SSL Certificates window

Use the window that is shown in Figure 9-75 to view, import, or delete SSL certificates to support secure connections to a Storage Authentication Service server from a TS7700 cluster. This page also allows the user to replace the MI HTTPS SSL certificate with a custom one.

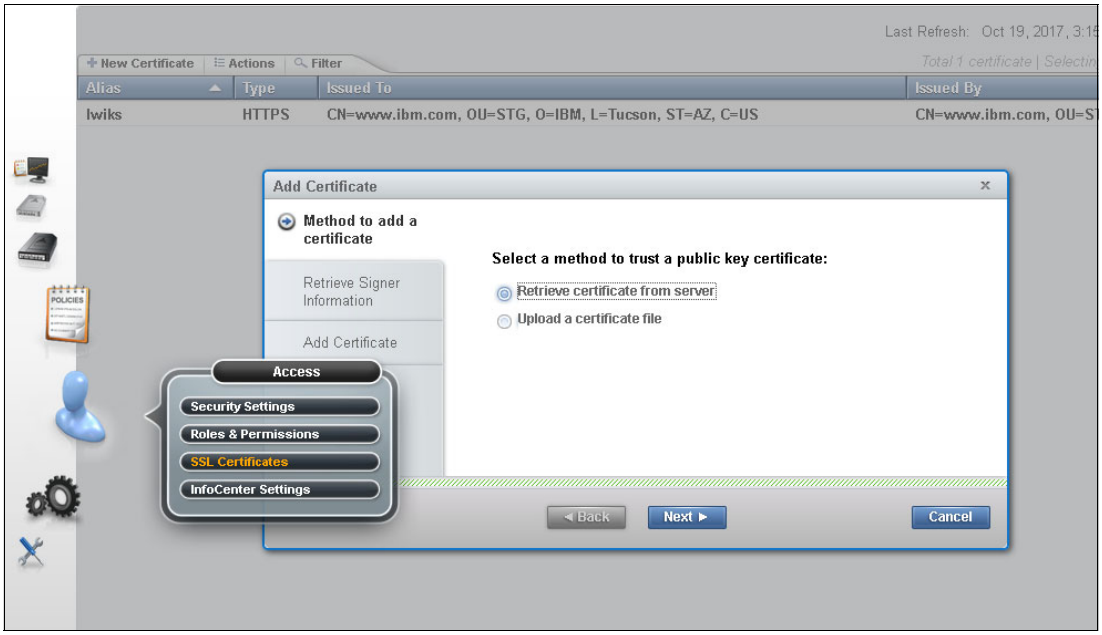

Figure 9-75 SSL Certificates window

If a Primary or alternative Server URL (which is defined by a Storage Authentication Service Policy) uses the HTTPS protocol, a certificate for that address must be defined in this window. The same is true for Direct LDAP policies if the Primary or Alternate server uses LDAPs. If the policy uses LDAP, a certificate is not required. The Certificates table displays identifying information for SSL certificates on the cluster.

The Certificates table displays the following identifying information for SSL certificates on the cluster:

- Alias: A unique name to identify the certificate on the system.
- Issued To: The distinguished name of the entity requesting the certificate.
- Fingerprint: A number that specifies the Secure Hash Algorithm (SHA) of the certificate. This number can be used to verify the hash for the certificate at another location, such as the client side of a connection.
- Expiration: The expiration date of the signer certificate for validation purposes.
- Issued By: The issuer of the certificate.
- Type: Shows the type of the SSL certificate. Can be a trusted certificate installed from a remote server, or HTTPS for a certificate that is used in https connections to the local MI.

To import a new SSL certificate, complete the following steps:

1. Click **Select Action** → **Retrieve from port** and then, click **Go**. The Retrieve from Port window opens.
2. Enter the host and port from which the certificate is retrieved, and a unique value for the alias.