



ENTRUST

Entrust Identity as a Service and Entrust CloudControl

Integration Guide

18 May 2023

Contents

1. Introduction	3
1.1. Product configurations	3
1.2. Requirements	3
2. Register for Entrust iDaaS and configure Active Directory	4
2.1. Register for Entrust IDaaS	4
2.2. Configure your Active Directory	4
3. Download and configure Entrust CloudControl	6
3.1. Download the Entrust CloudControl software	6
3.2. Deploy an Entrust CloudControl VM from the OVA	6
3.3. Power the Entrust CloudControl virtual appliance	7
3.4. Configure the Entrust CloudControl virtual appliance	7
4. Download and configure Entrust iDaaS Active Directory	12
4.1. Download the Entrust IDaaS gateway	12
4.2. Deploy Entrust IDaaS gateway VM from the OVA	12
4.3. Configure the Entrust IDaaS gateway virtual appliance	13
4.4. Add the gateway to the Entrust IDaaS	14
4.5. Tie Active Directory to Entrust IDaaS	16
5. Create a generic web application	20
5.1. Create Entrust IDaaS application	20
5.2. Add a resource rule to the application	22
5.3. Enable external authentication in Entrust CloudControl to use Entrust IDaaS	24
6. Test integration	28
6.1. Test Entrust IDaaS authentication	28
6.2. Test whitelist authentication	31

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.

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.
etccuser	Entrust CloudControl user to be validated by Entrust IDaaS authentication.

User	Role
idaasaduser	Entrust IDaaS synchronization with your domain controller.

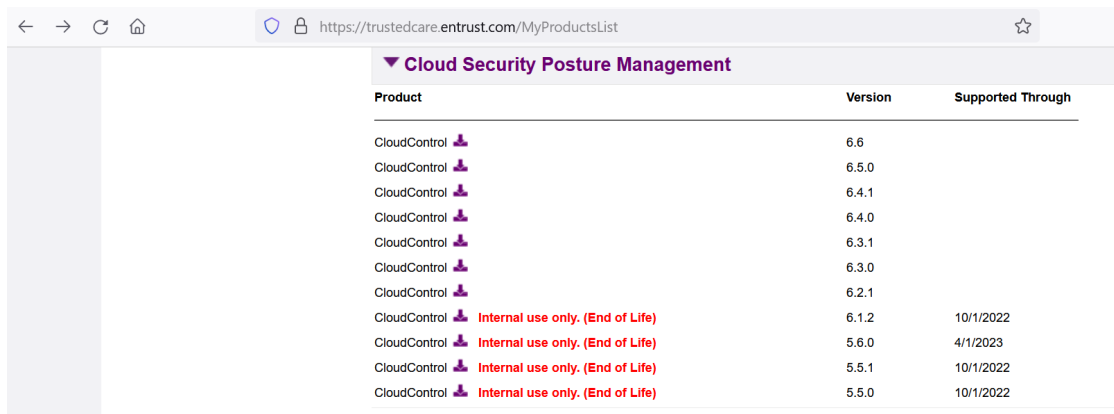
3. Create a group in Active Directory called **ASC_SuperAdmin**.
4. Make the **etccadmin** and **etccuser** users members of this group.

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 CloudControl 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.

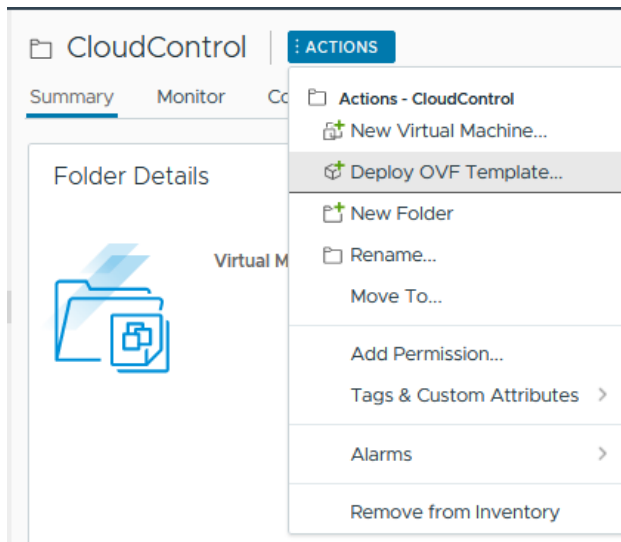


Product	Version	Supported Through
CloudControl	6.6	
CloudControl	6.5.0	
CloudControl	6.4.1	
CloudControl	6.4.0	
CloudControl	6.3.1	
CloudControl	6.3.0	
CloudControl	6.2.1	
CloudControl	6.1.2	10/1/2022
CloudControl	5.6.0	4/1/2023
CloudControl	5.5.1	10/1/2022
CloudControl	5.5.0	10/1/2022

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.



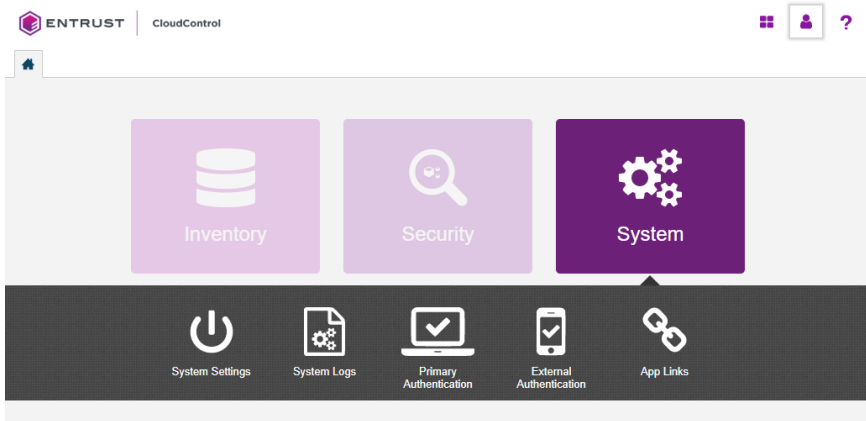
For more information refer to [Installing CloudControl from an OVA](#) in the online documentation.

3.3. Power the Entrust CloudControl 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.

Configure Active Directory



- 1: Details 2: Domain Controllers 3: Global Catalogs 4: ASC_SuperAdmin Role Mapping 5: Summary

Configuration Method

Automatic Manual

Add a default domain

★ Default Domain Name *

Root Domain Name *

Security

None SSL

Service Account

A service account used to integrate with Active Directory.

Account *

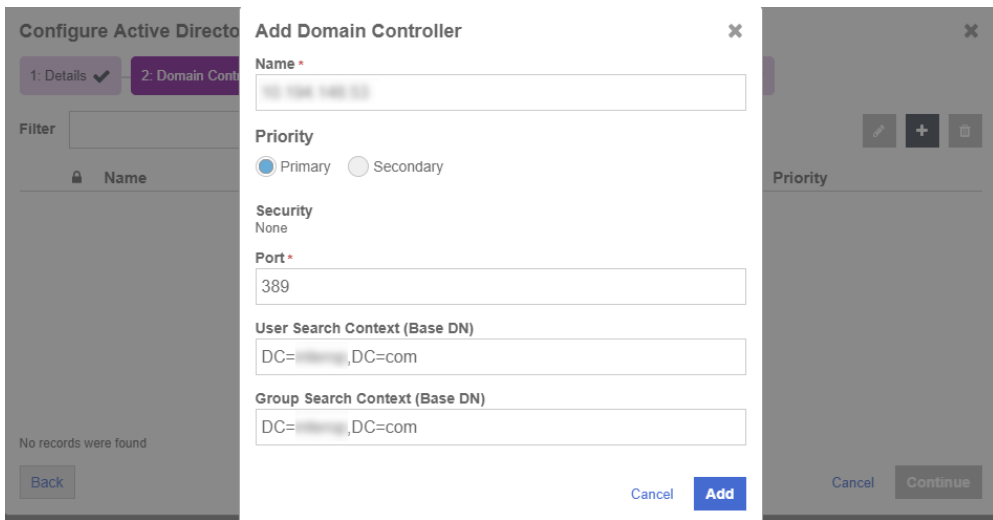
Password *

Cancel

Continue

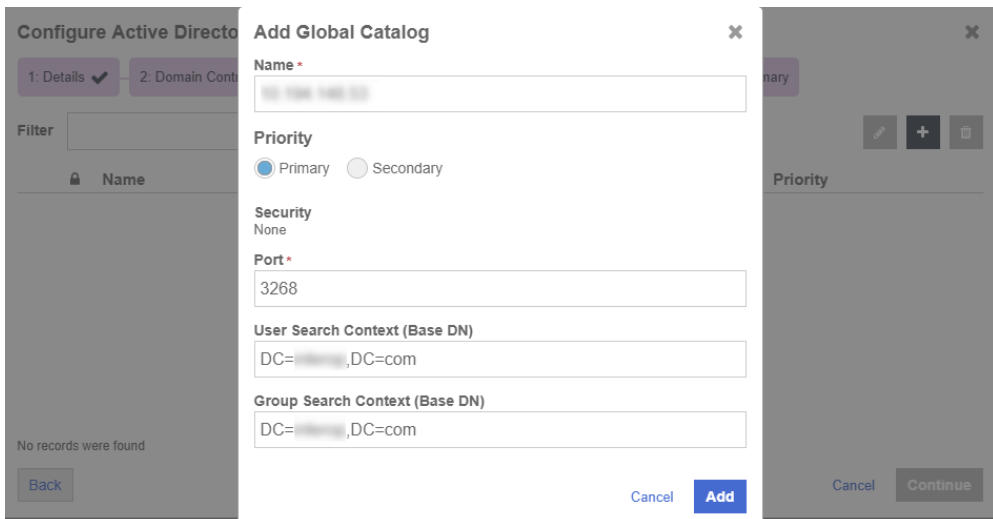
- In the **Domain Controllers** tab, select the **Add Domain Controller Now** link.
- In the **Add Domain Controller** window, enter the following information:

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



- Select **Add** and then **Continue**.
- In the **Add Additional Domains** window, select **Skip**.
- In the **ASC_SuperAdmin Role Mapping** tab, enter the Active Directory group created in [Configure your Active Directory](#).

Configure Active Directory interop.com ✕

1: Details ✓ 2: Domain Controllers ✓ 3: Global Catalogs ✓ 4: **ASC_SuperAdmin Role Mapping** 5: Summary

ASC_SuperAdmin Role Mapping
Enter the domain and group name that you want to map to the ASC_SuperAdmin role.

⚠ The Active Directory group selected below will be added to an Access Control rule for the ASC_SuperAdmin role. This rule will be added to the clone of the existing Access Control Trust Manifest assigned to the ROOT of the appliance.

Role: ASC_SuperAdmin

Domain: interop.com

Group Name: ASC_SuperAdmin ✕

Back Cancel Continue

- Select **Continue**.

The summary window displays the details.

Configure Active Directory interop.com ✕

1: Details ✓ 2: Domain Controllers ✓ 3: Global Catalogs ✓ 4: ASC_SuperAdmin Role Mapping ✓ 5: **Summary**

When you click 'Apply', CloudControl will convert to using the new root domain. **Therefore, this session will be terminated and you will need to log in using your Active Directory credentials.**

Summary

Service Account: interop\ServiceAccount
 Root Domain: interop.com
 Default Domain: ★ interop.com
 Domain Controllers: interop.com
 Global Catalogs: interop.com

Role-Group Mapping	Role	Group Name
	ASC_SuperAdmin	ASC_SuperAdmin@interop.com

Back Cancel Apply

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

4. Download and configure Entrust iDaaS Active Directory

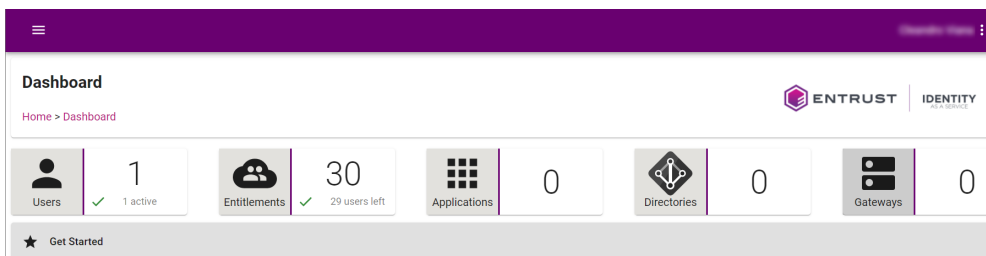
Configure Entrust IDaaS to use the same Active Directory services as Entrust CloudControl. Entrust provides an Entrust IDaaS gateway OVA to sync your on-premises Active Directory users to Entrust iDaaS. Changes made to your Active Directory are automatically synced with Entrust IDaaS through this gateway.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

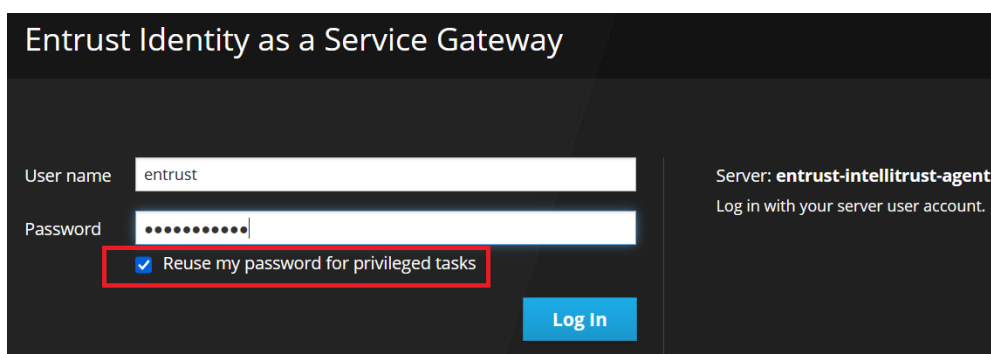
5. Follow the instructions during the deployment as needed.
6. After the VM is created, right-click the Entrust IDaaS gateway virtual machine and select **Power > Power On**.
7. Select **LAUNCH WEB CONSOLE** and make a note of the dynamic IP of the Entrust IDaaS gateway virtual machine. You will be able 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**.



Entrust Identity as a Service Gateway

User name:

Password:

Reuse my password for privileged tasks

Server: **entrust-intellitrust-agent**
Log in with your server user account.

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.

Waiting for Gateway to establish connection



Enter this information when prompted by the Gateway installer.


The registration code will expire in 24 hours.

This dialog will automatically close when the Gateway has registered.

Web Registration (5.5 or later)

Legacy (5.4.1 or earlier)

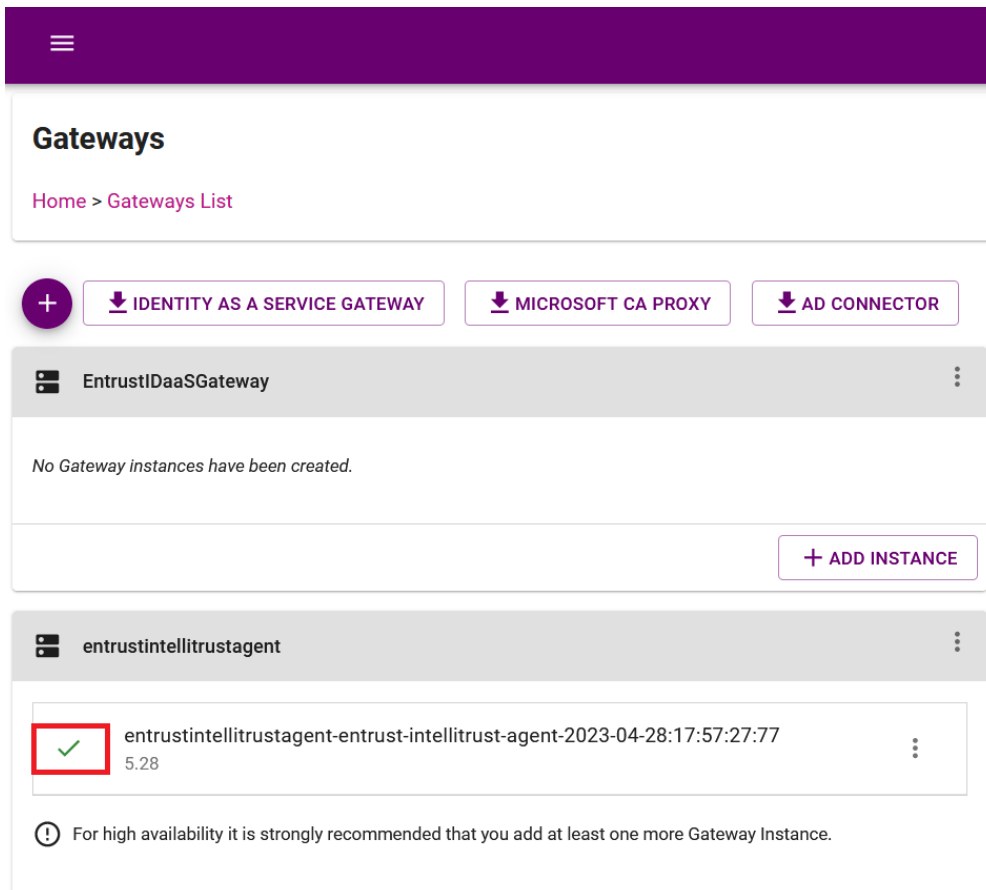
Registration Code

eyJpZCI6IjBmNGQ4Njc4LTlzMzYwITN [blurred] 

CLOSE

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.

Gateway Instance Details

Name: entrustintellitrustagent-entrust-intellitrust-agent-2023-04-28:17:57:27:77

Version: 5.28

State: Active

SSL Hostname: entrust-intellitrust-agent

Agents

✓	Directory Sync Last Heartbeat: 28 Apr 2023 14:29:35	■
✓	IdentityGuard Last Heartbeat: 28 Apr 2023 14:29:35	■
✓	Management Last Heartbeat: 28 Apr 2023 14:29:35	
✓	Password / Microsoft CA Gateway Last Heartbeat: 28 Apr 2023 14:29:40 Last Heartbeat from CA Gateway: 28 Apr 2023 14:29:41	■
✓	RADIUS Last Heartbeat: 28 Apr 2023 14:29:35	■
✓	SIEM Last Heartbeat: 28 Apr 2023 14:29:35	■

CLOSE

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 Configure your Active Directory)
Password	Password for idaasaduser
Directory Servers	IP/FQDN of the Active Directory server

Connection Settings

Directory Name *

Username *

Password 👁

Directory Servers ? ADD

📄 🔒 🗑

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)

SearchBases & Group Filters

Root Domain Naming Context *

SearchBases ? ADD

No SearchBases defined. The Root DN will be searched.

Group Filters ? ADD

🗑

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.

Synchronization

Synchronization Agent
entrustintellitrustagent

Page Size *
100

Crawl Frequency *
1 hr

User Object Class *
user

User Unique Id Attribute

Group Object Class *
group

Group Synchronization *
All Groups

Group Name Attribute *
sAMAccountName

User Desynchronization Policy *
User becomes a local Identity as a Service user and is disabled

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

Directories

Home > Directories List

ENTRUST | IDENTITY AS A SERVICE

Directories


Quick filter...

Conn...	Name ↑	Host Name	Type	Sync Status	Last Update	Actions
	...com	...	On-premise	Sync Complete	13 Apr 2022 15:27:54	↻ 👁 🗑










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 [Configure your Active Directory](#) appear in **Home > Users**.

Users List

Home > Users List

 Users List



<input type="checkbox"/>	State	User ID ↑	First Name	Last Name	Email	Source	Last Authenticatio...	Actions
<input type="checkbox"/>						Local	13 Apr 2022 15:31:11	  
<input type="checkbox"/>		etccadmin	etccadmin			Directory	Never	  
<input type="checkbox"/>		etccuser	etccuser			Directory	Never	  

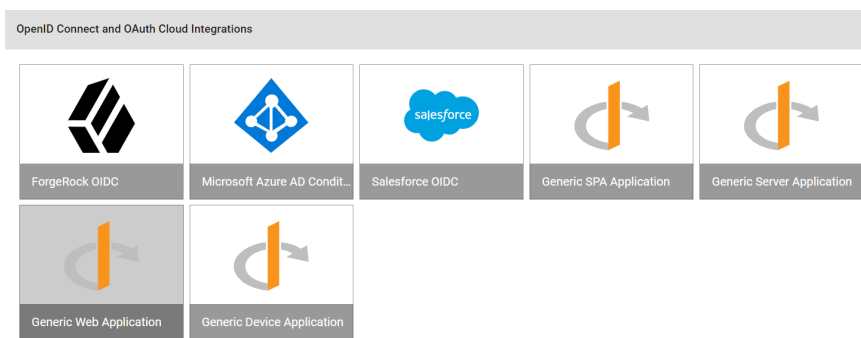
5. Create a generic web application

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.

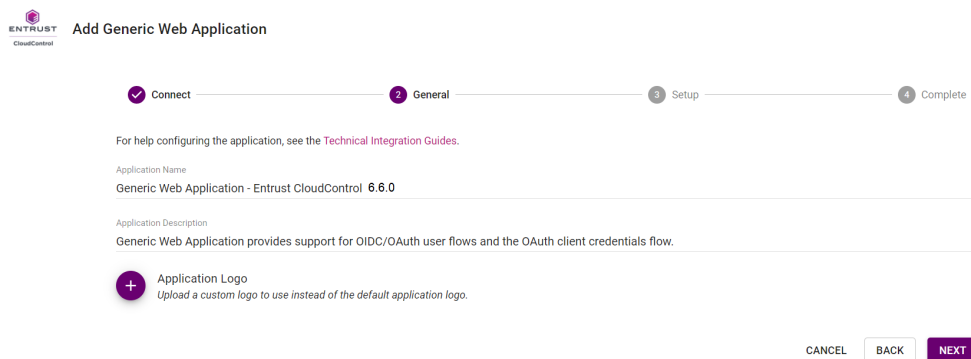
1. [Create Entrust IDaaS application](#)
2. [Add a resource rule to the application](#)
3. [Enable external authentication in Entrust CloudControl to use Entrust IDaaS](#)

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 paskey 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:

General Settings

Application Type
Web Application

Client ID
df6b805f-...
Copy the Client ID into your **Generic Web Application -CloudControl 6.6.0** application settings.

Client Secret *
.....

Token / Revocation Endpoint Client Authentication Method
Client Secret Post

Subject ID Attribute *
User Principal Name

Initiate Login URI (Optional)

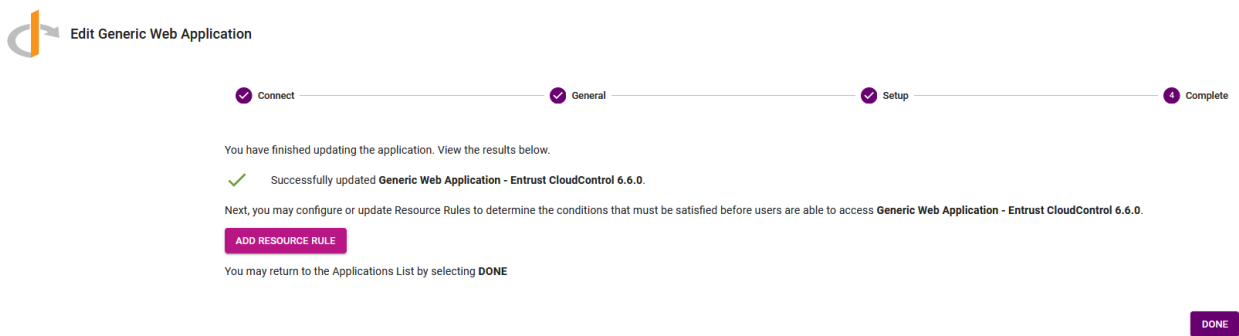
Login Redirect URI(s) *	ADD
https://entrust-cloudcontrol-660. com/asc/api/rest/v1/login	🗑️
Logout Redirect URI(s)	ADD
https://entrust-cloudcontrol-660. com/asc/api/rest/v1/sso/logout	🗑️

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.

Identity as a Service Portal Applications	OpenID Connect and OAuth Cloud Integrations
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  Administration Portal + </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ✓ Administration Portal - Administrators <small>Enables users with the appropriate role to authenticate to the Administr...</small> 📄 </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  User Portal + </div> <div style="border: 1px solid #ccc; padding: 5px;"> ✓ User Portal - All Users <small>Enables valid users to authenticate to the User Portal</small> 📄 </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  Generic Web Application - Entrust CloudControl + </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ✓ Generic Web Application - Entrust CloudControl ■ ⋮ </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">  Generic Web Application - Entrust CloudControl 6.6.0 + </div> <div style="border: 1px solid #ccc; padding: 5px;"> ⚠ No Resource Rule configured </div>

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 [Configure your Active Directory](#).

1 General Settings
2 Authentication Conditions

Name *

Generic Web Application - Entrust CloudControl 6.6.0

Description

Select Group to add

ASC_SuperAdmin × ▾

ASC_SuperAdmin ✕ Remove all

CANCEL
NEXT

5. In the **Authentication Conditions** page:
- Select **Password** from the **First Factor** pull-down menu.
 - 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

Second Factors - Drag and drop in order of preference

- One Time Password
- Entrust Soft Token Push
- Passkey/FIDO2
- Software / Hardware Token
- Grid Card
- Knowledge-based Authenticator
- Temporary Access Code

CANCEL BACK SUBMIT

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

Resource Rules ENTRUST IDENTITY AS A SERVICE

[Home > Resource Rules List](#)

Identity as a Service Portal Applications

- Administration Portal +
- Administration Portal - Administrators
Enables users with the appropriate role to authenticate to the Administr...
- User Portal +
- User Portal - All Users
Enables valid users to authenticate to the User Portal

OpenID Connect and OAuth Cloud Integrations

- Generic Web Application - Entrust CloudControl +
- Generic Web Application - Entrust CloudControl ■ ⋮
- Generic Web Application - Entrust CloudControl 6.6.0 +
- Generic Web Application - Entrust CloudControl 6.6.0 ■ ⋮

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**.

ENTRUST CloudControl ☰ 👤 ?

Inventory

Security

System

System Settings

System Logs

Primary Authentication

External Authentication

App Links

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 <code>api/oidc</code> .
Name	Enter a name.

For example:

External Authentication DISABLED

Configuration Whitelist

Configuration

Choose an authentication type to configure. To change an authentication type, external authentication must be disabled.

Authentication Type *

OpenID Connect

Configure CloudControl as an application in the OIDC provider. Within that application you will find the Client ID and Client Secret.

Client ID *

df6b805f-...

Client Secret *

.....

Base URL *

https://url.com/tenentid=xxxxx

ex. https://url.com/tenentid=xxxxx

Name

Entrust IDaaS 5.28

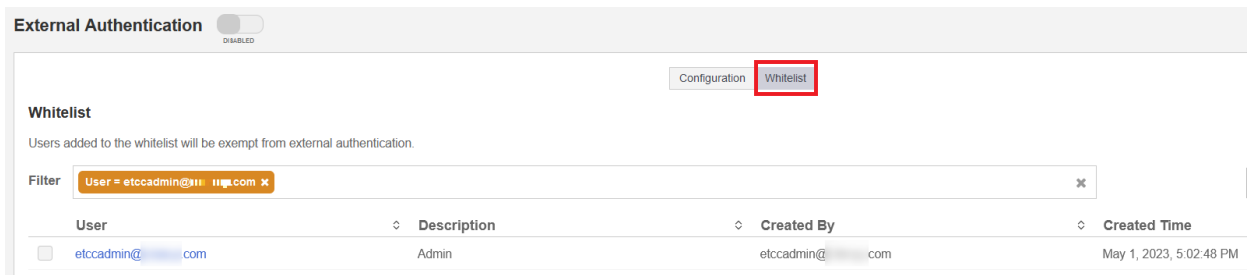
Name to identify this configuration throughout CloudControl

Enable

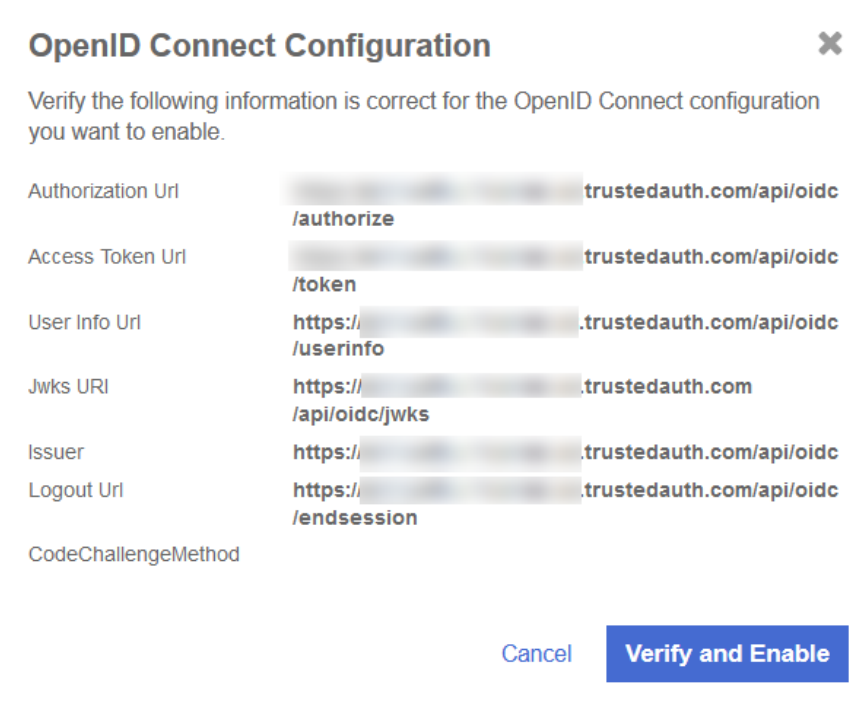
4. In the **External Authentication** tab, select **Whitelist**, and enter the **etccadmin** user created in [Configure your Active Directory](#). This user would be able to sign in without Entrust IDaaS authentication in the event of a configuration issue. Then select **Enable**.



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.

External Authentication



To change or edit authentication, external authentication must be disabled.

Authentication Type

OpenID Connect

Client ID

df6b805f-

Client Secret

Base URL

https://trustedauth.com/api/oidc

Name

Entrust IDaaS 5.28

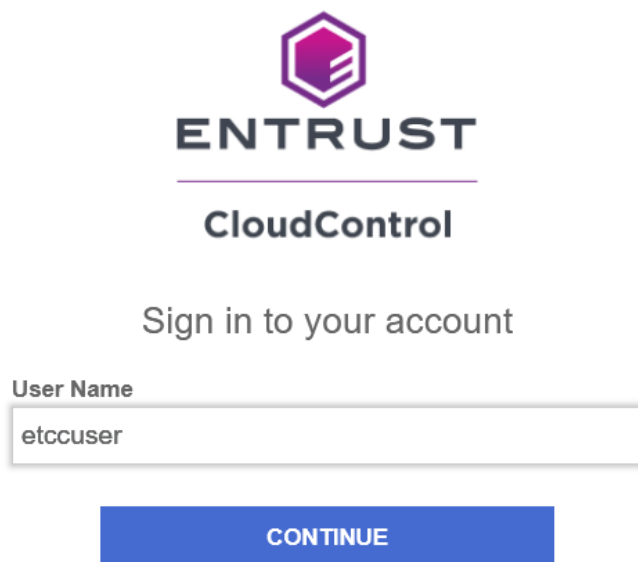
6. Test integration


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](#).




ENTRUST
CloudControl

Sign in to your account

User Name
etccuser

CONTINUE

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




ENTRUST

IDENTITY
AS A SERVICE

Login to access Entrust.

Enter User ID

 Click **GO BACK** to return to **Generic Web Application - Entrust CloudControl 6.6.0.**

Or

 Passkey

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



ENTRUST

IDENTITY
AS A SERVICE

Welcome

 etccuser

Enter your password

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



ENTRUST

IDENTITY
AS A SERVICE

Welcome

 etccuser

Enter the one-time password that was just sent to you.

Enter OTP

[Resend OTP using Email](#)

Remember Me

CANCEL

LOGIN

6. Select **Accept**.

Generic Web Application - Entrust CloudControl 6.6.0



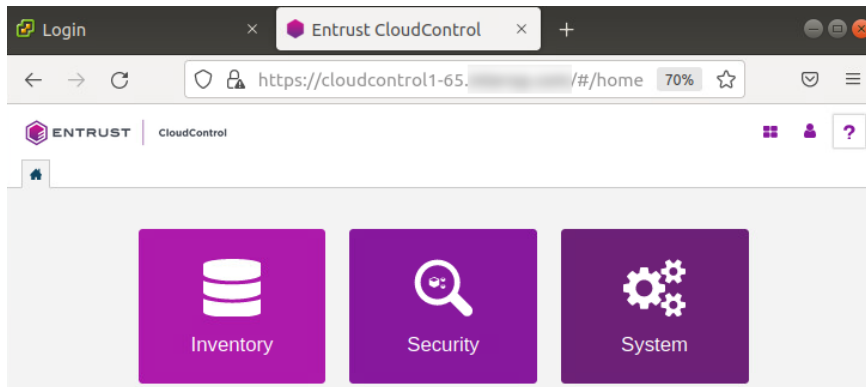
Authorize application **Generic Web Application - Entrust CloudControl 6.6.0** to access the following information from your **etccuser** account:

 Your unique identifier

CANCEL

ACCEPT

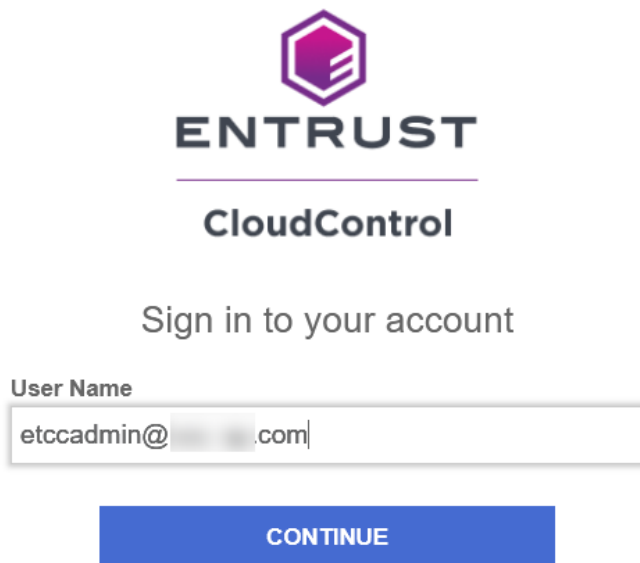
Entrust IDaaS authenticates the user and redirects you back to the CloudControl home screen.




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](#).




ENTRUST
CloudControl

Sign in to your account

User Name

CONTINUE

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



Sign in to your account

User Name

etccadmin@.com

Password

SIGN IN

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