Technical Report

# Security Hardening Guide for NetApp SANtricity 11.60

## Guidelines for Secure Deployment of SANtricity 11.60

Bernard Chan, NetApp
August 2020 | TR-4855


## Abstract

This security hardening guide provides guidance to help organizations deploy the NetApp E-Series SANtricity® 11.60 to meet prescribed security objectives for information system confidentiality, integrity, and availability.


NetApp®

## TABLE OF CONTENTS



## LIST OF TABLES



## LIST OF FIGURES

# 1 Introduction

The evolution of the current threat landscape presents an organization with unique challenges for protecting its most valuable assets: data and information. The advanced and dynamic threats and vulnerabilities that organizations face are ever increasing in sophistication. Coupled with an increase in the effectiveness of obfuscation and reconnaissance techniques on the part of potential intruders, system managers must address the security of data and information in a proactive manner. This guide seeks to assist operators and administrators in that task by leveraging the confidentiality, integrity, and availability integral to the NetApp solution.

# 2 Local Storage Administrator Accounts

## 2.1 Roles

With role-based access control (RBAC), local users have access to only the systems and options that are required for their job roles and functions. The RBAC solution in SANtricity limits users' administrative access to the level granted for their defined role, which allows administrators to manage local users by assigned role. SANtricity provides several predefined roles. The local user accounts are static and the assigned roles cannot be modified. Table 1 lists the predefined roles in SANtricity.

**Table 1) Predefined roles for local users.**

| Role | Brief Description |
|---|---|
| Admin | Top-level administrative account. This is the only role that allows the user to change the passwords of any local users and run any command supported by the storage system. |
| Security | This role allows the user to modify the security configuration on the storage system, including the ability to view audit logs, configure a secure syslog server, set LDAP/LDAPS server connections, and manage certificates.<br>This role does not provide write access to storage system properties like pool and volume creation/deletion, but it does have read access.<br>It also has privileges to enable/disable SYMbol access to the storage system. |
| Storage | This role has full read/write access to the storage system properties, but with no access to perform any security configuration functions. |
| Support | This role has access to all hardware resources on the storage system, failure data, MEL/audit log, and CFW upgrades. |
| Monitor | This role gives read-only access to all storage system properties. This user cannot view the security configuration. |

Table 2 lists the predefined users and the mapped roles in SANtricity.

**Table 2) Local user-to-roles mapping.**

| Local User | Mapped Roles |
|---|---|
| Admin | Root admin, security admin, storage admin, support admin, monitor |
| Security | Security admin, monitor |
| Storage | Storage admin, support admin, monitor |
| Support | Support admin, monitor |
| Monitor | Monitor |

SANtricity also supports the Lightweight Directory Application Protocol (LDAP/LDAPS) and Active Directory. With LDAP/Active Directory user accounts, administrators can create, modify, or delete custom access control roles, and they can specify account restrictions for specific users.

**Note:** NetApp recommends configuring Secure LDAP with TLS (LDAPS) for added security.

## 2.2 Log-In and Password Parameters

An effective security posture adheres to established organizational policies, guidelines, and any governance or standards that apply to the organization. Examples of these requirements include password-length requirements, handling failed login attempts, and automatic inactive logout of such accounts. The SANtricity solution provides features and functions to address these security constructs.

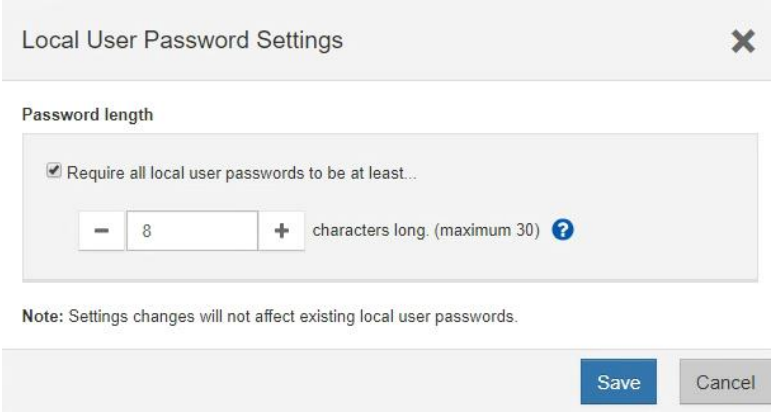
### Configuring Password Policies to Enforce a Minimum Number of Digits (1–30)

NetApp recommends increasing the minimum number of digits for the password length. The default is eight. Figure 1 illustrates the REST API and Figure 2 illustrates the System Manager (Settings > Access Management > View/Edit Settings) window for changing the minimum password length.

**Figure 1) REST API for changing the minimum password length.**

```
Administration > POST/storage-systems/{system-id}/local-users/password-length
{"minimumPasswordLength":30}
```

**Figure 2) System Manager window for changing the minimum password length.**




## Configuring Lockout Settings Due to Failed Login Attempts

### Lockout Mode (IP Address Versus User Name) for Failed Login Attempt

By default, SANtricity tracks the IP address of the web client that failed to log in into the storage system. With this setting, an attacker who has exceeded the maximum number of attempts allowed and is locked out, can go on a different host that has a different IP address, and attempt again. When changed to User Lockout mode, SANtricity locks out the user name after the maximum number of login attempts have been reached.

**Note:** NetApp recommends changing the lockout mode to user-based instead of IP-address-based (default). This setting can be changed by using the REST API, as shown in Figure 3.

### Lockout Time (In Minutes) After the Maximum Login Attempts Have Been Reached

The `lockoutTime` refers to the number of minutes the user is not able to log in to his/her account. The default value is 10 minutes.

**Note:** NetApp recommends leaving the lockout time as 10 minutes (default).

### Maximum Log-in Attempts Before the Account is Locked Out

The `maximumLoginAttempts` refers to the maximum number of attempts that the user is allowed to try before his/her account gets locked out. The default value is six. For example, if the value is set to six, after having entered six failed attempts, the account is locked out. The seventh log-in attempt might contain correct credentials, but SANtricity won't allow access until the user logs in again with the correct credentials after the `lockoutTime` period expires.

There can be up to two controllers in a storage array; the settings above apply to the entire storage array. However, each controller manages the lockout separately, and the accounting is not shared among the two controllers. Because the user can try to gain access to the storage array through either controller A or controller B (by providing either controller's IP address), technically, the user is allowed to have up to two times the value set in `maximumLoginAttempts`.

**Note:** NetApp recommends reducing the maximum number of log-in attempts from six (default) to five. This means on the sixth failed login attempt, the account is locked out. Figure 3 illustrates the REST API settings for the lockout mode, lockout time, and maximum log-in attempts.

**Figure 3) REST API for setting the lockout mode, lockout time, and the maximum log-in attempts.**

```
Administration > POST/storage-systems/{system-id}/settings/lockout
{"lockoutMode": "user", "lockoutTime": 10, "maximumLoginAttempts": 5}
```

### Defining the Account Inactive Limit

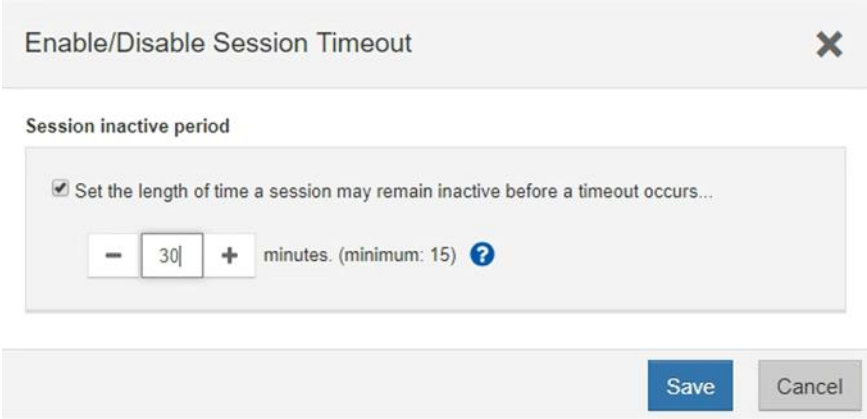
NetApp recommends reducing the session inactivity period from 30 minutes (default) to 15 minutes. This setting can be changed by using the REST API. Figure 4 illustrates the REST API and Figure 5 illustrates the System Manager (Settings > System > Enable/Disable Session Timeout) window for changing the inactive period.

**Figure 4) REST API for changing the inactive period.**

```
Administration > POST/storage-systems/{system-id}/settings/sessions

{"sessionInactivePeriod": <value in seconds>}
```

**Figure 5) System Manager window for changing the inactive period.**




### SHA-512 Support

To enhance password security, SANtricity supports the SHA-2 password hash function and defaults to using SHA-512 for hashing newly created or changed passwords. Operators and administrators can also expire or lock accounts as needed.

Preexisting SANtricity 11.50 user accounts with unchanged passwords continue to use the MD5 hash function after the upgrade to SANtricity 11.50 or later.

**Note:** NetApp strongly recommends that these user accounts migrate to the more secure SHA-512 solution by having users change their passwords.

# 3 System Administrator Methods

## 3.1 Console Access

Establishing secure access to the storage system console is a critical part for a secure troubleshooting. The most common console access options are SSH, Telnet, and RSH. Of these, SSH is the most secure, industry-standard best practice for remote console access.

Console access is reserved for troubleshooting by NetApp Support engineers—it is available through:

- **Serial USB cable**. After it is connected, the console is protected with a user login and password. The password is the same as the storage system password set by the user.
- **SSH**. For security reasons, SSH is disabled by default. If there is a requirement or unique need for a secure remote access, SSH must be manually enabled. The user can manually enable or disable SSH through the secure CLI or through the SANtricity System Manager.

**Note:** NetApp recommends disabling SSH at all times unless instructed by a NetApp Support engineer. The following section describes how to disable and enable SSH through HTTP.

### Disable and Enable SSH Through HTTP

To disable and enable SSH through HTTP, complete the following steps:

1. Allow remote login.

   **Note:** Remote log-in users from outside the LAN should start an SSH session and change the settings on the controller.

   **Note:** For security reasons, enable the remote login for use only by technical support.
2. Select Hardware.
3. If the graphic shows the drives, click Show Back of Shelf.

   The graphic changes to show the controllers instead of the drives.
4. Click the controller for which you want to enable remote login.

   The controller's context menu appears.
5. Select Change Remote Login, and confirm whether you want to perform the operation.

## 3.2 Command-Line Access

The NetApp E-Series storage system has multiple secure command-line access points.

### SANtricity Web Services REST API

To reach the REST API by using a web browser on the host where the proxy is installed, go to `https://localhost/devmgr/docs/#/.`

If this is the first time you are accessing the REST API, each type of browser displays the following:

- Chrome displays Your Connection is Not Private. Click Advanced to proceed to the website.
- Internet Explorer displays There is a Problem with This Website's Security Certificate. Click Continue to This Website (Not Recommended) to proceed to the website.
- Firefox displays Your Connection is Not Secure. Click the Advanced button and add an exception for the certificate to proceed to the website.

  **Note:** For security reasons, NetApp recommends disabling HTTP basic access authentication for the REST API. Figure 6 illustrates the REST API for how to disable Basic Authentication.

**Figure 6) REST API for how to disable Basic Authentication.**

**Administration > POST/storage-systems/ {system-id} /settings/authentication**

**{**

**"disableBasicAuthentication": true**

**}**

### Secure CLI

The secure SMcli allows an SMcli client to interact with a storage system through a secure HTTPS channel. It provides a thin HTTPS client that allows you to interoperate with storage systems by using traditional SANtricity SMcli grammar and command semantics, but with a secure protocol.

### CLI Session Timeout

The default CLI session timeout is 30 minutes. The timeout is important to prevent stale sessions and session piggybacking.

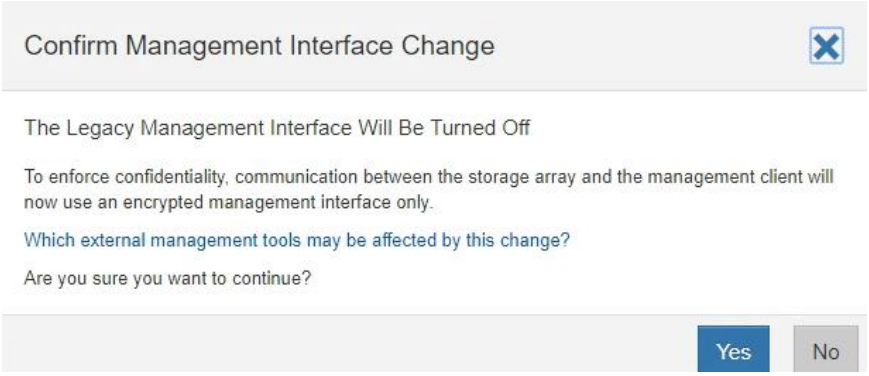
### Legacy Management Interface

Starting in SANtricity 11.40, NetApp introduced the new REST API but kept the proprietary legacy management interface (SYMbol) enabled by default from the factory in order to prevent certain external management tools from not functioning.

Tools that communicate directly with the legacy management interface, such as the SANtricity SMI-S Provider or NetApp OnCommand Insight, do not work unless the Legacy Management Interface setting is enabled. In addition, you cannot use legacy CLI commands or perform mirroring operations if this setting is disabled.

**Note:** If you're not using the affected external management tools, NetApp recommends changing the array to a secure interface by disabling the legacy management interface. Prior to doing that, you must install the appropriate certificate authority (CA) root, intermediate, and signed server certificates on both storage array controllers. After those are installed, change the array management interface to the secure mode by using the System Manager (Settings > System > Additional Settings >Change Management Interface), as shown in Figure 7.

**Figure 7) System Manager window for disabling the legacy management interface.**




## 3.3 Web Access

### SANtricity System Manager

If the SANtricity administrator prefers to use a graphical interface instead of the CLI for accessing and managing the storage system, he/she must use NetApp SANtricity System Manager, which is included with SANtricity as a web service, enabled by default, and accessible by using a browser. Point the browser (using https://) to the host name (if using DNS) or to the IPv4 or IPv6 address.

If the controllers use a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a CA-signed digital certificate.

**Note:** For security purposes, NetApp recommends installing a CA-signed digital certificate on the storage system for server authentication.

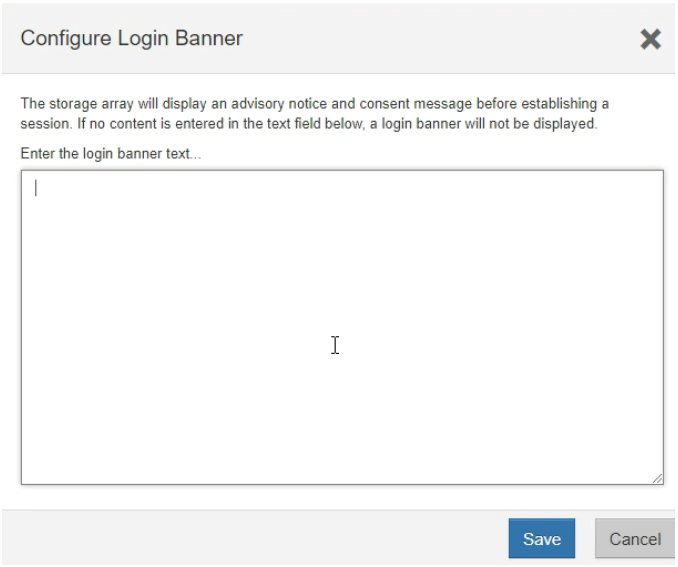
Starting with SANtricity 11.50, Security Assertion Markup Language (SAML) authentication is an option for SANtricity System Manager.

## Log-in Banners

Log-in banners allow an organization to present any operators, administrators, and even miscreants with terms and conditions of acceptable use, and they indicate who is permitted access to the system. This approach is helpful for establishing expectations for access and use of the system. Figure 8 illustrates the System Manager (Settings > System > Configure Login Banner) window on how to configure the log-in banner.

**Figure 8) System Manager window on how to configure the log-in banner.**




## SAML Authentication for SANtricity System Manager

SAML 2.0 is an industry standard for sending authentication requests and user data securely between multiple systems. This standard allows many applications to use a single service to manage all user authentication and session management.

Multifactor authentication (MFA) requires the user to provide two or more items as proof of identity to be successfully authenticated. The separate pieces of evidence are typically at least two of the following types: knowledge (something the user knows, such as a password); possession (something the user has, such as a device that provides a changing code); or inherence (something the user is, such as biometrics, like a fingerprint). The specific type of evidence required is configured by the end-user organization's security team.

Starting with SANtricity OS 11.40.2, SAML is integrated into NetApp E-Series products, making it possible to communicate with an external system that can authenticate a user with multiple forms of authentication and then report the success or failure of the authentication to the SANtricity System Manager application. The external system can be configured to use single-factor, two-factor, or multifactor authentication. The external system also provides the ability to support single sign-on capabilities with other applications.

After SAML is configured on the storage system, logging into SANtricity System Manager is possible only through a configured Identity Provider (IdP). When users attempt to access SANtricity System Manager, they are sent to their IdP's log-in page instead of to the default SANtricity System Manager log-in page. After entering their credentials, users are sent back to SANtricity System Manager with an authenticated session and are authorized based on attributes associated with their identity.

When SAML is enabled, it is the only method used to authenticate users for access to SANtricity System Manager. Other forms of management no longer work because they cannot authenticate. This includes

the EMW, SMcli client, software developer kit client, in-band management using UTM, REST API clients using HTTP basic authentication, and REST API clients using the standard login endpoint.

**Note:** NetApp recommends configuring MFA for added security.

### 3.4 SNMP Monitoring

SANtricity supports alert notifications to be sent through email, SNMP traps, and syslog. Alerts notify administrators about important events that occur on the storage array. SANtricity supports SNMPv2c, which does not support authentication and encryption.

**Note:** For security reasons, NetApp recommends not configuring SNMP, but configure secure syslog instead.

**Note:** If a secure syslog is unavailable, NetApp recommends configuring the SNMP community string in order to secure it. SNMP community string is like a user ID or password that allows access to a device's statistics.

## 4 Storage Administrative System Auditing

### 4.1 Sending Out Syslog

Log and audit information is invaluable to an organization from a support and availability standpoint. In addition, the information and details contained in logs (syslog), audit reports, and outputs are generally of a sensitive nature. To maintain security controls and posture, it is imperative that organizations manage log and audit data in a secure manner.

Offloading of syslog information is necessary for limiting the scope or footprint of a breach to a single system or solution.

**Note:** NetApp recommends securely offloading syslog information to a secure storage or retention location.

Configuration of the secure audit log channel is accomplished either through the SANtricity System Manager GUI or the REST API calls, as described in the following sections. For more information about how to configure syslog for audit logs, see the SANtricity System Manager online help topic "Configure Syslog Server for Audit Logs."

#### Configure Syslog for Audit Logs Using the SANtricity System Manager GUI

To configure syslog for audit logs by using SANtricity System Manager GUI, complete the following steps:

1. Select Settings > Access Management.
2. From the Audit Log tab, select Configure Syslog Servers.

   The Configure Syslog Servers dialog box is displayed.
3. Click Add.

   The Add Syslog Server dialog box is displayed.
4. Enter the server information and click Add:
   - **Server address:** Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.
   - **Protocol:** Select a protocol from the drop-down menu (for example, TLS, UDP, or TCP).
   - **Upload certificate (optional):** If you selected the TLS protocol and have not yet uploaded a signed CA certificate, click Browse to upload a certificate file. Audit logs are not archived to a syslog server without a trusted certificate.

   **Note:** If the certificate later becomes invalid, the TLS handshake will fail. As a result, an error message is posted to the audit log and messages are no longer sent to the syslog server. To

resolve this issue, you must fix the certificate on the syslog server and then go to Settings > Audit Log > Configure Syslog Servers > Test All.

- **Port:** Enter the port number for the syslog receiver.

  After you click Add, the Configure Syslog Servers dialog box opens and displays your configured syslog server on the page.

5. To test the server connection with the storage array, select Test All.

### Configure Syslog for Audit Logs Using the REST API

To configure syslog for audit logs by using the REST API, complete the following steps:

1. Set the syslog configuration for audit log events.

```
POST / storage-systems/ {system-id} / syslog
POST / storage-system/ {system-id} /syslog/{id} // update a specific syslog via server ID
```

2. Payload descriptor (array of syslog server descriptors).

```
[{
serverAddress*         string – Fully qualified name or IP address
port                   integer – example: 514, default: 514
protocol                       string – Transmission protocol (udp, tcp, tls)
example: udp, default: up
components [
type                   string – only supported value is “auditLog”
}]]
```

3. To set up a syslog server for secure transport, use the following payload with the POST request:

```
{
[
“serverAddress”: “153.78.2.2”,
“port”: 443,
“protocol”: “tls”,
“components”: [
{
“type”: “auditLog”
}
]
}
]
```

**Note:** In order for the connection and communication channel to be secure, NetApp recommends using the TLS protocol type. Therefore, the syslog server that is to receive the audit log messages must also be configured to support the TLS protocol (a minimum TLS version of 1.2).

# 5 Storage Encryption

Data-at-rest encryption is important to protect sensitive data in the event of a disk that is stolen, returned, or repurposed. E-Series storage systems provide at-rest data encryption through self-encrypting drives. These drives encrypt data on write operations and decrypt data on read operations regardless of whether the full disk encryption feature is enabled. If the SANtricity feature is not enabled, the data is encrypted at rest on the media, but automatically decrypted on a read request.

When the full disk encryption feature is enabled on the storage system, the drives protect the data at rest by locking the drive from read or write operations unless the storage system provides the correct security or authentication key. This process prevents another storage system from accessing the data without first importing the appropriate security key file to unlock the drives. It also prevents any third-party utility or operating system from accessing the data.

Starting with SANtricity 11.40, NetApp further enhances the full disk encryption feature by enabling you to manage the full disk encryption security key through a centralized key management system, such as

Gemalto SafeNet KeySecure Enterprise Encryption Key Management which adheres to the Key Management Interoperability Protocol (KMIP) standard. This feature is in addition to the internal security key management solution that exists in versions prior to SANtricity 11.40 and is available with the E2800, EF280, E5700, EF570, and EF600.

The encryption and decryption operations performed by the hardware in the drive are invisible to the user and do not affect the performance or user workflow. Each drive has its own unique encryption key that cannot be transferred, copied, or read from the drive. The encryption key is a 256-bit key as specified in the National Institute of Standards and Technology (NIST) AES. The entire drive, not just a portion, is encrypted.

For more information, see TR-4474: SANtricity Drive Security Using SANtricity OS 11.60.

**Note:** NetApp recommends enabling the drive security feature using a centralized key management system.

# 6 Managing SSL and TLS

Secure Sockets Layer (SSL) is the standard technology for keeping an internet connection secure. It safeguards any sensitive data that is being sent between two systems by using an encryption algorithm to scramble the data in transit, preventing hackers from reading it.

Transport Layer Security (TLS) is an updated and more secure version of SSL. These two terms (SSL and TLS) are used interchangeably in the industry.

SANtricity uses SSL to secure the following communication channels:

- SANtricity System Manager web client and the Web Server running on the storage system
- LDAP client running on the storage system and the LDAP/AD server
- Unified Manager/Web Server Proxy running on a host and the Web Server running on the storage system
- Storage system and the AutoSupport Server
- Storage system and the SAML Identity Provider
- Storage system and the syslog server
- Self-Encrypting Drive (SED/FDE) Lock Key Manager running on the storage system and the third-party external key manager

**Notes:**

- Starting with SANtricity 11.60, NetApp only supports TLS 1.2.
- NetApp recommends enabling strict certificate verification to check the expiration dates of the entire certificate chain. By default, it is disabled and only the server certificate date is checked for expiration. Figure 9 illustrates the REST API for enabling this feature.

# 7 Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) enables SANtricity applications that use TLS communications, such as LDAP over TLS, to receive digital certificate status when OCSP is enabled. The application receives a signed response signifying that the certificate requested is good, revoked, or unknown.

OCSP enables determination of the current status of a digital certificate without requiring certificate revocation lists (CRLs).

By default, OCSP certificate status checking is disabled. It can be turned on with the REST API. Figure 9 illustrates the REST API on how to configure OCSP.

**Figure 9) REST API on how to configure OCSP.**

```
Administration > POST/sslconfig/settings

{

"revocationChecking": true,

"ocspResponderAddress":"", //Can be empty if not wanting to set

"strictCertVerificationEnabled":true

}
```

**Note:** If your environment has an OCSP server, NetApp recommends configuring OCSP.

# 8 NetApp AutoSupport

The AutoSupport feature of SANtricity allows you to proactively monitor the health of your system and automatically send messages and details to NetApp technical support, your organization's internal support team, or a support partner. By default, AutoSupport messages to NetApp technical support are enabled when the storage system is configured for the first time. In addition, AutoSupport begins sending messages to NetApp technical support 24 hours after it is enabled. This 24-hour period is configurable. To leverage the communication to an organization's internal support team, the mail host configuration must be completed.

Only the storage administrator can perform AutoSupport management (configuration). The AutoSupport feature can be disabled. However, NetApp recommends enabling it because AutoSupport helps speed problem identification and resolution should an issue arise on the storage system. By default, the system collects AutoSupport information and stores it locally even if you disable AutoSupport.

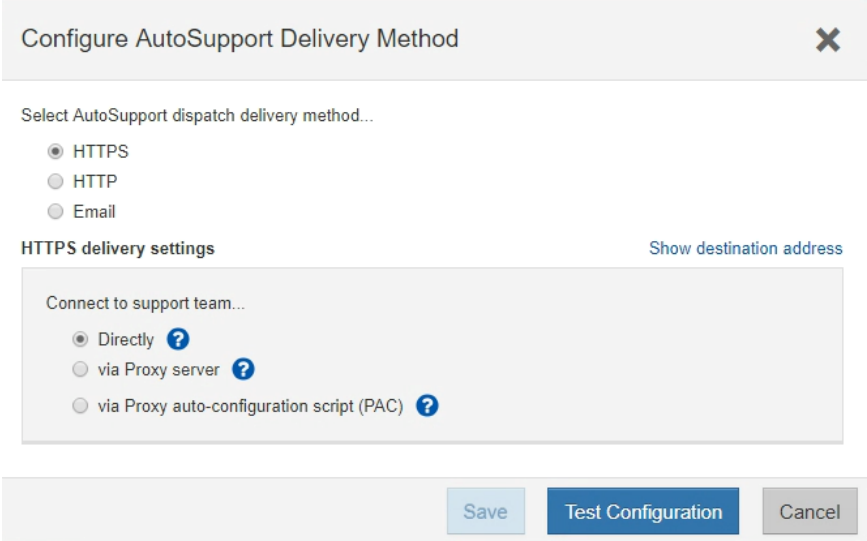
For more details regarding AutoSupport messages, including what is contained in the various messages and where different types of messages are sent, see the NetApp Support portal. AutoSupport messages contain sensitive data including, but not limited to, the following items:

- Log files
- Context-sensitive data regarding specific subsystems
- Configuration and status data
- Performance data

**Note:** AutoSupport supports HTTPS, HTTP, and SMTP for transport protocols. For best security, NetApp strongly recommends using HTTPS as the default transport protocol for sending AutoSupport messages to NetApp support. Figure 10 illustrates the System Manager (Support > AutoSupport > Configure AutoSupport Delivery Method) window on how to configure AutoSupport using HTTPS.

**Figure 10) System Manager window on how to configure AutoSupport using HTTPS.**

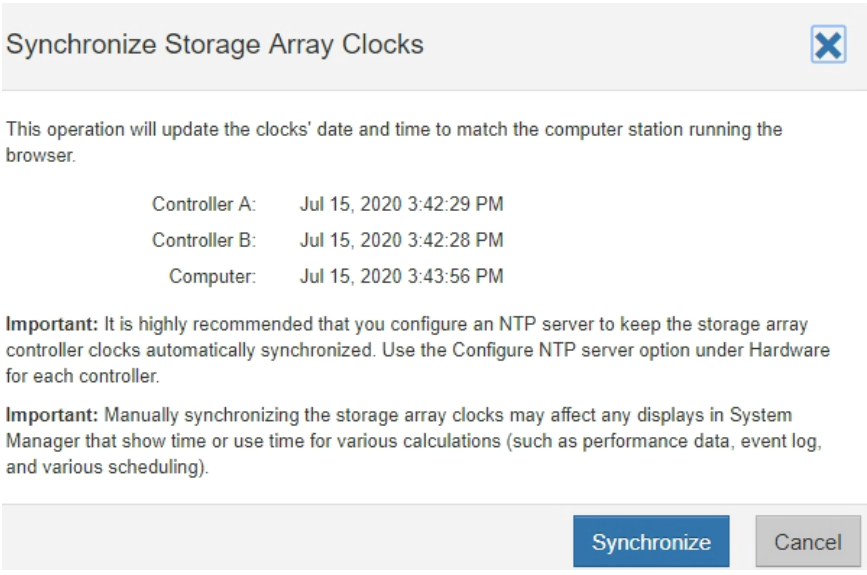



# 9 Network Time Protocol

SANtricity System Manager (Settings > System > Synchronize Storage Array Clocks) enables you to manually set the time zone, date, and time on the storage systems by synchronizing the clock to match the computer station running the browser (see Figure 11). It also supports NTP, but it does not support secure NTP. Without having the capability for the packets to be cryptographically signed for authentication, the NTP server can be susceptible to man-in-the-middle attacks.

**Note:** NetApp recommends manually setting the time zone, date, and time on the storage systems.

**Figure 11) System Manager window on how to manually synchronize the storage system clock.**



# 10 Securing Protocols and Ports

In addition to performing on-box security operations and functions, the hardening of a solution must also include off-box security mechanisms. Leveraging additional infrastructure devices, such as firewalls, intrusion prevention systems (IPSs), and other security devices, for filtering and limiting access to SANtricity is an effective way to establish and maintain a stringent security posture. Table 3 lists the common protocols and ports used in the SANtricity solution. This information is a key component for filtering and limiting access to the environment and its resources.

**Table 3) Commonly used protocols and ports.**

| Service | Port/Protocol | Description |
|---|---|---|
| SSH | 22/TCP | Secure Shell login |
| SMTP | 25/TCP | Simple Mail Transfer Protocol |
| HTTP | 80/TCP | Administrative REST interface (redirects to 8443) |
| NTP | 123/UDP | Network Time Protocol |
| SNMP | 161/TCP/UDP | Simple Network Management Protocol |
| SNMP | 162/UDP | Simple Network Management Protocol |
| LDAP | 389/(UCP/TCP) | Local directory |
| HTTPS | 443/TCP | Secure HTTP for administrative REST interface |
| Syslog | 515/UDP | Syslog server |
| LDAPS | 636/TCP | Secure LDAP |
| SYMbol | 2463/TCP | Legacy Management Interface |
| iSCSI | 3260/TCP | iSCSI target port |
| External Key Mgmt. | 5696/TCP | External Key Management |
| HTTP | 8080/TCP | Administrative REST interface (redirects to 8443) |
| HTTPS | 8443/TCP | Administrative REST interface |

# 11 Conclusion

Cyber security threats have become more prevalent in the recent years because attackers are in search of vulnerable systems. Following and implementing the recommendations specified in this guide will help reduce the security risk on the NetApp E-Series storage systems by eliminating potential attack vectors and securing the attack surfaces.

# Security Resources

For information regarding the reporting of vulnerabilities and incidents, NetApp security responses, and customer confidentiality, see the NetApp security portal.

## Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp SANtricity Storage Manager Online Help v11.60
- Federal Information Processing Standards Publication
  http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- NetApp SANtricity 11.50 Guidance Document 1.2 Common Criteria Guidance Document
  https://www.niap-ccevs.org/MMO/ProductCC/NetApp%20SANtricity%2011.50%20Guidance%20Document_1.2.pdf
- TR-4474: SANtricity Drive Security Using SANtricity OS 11.60
  https://www.netapp.com/us/media/tr-4474.pdf
- TR-4712: SANtricity Management Security Feature Details and Configuration Guide
  https://www.netapp.com/us/media/tr-4712.pdf
- NetApp Product Documentation
  https://docs.netapp.com

## Version History

| Version | Date | Document Version History |
|---|---|---|
| Version 1.0 | August 2020 | Initial release. |

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.



TR-4855-0820