Entrust Identity as a Service and Entrust CloudControl

Integration Guide

2024-02-12

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. Product configurations . . . 1
    1.2. Requirements . . . 1
2. Register for Entrust iDaaS and configure Active Directory . . . 2
    2.1. Register for Entrust IDaaS . . . 2
    2.2. Configure your Active Directory . . . 2
3. Download and configure Entrust CloudControl . . . 4
    3.1. Download the Entrust CloudControl software . . . 4
    3.2. Deploy an Entrust CloudControl VM from the OVA . . . 4
    3.3. Power the Entrust CloundControl virtual appliance . . . 5
    3.4. Configure the Entrust CloudControl virtual appliance . . . 5
4. Download and configure Entrust iDaaS Active Directory . . . 10
    4.1. Download the Entrust IDaaS gateway . . . 10
    4.2. Deploy Entrust IDaaS gateway VM from the OVA . . . 10
    4.3. Configure the Entrust IDaaS gateway virtual appliance . . . 11
    4.4. Add the gateway to the Entrust IDaaS. . . . 12
    4.5. Tie Active Directory to Entrust IDaaS . . . 14
5. Create a generic web application . . . 18
    5.1. Create Entrust IDaaS application . . . 18
    5.2. Add a resource rule to the application . . . 20
    5.3. Enable external authentication in Entrust CloudControl to use Entrust IDaaS . . . 22
6. Test integration . . . 25
    6.1. Test Entrust IDaaS authentication . . . 25
    6.2. Test whitelist authentication . . . 28
7. Additional resources and related products . . . 30
    7.1. CloudControl . . . 30
    7.2. Identity as Service . . . 30
    7.3. Entrust products . . . 30
    7.4. nShield product documentation . . . 30

Chapter 1. Introduction

This guide describes how to integrate Entrust Identity as a Service (IDaaS) with Entrust CloudControl. Entrust IDaaS is a cloud-based identity and access management (IAM) solution with multi-factor authentication (MFA), credential-based passwordless access, and single sign-on (SSO). Entrust CloudControl can be configured to use Entrust IDaaS as an external authentication method.

1.1. Product configurations

Entrust has successfully tested the integration of Entrust CloudControl with Entrust IDaaS in the following configurations:

System	Version
Entrust CloudControl	6.6.0
Entrust IDaaS gateway	5.28
VMware vCenter	8.0.0 U1

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- Entrust IDaaS. You can request a free trial at the Entrust Identity as a Service product page.
- The documentation and setup process for Entrust CloudControl. The online documentation contains everything you need to successfully install and deploy CloudControl.

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Register for Entrust iDaaS and configure Active Directory

This guide uses a standalone Entrust CloudControl deployment configured with Active Directory for authentication. CloudControl does support a cluster environment. For more information refer to the Entrust CloudControl Installation Guide in the online documentation.

1. Register for Entrust IDaaS
2. Configure your Active Directory

2.1. Register for Entrust IDaaS

1. Register at Start Free IDaaS Trial. Entrust provides a 60-day free trial.
2. Once registered you will be assigned a unique Entrust IDaaS registration URL, for example **https://example.US.trustedauth.com**. Bookmark this URL.

2.2. Configure your Active Directory

CloudControl supports both local authentication and Active Directory for authentication. This integration uses Active Directory authentication. The following steps configure your DNS server. This may be a task for your system admin depending on your level of access privileges.

See Active Directory Authentication.

1. Add a DNS entry for the Entrust CloudControl node in your domain controller.
2. Add the following Active Directory users.

Ensure the **Last Name** and **Email** fields are not empty.

User	Role
htaServiceAccount	Entrust CloudControl service account
etccadmin	Entrust CloudControl administrator whitelisted for direct login bypassing Entrust IDaaS authentication.

User	Role
etccuser	Entrust CloudControl user to be validated by Entrust IDaaS authentication.
idaasaduser	Entrust IDaaS synchronization with your domain controller.

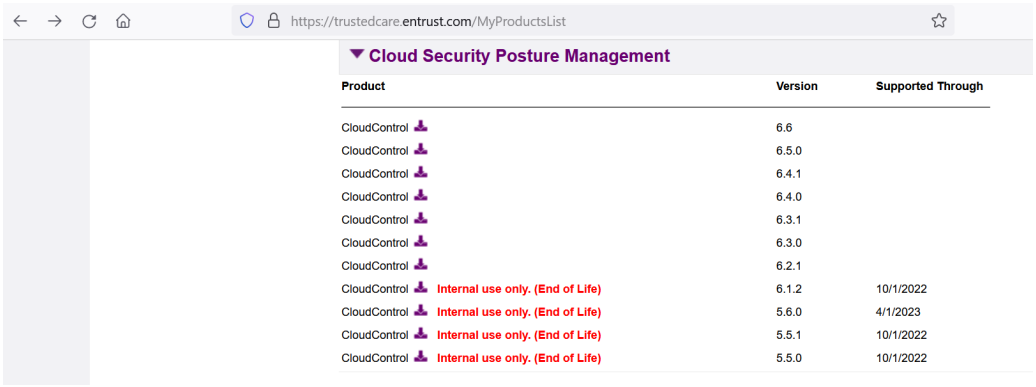
3. Create a group in Active Directory called **ASC_SuperAdmin**.
4. Make the **etccadmin** and **etccuser** users members of this group.

Chapter 3. Download and configure Entrust CloudControl

1. Download the Entrust CloudControl software
2. Deploy an Entrust CloudControl VM from the OVA
3. Power the Entrust CloundControl virtual appliance
4. Configure the Entrust CloudControl virtual appliance

3.1. Download the Entrust CloudControl software

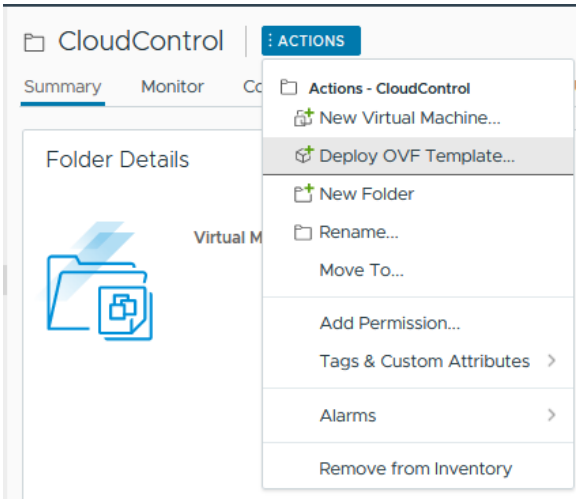
1. Go to https://trustedcare.entrust.com
2. Sign in with your Entrust Trusted Care account.
3. Select **Products** and then expand **Cloud Security Posture Management** under **CLOUD SECURITY**.
4. Select the Entrust CloudControl version and then select and download the OVA.



5. Open the downloaded ZIP file to access to the OVA file.

3.2. Deploy an Entrust CloudControl VM from the OVA

1. Log in to vCenter.
2. Select the cluster in which to create the Entrust CloudControl VM.
3. From the **Actions** menu, select **Deploy OVF template...**.



4. Select **Local file** and upload the Entrust CloudControl OVA file, and then select **Next**.
5. Follow the instructions during the deployment as needed.

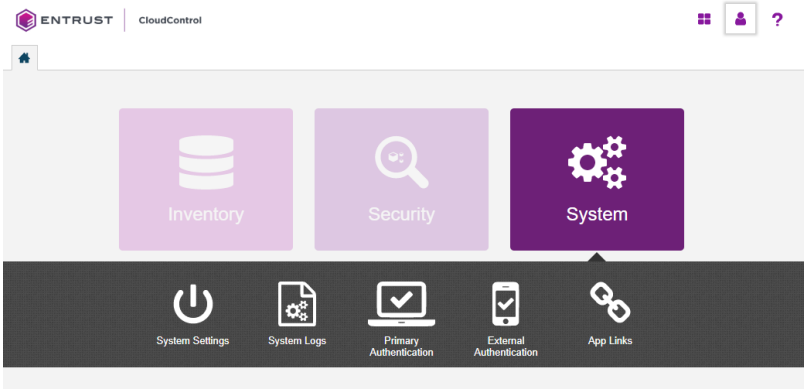
For more information refer to Installing CloudControl from an OVA in the online documentation.

3.3. Power the Entrust CloundControl virtual appliance

1. Sign in to the vCenter.
2. Locate the Entrust CloudControl virtual machine in the inventory.
3. Right-click the Entrust CloudControl virtual machine and select **Power > Power On**.

3.4. Configure the Entrust CloudControl virtual appliance

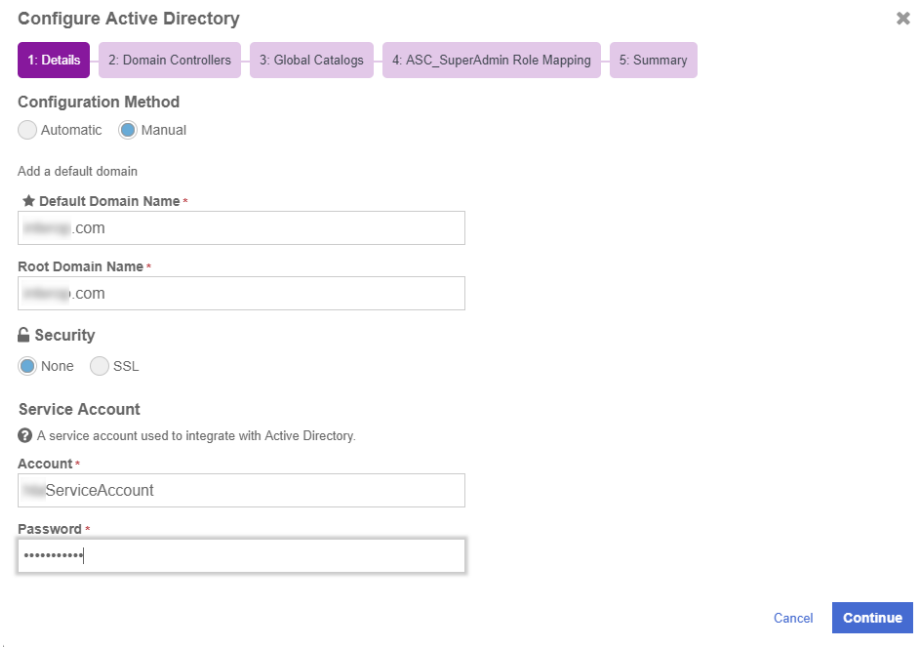
1. Create a standalone Entrust CloudControl node as described in Creating a Standalone Node.
2. Set up the CloudControl GUI as described in Setting Up the CloudControl GUI
3. Open a web browser and navigate to the IP address or hostname of the standalone Entrust CloudControl node created above. Bookmark this URL.
4. Login with the credentials from Entrust CloudControl GUI credentials.
5. Select **Home > System > Primary Authentication**.



6. Select **Configure Active Directory** and **Confirm** you want to configure Active Directory.
7. In the **Details** tab of the **Configure Active Directory** window, enter the following:

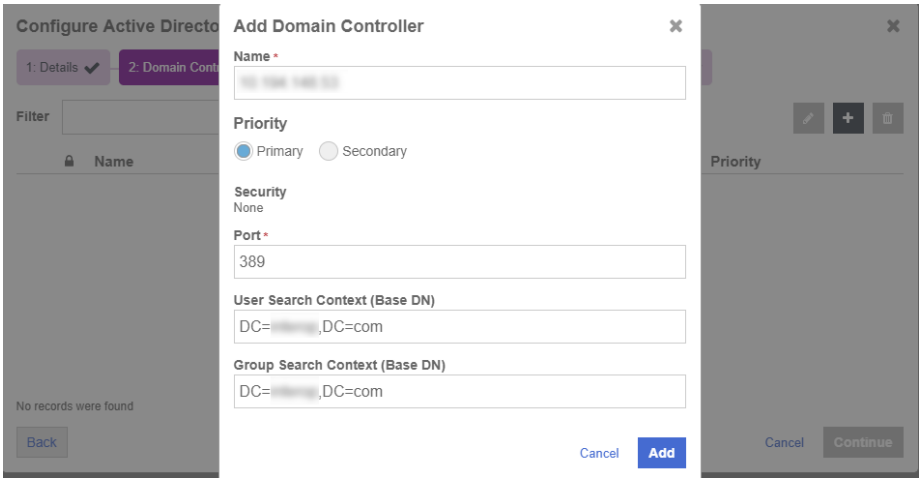
Item	Value
Configuration Method	**Manual**
Default Domain Name	Domain name
Root Domain Name	Domain name
Security	**None**
Service Account	Service account, for example, htaServiceAccount
Service Account Password	Password for account above

This guide uses a **Manual** configuration. However, in a production environment Entrust recommends that this field is set to **Automatic Mode**. The mode can also be changed later using the **Actions** > **Change to Automatic Mode** menu.



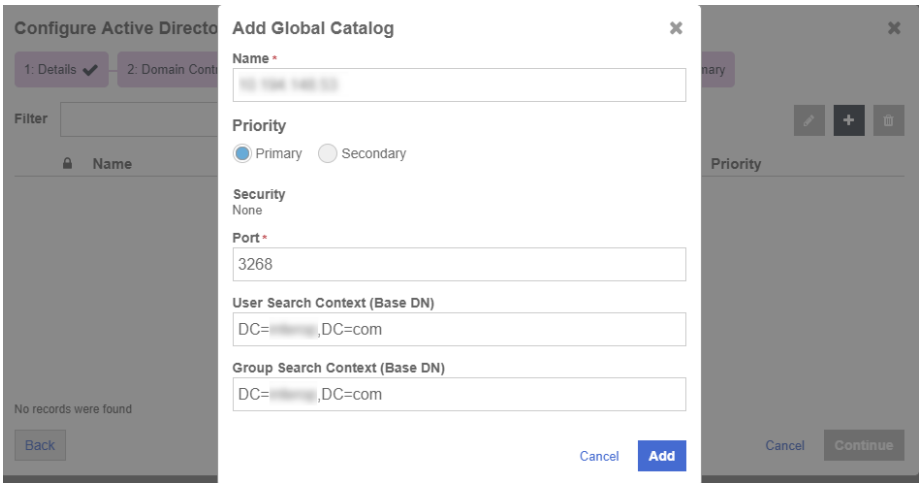
8. In the **Domain Controllers** tab, select the **Add Domain Controller Now** link.
9. In the **Add Domain Controller** window, enter the following information:

Item	Value
Name	IP address/FQDN of the Active Directory server
Priority	**Primary**
Port	389 (for LDAP)
User Search Context (Base DN)	Your search context, for example, DC=example,DC=com
Group Search Context (Base DN)	Your search context, for example, DC=example,DC=com

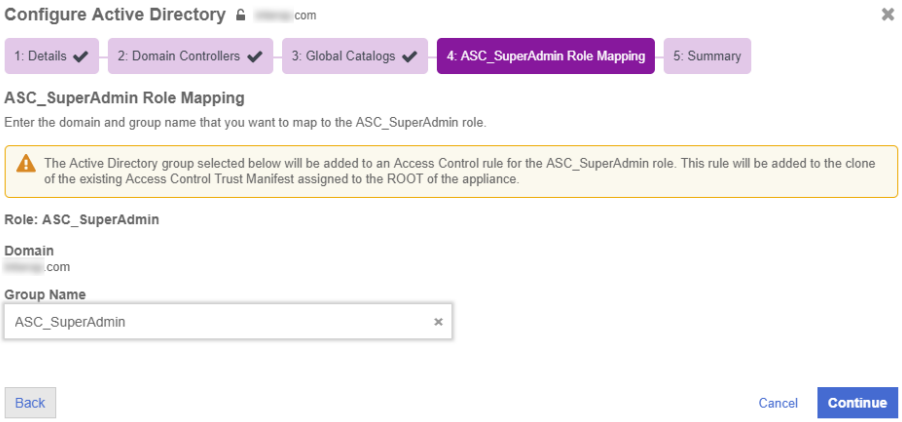


10. Select **Continue**.
11. In the **Global Catalogs** tab, select the **Add a Global Catalog Now** link.
12. In the **Add Global Catalog** window, enter the following information:

Item	Value
Name	IP address/FQDN of the Active Directory server
Priority	**Primary**
Port	3268
User Search Context (Base DN)	Your search context, for example, DC=example,DC=com
Group Search Context (Base DN)	Your search context, for example, DC=example,DC=com

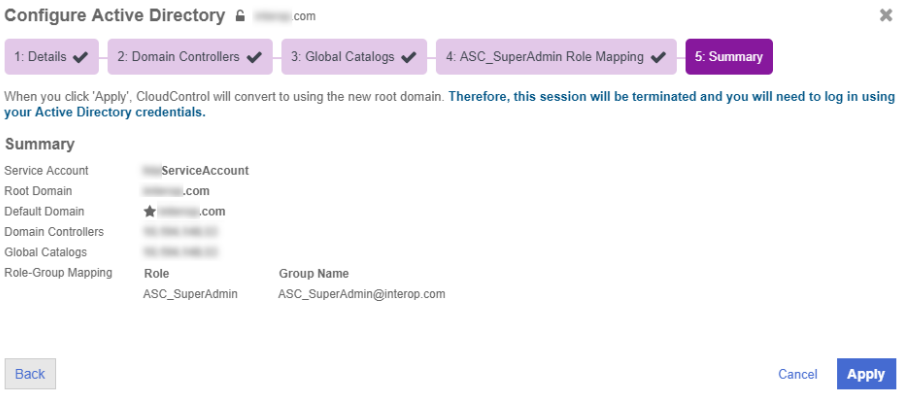


13. Select **Add** and then **Continue**.
14. In the **Add Additional Domains** window, select **Skip**.
15. In the **ASC_SuperAdmin Role Mapping** tab, enter the Active Directory group created in Configure your Active Directory.



16. Select **Continue**.

    The summary window displays the details.



17. Select **Apply** to make the changes effective. A confirmation window is shown asking you to confirm the changes to Active Directory.
18. Select **Apply AD Settings and Log Out**.
19. Sign back in either of the two accounts **etccadmin** or **etccuser** in the **ASC_SuperAdmin** group in Active Directory.

Chapter 4. Download and configure Entrust iDaaS Active Directory

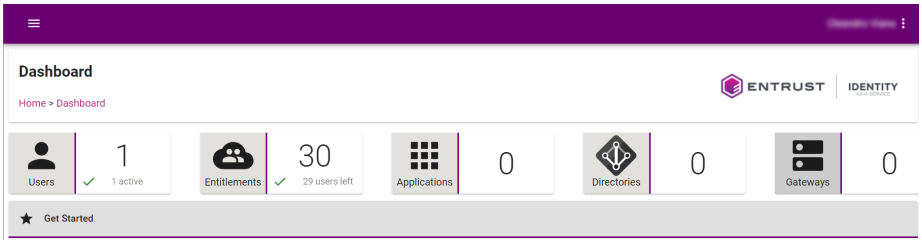
Configure Entrust IDaaS to use the same Active Directory services as Entrust CloudControl. Entrust provides an Entrust IDaaS gateway OVA to sync your on-premises Active Directory users to Entrust iDaaS. Changes made to your Active Directory are automatically synced with Entrust IDaaS through this gateway. Alternatively, you can configure your own gateway.

For additional information, refer to Entrust Identity as a Service Administrator Help.

1. Download the Entrust IDaaS gateway
2. Deploy Entrust IDaaS gateway VM from the OVA
3. Configure the Entrust IDaaS gateway virtual appliance
4. Add the gateway to the Entrust IDaaS.
5. Tie Active Directory to Entrust IDaaS

4.1. Download the Entrust IDaaS gateway

1. Sign in to your unique Entrust IDaaS registration URL bookmarked in section Register for Entrust IDaaS.



2. Select **Home** page, then select **Gateways**.
3. On the **Gateways** page, select **IDENTITY AS A SERVICE GATEWAY** to download the software. The **Identity as a Service Gateway Download URL** dialog appears.
4. Select the **VMware vSphere** to download a vSphere (.ova) image file.

4.2. Deploy Entrust IDaaS gateway VM from the OVA

1. Sign in to VMware vCenter.
2. Select the cluster in which to create the Entrust IDaaS gateway VM.
3. From the **Actions** menu, select **Deploy OVF template...**.

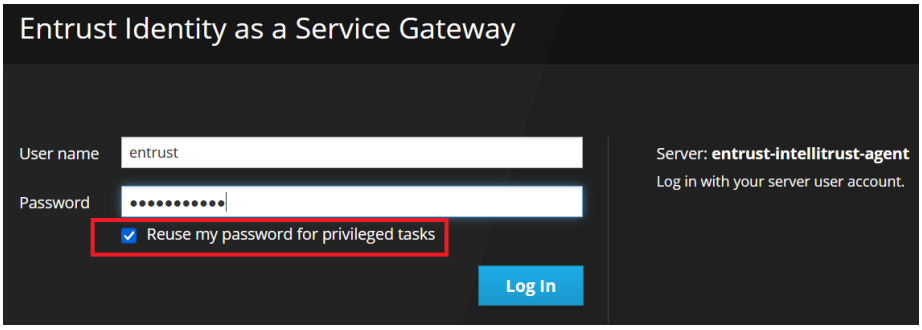
4. Select **Local file** and upload the Entrust IDaaS gateway OVA file, and then select **Next**.
5. Follow the instructions during the deployment as needed.
6. After the VM is ceated, right-click the Entrust IDaaS gateway virtual machine and select **Power > Power On**.
7. Select **LAUNCH WEB CONSOLE** and make a note of the dynamic IP of the Entrust IDaaS gateway virtual machine. You will be able to change this IP to static in the next section.
8. Close the web console.

4.3. Configure the Entrust IDaaS gateway virtual appliance

1. In a web browser, sign in to the Entrust IDaaS gateway dynamic IP with port 9090, for example, **https://xxx.xxx.xxx.xxx:9090**.
2. Accept the browser self-signed certificate warning. The Entrust IDaaS gateway Web Interface opens.
3. Sign in with the following credentials:

Credential	Value
User name	entrust
Password	entrust

4. Enter the new password when prompted.
5. Sign out and then sign back in. This time, select **Reuse my password for privileged tasks**.



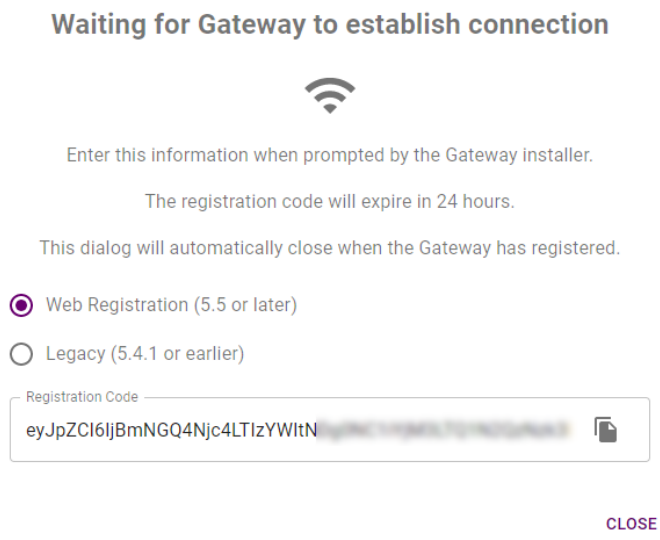
6. Select **Get Started**. The **Network Settings** page appears.
7. Select **Network** to change the hostname, IP address, and gateway address.
8. Optionally, change the hostname by selecting the corresponding hyperlink, and then select **Save**.

9. Change the IP address and gateway by selecting the corresponding hyperlink.
10. Enter the new static IP and gateway, and then select **Save**. You will be disconnected after saving is completed.
11. At the VMware vCenter, select **Actions** > **Power** > **Restart Guest OS**.
12. Sign back in to the Entrust IDaaS gateway with your browser using the new static IP with port 9090.
13. Select **Get Started**. The **Network Settings** page appears.
14. Select **System Time** to change the default NTP servers if needed, and then select **Save**.
15. If required, select **Proxy** to configure a proxy server, and then select **Save**. In this integration a proxy server was not necessary since we were able to access the Internet.

You do not need to select **Register** at this time. It will be done in the next section.

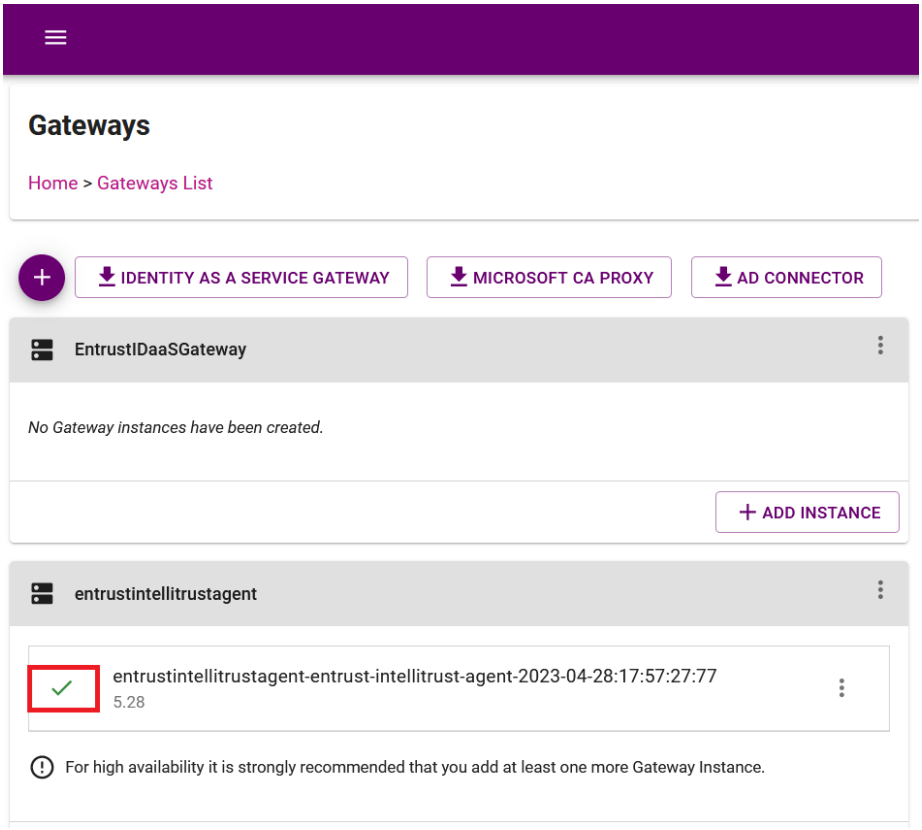
4.4. Add the gateway to the Entrust IDaaS.

1. Sign in to your unique Entrust IDaaS registration URL.
2. Select **Gateways**. The **Gateways** page appears.
3. Select the **+** icon on the left of the page and select **Gateway**. The **Add Gateway** dialog appears.
4. Enter a **Gateway Name** and then select **Add**. The **Waiting for Gateway to establish connection** dialog appears.

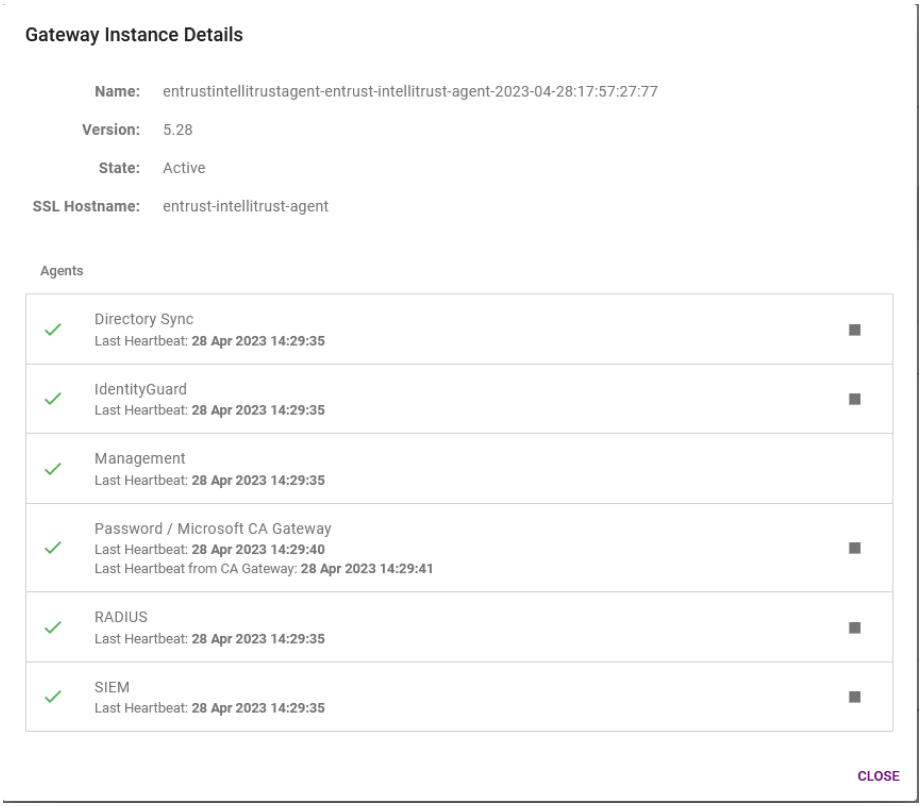


5. Copy the **Registration Code** by selecting the **Copy to clipboard** icon.

6. Sign in to the Entrust IDaaS gateway with your browser.
7. Select **Identity as a Service**.
8. Paste the registration code from above in the **Registration Code** text box, and then select **Register**.
9. Go back to your unique Entrust IDaaS registration URL. Close the **Waiting for Gateway to establish connection** dialog box if still open, and then sign in.
10. Select **Gateways**. There is a green check mark next to the gateway created above.



11. Hover over the gateway name to display the details.



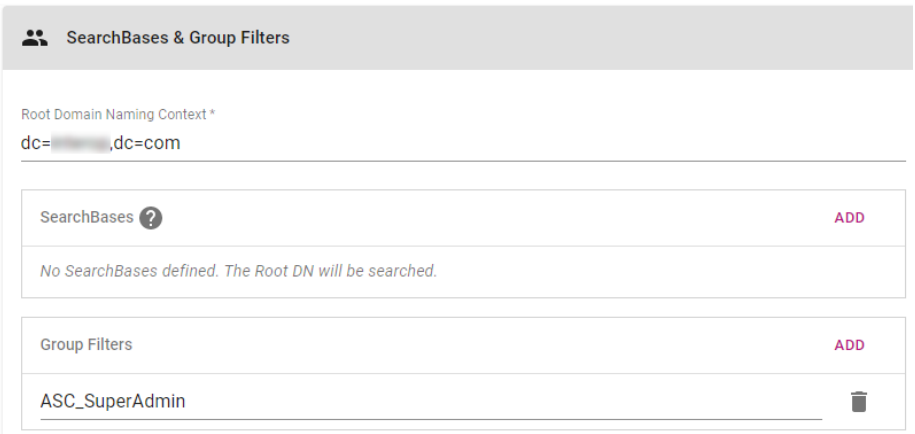
4.5. Tie Active Directory to Entrust IDaaS

1. Sign in to your unique Entrust IDaaS registration URL.
2. Select **Directories**.
3. Select the **+** icon on the left of the page and then select **Active Directory (on-premise)**. The **Add Directory** page appears.
4. In the **Connection Settings**, enter the following:

Item	Value
Directory Name	Domain name
Username	idaasaduser (user created in [download-configure-idaas-active-directory:::configure-active-directory])
Password	Password for idaasaduser
Directory Servers	IP/FQDN of the Active Directory server

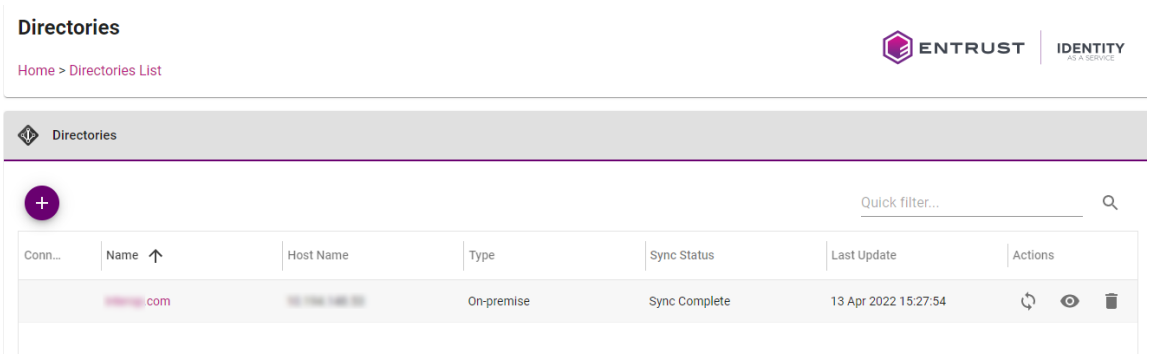
5. In the **Attribute Mappings** section, change the default settings if required.
6. In the **SearchBases & Group Filters** section, enter the following:

Item	Value
Root Domain Naming Context	search context, for example, DC=example,DC=com
Group Filters	ASC_SuperAdmin (group created in Configure your Active Directory)

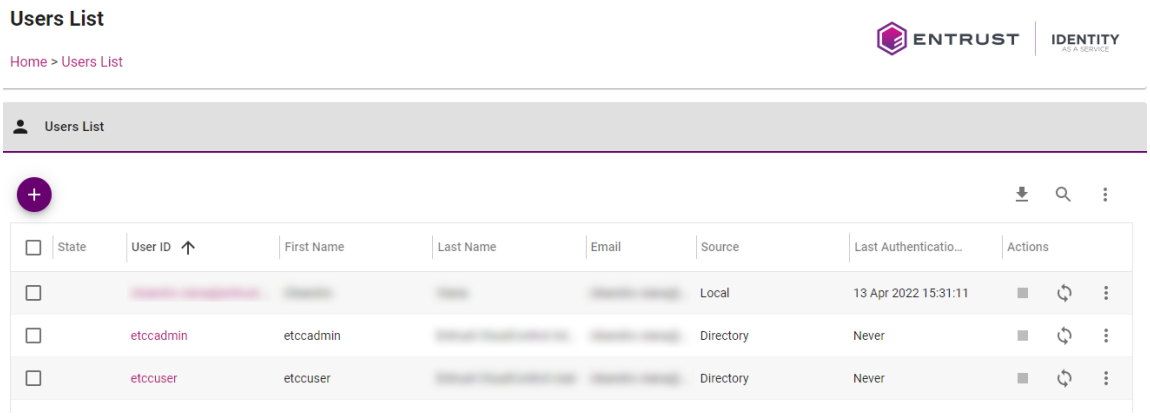


7. In the **Synchronization** section, do the following:
   a. Select the **Synchronization Agent** in the pull-down menu, that is the Entrust IDaaS gateway created in section Configure the Entrust IDaaS gateway virtual appliance.
   b. Once selected, edit the properties according to your AD settings or leave the defaults.

8. Once all the information has been provided, select **Add**. The **Directory List** page appears.



9. Select the **Sync** icon on the directory list row to sync the directory.
10. Once synced, verify the Active Directory users **etccadmin** and **etccuser** created in section [download-configure-idaas-active-directory:::configure-active-directory] appear in **Home** > **Users**.


Users List
Home > Users List
ENTRUST
IDENTITY
AS A SERVICE
Users List
State
User ID
First Name
Last Name
Email
Source
Last Authenticatio...
Actions
Local
13 Apr 2022 15:31:11
etccadmin
etccadmin
Directory
Never
etccuser
etccuser
Directory
Never

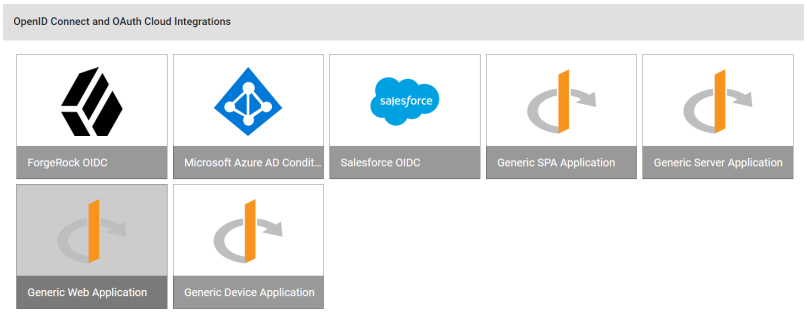
Chapter 5. Create a generic web application

Create a generic web application that uses OpenID Connect and OAUTH Cloud Integration. This is the application Entrust CloudControl uses to integrate with Entrust IDaaS.

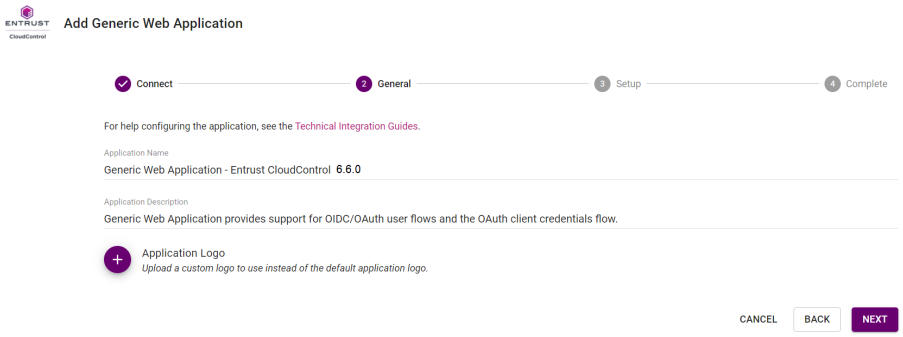
1. Create Entrust IDaaS application
2. Add a resource rule to the application
3. Enable external authentication in Entrust CloudControl to use Entrust IDaaS

5.1. Create Entrust IDaaS application

1. Sign in to your unique Entrust IDaaS registration URL.
2. Select **Home** > **Applications**.
3. Select the **+** icon on the left of the page and scroll down to **OpenID Connect and OAuth Cloud Integration**.
4. Select **Generic Web Application**. The **Add Generic Web Application** page appears.



5. Change the **Application Name**, **Description** and **Add an Application Logo** as required. Check both **Enable user login** and **Enable passkey login**.



6. Select **Next**.
7. In the Setup page, under General Settings, do the following:

    a. Copy and paste the **Client ID** and the **Client Secret** to a safe location. These will

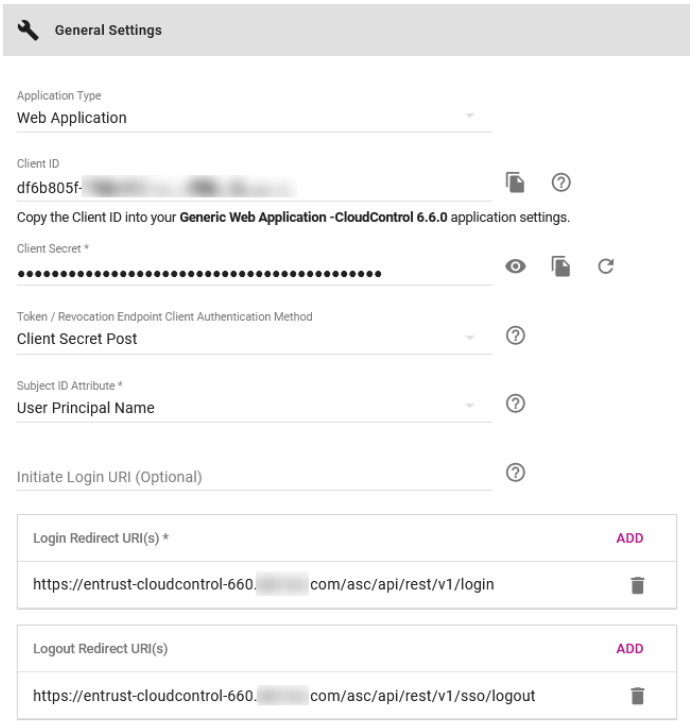
be used when configuring the OpenID connect in Entrust CloudControl.

b. Change **Token / Revocation Endpoint Client Authentication Method** to **Client Secret Post** using the pull-down menu.

c. Change **Subject ID Attribute** to **UserPrincipalName**.

d. For **Login Redirect URLs** and **Logout Redirect URLs**, select **ADD** and enter the URL as described in Configuring Entrust Identity as a Service to use with Entrust CloudControl.

For example:



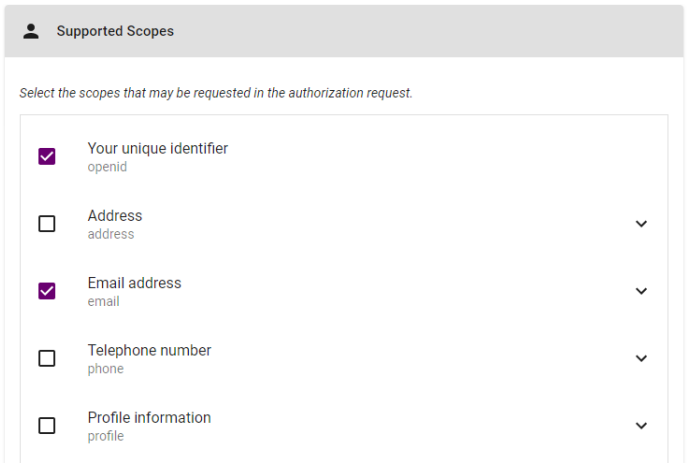
8. In the Setup page, under Supported Scopes:

a. Select **Your Unique Identifier**.

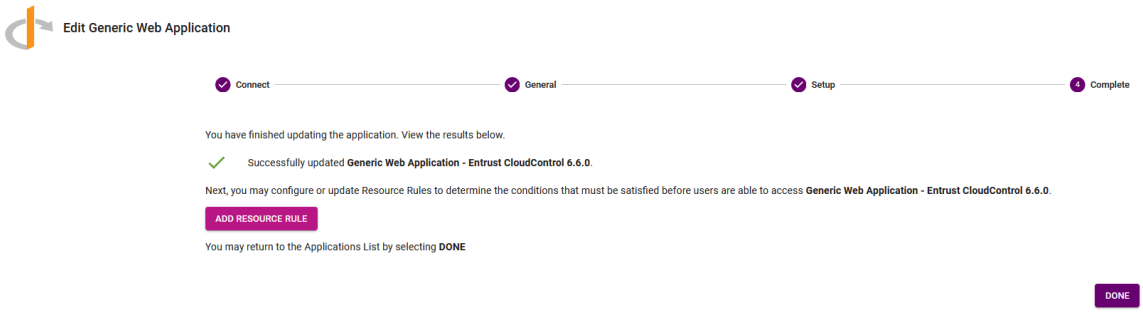
b. Select **Email Address**.

c. Leave all other settings as default.

For example:



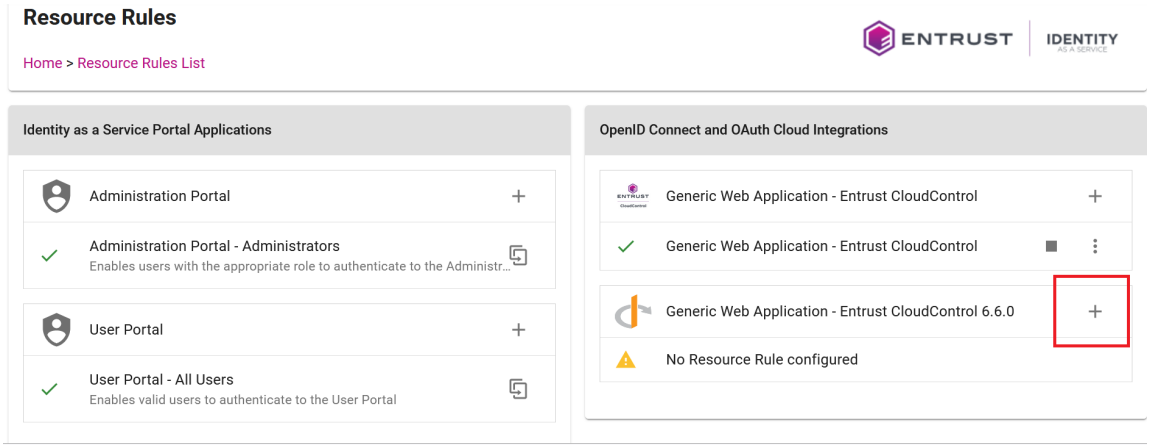
9. Select **Submit** to complete the application creation. The **Add Generic Web Application Complete** page appears.



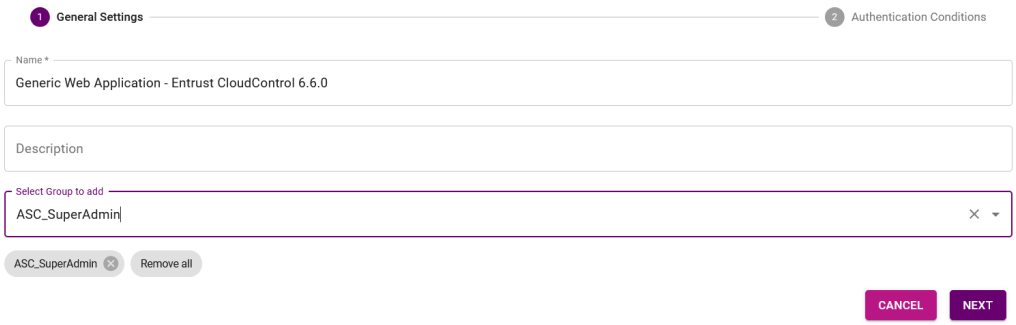
5.2. Add a resource rule to the application

Add a resource rule to the Entrust IDaaS application for the AD group and users to access the application. For additional information, refer to Create a resource rule in the online documentation.

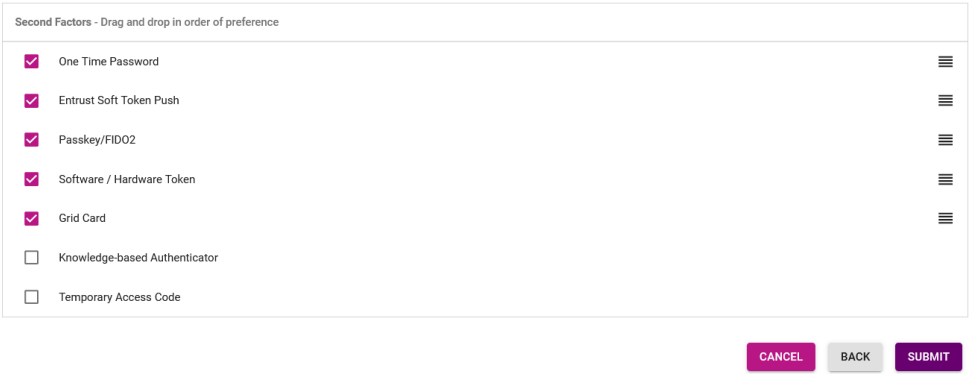
1. Sign in to your unique Entrust IDaaS registration URL.
2. From the **Main Menu** in the top-right, select **Resources** > **Resource Rules**. The **Resource Rules List** page appears.
3. Select the **+** icon on the generic web application created in Configure your Active Directory. The **Add Resource List** page appears.



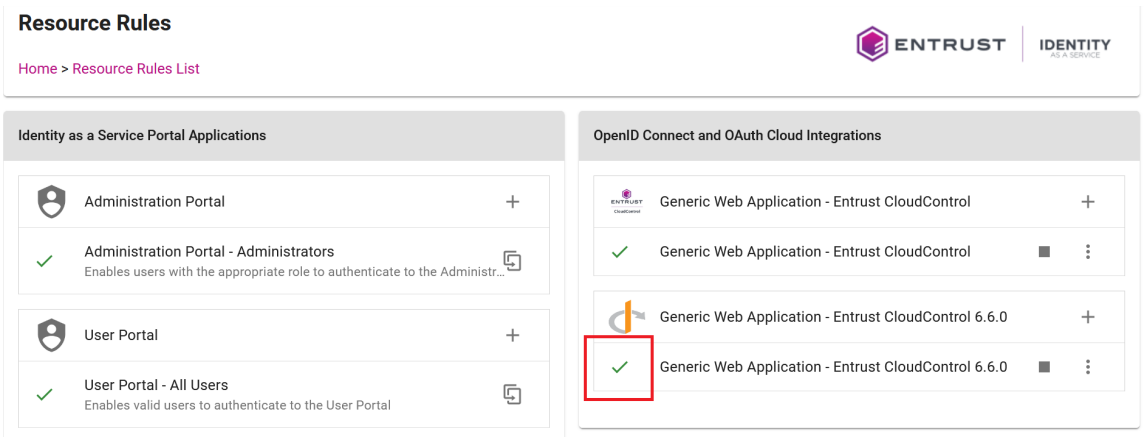
4. In the **General Settings** go to the the **Select Group to add** pull-down menu and select **ASC_SuperAdmin**, then select **Next**. This is the group created in [create-generic-web-application:::configure-active-directory].



5. In the **Authentication Conditions** page:
   a. Select **Password** from the **First Factor** pull-down menu.
   b. In the **Second Factor** box, select the checkboxes for the following factors and rearrange them into the order in which they are listed here, unless determined otherwise by your organization. Clear the checkboxes for all other factors not listed here.
      - One Time Password
      - Entrust Soft Token Push
      - Passkey/FIDO2
      - Software / Hardware Token
      - Grid Card

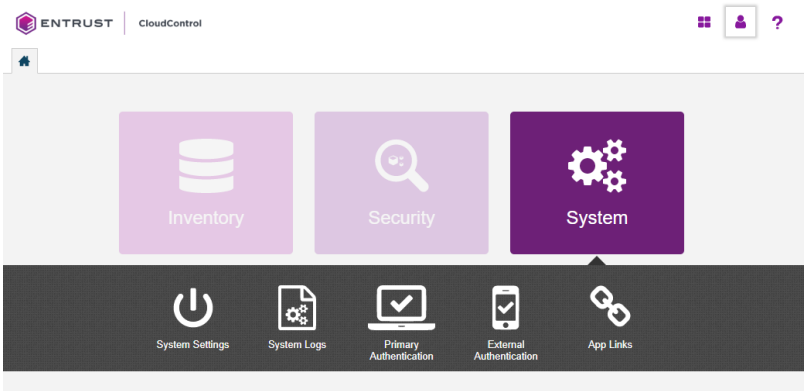


6. Select **Submit**. A check mark appears next to the generic web application.



5.3. Enable external authentication in Entrust CloudControl to use Entrust IDaaS

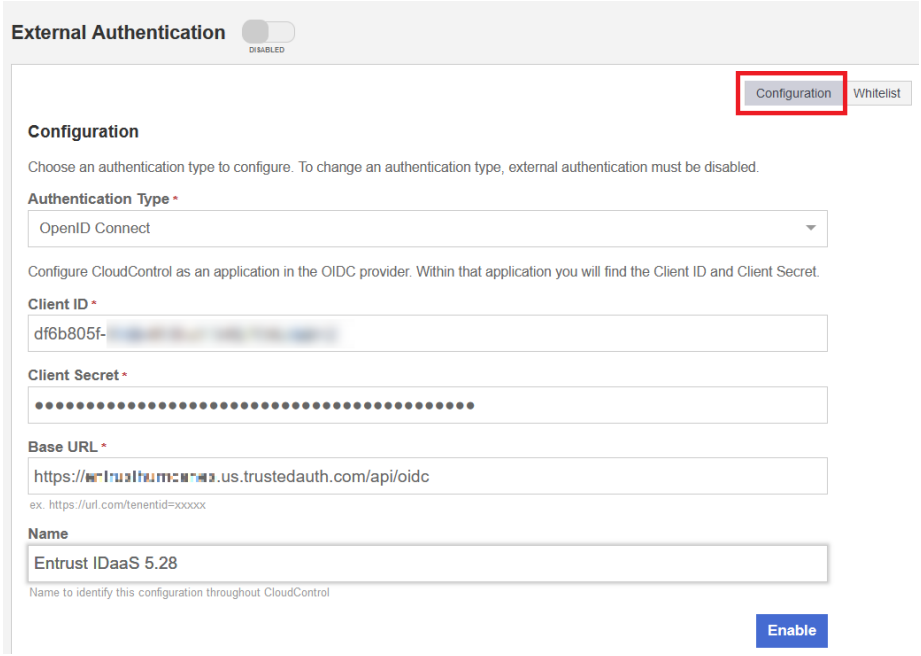
1. Sign in to the Entrust CloudControl virtual appliance with the **etccadmin** account created in Configure your Active Directory.
2. Select **Home** > **System** > **External Authentication**.



3. In the **External Authentication** tab, select **Configuration**, and enter the following information:

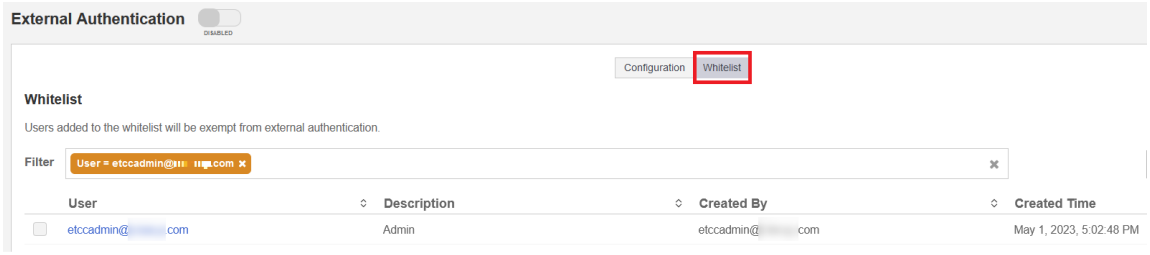
Item	Value
Authentication Type	OpenId Connect (from pull-down menu)
Client ID	Client ID from section Create Entrust IDaaS application
Client Secret	Client Secret from section Create Entrust IDaaS application
Base URL	Your unique Entrust IDaaS registration URL followed by `api/oidc`.
Name	Enter a name.

For example:

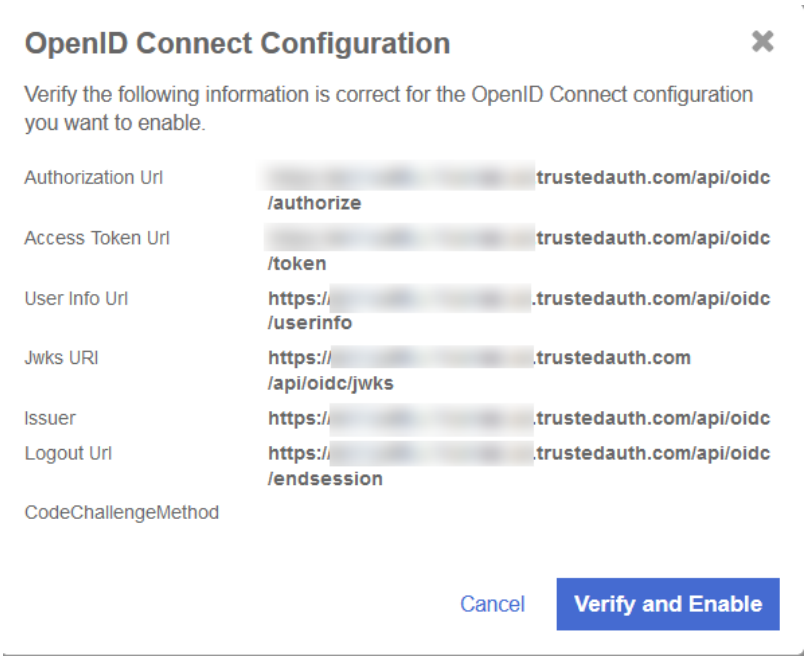


4. In the **External Authentication** tab, select **Whitelist**, and enter the **etccadmin** user created in Configure your Active Directory. This user would be able to sign in without Entrust IDaaS authentication in the event of a configuration issue. Then select **Enable**.

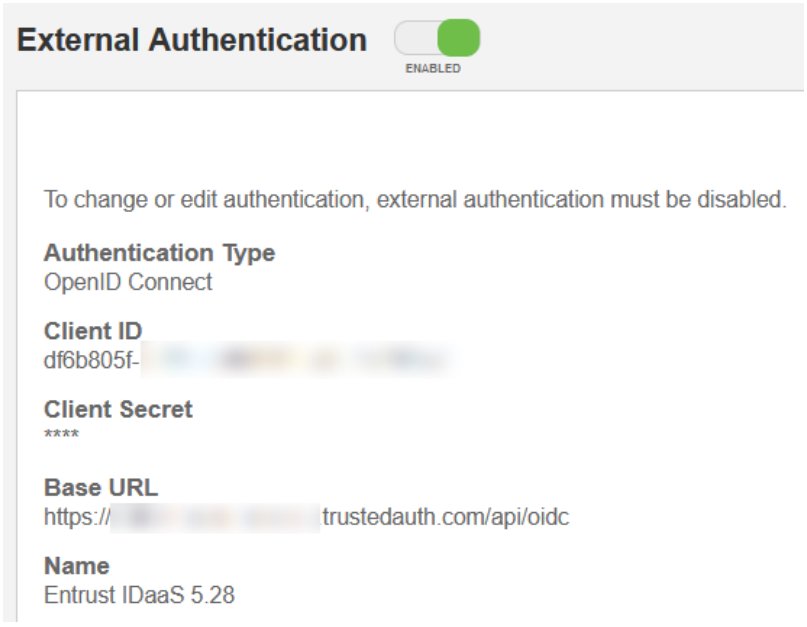
> Users on the whitelist are exempt from external authentication and can sign in directly using Active Directory credentials.



5. Select **Enable** back in **Configuration**. The **OpenID Connect Configuration** dialog appears.



6. Return to the **Configuration** screen, still in the **External Authentication** tab, and select **Enable**. External configuration is now enabled.



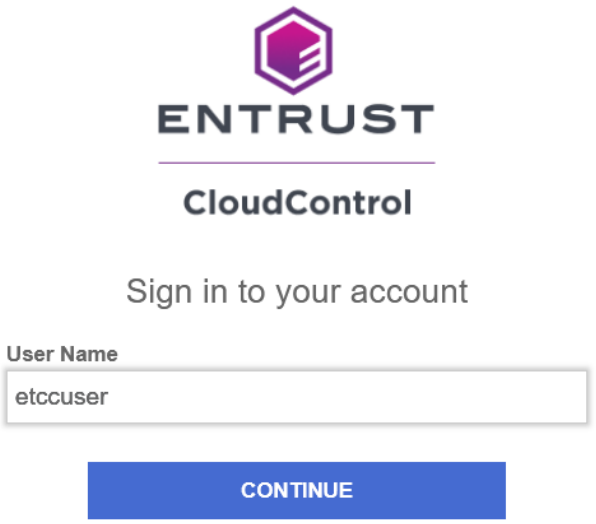
Chapter 6. Test integration

1. Test Entrust IDaaS authentication
2. Test whitelist authentication

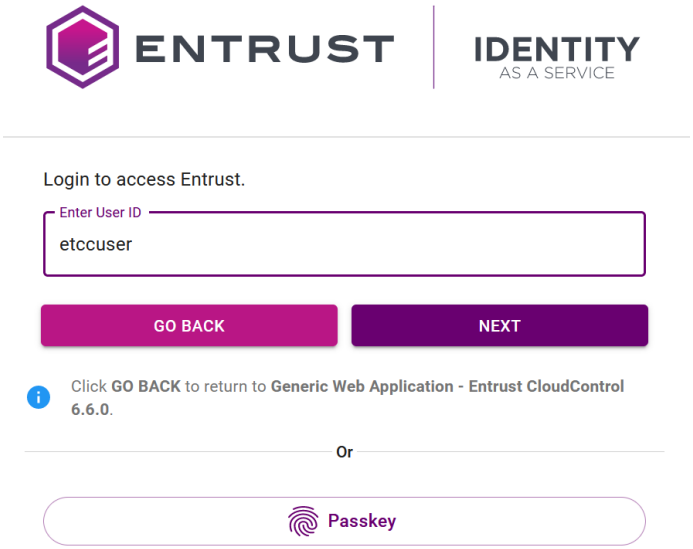
6.1. Test Entrust IDaaS authentication

This test verifies whether Entrust IDaaS is used to validate users attempting to sign in to Entrust CloudControl.

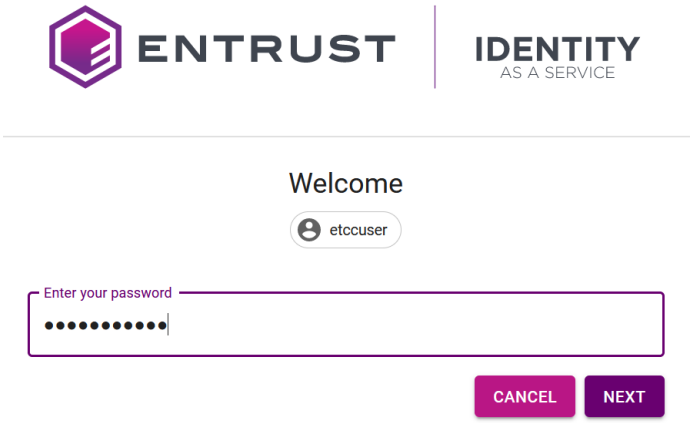
1. Sign in with user **etccuser** to the Entrust CloudControl URL. The user **etccuser** is a domain user defined in Configure your Active Directory.



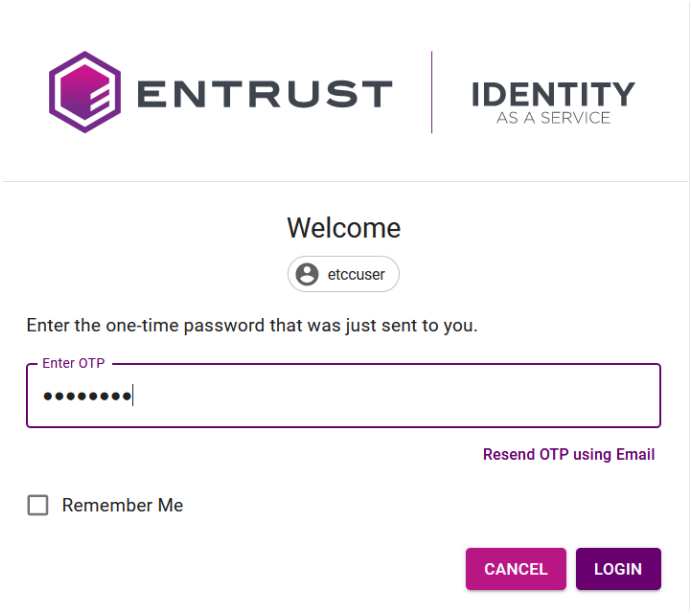
2. Select **Continue**. The Entrust IDaaS login screen appears.
3. Select **Next**.



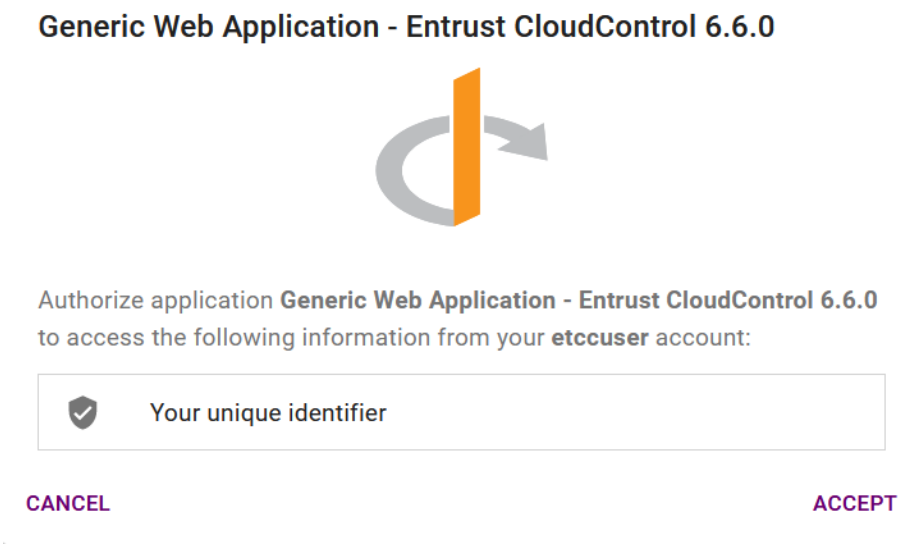
4. Enter the **etccuser** password, and then select **Next**. Entrust IDaaS then sends an OTP code to the email for **etccuser**.



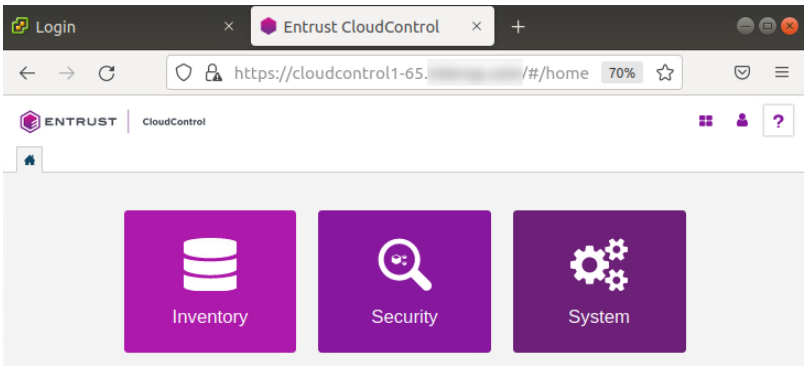
5. Enter the OTP code. Then select **Login**.



6. Select **Accept**.



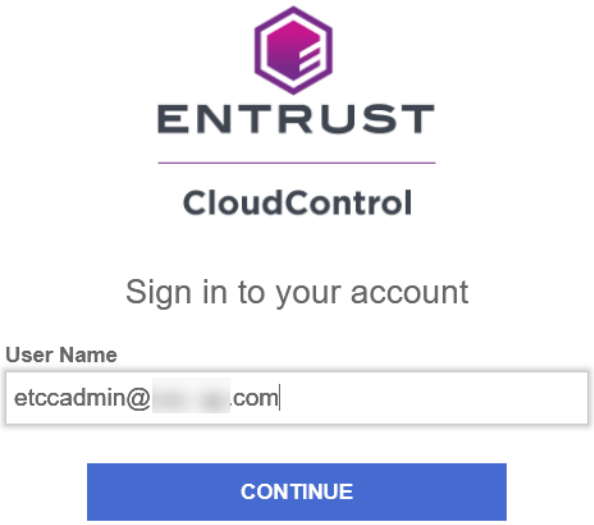
Entrust IDaaS authenticates the user and redirects you back to the CloudControl home screen.



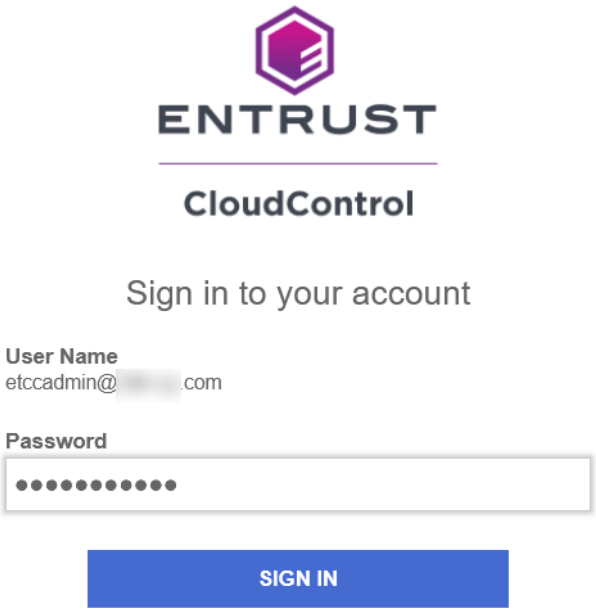
6.2. Test whitelist authentication

This tests verifies whether whitelisted users can sign in to Entrust CloudControl using local authentication.

1. Sign in as user **etccadmin** to the Entrust CloudControl URL. The user **etccadmin** is a domain user whitelisted in Enable external authentication in Entrust CloudControl to use Entrust IDaaS.



2. Select **Continue**. The **Password** field appears.
3. Enter the password and select **SIGN IN**.



CloudControl logs this user into the application without going to Entrust IDaaS.

Chapter 7. Additional resources and related products

7.1. CloudControl

7.2. Identity as Service

7.3. Entrust products

7.4. nShield product documentation