

Authentication

In order to access the Management API, you must be authenticated as a user with sufficient permissions to manage Gateway resources.

Authentication is handled by the REST Management API service. There are two ways to authenticate, HTTP Basic authentication or Client Certificate mutual authentication. We recommend that you implement client certificate mutual authentication for the strongest security. Follow these steps to implement client certificate mutual authentication:

Generate the client certificate and private key

1. In Policy Manager, go to **Tasks, Manage Private Keys**.
2. Click **Create**.
3. Enter an alias and click **Create**. For Internal Identity Providers, the alias must match the login for the migration Administrator.
4. Double-click the certificate in the list, and determine an export method:
 1. To export the certificate and key, click **Export Key**, optionally specify a password, and save to a location.
 2. To export with the private keys, click **View Certificate**, click **Export**, and save to a location.
5. (Optional). You can delete the private key that was used to create the certificate. Policy Manager does not need it.

Associate the client certificate with the Administrator

1. In Policy Manager, click the **Identity Providers** tab.
2. Under Identity Providers, right-click **Internal Identity Provider** and select **Search Identity Provider**.
3. Double-click the migration Administrator.
4. Select the **Certificate** tab, click **Import**.
5. In the Add Certificate Wizard, select **Import from a File**.
6. Click **Browse** to find your certificate and complete the wizard.

Authentication Requirements and Behaviours

When authenticated the Gateway will respond as follows:

- When attempting to access resources, you will receive a "401 Permission Denied" response if you have not been granted access.
- When listing resources, only the resources to which you have access will be returned. This may result in an empty list or only a partial list of the actual resources available on the Gateway.

Access to the Dependency analysis or Migration API calls require administrator access to the Gateway.
