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 215) 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 106)
- IGEL UMS 12: App Update(see page 126)
- 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 188)
- Configuring Single Sign-On (SSO)(see page 193)
- IGEL OS Notification Center(see page 213)
- IGEL Insight Service(see page 215)
- Debugging / How to Collect and Send Device Log Files to IGEL Support(see page 217)

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

Registering for the IGEL Customer Portal

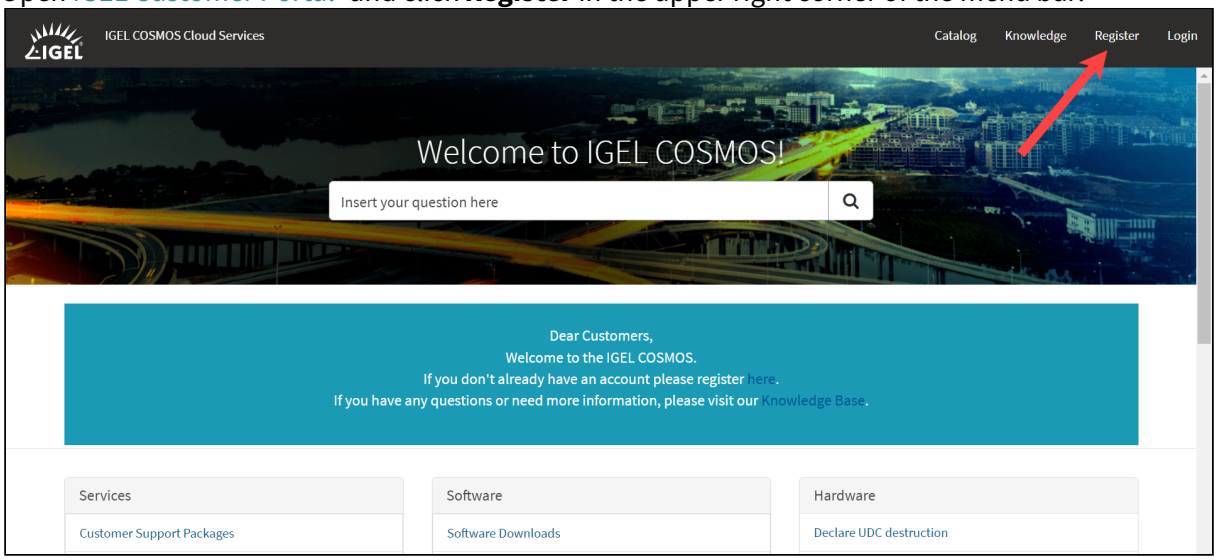
IGEL Customer Portal is the doorway to IGEL product-related services. Registering here your company account is the first step to start using IGEL products.

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:

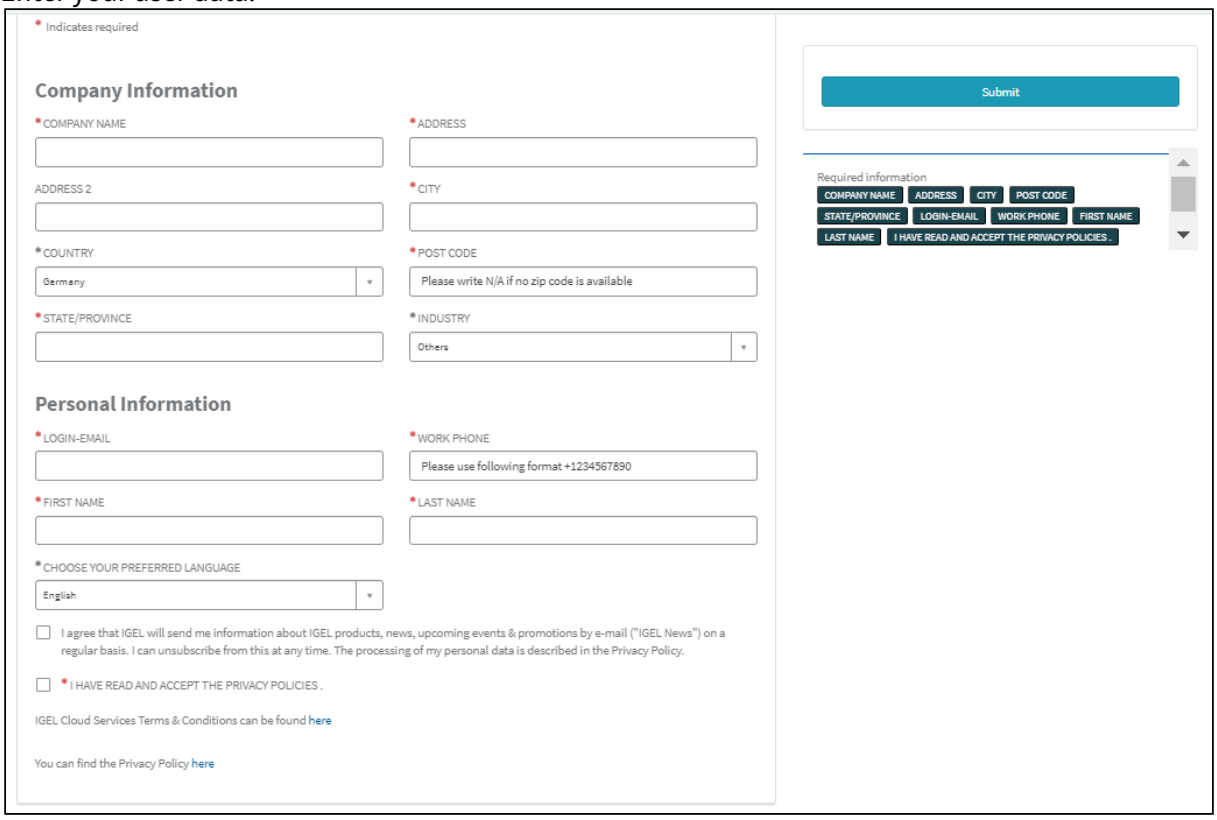
1. Open IGEL Customer Portal[3] and click **Register** in the upper right corner of the menu bar:



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

3 https://cosmos.igel.com/

2. Enter your user data:



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.

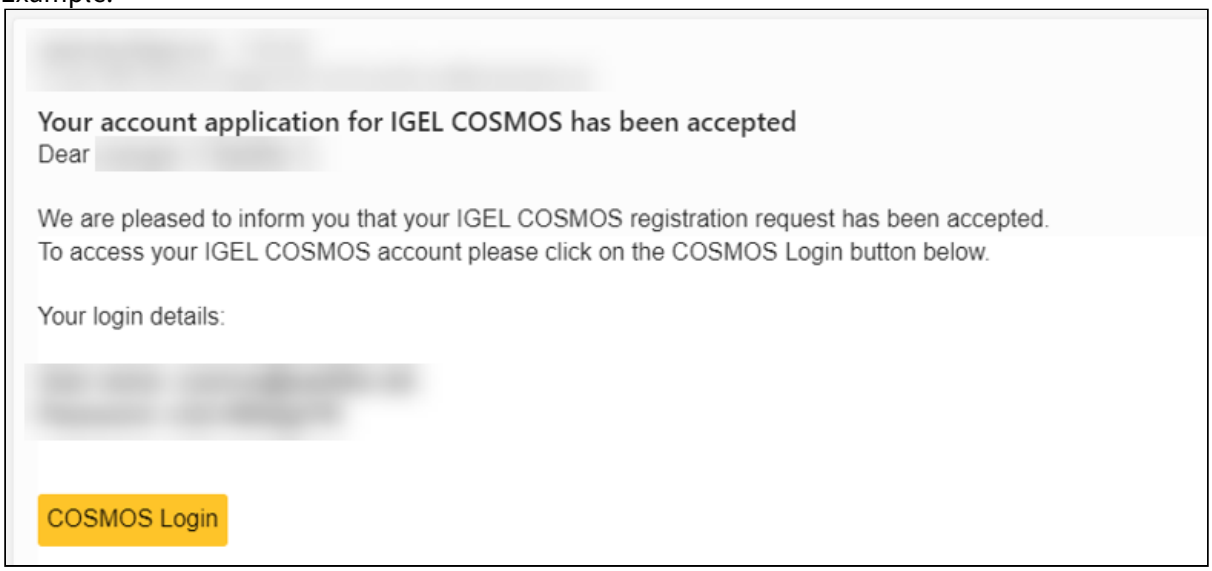
> **IGEL Company Account Requirements**
> - Your name and email address
> - Must be a business email address with your company domain
> - No personal email addresses (solely B2B)
> - No generic contact details or email addresses, e.g. (info@company.tld)
> - No shared (multi-user) accounts (e.g. support-team@company.tld)
> - 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:



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

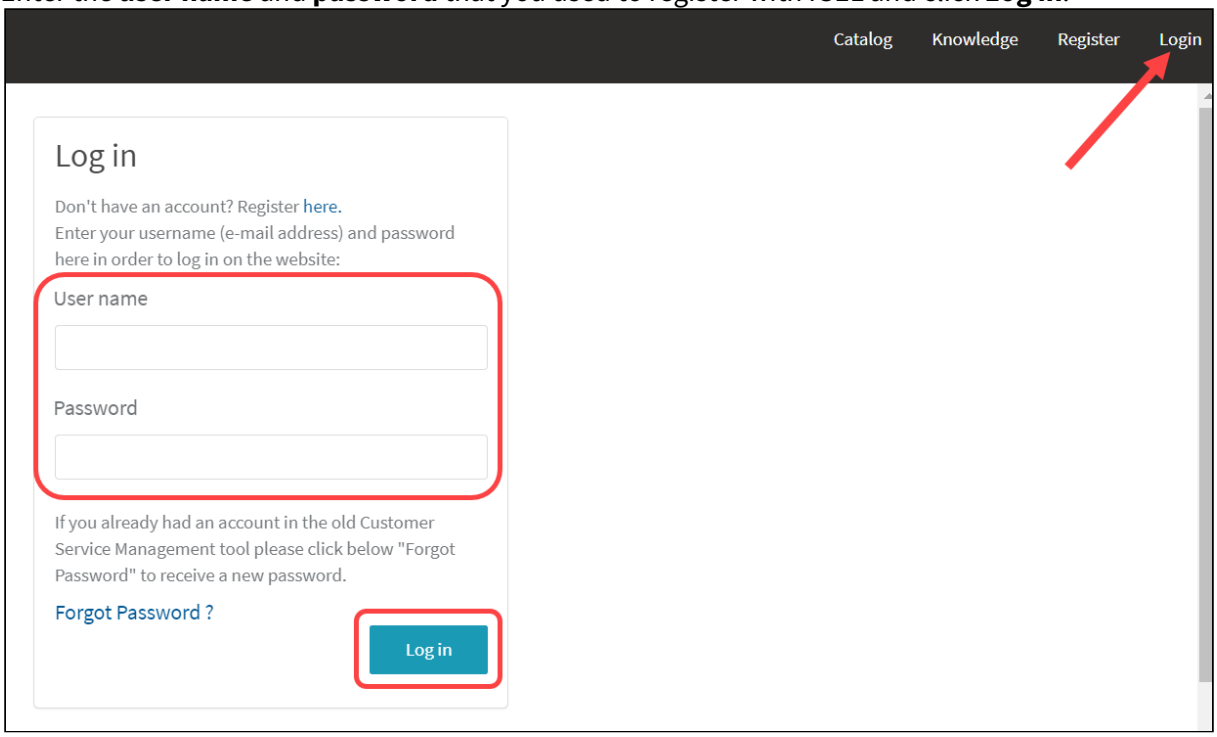
> ⚠ Please remember your login email. It will be used as Super Admin credentials, with which you can later invite new users and assign them specific roles, see Managing Users and Roles in the IGEL Customer Portal(see page 9).

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**.

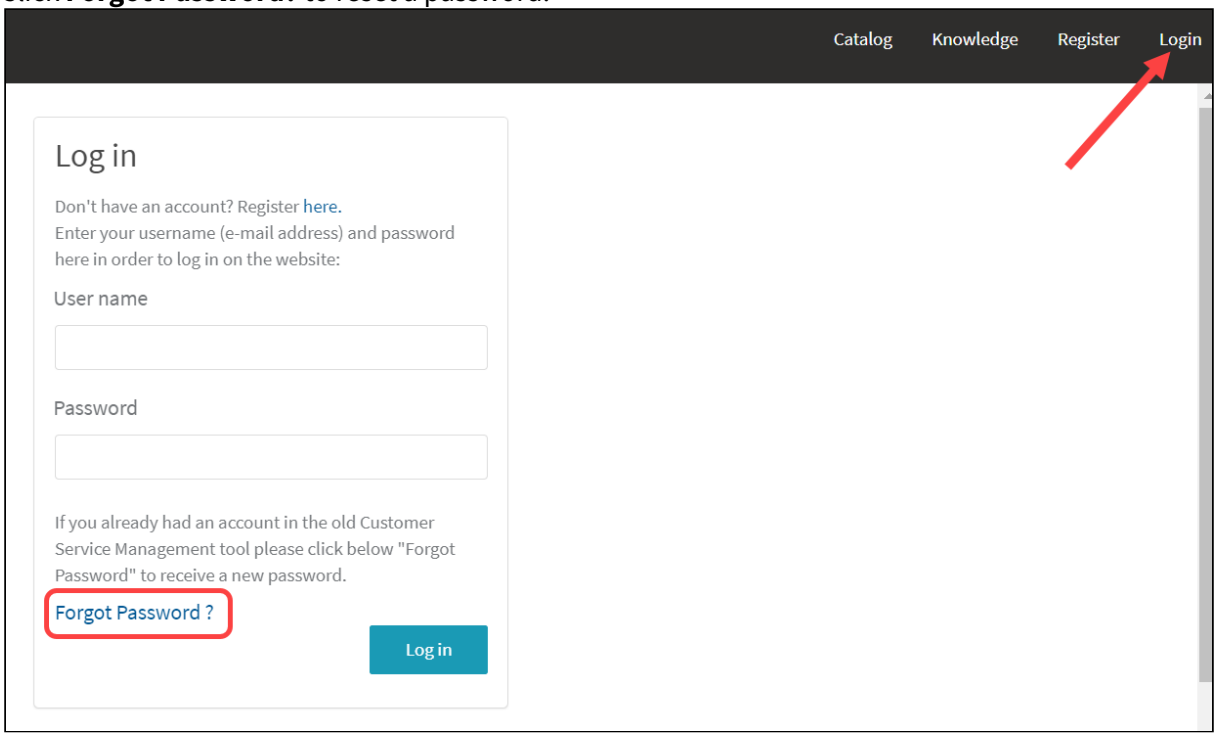


Login Credentials Forgotten?

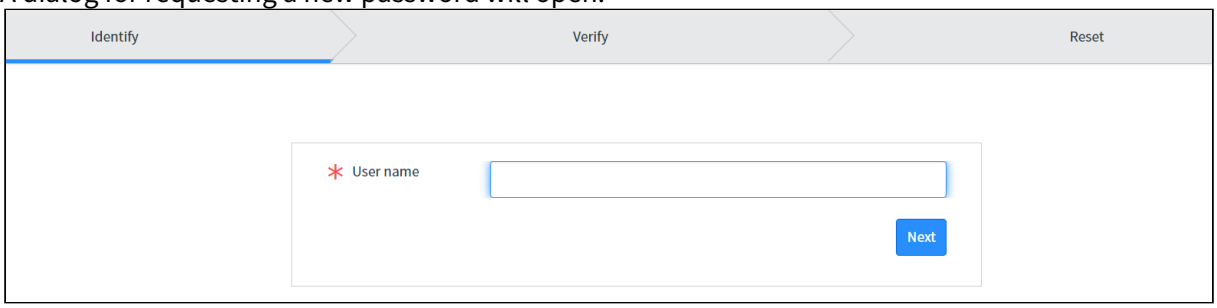
1. Open the IGEL Customer Portal[5] and click **Login**.

5 https://cosmos.igel.com/

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



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.

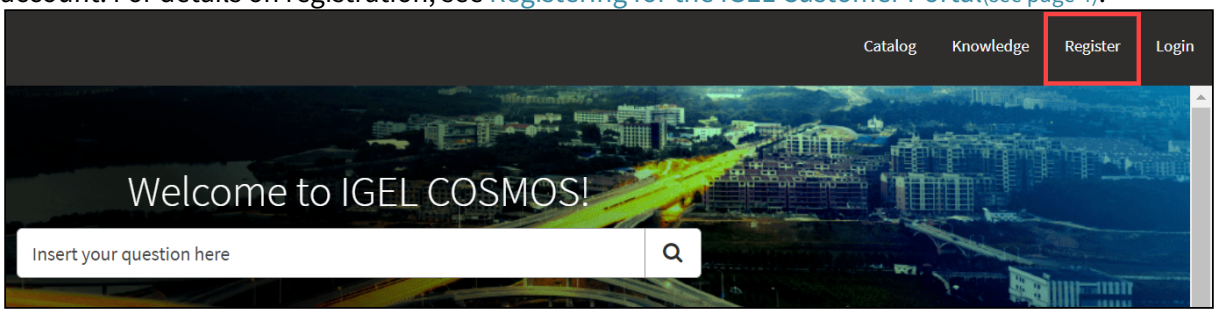
Managing Users and Roles in the IGEL Customer Portal

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	✓	✓			

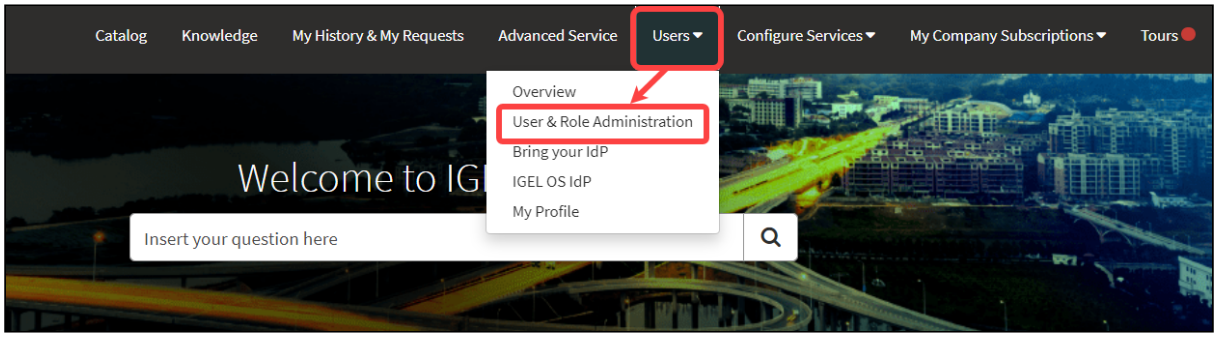
6 https://cosmos.igel.com/

	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	✓				✓

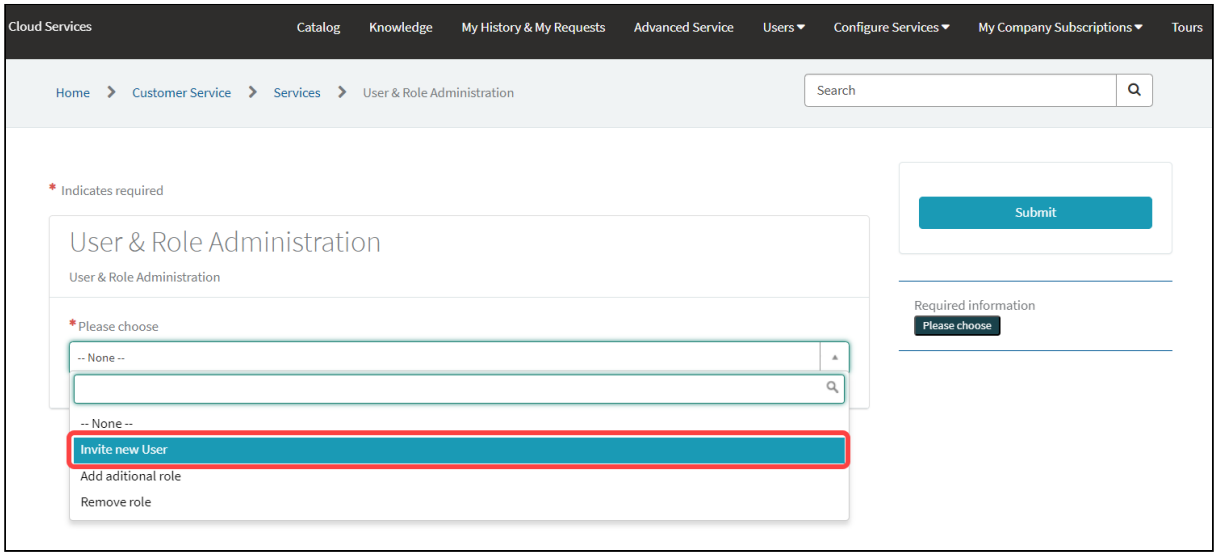
Inviting a User and Assigning a Role

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**.



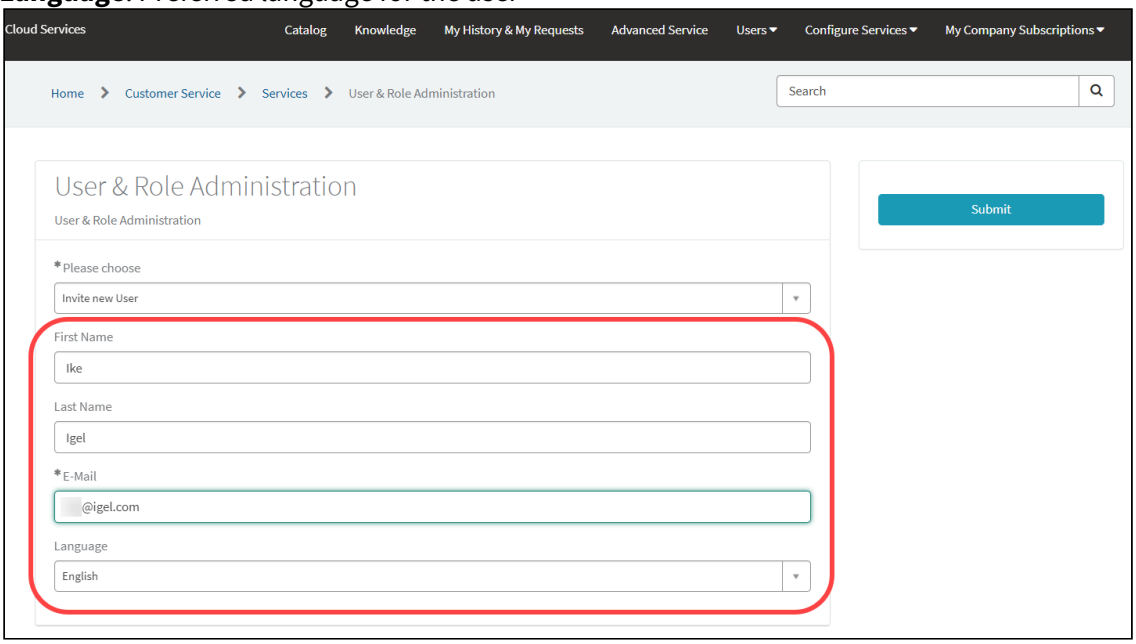
2. Select **Invite new user**.



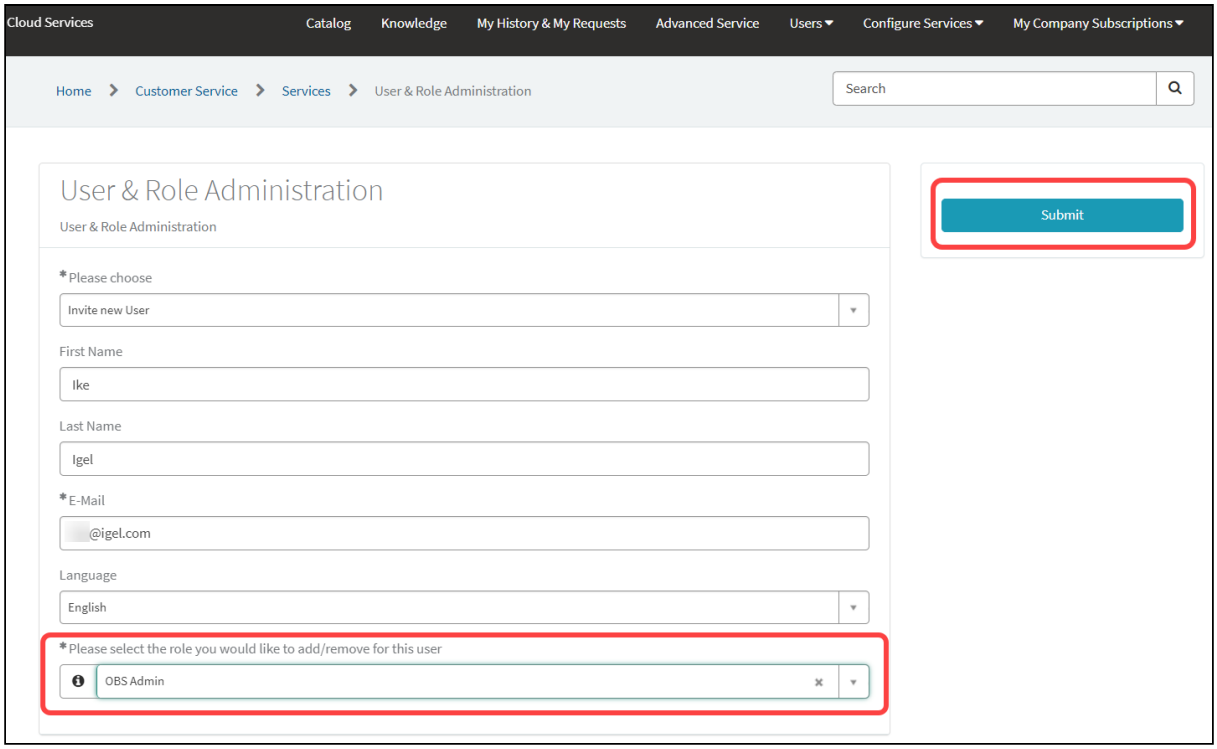
3. Provide the data of the new user:
   - **First name**: First name of the user
   - **Last name**: Last name of the user
   - **E-mail** (required): E-mail address of the user

7 https://cosmos.igel.com/

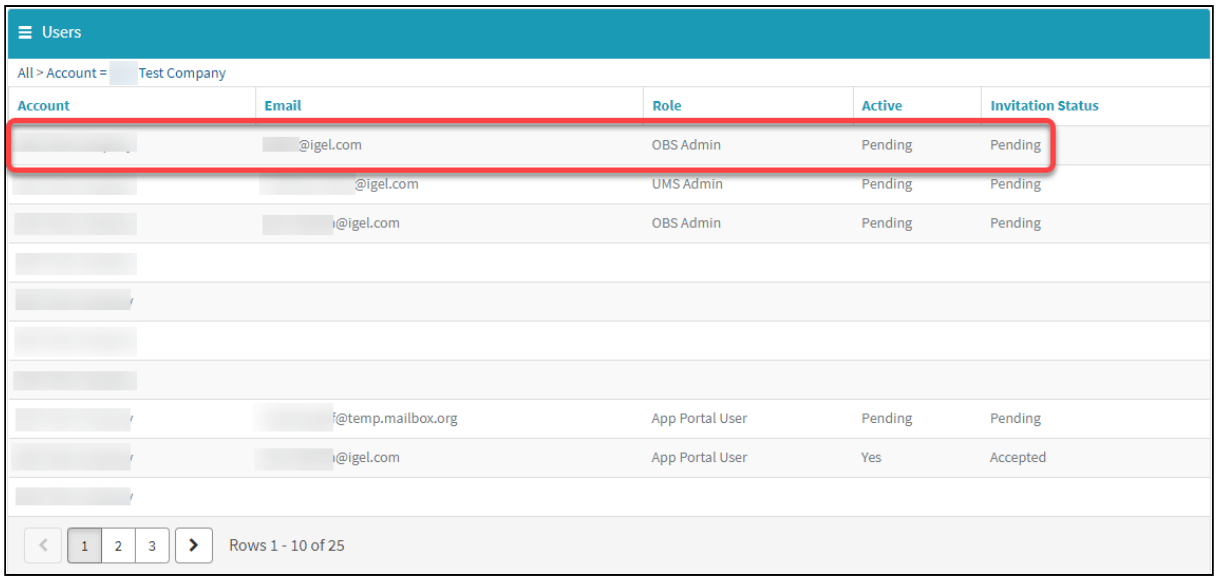
- **Language**: Preferred language for the user



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



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



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.

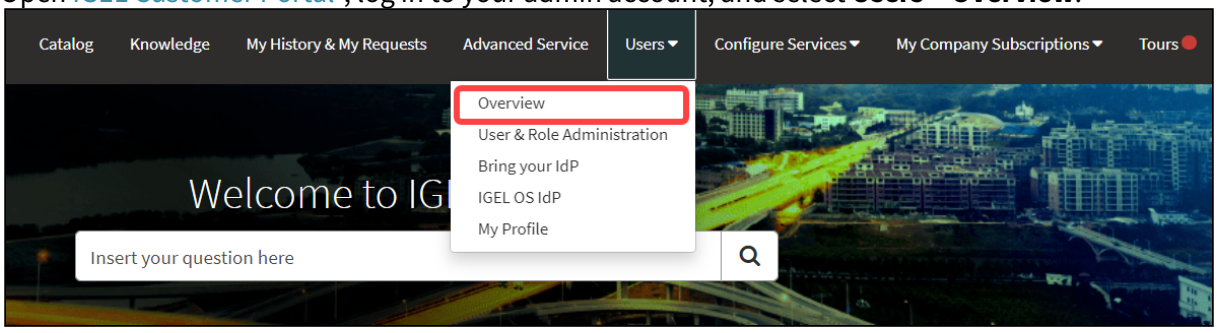
Canceling and Resending Invitations

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.

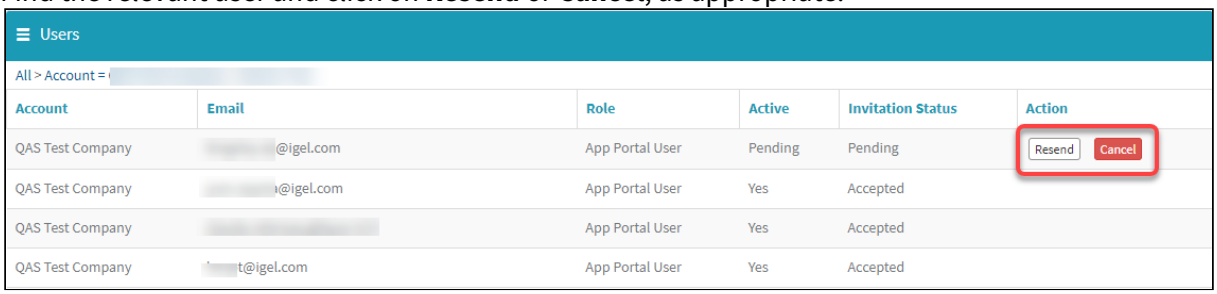
1. Open IGEL Customer Portal[8], log in to your admin account, and select **Users > Overview**.



The users are listed.

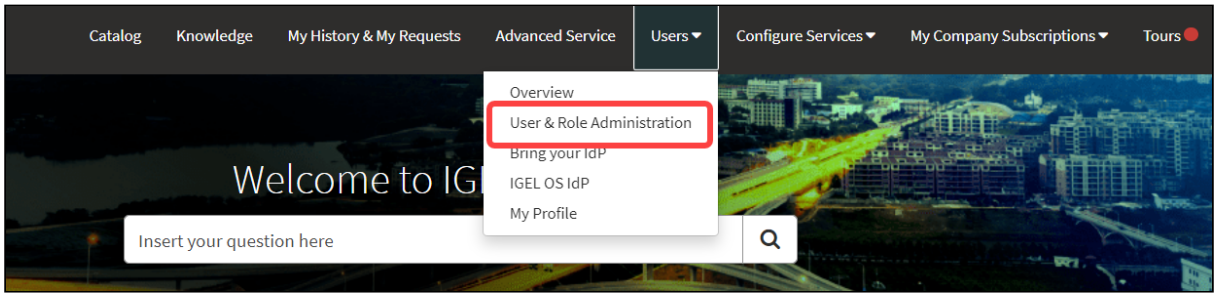
8 https://cosmos.igel.com/

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

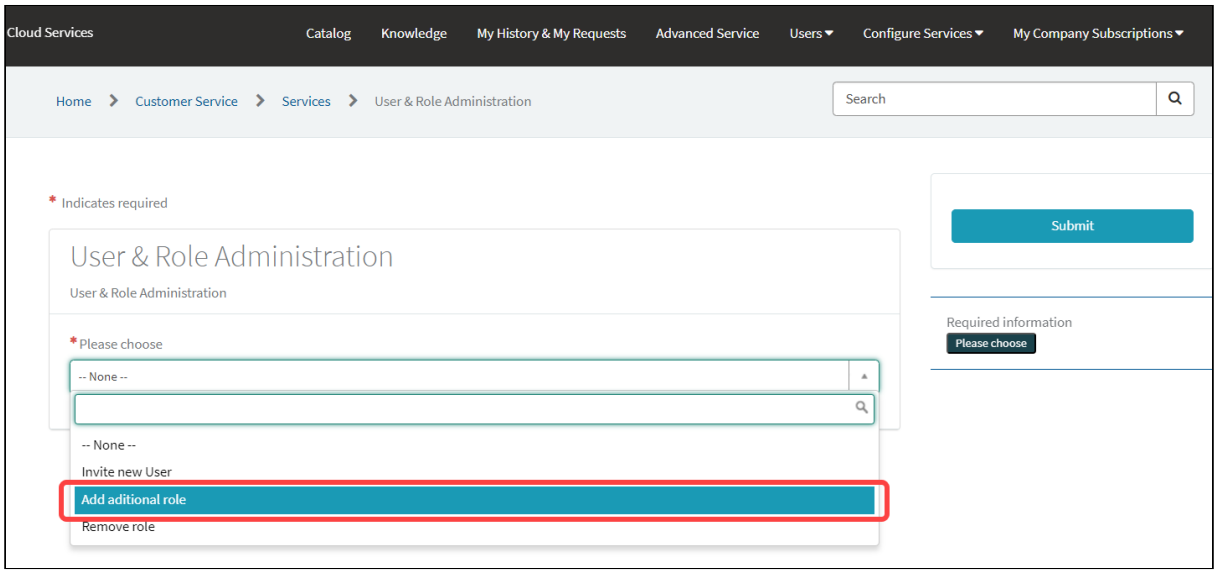


Adding a Role to an Existing User

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



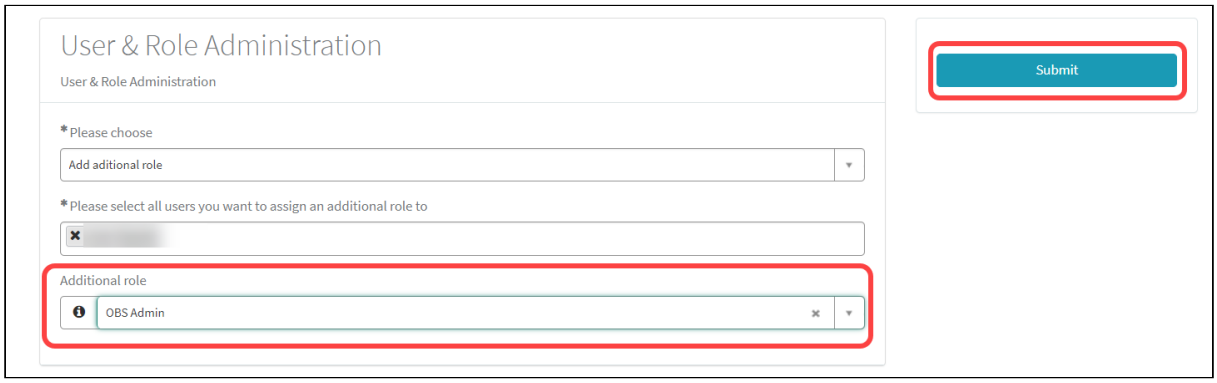
2. Select **Add additional role**.



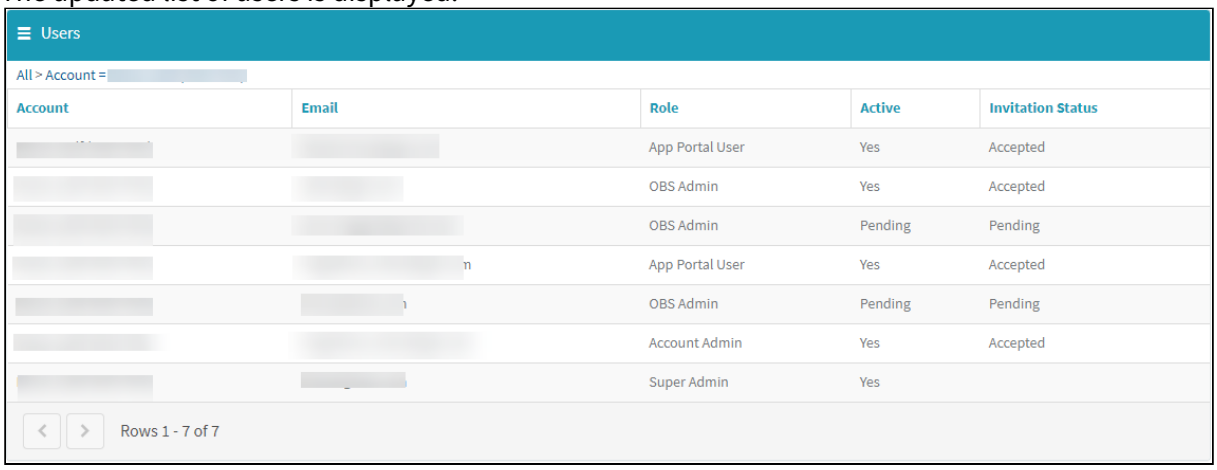
9 https://cosmos.igel.com/

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

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



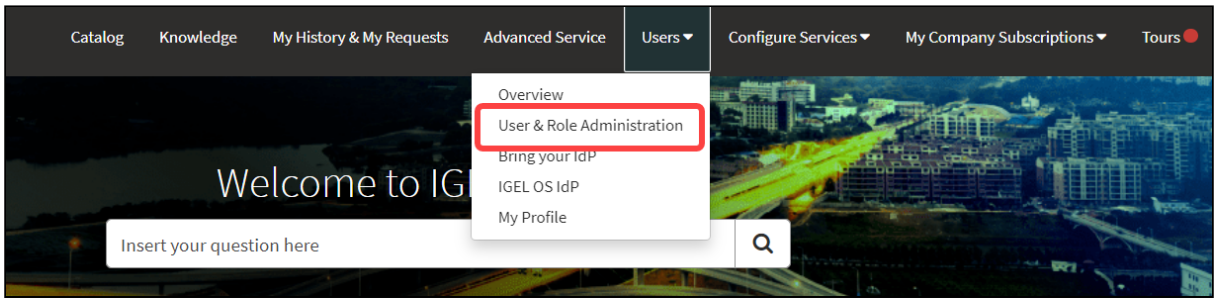
The updated list of users is displayed.



Removing a Role / Deactivating a User

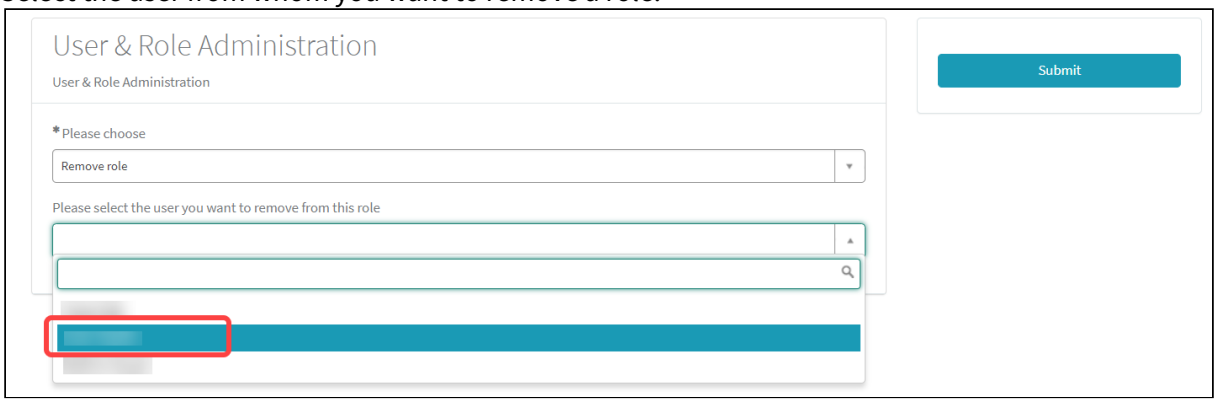
You can remove one or more rules from a user. If you deactivate a user, the account is deleted. No e-mails will be sent to this account anymore.

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



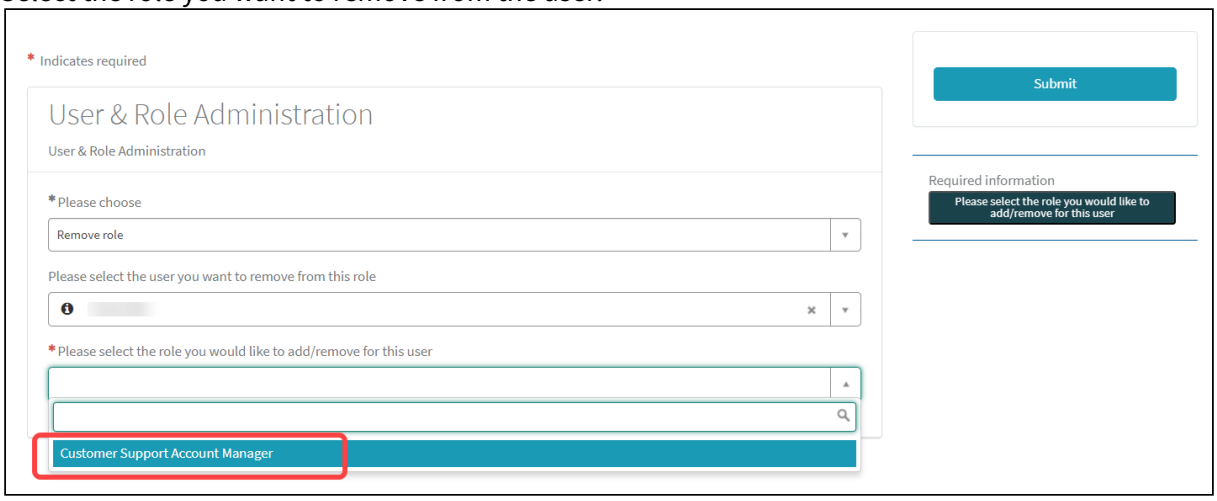
2. Select **Remove role**.

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

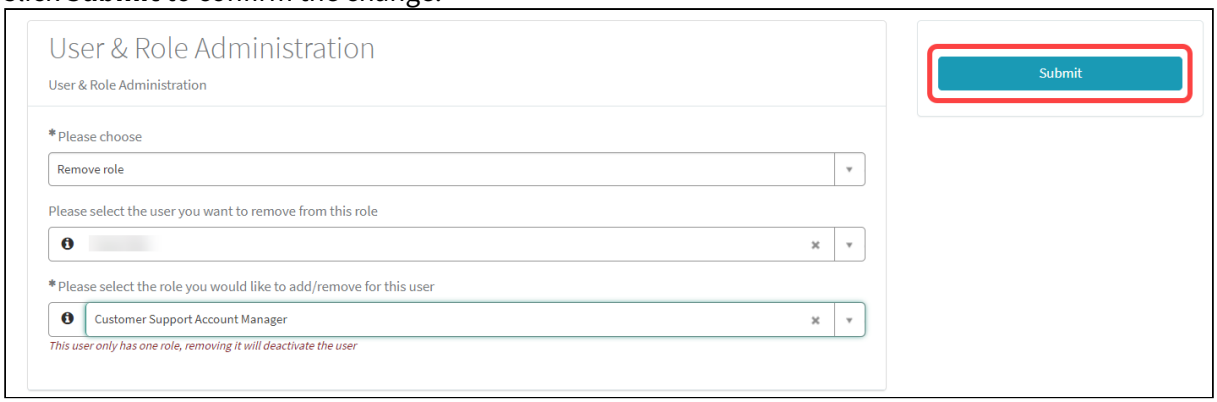


10 https://cosmos.igel.com/

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



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

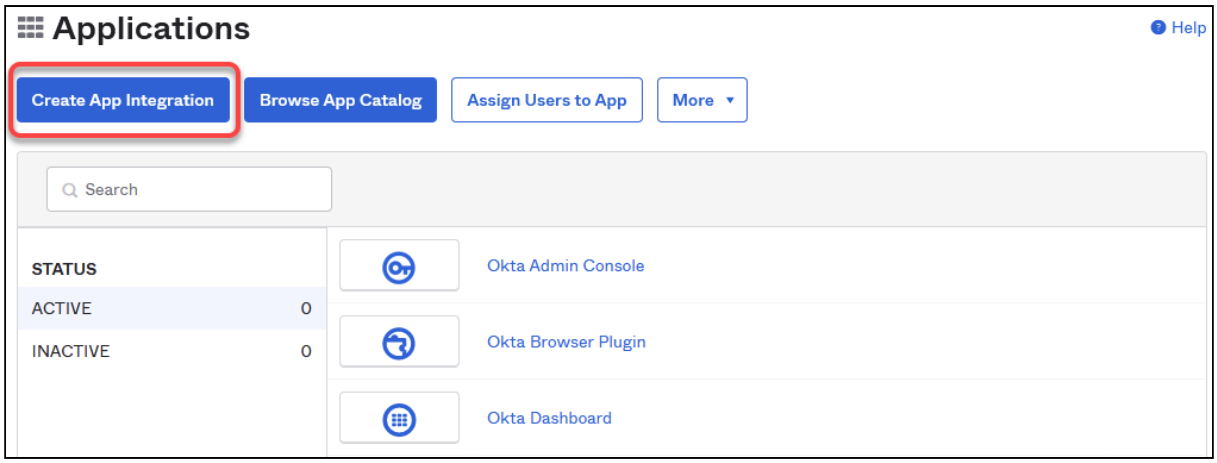


Using Okta as Federated Identity Provider

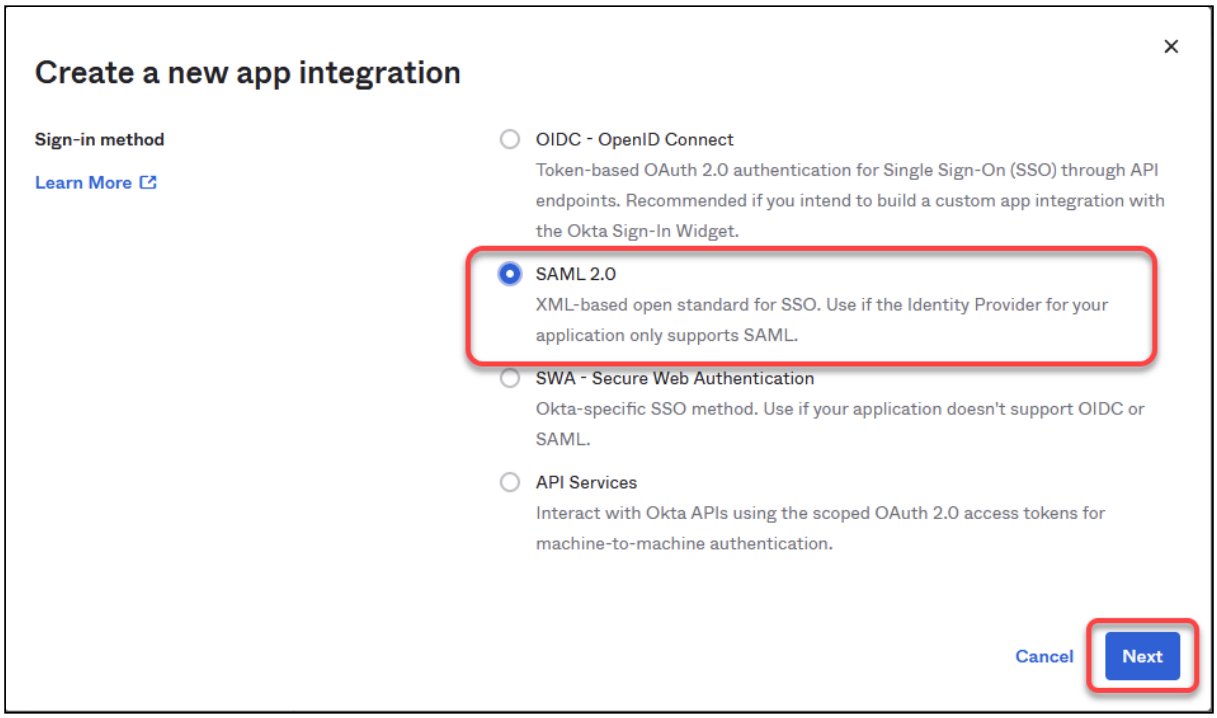
Setting Up an App Integration in Okta

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.

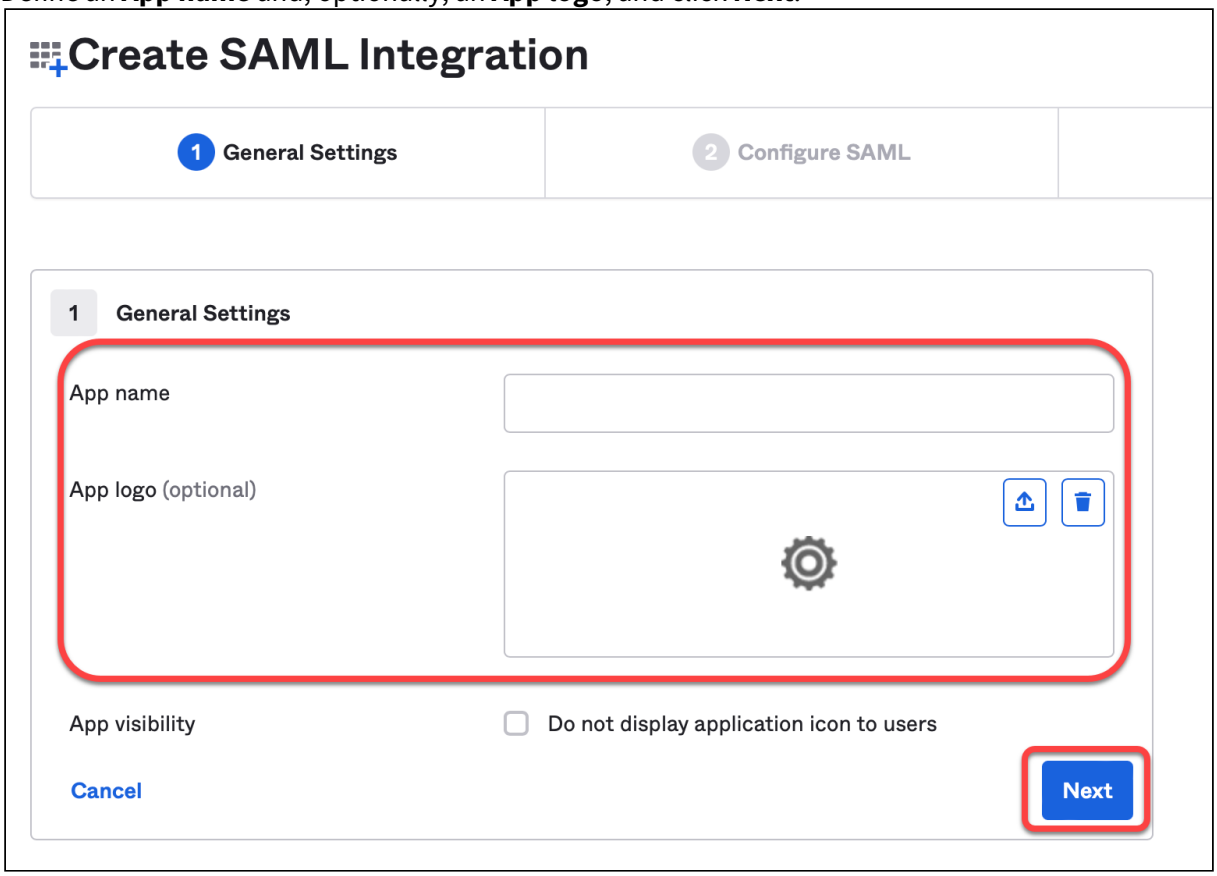
1. Log in to your administrator account at Okta, go to **Applications**, and click **Create App integration**.



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

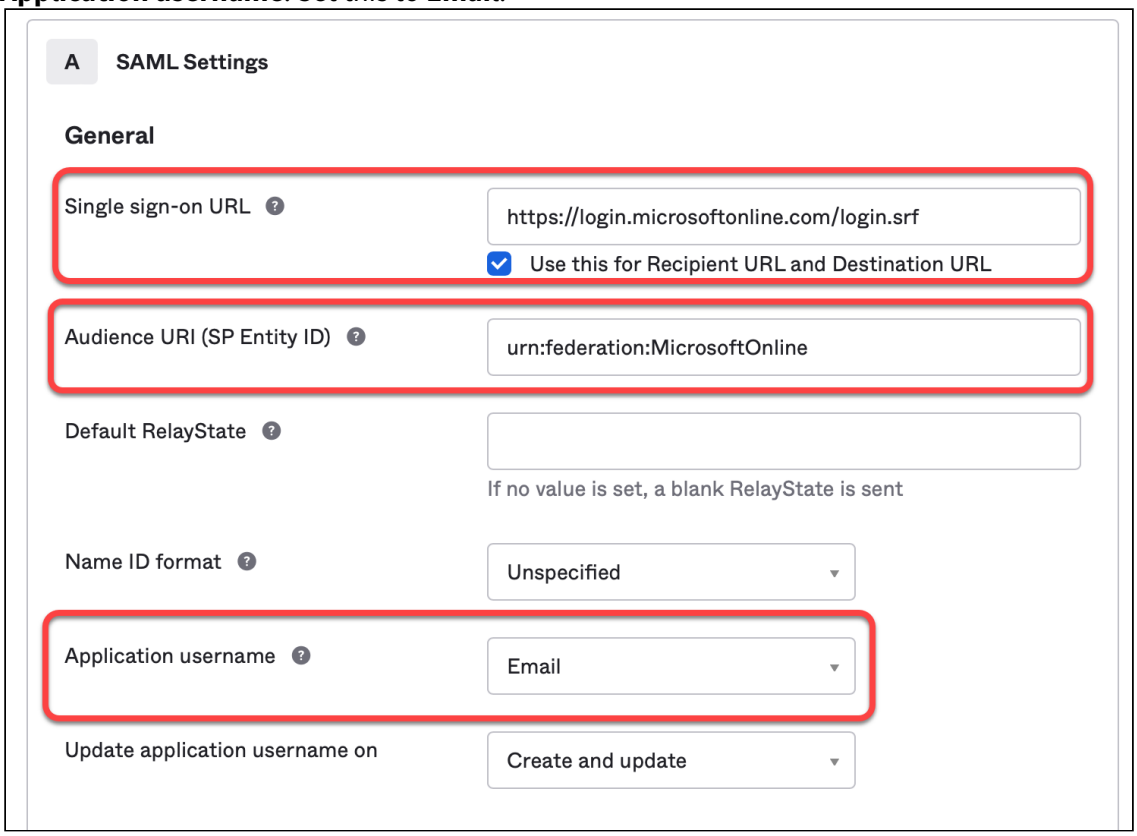


3. Define an **App name** and, optionally, an **App logo**, and click **Next**.

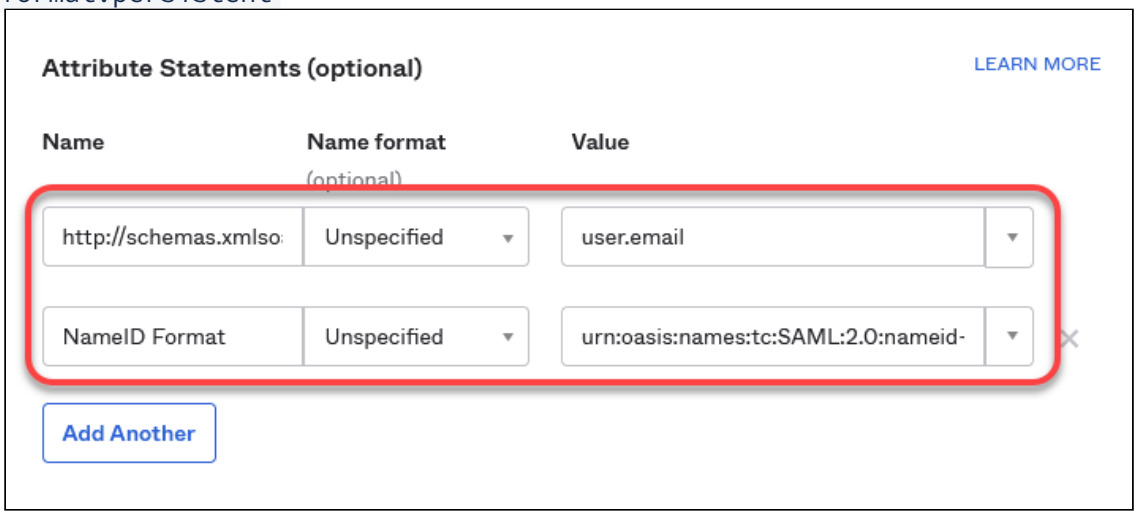


4. Edit the SAML connection details as follows:
   - **Single sign on URL**: Enter `https://login.microsoftonline.com/login.srf`
   - **Use this for Recipient URL and Destination URL**: Activate this checkbox.
   - **Audience URI (SP Entity ID)**: Enter `urn:federation:MicrosoftOnline`

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



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`

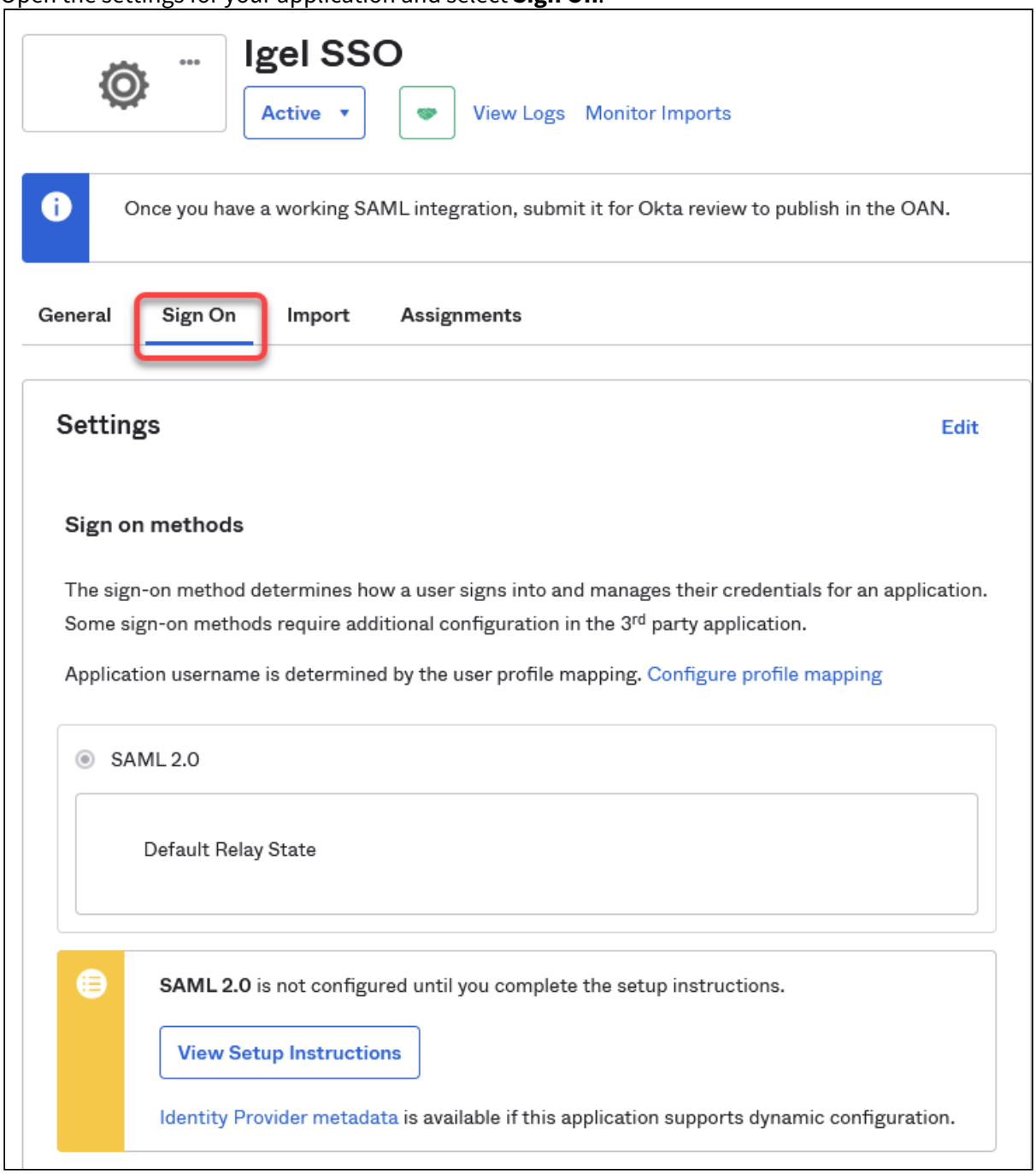


6. Finish your app integration.

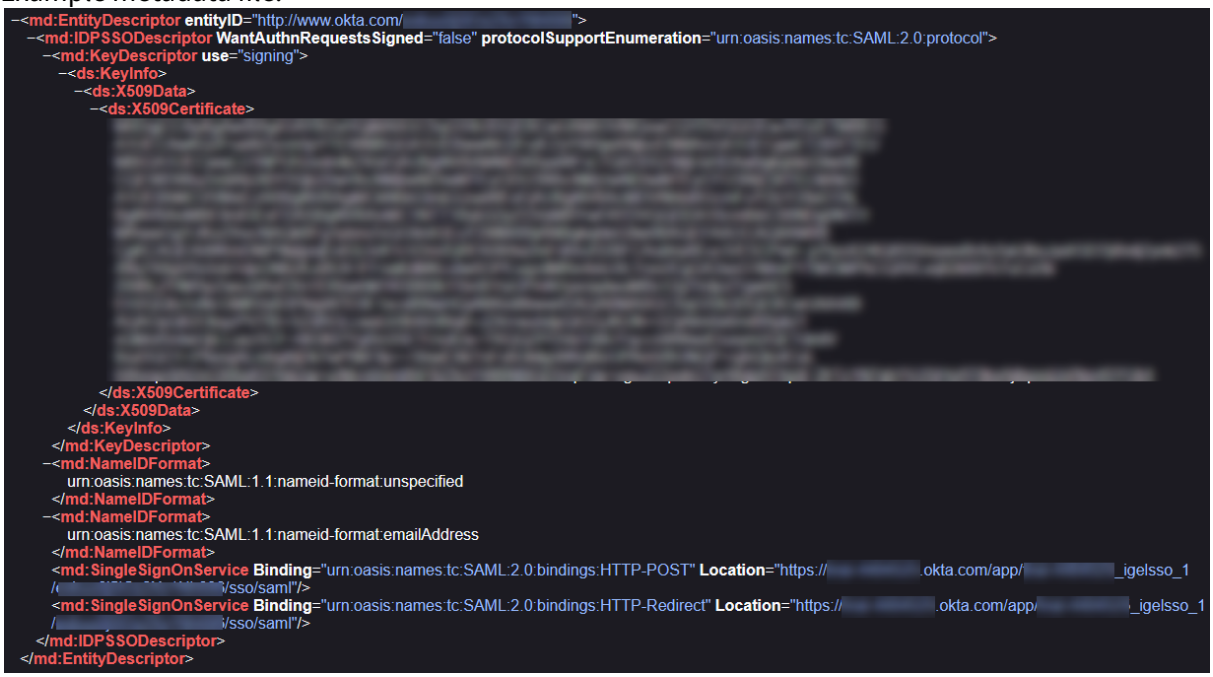
Extracting the SAML 2.0 Connection Data

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**.

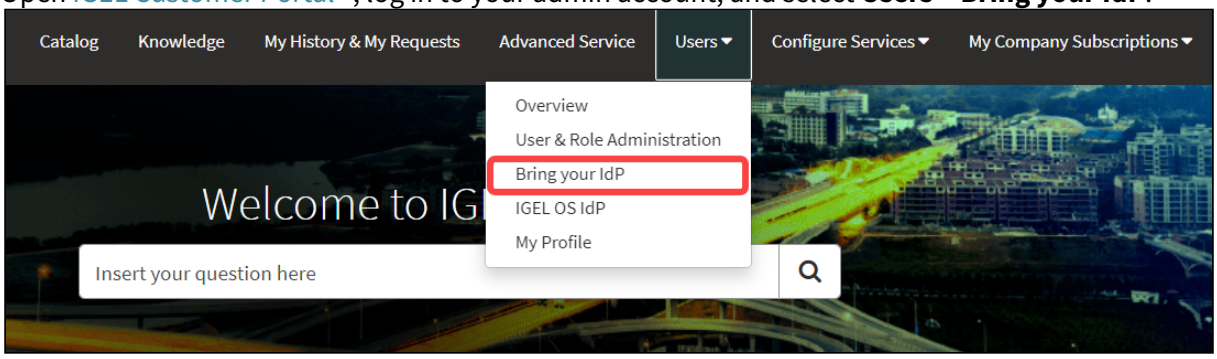


2. Click on the link **Identity Provider metadata** to download the data we will use afterward for configuring the IGEL Onboarding Service (OBS). The data is contained in an XML file. Also, note down the URL from this link, as we will need it later on.
Example metadata file:



Configuring Okta as Your Federated IdP

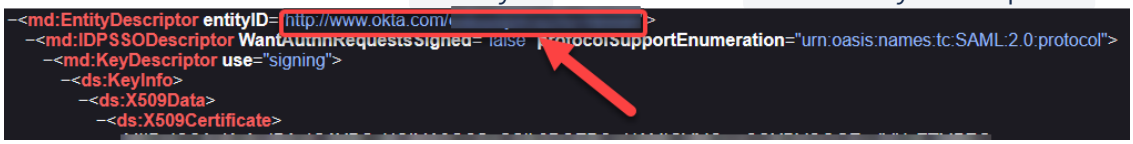
1. Open IGEL Customer Portal[11], log in to your admin account, and select **Users > Bring your IdP**.



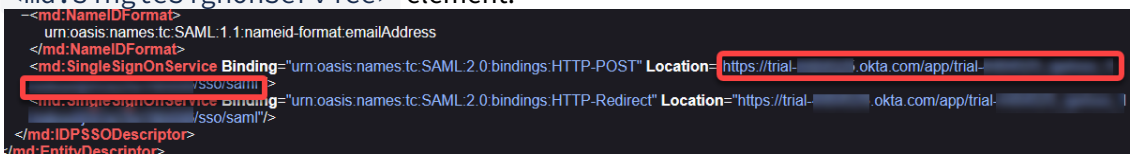
2. Enter the following data from your metadata file:

11 https://cosmos.igel.com/

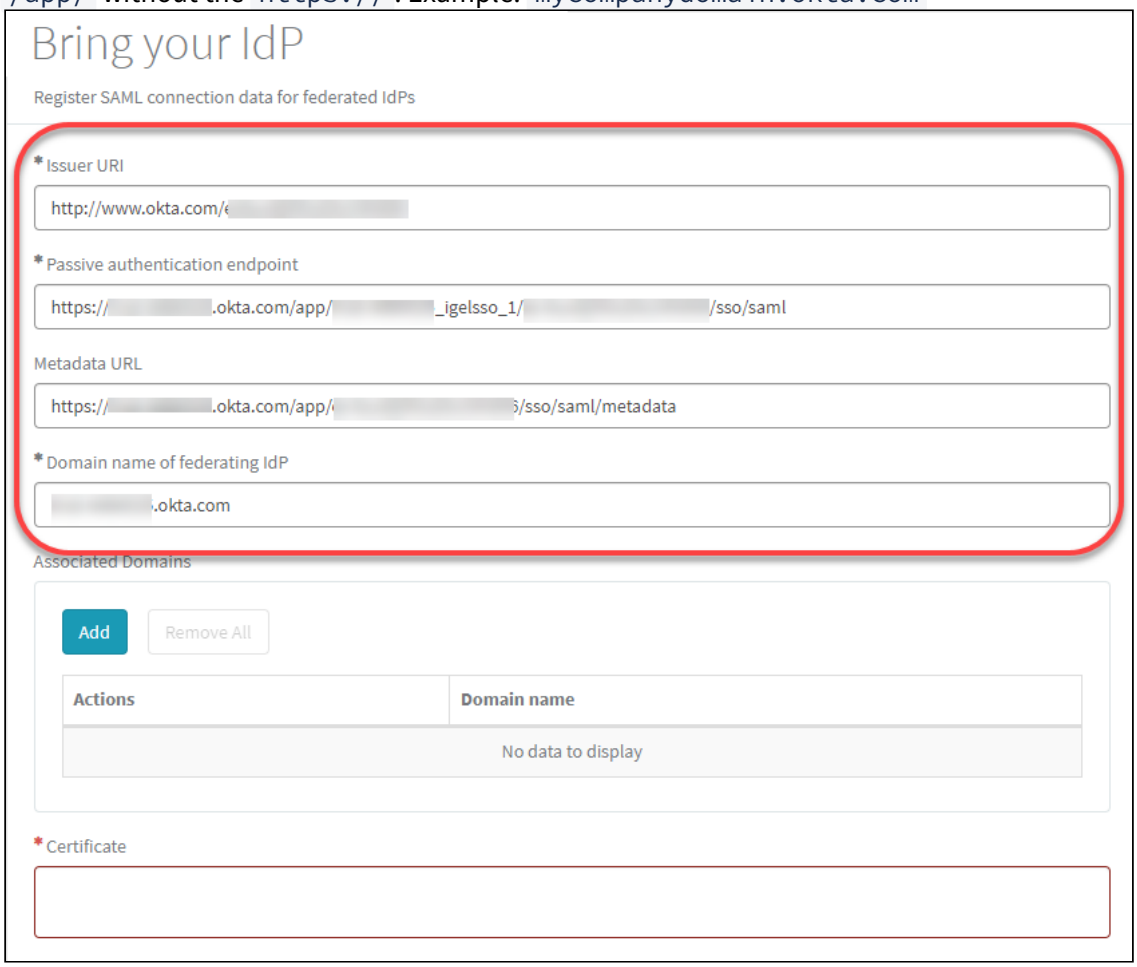
- **Issuer URI**: Value of the attribute `entityID` of the element `<md:EntityDescriptor>`



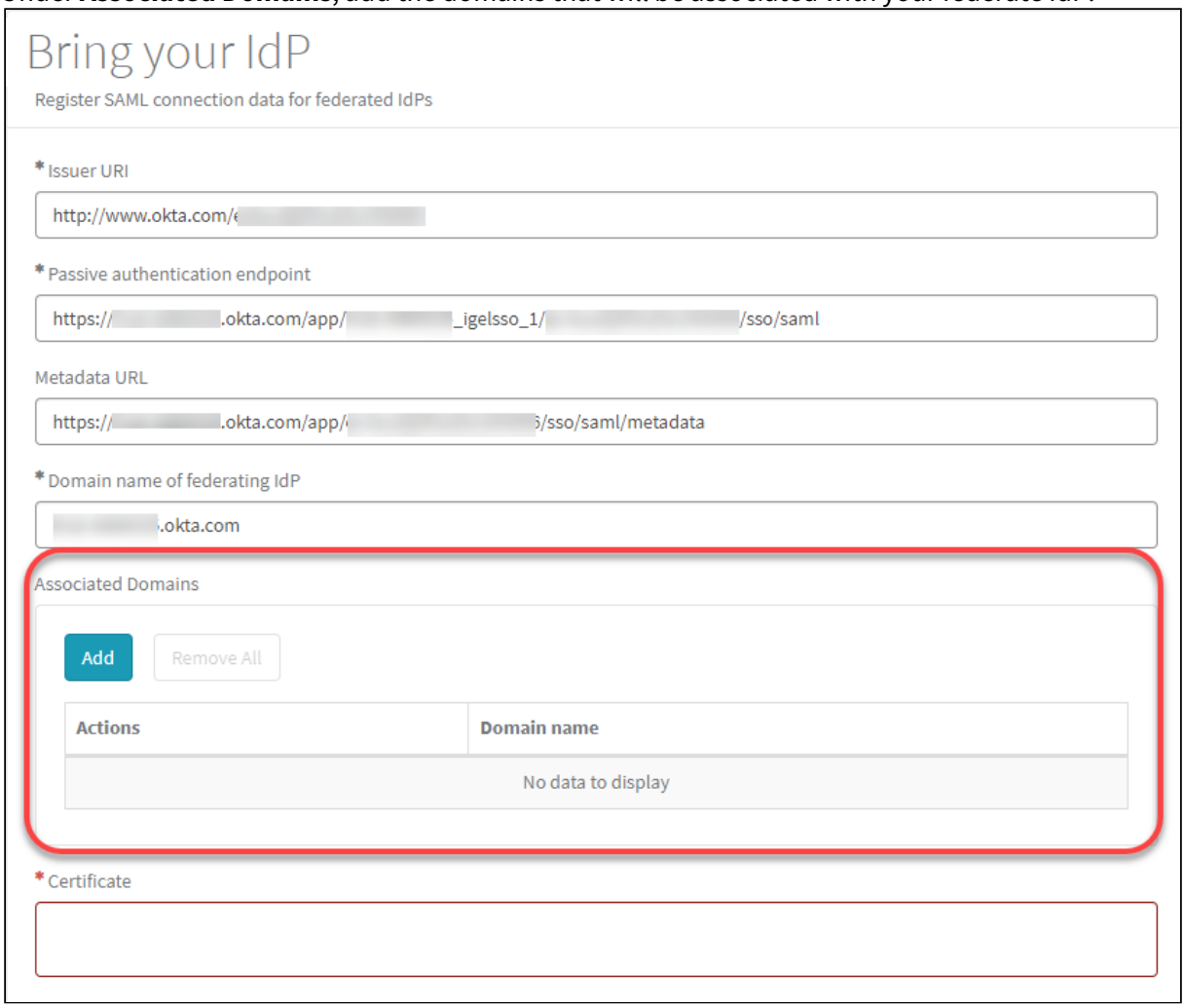
- **Passive authentication endpoint**: Enter the value of the `Location` attribute of the `<md:SingleSignOnService>` element.



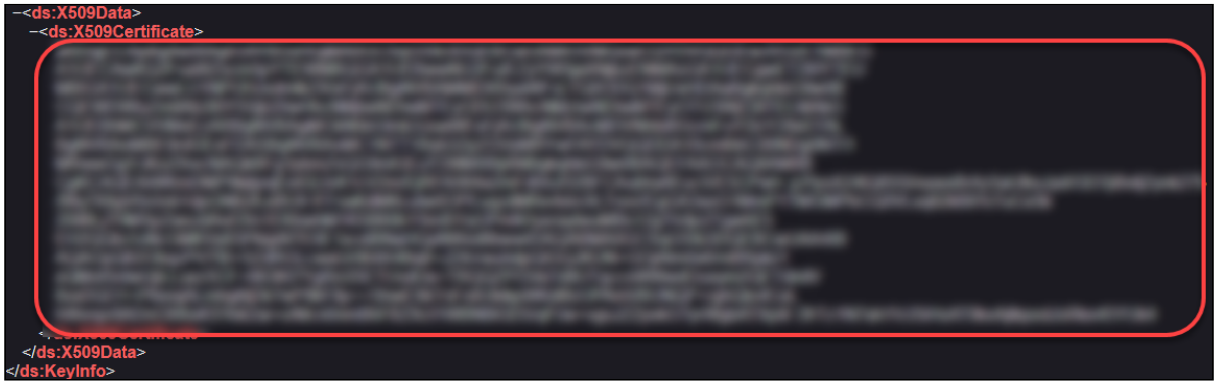
- **Metadata URL**: Enter the URL of the link **Identity Provider metadata** you have used before to download the metadata file.
- **Domain name of federating IdP**: The part of **Passive authentication endpoint** before the `/app/` without the `https://`. Example: `mycompanydomain.okta.com`

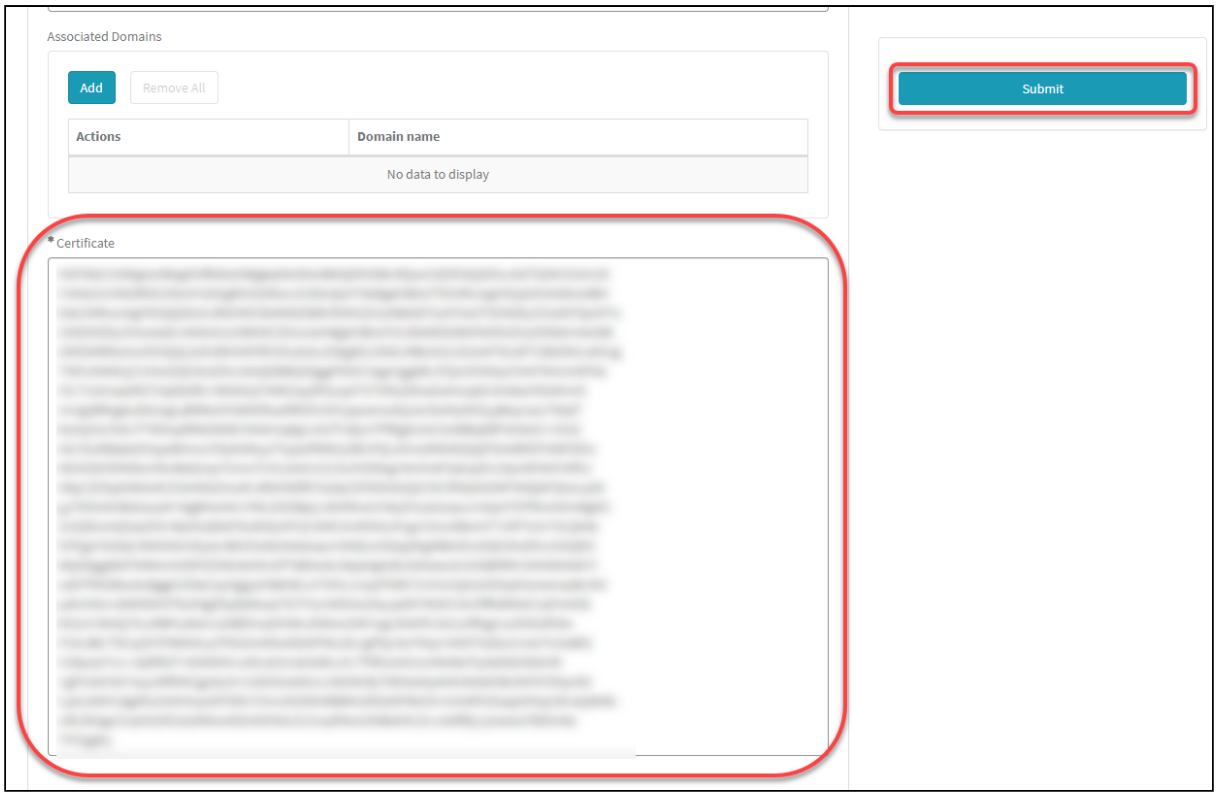


3. Under **Associated Domains**, add the domains that will be associated with your federate IdP.



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



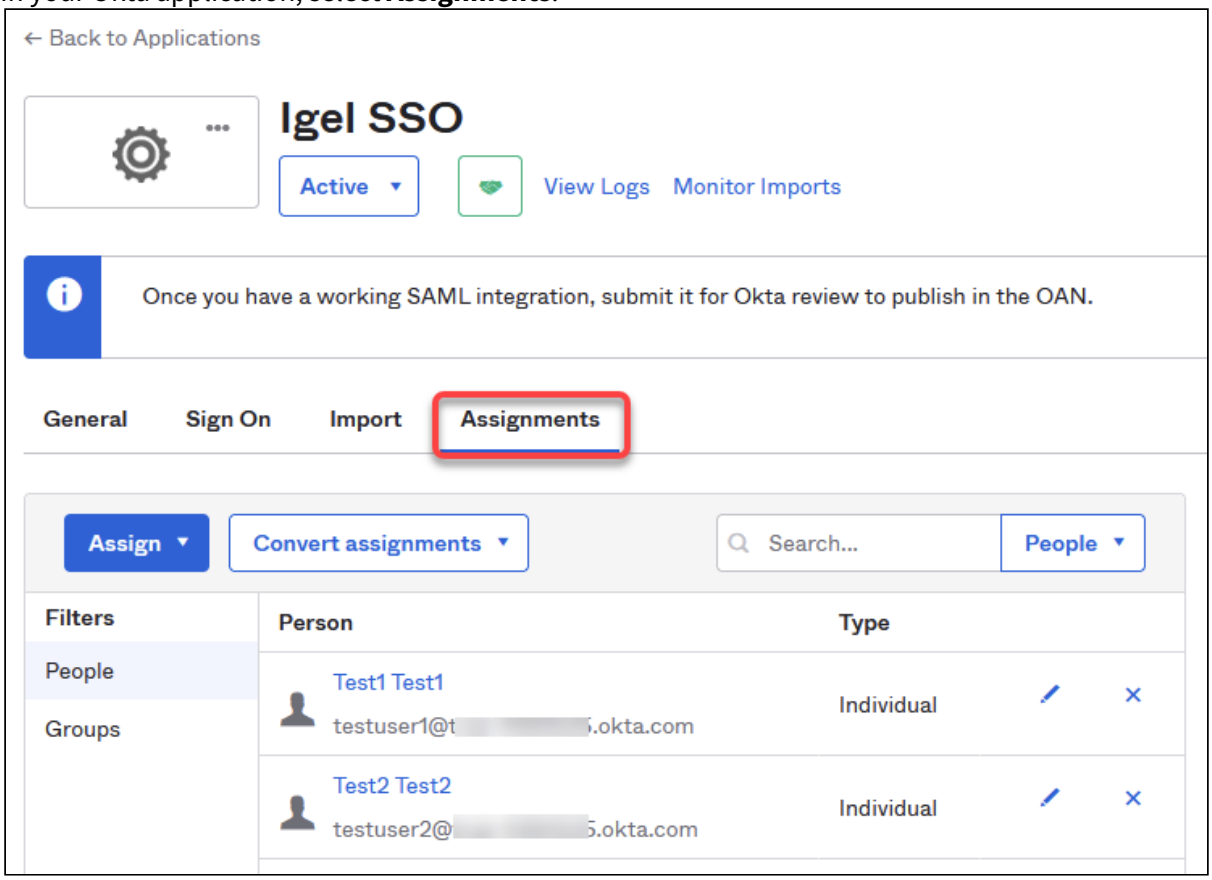


Assigning the Application to the Users

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**.



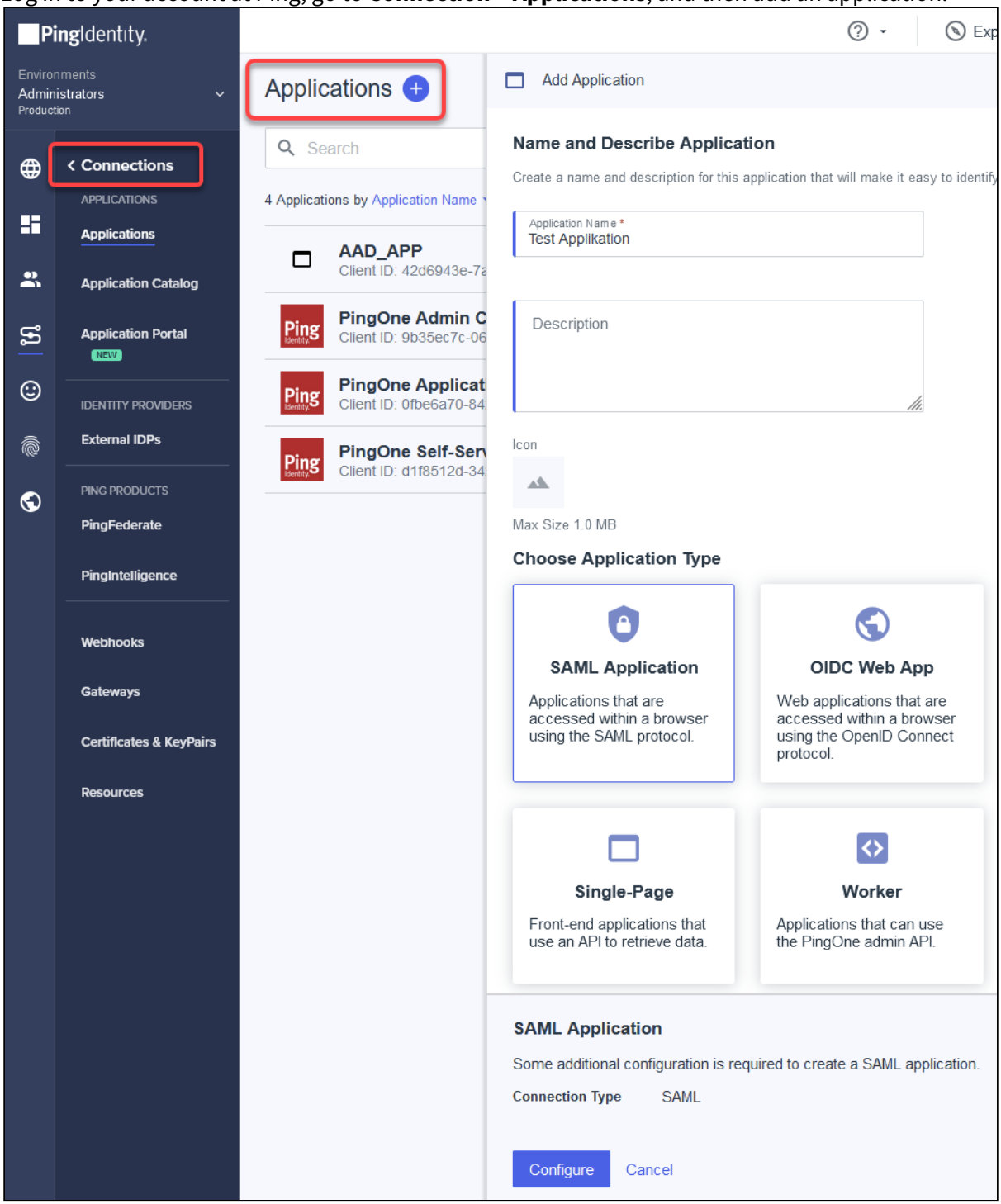
2. Assign the users to our new application.

Using Ping as Federated Identity Provider

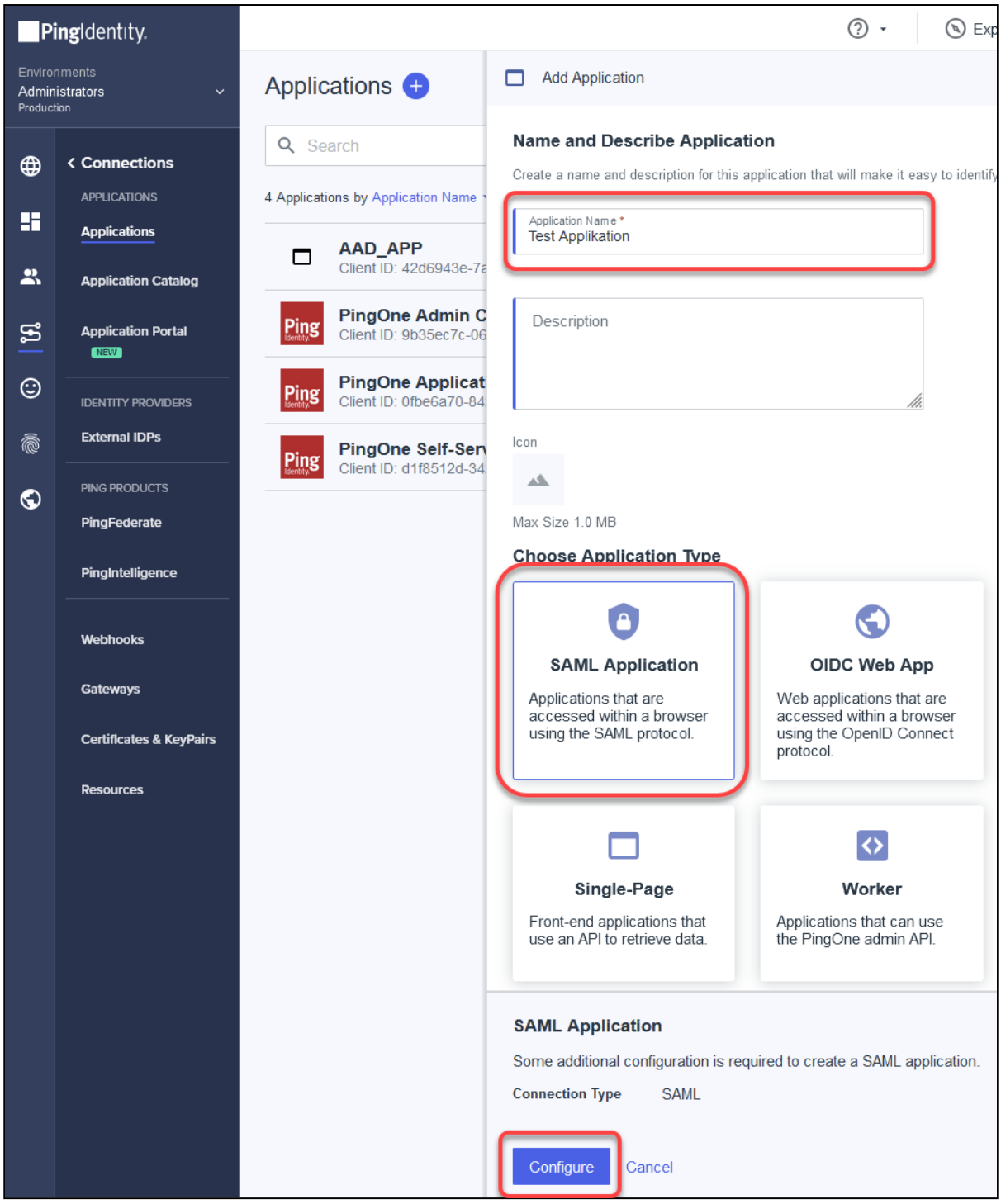
Setting Up an App Integration in Ping

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.

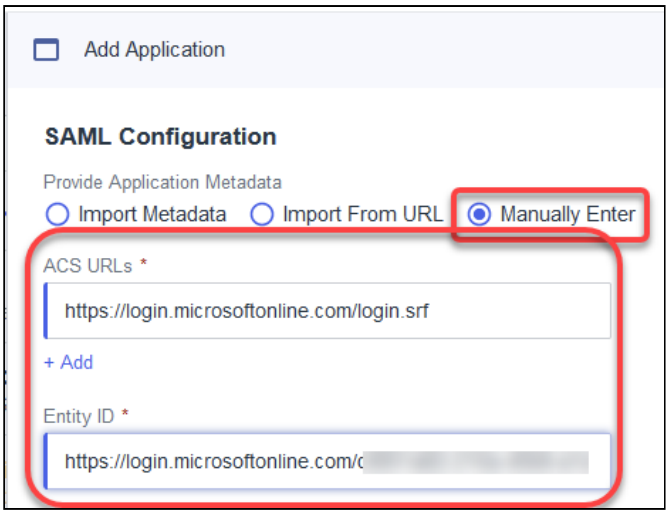
1. Log in to your account at Ping, go to **Connection > Applications**, and then add an application.



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

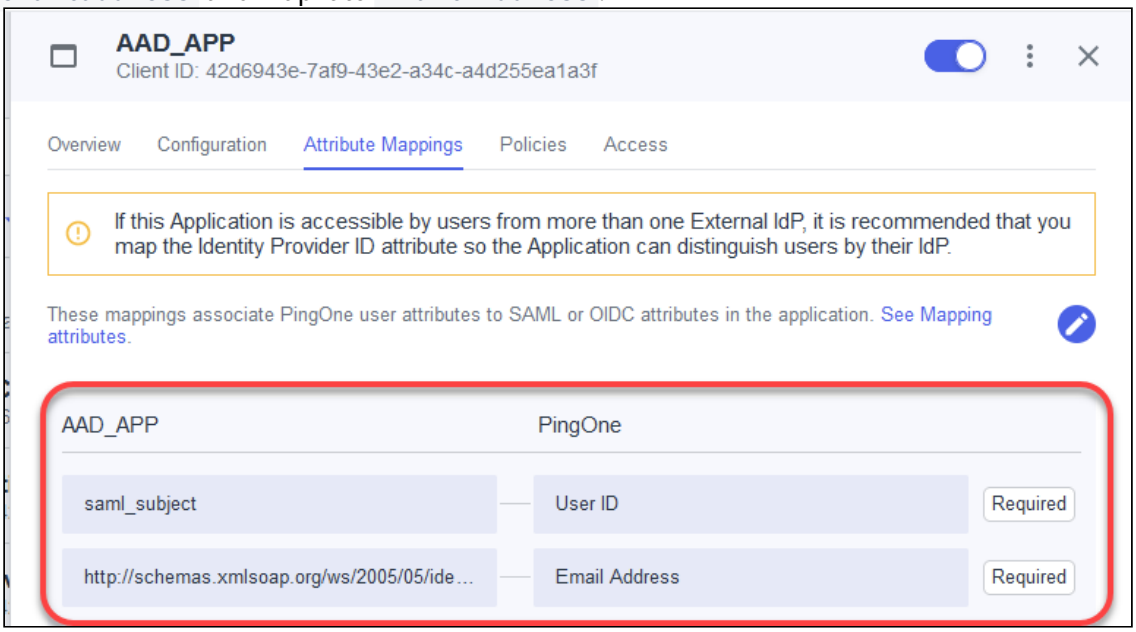


3. In the **SAML Configuration** dialog, select **Manually Enter** and enter the following data:
   - **ACS URLs**: Enter `https://login.microsoftonline.com/login.srf`
   - **Entity ID**: Enter the prefix `https://login.microsoftonline.com/` followed by the Azure Active Directory tenant ID.



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`.

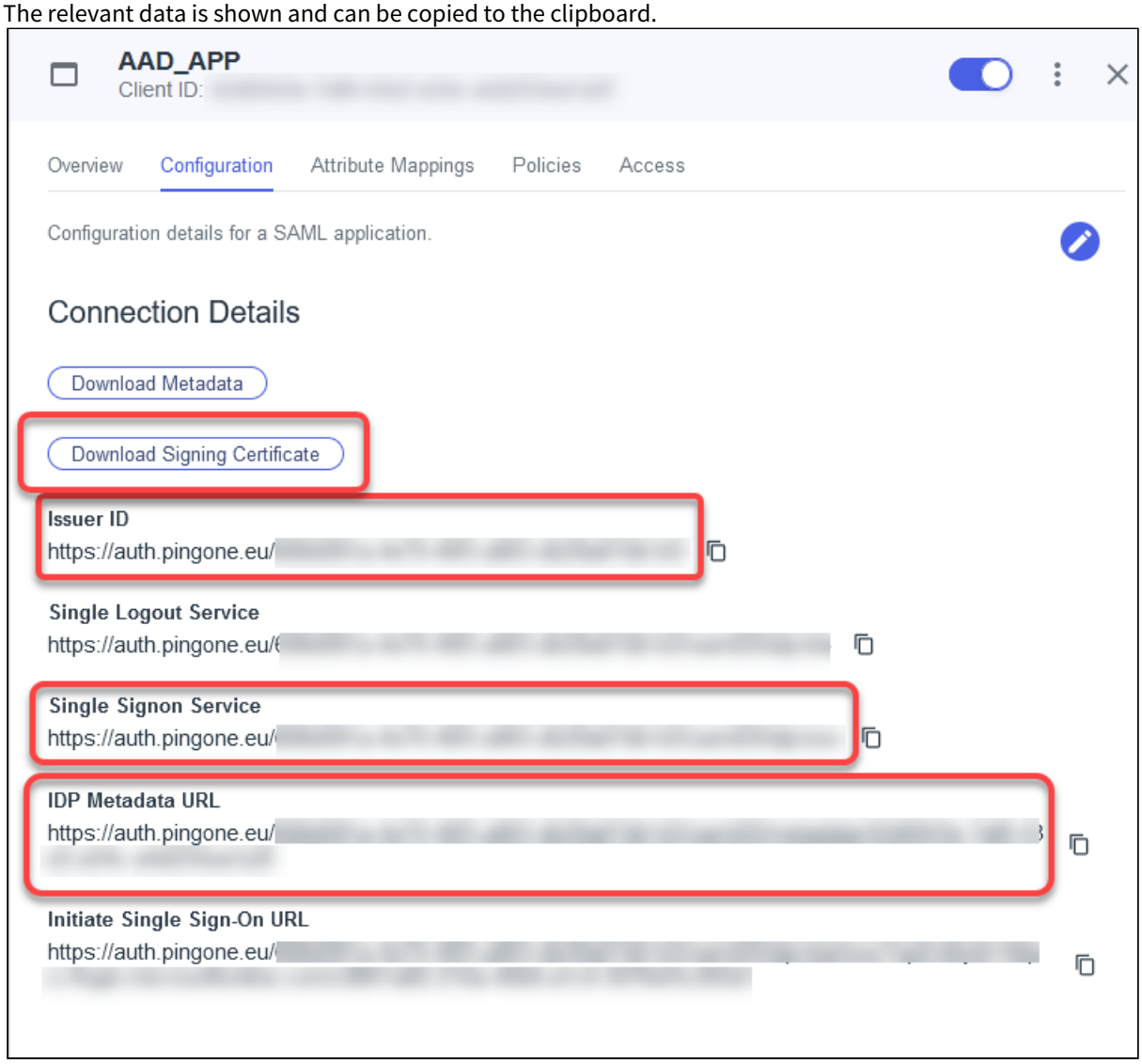


6. Finish the application setup.

Obtaining the SAML 2.0 Connection Data

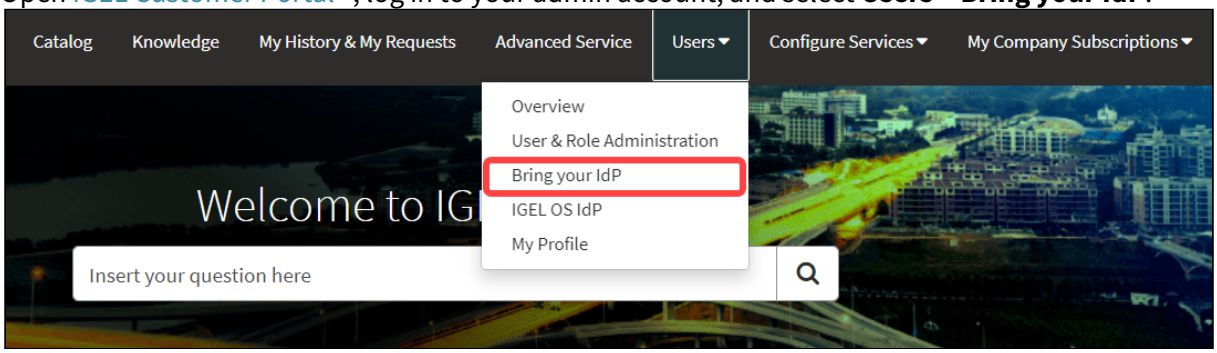
In this step, we will get the connection data which will be used for creating an external identity that will be used for the IGEL Onboarding Service (OBS).

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



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:

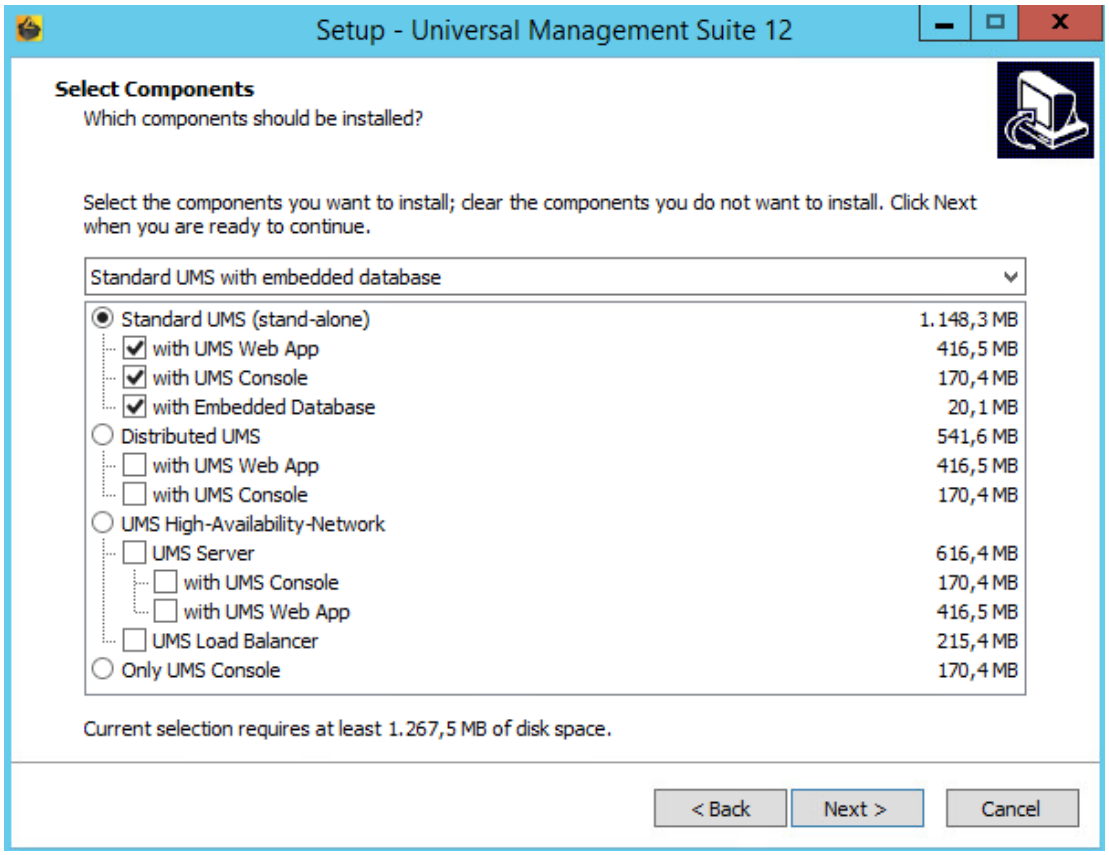
- ICG Manual
- ICG Prerequisites

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/



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

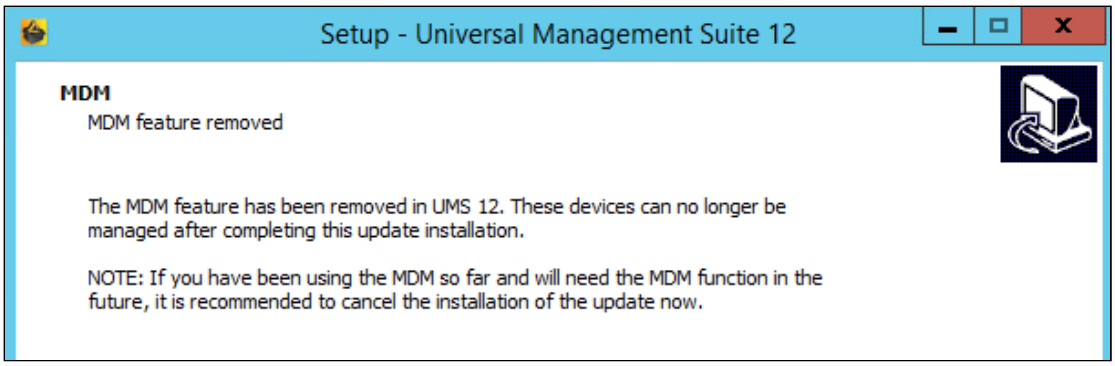
If you participated in the program for validation and testing of IGEL OS 12, you can also update to UMS 12.01.110 from
- UMS 12.00.900
- UMS 12.01.x

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:



- 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

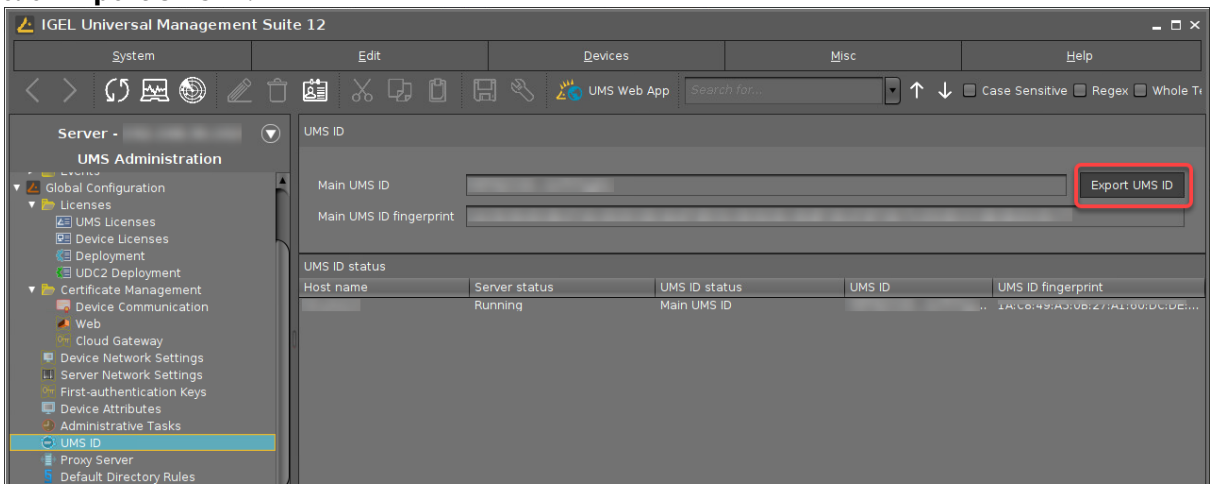
To authenticate your UMS to the IGEL Cloud Services, you must register your UMS. This involves uploading the UMS ID, which is essentially a certificate of your UMS, to the IGEL Customer Portal.

> 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.

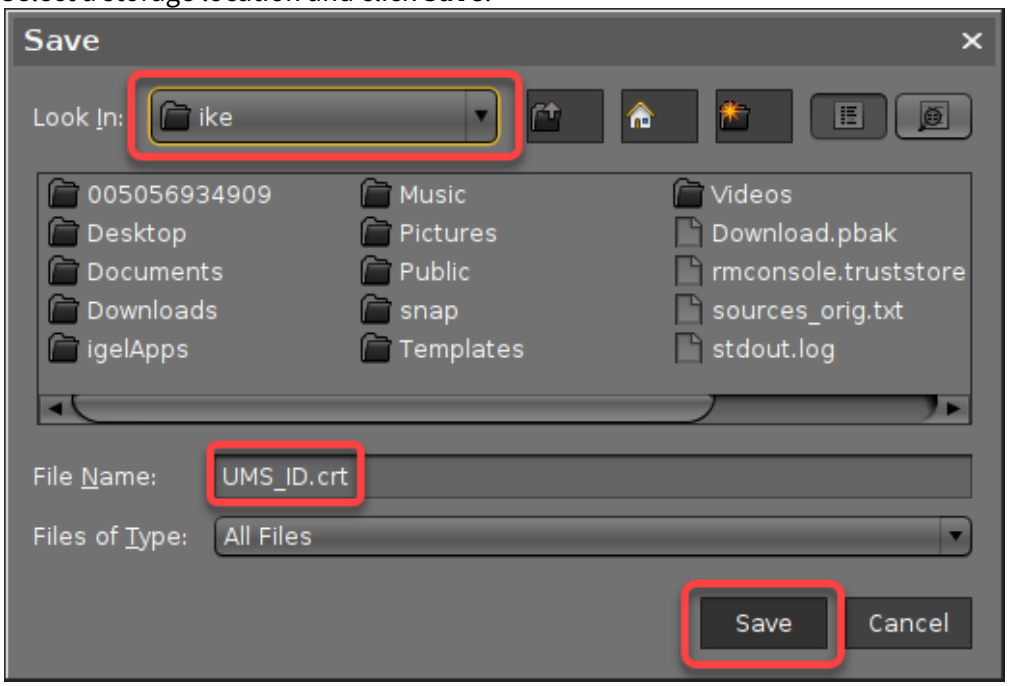
Exporting the UMS ID

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

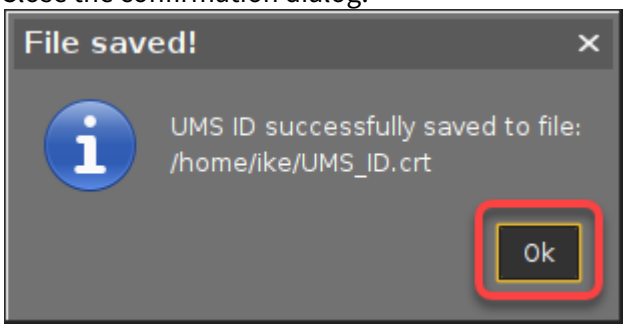
1. Open your UMS Console, go to **UMS Administration > Global Configuration > UMS ID**, and click **Export UMS ID**.



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



3. Close the confirmation dialog.

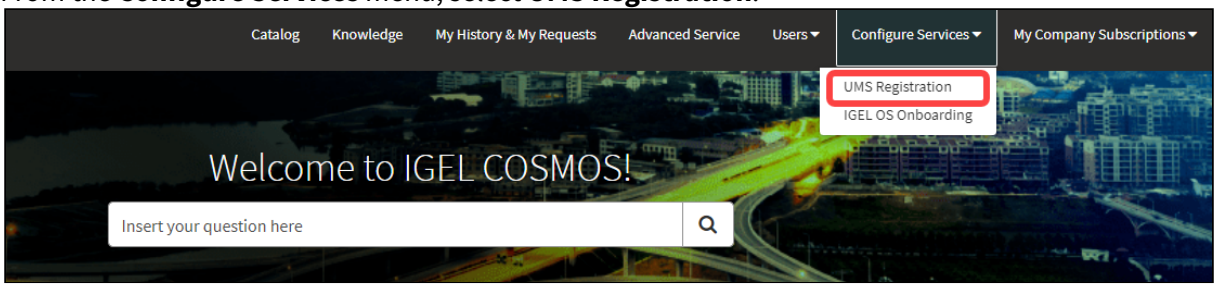


Registering the UMS

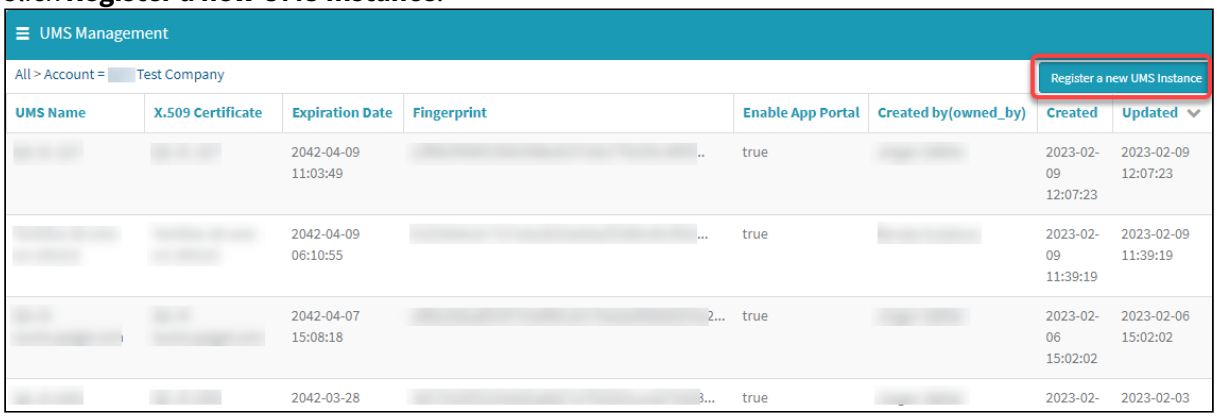
1. Open IGEL Customer Portal[14] in your browser and log in to your admin account.

14 https://cosmos.igel.com/

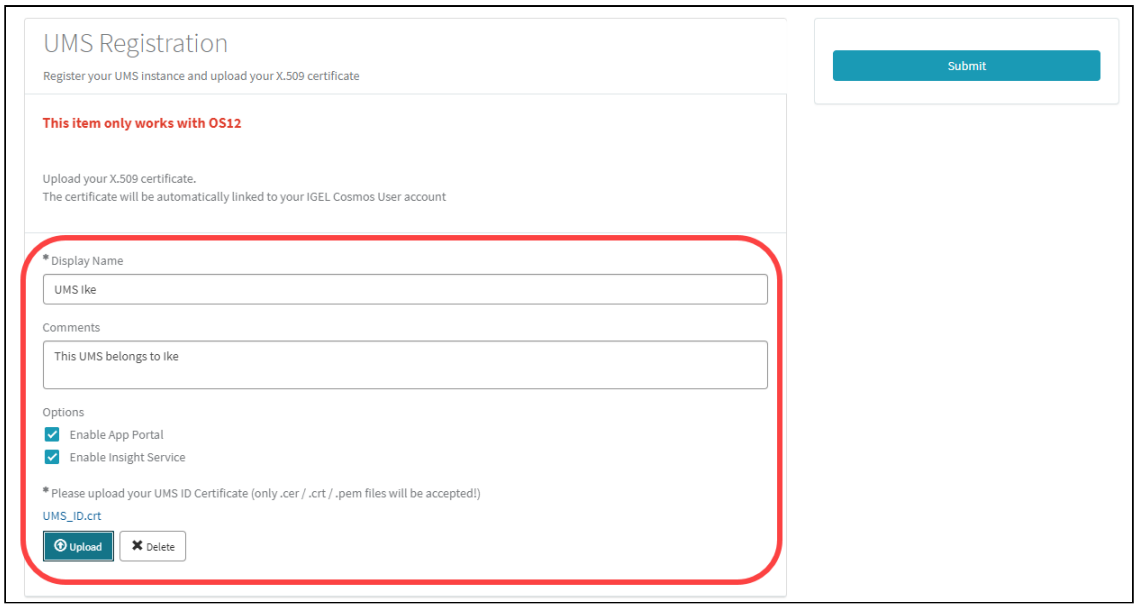
2. From the **Configure Services** menu, select **UMS Registration**.



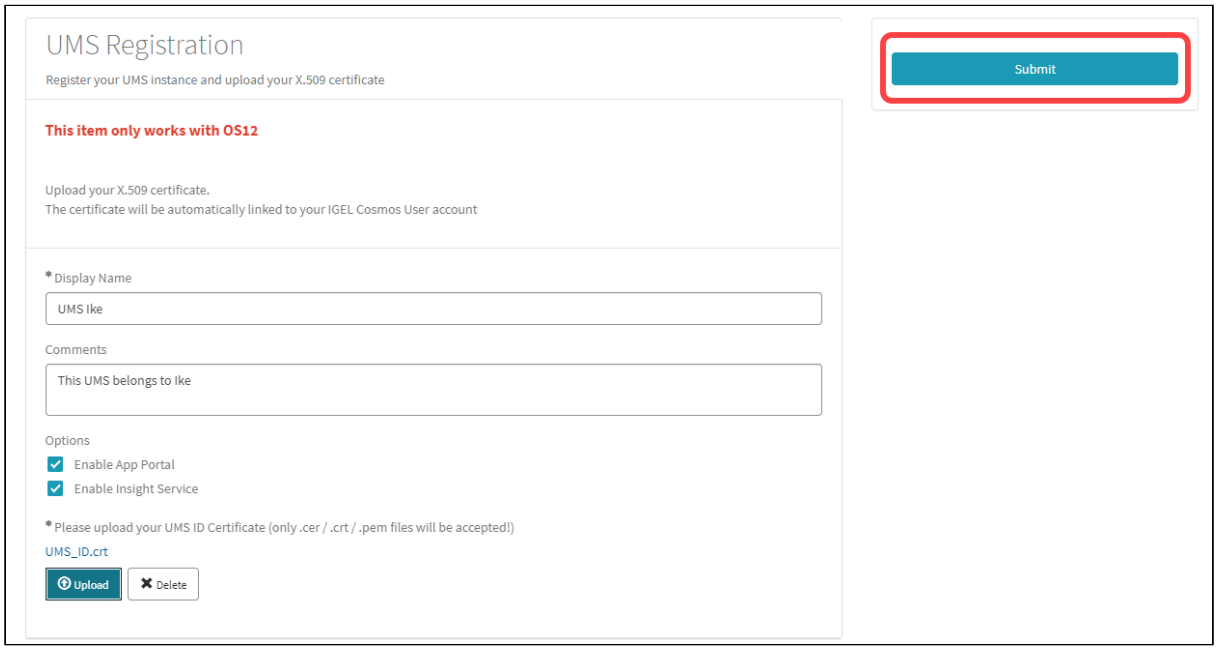
3. Click **Register a new UMS Instance**.



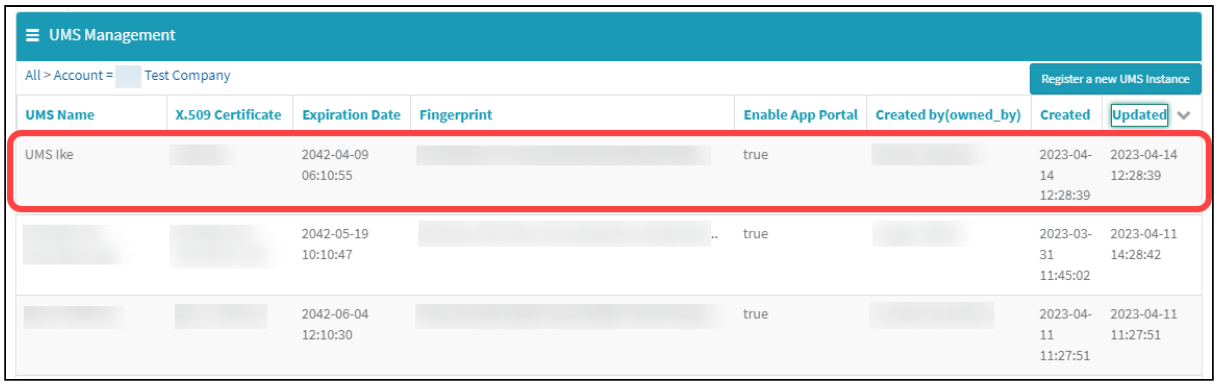
4. Edit the data as follows:
   - **UMS Name**: Display name for your UMS
   - **Comments**: Optional comment
   - **Enable App Portal**: Must be activated to enable access to the App Portal by the UMS. Technically, this option allows the App Portal to request the UMS ID.
   - **Enable Insight Service**: 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 215).
   - **Required - Upload**: Upload the certificate file (UMS ID) of your UMS. Make sure that the certificate file has the extension `.cer`, `.crt`, or .pem



5. Click **Submit**.



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 = Test Company
Register a new UMS Instance
UMS Name
X.509 Certificate
Expiration Date
Fingerprint
Enable App Portal
Created by(owned_by)
Created
Updated
UMS Ike
2042-04-09 06:10:55
true
2023-04-14 12:28:39
2023-04-14 12:28:39
2042-05-19 10:10:47
true
2023-03-31 11:45:02
2023-04-11 14:28:42
2042-06-04 12:10:30
true
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 Azure AD, Ping Identity, Okta or other IdP.

As an alternative, you can use the IGEL Onboarding Service not with the UMS, but with the IGEL Cloud Gateway (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 Azure AD 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 Azure AD, Ping Identity, or Okta, see:

- Azure AD(see page 54)
- Okta(see page 79)
- Ping Identity(see page 91)

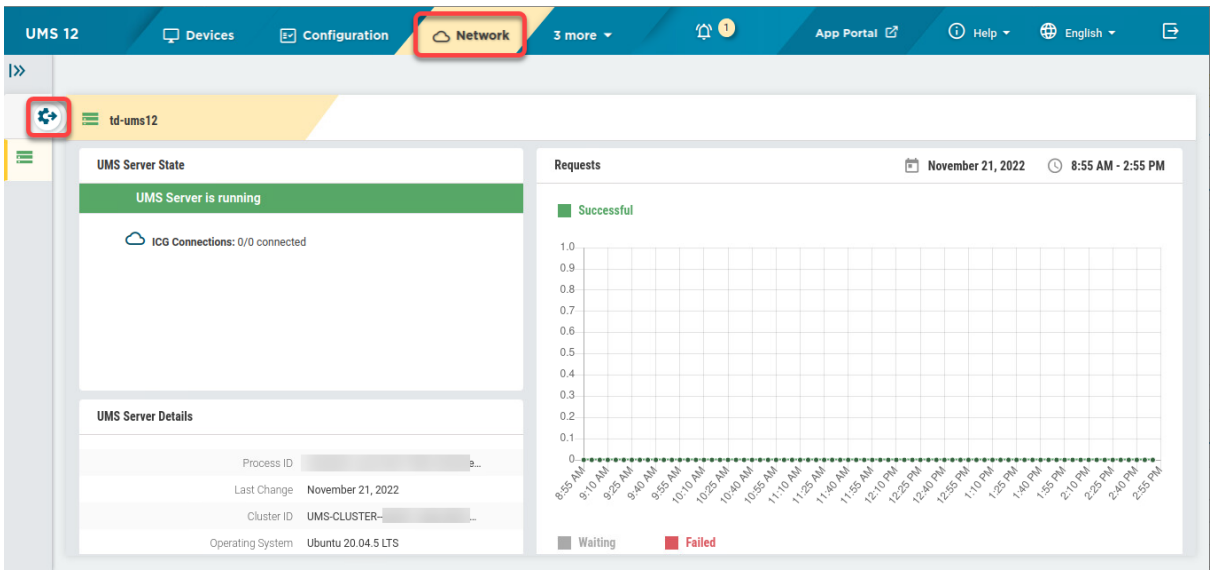
15 https://cosmos.igel.com/

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).

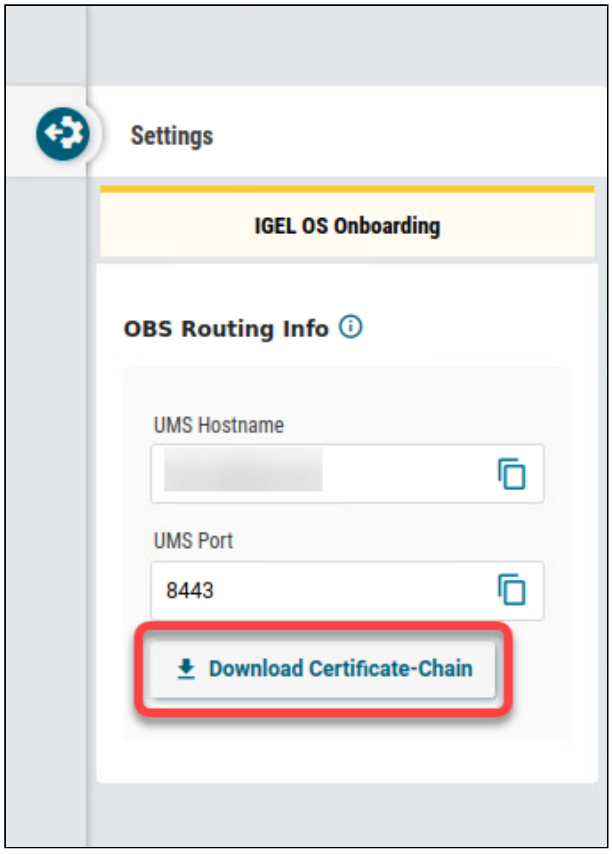
Of the UMS

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



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

3. Click **Download Certificate Chain**.



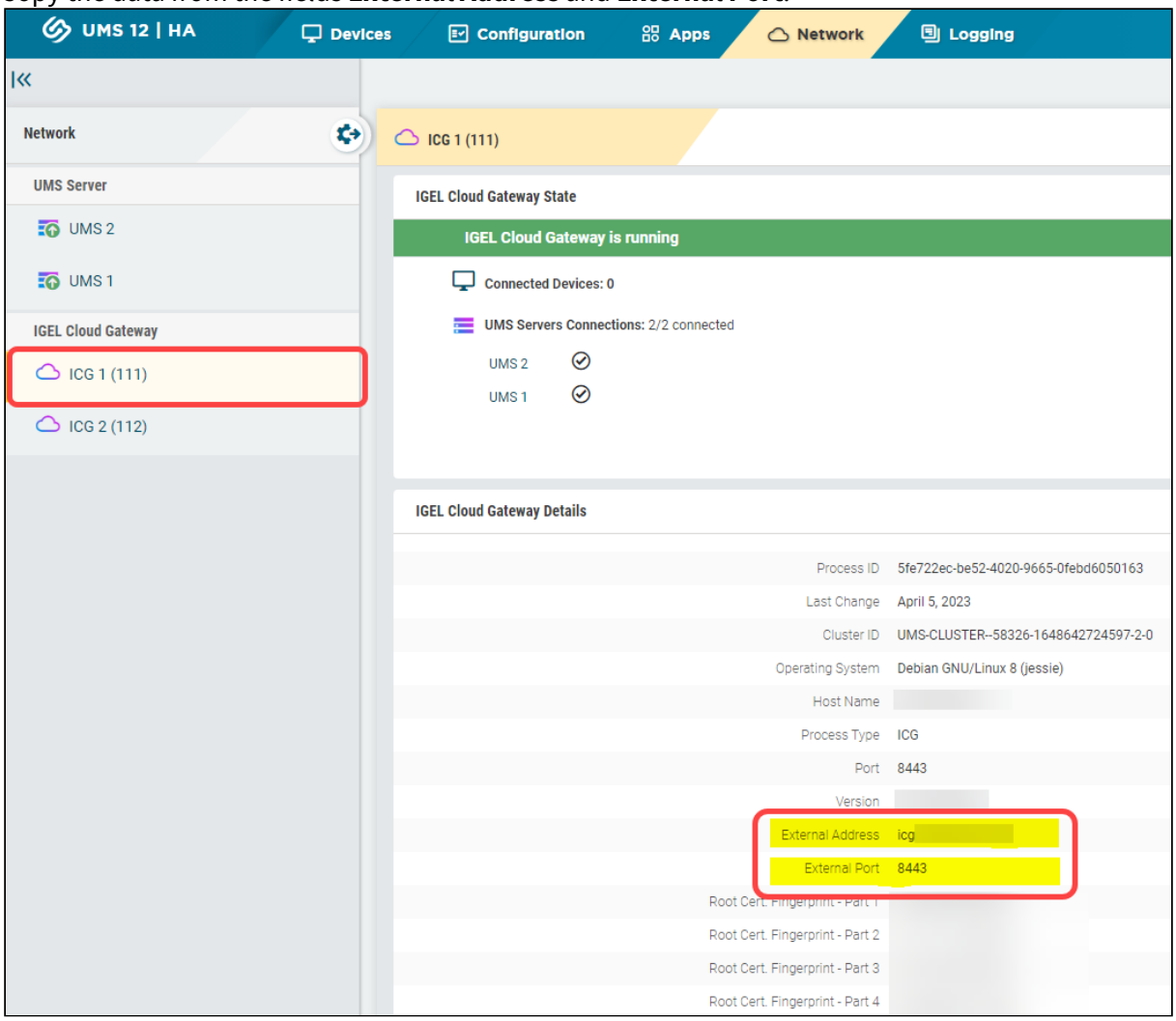
The certificate file is downloaded to your file system. In the following step, we will use it for the OBS routing.

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.

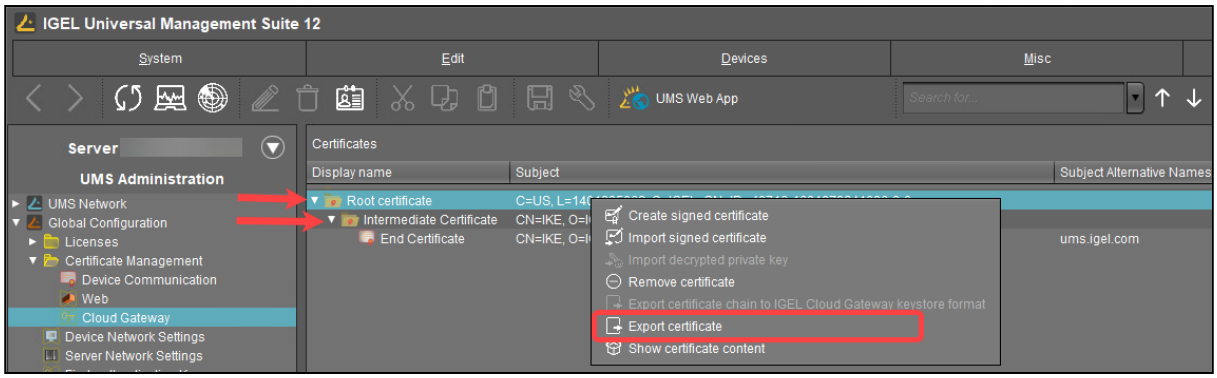
   If you have multiple ICG servers, it is possible to direct the OBS routing to one server only.

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



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.

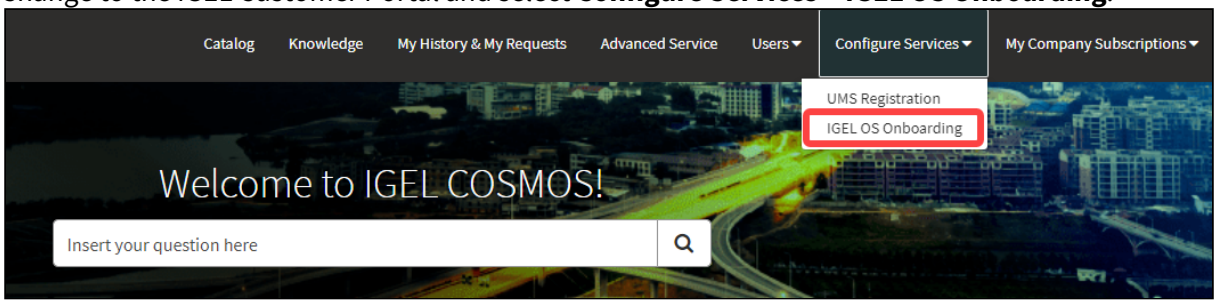


5. Copy the contents of each exported certificate in one file (the order of the certificates does not matter) and save the file as `icg_chain.crt`.
   Example:

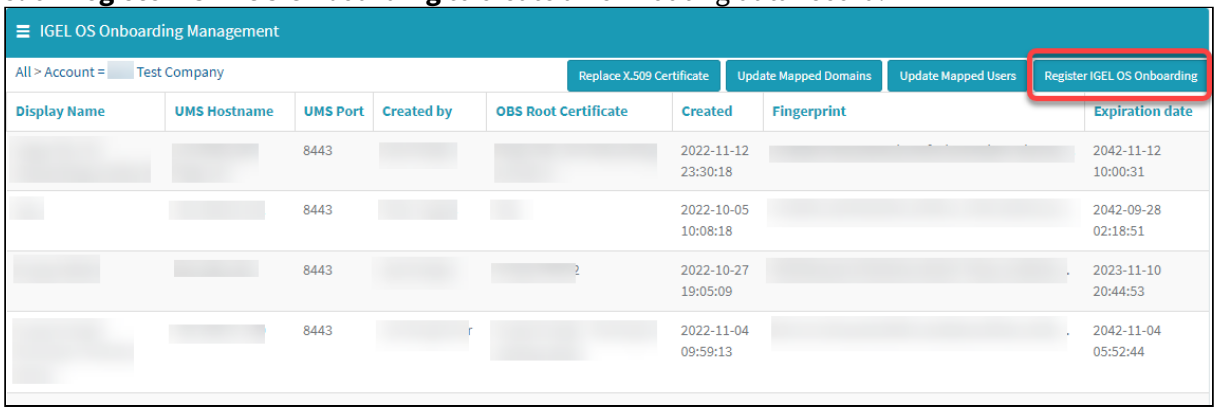
```
-----BEGIN CERTIFICATE-----
MIIFPTCCAyWgAwIBAgIFAIGKvrEwDQYJKoZIhvcNAQELBQAwVzEkMCIGA1UEAwwbSUQtLTQ5NzE2
LTE2ODE5NzkyNDEwOTYtOC0wMQ0wCwYDVQQKDARJR0VMMRMwEQYDVQQHDAoxNDAxODM1MDYyMQsw
.....................................
jqzhUGI+dZyTguXkzM2T4ACJUVm7G3mWDSCuMpt5laaE8kGEB2J6cbY9qV4QA5giCKFO1PgJ6mQZ
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**.



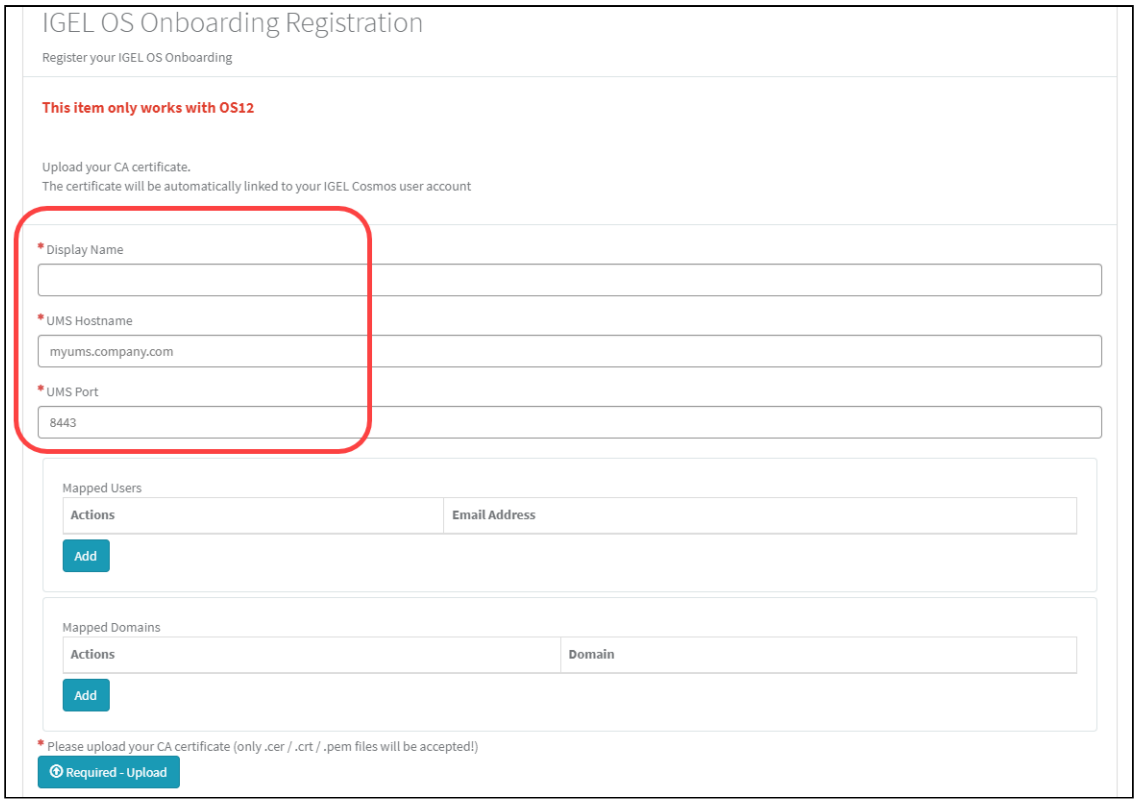
2. Click **Register IGEL OS Onboarding** to create a new routing data record.



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).

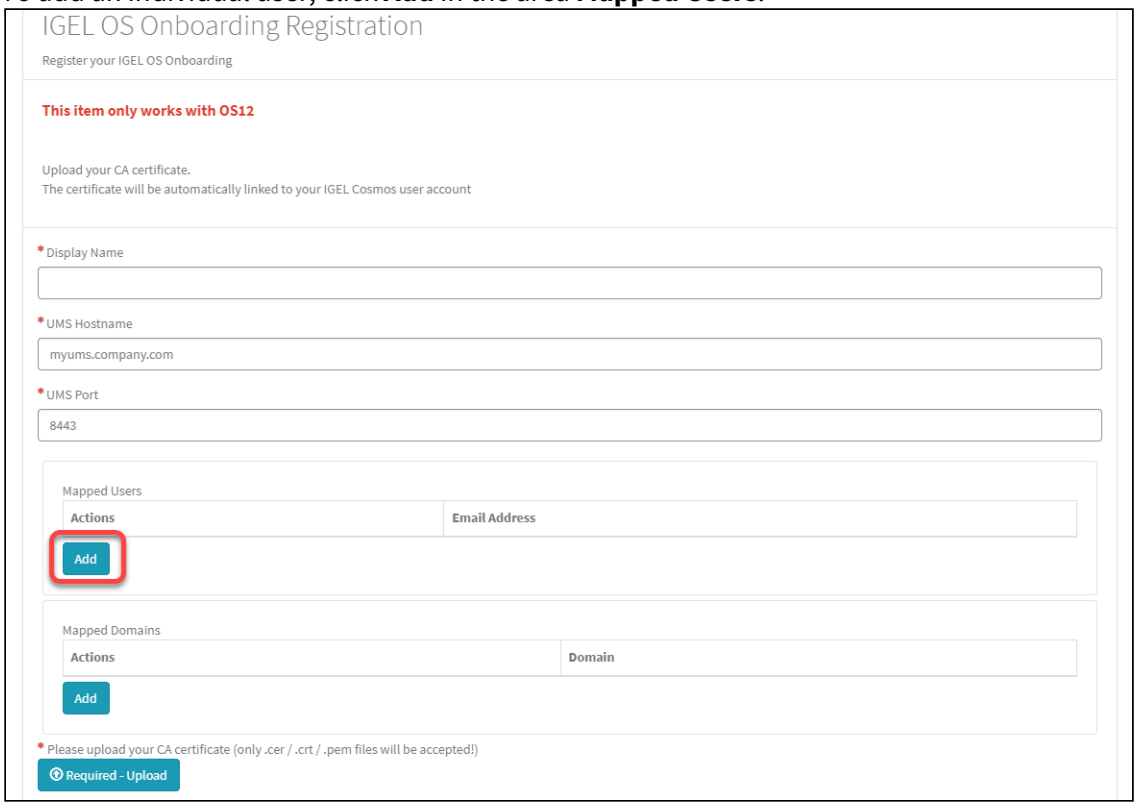
     > **UMS Hostname** is case-sensitive and should be written exactly as in the UMS.

   - **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).

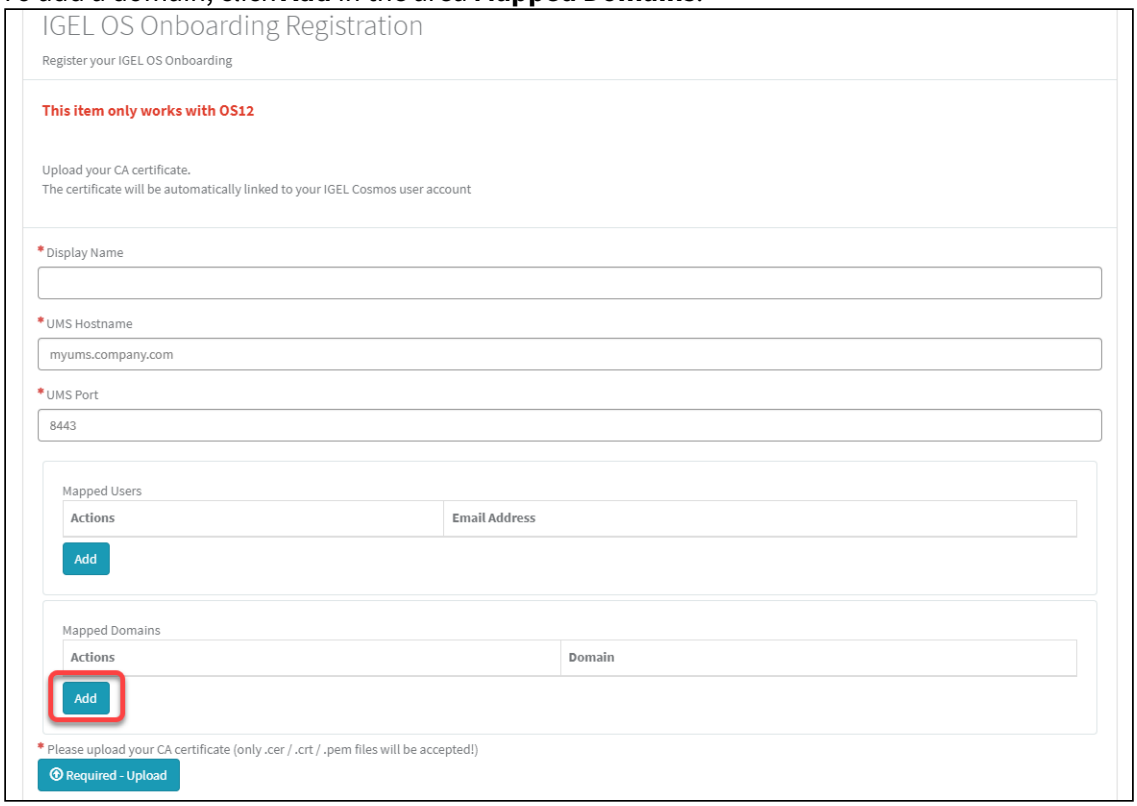


4. Proceed by adding individual users or one or more domains that include all e-mail addresses of these domains.

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

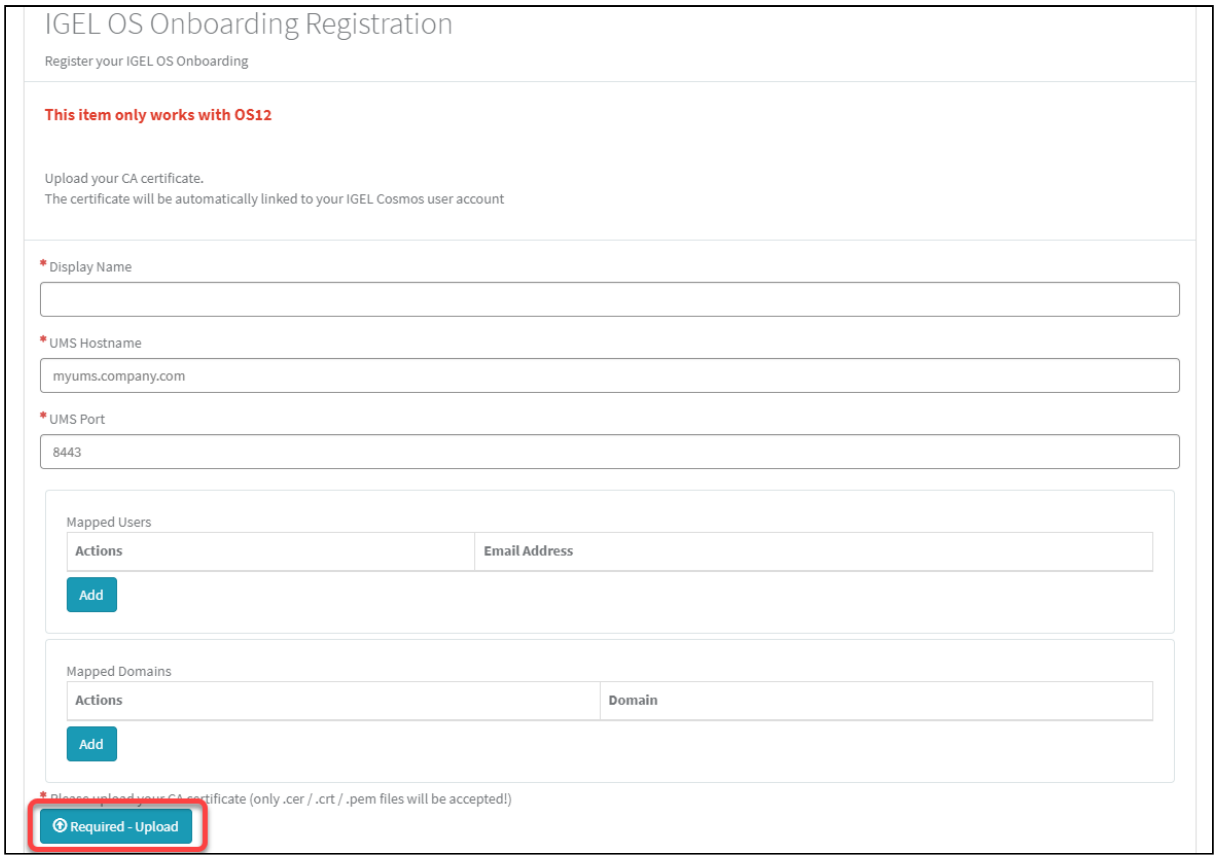


- To add a domain, click **Add** in the area **Mapped Domains**.

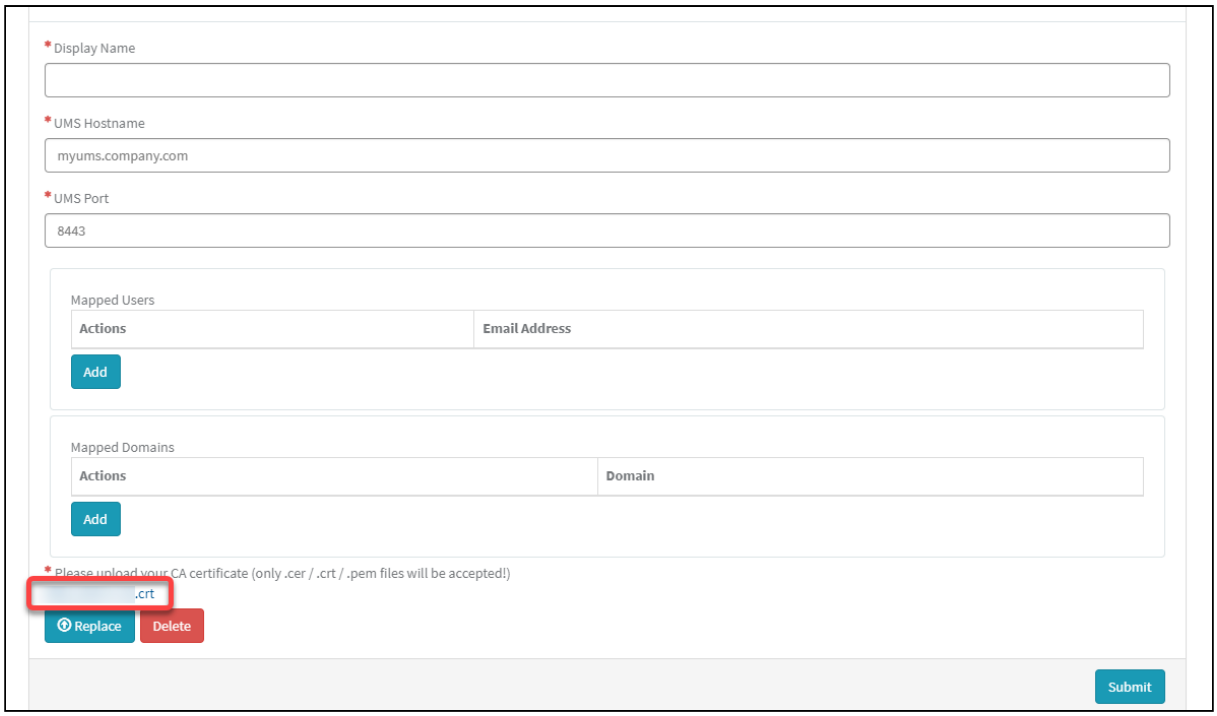


5. In the dialog, enter the e-mail address of the user we have created in Azure AD or the relevant domain and click **Add**.

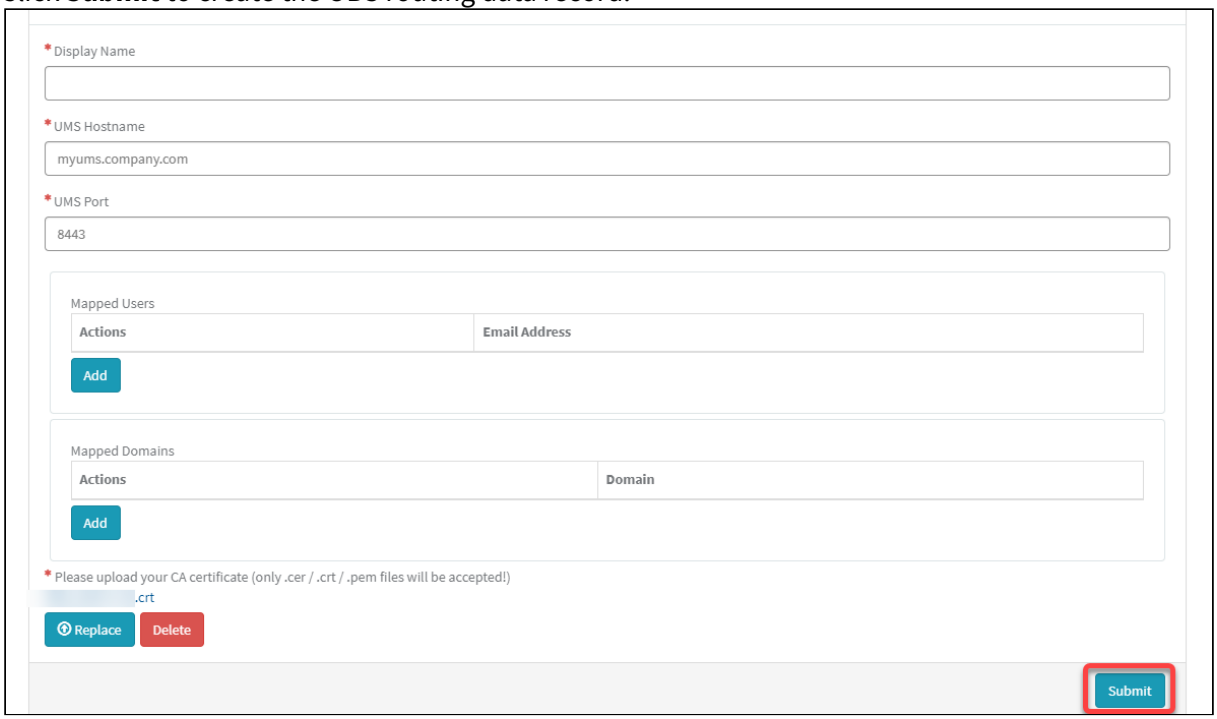
6. Click **Required - Upload** to upload the UMS root certificate chain.
If you want to use the OBS with the ICG, use here the file `icg_chain.crt` you obtained as described above(see page 43).



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

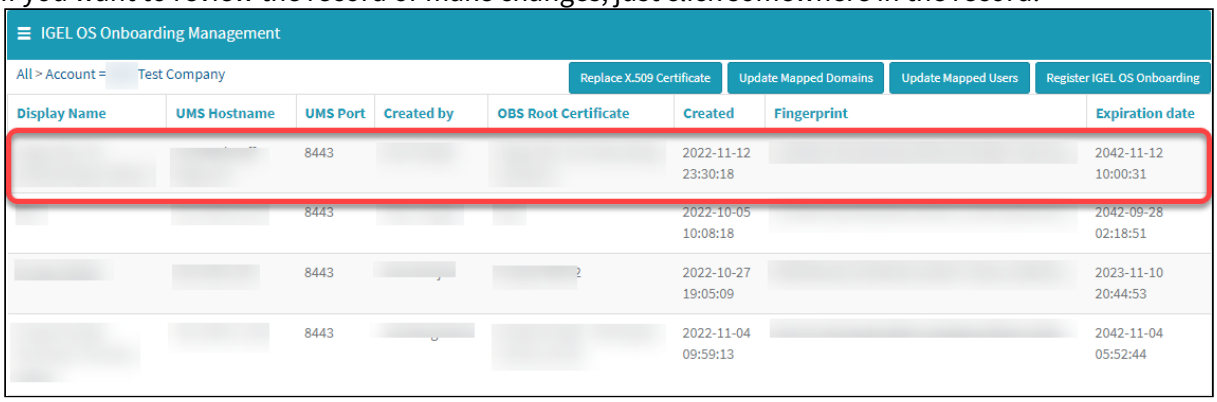


8. Click **Submit** to create the OBS routing data record.

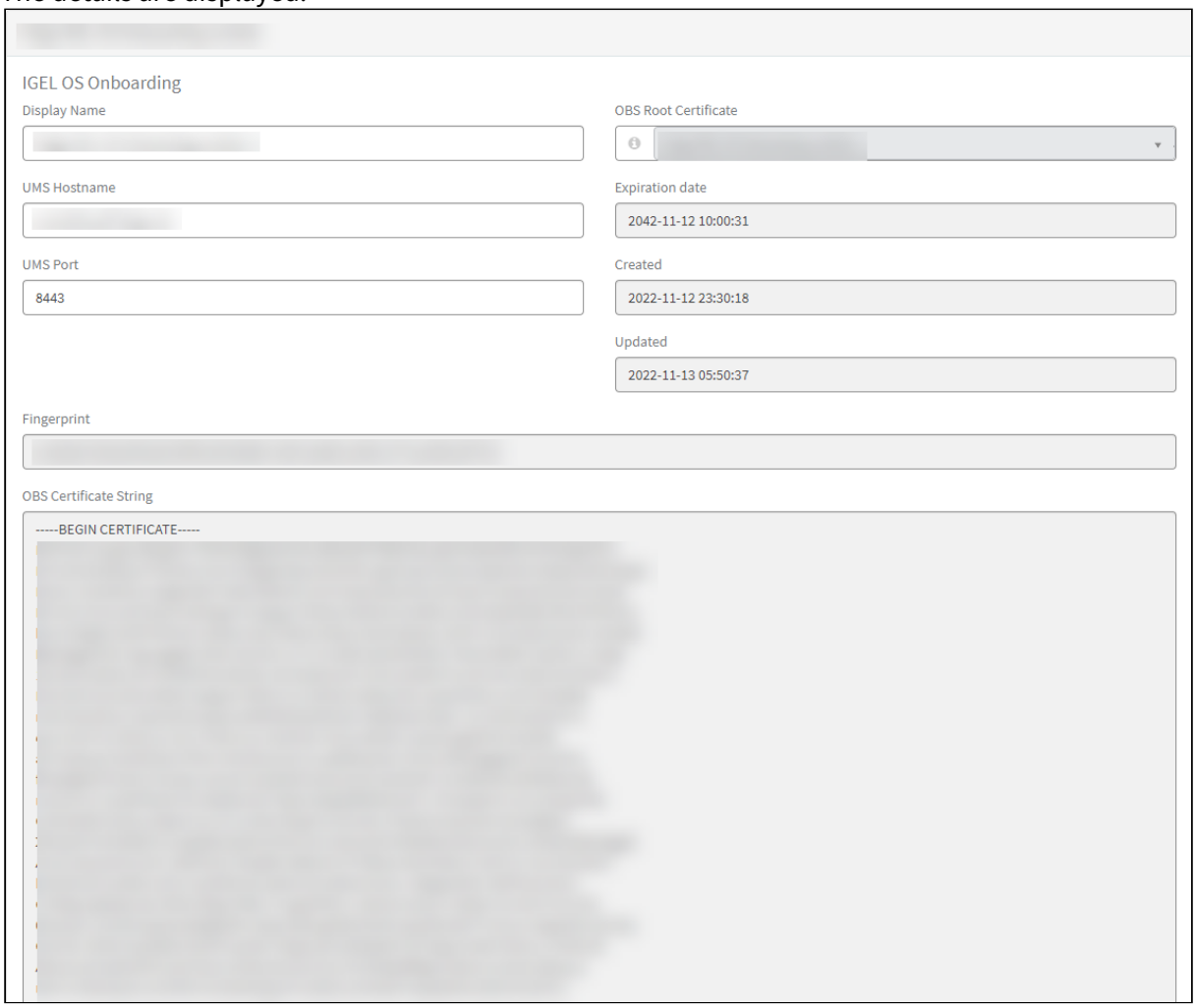


After a few seconds, the new data record is ready.

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



The details are displayed.



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).

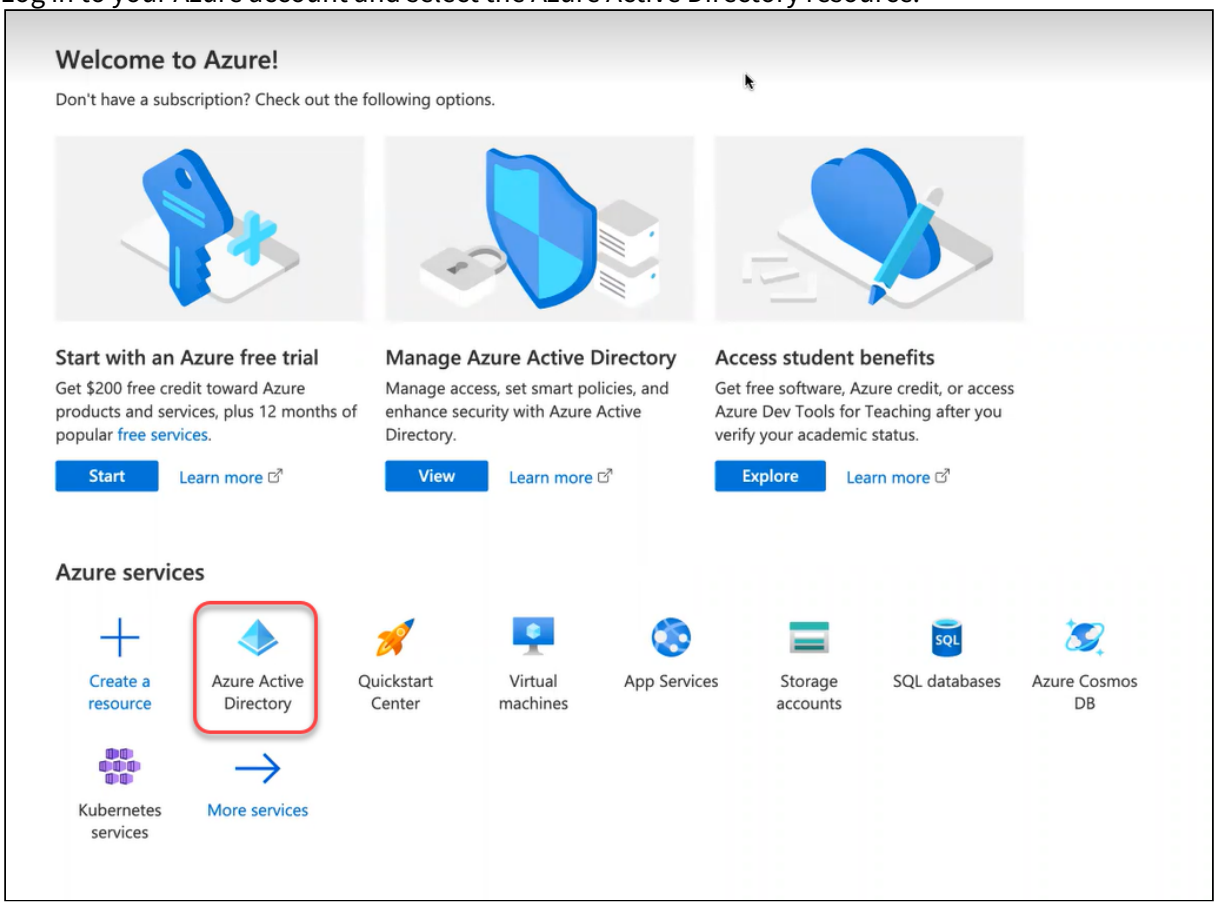
Configuring Azure as Identity Provider

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

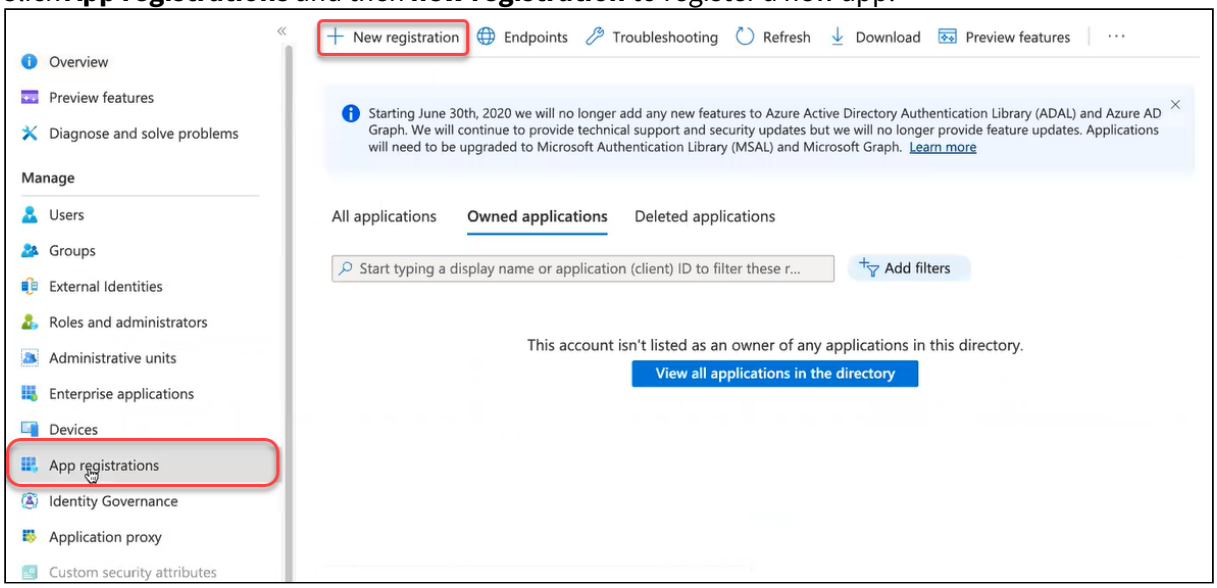
1. Creating an Azure Web Application That Will Serve as Identity Provider(see page 54): We register an application in Microsoft Azure to use its Azure AD services as an external identity provider.
2. Registering Our Azure Application in the IGEL Customer Portal(see page 60): This will enable IGEL Cloud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

Creating an Azure Web Application That Will Serve as Identity Provider

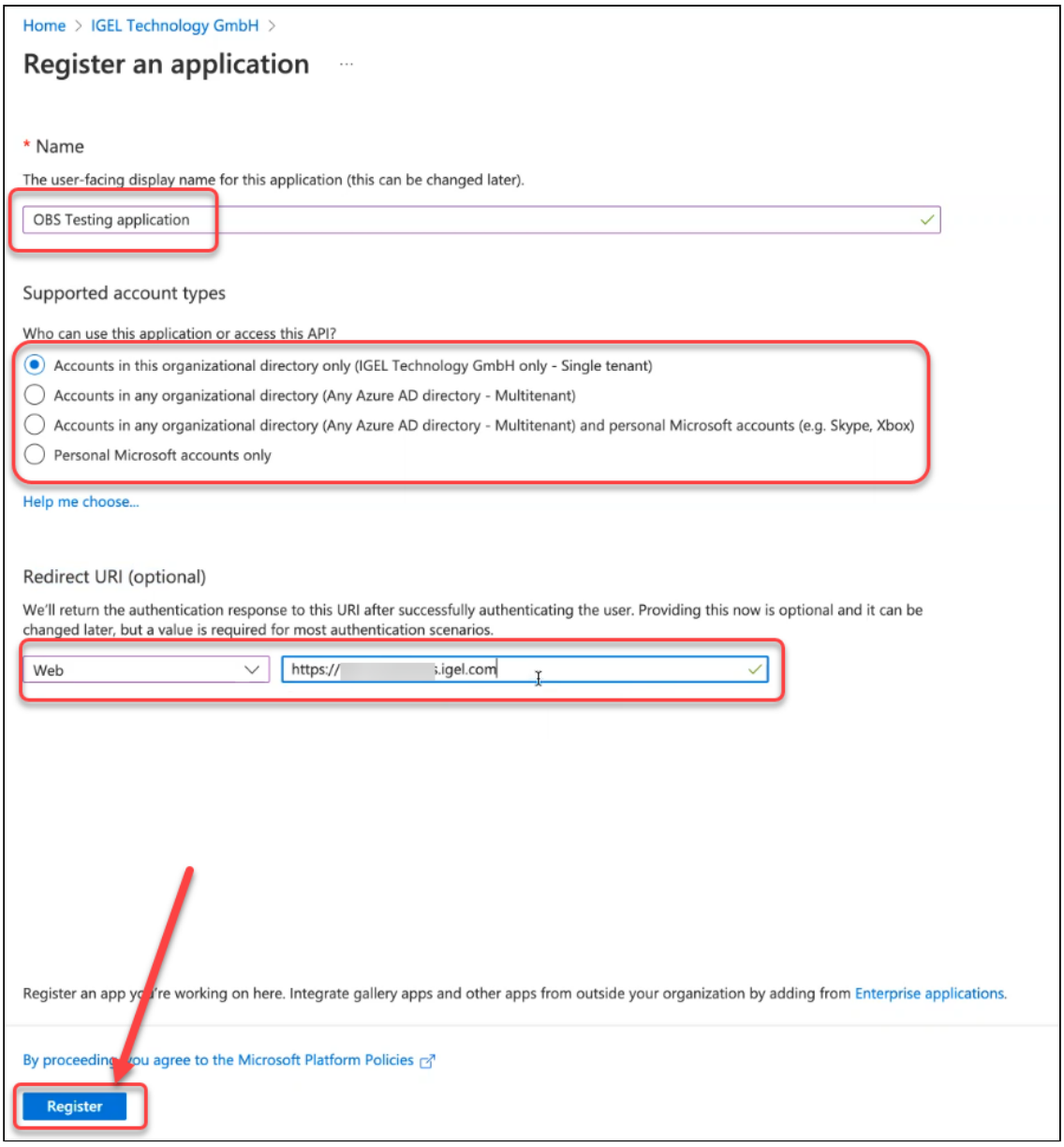
1. Log in to your Azure account and select the Azure Active Directory resource.



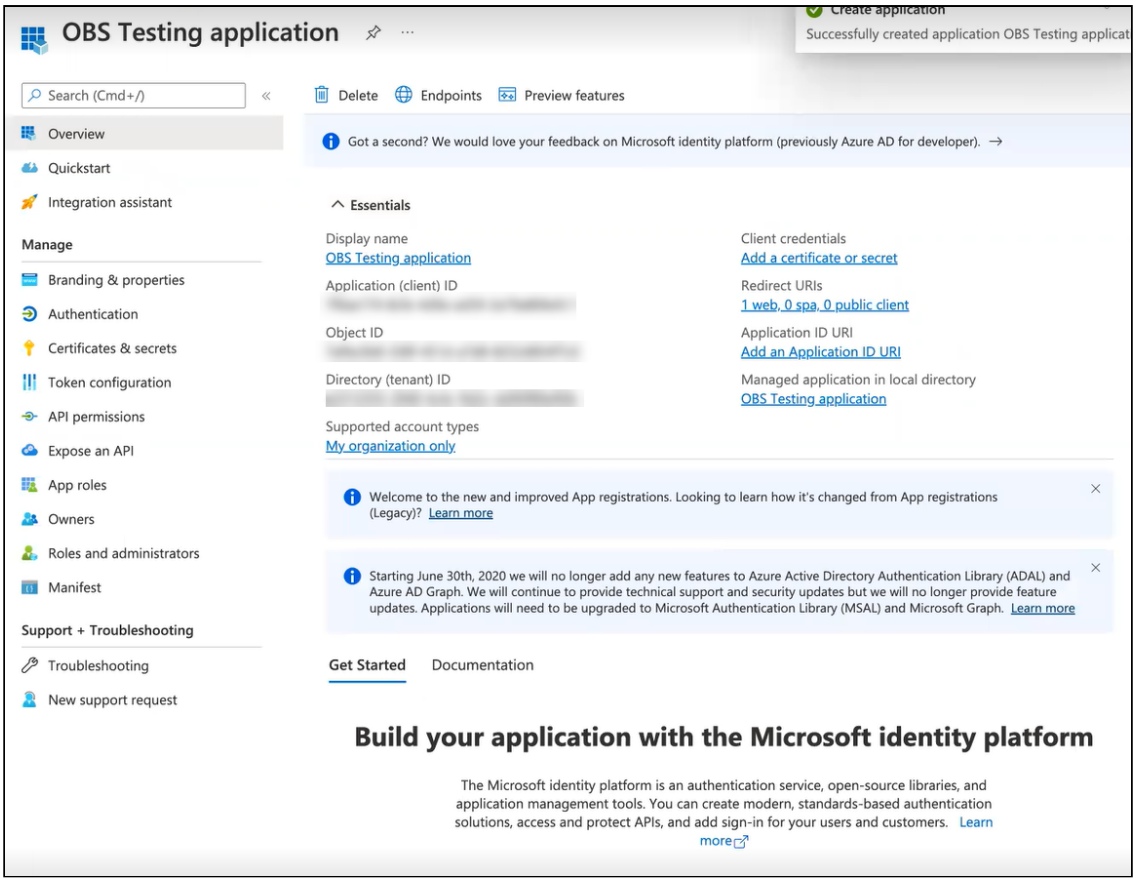
2. Click **App registrations** and then **new registration** to register a new app.



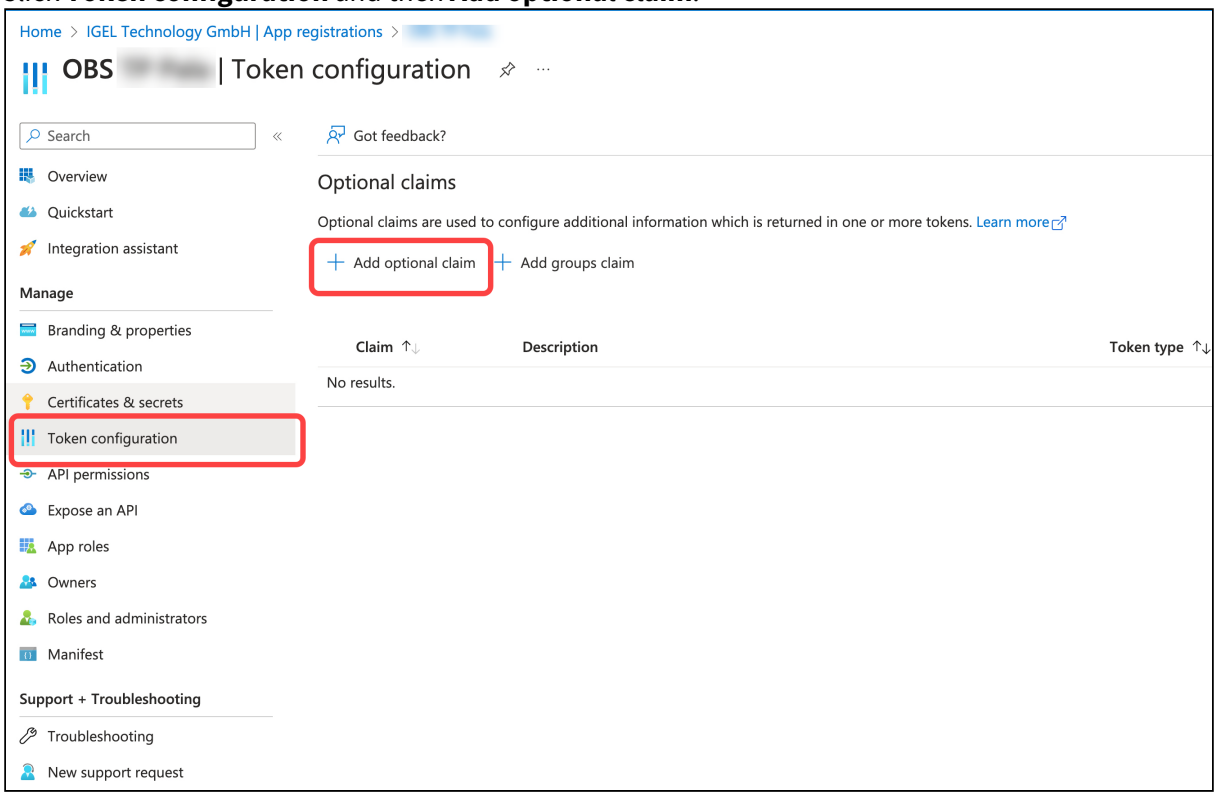
3. Edit the data as follows and then click **Register**:
   - **Name**: Display name for the app
   - **Supported account types**: Set the permissions according to your requirements.
   - **Redirect URI (optional)**: For our purposes, this setting is not optional but required. Set the first field to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



The application is created.
When you are creating the user accounts for onboarding, consider the following note:

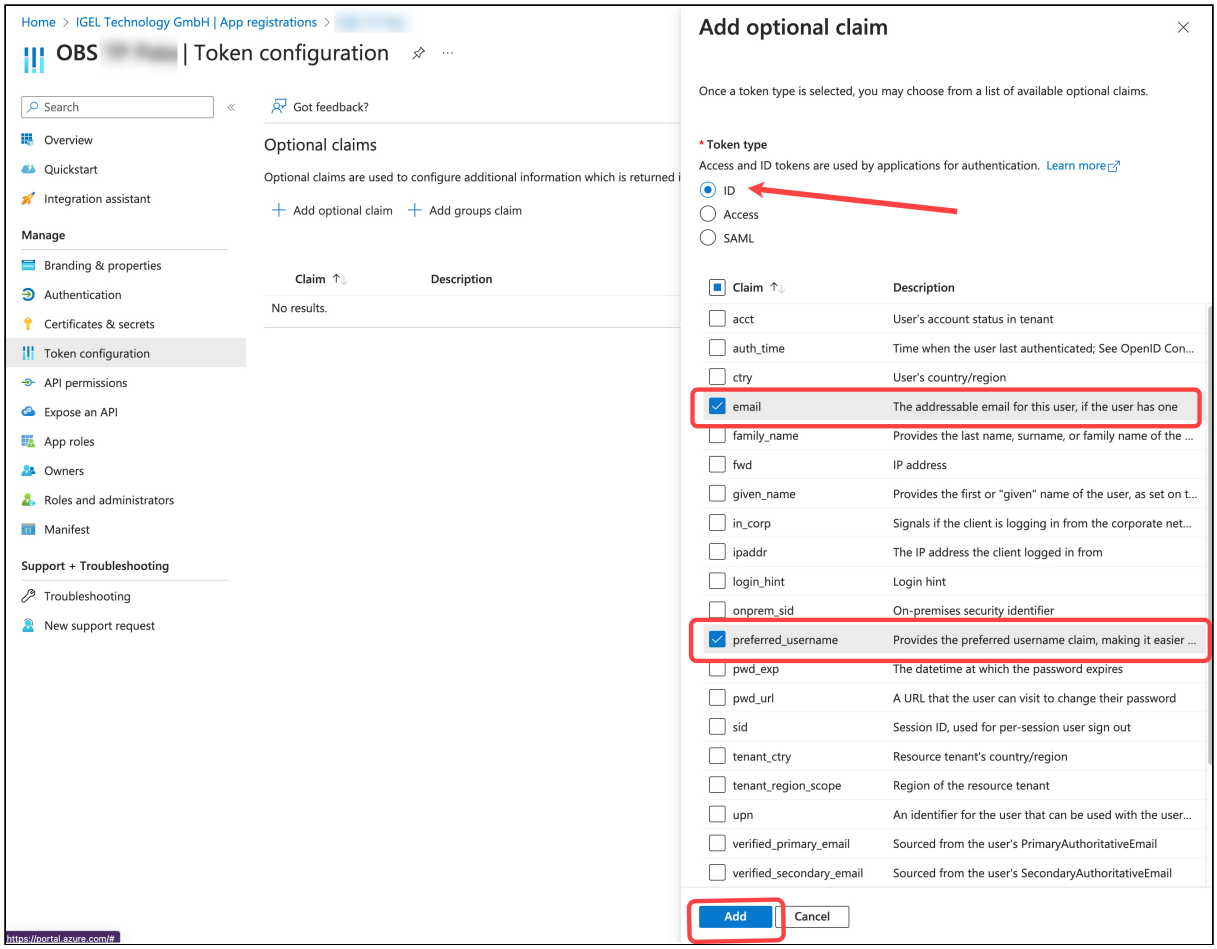

OBS Testing application
Create application
Successfully created application OBS Testing applicat
Search (Cmd+/)
Delete
Endpoints
Preview features
Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an 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
Object ID
Directory (tenant) ID
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
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**.

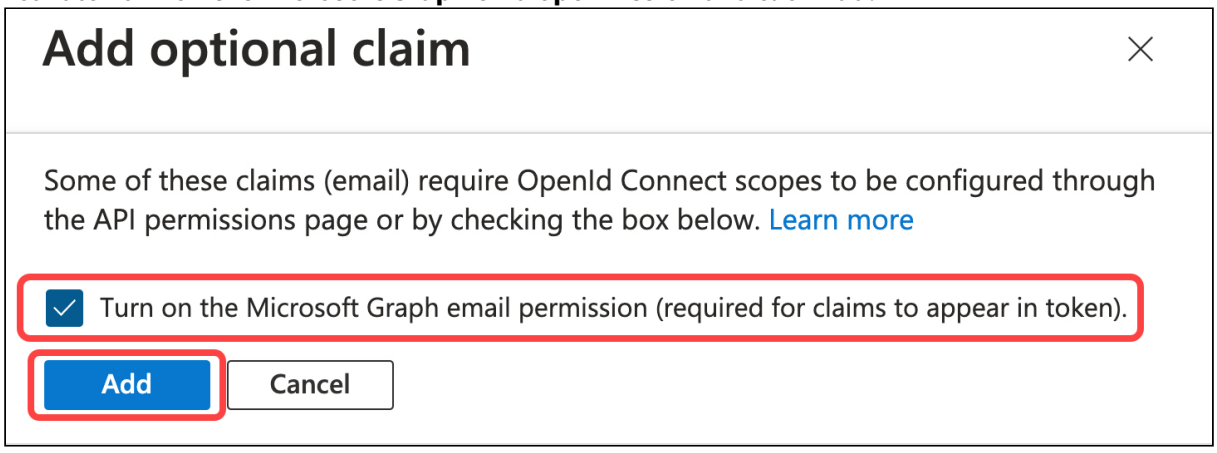


5. In the **Add optional claim** window, select **ID** under **Token type** and activate:
   - **email**
   - **preferred_username**

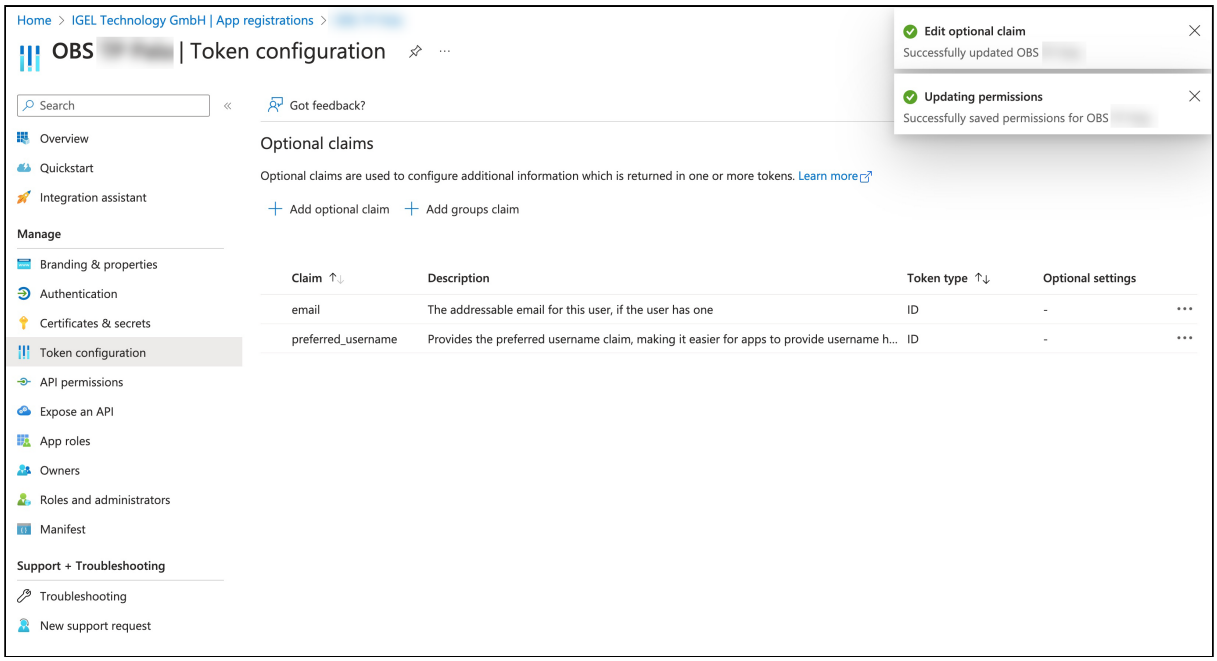
6. Click **Add**.



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



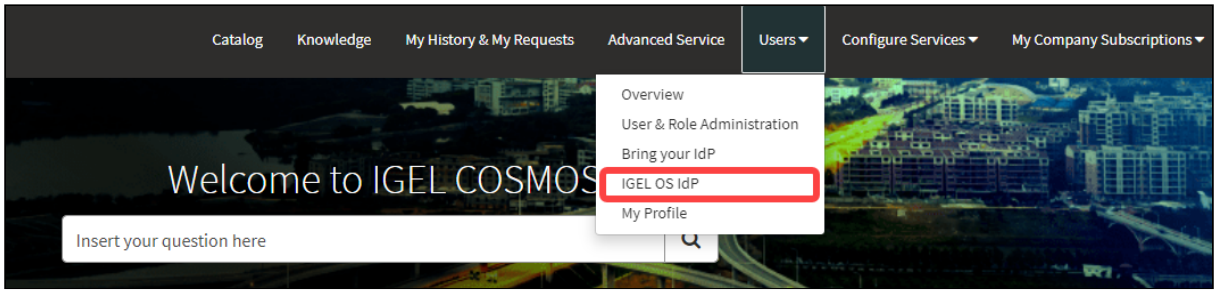
The token configuration is completed:



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

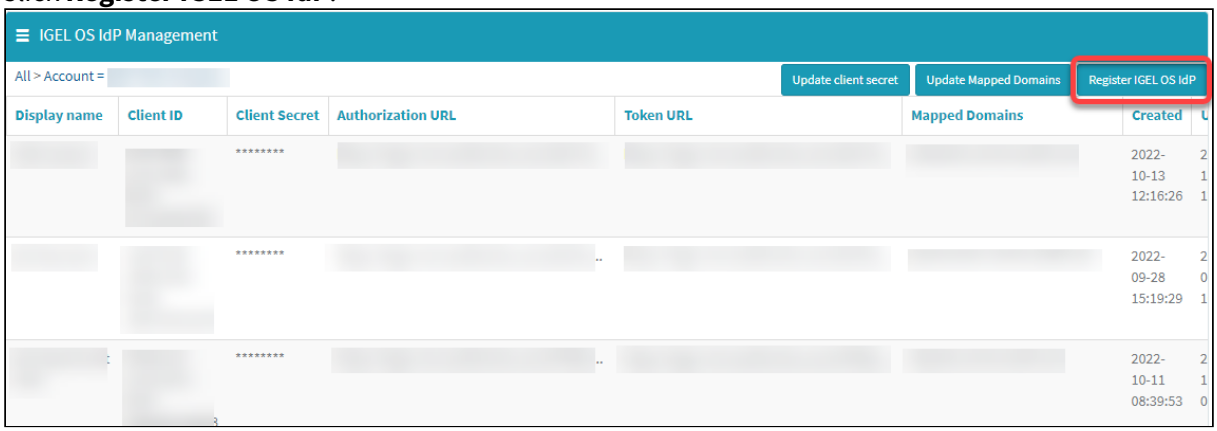
Registering Our Azure App in the IGEL Customer Portal

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

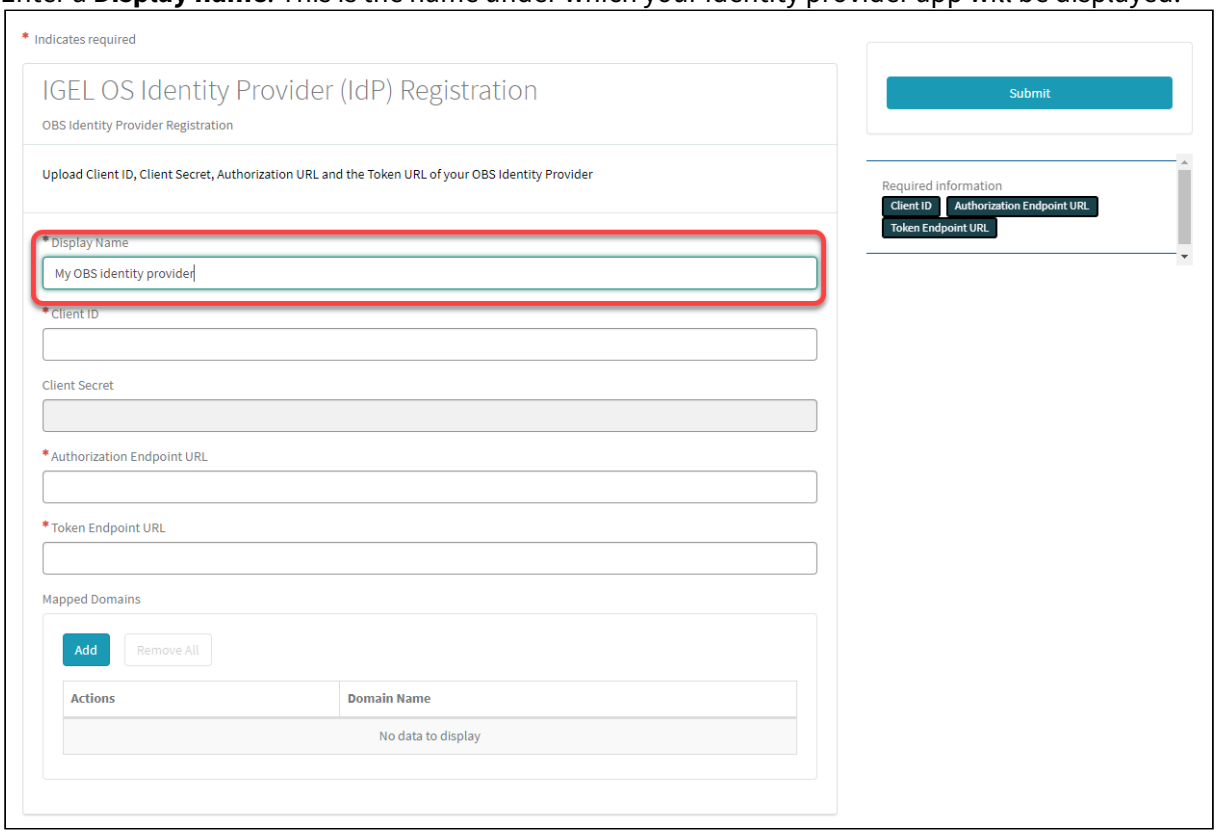


16 https://cosmos.igel.com/

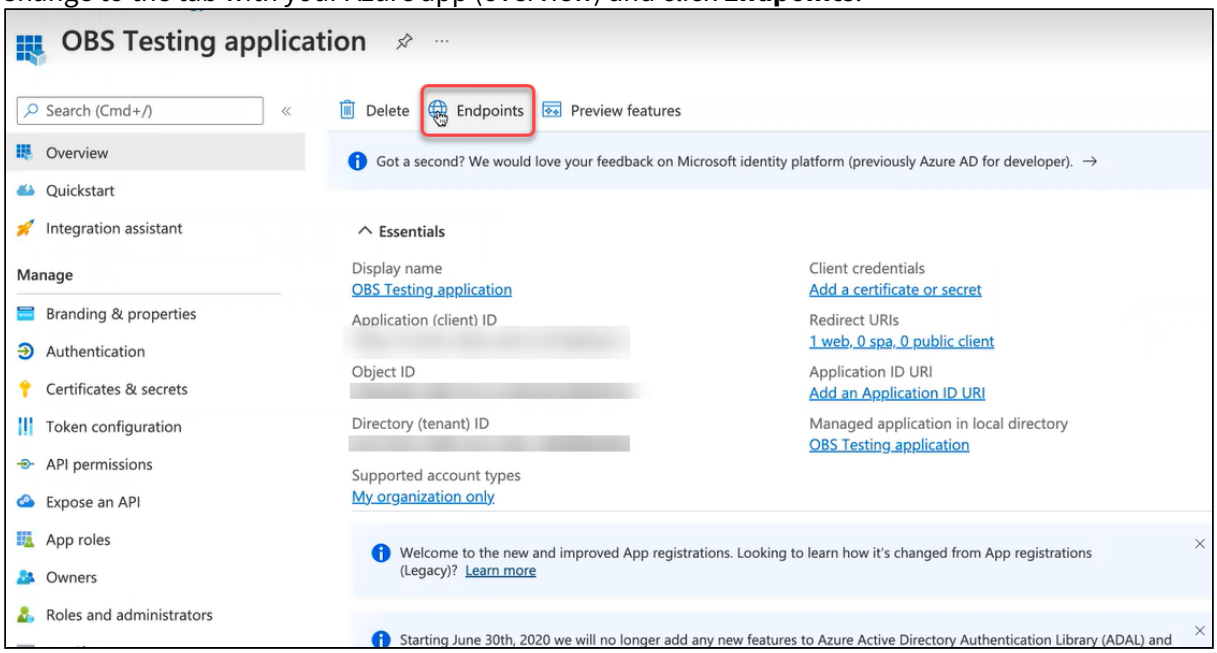
2. Click **Register IGEL OS IdP**.



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

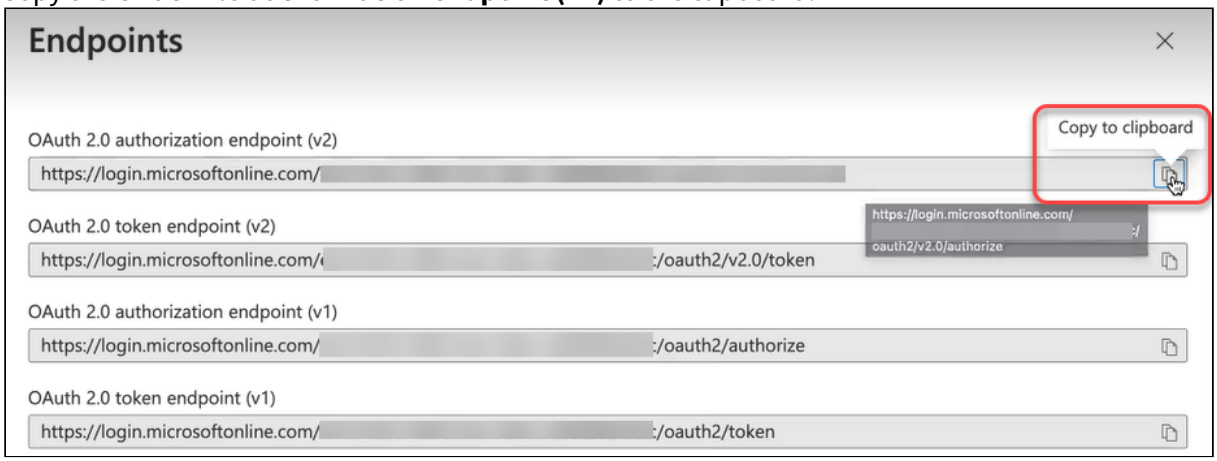


4. Change to the tab with your Azure app (overview) and click **Endpoints**.

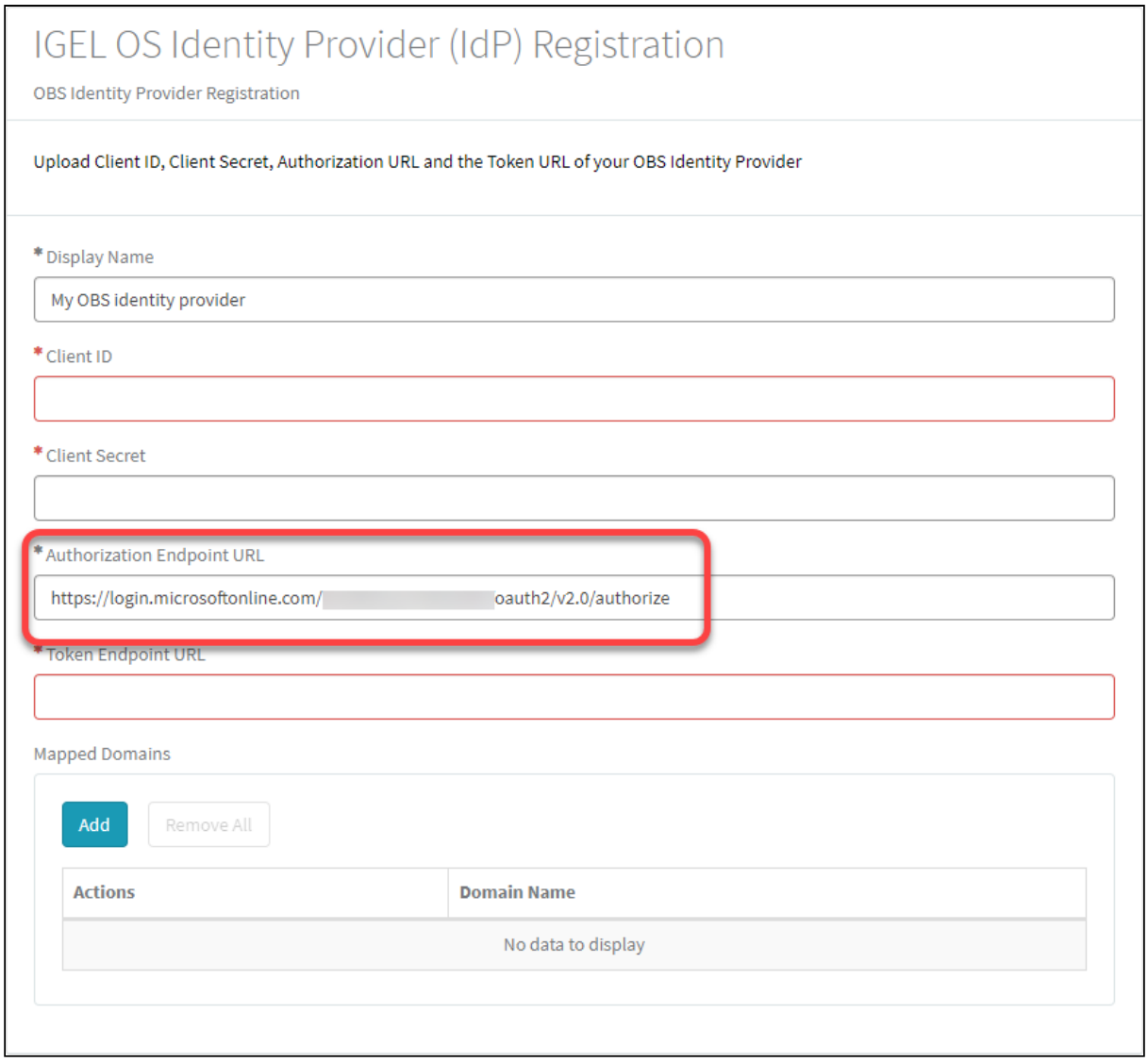


The endpoints for the app are shown. We will use the first 2 endpoints.

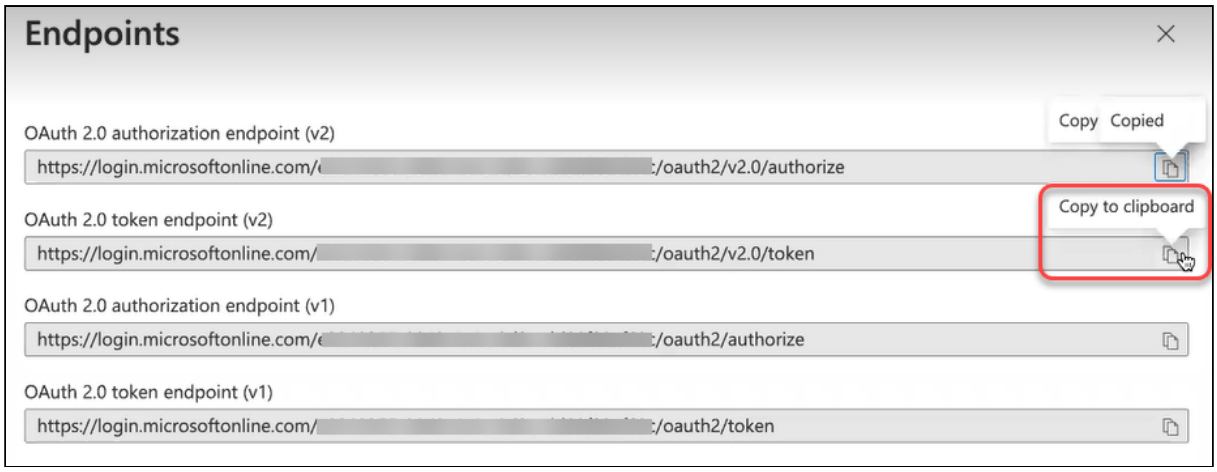
5. Copy the **OAuth 2.0 authorization endpoint (v2)** to the clipboard.



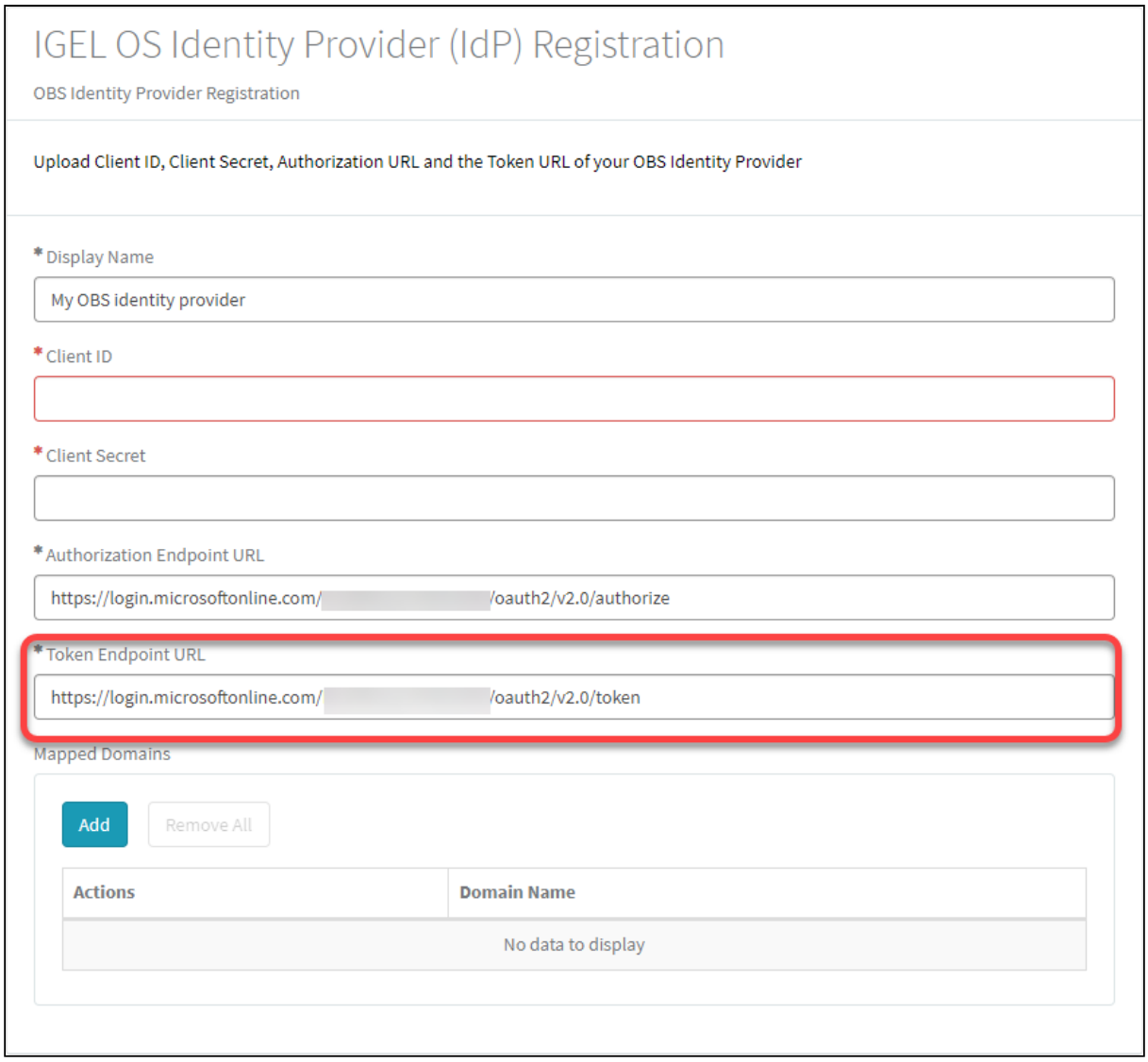
6. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the authorization endpoint into the field **Authorization Endpoint URL**.



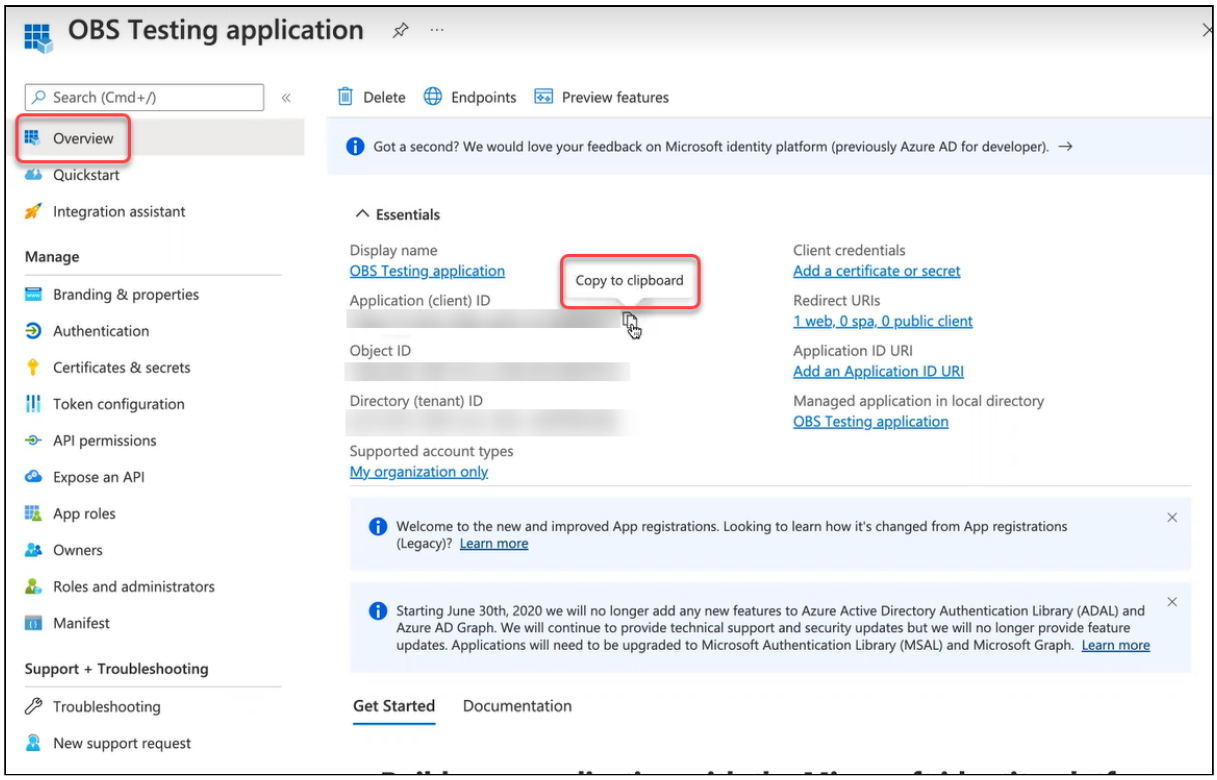
7. Change to the tab with your Azure app (**Endpoints**) and copy the **OAuth 2.0 token endpoint (v2)** to the clipboard.



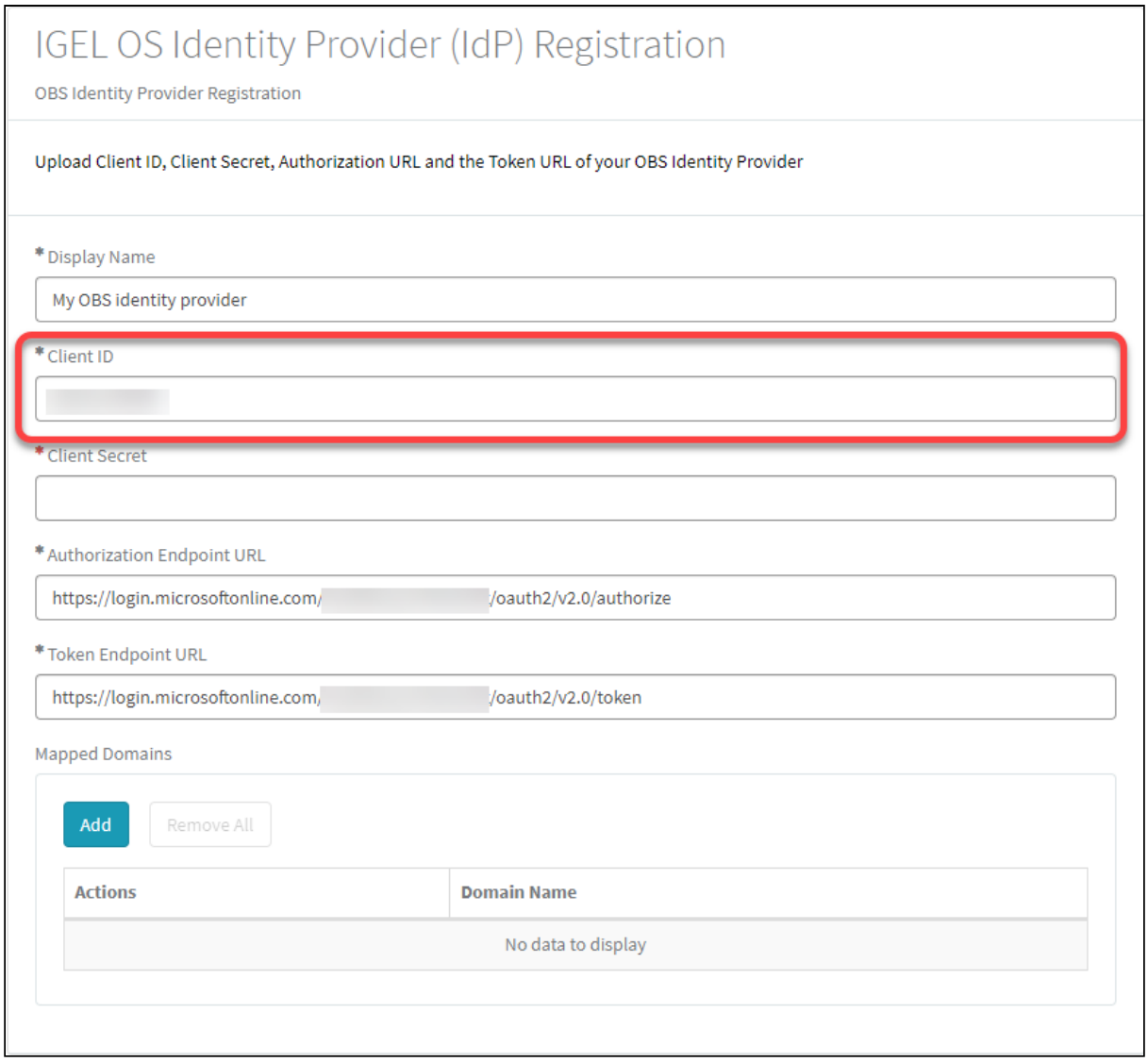
8. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the token endpoint into the field **Token Endpoint URL**.



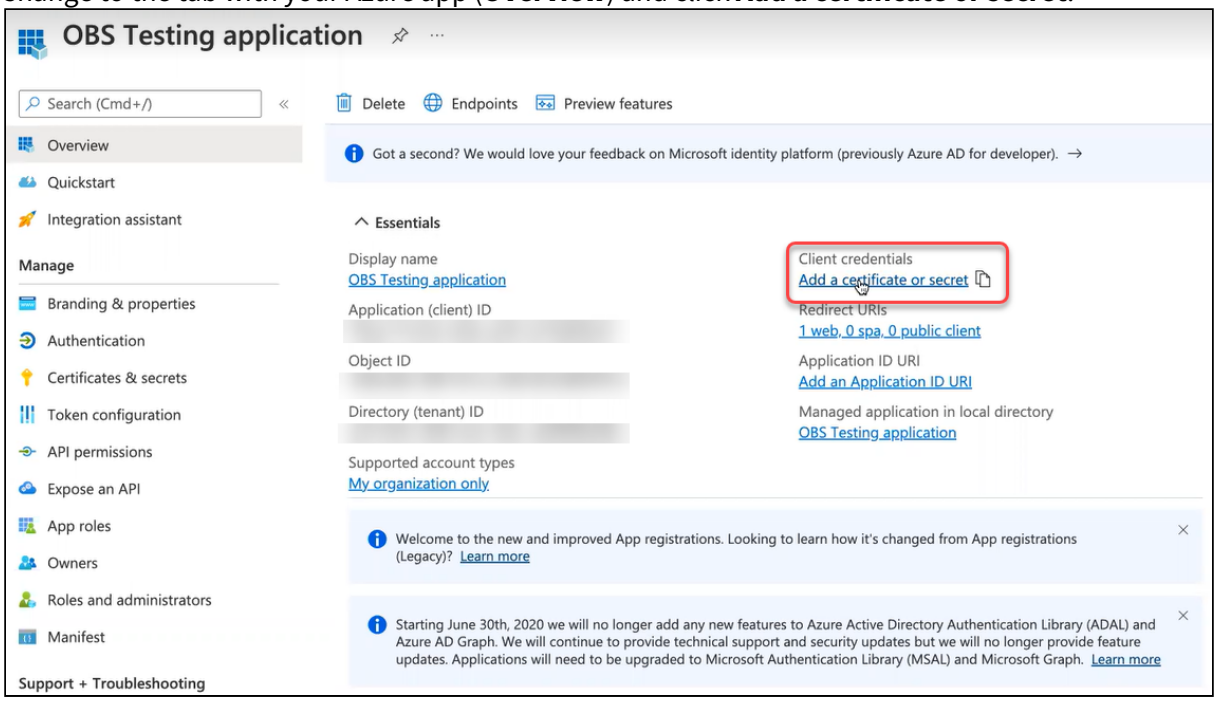
9. Change to the tab with your Azure app, go to **Overview**, and copy the **Application (client) ID** to the clipboard.



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

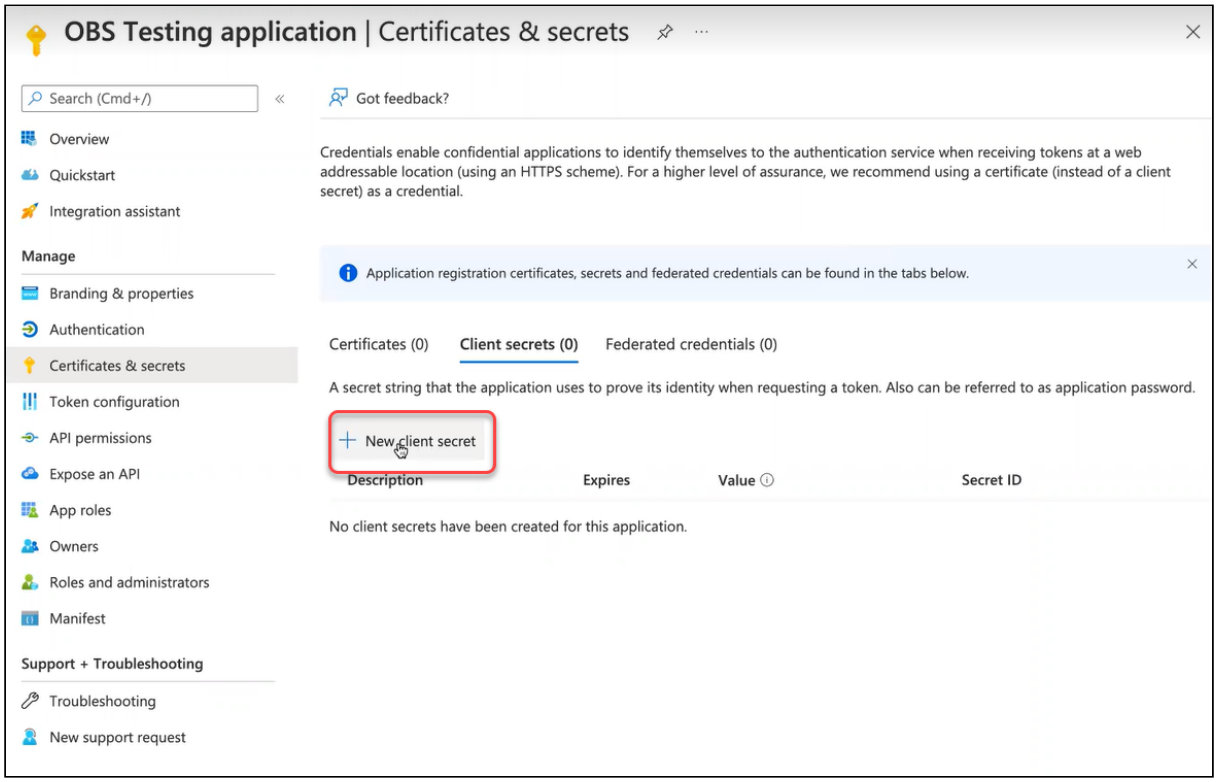

IGEL OS Identity Provider (IdP) Registration
OBS Identity Provider Registration
Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider
* Display Name
My OBS identity provider
* Client ID
* Client Secret
* Authorization Endpoint URL
https://login.microsoftonline.com/ /oauth2/v2.0/authorize
* Token Endpoint URL
https://login.microsoftonline.com/ /oauth2/v2.0/token
Mapped Domains
Add
Remove All
Actions
Domain Name
No data to display

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



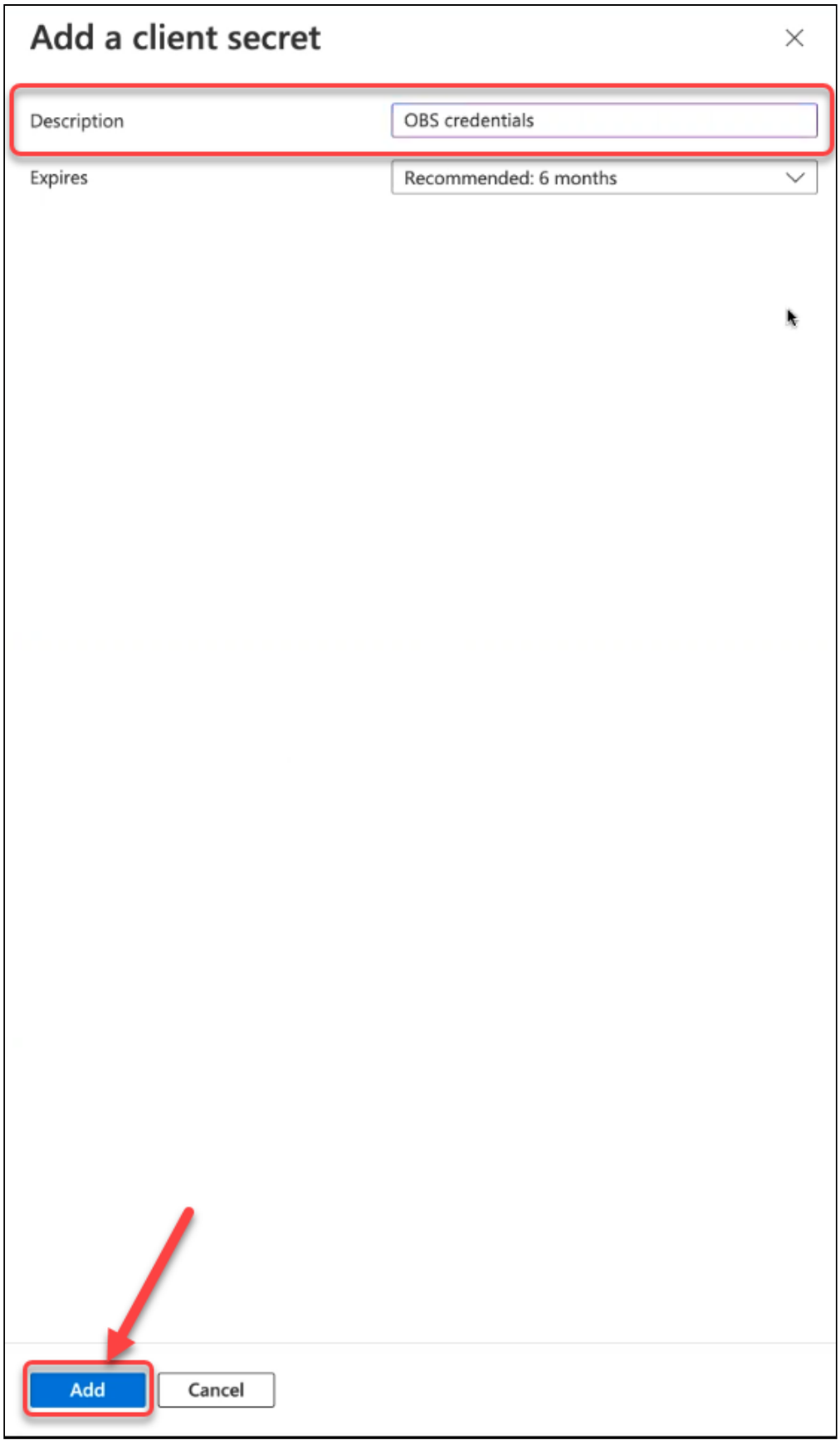
You are taken to the **Certificates & secrets** page.

12. Click **New client secret**.

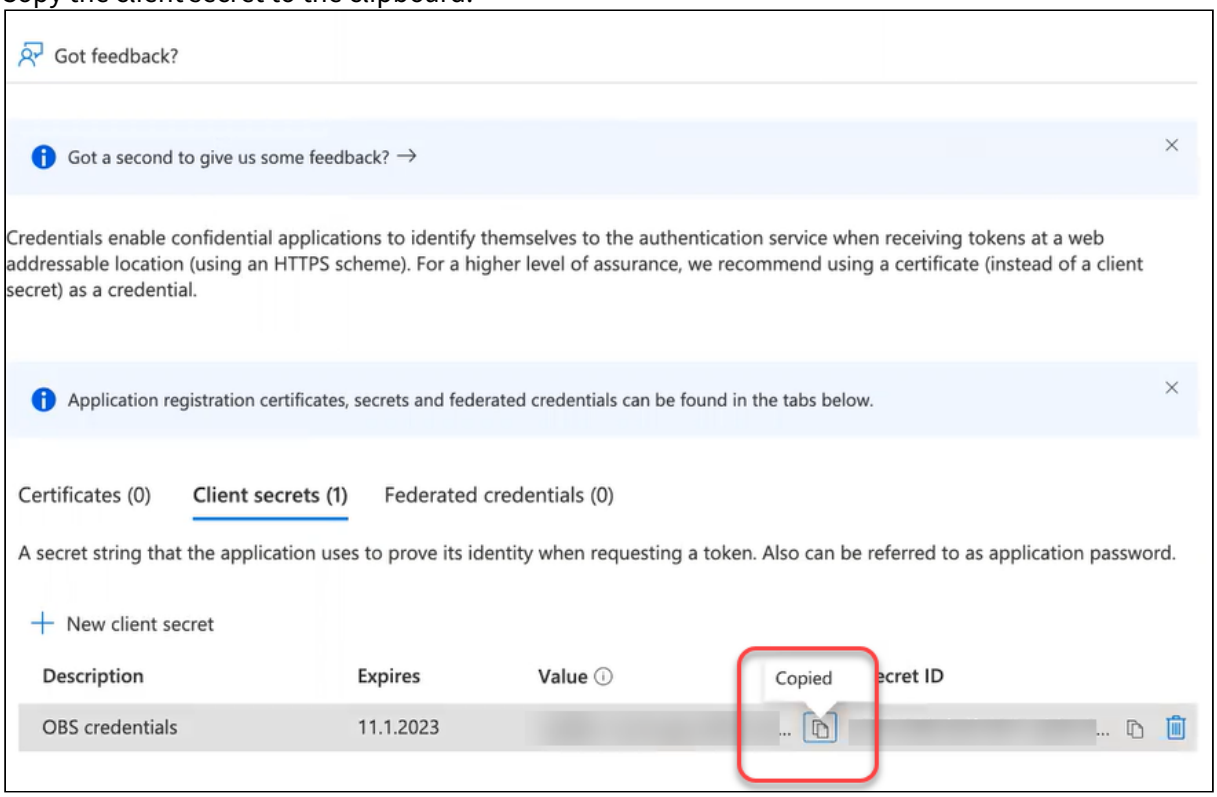


13. IMPORTANT! Make sure you have a safe and secure location to store the client secret; it can only be read out once. If you lose it, you must change it.

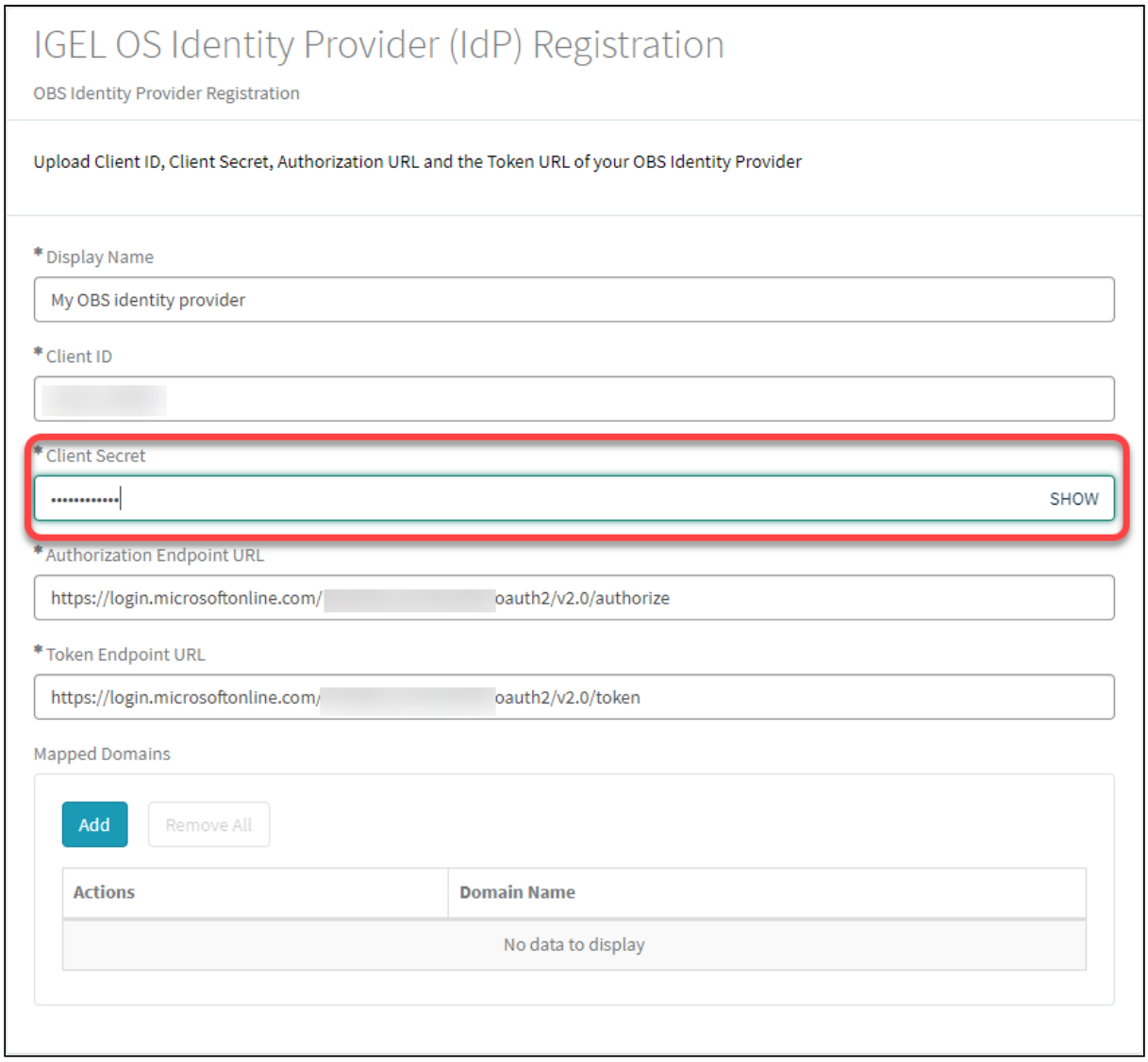
14. Enter a description and then click **Add**.


Add a client secret
Description
OBS credentials
Expires
Recommended: 6 months
Add
Cancel

15. Copy the client secret to the clipboard.

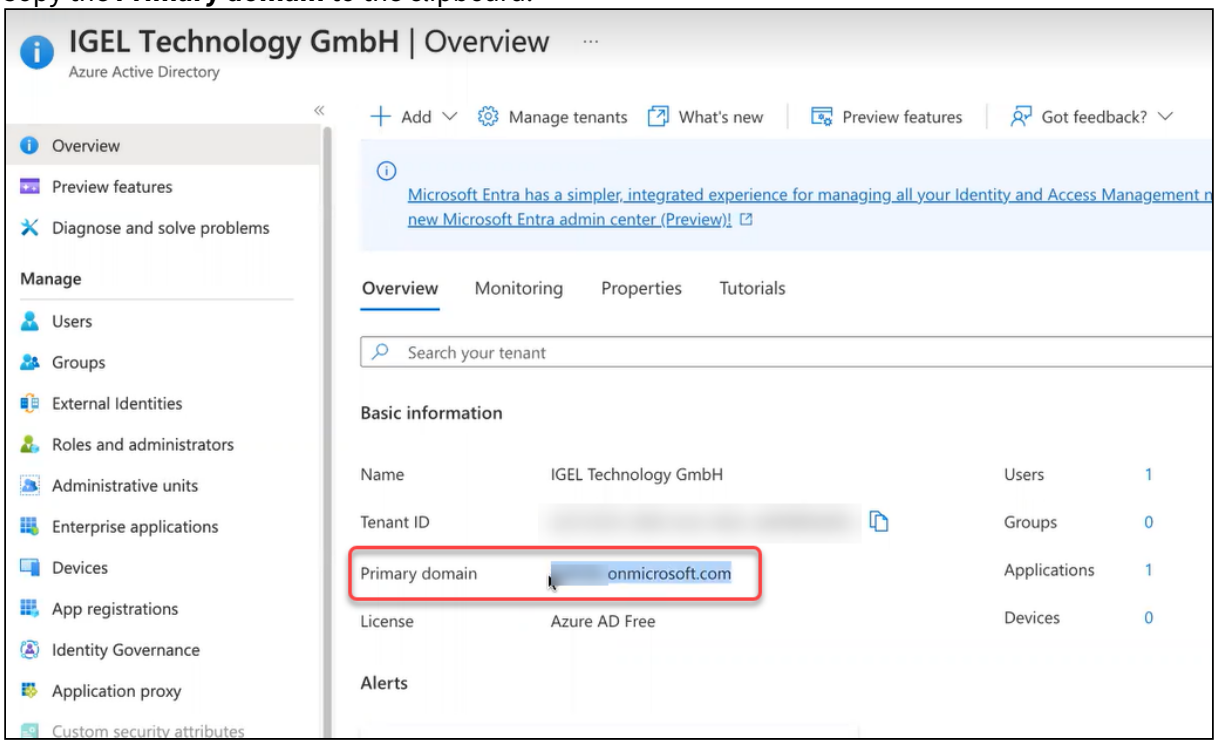


16. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client secret into the field **Client secret**.

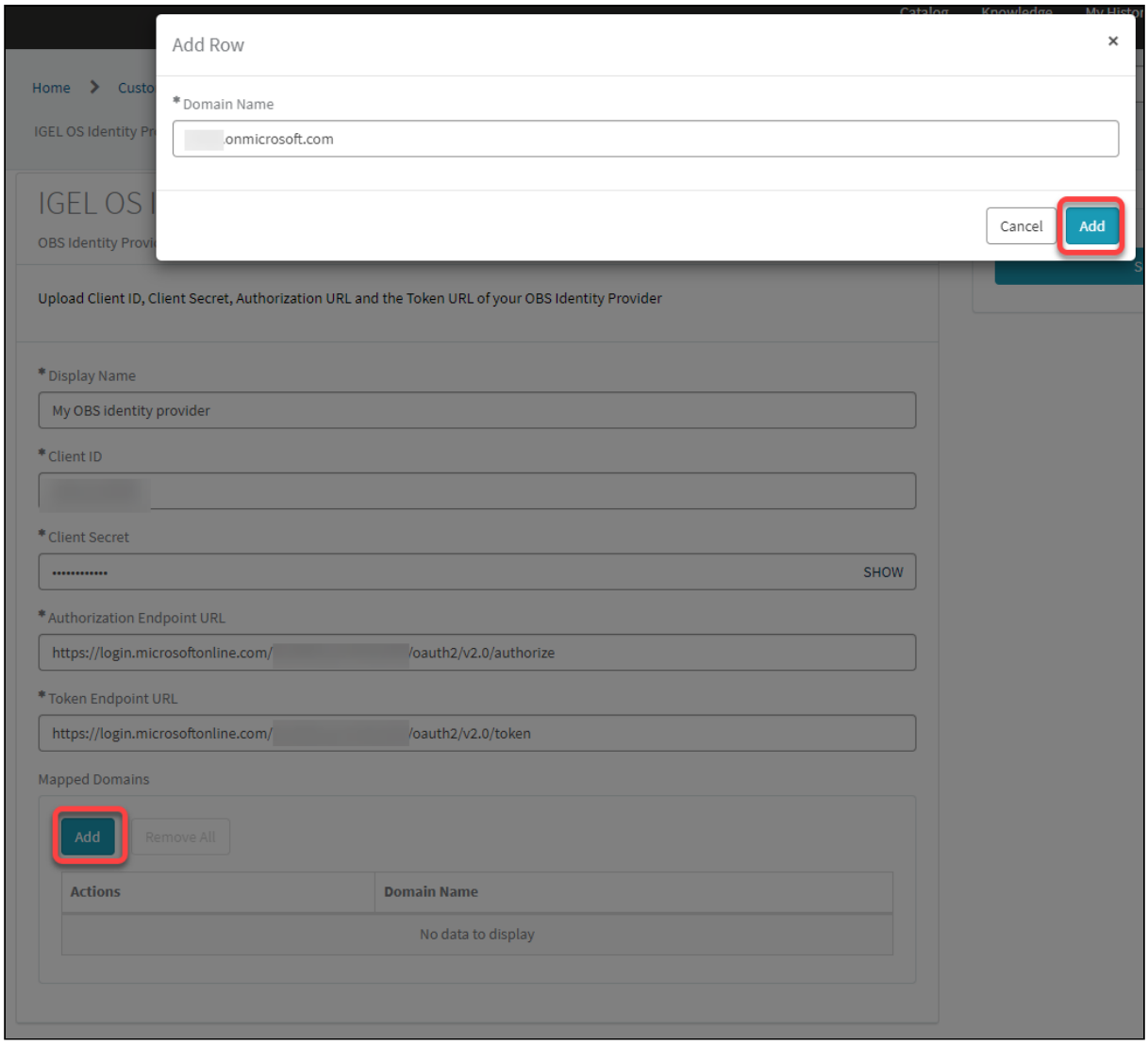


17. Change to the tab with your Azure app and change to the overview of your Azure tenant.

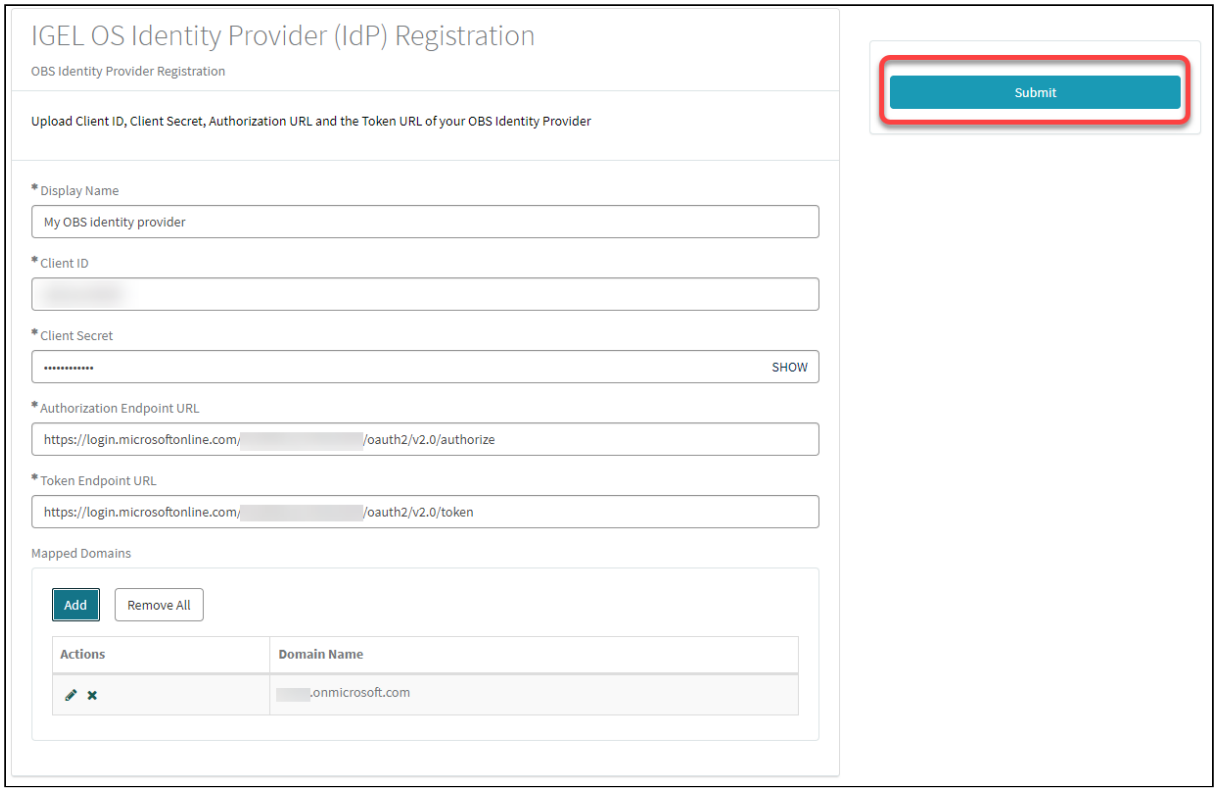
18. Copy the **Primary domain** to the clipboard.



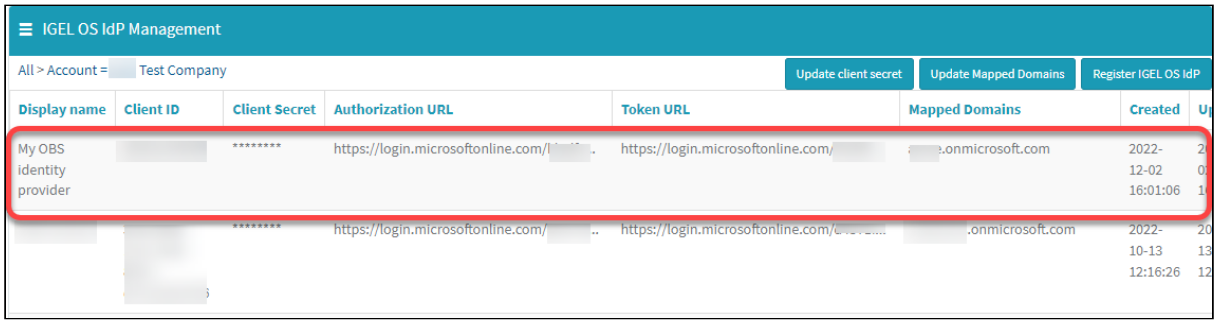
19. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab, click **Add**, paste the primary domain from the clipboard into the field **Domain name**, and then click **Add** in the dialog.


Add Row
Domain Name
onmicrosoft.com
Cancel
Add
Home
IGEL OS Identity Pr
IGEL OS
OBS Identity Provi
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
SHOW
Authorization Endpoint URL
https://login.microsoftonline.com/ /oauth2/v2.0/authorize
Token Endpoint URL
https://login.microsoftonline.com/ /oauth2/v2.0/token
Mapped Domains
Add
Remove All
Actions
Domain Name
No data to display

20. Click **Submit**.

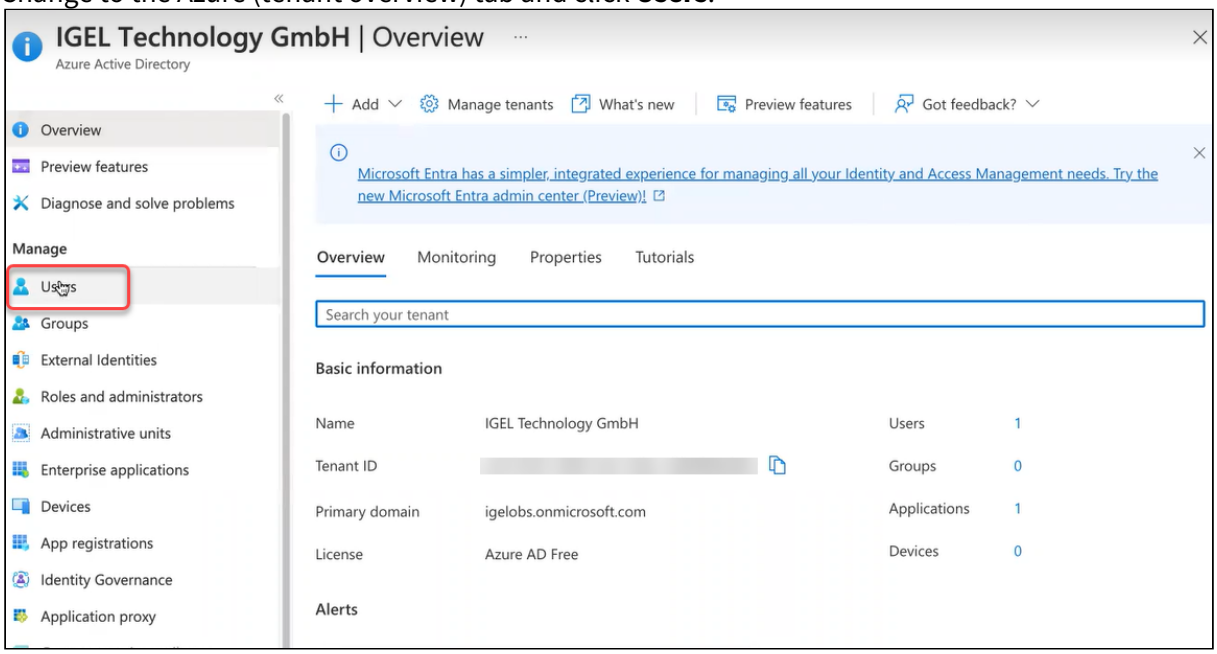


The data record is created.

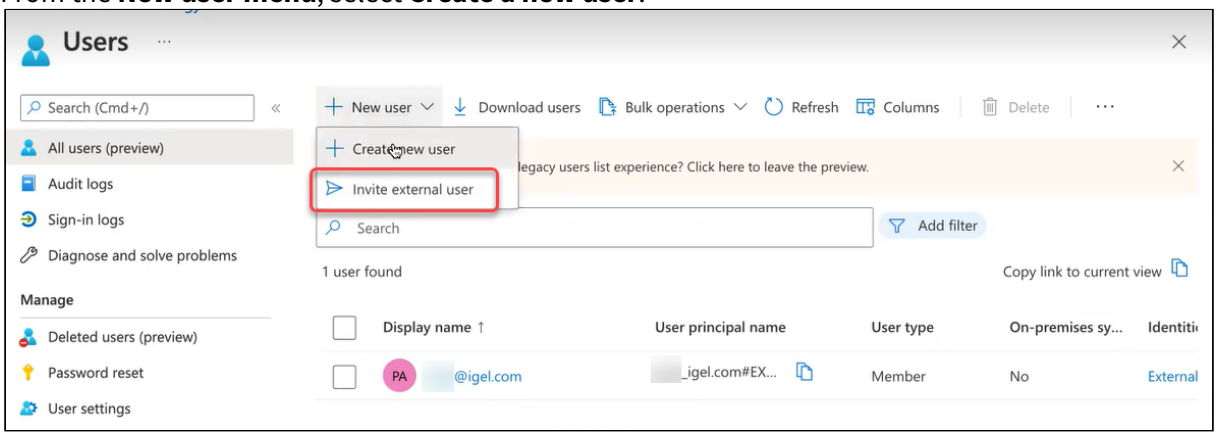


Creating a User in the Azure App

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

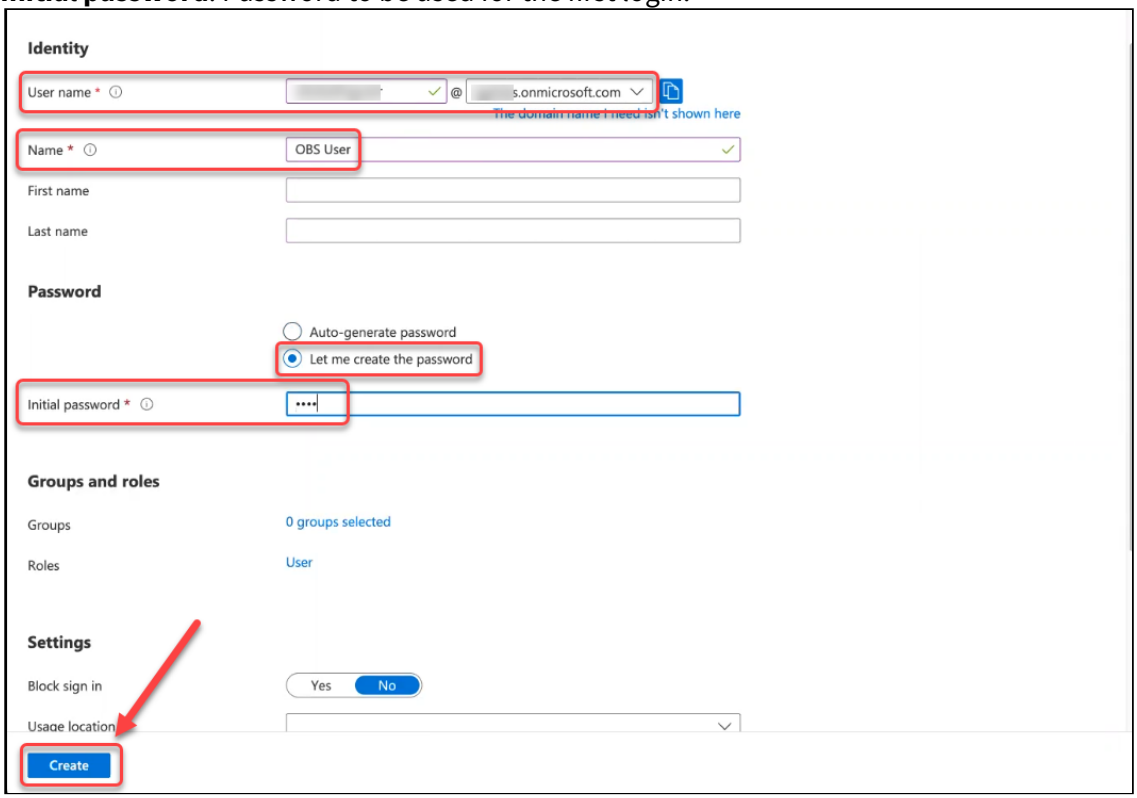


2. From the **New user menu**, select **Create a new user**.



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.



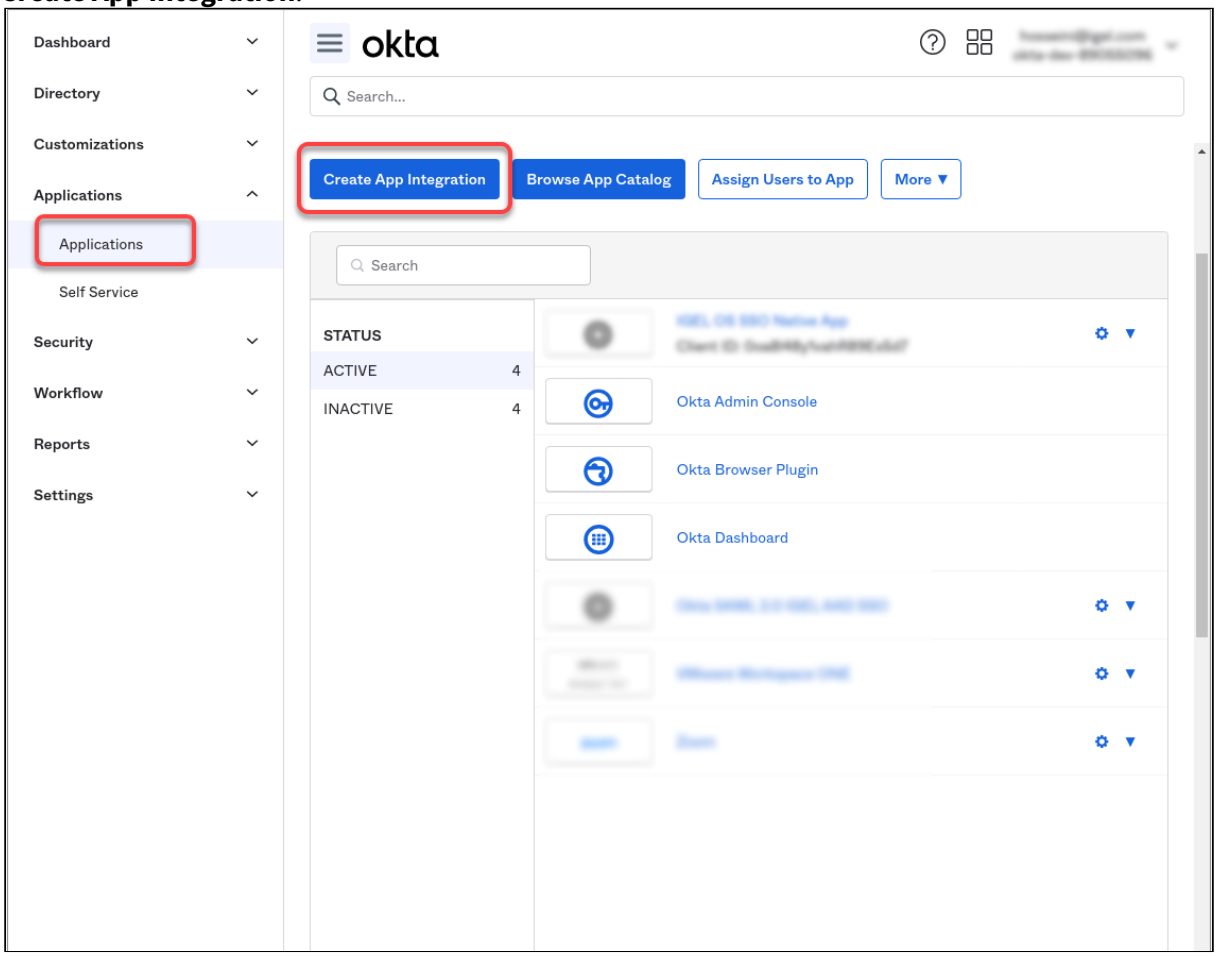
Configuring Okta as Identity Provider

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.

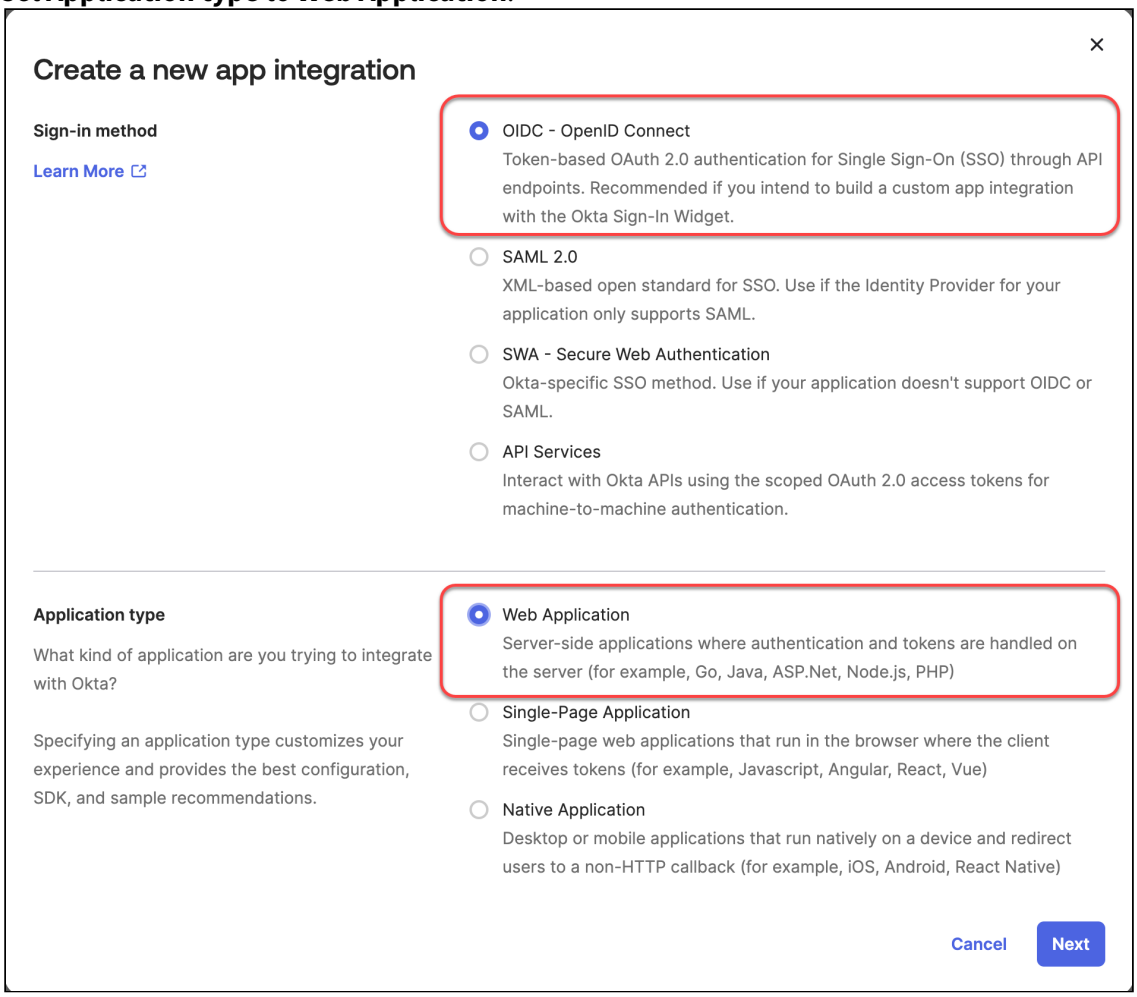
Creating an Okta Application That Will Serve as Identity Provider

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



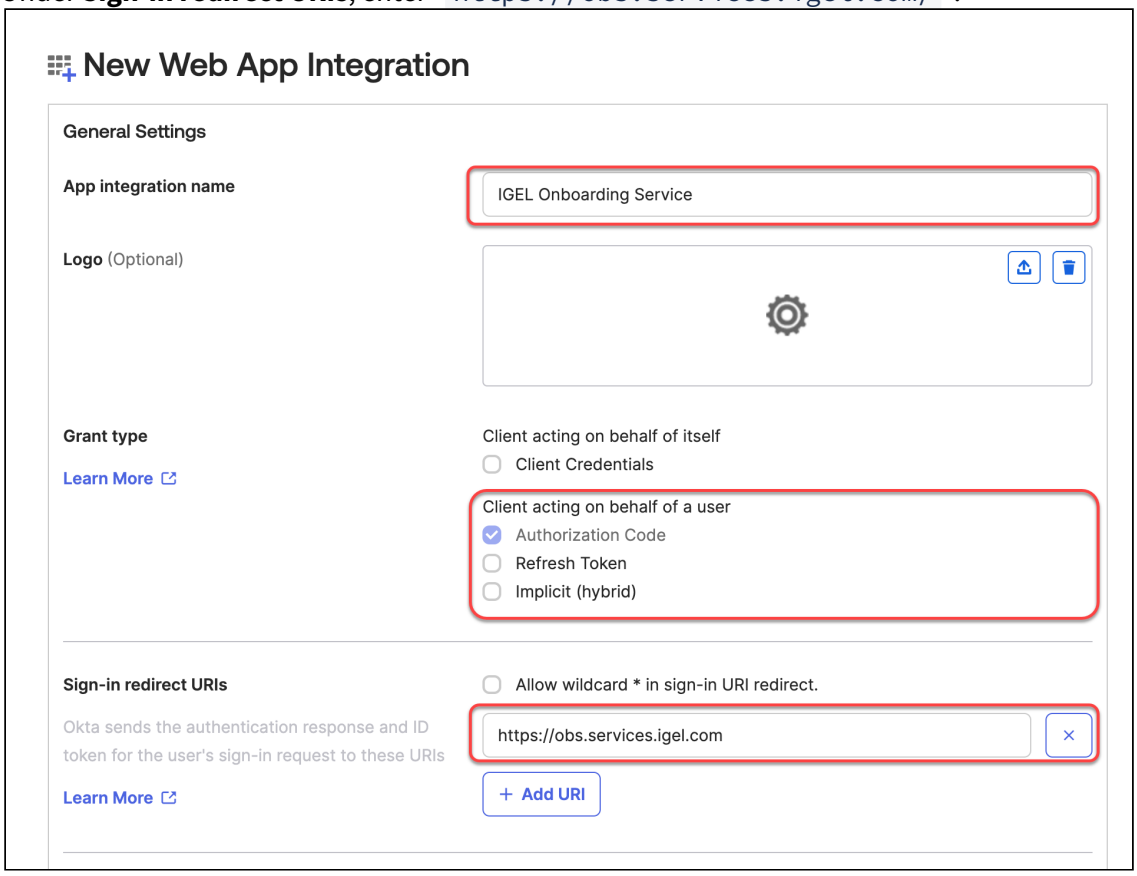
2. Edit the settings as follows and then click **Next**.
   - Set **Sign-in method** to **OIDC**.

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

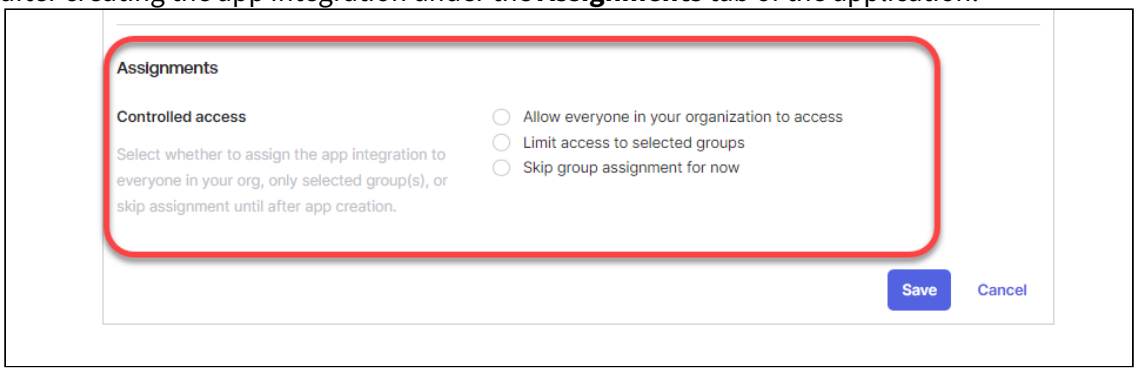


3. Edit the settings as follows and then click **Save**.
   - Under **App integration name**, enter a name for your application, e.g. "IGEL Onboarding Service".
   - Make sure that as the **Grant type**, the option **Authorization Code** is selected.

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

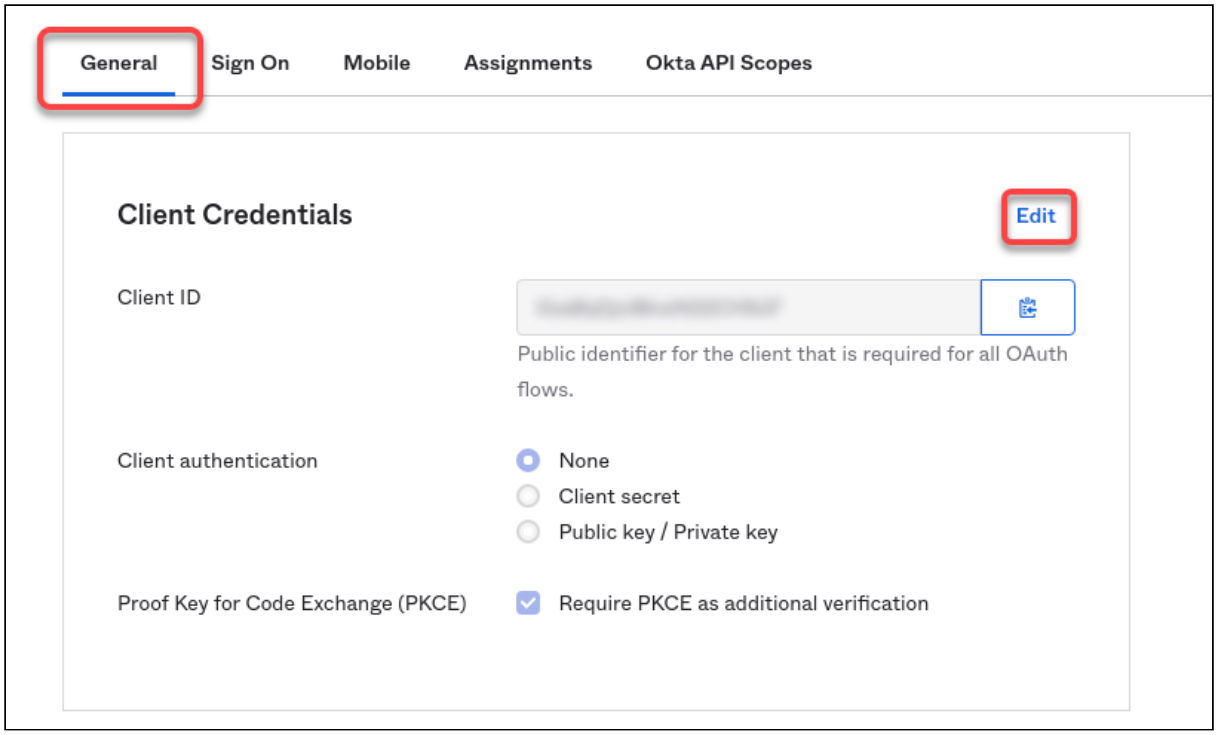


- Under **Assignments**, depending on your company policy, either allow everyone or select an existing group configured under **Directory > Groups**. You can change this configuration after creating the app integration under the **Assignments** tab of the application.

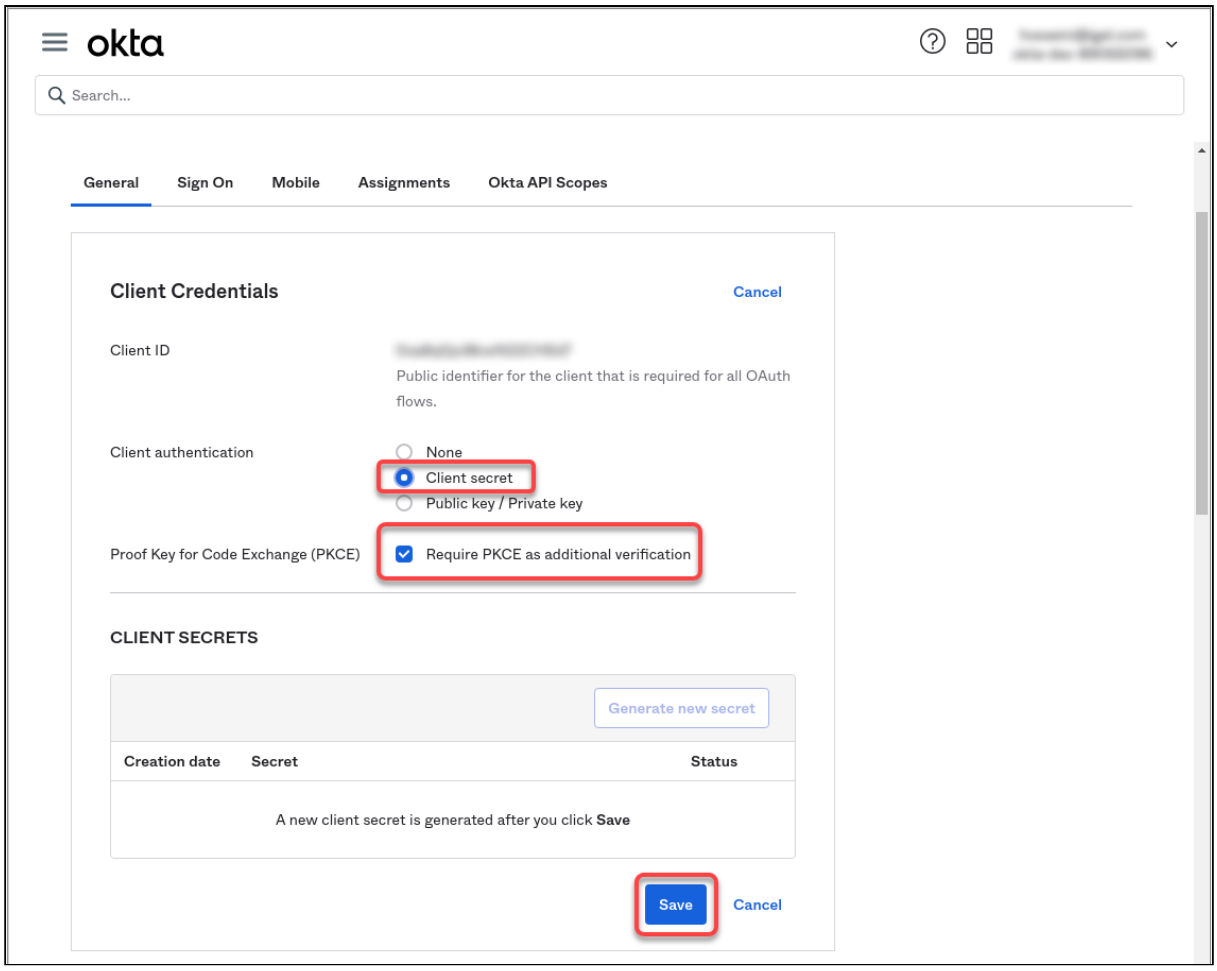


The app integration is created.

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



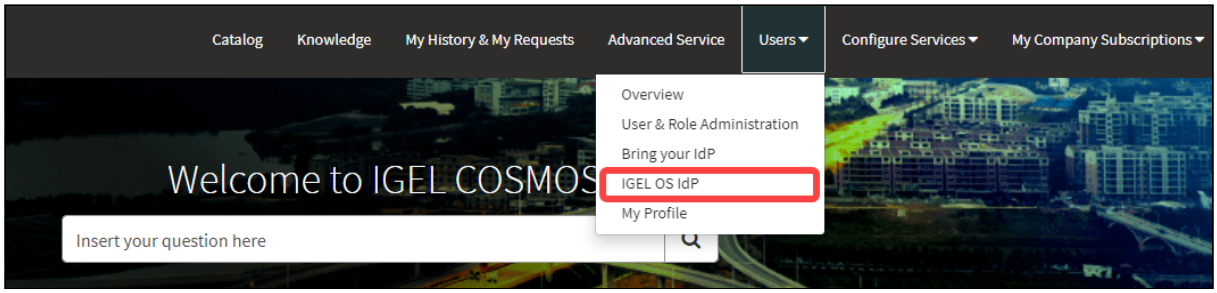
5. Under **Client authentication**, select **Client secret** and make sure that under **Proof Key for Code Exchange (PKCE)**, **Require PKCE as additional verification** is enabled. Afterward, click **Save**.



The client secret will be created.

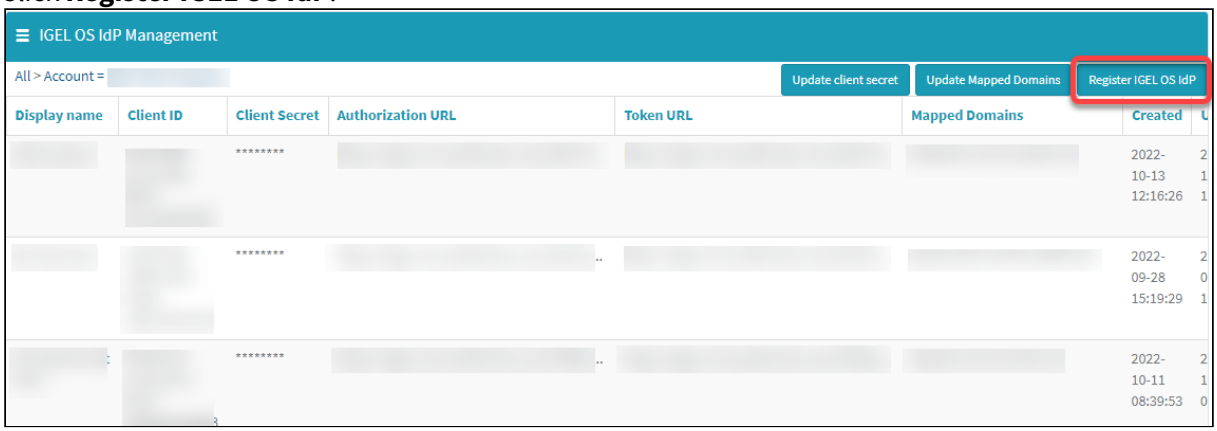
Registering Our Okta Application in the IGEL Customer Portal

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

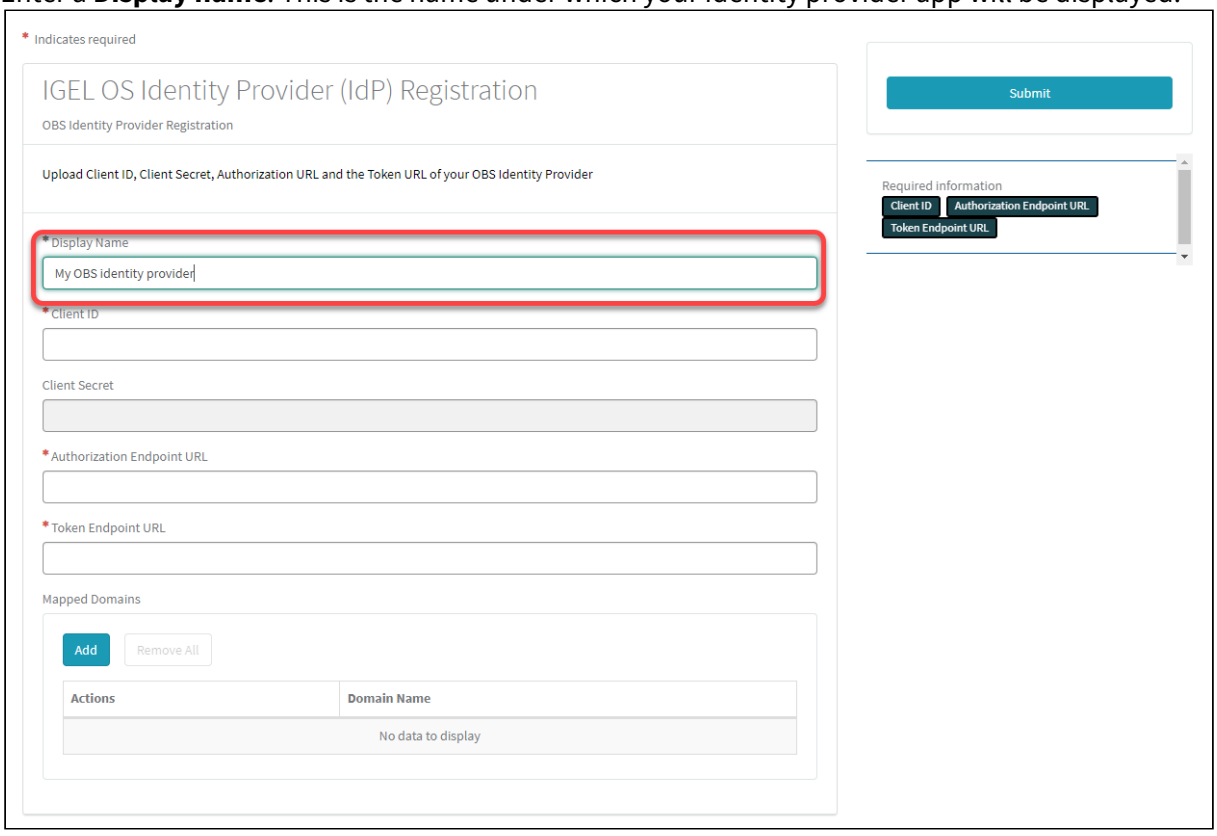


17 https://cosmos.igel.com/

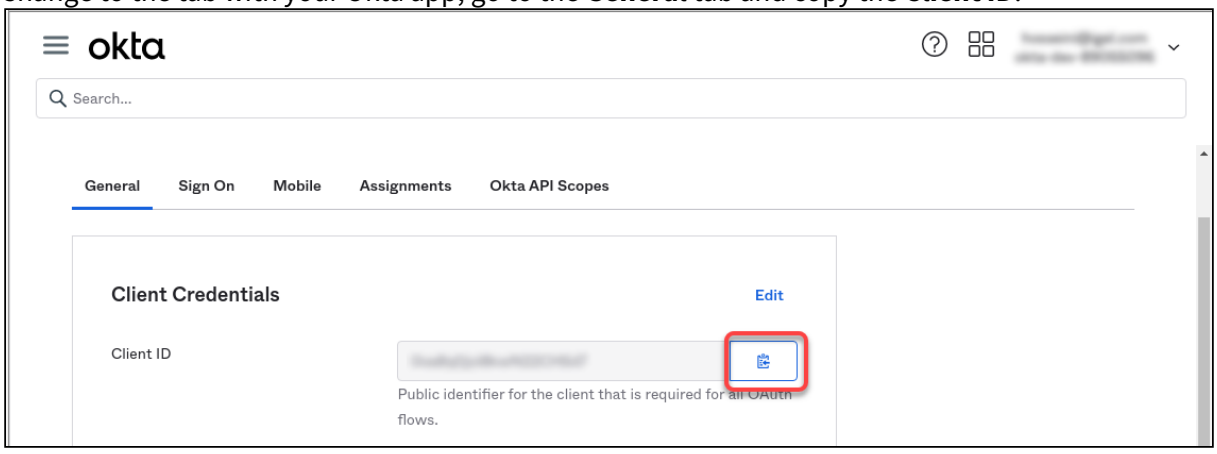
2. Click **Register IGEL OS IdP**.



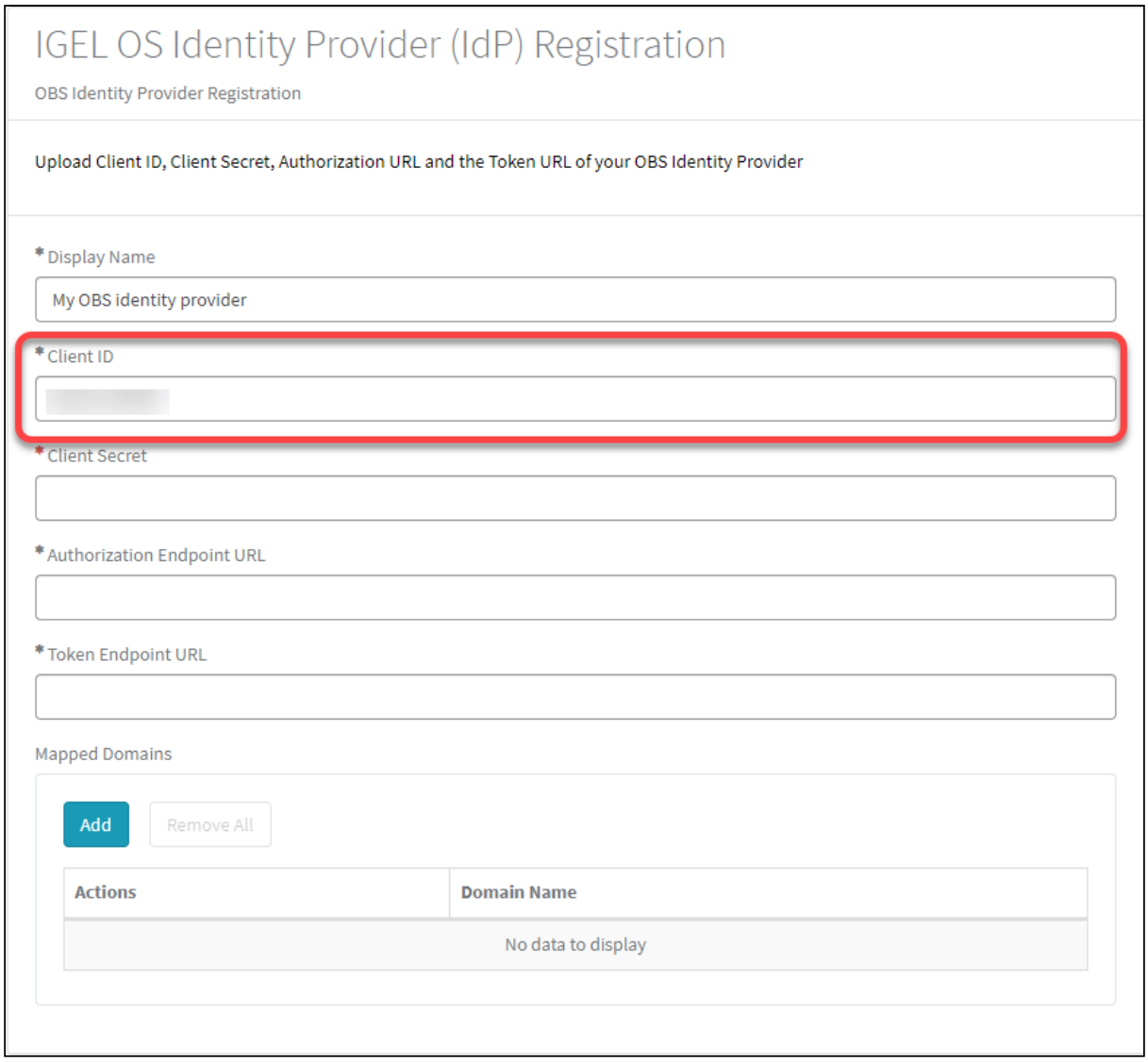
3. Enter a **Display name**. This is the name under which your identity provider app will be displayed.



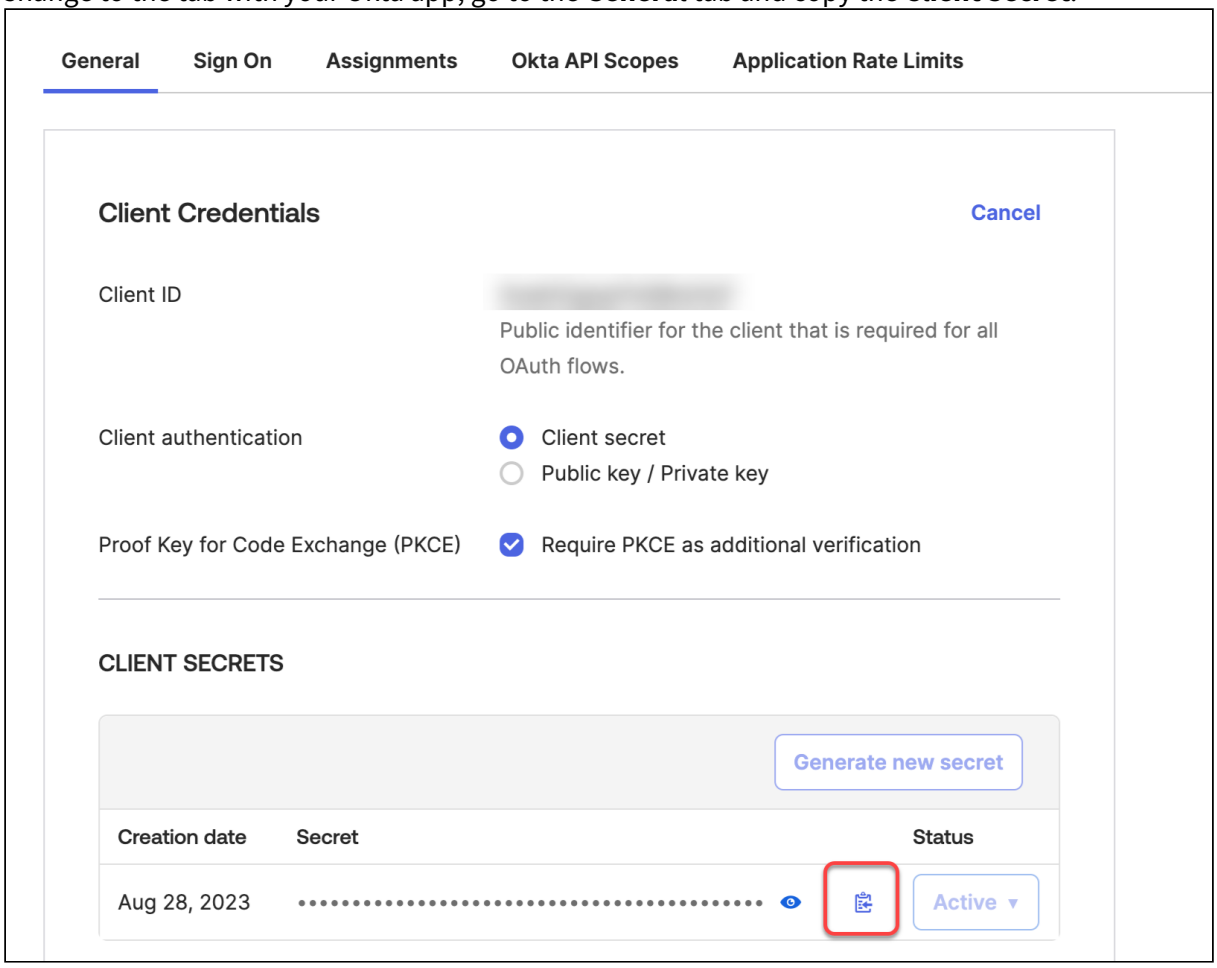
4. Change to the tab with your Okta app, go to the **General** tab and copy the **Client ID**.



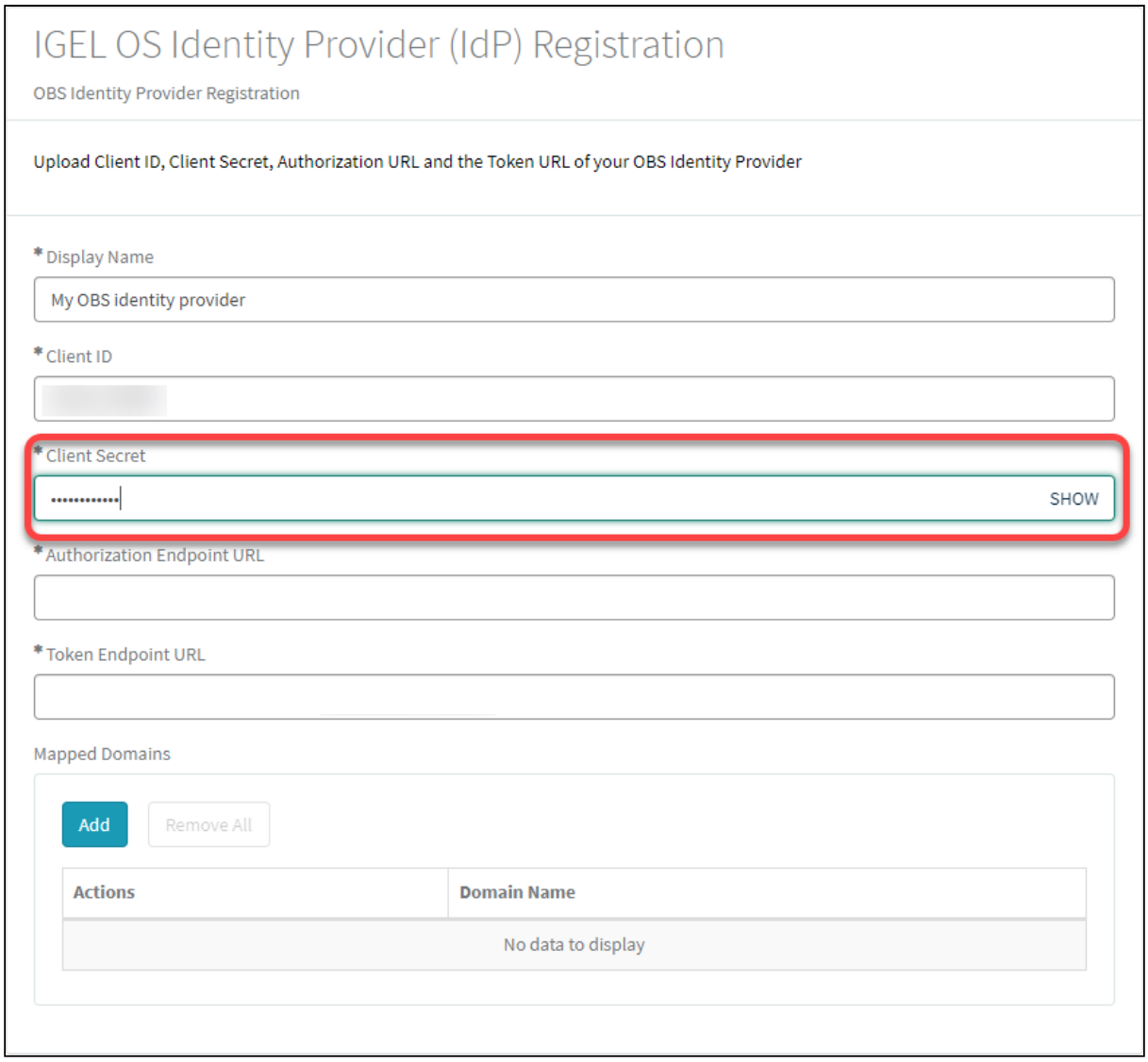
5. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client ID into the field **Client ID**.


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
Add
Remove All
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**.

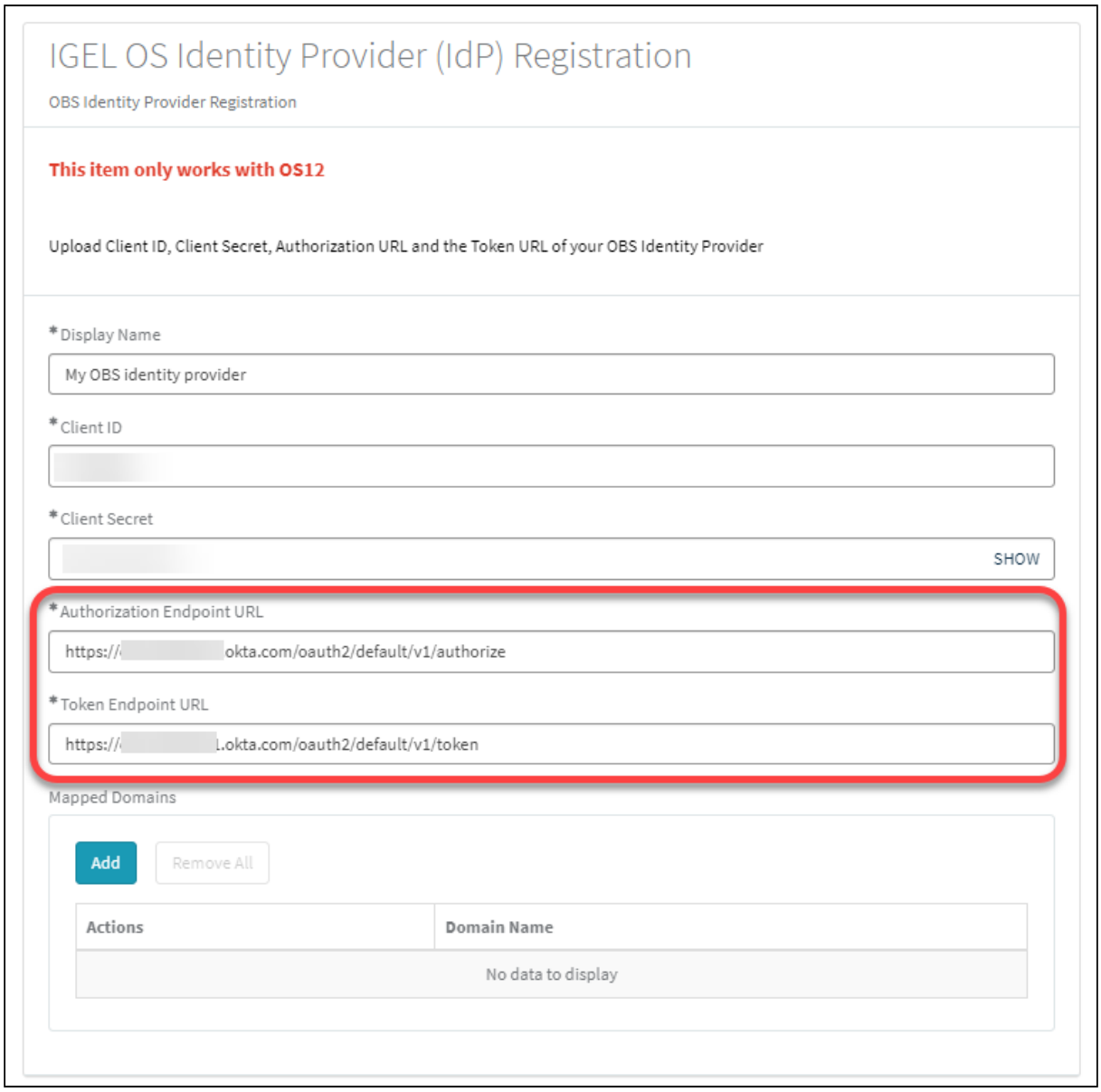


7. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client secret into the field **Client secret**.

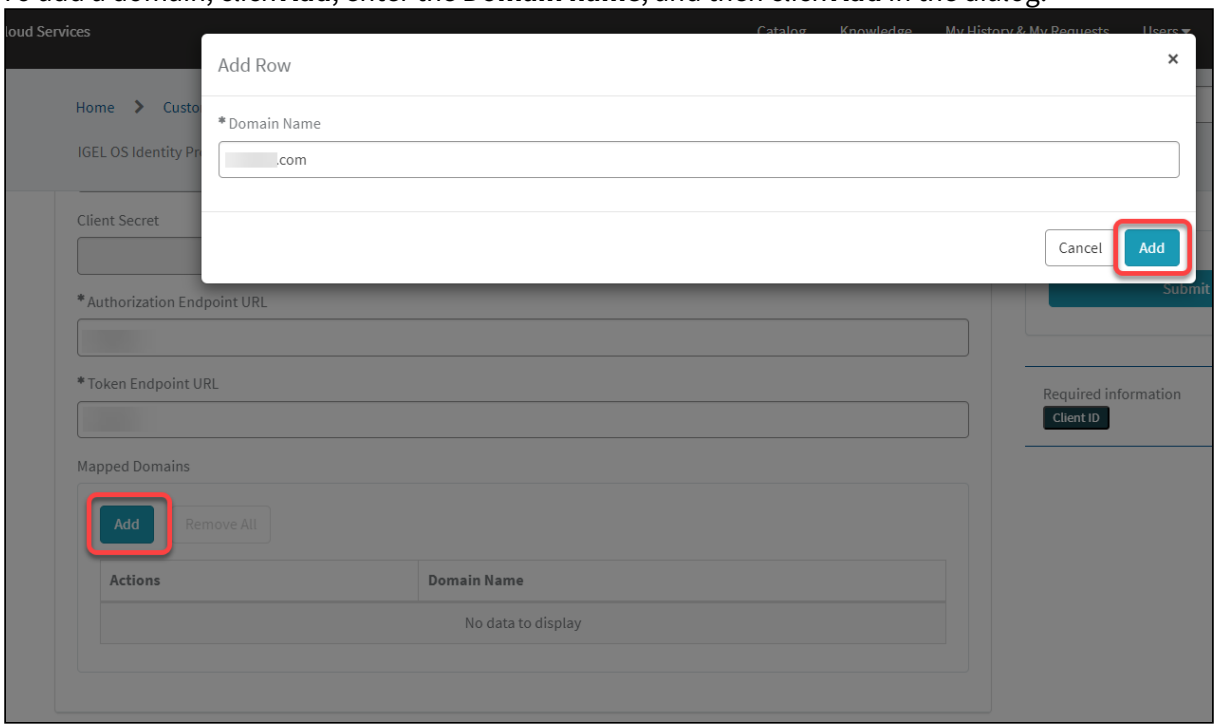


8. To get the **Authorization Endpoint URL** and **Token Endpoint URL** enter into your browser: `https://<yourOktaOrg>/.well-known/openid-configuration`
Example: https://dev-xxxxxx-admin.okta.com/.well-known/openid-configuration

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
*Client Secret
SHOW
*Authorization Endpoint URL
https://okta.com/oauth2/default/v1/authorize
*Token Endpoint URL
https://.okta.com/oauth2/default/v1/token
Mapped Domains
Add
Remove All
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.

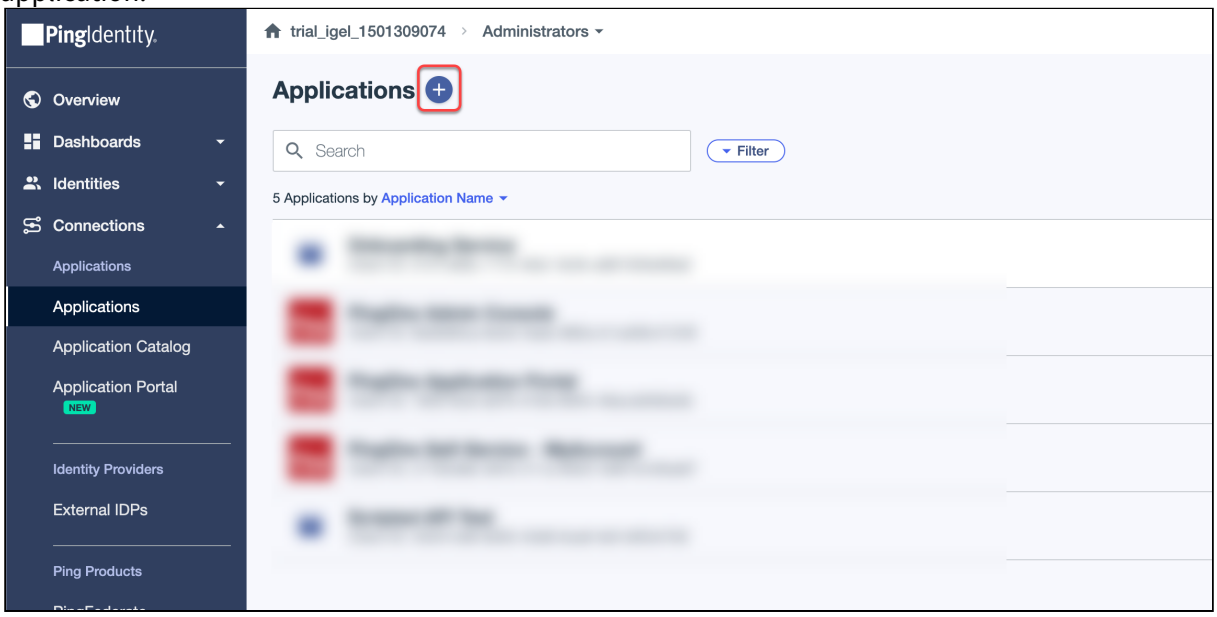
Configuring Ping as Identity Provider

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.

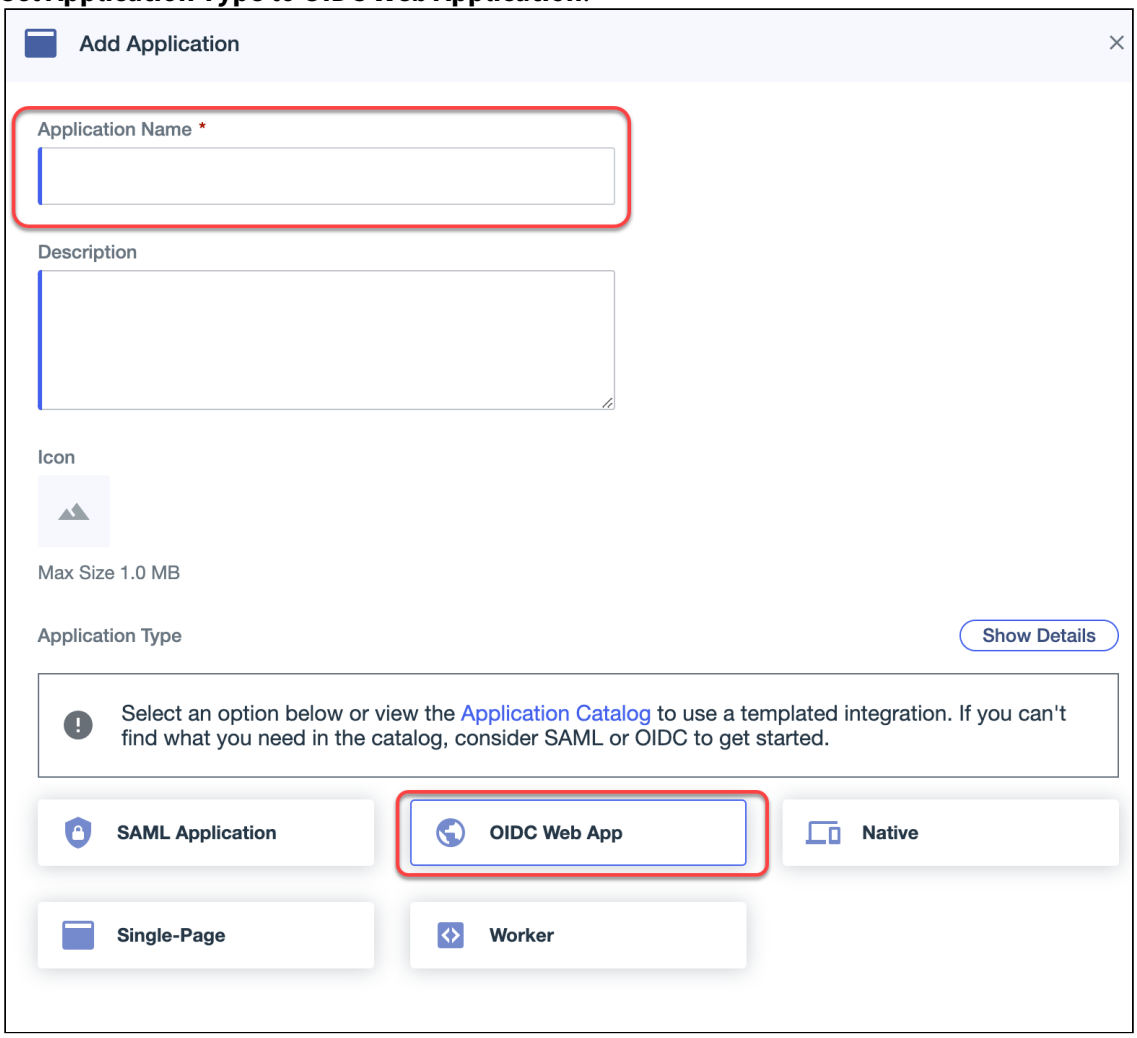
Creating a Ping Application That Will Serve as Identity Provider

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



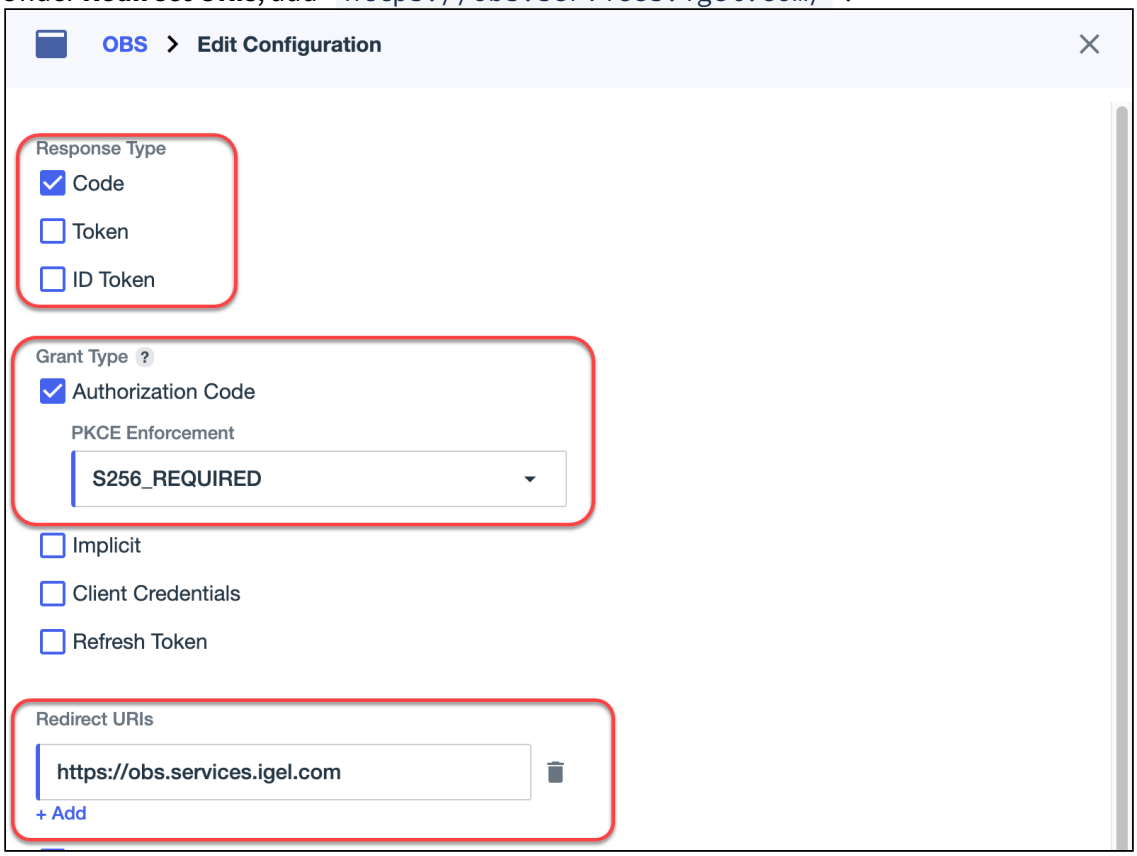
2. Edit the settings as follows and then click **Next**.
   - Under **Application Name**, enter a name for your application, e.g. "OBS".

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

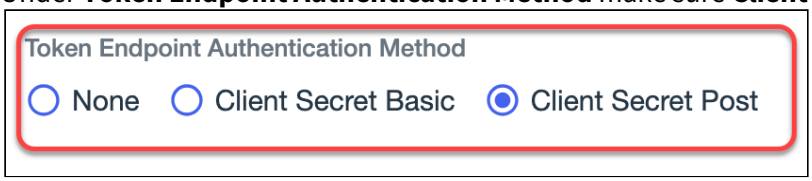


3. Edit the settings under **Edit Configuration** as follows and then click **Save**.
   - Under **Response Type**, make sure **Code** is selected.
   - Make sure that as the **Grant Type**, the option **Authorization Code** is selected and that the **Proof Key for Code Exchange (PKCE) Enforcement**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

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

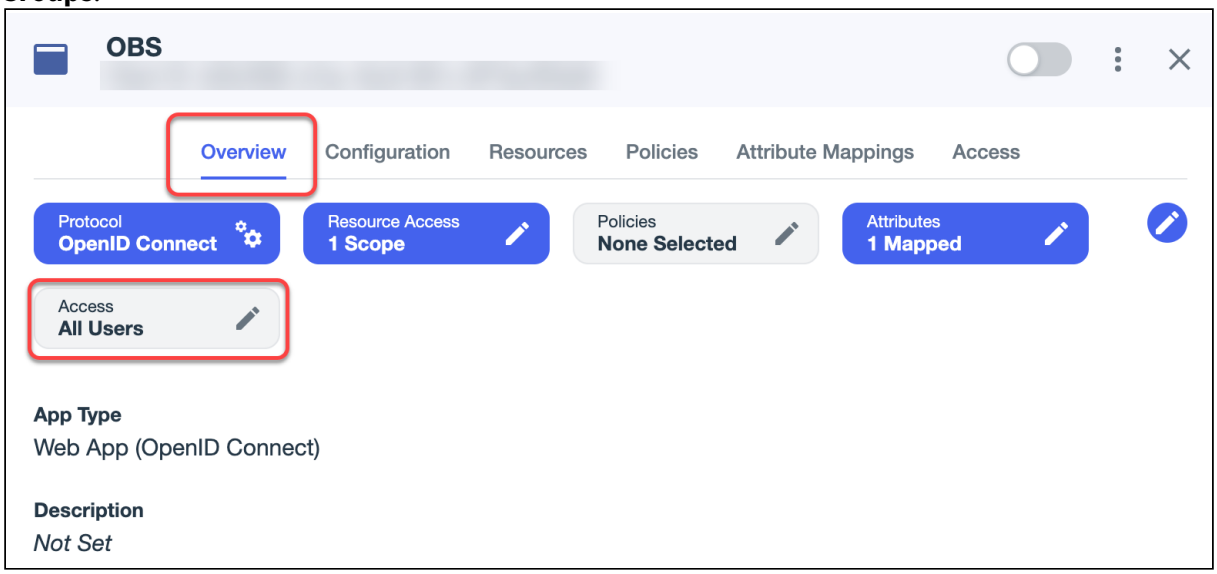


- Under **Token Endpoint Authentication Method** make sure **Client Secret Post** is selected.



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 >**

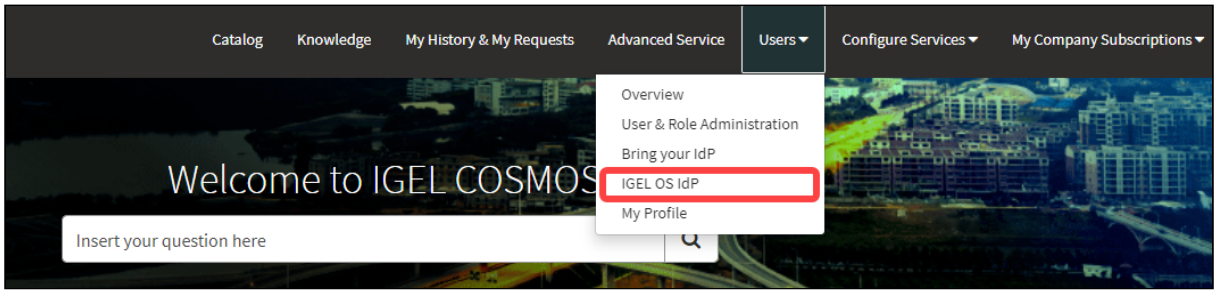
Groups.



The app integration is created.

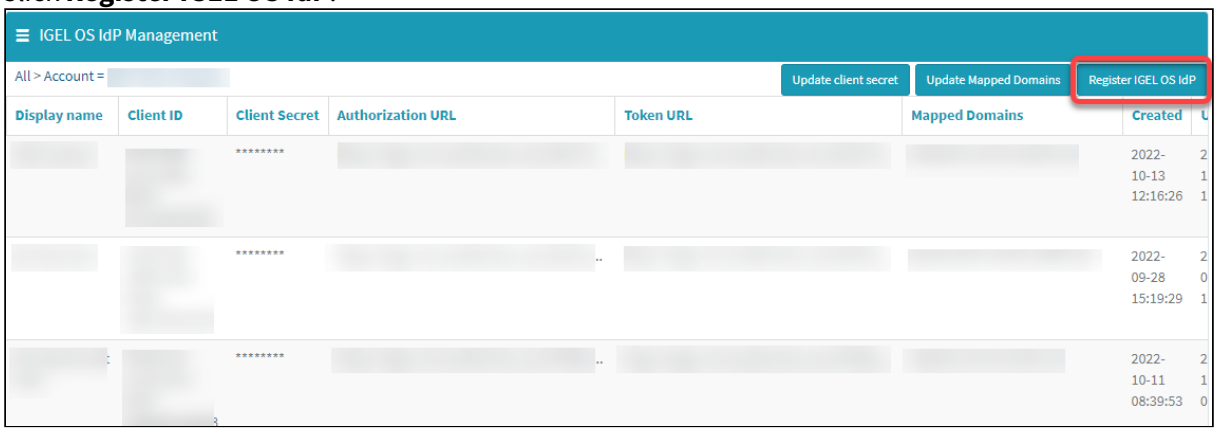
Registering Our Ping Application in the IGEL Customer Portal

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

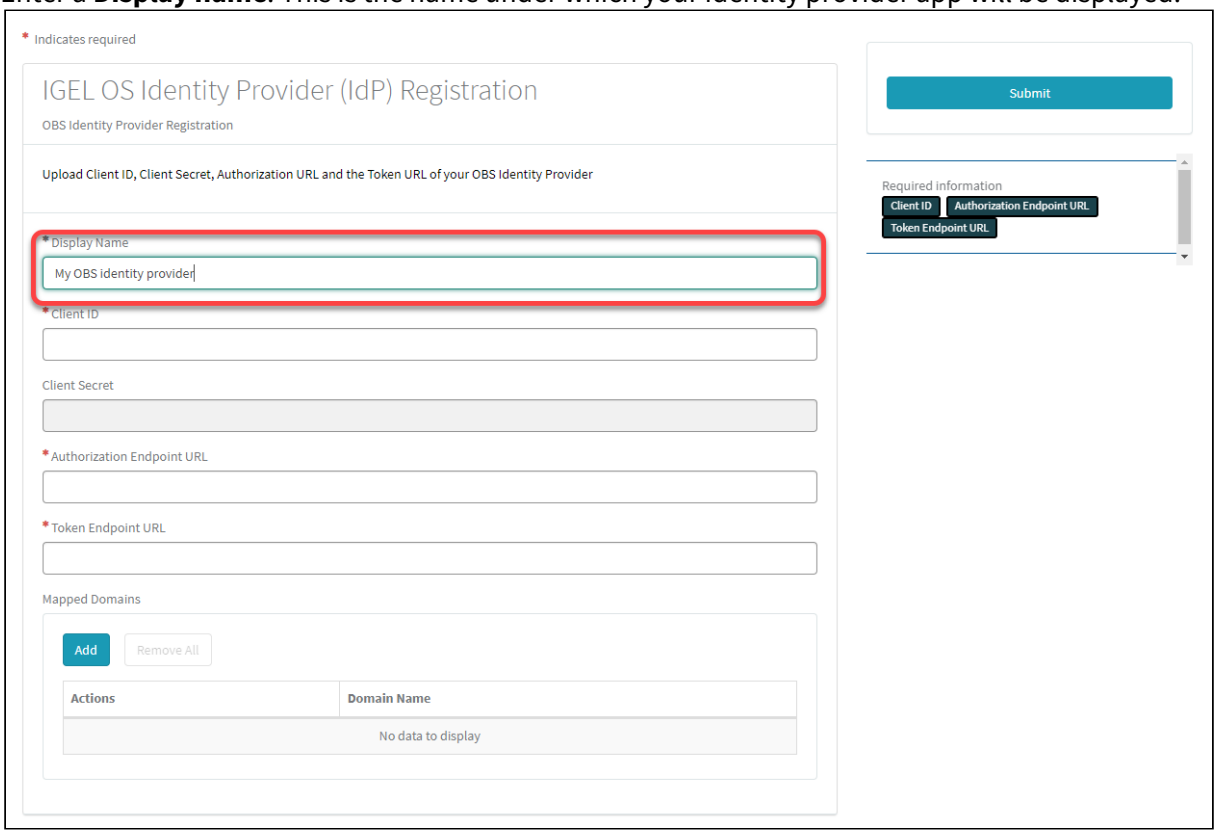


18 https://cosmos.igel.com/

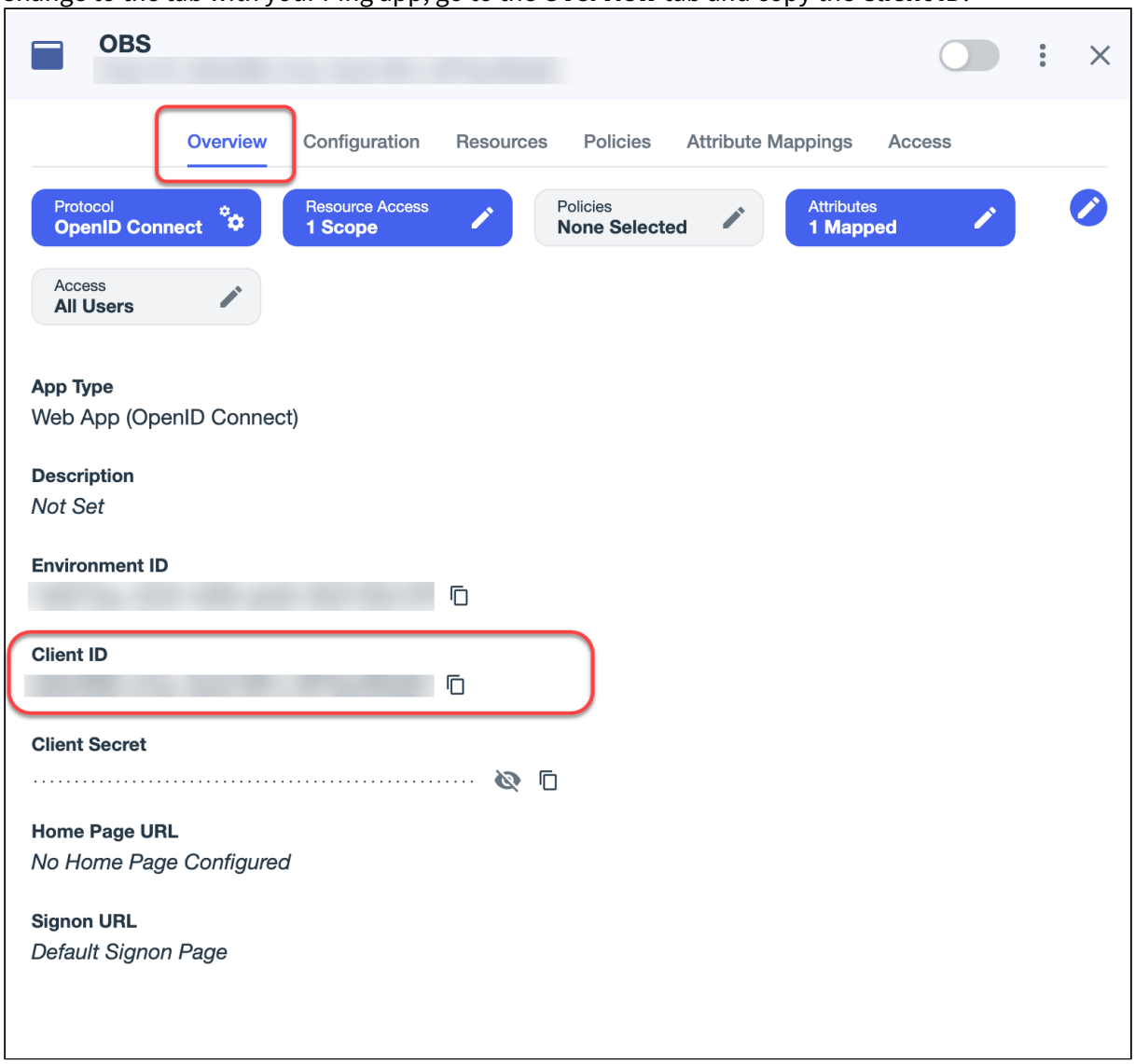
2. Click **Register IGEL OS IdP**.



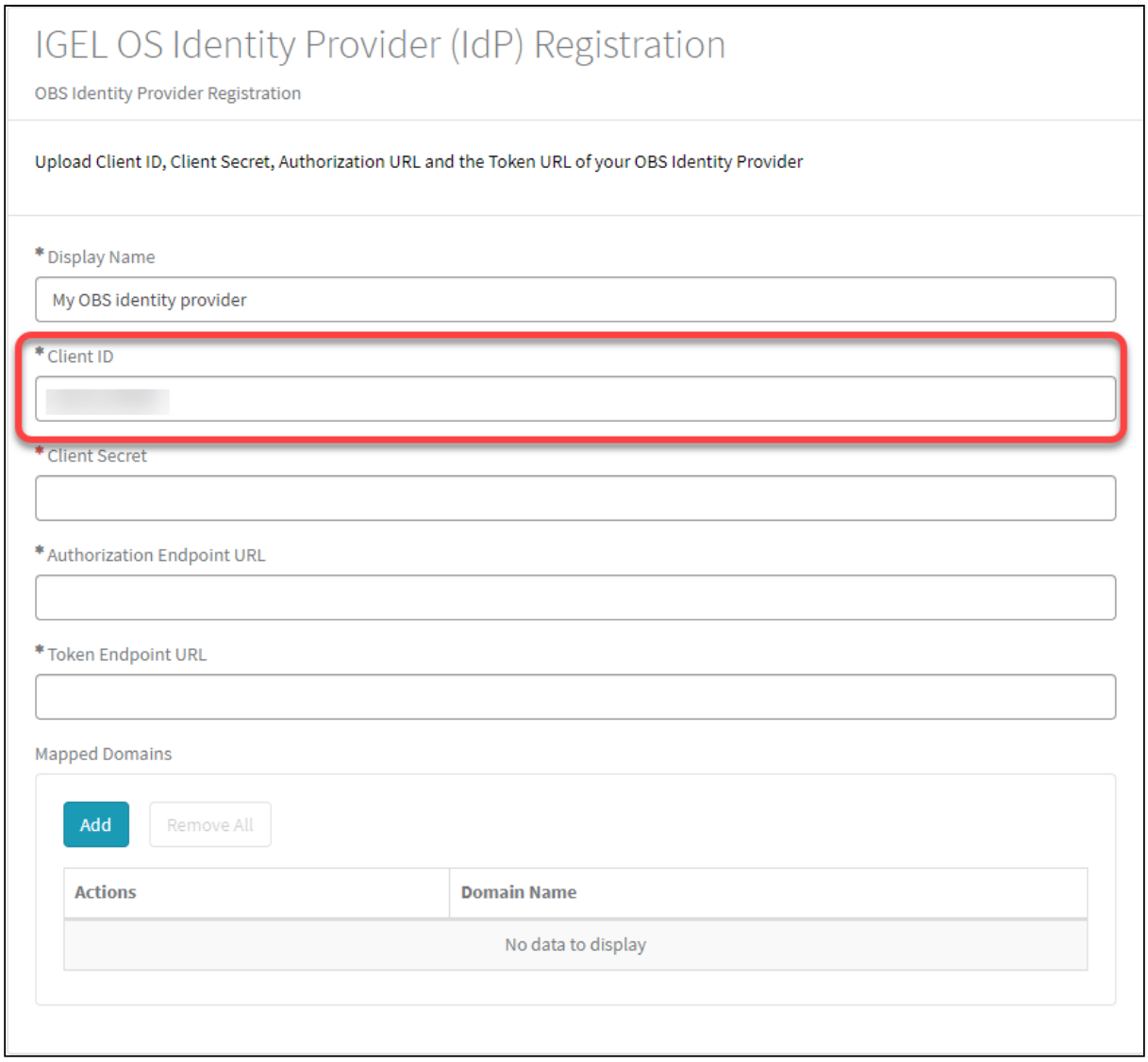
3. Enter a **Display name**. This is the name under which your identity provider app will be displayed.



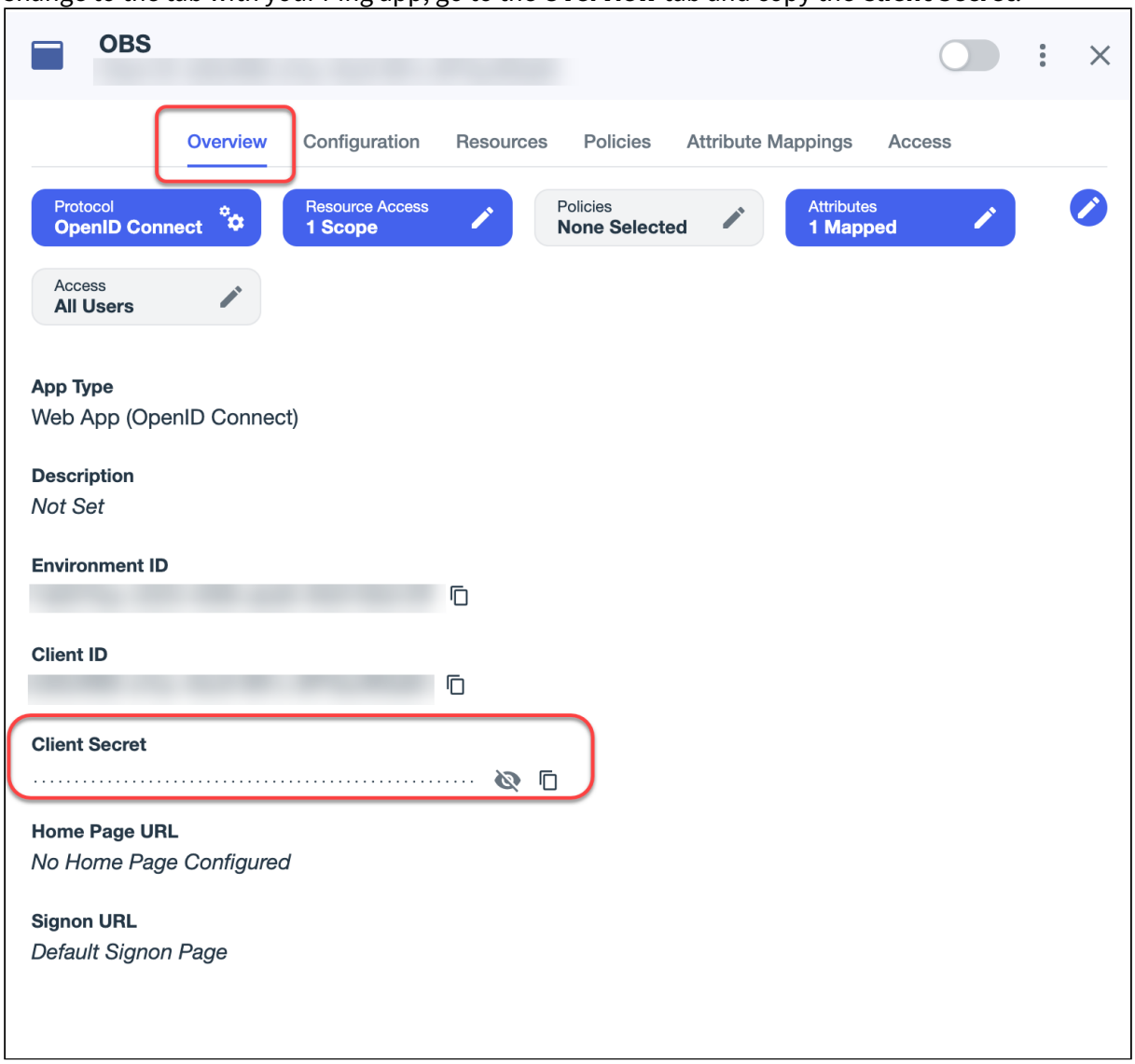
4. Change to the tab with your Ping app, go to the **Overview** tab and copy the **Client ID**.



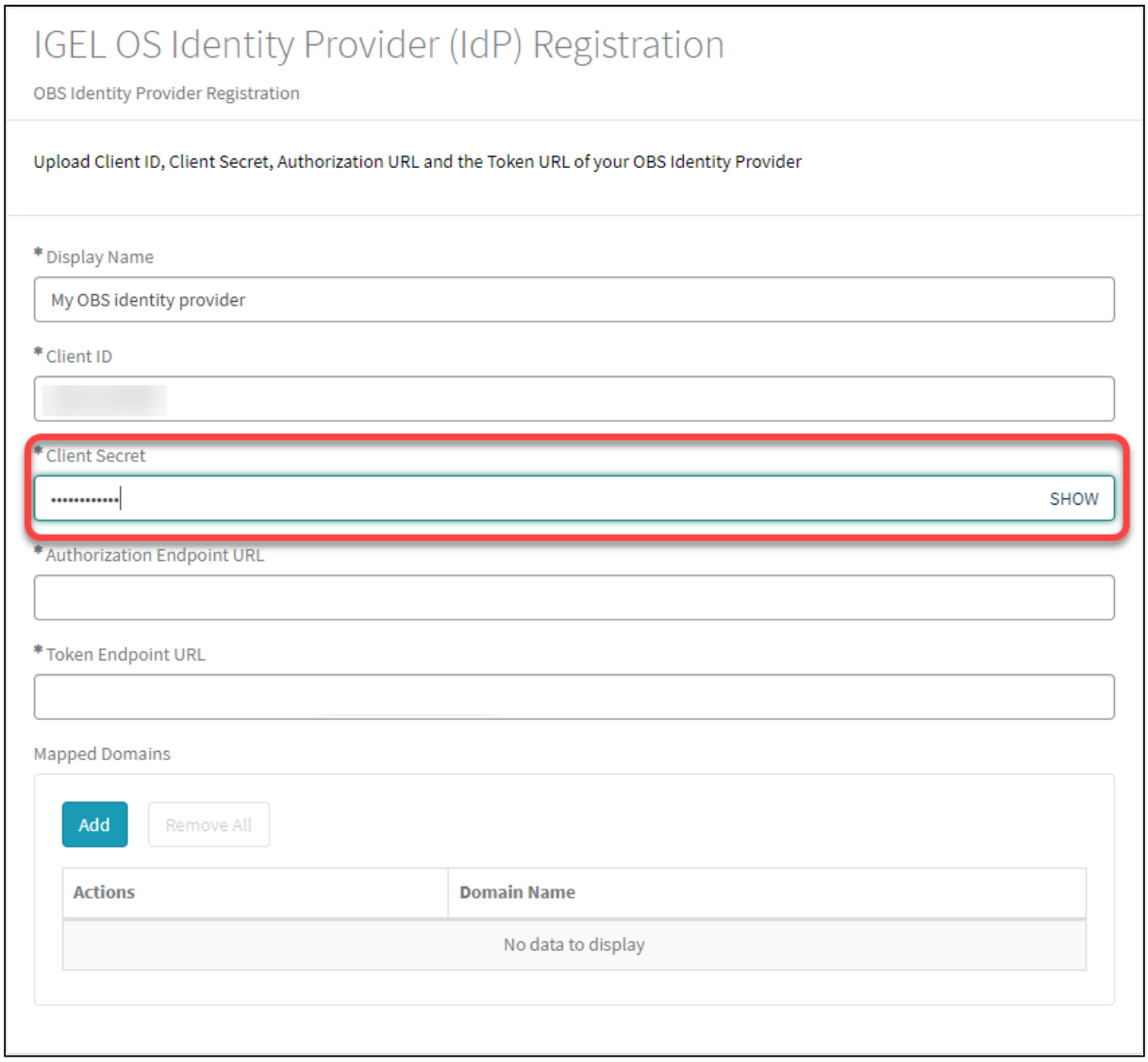
5. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client ID into the field **Client ID**.


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
Add
Remove All
Actions
Domain Name
No data to display

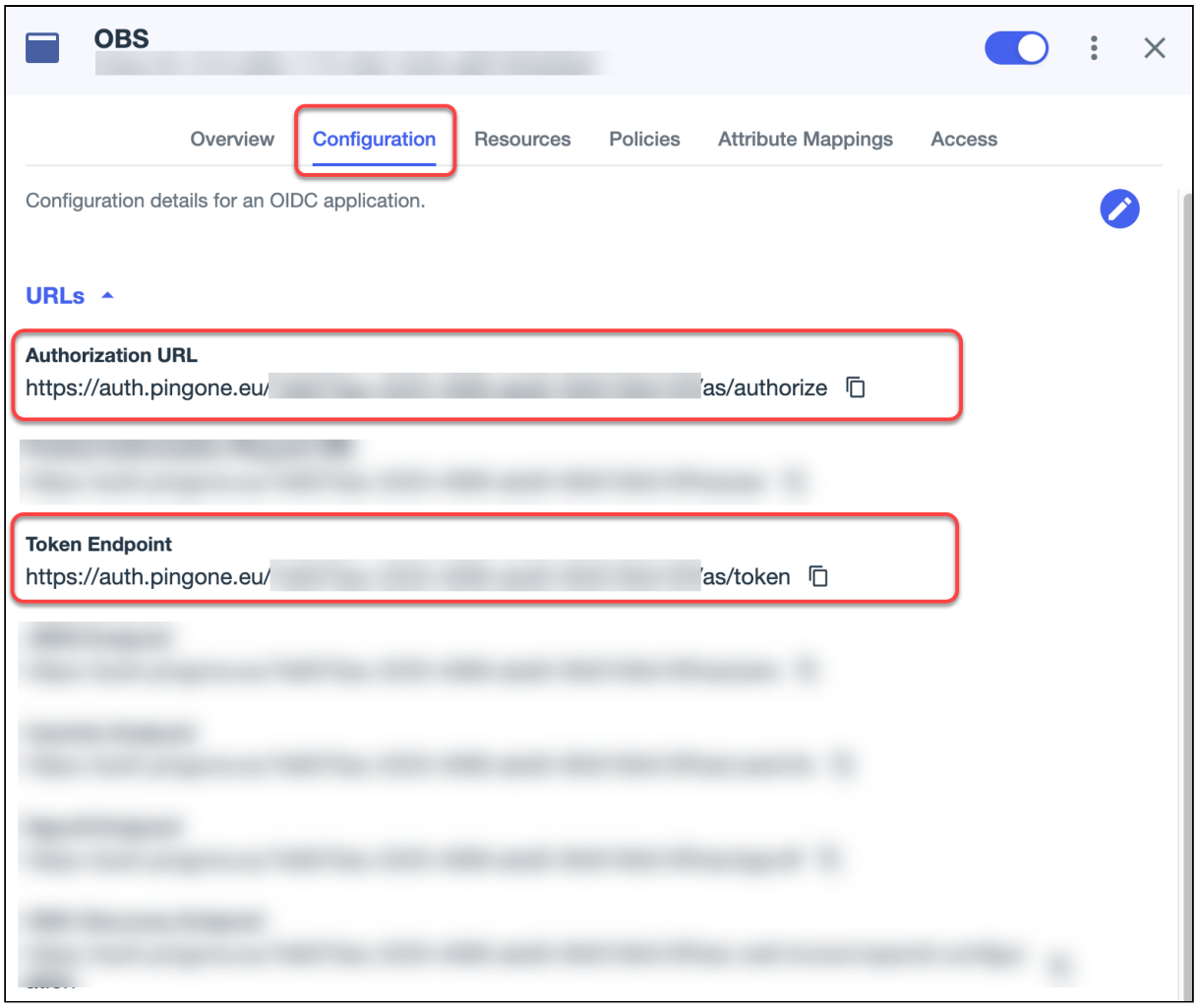
6. Change to the tab with your Ping app, go to the **Overview** tab and copy the **Client Secret**.



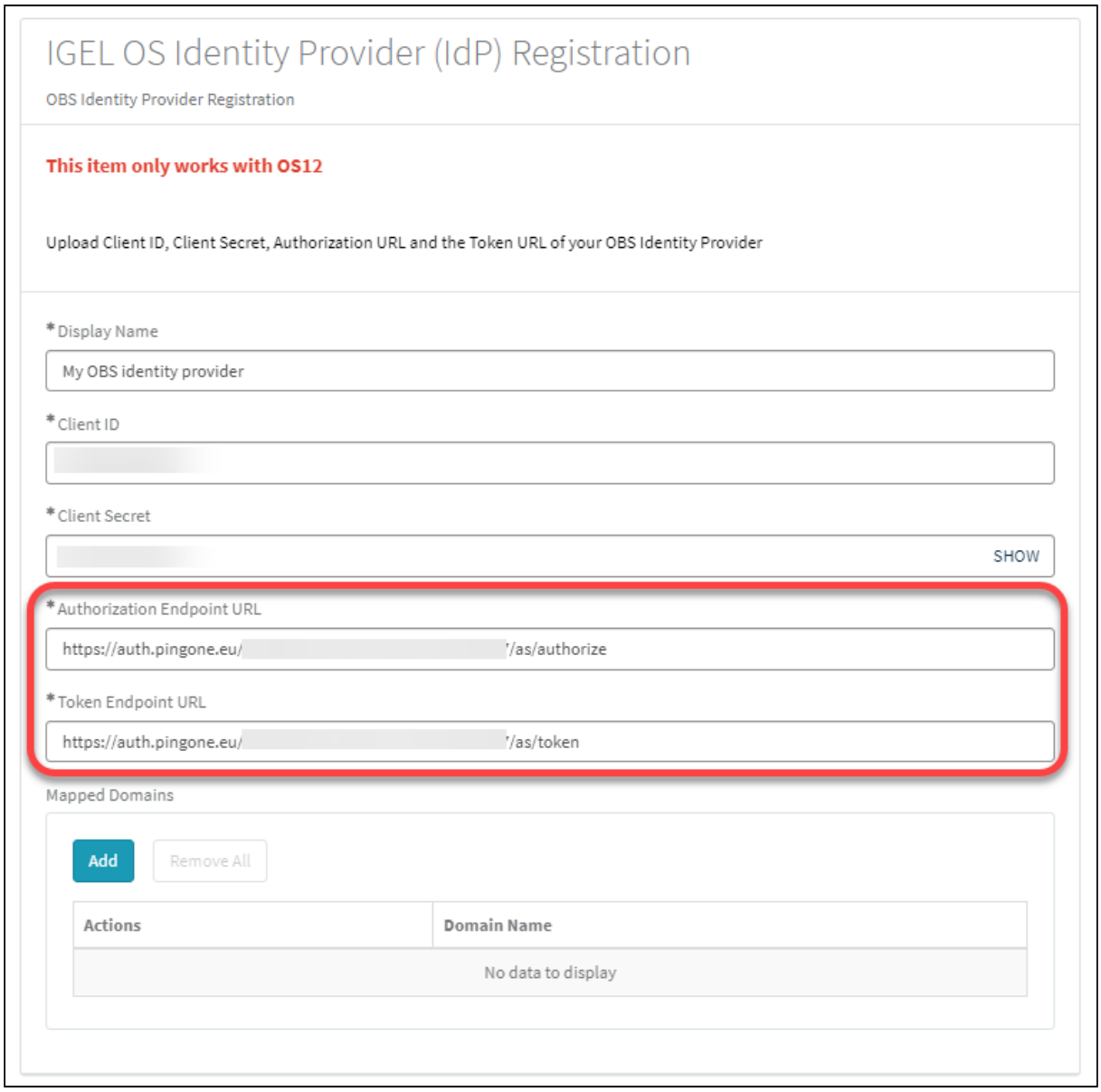
7. Change to the IGEL Customer Portal (**IGEL OS Identity Provider (IdP) Registration**) tab and paste the client secret into the field **Client secret**.



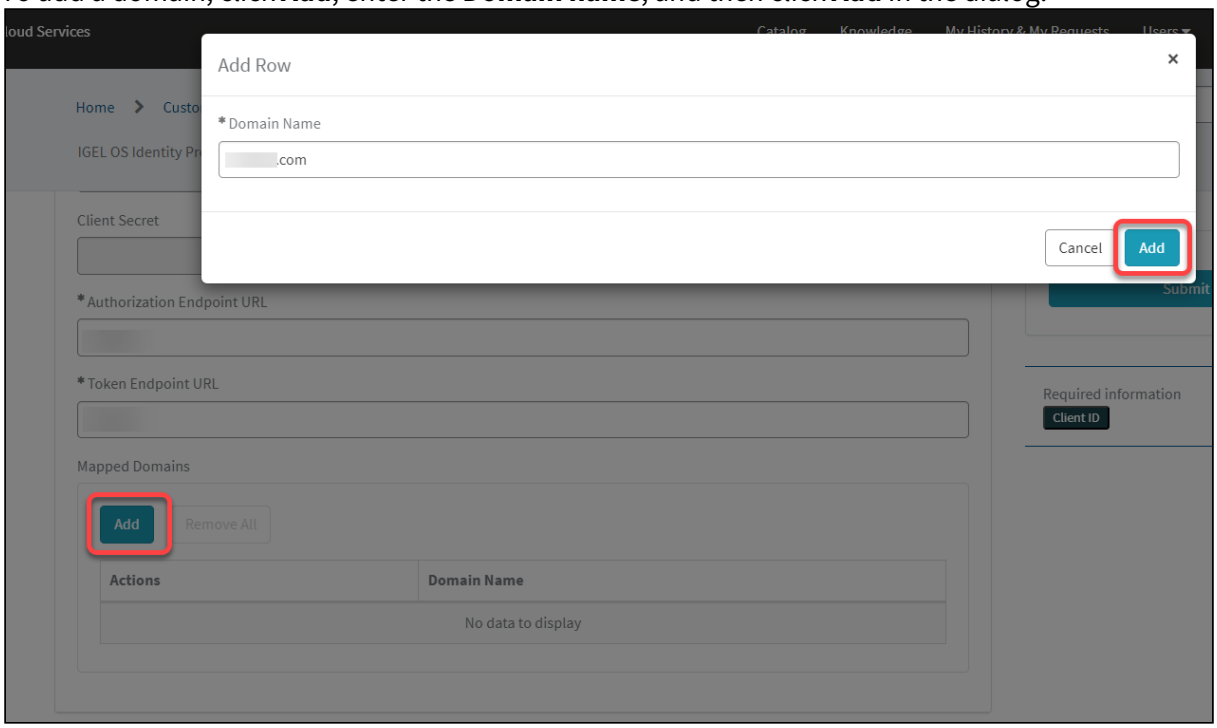
8. To get the **Authorization Endpoint URL** and **Token Endpoint URL**, change to the tab with your Ping app and go to the **Configuration** tab.



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
*Client Secret
SHOW
*Authorization Endpoint URL
https://auth.pingone.eu/ /as/authorize
*Token Endpoint URL
https://auth.pingone.eu/ /as/token
Mapped Domains
Add
Remove All
Actions
Domain Name
No data to display

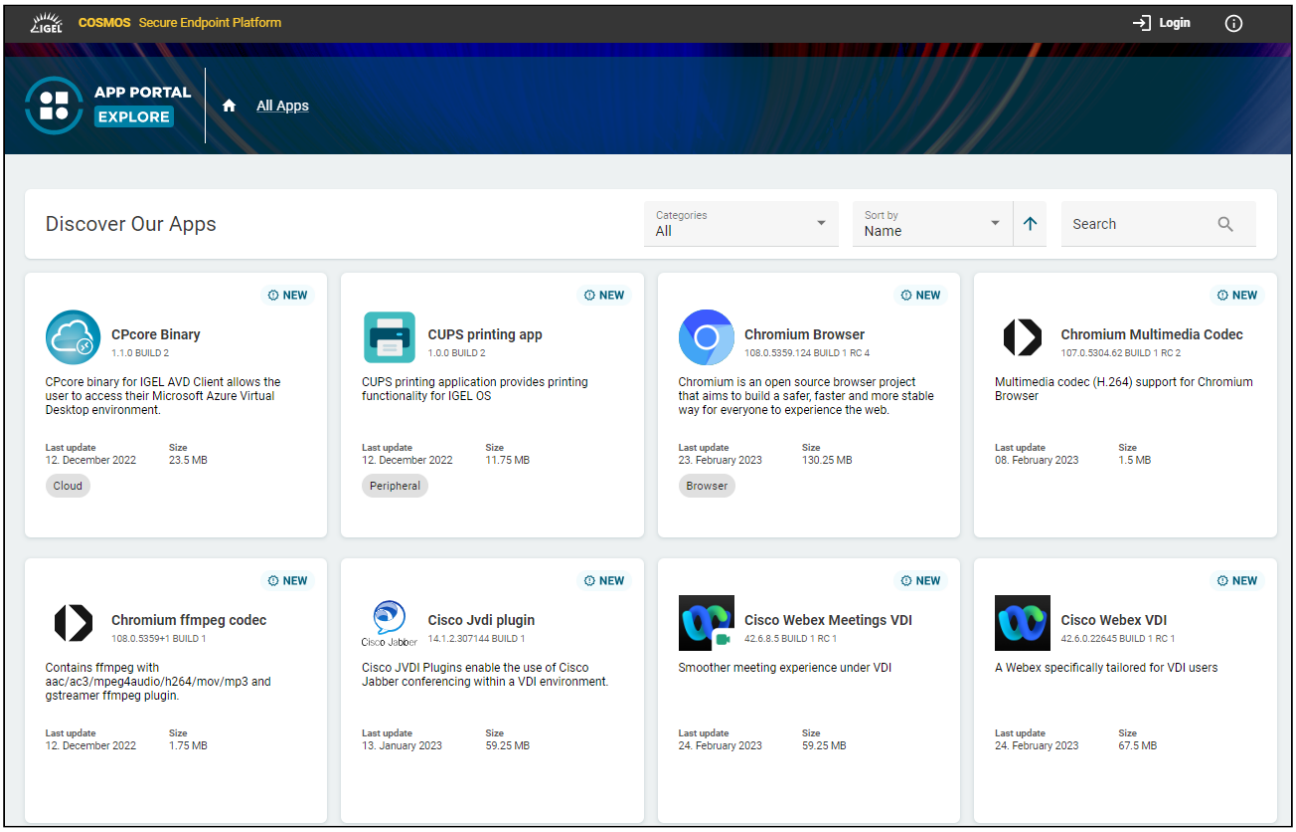
10. To add a domain, click **Add**, enter the **Domain name**, and then click **Add** in the dialog.



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.



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).

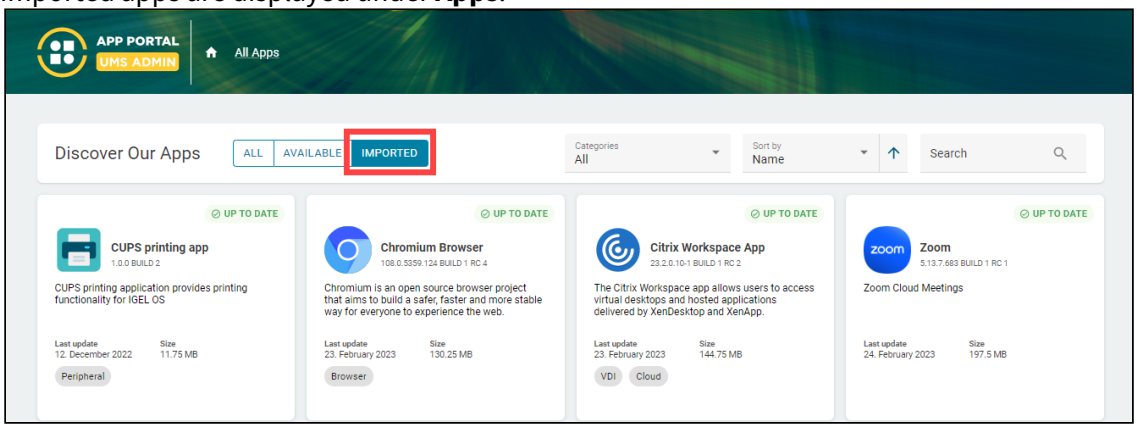
If the device is not managed with the UMS, the download of apps is possible but NOT for the devices with a Starter license. For more information on licenses, see Licensing(see page 151).

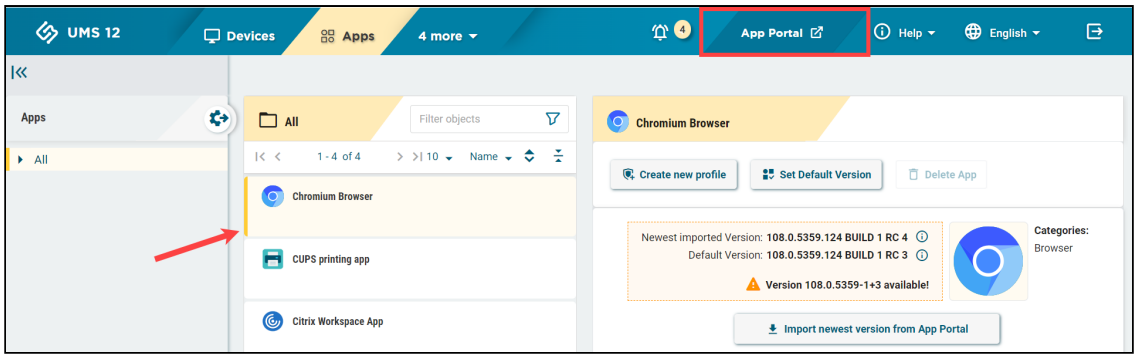
You can open the IGEL App Portal

- 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 188).
  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.
  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**.

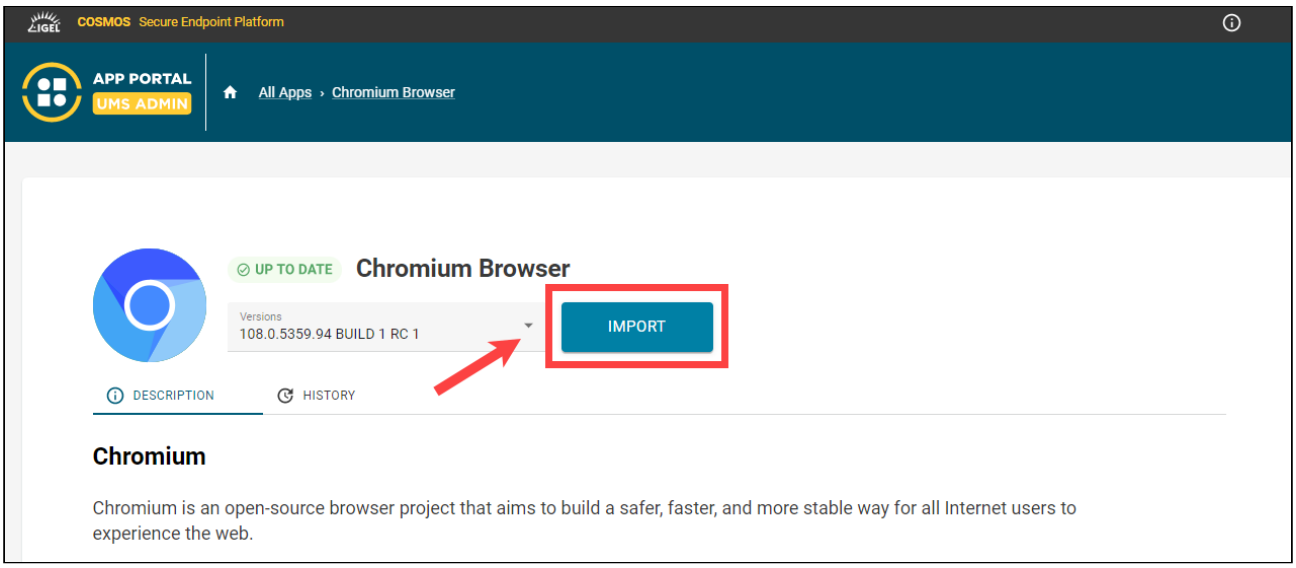




For permissions required for managing apps, see Important Information for the IGEL UMS Web App.

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.



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)

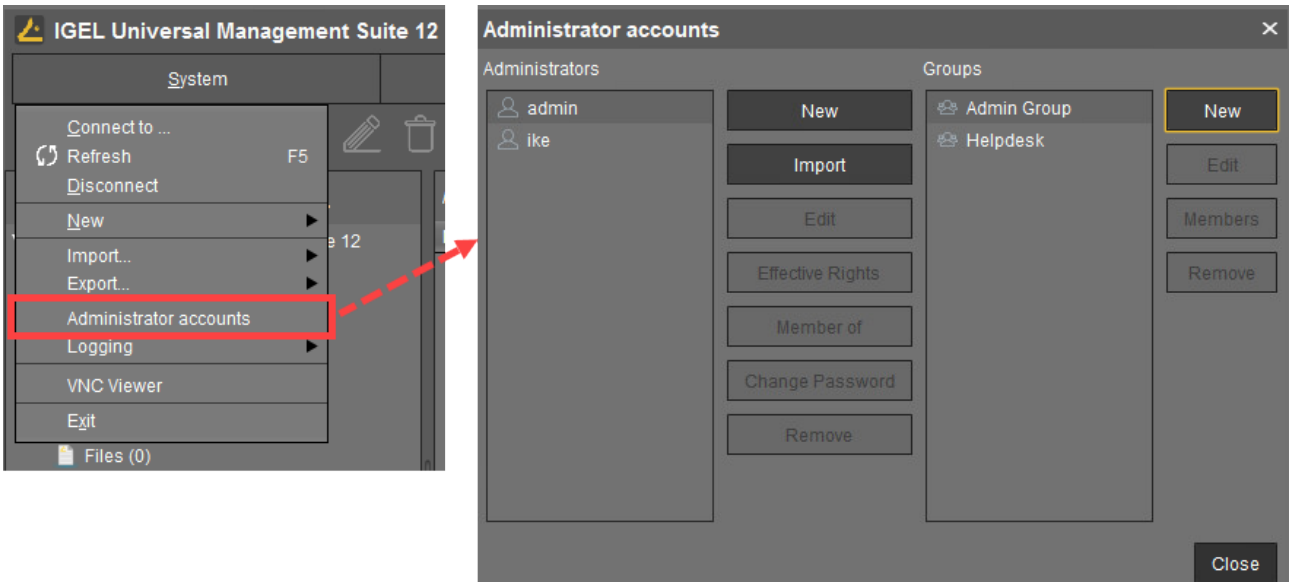
3. If you want to activate the naming convention for your devices, go to **UMS Administration > Global Configuration > Device Network Settings**. For more information, see Renaming IGEL OS Devices.

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**.

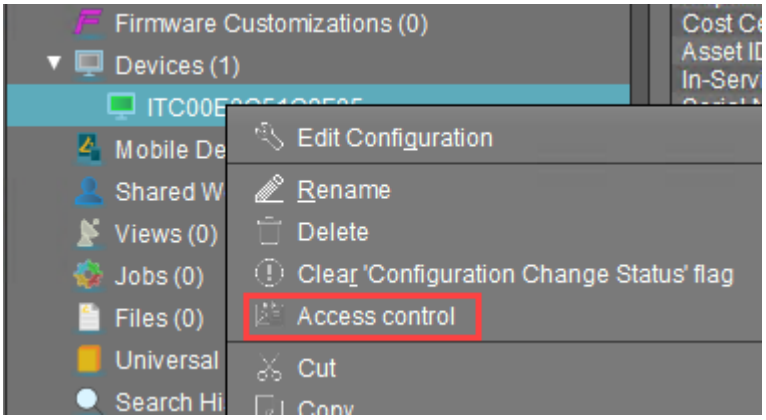
If you do not want to adopt the Active Directory structure, you can create local administrators and groups manually: **UMS Console > System > Administrator Accounts > New**.

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:

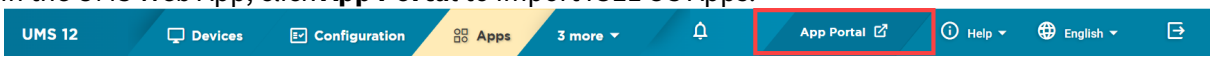
▶ Right-click an object in the structure tree and select **Access control** in the context menu to set object permissions.



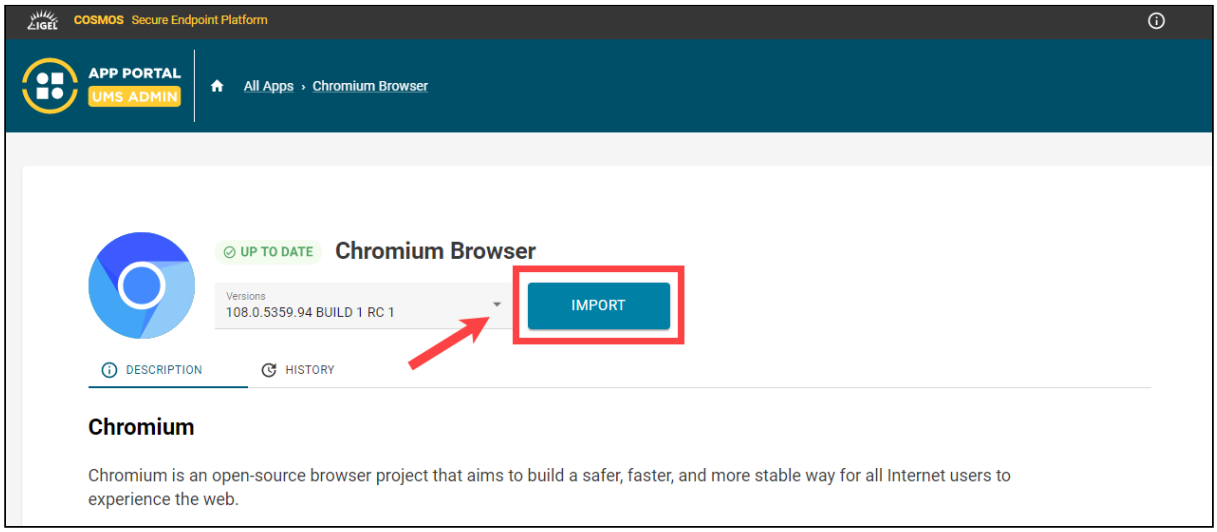
For more information on UMS administrator accounts and access rights, refer to Create Administrator Accounts.
For permissions required for the UMS Web App, incl. for managing apps, see Important Information for the IGEL UMS Web App.

Optional: Preconfiguring Your Devices Before Onboarding

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

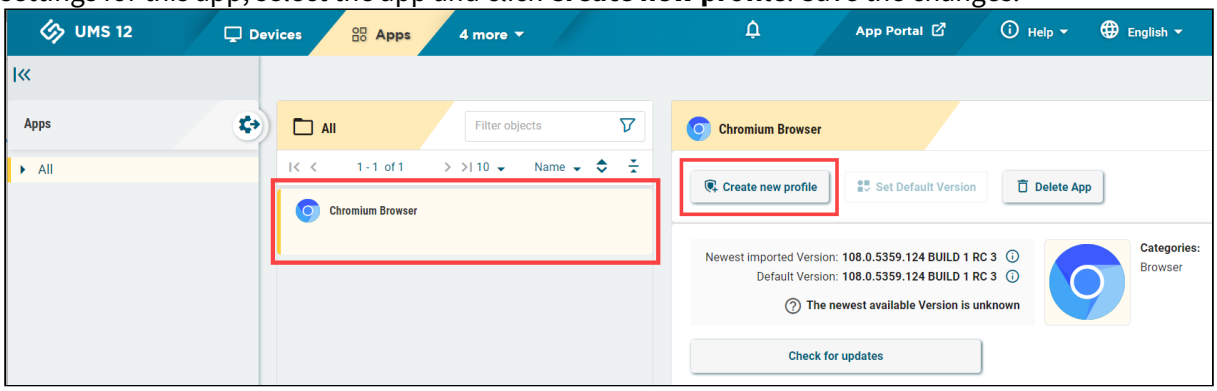


2. Select an app and the required version and click **Import**.
   After accepting the End User License Agreement (EULA), the selected app version will be imported into the UMS.

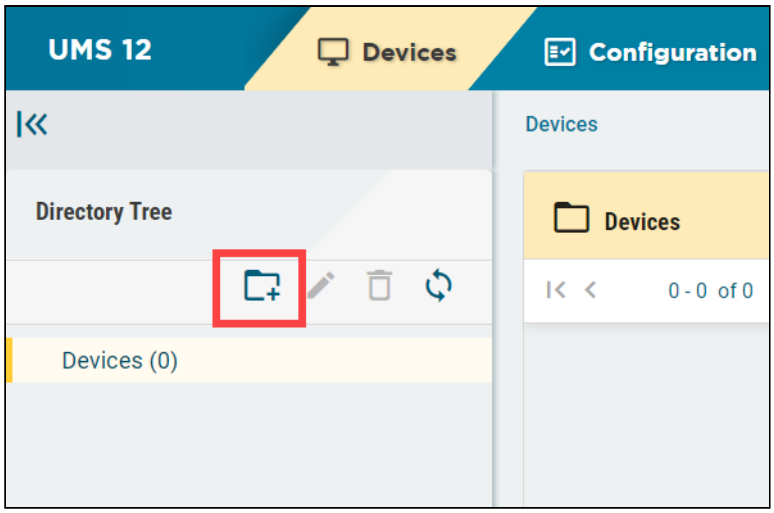


> ⚠ If you want to create profiles configuring IGEL OS Base System settings (e.g. corporate design, SSO(see page 193), accesories, etc.) before any of your IGEL OS 12 devices is registered with the UMS, import the IGEL OS Base System app. The latest app version is recommended. Alone for the purpose of profile creation, the subsequent assignment of the IGEL OS Base System app to a device / device directory is NOT necessary.

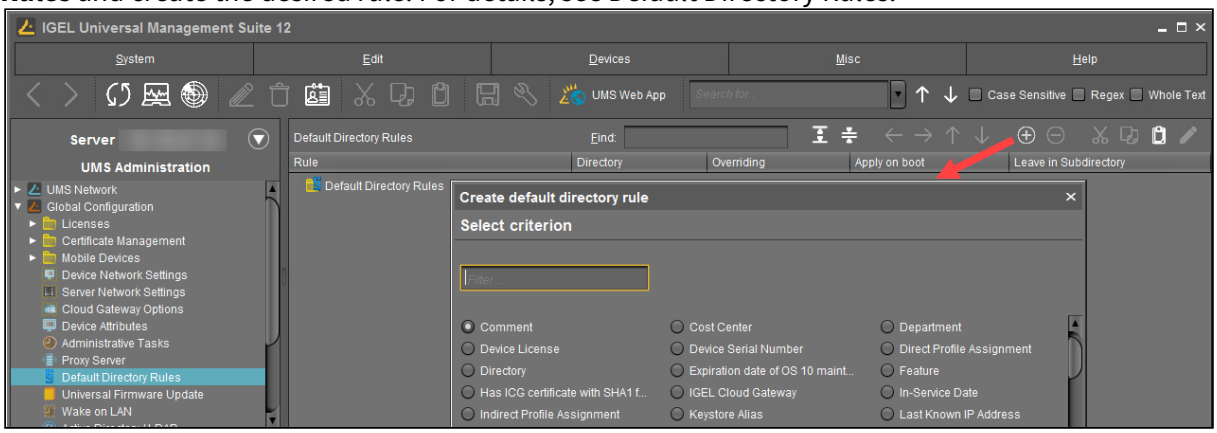
3. In the UMS Web App, go to **Apps** to view the imported app. To quickly configure the desired settings for this app, select the app and click **Create new profile**. Save the changes.



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: Click , type a directory name, and press [Enter]. For more information, see Creating a Directory Structure in the IGEL UMS Web App.



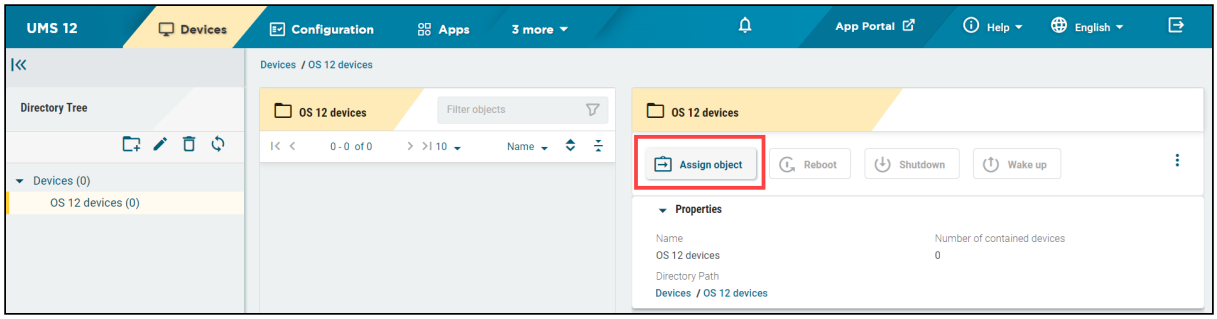
2) In the UMS Console, go to **UMS Administration > Global Configuration > Default Directory Rules** and create the desired rule. For details, see Default Directory Rules.

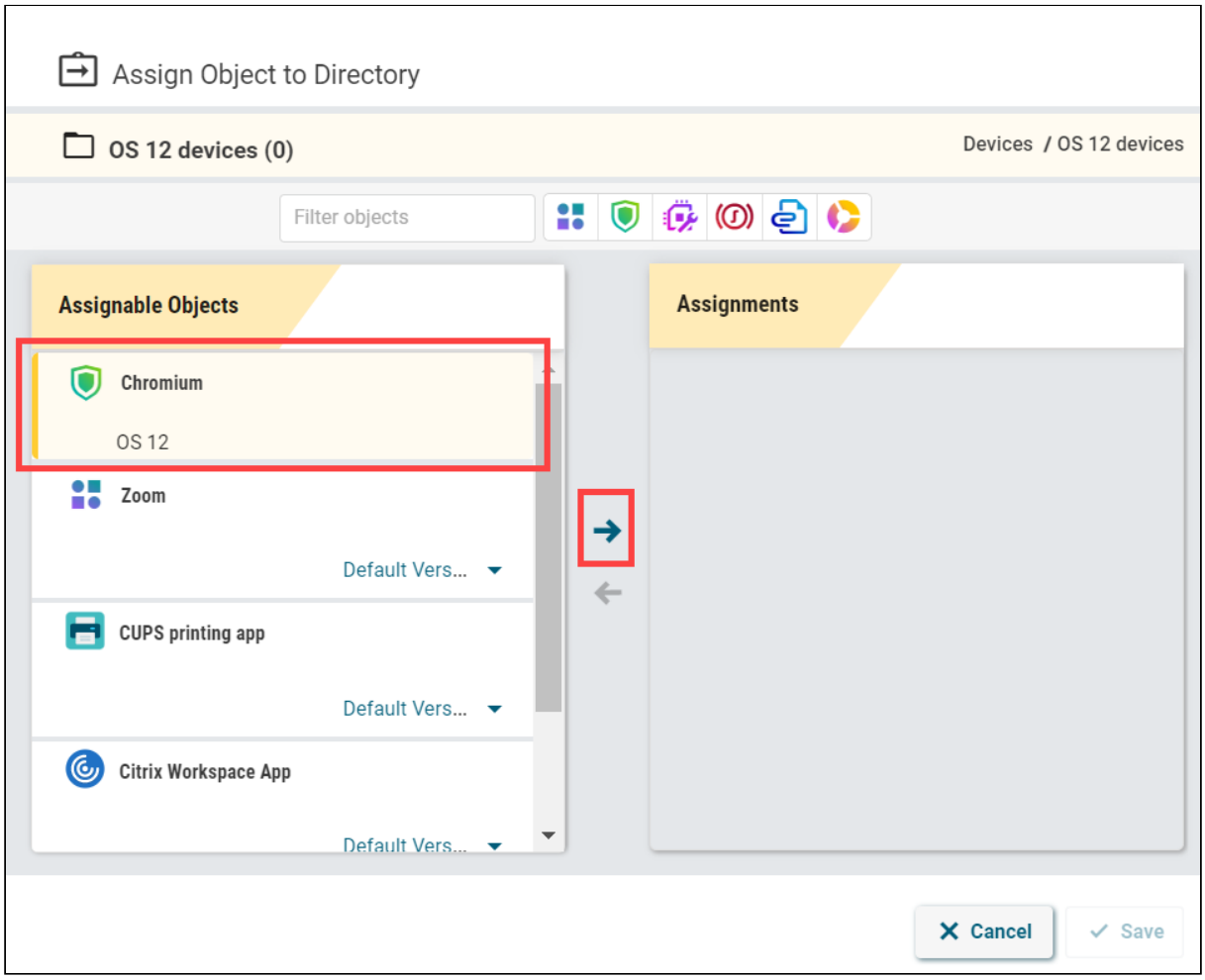


5. In the **UMS Web App > Devices**, assign the created profile to the device directory. Apply the changes.
   The app will be assigned to the devices via this profile (so-called "implicit app assignment") and will be installed on the devices. Exception: IGEL OS Base System app

   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.

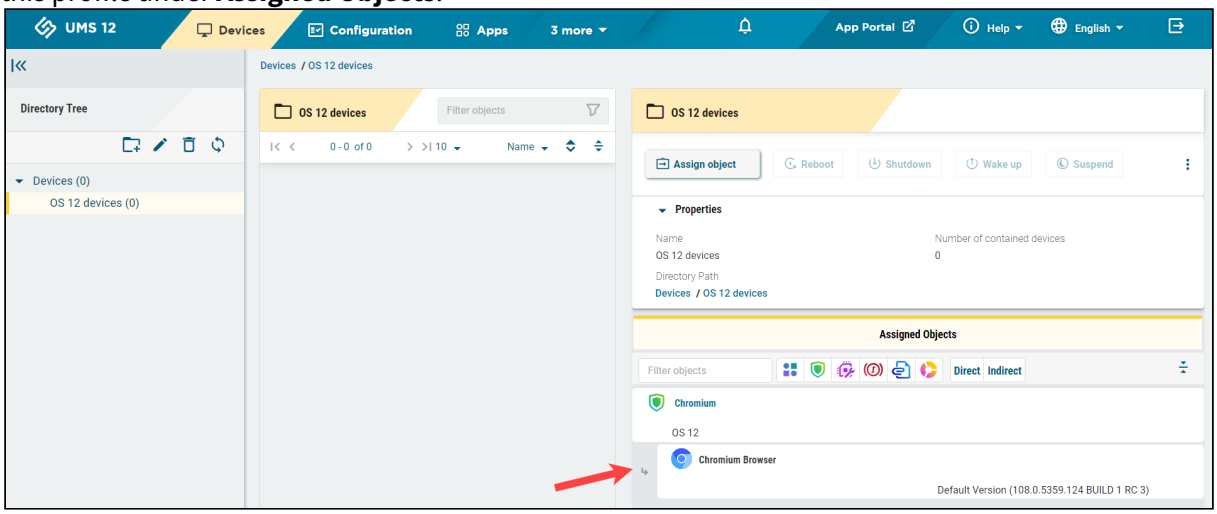
   > An implicit app assignment is overwritten if you assign an app explicitly, i.e. if you select an app as an object in the **Assign object** dialog.





All implicitly assigned apps, i.e. apps assigned to devices via a profile, are displayed directly under

this profile under **Assigned Objects**.

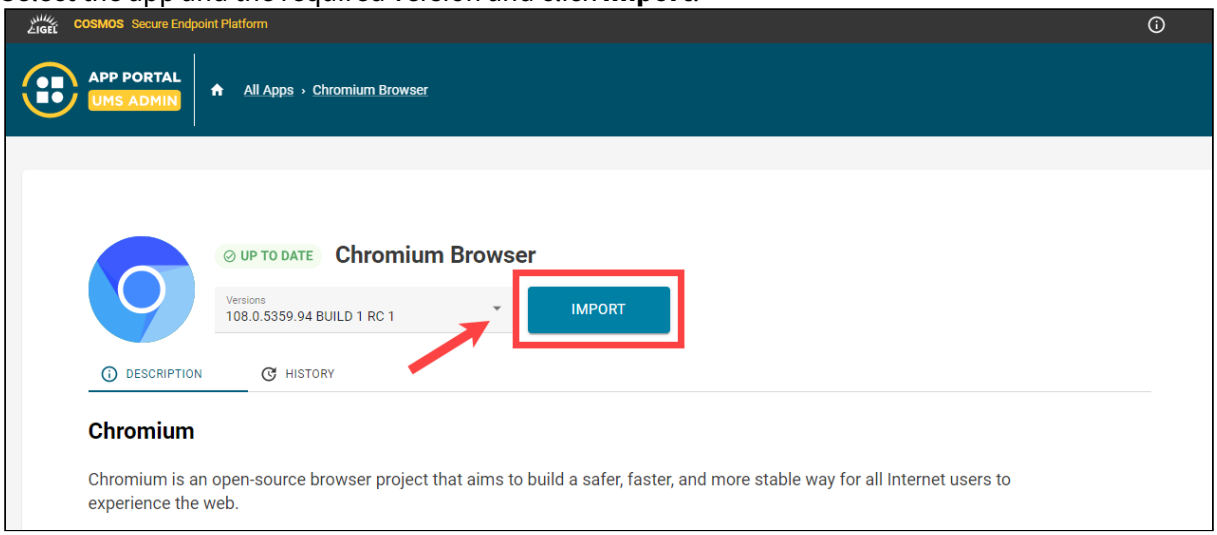


Importing IGEL OS Apps from the IGEL App Portal

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**.

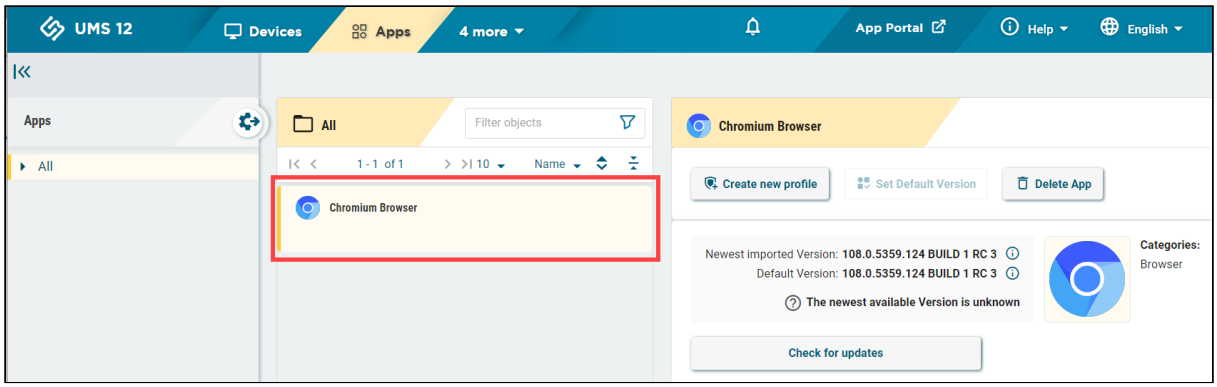
2. Select the app and the required version and click **Import**.



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**.

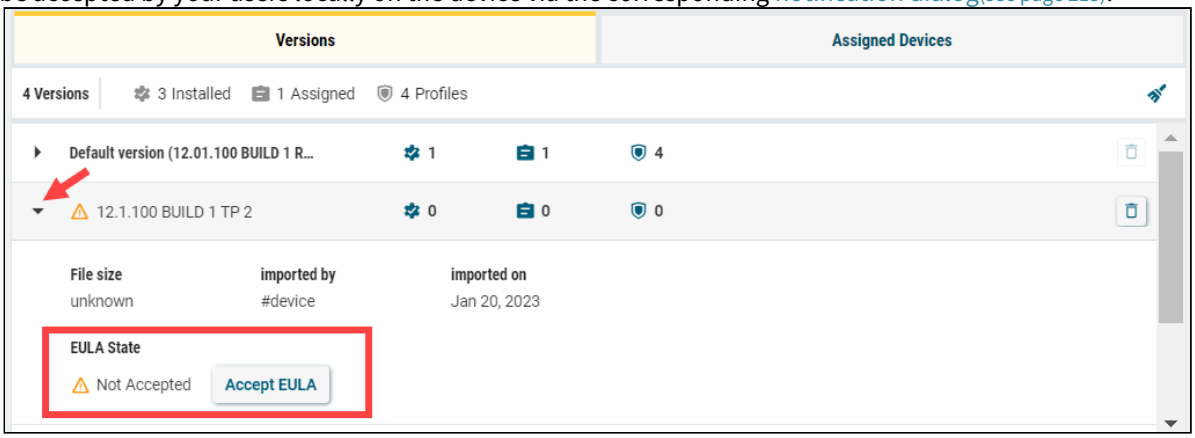


The results of the app import are also displayed under **Messages** . For more information on **Messages**, see Basic Overview of the IGEL UMS Web App.

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 188)) 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 213).



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 117).
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 118).

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.)

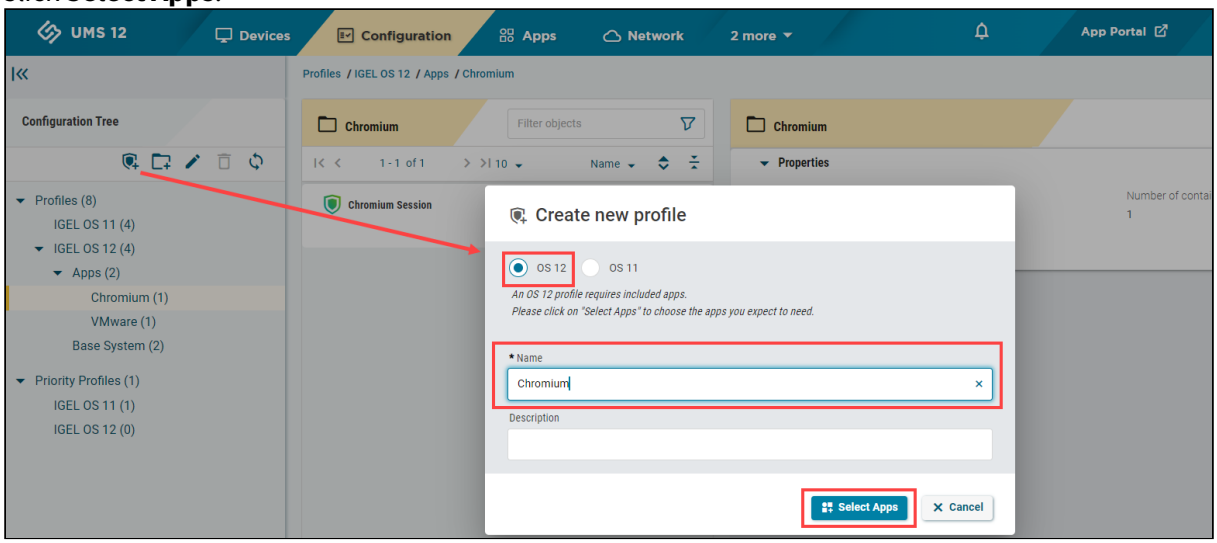
Profiles cannot currently be deleted in the UMS Web App.

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

Option 1: Via Configuration

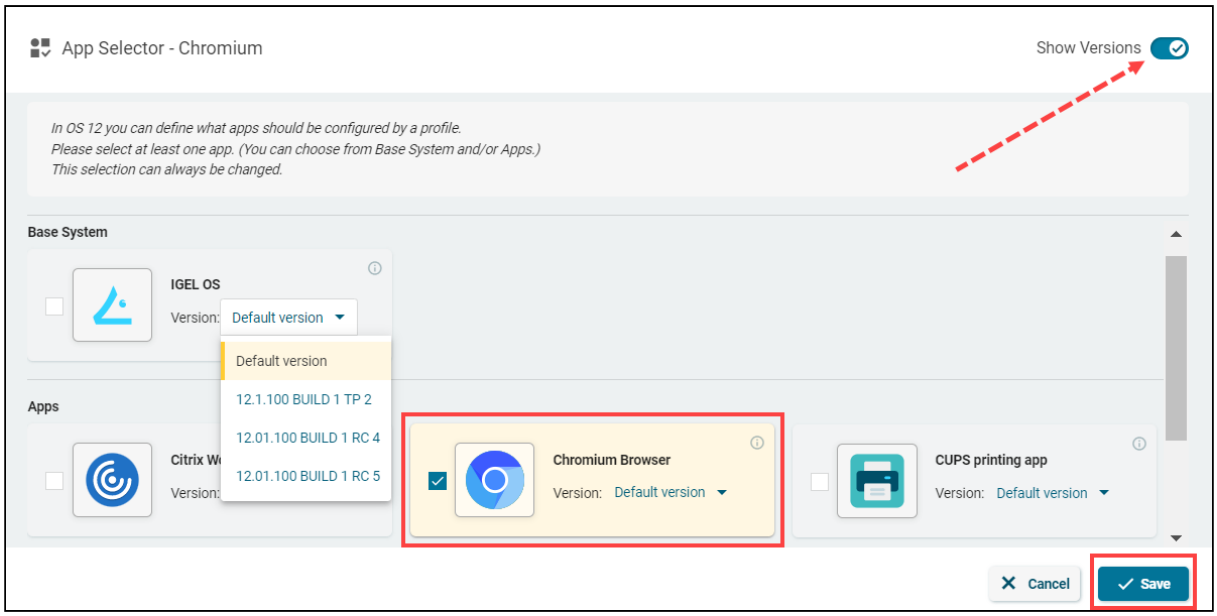
1. Under **UMS Web App > Configuration**, click **Create new profile** button.
2. Select **OS 12** (shown only if there are OS 11 devices registered in the UMS) and enter the **name** of the profile. If desired, add the **description** for the profile.

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 193), 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.

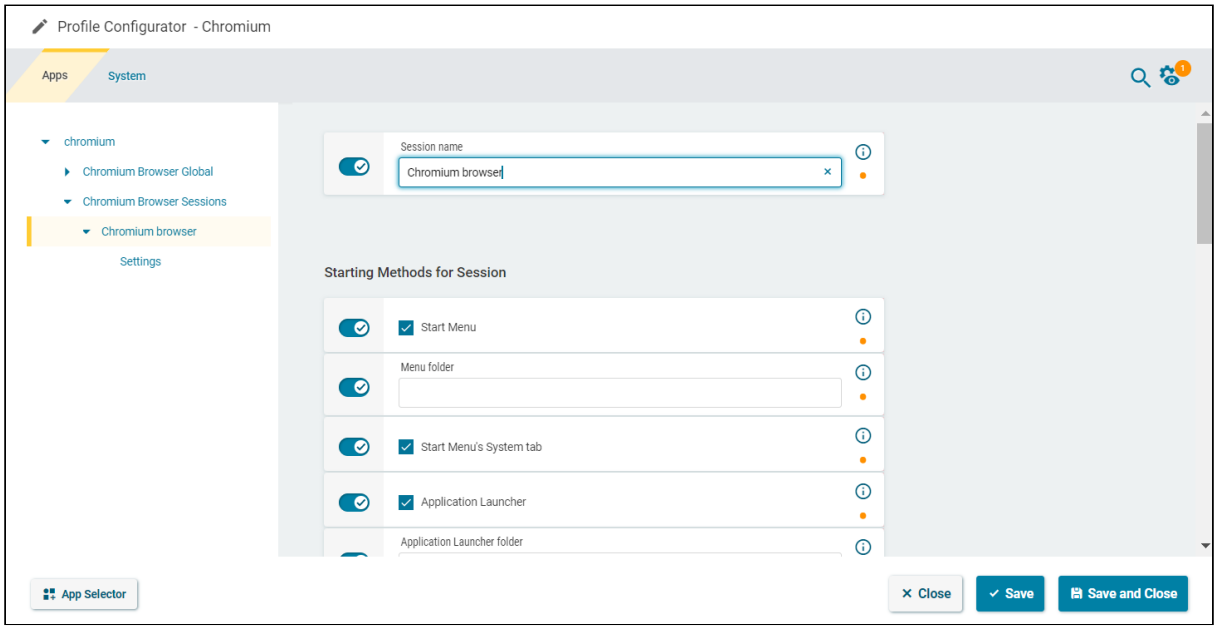


5. If you want to configure a profile for a specific app version, activate **Show Versions** and select the required version.

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.



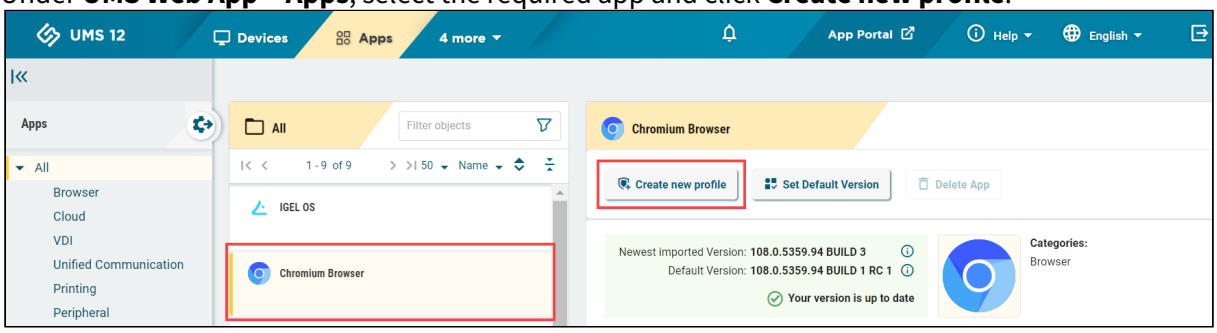
8. Save the changes.

9. Assign the profile to the required device / device directory. See Assignment of Apps and Profiles(see page 118).

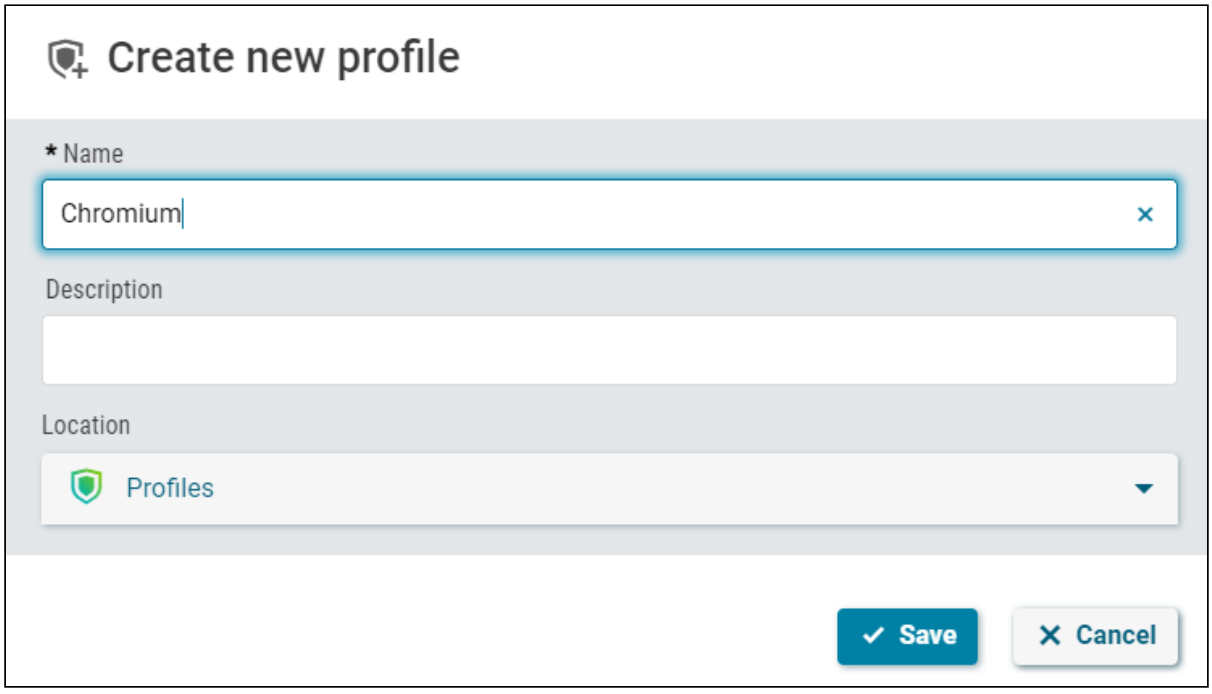
Option 2: Via Apps

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**.



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.

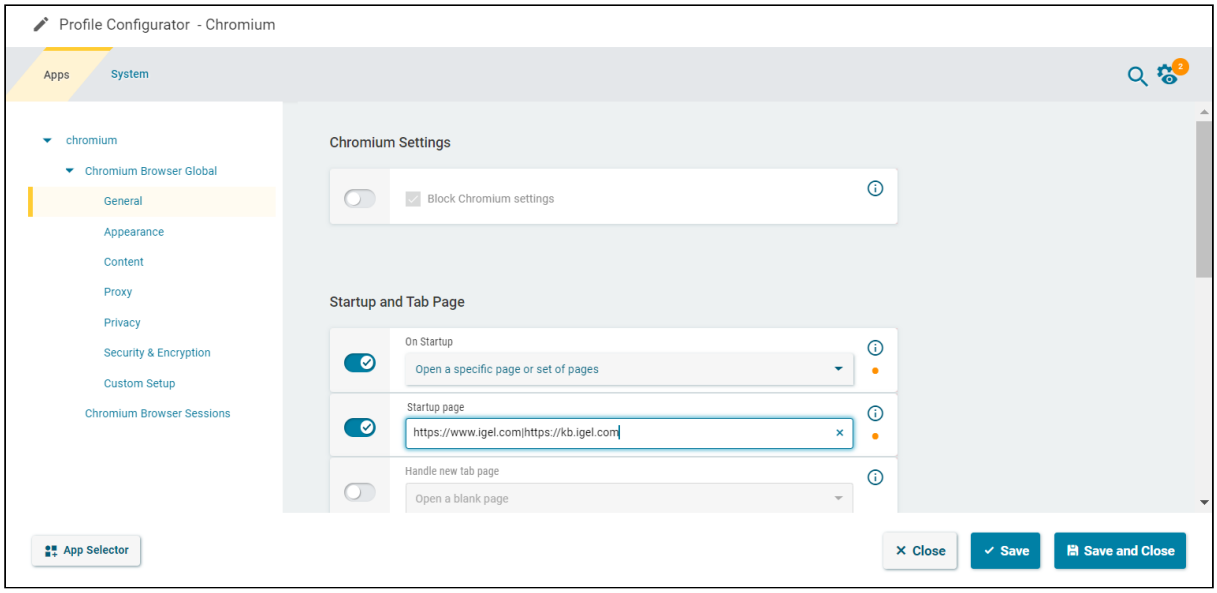


3. Click **Save**.
   The profile will be saved and listed under **Configuration > Profiles**, even if you will not configure any settings in the next step.

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.



5. Save the changes.
6. Assign the profile to the required device / device directory. See Assignment of Apps and Profiles(see page 118).

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.

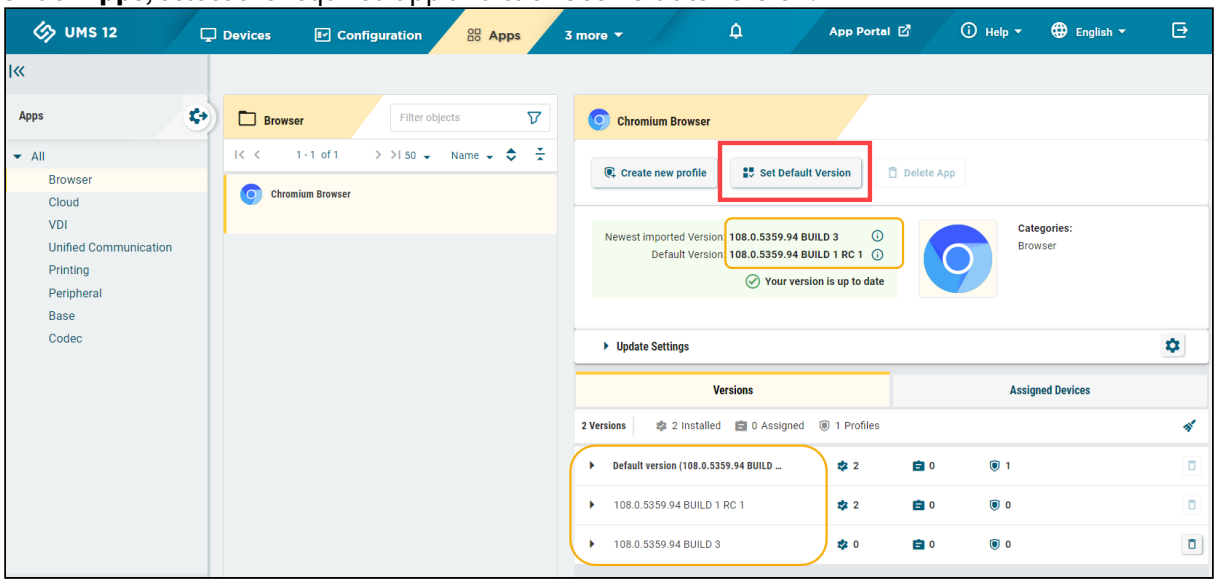
A **Default Version** is set globally: If changed, all assignments where no version was explicitly specified will change with it.

The best practice is to use the **Default Version** during the app assignment and profile creation.

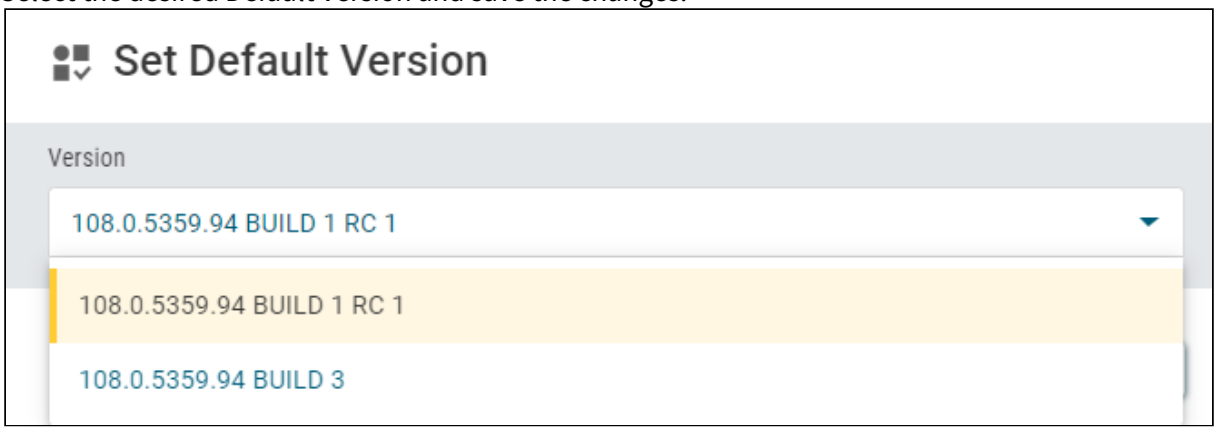
The use of a specific version during the app assignment and profile creation is recommended for test purposes, e.g. to test app updates. After successful testing, you can change your **Default Version**.

To set a Default Version:

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



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

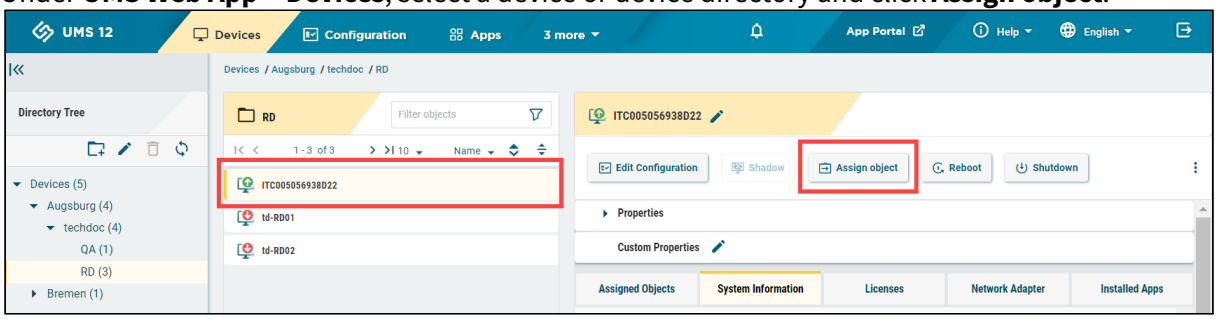
> An explicitly assigned app ALWAYS overwrites an implicitly assigned app.

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

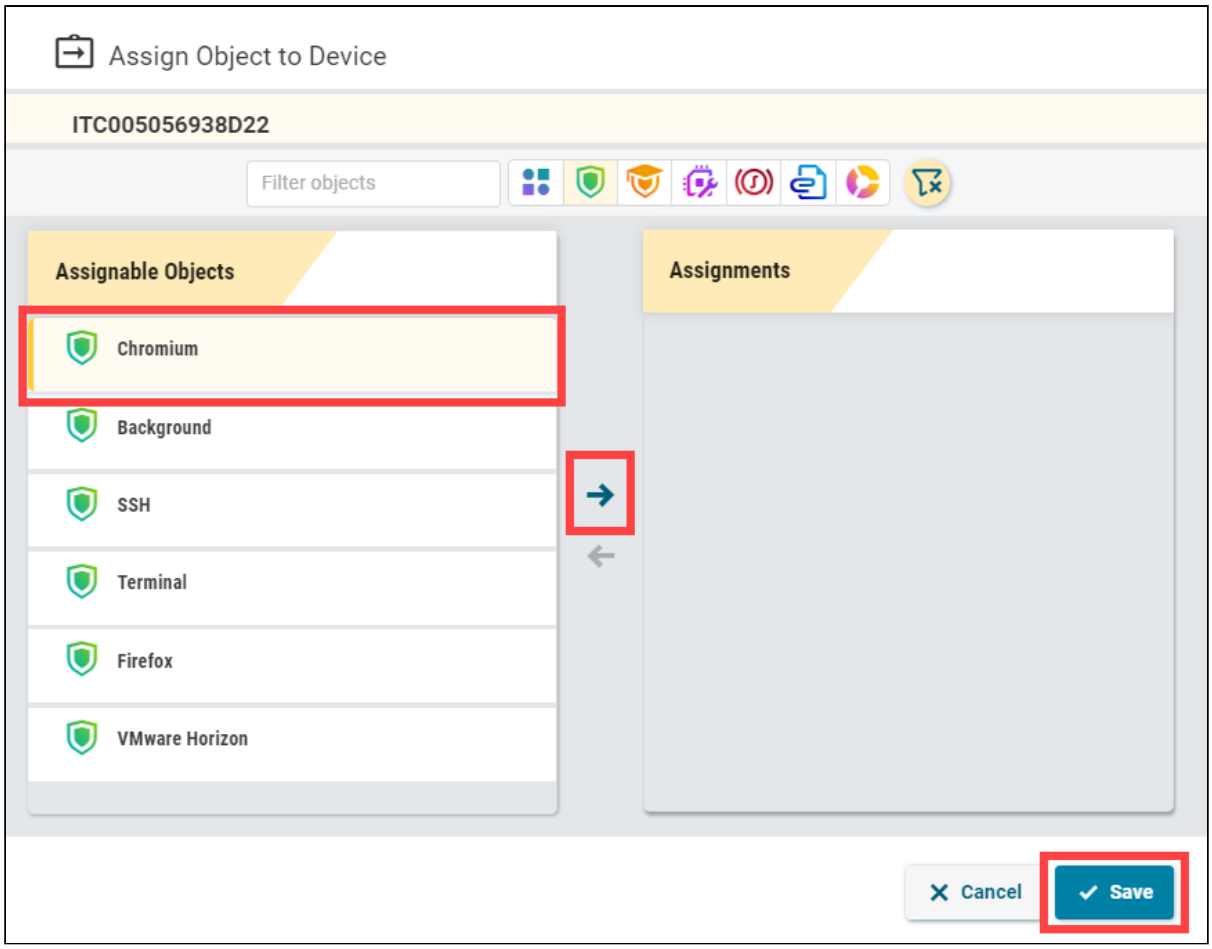
Implicit App Assignment via Profiles

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**.



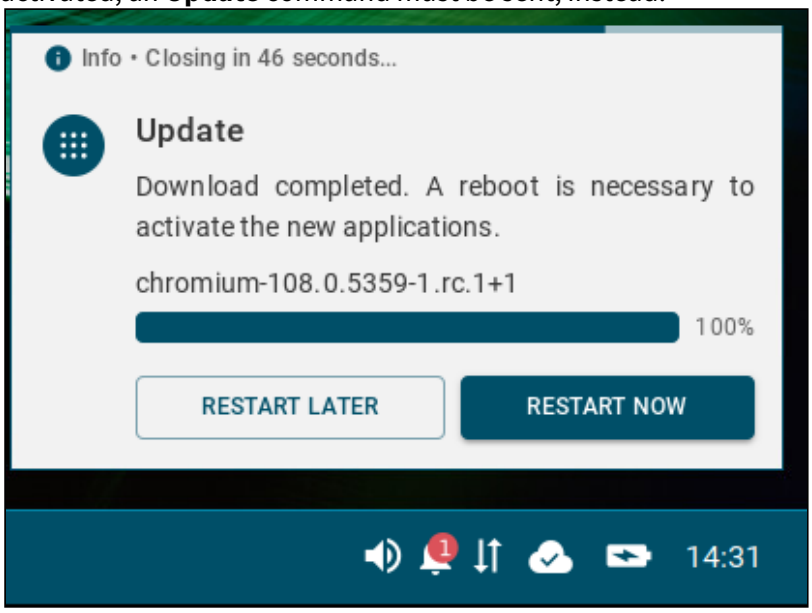
2. Select the profile you want to assign to the device / device directory and use the arrow button or drag & drop.



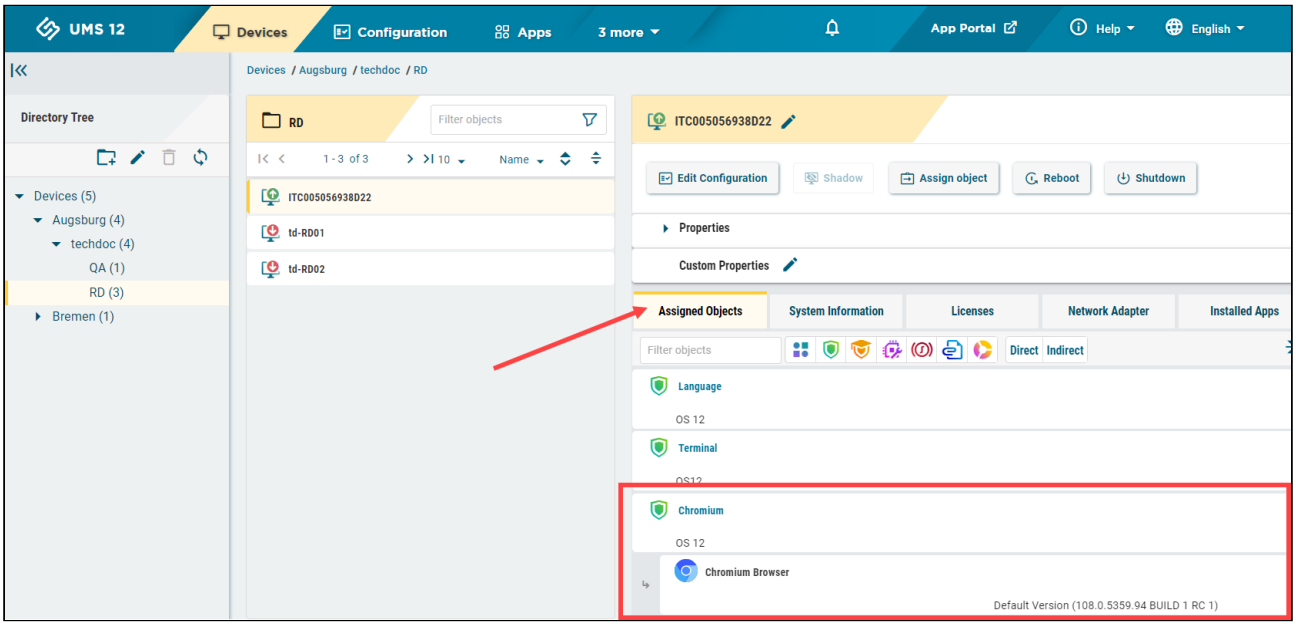
3. Save the changes.

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.



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

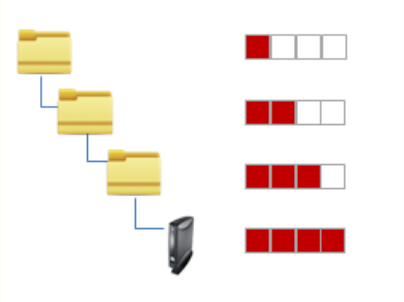


To check the installed apps, go to **Devices > [name of the device] > Installed Apps**; see Checking Installed Apps via the IGEL UMS Web App.

Explicit App Assignment

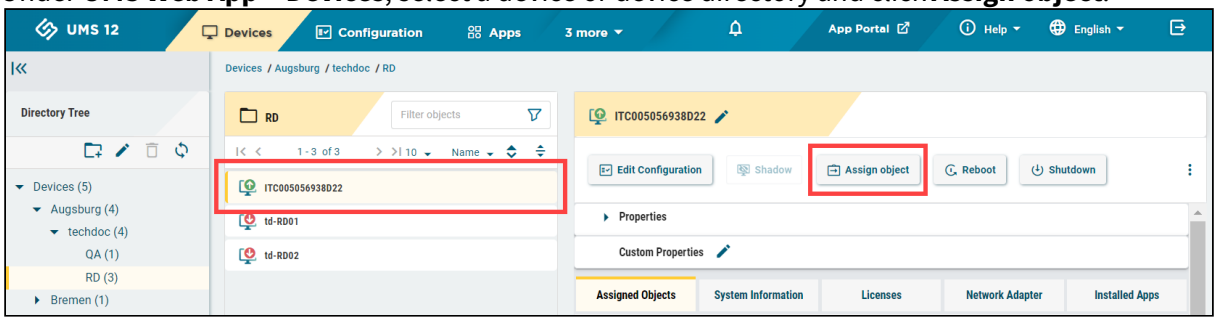
For the assignment of the IGEL OS Base System app, the permission **Assign Base System / Firmware Update** is required. You can set the permission in the UMS Console via **[context menu of a device / device directory] > Access control**.

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.



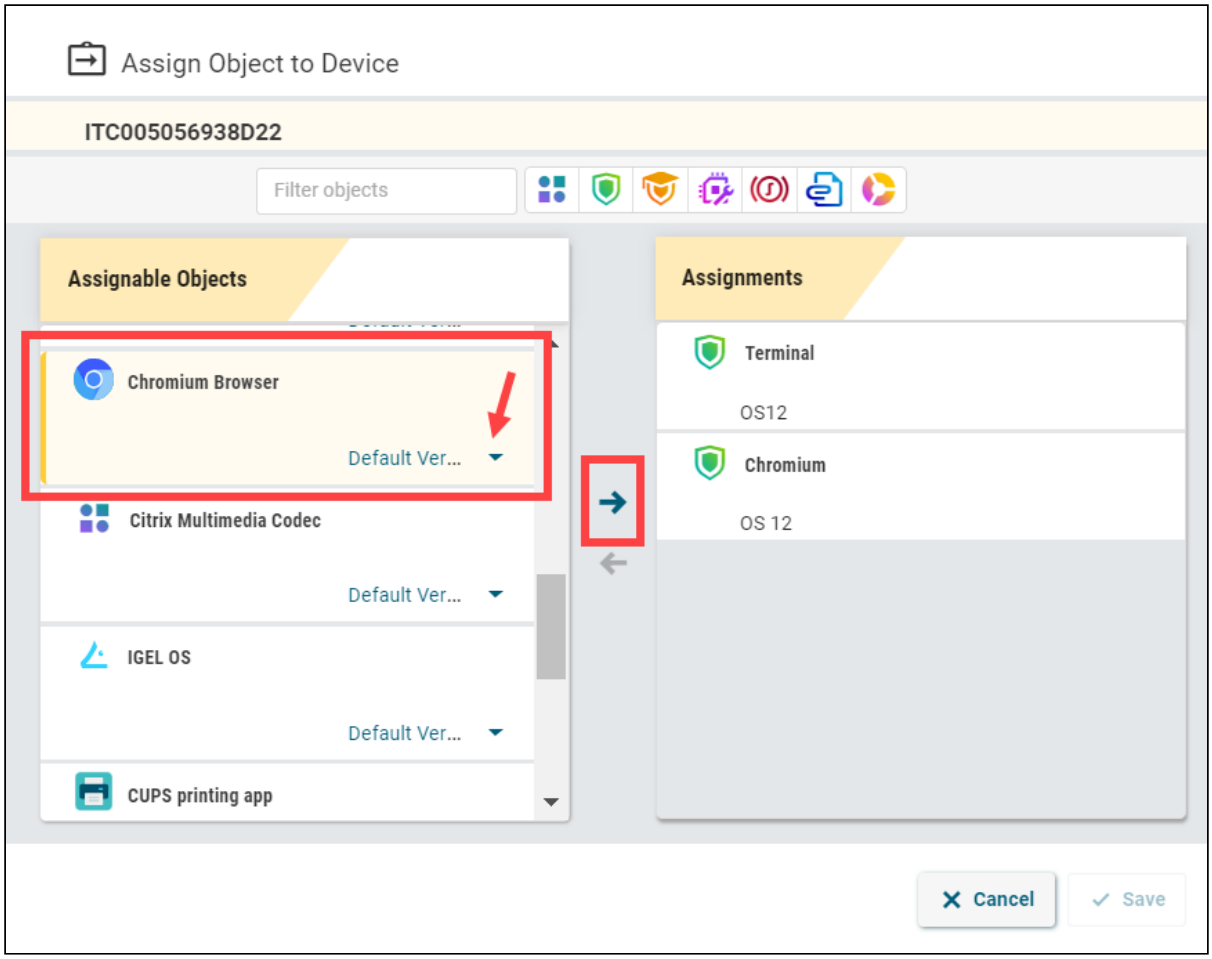
To assign apps to a device / device directory, proceed as follows:

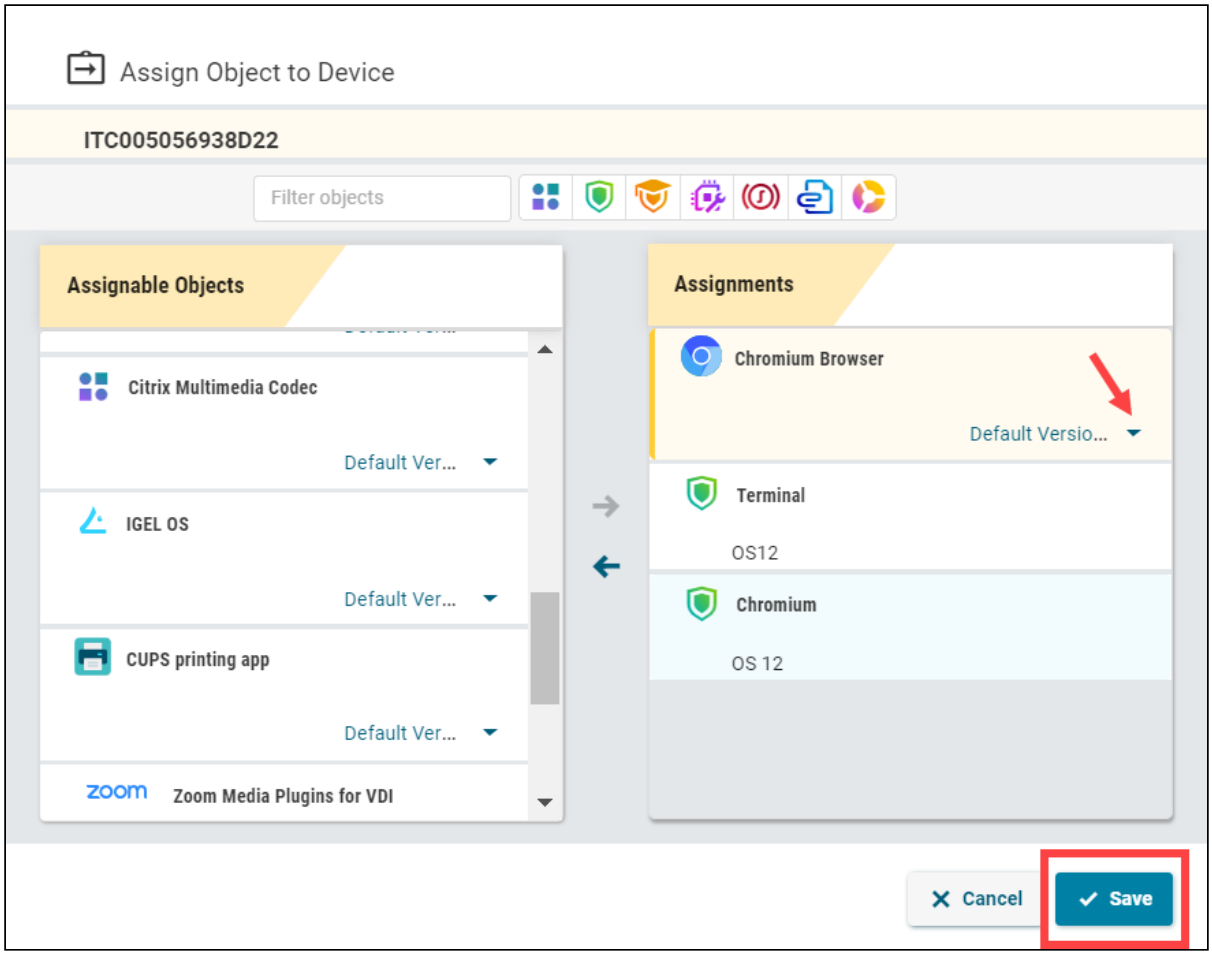
1. Under **UMS Web App > Devices**, select a device or device directory and click **Assign object**.



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 117) 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**.


Assign Object to Device
ITC005056938D22
Filter objects
Assignable Objects
Chromium Browser
Default Ver...
Citrix Multimedia Codec
Default Ver...
IGEL OS
Default Ver...
CUPS printing app
Assignments
Terminal
OS12
Chromium
OS 12
Cancel
Save

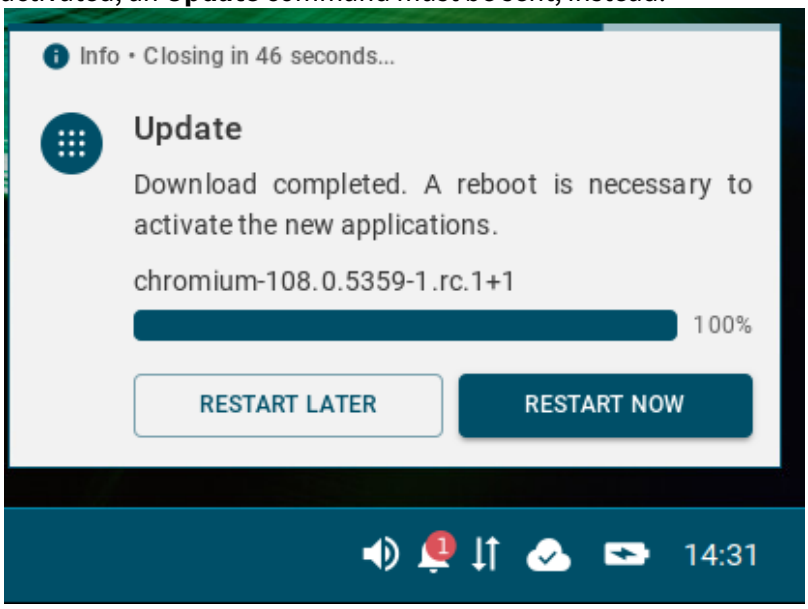


3. Save the changes.

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.



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 117) 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

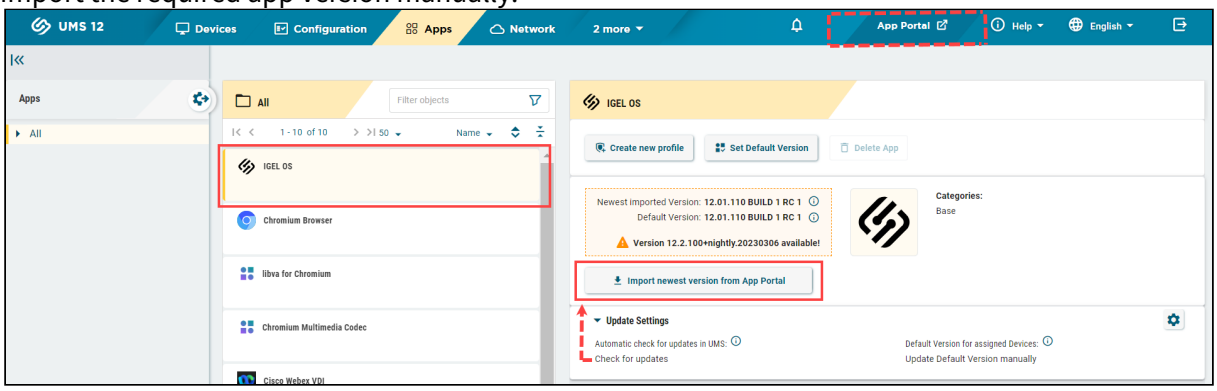
The procedure described below applies to the update of the IGEL OS Base System app.

ⓘ This procedure is also relevant for any explicitly assigned app(see page 118).

Preparing the Update

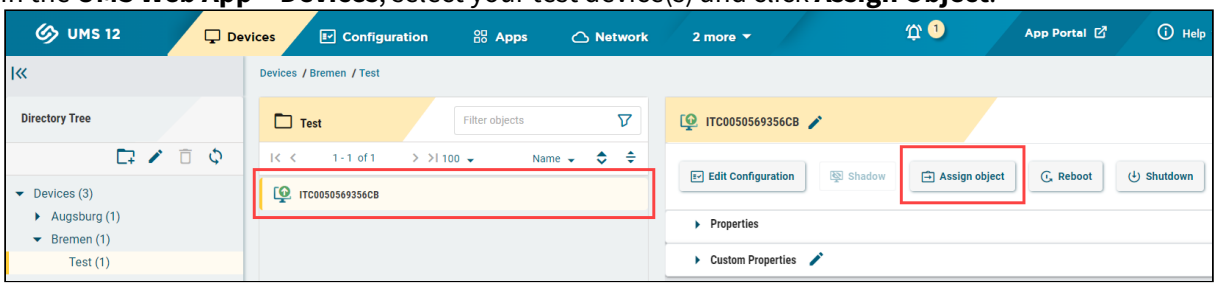
> For the assignment of the IGEL OS Base System app, the permission **Assign Base System / Firmware Update** is required. You can set the permission in the UMS Console via **[context menu of a device / device directory] > Access control**.

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

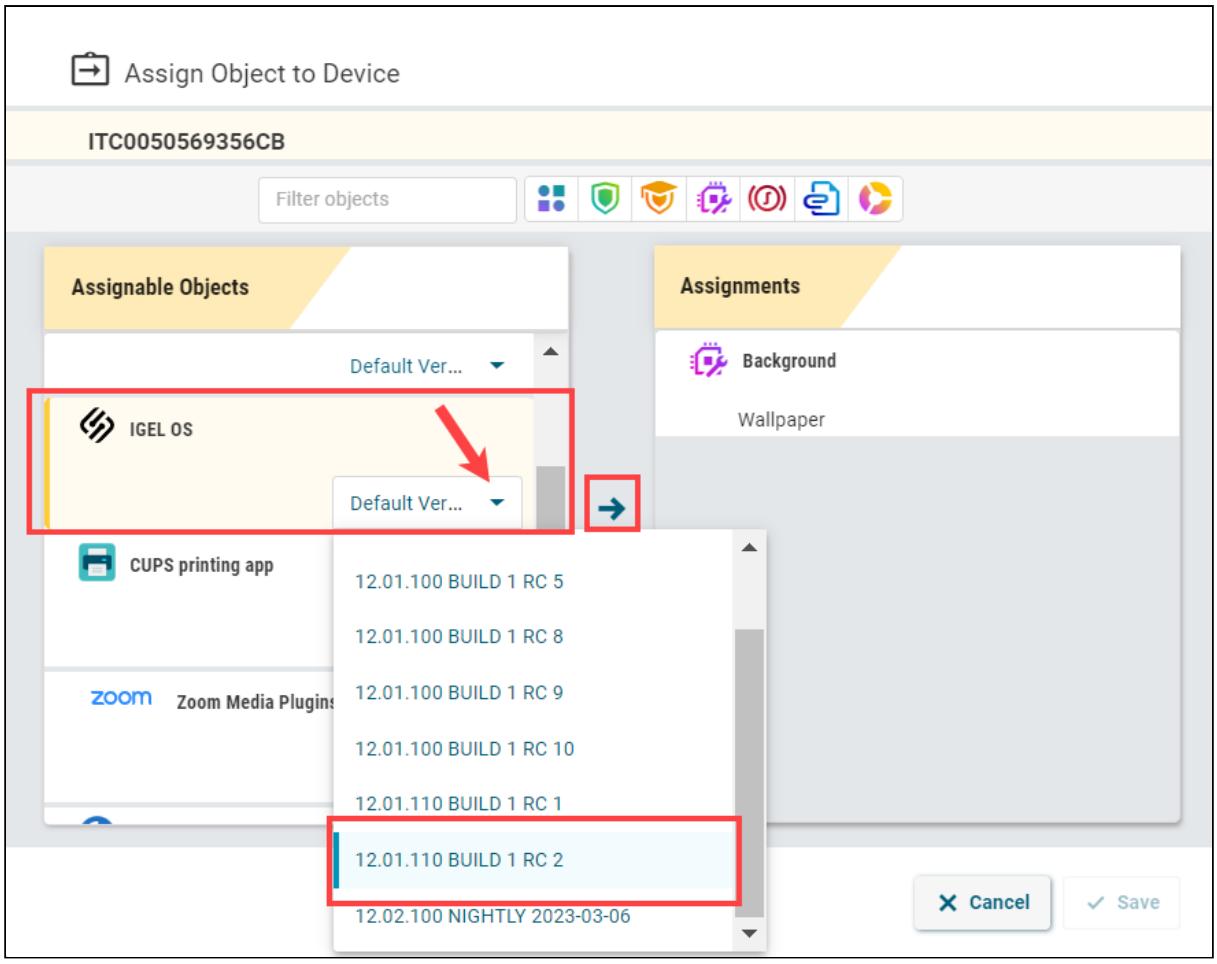


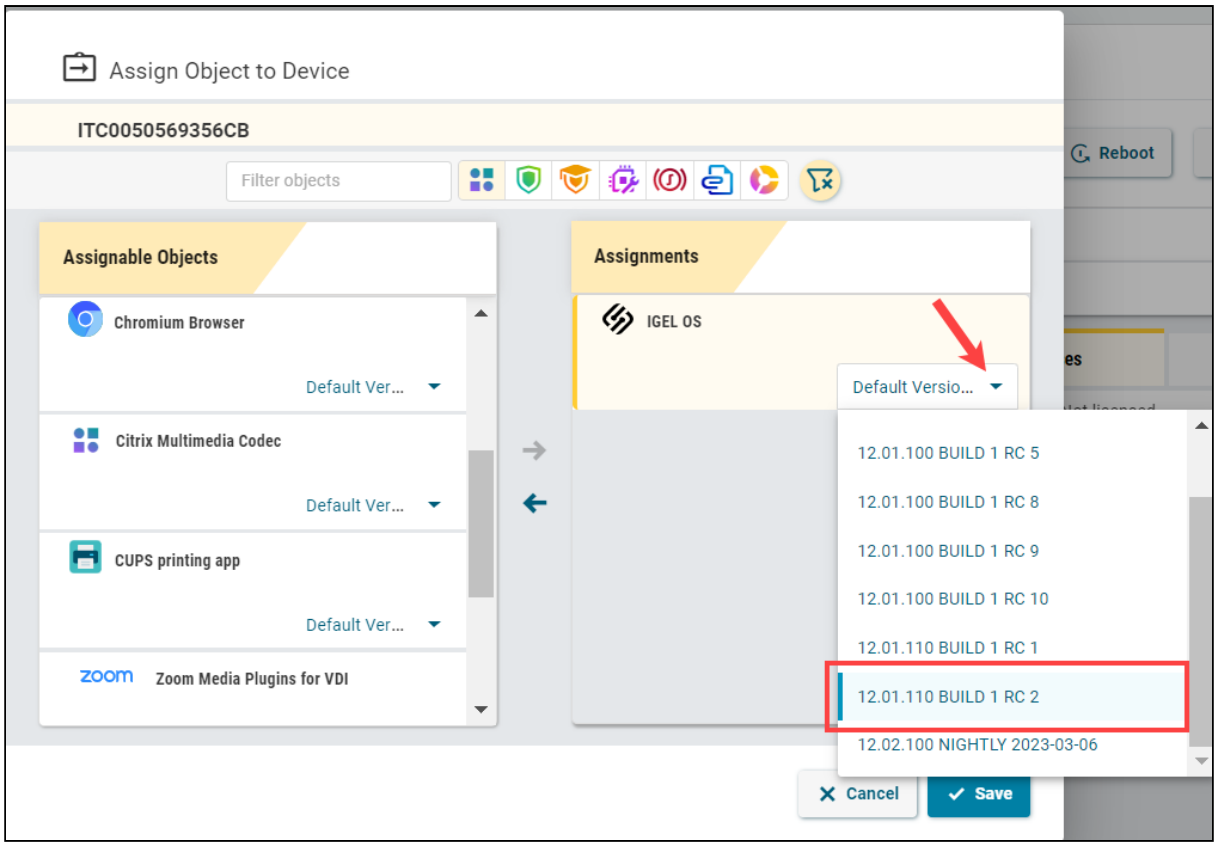
Testing the Update

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** and the required version. It is possible to select the version for an app either under **Assignable Objects** or under **Assignments**.


Assign Object to Device
ITC0050569356CB
Filter objects
Assignable Objects
Assignments
Default Ver...
IGEL OS
Default Ver...
Background
Wallpaper
CUPS printing app
zoom
Zoom Media Plugins
12.01.100 BUILD 1 RC 5
12.01.100 BUILD 1 RC 8
12.01.100 BUILD 1 RC 9
12.01.100 BUILD 1 RC 10
12.01.110 BUILD 1 RC 1
12.01.110 BUILD 1 RC 2
12.02.100 NIGHTLY 2023-03-06
Cancel
Save



3. Save the changes.

4. Decide when the changes should become effective.
   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.

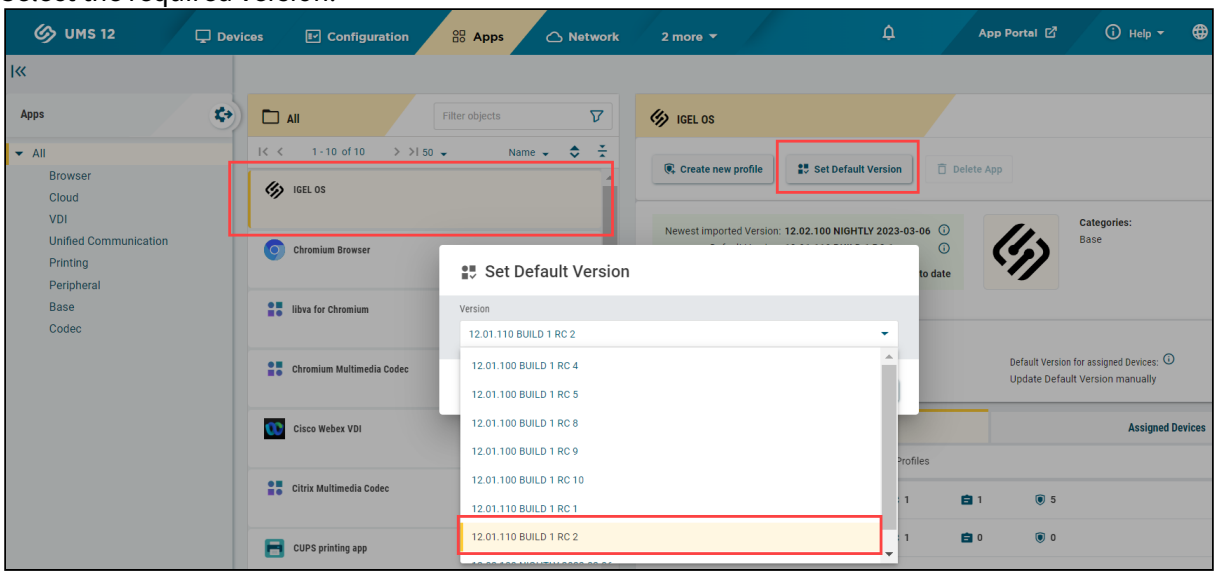
5. Under **Devices > [name of the device] > Installed Apps**, check the app, its version and state; see Checking Installed Apps via the IGEL UMS Web App.

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

Triggering the Mass Update

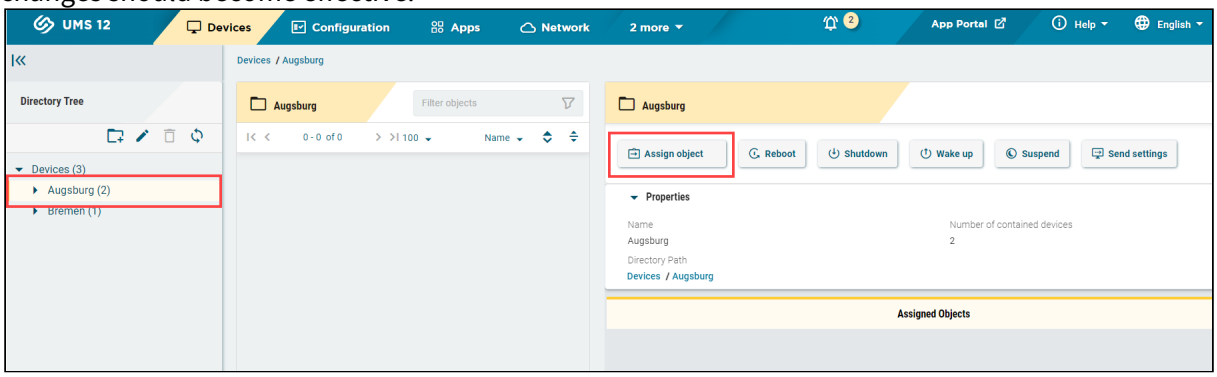
1. In the **UMS Web App > Apps**, select **IGEL OS** and click **Set Default Version**.

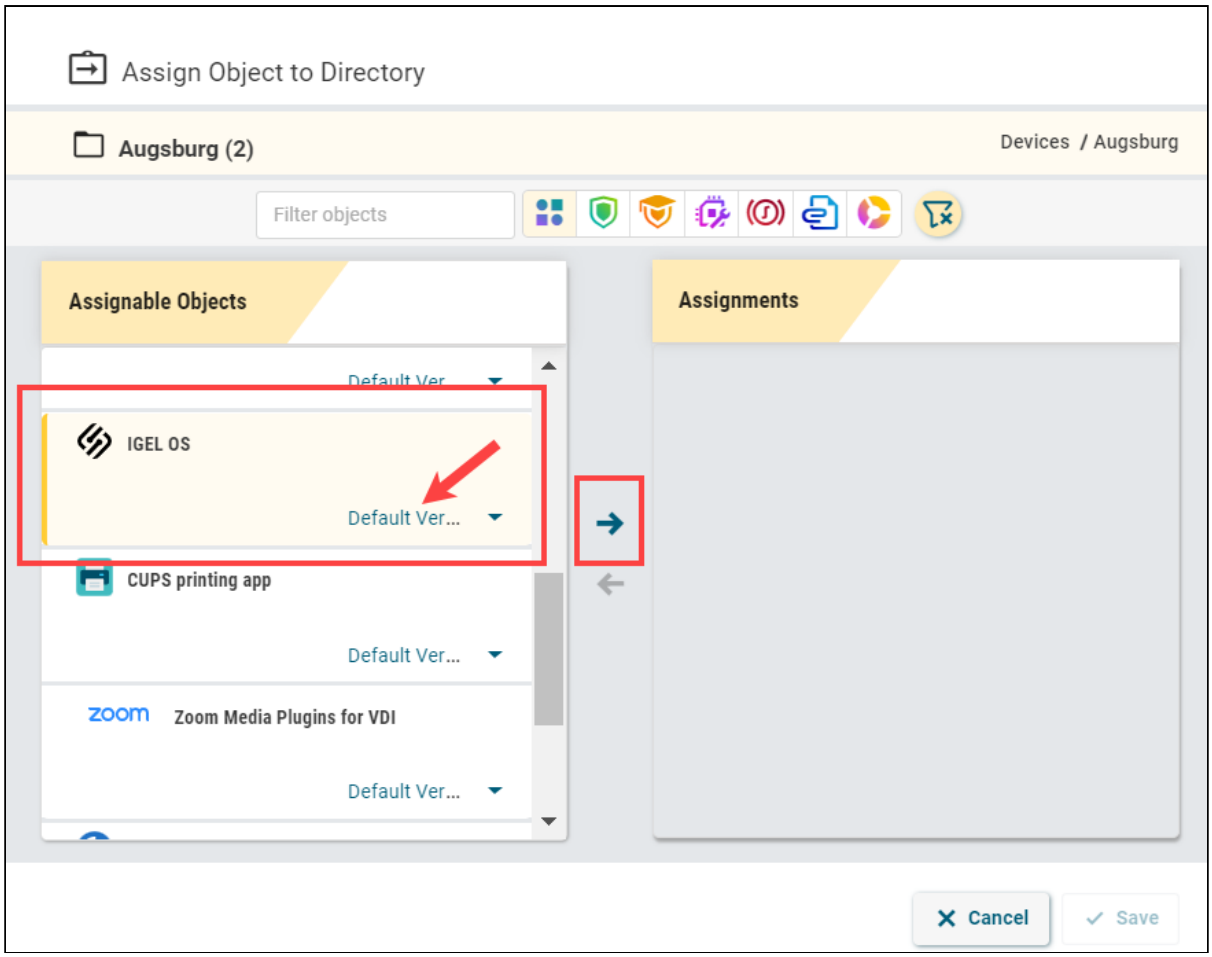
2. Select the required version.



3. Click **Save** and select when the changes should take effect.

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. Verify that **Default Version** is selected in the version picker. Click **Save** and decide when the changes should become effective.





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 213).
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.

5. 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

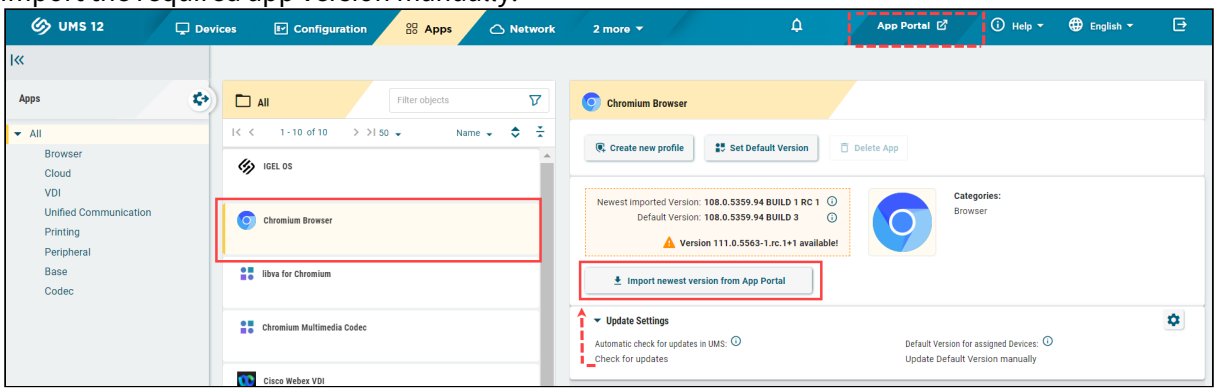
If you have decided not to use the explicit app assignment, and the apps are thus assigned to your devices implicitly, i.e. via profiles configuring these apps, you can use the following procedure for the app update. This procedure applies to the update of any app that has been assigned to devices implicitly; 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 118).

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.



Testing the Update

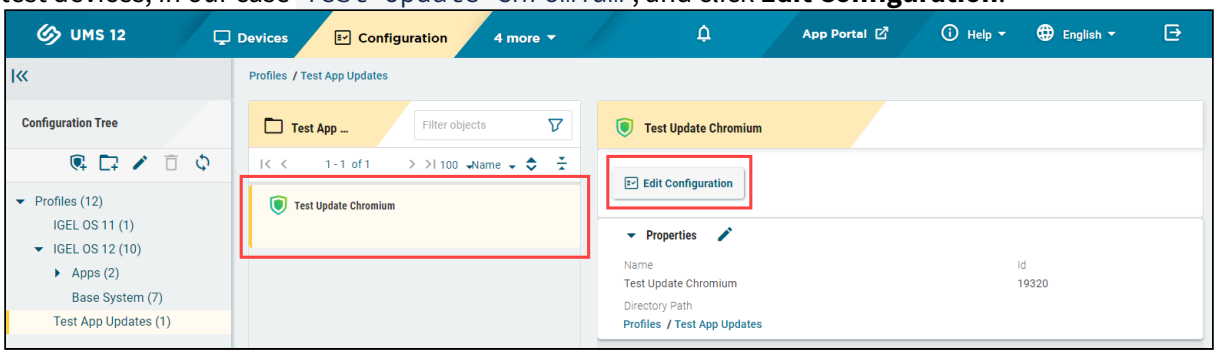
1. Go to **UMS Web App > Configuration** and create a test profile with the same settings and app(s) as the "productive" profile, e.g. `Test Update Chromium`. Leave the **Default Version** for the app(s) in the **App Selector** (as it was done for the productive devices). For how to create profiles, see Creating an OS 12 Profile(see page 113).

> 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

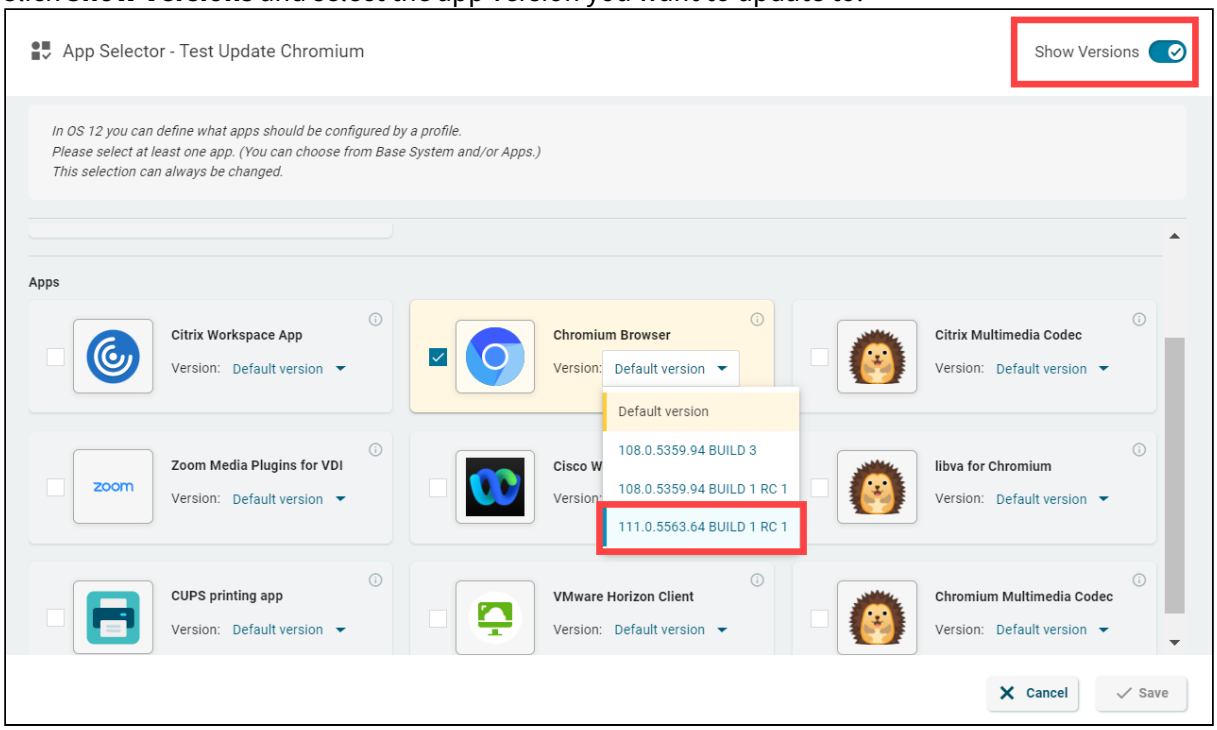
Profiles(see page 118).
As soon as your test devices have the app(s) of the same version as on the productive devices, proceed as follows.

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**.



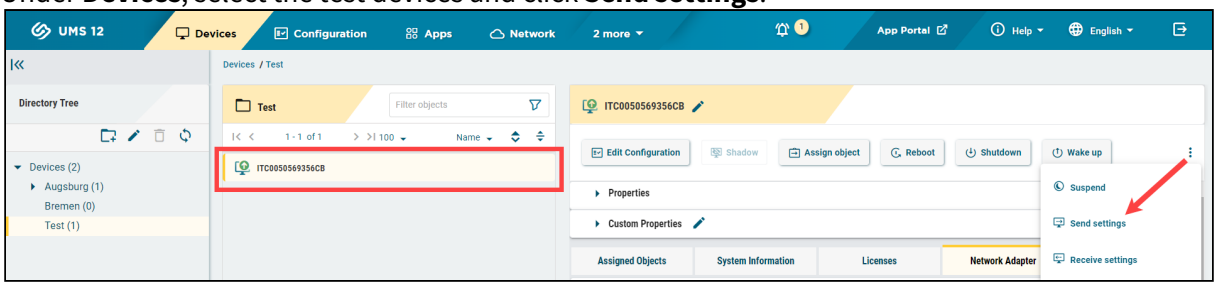
4. In the **Profile Configurator** dialog, click **App Selector**.

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



6. Save the changes.

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



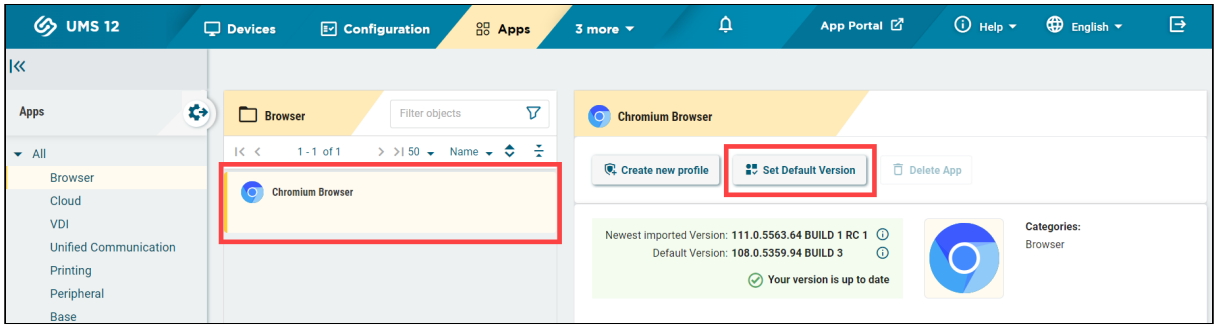
The new app version will be downloaded by the device.
By default, apps / app versions assigned to the device will be automatically activated at the next reboot. If you have configured the background app update, an **Update** command must be sent, instead; see How to Configure the Background App Update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

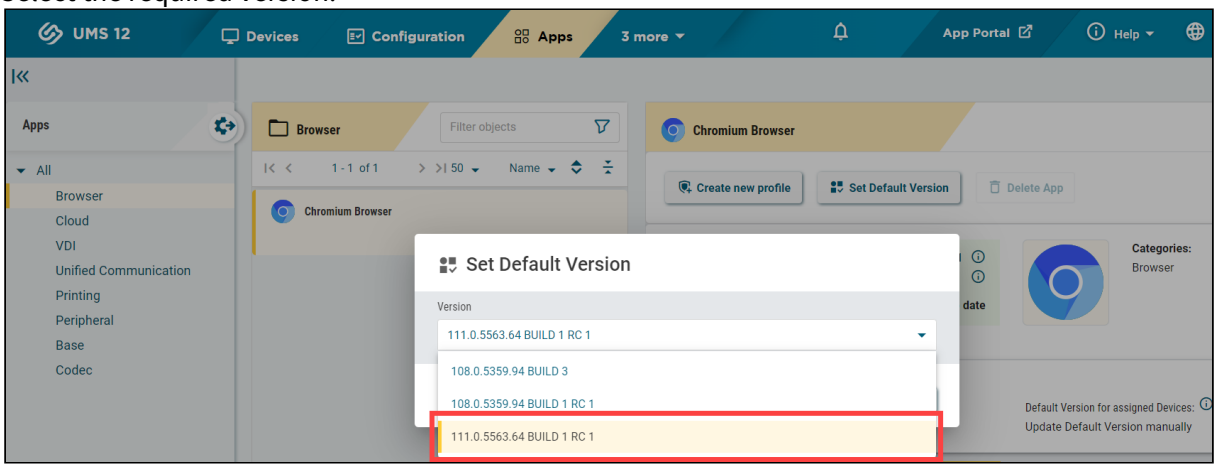
When the update test has been successful, you can update the app on all the required devices.

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.



3. Click **Save** and select when the changes should take effect.

> 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 213).
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

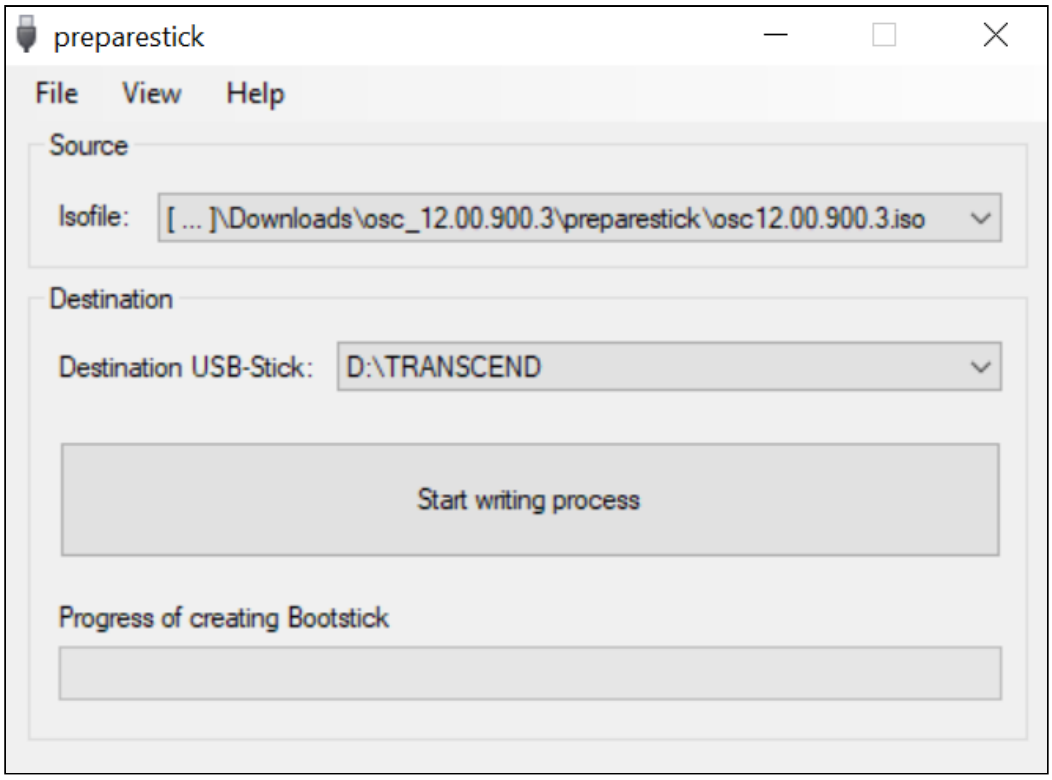
1. Download the ZIP archive for OS Creator from the IGEL Download Server[19]:
   - For new devices, use the standard installer (e.g. `osc_12.01.110.zip`).
   - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e.g. `osc_12.01.110_legacy.zip`).

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/



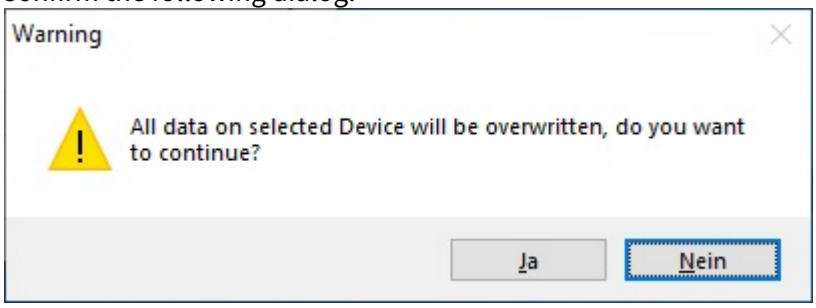
The dropdown menu **Isofile** shows the ISO files contained in the unzipped directory.

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

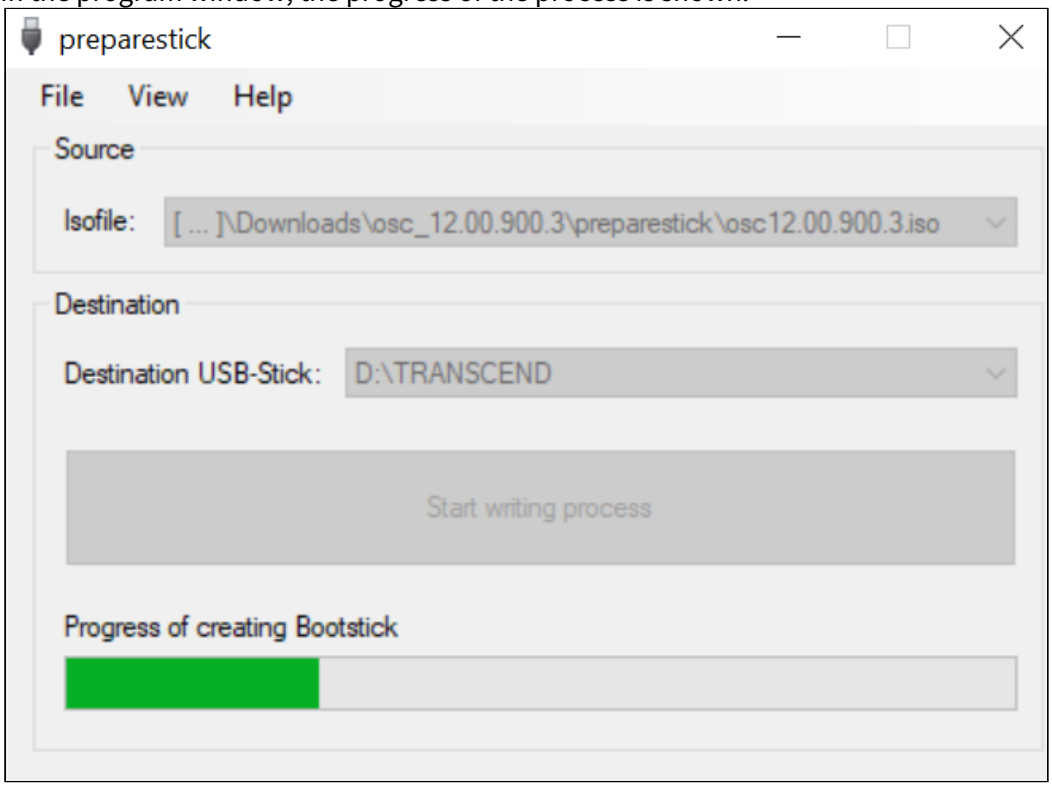
6. Under **Destination USB stick**, select the USB storage medium on which you would like to save the installation data.
   It is recommended that you only have one USB storage medium connected during this procedure.
   If you accidentally select the wrong medium, all data on it will be lost.
   Generally 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**.

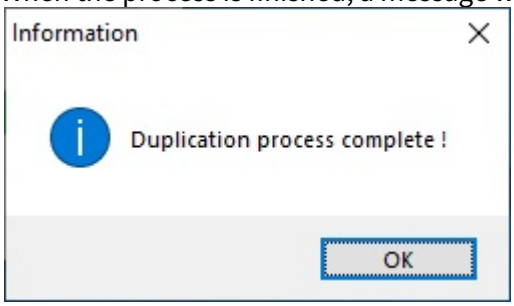
8. Confirm the following dialog:



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



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



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.

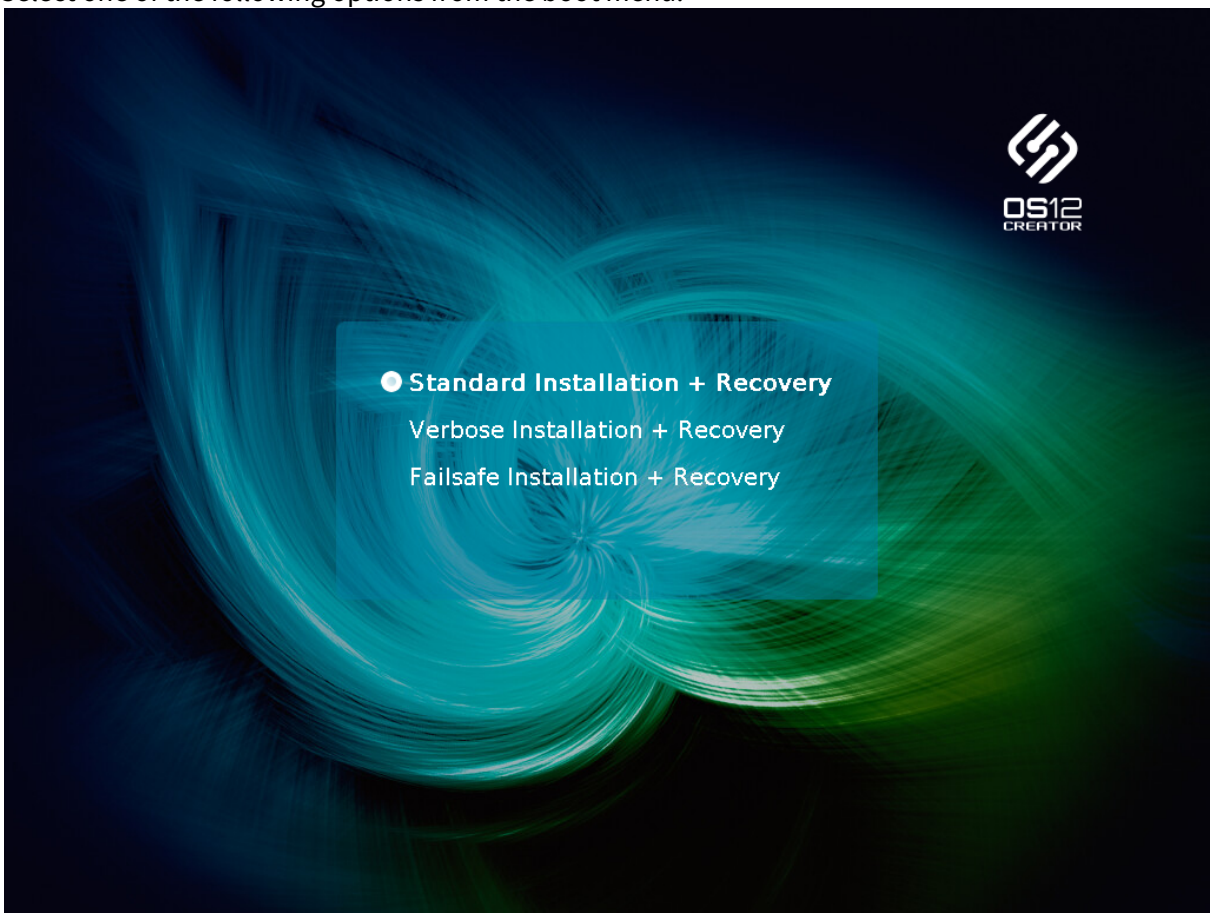
   The USB memory stick for OSC installation is ready for use.

Installation Procedure

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

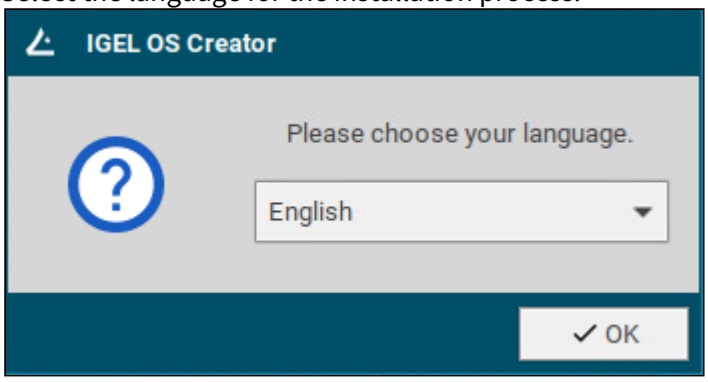
1. Connect the prepared USB memory stick to the target device and switch the target device on.
   General information on how you can boot from the stick can be found under Boot Settings.

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

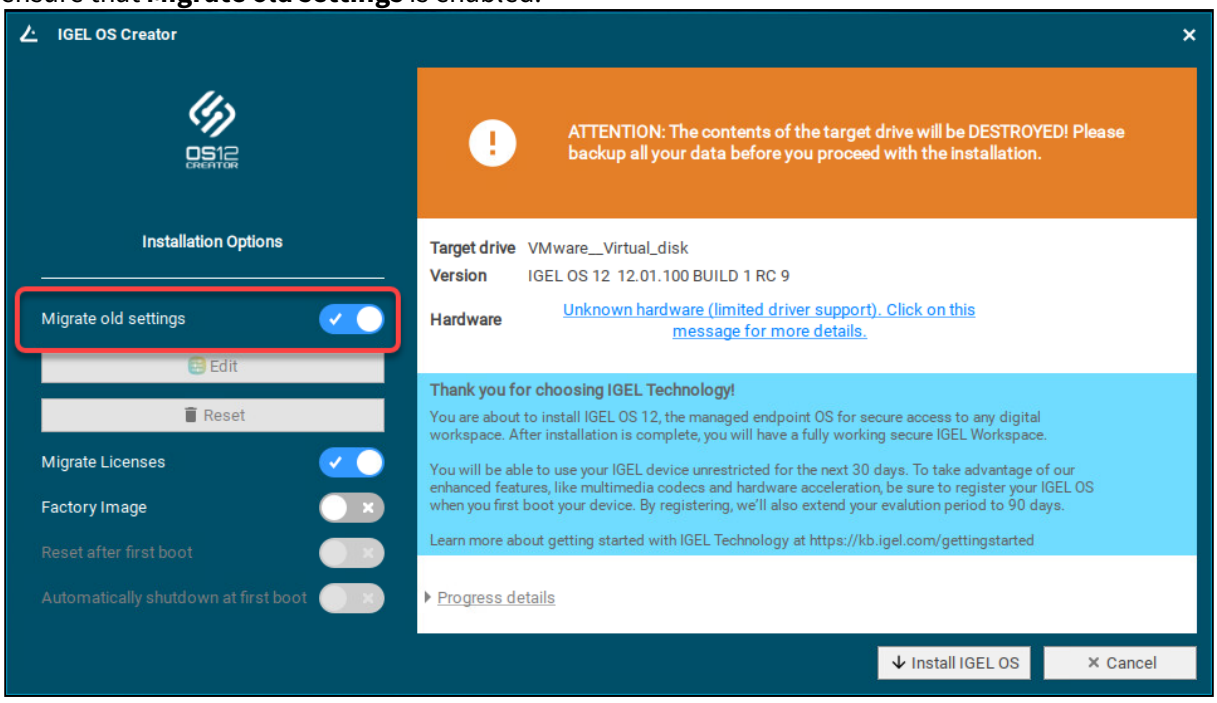


   - **Standard Installation + Recovery**: Boots the system with just a few messages from the USB memory stick and launches the installation program. (Default)
   - **Verbose Installation + Recovery**: Boots the system from the USB memory stick and shows the Linux boot messages in the process.
   - **Failsafe 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.

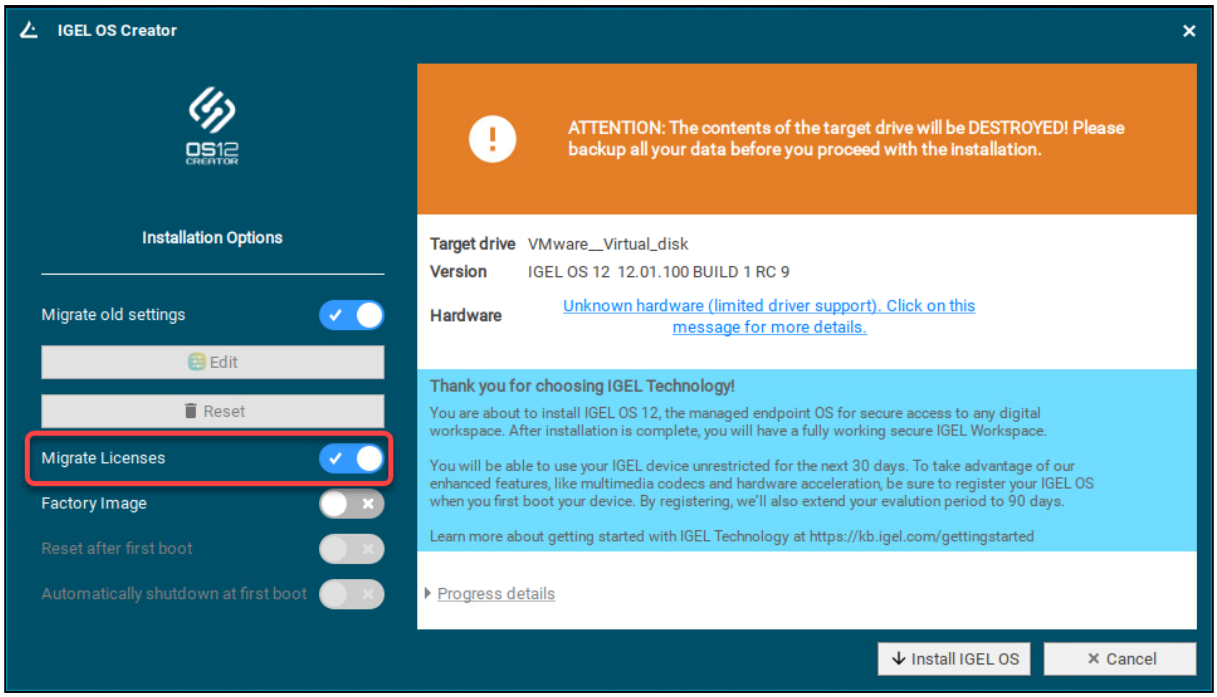
3. Select the language for the installation process.



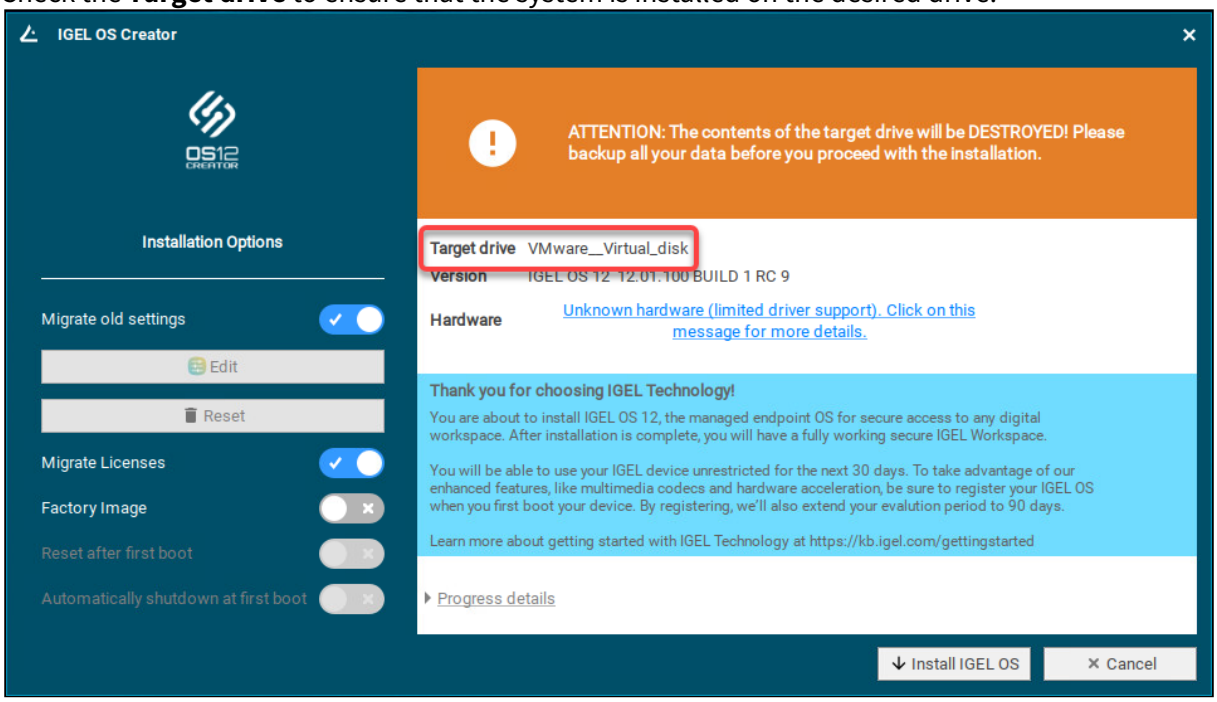
4. If IGEL OS 12 has been running on the device before and you want to preserve the device's settings, ensure that **Migrate old settings** is enabled.



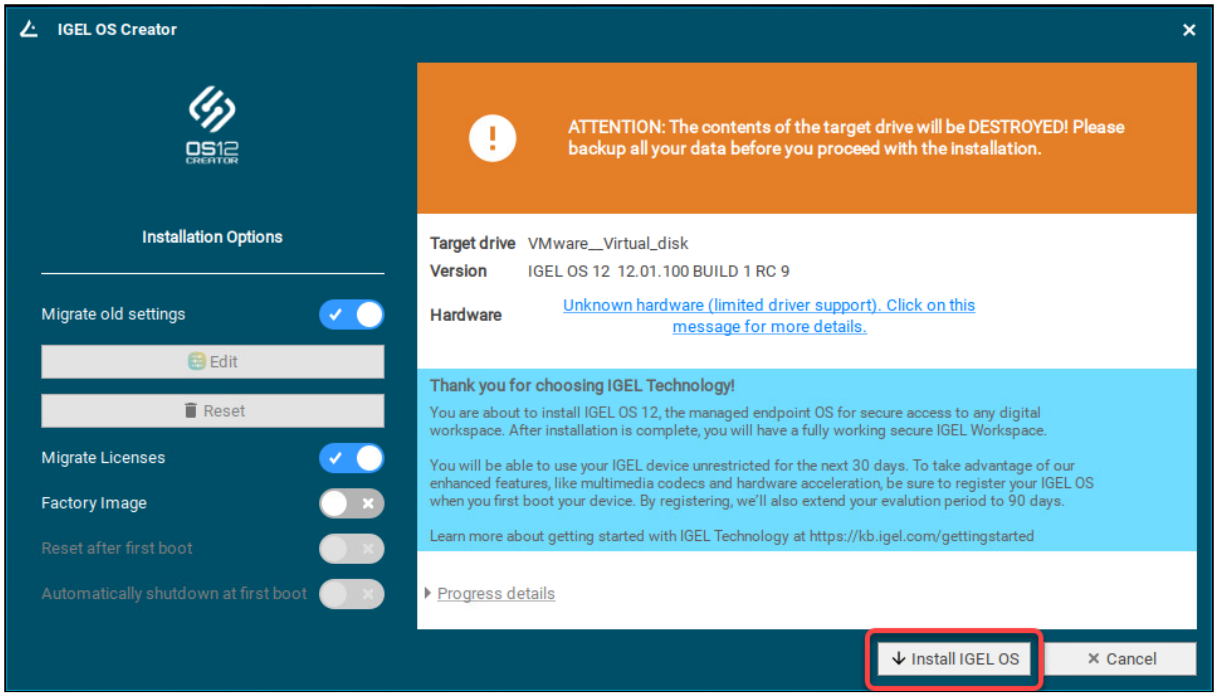
5. If one of the following is the case, make sure that **Migrate licenses** is enabled:
   - Your device has been operating with IGEL OS 11 before and you want to preserve the device's IGEL OS 11 licenses because you want to test IGEL OS 12 and downgrade to IGEL OS 11 afterward
   - Your device has been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



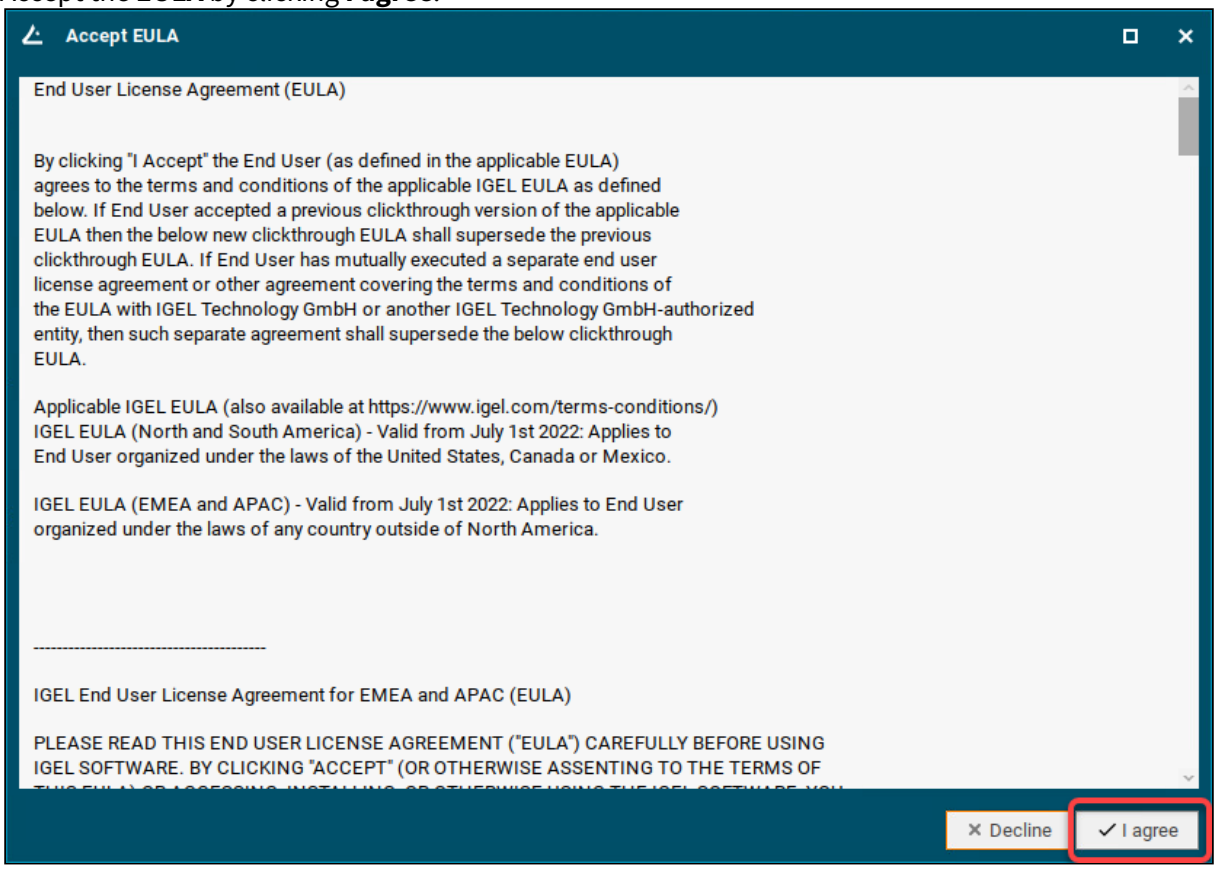
6. Check the **Target drive** to ensure that the system is installed on the desired drive.



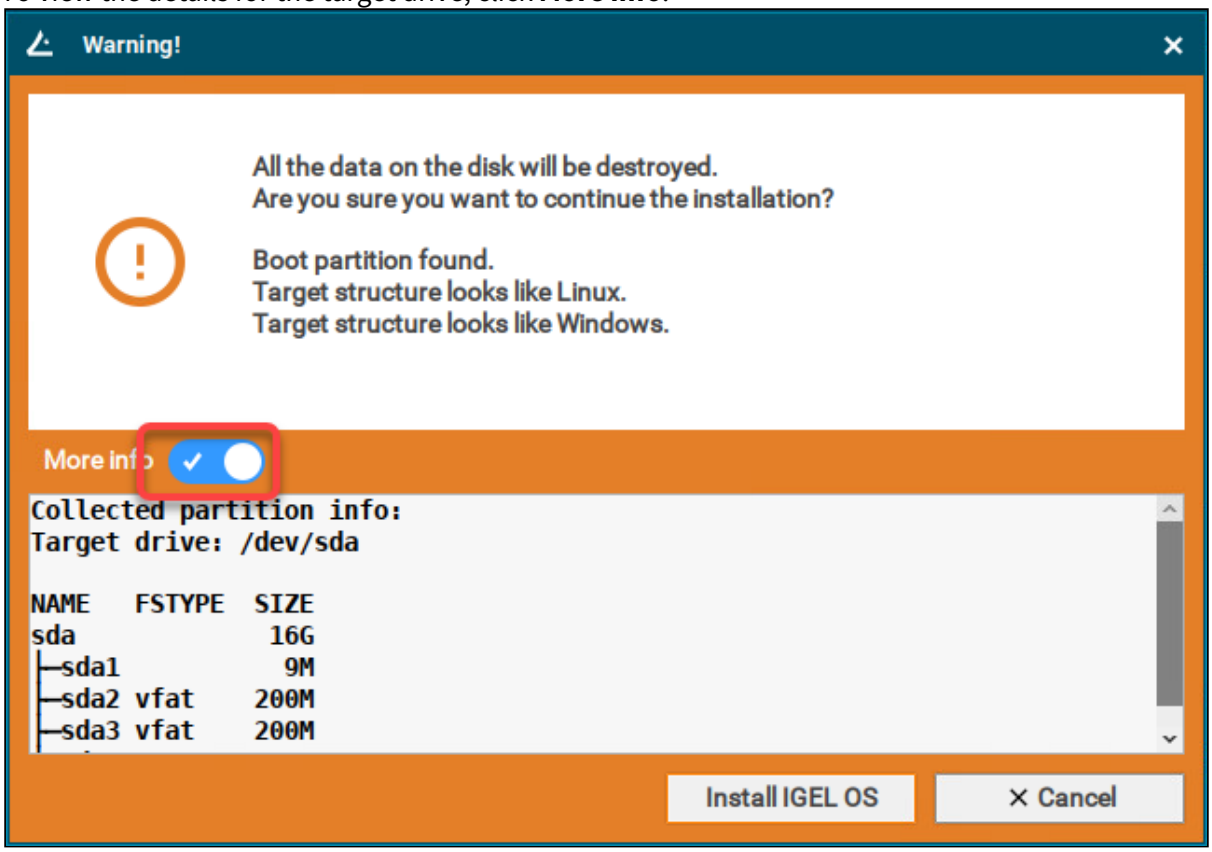
7. Click **Install IGEL OS**.



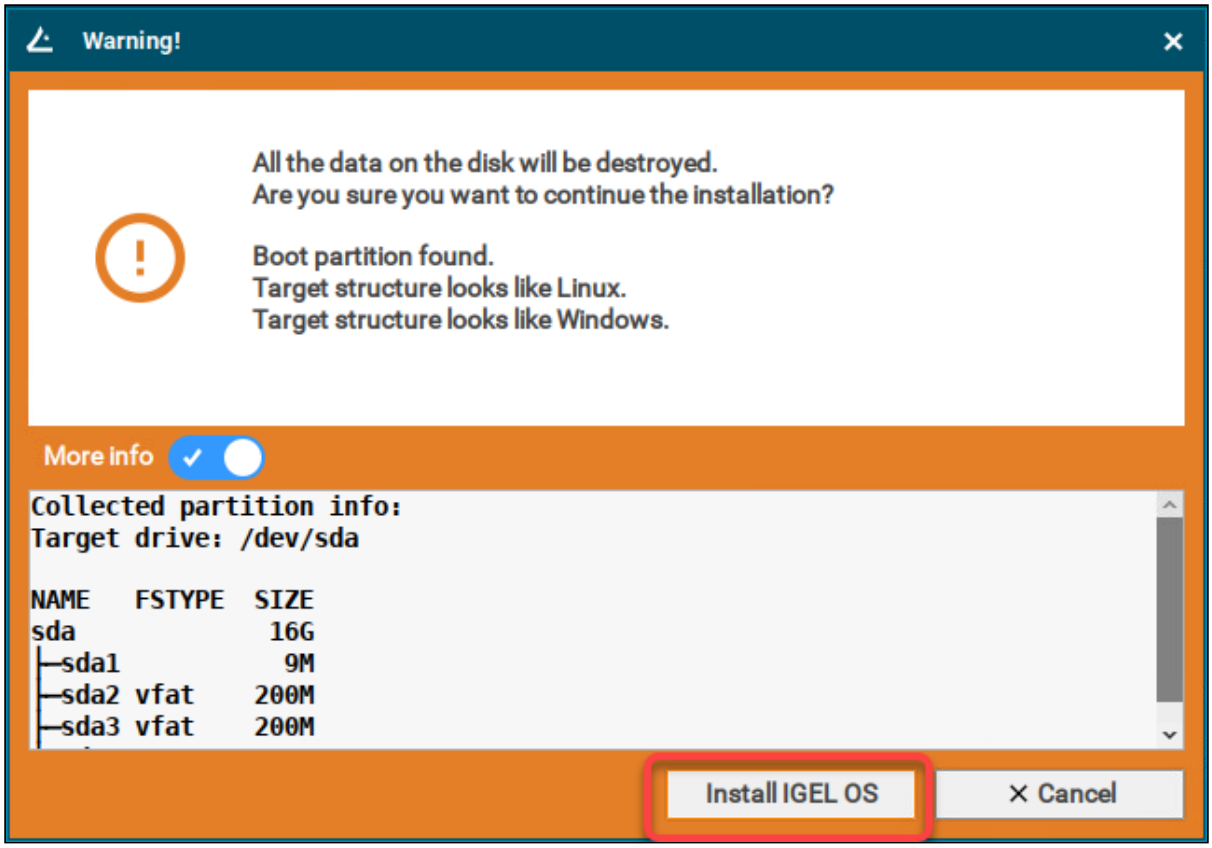
8. Accept the **EULA** by clicking **I agree**.



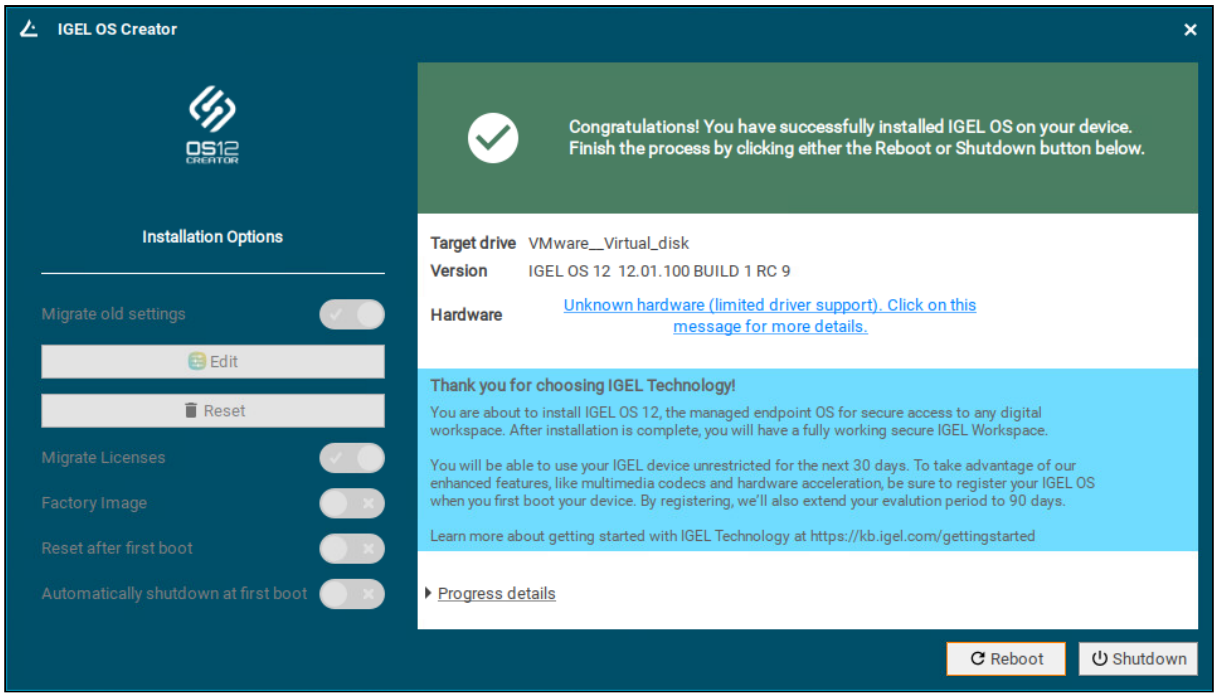
9. To view the details for the target drive, click **More Info**.



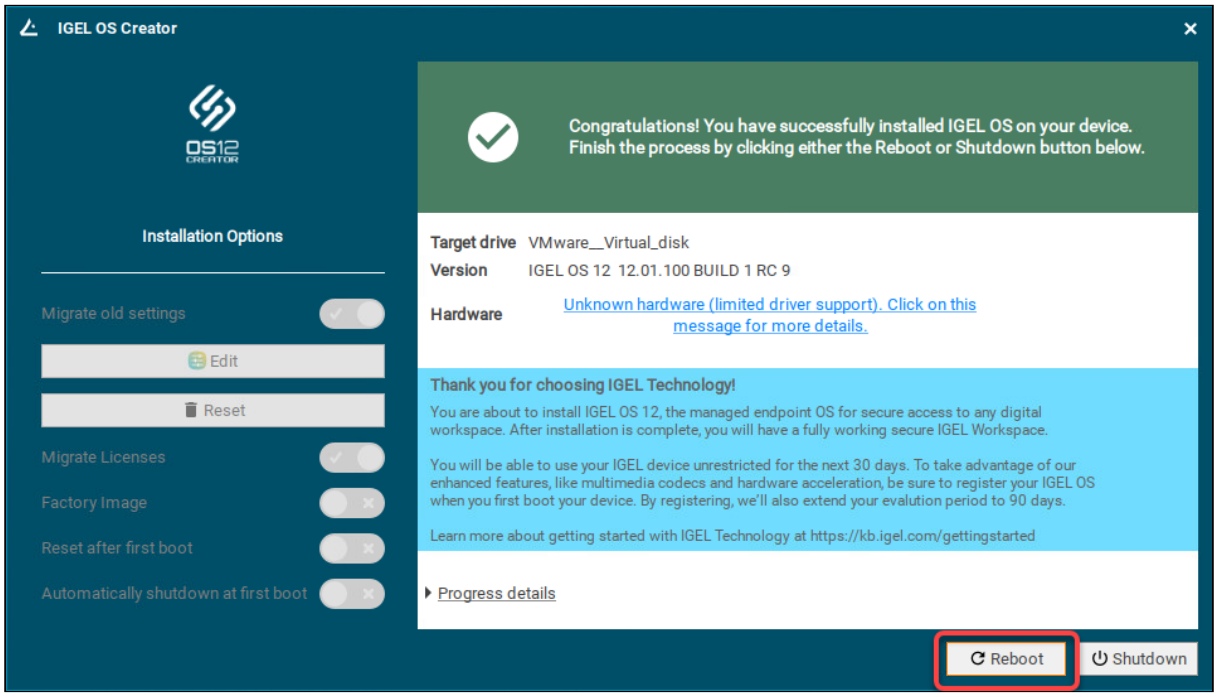
10. Click **Install IGEL OS**.



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

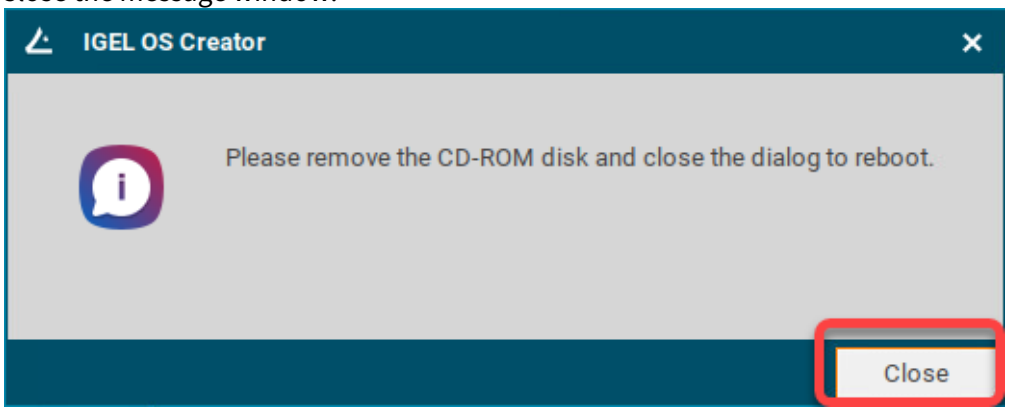


11. Click **Reboot**.



12. Remove the USB memory stick.

13. Close the message window.



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)

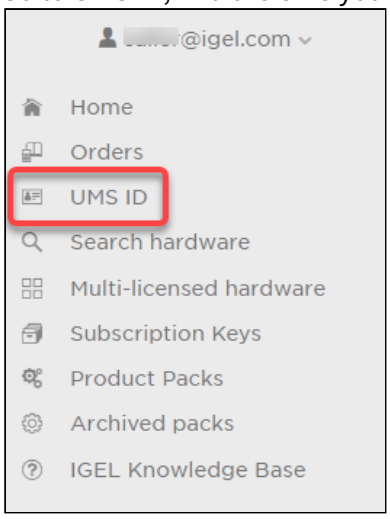
Function	Starter License (90 Days)	Demo License (90 Days)	After Expiry of Starter License / Demo License
Access OBS	✓	✓	✓
Redirect to UMS/ICG	✓	✓	✓

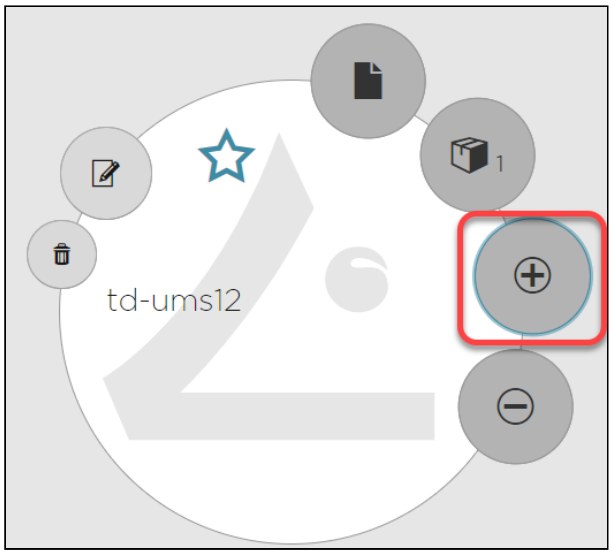
Getting Your Licenses Ready for Deployment

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).

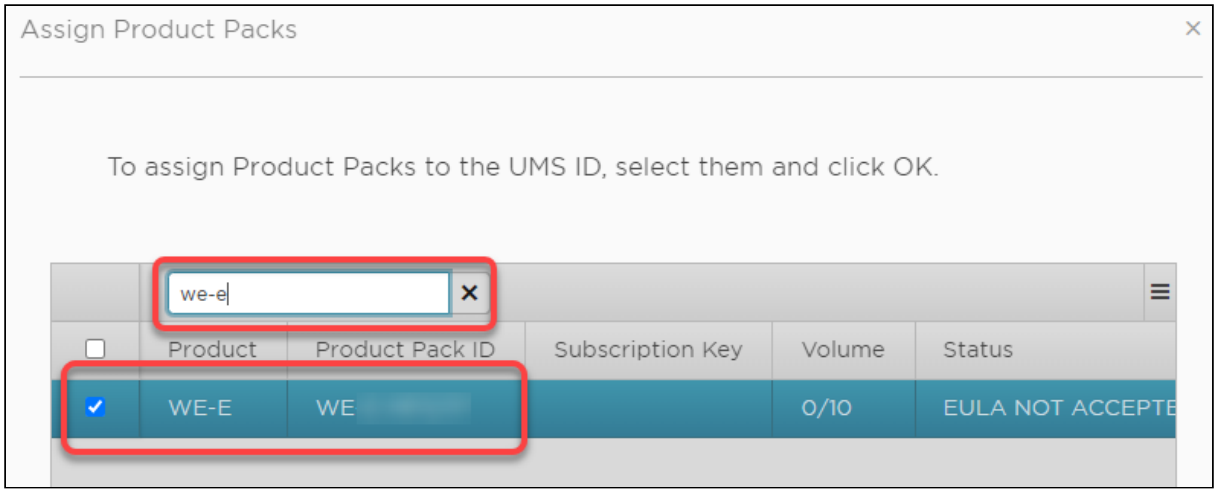
21 https://activation.igel.com/

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





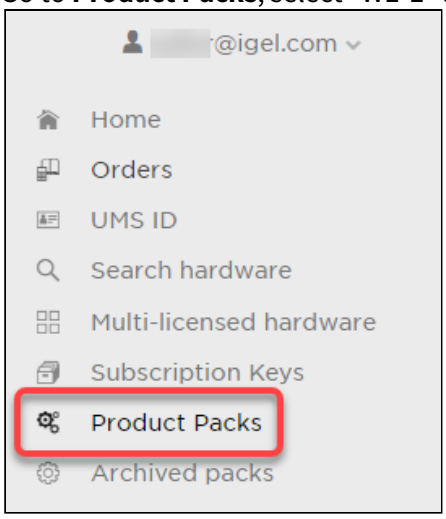
3. Search for "we-e" and select the relevant Product Pack.

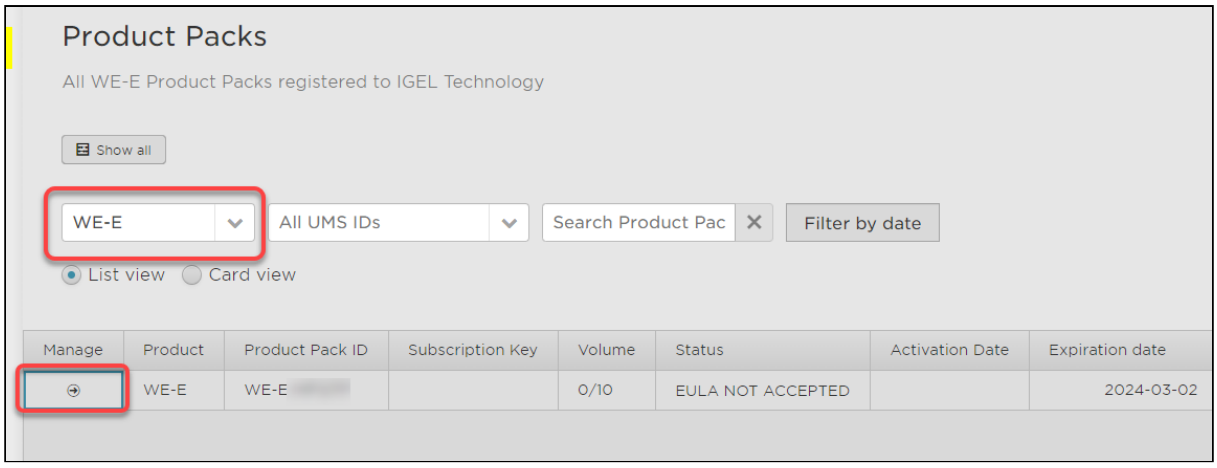


If you can not find the Product Pack, it may be that it has been assigned to another UMS that was defined as the default UMS resp. default UMS ID. (If a default UMS ID has been defined in your ILP, a new WE-E Product Pack will be assigned to that UMS automatically.)

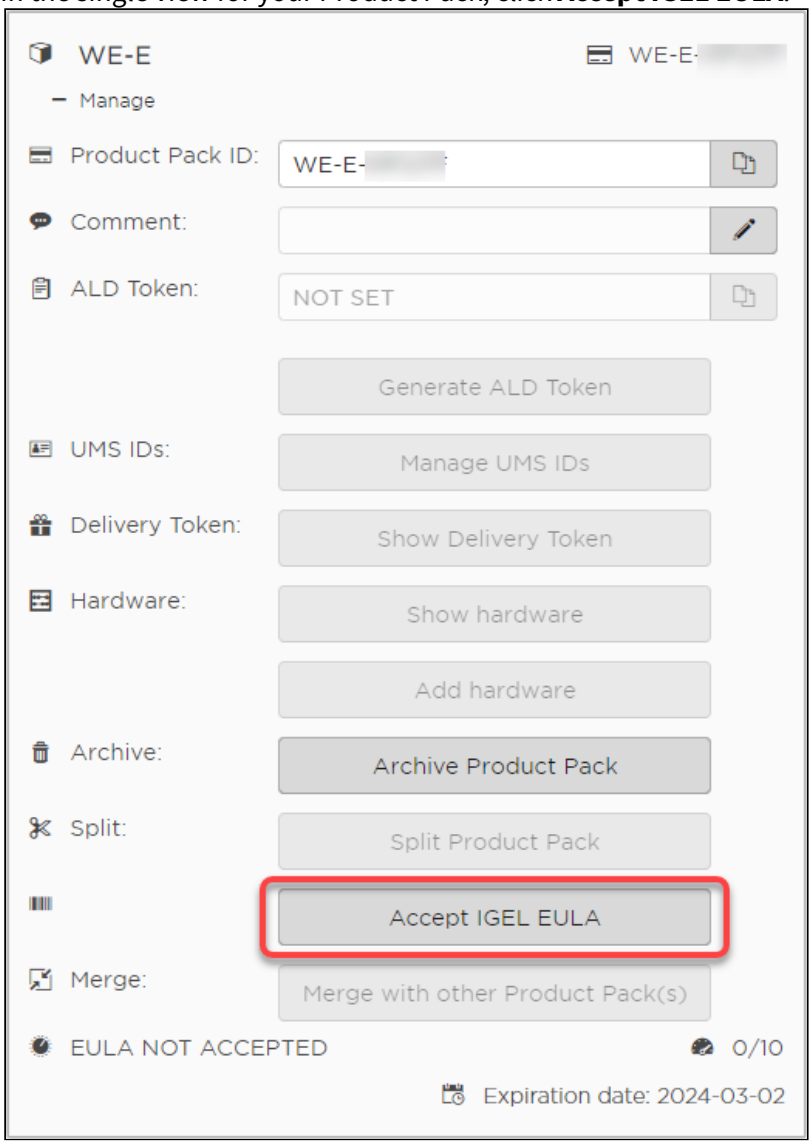
To correct this, go to the default UMS ID, which is marked with a  , click  , unassign the Product Pack from this UMS and then use  on the relevant UMS ID to assign it to the proper UMS.

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

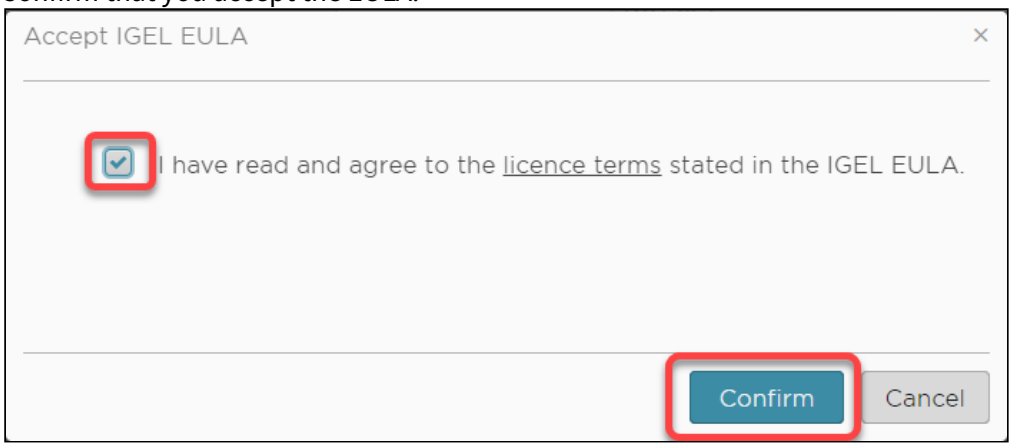



Product Packs
All WE-E Product Packs registered to IGEL Technology
Show all
WE-E
All UMS IDs
Search Product Pac
Filter by date
List view
Card view
Manage
Product
Product Pack ID
Subscription Key
Volume
Status
Activation Date
Expiration date
WE-E
WE-E
0/10
EULA NOT ACCEPTED
2024-03-02

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



6. Confirm that you accept the 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).

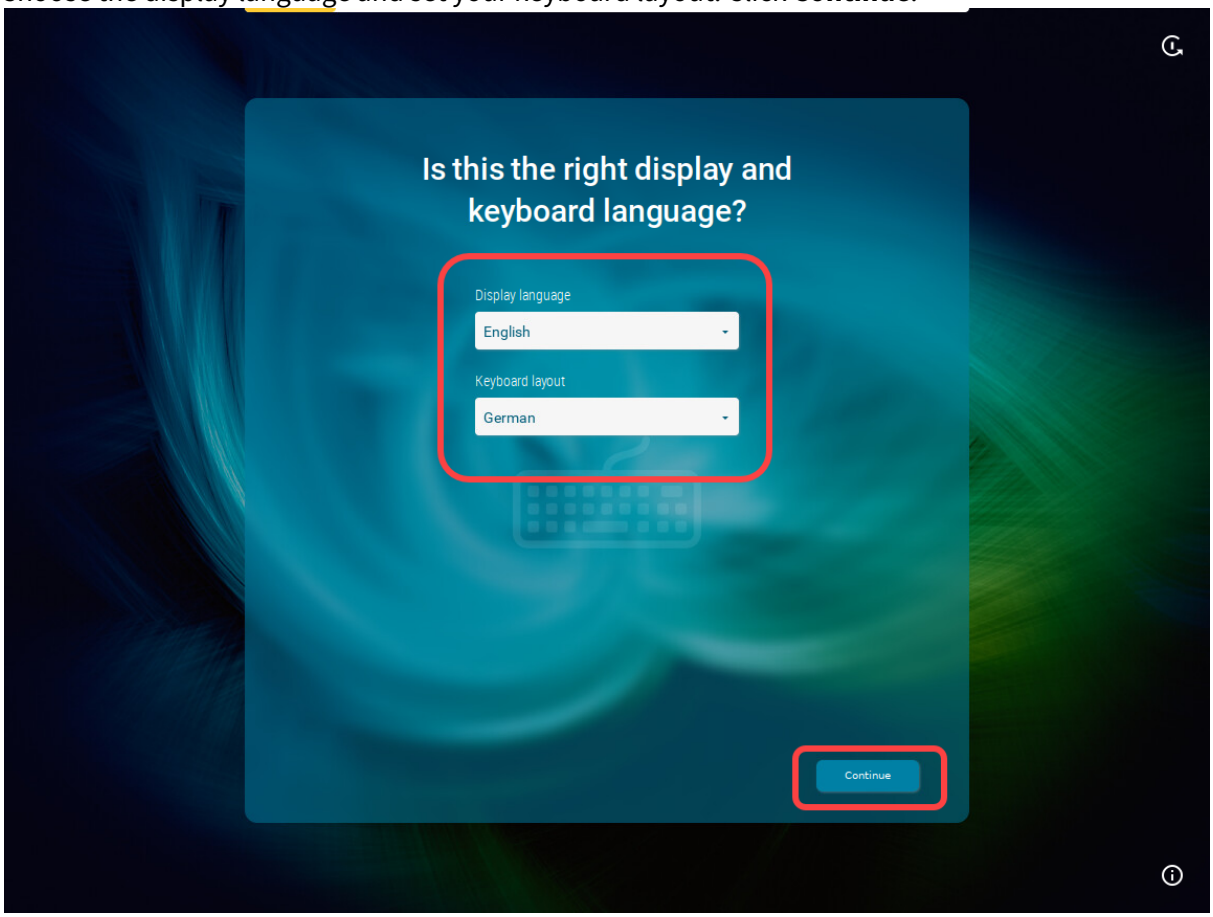
For an alternative device registration method, see Alternative Onboarding Method: Registering Devices with the UMS Using the One-Time Password(see page 165).

> 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.

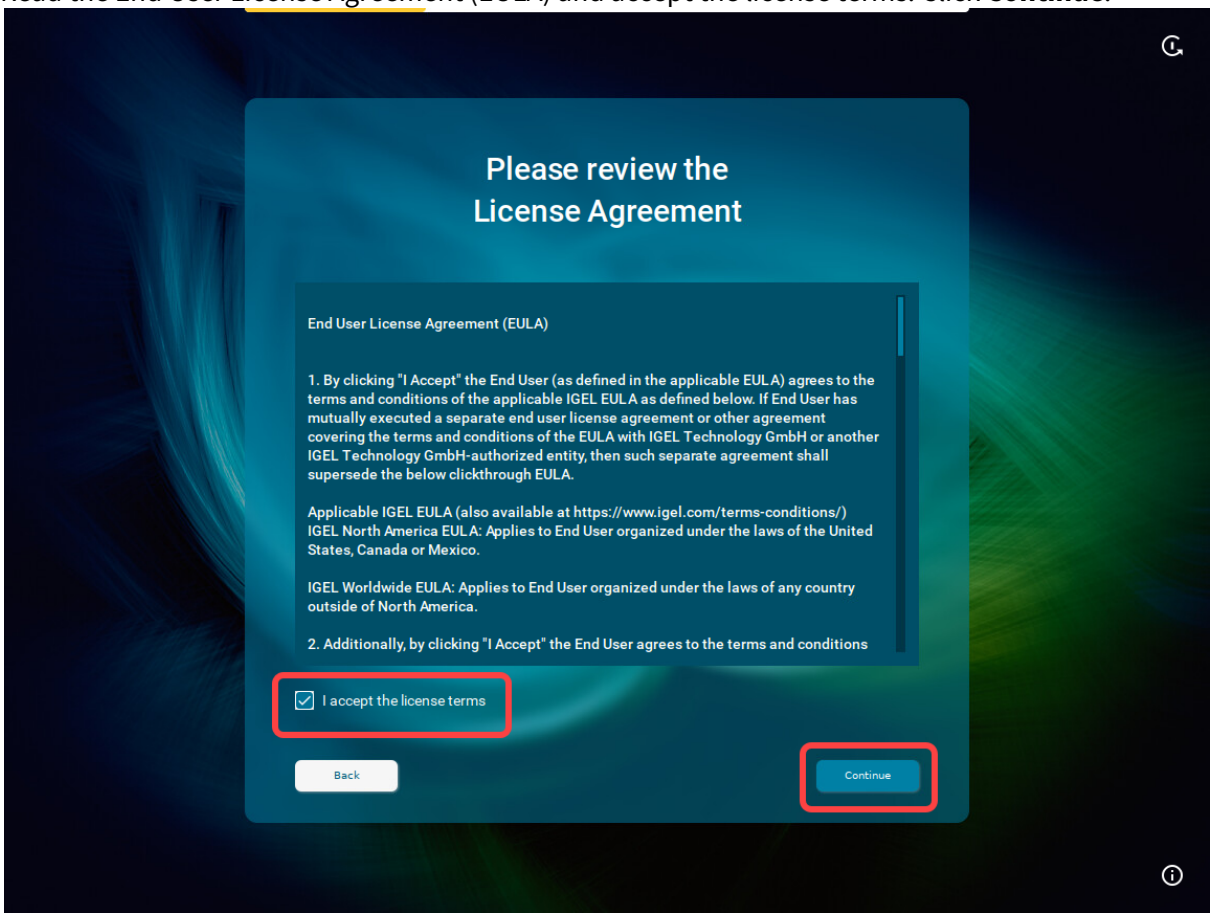
Register IGEL OS 12 Devices with the UMS via IGEL Onboarding Service

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

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

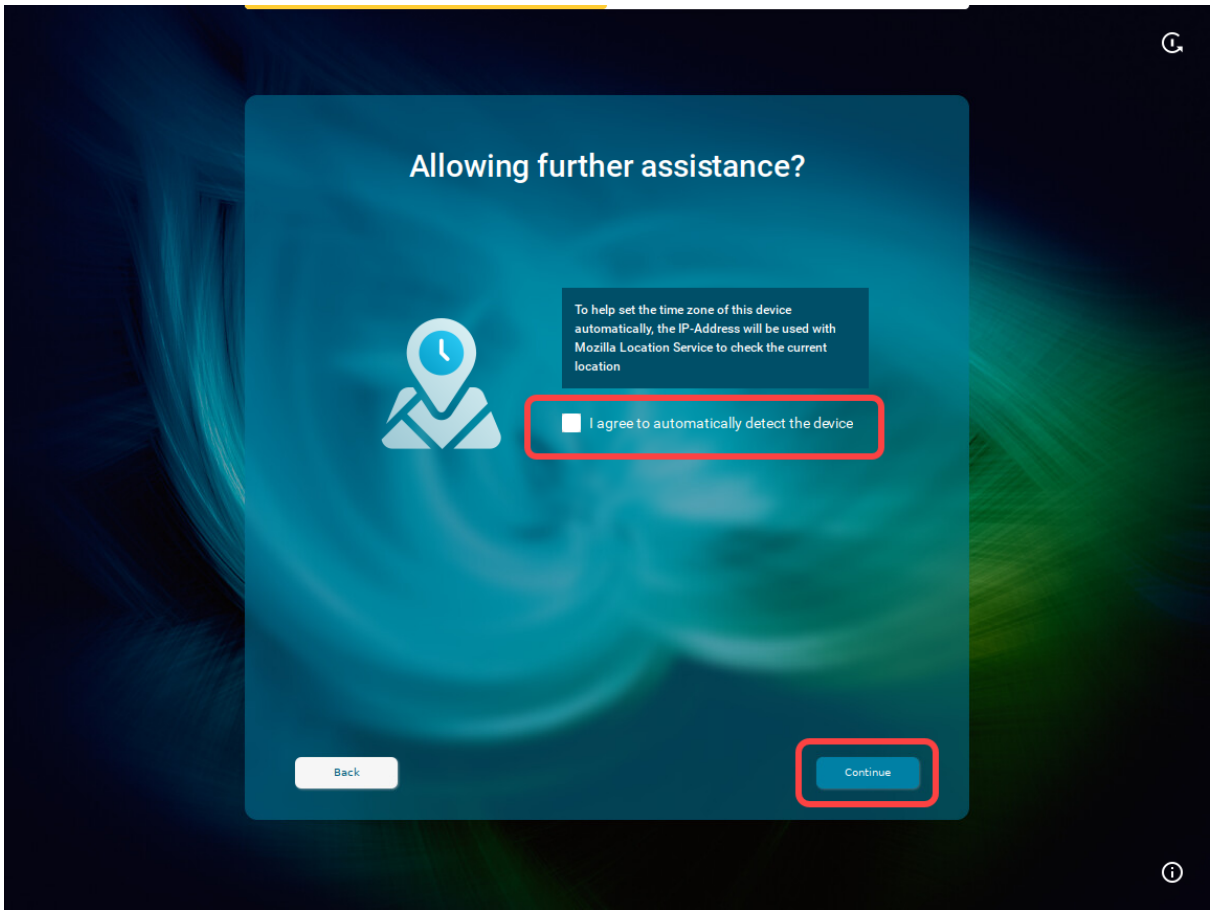


3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.

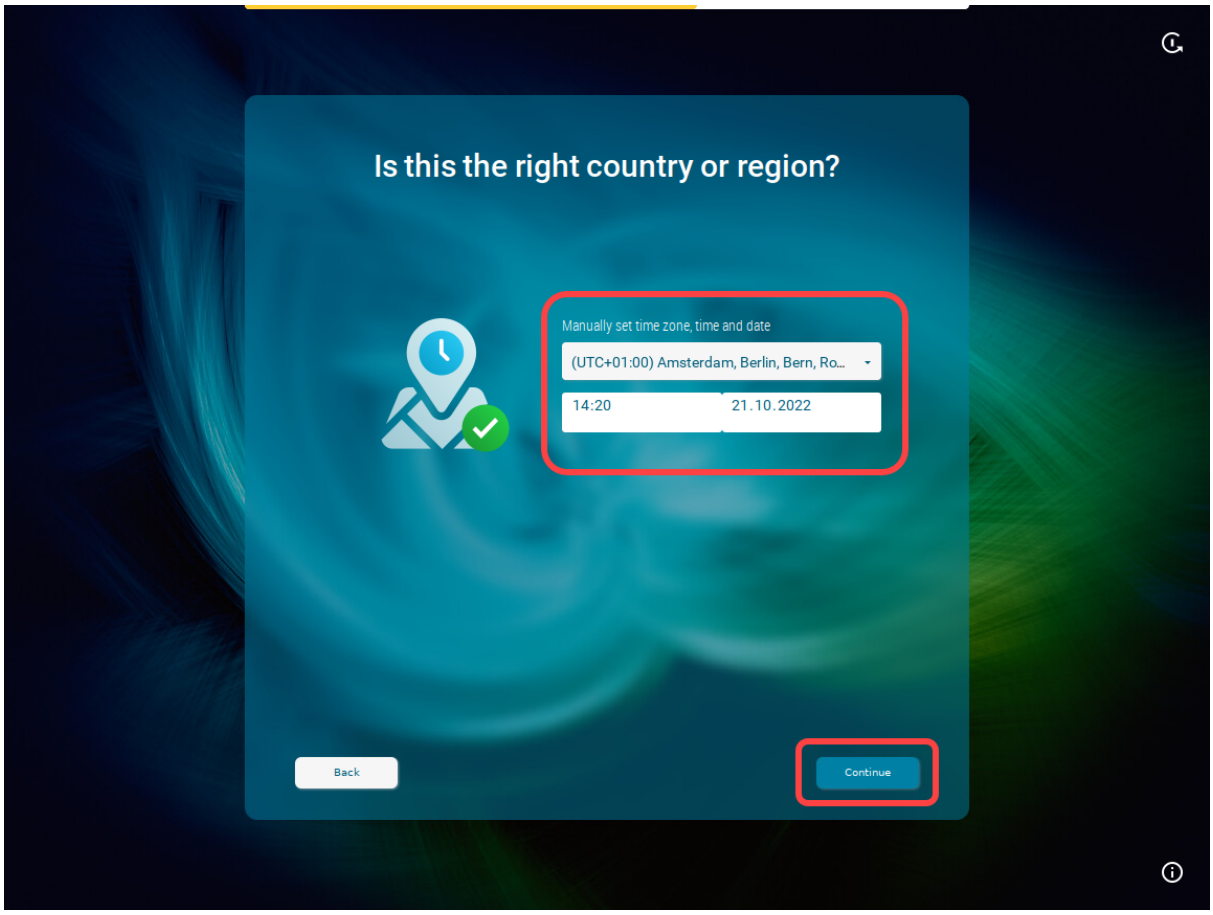


4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under Troubleshooting: Configuring a Network during the Onboarding(see page 174).

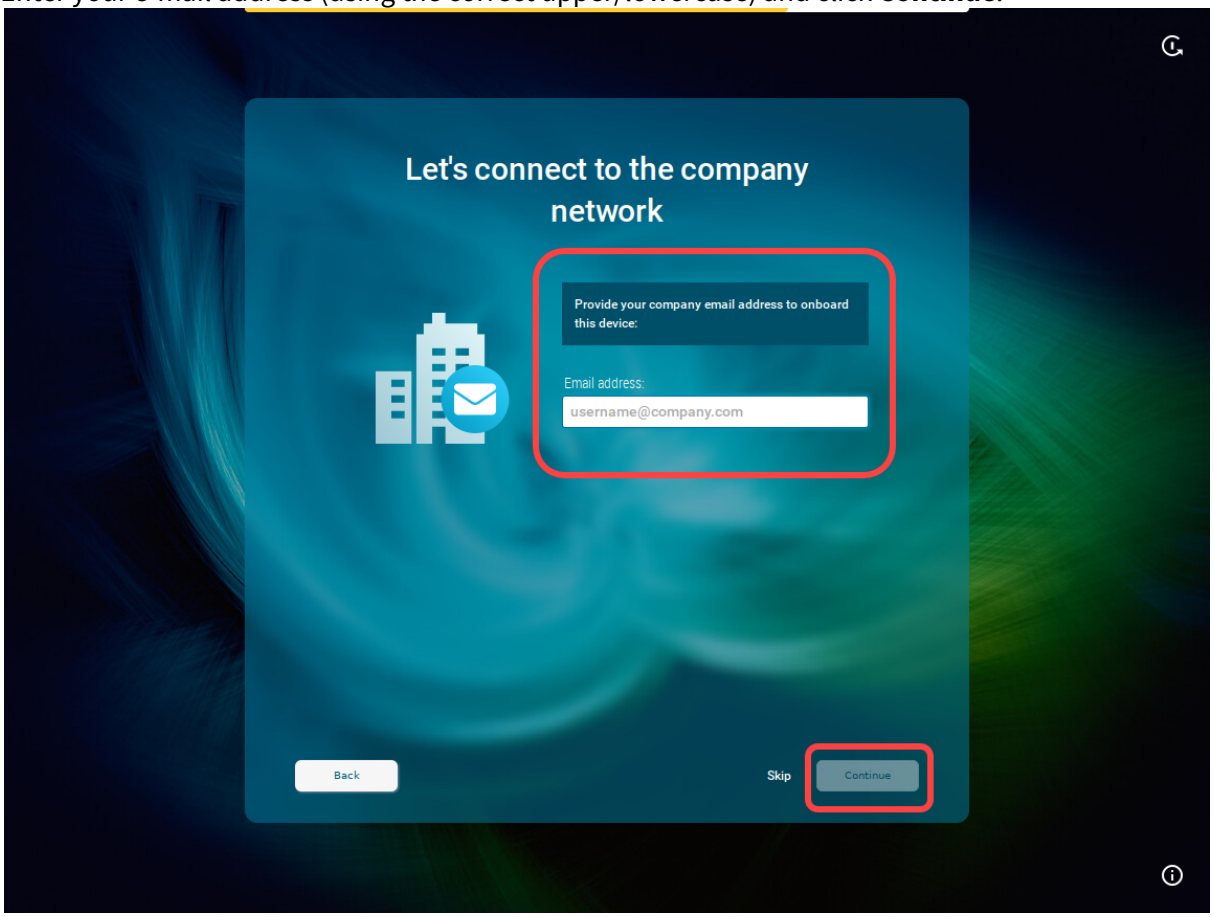
5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.



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

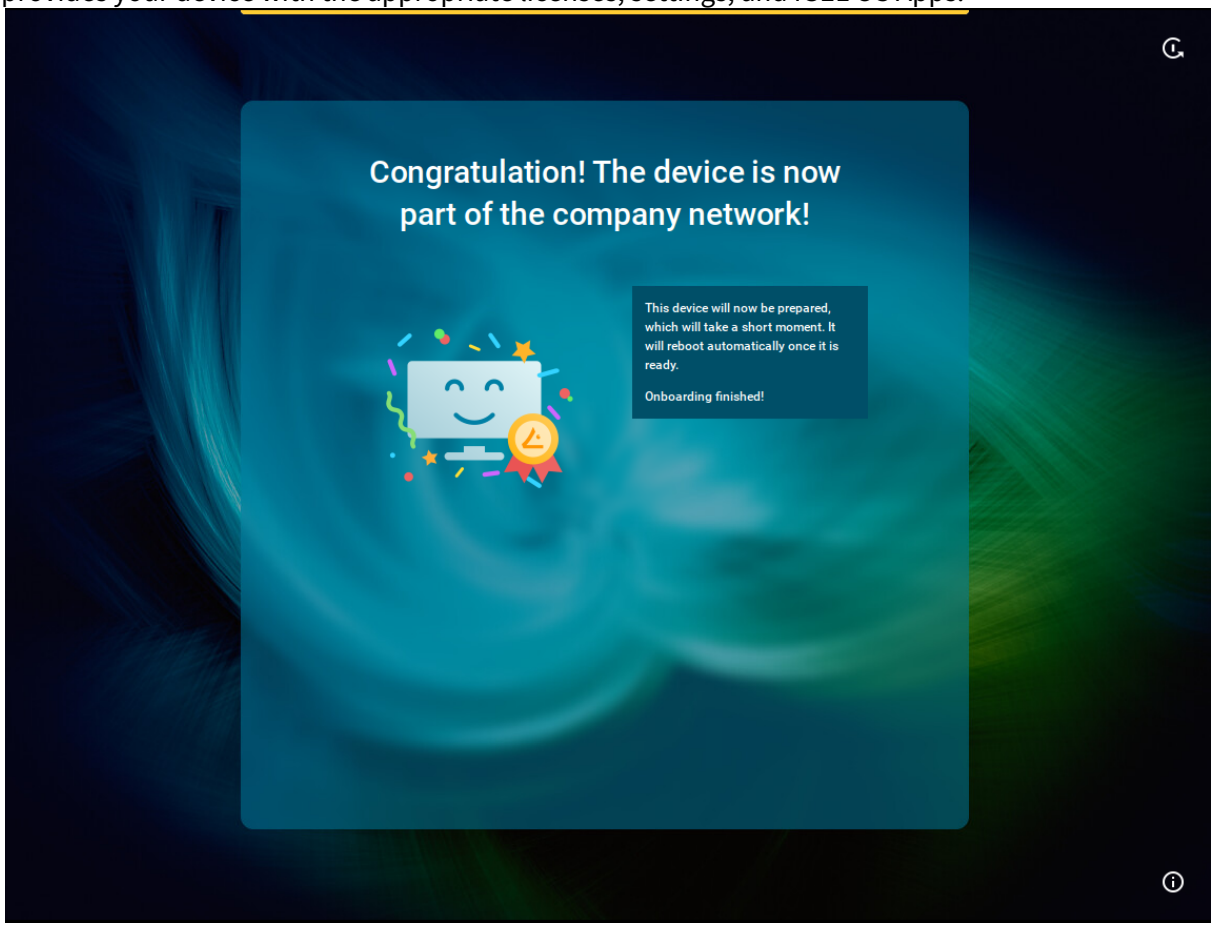

Is this the right country or region?
Manually set time zone, time and date
(UTC+01:00) Amsterdam, Berlin, Bern, Ro...
14:20
21.10.2022
Back
Continue

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

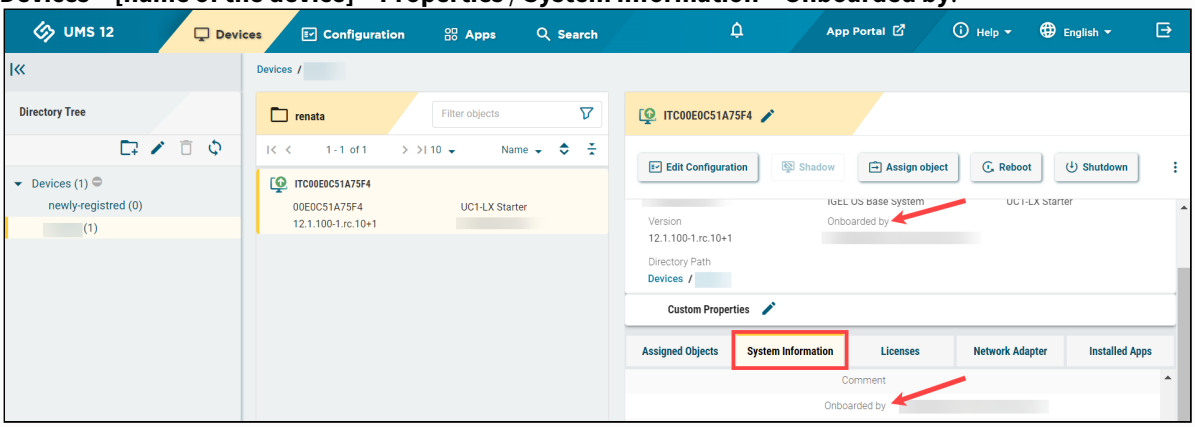


When everything went well, your device will be integrated into your company network after the reboot. This means it has been connected to your IGEL Universal Management Suite (UMS) which

provides your device with the appropriate licenses, settings, and IGEL OS Apps.



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**.

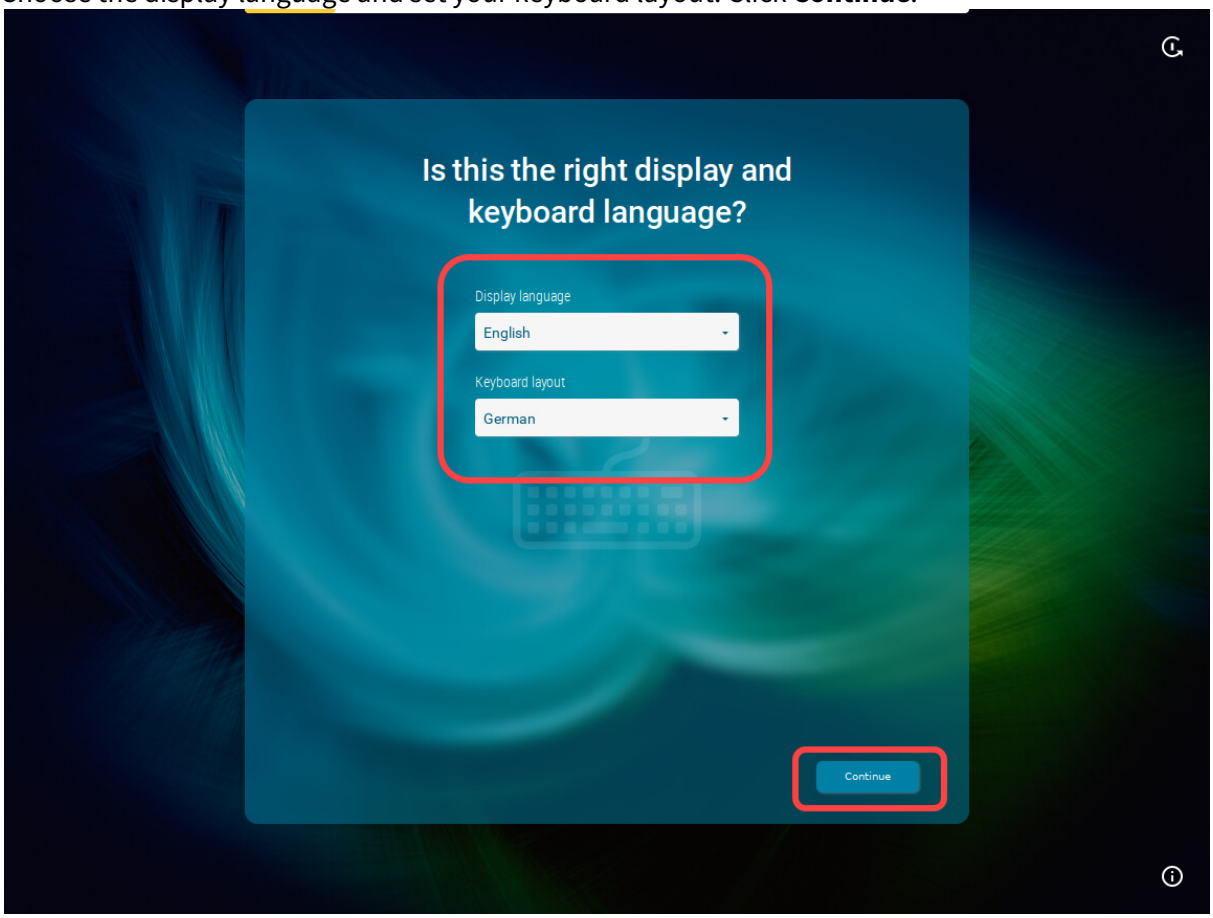


Alternative Onboarding Method: Registering Devices with the UMS Using the One-Time Password

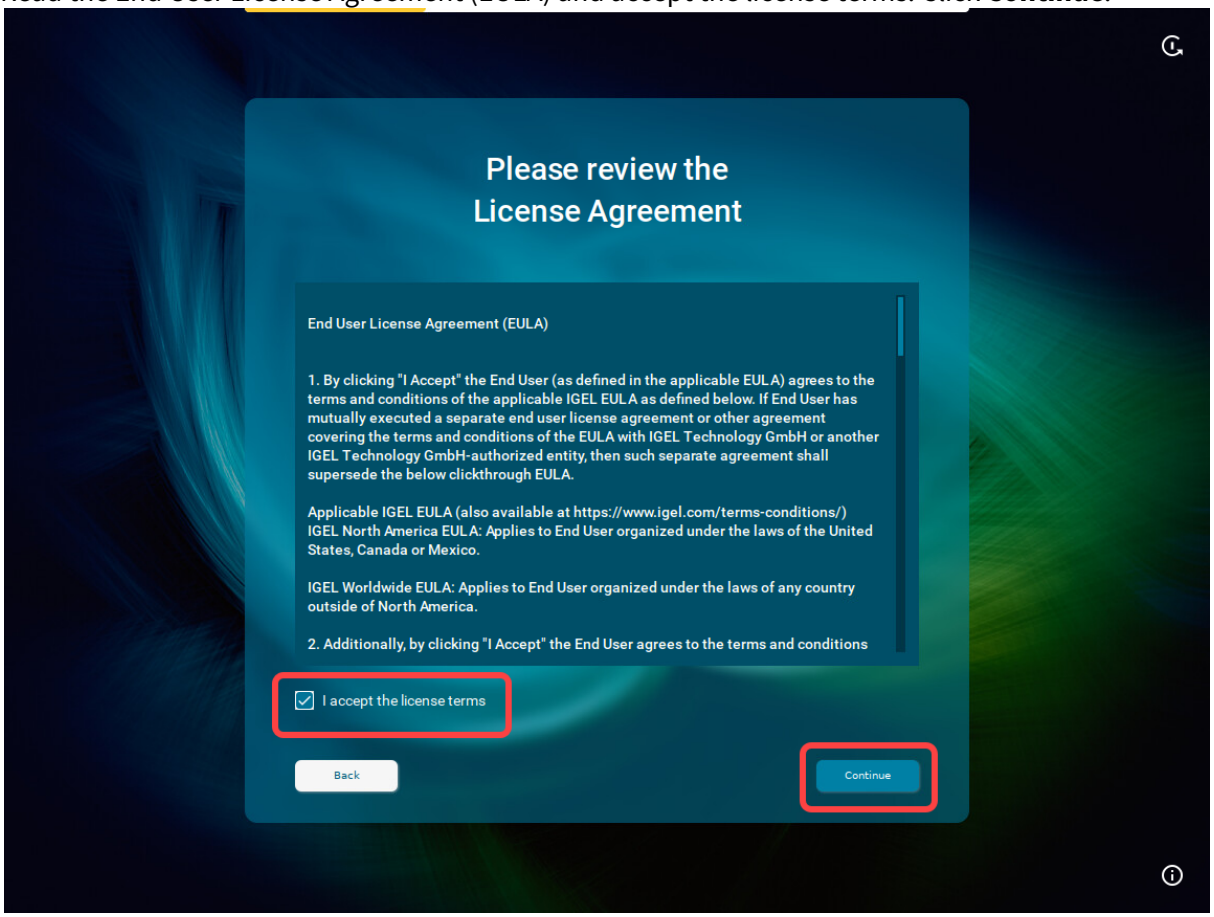
If you decided not to use IGEL Onboarding Service for the registration of your IGEL OS 12 devices, you can use a one-time password method as an alternative.

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

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

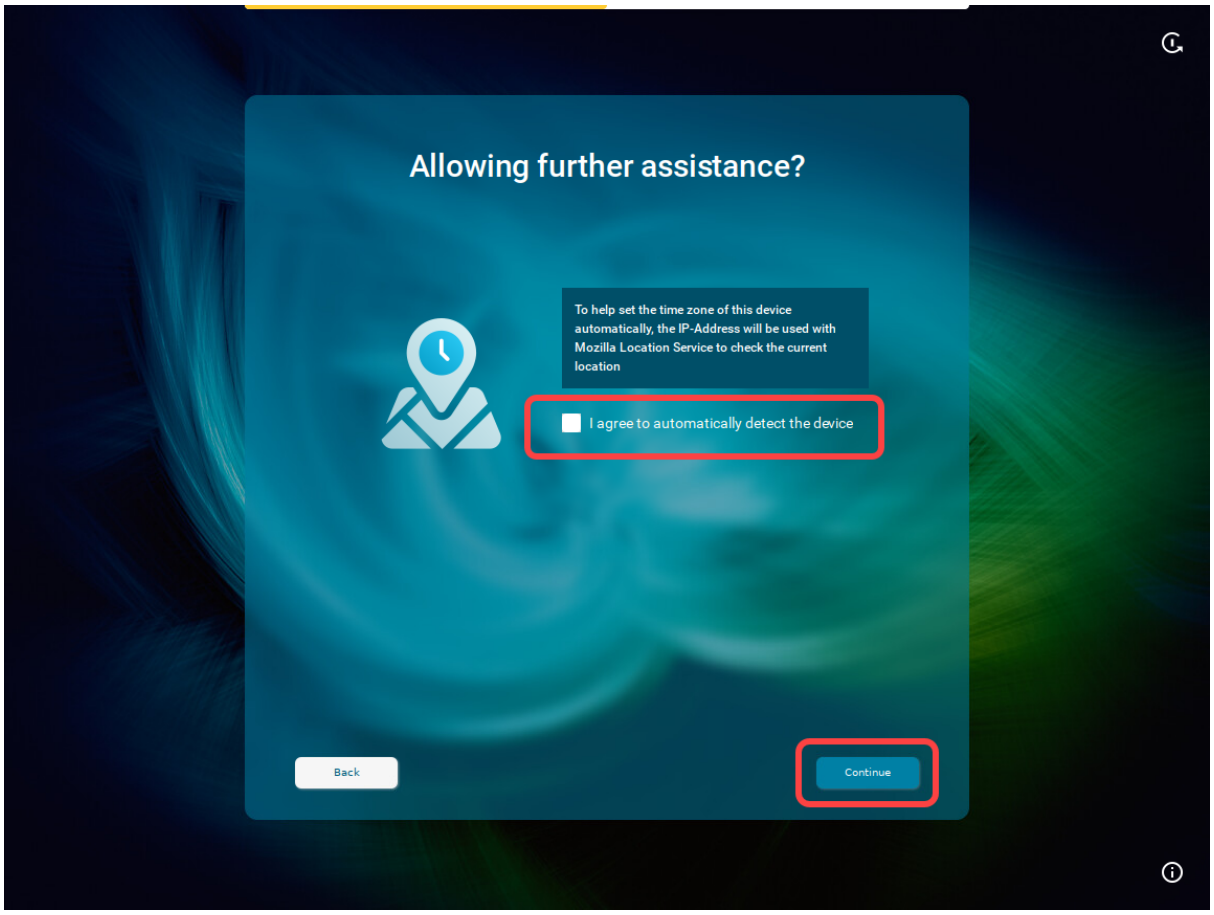


3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.

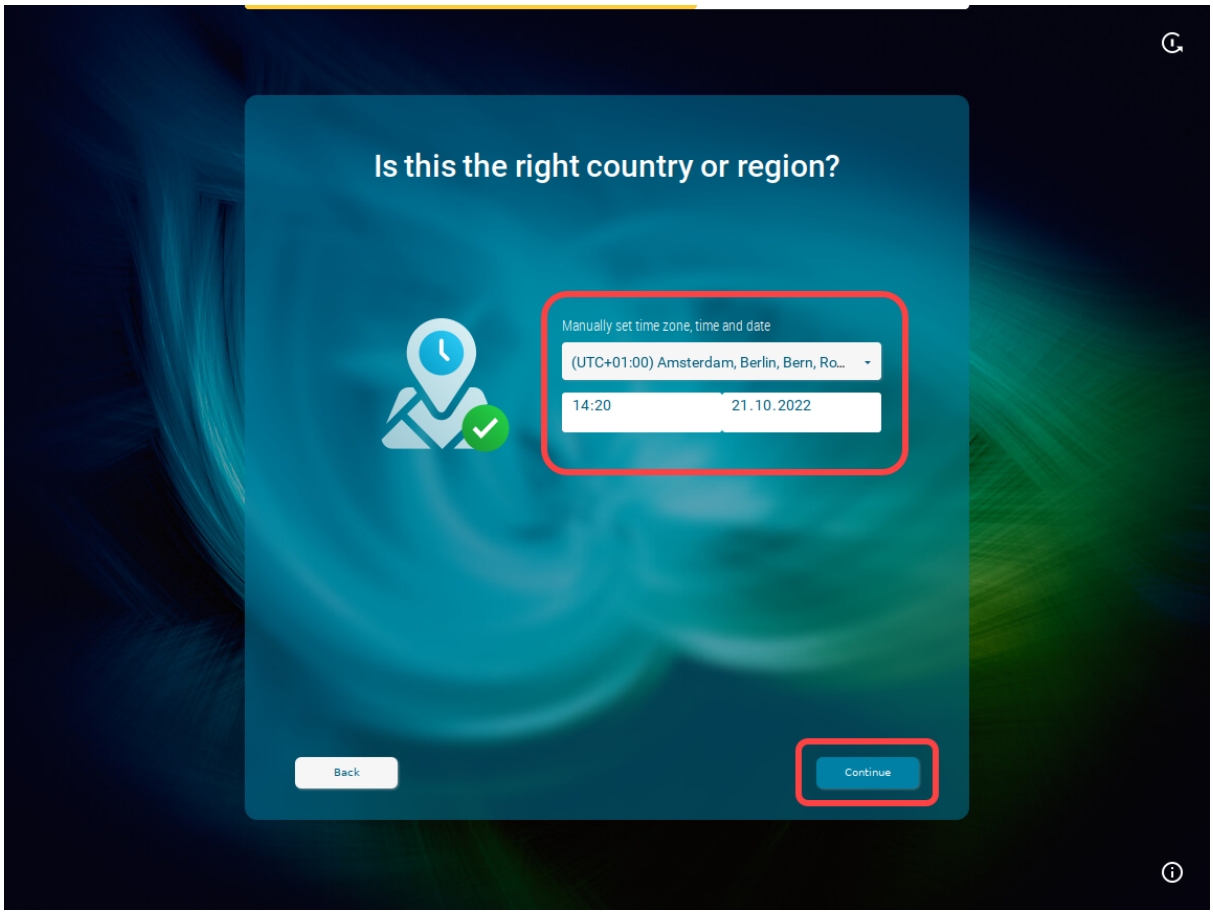


4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under Troubleshooting: Configuring a Network during the Onboarding(see page 174).

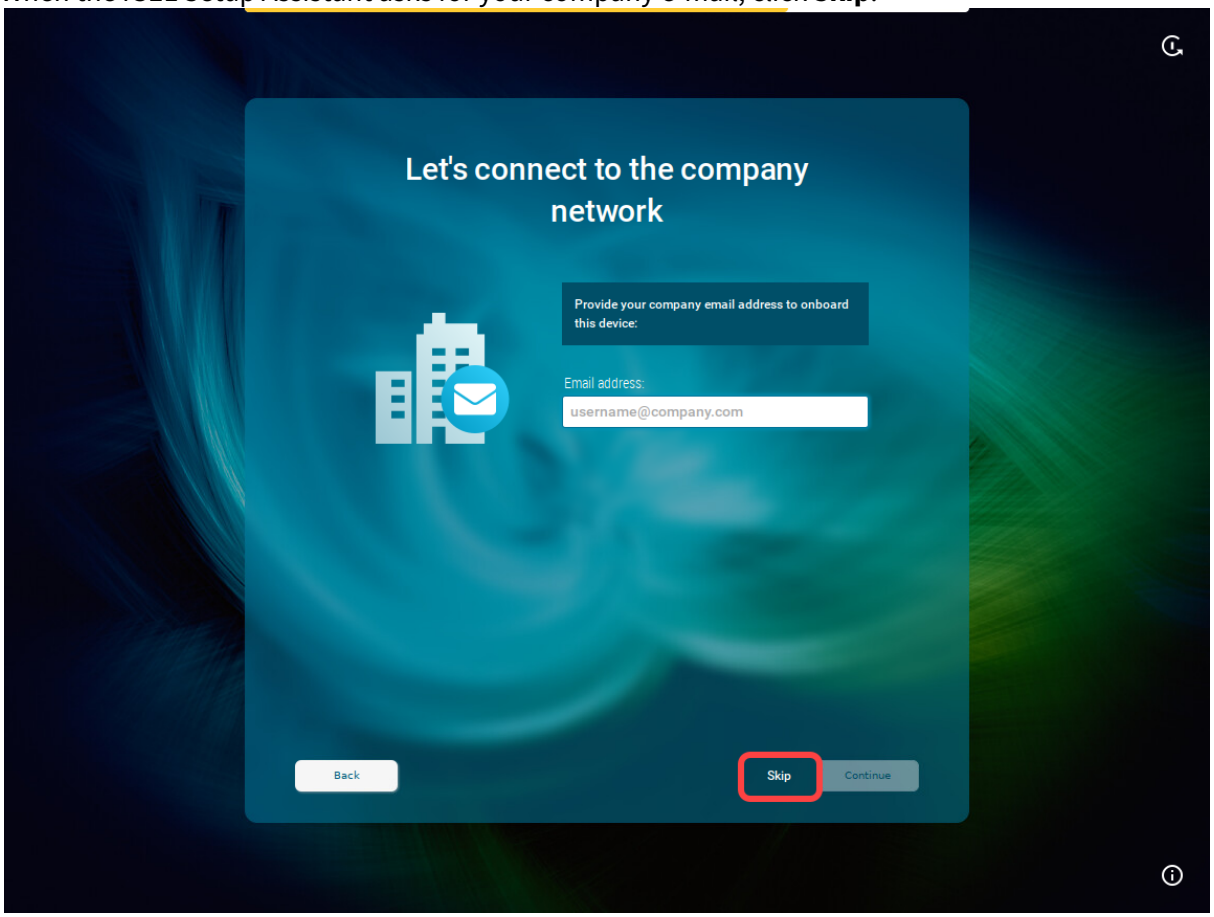
5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.



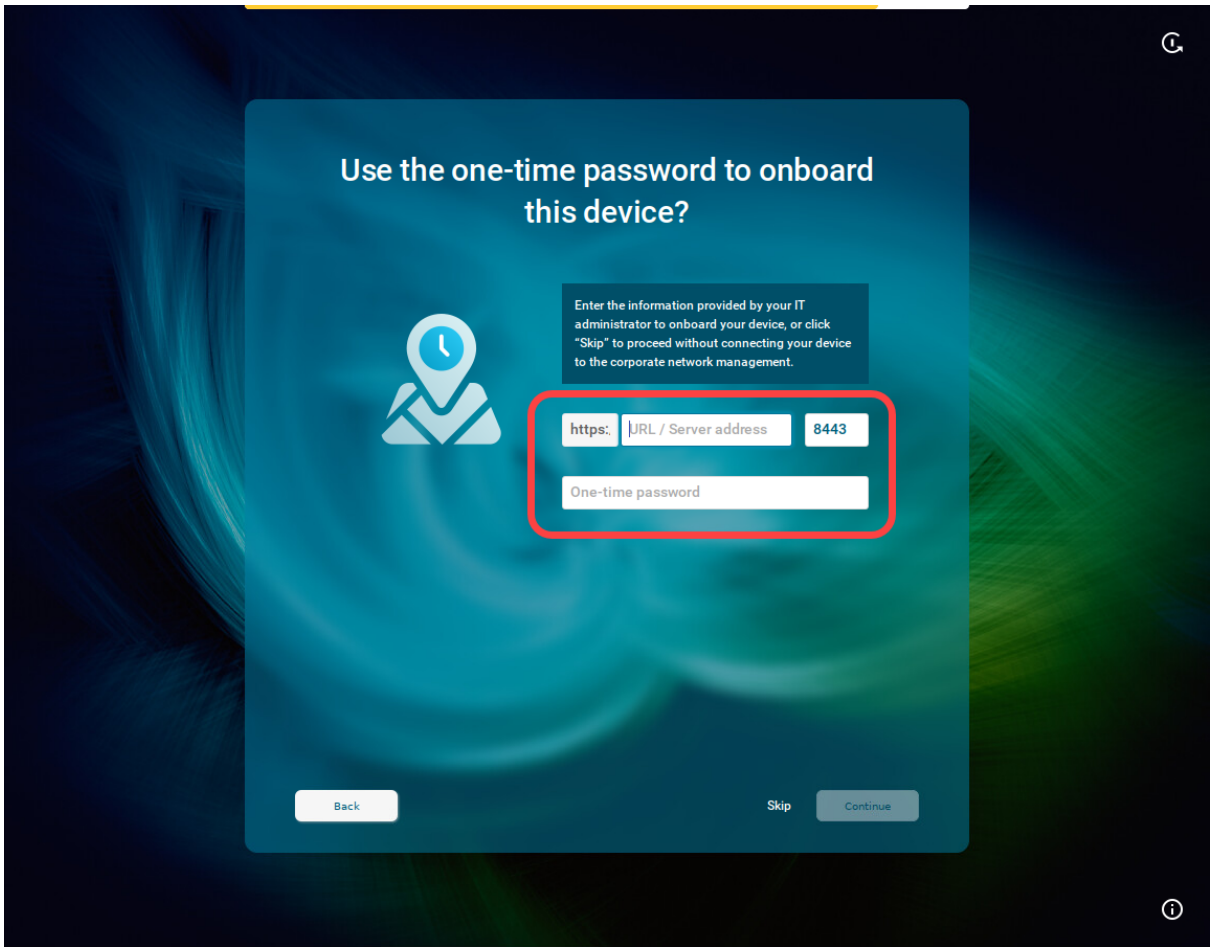
Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.


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
Back
Continue

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



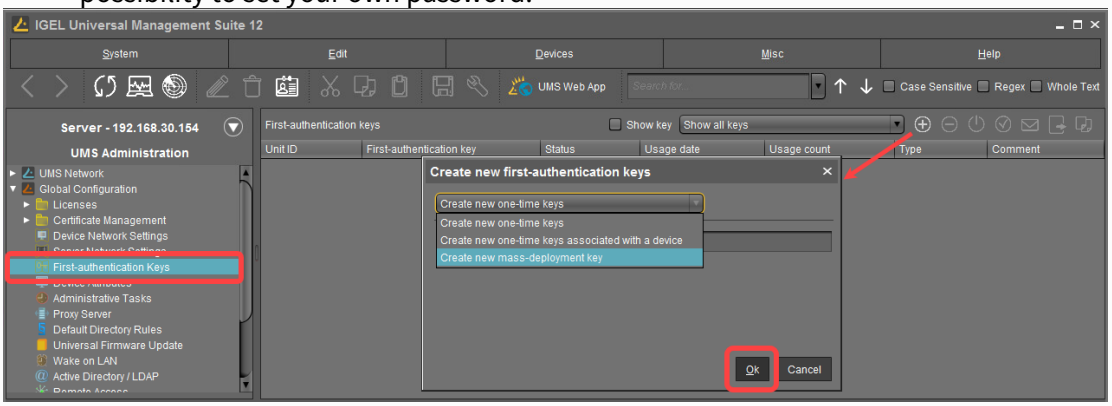
You will be asked to enter the data provided by your administrator:



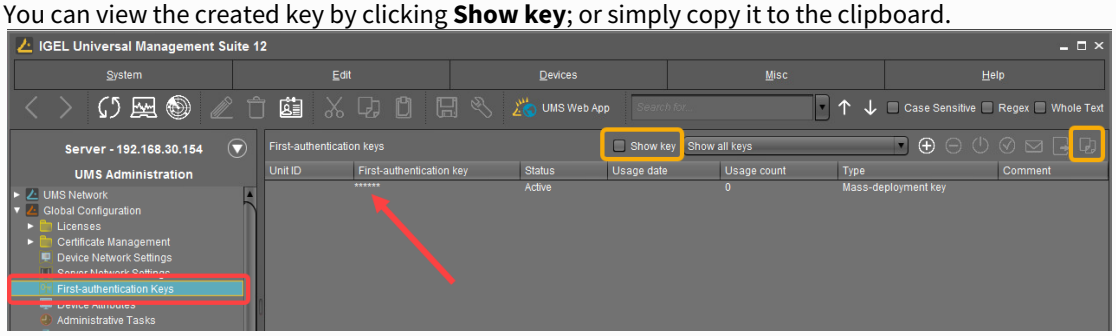
7. Enter the following data and click **Continue**:
   URL / Server address: Host name or IP address of the UMS Server. If configured, you can alternatively use the Public Address of the UMS Server or Cluster Address.
   Port: Web server port (Default: 8443). If configured, you can alternatively use 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.

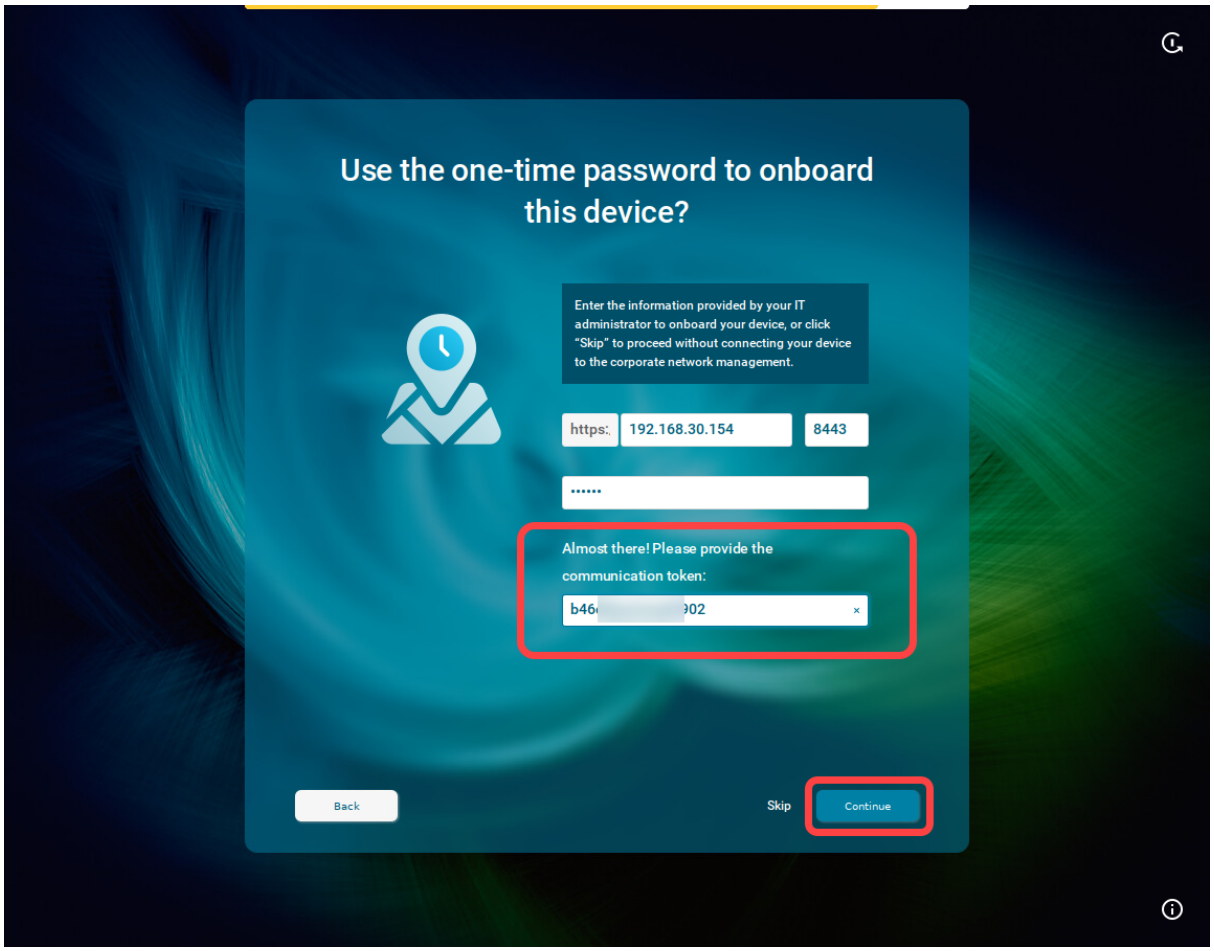
- Mass-deployment keys: Multiple-time keys that can be used by any device and will remain valid after use. If you choose to create a mass-deployment key, there is a possibility to set your own password.



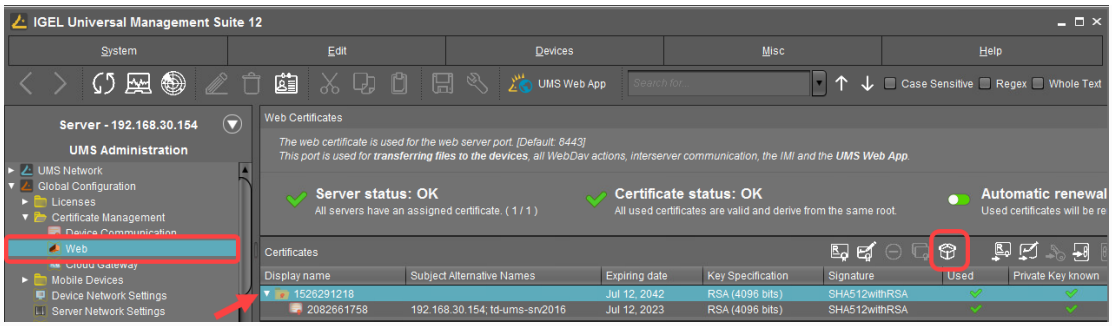
You can view the created key by clicking **Show key**; or simply copy it to the clipboard.

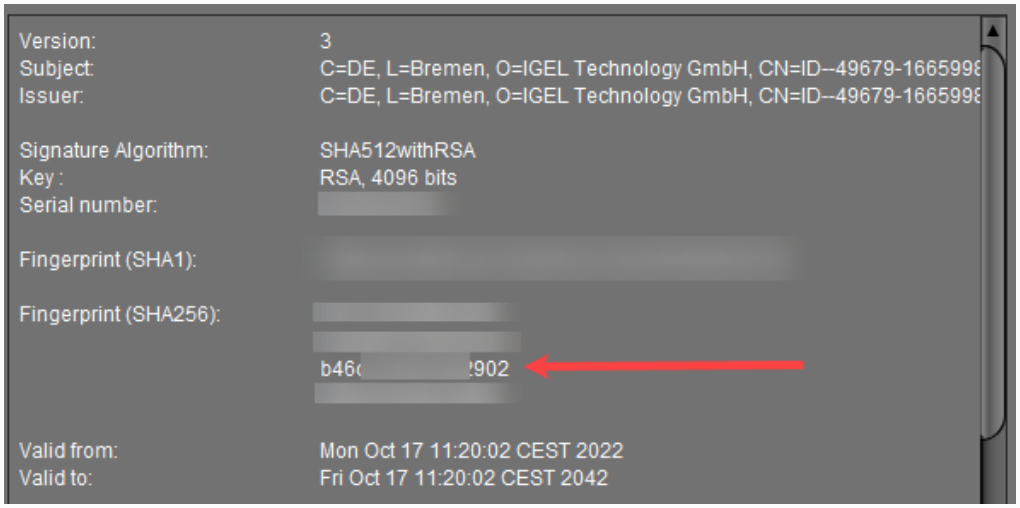


8. In the mask opened, enter the communication token. The communication token is **the third part of the SHA256 fingerprint of the root certificate of your UMS Server**. Then click **Continue**.

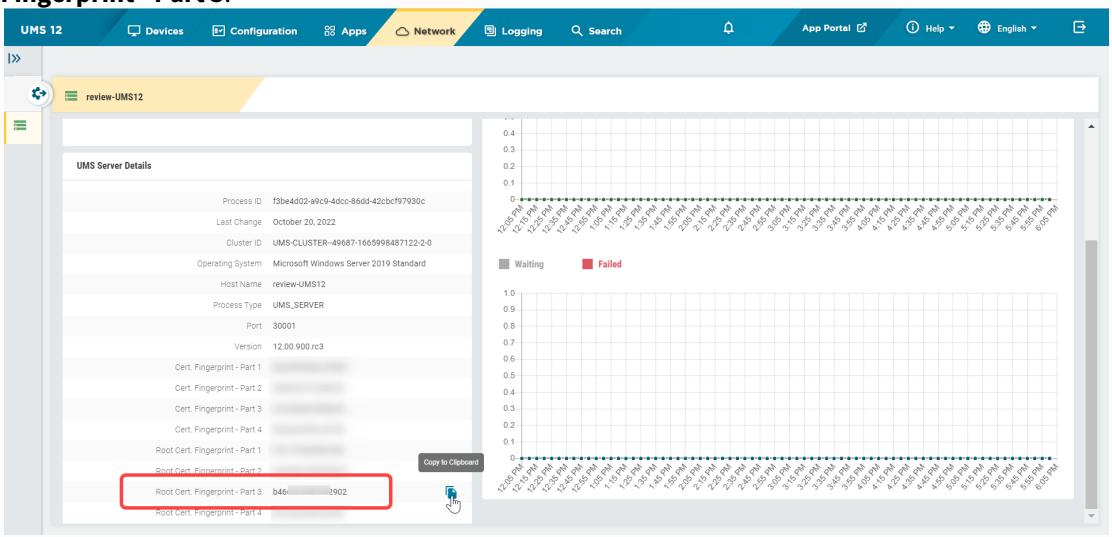


How to Find Out the Communication Token / Root Certificate Fingerprint (SHA256)
Go to **UMS Console > UMS Administration > Global Configuration > Certificate Management > Web**, select the certificate and click .



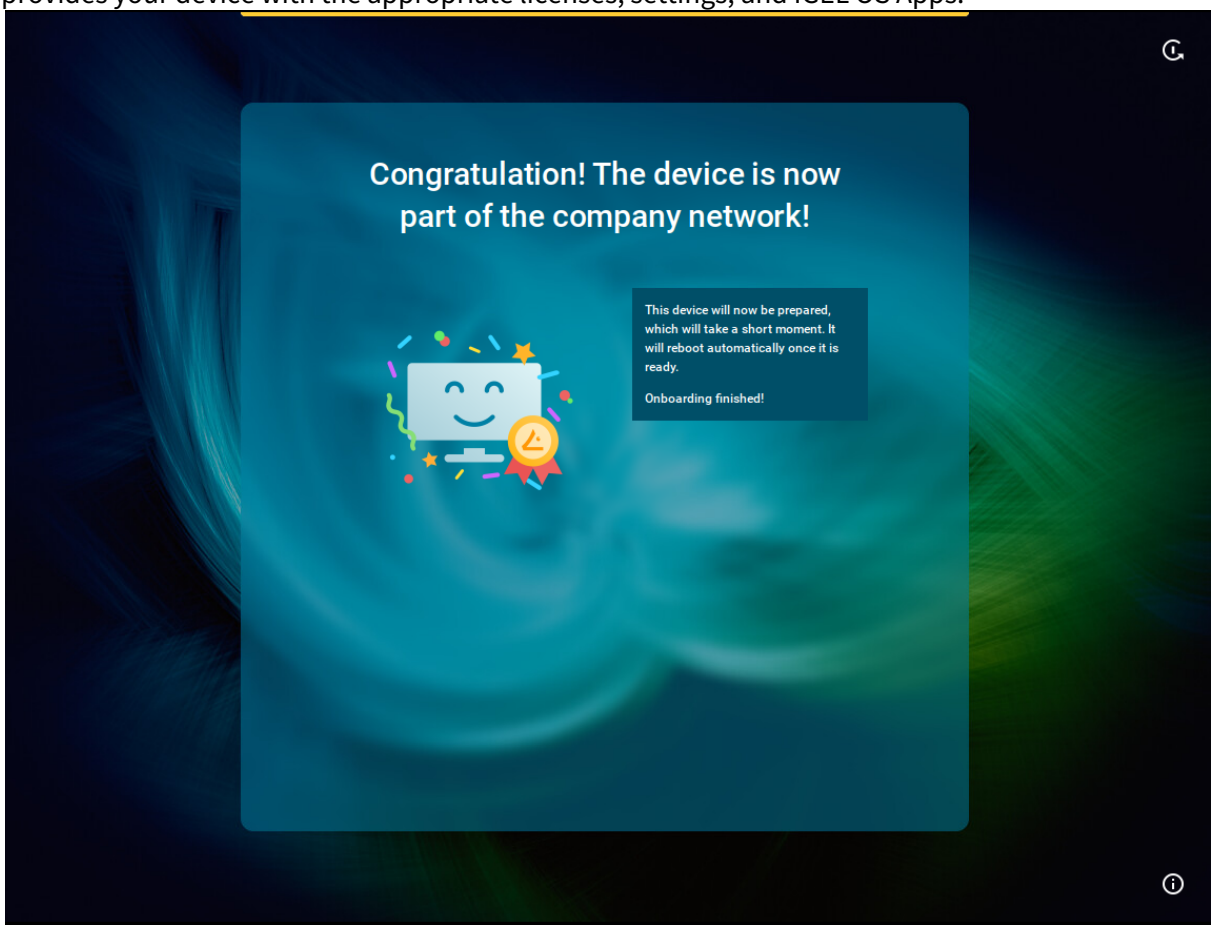


Alternatively, go to **UMS Web App > Network > UMS Server Details** and copy **Root Cert. Fingerprint - Part 3**.



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.



Troubleshooting: Configuring a Network during the Onboarding

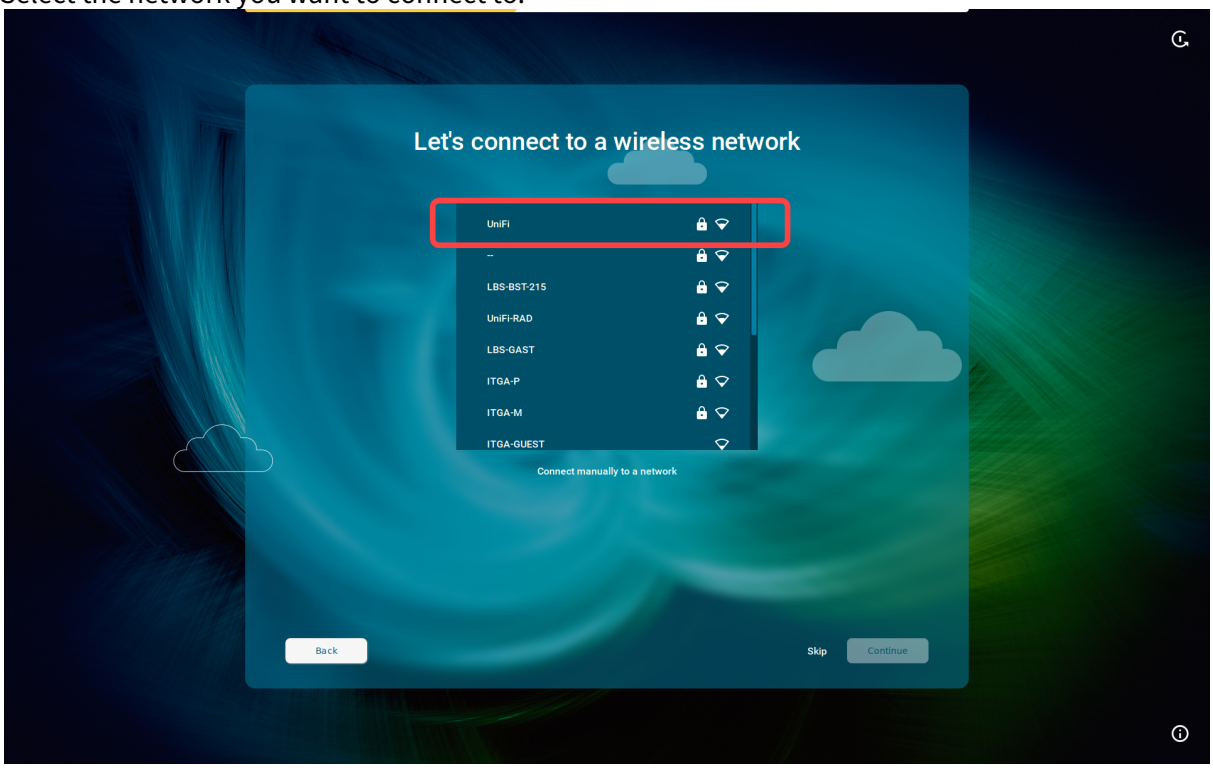
If your device cannot connect to the network instantly, the IGEL Setup Assistant will ask you to configure your network connection.

Connecting to a Wireless Network That Is Visible

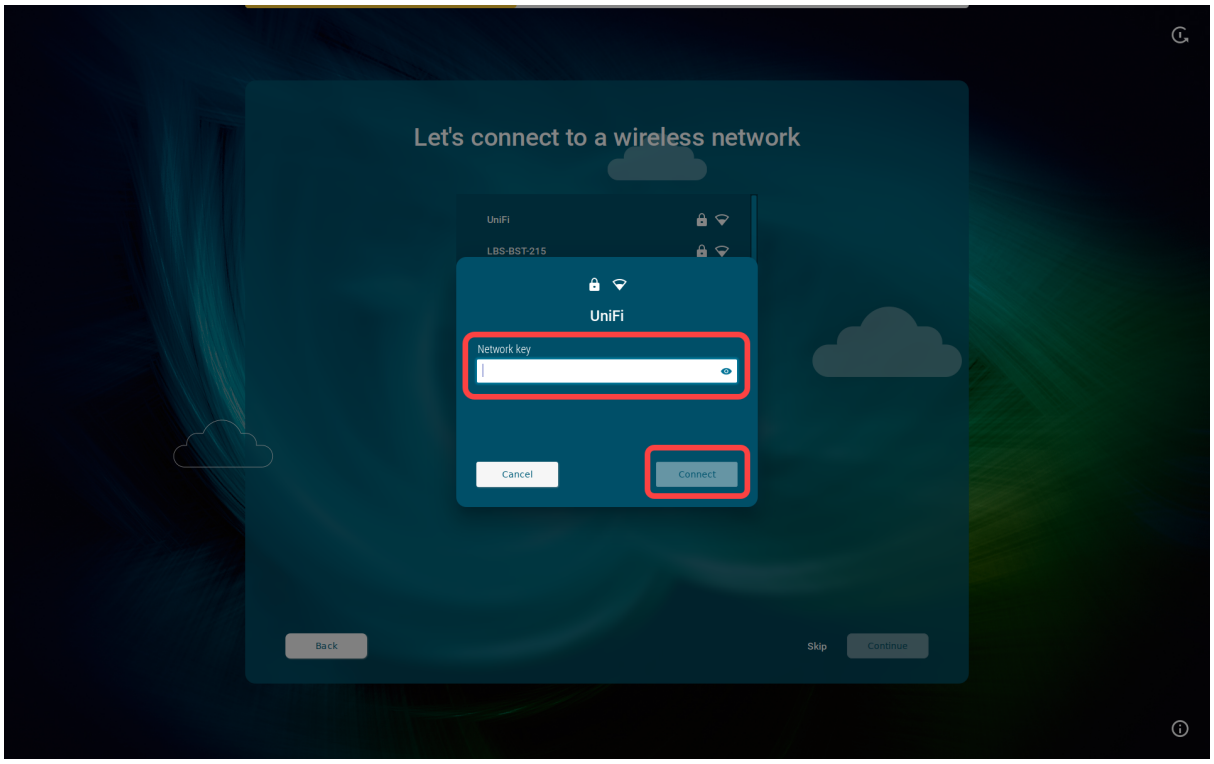
> Wi-Fi networks with certificates are not supported in the Setup Assistant.

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.



2. Enter the authentication data that are required by your network, e.g. **Network key** or **Password** and **Username**.



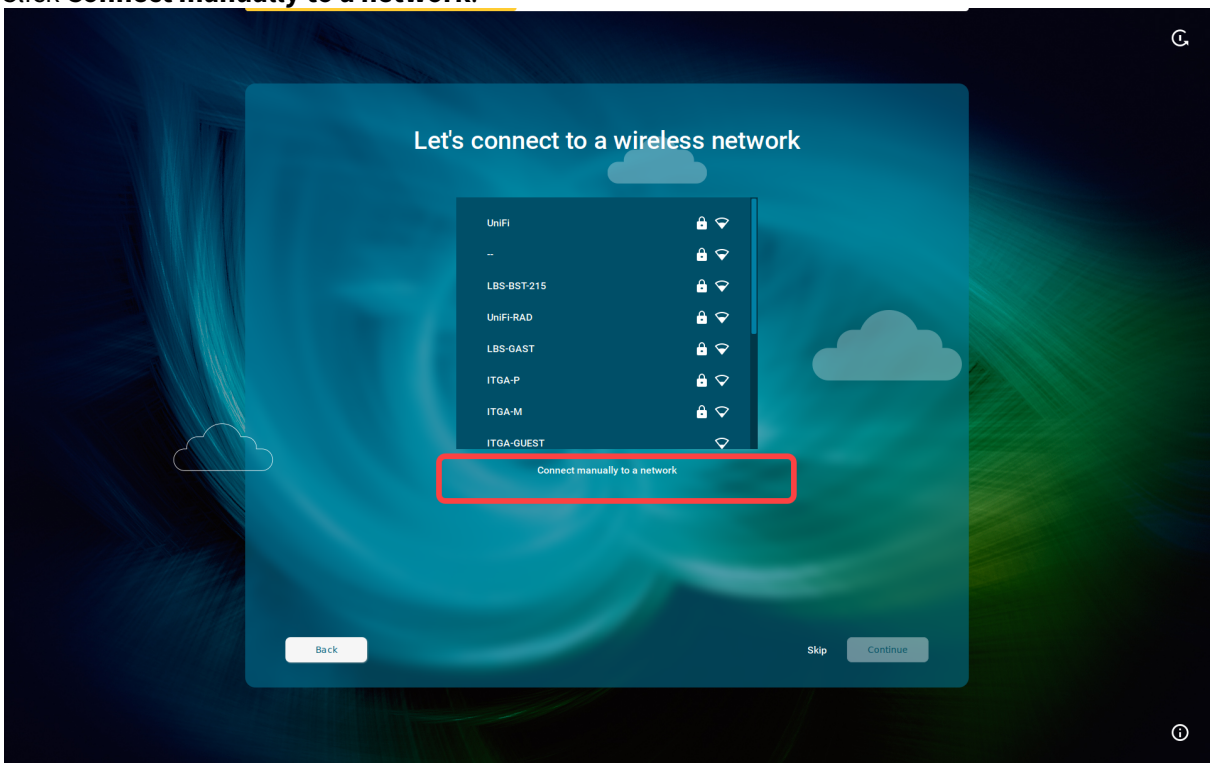
3. Click **Connect**.

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.

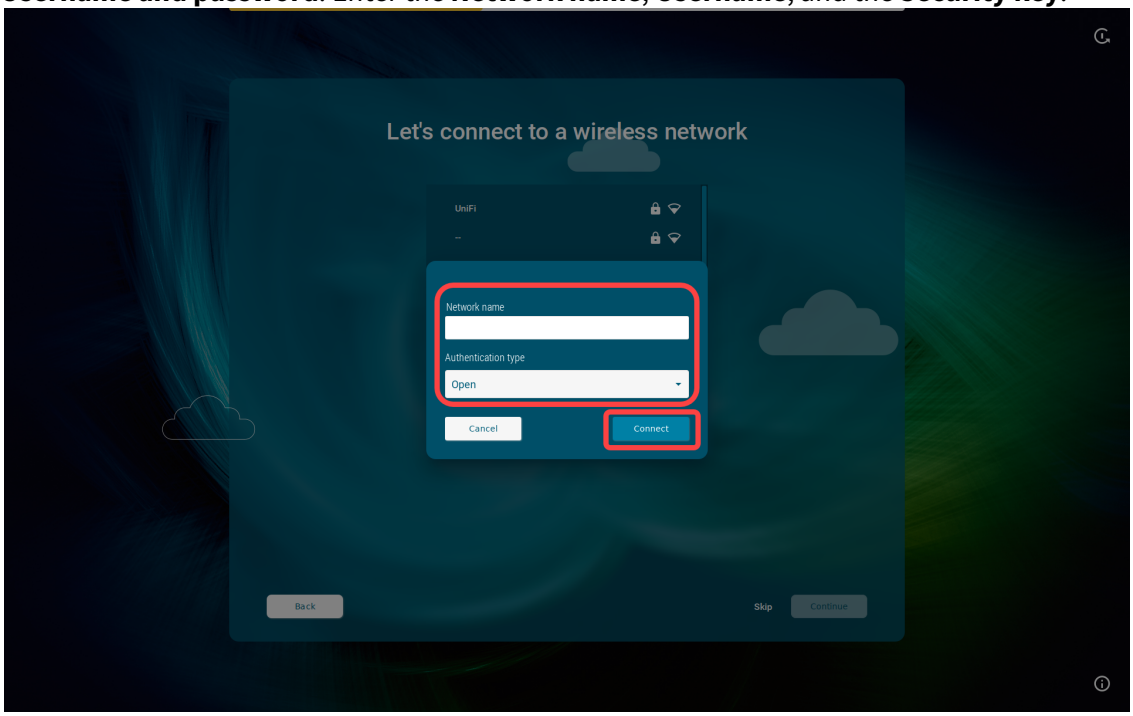
Connecting to a Wireless Network That Is Hidden

1. Click **Connect manually to a network**.



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**.

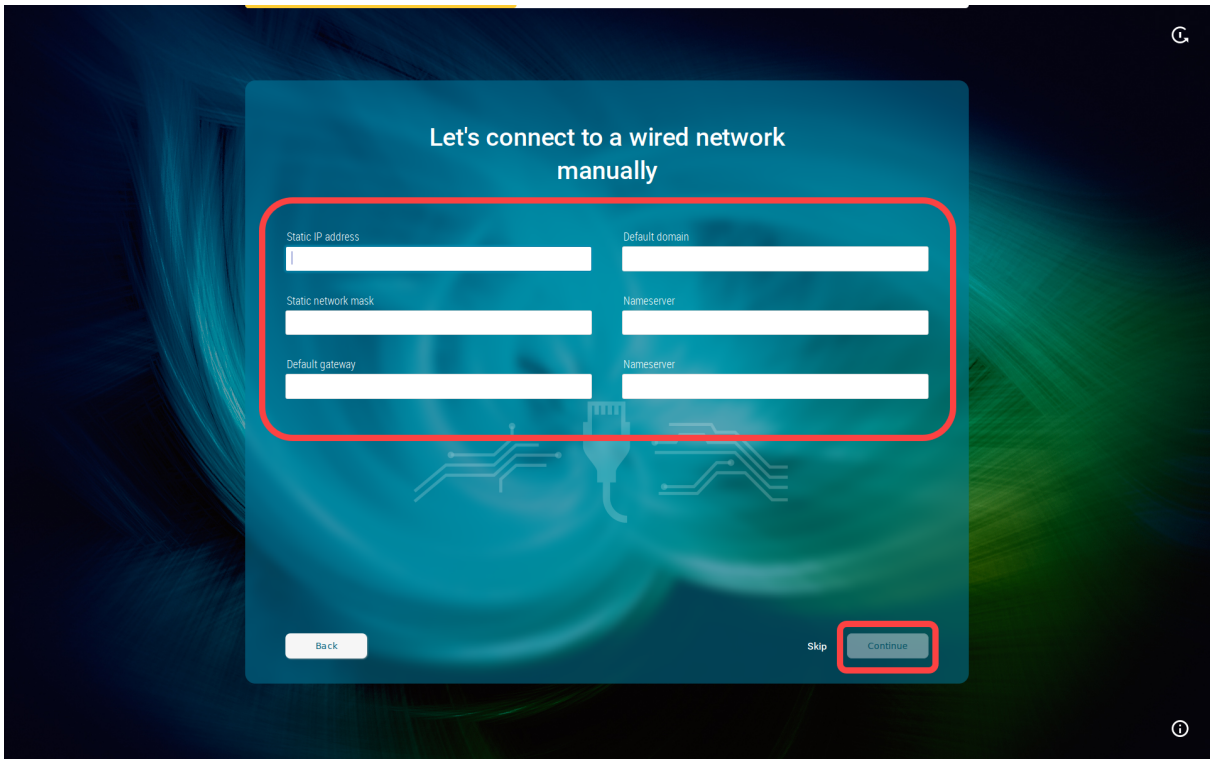


3. Click **Connect**.

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



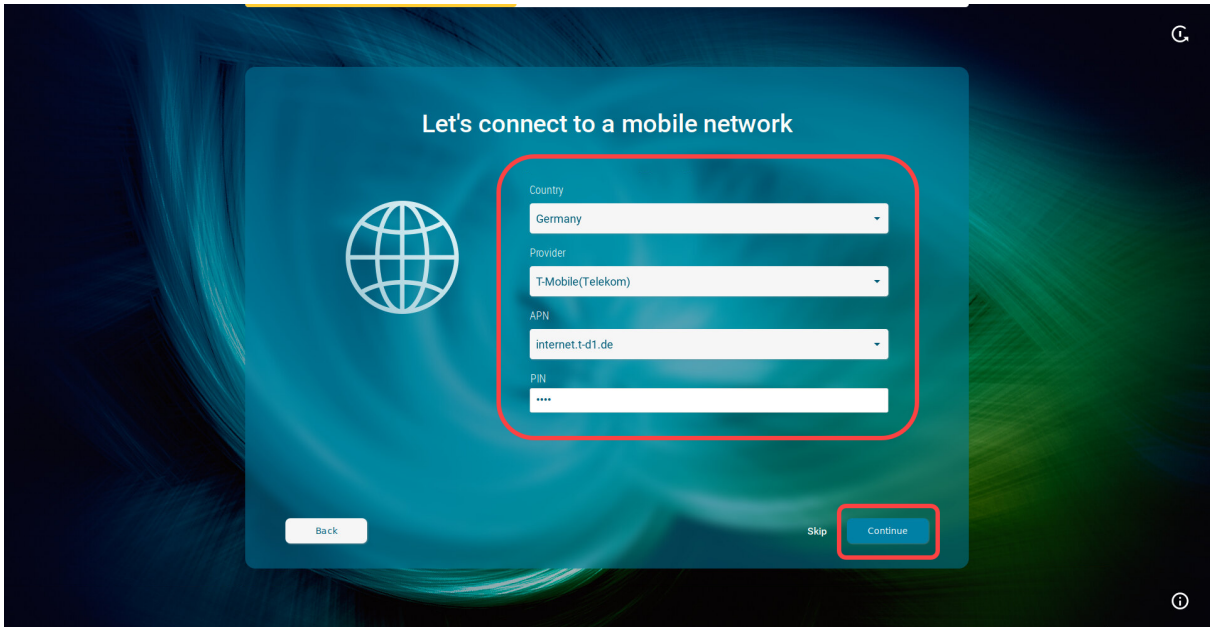
2. Click **Continue**.

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: The country of your provider
   Provider: Provider (the possible options depend on what you choose for **Country**)
   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**.



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 182).

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 217) 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.

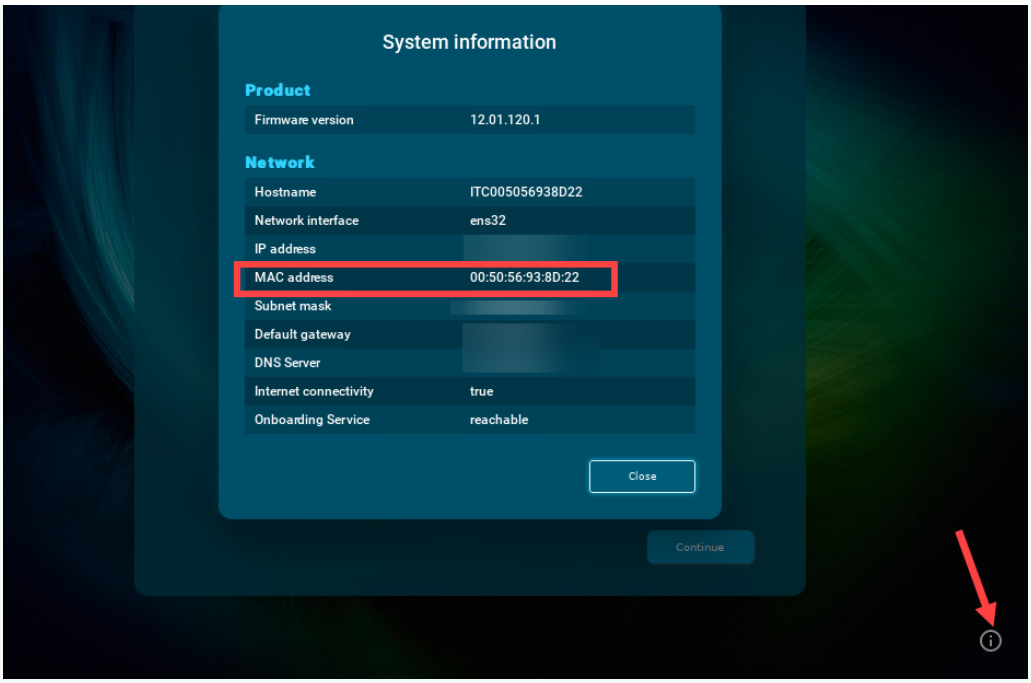
Solution

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).

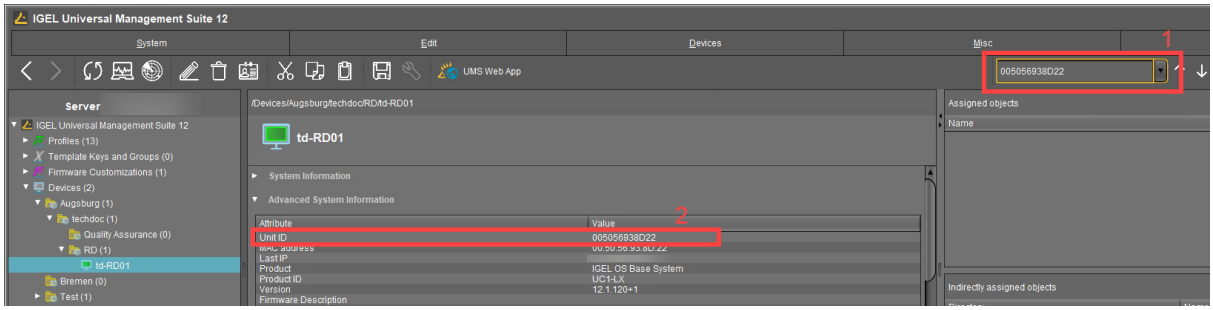
     Tip
     Alternatively, you can simply open the information dialog in the IGEL Setup Assistant and note the **MAC address** of the device and search for it in the UMS Console as described below:



2. Execute the following command:
   `echo $(get_unit_id)`

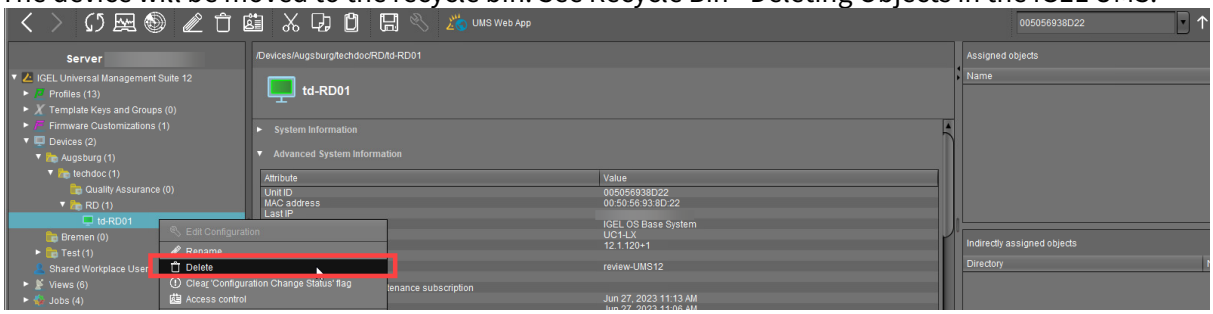
   This returns the Unit ID of the device:

3. Enter the Unit ID in the **Search** field, press `[Enter]` and validate that the located device has the correct Unit ID.

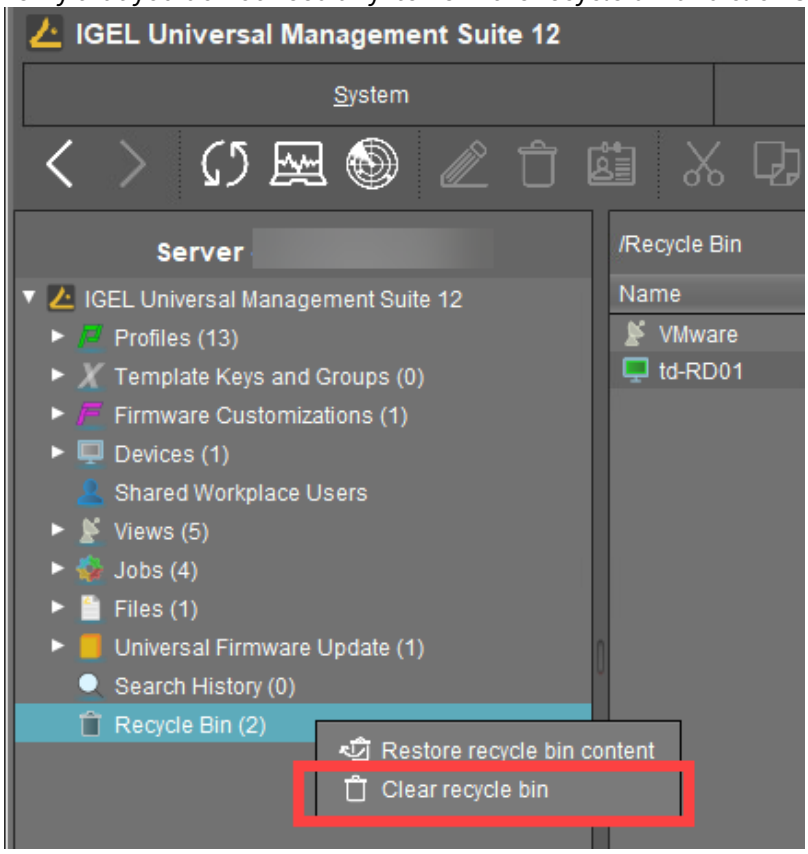


   If the device does not show up when running this search, skip the next step and go to the **Recycle Bin**.

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.



5. Verify that you do not need any items in the recycle bin and click **Clear recycle bin**.



   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.

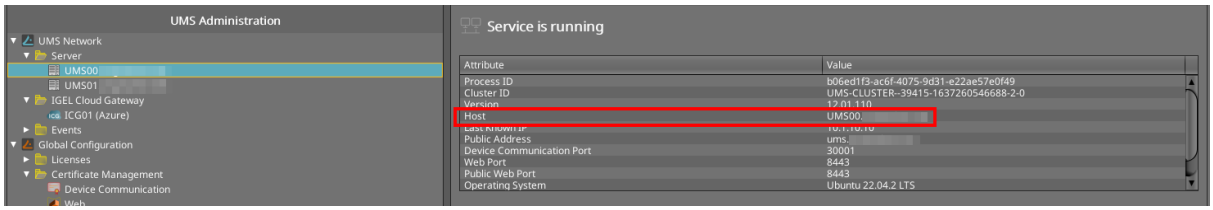
Please pay attention that hostnames should be spelled everywhere the same way (case-sensitive). The UMS hostname specified during the configuration of the IGEL Onboarding Service(see page 41) must be written exactly as in the UMS.

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:

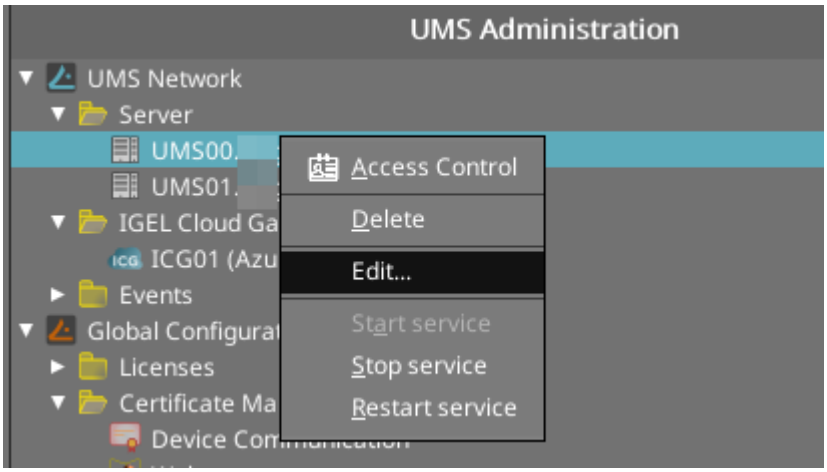
1. To identify and check your UMS hostname, go to **UMS Console > UMS Administration > UMS Network > Server** and select each server to view their details.



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).

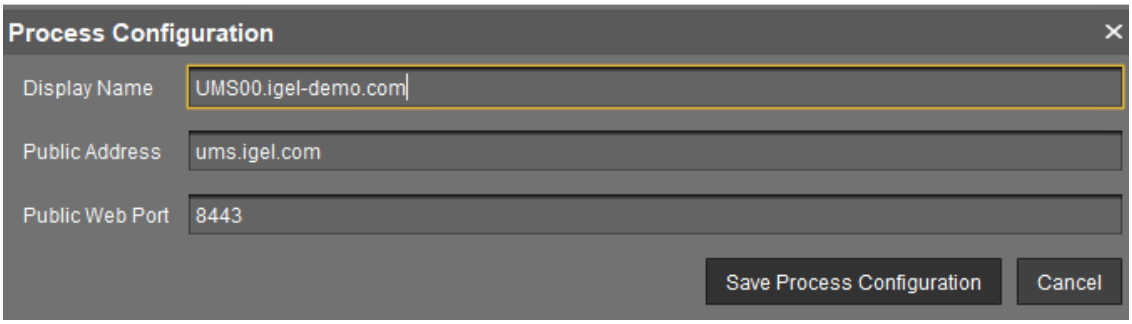
     OR

   - 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.



4. Restart the UMS Server service. For details on how you can do it, see IGEL UMS HA Services and Processes.

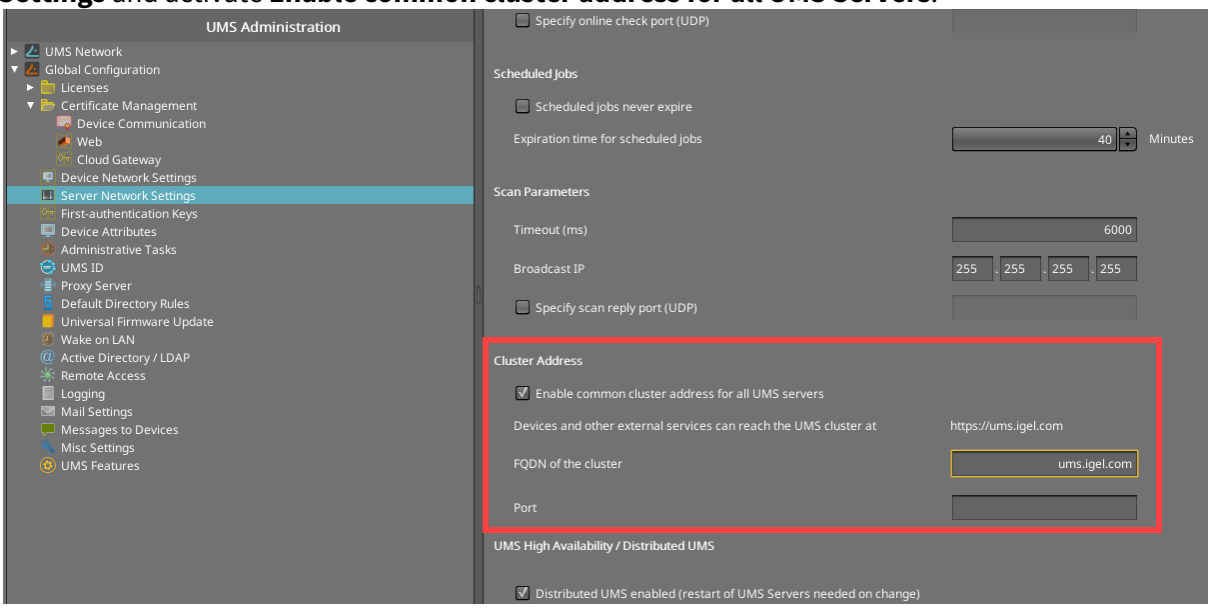
5. Validate that you can resolve the **Display Name** or **Public Address** of the UMS Server(s) from your IGEL OS devices.

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**.



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**.

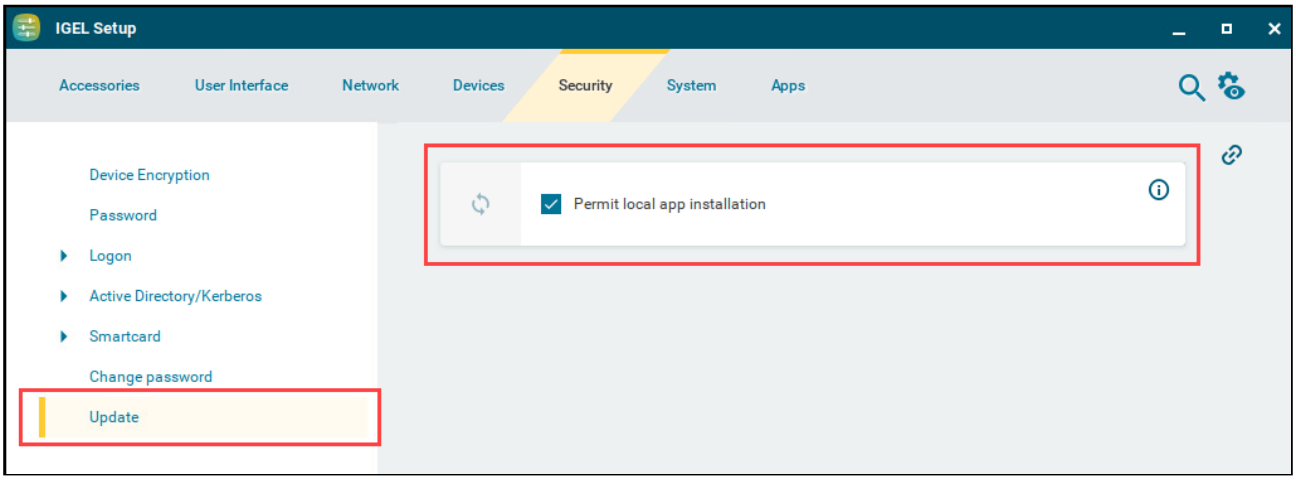
5. Save the settings.

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.

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**:



Starting methods for the App Portal can be defined under **Accessories > App Portal**.

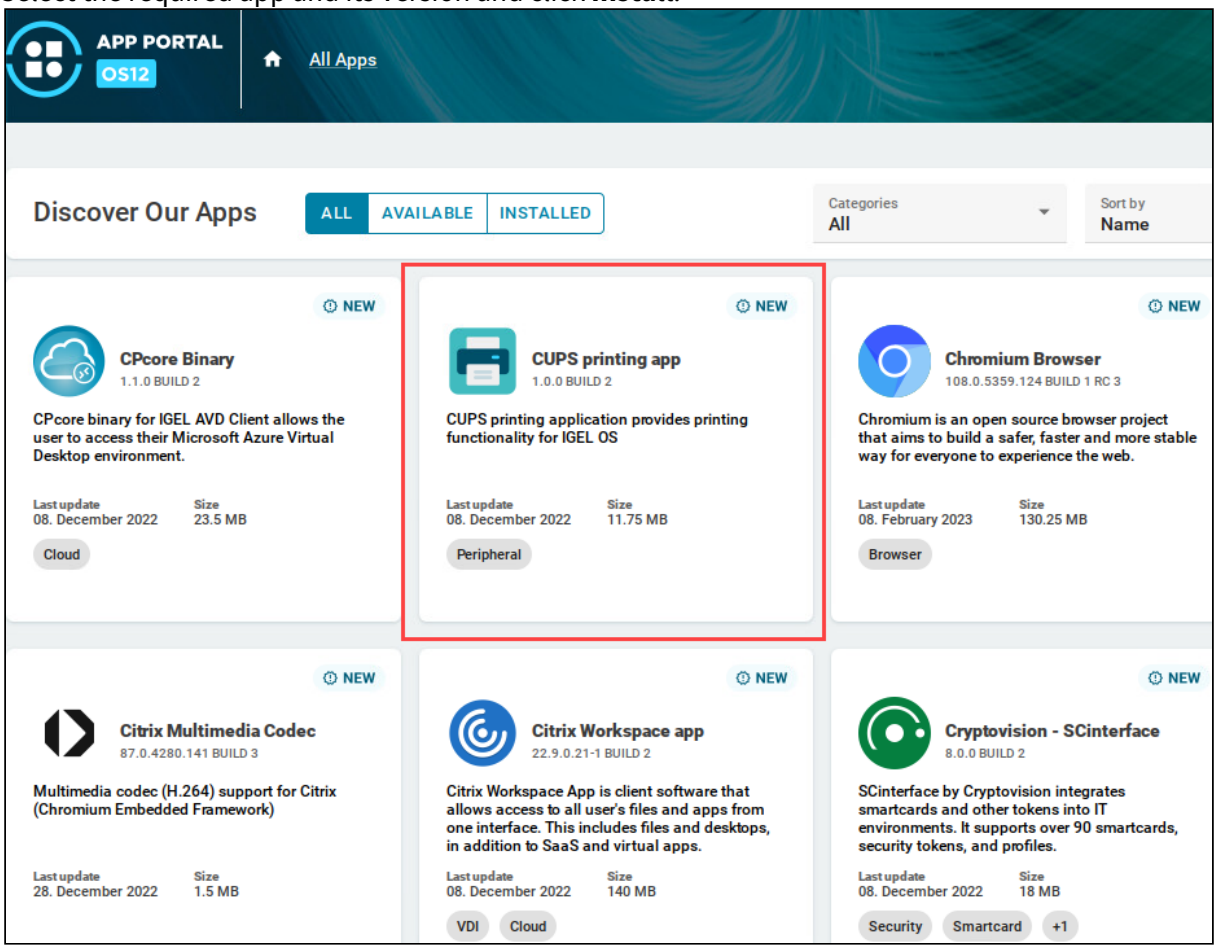
Access to the local App Portal and the download of apps is possible for UMS-managed devices if the UMS is registered in the IGEL Customer Portal. For the instructions, see Registering the UMS(see page 36).
If the device is not managed with the UMS, access to the local App Portal is possible but NOT for the devices with a Starter license. For more information on licenses, see Licensing(see page 151).

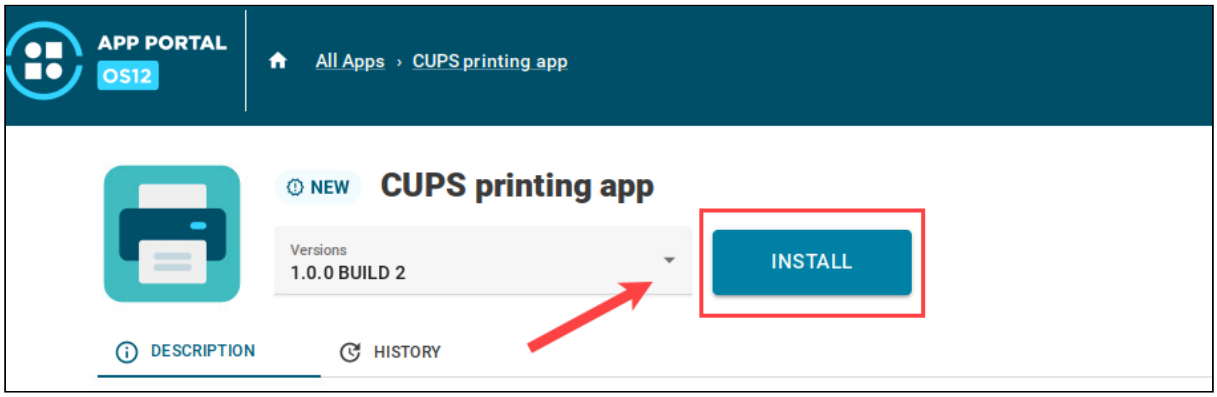
How to Locally Install Apps

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**.



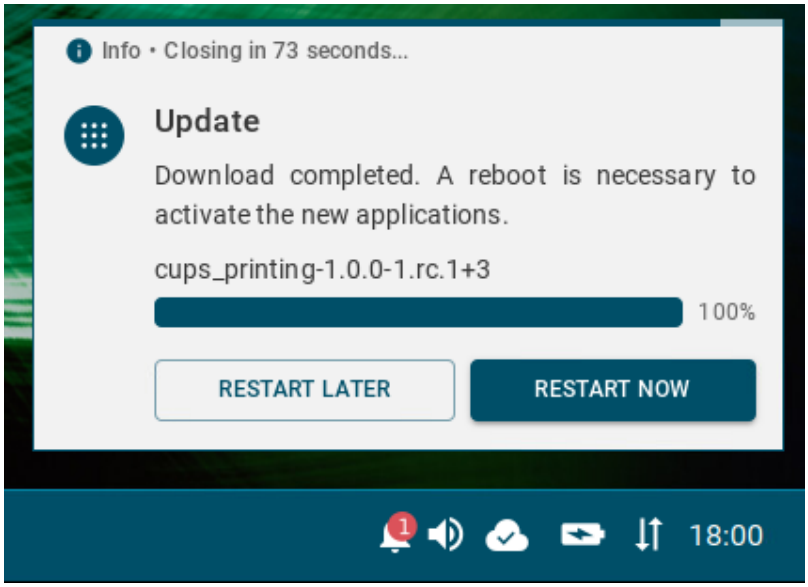


If the selected app / app version has already been installed, the **Uninstall** icon is shown.

3. Accept the End User License Agreement (EULA).

   The selected app version will be downloaded to the device. The corresponding notification will be

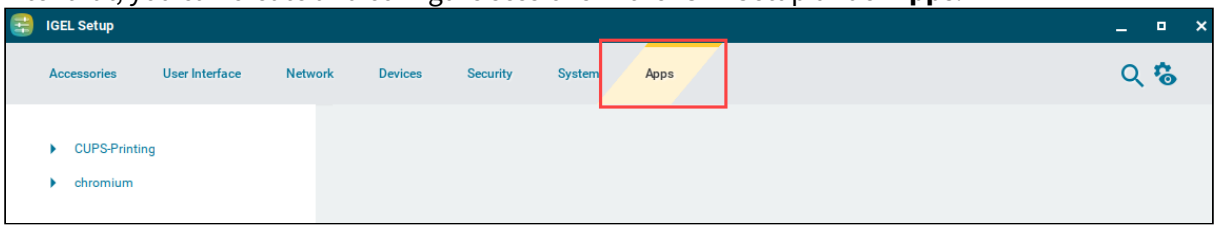
shown:



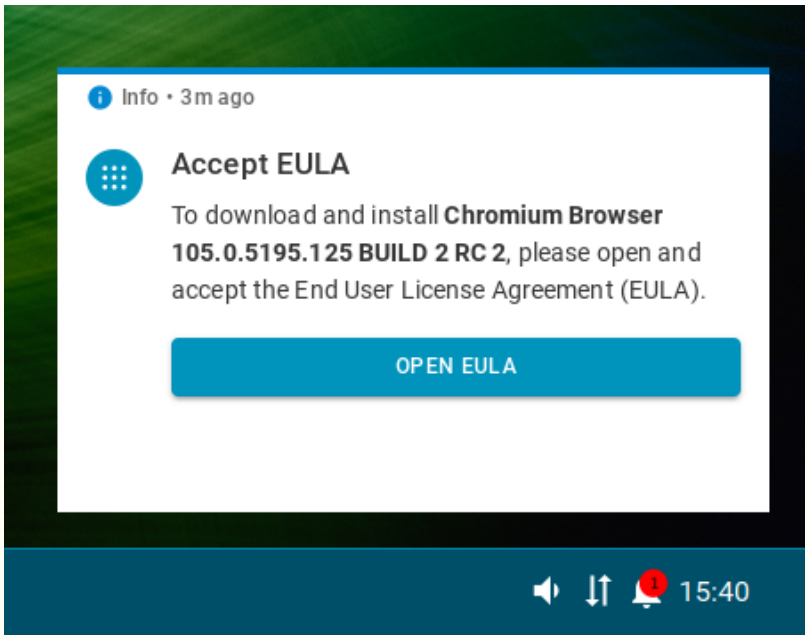
Dependant apps and codecs (e.g. Chromium Multimedia Codec, Fluendo libva for Chromium, Citrix Multimedia Codec) are automatically installed on the device during the installation of the main app (e.g. Chromium Browser app, Citrix Workspace app).

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):

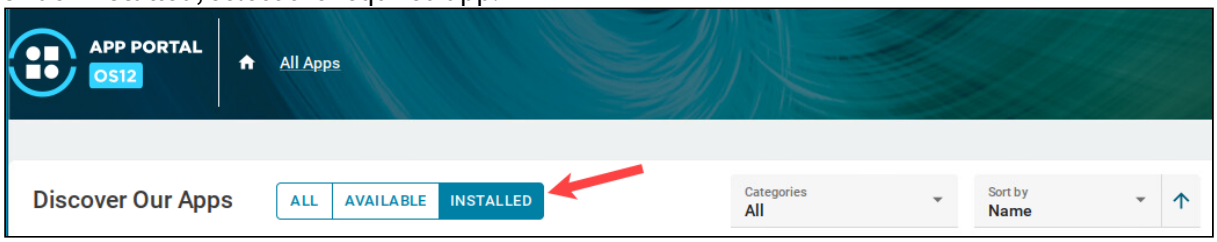


How to Locally Uninstall Apps

To uninstall apps on the device, proceed as follows:

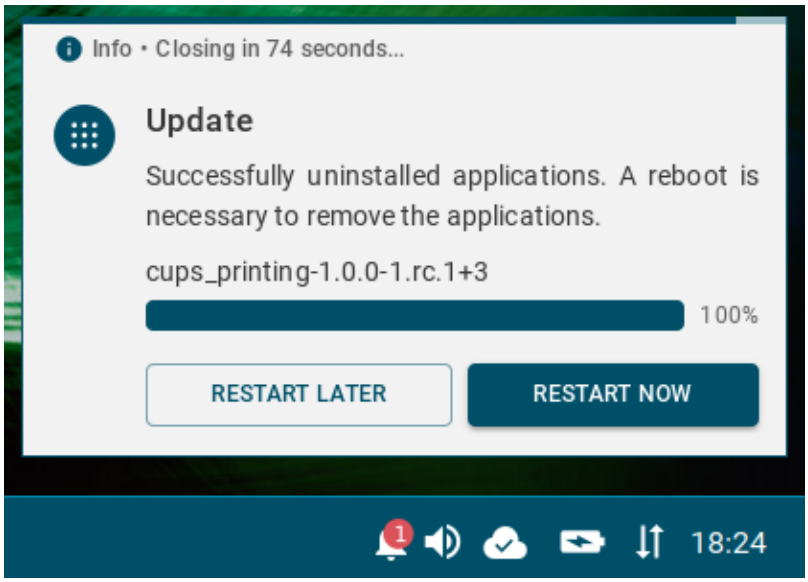
1. Open the App Portal locally on the device.

2. Under **Installed**, select the required app.



3. Click **Uninstall**.

   The user will receive a corresponding notification:



4. Restart the device to complete the app uninstallation.

Configuring Single Sign-On (SSO)

With IGEL OS 12, you can use Single Sign-On (SSO) via a cloud-based identity provider (IdP) to access the local device and apps.

The following identity providers are supported:

- Okta (https://www.okta.com/)
- Microsoft Azure AD

Generally, you can edit the IGEL OS 12 device configuration as follows:

- via the IGEL UMS Web App:
  - **Configuration > Create new profile**  (You select one or several apps which will be configured by the profile. If the IGEL OS base system app is selected, all other apps are shown under the tab "Apps"; if not, each app is displayed as a separate tab)
  - **Apps > [name of the app] > Create new profile** (used to quickly configure a profile for the selected app. It is also possible to add other apps which will be configured by this profile)
  - **Devices > [name of the device] > Edit Configuration** (shows all installed apps. Apps are displayed under the tab "Apps")
- via IGEL Setup locally on the device (shows all installed apps. Apps are displayed under the tab "Apps")

The best practice to configure your devices is via profiles. For details on how to create profiles, see Creating a Profile(see page 113).

Apps and Utilities for IGEL OS 12 That Support SSO with Okta

- Web apps, e. g. Okta portal (SSO via Chromium)
- Device login
- Screenlock

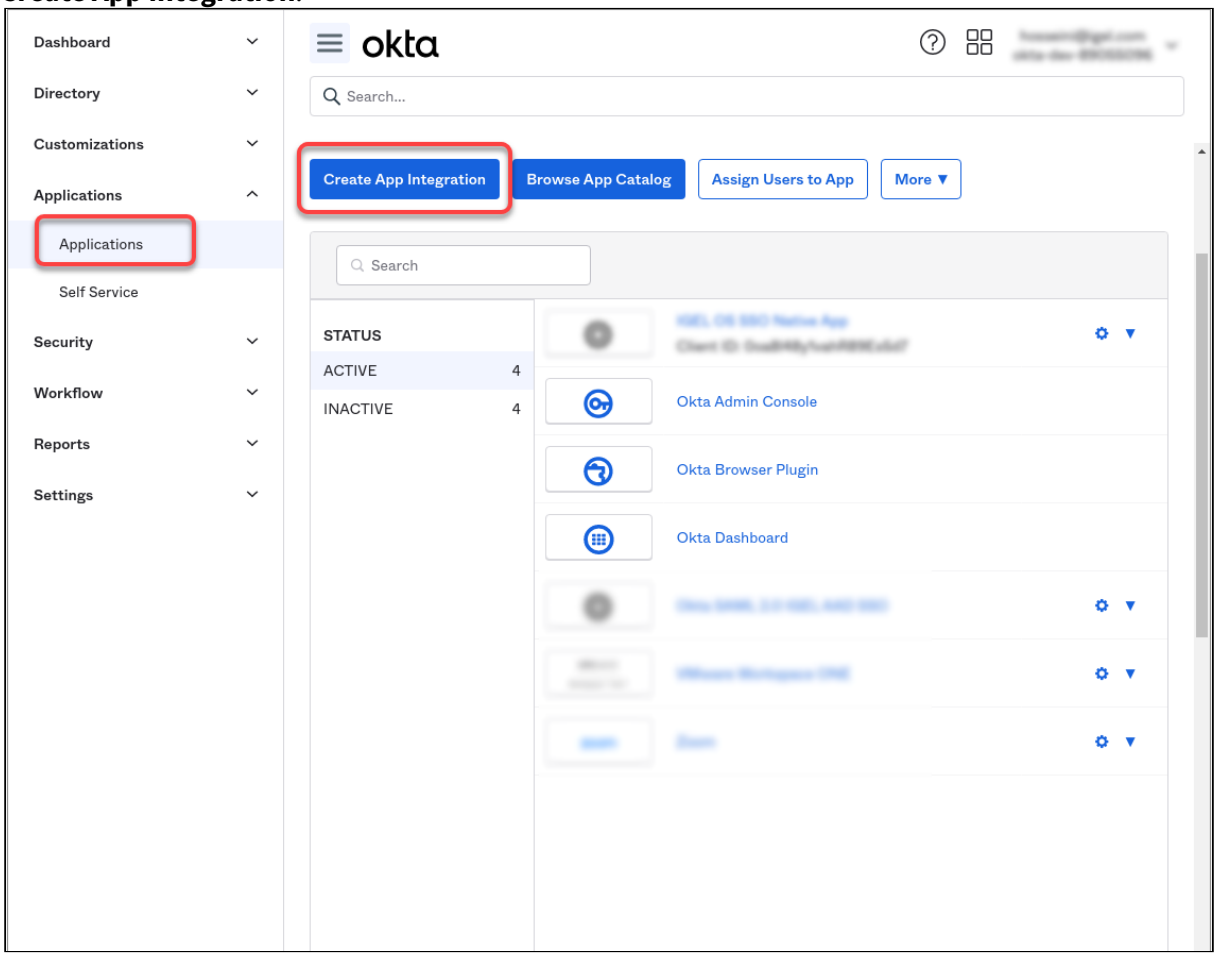
Apps and Utilities for IGEL OS 12 That Support SSO with Azure AD

- IGEL Azure Virtual Desktop Client (AVD)
- Zoom client (SSO via Chromium)
- Web apps, e. g. Office 365 (SSO via Chromium)
- Device login
- Screenlock

Configuring SSO with Okta

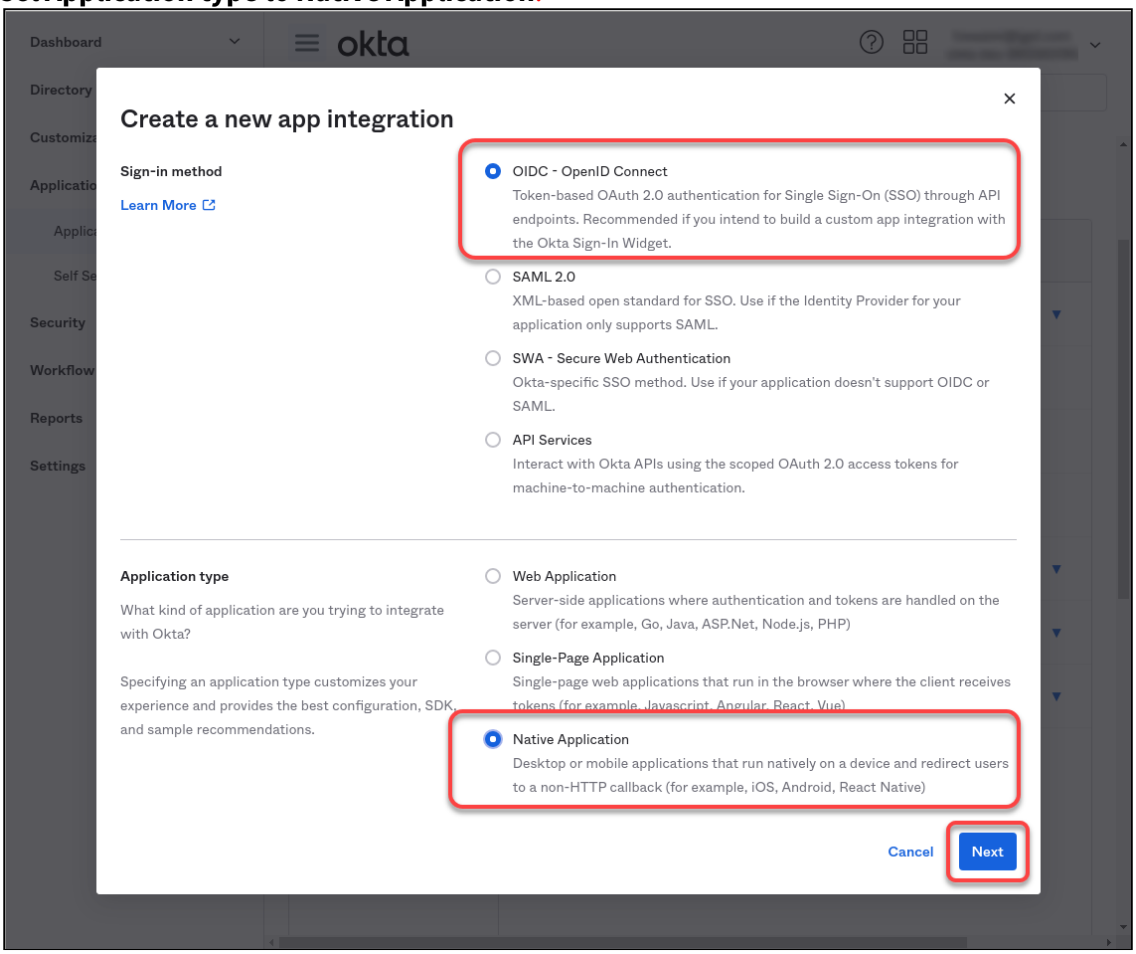
Registering an Application in Okta

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



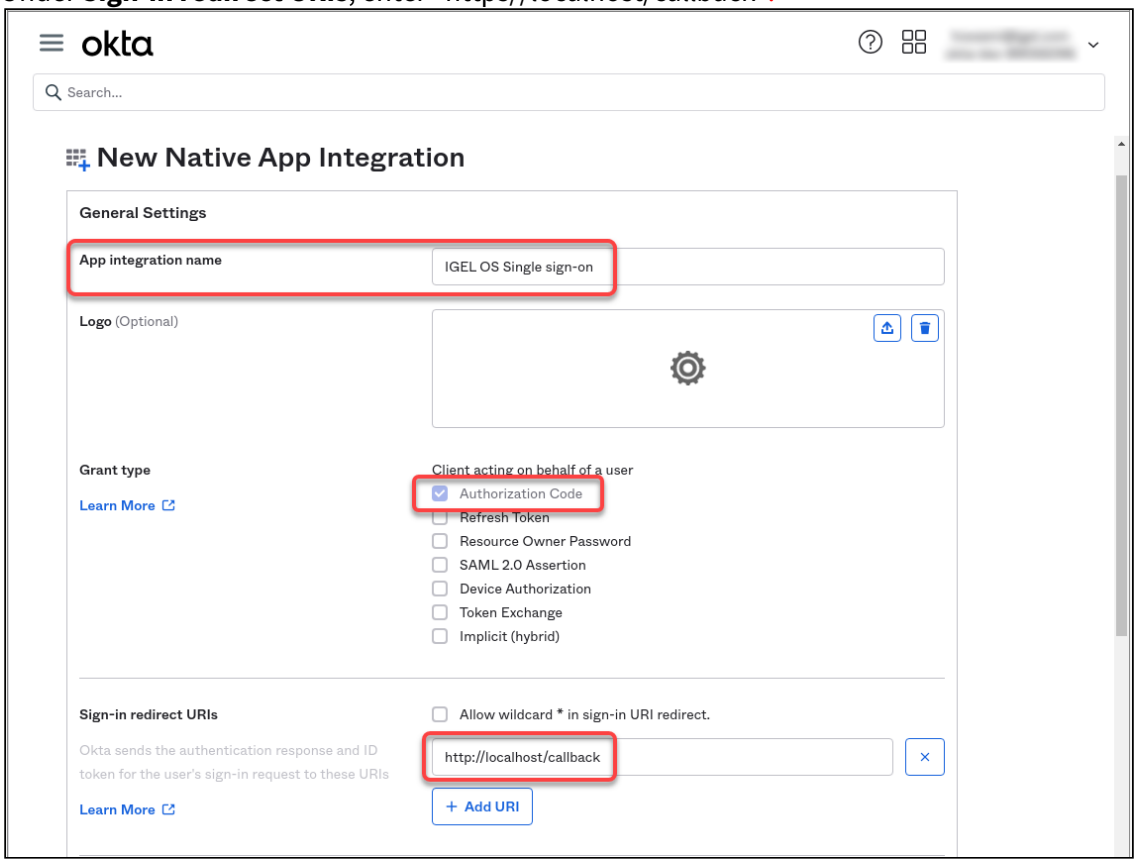
2. Edit the settings as follows and then click **Next**.
   - Set **Sign-in method** to **OIDC - OpenID Connect**.

- Set **Application type** to **Native Application**.



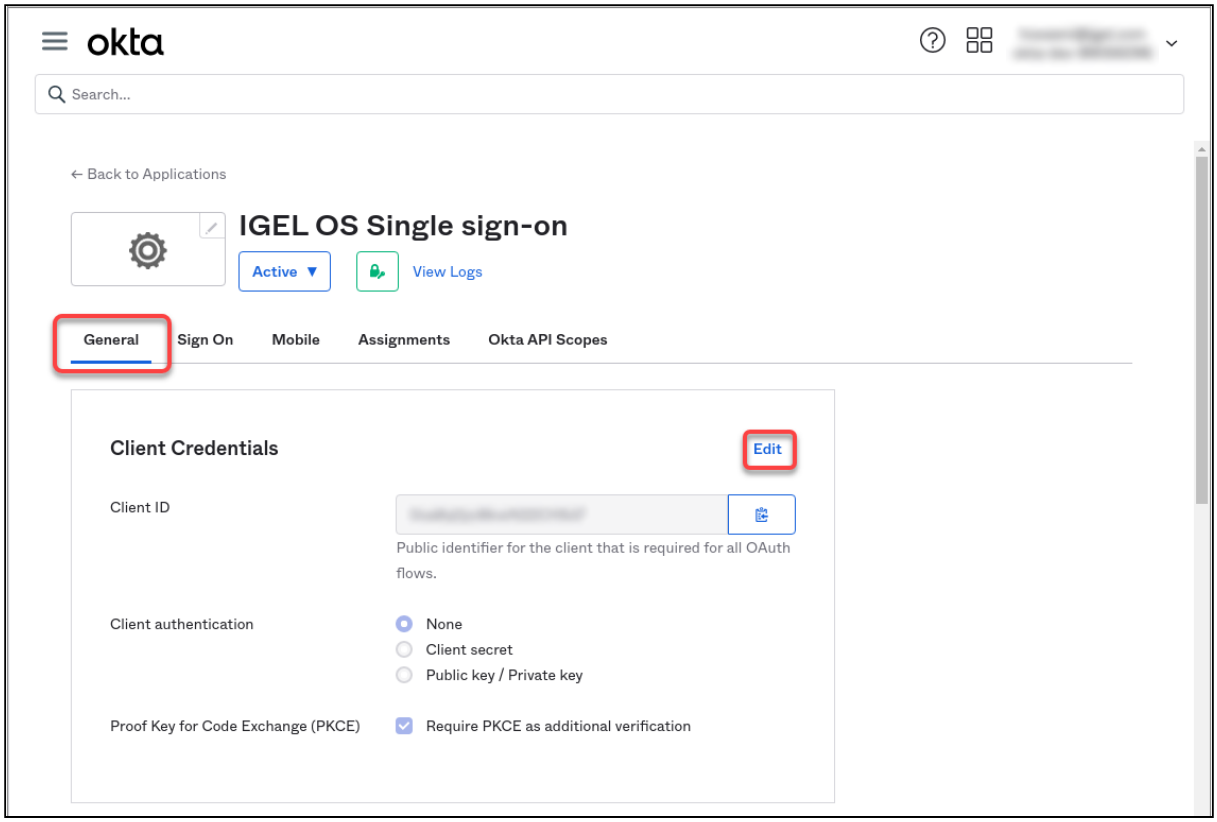
3. Edit the settings as follows and then click **Save**.
   - Under **App integration name**, enter a name for your application, e.g. "IGEL OS Single sign-on".
   - Make sure that as the **Grant type**, the option **Authorization Code** is selected.

- Under **Sign-in redirect URIs**, enter "https//localhost/callback".

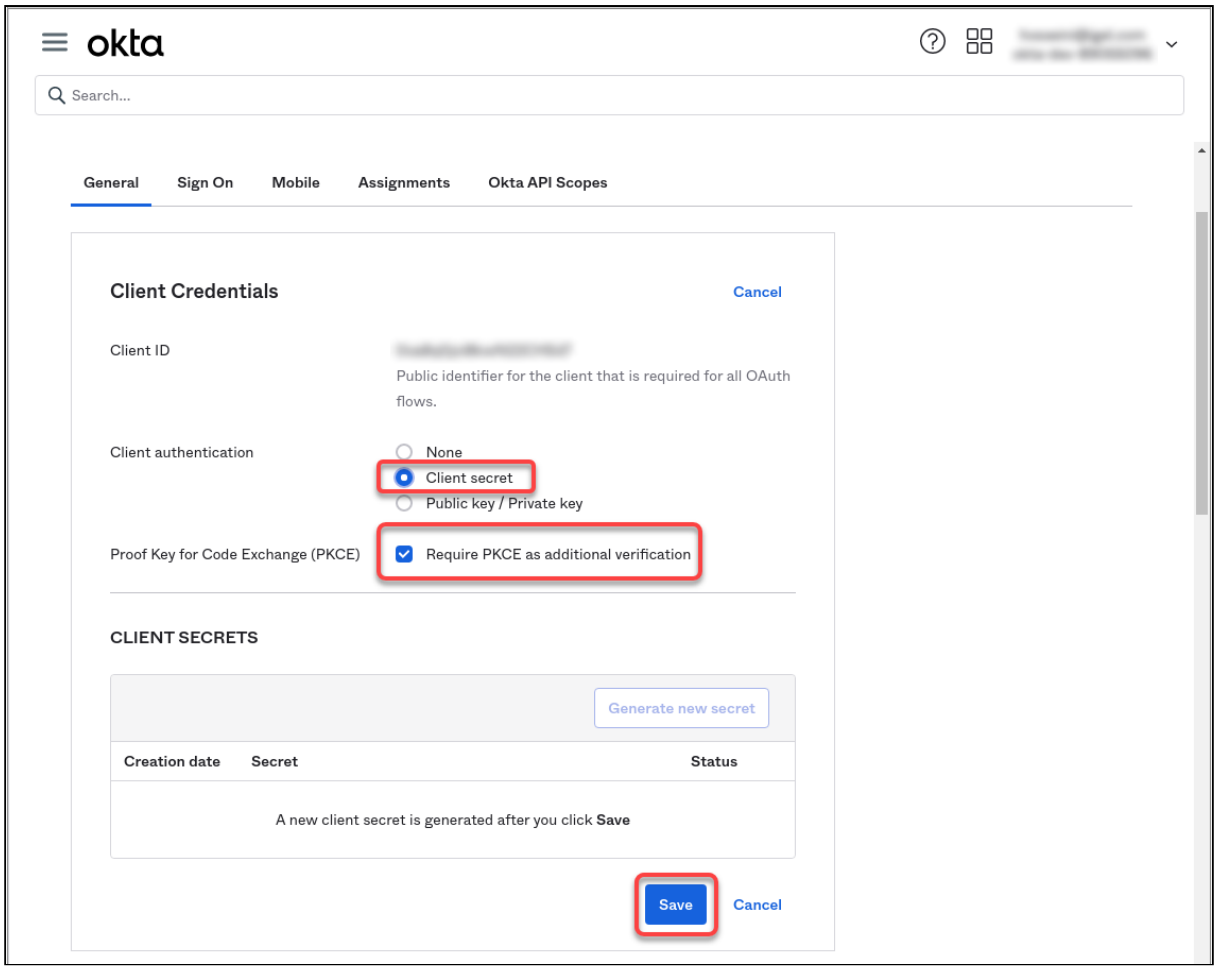


The app integration is created.

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

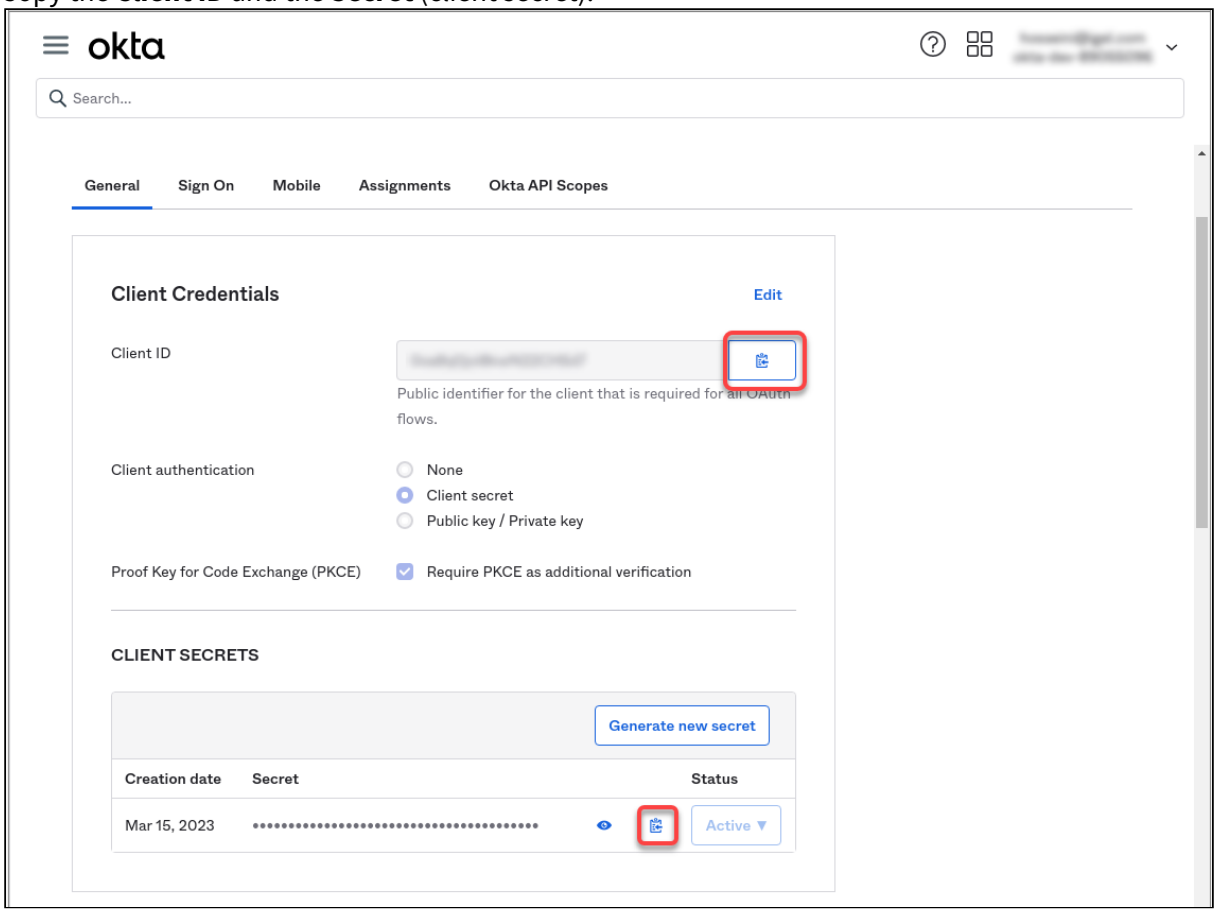


5. Under **Client authentication**, select **Client secret** and make sure that under **Proof Key for Code Exchange (PKCE)**, **Require PKCE as additional verification** is enabled. Afterward, click **Save**.



The client secret will be created.

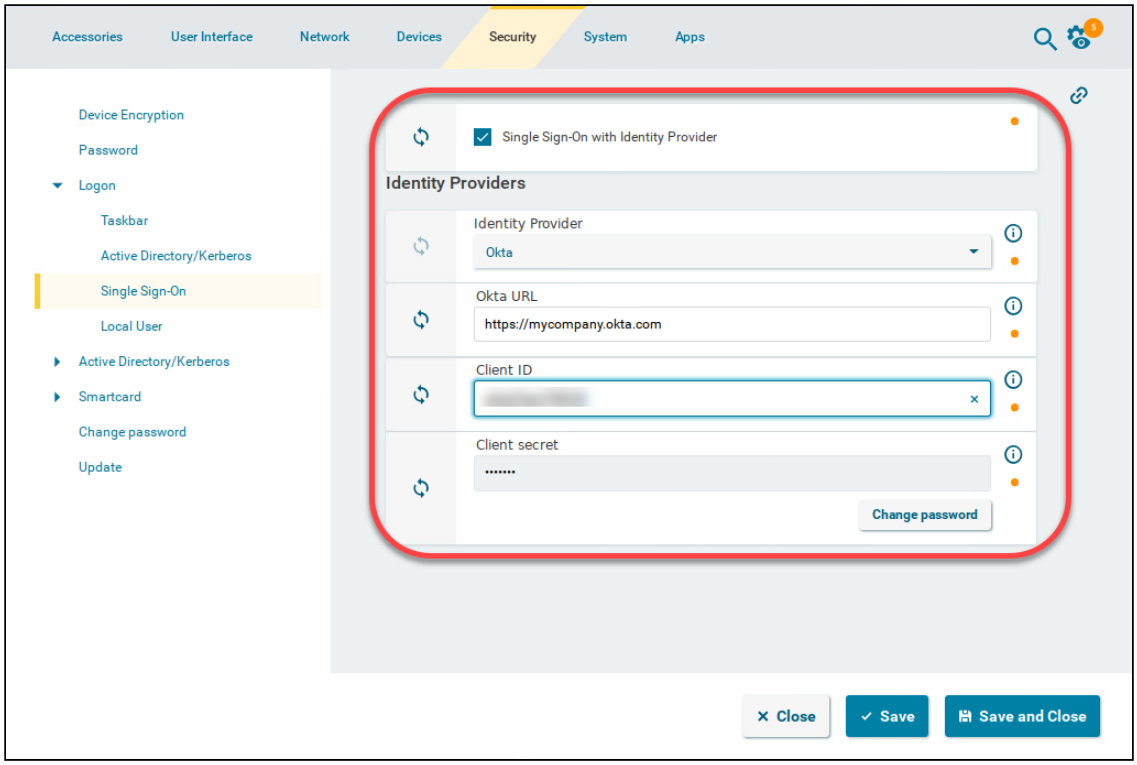
6. Copy the **Client ID** and the **Secret** (client secret).



Configuring IGEL OS for SSO with Okta

1. Go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **Okta**.
   - Provide the **Okta URL** for your user. This is the Okta organization URL. Example: "https://mycompany.okta.com"
   - Provide the **Client ID**. This is the client ID that was created in Okta.

- Provide the **Client secret**.



2. Click **Save** or **Save and close**.
   The desktop of the device is terminated after the profile is applied. The login screen is displayed. You can now use the apps and utilities for IGEL OS 12 that support SSO with Okta(see page 193).
   If you want to use multi-factor authentication, you can configure this in the Okta console. The available methods are Google Authenticator, E-Mail, and Okta Verify.

Setting up SSO with Azure AD

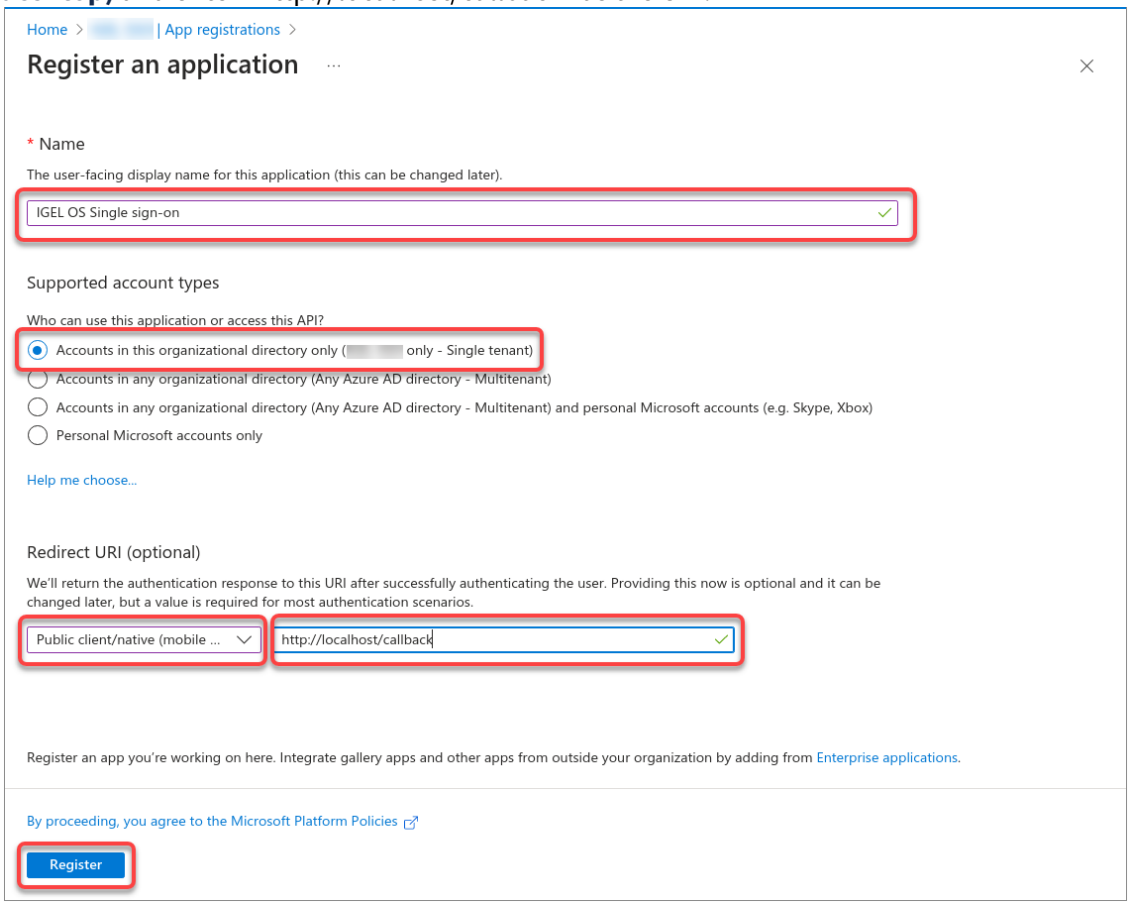
To enable SSO with Azure ID on IGEL OS 12 devices, an Azure application must be registered first. Then, you can configure IGEL OS 12 to use this application for authentication; the Azure application is referenced via its Public Client Identifier.

Registering an Azure Application

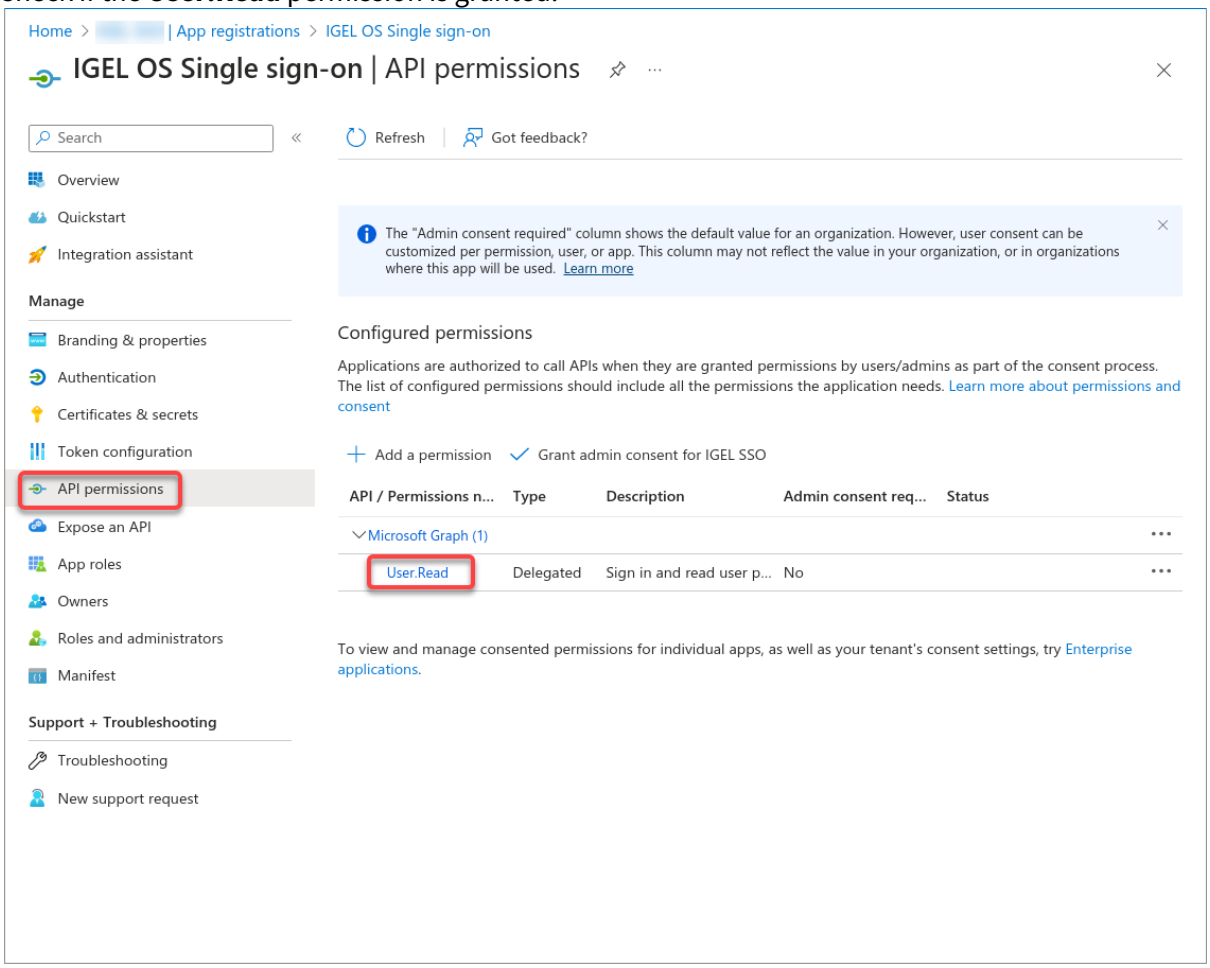
1. In your Azure AD Portal, go to **App registrations > New registration**.

2. Edit the data as follows and then click **Register**:
   - Add a proper name for the application. Note that this name will be visible to the user once during the consent process for granting permissions. In our example, "IGEL OS Single sign-on" is used as the name.
   - Select the option **Accounts in this organizational directory only ([name of your organization's AD Portal] only - Single tenant)**.

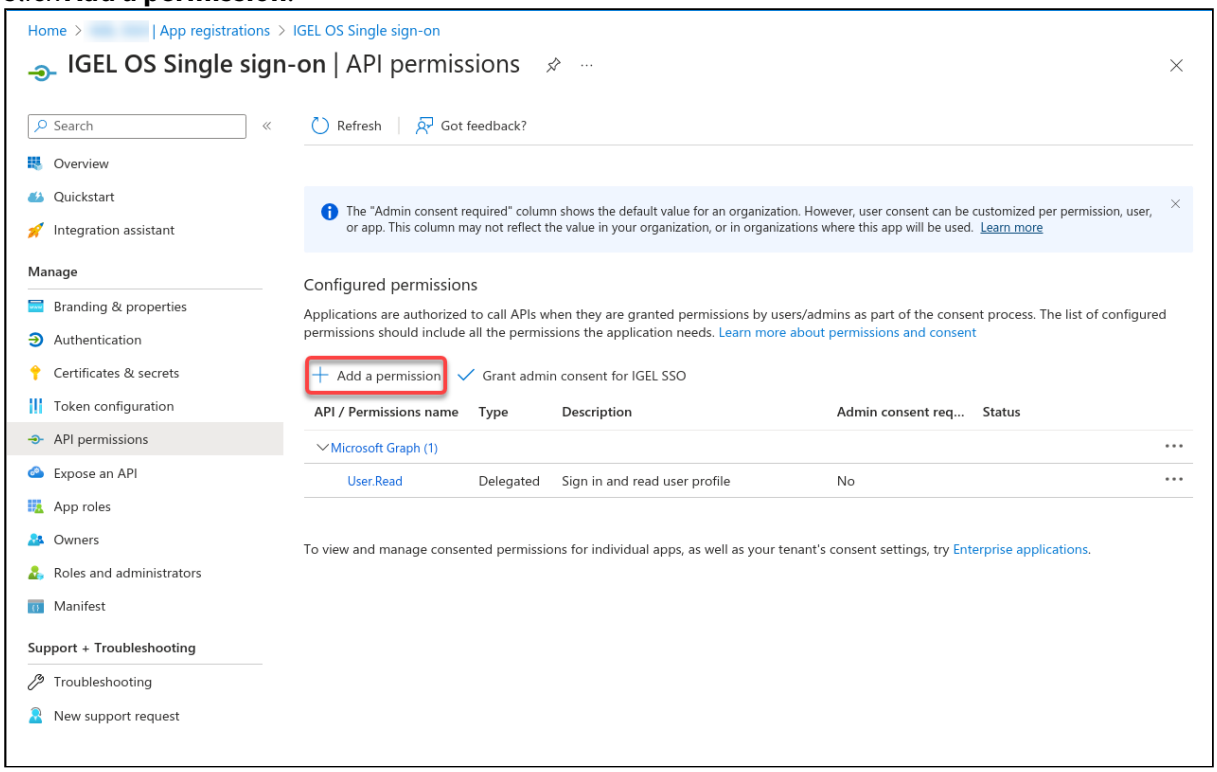
- Under **Redirect URI (optional)**, select the option **Public client/native (mobile & desktop)** and enter "http://localhost/callback" as the URI.



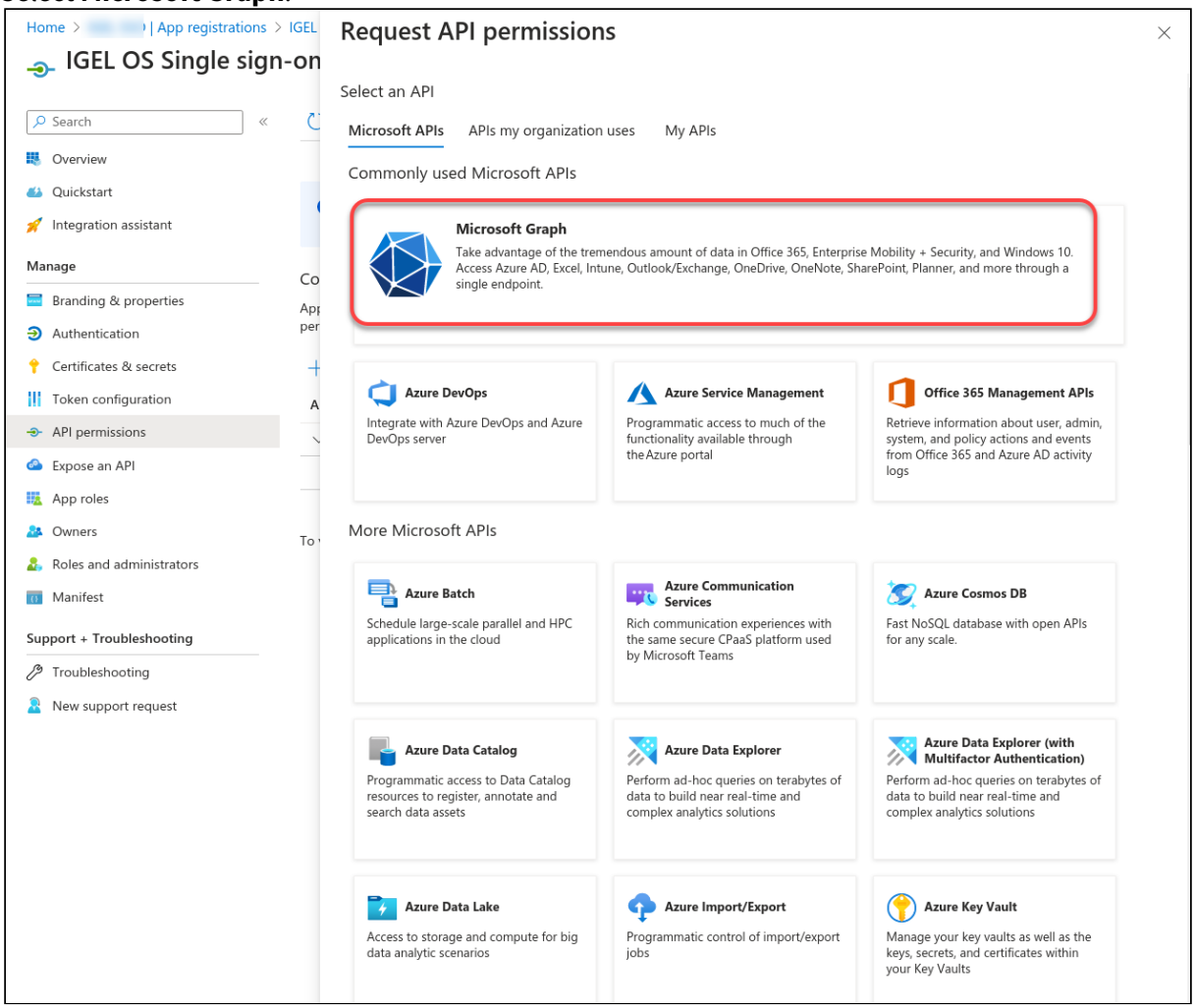
3. Check if the **User.Read** permission is granted.



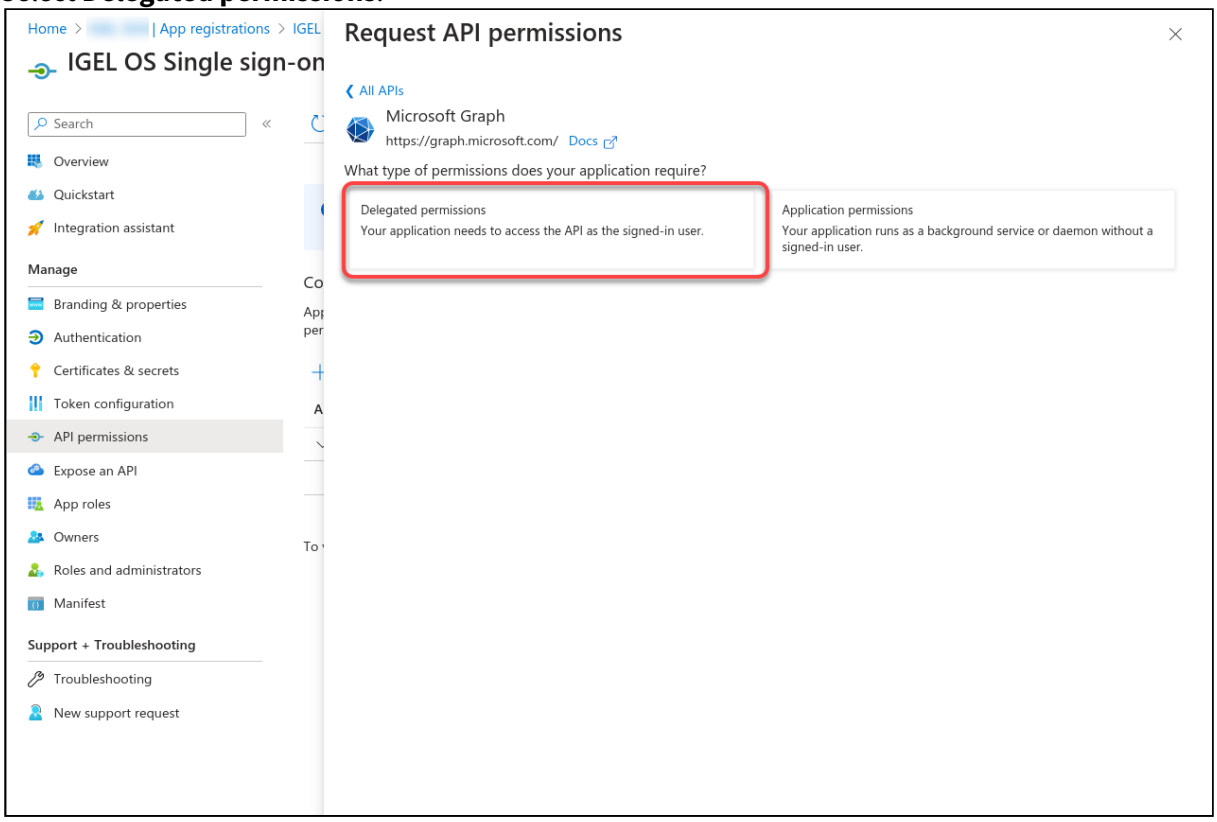
4. Click **Add a permission**.



5. Select **Microsoft Graph**.

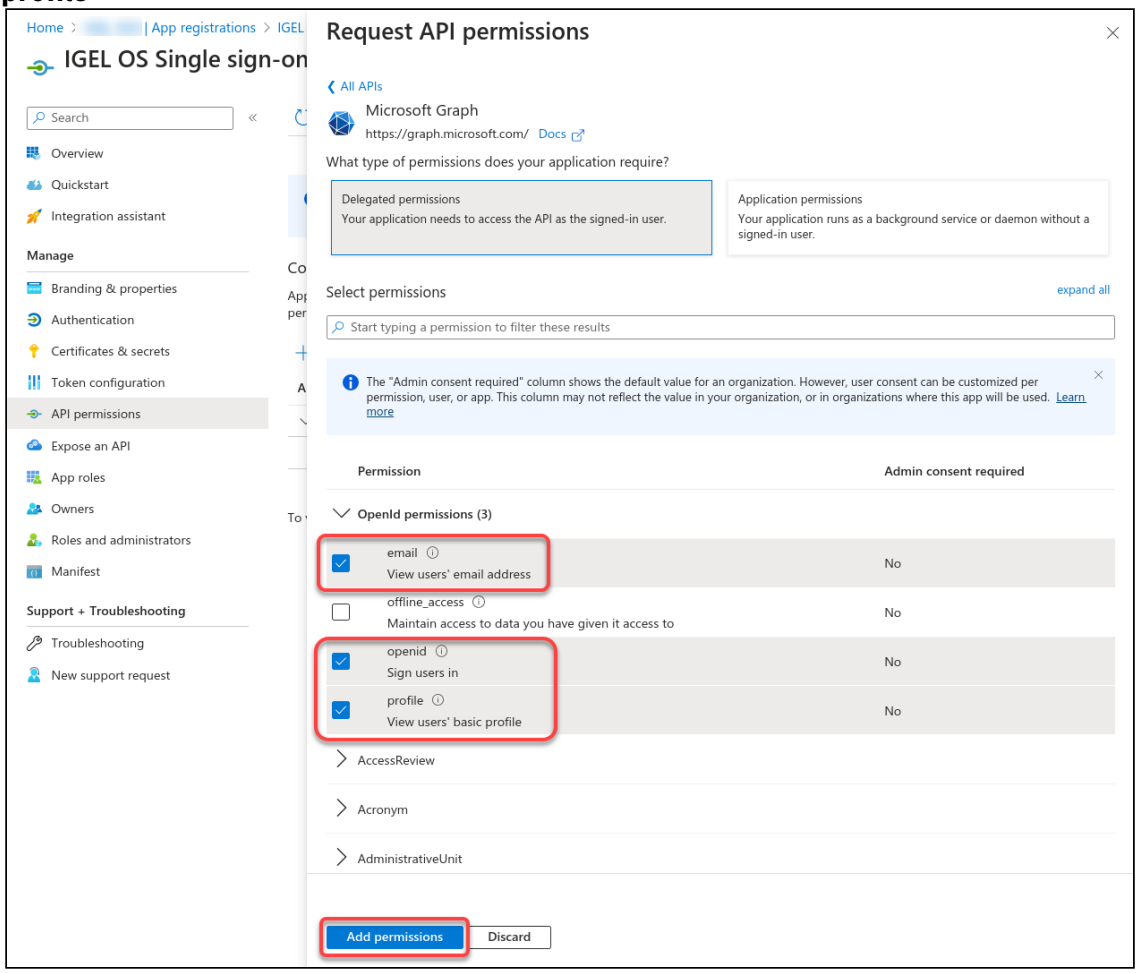


6. Select **Delegated permissions**.

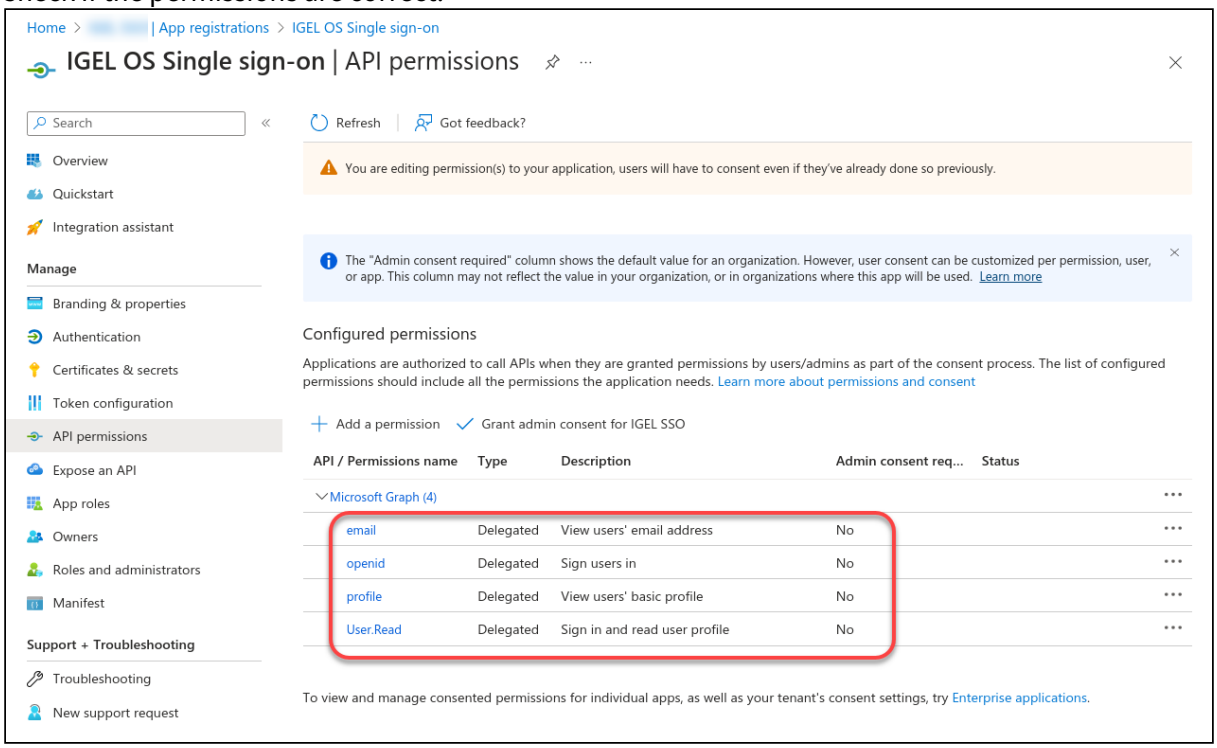


7. Enable the following permissions and then click **Add permissions**:
   - **email**
   - **openid**

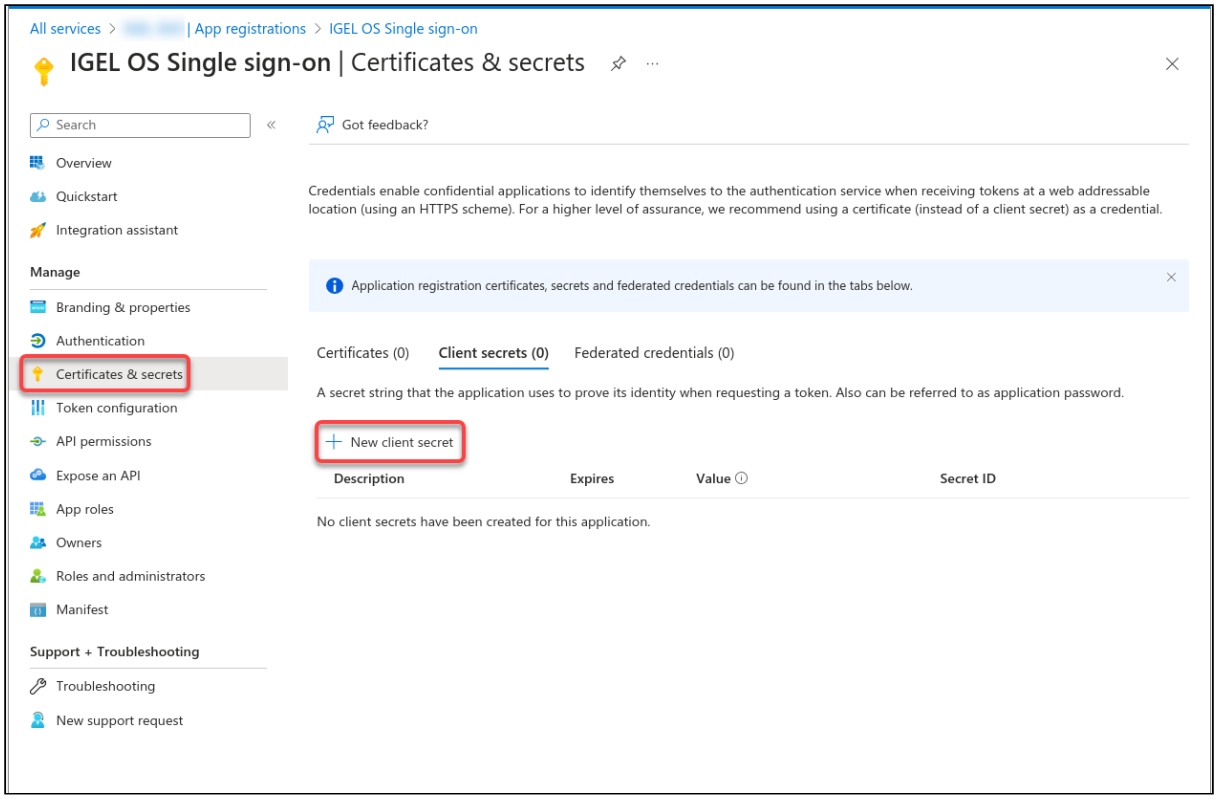
- **profile**


Home > | App registrations > IGEL
IGEL OS Single sign-on
Search
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
Request API permissions
All APIs
Microsoft Graph
https://graph.microsoft.com/ Docs
What type of permissions does your application require?
Delegated permissions
Your application needs to access the API as the signed-in user.
Application permissions
Your application runs as a background service or daemon without a signed-in user.
Select permissions
expand all
Start typing a permission to filter these results
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more
Permission
Admin consent required
OpenId permissions (3)
email
View users' email address
No
offline_access
Maintain access to data you have given it access to
No
openid
Sign users in
No
profile
View users' basic profile
No
AccessReview
Acronym
AdministrativeUnit
Add permissions
Discard

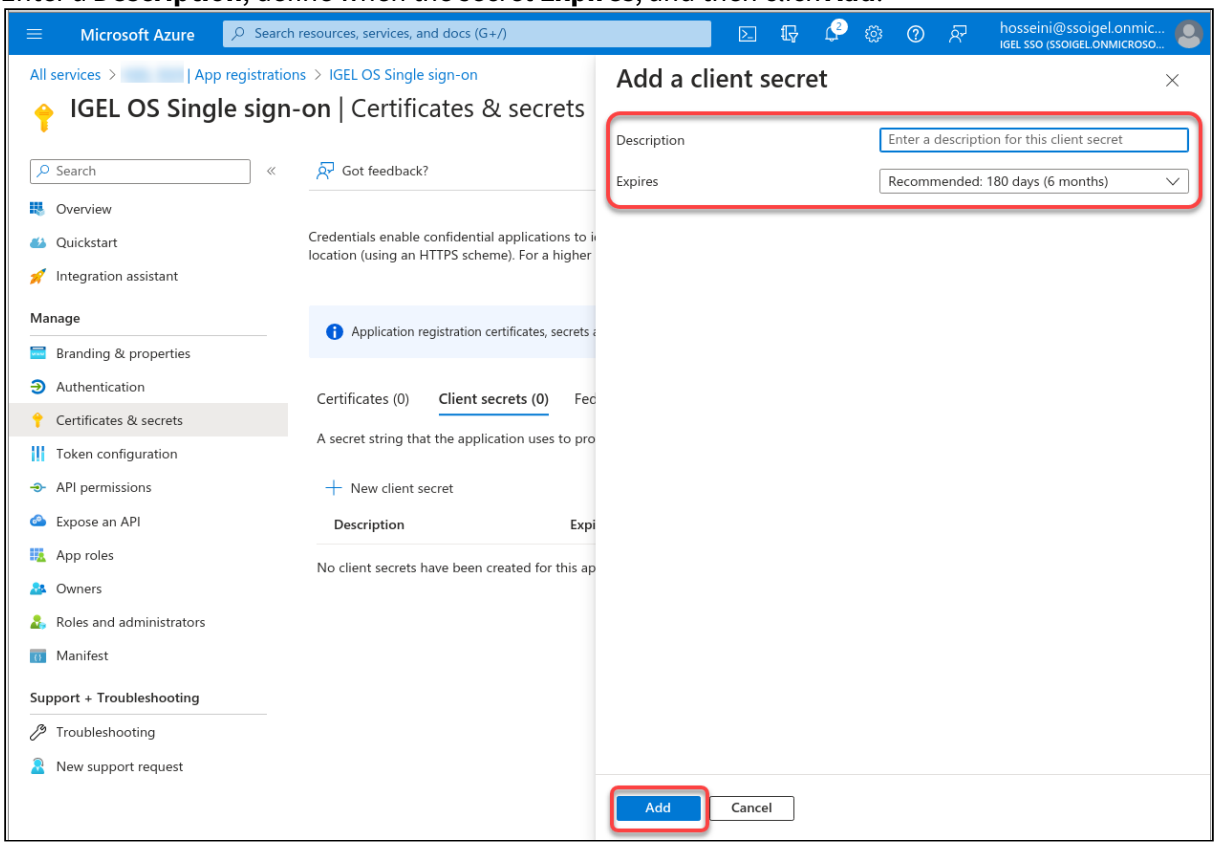
8. Check if the permissions are correct.



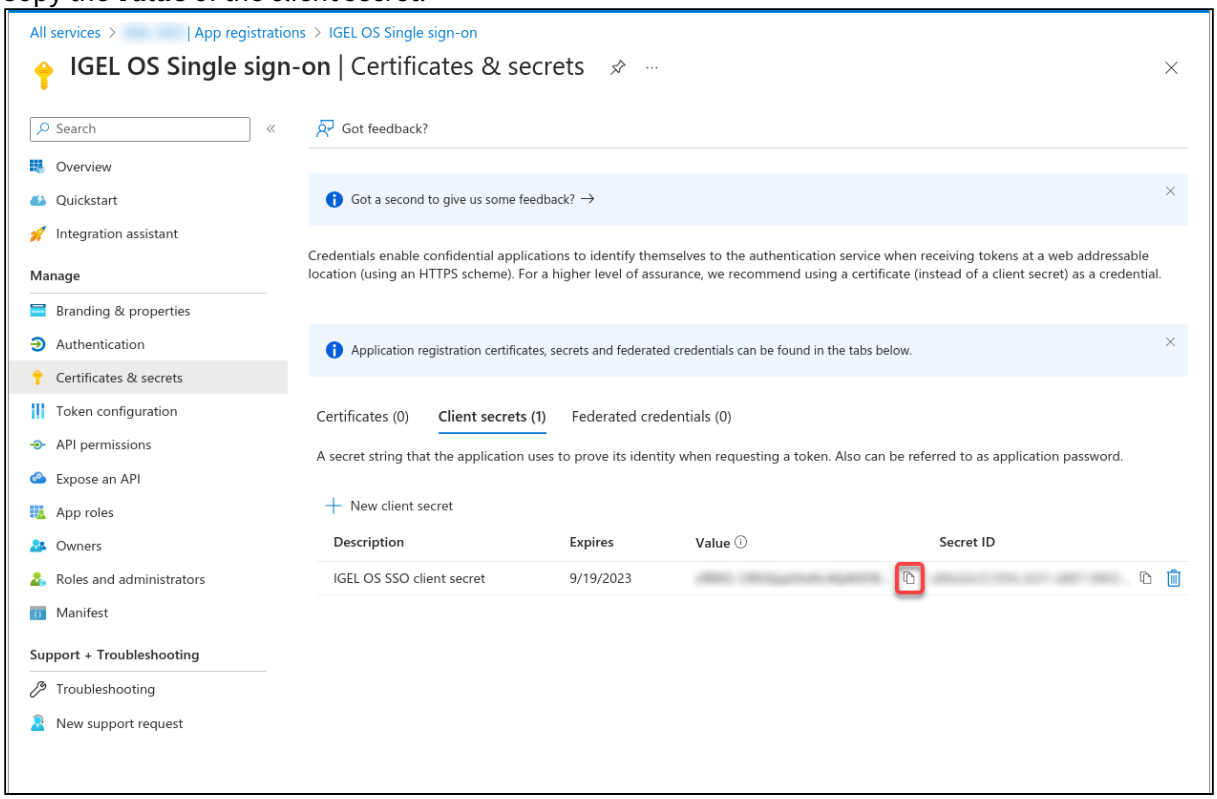
9. Go to **Certificates & secrets** and click **New client secret**.



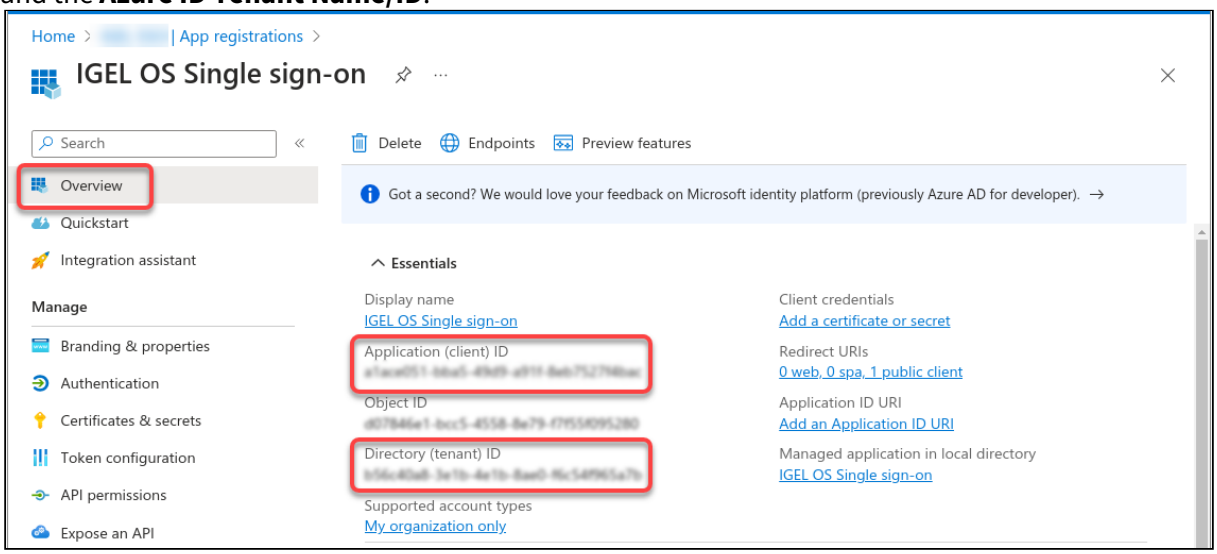
10. Enter a **Description**, define when the secret **Expires**, and then click **Add**.



11. Copy the **Value** of the client secret.

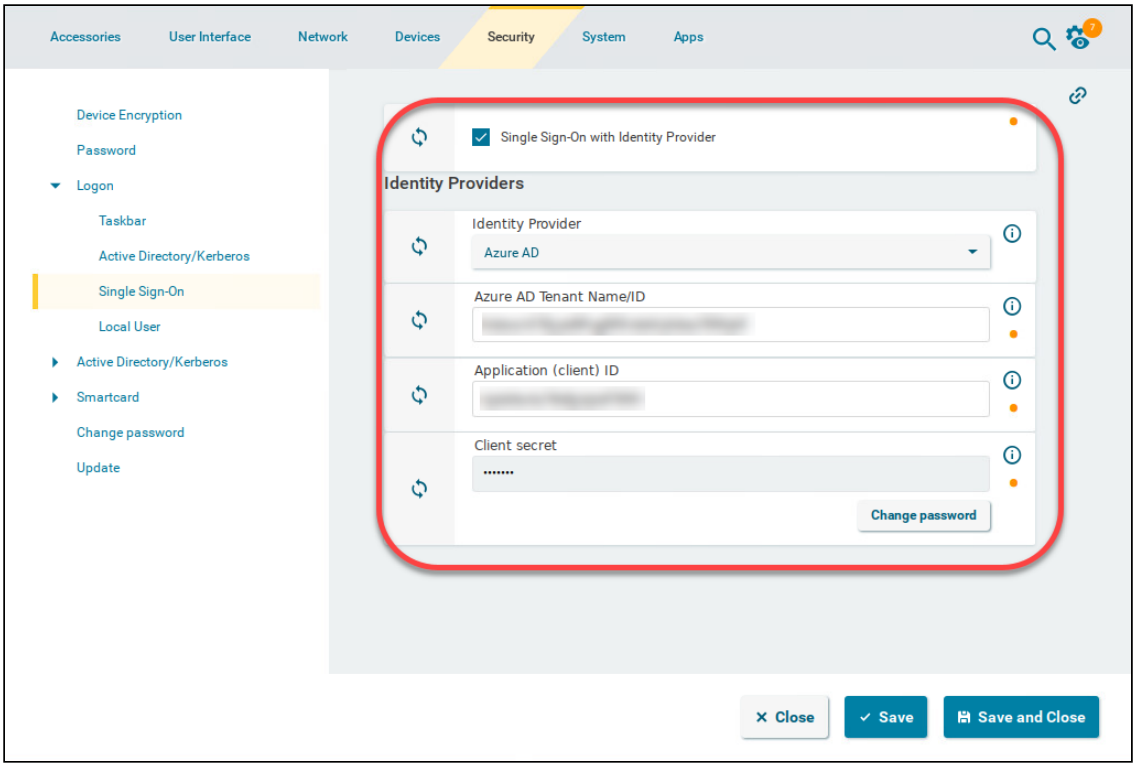


12. Go to **Overview** and copy the **Application (client) ID** and the **Directory (tenant) ID**. In the IGEL OS configuration, these values will be used as the **Public client identifier (client/application ID)** and the **Azure ID Tenant Name/ID**.



Configuring IGEL OS for SSO with Azure ID

1. Go to **Security > Logon > Single Sign-On** and edit the settings as follows:
   - Enable **Single Sign-On with Identity Provider**.
   - Set **Identity Provider** to **Azure ID**.
   - Enter the **Azure AD Tenant Name/ID**. This is the value you have obtained as **Directory (tenant) ID** in Azure AD Portal.
   - Set the appropriate **Application (client) ID**. This is the value you have obtained as **Application (client) ID** in your Azure AD Portal.
   - Enter the **Client secret**.



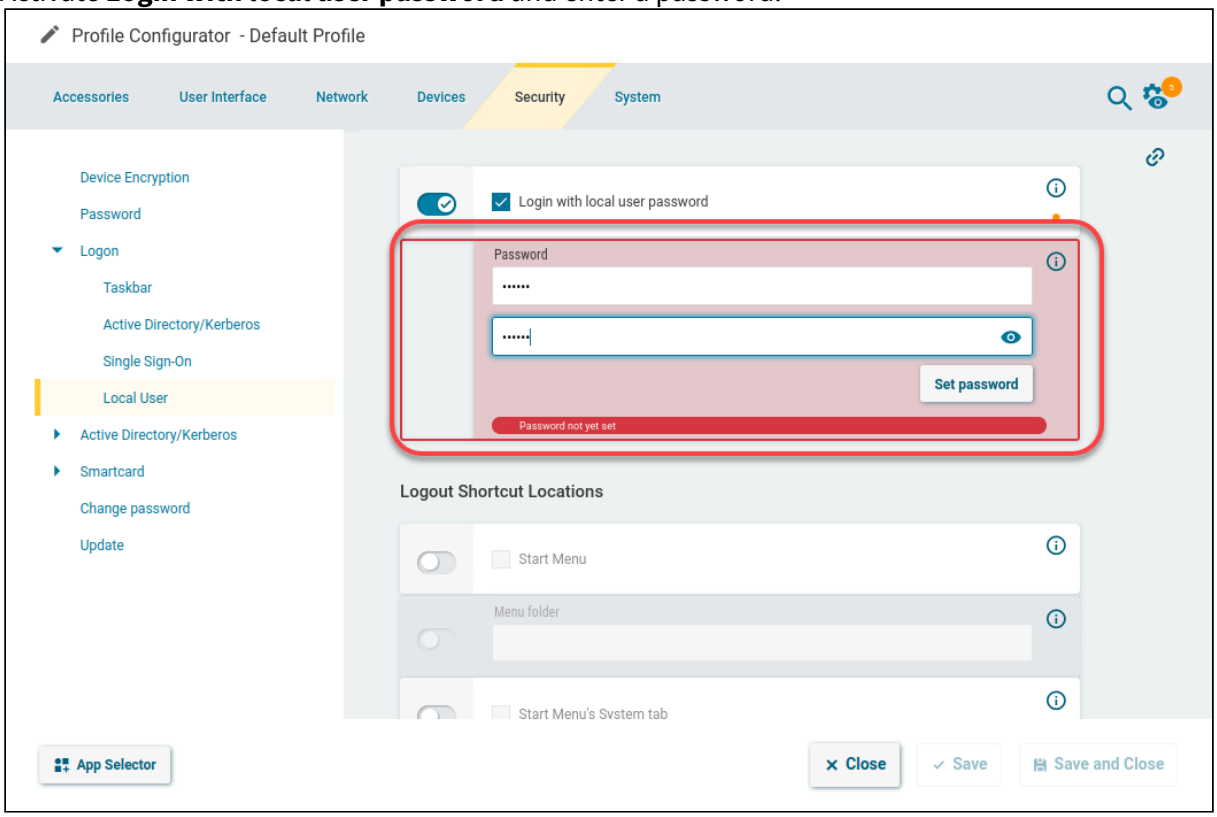
2. Click **Save** or **Save and close**.
   The desktop of the device is terminated. The login screen is displayed.
   You can now use the apps and utilities for IGEL OS 12 that support SSO with Azure AD(see page 193).
   For details on importing apps from the IGEL App Portal and installing them on IGEL OS devices, see IGEL UMS 12: Basic Configuration(see page 106) and Assignment of Apps and Profiles(see page 118).
   All methods of multi-factor authentication are available except the hardware token.

Enabling Local Login (Optional)

To have a fallback option if something goes wrong with SSO, e.g. a network failure, it is recommended to configure local login in addition.

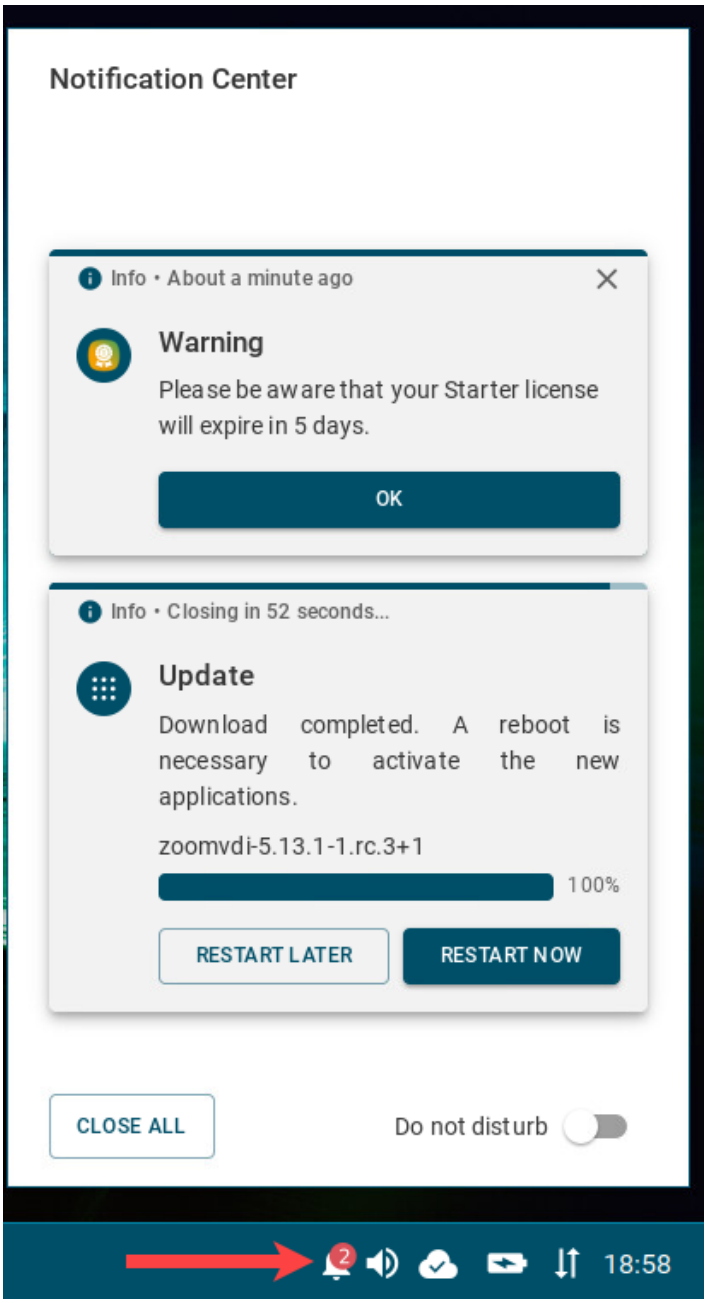
1. Open the profile configurator and go to **Security > Logon > Local user**.

2. Activate **Login with local user password** and enter a password.



IGEL OS Notification Center

On an IGEL OS device, you can view all non-closed notifications in the Notification Center.



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 112).
- 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

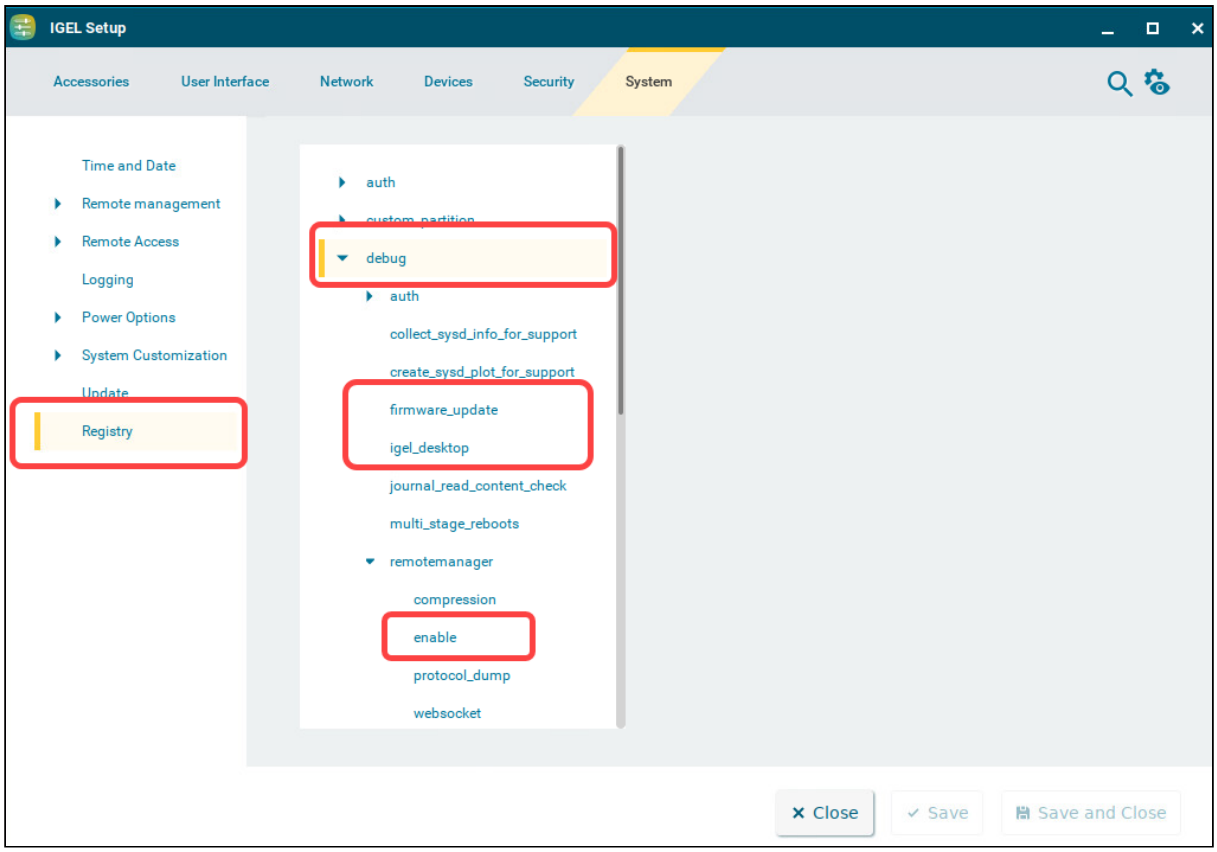
To collect the log files from the IGEL UMS Server, UMS Console, etc., you can use the Support Wizard: **UMS Console > Menu bar > Help > Save support information**. See Support Wizard in the IGEL UMS.

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



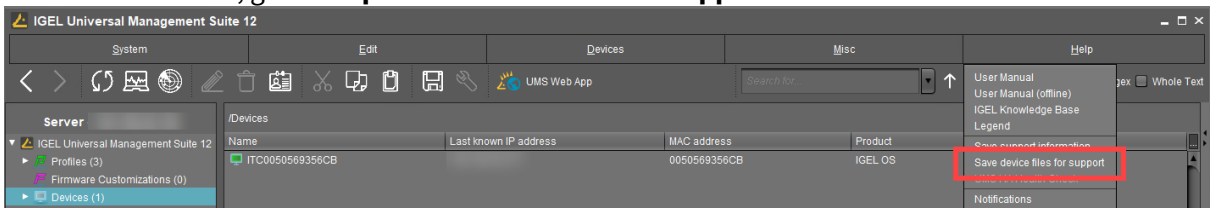
2. Click **Save** or **Apply**.

> 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

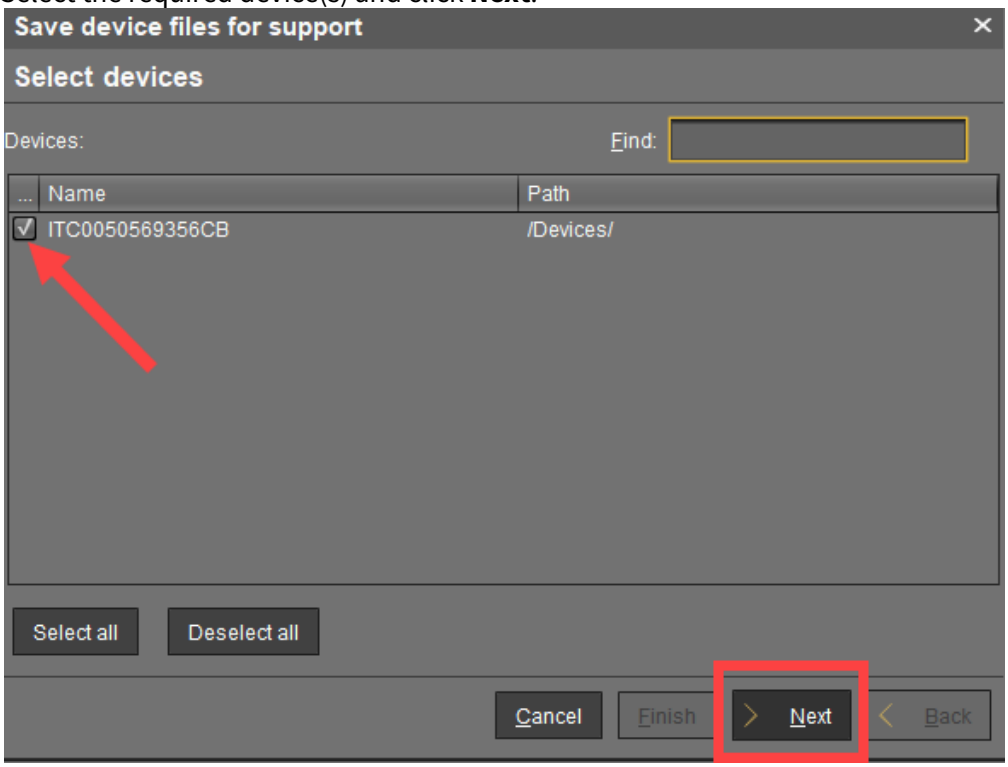
After you have activated the above registry keys, you can use the UMS Console to collect the device log files:

1. In the UMS Console, go to **Help > Save device files for support**.

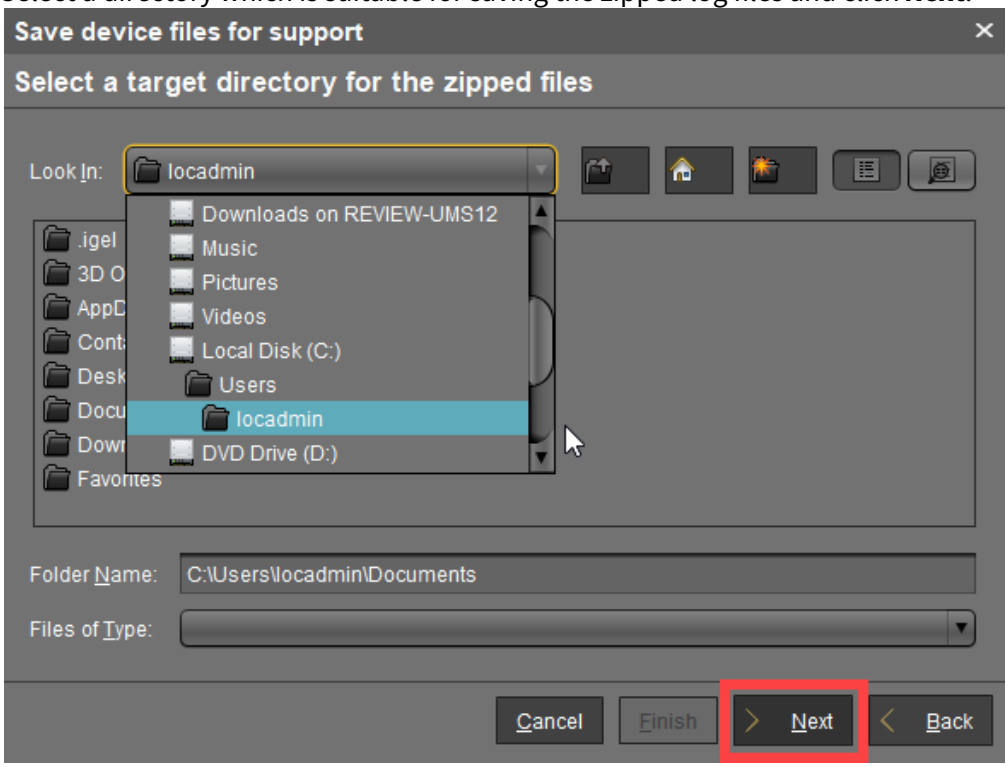


The dialog **Save device files for support** opens.

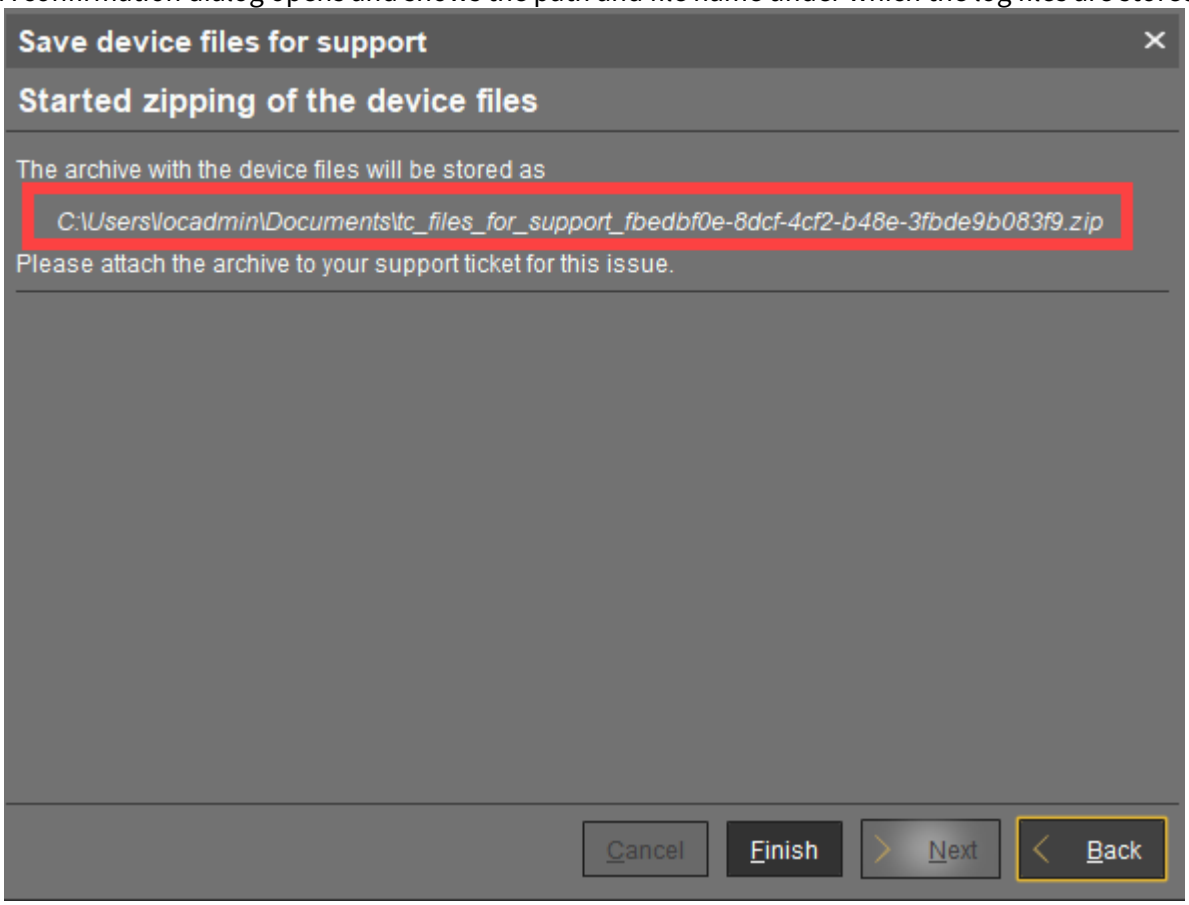
2. Select the required device(s) and click **Next**.



3. Select a directory which is suitable for saving the zipped log files and click **Next**.



A confirmation dialog opens and shows the path and file name under which the log files are stored.



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].

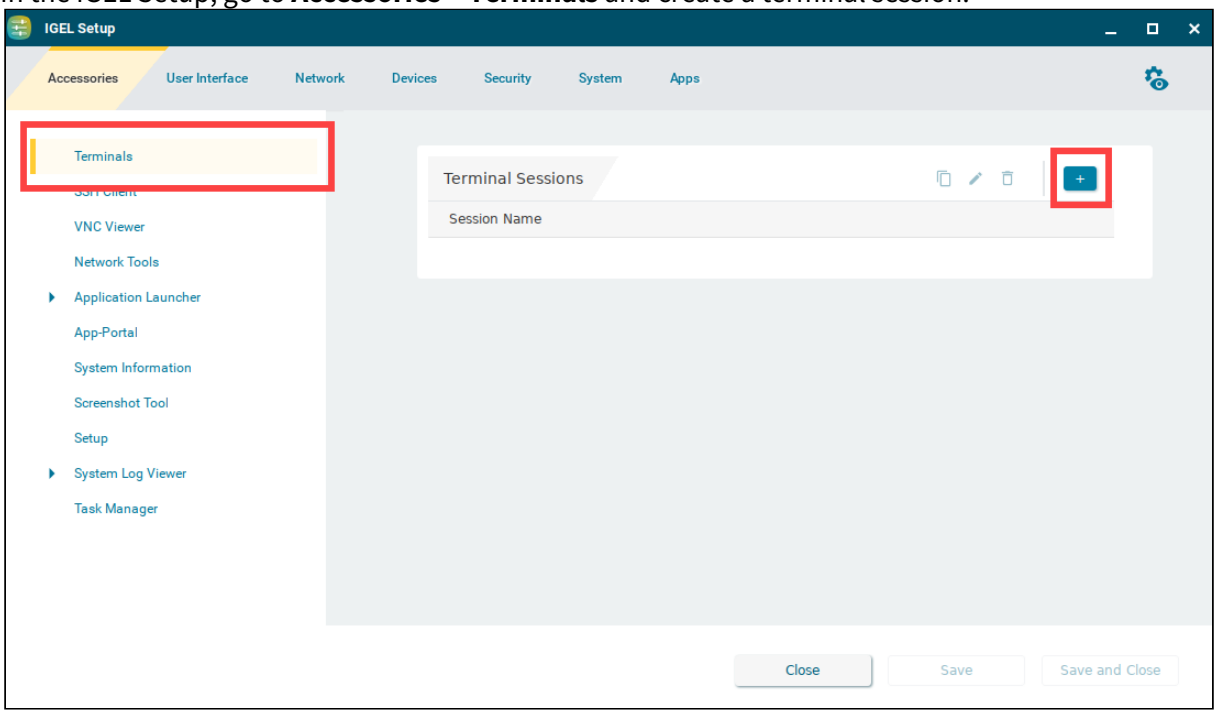
Collecting Device Logs without the UMS

When the UMS is not accessible or there is an issue with network connectivity, you can still extract logs from a device.

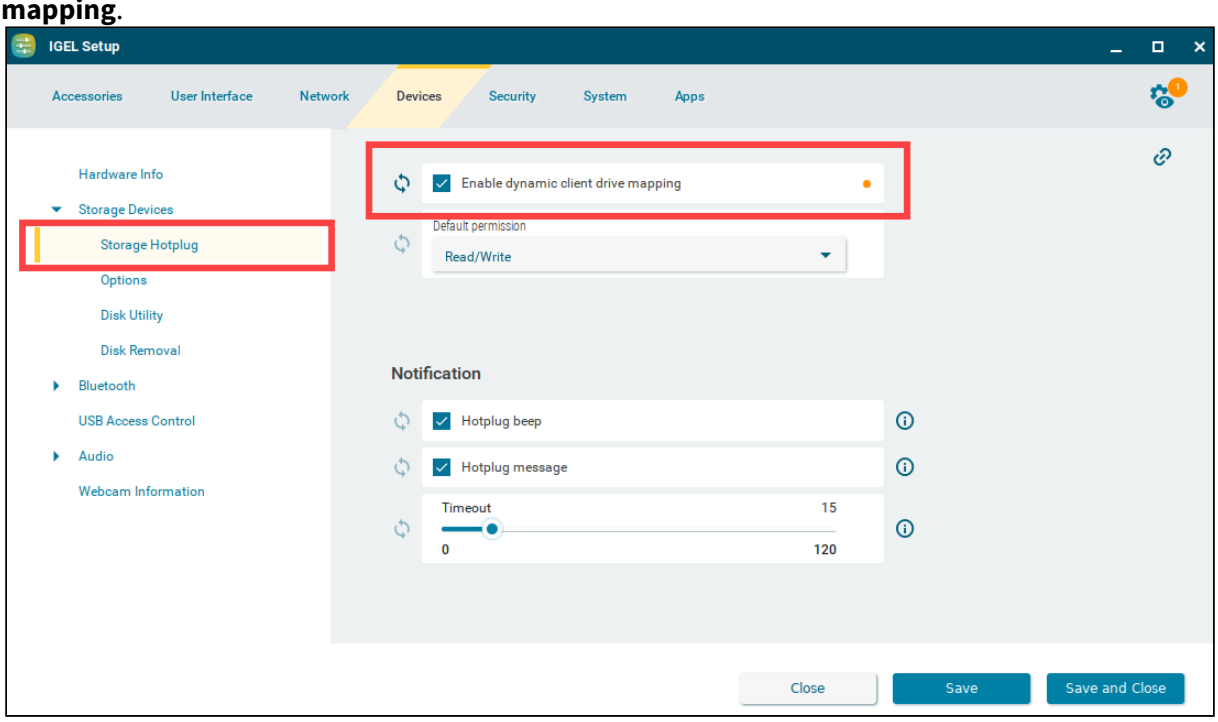
23 mailto:eap@igel.com
24 https://cosmos.igel.com/

Option 1: Via Local Terminal

1. In the IGEL Setup, go to **Accessories > Terminals** and create a terminal session.



2. Go to **Devices > Storage Devices > Storage Hotplug** and activate **Enable dynamic client drive mapping**.



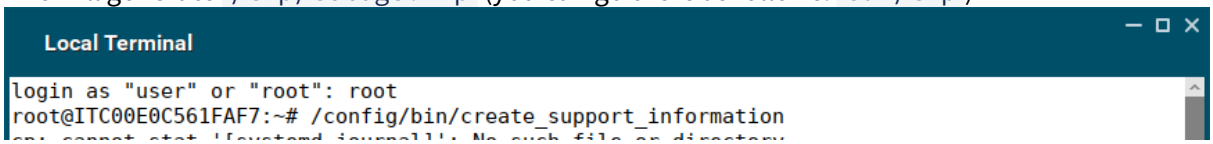
3. Verify that **System > Registry > debug > igel_desktop > Enable debug logging for IGEL desktop** is enabled.

4. Save the settings.

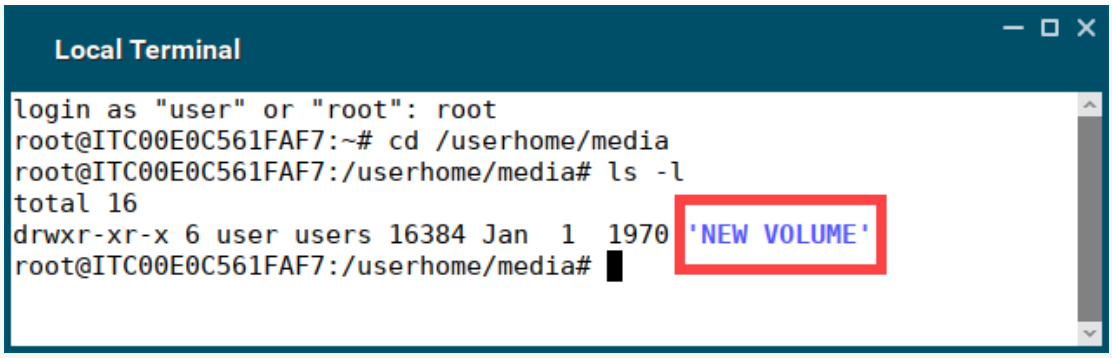
5. Plug the USB stick into the endpoint device and start the terminal session.

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`)



To find out the name of the USB stick, you can use the following commands:
```
cd /userhome/media
ls -l
```

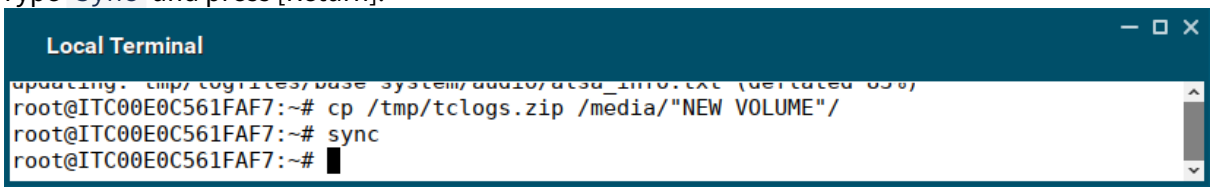


If there are spaces in the device name, you'll have to include it later in quotation marks. Example: `"NEW VOLUME"` .
If there are no spaces in the device name, quotation marks will not be required.

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].



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.

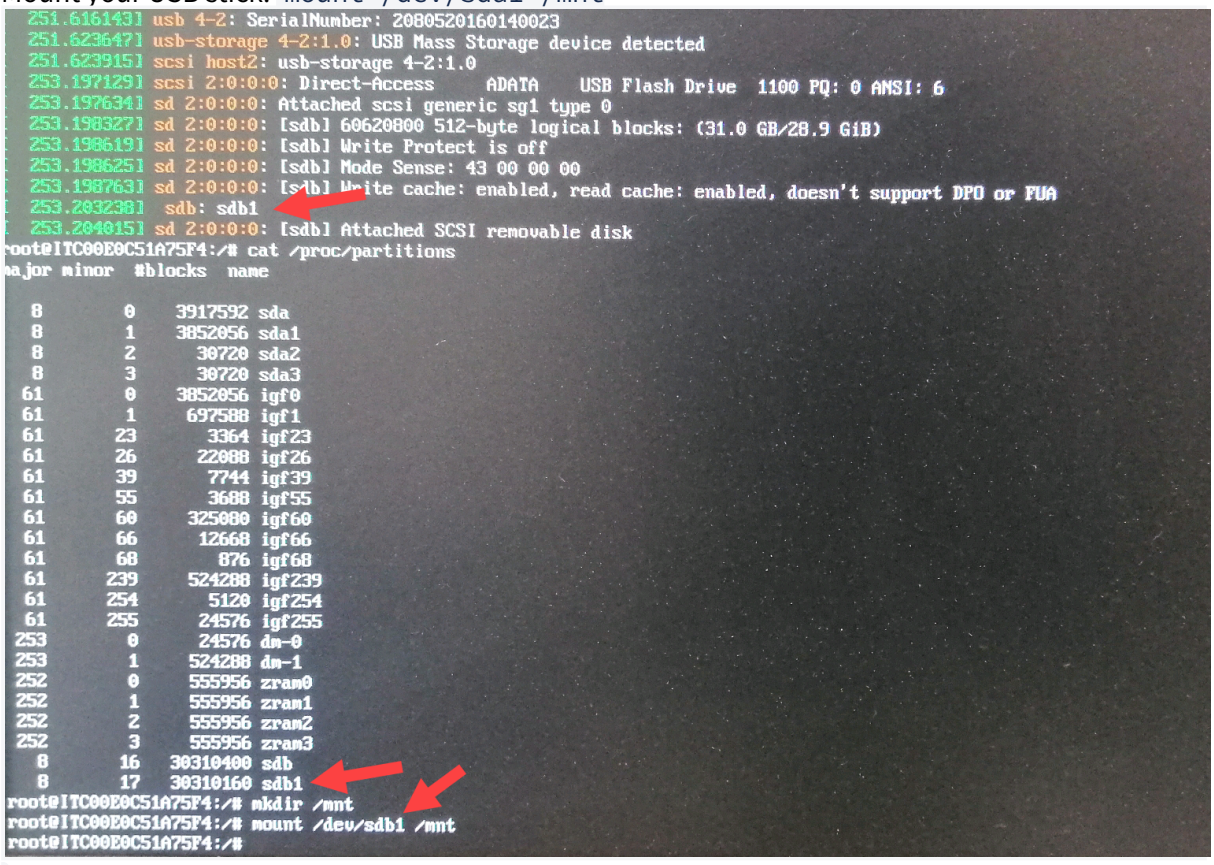
3. Execute the following command: `dmesg`
   This command is used to find out if the USB stick was correctly detected and which device name was assigned (`sda` , `sdb` , `sdc` , etc.)

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`

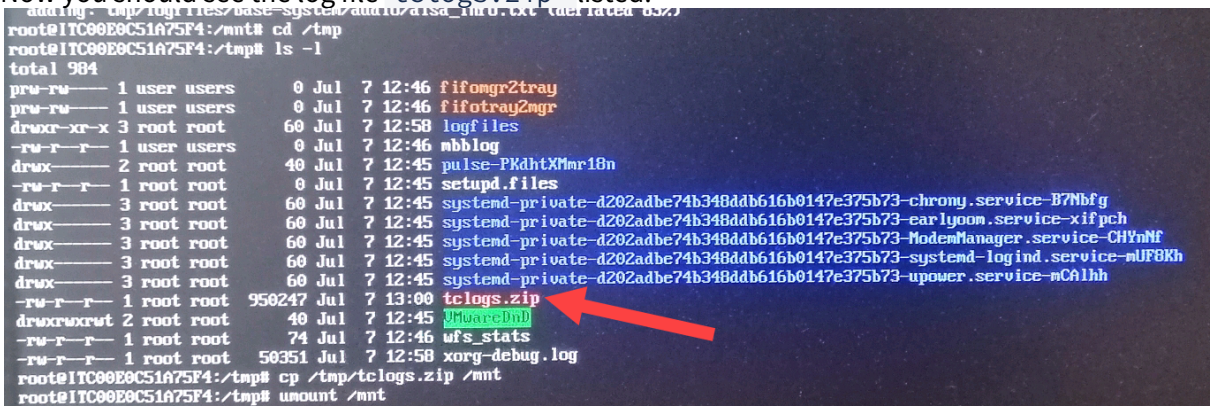


8. Check your data on your mounted USB stick:
   `cd /mnt`
   `ls -l`

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.



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/