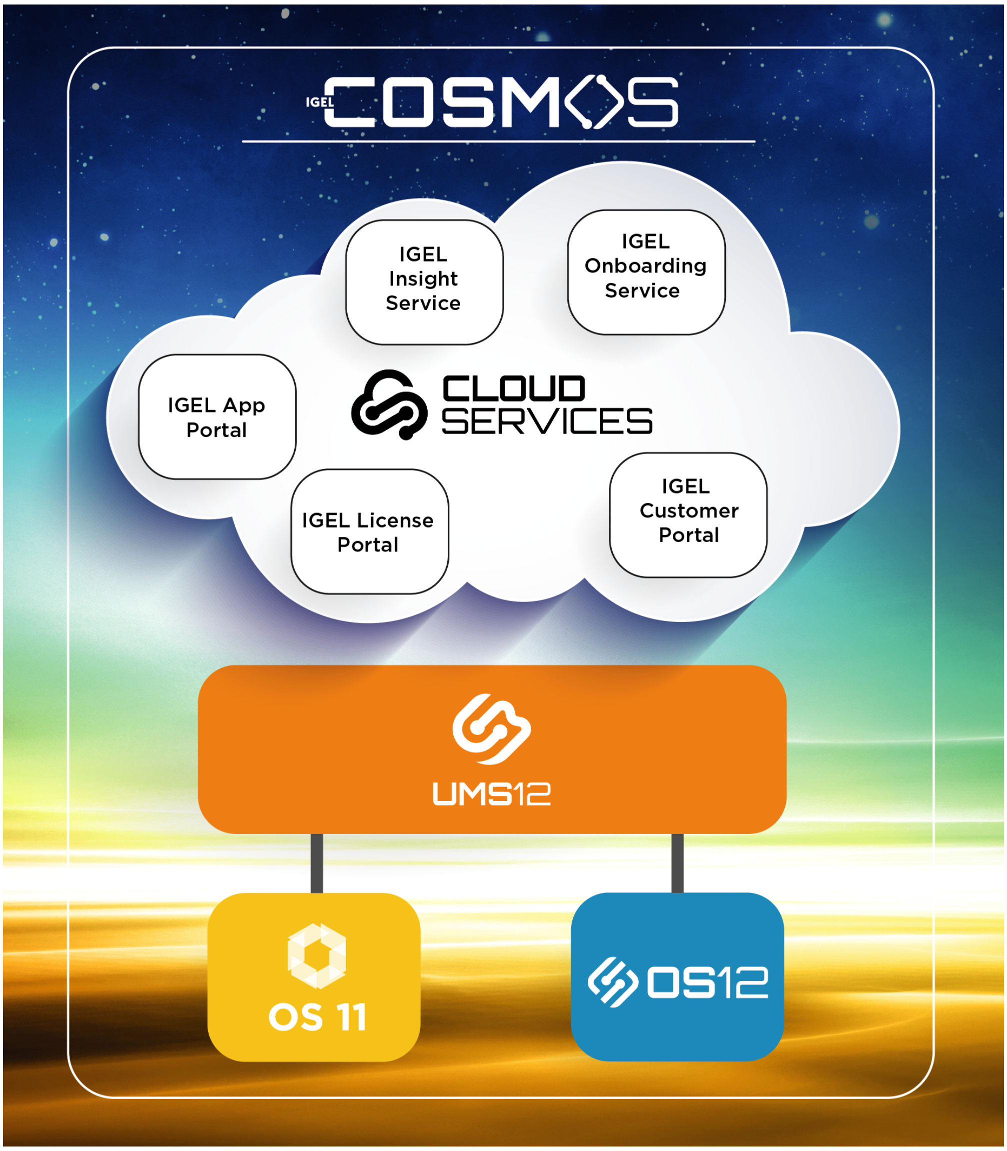
How to Start with IGEL COSMOS

IGEL COSMOS is an End User Computing platform that includes IGEL's endpoint operating system, management software for the secure remote administration of your endpoint devices, and cloud services.

Released with IGEL COSMOS, the operating system IGEL OS 12 fully separates the IGEL OS base system and IGEL OS Apps. With this modular principle, you can install and update single applications like Citrix, Chromium browser, etc. individually and independently from the IGEL OS base system and have maximum flexibility.



IGEL COSMOS comprises:

- IGEL Universal Management Suite (UMS) 12 for managing IGEL OS 12 and IGEL OS 11 devices. IGEL UMS 12 is a prerequisite for accessing all IGEL COSMOS Cloud Services.
- IGEL OS
- Various cloud-based services, for example:

- IGEL Customer Portal(see page 4) which is a doorway to the IGEL product-related services. Here, you register your company account and use it to invite other users and assign them specific roles(see page 9), e.g. for opening support cases. In the IGEL Customer Portal, you can also raise and view support requests, make necessary configurations for IGEL Onboarding Service, etc.
- IGEL App Portal(see page 103) where you can find all applications currently available for IGEL OS 12
- IGEL Onboarding Service(see page 41) which, if configured, allows your users to easily onboard IGEL OS 12 devices using only their corporate email
- IGEL Insight Service(see page 198) which collects analytical and usage data to improve IGEL products and services and provide a better customer experience
- IGEL License Portal(see page 151) where you can manage licenses for your IGEL OS devices

ⓘ For more information on IGEL COSMOS, you can also use IGEL Academy courses, e.g. Introducing IGEL COSMOS[1], and IGEL Community[2].
You may find it also useful to view https://igel-community.github.io/IGEL-Docs-v02/Docs/HOWTO-COSMOS/ and https://igel-community.github.io/IGEL-Docs-v02/Docs/Cheatsheet-IGELCommunity/.

In the following, you will find the overview of the first steps with IGEL COSMOS, IGEL OS 12 and UMS 12. Please read this guide fully, without skipping any steps:

- Registering for the IGEL Customer Portal(see page 4)
- Managing Users and Roles in the IGEL Customer Portal(see page 9)
- Installing / Upgrading to IGEL UMS 12(see page 32)
- Registering the UMS(see page 36)
- Initial Configuration of the IGEL Onboarding Service (OBS)(see page 41)
- IGEL App Portal(see page 103)
- IGEL UMS 12: Basic Configuration(see page 107)
- IGEL UMS 12: App Update(see page 127)
- Installing the Base System via IGEL OS Creator (OSC)(see page 137)
- Licensing(see page 151)
- Onboarding IGEL OS 12 Devices(see page 158)
- Installing IGEL OS Apps Locally on the Device(see page 190)
- Configuring Single Sign-On (SSO)(see page 195)
- IGEL OS Notification Center(see page 196)
- IGEL Insight Service(see page 198)
- Debugging / How to Collect and Send Device Log Files to IGEL Support(see page 200)

[1] https://learn.igel.com/learn/course/150/
[2] https://videos.igelcommunity.com/

Registering for the IGEL Customer Portal

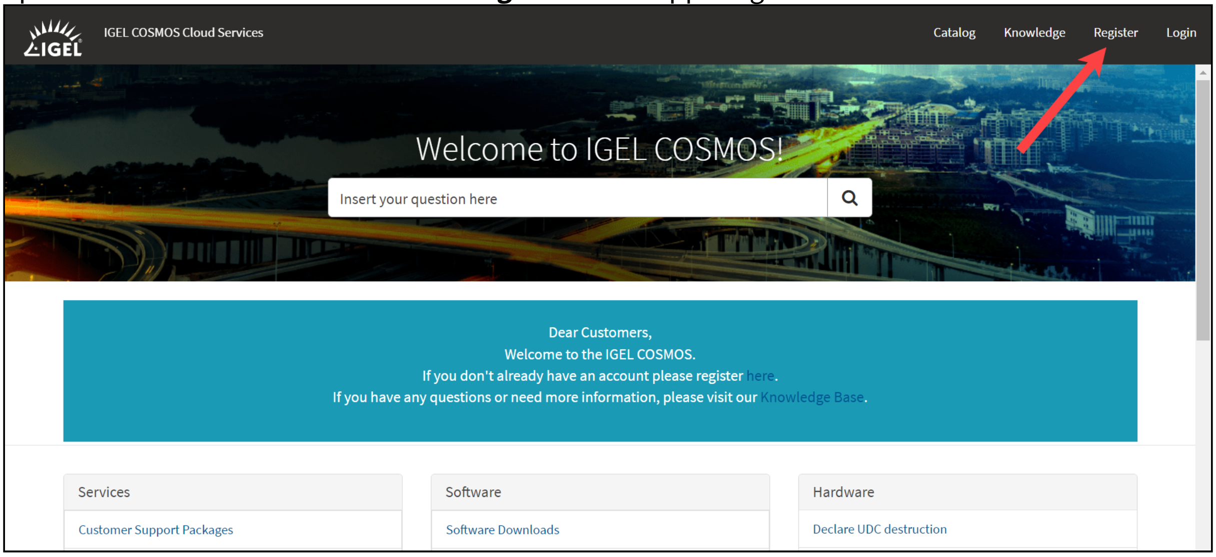
IGEL Customer Portal is the doorway to IGEL product-related services. Registering here your company account is the first step to start using IGEL products.

Registration to the IGEL Customer Portal

> ⓘ As a result of our continued commitment to provide the best COSMOS customer experience, we have temporarily turned off SSO Login while our internal teams work to implement a new product to achieve the next-level experience.
> All users will need to use a username (email address) and password to access the IGEL Customer Portal.

To register for the IGEL Customer Portal:

1. Open IGEL Customer Portal[3] and click **Register** in the upper right corner of the menu bar:

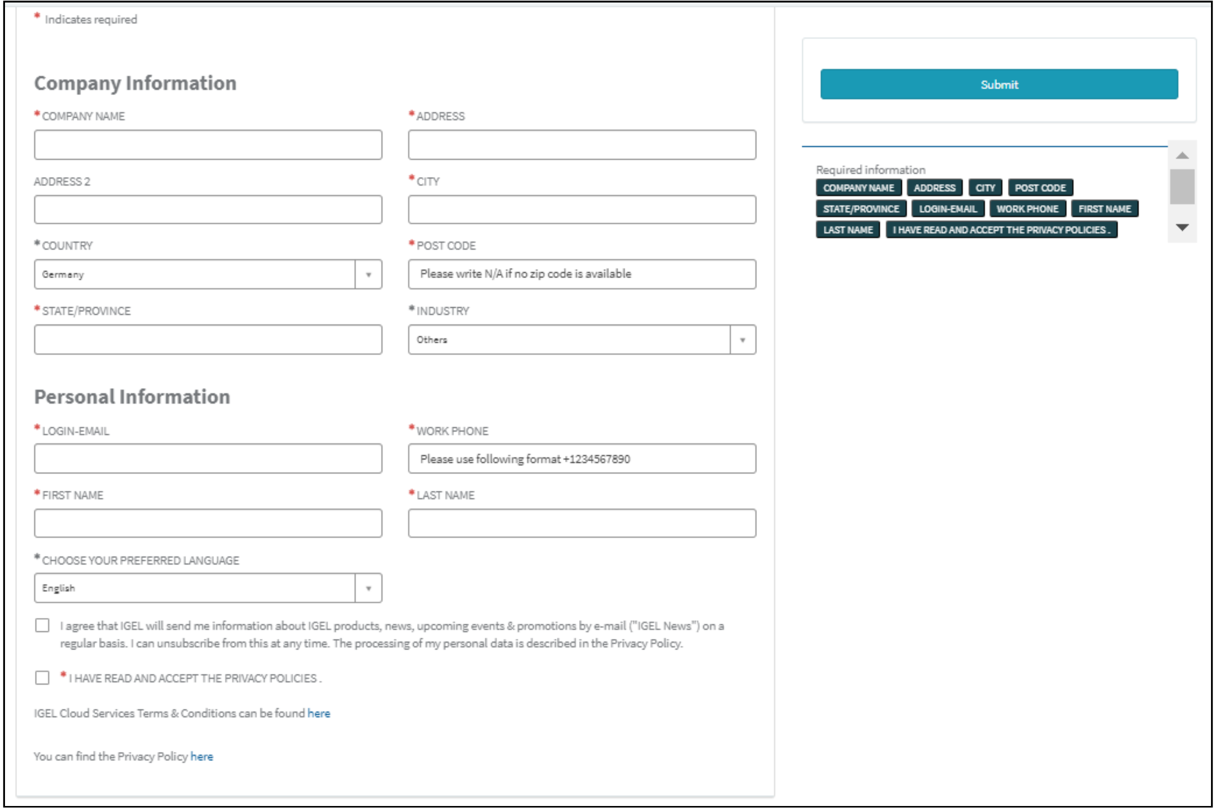


Dear Customers,
Welcome to the IGEL COSMOS.
If you don't already have an account please register here.
If you have any questions or need more information, please visit our Knowledge Base.

The **IGEL Customer & Account Registration** form will open.

[3] https://cosmos.igel.com/

2. Enter your user data:



* Indicates required

Company Information

*COMPANY NAME	*ADDRESS
ADDRESS 2	*CITY
*COUNTRY: Germany	*POST CODE: Please write N/A if no zip code is available
*STATE/PROVINCE	*INDUSTRY: Others

Personal Information

*LOGIN-EMAIL	*WORK PHONE: Please use following format +1234567890
*FIRST NAME	*LAST NAME
*CHOOSE YOUR PREFERRED LANGUAGE: English	

□ I agree that IGEL will send me information about IGEL products, news, upcoming events & promotions by e-mail ("IGEL News") on a regular basis. I can unsubscribe from this at any time. The processing of my personal data is described in the Privacy Policy.

□ * I HAVE READ AND ACCEPT THE PRIVACY POLICIES .

IGEL Cloud Services Terms & Conditions can be found here

You can find the Privacy Policy here

Required information

COMPANY NAME, ADDRESS, CITY, POST CODE, STATE/PROVINCE, LOGIN-EMAIL, WORK PHONE, FIRST NAME, LAST NAME, I HAVE READ AND ACCEPT THE PRIVACY POLICIES .

Required information is marked with an asterisk (*) and is displayed in the right pane at the same time.

When you have entered all the information, you will no longer see a reference to the information needed in the right pane.

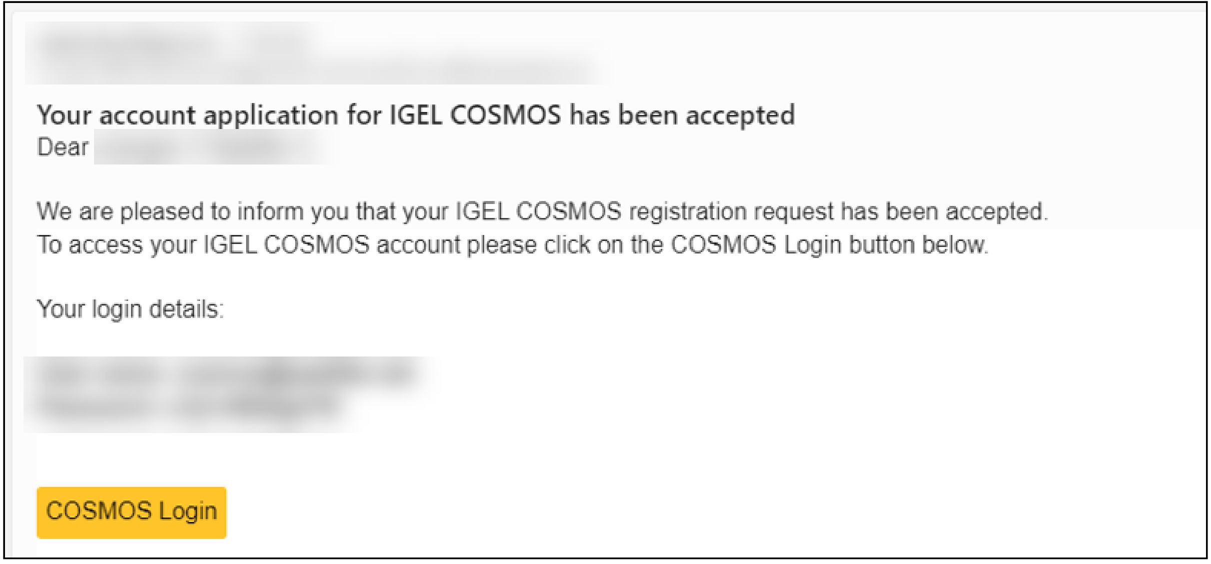
> ⓘ **IGEL Company Account Requirements**
> - Your name and email address
> - Must be a business email address with your company domain
> - No personal email addresses (solely B2B)
> - No generic contact details or email addresses, e.g. (info@company.tld)
> - No shared (multi-user) accounts (e.g. support-team@company.tld)
> - Free email provider domains are not allowed (e.g. gmail.com, yahoo.com, etc.)

3. Click **Submit**.
   A confirmation email will be sent to you.

4. Check your mailbox and confirm your registration by clicking on the appropriate link. If you have not received the email, please check your spam folder.
   Your user data will now be internally checked. You will receive an email confirmation when your registration has been approved containing your username and one-time password. As soon as you log in for the first time, you will be prompted to change your password. The registration approval

process usually takes no more than 24 hours.

Example:



[redacted]

Your account application for IGEL COSMOS has been accepted
Dear [redacted]

We are pleased to inform you that your IGEL COSMOS registration request has been accepted.
To access your IGEL COSMOS account please click on the COSMOS Login button below.

Your login details:

[redacted]

5. To log in to the IGEL Customer Portal, click the button **COSMOS Login** in the received email.

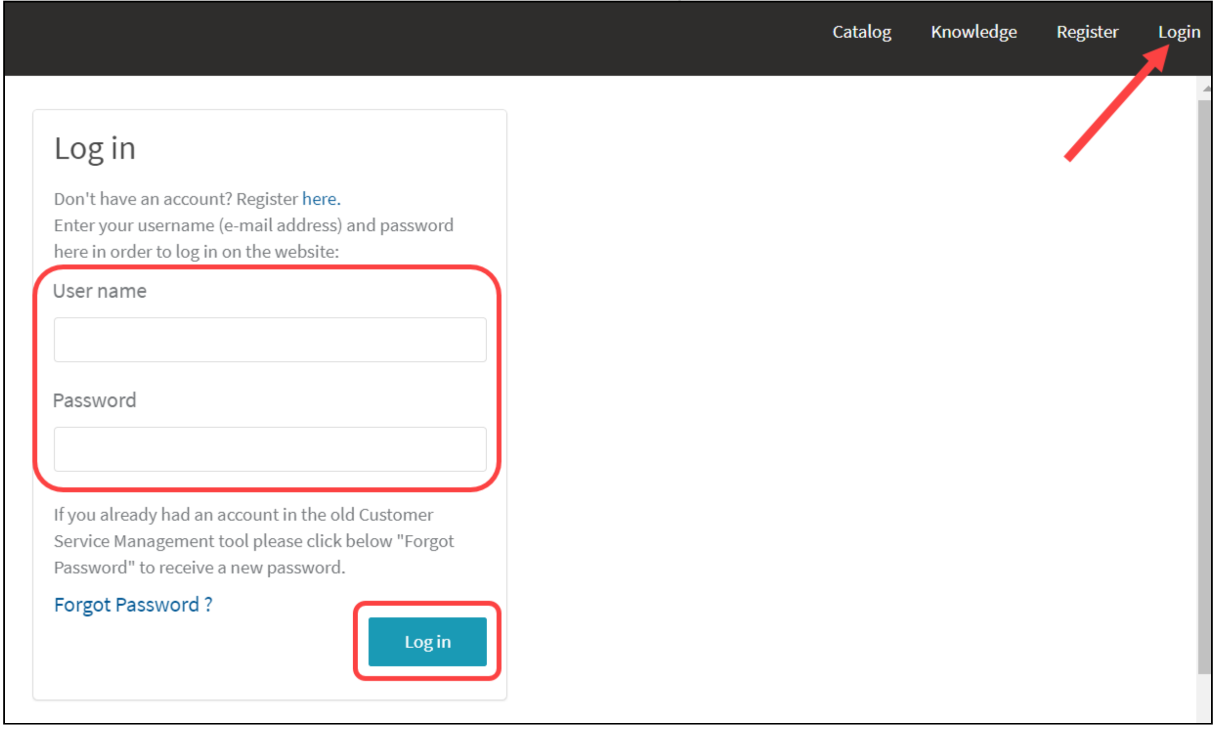
> ⚠ Please remember your login email. It will be used as Super Admin credentials, with which you can later invite new users and assign them specific roles, see Managing Users and Roles in the IGEL Customer Portal(see page 9).

Logging In to the IGEL Customer Portal

1. Open the IGEL Customer Portal[4] and click **Login**.

[4] https://cosmos.igel.com/

2. Enter the **user name** and **password** that you used to register with IGEL and click **Log in**.



Log in

Don't have an account? Register here.
Enter your username (e-mail address) and password here in order to log in on the website:

User name

Password

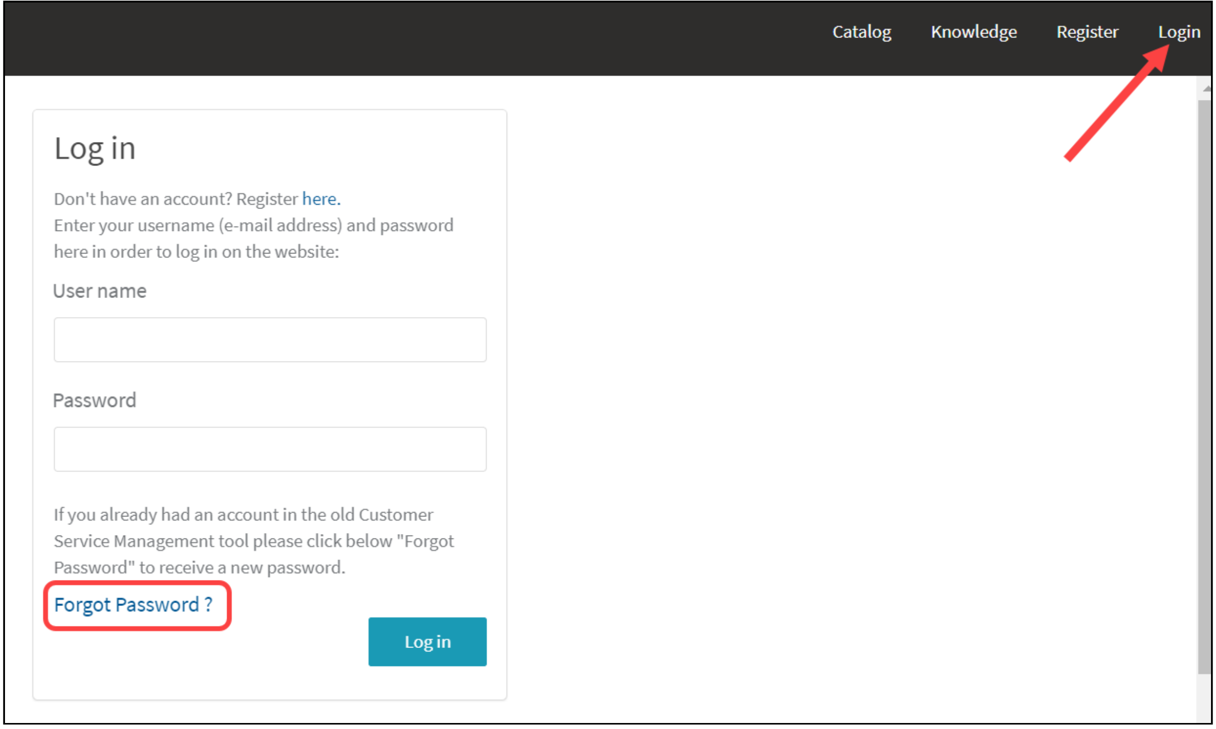
If you already had an account in the old Customer Service Management tool please click below "Forgot Password" to receive a new password.

Login Credentials Forgotten?

1. Open the IGEL Customer Portal[5] and click **Login**.

[5] https://cosmos.igel.com/

2. Click **Forgot Password?** to reset a password.



Log in

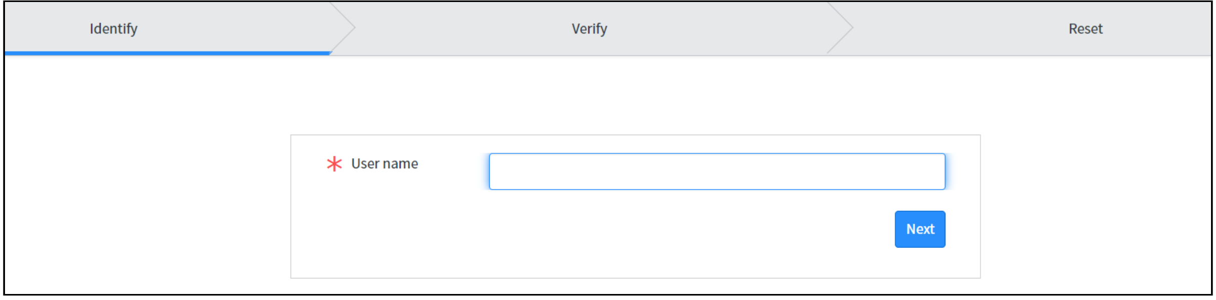
Don't have an account? Register here.
Enter your username (e-mail address) and password here in order to log in on the website:

User name

Password

If you already had an account in the old Customer Service Management tool please click below "Forgot Password" to receive a new password.

A dialog for requesting a new password will open:



The password change is done in three steps: **Identify**, **Verify**, **Reset**.

3. **Identify**: Enter your **user name** that you used to register with IGEL.

4. **Verify**: Enter your **email** address to which the verification email should be sent.

5. Check your email inbox and confirm it with the corresponding link. If you have not received the email, please check your spam folder.
The **Reset Password** dialog box will open in your default browser.

6. **Reset**: Set a new password following the displayed password rules and confirm by clicking **Reset Password**.
With the verified user data and the new password, you can now log in to the IGEL Customer Portal.

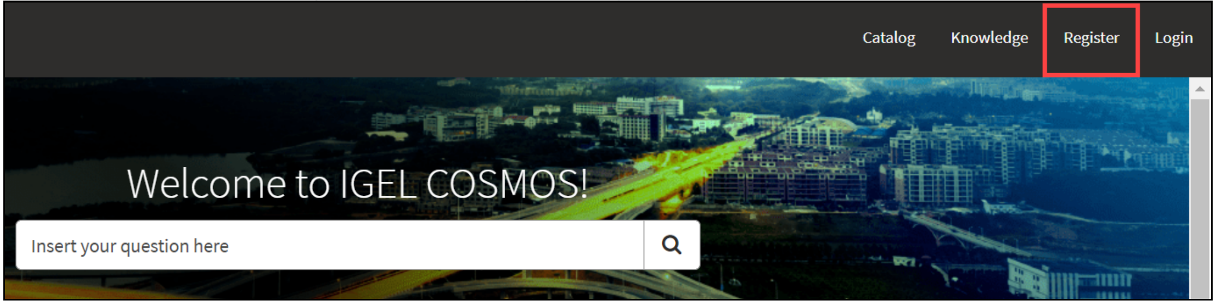
Managing Users and Roles in the IGEL Customer Portal

This article describes how to invite users, cancel or renew invitations, and add roles to a user or remove roles in the IGEL Customer Portal. Also included is a description of how to use Okta or Ping as federated identity providers (IdP) for logging in to your IGEL Cloud Services accounts.

Roles and Permissions

In the IGEL Customer Portal, you can find the following roles:

- Super Admin
  The first account you register in the IGEL Customer Portal[6] **> Register** is your Super Admin account. For details on registration, see Registering for the IGEL Customer Portal(see page 4).



  The Super Admin is the first user to register any new account.

- Account Admin
- OBS Admin
- UMS Admin
- Customer Support Account Manager

The users with these roles have the following permissions:

	Super Admin	**Account Admin**	**OBS Admin**	**UMS Admin**	**Customer Support Account Manager**
Account Management					
View account	✓	✓			
User Management					
View users	✓	✓			
Invite users	✓	✓			
Add / remove user roles	✓	✓			

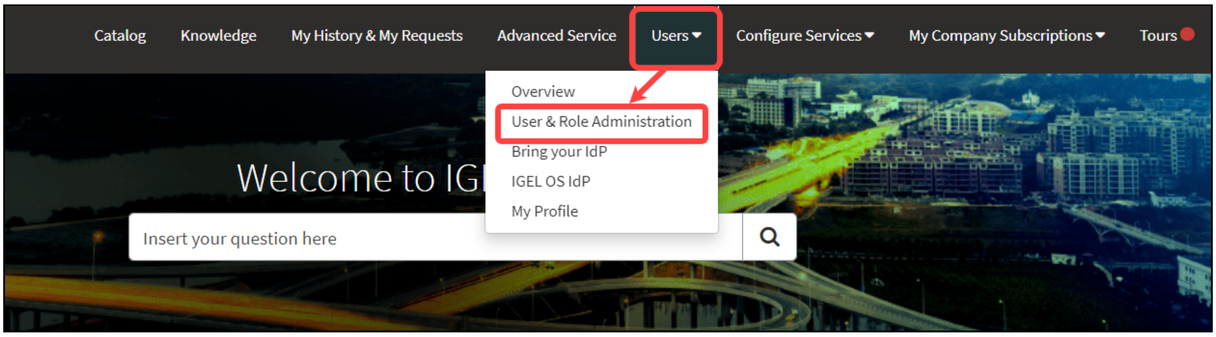
[6] https://cosmos.igel.com/

	Super Admin	Account Admin	OBS Admin	UMS Admin	Customer Support Account Manager
OBS IdP (Onboarding Service Identity Provider)					
Register IGEL OS IdP	✓		✓		
Use OBS instance	✓		✓		
IGEL OS Onboarding					
Register OBS instances	✓		✓		
View OBS attributes	✓		✓		
Use OBS attributes	✓		✓		
Create OBS attributes	✓		✓		
Add / change OBS attributes	✓		✓		
UMS Management					
View UMS instances	✓			✓	
Use UMS instances	✓			✓	
Create UMS instances	✓			✓	
Add / change UMS instances	✓			✓	
Support / Case Management					
View support cases	✓				✓
Submit support cases	✓				✓
View RMA cases	✓				✓
Submit an RMA case	✓				✓
Submit reset key cases	✓				✓
Submit license question cases	✓				✓

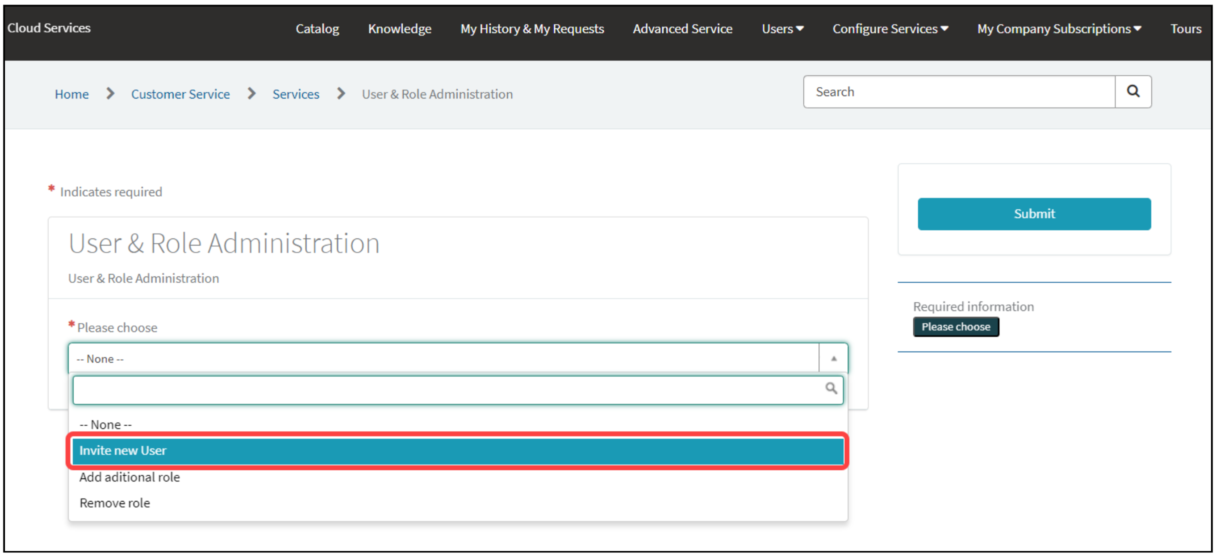
Inviting a User and Assigning a Role

In the following example, we will invite a new user and make this user an OBS administrator.

1. Open IGEL Customer Portal[7], log in to your admin account, and select **Users > User & Role Administration**.



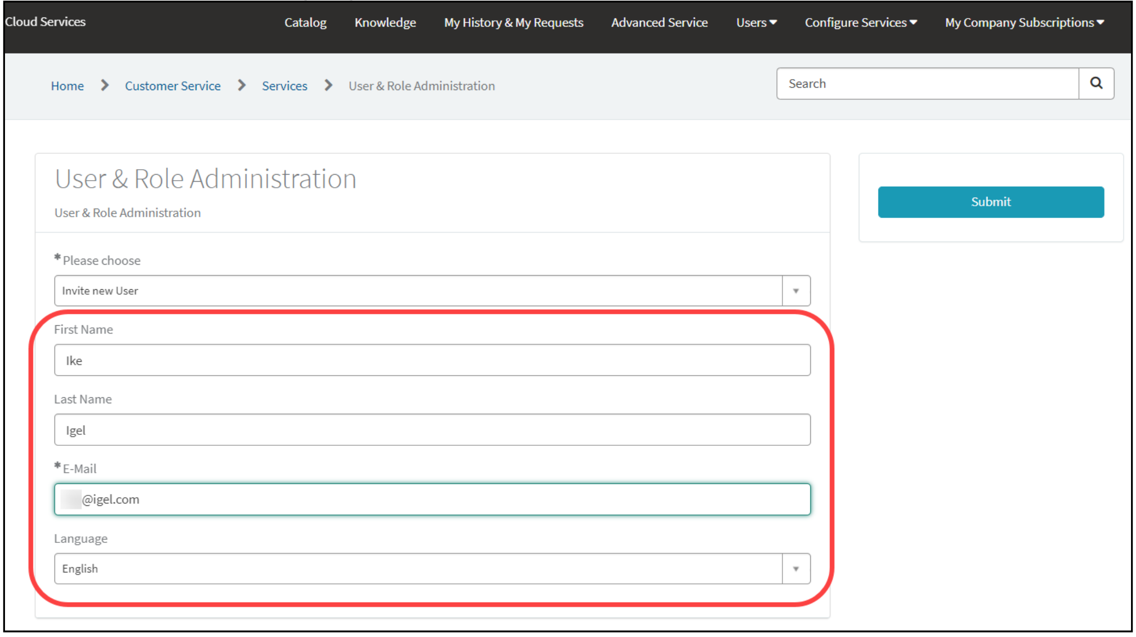
2. Select **Invite new user**.



3. Provide the data of the new user:
   - **First name**: First name of the user
   - **Last name**: Last name of the user
   - **E-mail** (required): E-mail address of the user

[7] https://cosmos.igel.com/

- **Language**: Preferred language for the user



User & Role Administration

User & Role Administration

*Please choose: Invite new User

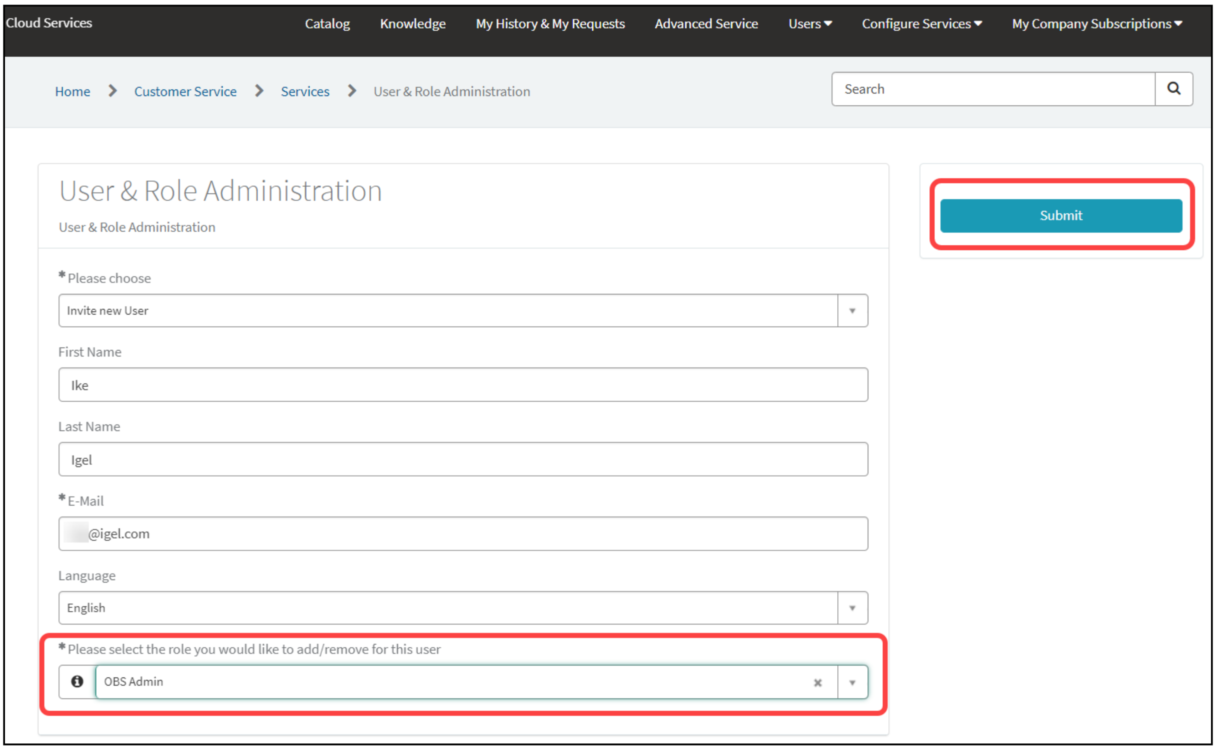
First Name: Ike

Last Name: Igel

*E-Mail: [redacted]@igel.com

Language: English

4. Select **OBS Admin** as the role and click **Submit**.



User & Role Administration

User & Role Administration

*Please choose: Invite new User

First Name: Ike

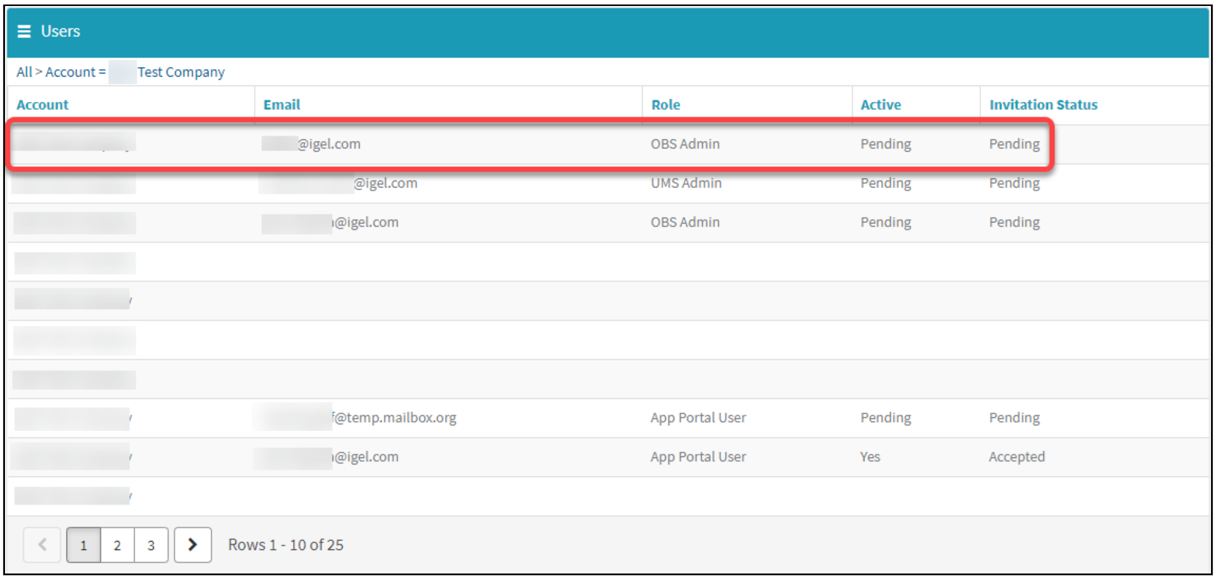
Last Name: Igel

*E-Mail: [redacted]@igel.com

Language: English

*Please select the role you would like to add/remove for this user: OBS Admin

The invitation mail is sent to the user.
The list of users is displayed; it includes the newly added user.



Account	Email	Role	Active	Invitation Status
[redacted]	[redacted]@igel.com	OBS Admin	Pending	Pending
[redacted]	[redacted]@igel.com	UMS Admin	Pending	Pending
[redacted]	[redacted]@igel.com	OBS Admin	Pending	Pending
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]	[redacted]@temp.mailbox.org	App Portal User	Pending	Pending
[redacted]	[redacted]@igel.com	App Portal User	Yes	Accepted
[redacted]				

When the user accepts the invitation, the account is created, and the role is assigned. (If the user declines, the account is not created.)
The Super Admin receives a confirmation e-mail.

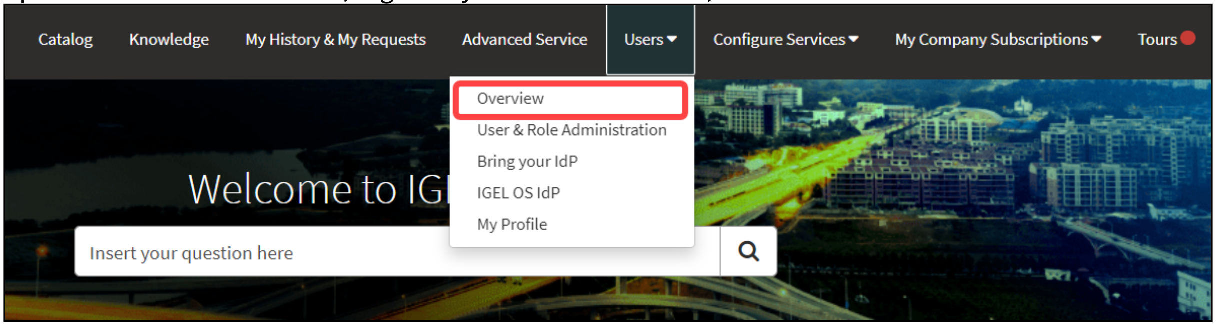
Canceling and Resending Invitations

You can cancel or resend pending invitations if you have one of the following roles:

- Super Admin
- Account Admin

> ⓘ Pending invitations older than 30 days will be deleted automatically. If an invitation has been deleted, you can create a new one.

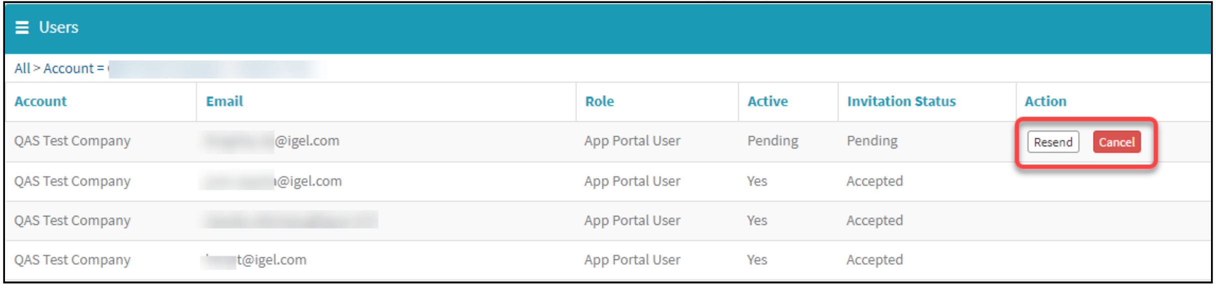
1. Open IGEL Customer Portal[8], log in to your admin account, and select **Users > Overview**.



The users are listed.

[8] https://cosmos.igel.com/

2. Find the relevant user and click on **Resend** or **Cancel**, as appropriate.



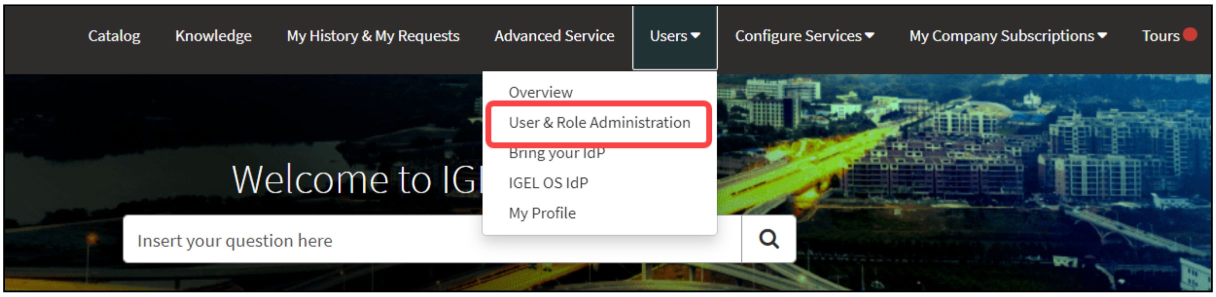
☰ Users

All > Account = [redacted]

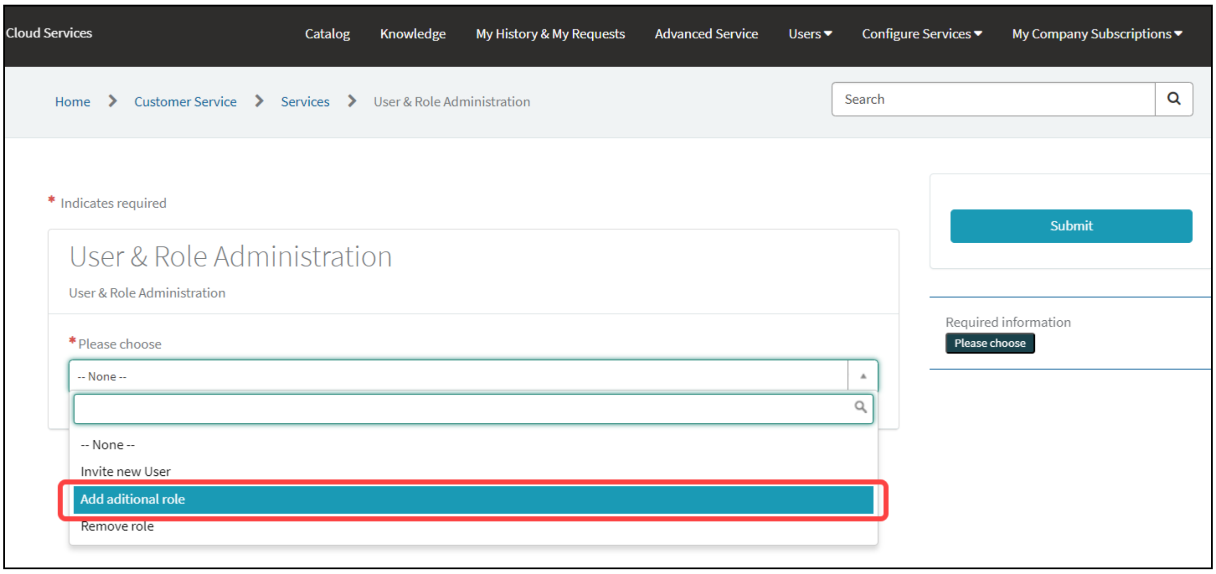
Account	Email	Role	Active	Invitation Status	Action
QAS Test Company	[redacted]@igel.com	App Portal User	Pending	Pending	Resend Cancel
QAS Test Company	[redacted]ı@igel.com	App Portal User	Yes	Accepted	
QAS Test Company	[redacted]	App Portal User	Yes	Accepted	
QAS Test Company	[redacted]t@igel.com	App Portal User	Yes	Accepted	

Adding a Role to an Existing User

1. Open IGEL Customer Portal[9], log in to your admin account, and select **Users > User & Role Administration**.

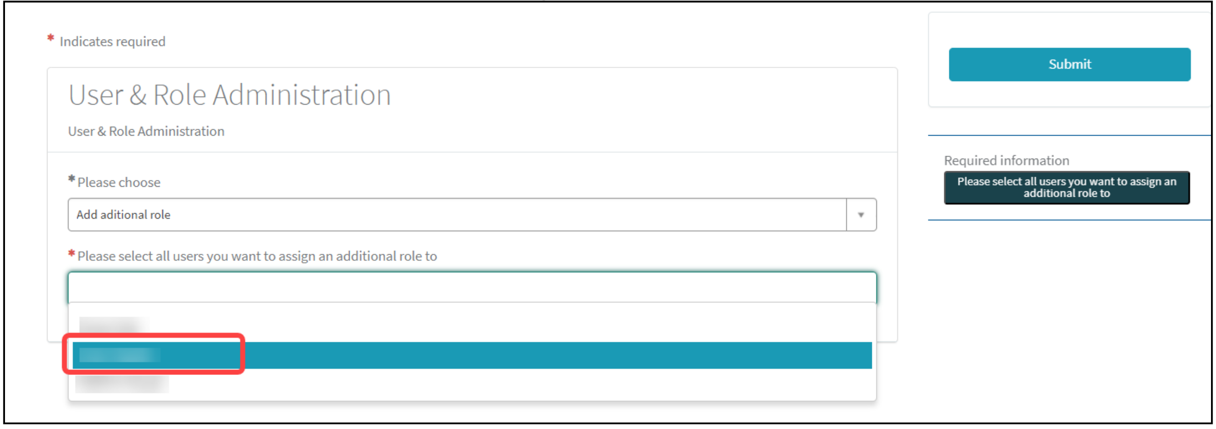


2. Select **Add additional role**.



[9] https://cosmos.igel.com/

3. Select one or more users that should be assigned the role.



* Indicates required

User & Role Administration

User & Role Administration

*Please choose

Add aditional role

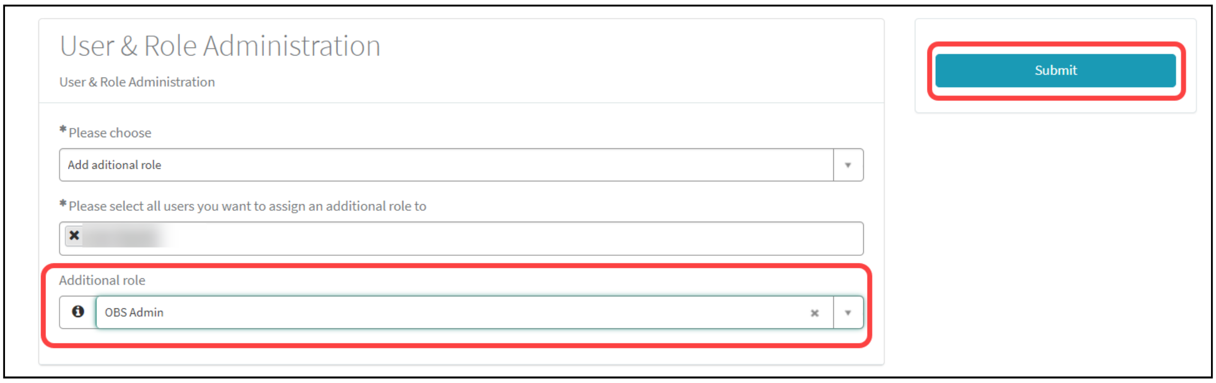
*Please select all users you want to assign an additional role to

[redacted]

Required information

Please select all users you want to assign an additional role to

4. Select **OBS Admin** as the additional role and click **Submit**.



User & Role Administration

User & Role Administration

*Please choose

Add aditional role

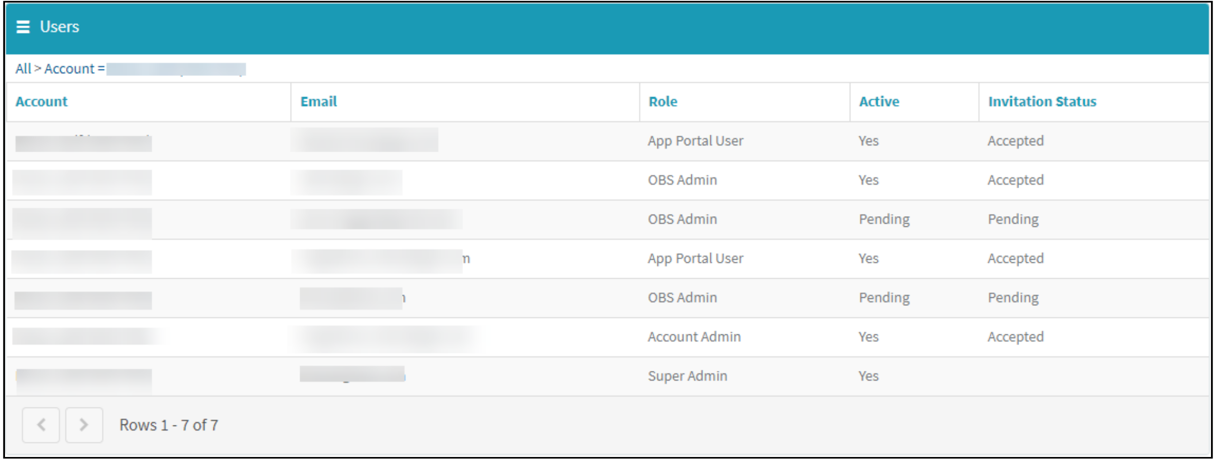
*Please select all users you want to assign an additional role to

[redacted]

Additional role

OBS Admin

The updated list of users is displayed.



Users

All > Account = [redacted]

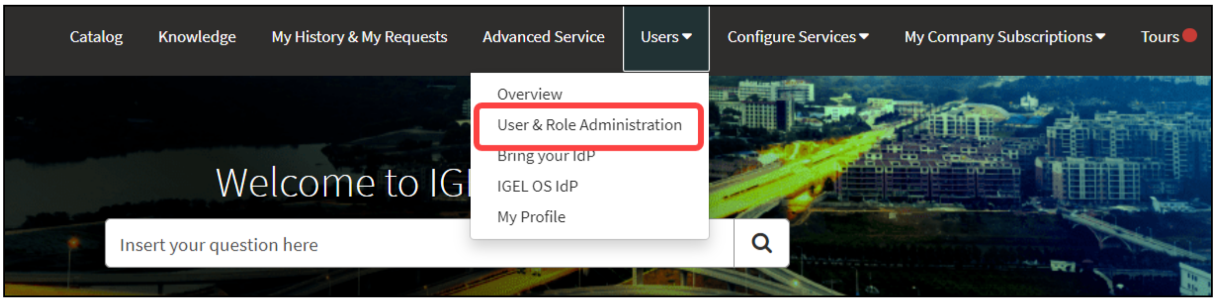
Account	Email	Role	Active	Invitation Status
[redacted]	[redacted]	App Portal User	Yes	Accepted
[redacted]	[redacted]	OBS Admin	Yes	Accepted
[redacted]	[redacted]	OBS Admin	Pending	Pending
[redacted]	[redacted]	App Portal User	Yes	Accepted
[redacted]	[redacted]	OBS Admin	Pending	Pending
[redacted]	[redacted]	Account Admin	Yes	Accepted
[redacted]	[redacted]	Super Admin	Yes	

Rows 1 - 7 of 7

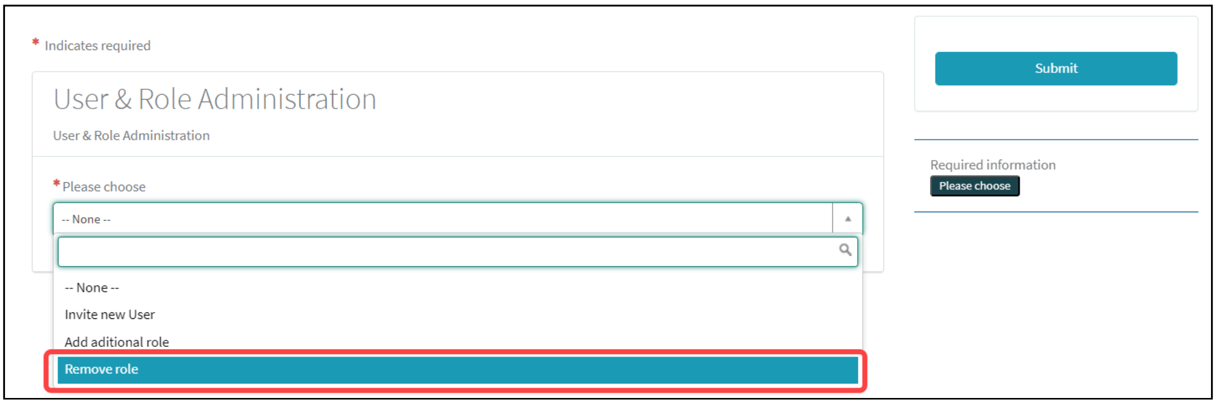
Removing a Role / Deactivating a User

You can remove one or more rules from a user. If you deactivate a user, the account is deleted. No e-mails will be sent to this account anymore.

1. Open IGEL Customer Portal[10], log in to your admin account, and select **Users > User & Role Administration**.



2. Select **Remove role**.


* Indicates required

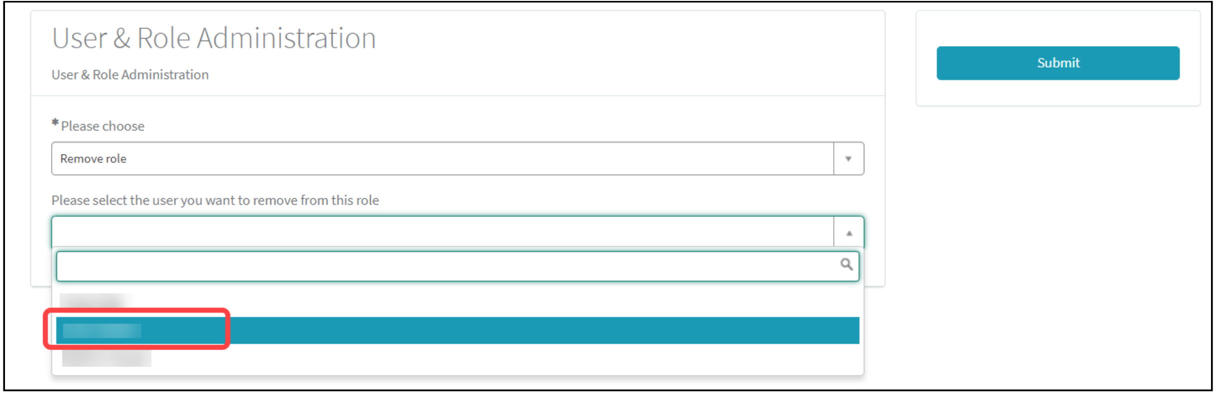
User & Role Administration

User & Role Administration

* Please choose

-- None --

3. Select the user from whom you want to remove a role.


User & Role Administration

User & Role Administration

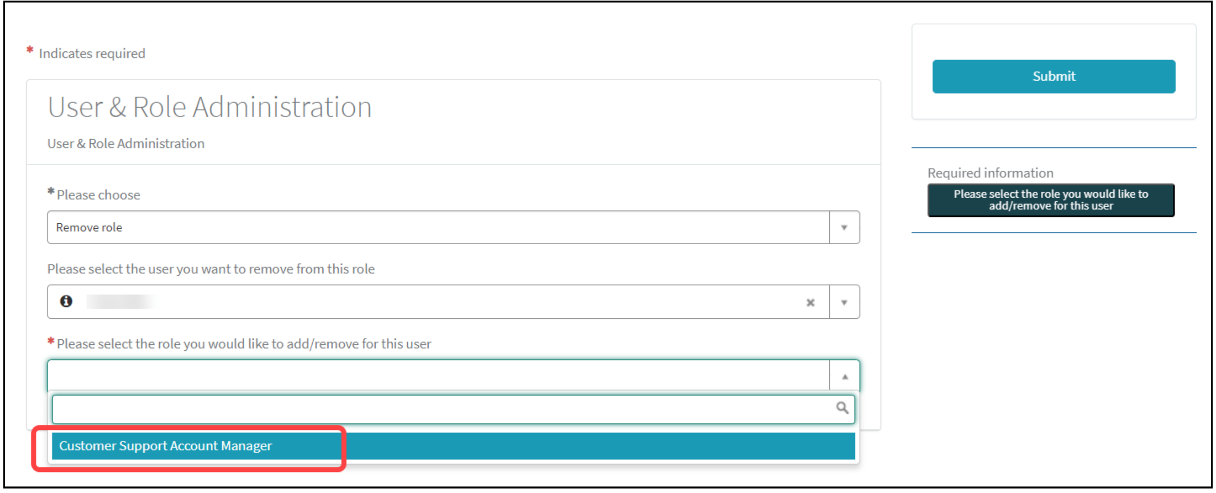
* Please choose

Remove role

Please select the user you want to remove from this role

[10] https://cosmos.igel.com/

4. Select the role you want to remove from the user.



* Indicates required

User & Role Administration

User & Role Administration

*Please choose

Remove role

Please select the user you want to remove from this role

[redacted]

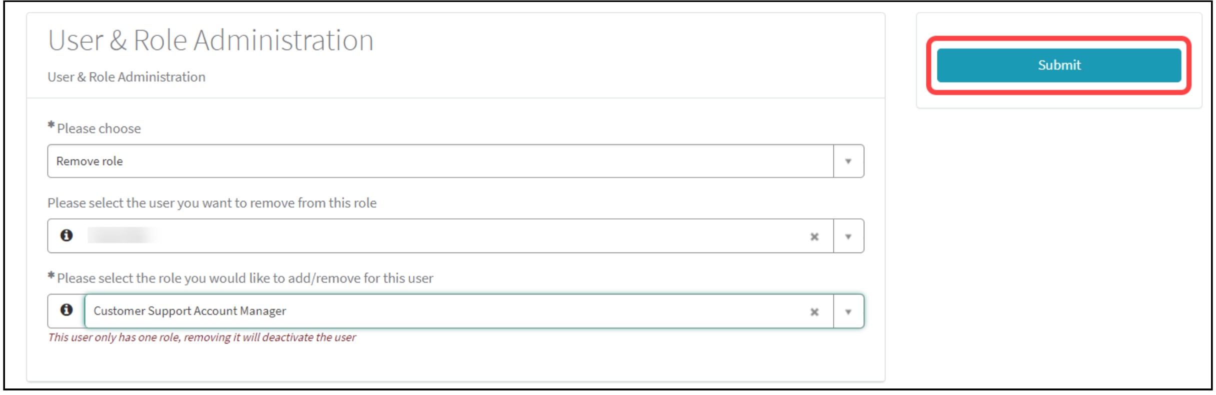
*Please select the role you would like to add/remove for this user

Customer Support Account Manager

Required information

Please select the role you would like to add/remove for this user

5. Click **Submit** to confirm the change.



User & Role Administration

User & Role Administration

*Please choose

Remove role

Please select the user you want to remove from this role

[redacted]

*Please select the role you would like to add/remove for this user

Customer Support Account Manager

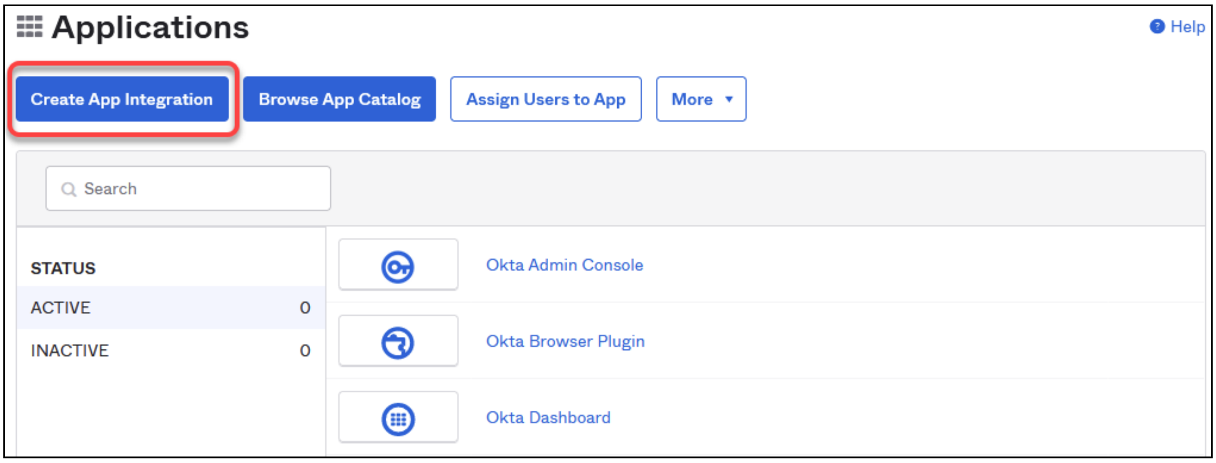
This user only has one role, removing it will deactivate the user

Using Okta as Federated Identity Provider

Setting Up an App Integration in Okta

For federating identities from Okta to Azure Active Directory (AAD), which is used in IGEL Cloud Services, you must set up an application integration in your Okta tenant. For this purpose, we will create a SAML 2.0 application.

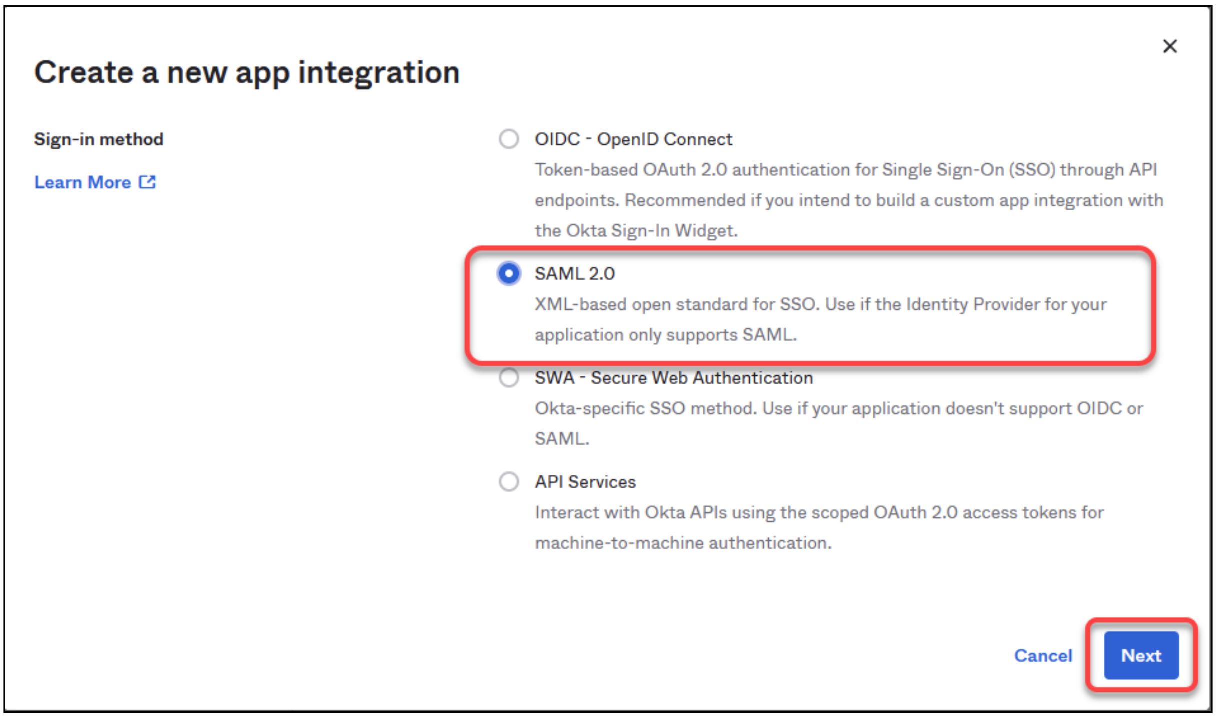
1. Log in to your administrator account at Okta, go to **Applications**, and click **Create App integration**.



STATUS	
ACTIVE	0
INACTIVE	0

- Okta Admin Console
- Okta Browser Plugin
- Okta Dashboard

2. Select **SAML 2.0** and click **Next**.



Create a new app integration

Sign-in method

Learn More

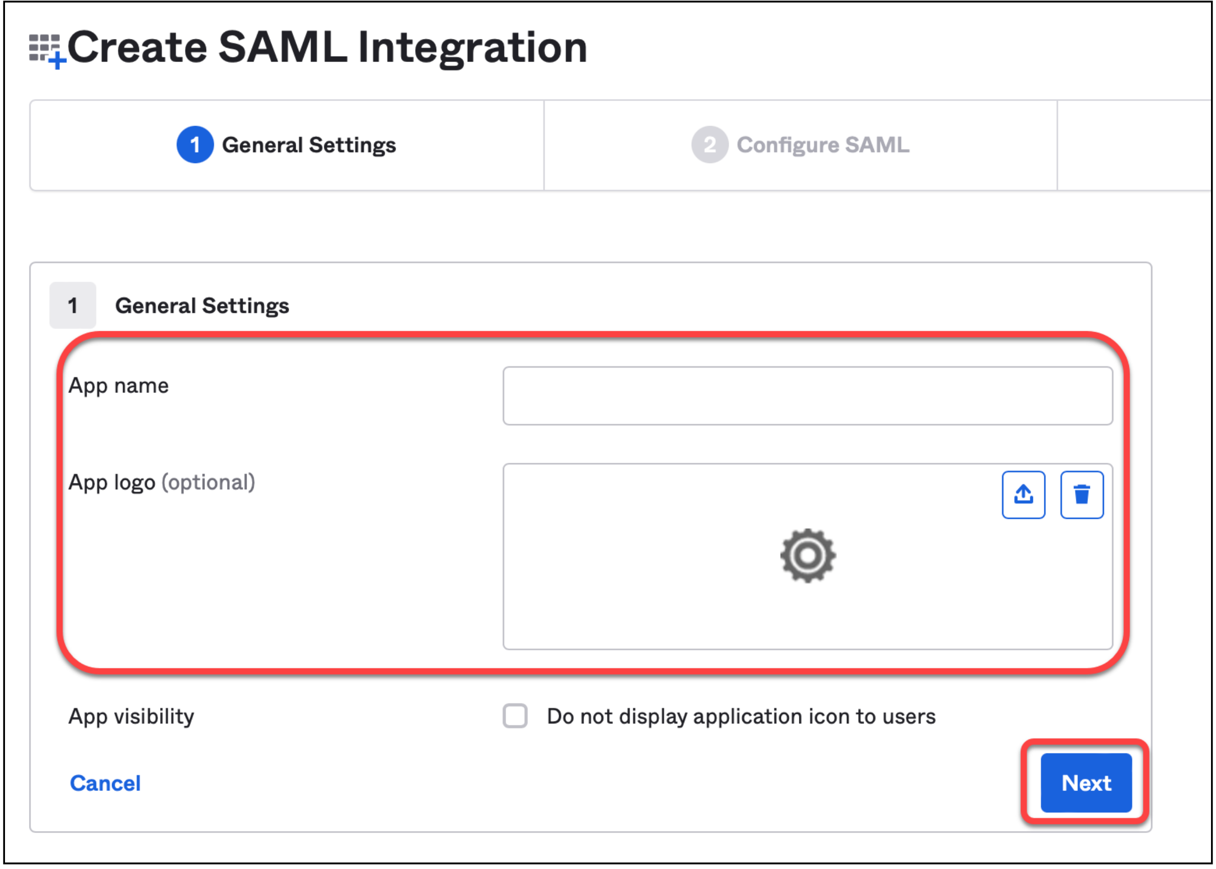
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

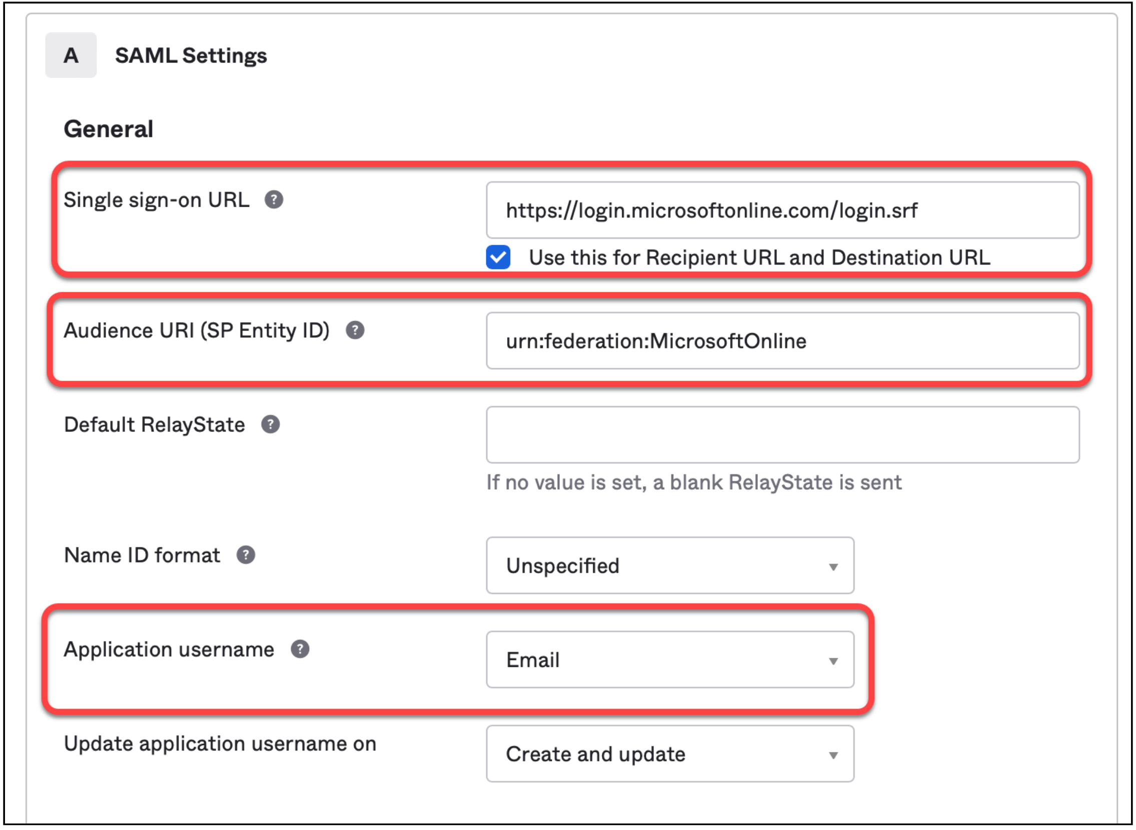
3. Define an **App name** and, optionally, an **App logo**, and click **Next**.



Create SAML Integration

4. Edit the SAML connection details as follows:
   - **Single sign on URL**: Enter `https://login.microsoftonline.com/login.srf`
   - **Use this for Recipient URL and Destination URL**: Activate this checkbox.
   - **Audience URI (SP Entity ID)**: Enter `urn:federation:MicrosoftOnline`

- **Application username**: Set this to **Email**.



A SAML Settings

General

Single sign-on URL: https://login.microsoftonline.com/login.srf

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): urn:federation:MicrosoftOnline

Default RelayState:

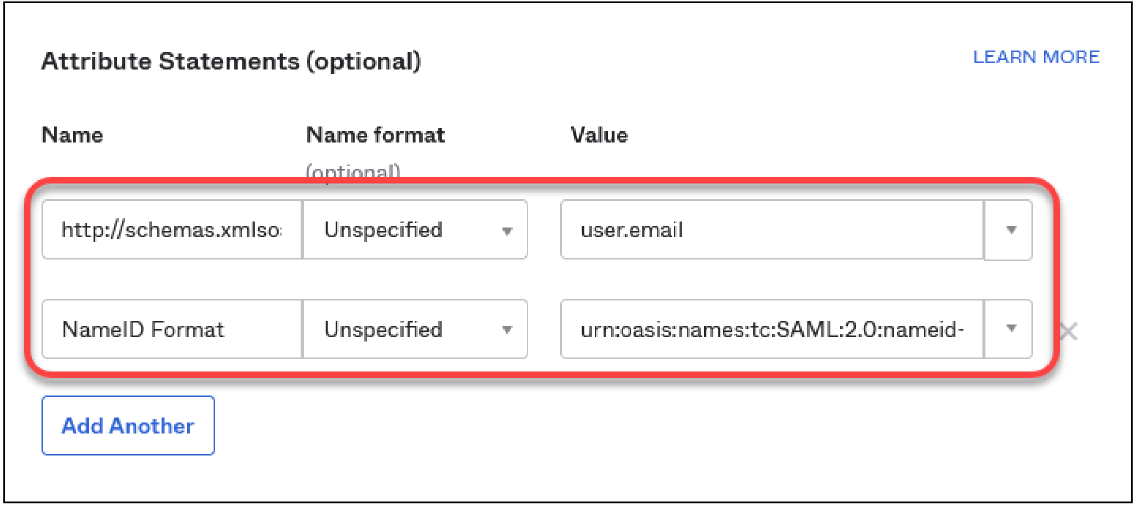
If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Email

Update application username on: Create and update

5. Add the following attributes:
   - **Name**: `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` ; **Value**: `user.email`
   - **Name**: `NameID Format` ; **Value**: `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`



Attribute Statements (optional)

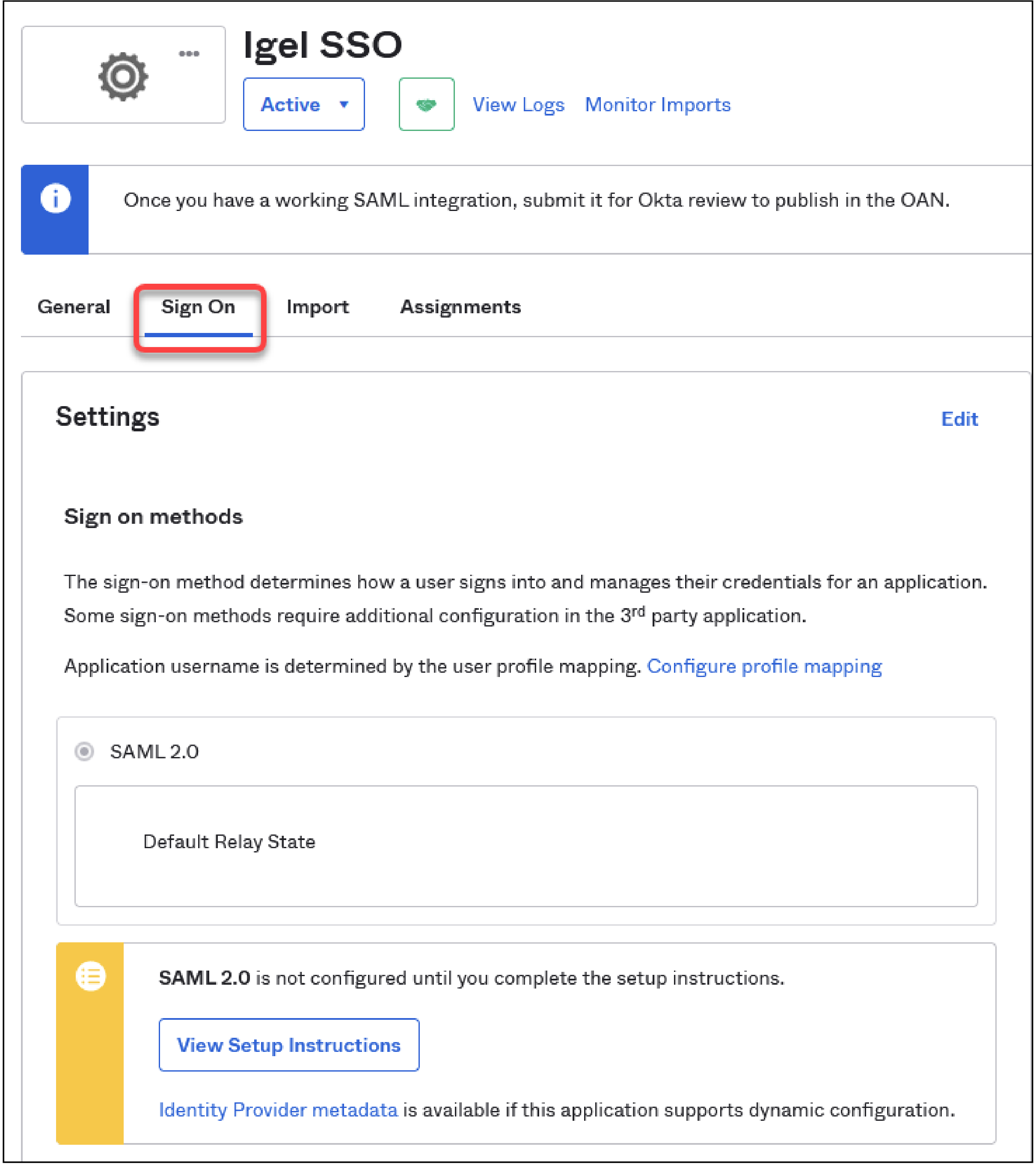
Name	Name format (optional)	Value
http://schemas.xmlso	Unspecified	user.email
NameID Format	Unspecified	urn:oasis:names:tc:SAML:2.0:nameid-

6. Finish your app integration.

Extracting the SAML 2.0 Connection Data

In this step, we will extract the connection data which will be used for creating an external identity that will be used for the IGEL Onboarding Service (OBS).

1. Open the settings for your application and select **Sign On**.



Igel SSO

Active ▾ View Logs Monitor Imports

Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

General Sign On Import Assignments

Settings Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

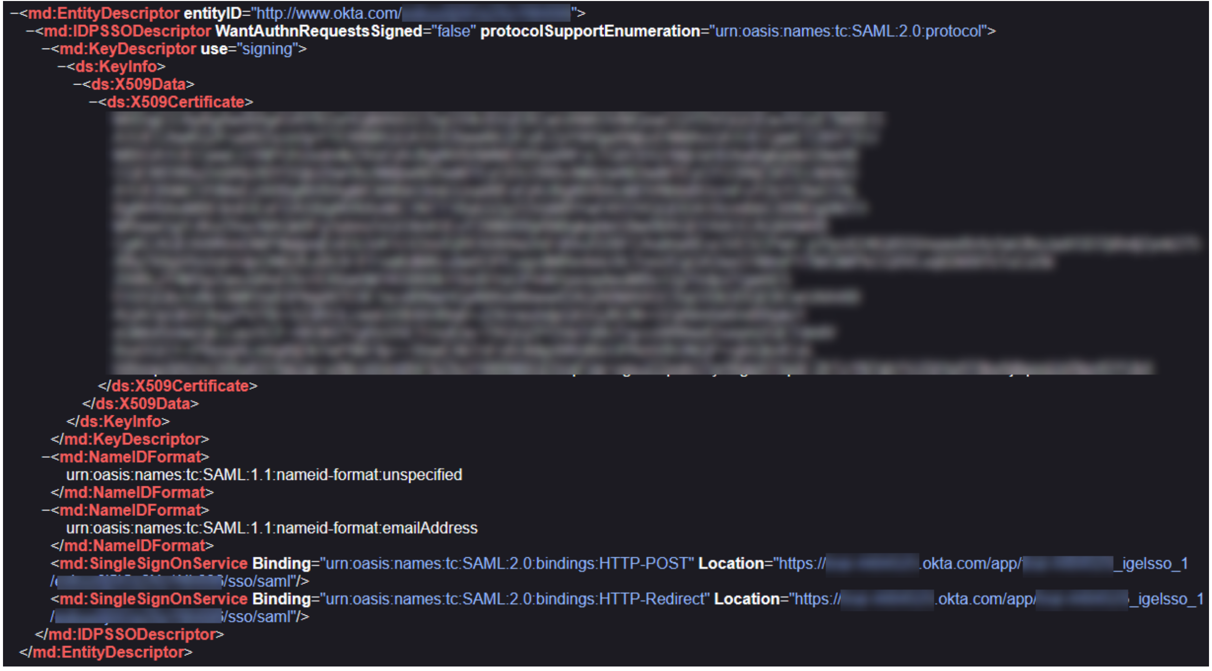
Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

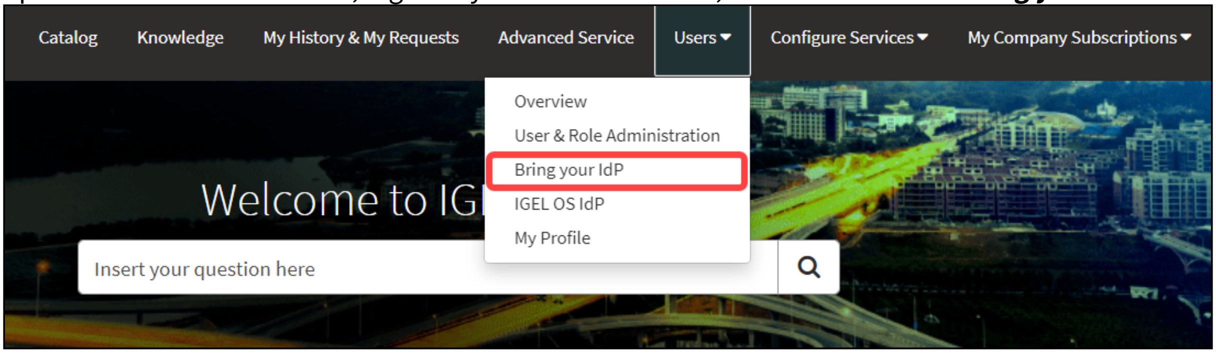
2. Click on the link **Identity Provider metadata** to download the data we will use afterward for configuring the IGEL Onboarding Service (OBS). The data is contained in an XML file. Also, note down the URL from this link, as we will need it later on.
   Example metadata file:



```
−<md:EntityDescriptor entityID="http://www.okta.com/[redacted]">
  −<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    −<md:KeyDescriptor use="signing">
      −<ds:KeyInfo>
        −<ds:X509Data>
          −<ds:X509Certificate>
              [redacted]
           </ds:X509Certificate>
         </ds:X509Data>
       </ds:KeyInfo>
     </md:KeyDescriptor>
    −<md:NameIDFormat>
       urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
     </md:NameIDFormat>
    −<md:NameIDFormat>
       urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
     </md:NameIDFormat>
     <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[redacted].okta.com/app/[redacted]_igelsso_1
     /[redacted]/sso/saml"/>
     <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://[redacted].okta.com/app/[redacted]_igelsso_1
     /[redacted]/sso/saml"/>
   </md:IDPSSODescriptor>
 </md:EntityDescriptor>
```

Configuring Okta as Your Federated IdP

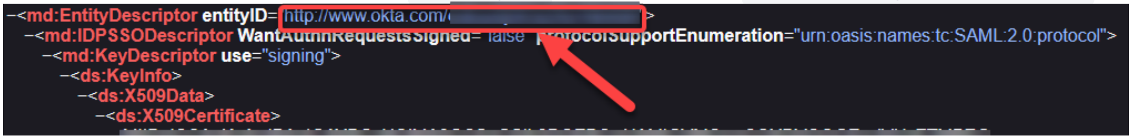
1. Open IGEL Customer Portal[11], log in to your admin account, and select **Users > Bring your IdP**.



2. Enter the following data from your metadata file:

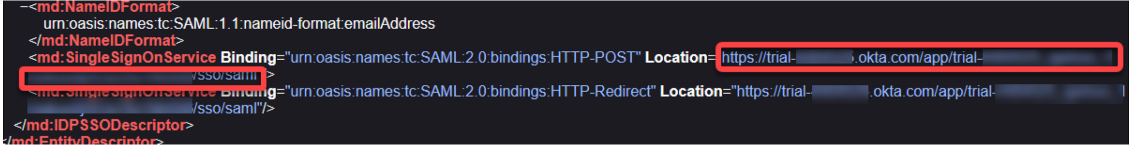
[11] https://cosmos.igel.com/

- **Issuer URI**: Value of the attribute `entityID` of the element `<md:EntityDescriptor>`



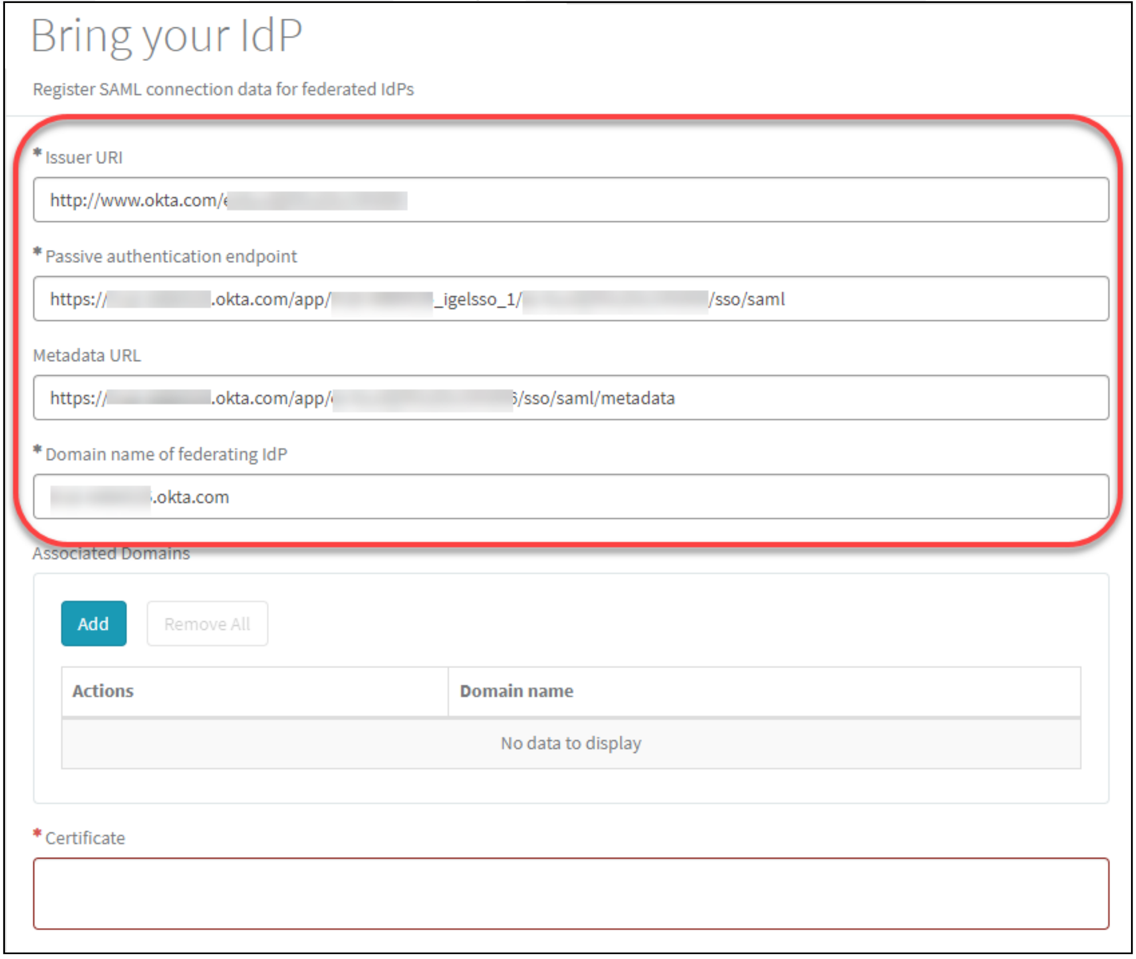
```
−<md:EntityDescriptor entityID="http://www.okta.com/[redacted]">
  −<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    −<md:KeyDescriptor use="signing">
      −<ds:KeyInfo>
        −<ds:X509Data>
          −<ds:X509Certificate>
```

- **Passive authentication endpoint**: Enter the value of the `Location` attribute of the `<md:SingleSignOnService>` element.



```
  −<md:NameIDFormat>
     urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
   </md:NameIDFormat>
   <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://trial-[redacted].okta.com/app/trial-[redacted]/sso/saml"/>
   <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://trial-[redacted].okta.com/app/trial-[redacted]/sso/saml"/>
 </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

- **Metadata URL**: Enter the URL of the link **Identity Provider metadata** you have used before to download the metadata file.
- **Domain name of federating IdP**: The part of **Passive authentication endpoint** before the `/app/` without the `https://`. Example: `mycompanydomain.okta.com`



Bring your IdP

Register SAML connection data for federated IdPs

* Issuer URI

http://www.okta.com/[redacted]

* Passive authentication endpoint

https://[redacted].okta.com/app/[redacted]_igelsso_1/[redacted]/sso/saml

Metadata URL

https://[redacted].okta.com/app/[redacted]/sso/saml/metadata

* Domain name of federating IdP

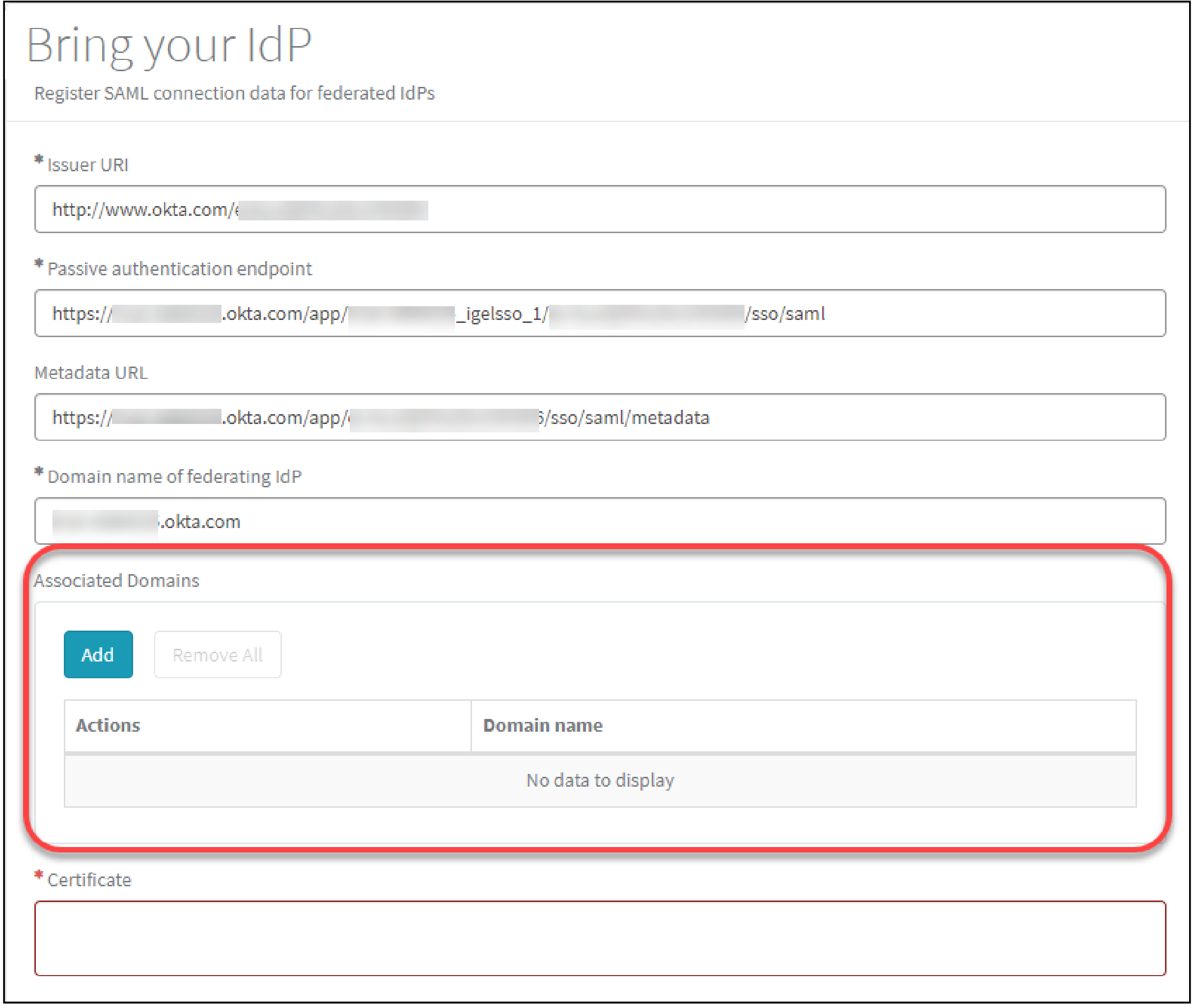
[redacted].okta.com

Associated Domains

Actions	Domain name
No data to display	

* Certificate

3. Under **Associated Domains**, add the domains that will be associated with your federate IdP.



Bring your IdP

Register SAML connection data for federated IdPs

* Issuer URI

http://www.okta.com/[redacted]

* Passive authentication endpoint

https://[redacted].okta.com/app/[redacted]_igelsso_1/[redacted]/sso/saml

Metadata URL

https://[redacted].okta.com/app/[redacted]/sso/saml/metadata

* Domain name of federating IdP

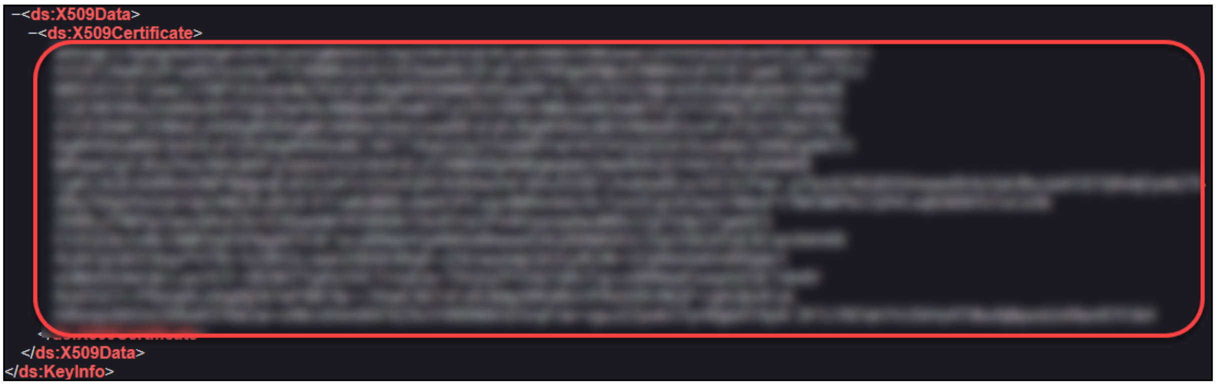
[redacted].okta.com

Associated Domains

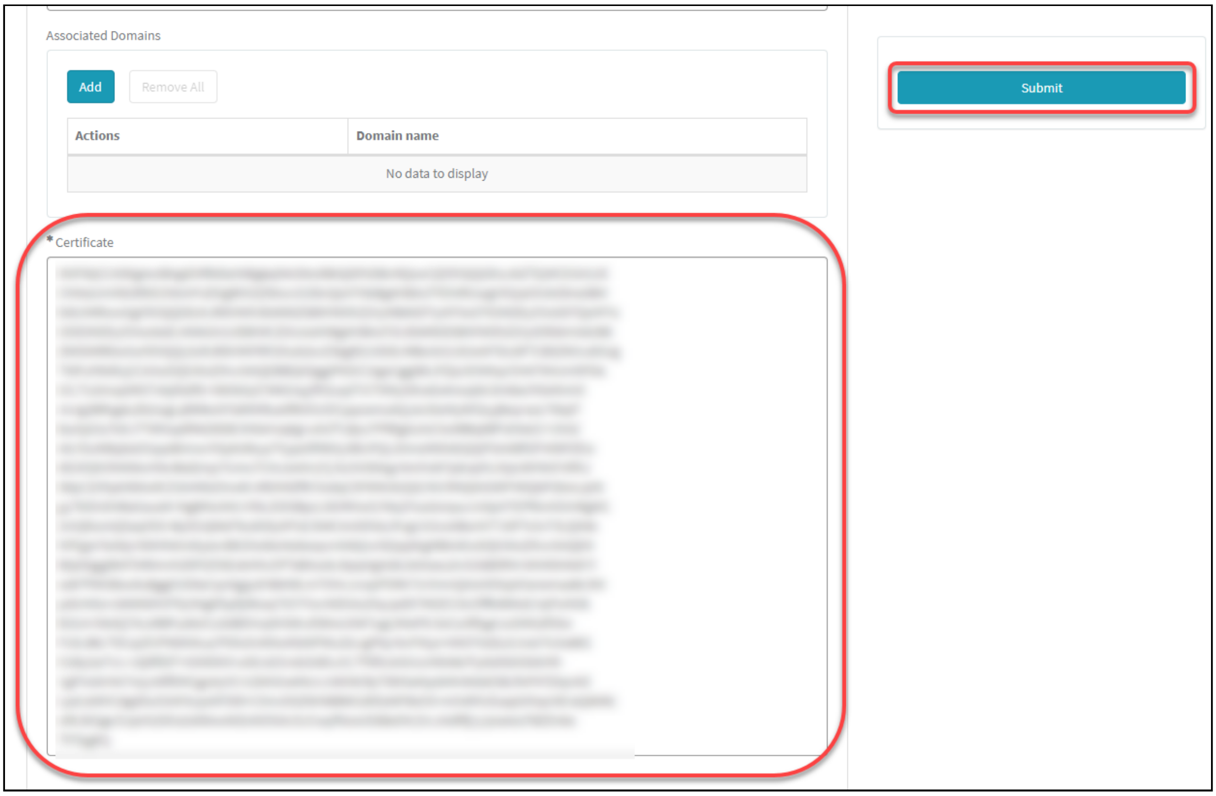
Actions	Domain name
No data to display	

* Certificate

4. Under **Certificate**, paste the content of the `<ds:X509Certificate>` element and then click **Submit**.



```
-<ds:X509Data>
  -<ds:X509Certificate>
    [redacted]
  </ds:X509Data>
</ds:KeyInfo>
```

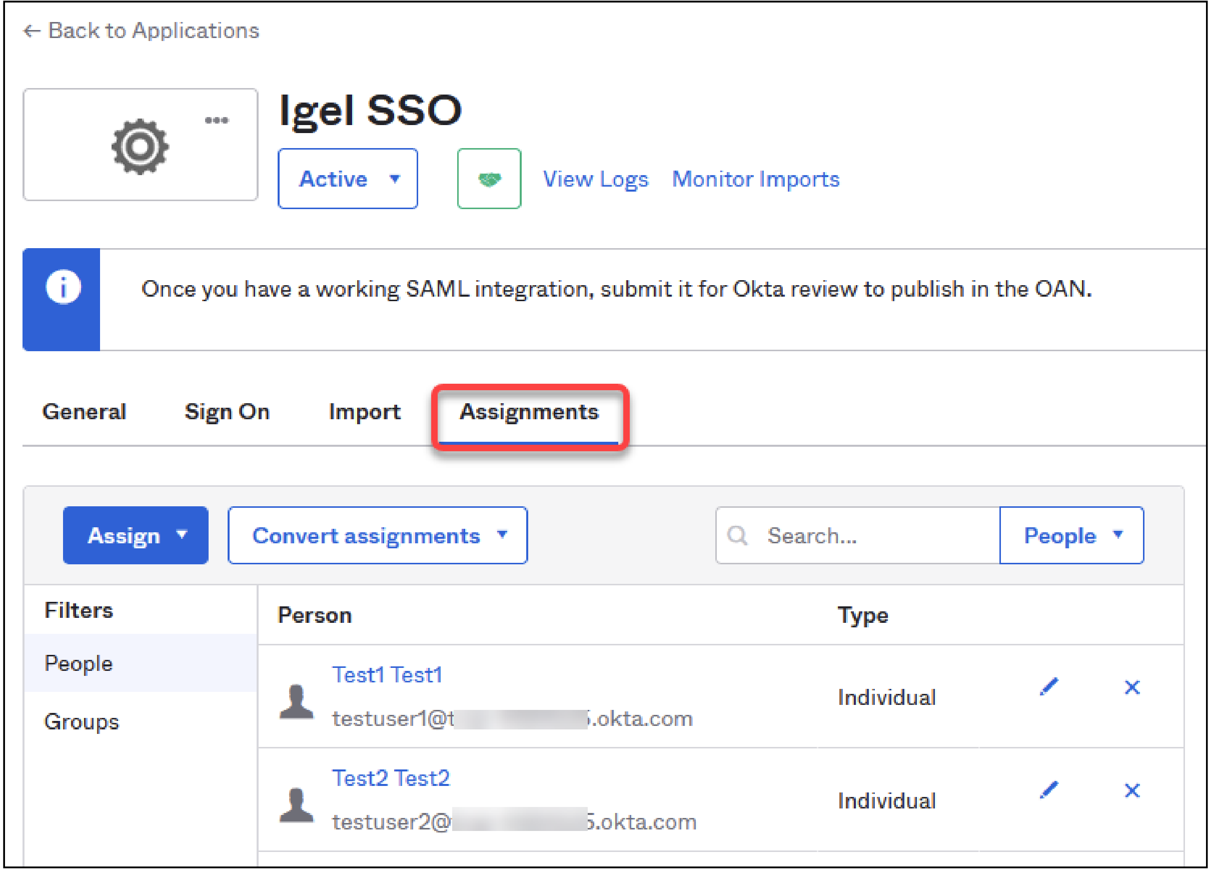


Assigning the Application to the Users

In the final step, we will assign the relevant users to the application we have created. When this is done, these users will be able to onboard their devices to the UMS in their company network.

You can assign groups of users or single users.

1. In your Okta application, select **Assignments**.



Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

Person	Type
Test1 Test1 testuser1@t[redacted].okta.com	Individual
Test2 Test2 testuser2@[redacted].okta.com	Individual

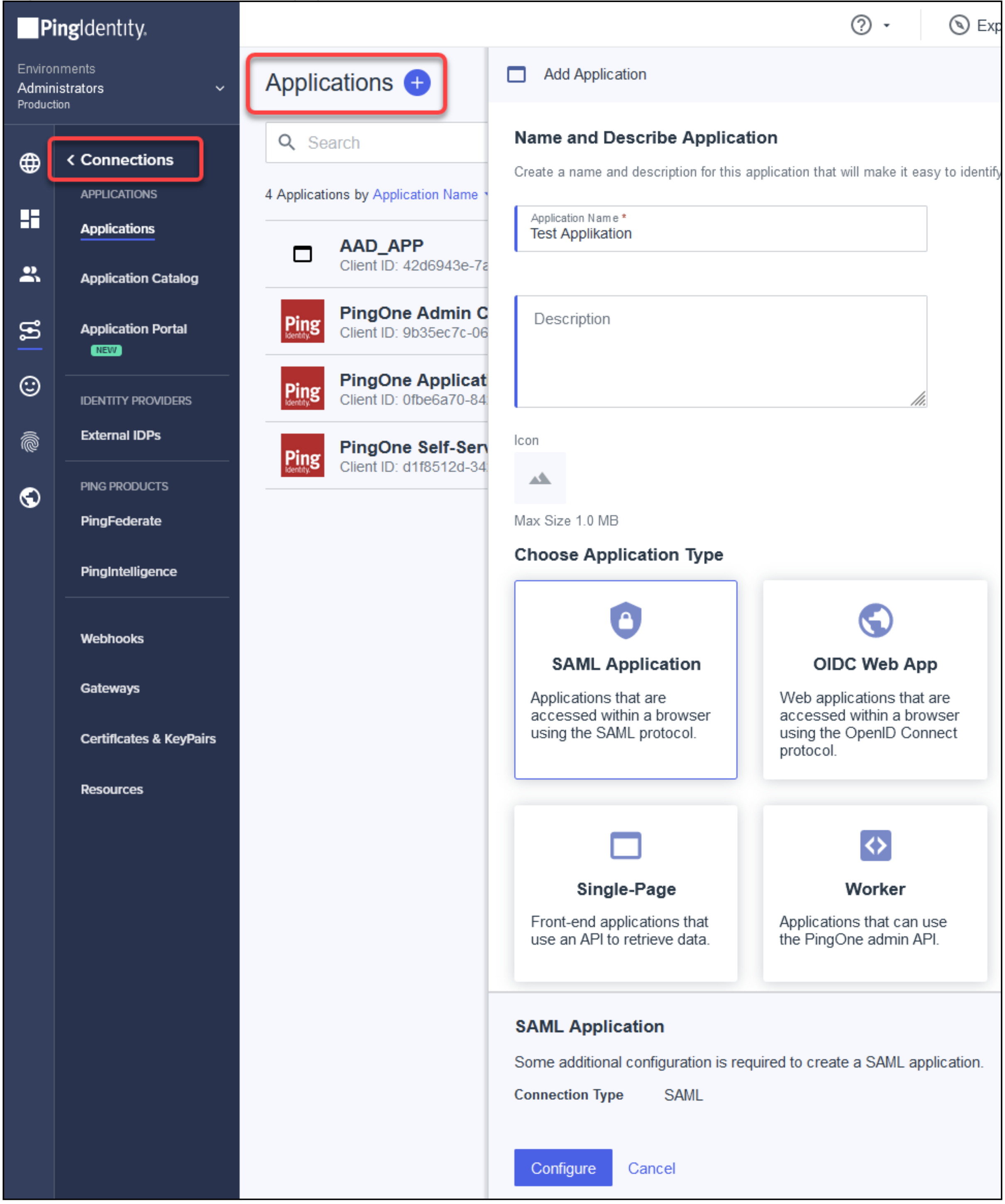
2. Assign the users to our new application.

Using Ping as Federated Identity Provider

Setting Up an App Integration in Ping

For federating identities from Ping to Azure Active Directory (AAD), you must set up an application integration in your Ping tenant. For this purpose, we will create a SAML 2.0 application.

1. Log in to your account at Ping, go to **Connection > Applications**, and then add an application.



Name and Describe Application

Create a name and description for this application that will make it easy to identify

Application Name * Test Applikation

Description

Icon

Max Size 1.0 MB

Choose Application Type

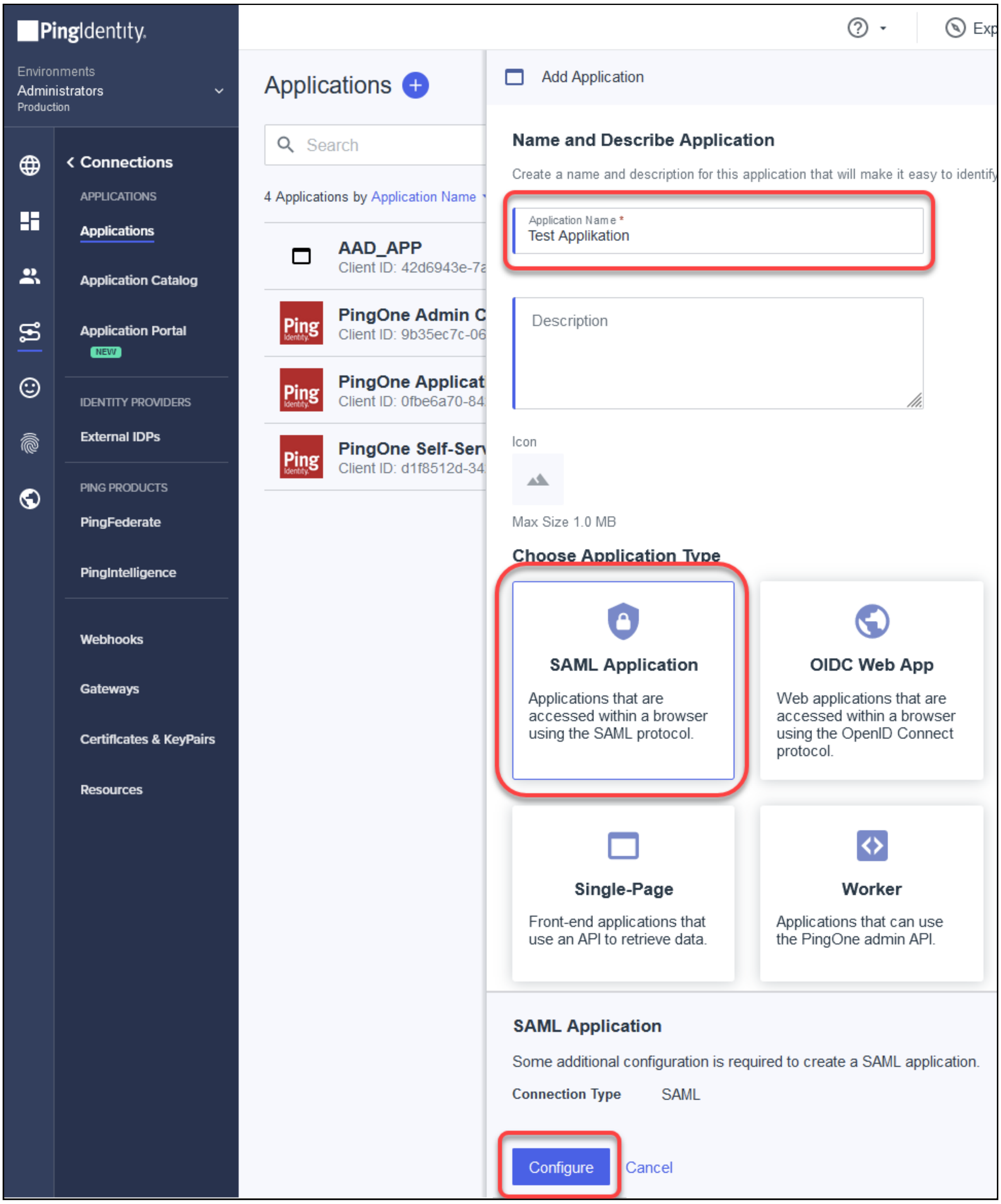
SAML Application
Applications that are accessed within a browser using the SAML protocol.
OIDC Web App
Web applications that are accessed within a browser using the OpenID Connect protocol.
Single-Page
Front-end applications that use an API to retrieve data.
Worker
Applications that can use the PingOne admin API.

SAML Application

Some additional configuration is required to create a SAML application.

Connection Type SAML

2. Enter an **Application Name**, select **SAML Application** as the application type, and then click **Configure**.



Name and Describe Application

Create a name and description for this application that will make it easy to identify

Application Name *: Test Applikation

Description

Icon

Max Size 1.0 MB

Choose Application Type

SAML Application: Applications that are accessed within a browser using the SAML protocol.

OIDC Web App: Web applications that are accessed within a browser using the OpenID Connect protocol.

Single-Page: Front-end applications that use an API to retrieve data.

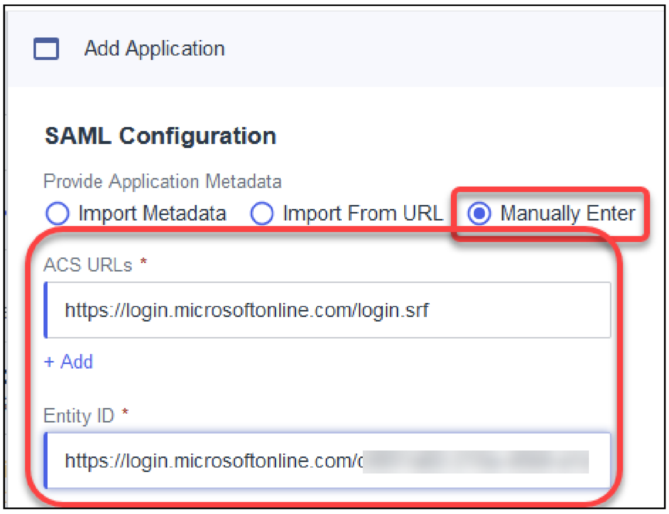
Worker: Applications that can use the PingOne admin API.

SAML Application

Some additional configuration is required to create a SAML application.

Connection Type: SAML

3. In the **SAML Configuration** dialog, select **Manually Enter** and enter the following data:
   - **ACS URLs**: Enter `https://login.microsoftonline.com/login.srf`
   - **Entity ID**: Enter the prefix `https://login.microsoftonline.com/` followed by the Azure Active Directory tenant ID.



Add Application

SAML Configuration

Provide Application Metadata

○ Import Metadata ○ Import From URL ● Manually Enter

ACS URLs *

https://login.microsoftonline.com/login.srf

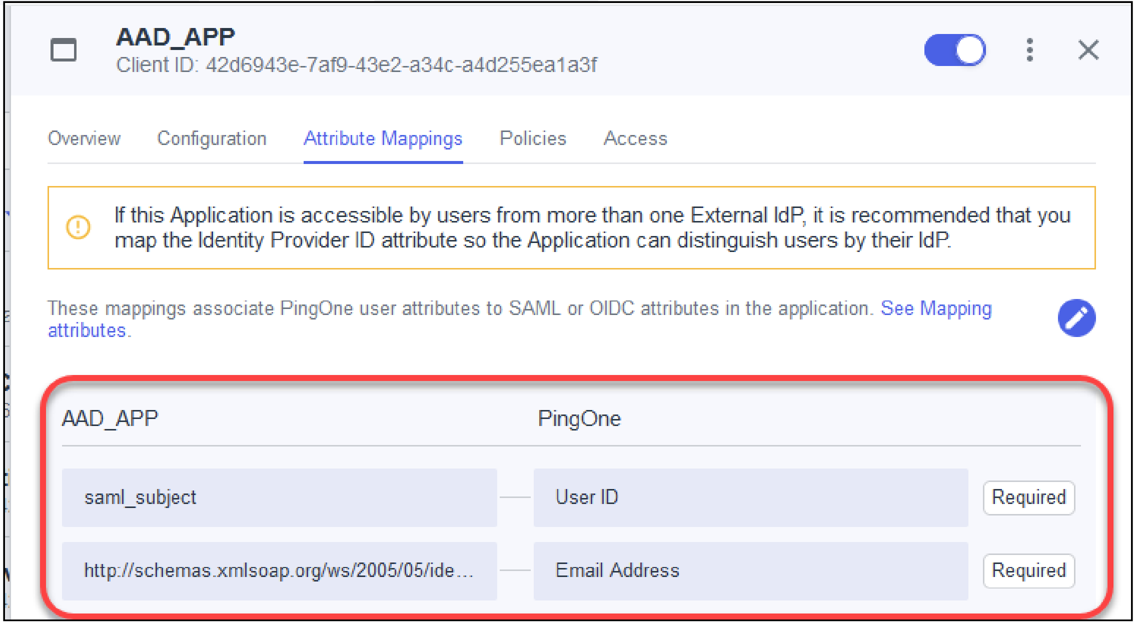
+ Add

Entity ID *

https://login.microsoftonline.com/[redacted]

4. Create the application.

5. Edit/create the following attribute mappings:
   - Map `saml_subject` to `User ID`.
   - Create the identifier `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress` and map it to `Email Address`.



If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See Mapping attributes.

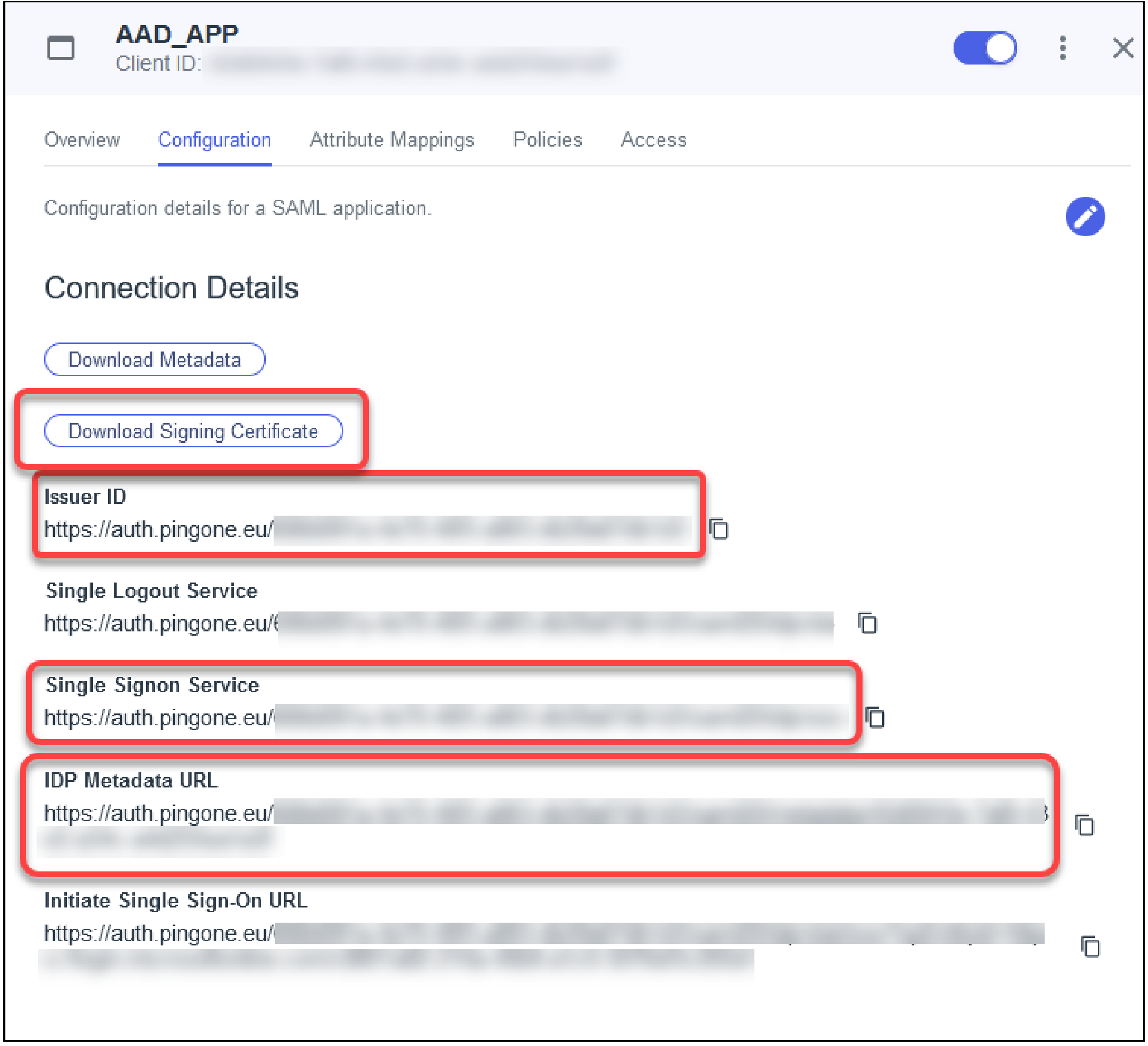
AAD_APP	PingOne	
saml_subject	User ID	Required
http://schemas.xmlsoap.org/ws/2005/05/ide…	Email Address	Required

6. Finish the application setup.

Obtaining the SAML 2.0 Connection Data

In this step, we will get the connection data which will be used for creating an external identity that will be used for the IGEL Onboarding Service (OBS).

▶ Open the settings for your application and select **Configuration**.
The relevant data is shown and can be copied to the clipboard.



AAD_APP
Client ID: [redacted]

Overview | Configuration | Attribute Mappings | Policies | Access

Configuration details for a SAML application.

Connection Details

Download Metadata

Download Signing Certificate

Issuer ID
https://auth.pingone.eu/[redacted]

Single Logout Service
https://auth.pingone.eu/[redacted]

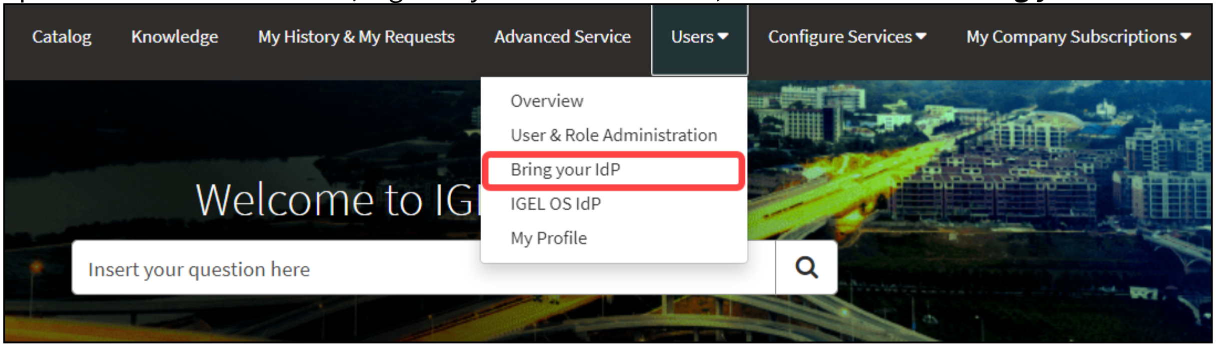
Single Signon Service
https://auth.pingone.eu/[redacted]

IDP Metadata URL
https://auth.pingone.eu/[redacted]

Initiate Single Sign-On URL
https://auth.pingone.eu/[redacted]

Configuring Ping as Your Federated IdP

1. Open IGEL Customer Portal[12], log in to your admin account, and select **Users > Bring your IdP**.



2. Enter the following data from your metadata file:
   - **Issuer URI**: The **Issuer ID** from the Ping **Configuration** page.
   - **Passive authentication endpoint**: The value of **Single Signon Service** from the Ping **Configuration** page.
   - **Metadata URL**: The **IDP Metadata URL** from the Ping **Configuration** page.
   - **Domain name of federating IdP**: Enter the domain name that is associated with your Ping account.

[12] https://cosmos.igel.com/

Installing / Upgrading to IGEL UMS 12

This article describes how to install IGEL Universal Management Suite (UMS) 12 or upgrade your existing UMS installation and provides information on what should be considered during the installation / update.

IGEL Cloud Gateway (ICG) with IGEL OS 12 and IGEL OS 11 Devices

If you exclusively manage IGEL OS 12 devices, you may not need an IGEL Cloud Gateway (ICG) between your UMS 12 and your devices, regardless of whether the devices are inside or outside the company network. Whether an ICG is required or not depends on your particular use case or policy. See IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices.
If you manage remote IGEL OS 11 devices and want to manage also your remote IGEL OS 12 devices via ICG, ICG 12 is required.
If you manage your remote IGEL OS 12 devices without ICG and your remote IGEL OS 11 devices with ICG, you can use ICG 12 or ICG 2.x.

Please note the following, especially if you use any special policies or other components between the devices and the IGEL Universal Management Suite (UMS) or the IGEL Cloud Gateway (ICG):

- IGEL OS 12 devices use TLS 1.3
- IGEL OS 11 devices use TLS 1.2

The hardware requirements for ICG 12 are the same as for ICG 2.x with the exception that ICG 12 requires 4 GB of RAM instead of 2 GB, see:

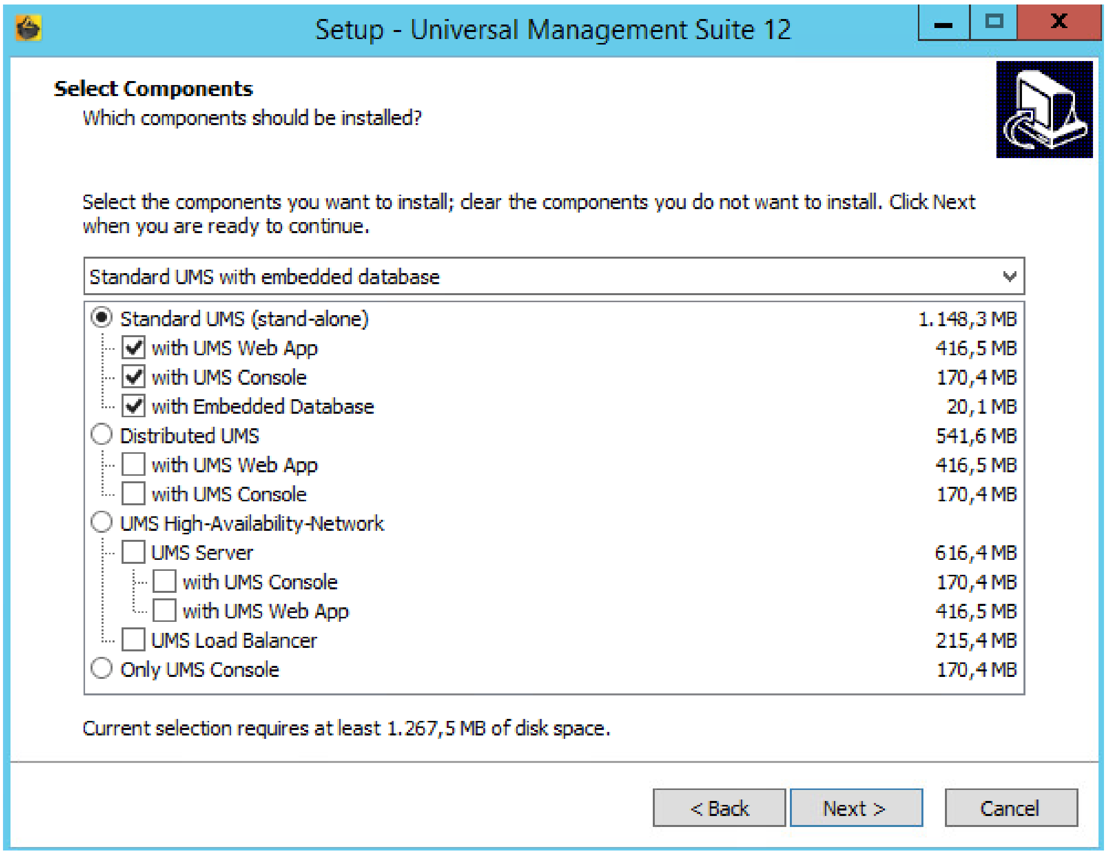
- ICG Manual
- ICG Prerequisites

1. Download IGEL UMS 12 from the IGEL Download Server[13].

2. Consider the installation requirements, see Installation Requirements for the IGEL UMS.
   If you are going to upgrade your existing UMS installation, see also Updating UMS.

3. Install the UMS. Depending on your needs, you can install **standard UMS**, **Distributed UMS**, or **UMS High Availability**. Include the **UMS Web App** and the **UMS Console** into the installation – both of them are currently required for the management of your UMS installation and devices.

[13] https://www.igel.com/software-downloads/cosmos/



Setup - Universal Management Suite 12

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Standard UMS with embedded database

● Standard UMS (stand-alone)	1.148,3 MB
☑ with UMS Web App	416,5 MB
☑ with UMS Console	170,4 MB
☑ with Embedded Database	20,1 MB
○ Distributed UMS	541,6 MB
□ with UMS Web App	416,5 MB
□ with UMS Console	170,4 MB
○ UMS High-Availability-Network	
□ UMS Server	616,4 MB
□ with UMS Console	170,4 MB
□ with UMS Web App	416,5 MB
□ UMS Load Balancer	215,4 MB
○ Only UMS Console	170,4 MB

Current selection requires at least 1.267,5 MB of disk space.

Information on how to install the UMS can be found under:
Windows: IGEL UMS Installation under Windows
Linux: IGEL UMS Installation under Linux

Information on how to upgrade the UMS can be found under:
Windows: Updating the IGEL UMS under Windows
Linux: Updating the IGEL UMS under Linux

You can update to UMS version 12.01.110 or higher from

- UMS 6.x

If you participated in the program for validation and testing of IGEL OS 12, you can also update to UMS 12.01.110 from

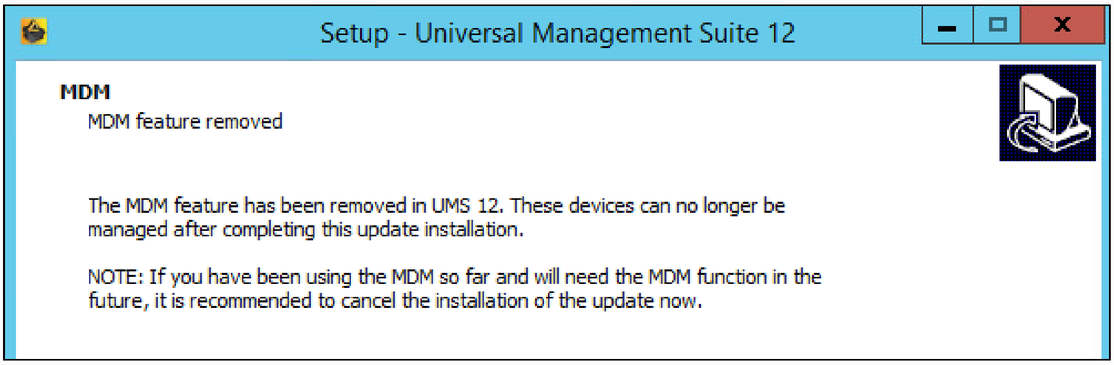
- UMS 12.00.900
- UMS 12.01.x

Before the update, it is always recommended to make a backup of your current system. For details on how to create backups, see Creating a Backup.

During the installation / update on Linux, you have to confirm or enter the IP address of the UMS Server. If you do not adjust the IP address, the web certificate of your UMS Server may contain the wrong IP, which results in problems with device registration. See Invalid Web Certificate and Errors by Device Registration after the Installation of the IGEL UMS 12 on Linux.

For Update Installations Only

- As of UMS 12, MDM feature is no longer available. Cancel the upgrade to UMS 12 if you still need the MDM feature:



MDM

MDM feature removed

The MDM feature has been removed in UMS 12. These devices can no longer be managed after completing this update installation.

NOTE: If you have been using the MDM so far and will need the MDM function in the future, it is recommended to cancel the installation of the update now.

- Only if you have a Distributed UMS installation: During the update installation, it will be checked whether only one UMS Server is running and the others are stopped. If not, stop all UMS Servers except one and proceed with the update; otherwise, you risk losing data. After the update on this server is complete, you can update the remaining UMS Servers, either simultaneously or one after another. But see also Known Issues UMS 12.01.110.

UMS 12 Communication Ports

If you are going to make network changes, consider the following ports and paths:

- For IGEL OS 12 devices, TCP 8443 `/device-connector/*` is required.
  SSL can be terminated at the reverse proxy / external load balancer (see IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) or at the UMS Server.
- For importing IGEL OS 12 Apps to the UMS from the IGEL App Portal, the URL https://app.igel.com/ (TCP 443) is required.
- For the UMS Web App, TCP 8443 `/webapp/*` and `/wums-app/*` are required.
- For the UMS Console, the root is required, i.e. TCP 8443 `/*`
- For IGEL OS 11 devices, TCP 30001 and TCP/UDP 30005 are required.

For more information on UMS ports, see IGEL UMS Communication Ports.

The web server port (default: 8443) can be changed under **UMS Administrator > Settings**. If you do not configure the Cluster Address, it is recommended to change the port before registering any IGEL OS 12 devices. This is due to the fact that the already registered IGEL OS 12 devices won't be manageable anymore after the change of the web server port if no Cluster Address is configured. In this case, you will have to register these devices anew.

ⓘ The FQDN and port of your external load balancer / reverse proxy must be specified in the UMS Console under **UMS Administration > Global Configuration > Server Network Settings > Cluster Address**. Information on the Cluster Address can be found under Server Network Settings in the IGEL UMS.

✓ It is recommended to check your rights since UMS 12 has new permissions, e.g. **UMS Console > System > Administrator accounts > New / Edit > General - WebApp > App Management** for managing IGEL OS Apps. See General Administrator Rights and Important Information for the IGEL UMS Web App.

Registering the UMS

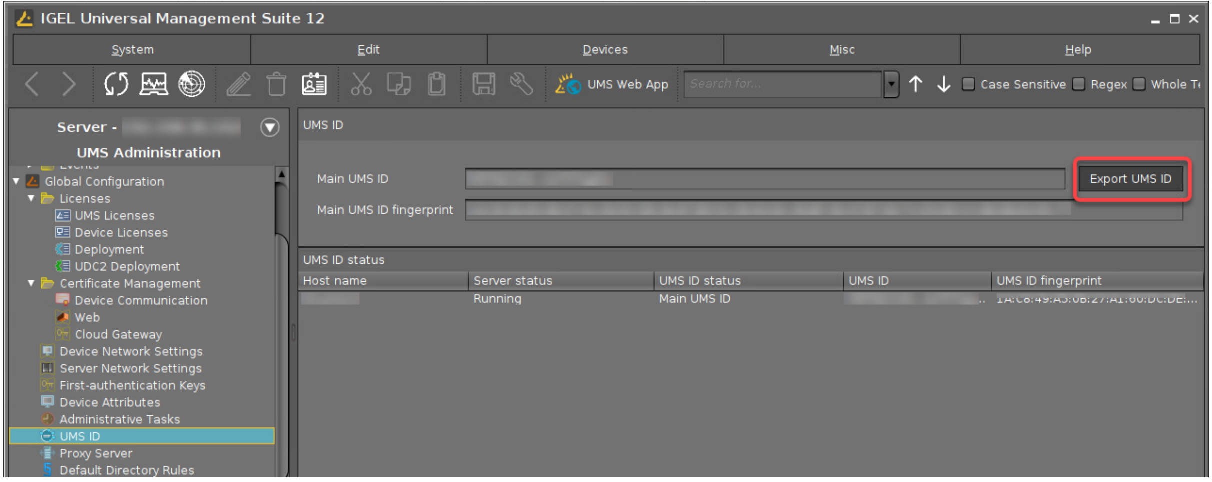
To authenticate your UMS to the IGEL Cloud Services, you must register your UMS. This involves uploading the UMS ID, which is essentially a certificate of your UMS, to the IGEL Customer Portal.

ⓘ The registration of the UMS is required if you manage IGEL OS 12 devices. If you manage IGEL OS 11 devices only, the registration of the UMS is recommended, but not obligatory.

Exporting the UMS ID

To upload the UMS ID, we must export it from the UMS.

1. Open your UMS Console, go to **UMS Administration > Global Configuration > UMS ID**, and click **Export UMS ID**.



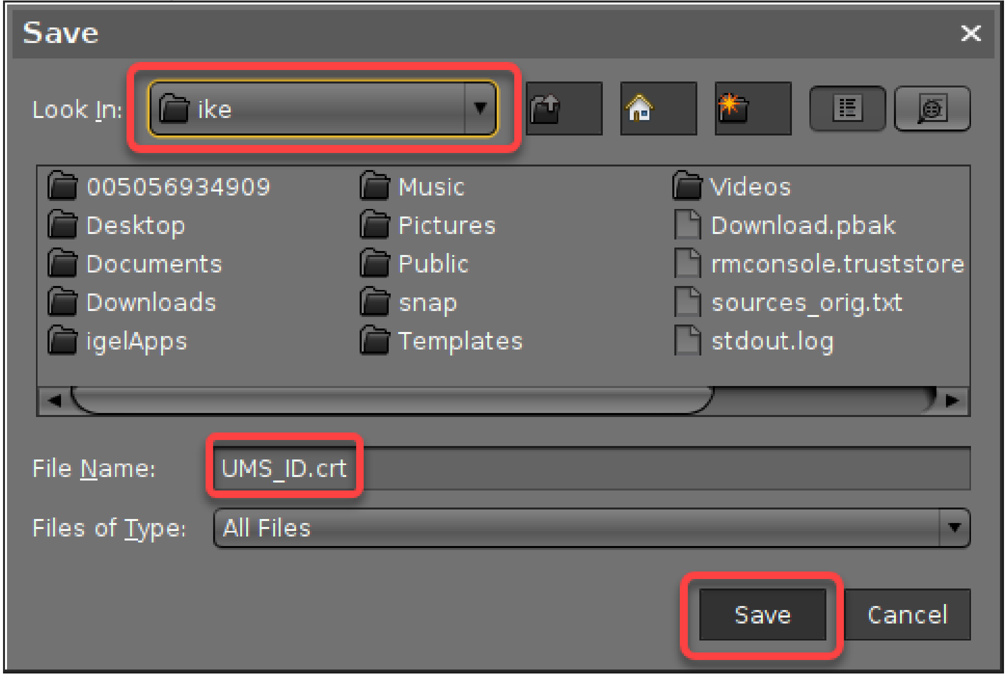
Main UMS ID [redacted]

Main UMS ID fingerprint [redacted]

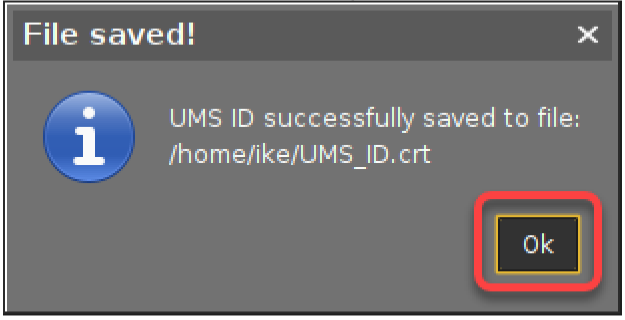
UMS ID status

Host name	Server status	UMS ID status	UMS ID	UMS ID fingerprint
[redacted]	Running	Main UMS ID	[redacted]	[redacted]

2. Select a storage location and click **Save**.



3. Close the confirmation dialog.



File saved!

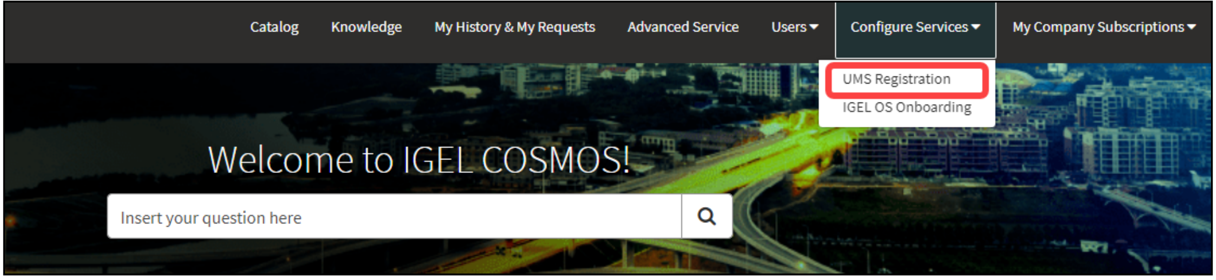
UMS ID successfully saved to file: /home/ike/UMS_ID.crt

Registering the UMS

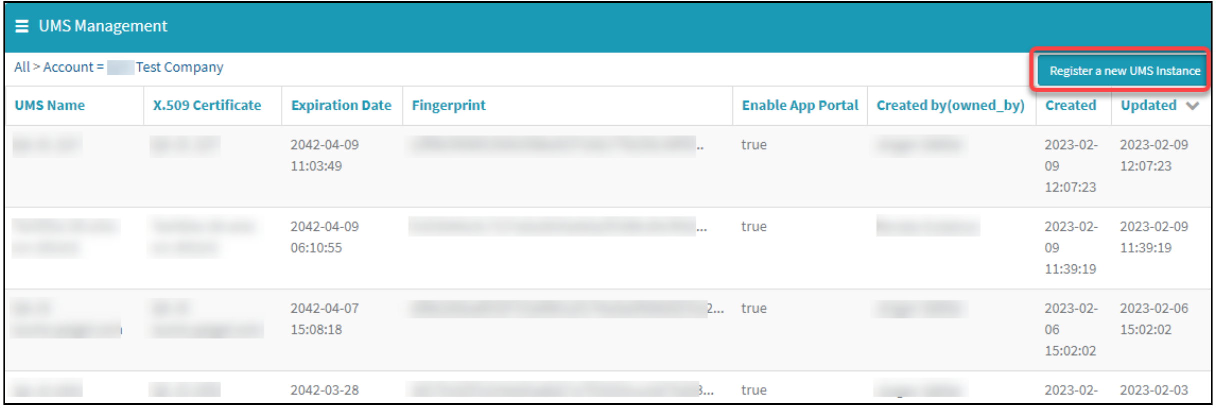
1. Open IGEL Customer Portal[14] in your browser and log in to your admin account.

[14] https://cosmos.igel.com/

2. From the **Configure Services** menu, select **UMS Registration**.



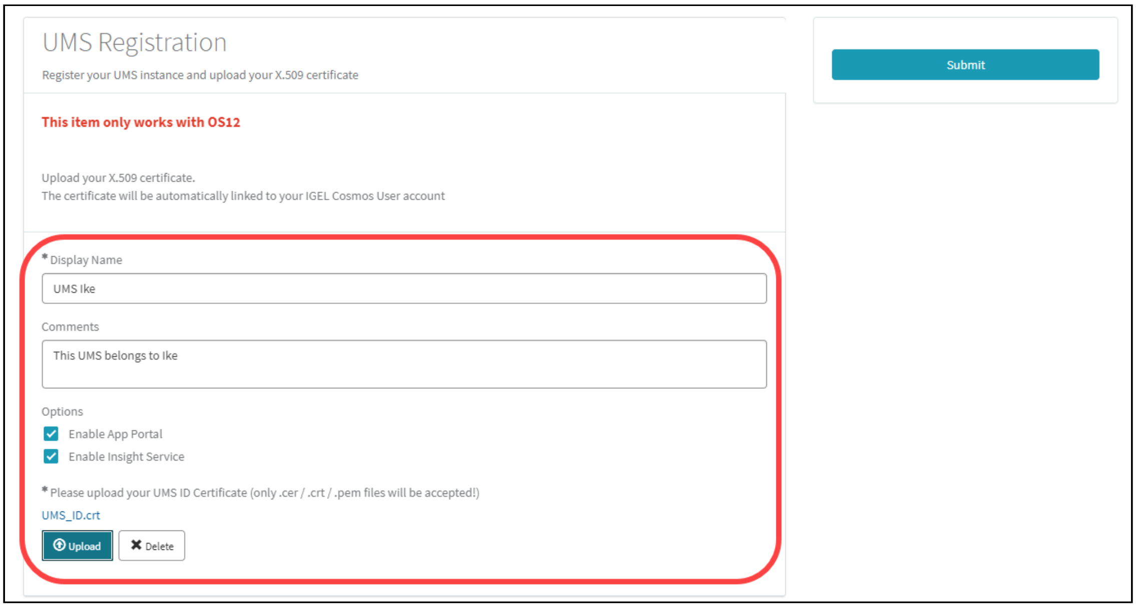
3. Click **Register a new UMS Instance**.



All > Account = [redacted] Test Company

UMS Name	X.509 Certificate	Expiration Date	Fingerprint	Enable App Portal	Created by(owned_by)	Created	Updated
[redacted]	[redacted]	2042-04-09 11:03:49	[redacted]..	true	[redacted]	2023-02-09 12:07:23	2023-02-09 12:07:23
[redacted]	[redacted]	2042-04-09 06:10:55	[redacted]...	true	[redacted]	2023-02-09 11:39:19	2023-02-09 11:39:19
[redacted]	[redacted]	2042-04-07 15:08:18	[redacted]2...	true	[redacted]	2023-02-06 15:02:02	2023-02-06 15:02:02
[redacted]	[redacted]	2042-03-28	[redacted]3...	true	[redacted]	2023-02-	2023-02-03

4. Edit the data as follows:
   - **UMS Name**: Display name for your UMS
   - **Comments**: Optional comment
   - **Enable App Portal**: Must be activated to enable access to the App Portal by the UMS. Technically, this option allows the App Portal to request the UMS ID.
   - **Enable Insight Service**: Allows the Insight Service to collect analytical and usage data for further improvement and inform you about available updates. For details, see IGEL Insight Service(see page 198).
   - **Required - Upload**: Upload the certificate file (UMS ID) of your UMS. Make sure that the certificate file has the extension `.cer`, `.crt`, or .pem



UMS Registration

Register your UMS instance and upload your X.509 certificate

This item only works with OS12

Upload your X.509 certificate.
The certificate will be automatically linked to your IGEL Cosmos User account

* Display Name: UMS Ike

Comments: This UMS belongs to Ike

Options

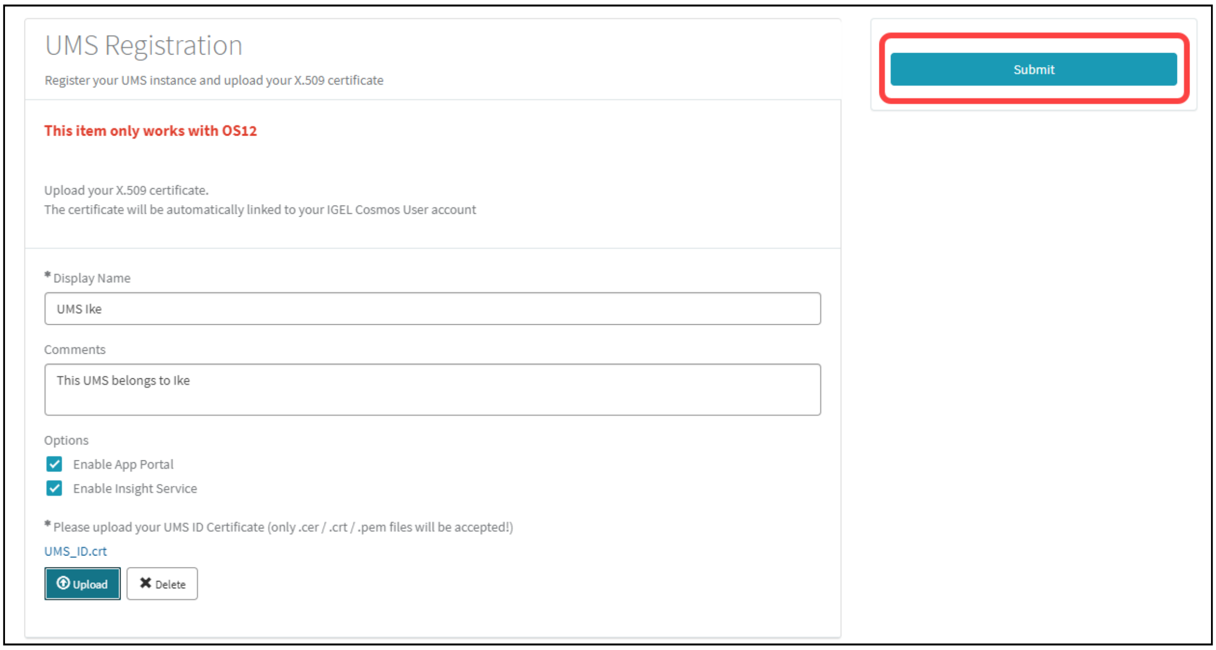
☑ Enable App Portal

☑ Enable Insight Service

* Please upload your UMS ID Certificate (only .cer / .crt / .pem files will be accepted!)

UMS_ID.crt

5. Click **Submit**.



UMS Registration

Register your UMS instance and upload your X.509 certificate

This item only works with OS12

Upload your X.509 certificate.
The certificate will be automatically linked to your IGEL Cosmos User account

* Display Name: UMS Ike

Comments: This UMS belongs to Ike

Options

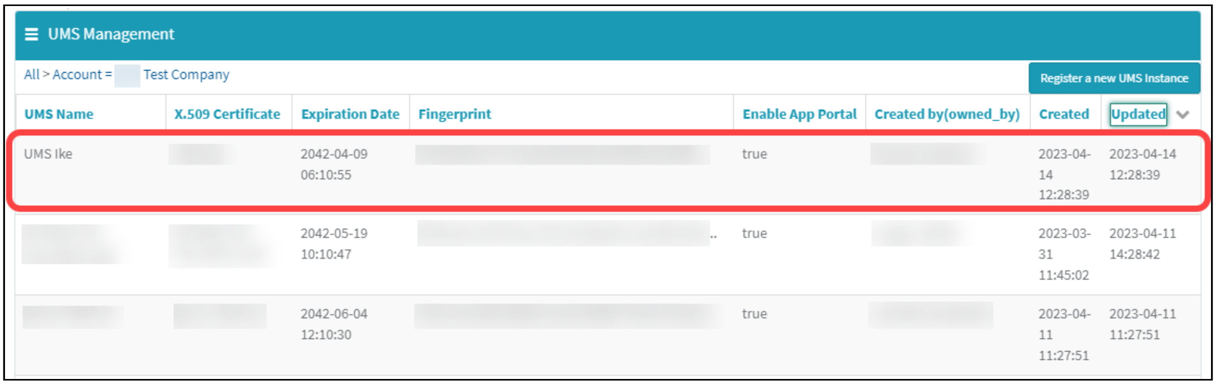
☑ Enable App Portal

☑ Enable Insight Service

* Please upload your UMS ID Certificate (only .cer / .crt / .pem files will be accepted!)

UMS_ID.crt

After a few seconds, the new UMS is registered. If you toggle the sorting by **Updated**, your newly registered UMS should be displayed on top.



☰ UMS Management

All > Account = [redacted] Test Company

UMS Name	X.509 Certificate	Expiration Date	Fingerprint	Enable App Portal	Created by(owned_by)	Created	Updated
UMS Ike	[redacted]	2042-04-09 06:10:55	[redacted]	true	[redacted]	2023-04-14 12:28:39	2023-04-14 12:28:39
[redacted]	[redacted]	2042-05-19 10:10:47	[redacted] ..	true	[redacted]	2023-03-31 11:45:02	2023-04-11 14:28:42
[redacted]	[redacted]	2042-06-04 12:10:30	[redacted]	true	[redacted]	2023-04-11 11:27:51	2023-04-11 11:27:51

Initial Configuration of the IGEL Onboarding Service (OBS)

For onboarding your users and devices, IGEL Cloud Services need to know your UMS and your users. The UMS is identified and authenticated by its fully qualified domain name (FQDN) or IP address and its root certificate. The users are authenticated by an external identity provider (IdP). For that, we are using the OpenID Standard to obtain user information and the standardised OAuth 2.0 authorisation protocols. Please follow our instructions to register the OBS as an app in your Microsoft Entra ID, Ping Identity, Okta or other IdP.

If you want to register your remote IGEL OS 12 devices via IGEL Onboarding Service and you use IGEL Cloud Gateway (ICG), you need to connect the IGEL Onboarding Service not with the UMS, but with the ICG. The ICG version 12.01 or higher is required.

The configuration of the Onboarding Service is done in the followings steps:

1. Activating the Onboarding Service (OBS)(see page 41)
2. Configuring the Identity Provider(see page 41)
3. Downloading the Root Certificate Chain of the UMS / ICG(see page 42): The root certificate chain is needed for defining the route to the appropriate UMS / ICG.
4. Creating the Record Set for the OBS Routing(see page 46): Define the route to the appropriate UMS / ICG. This includes linking our Microsoft Entra ID user to the UMS / ICG.

Activating the Onboarding Service (OBS)

> ⓘ The activation of the Onboarding Service (OBS) is required once and must be performed by one person from the company account. Once activated, the OBS can be managed by every user with the appropriate rule.

1. Log in to the IGEL Customer Portal[15].
2. From the menu, select **Activate IGEL OS Onboarding**.

Configuring the Identity Provider

For the instructions on how to register the OBS as an app in your Microsoft Entra ID, Ping Identity, or Okta, see:

- Microsoft Entra ID(see page 54)
- Okta(see page 79)
- Ping Identity(see page 91)

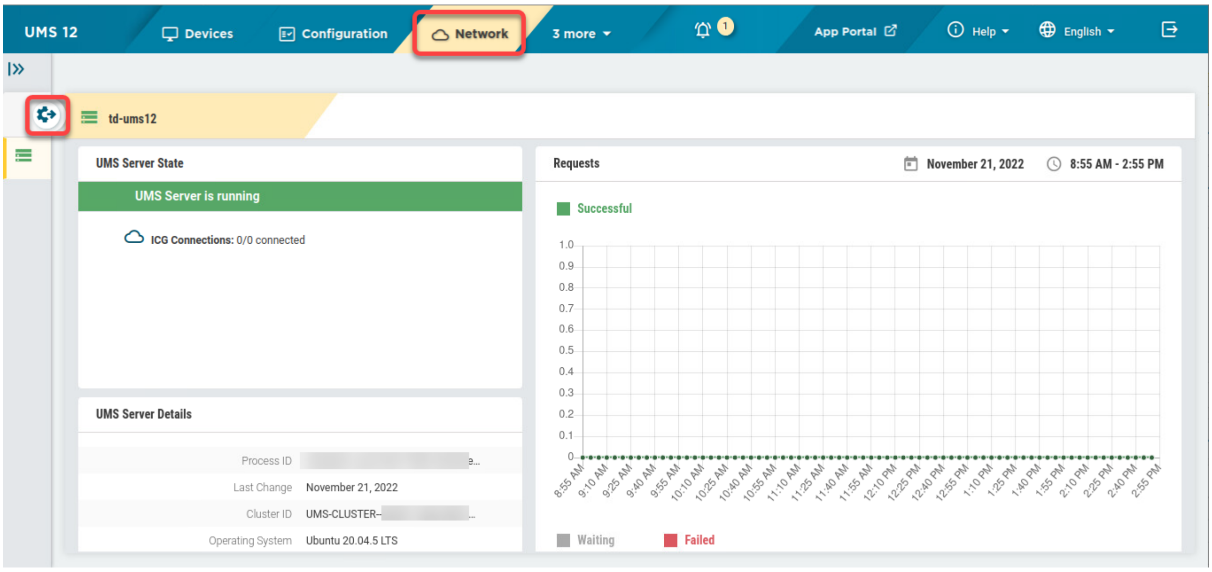
[15] https://cosmos.igel.com/

Downloading the Root Certificate Chain

If your UMS is to be connected directly to your endpoint devices, you download the certificate chain of the UMS; see Of the UMS(see page 42). If your UMS is to be connected via ICG, you download the certificate chain of the ICG; Of the ICG(see page 43).

Of the UMS

1. Open the UMS Web App of the UMS at which our OBS routing will be directed, select **Network** and click .



UMS Server is running

ICG Connections: 0/0 connected

Process ID [redacted]e...

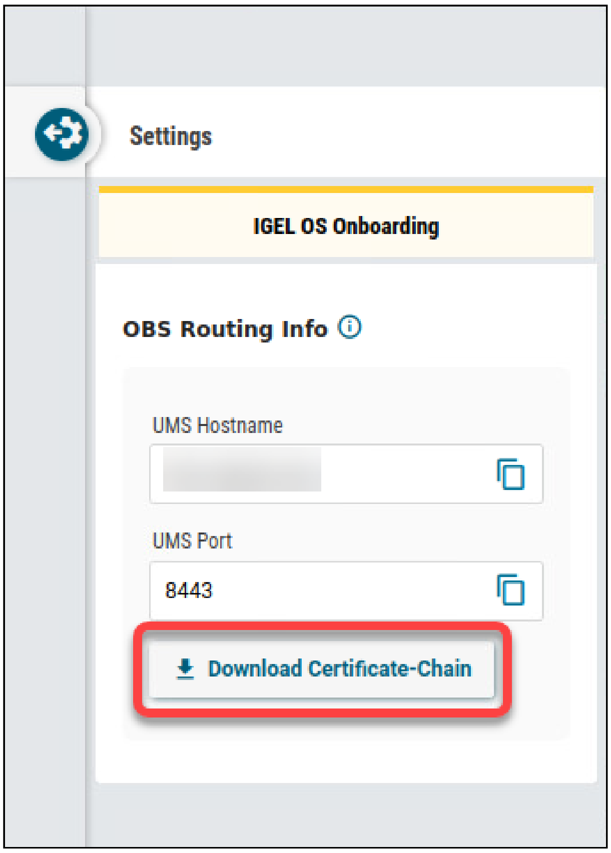
Last Change November 21, 2022

Cluster ID UMS-CLUSTER-[redacted]...

Operating System Ubuntu 20.04.5 LTS

2. Select the tab **IGEL OS Onboarding** and copy **UMS Hostname** and **UMS Port**.

3. Click **Download Certificate Chain**.



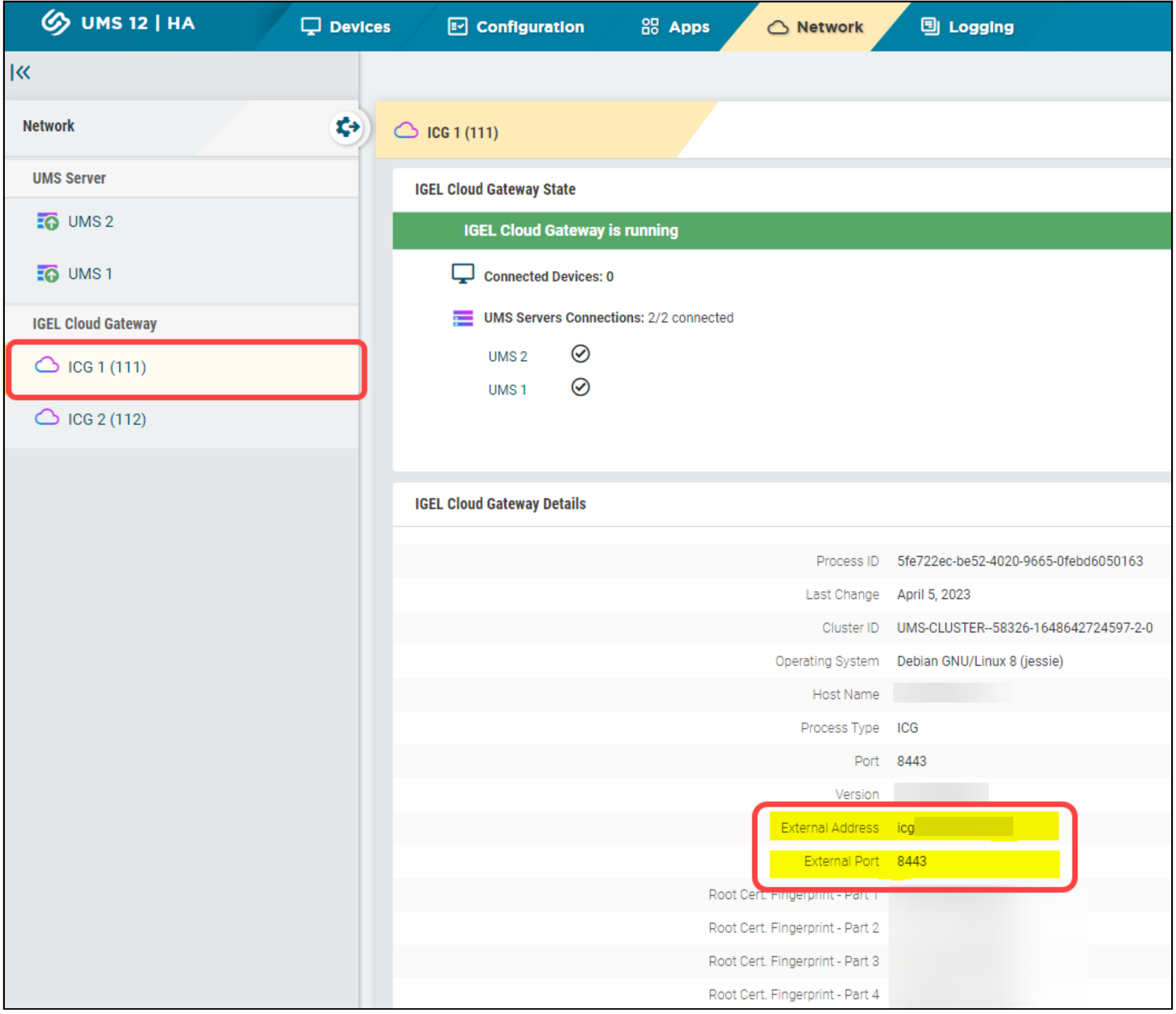
The certificate file is downloaded to your file system. In the following step, we will use it for the OBS routing.

Of the ICG (Required Only If the OBS Is Used with the ICG)

1. In the **UMS Web App > Network**, navigate to the **IGEL Cloud Gateway** area and select the ICG server to which you want to connect the OBS.

> ⓘ If you have multiple ICG servers, it is possible to direct the OBS routing to one server only.

2. Copy the data from the fields **External Address** and **External Port**.



IGEL Cloud Gateway State

IGEL Cloud Gateway is running

Connected Devices: 0

UMS Servers Connections: 2/2 connected

UMS 2 ✓

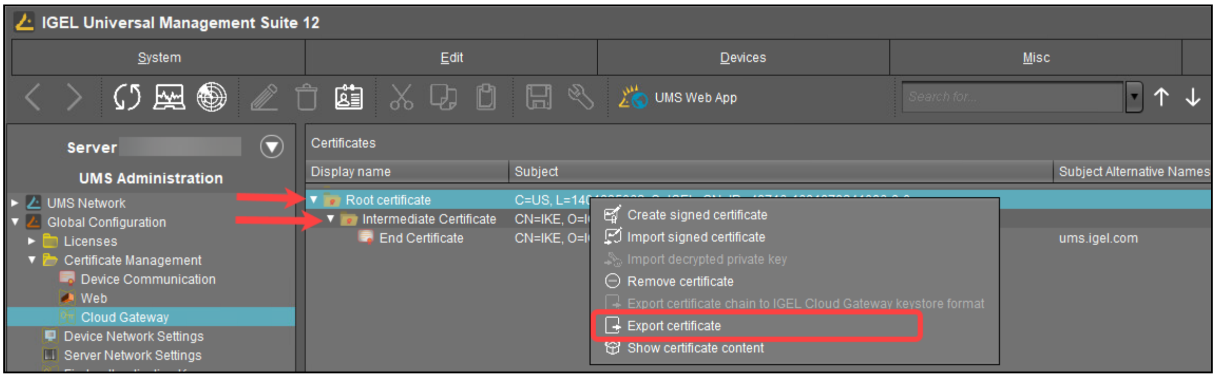
UMS 1 ✓

IGEL Cloud Gateway Details

Process ID	5fe722ec-be52-4020-9665-0febd6050163
Last Change	April 5, 2023
Cluster ID	UMS-CLUSTER--58326-1648642724597-2-0
Operating System	Debian GNU/Linux 8 (jessie)
Host Name	[redacted]
Process Type	ICG
Port	8443
Version	[redacted]
External Address	icg[redacted]
External Port	8443
Root Cert. Fingerprint - Part 1	[redacted]
Root Cert. Fingerprint - Part 2	[redacted]
Root Cert. Fingerprint - Part 3	[redacted]
Root Cert. Fingerprint - Part 4	[redacted]

3. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway**.

4. Export each certificate of the ICG's chain except for the end certificate: Right-click the certificate and select **Export certificate** in the context menu.

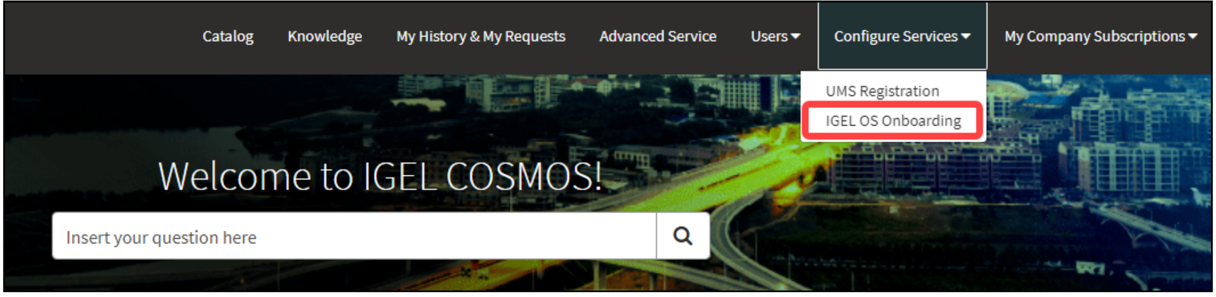


5. Copy the contents of each exported certificate in one file (the order of the certificates does not matter) and save the file as `icg_chain.crt`.
   Example:

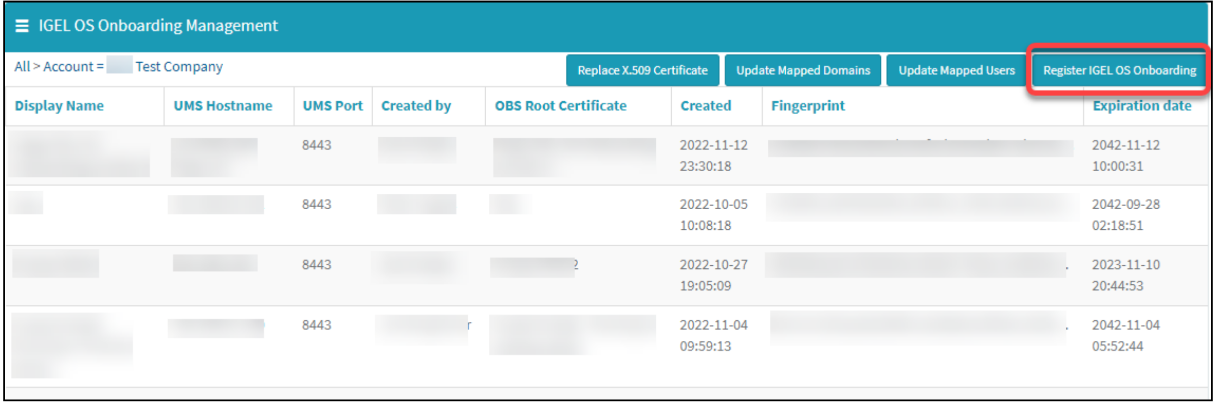
```
-----BEGIN CERTIFICATE-----
MIIFPTCCAyWgAwIBAgIFAIGKvrEwDQYJKoZIhvcNAQELBQAwVzEkMCIGA1UEAwwbSUQtLTQ5NzE2
LTE2ODE5NzkyNDEwOTYtOC0wMQ0wCwYDVQQKDARJR0VMMRMwEQYDVQQHDAoxNDAxODM1MDYyMQsw
.......................................
jqzhUGI+dZyTguXkzM2T4ACJUVm7G3mWDSCuMpt5laaE8kGEB2J6cbY9qV4QA5giCKFO1PgJ6mQZ
3kDHoNX9DlKSyJtAWS6CJaaGWMWX0wtuyEQ5sZ81UhGKnQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFMDCCAxigAwIBAgIFAPAz/aEwDQYJKoZIhvcNAQELBQAwVzEkMCIGA1UEAwwbSUQtLTQ5NzE2
LTE2ODE5NzkyNDEwOTYtOC0wMQ0wCwYDVQQKDARJR0VMMRMwEQYDVQQHDAoxNDAxODM1MDYyMQsw
........................................
wy/0Y3S4LVHhWtAiT1dBza97uWk9zKL65HbwPFwwZ021Pjb2NaWJPL+OEAHPpk5eamCmFzJeUQqe
0pwHv6AgvJyfEuxsMHURs98psMhW
-----END CERTIFICATE-----
```

Creating the Record Set for the OBS Routing

1. Change to the IGEL Customer Portal and select **Configure Services > IGEL OS Onboarding**.



2. Click **Register IGEL OS Onboarding** to create a new routing data record.

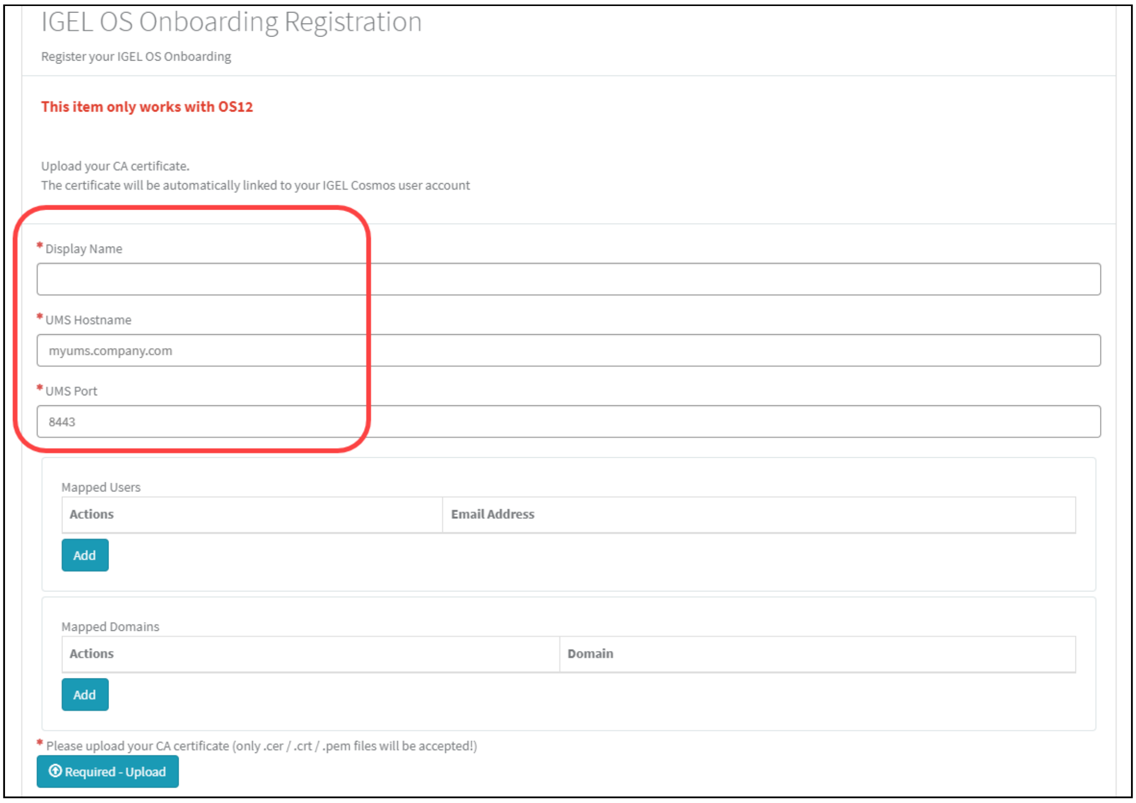

IGEL OS Onboarding Management
All > Account = [redacted] Test Company
Replace X.509 Certificate
Update Mapped Domains
Update Mapped Users
Register IGEL OS Onboarding

Display Name	UMS Hostname	UMS Port	Created by	OBS Root Certificate	Created	Fingerprint	Expiration date
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-11-12 23:30:18	[redacted]	2042-11-12 10:00:31
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-10-05 10:08:18	[redacted]	2042-09-28 02:18:51
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-10-27 19:05:09	[redacted]	2023-11-10 20:44:53
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-11-04 09:59:13	[redacted]	2042-11-04 05:52:44

3. Enter the following data:
   - **Display Name**: Display name for the UMS to which our user's device will be routed.
   - **UMS Hostname**: Hostname (Fully Qualified Domain Name) or IP address of the UMS; this is the hostname or IP address by which the UMS can be reached by the endpoint devices.
     If your endpoint devices are connected via the ICG, use the External Address of the ICG as described above(see page 43).

     > ⓘ **UMS Hostname** is case-sensitive and should be written exactly as in the UMS.

   - **UMS Port**: Port under which the UMS can be reached. The default port of the UMS web server is 8443. For details on the ports used by the UMS, see IGEL UMS Communication Ports.
     If your endpoint devices are connected via the ICG, use the External Port of the ICG as described above(see page 43).



IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

Upload your CA certificate.
The certificate will be automatically linked to your IGEL Cosmos user account

* Display Name

* UMS Hostname

myums.company.com

* UMS Port

8443

Mapped Users

Actions	Email Address

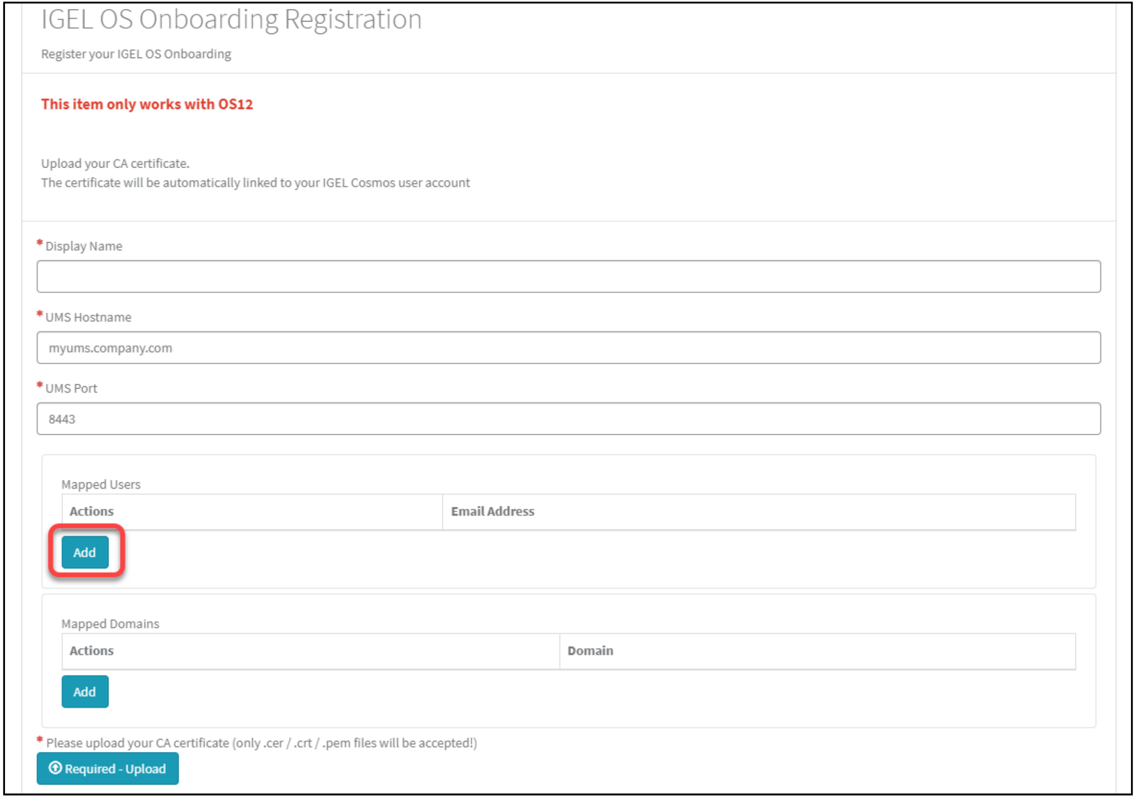
Mapped Domains

Actions	Domain

* Please upload your CA certificate (only .cer / .crt / .pem files will be accepted!)

4. Proceed by adding individual users or one or more domains that include all e-mail addresses of these domains.

- To add an individual user, click **Add** in the area **Mapped Users**.



IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

Upload your CA certificate.
The certificate will be automatically linked to your IGEL Cosmos user account

* Display Name

* UMS Hostname

myums.company.com

* UMS Port

8443

Mapped Users

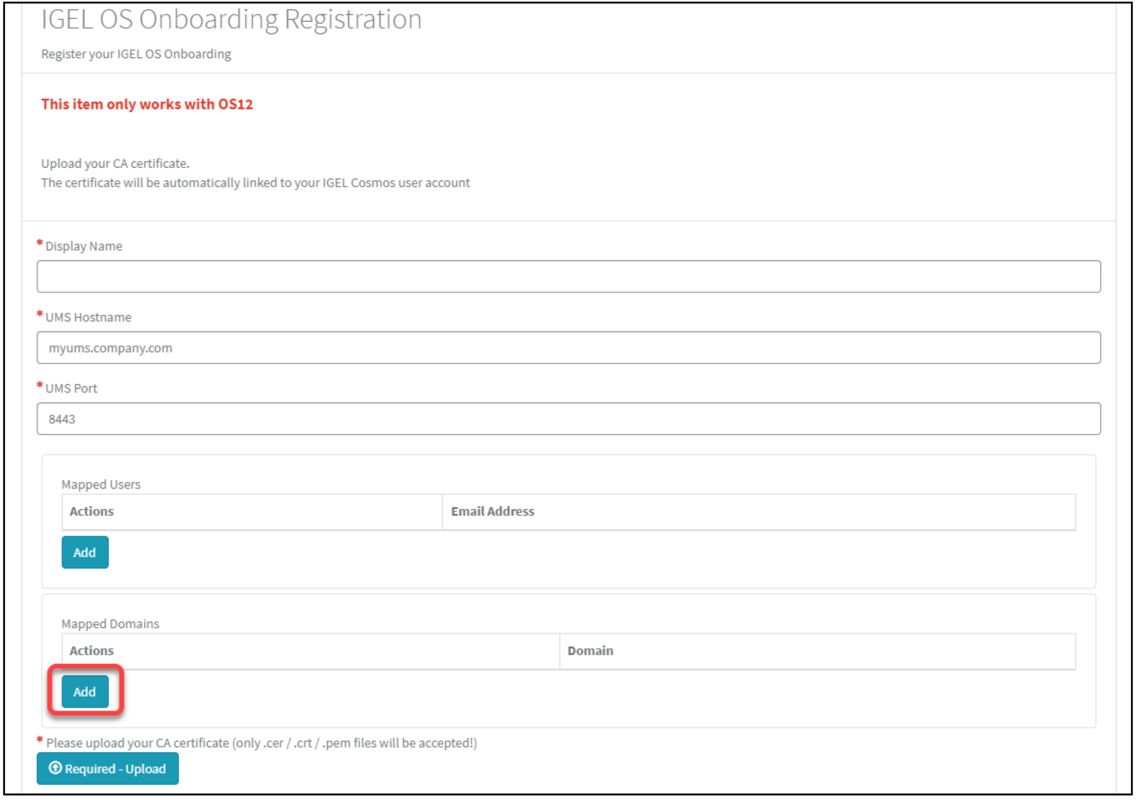
Actions	Email Address

Mapped Domains

Actions	Domain

* Please upload your CA certificate (only .cer / .crt / .pem files will be accepted!)

- To add a domain, click **Add** in the area **Mapped Domains**.



IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

Upload your CA certificate.
The certificate will be automatically linked to your IGEL Cosmos user account

* Display Name

* UMS Hostname

myums.company.com

* UMS Port

8443

Mapped Users

Actions	Email Address

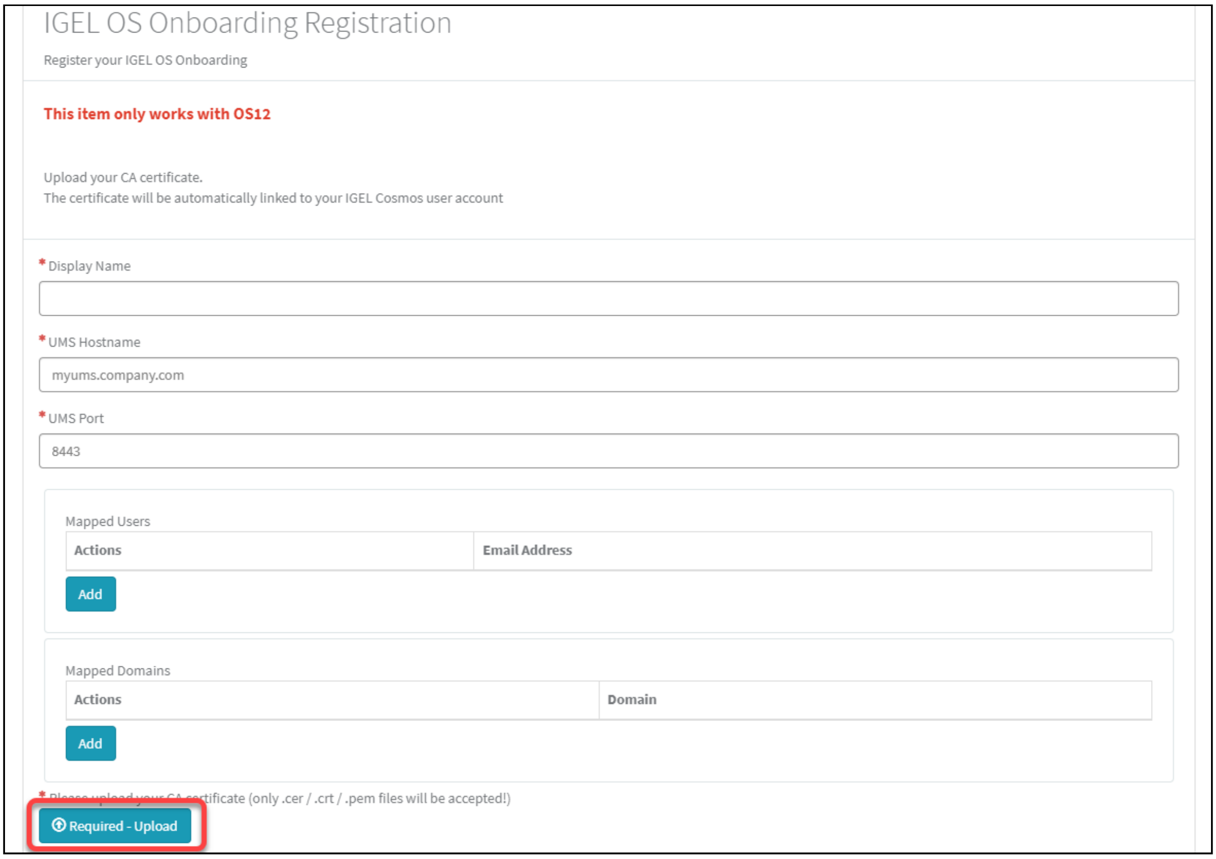
Mapped Domains

Actions	Domain

* Please upload your CA certificate (only .cer / .crt / .pem files will be accepted!)

5. In the dialog, enter the e-mail address of the user we have created in Microsoft Entra ID or the relevant domain and click **Add**.

6. Click **Required - Upload** to upload the UMS root certificate chain.
If you want to use the OBS with the ICG, use here the file `icg_chain.crt` you obtained as described above(see page 43).



IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

Upload your CA certificate.
The certificate will be automatically linked to your IGEL Cosmos user account

* Display Name

* UMS Hostname

myums.company.com

* UMS Port

8443

Mapped Users

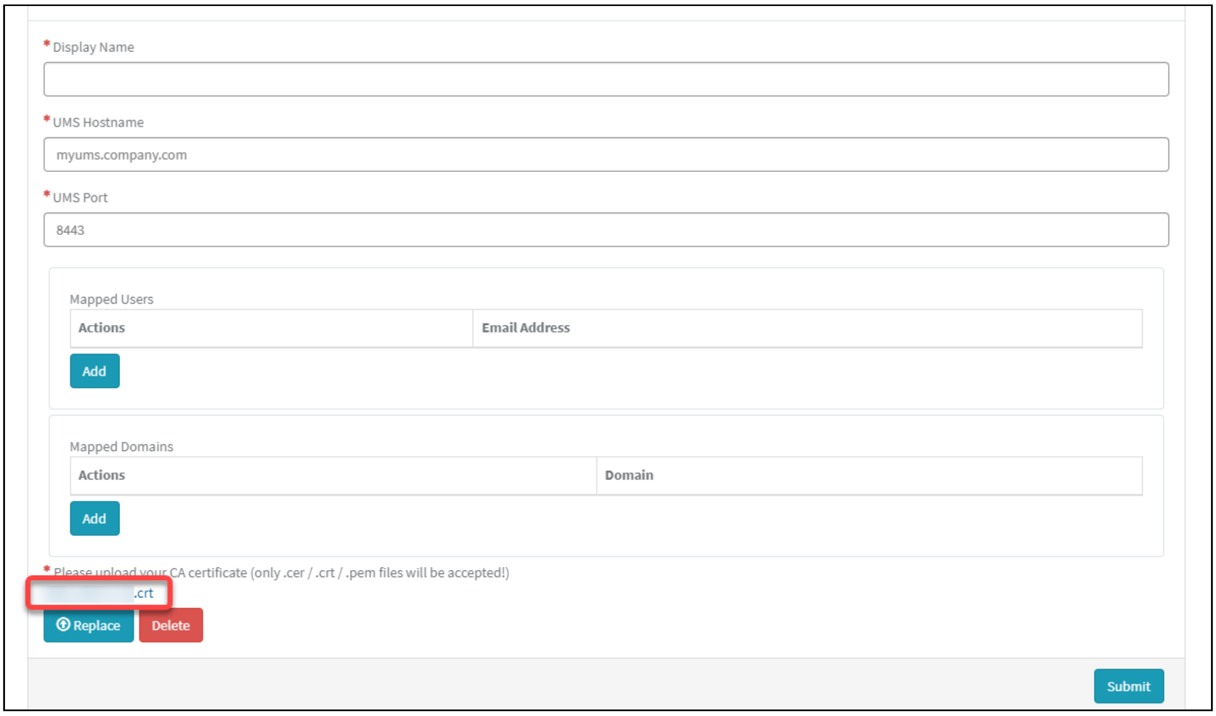
Actions	Email Address

Mapped Domains

Actions	Domain

* Please upload your CA certificate (only .cer / .crt / .pem files will be accepted!)

7. Choose the certificate file on your file system.
   The certificate file is uploaded.



* Display Name

* UMS Hostname: myums.company.com

* UMS Port: 8443

Mapped Users

Actions	Email Address

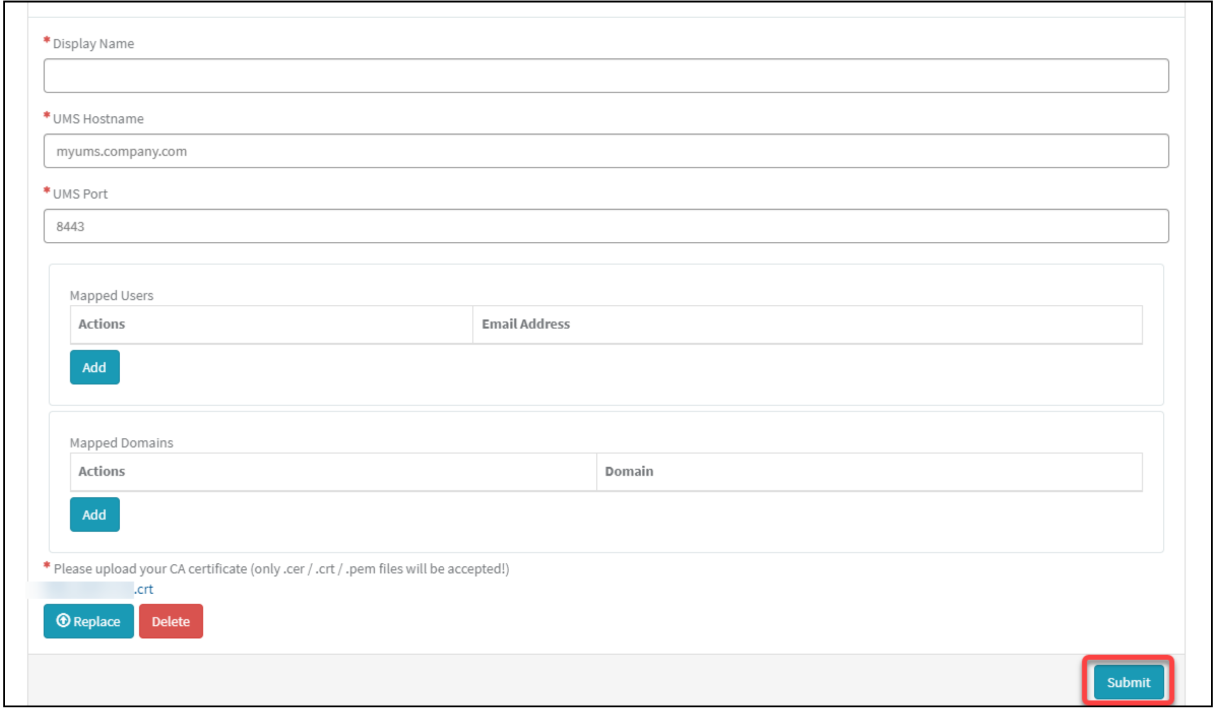
Mapped Domains

Actions	Domain

* Please upload your CA certificate (only .cer / .crt / .pem files will be accepted!)

[redacted].crt

8. Click **Submit** to create the OBS routing data record.



* Display Name

* UMS Hostname: myums.company.com

* UMS Port: 8443

Mapped Users

Actions	Email Address

Mapped Domains

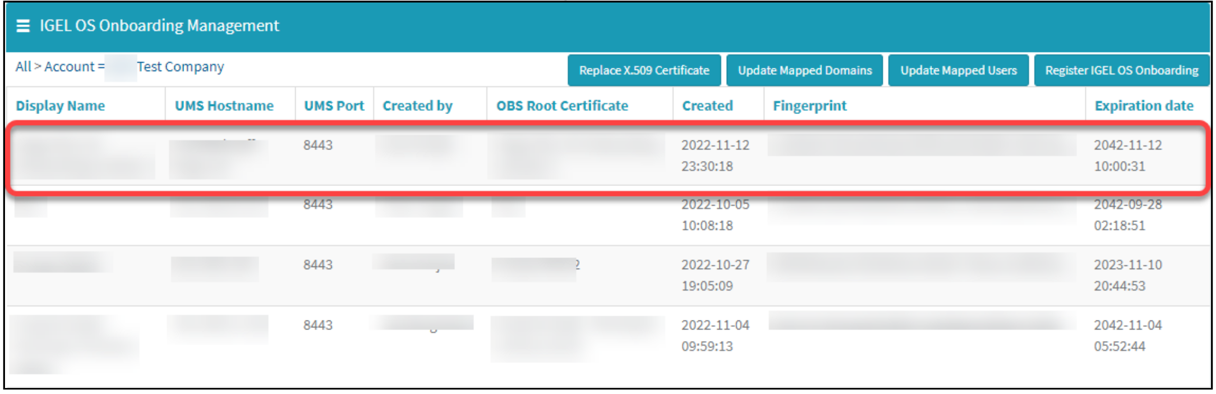
Actions	Domain

* Please upload your CA certificate (only .cer / .crt / .pem files will be accepted!)

[redacted].crt

After a few seconds, the new data record is ready.

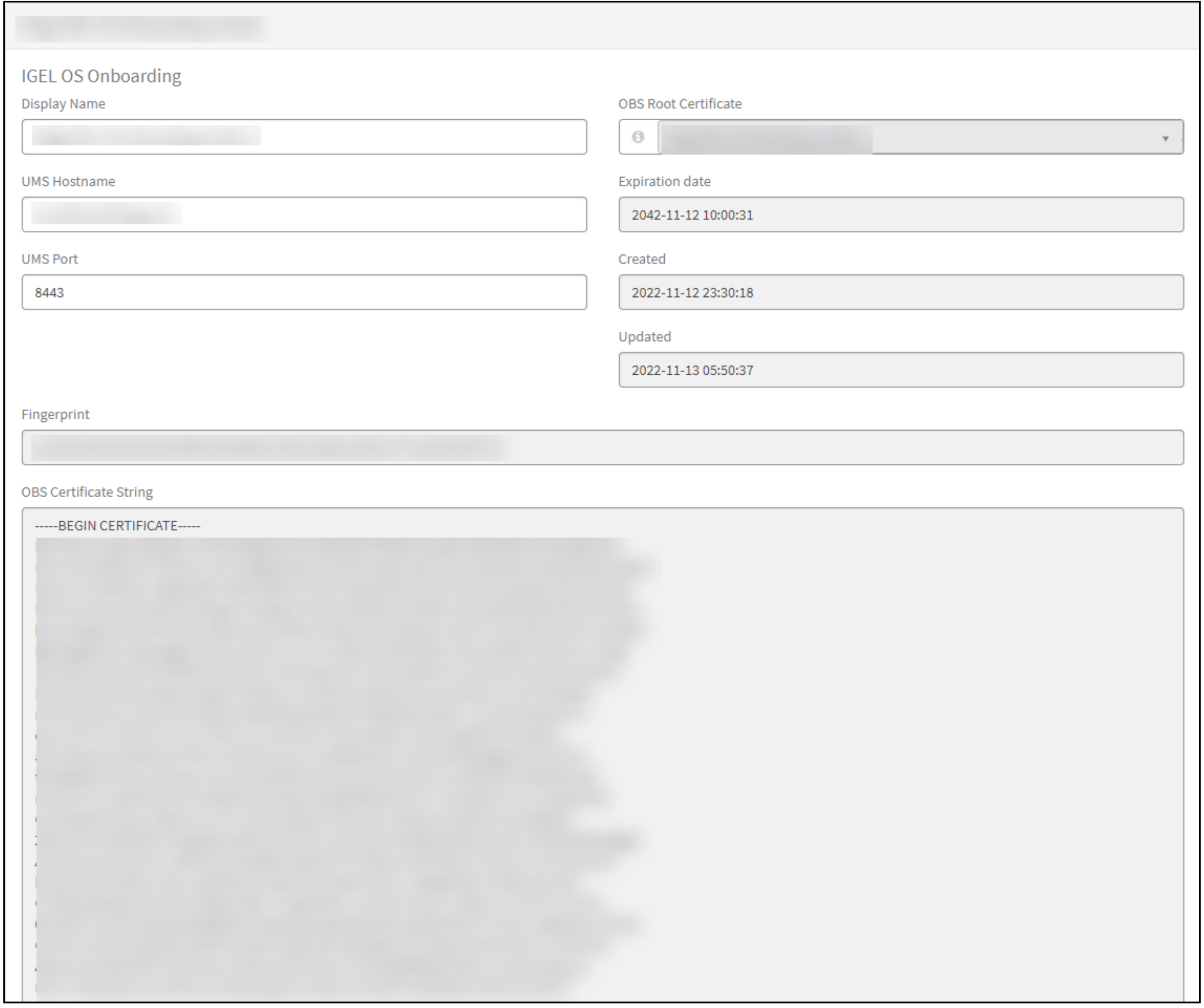
9. If you want to review the record or make changes, just click somewhere in the record.



≡ IGEL OS Onboarding Management
All > Account = [redacted] Test Company
Replace X.509 Certificate
Update Mapped Domains
Update Mapped Users
Register IGEL OS Onboarding

Display Name	UMS Hostname	UMS Port	Created by	OBS Root Certificate	Created	Fingerprint	Expiration date
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-11-12 23:30:18	[redacted]	2042-11-12 10:00:31
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-10-05 10:08:18	[redacted]	2042-09-28 02:18:51
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-10-27 19:05:09	[redacted]	2023-11-10 20:44:53
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-11-04 09:59:13	[redacted]	2042-11-04 05:52:44

The details are displayed.



[redacted]

IGEL OS Onboarding

Display Name: [redacted]

OBS Root Certificate: [redacted]

UMS Hostname: [redacted]

Expiration date: 2042-11-12 10:00:31

UMS Port: 8443

Created: 2022-11-12 23:30:18

Updated: 2022-11-13 05:50:37

Fingerprint: [redacted]

OBS Certificate String

-----BEGIN CERTIFICATE-----
[redacted]

You can update the certificate and update/add associated e-mails.

The user can now be onboarded. The onboarding process from the user's view is described under Onboarding IGEL OS 12 Devices(see page 158).

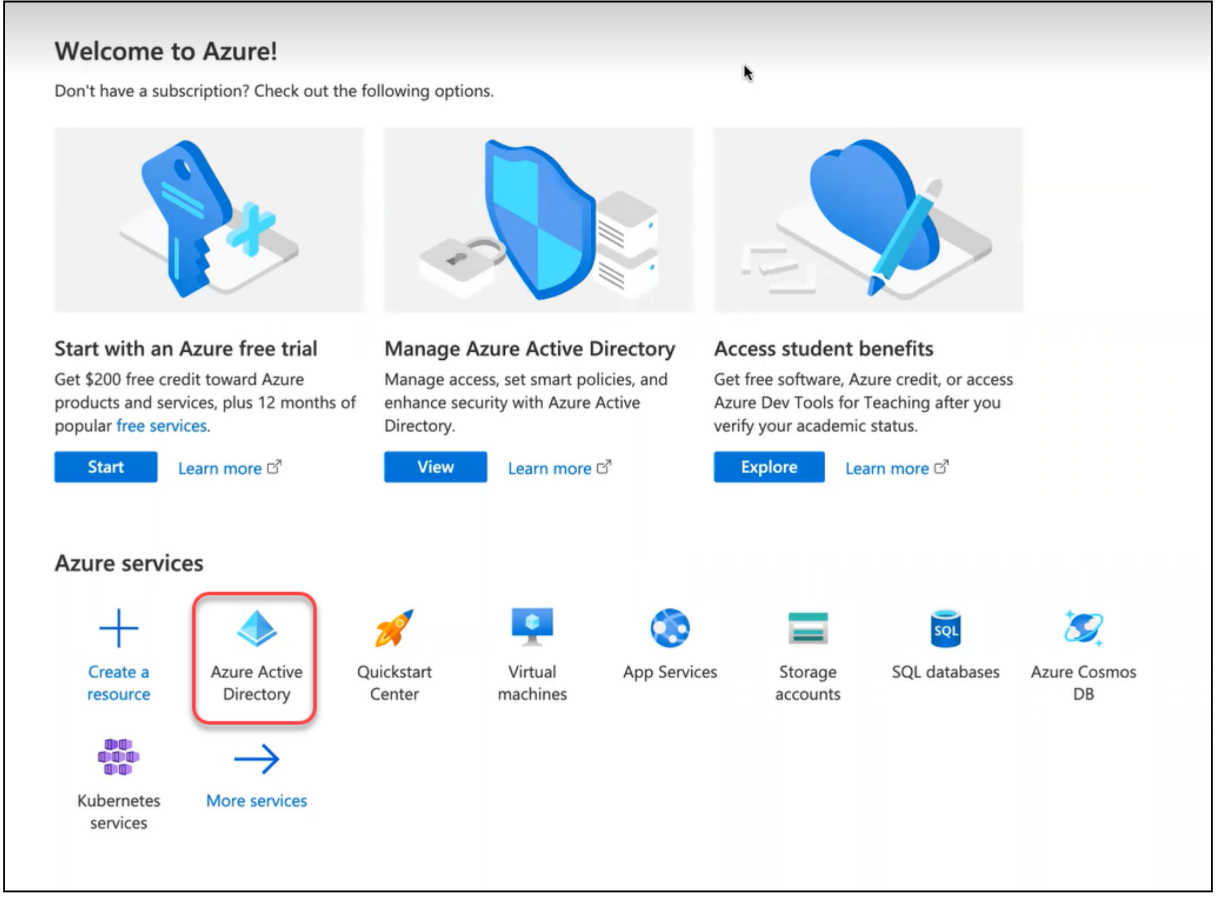
Configuring Microsoft Entra ID as Identity Provider

To configure Microsoft Entra ID as the identity provider, you need to do the following:

1. Creating a Microsoft Entra Web Application That Will Serve as Identity Provider(see page 54): We register an application in Microsoft Entra ID to use its services as an external identity provider.
2. Registering Our Microsoft Entra Application in the IGEL Customer Portal(see page 60): This will enable IGEL Cloud Services to use our Microsoft Entra Application as the external identity provider.
3. Creating a User in the Microsoft Entra App(see page 77): We create a user account in our application. These user credentials, consisting of an e-mail address and a password, will be entered by the user when onboarding his device.

Creating a Web Application That Will Serve as Identity Provider

1. Log in to your Microsoft Entra account and select the Microsoft Entra ID resource.



Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial

Get $200 free credit toward Azure products and services, plus 12 months of popular free services.

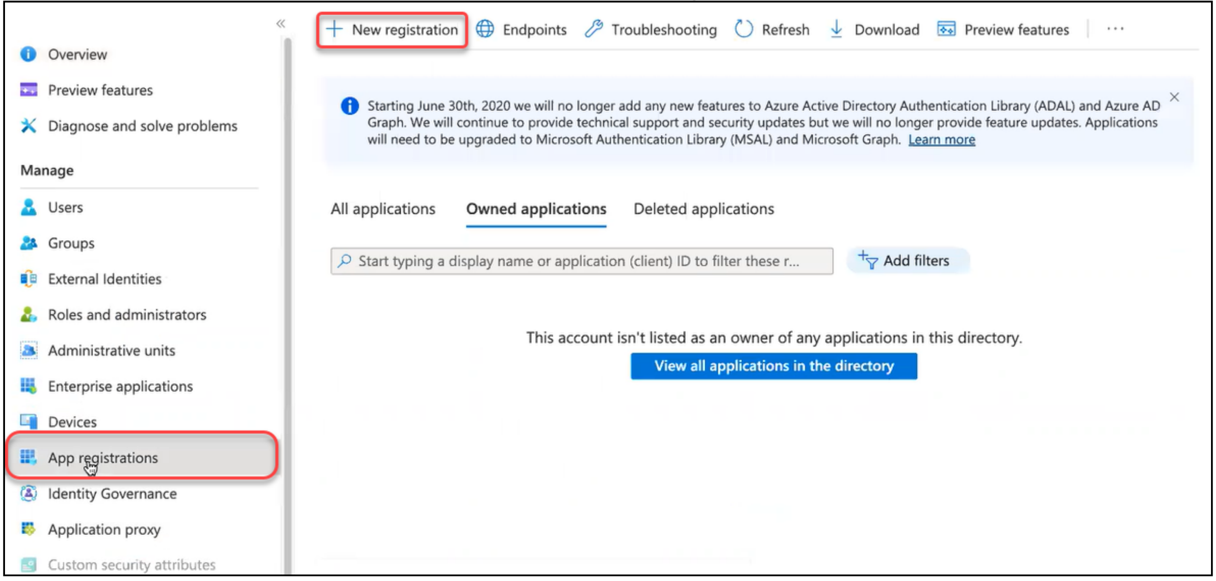
Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

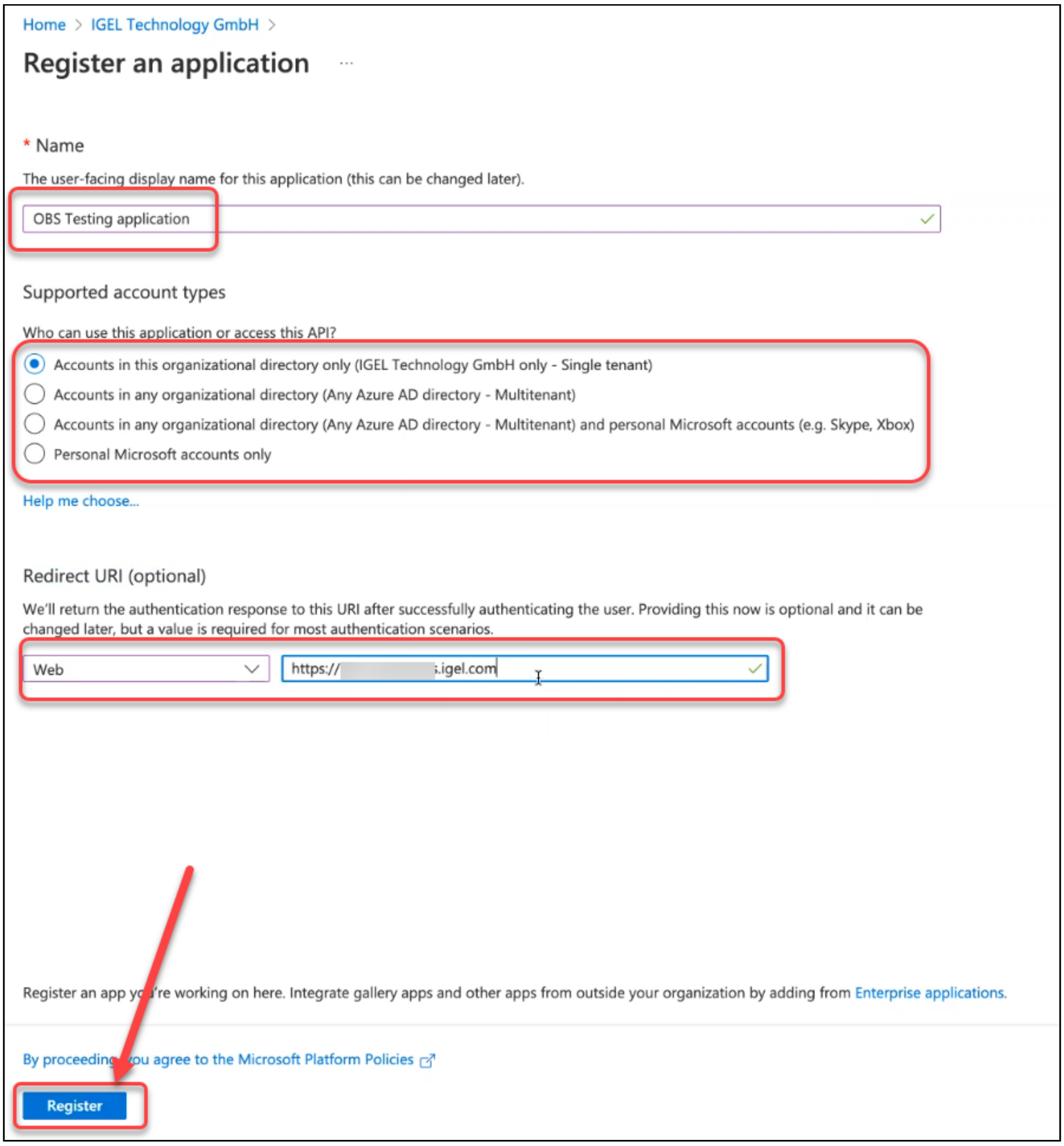
2. Click **App registrations** and then **new registration** to register a new app.



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

This account isn't listed as an owner of any applications in this directory.

3. Edit the data as follows and then click **Register**:
   - **Name**: Display name for the app
   - **Supported account types**: Set the permissions according to your requirements.
   - **Redirect URI (optional)**: For our purposes, this setting is not optional but required. Set the first field to **Web** and, in the second field, provide the URI of the onboarding service. This is "https://obs.services.igel.com/".



Home > IGEL Technology GmbH >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

OBS Testing application ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (IGEL Technology GmbH only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

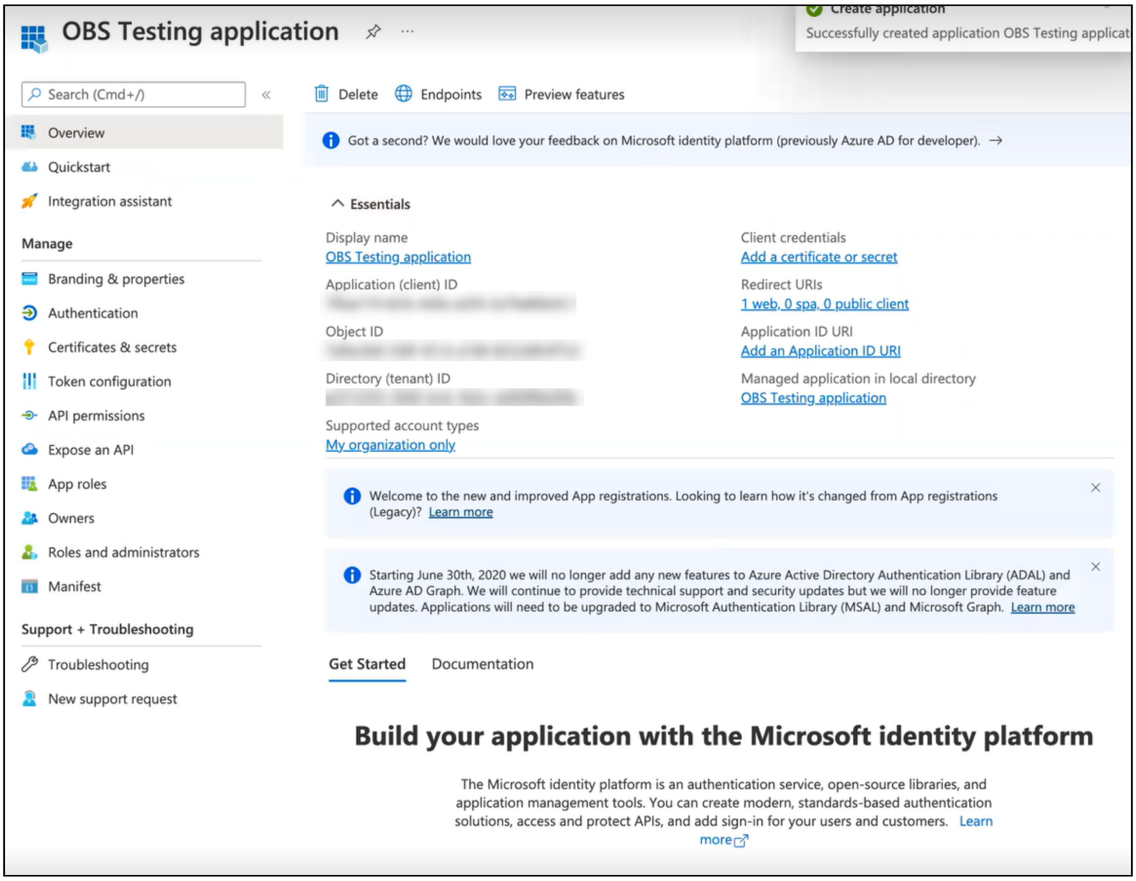
Web | https://[redacted].igel.com ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

The application is created.

When you are creating the user accounts for onboarding, consider the following note:



OBS Testing application

Create application
Successfully created application OBS Testing applicat

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name: OBS Testing application

Application (client) ID: [redacted]

Object ID: [redacted]

Directory (tenant) ID: [redacted]

Supported account types: My organization only

Client credentials: Add a certificate or secret

Redirect URIs: 1 web, 0 spa, 0 public client

Application ID URI: Add an Application ID URI

Managed application in local directory: OBS Testing application

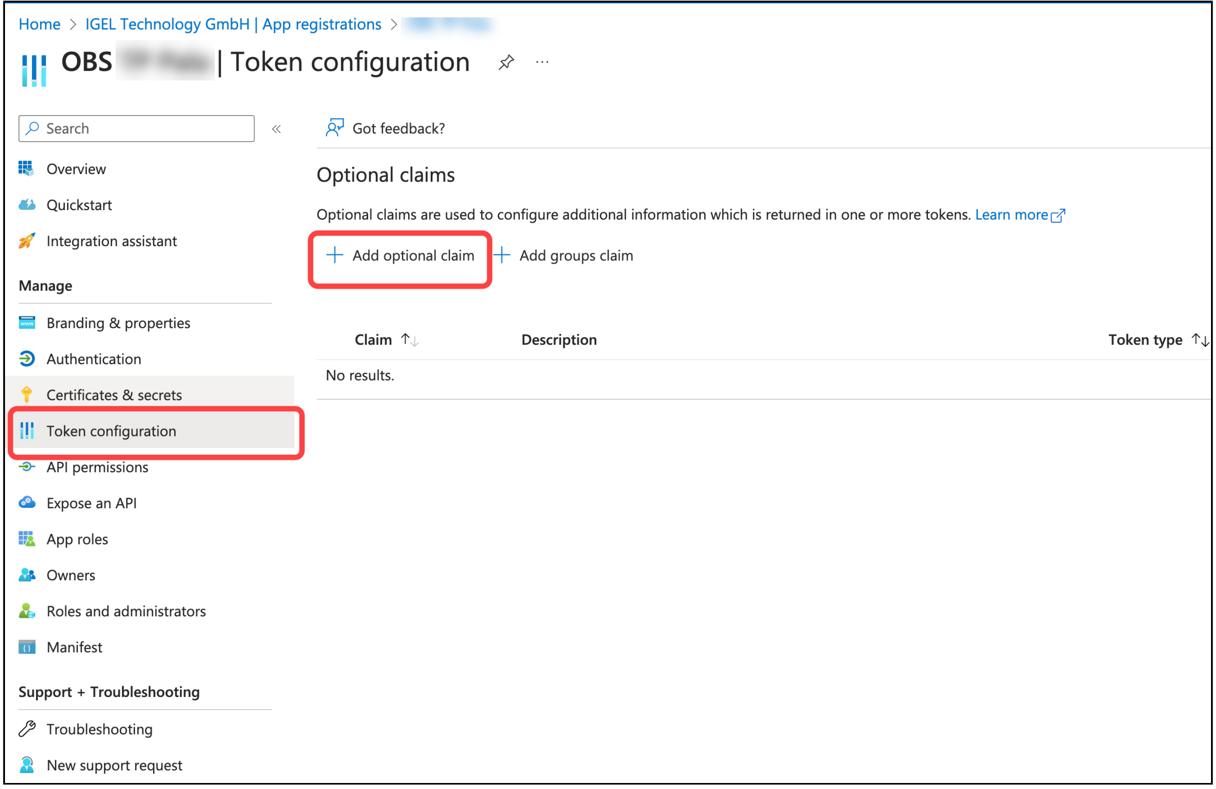
Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

4. Click **Token configuration** and then **Add optional claim**.



Home > IGEL Technology GmbH | App registrations > [redacted]

OBS [redacted] | Token configuration

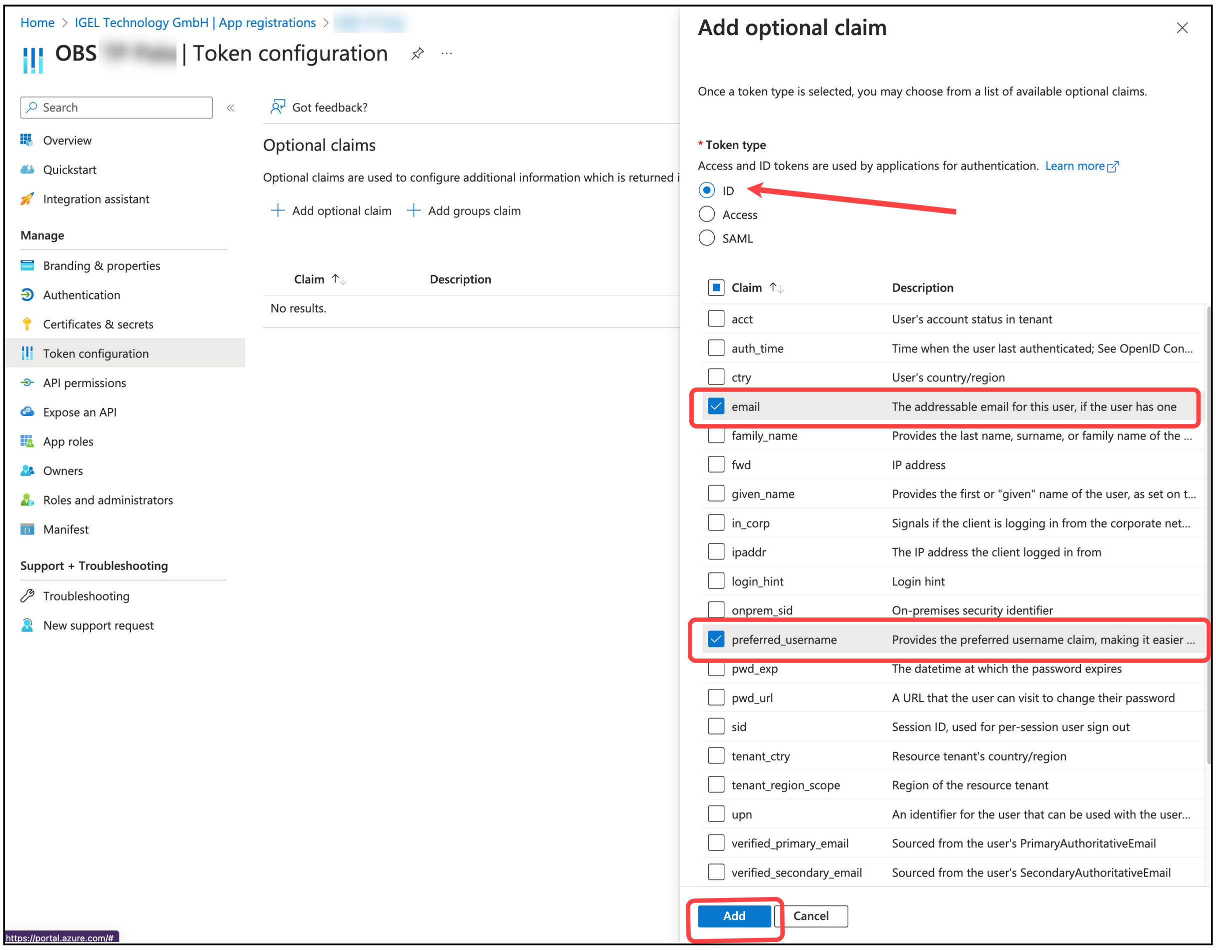
Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑↓	Description	Token type ↑↓
No results.		

5. In the **Add optional claim** window, select **ID** under **Token type** and activate:
   - **email**
   - **preferred_username**

6. Click **Add**.



Optional claims

Optional claims are used to configure additional information which is returned i

+ Add optional claim + Add groups claim

Claim ↑↓	Description
No results.	

Add optional claim

Once a token type is selected, you may choose from a list of available optional claims.

* Token type

Access and ID tokens are used by applications for authentication. Learn more

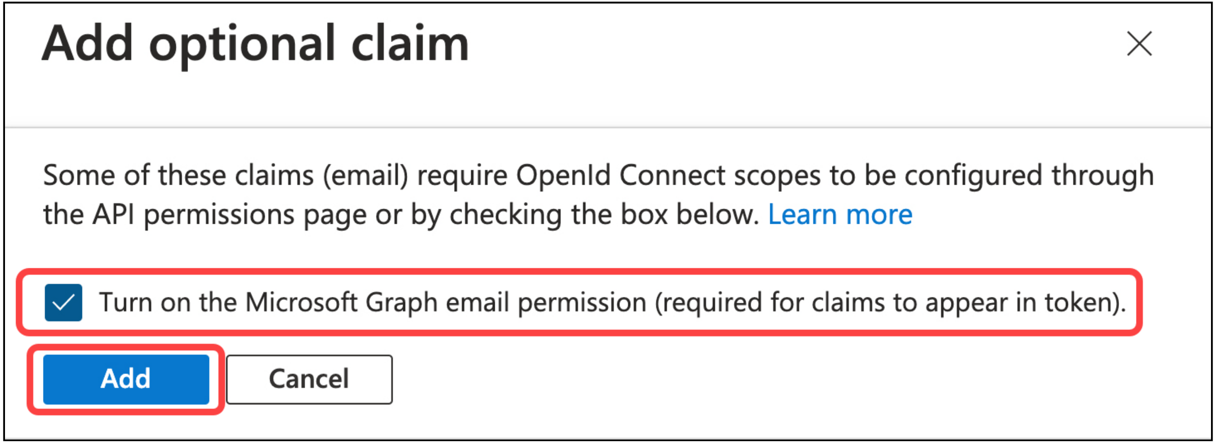
● ID

○ Access

○ SAML

■ Claim ↑↓	Description
□ acct	User's account status in tenant
□ auth_time	Time when the user last authenticated; See OpenID Con...
□ ctry	User's country/region
☑ email	The addressable email for this user, if the user has one
□ family_name	Provides the last name, surname, or family name of the ...
□ fwd	IP address
□ given_name	Provides the first or "given" name of the user, as set on t...
□ in_corp	Signals if the client is logging in from the corporate net...
□ ipaddr	The IP address the client logged in from
□ login_hint	Login hint
□ onprem_sid	On-premises security identifier
☑ preferred_username	Provides the preferred username claim, making it easier ...
□ pwd_exp	The datetime at which the password expires
□ pwd_url	A URL that the user can visit to change their password
□ sid	Session ID, used for per-session user sign out
□ tenant_ctry	Resource tenant's country/region
□ tenant_region_scope	Region of the resource tenant
□ upn	An identifier for the user that can be used with the user...
□ verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
□ verified_secondary_email	Sourced from the user's SecondaryAuthoritativeEmail

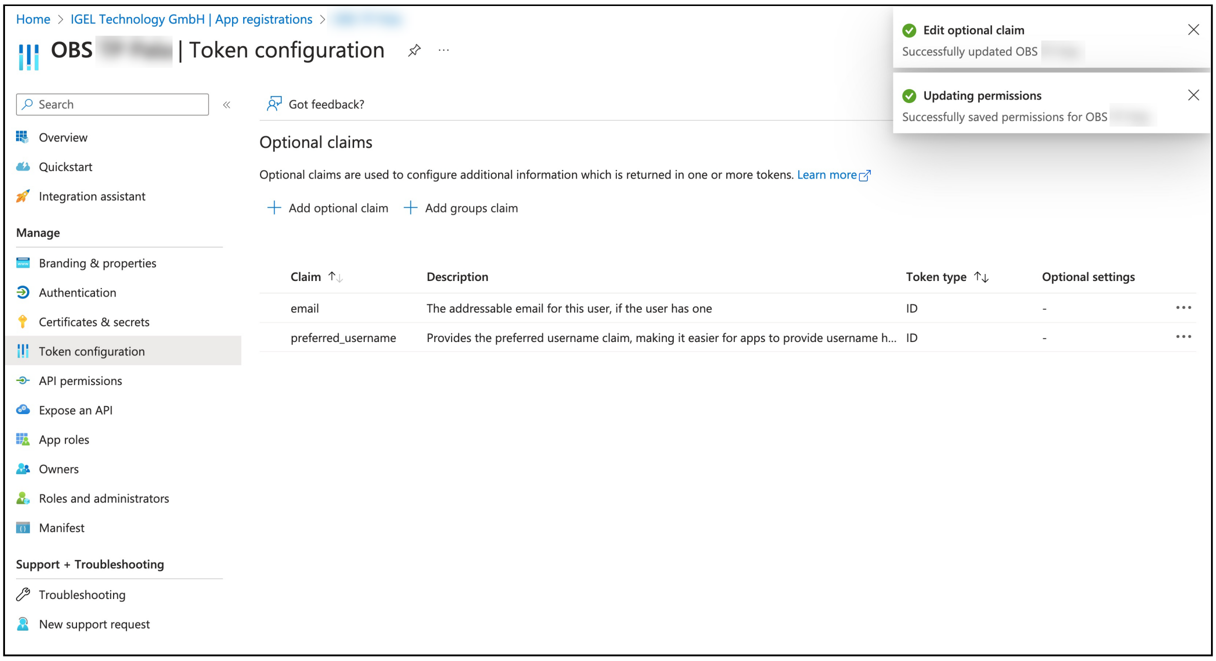
7. Activate **Turn on the Microsoft Graph email permission** and click **Add**.


Add optional claim

Some of these claims (email) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

☑ Turn on the Microsoft Graph email permission (required for claims to appear in token).

The token configuration is completed:



Home > IGEL Technology GmbH | App registrations > [redacted]

OBS [redacted] | Token configuration

Edit optional claim
Successfully updated OBS [redacted]

Updating permissions
Successfully saved permissions for OBS [redacted]

Optional claims

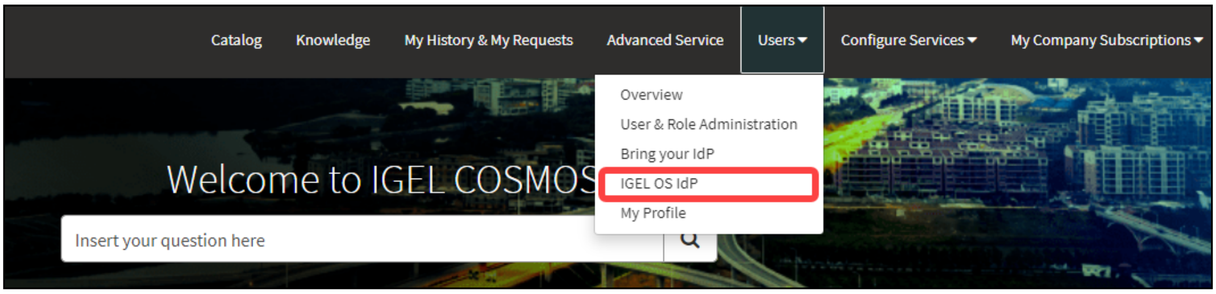
Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim ↑↓	Description	Token type ↑↓	Optional settings
email	The addressable email for this user, if the user has one	ID	-
preferred_username	Provides the preferred username claim, making it easier for apps to provide username h...	ID	-

8. Leave the browser tab open as we will need some of the data in the following steps.

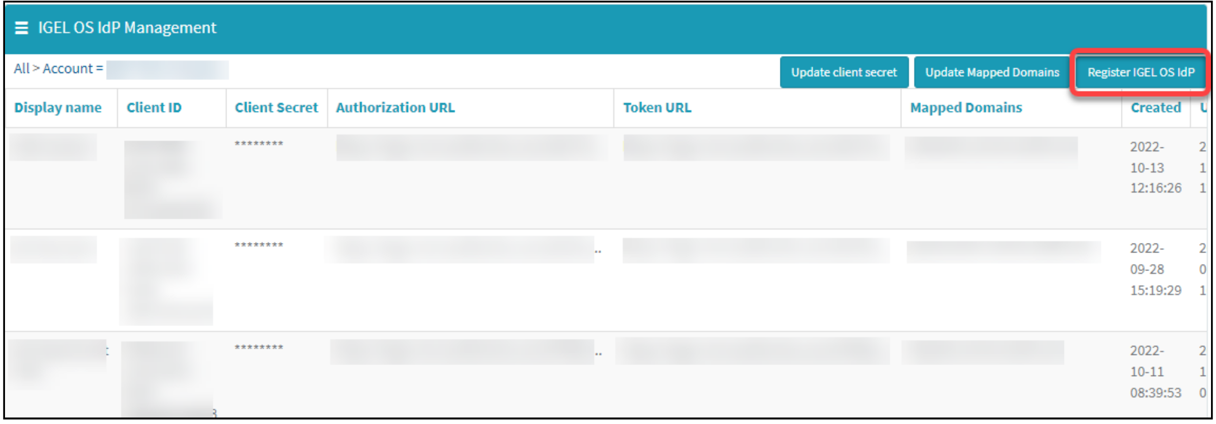
Registering Our Entra App in the IGEL Customer Portal

1. Open the IGEL Customer Portal[16] in your browser, log in to your admin account, and select **Users > IGEL OS IdP**.



[16] https://cosmos.igel.com/

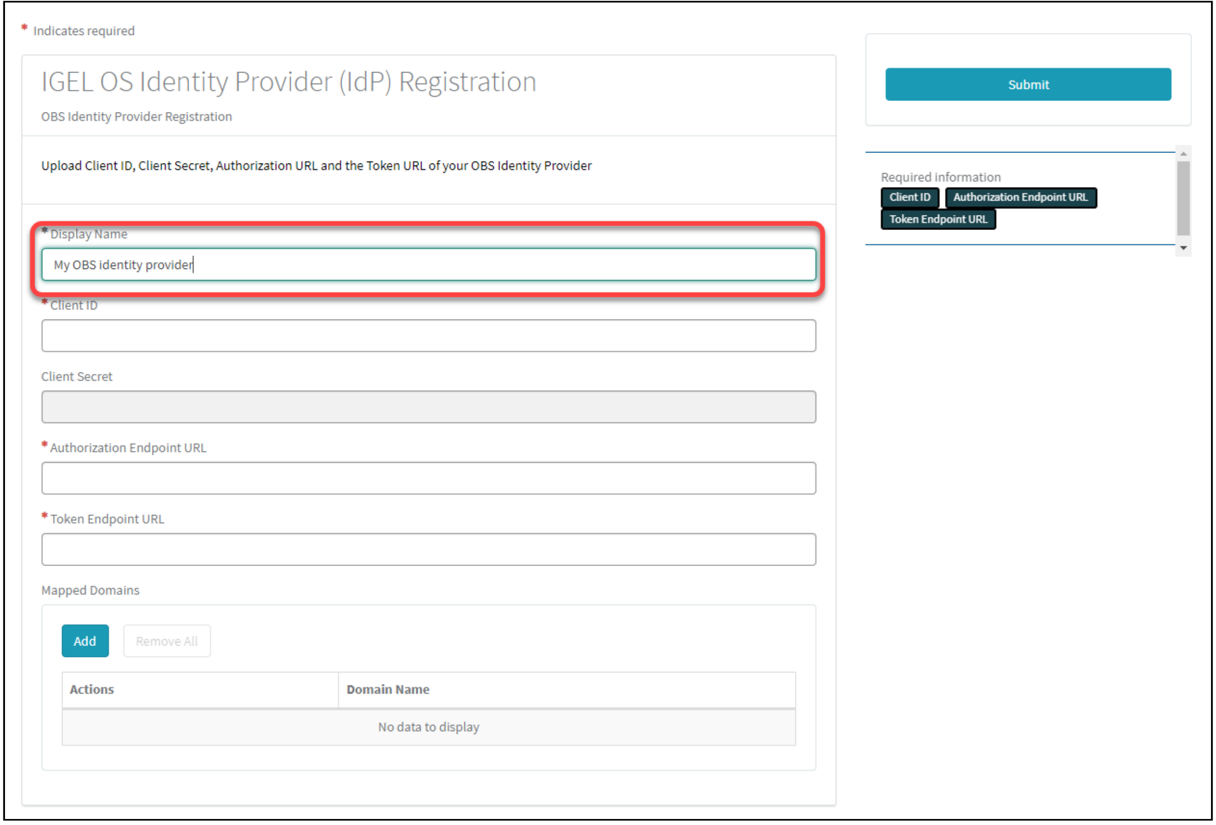
2. Click **Register IGEL OS IdP**.



All > Account = [redacted]

Display name	Client ID	Client Secret	Authorization URL	Token URL	Mapped Domains	Created	U
[redacted]	[redacted]	********	[redacted]	[redacted]	[redacted]	2022-10-13 12:16:26	2 1 1
[redacted]	[redacted]	********	[redacted]	[redacted]	[redacted]	2022-09-28 15:19:29	2 0 1
[redacted]	[redacted]	********	[redacted]	[redacted]	[redacted]	2022-10-11 08:39:53	2 1 0

3. Enter a **Display name**. This is the name under which your identity provider app will be displayed.



* Indicates required

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name: My OBS identity provider

* Client ID:

Client Secret:

* Authorization Endpoint URL:

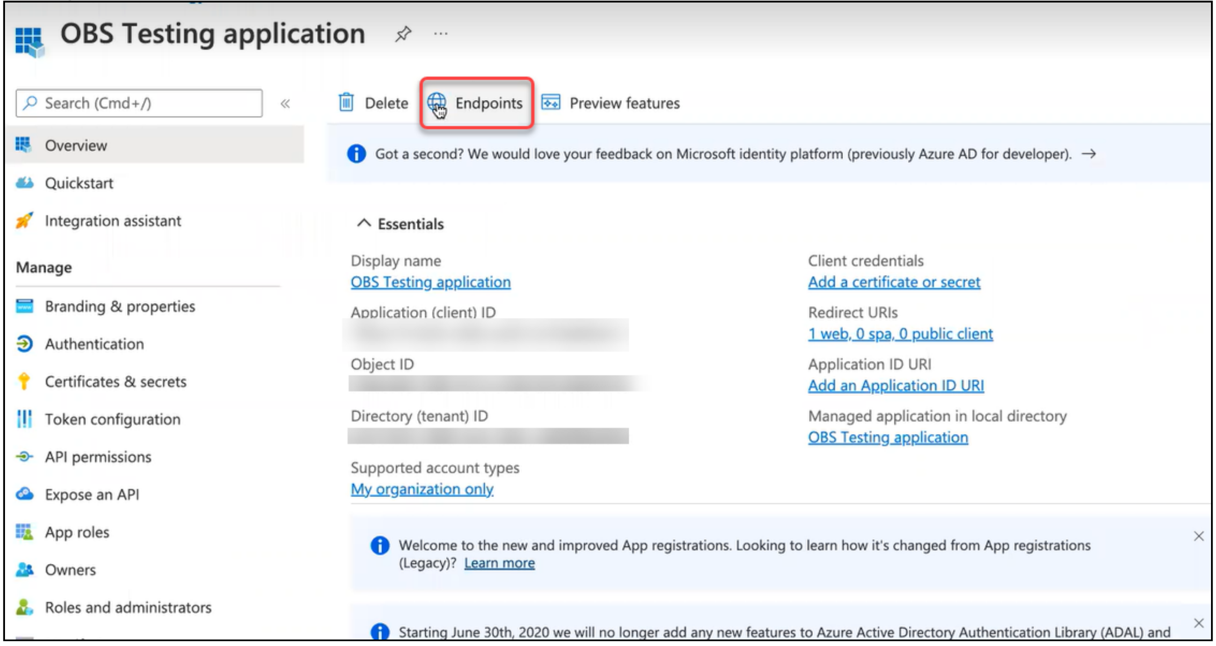
* Token Endpoint URL:

Mapped Domains

Actions	Domain Name
No data to display	

Required information: Client ID, Authorization Endpoint URL, Token Endpoint URL

4. Change to the tab with your Entra app (overview) and click **Endpoints**.



OBS Testing application

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name: OBS Testing application

Application (client) ID: [redacted]

Object ID: [redacted]

Directory (tenant) ID: [redacted]

Supported account types: My organization only

Client credentials: Add a certificate or secret

Redirect URIs: 1 web, 0 spa, 0 public client

Application ID URI: Add an Application ID URI

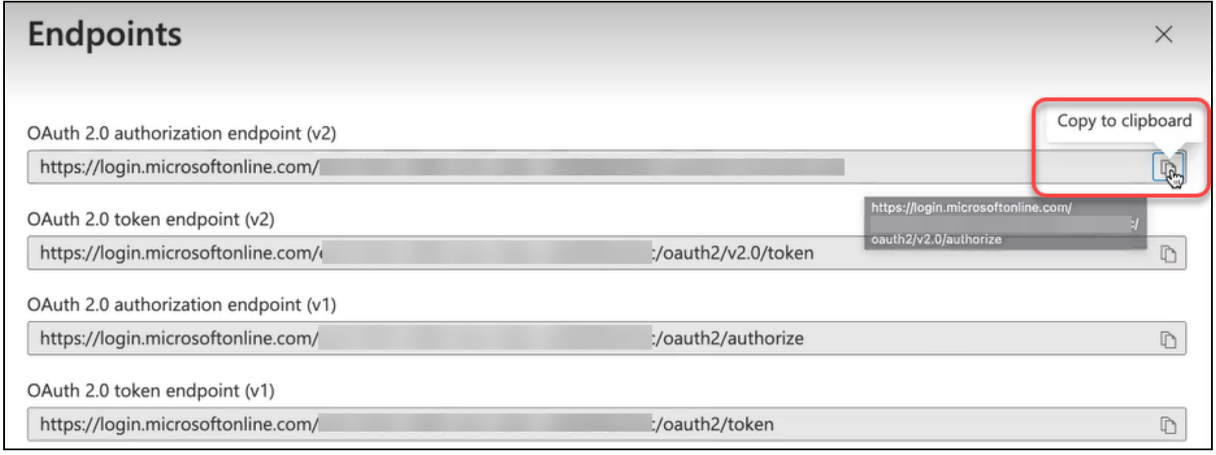
Managed application in local directory: OBS Testing application

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and

The endpoints for the app are shown. We will use the first 2 endpoints.

5. Copy the **OAuth 2.0 authorization endpoint (v2)** to the clipboard.



Endpoints

OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/[redacted]

Copy to clipboard

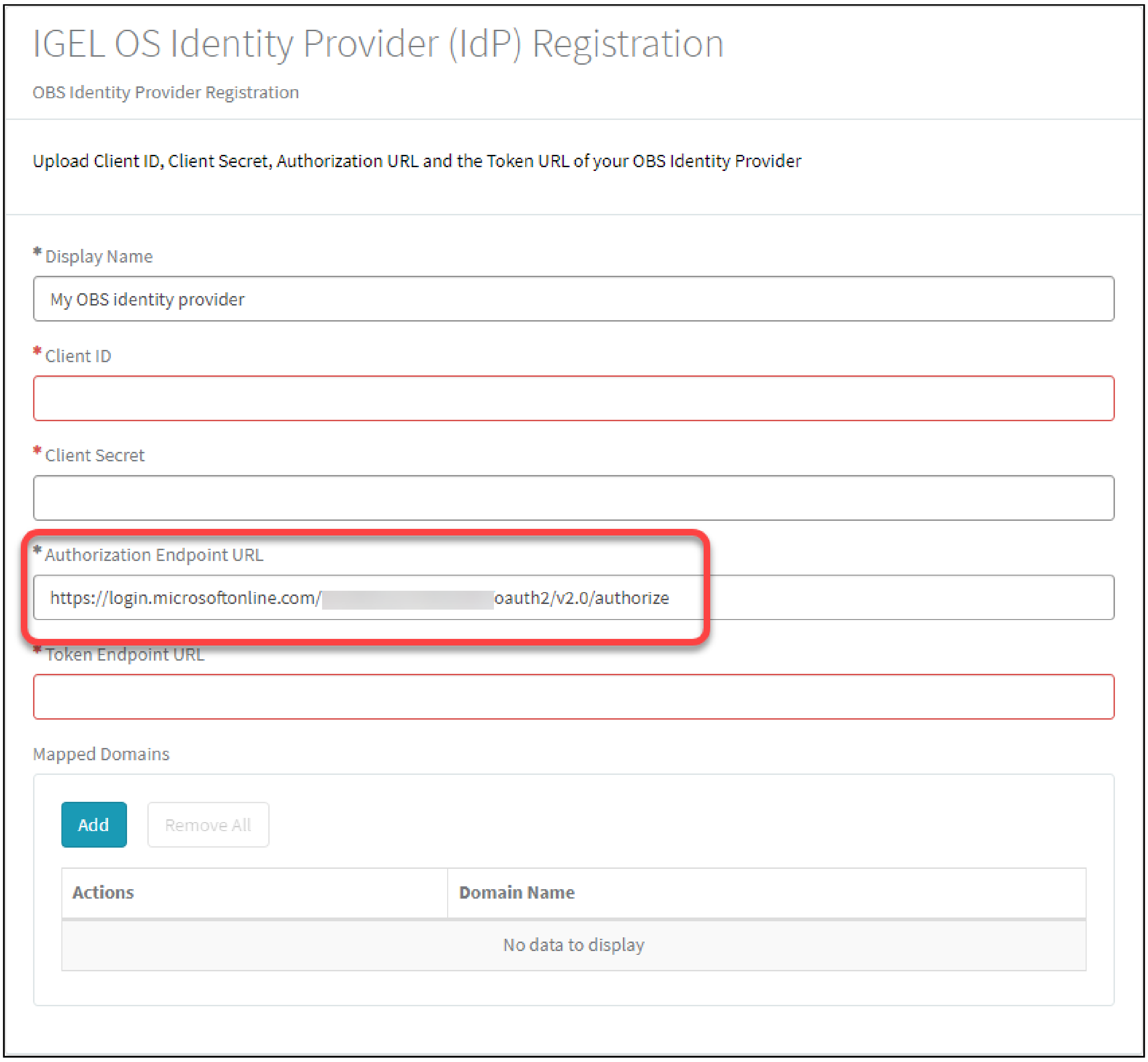
https://login.microsoftonline.com/[redacted]/
oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/token

6. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the authorization endpoint into the field **Authorization Endpoint URL**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name

My OBS identity provider

* Client ID

* Client Secret

* Authorization Endpoint URL

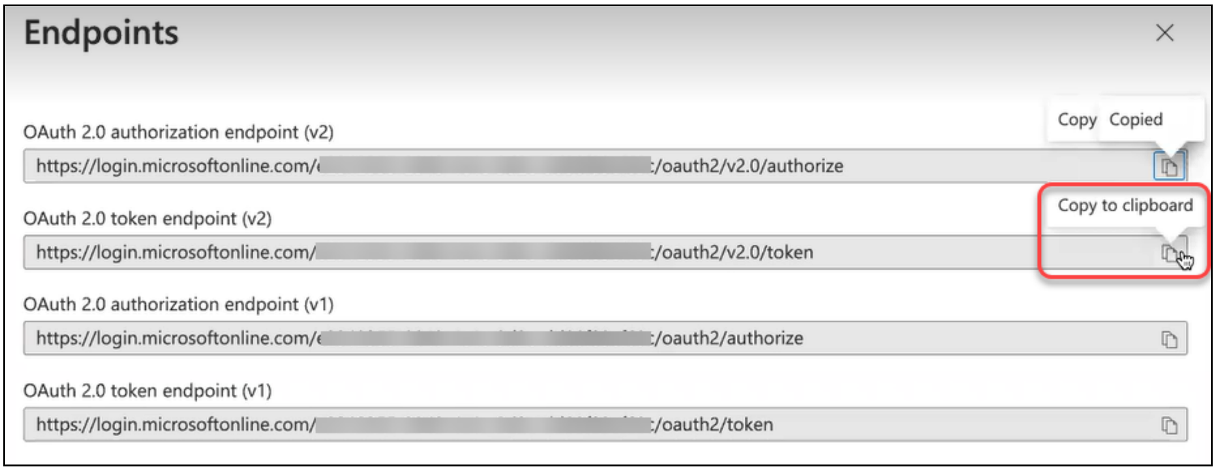
https://login.microsoftonline.com/[redacted]oauth2/v2.0/authorize

* Token Endpoint URL

Mapped Domains

Actions	Domain Name
No data to display	

7. Change to the tab with your Entra app (**Endpoints**) and copy the **OAuth 2.0 token endpoint (v2)** to the clipboard.


Endpoints

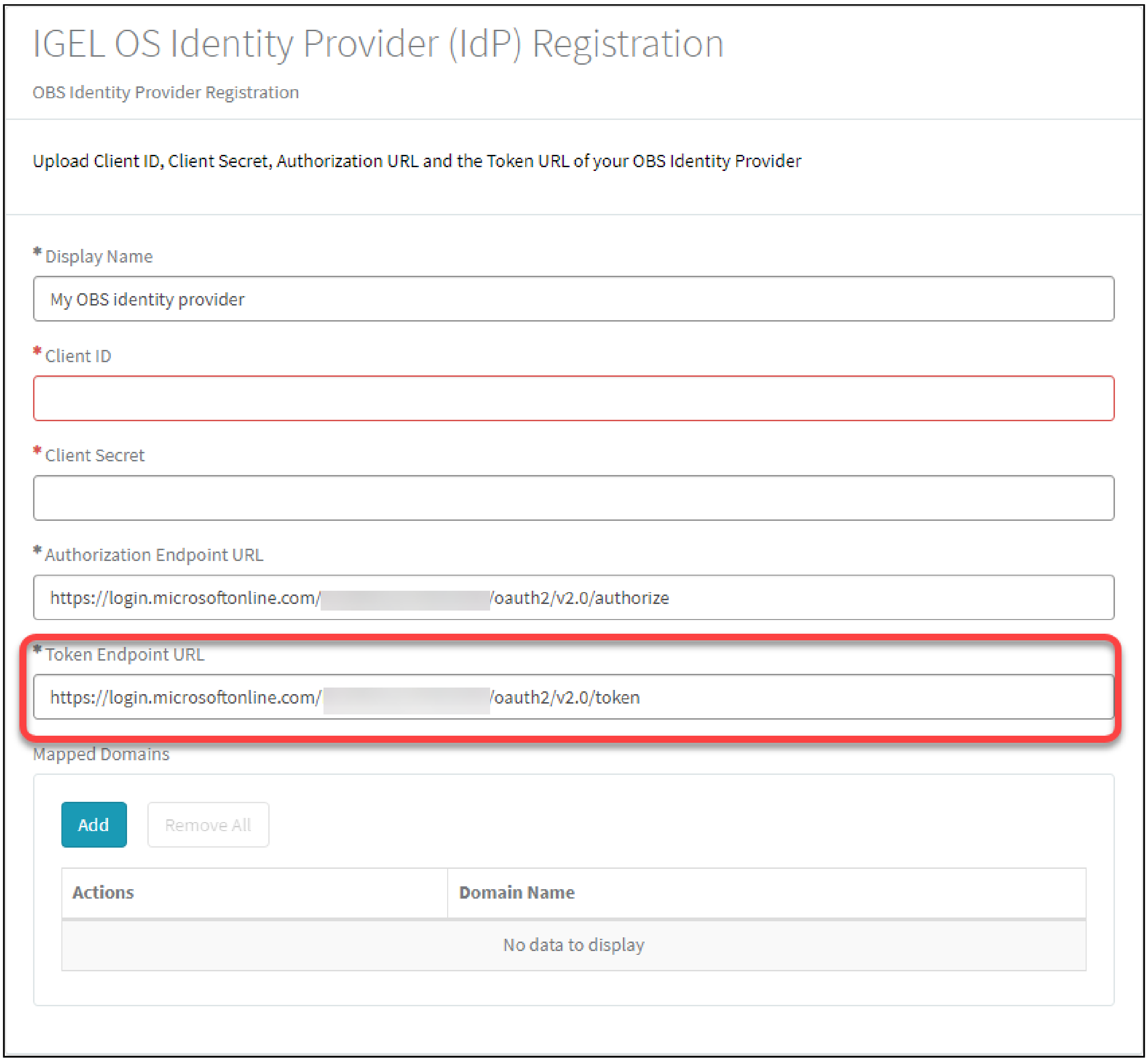
OAuth 2.0 authorization endpoint (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

OAuth 2.0 token endpoint (v2)
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

OAuth 2.0 authorization endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/authorize

OAuth 2.0 token endpoint (v1)
https://login.microsoftonline.com/[redacted]/oauth2/token

8. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the token endpoint into the field **Token Endpoint URL**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

*Display Name: My OBS identity provider

*Client ID:

*Client Secret:

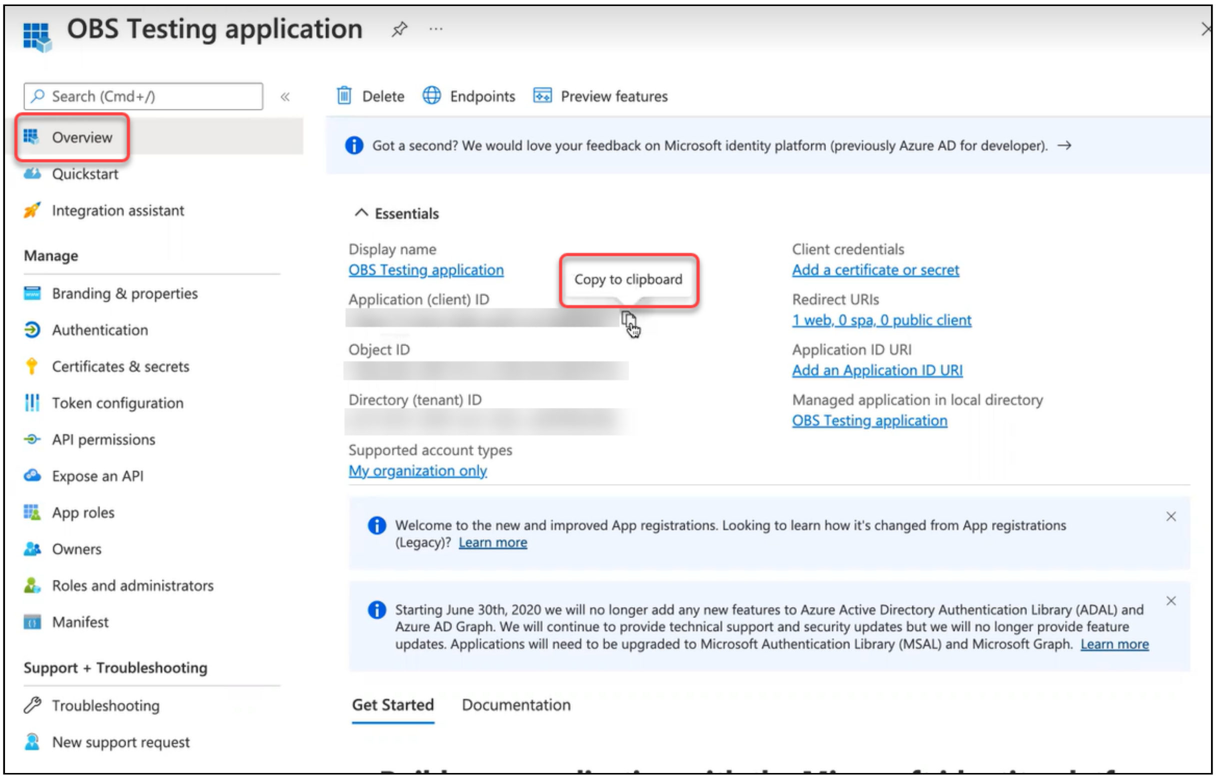
*Authorization Endpoint URL: https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

*Token Endpoint URL: https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

Mapped Domains

Actions	Domain Name
No data to display	

9. Change to the tab with your Entra app, go to **Overview**, and copy the **Application (client) ID** to the clipboard.



OBS Testing application

Search (Cmd+/)

Delete | Endpoints | Preview features

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name
OBS Testing application

Application (client) ID
[redacted]

Copy to clipboard

Object ID
[redacted]

Directory (tenant) ID
[redacted]

Supported account types
My organization only

Client credentials
Add a certificate or secret

Redirect URIs
1 web, 0 spa, 0 public client

Application ID URI
Add an Application ID URI

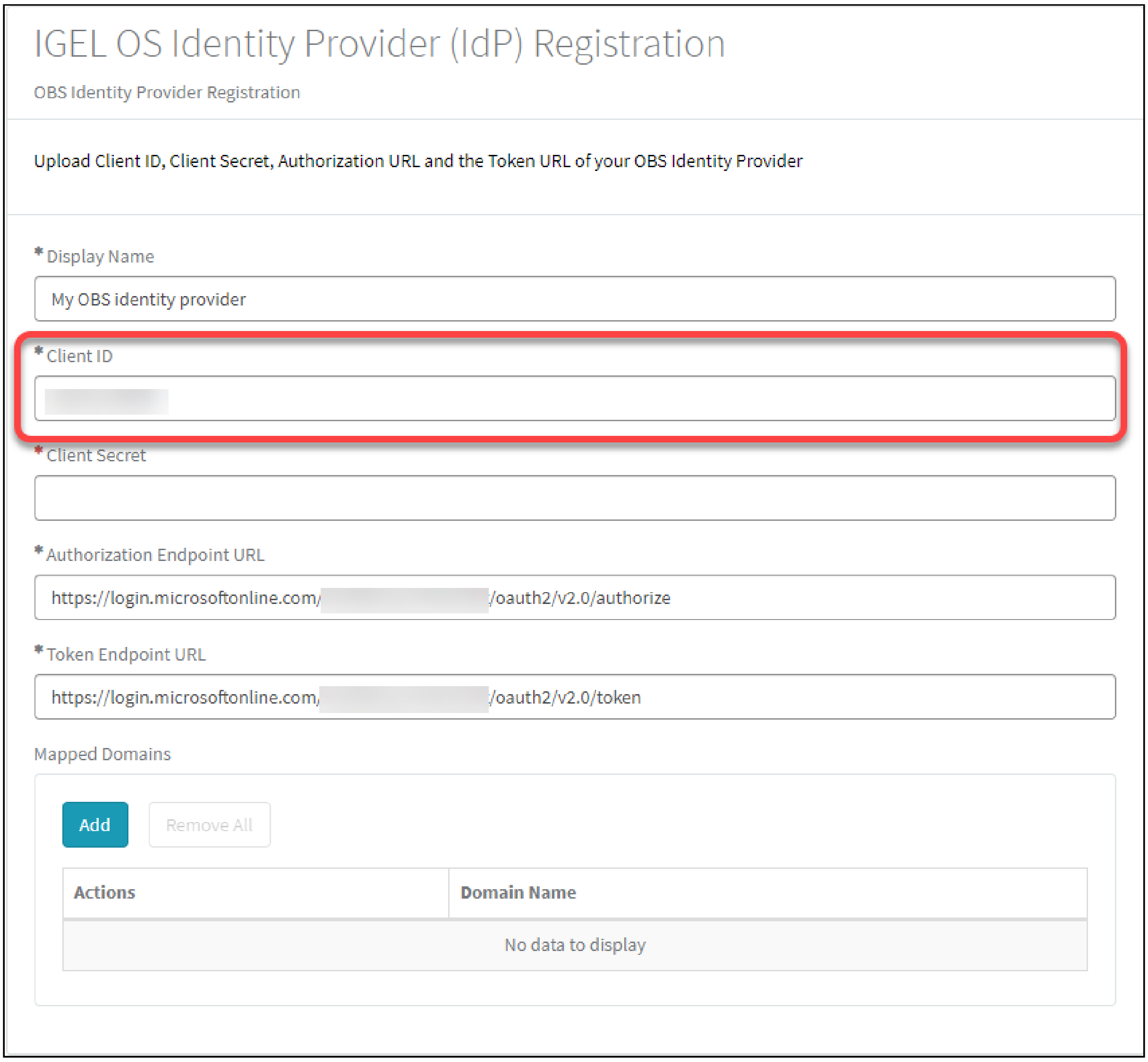
Managed application in local directory
OBS Testing application

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Get Started | Documentation

10. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the token endpoint into the field **Client ID**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name: My OBS identity provider

* Client ID: [redacted]

* Client Secret:

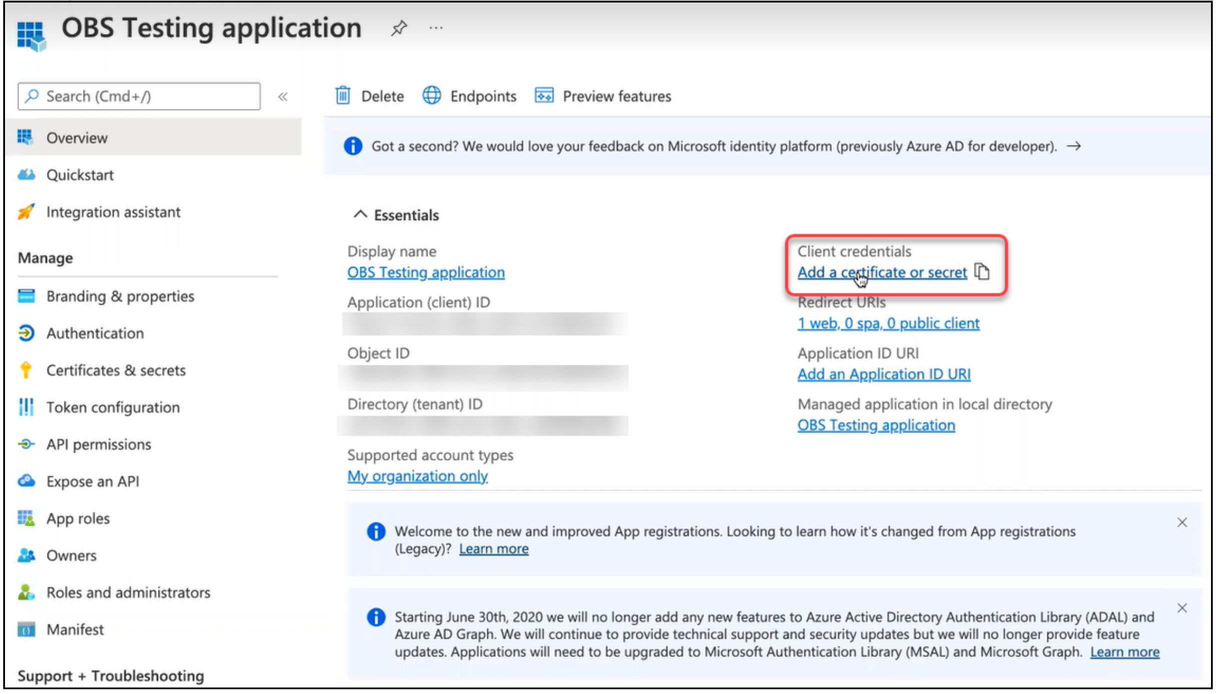
* Authorization Endpoint URL: https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

* Token Endpoint URL: https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

Mapped Domains

Actions	Domain Name
No data to display	

11. Change to the tab with your Entra app (**Overview**) and click **Add a certificate or secret**.



OBS Testing application

Search (Cmd+/)

Delete | Endpoints | Preview features

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name: OBS Testing application

Application (client) ID: [redacted]

Object ID: [redacted]

Directory (tenant) ID: [redacted]

Supported account types: My organization only

Client credentials: Add a certificate or secret

Redirect URIs: 1 web, 0 spa, 0 public client

Application ID URI: Add an Application ID URI

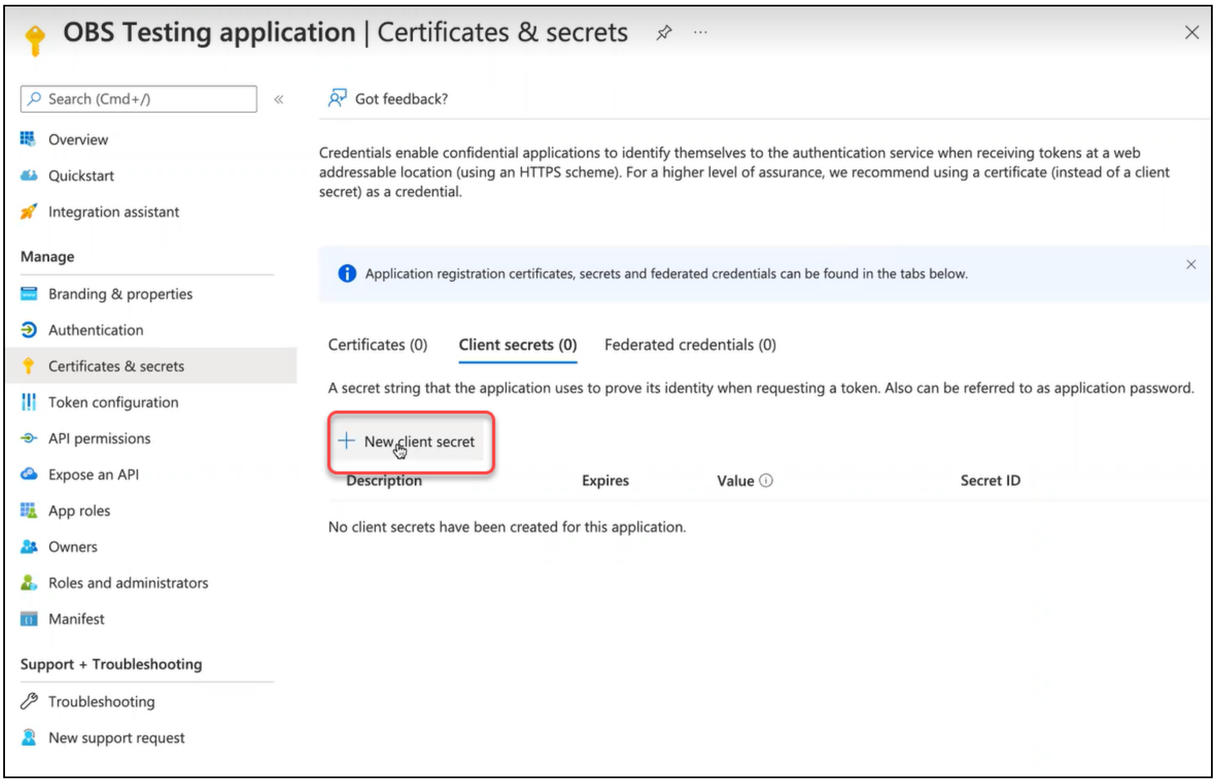
Managed application in local directory: OBS Testing application

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

You are taken to the **Certificates & secrets** page.

12. Click **New client secret**.



OBS Testing application | Certificates & secrets

Search (Cmd+/)

Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) | Client secrets (0) | Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

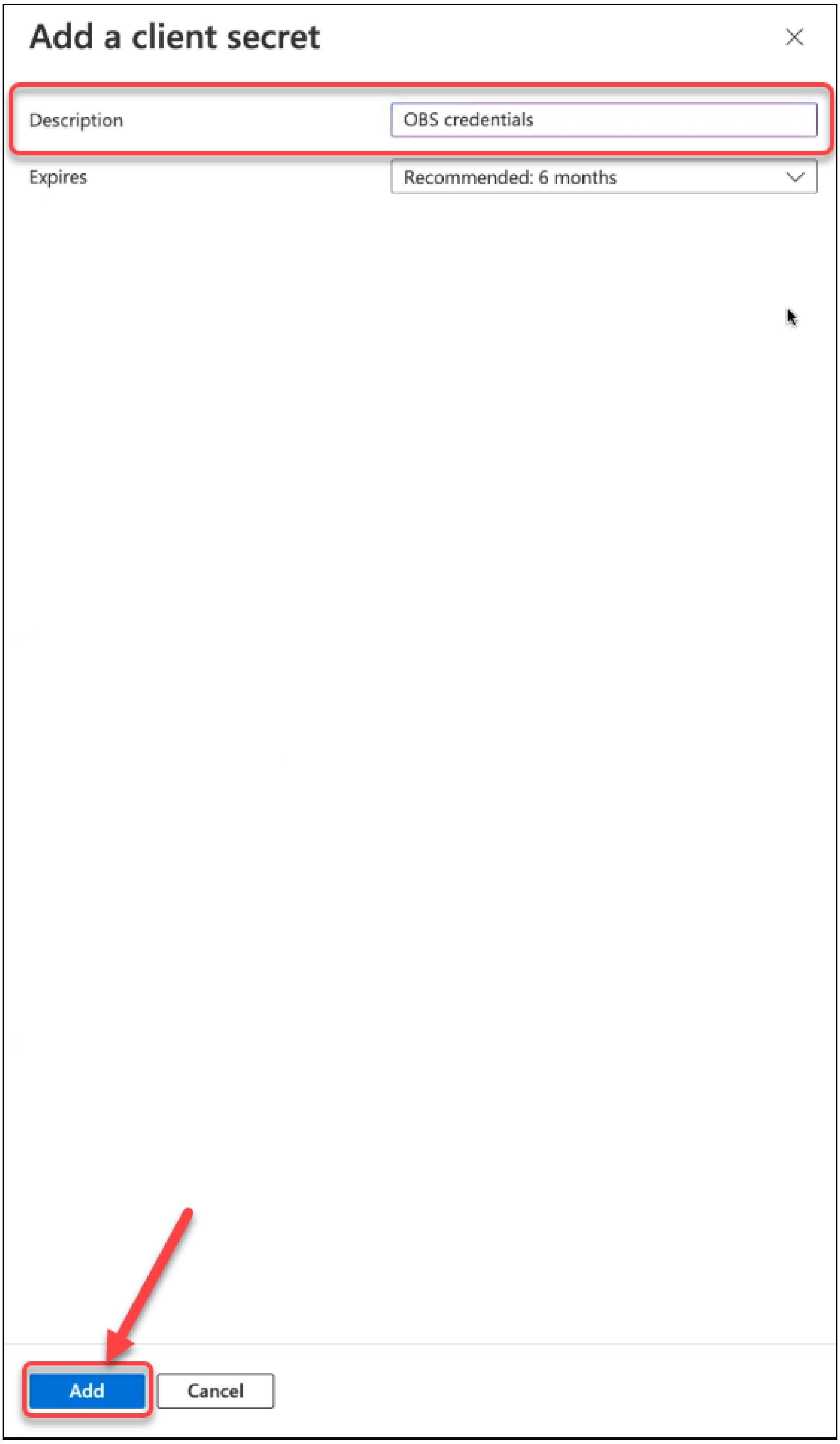
+ New client secret

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

13. IMPORTANT! Make sure you have a safe and secure location to store the client secret; it can only be read out once. If you lose it, you must change it.

14. Enter a description and then click **Add**.

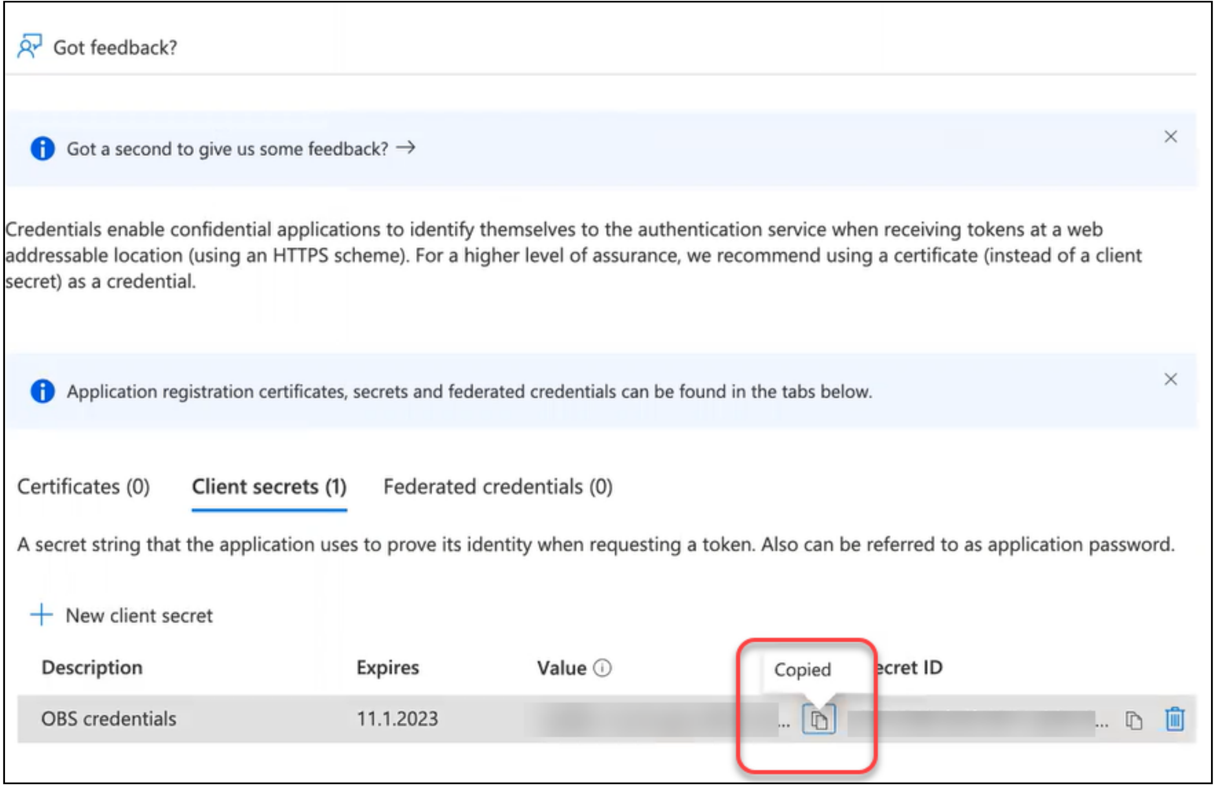


Add a client secret

Description: OBS credentials

Expires: Recommended: 6 months

15. Copy the client secret to the clipboard.



Got feedback?

Got a second to give us some feedback? →

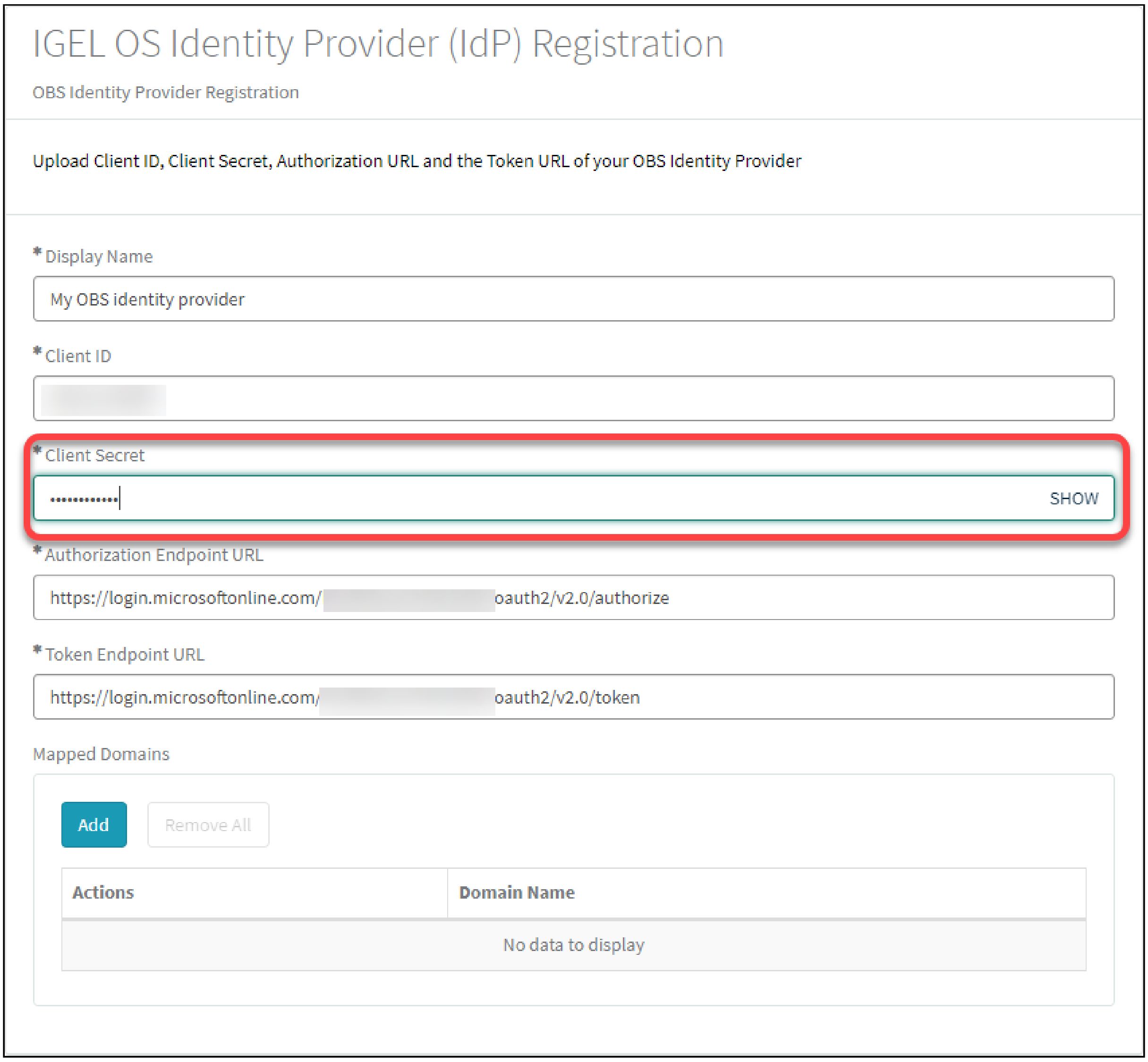
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ecret ID
OBS credentials	11.1.2023	[redacted] ...	[redacted] ...

16. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client secret into the field **Client secret**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name

My OBS identity provider

* Client ID

[redacted]

* Client Secret

•••••••••••• SHOW

* Authorization Endpoint URL

https://login.microsoftonline.com/[redacted]oauth2/v2.0/authorize

* Token Endpoint URL

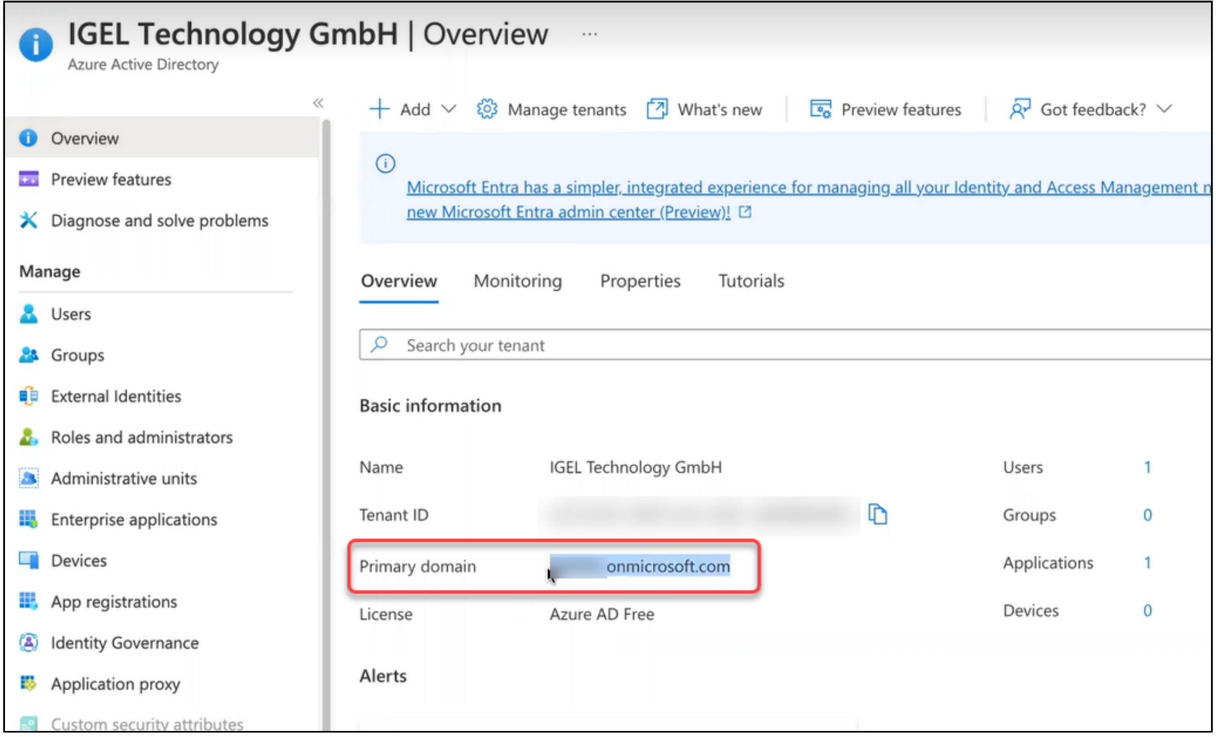
https://login.microsoftonline.com/[redacted]oauth2/v2.0/token

Mapped Domains

Actions	Domain Name
No data to display	

17. Change to the tab with your Entra app and change to the overview of your Entra tenant.

18. Copy the **Primary domain** to the clipboard.



IGEL Technology GmbH | Overview

Azure Active Directory

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management n

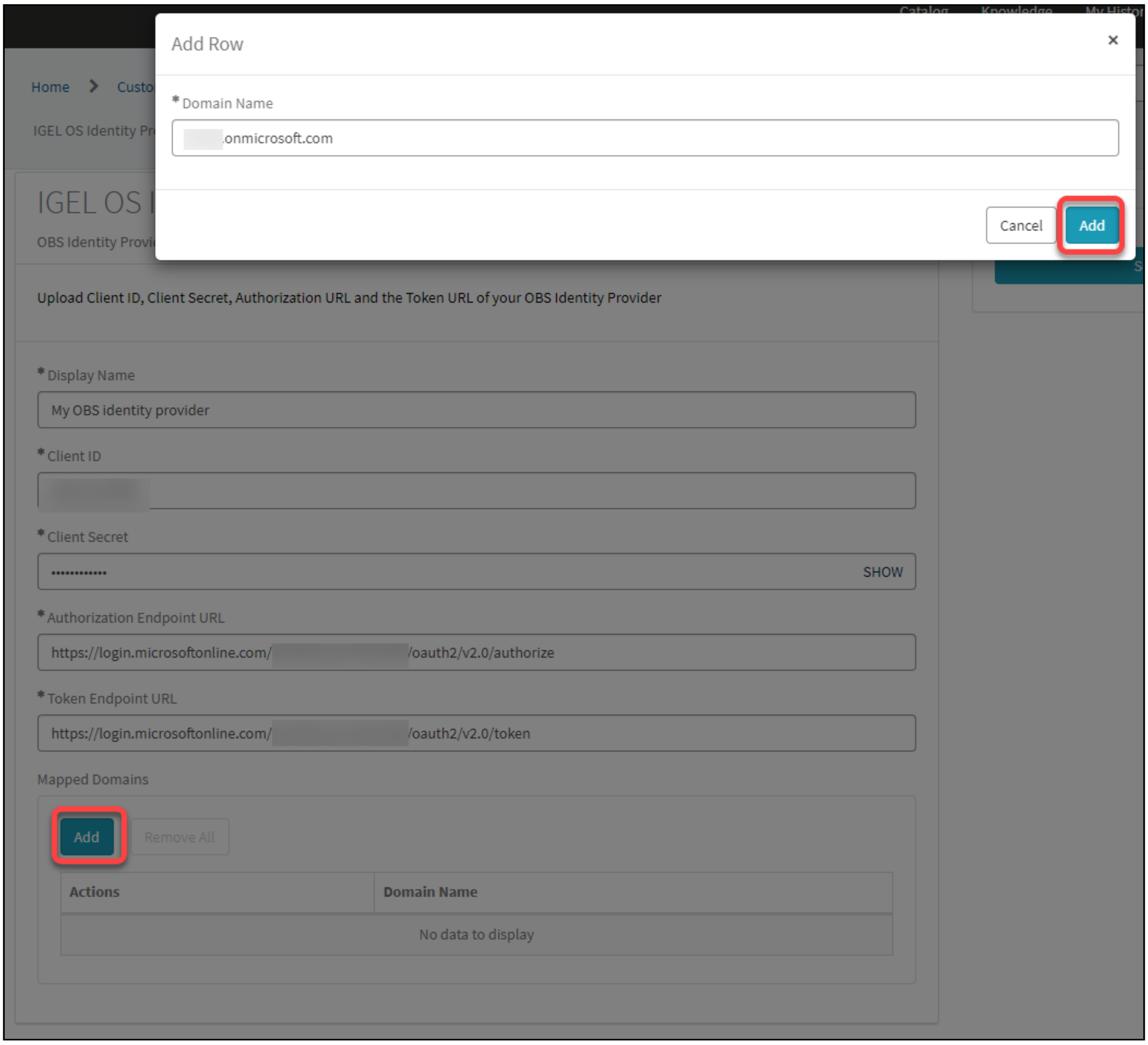
new Microsoft Entra admin center (Preview)!

Basic information

Name	IGEL Technology GmbH	Users	1
Tenant ID	[redacted]	Groups	0
Primary domain	[redacted]onmicrosoft.com	Applications	1
License	Azure AD Free	Devices	0

Alerts

19. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab, click **Add**, paste the primary domain from the clipboard into the field **Domain name**, and then click **Add** in the dialog.



Add Row

* Domain Name

[redacted]onmicrosoft.com

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name

My OBS identity provider

* Client ID

[redacted]

* Client Secret

••••••••••••

* Authorization Endpoint URL

https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

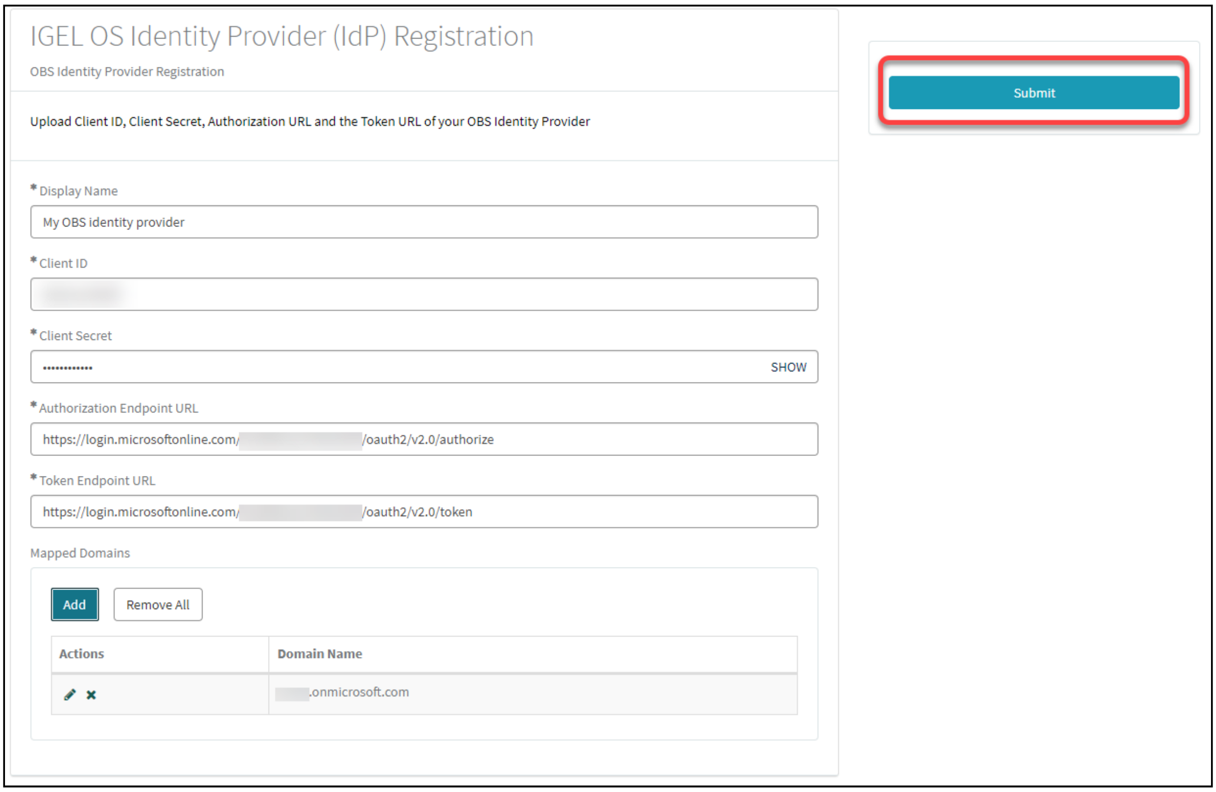
* Token Endpoint URL

https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

Mapped Domains

Actions	Domain Name
No data to display	

20. Click **Submit**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name: My OBS identity provider

* Client ID: [redacted]

* Client Secret: ••••••••••• SHOW

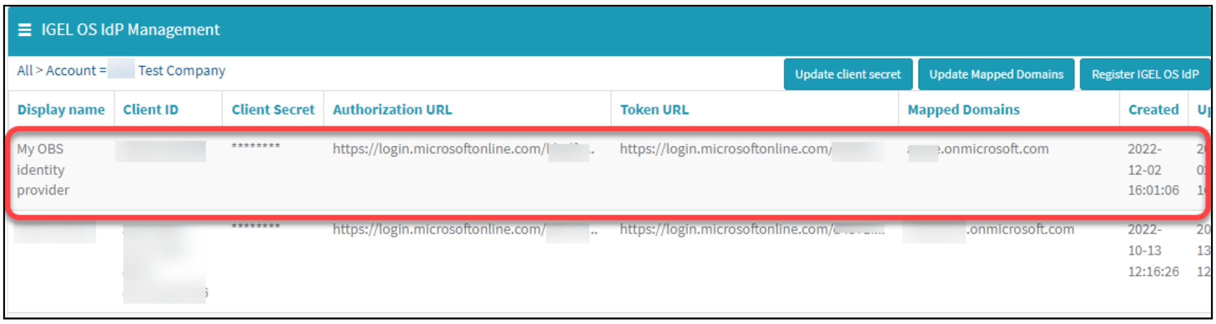
* Authorization Endpoint URL: https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

* Token Endpoint URL: https://login.microsoftonline.com/[redacted]/oauth2/v2.0/token

Mapped Domains

Actions	Domain Name
✎ ✖	[redacted].onmicrosoft.com

The data record is created.



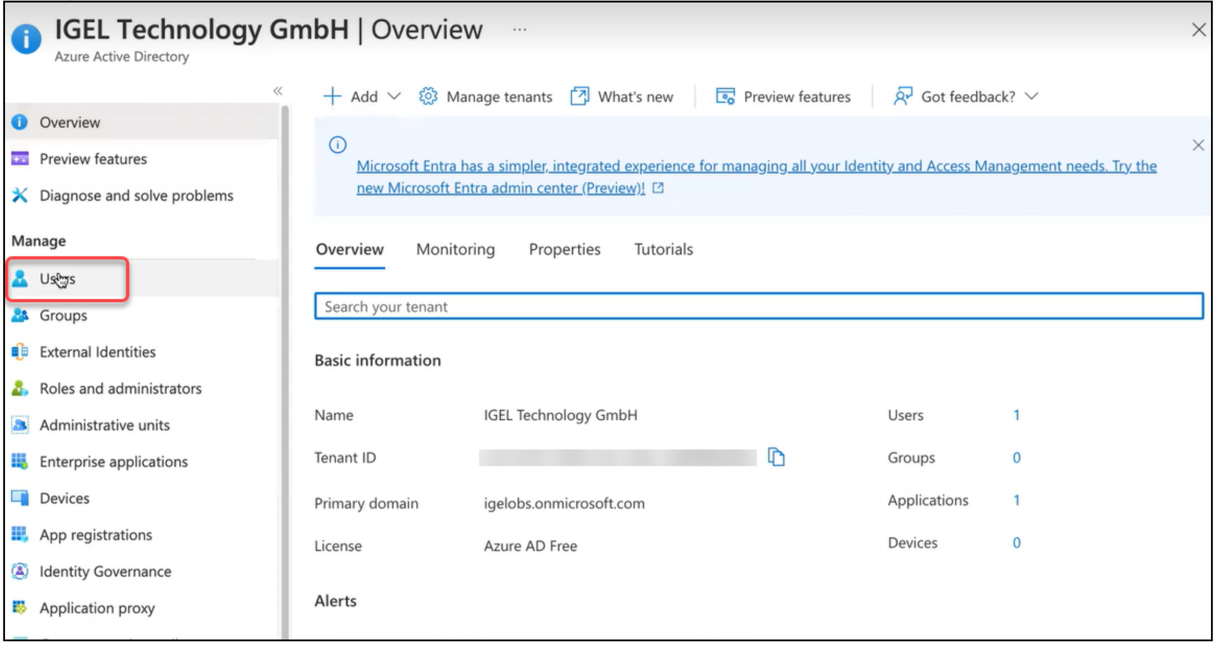
IGEL OS IdP Management

All > Account = [redacted] Test Company

Display name	Client ID	Client Secret	Authorization URL	Token URL	Mapped Domains	Created	U
My OBS identity provider	[redacted]	********	https://login.microsoftonline.com/[redacted].	https://login.microsoftonline.com/[redacted]	[redacted].onmicrosoft.com	2022-12-02 16:01:06	2 0 1
[redacted]	[redacted]	********	https://login.microsoftonline.com/[redacted]..	https://login.microsoftonline.com/[redacted]...	[redacted].onmicrosoft.com	2022-10-13 12:16:26	20 13 12

Creating a User in the Entra App

1. Change to the Entra (tenant overview) tab and click **Users**.

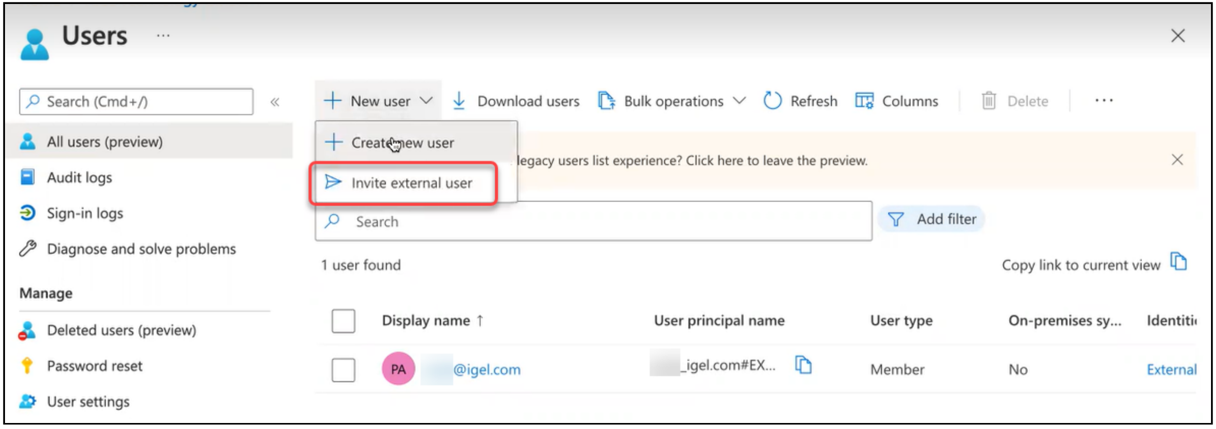


Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center (Preview)!

Basic information

Name	IGEL Technology GmbH	Users	1
Tenant ID	[redacted]	Groups	0
Primary domain	igelobs.onmicrosoft.com	Applications	1
License	Azure AD Free	Devices	0

2. From the **New user menu**, select **Create a new user**.



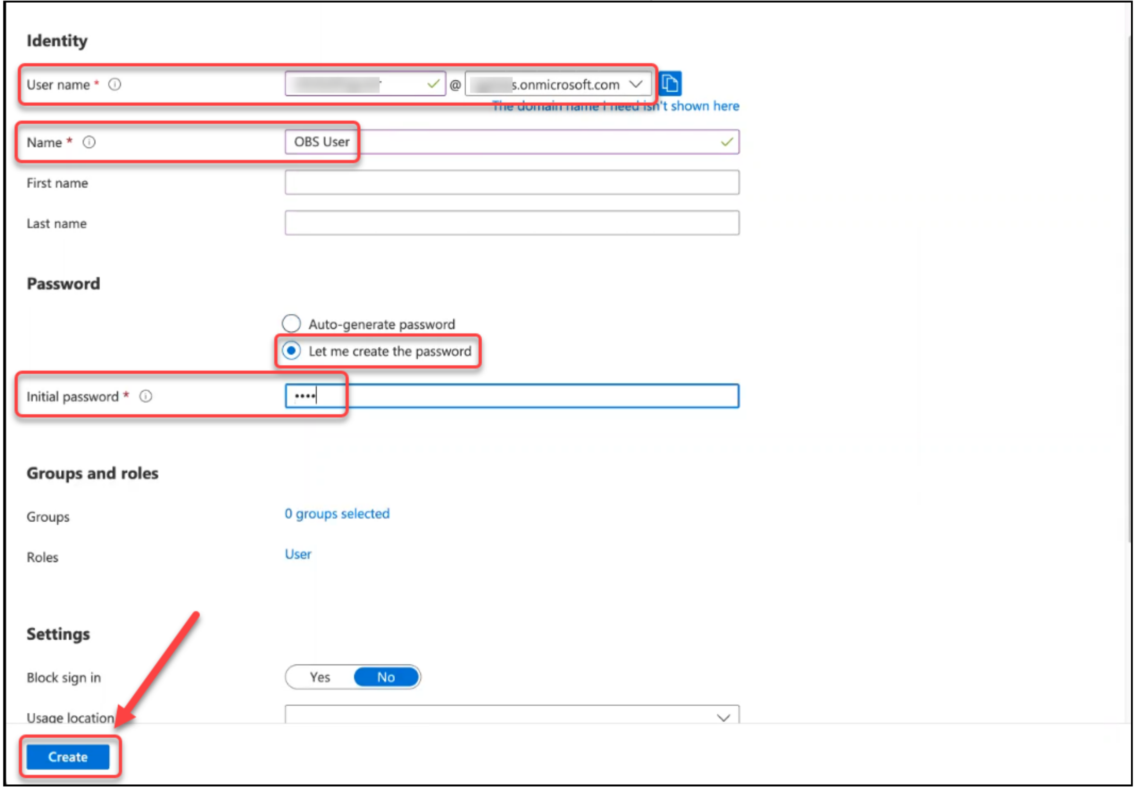
legacy users list experience? Click here to leave the preview.

1 user found

Display name ↑	User principal name	User type	On-premises sy...	Identiti
PA [redacted]@igel.com	[redacted]_igel.com#EX...	Member	No	External

3. Provide the necessary data and then click **Create**:
   - **User name**: A valid e-mail address.
   - **Name**: Display name
   - **Let me create the password**: For our purposes, you can use this option.

- **Initial password**: Password to be used for the first login.



Identity

User name * ⓘ [redacted] @ [redacted]s.onmicrosoft.com

The domain name I need isn't shown here

Name * ⓘ OBS User

First name

Last name

Password

○ Auto-generate password

● Let me create the password

Initial password * ⓘ ••••

Groups and roles

Groups: 0 groups selected

Roles: User

Settings

Block sign in: Yes [✓ No]

Usage location

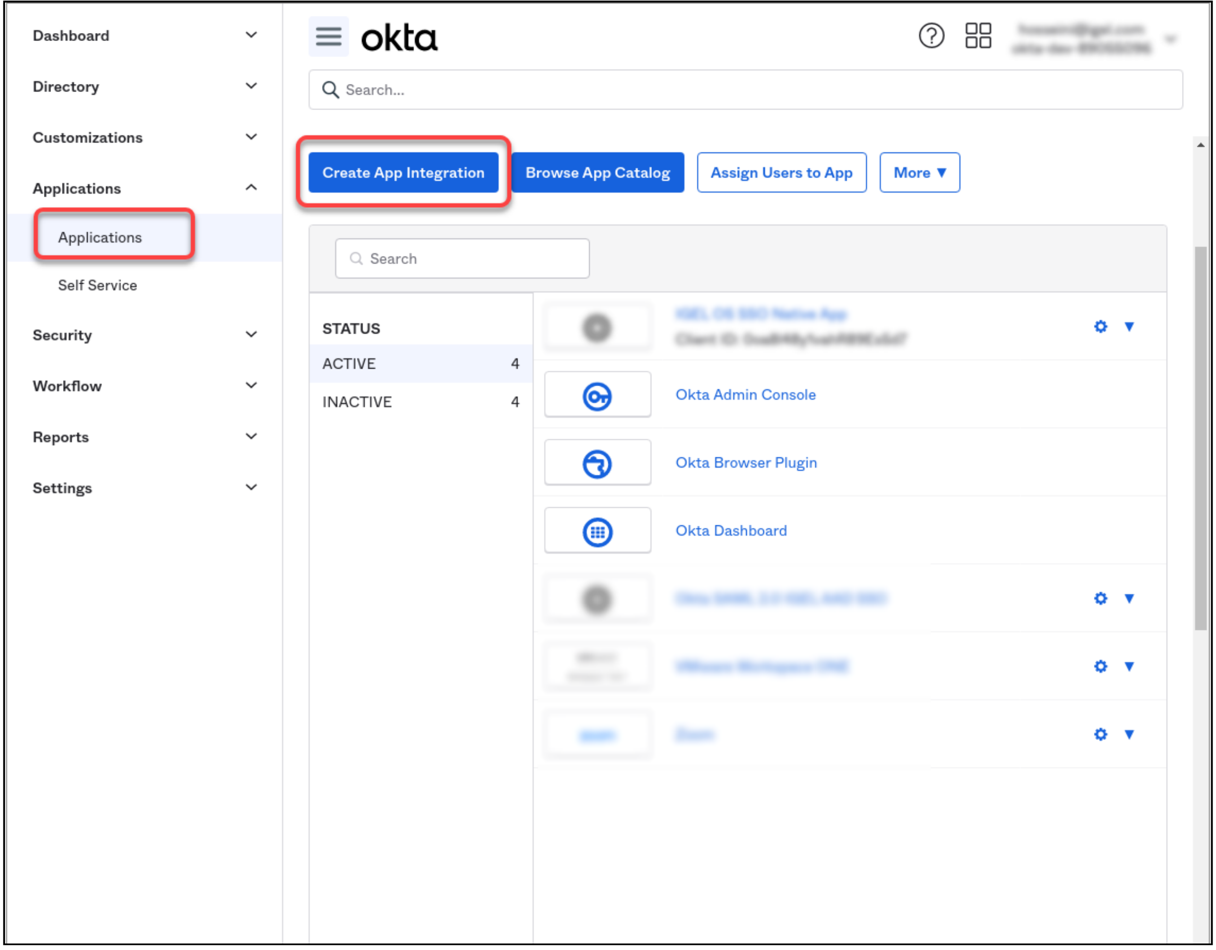
Configuring Okta as Identity Provider

To configure Okta as the identity provider, you need to do the following:

1. Creating an Okta Application That Will Serve as Identity Provider(see page 79): We register an application in Okta to use the service as an external identity provider.
2. Registering Our Okta Application in the IGEL Customer Portal(see page 83): This will enable IGEL Cloud Services to use our Okta Application as the external identity provider.

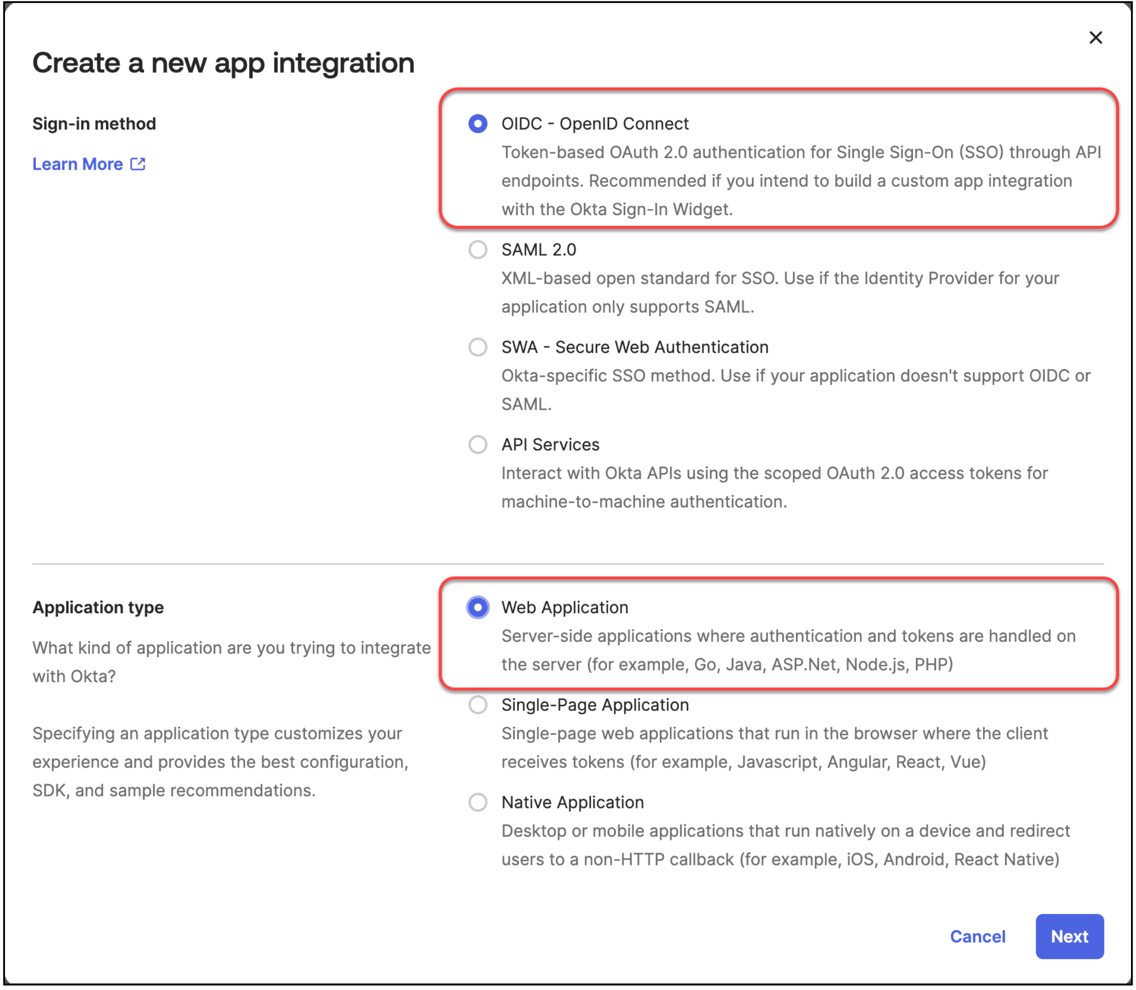
Creating an Okta Application That Will Serve as Identity Provider

1. Log in to Okta with your admin account, and from the **Applications** menu, select **Applications > Create App Integration**.



2. Edit the settings as follows and then click **Next**.
   - Set **Sign-in method** to **OIDC**.

- Set **Application type** to **Web Application**.



Create a new app integration

Sign-in method

Learn More

● OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

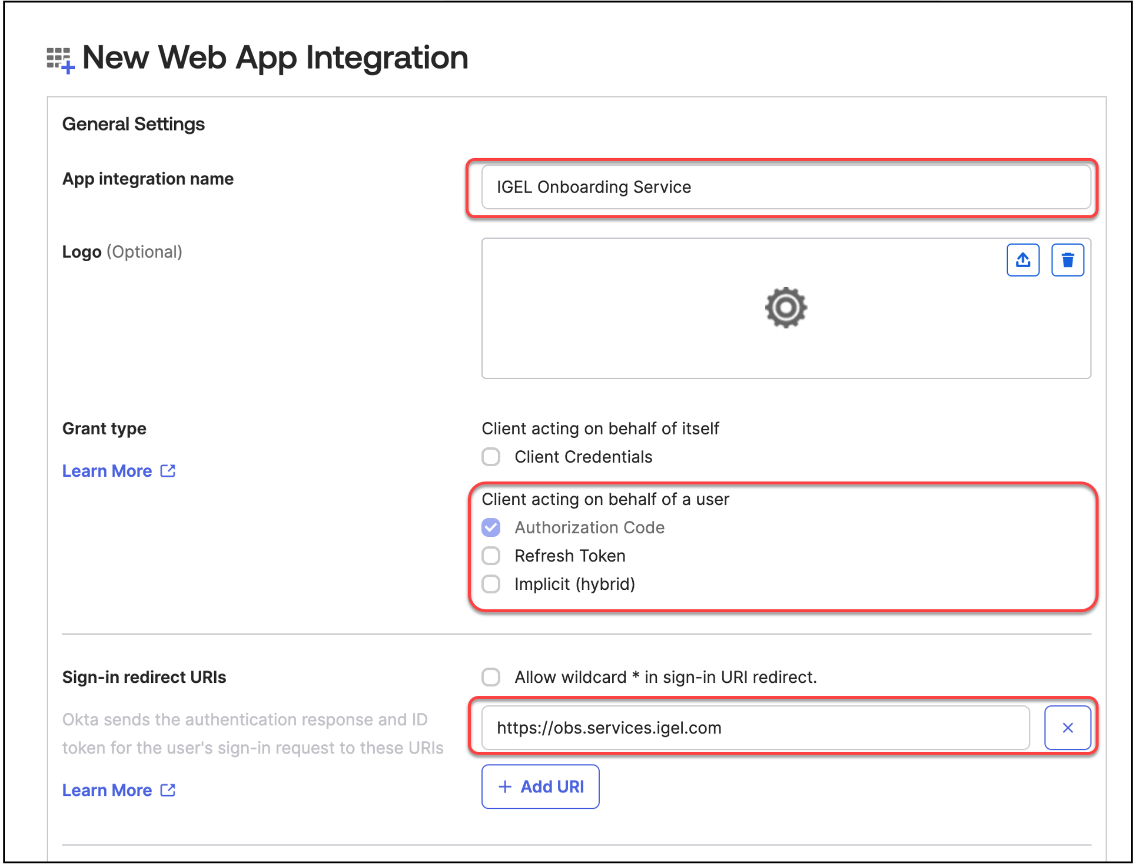
● Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

○ Single-Page Application
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

○ Native Application
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

3. Edit the settings as follows and then click **Save**.
   - Under **App integration name**, enter a name for your application, e.g. "IGEL Onboarding Service".
   - Make sure that as the **Grant type**, the option **Authorization Code** is selected.

- Under **Sign-in redirect URIs**, enter " `https://obs.services.igel.com/` ".



New Web App Integration

General Settings

App integration name: IGEL Onboarding Service

Logo (Optional)

Grant type

Learn More

Client acting on behalf of itself

□ Client Credentials

Client acting on behalf of a user

☑ Authorization Code

□ Refresh Token

□ Implicit (hybrid)

Sign-in redirect URIs

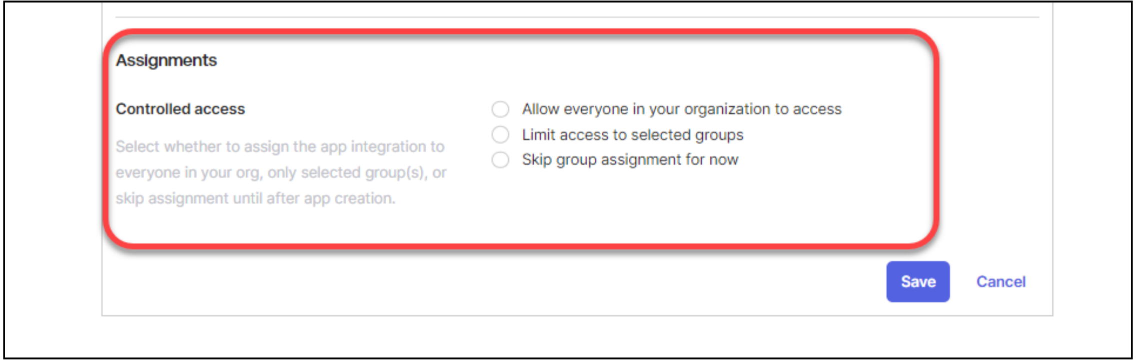
Okta sends the authentication response and ID token for the user's sign-in request to these URIs

Learn More

□ Allow wildcard * in sign-in URI redirect.

https://obs.services.igel.com

- Under **Assignments**, depending on your company policy, either allow everyone or select an existing group configured under **Directory > Groups**. You can change this configuration after creating the app integration under the **Assignments** tab of the application.



Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

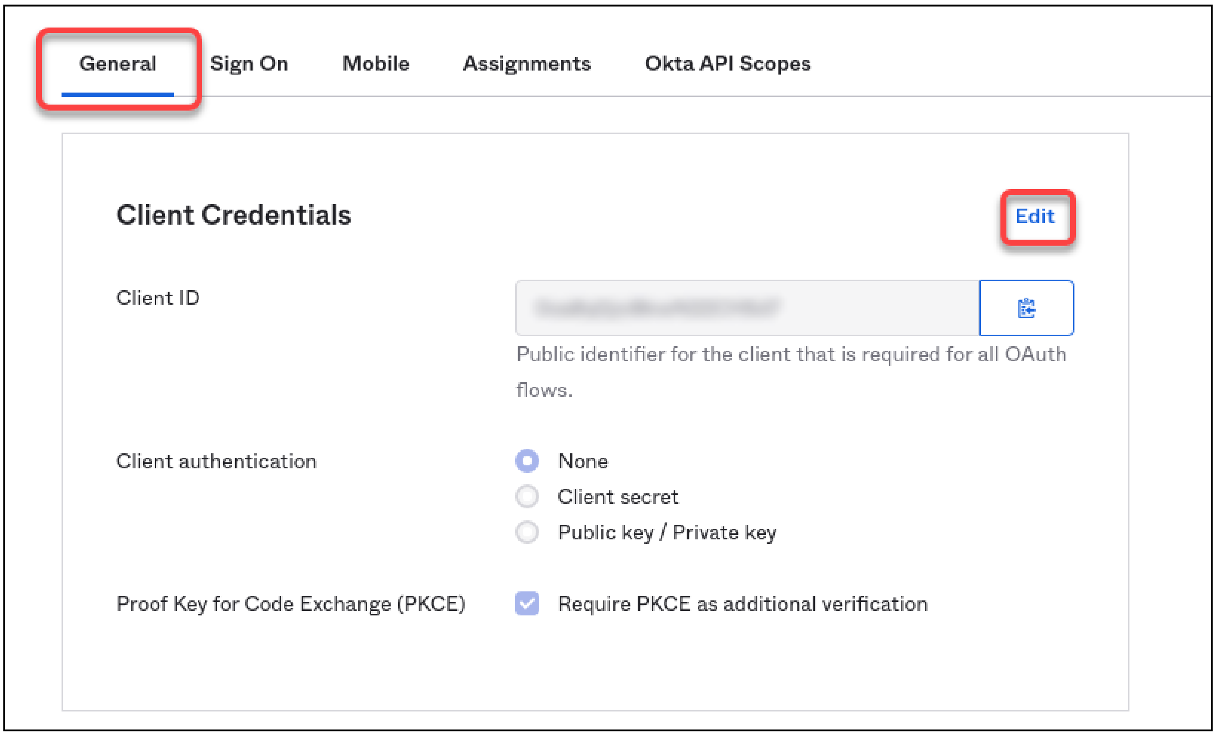
○ Allow everyone in your organization to access

○ Limit access to selected groups

○ Skip group assignment for now

The app integration is created.

4. Select the **General** tab and then click **Edit**.



Client Credentials

Client ID

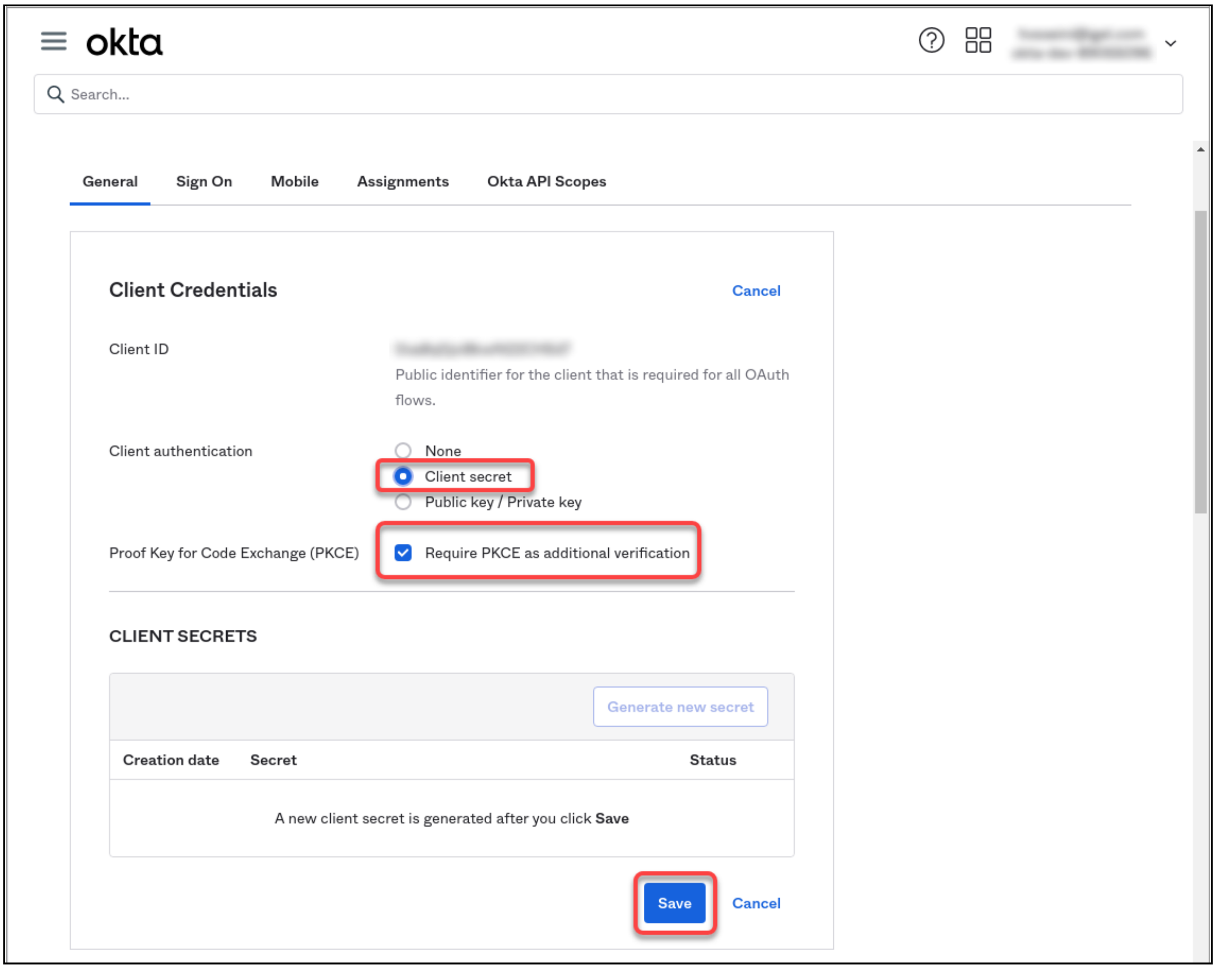
Public identifier for the client that is required for all OAuth flows.

Client authentication

● None
○ Client secret
○ Public key / Private key

Proof Key for Code Exchange (PKCE) ☑ Require PKCE as additional verification

5. Under **Client authentication**, select **Client secret** and make sure that under **Proof Key for Code Exchange (PKCE)**, **Require PKCE as additional verification** is enabled. Afterward, click **Save**.



Client Credentials

Cancel

Client ID: [redacted]

Public identifier for the client that is required for all OAuth flows.

Client authentication: ○ None ● Client secret ○ Public key / Private key

Proof Key for Code Exchange (PKCE): ☑ Require PKCE as additional verification

CLIENT SECRETS

Generate new secret

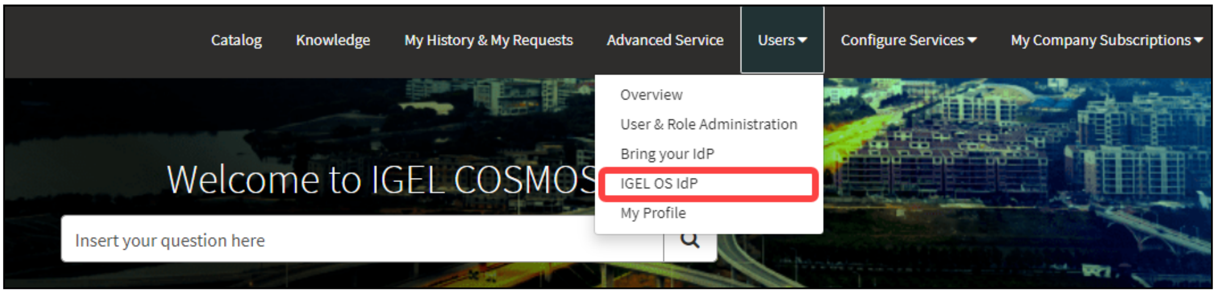
Creation date	Secret	Status
A new client secret is generated after you click **Save**		

Save Cancel

The client secret will be created.

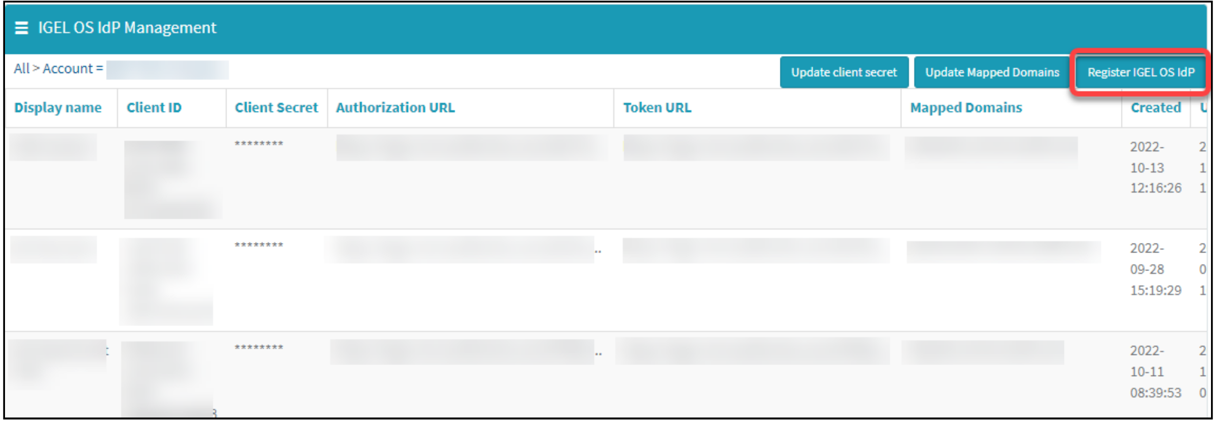
Registering Our Okta Application in the IGEL Customer Portal

1. Open the IGEL Customer Portal[17] in your browser, log in to your admin account, and select **Users > IGEL OS IdP**.



[17] https://cosmos.igel.com/

2. Click **Register IGEL OS IdP**.

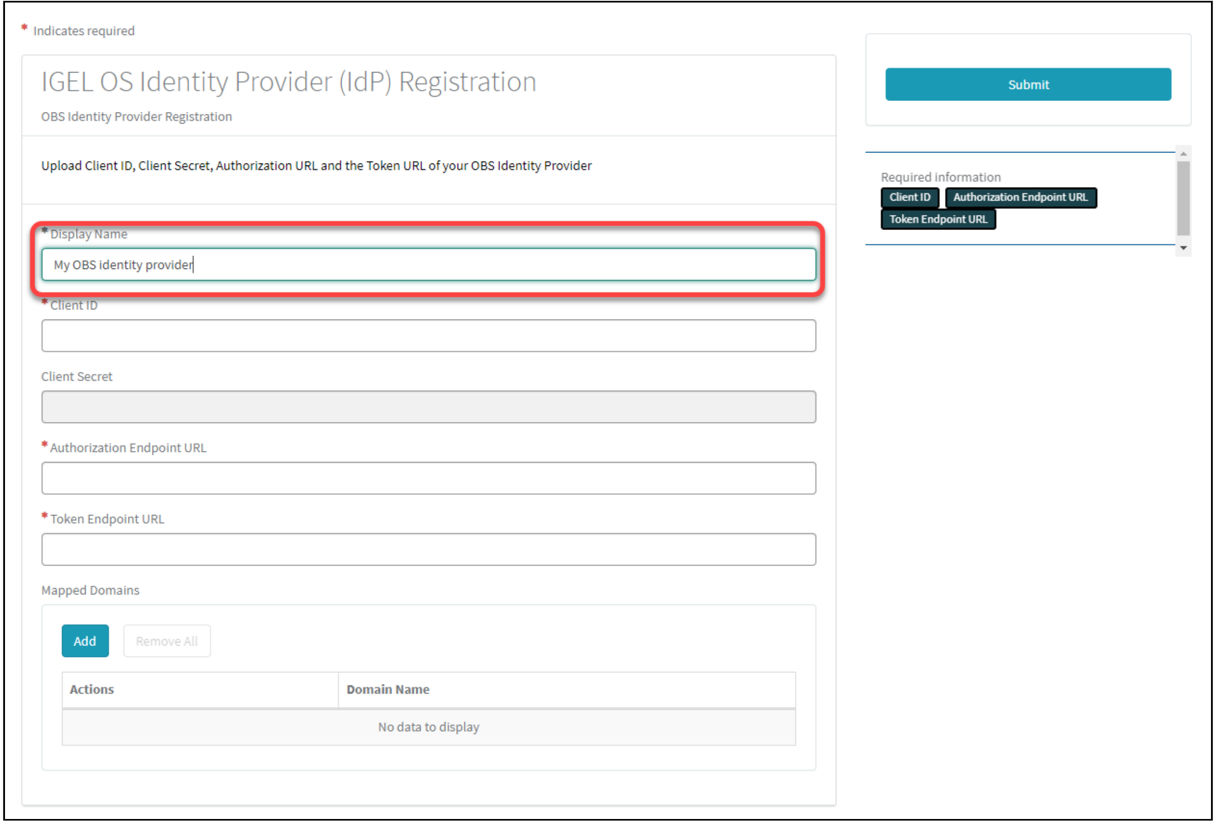


☰ IGEL OS IdP Management

All > Account =

Display name	Client ID	Client Secret	Authorization URL	Token URL	Mapped Domains	Created	U
		********				2022- 10-13 12:16:26	2 1 1
		********	..			2022- 09-28 15:19:29	2 0 1
:		********	..			2022- 10-11 08:39:53	2 1 0

3. Enter a **Display name**. This is the name under which your identity provider app will be displayed.



* Indicates required

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name: My OBS identity provider

* Client ID:

Client Secret:

* Authorization Endpoint URL:

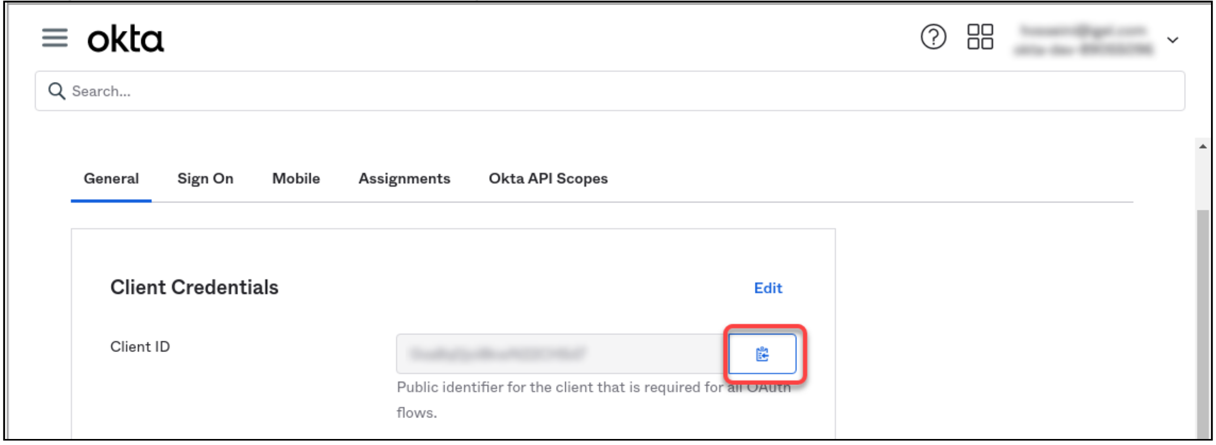
* Token Endpoint URL:

Mapped Domains

Actions	Domain Name
No data to display	

Required information

4. Change to the tab with your Okta app, go to the **General** tab and copy the **Client ID**.

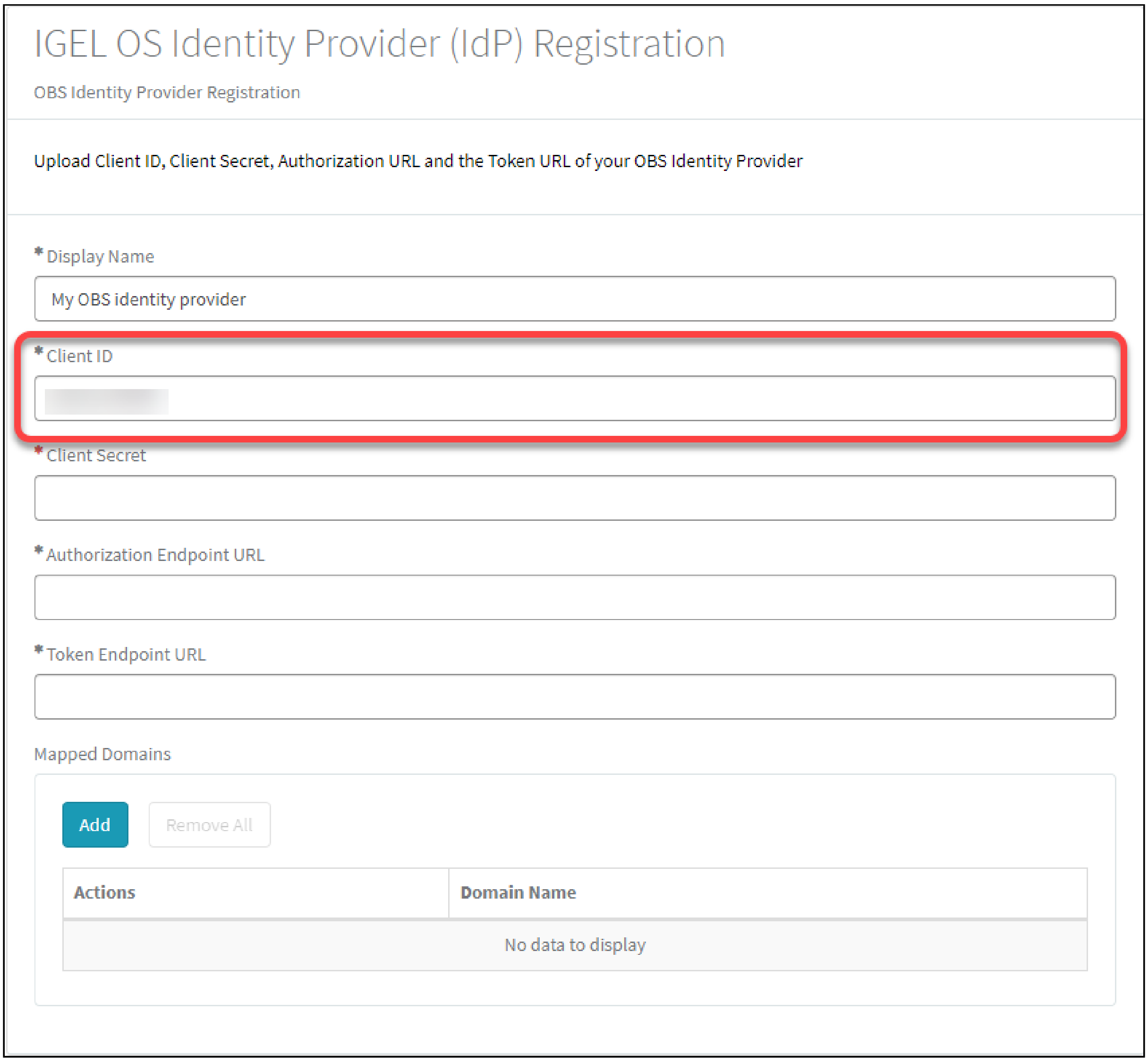


Client Credentials

Client ID

Public identifier for the client that is required for all OAuth flows.

5. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client ID into the field **Client ID**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name

My OBS identity provider

* Client ID

[redacted]

* Client Secret

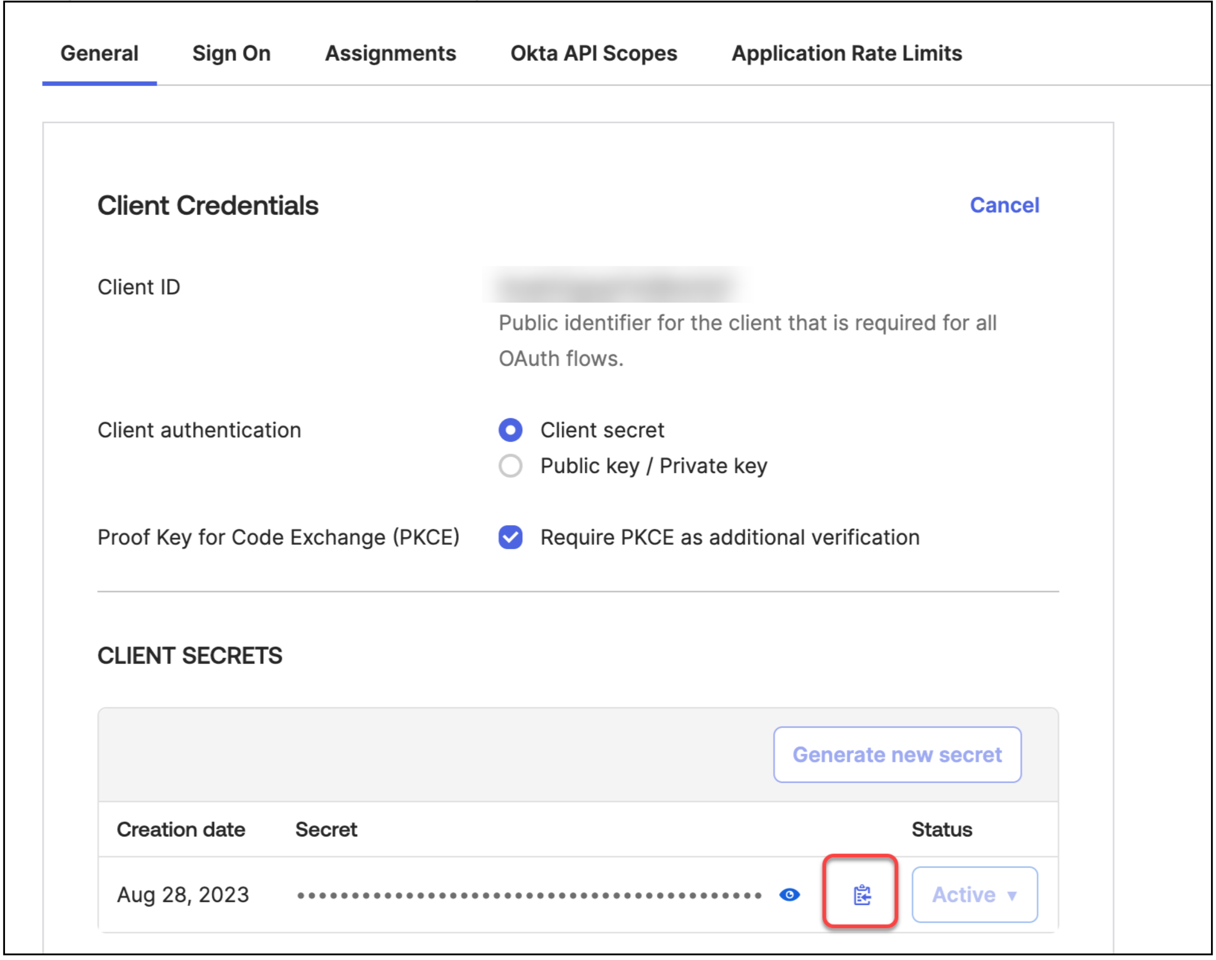
* Authorization Endpoint URL

* Token Endpoint URL

Mapped Domains

Actions	Domain Name
No data to display	

6. Change to the tab with your Okta app, go to the **General** tab and copy the **Client Secret**.



Client Credentials

Client ID

Public identifier for the client that is required for all OAuth flows.

Client authentication

● Client secret
○ Public key / Private key

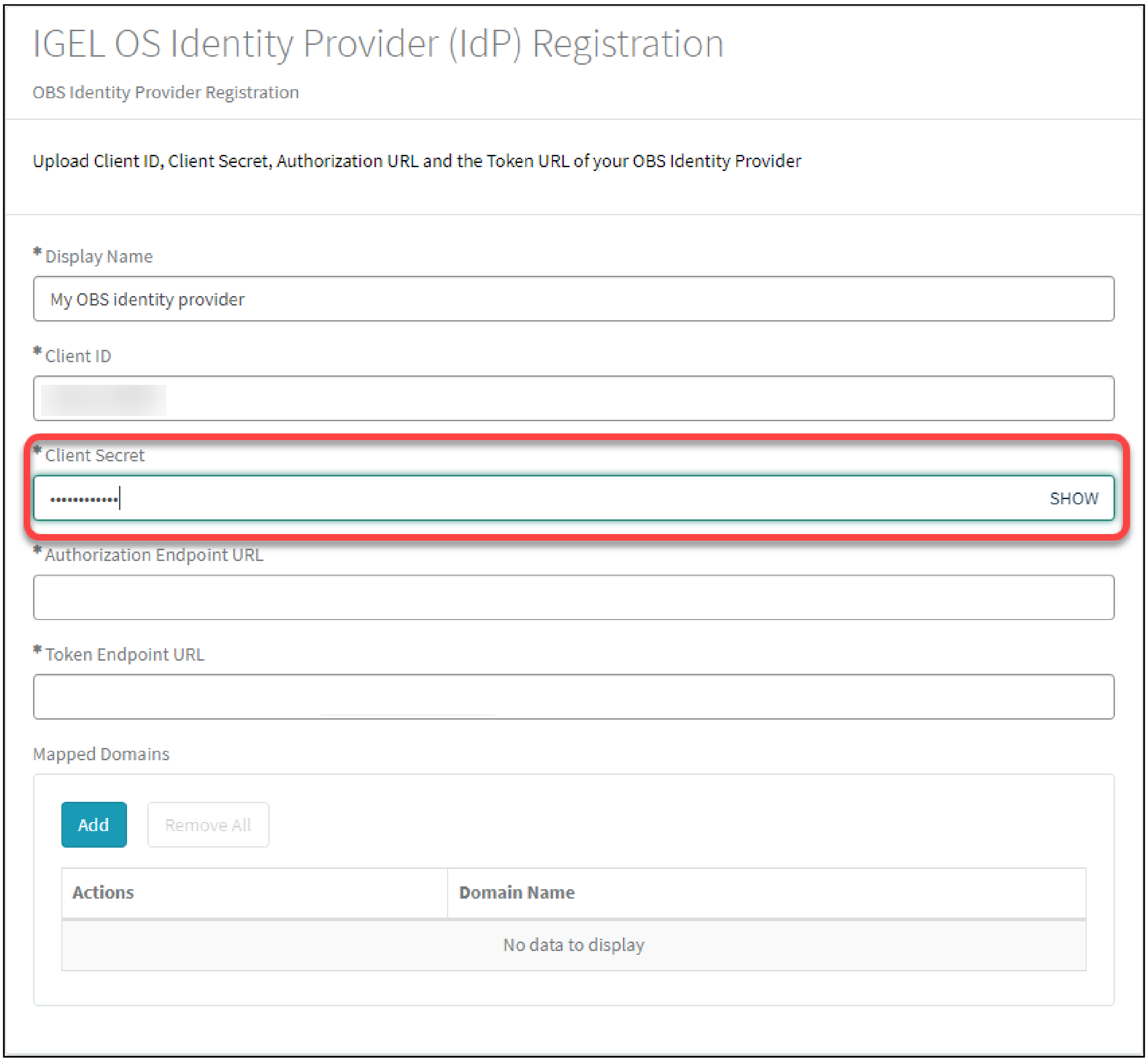
Proof Key for Code Exchange (PKCE)

☑ Require PKCE as additional verification

CLIENT SECRETS

Creation date	Secret	Status
Aug 28, 2023	••	Active ▾

7. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client secret into the field **Client secret**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

*Display Name

My OBS identity provider

*Client ID

[redacted]

*Client Secret

••••••••••••

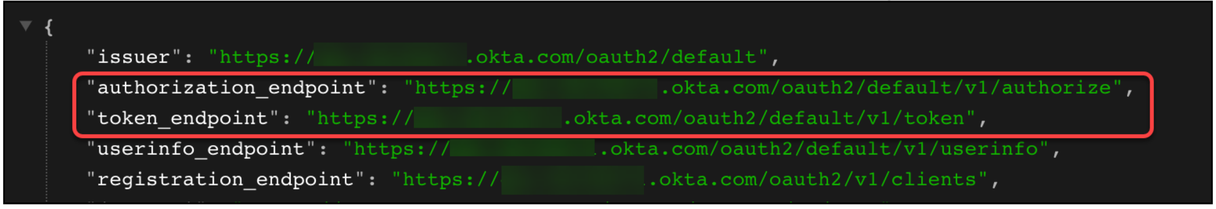
*Authorization Endpoint URL

*Token Endpoint URL

Mapped Domains

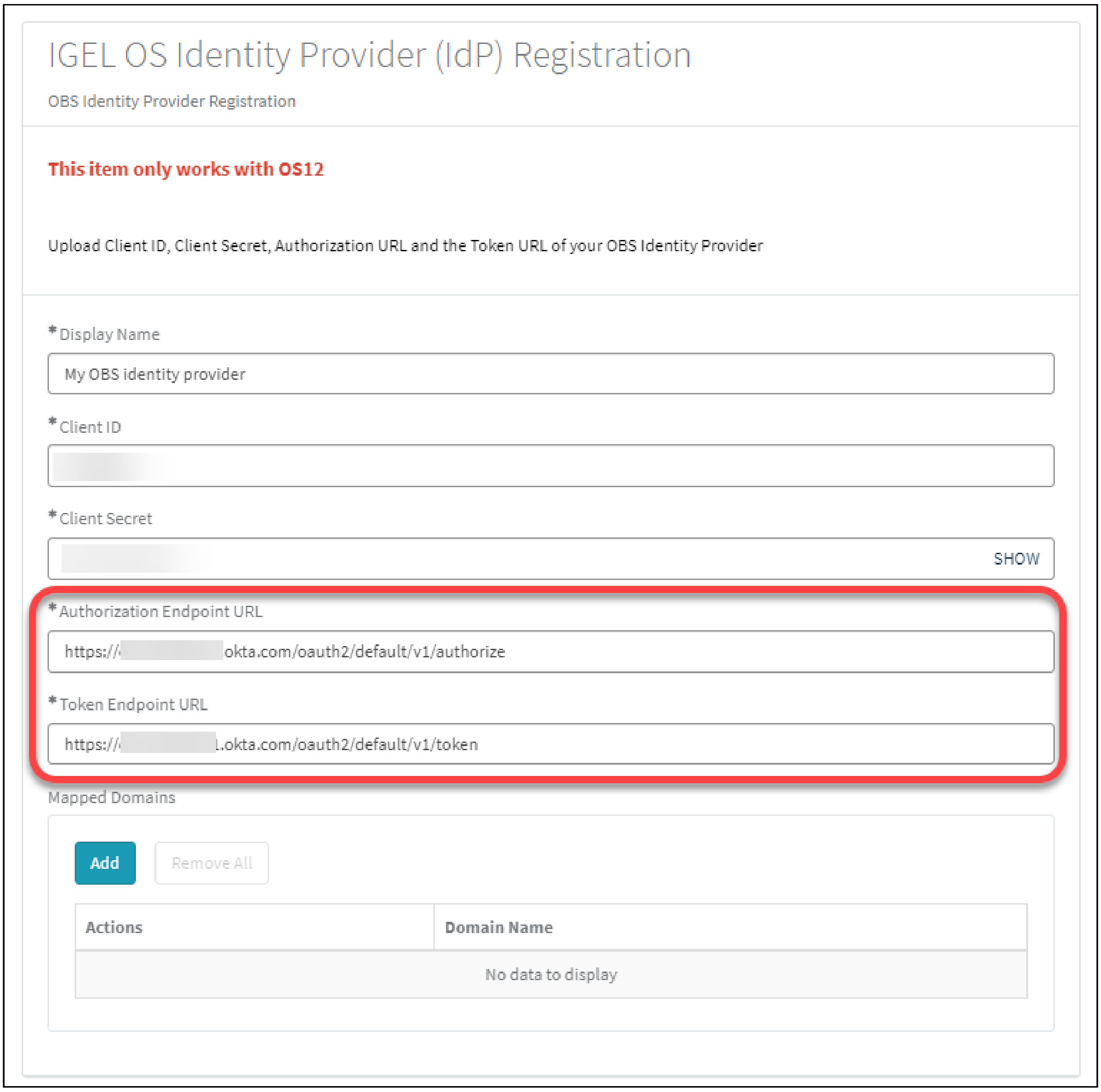
Actions	Domain Name
No data to display	

8. To get the **Authorization Endpoint URL** and **Token Endpoint URL** enter into your browser: `https://<yourOktaOrg>/.well-known/openid-configuration`
Example: https://dev-xxxxxx-admin.okta.com/.well-known/openid-configuration



```
▼ {
    "issuer": "https://[redacted].okta.com/oauth2/default",
    "authorization_endpoint": "https://[redacted].okta.com/oauth2/default/v1/authorize",
    "token_endpoint": "https://[redacted].okta.com/oauth2/default/v1/token",
    "userinfo_endpoint": "https://[redacted].okta.com/oauth2/default/v1/userinfo",
    "registration_endpoint": "https://[redacted].okta.com/oauth2/v1/clients",
```

9. Copy and paste the values into the **Authorization Endpoint URL** and **Token Endpoint URL** fields one by one.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

This item only works with OS12

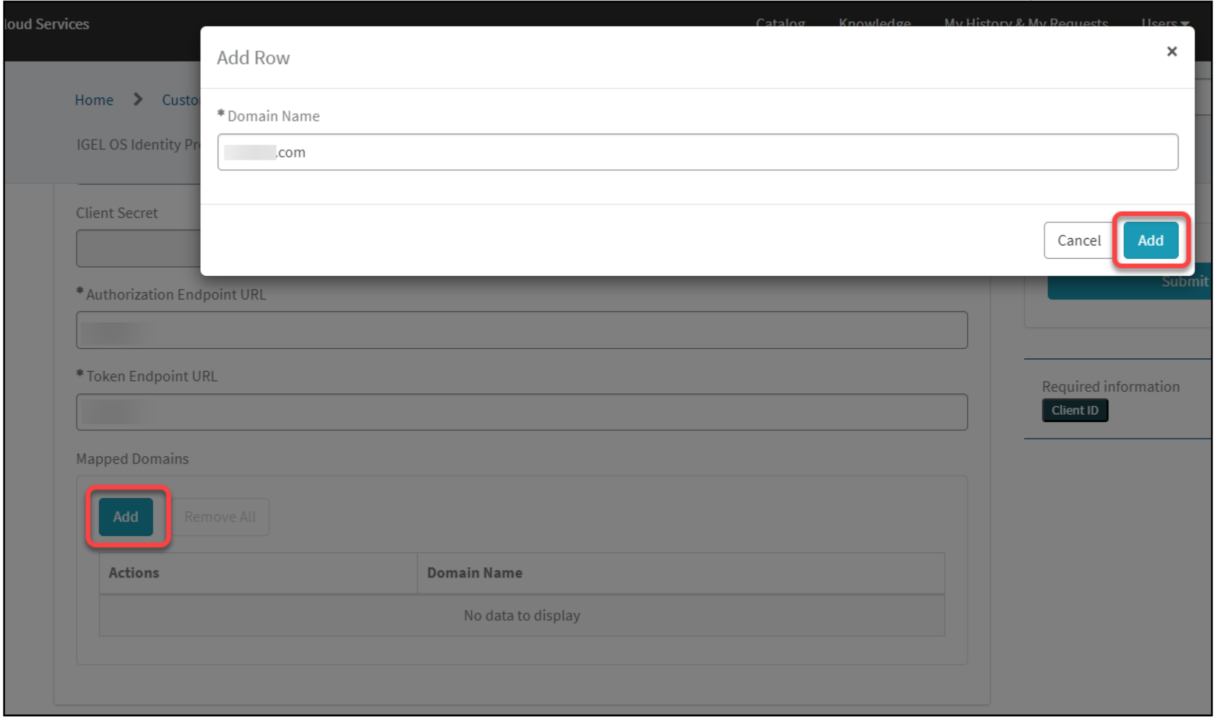
Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name	My OBS identity provider
* Client ID	[redacted]
* Client Secret	[redacted] SHOW
* Authorization Endpoint URL	https://[redacted]okta.com/oauth2/default/v1/authorize
* Token Endpoint URL	https://[redacted]1.okta.com/oauth2/default/v1/token

Mapped Domains

Actions	Domain Name
No data to display	

10. To add a domain, click **Add**, enter the **Domain name**, and then click **Add** in the dialog.



* Domain Name: [redacted].com

Actions	Domain Name
No data to display	

11. Click **Submit**.
    The data record is created.

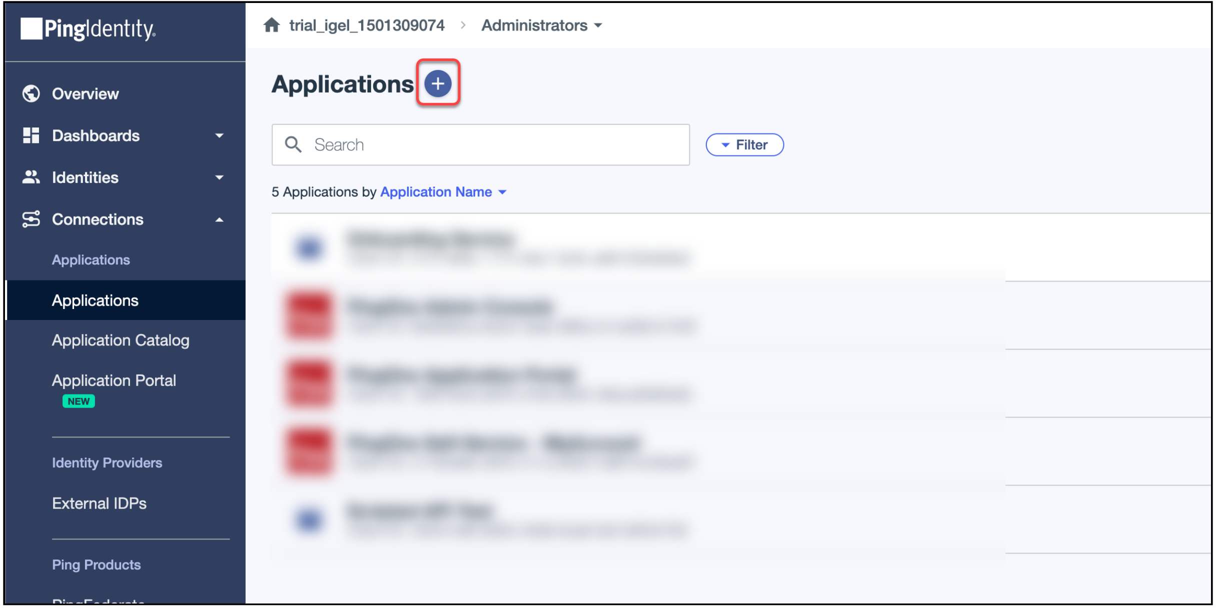
Configuring Ping as Identity Provider

To configure Ping as the identity provider, you need to do the following:

1. Creating a Ping Application That Will Serve as Identity Provider(see page 91): We register an application in Ping Identity to use the service as an external identity provider.
2. Registering Our Ping Application in the IGEL Customer Portal(see page 94): This will enable IGEL Cloud Services to use our Ping Application as the external identity provider.

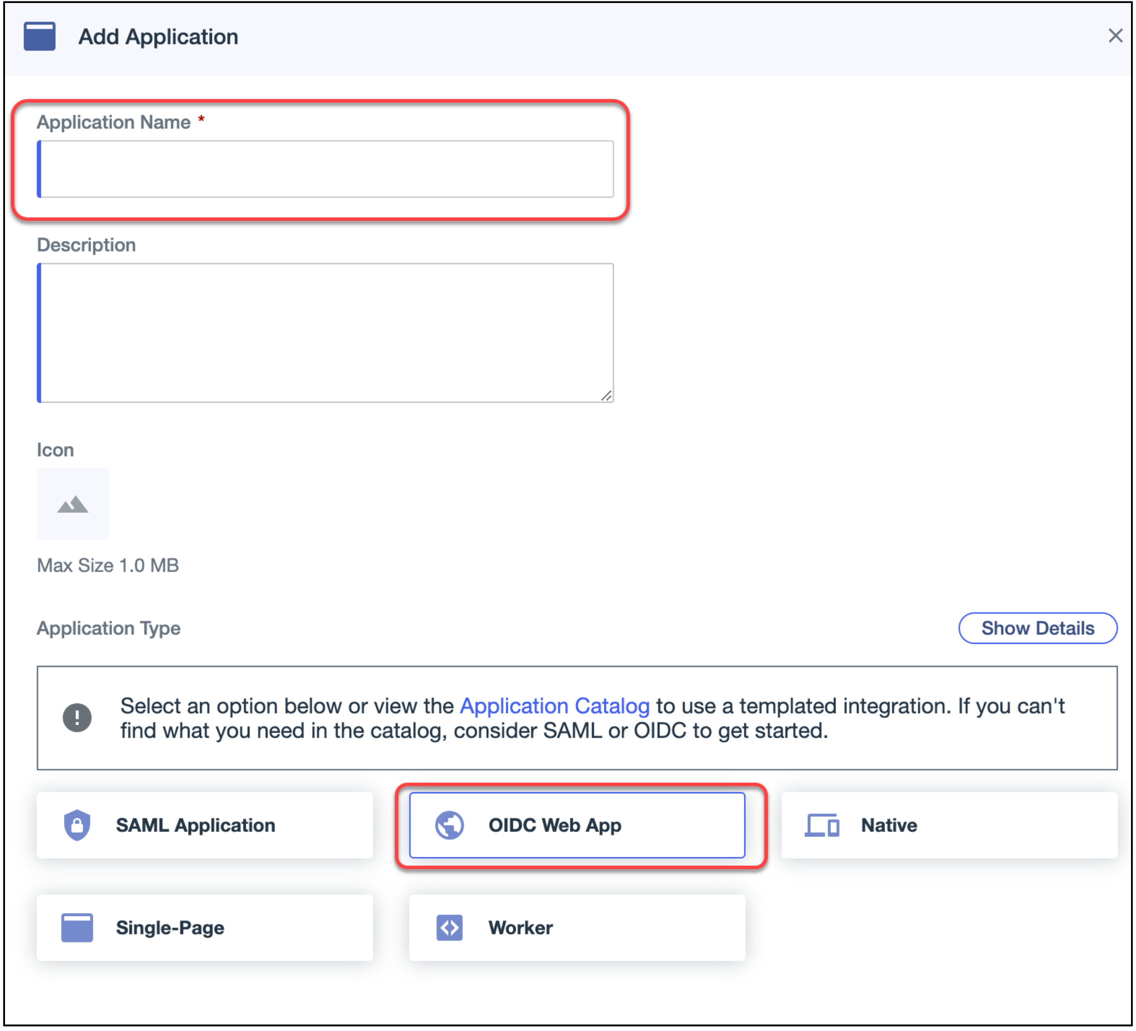
Creating a Ping Application That Will Serve as Identity Provider

1. Log in to Ping with your admin account, and on the **Connections > Applications** page add a new application.



2. Edit the settings as follows and then click **Next**.
   - Under **Application Name**, enter a name for your application, e.g. "OBS".

- Set **Application Type** to **OIDC Web Application**.



Add Application

Application Name *

Description

Icon

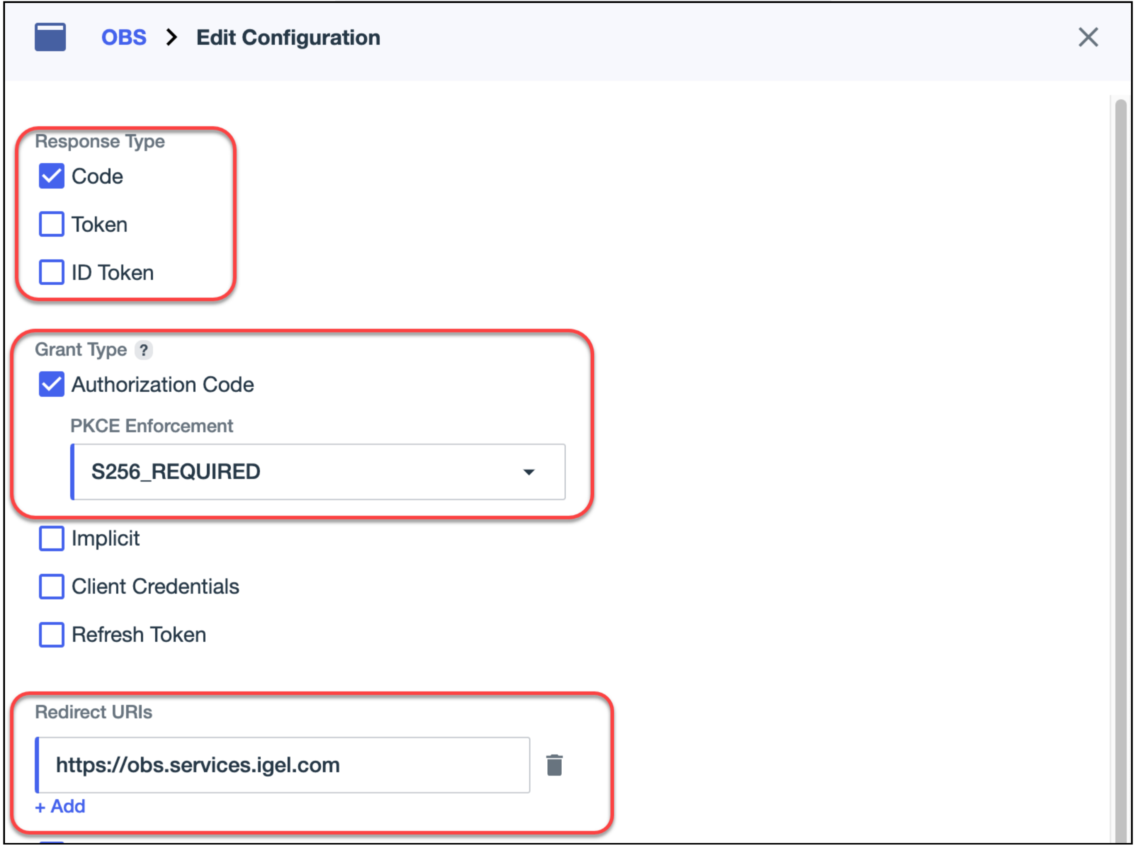
Max Size 1.0 MB

Application Type

Select an option below or view the Application Catalog to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

3. Edit the settings under **Edit Configuration** as follows and then click **Save**.
    - Under **Response Type**, make sure **Code** is selected.
    - Make sure that as the **Grant Type**, the option **Authorization Code** is selected and that the **Proof Key for Code Exchange (PKCE) Enforcement** is set to **S256_REQUIRED**.

- Under **Redirect URIs**, add " `https://obs.services.igel.com/` ".



Response Type

☑ Code

☐ Token

☐ ID Token

Grant Type ?

☑ Authorization Code

PKCE Enforcement

S256_REQUIRED

☐ Implicit

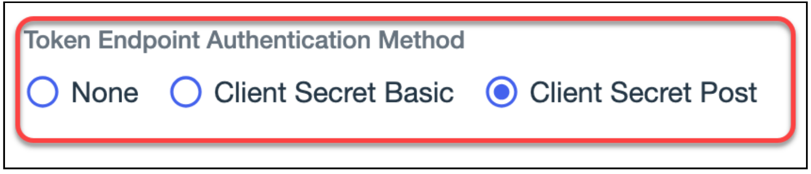
☐ Client Credentials

☐ Refresh Token

Redirect URIs

https://obs.services.igel.com

- Under **Token Endpoint Authentication Method** make sure **Client Secret Post** is selected.

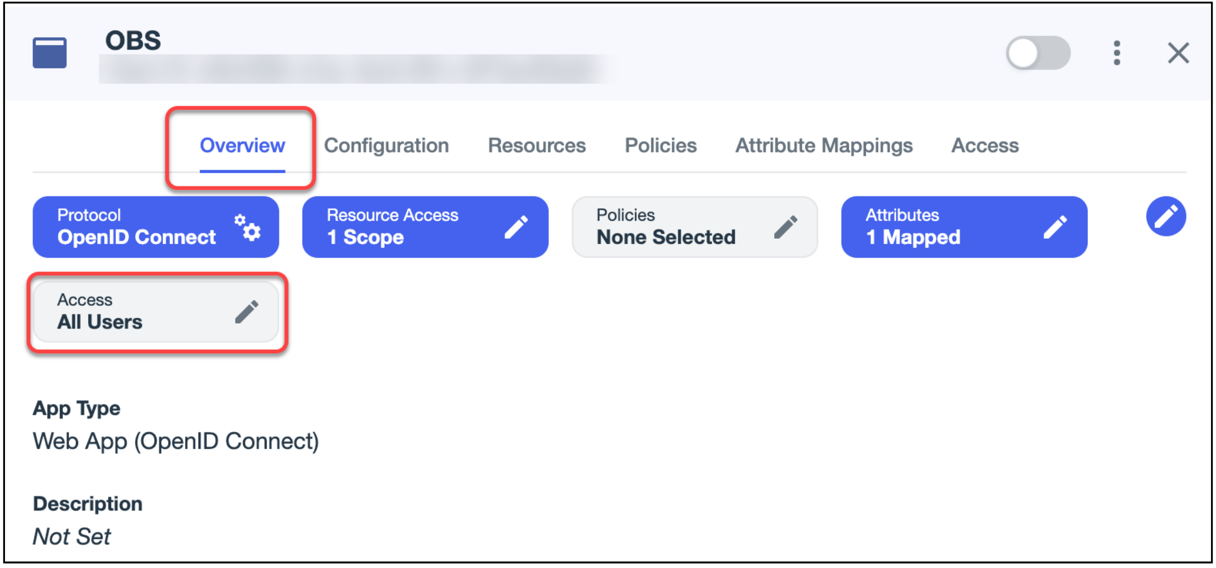


Token Endpoint Authentication Method

○ None ○ Client Secret Basic ● Client Secret Post

4. By default, access is granted for all users. To configure access, open the **Edit Access** page from the **Access** button and use group access by choosing an existing **Group** configured under **Identities >**

Groups.



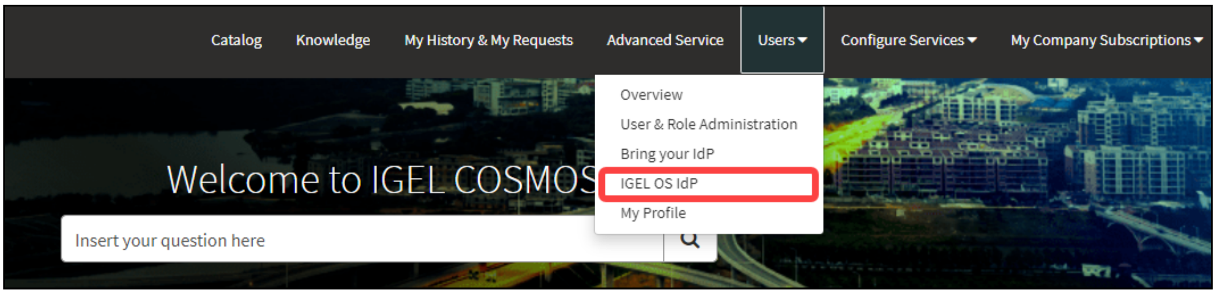
App Type
Web App (OpenID Connect)

Description
Not Set

The app integration is created.

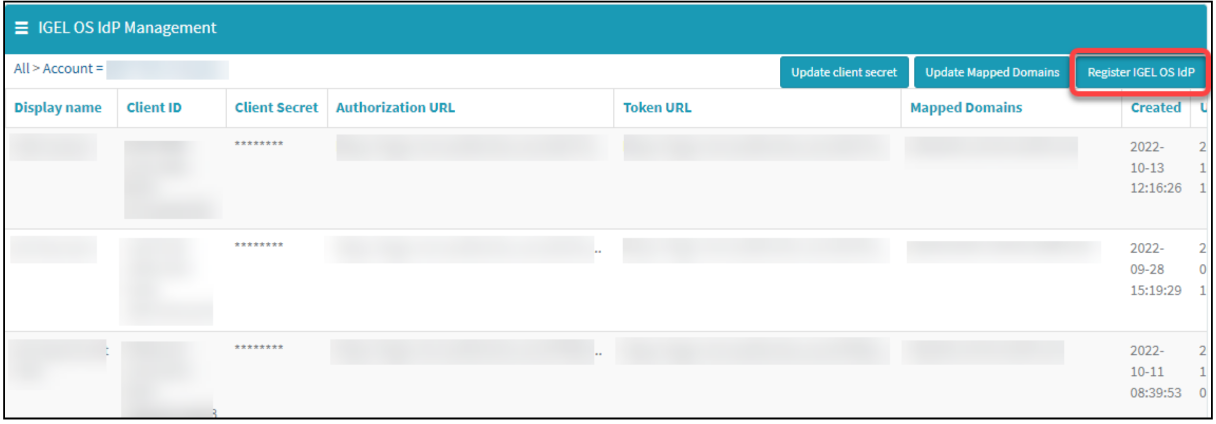
Registering Our Ping Application in the IGEL Customer Portal

1. Open the IGEL Customer Portal[18] in your browser, log in to your admin account, and select **Users > IGEL OS IdP**.



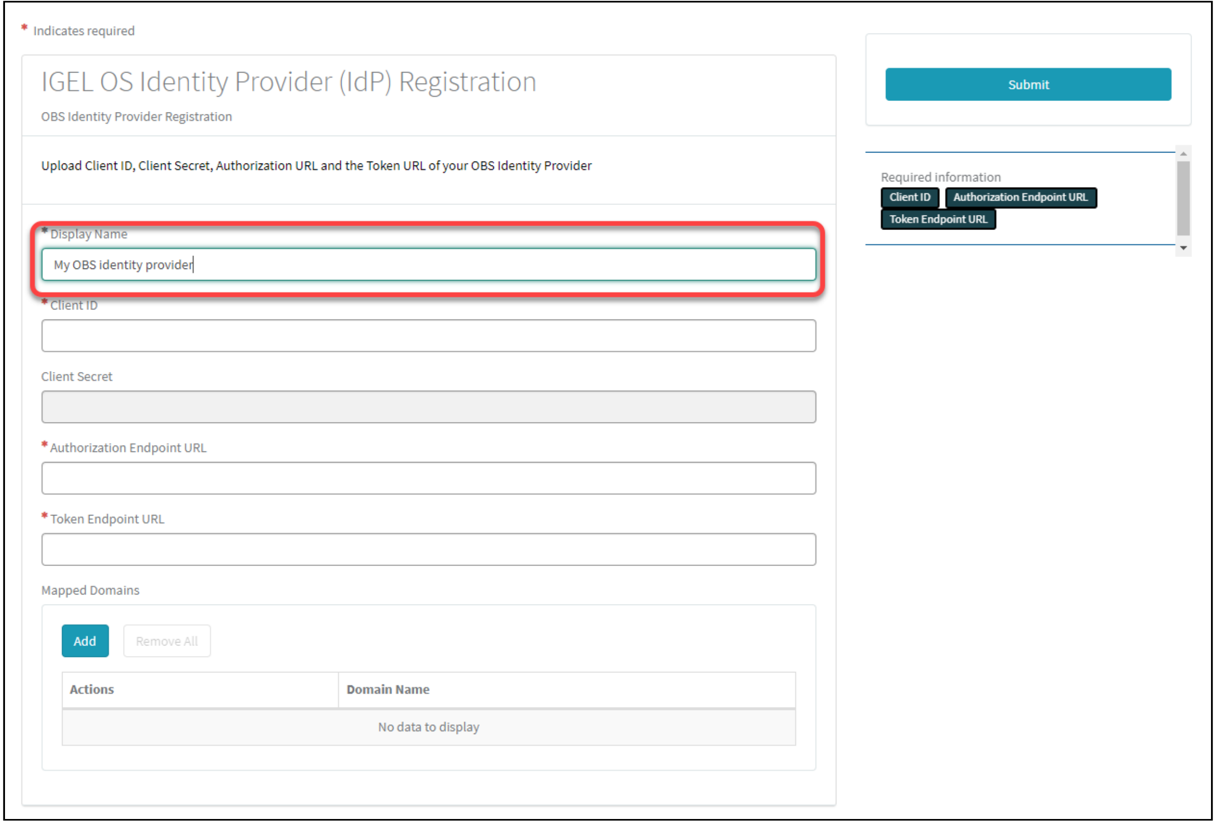
[18] https://cosmos.igel.com/

2. Click **Register IGEL OS IdP**.



Display name	Client ID	Client Secret	Authorization URL	Token URL	Mapped Domains	Created	U
		********				2022-10-13 12:16:26	2 1 1
		********				2022-09-28 15:19:29	2 0 1
		********				2022-10-11 08:39:53	2 1 0

3. Enter a **Display name**. This is the name under which your identity provider app will be displayed.



* Indicates required

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name: My OBS identity provider

* Client ID:

Client Secret:

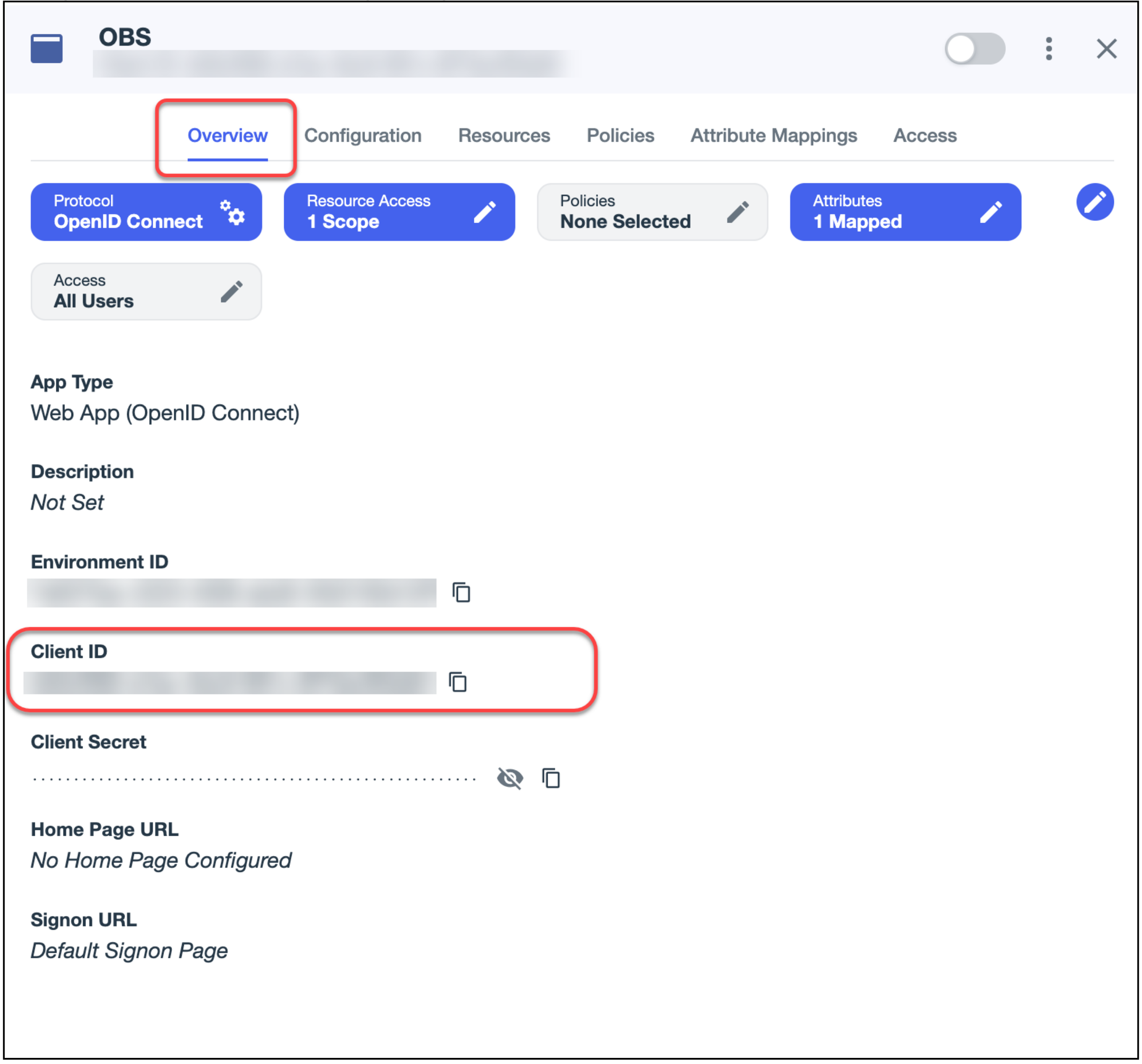
* Authorization Endpoint URL:

* Token Endpoint URL:

Mapped Domains

Actions	Domain Name
No data to display	

4. Change to the tab with your Ping app, go to the **Overview** tab and copy the **Client ID**.



OBS
[redacted]

Protocol
OpenID Connect

Resource Access
1 Scope

Policies
None Selected

Attributes
1 Mapped

Access
All Users

App Type
Web App (OpenID Connect)

Description
Not Set

Environment ID
[redacted]

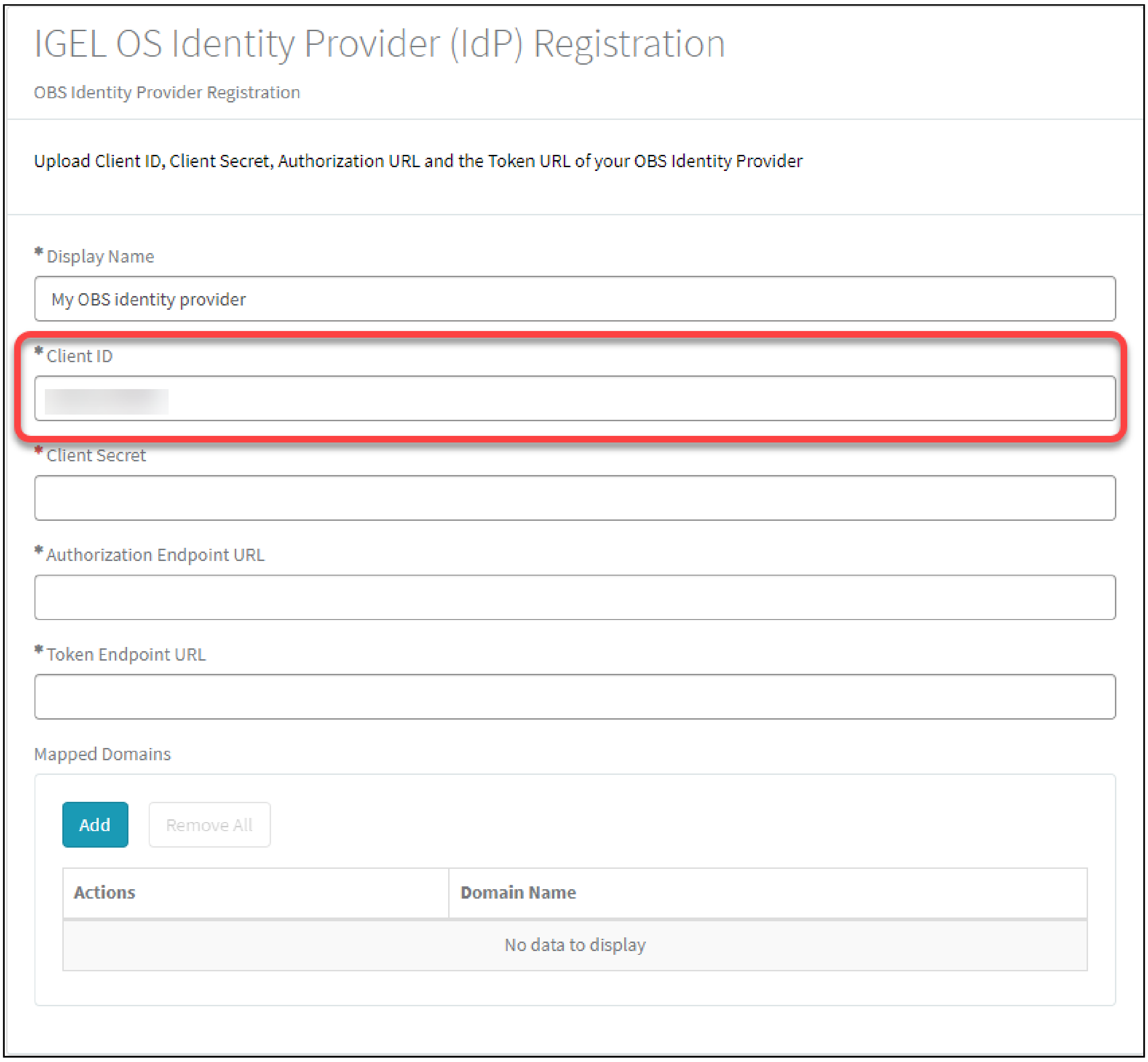
Client ID
[redacted]

Client Secret
....

Home Page URL
No Home Page Configured

Signon URL
Default Signon Page

5. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client ID into the field **Client ID**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

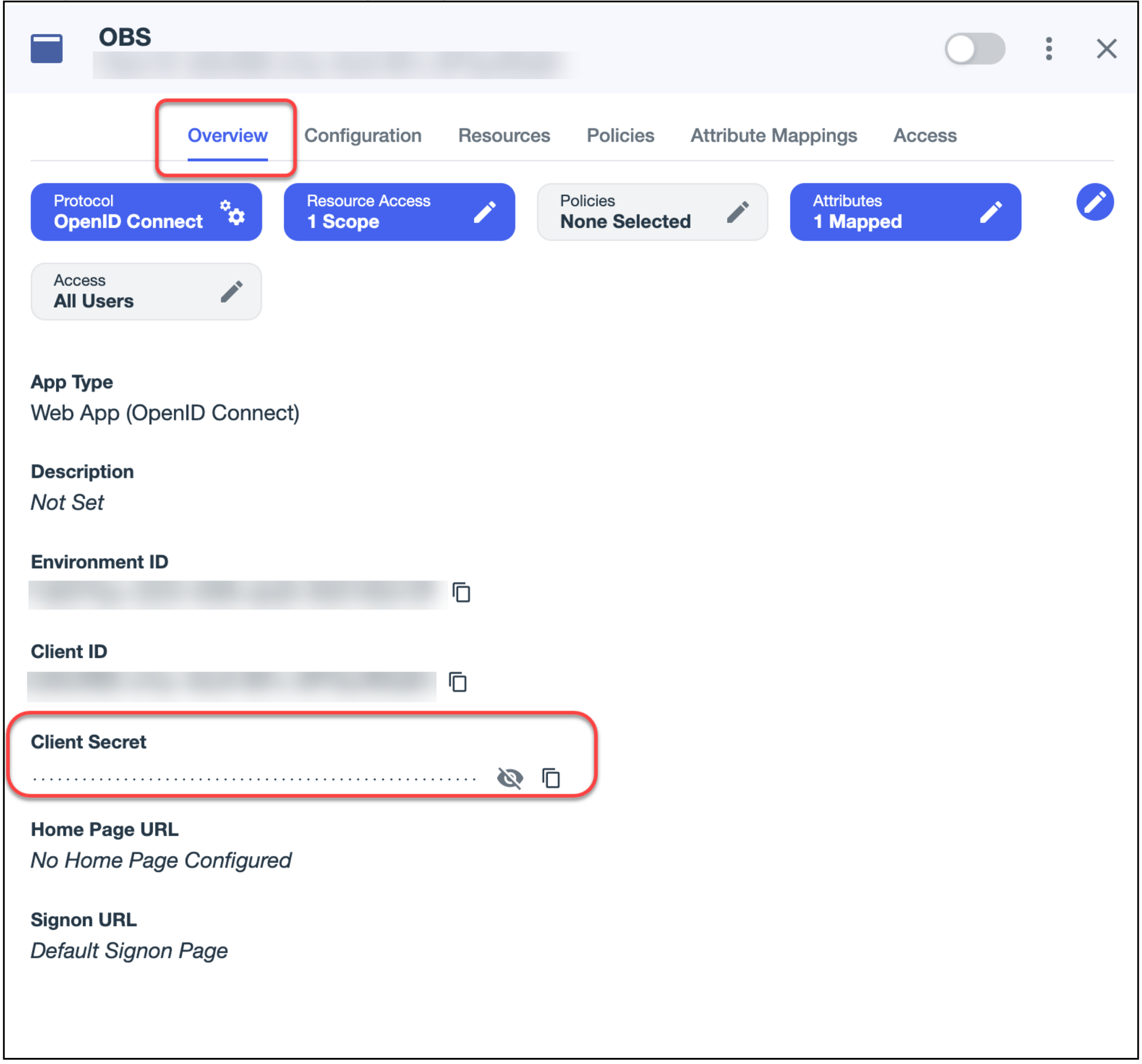
Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name: My OBS identity provider
* Client ID:
* Client Secret:
* Authorization Endpoint URL:
* Token Endpoint URL:

Mapped Domains

Actions	Domain Name
No data to display	

6. Change to the tab with your Ping app, go to the **Overview** tab and copy the **Client Secret**.



OBS

Protocol OpenID Connect

Resource Access 1 Scope

Policies None Selected

Attributes 1 Mapped

Access All Users

App Type
Web App (OpenID Connect)

Description
Not Set

Environment ID

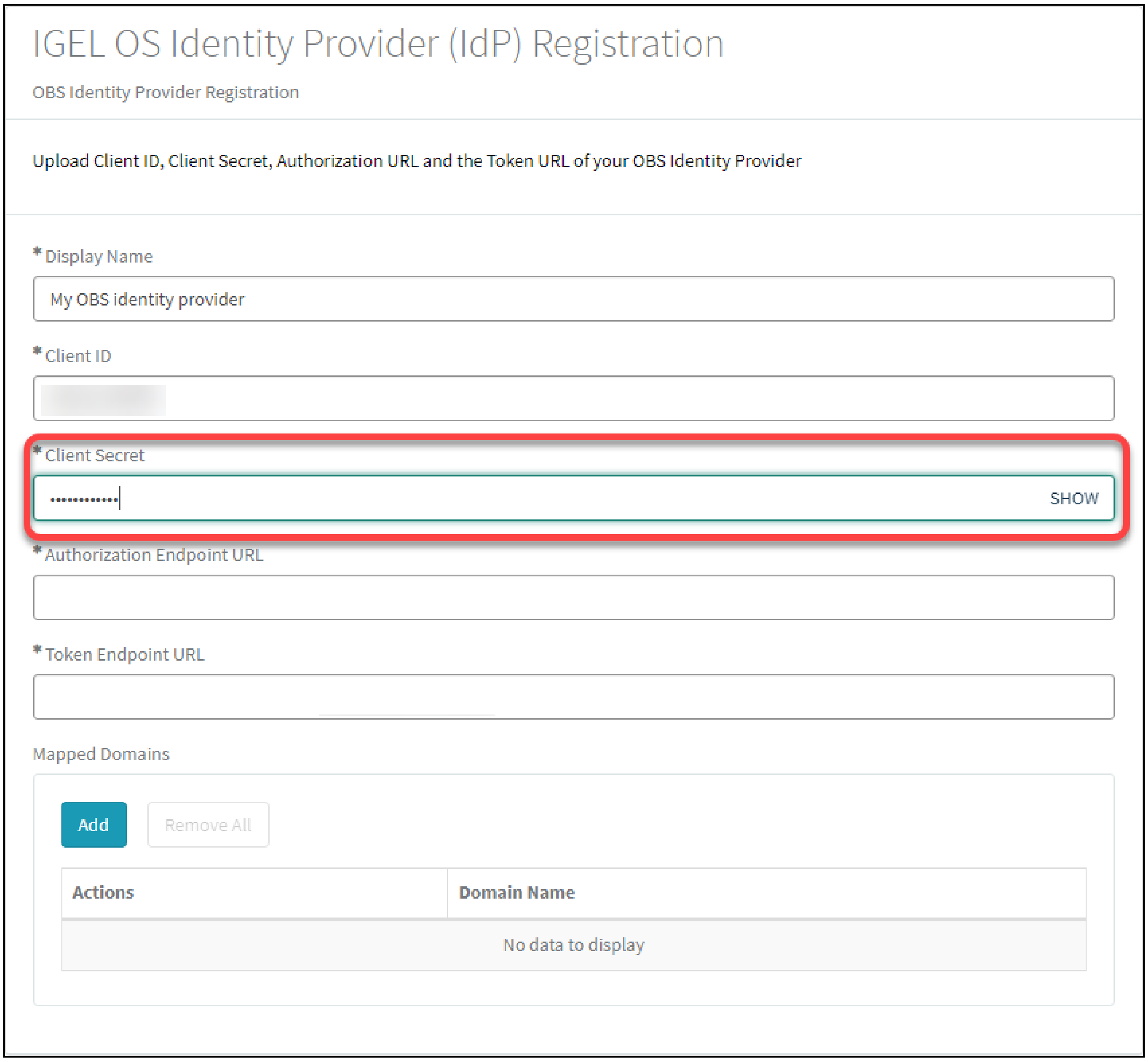
Client ID

Client Secret
···

Home Page URL
No Home Page Configured

Signon URL
Default Signon Page

7. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client secret into the field **Client secret**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

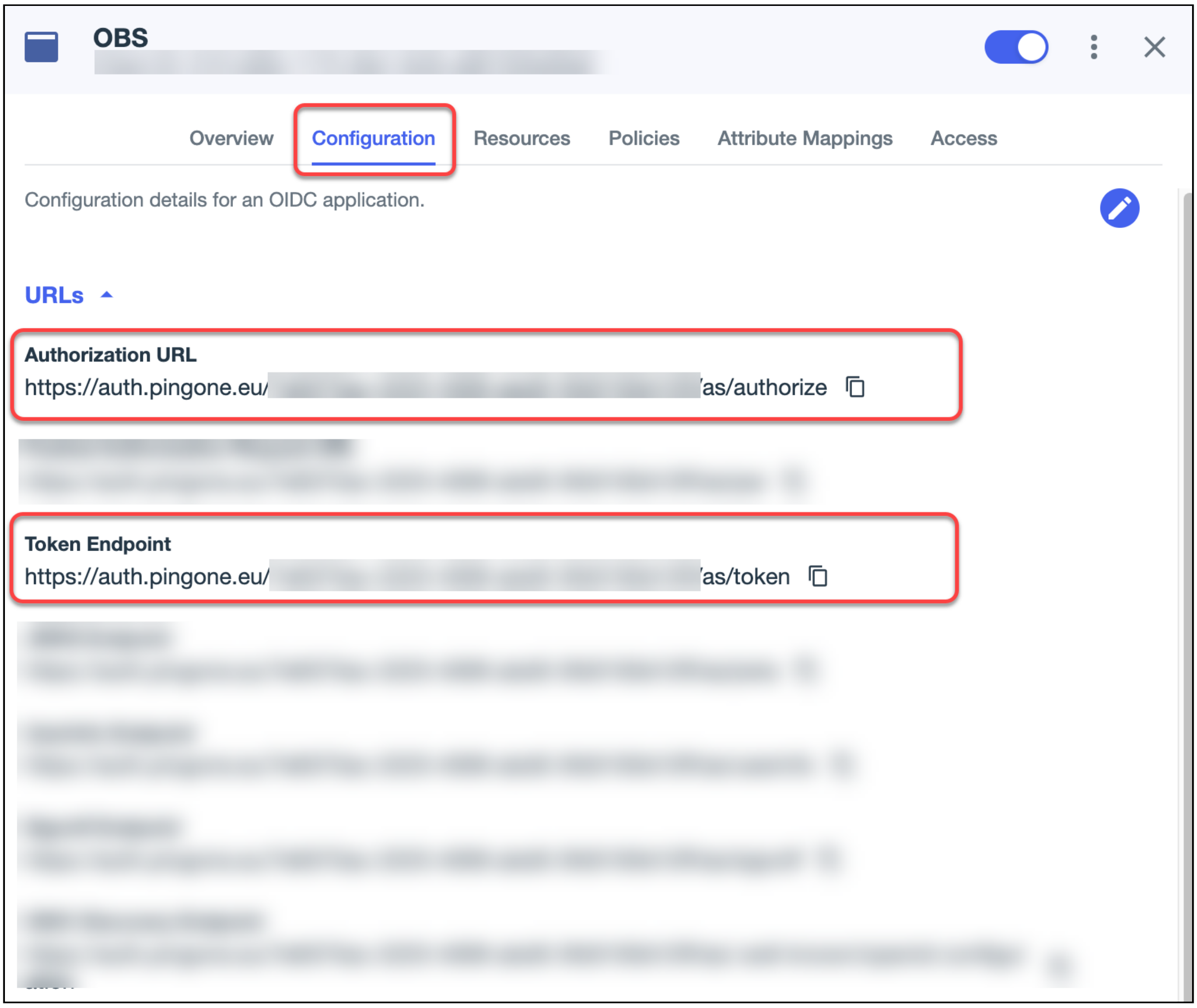
Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name	My OBS identity provider
* Client ID	
* Client Secret	••••••••••••
* Authorization Endpoint URL	
* Token Endpoint URL	

Mapped Domains

Actions	Domain Name
No data to display	

8. To get the **Authorization Endpoint URL** and **Token Endpoint URL**, change to the tab with your Ping app and go to the **Configuration** tab.



OBS

Configuration details for an OIDC application.

URLs

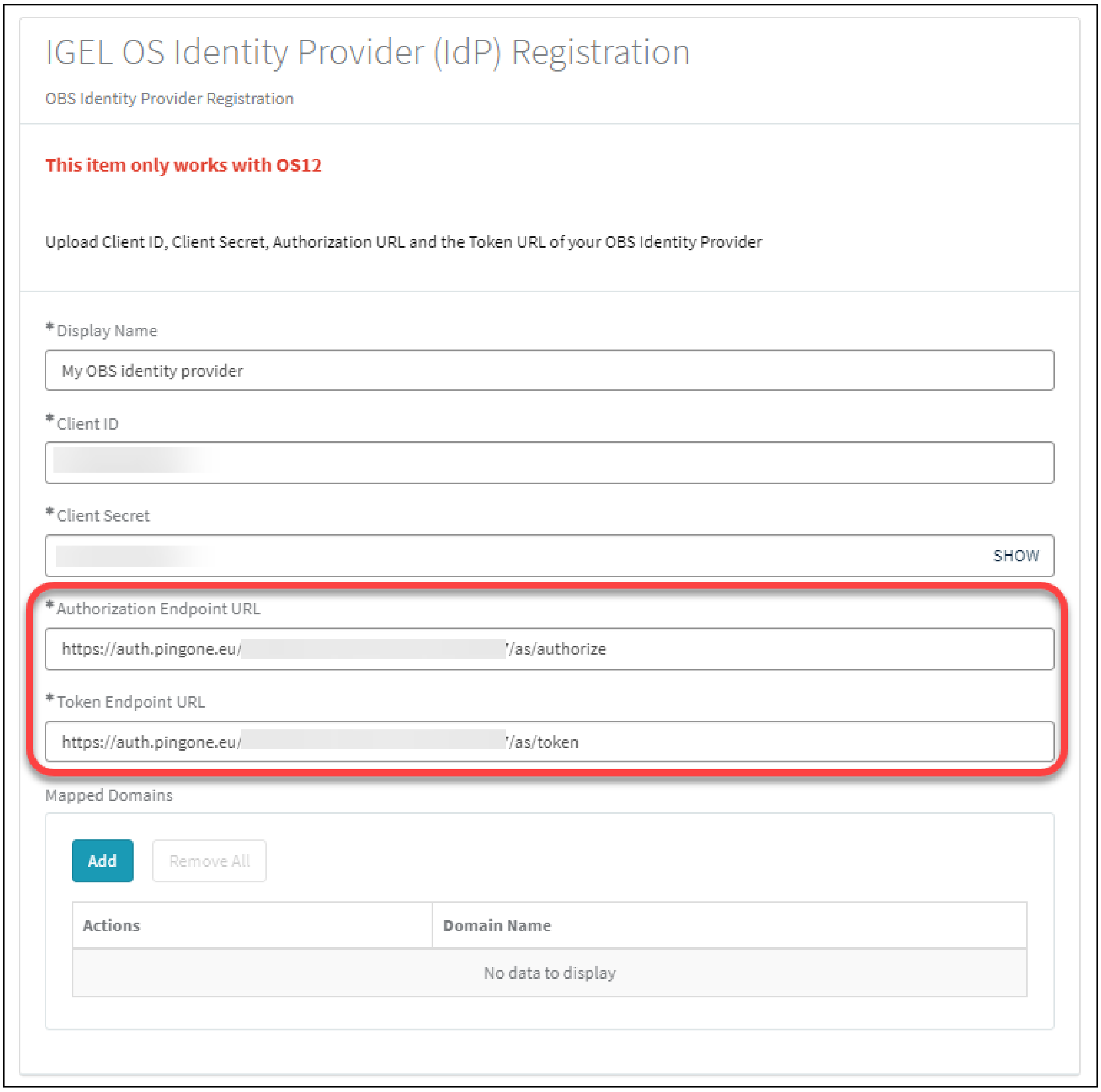
Authorization URL
https://auth.pingone.eu/[redacted]as/authorize

[redacted]

Token Endpoint
https://auth.pingone.eu/[redacted]as/token

[redacted]

9. Copy and paste the values into the **Authorization Endpoint URL** and **Token Endpoint URL** fields one by one.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

This item only works with OS12

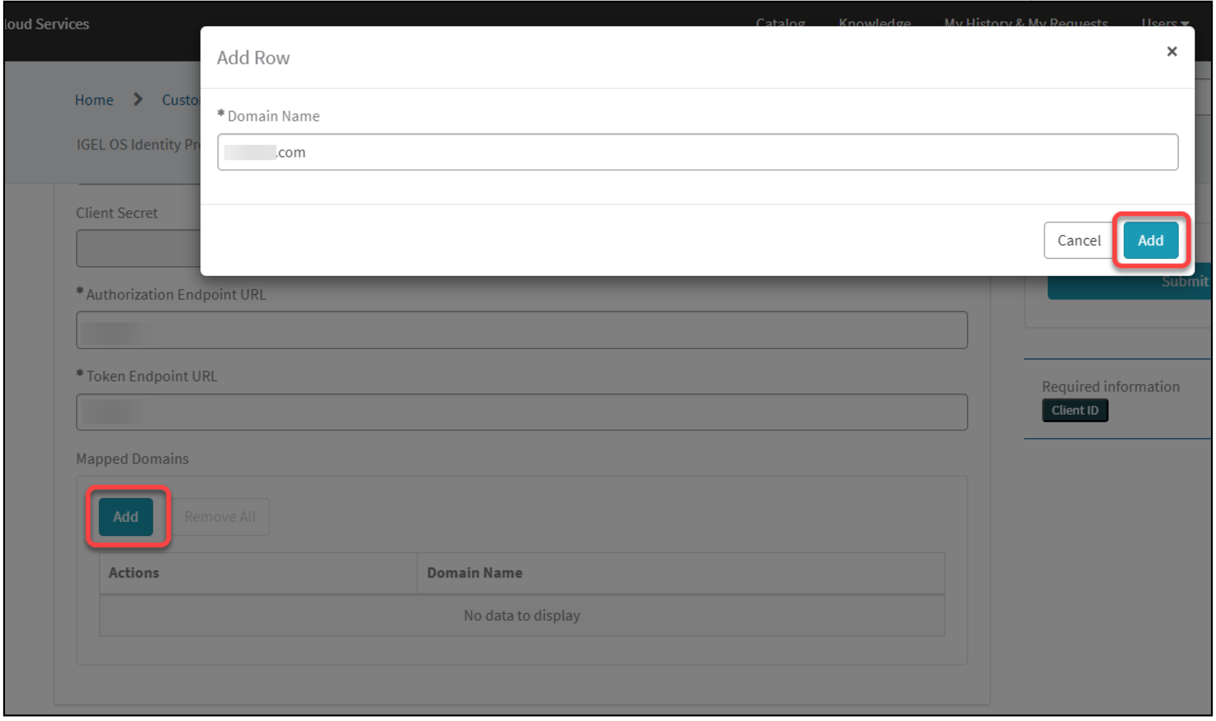
Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name	My OBS identity provider
* Client ID	[redacted]
* Client Secret	[redacted]
* Authorization Endpoint URL	https://auth.pingone.eu/[redacted]/as/authorize
* Token Endpoint URL	https://auth.pingone.eu/[redacted]/as/token

Mapped Domains

Actions	Domain Name
No data to display	

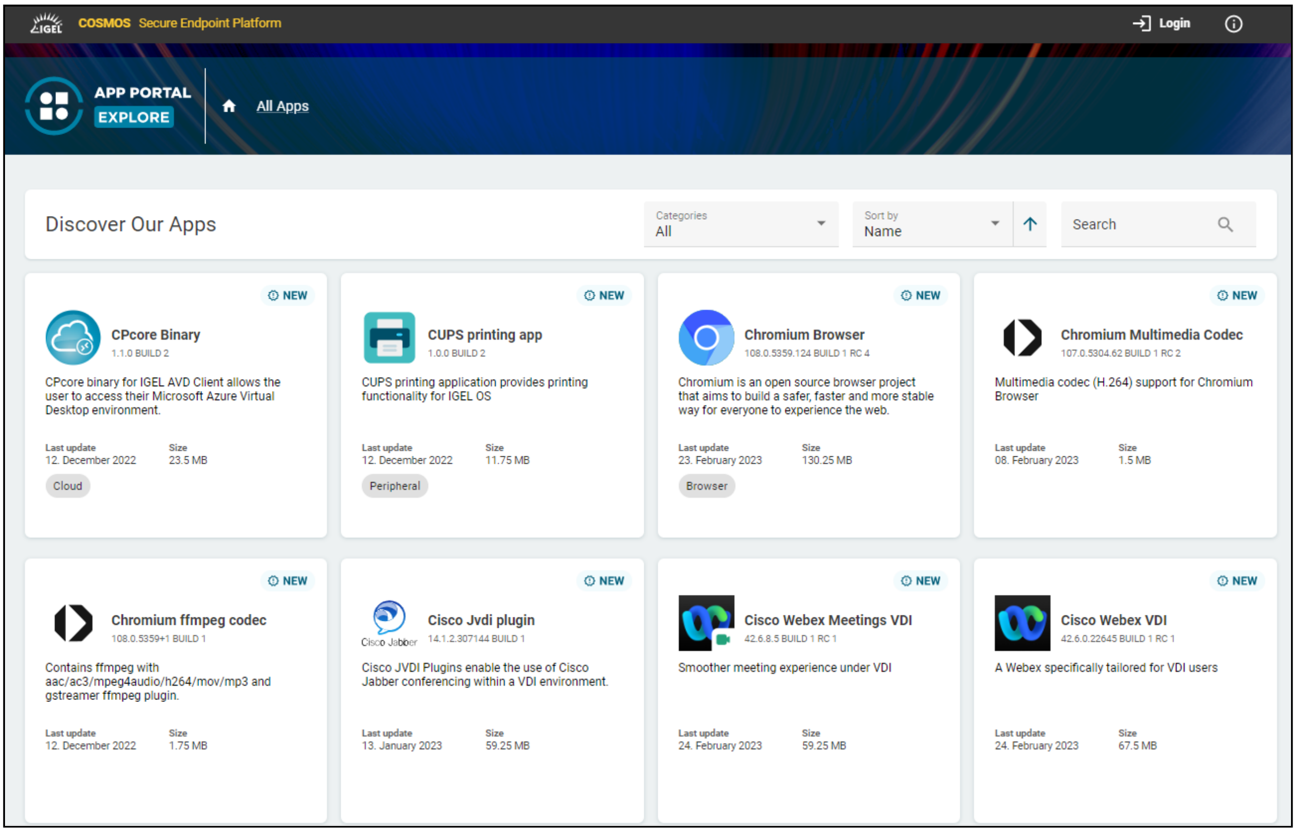
10. To add a domain, click **Add**, enter the **Domain name**, and then click **Add** in the dialog.



11. Click **Submit**.
The data record is created.

IGEL App Portal

With IGEL OS 12, the modular principle is introduced – you can install and update single applications like Citrix or AVD client, Chromium browser, etc. individually. All applications currently available for IGEL OS 12 can be found in the IGEL App Portal.



NEW
CPcore Binary
1.1.0 BUILD 2
CPcore binary for IGEL AVD Client allows the user to access their Microsoft Azure Virtual Desktop environment.
Last update 12. December 2022 Size 23.5 MB
Cloud

NEW
CUPS printing app
1.0.0 BUILD 2
CUPS printing application provides printing functionality for IGEL OS
Last update 12. December 2022 Size 11.75 MB
Peripheral

NEW
Chromium Browser
108.0.5359.124 BUILD 1 RC 4
Chromium is an open source browser project that aims to build a safer, faster and more stable way for everyone to experience the web.
Last update 23. February 2023 Size 130.25 MB
Browser

NEW
Chromium Multimedia Codec
107.0.5304.62 BUILD 1 RC 2
Multimedia codec (H.264) support for Chromium Browser
Last update 08. February 2023 Size 1.5 MB

NEW
Chromium ffmpeg codec
108.0.5359+1 BUILD 1
Contains ffmpeg with aac/ac3/mpeg4audio/h264/mov/mp3 and gstreamer ffmpeg plugin.
Last update 12. December 2022 Size 1.75 MB

NEW
Cisco Jvdi plugin
Cisco Jabber
14.1.2.307144 BUILD 1
Cisco JVDI Plugins enable the use of Cisco Jabber conferencing within a VDI environment.
Last update 13. January 2023 Size 59.25 MB

NEW
Cisco Webex Meetings VDI
42.6.8.5 BUILD 1 RC 1
Smoother meeting experience under VDI
Last update 24. February 2023 Size 59.25 MB

NEW
Cisco Webex VDI
42.6.0.22645 BUILD 1 RC 1
A Webex specifically tailored for VDI users
Last update 24. February 2023 Size 67.5 MB

> ⓘ Changelogs for IGEL OS Apps and IGEL OS Base System can be found in the IGEL App Portal.

> ⓘ **Where Are the IGEL COSMOS Cloud Services Data Stored?**
> Currently, the IGEL COSMOS Cloud Services and apps available in the IGEL App Portal are stored in Azure Region West-Europe, location Amsterdam. The associated app metadata are stored in Frankfurt (Germany west central).
> The Insight Service data are currently also stored in Frankfurt (Germany west central).
> All data centers and their operators are fully ISO/IEC 27001 certified.

Access to the IGEL App Portal

> ⚠ The import of apps to the UMS as well as the download of apps to the UMS-managed devices is only possible if the UMS is registered in the IGEL Customer Portal. For the instructions, see Registering the UMS(see page 36).

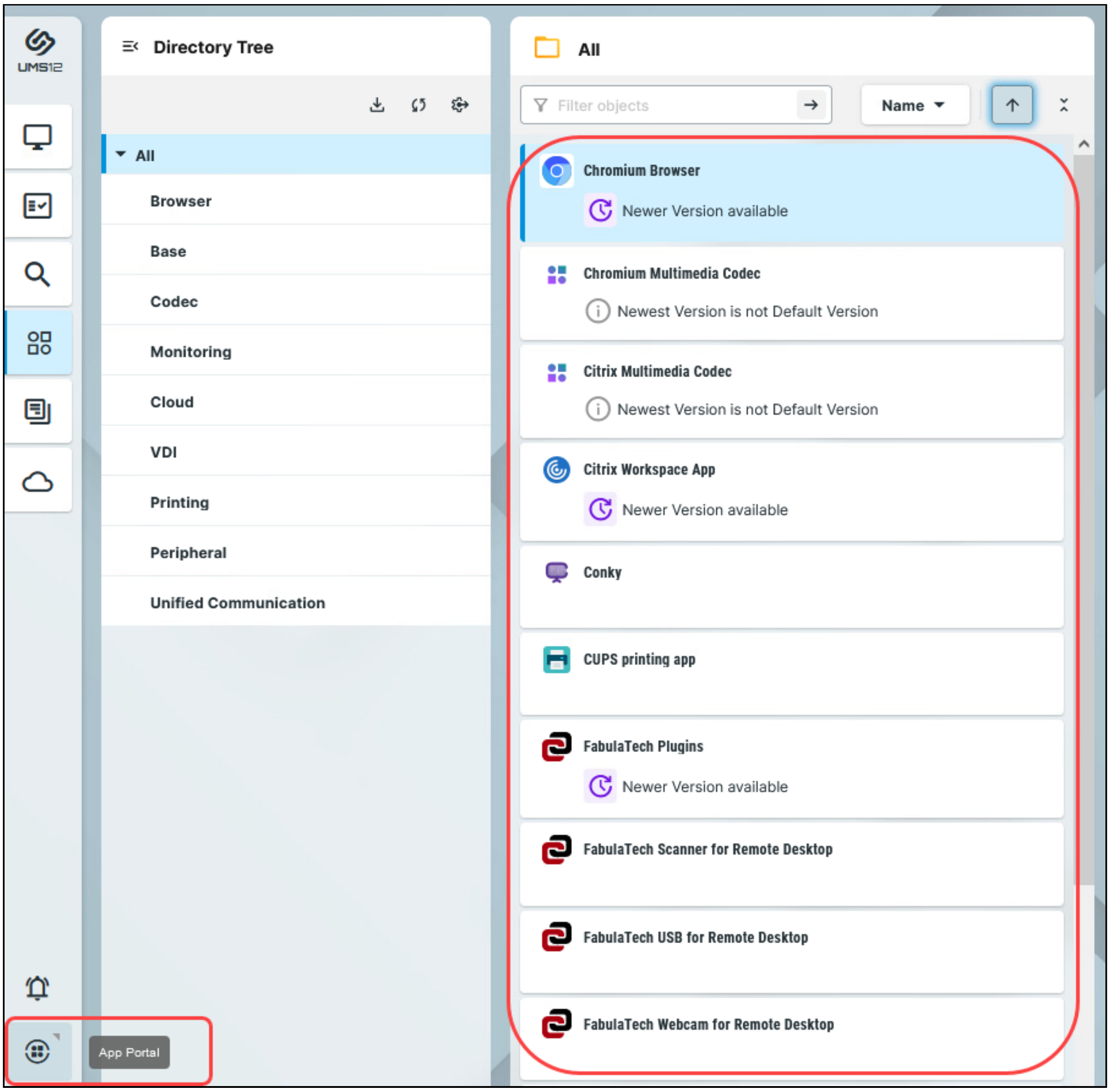
If the device is not managed with the UMS, the download of apps is possible but NOT for the devices with a Starter license. For more information on licenses, see Licensing(see page 151).

You can open the IGEL App Portal

- directly via https://app.igel.com/ (i.e. context: Explore)
  With this method, you can get a general overview of available apps.

- locally on the device via the **App Portal** application (i.e. context: OS12)
  With this method, you can install or uninstall apps locally on the device. For more information, see Installing IGEL OS Apps Locally on the Device(see page 190).
  Here, you can find the following buttons:
  - **All**: All apps
  - **Available**: All new apps and apps to be updated
  - **Installed**: All apps that have already been installed on the device

- via **UMS Web App > App Portal** (i.e. context: UMS admin)
  With this method, you can import apps in the UMS to deploy them to your endpoint devices.



Chromium Browser
Newer Version available

Chromium Multimedia Codec
Newest Version is not Default Version

Citrix Multimedia Codec
Newest Version is not Default Version

Citrix Workspace App
Newer Version available

Conky

CUPS printing app

FabulaTech Plugins
Newer Version available

FabulaTech Scanner for Remote Desktop

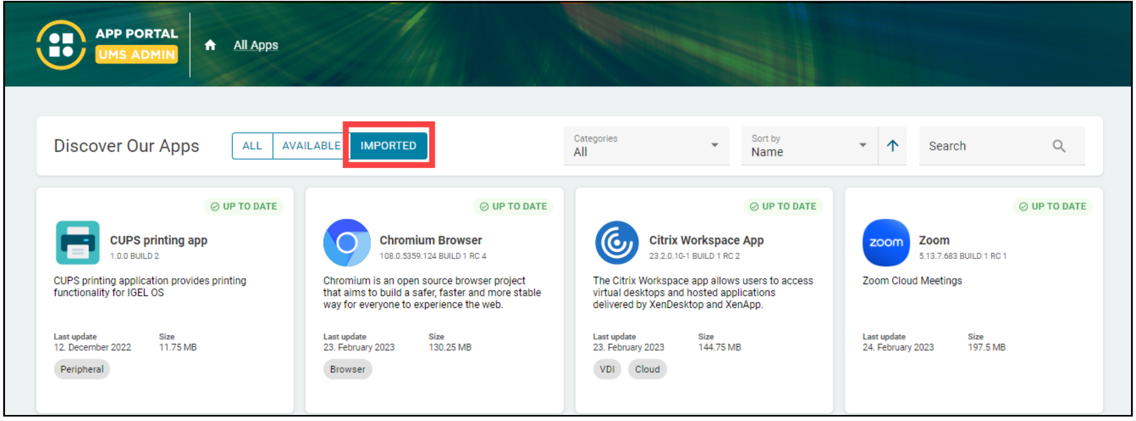
FabulaTech USB for Remote Desktop

FabulaTech Webcam for Remote Desktop

Here, you can find the following buttons:

- **All**: All apps
- **Available**: All new apps and apps to be updated

- **Imported**: All apps that have already been imported to the UMS. In the UMS Web App, the imported apps are displayed under **Apps**.



CUPS printing app
1.0.0 BUILD 2
CUPS printing application provides printing functionality for IGEL OS
Last update 12. December 2022 Size 11.75 MB
Peripheral

Chromium Browser
108.0.5359.124 BUILD 1 RC 4
Chromium is an open source browser project that aims to build a safer, faster and more stable way for everyone to experience the web.
Last update 23. February 2023 Size 130.25 MB
Browser

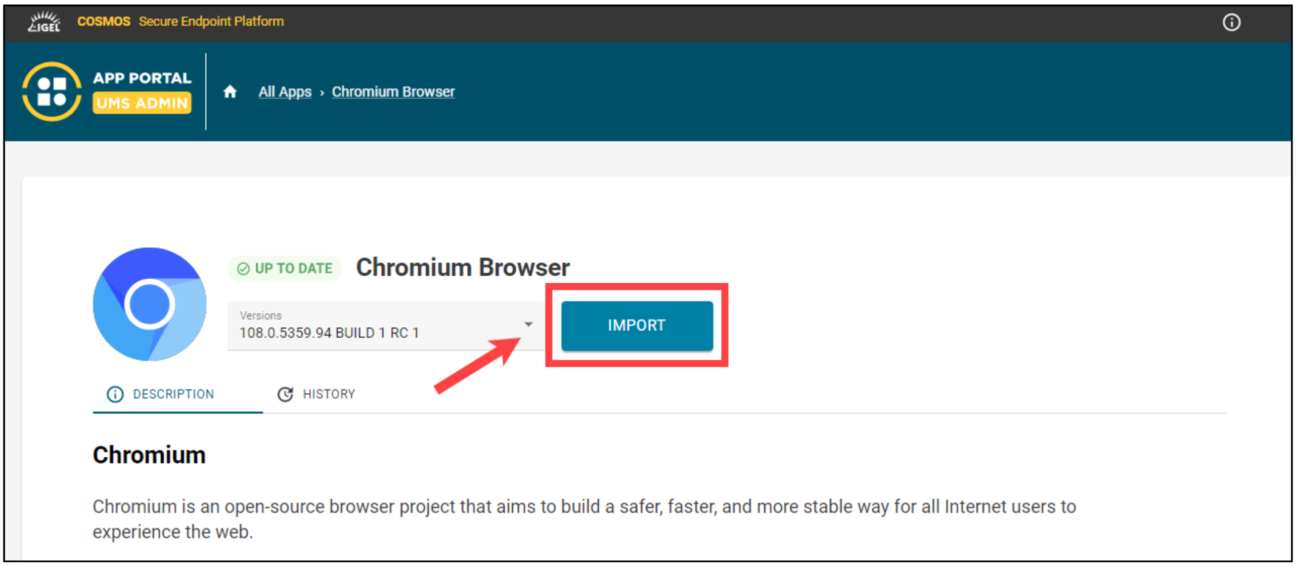
Citrix Workspace App
23.2.0.10-1 BUILD 1 RC 2
The Citrix Workspace app allows users to access virtual desktops and hosted applications delivered by XenDesktop and XenApp.
Last update 23. February 2023 Size 144.75 MB
VDI Cloud

Zoom
5.13.7.683 BUILD 1 RC 1
Zoom Cloud Meetings
Last update 24. February 2023 Size 197.5 MB

ⓘ For permissions required for managing apps, see Important Information for the IGEL UMS Web App.

Importing Apps to the IGEL UMS

To import an app from the IGEL App Portal, simply select the required app and its version and click **Import**. After accepting the End User License Agreement (EULA), the selected app version will be imported into the UMS.



Chromium Browser

Versions: 108.0.5359.94 BUILD 1 RC 1

Chromium

Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all Internet users to experience the web.

ⓘ If the selected app / app version has already been imported, the **Import** icon is greyed out.

IGEL UMS 12: Basic Configuration

IGEL UMS 12 uses a web-based user interface to administer IGEL OS devices – the UMS Web App.

To log in to the UMS Web App, you can use the credentials of the UMS superuser (if not changed under **UMS Administrator > Datasource > UMS superuser**, the same as the **User Credentials for DB-connect** you set when installing the UMS with the embedded database); see How to Log In to the IGEL UMS Web App.

First Steps in the IGEL UMS

It is recommended to consider the following settings before onboarding / registering your devices. These settings are made in the IGEL UMS Console.

You can log in to the UMS Console using the credentials you set under **User Credentials for DB-connect** when installing the UMS with the embedded database; for more information, see Connecting the UMS Console to the IGEL UMS Server.

System Configuration

1. Activate logging under **UMS Administration > Global Configuration > Logging**.

2. Under **UMS Administration > Administrative tasks**, create the following administrative tasks:
   - Create backup (for the embedded database only. If you use an external database, see Creating a Backup of the IGEL UMS)
   - Delete logging data
   - Other tasks to automatically clean up logs (job execution data, execution data of administrative tasks, process events, asset information history)

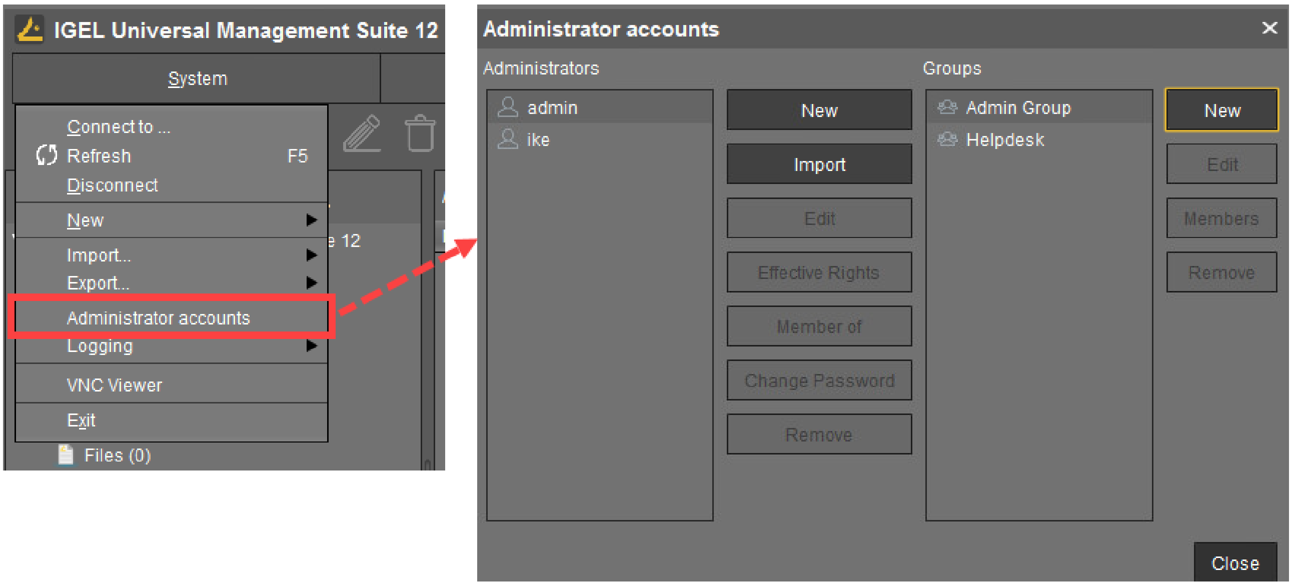
3. If you want to activate the naming convention for your devices, go to **UMS Administration > Global Configuration > Device Network Settings**. For more information, see Renaming IGEL OS Devices.

Administrator Accounts

In the IGEL UMS, you can import administrative accounts from your existing Active Directory (AD). If you want to do this, you have to link at first the UMS Server to the existing AD, see Active Directory / LDAP. After that, you can import users or user groups from your AD under **UMS Console > System > Administrator Accounts > Import**.

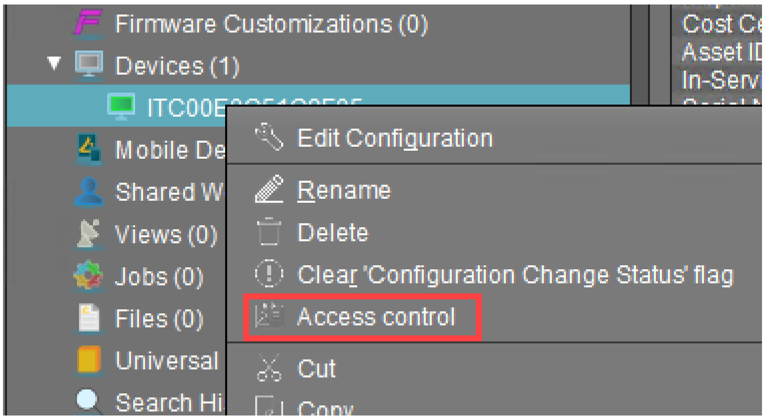
If you do not want to adopt the Active Directory structure, you can create local administrators and groups manually: **UMS Console > System > Administrator Accounts > New**.

Permission settings are performed in the same way for both groups and individual administrators.



Each administrator / group can be granted specific permissions with regard to objects in the structure tree:

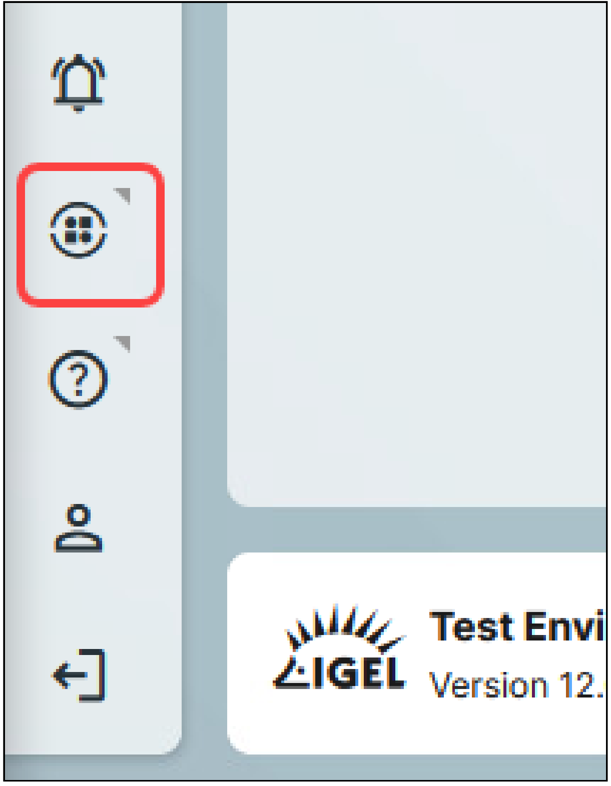
▶ Right-click an object in the structure tree and select **Access control** in the context menu to set object permissions.



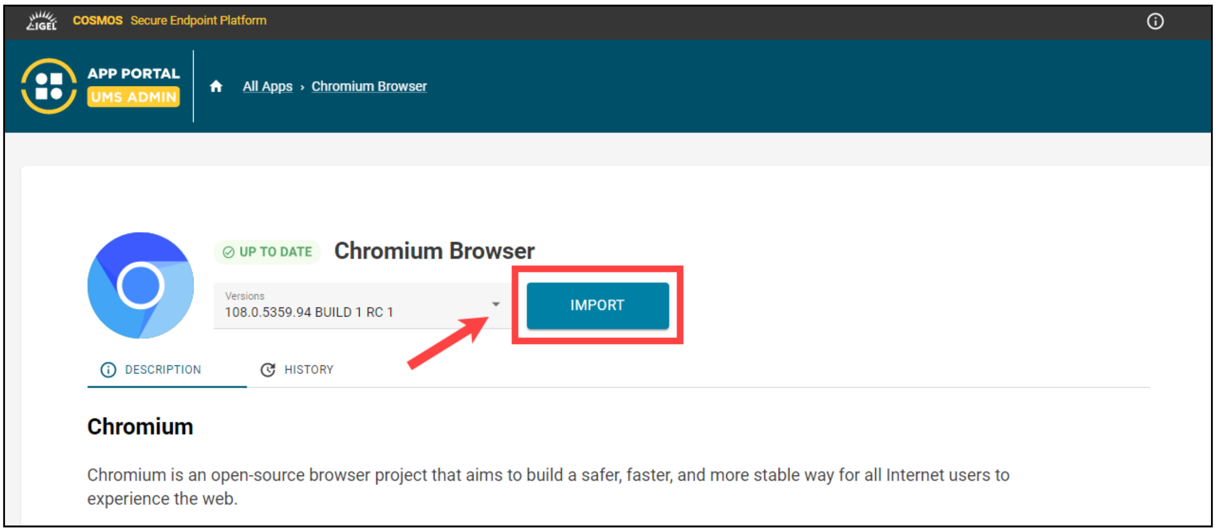
For more information on UMS administrator accounts and access rights, refer to Create Administrator Accounts.
For permissions required for the UMS Web App, incl. for managing apps, see Important Information for the IGEL UMS Web App.

Optional: Preconfiguring Your Devices Before Onboarding

1. In the UMS Web App, click **App Portal** to import IGEL OS Apps.



2. Select an app and the required version and click **Import**.
   After accepting the End User License Agreement (EULA), the selected app version will be imported into the UMS.

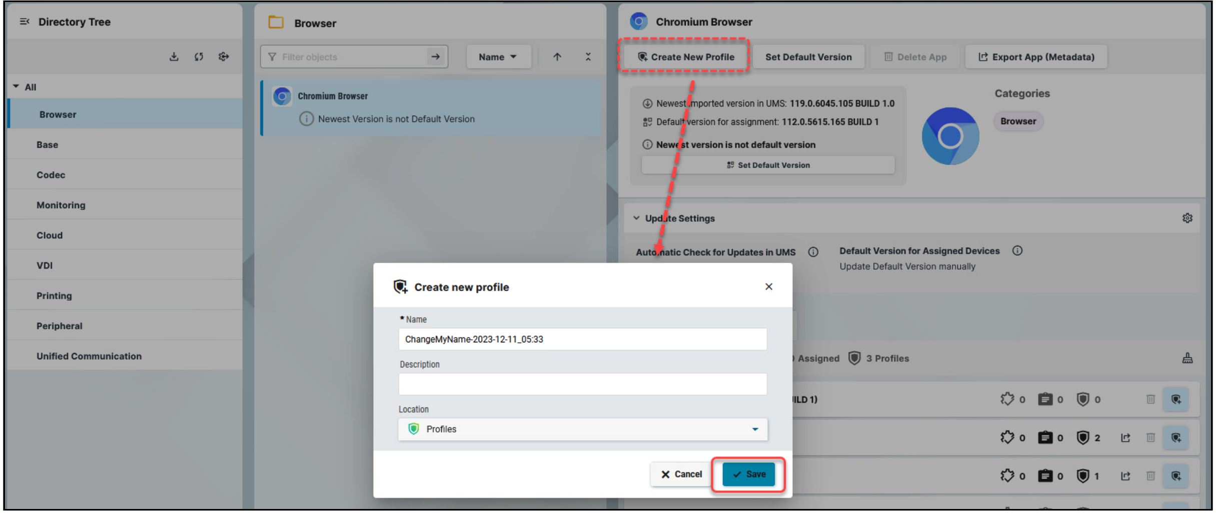

COSMOS Secure Endpoint Platform
APP PORTAL
UMS ADMIN
All Apps › Chromium Browser
UP TO DATE
Chromium Browser
Versions
108.0.5359.94 BUILD 1 RC 1
IMPORT
DESCRIPTION
HISTORY

Chromium

Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all Internet users to experience the web.

> ⚠ If you want to create profiles configuring IGEL OS Base System settings (e.g. corporate design, SSO(see page 195), accesories, etc.) before any of your IGEL OS 12 devices is registered with the UMS, import the IGEL OS Base System app. The latest app version is recommended. Alone for the purpose of profile creation, the subsequent assignment of the IGEL OS Base System app to a device / device directory is NOT necessary.

3. In the UMS Web App, go to **Apps** to view the imported app. To quickly configure the desired settings for this app, select the app and click **Create new profile**. Save the changes.



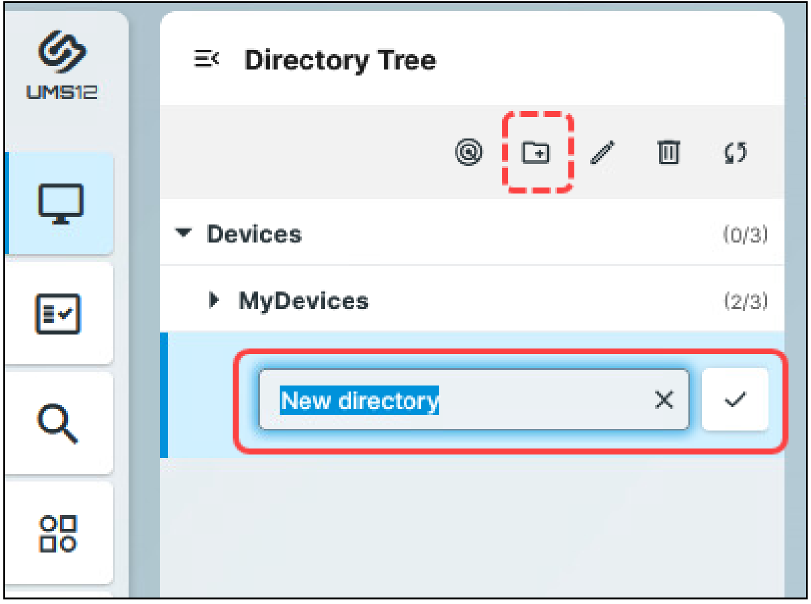
Chromium Browser – Newest Version is not Default Version

Newest imported version in UMS: 119.0.6045.105 BUILD 1.0
Default version for assignment: 112.0.5615.165 BUILD 1
Newest version is not default version

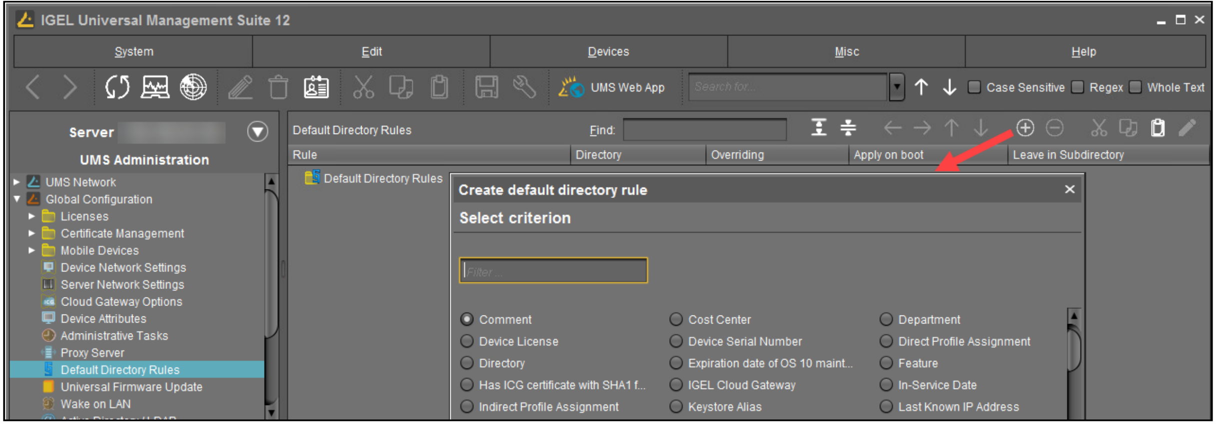
Automatic Check for Updates in UMS
Default Version for Assigned Devices: Update Default Version manually

Create new profile
* Name: ChangeMyName-2023-12-11_05:33
Description:
Location: Profiles

4. In order for your devices to be placed automatically in the specific directory according to certain rules during the onboarding:
1) In the **UMS Web App > Devices**, create a device directory. For more information, see Creating a Directory Structure in the IGEL UMS Web App.



2) In the UMS Console, go to **UMS Administration > Global Configuration > Default Directory Rules** and create the desired rule. For details, see Default Directory Rules.



Create default directory rule

Select criterion

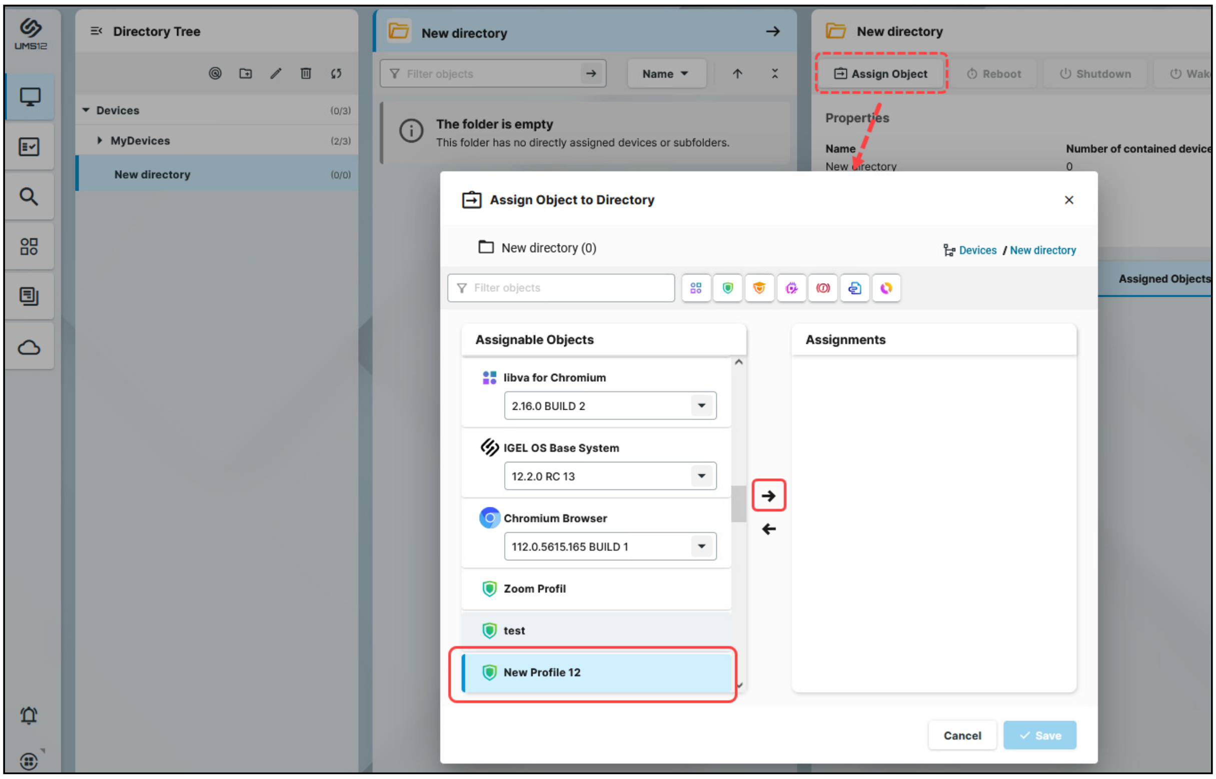
Filter ...

● Comment
○ Cost Center
○ Department
○ Device License
○ Device Serial Number
○ Direct Profile Assignment
○ Directory
○ Expiration date of OS 10 maint...
○ Feature
○ Has ICG certificate with SHA1 f...
○ IGEL Cloud Gateway
○ In-Service Date
○ Indirect Profile Assignment
○ Keystore Alias
○ Last Known IP Address

5. In the **UMS Web App > Devices**, assign the created profile to the device directory. Apply the changes.
   The app will be assigned to the devices via this profile (so-called "implicit app assignment") and will be installed on the devices. Exception: IGEL OS Base System app

   By default, apps / app versions assigned to the device will be automatically activated at the next reboot. If the background app update has been activated, an **Update** command must be sent, instead.

> ⓘ An implicit app assignment is overwritten if you assign an app explicitly, i.e. if you select an app as an object in the **Assign object** dialog.

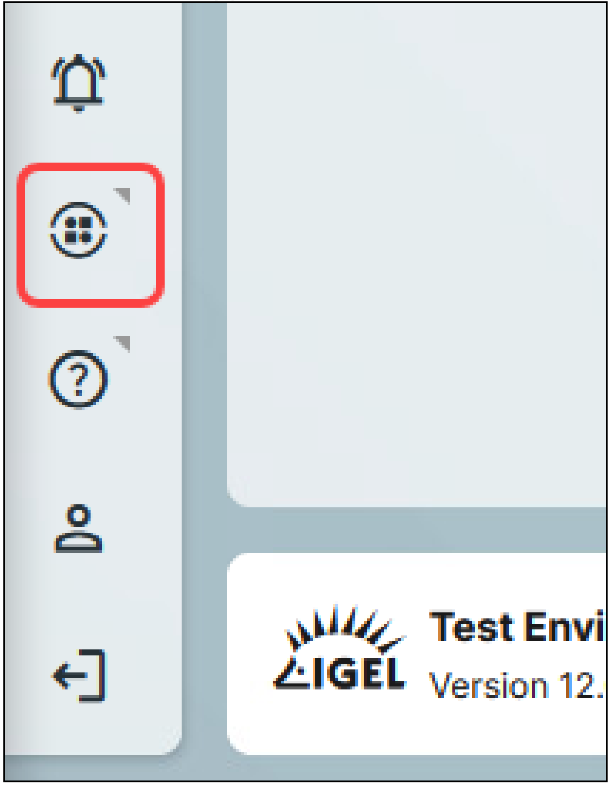


All implicitly assigned apps, i.e. apps assigned to devices via a profile, are displayed directly under the profile that contains them under **Assigned Objects**.
For more information, see How to Assign Apps to IGEL OS Devices via the UMS Web App.

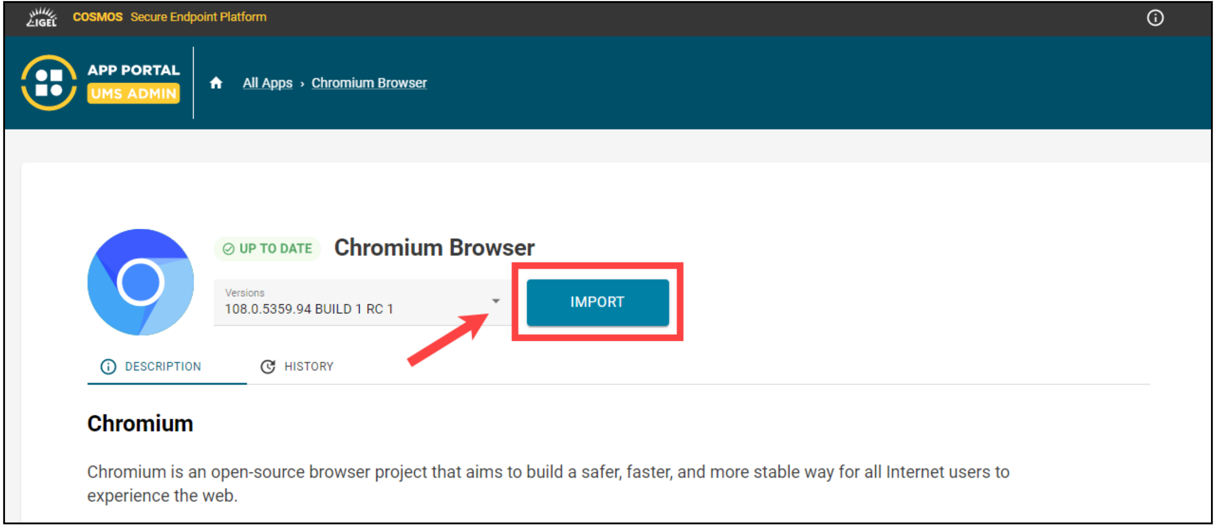
Importing IGEL OS Apps from the IGEL App Portal

To manage IGEL OS 12 devices, you need to import IGEL OS Apps of your choice from the IGEL App Portal:

1. In the UMS Web App, click **App Portal**.



2. Select the app and the required version and click **Import**.


COSMOS Secure Endpoint Platform
APP PORTAL
UMS ADMIN
All Apps › Chromium Browser
UP TO DATE
Chromium Browser
Versions
108.0.5359.94 BUILD 1 RC 1
IMPORT
DESCRIPTION
HISTORY

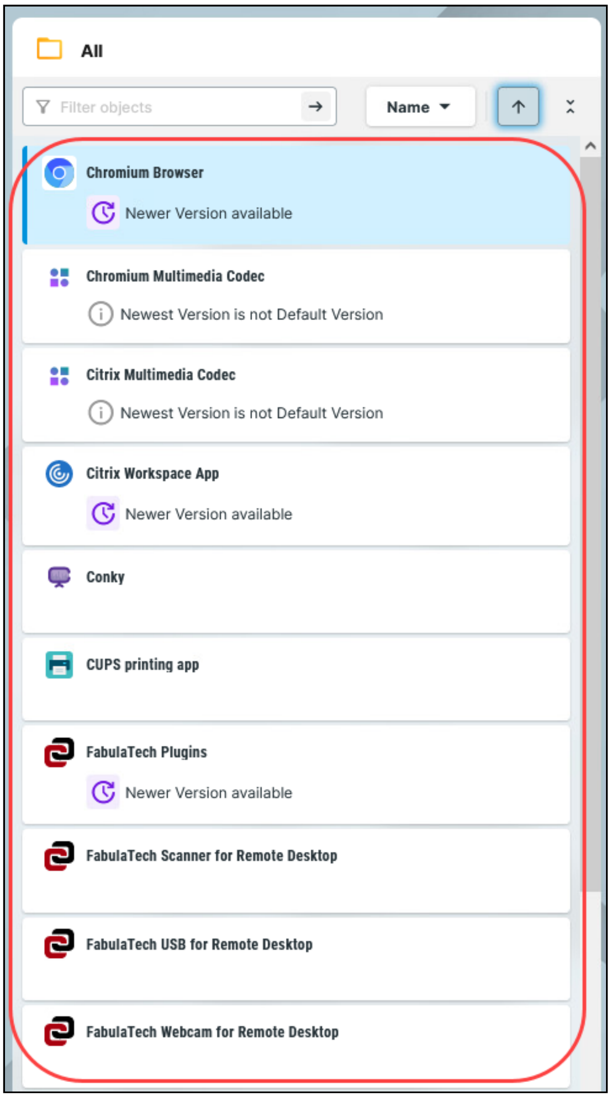
Chromium

Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all Internet users to experience the web.

3. Accept the End User License Agreement (EULA) and wait for the import to be finished.

4. In the UMS Web App, go to **Apps** to view the imported app.

ⓘ **App Management** permission is required to access the **Apps** area. You can set the permission in the **UMS Console > System > Administrator accounts**.



All

Filter objects

Name

Chromium Browser
Newer Version available

Chromium Multimedia Codec
Newest Version is not Default Version

Citrix Multimedia Codec
Newest Version is not Default Version

Citrix Workspace App
Newer Version available

Conky

CUPS printing app

FabulaTech Plugins
Newer Version available

FabulaTech Scanner for Remote Desktop

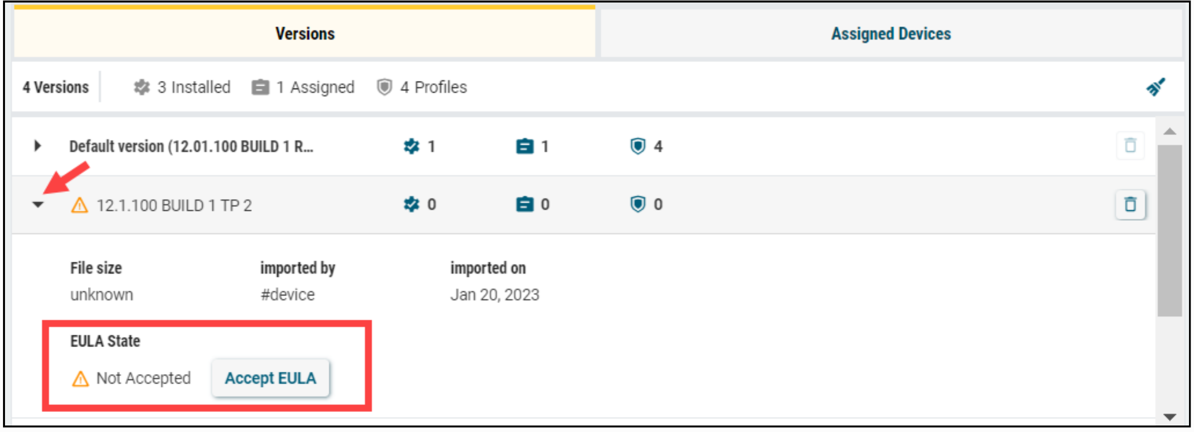
FabulaTech USB for Remote Desktop

FabulaTech Webcam for Remote Desktop

The results of the app import are also displayed under **Messages** 🔔. For more information on **Messages**, see IGEL UMS Web APP User Interface.

ⓘ **Accepting EULA in the UMS**
In the **Apps** section, you may sometimes see app versions marked with an exclamation mark, i.e. with End User License Agreement (EULA) not accepted.

Accepting EULA can be necessary, for example, for automatically registered apps (IGEL OS Base System, all locally installed apps(see page 190)) or if the EULA is changed. If not accepted in the UMS, the EULA can still be accepted by your users locally on the device via the corresponding notification dialog(see page 196).



If you need to delete an app / app version, see How to Delete Apps in the IGEL UMS Web App.

Creating an OS 12 Profile

As soon as you have imported an app, you can create a profile to configure settings for your IGEL OS 12 device. Information on how to create and assign profiles for IGEL OS 11 devices can be found under How to Create and Assign Profiles in the IGEL UMS Web App.

Implicit App Assignment via Profiles
An app is automatically assigned to a device via a profile which configures this app. Exception: IGEL OS Base System app
An app version selected in the profile will be assigned to a device. The best practice is to use the **Default Version**, see Setting a Default Version of an App(see page 120).
An implicit app assignment is overwritten if you assign an app explicitly, i.e. if you select an app as an object in the **Assign object** dialog.
For more information on the app assignment, see Assignment of Apps and Profiles(see page 121).

There are two methods to create a profile:

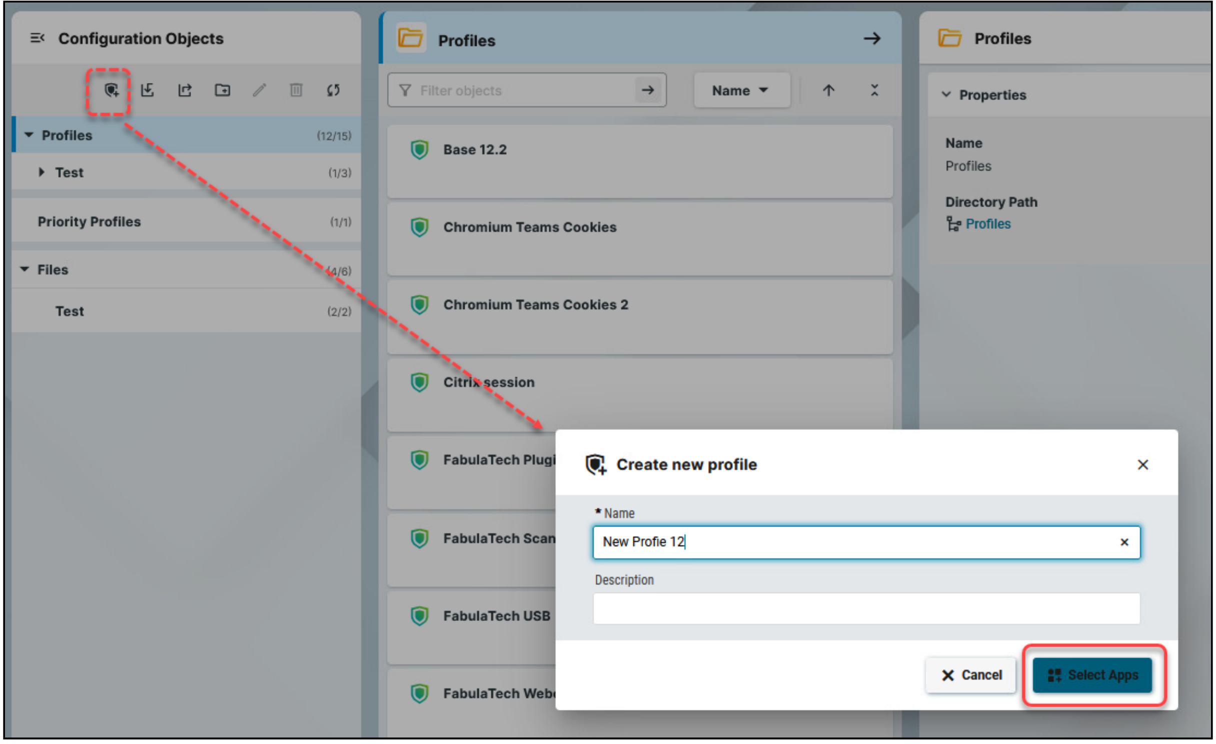
- Via **Configuration > Configuration Tree > Create new profile** (used to configure several apps. A profile configures ALL versions of an app, unless the version is specified.)
- Via **Apps > Create new profile** (used to quickly configure a profile for the selected app.)

Profiles cannot currently be deleted in the UMS Web App.

For apps which have no configurable parameters (e.g. codecs), it is not possible to create a profile.

Option 1: Via Configuration

1. Under **UMS Web App > Configuration**, click **Create new profile** button.



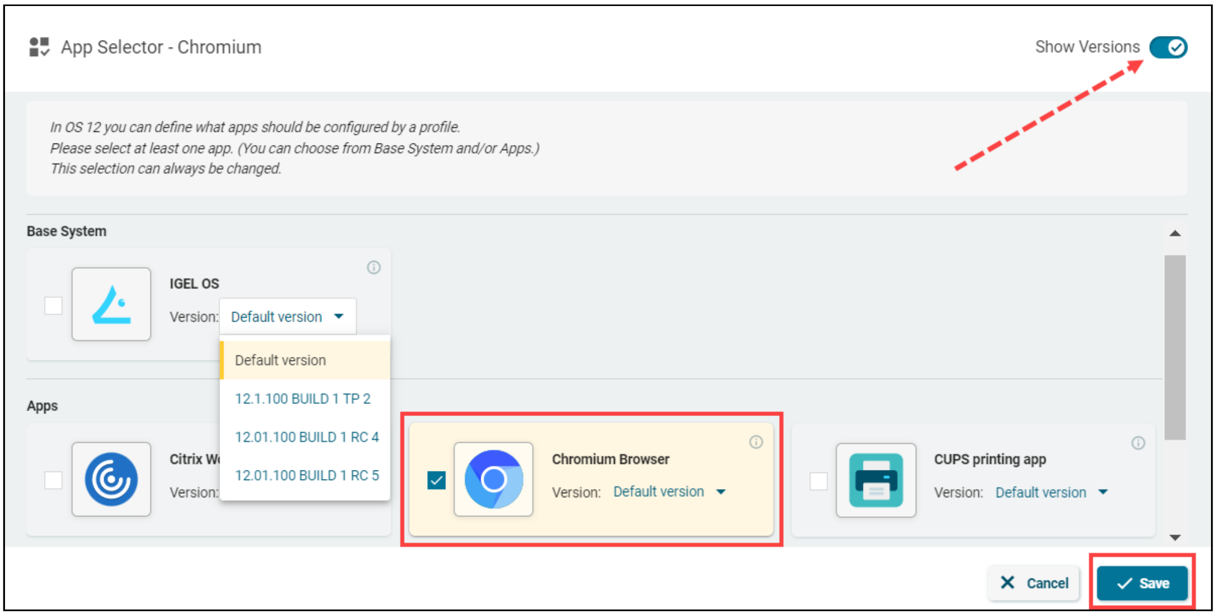
* Name: New Profie 12

2. Select **OS 12** (shown only if there are OS 11 devices registered in the UMS) and enter the **name** of the profile. If desired, add the **description** for the profile.

3. Click **Select Apps**.

4. In the **App Selector**, select the app(s) you want to configure. It is ALWAYS necessary to select at least one app when creating a profile for IGEL OS 12 devices.

   If you want to create profiles configuring IGEL OS Base System settings (e.g. corporate design, SSO(see page 195), accesories, etc.) before any of your IGEL OS 12 devices is registered with the UMS, import the IGEL OS Base System app. The latest app version is recommended. Alone for the purpose of profile creation, the subsequent assignment of the IGEL OS Base System app to a device / device directory is NOT necessary.



App Selector - Chromium

In OS 12 you can define what apps should be configured by a profile.
Please select at least one app. (You can choose from Base System and/or Apps.)
This selection can always be changed.

Base System

IGEL OS — Version: Default version

Apps

Citrix W… — Version:

☑ Chromium Browser — Version: Default version

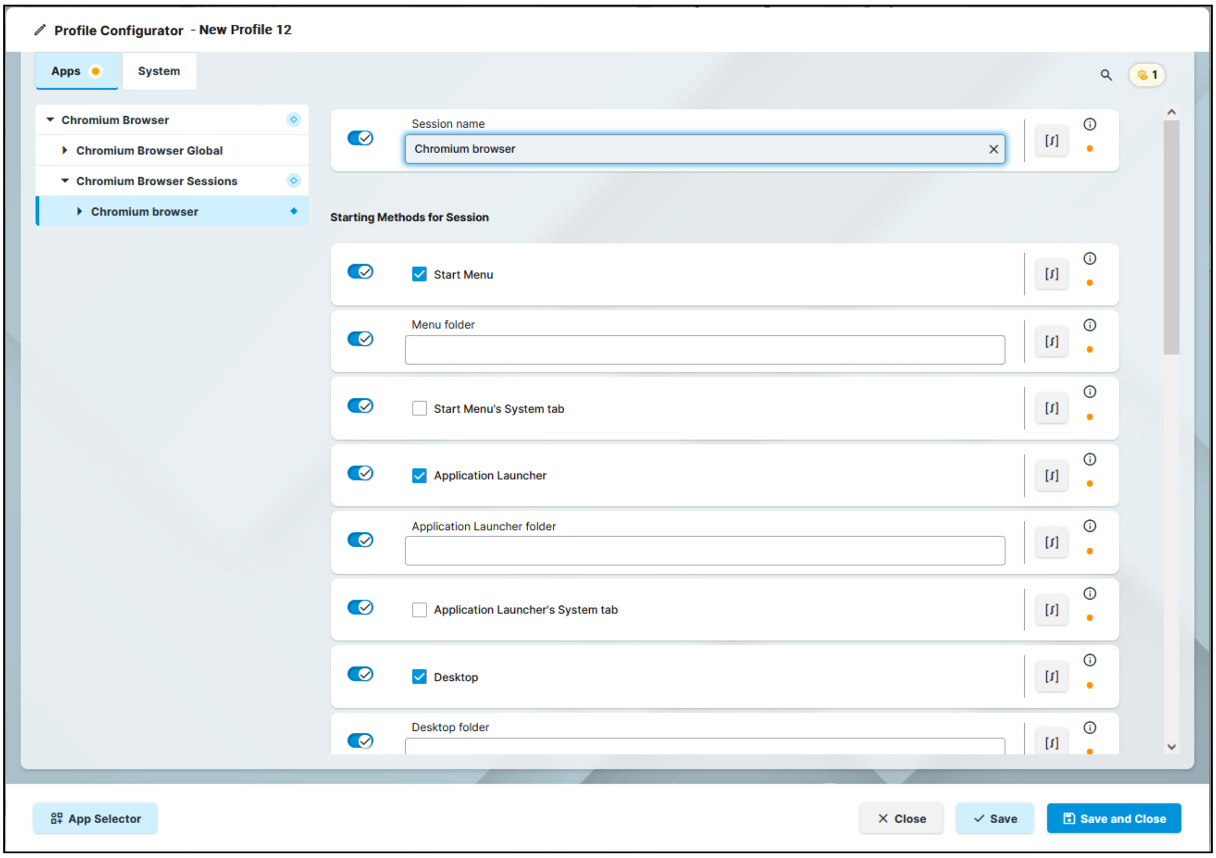
CUPS printing app — Version: Default version

5. If you want to configure a profile for a specific app version, activate **Show Versions** and select the required version.

6. Click **Save**.
   The profile will be saved and listed under **Configuration > Profiles**, even if you will not configure any settings in the next step.

7. Configure the desired settings.
   The configuration dialog shows only those settings that can be configured for the selected app(s).
   If you want to change the scope of the profile (i.e. redefine which apps should be configured by the profile), click **App Selector**.

○	The parameter is inactive and will not be configured by the profile. **IMPORTANT**: When you deactivate the parameter, the value will be automatically set back to the default value.
✓	The parameter is active and the set value will be configured by the profile.



Profile Configurator - New Profile 12

Session name: Chromium browser

Starting Methods for Session

- ☑ Start Menu
- Menu folder:
- ☐ Start Menu's System tab
- ☑ Application Launcher
- Application Launcher folder:
- ☐ Application Launcher's System tab
- ☑ Desktop
- Desktop folder:

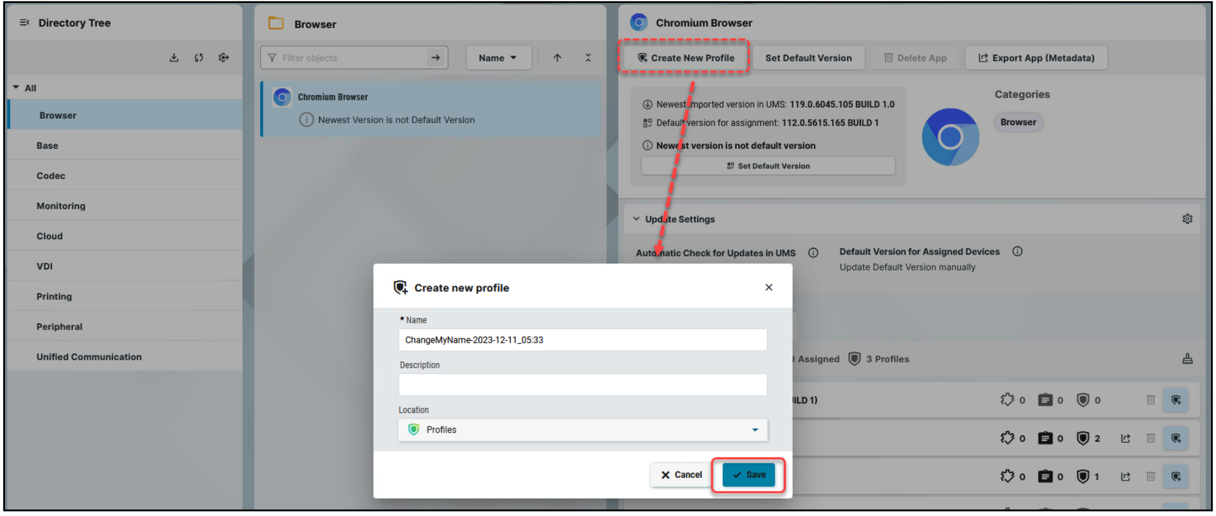
8. Save the changes.

9. Assign the profile to the required device / device directory. See Assignment of Apps and Profiles(see page 121).

Option 2: Via Apps

To quickly create a profile for an imported app, proceed as follows:

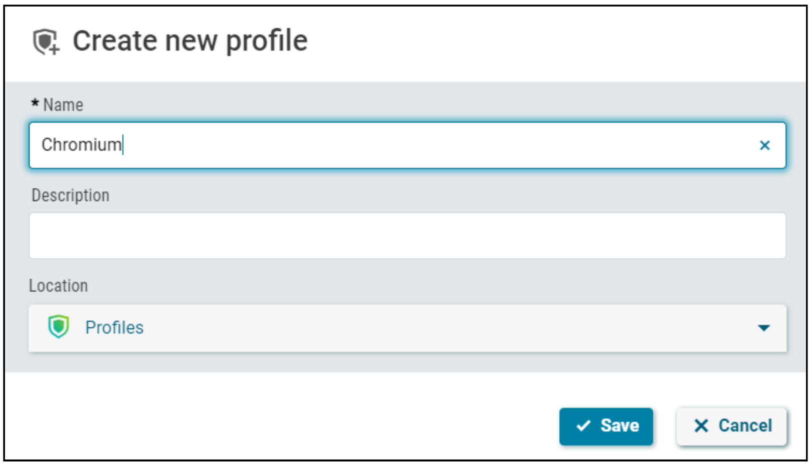
1. Under **UMS Web App > Apps**, select the required app and click **Create new profile**.



Newest imported version in UMS: 119.0.6045.105 BUILD 1.0
Default version for assignment: 112.0.5615.165 BUILD 1
Newest version is not default version

* Name: ChangeMyName-2023-12-11_05:33
Description:
Location: Profiles

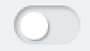
2. Enter the **name** of the profile and specify the desired directory for storing the profile under **Location**. If desired, add the **description** for the profile.



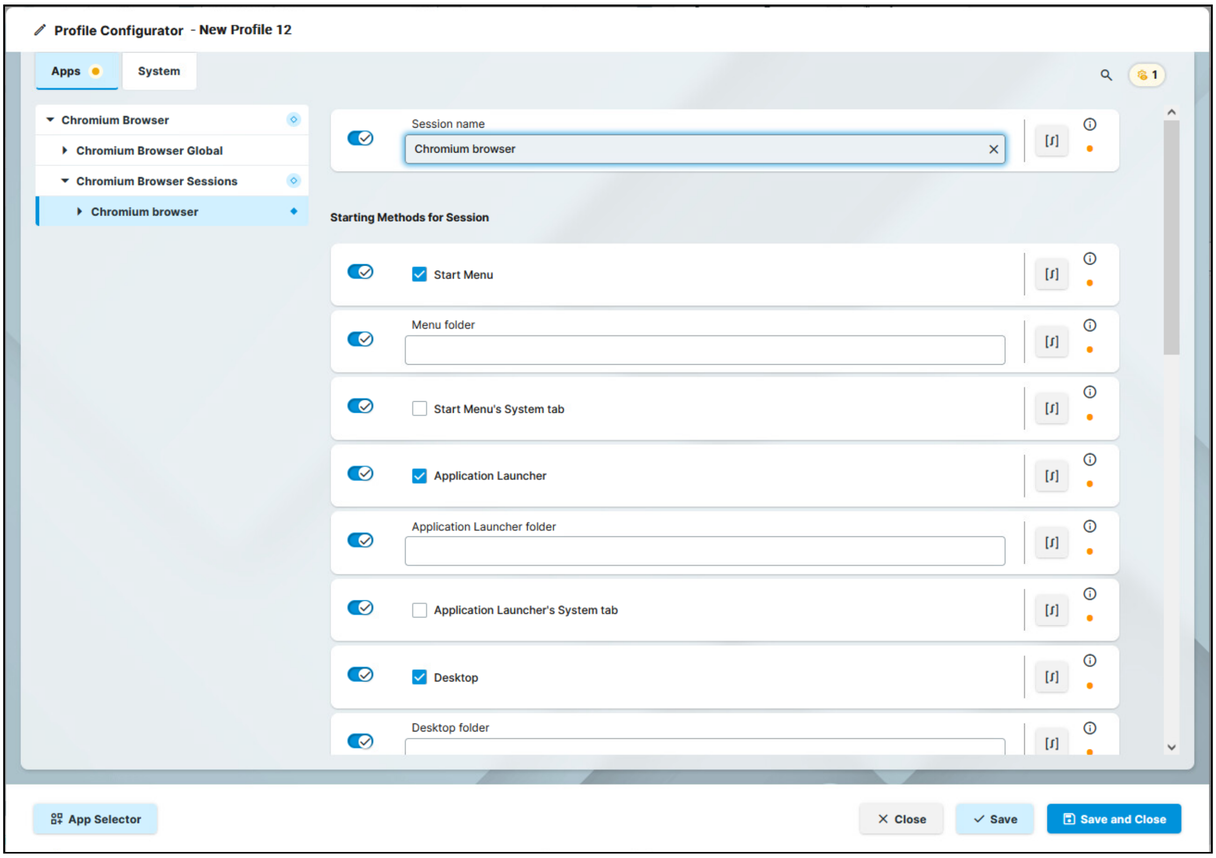
* Name: Chromium
Description:
Location: Profiles

3. Click **Save**.
The profile will be saved and listed under **Configuration > Profiles**, even if you will not configure any settings in the next step.

4. Configure the desired settings.
The configuration dialog shows only those settings that can be configured for the selected app. If you want to change the scope of the profile (i.e. redefine which apps should be configured by the profile), click **App Selector** .

	The parameter is inactive and will not be configured by the profile. **IMPORTANT**: When you deactivate the parameter, the value will be automatically set back to the default value.

✓	The parameter is active and the set value will be configured by the profile.



Session name: Chromium browser

Starting Methods for Session

☑ Start Menu

Menu folder:

□ Start Menu's System tab

☑ Application Launcher

Application Launcher folder:

□ Application Launcher's System tab

☑ Desktop

Desktop folder:

5. Save the changes.

6. Assign the profile to the required device / device directory. See Assignment of Apps and Profiles(see page 121).

Setting a Default Version of an App

If you have imported several versions of an app, you can define which version will be a **Default Version**.

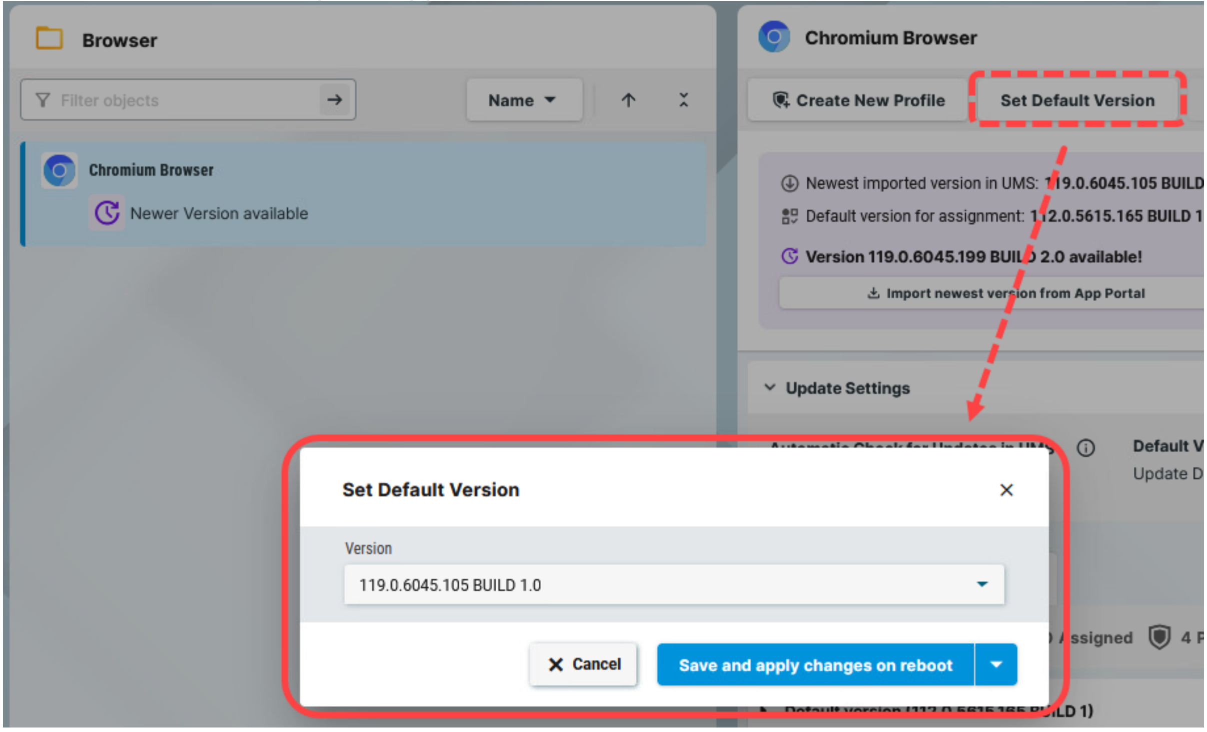
Default Version is a version that will be assigned to a device / device directory if no version is specified during the assignment of an app or during the creation of a profile configuring this app.

> ⓘ A **Default Version** is set globally: If changed, all assignments where no version was explicitly specified will change with it.

The best practice is to use the **Default Version** during the app assignment and profile creation.
The use of a specific version during the app assignment and profile creation is recommended for test purposes, e.g. to test app updates. After successful testing, you can change your **Default Version**.

To set a Default Version:

1. Under **Apps**, select the required app and click **Set Default Version**.



Newest imported version in UMS: 119.0.6045.105 BUILD

Default version for assignment: 112.0.5615.165 BUILD 1

Version 119.0.6045.199 BUILD 2.0 available!

Set Default Version

Version

119.0.6045.105 BUILD 1.0

2. Select the desired Default Version and save the changes.

Assignment of Apps and Profiles

In the UMS, there are two methods to assign an app to your devices:

- Implicit app assignment via profiles: An app is automatically assigned to a device via a profile which configures this app. Exception: IGEL OS Base System app
  The app version that will be installed on the device via the implicit assignment if several profiles configure this app (but in different versions) is defined by the priority rules for profiles, see Prioritization of Profiles in the IGEL UMS and Summary - Prioritization of IGEL UMS Profiles.
- Explicit app assignment via the **Assign object** dialog

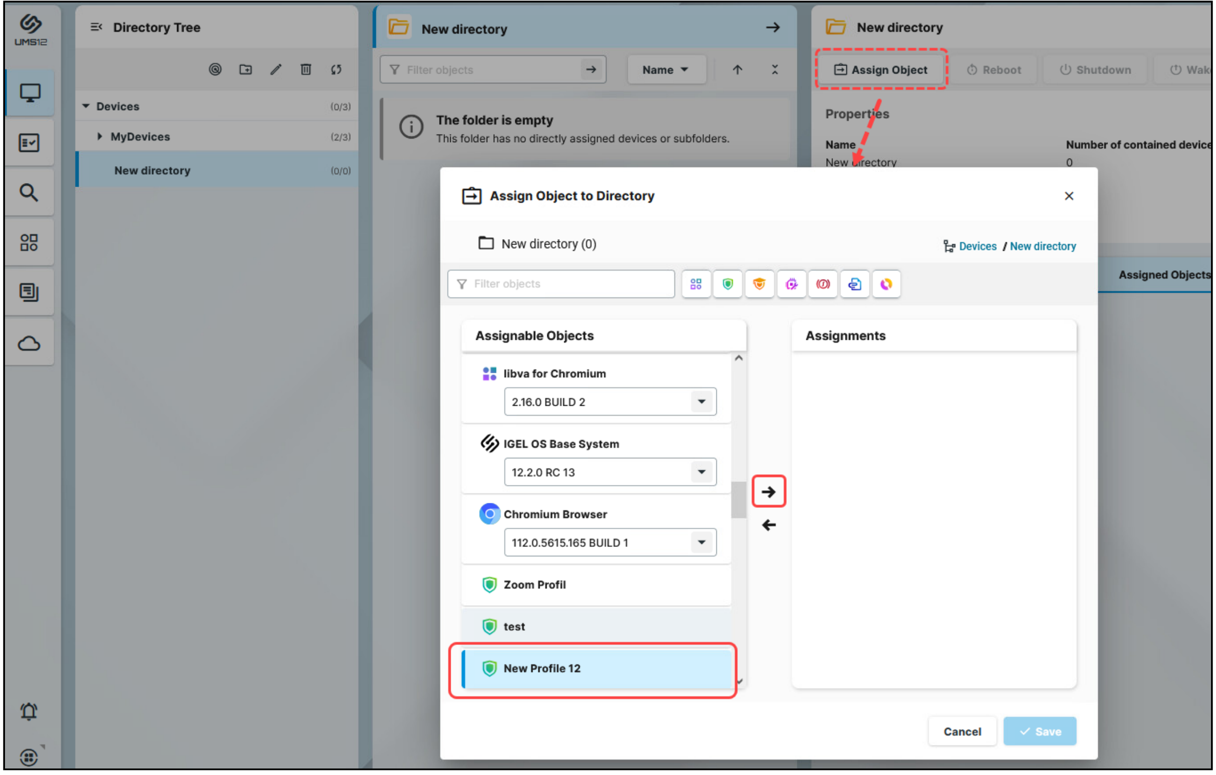
An explicitly assigned app ALWAYS overwrites an implicitly assigned app.

ⓘ If you need to detach an app from the device, see Detaching Apps from the IGEL OS Device.

Implicit App Assignment via Profiles

To assign profiles to a device / device directory, proceed as follows:

1. Under **UMS Web App > Devices**, select a device or device directory and click **Assign object**.

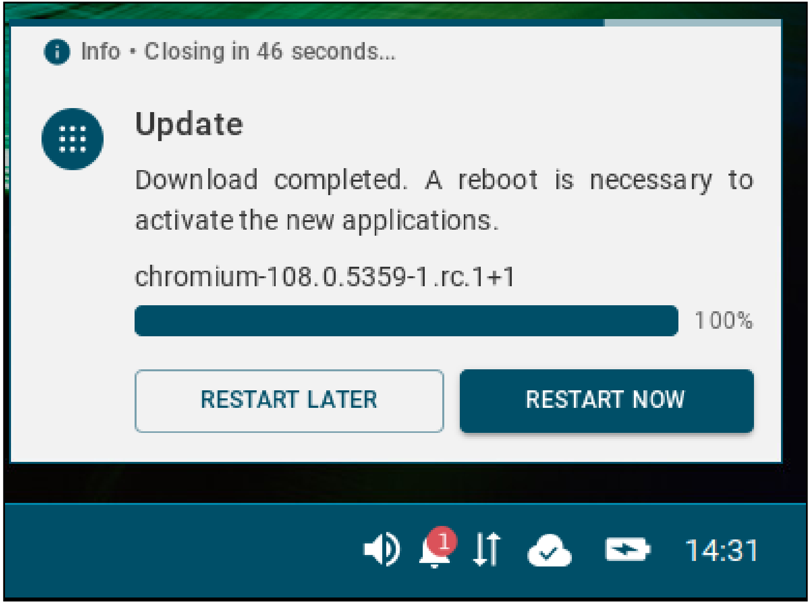


2. Select the profile you want to assign to the device / device directory and use the arrow button or drag & drop.

3. Save the changes.

4. Decide when the changes should become effective.
An app assigned via the profile will be downloaded by the device.
By default, apps / app versions assigned to the device will be automatically activated at the next reboot. The user will receive a corresponding notification. If the background app update has been

activated, an **Update** command must be sent, instead.



Info • Closing in 46 seconds...

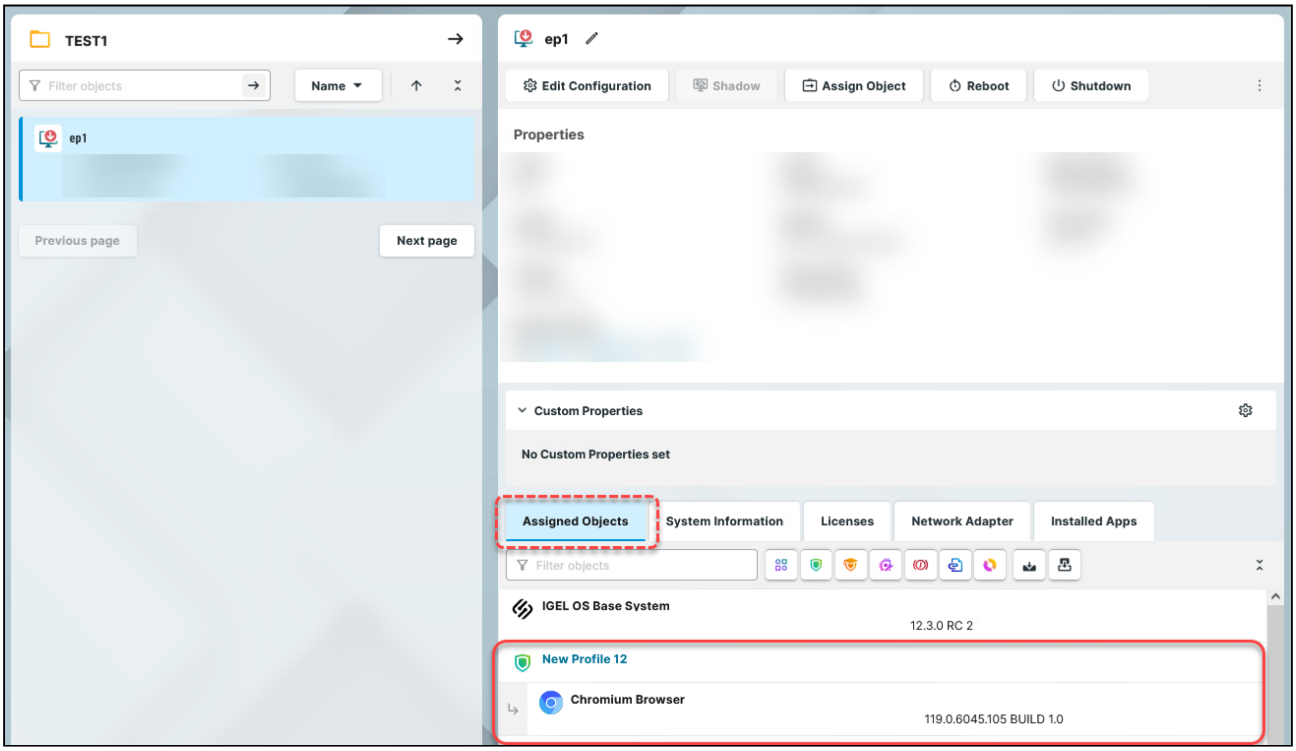
Update

Download completed. A reboot is necessary to activate the new applications.

chromium-108.0.5359-1.rc.1+1

100%

The assigned profile and the app assigned to the device via this profile are displayed under **Devices > Assigned Objects**.



No Custom Properties set

IGEL OS Base System 12.3.0 RC 2

New Profile 12

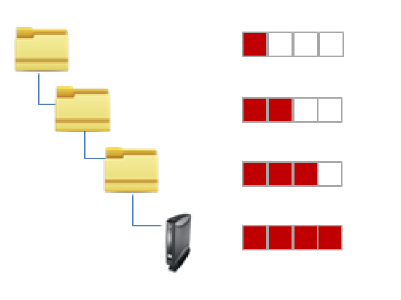
Chromium Browser 119.0.6045.105 BUILD 1.0

To check the installed apps, go to **Devices > [name of the device] > Installed Apps**; see Checking Installed Apps via the IGEL UMS Web App.

Explicit App Assignment

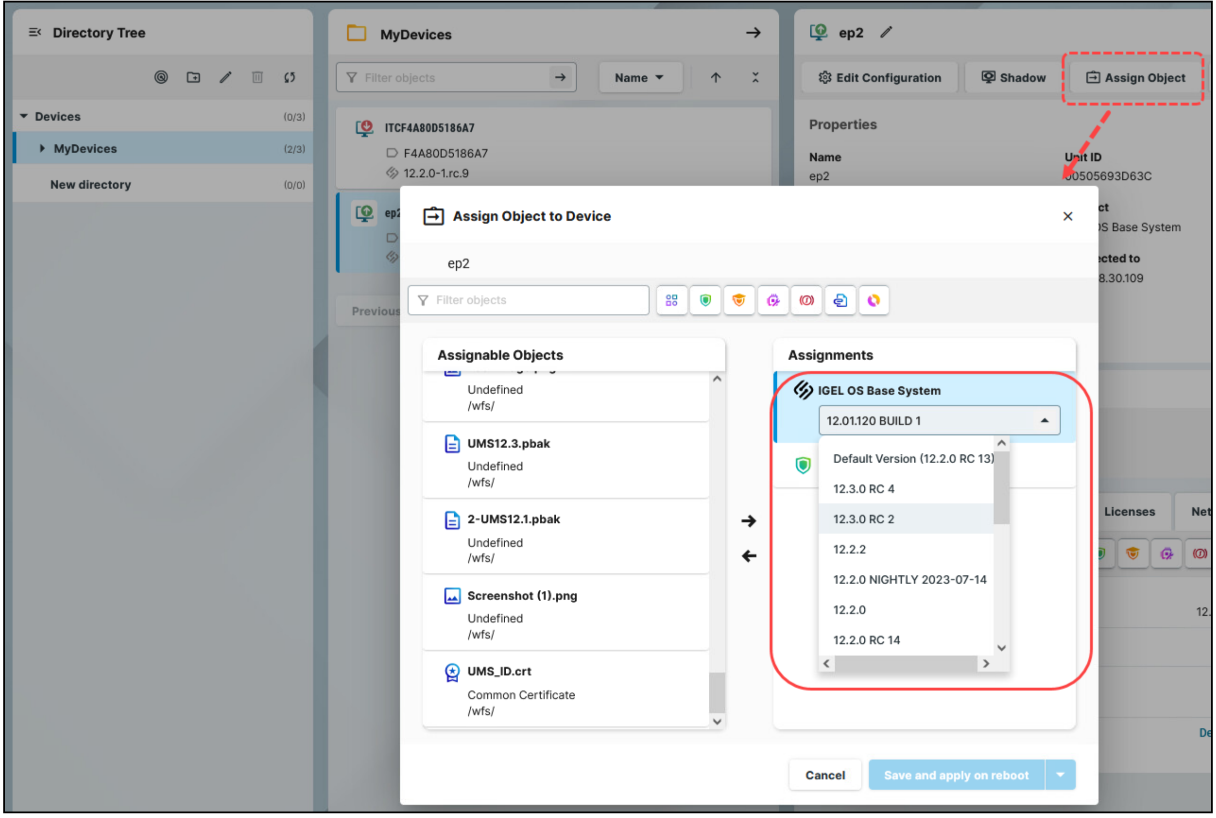
For the assignment of the IGEL OS Base System app, the permission **Assign Base System / Firmware Update** is required. You can set the permission in the UMS Console via **[context menu of a device / device directory] > Access control**.

If various app versions have been assigned to a device (e.g. via direct and indirect assignment), the version which is closer to the device in the directory tree will have the priority and will be installed on the device.



To assign apps to a device / device directory, proceed as follows:

1. Under **UMS Web App > Devices**, select a device or device directory and click **Assign object**.



2. Select the required app (and its specific version, if necessary).

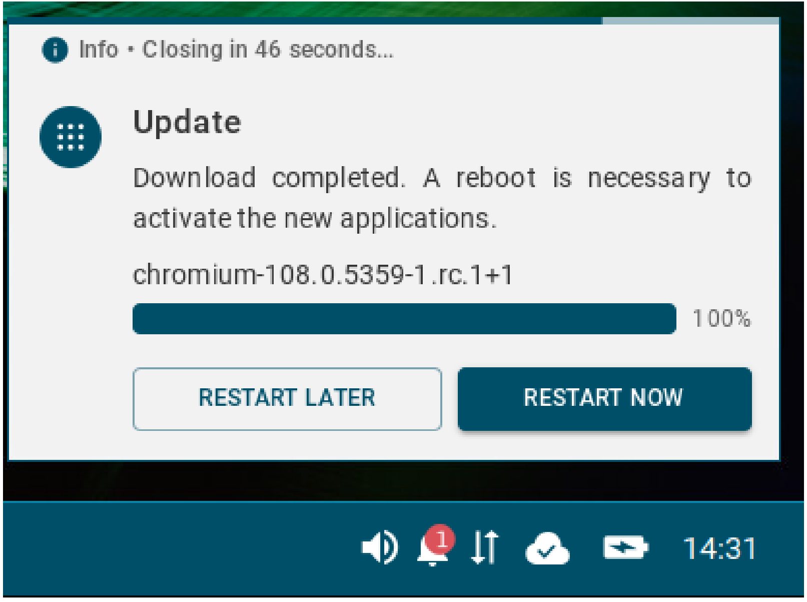
> ⓘ If no version is specified for an app during the assignment, the Default Version(see page 120) will be used. It is possible to select the version for an app in the **Assign Object** dialog either under **Assignable Objects** or under **Assignments**.

3. Save the changes.

4. Decide when the changes should become effective.

   The app will be downloaded by the device.
   By default, apps / app versions assigned to the device will be automatically activated at the next reboot. The user will receive a corresponding notification. If the background app update has been

activated, an **Update** command must be sent, instead.



Info • Closing in 46 seconds...

Update

Download completed. A reboot is necessary to activate the new applications.

chromium-108.0.5359-1.rc.1+1

100%

The assigned app is displayed in the UMS Web App under **Devices > Assigned Objects**.

To check the installed apps, go to **Devices > [name of the device] > Installed Apps**; see Checking Installed Apps via the IGEL UMS Web App.

You can also observe the desktop of a device via shadowing with VNC, see Remote Access to Devices via Shadowing in the IGEL UMS Web App.

IGEL UMS 12: App Update

The update procedure for the IGEL OS base system does not generally differ from the procedure for other apps. The update and downgrade procedures are also the same.

The update procedure includes the following steps:

1. Checking if the default global update settings under **UMS Web App > Apps > Settings** suit your needs. See Configuring Global Settings for the Update of IGEL OS Apps.
2. Checking if the default update settings under **UMS Web App > Apps > [name of the app] > Update Settings** suit your needs. See Configuring Update Settings for Individual IGEL OS Apps.
3. Checking if the default settings in **IGEL Setup > System > Update** suit your needs. Here, you can configure, for example, the timeout for an automatic reboot after the app installation, forbid the user to postpone the reboot, activate the background app update or set a bandwidth limit that will be used during the app update (see How to Configure the Background App Update in the IGEL UMS Web App).
4. Testing a new app version.
5. Updating an app on all the required devices. See How to Trigger the App Update in the IGEL UMS. See also the instructions below.

Preconditions

- You use the Default Version(see page 120) during the app assignment and profile creation (best practice).

> ⚠ Never change the **Default Version** before you have tested the update. A **Default Version** is set globally: If changed, all assignments where no version was explicitly specified will change with it.

- You have checked and, if necessary, changed the default global update settings.
- You have checked and, if necessary, changed the default update settings for individual apps. **Apps > [name of the app] > Update Settings > Default Version for Assigned Devices** has been set to **Update Default Version manually** (default).
- You have checked the default settings in **IGEL Setup > System > Update** and, if necessary, created a profile modifying these settings according to your needs and assigned it to the devices.
- All devices have a valid license. See Licensing(see page 151).
- Devices to be updated are online.
- All devices are connected to a regular LAN or WLAN (not OpenVPN, OpenConnect, genucard, NCP VPN, or mobile broadband).
- All devices are in a safe environment where the update process cannot be disrupted, e.g. by powering off the devices.

Update of the IGEL OS Base System

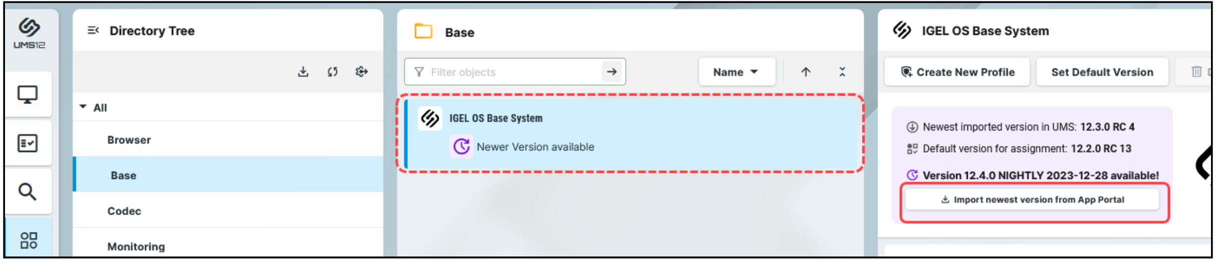
The procedure described below applies to the update of the IGEL OS Base System app.

> ⓘ This procedure is also relevant for any explicitly assigned app(see page 121).

Preparing the Update

For the assignment of the IGEL OS Base System app, the permission **Assign Base System / Firmware Update** is required. You can set the permission in the UMS Console via **[context menu of a device / device directory] > Access control**.

1. In the **UMS Web App > Apps**, select **IGEL OS Base System**.



Newest imported version in UMS: 12.3.0 RC 4

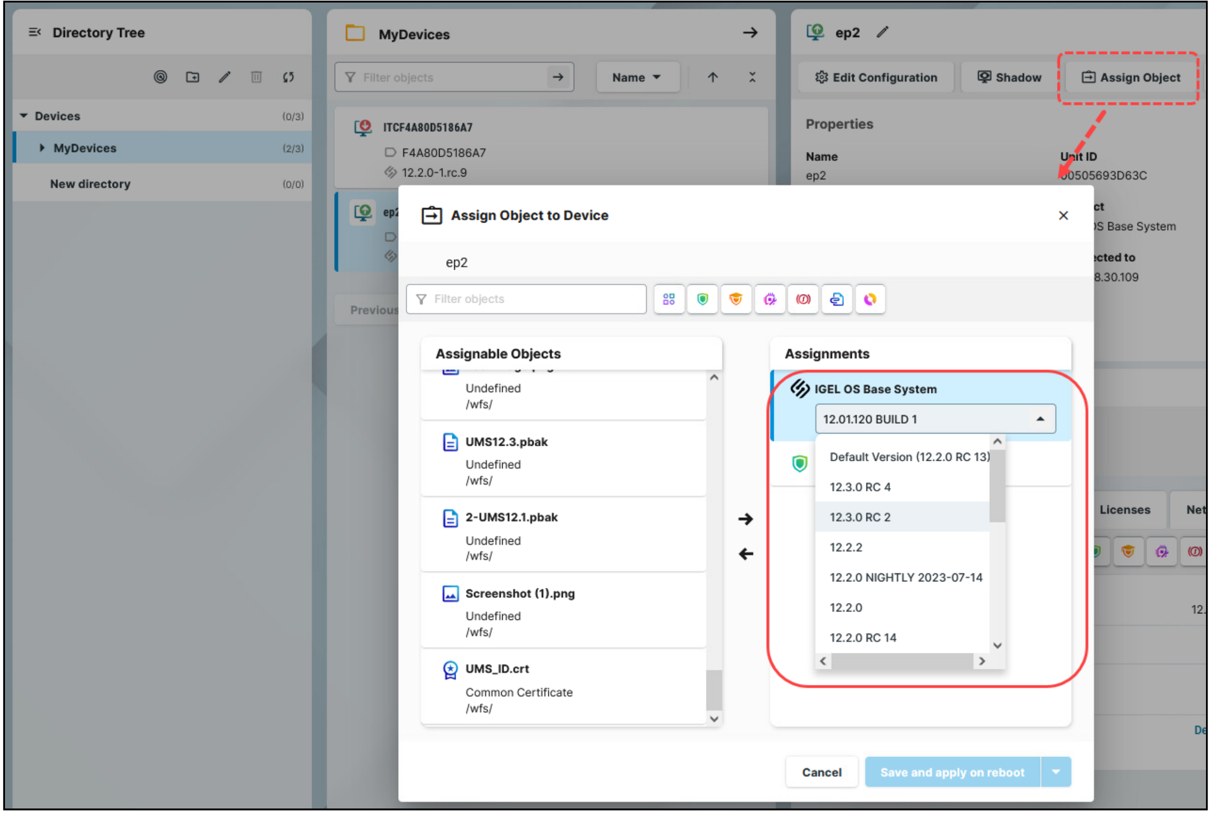
Default version for assignment: 12.2.0 RC 13

Version 12.4.0 NIGHTLY 2023-12-28 available!

2. If you have not activated the automatic import of updates under **Update Settings > Automatic check for updates in UMS**, click **Import newest version from App Portal** or go to the **App Portal** to import the required app version manually.

Testing the Update

1. In the **UMS Web App > Devices**, select your test device(s) and click **Assign Object**.



2. In the **Assign Object** dialog, select **IGEL OS Base System** and the required version. It is possible to select the version for an app either under **Assignable Objects** or under **Assignments**.

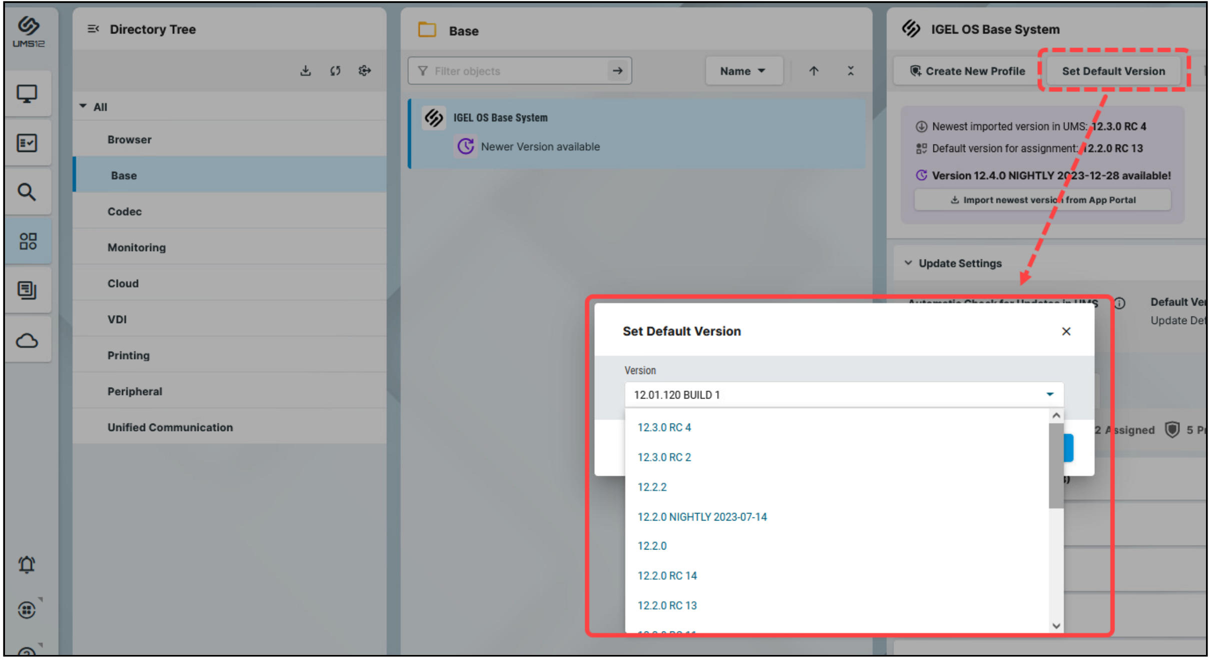
3. Decide when the changes should become effective, and save accordingly.
   The app version will be downloaded by the device.
   By default, apps / app versions assigned to the device will be automatically activated at the next reboot. If you have configured the background app update, an **Update** command must be sent, instead; see How to Configure the Background App Update in the IGEL UMS Web App.

4. Under **Devices > [name of the device] > Installed Apps**, check the app, its version and state; see Checking Installed Apps via the IGEL UMS Web App.

When the update test has been successful, you can update IGEL OS Base System on all the required devices.

Triggering the Mass Update

1. In the **UMS Web App > Apps**, select **IGEL OS Base System** and click **Set Default Version**.



Newest imported version in UMS: 12.3.0 RC 4

Default version for assignment: 12.2.0 RC 13

Version 12.4.0 NIGHTLY 2023-12-28 available!

Version: 12.01.120 BUILD 1

12.3.0 RC 4
12.3.0 RC 2
12.2.2
12.2.0 NIGHTLY 2023-07-14
12.2.0
12.2.0 RC 14
12.2.0 RC 13

2. Select the required version.

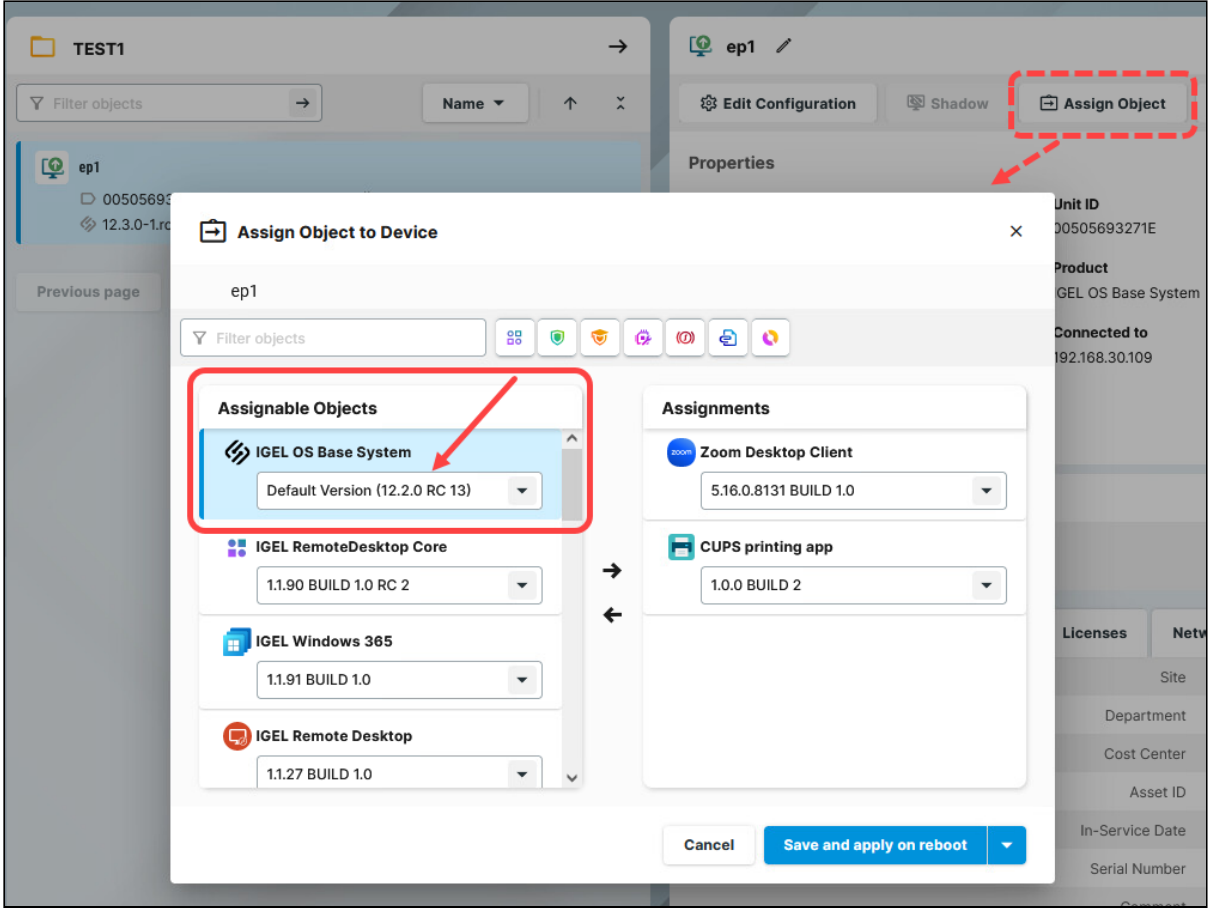
3. Select when the changes should take effect and save accordingly.

4. If the **IGEL OS Base System** app has not yet been assigned to the devices: Go to **UMS Web App > Devices > [name of the device / device directory]** and click **Assign object** to assign the app.

5. Verify that **Default Version** is selected in the version picker.

6. Assign the app.

7. Decide when the changes should become effective and save accordingly.



> If the changes should take effect on reboot, you can create a scheduled job for reboot and/or wakeup and assign it to the devices / device directory or a view (created in the **UMS Console > Views > [context menu] > New View > Installed Apps** criterion). For more information on jobs, see Jobs.

The new version will be downloaded by the devices.

By default, apps / app versions assigned to the device will be automatically activated at the next reboot. By default, the reboot is performed automatically after the timeout of 60 seconds after the app download if the user does not postpone the device restart, see IGEL OS Notification Center(see page 196).
If you have configured the background app update, an **Update** command must be sent instead of the reboot for the app activation; see How to Configure the Background App Update in the IGEL UMS Web App.

> ⓘ If there is not enough space for storing the new base system during the update of IGEL OS, the multistage update will be triggered. See Multistage Update of IGEL OS Base System.

8. To verify that all devices have been updated successfully: Under **Devices > [name of the device] > Installed Apps**, check the app, its version and state; or create a view in the **UMS Console > Views** using the **Installed Apps** criterion. See Checking Installed Apps via the IGEL UMS Web App.

Update of the Implicitly Assigned IGEL OS Apps

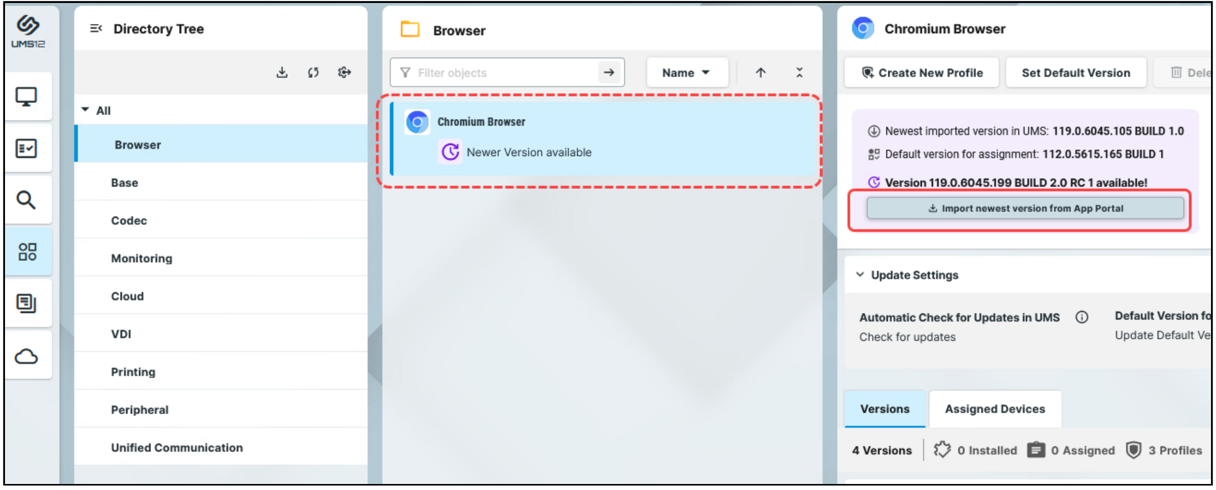
If you have decided not to use the explicit app assignment, and the apps are thus assigned to your devices implicitly, i.e. via profiles configuring these apps, you can use the following procedure for the app update. This procedure applies to the update of any app that has been assigned to devices implicitly; it is NOT applicable to the IGEL OS Base System since it can be assigned only explicitly.

For more information on the implicit app assignment, see Assignment of Apps and Profiles(see page 121).

Preparing the Update

1. In the **UMS Web App > Apps**, select the required app, e.g. Chromium.

2. If you have not activated the automatic import of updates under **Update Settings > Automatic check for updates in UMS**, click **Import newest version from App Portal** or click **App Portal** to import the required app version manually.



Newest imported version in UMS: **119.0.6045.105 BUILD 1.0**

Default version for assignment: **112.0.5615.165 BUILD 1**

Version 119.0.6045.199 BUILD 2.0 RC 1 available!

Automatic Check for Updates in UMS
Check for updates

Default Version fo
Update Default Ve

4 Versions | 0 Installed 0 Assigned 3 Profiles

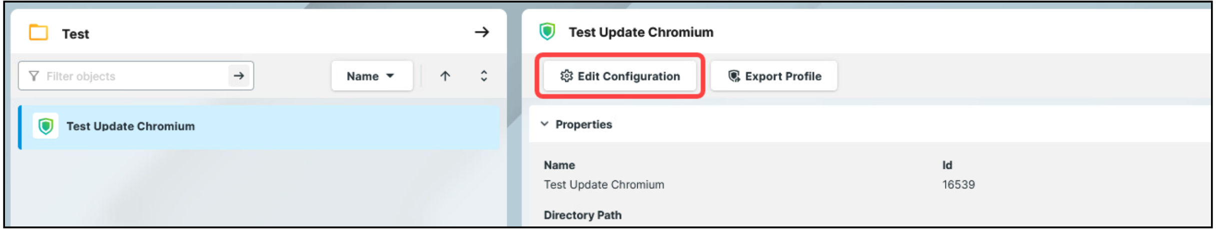
Testing the Update

1. Go to **UMS Web App > Configuration** and create a test profile with the same settings and app(s) as the "productive" profile, e.g. `Test Update Chromium`. Leave the **Default Version** for the app(s) in the **App Selector** (as it was done for the productive devices). For how to create profiles, see Creating an OS 12 Profile(see page 115).

Currently, copying of OS 12 profiles is not possible.

2. In the **UMS Web App > Devices**, select your test device(s) and assign the created profile `Test Update Chromium`. For more information on the assignment, see Implicit App Assignment via Profiles(see page 121).
   As soon as your test devices have the app(s) of the same version as on the productive devices, proceed as follows.

3. In the **UMS Web App > Configuration**, select the test profile via which apps are assigned to your test devices, in our case `Test Update Chromium`, and click **Edit Configuration**.

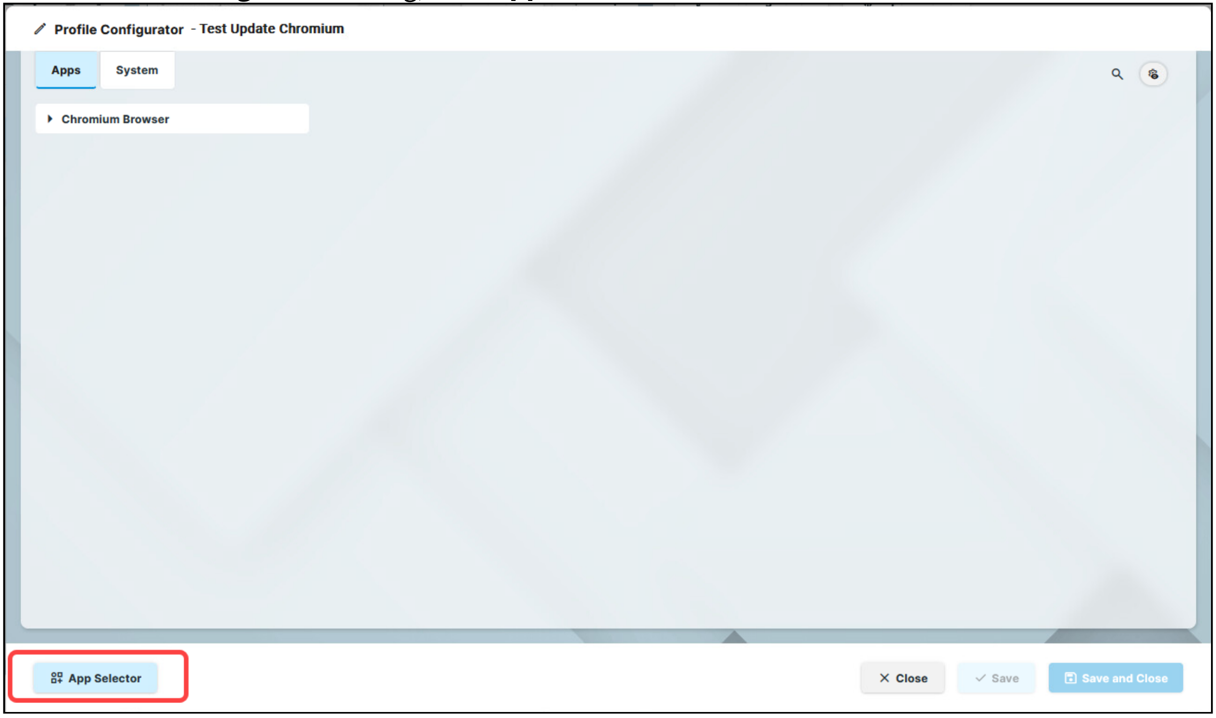


Name
Test Update Chromium

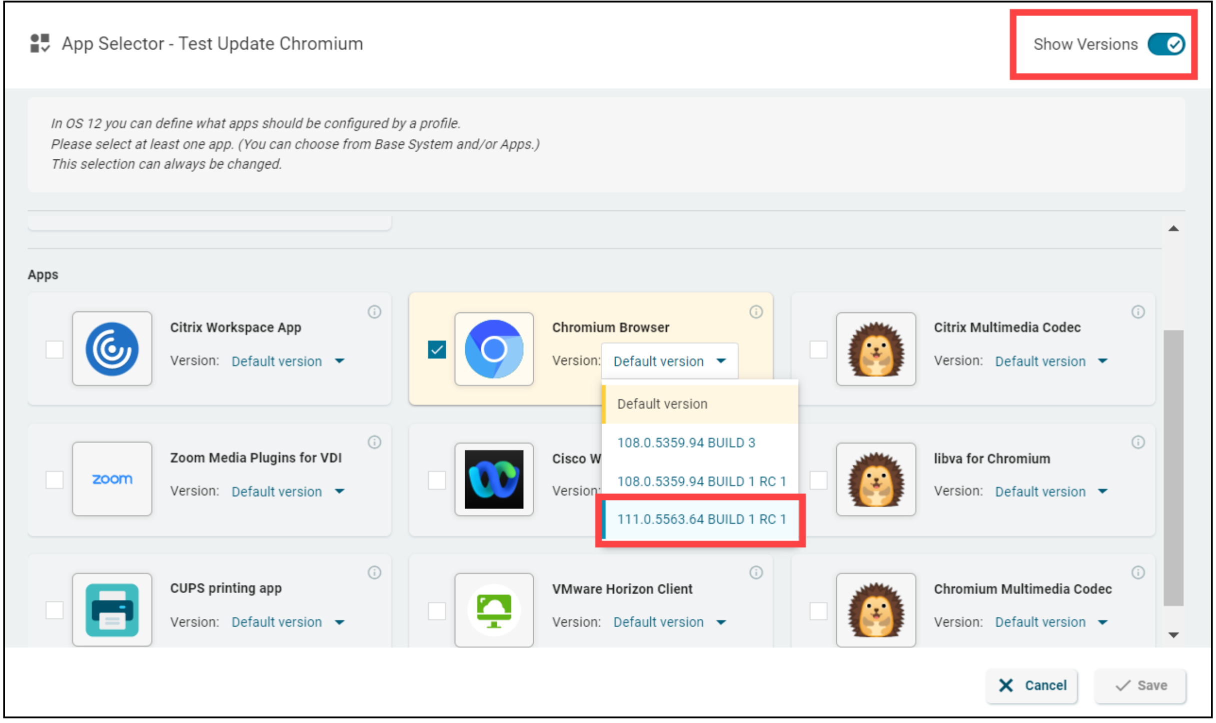
Id
16539

Directory Path

4. In the **Profile Configurator** dialog, click **App Selector**.



5. Click **Show Versions** and select the app version you want to update to.



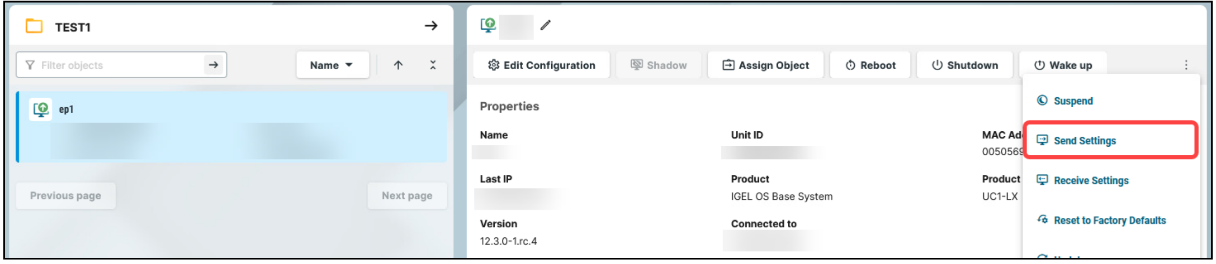
App Selector - Test Update Chromium

Show Versions

In OS 12 you can define what apps should be configured by a profile.
Please select at least one app. (You can choose from Base System and/or Apps.)
This selection can always be changed.

6. Save the changes.

7. Under **Devices**, select the test devices and click **Send settings**.



Properties

Name

Unit ID

MAC Ad 0050569

Last IP

Product IGEL OS Base System

Product UC1-LX

Version 12.3.0-1.rc.4

Connected to

The new app version will be downloaded by the device.
By default, apps / app versions assigned to the device will be automatically activated at the next reboot. If you have configured the background app update, an **Update** command must be sent, instead; see How to Configure the Background App Update in the IGEL UMS Web App.

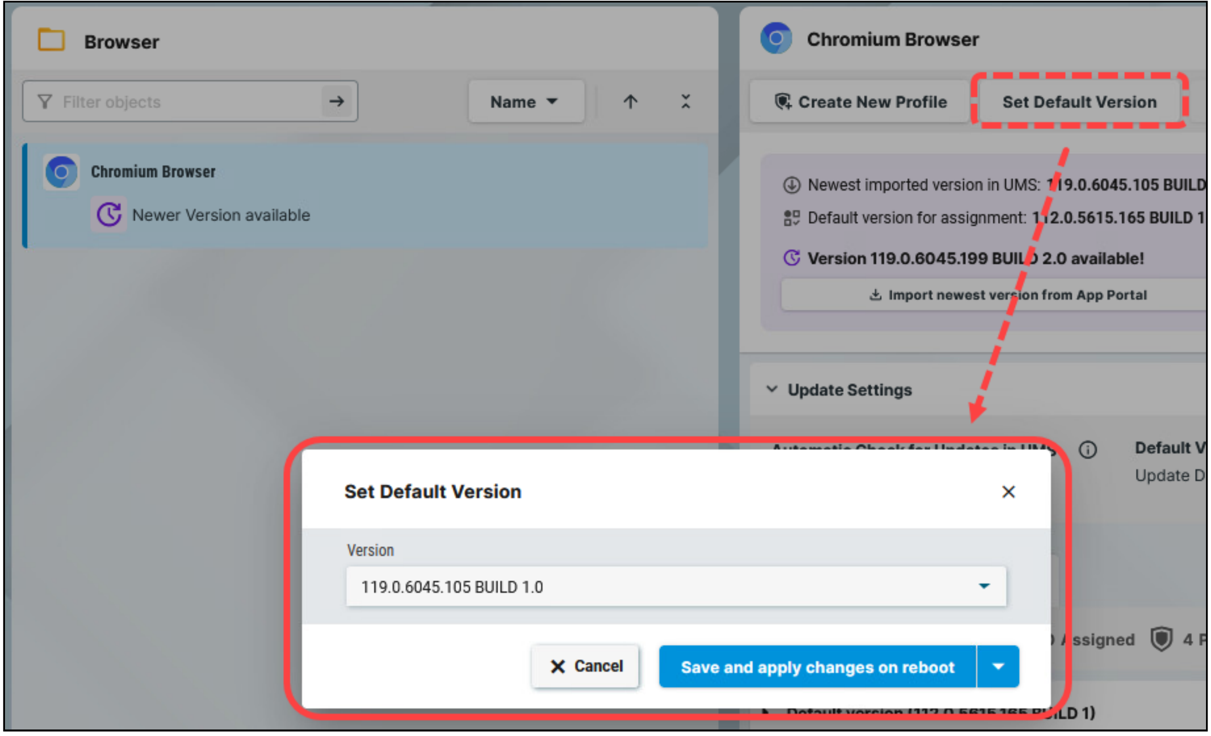
8. Under **Devices > [name of the device] > Installed Apps**, check the app, its version and state; see Checking Installed Apps via the IGEL UMS Web App.

When the update test has been successful, you can update the app on all the required devices.

Triggering the Mass Update

1. In the **UMS Web App > Apps**, select the app to be updated (in our case, Chromium) and click **Set Default Version**.

2. Select the required version.


Browser
Filter objects
Name
Chromium Browser
Newer Version available
Chromium Browser
Create New Profile
Set Default Version
Newest imported version in UMS: 119.0.6045.105 BUILD
Default version for assignment: 112.0.5615.165 BUILD 1
Version 119.0.6045.199 BUILD 2.0 available!
Import newest version from App Portal
Update Settings
Default V
Update D
Set Default Version
Version
119.0.6045.105 BUILD 1.0
Cancel
Save and apply changes on reboot
Assigned
Default version (112.0.5615.165 BUILD 1)

3. Decide when the changes should take effect and save accordingly.

> ✓ If the changes should take effect on reboot, you can create a scheduled job for reboot and/or wakeup and assign it to the devices / device directory or a view (created in the **UMS Console > Views > [context menu] > New View > Installed Apps** criterion). For more information on jobs, see Jobs.

The new version will be downloaded by the devices.

By default, apps / app versions assigned to the device will be automatically activated at the next reboot. By default, the reboot is performed automatically after the timeout of 60 seconds after the app download if the user does not postpone the device restart, see IGEL OS Notification Center(see page 196).
If you have configured the background app update, an **Update** command must be sent instead of the reboot for the app activation; see How to Configure the Background App Update in the IGEL UMS Web App.

4. To verify that all devices have been updated successfully: Under **Devices > [name of the device] > Installed Apps** , check the app, its version and state; or create a view in the **UMS Console > Views** using the **Installed Apps** criterion. See Checking Installed Apps via the IGEL UMS Web App.

Installing the Base System via IGEL OS Creator (OSC)

Installation Requirements and Devices Supported by IGEL OS 12

For the requirements for IGEL OS 12 and the list of the officially supported devices, see https://kb.igel.com/os12-supported-hardware.

Create USB Installation Medium

Windows

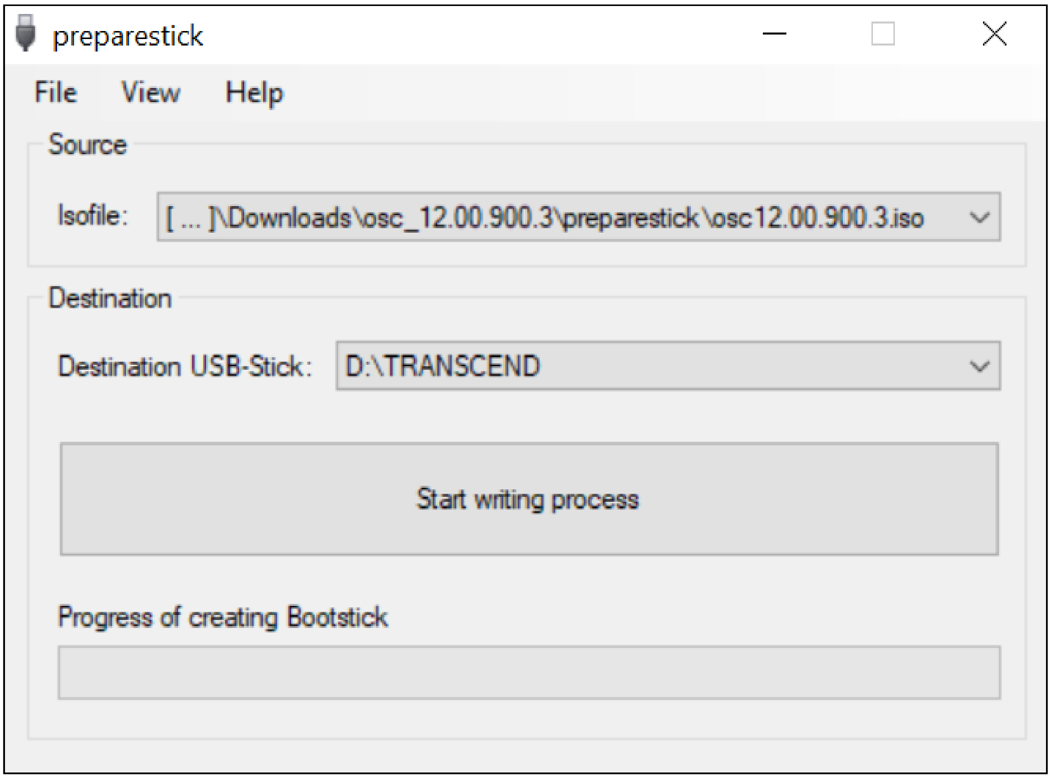
1. Download the ZIP archive for OS Creator from the IGEL Download Server[19]:
   - For new devices, use the standard installer (e.g. `osc_12.01.110.zip`).
   - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e.g. `osc_12.01.110_legacy.zip`).

2. Unzip the contents into a local directory.

3. Connect a USB memory stick with at least 4 GB capacity to the computer.
   All existing data on the USB memory stick will be destroyed.

4. Double-click the `preparestick.exe` file from the unzipped directory.
   If you are in the "administrators" group, the program will start after you have confirmed a dialog. If you are not in the "administrators" group, you must enter the administrator password to start the program.

[19] https://www.igel.com/software-downloads/cosmos/



Isofile: [...]\Downloads\osc_12.00.900.3\preparestick\osc12.00.900.3.iso

Destination USB-Stick: D:\TRANSCEND

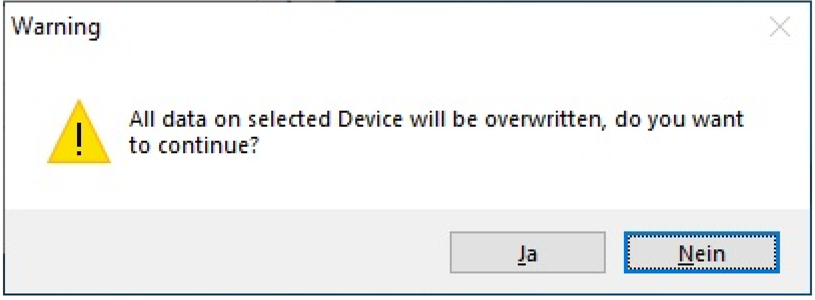
The dropdown menu **Isofile** shows the ISO files contained in the unzipped directory.

5. Under **Isofile**, select the appropriate ISO file, e.g. `osc12.01.110.iso`

6. Under **Destination USB stick**, select the USB storage medium on which you would like to save the installation data.
   It is recommended that you only have one USB storage medium connected during this procedure. If you accidentally select the wrong medium, all data on it will be lost.
   Generally speaking, the list of available USB storage media is refreshed automatically. If, however, you would like to refresh it manually, click on **View > Refresh USB Device List**.

7. Click **Start writing process**.

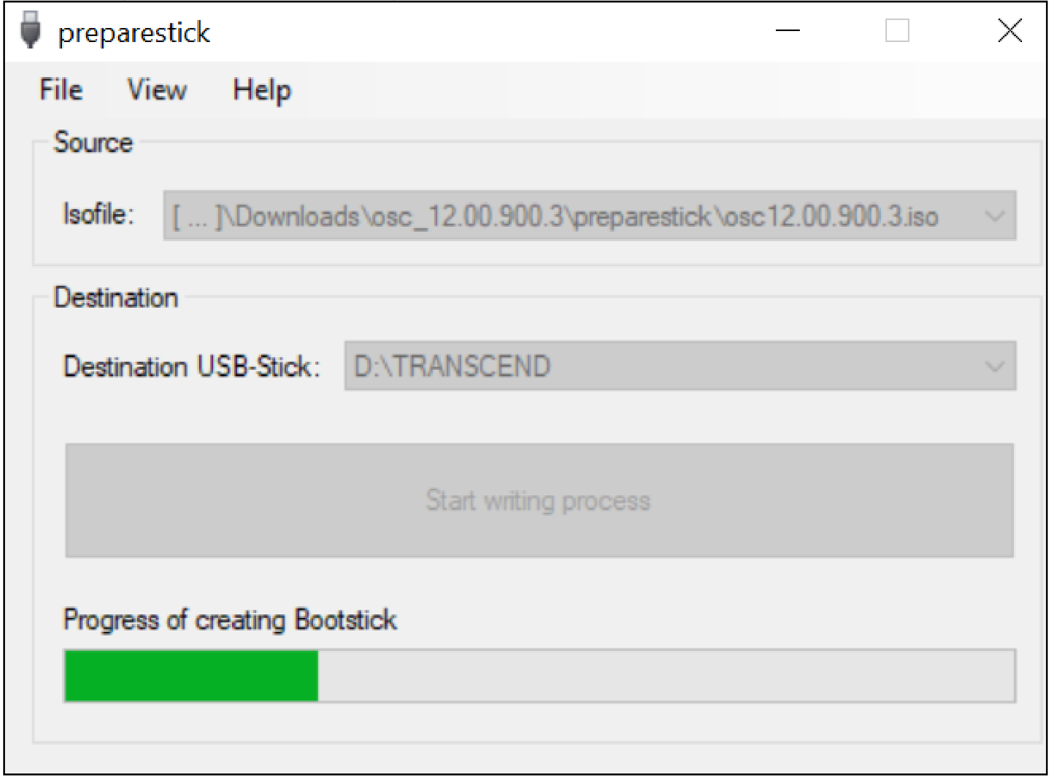
8. Confirm the following dialog:



Warning

All data on selected Device will be overwritten, do you want to continue?

In the program window, the progress of the process is shown.



preparestick

Source

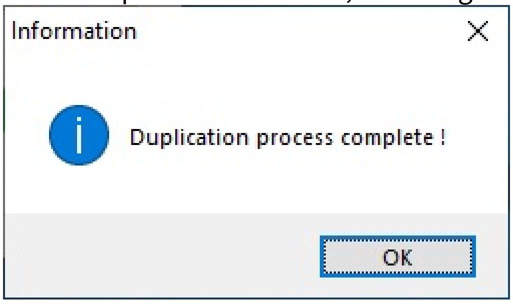
Isofile: [...]\Downloads\osc_12.00.900.3\preparestick\osc12.00.900.3.iso

Destination

Destination USB-Stick: D:\TRANSCEND

Progress of creating Bootstick

When the process is finished, a message window is displayed.



Information

Duplication process complete !

9. Close the message window and the program.

10. After about 3 seconds, remove the USB memory stick.

    > If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

    The USB memory stick for OSC installation is ready for use.

Linux

1. Download the ZIP archive for OS Creator from the IGEL Download Server[20]:
   - For new devices, use the standard installer (e.g. `osc_12.01.110.zip`).
   - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e.g. `osc_12.01.110_legacy.zip`).

2. Unzip the contents into a local directory.

3. From this directory, you will need the ISO file (e.g. `osc12.01.110.iso` or `osc12.01.110_legacy.iso`) to create a bootable medium.

4. Connect a USB memory stick with at least 4 GB capacity to the computer.

   > All existing data on the USB memory stick will be destroyed.

5. Open a terminal emulator and enter the command `dmesg` to determine the device name of the USB memory stick.
   Example output:

   ```
   [...]
   [19514.742229] scsi 3:0:0:0: Direct-Access JetFlash Transcend 8GB 1100 PQ: 0 ANSI: 6
   [19514.742805] sd 3:0:0:0: Attached scsi generic sg1 type 0
   [19514.744688] sd 3:0:0:0: [sdb] 15425536 512-byte logical blocks: (7.89 GB/7.35 GiB)
   [19514.745370] sd 3:0:0:0: [sdb] Write Protect is off
   [19514.745376] sd 3:0:0:0: [sdb] Mode Sense: 43 (0) 00 00 00
   [19514.746040] sd 3:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
   [19514.752438] sdb: sdb1
   ```

   In this example, the device name searched for is `/dev/sdb`.

[20] https://www.igel.com/software-downloads/cosmos/

> Ensure that you have determined the correct device name. Use of the `dd` command in the next step can destroy your operating system if you use the wrong device name.

6. The following command writes the installation data to the USB memory stick:
   `dd if=osc12.01.110.iso of=/dev/sdX bs=1M oflag=direct`
   Replace `sdX` with the device name of the USB memory stick that you have determined.
   When the `dd` command has terminated, you can see the terminal emulator input prompt again.

7. Wait for about 3 seconds after the `dd` command has terminated, and remove the USB memory stick.

   > If you remove the USB memory stick immediately, there is a possibility that the writing process has not been completed. In this case, the data on the memory stick gets corrupted.

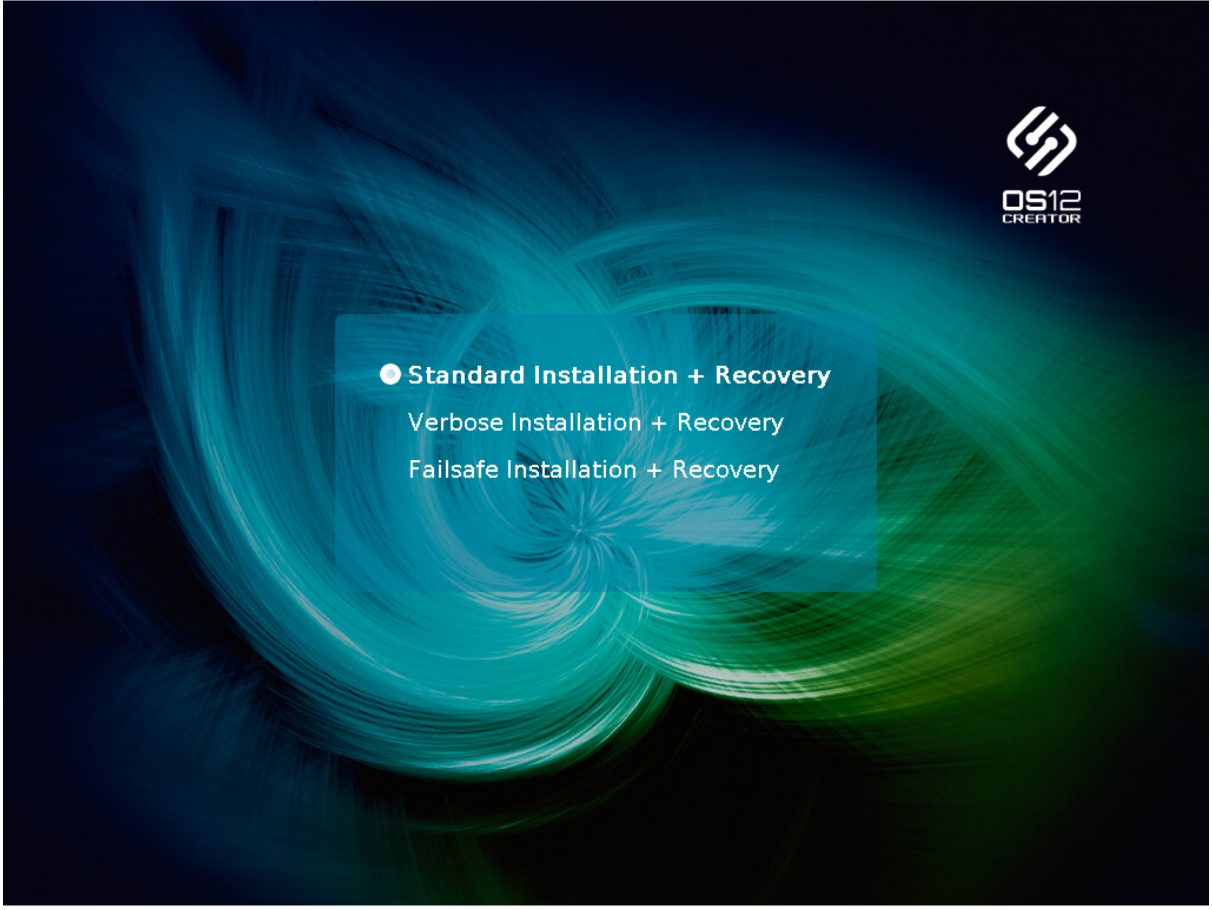
   The USB memory stick for OSC installation is ready for use.

Installation Procedure

> The installation will overwrite all existing data on the target drive.

1. Connect the prepared USB memory stick to the target device and switch the target device on. General information on how you can boot from the stick can be found under Boot Settings.

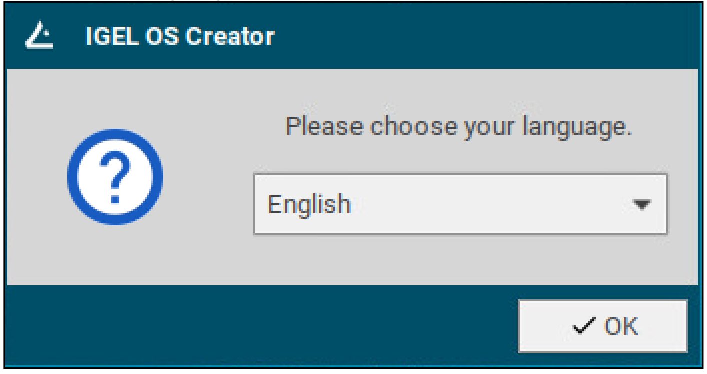
2. Select one of the following options from the boot menu:



● Standard Installation + Recovery
Verbose Installation + Recovery
Failsafe Installation + Recovery

- **Standard Installation + Recovery**: Boots the system with just a few messages from the USB memory stick and launches the installation program. (Default)
- **Verbose Installation + Recovery**: Boots the system from the USB memory stick and shows the Linux boot messages in the process.
- **Failsafe Installation + Recovery**: Fallback mode; to be used if the graphical boot screen cannot be displayed.
- **Memory Test**: Memory test, only available in legacy/BIOS mode. This option does not carry out an installation.

3. Select the language for the installation process.

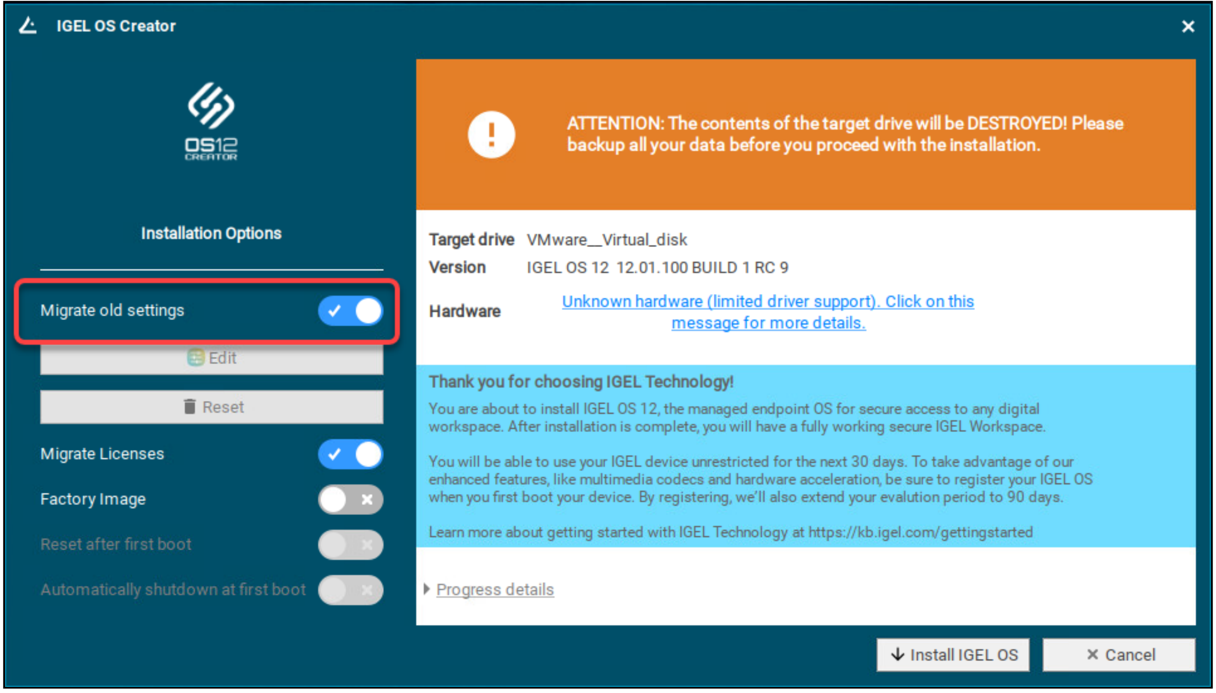


IGEL OS Creator

Please choose your language.

English

4. If IGEL OS 12 has been running on the device before and you want to preserve the device's settings, ensure that **Migrate old settings** is enabled.



IGEL OS Creator

ATTENTION: The contents of the target drive will be DESTROYED! Please backup all your data before you proceed with the installation.

Installation Options

Migrate old settings ☑

Migrate Licenses ☑

Factory Image ☒

Reset after first boot ☒

Automatically shutdown at first boot ☒

Target drive VMware__Virtual_disk

Version IGEL OS 12 12.01.100 BUILD 1 RC 9

Hardware Unknown hardware (limited driver support). Click on this message for more details.

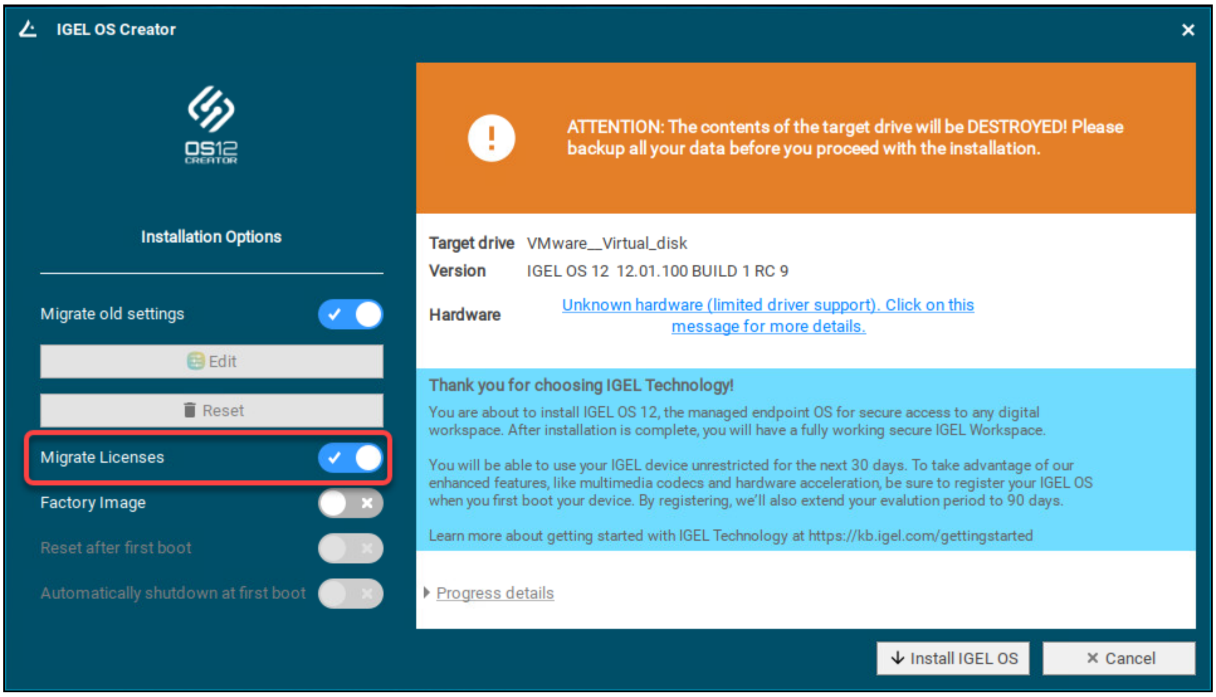
Thank you for choosing IGEL Technology!

You are about to install IGEL OS 12, the managed endpoint OS for secure access to any digital workspace. After installation is complete, you will have a fully working secure IGEL Workspace.

You will be able to use your IGEL device unrestricted for the next 30 days. To take advantage of our enhanced features, like multimedia codecs and hardware acceleration, be sure to register your IGEL OS when you first boot your device. By registering, we'll also extend your evalution period to 90 days.

Learn more about getting started with IGEL Technology at https://kb.igel.com/gettingstarted

5. If one of the following is the case, make sure that **Migrate licenses** is enabled:
- Your device has been operating with IGEL OS 11 before and you want to preserve the device's IGEL OS 11 licenses because you want to test IGEL OS 12 and downgrade to IGEL OS 11 afterward
- Your device has been operating with IGEL OS 12 before and you want to keep the licenses on the device



IGEL OS Creator

Installation Options

- Migrate old settings: ✓ on
- Edit
- Reset
- Migrate Licenses: ✓ on
- Factory Image: off
- Reset after first boot: off
- Automatically shutdown at first boot: off

ATTENTION: The contents of the target drive will be DESTROYED! Please backup all your data before you proceed with the installation.

Target drive VMware__Virtual_disk
Version IGEL OS 12 12.01.100 BUILD 1 RC 9
Hardware Unknown hardware (limited driver support). Click on this message for more details.

Thank you for choosing IGEL Technology!

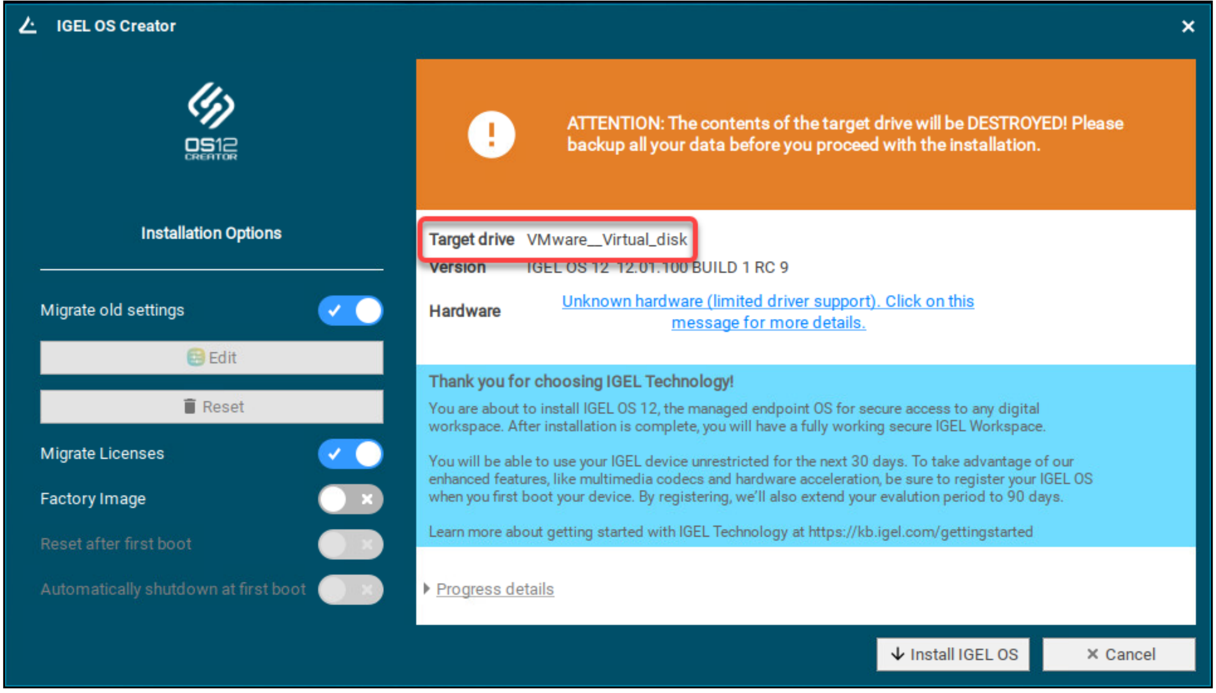
You are about to install IGEL OS 12, the managed endpoint OS for secure access to any digital workspace. After installation is complete, you will have a fully working secure IGEL Workspace.

You will be able to use your IGEL device unrestricted for the next 30 days. To take advantage of our enhanced features, like multimedia codecs and hardware acceleration, be sure to register your IGEL OS when you first boot your device. By registering, we'll also extend your evalution period to 90 days.

Learn more about getting started with IGEL Technology at https://kb.igel.com/gettingstarted

Progress details

6. Check the **Target drive** to ensure that the system is installed on the desired drive.



IGEL OS Creator

Installation Options

- Migrate old settings: ✓ on
- Edit
- Reset
- Migrate Licenses: ✓ on
- Factory Image: off
- Reset after first boot: off
- Automatically shutdown at first boot: off

ATTENTION: The contents of the target drive will be DESTROYED! Please backup all your data before you proceed with the installation.

Target drive VMware__Virtual_disk
Version IGEL OS 12 12.01.100 BUILD 1 RC 9
Hardware Unknown hardware (limited driver support). Click on this message for more details.

Thank you for choosing IGEL Technology!

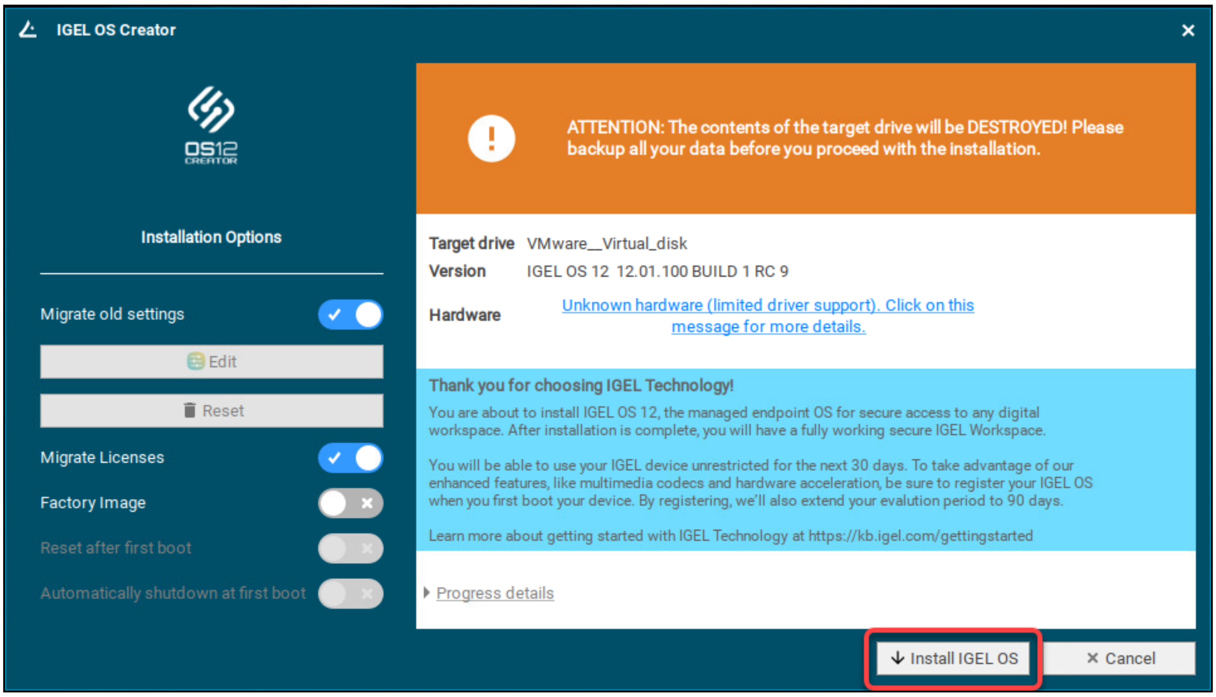
You are about to install IGEL OS 12, the managed endpoint OS for secure access to any digital workspace. After installation is complete, you will have a fully working secure IGEL Workspace.

You will be able to use your IGEL device unrestricted for the next 30 days. To take advantage of our enhanced features, like multimedia codecs and hardware acceleration, be sure to register your IGEL OS when you first boot your device. By registering, we'll also extend your evalution period to 90 days.

Learn more about getting started with IGEL Technology at https://kb.igel.com/gettingstarted

Progress details

7. Click **Install IGEL OS**.



Migrate old settings ●

Migrate Licenses ●

Factory Image ○

Reset after first boot ○

Automatically shutdown at first boot ○

ATTENTION: The contents of the target drive will be DESTROYED! Please backup all your data before you proceed with the installation.

Target drive VMware__Virtual_disk

Version IGEL OS 12 12.01.100 BUILD 1 RC 9

Hardware Unknown hardware (limited driver support). Click on this message for more details.

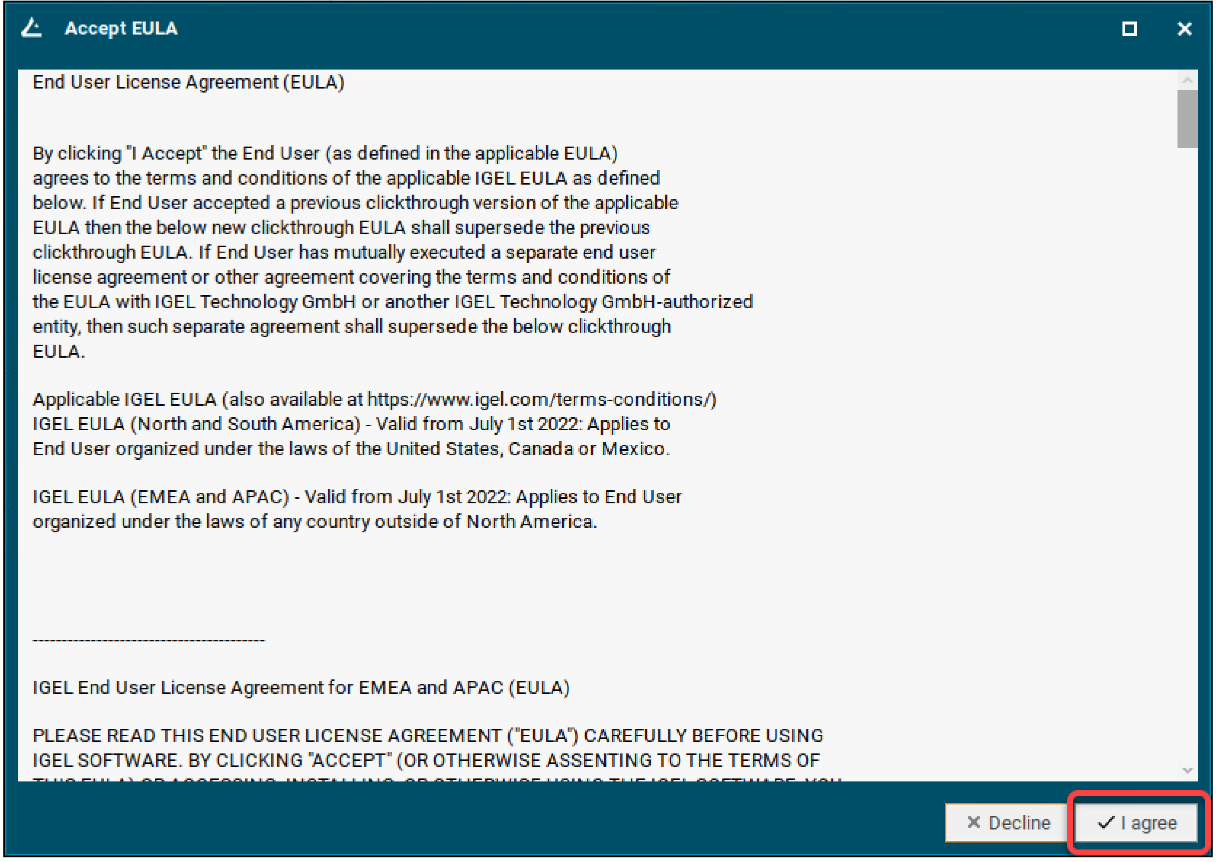
Thank you for choosing IGEL Technology!

You are about to install IGEL OS 12, the managed endpoint OS for secure access to any digital workspace. After installation is complete, you will have a fully working secure IGEL Workspace.

You will be able to use your IGEL device unrestricted for the next 30 days. To take advantage of our enhanced features, like multimedia codecs and hardware acceleration, be sure to register your IGEL OS when you first boot your device. By registering, we'll also extend your evalution period to 90 days.

Learn more about getting started with IGEL Technology at https://kb.igel.com/gettingstarted

8. Accept the **EULA** by clicking **I agree**.



End User License Agreement (EULA)

By clicking "I Accept" the End User (as defined in the applicable EULA) agrees to the terms and conditions of the applicable IGEL EULA as defined below. If End User accepted a previous clickthrough version of the applicable EULA then the below new clickthrough EULA shall supersede the previous clickthrough EULA. If End User has mutually executed a separate end user license agreement or other agreement covering the terms and conditions of the EULA with IGEL Technology GmbH or another IGEL Technology GmbH-authorized entity, then such separate agreement shall supersede the below clickthrough EULA.

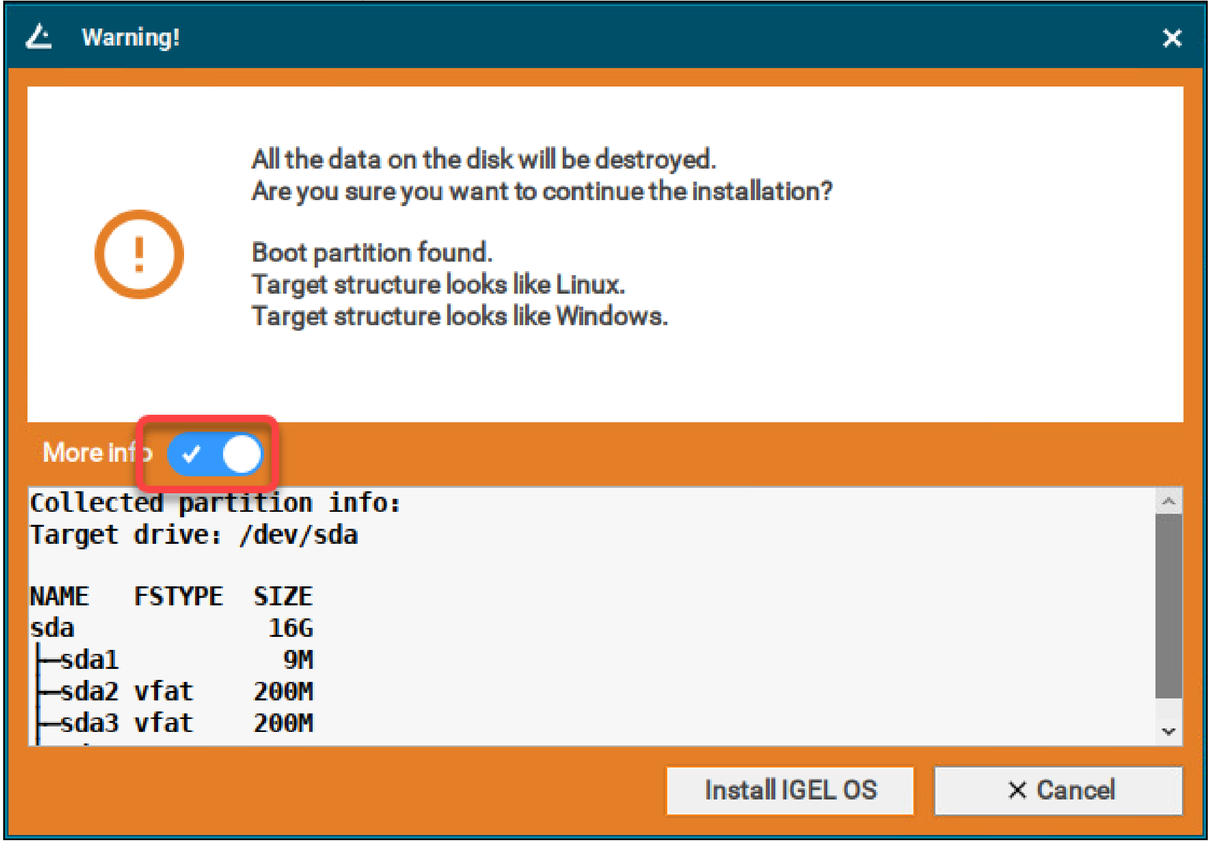
Applicable IGEL EULA (also available at https://www.igel.com/terms-conditions/)
IGEL EULA (North and South America) - Valid from July 1st 2022: Applies to End User organized under the laws of the United States, Canada or Mexico.

IGEL EULA (EMEA and APAC) - Valid from July 1st 2022: Applies to End User organized under the laws of any country outside of North America.

IGEL End User License Agreement for EMEA and APAC (EULA)

PLEASE READ THIS END USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE USING IGEL SOFTWARE. BY CLICKING "ACCEPT" (OR OTHERWISE ASSENTING TO THE TERMS OF

9. To view the details for the target drive, click **More Info**.

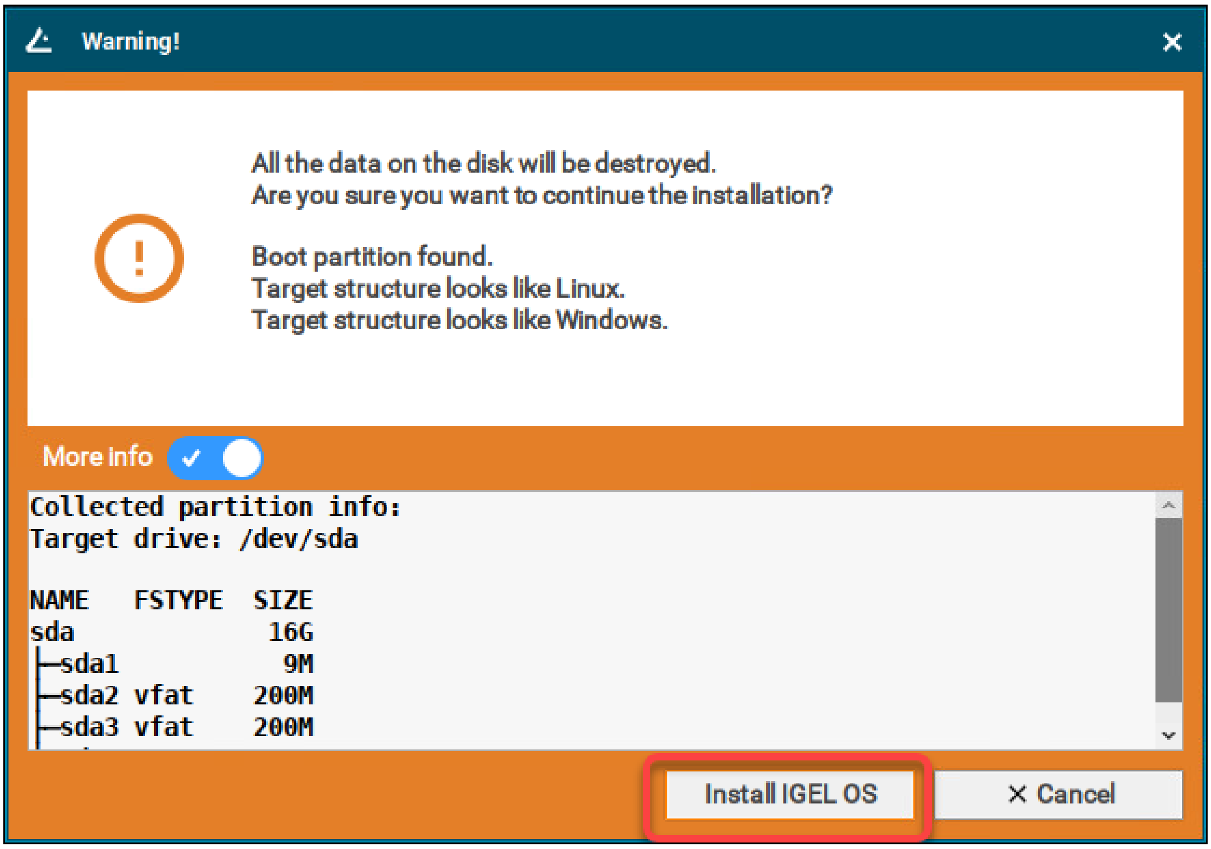


All the data on the disk will be destroyed.
Are you sure you want to continue the installation?

Boot partition found.
Target structure looks like Linux.
Target structure looks like Windows.

```
Collected partition info:
Target drive: /dev/sda

NAME   FSTYPE  SIZE
sda             16G
├─sda1           9M
├─sda2 vfat    200M
├─sda3 vfat    200M
```

10. Click **Install IGEL OS**.



Warning!

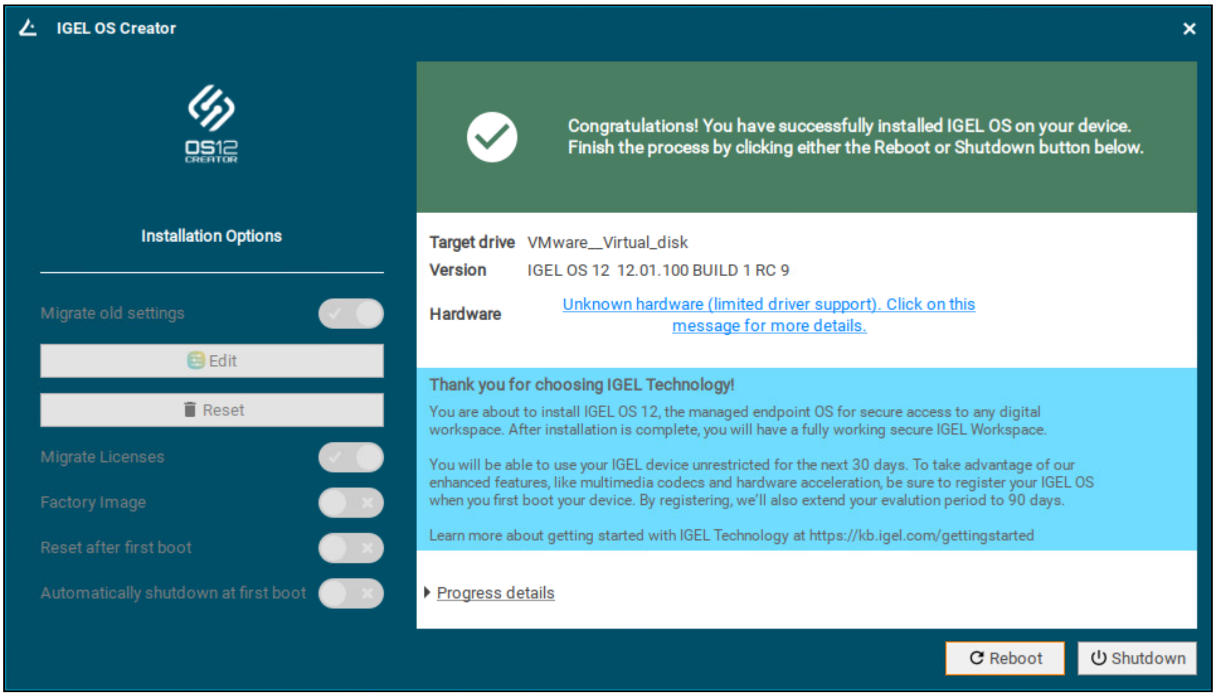
All the data on the disk will be destroyed.
Are you sure you want to continue the installation?

Boot partition found.
Target structure looks like Linux.
Target structure looks like Windows.

More info ✓

```
Collected partition info:
Target drive: /dev/sda

NAME    FSTYPE   SIZE
sda               16G
├─sda1             9M
├─sda2 vfat      200M
├─sda3 vfat      200M
```

The installation program will install IGEL OS 12 on the target drive. If you see the success message, the installation is complete.



IGEL OS Creator

Installation Options

Migrate old settings

Edit

Reset

Migrate Licenses

Factory Image

Reset after first boot

Automatically shutdown at first boot

Congratulations! You have successfully installed IGEL OS on your device. Finish the process by clicking either the Reboot or Shutdown button below.

Target drive VMware__Virtual_disk

Version IGEL OS 12 12.01.100 BUILD 1 RC 9

Hardware Unknown hardware (limited driver support). Click on this message for more details.

Thank you for choosing IGEL Technology!

You are about to install IGEL OS 12, the managed endpoint OS for secure access to any digital workspace. After installation is complete, you will have a fully working secure IGEL Workspace.

You will be able to use your IGEL device unrestricted for the next 30 days. To take advantage of our enhanced features, like multimedia codecs and hardware acceleration, be sure to register your IGEL OS when you first boot your device. By registering, we'll also extend your evalution period to 90 days.

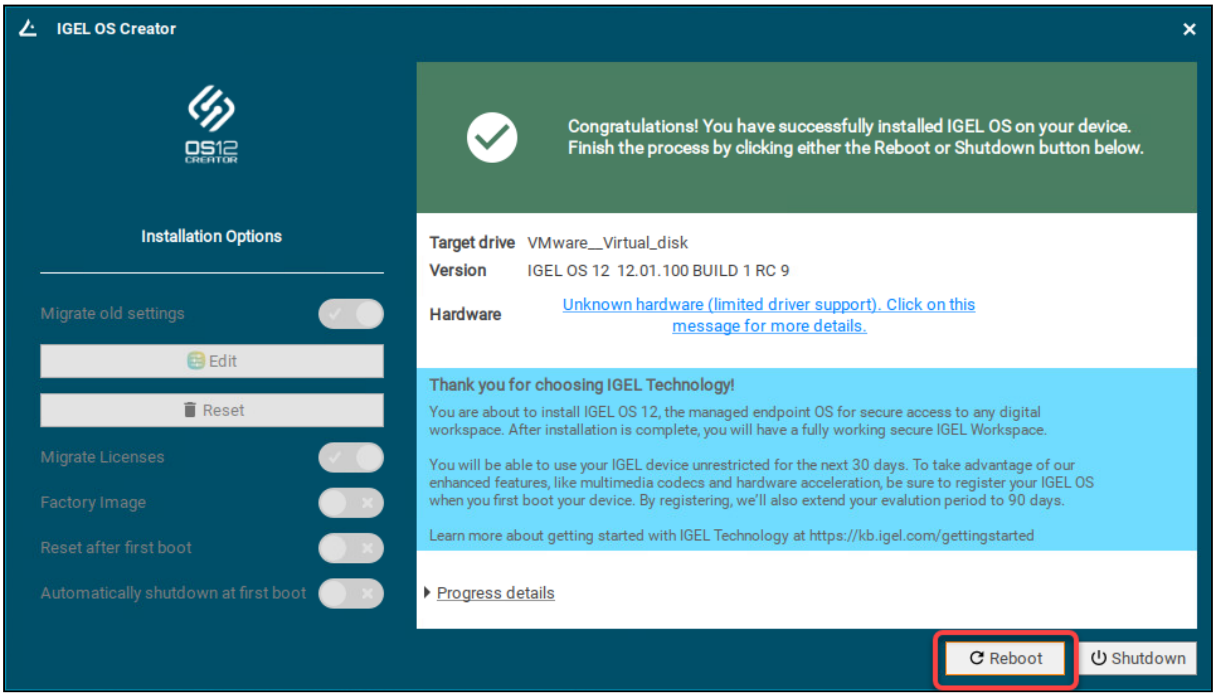
Learn more about getting started with IGEL Technology at https://kb.igel.com/gettingstarted

Progress details

Reboot

Shutdown

11. Click **Reboot**.



IGEL OS Creator

Installation Options

Migrate old settings

Edit

Reset

Migrate Licenses

Factory Image

Reset after first boot

Automatically shutdown at first boot

Congratulations! You have successfully installed IGEL OS on your device. Finish the process by clicking either the Reboot or Shutdown button below.

Target drive VMware__Virtual_disk

Version IGEL OS 12 12.01.100 BUILD 1 RC 9

Hardware Unknown hardware (limited driver support). Click on this message for more details.

Thank you for choosing IGEL Technology!

You are about to install IGEL OS 12, the managed endpoint OS for secure access to any digital workspace. After installation is complete, you will have a fully working secure IGEL Workspace.

You will be able to use your IGEL device unrestricted for the next 30 days. To take advantage of our enhanced features, like multimedia codecs and hardware acceleration, be sure to register your IGEL OS when you first boot your device. By registering, we'll also extend your evalution period to 90 days.

Learn more about getting started with IGEL Technology at https://kb.igel.com/gettingstarted

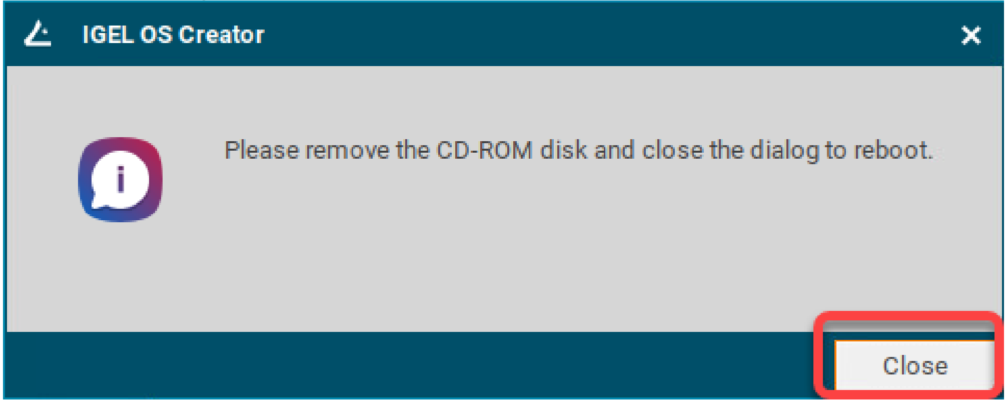
Progress details

Reboot

Shutdown

12. Remove the USB memory stick.

13. Close the message window.



Please remove the CD-ROM disk and close the dialog to reboot.

The system will shut down and then boot IGEL OS 12.
The device is ready for onboarding; for details, see Onboarding IGEL OS 12 Devices(see page 158).

Licensing

To work with your IGEL environment, your devices must have valid licenses.

You can deploy your licenses via Automatic License Deployment (ALD), which is the preferred method, or manually. For a list of all deployment methods, see Deploying Licenses.

EULA Must Be Accepted

To prepare your licenses for deployment, you must accept the EULA for the Product Pack that contains your licenses. For instructions, see Accepting the EULA(see page 152).

Starter License, Demo Licenses, and Limitations on Expiry

As long as no demo license has been deployed, your IGEL OS 12 devices will use a starter license that is valid for 30 days. The following tables show which features are supported by which license and what happens if the demo license expires:

Endpoint Device / Apps

Function	Starter License (30 Days)	Demo License (90 Days)	After Expiry of Starter License / Demo License
Connect to UMS/ICG	✓	✓	✓
Use installed apps	✓	✓	✗
Activate multimedia codecs	✗	✓	✗
Shared Workplace	✓	✓	✗
Connect to ICG	✓	✓	✗
Install/update apps locally	✓ *	✓	✗
Update IGEL OS locally	✓ *	✓	✗

*Only if the device is managed by the UMS

Remote Management (UMS)

Function	Starter License (30 Days)	Demo License (90 Days)	After Expiry of Starter License / Demo License
Deploy productive license	✓	✓	✓
Shadow device (always secure)	✓	✓	✓

Function	Starter License (30 Days)	Demo License (90 Days)	After Expiry of Starter License / Demo License
Power control commands	✓	✓	✓
IGEL Management Interface (IMI)	✓	✓	✓
Perform device configuration changes (profiles/TC settings)	✓	✓	✗
Trigger update to the latest OS	✓	✓	✗
Trigger app installation/updates	✓	✓	✗
Asset Inventory Tracker (AIT)	✓	✓	✗
Modern Management (e.g. WS1)	✓	✓	✗
Enable app auto-update	✓	✓	✗

Onboarding Service (OBS)

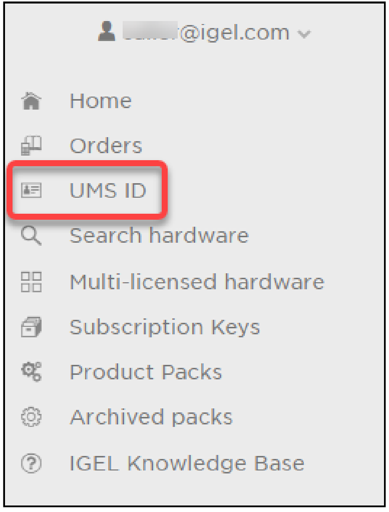
Function	Starter License (90 Days)	Demo License (90 Days)	After Expiry of Starter License / Demo License
Access OBS	✓	✓	✓
Redirect to UMS/ICG	✓	✓	✓

Getting Your Licenses Ready for Deployment

1. Log in to the IGEL License Portal (ILP) at https://activation.igel.com[21]. If you do not have an ILP account yet, you must register with the ILP. For details, see Registering on the IGEL License Portal (ILP).

[21] https://activation.igel.com/

2. Go to **UMS ID**, find the UMS you want to use for deployment, and click ⊕.



[redacted]@igel.com

Home

Orders

UMS ID

Search hardware

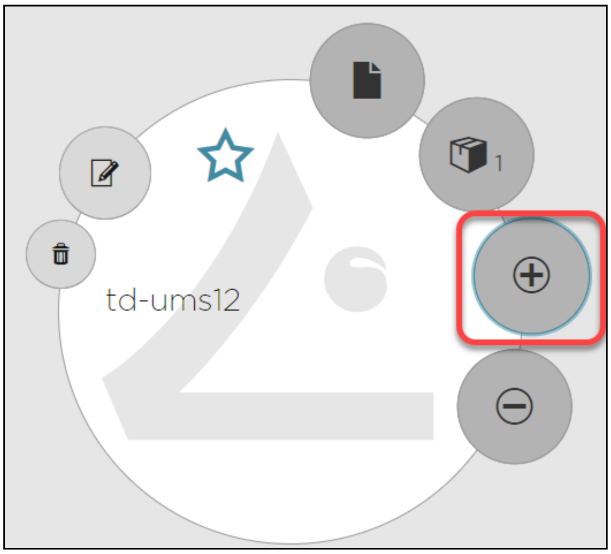
Multi-licensed hardware

Subscription Keys

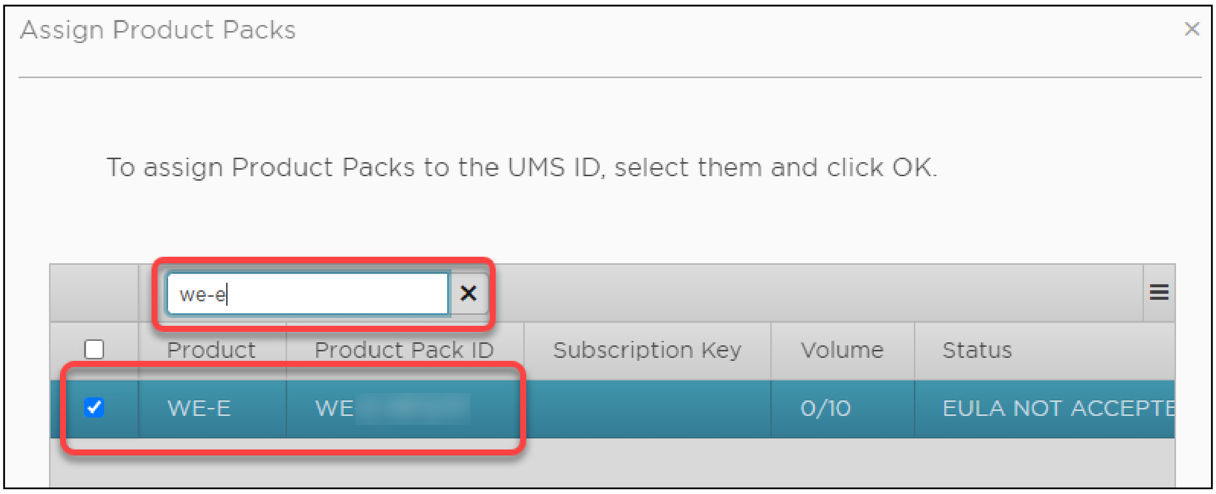
Product Packs

Archived packs

IGEL Knowledge Base



3. Search for "we-e" and select the relevant Product Pack.



Assign Product Packs

To assign Product Packs to the UMS ID, select them and click OK.

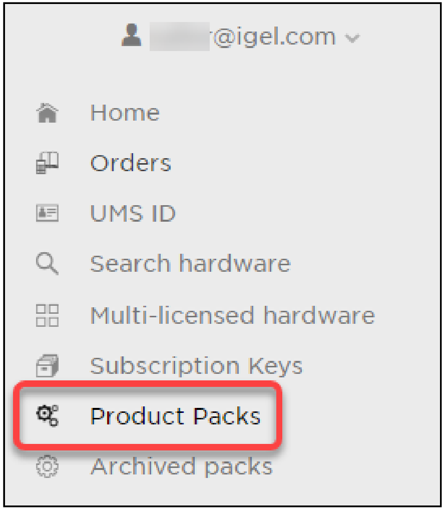
we-e

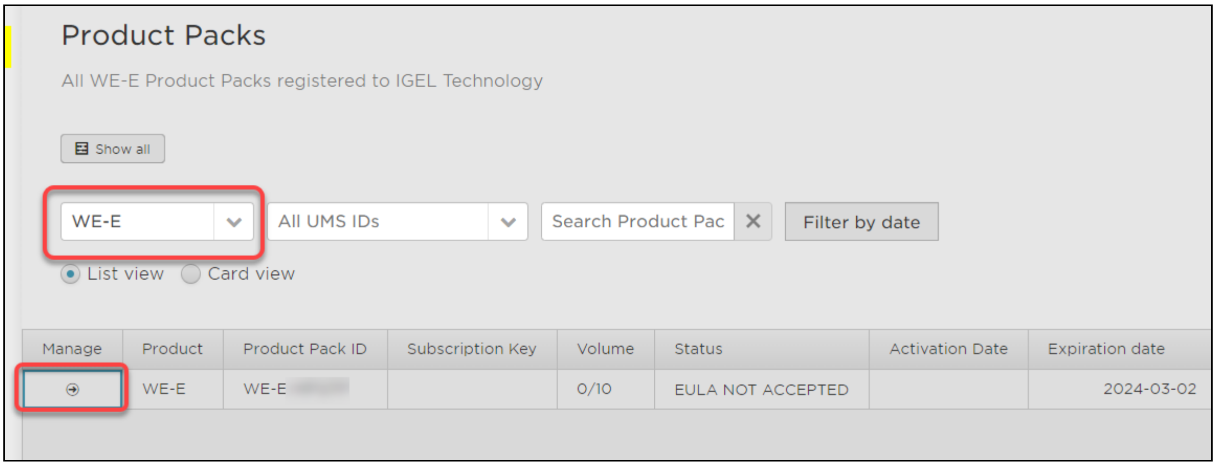
□	Product	Product Pack ID	Subscription Key	Volume	Status
☑	WE-E	WE [redacted]		0/10	EULA NOT ACCEPTE

If you can not find the Product Pack, it may be that it has been assigned to another UMS that was defined as the default UMS resp. default UMS ID. (If a default UMS ID has been defined in your ILP, a new WE-E Product Pack will be assigned to that UMS automatically.)

To correct this, go to the default UMS ID, which is marked with a ★, click ⊖, unassign the Product Pack from this UMS and then use ⊕ on the relevant UMS ID to assign it to the proper UMS.

4. Go to **Product Packs**, select "WE-E" and then select the relevant Product Pack.





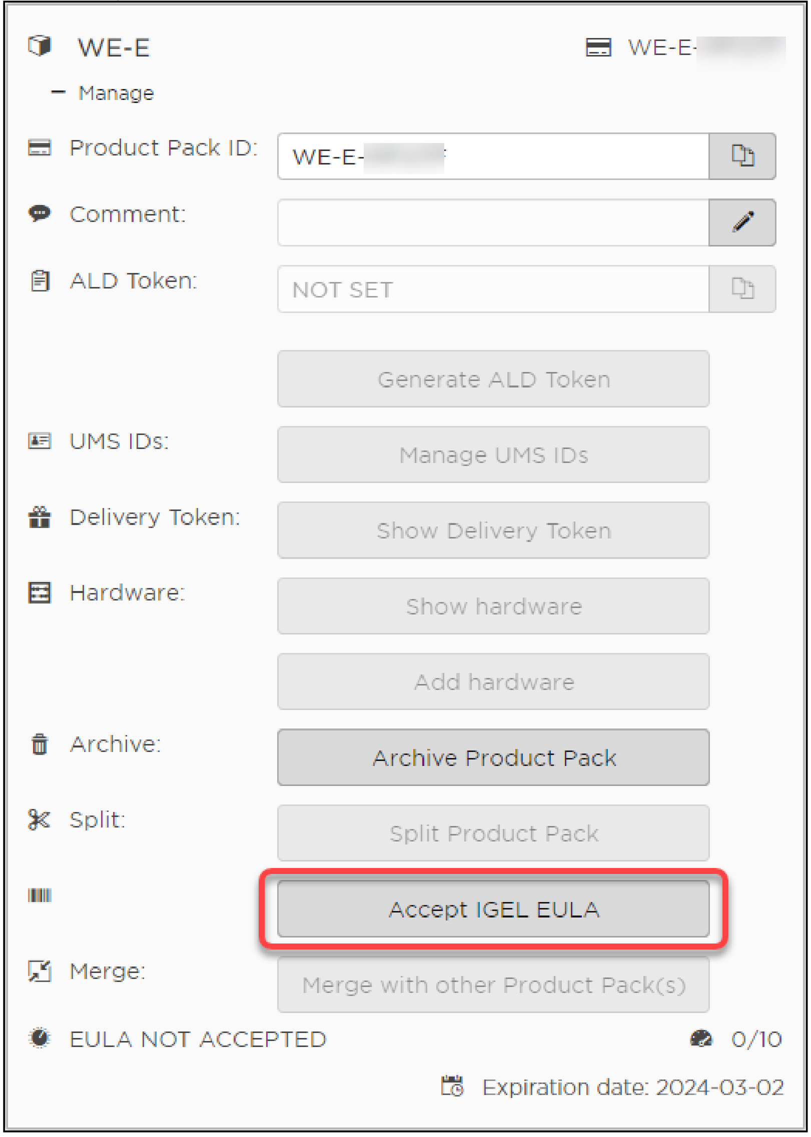
Product Packs

All WE-E Product Packs registered to IGEL Technology

● List view ○ Card view

Manage	Product	Product Pack ID	Subscription Key	Volume	Status	Activation Date	Expiration date
⊕	WE-E	WE-E [redacted]		0/10	EULA NOT ACCEPTED		2024-03-02

5. In the single view for your Product Pack, click **Accept IGEL EULA**.



WE-E

WE-E-[redacted]

Product Pack ID: WE-E-[redacted]

Comment:

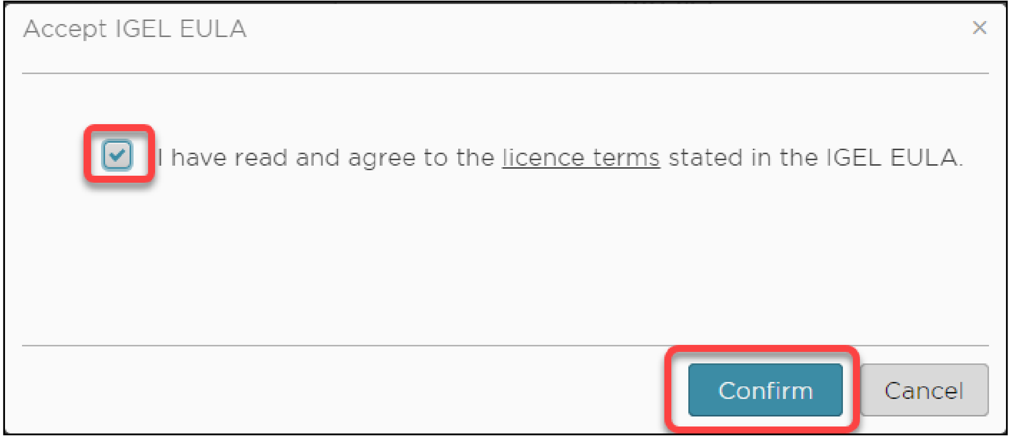
ALD Token: NOT SET

EULA NOT ACCEPTED

0/10

Expiration date: 2024-03-02

6. Confirm that you accept the EULA.



Accept IGEL EULA

☑ I have read and agree to the licence terms stated in the IGEL EULA.

Your licenses are ready for deployment.
You can continue with Setting up Automatic License Deployment (ALD).

Onboarding IGEL OS 12 Devices

If you have configured the IGEL Onboarding Service(see page 41), you use it to register your IGEL OS 12; see Register IGEL OS 12 Devices with the UMS via IGEL Onboarding Service(see page 158).

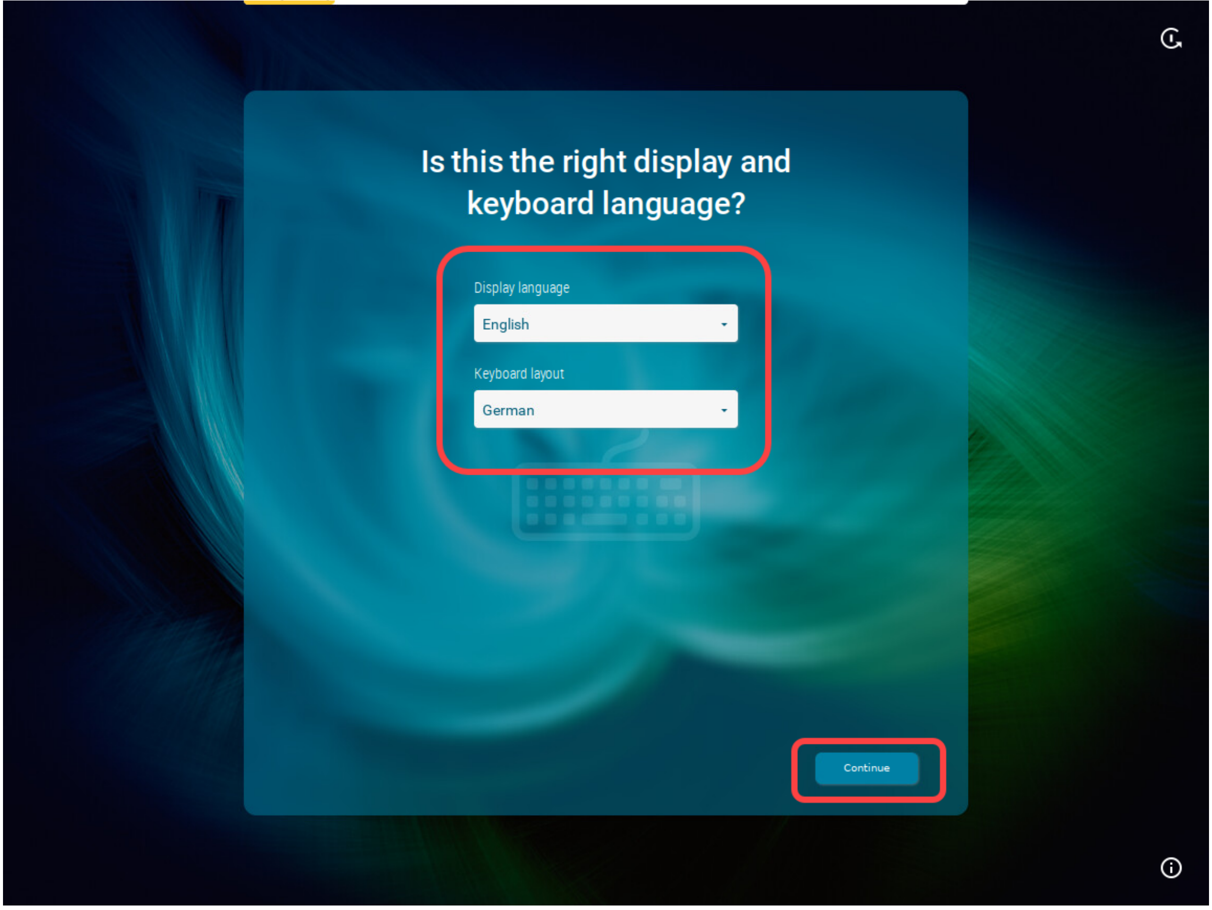
For an alternative device registration method, see Alternative Onboarding Method: Registering Devices with the UMS Using the One-Time Password(see page 165).

> ⓘ If you decide for some reason not to use the IGEL Onboarding Service or the one-time password method, you can skip the corresponding steps in the Setup Assistant. Your IGEL OS 12 device will start with a Starter license(see page 151).
> To register this device with the UMS Server, you can use the **Scan for devices** function, see Scanning the Network for Devices and Registering Devices on the IGEL UMS. For other device registration methods, see Registering IGEL OS Devices on the UMS Server.

Register IGEL OS 12 Devices with the UMS via IGEL Onboarding Service

1. Switch your device on.
   The Setup Assistant starts.

2. Choose the display language and set your keyboard layout. Click **Continue**.

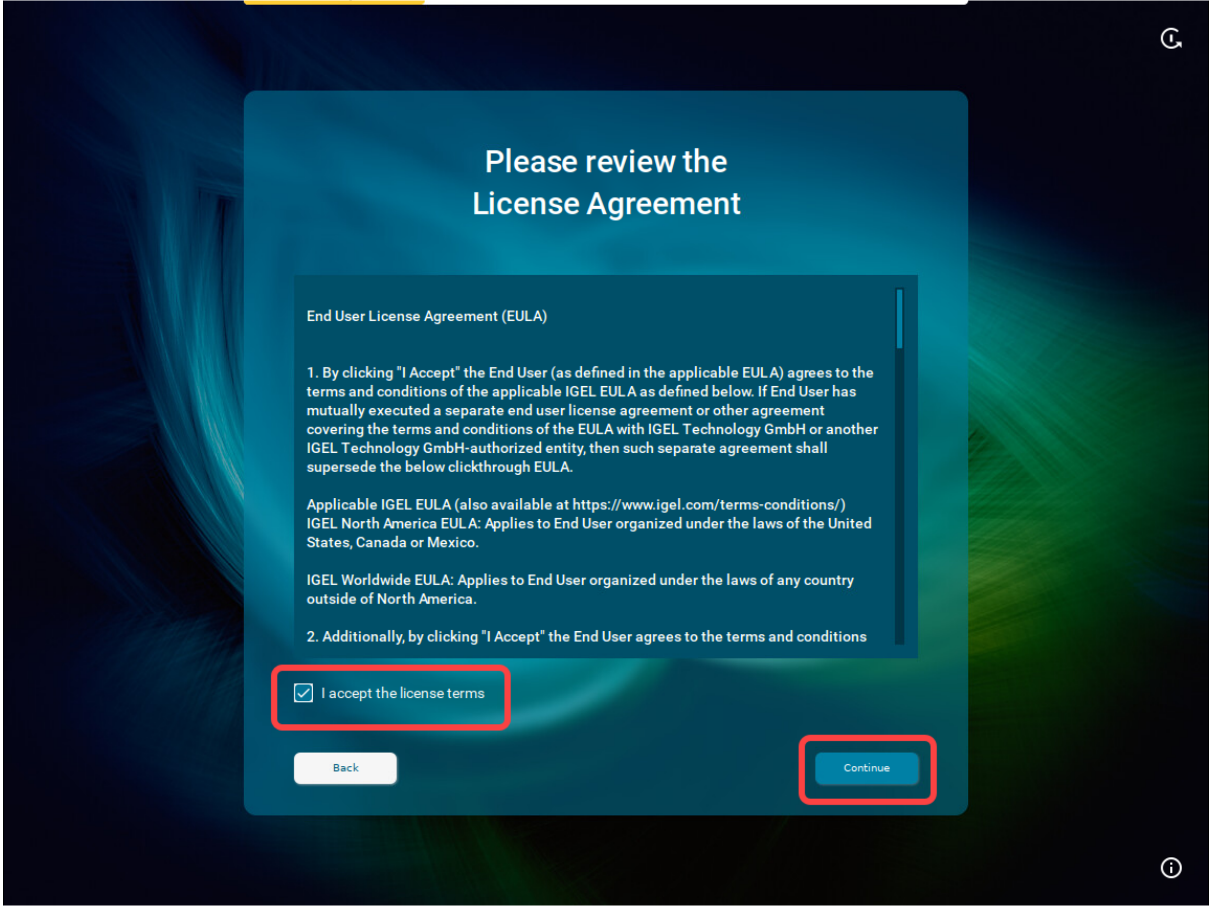


Is this the right display and keyboard language?

Display language: English

Keyboard layout: German

3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.



Please review the License Agreement

End User License Agreement (EULA)

1. By clicking "I Accept" the End User (as defined in the applicable EULA) agrees to the terms and conditions of the applicable IGEL EULA as defined below. If End User has mutually executed a separate end user license agreement or other agreement covering the terms and conditions of the EULA with IGEL Technology GmbH or another IGEL Technology GmbH-authorized entity, then such separate agreement shall supersede the below clickthrough EULA.

Applicable IGEL EULA (also available at https://www.igel.com/terms-conditions/) IGEL North America EULA: Applies to End User organized under the laws of the United States, Canada or Mexico.

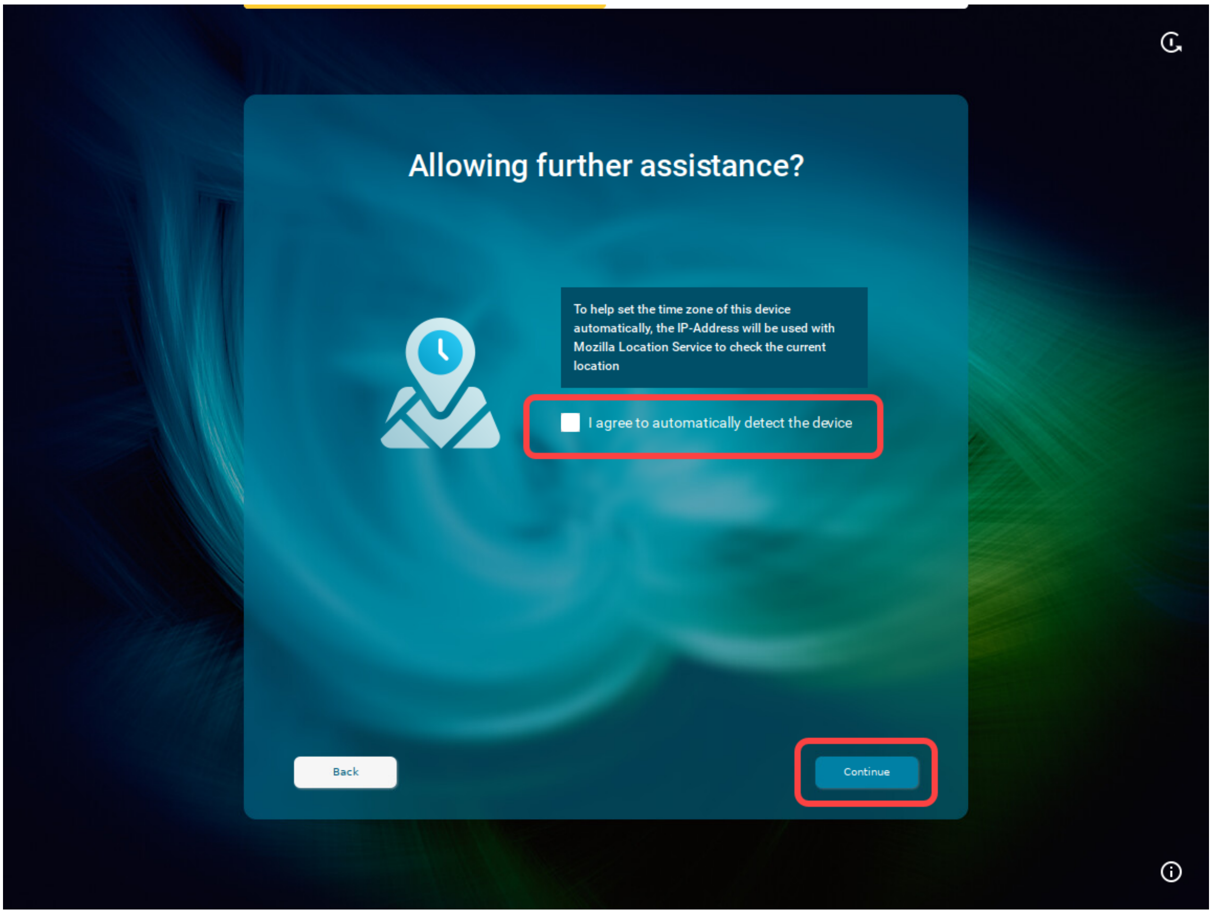
IGEL Worldwide EULA: Applies to End User organized under the laws of any country outside of North America.

2. Additionally, by clicking "I Accept" the End User agrees to the terms and conditions

☑ I accept the license terms

4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under Troubleshooting: Configuring a Network during the Onboarding(see page 175).

5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.

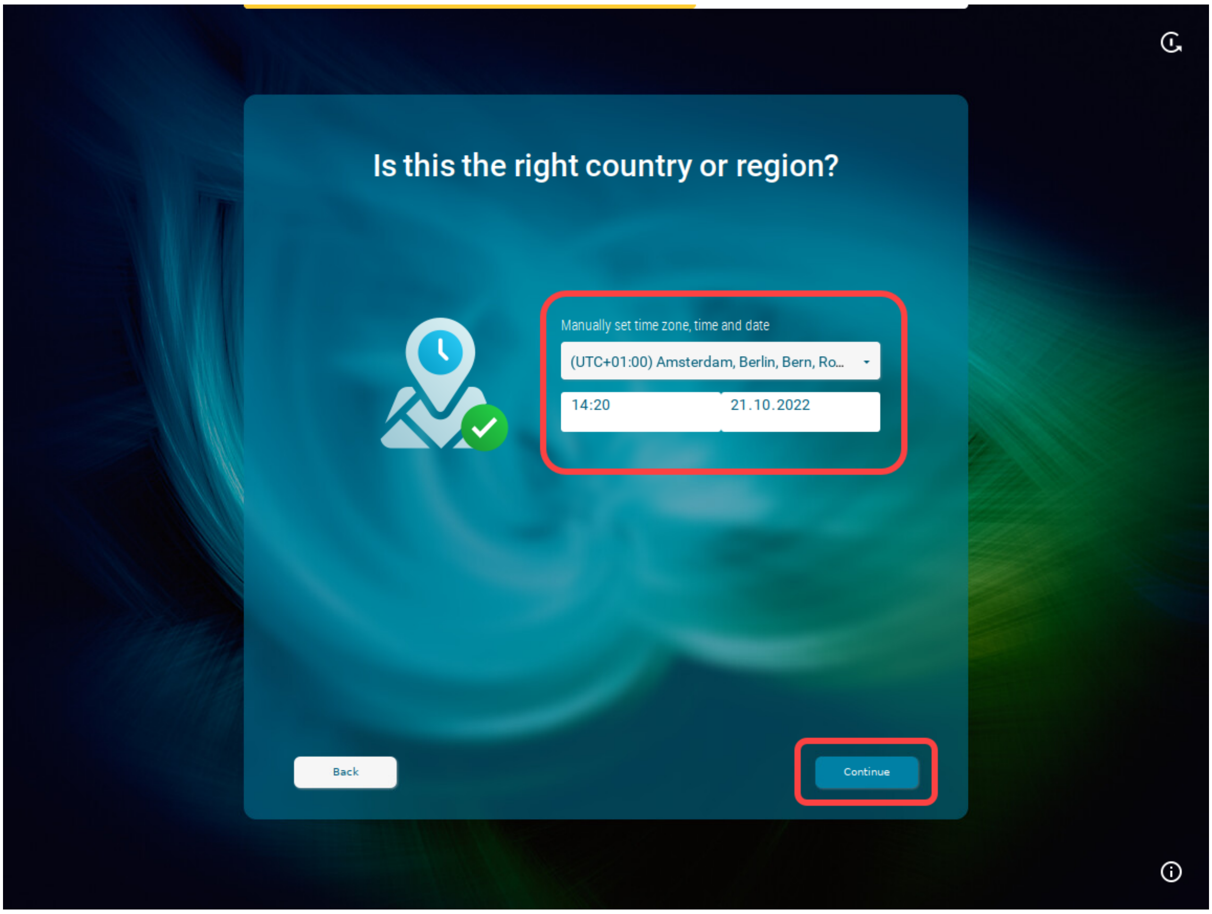


Allowing further assistance?

To help set the time zone of this device automatically, the IP-Address will be used with Mozilla Location Service to check the current location

□ I agree to automatically detect the device

Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.



Is this the right country or region?

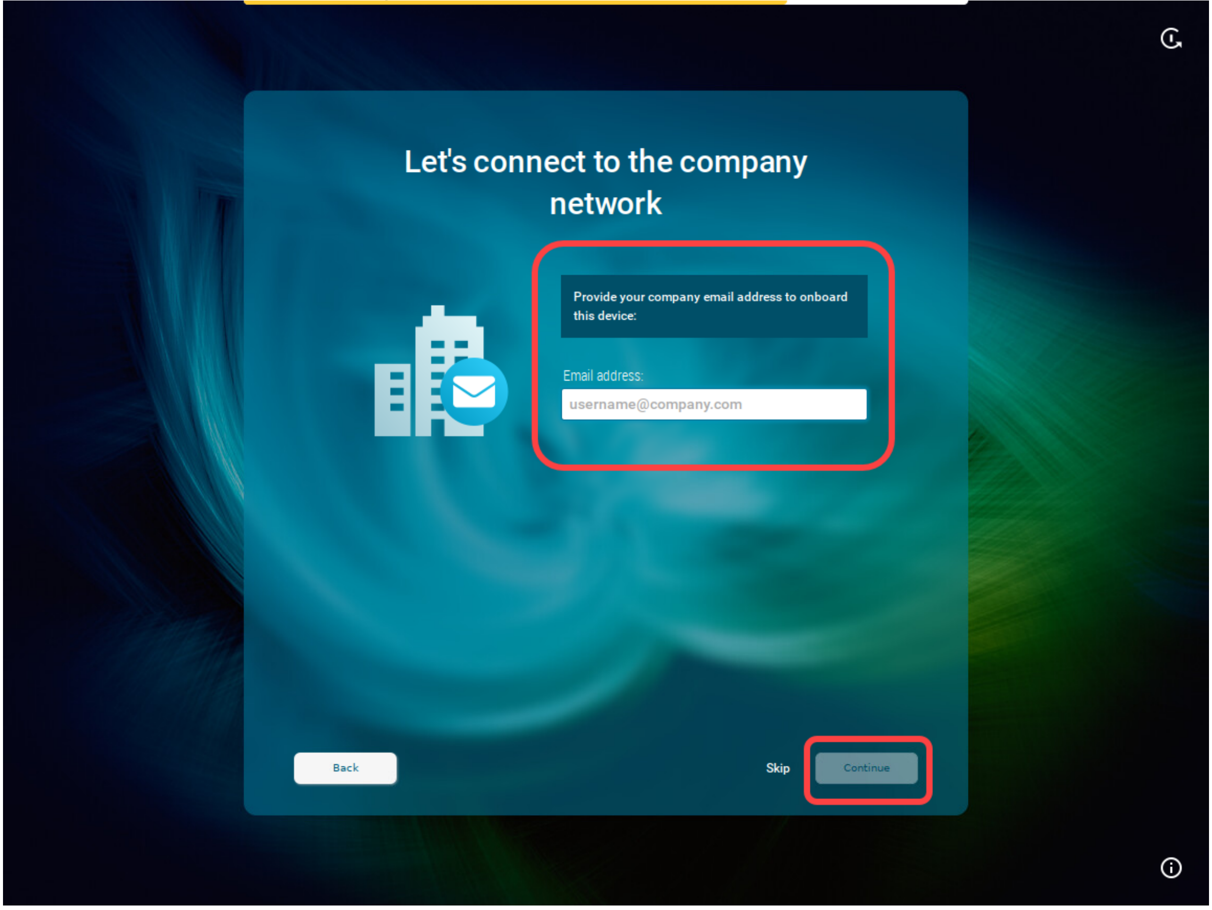
Manually set time zone, time and date

(UTC+01:00) Amsterdam, Berlin, Bern, Ro...

14:20

21.10.2022

6. Enter your e-mail address (using the correct upper/lowercase) and click **Continue**.



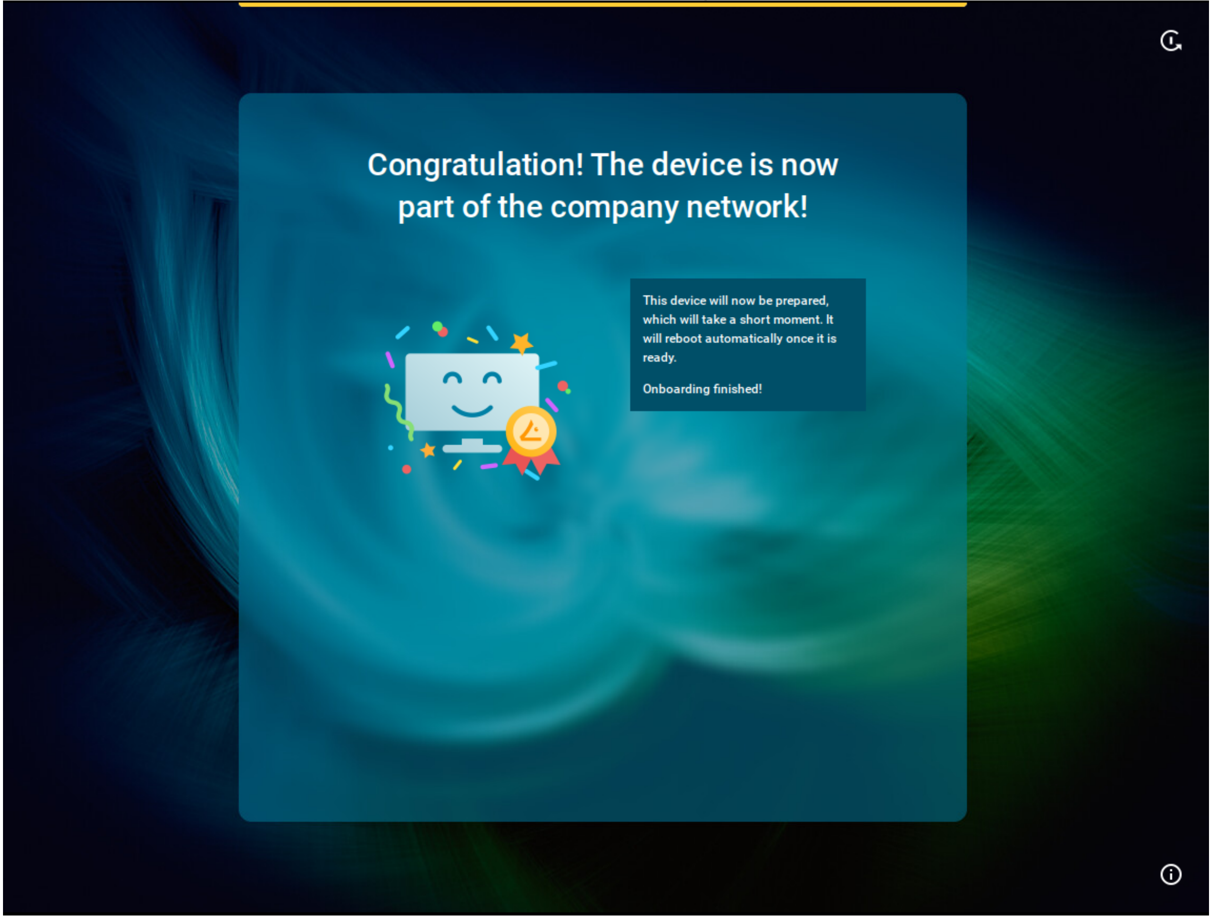
Let's connect to the company network

Provide your company email address to onboard this device:

Email address:

username@company.com

When everything went well, your device will be integrated into your company network after the reboot. This means it has been connected to your IGEL Universal Management Suite (UMS) which provides your device with the appropriate licenses, settings, and IGEL OS Apps.

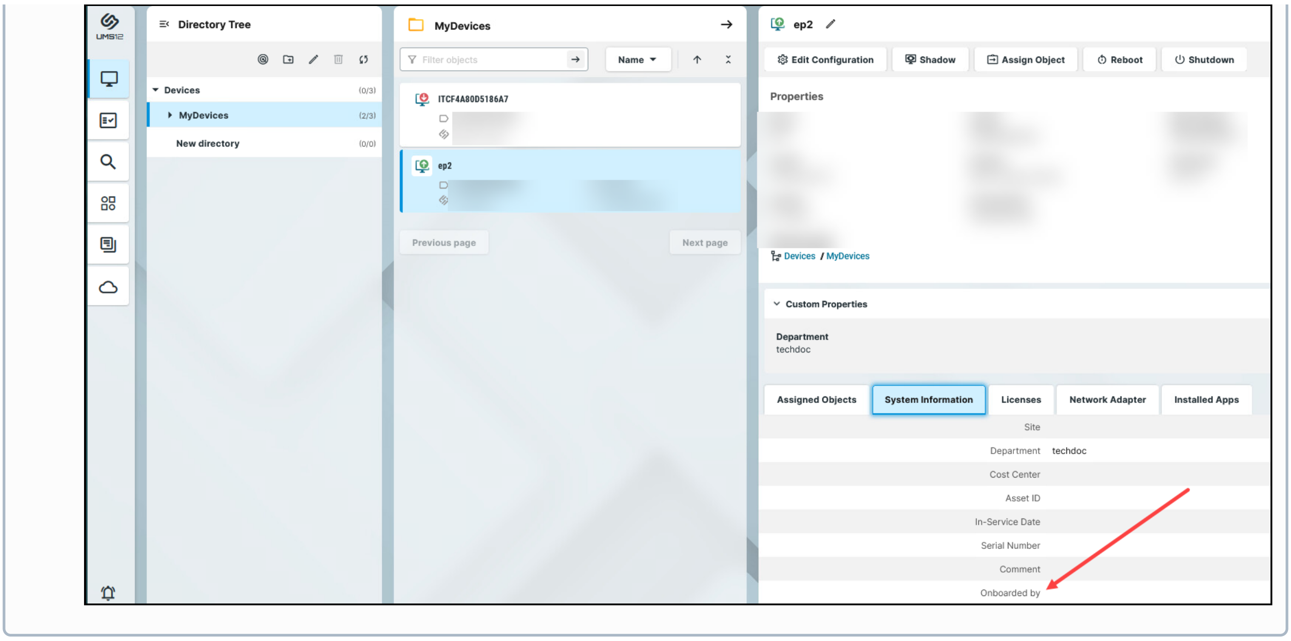


Congratulation! The device is now part of the company network!

This device will now be prepared, which will take a short moment. It will reboot automatically once it is ready.

Onboarding finished!

ⓘ If you need later to check who onboarded the device, you can view this information in the **UMS Web App > Devices > [name of the device] > Properties** / **System Information > Onboarded by**.



Department
techdoc

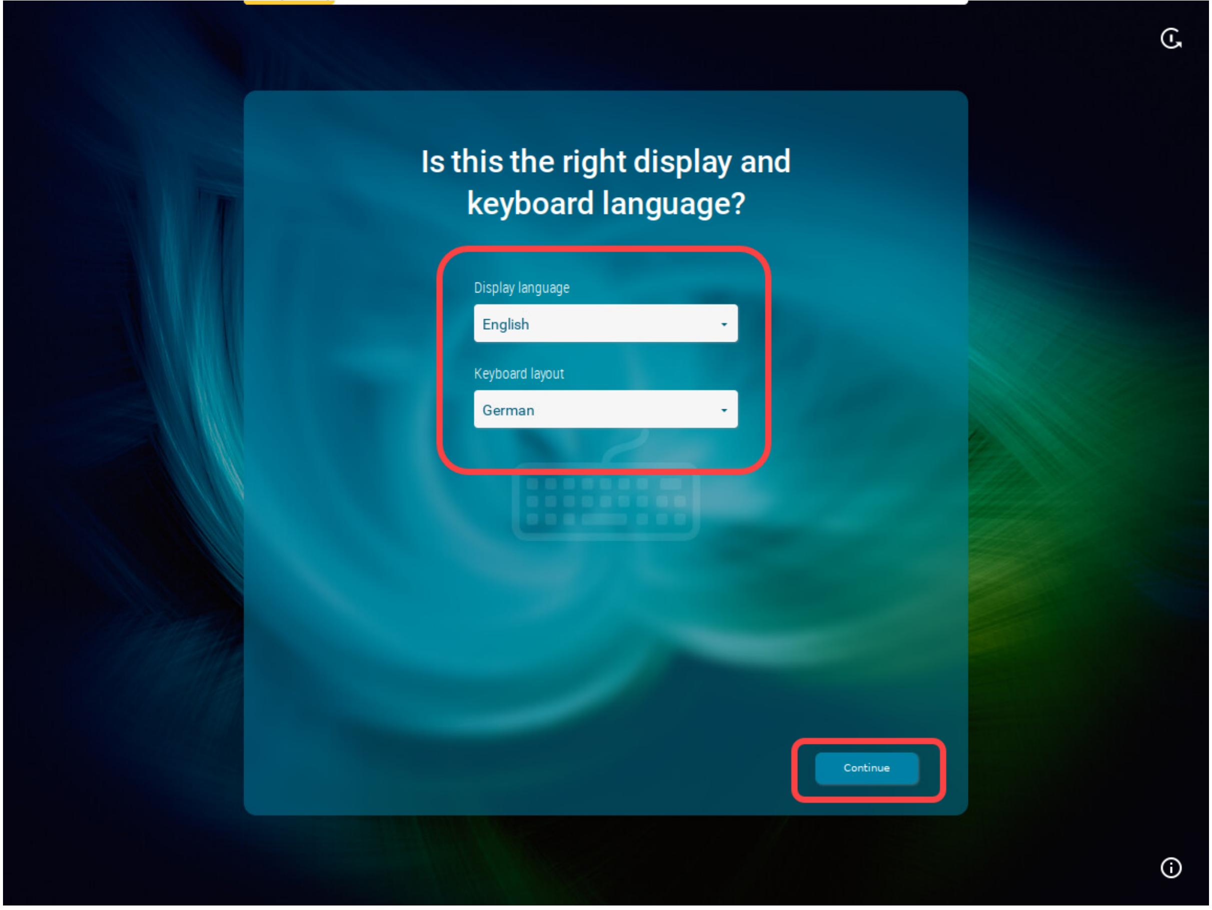
Site	
Department	techdoc
Cost Center	
Asset ID	
In-Service Date	
Serial Number	
Comment	
Onboarded by	

Alternative Onboarding Method: Registering Devices with the UMS Using the One-Time Password

If you decided not to use IGEL Onboarding Service for the registration of your IGEL OS 12 devices, you can use a one-time password method as an alternative.

1. Switch your device on.
   The Setup Assistant starts.

2. Choose the display language and set your keyboard layout. Click **Continue**.

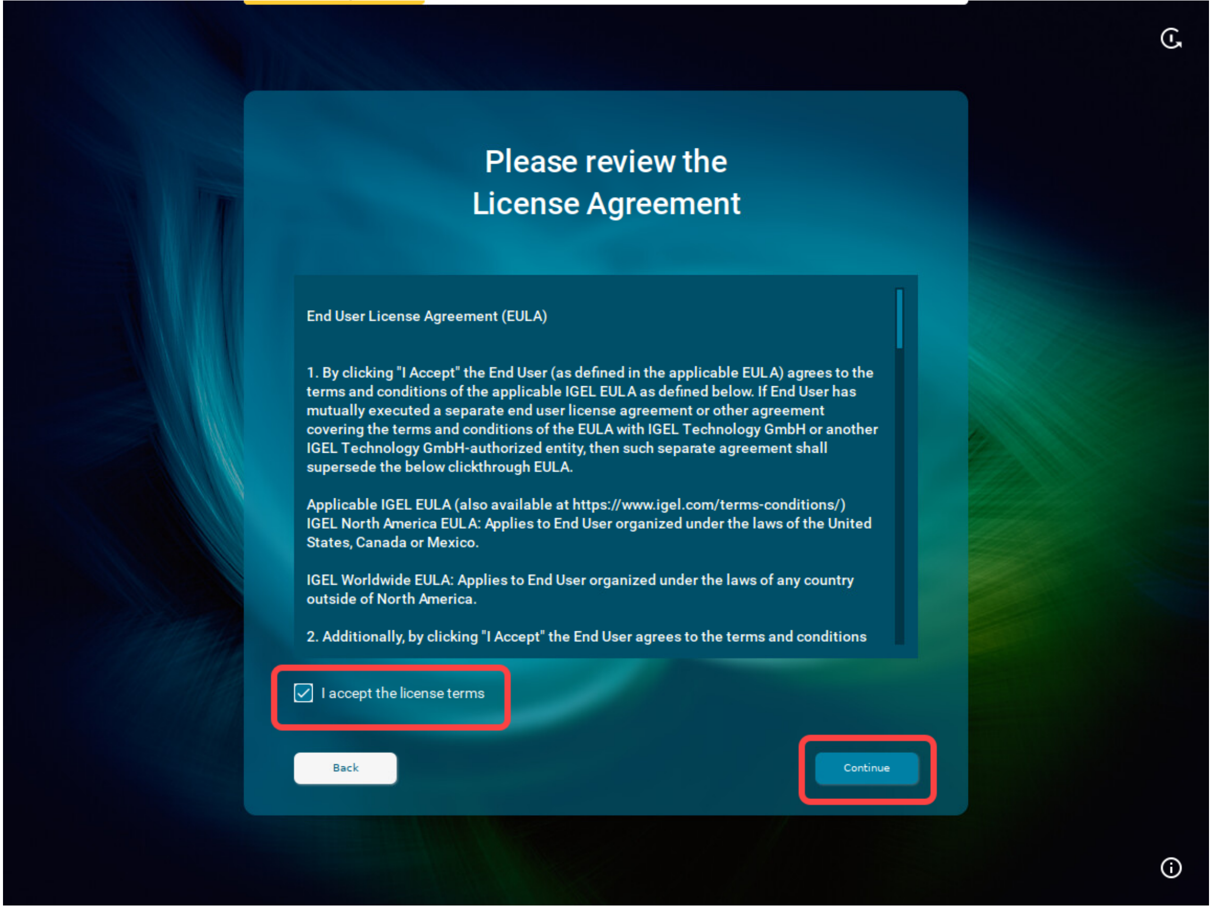


Is this the right display and keyboard language?

Display language: English

Keyboard layout: German

3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.



Please review the License Agreement

End User License Agreement (EULA)

1. By clicking "I Accept" the End User (as defined in the applicable EULA) agrees to the terms and conditions of the applicable IGEL EULA as defined below. If End User has mutually executed a separate end user license agreement or other agreement covering the terms and conditions of the EULA with IGEL Technology GmbH or another IGEL Technology GmbH-authorized entity, then such separate agreement shall supersede the below clickthrough EULA.

Applicable IGEL EULA (also available at https://www.igel.com/terms-conditions/)
IGEL North America EULA: Applies to End User organized under the laws of the United States, Canada or Mexico.

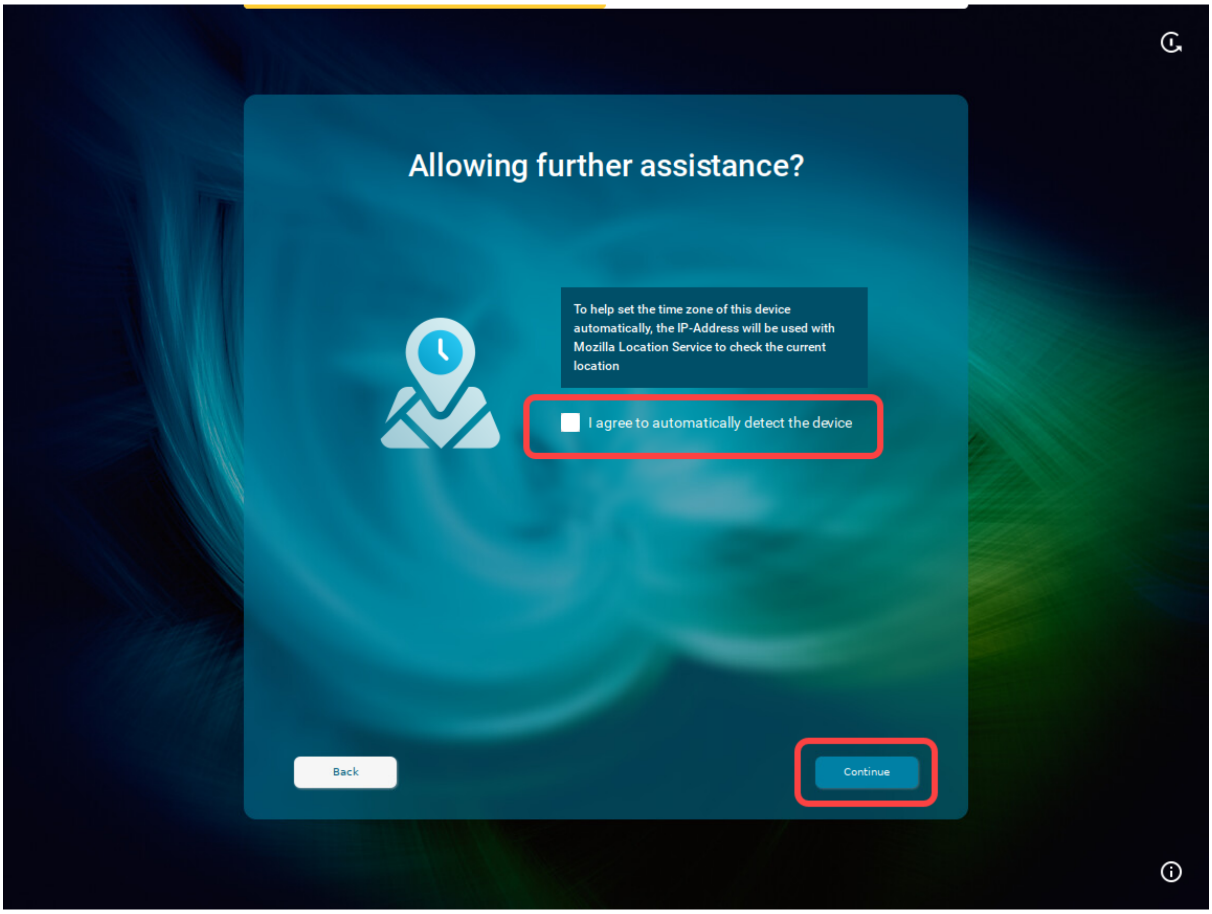
IGEL Worldwide EULA: Applies to End User organized under the laws of any country outside of North America.

2. Additionally, by clicking "I Accept" the End User agrees to the terms and conditions

☑ I accept the license terms

4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under Troubleshooting: Configuring a Network during the Onboarding(see page 175).

5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.

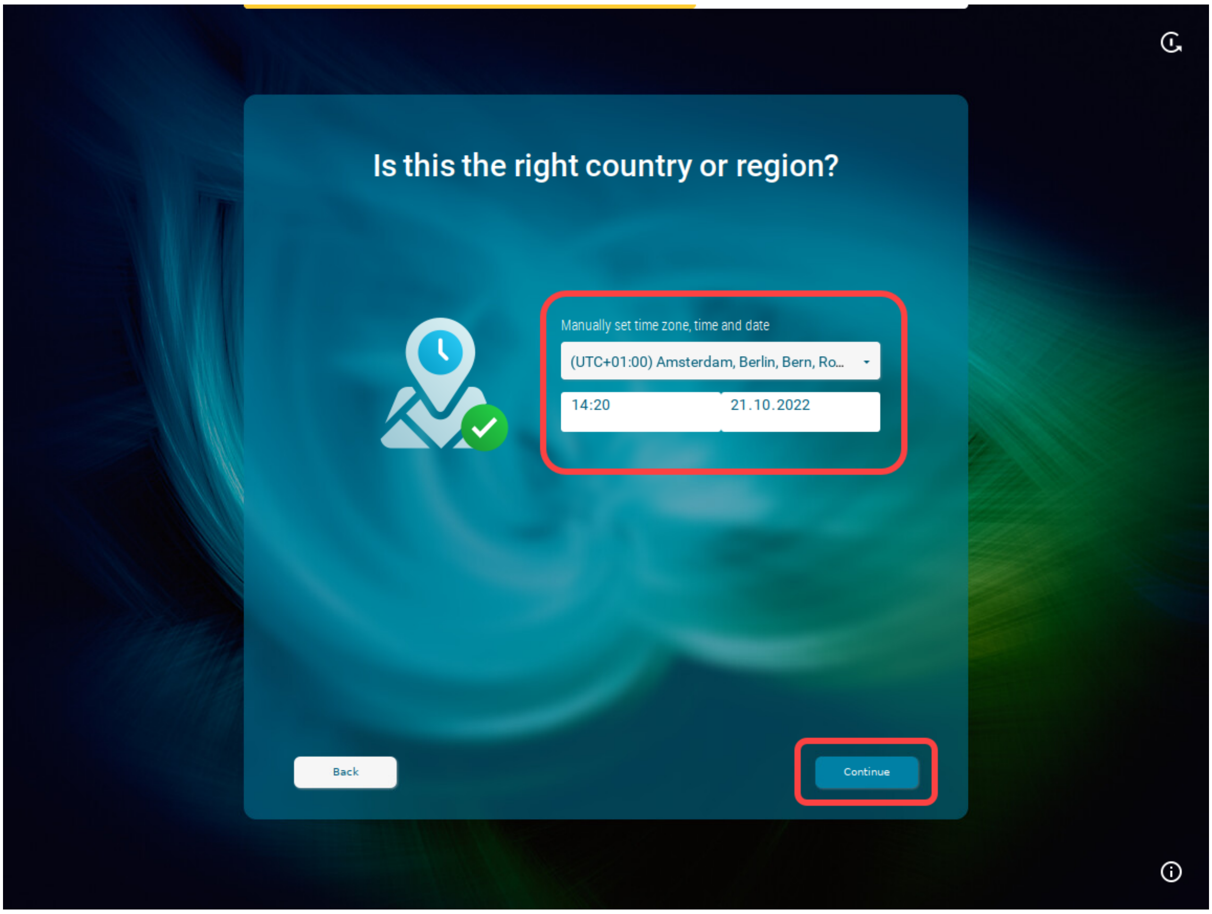


Allowing further assistance?

To help set the time zone of this device automatically, the IP-Address will be used with Mozilla Location Service to check the current location

□ I agree to automatically detect the device

Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.



Is this the right country or region?

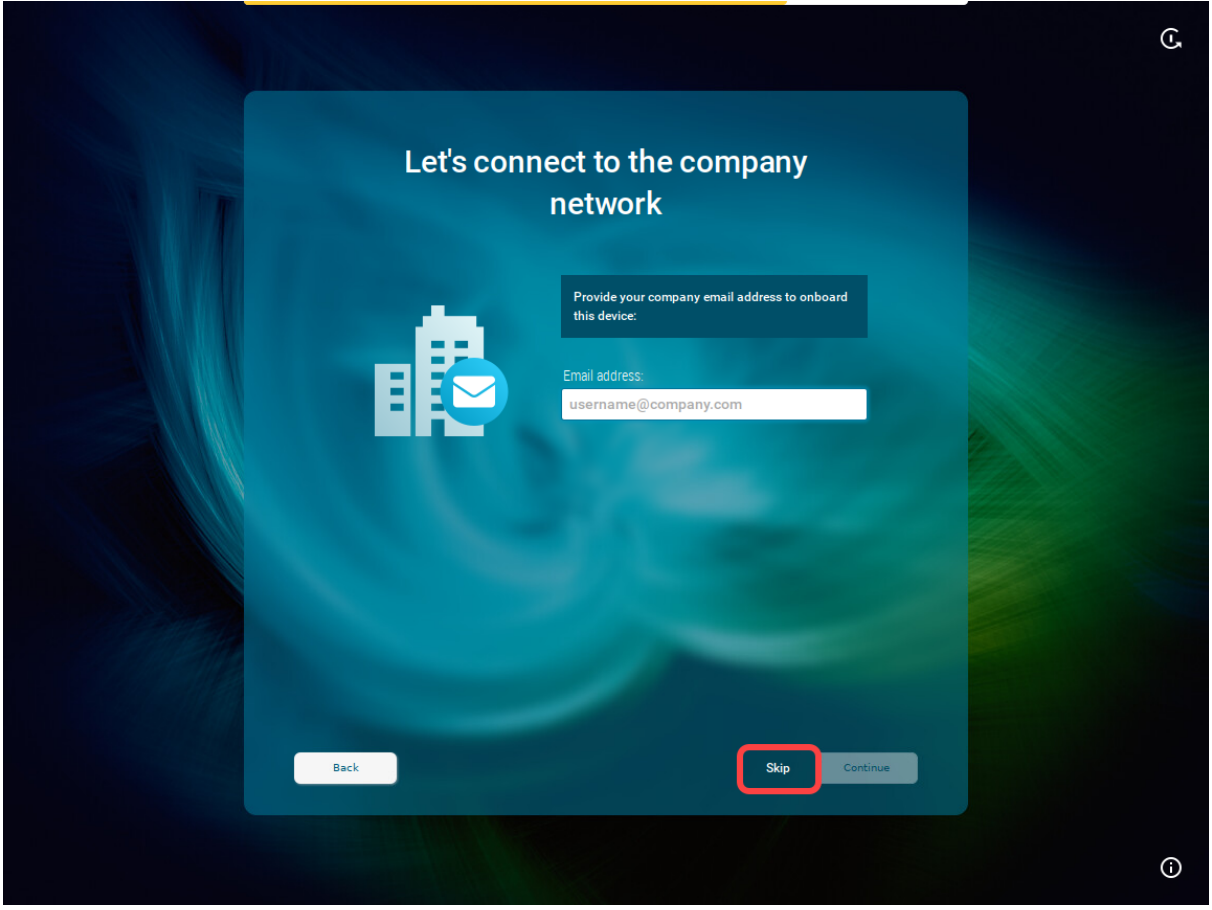
Manually set time zone, time and date

(UTC+01:00) Amsterdam, Berlin, Bern, Ro...

14:20

21.10.2022

6. When the IGEL Setup Assistant asks for your company e-mail, click **Skip**.

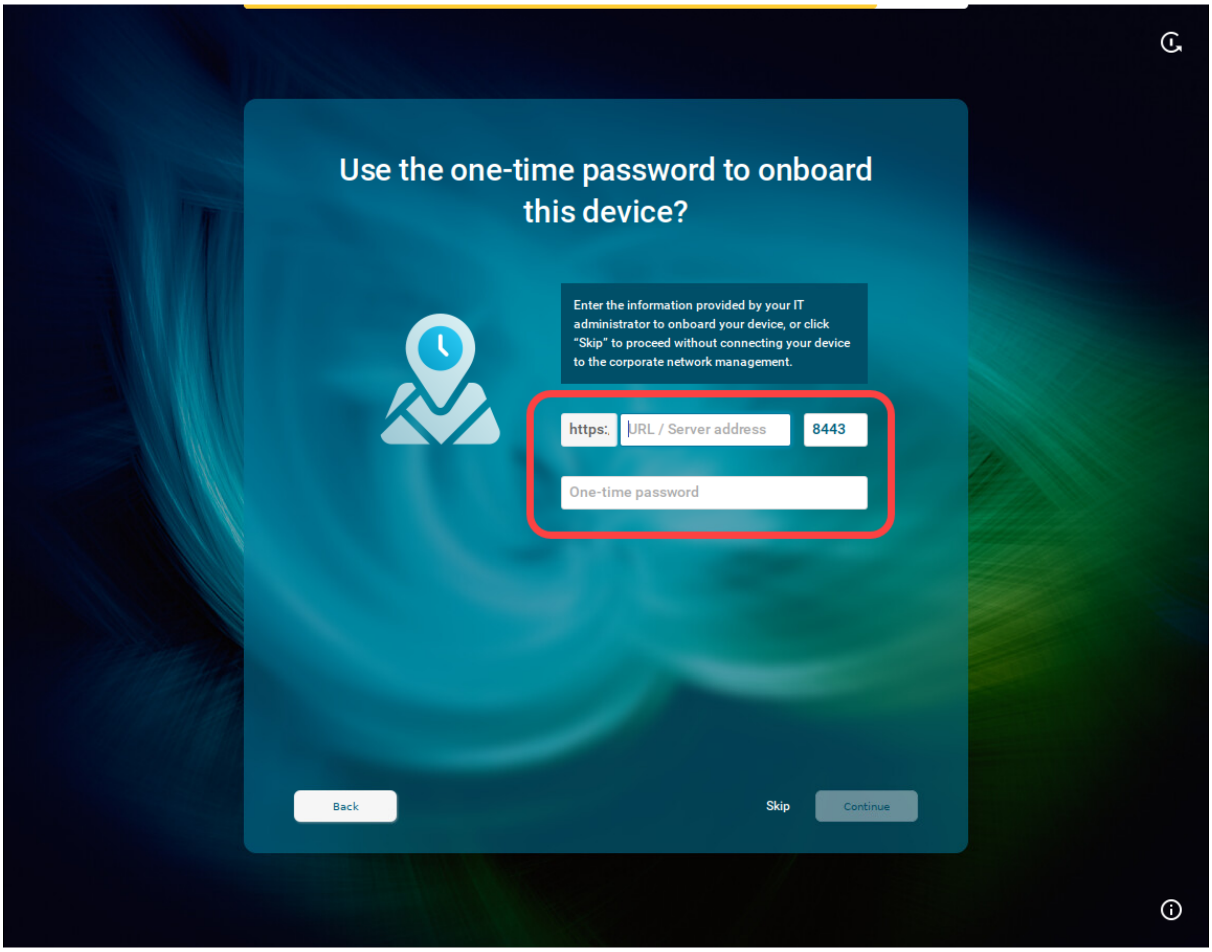


Let's connect to the company network

Provide your company email address to onboard this device:

Email address: username@company.com

You will be asked to enter the data provided by your administrator:



Use the one-time password to onboard this device?

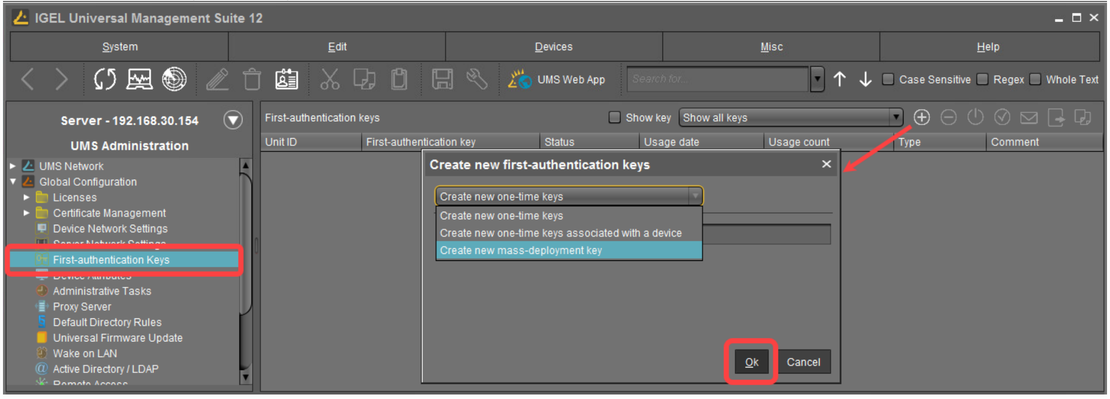
Enter the information provided by your IT administrator to onboard your device, or click "Skip" to proceed without connecting your device to the corporate network management.

7. Enter the following data and click **Continue**:
   URL / Server address: Host name or IP address of the UMS Server. If configured, you can alternatively use the Public Address of the UMS Server or Cluster Address.
   Port: Web server port (Default: 8443). If configured, you can alternatively use the Public Web Port or Cluster Address Port.
   One-time password: First-authentication key (no matter one-time key or mass-deployment key), which you create under **UMS Console > UMS Administration > Global Configuration > First-authentication Keys**.

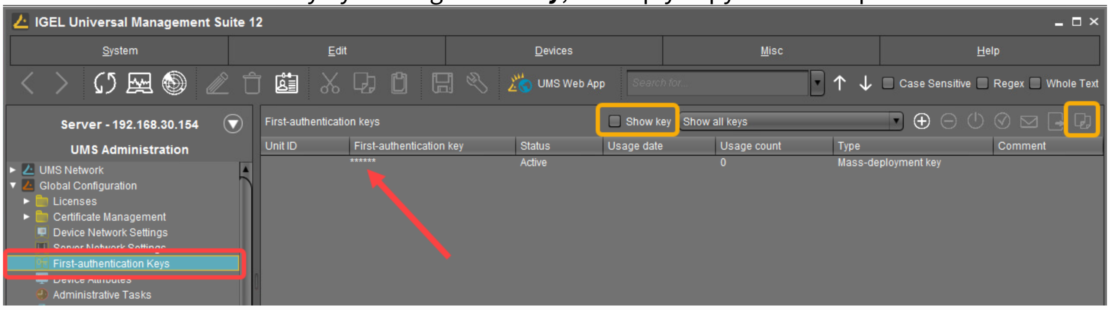
ⓘ **Creating a one-time password in the UMS Console**
You can create the following first-authentication keys:

- One-time keys: Can be used by any random device, but cannot be re-used by any other device. Hence, the number of keys must match the number of devices.
- One-time keys associated with a device: Can only be used by a specific device and will be invalidated after use. Therefore, only devices with the specified UnitIDs will be registered.

- Mass-deployment keys: Multiple-time keys that can be used by any device and will remain valid after use. If you choose to create a mass-deployment key, there is a possibility to set your own password.

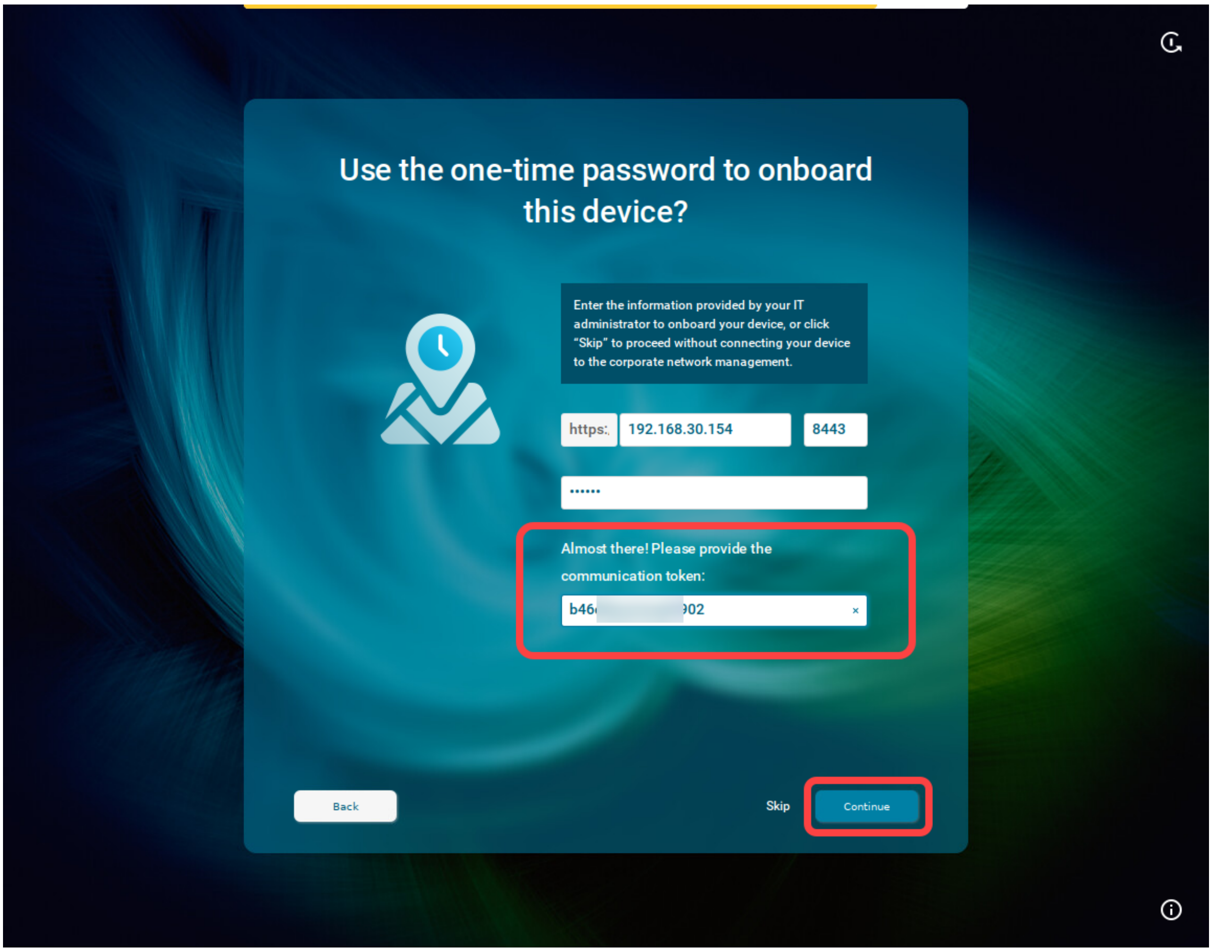


You can view the created key by clicking **Show key**; or simply copy it to the clipboard.



Unit ID	First-authentication key	Status	Usage date	Usage count	Type	Comment
	******	Active		0	Mass-deployment key	

8. In the mask opened, enter the communication token. The communication token is **the third part of the SHA256 fingerprint of the root certificate of your UMS Server**. Then click **Continue**.



Use the one-time password to onboard this device?

Enter the information provided by your IT administrator to onboard your device, or click "Skip" to proceed without connecting your device to the corporate network management.

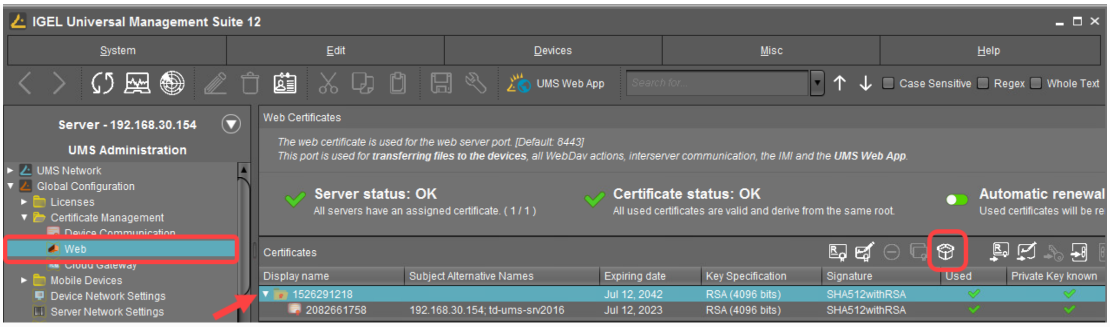
https: 192.168.30.154 8443

••••••

Almost there! Please provide the communication token:

b46[redacted]02

How to Find Out the Communication Token / Root Certificate Fingerprint (SHA256)
Go to **UMS Console > UMS Administration > Global Configuration > Certificate Management > Web**, select the certificate and click .



IGEL Universal Management Suite 12

Web Certificates

The web certificate is used for the web server port. [Default: 8443]
*This port is used for **transferring files to the devices**, all WebDav actions, interserver communication, the IMI and the **UMS Web App**.*

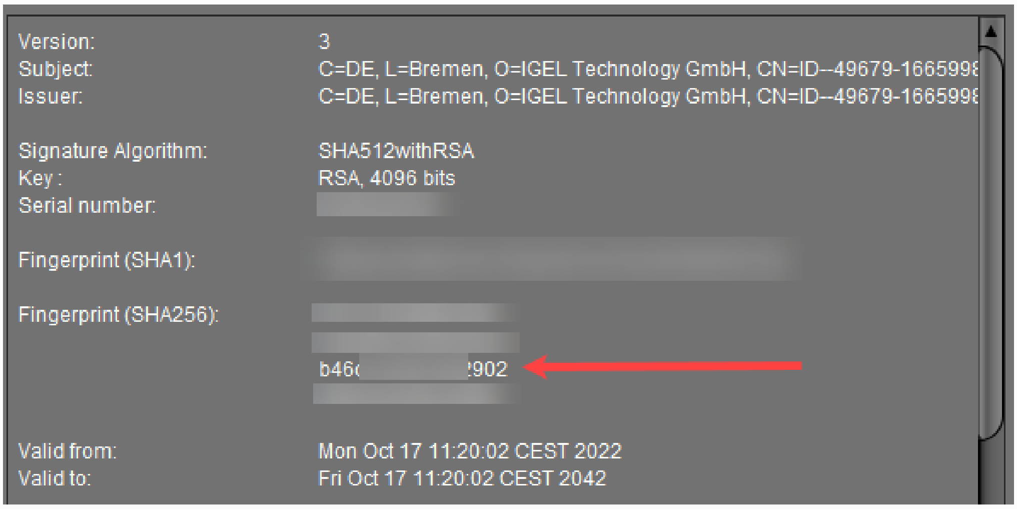
Server status: OK
All servers have an assigned certificate. (1 / 1)

Certificate status: OK
All used certificates are valid and derive from the same root.

Automatic renewal
Used certificates will be re

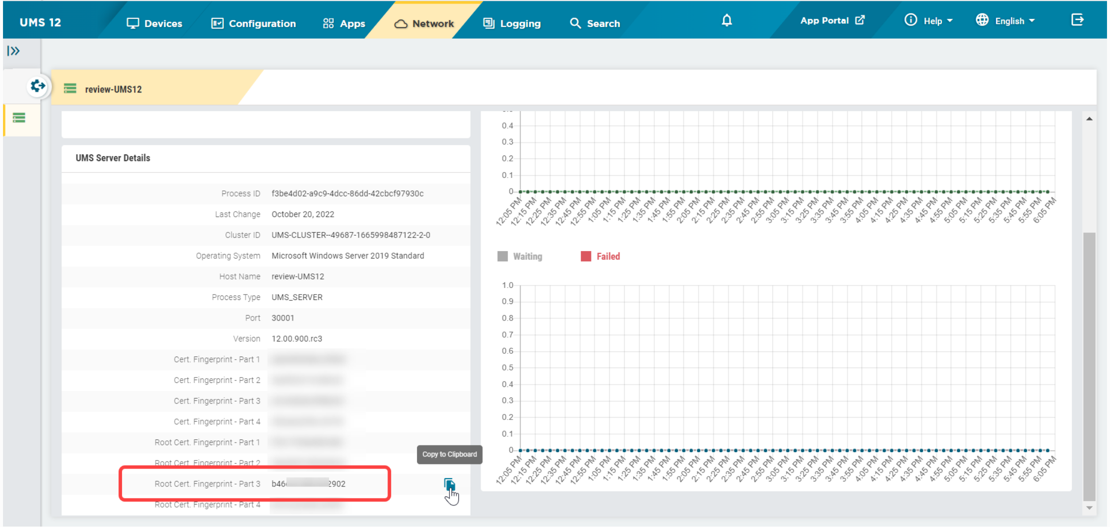
Certificates

Display name	Subject Alternative Names	Expiring date	Key Specification	Signature	Used	Private Key known
1526291218		Jul 12, 2042	RSA (4096 bits)	SHA512withRSA	✓	✓
2082661758	192.168.30.154; td-ums-srv2016	Jul 12, 2023	RSA (4096 bits)	SHA512withRSA	✓	✓



Version:	3
Subject:	C=DE, L=Bremen, O=IGEL Technology GmbH, CN=ID--49679-1665998
Issuer:	C=DE, L=Bremen, O=IGEL Technology GmbH, CN=ID--49679-1665998
Signature Algorithm:	SHA512withRSA
Key :	RSA, 4096 bits
Serial number:	[redacted]
Fingerprint (SHA1):	[redacted]
Fingerprint (SHA256):	[redacted] b46[redacted]902
Valid from:	Mon Oct 17 11:20:02 CEST 2022
Valid to:	Fri Oct 17 11:20:02 CEST 2042

Alternatively, go to **UMS Web App > Network > UMS Server Details** and copy **Root Cert. Fingerprint - Part 3**.

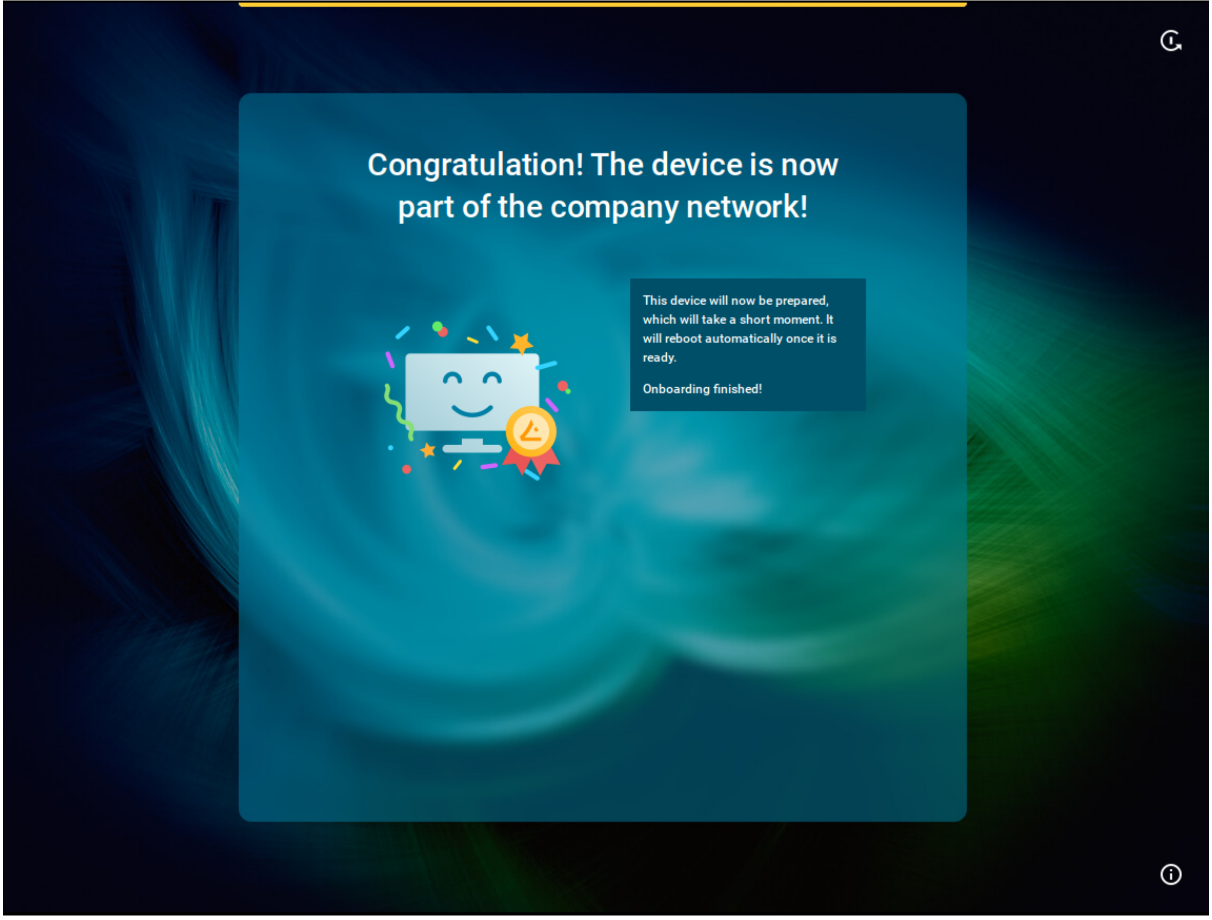


UMS Server Details

Process ID	f3be4d02-a9c9-4dcc-86dd-42cbcf97930c
Last Change	October 20, 2022
Cluster ID	UMS-CLUSTER--49687-1665998487122-2-0
Operating System	Microsoft Windows Server 2019 Standard
Host Name	review-UMS12
Process Type	UMS_SERVER
Port	30001
Version	12.00.900.rc3
Cert. Fingerprint - Part 1	[redacted]
Cert. Fingerprint - Part 2	[redacted]
Cert. Fingerprint - Part 3	[redacted]
Cert. Fingerprint - Part 4	[redacted]
Root Cert. Fingerprint - Part 1	[redacted]
Root Cert. Fingerprint - Part 2	[redacted]
Root Cert. Fingerprint - Part 3	b46[redacted]2902
Root Cert. Fingerprint - Part 4	[redacted]

If You Use IGEL Cloud Gateway
If you want to connect the device via the IGEL Cloud Gateway (ICG), use the following as credentials under steps 7 and 8:
URL / Server address: Host name or IP address of the ICG server
Port: ICG port (Default: 8443)
One-time password: First-authentication key created as described above. You may find it also interesting to read Generating and Distributing First-Authentication Keys for Devices.
Communication token: Fingerprint of the root certificate of the ICG server (the third part)

When everything went well, your device will be integrated into your company network after the reboot. This means it has been connected to your IGEL Universal Management Suite (UMS) which provides your device with the appropriate licenses, settings, and IGEL OS Apps.



Congratulation! The device is now part of the company network!

This device will now be prepared, which will take a short moment. It will reboot automatically once it is ready.

Onboarding finished!

Troubleshooting: Configuring a Network during the Onboarding

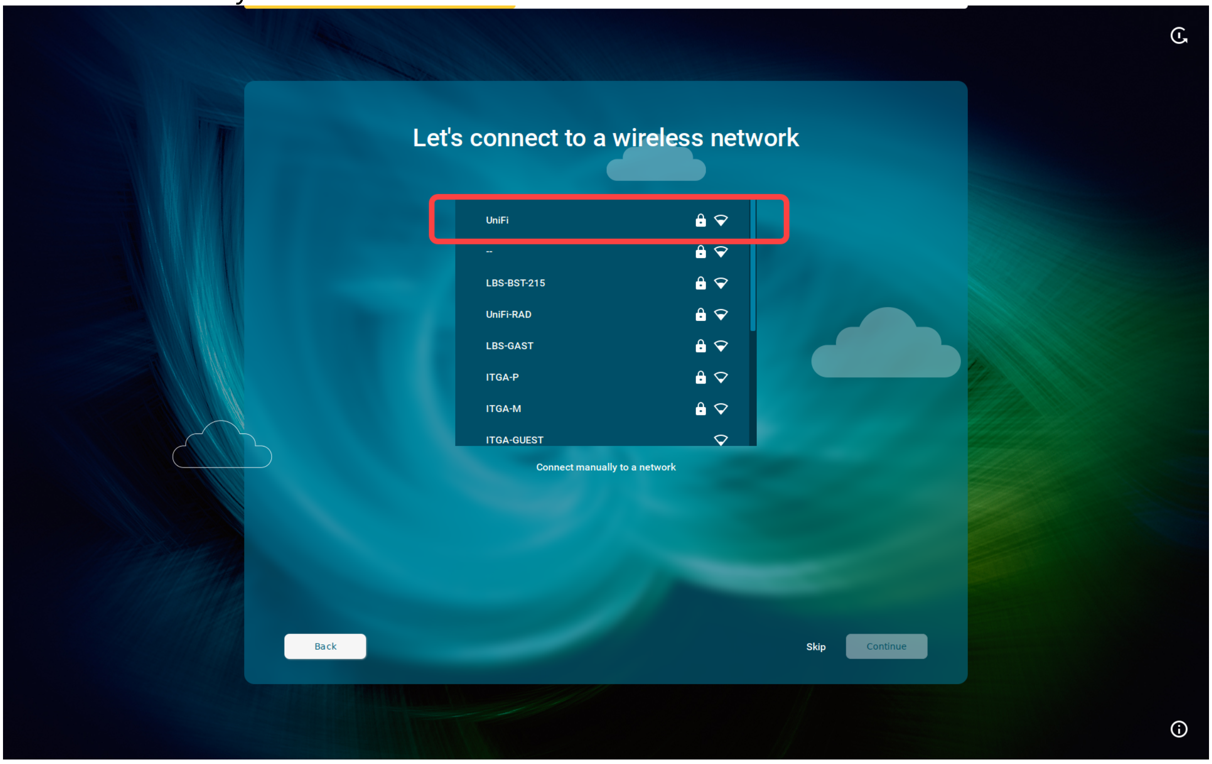
If your device cannot connect to the network instantly, the IGEL Setup Assistant will ask you to configure your network connection.

Connecting to a Wireless Network That Is Visible

ⓘ Wi-Fi networks with certificates are not supported in the Setup Assistant.

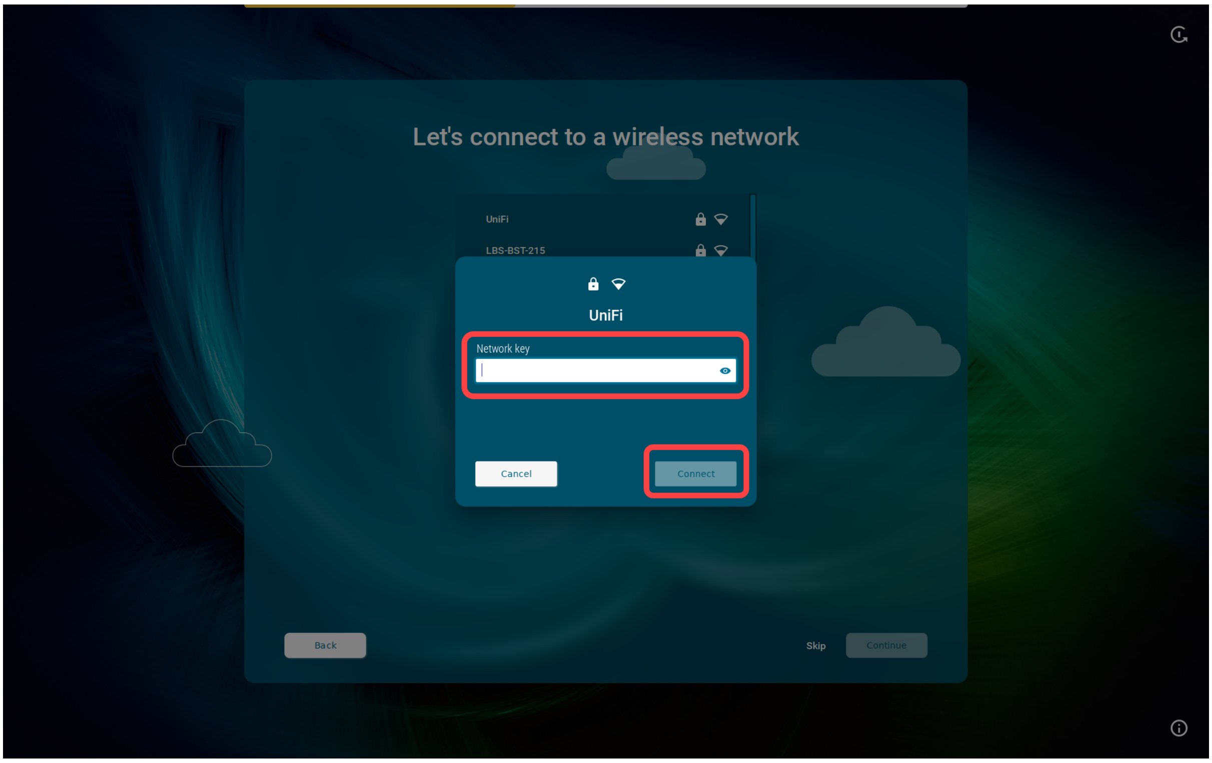
This configuration step is available if a WLAN adapter was found when starting the device. The device will search for available WLAN access points as soon as the configuration step is opened. The WLAN access points found will be listed.

1. Select the network you want to connect to.



Let's connect to a wireless network

2. Enter the authentication data that are required by your network, e.g. **Network key** or **Password** and **Username**.



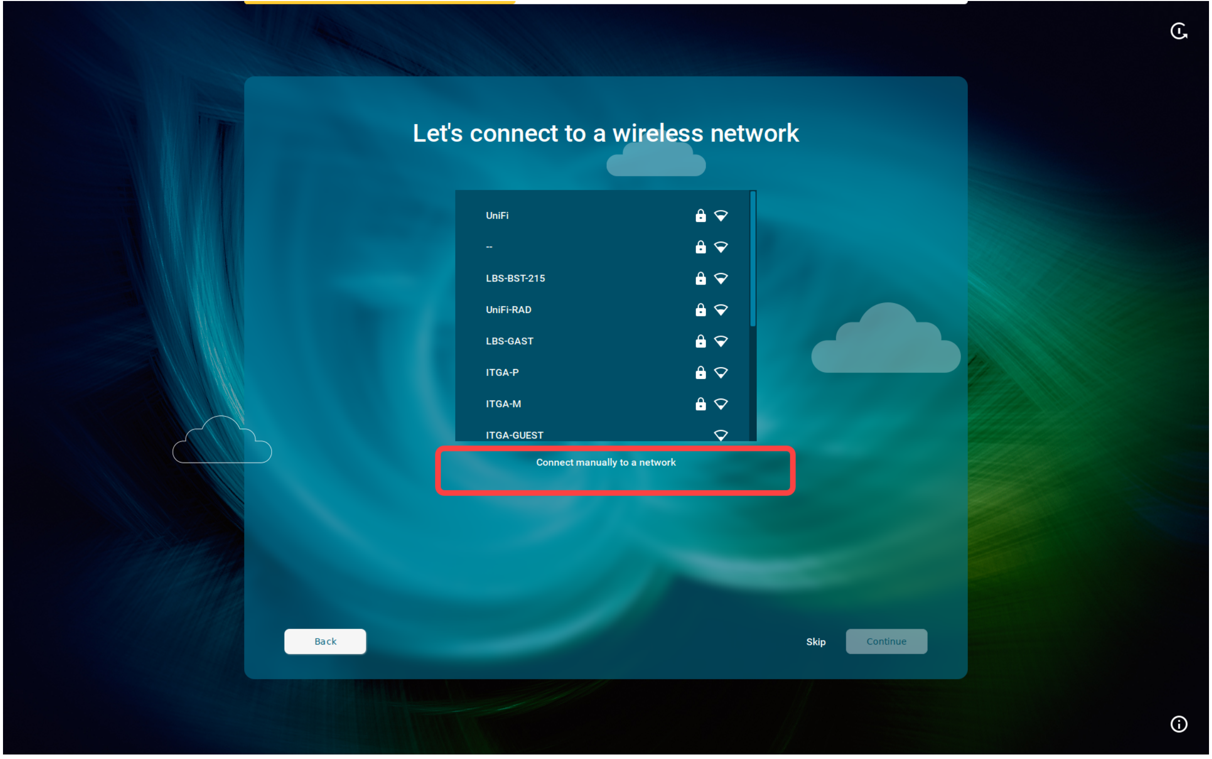
3. Click **Connect**.

ⓘ If no Wi-Fi adapter is found, please check if:

- There is a hardware switch on your device.
- There is a BIOS setting that disables Wi-Fi if Ethernet is connected.
- There is a BIOS update for your endpoint.

Connecting to a Wireless Network That Is Hidden

1. Click **Connect manually to a network**.

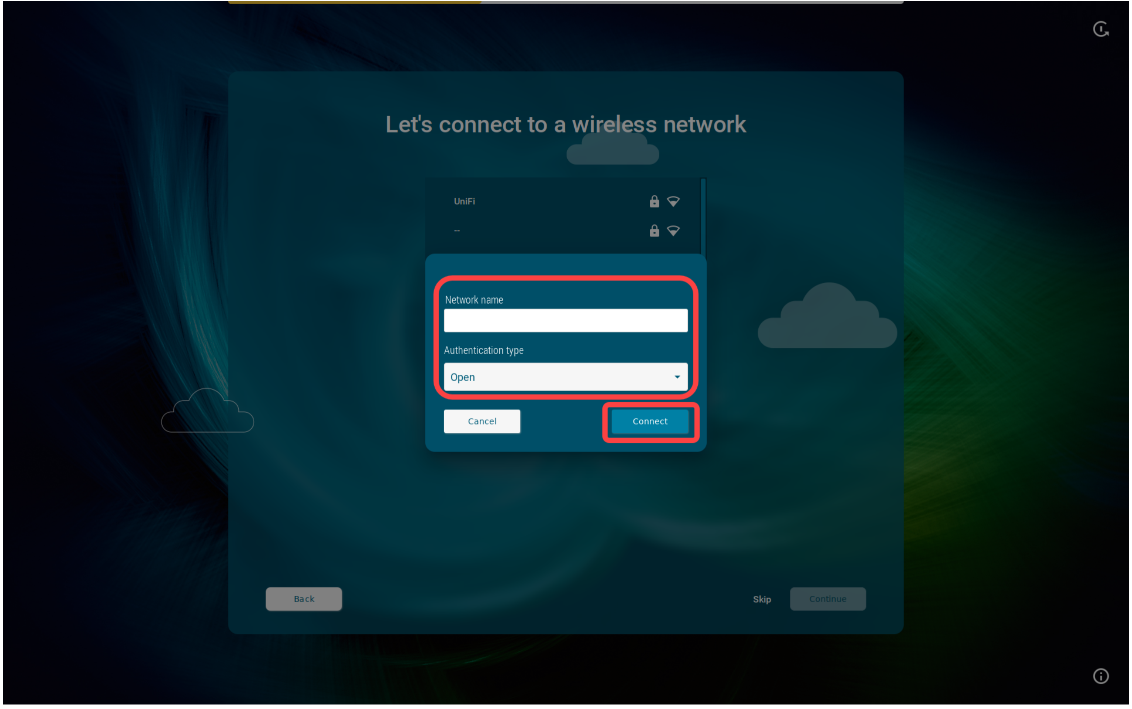


Let's connect to a wireless network

UniFi
--
LBS-BST-215
UniFi-RAD
LBS-GAST
ITGA-P
ITGA-M
ITGA-GUEST

2. Select the **Authentication type** and enter the required authentication data.
   Possible options:
   - **Open**: Enter the **Network name**.
   - **Security key**: Enter the **Network name** and the **Security key**.

- **Username and password**: Enter the **Network name**, **Username**, and the **Security key**.

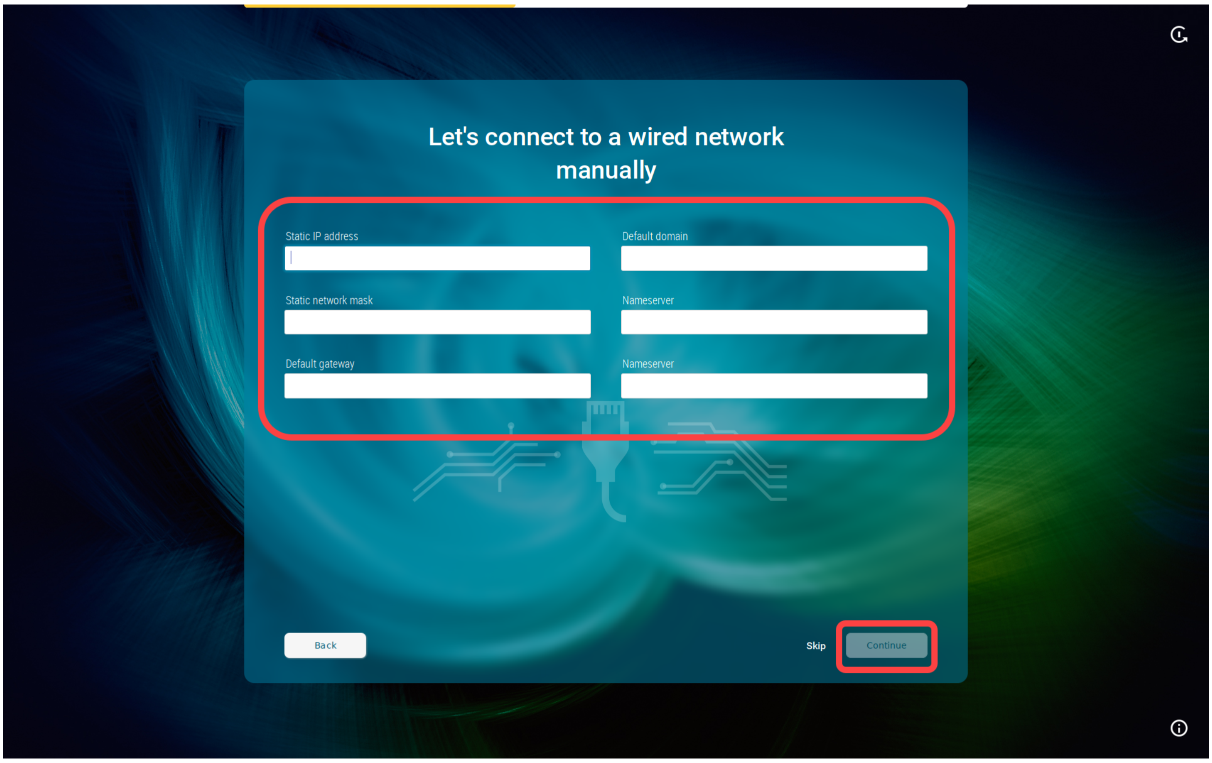


3. Click **Connect**.

Advanced Wired Network Configuration

This configuration step is available if a wired network has been detected, but the connection to the LAN could not be established automatically (e.g. because the IP address could not be automatically received from the DHCP server for some reason).

1. Enter the appropriate settings for your wired network:
   Static IP address: Static IP address of the device
   Static network mask: Static network mask of the device
   Default gateway: IP address of the default gateway
   AND/OR
   Default domain: Usually the name of the local network
   Name server: IP address of the name server to be used
   Name server: IP address of an alternative name server



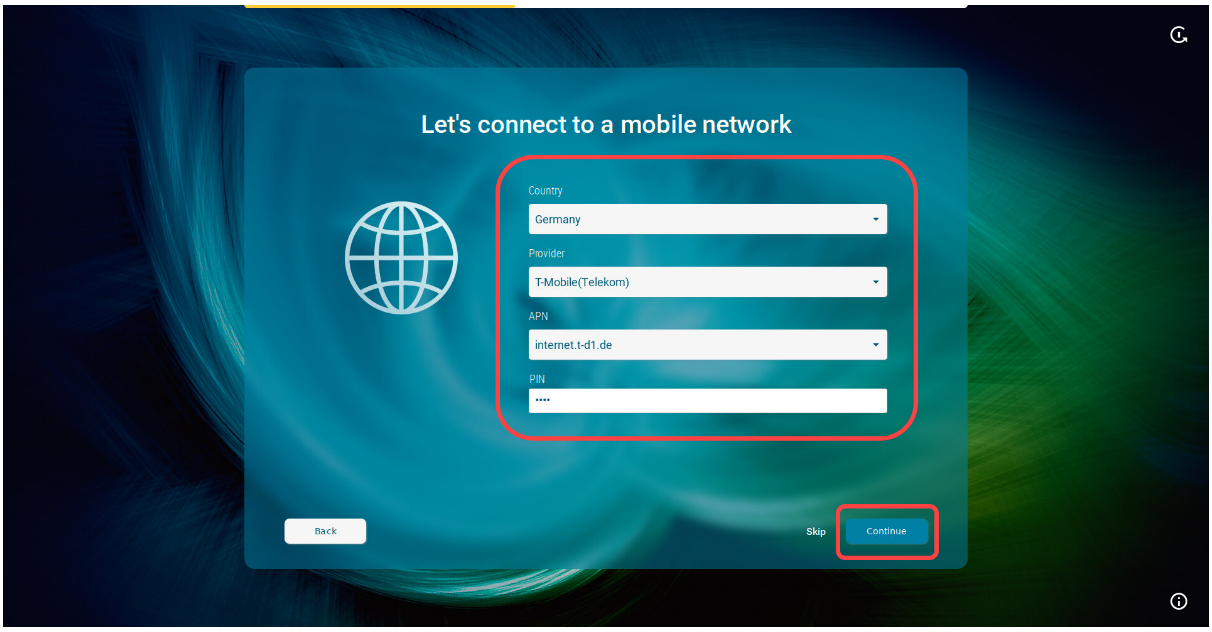
2. Click **Continue**.

Mobile Broadband

This configuration step is available if there is no LAN or wi-fi connection, but a surf stick / modem has been detected. If not detected, reboot your endpoint device.

1. Enter the required data:
   Country or region: The country or region of your provider
   Provider: Provider (the possible options depend on what you choose for **Country or region**)
   APN: Access point name (the possible options depend on what you choose for **Provider**)
   PIN (displayed if the SIM card is locked): PIN for the SIM card used

2. Click **Continue**.



Let's connect to a mobile network

Country: Germany

Provider: T-Mobile(Telekom)

APN: internet.t-d1.de

PIN: ····

Troubleshooting: Possible Error Codes During the Onboarding

During the onboarding with the IGEL Onboarding Service or with the one-time password method, the following internal errors may occur.

Error message: " `Could not manage your device because of an internal error (<error-code>)` "

Error Code	Meaning
30	Onboarding service not reachable anymore
32	Invalid arguments
33	Failed to initialize EST API
34	Failed to load trust chain
35	Failed to load key pair
36	Failed to load private key
37	Failed to get CA certificates from server
38	Failed to enroll a certificate from server For information on the solution, see Troubleshooting: Error 38 during the Onboarding of an IGEL OS 12 Device(see page 183).

Error Code	Meaning
39	Failed to retrieve the enrolled certificate
40	Failed to convert the enrolled certificate to PEM
41	Failed to save the enrolled certificate
42	Failed to create a TLS context
43	Failed to create a TLS handle
44	Failed to establish a TCP connection
45	Failed to establish a TLS connection
46	Failed to verify TLS certificate chain
47	Failed to load system trust store

ⓘ If you have checked your configuration and everything seems to be correct, collect the log files as described under Debugging / How to Collect and Send Device Log Files to IGEL Support(see page 200) and contact IGEL Support.

Troubleshooting: Error 38 during the Onboarding of an IGEL OS 12 Device

During the onboarding with the IGEL Onboarding Service or with the one-time password method, you get the following error message: "`Could not manage your device because of an internal error (<38>)`". Error 38 indicates that the device was unable to register the certificate from the UMS Server(s).

Problem

Possible causes for error 38 may be:

1. The device already exists on the UMS Server.
   Typical use case: the device was once registered in the UMS, but was deleted, but not permanently, and remained in the UMS in the recycle bin.
2. Uncommon FQDN of the UMS Server
3. The Public Address is not resolvable by the endpoint devices, or it is not set, and the devices cannot resolve the internal address.
4. Multiple UMS Servers are behind a single external address / load balancer.

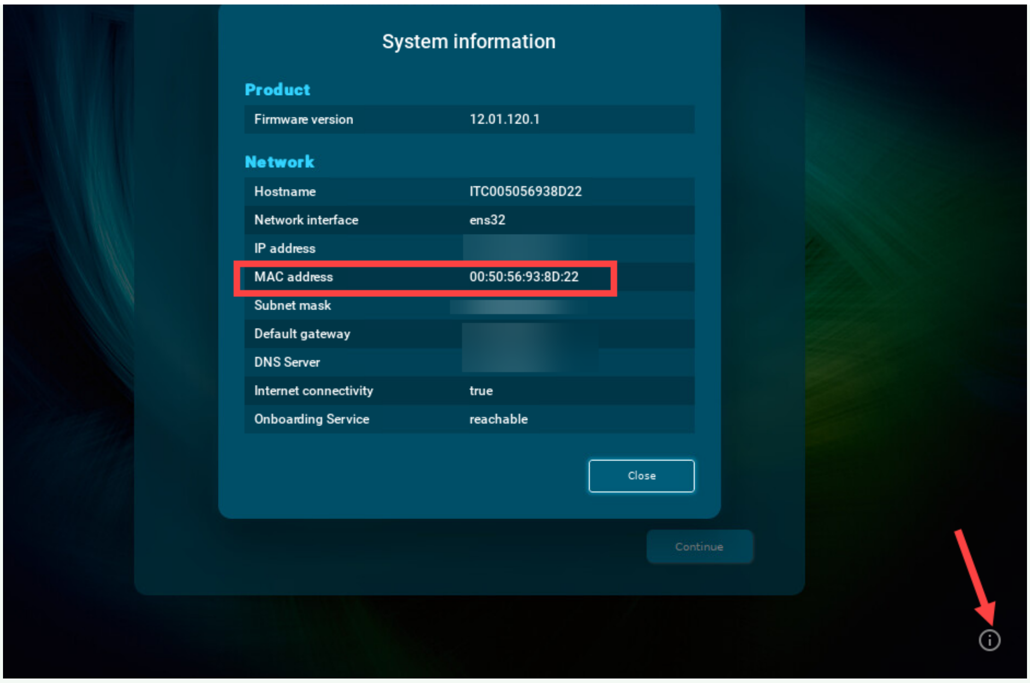
Solution

The Device Already Exists on the UMS Server

If you get error 38 during the device onboarding, the first thing to check is if the device has already been registered on the UMS Server. To do this, we will find out the current Unit ID of the device, search for it in the UMS, and will remove the device from the UMS:

1. To find out the Unit ID of the device:
   - If you are still in the IGEL Setup Assistant: Press anytime `[CTRL+ALT+F12]` or `[CTRL+ALT+F11]` to enter the command line interface (CLI) and then press `[Enter]` to log in as root.
   - If you skipped all steps in the IGEL Setup Assistant and started the device with a Starter license: In the **IGEL Setup > Accessories > Terminals**, add a terminal session and log in to the local terminal as root (by default, the password is empty on new devices).

     Tip
     Alternatively, you can simply open the information dialog in the IGEL Setup Assistant and note the **MAC address** of the device and search for it in the UMS Console as described below:



System information

Product

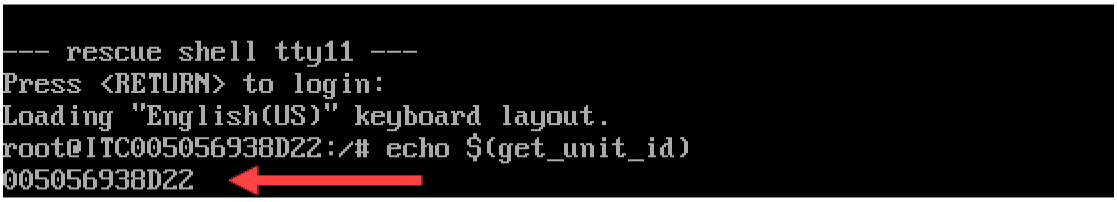
Firmware version	12.01.120.1

Network

Hostname	ITC005056938D22
Network interface	ens32
IP address	
MAC address	00:50:56:93:8D:22
Subnet mask	
Default gateway	
DNS Server	
Internet connectivity	true
Onboarding Service	reachable

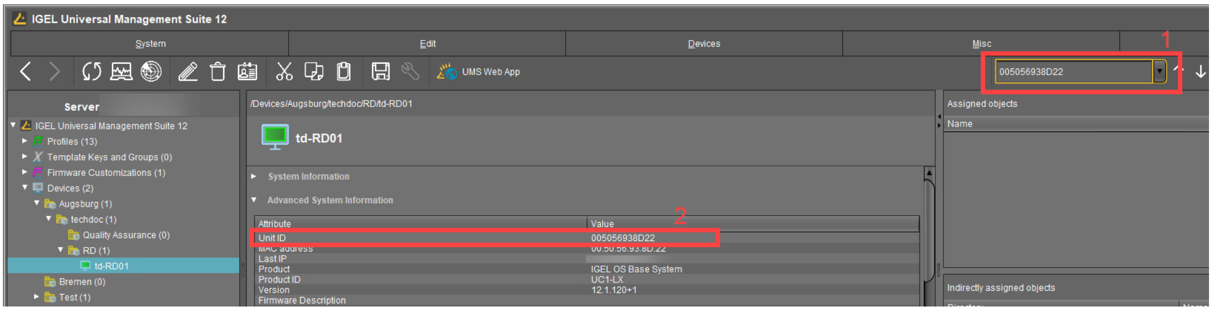
2. Execute the following command:
   `echo $(get_unit_id)`

   This returns the Unit ID of the device:



```
--- rescue shell tty11 ---
Press <RETURN> to login:
Loading "English(US)" keyboard layout.
root@ITC005056938D22:/# echo $(get_unit_id)
005056938D22
```

3. Enter the Unit ID in the **Search** field, press `[Enter]` and validate that the located device has the correct Unit ID.

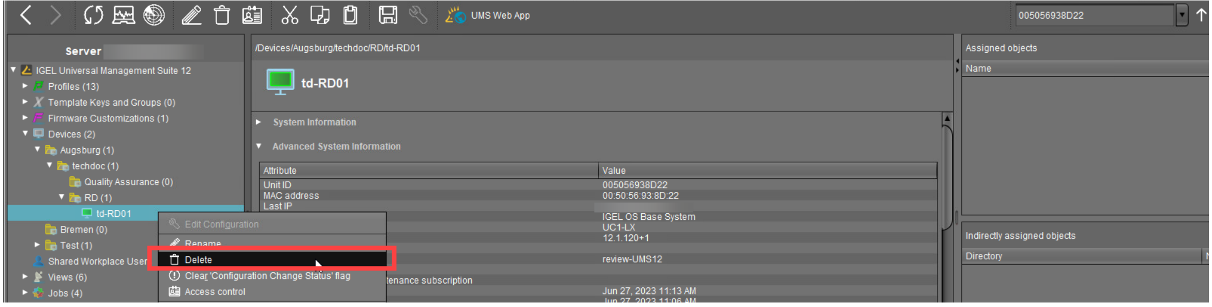


IGEL Universal Management Suite 12
System
Edit
Devices
Misc
UMS Web App
005056938D22
1
2
Server
IGEL Universal Management Suite 12
Profiles (13)
Template Keys and Groups (0)
Firmware Customizations (1)
Devices (2)
Augsburg (1)
techdoc (1)
Quality Assurance (0)
RD (1)
td-RD01
Bremen (0)
Test (1)
/Devices/Augsburg/techdoc/RD/td-RD01
td-RD01
System Information
Advanced System Information
Assigned objects
Name
Indirectly assigned objects

Attribute	Value
Unit ID	005056938D22
MAC address	00:50:56:93:8D:22
Last IP	
Product	IGEL OS Base System
Product ID	UC1-LX
Version	12.1.120+1
Firmware Description	

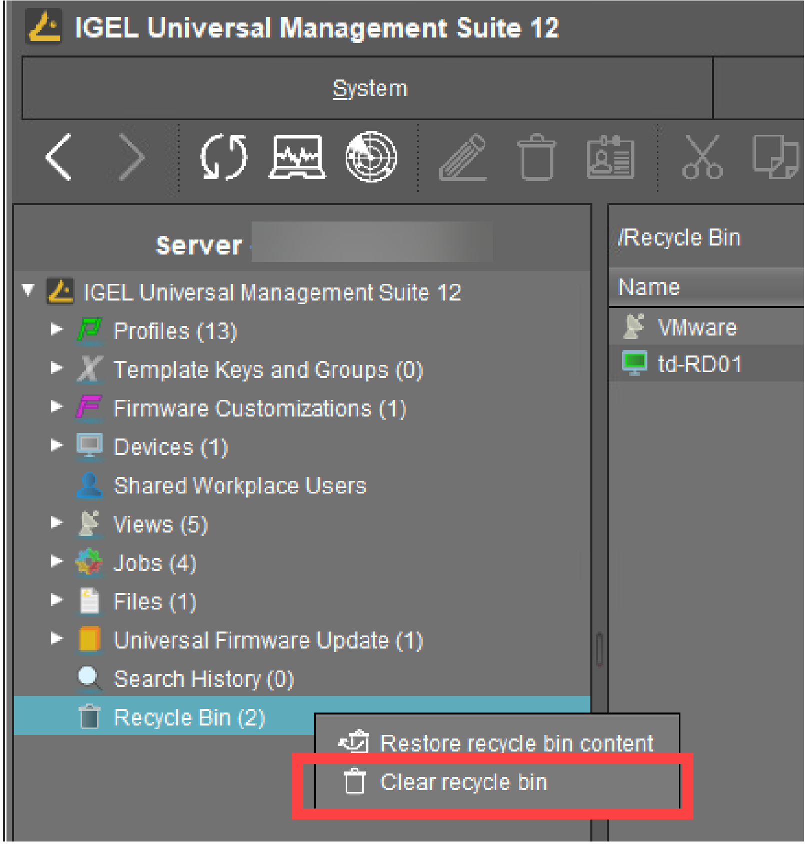
If the device does not show up when running this search, skip the next step and go to the **Recycle Bin**.

4. Right-click the device, select **Delete** and confirm the deletion.
   The device will be moved to the recycle bin. See Recycle Bin - Deleting Objects in the IGEL UMS.



Attribute	Value
Unit ID	005056938D22
MAC address	00:50:56:93:8D:22
Last IP	
	IGEL OS Base System
	UC1-LX
	12.1.120+1
	review-UMS12
	Jun 27, 2023 11:13 AM

5. Verify that you do not need any items in the recycle bin and click **Clear recycle bin**.


IGEL Universal Management Suite 12
System
Server
IGEL Universal Management Suite 12
Profiles (13)
Template Keys and Groups (0)
Firmware Customizations (1)
Devices (1)
Shared Workplace Users
Views (5)
Jobs (4)
Files (1)
Universal Firmware Update (1)
Search History (0)
Recycle Bin (2)
Restore recycle bin content
Clear recycle bin
/Recycle Bin
Name
VMware
td-RD01

Now, when the device was permanently removed from the UMS, you can repeat the onboarding procedure.

Checking Host Names, FQDNs, and Public Address of the UMS Server

Having incorrect host or public names defined in the UMS can cause issues with devices identifying the UMS and installing the UMS certificates properly, thus resulting in error 38 during the device onboarding.

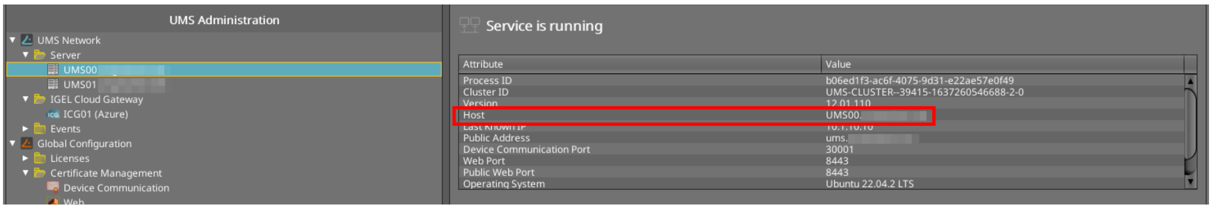
> ⓘ Please pay attention that hostnames should be spelled everywhere the same way (case-sensitive). The UMS hostname specified during the configuration of the IGEL Onboarding Service(see page 41) must be written exactly as in the UMS.

The hostname of the UMS must match the DNS name or SAN name for your UMS web certificate.

> ⓘ The best practice is to use the common / routable FQDN and not the automatically generated name for the hostname. It is generally recommended to check for hostname oddities. For example, such names as `ums00.dci3rsbtfpeunizc5g5gghfhwg.ux.internal.cloudapp.net` are common for cloud-hosted servers and generated automatically when creating a VM, e.g. in Azure – they should be renamed to simpler FQDNs such as `ums00.igel-demo.com`.
> Note that the maximal length of the FQDN is restricted to 255 characters.

If the hostnames do not meet these requirements, you need to update them:

1. To identify and check your UMS hostname, go to **UMS Console > UMS Administration > UMS Network > Server** and select each server to view their details.



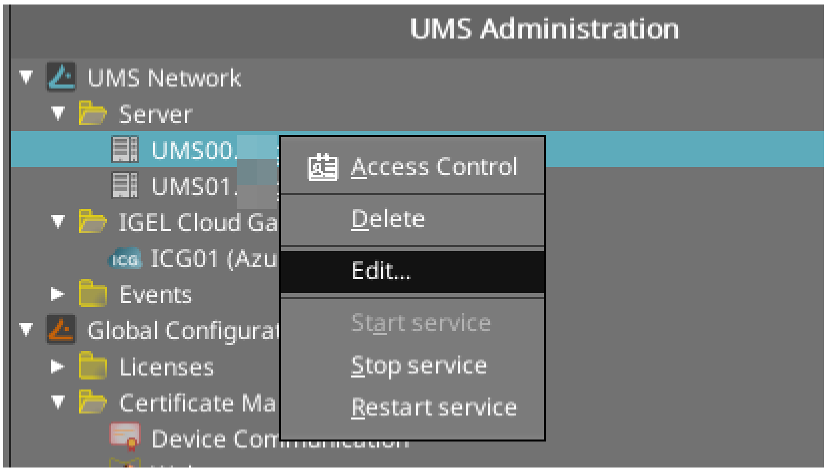
Service is running

Attribute	Value
Process ID	b06ed1f3-ac6f-4075-9d31-e22ae57e0f49
Cluster ID	UMS-CLUSTER--39415-1637260546688-2-0
Version	12.01.110
Host	UMS00.[redacted]
Last Known IP	10.1.10.10
Public Address	ums.[redacted]
Device Communication Port	30001
Web Port	8443
Public Web Port	8443
Operating System	Ubuntu 22.04.2 LTS

2. Change the hostname:
   - via your operating system
     The proper way is to update the hostname of the UMS Server itself. To do this, simply follow your OS vendor's instructions for changing the hostname, and then reboot the server. After that, you should see the changes reflected in the UMS (see step 1).

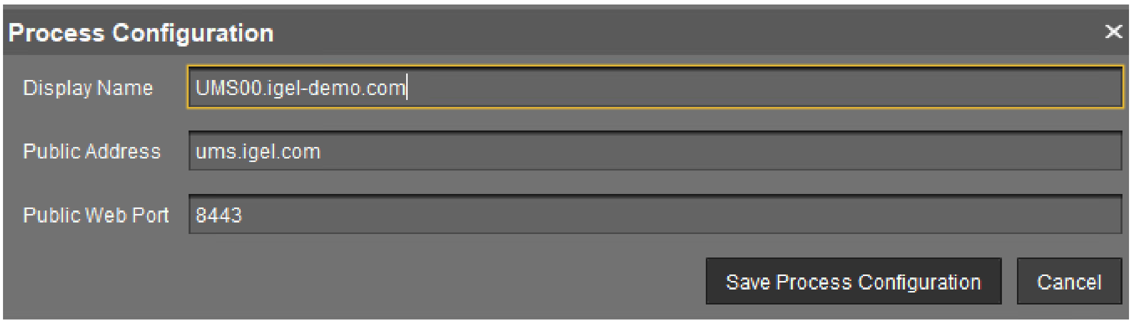
     OR

   - via the UMS
     If changing the hostname of your server is not allowed, then you can change the **Display Name** and **Public Address** of your UMS Servers:
     1. In the UMS Console, right-click the server under **UMS Console > UMS Administration > UMS Network > Server** and select **Edit**.



2. Update the **Display Name** to easily resolvable FQDN of the server.

3. If you have a different external name for the server, enter it under **Public Address**. For more information on the Public Address, see Server - View Your IGEL UMS Server Information.



Process Configuration

Display Name: UMS00.igel-demo.com

Public Address: ums.igel.com

Public Web Port: 8443

4. Restart the UMS Server service. For details on how you can do it, see IGEL UMS HA Services and Processes.

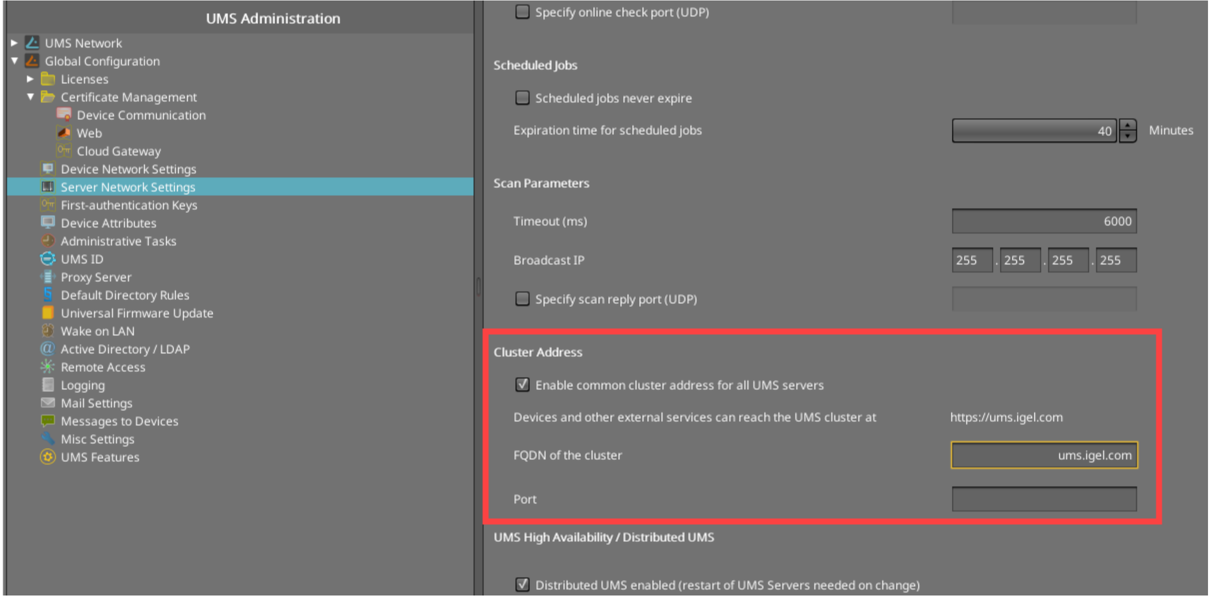
5. Validate that you can resolve the **Display Name** or **Public Address** of the UMS Server(s) from your IGEL OS devices.

Specifying the Cluster Addresses of the UMS Server

If you are using multiple UMS Servers and they share a single external address, then you will need to update the FQDN of the UMS cluster; see "Cluster Address" section under Server Network Settings in the IGEL UMS. To do this, you can follow the steps below:

1. Confirm you can resolve / ping the unified FQDN and that it resolves to the correct IP(s) for your UMS cluster.

2. In the UMS Console, go to **UMS Administration > Global Configuration > Server Network Settings** and activate **Enable common cluster address for all UMS Servers**.



☐ Specify online check port (UDP)

Scheduled Jobs

☐ Scheduled jobs never expire

Expiration time for scheduled jobs: 40 Minutes

Scan Parameters

Timeout (ms): 6000

Broadcast IP: 255 . 255 . 255 . 255

☐ Specify scan reply port (UDP)

Cluster Address

☑ Enable common cluster address for all UMS servers

Devices and other external services can reach the UMS cluster at https://ums.igel.com

FQDN of the cluster: ums.igel.com

Port:

UMS High Availability / Distributed UMS

☑ Distributed UMS enabled (restart of UMS Servers needed on change)

3. Under **FQDN of the cluster**, enter the FQDN that your devices can use to resolve the UMS cluster.

4. If you have configured the custom port, specify it under **Port**.

5. Save the settings.

6. Configure a web certificate for all servers as described under Server Network Settings in the IGEL UMS.

7. Restart the UMS Server service on all servers. For details on how you can do it, see IGEL UMS HA Services and Processes.

Troubleshooting: Error 37 during Onboarding of an IGEL OS12 Device

During the onboarding with the IGEL Onboarding Service or with the one-time password method, you get the following error message: " `Could not manage your device because of an internal error (<37>)` ". Error 37 indicates that the device was unable to get the CA certificates from the Universal Management Suite (UMS) Server(s).

Problem

Possible causes for error 37 may be:

- NO HTTPS connection to the UMS Server
  Getting the CA certificates from the UMS Server is the first step of the onboarding process, so the error 37 can indicate that the device is unable to establish a HTTPS connection to the UMS Server. This can be caused by the network environment configuration, like a firewall or TLS inspection.

- CA certificates cannot be verified due to an incomplete CA chain
  The downloaded CA certificates are verified by the device, so the error 37 can occur if the downloaded CA certificates cannot be verified by IGEL OS. This can be caused by an incomplete chain of CA certificates, for example, a missing certificate of the root CA.

Solution

No HTTPS Connection to the UMS Server

To diagnose network issues, use the `curl` command, the standard HTTP(s) tool included in IGEL OS 12/OS 11 and other Linux OS. Execute the following command to download CA certificates from the UMS Server:

```
curl --tlsv1.3 --insecure https://<YOUR_UMS_ADDRESS>:<PORT>/device-connector/
device/.well-known/est/cacerts
```

If the command fails to download CA certificates, you potentially have a networking or firewall problem. Try to adjust firewall settings or TLS inspection to allow the necessary HTTPS connections.

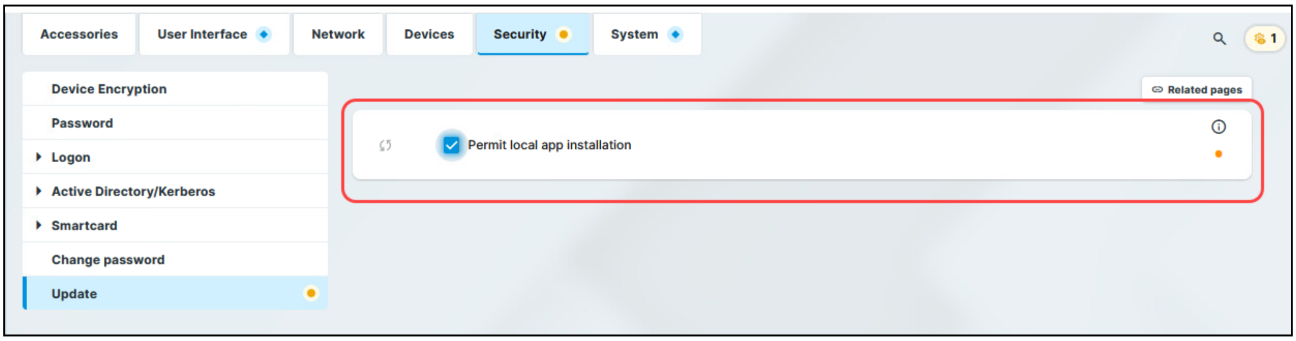
CA Certificates Cannot Be Verified Due to an Incomplete CA Chain

To solve this, import the complete CA chain as it described in Installing an Existing Certificate Chain.

If the missing certificate belongs to a public CA, try to update to IGEL OS 12.3.0. or above. These IGEL OS versions can automatically complete the CA chain with the required issuer certificates from the repository of public CA certificates contained in IGEL OS 12.

Installing IGEL OS Apps Locally on the Device

You can install / uninstall apps on your devices not only via the IGEL Universal Management Suite (UMS), but also via the App Portal application on your devices. This is possible if **Permit local app installation** is enabled under **Security > Update**:



☑ Permit local app installation

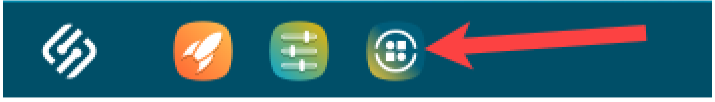
Starting methods for the App Portal can be defined under **Accessories > App Portal**.

Access to the local App Portal and the download of apps is possible for UMS-managed devices if the UMS is registered in the IGEL Customer Portal. For the instructions, see Registering the UMS(see page 36).
If the device is not managed with the UMS, access to the local App Portal is possible but NOT for the devices with a Starter license. For more information on licenses, see Licensing(see page 151).

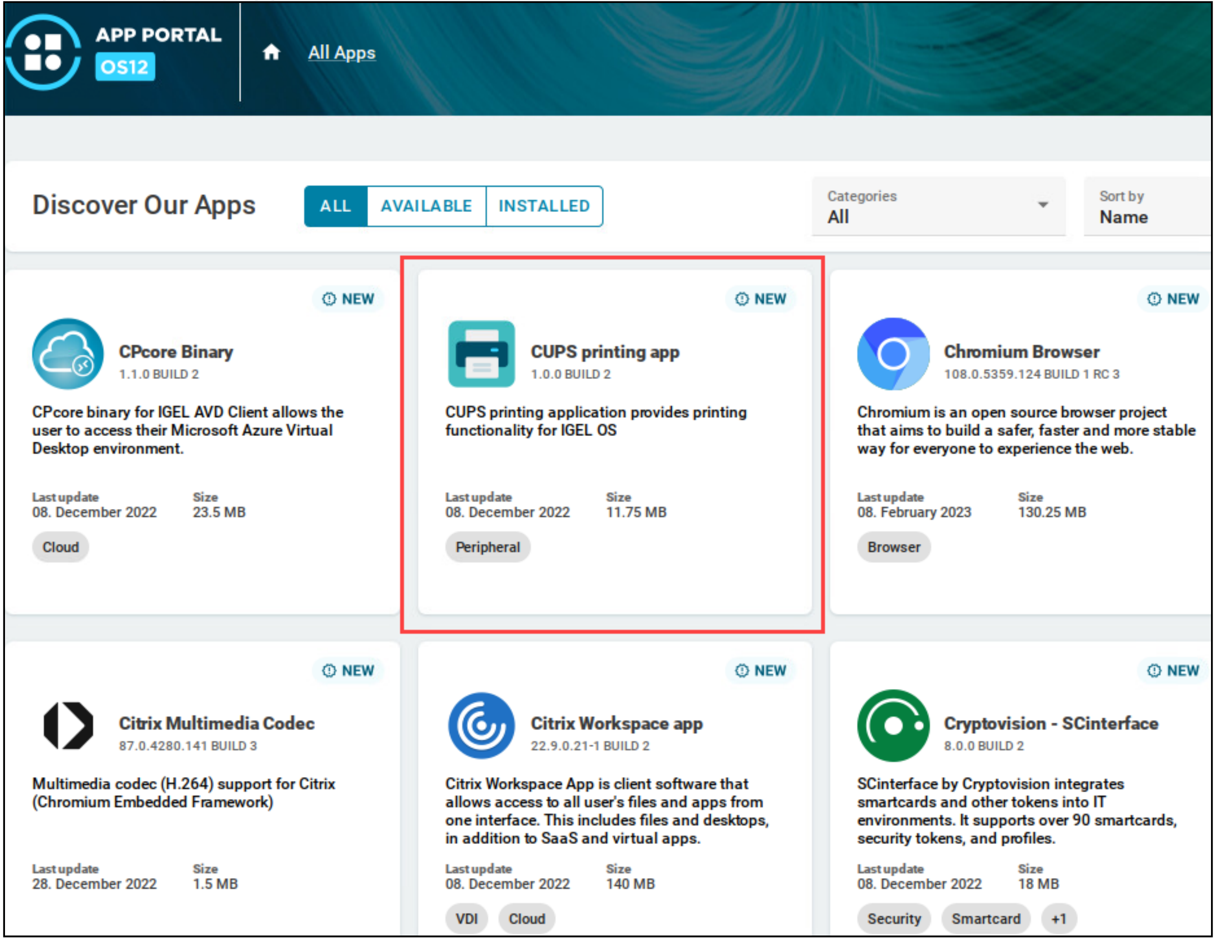
How to Locally Install Apps

To install apps, proceed as follows:

1. Open the App Portal locally on the device.



2. Select the required app and its version and click **Install**.



APP PORTAL OS12 | All Apps

Discover Our Apps — ALL | AVAILABLE | INSTALLED — Categories: All — Sort by: Name

CPcore Binary (NEW) 1.1.0 BUILD 2
CPcore binary for IGEL AVD Client allows the user to access their Microsoft Azure Virtual Desktop environment.
Last update 08. December 2022 — Size 23.5 MB — Cloud

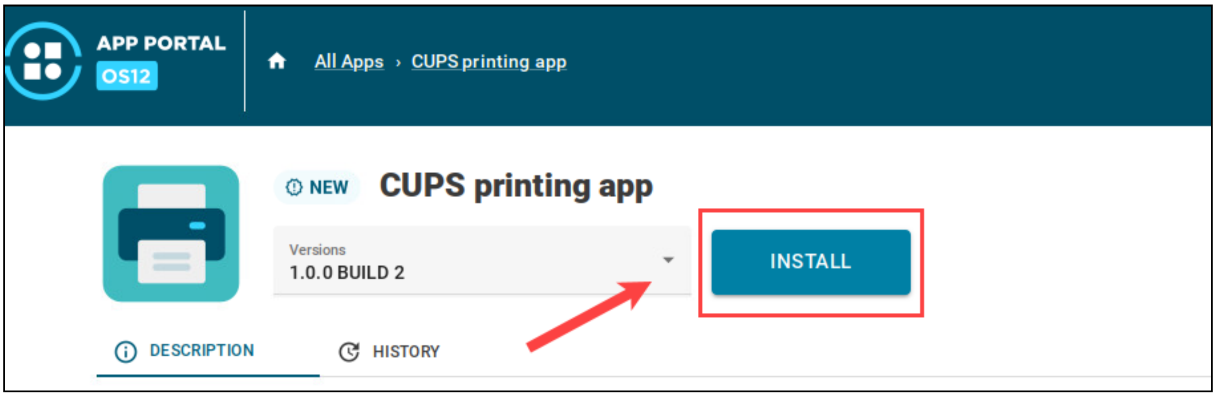
CUPS printing app (NEW) 1.0.0 BUILD 2
CUPS printing application provides printing functionality for IGEL OS
Last update 08. December 2022 — Size 11.75 MB — Peripheral

Chromium Browser (NEW) 108.0.5359.124 BUILD 1 RC 3
Chromium is an open source browser project that aims to build a safer, faster and more stable way for everyone to experience the web.
Last update 08. February 2023 — Size 130.25 MB — Browser

Citrix Multimedia Codec (NEW) 87.0.4280.141 BUILD 3
Multimedia codec (H.264) support for Citrix (Chromium Embedded Framework)
Last update 28. December 2022 — Size 1.5 MB

Citrix Workspace app (NEW) 22.9.0.21-1 BUILD 2
Citrix Workspace App is client software that allows access to all user's files and apps from one interface. This includes files and desktops, in addition to SaaS and virtual apps.
Last update 08. December 2022 — Size 140 MB — VDI — Cloud

Cryptovision - SCinterface (NEW) 8.0.0 BUILD 2
SCinterface by Cryptovision integrates smartcards and other tokens into IT environments. It supports over 90 smartcards, security tokens, and profiles.
Last update 08. December 2022 — Size 18 MB — Security — Smartcard — +1



APP PORTAL OS12 | All Apps › CUPS printing app

NEW **CUPS printing app**

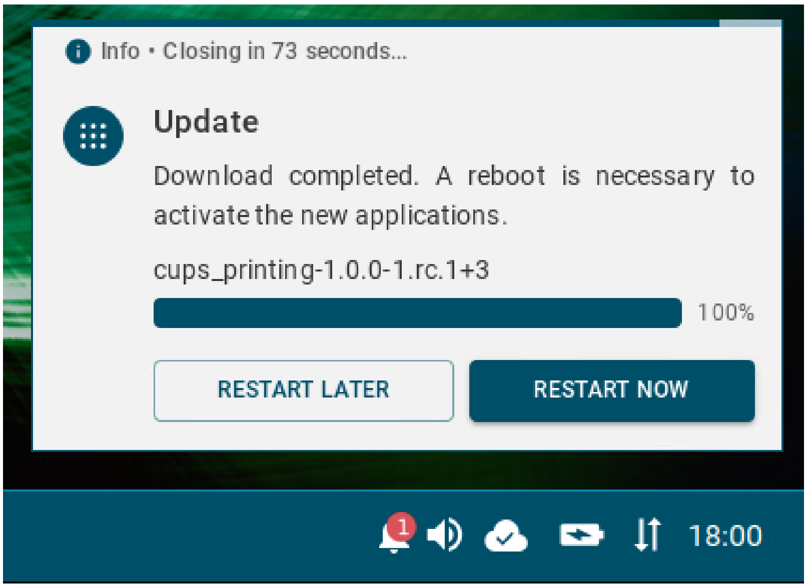
Versions: 1.0.0 BUILD 2 — INSTALL

DESCRIPTION — HISTORY

ⓘ If the selected app / app version has already been installed, the **Uninstall** icon is shown.

3. Accept the End User License Agreement (EULA).

The selected app version will be downloaded to the device. The corresponding notification will be shown:



Info • Closing in 73 seconds...

Update

Download completed. A reboot is necessary to activate the new applications.

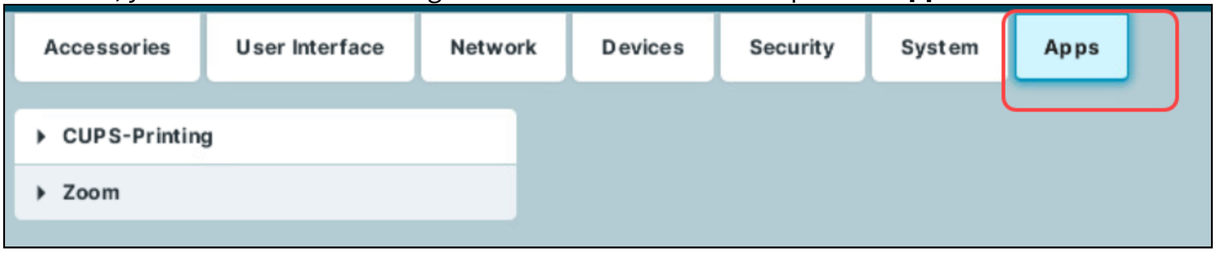
cups_printing-1.0.0-1.rc.1+3

100%

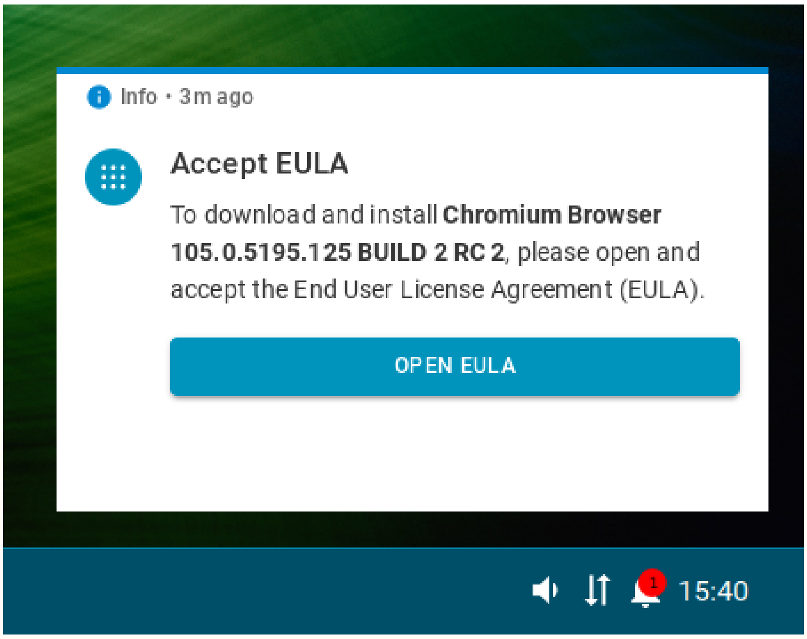
Dependant apps and codecs (e.g. Chromium Multimedia Codec, Fluendo libva for Chromium, Citrix Multimedia Codec) are automatically installed on the device during the installation of the main app (e.g. Chromium Browser app, Citrix Workspace app).

4. Restart the device to complete the app installation.

   After that, you can create and configure sessions in the IGEL Setup under **Apps**.



IGEL OS Base System as well as all locally installed apps are automatically recognized by the UMS and listed in the **UMS Web App > Apps**. If no such app has been imported to the UMS from the IGEL App Portal before and you assign an "automatically registered" app to other devices, the user will have to accept the End User Licence Agreement (EULA):



Info • 3m ago

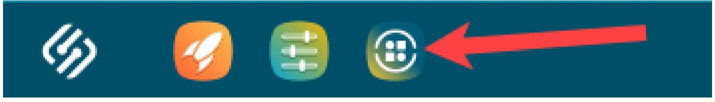
Accept EULA

To download and install **Chromium Browser 105.0.5195.125 BUILD 2 RC 2**, please open and accept the End User License Agreement (EULA).

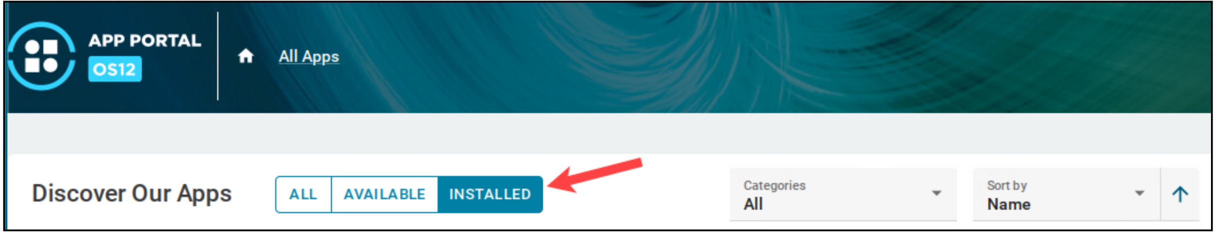
How to Locally Uninstall Apps

To uninstall apps on the device, proceed as follows:

1. Open the App Portal locally on the device.

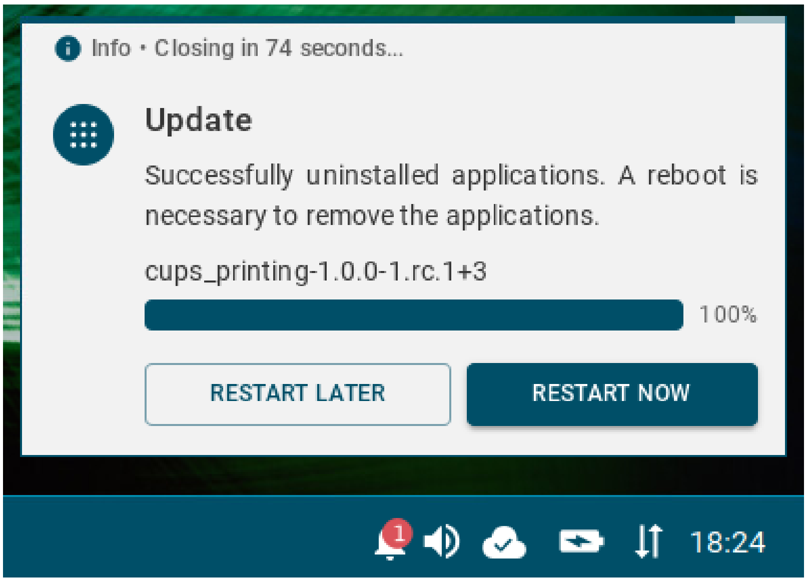


2. Under **Installed**, select the required app.



3. Click **Uninstall**.

The user will receive a corresponding notification:



Info • Closing in 74 seconds...

Update

Successfully uninstalled applications. A reboot is necessary to remove the applications.

cups_printing-1.0.0-1.rc.1+3

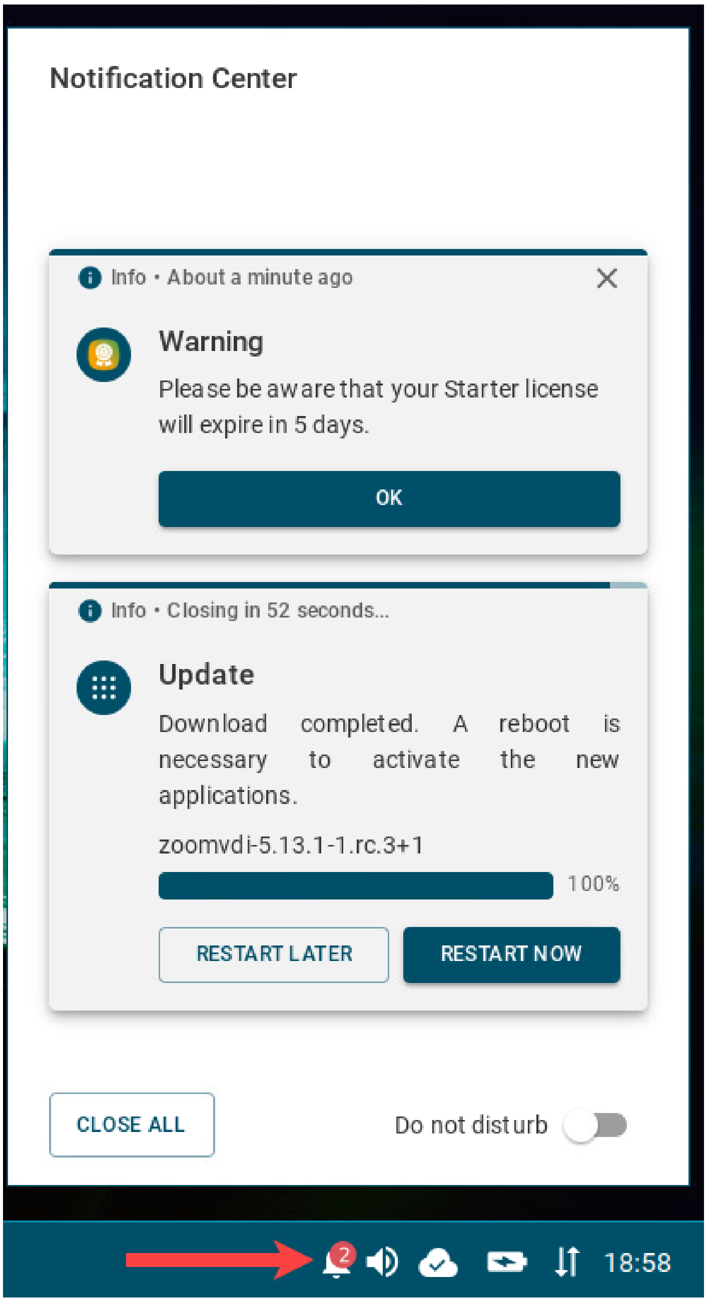
4. Restart the device to complete the app uninstallation.

Configuring Single Sign-On (SSO)

For detailed information, see How to Configure Single Sign-On (SSO) on IGEL OS 12.

IGEL OS Notification Center

On an IGEL OS device, you can view all non-closed notifications in the Notification Center.



Notification Center

Info • About a minute ago

Warning

Please be aware that your Starter license will expire in 5 days.

OK

Info • Closing in 52 seconds...

Update

Download completed. A reboot is necessary to activate the new applications.

zoomvdi-5.13.1-1.rc.3+1

100%

RESTART LATER

RESTART NOW

CLOSE ALL

Do not disturb

ⓘ Notification Center icon 🔔 is displayed if the taskbar and taskbar system tray are activated (**User Interface > Desktop > Taskbar** and **Taskbar Items**; both are enabled by default).

ⓘ If you do not want to see floating notifications, you can activate the **Do not disturb** function.

In the Notification Center, you can see

- Update notifications prompting the user to reboot the device to complete the app installation. The device will be restarted automatically if the user will not react within 60 seconds; this timeout can be changed under **System > Update > Timeout for automatical reboot in seconds**.

  ⓘ If you do not want the user to see the dialog offering to restart the device immediately or postpone the restart, you can enable **Automatical reboot of system once app is installed** under **System > Update**.

  Note: The update notification is different if **Activate app after the installation** is disabled under **System > Update**, see How to Configure the Background App Update in the IGEL UMS Web App.

- EULA notifications if the End User Licence Agreement has to be accepted. When this may be necessary is described under Accepting EULA in the UMS(see page 114).
- Messages sent by the UMS administrator
- Warnings, e.g. about license expiration, and errors
- Other notifications, e.g. about a new configuration the system has received

IGEL Insight Service

At the first start of the IGEL UMS Console or the UMS Web App after the UMS installation, you are presented with a dialog offering to activate IGEL Insight Service. If you are not sure, you can skip this step to decide later; in this case, the dialog will be presented on each start of the UMS Console / the UMS Web App until the feature is accepted or declined.

> ⓘ IGEL Insight Service can be anytime activated or deactivated under **UMS Console > UMS Administration > Global Configuration > UMS Features** or under **UMS Web App > Network > Settings > UMS Features**.

IGEL Insight Service collects analytical and usage data from all users to

- improve IGEL products and services and the user experience
- inform you about available software and security updates
- provide recommendations for system optimization (software and hardware)
- identify potential performance issues regarding apps in your setup
- improve customer support and consulting

The identity of the individual IGEL OS device will only be stored pseudonymously. All data will be anonymized after two years.

The consent can be withdrawn by disabling the Insight Service functionality as described above. By withdrawing the consent, you will not receive further recommendations based on your setup.

For more information, please refer to IGEL's privacy policy[22].

> ⓘ **Where Are the IGEL COSMOS Cloud Services Data Stored?**
> Currently, the IGEL COSMOS Cloud Services and apps available in the IGEL App Portal are stored in Azure Region West-Europe, location Amsterdam. The associated app metadata are stored in Frankfurt (Germany west central).
> The Insight Service data are currently also stored in Frankfurt (Germany west central).
> All data centers and their operators are fully ISO/IEC 27001 certified.

Data Collected by the IGEL Insight Service

- Company identifier
- UMS identifier
- Pseudonymized device identifier
- Name of the application
- Version of the application
- Manufacturer of the device
- Model of the device
- CPU of the device
- RAM of the device
- Mainboard of the device
- GPU of the device

[22] https://www.igel.com/privacy-policy/

- Storage hardware of the device
- Network / Wi-Fi hardware information of the device
- Peripheral hardware information of the device
- Timestamp
- Client type (Insight Service Data Collector)
- Client version (Insight Service Data Collector)

IGEL does not share your data with third parties outside the IGEL group.

Debugging / How to Collect and Send Device Log Files to IGEL Support

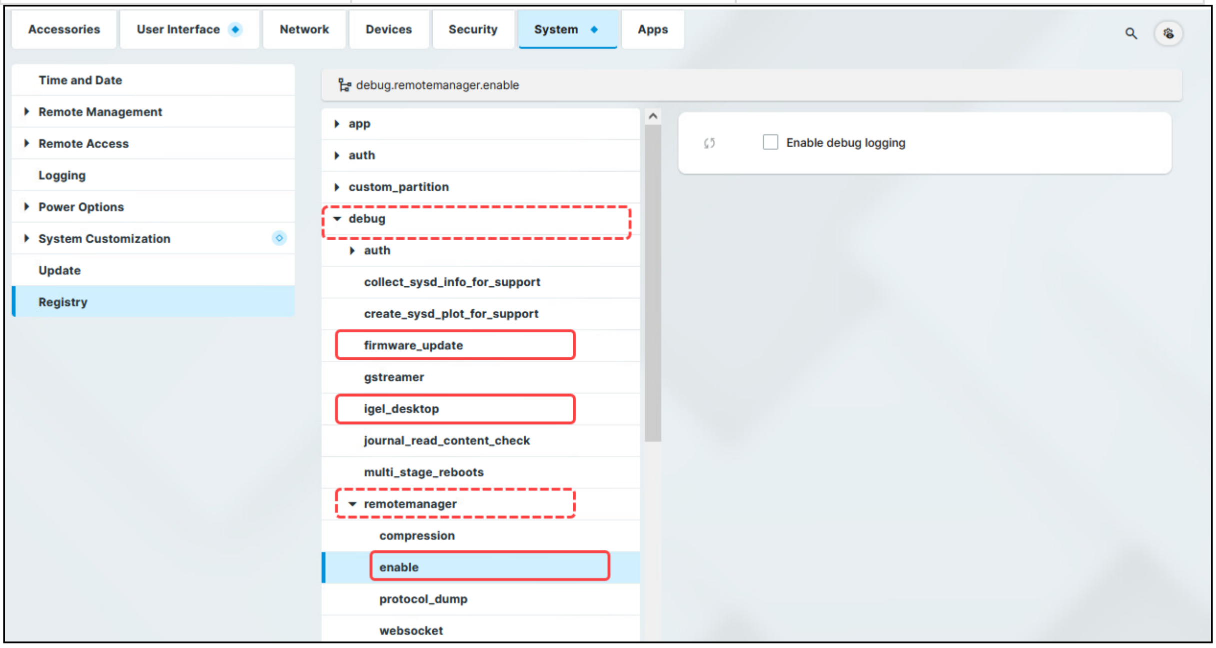
To collect the log files from the IGEL UMS Server, UMS Console, etc., you can use the Support Wizard: **UMS Console > Menu bar > Help > Save support information**. See Support Wizard in the IGEL UMS.

To collect the device log files, see the instructions below.

With IGEL OS 12, additional logging functionalities have been introduced to facilitate debugging. To enable debug mode, proceed as follows:

1. In the IGEL Setup, go to **System > Registry** and activate the following registry keys:

Registry	Parameter	Function
`debug.igel_desktop`	**Enable debug logging for IGEL desktop**	Debug logging for user interface applications like the Setup Assistant and the Setup
`debug.firmware_update`	**Enable debug logging for firmware update**	Debug logging for updates and installations of IGEL OS Apps
`debug.remotemanager.enable`	**Enable debug logging**	Debug logging for RMagent communication



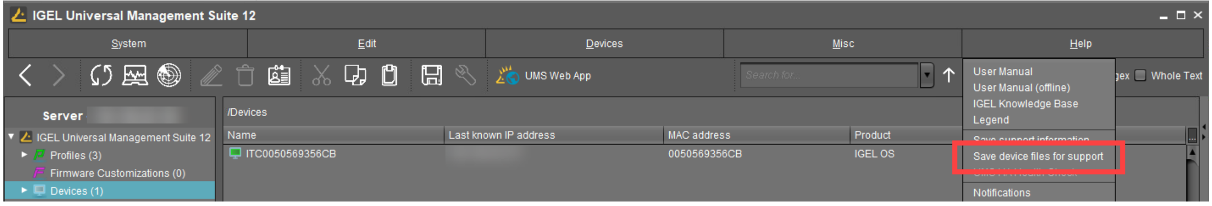
2. Save the setting.

Optionally, you can also enable protocol dump output via `debug.remotemanager.protocol_dump` . This activates debug logging for all commands sent from the UMS to the device or vice versa:
`/var/log/rmagent-ws-in.log`
`/var/log/rmagent-ws-out.log`
Activate this registry key only if required.

Collecting Device Logs via the UMS

After you have activated the above registry keys, you can use the UMS Console to collect the device log files:

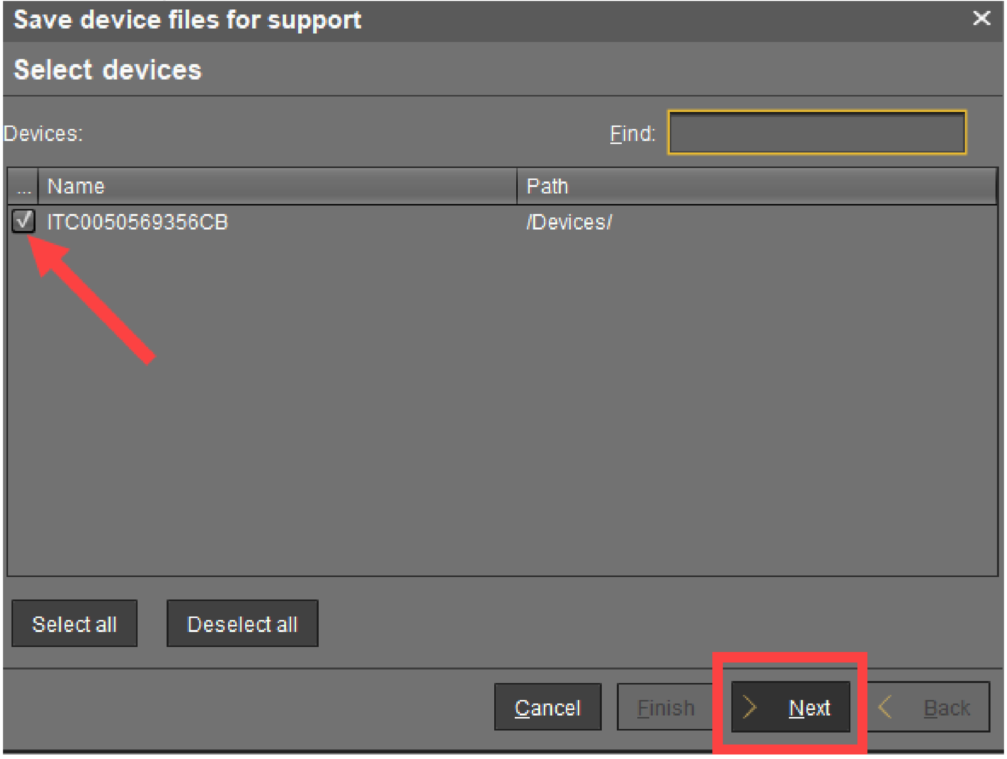
1. In the UMS Console, go to **Help > Save device files for support**.



Name	Last known IP address	MAC address	Product
ITC0050569356CB	[redacted]	0050569356CB	IGEL OS

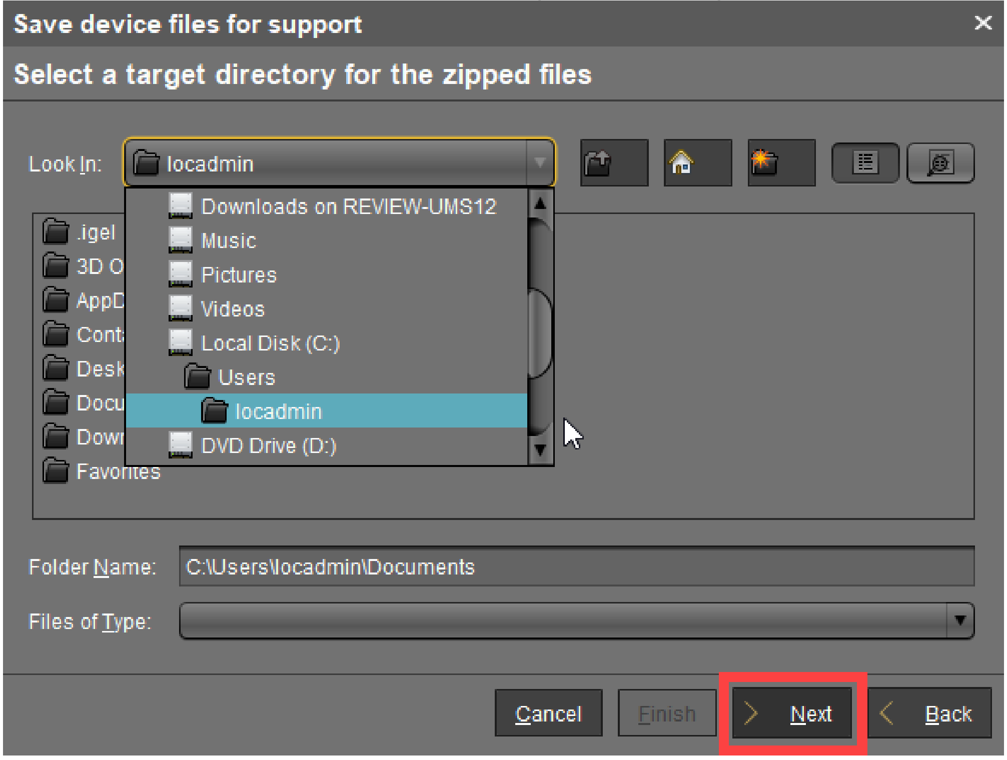
The dialog **Save device files for support** opens.

2. Select the required device(s) and click **Next**.



...	Name	Path
☑	ITC0050569356CB	/Devices/

3. Select a directory which is suitable for saving the zipped log files and click **Next**.



Save device files for support

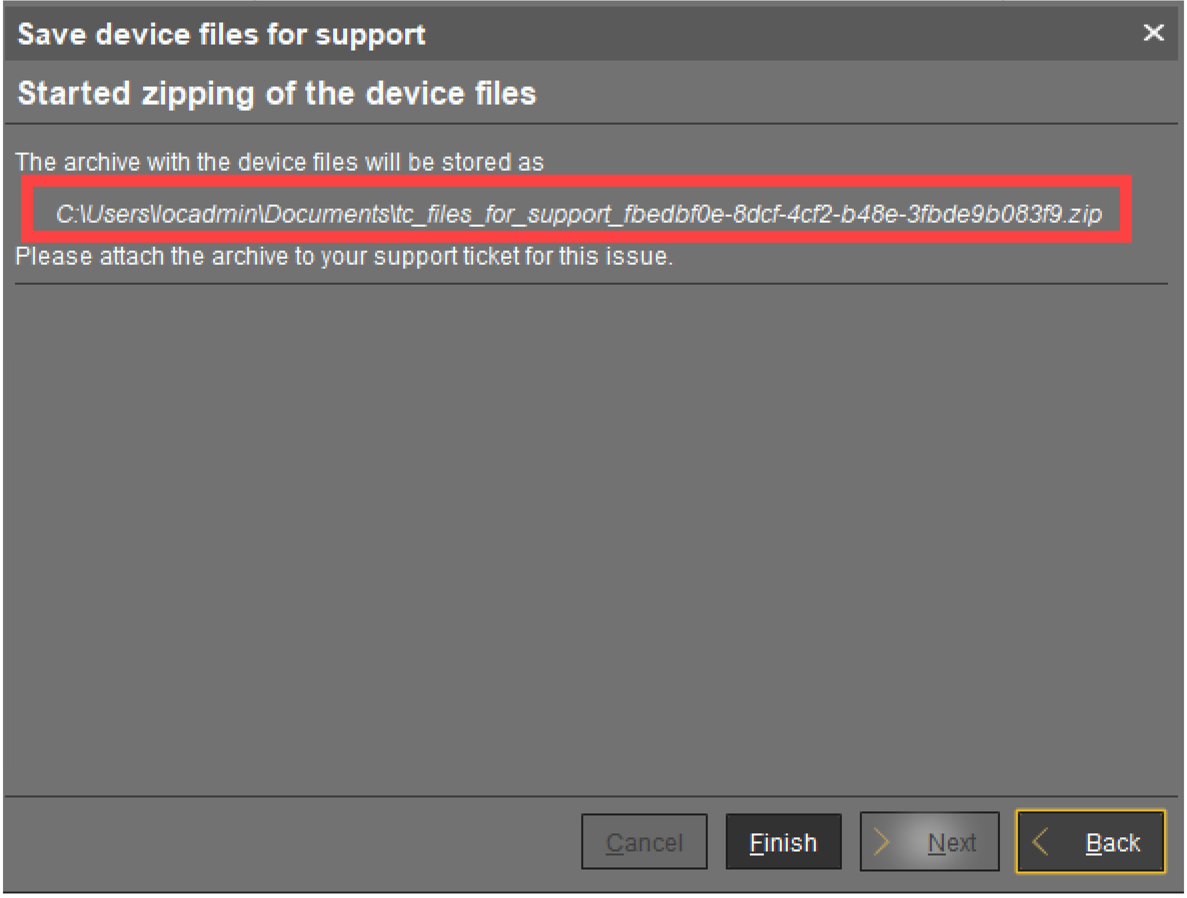
Select a target directory for the zipped files

Look In: locadmin

Folder Name: C:\Users\locadmin\Documents

Files of Type:

A confirmation dialog opens and shows the path and file name under which the log files are stored.



Save device files for support

Started zipping of the device files

The archive with the device files will be stored as

C:\Users\locadmin\Documents\tc_files_for_support_fbedbf0e-8dcf-4cf2-b48e-3fbde9b083f9.zip

Please attach the archive to your support ticket for this issue.

4. When the log collecting procedure is complete, close the confirmation dialog by clicking **Finish**.

5. Find the ZIP file "`tc_files_for_support_...`" in the directory you selected and send it to I[23]GEL Support via the IGEL Customer Portal[24].

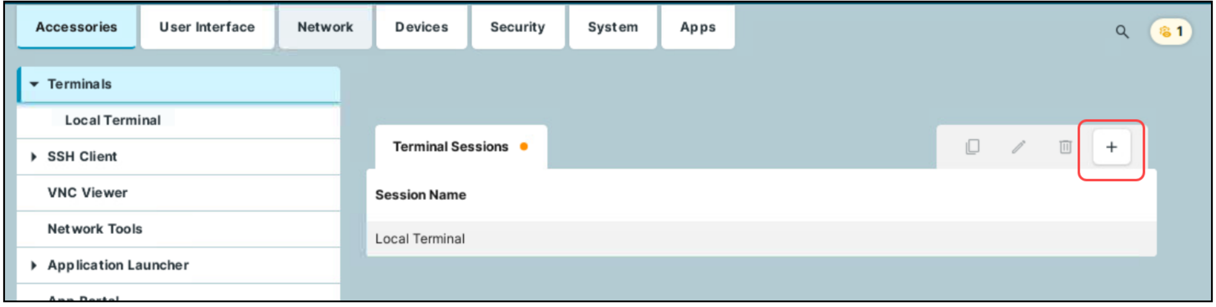
Collecting Device Logs without the UMS

When the UMS is not accessible or there is an issue with network connectivity, you can still extract logs from a device.

[23] mailto:eap@igel.com
[24] https://cosmos.igel.com/

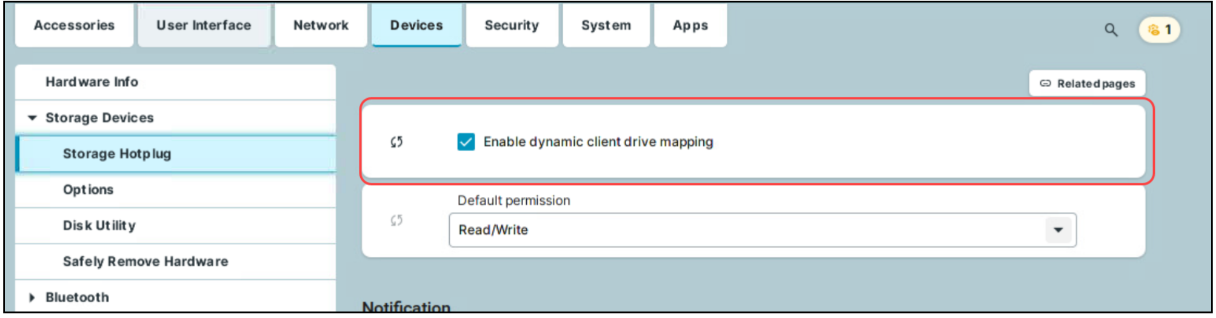
Option 1: Via Local Terminal

1. In the IGEL Setup, go to **Accessories > Terminals** and create a terminal session.



Session Name
Local Terminal

2. Go to **Devices > Storage Devices > Storage Hotplug** and activate **Enable dynamic client drive mapping**.



☑ Enable dynamic client drive mapping

Default permission: Read/Write

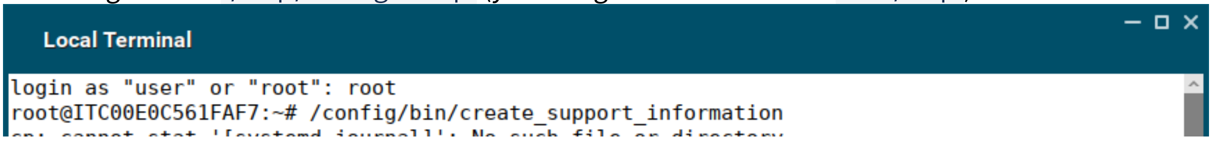
3. Verify that **System > Registry > debug > igel_desktop > Enable debug logging for IGEL desktop** is enabled.

4. Save the settings.

5. Plug the USB stick into the endpoint device and start the terminal session.

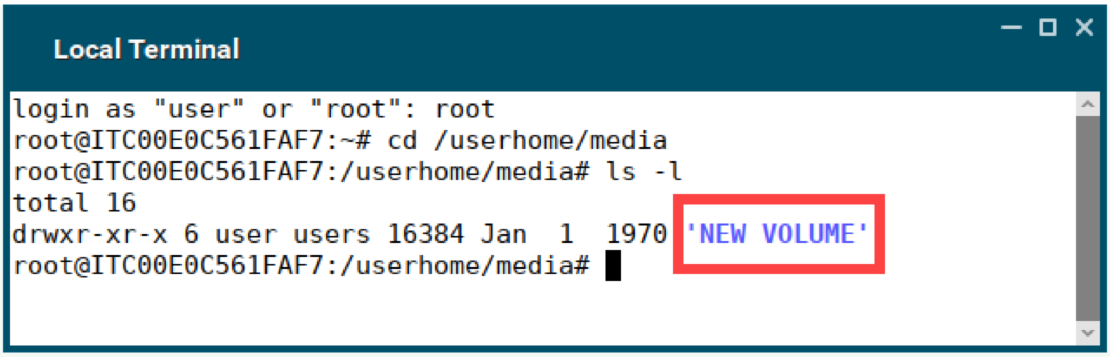
6. Log in as `root` (by default, no password).

7. To create the log files, execute the command `/config/bin/create_support_information` This will generate `/tmp/tclogs.zip` (you can go there as follows: `cd /tmp`)



```
login as "user" or "root": root
root@ITC00E0C561FAF7:~# /config/bin/create_support_information
```

> ✓ To find out the name of the USB stick, you can use the following commands:
> ```
> cd /userhome/media
> ls -l
> ```



Local Terminal

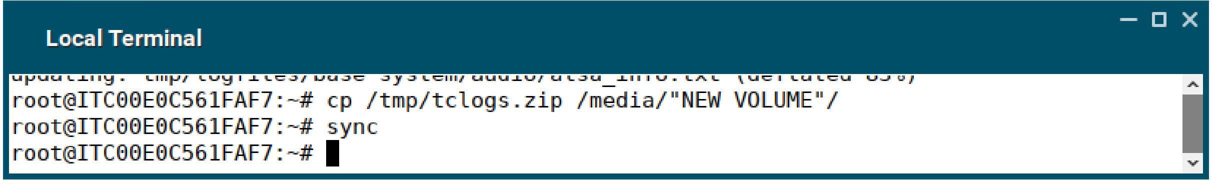
```
login as "user" or "root": root
root@ITC00E0C561FAF7:~# cd /userhome/media
root@ITC00E0C561FAF7:/userhome/media# ls -l
total 16
drwxr-xr-x 6 user users 16384 Jan  1  1970 'NEW VOLUME'
root@ITC00E0C561FAF7:/userhome/media# █
```

If there are spaces in the device name, you'll have to include it later in quotation marks. Example: `"NEW VOLUME"`.
If there are no spaces in the device name, quotation marks will not be required.

8. To copy the log files from your endpoint device to the USB stick, run the command `cp /tmp/tclogs.zip /media/[name of your USB stick]/` and press [Return].

Tip
After `/media/`, you can press the tab key for autocompletion.

9. Type `sync` and press [Return].



Local Terminal

```
updating: tmp/logfiles/base-system/audio/alsa_info.txt (deflated 65%)
root@ITC00E0C561FAF7:~# cp /tmp/tclogs.zip /media/"NEW VOLUME"/
root@ITC00E0C561FAF7:~# sync
root@ITC00E0C561FAF7:~# █
```

10. Wait a few seconds before safely ejecting the USB stick from the endpoint device.

11. Send the log files to I[25]GEL Support via the IGEL Customer Portal[26].

Option 2: Via CLI

You can collect log files also via command line interface (CLI). This method can be useful, for example, if you experience problems on the stage of device onboarding.

1. Press anytime [CTRL+ALT+F12] to enter CLI and then press [Return].

2. Plug in your USB stick.

[25] mailto:eap@igel.com
[26] https://cosmos.igel.com/

> ⓘ Use a FAT32-formatted USB stick.

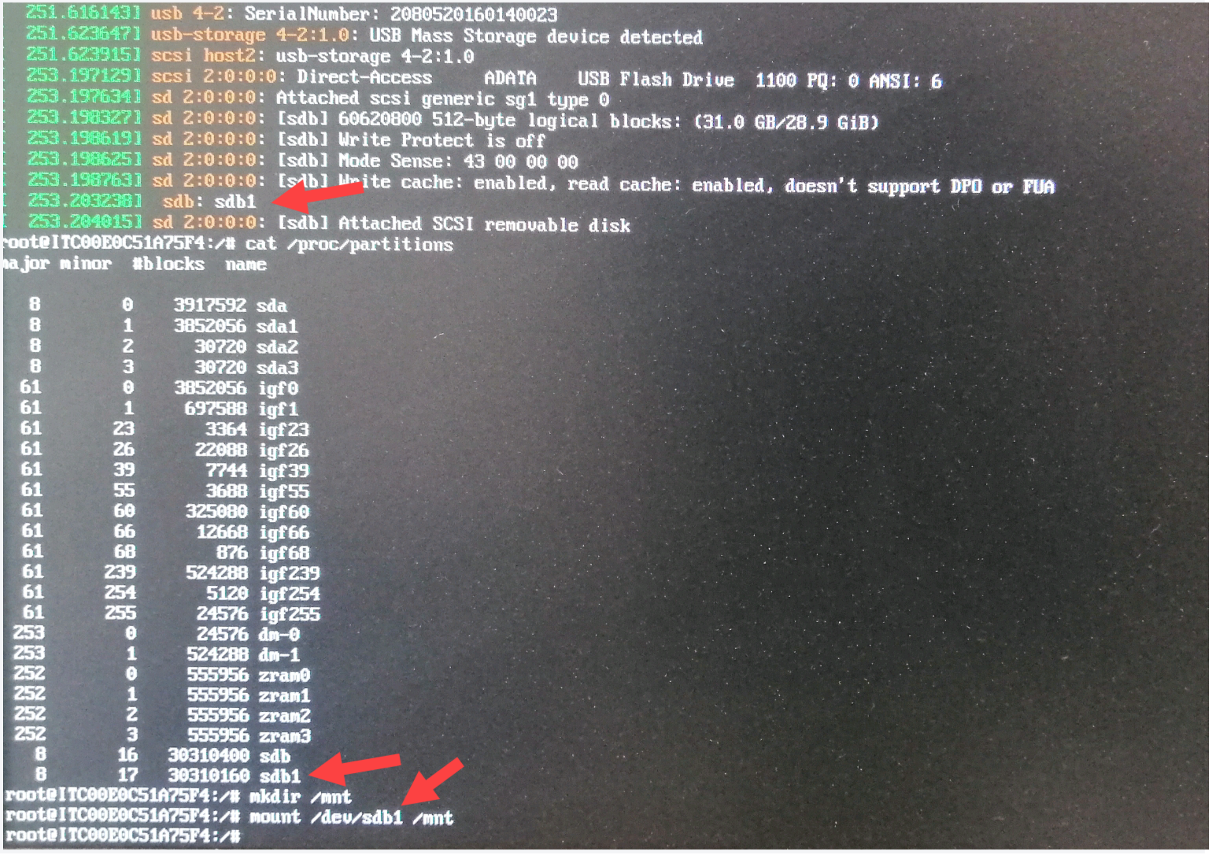
3. Execute the following command: `dmesg`
   This command is used to find out if the USB stick was correctly detected and which device name was assigned (`sda` , `sdb` , `sdc` , etc.)

4. Type `cat /proc/partitions`
   Search for `sda` , `sdb` , `sdc` , etc. and search for the next line showing the partitions (Example: `sda1` , `sdb1` , etc.)

5. Create the mountpoint directory: `mkdir /mnt`

6. The device name for mounting the USB stick for the following command in step 7 needs an additional partition number. Example: `sda1` , `sdb1` , `sdc1` , etc.

7. Mount your USB stick: `mount /dev/sda1 /mnt`



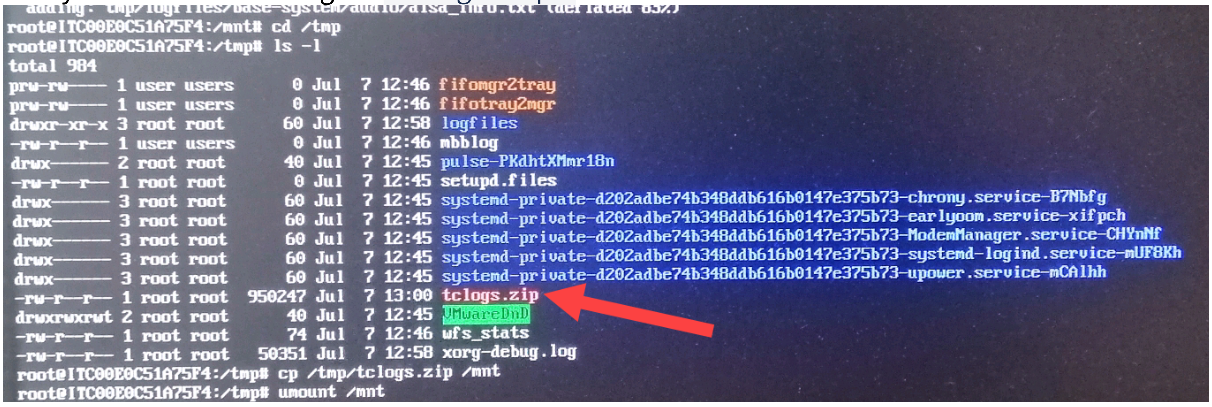
```
 251.616143] usb 4-2: SerialNumber: 2080520160140023
 251.623647] usb-storage 4-2:1.0: USB Mass Storage device detected
 251.623915] scsi host2: usb-storage 4-2:1.0
 253.197129] scsi 2:0:0:0: Direct-Access     ADATA    USB Flash Drive  1100 PQ: 0 ANSI: 6
 253.197634] sd 2:0:0:0: Attached scsi generic sg1 type 0
 253.198327] sd 2:0:0:0: [sdb] 60620800 512-byte logical blocks: (31.0 GB/28.9 GiB)
[ 253.198619] sd 2:0:0:0: [sdb] Write Protect is off
[ 253.198625] sd 2:0:0:0: [sdb] Mode Sense: 43 00 00 00
[ 253.198763] sd 2:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[ 253.203238]  sdb: sdb1
[ 253.204015] sd 2:0:0:0: [sdb] Attached SCSI removable disk
oot@ITC00E0C51A75F4:/# cat /proc/partitions
ajor minor  #blocks  name

   8        0    3917592 sda
   8        1    3852056 sda1
   8        2      30720 sda2
   8        3      30720 sda3
  61        0    3852056 igf0
  61        1     697588 igf1
  61       23       3364 igf23
  61       26      22088 igf26
  61       39       7744 igf39
  61       55       3688 igf55
  61       60     325080 igf60
  61       66      12668 igf66
  61       68        876 igf68
  61      239     524288 igf239
  61      254       5120 igf254
  61      255      24576 igf255
 253        0      24576 dm-0
 253        1     524288 dm-1
 252        0     555956 zram0
 252        1     555956 zram1
 252        2     555956 zram2
 252        3     555956 zram3
   8       16   30310400 sdb
   8       17   30310160 sdb1
root@ITC00E0C51A75F4:/# mkdir /mnt
root@ITC00E0C51A75F4:/# mount /dev/sdb1 /mnt
root@ITC00E0C51A75F4:/#
```

8. Check your data on your mounted USB stick:
   `cd /mnt`
   `ls -l`

Now you should see your data on the USB stick.

9. Generate log files: `/config/bin/create_support_information`
   It can take some time till the log file generation is complete.

10. Type:
    ```
    cd /tmp
    ls -l
    ```
    Now you should see the log file `tclogs.zip` listed.



```
  adding: tmp/logfiles/base-system/audio/alsa_info.txt (deflated 83%)
root@ITC00E0C51A75F4:/mnt# cd /tmp
root@ITC00E0C51A75F4:/tmp# ls -l
total 984
prw-rw----  1 user users      0 Jul  7 12:46 fifomgr2tray
prw-rw----  1 user users      0 Jul  7 12:46 fifotray2mgr
drwxr-xr-x 3 root root      60 Jul  7 12:58 logfiles
-rw-r--r--  1 user users      0 Jul  7 12:46 mbblog
drwx------  2 root root      40 Jul  7 12:45 pulse-PKdhtXMmr18n
-rw-r--r--  1 root root       0 Jul  7 12:45 setupd.files
drwx------  3 root root      60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-chrony.service-B7Nbfg
drwx------  3 root root      60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-earlyoom.service-xifpch
drwx------  3 root root      60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-ModemManager.service-CHYnNf
drwx------  3 root root      60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-systemd-logind.service-mUF8Kh
drwx------  3 root root      60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-upower.service-mCAlhh
-rw-r--r--  1 root root  950247 Jul  7 13:00 tclogs.zip
drwxrwxrwt 2 root root      40 Jul  7 12:45 VMwareDnD
-rw-r--r--  1 root root      74 Jul  7 12:46 wfs_stats
-rw-r--r--  1 root root   50351 Jul  7 12:58 xorg-debug.log
root@ITC00E0C51A75F4:/tmp# cp /tmp/tclogs.zip /mnt
root@ITC00E0C51A75F4:/tmp# umount /mnt
```

11. To copy `tclogs.zip` from your endpoint device to the USB stick, type `cp /tmp/tclogs.zip /mnt` and press [Return].

12. To unmount your USB stick, use the command `umount /mnt`

13. Now you can safely remove your USB stick.

14. To close CLI, press [CTRL+ALT+F1].

15. Send `tclogs.zip` to IGEL Support via the IGEL Customer Portal[27].

[27] https://cosmos.igel.com/