Manage certificates

StorageGRID

NetApp
March 03, 2022

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-116/admin/using-storagegrid-security-certificates.html on March 03, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Manage certificates

About security certificates

Security certificates are small data files used to create secure, trusted connections between StorageGRID components and between StorageGRID components and external systems.

StorageGRID uses two types of security certificates:

- **Server certificates** are required when you use HTTPS connections. Server certificates are used to establish secure connections between clients and servers, authenticating the identity of a server to its clients and providing a secure communication path for data. The server and the client each have a copy of the certificate.
- **Client certificates** authenticate a client or user identity to the server, providing more secure authentication than passwords alone. Client certificates do not encrypt data.

When a client connects to the server using HTTPS, the server responds with the server certificate, which contains a public key. The client verifies this certificate by comparing the server signature to the signature on its copy of the certificate. If the signatures match, the client starts a session with the server using the same public key.

StorageGRID functions as the server for some connections (such as the load balancer endpoint) or as the client for other connections (such as the CloudMirror replication service).

Default Grid CA certificate

StorageGRID includes a built-in certificate authority (CA) that generates an internal Grid CA certificate during system installation. The Grid CA certificate is used, by default, to secure internal StorageGRID traffic. An external certificate authority (CA) can issue custom certificates that are fully compliant with your organization's information security policies. Although you can use the Grid CA certificate for a non-production environment, the best practice for a production environment is to use custom certificates signed by an external certificate authority. Unsecured connections with no certificate are also supported but are not recommended.

- Custom CA certificates do not remove the internal certificates; however, the custom certificates should be the ones specified for verifying server connections.
- All custom certificates must meet the system hardening guidelines for server certificates.
- StorageGRID supports bundling of certificates from a CA into a single file (known as a CA certificate bundle).

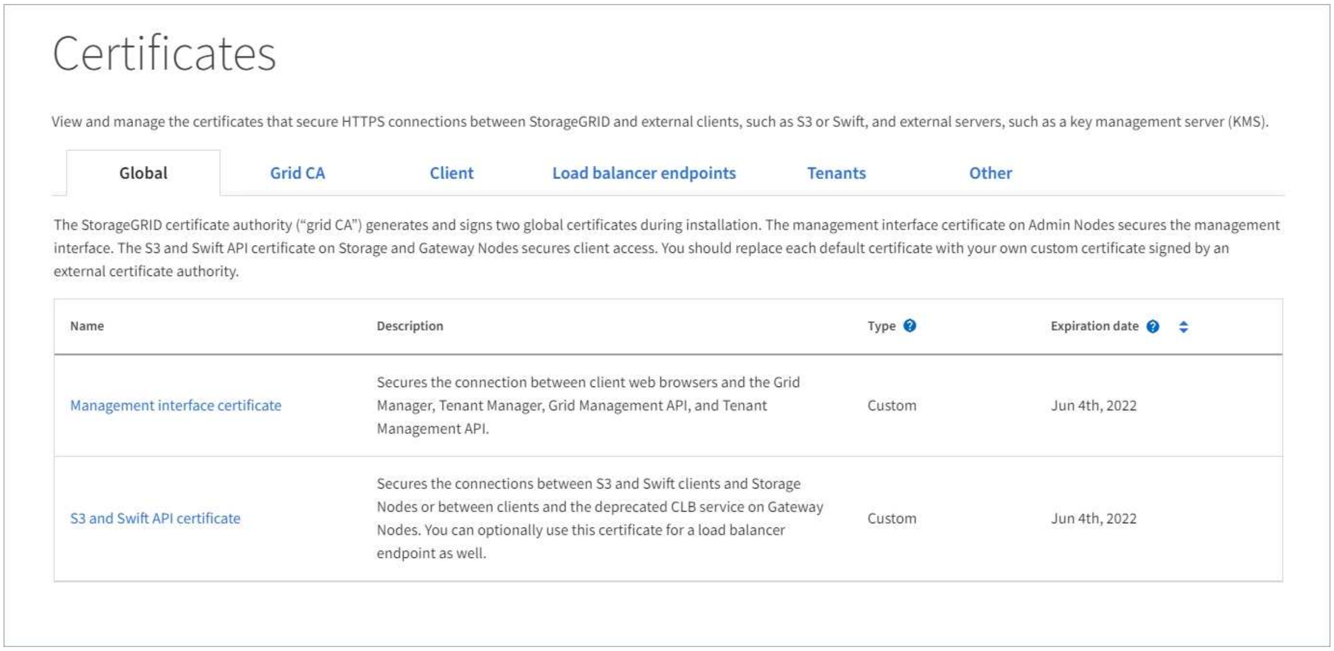
> ⓘ StorageGRID also includes operating system CA certificates that are the same on all grids. In production environments, make sure that you specify a custom certificate signed by an external certificate authority in place of the operating system CA certificate.

Variants of the server and client certificate types are implemented in several ways. You should have all the certificates needed for your specific StorageGRID configuration ready before you configure the system.

Access security certificates

You can access information about all StorageGRID certificates in a single location, along with links to the configuration workflow for each certificate.

1. From Grid Manager, select **CONFIGURATON** > **Security** > **Certificates**.



Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

The StorageGRID certificate authority (“grid CA”) generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type	Expiration date
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Select a tab on the Certificates page for information about each certificate category and to access the certificate settings. You can only access a tab if you have the appropriate permission.

   - **Global**: Secures StorageGRID access from web browsers and external API clients.
   - **Grid CA**: Secures internal StorageGRID traffic.
   - **Client**: Secures connections between external clients and the StorageGRID Prometheus database.
   - **Load balancer endpoints**: Secures connections between S3 and Swift clients and the StorageGRID Load Balancer.
   - **Tenants**: Secures connections to identity federation servers or from platform service endpoints to S3 storage resources.
   - **Other**: Secures StorageGRID connections requiring specific certificates.

   Each tab is described below with links to additional certificate details.

Global

The global certificates secure StorageGRID access from web browsers and external S3 and Swift API clients. Two global certificates are initially generated by the StorageGRID certificate authority during installation. The best practice for a production environment is to use custom certificates signed by an external certificate authority.

- Management interface certificate: Secures client web-browser connections to StorageGRID management interfaces.
- S3 and Swift API certificate: Secures client API connections to Storage Nodes, Admin Nodes, and Gateway Nodes, which S3 and Swift client applications use to upload and download object data.

Information about the global certificates that are installed includes:

- **Name**: Certificate name with link to managing the certificate.
- **Description**
- **Type**: Custom or default.
  You should always use a custom certificate for improved grid security.
- **Expiration date**: If using the default certificate, no expiration date is shown.

You can:

- Replace the default certificates with custom certificates signed by an external certificate authority for improved grid security:
  - Replace the default StorageGRID-generated management interface certificate used for Grid Manager and Tenant Manager connections.
  - Replace the S3 and Swift API certificate used for Storage Node, CLB service (deprecated), and load balancer endpoint (optional) connections.
- Restore the default management interface certificate.
- Restore the default S3 and Swift API certificate.
- Use a script to generate a new self-signed management interface certificate.
- Copy or download the management interface certificate or S3 and Swift API certificate.

Grid CA

The Grid CA certificate, generated by the StorageGRID certificate authority during StorageGRID installation, secures all internal StorageGRID traffic.

Certificate information includes the certificate expiration date and the certificate contents.

You can Copy or download the Grid CA certificate, but you cannot change it.

Client

Client certificates, generated by an external certificate authority, secure the connections between external monitoring tools and the StorageGRID Prometheus database.

The certificate table has a row for each configured client certificate and indicates whether the certificate can be used for Prometheus database access, along with the certificate expiration date.

You can:

- Upload or generate a new client certificate.
- Select a certificate name to display the certificate details where you can:
  - Change the client certificate name.
  - Set the Prometheus access permission.
  - Upload and replace the client certificate.
  - Copy or download the client certificate.
  - Remove the client certificate.
- Select **Actions** to quickly edit, attach, or remove a client certificate. You can select up to 10 client certificates and remove them at one time using **Actions** > **Remove**.

Load balancer endpoints

Load balancer endpoint certificates, that you upload or generate, secure the connections between S3 and Swift clients and the StorageGRID Load Balancer service on Gateway Nodes and Admin Nodes.

The load balancer endpoint table has a row for each configured load balancer endpoint and indicates whether the global S3 and Swift API certificate or a custom load balancer endpoint certificate is being used for the endpoint. The expiration date for each certificate is also displayed.

ⓘ Changes to an endpoint certificate can take up to 15 minutes to be applied to all nodes.

You can:

- Select an endpoint name to open a browser tab with information about the load balancer endpoint, including its certificate details.
- Specify a load balancer endpoint certificate for FabricPool.
- Use the global S3 and Swift API certificate instead of generating a new load balancer endpoint certificate.

Tenants

Tenants can use identity federation server certificates or platform service endpoint certificates to secure their connections with StorageGRID.

The tenant table has a row for each tenant and indicates if each tenant has permission to use its own identity source or platform services.

You can:

- Select a tenant name to sign in to the Tenant Manager
- Select a tenant name to view the tenant identity federation details
- Select a tenant name to view tenant platform services details
- Specify a platform service endpoint certificate during endpoint creation

Other

StorageGRID uses other security certificates for specific purposes. These certificates are listed by their functional name. Other security certificates include:

- Identity federation certificates

- Cloud Storage Pool certificates
- Key management server (KMS) certificates
- Single sign-on certificates
- Email alert notification certificates
- External syslog server certificates

Information indicates the type of certificate a function uses and its server and client certificate expiration dates, as applicable. Selecting a function name opens a browser tab where you can view and edit the certificate details.

ⓘ You can only view and access information for other certificates if you have the appropriate permission.

You can:

- View and edit an identity federation certificate
- Upload key management server (KMS) server and client certificates
- Specify a Cloud Storage Pool certificate for S3, C2S S3, or Azure
- Manually specify an SSO certificate for relying party trust
- Specify a certificate for alert email notifications
- Specify an external syslog server certificate

Security certificate details

Each type of security certificate is described below, with links to articles that contain implementation instructions.

Management interface certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection between client web browsers and the StorageGRID management interface, allowing users to access the Grid Manager and Tenant Manager without security warnings. This certificate also authenticates Grid Management API and Tenant Management API connections. You can use the default certificate created during installation or upload a custom certificate.	**CONFIGURATION** > **Security** > **Certificates**, select the **Global** tab, and then select **Management interface certificate**	Configure management interface certificates

S3 and Swift API certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates secure S3 or Swift client connections to a Storage Node, to the deprecated Connection Load Balancer (CLB) service on a Gateway Node, and load balancer endpoints (optional).	**CONFIGURATION** > **Security** > **Certificates**, select the **Global** tab, and then select **S3 and Swift API certificate**	Configure S3 and Swift API certificates

Grid CA certificate

See the Default Grid CA certificate description.

Administrator client certificate

Certificate type	Description	Navigation location	Details
Client	Installed on each client, allowing StorageGRID to authenticate external client access. • Allows authorized external clients to access the StorageGRID Prometheus database. • Allows secure monitoring of StorageGRID using external tools.	**CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab	Configure client certificates

Load balancer endpoint certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection between S3 or Swift clients and the StorageGRID Load Balancer service on Gateway Nodes and Admin Nodes. You can upload or generate a load balancer certificate when you configure a load balancer endpoint. Client applications use the load balancer certificate when connecting to StorageGRID to save and retrieve object data. You can also use a custom version of the global S3 and Swift API certificate certificate to authenticate connections to the Load Balancer service. If the global certificate is used to authenticate load balancer connections, you do not need to upload or generate a separate certificate for each load balancer endpoint. **Note:** The certificate used for load balancer authentication is the most used certificate during normal StorageGRID operation.	**CONFIGURATION** > **Network** > **Load balancer endpoints**	• Configure load balancer endpoints • Create a load balancer endpoint for FabricPool

Identity federation certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection between StorageGRID and an external identity provider, such as Active Directory, OpenLDAP, or Oracle Directory Server. Used for identity federation, which allows admin groups and users to be managed by an external system.	**CONFIGURATION** > **Access Control** > **Identity federation**	Use identity federation

Platform services endpoint certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection from the StorageGRID platform service to an S3 storage resource.	**Tenant Manager** > **STORAGE (S3)** > **Platform services endpoints**	Create platform services endpoint Edit platform services endpoint

Cloud Storage Pool endpoint certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection from a StorageGRID Cloud Storage Pool to an external storage location, such as S3 Glacier or Microsoft Azure Blob storage. A different certificate is required for each cloud provider type.	**ILM** > **Storage pools**	Create a Cloud Storage Pool

Key management server (KMS) certificate

Certificate type	Description	Navigation location	Details
Server and client	Authenticates the connection between StorageGRID and an external key management server (KMS), which provides encryption keys to StorageGRID appliance nodes.	**CONFIGURATION** > **Security** > **Key management server**	Add key management server (KMS)

Single sign-on (SSO) certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the connection between identity federation services, such as Active Directory Federation Services (AD FS), and StorageGRID that are used for single sign-on (SSO) requests.	**CONFIGURATION** > **Access control** > **Single sign-on**	Configure single sign-on

Email alert notification certificate

Certificate type	Description	Navigation location	Details
Server and client	Authenticates the connection between an SMTP email server and StorageGRID that is used for alert notifications. • If communications with the SMTP server requires Transport Layer Security (TLS), you must specify the email server CA certificate. • Specify a client certificate only if the SMTP email server requires client certificates for authentication.	**ALERTS** > **Email setup**	Set up email notifications for alerts

External syslog server certificate

Certificate type	Description	Navigation location	Details
Server	Authenticates the TLS or RELP/TLS connection between an external syslog server that logs events in StorageGRID. **Note:** An external syslog server certificate is not required for TCP, RELP/TCP, and UDP connections to an external syslog server.	**CONFIGURATION** > **Monitoring** > **Audit and syslog server** and then select **Configure external syslog server**	Configure an external syslog server

Certificate examples

Example 1: Load Balancer service

In this example, StorageGRID acts as the server.

1. You configure a load balancer endpoint and upload or generate a server certificate in StorageGRID.
2. You configure an S3 or Swift client connection to the load balancer endpoint and upload the same certificate to the client.
3. When the client wants to save or retrieve data, it connects to the load balancer endpoint using HTTPS.
4. StorageGRID responds with the server certificate, which contains a public key, and with a signature based on the private key.
5. The client verifies this certificate by comparing the server signature to the signature on its copy of the certificate. If the signatures match, the client starts a session using the same public key.
6. The client sends object data to StorageGRID.

Example 2: External key management server (KMS)

In this example, StorageGRID acts as the client.

1. Using external Key Management Server software, you configure StorageGRID as a KMS client and obtain a CA-signed server certificate, a public client certificate, and the private key for the client certificate.
2. Using the Grid Manager, you configure a KMS server and upload the server and client certificates and the client private key.
3. When a StorageGRID node needs an encryption key, it makes a request to the KMS server that includes data from the certificate and a signature based on the private key.
4. The KMS server validates the certificate signature and decides that it can trust StorageGRID.
5. The KMS server responds using the validated connection.

Configure server certificates

Supported server certificate types

The StorageGRID system supports custom certificates encrypted with RSA or ECDSA (Elliptic Curve Digital Signature Algorithm).

For more information on how StorageGRID secures client connections for the REST API, see Use S3 or Use Swift.

Configure management interface certificates

You can replace the default management interface certificate with a single custom certificate that allows users to access the Grid Manager and the Tenant Manager without encountering security warnings. You can also revert to the default management interface certificate or generate a new one.

About this task

By default, every Admin Node is issued a certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom management interface certificate and corresponding private key.

Because a single custom management interface certificate is used for all Admin Nodes, you must specify the certificate as a wildcard or multi-domain certificate if clients need to verify the hostname when connecting to the Grid Manager and Tenant Manager. Define the custom certificate such that it matches all Admin Nodes in the grid.

You need to complete configuration on the server, and depending on the root certificate authority (CA) you are using, users might also need to install the Grid CA certificate in the web browser they will use to access the Grid Manager and the Tenant Manager.

> ⓘ To ensure that operations are not disrupted by a failed server certificate, the **Expiration of server certificate for Management Interface** alert is triggered when this server certificate is about to expire. As required, you can view when the current certificate expires by selecting **CONFIGURATION** > **Security** > **Certificates** and looking at the Expiration date for the management interface certificate on the Global tab.

> ⓘ If you are accessing the Grid Manager or Tenant Manager using a domain name instead of an IP address, the browser shows a certificate error without an option to bypass if either of the following occurs:
>
> - Your custom management interface certificate expires.
> - You revert from a custom management interface certificate to the default server certificate.

Add a custom management interface certificate

To add a custom management interface certificate, you can provide your own certificate or generate one using the Grid Manager.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates**.

2. On the **Global** tab, select **Management interface certificate**.
3. Select **Use custom certificate**.
4. Upload or generate the certificate.

Upload certificate

Upload the required server certificate files.

1. Select **Upload certificate**.
2. Upload the required server certificate files:
   - **Server certificate**: The custom server certificate file (PEM encoded).
   - **Certificate private key**: The custom server certificate private key file (`.key`).

     > EC private keys must be 224 bits or larger. RSA private keys must be 2048 bits or larger.

   - **CA bundle**: A single optional file containing the certificates from each intermediate issuing certificate authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.
3. Expand **Certificate details** to see the metadata for each certificate you uploaded. If you uploaded an optional CA bundle, each certificate displays on its own tab.
   - Select **Download certificate** to save the certificate file or select **Download CA bundle** to save the certificate bundle.

     Specify the certificate file name and download location. Save the file with the extension `.pem`.

     For example: `storagegrid_certificate.pem`
   - Select **Copy certificate PEM** or **Copy CA bundle PEM** to copy the certificate contents for pasting elsewhere.
4. Select **Save**.
   The custom management interface certificate is used for all subsequent new connections to the Grid Manager, Tenant Manager, Grid Manager API or Tenant Manager API.

Generate certificate

Generate the server certificate files.

> The best practice for a production environment is to use a custom management interface certificate signed by an external certificate authority.

1. Select **Generate certificate**.
2. Specify the certificate information:
   - **Domain name**: One or more fully qualified domain names to include in the certificate. Use an * as a wildcard to represent multiple domain names.
   - **IP**: One or more IP addresses to include in the certificate.
   - **Subject**: X.509 subject or distinguished name (DN) of the certificate owner.
   - **Days valid**: Number of days after creation that the certificate expires.
3. Select **Generate**.
4. Select **Certificate details** to see the metadata for the generated certificate.
   - Select **Download certificate** to save the certificate file.

Specify the certificate file name and download location. Save the file with the extension `.pem`.

For example: `storagegrid_certificate.pem`

- Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.

5. Select **Save**.
The custom management interface certificate is used for all subsequent new connections to the Grid Manager, Tenant Manager, Grid Manager API or Tenant Manager API.

5. Refresh the page to ensure the web browser is updated.

> ⓘ After uploading or generating a new certificate, allow up to one day for any related certificate expiration alerts to clear.

6. After you add a custom management interface certificate, the Management interface certificate page displays detailed certificate information for the certificates that are in use.
You can download or copy the certificate PEM as required.

Restore the default management interface certificate

You can revert to using the default management interface certificate for Grid Manager and Tenant Manager connections.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates**.
2. On the **Global** tab, select **Management interface certificate**.
3. Select **Use default certificate**.

   When you restore the default management interface certificate, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default management interface certificate is used for all subsequent new client connections.

4. Refresh the page to ensure the web browser is updated.

Use a script to generate a new self-signed management interface certificate

If strict hostname validation is required, you can use a script to generate the management interface certificate.

What you'll need

- You have specific access permissions.
- You have the `Passwords.txt` file.

About this task

The best practice for a production environment is to use a certificate signed by an external certificate authority.

Steps

1. Obtain the fully qualified domain name (FQDN) of each Admin Node.
2. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

3. Configure StorageGRID with a new self-signed certificate.

   `$ sudo make-certificate --domains` *`wildcard-admin-node-fqdn`* `--type management`

   - For `--domains`, use wildcards to represent the fully qualified domain names of all Admin Nodes. For example, `*.ui.storagegrid.example.com` uses the * wildcard to represent `admin1.ui.storagegrid.example.com` and `admin2.ui.storagegrid.example.com`.
   - Set `--type` to `management` to configure the management interface certificate, which is used by Grid Manager and Tenant Manager.
   - By default, generated certificates are valid for one year (365 days) and must be recreated before they expire. You can use the `--days` argument to override the default validity period.

     > A certificate's validity period begins when `make-certificate` is run. You must ensure the management client is synchronized to the same time source as StorageGRID; otherwise, the client might reject the certificate.

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
     management --days 720
     ```

     The resulting output contains the public certificate needed by your management API client.

4. Select and copy the certificate.

   Include the BEGIN and the END tags in your selection.

5. Log out of the command shell. `$ exit`

6. Confirm the certificate was configured:

   a. Access the Grid Manager.

   b. Select **CONFIGURATION** > **Security** > **Certificates**

   c. On the **Global** tab, select **Management interface certificate**.

7. Configure your management client to use the public certificate you copied. Include the BEGIN and END tags.

Download or copy the management interface certificate

You can save or copy the management interface certificate contents for use elsewhere.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates**.
2. On the **Global** tab, select **Management interface certificate**.

3. Select the **Server** or **CA bundle** tab and then download or copy the certificate.

Download certificate file or CA bundle

Download the certificate or CA bundle `.pem` file. If you are using an optional CA bundle, each certificate in the bundle displays on its own sub-tab.

1. Select **Download certificate** or **Download CA bundle**.

   If you are downloading a CA bundle, all the certificates in the CA bundle secondary tabs download as a single file.

2. Specify the certificate file name and download location. Save the file with the extension `.pem`.

   For example: `storagegrid_certificate.pem`

Copy certificate or CA bundle PEM

Copy the certificate text to paste elsewhere. If you are using an optional CA bundle, each certificate in the bundle displays on its own sub-tab.

1. Select **Copy certificate PEM** or **Copy CA bundle PEM**.

   If you are copying a CA bundle, all the certificates in the CA bundle secondary tabs copy together.

2. Paste the copied certificate into a text editor.
3. Save the text file with the extension `.pem`.

   For example: `storagegrid_certificate.pem`

Configure S3 and Swift API certificates

You can replace or restore the server certificate that is used for S3 or Swift client connections to Storage Nodes, the deprecated Connection Load Balancer (CLB) service on Gateway Nodes, or to load balancer endpoints. The replacement custom server certificate is specific to your organization.

About this task

By default, every Storage Node is issued a X.509 server certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

A single custom server certificate is used for all Storage Nodes, so you must specify the certificate as a wildcard or multi-domain certificate if clients need to verify the hostname when connecting to the storage endpoint. Define the custom certificate such that it matches all Storage Nodes in the grid.

After completing configuration on the server, you might also need to install the Grid CA certificate in the S3 or Swift API client you will use to access the system, depending on the root certificate authority (CA) you are using.

ⓘ To ensure that operations are not disrupted by a failed server certificate, the **Expiration of global server certificate for S3 and Swift API** alert is triggered when the root server certificate is about to expire. As required, you can view when the current certificate expires by selecting **CONFIGURATION** > **Security** > **Certificates** and looking at the Expiration date for the S3 and Swift API certificate on the Global tab.

You can upload or generate a custom S3 and Swift API certificate.

Add a custom S3 and Swift API certificate

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates**.
2. On the **Global** tab, select **S3 and Swift API certificate**.
3. Select **Use custom certificate**.
4. Upload or generate the certificate.

Upload certificate

Upload the required server certificate files.

1. Select **Upload certificate**.
2. Upload the required server certificate files:
   - **Server certificate**: The custom server certificate file (PEM encoded).
   - **Certificate private key**: The custom server certificate private key file (`.key`).

     > EC private keys must be 224 bits or larger. RSA private keys must be 2048 bits or larger.

   - **CA bundle**: A single optional file containing the certificates from each intermediate issuing certificate authority. The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.
3. Select the certificate details to display the metadata and PEM for each custom S3 and Swift API certificate that was uploaded. If you uploaded an optional CA bundle, each certificate displays on its own tab.
   - Select **Download certificate** to save the certificate file or select **Download CA bundle** to save the certificate bundle.

     Specify the certificate file name and download location. Save the file with the extension `.pem`.

     For example: `storagegrid_certificate.pem`
   - Select **Copy certificate PEM** or **Copy CA bundle PEM** to copy the certificate contents for pasting elsewhere.
4. Select **Save**.

   The custom server certificate is used for subsequent new S3 and Swift client connections.

Generate certificate

Generate the server certificate files.

1. Select **Generate certificate**.
2. Specify the certificate information:
   - **Domain name**: One or more fully qualified domain names to include in the certificate. Use an * as a wildcard to represent multiple domain names.
   - **IP**: One or more IP addresses to include in the certificate.
   - **Subject**: X.509 subject or distinguished name (DN) of the certificate owner.
   - **Days valid**: Number of days after creation that the certificate expires.
3. Select **Generate**.
4. Select **Certificate Details** to display the metadata and PEM for the custom S3 and Swift API certificate that was generated.
   - Select **Download certificate** to save the certificate file.

Specify the certificate file name and download location. Save the file with the extension `.pem`.

For example: `storagegrid_certificate.pem`

- Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.

5. Select **Save**.

   The custom server certificate is used for subsequent new S3 and Swift client connections.

5. Select a tab to display metadata for the default StorageGRID server certificate, a CA signed certificate that was uploaded, or a custom certificate that was generated.

   ⓘ After uploading or generating a new certificate, allow up to one day for any related certificate expiration alerts to clear.

6. Refresh the page to ensure the web browser is updated.
7. After you add a custom S3 and Swift API certificate the S3 and Swift API certificate page displays detailed certificate information for the custom S3 and Swift API certificate that is in use.
   You can download or copy the certificate PEM as required.

Restore the default S3 and Swift API certificate

You can revert to using the default S3 and Swift API certificate for S3 and Swift client connections to Storage Nodes and to the deprecated CLB service on Gateway Nodes. However, you cannot use the default S3 and Swift API certificate for a load balancer endpoint.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates**.
2. On the **Global** tab, select **S3 and Swift API certificate**.
3. Select **Use default certificate**.

   When you restore the default version of the global S3 and Swift API certificate, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default S3 and Swift API certificate will be used for subsequent new S3 and Swift client connections to Storage Nodes and to the deprecated CLB service on Gateway Nodes.

4. Select **OK** to confirm the warning and restore the default S3 and Swift API certificate.

   If you have Root access permission and the custom S3 and Swift API certificate was used for load balancer endpoint connections, a list is displayed of load balancer endpoints that will no longer be accessible using the default S3 and Swift API certificate. Go to Configure load balancer endpoints to edit or remove the affected endpoints.

5. Refresh the page to ensure the web browser is updated.

Download or copy the S3 and Swift API certificate

You can save or copy the S3 and Swift API certificate contents for use elsewhere.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates**.
2. On the **Global** tab, select **S3 and Swift API certificate**.
3. Select the **Server** or **CA bundle** tab and then download or copy the certificate.

Download certificate file or CA bundle

Download the certificate or CA bundle `.pem` file. If you are using an optional CA bundle, each certificate in the bundle displays on its own sub-tab.

a. Select **Download certificate** or **Download CA bundle**.

   If you are downloading a CA bundle, all the certificates in the CA bundle secondary tabs download as a single file.

b. Specify the certificate file name and download location. Save the file with the extension `.pem`.

   For example: `storagegrid_certificate.pem`

Copy certificate or CA bundle PEM

Copy the certificate text to paste elsewhere. If you are using an optional CA bundle, each certificate in the bundle displays on its own sub-tab.

a. Select **Copy certificate PEM** or **Copy CA bundle PEM**.

   If you are copying a CA bundle, all the certificates in the CA bundle secondary tabs copy together.

b. Paste the copied certificate into a text editor.

c. Save the text file with the extension `.pem`.

   For example: `storagegrid_certificate.pem`

Related information

- Use S3
- Use Swift
- Configure S3 API endpoint domain names

Copy the Grid CA certificate

StorageGRID uses an internal certificate authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have specific access permissions.

About this task

If a custom server certificate has been configured, client applications should verify the server using the custom server certificate. They should not copy the CA certificate from the StorageGRID system.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates** and then select the **Grid CA** tab.
2. In the **Certificate PEM** section download or copy the certificate.

Download certificate file

Download the certificate `.pem` file.

1. Select **Download certificate**.
2. Specify the certificate file name and download location. Save the file with the extension `.pem`.

   For example: `storagegrid_certificate.pem`

Copy certificate PEM

Copy the certificate text to paste elsewhere.

1. Select **Copy certificate PEM**.
2. Paste the copied certificate into a text editor.
3. Save the text file with the extension `.pem`.

   For example: `storagegrid_certificate.pem`

Configure StorageGRID certificates for FabricPool

For S3 clients that perform strict hostname validation and do not support disabling strict hostname validation, such as ONTAP clients using FabricPool, you can generate or upload a server certificate when you configure the load balancer endpoint.

What you'll need

- You have specific access permissions.
- You are signed in to the Grid Manager using a supported web browser.

About this task

When you create a load balancer endpoint, you can generate a self-signed server certificate or upload a certificate that is signed by a known certificate authority (CA). In production environments, you should use a certificate that is signed by a known CA. Certificates signed by a CA can be rotated non-disruptively. They are also more secure because they provide better protection against man-in-the-middle attacks.

The following steps provide general guidelines for S3 clients that use FabricPool. For more detailed information and procedures, see Configure StorageGRID for FabricPool.

ⓘ The separate Connection Load Balancer (CLB) service on Gateway Nodes is deprecated and not recommended for use with FabricPool.

Steps

1. Optionally, configure a high availability (HA) group for FabricPool to use.

2. Create an S3 load balancer endpoint for FabricPool to use.

   When you create an HTTPS load balancer endpoint, you are prompted to upload your server certificate, certificate private key, and optional CA bundle.

3. Attach StorageGRID as a cloud tier in ONTAP.

   Specify the load balancer endpoint port and the fully qualified domain name used in the CA certificate you uploaded. Then, provide the CA certificate.

   > If an intermediate CA issued the StorageGRID certificate, you must provide the intermediate CA certificate. If the StorageGRID certificate was issued directly by the Root CA, you must provide the Root CA certificate.

Configure client certificates

Client certificates allow authorized external clients to access the StorageGRID Prometheus database, providing a secure way for external tools to monitor StorageGRID.

If you need to access StorageGRID using an external monitoring tool, you must upload or generate an administrator client certificate using the Grid Manager and copy the certificate information to the external tool.

See the information about general security certificate use and configuring custom server certificates.

> To ensure that operations are not disrupted by a failed server certificate, the **Expiration of client certificates configured on the Certificates page** alert is triggered when this server certificate is about to expire. As required, you can view when the current certificate expires by selecting **CONFIGURATION** > **Security** > **Certificates** and looking at the Expiration date for the client certificate on the Client tab.

> If you are using a key management server (KMS) to protect the data on specially configured appliance nodes, see the specific information about uploading a KMS client certificate.

What you'll need

- You have Root access permission.
- You are signed in to the Grid Manager using a supported web browser.
- To configure a client certificate:
  - You have the IP address or domain name of the Admin Node.
  - You have configured the StorageGRID management interface certificate and have the corresponding optional CA bundle.
  - To upload your own certificate, the public key and private key for the certificate are available on your local computer.
- To edit a client certificate:
  - You have the IP address or domain name of the Admin Node.
  - To upload a new certificate and private key, the public key and private key for the certificate are available on your local computer.

Add client certificates

To add an administrator client certificate, you can provide your own certificate or generate one using the Grid Manager.

Steps

1. In the Grid Manager, select **CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab.
2. Select **Add**.
3. Enter a certificate name between 1 and 32 characters.
4. To access Prometheus metrics using your external monitoring tool, select **Allow Prometheus**.
5. In the **Certificate type** section, upload or generate the certificate.

Upload certificate

Upload the certificate `.pem` file.

1. Select **Upload certificate** and then select **Continue**.
2. Upload the client certificate name (`.pem`).

   Select **Client certificate details** to display the certificate metadata and certificate PEM.

   - Select **Download certificate** to save the certificate file.

     Specify the certificate file name and download location. Save the file with the extension `.pem`.

     For example: `storagegrid_certificate.pem`

   - Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.
3. Select **Create** to save the certificate in the Grid Manager.

   The new certificate appears on the Client tab.

Generate certificate

Generate the certificate text to paste elsewhere.

1. Select **Generate certificate**.
2. Specify the certificate information:
   - **Domain name**: One or more fully qualified domain names to include in the certificate. Use an * as a wildcard to represent multiple domain names.
   - **IP**: One or more IP addresses to include in the certificate.
   - **Subject**: X.509 subject or distinguished name (DN) of the certificate owner.
   - **Days valid**: Number of days after creation that the certificate expires.
3. Select **Generate**.
4. Select **Client certificate details** to display the certificate metadata and certificate PEM.

   > You will not be able to view the certificate private key after you close the dialog. Copy or download the key to a safe location.

   - Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.
   - Select **Download certificate** to save the certificate file.

     Specify the certificate file name and download location. Save the file with the extension `.pem`.

     For example: `storagegrid_certificate.pem`

   - Select **Copy private key** to copy the certificate private key for pasting elsewhere.
   - Select **Download private key** to save the private key as a file.

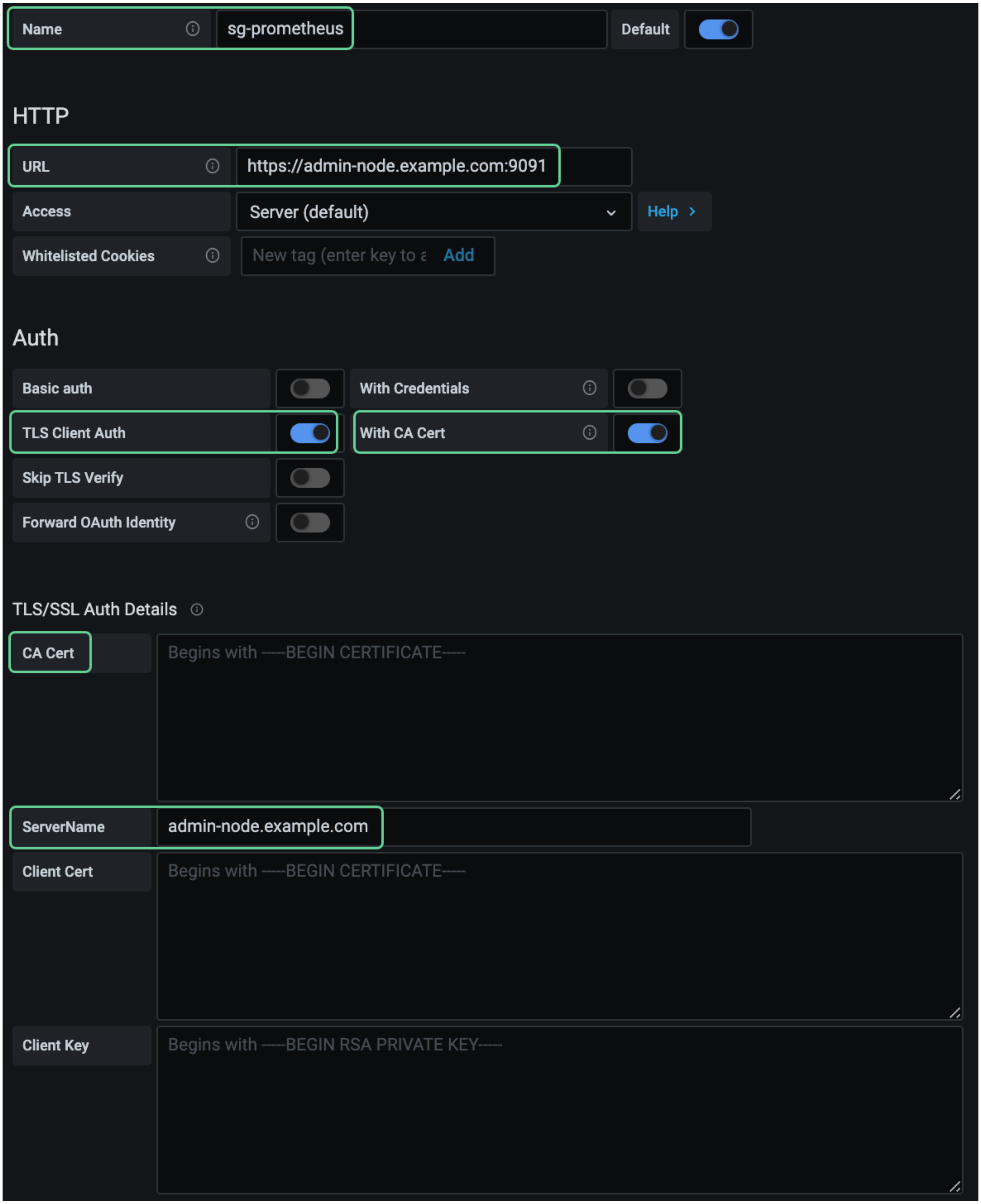
     Specify the private key file name and download location.

5. Select **Create** to save the certificate in the Grid Manager.

   The new certificate appears on the Client tab.

6. Configure the following settings on your external monitoring tool, such as Grafana.

   A Grafana example is shown in the following screenshot:



Name: sg-prometheus
Default: on

HTTP

URL: https://admin-node.example.com:9091
Access: Server (default)
Whitelisted Cookies: New tag (enter key to a Add

Auth

Basic auth: off
With Credentials: off
TLS Client Auth: on
With CA Cert: on
Skip TLS Verify: off
Forward OAuth Identity: off

TLS/SSL Auth Details

CA Cert: Begins with -----BEGIN CERTIFICATE-----
ServerName: admin-node.example.com
Client Cert: Begins with -----BEGIN CERTIFICATE-----
Client Key: Begins with -----BEGIN RSA PRIVATE KEY-----

a. **Name**: Enter a name for the connection.

   StorageGRID does not require this information, but you must provide a name to test the connection.

b. **URL**: Enter the domain name or IP address for the Admin Node. Specify HTTPS and port 9091.

For example: `https://admin-node.example.com:9091`

c. Enable **TLS Client Auth** and **With CA Cert**.

d. Copy and paste the management interface certificate or optional CA bundle to **CA Cert** under TLS/SSL Auth Details.

e. **ServerName**: Enter the domain name of the Admin Node.

ServerName must match the domain name as it appears in the management interface certificate.

f. Save and test the certificate and private key that you copied from StorageGRID or a local file.

You can now access the Prometheus metrics from StorageGRID with your external monitoring tool.

For information about the metrics, see the instructions for monitoring StorageGRID.

Edit client certificates

You can edit an administrator client certificate to change its name, enable or disable Prometheus access, or upload a new certificate when the current one has expired.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab.

   Certificate expiration dates and Prometheus access permissions are listed in the table. If a certificate will expire soon or is already expired, a message appears in the table and an alert is triggered.

2. Select the certificate you want to edit.
3. Select **Edit** and then select **Edit name and permission**
4. Enter a certificate name between 1 and 32 characters.
5. To access Prometheus metrics using your external monitoring tool, select **Allow Prometheus**.
6. Select **Continue** to save the certificate in the Grid Manager.

   The updated certificate displays on the Client tab.

Attach new client certificate

You can upload a new certificate when the current one has expired.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab.

   Certificate expiration dates and Prometheus access permissions are listed in the table. If a certificate will expire soon or is already expired, a message appears in the table and an alert is triggered.

2. Select the certificate you want to edit.
3. Select **Edit** and then select an edit option.

Upload certificate

Copy the certificate text to paste elsewhere.

1. Select **Upload certificate** and then select **Continue**.
2. Upload the client certificate name (`.pem`).

   Select **Client certificate details** to display the certificate metadata and certificate PEM.

   - Select **Download certificate** to save the certificate file.

     Specify the certificate file name and download location. Save the file with the extension `.pem`.

     For example: `storagegrid_certificate.pem`

   - Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.
3. Select **Create** to save the certificate in the Grid Manager.

   The updated certificate displays on the Client tab.

Generate certificate

Generate the certificate text to paste elsewhere.

1. Select **Generate certificate**.
2. Specify the certificate information:
   - **Domain name**: One or more fully qualified domain names to include in the certificate. Use an * as a wildcard to represent multiple domain names.
   - **IP**: One or more IP addresses to include in the certificate.
   - **Subject**: X.509 subject or distinguished name (DN) of the certificate owner.
   - **Days valid**: Number of days after creation that the certificate expires.
3. Select **Generate**.
4. Select **Client certificate details** to display the certificate metadata and certificate PEM.

   > ⓘ You will not be able to view the certificate private key after you close the dialog. Copy or download the key to a safe location.

   - Select **Copy certificate PEM** to copy the certificate contents for pasting elsewhere.
   - Select **Download certificate** to save the certificate file.

     Specify the certificate file name and download location. Save the file with the extension `.pem`.

     For example: `storagegrid_certificate.pem`

   - Select **Copy private key** to copy the certificate private key for pasting elsewhere.
   - Select **Download private key** to save the private key as a file.

     Specify the private key file name and download location.

5. Select **Create** to save the certificate in the Grid Manager.

   The new certificate appears on the Client tab.

Download or copy client certificates

You can download or copy a client certificate for use elsewhere.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab.
2. Select the certificate you want to copy or download.
3. Download or copy the certificate.

   Download certificate file

   Download the certificate `.pem` file.

   1. Select **Download certificate**.
   2. Specify the certificate file name and download location. Save the file with the extension `.pem`.

      For example: `storagegrid_certificate.pem`

   Copy certificate

   Copy the certificate text to paste elsewhere.

   1. Select **Copy certificate PEM**.
   2. Paste the copied certificate into a text editor.
   3. Save the text file with the extension `.pem`.

      For example: `storagegrid_certificate.pem`

Remove client certificates

If you no longer need an administrator client certificate, you can remove it.

Steps

1. Select **CONFIGURATION** > **Security** > **Certificates** and then select the **Client** tab.
2. Select the certificate you want to remove.
3. Select **Delete** and then confirm.

> ⓘ To remove up to 10 certificates, select each certificate to remove on the Client tab and then select **Actions** > **Delete**.

After a certificate is removed, clients that used the certificate must specify a new client certificate to access the StorageGRID Prometheus database.

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.