



How to Start with IGEL



IGEL provides 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.

Introduction

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.

The IGEL platform comprises:

- IGEL Universal Management Suite (UMS) for managing IGEL OS 12 and IGEL OS 11 devices.
- IGEL OS 12
- The IGEL Cloud Services:
 - **IGEL Customer Portal** (see page 4) which is a doorway to the IGEL Cloud Services listed below. Here, you register your company account to invite other **users and assign them specific roles** (see page 23), 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** where you can find all applications currently available for IGEL OS 12
 - **IGEL App Creator Portal** that enables you to create your custom applications for IGEL OS 12
 - **IGEL Onboarding Service** (see page 58) which allows your users to easily onboard IGEL OS 12 devices using only their corporate e-mail
 - **IGEL Insight Service** (see page 217) which collects analytical and usage data to improve IGEL products and services and provide a better customer experience
 - **IGEL License Portal** (see page 168) where you can manage licenses for your IGEL OS devices

In this guide, you will find the first steps with the IGEL platform, IGEL OS 12, and UMS 12. Please read this guide fully, without skipping any steps.



Information about data storage of personal data can be found in the [IGEL privacy policy](#)¹.



Further Resources

For more information on the IGEL platform, check [IGEL Academy](#)² and [IGEL Community](#)³.

You may also find it useful to check the community docs:

- [HOWTO IGEL](#)⁴
- [Cheatsheet IGELCommunity](#)⁵.

1. <https://www.igel.com/privacy-policy/>

2. <https://learn.igel.com/>

3. <https://videos.igelcommunity.com/>

4. <https://igel-community.github.io/IGEL-Docs-v02/Docs/HOWTO-COSMOS/>

5. <https://igel-community.github.io/IGEL-Docs-v02/Docs/Cheatsheet-IGELCommunity/>



Using the IGEL Customer Portal

IGEL Customer Portal⁶ is the doorway to IGEL product-related services. Registering your company account here is the first step to using IGEL products. After registration, you can also use the IGEL Customer Portal to submit and manage support cases.

Registering for the IGEL Customer Portal

To register for the IGEL Customer Portal:

1. Open the [IGEL Customer Portal](https://support.igel.com/csm)⁷ and click **Register** in the upper right corner of the menu bar:

A screenshot of the IGEL Customer Portal homepage. The top navigation bar includes links for Catalog, Knowledge, Register (which has a red arrow pointing to it), and Log In. Below the header is a banner with a cityscape background and the text "Welcome to IGEL Cloud Services!". A search bar with placeholder text "Insert your question here" and a magnifying glass icon is positioned below the banner. A central blue callout box contains a message for customers, a link to register, and a link to the knowledge base. At the bottom of the page are three navigation links: Services, Software, and Hardware, each with its own sub-links.

The **IGEL Customer & Account Registration** form opens.

2. Enter your user data.

6. <https://support.igel.com/csm>
7. <https://support.igel.com/csm>

* Indicates required

Company Information

<p>* COMPANY NAME <input type="text"/></p> <p>ADDRESS 2 <input type="text"/></p> <p>* COUNTRY <input type="text"/> Germany</p> <p>* STATE/PROVINCE <input type="text"/></p>	<p>* ADDRESS <input type="text"/></p> <p>* CITY <input type="text"/></p> <p>* POST CODE <input type="text"/> Please write N/A if no zip code is available</p> <p>* INDUSTRY <input type="text"/> Others</p>
---	---

Personal Information

<p>* LOGIN-EMAIL <input type="text"/></p> <p>* FIRST NAME <input type="text"/></p> <p>* CHOOSE YOUR PREFERRED LANGUAGE <input type="text"/> English</p>	<p>* WORK PHONE <input type="text"/> Please use following format +1234567890</p> <p>* LAST NAME <input type="text"/></p>
--	--

I agree that IGEL will send me information about IGEL products, news, upcoming events & promotions by e-mail ("IGEL News") on a regular basis. I can unsubscribe from this at any time. The processing of my personal data is described in the Privacy Policy.
 * I HAVE READ AND ACCEPT THE IGEL CLOUD SERVICES TERMS AND CONDITIONS
 * I HAVE READ AND ACCEPT THE IGEL APP CREATOR PORTAL TERMS AND CONDITIONS

IGEL Cloud Services Terms & Conditions can be found [here](#)
 IGEL App Creator Portal Terms & Conditions can be found [here](#)

Required information

COMPANY NAME

ADDRESS

CITY

POST CODE

STATE/PROVINCE

LOGIN-EMAIL

WORK PHONE

FIRST NAME

LAST NAME

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 required information in the right pane.

i 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, http://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. When your registration has been approved, you will receive an email confirmation 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.

⚠ To ensure communication related to your registration is delivered, make sure your IT organisation does not block noreply@id.igel.com⁸. If you have registered, and your registration has been approved, please make sure the welcome email containing your password is not in your spam folder, and has not been quarantined by your organisation's email system.

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

⚠ Please remember your login email address. 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 23).

Enabling Multi-Factor Authentication (MFA) for the IGEL Customer Portal

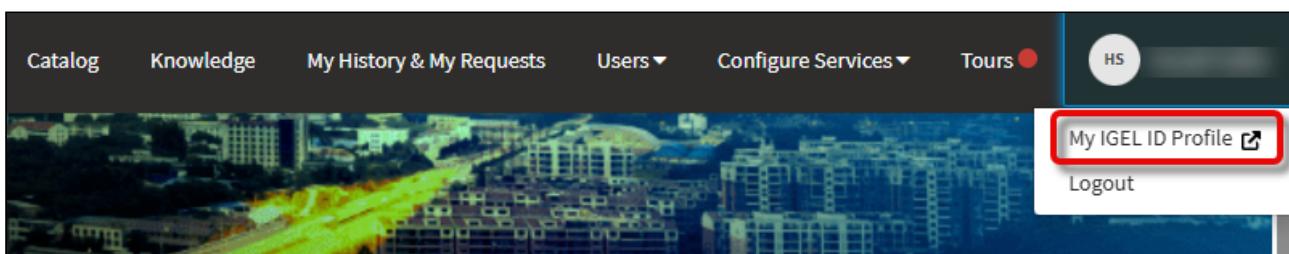
It is recommended to add multi-factor authentication (MFA) to your IGEL Customer Portal account.

The following methods are available:

- Authenticator app; the supported apps are:
 - Google Authenticator
 - Microsoft Authenticator
 - Authy
- Email verification

Authenticator App

1. In the IGEL Customer Portal, open the user menu and select **My IGEL ID Profile**.



8. mailto:noreply@id.igel.com



You are taken to the **IGEL ID Profile Management** site in a separate browser tab or browser window.

2. Select **MFA Settings**.

A screenshot of the "IGEL ID Profile Management" web interface. At the top, there is a navigation bar with three buttons: "Profile Details", "MFA Settings" (which is highlighted with a red box), and "Change Password". To the right of the "MFA Settings" button is a "Sign Out" link. Below the navigation bar, the main content area has a title "Multi-Factor Authentication". Under this title, there is a section titled "Current MFA Status" containing two items: "Authenticator App: Disabled" and "Email Verification: Disabled". In the "MFA Options" section, there are two options: "Authenticator App" (with a "Set up Authenticator App" button) and "Email MFA" (with an "Enable Email MFA" button).

IGEL ID Profile Management

Profile Details MFA Settings Change Password Sign Out

Multi-Factor Authentication

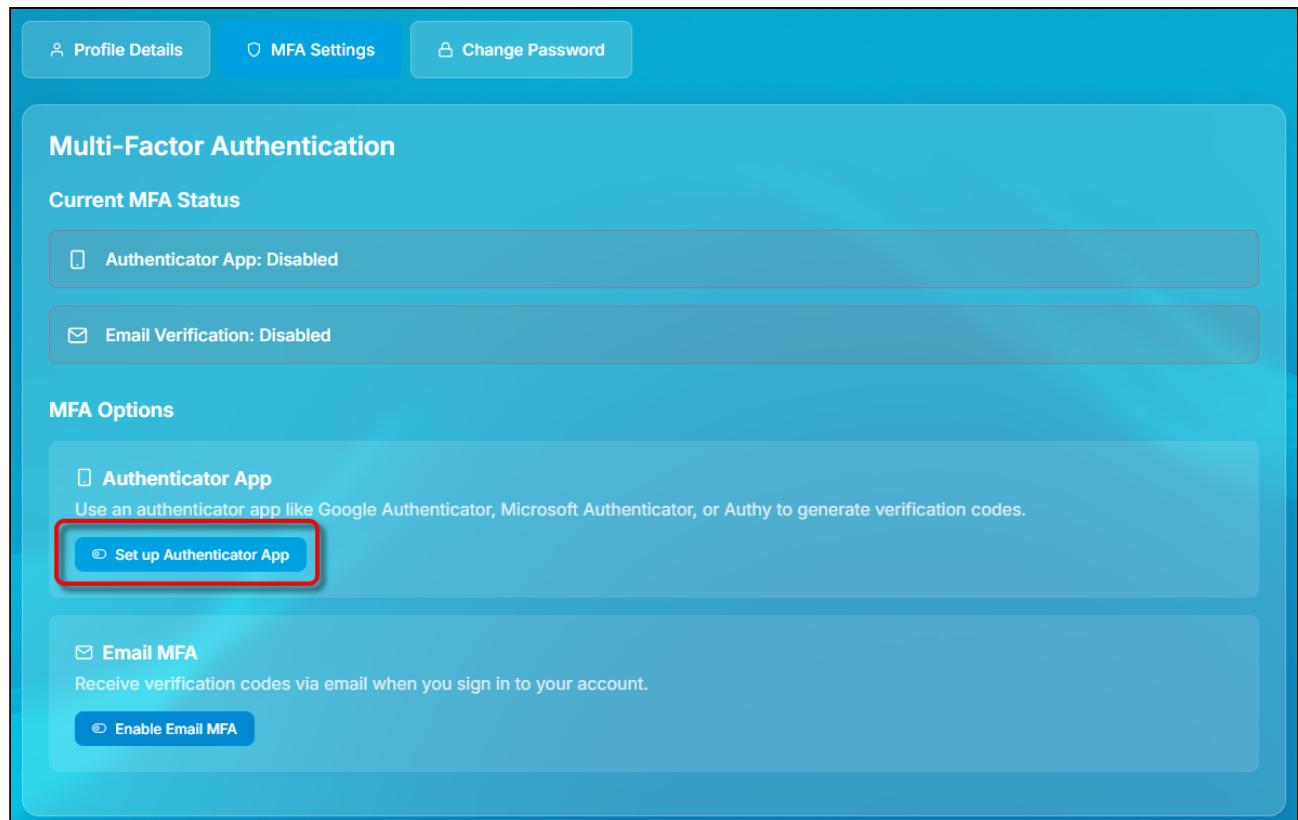
Current MFA Status

- Authenticator App: Disabled
- Email Verification: Disabled

MFA Options

- Authenticator App
 - Set up Authenticator App
- Email MFA
 - Enable Email MFA

3. Click **Set up Authenticator App**.



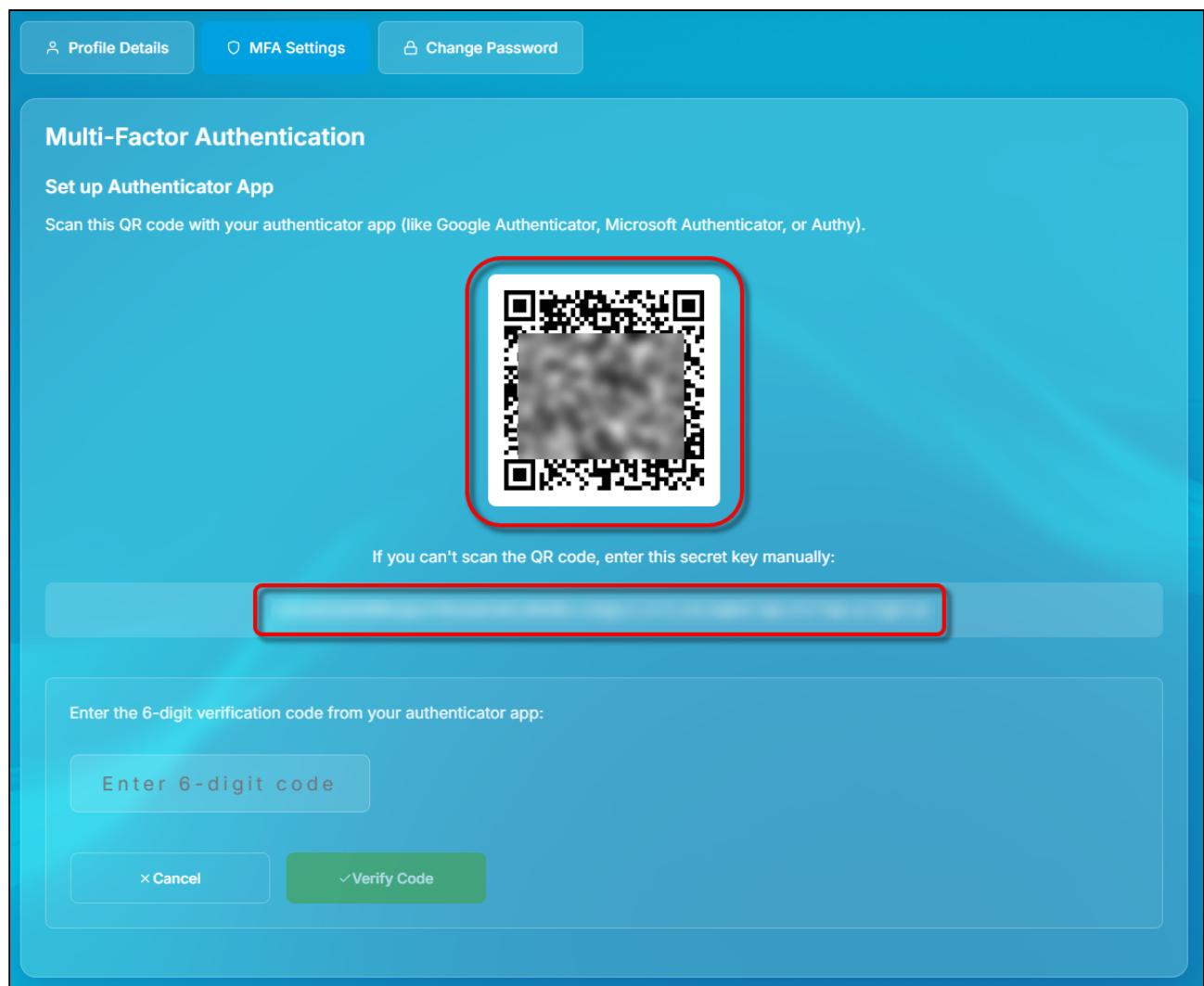
Authenticator App: Disabled
Use an authenticator app like Google Authenticator, Microsoft Authenticator, or Authy to generate verification codes.

Email Verification: Disabled

Authenticator App
Use an authenticator app like Google Authenticator, Microsoft Authenticator, or Authy to generate verification codes.
Set up Authenticator App

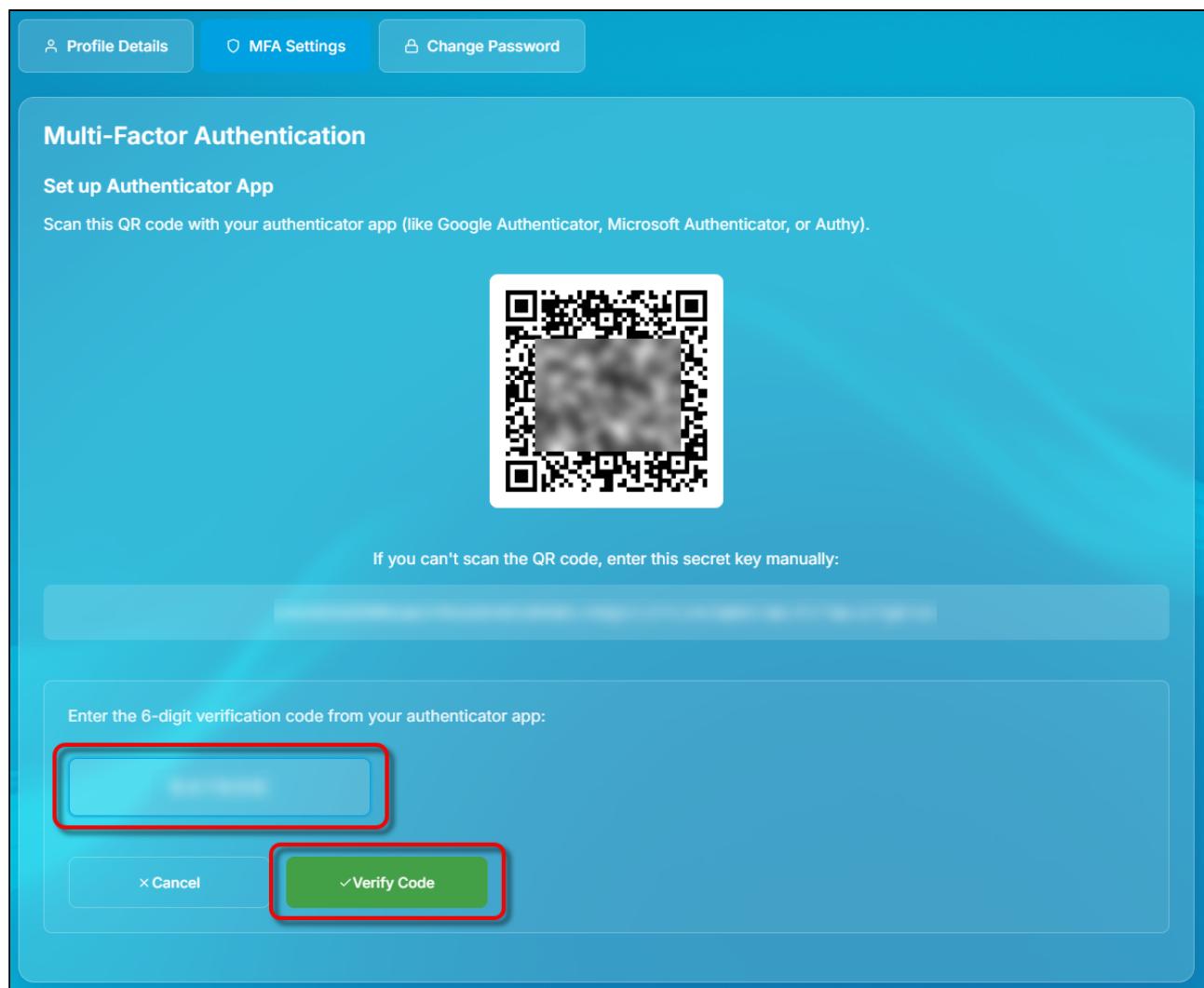
Email MFA
Receive verification codes via email when you sign in to your account.
Enable Email MFA

4. Scan the QR code with your authenticator app or enter the secret key manually.



The screenshot shows the 'Multi-Factor Authentication' section of the IGEL Customer Portal. At the top, there are three tabs: 'Profile Details', 'MFA Settings' (which is selected), and 'Change Password'. The main area is titled 'Multi-Factor Authentication' and contains the sub-section 'Set up Authenticator App'. It instructs users to scan a QR code with their authenticator app (Google Authenticator, Microsoft Authenticator, or Authy). A QR code is displayed in the center, enclosed in a red rectangular box. Below the QR code is a text link: 'If you can't scan the QR code, enter this secret key manually:' followed by a large, empty text input field also enclosed in a red rectangular box. Further down, there is a section for entering a 6-digit verification code from the authenticator app, featuring a placeholder 'Enter 6-digit code', a 'Cancel' button, and a green 'Verify Code' button.

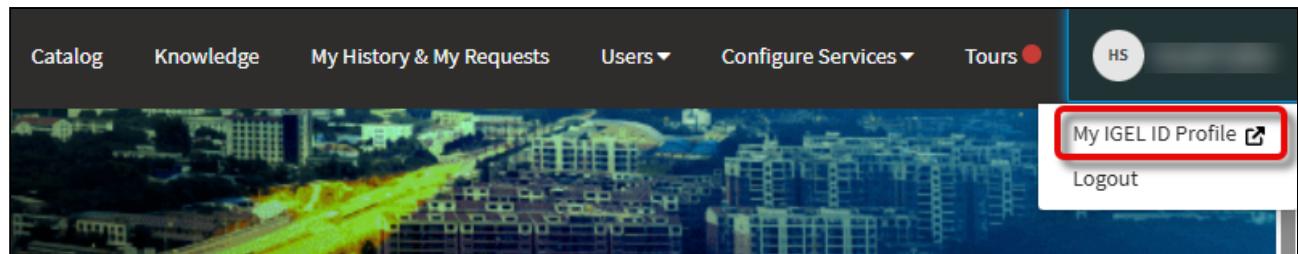
5. Enter the 6-digit verification code from your authenticator app and verify it.



When you log in to the IGEL Customer Portal, you will be prompted to enter the current verification code from your authenticator app.

Email Verification

1. In the IGEL Customer Portal, open the user menu and select **My IGEL ID Profile**.



You are taken to the **IGEL ID Profile Management** site in a separate browser tab or browser window.

2. Select **MFA Settings**.

The screenshot shows the 'IGEL ID Profile Management' interface. At the top, there are three tabs: 'Profile Details', 'MFA Settings' (which is highlighted with a red box), and 'Change Password'. Below the tabs, the 'Multi-Factor Authentication' section is displayed. It includes 'Current MFA Status' which lists 'Authenticator App: Disabled' and 'Email Verification: Disabled'. Under 'MFA Options', there are two sections: 'Authenticator App' (described as using an authenticator app like Google Authenticator, Microsoft Authenticator, or Authy to generate verification codes) and 'Email MFA' (described as receiving verification codes via email when signing in). Both sections have a 'Set up' button: 'Set up Authenticator App' for the first and 'Enable Email MFA' for the second.

3. Click **Enable Email MFA**.



The screenshot shows the 'IGEL ID Profile Management' interface. At the top, there are three tabs: 'Profile Details', 'MFA Settings' (which is selected), and 'Change Password'. Below the tabs, the 'Multi-Factor Authentication' section is displayed. It includes a 'Current MFA Status' table with two rows: 'Authenticator App: Disabled' and 'Email Verification: Disabled'. Under 'MFA Options', there are two sections: 'Authenticator App' (with a note about using Google Authenticator or Microsoft Authenticator) and 'Email MFA' (with a note about receiving verification codes via email). A red box highlights the 'Enable Email MFA' button.

When you log in to the IGEL Customer Portal, you will be prompted to enter the one-time authentication code sent to you via email.

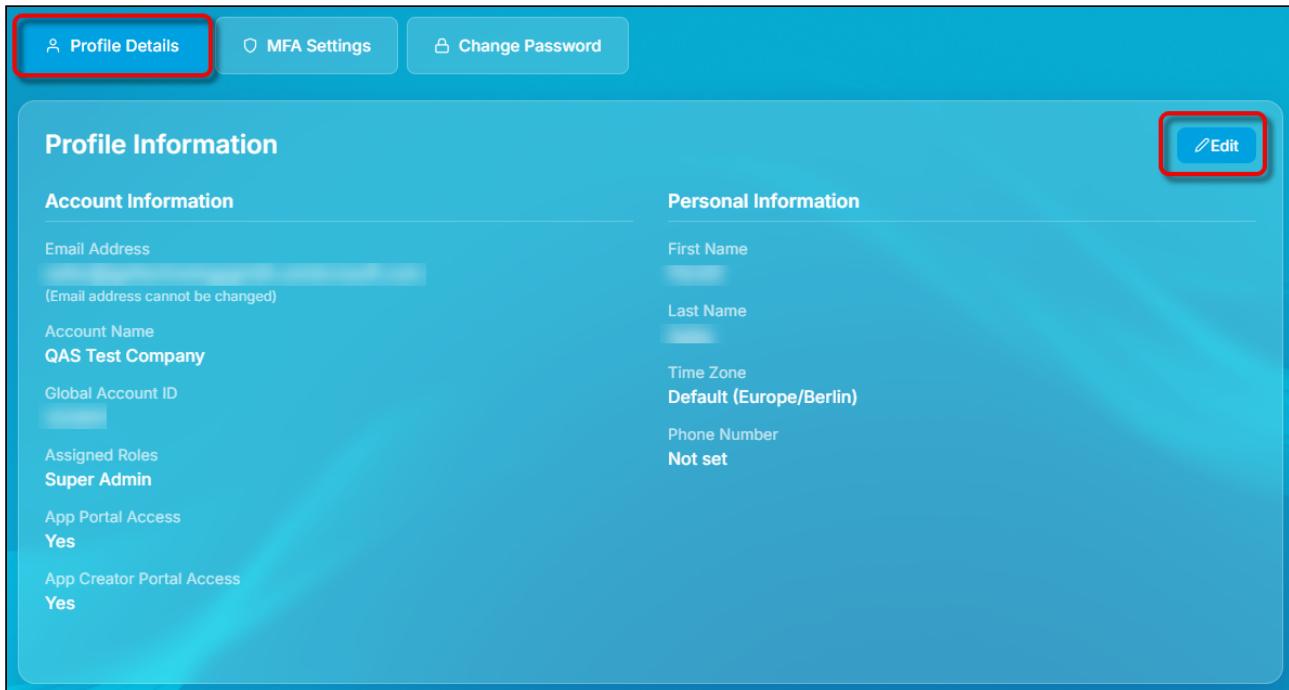
Changing Your Personal Information in the IGEL Customer Portal

1. In the IGEL Customer Portal, open the user menu and select **My IGEL ID Profile**.

The screenshot shows the top navigation bar of the IGEL Customer Portal. The menu items include Catalog, Knowledge, My History & My Requests, Users (with a dropdown arrow), Configure Services (with a dropdown arrow), Tours (with a red notification dot), and a user profile icon labeled 'HS'. A red box highlights the 'My IGEL ID Profile' link in the dropdown menu, which also includes 'Logout'.

You are taken to the **IGEL ID Profile Management** site in a separate browser tab or browser window.

2. Ensure that **Profile Details** is active and click **Edit**.



The screenshot shows the 'Profile Information' page. At the top, there are three tabs: 'Profile Details' (highlighted with a red box), 'MFA Settings', and 'Change Password'. Below the tabs, the page is divided into two main sections: 'Account Information' on the left and 'Personal Information' on the right. Under 'Account Information', fields include 'Email Address' (disabled, shown as [REDACTED]), 'Account Name' (set to 'QAS Test Company'), 'Global Account ID' (shown as [REDACTED]), 'Assigned Roles' (set to 'Super Admin'), 'App Portal Access' (set to 'Yes'), and 'App Creator Portal Access' (set to 'Yes'). Under 'Personal Information', fields include 'First Name' (shown as [REDACTED]), 'Last Name' (shown as [REDACTED]), 'Time Zone' (set to 'Default (Europe/Berlin)'), and 'Phone Number' (set to 'Not set'). In the top right corner of the page area, there is a blue 'Edit' button with a pencil icon, also highlighted with a red box.

3. Edit your personal information as desired and click **Save**.

- i Please note the following about the phone number:
 - When you set/edit your phone number, a text message is sent to that number for verification purposes.
 - Your phone number will be used to send a verification code for password reset (see [Login Credentials Forgotten?](#) (see page 17)). If you have not provided a phone number, your email address will be used instead.



Screenshot of the IGEL Customer Portal Profile Information page.

The page has three tabs at the top: Profile Details, MFA Settings, and Change Password. The Change Password tab is selected.

The main area is divided into two sections: Account Information and Personal Information.

Account Information:

- Email Address: [REDACTED] (Email address cannot be changed)
- Account Name: [REDACTED]
- Global Account ID: [REDACTED]
- Assigned Roles:
Super Admin
- App Portal Access: Yes
- App Creator Portal Access: Yes

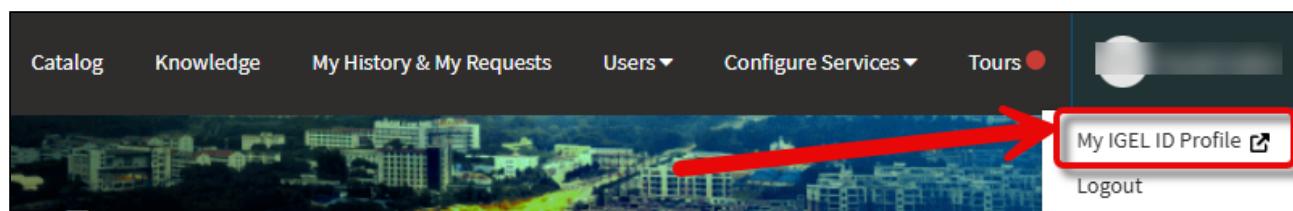
Personal Information: (This section is highlighted with a red box.)

- First Name: [REDACTED]
- Last Name: [REDACTED]
- Time Zone: Default (Europe/Berlin)
- Phone Number: +1234567890
Please include country code (e.g., +1 for US)

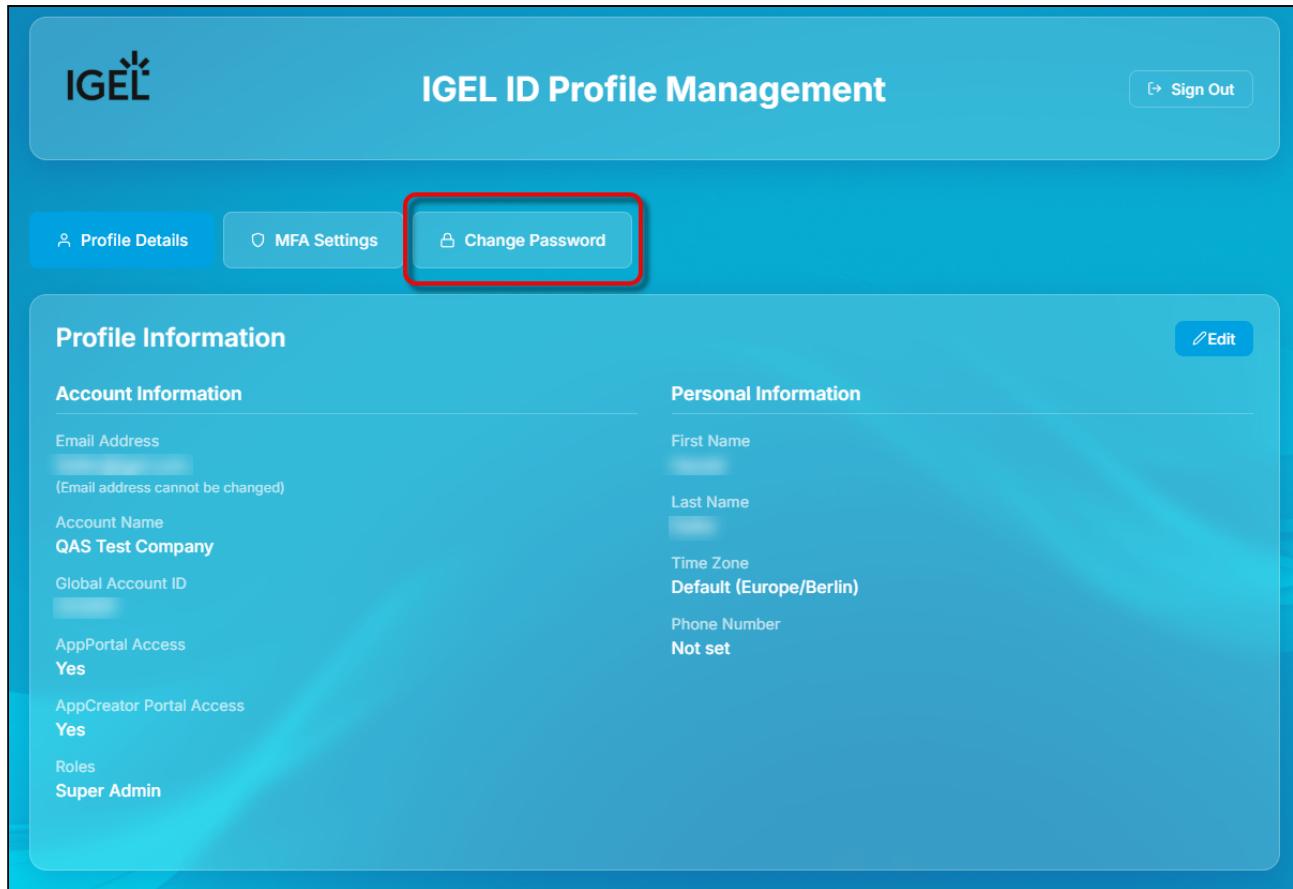
Buttons at the bottom right: Cancel and Save (Save is highlighted with a red box).

Changing Your Password in the IGEL Customer Portal

1. In the user menu, click **My IGEL ID Profile**.

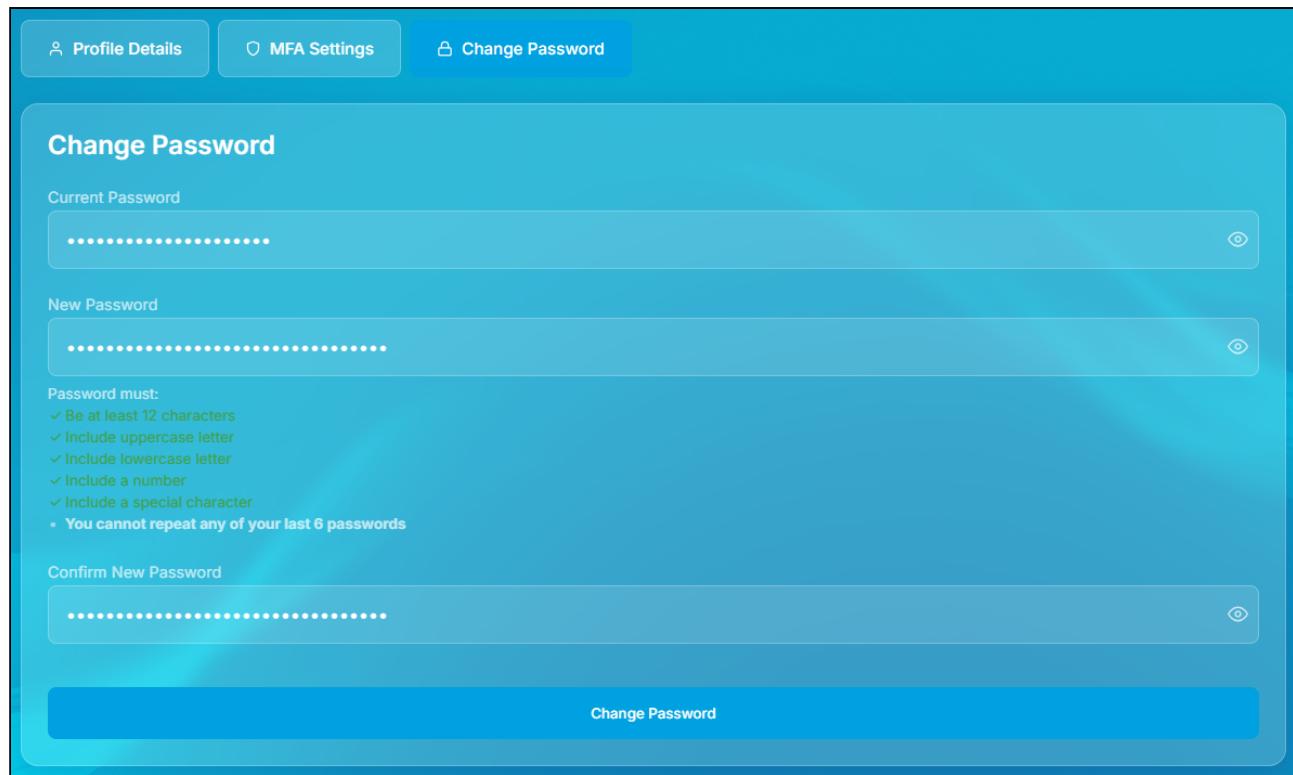


2. Click **Change Password**.



The screenshot shows the 'IGEL ID Profile Management' interface. At the top, there are three navigation buttons: 'Profile Details' (selected), 'MFA Settings', and 'Change Password' (highlighted with a red box). Below these are two main sections: 'Profile Information' and 'Personal Information'. The 'Profile Information' section contains fields for Email Address (disabled), Account Name (QAS Test Company), Global Account ID, AppPortal Access (Yes), AppCreator Portal Access (Yes), and Roles (Super Admin). The 'Personal Information' section contains fields for First Name, Last Name, Time Zone (Default (Europe/Berlin)), and Phone Number (Not set). There is also an 'Edit' button in the top right corner of the profile information area.

3. Enter your current password and the new password, and confirm with **Change Password**. Please note the password requirements.



The screenshot shows the 'Change Password' section of the IGEL Customer Portal. At the top, there are three tabs: 'Profile Details', 'MFA Settings', and 'Change Password' (which is selected). The main area is titled 'Change Password'. It contains three password input fields with visibility toggles. Below the 'New Password' field is a list of password requirements:

- ✓ Be at least 12 characters
- ✓ Include uppercase letter
- ✓ Include lowercase letter
- ✓ Include a number
- ✓ Include a special character
- You cannot repeat any of your last 6 passwords

At the bottom is a large blue 'Change Password' button.

A confirmation message will be displayed briefly.

Logging in to the IGEL Customer Portal

1. Open the [IGEL Customer Portal](https://support.igel.com/)⁹ and click **Login**.

i If your browser is already logged in to the IGEL Customer Portal, the IGEL App Portal, or the IGEL App Creator Portal, you do not need to authenticate again. When you select **Login**, you are automatically logged in via SSO.

2. Enter the credentials you used to register with IGEL and click **Sign in**.

9. <https://support.igel.com/>

A screenshot of the IGEL Customer Portal login page. At the top, the IGEL logo is displayed. Below it, the text "Sign in with your email and password" is centered. There are two input fields: one for "Email" containing "name@host.com" and one for "Password". Below the password field is a link "Forgot your password?". At the bottom is a large yellow button with the text "Sign in" in white.

The IGEL Customer Portal opens. If you have configured MFA, you must enter a verification code first.

Login Credentials Forgotten?

1. Open the [IGEL Customer Portal](https://support.igel.com/)¹⁰ and click **Login**.

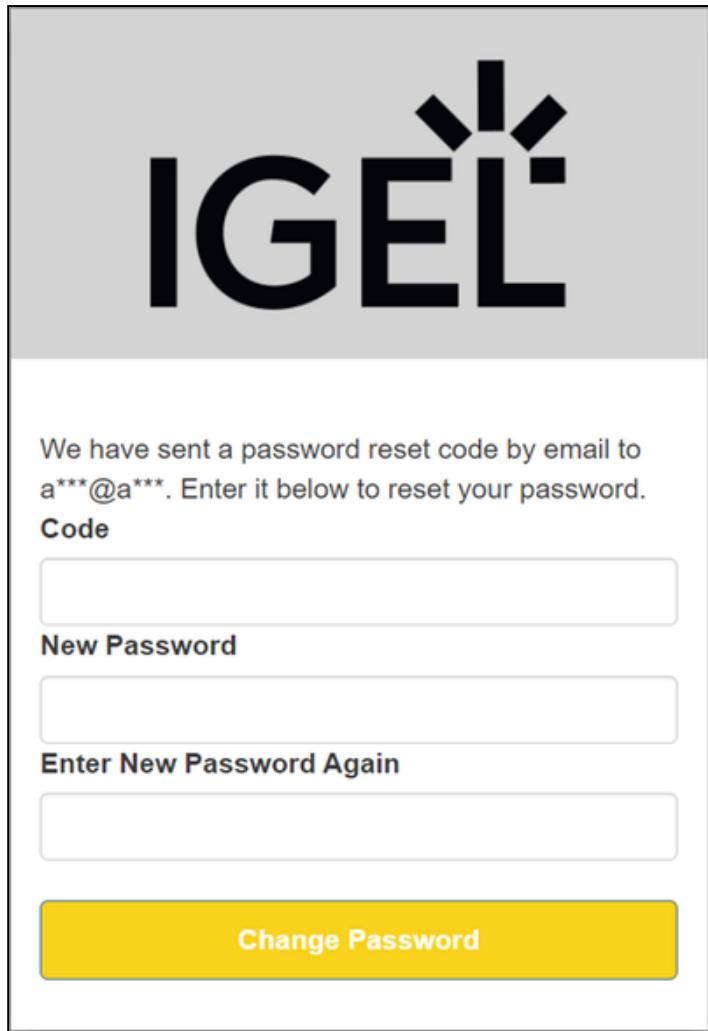
2. Click **Forgot your password?** to reset a password.

A dialog for requesting a new password opens.

10. <https://support.igel.com/>



3. Enter the email address to which the verification code should be sent and click **Reset my password**.
4. Check your email inbox for the email with the code. If you have not received the email, please check your spam folder.
5. Provide the code you received under **Code** and set a new password.

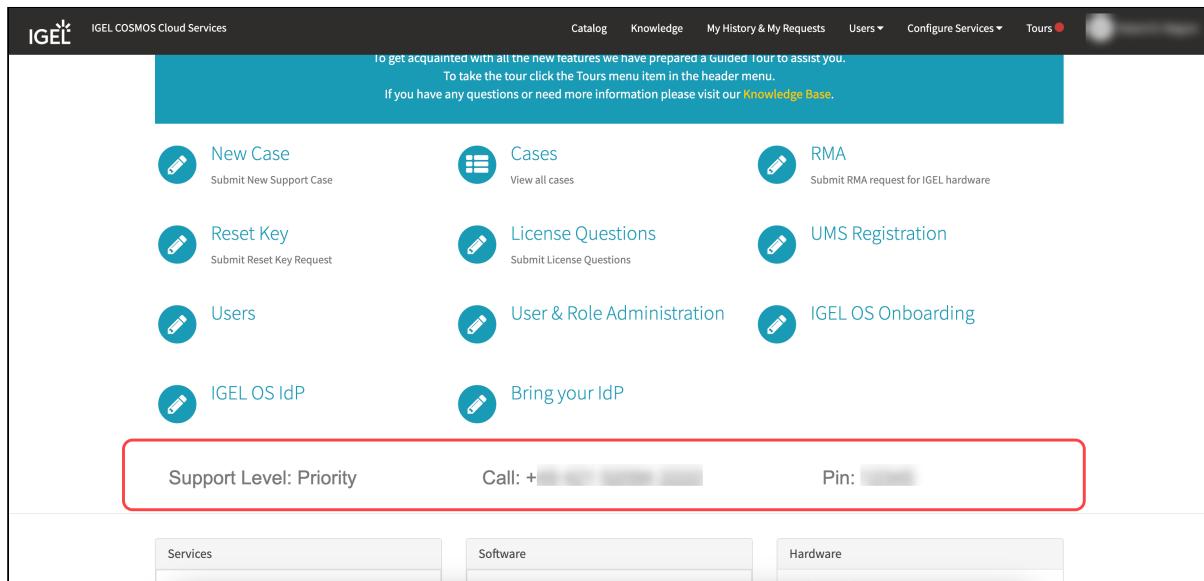


The screenshot shows a password reset form. At the top, the IGEL logo is displayed. Below it, a message states: "We have sent a password reset code by email to a***@a***. Enter it below to reset your password." A field labeled "Code" contains a redacted password reset code. Below this are two fields for entering a new password: "New Password" and "Enter New Password Again", both containing redacted entries. At the bottom is a large yellow button labeled "Change Password".

6. Confirm by clicking **Change Password**.

With the verified user data and the new password, you can now log in to the IGEL Customer Portal.

IGEL Support Information on the IGEL Customer Portal



If you have Priority or Plus support, you can find the following support information on the landing page after login:

- Support Level**
The level of support you have. You can find more information on support levels at <https://www.igel.com/support/>.
- Call**
Regional support number.
- PIN**
The PIN that you use for authentication during a support call.



Changes in Support Contact Information

Starting from 12 August 2024 a new phone system is introduced at IGEL Support. As a result, the following will change:

- New phone number to contact IGEL Support.
- New 8 digit authentication PIN. The new PINs are assigned to individual users and not to customer accounts and they will change periodically.

You will find the new information after login under **Call** and **PIN**.

Creating Support Cases in the IGEL Customer Portal for Different Environments

When submitting a new case, you need to select the type of your environment under **Is this a production environment?**

Is this a production environment? *

POC / POV Environment

-- None --
Production Environment
Test Environment
✓ POC / POV Environment

Select one of the three options using the drop-down menu:

- **Production Environment** - Your case is connected to a production environment. A production environment is a real-time setting where users are working with the software.
- **Test Environment** - Your case is connected to a test environment. A test environment is an internal environment, used to test, check, and validate new technology. The system is not used in production.
- **POC/POV Environment** - Your case is connected to an IGEL supported Proof of Concept (POC) or Proof of Value (POV) environment, where IGEL Presales and you are in touch.

Creating an RMA Request in the IGEL Customer Portal

You can submit a Return Material Authorization (RMA) request after registering for the IGEL Customer Portal.



The RMA request form is for IGEL hardware only.
If you would like to request an RMA for hardware produced by an IGEL partner, you need to refer to the vendor's RMA process.

1. Click **RMA** or **Request an RMA**.



2. Fill out the RMA form with the following information:

Mandatory fields:

- **Serial Number**
- **Complete description**
- **Delivery address** (for new, or repaired devices)

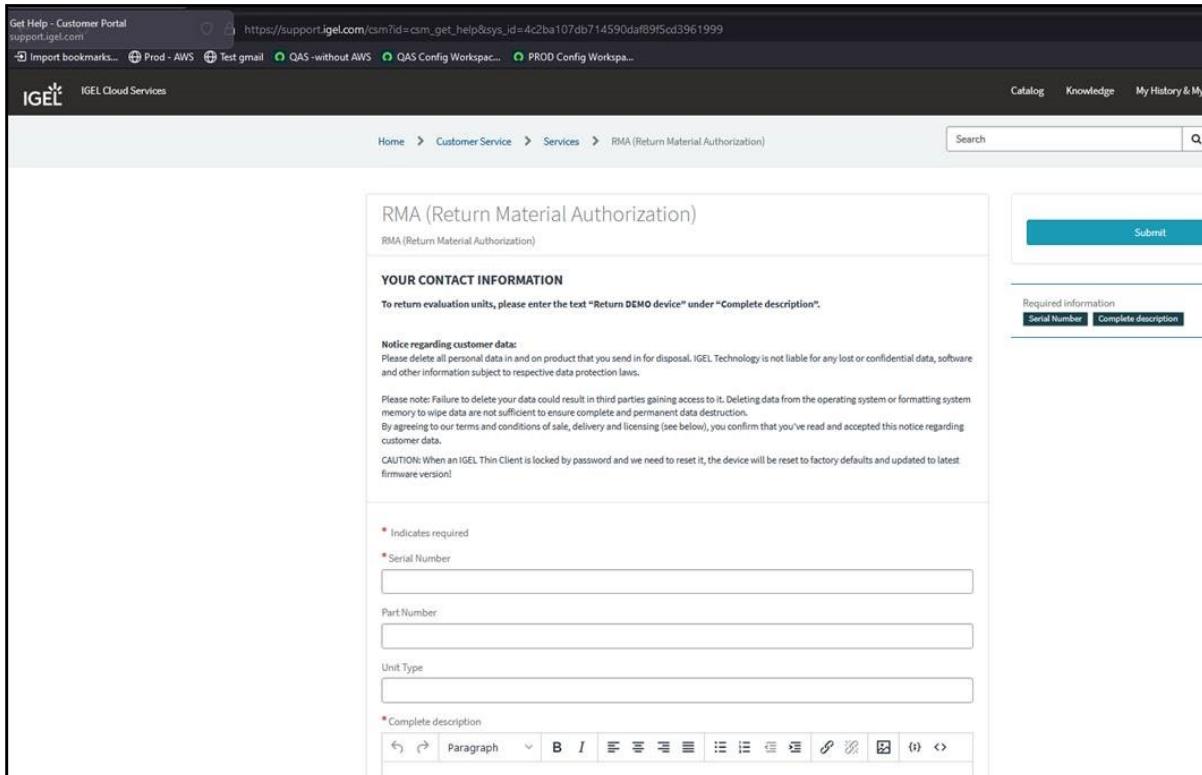


The delivery address must be checked as it is not updated automatically and gets taken from the customer's registered details.

Optional fields:

- **Part Number**
- **Unit Type**
- **“MORE THAN ONE DEVICE”**

If this drop-down is set to **Yes**, you can insert additional Serial Numbers of endpoints showing a similar issue.



The screenshot shows the 'RMA (Return Material Authorization)' page on the IGEL Customer Portal. The URL in the address bar is https://support.igel.com/csm?id=csm_get_help&sys_id=4c2ba107db714590dalb9f5cd3961999. The page header includes the IGEL logo and navigation links for Catalog, Knowledge, My History & My.

The main content area has a title 'RMA (Return Material Authorization)' and a sub-section 'YOUR CONTACT INFORMATION'. It asks to enter the text 'Return DEMO device' under 'Complete description'. There is a note about data deletion and a CAUTION about password-locked devices.

Form fields include:

- Serial Number (marked with an asterisk)
- Part Number
- Unit Type
- Complete description (with rich text editor toolbar)

A sidebar on the right is titled 'Required Information' and lists 'Serial Number' and 'Complete description'.

Managing Users and Roles in the IGEL Customer Portal

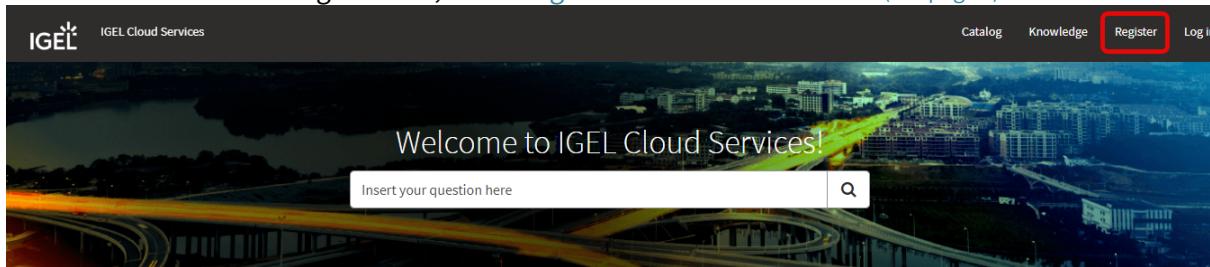
This article describes how to invite users, cancel or renew invitations, and add roles to a user or remove roles in the IGEL Customer Portal. Also included is a description of how to use Okta or Ping as federated identity providers (IdP) for logging in to your IGEL Cloud Services accounts.

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 Portal¹¹](#) > **Register** is your Super Admin account. For details on registration, see [Using 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
- App Creator
- Customer Support Account Manager

The users with these roles have the following permissions:

	Super Admin	Account Admin	OBS Admin	UMS Admin	App Creator	Customer Support Account Manager
Account Management						
View account	✓	✓				
User Management						
View users	✓	✓				
Invite users	✓	✓				
Add / remove user roles	✓	✓				
OBS IdP (Onboarding Service Identity Provider)						

11. <https://support.igel.com>

	Super Admin	Account Admin	OBS Admin	UMS Admin	App Creator	Customer Support Account Manager
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	✓			✓		
App Creator Portal						
Create apps via the IGEL App Creator Portal	✓				✓	
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 the [IGEL Customer Portal](#)¹², log in to your admin account, and select **Users > User & Role Administration**.

The screenshot shows the IGEL Customer Portal homepage. At the top, there is a navigation bar with links for Catalog, Knowledge, My History & My Requests, Advanced Service, and a dropdown menu labeled "Users". The "Users" dropdown menu is open, showing options: Overview, User & Role Administration (which is highlighted with a red box and has an arrow pointing to it), Bring your IdP, IGEL OS IdP, and My Profile. Below the navigation bar, there is a search bar with the placeholder "Insert your question here" and a search icon. The main content area features a "Welcome to IGEL" banner and a cityscape background.

2. Select **Invite new user**.

The screenshot shows the "User & Role Administration" page. At the top, there is a breadcrumb navigation: Home > Customer Service > Services > User & Role Administration. To the right is a search bar. The main form is titled "User & Role Administration" and contains a section for "User & Role Administration". It includes a dropdown field with "Please choose" and two buttons: "-- None --" and "Invite new User" (which is highlighted with a red box). Below this are buttons for "Add additional role" and "Remove role". On the right side of the form, there is a "Submit" button and a "Required information" section with a "Please choose" dropdown. A note at the top left says "* Indicates required".

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

12. <https://support.igel.com>

Managing Users and Roles in the IGEL Customer Portal



The screenshot shows the 'User & Role Administration' page. A red box highlights the input fields for First Name ('Ike'), Last Name ('Igel'), and E-Mail ('@igel.com'). The 'Submit' button is located in the top right corner of the form area.

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

The screenshot shows the 'User & Role Administration' page. A red box highlights the 'Select Role' dropdown menu, which contains the option 'OBS Admin'. The 'Submit' button is also highlighted with a red box. The rest of the form fields (First Name, Last Name, E-Mail) are identical to the previous screenshot.

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.

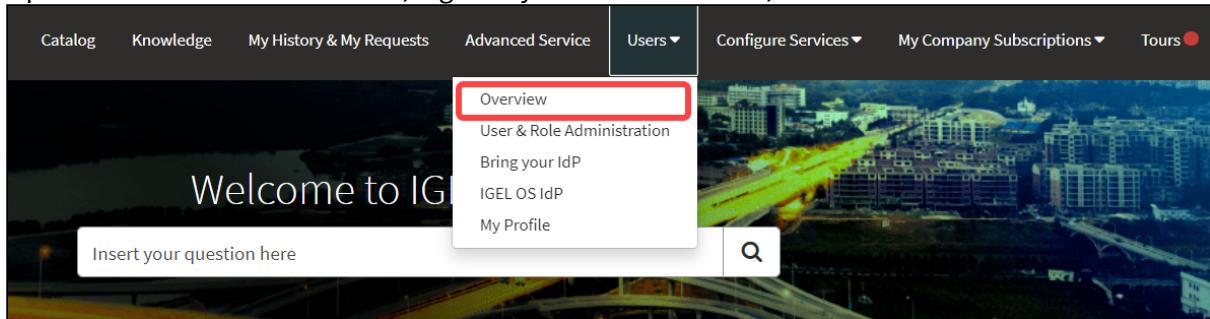
Canceling and Resending Invitations

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

- Super Admin
 - Account Admin

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

1. Open the **IGEL Customer Portal**¹³, log in to your admin account, and select **Users > Overview**.



The users are listed.

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

13. <https://support.igel.com>

Users						
All > Account =	Account	Email	Role	Active	Invitation Status	Action
	QAS Test Company	@igel.com	App Portal User	Pending	Pending	Resend Cancel
	QAS Test Company	1@igel.com	App Portal User	Yes	Accepted	
	QAS Test Company	[REDACTED]	App Portal User	Yes	Accepted	
	QAS Test Company	[REDACTED]t@igel.com	App Portal User	Yes	Accepted	

Adding a Role to an Existing User

1. Open the [IGEL Customer Portal](#)¹⁴, log in to your admin account, and select **Users > User & Role Administration**.

The screenshot shows the IGEL Customer Portal homepage. At the top, there is a navigation bar with links for Catalog, Knowledge, My History & My Requests, Advanced Service, and Users (with a dropdown arrow). Below the navigation bar is a search bar containing the placeholder "Insert your question here". A large banner in the center says "Welcome to IGEL". To the right of the banner is a sidebar with options: Overview, User & Role Administration (which is highlighted with a red box), Bring your IdP, IGEL OS IdP, and My Profile. A magnifying glass icon is also present in the sidebar.

2. Select **Add additional role**.

The screenshot shows the "User & Role Administration" page. At the top, there is a breadcrumb navigation: Home > Customer Service > Services > User & Role Administration. Below the breadcrumb is a search bar. The main area has a note "* Indicates required". It contains a form with a dropdown menu labeled "Please choose" with options like "... None ..." and "Add additional role" (which is highlighted with a red box). There is also a "Submit" button and a note "Required information Please choose".

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

14. <https://support.igel.com>

* Indicates required

User & Role Administration

User & Role Administration

* Please choose

Add additional role

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

[Red Box]

Submit

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

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

User & Role Administration

User & Role Administration

* Please choose

Add additional role

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

[Red Box]

Additional role

OBS Admin [Red Box]

Submit

The updated list of users is displayed.

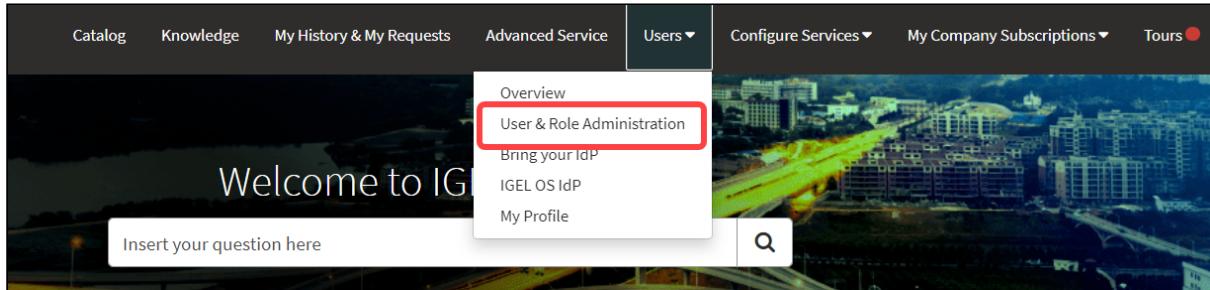
Users				
All > Account =	Email	Role	Active	Invitation Status
[Redacted]	[Redacted]	App Portal User	Yes	Accepted
[Redacted]	[Redacted]	OBS Admin	Yes	Accepted
[Redacted]	[Redacted]	OBS Admin	Pending	Pending
[Redacted]	[Redacted]	App Portal User	Yes	Accepted
[Redacted]	[Redacted]	OBS Admin	Pending	Pending
[Redacted]	[Redacted]	Account Admin	Yes	Accepted
[Redacted]	[Redacted]	Super Admin	Yes	

Rows 1 - 7 of 7

Removing a Role / Deactivating a User

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

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

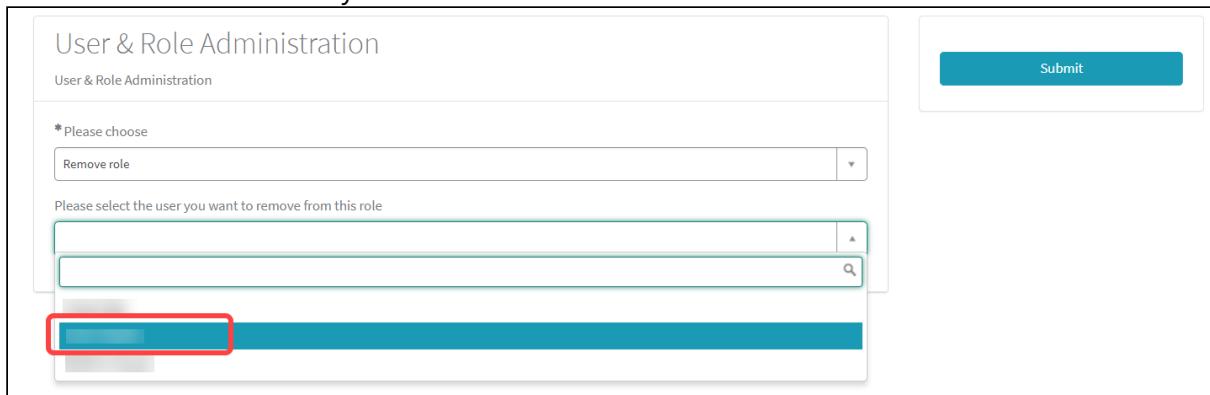


2. Select **Remove role**.



A screenshot of the 'User & Role Administration' page. The page has a header with 'User & Role Administration' and a sub-header 'User & Role Administration'. There is a note '* Please choose' above a dropdown menu. The dropdown menu has an option '-- None --' and a search bar. Below the dropdown, there are links: '-- None --', 'Invite new User', 'Add additional role', and a blue button labeled 'Remove role' which is highlighted with a red box. To the right, there is a 'Submit' button and a note 'Required information' with a 'Please choose' button.

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



A screenshot of the 'User & Role Administration' page. The page has a header with 'User & Role Administration' and a sub-header 'User & Role Administration'. There is a note '* Please choose' above a dropdown menu. The dropdown menu has an option 'Remove role' and a search bar. Below the dropdown, there is a note 'Please select the user you want to remove from this role' and a dropdown menu with several user names listed. One user name is highlighted with a red box. To the right, there is a 'Submit' button.

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

* Indicates required

User & Role Administration

User & Role Administration

* Please choose
Remove role

Please select the user you want to remove from this role
[User Selection]

* Please select the role you would like to add/remove for this user
[Role Selection]
Customer Support Account Manager

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

Submit

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

User & Role Administration

User & Role Administration

* Please choose
Remove role

Please select the user you want to remove from this role
[User Selection]

* Please select the role you would like to add/remove for this user
[Role Selection]
Customer Support Account Manager

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

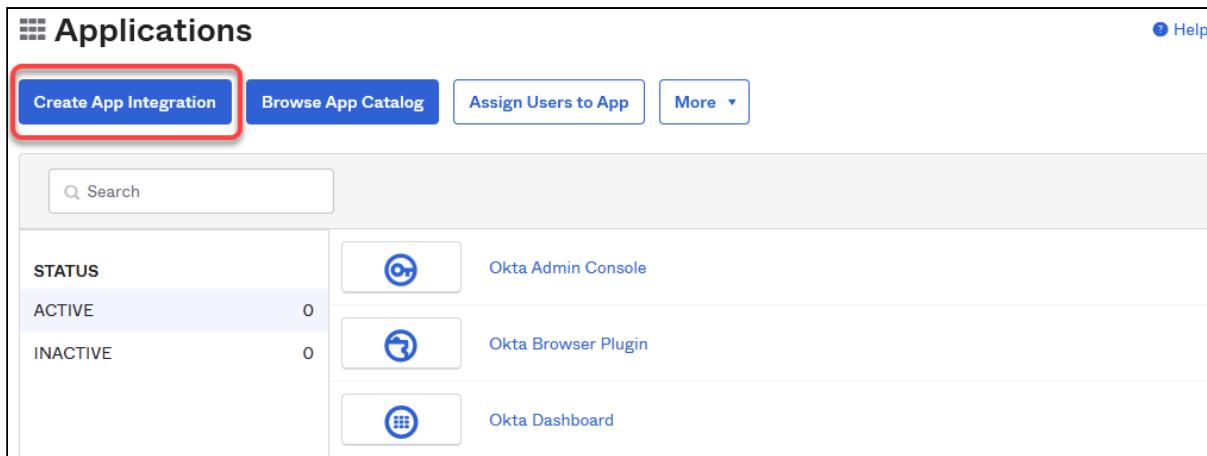
Submit

Using Okta as Federated Identity Provider

Setting Up an App Integration in Okta

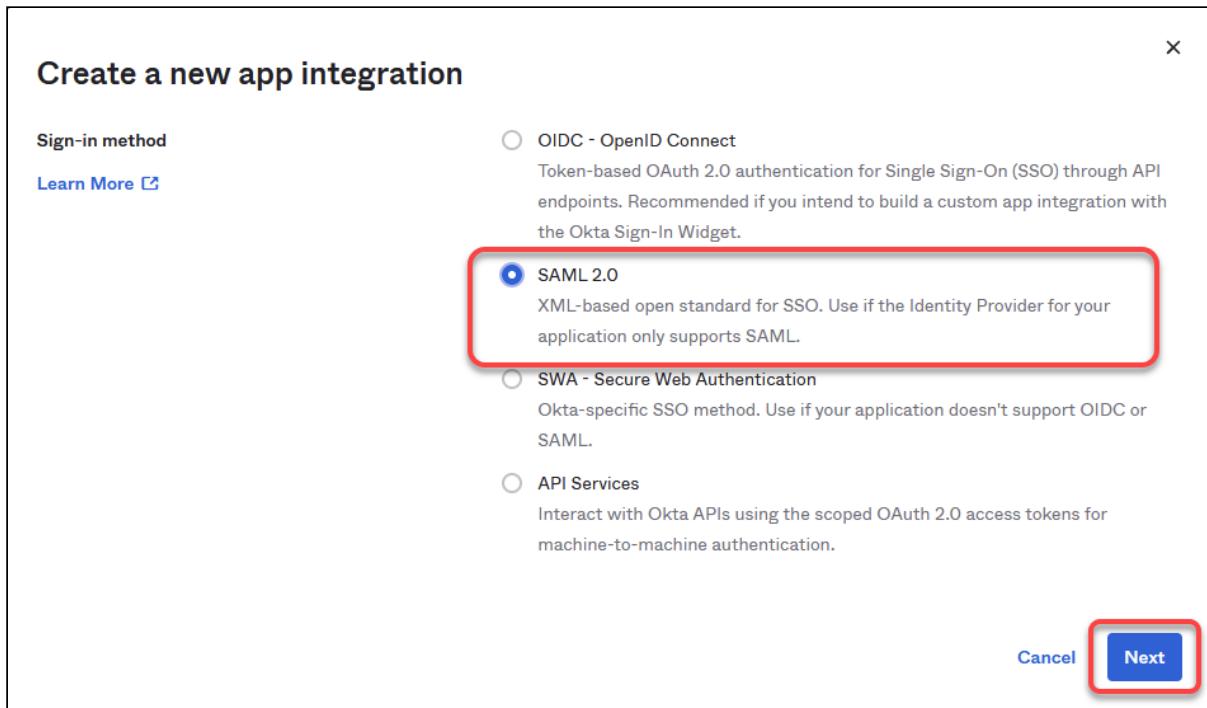
For federating identities from Okta to Azure Active Directory (AAD), which is used in IGEL Cloud Services, you must set up an application integration in your Okta tenant. For this purpose, we will create a SAML 2.0 application.

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



The screenshot shows the 'Applications' page. At the top, there are four buttons: 'Create App Integration' (highlighted with a red box), 'Browse App Catalog', 'Assign Users to App', and 'More'. Below the buttons is a search bar labeled 'Search'. A table follows, with columns 'STATUS', 'ACTIVE' (0), and 'INACTIVE' (0). It lists three items: 'Okta Admin Console' (with a user icon), 'Okta Browser Plugin' (with a lock icon), and 'Okta Dashboard' (with a globe icon).

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



The dialog title is 'Create a new app integration'. On the left, 'Sign-in method' is listed with a 'Learn More' link. On the right, four options are shown with descriptions:

- OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

At the bottom right are 'Cancel' and 'Next' buttons, with 'Next' highlighted by a red box.

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

Create SAML Integration

1 General Settings 2 Configure SAML

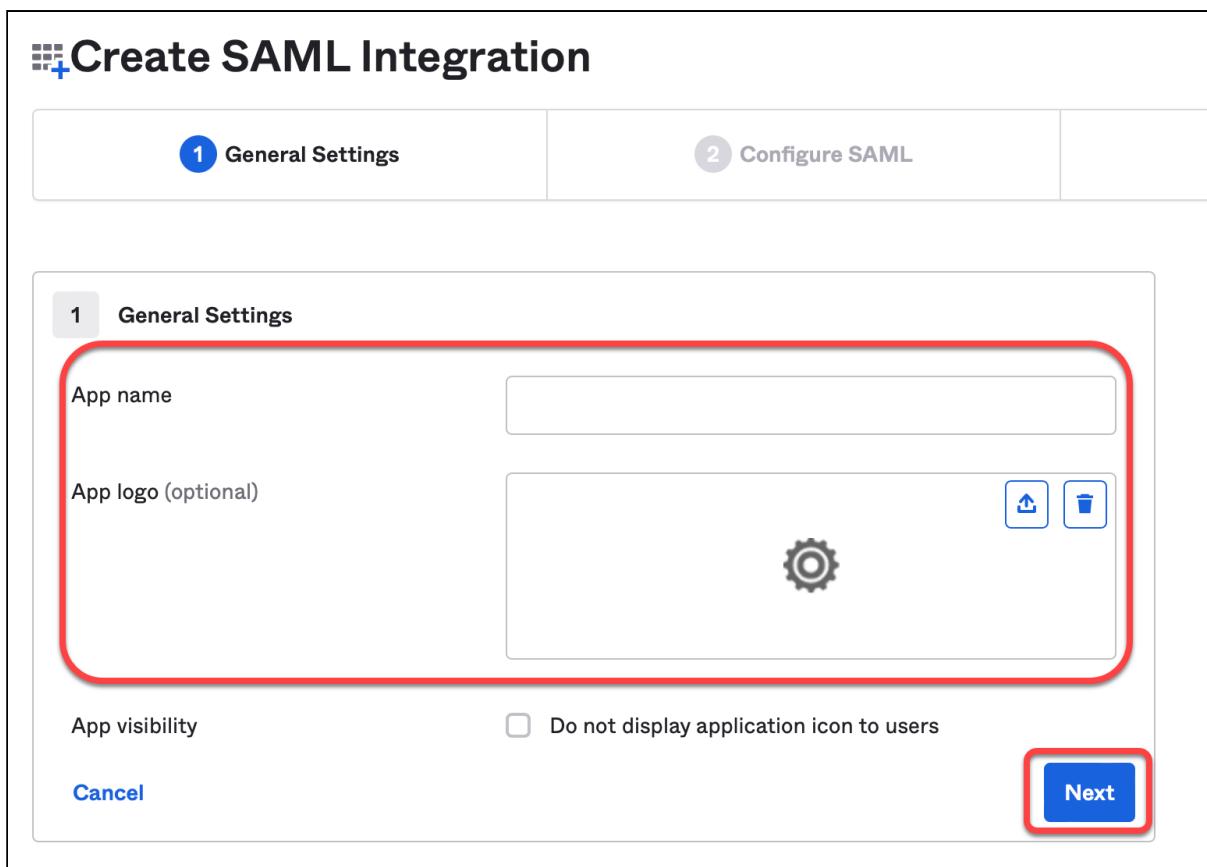
1 General Settings

App name

App logo (optional)  

App visibility Do not display application icon to users

[Cancel](#) [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`.

A SAML Settings

General

Single sign-on URL	<code>https://login.microsoftonline.com/login.srf</code>	<input checked="" type="checkbox"/> Use this for Recipient URL and Destination URL
Audience URI (SP Entity ID)	<code>urn:federation:MicrosoftOnline</code>	
Default RelayState	If no value is set, a blank RelayState is sent	
Name ID format	Unspecified	
Application username	Email	
Update application username on	Create and update	

5. Add the following attributes:

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

Attribute Statements (optional)

LEARN MORE

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

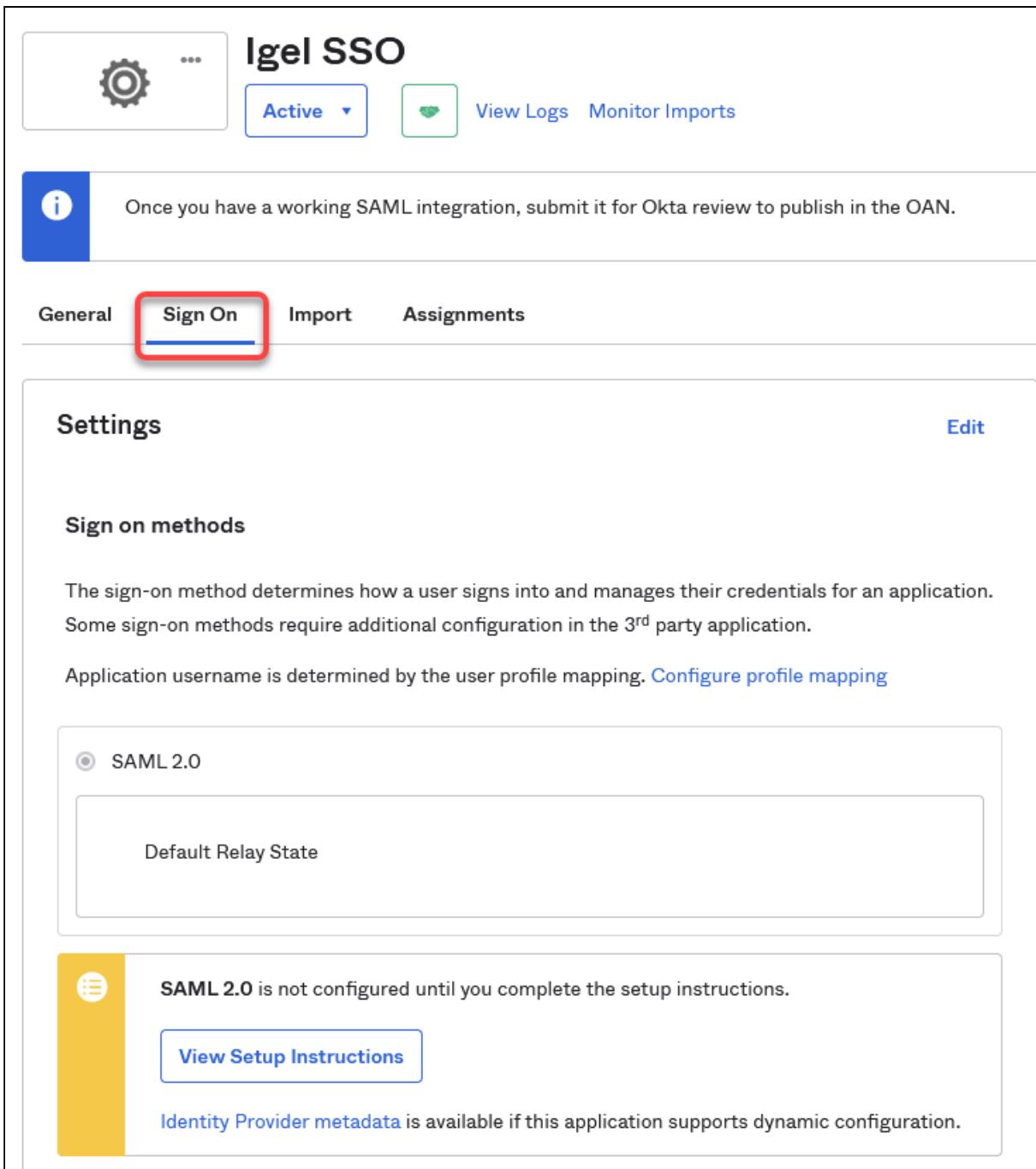
Add Another

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**.



The screenshot shows the Igel SSO configuration interface. At the top, there is a gear icon, a three-dot menu icon, and a status bar with "Active" and "View Logs Monitor Imports". Below this, a message says: "Once you have a working SAML integration, submit it for Okta review to publish in the OAN." The "Sign On" tab is highlighted with a red box. Under the "Settings" section, the "Sign on methods" heading is visible. It shows "SAML 2.0" selected. A "Default Relay State" input field is present. A yellow sidebar on the left indicates that "SAML 2.0 is not configured until you complete the setup instructions." It includes a "View Setup Instructions" button and a note about "Identity Provider metadata".

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

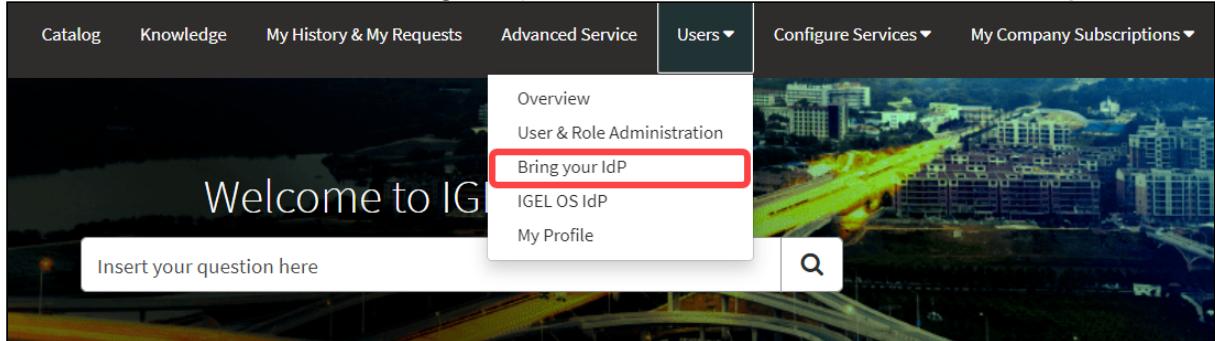
```

<md:EntityDescriptor entityID="http://www.okta.com/">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
            ...
          </ds:X509Certificate>
        </ds:KeyInfo>
      </md:KeyDescriptor>
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    </md:NameIDFormat>
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[REDACTED].okta.com/app/[REDACTED]_igelssso_1
    /[REDACTED]/sso/saml"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://[REDACTED].okta.com/app/[REDACTED]_igelssso_1
    /[REDACTED]/sso/saml"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>

```

Configuring Okta as Your Federated IdP

1. Open the [IGEL Customer Portal](#)¹⁵, log in to your admin account, and select **Users > Bring your IdP**.



2. Enter the following data from your metadata file:

- **Issuer URI:** Value of the attribute `entityID` of the

element `<md:EntityDescriptor>`

```

<md:EntityDescriptor entityID="http://www.okta.com/">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
            ...
          </ds:X509Certificate>
        </ds:KeyInfo>
      </md:KeyDescriptor>
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    </md:NameIDFormat>
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[REDACTED].okta.com/app/[REDACTED]_igelssso_1
    /[REDACTED]/sso/saml"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://[REDACTED].okta.com/app/[REDACTED]_igelssso_1
    /[REDACTED]/sso/saml"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>

```

15. <https://support.igel.com>

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

```

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

```

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

Bring your IdP

Register SAML connection data for federated IdPs

* Issuer URI
http://www.okta.com/[REDACTED]

* Passive authentication endpoint
https://[REDACTED].okta.com/app/_igelsso_1/[REDACTED]/sso/saml

Metadata URL
https://[REDACTED].okta.com/app/[REDACTED]/sso/saml/metadata

* Domain name of federating IdP
.okta.com

Associated Domains

Actions	Domain name
Add	Remove All
	No data to display

* Certificate

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

Bring your IdP

Register SAML connection data for federated IdPs

* Issuer URI

* Passive authentication endpoint

Metadata URL

* Domain name of federating IdP

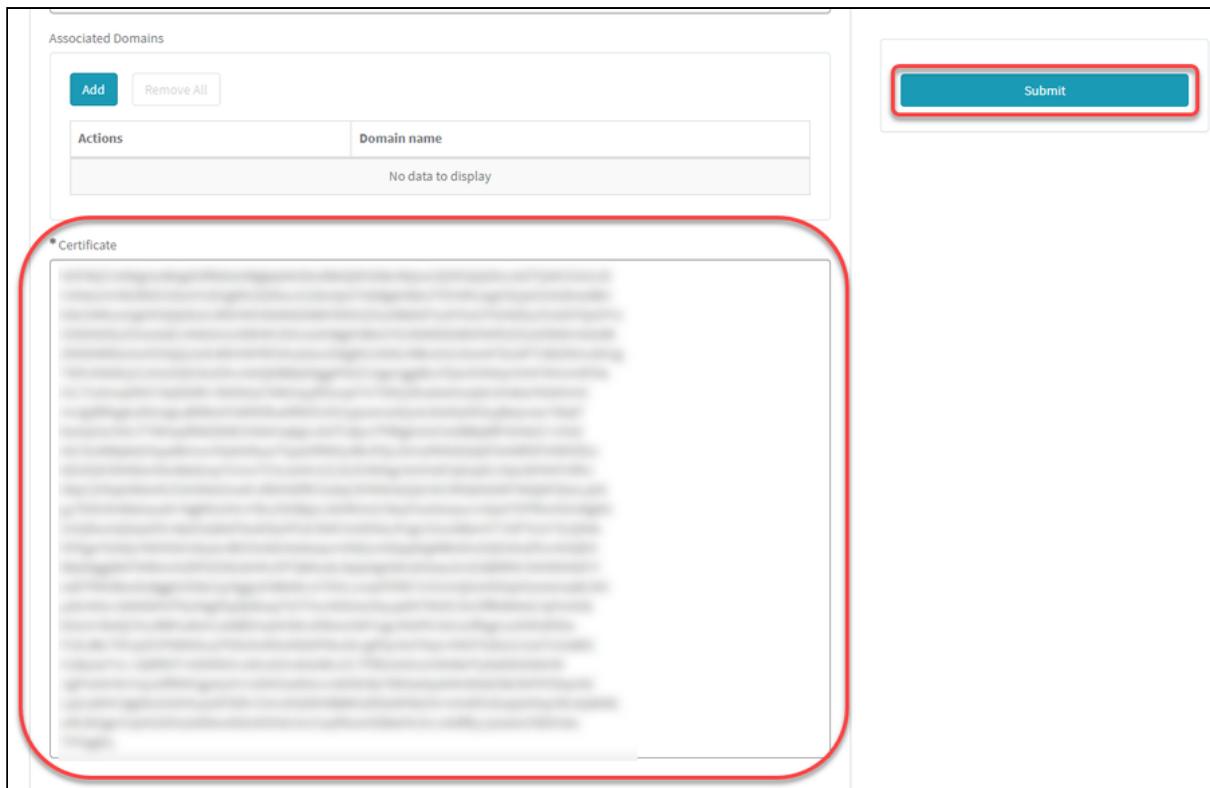
Associated Domains

Actions	Domain name
	No data to display

* Certificate

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

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

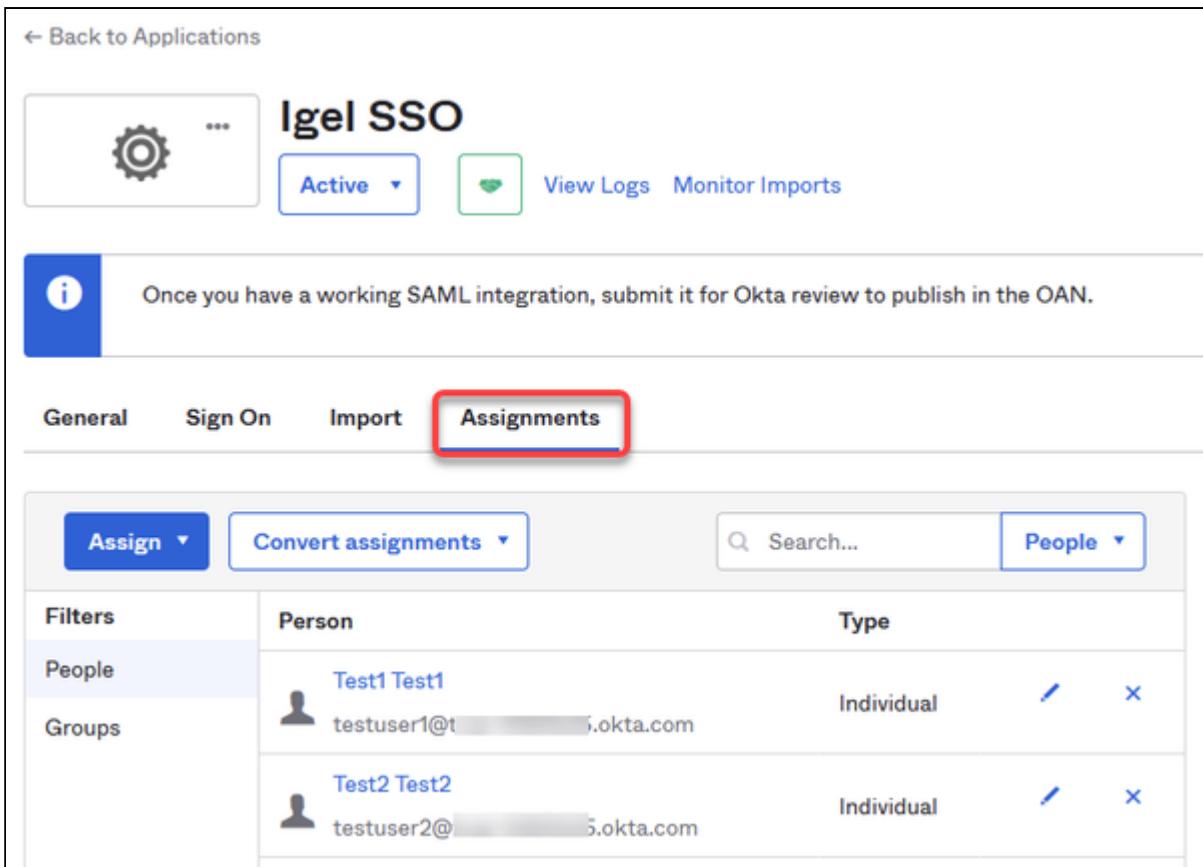


Assigning the Application to the Users

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

You can assign groups of users or single users.

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



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

Filters	Person	Type
People	Test1 Test1 testuser1@t...okta.com	Individual
Groups	Test2 Test2 testuser2@t...okta.com	Individual

2. Assign the users to our new application.

Using Ping as Federated Identity Provider

Setting Up an App Integration in Ping

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

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

The screenshot shows the PingIdentity application management interface. On the left, a sidebar menu includes sections like Environments, Administrators, Production, Applications (selected), Application Catalog, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. A red box highlights the 'Connections' section under Applications. On the right, the main panel shows a list of existing applications: AAD_APP, PingOne Admin C, PingOne Application, and PingOne Self-Service. A red box highlights the 'Applications +' button at the top of the list. The right side also features a 'Name and Describe Application' form with fields for Application Name (Test Application) and Description, and a file upload section for an icon. Below this is a 'Choose Application Type' section with four options: SAML Application, OIDC Web App, Single-Page, and Worker. The SAML Application option is highlighted with a blue border. Its details show it's a browser-accessed application using the SAML protocol. At the bottom, there are 'Configure' and 'Cancel' buttons.

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

The screenshot shows the PingIdentity application management interface. On the left, there is a sidebar with various navigation options like Connections, Applications, Application Catalog, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The 'Applications' option is selected.

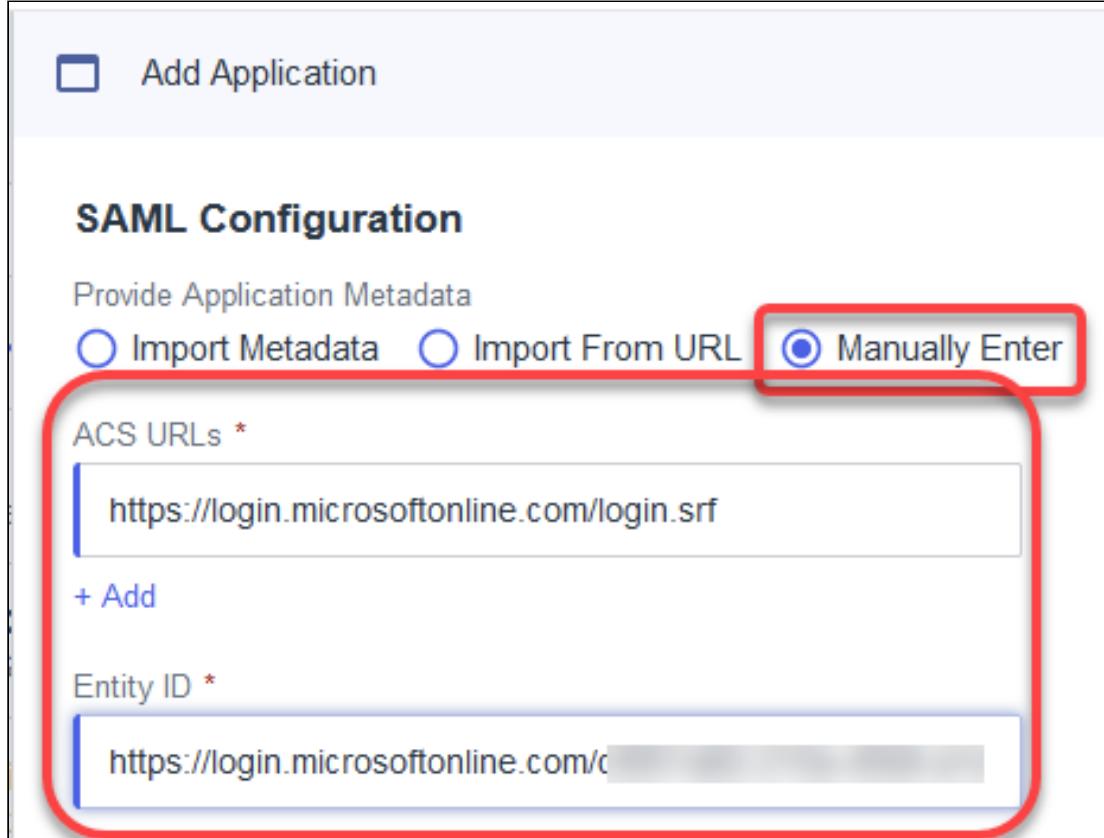
In the main area, there is a list of existing applications: AAD_APP, PingOne Admin C, PingOne Application, and PingOne Self-Service. Below this, there is a form for creating a new application:

- Name and Describe Application**: A red box highlights the "Application Name" field, which contains "Test Application".
- Description**: A text input field.
- Icon**: A placeholder for an icon upload.
- Choose Application Type**: A red box highlights the "SAML Application" option, which is described as "Applications that are accessed within a browser using the SAML protocol".
- OIDC Web App**: Described as "Web applications that are accessed within a browser using the OpenID Connect protocol".
- Single-Page**: Described as "Front-end applications that use an API to retrieve data".
- Worker**: Described as "Applications that can use the PingOne admin API".
- SAML Application**: A detailed description of the SAML application type.
- Configure**: A blue button at the bottom of the SAML Application section, which is also highlighted with a red box.
- Cancel**: A blue button next to the Configure button.

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.

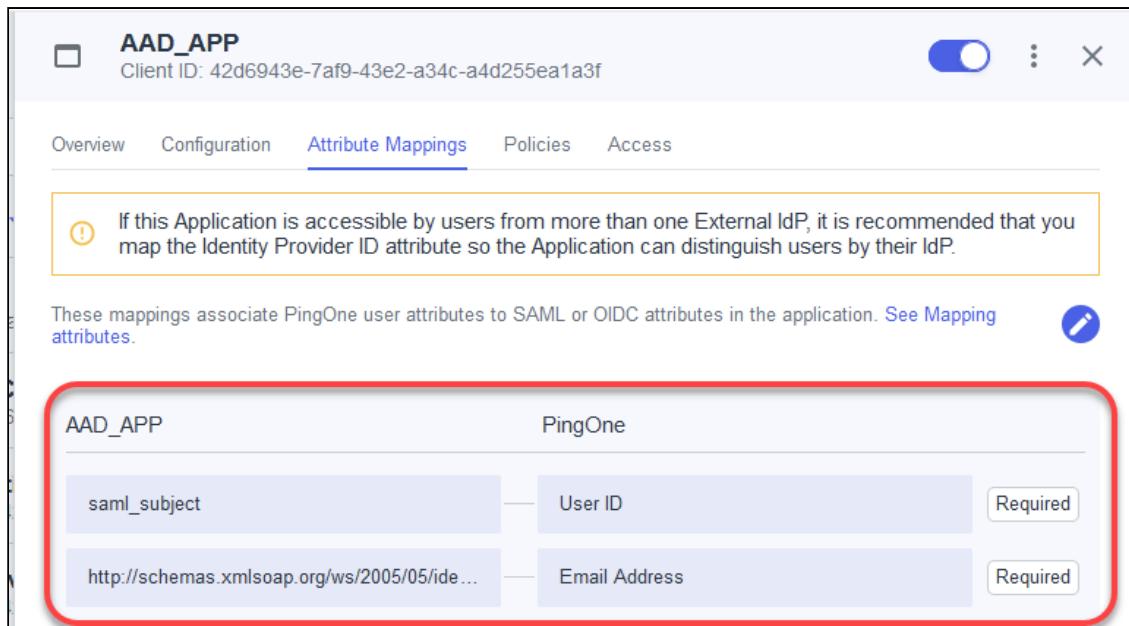


The screenshot shows the 'SAML Configuration' section of a web interface. At the top, there is a link to 'Add Application'. Below it, the title 'SAML Configuration' is displayed. A sub-section titled 'Provide Application Metadata' contains three radio button options: 'Import Metadata', 'Import From URL', and 'Manually Enter'. The 'Manually Enter' option is selected and highlighted with a red box. Below this, there are two input fields: 'ACS URLs *' containing the value 'https://login.microsoftonline.com/login.srf' and 'Entity ID *' containing the value 'https://login.microsoftonline.com/c...'. Both of these fields are also highlighted with red boxes.

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`.



The screenshot shows the 'Attribute Mappings' tab for the 'AAD_APP' application. It displays two mappings:

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

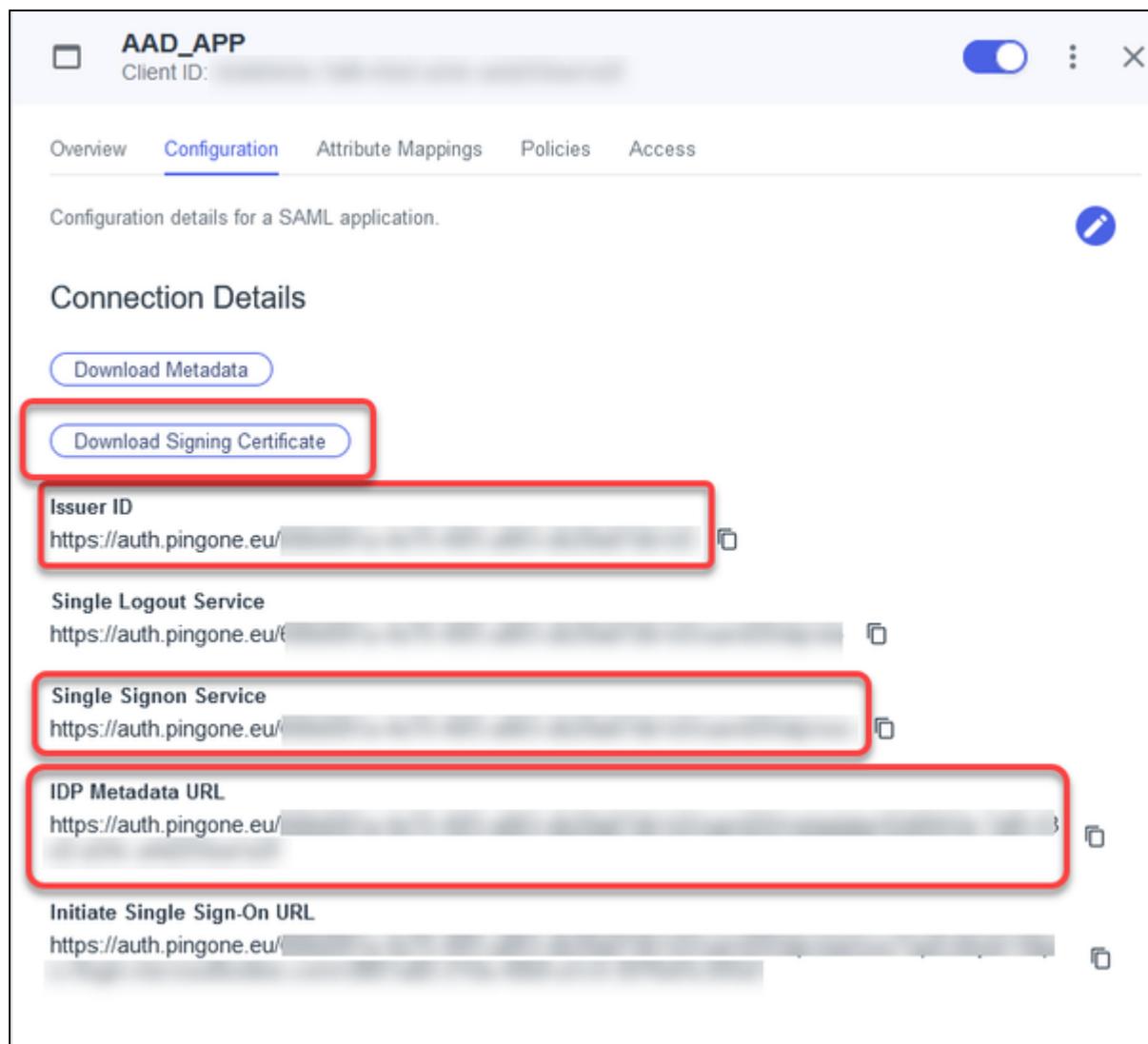
Both mappings are marked as 'Required'. A red box highlights the first mapping (saml_subject to User ID).

6. Finish the application setup.

Obtaining the SAML 2.0 Connection Data

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

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



AAD_APP
Client ID: [REDACTED]

Overview Configuration Attribute Mappings Policies Access

Configuration details for a SAML application.

Connection Details

Download Metadata

Download Signing Certificate

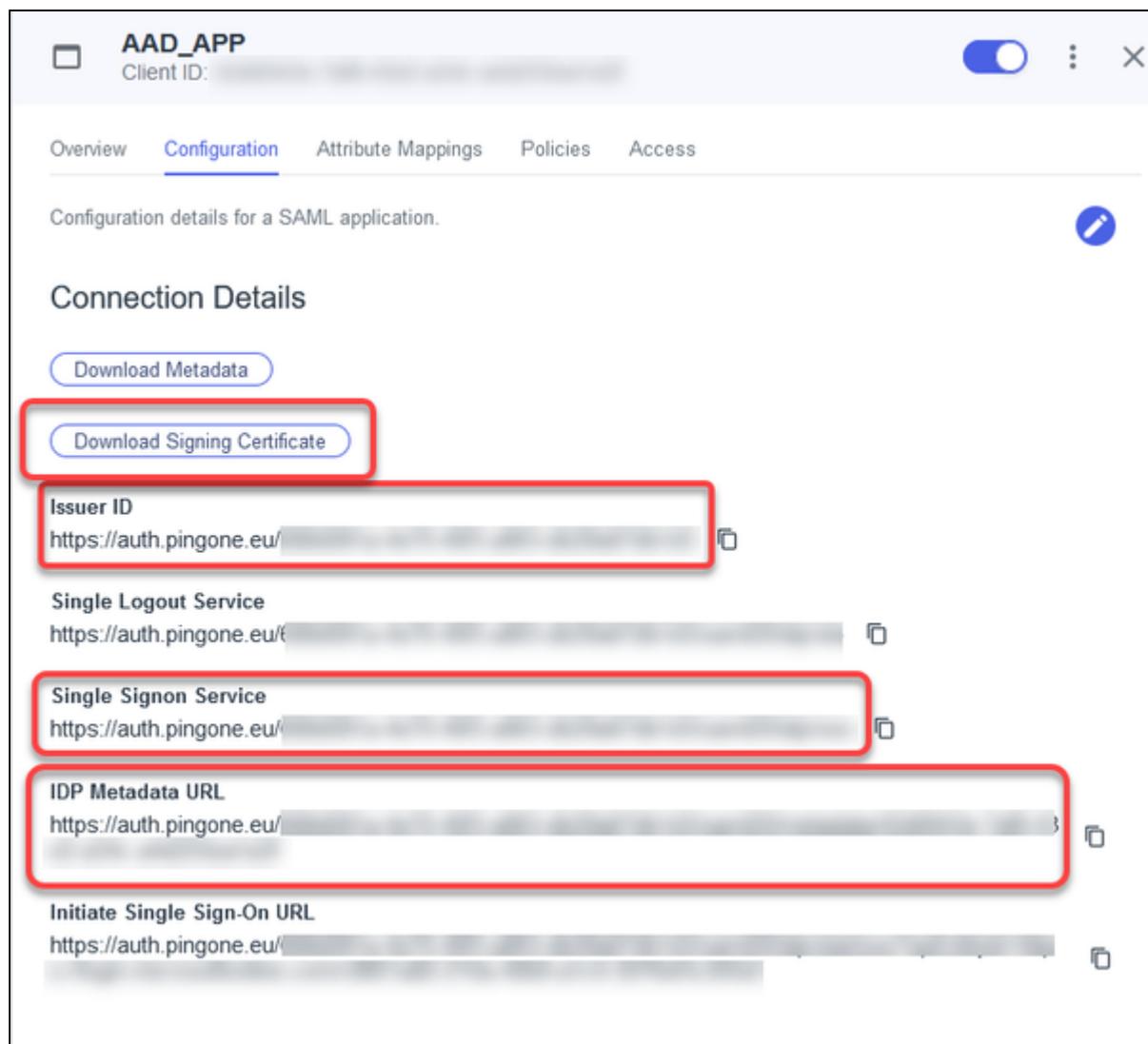
Issuer ID
https://auth.pingone.eu/ [REDACTED]

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

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

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

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



AAD_APP
Client ID: [REDACTED]

Overview Configuration Attribute Mappings Policies Access

Configuration details for a SAML application.

Connection Details

Download Metadata

Download Signing Certificate

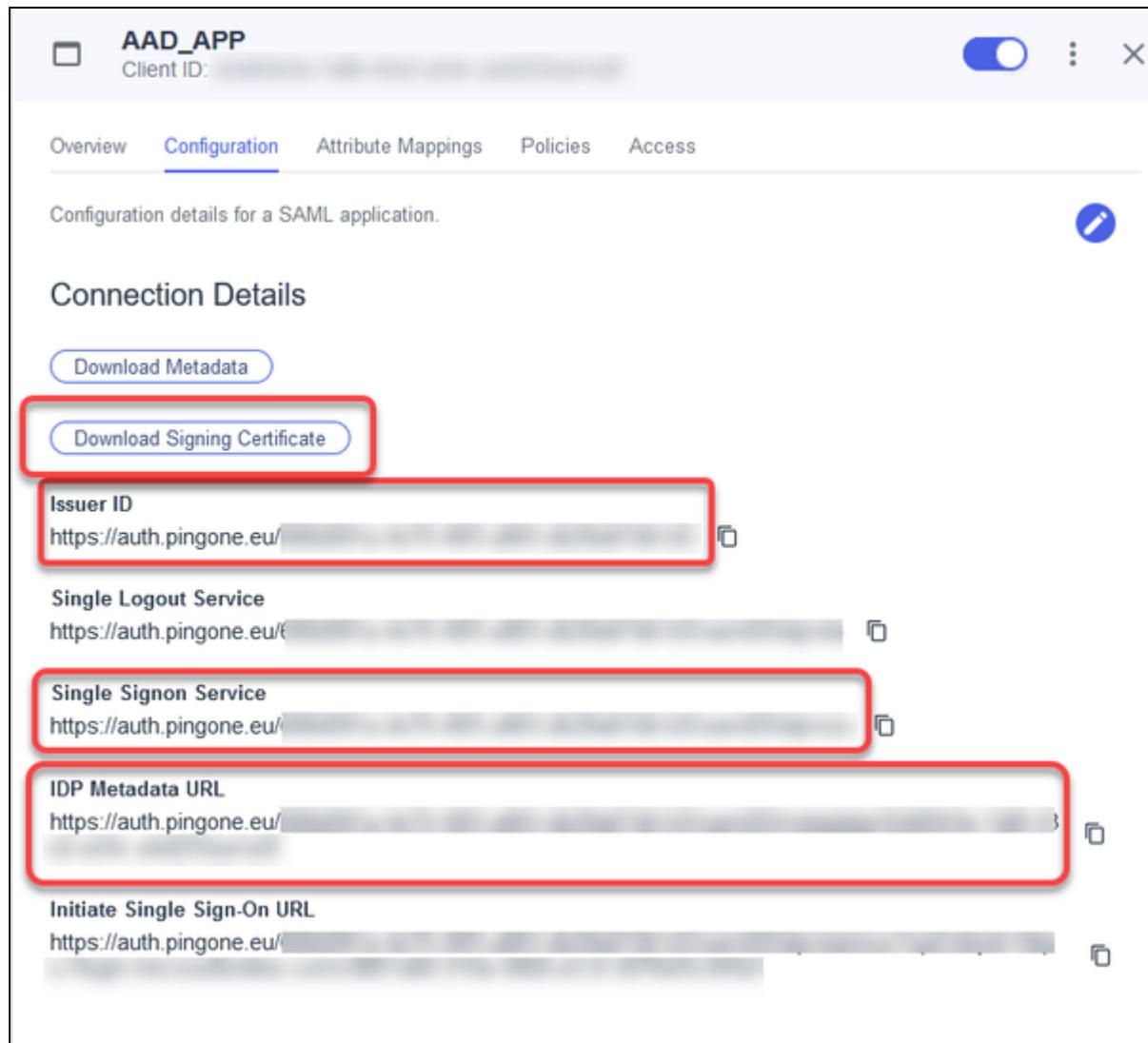
Issuer ID
https://auth.pingone.eu/ [REDACTED]

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

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

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

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



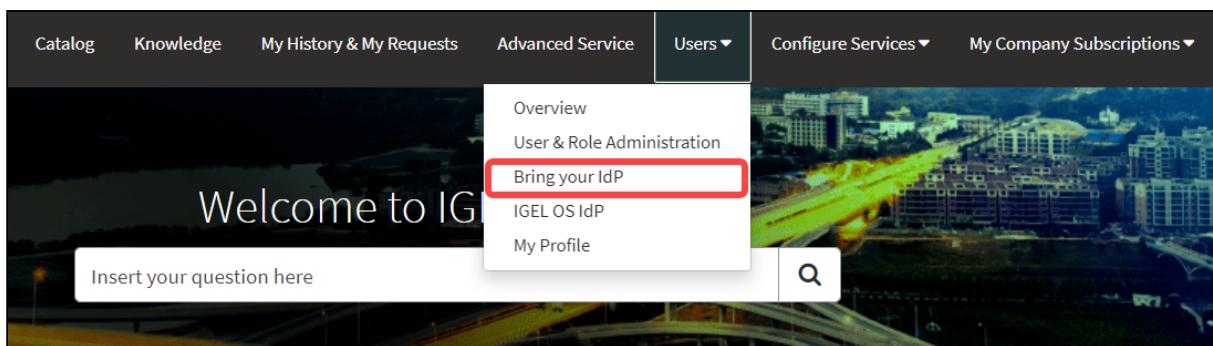
The screenshot shows the 'Configuration' tab of a SAML application named 'AAD_APP'. The 'Connection Details' section contains several configuration fields:

- Download Metadata** (button)
- Download Signing Certificate** (button, highlighted with a red box)
- Issuer ID**: https://auth.pingone.eu/ (text input field, highlighted with a red box)
- Single Logout Service**: https://auth.pingone.eu/ (text input field)
- Single Signon Service**: https://auth.pingone.eu/ (text input field, highlighted with a red box)
- IDP Metadata URL**: https://auth.pingone.eu/ (text input field, highlighted with a red box)
- Initiate Single Sign-On URL**: https://auth.pingone.eu/ (text input field)

Configuring Ping as Your Federated IdP

1. Open the [IGEL Customer Portal](#)¹⁶, log in to your admin account, and select **Users > Bring your IdP**.

16. <https://support.igel.com>



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.

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 before and during the installation / update.

Before Installation / Upgrade

UMS Licensing

The feature-based licensing model for the IGEL UMS is released with UMS version 12.07.100. With the feature-based license model, UMS features are activated based on the deployed UMS License. For details, see [IGEL Software Licenses for IGEL OS and IGEL UMS](#)¹⁷.

- i The IGEL UMS can be installed without a technical license, providing access to features of the Essential UMS License. You need a UMS License to unlock Standard and Enterprise features of the UMS. For details, see [IGEL OS Editions](#)¹⁸.

Update Requirements

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 of the IGEL UMS](#)¹⁹.

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](#)²⁰. 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.

- ! 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):

17. <https://kb.igel.com/en/igel-subscription-and-more/current/igel-software-licenses-for-igel-os-and-igel-ums>

18. <https://kb.igel.com/en/igel-subscription-and-more/current/igel-os-editions>

19. <https://kb.igel.com/en/universal-management-suite/current/creating-a-backup-of-the-igel-ums>

20. <https://kb.igel.com/en/universal-management-suite/current/igel-cloud-gateway-vs-reverse-proxy-for-the-commun>

- 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 [Prerequisites for Installing IGEL Cloud Gateway²¹](#).

Installing / Upgrading the IGEL UMS

1. Download IGEL UMS 12 from the [IGEL Download Server²²](#).
2. Consider the installation requirements, see [Sizing Guidelines for IGEL UMS 12 and IGEL OS 12²³](#) and [Installation Requirements for the IGEL UMS²⁴](#).
If you are going to upgrade your existing UMS installation, see also [IGEL UMS Update²⁵](#).
3. Install / update the UMS. Depending on your needs, you can install standard UMS, Distributed UMS, or UMS High Availability.
When selecting the installed components, 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.

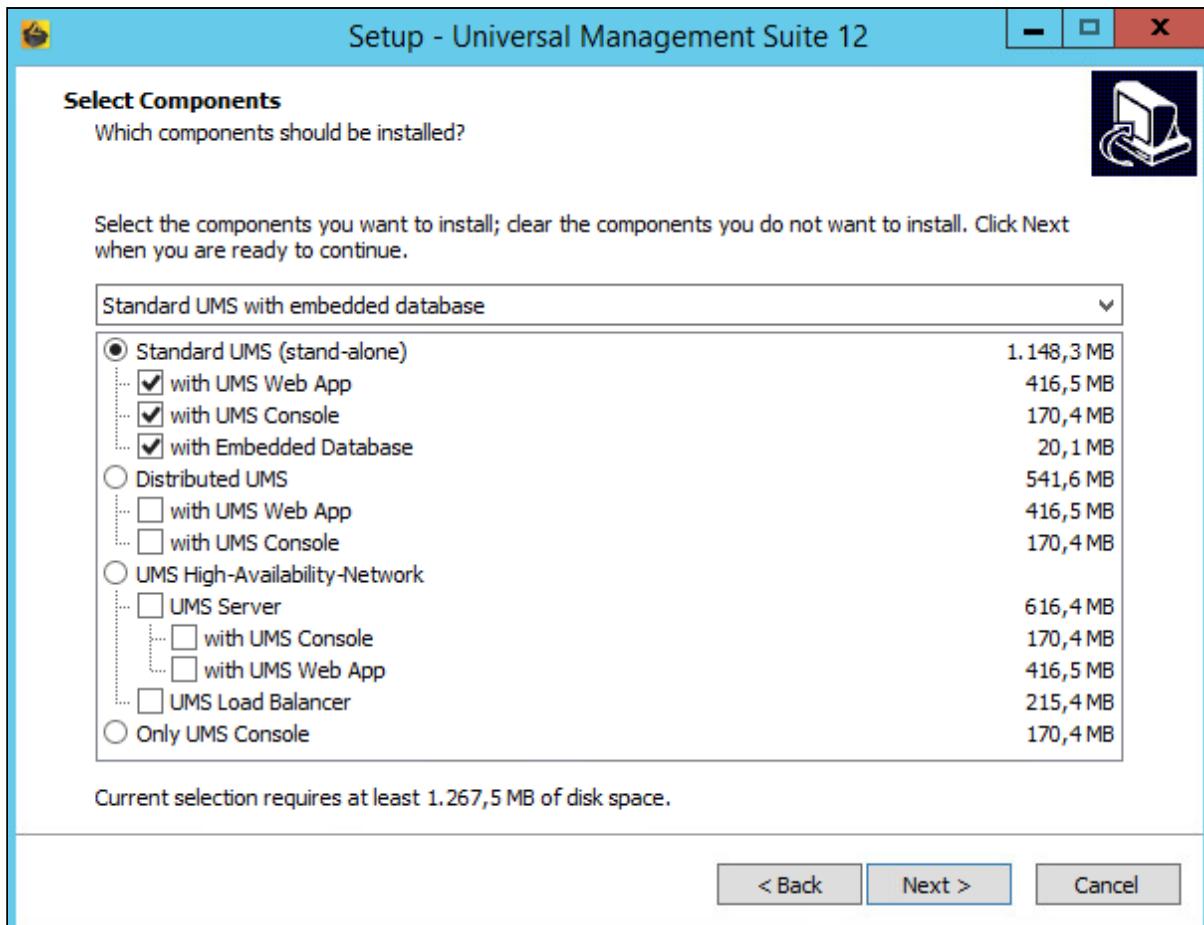
21. <https://kb.igel.com/en/igel-cloud-gateway/current/prerequisites-for-installing-igel-cloud-gateway>

22. <https://www.igel.com/software-downloads/>

23. <https://kb.igel.com/en/universal-management-suite/current/sizing-guidelines-for-igel-ums-12-and-igel-os-12>

24. <https://kb.igel.com/en/universal-management-suite/current/installation-requirements-for-the-igel-ums>

25. <https://kb.igel.com/en/universal-management-suite/current/igel-ums-update>



Detailed Instructions

Detailed information on how to install the UMS can be found under:

Windows: [IGEL UMS Installation under Windows²⁶](#)

Linux: [IGEL UMS Installation under Linux²⁷](#)

Post Installation Configurations: [Post-Installation Configuration of the IGEL UMS Server²⁸](#)

⚠ 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 [Troubleshooting Invalid Web Certificate and Errors by Device Registration after the Installation of the IGEL UMS 12 on Linux²⁹](#).

26. <https://kb.igel.com/en/universal-management-suite/current/igel-ums-installation-under-windows>

27. <https://kb.igel.com/en/universal-management-suite/current/igel-ums-installation-under-linux>

28. <https://kb.igel.com/en/universal-management-suite/current/post-installation-configuration-of-the-igel-ums-server>

29. <https://kb.igel.com/en/universal-management-suite/current/troubleshooting-invalid-web-certificate-and-errors>

Detailed information on how to upgrade the UMS can be found under:

Windows: Updating the IGEL UMS under Windows³⁰

Linux: How to Update the IGEL UMS under Linux³¹

i For Update Installations Only

As of UMS 12, the 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](#)³².

- ✓ 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 in IGEL UMS](#)³³. See also [User Management and IdP Management](#) in the IGEL UMS Web App³⁴.

Network Changes - 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 [Configure the UMS to Integrate Reverse Proxy with SSL Offloading](#)³⁵) 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.

30. <https://kb.igel.com/en/universal-management-suite/current/updating-the-igel-ums-under-windows>

31. <https://kb.igel.com/en/universal-management-suite/current/how-to-update-the-igel-ums-under-linux>

32. <https://kb.igel.com/en/universal-management-suite/current/known-issues-ums-12-01-110>

33. <https://kb.igel.com/en/universal-management-suite/current/general-administrator-rights-in-igel-ums>

34. <https://kb.igel.com/en/universal-management-suite/current/user-management-and-idp-management-in-the-igel-ums>

35. <https://kb.igel.com/en/universal-management-suite/current/configure-the-ums-to-integrate-reverse-proxy-with->

- 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 Ports³⁶](#).

⚠ 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.

i 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 UMS³⁷](#).

36. <https://kb.igel.com/en/universal-management-suite/current/igel-ums-communication-ports>

37. <https://kb.igel.com/en/universal-management-suite/current/server-network-settings-in-the-igel-ums>

Registering the UMS

To authenticate your IGEL Universal Management Suite (UMS) to the IGEL Cloud Services and the IGEL License Portal (ILP), you must register your UMS. This involves uploading the UMS ID, essentially a certificate of your UMS, to the IGEL Customer Portal and the ILP.

Exporting the UMS ID

To upload the UMS ID, we must export it from the UMS. For details, see [How to Export the UMS ID³⁸](#).

Registering the UMS in the IGEL License Portal (ILP)

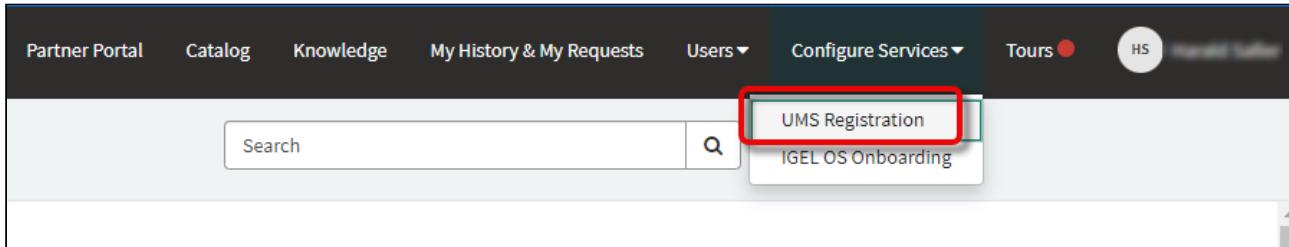
For a step-by-step guide, see [How to Register the UMS ID in ILP³⁹](#).

Registering the UMS in 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.

1. Open the [IGEL Customer Portal⁴⁰](#) in your browser and log in to your admin account.

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



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

38. <https://kb.igel.com/en/universal-management-suite/current/how-to-export-the-ums-id>

39. <https://kb.igel.com/en/igel-subscription-and-more/current/how-to-register-the-ums-id-in-ilp>

40. <https://support.igel.com/>

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
[REDACTED]	[REDACTED]	2042-04-09 11:03:49	[REDACTED]	...	true	[REDACTED]	2023-02-09 12:07:23
[REDACTED]	[REDACTED]	2042-04-09 06:10:55	[REDACTED]	...	true	[REDACTED]	2023-02-09 11:39:19
[REDACTED]	[REDACTED]	2042-04-07 15:08:18	[REDACTED]	2...	true	[REDACTED]	2023-02-06 15:02:02
[REDACTED]	[REDACTED]	2042-03-28	[REDACTED]	3...	true	[REDACTED]	2023-02-23 2023-02-03

4. Edit the data as follows:

- **UMS Name:** Display name for your UMS
- **Comments:** Optional comment
- **Enable App Portal:** Must be activated to enable access to the App Portal by the UMS. Technically, this option allows the App Portal to request the UMS ID.
- **Enable Insight Service:** Allows the Insight Service to collect analytical and usage data for further improvement and inform you about available updates. For details, see [IGEL Insight Service](#) (see page 217).
- **Required - Upload:** Upload the certificate file (UMS ID) of your UMS. Make sure that the certificate file has the extension `.cer`, `.crt`, or `.pem`

UMS Registration

Register your UMS instance and upload your X.509 certificate

This item only works with OS12

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

*Display Name

Comments

Options
 Enable App Portal
 Enable Insight Service

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

UMS_ID.crt

Submit

5. Click **Submit**.

UMS Registration

Register your UMS instance and upload your X.509 certificate

This item only works with OS12

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

* Display Name
UMS Ike

Comments
This UMS belongs to Ike

Options
 Enable App Portal
 Enable Insight Service

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

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

UMS Management

All > Account = 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	[Redacted]	2042-04-09 06:10:55	[Redacted]	true	[Redacted]	2023-04-14 12:28:39	2023-04-14 12:28:39
[Redacted]	[Redacted]	2042-05-19 10:10:47	[Redacted]	..	true	2023-03-31 11:45:02	2023-04-11 14:28:42
[Redacted]	[Redacted]	2042-06-04 12:10:30	[Redacted]	true	[Redacted]	2023-04-11 11:27:51	2023-04-11 11:27:51

Initial Configuration of the IGEL Onboarding Service (OBS)

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

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

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

1. [Activating the Onboarding Service \(OBS\) \(see page 58\)](#)
2. [Configuring the Identity Provider \(see page 58\)](#)
3. [Downloading the Root Certificate Chain of the UMS / ICG \(see page 59\)](#): The root certificate chain is needed for defining the route to the appropriate UMS / ICG.
4. [Creating the Record Set for the OBS Routing \(see page 62\)](#): Define the route to the appropriate UMS / ICG. This includes linking our Microsoft Entra ID user to the UMS / ICG.

Activating the Onboarding Service (OBS)

- i** 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](#)⁴¹.
2. From the menu, select **Activate IGEL OS Onboarding**.

Configuring the Identity Provider

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

- [Microsoft Entra ID \(see page 71\)](#)
- [Okta \(see page 94\)](#)
- [Ping Identity \(see page 106\)](#)
- [Other Identity Provider \(see page 118\)](#)

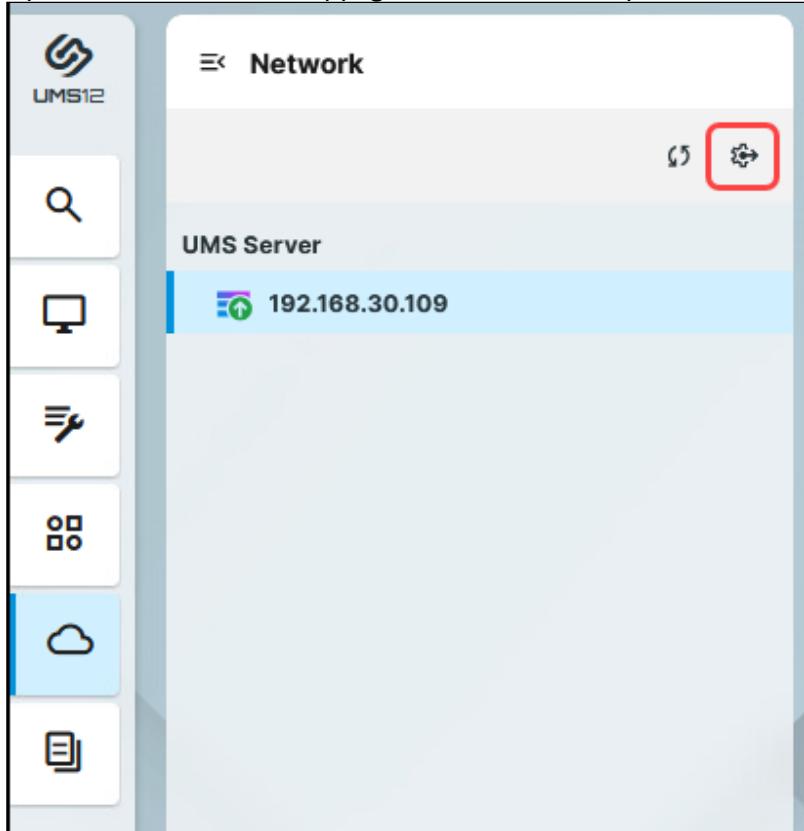
41. <https://support.igel.com/>

Downloading the Root Certificate Chain

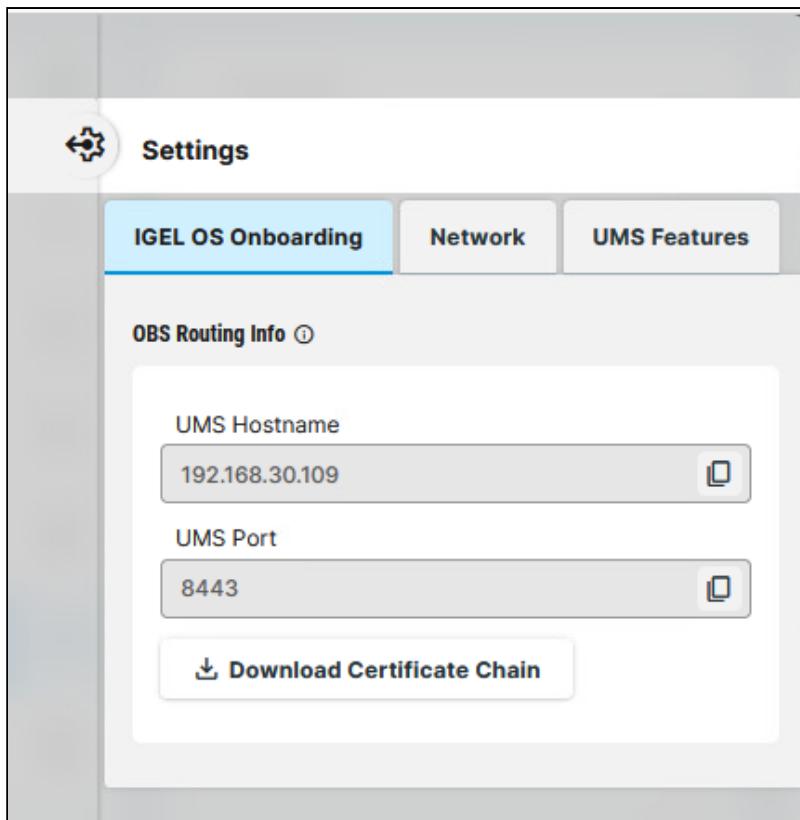
If your UMS is to be connected directly to your endpoint devices, you download the certificate chain of the UMS; see [Of the UMS \(see page 59\)](#). If your UMS is to be connected via ICG, you download the certificate chain of the ICG; [Of the ICG \(see page 60\)](#).

Of the UMS

1. Open the IGEL UMS Web App, go to **Network** and open the **Settings**.



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. Open the IGEL UMS Web App, go to **Network**, and select the ICG server to which you want to connect the OBS under **IGEL Cloud Gateway**.

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

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

IGEL Cloud Gateway Details

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

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

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

The screenshot shows the UMS Administration interface with the 'Cloud Gateway' section selected. In the 'Certificates' table, the 'Intermediate Certificate' is highlighted. A context menu is open over this certificate, with the 'Export certificate' option clearly visible and highlighted with a red box.

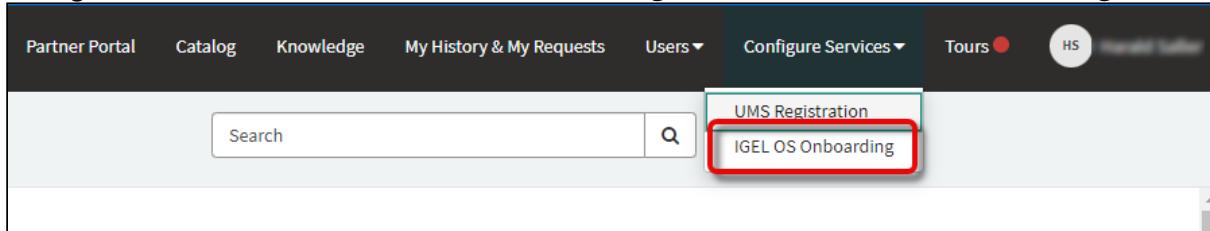
5. Copy the contents of each exported certificate in one file (the order of the certificates does not matter) and save the file as `icg_chain.crt`.

Example:

```
-----BEGIN CERTIFICATE-----  
MIIFPTCCAyWgAwIBAgIFAIGKvrEwDQYJKoZIhvcNAQELBQAwVzEkMCIGA1UEAwwbSUQ  
tLTQ5NzE2  
LTE20DE5NzkyNDEwOTYtOC0wMQ0wCwYDVQQKDARJR0VMMRMwEQYDVQQHDAoxNDAxODM  
1MDYyMQsw  
.....  
jqzhUGI+dZyTguXkzM2T4ACJUVm7G3mWDSCuMpt5laaE8kGEB2J6cbY9qV4QA5giCKF  
01PgJ6mZ  
3kDHoNX9DlKSyJtAWS6CJaaGWMWX0wtuyEQ5sZ81UhGKnQ==  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
MIIFMDCCAxiAwIBAgIFAPAz/  
aEwDQYJKoZIhvcNAQELBQAwVzEkMCIGA1UEAwwbSUQtLTQ5NzE2  
LTE20DE5NzkyNDEwOTYtOC0wMQ0wCwYDVQQKDARJR0VMMRMwEQYDVQQHDAoxNDAxODM  
1MDYyMQsw  
.....  
wy/  
0Y3S4LVHhWtAiT1dBza97uWk9zKL65HbwPFwwZ021Pjb2NaWJPL+OEAHPk5eamCmFzJ  
eUQqe  
0pwHv6AgvJyfEuxsMHURs98psMhW  
-----END CERTIFICATE-----
```

Creating the Record Set for the OBS Routing

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



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

IGEL OS Onboarding Management							
All > Account = Test Company				Replace X.509 Certificate	Update Mapped Domains	Update Mapped Users	Register IGEL OS Onboarding
Display Name	UMS Hostname	UMS Port	Created by	OBS Root Certificate	Created	Fingerprint	Expiration date
[REDACTED]	[REDACTED]	8443	[REDACTED]	[REDACTED]	2022-11-12 23:30:18	[REDACTED]	2042-11-12 10:00:31
[REDACTED]	[REDACTED]	8443	[REDACTED]	[REDACTED]	2022-10-05 10:08:18	[REDACTED]	2042-09-28 02:18:51
[REDACTED]	[REDACTED]	8443	[REDACTED]	[REDACTED]	2022-10-27 19:05:09	[REDACTED]	2023-11-10 20:44:53
[REDACTED]	[REDACTED]	8443	[REDACTED]	[REDACTED]	2022-11-04 09:59:13	[REDACTED]	2042-11-04 05:52:44

3. Enter the following data:

- **Display Name:** Display name for the UMS to which our user's device will be routed.
- **UMS Hostname:** Hostname (Fully Qualified Domain Name) or IP address of the UMS; this is the hostname or IP address by which the UMS can be reached by the endpoint devices.
If your endpoint devices are connected via the ICG, use the [External Address of the ICG as described above \(see page 60\)](#). Please note that the 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 Ports⁴²](#).
If your endpoint devices are connected via the ICG, use the [External Port of the ICG as described above \(see page 60\)](#).

42. <https://kb.igel.com/en/universal-management-suite/current/igel-ums-communication-ports>

IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name
myums

* UMS Hostname
myums.company.com

* UMS Port
8443

Mapped Users

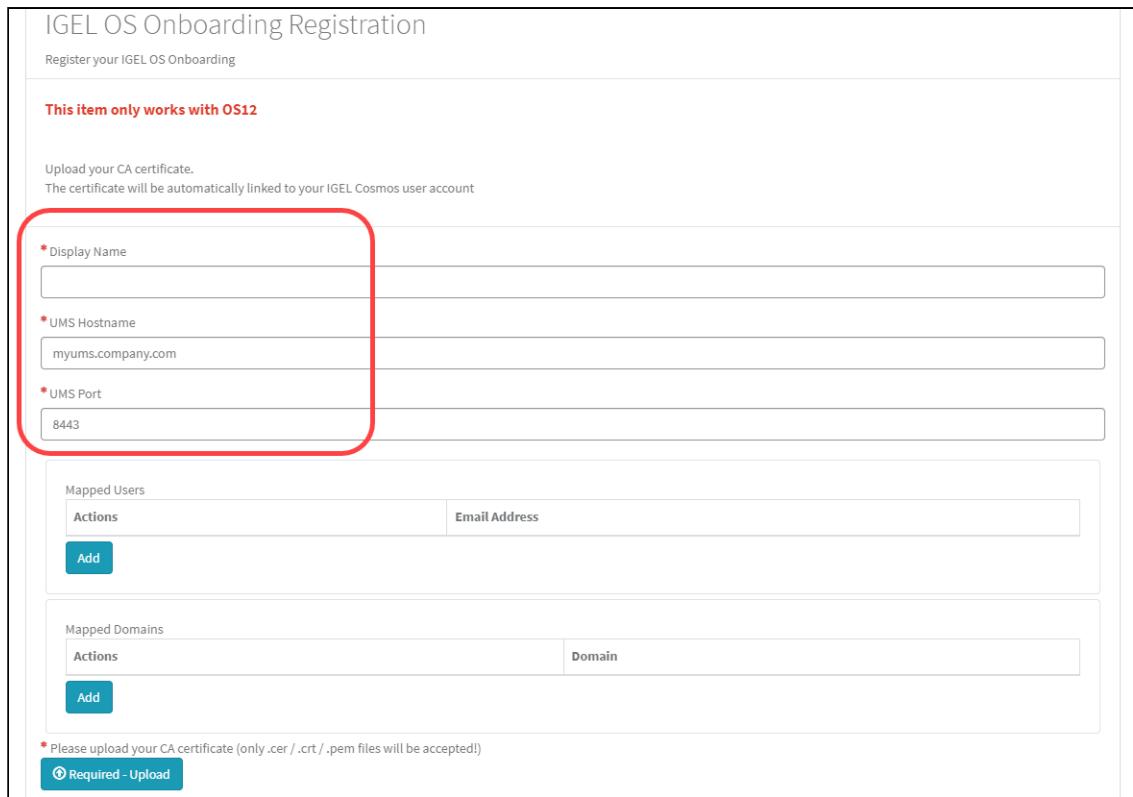
Actions	Email Address
Add	

Mapped Domains

Actions	Domain
Add	

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

Required - Upload



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

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

IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name

* UMS Hostname

* UMS Port

Mapped Users

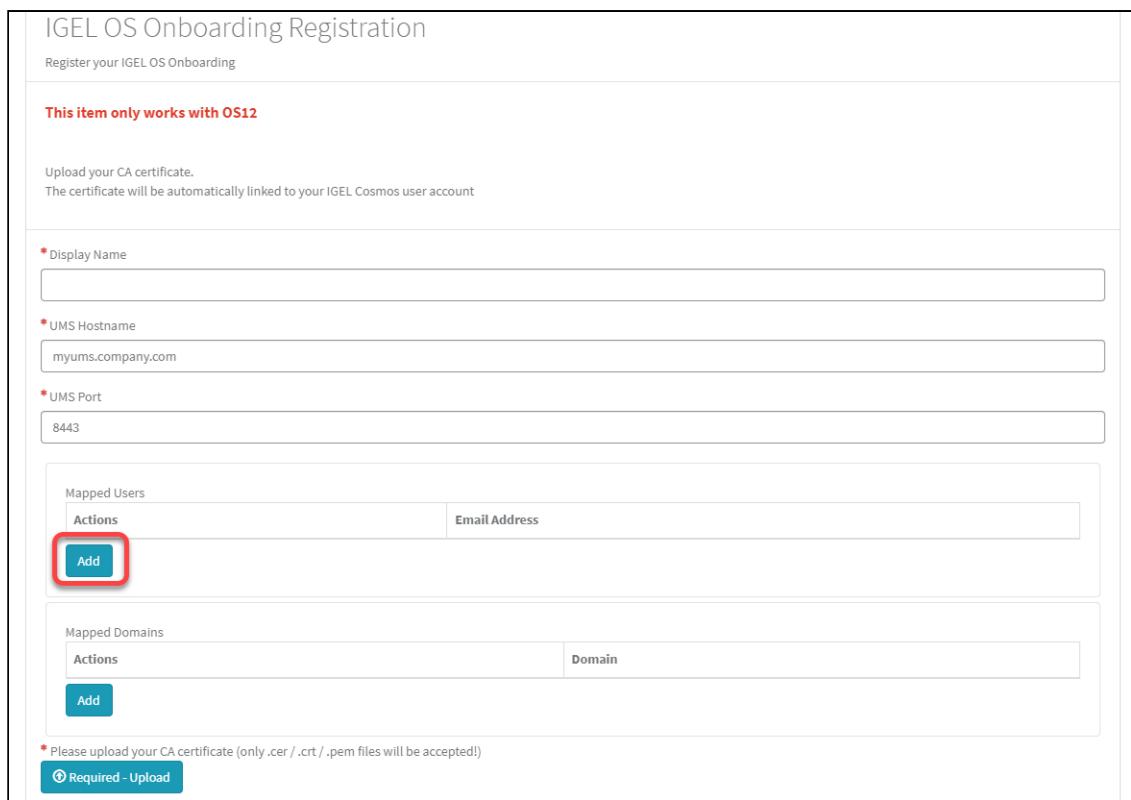
Actions	Email Address
Add	

Mapped Domains

Actions	Domain
Add	

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

Required - Upload



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

IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name

* UMS Hostname

* UMS Port

Mapped Users

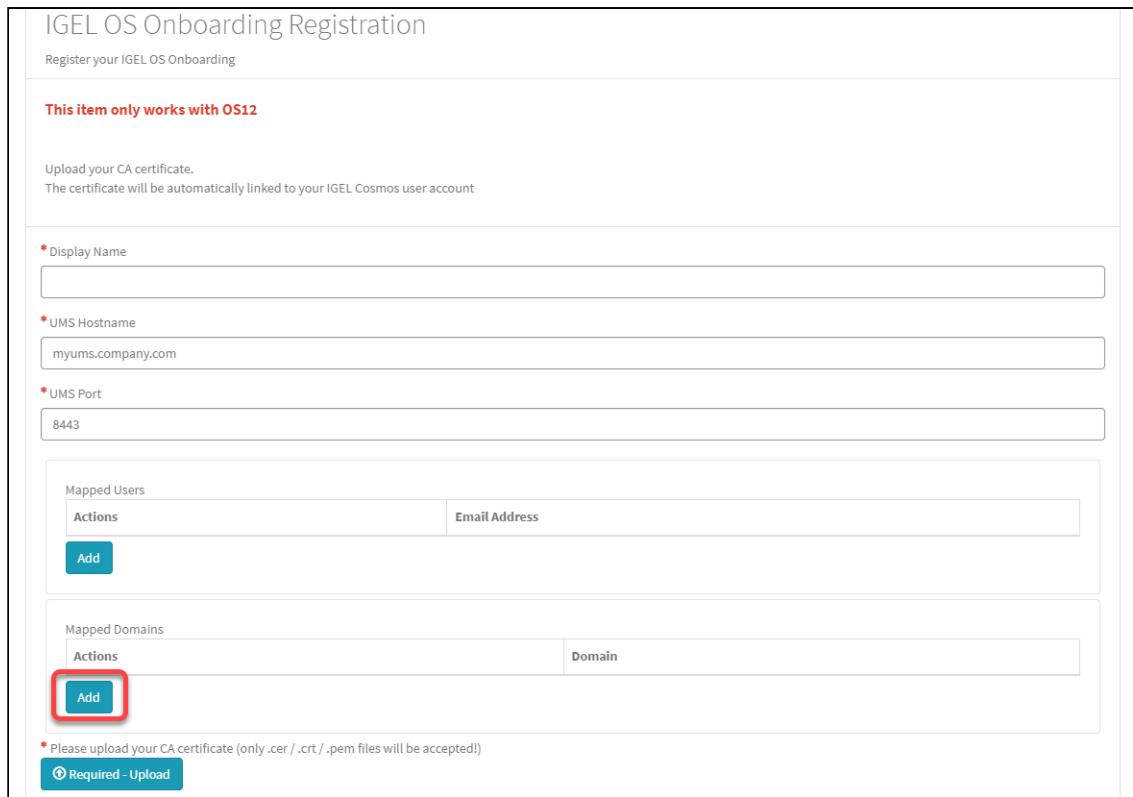
Actions	Email Address
Add	

Mapped Domains

Actions	Domain
Add	

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

Required - Upload



5. In the dialog, enter the e-mail address of the user we have created in Microsoft Entra ID or the relevant domain and click **Add**.
6. Click **Required - Upload** to upload the UMS root certificate chain.
If you want to use the OBS with the ICG, use here the file [icg_chain.crt](#) you obtained as described above (see page 60).

IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name

* UMS Hostname

* UMS Port

Mapped Users

Actions	Email Address
Add	

Mapped Domains

Actions	Domain
Add	

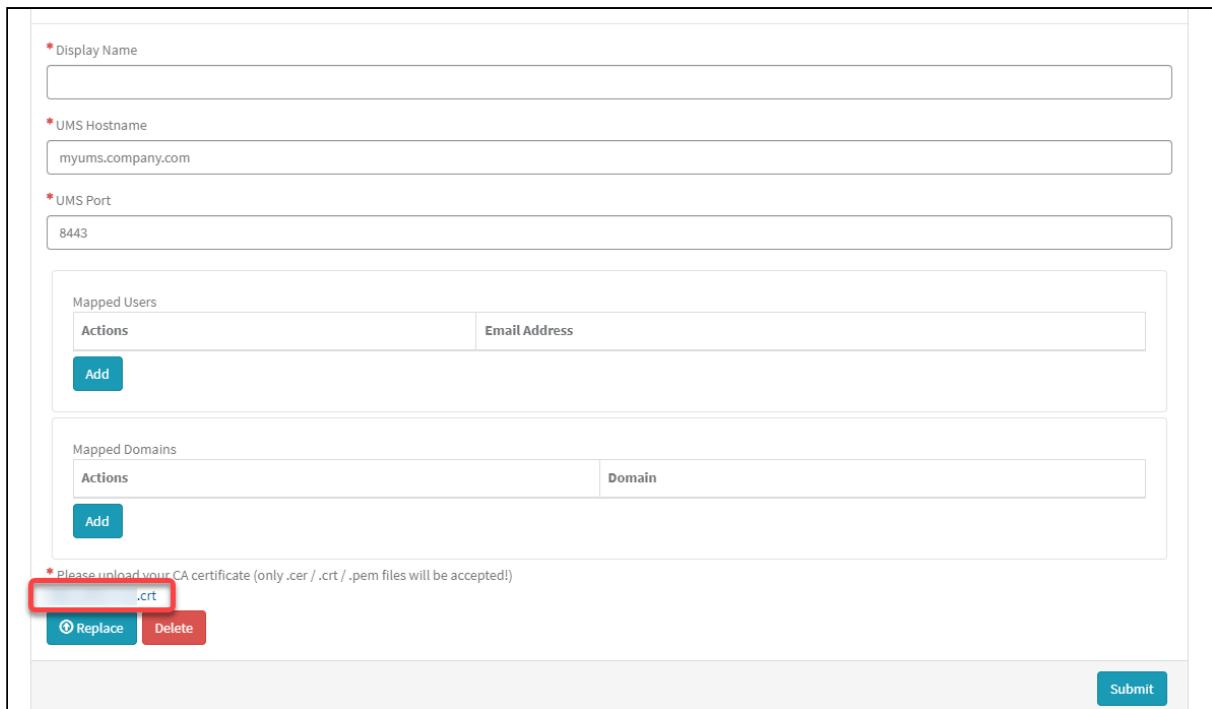
* Please upload your CA certificate (only .cer / .crt / .pem files will be accepted!)

Required - Upload



7. Choose the certificate file on your file system.

The certificate file is uploaded.



* Display Name

* UMS Hostname
myums.company.com

* UMS Port
8443

Mapped Users

Actions	Email Address
Add	

Mapped Domains

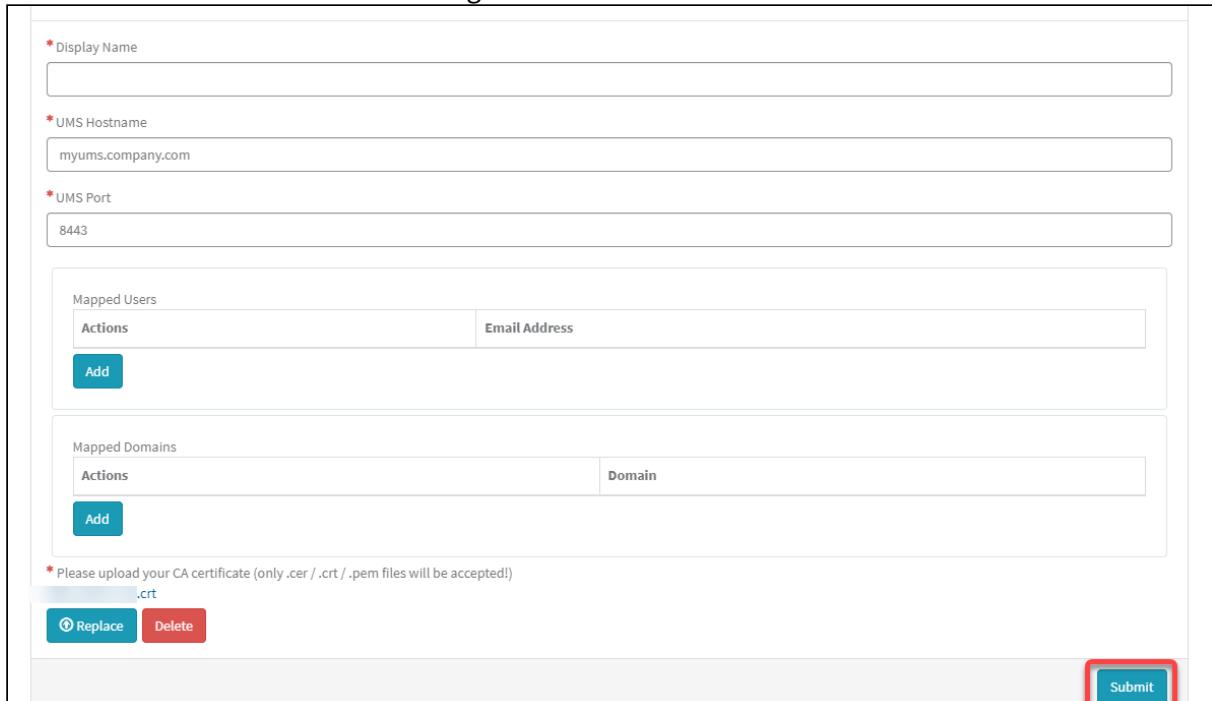
Actions	Domain
Add	

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

Replace Delete

Submit

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



* Display Name

* UMS Hostname
myums.company.com

* UMS Port
8443

Mapped Users

Actions	Email Address
Add	

Mapped Domains

Actions	Domain
Add	

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

Replace Delete

Submit

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

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

IGEL OS Onboarding Management								
All > Account = Test Company					Replace X.509 Certificate	Update Mapped Domains	Update Mapped Users	Register IGEL OS Onboarding
Display Name	UMS Hostname	UMS Port	Created by	OBS Root Certificate	Created	Fingerprint	Expiration date	
		8443			2022-11-12 23:30:18		2042-11-12 10:00:31	
		8443			2022-10-05 10:08:18		2042-09-28 02:18:51	
		8443			2022-10-27 19:05:09		2023-11-10 20:44:53	
		8443			2022-11-04 09:59:13		2042-11-04 05:52:44	

The details are displayed.

IGEL OS Onboarding

Display Name	OBS Root Certificate
<input type="text"/>	<input type="button"/>
UMS Hostname	Expiration date
<input type="text"/>	<input type="text"/>
UMS Port	Created
<input type="text"/>	<input type="text"/>
Fingerprint	Updated
<input type="text"/>	<input type="text"/>
OBS Certificate String	
-----BEGIN CERTIFICATE-----	
<input type="text"/>	

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 (en) Onboarding IGEL OS 12 Devices .

Configuring Microsoft Entra ID as Identity Provider

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

1. [Creating a Microsoft Entra Web Application That Will Serve as Identity Provider \(see page 71\)](#): We register an application in Microsoft Entra ID to use its services as an external identity provider.
2. [Registering Our Microsoft Entra Application in the IGEL Customer Portal \(see page 77\)](#): This will enable IGEL Cloud Services to use our Microsoft Entra Application as the external identity provider.
3. [Creating a User in the Microsoft Entra App \(see page 91\)](#): We create a user account in our application. These user credentials, consisting of an e-mail address and a password, will be entered by the user when onboarding his device.
4. [Configuring roles \(see page 93\)](#): We make the user role information accessible for the **Default Directory Rules**⁴³ feature of the UMS.

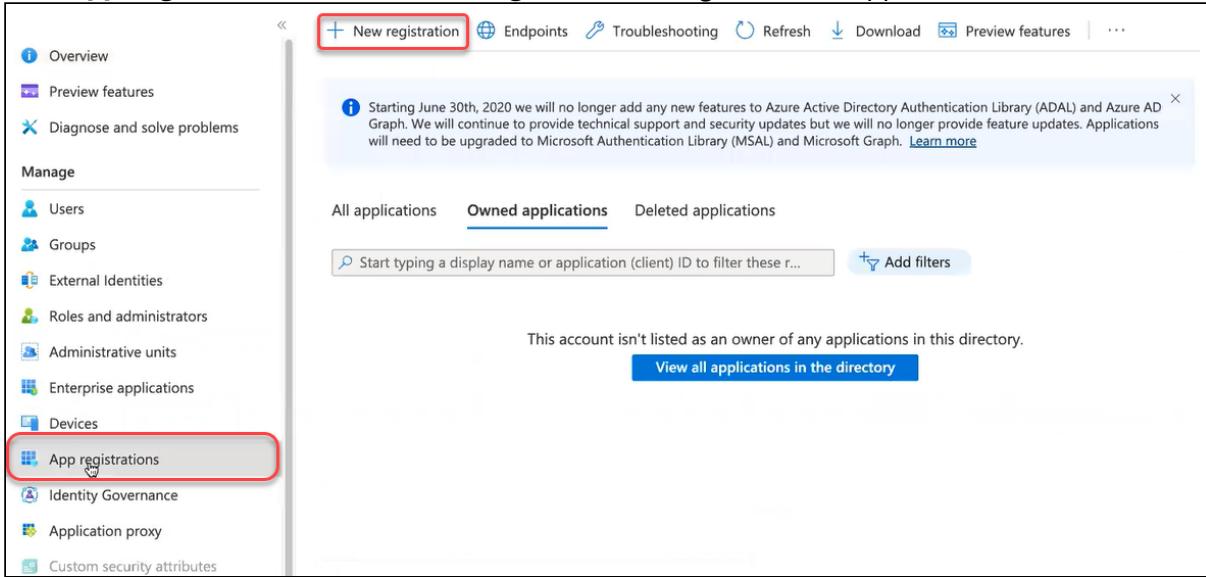
Creating a Web Application That Will Serve as Identity Provider

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

The screenshot shows the Azure portal's "Welcome to Azure!" page. At the top, there are three main sections: "Start with an Azure free trial", "Manage Azure Active Directory", and "Access student benefits". Below these, under "Azure services", there is a grid of icons for various Azure products. The "Azure Active Directory" icon is highlighted with a red box and an arrow points from it to a "More services" button. Other visible icons include "Create a resource", "Quickstart Center", "Virtual machines", "App Services", "Storage accounts", "SQL databases", and "Azure Cosmos DB".

43. <https://kb.igel.com/en/universal-management-suite/current/default-directory-rules>

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



The screenshot shows the Azure Active Directory 'App registrations' page. At the top, there's a navigation bar with links for Overview, Preview features, Diagnose and solve problems, and a 'New registration' button, which is highlighted with a red box. Below the navigation bar is a message about the deprecation of ADAL and Azure AD Graph. The main area has tabs for All applications, Owned applications (which is selected and highlighted with a blue underline), and Deleted applications. A search bar and a 'Add filters' button are also present. A message states that the account isn't listed as an owner of any applications, with a 'View all applications in the directory' button. On the left, a sidebar titled 'Manage' lists various options: Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations (which is highlighted with a red box), Identity Governance, Application proxy, and Custom security attributes.

3. Edit the data as follows and then click **Register**:

- **Name:** Display name of 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 URL of the onboarding service. This is "<https://obs.services.igel.com/>".

Home > IGEL Technology GmbH >

Register an application ...

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

OBS Testing application

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (IGEL Technology GmbH only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only

Help me choose...

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

Web https://igel.com

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

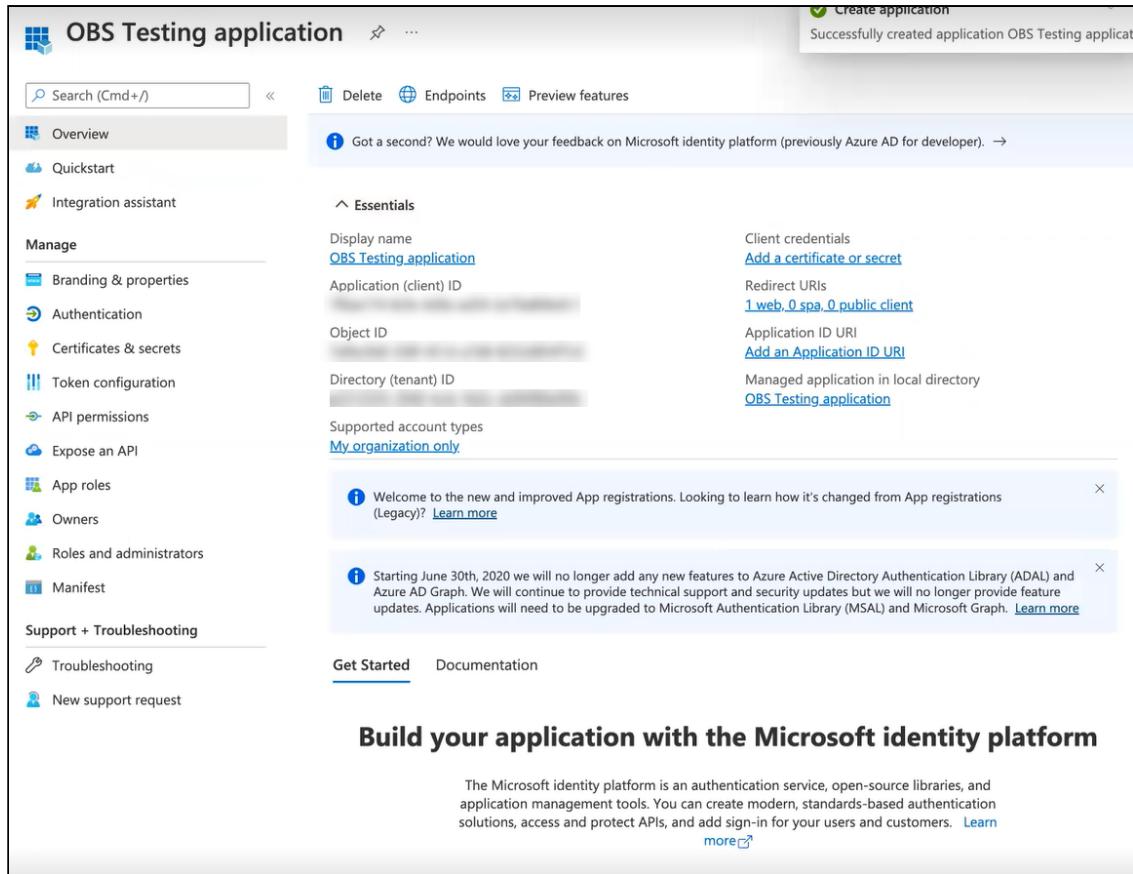
By proceeding, you agree to the Microsoft Platform Policies [□](#)

Register



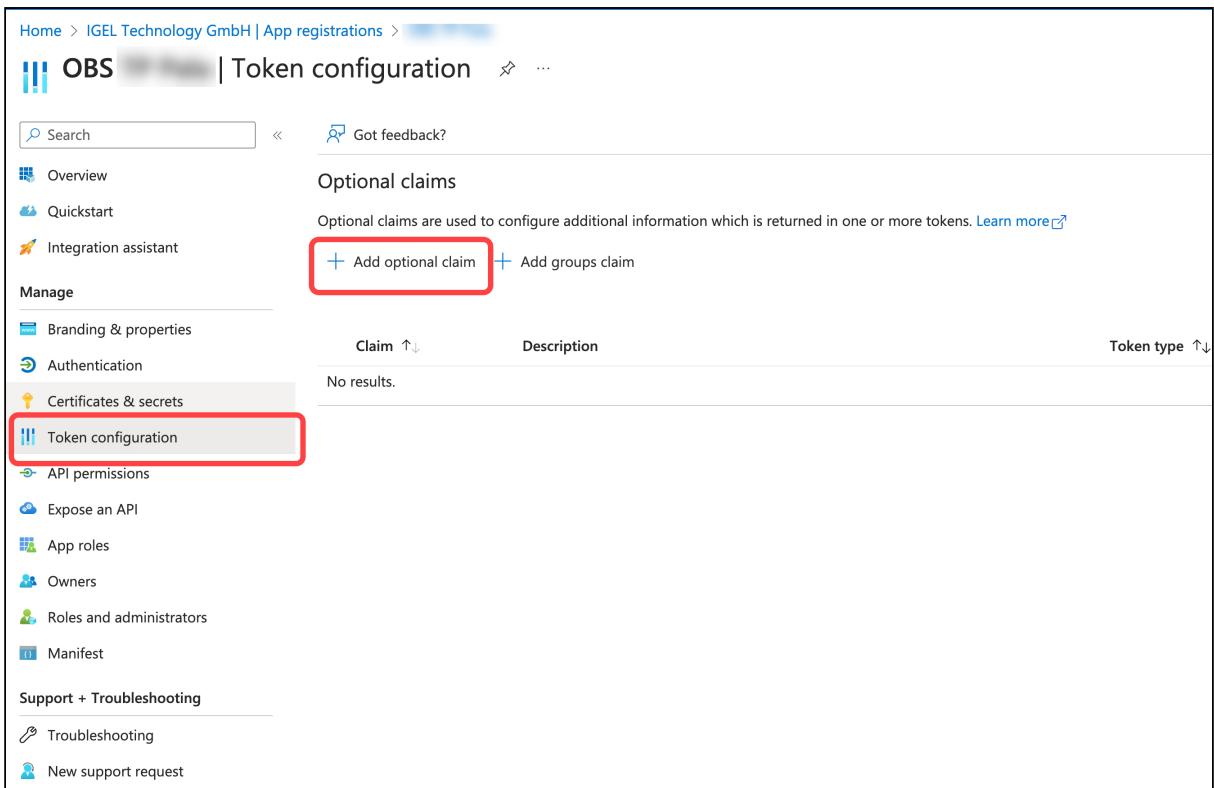
The application is created.

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



The screenshot shows the 'OBS Testing application' configuration page in the Microsoft Azure portal. The left sidebar includes links for Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area displays the 'Essentials' section with fields for Display name (OBS Testing application), Application (client) ID, Object ID, Directory (tenant) ID, Client credentials (Add a certificate or secret), Redirect URIs (1 web, 0 spa, 0 public client), Application ID URI (Add an Application ID URI), and Managed application in local directory (OBS Testing application). Below this, there are two informational cards: one about the new App registrations experience and another about the end-of-life of ADAL and Azure AD Graph. At the bottom, there are 'Get Started' and 'Documentation' links, and a section titled 'Build your application with the Microsoft identity platform'.

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



The screenshot shows the Azure portal interface for managing an app registration. The left sidebar lists several sections: Overview, Quickstart, Integration assistant, Manage (with sub-options like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest), and Support + Troubleshooting. The 'Token configuration' option under 'Manage' is highlighted with a red box. In the main content area, the title is 'Token configuration'. Below it, there's a section titled 'Optional claims' with a sub-section 'Optional claims are used to configure additional information which is returned in one or more tokens.' It includes two buttons: '+ Add optional claim' and '+ Add groups claim', both of which are also highlighted with red boxes. A table below shows 'No results.' under columns 'Claim', 'Description', and 'Token type'.

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

- **email**
- **preferred_username**

6. Click **Add**.

Add optional claim

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

* Token type
Access and ID tokens are used by applications for authentication. [Learn more](#)

ID (highlighted)

Access

SAML

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

Add (highlighted) **Cancel**

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

Add optional claim

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

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

Add (highlighted) **Cancel**

The token configuration is completed:



The screenshot shows the 'Token configuration' page for an app registration. The left sidebar lists various management options like 'Overview', 'Quickstart', 'Integration assistant', 'Authentication', 'Certificates & secrets', 'Token configuration' (which is selected), 'API permissions', 'Expose an API', 'App roles', 'Owners', 'Roles and administrators', and 'Manifest'. The main area displays 'Optional claims' with descriptions and token types. Two claims are listed: 'email' (description: 'The addressable email for this user, if the user has one') and 'preferred_username' (description: 'Provides the preferred username claim, making it easier for apps to provide username h...'). A success message at the top right says 'Successfully updated OBS' and another says 'Successfully saved permissions for OBS'.

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

Registering Our Entra App in the IGEL Customer Portal

1. Open the [IGEL Customer Portal](#)⁴⁴ in your browser, log in to your admin account, and select **Users** > **IGEL OS IdP**.

The screenshot shows the 'Users' menu in the IGEL Customer Portal. A sub-menu is displayed for 'IGEL OS IdP' (highlighted with a red box). Other options in the sub-menu include 'Overview', 'User & Role Administration', and 'My Profile'.

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

44. <https://support.igel.com/>

IGEL OS IdP Management						
All > Account =					Update client secret	Update Mapped Domains
Display name	Client ID	Client Secret	Authorization URL	Token URL	Mapped Domains	Created
*****	*****	*****	*****	*****	*****	2022-10-13 12:16:26
*****	*****	*****	..	*****	*****	2022-09-28 15:19:29
*****	*****	*****	..	*****	*****	2022-10-11 08:39:53

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

* Indicates required

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

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

Mapped Domains

Add	Remove All
Actions	Domain Name
No data to display	

Submit

Required information

Client ID Authorization Endpoint URL
Token Endpoint URL

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

The screenshot shows the Azure Active Directory App Registrations interface. On the left, there's a sidebar with options like Overview, Quickstart, Integration assistant, Manage (with sub-options: Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators), and a search bar at the top. The main area is titled 'OBS Testing application'. At the top of this area are buttons for Delete, Endpoints (which is highlighted with a red box), and Preview features. Below this, there's a message: 'Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →'. The main content area is divided into sections: 'Essentials' (Display name: OBS Testing application, Application (client) ID, Object ID, Directory (tenant) ID), 'Client credentials' (Add a certificate or secret), 'Redirect URLs' (1 web, 0 spa, 0 public client), 'Application ID URI' (Add an Application ID URI), and 'Managed application in local directory' (OBS Testing application). There are also two informational pop-ups at the bottom: one about the new App registrations experience and another about the end of support for ADAL.

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.

The screenshot shows the 'Endpoints' section of the Azure Active Directory App Registrations page. It lists four endpoints: OAuth 2.0 authorization endpoint (v2) (https://login.microsoftonline.com/), OAuth 2.0 token endpoint (v2) (https://login.microsoftonline.com/.oauth2/v2.0/token), OAuth 2.0 authorization endpoint (v1) (https://login.microsoftonline.com/.oauth2/authorize), and OAuth 2.0 token endpoint (v1) (https://login.microsoftonline.com/.oauth2/token). The 'Copy to clipboard' button for the v2 authorization endpoint is highlighted with a red box.

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

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name
My OBS identity provider

* Client ID

* Client Secret

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

* Token Endpoint URL

Mapped Domains

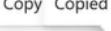
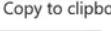
Add Remove All

Actions	Domain Name
	No data to display



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

Endpoints

OAuth 2.0 authorization endpoint (v2) https://login.microsoftonline.com/	:/oauth2/v2.0/authorize  Copied
OAuth 2.0 token endpoint (v2) https://login.microsoftonline.com/	:/oauth2/v2.0/token  Copy to clipboard
OAuth 2.0 authorization endpoint (v1) https://login.microsoftonline.com/	:/oauth2/authorize 
OAuth 2.0 token endpoint (v1) https://login.microsoftonline.com/	:/oauth2/token 

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

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name
My OBS identity provider

* Client ID

* Client Secret

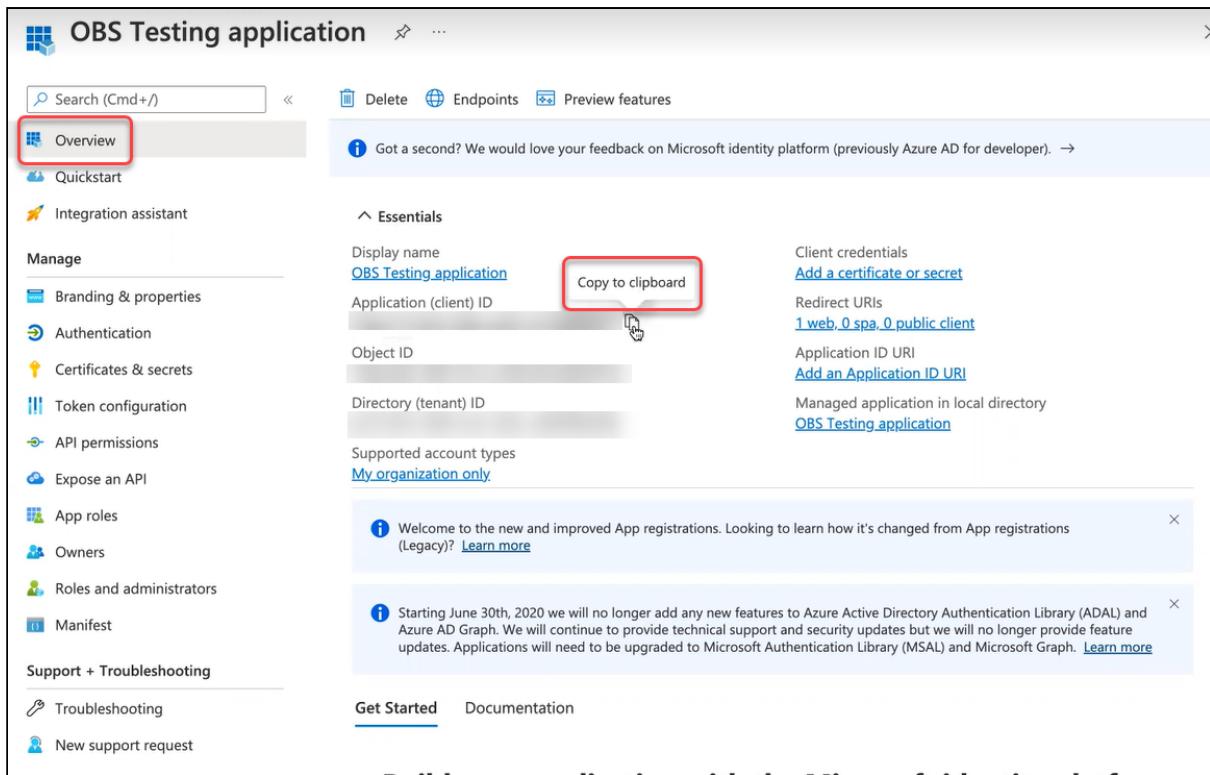
* Authorization Endpoint URL
https://login.microsoftonline.com/ /oauth2/v2.0/authorize

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

Mapped Domains

Actions	Domain Name
	No data to display

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



The screenshot shows the 'Overview' tab selected in the Azure Active Directory App Registrations interface. The 'Application (client) ID' field is highlighted with a red box, and the 'Copy to clipboard' button next to it is also highlighted with a red box.

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

* Token Endpoint URL

Mapped Domains

Actions	Domain Name
	No data to display

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

The screenshot shows the 'OBS Testing application' overview page in the Azure portal. The left sidebar lists various management options like Overview, Quickstart, Integration assistant, and Certificates & secrets. The main area displays the application's details under the 'Essentials' tab. A red box highlights the 'Client credentials' section, which includes a button labeled 'Add a certificate or secret'. Other visible fields include 'Display name' (OBS Testing application), 'Application (client) ID', 'Object ID', 'Directory (tenant) ID', 'Supported account types' (My organization only), 'Redirect URIs' (1 web, 0 spa, 0 public client), 'Application ID URI' (Add an Application ID URI), and a note about being a managed application in the local directory.

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

12. Click **New client secret**.

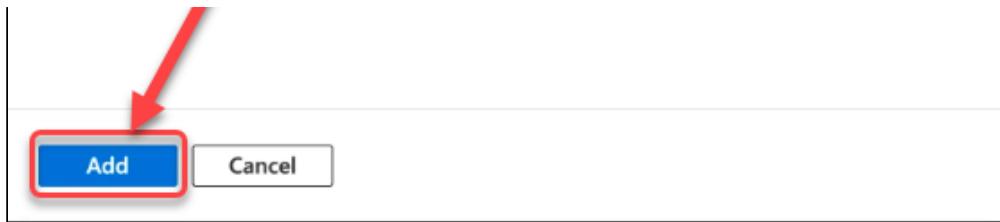
The screenshot shows the 'Certificates & secrets' page for the 'OBS Testing application'. The left sidebar shows the 'Certificates & secrets' option is selected. The main area has tabs for 'Certificates (0)', 'Client secrets (0)' (which is selected and highlighted with a red box), and 'Federated credentials (0)'. Below the tabs, it says 'A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.' A red box highlights the '+ New client secret' button. A note at the bottom states 'No client secrets have been created for this application.'

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

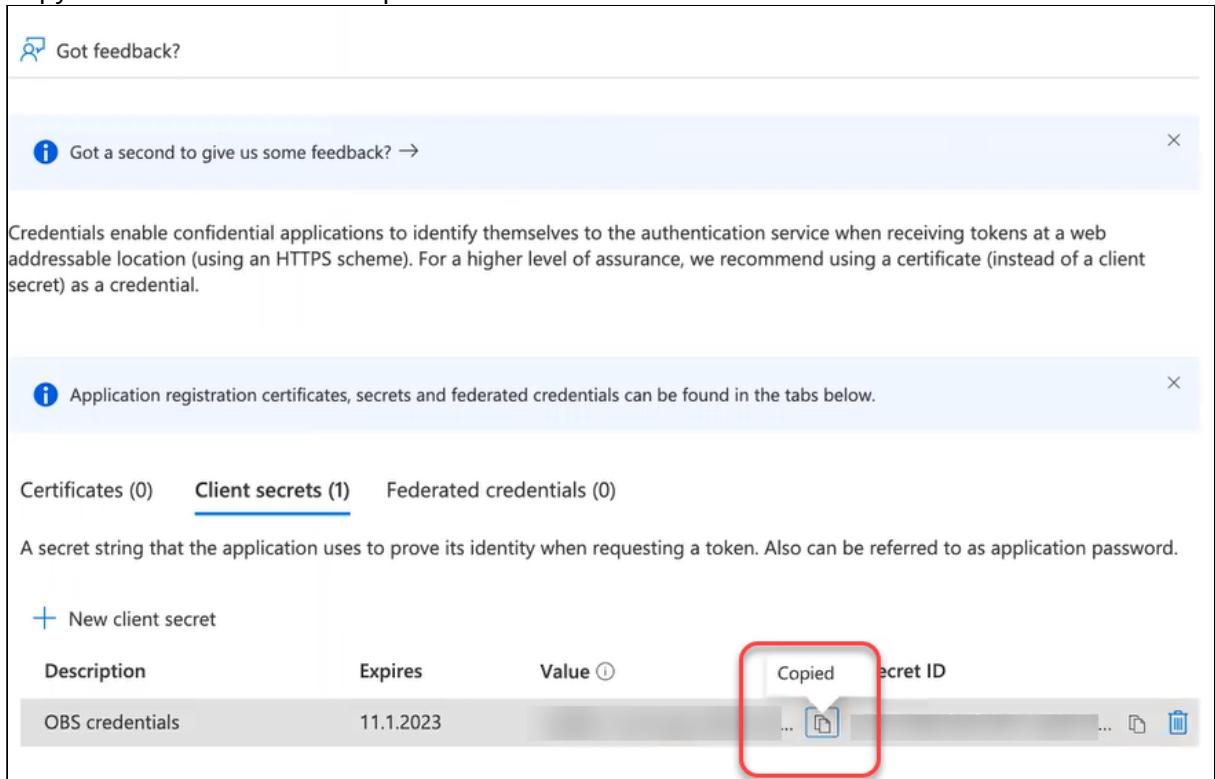
14. Enter a description and then click **Add**.

Add a client secret

Description	OBS credentials
Expires	Recommended: 6 months



15. Copy the client secret to the clipboard.



Got feedback?

Got a second to give us some feedback? →

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

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

Certificates (0) Client secrets (1) Federated credentials (0)

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

+ New client secret

Description	Expires	Value ⓘ	Secret ID	...	Copy	Delete
OBS credentials	11.1.2023	Copied

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

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name
My OBS identity provider

* Client ID

* Client Secret
| SHOW

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

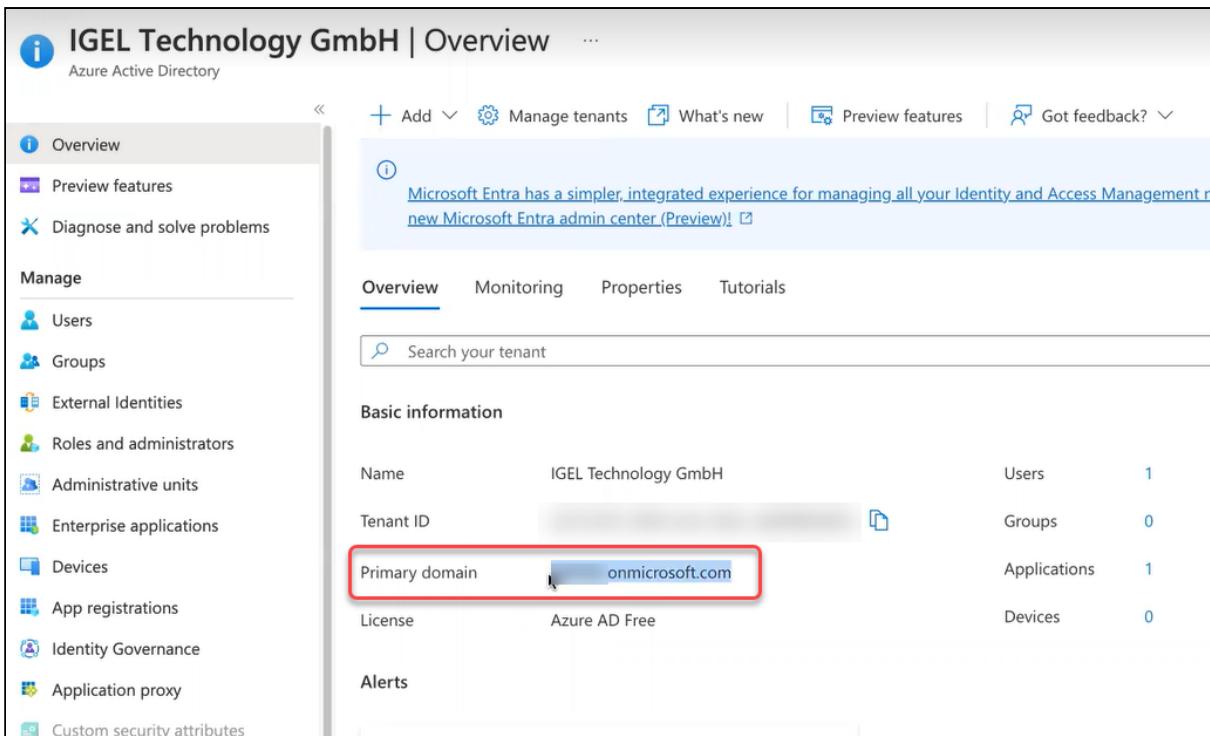
* Token Endpoint URL
https://login.microsoftonline.com/ oauth2/v2.0/token

Mapped Domains

Actions	Domain Name
	No data to display

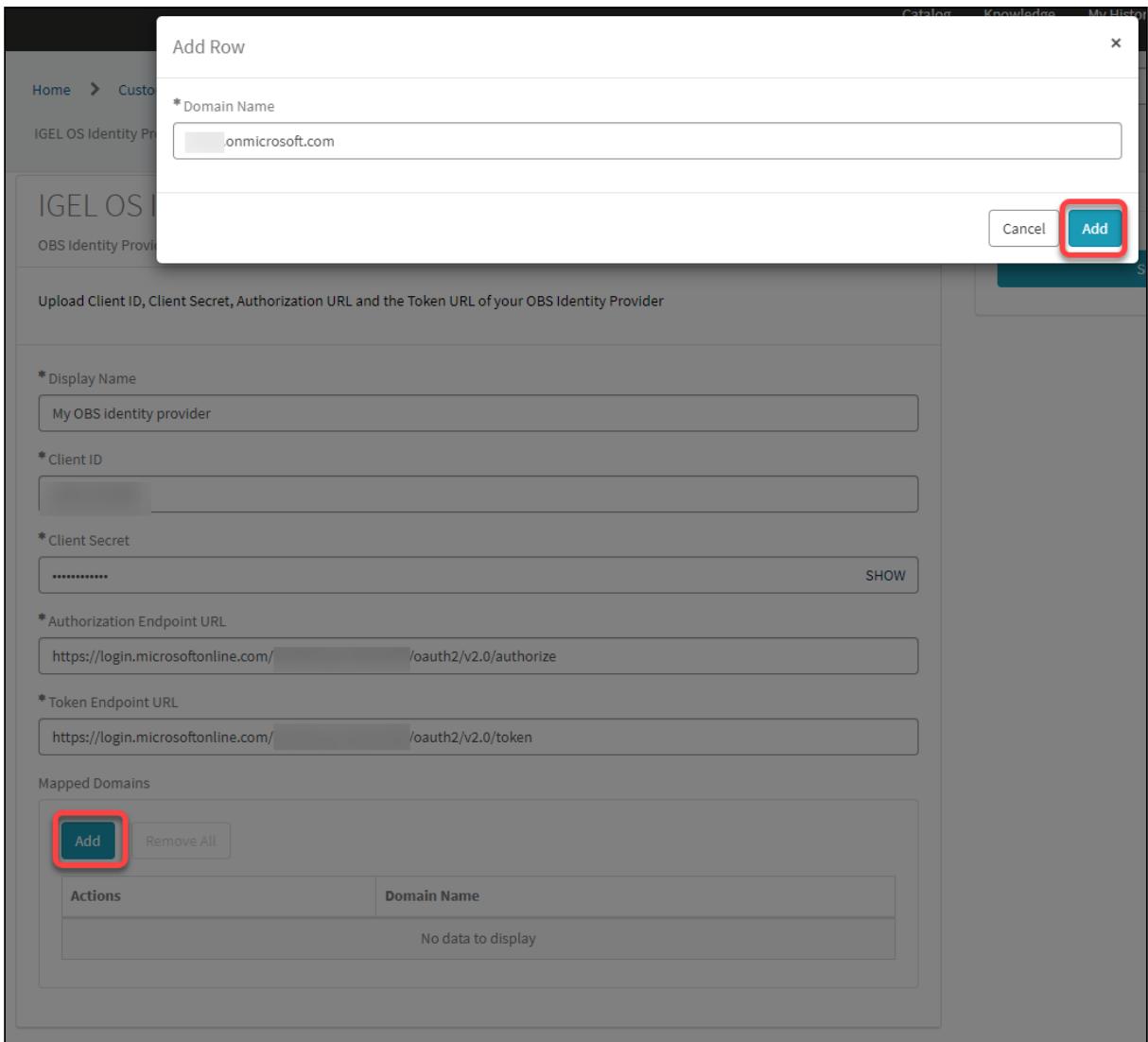
17. Change to the tab with your Entra app and change to the overview of your Entra tenant.

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



The screenshot shows the Azure Active Directory Overview page for the tenant "IGEL Technology GmbH". The left sidebar lists various management options like Users, Groups, External Identities, etc. The main area displays basic information about the tenant, including the Name (IGEL Technology GmbH), Tenant ID, Primary domain (onmicrosoft.com), License (Azure AD Free), and usage statistics for Users (1), Groups (0), Applications (1), and Devices (0). The "Primary domain" field is highlighted with a red box.

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.



The screenshot shows the IGEL Onboarding Service (OBS) configuration interface. A modal dialog titled "Add Row" is open, prompting for a "Domain Name" which is set to "onmicrosoft.com". In the top right corner of this dialog, there are two buttons: "Cancel" and "Add", with "Add" being highlighted by a red box. The background of the main configuration page displays fields for "Display Name" ("My OBS Identity provider"), "Client ID" (redacted), "Client Secret" (redacted), "Authorization Endpoint URL" ("https://login.microsoftonline.com/ /oauth2/v2.0/authorize"), and "Token Endpoint URL" ("https://login.microsoftonline.com/ /oauth2/v2.0/token"). Below these fields is a section titled "Mapped Domains" with an "Add" button, also highlighted by a red box.

20. Click **Submit**.

Initial Configuration of the IGEL Onboarding Service (OBS)



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name
My OBS identity provider

* Client ID
[redacted]

* Client Secret
***** SHOW

* Authorization Endpoint URL
<https://login.microsoftonline.com/>/oauth2/v2.0/authorize

* Token Endpoint URL
<https://login.microsoftonline.com/>/oauth2/v2.0/token

Mapped Domains

Add Remove All

Actions	Domain Name
edit x	.onmicrosoft.com

Submit

The data record is created.

IGEL OS IdP Management						
All > Account = Test Company				Update client secret	Update Mapped Domains	Register IGEL OS IdP
Display name	Client ID	Client Secret	Authorization URL	Token URL	Mapped Domains	Created
My OBS identity provider	[redacted]	*****	https://login.microsoftonline.com/	https://login.microsoftonline.com/	.onmicrosoft.com	2022-12-01 16:01:06
	[redacted]	*****	https://login.microsoftonline.com/	https://login.microsoftonline.com/	.onmicrosoft.com	2022-10-13 12:16:26

Creating a User in the Entra App

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

IGEL Technology GmbH | Overview

Azure Active Directory

Manage

- Users** (highlighted with a red box)
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy

Overview **Monitoring** **Properties** **Tutorials**

Search your tenant

Basic information

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

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

Users

Search (Cmd+ /) New user Download users Bulk operations Refresh Columns Delete ...

All users (preview) Create a new user Invite external user

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

Search Add filter Copy link to current view

1 user found

Display name ↑	User principal name	User type	On-premises sync	Identity	
PA	@igel.com	_igel.com#EX...	Member	No	External

3. Provide the necessary data and then click **Create**:

- **User name:** A valid e-mail address.
- **Name:** Display name
- **Let me create the password:** For our purposes, you can use this option.
- **Initial password:** Password to be used for the first login.

Identity

User name * (red box) @ s.onmicrosoft.com

Name * (red box) OBS User

First name

Last name

Password

Auto-generate password
 Let me create the password (red box)

Initial password * (red box)

Groups and roles

Groups 0 groups selected

Roles User

Settings

Block sign in Yes No

Usage location

Create (red box)

Assigning Roles to Users

1. Create roles and assign users.

For information, see: <https://learn.microsoft.com/en-us/entra/identity-platform/howto-add-app-roles-in-apps>

2. You can then use the configured roles to create default directory rules in the UMS to automatically classify devices into specific directories during registration. For details, see [Default Directory Rules⁴⁵](#) and [How to Automate the Rollout Process in the IGEL UMS⁴⁶](#).

45. <https://kb.igel.com/en/universal-management-suite/current/default-directory-rules>

46. <https://kb.igel.com/en/universal-management-suite/current/how-to-automate-the-rollout-process-in-the-igel-um>

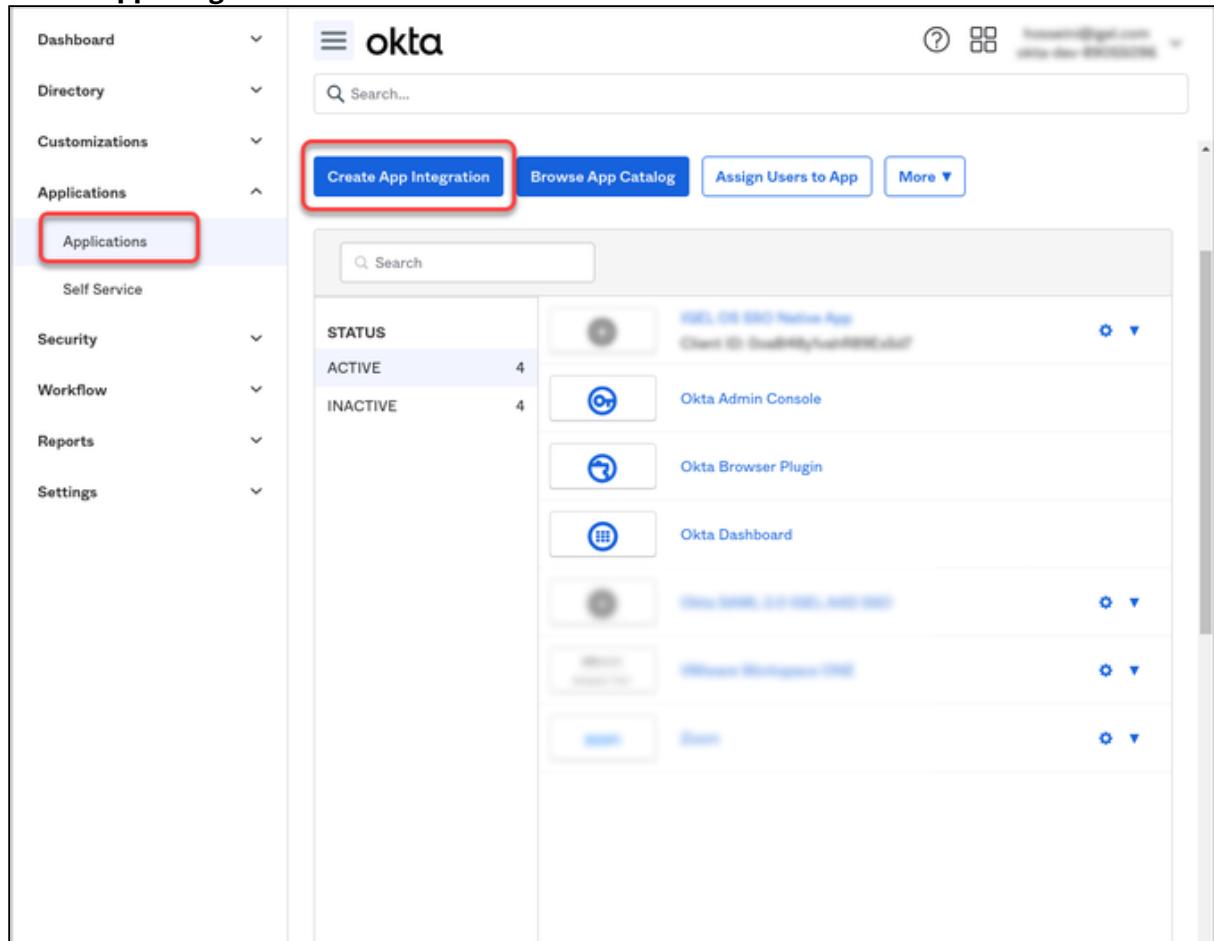
Configuring Okta as Identity Provider

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

1. [Creating an Okta Application That Will Serve as Identity Provider](#): 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 98): This will enable IGEL Cloud Services to use our Okta Application as the external identity provider.
3. [Configuring roles](#) (see page 105): We make the user role information accessible for the [Default Directory Rules](#)⁴⁷ feature of the UMS.

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**.

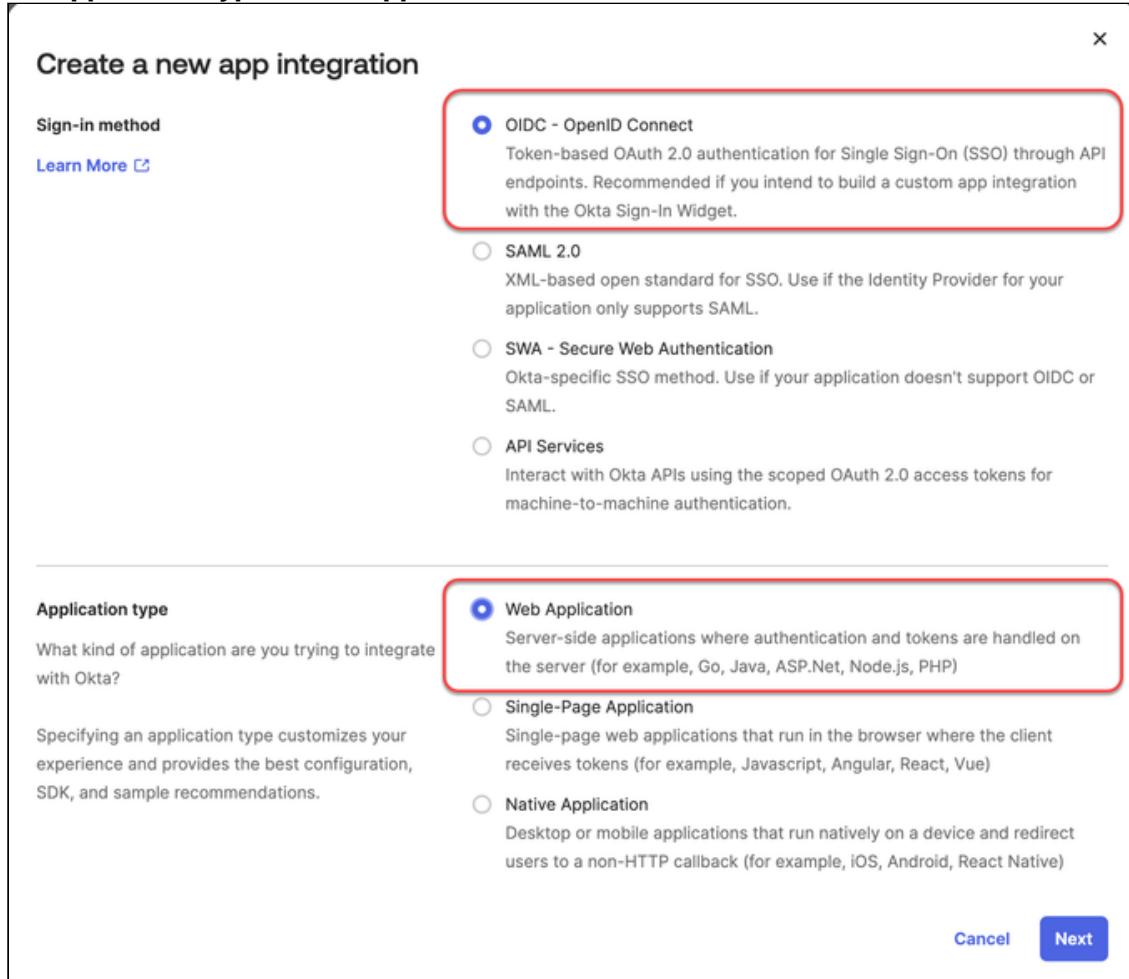


The screenshot shows the Okta Admin Console interface. On the left, there is a sidebar with various menu items: Dashboard, Directory, Customizations, Applications (which is currently selected and highlighted with a red box), Self Service, Security, Workflow, Reports, and Settings. In the main content area, the title 'okta' is displayed above a search bar. Below the search bar are four buttons: 'Create App Integration' (which is highlighted with a red box), 'Browse App Catalog', 'Assign Users to App', and 'More'. Underneath these buttons is a table with a header 'Search'. The table has two columns: 'STATUS' and 'Name'. The 'STATUS' column shows 'ACTIVE' and 'INACTIVE' with counts of 4 each. The 'Name' column lists several Okta applications: 'IGEL OBS 9900 Native App' (Client ID: 0ad8061c-0a0d-40e0-9f80-000000000000), 'Okta Admin Console', 'Okta Browser Plugin', and 'Okta Dashboard'. Each application entry includes a small icon and a dropdown arrow.

47. <https://kb.igel.com/en/universal-management-suite/current/default-directory-rules>

2. Edit the settings as follows and then click **Next**.

- Set **Sign-in method** to **OIDC**.
- Set **Application type** to **Web Application**.



Create a new app integration

Sign-in method

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

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

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

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

Application type

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

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

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

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

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

Cancel Next

3. Edit the settings as follows and then click **Save**.

- Under **App integration name**, enter a name for your application, e.g. "IGEL Onboarding Service".
- Make sure that as the **Grant type**, the option **Authorization Code** is selected.
- Under **Sign-in redirect URIs**, enter "`https://obs.services.igel.com/`".

New Web App Integration

General Settings

App integration name (highlighted with a red box)

Logo (Optional)

Grant type

Client acting on behalf of itself Client Credentials

Client acting on behalf of a user Authorization Code Refresh Token Implicit (hybrid) (highlighted with a red box)

Sign-in redirect URIs

Allow wildcard * in sign-in URI redirect.

(highlighted with a red box)

[Learn More](#) [+ Add URI](#)

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

Assignments

Controlled access

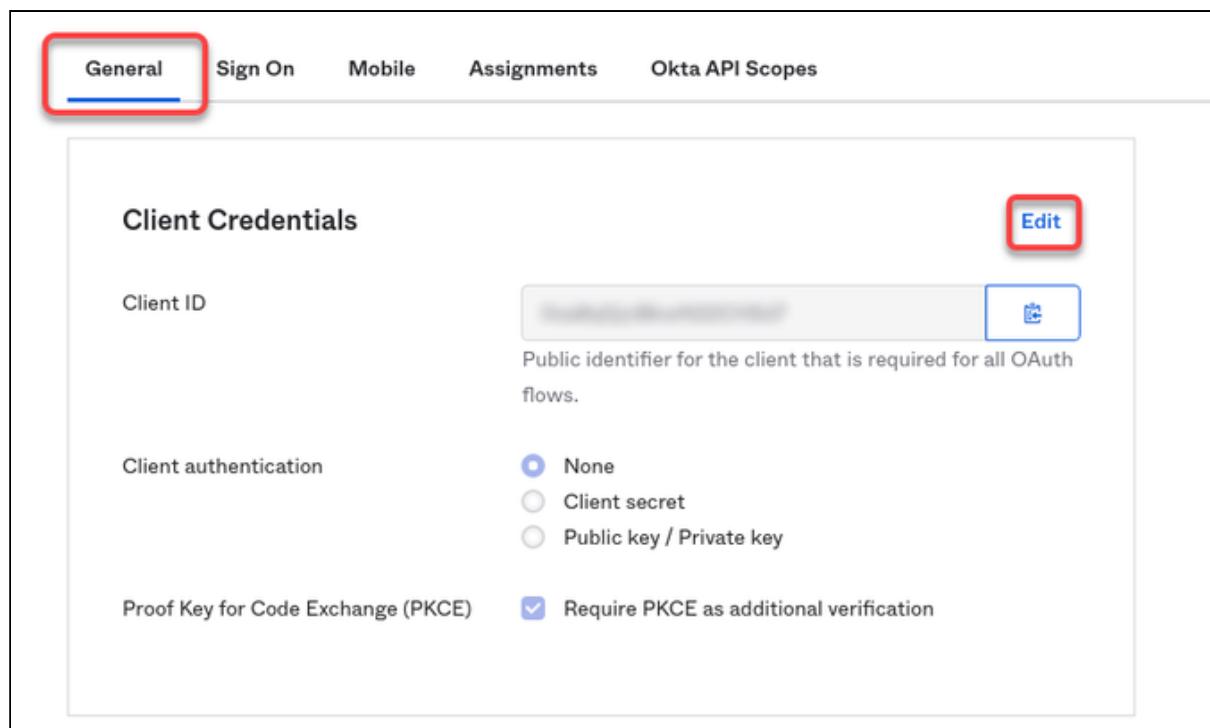
Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

Allow everyone in your organization to access
 Limit access to selected groups
 Skip group assignment for now (highlighted with a red box)

Save **Cancel**

The app integration is created.

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



The screenshot shows the 'General' tab selected in the top navigation bar. The 'Client Credentials' section is expanded, displaying the following configuration:

- Client ID:** A text input field containing a blurred value, with an 'Edit' button to its right.
- Client authentication:** A radio button group where 'None' is selected, while 'Client secret' and 'Public key / Private key' are unselected.
- Proof Key for Code Exchange (PKCE):** A checkbox labeled 'Require PKCE as additional verification' is checked.

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

Registering Our Okta Application in the IGEL Customer Portal

1. Open the [IGEL Customer Portal](#)⁴⁸ in your browser, log in to your admin account, and select **Users > IGEL OS IdP**.

48. <https://support.igel.com/>

2. Click Register IGEL OS IdP.

IGEL OS IdP Management							
All > Account =					Update client secret	Update Mapped Domains	Register IGEL OS IdP
Display name	Client ID	Client Secret	Authorization URL	Token URL	Mapped Domains	Created	Actions
*****	*****	*****	*****	*****	*****	2022-10-13 12:16:26	2
*****	*****	*****	..	*****	*****	2022-09-28 15:19:29	2
*****	*****	*****	..	*****	*****	2022-10-11 08:39:53	2

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

* Indicates required

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

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

Mapped Domains

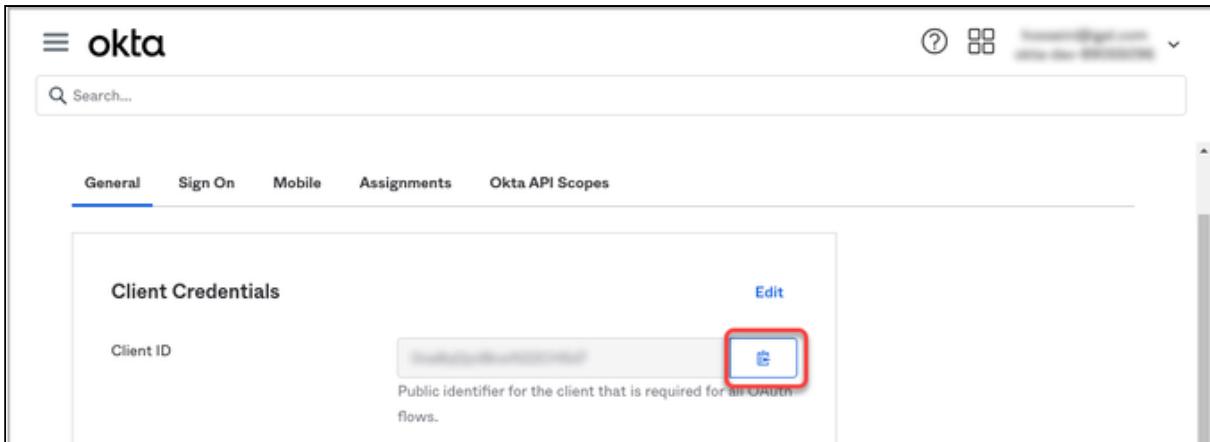
Add	Remove All
Actions	Domain Name
No data to display	

Submit

Required information

Client ID **Authorization Endpoint URL** **Token Endpoint URL**

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



The screenshot shows the Okta General settings page. At the top, there are tabs for General, Sign On, Mobile, Assignments, and Okta API Scopes. The General tab is selected. Below the tabs, there is a section titled "Client Credentials". Inside this section, there is a "Client ID" field containing a blurred value. To the right of the field is an "Edit" button. A red box highlights the "Client ID" field.

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
 (The input field is highlighted with a red rectangle.)

* 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**.

General Sign On Assignments Okta API Scopes Application Rate Limits

Client Credentials

Client ID: [REDACTED] [Cancel](#)

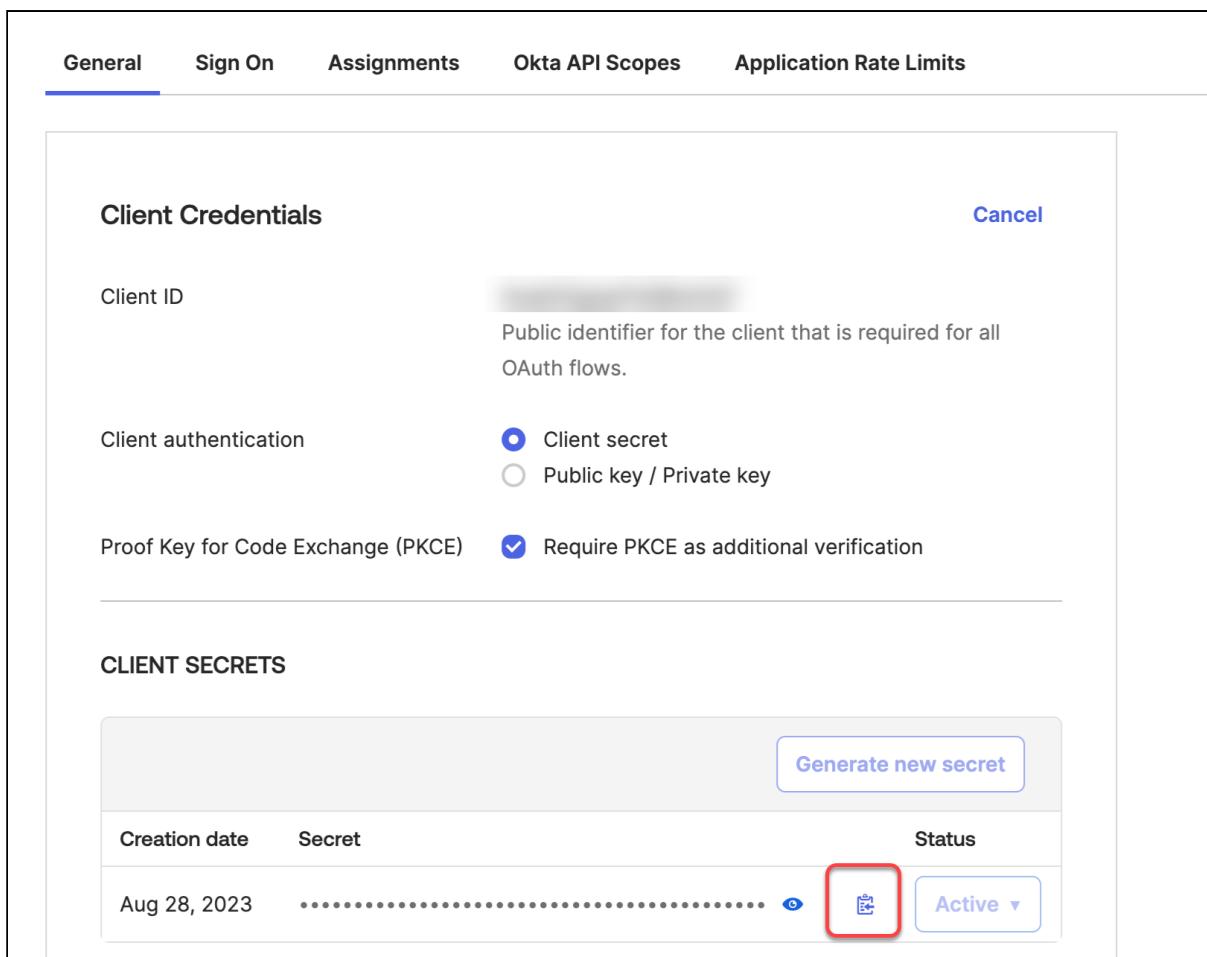
Client authentication: Client secret Public key / Private key

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

CLIENT SECRETS

Creation date	Secret	Status
Aug 28, 2023	 Active ▾

[Generate new 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**.

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	<input type="text" value="My OBS identity provider"/>				
* Client ID	<input type="text"/>				
* Client Secret	<input type="password" value="....."/> SHOW				
* Authorization Endpoint URL	<input type="text"/>				
* Token Endpoint URL	<input type="text"/>				
Mapped Domains <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #0072BC; color: white;">Actions</th> <th style="background-color: #0072BC; color: white;">Domain Name</th> </tr> </thead> <tbody> <tr> <td></td> <td>No data to display</td> </tr> </tbody> </table>		Actions	Domain Name		No data to display
Actions	Domain Name				
	No data to display				

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

```

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

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

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

This item only works with OS12

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

* Display Name
My OBS identity provider

* Client ID
[redacted]

* Client Secret
[redacted] [SHOW](#)

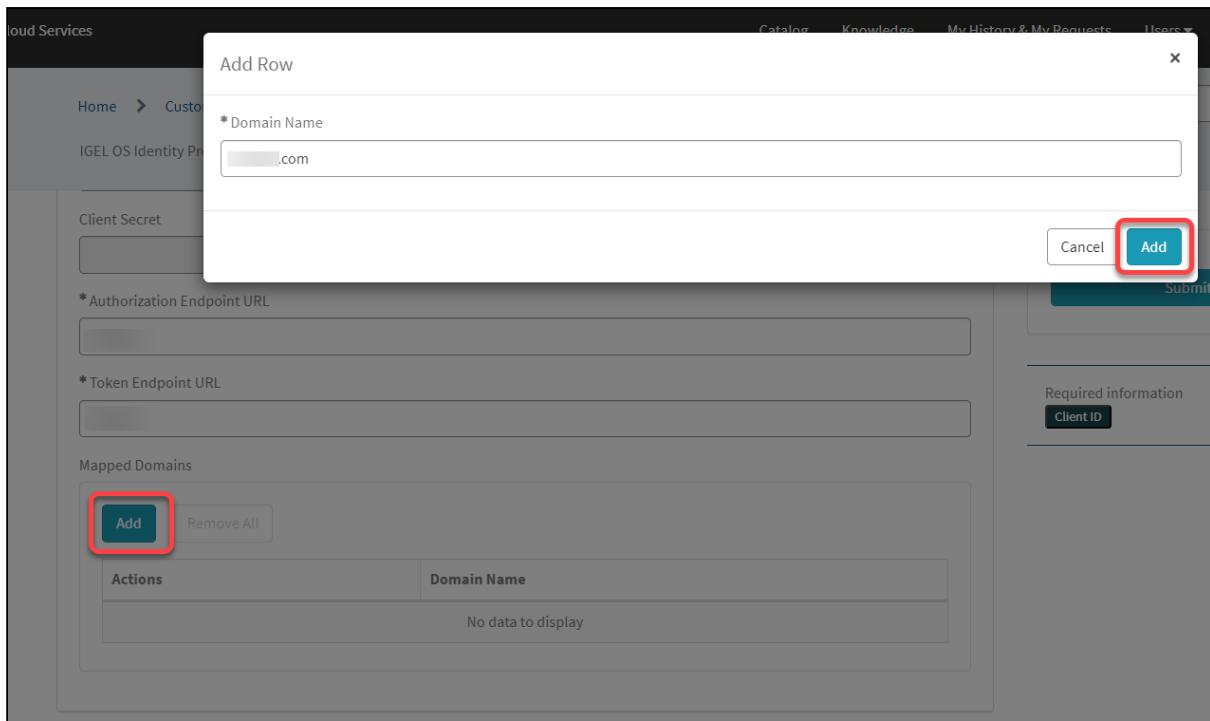
* Authorization Endpoint URL
https://i.okta.com/oauth2/default/v1/authorize

* Token Endpoint URL
https://i.okta.com/oauth2/default/v1/token

Mapped Domains

Actions	Domain Name
	No data to display

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



11. Click **Submit.**

The data record is created.

Configuring Roles

For information, see: <https://developer.okta.com/docs/guides/customize-tokens-returned-from-okta/main/>

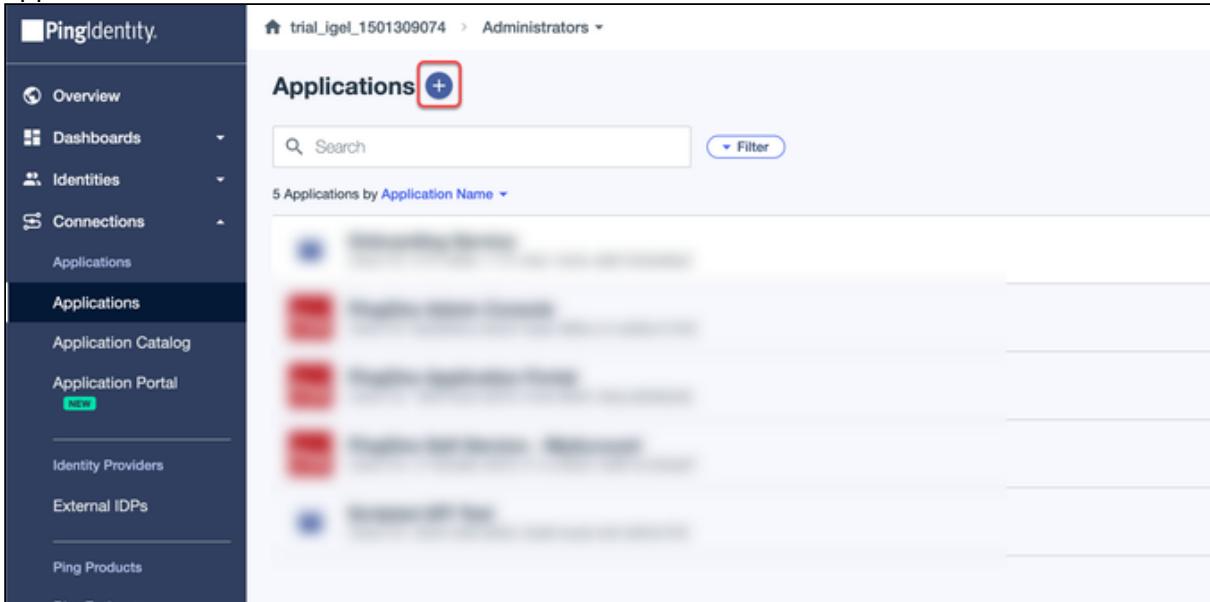
Configuring Ping as Identity Provider

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

1. [Creating a Ping Application That Will Serve as Identity Provider \(see page 106\)](#): 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 \(see page 109\)](#): This will enable IGEL Cloud Services to use our Ping Application as the external identity provider.
3. [Configuring roles \(see page 117\)](#): We make the user role information accessible for the (12.04.120) Default Directory Rules feature of the UMS.

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.



The screenshot shows the 'PingIdentity' interface. The left sidebar has a dark theme with white text and icons. It includes sections for Overview, Dashboards, Identities, Connections, Applications (which is currently selected), Application Catalog, Application Portal (with a 'New' button), Identity Providers, External IDPs, and Ping Products. The main content area is titled 'trial_igel_1501309074 > Administrators'. It shows a list of applications under the heading 'Applications'. A red box highlights the blue '+' button at the top right of the application list. Below the '+' button is a search bar and a 'Filter' dropdown. The list contains several blurred application entries.

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

Add Application

Application Name *

Description

Icon



Max Size 1.0 MB

Application Type

Show Details

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

SAML Application

OIDC Web App

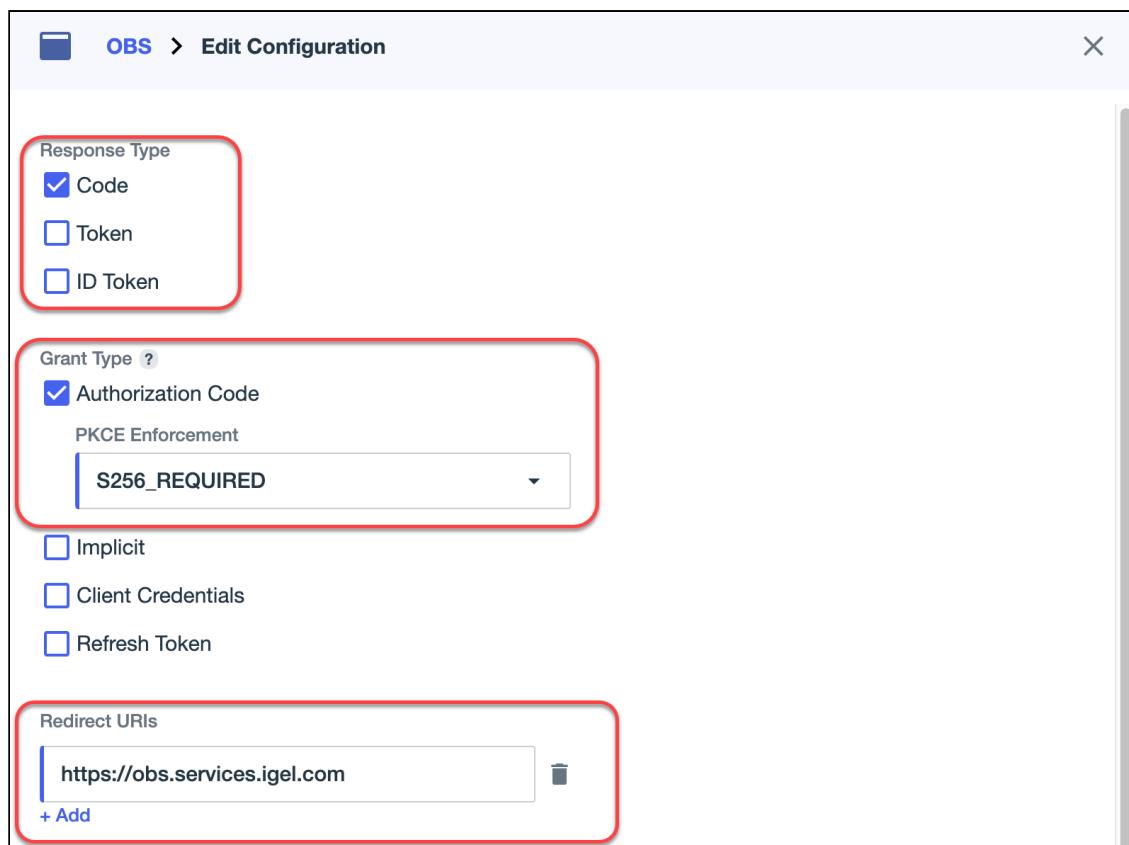
Native

Single-Page

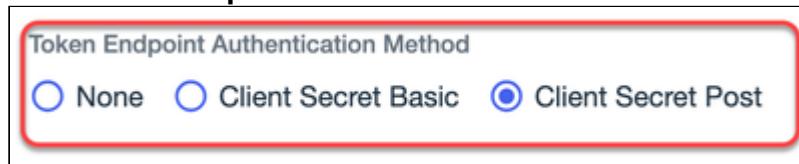
Worker

3. Edit the settings under **Edit Configuration** as follows and then click **Save**.

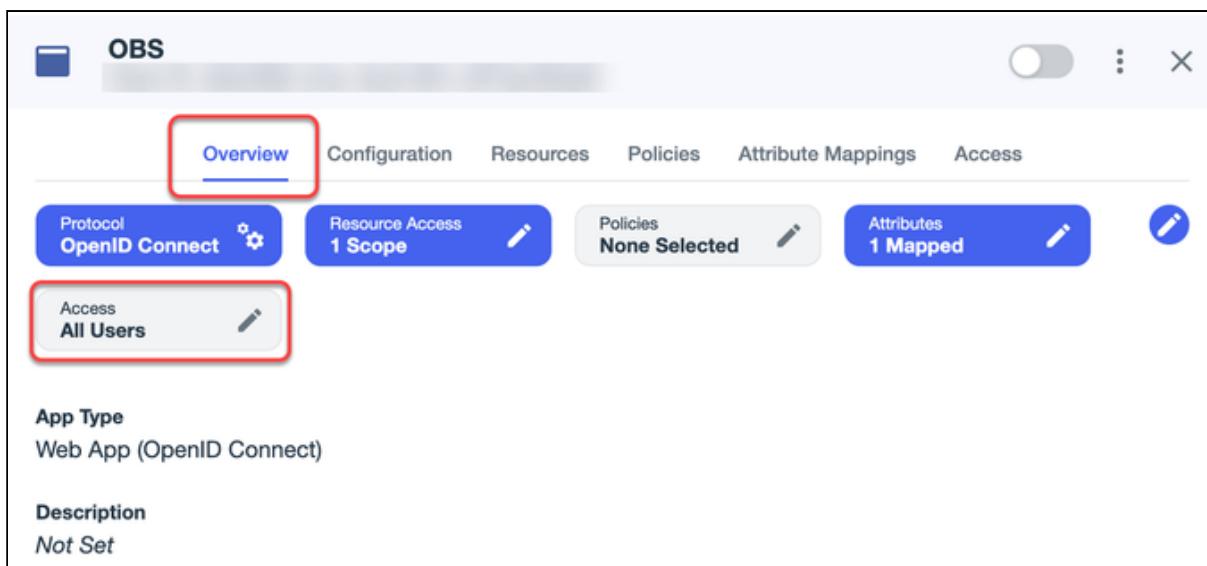
- Under **Response Type**, make sure **Code** is selected.
- Make sure that as the **Grant Type**, the option **Authorization Code** is selected and that the **Proof Key for Code Exchange (PKCE) Enforcement** is set to **S256_REQUIRED**.
- Under **Redirect URIs**, add " <https://obs.services.igel.com/> ".



- 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 screenshot shows the OBS interface with the 'Overview' tab selected. Key components include:

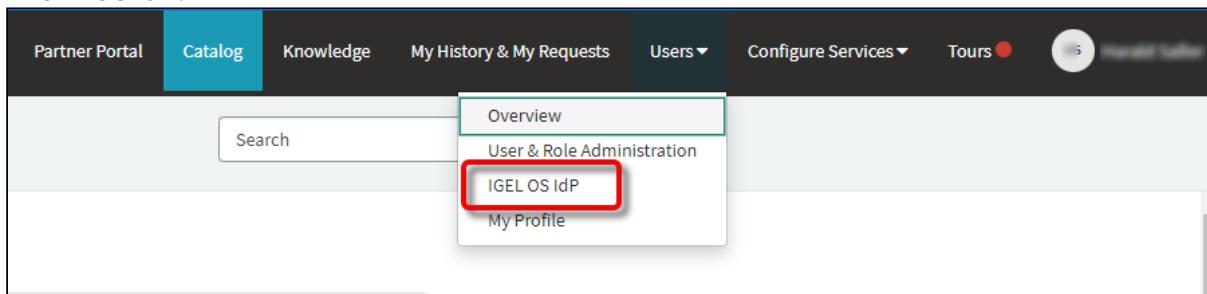
- Protocol:** OpenID Connect
- Resource Access:** 1 Scope
- Policies:** None Selected
- Attributes:** 1 Mapped
- Access:** All Users (highlighted with a red box)

Below these, there are sections for **App Type** (Web App (OpenID Connect)) and **Description** (Not Set).

The app integration is created.

Registering Our Ping Application in the IGEL Customer Portal

1. Open the [IGEL Customer Portal](#)⁴⁹ in your browser, log in to your admin account, and select **Users > IGEL OS IdP**.



The screenshot shows the IGEL Customer Portal navigation bar with the 'Users' dropdown menu open. The 'IGEL OS IdP' option is highlighted with a red box.

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

49. <https://support.igel.com>

IGEL OS IdP Management							
All > Account =					Update client secret	Update Mapped Domains	Register IGEL OS IdP
Display name	Client ID	Client Secret	Authorization URL	Token URL	Mapped Domains	Created	Last modified
*****	*****	*****	*****	*****	*****	2022-10-13 12:16:26	1
*****	*****	*****	..	*****	*****	2022-09-28 15:19:29	1
*****	*****	*****	..	*****	*****	2022-10-11 08:39:53	0

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

* Indicates required

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

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

Mapped Domains

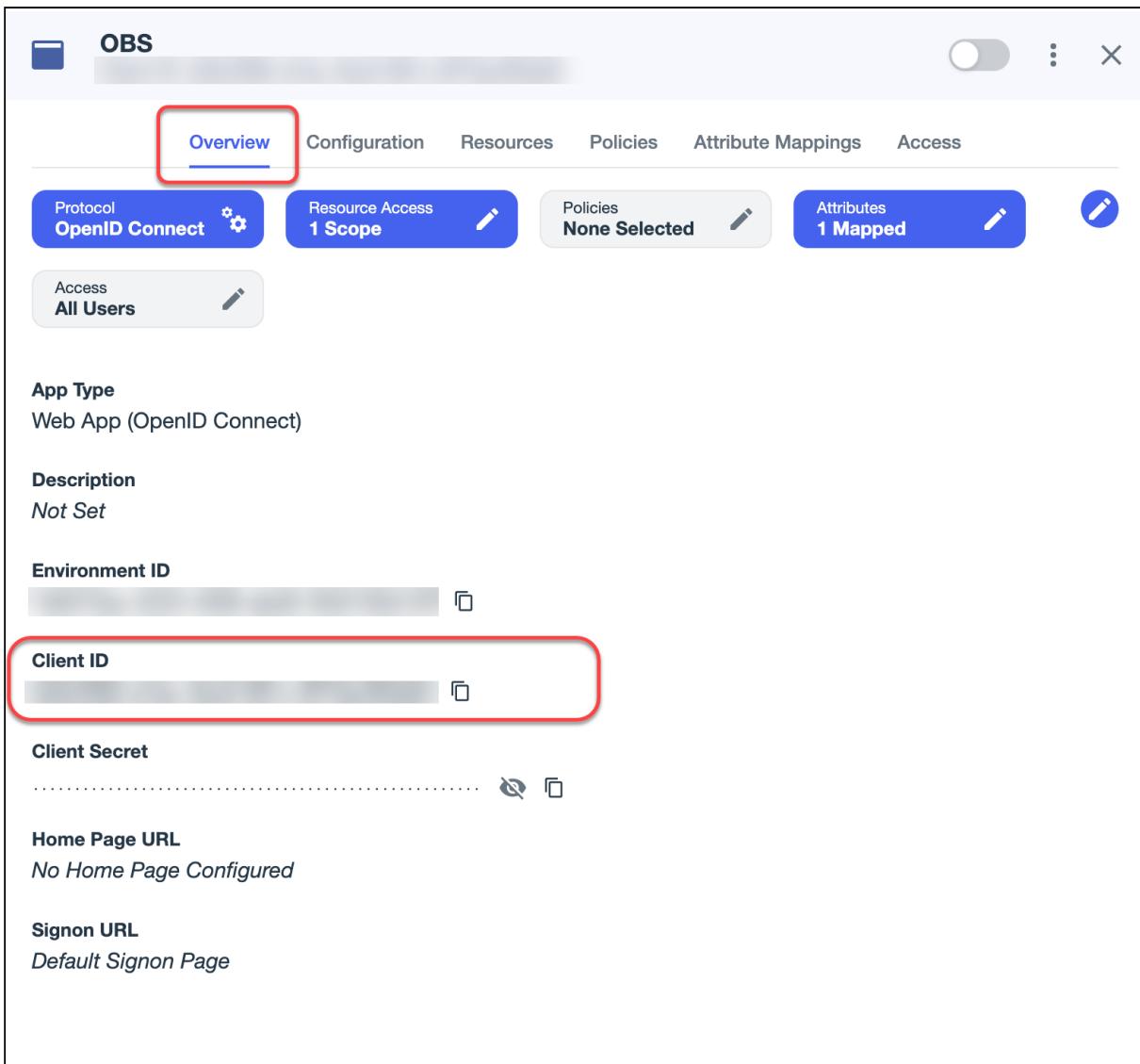
Add	Remove All
Actions	Domain Name
No data to display	

Submit

Required information

Client ID **Authorization Endpoint URL**
Token Endpoint URL

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



The screenshot shows the OBS configuration interface. The top navigation bar includes tabs for Configuration, Resources, Policies, Attribute Mappings, and Access. Below the tabs are several status indicators: Protocol (OpenID Connect), Resource Access (1 Scope), Policies (None Selected), and Attributes (1 Mapped). The main content area displays configuration details:

- App Type:** Web App (OpenID Connect)
- Description:** Not Set
- Environment ID:** (redacted)
- Client ID:** (redacted) (highlighted with a red box)
- Client Secret:** (redacted) (with copy and clear icons)
- Home Page URL:** No Home Page Configured
- Signon URL:** Default Signon Page

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

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name
My OBS identity provider

* Client ID

* Client Secret

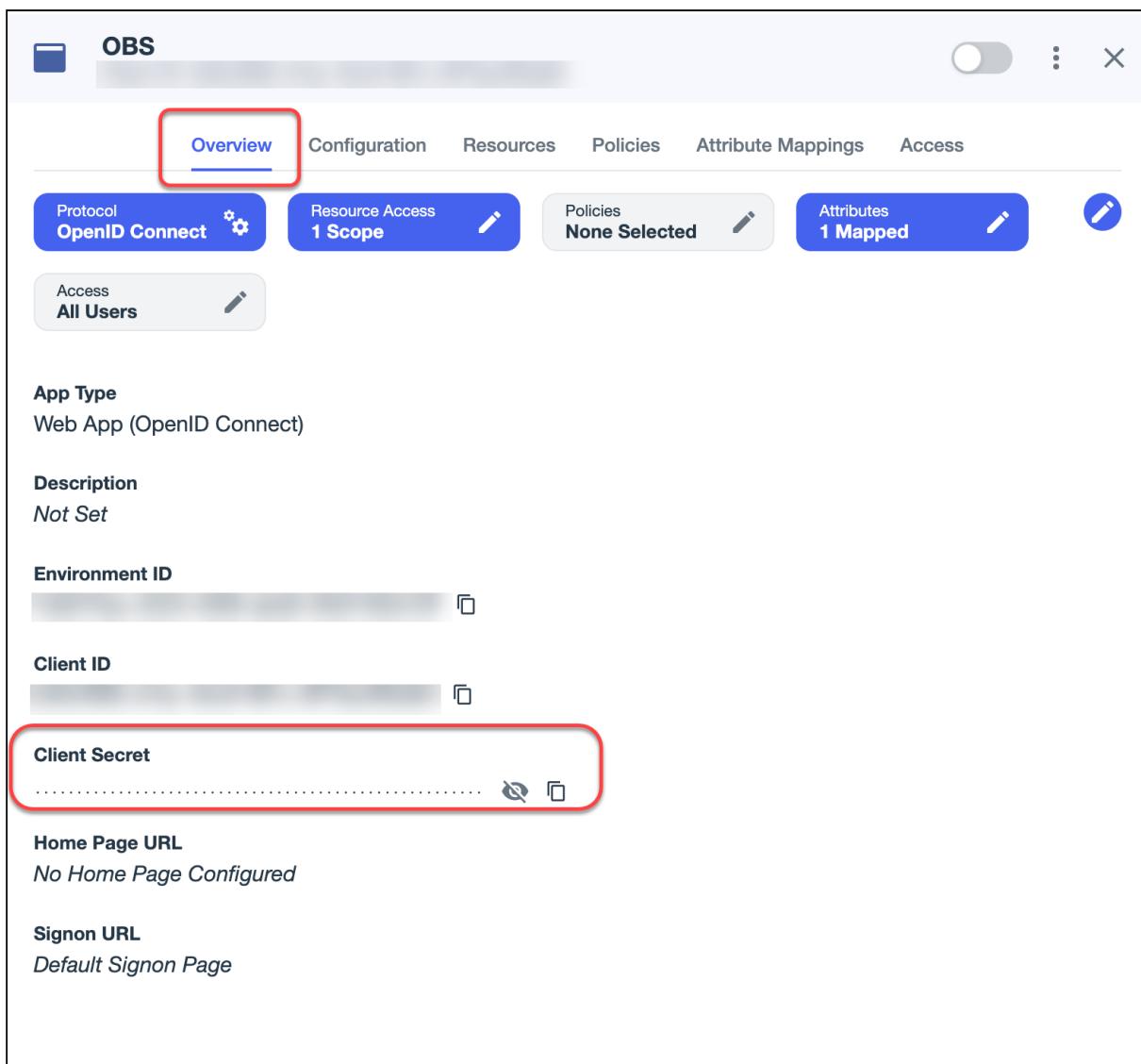
* Authorization Endpoint URL

* Token Endpoint URL

Mapped Domains

Actions	Domain Name
No data to display	

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



Protocol
OpenID Connect 

Resource Access
1 Scope 

Policies
None Selected 

Attributes
1 Mapped  

Access
All Users 

App Type
Web App (OpenID Connect)

Description
Not Set

Environment ID
[REDACTED] 

Client ID
[REDACTED] 

Client Secret
.....  

Home Page URL
No Home Page Configured 

Signon URL
Default Signon Page

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

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name
My OBS identity provider

* Client ID

* Client Secret
| SHOW

* Authorization Endpoint URL

* Token Endpoint URL

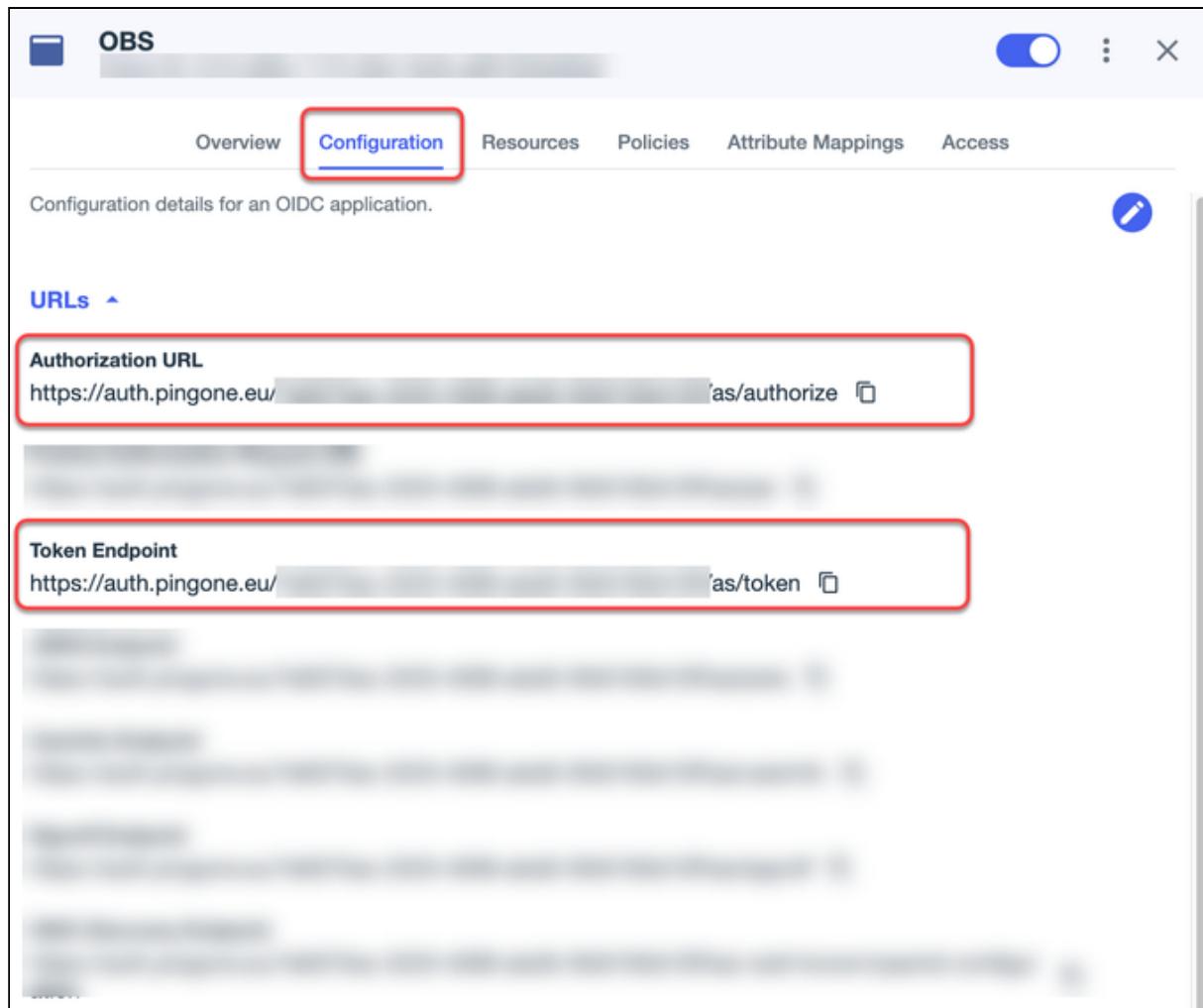
Mapped Domains

Add Remove All

Actions	Domain Name
	No data to display



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



The screenshot shows the OBS configuration interface. The 'Configuration' tab is selected. Below it, there is a section titled 'Configuration details for an OIDC application.' with a blue edit icon. The 'URLs' section contains two fields highlighted with red boxes:

- Authorization URL:** https://auth.pingone.eu/as/authorize
- Token Endpoint:** https://auth.pingone.eu/as/token

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

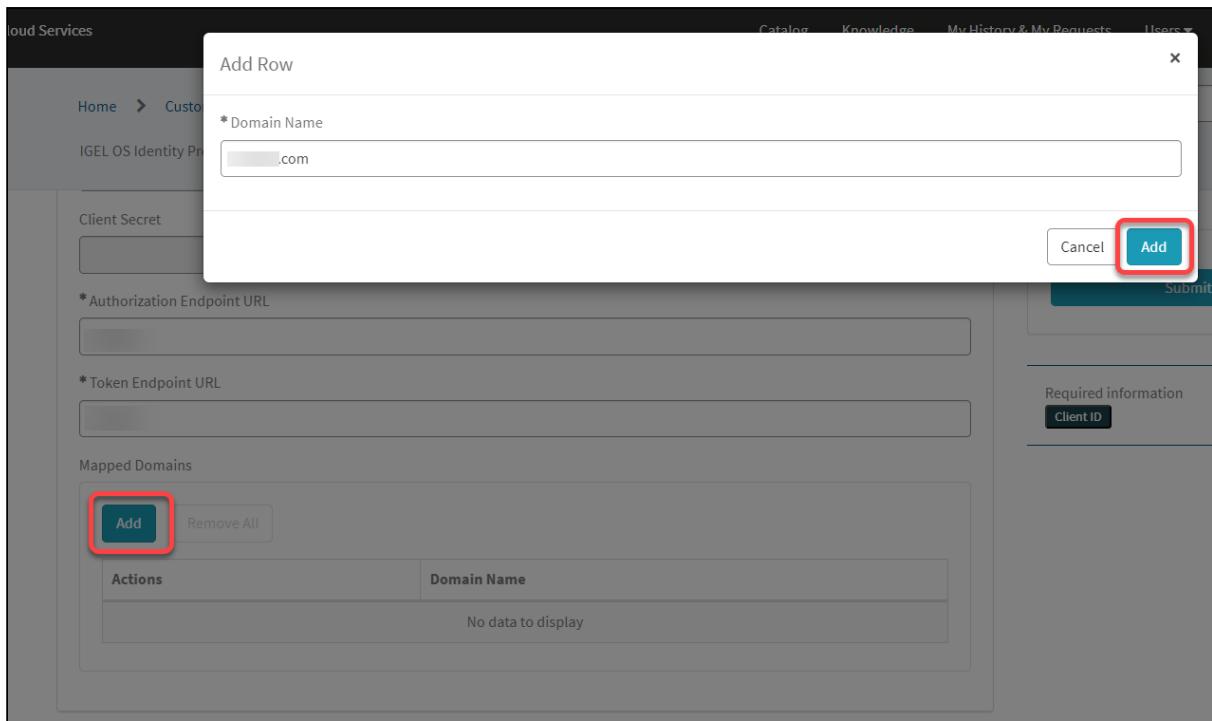
* Authorization Endpoint URL
https://auth.pingone.eu/ /as/authorize

* Token Endpoint URL
https://auth.pingone.eu/ /as/token

Mapped Domains

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.



The screenshot shows the 'Add Row' dialog for creating a new identity provider. The dialog has fields for 'Domain Name' (containing '.com'), 'Client Secret' (redacted), 'Authorization Endpoint URL' (redacted), and 'Token Endpoint URL' (redacted). At the bottom right of the dialog are 'Cancel' and 'Add' buttons, with 'Add' being highlighted by a red box. In the background, there's a table titled 'Mapped Domains' with an 'Add' button highlighted by a red box.

11. Click **Submit.**

The data record is created.

Configuring Roles

For information, see https://docs.pingidentity.com/pingone/directory/p1_user_attributes.html.

Configuring Other Identity Providers

If you are using a different Identity Provider that supports the OpenID Standard, you will need to add an Application Integration with the following parameters:

- **Type:** Web Application
- **Proof Key for Code Exchange:** Authorisation code flow with PKCE grant
- **Redirect URI:** `https://obs.services.igel.com`
- The following `scope` and claim values must be supported:
 - `openid`
 - `profile`

The following Claim Values need to be requested by `profile` :

- `name`
- `preferred_username`
- `email`

The following Claim Values need to be requested by `email` :

- `email`

For the detailed description of scope and claim values, see the relevant section of the OpenID Connect Basic Client Implementer's Guide at https://openid.net/specs/openid-connect-basic-1_0.html#Scopes.

With this configured on your Application Integration, you provide the following information in our [IGEL Customer Portal](#)⁵⁰:

- **Authorization Endpoint**
The URL to initiate the authentication
- **TOKEN Endpoint**
URL to request a token from
- **CLIENT ID**
ID of the registered application in the IdP
- **CLIENT SECRET**
Secret of the registered application in the IdP

50. <https://support.igel.com/>

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](https://app.igel.com/)⁵¹, along with the relevant changelogs / release notes.

Access to the IGEL App Portal

To import apps from the IGEL App Portal, your Universal Management Suite (UMS) must be registered in the [IGEL Customer Portal](https://now.igel.com/)⁵². If your UMS is not registered yet, refer to Registering the UMS. Please note that you must have an account with the role **UMS Admin** or **Super Admin** to register a UMS. For details, see Managing Users and Roles in the IGEL Customer Portal.

- Depending on how you access the App Portal, you can perform different actions on the selected apps. For example, if you access the portal from the UMS Web App, you can import apps to the UMS.

Local Access on IGEL OS 12

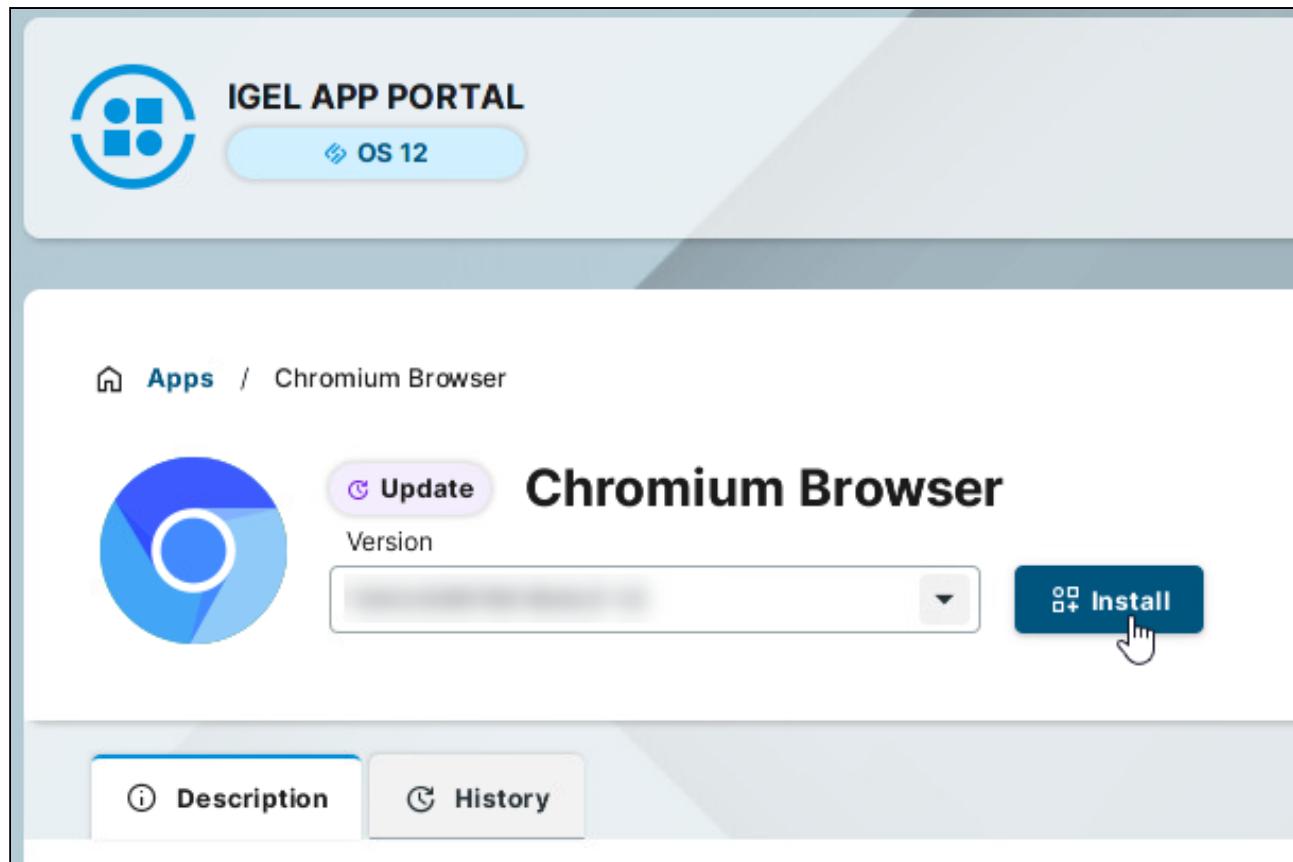
If the device is not managed with the UMS, downloading apps is possible through local access but NOT for the devices with a Starter license. For more information on licenses, see Licensing.

You can reach the App Portal locally on the device via the **App Portal** application.



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](#).

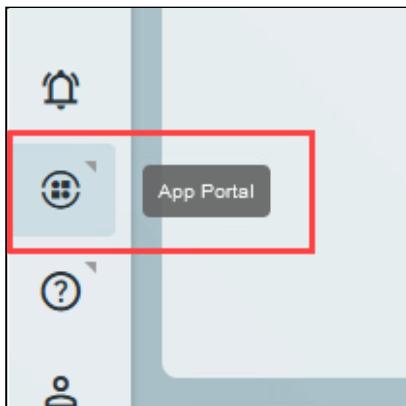
51. <https://app.igel.com/>
52. <https://now.igel.com/>



The screenshot shows the IGEL APP PORTAL interface. At the top, there's a logo and a blue button labeled "OS 12". Below that, a navigation bar shows "Apps / Chromium Browser". On the left, there's a large icon of the Chromium browser. Next to it is a purple "Update" button and a dropdown menu for "Version". To the right is a large "Install" button with a hand cursor icon. At the bottom, there are two tabs: "Description" (which is selected) and "History".

Access through the UMS Web App

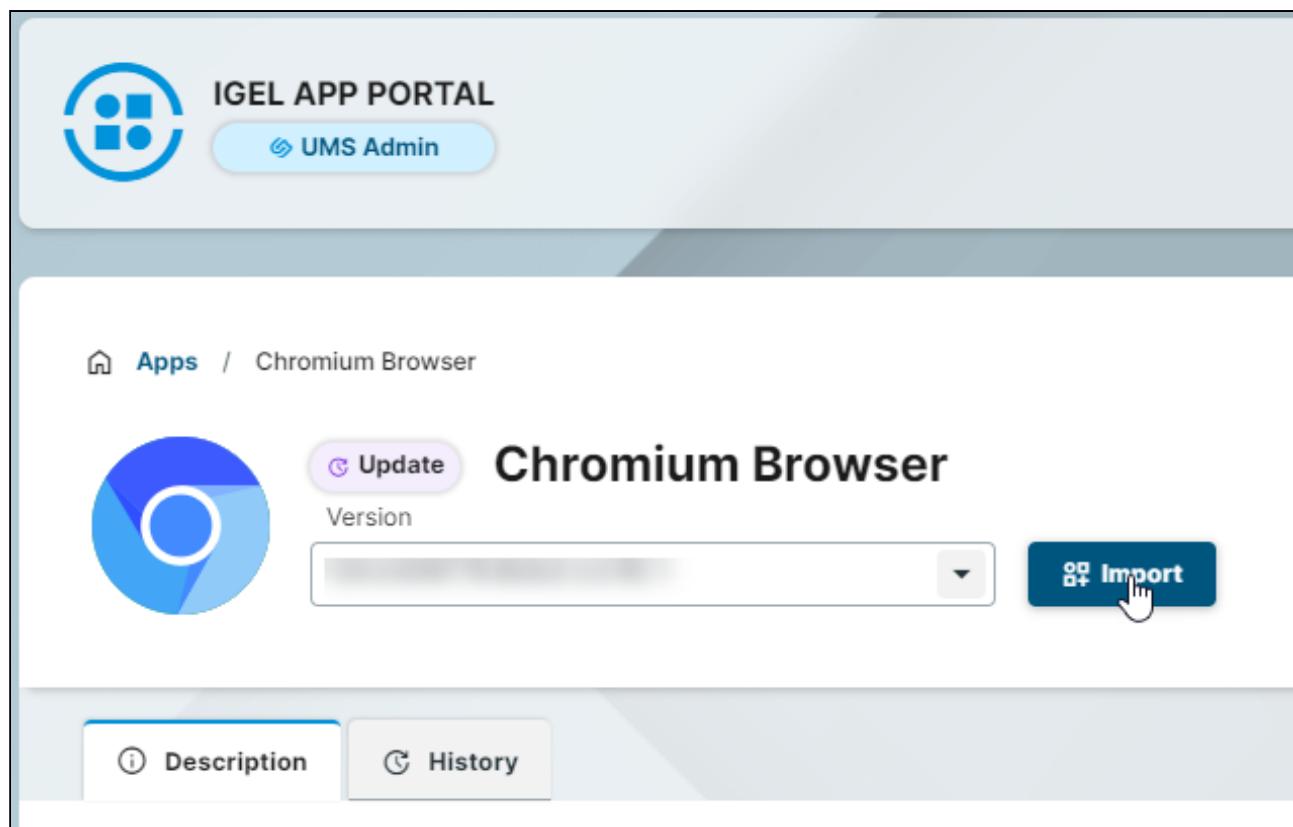
You can click the **App Portal** sidebar button. The IGEL App Portal opens in a new browser tab.



With this method, you can import apps to the UMS Web App to then deploy them to your devices. For more information, see [How to Import IGEL OS Apps from the IGEL App Portal⁵³](#) and [IGEL UMS 12: App Update⁵⁴](#).

53. <https://kb.igel.com/en/universal-management-suite/current/how-to-import-igel-os-apps-from-the-igel-app-portal>

54. <https://kb.igel.com/en/how-to-start-with-igel/current/igel-ums-12-app-update>



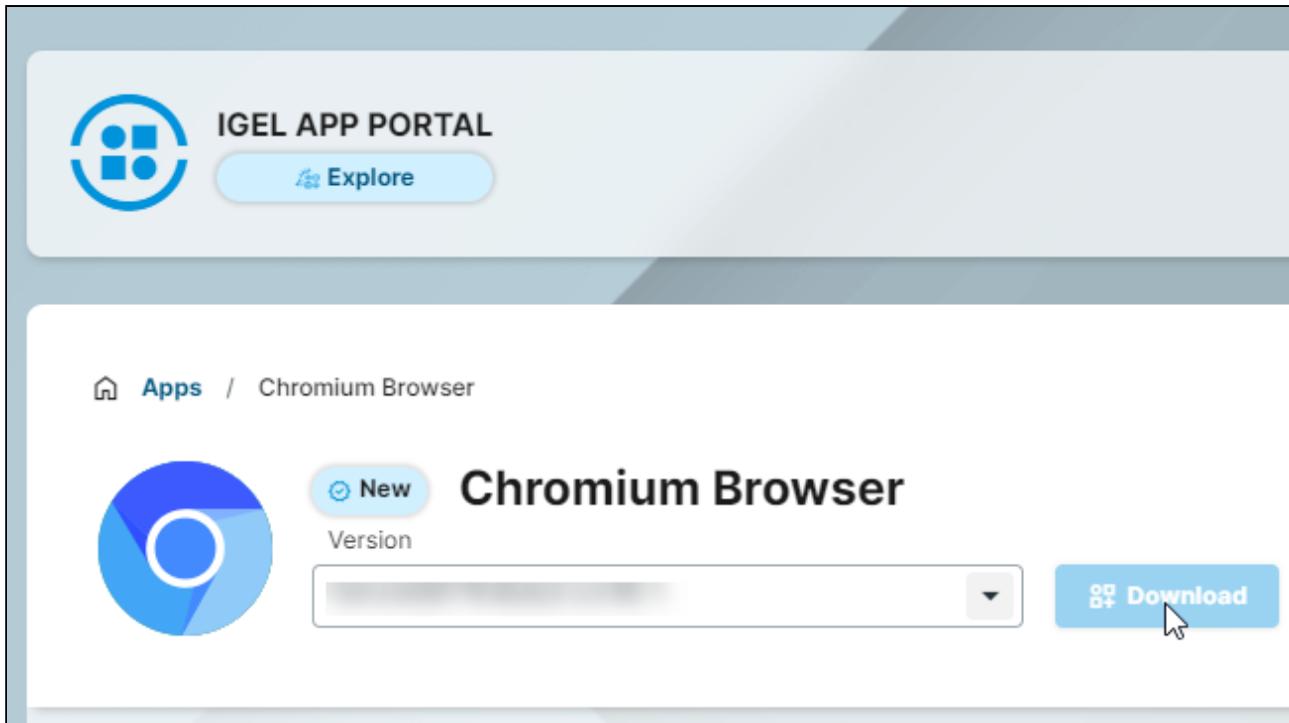
The screenshot shows the IGEL APP PORTAL interface. At the top, there's a logo and a 'UMS Admin' button. Below that, the navigation bar shows 'Apps / Chromium Browser'. The main content area features a large blue circular icon representing the app. To its right, the app name 'Chromium Browser' is displayed in bold black text. Above the name is an 'Update' button with a clock icon. Next to it is a dropdown menu labeled 'Version'. To the right of the dropdown is a large blue button with a white 'Import' icon and a hand cursor icon pointing at it. At the bottom of the screen, there are two tabs: 'Description' (which is highlighted with a blue border) and 'History'.

i For permissions required for managing apps, see [Important Information for the IGEL UMS Web App⁵⁵](#).

Direct Access through Login

By logging in directly, you can access the App Portal without a direct connection between the IGEL UMS/OS and the App Portal.

55. <https://kb.igel.com/en/universal-management-suite/current/important-information-for-the-igel-ums-web-app>



With this access method, you can download app packages to manually import them to the UMS Web App. This is used in environments with limited internet access. For more information, see [How to Install OS 12 Apps in a UMS Environment with Limited or No Internet Access](#)⁵⁶.

For direct access:

1. Open the [IGEL App Portal](#)⁵⁷.

The App Portal opens in Explore mode. Here, you can get a general overview of all the available apps even without logging in.



2. Click **Login**.

i If you logged in to the IGEL Customer Portal or the IGEL App Portal before using the same browser, you do not need to authenticate again. You are automatically logged in through SSO after clicking **Login**.

3. Enter the **user name** and **password** that you used to register on the IGEL Customer Portal and click **Sign in**. For more information on registration, see [Using the IGEL Customer Portal](#).

56. <https://kb.igel.com/en/universal-management-suite/current/how-to-install-os-12-apps-in-a-ums-environment-with-limited-or-no-internet-access>
57. <https://app.igel.com/>

User Interface - Browsing the IGEL App Portal

The screenshot shows the IGEL App Portal interface. At the top left is the IGEL logo and "App Portal". At the top right are "Login", "Logout", and "Help" buttons. Below the header is a navigation bar with "Discover Our Apps" (highlighted with a red box), "Applications" (highlighted with a red box), "Software" (highlighted with a red box), a search bar, and a dropdown menu.

Discover Our Apps

Categories

- All
- Authentication
- Base System
- BIOS
- Browser
- Browser-Based Application
- Cloud
- Codec
- Debug
- Device Redirection
- Dictation
- Digital Signage
- IGEL Ready
- Management
- Miscellaneous
- Monitoring
- Multimedia
- Network

Apps in Spotlight

Discover what makes a difference. Apps in Spotlight boost productivity, enhance user experience and bring innovation to the digital workspace. Simply IGEL it!

App	Description	Last update	Size	New
ThinPrint Client	Printing with ThinPrint? This ThinPrint app allows you to integrate thin clients with IGEL OS 12 in your ThinPrint environment.	08. October 2025	768 KB	
Zoom Desktop Client	Zoom Desktop app	06. October 2025	282.75 MB	
Chromium Browser	Chromium is an open source browser project that aims to build a safer, faster and more stable way for everyone to experience the web.	01. October 2025	200.5 MB	

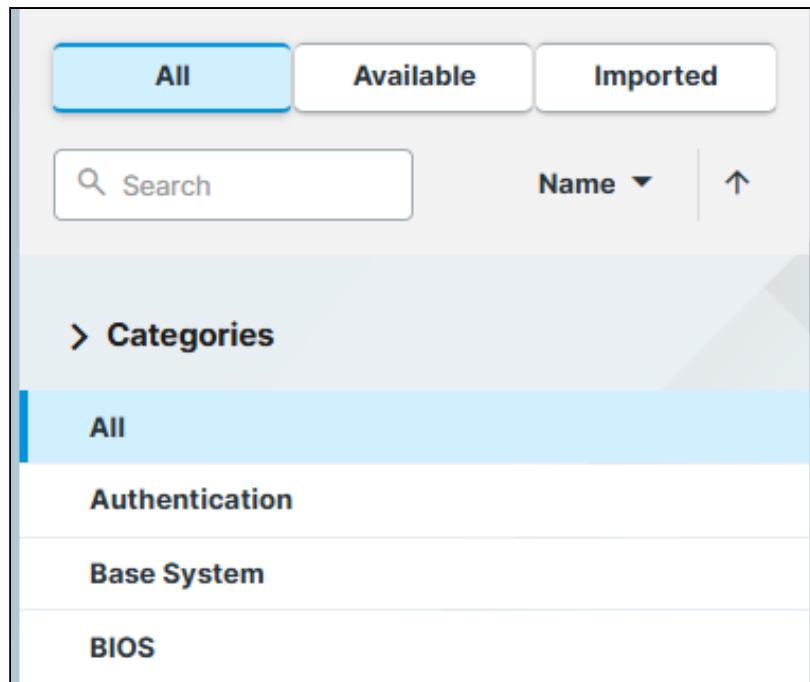
All apps

App	Description	Last update	Size	Downloads	New
90meter Smart Card PKCS#11	PKCS#11 Library to enable smartcard support for NIPRnet on Virtual Desktop Infrastructures	17. March 2025	512 KB	< 1K	
ACME Client	ACME means Automatic Certificate Management Environment. It allows for easily obtaining a machine certificate from a certificate authority...	10. October 2025	256 KB	< 1K	
Amazon WorkSpaces Client	A user can connect to an Amazon WorkSpace from IGEL OS using this Amazon WorkSpaces client.	10. October 2025	36.75 MB	3.11K	

On the left side of the portal, you can find the following tabs:

- **Applications:** Here you can find all apps available for IGEL OS 12.
 - In the area **Apps in Spotlight**, new IGEL OS 12 apps or important app updates are highlighted.
- **Software:** Here you can download the latest software versions of the IGEL UMS, IGEL OS Creator and other IGEL software products.
Older and new software versions are also available at <https://www.igel.com/software-downloads/>.

Under **Applications**, you have the filter and search options for easier browsing of the apps.



The screenshot shows the IGEL App Portal interface. At the top, there are three filter buttons: 'All' (highlighted in blue), 'Available', and 'Imported'. Below the buttons is a search bar with a magnifying glass icon and the word 'Search'. To the right of the search bar is a sorting dropdown set to 'Name' with an upward arrow icon. The main area is titled '> Categories' and contains a list of categories: 'All' (highlighted in blue), 'Authentication', 'Base System', and 'BIOS'.

If you access the portal from the UMS, you can use the following filter 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**.

If you access the portal from the OS, you can use the following filter buttons:

- **All:** All apps
- **Available:** All new apps and apps to be updated
- **Installed:** All apps that have already been installed on the device

You can modify the sorting of the listed apps according to your needs, and if you are looking for a specific app, you can also use the **Search** bar.

Under **Categories**, you can find category groups that collect apps according to their functions for an easier overview.

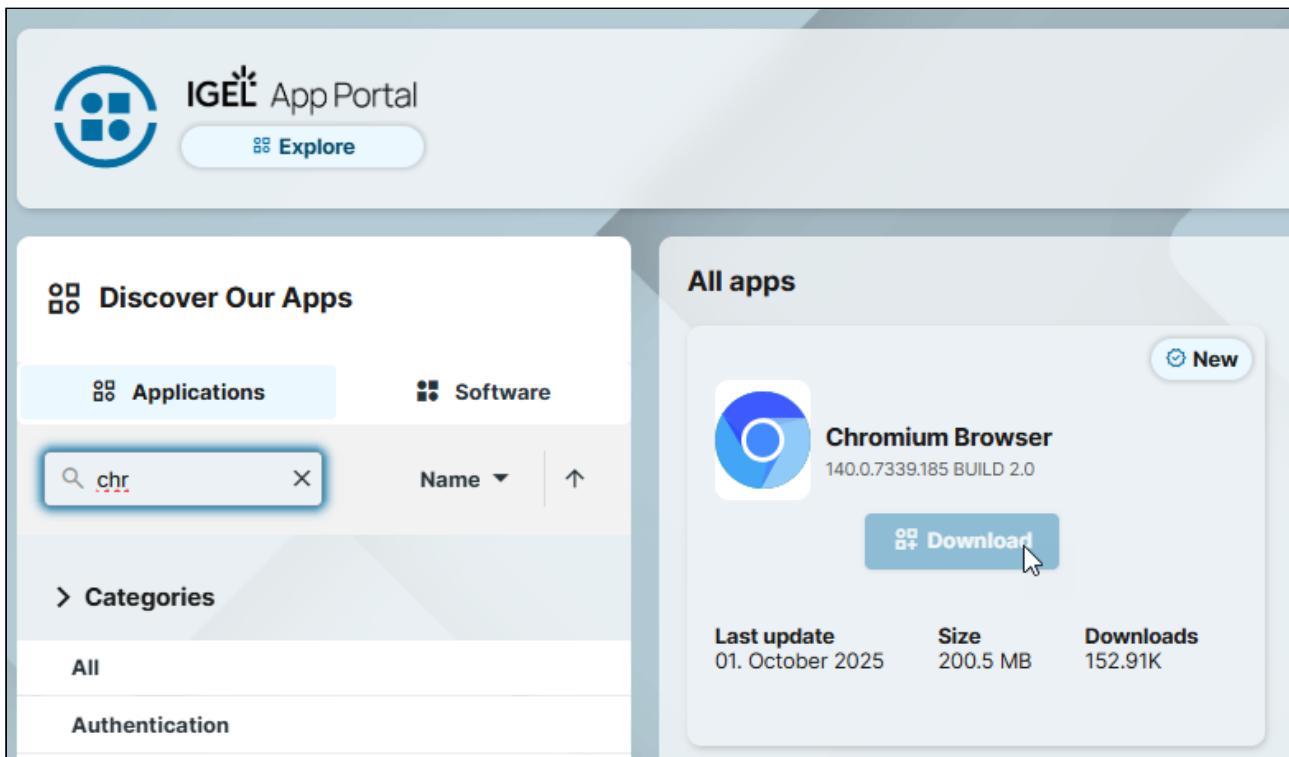


 **IGEL Ready Apps**

In the category **IGEL Ready**, you can find applications developed by IGEL Ready partners. For more information, visit the IGEL Ready page at <https://www.igel.com/ready/showcase-categories/software-and-applications/>.

Actions on Cards

The applications that correspond to the selected category/given search criteria are shown as cards. You can click the action button on the card to perform the action for the latest version of the app. The available action depends on the access mode, see the description above.



The screenshot shows the IGEL App Portal interface. On the left, there's a sidebar titled "Discover Our Apps" with categories "Applications" (selected) and "Software". A search bar contains "chr" and dropdown filters for "Name" and sorting. Below the sidebar are "Categories" links for "All" and "Authentication". On the right, a main panel titled "All apps" lists "Chromium Browser" as a "New" application. The card includes the app icon, name, version ("140.0.7339.185 BUILD 2.0"), a "Download" button, and stats ("Last update 01. October 2025", "Size 200.5 MB", "Downloads 152.91K").

App Details View

You can click the card to open the details view of the app. Here you can find the basic information under **Description** and the changelog under **History**.

The screenshot shows the IGEL APP PORTAL interface. At the top, there's a navigation bar with the IGEL logo, a 'Login' button, and a user icon. Below the navigation is a search bar with the placeholder 'Explore'. A banner on the right says 'We enable people to build amazing things'. The main content area shows the 'Chromium Browser' app details. It has a large blue circular icon, a 'New' button, a dropdown menu for 'Version', and a prominent 'Download' button. Below this, there are tabs for 'Description' and 'History'. The 'Description' tab contains a section about Chromium being an open source browser project. Technical details are listed in a table:

Categories	Author	Version	Published Date
browser	IGEL Technology GmbH	124.0.6367.78 BUILD 2.0 RC 1	02. May 2024
Architectures	Size	Vendor	
x64	133.25MB	The Chromium Authors	

Dark Mode and Light Mode

You can use the App Portal in light or dark mode. The default setting is light mode. To switch from light to dark mode, click the button in the top right corner.

The screenshot shows the same IGEL APP PORTAL interface, but it is now in dark mode. The background is dark grey, and the UI elements are white or light grey. The 'Login' button and user icon are visible in the top right corner. A red arrow points to the top right corner of the header, highlighting the mode switcher button.

The mode setting is saved locally, meaning a refresh of the browser page will keep the setting active. To go back to light mode, click the button again.

The screenshot shows the IGEL APP PORTAL interface in dark mode. The left sidebar has a dark theme with white text. The main content area displays a grid of app cards. A red arrow points to the top right corner of the header, highlighting the mode switcher button. The cards show various browsers: Chromium Browser, Firefox ESR, Microsoft Edge, and Prisma Access Browser, each with its version number, last update, size, and download count.

Useful Links

At the bottom of the portal, you can find links to IGEL social media sites and other useful links, like Terms & Conditions.

IGEL UMS 12: Basic Configuration

IGEL UMS 12 uses a web-based user interface to administer IGEL OS devices, see [IGEL UMS Web App⁵⁸](#).

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 App⁵⁹](#).

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 Server⁶⁰](#).

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 UMS⁶¹](#)).
 - 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 [How to Rename IGEL OS Devices⁶²](#).

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 the UMS Server to the existing AD, see [Active Directory / LDAP in the IGEL UMS⁶³](#).

After that, you can import users or user groups from your AD under **UMS Console > System > Administrator Accounts > Import**.

58. <https://kb.igel.com/en/universal-management-suite/current/igel-ums-web-app>

59. <https://kb.igel.com/en/universal-management-suite/current/how-to-log-in-to-the-igel-ums-web-app>

60. <https://kb.igel.com/en/universal-management-suite/current/connecting-the-ums-console-to-the-igel-ums-server>

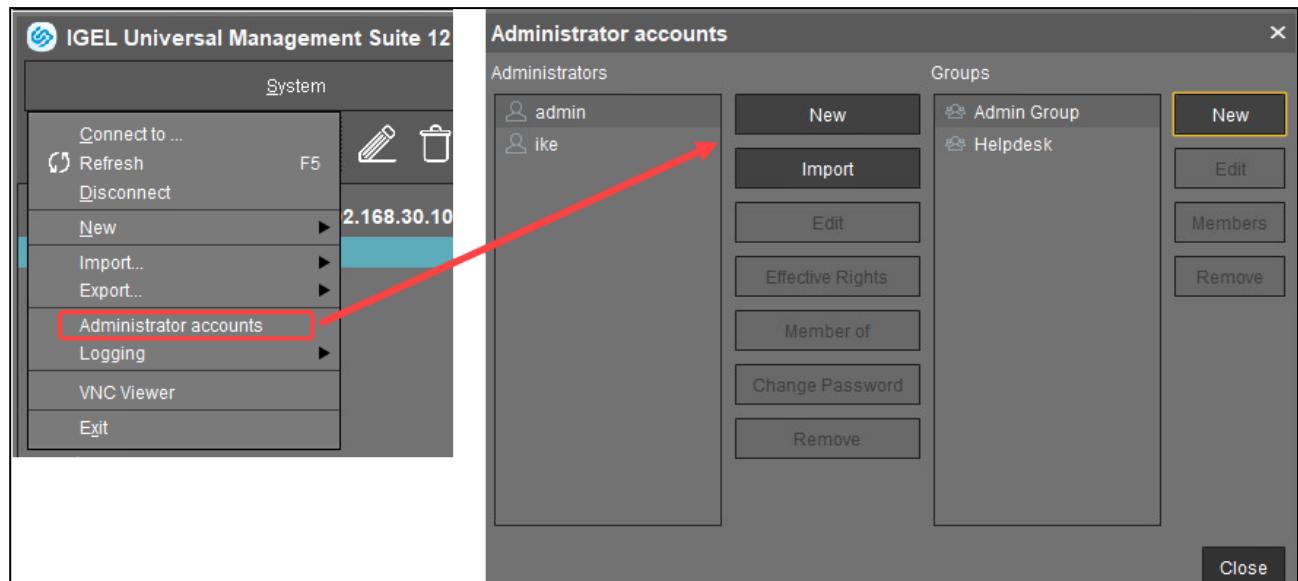
61. <https://kb.igel.com/en/universal-management-suite/current/creating-a-backup-of-the-igel-ums>

62. <https://kb.igel.com/en/universal-management-suite/current/how-to-rename-igel-os-devices>

63. <https://kb.igel.com/en/universal-management-suite/current/active-directory-ldap-in-the-igel-ums>

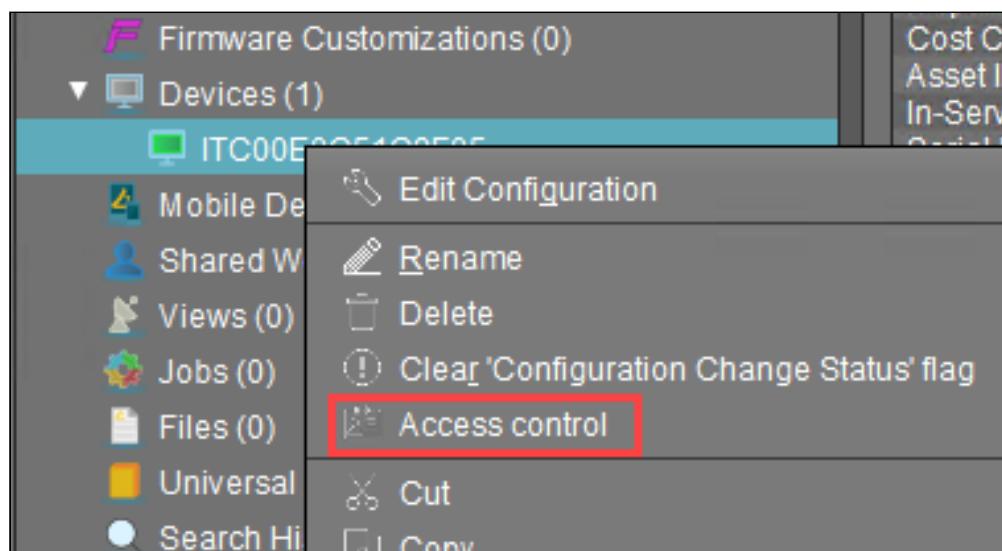
If you do not want to adopt the Active Directory structure, you can create local administrators and groups manually:
UMS Console > System > Administrator Accounts > New.

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 [Administrator Accounts in the IGEL UMS](#)⁶⁴ and [User Management and IdP Management in the IGEL UMS Web App](#)⁶⁵.

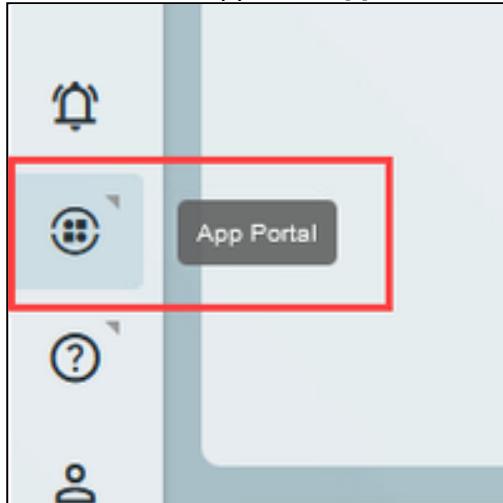
64. <https://kb.igel.com/en/universal-management-suite/current/how-to-create-administrator-accounts-in-the-igel-u>

65. <https://kb.igel.com/en/universal-management-suite/current/user-management-and-idp-management-in-the-igel-ums>

For permissions required for the UMS Web App, incl. for managing apps, see [Important Information for the IGEL UMS Web App⁶⁶](#).

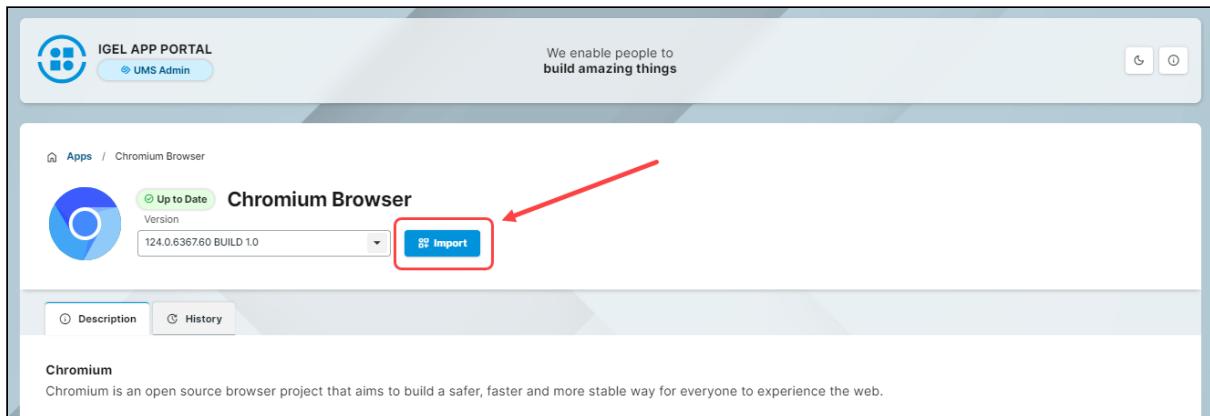
Optional: Preconfiguring Your Devices Before Onboarding

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**.

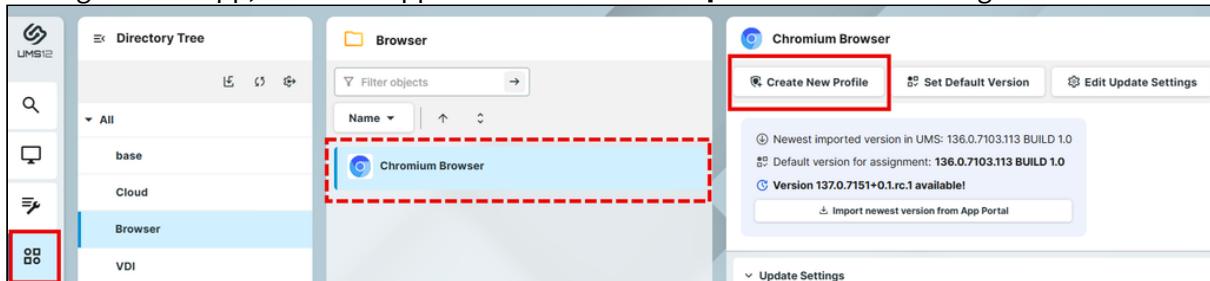
After accepting the End User License Agreement (EULA), the selected app version will be imported into the UMS.



66. <https://kb.igel.com/en/universal-management-suite/current/important-information-for-the-igel-ums-web-app>

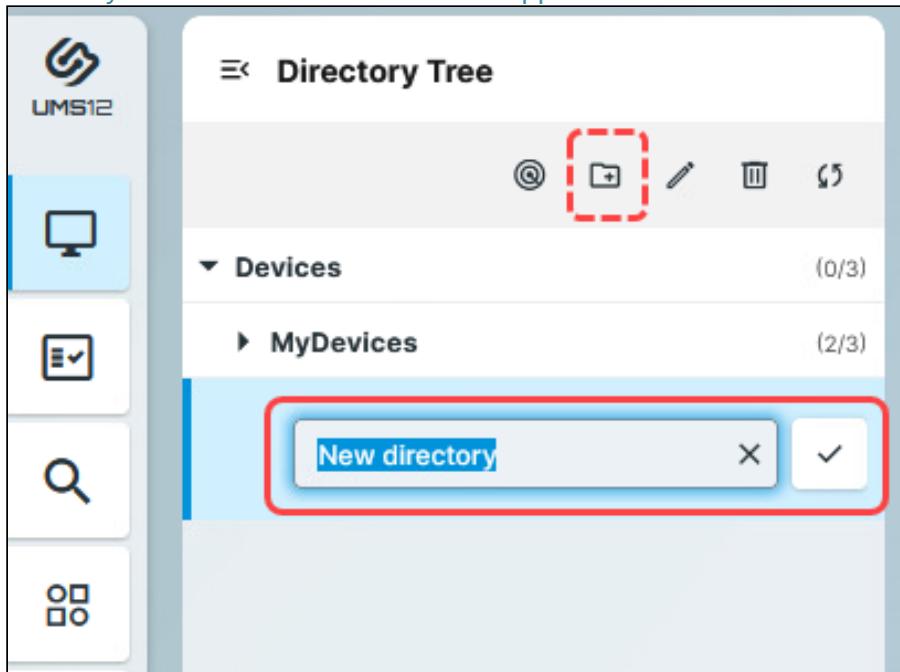
⚠ If you want to create profiles configuring IGEL OS Base System settings (e.g. SSO, accessories, etc.) before any of your IGEL OS 12 devices is registered with the UMS, import the IGEL OS Base System app. The latest app version is recommended. Alone for the purpose of profile creation, the subsequent 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.



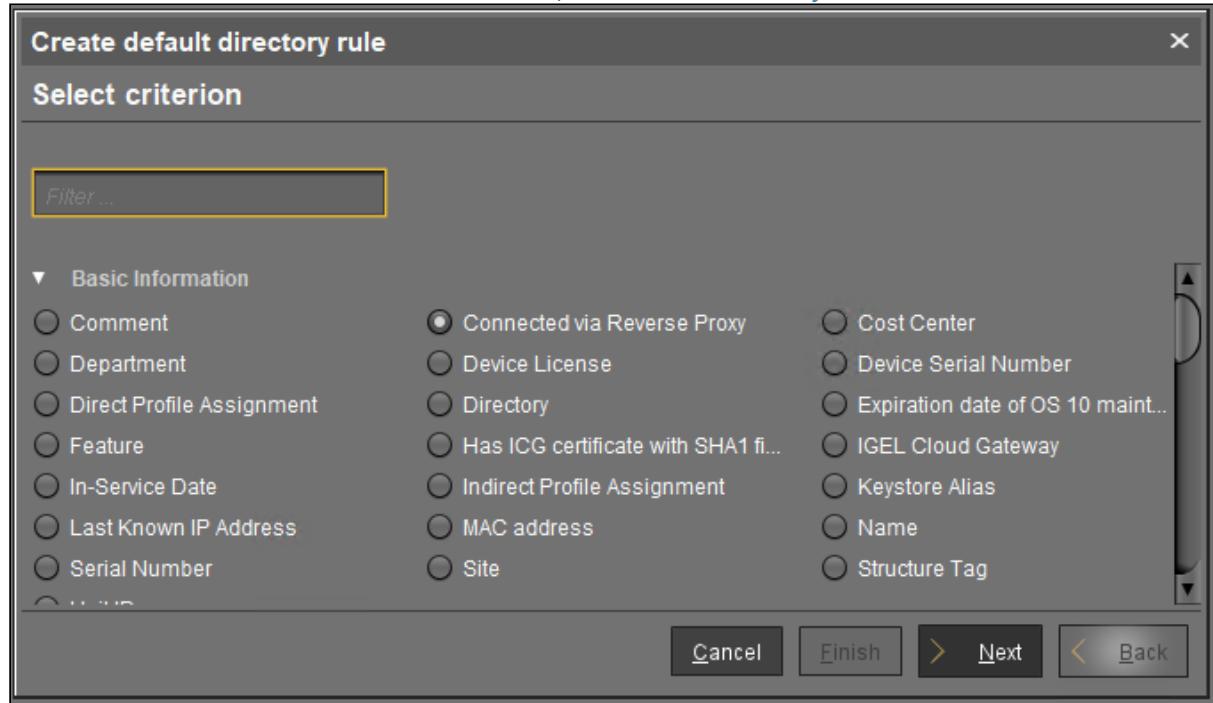
4. In order for your devices to be placed automatically in the specific directory according to certain rules during the onboarding:

1) In **UMS Web App > Devices**, create a device directory. For more information, see [Creating a Directory Structure in the IGEL UMS Web App](#)⁶⁷.



67. <https://kb.igel.com/en/universal-management-suite/current/creating-a-directory-structure-in-the-igel-ums-web>

2) In the UMS Console, go to **UMS Administration > Global Configuration > Default Directory Rules** and create the desired rule. For details, see [Default Directory Rules⁶⁸](#).



5. In the **UMS Web App > Devices**, assign the created profile to the device directory. Apply the changes.

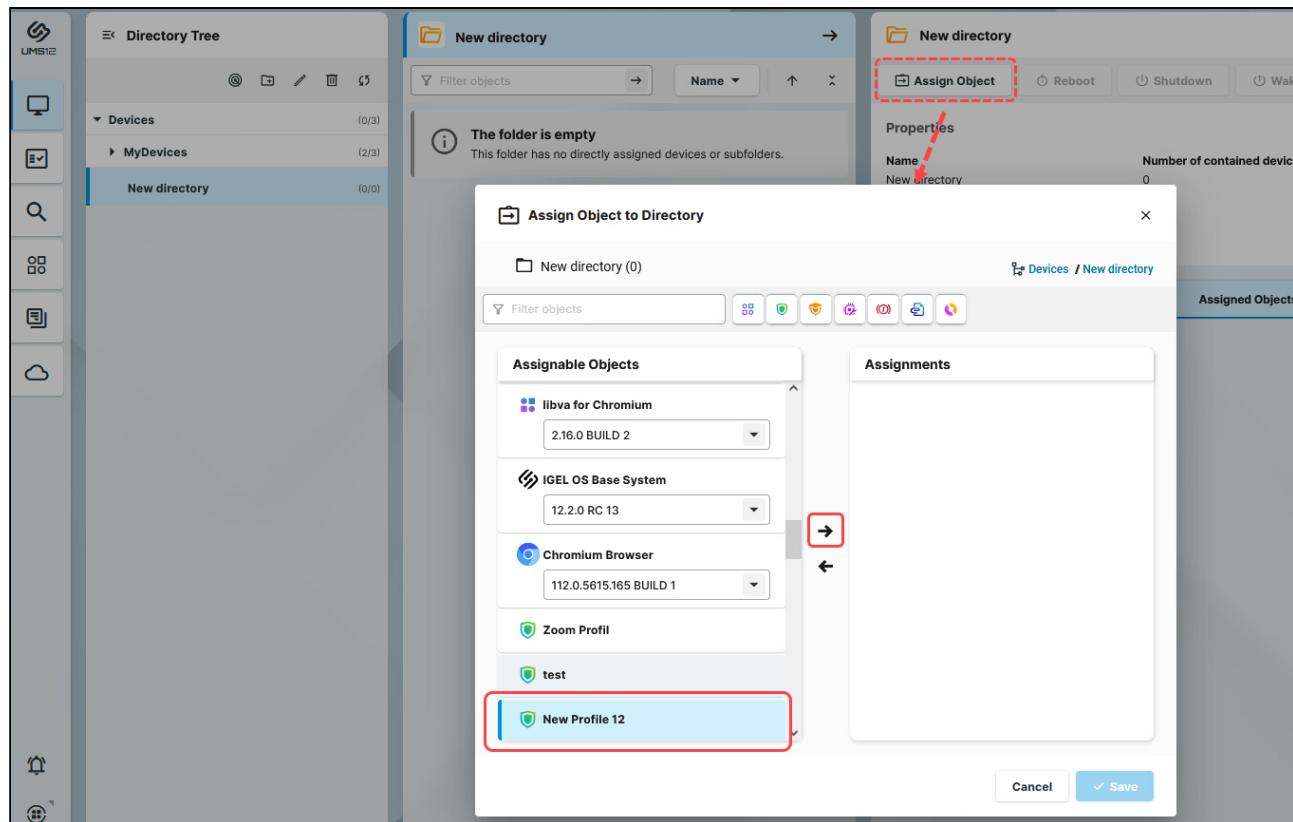
The app will be assigned to the devices via this profile (so-called "implicit app assignment") and will be installed on the devices. Exception: IGEL OS Base System app

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. For details, see [How to Configure the Background App Update in the IGEL UMS Web App⁶⁹](#).

- i 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.

68. <https://kb.igel.com/en/universal-management-suite/current/default-directory-rules>

69. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the->



All implicitly assigned apps, i.e. apps assigned to devices via a profile, are displayed directly under the profile that contains them under **Assigned Objects**.

For more information, see [How to Assign Apps to IGEL OS Devices via the UMS Web App⁷⁰](#).

- ✓ Configuring corporate design settings is easier not via profiles, but via Corporate Identity Customizations (CICs). See [How to Use Corporate Identity Customizations in IGEL UMS Web App⁷¹](#).

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:

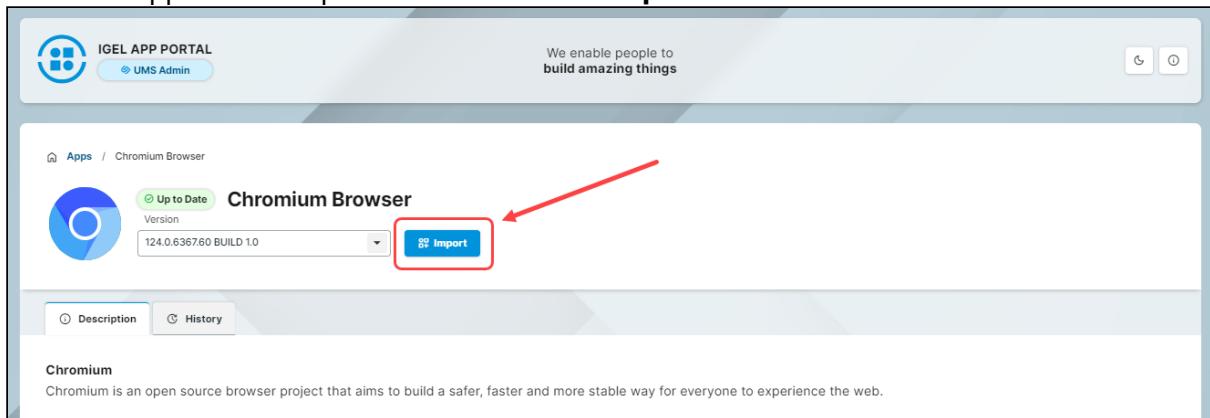
1. In the UMS Web App, click **App Portal**.

⁷⁰ <https://kb.igel.com/en/universal-management-suite/current/how-to-assign-apps-to-igel-os-devices-via-the-ums-web-app/>

⁷¹ <https://kb.igel.com/en/universal-management-suite/current/how-to-use-corporate-identity-customizations-in-igel-ums-web-app/>



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



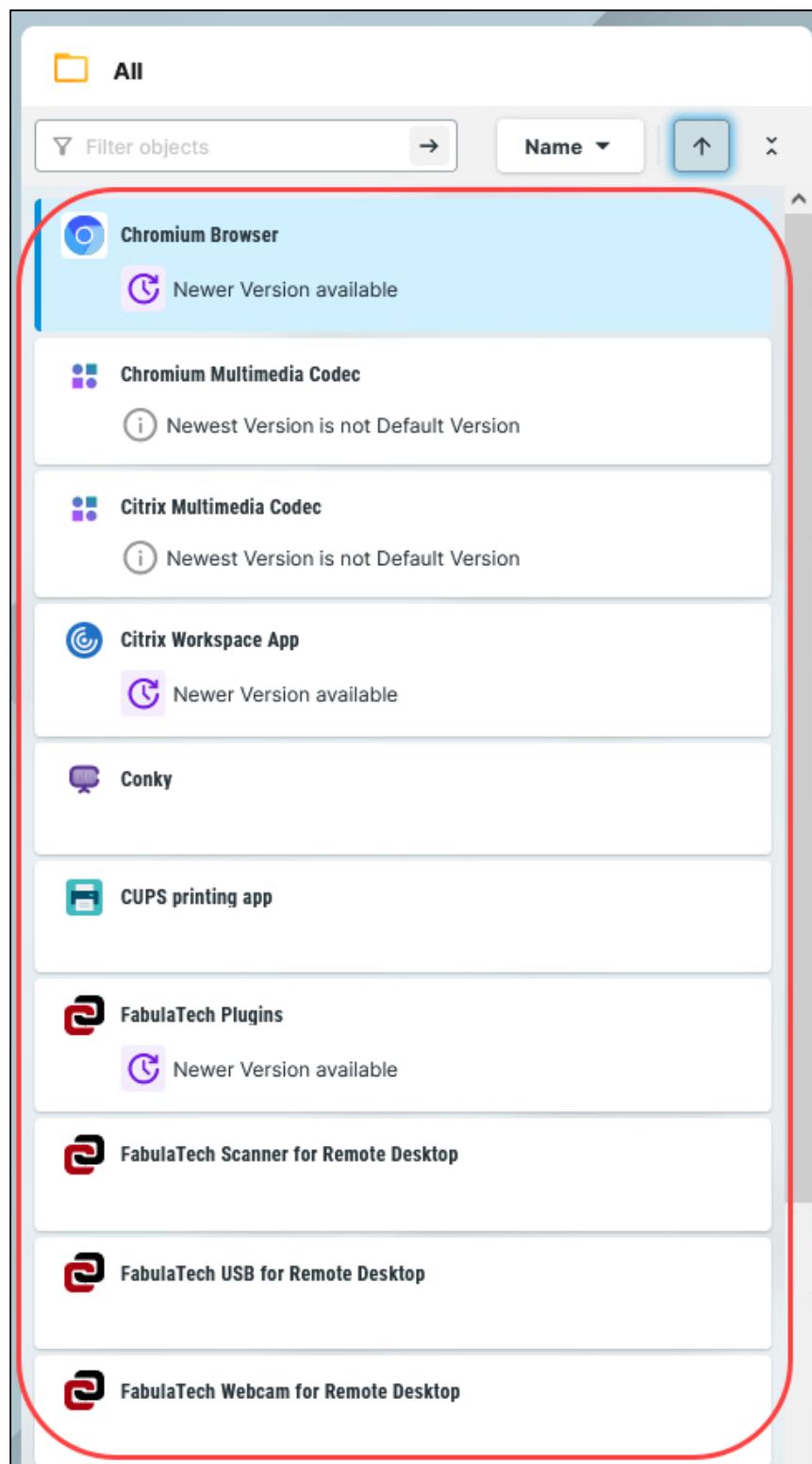
The screenshot shows the IGEL APP PORTAL interface. At the top, there's a header with the IGEL logo and a 'UMS Admin' link. Below the header, the URL 'Apps / Chromium Browser' is visible. The main content area displays the 'Chromium Browser' application details. It includes a blue circular icon, a green 'Up to Date' badge, the text 'Version 124.0.6367.60 BUILD 1.0', and a blue 'Import' button. The 'Import' button is highlighted with a red box and has a red arrow pointing to it from the left. Below the main content, there are tabs for 'Description' and 'History', and a brief description of what Chromium is.

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 under **UMS Web App > User Management** (see [User Management and IdP Management in the IGEL UMS Web App⁷²](#)) or under **UMS Console > System > Administrator accounts**.

72. <https://kb.igel.com/en/universal-management-suite/current/user-management-and-idp-management-in-the-igel-ums>



The screenshot shows a list of software packages in the IGEL UMS application. The list includes:

- Chromium Browser**: Status: Newer Version available.
- Chromium Multimedia Codec**: Status: Newest Version is not Default Version.
- Citrix Multimedia Codec**: Status: Newest Version is not Default Version.
- Citrix Workspace App**: Status: Newer Version available.
- Conky**: Status: None.
- CUPS printing app**: Status: None.
- FabulaTech Plugins**: Status: Newer Version available.
- FabulaTech Scanner for Remote Desktop**: Status: None.
- FabulaTech USB for Remote Desktop**: Status: None.
- FabulaTech Webcam for Remote Desktop**: Status: None.

The results of the app import are also displayed under **Messages** . For more information on **Messages**, see [IGEL UMS Web App User Interface](#)⁷³.

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) 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.

Versions		Assigned Devices		
4 Versions		3 Installed 1 Assigned 4 Profiles		
▶ Default version (12.01.100 BUILD 1 R...	⚙ 1	✉ 1	🛡 4	
▼ 12.1.100 BUILD 1 TP 2	⚙ 0	✉ 0	🛡 0	
File size unknown	imported by #device	imported on Jan 20, 2023		
EULA State Not Accepted				

- If you need to delete an app / app version, see [How to Delete Apps in the IGEL UMS Web App](#)⁷⁴.

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.

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 [How to Set a Default Version of an App in the IGEL UMS Web App](#)⁷⁵.

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 142).

There are two methods to create a profile:

- Via **Configuration > Profiles > Create new profile** (used to configure several apps. A profile configures ALL versions of an app, unless the version is specified.) For details, see [How to Create and Assign Profiles in the IGEL UMS Web App](#)⁷⁶.

73. <https://kb.igel.com/en/universal-management-suite/current/igel-ums-web-app-user-interface>

74. <https://kb.igel.com/en/universal-management-suite/current/how-to-delete-apps-in-the-igel-ums-web-app>

75. <https://kb.igel.com/en/universal-management-suite/current/how-to-set-a-default-version-of-an-app-in-the-igel>

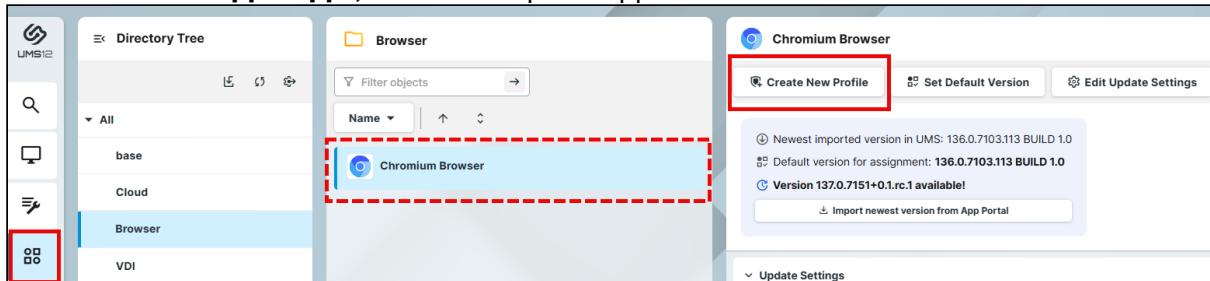
- Via **Apps > Create new profile** (used to quickly configure a profile for the selected app.) See the instructions below.

- For apps that have no configurable parameters (e.g. codecs), it is not possible to create a profile.
- If you need to delete a profile, see [How to Use the Recycle Bin in the IGEL UMS Web App](#)⁷⁷.

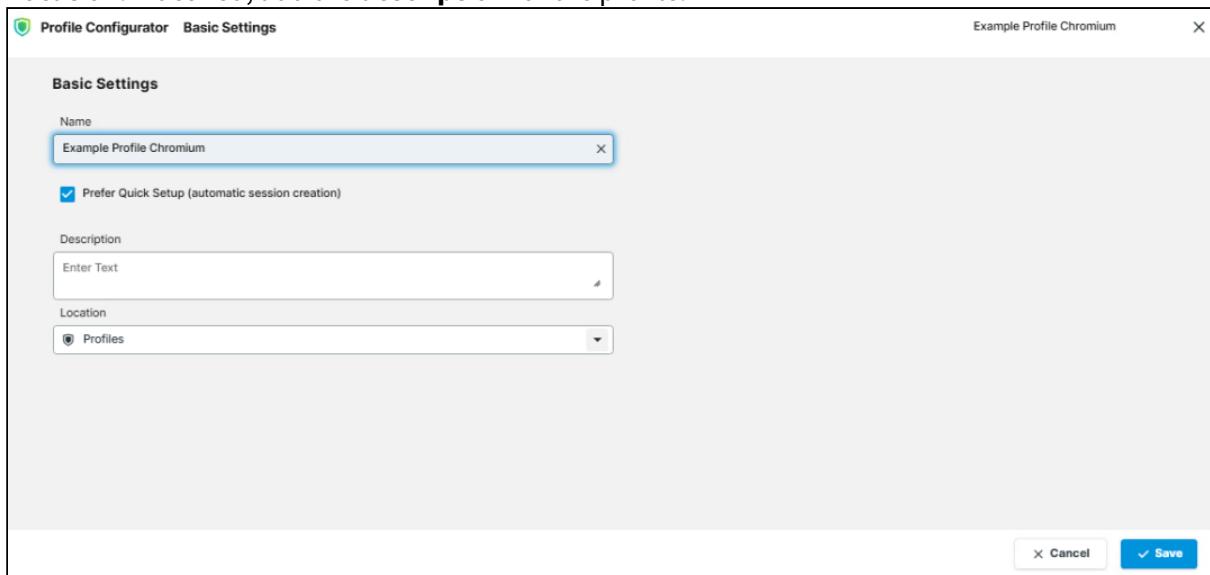
Creating a Profile in the “Apps” Tab

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.



76. <https://kb.igel.com/en/universal-management-suite/current/how-to-create-and-assign-profiles-in-the-igel-ums>
 77. <https://kb.igel.com/en/universal-management-suite/current/how-to-use-the-recycle-bin-in-the-igel-ums-web-app>

3. Optional (for a quicker profile creation): If you do not want to see all app settings available for configuration, but only those relevant for the quick start with the app, leave

Prefer Quick Setup (automatic session creation) enabled.

Quick Setup mode for the configuration dialog will be opened if available.

Note the following:

- Quick Setup mode is currently available for specific apps only.
- Quick Setup mode is available only when creating a new profile, not while editing the existing profile.
- Quick Setup mode is available for OS 12 profiles only.
- Quick Setup mode is displayed only if one app supporting it is selected in the **App Selector**. In case multiple apps or an app not supporting the Quick Setup mode are selected, Advanced Setup with all available app settings will be displayed even if **Prefer Quick Setup (automatic session creation)** is enabled.

4. Click **Save**.

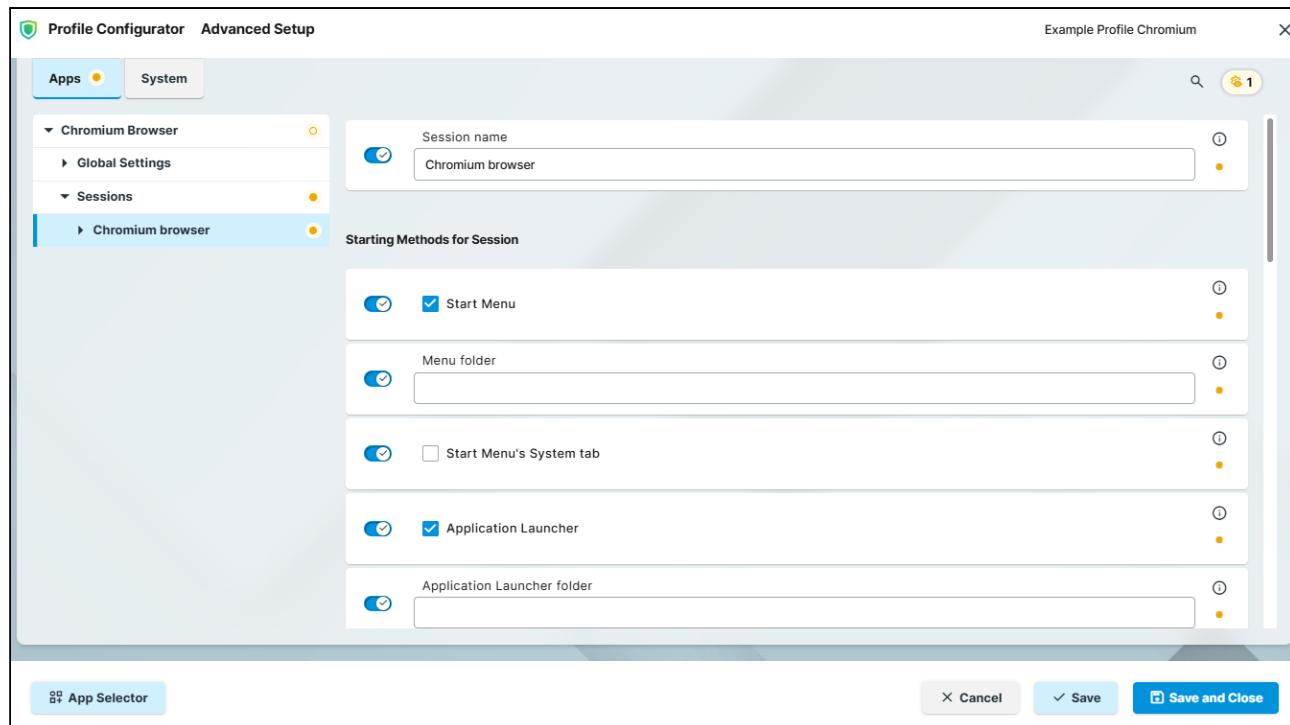
The profile will be listed under **Configuration > Profiles**.

5. 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 active and the set value will be configured by the profile.
	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.
For information on the colored icons for tracking the changes, see Configuration of IGEL OS 12 Device Settings⁷⁸ .	

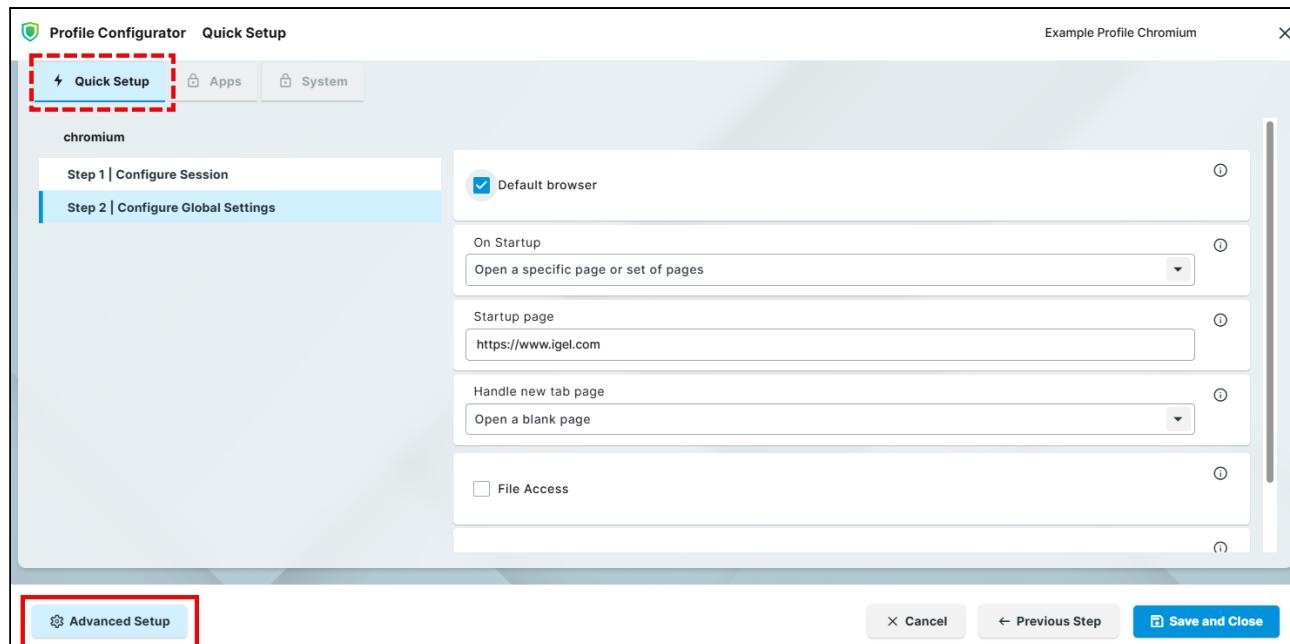
78. <https://kb.igel.com/en/igel-os-base-system/current/configuration-of-igel-os-12-device-settings>



If the Quick Setup mode is displayed, click **Advanced Setup** to show all settings available for configuration or to open **App Selector** for changing the scope of the profile.

Note the following:

- If you navigate from Quick Setup to Advanced Setup, all changes are saved and, if relevant for the selected app, one app session is automatically created.
- If you click **Cancel** while in Quick Setup mode, the profile is permanently deleted straight away.



6. Save the changes.
7. Assign the profile to the required device / device directory. See [Assignment of Apps and Profiles](#) (see page 142).

Setting a Default Version of an App

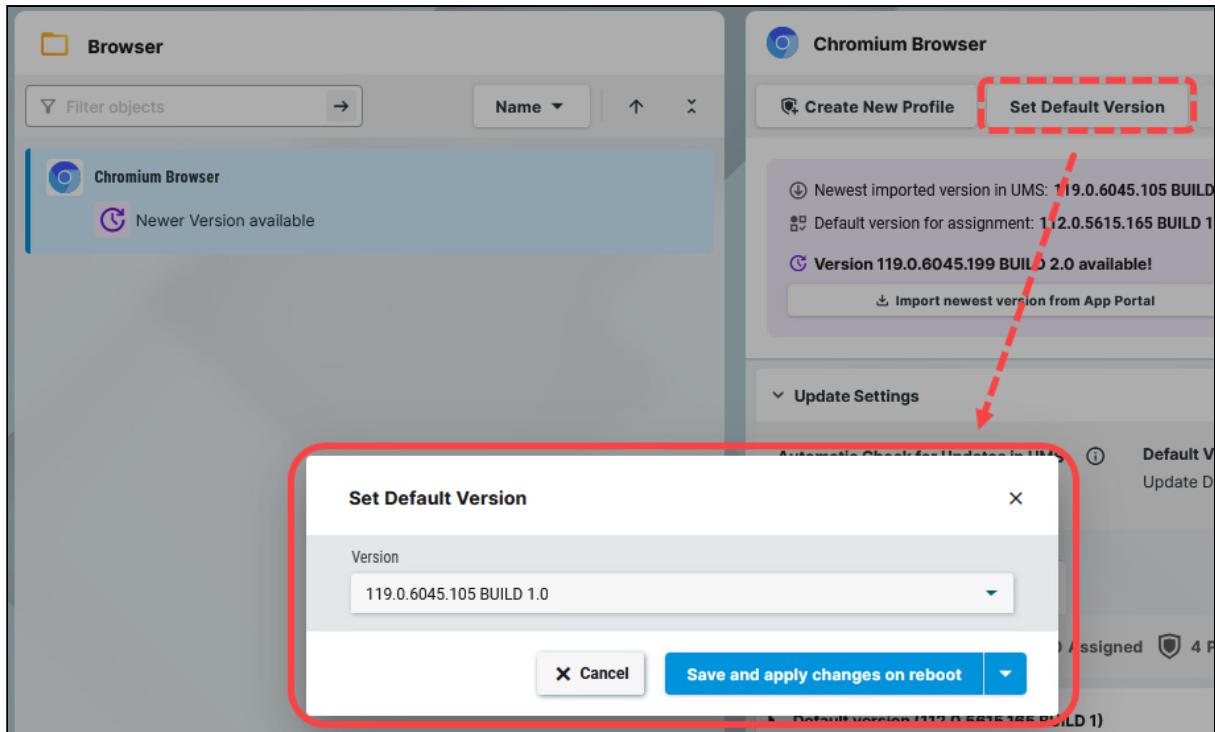
If you have imported several versions of an app, you can define which version will be a **Default Version**.

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 that 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 [Summary - Prioritization of IGEL UMS Profiles⁷⁹](#).
- Explicit app assignment via the **Assign object** dialog

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

i If you need to detach an app from the device, see [Detaching Apps from the IGEL OS Device in IGEL UMS Web App⁸⁰](#).

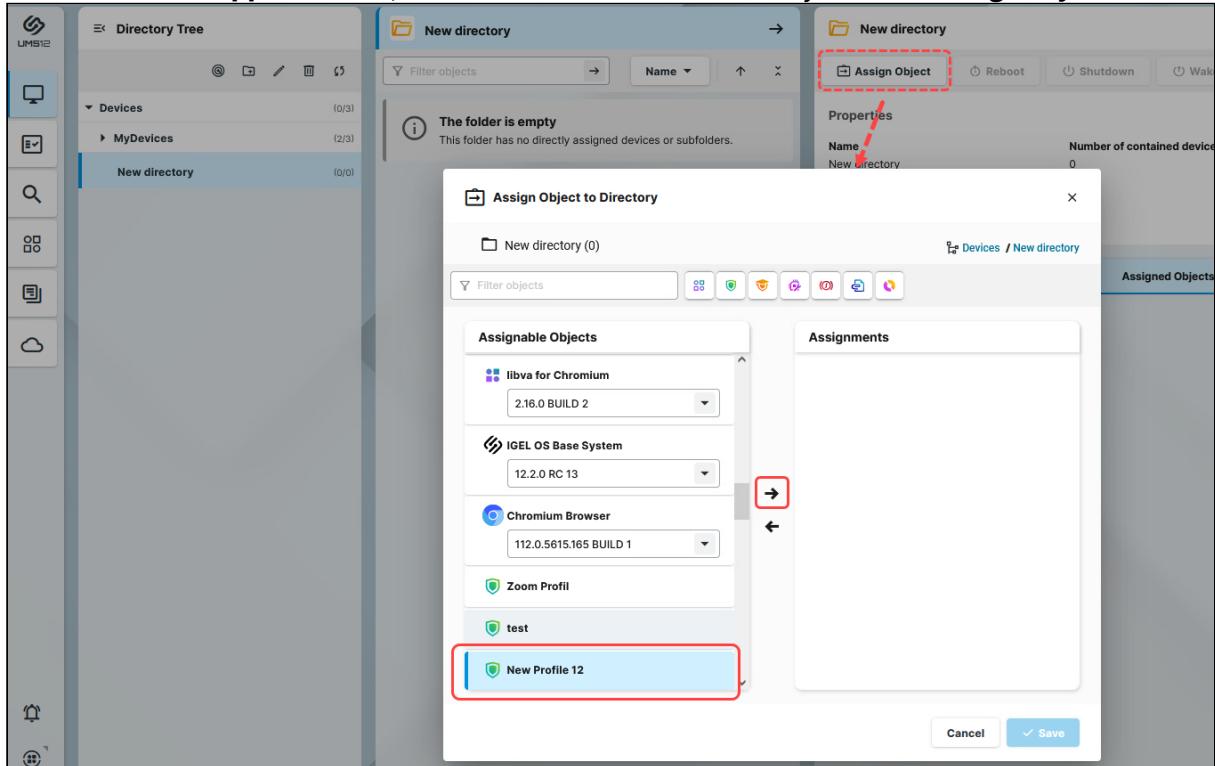
79. <https://kb.igel.com/en/universal-management-suite/current/summary-prioritization-of-igel-ums-profiles>

80. <https://kb.igel.com/en/universal-management-suite/current/detaching-apps-from-the-igel-os-device-in-igel-ums>

Implicit App Assignment via Profiles

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

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



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

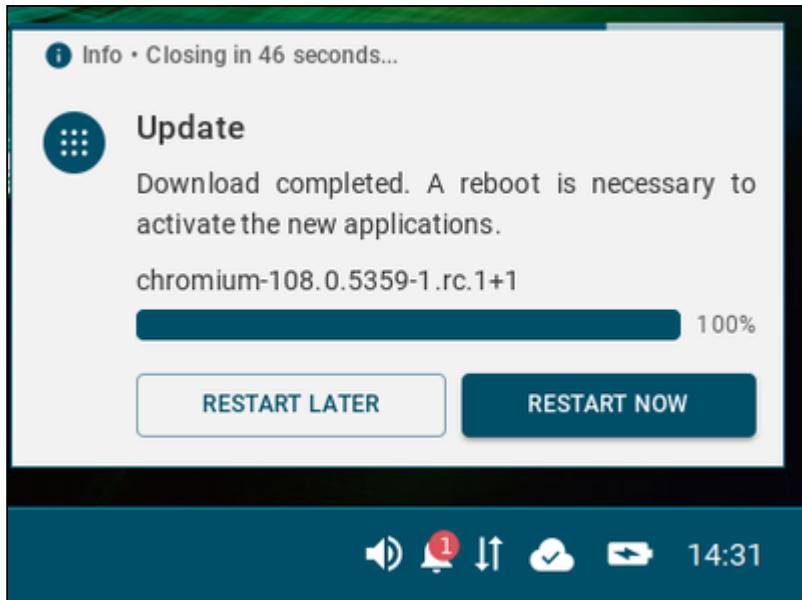
- Save the changes.

- 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; see [How to Configure the Background App Update in the IGEL UMS Web App⁸¹](#).

⁸¹. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the->



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

Assigned Object
Chromium Browser

To check the installed apps, go to **Devices > [name of the device] > Installed Apps**; see [Checking Installed Apps via the IGEL UMS Web App⁸²](#).

82. <https://kb.igel.com/en/universal-management-suite/current/checking-installed-apps-via-the-igel-ums-web-app>

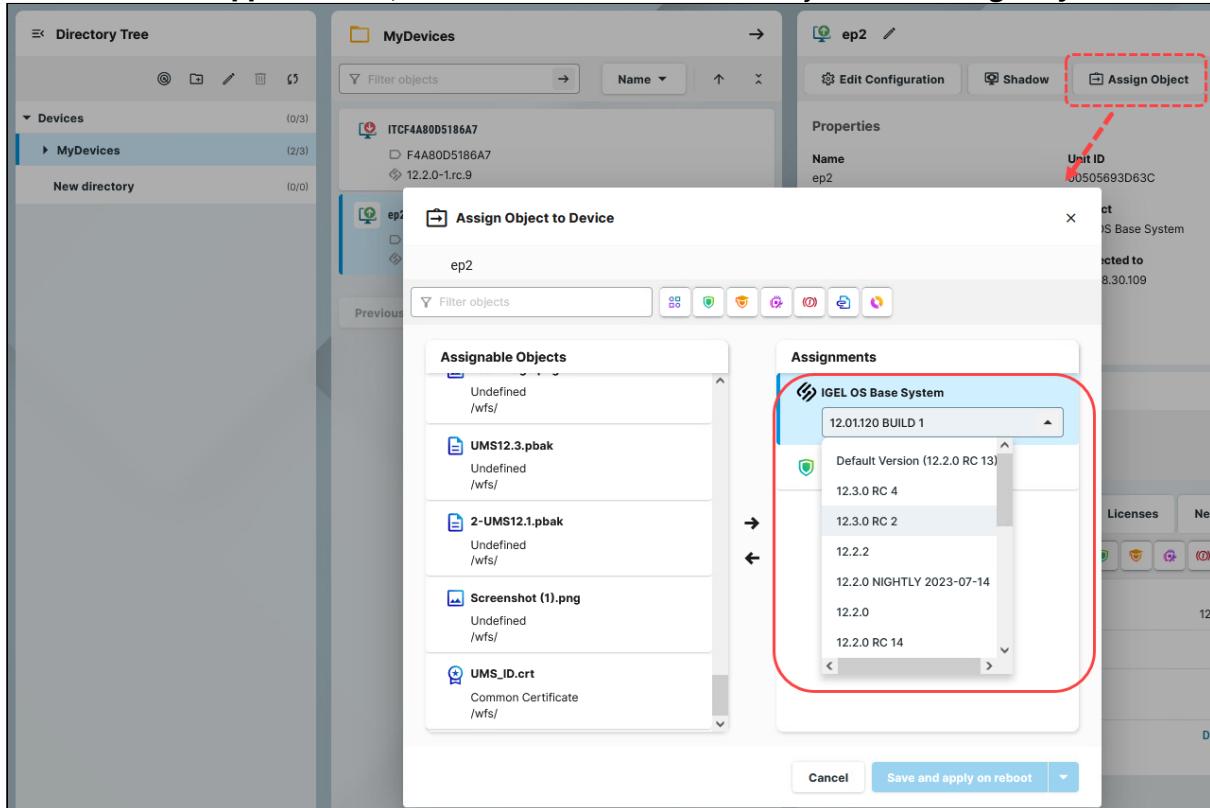
Explicit App Assignment

- 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 that is closer to the device in the directory tree will have the priority and will be installed on the device, see [Detaching Apps from the IGEL OS Device in IGEL UMS Web App⁸³](#).

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

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



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

83. <https://kb.igel.com/en/universal-management-suite/current/detaching-apps-from-the-igel-os-device-in-igel-ums>

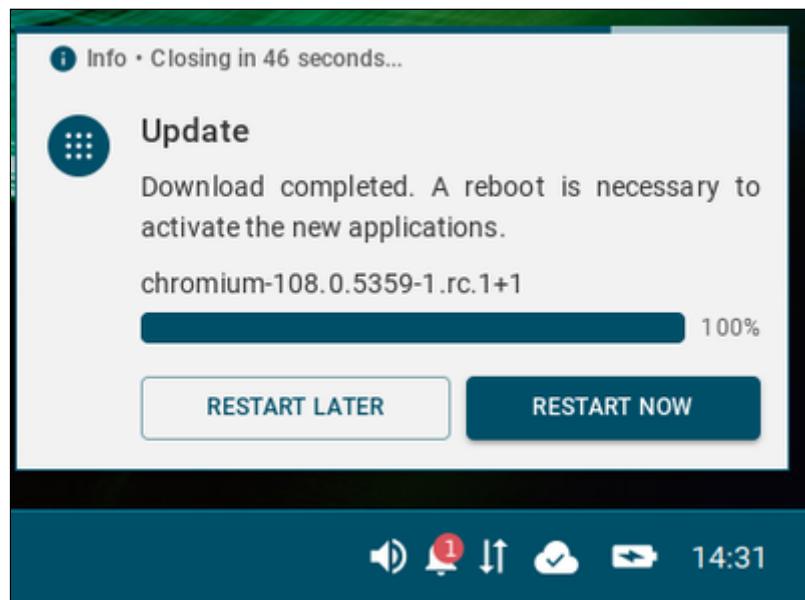
- i** If no version is specified for an app during the assignment, the default version will be used. It is possible to select the version for an app in the Assign Object dialog either under **Assignable Objects** or under **Assignments**.

3. Save the changes.

4. Decide when the changes should become effective.

The app will be downloaded by the device.

By default, apps / app versions assigned to the device will be automatically activated at the next reboot. The user will receive a corresponding notification. If the background app update has been activated, an **Update** command must be sent, instead; see [How to Configure the Background App Update in the IGEL UMS Web App⁸⁴](#).



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 App⁸⁵](#).

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 App⁸⁶](#).

84. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the->

85. <https://kb.igel.com/en/universal-management-suite/current/checking-installed-apps-via-the-igel-ums-web-app>

86. <https://kb.igel.com/en/universal-management-suite/current/remote-access-to-devices-via-shadowing-in-the-igel>

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.

- As of IGEL OS 12.7.1, there is a downgrade limit for IGEL OS Base System app, see [Downgrade Limit on IGEL OS 12.7.1 or Higher⁸⁷](#).

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 Apps⁸⁸](#).
2. Checking if the default update settings under **UMS Web App > Apps > [name of the app] > Edit Update Settings** suit your needs. See [How to Configure Update Settings for Apps in the IGEL UMS Web App⁸⁹](#).
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 App⁹⁰](#)).
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 UMS⁹¹](#).
See also the instructions below.

Preconditions

- You use the default version 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] > Edit 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 168).

87. <https://kb.igel.com/en/igel-os-base-system/current/downgrade-limit-on-igel-os-12-7-1-or-higher>

88. <https://kb.igel.com/en/universal-management-suite/current/configuring-global-settings-for-the-update-of-igel>

89. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-update-settings-for-apps-in-the-i>

90. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the->

91. <https://kb.igel.com/en/universal-management-suite/current/how-to-trigger-the-app-update-in-the-igel-ums>

- 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

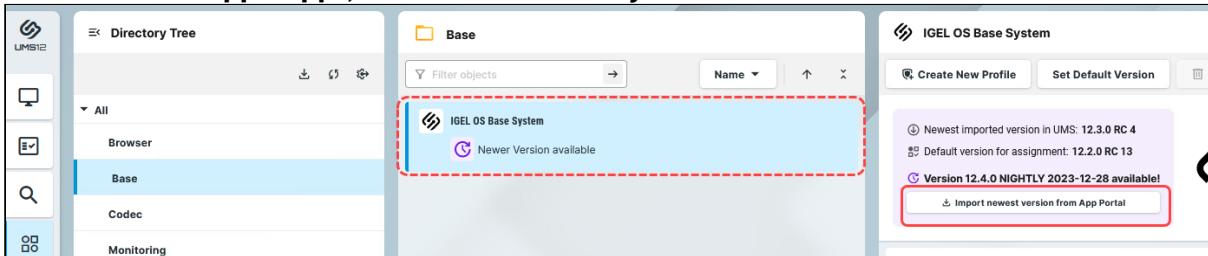
The procedure described below applies to the update of the IGEL OS Base System app.

i This procedure is also relevant for any explicitly assigned app.

Preparing the Update

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

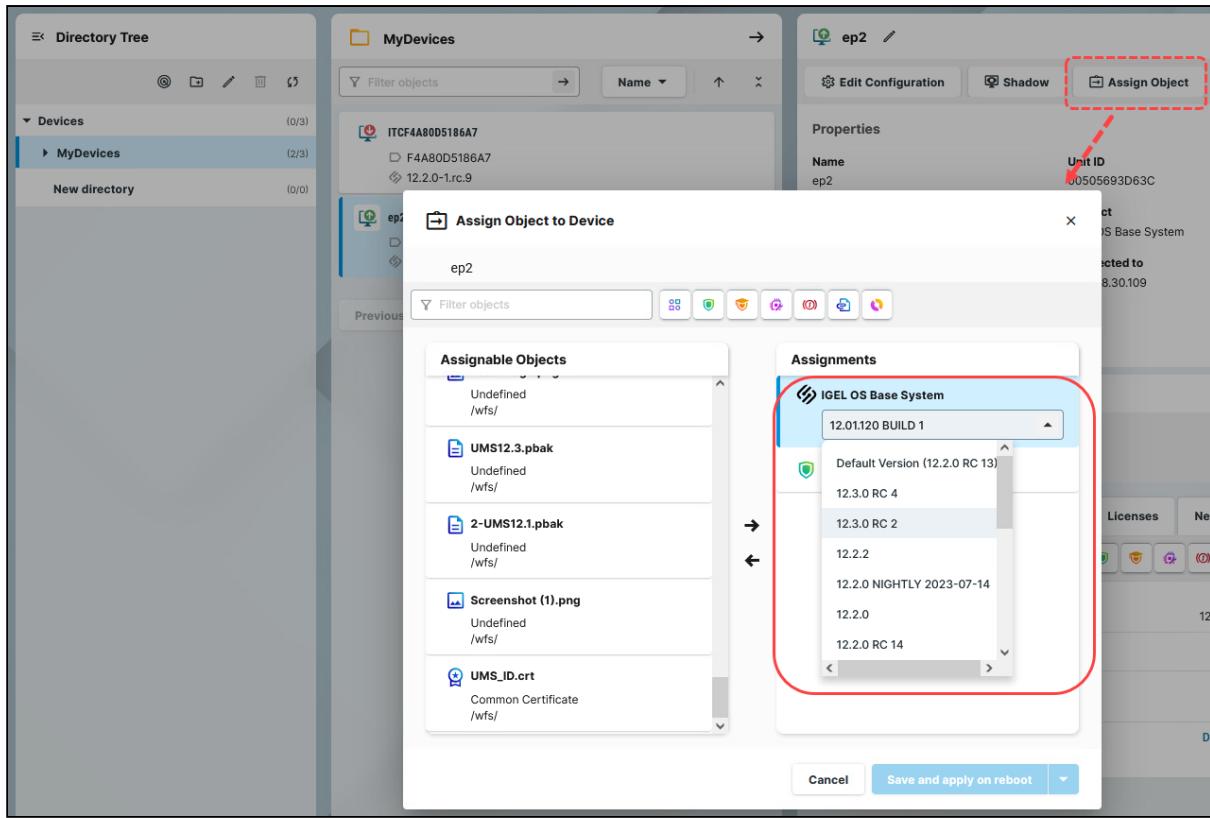
1. In the **UMS Web App > Apps**, select **IGEL OS Base System**.



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

Testing the Update

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



2. In the **Assign Object** dialog, select **IGEL OS Base System** and the required version. It is possible to select the version for an app either under **Assignable Objects** or under **Assignments**.
3. Decide when the changes should become effective, and save accordingly.
The app version will be downloaded by the device.
By default, apps / app versions assigned to the device will be automatically activated at the next reboot. If you have configured the background app update, an **Update** command must be sent, instead; see [How to Configure the Background App Update in the IGEL UMS Web App](#)⁹².
4. Under **Devices > [name of the device] > Installed Apps**, check the app, its version, and state; see [Checking Installed Apps via the IGEL UMS Web App](#)⁹³.

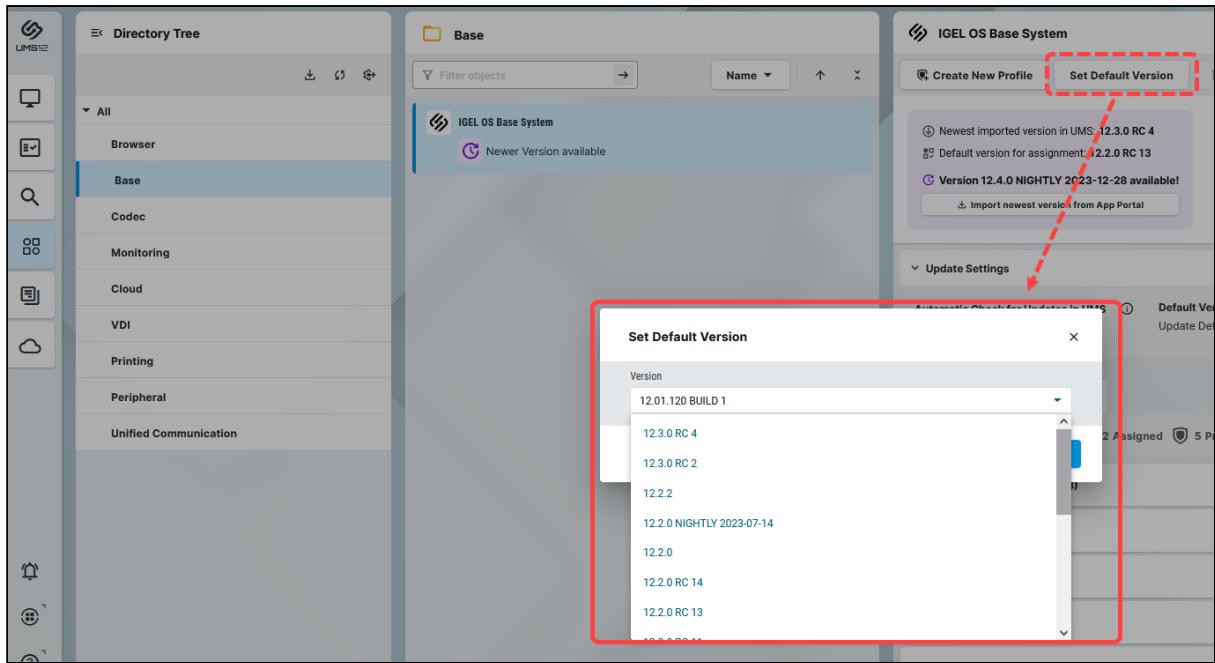
When the update test has been successful, you can update IGEL OS Base System on all the required devices.

Triggering the Mass Update

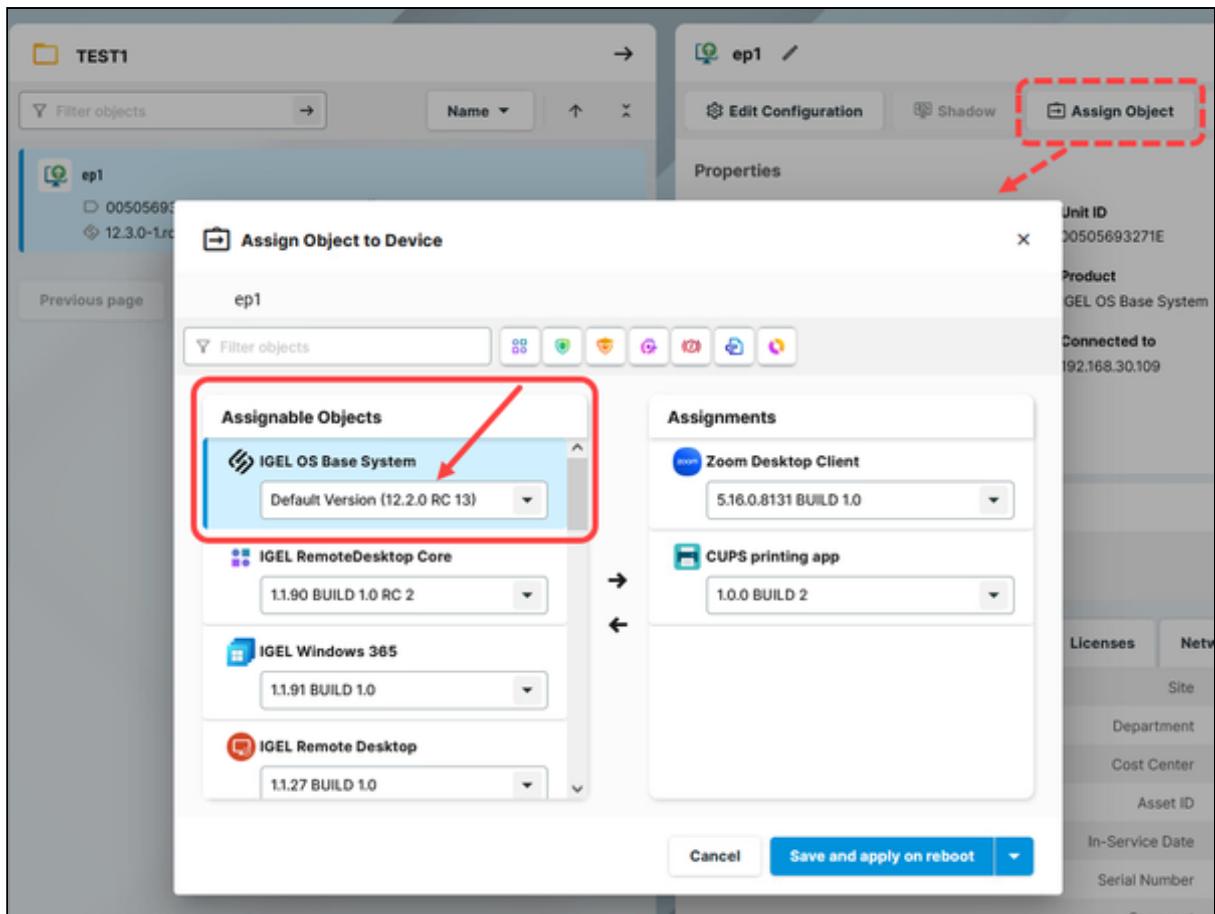
1. In the **UMS Web App > Apps**, select **IGEL OS Base System** and click **Set Default Version**.

92. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the-igel-ums-web-app>

93. <https://kb.igel.com/en/universal-management-suite/current/checking-installed-apps-via-the-igel-ums-web-app>



2. Select the required version.
3. Select when the changes should take effect and save accordingly.
4. If the **IGEL OS Base System** app has not yet been assigned to the devices: Go to **UMS Web App > Devices > [name of the device / device directory]** and click **Assign object** to assign the app.
5. Verify that **Default Version** is selected in the version picker.
6. Assign the app.
7. Decide when the changes should become effective and save accordingly.



- If the changes should take effect on reboot, you can create a scheduled job for reboot and/or wakeup and assign it to the devices / device directory or a view (created in the **UMS Console > Views > [context menu] > New View > Installed Apps criterion**). For more information on jobs, see [Jobs - Sending Automated Commands to Devices in the IGEL UMS](#)⁹⁴.

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 215).

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](#)⁹⁵.

- 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 the IGEL OS Base System](#)⁹⁶.

94. <https://kb.igel.com/en/universal-management-suite/current/jobs-sending-automated-commands-to-devices-in-the->

95. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the->

96. <https://kb.igel.com/en/universal-management-suite/current/multistage-update-of-the-igel-os-base-system>

9. 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](#)⁹⁷.

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 [IGEL UMS 12: Basic Configuration](#)⁹⁸, "Assignment of Apps and Profiles."

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 **Edit 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.

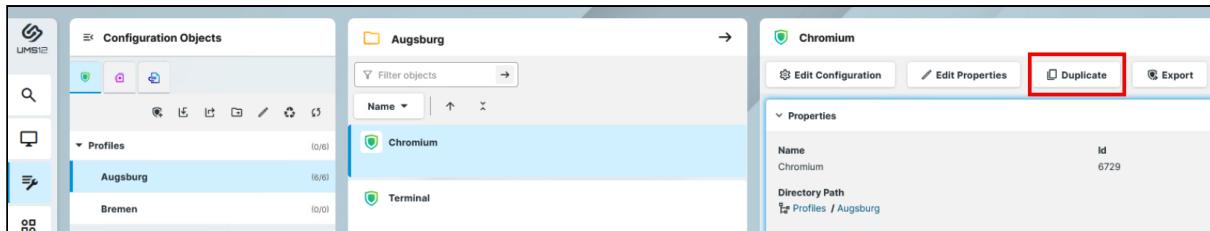
The screenshot shows the UMS Web App interface. On the left, the Directory Tree lists categories like All, Browser, Base, Codec, Monitoring, Cloud, VDI, Printing, Peripheral, and Unified Communication. The 'Browser' category is selected. In the center, the 'Browser' app details page is shown. It lists 'Chromium Browser' with a note 'Newer Version available'. On the right, a detailed view for 'Chromium Browser' shows the 'Update Settings' section. Under 'Automatic Check for Updates in UMS', there is a button labeled 'Import newest version from App Portal' which is highlighted with a red box. Below this, the 'Versions' tab is selected, showing 4 Versions, 0 Installed, 0 Assigned, and 3 Profiles.

Testing the Update

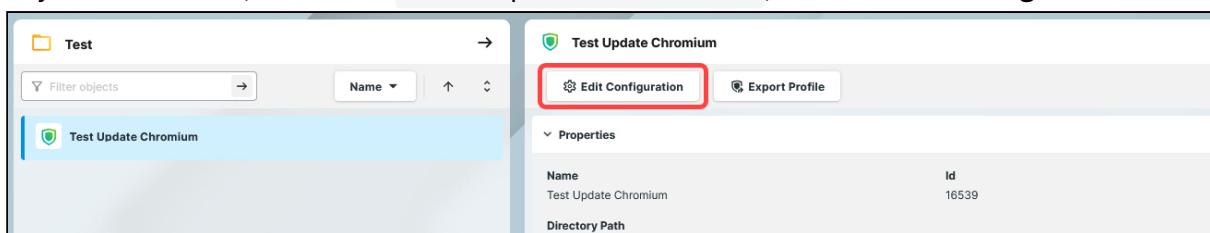
1. In the **UMS Web App > Configuration > Profiles**, select the "productive" profile, e.g. **Chromium**, and click **Duplicate** to copy it. The created test profile will have the same settings as the original profile (incl. the setting **Default Version** for the app(s) in the **App Selector**).

97. <https://kb.igel.com/en/universal-management-suite/current/checking-installed-apps-via-the-igel-ums-web-app>

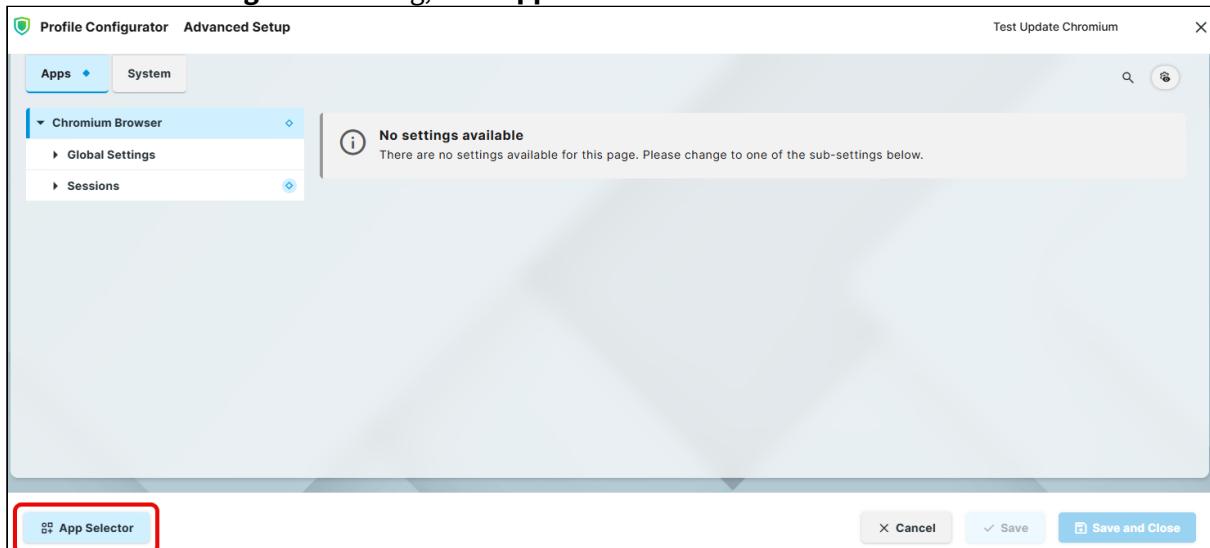
98. <https://kb.igel.com/en/how-to-start-with-igel/current/igel-ums-12-basic-configuration>



2. Click **Edit Properties** to rename the created test profile, e.g. `Test Update Chromium`.
3. In the **UMS Web App > Devices**, select your test device(s) and assign the created test profile `Test Update Chromium`. For more information on the assignment, see [IGEL UMS 12: Basic Configuration](#)⁹⁹, "Implicit App Assignment via Profiles". As soon as your test devices have the app(s) of the same version as on the productive devices, proceed as follows.
4. In the **UMS Web App > Configuration > Profiles**, select the test profile via which apps are assigned to your test devices, in our case `Test Update Chromium`, and click **Edit Configuration**.

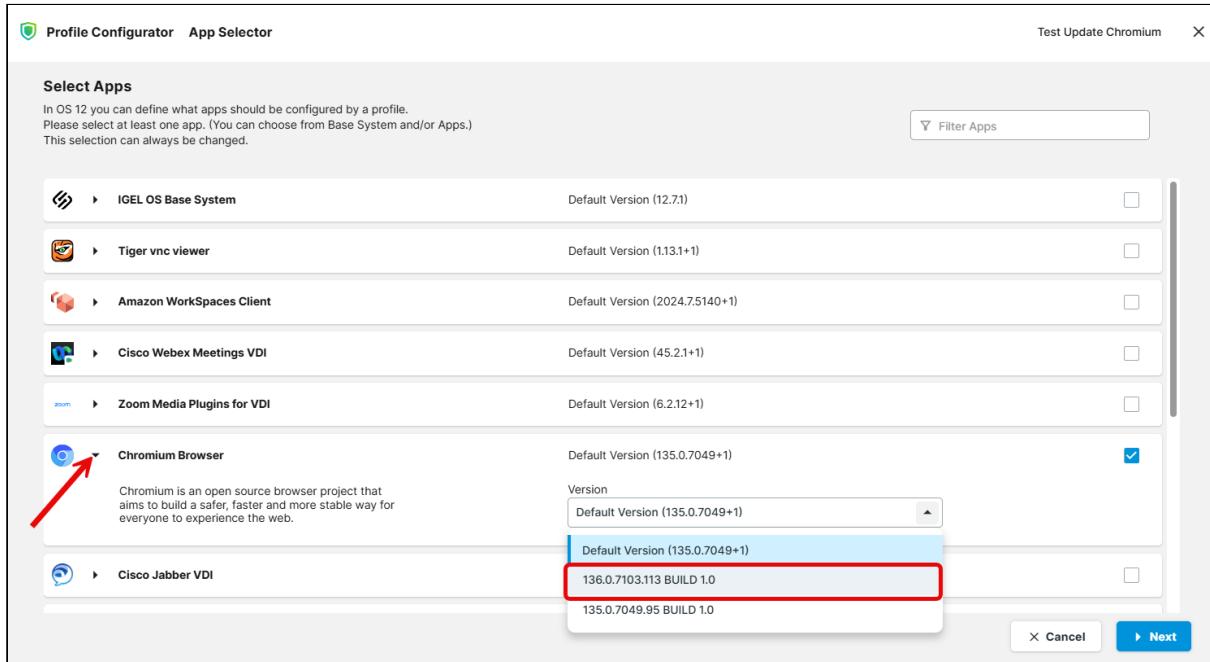


5. In the **Profile Configurator** dialog, click **App Selector**.



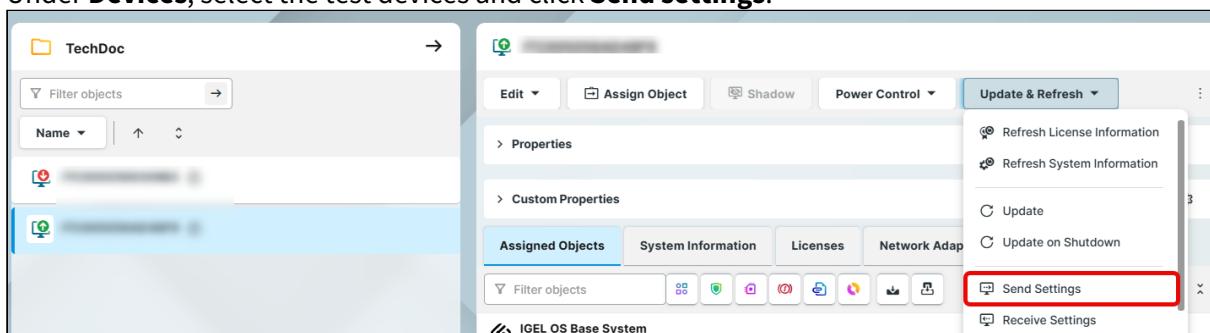
99. <https://kb.igel.com/en/how-to-start-with-igel/current/igel-ums-12-basic-configuration>

6. Click and select the app version you want to update to.



7. Save the changes.

8. 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 App¹⁰⁰](#).

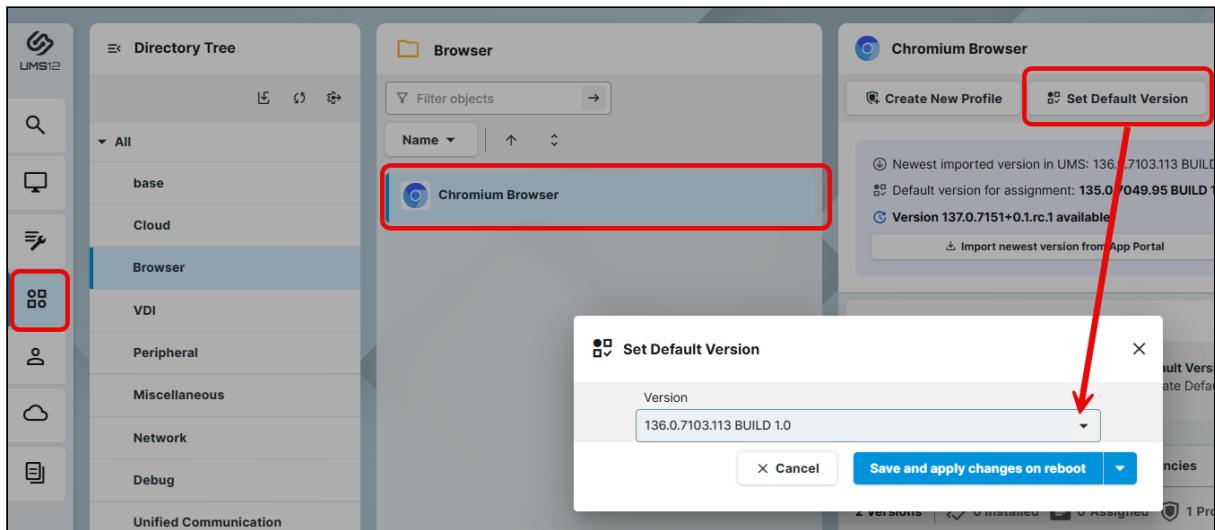
9. Under **Devices > [name of the device] > Installed Apps**, check the app, its version, and state; see [Checking Installed Apps via the IGEL UMS Web App¹⁰¹](#).

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

100. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the->
101. <https://kb.igel.com/en/universal-management-suite/current/checking-installed-apps-via-the-igel-ums-web-app>¹⁰¹

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

- ✓ If the changes should take effect on reboot, you can create a scheduled job for reboot and/or wakeup and assign it to the devices / device directory or a view (created in the **UMS Console > Views > [context menu] > New View > Installed Apps criterion**). For more information on jobs, see [Jobs - Sending Automated Commands to Devices in the IGEL UMS](#)¹⁰².

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 215).

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](#)¹⁰³.

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](#)¹⁰⁴.

102. <https://kb.igel.com/en/universal-management-suite/current/jobs-sending-automated-commands-to-devices-in-the->

103. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the->

104. <https://kb.igel.com/en/universal-management-suite/current/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 [Devices Supported by IGEL OS 12¹⁰⁵](#).

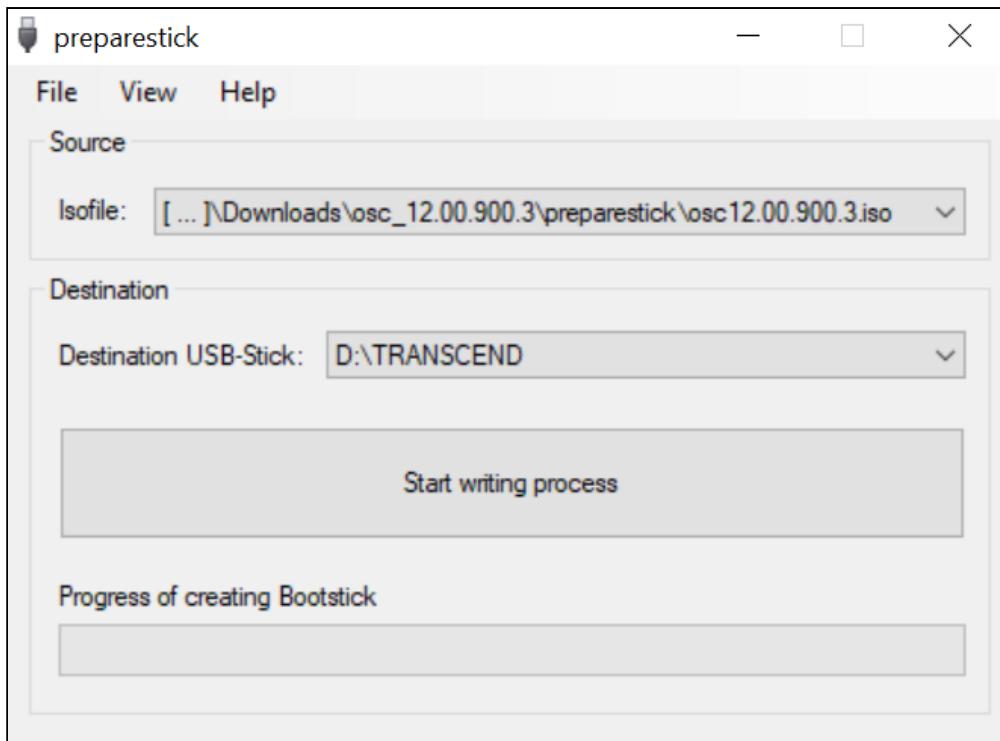
Create USB Installation Medium

Windows

1. Download the ZIP archive for OS Creator from the [IGEL download server¹⁰⁶](#):
 - 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.

105. <https://kb.igel.com/en/hardware/current/devices-supported-by-igel-os-12-1>

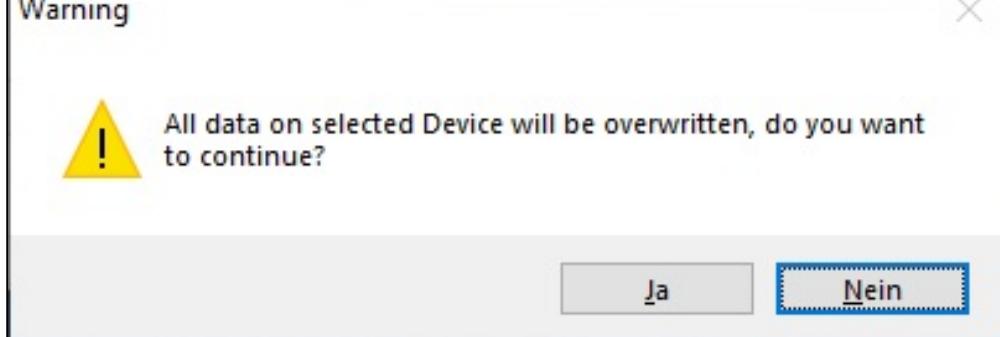
106. <https://www.igel.com/software-downloads/igel-os-12-secure-endpoint/>



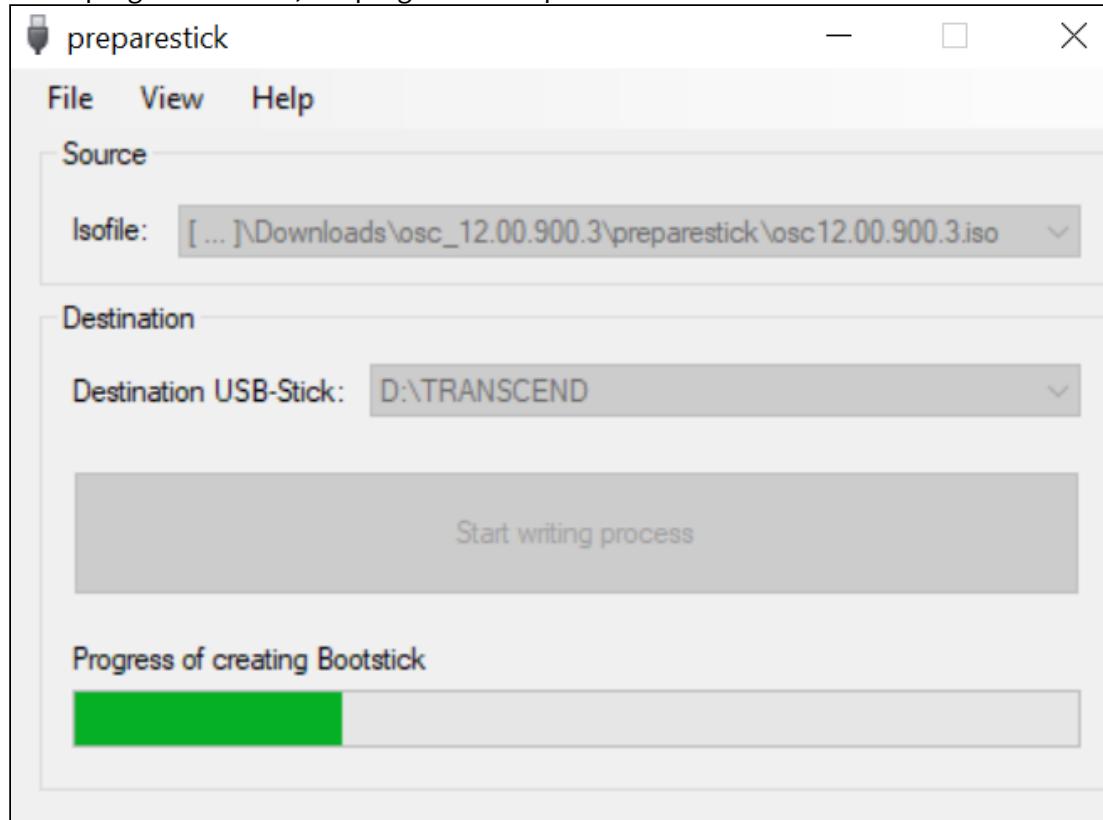
The dropdown menu **Isofile** shows the ISO files contained in the unzipped directory.

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**.

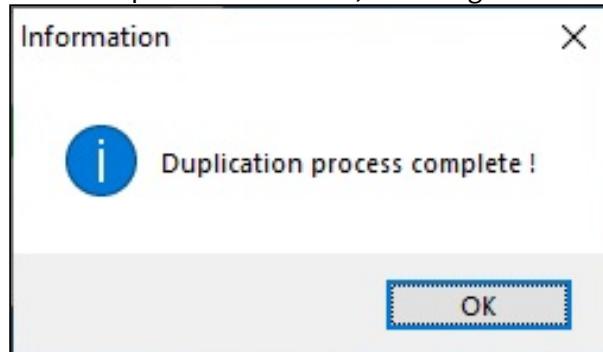
8. Confirm the following dialog:



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](#)¹⁰⁷:
 - 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`.

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.

107. <https://www.igel.com/software-downloads/igel-os-12-secure-endpoint/>

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.

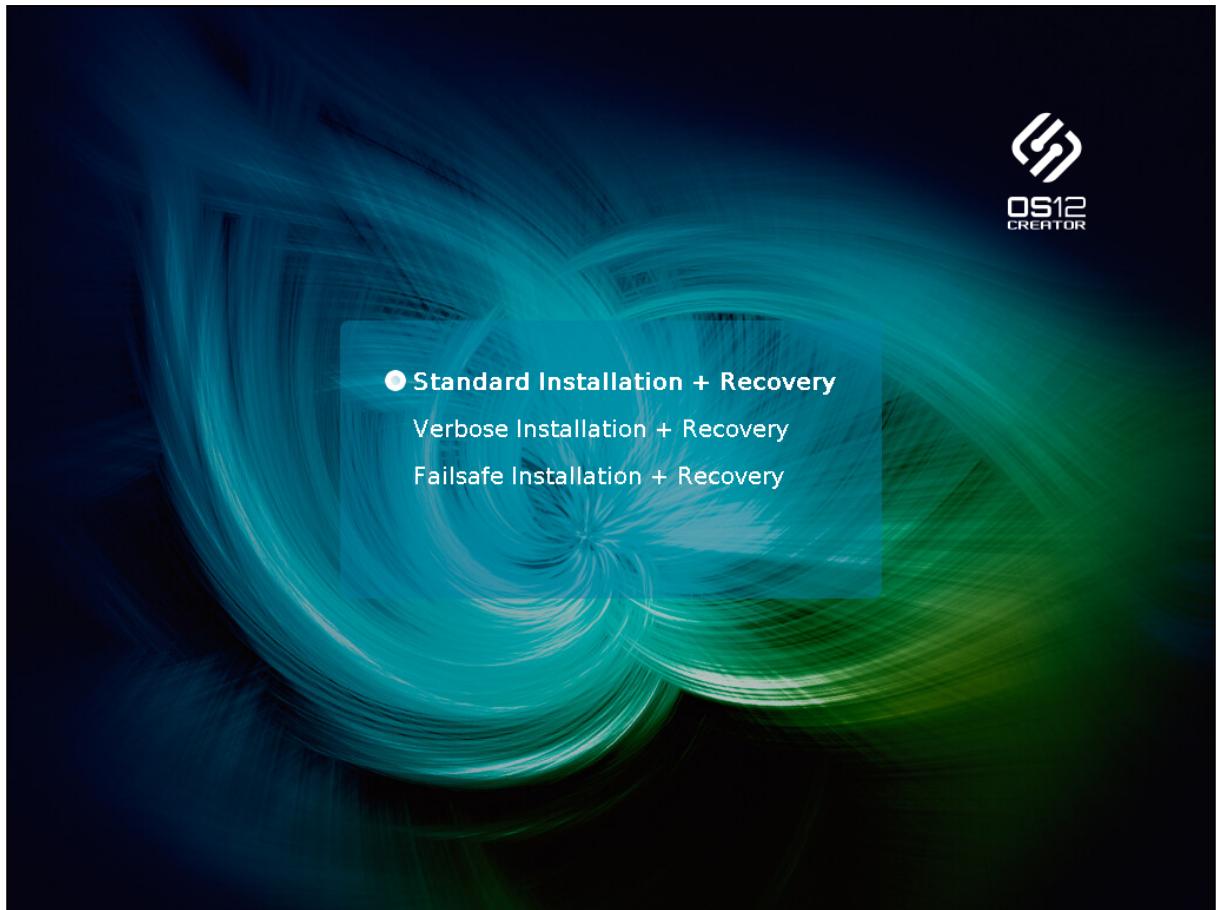
Installation Procedure

- ✖ 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 [Installing the Base System via IGEL OS Creator \(OSC\)](#)¹⁰⁸.

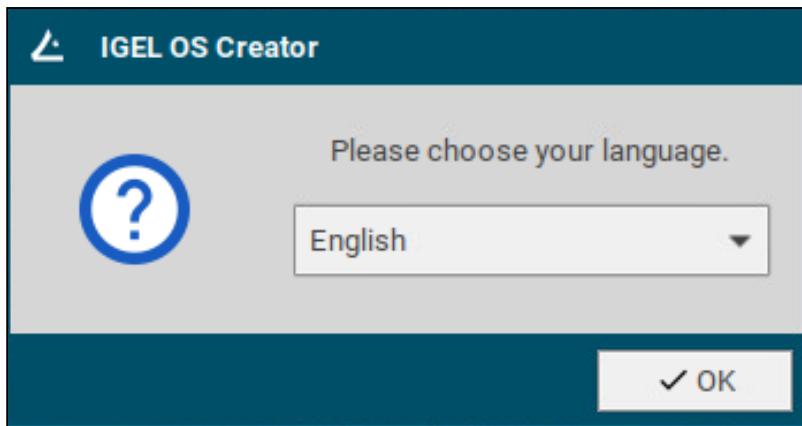
2. Select one of the following options from the boot menu:

108. <https://kb.igel.com/en/how-to-start-with-igel/current/installing-the-base-system-via-igel-os-creator-osc>

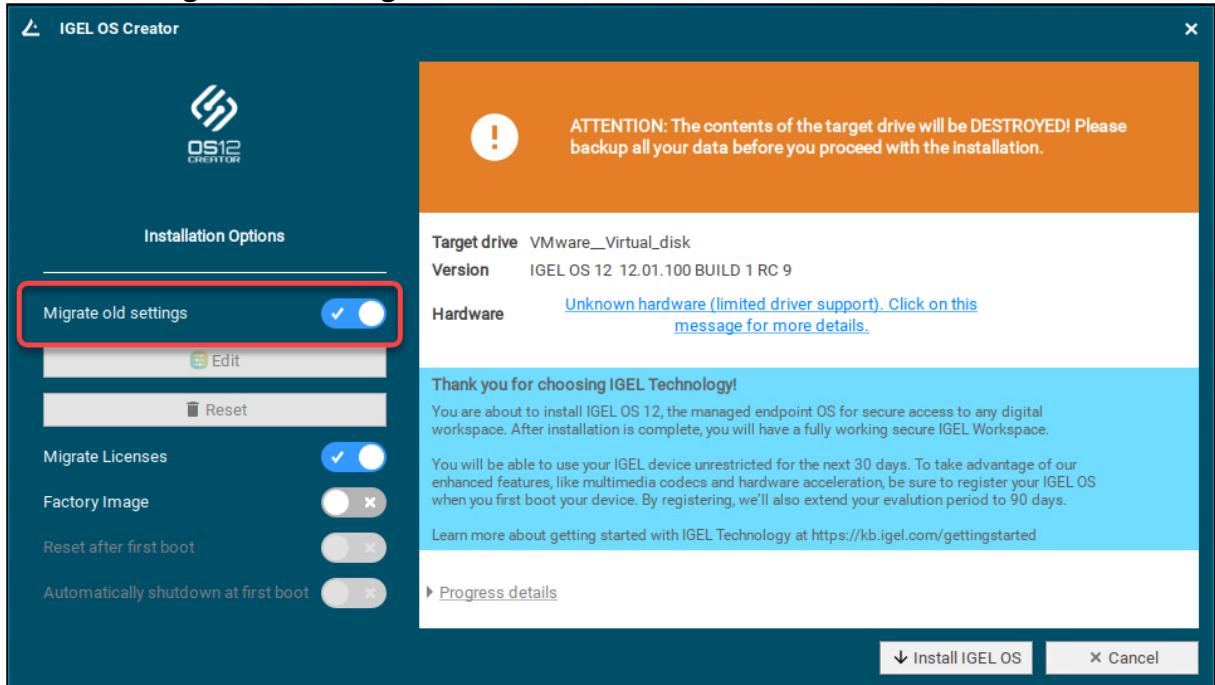


- **Standard Installation + Recovery:** Boots the system with just a few messages from the USB memory stick and launches the installation program. (Default)
- **Verbose Installation + Recovery:** Boots the system from the USB memory stick and shows the Linux boot messages in the process.
- **Failsafe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



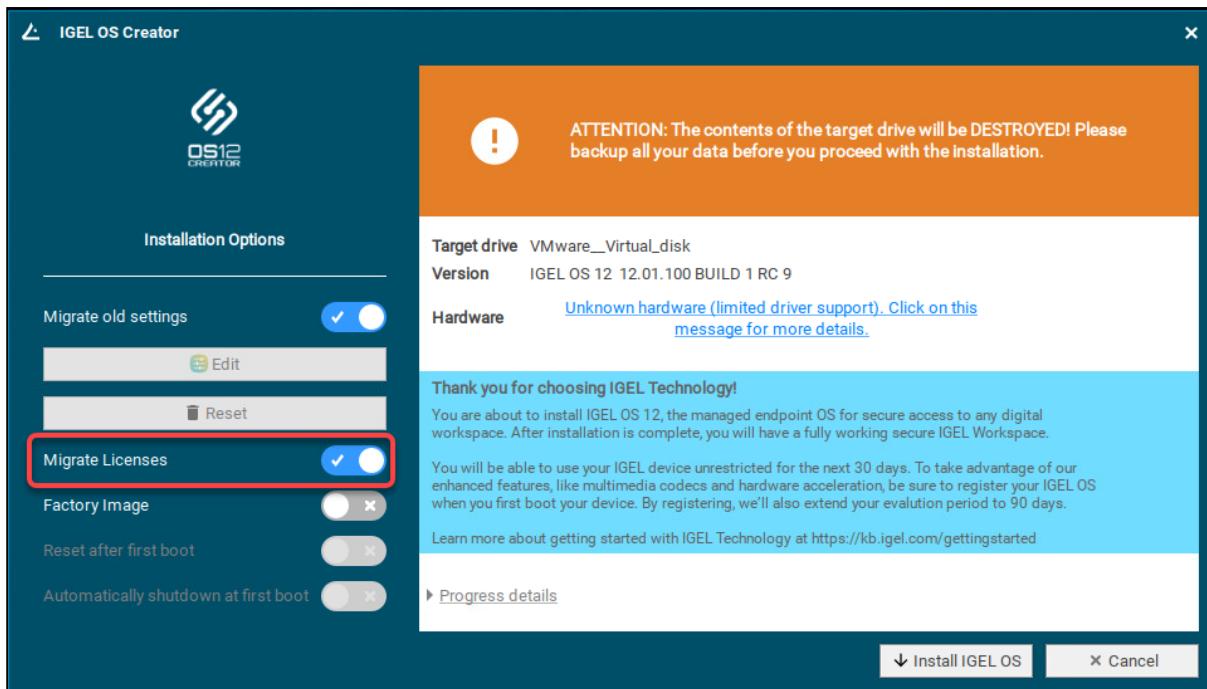
4. If IGEL OS 12 has been running on the device before and you want to preserve the device's settings, ensure that **Migrate old settings** is enabled.



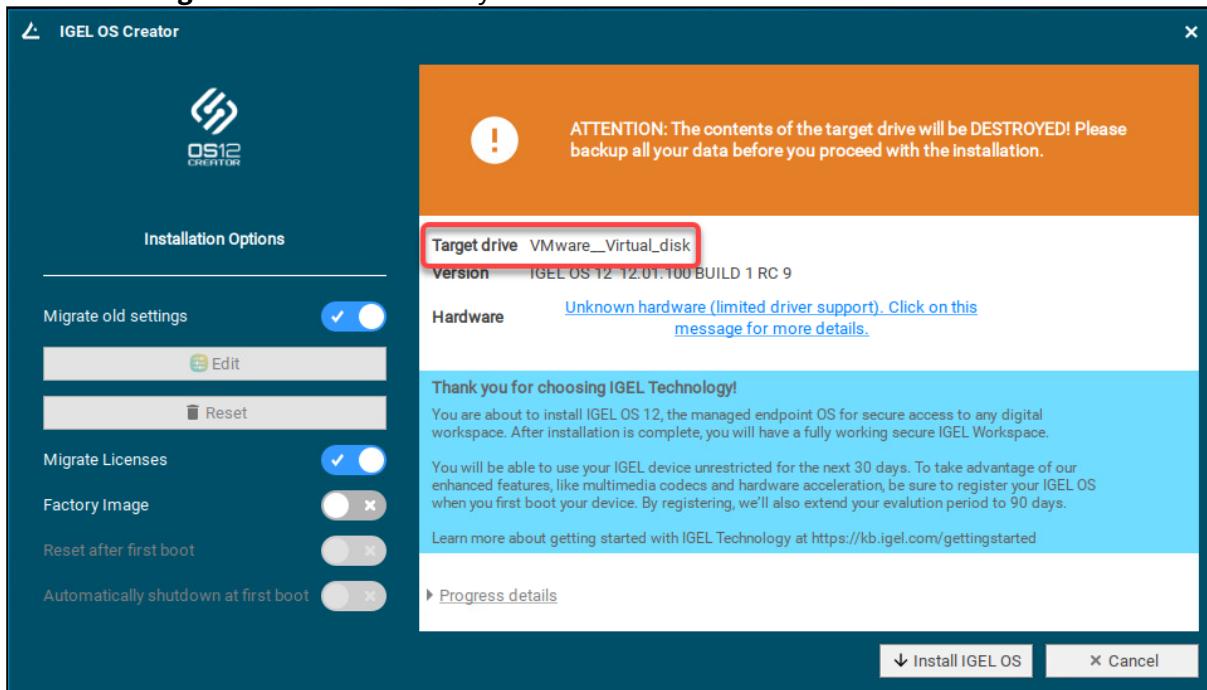
5. If one of the following is the case, make sure that **Migrate licenses** is enabled:

- 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

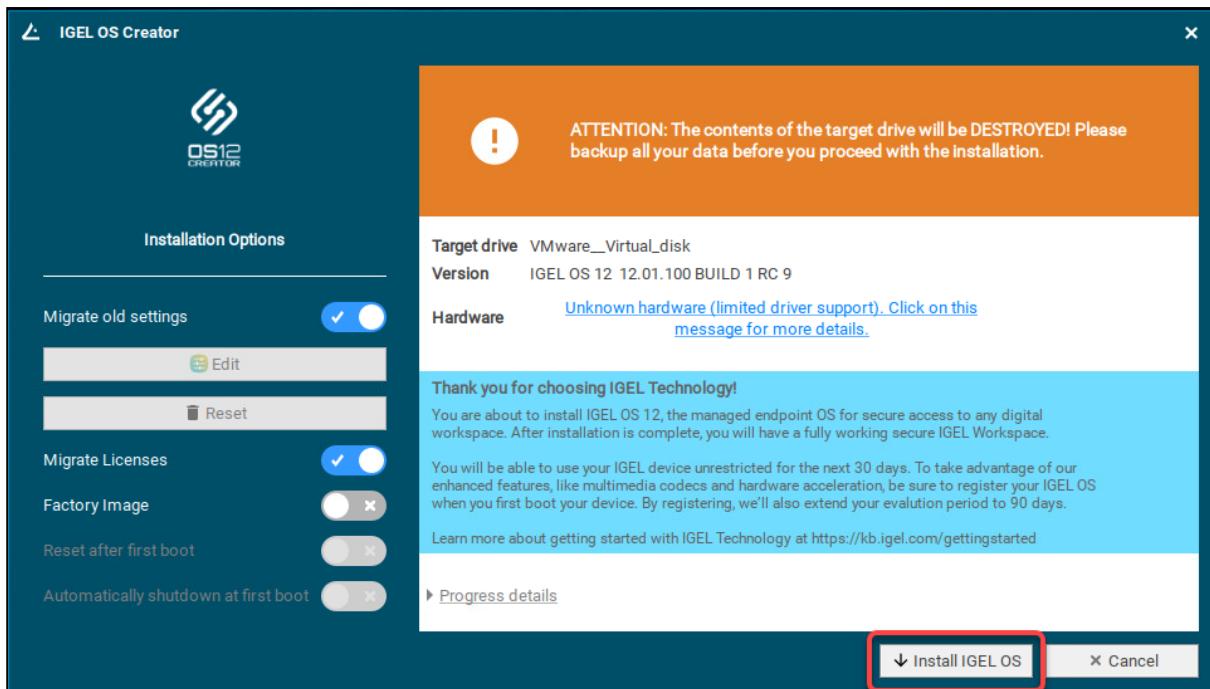
Installing the Base System via IGEL OS Creator (OSC)



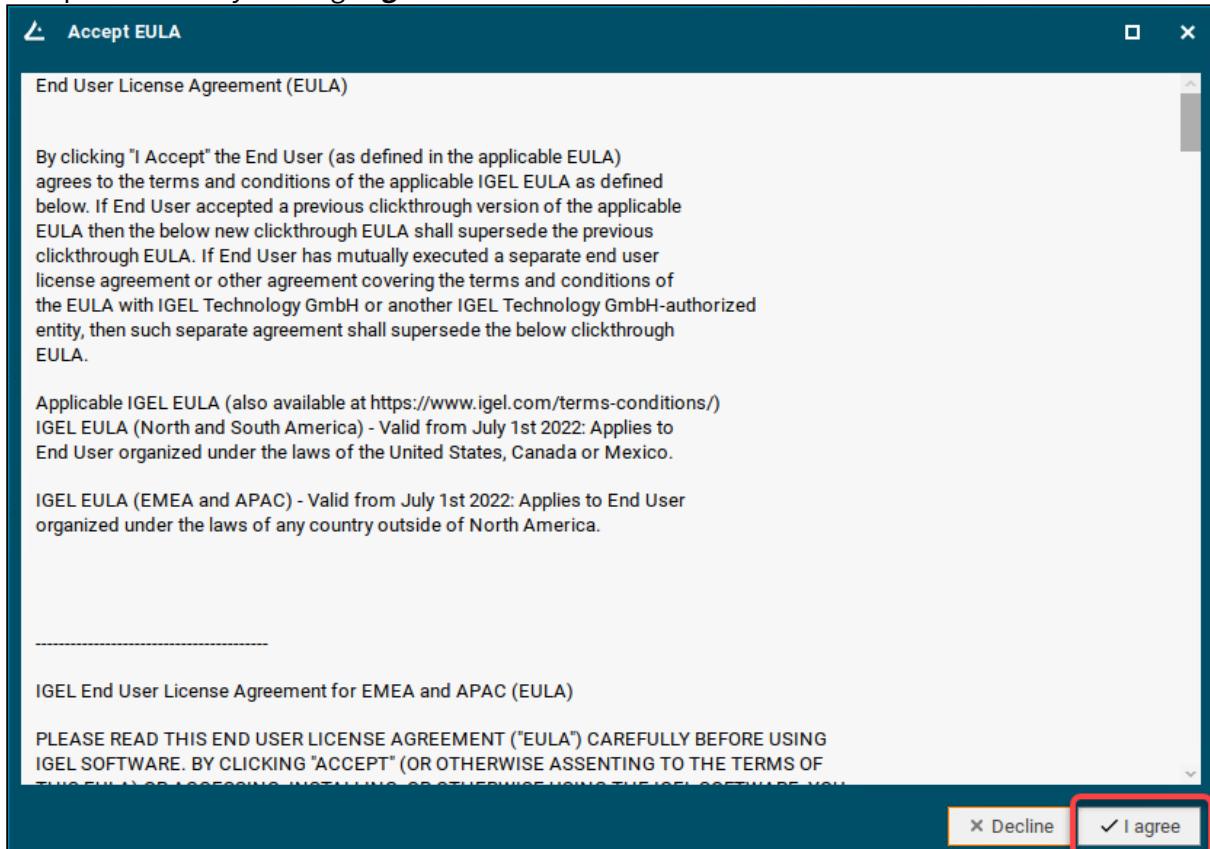
6. Check the **Target drive** to ensure the system is installed on the desired drive.



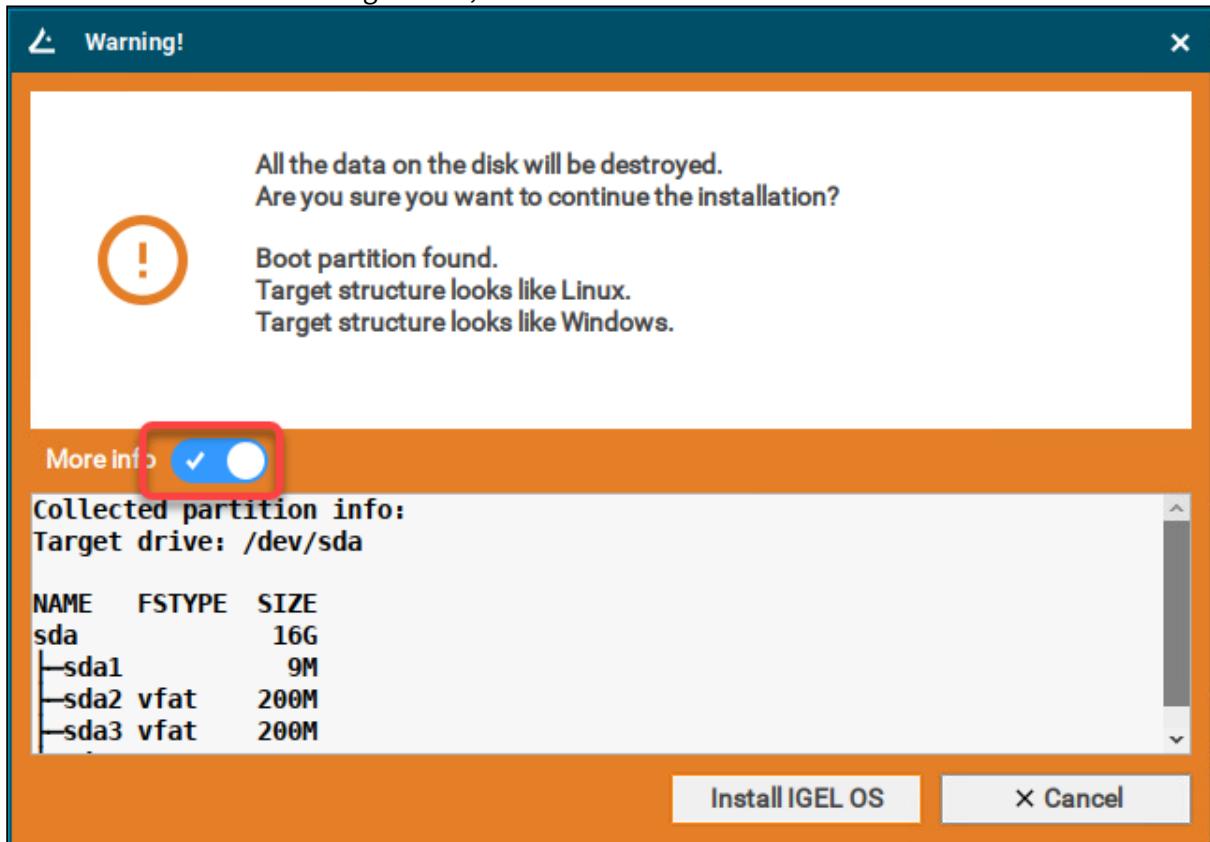
7. Click **Install IGEL OS**.



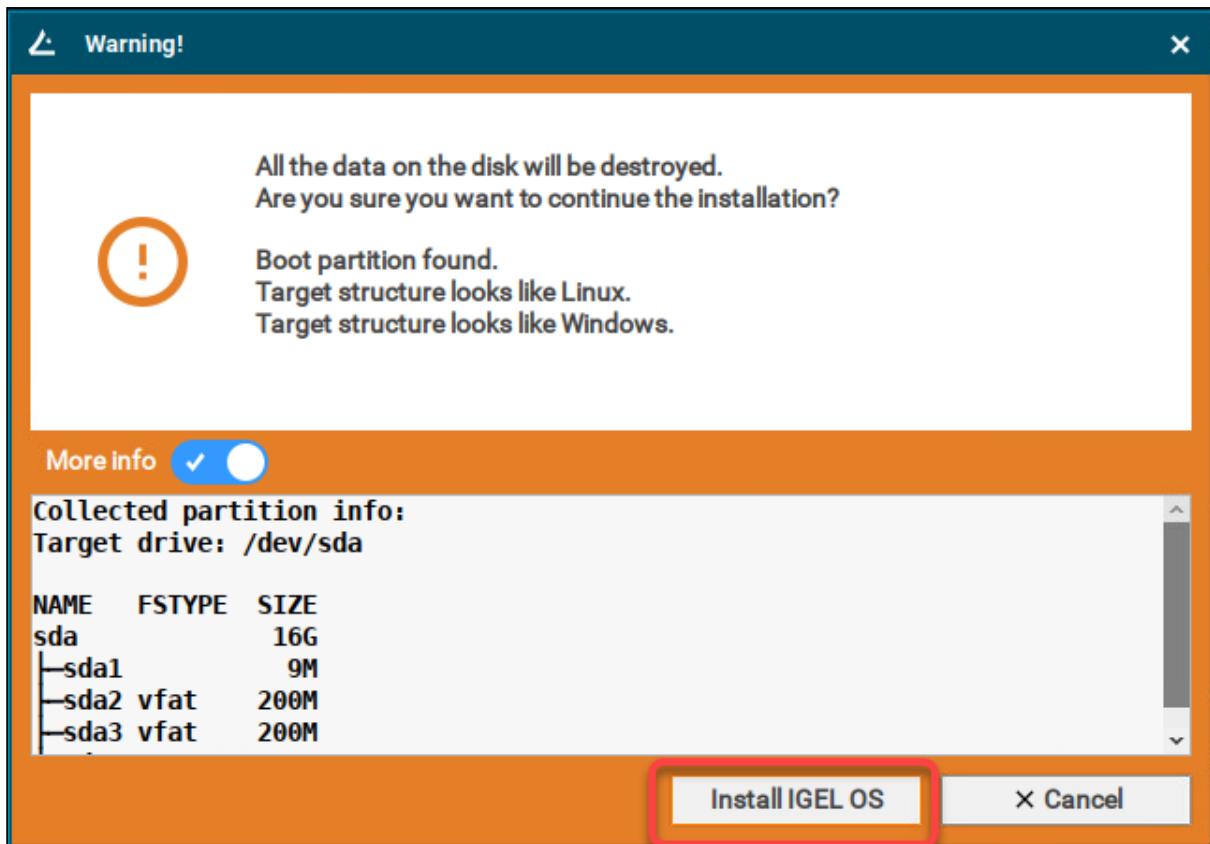
8. Accept the EULA by clicking I agree.



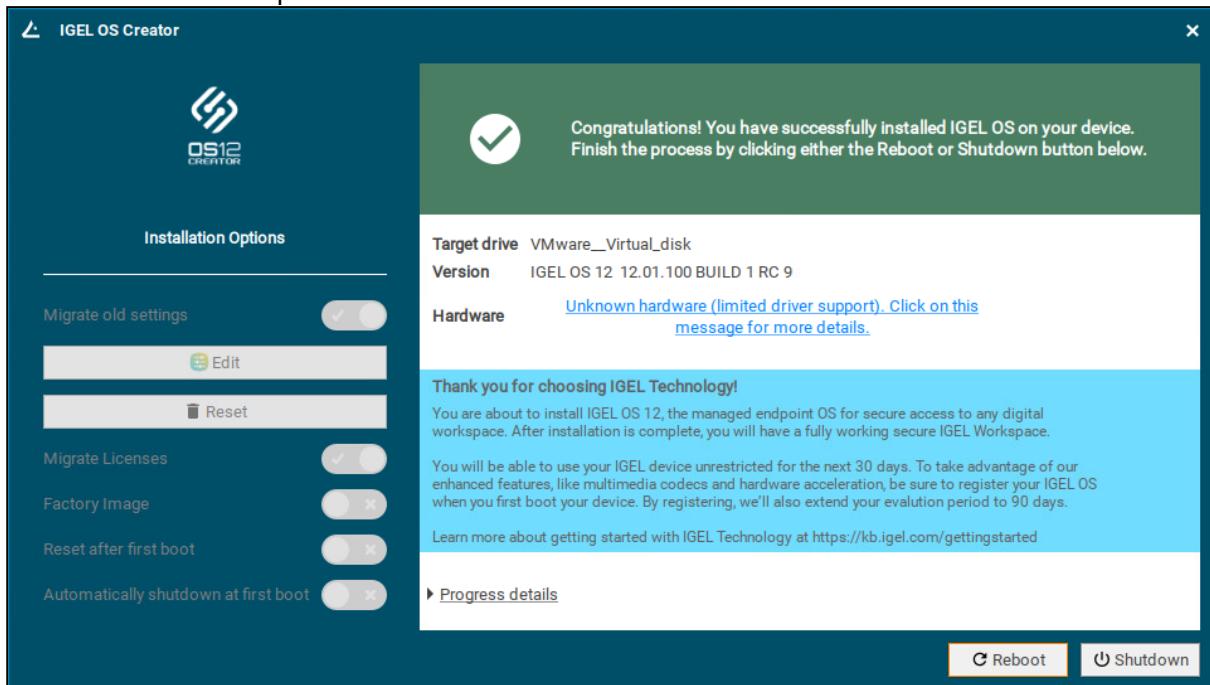
9. To view the details for the target drive, click **More Info**.



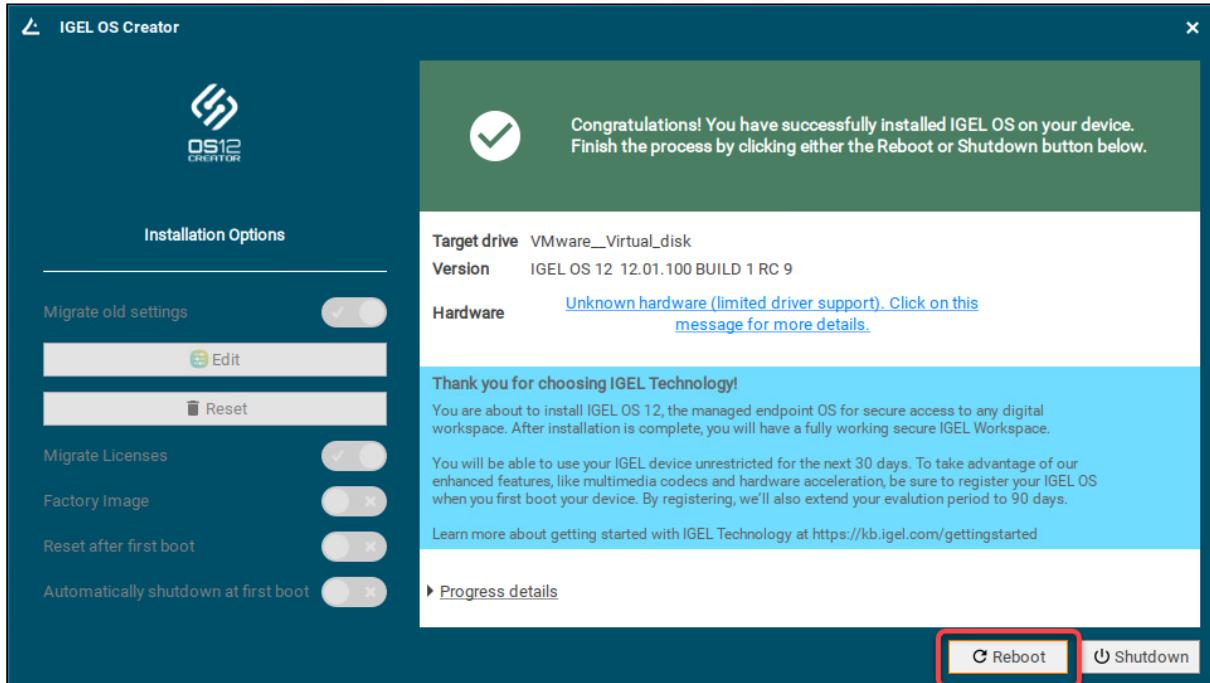
10. Click **Install IGEL OS**.



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

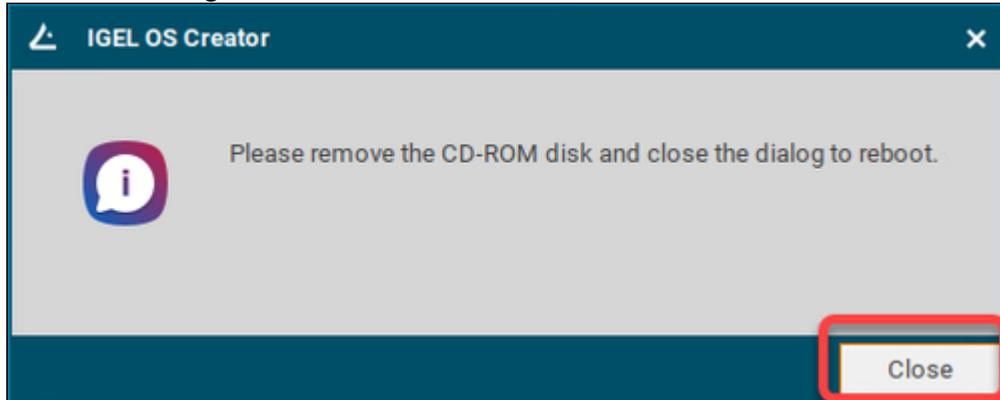


11. Click **Reboot**.



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](#).

Licensing

To work with your IGEL environment, your IGEL OS devices and your IGEL Universal Management Suite (UMS) must have valid licenses from your IGEL subscription. For details, see [IGEL Subscription](#)¹⁰⁹.

You can deploy your licenses via Automatic License Deployment (ALD), which is the preferred method, or manually. For details, see [Setting up Automatic License Deployment \(ALD\)](#)¹¹⁰. For a list of all deployment methods, see [Deploying Licenses](#)¹¹¹.



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 171).

Starter Licenses and Evaluation Licenses

As long as no license has been deployed, your IGEL OS 12 devices will use a starter license that is valid for 30 days.

You can also request evaluation licenses (or demo licenses) for testing purposes with a limited license period. You can request the licenses both for the IGEL OS devices and for the IGEL UMS. For more information, see [Evaluation Licenses for IGEL OS 12 and IGEL UMS](#)¹¹².

For the effects of evaluation license expiration, see [IGEL Subscription - Entitlements and Effects of Expiration](#)¹¹³.

Licensing Your IGEL UMS

Starting from version 12.07.100, the IGEL UMS needs to have a license in place to provide access to UMS features. For instructions on how to license your UMS, see [How to License the IGEL UMS](#)¹¹⁴.

- The IGEL UMS can be installed without a technical license, providing access to features of the Essential UMS License out of the box.

Getting Your Device Licenses Ready for Deployment

1. Log in to the IGEL License Portal (ILP) at <https://activation.igel.com>¹¹⁵. If you do not have an ILP account yet, you must register with the ILP. For details, see [Registering on the IGEL License Portal \(ILP\)](#).

109. <https://kb.igel.com/en/igel-subscription-and-more/current/igel-subscription>

110. <https://kb.igel.com/en/igel-subscription-and-more/current/setting-up-automatic-license-deployment-ald>

111. <https://kb.igel.com/en/igel-subscription-and-more/current/deploying-licenses>

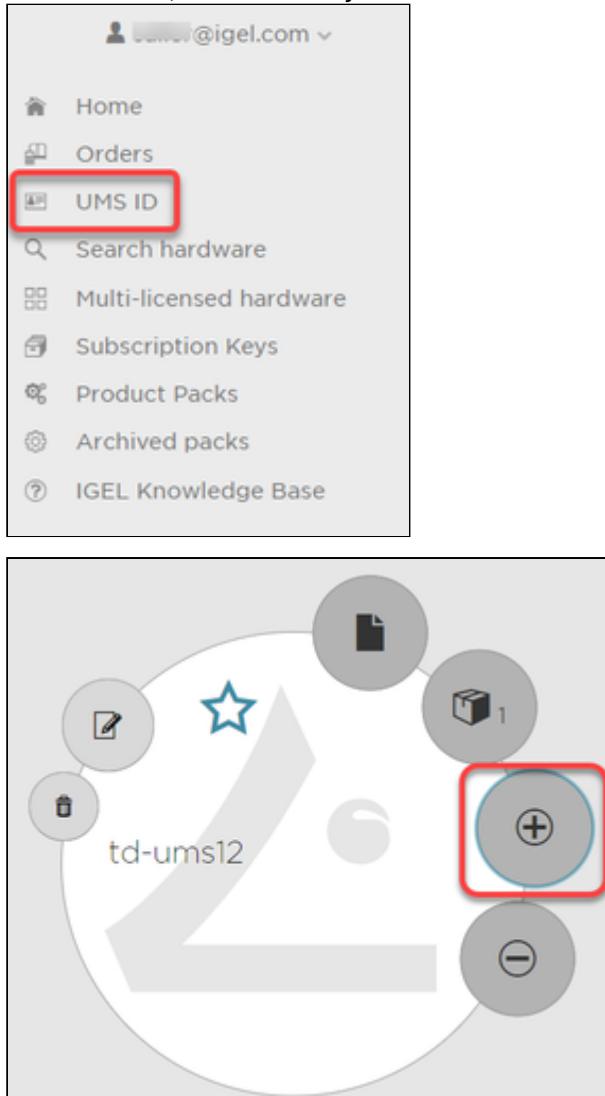
112. <https://kb.igel.com/en/igel-subscription-and-more/current/igel-software-licenses-for-igel-os-and-igel-ums#IGELSoftwareLicensesforIGELOSandIGELUMSEvaluationLicensesforIGELOS12andIGELUMS>

113. <https://kb.igel.com/en/igel-subscription-and-more/current/igel-subscription-entitlements-and-effects-of-expiration>

114. <https://kb.igel.com/en/igel-subscription-and-more/current/how-to-license-the-igel-ums>

115. <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.

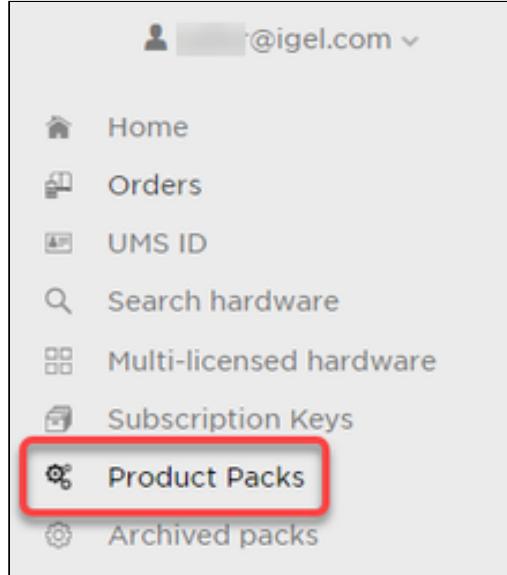
Assign Product Packs

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

	Product	Product Pack ID	Subscription Key	Volume	Status
<input type="checkbox"/>	WE-E	WE		0/10	EULA NOT ACCEPTED

- i** 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.



- Home
- Orders
- UMS ID
- Search hardware
- Multi-licensed hardware
- Subscription Keys
- Product Packs**
- Archived packs

Product Packs

All WE-E Product Packs registered to IGEL Technology

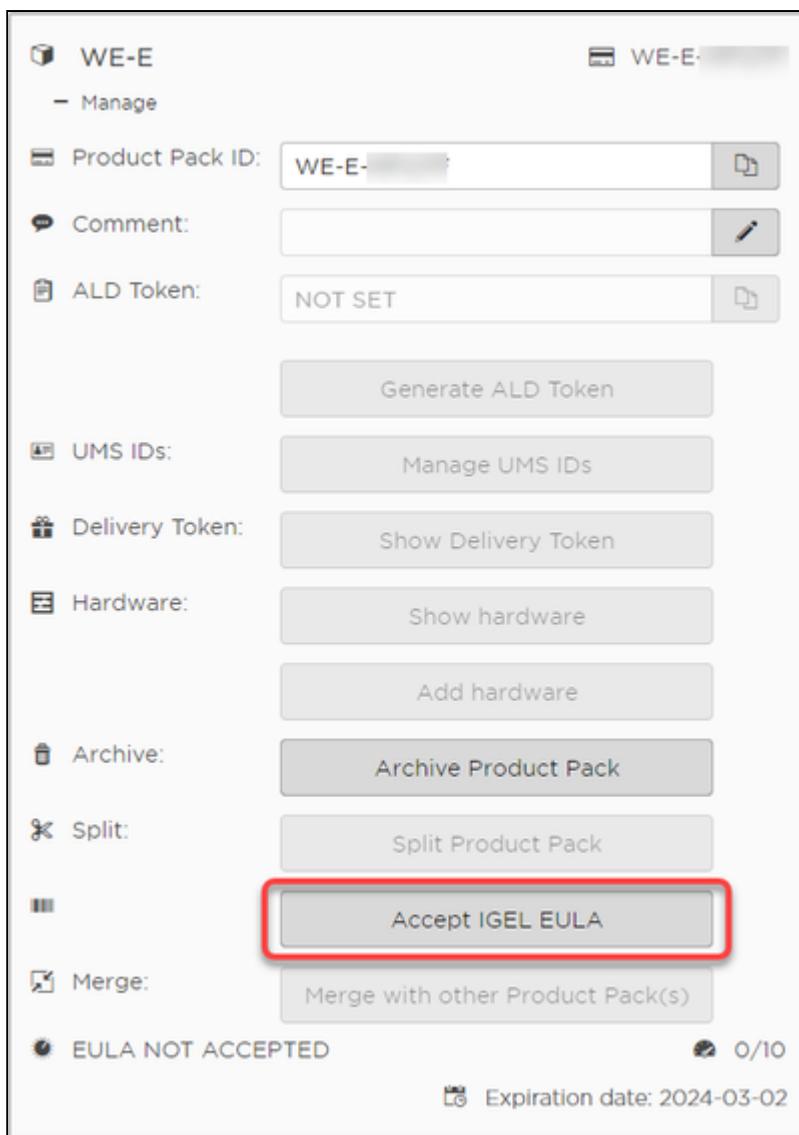
Show all

WE-E All UMS IDs Search Product Pac Filter by date

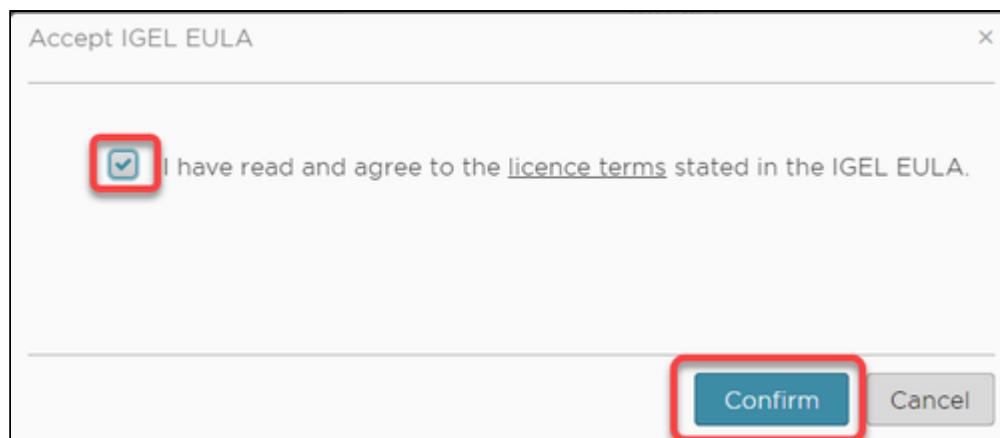
List view Card view

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), see [Setting up Automatic License Deployment \(ALD\)](#).

Onboarding IGEL OS 12 Devices

If you have configured the IGEL Onboarding Service, you use it to register your IGEL OS 12; see Register IGEL OS 12 Devices with the UMS via IGEL Onboarding Service (see page 174).

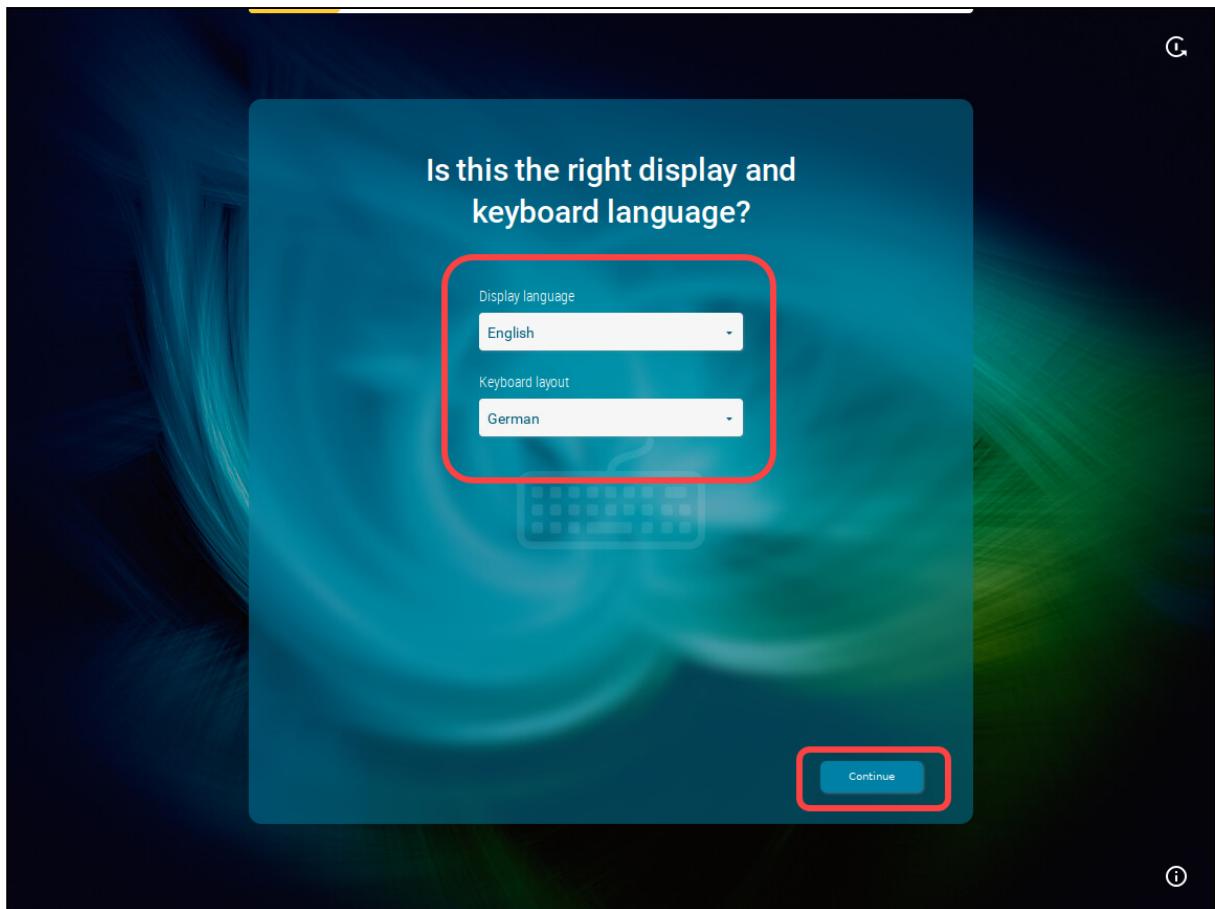
For an alternative device registration method, see Alternative Onboarding Method: Registering Devices with the UMS Using the One-Time Password (see page 181) .

- ❶ 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.
To register this device with the UMS Server, you can use the **Scan for devices** function, see [How to Scan the Network for Devices and Register Devices on the IGEL UMS¹¹⁶](#). For other device registration methods, see [Registering IGEL OS Devices on the UMS Server¹¹⁷](#).

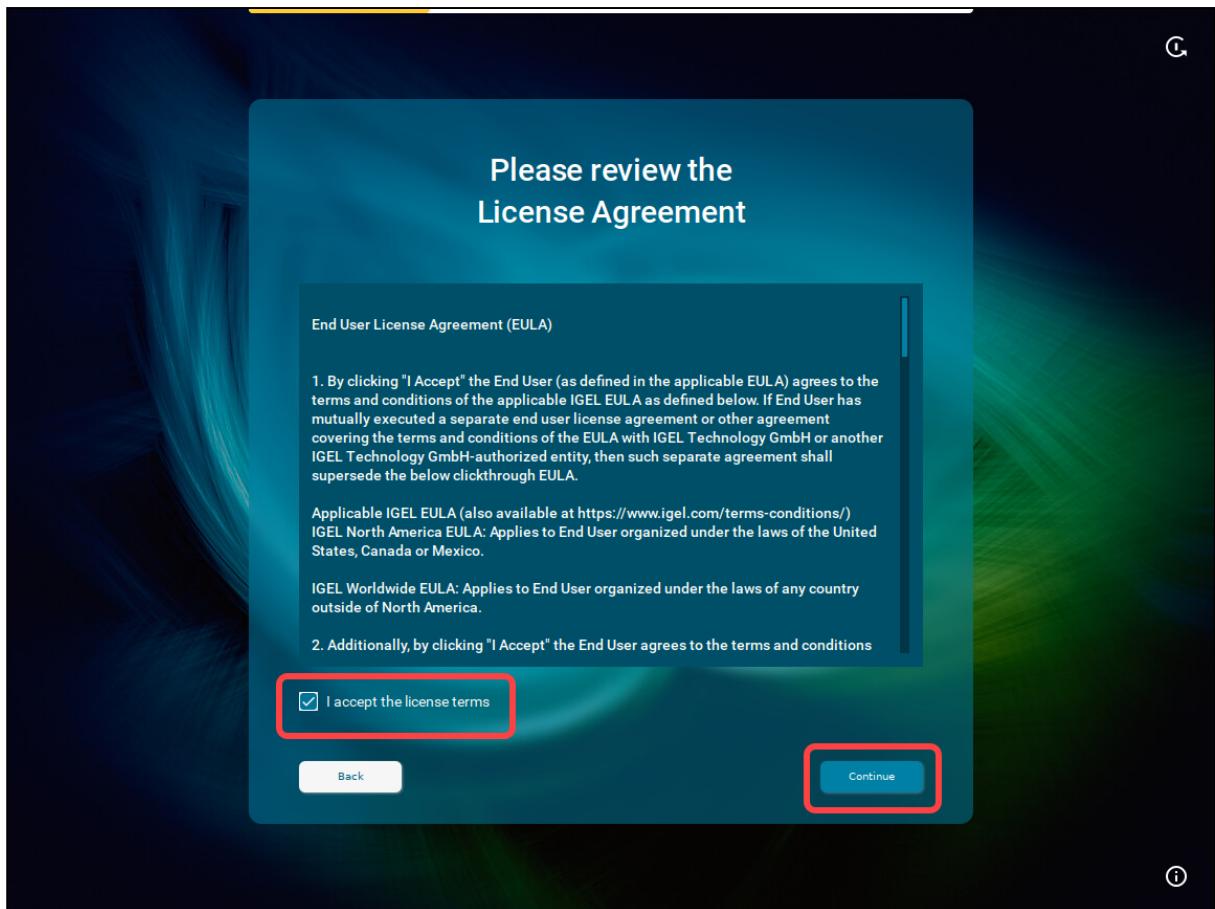
Register IGEL OS 12 Devices with the UMS via IGEL Onboarding Service

1. Switch your device on.
The Setup Assistant starts.
2. Choose the display language and set your keyboard layout. Click **Continue**.

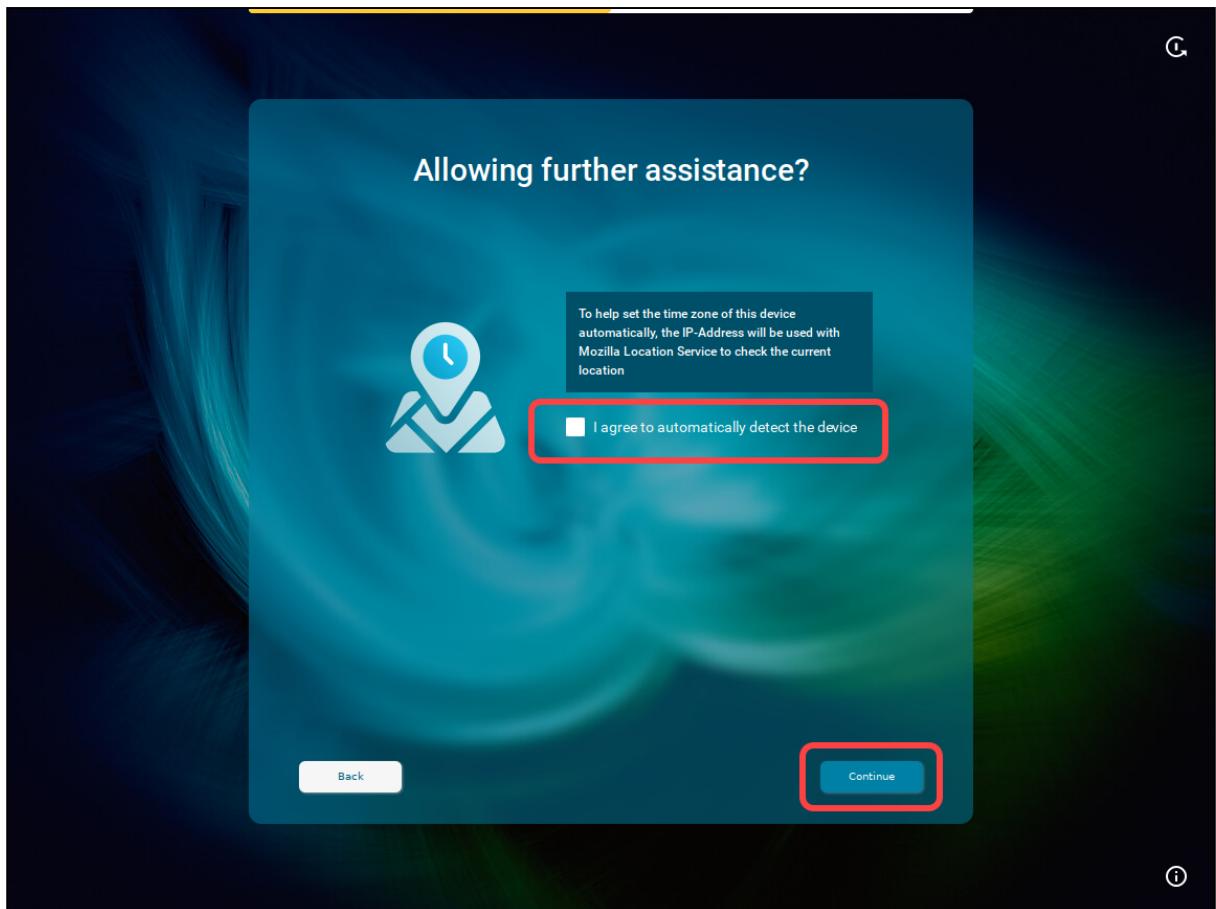
116. <https://kb.igel.com/en/universal-management-suite/current/how-to-scan-the-network-for-devices-and-register-d>
117. <https://kb.igel.com/en/universal-management-suite/current/registering-igel-os-devices-on-the-ums-server>



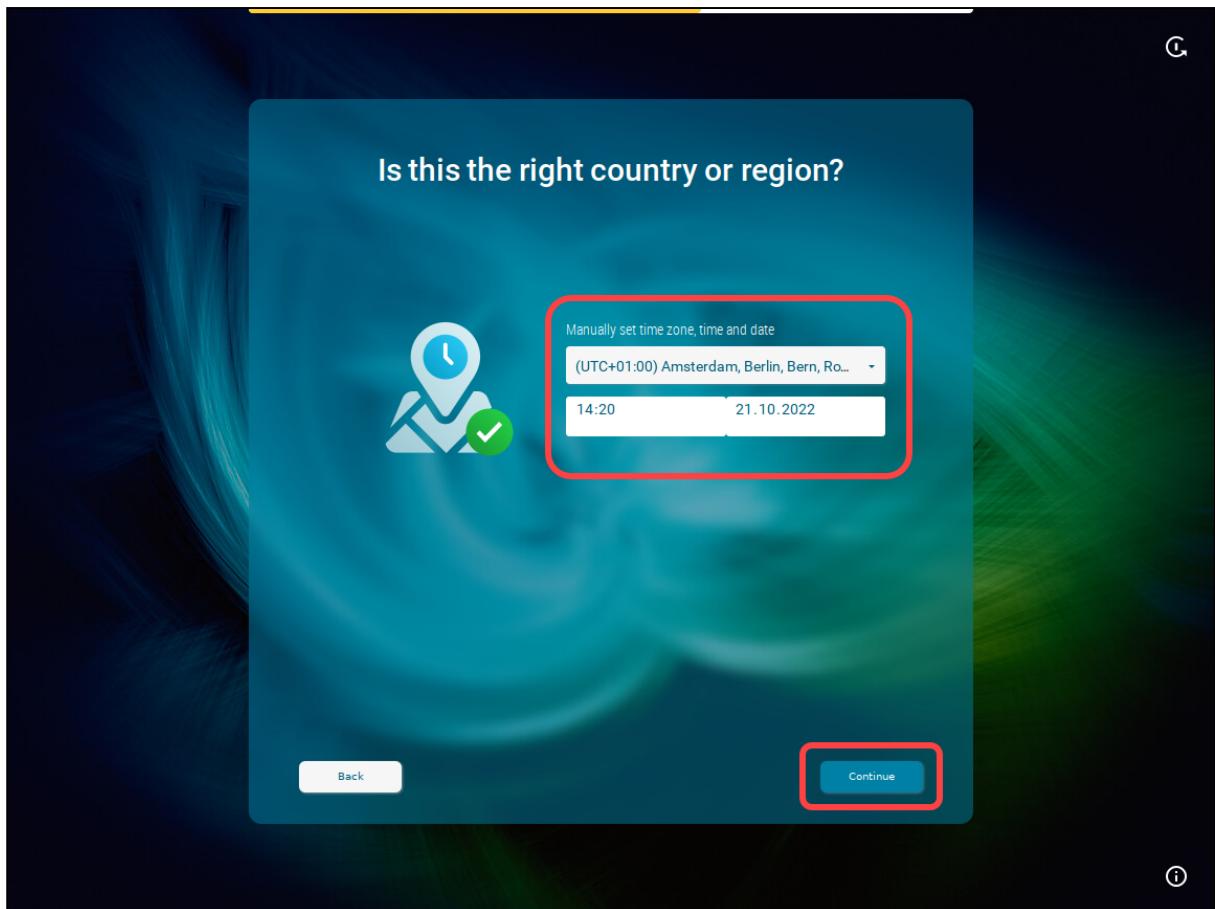
3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.



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



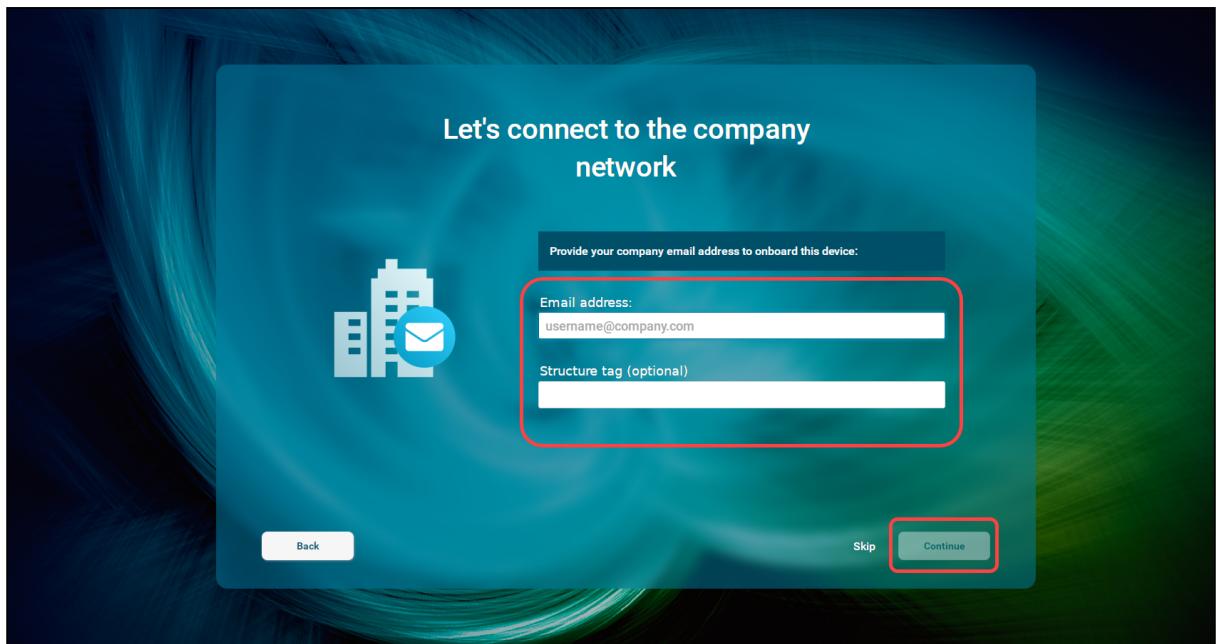
Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.



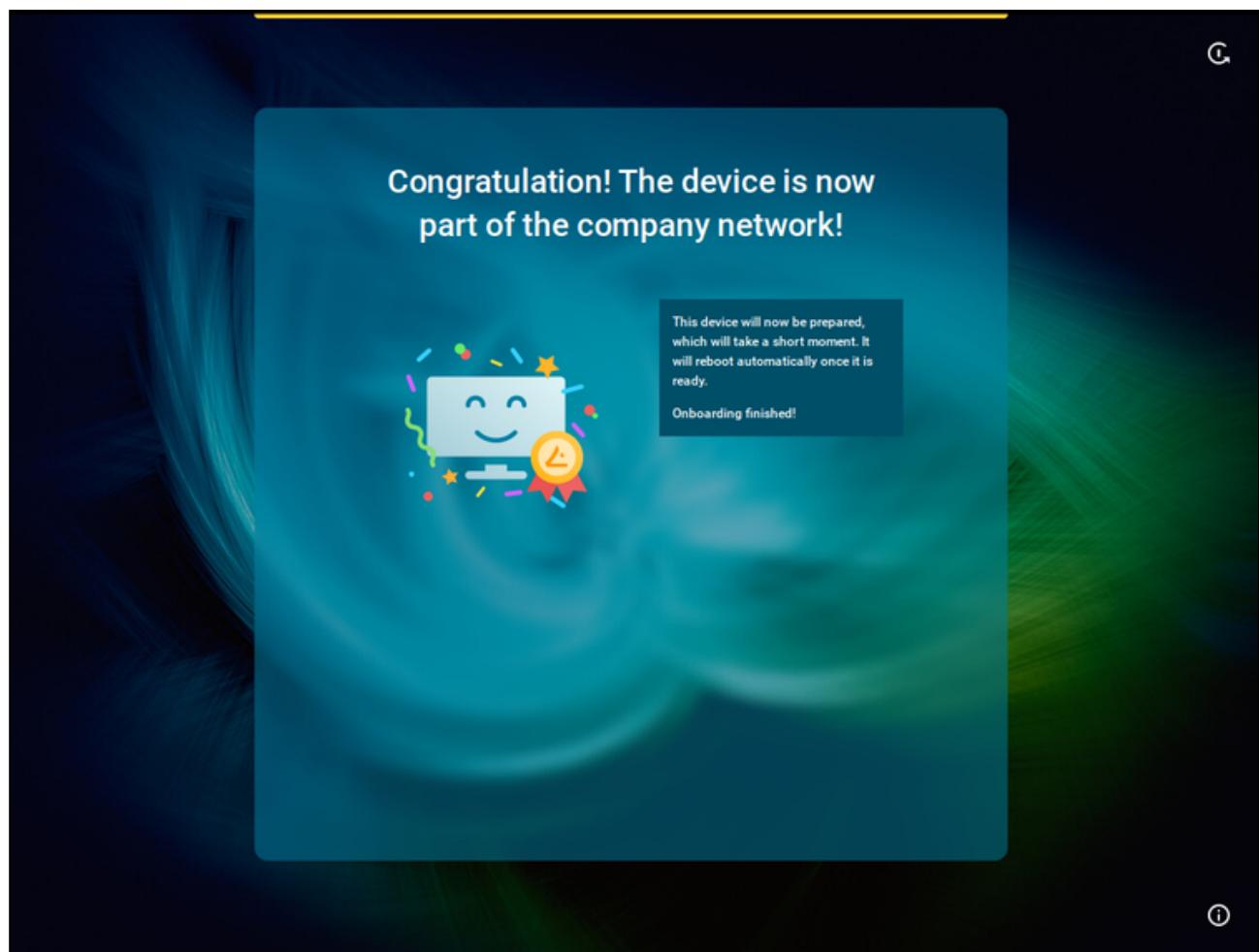
6. Enter your e-mail address (using the correct upper/lowercase) and click **Continue**.

Optionally, you can also enter a **Structure tag** starting from IGEL OS 12.7.3. Using structure tags, newly registered devices will automatically have the information on where they are to be placed in the structure tree of the UMS Console. For details, see [How to Automate the Rollout Process in the IGEL UMS¹¹⁸](#) and [Using Structure Tags with IGEL OS Devices¹¹⁹](#).

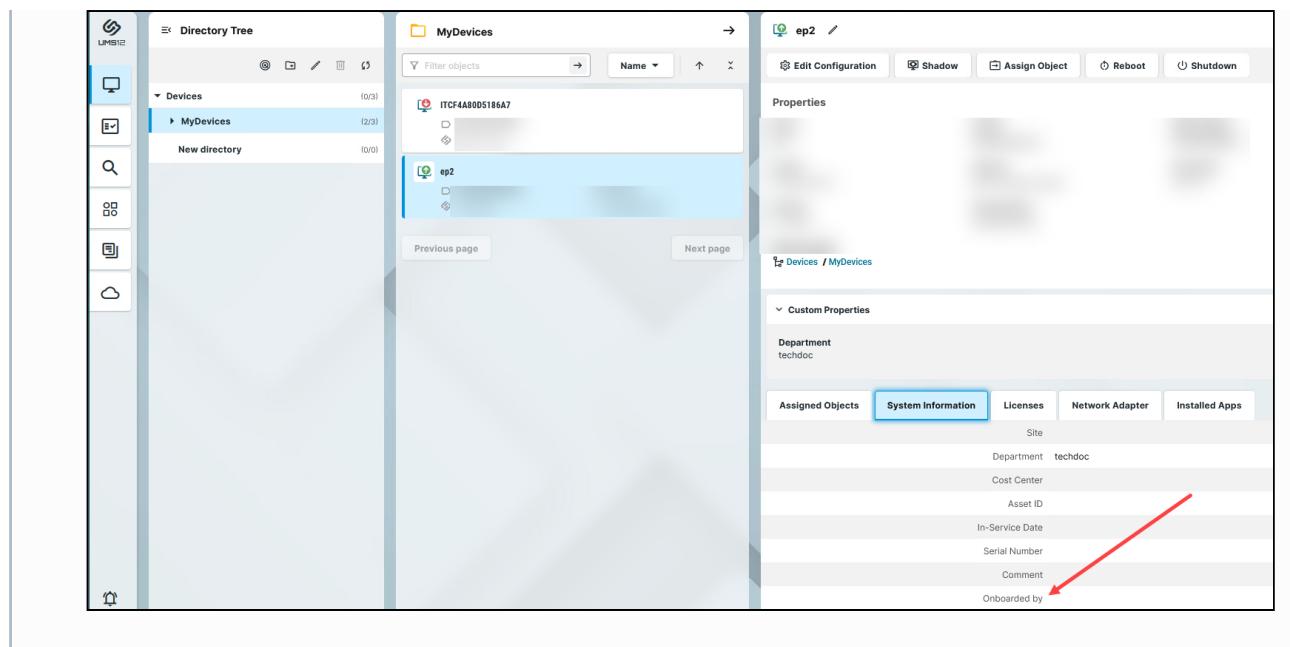
¹¹⁸. <https://kb.igel.com/en/universal-management-suite/current/how-to-automate-the-rollout-process-in-the-igel-um>
¹¹⁹. <https://kb.igel.com/en/universal-management-suite/current/using-structure-tags-with-igel-os-11-devices>



When everything goes 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.



- i 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**.



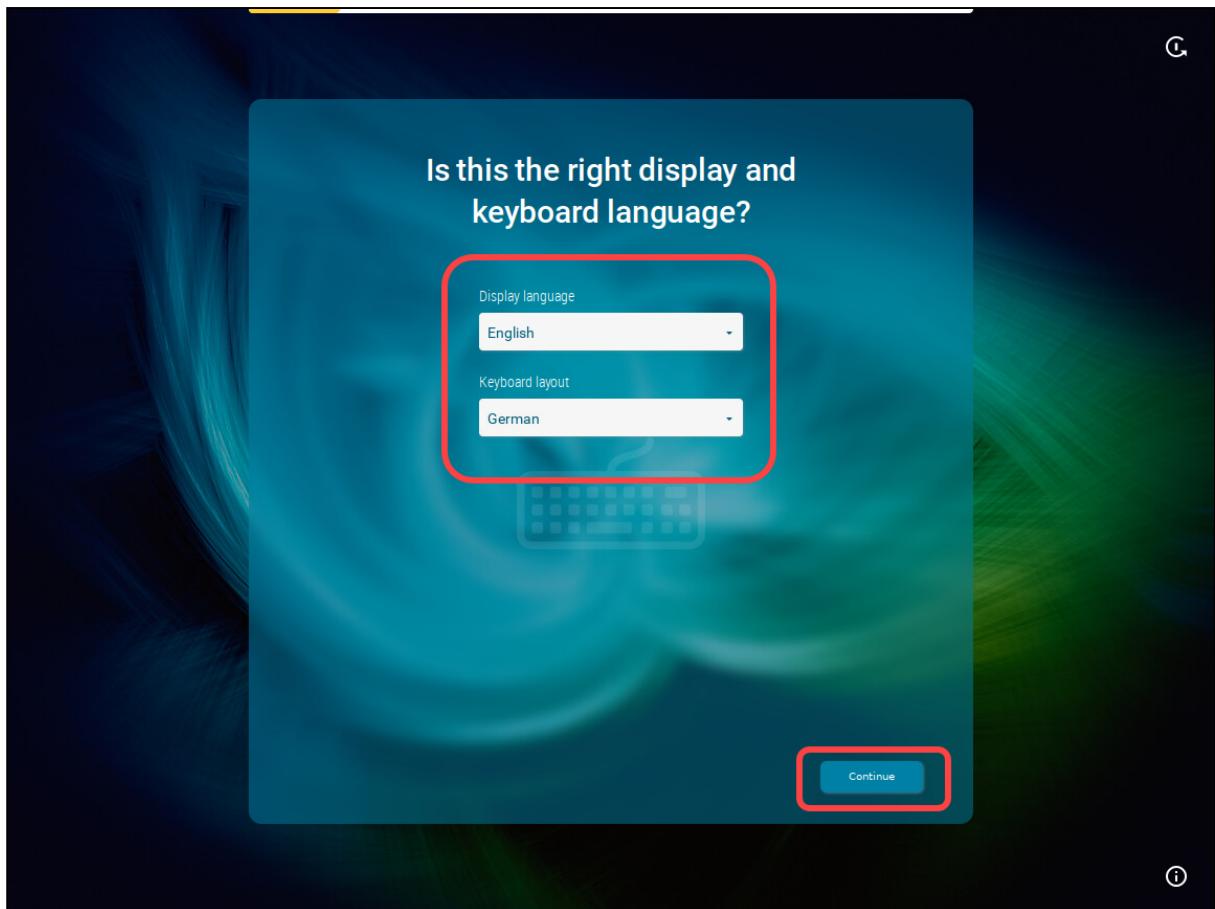
The screenshot shows the UMS interface with the following details:

- Left Sidebar:** Shows icons for Home, Devices, Groups, and Help.
- Directory Tree:** Under Devices, there is a folder named "MyDevices".
- MyDevices View:** Displays a list of devices. One device, "ITCF4A80DS186A7", is selected. Below it, another device, "ep2", is also selected.
- Properties Panel:** Shows the properties for the selected device "ep2".
 - Custom Properties:** Department: techdoc
 - Assigned Objects:** Site, Department: techdoc, Cost Center, Asset ID, In-Service Date, Serial Number, Comment
 - System Information Tab:** Active tab. It includes fields for Site, Department, Cost Center, Asset ID, In-Service Date, Serial Number, and Comment. The "Onboarded by" field is highlighted with a red arrow.
 - Licenses, Network Adapter, Installed Apps:** Other tabs in the properties panel.

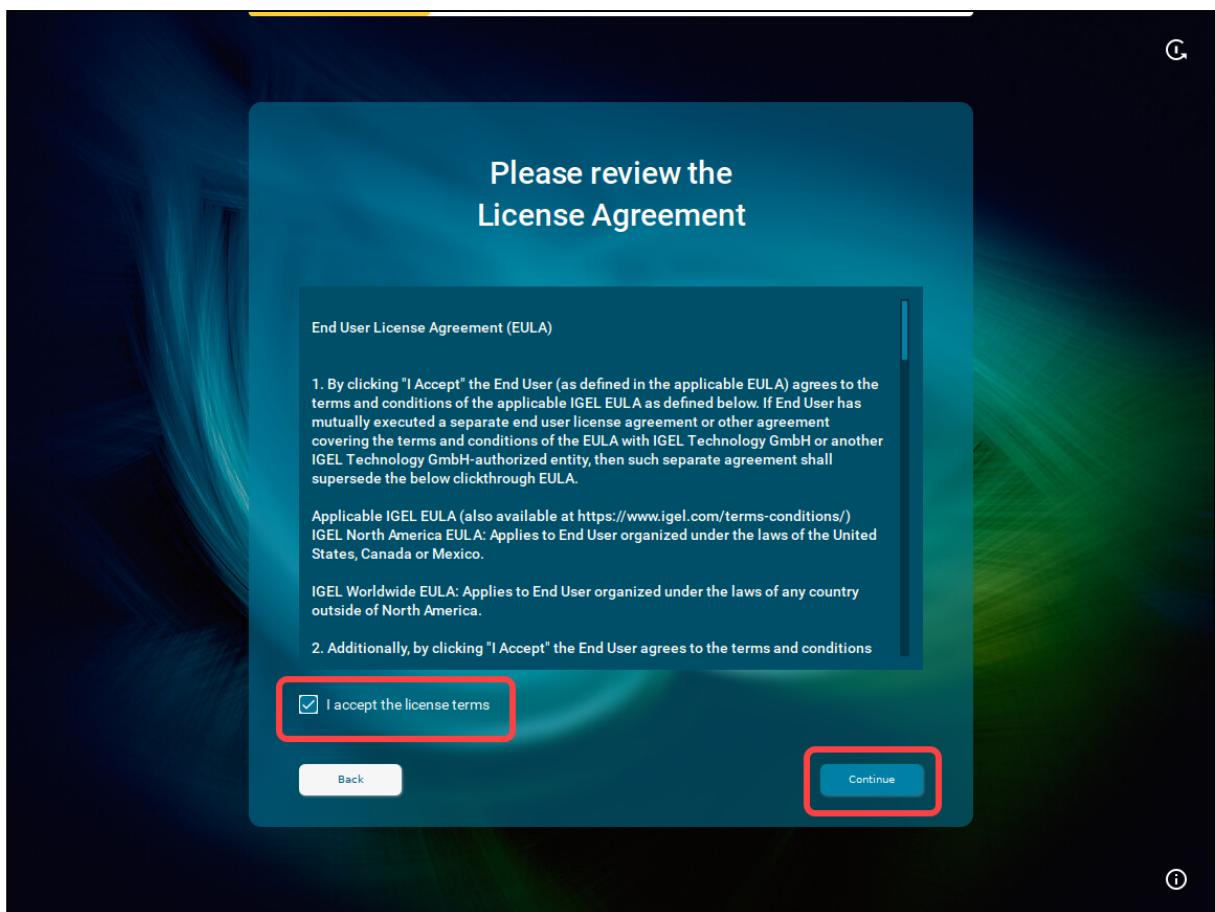
Alternative Onboarding Method: Registering Devices with the UMS Using the One-Time Password

If you decide 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.

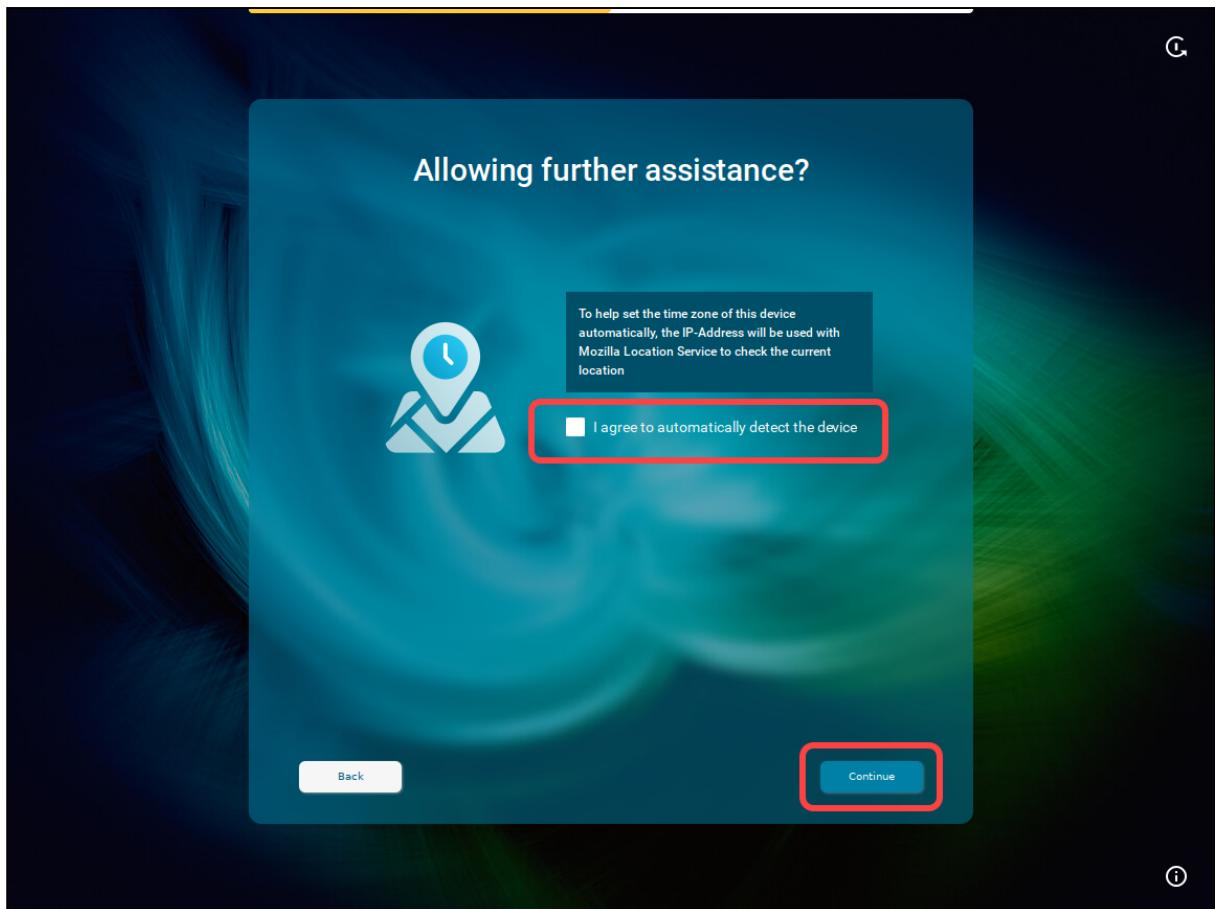
1. Switch your device on.
The Setup Assistant starts.
2. Choose the display language and set your keyboard layout. Click **Continue**.



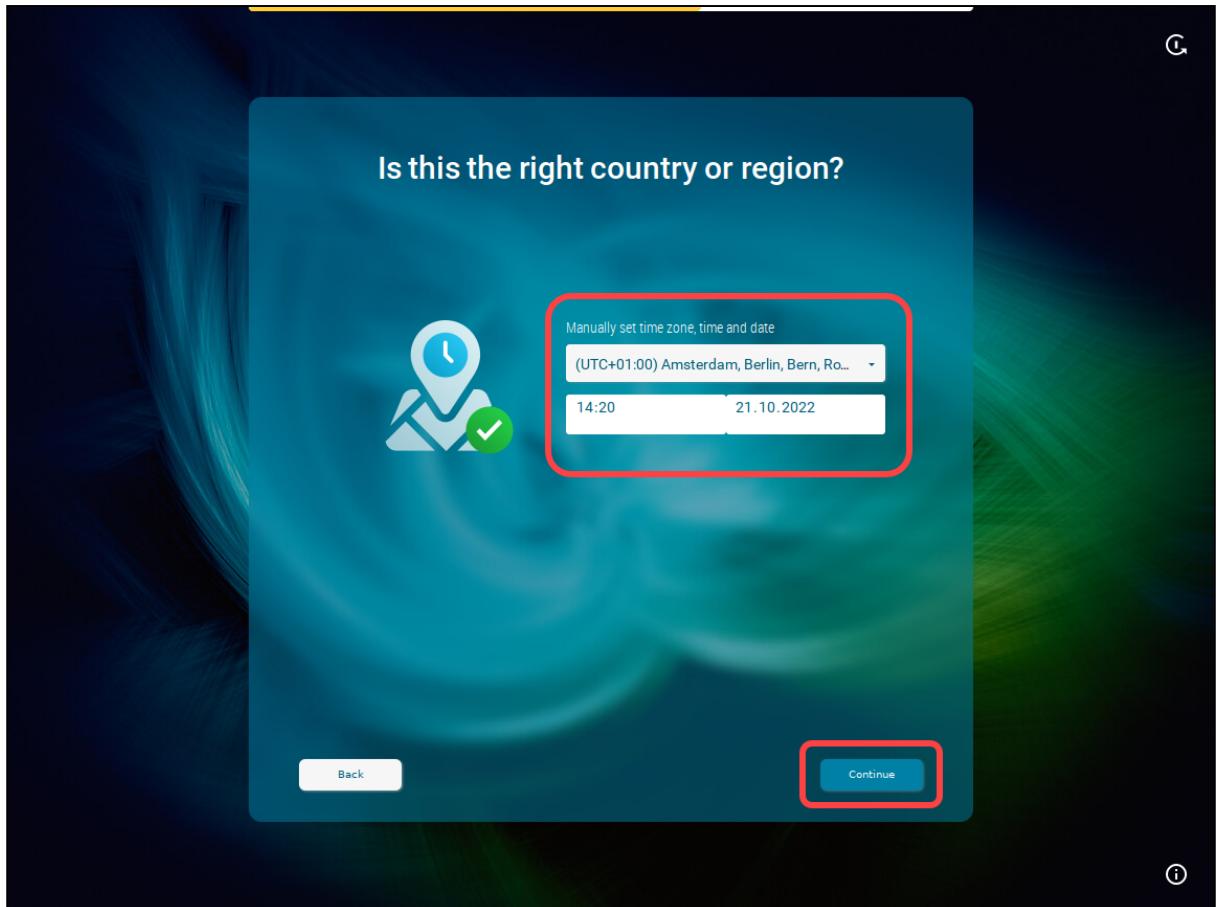
3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.



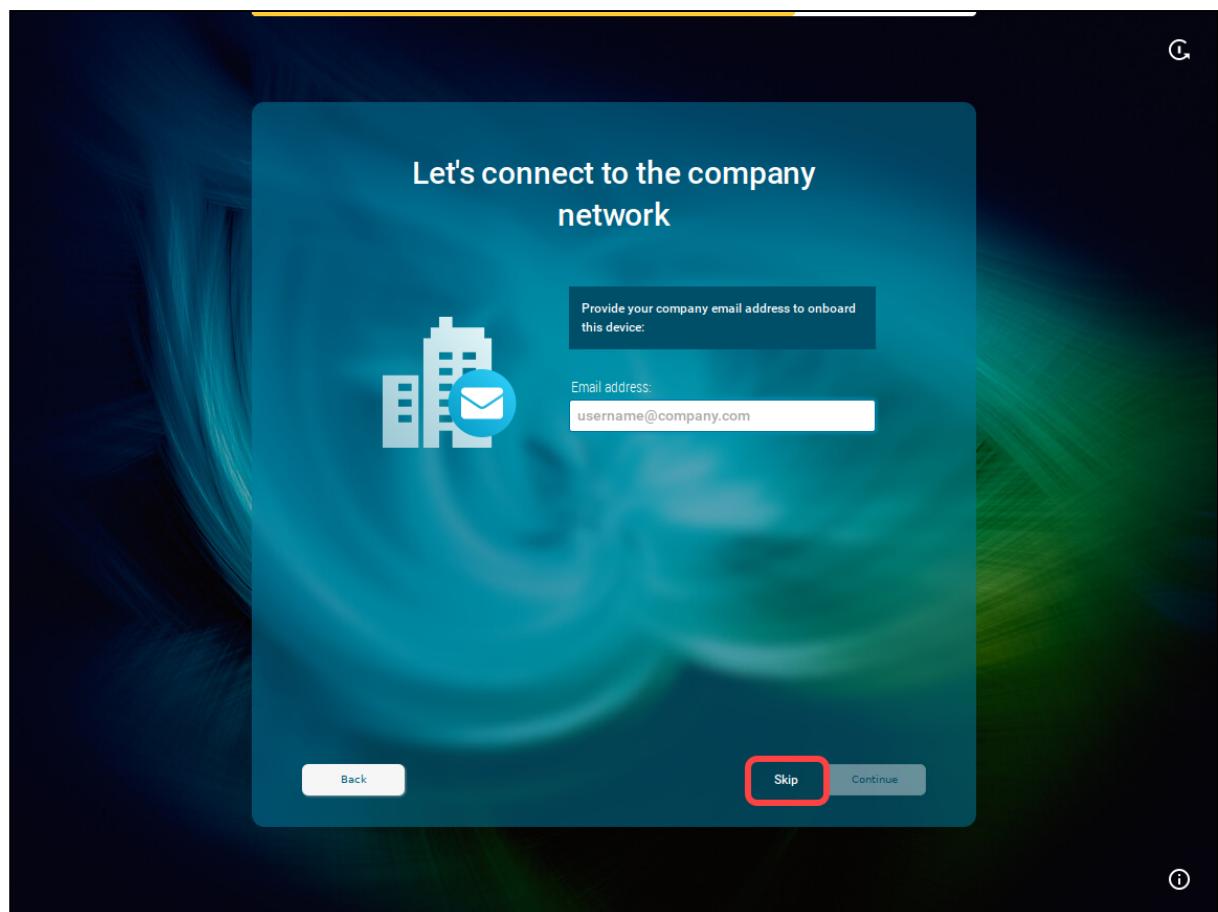
4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under Troubleshooting: Configuring a Network during the Onboarding.
5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.



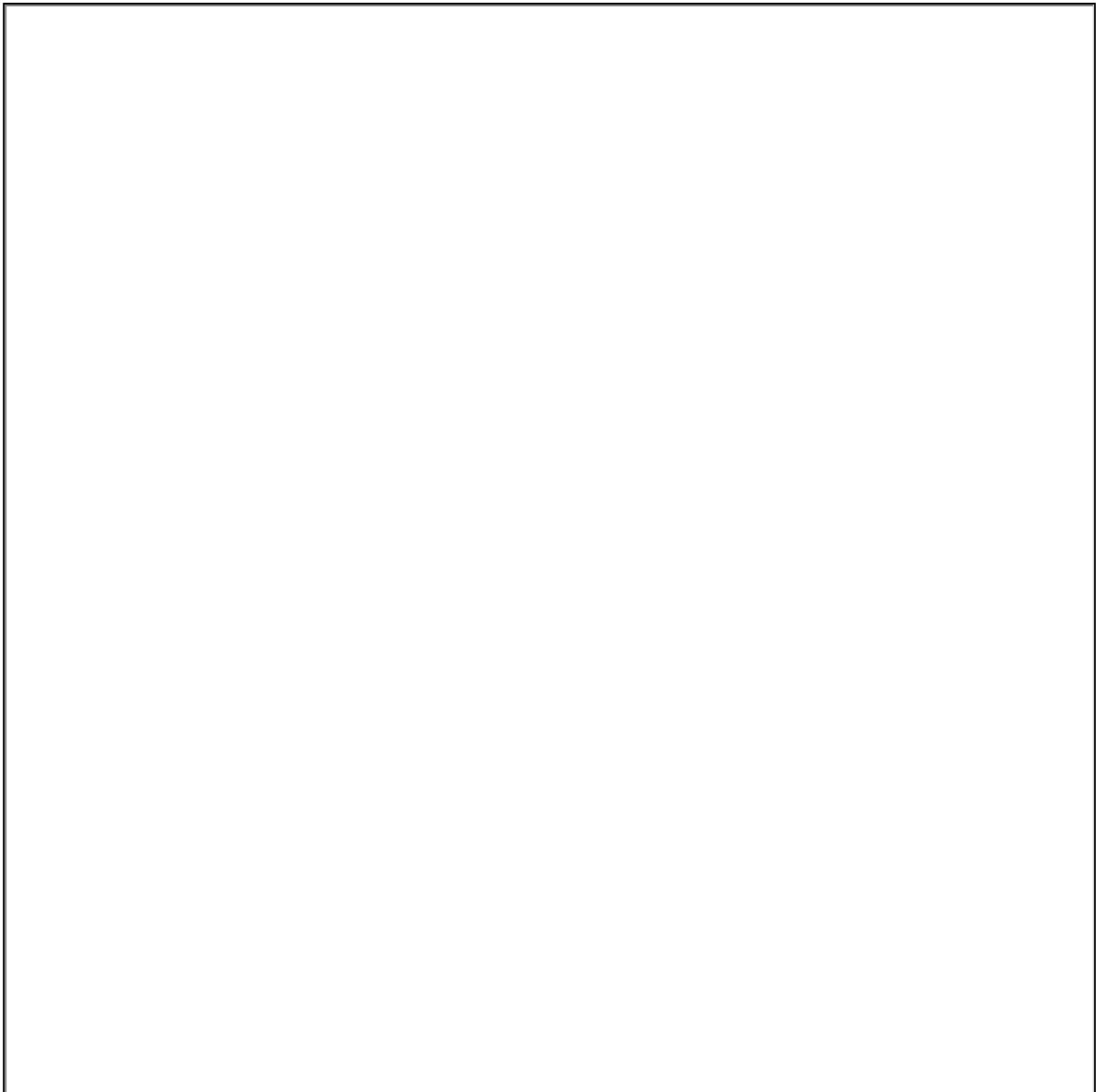
Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.



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 (see [Server - View Your IGEL UMS Server Information¹²⁰](#)) of the UMS Server or the cluster address (see [Server Network Settings in the IGEL UMS¹²¹](#)).

Port: Web server port (Default: 8443). If configured, you can alternatively use the public web port (see [Server Network Settings in the IGEL UMS¹²²](#)).

120. <https://kb.igel.com/en/universal-management-suite/current/server-view-your-igel-ums-server-information>
121. <https://kb.igel.com/en/universal-management-suite/current/server-network-settings-in-the-igel-ums>

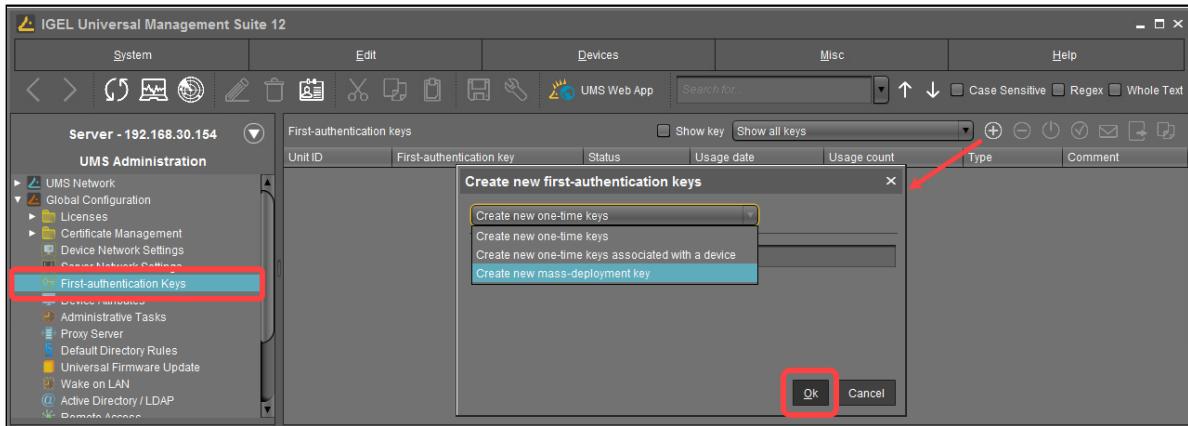
One-time password: First-authentication key (no matter one-time key or mass-deployment key), which you create under **UMS Console > UMS Administration > Global Configuration > First-authentication Keys**.

Structure tag: Using structure tags, newly registered devices will automatically have the information where they are to be placed in the structure tree of the UMS Console. For details, see [How to Automate the Rollout Process in the IGEL UMS¹²³](#) and [Using Structure Tags with IGEL OS Devices¹²⁴](#).

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.

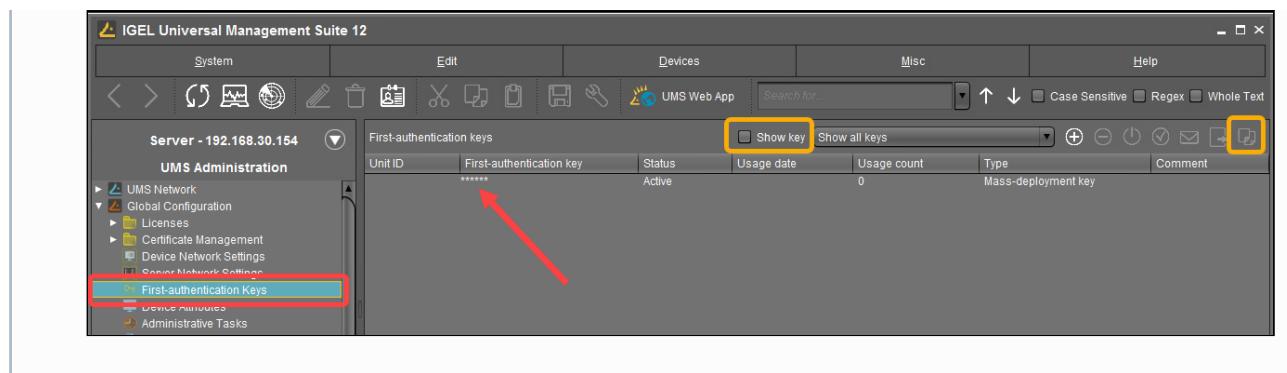


You can view the created key by clicking **Show key**; or simply copy it to the clipboard.

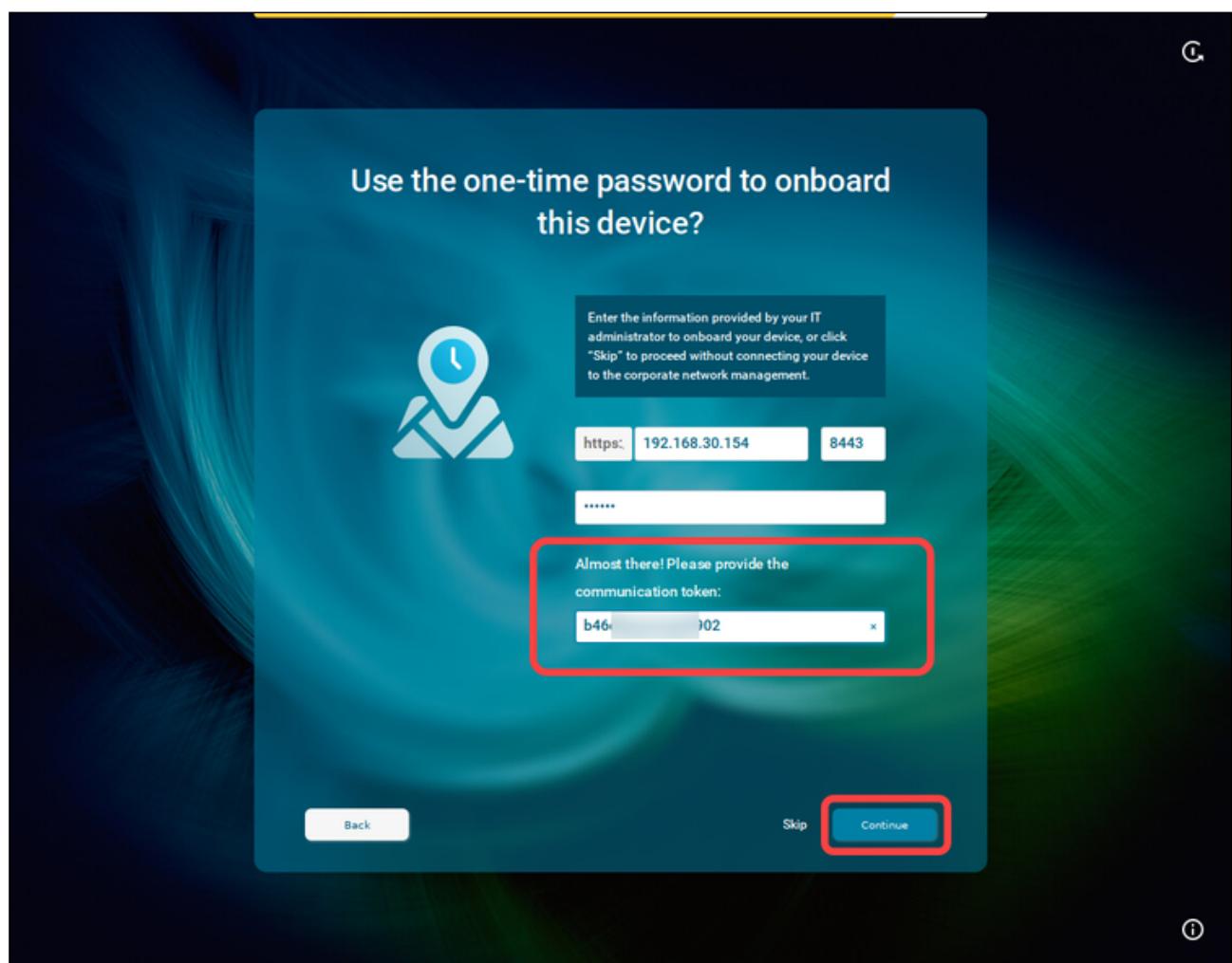
122. <https://kb.igel.com/en/universal-management-suite/current/server-network-settings-in-the-igel-ums>

123. <https://kb.igel.com/en/universal-management-suite/current/how-to-automate-the-rollout-process-in-the-igel-um>

124. <https://kb.igel.com/en/universal-management-suite/current/using-structure-tags-with-igel-os-11-devices>



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**.



i 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

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

Version: 3
 Subject: C=DE, L=Bremen, O=IGEL Technology GmbH, CN=ID--49679-1665998
 Issuer: C=DE, L=Bremen, O=IGEL Technology GmbH, CN=ID--49679-1665998
 Signature Algorithm: SHA512withRSA
 Key: RSA, 4096 bits
 Serial number:
 Fingerprint (SHA1): b46c...902
 Fingerprint (SHA256):
 Valid from: Mon Oct 17 11:20:02 CEST 2022
 Valid to: Fri Oct 17 11:20:02 CEST 2042

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

The screenshot shows the UMS interface with the following details:

- UMS Server Details:**
 - Process ID: 2
 - Last Change: Fri
 - Cluster ID: U
 - Operating System: M ver 2019
 - Host Name: 1t
 - Process Type: U
 - Port: 31
 - Version: 12
 - Cert. Fingerprint - Part 1: e1
 - Cert. Fingerprint - Part 2: 3
 - Cert. Fingerprint - Part 3: 4
 - Cert. Fingerprint - Part 4: fa
 - Root Cert. Fingerprint - Part 1: e1
 - Root Cert. Fingerprint - Part 2: 10
 - Root Cert. Fingerprint - Part 3: 5d
 - Root Cert. Fingerprint - Part 4: 0f
 - Communication Token: 3
- Requests:** A line chart showing successful requests over time. The Y-axis ranges from 0 to 1.0, and the X-axis shows dates from 2024-02-16 to 2024-02-17. The chart shows a constant green line at 1.0, indicating 100% successful requests.

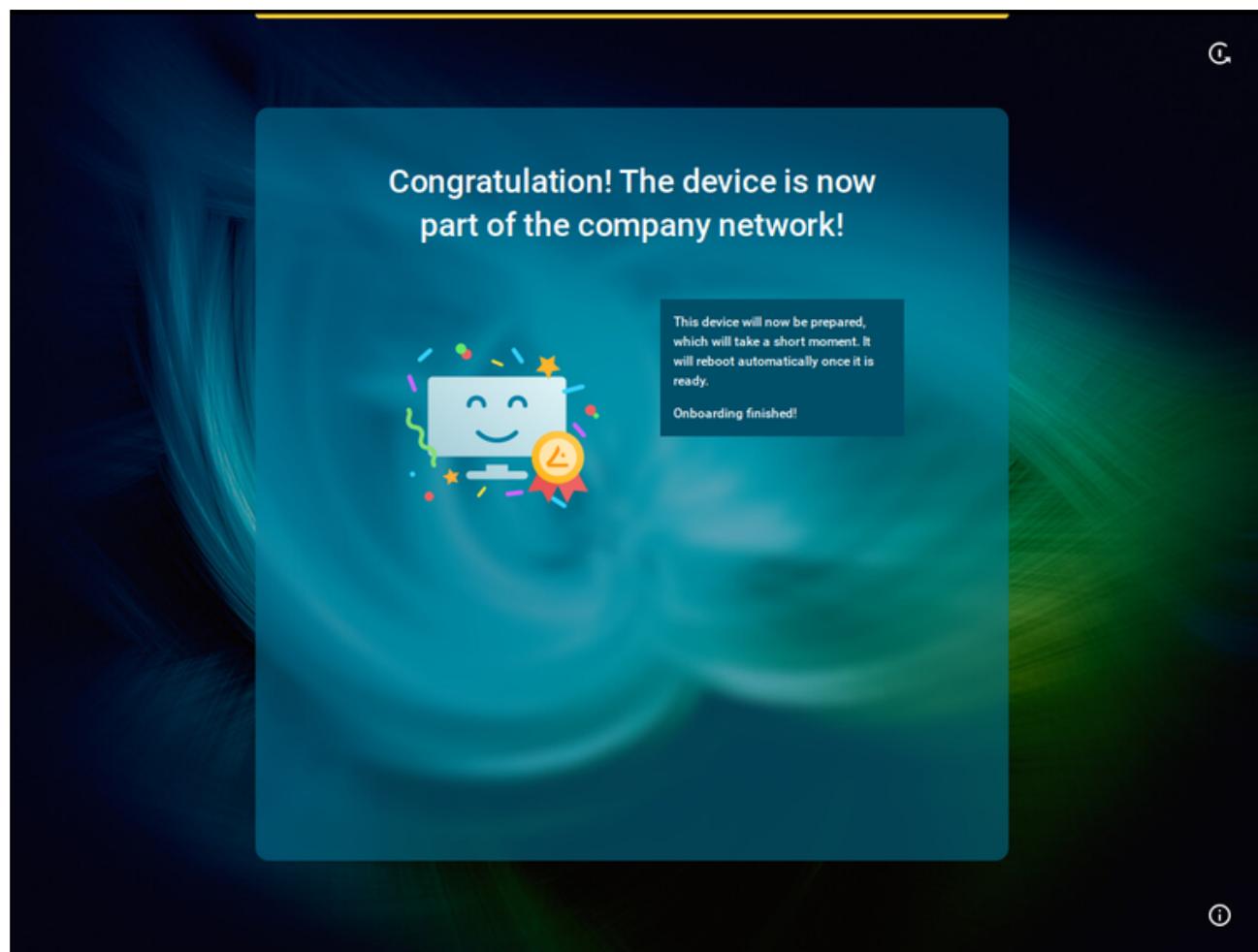
i If You Use IGEL Cloud Gateway

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](#)¹²⁵.
- **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.

125. <https://kb.igel.com/en/igel-cloud-gateway/current/generating-and-distributing-first-authentication-k>



Troubleshooting: Configuring a Network during the Onboarding

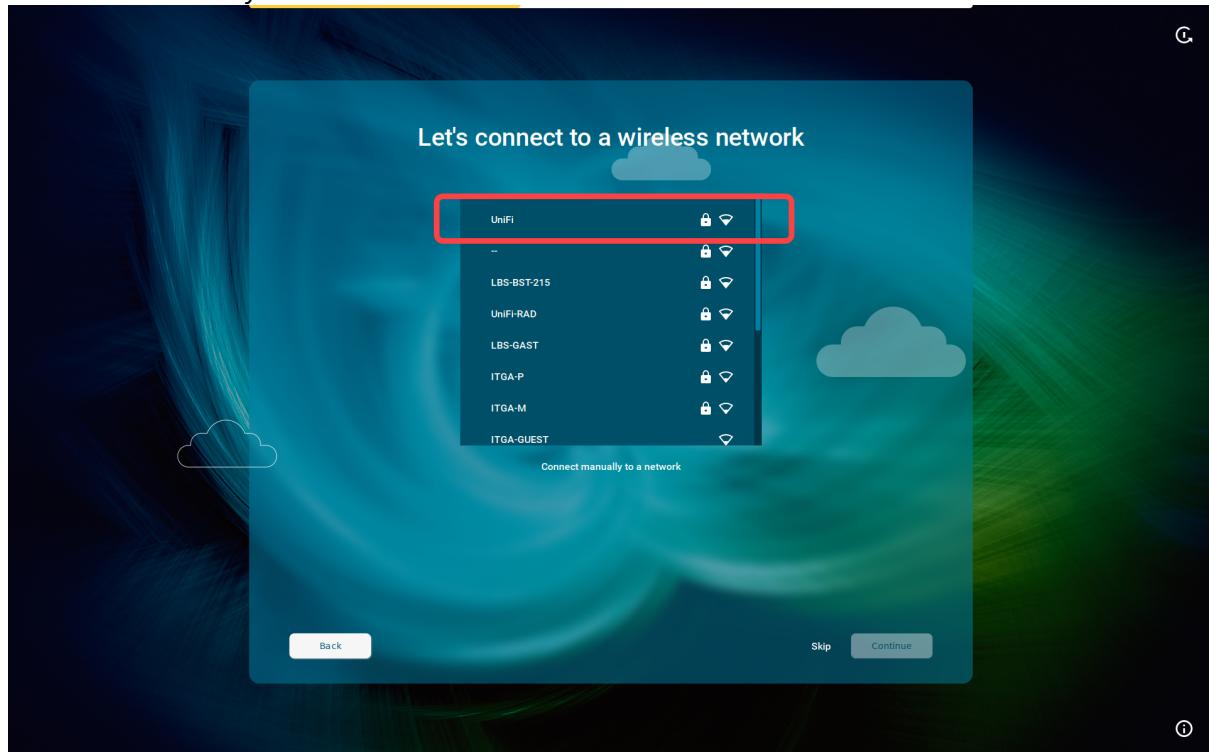
If your device cannot connect to the network instantly, the IGEL Setup Assistant will ask you to configure your network connection.

Connecting to a Wireless Network That Is Visible

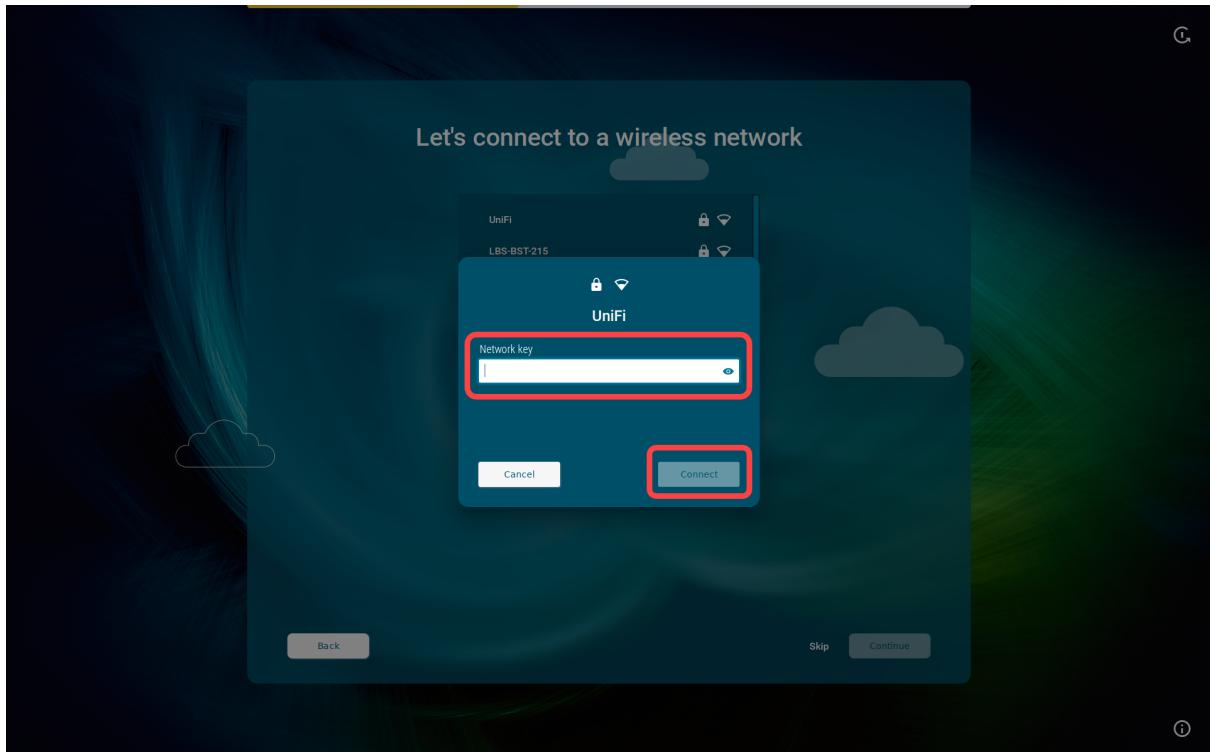
- Wi-Fi networks with certificates are not supported in the Setup Assistant.

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.

- Select the network you want to connect to.



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

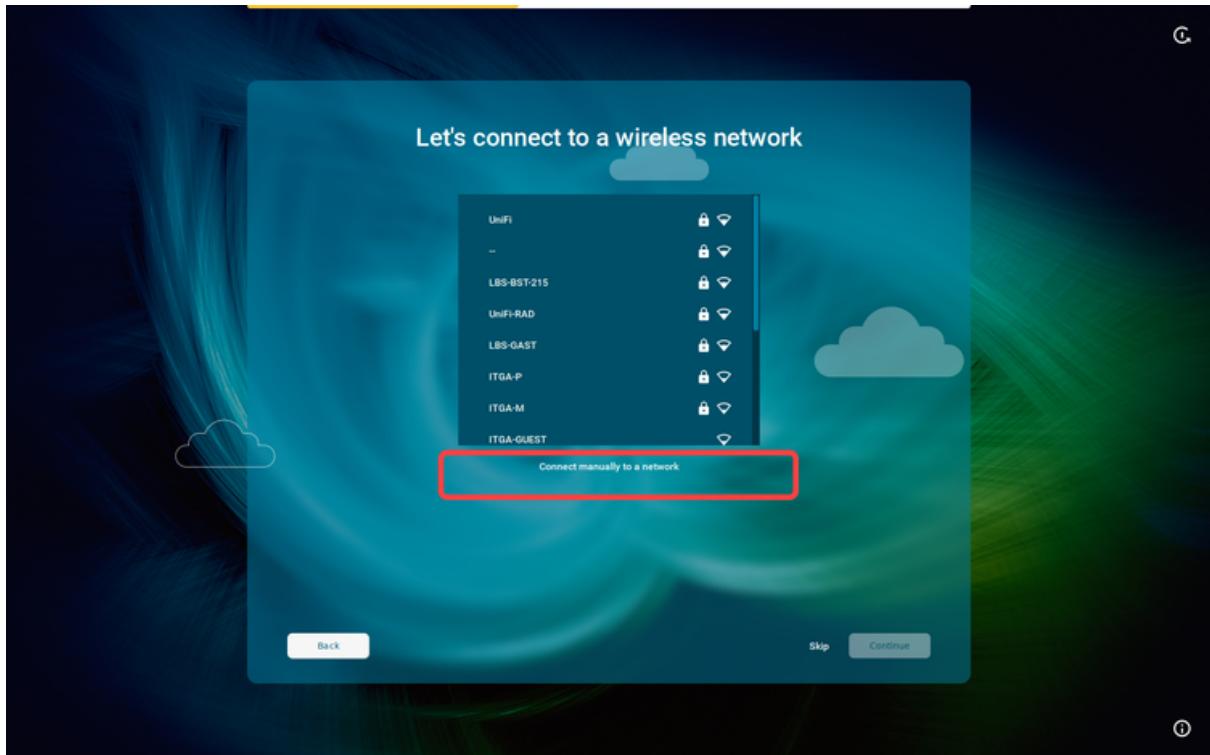


3. Click **Connect.**

- i** 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

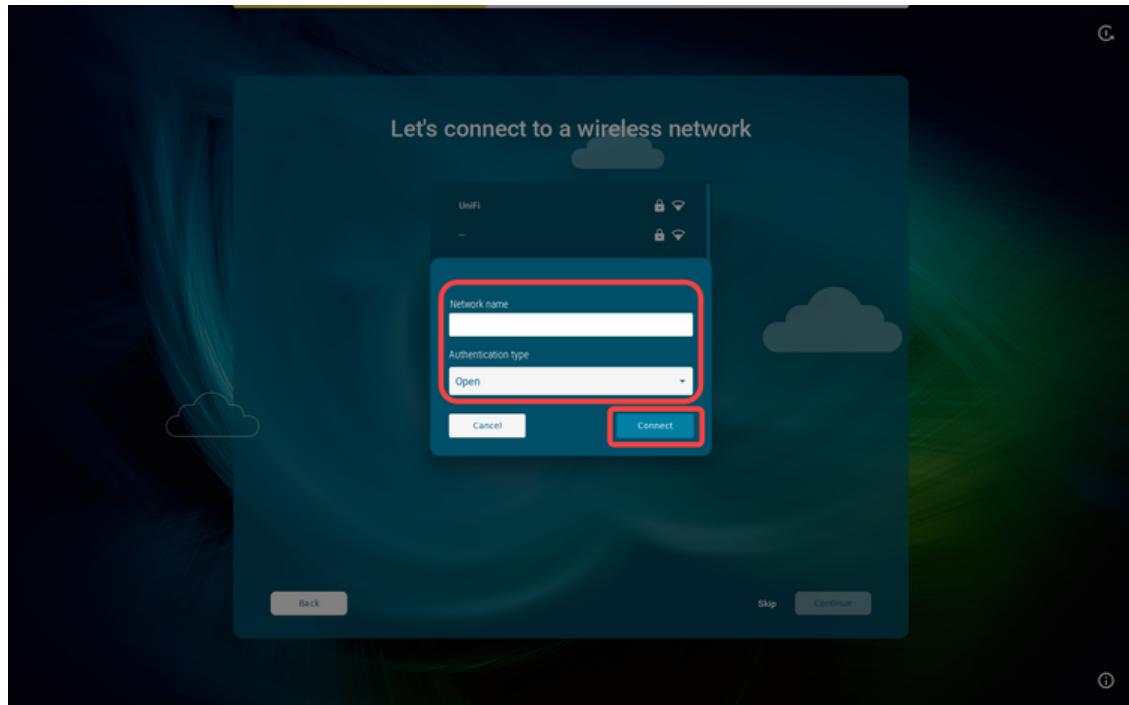
1. Click **Connect manually to a network.**



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

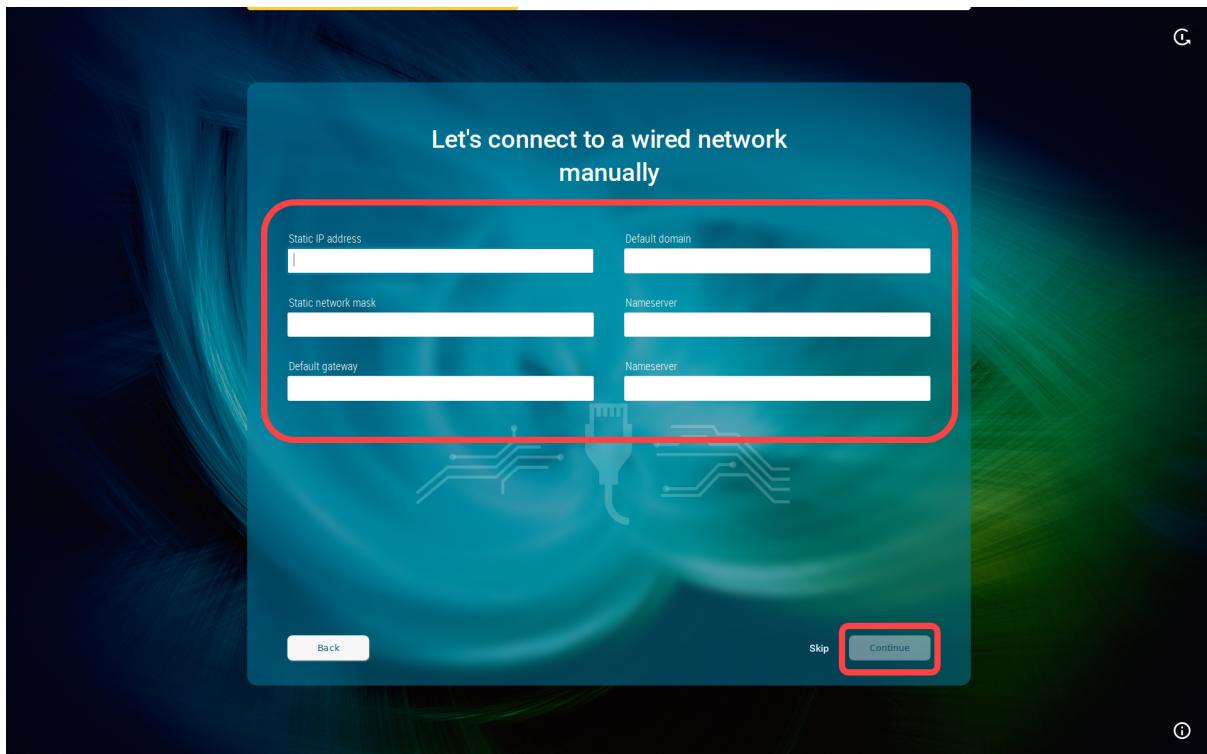
Default gateway: IP address of the default gateway

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:

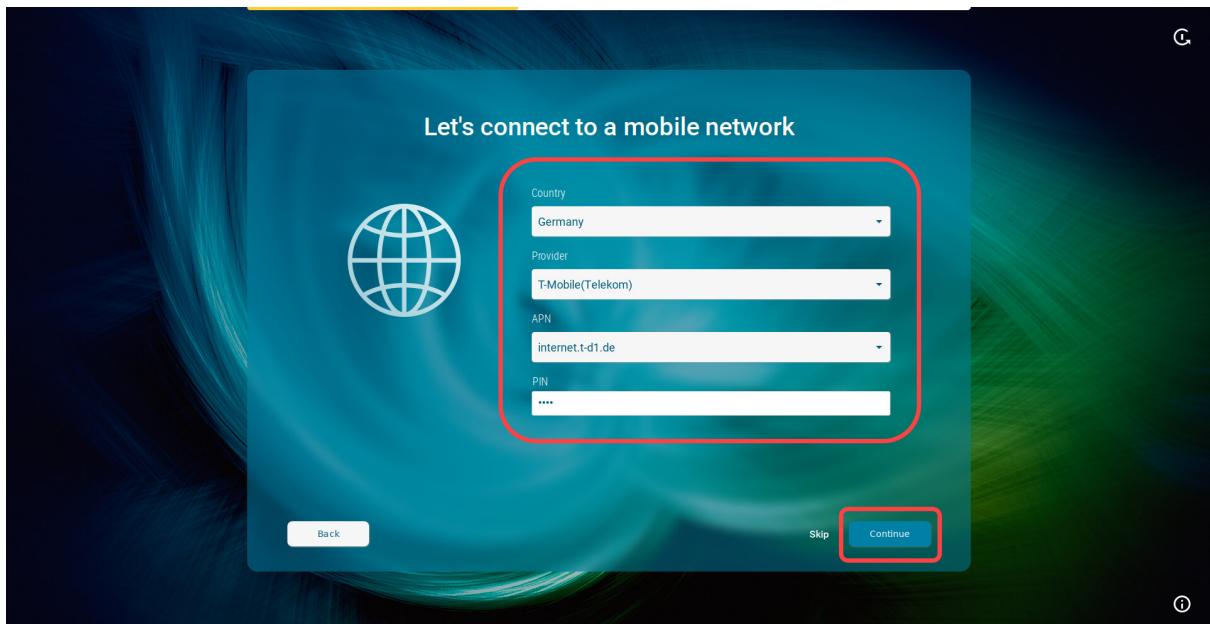
Country or region: The country or region of your provider

Provider: Provider (the possible options depend on what you choose for **Country or region**)

APN: Access point name (the possible options depend on what you choose for **Provider**)

PIN (displayed if the SIM card is locked): PIN for the SIM card used

2. Click **Continue**.



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 For information on the solution, see Troubleshooting: Error 37 during Onboarding of an IGEL OS12 Device (see page 201) .
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 202) .
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 223) and contact IGEL Support.

Troubleshooting: Error 37 during Onboarding of an IGEL OS12 Device

During the onboarding with the IGEL Onboarding Service or with the one-time password method, you get the following error message: " Could not manage your device because of an internal error (<37>) ". Error 37 indicates that the device was unable to get the CA certificates from the Universal Management Suite (UMS) Server(s).

Problem

Possible causes for error 37 may be:

- NO HTTPS connection to the UMS Server
Getting the CA certificates from the UMS Server is the first step of the onboarding process, so the error 37 can indicate that the device is unable to establish a HTTPS connection to the UMS Server. This can be caused by the network environment configuration, like a firewall or TLS inspection.
- CA certificates cannot be verified due to an incomplete CA chain
The downloaded CA certificates are verified by the device, so the error 37 can occur if the downloaded CA certificates cannot be verified by IGEL OS. This can be caused by an incomplete chain of CA certificates, for example, a missing certificate of the root CA.

Solution

No HTTPS Connection to the UMS Server

To diagnose network issues, use the `curl` command, the standard HTTP(s) tool included in IGEL OS 12/OS 11 and other Linux OS. Execute the following command to download CA certificates from the UMS Server:

```
curl --tlsv1.3 --insecure https://<YOUR_UMS_ADDRESS>:<PORT>/device-connector/device/.well-known/est/cacerts
```

If the command fails to download CA certificates, you potentially have a networking or firewall problem. Try to adjust firewall settings or TLS inspection to allow the necessary HTTPS connections.

CA Certificates Cannot Be Verified Due to an Incomplete CA Chain

To solve this, import the complete CA chain as it described in [Installing an Existing Certificate Chain for the ICG¹²⁶](#).

If the missing certificate belongs to a public CA, try to update to IGEL OS 12.3.0. or above. These IGEL OS versions can automatically complete the CA chain with the required issuer certificates from the repository of public CA certificates contained in IGEL OS 12.

126. <https://kb.igel.com/en/igel-cloud-gateway/current/installing-an-existing-certificate-chain-for-the-i>

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.

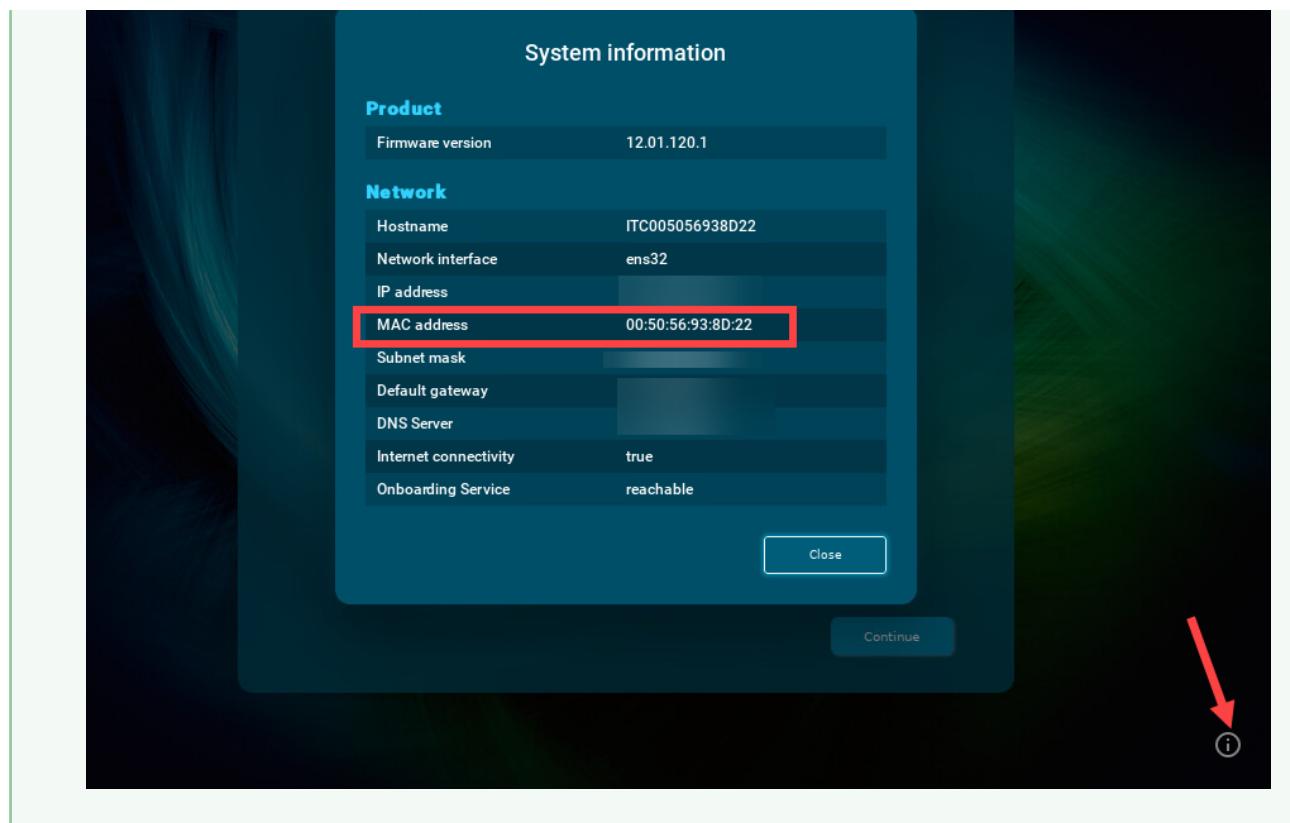
Solution

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).

- ✓ 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:



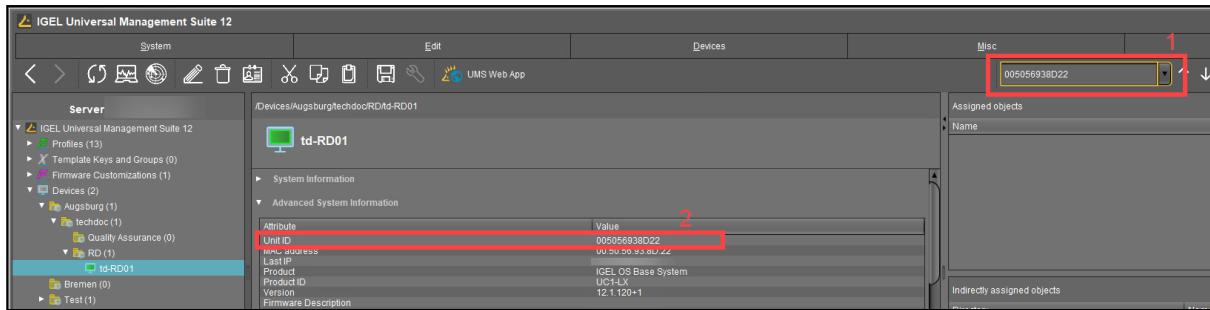
2. Execute the following command:

```
echo $(get_unit_id)
```

This returns the Unit ID of the device:

```
--- rescue shell tty11 ---
Press <RETURN> to login:
Loading "English(US)" keyboard layout.
root@ITC005056938D22:/# echo $(get_unit_id)
005056938D22 ←
```

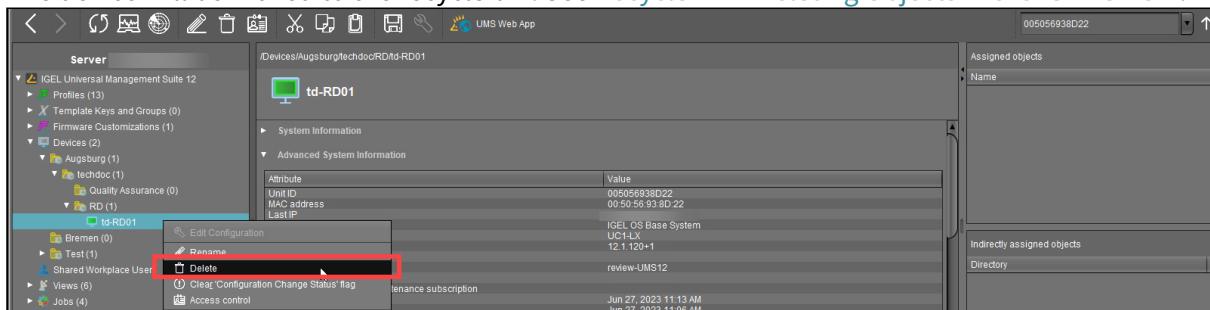
3. Enter the Unit ID in the **Search** field, press **[Enter]** and validate that the located device has the correct Unit ID.



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

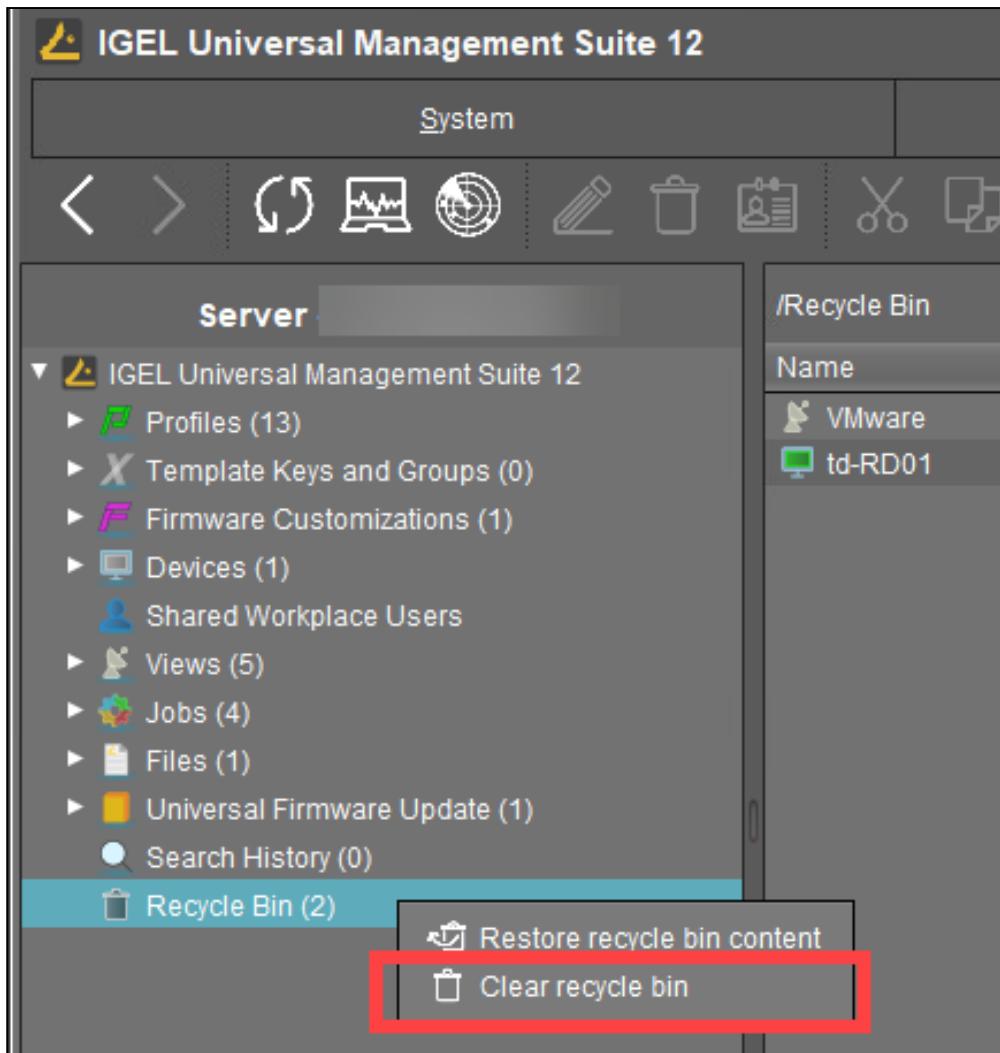
4. Right-click the device, select **Delete** and confirm the deletion.

The device will be moved to the recycle bin. See [Recycle Bin - Deleting Objects in the IGEL UMS](#)¹²⁷.



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

127. <https://kb.igel.com/en/universal-management-suite/current/recycle-bin-deleting-objects-in-the-igel-ums>



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.

- i 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 \(see page 58\)](#) 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 (see [Web Certificates in the IGEL UMS¹²⁸](#)).

- i** 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.dci3rsbtpeunizc5g5gghfhwg.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`.
As a best practice, only use lowercase letters in the **FQDN**.
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.

Attribute	Value
Process ID	b9edcf5-ac6f-4075-9d31-e22ae57e0f49
Cluster	UMS CLUSTER-39415-1637260546688-2-0
Version	12.01.11n
Host	UMS00
Last Known IP	192.168.1.10
Public Address	ums.
Device Communication Port	30000
Web Port	8443
Public Web Port	8443
Operating System	Ubuntu 22.04.2 LTS

2. Change the hostname:

- via your operating system

The proper way is to update the hostname of the UMS Server itself. To do this, simply follow your OS vendor's instructions for changing the hostname, and then reboot the server.

After that, you should see the changes reflected in the UMS (see step 1).

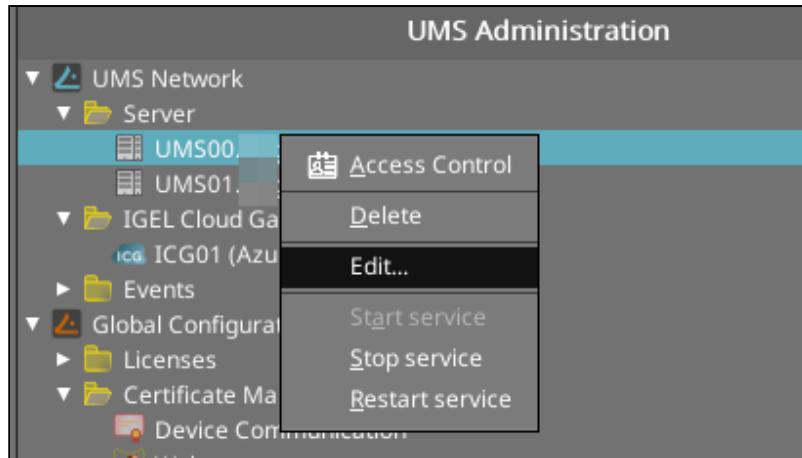
OR

- via the UMS

If changing the hostname of your server is not allowed, then you can change the **Display Name** and **Public Address** of your UMS Servers:

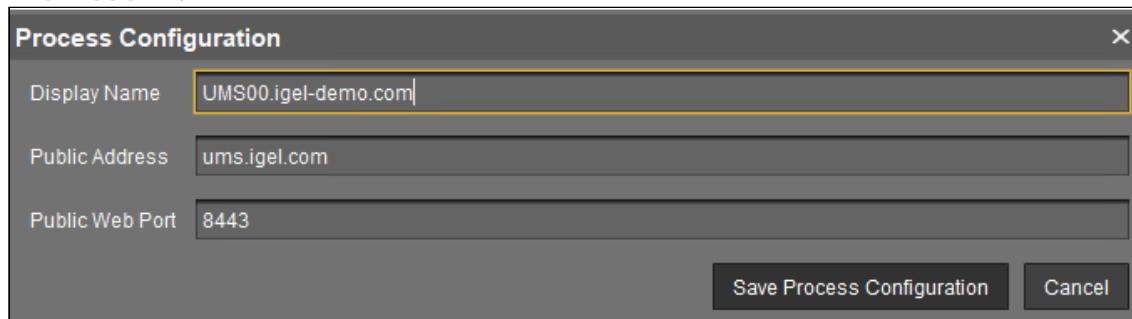
1. In the UMS Console, right-click the server under **UMS Console > UMS Administration > UMS Network > Server** and select **Edit**.

128. <https://kb.igel.com/en/universal-management-suite/current/web-certificates-in-the-igel-ums>



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](#)¹²⁹.



4. Restart the UMS Server service.

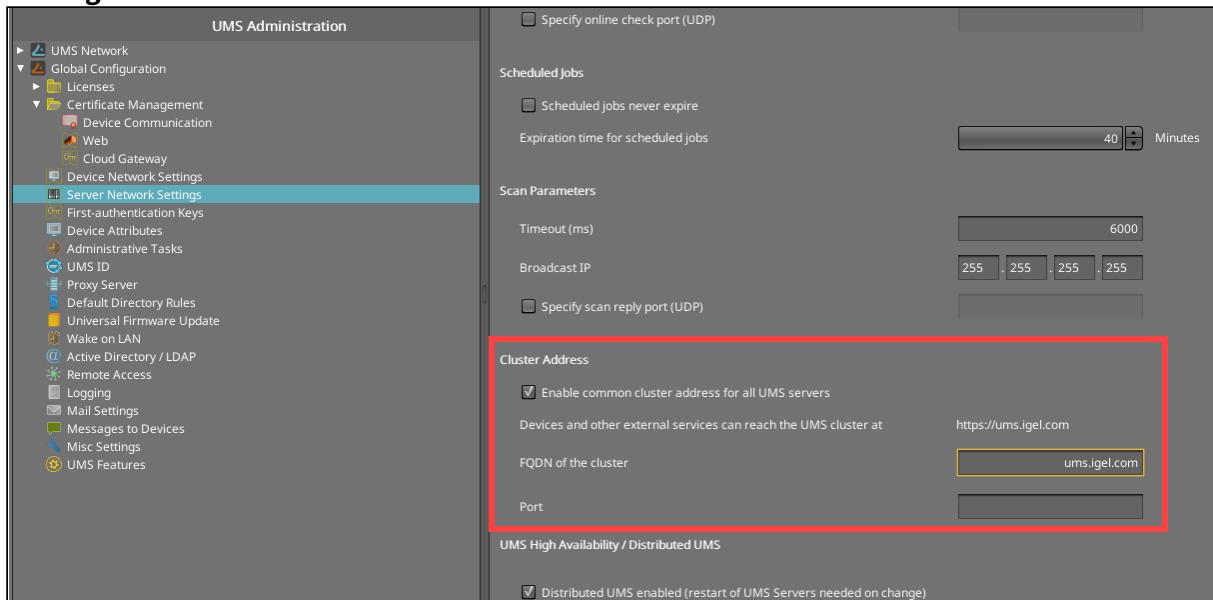
5. Validate that you can resolve the **Display Name** or **Public Address** of the UMS Server(s) from your IGEL OS devices.

129. <https://kb.igel.com/en/universal-management-suite/current/server-view-your-igel-ums-server-information>

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 UMS¹³⁰](#). 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 UMS¹³¹](#).
7. Restart the UMS Server service on all servers.

130. <https://kb.igel.com/en/universal-management-suite/current/server-network-settings-in-the-igel-ums>
 131. <https://kb.igel.com/en/universal-management-suite/current/server-network-settings-in-the-igel-ums>

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**:

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

i 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 55). 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 168).

How to Locally Install Apps

To install apps, proceed as follows:

1. Open the App Portal locally on the device.

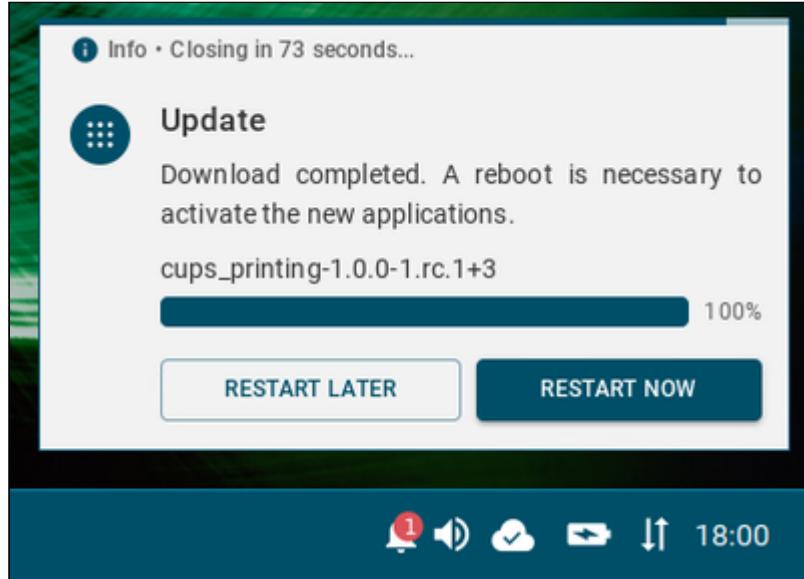


2. Select the required app and its version and click **Install**.

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

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

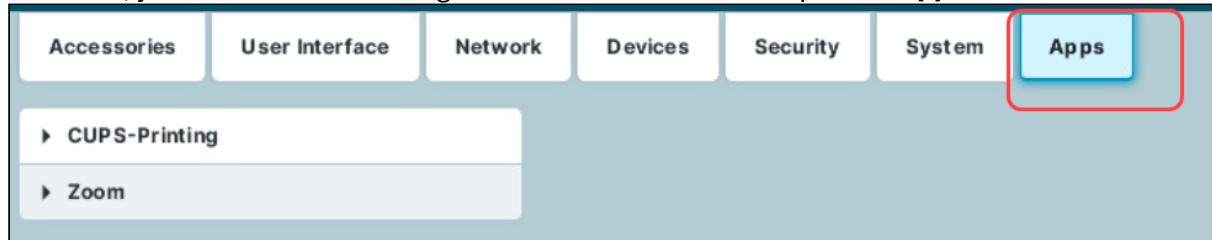
The selected app version will be downloaded to the device. The corresponding notification will be shown:



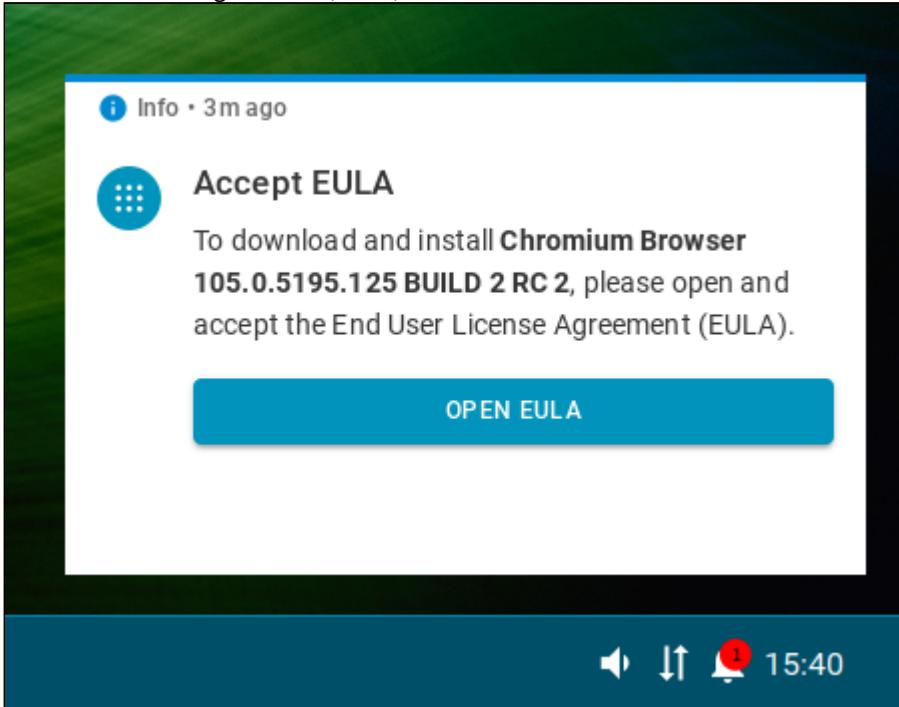
- Dependant apps and codecs (e.g. Chromium Multimedia Codec, Fluendo libva for Chromium, Citrix Multimedia Codec) are automatically installed on the device during the installation of the main app (e.g. Chromium Browser app, Citrix Workspace app).

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):



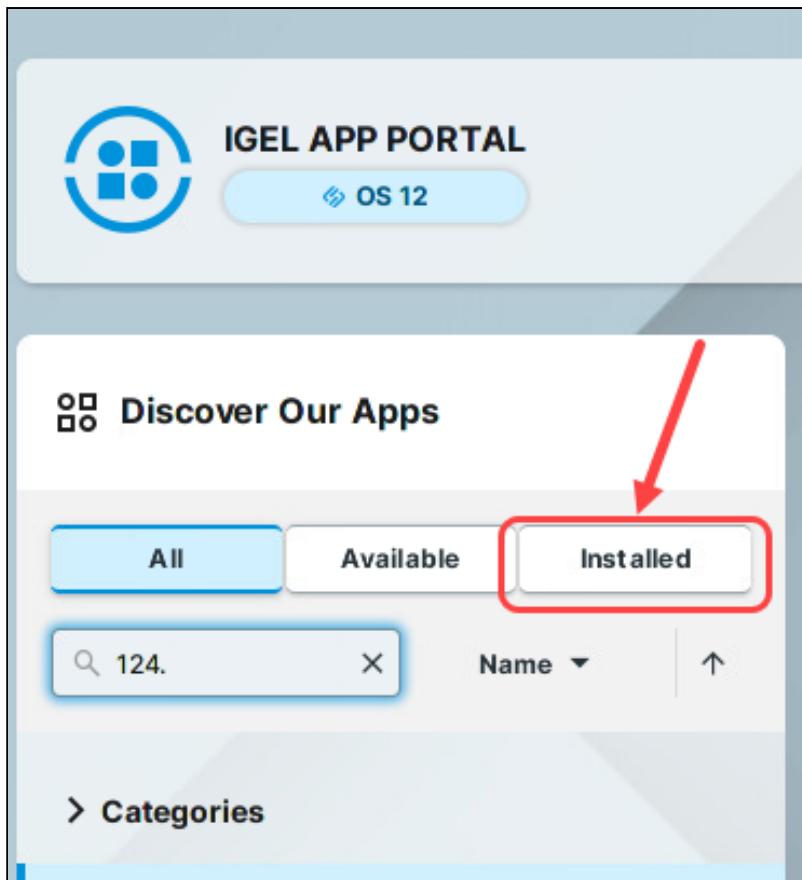
How to Locally Uninstall Apps

To uninstall apps on the device, proceed as follows:

1. Open the App Portal locally on the device.

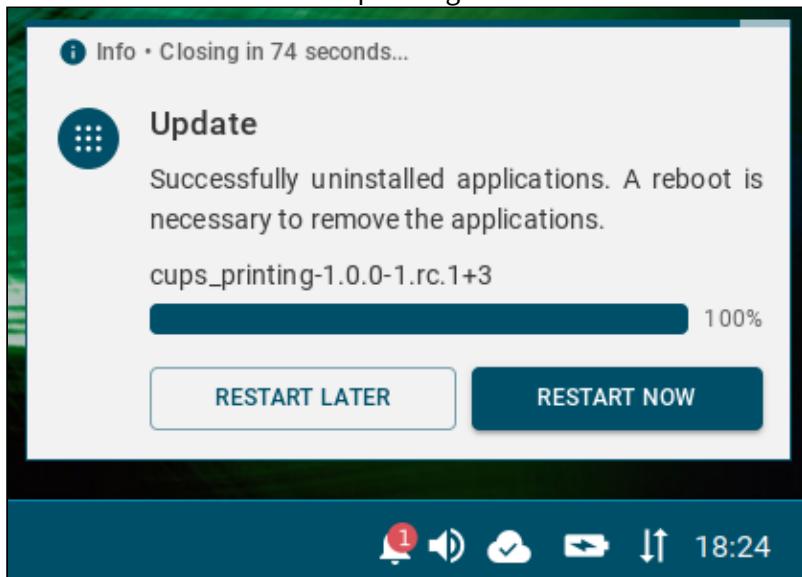


2. Filter for **Installed** apps and select the required app.



3. Click **Uninstall**.

The user will receive a corresponding notification:





4. Restart the device to complete the app uninstallation.

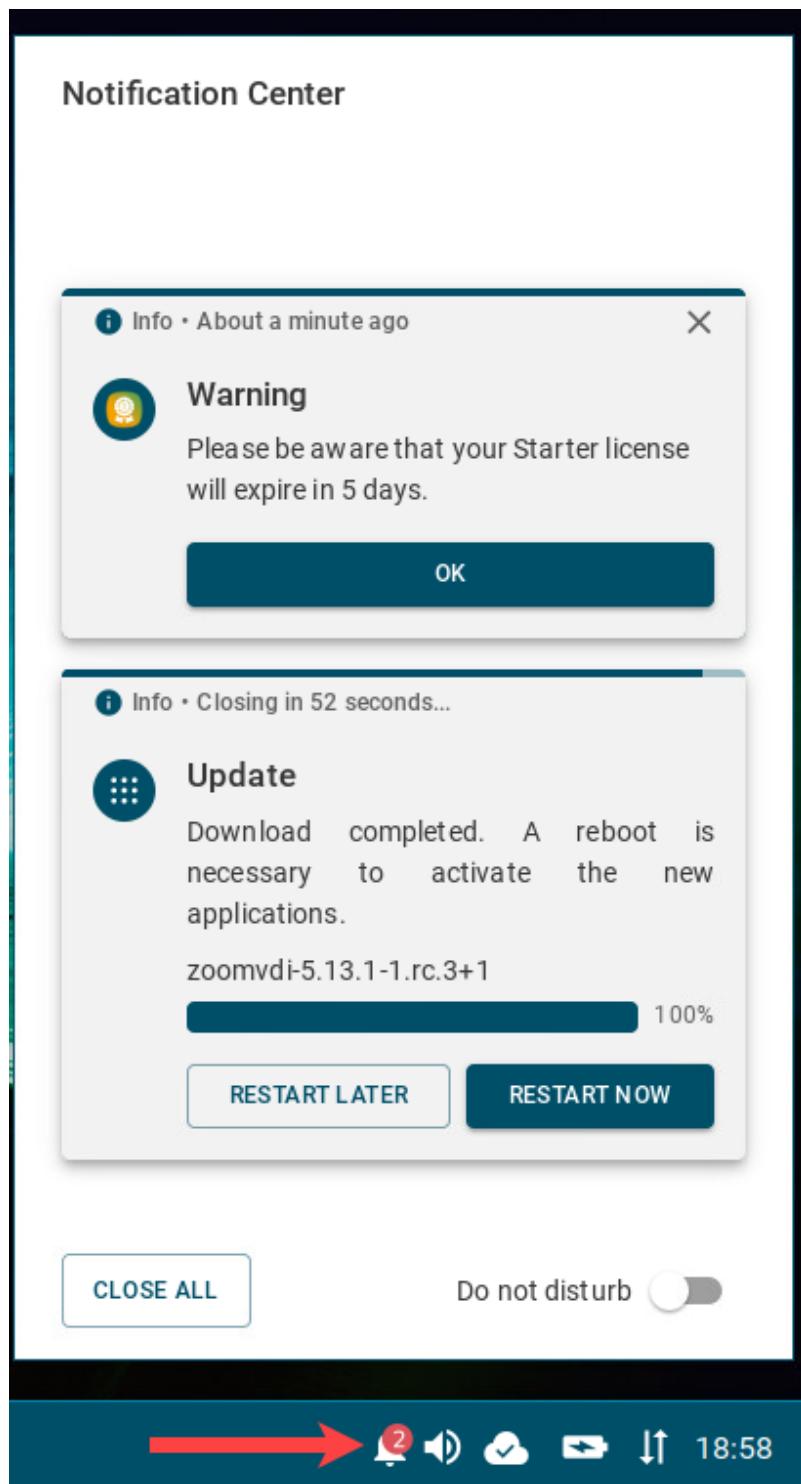
Configuring Single Sign-On (SSO)

For detailed information, see [How to Configure Single Sign-On \(SSO\) on IGEL OS 12¹³².](#)

132. <https://kb.igel.com/en/igel-os-base-system/current/how-to-configure-single-sign-on-sso-on-igel-os-12>

IGEL OS Notification Center

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



- Notification Center 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 update notifications, check the settings under **System > Update > Action after app activation**. See [Update - App Update Settings in IGEL OS 12](#)¹³³.

Note: The update notification is different if you have configured the background app update, see [How to Configure the Background App Update in the IGEL UMS Web App](#)¹³⁴.

- 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 137).
- 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

133. <https://kb.igel.com/en/igel-os-base-system/current/update-app-update-settings-in-igel-os-12>

134. <https://kb.igel.com/en/universal-management-suite/current/how-to-configure-the-background-app-update-in-the->

IGEL Insight Service



IGEL is working on a new version of the feature. To learn more about what is coming, see [IGEL Insights to Deliver Unified Endpoint Telemetry & Management Data¹³⁵](#).

IGEL Insight Service is activated by default after a Universal Management Suite (UMS) installation. After the installation, at the first start of the IGEL UMS Console or the UMS Web App, you are presented with a dialog with information on the IGEL Insight Service. If you want to deactivate the IGEL Insight Service, click **Go to Settings** and disable it under **Disable Insight Service**. If you close the dialog, IGEL Insight Service remains activated.



IGEL Insight Service can be activated or deactivated anytime under **UMS Console > UMS Administration > Global Configuration > UMS Features** or under **UMS Web App > Network > Settings > UMS Features**. The configuration of the IGEL Insight Service is preserved in case of an update installation.

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
- provide you with direct access to software and hardware insights, e.g. reports, based on your data

Legal basis for the data processing is IGEL's legitimate interest in accordance with Art. 6 (1) (f) General Data Protection Regulation (GDPR). It is IGEL's legitimate interest to pursue the above detailed purposes to improve its products and services, and to provide its customers with more secure, up-to-date, and optimized software as well as optimal customer support.

We do not share your data with third parties outside the IGEL group. Your data is stored on servers in the EU.

The identity of the individual IGEL OS device will only be stored pseudonymously. The data will be deleted after five years.

You can object to the processing by disabling the Insight Service functionality in your settings. By objecting you will not receive further recommendation based on your setup and you cannot be provided with access to software and hardware insights based on your data.

Data Collected by the IGEL Insight Service

- Company identifier
- UMS identifier
- Pseudonymized device identifier
- Name of the application
- Version of the application

135. <https://www.igel.com/blog/igel-insights-telemetry-and-data-management-platform/>

- Manufacturer of the device
- Model of the device
- CPU of the device
- RAM of the device
- Mainboard of the device
- GPU of the device
- 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)

Quick Start Configuration Profiles for Setting up Your IGEL Environment

IGEL provides you with preconfigured profiles for the IGEL Universal Management Suite (UMS) is designed to help you set up your IGEL environment. The profiles are organized into thematic packages: **IGEL OS**, **Citrix**, **Omnissa**, **Microsoft**, and **Local Apps**.

Disclaimer

The Quick Start Configuration profiles provided by IGEL are only intended as a template for setting up your UMS. It is very important to understand that they may not be suitable for every use case. While every effort has been made to ensure the accuracy and reliability of the profiles, they are provided "as is" without any warranties or guarantees of any kind. The implementation of the profiles provided by IGEL is at your own risk and the profiles are not a substitute for professional advice in the individual case.

Packages

IGEL OS

The **IGEL OS** profiles provide typical settings such as device shadowing, a local terminal, touchscreen configuration, security-related settings, and pre-defined language and timezone settings.

Citrix

The **Citrix** profiles provide the Citrix Workspace App (CWA), plugins for the Citrix Workspace App (CWA), and various configurations for your Citrix environment.

Omnissa

The **Omnissa** profiles provide the VMware Horizon client, plugins for the VMware Horizon client, and configurations for your Omnissa environment.

Microsoft

The Microsoft profiles provide the clients Microsoft Azure Virtual Desktop (AVD), IGEL Remote Desktop (IGEL's RDP client for an on-premise environment), IGEL Remote Desktop Web Access (IGEL's RDP client for a web-based environment), IGEL Windows 365 (IGEL's Windows 365 client), and the Zoom plugin for these clients.

Local Apps

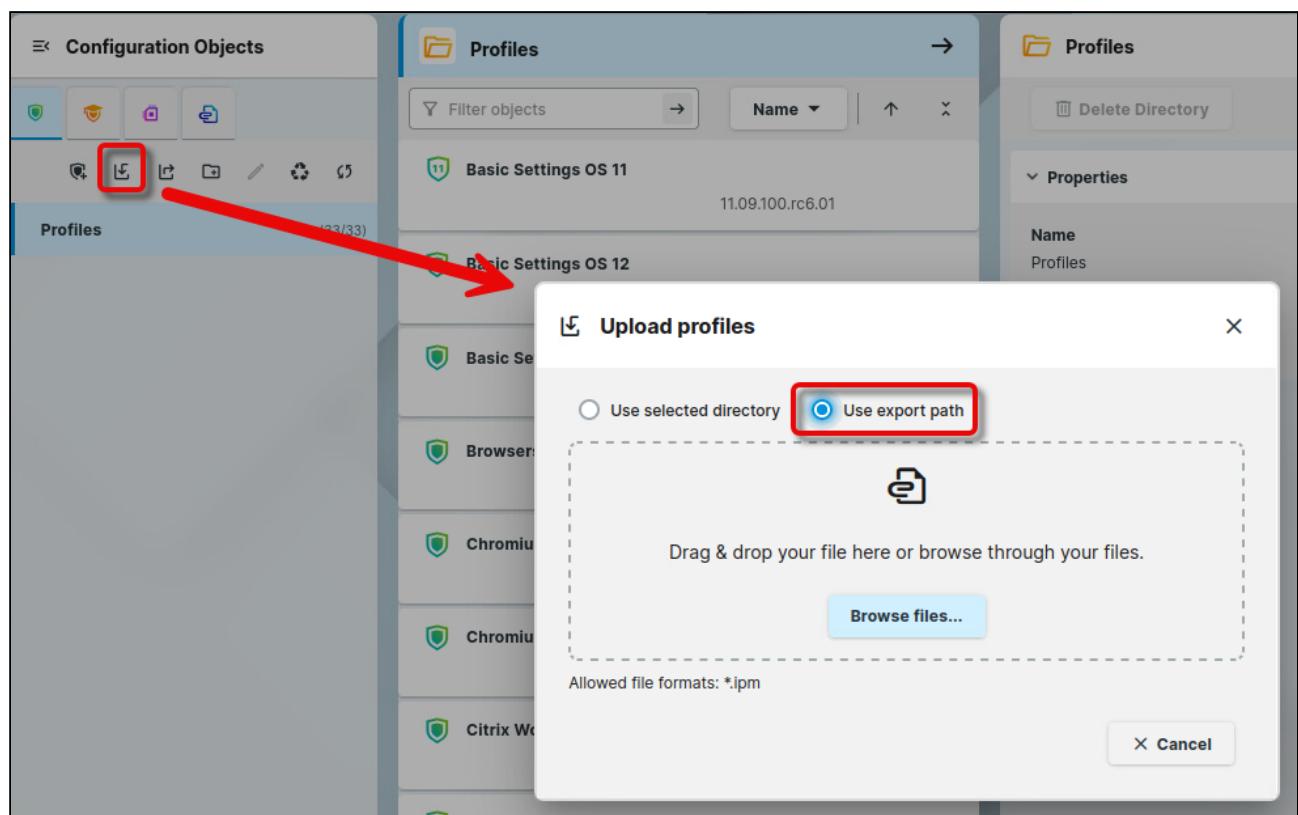
The **Local Apps** profiles provide the Media Player, the Zoom client, web browsers, and Microsoft Teams as Progressive Web App (PWA).

How to Import the Example Profiles into Your UMS

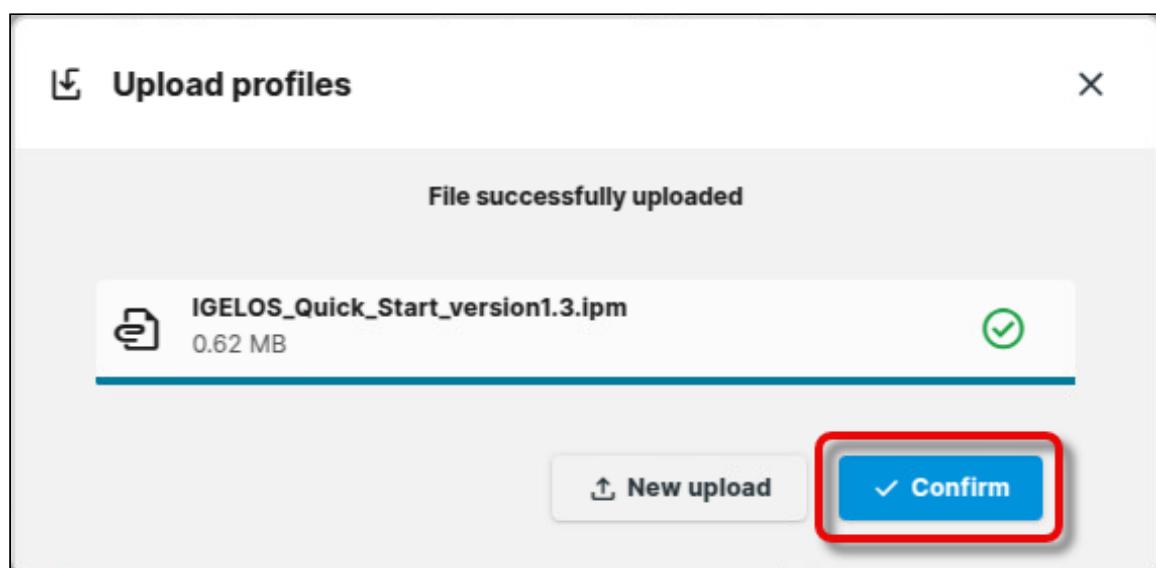
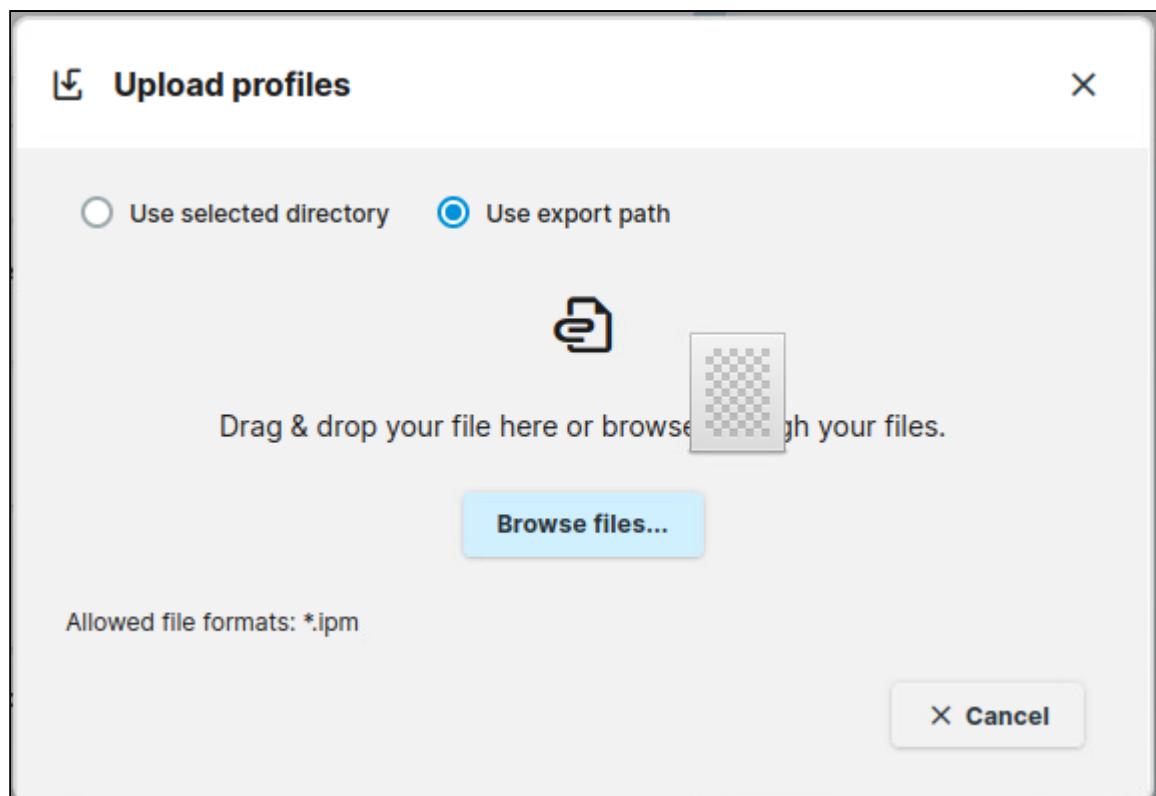
1. Download the relevant profile packages here:

- **IGEL OS:** IGELOS_Quick_Start_version1.3.ipm
- **Citrix:** Citrix_Quick_Start_version1.1.ipm
- **Omnissa:** Omnissa_Quick_Start_version1.1.ipm
- **Microsoft:** Microsoft_Quick_Start_version1.1.ipm
- **Local Apps:** LocalApps_Quick_Start_version1.1.ipm

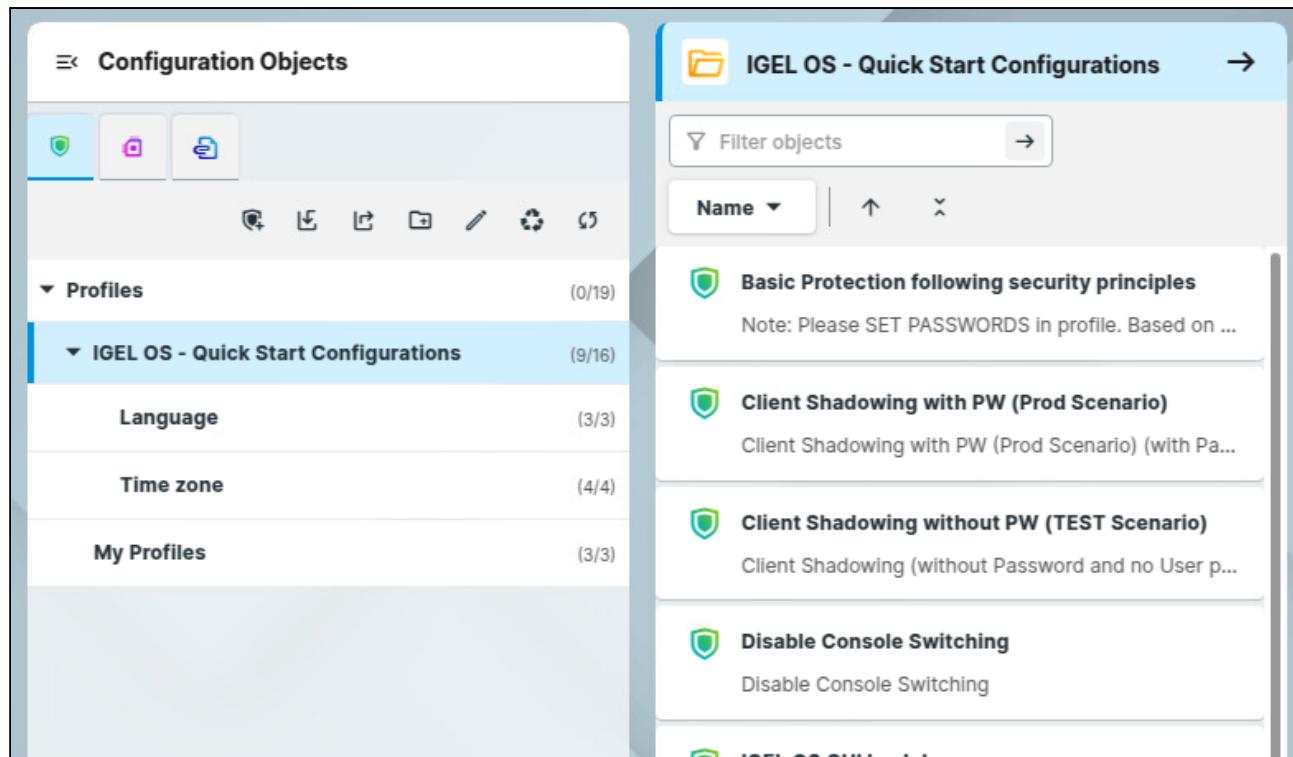
2. Click  and select **Use export path**. With this option, your profiles will be arranged in a folder structure.



3. Select the package file by Drag & Drop or with the file chooser and, when the package is processed, click **Confirm**.



The profiles are available in your UMS as a folder structure.



The screenshot shows the IGEL Management interface. On the left, the "Configuration Objects" screen displays a list of profiles, with "IGEL OS - Quick Start Configurations" selected. On the right, the "IGEL OS - Quick Start Configurations" screen lists several configuration profiles:

- Basic Protection following security principles**
Note: Please SET PASSWORDS in profile. Based on ...
- Client Shadowing with PW (Prod Scenario)**
Client Shadowing with PW (Prod Scenario) (with Pa...)
- Client Shadowing without PW (TEST Scenario)**
Client Shadowing (without Password and no User p...)
- Disable Console Switching**
Disable Console Switching

Debugging / How to Collect and Send Device Log Files to IGEL Support

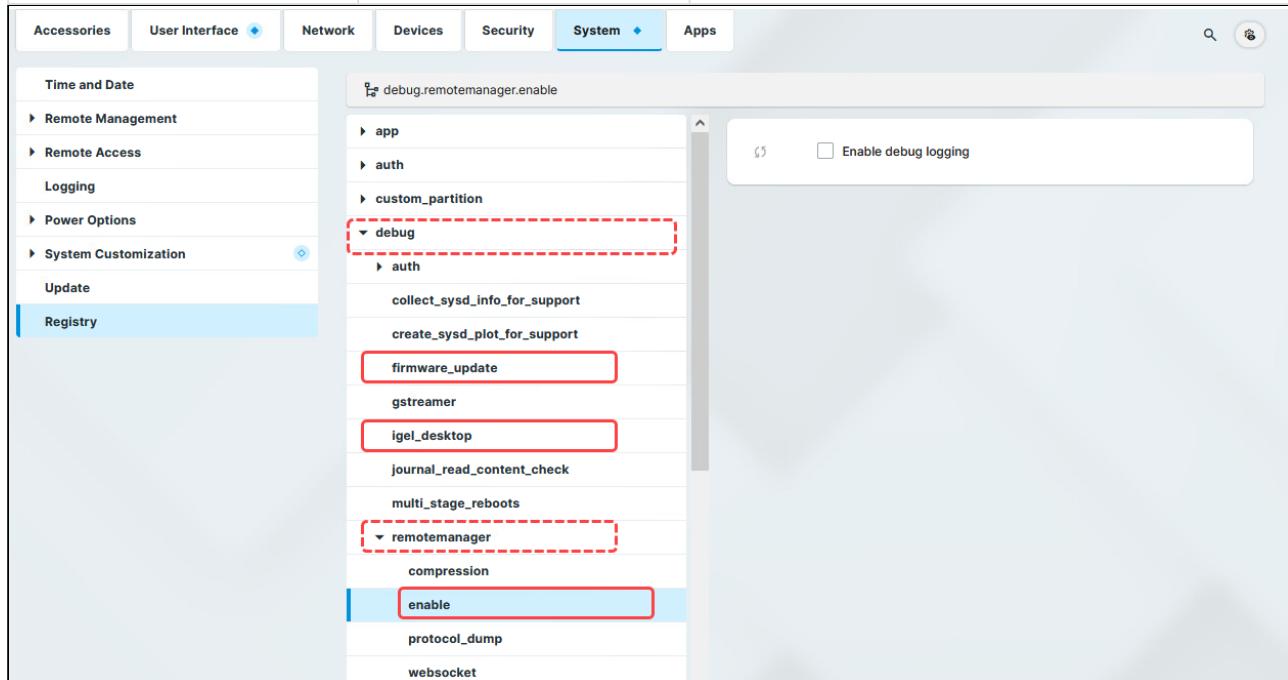
To collect the log files from the IGEL UMS Server, UMS Console, etc., you can use the Support Wizard: **UMS Console** > **Menu bar > Help > Save support information**. See [Support Wizard - How to Send Log Files in the IGEL UMS](#)¹³⁶. For more information on UMS log files, see [Where Can I Find the IGEL UMS Log Files?](#)¹³⁷.

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.remotemanag er.enable	Enable debug logging	Debug logging for RMagent communication
debug.igel_desktop p	Enable debug logging for IGEL desktop	Debug logging for user interface applications like the Setup Assistant and the Setup
debug.firmware_up date	Enable debug logging for firmware update	Debug logging for updates and installations of IGEL OS Apps



136. <https://kb.igel.com/en/universal-management-suite/current/support-wizard-how-to-send-log-files-in-the-igel-u>

137. <https://kb.igel.com/en/universal-management-suite/current/where-can-i-find-the-igel-ums-log-files>

4. Save the setting.

- i** 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 IGEL UMS

After you have activated the above registry keys, you can use the UMS Console or the UMS Web App to collect the device log files.

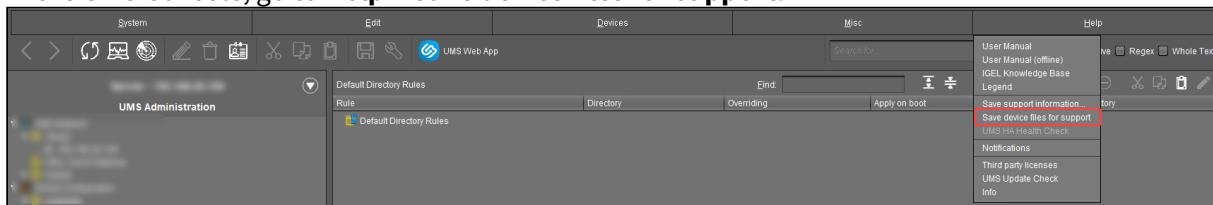
Collecting Device Logs from the IGEL UMS Web App

To collect the device log files, see the instructions under [How to Save Support Information and Log Files in the IGEL UMS Web App](#)¹³⁸.

Collecting Device Logs from the IGEL UMS Console

To collect the device log files:

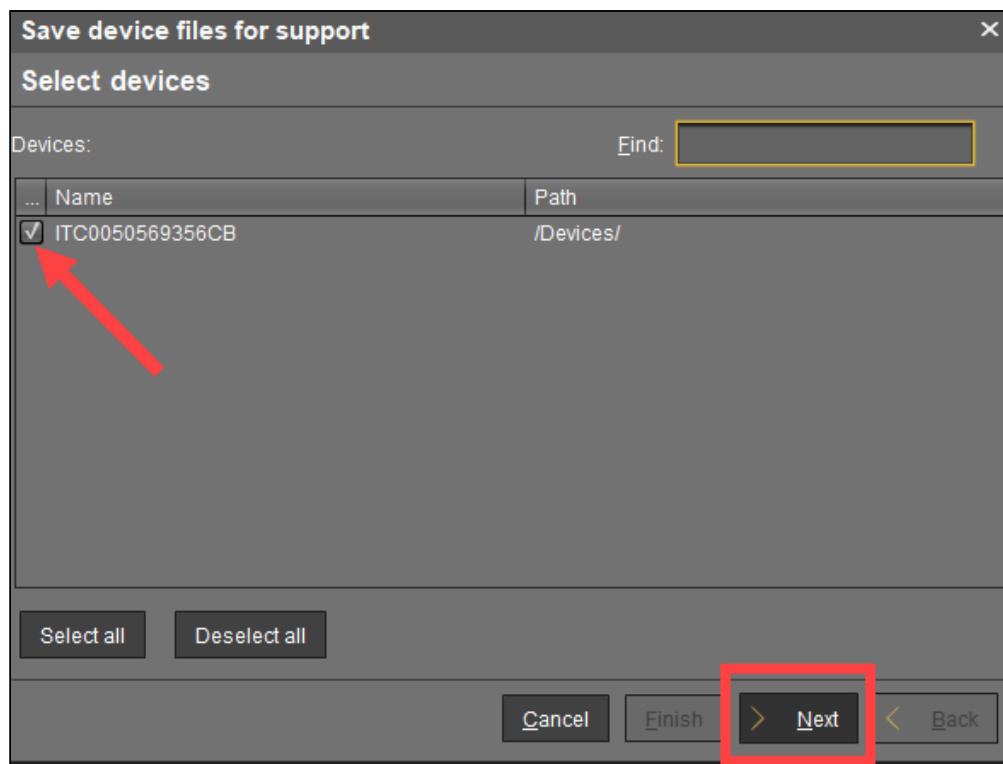
1. In the UMS Console, go to **Help > Save device files for support**.



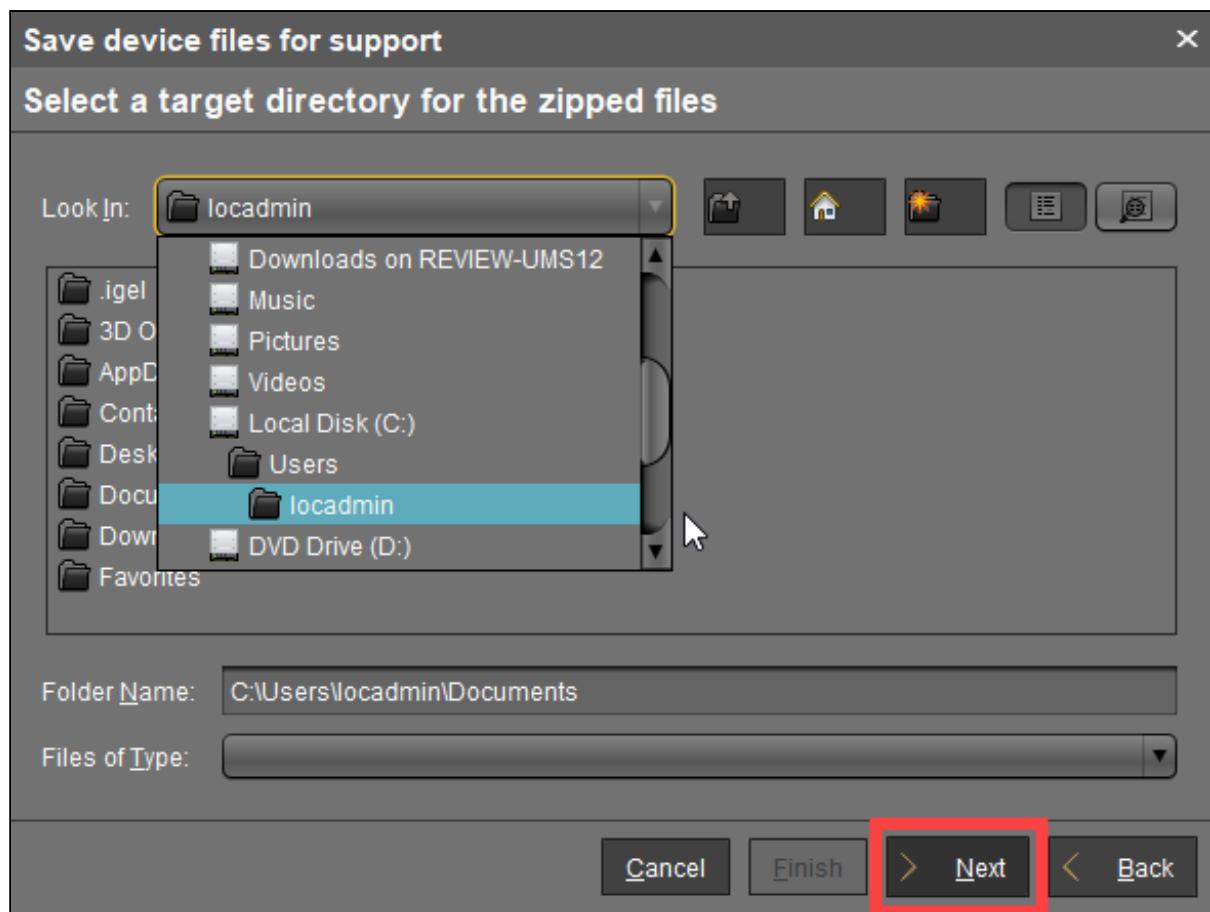
The dialog **Save device files for support** opens.

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

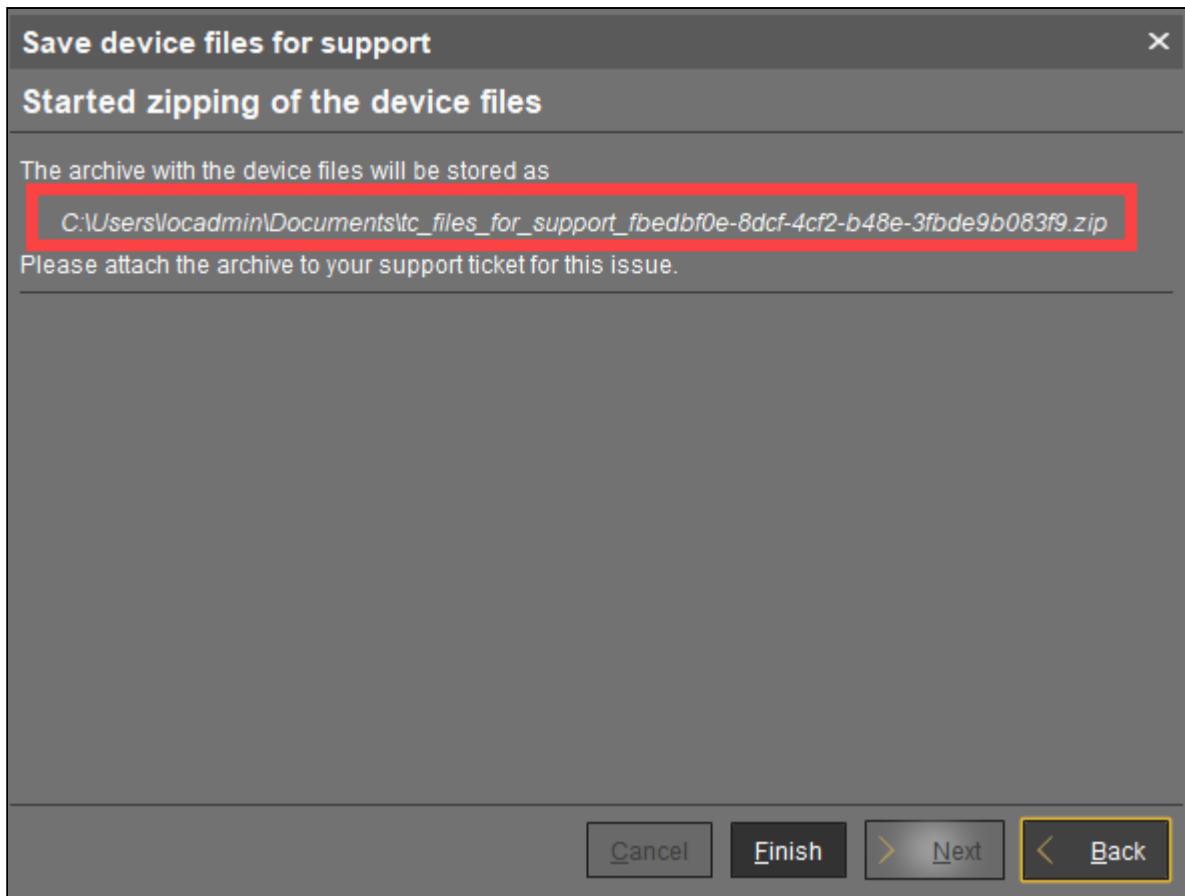
¹³⁸. <https://kb.igel.com/en/universal-management-suite/current/how-to-save-support-information-and-log-files-in-t>



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
¹³⁹IGEL Support via the [IGEL Customer Portal](#)¹⁴⁰.

Collecting Device Logs without the UMS

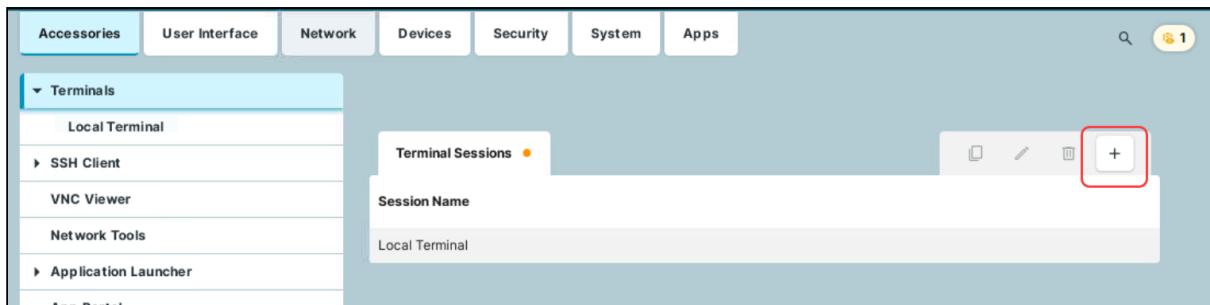
When the UMS is not accessible or there is an issue with network connectivity, you can still extract logs from a device.

Option 1: Via Local Terminal

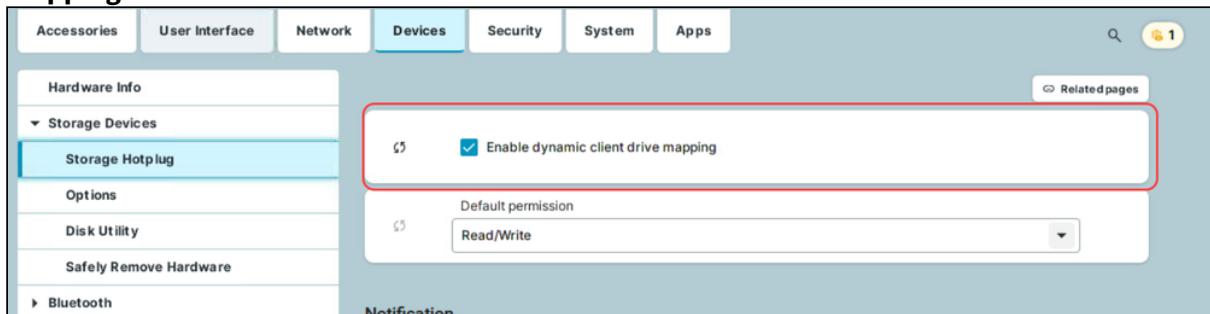
1. In the IGEL Setup, go to **Accessories > Terminals** and create a terminal session.

139. mailto:eap@igel.com

140. <https://support.igel.com/>



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`)

Local Terminal

```
login as "user" or "root": root
root@ITC00E0C561FAF7:~# /config/bin/create_support_information
root@ITC00E0C561FAF7:~# ls -l
total 16
drwxr-xr-x 6 user users 16384 Jan 1 1970 'NEW VOLUME'
```

- To find out the name of the USB stick, you can use the following commands:

```
cd /userhome/media
ls -l
```

Local Terminal

```
login as "user" or "root": root
root@ITC00E0C561FAF7:~# cd /userhome/media
root@ITC00E0C561FAF7:/userhome/media# ls -l
total 16
drwxr-xr-x 6 user users 16384 Jan 1 1970 'NEW VOLUME'
```

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.

- 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].

- After `/media/`, you can press the tab key for autocompletion.

- Type `sync` and press [Return].

Local Terminal

```
updating: /tmp/tclogs.zip/base System/audio/dtsa_info.txt (depreciated)
root@ITC00E0C561FAF7:~# cp /tmp/tclogs.zip /media/"NEW VOLUME"/
root@ITC00E0C561FAF7:~# sync
root@ITC00E0C561FAF7:~#
```

- Wait a few seconds before safely ejecting the USB stick from the endpoint device.

12. Send the log files to [IGEL Support](mailto:eap@igel.com) via the [IGEL Customer Portal](https://support.igel.com/)¹⁴².

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 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`

141. <mailto:eap@igel.com>

142. <https://support.igel.com/>

```

251.6161431 usb 4-2: SerialNumber: 2080520160140023
251.6236471 usb-storage 4-2:1.0: USB Mass Storage device detected
251.6239151 scsi host2: usb-storage 4-2:1.0
253.1971291 scsi 2:0:0:0: Direct-Access      ADATA      USB Flash Drive  1100 PQ: 0 ANSI: 6
253.1976341 sd 2:0:0:0: Attached scsi generic sg1 type 0
253.1982711 sd 2:0:0:0: [sdb] 60620800 512-byte logical blocks: (31.0 GB/28.9 GiB)
253.1986191 sd 2:0:0:0: [sdb] Write Protect is off
253.1986251 sd 2:0:0:0: [sdb] Mode Sense: 43 00 00 00
253.1987631 sd 2:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
253.2032381 sdb: sdb1 ←
253.2040151 sd 2:0:0:0: [sdb] Attached SCSI removable disk
root@ITC00E0C51A75F4:~# cat /proc/partitions
major minor #blocks name
          8      0   3917592 sda
          8      1   3852056 sda1
          8      2    30720 sda2
          8      3    30720 sda3
         61      0   3852056 igf0
         61      1    697588 igf1
         61     23     3364 igf23
         61     26    22088 igf26
         61     39     7744 igf39
         61     55     3688 igf55
         61     60    325000 igf60
         61     66    12668 igf66
         61     68     876 igf68
         61    239    524288 igf239
         61    254     5128 igf254
         61    255    24576 igf255
        253      0    24576 dm-0
        253      1    524288 dm-1
        252      0    555956 zram0
        252      1    555956 zram1
        252      2    555956 zram2
        252      3    555956 zram3
          8     16   30310400 sdb
          8     17   30310160 sdb1 ←
root@ITC00E0C51A75F4:~# mkdir /mnt
root@ITC00E0C51A75F4:~# mount /dev/sdb1 /mnt
root@ITC00E0C51A75F4:~#

```

8. Check your data on your mounted USB stick:

```
cd /mnt
```

```
ls -l
```

Now you should see your data on the USB stick.

9. Generate log files: /config/bin/create_support_information

It can take some time till the log file generation is complete.

10. Type:

```
cd /tmp
```

```
ls -l
```

Now you should see the log file `tclogs.zip` listed.

```

adding: /tmp/logfiles/base/system/audio/d1sd_mru.txt (dereferenced 0x7)
root@ITC00E0C51A75F4:/mnt# cd /tmp
root@ITC00E0C51A75F4:/tmp# ls -l
total 984
prw-r----- 1 user users      0 Jul  7 12:46 fifomngr2tray
prw-r----- 1 user users      0 Jul  7 12:46 fifotray2mgr
drwxr-xr-x  3 root root     60 Jul  7 12:58 logfiles
-rw-r--r--  1 user users      0 Jul  7 12:46 mbblog
drwxr--r--  2 root root     40 Jul  7 12:45 pulse-PKdhtXMr18n
-rw-r--r--  1 root root      0 Jul  7 12:45 setupd.files
drwxr--r--  3 root root     60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-chrony.service-87Nbfg
drwxr--r--  3 root root     60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-earlyoom.service-xifpch
drwxr--r--  3 root root     60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-ModemManager.service-CHYnHf
drwxr--r--  3 root root     60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-systemd-logind.service-mUP8Kh
drwxr--r--  3 root root     60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-upower.service-mCALhh
-rw-r--r--  1 root root  950247 Jul  7 13:00 tclogs.zip
drwxrwxrwt  2 root root    40 Jul  7 12:45 QMaarcDm
-rw-r--r--  1 root root      74 Jul  7 12:46 wfs_stats
-rw-r--r--  1 root root   50351 Jul  7 12:58 xorg-debug.log
root@ITC00E0C51A75F4:/tmp# cp /tmp/tclogs.zip /mnt
root@ITC00E0C51A75F4:/tmp# umount /mnt

```

11. To copy `tclogs.zip` from your endpoint device to the USB stick, type `cp /tmp/tclogs.zip /mnt` and press [Return].

12. To unmount your USB stick, use the command `umount /mnt`

13. Now you can safely remove your USB stick.

14. To close CLI, press [CTRL+ALT+F1].

15. Send `tclogs.zip` to IGEL Support via the [IGEL Customer Portal](#)¹⁴³.

143. <https://support.igel.com/>