



## How to Start with IGEL COSMOS



IGEL COSMOS is a platform which has fully separated the IGEL OS operating system and IGEL OS Apps. With the modular principle introduced with IGEL OS 12, you can install and update single applications like Citrix, Chromium browser, etc. individually and independently from the IGEL OS base system.

IGEL COSMOS comprises:

- IGEL Universal Management Suite (UMS) 12 for managing IGEL OS 12 and IGEL OS 11 devices. IGEL UMS 12 is a prerequisite for accessing all IGEL COSMOS Cloud Services.
- IGEL OS
- Various cloud-based services, for example:
  - [IGEL Customer Portal](#)(see page 4) which is a doorway to the IGEL product-related services. Here, you register your company account and use it to invite other [users and assign them specific roles](#)(see page 7), e.g. for opening support cases. In the IGEL Customer Portal, you can



also raise and view support requests, make necessary configurations for IGEL Onboarding Service, etc.

- [IGEL App Portal](#)(see page 73) where you can find all applications currently available for IGEL OS 12
- [IGEL Onboarding Service](#)(see page 39) which, if configured, allows your users to easily onboard IGEL OS 12 devices using only their corporate email
- [IGEL Insight Service](#)(see page 170) which collects analytical and usage data to improve IGEL products and services and provide a better customer experience
- [IGEL License Portal](#)(see page 119) where you can manage licenses for your IGEL OS devices

Please read this guide fully, without skipping any steps.

- ⓘ For more information on IGEL COSMOS, you can also use IGEL Academy courses, e.g. [Introducing IGEL COSMOS](#)<sup>1</sup>, and [IGEL Community](#)<sup>2</sup>.

---

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



## Registering for the IGEL Customer Portal

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

- ⓘ If you have already registered for the IGEL Customer Portal, you can use your existing account. If you forgot your password, click **Login > Forgot Password?** The password change is done in three steps: **Identify, Verify, Reset**.
- **Identify:** Enter your username that you used to register with IGEL.
  - **Verify:** Enter your email address to which the verification email should be sent. After that, check your email inbox and confirm it with the corresponding link. If you have not received the email, please check your spam folder.
  - **Reset:** Set a new password in the **Reset Password** dialog, which opens in your default browser.

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

To register for the IGEL Customer Portal:

1. Open [IGEL Customer Portal<sup>3</sup>](https://cosmos.igel.com/) and click **Register** in the upper right corner of the menu bar:

A screenshot of the IGEL COSMOS website. At the top, there's a dark header with the IGEL logo, the text "IGEL COSMOS Cloud Services", and a navigation bar with links for "Catalog", "Knowledge", "Register" (which has a red arrow pointing to it), and "Login". Below the header is a banner with a night-time cityscape background and the text "Welcome to IGEL COSMOS!". A search bar with the placeholder "Insert your question here" is positioned below the banner. In the center, there's a blue callout box containing text: "Dear Customers, Welcome to the IGEL COSMOS. If you don't already have an account please register [here](#). If you have any questions or need more information, please visit our [Knowledge Base](#)." At the bottom, there are three tabs: "Services" (with "Customer Support Packages" as a sub-item), "Software" (with "Software Downloads" as a sub-item), and "Hardware" (with "Declare UDC destruction" as a sub-item).

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

<sup>3</sup> <https://cosmos.igel.com/>



## 2. Enter your user data:

\* Indicates required

<b>Company Information</b>		<b>ADDRESS</b>	<b>Submit</b>
<b>* COMPANY NAME</b>	<input type="text"/>	<input type="text"/>	
ADDRESS 2	<input type="text"/>	ADDRESS 3	
<b>* CITY</b>	<input type="text"/>	<b>* COUNTRY</b>	-- None --
<b>* POST CODE</b>	<input type="text"/> Please write N/A if no zip code is available	<b>* STATE/PROVINCE</b>	<input type="text"/>
INDUSTRY	<input type="text"/> -- None --		
<b>Personal Information</b>			
<b>* LOGIN-EMAIL</b>	<input type="text"/>		
<b>* FIRST NAME</b>	<b>* LAST NAME</b>	<b>Required information</b>	
<input type="text"/>	<input type="text"/>	COMPANY NAME	ADDRESS
<b>* WORK PHONE</b>	<b>* CHOOSE YOUR PREFERRED LANGUAGE</b>	CITY	COUNTRY
<input type="text"/> Please use following format +1234567890	<input type="text"/> -- None --	POST CODE	WORK PHONE
<input type="checkbox"/> 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. <input type="checkbox"/> * I HAVE READ AND ACCEPT THE IGEL CLOUD SERVICES TERMS AND CONDITIONS <small>IGEL Cloud Services Terms &amp; Conditions can be found <a href="#">here</a></small> <small>You can find the Privacy Policy <a href="#">here</a></small>			

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

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

### **i** IGEL Company Account Requirements

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

## 3. Click **Submit**.

You will now be sent a confirmation email.

## 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 and released.

The approval of your registration will be confirmed by email. In this email, you will find the link to the IGEL Customer Portal and an initial password (one-time password).

5. Open the IGEL Customer Portal via the link and click **Login** in the upper right corner of the menu bar.
6. Enter your **Username** and your initial **Password** (one-time password).  
The **Change Password** dialog box will open:

**Change Password**

test2@test.com

**Current Password:**

**New password:**

**Confirm New Password:**

**Submit**

7. Enter your **Current Password** and your **New Password** according to the requirements.

8. Confirm the new password by clicking **Submit**.

The IGEL Customer Portal will open, and you will be logged in.

**(i)** Please remember your login data or store them in a safe place. These credentials are Super Admin credentials, with which you can invite new users and assign them specific roles, see [Managing Users and Roles in the IGEL Customer Portal](#)(see page 7).



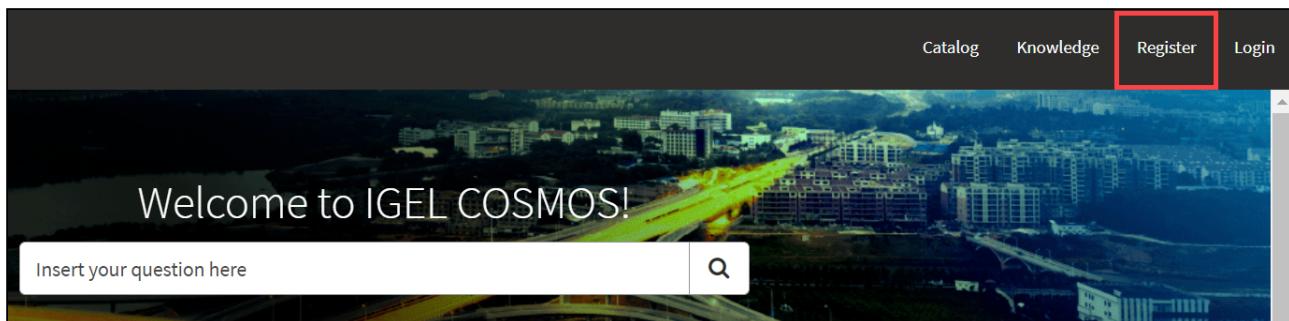
## Managing Users and Roles in the IGEL Customer Portal

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

#### Super Admin

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



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

The Super Admin has the following permissions:

	<b>Invite</b>	<b>Deactivate</b>	<b>Register</b>	<b>Change / Add / Revise</b>	<b>View</b>	<b>Assign Roles</b>	<b>Use</b>
<b>Users</b>	yes	yes	n/a, users are invited	yes	yes	yes	n/a
<b>Account</b>	n/a	n/a	n/a; account registration to follow the existing process	yes	yes	n/a	yes
<b>UMS Instances</b>	n/a	yes	yes	yes	yes	n/a	yes
<b>EST Instances</b>	n/a	yes	yes	yes	yes	n/a	yes

<sup>4</sup> <https://cosmos.igel.com/>



<b>IdP OBS</b>	n/a	yes	yes	yes	yes	yes	n/a	yes
<b>App Portal</b>	n/a	yes	n/a	n/a	yes	yes	n/a	yes (Azure)
<b>OBS</b>	n/a	n/a	n/a	n/a	n/a	n/a	n/a	yes
<b>Customer Support</b>	yes	yes	n/a, users are invited	n/a	yes	n/a	n/a	yes

## Account Admin

The Account Admin has the following permissions:

	<b>Invite</b>	<b>Deactivate</b>	<b>Create/ Register</b>	<b>Change / Add / Revise</b>	<b>View</b>	<b>Assign Roles</b>	<b>Use</b>
<b>Users</b>	yes	n/a	n/a; users are invited	yes	yes	yes	n/a
<b>Account</b>	n/a	n/a	n/a	n/a	yes	n/a	n/a
<b>UMS Instances</b>	n/a	n/a	no	no	no	n/a	no
<b>EST Instances</b>	n/a	n/a	no	no	no	n/a	no
<b>IdP OBS</b>	n/a	n/a	no	no	no	n/a	no
<b>App Portal</b>	n/a	n/a	n/a	n/a	no	n/a	no
<b>OBS</b>	n/a	n/a	n/a	n/a	no	n/a	no

## OBS Admin

The OBS Admin has the following permissions:

	<b>Invite</b>	<b>Deactivate</b>	<b>Create</b>	<b>Change / Add</b>	<b>View</b>	<b>Assign Roles</b>	<b>Use</b>
<b>Users</b>	no	n/a	no	no	no	no	n/a
<b>Account</b>	n/a	n/a	no	no	yes	n/a	n/a
<b>UMS Instances</b>	n/a	n/a	no	no	no	n/a	yes
<b>EST Attributes</b>	n/a	n/a	yes	yes	yes	n/a	yes
<b>IdP (OBS)</b>	n/a	n/a	no	no	no	n/a	no
<b>App Portal</b>	n/a	n/a	n/a	n/a	n/a	n/a	no



## UMS Admin

The UMS Admin has the following permissions:

	<b>Invite</b>	<b>Deactivate</b>	<b>Create</b>	<b>Change / Add</b>	<b>View</b>	<b>Assign Roles</b>	<b>Use</b>
<b>Users</b>	no	n/a	no	no	no	no	n/a
<b>Account</b>	n/a	n/a	no	no	yes	n/a	n/a
<b>UMS Instances</b>	n/a	n/a	yes	yes	yes	n/a	yes
<b>EST Attributes</b>	n/a	n/a	no	no	no	n/a	no
<b>IdP (OBS)</b>	n/a	n/a	no	no	no	n/a	no
<b>App Portal</b>	n/a	n/a	n/a	n/a	n/a	n/a	no
<b>OBS</b>	n/a	n/a	n/a	n/a	n/a	no	no

## Customer Support Account Manager

The Customer Support Account Manager has the following permissions:

- Raise & View Support Cases
- Submit RMA Cases
- Submit Reset Key Cases
- Submit License Question Cases

## Inviting a User and Assigning a Role

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

1. Open [IGEL Customer Portal](https://cosmos.igel.com/)<sup>5</sup>, log in to your admin account, and select **Users > User & Role Administration**.

The screenshot shows the top navigation bar of the IGEL Customer Portal. The 'Users' dropdown menu is open, revealing options like 'Overview', 'User & Role Administration' (which is highlighted with a red box and an arrow pointing to it), 'Bring your IdP', 'IGEL OS IdP', and 'My Profile'. The rest of the page includes a 'Welcome to IGEL' banner, a search bar, and other navigation links.

<sup>5</sup> <https://cosmos.igel.com/>



## 2. Select **Invite new user**.

The screenshot shows the 'User & Role Administration' page. At the top left, there is a note: '\* Indicates required'. Below it, a dropdown menu is open with the placeholder '\* Please choose'. The option 'Invite new User' is highlighted with a red rectangle. To the right, there is a 'Submit' button and a note: 'Required information Please choose'.

## 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

The screenshot shows the 'User & Role Administration' page. A red rectangle highlights a group of input fields: 'First Name' (value: 'Ike'), 'Last Name' (value: 'Igel'), '\* E-Mail' (value: '@igel.com'), and 'Language' (value: 'English'). Above these fields, the 'Invite new User' option from the previous step is still visible in the dropdown menu. To the right, there is a 'Submit' button.



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

The screenshot shows the 'User & Role Administration' page. The 'Role' dropdown menu is open, and the option 'OBS Admin' is selected and highlighted with a red box. The 'Submit' button at the bottom right of the form is also highlighted with a red box.

The invitation mail is sent to the user.

The list of users is displayed; it includes the newly added user.

The screenshot shows a table titled 'Users' with columns: Account, Email, Role, Active, and Invitation Status. The table lists several accounts, including one with the email '@igel.com' and role 'OBS Admin', which is highlighted with a red box. The 'Invitation Status' for this account is 'Pending'.

All > Account =	Test Company	Account	Email	Role	Active	Invitation Status
		[Redacted]	@igel.com	OBS Admin	Pending	Pending
		[Redacted]	@igel.com	UMS Admin	Pending	Pending
		[Redacted]	i@igel.com	OBS Admin	Pending	Pending
		[Redacted]				
		[Redacted]				
		[Redacted]				
		[Redacted]	@temp.mailbox.org	App Portal User	Pending	Pending
		[Redacted]	i@igel.com	App Portal User	Yes	Accepted
		[Redacted]				

When the user accepts the invitation, the account is created, and the role is assigned. (If the user declines, the account is not created.)

The Super Admin receives a confirmation e-mail.



## Canceling and Resending Invitations

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

- Super Admin
- Account Admin

**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 [IGEL Customer Portal](#)<sup>6</sup>, log in to your admin account, and select **Users > Overview**.

The screenshot shows the top navigation bar of the IGEL Customer Portal. The 'Users' dropdown menu is open, and the 'Overview' option is highlighted with a red box. Other options in the dropdown include 'User & Role Administration', 'Bring your IdP', 'IGEL OS IdP', and 'My Profile'. Below the navigation bar, there's a search bar with the placeholder 'Insert your question here' and a cityscape background image.

The users are listed.

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

The screenshot shows the 'Users' overview page. The table lists four users from 'QAS Test Company' with their email addresses and status. In the 'Action' column for each user, there are two buttons: 'Resend' and 'Cancel', both of which are highlighted with a red box.

Account	Email	Role	Active	Invitation Status	Action
QAS Test Company	@igel.com	App Portal User	Pending	Pending	<b>Resend</b> <b>Cancel</b>
QAS Test Company	i@igel.com	App Portal User	Yes	Accepted	
QAS Test Company		App Portal User	Yes	Accepted	
QAS Test Company	t@igel.com	App Portal User	Yes	Accepted	

## Adding a Role to an Existing User

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

<sup>6</sup> <https://cosmos.igel.com/>  
<sup>7</sup> <https://cosmos.igel.com/>



The screenshot shows the IGEL Customer Portal homepage. At the top, there is a navigation bar with links: Catalog, Knowledge, My History & My Requests, Advanced Service, Users (with a dropdown arrow), Configure Services, My Company Subscriptions, and Tours. A red box highlights the 'User & Role Administration' option under the 'Users' dropdown menu.

## 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 heading 'User & Role Administration' and a sub-section 'User & Role Administration'. It contains a dropdown labeled 'Please choose' with options: '-- None --' and 'Add additional role'. A red box highlights the 'Add additional role' button. On the right side, there is a 'Submit' button and a 'Required information' section with a 'Please choose' button.

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

The screenshot shows the 'User & Role Administration' page. It has a similar structure to the previous screenshot, with a breadcrumb, search bar, and main section. The 'User & Role Administration' sub-section includes a dropdown 'Please choose' with 'Add additional role' selected, and a list box for selecting users with a red box highlighting it. The right side features a 'Submit' button and a 'Required information' section with a 'Please select all users you want to assign an additional role to' button.



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  
x

Additional role  
OBS Admin

Submit

The updated list of users is displayed.

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

Rows 1 - 7 of 7

## Removing a Role / Deactivating a User

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

1. Open [IGEL Customer Portal](https://cosmos.igel.com/)<sup>8</sup>, log in to your admin account, and select **Users > User & Role Administration**.

Catalog Knowledge My History & My Requests Advanced Service Users ▾ Configure Services ▾ My Company Subscriptions ▾ Tours ●

Welcome to IGEL

Insert your question here

Overview

User & Role Administration

Bring your IDP

IGEL OS IDP

My Profile

<sup>8</sup> <https://cosmos.igel.com/>

**2. Select Remove role.**

\* Indicates required

User & Role Administration

User & Role Administration

\*Please choose

-- None --

-- None --

Invite new User

Add additional role

**Remove role**

Submit

Required information  
Please choose

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

User & Role Administration

User & Role Administration

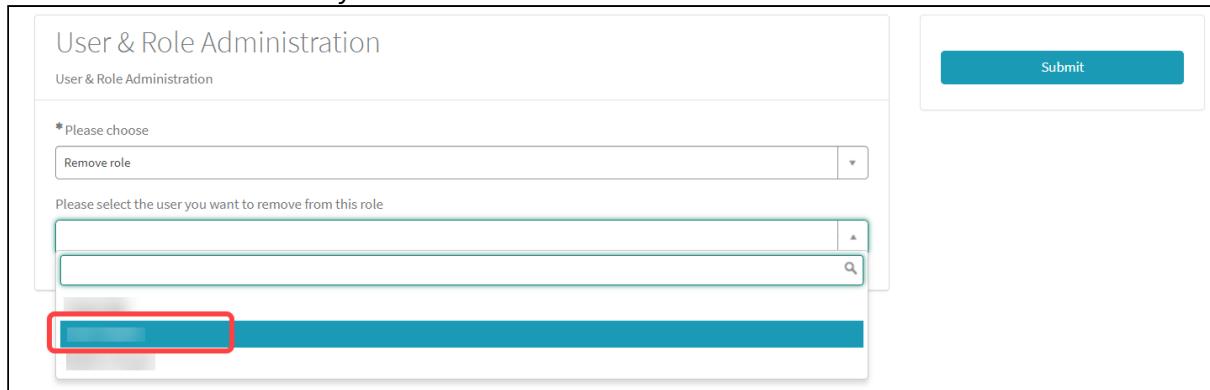
\*Please choose

Remove role

Please select the user you want to remove from this role

**[Redacted]**

Submit

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

\* Indicates required

User & Role Administration

User & Role Administration

\*Please choose

Remove role

Please select the user you want to remove from this role

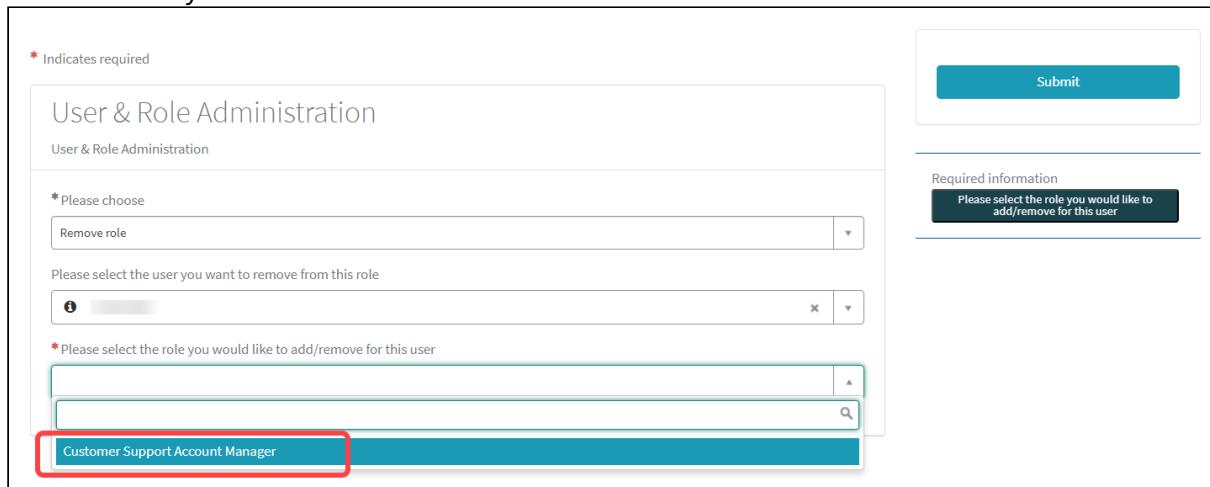
**[Redacted]**

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

**Customer Support Account Manager**

Submit

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





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



A screenshot of the "User & Role Administration" page. It shows fields for selecting a role to remove, a user to remove from that role, and a role to add or remove for the selected user. A red box highlights the "Submit" button in the top right corner.

User & Role Administration

\*Please choose  
Remove role

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

\*Please select the role you would like to add/remove for this user  
Customer Support Account Manager

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

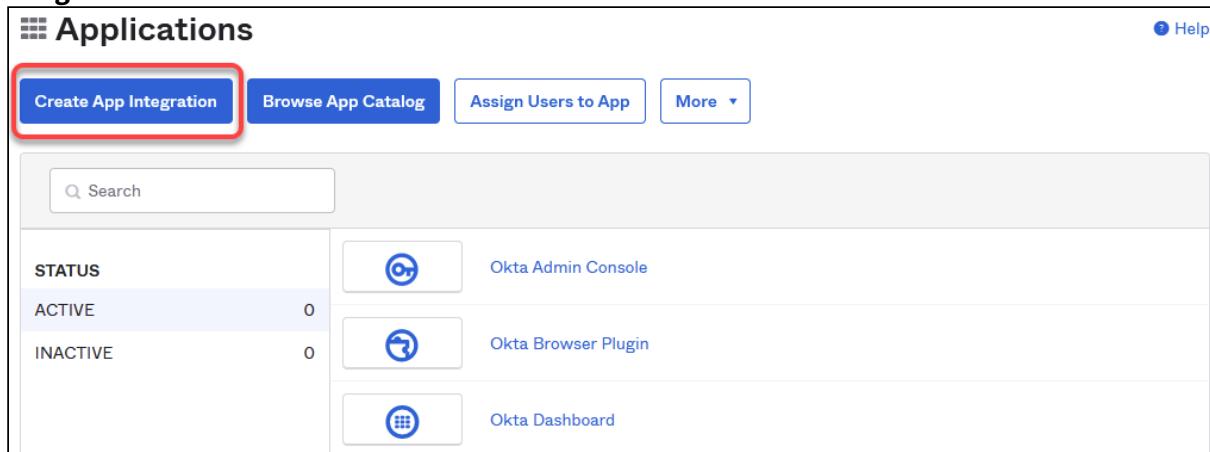
Submit

## 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**.



A screenshot of the Okta Applications dashboard. At the top, there are buttons for "Create App Integration" (which is highlighted with a red box), "Browse App Catalog", "Assign Users to App", and "More". Below this is a search bar. The main area shows a table with columns for STATUS, ACTIVE, and INACTIVE. It lists three applications: "Okta Admin Console", "Okta Browser Plugin", and "Okta Dashboard".

STATUS	ACTIVE	INACTIVE
ACTIVE	0	
INACTIVE	0	

Okta Admin Console

Okta Browser Plugin

Okta Dashboard



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

### Create a new app integration

**Sign-in method**

[Learn More ↗](#)

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

[Cancel](#) **Next**



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

**Create SAML Integration**

<b>1 General Settings</b>	<b>2 Configure SAML</b>
---------------------------	-------------------------

**1 General Settings**

App name

App logo (optional)

App visibility  Do not display application icon to users

**Cancel** **Next**

The "App name" field and the "App logo" section are highlighted with a red rounded rectangle. The "Next" button is also highlighted with a red rounded rectangle.

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>
<code>NameID Format</code>	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 'Sign On' tab selected in the navigation bar. Below it, the 'Settings' section is displayed. Under 'Sign on methods', 'SAML 2.0' is selected. A note states: 'SAML 2.0 is not configured until you complete the setup instructions.' A blue button labeled 'View Setup Instructions' is visible. At the bottom, a note says: 'Identity Provider metadata is available if this application supports dynamic configuration.'

Igel SSO

Active

View Logs Monitor Imports

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

General Sign On Import Assignments

**Settings** Edit

**Sign on methods**

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

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

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

[View Setup Instructions](#)

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



- 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>
            [REDACTED]
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    </md:NameIDFormat>
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[REDACTED].okta.com/app/[REDACTED]_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

- Open [IGEL Customer Portal](https://cosmos.igel.com/)<sup>9</sup>, log in to your admin account, and select **Users > Bring your IdP**.

- Enter the following data from your metadata file:

<sup>9</sup> <https://cosmos.igel.com/>



- **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>
```

- **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-...okta.com/app/trial-.../sso/saml">
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://trial-...okta.com/app/trial-.../sso/saml"/>
  </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/...
* Passive authentication endpoint	https://...okta.com/app/..._igelssso_1/.../sso/saml
Metadata URL	https://...okta.com/app/.../sso/saml/metadata
* Domain name of federating IdP	.okta.com
Associated Domains	
Add	Remove All
Actions	Domain name
No data to display	
* Certificate	



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

Bring your IdP

Register SAML connection data for federated IdPs

\* Issuer URI  
http://www.okta.com/

\* Passive authentication endpoint  
https://.okta.com/app/\_igelssso\_1/\_sso/saml

Metadata URL  
https://.okta.com/app/\_sso/saml/metadata

\* Domain name of federating IdP  
.okta.com

**Associated Domains**

Actions	Domain name
No data to display	

\* Certificate

The "Associated Domains" section is highlighted with a red box.

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

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

A screenshot of a web-based application interface titled "Associated Domains". On the left, there's a sidebar with a "Actions" dropdown menu and a "Domain name" search input field. Below this, a message says "No data to display". On the right, there's a large text area labeled "\* Certificate" which is heavily redacted with horizontal grey bars. At the bottom right of the page is a blue "Submit" button, which is also highlighted with a red rectangular border.

## 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**.

A screenshot of the Okta Assignments page for the "Igel SSO" application. The page has a header with a gear icon, three dots, and the text "Igel SSO". Below the header are buttons for "Active" (selected), "View Logs", and "Monitor Imports". A blue info icon with an "i" contains the text: "Once you have a working SAML integration, submit it for Okta review to publish in the OAN." Below the header is a navigation bar with tabs: General, Sign On, Import, and Assignments (which is highlighted with a red box). Underneath the tabs are buttons for "Assign" (with a dropdown arrow), "Convert assignments" (with a dropdown arrow), a search bar containing "Search...", and a "People" dropdown. A table lists users assigned to the application. The table has columns for Filters (dropdowns for People and Groups), Person (displaying name and email), and Type (Individual). Two users are listed:

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 web interface. On the left, a sidebar menu includes sections for Environments, Administrators, Production, Connections (which is highlighted with a red box), Applications, Application Catalog, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main content area shows a list of existing applications: AAD\_APP, PingOne Admin C, PingOne Application, and PingOne Self-Service. A red box highlights the 'Applications' button in the top navigation bar. Below it, a search bar and a link to 'Add Application' are visible. A modal dialog is open for creating a new application, titled 'Name and Describe Application'. It contains fields for 'Application Name' (set to 'Test Application'), 'Description' (empty), and an 'Icon' (a small placeholder icon). The 'Choose Application Type' section offers four options: SAML Application, OIDC Web App, Single-Page, and Worker. The 'SAML Application' option is selected and detailed in the modal. It describes SAML applications as being accessed via a browser using the SAML protocol. The 'Configure' button at the bottom right of the modal is also highlighted with a red box.

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, a sidebar menu includes sections like Applications, Application Catalog, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main area displays a list of existing applications: AAD\_APP, PingOne Admin C, PingOne Application, and PingOne Self-Service. A search bar is at the top. To the right, a form for creating a new application is shown. The 'Name and Describe Application' section has a red box around the 'Application Name \*' field, which contains 'Test Application'. Below it is a 'Description' field and an 'Icon' upload area. The 'Choose Application Type' section has a red box around the 'SAML Application' option, which is described as 'Applications that are accessed within a browser using the SAML protocol'. Other options include 'OIDC Web App', 'Single-Page', and 'Worker'. The 'SAML Application' configuration dialog is open, showing 'Connection Type: SAML' and a 'Configure' button, which is also highlighted with a red box.

3. In the **SAML Configuration** dialog, select **Manually Enter** and enter the following data:

- **ACS URLs:** Enter <https://login.microsoftonline.com/login.srf>
- **Entity ID:** Enter the prefix <https://login.microsoftonline.com/> followed by the Azure Active Directory tenant ID.



Add Application

### SAML Configuration

Provide Application Metadata

Import Metadata  Import From URL  Manually Enter

ACS URLs \*

+ Add

Entity ID \*

4. Create the application.

5. Edit/create the following attribute mappings:

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

**AAD\_APP** Client ID: 42d6943e-7af9-43e2-a34c-a4d255ea1a3f

Overview Configuration Attribute Mappings Policies Access

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

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

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

6. Finish the application setup.



## Obtaining the SAML 2.0 Connection Data

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

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

The screenshot shows a web-based application configuration interface for a SAML application named "AAD\_APP". The "Configuration" tab is selected. The "Connection Details" section contains several fields:

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



## Configuring Ping as Your Federated IdP

1. Open [IGEL Customer Portal](#)<sup>10</sup>, log in to your admin account, and select **Users > Bring your IdP**.

A screenshot of the IGEL Customer Portal's navigation bar. The bar includes links for Catalog, Knowledge, My History &amp; My Requests, Advanced Service, Users (with a dropdown arrow), Configure Services, and My Company Subscriptions. A dropdown menu is open over the 'Users' link, listing five options: Overview, User &amp; Role Administration, Bring your IdP (which is highlighted with a red box), IGEL OS IdP, and My Profile. Below the navigation bar, there is a dark banner with the text 'Welcome to IG' and a search bar containing 'Insert your question here'.

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.

---

<sup>10</sup> <https://cosmos.igel.com/>



## Installing the IGEL UMS

### **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.

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.

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. For details, see the ICG 2.x documentation:

- [ICG Manual](#)
- [ICG Prerequisites](#)

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



**Setup - Universal Management Suite 12**

### Select Components

Which components should be installed?

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

Standard UMS with embedded database

Component	File Size
Standard UMS (stand-alone)	1.146,8 MB
with UMS Web App	416,5 MB
with UMS Console	168,8 MB
with Embedded Database	20,1 MB
Distributed UMS	541,7 MB
with UMS Web App	416,5 MB
with UMS Console	168,8 MB
UMS High-Availability-Network	616,5 MB
UMS Server	168,8 MB
with UMS Console	416,5 MB
with UMS Web App	215,4 MB
UMS Load Balancer	168,8 MB
Only UMS Console	

Current selection requires at least 1.266,0 MB of disk space.

< Back **Next >** Cancel

Requirements for the installation of the UMS can be found under Installation Requirements for the IGEL UMS.

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

**Windows:** IGEL UMS Installation under Windows

**Linux:** IGEL UMS Installation under Linux

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

- i** You can update to UMS version 12.01.110 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 RCs

**ⓘ For Update Installations Only**

- As of UMS 12, MDM feature is no longer available; the corresponding notification will be shown during the update to UMS 12 or higher if you have MDM devices.
- 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.

**ⓘ 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. Currently, SSL must be terminated at the UMS Server.
- 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.

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

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



## Registering the UMS

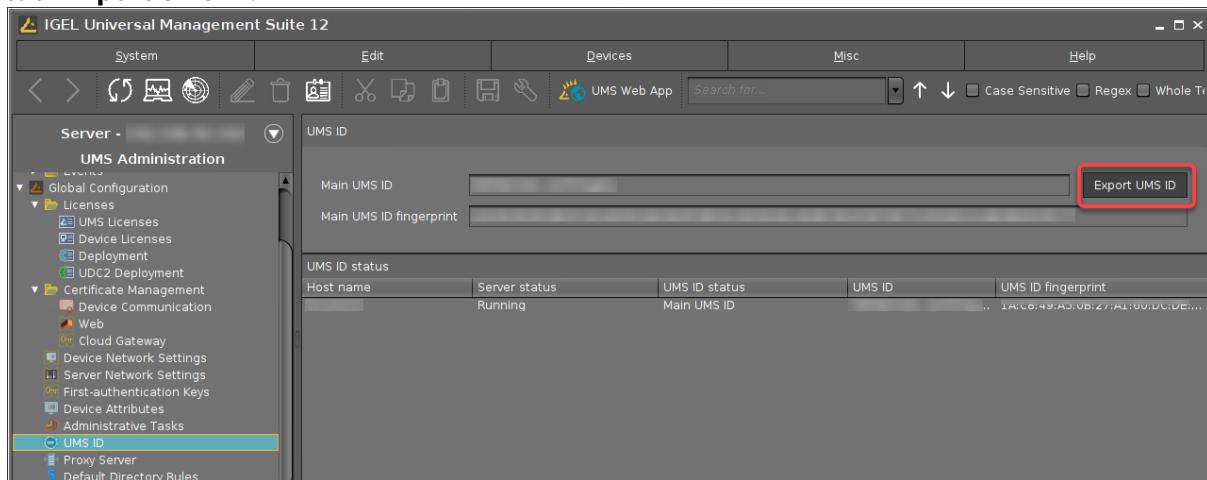
To authenticate your UMS to the IGEL Cloud Services, you must register your UMS. This involves uploading the UMS ID, which is essentially a certificate of your UMS, to the IGEL Customer Portal.

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

## Exporting the UMS ID

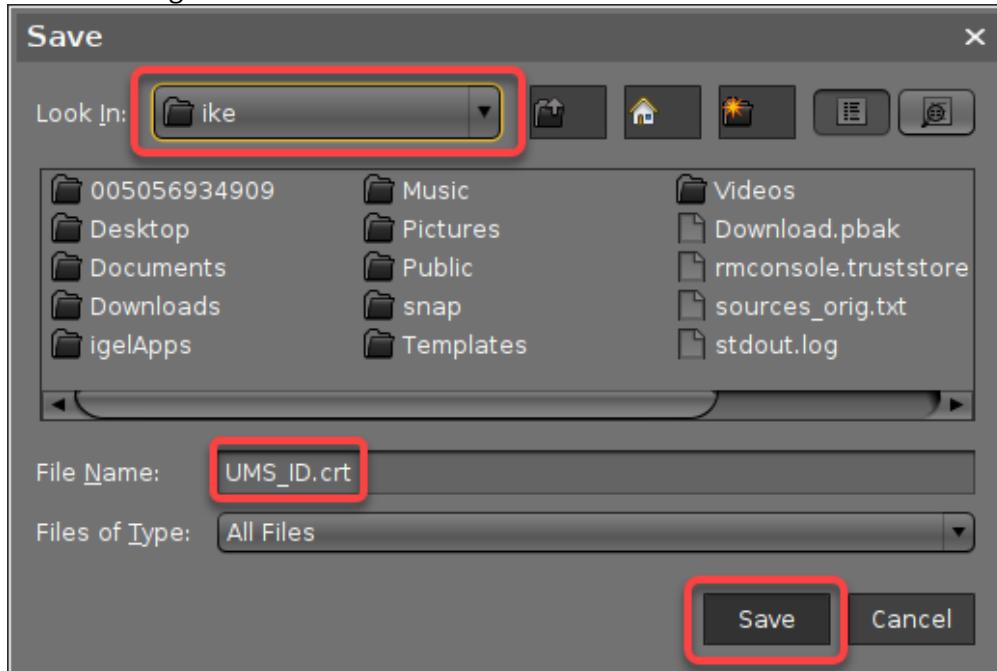
To upload the UMS ID, we must export it from the UMS.

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

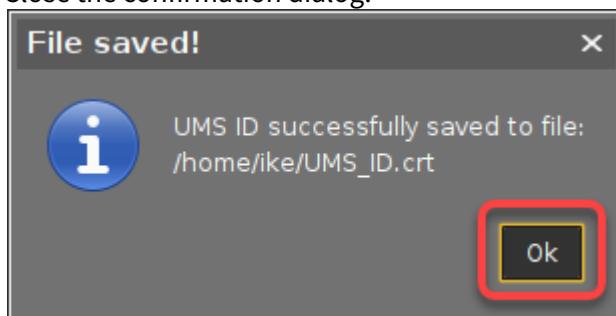




2. Select a storage location and click **Save**.



3. Close the confirmation dialog.



## Registering the UMS

1. Open [IGEL Customer Portal<sup>11</sup>](https://cosmos.igel.com/) in your browser and log in to your admin account.

<sup>11</sup> <https://cosmos.igel.com/>



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

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

UMS Management							
All > Account = Test Company							<a href="#">Register a new UMS Instance</a>
UMS Name	X.509 Certificate	Expiration Date	Fingerprint	Enable App Portal	Created by(owned_by)	Created	Updated
[REDACTED]	[REDACTED]	2042-04-09 11:03:49	[REDACTED] ...	true	[REDACTED]	2023-02-09 12:07:23	2023-02-09
[REDACTED]	[REDACTED]	2042-04-09 06:10:55	[REDACTED] ...	true	[REDACTED]	2023-02-09 11:39:19	2023-02-09
[REDACTED]	[REDACTED]	2042-04-07 15:08:18	[REDACTED] 2...	true	[REDACTED]	2023-02-06 15:02:02	2023-02-06
[REDACTED]	[REDACTED]	2042-03-28	[REDACTED] 3...	true	[REDACTED]	2023-02-03	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 170).
- **Required - Upload:** Upload the certificate file (UMS ID) of your UMS. Make sure that the certificate file has the extension `.cer`, `.crt`, or `.pem`

## Registering the UMS



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

Upload Delete

**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

Upload Delete

**Submit**

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

## Registering the UMS



UMS Management							<a href="#">Register a new UMS Instance</a>
All > Account =	Test Company						
UMS Name	X.509 Certificate	Expiration Date	Fingerprint	Enable App Portal	Created by(owned_by)	Created	Updated
UMS Ike	[REDACTED]	2042-04-09 06:10:55	[REDACTED]	true	[REDACTED]	2023-04-14 14 12:28:39	2023-04-14 12:28:39
[REDACTED]	[REDACTED]	2042-05-19 10:10:47	[REDACTED]	.. true	[REDACTED]	2023-03-31 14:28:42 11:45:02	2023-04-11 14:28:42
[REDACTED]	[REDACTED]	2042-06-04 12:10:30	[REDACTED]	true	[REDACTED]	2023-04-11 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); we will use Azure AD.

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

1. [Activating the Onboarding Service \(OBS\)](#)(see page 39)
2. [Creating an Azure Web Application That Will Serve as Identity Provider](#)(see page 40): We register an application in Microsoft Azure to use its Azure AD services as an external identity provider.
3. [Registering Our Azure Application in the IGEL Customer Portal](#)(see page 46): This will enable IGEL Cloud Services to use our Azure Application as the external identity provider.
4. [Creating a User in the Azure App](#)(see page 63): We create a user account in our Azure application. These user credentials, consisting of an e-mail address and a password, will be entered by the user when onboarding his device.
5. [Downloading the Root Certificate of the UMS](#)(see page 64): The root certificate is needed for defining the route to the appropriate UMS
6. [Creating the Record Set for the OBS Routing](#)(see page 65): Define the route to the appropriate UMS. This includes linking our Azure AD user to the UMS.

### Activating the Onboarding Service (OBS)

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

1. Log in to the [IGEL Customer Portal](#)<sup>12</sup>.
2. From the menu, select **Activate IGEL OS Onboarding**.

---

<sup>12</sup> <https://cosmos.igel.com/>



## Creating an Azure Web Application That Will Serve as Identity Provider

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

A screenshot of the Azure portal's main dashboard. At the top, there's a "Welcome to Azure!" message with three cards: "Start with an Azure free trial", "Manage Azure Active Directory", and "Access student benefits". Below this, there's a section titled "Azure services" with various icons for different services like Quickstart Center, Virtual machines, App Services, Storage accounts, SQL databases, and Azure Cosmos DB. In the center, there's a "Create a resource" button and an "Azure Active Directory" button, which is highlighted with a red box and a blue arrow pointing to it from below. To the left, there's a "Kubernetes services" button. At the bottom, there's a "More services" link.



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

A screenshot of the Azure Active Directory portal. 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, a message states: "Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph." A "Learn more" link is provided. The main area shows tabs for All applications, Owned applications (which is underlined), and Deleted applications. There's a search bar with placeholder text "Start typing a display name or application (client) ID to filter these r..." and an "Add filters" button. A message below the tabs says "This account isn't listed as an owner of any applications in this directory." A blue "View all applications in the directory" button is visible. On the left side, there's a sidebar titled "Manage" with sections for Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations (which is also 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 for the app
- **Supported account types:** Set the permissions according to your requirements.
- **Redirect URI (optional):** For our purposes, this setting is not optional but required. Set the first field to **Web** and, in the second field, provide the URI of the onboarding service. This is "<https://obs.services.igel.com>".



Home > IGEL Technology GmbH >

## Register an application

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

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.  
  ✓

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:

## Initial Configuration of the IGEL Onboarding Service (OBS)



Screenshot of the Microsoft Azure portal showing the configuration of the "OBS Testing application".

**Application Overview:** The application is named "OBS Testing application". It has an Application (client) ID and an Object ID. The Directory (tenant) ID is listed as "Local directory". The supported account type is "My organization only".

**Client credentials:** A "Client credentials" section is present, with a link to "Add a certificate or secret".

**Redirect URIs:** One redirect URI is listed: "1web.0.spa.0.public client".

**Application ID URI:** A link to "Add an Application ID URI" is shown.

**Managed application in local directory:** A link to "OBS Testing application" is shown.

**Feedback and Notices:** Two informational messages are displayed:

- "Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)"
- "Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)"

**Get Started:** A "Get Started" button is located at the bottom left, and "Documentation" is linked to the right.

**Call-to-action:** A large button at the bottom encourages users to "Build your application with the Microsoft identity platform".



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

A screenshot of the Azure portal interface. The left sidebar shows a tree view of app settings: Overview, Quickstart, Integration assistant, Manage (with sub-options like Branding &amp; properties, Authentication, Certificates &amp; secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting (with sub-options like Troubleshooting and New support request). The 'Token configuration' option under 'Manage' is highlighted with a red box. The main content area is titled 'Token configuration' and shows the 'Optional claims' section. It includes a note about optional claims being used to configure additional information returned in tokens, a 'Learn more' link, and two buttons: '+ Add optional claim' (which is also highlighted with a red box) and '+ Add groups claim'. A table below lists 'Optional claims' with columns for 'Claim', 'Description', and 'Token type'. The table header indicates sorting by 'Claim' (ascending) and 'Token type' (descending). The table body displays the message 'No results.'

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

- **email**
- **preferred\_username**



## 6. Click Add.

The screenshot shows the Microsoft Azure portal's 'Token configuration' page for an app registration named 'OBS'. The 'Optional claims' section is visible, showing a table with columns 'Claim' and 'Description'. Below the table, there are two checked checkboxes: 'email' and 'preferred\_username'. A red box highlights both checkboxes. At the bottom of the modal, there is an 'Add' button, which is also highlighted with a red box.

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

The screenshot shows a confirmation dialog box with the title 'Add optional claim'. Inside, there is a message: 'Some of these claims (email) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below.' Below this message is a checkbox labeled 'Turn on the Microsoft Graph email permission (required for claims to appear in token)'. The 'Add' button at the bottom left is highlighted with a red box.

The token configuration is completed:



The screenshot shows the Azure portal's App registrations section. A modal window titled "Token configuration" is open. In the "Optional claims" section, there are two entries: "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..."). Below the table, there are buttons for "Add optional claim" and "Add groups claim". At the top right of the modal, there are success messages: "Edit optional claim Successfully updated OBS" and "Updating permissions Successfully saved permissions for OBS". The left sidebar shows the navigation menu for the app registration.

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

## Registering Our Azure App in the IGEL Customer Portal

- Open the [IGEL Customer Portal](#)<sup>13</sup> in your browser, log in to your admin account, and select **Users > IGEL OS IdP**.

The screenshot shows the IGEL COSMOS customer portal. The top navigation bar includes links for Catalog, Knowledge, My History & My Requests, Advanced Service, Users (with a dropdown menu), Configure Services, and My Company Subscriptions. A search bar and a "Welcome to IGEL COSMOS" banner are also present. The "Users" dropdown menu is open, listing several options: Overview, User & Role Administration, Bring your IdP, and IGEL OS IdP. The "IGEL OS IdP" option is highlighted with a red box.

<sup>13</sup> <https://cosmos.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	U
*****	*****	*****	*****	*****	*****	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

Actions	Domain Name
Add	No data to display
Remove All	

**Submit**

Required information

Client ID
Authorization Endpoint URL

Token Endpoint URL



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

The screenshot shows the Azure portal interface for the 'OBS Testing application'. The left sidebar has sections like 'Manage', 'Branding & properties', 'Authentication', 'Certificates & secrets', 'Token configuration', 'API permissions', 'Expose an API', 'App roles', 'Owners', and 'Roles and administrators'. The main area is titled 'Essentials' and contains fields for 'Display name' (set to 'OBS Testing application'), 'Application (client) ID' (redacted), 'Object ID' (redacted), 'Directory (tenant) ID' (redacted), 'Client credentials' (with a link to 'Add a certificate or secret'), 'Redirect URLs' (set to '1 web, 0 spa, 0 public client'), 'Application ID URI' (with a link to 'Add an Application ID URI'), and 'Managed application in local directory' (set to 'OBS Testing application'). Below these fields, it says 'Supported account types' (set to 'My organization only'). There are also informational messages about the new App registrations experience and the end of ADAL support.

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' blade in the Azure portal. It lists four endpoints: 'OAuth 2.0 authorization endpoint (v2)' (value: https://login.microsoftonline.com/), 'OAuth 2.0 token endpoint (v2)' (value: https://login.microsoftonline.com/:/oauth2/v2.0/token), 'OAuth 2.0 authorization endpoint (v1)' (value: https://login.microsoftonline.com/:/oauth2/authorize), and 'OAuth 2.0 token endpoint (v1)' (value: https://login.microsoftonline.com/:/oauth2/token). A 'Copy to clipboard' button is located next to the v2 authorization endpoint's value, with a red box highlighting it.

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

Actions	Domain Name
	No data to display

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



**Endpoints**

Endpoint Type	URL	Action
OAuth 2.0 authorization endpoint (v2)	<a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> /:oauth2/v2.0/authorize	<a href="#">Copy</a> <a href="#">Copied</a>
OAuth 2.0 token endpoint (v2)	<a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> /:oauth2/v2.0/token	<a href="#">Copy to clipboard</a> 
OAuth 2.0 authorization endpoint (v1)	<a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> /:oauth2/authorize	<a href="#">Copy</a>
OAuth 2.0 token endpoint (v1)	<a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> /:oauth2/token	<a href="#">Copy</a>

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 Azure app, go to **Overview**, and copy the **Application (client) ID** to the clipboard.



A screenshot of the Azure portal showing the "OBS Testing application" overview page. The left sidebar shows navigation options like Overview, Quickstart, Integration assistant, Manage (Branding &amp; properties, Authentication, Certificates &amp; 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 has tabs for Overview, Endpoints, and Preview features. The Overview tab is selected. It displays the application's details under the "Essentials" section: Display name (OBS Testing application), Application (client) ID (highlighted with a red box and a "Copy to clipboard" button), 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). There are also two informational cards at the bottom: one about the new App registrations experience and another about the deprecation of ADAL and Graph starting June 30th, 2020.

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 Azure app (**Overview**) and click **Add a certificate or secret**.

The screenshot shows the Azure portal interface for managing an application. The left sidebar has a 'Manage' section with various options like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest, and Support + Troubleshooting. The 'Certificates & secrets' option is selected. The main area shows the application details: Display name 'OBS Testing application', Application (client) ID, Object ID, Directory (tenant) ID, and Supported account types 'My organization only'. A red box highlights the 'Add a certificate or secret' button under the 'Client credentials' section. There are also informational messages about feedback, redirect URLs, application ID URIs, and managed applications.

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 includes the same 'Manage' section as the previous screenshot. The main area has tabs for Certificates (0), Client secrets (0), and Federated credentials (0). A message states that client secrets are used to prove an application's identity. Below this, there is a table with columns for Description, Expires, Value (with a help icon), and Secret ID. A red box highlights the '+ New client secret' button. A note at the bottom says '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

**Add** **Cancel**

A screenshot of a dialog box titled "Add a client secret". It contains two input fields: "Description" (containing "OBS credentials") and "Expires" (set to "Recommended: 6 months"). A red arrow points from the bottom left towards the "Add" button, which is highlighted with a red border. The "Cancel" button is also visible at the bottom.



## 15. Copy the client secret to the clipboard.

A screenshot of the IGEL Onboarding Service interface. At the top, there is a feedback pop-up and a general information message about credentials. Below this, the "Client secrets" tab is selected, showing one entry: "OBS credentials" with an expiration date of "11.1.2023". The "Value" column contains the client secret, which has been highlighted and has a red border around the copy icon, indicating it is ready to be copied.

Description	Expires	Value	Secret ID
OBS credentials	11.1.2023	Copied	[Redacted]

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



## IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

\* Display Name  
My OBS identity provider

\* Client ID  
[REDACTED]

\* Client Secret  
.....| SHOW

\* Authorization Endpoint URL  
`https://login.microsoftonline.com/` 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 Azure app and change to the overview of your Azure tenant.

18. Copy the **Primary domain** to the clipboard.A screenshot of the Azure Active Directory Overview page for the tenant "IGEL Technology GmbH". The left sidebar shows navigation options like Overview, Preview features, and Manage (Users, Groups, External Identities, etc.). The main area displays basic information: Name (IGEL Technology GmbH), Tenant ID (redacted), Primary domain (onmicrosoft.com, highlighted with a red box), License (Azure AD Free), and summary statistics for Users (1), Groups (0), Applications (1), and Devices (0).

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

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.

## Initial Configuration of the IGEL Onboarding Service (OBS)



IGEL OS Identity Provider

Add Row

\* Domain Name  
onmicrosoft.com

\* 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	

**Add** **Cancel** **Add**

The screenshot shows the configuration interface for the IGEL Onboarding Service. A modal window titled 'Add Row' is open, prompting for a 'Domain Name' (onmicrosoft.com). The main configuration area below lists 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). At the bottom, a 'Mapped Domains' section contains a table with two columns: 'Actions' and 'Domain Name'. The table displays the message 'No data to display'. Two buttons, 'Add' (highlighted with a red box) and 'Cancel', are located at the bottom left of the modal, while another 'Add' button is at the bottom right of the main configuration area.

20. Click **Submit**.

The screenshot shows the 'IGEL OS Identity Provider (IdP) Registration' page. It includes 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, there's a 'Mapped Domains' section with an 'Add' button and a table showing one entry: .onmicrosoft.com. A 'Submit' button is at the top right, which is highlighted with a red box.

The data record is created.

The screenshot shows the 'IGEL OS IdP Management' table. The newly created record is highlighted with a red box. The table columns are: Display name, Client ID, Client Secret, Authorization URL, Token URL, Mapped Domains, Created, and Updated. The highlighted row contains: My OBS identity provider, redacted, redacted, https://login.microsoftonline.com/.../authorize, https://login.microsoftonline.com/.../.onmicrosoft.com, 2022-12-01 16:01:06, and 2022-12-01 16:01:06. There is another row below it with similar data.

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	Updated
My OBS identity provider	redacted	*****	https://login.microsoftonline.com/.../authorize	https://login.microsoftonline.com/.../.onmicrosoft.com	2022-12-01 16:01:06	2022-12-01 16:01:06	2022-12-01 16:01:06
	redacted	*****	https://login.microsoftonline.com/.../authorize	https://login.microsoftonline.com/.../.onmicrosoft.com	2022-10-13 12:16:26	2022-10-13 12:16:26	2022-10-13 12:16:26



## Creating a User in the Azure App

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

The screenshot shows the Azure Active Directory Overview page for 'IGEL Technology GmbH'. The left sidebar has a 'Manage' section with options like Overview, Preview features, Diagnose and solve problems, and a prominent 'Users' option which is highlighted with a red box. The main area displays basic information about the tenant, including Name (IGEL Technology GmbH), Users (1), Tenant ID, Primary domain (igelobs.onmicrosoft.com), License (Azure AD Free), and Applications (1). There are tabs for Overview, Monitoring, Properties, and Tutorials, and a search bar at the top.

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

The screenshot shows the 'Users' page in the Azure portal. The left sidebar includes options like All users (preview), Audit logs, Sign-in logs, and Manage. The main area has a 'Create a new user' button, and below it, an 'Invite external user' option is highlighted with a red box. A tooltip says 'legacy users list experience? Click here to leave the preview.' The table below lists one user found, showing columns for Display name, User principal name, User type, On-premises sync status, and Identity provider.

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 \*  s.onmicrosoft.com

Name \*  OBS User

First name

Last name

**Password**

Auto-generate password  
 Let me create the password

Initial password \*

**Groups and roles**

Groups 0 groups selected

Roles User

**Settings**

Block sign in  Yes  No

Usaue location

**Create**

## Downloading the Root Certificate of the UMS

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

UMS 12

Devices Configuration **Network** 3 more ▾ App Portal Help English

td-ums12

**UMS Server State**  
UMS Server is running  
ICG Connections: 0/0 connected

**UMS Server Details**  
Process ID: [redacted]  
Last Change: November 21, 2022  
Cluster ID: UMS-CLUSTER-[redacted]  
Operating System: Ubuntu 20.04.5 LTS

**Requests** November 21, 2022 8:55 AM - 2:55 PM

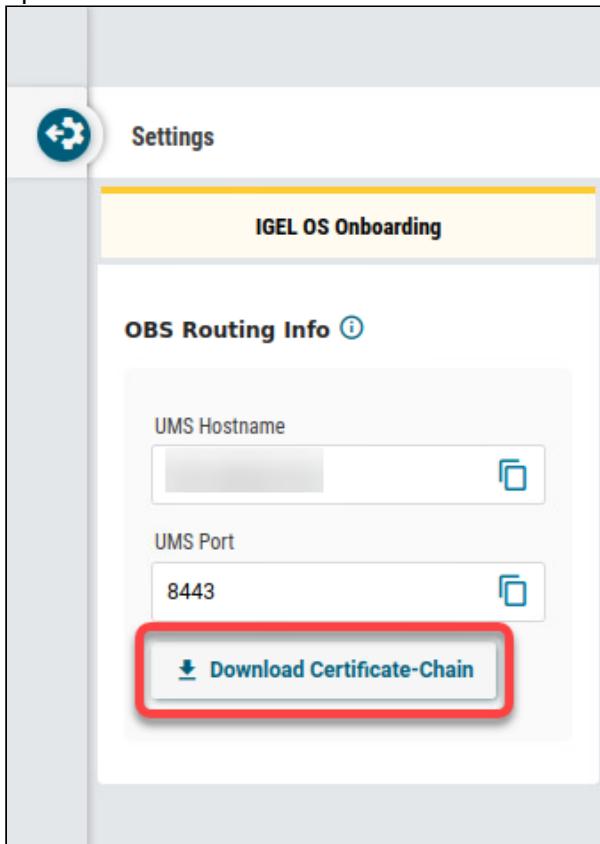
Successful

Waiting Failed

Time	Successful	Waiting	Failed
8:55 AM	0.0	0.0	0.0
9:10 AM	0.0	0.0	0.0
9:25 AM	0.0	0.0	0.0
9:40 AM	0.0	0.0	0.0
9:55 AM	0.0	0.0	0.0
10:10 AM	0.0	0.0	0.0
10:25 AM	0.0	0.0	0.0
10:40 AM	0.0	0.0	0.0
10:55 AM	0.0	0.0	0.0
11:10 AM	0.0	0.0	0.0
11:25 AM	0.0	0.0	0.0
11:40 AM	0.0	0.0	0.0
11:55 AM	0.0	0.0	0.0
12:10 PM	0.0	0.0	0.0
12:25 PM	0.0	0.0	0.0
12:40 PM	0.0	0.0	0.0
1:10 PM	0.0	0.0	0.0
1:25 PM	0.0	0.0	0.0
1:40 PM	0.0	0.0	0.0
1:55 PM	0.0	0.0	0.0
2:10 PM	0.0	0.0	0.0
2:25 PM	0.0	0.0	0.0
2:40 PM	0.0	0.0	0.0
2:55 PM	0.0	0.0	0.0



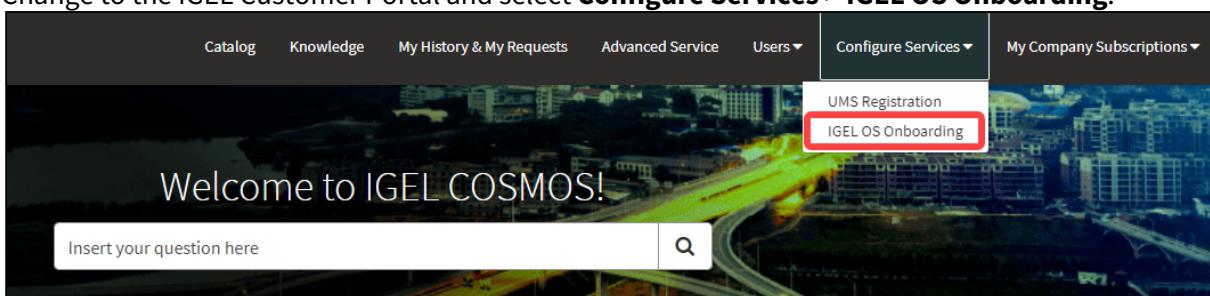
2. Open the context menu for the root certificate and select **Download Certificate Chain**.



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

## 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	
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]	2042-11-10 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
- **UMS Port:** Port under which the UMS can be reached. The default port of the UMS web server is 8443. For details on the ports used by the UMS, see IGEL UMS Communication Ports.

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.company.com
* 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!)

① 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
<b>Add</b>	

Mapped Domains

Actions	Domain
<b>Add</b>	

\* 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
<b>Add</b>	

Mapped Domains

Actions	Domain
<b>Add</b>	

\* 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 Azure or the relevant domain and click **Add**.



6. Click **Required - Upload** to upload the UMS root certificate.

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
<a href="#">Add</a>	

Mapped Domains

Actions	Domain
<a href="#">Add</a>	

\* 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  
myums.company.com

\* UMS Hostname  
myums.company.com

\* UMS Port  
8443

Mapped Users

Actions	Email Address
<b>Add</b>	

Mapped Domains

Actions	Domain
<b>Add</b>	

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

**Replace** **Delete**

**Submit**

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

\* Display Name  
myums.company.com

\* UMS Hostname  
myums.company.com

\* UMS Port  
8443

Mapped Users

Actions	Email Address
<b>Add</b>	

Mapped Domains

Actions	Domain
<b>Add</b>	

\* 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
[REDACTED]	8443				2022-11-12 23:30:18		2042-11-12 10:00:31
[REDACTED]	8443				2022-10-05 10:08:18		2042-09-28 02:18:51
[REDACTED]	8443			2	2022-10-27 19:05:09		2023-11-10 20:44:53
[REDACTED]	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
[REDACTED]	[REDACTED]
UMS Hostname	Expiration date
[REDACTED]	2042-11-12 10:00:31
UMS Port	Created
8443	2022-11-12 23:30:18
	Updated
	2022-11-13 05:50:37
Fingerprint	
[REDACTED]	
OBS Certificate String	
-----BEGIN CERTIFICATE-----	[REDACTED]

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



The user can now be onboarded. The onboarding process from the user's view is described under [Onboarding IGEL OS 12 Devices](#)(see page 126).



## 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.

The screenshot shows the 'APP PORTAL EXPLORE' section of the COSMOS Secure Endpoint Platform. At the top, there's a search bar and filters for 'Categories' (set to 'All') and 'Sort by' (set to 'Name'). Below the search bar, there's a 'Discover Our Apps' section. The main area displays a grid of eight application cards:

- CPcore Binary** (1.1.0 BUILD 2) - NEW: Last update 12. December 2022, Size 23.5 MB. Description: CPcore binary for IGEL AVD Client allows the user to access their Microsoft Azure Virtual Desktop environment.
- CUPS printing app** (1.0.0 BUILD 2) - NEW: Last update 12. December 2022, Size 11.75 MB. Description: CUPS printing application provides printing functionality for IGEL OS.
- Chromium Browser** (108.0.5359.124 BUILD 1 RC 4) - NEW: Last update 23. February 2023, Size 130.25 MB. Description: Chromium is an open source browser project that aims to build a safer, faster and more stable way for everyone to experience the web.
- Chromium Multimedia Codec** (107.0.5304.62 BUILD 1 RC 2) - NEW: Last update 08. February 2023, Size 1.5 MB. Description: Multimedia codec (H.264) support for Chromium Browser.
- Chromium ffmpeg codec** (108.0.5359+1 BUILD 1) - NEW: Last update 12. December 2022, Size 1.75 MB. Description: Contains ffmpeg with aac/ac3/mpg4audio/h264/mov/mp3 and gstreamer ffmpeg plugin.
- Cisco Jvdi plugin** (Cisco Jabber 14.1.2.307144 BUILD 1) - NEW: Last update 13. January 2023, Size 59.25 MB. Description: Cisco JVDI Plugins enable the use of Cisco Jabber conferencing within a VDI environment.
- Cisco Webex Meetings VDI** (42.6.8.5 BUILD 1 RC 1) - NEW: Last update 24. February 2023, Size 59.25 MB. Description: Smoother meeting experience under VDI.
- Cisco Webex VDI** (42.6.0.22645 BUILD 1 RC 1) - NEW: Last update 24. February 2023, Size 67.5 MB. Description: A Webex specifically tailored for VDI users.

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

## Access to the IGEL App Portal

- ⚠** The import of apps to the UMS as well as the download of apps to the UMS-managed devices is only possible if the UMS is registered in the IGEL Customer Portal. For the instructions, see [Registering the UMS](#)(see page 34).  
If the device is not managed with the UMS, the download of apps is possible but NOT for the devices with a Starter license. For more information on licenses, see [Licensing](#)(see page 119).

You can open the IGEL App Portal

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



- locally on the device via the **App Portal** application (i.e. context: OS12)  
With this method, you can install or uninstall apps locally on the device. For more information, see [Installing IGEL OS Apps Locally on the Device](#)(see page 150).  
Here, you can find the following buttons:
  - All:** All apps
  - Available:** All new apps and apps to be updated
  - Installed:** All apps that have already been installed on the device
- via **UMS Web App > App Portal** (i.e. context: UMS admin)  
With this method, you can import apps in the UMS to deploy them to your endpoint devices.  
Here, you can find the following buttons:
  - All:** All apps
  - Available:** All new apps and apps to be updated
  - Imported:** All apps that have already been imported to the UMS. In the UMS Web App, the imported apps are displayed under **Apps**.

The screenshot shows the 'APP PORTAL UMS ADMIN' interface. At the top, there's a navigation bar with 'All Apps'. Below it is a search bar and a 'Discover Our Apps' section. Underneath, there are four cards representing imported apps: 'CUPS printing app', 'Chromium Browser', 'Citrix Workspace App', and 'Zoom'. Each card includes details like last update date, size, and category. A red box highlights the 'IMPORTED' button in the top navigation bar.

The screenshot shows the 'UMS 12' interface with a navigation bar including 'Devices', 'Apps' (which is the active tab), and '4 more'. A red box highlights the 'App Portal' button in the top right. Below the navigation, there's a sidebar with 'Apps' and a main content area showing a list of imported apps: 'Chromium Browser', 'CUPS printing app', and 'Citrix Workspace App'. An arrow points from the 'App Portal' button in the top bar down to the 'App Portal' button in the sidebar. To the right, there's a detailed view of the 'Chromium Browser' app, showing its version history and a button to 'Import newest version from App Portal'.

## Importing Apps to the IGEL UMS

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

A screenshot of the COSMOS App Portal interface. At the top, there's a navigation bar with the IGEL logo, the text "COSMOS Secure Endpoint Platform", and "APP PORTAL UMS ADMIN". Below this, the main content area shows a list of apps under "All Apps". A specific app entry for "Chromium Browser" is highlighted. The app card includes a blue circular icon, the text "UP TO DATE", the name "Chromium Browser", the version "108.0.5359.94 BUILD 1 RC 1", and a red-bordered "IMPORT" button. A red arrow points from the text below to this "IMPORT" button. Below the app card, there's a section titled "Chromium" with a brief description: "Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all Internet users to experience the web."

UP TO DATE Chromium Browser

Versions 108.0.5359.94 BUILD 1 RC 1

IMPORT

DESCRIPTION HISTORY

### Chromium

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

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



## IGEL UMS 12: Basic Configuration

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

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

### First Steps in the IGEL UMS

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

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

### System Configuration

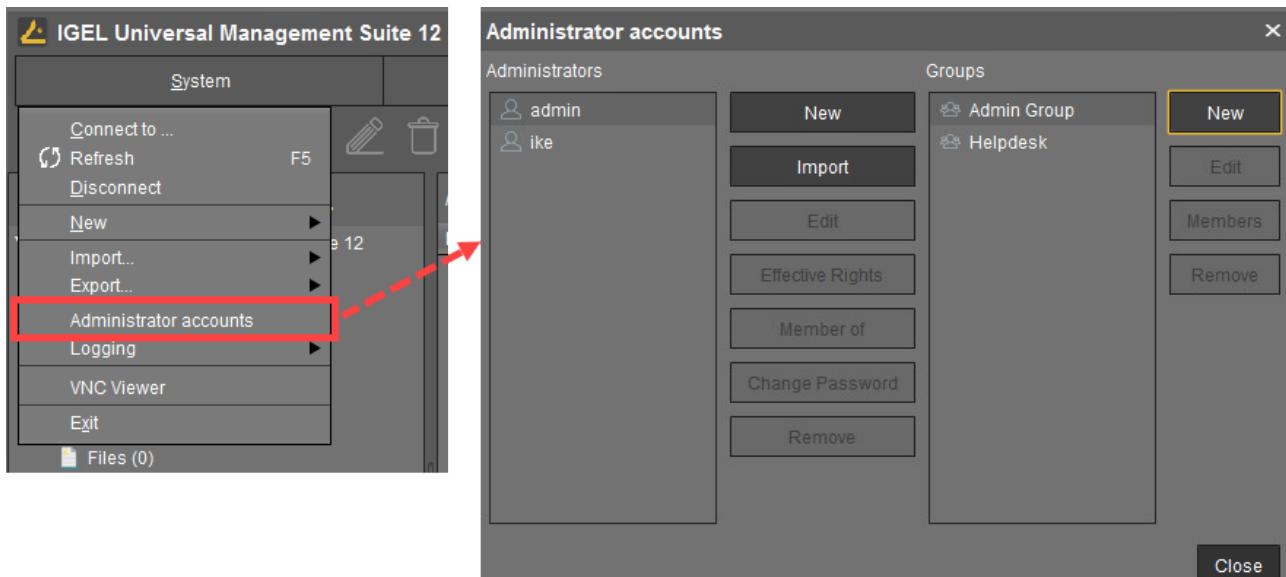
1. Activate logging under **UMS Administration > Global Configuration > Logging**.
2. Under **UMS Administration > Administrative tasks**, create the following administrative tasks:
  - Create backup
  - Delete logging data
  - Other tasks to automatically clean up logs (job execution data, execution data of administrative tasks, process events, asset information history)
3. If you want to activate the naming convention for your devices, go to **UMS Administration > Global Configuration > Device Network Settings**. For more information, see Renaming IGEL OS Devices.

### Administrator Accounts

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

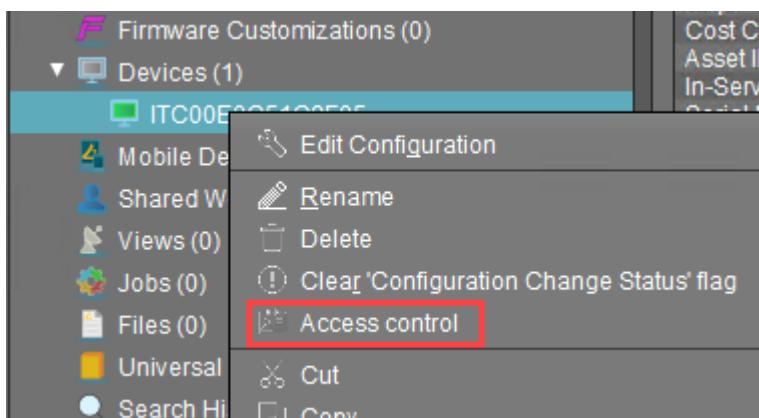
If you do not want to adopt the Active Directory structure, you can create local administrators and groups manually: **UMS Console > System > Administrator Accounts > New**.

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



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

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



For more information on UMS administrator accounts and access rights, refer to Create Administrator Accounts.

## 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.



The screenshot shows the COSMOS Secure Endpoint Platform App Portal. In the center, there's a card for the 'Chromium Browser' app. At the top left is a blue circular icon with a white 'O'. To its right, the text 'UP TO DATE' is followed by 'Chromium Browser'. Below that, it says 'Versions 108.0.5359.94 BUILD 1 RC 1'. On the far right of this row is a large blue button with the word 'IMPORT' in white. A red arrow points from the text 'Import the app' to this button. Below this row are two tabs: 'DESCRIPTION' and 'HISTORY'. Under the 'DESCRIPTION' tab, there's a section titled 'Chromium' with a short description: 'Chromium is an open-source browser project that aims to build a safer, faster, and more stable way for all Internet users to experience the web.'

**⚠** If you want to create profiles configuring IGEL OS Base System settings (e.g. corporate design, SSO, 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.

- 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.

The screenshot shows the UMS 12 Web App interface. At the top, there's a navigation bar with 'UMS 12', 'Devices', 'Apps' (which is highlighted in yellow), and '4 more'. Below this is a sidebar with 'Apps' and a filter. The main area shows a list of apps under 'All', with 'Chromium Browser' selected. To the right of the list is a detailed card for 'Chromium Browser'. This card includes a 'Create new profile' button (which is highlighted with a red box), a 'Set Default Version' link, a 'Delete App' link, and some status information: 'Newest imported Version: 108.0.5359.124 BUILD 1 RC 3' and 'Default Version: 108.0.5359.124 BUILD 1 RC 3'. It also shows a small icon of the browser and the text 'Categories: Browser'. At the bottom of the card is a 'Check for updates' button.

- In order for your devices to be placed automatically in the specific directory according to certain rules during the onboarding:
  - In the **UMS Web App > Devices**, create a device directory: Click , type a directory name, and press [Enter]. For more information, see Creating a Directory Structure in the IGEL UMS Web App.



The screenshot shows the UMS 12 interface. The top navigation bar has tabs for 'UMS 12', 'Devices', and 'Configuration'. The 'Devices' tab is selected. Below the navigation bar is a 'Directory Tree' section containing a 'Devices (0)' folder. To the right is a 'Devices' list view showing 0-0 of 0 devices. The 'Devices' icon in the top bar is highlighted with a red box.

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

The screenshot shows the UMS Administration interface. On the left is a tree view of configuration categories. Under 'Global Configuration', 'Default Directory Rules' is selected. The main pane shows a 'Default Directory Rules' table with columns for 'Rule', 'Directory', 'Overriding', and 'Apply on boot'. A red arrow points to the 'Leave in Subdirectory' checkbox in the toolbar above the table.

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.

- 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.



A screenshot of the IGEL UMS 12 web interface. The top navigation bar includes tabs for UMS 12, Devices, Configuration, Apps, and more. The main area shows a directory tree under 'Devices / OS 12 devices' with a single item 'OS 12 devices (0)'. On the right, there's a panel for 'OS 12 devices' with options like Reboot, Shutdown, and Wake up. A red box highlights the 'Assign object' button. Below it, the 'Properties' section shows the device name and path.

A detailed view of the 'Assign Object to Directory' dialog. It has two main sections: 'Assignable Objects' on the left and 'Assignments' on the right. In the 'Assignable Objects' section, a list of apps is shown: Chromium (selected and highlighted with a red box), Zoom, CUPS printing app, and Citrix Workspace App. Each item has a 'Default Vers...' dropdown. An arrow button between the two sections indicates the transfer of objects. At the bottom are 'Cancel' and 'Save' buttons.

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



this profile under **Assigned Objects**.

The screenshot shows the 'Assigned Objects' section for the 'OS 12 devices' folder. It lists the 'Chromium' app with its version 'OS 12'. A red arrow points to the 'Chromium Browser' entry in the list.

## Importing IGEL OS Apps from the IGEL App Portal

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

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

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

The screenshot shows the 'Chromium Browser' app page in the IGEL App Portal. The 'IMPORT' button is highlighted with a red box and a red arrow points to it from the previous step's description.

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

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



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

The screenshot shows the IGEL UMS 12 interface. The top navigation bar includes 'UMS 12', 'Devices', 'Apps' (which is selected), '4 more', 'App Portal', 'Help', and language settings ('English'). The main content area has a sidebar labeled 'Apps' with a filter icon. The main panel displays a list of apps under 'All'. One item, 'Chromium Browser', is highlighted with a red box. To its right, there's a detailed view with a blue icon, the name 'Chromium Browser', and buttons for 'Create new profile', 'Set Default Version', and 'Delete App'. Below this, it shows 'Newest imported Version: 108.0.5359.124 BUILD 1 RC 3', 'Default Version: 108.0.5359.124 BUILD 1 RC 3', and a note that 'The newest available Version is unknown'. It also includes a 'Check for updates' button and a category icon for 'Browser'.

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

**Accepting EULA in the UMS**

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

Accepting EULA can be necessary, for example, for automatically registered apps (IGEL OS Base System, all [locally installed apps](#)(see page 150)) or if the EULA is changed. If not accepted in the UMS, the EULA can still be accepted by your users locally on the device via the corresponding [notification dialog](#)(see page 168).

The screenshot shows the 'Versions' tab in the Apps section. At the top, it says '4 Versions' with counts for 'Installed' (3), 'Assigned' (1), and 'Profiles' (4). Below this, two rows of app versions are listed. The first row is 'Default version (12.01.100 BUILD 1 R...)' with status icons for 1 installed, 1 assigned, and 4 profiles. The second row is '12.1.100 BUILD 1 TP 2' with status icons for 0 installed, 0 assigned, and 0 profiles. An orange arrow points to the second row. At the bottom, there's a summary: 'File size unknown', 'imported by #device', and 'imported on Jan 20, 2023'. Below this is a 'EULA State' section with a yellow warning icon and the text 'Not Accepted'. A red box surrounds this entire section, and a red arrow points to the 'Accept EULA' button.

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



## Creating an OS 12 Profile

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

### **⚠ Implicit App Assignment via Profiles**

An app is automatically assigned to a device via a profile which configures this app. Exception: IGEL OS Base System app

An app version selected in the profile will be assigned to a device. The best practice is to use the **Default Version**, see [Setting a Default Version of an App](#)(see page 83).

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 83).

There are two methods to create a profile:

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

**i** Profiles cannot currently be deleted in the UMS Web App.

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

### Option 1: Via Configuration

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



### 3. Click Select Apps.

The screenshot shows the UMS 12 interface with the 'Configuration' tab selected. In the left sidebar, under 'Profiles', there is a section for 'IGEL OS 12 (4)' which includes 'Apps (2)'. One of these apps is 'Chromium'. A red arrow points from this section to a modal dialog titled 'Create new profile'. Inside the dialog, the 'OS 12' radio button is selected. Below it, the 'Name' field contains 'Chromium' and is also highlighted with a red border. At the bottom right of the dialog is a blue 'Select Apps' button, which is also highlighted with a red border.

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

**i** If you want to create profiles configuring IGEL OS Base System settings (e.g. corporate design, 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.

The screenshot shows the 'App Selector - Chromium' dialog. At the top, there is a note: 'In OS 12 you can define what apps should be configured by a profile. Please select at least one app. (You can choose from Base System and/or Apps.) This selection can always be changed.' On the left, there is a 'Base System' section with an 'IGEL OS' icon and a dropdown menu showing 'Default version'. Below it is an 'Apps' section with icons for 'IGEL OS', 'Citrix Workspace', and 'Chromium Browser'. The 'Chromium Browser' icon has a red box around it, indicating it is selected. To its right is another 'CUPS printing app'. At the bottom right of the dialog are 'Cancel' and 'Save' buttons, with 'Save' being highlighted with a red border. A red dashed arrow points from the 'Show Versions' toggle switch at the top right to the 'Save' button.



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

6. Click **Save**.

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

7. Configure the desired settings.

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

profile), click **App Selector**

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

The screenshot shows the 'Profile Configurator - Chromium' window. On the left, there's a sidebar with 'Apps' selected, showing a tree structure with 'chromium' expanded, containing 'Chromium Browser Global', 'Chromium Browser Sessions', and 'Chromium browser'. Below this is a 'Settings' section. The main area has tabs for 'Session name' (set to 'Chromium browser') and 'Starting Methods for Session'. Under 'Starting Methods for Session', there are five items, each with a switch and a checkbox. All checkboxes are checked: 'Start Menu', 'Menu folder' (empty), 'Start Menu's System tab', 'Application Launcher', and 'Application Launcher folder'. At the bottom are buttons for 'Close', 'Save', and 'Save and Close'.

8. Save the changes.

9. Assign the profile to the required device / device directory. See [Assignment of Apps and Profiles](#)(see page 85).



## Option 2: Via Apps

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

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

- 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.

<b>Name</b>	Chromium
<b>Description</b>	(empty)
<b>Location</b>	Profiles
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- Click **Save**.

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

- Configure the desired settings.

The configuration dialog shows only those settings that can be configured for the selected app. If you want to change the scope of the profile (i.e. redefine which apps should be configured by the



profile), click **App Selector**

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

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

The screenshot shows the 'Profile Configurator - Chromium' interface. On the left, there's a sidebar with 'Apps' selected, showing sections for 'chromium' and 'Chromium Browser Global'. Under 'chromium', 'General' is selected, with other options like 'Appearance', 'Content', 'Proxy', 'Privacy', 'Security & Encryption', and 'Custom Setup'. On the right, under 'Chromium Settings', there's a 'Block Chromium settings' switch. Below it, the 'Startup and Tab Page' section has two dropdown menus: 'On Startup' set to 'Open a specific page or set of pages' and 'Startup page' set to 'https://www.igel.com|https://kb.igel.com'. There's also a 'Handle new tab page' dropdown set to 'Open a blank page'. At the bottom, there are buttons for 'Close', 'Save', and 'Save and Close'.

5. Save the changes.
6. Assign the profile to the required device / device directory. See [Assignment of Apps and Profiles](#)(see page 87).

## 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:

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

The screenshot shows the 'Chromium Browser' app details page in the UMS 12 interface. The 'Set Default Version' button is highlighted with a red box. Below it, the 'Default version' entry in the list of versions is highlighted with a yellow box.

Version	Installed	Assigned	Profiles
Default version (108.0.5359.94 BUILD ...)	2	0	1
108.0.5359.94 BUILD 1 RC 1	2	0	0
108.0.5359.94 BUILD 3	0	0	0

- Select the desired Default Version and save the changes.

The screenshot shows the 'Set Default Version' dialog box. The selected version, '108.0.5359.94 BUILD 1 RC 1', is highlighted with a yellow background.

## Assignment of Apps and Profiles

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

- Implicit app assignment via profiles:** An app is automatically assigned to a device via a profile which configures this app. Exception: IGEL OS Base System app  
The app version that will be installed on the device via the implicit assignment if several profiles



configure this app (but in different versions) is defined by the priority rules for profiles, see Prioritization of Profiles in the IGEL UMS and Summary - Prioritization of IGEL UMS Profiles.

- Explicit app assignment via the **Assign object** dialog

**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.

## Implicit App Assignment via Profiles

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

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

The screenshot shows the IGEL UMS 12 web interface. In the top navigation bar, 'Devices' is selected. On the left, a 'Directory Tree' sidebar shows a hierarchy of devices: 'Devices (5)' including 'Augsburg (4)' which contains 'techdoc (4)' with 'QA (1)' and 'RD (3)'. 'RD' is currently selected. The main content area displays a list of objects under 'RD': 'ITC005056938D22' (selected and highlighted with a red box), 'td-RD01', and 'td-RD02'. To the right of the list is a detailed view for 'ITC005056938D22' with tabs for 'Assigned Objects', 'System Information', 'Licenses', 'Network Adapter', and 'Installed Apps'. A red box highlights the 'Assign object' button in the top right of this view.

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

A screenshot of the "Assign Object to Device" dialog box. The title bar shows "Assign Object to Device" and the device ID "ITC005056938D22". Below the title bar is a toolbar with a "Filter objects" input field and several icons: a grid, shield, graduation cap, user, network, file, and a trash can. The main interface is divided into two sections: "Assignable Objects" on the left and "Assignments" on the right. The "Assignable Objects" section contains a list of apps with shield icons: Chromium, Background, SSH, Terminal, Firefox, and VMware Horizon. The "Chromium" item is highlighted with a red box. To the right of this list is a large red-bordered arrow pointing from left to right. The "Assignments" section is currently empty. At the bottom right are "Cancel" and "Save" buttons, with the "Save" button also enclosed in a red box.

The screenshot shows the "Assignable Objects" list with "Chromium" selected and highlighted by a red box. A large red box surrounds the central transfer arrow. Another red box highlights the "Save" button at the bottom right.

3. Save the changes.

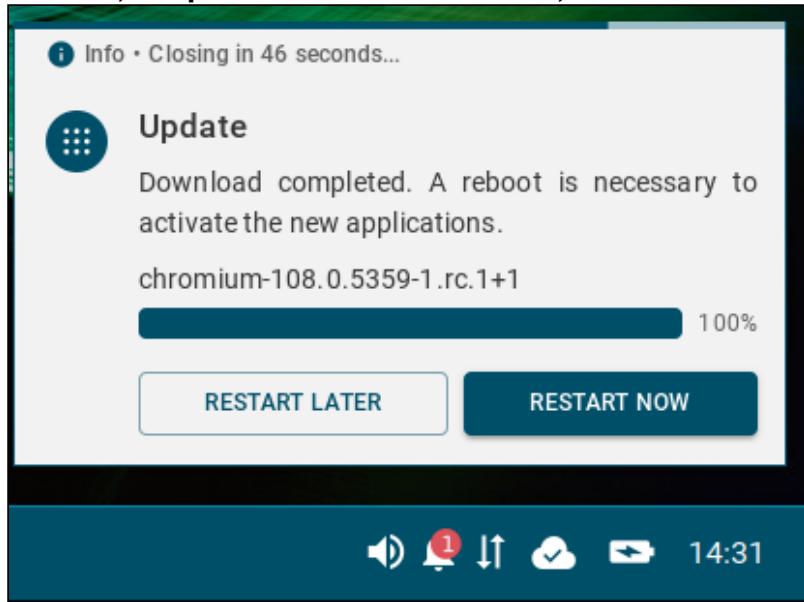
4. Decide when the changes should become effective.

An app assigned via the profile will be downloaded by the device.

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



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



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

Category	Object	Description
Language	OS 12	
Terminal	OS 12	
Installed Apps	Chromium	Chromium Browser Default Version (108.0.5359.94 BUILD 1 RC 1)

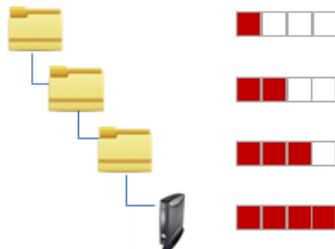
To check the installed apps, go to **Devices > [name of the device] > Installed Apps**; see Checking Installed Apps via the IGEL UMS Web App.



## Explicit App Assignment

- 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**.

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



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

- 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).

- i** If no version is specified for an app during the assignment, the [Default Version](#)(see page 87) will be used. It is possible to select the version for an app in the **Assign Object** dialog either under **Assignable Objects** or under **Assignments**.



Assign Object to Device

ITC005056938D22

Assignable Objects

- Chromium Browser (selected, highlighted with a red box)
- Citrix Multimedia Codec
- IGEL OS
- CUPS printing app

Default Ver... ▾

Assignments

- Terminal (OS12)
- Chromium (OS 12)

→ ←

Cancel Save

A screenshot of the IGEL UMS interface showing the "Assign Object to Device" dialog. The left panel, titled "Assignable Objects", lists several items: Chromium Browser, Citrix Multimedia Codec, IGEL OS, and CUPS printing app. The "Chromium Browser" item is selected and highlighted with a red box. Below it is a dropdown menu with the text "Default Ver..." and a downward arrow. To the right is the "Assignments" panel, which shows two assignments: "Terminal" (under "OS12") and "Chromium" (under "OS 12"). Between the two panels are two large red-bordered arrows: a right-pointing arrow on top and a left-pointing arrow below it. At the bottom right are "Cancel" and "Save" buttons.



A screenshot of the "Assign Object to Device" dialog in IGEL UMS 12. The dialog has two main sections: "Assignable Objects" on the left and "Assignments" on the right. In the "Assignable Objects" section, there are four items: "Citrix Multimedia Codec", "IGEL OS", "CUPS printing app", and "Zoom Media Plugins for VDI". Each item has a dropdown menu labeled "Default Ver...". In the "Assignments" section, there are four assignments: "Chromium Browser", "Terminal", "OS12", and "Chromium". A red arrow points from the "Chromium Browser" assignment to its "Default Version" dropdown. At the bottom right of the dialog are "Cancel" and "Save" buttons, with "Save" being highlighted by a red box.

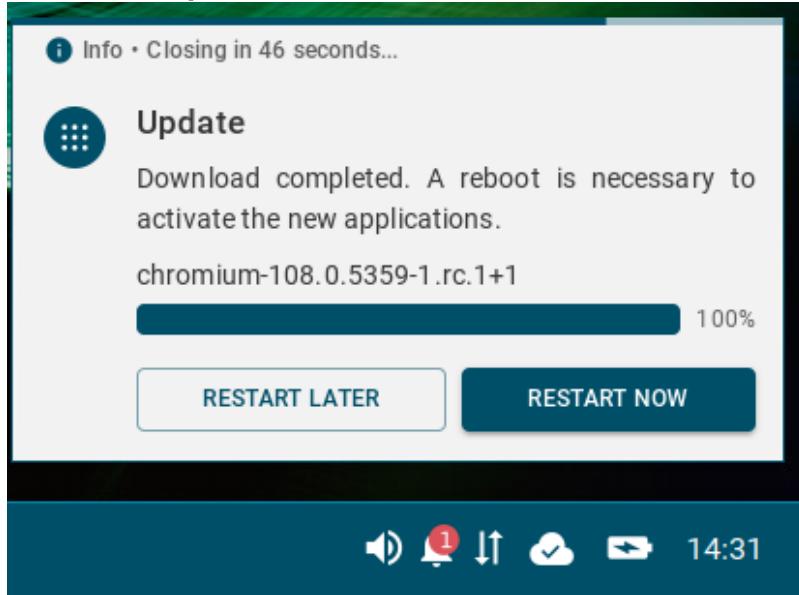
3. Save the changes.
4. Decide when the changes should become effective.

The app will be downloaded by the device.

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



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



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

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

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



## IGEL UMS 12: App Update

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

The update procedure includes the following steps:

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

### Preconditions

- You use the [Default Version](#)(see page 87) during the app assignment and profile creation (best practice).

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

- You have checked and, if necessary, changed the default global update settings.
- You have checked and, if necessary, changed the default update settings for individual apps. **Apps > [name of the app] > Update Settings > Default Version for Assigned Devices** has been set to **Update Default Version manually** (default).
- You have checked the default settings in **IGEL Setup > System > Update** and, if necessary, created a profile modifying these settings according to your needs and assigned it to the devices.
- All devices have a valid license. See [Licensing](#)(see page 119).
- Devices to be updated are online.
- All devices are connected to a regular LAN or WLAN (not OpenVPN, OpenConnect, genucard, NCP VPN, or mobile broadband).
- All devices are in a safe environment where the update process cannot be disrupted, e.g. by powering off the devices.

### Update of the IGEL OS Base System

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

**ⓘ** This procedure is also relevant for any [explicitly assigned app](#)(see page 88).



## Preparing the Update

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

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

## Testing the Update

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

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



Assign Object to Device

ITC0050569356CB

Filter objects

Assignable Objects

Default Ver... ▾

IGEL OS

CUPS printing app

zoom Zoom Media Plugins

Default Ver... ▾ →

Background

Wallpaper

12.01.100 BUILD 1 RC 5

12.01.100 BUILD 1 RC 8

12.01.100 BUILD 1 RC 9

12.01.100 BUILD 1 RC 10

12.01.110 BUILD 1 RC 1

12.01.110 BUILD 1 RC 2

12.02.100 NIGHTLY 2023-03-06

Cancel Save

This screenshot shows the 'Assign Object to Device' dialog in IGEL UMS 12. The 'Assignable Objects' section on the left lists several items, with 'IGEL OS' selected and highlighted by a red box. A red arrow points from the 'Default Ver...' dropdown menu to the list of available versions below. Another red box highlights the version '12.01.110 BUILD 1 RC 2' in the list. The 'Assignments' section on the right shows 'Background' and 'Wallpaper' assigned. At the bottom right are 'Cancel' and 'Save' buttons.



3. Save the changes.
4. Decide when the changes should become effective.  
The app version will be downloaded by the device.  
By default, apps / app versions assigned to the device will be automatically activated at the next reboot. If you have configured the background app update, an **Update** command must be sent, instead; see How to Configure the Background App Update in the IGEL UMS Web App.
5. Under **Devices > [name of the device] > Installed Apps**, check the app, its version and state; see Checking Installed Apps via the IGEL UMS Web App.

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

## Triggering the Mass Update

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



2. Select the required version.

The screenshot shows the UMS 12 web interface. In the top navigation bar, the 'Apps' tab is selected. On the left, a sidebar lists categories like Browser, Cloud, VDI, etc. The main pane displays a list of apps, with 'IGEL OS' selected and highlighted by a red box. A modal window titled 'Set Default Version' is open over the list, also with a red box around it. This modal lists several software versions for IGEL OS, with '12.01.110 BUILD 1 RC 2' highlighted by another red box at the bottom of the list.

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

4. If the **IGEL OS Base System app** has not yet been assigned to the devices: Go to **UMS Web App > Devices > [name of the device / device directory]** and click **Assign object** to assign the app. Verify that **Default Version** is selected in the version picker. Click **Save** and decide when the changes should become effective.

The screenshot shows the UMS 12 web interface with the 'Devices' tab selected. The left sidebar shows a 'Directory Tree' with 'Devices (3)' expanded, showing 'Augsburg (2)' and 'Bremen (1)', both highlighted with a red box. The main pane shows the 'Augsburg' device details. A button labeled 'Assign object' is highlighted with a red box. Below it, the 'Properties' section shows the device name and path. At the bottom, there is a 'Assigned Objects' section.

A screenshot of the "Assign Object to Directory" dialog in the IGEL UMS web interface. The title bar shows "Assign Object to Directory" and the path "Devices / Augsburg (2)". The main area has two sections: "Assignable Objects" on the left and "Assignments" on the right. In the "Assignable Objects" section, there is a list of objects with dropdown menus labeled "Default Ver...":

- IGEL OS (selected, highlighted with a red box and a red arrow pointing to the "Default Ver..." dropdown)
- CUPS printing app
- zoom Zoom Media Plugins for VDI

A large blue "→" button is positioned between the two sections. At the bottom right are "Cancel" and "Save" buttons.

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

The new version will be downloaded by the devices.

By default, apps / app versions assigned to the device will be automatically activated at the next reboot. By default, the reboot is performed automatically after the timeout of 60 seconds after the app download if the user does not postpone the device restart, see [IGEL OS Notification Center](#)(see [page 168](#)).

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](#).



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

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

## Update of the Implicitly Assigned IGEL OS Apps

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

For more information on the implicit app assignment, see [Assignment of Apps and Profiles](#)(see page 88).

### Preparing the Update

- In the **UMS Web App > Apps**, select the required app, e.g. Chromium.
- If you have not activated the automatic import of updates under **Update Settings > Automatic check for updates in UMS**, click **Import newest version from App Portal** or click **App Portal** to import the required app version manually.

### Testing the Update

- Go to **UMS Web App > Configuration** and create a test profile with the same settings and app(s) as the "productive" profile, e.g. **Test Update Chromium**. Leave the **Default Version** for the app(s) in the **App Selector** (as it was done for the productive devices). For how to create profiles, see [Creating an OS 12 Profile](#)(see page 83).
 

**i** Currently, copying of OS 12 profiles is not possible.
- In the **UMS Web App > Devices**, select your test device(s) and assign the created profile **Test Update Chromium**. For more information on the assignment, see [Implicit App Assignment via](#)



Profiles(see page 88).

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

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

A screenshot of the UMS Web App interface. The top navigation bar shows 'UMS 12', 'Devices', 'Configuration' (which is highlighted in yellow), and '4 more'. Below the navigation is a 'Profiles / Test App Updates' section. On the left is a 'Configuration Tree' pane with 'Profiles (12)' expanded, showing 'IGEL OS 11 (1)', 'IGEL OS 12 (10)' (with 'Apps (2)' expanded), 'Base System (7)', and 'Test App Updates (1)'. The main area shows a list of profiles: 'Test App ...' (with a folder icon), 'Test Update Chromium' (with a shield icon). A red box highlights the 'Edit Configuration' button next to 'Test Update Chromium'. To the right is a 'Properties' panel for 'Test Update Chromium' with fields for Name (Test Update Chromium), Directory Path (Profiles / Test App Updates), and Id (19320).

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

A screenshot of the 'Profile Configurator - Test Update Chromium' dialog. At the top is a header with a pencil icon and the title. Below it is a navigation bar with 'Apps' (highlighted in yellow) and 'System' tabs, and a search icon. The main content area shows a tree view with a single node 'chromium' under 'Apps'. At the bottom is a footer with buttons for 'Close', 'Save', and 'Save and Close'. A red box highlights the 'App Selector' button in the footer.



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

The screenshot shows the 'App Selector - Test Update Chromium' interface. At the top right, there is a 'Show Versions' button with a checked checkbox, which is highlighted with a red box. Below it, a message says: 'In OS 12 you can define what apps should be configured by a profile. Please select at least one app. (You can choose from Base System and/or Apps.) This selection can always be changed.' The main area is titled 'Apps' and lists several applications with their versions. The 'Chromium Browser' app is selected, and its version dropdown menu is open, showing 'Default version' at the top, followed by '108.0.5359.94 BUILD 3', '108.0.5359.94 BUILD 1 RC 1', and '111.0.5563.64 BUILD 1 RC 1'. The '111.0.5563.64 BUILD 1 RC 1' option is highlighted with a red box. At the bottom right, there are 'Cancel' and 'Save' buttons.

6. Save the changes.

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

The screenshot shows the 'Devices / Test' page in the IGEL UMS 12 interface. On the left, the 'Devices' section shows a list with 'Test (1)' selected. In the main pane, a device named 'ITC0050569356CB' is selected, highlighted with a red box. On the right, there is a detailed view of this device with various configuration options. A red arrow points to the 'Send settings' button in the toolbar.

The new app version will be downloaded by the device.

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

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

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



## Triggering the Mass Update

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

The screenshot shows the UMS 12 interface with the 'Apps' tab selected. In the main pane, under the 'Browser' category, 'Chromium Browser' is listed. To its right, there's a detailed view of the app with a 'Set Default Version' button highlighted by a red box.

- Select the required version.

The screenshot shows the 'Set Default Version' dialog box overlaid on the UMS interface. It displays a dropdown menu with several version options, and the option '111.0.5563.64 BUILD 1 RC 1' is highlighted by a red box.

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

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

The new version will be downloaded by the devices.

By default, apps / app versions assigned to the device will be automatically activated at the next reboot. By default, the reboot is performed automatically after the timeout of 60 seconds after the app download if the user does not postpone the device restart, see [IGEL OS Notification Center](#)(see [page 168](#)).

If you have configured the background app update, an **Update** command must be sent instead of the reboot for the app activation; see [How to Configure the Background App Update in the IGEL UMS Web App](#).



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



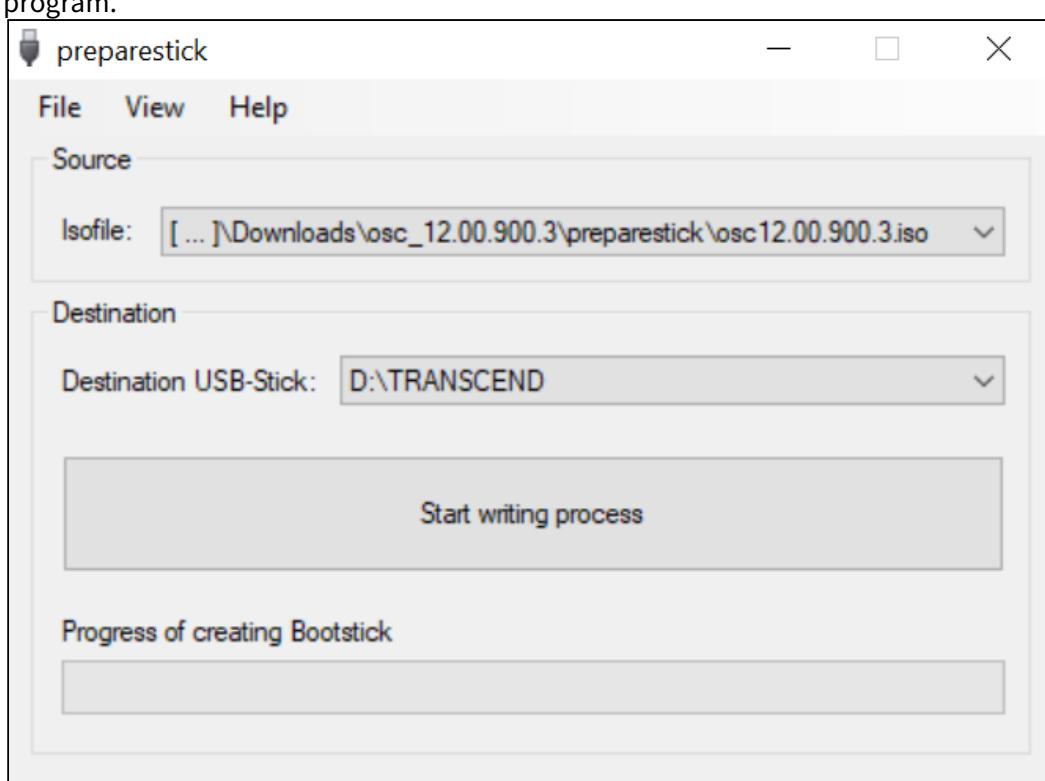
## Installing the Base System via IGEL OS Creator (OSC)

### Installation Requirements and Devices Supported by IGEL OS 12

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

### Create USB Installation Medium (Windows)

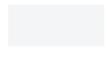
1. Unzip the contents of the ZIP archive for OSC that you received from IGEL into a local directory.
  - For new devices, use the standard installer (e.g. `osc_12.01.110.zip`).
  - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e.g. `osc_12.01.110_legacy.zip`).
2. 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.
3. 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.





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

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



5. Under **Destination USB stick**, select the USB storage medium on which you would like to save the installation data.

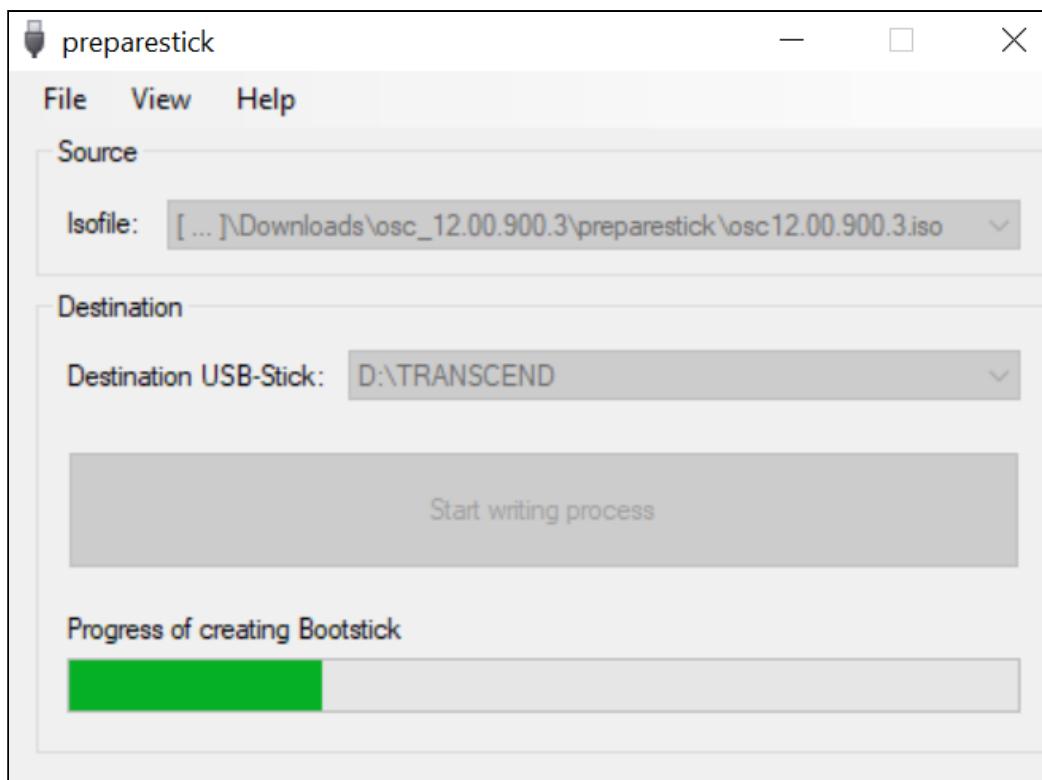
It is recommended that you only have one USB storage medium connected during this procedure. If you accidentally select the wrong medium, all data on it will be lost. Generally speaking, the list of available USB storage media is refreshed automatically. If, however, you would like to refresh it manually,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

6. Click **Start writing process**.

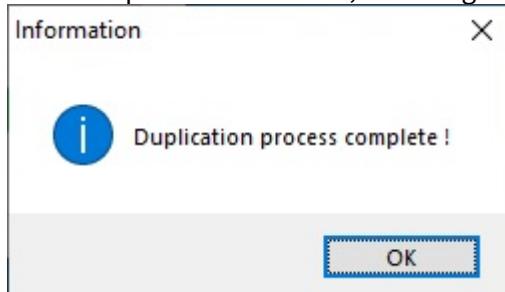
7. Confirm the following dialog:



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



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



8. Close the message window and the program.
9. 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.

General information on how to create a USB installation medium for Linux can be found under Create USB installation medium (Linux).



## Installation Procedure

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

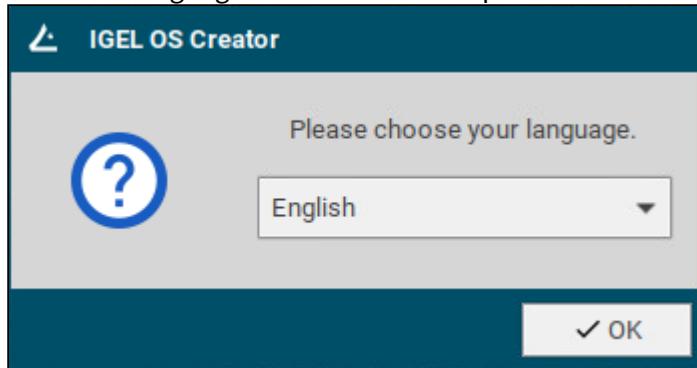
1. Connect the prepared USB memory stick to the target device and switch the target device on.
2. Select one of the following options from the boot menu:



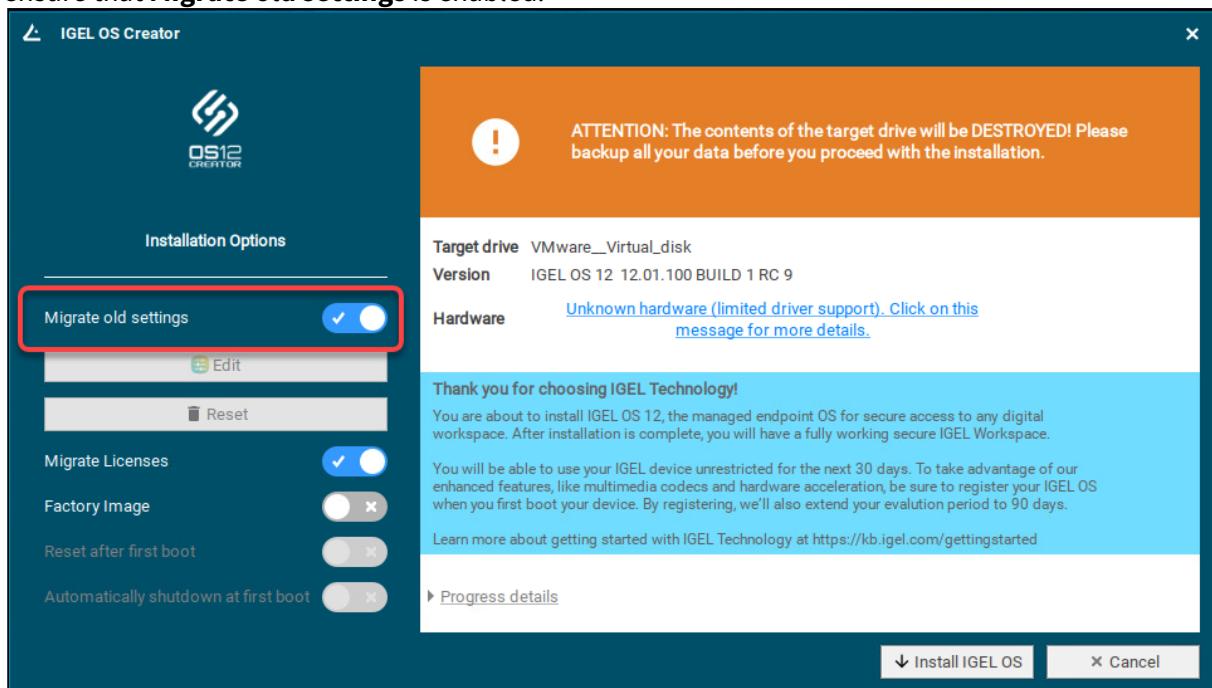
- **Standard Installation + Recovery:** Boots the system with just a few messages from the USB memory stick and launches the installation program. (Default)
- **Verbose Installation + Recovery:** Boots the system from the USB memory stick and shows the Linux boot messages in the process.
- **Failsafe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



3. Select the language for the installation process.



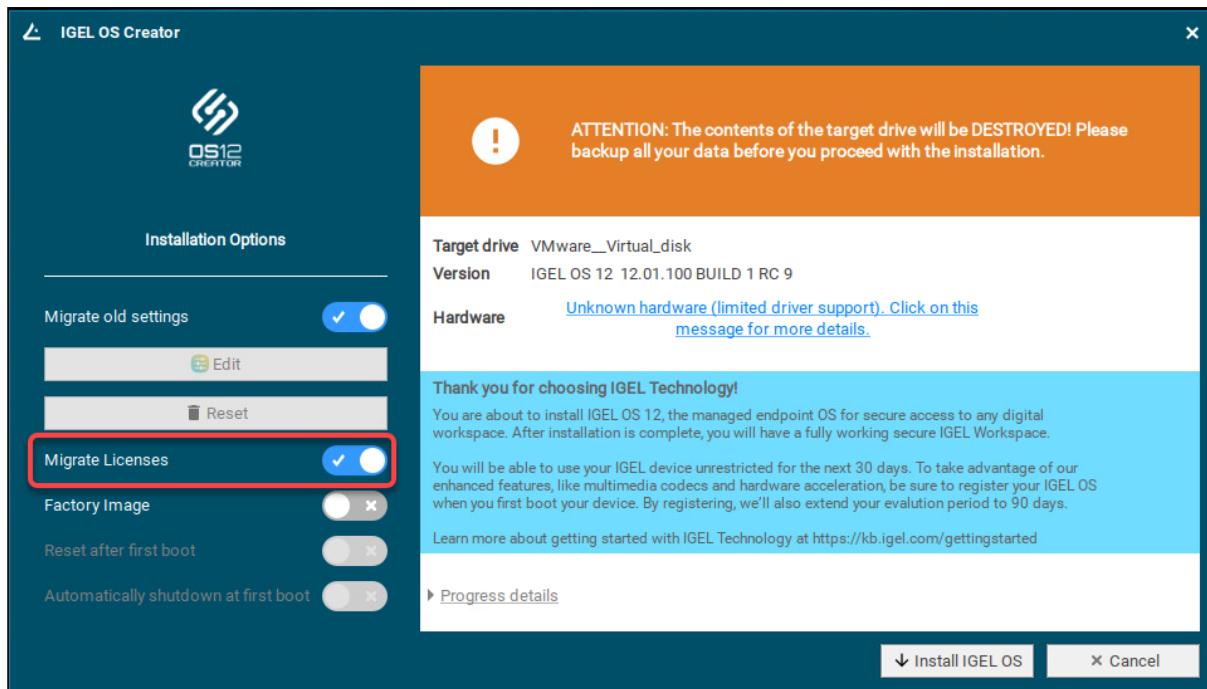
4. If IGEL OS 12 has been running on the device before and you want to preserve the device's settings, ensure that **Migrate old settings** is enabled.



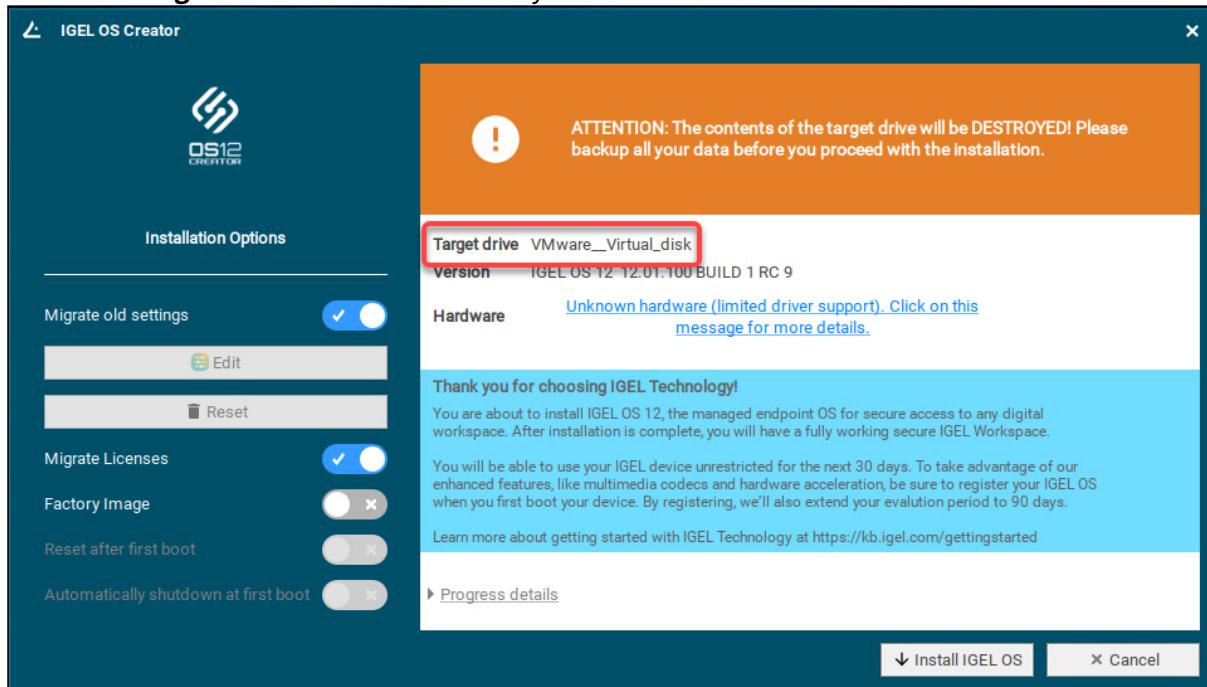
5. If one of the following is the case, make sure that **Migrate licenses** is enabled:

- Your device has been operating with IGEL OS 11 before and you want to preserve the device's IGEL OS 11 licenses because you want to test IGEL OS 12 and downgrade to IGEL OS 11 afterward
- Your device has been operating with IGEL OS 12 before and you want to keep the licenses on the device

## Installing the Base System via IGEL OS Creator (OSC)

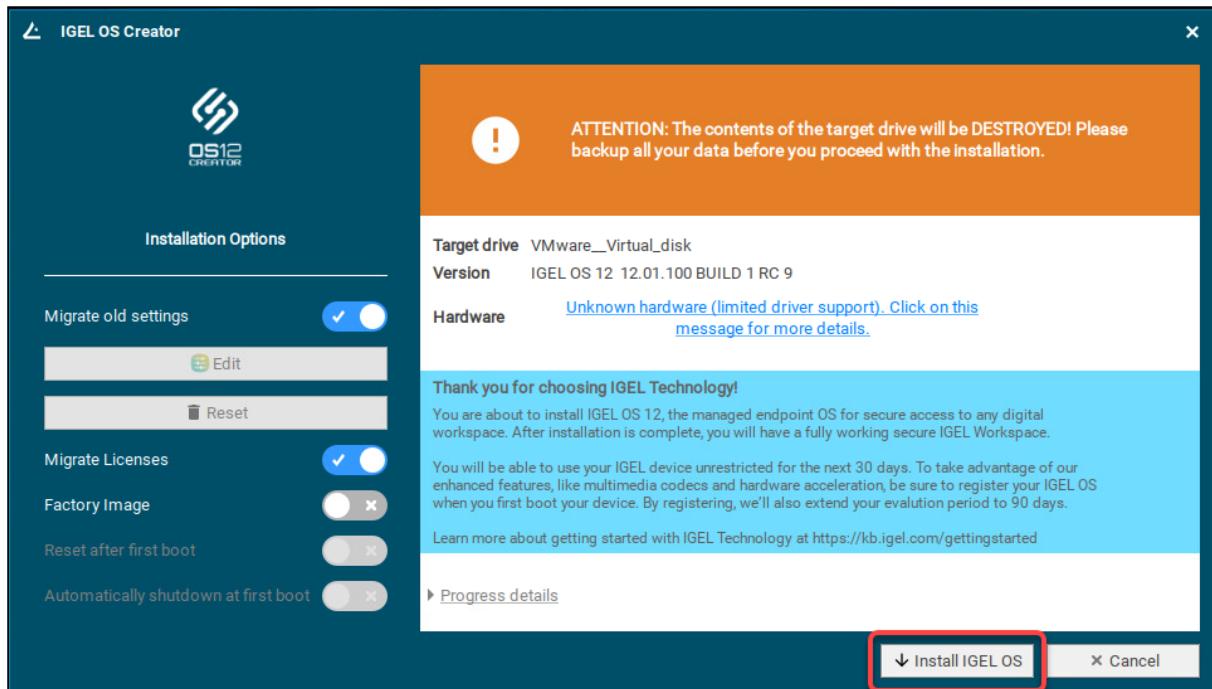


6. Check the **Target drive** to ensure that the system is installed on the desired drive.



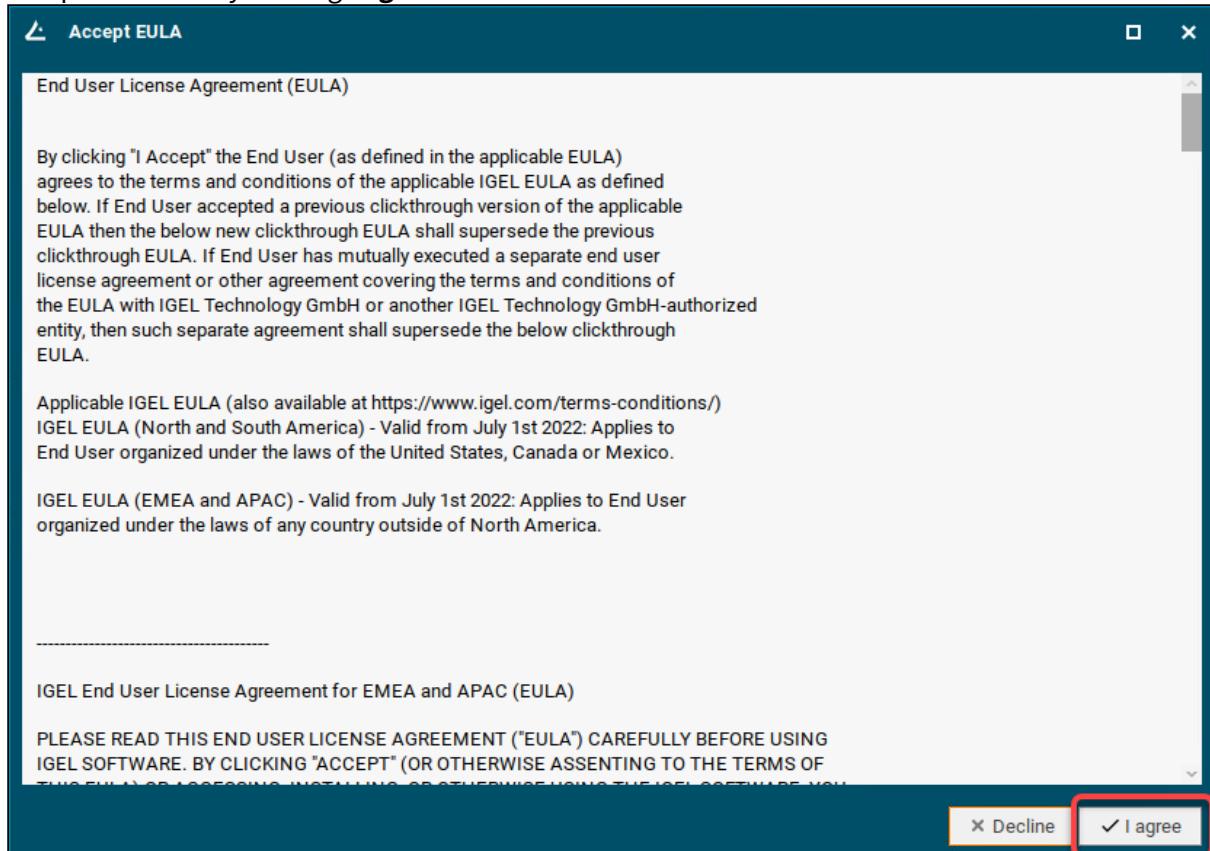


7. Click **Install IGEL OS**.



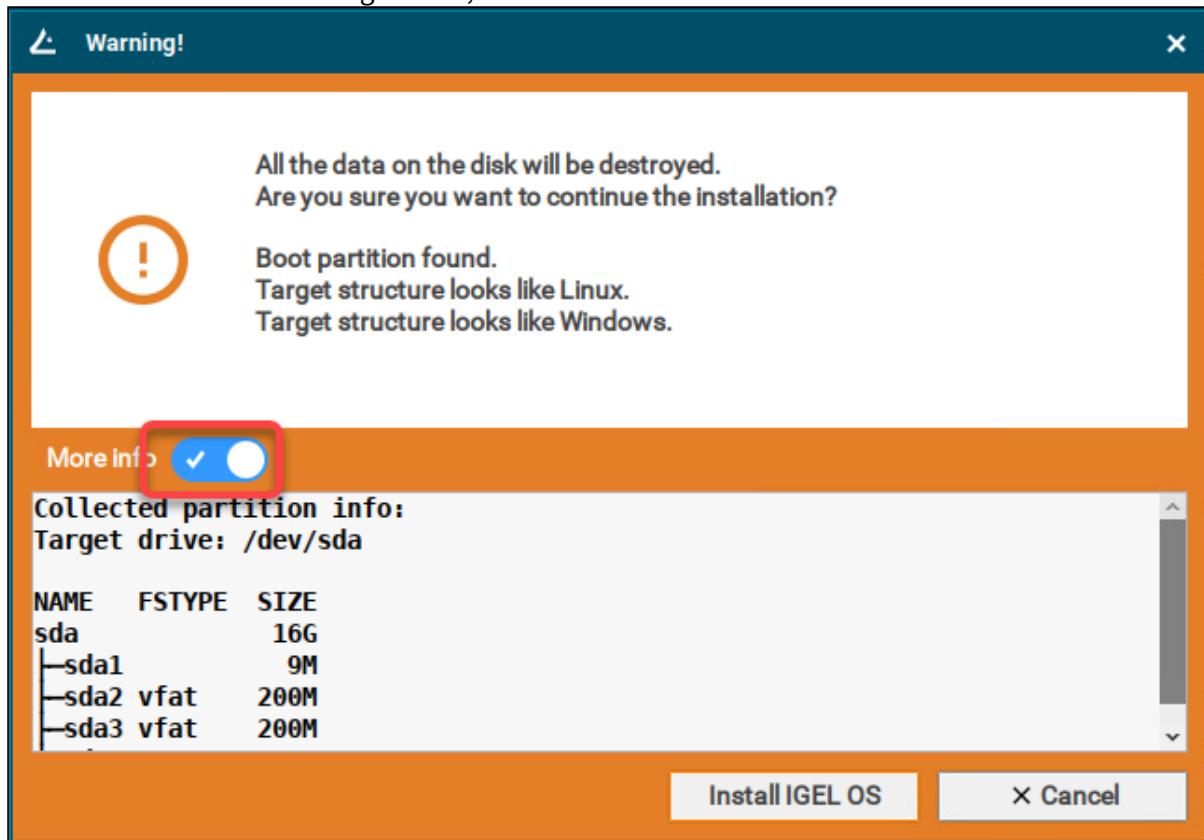


8. Accept the **EULA** by clicking **I agree**.



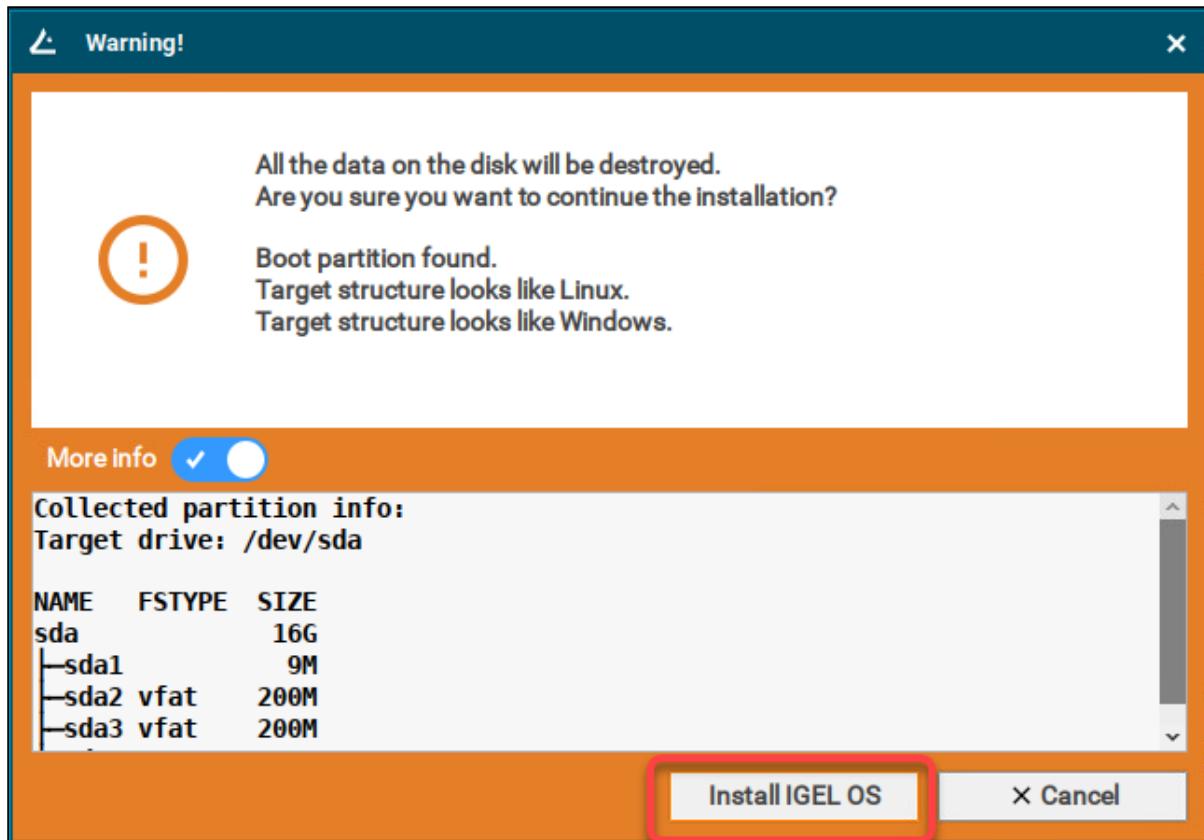


9. To view the details for the target drive, click **More Info**.



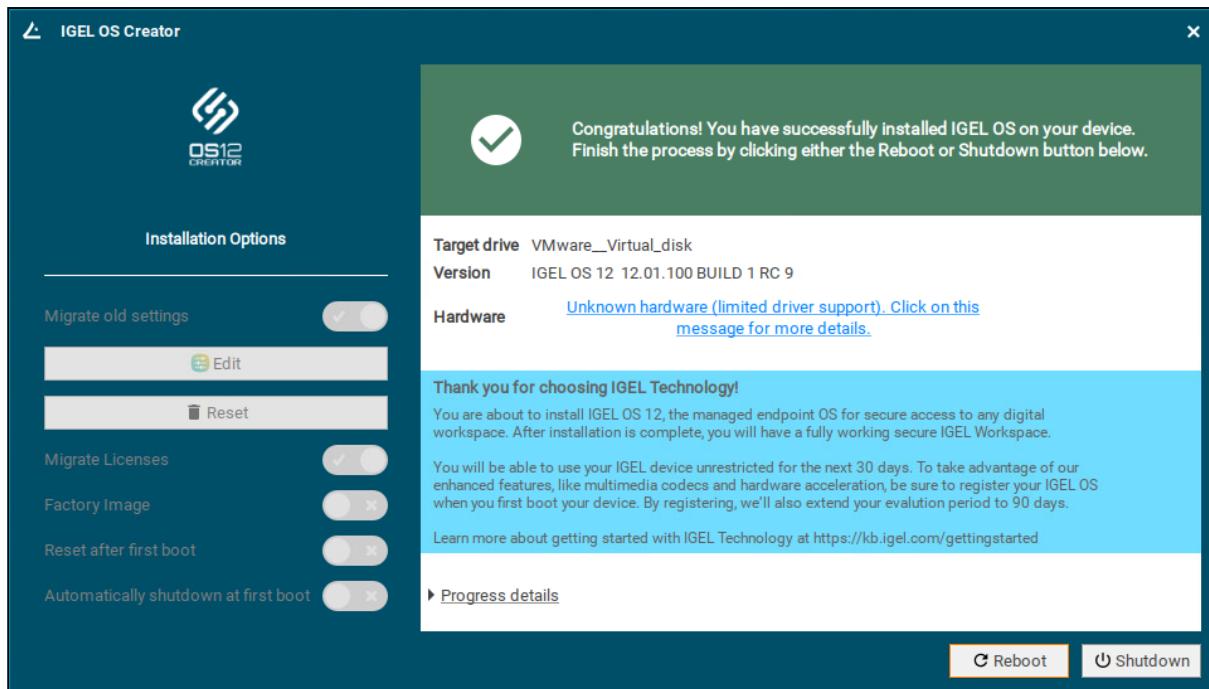


10. Click **Install IGEL OS**.

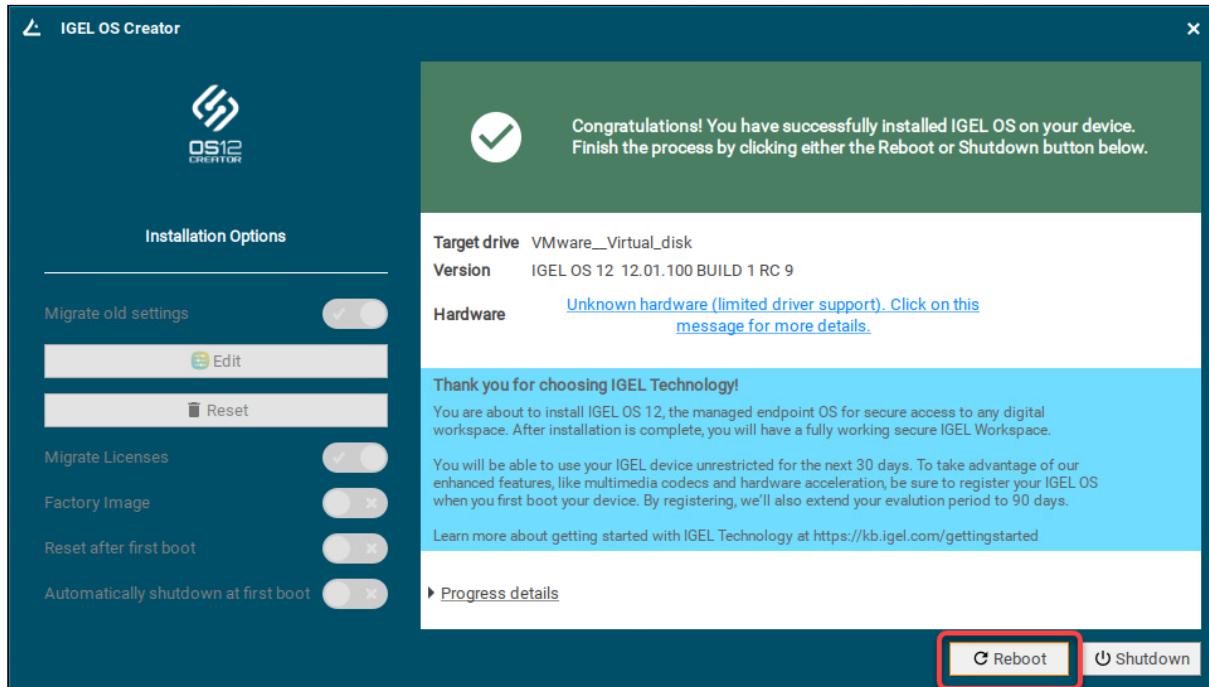


The installation program will install IGEL OS 12 on the target drive. If you see the success message, the installation is complete.

## Installing the Base System via IGEL OS Creator (OSC)



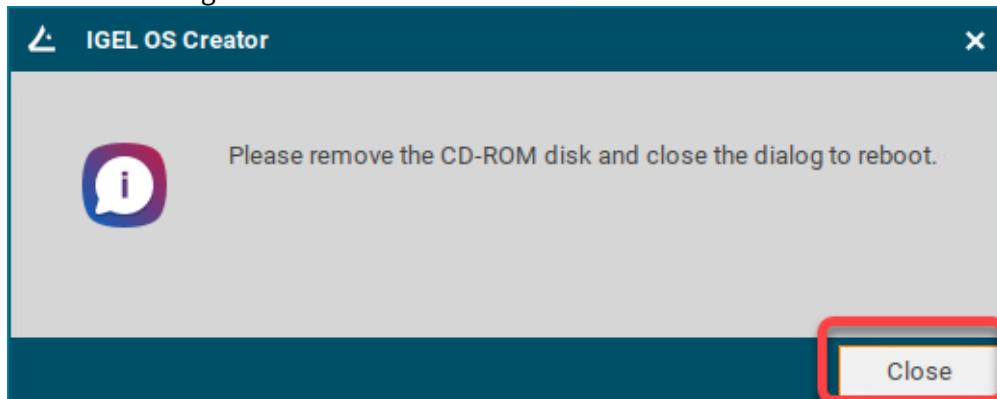
### 11. Click Reboot.



### 12. Remove the USB memory stick.



13. Close the message window.



The system will shut down and then boot IGEL OS 12.

The device is ready for onboarding; for details, see [Onboarding IGEL OS 12 Devices](#)(see page 126).



## Licensing

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

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

**⚠ EULA Must Be Accepted**

To prepare your licenses for deployment, you must accept the EULA for the Product Pack that contains your licenses. For instructions, see [Accepting the EULA](#)(see page 120).

## Starter License, Demo Licenses, and Limitations on Expiry

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

### Endpoint Device / Apps

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

\*Only if the device is managed by the UMS

### Remote Management (UMS)

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



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

## Onboarding Service (OBS)

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

## Getting Your Licenses Ready for Deployment

1. Log in to the IGEL License Portal (ILP) at <https://activation.igel.com><sup>14</sup>. 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).

<sup>14</sup> <https://activation.igel.com/>



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

The image consists of two screenshots of the IGEL COSMOS web interface. The top screenshot shows a navigation sidebar with the following items: Home, Orders, UMS ID, Search hardware, Multi-licensed hardware, Subscription Keys, Product Packs, Archived packs, and IGEL Knowledge Base. The 'UMS ID' item is highlighted with a red box. The bottom screenshot shows a list of UMS entries. One entry, 'td-ums12', is highlighted with a red box. To the right of this entry is a circular button containing a plus sign (+), which is also highlighted with a red box. Other entries in the list include a circled edit icon, a circled trash bin icon, a circled file icon, and a circled cube icon labeled '1'. A blue star icon is positioned above the 'td-ums12' entry.



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

The search bar contains "we-e" and the first row is selected, highlighted with a red box. The "Product" column shows "WE-E" and the "Product Pack ID" column shows "WE".

- 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.

✉ [\[redacted\]@igel.com](#) ▾

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



## Product Packs

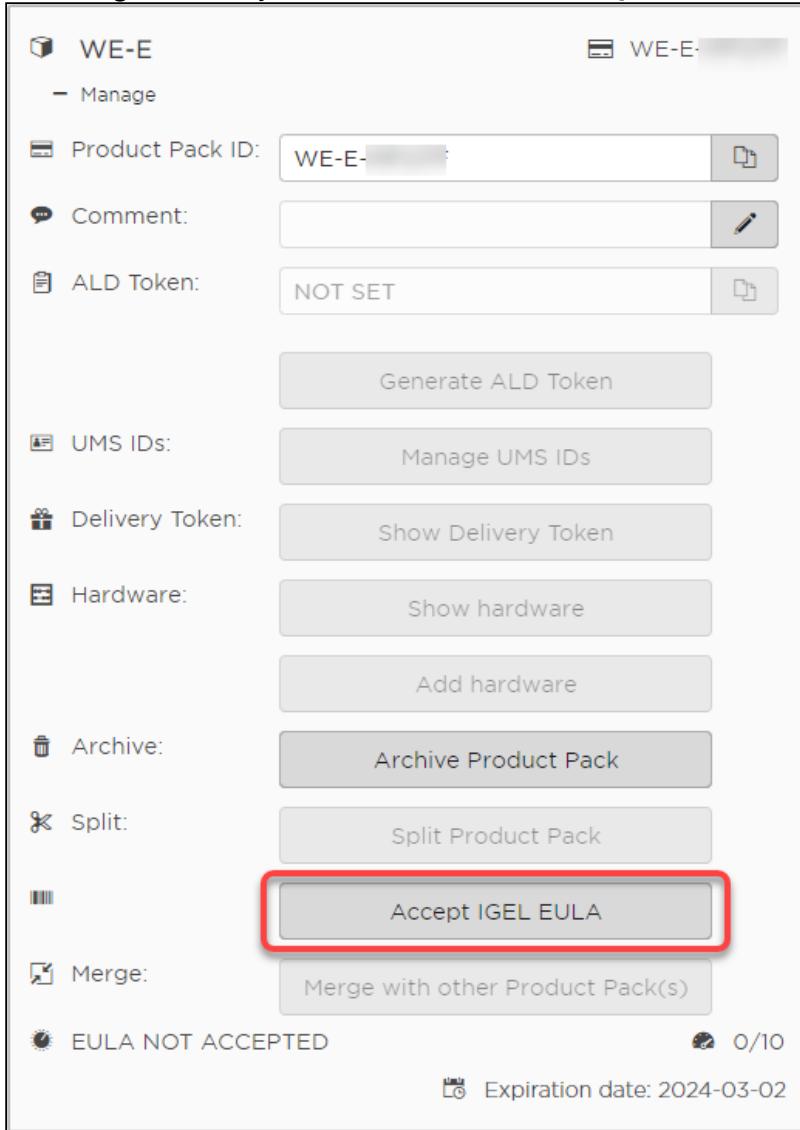
All WE-E Product Packs registered to IGEL Technology

Show all

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

List view Card view

Manage	Product	Product Pack ID	Subscription Key	Volume	Status	Activation Date	Expiration date
<a href="#">+</a>	WE-E	WE-E [REDACTED]		0/10	EULA NOT ACCEPTED		2024-03-02

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

The screenshot shows the 'WE-E' Product Pack details page. At the top, there's a 'Manage' link and a 'Product Pack ID' field set to 'WE-E-'. Below that are fields for 'Comment' and 'ALD Token' (set to 'NOT SET'), each with a edit icon. A 'Generate ALD Token' button is available. Under 'UMS IDs', there's a 'Manage UMS IDs' button. Under 'Delivery Token', a 'Show Delivery Token' button is present. Under 'Hardware', there are 'Show hardware' and 'Add hardware' buttons. An 'Archive' button leads to 'Archive Product Pack'. A 'Split' button leads to 'Split Product Pack'. The central button, 'Accept IGEL EULA', is highlighted with a red rectangular border. Below it, a 'Merge' button leads to 'Merge with other Product Pack(s)'. At the bottom left, a note says 'EULA NOT ACCEPTED'. On the right, a progress bar shows '0/10' and an expiration date of '2024-03-02'.



6. Confirm that you accept the EULA.

Accept IGEL EULA

I have read and agree to the [licence terms](#) stated in the IGEL EULA.

Confirm Cancel

Your licenses are ready for deployment.

You can continue with Setting up Automatic License Deployment (ALD).



## Onboarding IGEL OS 12 Devices

If you have [configured the IGEL Onboarding Service](#)(see page 39), you use it to register your IGEL OS 12; see [Register IGEL OS 12 Devices with the UMS via IGEL Onboarding Service](#)(see page 126).

For an alternative device registration method, see [Alternative Onboarding Method: Registering Devices with the UMS Using the One-Time Password](#)(see page 133).

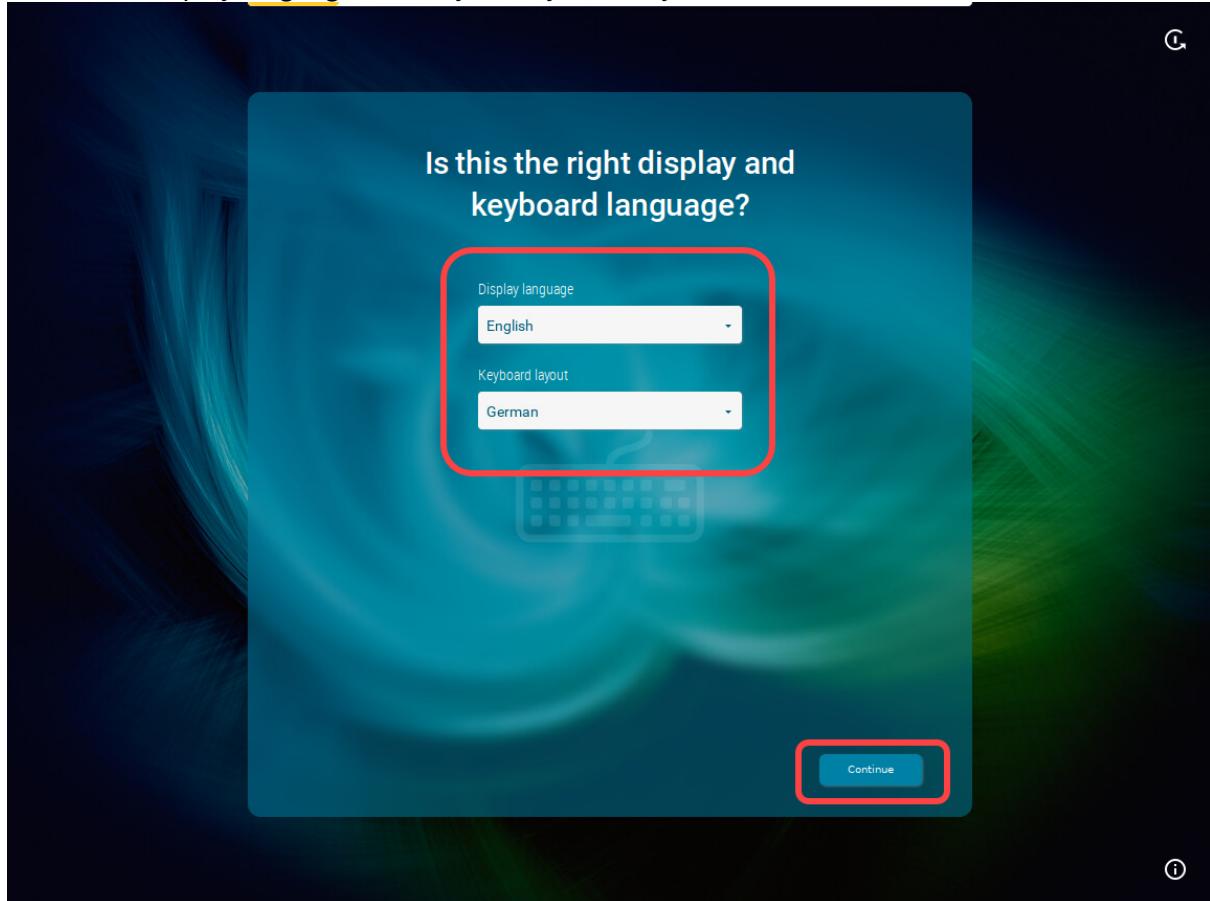
- ⓘ If you decide for some reason not to use the IGEL Onboarding Service or the one-time password method, you can skip the corresponding steps in the Setup Assistant. Your IGEL OS 12 device will start with a [Starter license](#)(see page 119).  
To register this device with the UMS Server, you can use the **Scan for devices** function in the UMS Console, see [Scanning the Network for Devices and Registering Devices on the IGEL UMS](#). For other device registration methods, see [Registering IGEL OS Devices on the UMS Server](#).

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

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

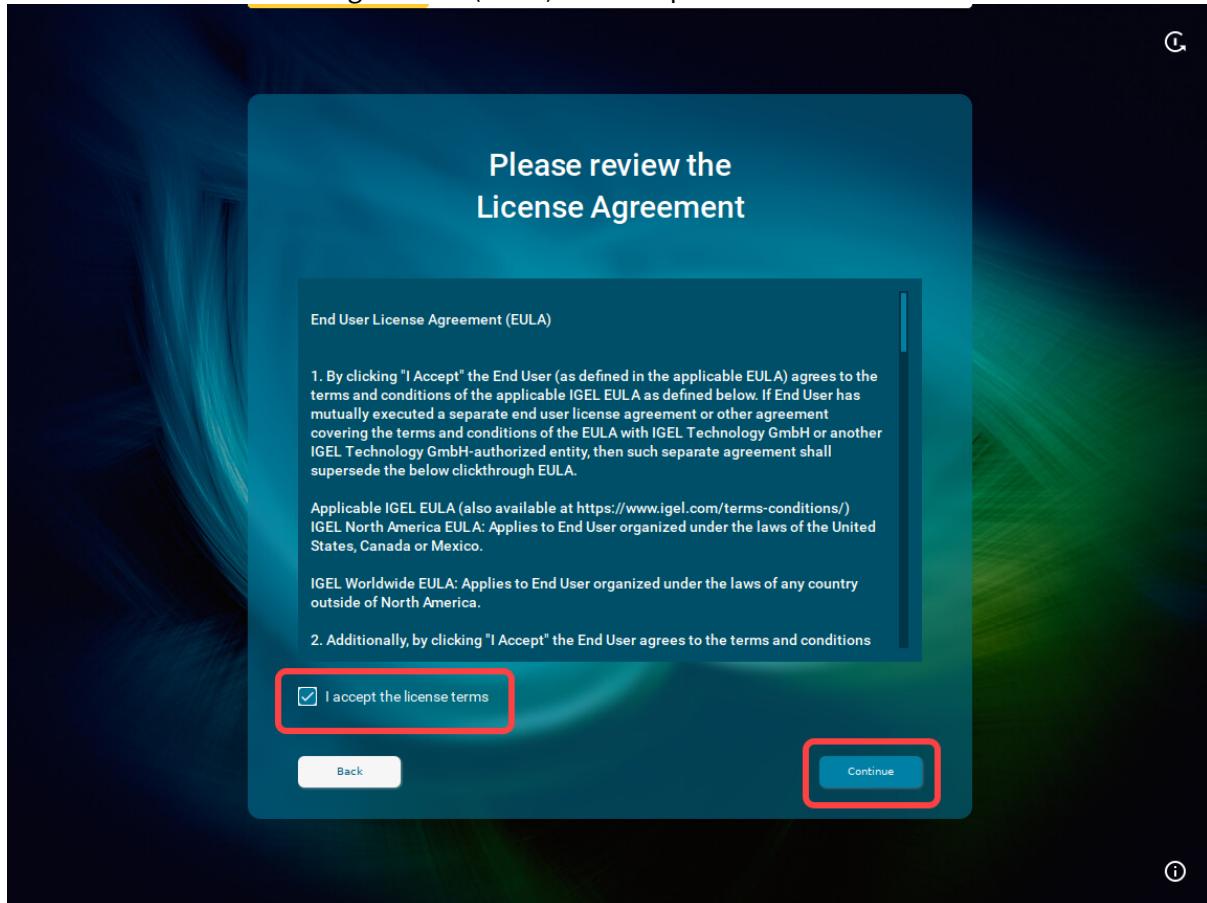


2. Choose the display language and set your keyboard layout. Click **Continue**.

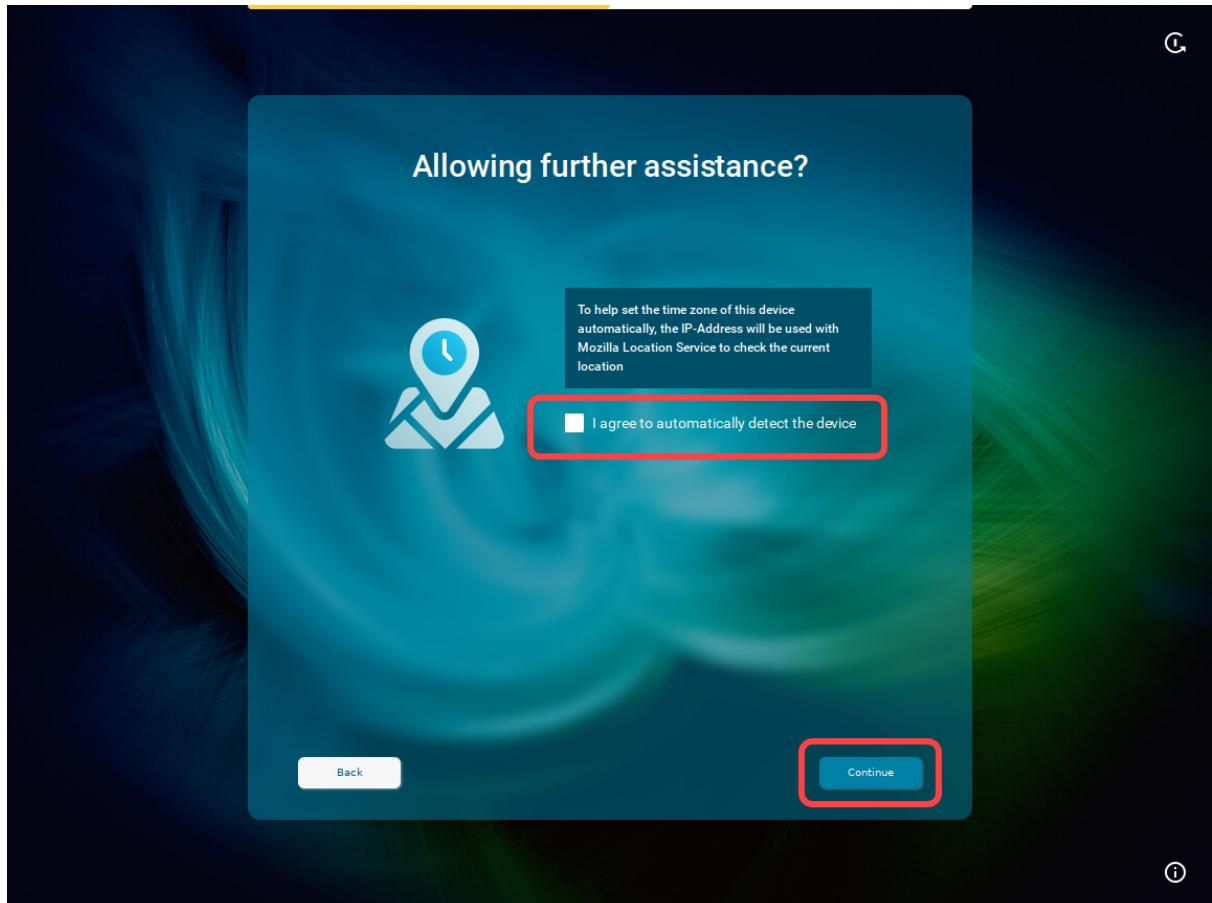




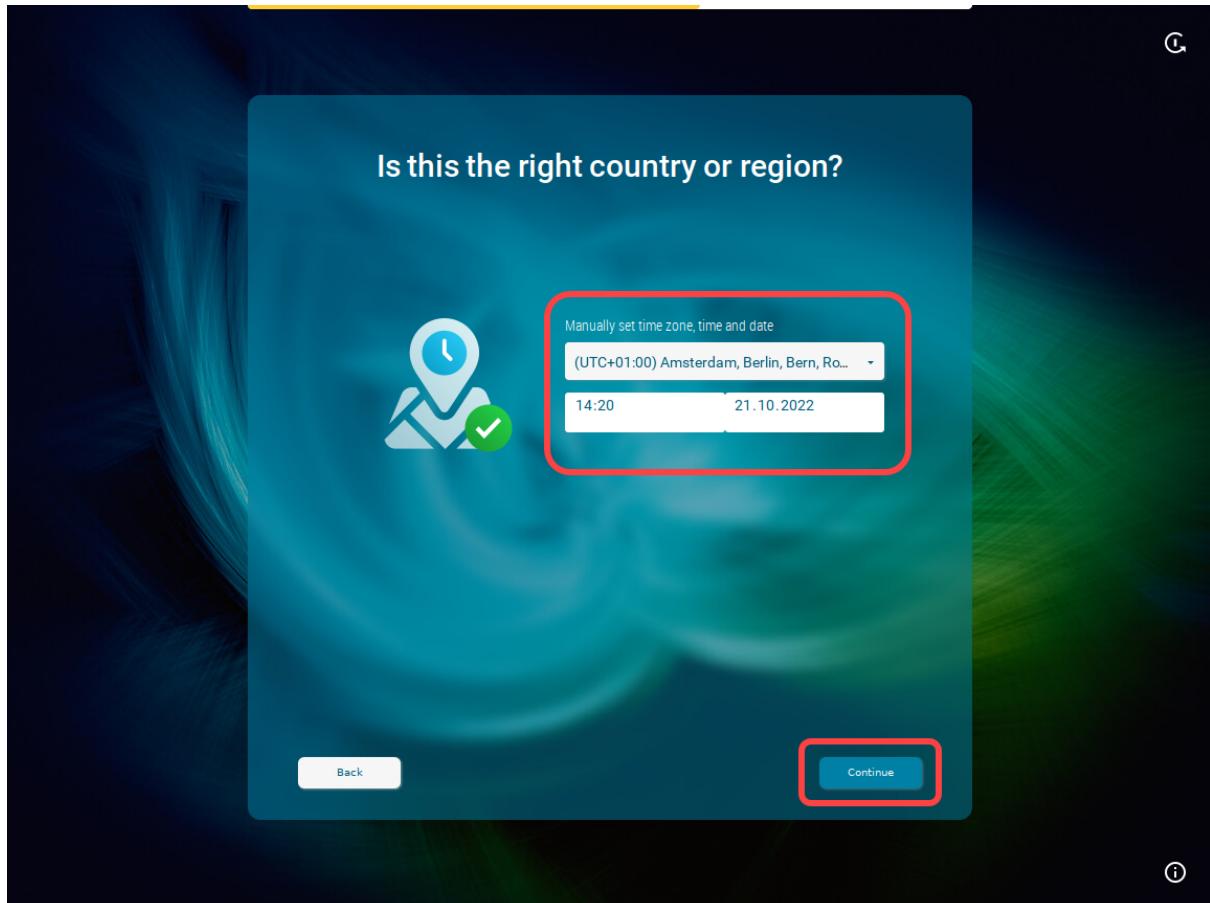
3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.



4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under [Troubleshooting: Configuring a Network during the Onboarding](#)(see page 142).
5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.

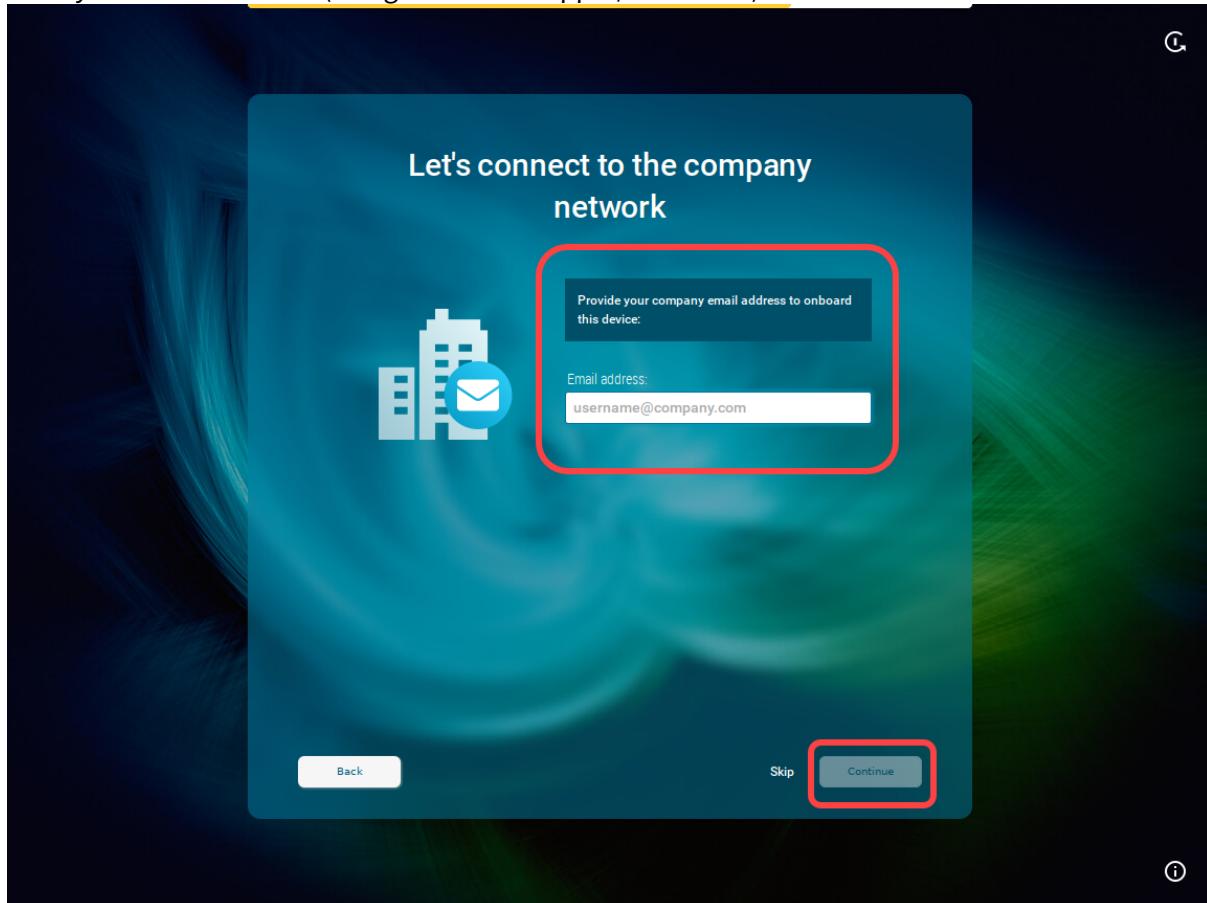


Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.





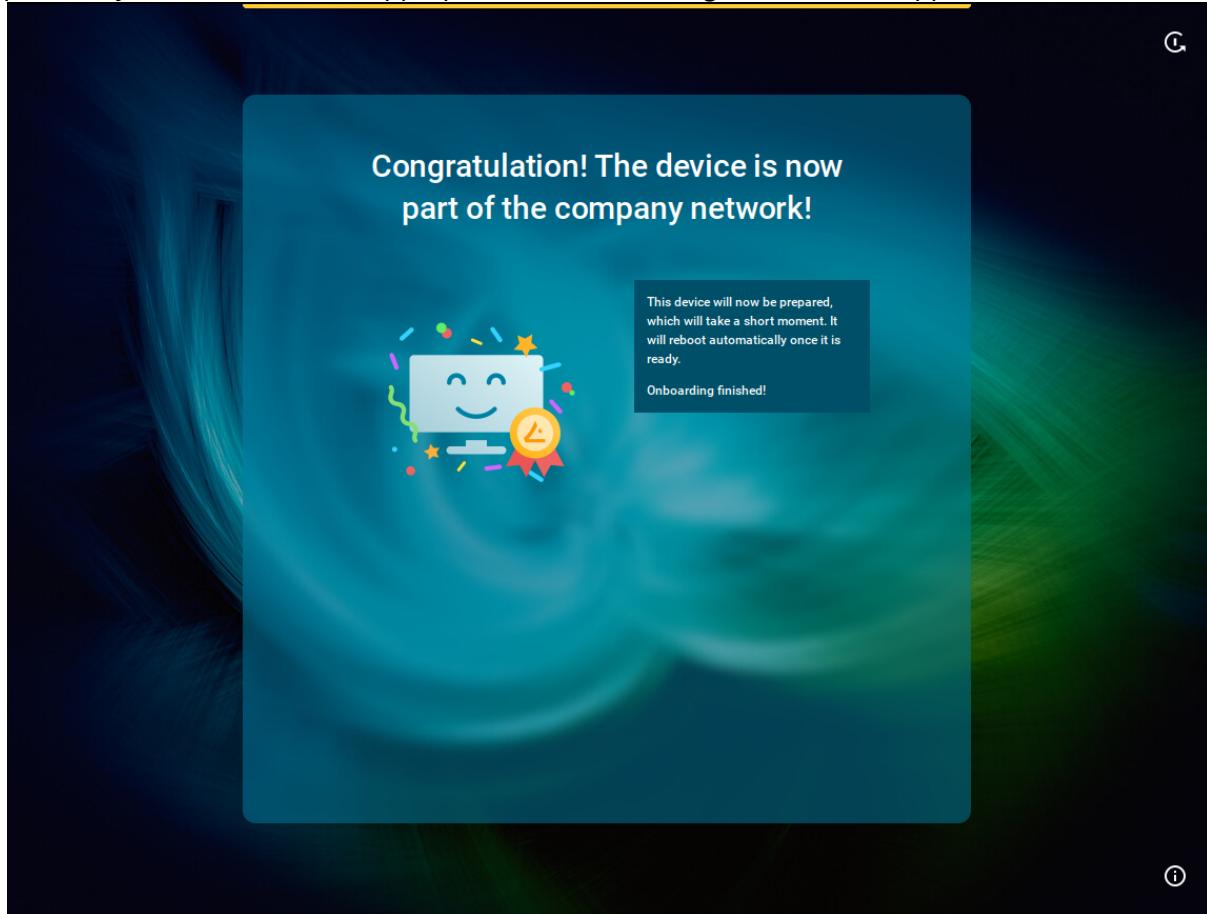
6. Enter your e-mail address (using the correct upper/lowercase) and click **Continue**.



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



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



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

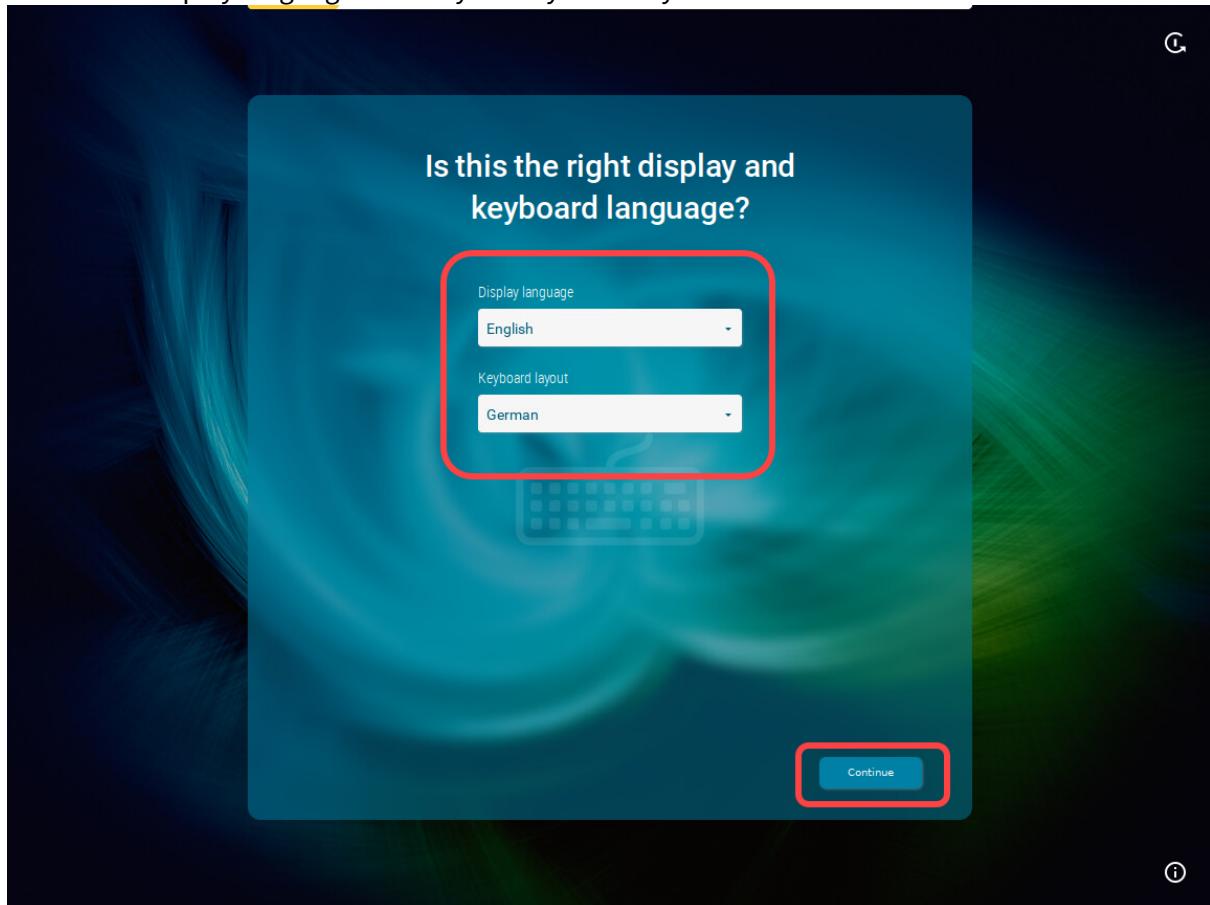
A screenshot of the UMS Web App interface. The top navigation bar includes "Devices", "Configuration", "Apps", "Search", "App Portal", "Help", "English", and a refresh icon. The left sidebar shows a "Directory Tree" with "Devices (1)" under "newly-registered (0)". The main content area shows a list of devices under "renata" with one item: "ITC00E0C51A75F4" (00E0C51A75F4, 12.1.100-1.rc.10+1, UC1-LX Starter). On the right, a detailed view for "ITC00E0C51A75F4" shows tabs for "Edit Configuration", "Shadow", "Assign object", "Reboot", and "Shutdown". Under "Custom Properties", the "System Information" tab is highlighted with a red box and arrow. It shows "Onboarded by: IGEL US base System". Another red arrow points to the "Onboarded by" field in the "Assigned Objects" section of the "System Information" tab, which also lists "Comment" and "Onboarded by".



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

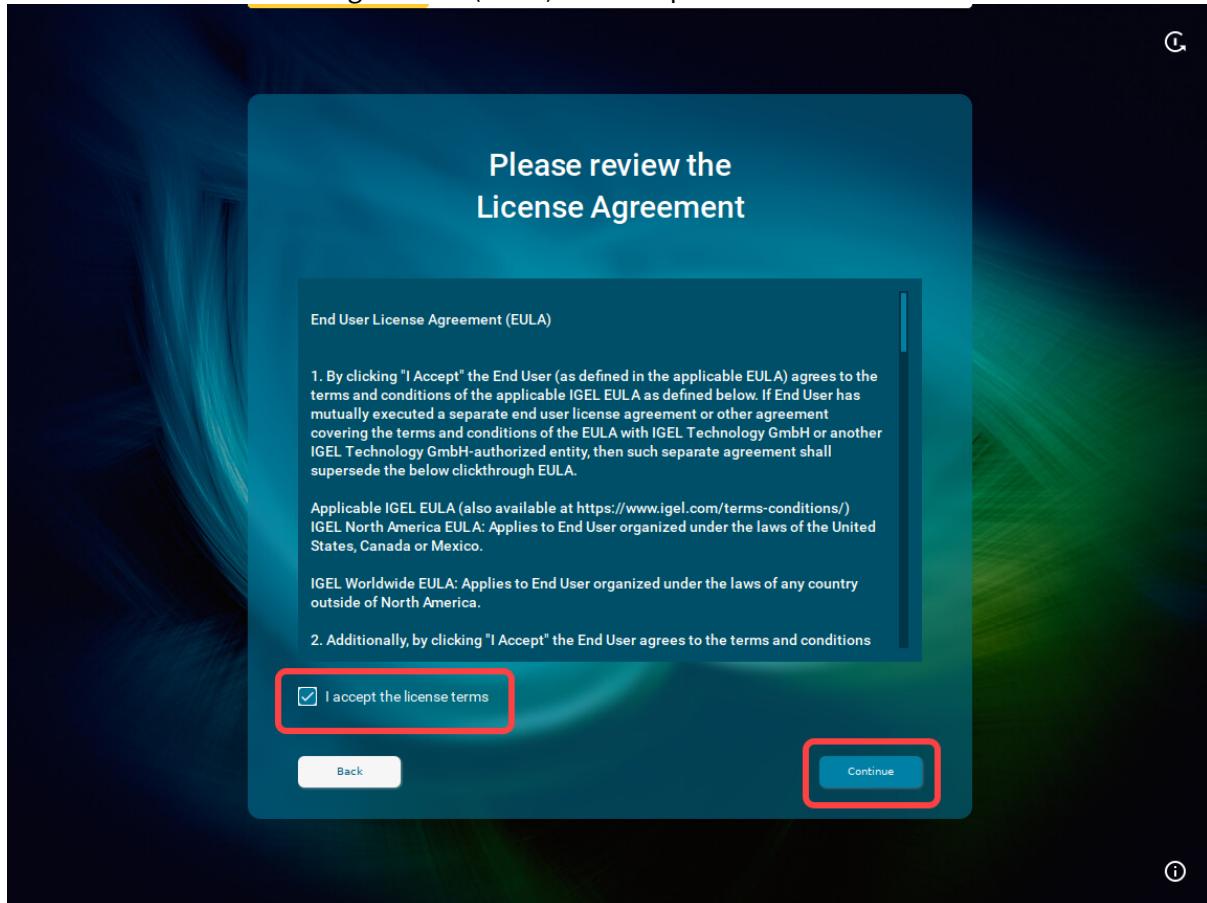
If you decided not to use IGEL Onboarding Service for the registration of your IGEL OS 12 devices, you can use a one-time password method as an alternative.

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

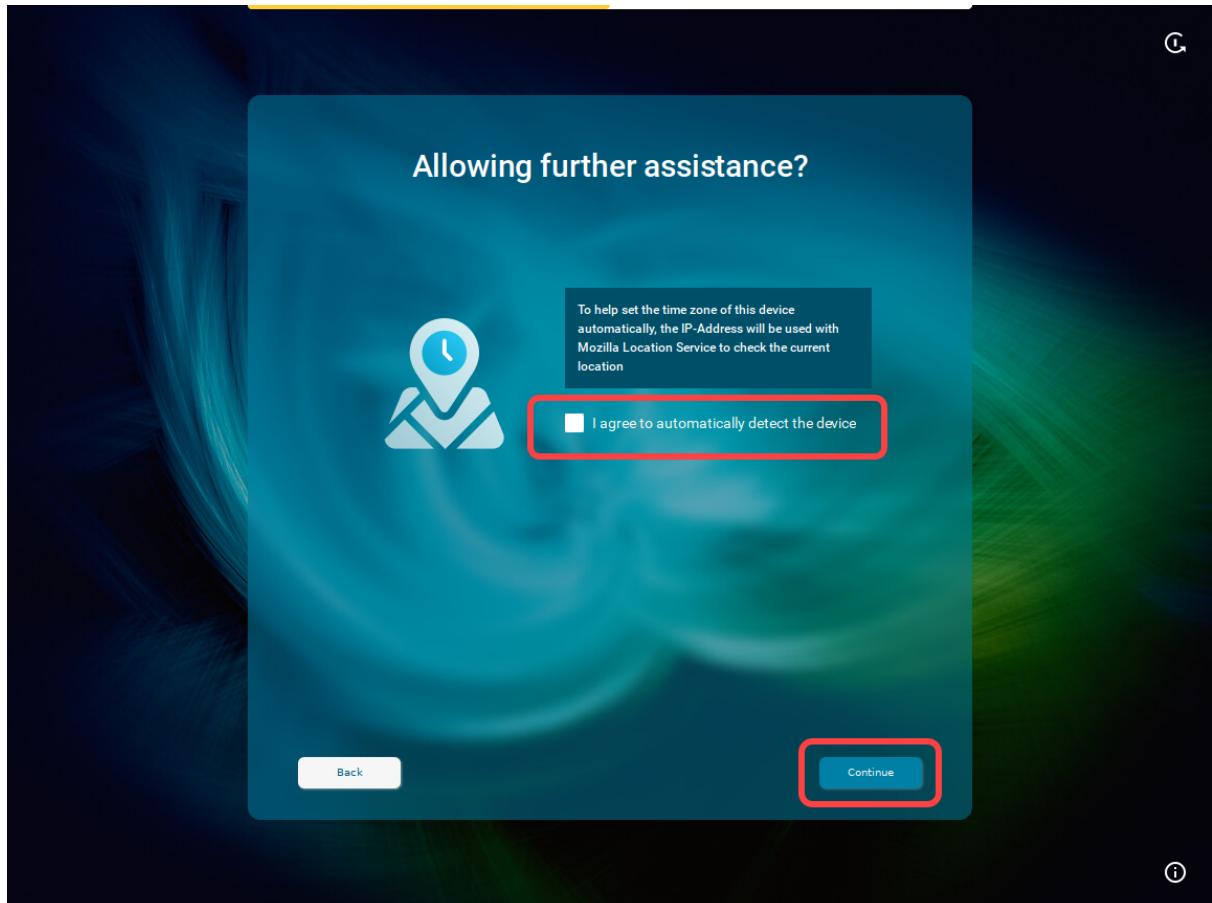




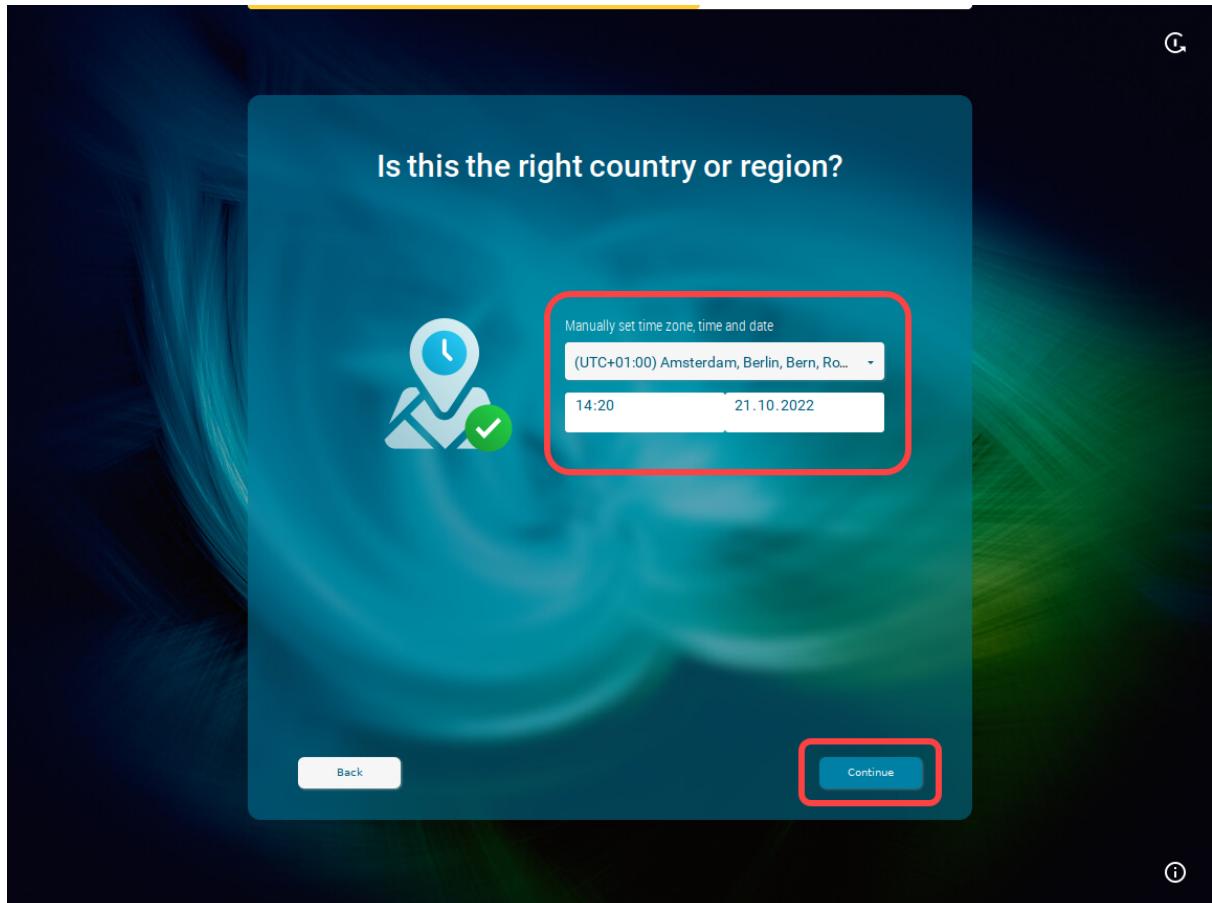
3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.



4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under [Troubleshooting: Configuring a Network during the Onboarding](#)(see page 142).
5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.

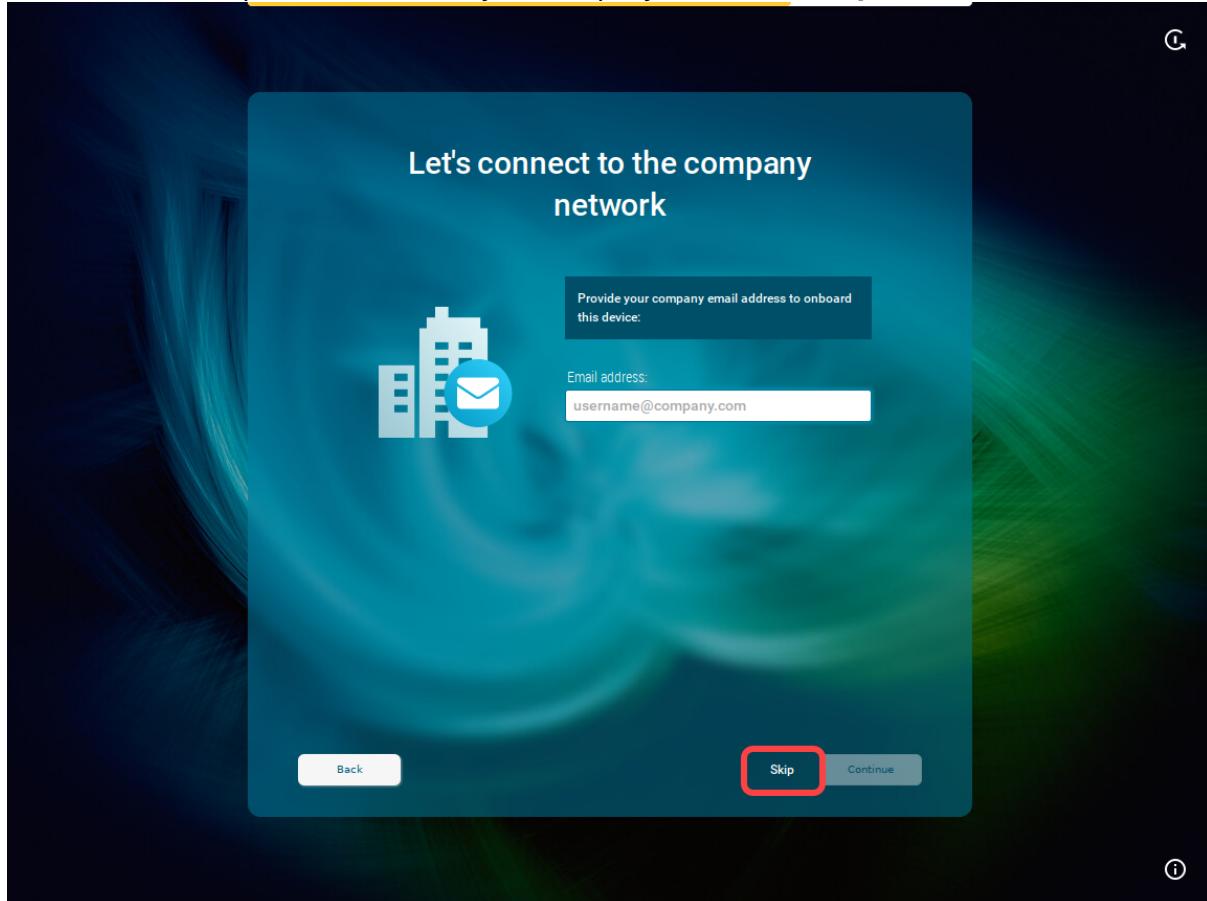


Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.

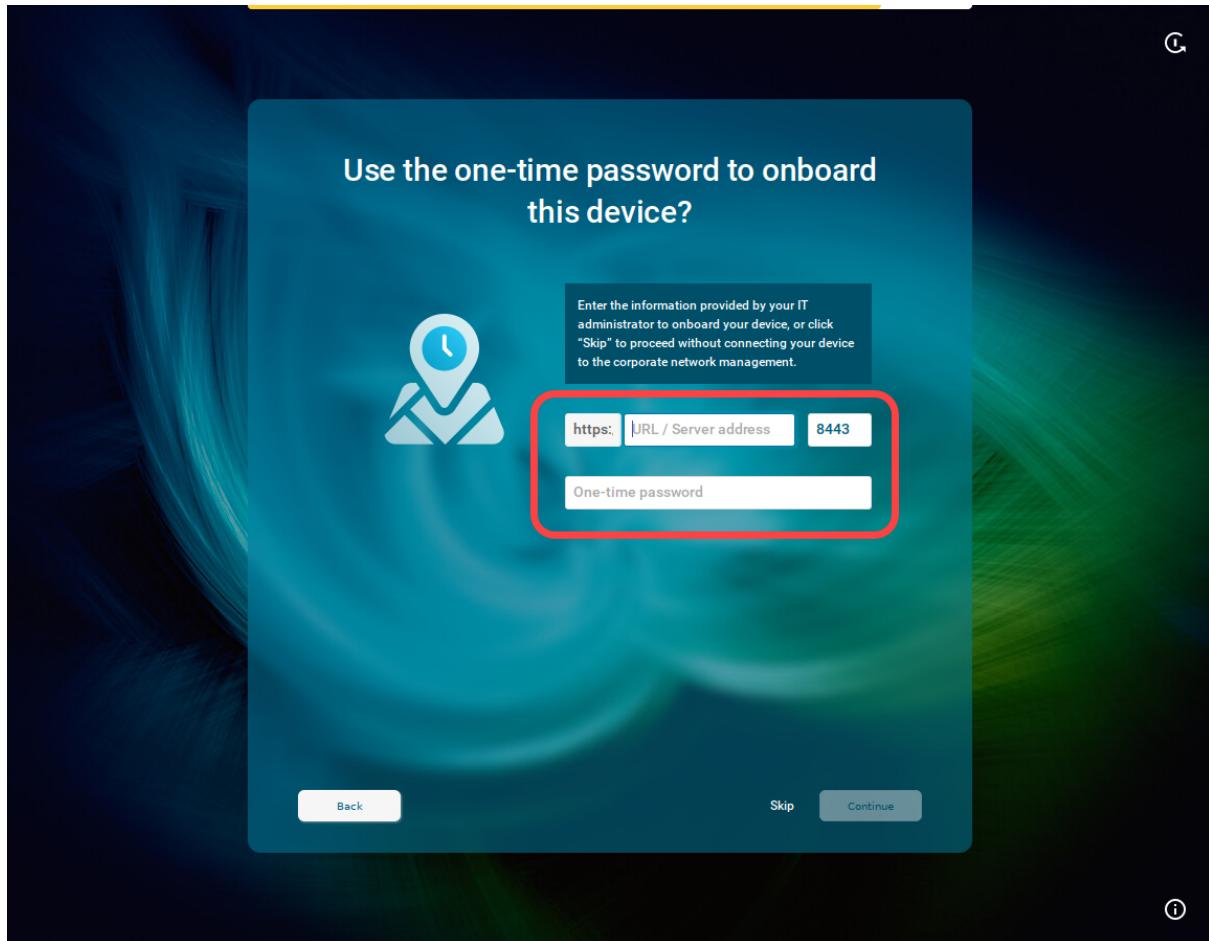




6. When the IGEL Setup Assistant asks for your company e-mail, click **Skip**.



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



7. Enter the following data and click **Continue**:

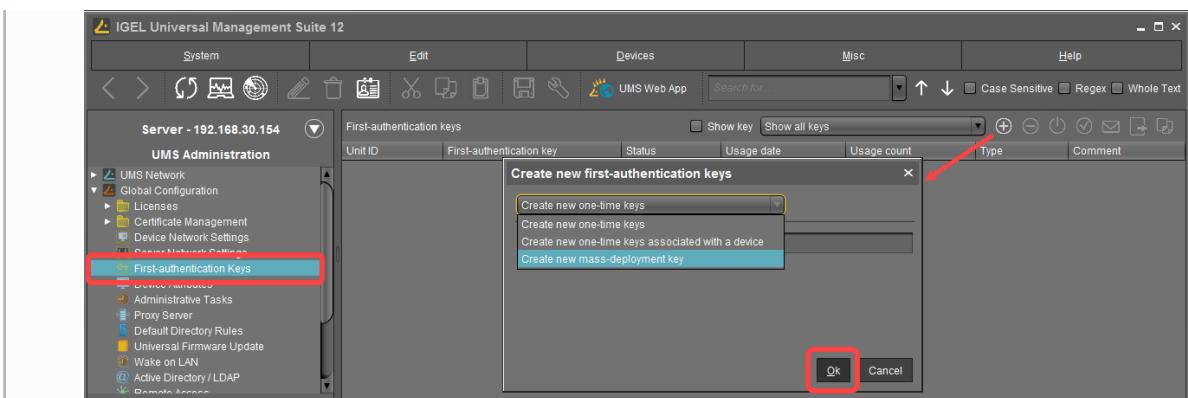
**URL / Server address:** Host name or IP address of the UMS Server. If configured, you can alternatively use the Public Address of the UMS Server or Cluster Address.

**Port:** Web server port (Default: 8443). If configured, you can alternatively use the Public Web Port or Cluster Address Port.

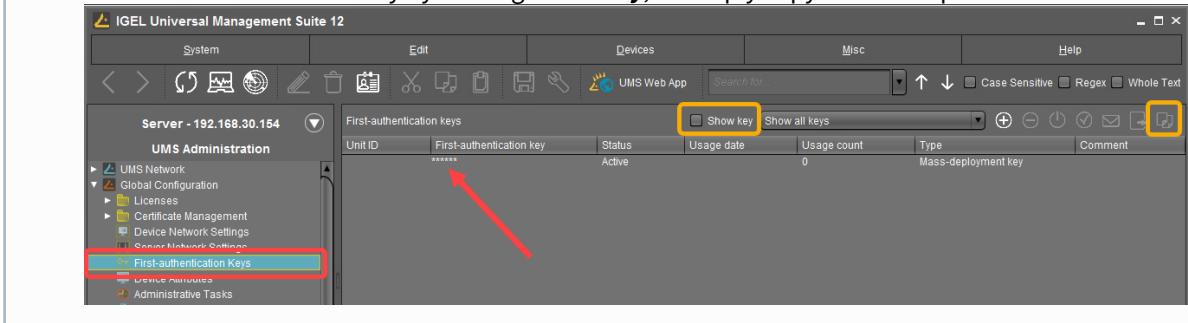
**One-time password:** First-authentication key (no matter one-time key or mass-deployment key), which you create under **UMS Console > UMS Administration > Global Configuration > First-authentication Keys**.

(i) **Creating a one-time password in the UMS Console**

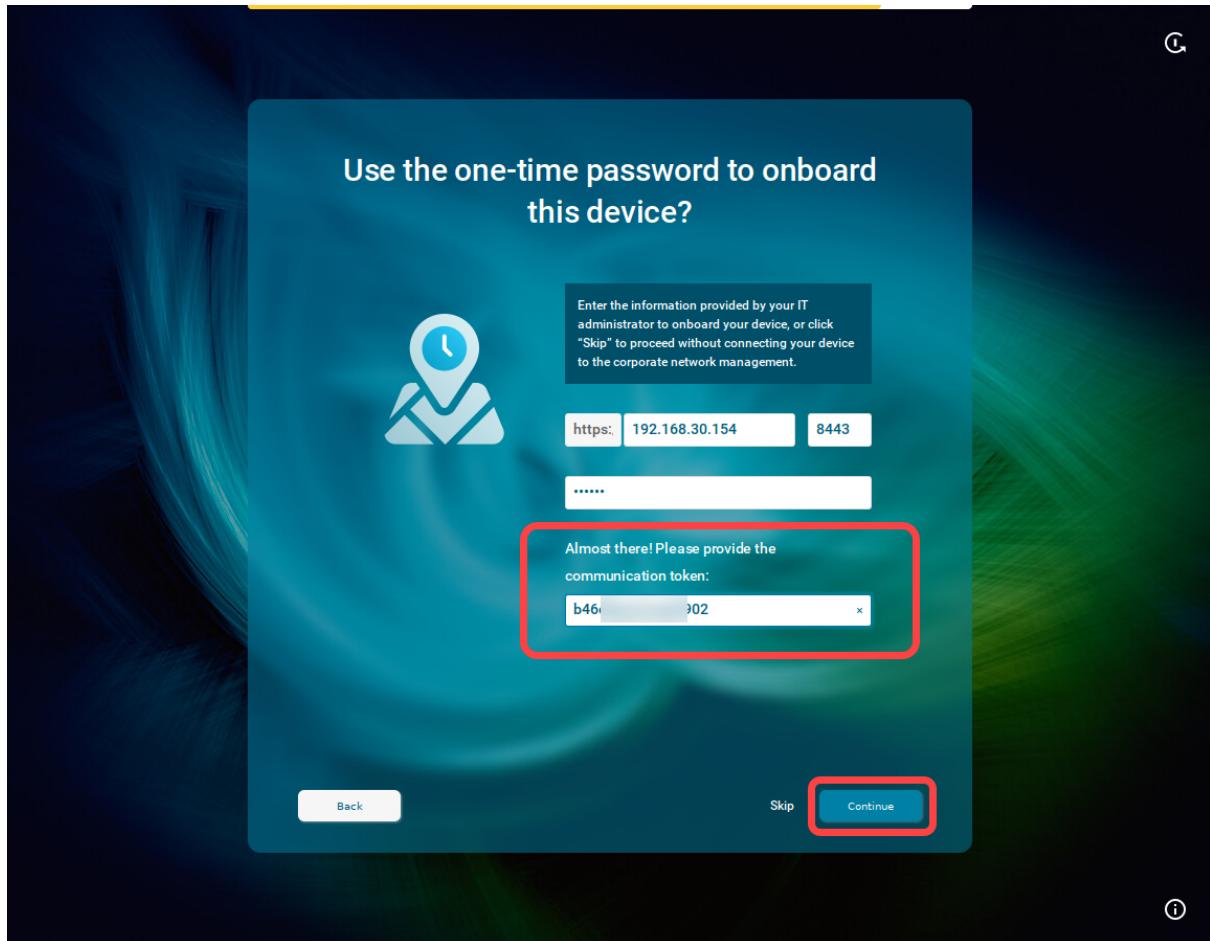
**Tip:** If you choose to create a mass-deployment key, there is a possibility to set your own password.



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



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



- 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 .

## Onboarding IGEL OS 12 Devices



**IGEL Universal Management Suite 12**

Server - 192.168.30.154

UMS Administration

- UMS Network
- Global Configuration
- Licenses
- Certificate Management
- Device Communication
- Web (highlighted with red box)
- Cloud Gateway
- Mobile Devices
- Device Network Settings
- Server Network Settings

Web Certificates

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

**Server status: OK** All servers have an assigned certificate. (1 / 1) **Certificate status: OK** All used certificates are valid and derive from the same root.

Automatic renewal  
Used certificates will be renewed automatically.

Display name	Subject Alternative Names	Expiring date	Key Specification	Signature	Used	Private Key Known
1526291218	192.168.30.154;td-ums-srv2016	Jul 12, 2042	RSA (4096 bits)	SHA512withRSA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2082661758	192.168.30.154;td-ums-srv2016	Jul 12, 2023	RSA (4096 bits)	SHA512withRSA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Version: 3

Subject: C=DE, L=Bremen, O=IGEL Technology GmbH, CN=ID--49679-1665998

Issuer: C=DE, L=Bremen, O=IGEL Technology GmbH, CN=ID--49679-1665998

Signature Algorithm: SHA512withRSA

Key: RSA, 4096 bits

Serial number: [REDACTED]

Fingerprint (SHA1): [REDACTED]

Fingerprint (SHA256): b46c 1902

Valid from: Mon Oct 17 11:20:02 CEST 2022

Valid to: Fri Oct 17 11:20:02 CEST 2042

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

UMS 12

Devices Configuration Apps Network Logging Search Help English

review-UMS12

UMS Server Details

Process ID: f9be4402-a919-4ddc-96dd-42cbef97930c
Last Change: October 20, 2022
Cluster ID: UMS-CLUSTER-49679-1665998487122-2-0
Operating System: Microsoft Windows Server 2019 Standard
Host Name: review-UMS12
Process Type: UMS_SERVER
Port: 30001
Version: 12.00.900.rc3
Cert. Fingerprint - Part 1
Cert. Fingerprint - Part 2
Cert. Fingerprint - Part 3
Cert. Fingerprint - Part 4
Root Cert. Fingerprint - Part 1
Root Cert. Fingerprint - Part 2
Root Cert. Fingerprint - Part 3: b46c 1902
Root Cert. Fingerprint - Part 4

Copy to Clipboard

Waiting Failed

12:05 PM 12:10 PM 12:15 PM 12:20 PM 12:25 PM 12:30 PM 12:35 PM 12:40 PM 12:45 PM 12:50 PM 12:55 PM 1:00 PM 1:05 PM 1:10 PM 1:15 PM 1:20 PM 1:25 PM 1:30 PM 1:35 PM 1:40 PM 1:45 PM 1:50 PM 1:55 PM 2:00 PM 2:05 PM 2:10 PM 2:15 PM 2:20 PM 2:25 PM 2:30 PM 2:35 PM 2:40 PM 2:45 PM 2:50 PM 2:55 PM 3:00 PM 3:05 PM 3:10 PM 3:15 PM 3:20 PM 3:25 PM 3:30 PM 3:35 PM 3:40 PM 3:45 PM 3:50 PM 3:55 PM 4:00 PM 4:05 PM 4:10 PM 4:15 PM 4:20 PM 4:25 PM 4:30 PM 4:35 PM 4:40 PM 4:45 PM 4:50 PM 4:55 PM 5:00 PM 5:05 PM 5:10 PM 5:15 PM 5:20 PM 5:25 PM 5:30 PM 5:35 PM 5:40 PM 5:45 PM 5:50 PM 5:55 PM 6:00 PM



**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:

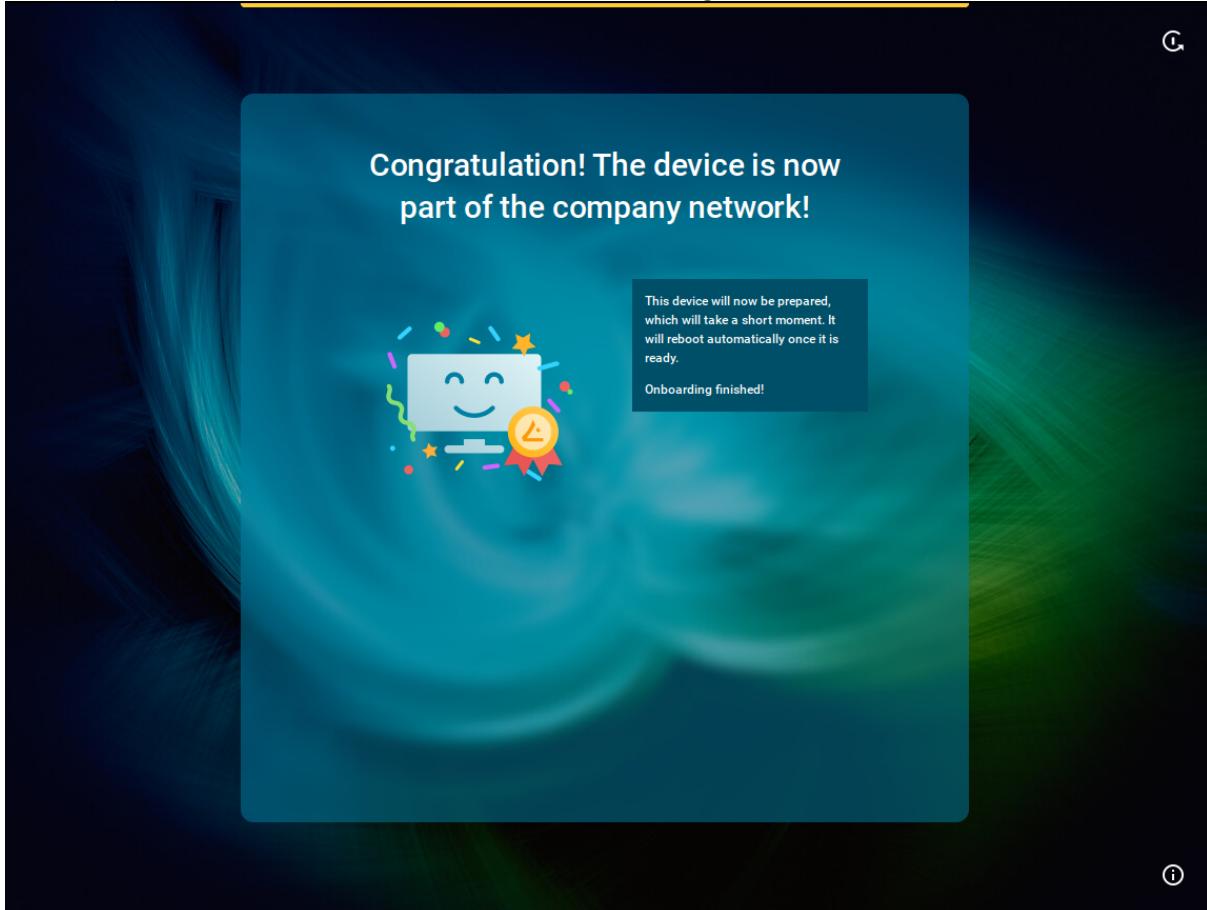
**URL / Server address:** Host name or IP address of the ICG server

**Port:** ICG port (Default: 8443)

**One-time password:** First-authentication key created as described above

**Communication token:** Fingerprint of the root certificate of the ICG server (the third part)

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



## Troubleshooting: Configuring a Network during the Onboarding

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

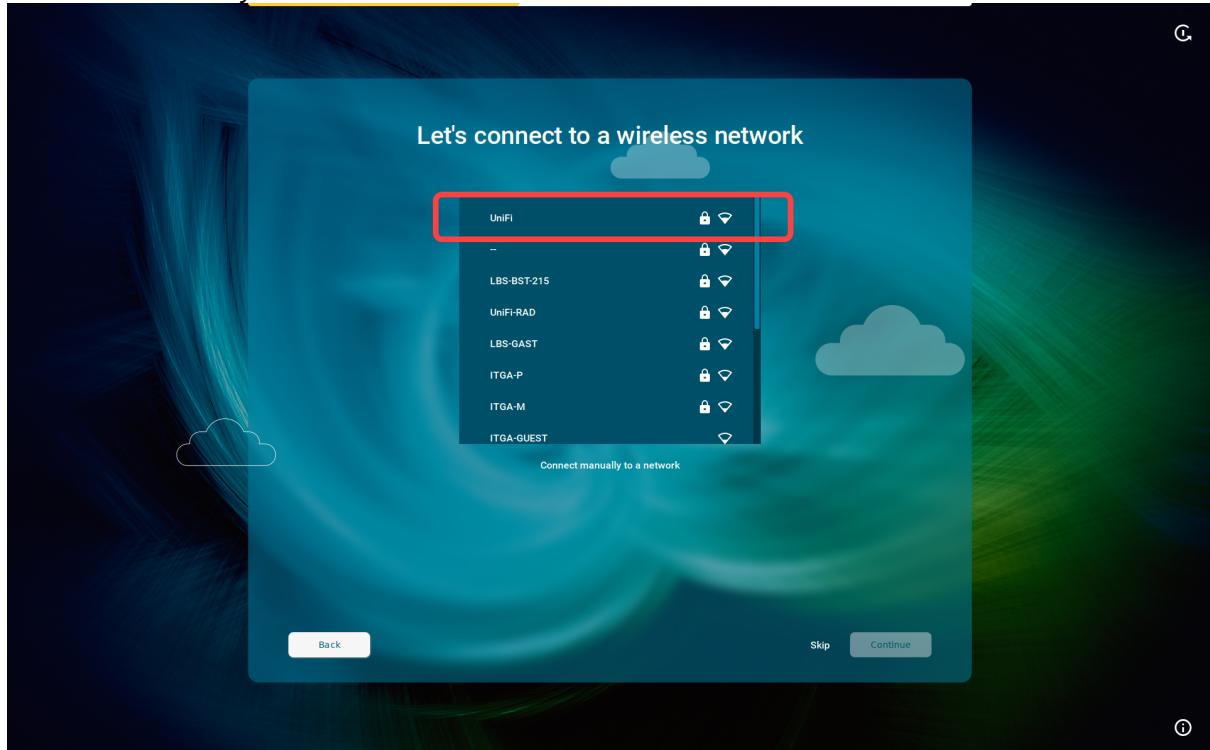


## Connecting to a Wireless Network That Is Visible

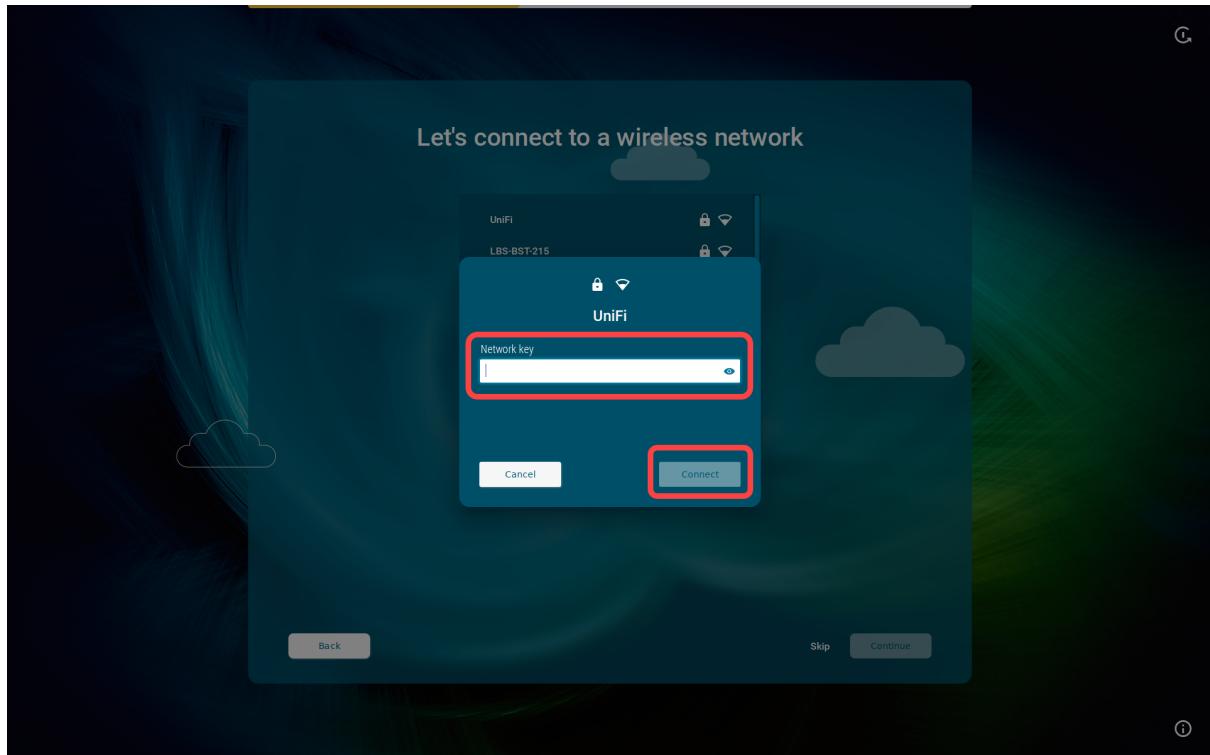
- i Wi-Fi networks with certificates are not supported in the Setup Assistant.

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

1. Select the network you want to connect to.



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



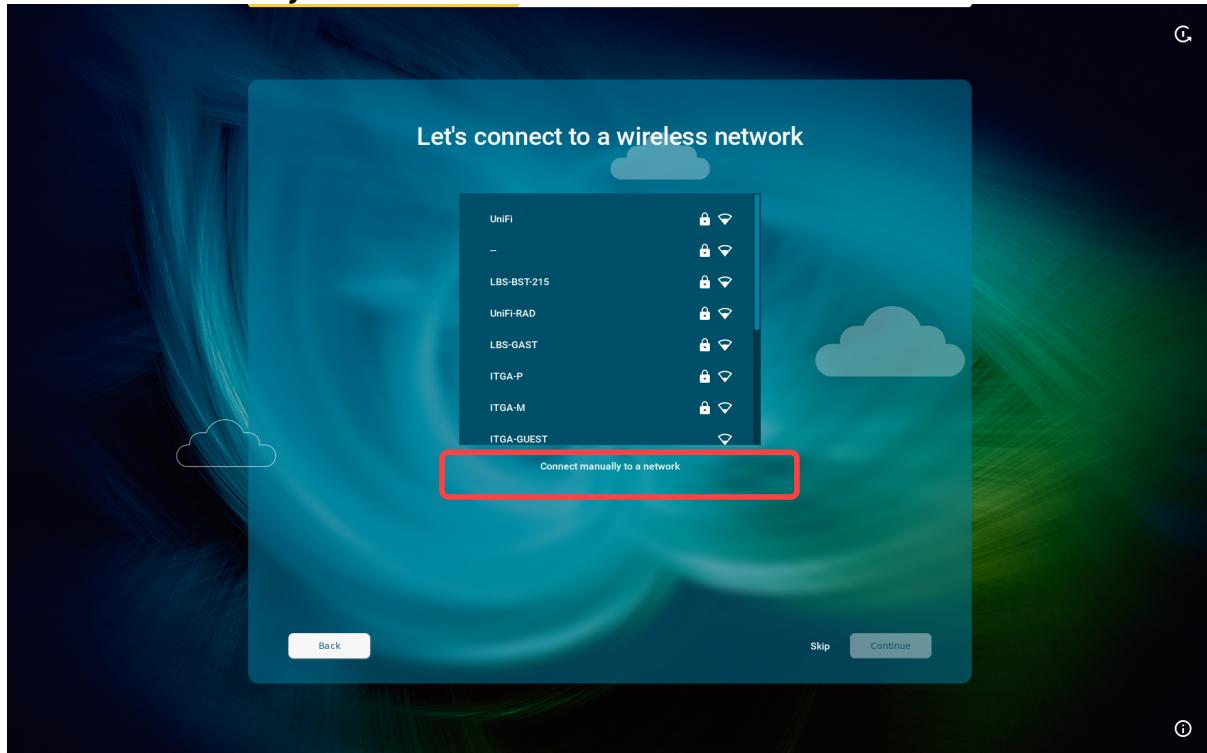
3. Click **Connect**.

- 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**.



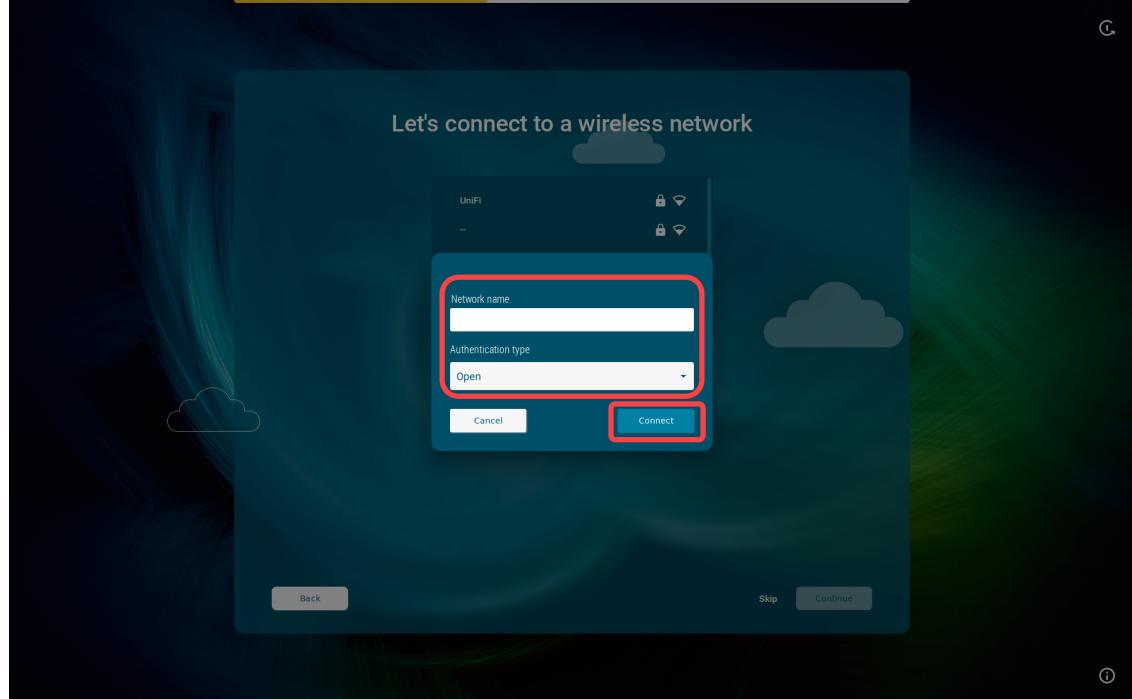
2. Select the **Authentication type** and enter the required authentication data.

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**.

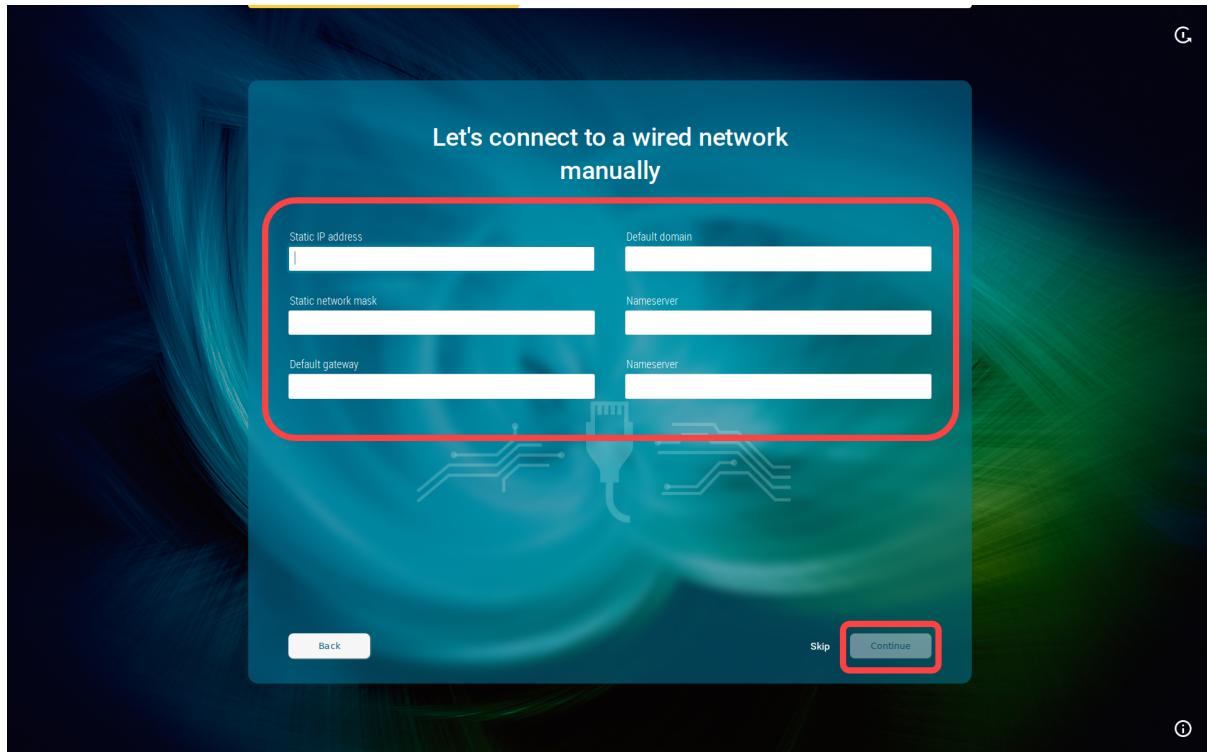


3. Click **Connect**.

## 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:** The country of your provider

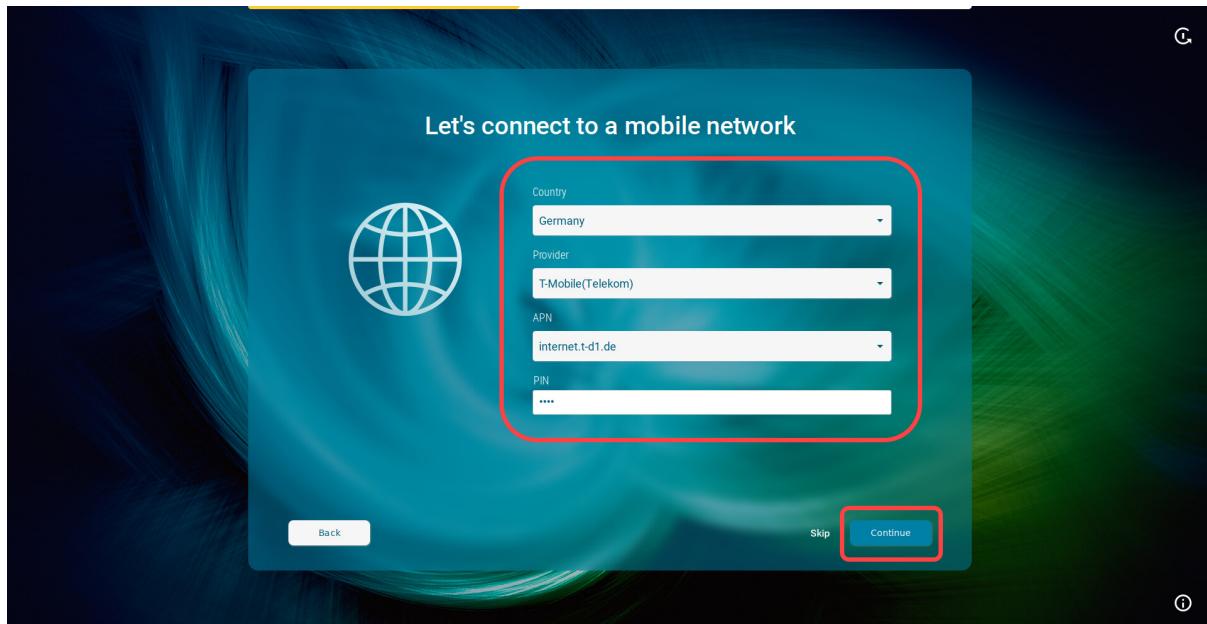
**Provider:** Provider (the possible options depend on what you choose for **Country**)

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

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



2. Click **Continue**.



## Troubleshooting: Possible Error Codes During the Onboarding

During the onboarding with the IGEL Onboarding Service or with the one-time password method, the following internal errors may occur.

Error message: "Could not manage your device because of an internal error (<error-code>) "

Error Code	Meaning
30	Onboarding service not reachable anymore
32	Invalid arguments
33	Failed to initialize EST API
34	Failed to load trust chain
35	Failed to load key pair
36	Failed to load private key
37	Failed to get CA certificates from server
38	Failed to enroll a certificate from server
39	Failed to retrieve the enrolled certificate
40	Failed to convert the enrolled certificate to PEM



Error Code	Meaning
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

- i** 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 171) and contact IGEL Support.



## 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**:

A screenshot of the IGEL Setup software interface. The window title is "IGEL Setup". The top navigation bar includes tabs for Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), System, and Apps. On the right side of the header are search and settings icons. The main content area has a sidebar on the left with sections like Device Encryption, Password, Logon (with sub-options Active Directory/Kerberos and Smartcard), Change password, and a prominent "Update" button. The "Update" button is highlighted with a red box. In the center, there's a configuration panel with a circular refresh icon and a checked checkbox labeled "Permit local app installation". This central panel is also highlighted with a red box.

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

ⓘ Access to the local App Portal and the download of apps is possible for UMS-managed devices if the UMS is registered in the IGEL Customer Portal. For the instructions, see [Registering the UMS](#)(see page 34). 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 119).

## How to Locally Install Apps

To install apps, proceed as follows:

1. Open the App Portal locally on the device.





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

**APP PORTAL OS12**

All Apps

Discover Our Apps

ALL AVAILABLE INSTALLED

Categories All Sort by Name

<b>CUPSCore Binary</b> 1.1.0 BUILD 2  CPCore binary for IGEL AVD Client allows the user to access their Microsoft Azure Virtual Desktop environment.  Last update 08. December 2022 Size 23.5 MB Cloud	<b>CUPS printing app</b> 1.0.0 BUILD 2  CUPS printing application provides printing functionality for IGEL OS  Last update 08. December 2022 Size 11.75 MB Peripheral	<b>Chromium Browser</b> 108.0.5359.124 BUILD 1 RC 3  Chromium is an open source browser project that aims to build a safer, faster and more stable way for everyone to experience the web.  Last update 08. February 2023 Size 130.25 MB Browser
<b>Citrix Multimedia Codec</b> 87.0.4280.141 BUILD 3  Multimedia codec (H.264) support for Citrix (Chromium Embedded Framework)  Last update 28. December 2022 Size 1.5 MB	<b>Citrix Workspace app</b> 22.9.0.21-1 BUILD 2  Citrix Workspace App is client software that allows access to all user's files and apps from one interface. This includes files and desktops, in addition to SaaS and virtual apps.  Last update 08. December 2022 Size 140 MB VDI Cloud	<b>Cryptovision - SCinterface</b> 8.0.0 BUILD 2  SCinterface by Cryptovision integrates smartcards and other tokens into IT environments. It supports over 90 smartcards, security tokens, and profiles.  Last update 08. December 2022 Size 18 MB Security Smartcard +1

**APP PORTAL OS12**

All Apps > CUPS printing app

**CUPS printing app**

Versions 1.0.0 BUILD 2

DESCRIPTION HISTORY

INSTALL

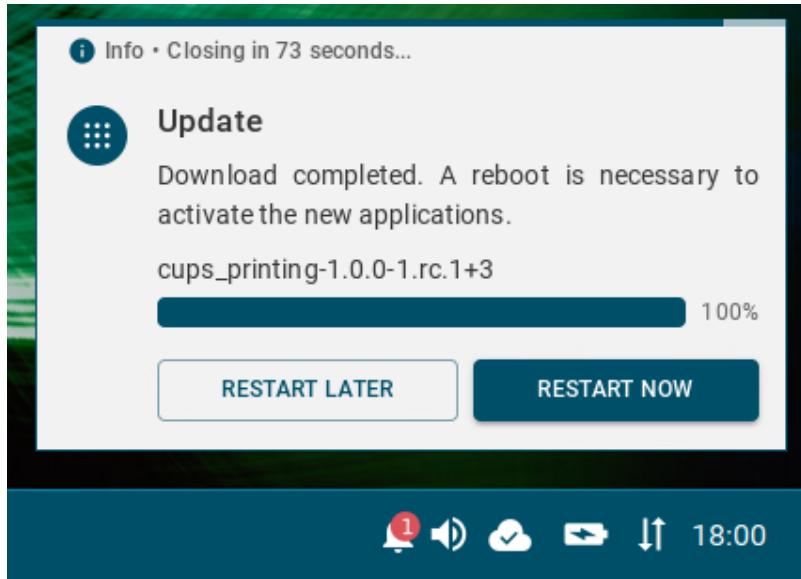
**Info** If the selected app / app version has already been installed, the **Uninstall** icon is shown.

- Accept the End User License Agreement (EULA).

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



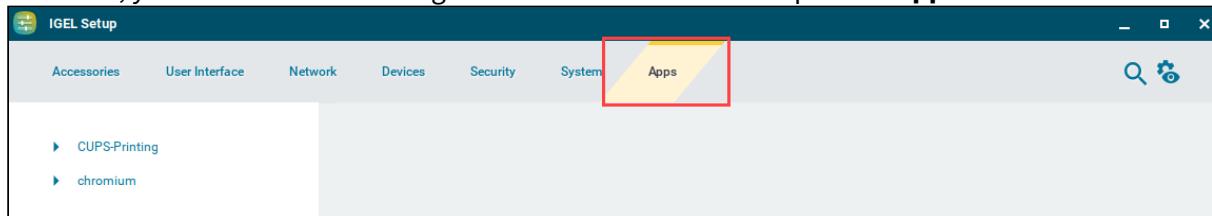
shown:



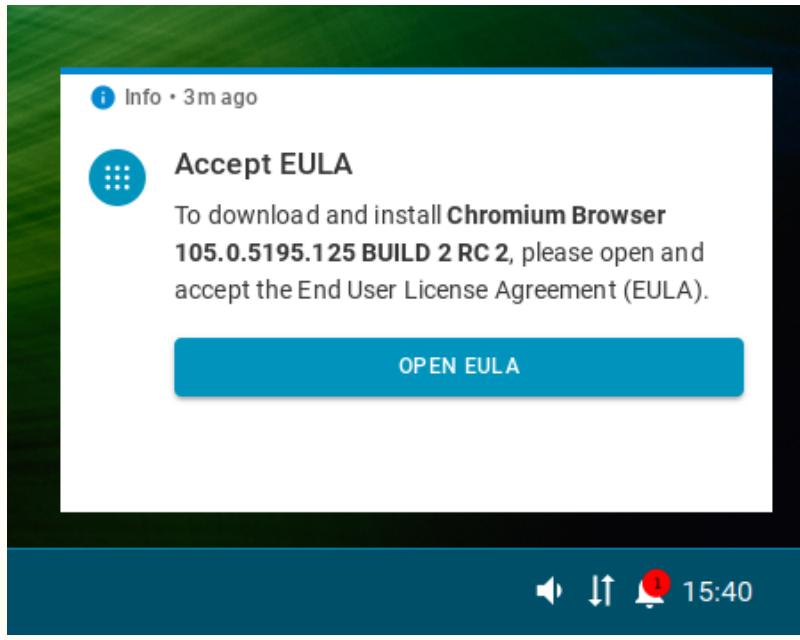
- i Dependant apps and codecs (e.g. Chromium Multimedia Codec, Fluendo libva for Chromium, Citrix Multimedia Codec) are automatically installed on the device during the installation of the main app (e.g. Chromium Browser app, Citrix Workspace app).

4. Restart the device to complete the app installation.

After that, you can create and configure sessions in the IGEL Setup under **Apps**.



- ⚠ IGEL OS Base System as well as all locally installed apps are automatically recognized by the UMS and listed in the **UMS Web App > Apps**. If no such app has been imported to the UMS from the IGEL App Portal before and you assign an "automatically registered" app to other devices, the user will have to accept the End User Licence Agreement (EULA):



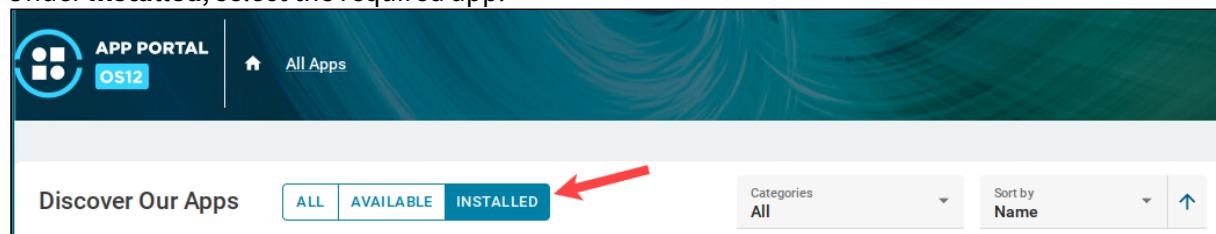
## How to Locally Uninstall Apps

To uninstall apps on the device, proceed as follows:

1. Open the App Portal locally on the device.

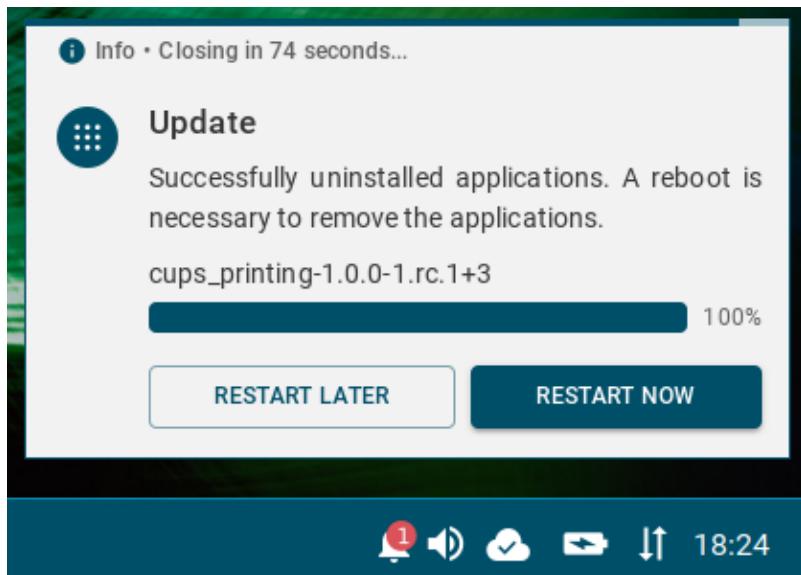


2. Under **Installed**, select the required app.



3. Click **Uninstall**.

The user will receive a corresponding notification:



4. Restart the device to complete the app uninstallation.



## Configuring Single Sign-On (SSO)

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

The following identity providers are supported:

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

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

- via the IGEL UMS Web App:

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

- via IGEL Setup locally on the device (shows all installed apps. Apps are displayed under the tab "Apps")

The best practice to configure your devices is via profiles. For details on how to create profiles, see [Creating a Profile](#)(see page 83).

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

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

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

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

### Configuring SSO with Okta

1. Go to **Security > Logon > Single Sign-On** and edit the settings as follows:



- Enable **Single Sign-On with Identity Provider**.
- Set **Identity Provider** to **Okta**.
- Provide the **Identity Provider URL** for your user. This is the Okta organization URL.  
Example: "https://mycompany.okta.com"
- Provide the **Public Client Identifier (Client/Application ID)**.
- Provide the **Client secret**.

The screenshot shows the 'Profile Configurator - Base Profile' window with the 'Devices' tab selected. On the left, a sidebar menu includes 'Device Encryption', 'Password', 'Logon' (with 'Single Sign-On' highlighted), 'Taskbar', 'Active Directory/Kerberos', 'Local User', 'Active Directory/Kerberos', 'Smartcard', 'Change password', and 'Update'. The main panel displays the 'Security' configuration, specifically the 'Single Sign-On with Identity Provider' section. It shows the 'Identity Provider' set to 'Okta', 'Identity Provider URL' as 'https://mycompany.okta.com', 'Public Client Identifier (Client/Application ID)' (redacted), and 'Client secret' (redacted). There is also a 'Change password' button. At the bottom, there are 'Logout Shortcut Locations' and action buttons: 'App Selector', 'Close', 'Save', and 'Save and Close'.



2. Click **Save** or **Save and close**.

The desktop of the device is terminated. The login screen is displayed.

You can now use the [apps and utilities for IGEL OS 12 that support SSO with Okta](#)(see page 155).

If you want to use multi-factor authentication, you can configure this in the Okta console. The available methods are Google Authenticator, E-Mail, and Okta Verify.

## Setting up SSO with Azure AD

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

### Registering an Azure Application

1. In your Azure AD Portal, go to **App registrations > New registration**.
2. Edit the data as follows and then click **Register**:
  - Add a proper name for the application. Note that this name will be visible to the user once during the consent process for granting permissions.
  - Select the option **Accounts in this organizational directory only ([name of your organization's AD Portal] only - Single tenant)**.
  - Under **Redirect URI (optional)**, select the option **Single-page application (SPA)** and enter "http://localhost/callback" as the URI.



The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The 'Name' field is filled with 'IGEL OS Azure AD Login'. The 'Supported account types' section has 'Accounts in this organizational directory only (Single tenant)' selected. The 'Redirect URI (optional)' field contains 'http://localhost/callback'. A red box highlights the 'Name' and 'Redirect URI' fields. A note at the bottom states: 'By proceeding, you agree to the Microsoft Platform Policies'.

When the application has been registered successfully, you can go to **Authentication** (in our example **IGEL OS Azure AD Login**) > **Authentication** and perform the next step.



3. Enable **ID tokens (used for implicit and hybrid flows)** and click **Save**.

The screenshot shows the 'Authentication' section of the Azure App registrations page for the 'IGEL OS Azure AD Login' application. The left sidebar lists various management options like Overview, Quickstart, Integration assistant, Branding & properties, Authentication (which is selected and highlighted with a red box), Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main content area shows the 'Add URI' field containing 'http://localhost/callback' and a note that it is eligible for the Authorization Code Flow with PKCE. Below this is the 'Grant types' section with a checked checkbox. The 'Front-channel logout URL' section contains a text input field with 'e.g. https://example.com/logout'. Under 'Implicit grant and hybrid flows', there is a note about requesting tokens directly from the authorization endpoint. It includes two checkboxes: 'Access tokens (used for implicit flows)' and 'ID tokens (used for implicit and hybrid flows)', with the latter being checked and highlighted with a red box. The 'Supported account types' section is partially visible. At the bottom are 'Save' and 'Discard' buttons, with 'Save' also highlighted with a red box.

4. To configure the correct permissions for this application, go to **API permissions**. and click **Add a permission**.

## Configuring Single Sign-On (SSO)



The screenshot shows the Azure portal interface for managing API permissions. The left sidebar lists several categories under 'Manage': Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions (which is highlighted with a red box), Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main content area is titled 'IGEL OS Azure AD Login | API permissions'. It includes a search bar, refresh button, and feedback link. A note states: 'The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used.' Below this is a section titled 'Configured permissions' with a note: 'Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.' A 'Grant admin consent for IGEL SSO' button is visible. A table lists the configured permissions:

API / Permissions n...	Type	Description	Admin consent req...	Status
Microsoft Graph (1)	User.Read	Delegated	Sign in and read user profile	No

At the bottom, a note says: 'To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.'



## 5. Select Microsoft Graph.

**Request API permissions**

Select an API

**Microsoft APIs**   **APIs my organization uses**   **My APIs**

Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

<p><b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server</p>	<p><b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal</p>	<p><b>Office 365 Management APIs</b> Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs</p>
<b>More Microsoft APIs</b>		
<p><b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud</p>	<p><b>Azure Communication Services</b> Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams</p>	<p><b>Azure Cosmos DB</b> Fast NoSQL database with open APIs for any scale.</p>
<p><b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets</p>	<p><b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>	<p><b>Azure Data Explorer (with Multifactor Authentication)</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>
<p><b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios</p>	<p><b>Azure Import/Export</b> Programmatic control of import/export jobs</p>	<p><b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>



6. Select **Delegated permissions**.

The screenshot shows the Microsoft Azure AD App registrations interface. On the left, there's a sidebar with options like Overview, Quickstart, Integration assistant, Manage (with Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions), Support + Troubleshooting (with Troubleshooting and New support request). The main area is titled "Request API permissions" for the application "IGEL OS Azure AD". It shows "All APIs" and "Microsoft Graph" with a link to its documentation. A red box highlights the "Delegated permissions" section, which states: "Your application needs to access the API as the signed-in user." To the right, another section for "Application permissions" is shown with the note: "Your application runs as a background service or daemon without a signed-in user." At the bottom are "Add permissions" and "Discard" buttons.

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

- **email**
- **openid**



- profile

**Request API permissions**

All APIs Microsoft Graph https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
--	--

Select permissions

Start typing a permission to filter these results

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
email ⓘ View users' email address	No
offline_access ⓘ Maintain access to data you have given it access to	No
openid ⓘ Sign users in	No
profile ⓘ View users' basic profile	No

Add permissions Discard



## 8. Check if the permissions are correct.

A screenshot of the Microsoft Azure portal showing the "API permissions" section for the "IGEL OS Azure AD Login" application. The left sidebar shows navigation options like Overview, Quickstart, Integration assistant, Manage (selected), Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions (selected), Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main content area is titled "Configured permissions" with a note about admin consent. It shows a table of permissions for "Microsoft Graph (4)" with four rows: "email" (Delegated, View users' email address, No), "openid" (Delegated, Sign users in, No), "profile" (Delegated, View users' basic profile, No), and "User.Read" (Delegated, Sign in and read user profile, No). The last three rows are highlighted with a red box. Below the table, a note says "To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications."

API / Permissions n...	Type	Description	Admin consent req...	Status
email	Delegated	View users' email address	No	...
openid	Delegated	Sign users in	No	...
profile	Delegated	View users' basic profile	No	...
User.Read	Delegated	Sign in and read user profile	No	...



9. Go to **Overview** and copy the **Application (client) ID**. This value will be used as the **Public client identifier (client/application ID)** in the IGEL OS configuration.

The screenshot shows the Azure Active Directory (Azure AD) portal's 'App registrations' section. A specific application named 'IGEL OS Azure AD Login' is selected. The 'Overview' tab is active. In the main content area, under the 'Essentials' section, the 'Application (client) ID' field is highlighted with a red box, and a 'Copy to clipboard' button is visible next to it. Other fields like 'Object ID' and 'Directory (tenant) ID' are also present. To the right, there are sections for 'Client credentials', 'Redirect URIs', 'Application ID URI', and 'Supported account types'. A note at the bottom states that starting June 30th, 2020, no new features will be added to ADAL and Azure AD Graph, but technical support and security updates will continue. Below this, there are sections for 'Build your application with the Microsoft identity platform', 'Call APIs', and 'Sign in users in 5 minutes'.

## Configuring IGEL OS

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

## Configuring Single Sign-On (SSO)



- Enter the **Client secret**.

The screenshot shows the 'Profile Configurator - Base Profile' window with the 'Security' tab selected. On the left, a sidebar lists various configuration categories like 'Device Encryption', 'Password', 'Logon', 'Taskbar', 'Active Directory/Kerberos', 'Single Sign-On' (which is highlighted with a yellow bar), 'Local User', 'Active Directory/Kerberos', 'Smartcard', 'Change password', and 'Update'. The main panel contains a section titled 'Identity Providers' with a sub-section for 'Single Sign-On with Identity Provider'. It shows the 'Identity Provider' set to 'Azure AD', 'Azure AD Tenant Name/ID' (with a blurred value), 'Public Client Identifier (Client/Application ID)' (with a blurred value), and 'Client secret' (with a blurred value). A 'Change password' button is also present. At the bottom right are buttons for 'Close', 'Save', and 'Save and Close'.

2. Click **Save or Save and close**.

This screenshot is identical to the previous one, showing the 'Profile Configurator - Base Profile' window with the 'Security' tab selected. The 'Single Sign-On' category in the sidebar is still highlighted. The main panel shows the same 'Identity Providers' configuration. However, the bottom right buttons have changed: the 'Close' button is now greyed out, while 'Save' and 'Save and Close' are shown in blue with a red rectangular box highlighting the 'Save and Close' button.

The desktop of the device is terminated. The login screen is displayed.  
You can now use the [apps and utilities for IGEL OS 12 that support SSO with Azure AD](#)(see page 155).



For details on importing apps from the IGEL App Portal and installing them on IGEL OS devices, see [IGEL UMS 12: Basic Configuration](#)(see page 76) and [Assignment of Apps and Profiles](#)(see page 88). All methods of multi-factor authentication are available except the hardware token.

## Enabling Local Login (Optional)

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

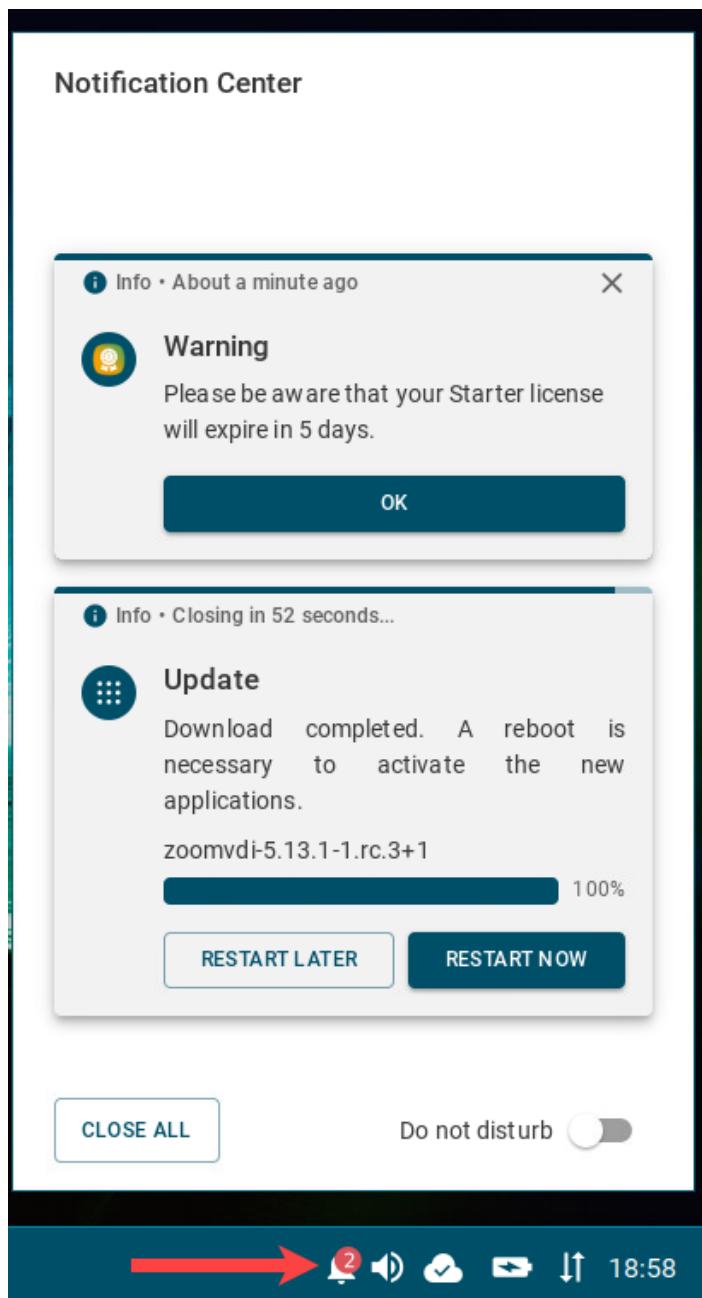
1. Open the profile configurator and go to **Security > Logon > Local user**.
2. Activate **Login with local user password** and enter a password.

A screenshot of the Profile Configurator interface. The top navigation bar shows tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), and System. Below the tabs, there's a search bar and a gear icon with a notification count of 3. On the left, a sidebar menu lists: Device Encryption, Password, Logon (with Taskbar, Active Directory/Kerberos, Single Sign-On, and Local User selected), and Logout Shortcut Locations. The Local User section under Logon is expanded, showing Active Directory/Kerberos, Smartcard, Change password, and Update. A red box highlights the "Login with local user password" checkbox, which is checked. Below it, there are two password input fields, both containing ".....", and a "Set password" button. At the bottom right of the main window are buttons for Close, Save, and Save and Close.



## IGEL OS Notification Center

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



Notification Center icon  is displayed if the taskbar and taskbar system tray are activated (**User Interface > Desktop > Taskbar** and **Taskbar Items**; both are enabled by default).



- ⓘ If you do not want to see floating notifications, you can activate the **Do not disturb** function.

In the Notification Center, you can see

- Update notifications prompting the user to reboot the device to complete the app installation. The device will be restarted automatically if the user will not react within 60 seconds; this timeout can be changed under **System > Update > Timeout for automatical reboot in seconds**.

- ⓘ If you do not want the user to see the dialog offering to restart the device immediately or postpone the restart, you can enable **Automatical reboot of system once app is installed** under **System > Update**.

Note: The update notification is different if **Activate app after the installation** is disabled under **System > Update**, see How to Configure the Background App Update in the IGEL UMS Web App.

- EULA notifications if the End User Licence Agreement has to be accepted. When this may be necessary is described under [Accepting EULA in the UMS](#)(see page 82).
- Messages sent by the UMS administrator
- Warnings, e.g. about license expiration, and errors
- Other notifications, e.g. about a new configuration the system has received



## IGEL Insight Service

At the first start of the IGEL UMS Console or the UMS Web App after the UMS installation, you are presented with a dialog offering to activate IGEL Insight Service. If you are not sure, you can skip this step to decide later; in this case, the dialog will be presented on each start of the UMS Console / the UMS Web App until the feature is accepted or declined.

- ⓘ IGEL Insight Service can be anytime activated or deactivated under **UMS Console > UMS Administration > Global Configuration > UMS Features** or under **UMS Web App > Network > Settings > UMS Features**.

IGEL Insight Service collects analytical and usage data from all users to

- improve IGEL products and services and the user experience
- inform you about available software and security updates
- provide recommendations for system optimization (software and hardware)
- identify potential performance issues regarding apps in your setup
- improve customer support and consulting

The identity of the individual IGEL OS device will only be stored pseudonymously. All data will be anonymized after two years.

The consent can be withdrawn by disabling the Insight Service functionality as described above. By withdrawing the consent, you will not receive further recommendations based on your setup.

For more information, please refer to IGEL's [privacy policy<sup>15</sup>](#).

### Data Collected by the IGEL Insight Service

- Company identifier
- UMS identifier
- Pseudonymized device identifier
- Name of the application
- Version of the application
- Manufacturer of the device
- Model of the device
- CPU of the device
- RAM of the device
- Mainboard of the device
- GPU of the device
- Storage hardware of the device
- Network / Wi-Fi hardware information of the device
- Peripheral hardware information of the device
- Timestamp
- Client type (Insight Service Data Collector)
- Client version (Insight Service Data Collector)

IGEL does not share your data with third parties outside the IGEL group.

<sup>15</sup> <https://www.igel.com/privacy-policy/>



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

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

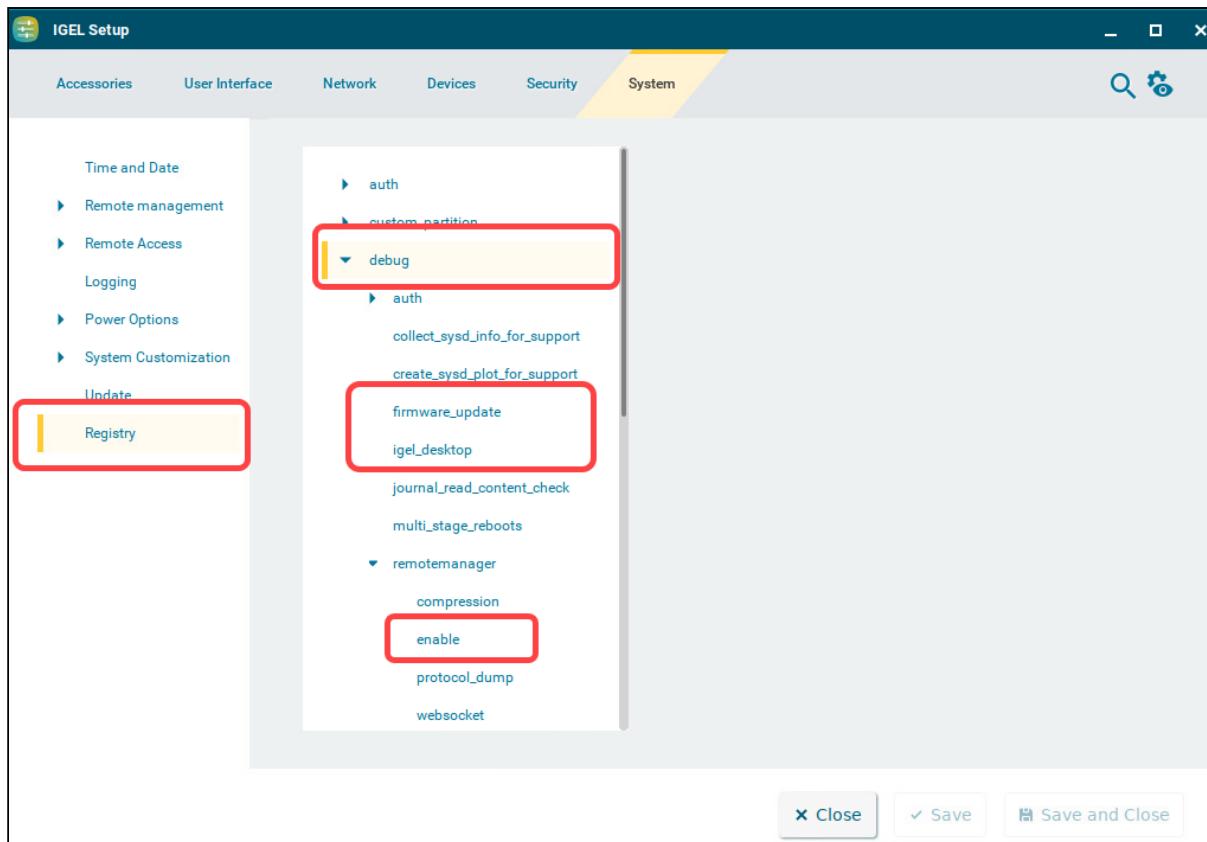
To collect the device log files, see the instructions below.

---

With IGEL OS 12, additional logging functionalities have been introduced to facilitate debugging. To enable debug mode, proceed as follows:

1. In the IGEL Setup, go to **System > Registry** and activate the following registry keys:

Registry	Parameter	Function
debug.igel_desktop	<b>Enable debug logging for IGEL desktop</b>	Debug logging for user interface applications like the Setup Assistant and the Setup
debug.firmware_update	<b>Enable debug logging for firmware update</b>	Debug logging for updates and installations of IGEL OS Apps
debug.remotemanager.enabled	<b>Enable debug logging</b>	Debug logging for RMagent communication



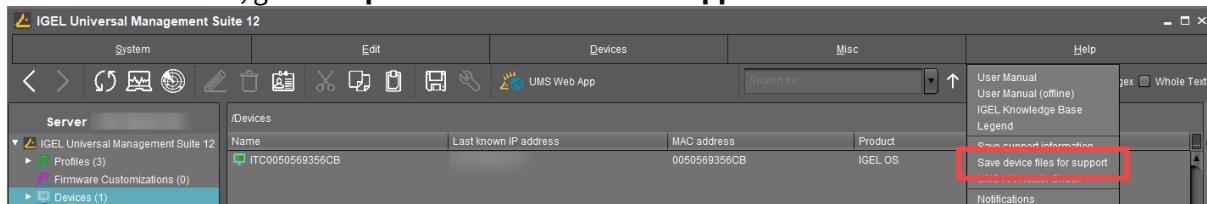
## 2. Click **Save or Apply**.

- 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 UMS

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

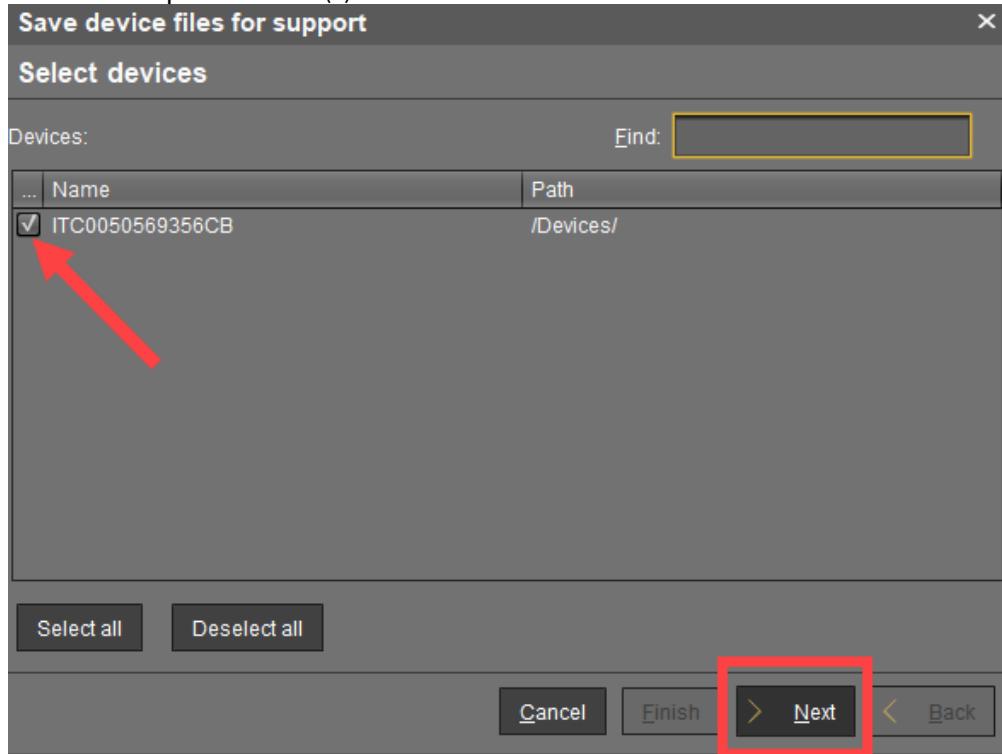
### 1. In the UMS Console, go to **Help > Save device files for support**.





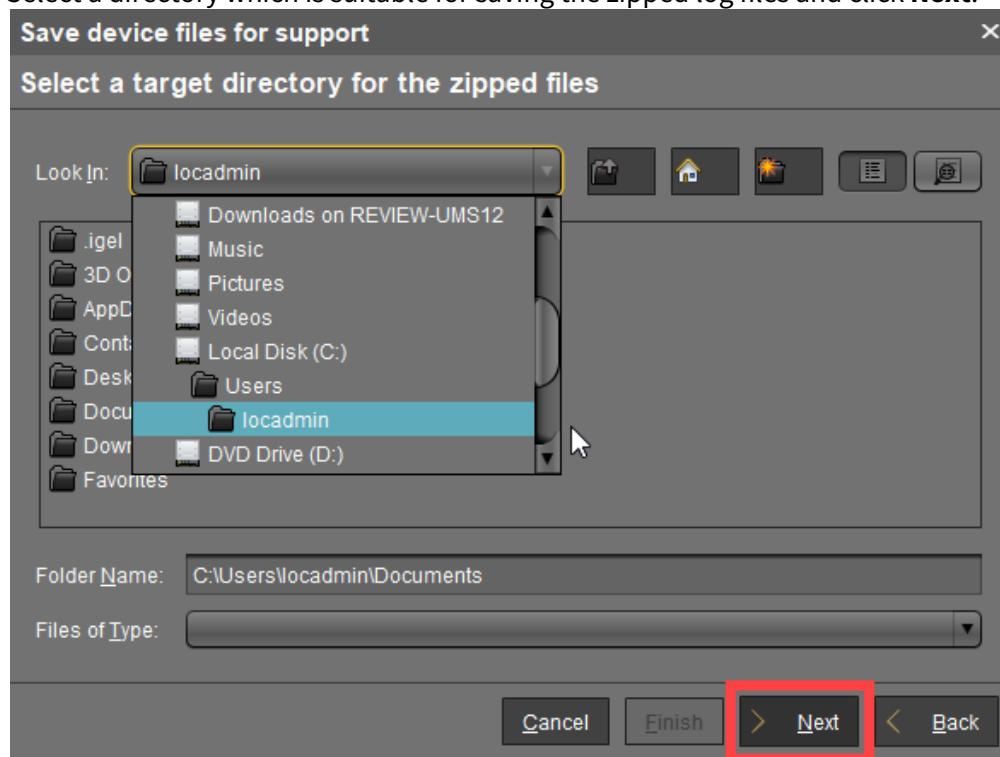
The dialog **Save device files for support** opens.

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



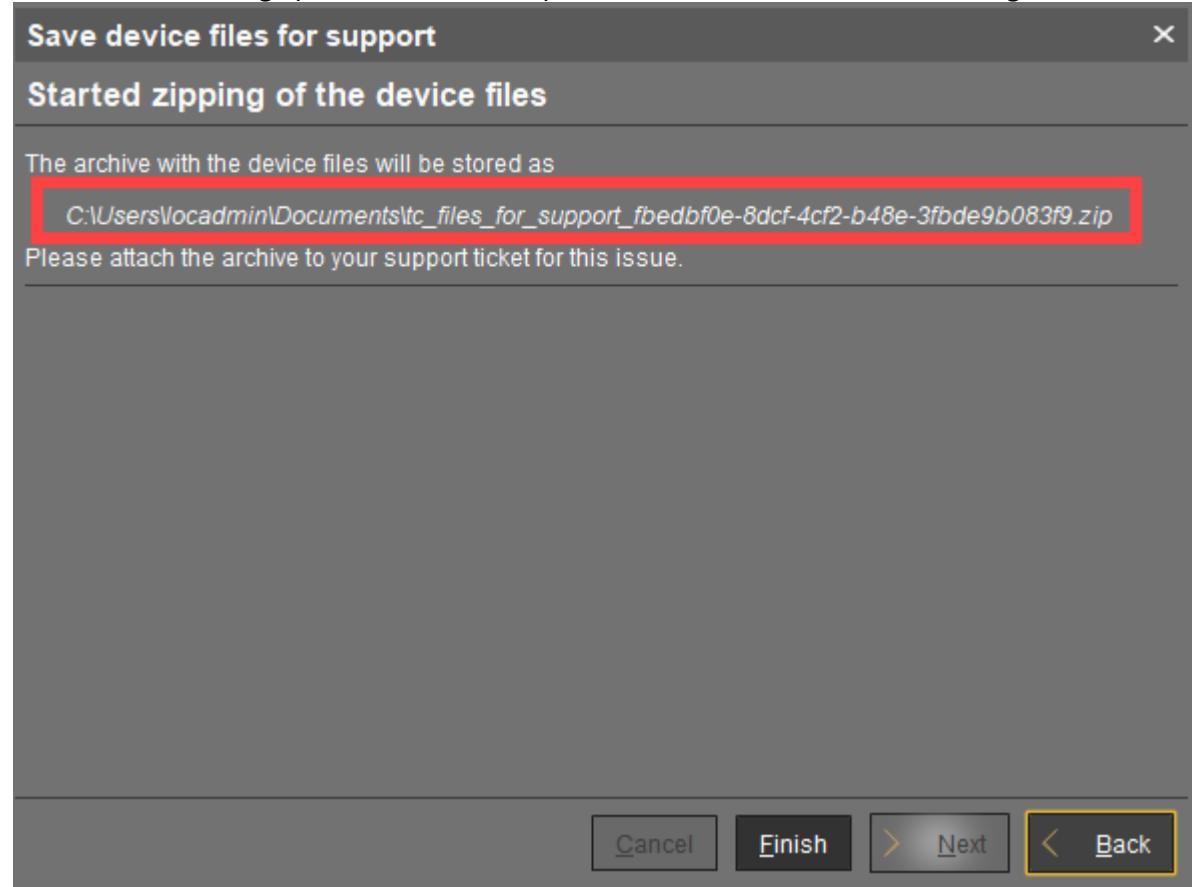


3. Select a directory which is suitable for saving the zipped log files and click **Next**.





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



4. When the log collecting procedure is complete, close the confirmation dialog by clicking **Finish**.
5. Find the ZIP file "tc\_files\_for\_support\_..." in the directory you selected and send it to <sup>16</sup>GEL Support via the [IGEL Customer Portal](#)<sup>17</sup>.

## 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.

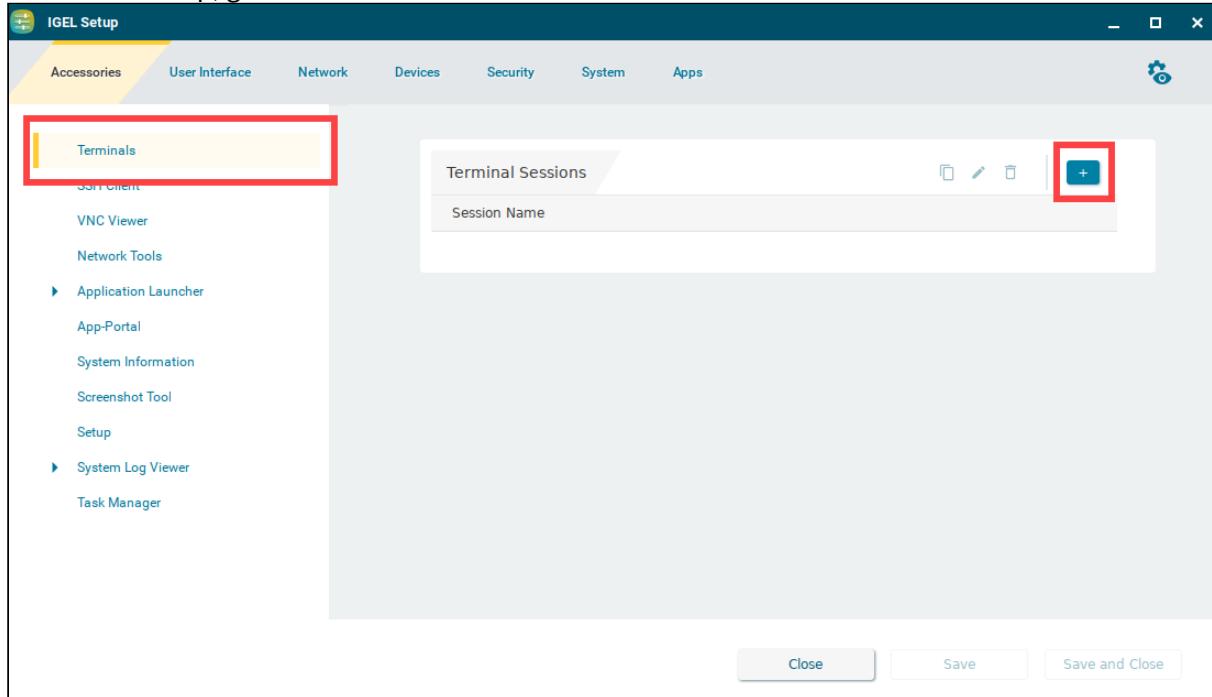
<sup>16</sup>mailto:eap@igel.com

<sup>17</sup><https://cosmos.igel.com/>



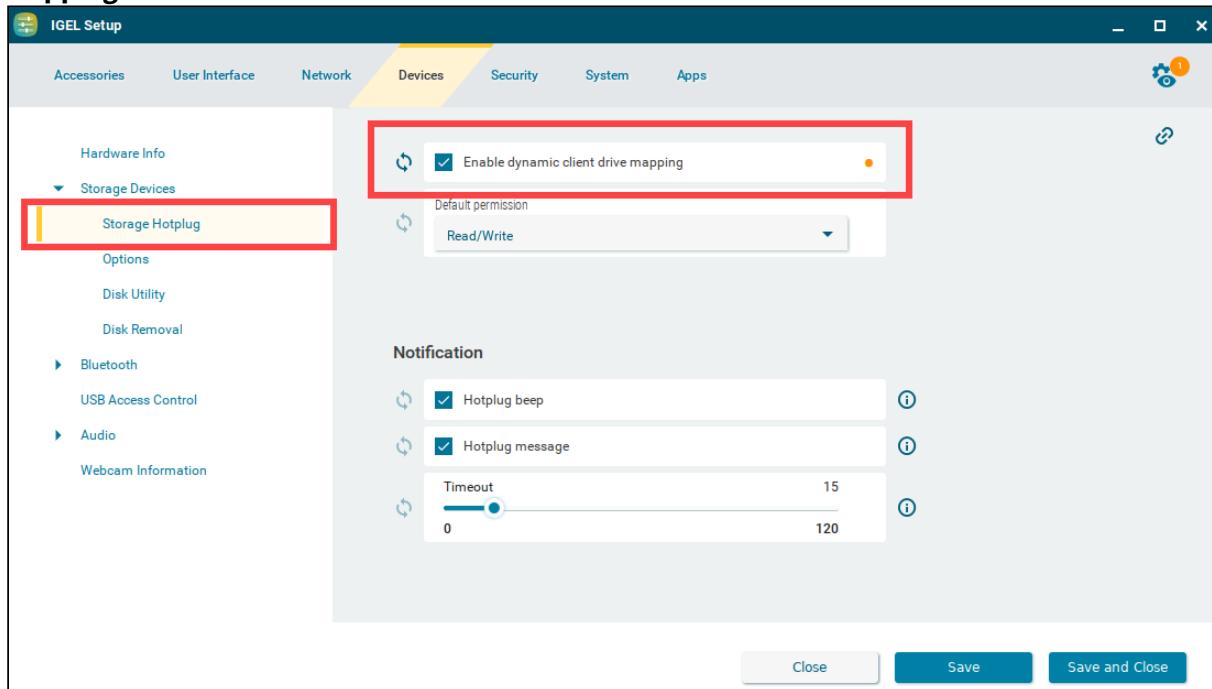
## Option 1: Via Local Terminal

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





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



3. Verify that **System > Registry > debug > igel\_desktop > Enable debug logging for IGEL desktop** is enabled.
4. Save the settings.
5. Plug the USB stick into the endpoint device and start the terminal session.
6. Log in as `root` (by default, no password).
7. To create the log files, execute the command `/config/bin/create_support_information`. This will generate `/tmp/tclogs.zip` (you can go there as follows: `cd /tmp`)

```
Local Terminal
login as "user" or "root": root
root@ITC00E0C561FAF7:~# /config/bin/create_support_information
stat: cannot stat '/tmp/tclogs': No such file or directory
```

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



**Local Terminal**

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

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

- To copy the log files from your endpoint device to the USB stick, run the command `cp /tmp/tclogs.zip /media/[name of your USB stick]/` and press [Return].

**Tip**

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

- Type `sync` and press [Return].

**Local Terminal**

```
updating: /tmp/tclogs.zip/base_system/audio/alsa_info.txt (duplicated 0.0%)
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.

- Send the log files to <sup>18</sup>GEL Support via the [IGEL Customer Portal](#)<sup>19</sup>.

## 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.

- Press anytime [CTRL+ALT+F12] to enter CLI and then press [Return].
- Plug in your USB stick.

<sup>18</sup> <mailto:eap@igel.com>

<sup>19</sup> <https://cosmos.igel.com/>



i Use a FAT32-formatted USB stick.

3. Execute the following command: `dmesg`

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

4. Type `cat /proc/partitions`

Search for `sda` , `sdb` , `sdc` , etc. and search for the next line showing the partitions (Example: `sda1` , `sdb1` , etc.)

5. Create the mountpoint directory: `mkdir /mnt`

6. The device name for mounting the USB stick for the following command in step 7 needs an additional partition number. Example: `sda1` , `sdb1` , `sdc1` , etc.

7. Mount your USB stick: `mount /dev/sda1 /mnt`

```
251.6161431 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
253.1983271 sd 2:0:0:0: [sdb] 60620000 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@ITC00E00C51A75F4:/# 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    325080 igf60
61     66    12668 igf66
61     68     876 igf68
61    239    524288 igf239
61    254     5120 igf254
61    255    24576 igf255
253     0    24576 dm-0
253     1    524288 dm-1
252     0    555956 zram0
252     1    555956 zram1
252     2    555956 zram2
252     3    555956 zram3
8      16   30310400 sdb
8      17   30310160 sdb1
root@ITC00E00C51A75F4:/# mkdir /mnt
root@ITC00E00C51A75F4:/# mount /dev/sdb1 /mnt
root@ITC00E00C51A75F4:/#
```

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.

```
root@ITC00E0C51A75F4:/mnt# cd /tmp
root@ITC00E0C51A75F4:/tmp# ls -l
total 984
prw-rw--- 1 user users      0 Jul  7 12:46 fifomgr2tray
prw-rw--- 1 user users      0 Jul  7 12:46 fifotray2mgr
drwxr-xr-x  3 root root    60 Jul  7 12:58 logfiles
-rw-r--r--  1 user users      0 Jul  7 12:46 mblog
drwxr--r--  2 root root    40 Jul  7 12:45 pulse-PKdhtXMmr1Bn
-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-B7Nbfg
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-CHYnMf
drwxr--r--  3 root root    60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-systemd-logind.service-mUF8Kh
drwxr--r--  3 root root    60 Jul  7 12:45 systemd-private-d202adbe74b348ddb616b0147e375b73-upower.service-mCaLhh
-rw-r--r--  1 root root  958247 Jul  7 13:00 tclogs.zip
drwxrwxrwt  2 root root    40 Jul  7 12:45 VMwareDnD
-rw-r--r--  1 root root     74 Jul  7 12:46 wfs_stats
-rw-r--r--  1 root root   50351 Jul  7 12:58 xorg-debug.log
root@ITC00E0C51A75F4:/tmp# cp /tmp/tclogs.zip /mnt
root@ITC00E0C51A75F4:/tmp# umount /mnt
```

11. To copy `tclogs.zip` from your endpoint device to the USB stick, type `cp /tmp/tclogs.zip /mnt` and press [Return].
12. To unmount your USB stick, use the command `umount /mnt`
13. Now you can safely remove your USB stick.
14. To close CLI, press [CTRL+ALT+F1].
15. Send `tclogs.zip` to IGEL Support via the [IGEL Customer Portal](#)<sup>20</sup>.

---

<sup>20</sup> <https://cosmos.igel.com/>