You can choose between two types of authentication for the staging service – Username and password authentication, and X.509 certificates. X.509 authentication is slower and more difficult to configure, but also more secure.

Importing certificates

To use X.509 authentication, you first need to obtain server and client certificates (*.pfx* files) and import them onto your servers. Typically, certificates are issued by a trusted certification authority.

Import the certificates onto the servers hosting your staging instances. The server certificate is required for target staging instances, and the client certificate on source staging instances. We recommend importing both certificates on all servers to ensure that your environment is ready to support bidirectional staging.

If you manage your own servers or are setting up a local development instance, you need to import the certificates to the appropriate certificate store. For example, you can use the Microsoft Management Console (MMC) snap-in tool:

1. In Windows, run the **mmc** command (via the command prompt or the Start menu).
2. In the console window, select **File -> Add/Remove Snap-in**.
3. Select **Certificates** and click **Add**.
    a. For the *server* certificate, choose **Computer account**.
    b. For the *client* certificate, choose **My user account**.
4. Close the **Add or Remove Snap-ins** window by clicking **OK**.
5. Under the console root, expand the *Certificates* snap-in (**Certificates (Local Computer)** or **Certificates - Current User**), right-click the appropriate certificate store folder for your certificate type, and select **All Tasks -> Import**.
6. Import your certificate using the **Certificate Import Wizard**.

> **Certificate store permissions**
>
> The ASP.NET account under which your Kentico application is running (configured for the application pool in IIS) must have the **Read** permission to access the certificates.
>
> You can manage permissions for certificates in the Microsoft Management Console (navigate to the appropriate certificate store folder, right-click the certificate, and select **All Tasks -> Manage Private Keys**).

Getting the certificate key identifiers

To configure X.509 authentication in Kentico, you need to enter key identifier values for both the client and server certificate. If you do not know the values, you can obtain them from the certificate files, for example by running a PowerShell script:

```
# Adds classes from the 'Microsoft.Web.Services3.dll' library to the PowerShell session
# Adjust the path to the location of your Kentico project's 'Lib' folder
Add-Type -Path "C:\inetpub\wwwroot\Kentico\Lib\Microsoft.Web.Services3.dll"

# Stores the specified certificate into a variable
$certificate = Get-PfxCertificate -FilePath "C:\Certificates\Certificate.pfx"

# Gets the key identifier for the certificate and displays it in the script output
$bytes = [Microsoft.Web.Services3.Security.X509.X509Util]::GetKeyIdentifier
($certificate)
[System.Convert]::ToBase64String($bytes)
```

When you run the above script, you will be prompted to enter the certificate password. Get the key identifier for both your client and server certificate and note down the values.

Configuring staging to use certificates

After importing the certificates to your servers and obtaining the key identifier values, adjust the staging settings in Kentico to use the certificates for authentication.

Target servers

On instances that work as a target staging server, change the staging service authentication type:

1. Open the **Settings** application.
2. Select the **Versioning & Synchronization -> Staging** category.
3. Set the **Staging service authentication** setting to **X.509**.
4. Fill in the **Client key ID** and **Server key ID** (copy the key identifier values of your certificates).
5. Click **Save**.

Source servers

On instances that work as a source staging server, adjust the settings of the target servers:

1. Open the **Staging** application.
2. Select the **Servers** tab.
3. Edit () the target servers.
4. Switch the **Server authentication** to **X509**.
5. Fill in the **Client key ID** and **Server key ID** (copy the key identifier values of your certificates).
6. **Save** the configuration.

The staging service now uses certificates for authentication.