JSON Web Token (JWT) configuration in OnGuard

Last Modified on 10/02/2024 10:38 am EDT

JWT Configuration in OnGuard (Microsoft Entra ID example)

Prerequisites

The certificate must be prepared by a trusted certificate issuer. For testing purposes, you can prepare a self-signed certificate by using the following powershell command:

$cert = New-SelfSignedCertificate -Subject "CN=MyCertificateForTesting" -CertStoreLocation "Cert:\LocalMachine\My" -KeyExportPolicy Exportable -KeySpec Signature

Supported Certificate-Based Authentication Methods for “OpenId Connect” Directory Type

Reading Directly from Local Certificate Manager by Thumbprint Identifier

Perform the following procedure:

1. Export the certificate (without private key) using Manage Computer Certificates and add it to the known certificates of the application registered in Azure.
2. In **System Administration > Directories**, choose your directory and replace the Client Secret with: **###CBA###*<your certificate thumbprint>*.thumbprint###CBA###**

   For example:
   ###CBA###9cb34c8dc98833a17e7f8fc59c7096a54843fd41.thumbprint###CBA###

Using a PKCS#12 (*.pfx, password protected) File Exported from Certificate Manager or Received from Trusted Certificate Issuer

Perform the following procedure:

1. Add your certificate stored in the *.pfx file to the known certificates of the application registered in Azure.
2. Move your certificate stored in the *.pfx file to the certificate directory (**C:\Program Files (x86)\OnGuard\Certificates** by default; path can also be defined in the **OpenAccess.ini** file).
3. In **System Administration > Directories**, choose your directory and replace Client Secret with: **###CBA###*<certificate password>*###PW###*<certificate file name>*.pfx###CBA###**

For example:
###CBA###someP@ssword123###PW###pkcs12WithPasswordForEntraID.pfx###CBA###

Configuring Directory in System Administration (Microsoft Entra ID example)

1. Open System Administration with a user that has sufficient permissions to add a directory.
2. Navigate to **Administration > Directories**.
3. Provide the necessary properties:
   a. General tab:
   Name:*<your_directory_name>*
   Base URL: https://login.microsoftonline.com/<your_tenant_ID>/v2.0
   b. Authentication tab:
   Client ID:*<your_client_application_id>*
   Client Secret: ###CBA###*<your_certificate_thumbprint>*.thumbprint###CBA###
   or
   ###CBA###*<certificate password>*###PW###<certificate file name>.pfx###CBA###
   Claim: upn (User Principal Name, formatted like an email address)
   c. Advanced tab:
   - Uncheck **Require Access Token Hash**
   Additional Endpoints:
   - https://login.microsoftonline.com/<your_tenant_id>/oauth2/v2.0/
   - https://login.microsoftonline.com/<your_tenant_id>/discovery/v2.0/
   - https://graph.microsoft.com/oidc/userinfo
   - https://login.microsoftonline.com/<your_tenant_id>/kerberos
4. Save the directory and navigate to **Administration > Users**.
5. Modify the desired user's directory account assignment to utilize JWT authentication.
6. Click [Link], select the *<your_directory_name>* directory, provide Claim Value (for example, user@email.com), and click [OK].

JWT authentication is now configured.

Applies To

OnGuard 8.3 and later.

Additional Information