItool. The IPMItool is a network tool similar to ssh or telnet that interfaces with each SP over an Ethernet connection by using the IPMI protocol. The IPMItool is a Windows utility that negotiates a secure communication channel to access the SP console of a storage system. This utility requires login credentials and an IP address to activate the console. For more information about the IPMItool, see the *IPMItool User Guide Technical Notes*.

The SP Ethernet service port interface provides the same functions and features as the service SSH interface and is also subject to the same restrictions. The difference is that users access the interface through an Ethernet port connection rather than an SSH client.

For a list of service commands refer to the *Service Commands Technical Notes*.

SMI-S provider

The SMI-S provider does not introduce any change with regards to security. An SMI-S client connects to the storage system through HTTPS port 5989. The login credentials are the same as those of Unisphere UI or CLI users. All security rules that apply to UI and CLI users also apply to SMI-S connections. Unisphere UI and CLI users can authenticate using the SMI-S interface. No separate users are defined for the SMI-S interface. Once authenticated, the SMI-S client has the same privilege as defined for those Unisphere UI and CLI users. The *SMI-S Provider Programmer's Guide* for your storage system product provides information about configuring this service.

vSphere Storage API for Storage Awareness support

vSphere Storage API for Storage Awareness (VASA) is a VMware-defined, vendor-neutral API for storage awareness. A VASA Provider (VP) is a storage-side software component that acts as a storage awareness service for vSphere. ESXi hosts and vCenter Server connect to the VP and obtain information about available storage topology, capabilities, and status. Subsequently, vCenter Server provides this information to vSphere clients. VASA is used by VMware clients rather than Unisphere clients.

The VP runs on the active Storage Processor (SP) of the storage system. The vSphere user must configure this VP instance as the provider of VASA information for each storage system. In the event that an SP goes down, the related process will restart on the peer SP, along with the VASA VP. The IP address fails over automatically. Internally, the protocol will see a fault when obtaining configuration change events from the newly active VP, but this will cause an automatic resynchronization of the VASA objects without user intervention.

The storage system provides VASA 3.0 and VASA 2.0 interfaces for vSphere 6, and VASA 1.0 interfaces for vSphere 5.x.

VASA 1.0 is used for monitoring only and is used by VMware clients rather than Unisphere clients. VASA 1.0 is a reporting interface only and is used to request basic information about the storage system and the storage devices it exposes to the virtual environment in order to facilitate day-to-day provisioning, monitoring, and troubleshooting through vSphere:

- Storage visibilty: internally detects property changes, sending the updated information to vCenter
- Health and Capacity alarms: internally monitors for health status changes and for capacity related thresholds being crossed, raising the appropriate alarms to vCenter:
  - health status for the array, SPs, I/O ports, LUNs, and File Systems
  - class-level change indications for a change in health status for any of these objects
  - space capacity alarms for LUNs and File Systems
- VASA storage capabilities: internally monitor for storage capability changes, reporting updated capabilities to vCenter
- Storage DRS integration: vSphere will rely on information obtained internally from the VP and feed it into its business logic for various Storage DRS work-flows.

VASA 3.0 and 2.0 support Virtual Volumes (VVols). VASA 3.0 and VASA 2.0 support interfaces to query storage abstractions such as VVols and Storage Containers. This information helps storage policy based management (SPBM) make decisions about virtual disk placement and compliance. VASA 3.0 and VASA 2.0 also support interfaces to provision and manage the lifecycle of Virtual Volumes used to back virtual disks. These interfaces are directly invoked by ESXi hosts.

For more information related to VASA, vSphere, and VVols, refer to the VMware documentation and the Unisphere online help.

Authentication related to VASA

In order to initiate a connection from vCenter to the Unisphere VP, you must use the vSphere client to enter three key pieces of information:

- the URL of the VP, using the following format:
  - For VASA 3.0 and VASA 2.0, https://<Management IP address>:8443/vasa/version.xml
  - For VASA 1.0, https://<Management IP address>:8444/vasa/version.xml or https://<Management IP address>:8444/vasa/services/vasaService
- the username of a Unisphere user (the role must be either VM Administrator or administrator):

Note

The VM Administrator role is strictly used as a means to register certificates.

  - for local users use the syntax: local/<username>
  - for LDAP users use the syntax: <domain>/<username>
- the password associated with this user

The Unisphere credentials used here are only used during this initial step of the connection. If the Unisphere credentials are valid for the target storage system, the certificate of the vCenter Server is automatically registered with the storage system. It is this certificate that is used to authenticate all subsequent requests from the vCenter. No manual steps are required to install or upload this certificate to the VP. If the certificate has expired, the vCenter must register a new certificate to support a new session. If the certificate is revoked by the user, the session is invalidated and the connection is severed.

vCenter session, secure connection and credentials

A vCenter session begins when a vSphere administrator uses the vSphere Client to supply the vCenter Server with the VP URL and login credentials. The vCenter Server uses the URL, credentials, and the SSL certificate of the VP to establish a secure connection with the VP. A vCenter session ends when one of the following events occurs:

- An administrator uses the vSphere Client to remove the VP from the vCenter configuration and the vCenter Server terminates the connection.
- The vCenter Server fails or a vCenter Server service fails, terminating the connection. When vCenter or the service starts again, it will attempt to reestablish the SSL connection. If it cannot, it will start a new SSL connection.
- The VASA Provider fails, terminating the connection. When the VASA Provider starts up, it can respond to communication from the vCenter Server to reestablish the SSL connection and VASA session.

A vCenter session is based on secure HTTPS communication between a vCenter Server and a VP. The VASA architecture uses SSL certificates and VASA session identifiers to support secure connections. With VASA 1.0, the vCenter Server added the VP certificate to its truststore as part of the VP installation, or when it created a VASA session connection. The VP added the vCenter Server certificate to its truststore when Storage Monitoring Service (SMS) called the registerVASACertificate function. In VASA 3.0 and VASA 2.0, vCenter Server acts as the VMware certificate authority (VMCA). The VP transmits a self-signed certificate on request, after authorizing the request. It adds the vCenter Server certificate to its truststore, then issues a certificate signing request, and replaces its self-signed certificate with the VMCA signed certificate. Future connections will be authenticated by the server (the VP) using the client (SMS) certificate validated against the previously registered root signing certificate. A VP generates unique identifiers for storage entity objects, and vCenter Server uses the identifier to request data for a specific entity.

A VP uses SSL certificates and the VASA session identifier to validate VASA sessions. After the session is established, a VP must validate both the SSL certificate and the VASA session identifier associated with each function call from the vCenter Server. The VP uses the vCenter Server certificate stored in its truststore to validate the certificate associated with function calls from the vCenter SMS. A VASA session persists across multiple SSL connections. If an SSL connection is dropped, the vCenter Server will perform an SSL handshake with the VP to re-establish the SSL connection within the context of the same VASA session. If an SSL certificate expires, the vSphere administrator must generate a new certificate. The vCenter Server will establish a new SSL connection and register the new certificate with the VP.

Note

Unregistration of 3.0 and 2.0 VPs differs from unregistration of 1.0 VPs. SMS does not call the unregisterVASACertificate function against a 3.0 or 2.0 VP, so even after unregistration, the VP can continue to use its VMCA signed certificate obtained from SMS and continues to have access to the VMCA root certificate.

Single sign-on with Unisphere Central

The single sign-on capability added to Unisphere Central provides authentication services for multiple storage systems that are configured to use this feature. This feature provides an easy way for a user to log in to each system without requiring the user to re-authenticate to each system.

Unisphere Central is the centralized authentication server that facilitates single sign-on. This functionality allows a user to:

- Log in to Unisphere Central, then select and launch Unisphere on a storage system without supplying your login credentials again.
- Log in to one storage system and then select other storage systems associated with the same Unisphere Central to log in to without supplying your login credentials again.

Unisphere Central will periodically execute a query to request status information from the storage systems that it is managing. The identity associated with requests executed in this context is the Unisphere Central SSL/X.509 certificate. This certificate is signed by the Unisphere Central Certificate Authority, which is trusted by each storage system instance that Unisphere Central is configured to manage.

Additionally, this feature provides a single sign-off capability; that is, when you log off Unisphere Central, you log off all of the associated storage system sessions at once.

Requirements

To use single sign-on:

- Unity and UnityVSA storage systems must be running OE version 4.0 or later.
- Unisphere Central version 4.0 or later must be used.
- Both the Unisphere Central server and the storage systems must be configured to authenticate against the same AD/LDAP directory.
- The LDAP user must be directly mapped to a Unisphere role, or be a member of an AD/LDAP group that maps to a Unisphere role on both the storage system and Unisphere Central.
- Each storage system must have single sign-on enabled.
- The user must log in as an LDAP user.

Note

In cases where these requirements are not met, the user must log in to the individual system as a local user and provide authentication credentials to access that system.

You must have Administrator privileges to enable single sign-on. Users with Storage Administrator, Operator, or VM Administrator privileges cannot enable single sign-on. Use the following uemcli command to enable single sign-on:

```
uemcli -d <IP address> -u <username> -p <password> /sys/ur set -
ssoEnabled yes
```

Each storage system that is configured with this feature enabled can be a client of the centralized authentication server and participate in the single sign-on environment.

For more information about this command, refer to the *Unisphere Command Line Interface User Guide*.

Considerations and Restrictions

The user session timeout between the web client and centralized authentication server is 45 minutes.

The application session timeout between the web client and the storage system is one hour.

Note

For compatibility and interoperability information related to web browsers, refer to the Simple Support Matrix for the storage system on the support website.

Single sign-on process flows

The following sequences represent the authentication process flows related to single sign-on associated with Unisphere Central.

Access to a storage system through Unisphere Central

1. User launches a web browser on a management workstation and specifies the network address of Unisphere Central as the URL.
2. The browser is redirected by the web server to a local Unisphere Central login URL and the user is presented with a login screen.
3. The user types and submits LDAP login credentials. The username is in the form <LDAP DOMAIN>/username.
4. A session token is set and the browser is redirected by the system back to the original URL that was specified.
5. The browser downloads the Unisphere content and Unisphere Central is instantiated.
6. The user then navigates through Unisphere to a particular storage system to monitor.
7. The user clicks on the network address for the storage system.
8. A new browser window is created with the URL of the storage system.
9. The browser is redirected to the Unisphere Central authentication server where the user has already authenticated.
10. The browser is redirected back to the Unisphere download page and a session is established with the storage system using the new service ticket.
11. Unisphere is downloaded and instantiated.
12. The user starts managing/monitoring the storage system.

Access to storage systems associated with Unisphere Central

1. User launches a web browser on a management workstation and specifies the network address of a storage system as the URL.
2. The browser is redirected to the local Unisphere Central login service and the user is presented with a login screen.
3. The user types and submits LDAP login credentials. The username is in the form <LDAP DOMAIN>/username.

4. A session token is set as a cookie and the browser is redirected by the system back to the original URL that was specified.
5. The browser downloads the Unisphere content and Unisphere is instantiated.
6. The user then opens another web browser window or tab and specifies the network address of another storage system as the URL.
7. The browser is redirected to the Unisphere Central authentication server where the user is already authenticated. A new service ticket is obtained.
8. The browser is redirected back to the Unisphere download page and establishes a session with the second storage system using the new service ticket.
9. Unisphere for the second storage system is downloaded and instantiated.
10. The user starts managing/monitoring the second storage system.

Logging in to a local storage system

When you use a local account, or, if connectivity to the Unisphere Central authentication server is not available, you can log in to a local storage system using the authentication server resident on the system instead of logging in through Unisphere Central. There are two ways to log into the storage system locally:

- When the browser is redirected to the Unisphere Central authentication server, an option is available that allows the user to redirect back to the system and log in locally.
- If Unisphere Central is inaccessible, the following url syntax can be used to browse or access the system and log in locally: `https://<storagesystemIP>?casHome=LOCAL`

where *storagesystemIP* is the IP address of the storage system.

Single sign-on and NAT support

Single sign-on does not support a NAT configuration. Also, NAT is not supported for local login through Unisphere to the storage system.

Security on file system objects

In a multiprotocol environment, security policy is set at the file system level, and is independent for each file system. Each file system uses its access policy to determine how to reconcile the differences between NFS and SMB access control semantics. Selecting an access policy determines which mechanism is used to enforce file security on the particular file system.

NOTICE

If the older SMB1 protocol does not need to be supported in your environment, it can be disabled by using the `svc_nas` service command. For more information about this service command, see the *Service Commands Technical Notes*.

UNIX security model

When the UNIX policy is selected, any attempt to change file level security from the SMB protocol, such as changes to access control lists (ACLs), is ignored. UNIX access rights are referred to as the mode bits or NFSv4 ACL of a file system object. Mode bits are represented by a bit string. Each bit represents an access mode or privilege that is granted to the user owning the file, the group associated with the file system object, and all other users. UNIX mode bits are represented as three sets of

concatenated rwx (read, write, and execute) triplets for each category of users (user, group, or other). An ACL is a list of users and groups of users by which access to, and denial of, services is controlled.

Windows security model

The Windows security model is based primarily on object rights, which involve the use of a security descriptor (SD) and its ACL. When SMB policy is selected, changes to the mode bits from NFS protocol are ignored.

Access to a file system object is based on whether permissions have been set to Allow or Deny through the use of a security descriptor. The SD describes the owner of the object and group SIDs for the object along with its ACLs. An ACL is part of the security descriptor for each object. Each ACL contains access control entries (ACEs). Each ACE in turn, contains a single SID that identifies a user, group, or computer and a list of rights that are denied or allowed for that SID.

File systems access in a multiprotocol environment

File access is provided through NAS servers. A NAS server contains a set of file systems where data is stored. The NAS server provides access to this data for NFS and SMB file protocols by sharing file systems through SMB shares and NFS shares. The NAS server mode for multiprotocol sharing allows the sharing of the same data between SMB and NFS. Because the multiprotocol sharing mode provides simultaneous SMB and NFS access to a file system, the mapping of Windows users to UNIX users and defining the security rules to use (mode bits, ACL, and user credentials) must be considered and configured properly for multiprotocol sharing.

Note

For information about configuring and managing NAS servers with regards to multiprotocol sharing, user mapping, access policies, and user credentials, refer to the Unisphere online help and the *Unisphere Command Line Interface User Guide*.

User mapping

In a multiprotocol context, a Windows user needs to be matched to a UNIX user. However, a UNIX user has to be mapped to a Windows user only when the access policy is Windows. This matching is necessary so that file system security can be enforced, even if it is not native to the protocol. The following components are involved in user mapping:

- UNIX Directory Services, local files, or both
- Windows resolvers
- Secure mapping (secmap) - a cache that contains all mappings between SIDs, and UID or GIDs used by a NAS server.
- ntxmap

Note

User mapping does not affect the users or groups that are local to the SMB server.

UNIX Directory Services and local files

UNIX Directory Services (UDSs) and local files are used to do the following:

- Return the corresponding UNIX account name for a particular user identifier (UID).

- Return the corresponding UID and primary group identifier (GID) for a particular UNIX account name.

The supported services are:

- LDAP
- NIS
- Local files
- None (the only possible mapping is through the default user)

There should be one UDS enabled or local files enabled, or both local files and a UDS enabled for the NAS server when multiprotocol sharing is enabled. The Unix directory service property of the NAS server determines which is used for user mapping.

Windows resolvers
Windows resolvers are used to do the following for user mapping:

- Return the corresponding Windows account name for a particular security identifier (SID)
- Return the corresponding SID for a particular Windows account name

The Windows resolvers are:

- The domain controller (DC) of the domain
- The local group database (LGDB) of the SMB server

secmap
The function of secmap is to store all SID-to-UID and primary GID and UID-to-SID mappings to ensure coherency across all file systems of the NAS server.

ntxmap
ntxmap is used to associate a Windows account to a UNIX account when the name is different. For example, if there is a user who has an account that is called Gerald on Windows but the account on UNIX is called Gerry, ntxmap is used to make the correlation between the two.

SID to UID, primary GID mapping
The following sequence is the process used to resolve an SID to a UID, primary GID mapping:

1. secmap is searched for the SID. If the SID is found, the UID and GID mapping is resolved.
2. If the SID is not found in secmap, the Windows name related to the SID must be found.
   a. The local group databases of the SMB servers of the NAS are searched for the SID. If the SID is found, the related Windows name is the local user name along with the SMB server name.
   b. If the SID is not found in the local group database, the DC of the domain is searched. If the SID is found, the related Windows name is the user name. If the SID is not resolvable, access is denied.
3. The Windows name is translated into a UNIX name. The ntxmap is used for this purpose.
   a. If the Windows name is found in ntxmap, the entry is used as the UNIX name.
   b. If the Windows name is not found in ntxmap, the Windows name is used as the UNIX name.
4. The UDS (NIS server, LDAP server, or local files) is searched using the UNIX name.

a. If the UNIX user name is found in the UDS, the UID and GID mapping is resolved.

b. If the UNIX name is not found, but the automatic mapping for unmapped Windows accounts feature is enabled, the UID is automatically assigned.

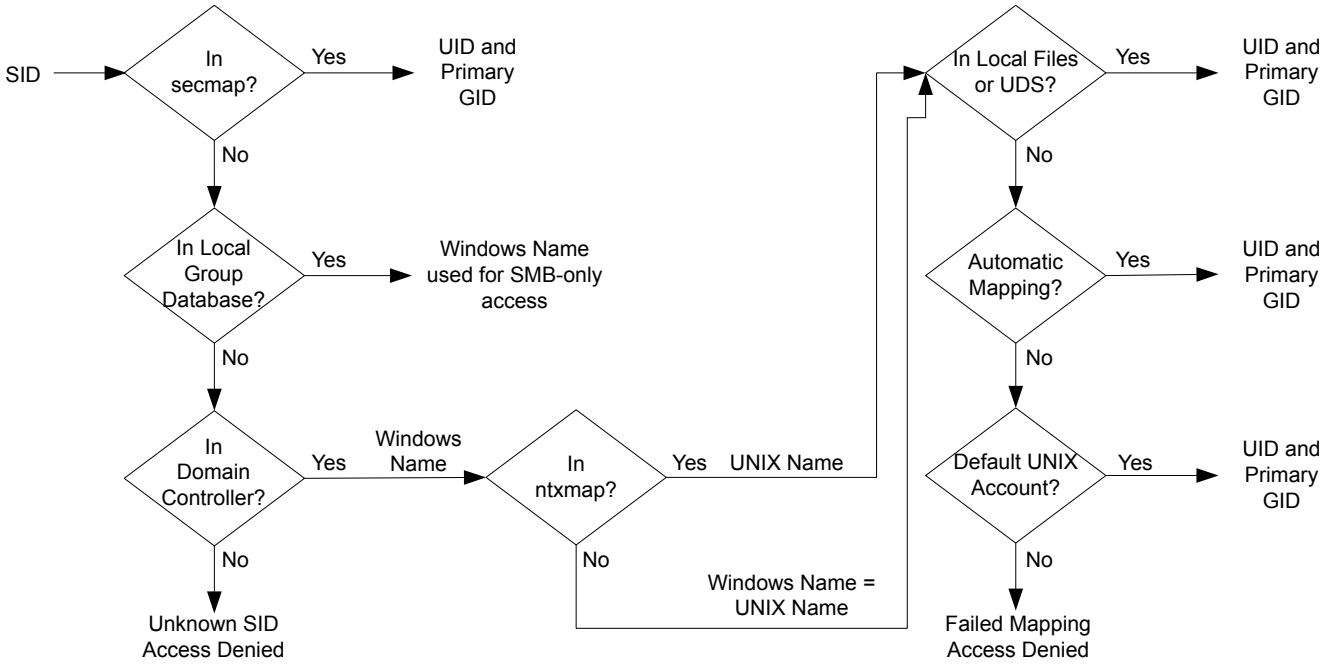
c. If the UNIX user name is not found in the UDS but there is a default UNIX account, the UID and GID mapping is resolved to that of the default UNIX account.

d. If the SID is not resolvable, access is denied.

If the mapping is found, it is added in the persistent secmap database. If the mapping is not found, the failed mapping is added to the persistent secmap database.

The following diagram illustrates the process used to resolve an SID to a UID, primary GID mapping:

Figure 1 Process for resolving an SID to a UID, primary GID mapping



UID to SID mapping

The following sequence is the process used to resolve a UID to an SID mapping:

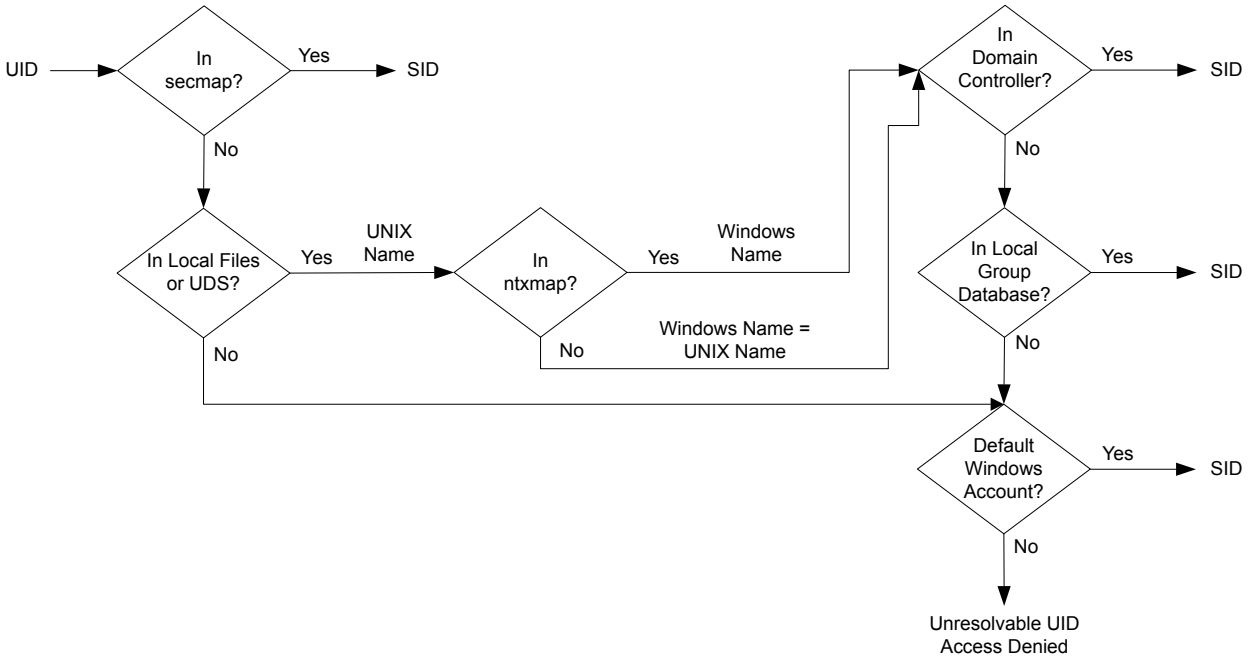
1. secmap is searched for the UID. If the UID is found, the SID mapping is resolved.
2. If the UID is not found in secmap, the UNIX name related to the UID must be found.
   a. The UDS (NIS server, LDAP server, or local files) is searched using the UID. If the UID is found, the related UNIX name is the user name.
   b. If the UID is not found in the UDS but there is a default Windows account, the UID is mapped to the SID of the default Windows account.
3. If the default Windows account information is not used, the UNIX name is translated into a Windows name. The ntxmap is used for this purpose.
   a. If the UNIX name is found in ntxmap, the entry is used as the Windows name.
   b. If the UNIX name is not found in ntxmap, the UNIX name is used as the Windows name.

4. The Windows DC or the local group database is searched using the Windows name.
   a. If the Windows name is found, the SID mapping is resolved.
   b. If the Windows name contains a period, and the part of the name following the last period (.) matches an SMB server name, the local group database of that SMB server is searched to resolve the SID mapping.
   c. If the Windows name is not found but there is a default Windows account, the SID is mapped to that of the default Windows account.
   d. If the SID is not resolvable, access is denied.

If the mapping is found, it is added in the persistent Secmap database. If the mapping is not found, the failed mapping is added to the persistent secmap database.

The following diagram illustrates the process used to resolve a UID to an SID mapping:

Figure 2 Process used to resolve a UID to an SID mapping



Access policies for NFS, SMB, and FTP

In a multiprotocol environment, the storage system uses file system access policies to manage user access control of its file systems. There are two kinds of security, UNIX and Windows.

For UNIX security authentication, the credential is built from the UNIX Directory Services (UDS) with the exception for non-secure NFS access, where the credential is provided by the host client. User rights are determined from the mode bits and NFSv4 ACL. The user and group identifiers (UID and GID, respectively) are used for identification. There are no privileges associated with UNIX security.

For Windows security authentication, the credential is built from the Windows Domain Controller (DC) and Local Group Database (LGDB) of the SMB server. User rights are determined from the SMB ACLs. The security identifier (SID) is used for identification. There are privileges associated with Windows security, such as TakeOwnership, Backup, and Restore, that are granted by the LGDB or group policy object (GPO) of the SMB server.

The following table describes the access policies that define what security is used by which protocols:

Access policy	Description
Native (default)	• Each protocol manages access with its native security. • Security for NFS shares uses the UNIX credential associated with the request to check the NFSv3 UNIX mode bits or NFSv4 ACL. The access is then granted or denied. • Security for SMB shares uses the Windows credential associated with the request to check the SMB ACL. The access is then granted or denied. • NFSv3 UNIX mode bits and NFSv4 ACL permission changes are synchronized to each other. • There is no synchronization between the Unix and Windows permissions.
Windows	• Secures file level access for Windows and UNIX using Windows security. • Uses a Windows credential to check the SMB ACL. • Permissions for newly created files are determined by an SMB ACL conversion. SMB ACL permission changes are synchronized to the NFSv3 UNIX mode bits or NFSv4 ACL. • NFSv3 mode bits and NFSv4 ACL permission changes are denied.
UNIX	• Secures file level access for Windows and UNIX using UNIX security. • Upon request for SMB access, the UNIX credential built from the local files or UDS is used to check the NFSv3 mode bits or NFSv4 ACL for permissions. • Permissions for newly created files are determined by the UMASK. • NFSv3 UNIX mode bits or NFSv4 ACL permission changes are synchronized to the SMB ACL. • SMB ACL permission changes are allowed in order to avoid causing disruption, but these permissions are not maintained.

For FTP, authentication with Windows or UNIX depends on the user name format that is used when authenticating to the NAS server. If Windows authentication is used, FTP access control is similar to that for SMB; otherwise, authentication is similar to that for NFS. FTP and SFTP clients are authenticated when they connect to the NAS server. It could be an SMB authentication (when the format of the user name is `domain\user` or `user@domain`) or a UNIX authentication (for the other formats of a single user name). The SMB authentication is ensured by the Windows DC of the domain defined in the NAS server. The UNIX authentication is ensured by the NAS server according to the encrypted password stored in either a remote LDAP server, a remote NIS server, or in the local password file of the NAS server.

Credentials for file level security

To enforce file-level security, the storage system must build a credential that is associated with the SMB or NFS request being handled. There are two kinds of credentials, Windows and UNIX. UNIX and Windows credentials are built by the NAS server for the following use cases:

- To build a UNIX credential with more than 16 groups for an NFS request. The extended credential property of the NAS server must be set to provide this ability.

- To build a UNIX credential for an SMB request when the access policy for the file system is UNIX.
- To build a Windows credential for an SMB request.
- To build a Windows credential for an NFS request when the access policy for the file system is Windows.

Note

For an NFS request when the extended credential property is not set, the UNIX credential from the NFS request is used. When using Kerberos authentication for an SMB request, the Windows credential of the domain user is included in the Kerberos ticket of the session setup request.

A persistent credential cache is used for the following:

- Windows credentials built for access to a file system having a Windows access policy.
- Unix credential for access through NFS if the extended credential option is enabled.

There is one cache instance for each NAS server.

Granting access to unmapped users

Multiprotocol requires the following:

- A Windows user must be mapped to a UNIX user.
- A UNIX user must be mapped to a Windows user in order to build the Windows credential when the user is accessing a file system that has a Windows access policy.

Two properties are associated to the NAS server with regards to unmapped users:

- The default UNIX user.
- The default Windows user.

When an unmapped Windows user attempts to connect to a multiprotocol file system and the default UNIX user account is configured for the NAS server, the user identifier (UID) and primary group identifier (GID) of the default UNIX user are used in the Windows credential. Similarly, when an unmapped UNIX user attempts to connect to a multiprotocol file system and the default Windows user account is configured for the NAS server, the Windows credential of the default Windows user is used.

NOTICE

If the default UNIX user is not set in the UNIX Directory Services (UDS), SMB access is denied for unmapped users. If the default Windows user is not found in the Windows DC or the LGDB, NFS access on a file system that has a Windows access policy is denied for unmapped users.

Note

The default UNIX user can be a valid existing UNIX account name or follow the new format `@uid=xxxx,gid=yyyy@`, where *xxxx* and *yyyy* are the decimal numerical values of the UID and the primary GID, respectively, and can be configured on the system through either Unisphere or CLI.

UNIX credential for NFS requests

To handle NFS requests for an NFS only or multi-protocol file system with a UNIX or native access policy, a UNIX credential must be used. The UNIX credential is always

embedded in each request; however, the credential is limited to 16 extra groups. The NFS server `extendedUnixCredEnabled` property provides the ability to build a credential with more than 16 groups. If this property is set, the active UDS is queried with the UID to get the primary GID and all the group GIDs to which it belongs. If the UID is not found in the UDS, the UNIX credential embedded in the request is used.

Note

For NFS secure access, the credential is always built using the UDS.

UNIX credential for SMB requests

To handle SMB requests for a multi-protocol file system with a UNIX access policy, a Windows credential must first be built for the SMB user at the session setup time. The SID of the Windows user is used to find the name from the AD. That name is then used (optionally through ntxmap) to find a Unix UID and GID from the UDS or local file (passwd file). The owner UID of the user is included in the Windows credential. When accessing a file system with a UNIX access policy, the UID of the user is used to query the UDS to build the UNIX credential, similar to building an extended credential for NFS. The UID is required for quota management.

Windows credential for SMB requests

To handle SMB requests for an SMB only or a multi-protocol file system with a Windows or native access policy, a Windows credential must be used. The Windows credential for SMB needs to be built only once at the session setup request time when the user connects.

When using Kerberos authentication, the credential of the user is included in the Kerberos ticket of the session setup request, unlike when using NT LAN Manager (NTLM). Other information is queried from the Windows DC or the LGDB. For Kerberos the list of extra group SIDs is taken from the Kerberos ticket and the list of extra local group SIDs. The list of privileges are taken from the LGDB. For NTLM the list of extra group SIDs is taken from the Windows DC and the list of extra local group SIDs. The list of privileges are taken from the LGDB.

Additionally, the corresponding UID and primary GID are also retrieved from the user mapping component. Since the primary group SID is not used for access checking, the UNIX primary GID is used instead.

Note

NTLM is an older suite of proprietary security protocols that provides authentication, integrity, and confidentiality to users. Kerberos is an open standard protocol that provides faster authentication through the use of a ticketing system. Kerberos adds greater security than NTLM to systems on a network.

Windows credential for NFS requests

The Windows credential is only built or retrieved when a user through an NFS request attempts to access a file system that has a Windows access policy. The UID is extracted from the NFS request. There is a global Windows credential cache to help avoid building the credential on each NFS request with an associated retention time. If the Windows credential is found in this cache, no other action is required. If the Windows credential is not found, the UDS or local file is queried to find the name for the UID. The name is then used (optionally, through ntxmap) to find a Windows user, and the credential is retrieved from the Windows DC or LGDB. If the mapping is not found, the Windows credential of the default Windows user is used instead, or the access is denied.

NFS secure

NFS secure is the use of Kerberos for authenticating users with NFSv3 and NFSv4. Kerberos provides integrity (signing) and privacy (encryption). Integrity and privacy are not required to be enabled, they are NFS export options.

Without Kerberos, the server relies entirely on the client to authenticate users: the server trusts the client. With Kerberos this is not the case, the server trusts the Key Distribution Center (KDC). It is the KDC which handles the authentication and manages accounts (principals) and password. Moreover, no password in any forms is sent on the wire.

Without Kerberos, the credential of the user is sent on the wire un-encrypted and thus can easily be spoofed. With Kerberos, the identity (principal) of the user is included in the encrypted Kerberos ticket, which can only be read by the target server and KDC. They are the only ones to know the encryption key.

In conjunction with NFS secure, AES128 and AES256 encryption in Kerberos is supported. Along with NFS secure, this also impacts SMB and LDAP. These encryptions are now supported by default by Windows and Linux. These new encryptions are much more secure; however, it is up to the client whether they are used. From that user principal, the server builds the credential of that user by querying the active UDS. Since NIS is not secured, it is not recommended to use it with NFS secure. It is recommended to use Kerberos with LDAP or LDAPS.

NFS secure can be configured either through Unisphere or the UEM CLI.

File protocol relationships

With Kerberos the following is required:

- DNS - You must use DNS name in place of IP addresses
- NTP - All participants must be timely synchronized
- UDS - To build credentials
- Hostname - Kerberos works with names and not IP addresses

NFS secure uses one or two SPNs depending on the value of the hostname. If the hostname is in FQDN format host.domain:

- The short SPN: nfs/host@REALM
- The long SPN: nfs/host.domainFQDN@REALM

If the hostname is not in FQDN format, only the short SPN will be used.

Similarly to SMB, where a SMB server can be joined to a domain, a NFS server can be joined to a realm (the Kerberos equivalent term for domain). There are two options for this:

- Use the configured windows domain if any
- Entirely configure a UNIX KDC based Kerberos realm

If the administrator selects to use the configured windows domain, there is nothing else to do. Every SPN used by the NFS service is automatically added/removed into the KDC when joining/unjoining the SMB server. Note that the SMB server cannot be destroyed if NFS secure is configured to use the SMB configuration.

If the administrator selects to use a UNIX based Kerberos realm, more configuration is needed:

- Realm name: The name of the Kerberos realm, which generally contains all upper-case letters.

- Entirely configure a UNIX KDC based Kerberos realm.

To ensure that a client mounts an NFS export with a specific security, a security parameter, sec, is provided that indicates which minimal security is allowed. There are 4 kinds of security:

- AUTH_SYS: Standard legacy security which does not use Kerberos. The server trust the credential provided by the client
- KRB5: Authentication using Kerberos v5
- KRB5i: Kerberos authentication plus integrity (signing)
- KRB5p: Kerberos authentication plus integrity plus privacy (encryption)

If a NFS client tries to mount an export with a security that is lower than the configured minimal security, the access will be denied. For example, if minimal access is KRB5i, any mount using AUTH_SYS or KRB5 will be rejected.

Building a credential

When a user connects to the system, it presents only its principal, user@REALM, which is extracted from the Kerberos ticket. Unlike AUTH_SYS security, the credential is not included in the NFS request. From the principal, the user part (before the @) is extracted and used to lookup the UDS for the corresponding uid. From that uid, the credential is built by the system using the active UDS, similar to when the Extended NFS credential is enabled (with the exception that, without Kerberos, the uid is provided directly by the request).

If the principal is not mapped in the UDS, the configured default UNIX user credential is used instead. If the default UNIX user is not set, the credential used will be nobody.

Replication

When a NAS server is the target of a replication, there is the possibility to access data through NFS for backup or disaster recovery. NFS secure cannot be used in these case since the usage of direct IP addresses is not compatible with Kerberos. Also, FQDN cannot be used because it could resolve to either the production interfaces on the source or the local interfaces on the destination.

Dynamic Access Control

Dynamic Access Control (DAC) enables administrators to apply access-control permissions and restrictions on resources based on well-defined rules that can include the sensitivity of the resources, the job or role of the user, and the configuration of the device that is used to access these resources.

DAC Claims Based Access Control (CBAC) is a feature of Windows Server 2012 that allows access control to be defined on the domain controller through a set of Central Access Policies (CAPs). Each Central Access Policy (identified by its CAPID) has a number of Central Access Rules (CARs) associated with it. CAPs can be assigned to Group Policy Objects (GPOs). This is the mechanism used to distribute CAPs to individual file servers. The CAP that applies to a particular resource (that is, a directory or file) is determined by the CAPID. When a NAS Server is created with Windows Shares (SMB), it will pick up the correct CAP and CAR when it joins the domain.

Each CAR has the following attributes:

- Resource Target Expression
- Current Permissions ACL
- Proposed Permissions ACL (optional)

The Resource Target Expression (applicability expression) is evaluated to determine whether or not the CAR is applicable to a given resource or not (for example,

@Resource.Department != @User.Department). If this expression evaluates to TRUE, the Current Permissions ACL is used during the access check; otherwise, the rule is ignored. The Proposed Permissions ACL allows the administrator to see the effect of proposed changes to the current permissions. When the evaluation of proposed permissions is enabled, any differences between current and proposed permissions during an access check are logged (in the server log).

A Windows client (Windows Server 2012 or Windows 8.x) can be used to associate a CAP with resources (that is, directories or files), if required (it is optional). When this is done, the specified CAP will be enforced by the NAS Server for the applicable resources. A Windows client can also be used to perform manual classification of resources (for example, setting the country or department).

DAC CBAC is enabled on the storage system by default; however, a service command, `svc_dac`, allows you to do the following:

- Enable or disable the DAC feature - when disabled the CAP associated with a resource is ignored (that is, only the DACL determines access).
- Enable or disable the evaluation of proposed permissions. Each CAR may have proposed permissions and these are distributed to the file servers. Usually, only these permissions are not evaluated. The `svc_dac` command can be used to enable the evaluation of these permissions. Once enabled any differences between the effective permissions and the proposed permissions will be sent to the server log. The evaluation of proposed permissions allows you to safely test proposed changes to CARs.
- Query the CAPs or CARs associated with a NAS Server compname (all, by distinguished name or by id).
- Add or remove custom recovery rules (to replace the default recovery rule).
- Control the verbosity of the logging produced by DAC for diagnostic purposes.

For detailed information about the `svc_dac` command, refer to the *EMC Unity Family Service Commands Technical Notes*.

CHAPTER 3

Logging

This chapter describes a variety of logging features implemented on the storage system.

Topics include:

Logging

The storage system maintains the types of logs that are listed in the following table for tracking events that occur on the system.

Table 8 Logs

Log type	Description
System log	Information displayed in Unisphere to notify users about storage system user-actionable events. These records are localized according to the default language setting specified for the system. **Note** User-actionable events include audit events. However, not all logged events show up in the GUI. Those audit log entries that do not meet a certain severity threshold are logged by the system but do not appear in the GUI.
System alert	Information used by the Service personnel to diagnose or monitor the storage system status or behavior. These records are recorded in English only.

Viewing and managing logs

The logging features that are listed in the following table are available for storage systems.

Table 9 Logging features

Feature	Description
Log roll-over	When the storage system log system accumulates two million log entries, it purges the oldest 500K entries (as determined by log record time) to return to 1.5 million log entries. You can archive log entries by enabling remote logging so that log entries are uploaded to a remote network node where they can be archived or backed up. The Logging on page 36 section provides more information.
Logging levels	Logging levels are not configurable for the storage system. Log levels can only be configured for exported log files as described in the Logging on page 36 section.
Alert integration	You can view storage system alert information in the following ways: • View alerts only: ▪ In Unisphere, go to **Events** > **Alerts**. • View log events: ▪ Using the Unisphere CLI, type the command `uemcli /event/alert/hist show`. ▪ In Unisphere, go to **System** > **Service** > **Logs**.
External log management	You can archive log entries by enabling remote logging so that log entries are uploaded to a remote network node where they can be archived or backed up. There, you can use tools such as syslog to

Table 9 Logging features (continued)

Feature	Description
	filter and analyze log results. The Logging on page 36 section provides more information.
Time synchronization	Log time is recorded in GMT format and is maintained according to the storage system time (which may be synchronized to the local network time through an NTP server).

Remote logging options

The storage system supports logging user/audit messages to a maximum of five remote hosts. The remote host must be accessible from the storage system, and security for the log information must be provided through network access controls or the system security at the remote host.

By default, the storage system transfers log information on port 514 using UDP. The following remote logging settings are configurable through Unisphere. Log into Unisphere and click **Settings** > **Management** > **Remote Logging**.

- Enable logging to a remote host.
- Network name or IP address where the storage system sends remote log information.
- Type of log messages to send. Use the Facility field to set the type of log messages. It is recommended that you select the User-Level Messages options.
- Severity level of events to send to a remote host
- Port number and type (UDP or TCP) to use for log transmission.

Configuring a host to receive storage system log messages

Before configuring remote logging for a storage system, you must configure each remote system to receive logging messages from the storage system. A root/administrator on the receiving computer can configure the remote syslog server or rsyslog server to receive log information by editing the syslog server or rsyslog server configuration file (syslogng.conf or rsyslog.conf) on the remote system.

Note

For more information on setting up and running a remote syslog server, refer to the documentation for the operating system running on the remote system.

CHAPTER 4

Communication Security

This chapter describes a variety of communication security features implemented on the storage system.

Topics include:

Port usage

Communications with the Unisphere and CLI interfaces are conducted through HTTPS on port 443. Attempts to access Unisphere on port 80 (through HTTP) are automatically redirected to port 443.

Storage system network ports

Table 10 on page 40 outlines the collection of network services (and the corresponding ports) that may be found on the storage system.

Table 10 Storage system network ports

Service	Protocol	Port	Description
FTP	TCP	21	Port 21 is the control port on which the FTP service listens for incoming FTP requests.
SFTP	TCP/UDP	22	Allows alert notifications through SFTP (FTP over SSH). SFTP is a client/server protocol. Users can use SFTP to perform file transfers on a storage system on the local subnet. Also provides outgoing FTP control connection. If closed, FTP will not be available.
SSH/SSHD, VSI	TCP/UDP	22	Allows SSH access (if enabled). Also used for VSI plugin. If closed, management connections using SSH will be unavailable and VSI plugin will not be available.
Dynamic DNS update	TCP/UDP	53	Used to transmit DNS queries to the DNS server in conjunction with the Dynamic Host Control Protocol (DHCP). If closed, DNS name resolution will not work.
DHCP client	UDP	67	Allows the storage system to act as a DHCP client during the initial configuration process and is used to transmit messages from the client (storage system) to the DHCP server to automatically obtain management interface information. Also, used to configure DHCP for the management interface of a storage system which has already been deployed. If closed, dynamic IP addresses will not be assigned using DHCP.
DHCP client	UDP	68	Allows the storage system to act as a DHCP client during the initial configuration process and is used to

Table 10 Storage system network ports (continued)

Service	Protocol	Port	Description
			receive messages from DHCP server to the client (storage system) to automatically obtain its management interface information. Also, used to configure DHCP for the management interface of a storage system which has already been deployed. If closed, dynamic IP addresses will not be assigned using DHCP.
HTTP	TCP/UDP	80	Redirect for HTTP traffic to Unisphere and the Unisphere CLI. If closed, management traffic to the default HTTP port will be unavailable.
NAS, VAAI-NAS	TCP	111	Provides NAS datastores for VMware and is used for VAAI-NAS. If closed, NAS datastores and VAAI-NAS will be unavailable.
Portmapper, rpcbind (Network infrastructure)	TCP/UDP	111	Opened by the standard portmapper or rpcbind service and is an ancillary storage system network service. It cannot be stopped. By definition, if a client system has network connectivity to the port, it can query it. No authentication is performed.
NTP	UDP	123	NTP time synchronization. If closed, time will not be synchronized among arrays.
DCE Remote Procedure Call (DCERPC) and NDMP	UDP	135	Multiple purposes for MicroSoft Client. Also used for NDMP.
NETBIOS Name Service (SMB)	TCP/UDP	137	The NETBIOS Name Service is associated with the storage system SMB file sharing services and is a core component of that feature (Wins). If disabled, this port disables all SMB-related services.
NETBIOS Datagram Service (SMB)	UDP	138	The NETBIOS Datagram Service is associated with the storage system SMB file sharing services and is a core component of that feature. Only Browse service is used. If disabled, this port disables Browsing capability.
NETBIOS Session Service (SMB)	TCP/UDP	139	The NETBIOS Session Service is associated with storage system SMB file sharing services and is a core component of that functionality. If SMB services are enabled, this port is open. It is specifically required for earlier

Table 10 Storage system network ports (continued)

Service	Protocol	Port	Description
			versions of the Windows OS (pre-Windows 2000). Clients with legitimate access to the storage system SMB services must have network connectivity to the port for continued operation.
SNMP Unix Multiplexer	TCP	199	SNMP communications. If closed, storage system alert mechanisms which rely on SNMP will not be sent.
LDAP	TCP/UDP	389	Unsecure LDAP queries. If closed, Unsecure LDAP authentication queries will be unavailable. Secure LDAP is configurable as an alternative.
Service Location Protocol (SLP)	TCP/UDP	427	Allows hosts (or other resources) to discover available services provided by a storage system.
HTTPS	TCP/UDP	443	Secure HTTP traffic to the Unisphere and Unisphere CLI. If closed, communication with the array will be unavailable. **Note** For SMI-S, used for array management; however, port 5989 is the default port used for this purpose.
SMB	TCP	445	SMB (on domain controller) and SMB connectivity port for Windows 2000 and later clients. Clients with legitimate access to the storage system SMB services must have network connectivity to the port for continued operation. Disabling this port disables all SMB-related services. If port 139 is also disabled, SMB file sharing is disabled.
DHCP (IPv6 only)	UDP	546	DHCP(v6) Client. If closed, dynamic IP addresses will not be assigned using DHCP.
DHCP (IPv6 only)	UDP	547	DHCP(v6) Server. If closed, dynamic IP addresses will not be assigned using DHCP.
LDAPS	TCP/UDP	636	Secure LDAP queries. If closed, secure LDAP authentication will be unavailable.
FTP	TCP	1024:65535	Used for passive FTP. Port 1024:65535 is related to data while port 1025:65535 is related to management.

Table 10 Storage system network ports (continued)

Service	Protocol	Port	Description
mountd (NFS)	TCP/UDP	1234	Used for the mount service, which is a core component of the NFS service (versions 2, 3, and 4) and is an important component of the SP to NAS Server interaction.
NAS, VAAI-NAS	TCP	2049	Provides NAS datastores for VMware and is used for VAAI-NAS. If closed, NAS datastores and VAAI-NAS will be unavailable.
NFS	TCP/UDP	2049	Used to provide NFS services.
UDI SSH	TCP	2222	Redirects traffic from port 22 for device eth*.
iSCSI	TCP	3260	Provides access to iSCSI services. If closed, file-based iSCSI services will be unavailable.
NFS	TCP/UDP	4000	Used to provide NFS statd services. statd is the NFS file-locking status monitor and works in conjunction with lockd to provide crash and recovery functions for NFS. If closed, NAS statd services will be unavailable.
NFS	TCP/UDP	4001	Used to provide NFS lockd services. lockd is the NFS file-locking daemon. It processes lock requests from NFS clients and works in conjunction with the statd daemon. If closed, NAS lockd services will be unavailable.
NFS	TCP/UDP	4002	Used to provide NFS rquotad services. The rquotad daemon provides quota information to NFS clients that have mounted a file system. If closed, NAS rquotad services will be unavailable.
SMB	UDP	4003	Allows SMB ACL to be viewed or changed from a Linux host with `emcgetsd` or `emcsetsd` tools.
Portable Archive Interchange (PAX) (Backup Services)	TCP	4658	• PAX is a storage system archive protocol that works with standard UNIX tape formats. • This service must bind to multiple internal network interfaces and as a consequence, it binds to the external interface as well. However, incoming requests over the external network are rejected.

Table 10 Storage system network ports (continued)

Service	Protocol	Port	Description
			• Background information on PAX is contained in the relevant EMC documentation on backups. There are several technical modules on this topic to deal with a variety of backup tools.
VSI	TCP	5080	This port provides for VSI plugin. If closed, VSI plugin will not be available.
Replication services	TCP	5085	Associated with replication services
Key Management Interoperability Protocol (KMIP)	TCP	5696	For KMIP, supports external key management using KMIP. If closed, KMIP services will be unavailable.
SMI-S	TCP	5989	For SMI-S, used for array management. SMI-S client connects to array using SMI-S TCP 5989 HTTPS. The *SMI-S Provider Programmer's Guide* provides more information about configuring this service.
VASA	TCP	8443	VASA Vendor provider for VASA 2.0.
VASA	TCP	8444	VASA Vendor provider for VASA 1.0.
RCP (Replication services)	TCP	8888	Used by the replicator (on the secondary side). It is left open by the replicator as soon as some data has to be replicated. After it is started, there is no way to stop the service.
NDMP	TCP	10000	• Enables you to control the backup and recovery of a Network Data Management Protocol (NDMP) server through a network backup application, without installing third-party software on the server. In a storage system, the NAS Server functions as the NDMP server. • The NDMP service can be disabled if NDMP tape backup is not used. • The NDMP service is authenticated with a username/password pair. The username is configurable. The NDMP documentation describes how to configure the password for a variety of environments.
NDMP	TCP	10500:10531	For three-way backup/restore sessions, NAS Servers use ports 10500 to 10531.

Table 10 Storage system network ports (continued)

Service	Protocol	Port	Description
IWD	Internal	60260	IWD initial configuration daemon. If closed, initialization of the array will be unavailable through the network.

Ports the storage system may contact

The storage system functions as a network client in several circumstances, for example, in communicating with an LDAP server. In these instances, the storage system initiates communication and the network infrastructure will need to support these connections. Table 11 on page 45 describes the ports that a storage system must be allowed to access for the corresponding service to function properly. This includes the Unisphere CLI.

Table 11 Network connections that may be initiated by the storage system

Service	Protocol	Port	Description
FTP	TCP	20	Port used for FTP data transfers. This port can be opened by enabling FTP as described in the next row. Authentication is performed on port 21 and defined by the FTP protocol.
FTP/SFTP	TCP	21	Allows alert notifications through SFTP (FTP over SSH). SFTP is a client/server protocol. Users can use SFTP to perform file transfers on a storage system on the local subnet. Also provides outgoing FTP control connection. If closed, FTP will not be available.
SSH/SSHD, VSI	TCP	22	Allows SSH access (if enabled). Also used for VSI plugin. If closed, management connections using SSH and VSI plugin will not be available.
SMTP	TCP	25	Allows the system to send email. If closed, email notifications will be unavailable.
DNS	TCP/UDP	53	DNS queries. If closed, DNS name resolution will not work.
DHCP	UDP	67-68	Allows the storage system to act as a DHCP client. If closed, dynamic IP addresses will not be assigned using DHCP.
HTTP	TCP	80	Redirect for HTTP traffic to Unisphere and the Unisphere CLI. If closed, management traffic to the default HTTP port will be unavailable.
Kerberos	TCP/UDP	88	Provides outgoing Kerberos ticket. If closed, Kerberos authentication and all protocols that use it; for example, SMB, LDAP, GPO, secNFS, and such, will not be available.
Portmapper, rpcbind (Network infrastructure)	TCP/UDP	111	Opened by the standard portmapper or rpcbind service and is an ancillary storage system network service. It cannot be stopped. By definition, if a client system has network connectivity to the port, it can query it. No authentication is performed.

Table 11 Network connections that may be initiated by the storage system (continued)

Service	Protocol	Port	Description
NTP	UDP	123	NTP time synchronization. If closed, time will not be synchronized among arrays.
NETBIOS Name Service (SMB)	TCP/UDP	137	The NETBIOS Name Service is associated with the storage system SMB file sharing services and is a core component of that feature (Wins). If disabled, this port disables all SMB-related services.
NETBIOS Datagram Service (SMB)	UDP	138	The NETBIOS Datagram Service is associated with the storage system SMB file sharing services and is a core component of that feature. Only Browse service is used. If disabled, this port disables Browsing capability.
NETBIOS Session Service (SMB)	TCP/UDP	139	The NETBIOS Session Service is associated with storage system SMB file sharing services and is a core component of that functionality. If SMB services are enabled, this port is open. It is specifically required for earlier versions of the Windows OS (pre-Windows 2000). Clients with legitimate access to the storage system SMB services must have network connectivity to the port for continued operation.
LDAP	TCP/UDP	389[a]	Unsecure LDAP queries. If closed, Unsecure LDAP authentication queries will be unavailable. Secure LDAP is configurable as an alternative.
Service Location Protocol (SLP)	TCP/UDP	427	Allows hosts (or other resources) to discover available services provided by a storage system.
HTTPS	TCP	443	HTTPS traffic to the Unisphere and Unisphere CLI, and for secure remote services when ESRS is enabled and Integrated ESRS is configured on the storage system. If closed, communication with the array will be unavailable.
Kerberos	TCP/UDP	464	Provides Kerberos Password Change and Set. If closed, impacts SMB.
Remote Syslog	UDP	514[a]	Syslog - Log system messages to a remote host. You can configure the host port that the system uses.
LDAPS	TCP/UDP	636[a]	Secure LDAP queries. If closed, secure LDAP authentication will be unavailable.
VMware	TCP	843	VMawareness - Allows VMware SDK communication with vSphere. If closed, VCenter/ESX discovery will be unavailable.
FTP	TCP	1024:65535	Provides outgoing FTP control connection. If closed, FTP will not be available.
SOCKS	TCP	1080	Port 1080 is the default used when the port is not specified and ESRS is enabled and Integrated ESRS is configured on the storage system, and a firewall is employed between the storage system and a Proxy server. If the default or user-specified port is closed, communication with the array through the port will be unavailable.

Table 11 Network connections that may be initiated by the storage system (continued)

Service	Protocol	Port	Description
mountd (NFS)	TCP/UDP	1234	Used for the mount service, which is a core component of the NFS service (versions 2, 3, and 4) and is an important component of the SP to NAS Server interaction.
NFS	TCP/UDP	2049	Used to provide NFS services.
HTTP	TCP	3128	Port 3128 is the default used when the port is not specified and ESRS is enabled and Integrated ESRS is configured on the storage system, and a firewall is employed between the storage system and a Proxy server. If the default or user-specified port is closed, communication with the array through the port will be unavailable.
iSNS	TCP	3205	Used to send Internet storage naming service (iSNS) registrations to the iSNS server.
iSCSI	TCP	3260	Provides access to iSCSI services. If closed, file-based iSCSI services will be unavailable.
NFS	TCP/UDP	4000	Used to provide NFS statd services. statd is the NFS file-locking status monitor and works in conjunction with lockd to provide crash and recovery functions for NFS.
NFS	TCP/UDP	4001	Used to provide NFS lockd services.lockd is the NFS file-locking daemon. It processes lock requests from NFS clients and works in conjunction with the statd daemon.
NFS	TCP/UDP	4002	Used to provide NFS rquotad services. The rquotad daemon provides quota information to NFS clients that have mounted a file system.
VSI	TCP	5080	This port provides for VSI plugin. If closed, VSI plugin will not be available.
KMIP	TCP	5696	For KMIP, supports external key management using KMIP. If closed, KMIP services will be unavailable.
HTTPS	TCP	8443	HTTPS traffic for secure remote support when ESRS is enabled and Integrated ESRS is configured on the storage system. If closed, there will be a significant decrease in remote support performance, which will directly impact the time to resolve issues on the Unity storage system.
REST	TCP	9443	Used to send service notifications to an ESRS gateway server when ESRS is enabled and Centralized ESRS is configured on the storage system.
Common AntiVirus Agent (CAVA)	TCP	12228	Used to provide a CAVA anti-virus solution to clients using a NAS server. If closed, CAVA anti-virus solution will not be available.
IWD	Internal	60260	IWD initial configuration daemon. If closed, initialization of the array will be unavailable through the network.

a. The LDAP and LDAPS port numbers can be overridden from inside Unisphere when configuring Directory Services. The default port number is displayed in an entry box that can be overridden by the user. Also, the Remote Syslog port number can be overridden from inside Unisphere.

Storage system certificate

The storage system automatically generates a self-signed certificate during its first initialization. The certificate is preserved both in NVRAM and on the backend LUN. Later, the storage system presents it to a client when the client attempts to connect to the storage system through the management port.

The certificate is set to expire after 3 years; however, the storage system will regenerate the certificate one month before its expiration date. Also, you can upload a new certificate by using the `svc_custom_cert` service command. This command installs a specified SSL certificate in PEM format for use with the Unisphere management interface. For more information about this service command, see the *Service Commands Technical Notes* document. You cannot view the certificate through Unisphere or the Unisphere CLI; however, you can view the certificate through a browser client or a web tool that tries to connect to the management port.

Note

When the array is in FIPS mode and a certificate is generated off-array, in addition to the certificate being in PEM format, the private key needs to be in PKCS#1 format. You can use an openssl command to do this conversion. Once the .cer and .pk files are generated, this additional step is required when the certificate will be used on an array in FIPS mode.

To increase security, some organizations use CA certificate chaining. Certificate chaining links two or more CA certificates together. The primary CA certificate is the root certificate at the end of the CA certificate chain. Since the system needs the complete certificate chain to verify the authenticity of a certificate that is received, ask the directory server administrator if certificate chaining is used. If so, you must concatenate all the relevant certificates into a single file and upload that version. The certificate must be in PEM/Base64 encoded format and use the suffix .cer.

Replacing storage system self-signed certificate with signed certificates from a local Certificate Authority

Before you can upload new certificates for the storage system from a local Certificate Authority to replace the existing Unisphere self-signed SSL certificates, you need to do the following:

1. Create a private key on the storage processor (SP).

   Note

   For example:

   ```
   22:59:02 service@unknown spa:~/openssl> openssl genrsa -des3 -out
   unitycert.key -passout pass:emcemc
   Generating RSA private key, 2048 bit long modulus
   ..........................+++
   ..................................................................................
   +++
   e is 65537 (0x10001)
   ```

2. Remove the passphrase from the key on the SP.

NOTICE

This step is very important. If the passphrase is not removed from the key, it will cause an SP panic.

Note

For example:

```
22:59:08 service@unknown spa:~/openssl> openssl rsa -in unitycert.key -
passin pass:emcemc -out unitycert.pk
writing RSA key
```

3. Request a CSR on the SP.

Note

For example:

```
22:59:12 service@unknown spa:~/openssl> openssl req -new -sha256 -key
unitycert.pk -out unitycert.csr -days 1825
-subj '/C=US/ST=MA/L=Sarasota/O=MyCust/CN=10.0.0.1'
```

Here **`-subj '/C=US/ST=MA/L=Sarasota/O=MyCust/CN=10.0.0.1'`** is an example, you should change it to correspond to your environment.

4. Get the CSR signed by your CA (Windows CA server, Openssl CA server, or another CA server). The following are examples of sending a CSR to a CA server for signing by the following means:
   - Print the CSR using the `cat` command, copy or paste it to your local notepad, and name it as unitycert.csr.

```
23:00:01 service@unknown spa:~/openssl> cat unitycert.csr
 -----BEGIN CERTIFICATE REQUEST-----
MIICljCCAX4CAQAwUTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1BMREwDwYDVQ
QH
DAhTYXJhc290YTEPMA0GA1UECgwGTXlDdXN0MREwDwYDVQQDDAgxMC4wLjAuMT
CC

ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOBxqufN1Vpm0hq5K5UU0o
cd
teL2hJr5T1WIOmwQreX4nIdHIxVoWmyepmT7IZJIrQZQc8GuFDRx5qZ/
cwlxoup7
3aprMKCx8Ka6nQE3ue46tehYxqwA7mCyT1XYIW7c5l1HJmEddj
+Lqj23OwXTkOjX
skzubLfI08zDgYyW+KrmMmnAQIpPucHiX8FmjhilNGUXXiN7f/
jtDq4M1QZcj2Vp
CVySMB5b1bGs1u10HQcv/
aBSE5cU7FAxaLyJpIHJnk8fPXJo02hSu6B3NG7RDa1B
35gW6qqlbFIjXUlWtzi4JKA6GIzCq576YcGeQA5QuIrKqE6feeTjsKD1Ac9tXa
cC
AwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQBpJn2Fu9noAMhn
+IbTJf9EVTAYsZGc
ddtgZcnVgEpI/dxB0p4ME210hg28UEwKl0wFAypGm8LaMxg0lbtfpUpU31JbaS
+2
lJc/79vxTfrWWNnSF95C+wer2LB93VLov8MSQqPZfl0LPb4NRU/
XaE4l9Vh5DYl4
```

```
/FmwHXsifwV5f1TUkvhC8YTwn5frWQjruz
+ItZ3z9DetQX0OXYXMcaPX5Qp6aU5m
dsXFHDDiaVbOofJN9z6OPOsWUhn0ZwEpnW8q/
+V72MdBIfiwEjoQqZZKh4w1l0/7
uElP8BfS7vH/i87OCqHJM0g/O3IndF+p5wYzmhrDPg/f3belQVQvKs7Z
-----END CERTIFICATE REQUEST-----
```

- Download CSR by Secure Copy Protocol (SCP).

  Note

  To download CSR files using SCP, use a third party tool (for example, WinSCP) to connect to the Unity management IP interface (username: service), and then copy the `unitycert.csr` file to the local computer.

5. After you get the signed certificate from the CA server, upload it to the SP and save its name as `unitycert.crt` (coresponding to `unitycert.pk`).

   Note

   For example:

```
$ svc_custom_cert unitycert

Example:
service@spa spa:~> svc_custom_cert pod6 Successfully installed custom
certificate files. Restarting web server ...
Unsupported
Sun May 22 05:37:48 2016:7645\0x7f44ba3e27c0:32:Module CIC/1.1.10.6
loaded
```

Storage system interfaces, services, and features that support Internet Protocol version 6

You can configure the interfaces on a system and use Internet Protocol version 6 (IPv6) addresses to configure different services and features. The following list contains features where IPv6 protocol is supported:

- Interfaces (SF, iSCSI) - to statically assign an IPv4 or IPv6 address to an interface
- Hosts - to enter a network name, an IPv4 address or an IPv6 address of a host
- Routes - to configure a route for IPv4 or IPv6 protocol
- Diagnostics - to initiate a diagnostic `ping` CLI command using either an IPv4 or IPv6 destination address. In Unisphere select **Settings** > **Access** > **Routing** > **Ping/Trace** to access the Ping/Trace screen which supports the IPv6 destination addresses as well.

All storage system components support IPv4, and most support IPv6. Table 12 on page 50 shows the availability of IPv6 support by setting type and component:

Table 12 IPv6 support by setting type and component

Setting Type	Component	IPv6 Supported
Unisphere management settings	Management port	Yes
	Domain Name Server (DNS)	Yes

Table 12 IPv6 support by setting type and component (continued)

Setting Type	Component	IPv6 Supported
	NTP (network time protocol) server	Yes
	Remote logging server	Yes
	LDAP server	No
Unisphere host configuration setting	Microsoft Exchange	Yes
	VMware datastore (NFS)	Yes
	VMware datastore (VMFS)	Yes
	Hyper-V datastore	Yes
Unisphere alert setting	SNMP trap destinations	Yes
	SMTP server	Yes
	EMC Secure Remote Services (ESRS)	No
Storage server setting	iSCSI server	Yes
	Shared Folder server	Yes
	Network Information Service (NIS) server (for NFS NAS Servers)	Yes
	Active Directory server (for SMB NAS Servers)	Yes
	Internet Storage Service (iSNS) server	Yes
Other	PING destinations	Yes
	Remote log	Yes
	LDAP	Yes

IPv6 address standard

Internet Protocol version 6 (IPv6) is an Internet Protocol address standard developed by the Internet Engineering Task Force (IETF) to supplement and eventually replace the IPv4 address standard that most Internet services use today.

IPv4 uses 32-bit IP addresses, which provides approximately 4.3 billion possible addresses. With the explosive growth of Internet users and Internet-connected devices, the available IPv4 address space is insufficient. IPv6 solves the address shortage issue, because it uses 128-bit addresses, which provides approximately 340 trillion addresses. IPv6 also solves other IPv4 issues, including mobility, autoconfiguration, and overall extensibility issues.

An IPv6 address is a hexadecimal value that contains eight, 16-bit, colon-separated fields:

`hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh`

Each digit in an IPv6 address can be a number from 0-9 or a letter from A-F.

For more information about the IPv6 standard, see information about the IPv6 standard (RFC 2460) on the IETF website (http://www.ietf.org).

Storage system management interface access using IPv6

When you set up management connections in the storage system, you can configure the system to accept the following types of IP addresses:

- Static Internet Protocol version 6 (IPv6) addresses, IPv4 addresses obtained through DHCP, and static IPv4 addresses
- IPv4 addresses only

You can statically assign the IPv6 addresses to the management interface. An IPv6 address on the management interface can be set to one of two modes, manual/static or disabled. When you disable IPv6, the protocol does not unbind from the interface. The disable command removes any unicast IPv6 addresses assigned to the management interface and the storage system will no longer answer requests addressed over IPv6. IPv6 is disabled by default.

After you finish installing, cabling, and powering up the system, an IP address must be assigned to the storage system management interface. If you are not running the storage system on a dynamic network, or if you would rather manually assign a static IP address, you must download, install, and run the Connection Utility. For more information about the Connection Utility, see Running the Connection Utility on page 53.

Inbound requests using IPv6 to the storage system through the management interface are supported. You can configure the management interface on a storage system to operate in an IPv4-only, IPv6-only, or a combined IPv4 and IPv6 environment and you can manage the storage system using Unisphere UI and the command line interface (CLI).

Outbound services such as Network Time Protocol (NTP) and Domain Naming System (DNS) support IPv6 addressing either by using explicit IPv6 addresses or by using DNS names. If a DNS name resolves to both IPv6 and IPv4, the storage system will communicate with the server over IPv6.

The manage network interface set and show CLI commands that are used to manage the management interfaces include attributes related to IPv6. For more information about these manage network interface commands and attributes, refer to the *Unisphere Command Line Interface User Guide*.

Configuring the management interface using DHCP

After you finish installing, cabling, and powering up the system, an IP address must be assigned to the storage system management interface. If you are running the storage system on a dynamic network that includes a Dynamic Host Control Protocol (DHCP) server and a Domain Name System (DNS) server, the management IP address can be assigned automatically.

Note

If you are not running the storage system in a dynamic network environment, or you would rather manually assign a static IP address, you must install and run the Connection Utility. For more information concerning the Connection Utility, see Running the Connection Utility on page 53.

The appropriate network configuration must include setting the range of available IP addresses, the correct subnet masks, and gateway and name server addresses. Consult your specific network's documentation for more information on setting up DHCP and DNS servers.

DHCP is a protocol for assigning dynamic Internet Protocol (IP) addresses to devices on a network. DHCP allows you to control Internet Protocol (IP) addresses from a centralized server and automatically assign a new, unique IP address when a storage system is plugged into your organization's network. This dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task.

The DNS server is an IP-based server that translates domain names into IP addresses. As opposed to numeric IP addresses, domain names are alphabetic and are usually easier to remember. Since an IP network is based on IP addresses, every time you use a domain name, the DNS server must translate the name into a corresponding IP address. For example, the domain name www.Javanet.com translates to the IP address 209.94.128.8.

No administrative information such as user names, passwords, and such are exchanged during the DHCP/Dynamic DNS configuration. Configuration of the management IP items (DHCP preference, DNS and NTP server configuration) fall under the existing Unisphere framework related to security. DNS and DHCP events including obtaining a new IP address on lease expiration are recorded in storage system audit logs. If DHCP is not used for the storage system management IP configuration, no additional network ports will be opened.

Dynamic IP addresses (DHCP) should not be used for any components of the EMC Secure Remote Services (ESRS) Virtual Edition (VE) servers, Policy Manager servers, or managed devices.

Note

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

Running the Connection Utility

Note

If you are running the storage system in a dynamic network environment that includes a DHCP server and a DNS server, you do not have to use the Connection Utility and instead can automatically assign a dynamic IP address (IPv4 only) for the storage system management interface. When a storage system uses a static IP address, it is manually configured with the Connection Utility to use a specific IP address. One problem with static assignment, which can result from a mistake or inattention to detail, occurs when two storage systems are configured with the same management IP address. This creates a conflict that could result in loss of network connectivity. Using DHCP to dynamically assign IP addresses minimizes these types of conflicts. Storage systems configured to use DHCP for IP assignment do not need to use statically assigned IP addresses.

Connection Utility installation software is available from the EMC Online Support website (https://support.emc.com), under the **Downloads** selection on the menu bar

of the product page for your storage system. After you download the software, install the program on a Windows host. When you run the Connection Utility from a computer on the same subnet as the storage system, the Connection Utility automatically discovers any unconfigured storage systems. If you run the Connection Utility on a different subnet, you can save the configuration to a USB drive and then transfer it to the storage system. If the storage system is located on a different subnet than the host running the Connection Utility, you can select to manually configure and save IP network and Hostname information to a USB drive as a text file, then insert the USB drive into either SP, which will then automatically set the IP network and Hostname information.

Note

You cannot change the management IP address when both of the Storage Processors (SP) are in Service mode.

After you run the Connection Utility and transfer the configuration to your storage system, you can connect to the storage system through a web browser using the IP address that you assigned to the storage system management interface.

The first time you connect to the storage system, the storage system Initial Configuration Wizard starts. The Initial Configuration Wizard lets you set up the initial configuration of the storage system so that you can start to create storage resources.

Note

For more information concerning the Connection Utility, see the *Unity Series Installation Guide*.

Protocol (SMB) encryption and signing

SMB 3.0 and Windows 2012 support on the storage system provides SMB encryption for those hosts capable of using SMB. SMB Encryption provides secure access to data on SMB file shares. This encryption provides security to data on untrusted networks, that is, it provides end-to-end encryption of SMB data sent between the array and the host. The data is protected from eavesdropping/snooping attacks on untrusted networks.

SMB Encryption can be configured for each share. Once a share is defined as encrypted, any SMB3 client must encrypt all its requests related to the share; otherwise, access to the share will be denied.

To enable SMB Encryption, you either set the **Protocol Encryption** option in the advanced SMB share properties in Unisphere or set it through the `create` and `set` CLI commands for SMB shares. There is no setting required on the SMB client.

Note

For more information about setting SMB encryption, refer to the Unisphere online help and the *Unisphere Command Line Interface User Guide*.

SMB also provides data integrity validation (signing). This mechanism ensures that packets have not been intercepted, changed, or replayed. SMB signing adds a signature to every packet and guarantees that a third party has not changed the packets.

To use SMB signing, the client and the server in a transaction must have SMB signing enabled. By default, Windows Server domain controllers require that the clients use

SMB signing. For Windows Server domains (Windows 2000 and later), SMB signing is set by using a group policy object (GPO) policy. For Windows XP, GPO services for SMB signing are not available; you must use the Windows Registry settings.

Note

Configuring SMB signing through GPOs affects all clients and servers within the domain and overrides individual Registry settings. Refer to Microsoft's security documentation for detailed information about enabling and configuring SMB signing.

In SMB1, enabling signing significantly decreases performance, especially when going across a WAN. There is limited degradation in performance with SMB2 and SMB3 signing as compared to SMB1. The performance impact of signing will be greater when using faster networks.

NOTICE

If the older SMB1 protocol does not need to be supported in your environment, it can be disabled by using the `svc_nas` service command. For more information about this service command, see the *Service Commands Technical Notes*.

Configure SMB signing with GPOs

Table 13 on page 55 explains the GPOs available for SMB1 signing.

Note

For SMB2 and SMB3, each version has a GPO for each side (server-side and client-side) to enable the Digitally sign communications (always) option. Neither server-side nor client-side has a GPO to enable the Digitally sign communications (if client agrees) option.

Table 13 SMB1 signing GPOs

GPO name	What it controls	Default setting
Microsoft network server: Digitally sign communications (always)	Whether the server-side SMB component requires signing	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Whether the server-side SMB component has signing enabled	Disabled
Microsoft network client: Digitally sign communications (always)	Whether the client-side SMB component requires signing	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Whether the client-side SMB component has signing enabled	Enabled

You can also configure SMB signing through the Windows Registry. If a GPO service is not available, such as in a Windows NT environment, the Registry settings are used.

Configure SMB signing with the Windows Registry

Registry settings affect only the individual server or client that you configure. Registry settings are configured on individual Windows workstations and servers and affect individual Windows workstations and servers.

Note

The following Registry settings pertain to Windows NT with SP 4 or later. These Registry entries exist in Windows Server, but should be set through GPOs.

The server-side settings are located in: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanserver\parameters\`

Note

For SMB2 and SMB3, each version has a Registry key for each side (server-side and client-side) to enable the requiresecuritysignature option. Neither server-side nor client-side has a Registry key to enable the enablesecuritysignature option.

Table 14 Server-side SMB1 signing Registry entries

Registry entries	Values	Purpose
`enablesecuritysignature`	• 0 disabled (default) • 1 enabled	Determines if SMB signing is enabled.
`requiresecuritysignature`	• 0 disabled (default) • 1 enabled	Determines if SMB signing is required.

The client-side settings are located in: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lanmanworkstation\parameters\`

Table 15 Client-side SMB1 signing Registry entries

Registry entries	Values	Purpose
`enablesecuritysignature`	• 0 disabled • 1 enabled (default)	Determines if SMB signing is enabled.
`requiresecuritysignature`	• 0 disabled (default) • 1 enabled	Determines if SMB signing is required.

IP packet reflect

IP packet reflect provides your network with an additional security level. Because the majority of network traffic on a NAS server (including all file system I/O) is client initiated, the NAS server uses Packet Reflect to reply to client requests. With Packet Reflect, there is no need to determine the route to send the reply packets. Because reply packets always go out the same interface as the request packets, request packets cannot be used to indirectly flood other LANs. In cases where two network devices exist, one connected to the Internet and the other connected to the intranet, replies to Internet requests do not appear on the intranet. Also, the internal networks used by the storage system are not affected by any packet from external networks.

IP packet reflect can be enabled for each NAS server. It is disabled for all NAS servers by default.

IP multi-tenancy

IP multi-tenancy provides the ability to assign isolated, file-based storage partitions to the NAS servers on a storage processor. Tenants are used to enable the cost-effective management of available resources, while at the same time ensuring that tenant visibility and management is restricted to assigned resources only.

Note

If this is the first creation of a tenant in your environment, have the system automatically generate a Universal Unique Identifier (UUID) value for the tenant. For existing tenants in your environment that have a system generated UUID value, enter that UUID value manually.

With IP multi-tenancy, each tenant can have its own:

- IP addresses and port numbers.
- VLAN domain.
- Routing table.
- IP firewall.
- DNS server or other administrative servers to allow the tenant to have its own authentication and security validation.

IP multi-tenancy is implemented by adding a tenant to the storage system, associating a set of VLANs with the tenant, and then creating one NAS server for each of the tenant's VLANs, as needed. It is recommended that you create a separate pool for the tenant and that you associate that pool with all of the tenant's NAS servers.

Note

A pool is a set of drives that provide specific storage characteristics for the resources that use them.

Note the following about the IP multi-tenancy feature:

- There is a one-to-many relationship between tenants and NAS servers. A tenant can be associated with multiple NAS servers, but a NAS server can be associated with only one tenant.
- You can associate a NAS server with a tenant when you create the NAS server. Once you create a NAS server that is associated with a tenant, you cannot change any of its properties.
- During replication, data for a tenant is transferred over the service provider's network rather than the tenant's network.
- Because multiple tenants can share the same storage system, a spike in traffic for one tenant can negatively impact the response time for other tenants.

About VLANs

VLANs are logical networks that function independently of the physical network configuration. For example, VLANs enable you to put all of a department's computers on the same logical subnet, which can increase security and reduce network broadcast traffic.

When a single NIC is assigned multiple logical interfaces, a different VLAN can be assigned to each interface. When each interface has a different VLAN, a packet is

accepted only if its destination IP address is the same as the IP address of the interface, and the packet's VLAN tag is the same as the interface's VLAN ID. If the VLAN ID of an interface is set to zero, packets are sent without VLAN tags.

There are two ways to work with VLANs:

- Configure a switch port with a VLAN identifier and connect a NAS server port or iSCSI interface to that switch port. The Unity system is unaware that it is part of the VLAN, and no special configuration of the NAS server or iSCSI interface is needed. In this case, the VLAN ID is set to zero.
- Implement IP multi-tenancy using VLANs. In this scenario, each tenant is associated with a set of one or more VLANs, and the NAS server is responsible for interpreting the VLAN tags and processing the packets appropriately. This enables the NAS server to connect to multiple VLANs and their corresponding subnets through a single physical connection. In this method, the switch ports for servers are configured to include VLAN tags on packets sent to the server.

Management support for FIPS 140-2

Federal Information Processing Standard 140-2 (FIPS 140-2) is a standard that describes US Federal government requirements that IT products should meet for Sensitive, but Unclassified (SBU) use. The standard defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems. To learn more about FIPS 140-2, refer to FIPS 1402-2 publication.

The storage system supports FIPS 140-2 mode for the SSL modules that handle client management traffic. Management communication into and out of the system is encrypted using SSL. As a part of this process, the client and the storage management software negotiate a cipher suite to use in the exchange. Enabling FIPS 140-2 mode restricts the negotiable set of cipher suites to only those that are listed in the FIPS 140-2 Approved Security Functions publication. If FIPS 140-2 mode is enabled, you may find that some of your existing clients can no longer communicate with the management ports of the system if they do not support FIPS 140-2 Approved cipher suites. FIPS 140-2 mode cannot be enabled on a storage system when non-FIPS-compliant certificates exist in the certificate store. You must remove all non-FIPS compliant certificates from the storage system before you enable the FIPS 140-2 mode.

Managing FIPS 140-2 mode on the storage system

Only the Administrator and Security Administrator have the privileges to manage the FIPS 140-2 mode setting. Use the following CLI command to set the FIPS 140-2 mode setting on a storage system:

`uemcli /sys/security set -fips140Enabled yes` will set it to FIPS 140-2 mode.

`uemcli /sys/security set -fips140Enabled no` will set it to non-FIPS 140-2 mode.

Use the following CLI command to determine the current FIPS 140-2 mode for the storage system:

```
uemcli /sys/security show
```

When you change the FIPS 140-2 mode setting on a storage system, both SPs are automatically rebooted in sequence in order to apply the new setting. When the first SP has completed rebooting, the other SP is rebooted. The system will only operate fully in the configured FIPS 140-2 mode after both SPs have completed rebooting.

Management support for SSL communications

Management communication into and out of the storage system is encrypted using SSL. As a part of this process, the client and the storage system negotiate an SSL protocol to use. By default, the storage system supports TLS 1.0, TLS 1.1, and TLS 1.2 protocols for SSL communications. The storage system includes an administrative setting to disable TLS 1.0 from the system. Disabling the TLS 1.0 protocol using this setting means that the storage system will only support SSL communications using the TLS 1.1 and TLS 1.2 protocols and TLS 1.0 will not be considered a valid protocol.

Note

Disabling TLS 1.0 may impact existing client applications which are not compatible with TLS 1.1 or TLS 1.2 protocols. In this case, TLS 1.0 support should remain enabled. The following functionality will not work when TLS 1.0 is disabled:

- Technical advisories
- Software, drive firmware, and language pack upgrade notifications
- Replication from OE versions earlier than 4.3 to OE version 4.3

Managing TLS 1.0 on the storage system

Only the Administrator or Security Administrator have the privileges to manage the TLS 1.0 enable setting. Use the following command to set the TLS 1.0 enable setting on a storage system:

`uemcli /sys/security set -tls1Enabled yes` enables the use of the TLS 1.0 protocol.

`uemcli /sys/security set -tls1Enabled no` disables the use of the TLS 1.0 protocol.

For more information about this command, refer to the *Unisphere Command Line Interface User Guide*.

Management support for restricted shell (rbash) mode

The storage system SSH service interface is hardened with restricted shell (rbash) mode. This feature is enabled by default for the service account upon upgrading to Unity OE version 4.5 or later. Although temporarily disabling restricted shell mode is possible, it is not persistent and it will be automatically re-enabled when one of the following occurs:

- The primary Service Processor is re-booted.
- 24 hours elapse since restricted shell mode was disabled.

This feature enhances the security posture of the Unity storage system by restricting service account users to the following functions:

- Operate only a limited set of commands that are assigned to a member of a non-privileged Linux user account in restricted shell mode. The service user account does not have access to proprietary system files, configuration files, or user or customer data.
- Restricts service users from executing untrusted code that could be potentially leveraged to exploit local privilege escalation vulnerabilities.

Besides service scripts, a white list contains basic commands that are available to service personnel. These are the safe commands or the commands with security control from which users cannot escape the restricted shell mode. These commands are essential for Dell EMC service personnel to provide maintenance service without elevating the privilege to root. For information about these commands, see Knowledge Based Article 528422.

NOTICE

A network vulnerability scan cannot be performed with restricted shell by default. Unisphere Admin users need to disable restricted shell mode in order to facilitate a security scan. For maximum system security, it is highly recommended to leave the restricted shell mode enabled at all times unless it is needed to perform a security scan. To ensure that the system is not exposed to local privilege escalation vulnerabilities, enable restricted shell mode as soon as the security scan completes.

Managing restricted shell mode on the storage system

Only the Administrator has the privileges to manage the restricted shell mode setting. Use the following CLI command to set the restricted shell mode setting on a storage system:

`uemcli /sys/security set -rbashEnabled yes` enables restricted shell mode for service user mode.

`uemcli /sys/security set -rbashEnabled no` disables restricted shell mode.

Use the following CLI command to determine the current restricted shell mode for the storage system:

```
uemcli /sys/security show
```

CHAPTER 5

Data Security Settings

This chapter describes the security features that are available on the storage system for supported storage types.

Topics include:

About Data at Rest Encryption (physical deployments only)

Data at Rest Encryption (D@RE) is provided through controller-based encryption (CBE) at a physical drive level. The goal of this feature is to ensure that all customer data and identifying information will be encrypted with strong encryption, primarily to ensure security in the event of loss of a drive.

A unique data encryption key (DEK) is generated for each drive and is used to encrypt data as it is sent to the drive. The DEK is used to encrypt/decrypt user data using 256-bit Advanced Encryption Standard (AES) algorithm with the XOR Encrypt XOR Tweakable Block Cipher with Ciphertext Stealing (XTS) mode of operation.

The Key Encryption Key (KEK) is a 256-bit randomly generated key created by RSA BSAFE and is used to wrap the DEKs at the time of DEK generation so that the DEKs are protected and secured as they move through the storage system. The algorithm used to wrap and unwrap the DEKs using the KEK is 256-bit AES Key Wrap, as specified in RFC 3394.

The Key Encryption Key Wrapping Key (KWK) is a 256-bit randomly generated key created by RSA BSAFE and is used to wrap the KEK at the time of generation so that the KEK is protected as it travels throughout the array and to the SAS (Serial Attached SCSI) controller. The algorithm used to wrap and unwrap the KEK using the KWK is 256-bit AES Key Wrap, as specified in RFC 3394.

Separate from CBE, system space on the Storage Processors (SPs) is encrypted using an encryption capability (dm_crypt) that is native to the Linux distribution. Specific partitions on the system drive are encrypted by default unless encryption is not activated on the system at manufacture time. For those system partitions that are not encrypted, some unencrypted data, such as diagnostic dumps, could be present. In addition, there is potential for small amounts of unencrypted user data as a result of writing diagnostic materials to the system partition. All the data written to the array by using regular I/O protocols (iSCSI, FC) are encrypted. Anything that comes into the array by using the control path will not be encrypted by this solution; however, information that is sensitive (for example, passwords) are encrypted by a different mechanism (as they are on non-encrypting arrays).

A component, referred to as the Key Manager, is responsible for generating, storing and otherwise managing the encryption keys for the system. The keystore that is generated to store the encryption keys resides on a managed LUN in private space on the system. Keys are generated or deleted in response to notifications that a storage pool has been added or removed. Key backups are performed automatically by the system. In addition, changes to the configuration of the system that result in changes to the keystore will generate information alerts that recommend key backups be created. When an operation that results in a change to the keystore occurs, an alert will appear and persist.

A separate auditing function is provided for general key operations that track all key establishment, deletion, backup, and restore changes as well as SLIC addition.

For additional information about the Data at Rest Encryption feature, refer to the *Unity: Data at Rest Encryption* white paper.

Feature activation

D@RE is a licensed feature. The license must be installed during the initial configuration of your system. Once activated, the encryption operation cannot be reverted.

The encryption operation will cause data encryption keys to be created and all user data will begin to be encrypted. The encryption keys are stored in a keystore file. The

keystore file that is generated resides on a managed LUN in private space on the system.

It is strongly recommended that you backup the generated keystore file to another location which is external to the system where the keystore can be kept safe and secret. In the event that the keystore on the system becomes corrupted, the system will be nonfunctional. The system will enter service mode; only the operating system boots. In this state, attempts to access the system through Unisphere will return an error indicating that the keystore is in an inaccessible state. In this case, the backup keystore file and a service engagement are required for resolution.

Encryption status

The following D@RE feature status can be viewed either through Unisphere or a CLI command:

- Encryption Mode: type of encryption in use; for example, Controller-Based Encryption.
- Encryption Status: based on the actual encryption status:
  - Unsupported, encryption of the system space on the SPs is disabled.
  - Not licensed, the Data at Rest Encryption license has not been installed on the system.
  - Encrypted, encryption is complete.
  - Not encrypting, CBE is disabled.
  - Scrubbing, the process of writing random data to unused space on drives or zeroing unbound drives to erase residual data from previous use.

    Note

    For SAS Flash 2 drives, unmap is used to scrub the drives rather than zeroing. For more information about Data at Rest Encryption and the scrubbing process, refer to the *EMC Unity: Data at Rest Encryption* white paper located at Online Support (https://support.emc.com).
  - Encrypting, encryption is in progress.
- KMIP Status, whether KMIP is enabled or disabled.

To view the status of the D@RE feature in Unisphere, select **Settings** > **Management** > **Encryption**. The status of the encryption appears under **Manage Encryption**.

Note

As an alternative, use the CLI command `uemcli -u <username> -p <password> /prot/encrypt show -detail` to view the feature status (Encryption mode, Encryption status, Percent encrypted, Backup keystore status, and KMIP status). You can also use this CLI command to view the status of the keystore and to determine whether any user operations are required. See the *Unisphere Command Line Interface User Guide* for detailed information about these CLI commands.

External key management

Support for external key management is provided through the use of the Key Management Interoperability Protocol (KMIP). KMIP defines how a client operates with an external key manager.

Note

External key management is only supported with key management servers that have implemented the KMIP protocol developed by OASIS. If a Gemalto KeySecure KMIP server is used, the Key Manager on the storage system requires the user name and password to be configured on the server.

Enabling and configuring support for KMIP on the storage system is dependent upon encryption being enabled on the storage system. When encryption is enabled and KMIP is enabled, the ignition key is migrated from the storage system to an external key manager, and the local copy is deleted. Also, the old location of the locally stored keys is reprogrammed and cannot be opened once the keys are migrated. Generating a new keystore file backup is recommended.

A user role of administrator or storage administrator is required to configure external key management. To configure external key management, select **Settings** > **Management** > **Encryption** and, under **Manage Encryption** > **External Key Management**, select **Configure**. Fill in the information that is required in the dialog box that appears to configure key management server properties and to add the KMIP server to the KMIP server cluster. The dialog box also provides the means to import and manage the relevant CA and client certificates and to verify the configuration. The configuration requires two certificates:

- CA certificate in PEM format
- A password protected PKCS #12 file which contains the client certificate

A copy of the configuration for the KMIP server, including the certificates and server configuration data, is stored locally in secure locations on the storage system as well as backend system drives to provide redundancy.

Note

For compatibility and interoperability information related to the KMIP servers, refer to the Simple Support Matrix for the storage system on the support website.

Certificates are downloaded onto the active SP. At boot time, whenever a problem with certificate is reported, the system restores the certificates from its local copy of the lockbox, and retries. If it fails again, the system goes into service mode. If a difference is found, the lockbox content on the backend is updated.

Note

As an alternative, use the CLI command `uemcli -u<username> -p<password> /prot/encrypt/kmip -set -username <value> {-passwd <value> | -passwdSecure} -port <value> [-timeout <value>] -server <value>` to configure KMIP. Use the CLI command `uemcli -u<username> -p<password> /sys/cert [ -type { CA | Server | Client | TrustedPeer } ] [ -service {Mgmt_LDAP | Mgmt_KMIP | VASA_HTTP } [ -scope <value> ] ] [ -id <value> ]` to import CA and client certificates. Use the CLI command `uemcli -u<username> -p<password> /prot/encrypt/kmip -verify` to verify the configuration. See the *Unisphere Command Line Interface User Guide* for detailed information about these CLI commands.

If there is a problem with or unexpected change to the KMIP configuration or status, the system cannot confirm the correct configuration or status and starts in Service Mode. The system cannot return to Normal Mode until the issue is resolved. A service

script, `svc_kmip`, can be used to restore the correct KMIP server configuration and, if necessary, the Unity certificates so that the system can return to Normal Mode.

NOTICE

The service script, `svc_kmip`, is only for recovery and cannot be used to set up the KMIP configuration and enable it on a new system. For more information about this service script, see the *Service Commands Technical Notes*.

Backup keystore file

Changes to the configuration of the system that result in changes to the keystore generate information alerts which persist and recommend key backups be created. A new alert will be generated only after the keystore has been retrieved from the system for backup.

Note

It is strongly recommended to backup the generated keystore file to another location which is external to the system where the keystore can be kept safe and secret. In the event that the keystore files on the system become corrupted and in an inaccessible state, the system will enter service mode. In this case, the backup keystore file and a service engagement are required for resolution.

A user role of administrator or storage administrator is required to backup the keystore file. To backup the keystore file to a location that is external to the system where the keystore can be kept safe and secret, select **Settings** > **Management** > **Encryption** and, under **Manage Encryption** > **Keystore**, select **Backup Keystore File**. The dialog box that appears directs you through the steps to backup the generated keystore file.

Note

As an alternative, use the CLI command `uemcli -u<username> -p<password> -download encryption -type backupKeys` to backup the keystore file to a location that is external to the system where the keystore can be kept safe and secret. See the *Unisphere Command Line Interface User Guide* for detailed information about this CLI command.

Data at Rest Encryption audit logging

The D@RE feature provides a separate auditing function that supports logging of the following keystore operations:

- Feature activation
- Key creation
- Key destroy
- Keystore backup
- Disk encryption completed
- SLIC addition

The audit log for keystore operations is stored in the private space on the system. To download either the entire audit log and checksum information or the information for a specific year and month, select **Settings** > **Management** > **Encryption** and, under **Manage Encryption** > **Audit Log**, select **Download Audit Log & Chksum**. To download a newly generated checksum file for the audit log file that was retrieved at

an earlier time, select **Settings** > **Management** > **Encryption** and, under **Manage Encryption** > **Audit Log**, select **Download Chksum**. The filename that you supply must match exactly to the auditlog file that was retrieved previously.

Note

As an alternative, use the `uemcli -u<username> -p<password> -download encryption -type auditLog -entries <all or YYYY-MM>` CLI command to download the entire audit log and checksum information or a partial audit log, respectively. See the *Unisphere Command Line Interface User Guide* for detailed information about this CLI command.

Hot spare operations

When a system is already configured with DEKs for all the disk drives in the system that are in provisioned pools, drives that are not currently in a provisioned pool are considered unbound drives. Removal of unbound drives or unbound drives that become faulted have no affect on the keystore and therefore do not require a backup of the keystore file. Likewise, replacement of an unbound drive has no affect on the keystore and therefore does not require a backup of the keystore file.

Note

Disk drives that are not bound will be overwritten with default data to remove pre-existing data.

When a system is already configured with DEKs for all the drives in the system that are in provisioned pools, those drives are considered bound drives. If a bound drive is removed or the drive becomes faulted, and after a period of five minutes a permanent hot spare replaces the removed or faulted drive, a DEK is generated for the hot spare, and rebuild begins. The DEK from the removed drive will be removed immediately from the keystore. A keystore modified status will be set by the Key Manager at this point and will trigger an alert to back up the keystore because DEK modifications were made to the keystore.

If the removed disk drive is reinserted anywhere in the system before the five minute period has expired, a rebuild will not be required and modifications will not be made to the keystore. The DEK will remain the same because the key is associated with the disk drive, not the slot. Also, a keystore modified status alert will not be generated.

Note

If sanitizing or destruction of the removed drive is required, it should be done independently.

Adding a disk drive to a storage system with encryption activated

Inserting one or more new disks into the system does not trigger generation of a new DEK for each disk. This operation will not occur for a new disk until the disk is provisioned into a pool. A keystore modified status will be set by the Key Manager at this point and will trigger an alert to back up the keystore because DEK modifications were made to the keystore.

When you add a new disk drive to a storage system, the drive is considered unbound. Disk drives that are not bound are overwritten with default data to remove pre-existing data. Only the addressable space of the drive is overwritten. Any residual

plaintext data that may be hidden in obscured locations within the drive will not be overwritten.

NOTICE

If the potential access to data remnants from the previous use of a drive violates your security policy, you must independently sanitize the drive before it is inserted in the storage system with encryption activated.

Removing a disk drive from a storage system with encryption enabled

When a system is already configured with DEKs for all the drives in the system that are in provisioned pools, those drives are considered bound drives. If a bound drive is removed and after a period of five minutes is not replaced, the DEK for the drive will not be removed from the keystore. The key will remain valid until the provisioned pool is deleted, or until a new drive is swapped in. If the removed disk drive is reinserted anywhere in the system before the five minute period has expired, a rebuild will not be required, as in the case of a replacement drive, and modifications will not be made to the keystore. The DEK will remain the same because the key is associated with the disk drive, not the slot. Also, a keystore modified status alert will not be generated.

Note

If sanitizing or destruction of the removed drive is required, it should be done independently.

Replacing a chassis and SPs from a storage system with encryption enabled

The generated keystore has a relationship to the hardware in the storage system. A service engagement is required to replace a chassis and SPs from a storage system with encryption enabled.

Data security settings

Table 16 on page 67 shows security features available for supported storage system storage types.

Table 16 Security features

Storage type	Port	Protocol	Security settings
iSCSI storage	3260	TCP	• iSCSI host (initiator) level access control is available through Unisphere (allowing clients to access primary storage, snapshots, or both). • CHAP authentication is supported so that storage system iSCSI Servers (targets) can authenticate iSCSI hosts (initiators) that attempt to access iSCSI-based storage. • Mutual CHAP authentication is supported so that iSCSI hosts (initiators) can authenticate storage system iSCSI Servers.
SMB storage	445	TCP, UDP	• Authentication for domain and administrative actions is provided through Active Directory user and group accounts.

Table 16 Security features (continued)

Storage type	Port	Protocol	Security settings
			• File and share access controls are provided through Windows directory services. SMB share access control list (ACL) can also be configured through an SMI-S interface. • Security signatures are supported through SMB signing. • SMB encryption is provided through SMB 3.0 and Windows 2012 for those hosts capable of using SMB. • Supports optional file-level retention services through add-on software.
NFS storage	2049	TCP	• Share-based access control provided through Unisphere. • Support for NFS authentication and access control methods identified in NFS versions 3 and 4. • Supports optional file-level retention services through add-on software.
KDC	88		• Key Distribution Center. Kerberos server that delivers Kerberos tickets to connect to Kerberos services.
Backup and restore			• NDMP security can be implemented based on NDMP shared secrets.

CHAPTER 6

Security Maintenance

This chapter describes a variety of security maintenance features implemented on the storage system.

Topics include:

Secure maintenance

The storage system provides the following secure functions for performing remote system maintenance and update tasks:

- License activation
- Software upgrade
- Software Hotfixes

License update

The license update feature allows users to obtain and install licenses for specific storage system functionality. Table 17 on page 70 shows security features that are associated with the license update feature.

Table 17 License update security features

Process	Security
Obtaining licenses from the EMC Online Support website	License acquisition is performed from within an authenticated session on the EMC Online Support website.
Receiving license files	Licenses are sent to an email address specified within an authenticated EMC Online Support website transaction.
Uploading and installing licenses through Unisphere client to the storage system	• License file uploads to the storage system occur within Unisphere sessions authenticated through HTTPS. • The storage system validates received license files using digital signatures. Each licensed feature is validated by a unique signature within the license file.

Software upgrade

The storage system software update feature allows users to obtain and install software for upgrading or updating the software running on the storage system. Table 18 on page 70 shows security features that are associated with the storage system software upgrade feature.

Table 18 Software upgrade security features

Process	Description
Downloading storage system software from the EMC Online Support website	License acquisition is performed from within an authenticated session on the EMC Online Support website.
Uploading storage system software	Software upload to the storage system occurs within an authenticated Unisphere session through HTTPS.

EMC Secure Remote Services for your storage system

The EMC Secure Remote Services (ESRS) feature provides your authorized service provider with remote access capabilities to your storage system using a secure and encrypted tunnel. For outbound access, the storage system management IP network must allow outbound and inbound HTTPS traffic. The secure tunnel that ESRS establishes between the storage system device and authorized systems on the Support Center network can also be used to transfer files out to the storage system or transfer files back to the Support Center's network.

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

- Centralized ESRS Virtual Edition (VE)
- Integrated ESRS (physical deployments only)

Centralized EMC Secure Remote Services

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

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

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

Integrated EMC Secure Remote Services (physical deployments only)

Note

This feature may not be available in your implementation.

Integrated ESRS runs directly on your storage system. When you select this option, your storage system sets up a secure connection between itself and Support Center servers. The Integrated remote service option can be configured as either outbound only or outbound/inbound, which is the default. The outbound only configuration enables remote service connectivity capability for remote transfer to the Support Center from the storage system. The outbound/inbound configuration enables remote service connectivity capability for remote transfer to and remote transfer from the Support Center with the storage system. When the outbound/inbound configuration option is selected, the connection from the storage system to an optional Policy Manager and any associated proxy servers must be configured through either Unisphere or the CLI.

CHAPTER 7

Security Alert Settings

This chapter describes the different methods available to notify administrators of alerts that occur on the storage system.

Topics include:

Alert settings

Storage system alerts inform administrators of actionable events that occur on the storage system. Storage system events can be reported as shown in Table 19 on page 74.

Table 19 Alert settings

Alert type	Description
Visual notification	Displays informational pop-up messages when users log in to the interface and in real-time to indicate when alert conditions occur. Pop-ups provide basic information about the alert condition. You can obtain additional information from the **Settings** > **Alerts** > **Specify Email Alerts and SMTP Configuration**. **Note** Storage system visual alert notifications are not configurable. Also, the storage system does not have an option of authentication to an SMTP mail server. If your mail server requires all clients to authenticate to relay an email, the storage system cannot send email alerts through that mail server.
Email notification	Enables you to specify one or more email addresses to which to send alert messages. You can configure the following settings: • Email addresses to which to send storage system alerts. • Severity level (critical, error, warning, notice, or information) required for email notification. **Note** For storage system alert email notification to work, you must configure a target SMTP server for the storage system.

SNMP traps	Transfer alert information to designated hosts (trap destinations) that act as repositories for generated alert information by the storage network system. You can configure SNMP traps through Unisphere. Settings include:
	• IP address of a network SNMP trap destination
	• Optional security settings for trap data transmission
	  ▪ Authentication protocol: Hashing algorithm used for SNMP traps (SHA or MD5)
	  ▪ Privacy protocol: Encryption algorithm used for SNMP traps (DES or AES)
	  ▪ Version: Version used for SNMP traps (v2c or v3)
	  ▪ Community: SNMP community string (applicable only to v2c SNMP destination)
	The Unisphere Online Help provides more information.

EMC Secure Remote Services (ESRS)	ESRS provides an IP-based connection that enables EMC Support to receive error files and alert messages from your storage system, and to perform remote troubleshooting resulting in a fast and efficient time to resolution. **Note** Available with operating environment (OE) version 4.0 or later. For ESRS to work, you must enable it on the storage system.

Configuring alert settings

You can configure storage system alert settings for email notifications and SNMP traps from the storage system.

Configure alert settings for email notifications

Using Unisphere:

Procedure

1. Select **Settings** > **Alerts** > **Email and SMTP**.
2. In the **Specify Email Alerts and SMTP Configuration** section under **Send email Alerts to the following email list**, configure the email addresses to which to send alert notifications.
3. Under **Severity level of alerts to send:**, configure the severity level at which alert email messages are generated to one of the following:
   - Critical
   - Error and Above
   - Warning and Above
   - Notice and Above
   - Information and Above

   Note

   For the storage system alert email mechanism to work, a target SMTP server must be configured for the storage system.
4. Under **Specify SMTP network settings:**, configure the target SMTP server.

Configure alert settings for SNMP traps

Using Unisphere:

Procedure

1. Select **Settings** > **Alerts** > **SNMP**.
2. In the **Manage SNMP Alerts** section under **Send alerts through SNMP traps to these destinations:**, configure the following information for the SNMP trap destinations:
   - Network name or IP address
   - Authentication protocol to use
   - Privacy protocol to use
   - Version of SNMP to use
   - Community string (applicable to v2c SNMP only)
3. Under **Severity level of alerts to send:**, configure the severity level at which SNMP traps are generated to one of the following:

- Critical
- Error and above
- Warning and above
- Notice and above
- Information and above

CHAPTER 8

Other Security Settings

This chapter contains other information that is relevant for ensuring the secure operation of the storage system.

Topics include:

About STIG

A Security Technical Implementation Guide (STIG) defines a configuration and maintenance standard for computer deployments required by the US Department of Defense (DoD) Information Assurance (IA) program. These guidelines are designed to enhance security settings and configuration options before the systems are connected to a network. More information about the various STIGs is available at http://iase.disa.mil/stigs/index.html.

Some of the hardening steps to meet STIG requirements are turned on by running service scripts. The `svc_stig` service command enables or disables STIG mode on a Unity system (physical deployments only) and provides the status of the STIG mode. This service command provides a simple and automated mechanism to apply these changes. These changes can also be undone if there is a requirement to do so at a later date (for example, to troubleshoot an operational issue).

Note

While the changes implemented by the STIG mode to configuration and management options can be undone, not all of the related settings are returned to their default values. Some settings, such as permission and privilege changes to file systems at the OE level, are retained.

The storage system persists the STIG mode, and it remains preserved through software upgrade.

Manage STIG mode (physical deployments only)

When STIG mode is enabled through the `svc_stig` service command, the status of each of the STIGs (Category I or Category II, or both) that are applied is shown. You can specify the categories that get applied, however, using `svc_stig -e` without specifying options applies both CAT I and CAT II STIGs by default. When CAT II is enabled, both the storage system SSH service interface and Unisphere will show a DoD login banner for interactive sessions.

To harden your storage system, follow these three steps in order:

1. Enable STIG mode. This process applies the changes on the passive SP and reboots the passive SP. Once the passive SP is fully up, it becomes the active SP. The changes are then applied on the previous active SP and a reboot is issued on that SP.
2. Enable FIPS 140-2 mode. This process causes the SPs to reboot again. For information about FIPS 140-2 mode, see Management support for FIPS 140-2 on page 58.
3. Enable STIG-compliant user account settings. For information about STIG-compliant user account settings, see Manage user account settings within STIG mode (physical deployments only) on page 80.

To disable hardening of your storage system, follow these three steps in order:

1. Disable STIG-compliant user account settings.
2. Disable FIPS 140-2 mode.
3. Disable STIG mode.

Use Cases

```
Usage: svc_stig [<qualifiers>] where the qualifiers are:

  -h|--help             : Display this message
  -d|--disable       [options] : Disable STIGs
  -e|--enable        [options] : Enable STIGs
  -s|--status        [options] : Get status for STIGs

This script enables, disables, and provides current status for each
catgory of STIGs.

See the help text below for more information on options.

Refer to the system documentation for a complete description of
STIGs
supported.

-d|--disable:
  Used to Disable all STIGs (no option specified).
  Options:

    -c|--cat [X]    : disable a specific category of STIGs

-e|--enable:
  Used to Enable all STIGs (no option specified).
  Options:

    -c|--cat [X]    : enable a specific category of STIGs

-s|--status:
  Used to show the current status (enabled or disabled) for all
STIGs
  (no option specified).
  Options:

    -c|--cat [X]    : show status for a specific Category of STIGs
    -b|--boolean-format : show boolean status for a specific
Category of STIGs
```

Example 1 Enable STIG mode

```
12:51:21 service@OB-M1204-spb spb:~> svc_stig -e
##################################################################
###########
WARNING:
WARNING: This action will cause a reboot of the system!!
WARNING:
##################################################################
###########

##################################################################
###########
INFO:
INFO: Both Storage Processors will reboot in sequence, starting
with peer SP.
INFO: When primary SP comes back from reboot, the process will
automatically
INFO: restart to finish applying. Monitor status with 'svc_stig -
s'. If status
INFO: does not change to expected value within 30 minutes, contact
service
INFO: provider.
INFO:
```

Example 1 Enable STIG mode (continued)

```
##################################################################
###########
Enter "yes" if want to proceed with this action:
```

Example 2 Show STIG mode status

```
13:25:15 service@OB-M1204-spa spa:~> svc_stig -s
STIG CATEGORY 1: ENABLED
STIG CATEGORY 2: ENABLED
```

Manage user account settings within STIG mode (physical deployments only)

A user with an administrator or security administrator role has the capability to enable, disable, view, and configure settings related to user accounts. The settings apply to all user accounts unless specified otherwise. When user account settings is enabled without specifying a particular value for each setting, the default value that is STIG-compliant is automatically applied. When user account settings is disabled, each setting reverts to its value before the functionality was enabled. The following functionality for user account settings is only applicable on systems that have STIG mode enabled:

- Additional password requirements
- Failed login requirements
- Lockout period
- Session idle timeout
- Enable default admin lockout

The following is a summary of the limitations for the user account settings functionality:

- The functionality is only available through the UEMCLI commands `/user/account/settings set` and `/user/account/settings show`.
- Only a user with an administrator or security administrator role can perform this command.
- The password for the default admin account never expires.
- The command returns an error if it is used when STIG mode is not enabled.
- This functionality needs to be enabled separately after STIG mode is enabled.
- This functionality needs to be disabled separately before STIG mode is disabled.

Additional Password requirements

Additional password requirements are added for user accounts created or modified after STIG mode is enabled:

- Minimum password size

- Password count
- Password period

The minimum password size (`-passwdMinSize`) setting represents the minimum size that passwords for local user accounts must meet when a user account is created or when a password is modified. The minimum size for the password can be configured to be within the range of 8 - 40 characters. The default value when user account settings is enabled without specifying the minimum password size is 15 characters. When user account settings is disabled, the minimum password size is set to 8 characters. Any change to this setting does not impact local user accounts that were created prior to the change unless the password is modified.

The password count (`-passwdCount`) setting represents the number of passwords that cannot be reused for local user accounts. The password count can be configured to be within the range of 3 - 12 passwords. The default value when user account settings is enabled without specifying the password count is 5 passwords. When user account settings is disabled, the password count is set to 3 passwords. This setting impacts all pre-existing and new local user accounts.

The password period (`-passwdPeriod`) setting represents the time period in days when the password expires for local user accounts. The password period can be configured to be within the range of 1 - 180 days, where the value -noPasswdPeriod means that a password will never expire. The default value when user account settings is enabled without specifying the password period is 60 days. When user account settings is disabled, the password period is set to empty. This setting impacts all pre-existing and new local user accounts. However, this setting does not apply to the default admin user account in which the password never expires.

Password expiration status

A user with an administrator or security administrator role can view the password expiration status parameter for all local user accounts. This parameter cannot be set. It can only be viewed when the `-detail` option is specified in the `/user/account/settings show` UEMCLI command.

The password expiration status for a user account appears as one of the following values:

- N/A: Appears when a password is set to never expire, when the user account is of type LDAP, or when user account settings is disabled.
- # days remaining: Appears when user account settings is enabled and the password period is configured to a value greater than 0.
- expired: Appears when the password has expired for the user account.

Failed login requirements

The following failed login requirements are added for local user accounts after STIG mode is enabled:

- Maximum failed logins
- Failed login period

The maximum number of consecutive failed logins allowed for local user accounts can be configured to be within the range of 1 - 10 consecutive failed logins. The default value when user account settings is enabled without specifying the maximum failed logins is 3 consecutive failed logins. When user account settings is disabled, the maximum number of consecutive failed logins is set to empty.

Note

The failed login period (`-failedLoginPeriod`) and lockout period (`-lockoutPeriod`) settings must be specified with a value when the maximum failed logins (`-maxFailedLogins`) setting is specified. The value `-noMaxFailedLogins` means that there is no maximum on the number of consecutive failed logins that are allowed. Also, `-noFailedLoginPeriod` and `-noLockoutPeriod` must be specified when `-noMaxFailedLogins` is specified. For more information about these settings, see Disabling/Re-enabling failed login counting on page 82.

The failed login period setting represents the time period in seconds in which the number of failed logins are tracked for local user accounts. The time period can be configured to be within the range of 1 - 3600 seconds. The default value when user account settings is enabled without specifying the failed login period is 900 seconds. When user account settings is disabled, the failed login period is set to empty.

Note

The failed login period (`-maxFailedLogins`) and lockout period (`-lockoutPeriod`) settings must be specified with a value when the failed login period (`-failedLoginPeriod`) setting is specified. The value `-noFailedLoginPeriod` means that the number of consecutive failed logins is not being tracked within a time period. Also, `-noMaxFailedLogins` and `-noLockoutPeriod` must be specified when `-noFailedLoginPeriod` is specified. For more information about these settings, see Disabling/Re-enabling failed login counting on page 82.

Lockout period

The lockout period setting represents the time period in seconds in which the local user account is locked when the maximum number of consecutive failed logins has been reached within the failed login time window. The time period can be configured to be within the range of 1 - 86400 seconds. The default value when user account settings is enabled without specifying the lockout period is 3600 seconds. When user account settings is disabled, the lockout period is set to empty.

Note

The maximum failed logins (`-maxFailedLogins`) and failed login period (`-failedLoginPeriod`) settings must be specified with a value when the lockout period (`-lockoutPeriod`) setting is specified. The value `-noLockoutPeriod` means the account will not be locked due to meeting the maximum failed logins requirement within the failed login period requirement. Also, `-noMaxFailedLogins` and `-noFailedLoginPeriod` must be specified when `-noLockoutPeriod` is specified. For more information about these settings, see Disabling/Re-enabling failed login counting on page 82.

Disabling/Re-enabling failed login counting

A user with an administrator or security administrator role may choose to disable all login restrictions by simultaneously setting `-noMaxFailedLogins`, `-noFailedLoginPeriod`, and `-noLockoutPeriod` in one command, for example:

```
uemcli -d 10.0.0.1 -u Local/admin -p MyPassword456! /user/account/
settings set -noMaxFailedLogins -noFailedLoginPeriod -noLockoutPeriod
```

⚠ CAUTION

It is not recommended to run this command while in STIG mode. While this setting is in effect, a brute-force password attack could be allowed because no checking is being performed.

To re-enable all login restrictions, simultaneously set `-maxFailedLogins`, `-failedLoginPeriod`, and `-lockoutPeriod` with values in one command, for example:

```
uemcli -d 10.0.0.1 -u Local/admin -p MyPassword456! /user/account/
settings set -maxFailedLogins 3 -failedLoginPeriod 900 -lockoutPeriod
3600
```

Session idle timeout

The session idle timeout setting represents the time period in seconds in which a session for a user can be idle before the session is automatically terminated. The time period can be configured to be within the range of 1 - 3600 seconds. The default value when user account settings is enabled without specifying the session idle timeout is 600 seconds. When user account settings is disabled, the session idle timeout is set to empty. This setting is applicable to both local and LDAP user accounts.

Note

The value `-noSessionIdleTimeout` means the session will not timeout due to being idle.

Enable default admin lockout

The enable default admin lockout setting represents whether the manual and automatic account lockout functionality will apply to the local default admin user account. This setting can be configured to be either `yes` or `no`. The default value is `no` when user account settings is enabled without specifying this setting. A `no` value means that the manual and automatic account lockout functionality do not apply to the local default admin user account.

Manual account lock/unlock (physical deployments only)

A user with an administrator role has the capability to manually lock/unlock user accounts. Once a user account is manually locked, the user is unable to successfully authenticate even if the credentials are valid. Also, the user account remains locked until an administrator manually unlocks the user account.

The following is a summary of the limitations for the manual lock/unlock functionality:

- The functionality is only available through the UEMCLI, `/user/account/ -id <administrator_id> set -locked {yes|no}`.
- Only a user with an administrator role can perform this command.
- The default admin account cannot be locked/unlocked.
- A user cannot lock/unlock their own accounts.
- The command returns an error if it is used when STIG mode is not enabled.

Physical security controls (physical deployments only)

The area where the storage system resides must be chosen and modified to provide for the physical security of the storage system. These include basic measures such as

providing sufficient doors and locks, permitting only authorized and monitored physical access to the system, providing reliable power source, and following standard cabling best practices.

In addition, the following storage system components require particular care:

- Password reset button: Temporarily resets the factory default passwords for both the storage system default administrator account and service account - until an administrator resets the password.
- SP Ethernet service port connector: Allows authenticated access through an SP Ethernet service port connection.

Antivirus protection

The storage system supports Common AntiVirus Agent (CAVA). CAVA, a component of the Common Event Enabler (CEE), provides an antivirus solution to clients using a storage system. It uses an industry-standard SMB protocol in a Microsoft Windows Server environment. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the storage system. The CEE installer, which contains the CAVA installer, and the CEE release notes are available at Online Support under **Support By Product** for Unity Family, UnityVSA, Unity Hybrid, or Unity All Flash in **Downloads** > **Full Release**.

APPENDIX A

TLS cipher suites

This appendix lists the TLS cipher suites supported by the storage system.

Topics include:

Supported TLS cipher suites

A cipher suite defines a set of technologies to secure your TLS communications:

- Key exchange algorithm (how the secret key used to encrypt the data is communicated from the client to the server). Examples: RSA key or Diffie-Hellman (DH)
- Authentication method (how hosts can authenticate the identity of remote hosts). Examples: RSA certificate, DSS certificate, or no authentication
- Encryption cipher (how to encrypt data). Examples: AES (256 or 128 bits)
- Hash algorithm (ensuring data by providing a way to determine if data has been modified). Examples: SHA-2 or SHA-1

The supported cipher suites combine all these items.

The following list gives the OpenSSL names of the TLS cipher suites for the storage system and the associated ports.

Table 20 Default/Supported TLS cipher suites supported on the storage system

Cipher Suites	Protocols	Ports
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443, 8444
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443, 8444
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989

Table 20 Default/Supported TLS cipher suites supported on the storage system (continued)

Cipher Suites	Protocols	Ports
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	5989
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	5989
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	5989
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1, TLSv1.1, TLSv1.2	5989
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	5989

APPENDIX B

LDAP Configuration

This appendix describes how to configure the Unity system to connect to an LDAP server for authentication, and how to assign roles to LDAP users and groups.

Topics include:

About configuring LDAP

The Lightweight Directory Access Protocol (LDAP), is an application protocol for querying and modifying directory services running on TCP/IP networks. LDAP helps centralize the management of network authentication and authorization operations. Integrating Unisphere users into an existing LDAP environment provides a way to control management access based on established user and group accounts within the LDAP directory.

Before you configure LDAP, you must configure the Unity system to connect to a DNS server. This action is required to resolve the IP address and fully qualified hostname for each LDAP server that is configured.

Networked entities that exchange data use certificates to authenticate each other. For secure communications to occur between two networked entities, one entity must trust (accept) the certificate from the other. Unisphere uses the SSL/TLS and the X.509 certificate standard to secure client (storage system) and server (LDAP) communications. The Unity system requires the certificate chain file to be uploaded, to properly verify the server certificate received from the LDAP server when the TLS session is established.

After you configure the LDAP settings for the Unity system, you can perform user management functions. For example, you can assign access permissions to Unisphere based on existing users and groups, within the context of an established LDAP directory structure.

Follow this sequence of steps to configure LDAP on a Unity system:

1. Configure the DNS server

   Note

   Required only when host names are used for the LDAP IP addresses or when the dynamic LDAP feature is used. Otherwise, this step is optional.

2. Configure the LDAP server.
3. Verify the LDAP server connection.
4. Configure LDAPS for the LDAP server.
5. Verify the LDAP server connection using the LDAPS protocol.
6. Configure LDAP Users and Groups.

Note

The *Unisphere Online Help* provides more information about LDAP and DNS and the steps to configure the Unity system to connect to an LDAP server and a DNS server, and how to assign roles to and manage LDAP users and groups.

Configure DNS server

DNS must be configured before configuring the LDAP server to resolve the LDAP server addresses. This is required to ensure that the IP address and fully qualified hostname for each LDAP server can be resolved.

To configure the DNS, do the following:

Procedure

1. In Unisphere, click the gear icon in the top menu bar to display the **Settings** page.
2. In the left panel under **Management**, click **DNS Server**.

   The **Manage Domain Name Servers** page appears.
3. Depending on your site configuration, do one of the following:
   - If the system is configured to retrieve the DNS server addresses from a remote source, select **Obtain DNS server address automatically**.
   - For a DNS server that has the LDAP server configured, select **Configure DNS server address manually** and enter at least one IP address. If the LDAP servers are to be manually configured using IP addresses, the LDAP Servers must be in both forward and reverse lookup zones on the DNS server.
4. Once the DNS server addresses are configured, click **Apply** to save the DNS server configuration.

Configure LDAP server

LDAP server configuration consists of specifying the configuration information needed to connect to the LDAP server.

To configure LDAP, do the following:

Procedure

1. In Unisphere, click the gear icon in the top menu bar to display the **Settings** page.
2. In the left panel under **Users and Groups**, click **Directory Services**.

   The **Configure LDAP Server Credentials** page appears.
3. For **Domain Name**, type the Domain name of the LDAP authentication server.

   The Domain name must be filled in when the LDAP server configuration is created. After that, it is grayed out because it cannot be changed without deleting and re-creating the LDAP server configuration.
4. For **Distinguished Name**, type the distinguished name of the LDAP user with administrator privileges.

   The distinguished name should be specified in one of the following formats:
   - LDAP notation format (for example, `cn=Administrator,cn=Users,dc=mycompany,dc=com`)
   - <*user*>@<*domain*> format (for example, `Administrator@mycompany.com`)
   - <*domain*>/<*user*> format (for example, `mycompany.com/Administrator`)
5. For **Password**, type the password for the user specified in **Distinguished Name**.
6. If the LDAP server uses a different port for LDAP than the default port number 389, change the port to the required port number.

   For example, specify port 3268 for LDAP with forest-level authentication. (`nsroot.net` instead of `nam.nsroot.net` using LDAP allows customers to query the entire Active Directory (AD) forest (port 3268) instead of just the AD

domain (TCP port 389). Also, AD role association is based on group scopes for Domain Local Groups and Universal Groups. This allows end-users to search the AD using an appropriate scope as needed and to avoid unnecessary group searches.) It is strongly recommended that LDAP be configured and verified before configuring Secure LDAP (LDAPS). This will minimize any troubleshooting that may be necessary when enabling LDAPS.

7. In **Server Address**, do one of the following:
   - To manually add a server address, click **Add** to display the **LDAP Server** dialog box, enter the IP address or fully qualified hostname, and click **OK**. To remove a server address, select the address in the text box and click **Remove**.
   - To automatically retrieve the server addresses from DNS, click **Auto Discover**.
8. If the LDAP server has a different search path than the default `cn=Users,dc=` for either User or Group, or both, click **Advanced**.

   The **Advanced** dialog box appears.
9. In the **Advanced** window, update the search paths or other fields as necessary, then click **OK** to save the advanced configuration changes.

   For example, if you are configuring forest-level authentication, select **Advanced** to access the **Advanced** window and specify `userPrincipalName` in the **User ID Attribute** field. If the LDAP server has a different search path than the default (cn=Users,dc=) for either users, groups, or both, access the **Advanced** window to update the search paths or other properties as necessary.
10. After all the LDAP configuration information is specified, click **Apply** to save the configuration.

    If **Auto Discover** was selected to automatically retrieve the server addresses from DNS, the server addresses obtained from DNS are displayed grayed out in **Server Address**.

After you finish

After the LDAP server configuration is saved, the configuration should be verified to confirm that the connections to the LDAP server will be successful.

Verify LDAP configuration

To verify connection to the LDAP server will be successful, do the following:

Procedure

1. Click **Verify Connection** on the **Configure LDAP Server Credentials** page.

   If the configuration is valid, a connection will be established with the LDAP server and a green check mark along with the text **Connection Verified** will appear.
2. If the verification fails, the following steps are recommended to troubleshoot the failure:
   a. Verify the **Configure LDAP Server Credentials** configuration information, in particular the **Distinguished Name** (user name), **Password**, and the **Server Address** (IP address or hostname).
   b. Verify the LDAP server is online.

c. Verify there are no network issues; for example, firewall rules that would block access to the LDAP port, network router configuration that prevents the connection, and such.

Configure Secure LDAP

Configuring Secure LDAP (LDAPS) requires the following:

- Configure LDAPS protocol and the port
- Configure the certificate chain

When LDAPS is configured, the Unity system connects to the LDAP server using TLS. The Unity system requires the certificate chain file to be uploaded, to properly verify the server certificate received from the LDAP server when the TLS session is established.

The format of the certificate file to be uploaded is as follows:

- The certificate file must end in a `cer` file extension. Example: `LdapServerChain.cer`
- All certificates in the certificate file to be uploaded must be in PEM format. PEM formatted certificates are ASCII text that begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.
- The LDAP server certificate must have the Server Name, as specified in the LDAP configuration, in the Subject or Subject Alternative Name field in the certificate. This is required to verify that the certificate is from the desired LDAP server.
- If the LDAP server certificate is self-signed, only the server certificate is required.
- If the LDAP server certificate is signed by a Certificate Authority, then the certificate chain, up to the root certificate Authority, must be in the certificate file to be uploaded in the following order:
  1. Intermediate Certificate Authority certificate (if any).
  2. ...
  3. Root Certificate Authority certificate.
  4. If there are multiple certificates in the file to be uploaded, there must be a new line between each certificate.

To configure LDAPS, do the following:

Procedure

1. Click the **Use LDAPS Protocol** checkbox on the **Configure LDAP Server Credentials** page.

   The **Port** is automatically changed to 636, which is the default LDAPS port number. If the LDAP server uses a different port for LDAPS, change the port to the required port number. For example, specify port 3269 for LDAPS with forest-level authentication. (`nsroot.net` instead of `nam.nsroot.net` using LDAPS allows customers to query the entire AD forest (port 3269) instead of just the AD domain (TCP port 636). Also, AD role association is based on group scopes for Domain Local Groups and Universal Groups. This allows end-users to search the AD using an appropriate scope as needed and to avoid unnecessary group searches.) Also, **Upload Certificate** becomes active when the **Use LDAPS Protocol** checkbox is selected.

2. Click **Upload Certificate**.

   The **Upload File** dialog box appears.

3. Click **Choose File**.
4. Browse to the desired certificate file, then select the file and click **Start Upload**.
5. After the file upload completes, click **Apply** to save the configuration changes.

After you finish

It is strongly recommended to verify the configuration after configuring LDAP and uploading the server certificate file.

Verify LDAPS configuration

To verify the LDAPS configuration, do the following:

Procedure

1. Click **Verify Connection** on the **Configure LDAP Server Credentials** page.

   If the configuration is valid, a connection will be established with the LDAP server and a green check mark along with the text **Connection Verified** will appear.
2. If the verification fails, the following steps are recommended to troubleshoot the failure:
   a. Verify the **Configure LDAP Server Credentials** configuration information, in particular the port number.
   b. Verify the LDAP server is online and configured for LDAPS.
   c. Verify the certificates in the uploaded certificate file are valid, for example, not expired and in the correct order.
   d. Verify the configured **Server Name** is in the Subject or Subject Alternative Name field in the LDAP server certificate.
   e. Verify there are no network issues; for example, firewall rules that would block access to the LDAPS port, and such.

After you finish

After the LDAP server is configured, one or more LDAP users or groups must be added to the Unity system to map the users (or groups) to roles. Otherwise, LDAP authentication will succeed on login, but the login will fail because no role could be assigned to the user.

Configure LDAP user

The procedure for creating an LDAP group on the Unity system is the same as creating an LDAP user, except that the LDAP group must also be created on the LDAP server, and LDAP users added as members of that group. Creating an LDAP group has the advantage of an LDAP group being configured on the Unity system and then assigned to multiple LDAP users.

To create an LDAP user or group, do the following:

Note

LDAP server must be configured before an LDAP user or group can be created.

Procedure

1. In Unisphere, click the gear icon in the top menu bar to display the **Settings** page.
2. In the left panel under **Users and Groups**, click **User Management**.

   The **Manage Users & Groups** page appears.
3. Click the add icon (plus sign).

   The **Create User or Group** wizard appears.
4. Do one of the following:
   - Click **LDAP User**.
   - Click **LDAP Group**.
5. Click **Next**.

   The **LDAP Information** page appears with the LDAP Authority displayed on the page.
6. For **LDAP User**, type the user name that is listed in the LDAP server.
7. Click **Next**.

   The **Role** page appears.
8. Click the radio button for the role to be assigned.
9. Click **Next**.

   The **Summary** page appears.
10. After verifying that the LDAP user or group name and the role are correct, click **Finish** to complete the transaction or **Back** to change the user configuration.

    When the user or group is successfully created, the **Results** page appears.
11. Click **Close** to close the **Create User or Group** wizard.

    The LDAP user or group just added will appear in the list of users on the **Manage Users and Groups** page.