



How to Start with IGEL COSMOS



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

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



IGEL COSMOS comprises:

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



- [IGEL Customer Portal](#)(see page 4) which is a doorway to the IGEL product-related services. Here, you register your company account and use it to invite other [users and assign them specific roles](#)(see page 9), e.g. for opening support cases. In the IGEL Customer Portal, you can also raise and view support requests, make necessary configurations for IGEL Onboarding Service, etc.
- [IGEL App Portal](#)(see page 103) where you can find all applications currently available for IGEL OS 12
- [IGEL Onboarding Service](#)(see page 41) which, if configured, allows your users to easily onboard IGEL OS 12 devices using only their corporate email
- [IGEL Insight Service](#)(see page 215) which collects analytical and usage data to improve IGEL products and services and provide a better customer experience
- [IGEL License Portal](#)(see page 151) where you can manage licenses for your IGEL OS devices

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

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

- Registering for the [IGEL Customer Portal](#)(see page 4)
- Managing Users and Roles in the [IGEL Customer Portal](#)(see page 9)
- Installing / Upgrading to [IGEL UMS 12](#)(see page 32)
- Registering the [UMS](#)(see page 36)
- Initial Configuration of the [IGEL Onboarding Service \(OBS\)](#)(see page 41)
- [IGEL App Portal](#)(see page 103)
- [IGEL UMS 12: Basic Configuration](#)(see page 106)
- [IGEL UMS 12: App Update](#)(see page 126)
- Installing the Base System via [IGEL OS Creator \(OSC\)](#)(see page 137)
- Licensing(see page 151)
- Onboarding [IGEL OS 12 Devices](#)(see page 158)
- Installing [IGEL OS Apps Locally on the Device](#)(see page 188)
- Configuring Single Sign-On (SSO)(see page 193)
- [IGEL OS Notification Center](#)(see page 213)
- [IGEL Insight Service](#)(see page 215)
- Debugging / How to Collect and Send Device Log Files to [IGEL Support](#)(see page 217)

¹ <https://learn.igel.com/learn/course/150/>

² <https://videos.igelcommunity.com/>



Registering for the IGEL Customer Portal

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

Registration to the IGEL Customer Portal

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

To register for the IGEL Customer Portal:

1. Open [IGEL Customer Portal³](https://cosmos.igel.com/) and click **Register** in the upper right corner of the menu bar:

A screenshot of the IGEL COSMOS homepage. At the top, there's a dark banner 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 banner is a large banner image of a city at night with a bridge. In the center of the page, there's a "Welcome to IGEL COSMOS!" message and a search bar with the placeholder "Insert your question here". A blue callout box contains 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" underneath), "Software" (with "Software Downloads" underneath), and "Hardware" (with "Declare UDC destruction" underneath).

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

³ <https://cosmos.igel.com/>



2. Enter your user data:

* Indicates required

Company Information	
* COMPANY NAME	* ADDRESS
<input type="text"/>	<input type="text"/>
ADDRESS 2	* CITY
<input type="text"/>	<input type="text"/>
* COUNTRY	* POST CODE
<input type="text"/> Germany	<input type="text"/> Please write N/A if no zip code is available
* STATE/PROVINCE	* INDUSTRY
<input type="text"/>	<input type="text"/> Others
Personal Information	
* LOGIN-EMAIL	* WORK PHONE
<input type="text"/>	<input type="text"/> Please use following format +1234567890
* FIRST NAME	* LAST NAME
<input type="text"/>	<input type="text"/>
* CHOOSE YOUR PREFERRED LANGUAGE	
<input type="text"/> English	
<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 PRIVACY POLICIES.	
<small>IGEL Cloud Services Terms & Conditions can be found here</small> <small>You can find the Privacy Policy here</small>	

Submit

Required Information

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

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

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

IGEL Company Account Requirements

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

3. Click **Submit**.

A confirmation email will be sent to you.

4. Check your mailbox and confirm your registration by clicking on the appropriate link. If you have not received the email, please check your spam folder.

Your user data will now be internally checked. You will receive an email confirmation when your registration has been approved containing your username and one-time password. As soon as you log in for the first time, you will be prompted to change your password. The registration approval



process usually takes no more than 24 hours.

Example:

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

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

Your login details:
[REDACTED]

COSMOS Login

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

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

Logging In to the IGEL Customer Portal

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

⁴ <https://cosmos.igel.com/>



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

The screenshot shows the login interface of the IGEL Customer Portal. At the top, there is a dark navigation bar with the words "Catalog", "Knowledge", "Register", and "Login". A red arrow points to the "Login" button. Below the navigation bar is a white login form titled "Log in". The form includes instructions: "Don't have an account? Register [here](#). Enter your username (e-mail address) and password here in order to log in on the website:". There are two input fields: "User name" and "Password", both of which are highlighted with a red rounded rectangle. Below these fields is a link "Forgot Password ?". At the bottom of the form is a blue "Log in" button, which is also highlighted with a red rounded rectangle.

Login Credentials Forgotten?

1. Open the [IGEL Customer Portal](https://cosmos.igel.com/)⁵ and click **Login**.

⁵ <https://cosmos.igel.com/>



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

The screenshot shows the login page of the IGEL Customer Portal. At the top right, there are four buttons: Catalog, Knowledge, Register, and Login. A red arrow points to the 'Login' button. The main area is titled 'Log in' and contains fields for 'User name' and 'Password'. Below these fields is a note about forgot passwords, followed by a red-bordered 'Forgot Password ?' link and a blue 'Log in' button.

A dialog for requesting a new password will open:

The screenshot shows the first step of a three-step process for password reset, labeled 'Identify'. It features three arrows at the top: 'Identify' (highlighted in blue), 'Verify', and 'Reset'. Below the arrows is a form field with a red asterisk next to 'User name' and a blue 'Next' button.

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

3. **Identify:** Enter your **user name** that you used to register with IGEL.
4. **Verify:** Enter your **email** address to which the verification email should be sent.
5. Check your email inbox and confirm it with the corresponding link. If you have not received the email, please check your spam folder.
The **Reset Password** dialog box will open in your default browser.
6. **Reset:** Set a new password following the displayed password rules and confirm by clicking **Reset Password**.

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



Managing Users and Roles in the IGEL Customer Portal

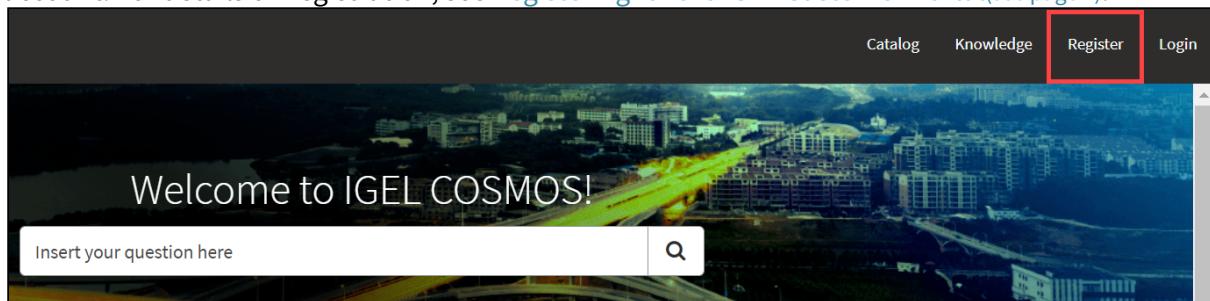
This article describes how to invite users, cancel or renew invitations, and add roles to a user or remove roles in the IGEL Customer Portal. Also included is a description of how to use Okta or Ping as federated identity providers (IdP) for logging in to your IGEL Cloud Services accounts.

Roles and Permissions

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

- Super Admin

The first account you register in the [IGEL Customer Portal⁶](#) > **Register** is your Super Admin account. For details on registration, see [Registering for the IGEL Customer Portal](#)(see page 4).



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

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

The users with these roles have the following permissions:

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

⁶ <https://cosmos.igel.com/>



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

Inviting a User and Assigning a Role

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



1. Open [IGEL Customer Portal](https://cosmos.igel.com/)⁷, log in to your admin account, and select **Users > User & Role Administration**.

A screenshot of the IGEL Customer Portal homepage. At the top, there is a navigation bar with links for 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 'Users' link, and a red arrow points to the 'User & Role Administration' option in the dropdown menu. Below the navigation bar, there is a search bar with the placeholder 'Insert your question here' and a magnifying glass icon.

2. Select **Invite new user**.

A screenshot of the 'User & Role Administration' page. The page title is 'User & Role Administration'. On the left, there is a sidebar with a dropdown menu labeled 'Please choose' containing options like '-- None --' and 'Invite new User'. The 'Invite new User' option is highlighted with a red box. On the right, there is a large input field labeled 'Required information' with a 'Please choose' button. At the bottom right of the page, there is a blue 'Submit' button.

3. Provide the data of the new user:

- **First name:** First name of the user
- **Last name:** Last name of the user
- **E-mail (required):** E-mail address of the user

⁷ <https://cosmos.igel.com/>



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

User & Role Administration

First Name: Ike

Last Name: Igel

E-Mail: @igel.com

Language: English

Submit

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

User & Role Administration

First Name: Ike

Last Name: Igel

E-Mail: @igel.com

Language: English

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

Submit

The invitation mail is sent to the user.

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



All > Account = Test Company

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

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.

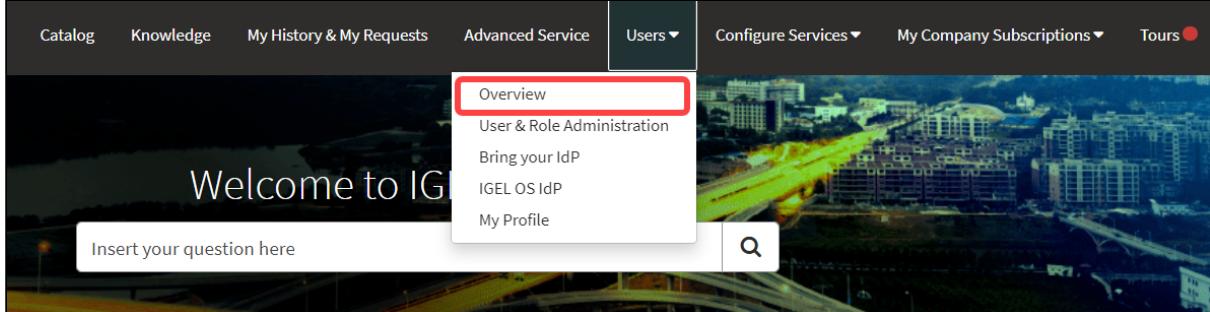
Cancelling and Resending Invitations

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](#)⁸, log in to your admin account, and select **Users > Overview**.



The users are listed.

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



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

Users					
All > Account =	Email	Role	Active	Invitation Status	Action
QAS Test Company	@igel.com	App Portal User	Pending	Pending	<button>Resend</button> <button>Cancel</button>
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](https://cosmos.igel.com/)⁹, log in to your admin account, and select **Users > User & Role Administration**.

2. Select **Add additional role**.

⁹ <https://cosmos.igel.com/>



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

* Indicates required

User & Role Administration

User & Role Administration

*Please choose

Add additional role

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

Submit

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

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

* Please choose

Add additional role

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

Submit

Additional role

OBS Admin

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 roles from a user. If you deactivate a user, the account is deleted. No e-mails will be sent to this account anymore.

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

A screenshot of the IGEL Customer Portal homepage. At the top, there is a navigation bar with links for Catalog, Knowledge, My History & My Requests, Advanced Service, Users (with a dropdown arrow), Configure Services, My Company Subscriptions, and Tours. Below the navigation bar is a banner with a cityscape background and the text "Welcome to IGEL". A search bar is present with the placeholder "Insert your question here". On the right side of the banner, there is a dropdown menu with options: Overview, User & Role Administration (which is highlighted with a red box), Bring your IdP, IGEL OS IdP, and My Profile. A magnifying glass icon is also visible.

2. Select **Remove role**.

A screenshot of the "User & Role Administration" page. The page has a header with a "Submit" button. Below the header, there is a section titled "User & Role Administration" with a note "* Indicates required". A dropdown menu is open, showing options: "-- None --" (selected), "None", "Invite new User", "Add additional role", and "Remove role" (which is highlighted with a red box). To the right of the dropdown, there is a note "Required information" and a "Please choose" button. The "Submit" button is located at the bottom right of the page.

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

A screenshot of the "User & Role Administration" page. The page has a header with a "Submit" button. Below the header, there is a section titled "User & Role Administration" with a note "* Please choose". A dropdown menu is open, showing the option "Remove role". Below the dropdown, there is a note "Please select the user you want to remove from this role". A dropdown menu is open, showing a list of users. One user name is highlighted with a red box. The "Submit" button is located at the bottom right of the page.

¹⁰ <https://cosmos.igel.com/>



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

The screenshot shows the 'User & Role Administration' page. In the 'Add/Remove Role' section, there is a dropdown menu labeled 'Remove role' with a placeholder 'Please choose'. Below it is a dropdown menu for selecting a user to remove from a role, showing a single entry with a delete button. A third dropdown menu for selecting a role to add or remove for the user is shown, with the option 'Customer Support Account Manager' highlighted with a red box. A required information message at the top right says 'Please select the role you would like to add/remove for this user'.

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

The screenshot shows the same 'User & Role Administration' page after the change was submitted. The 'Customer Support Account Manager' role is now selected in the dropdown menu. A note at the bottom left states 'This user only has one role, removing it will deactivate the user'. The 'Submit' button is highlighted with a red box.

Using Okta as Federated Identity Provider

Setting Up an App Integration in Okta

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

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



The screenshot shows the 'Applications' page with a search bar and a table of applications. The table has two columns: 'STATUS' and 'Name'. It lists three items: 'ACTIVE' (0) with 'Okta Admin Console', 'INACTIVE' (0) with 'Okta Browser Plugin', and another entry with 'Okta Dashboard'.

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

The dialog title is 'Create a new app integration'. Under 'Sign-in method', there are four options: 'OIDC - OpenID Connect', 'SAML 2.0' (selected), 'SWA - Secure Web Authentication', and 'API Services'. Descriptions for each option are provided. At the bottom right are 'Cancel' and 'Next' buttons, with 'Next' highlighted by a red box.



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

Create SAML Integration

1 General Settings	2 Configure SAML
---------------------------	-------------------------

1 General Settings

App name

App logo (optional)

App visibility Do not display application icon to users

Cancel **Next**

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 <small>?</small>	<input type="text" value="https://login.microsoftonline.com/login.srf"/>
<input checked="" type="checkbox"/> Use this for Recipient URL and Destination URL	
Audience URI (SP Entity ID) <small>?</small>	<input type="text" value="urn:federation:MicrosoftOnline"/>
Default RelayState <small>?</small>	<input type="text"/>
If no value is set, a blank RelayState is sent	
Name ID format <small>?</small>	<input type="text" value="Unspecified"/>
Application username <small>?</small>	<input type="text" value="Email"/>
Update application username on	<input type="text" value="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
<input type="text" value="http://schemas.xmlso:"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>
<input type="text" value="NameID Format"/>	<input type="text" value="Unspecified"/>	<input type="text" value="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"/>
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 Okta Application Settings page for an application named "Igel SSO". The top navigation bar includes a gear icon, an ellipsis button, a status indicator showing "Active", and links for "View Logs" and "Monitor Imports". A message box indicates that once a working SAML integration is submitted, it can be published in the OAN. Below the message, there are tabs for "General", "Sign On" (which is highlighted with a red box), "Import", and "Assignments". The "Sign On" tab leads to the "Settings" page for SAML 2.0 configuration. The "Edit" link is located in the top right corner of this section. The "Sign on methods" section describes how sign-on methods determine user access and mentions profile mapping. It shows that SAML 2.0 is selected as the method. The "Default Relay State" field is empty. A note states that SAML 2.0 is not configured until setup instructions are completed, with a "View Setup Instructions" button. A separate note about Identity Provider metadata is also present.

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

General Sign On Import Assignments

Settings

[Edit](#)

Sign on methods

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

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

SAML 2.0

Default Relay State

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

[View Setup Instructions](#)

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



- 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/)¹¹, log in to your admin account, and select **Users > Bring your IdP**.

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', 'Bring your IdP' (which is highlighted with a red box), 'IGEL OS IdP', and 'My Profile'. Below the navigation bar, there's a search bar with a magnifying glass icon and a placeholder 'Insert your question here'.

- Enter the following data from your metadata file:

¹¹ <https://cosmos.igel.com/>



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

```
<md:EntityDescriptor entityID="http://www.okta.com/...">
  <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" 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 lines. 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, there are tabs: General, Sign On, Import, and Assignments, with "Assignments" highlighted and surrounded by a red box. Below 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:

Filters	Person	Type	Action
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 (marked as NEW), Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main content area displays a list of existing applications: AAD_APP (Client ID: 42d6943e-7a), PingOne Admin C (Client ID: 9b35ec7c-06), PingOne Application (Client ID: 0fbe6a70-84), and PingOne Self-Serv (Client ID: d1f8512d-34). 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. The 'Name and Describe Application' section contains fields for 'Application Name' (set to 'Test Application') and 'Description'. An 'Icon' field is present with a placeholder image. The 'Choose Application Type' section offers four options: SAML Application, OIDC Web App, Single-Page, and Worker. The 'SAML Application' option is selected and expanded, showing its description: 'Applications that are accessed within a browser using the SAML protocol.' The 'OIDC Web App' section describes web applications using OpenID Connect. The 'Single-Page' section describes front-end applications using APIs. The 'Worker' section describes applications using the PingOne admin API. At the bottom of the dialog, there are 'Configure' and 'Cancel' buttons.

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



The screenshot shows the 'Applications' page in the PingIdentity interface. A red box highlights the 'Application Name' field, which contains 'Test Application'. Another red box highlights the 'SAML Application' option under 'Choose Application Type', which is described as 'Applications that are accessed within a browser using the SAML protocol'. At the bottom right of the configuration dialog, a red box highlights the 'Configure' button.

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

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



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 the 'Configuration' tab of the AAD_APP application settings. It displays several SAML connection details:

- 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](#)¹², 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 & 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 & 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.

¹² <https://cosmos.igel.com/>



Installing / Upgrading to IGEL UMS 12

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

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

If you exclusively manage IGEL OS 12 devices, you may not need an IGEL Cloud Gateway (ICG) between your UMS 12 and your devices, regardless of whether the devices are inside or outside the company network. Whether an ICG is required or not depends on your particular use case or policy. See [IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices](#).

If you manage remote IGEL OS 11 devices and want to manage also your remote IGEL OS 12 devices via ICG, ICG 12 is required.

If you manage your remote IGEL OS 12 devices without ICG and your remote IGEL OS 11 devices with ICG, you can use ICG 12 or ICG 2.x.

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

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

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

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

1. Download IGEL UMS 12 from the [IGEL Download Server](#)¹³.
2. Consider the installation requirements, see [Installation Requirements for the IGEL UMS](#). If you are going to upgrade your existing UMS installation, see also [Updating UMS](#).
3. Install the UMS. Depending on your needs, you can install **standard UMS**, **Distributed UMS**, or **UMS High Availability**. Include the **UMS Web App** and the **UMS Console** into the installation – both of them are currently required for the management of your UMS installation and devices.

¹³ <https://www.igel.com/software-downloads/cosmos/>



Setup - Universal Management Suite 12

Select Components

Which components should be installed?

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

Standard UMS with embedded database	
<input checked="" type="radio"/> Standard UMS (stand-alone)	1.148,3 MB
<input checked="" type="checkbox"/> with UMS Web App	416,5 MB
<input checked="" type="checkbox"/> with UMS Console	170,4 MB
<input checked="" type="checkbox"/> with Embedded Database	20,1 MB
<input type="radio"/> Distributed UMS	541,6 MB
<input type="checkbox"/> with UMS Web App	416,5 MB
<input type="checkbox"/> with UMS Console	170,4 MB
<input type="radio"/> UMS High-Availability-Network	616,4 MB
<input type="checkbox"/> UMS Server	170,4 MB
<input type="checkbox"/> with UMS Console	416,5 MB
<input type="checkbox"/> with UMS Web App	215,4 MB
<input type="checkbox"/> UMS Load Balancer	170,4 MB
<input type="radio"/> Only UMS Console	

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

< Back Next > Cancel

Information on how to install the UMS can be found under:

Windows: IGEL UMS Installation under Windows

Linux: IGEL UMS Installation under Linux

Information on how to upgrade the UMS can be found under:

Windows: Updating the IGEL UMS under Windows

Linux: Updating the IGEL UMS under Linux

- ⓘ You can update to UMS version 12.01.110 or higher from

- UMS 6.x

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

- UMS 12.00.900
 - UMS 12.01.x

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



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

i For Update Installations Only

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



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

i UMS 12 Communication Ports

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

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

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

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



- ⓘ The FQDN and port of your external load balancer / reverse proxy must be specified in the UMS Console under **UMS Administration > Global Configuration > Server Network Settings > Cluster Address**. Information on the Cluster Address can be found under Server Network Settings in the IGEL UMS.
- ✓ It is recommended to check your rights since UMS 12 has new permissions, e.g. **UMS Console > System > Administrator accounts > New / Edit > General - WebApp > App Management** for managing IGEL OS Apps. See General Administrator Rights and Important Information for the IGEL UMS Web App.



Registering the UMS

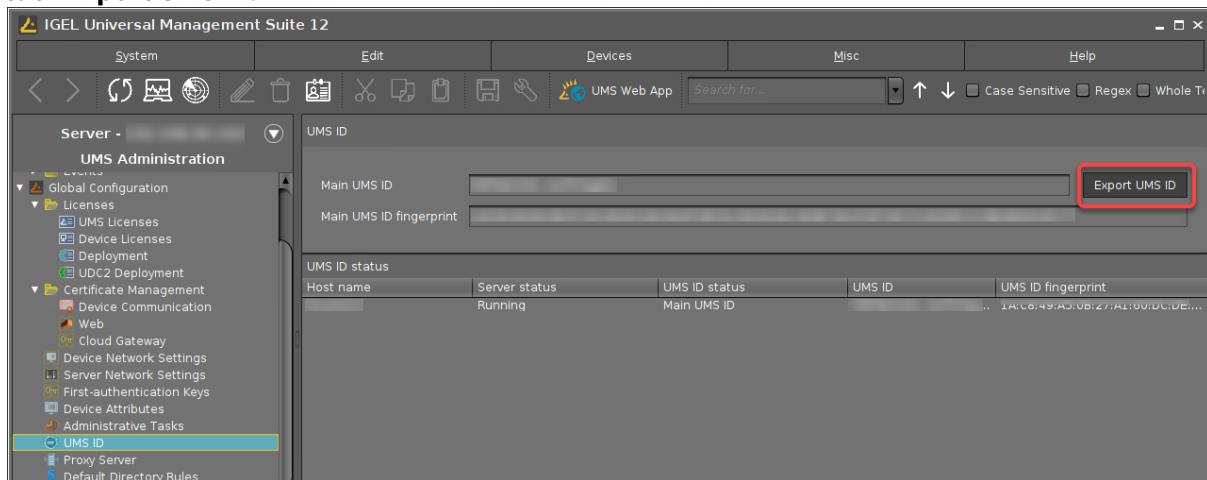
To authenticate your UMS to the IGEL Cloud Services, you must register your UMS. This involves uploading the UMS ID, which is essentially a certificate of your UMS, to the IGEL Customer Portal.

- 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

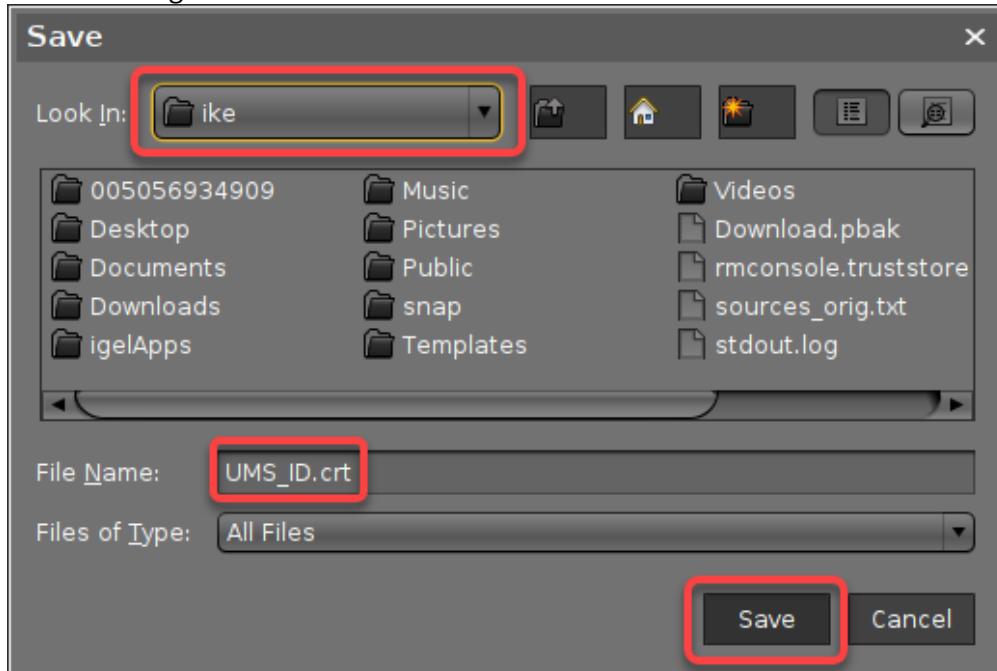
To upload the UMS ID, we must export it from the UMS.

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

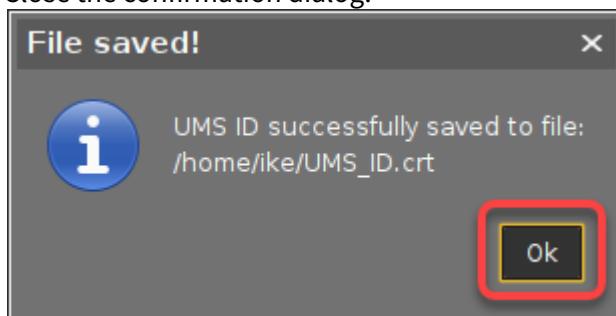




2. Select a storage location and click **Save**.



3. Close the confirmation dialog.



Registering the UMS

1. Open [IGEL Customer Portal¹⁴](#) in your browser and log in to your admin account.

¹⁴ <https://cosmos.igel.com/>



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

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

UMS Management								Register a new UMS Instance
All > Account = Test Company	UMS Name	X.509 Certificate	Expiration Date	Fingerprint	Enable App Portal	Created by(owned_by)	Created	Updated
			2042-04-09 11:03:49	...	true		2023-02-09 12:07:23	
			2042-04-09 06:10:55	...	true		2023-02-09 11:39:19	
			2042-04-07 15:08:18	2...	true		2023-02-06 15:02:02	
			2042-03-28	3...	true		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 215).
- **Required - Upload:** Upload the certificate file (UMS ID) of your UMS. Make sure that the certificate file has the extension `.cer`, `.crt`, or `.pem`

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							Register a new UMS Instance
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). For that, we are using the OpenID Standard to obtain user information and the standardised OAuth 2.0 authorisation protocols. Please follow our instructions to register the OBS as an app in your Azure AD, Ping Identity, Okta or other IdP.

As an alternative, you can use the IGEL Onboarding Service not with the UMS, but with the IGEL Cloud Gateway (ICG). The ICG version 12.01 or higher is required.

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

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

Activating the Onboarding Service (OBS)

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

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

Configuring the Identity Provider

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

- [Azure AD\(see page 54\)](#)
- [Okta\(see page 79\)](#)
- [Ping Identity\(see page 91\)](#)

¹⁵ <https://cosmos.igel.com/>



Downloading the Root Certificate Chain

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

Of the UMS

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

A screenshot of the UMS 12 web interface. At the top, there is a navigation bar with tabs: UMS 12, Devices, Configuration, Network (which is highlighted with a red box), and three more. Below the navigation bar, there is a sidebar with a gear icon (highlighted with a red box) and a server name 'td-ums12'. The main content area shows 'UMS Server State' with a green banner stating 'UMS Server is running' and 'ICG Connections: 0/0 connected'. To the right, there is a 'Requests' chart showing successful requests over time from 8:55 AM to 2:55 PM on November 21, 2022. The chart has three series: Successful (green), Waiting (grey), and Failed (red). All series show zero activity.

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



3. Click **Download Certificate Chain**.

A screenshot of the UMS Web App interface. On the left is a sidebar with a gear icon labeled "Settings". The main content area has a header "IGEL OS Onboarding". Below it is a section titled "OBS Routing Info" with an information icon. It contains two input fields: "UMS Hostname" with a placeholder and a copy icon, and "UMS Port" set to "8443" with a copy icon. At the bottom of this section is a button labeled "Download Certificate-Chain" with a download icon, which is enclosed in a red rectangular box.

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

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

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

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



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

The screenshot shows the UMS 12 | HA interface. The top navigation bar includes tabs for UMS 12 | HA, Devices, Configuration, Apps, Network, and Logging. The Network tab is active. On the left, a sidebar lists UMS Server (UMS 2, UMS 1) and IGEL Cloud Gateway (ICG 1 (111), ICG 2 (112)). The main content area displays the 'IGEL Cloud Gateway State' for ICG 1 (111). It shows 'Connected Devices: 0' and 'UMS Servers Connections: 2/2 connected' (UMS 2 and UMS 1). Below this is the 'IGEL Cloud Gateway Details' section, which includes fields for Process ID, Last Change, Cluster ID, Operating System, Host Name, Process Type, Port, and Version. The 'External Address' field contains 'icg' and the 'External Port' field contains '8443'. Both of these fields are highlighted with yellow boxes.

Field	Value
External Address	icg
External Port	8443

3. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway**.
4. Export each certificate of the ICG's chain except for the end certificate: Right-click the certificate and select **Export certificate** in the context menu.



The screenshot shows the 'Certificates' section of the UMS Administration module. The left sidebar shows 'UMS Administration' with 'UMS Network' and 'Global Configuration' expanded. In the main pane, there are three certificates listed: 'Root certificate', 'Intermediate Certificate', and 'End Certificate'. A context menu is open over the 'Intermediate Certificate', with the 'Export certificate' option highlighted.

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

Example:

```
-----BEGIN CERTIFICATE-----
MIIFPTCCAyWgAwIBAgIFAIKGvrEwDQYJKoZIhvcNAQELBQAwVzEkMCIGA1UEAw
bSUQtLTQ5NzE2
LTE2ODE5NzkyNDEwOTYtOC0wMQ0wCwYDVQQKDARJR0VMMRMwEQYDVQQHDAoxND
AxODM1MDYyMQ
SW
.....
jqzhUGI+dZyTguXkzM2T4ACJUVm7G3mWDSCuMpt5laaE8kGEB2J6cbY9qV4QA5gi
CKF01PgJ6m
QZ
3kDHoNX9DLKSyJtAWS6CJaaGWMWX0wtuyEQ5sZ81UhGKnQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFMDCCAxigAwIBAgIFAPAz/
aEwDQYJKoZIhvcNAQELBQAwVzEkMCIGA1UEAw
bSUQtLTQ5NzE2
LTE2ODE5NzkyNDEwOTYtOC0wMQ0wCwYDVQQKDARJR0VMMRMwEQYDVQQHDAoxND
AxODM1MDYyMQ
SW
.....
wy/
0Y3S4LVHhWtAiT1dBza97uWk9zKL65HbwPFwwZ021Pjb2NaWJPL+OEAHPk5eamCm
FzJeUQqe
0pwHv6AgvJyfEuxsMHURs98psMhw
-----END CERTIFICATE-----
```



Creating the Record Set for the OBS Routing

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

Welcome to IGEL COSMOS!

Insert your question here

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
		8443			2022-11-12 23:30:18		2042-11-12 10:00:31
		8443			2022-10-05 10:08:18		2042-09-28 02:18:51
		8443		?	2022-10-27 19:05:09		2023-11-10 20:44:53
		8443	r		2022-11-04 09:59:13		2042-11-04 05:52:44

3. Enter the following data:

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

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

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



IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name

* UMS Hostname

* UMS Port

Mapped Users

Actions	Email Address
<button>Add</button>	

Mapped Domains

Actions	Domain
<button>Add</button>	

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

Required - Upload

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



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

IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name

* UMS Hostname

* UMS Port

Mapped Users

Actions	Email Address
Add	

Mapped Domains

Actions	Domain
Add	

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

Required - Upload



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

The screenshot shows the 'IGEL OS Onboarding Registration' page. At the top, it says 'Register your IGEL OS Onboarding'. Below that, a note says 'This item only works with OS12'. It asks to upload a CA certificate, stating that the certificate will be automatically linked to the user account. There are three input fields: 'Display Name' (empty), 'UMS Hostname' (containing 'myums.company.com'), and 'UMS Port' (containing '8443'). Under 'Mapped Users', there is a table with columns 'Actions' and 'Email Address', and a blue 'Add' button. Under 'Mapped Domains', there is a table with columns 'Actions' and 'Domain', and a red-bordered blue 'Add' button. A note at the bottom says 'Please upload your CA certificate (only .cer / .crt / .pem files will be accepted!)'. A blue 'Required - Upload' button is also present.

5. In the dialog, enter the e-mail address of the user we have created in Azure AD or the relevant domain and click **Add**.
6. Click **Required - Upload** to upload the UMS root certificate chain.
If you want to use the OBS with the ICG, use here the file `icg_chain.crt` you obtained as described above(see page 43).



IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name

* UMS Hostname

* UMS Port

Mapped Users

Actions	Email Address
Add	

Mapped Domains

Actions	Domain
Add	

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

Required - Upload

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



Screenshot of the Initial Configuration of the IGEL Onboarding Service (OBS) interface. The form includes fields for Display Name, UMS Hostname, and UMS Port. Below these are sections for Mapped Users and Mapped Domains, each with an "Add" button. A note at the bottom asks to upload a CA certificate (.cer/.crt/.pem). The "Submit" button is located at the bottom right.

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

Screenshot of the same configuration interface after step 8. The "Submit" button is highlighted with a red box.

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 158).



Configuring Azure as Identity Provider

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

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

Creating an Azure Web Application That Will Serve as Identity Provider

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

A screenshot of the Azure portal's homepage. At the top, there's a "Welcome to Azure!" message and three promotional cards: "Start with an Azure free trial", "Manage Azure Active Directory", and "Access student benefits". Below these, 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. A red box highlights the "Azure Active Directory" icon, which is also circled. To the left of the main content area, there are buttons for "Create a resource" and "More services", with an arrow pointing from the "More services" button towards the highlighted "Azure Active Directory" icon.



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, there's a message about the end of support for ADAL and Azure AD Graph. The main area shows tabs for All applications, Owned applications (which is selected and highlighted with a blue underline), and Deleted applications. There's a search bar and a 'View all applications in the directory' button. On the left, there's a sidebar under 'Manage' with options like 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 also listed. 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: The redirect URI is listed as "1web.0spa.0public client".

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

Managed application in local directory: The application is identified as "OBS Testing application".

Feedback and Notices: There are two informational notices at the bottom:

- "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 at the bottom 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**.

The screenshot shows the Azure portal interface for managing an app registration. The left sidebar lists several sections: Overview, Quickstart, Integration assistant, Manage (with sub-options like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest), and Support + Troubleshooting (with 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 displays 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 shows no results, with columns for Claim, Description, and Token type.

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

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



6. Click Add.

The screenshot shows the Microsoft Azure portal's 'Token configuration' page for an app registration. 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'. The 'Add' button at the bottom left of the modal is highlighted with a red box.

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

The screenshot shows the 'Add optional claim' modal window. It contains a note: '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 note 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:



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

- 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](#)¹⁶ in your browser, log in to your admin account, and select **Users > IGEL OS IdP**.

¹⁶ <https://cosmos.igel.com/>



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

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	<input type="text" value="My OBS identity provider"/>	Submit				
Client ID	<input type="text"/>					
Client Secret	<input type="text"/>					
* Authorization Endpoint URL	<input type="text"/>					
* Token Endpoint URL	<input type="text"/>					
Mapped Domains <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Add Remove All <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 10%;">Actions</th> <th style="width: 90%;">Domain Name</th> </tr> </thead> <tbody> <tr> <td colspan="2">No data to display</td> </tr> </tbody> </table> </div>			Actions	Domain Name	No data to display	
Actions	Domain Name					
No data to display						

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 managing an application. The left sidebar lists various management sections like Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, and Roles and administrators. The main content area is titled 'OBS Testing application' and shows the 'Endpoints' tab selected. Under the 'Essentials' section, it displays the application's display name ('OBS Testing application'), client ID, object ID, directory ID, and supported account types ('My organization only'). A note at the bottom indicates that starting June 30th, 2020, no new features will be added to ADAL.

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

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

This screenshot shows the 'Endpoints' page for the 'OBS Testing application'. It lists four OAuth 2.0 endpoints: v2, v1, and two for token endpoints. The 'OAuth 2.0 authorization endpoint (v2)' is listed as 'https://login.microsoftonline.com/'. To its right, there is a 'Copy to clipboard' button, which is highlighted with a red box. Below the URL, there is a dropdown menu showing the full URL: 'https://login.microsoftonline.com/oauth2/v2.0/authorize'.

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

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" registration details. The "Overview" tab is selected. In the "Essentials" section, the "Application (client) ID" field is highlighted with a red box, and a "Copy to clipboard" button is also highlighted with a red box. The "Client credentials" section shows "Add a certificate or secret". The "Redirect URIs" section shows "1 web, 0 spa, 0 public client". The "Application ID URI" section shows "Add an Application ID URI". The "Managed application in local directory" section shows "OBS Testing application".

The screenshot shows the Azure portal interface for managing app registrations. The "OBS Testing application" is registered under the "Web" type. The "Application (client) ID" is listed as "1 web, 0 spa, 0 public client". A "Copy to clipboard" button is visible next to the ID. The "Client credentials" section includes a link to "Add a certificate or secret". The "Redirect URIs" section lists "1 web, 0 spa, 0 public client". The "Application ID URI" section has a link to "Add an Application ID URI". The "Managed application in local directory" section shows the application name again. There are two informational cards at the bottom: one about the new App registrations experience and another about the deprecation of ADAL and Graph starting June 30, 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
[Redacted]

* Client Secret
[Redacted]

* 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



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

The screenshot shows the Azure portal's App Registrations blade. The left sidebar has 'OBS Testing application' selected. The main area shows the 'Overview' tab is active. In the 'Essentials' section, there are fields for 'Display name' (set to 'OBS Testing application'), 'Application (client) ID', 'Object ID', 'Directory (tenant) ID', and 'Supported account types' (set to 'My organization only'). To the right, under 'Client credentials', a red box highlights the 'Add a certificate or secret' button. Below it are 'Redirect URLs' (set to '1 web, 0 spa, 0 public client') and 'Application ID URI' (with a link to 'Add an Application ID URI'). A note states 'Managed application in local directory OBS Testing application'. At the bottom, there are two informational messages about the new App registrations experience and the end of support for ADAL.

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 has 'Certificates & secrets' selected. The main area shows tabs for 'Certificates (0)', 'Client secrets (0)' (which is selected), and 'Federated credentials (0)'. A note says 'Application registration certificates, secrets and federated credentials can be found in the tabs below.' Below the tabs, it says 'A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.' A red box highlights the '+ New client secret' button. A note at the bottom 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 red arrow points from the bottom left towards the "Add" button, which is highlighted with a red border.



15. Copy the client secret to the clipboard.

A screenshot of the IGEL Onboarding Service interface. At the top, there are two notifications: one about giving feedback and another about application registration certificates. Below them, the "Client secrets" tab is selected, showing a single entry for "OBS credentials". The "Value" column contains the client secret, which has a "Copied" status indicator and a copy icon. A red box highlights this copy icon. Other columns include "Description" (OBS credentials), "Expires" (11.1.2023), and "Secret ID".

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



Add Row

* Domain Name
onmicrosoft.com

* Display Name
My OBS identity provider

* Client ID

* Client Secret
.....

SHOW

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

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

Mapped Domains

Actions	Domain Name
	No data to display

Add **Cancel** **Add**

The screenshot shows the 'Add Row' dialog for configuring an OBS Identity Provider. It includes fields for 'Domain Name' (onmicrosoft.com), '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 this, a 'Mapped Domains' section is shown with an 'Add' button (highlighted with a red box) and a table with no data. The 'Add' button in the table section is also highlighted with a red box.

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. The 'Submit' button at the top right 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/.../oauth2/v2.0/authorize, https://login.microsoftonline.com/.../oauth2/v2.0/token, .onmicrosoft.com, 2022-12-01 16:01:06, and 2022-12-01 16:01:06.

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/.../oauth2/v2.0/authorize	https://login.microsoftonline.com/.../oauth2/v2.0/token	.onmicrosoft.com	2022-12-01 16:01:06	2022-12-01 16:01:06
		*****	https://login.microsoftonline.com/.../oauth2/v2.0/authorize	https://login.microsoftonline.com/.../oauth2/v2.0/token	.onmicrosoft.com	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 various options like Overview, Preview features, Diagnose and solve problems, and a prominent 'Users' option which is highlighted with a red box. The main content area displays basic information about the tenant, including Name (IGEL Technology GmbH), Tenant ID, Primary domain (igelobs.onmicrosoft.com), License (Azure AD Free), and counts for Users (1), Groups (0), Applications (1), and Devices (0). A search bar at the top says 'Search your tenant'.

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

The screenshot shows the 'Users' page in Azure. The left sidebar includes 'All users (preview)', 'Audit logs', 'Sign-in logs', and 'Manage' sections. The main area shows a table with one user listed: Display name PA, User principal name igel.com#EX..., User type Member, On-premises sync No, and Identity External. Above the table, there is a 'New user' dropdown menu with two options: 'Create a new user' (highlighted with a red box) and 'Invite external user'.

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

- **User name:** A valid e-mail address.
- **Name:** Display name
- **Let me create the password:** For our purposes, you can use this option.



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

The screenshot shows the 'Identity' section of the user creation form. Fields highlighted with red boxes include 'User name' (containing 's.onmicrosoft.com'), 'Name' (containing 'OBS User'), and 'Initial password' (containing '****'). A red arrow points from the 'Create' button at the bottom to the 'Usaage location' field. The 'Password' section shows the 'Let me create the password' option selected. The 'Groups and roles' section shows '0 groups selected' and 'User' under Roles. The 'Settings' section includes 'Block sign in' (Yes/No) and 'Usaage location' fields.

Identity

User name * (s.onmicrosoft.com)
Name * (OBS User)
First name
Last name

Password

Auto-generate password
Let me create the password (selected)

Initial password * (****)

Groups and roles

Groups (0 groups selected)
Roles (User)

Settings

Block sign in (Yes/No)
Usaage location
Create



Configuring Okta as Identity Provider

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

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

Creating an Okta Application That Will Serve as Identity Provider

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

A screenshot of the Okta Applications dashboard. On the left, there is a sidebar with various menu items: Dashboard, Directory, Customizations, Applications (which is selected and highlighted with a red box), Self Service, Security, Workflow, Reports, and Settings. In the main content area, there is a search bar at the top. Below it, there are two buttons: 'Create App Integration' (highlighted with a red box) and 'Browse App Catalog'. Underneath these buttons is a table with columns for 'STATUS' (ACTIVE and INACTIVE) and a list of applications. Each application entry includes a small icon, the application name, and a settings gear icon. The 'Create App Integration' button is the primary focus of the screenshot.

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



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

Create a new app integration

Sign-in method

[Learn More](#)

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

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

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

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

Application type

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

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

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

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

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

[Cancel](#) [Next](#)

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

- Under **App integration name**, enter a name for your application, e.g. "IGEL Onboarding Service".
- Make sure that as the **Grant type**, the option **Authorization Code** is selected.



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

New Web App Integration

General Settings

App integration name (highlighted with a red box)

Logo (Optional)

Grant type

[Learn More](#)

Client acting on behalf of itself
 Client Credentials

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

Sign-in redirect URIs Allow wildcard * in sign-in URI redirect.
 (highlighted with a red box)
[+ Add URI](#)

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

Assignments

Controlled access

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

Allow everyone in your organization to access
 Limit access to selected groups
 Skip group assignment for now

Save **Cancel**

The app integration is created.



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

The screenshot shows the 'General' tab selected in a navigation bar with other tabs like 'Sign On', 'Mobile', 'Assignments', and 'Okta API Scopes'. Below the tabs is a section titled 'Client Credentials' with an 'Edit' button. Under 'Client ID', there is a blurred input field and a blue 'Edit' button. A tooltip explains it's a public identifier for OAuth flows. Under 'Client authentication', 'None' is selected. There are three radio buttons: 'None' (selected), 'Client secret', and 'Public key / Private key'. Below this, under 'Proof Key for Code Exchange (PKCE)', the 'Require PKCE as additional verification' checkbox is checked. The entire 'Client Credentials' section is enclosed in a light gray box.

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



The client secret will be created.

Registering Our Okta Application in the IGEL Customer Portal

1. Open the [IGEL Customer Portal](https://cosmos.igel.com/)¹⁷ in your browser, log in to your admin account, and select **Users > IGEL OS IdP**.

¹⁷ <https://cosmos.igel.com/>



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

IGEL OS IdP Management							
All > Account =					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

Submit

Required information

Client ID
Authorization Endpoint URL

Token Endpoint URL



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

A screenshot of the Okta application interface. The top navigation bar shows the word "okta". Below it is a search bar with placeholder text "Search...". A horizontal menu bar contains five tabs: "General" (which is underlined in blue, indicating it is selected), "Sign On", "Mobile", "Assignments", and "Okta API Scopes". Under the "General" tab, there is a section titled "Client Credentials". Within this section, there is a field labeled "Client ID" containing a redacted value. To the right of this field is a blue "Edit" button, which is also enclosed in a red rectangular box. Below the "Client ID" field is a descriptive text: "Public identifier for the client that is required for all OAuth flows." The entire screenshot is framed by a thick black border.

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name
My OBS identity provider

* Client ID

* Client Secret

* Authorization Endpoint URL

* Token Endpoint URL

Mapped Domains

Add Remove All

Actions	Domain Name
No data to display	



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

The screenshot shows the 'General' tab selected in the Okta application settings. Under 'Client Credentials', the 'Client ID' is listed with a note about it being a public identifier for OAuth flows. The 'Client authentication' section shows 'Client secret' selected. Under 'Proof Key for Code Exchange (PKCE)', the 'Require PKCE as additional verification' checkbox is checked. In the 'CLIENT SECRETS' section, a table lists a single secret created on Aug 28, 2023. The 'Secret' column shows a redacted string of characters. The 'Status' column shows 'Active' with a dropdown arrow. A red box highlights the 'Copy' icon next to the secret value.

Creation date	Secret	Status
Aug 28, 2023	Active ▾

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name	My OBS identity provider				
* Client ID	<input type="text"/>				
* Client Secret	<input type="password"/> SHOW				
* Authorization Endpoint URL	<input type="text"/>				
* Token Endpoint URL	<input type="text"/>				
Mapped Domains					
<input type="button" value="Add"/> <input type="button" value="Remove All"/> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Actions</th> <th style="width: 90%;">Domain Name</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">No data to display</td> </tr> </tbody> </table>		Actions	Domain Name	No data to display	
Actions	Domain Name				
No data to display					

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

```

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

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

This item only works with OS12

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

* Display Name
My OBS identity provider

* Client ID
[Redacted]

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

* Authorization Endpoint URL
https://[REDACTED].okta.com/oauth2/default/v1/authorize

* Token Endpoint URL
https://[REDACTED].okta.com/oauth2/default/v1/token

Mapped Domains

Actions	Domain Name
	No data to display



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

The screenshot shows a modal dialog titled 'Add Row' over a background configuration page. The dialog has a field labeled '* Domain Name' containing '.com'. In the background, there's a section for 'Mapped Domains' with an 'Add' button highlighted by a red box. Another 'Add' button is highlighted in the top right corner of the dialog itself.

11. Click **Submit**.

The data record is created.



Configuring Ping as Identity Provider

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

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

Creating a Ping Application That Will Serve as Identity Provider

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

A screenshot of the Ping Identity web interface. The left sidebar has a dark blue background with white text and icons. It includes sections for Overview, Dashboards, Identities, Connections (with Applications selected), Applications Catalog, Application Portal (marked as NEW), Identity Providers, External IDPs, and Ping Products. The main content area shows a header with a back arrow, the URL trial_igel_1501309074, and a dropdown for Administrators. Below this is a search bar and a 'Filter' button. A large red square highlights the 'Applications' button in the top navigation bar. The main list area shows five blurred application entries, each with a small colored thumbnail (blue, red, red, red, blue) and a blurred name.

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



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

The screenshot shows the 'Add Application' dialog box. At the top left is a blue folder icon followed by the text 'Add Application'. In the top right corner is a small 'X' button. Below the title, there are three input fields: 'Application Name *' (with a red border around it), 'Description' (with a blue border around it), and 'Icon' (which contains a small mountain icon). Below the icon field is the text 'Max Size 1.0 MB'. Under the 'Application Type' heading, there is a 'Show Details' button. A callout box with an exclamation mark says: 'Select an option below or view the [Application Catalog](#) to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.' Below this are five options: 'SAML Application', 'OIDC Web App' (which has a red border around it), 'Native', 'Single-Page', and 'Worker'.

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

- Under **Response Type**, make sure **Code** is selected.
- Make sure that as the **Grant Type**, the option **Authorization Code** is selected and that the **Proof Key for Code Exchange (PKCE) Enforcement** is set to **S256_REQUIRED**.



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

The screenshot shows the 'Edit Configuration' page for the OBS. It highlights three sections with red boxes:

- Response Type**: Shows checkboxes for 'Code' (checked), 'Token', and 'ID Token'. 'Code' is highlighted with a red box.
- Grant Type**: Shows checkboxes for 'Authorization Code' (checked), 'Implicit', 'Client Credentials', and 'Refresh Token'. 'Authorization Code' is checked and highlighted with a red box. Below it, 'PKCE Enforcement' is set to 'S256_REQUIRED'.
- Redirect URIs**: Shows a text input field containing 'https://obs.services.igel.com' and a '+ Add' button. The entire 'Redirect URIs' section is highlighted with a red box.

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

The screenshot shows the 'Token Endpoint Authentication Method' section. It contains three radio buttons: 'None', 'Client Secret Basic', and 'Client Secret Post'. 'Client Secret Post' is selected and highlighted with a red box.

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



Groups.

A screenshot of the IGEL Onboarding Service (OBS) interface. At the top, there's a navigation bar with tabs: Overview (which is highlighted with a red box), Configuration, Resources, Policies, Attribute Mappings, and Access. Below the tabs are several cards: 'Protocol OpenID Connect' (with a gear icon), 'Resource Access 1 Scope' (with a pencil icon), 'Policies None Selected' (with a pencil icon), 'Attributes 1 Mapped' (with a pencil icon), and 'Access All Users' (with a pencil icon). The 'All Users' card is also highlighted with a red box. Below these cards, there are sections for 'App Type' (Web App (OpenID Connect)) and 'Description' (Not Set).

The app integration is created.

Registering Our Ping Application in the IGEL Customer Portal

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

A screenshot of the IGEL COSMOS customer portal. The top navigation bar includes links for Catalog, Knowledge, My History & My Requests, Advanced Service, Users (which is currently selected and has a dropdown arrow), Configure Services, and My Company Subscriptions. A dropdown menu is open under the 'Users' link, listing: Overview, User & Role Administration, Bring your IdP, IGEL OS IdP (which is highlighted with a red box), and My Profile.

¹⁸ <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

* Client ID

Client Secret

* Authorization Endpoint URL

* Token Endpoint URL

Mapped Domains

Actions	Domain Name
Add	No data to display

Submit

Required information

Client ID Authorization Endpoint URL
 Token Endpoint URL



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

A screenshot of the IGEL Onboarding Service (OBS) interface. At the top, there's a navigation bar with tabs: Overview (which is highlighted with a red box), Configuration, Resources, Policies, Attribute Mappings, and Access. Below the tabs, there are several sections: Protocol (OpenID Connect), Resource Access (1 Scope), Policies (None Selected), and Attributes (1 Mapped). Under the Overview tab, there are sections for App Type (Web App (OpenID Connect)), Description (Not Set), Environment ID, Client ID (which is highlighted with a red box), Client Secret, Home Page URL (No Home Page Configured), and Signon URL (Default Signon Page).

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name

My OBS identity provider

* Client ID

* Client Secret

* Authorization Endpoint URL

* Token Endpoint URL

Mapped Domains

Add

Remove All

Actions	Domain Name
	No data to display



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

A screenshot of the IGEL Onboarding Service (OBS) interface. At the top, there is a navigation bar with tabs: Overview (which is selected and highlighted with a red box), Configuration, Resources, Policies, Attribute Mappings, and Access. Below the navigation bar, there are several sections: Protocol (OpenID Connect), Resource Access (1 Scope), Policies (None Selected), Attributes (1 Mapped), and Access (All Users). The main content area contains fields for App Type (Web App (OpenID Connect)), Description (Not Set), Environment ID, Client ID, and Client Secret. The Client Secret field is highlighted with a red box. Other sections include Home Page URL (No Home Page Configured) and Signon URL (Default Signon Page).

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name
My OBS identity provider

* Client ID

* Client Secret
.....| SHOW

* Authorization Endpoint URL

* Token Endpoint URL

Mapped Domains

Add Remove All

Actions	Domain Name
No data to display	

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

A screenshot of the IGEL Onboarding Service (OBS) configuration interface. The top navigation bar includes a folder icon labeled "OBS", a switch, and a close button. Below the bar, tabs for "Overview", "Configuration", "Resources", "Policies", "Attribute Mappings", and "Access" are present, with "Configuration" being the active tab. A sub-header below the tabs reads "Configuration details for an OIDC application." A blue edit icon is located in the top right corner of the main content area. The main content area is titled "URLs" and contains two fields highlighted with red boxes:

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

The URL fields contain placeholder text "[REDACTED]" where specific values have been removed.

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

This item only works with OS12

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

* Display Name
My OBS identity provider

* Client ID

* Client Secret
 SHOW

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

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

Mapped Domains

Actions	Domain Name
	No data to display



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

The screenshot shows the 'Add Row' dialog box overlaid on the main configuration page. The dialog has a title 'Add Row' and a field labeled '* Domain Name' containing '.com'. At the bottom right of the dialog are two buttons: 'Cancel' and 'Add', with 'Add' being highlighted by a red box. In the background, the main page shows sections for 'Client Secret', 'Authorization Endpoint URL', and 'Token Endpoint URL'. Below these is a table titled 'Mapped Domains' with a single row. The 'Actions' column contains an 'Add' button, which is also highlighted by a red box. The 'Domain Name' column shows 'No data to display'.

11. Click **Submit**.

The data record is created.



IGEL App Portal

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

The screenshot shows the IGEL App Portal interface. At the top, there's a header with the IGEL logo, the text "COSMOS Secure Endpoint Platform", a "Login" button, and an information icon. Below the header, there's a navigation bar with "APP PORTAL EXPLORE" and a "All Apps" link. The main area is titled "Discover Our Apps" and features a search bar with "Sort by Name" and a "Search" button. Below the search bar, there are two dropdown menus: "Categories" set to "All" and "Sort by" set to "Name". The main content area displays a grid of application cards. Each card includes the app icon, name, version, last update, size, and a brief description. Some cards have a "NEW" badge. The applications shown are:

- CPcore Binary**: Version 1.1.0 BUILD 2. Last updated 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. Category: Cloud.
- CUPS printing app**: Version 1.0.0 BUILD 2. Last updated 12. December 2022. Size 11.75 MB. Description: CUPS printing application provides printing functionality for IGEL OS. Category: Peripheral.
- Chromium Browser**: Version 108.0.5359.124 BUILD 1 RC 4. Last updated 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. Category: Browser.
- Chromium Multimedia Codec**: Version 107.0.5304.62 BUILD 1 RC 2. Last updated 08. February 2023. Size 1.5 MB. Description: Multimedia codec (H.264) support for Chromium Browser.
- Chromium ffmpeg codec**: Version 108.0.5359+1 BUILD 1. Last updated 12. December 2022. Size 1.75 MB. Description: Contains ffmpeg with aac/ac3/mpg4audio/h264/mov/mp3 and gstreamer ffmpeg plugin.
- Cisco Jvdi plugin**: Version 14.1.2.307144 BUILD 1. Last updated 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**: Version 42.6.8.5 BUILD 1 RC 1. Last updated 24. February 2023. Size 59.25 MB. Description: Smoother meeting experience under VDI.
- Cisco Webex VDI**: Version 42.6.0.22645 BUILD 1 RC 1. Last updated 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.

i **Where Are the IGEL COSMOS Cloud Services Data Stored?**

Currently, the IGEL COSMOS Cloud Services and apps available in the IGEL App Portal are stored in Azure Region West-Europe, location Amsterdam. The associated app metadata are stored in Frankfurt (Germany west central).

The Insight Service data are currently also stored in Frankfurt (Germany west central). All data centers and their operators are fully ISO/IEC 27001 certified.

Access to the IGEL App Portal

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



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

You can open the IGEL App Portal

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



- locally on the device via the **App Portal** application (i.e. context: OS12)
With this method, you can install or uninstall apps locally on the device. For more information, see [Installing IGEL OS Apps Locally on the Device](#)(see page 188).

Here, you can find the following buttons:

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

- via **UMS Web App > App Portal** (i.e. context: UMS admin)

With this method, you can import apps in the UMS to deploy them to your endpoint devices.

Here, you can find the following buttons:

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

The screenshot shows the 'APP PORTAL UMS ADMIN' interface. At the top, there's a navigation bar with 'APP PORTAL' and 'UMS ADMIN'. Below it, a search bar says 'Discover Our Apps' with buttons for 'ALL', 'AVAILABLE', and 'IMPORTED' (which is highlighted with a red box). To the right are filters for 'Categories' (set to 'All') and 'Sort by' (set to 'Name'). A search bar and a magnifying glass icon are also present. The main area displays four app cards:

- CUPS printing app**: Version 1.0.0 BUILD 2. Last update: 12. December 2022. Size: 11.75 MB. Category: Peripheral.
- Chromium Browser**: Version 108.0.5359.124 BUILD 1 RC 4. Last update: 23. February 2023. Size: 130.25 MB. Category: Browser.
- Citrix Workspace App**: Version 23.2.0.10-1 BUILD 1 RC 2. Last update: 23. February 2023. Size: 144.75 MB. Categories: VDI, Cloud.
- Zoom**: Version 5.13.7.683 BUILD 1 RC 1. Last update: 24. February 2023. Size: 197.5 MB. Category: Zoom Cloud Meetings.



The screenshot shows the IGEL UMS 12 web interface. At the top, there are tabs for 'UMS 12', 'Devices', 'Apps' (which is the active tab), and '4 more'. Below the tabs, there's a sidebar labeled 'Apps' with a 'All' button. The main content area shows a list of apps: 'Chromium Browser' (selected), 'CUPS printing app', and 'Citrix Workspace App'. To the right of the list, there's a detailed view for 'Chromium Browser' with options like 'Create new profile', 'Set Default Version', and 'Delete App'. A red arrow points from the 'Apps' tab in the top navigation to the 'Chromium Browser' entry in the list.

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

Importing Apps to the IGEL UMS

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

The screenshot shows the IGEL COSMOS Secure Endpoint Platform App Portal. The top navigation bar includes 'COSMOS Secure Endpoint Platform', 'APP PORTAL', 'UMS ADMIN', and a user icon. Below the navigation, the path 'All Apps > Chromium Browser' is shown. The main content area displays the 'Chromium Browser' app details. It shows the app icon, status 'UP TO DATE', version '108.0.5359.94 BUILD 1 RC 1', and a large blue 'IMPORT' button. A red arrow points from the 'IMPORT' button to the button itself. Below the app details, there's a section titled 'Chromium' with a 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 the selected app / app version has already been imported, the **Import** icon is greyed out.



IGEL UMS 12: Basic Configuration

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

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

First Steps in the IGEL UMS

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

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

System Configuration

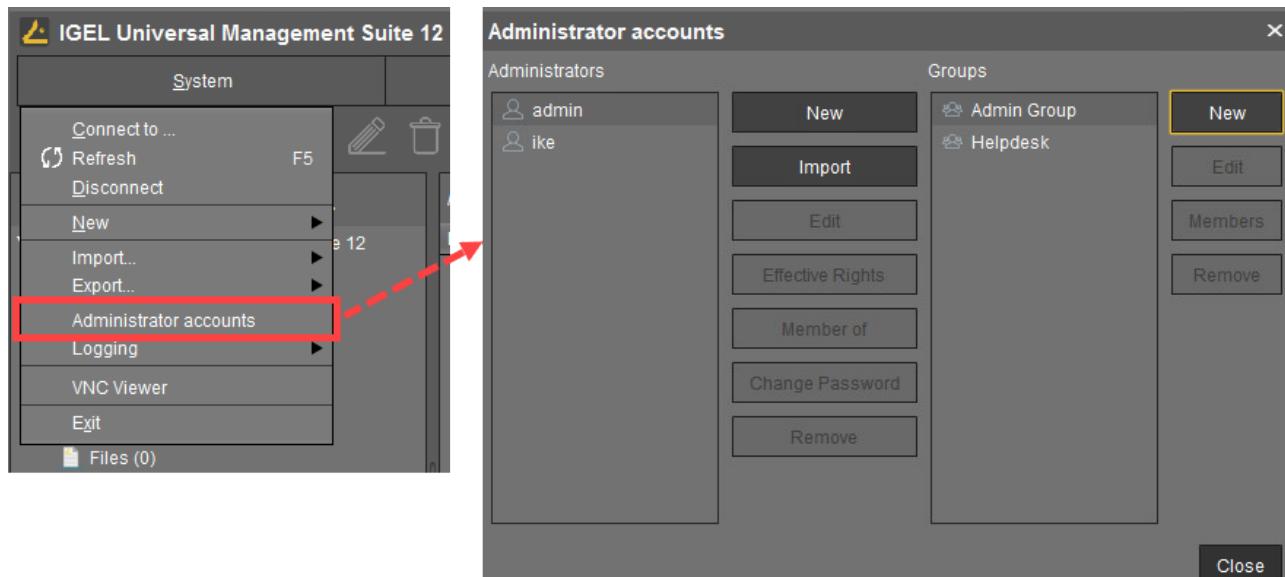
1. Activate logging under **UMS Administration > Global Configuration > Logging**.
2. Under **UMS Administration > Administrative tasks**, create the following administrative tasks:
 - Create backup (for the embedded database only. If you use an external database, see Creating a Backup of the IGEL UMS)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

Administrator Accounts

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

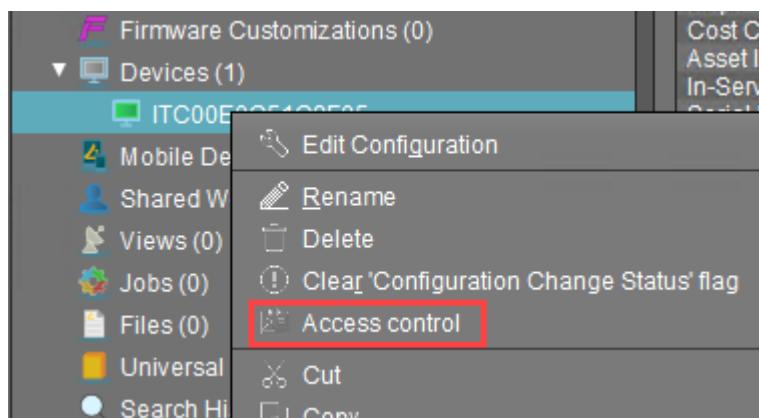
If you do not want to adopt the Active Directory structure, you can create local administrators and groups manually: **UMS Console > System > Administrator Accounts > New**.

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



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

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



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

Optional: Preconfiguring Your Devices Before Onboarding

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





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

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

The screenshot shows the 'APP PORTAL' section of the COSMOS interface. A red arrow points from the 'DESCRIPTION' tab to the 'IMPORT' button, which is highlighted with a red box. The 'Chromium Browser' app is listed as 'UP TO DATE' with version '108.0.5359.94 BUILD 1 RC 1'. Below the app details, there is a brief description of Chromium as an open-source browser project.

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

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

The screenshot shows the 'UMS 12' web application interface. The 'Devices' tab is active. On the left, the 'Apps' section shows a list of imported apps, with 'Chromium Browser' selected and its details displayed on the right. A red box highlights the 'Create new profile' button, which is located next to the 'Set Default Version' and 'Delete App' buttons. The right panel also displays the newest imported version of the app and a 'Check for updates' button.

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

- 1) In the **UMS Web App > Devices**, create a device directory: Click , type a directory name, and press [Enter]. For more information, see Creating a Directory Structure in the IGEL UMS Web App.



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' panel showing a list of devices with 0-0 of 0 entries. 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 'Default Directory Rules' section in the UMS Administration module. The left sidebar shows 'Default Directory Rules' is selected under 'Global Configuration'. The main area displays a 'Create default directory rule' dialog with a 'Select criterion' section. A red arrow points to the 'Leave in Subdirectory' checkbox in the toolbar above the dialog.

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 entry 'OS 12 devices (0)'. On the right, a detailed view of 'OS 12 devices' is shown with a red box highlighting the 'Assign object' button. Below it, the 'Properties' section lists the name 'OS 12 devices', directory path 'Devices / OS 12 devices', and 'Number of contained devices' as 0.

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. In the 'Assignments' section, there is a large empty area where assigned objects would appear. At the bottom right are 'Cancel' and 'Save' buttons, with 'Save' being checked.

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 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 'Apps' section of the UMS 12 web interface. On the left, there's a sidebar with 'All' selected. In the main area, a list of apps is shown with 'Chromium Browser' highlighted by a red box. To the right of the list, there's a detailed view for 'Chromium Browser' with options like 'Create new profile', 'Set Default Version', and 'Delete App'. It also displays the newest imported version (108.0.5359.124 BUILD 1 RC 3), the default version (108.0.5359.124 BUILD 1 RC 3), and a note that the newest available version is unknown. A 'Check for updates' button is also present.

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.

i Accepting EULA in the UMS

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

Accepting EULA can be necessary, for example, for automatically registered apps (IGEL OS Base System, all [locally installed apps](#)(see page 188)) or if the EULA is changed. If not accepted in the UMS, the EULA can still be accepted by your users locally on the device via the corresponding [notification dialog](#)(see page 213).

The screenshot shows the 'Versions' tab in the Apps section. It lists two versions: 'Default version (12.01.100 BUILD 1 R...)' and '12.1.100 BUILD 1 TP 2'. The second version has an exclamation mark icon next to it. At the bottom, there's a section for 'EULA State' with a red box around it. It shows 'Not Accepted' and a button labeled 'Accept EULA'.

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



Creating an OS 12 Profile

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

⚠ Implicit App Assignment via Profiles

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

An app version selected in the profile will be assigned to a device. The best practice is to use the **Default Version**, see [Setting a Default Version of an App](#)(see page 117).

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

For more information on the app assignment, see [Assignment of Apps and Profiles](#)(see page 118).

There are two methods to create a profile:

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

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 are profiles for IGEL OS 11 and IGEL OS 12. A red arrow points from the 'IGEL OS 12 (4)' section to the 'Create new profile' dialog. Another red arrow points from the 'Name' input field ('Chromium') to the 'Select Apps' button at the bottom of the dialog.

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(see page 193), 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. Under 'Base System', the 'IGEL OS' app is listed with 'Default version'. Under 'Apps', the 'Chromium Browser' app is selected, indicated by a checked checkbox and highlighted with a red box. Other apps like 'Citrix' and 'CUPS printing app' are also listed. A red arrow points from the 'Show Versions' toggle switch to the 'Save' button at the bottom right of the dialog.



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

6. Click **Save**.

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

7. Configure the desired settings.

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

profile), click **App Selector**

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

The screenshot shows the 'Profile Configurator - Chromium' window. The left sidebar has 'Apps' selected, showing a tree view with 'chromium' expanded, containing 'Chromium Browser Global', 'Chromium Browser Sessions', and 'Chromium browser'. The 'Chromium browser' node is selected. The main area shows a 'Session name' input field with 'Chromium browser' typed into it. Below it is a section titled 'Starting Methods for Session' with five items, each with a switch and a checkbox. The items are: 'Start Menu' (switch on, checkbox checked), 'Menu folder' (switch on, checkbox unchecked), 'Start Menu's System tab' (switch on, checkbox checked), 'Application Launcher' (switch on, checkbox checked), and 'Application Launcher folder' (switch off, checkbox unchecked). 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 118).



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.

Name	Chromium
Description	(empty)
Location	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. IMPORTANT: When you deactivate the parameter, the value will be automatically set back to the default value.
	The parameter is active and the set value will be configured by the profile.

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 main settings: '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' option. At the bottom right 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 118).

Setting a Default Version of an App

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

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

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

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



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

To set a Default Version:

- 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 list of versions is shown, with the 'Default version' entry 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: Chromium, Background, SSH, Terminal, Firefox, and VMware Horizon. The "Chromium" item is highlighted with a red box. To its right is a large blue arrow pointing from left to right, also enclosed in a red box. The "Assignments" section is currently empty. At the bottom right are "Cancel" and "Save" buttons, with the "Save" button being the one highlighted by a red box.

3. Save the changes.

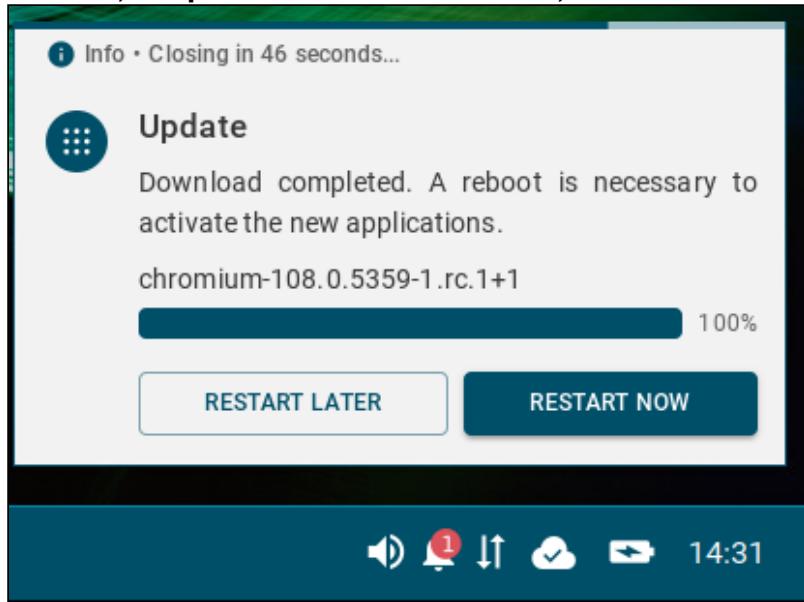
4. Decide when the changes should become effective.

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	Item
Language	OS 12
Terminal	OS 12
Installed Apps	Chromium Chromium Browser

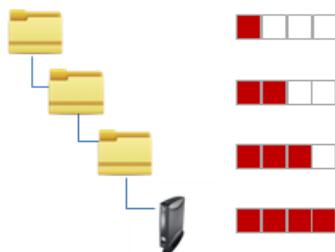
To check the installed apps, go to **Devices > [name of the device] > Installed Apps**; see Checking Installed Apps via the IGEL UMS Web App.



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 117) will be used. It is possible to select the version for an app in the **Assign Object** dialog either under **Assignable Objects** or under **Assignments**.



Assign Object to Device

ITC005056938D22

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.

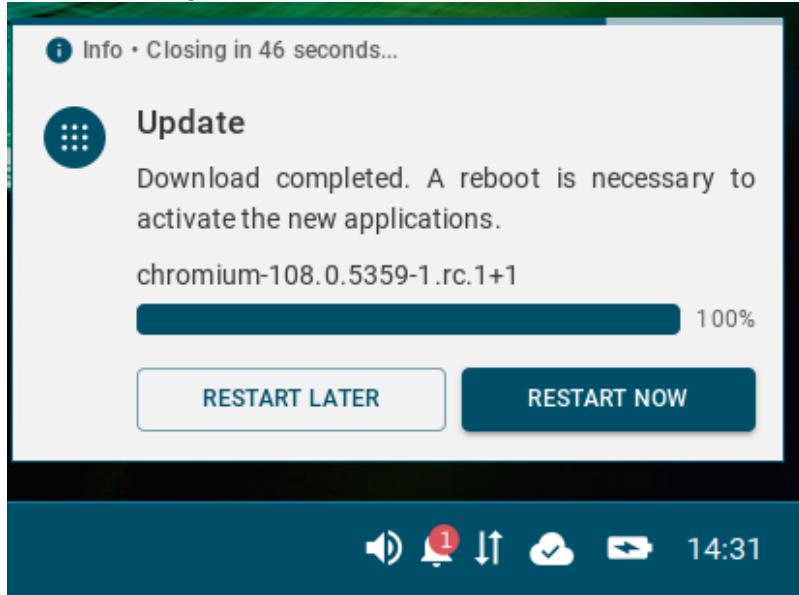
3. Save the changes.
4. Decide when the changes should become effective.

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 117) during the app assignment and profile creation (best practice).

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

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

Update of the IGEL OS Base System

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

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



Preparing the Update

- 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

How to Start with IGEL COSMOS

128 / 226



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 panel displays a list of apps, with 'IGEL OS' highlighted and a red box around it. A modal window titled 'Set Default Version' is open over the list, also with a red box around its title. The modal contains a dropdown menu labeled 'Version' with several options listed. The option '12.01.110 BUILD 1 RC 2' is highlighted with a red box.

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. On the left, the 'Directory Tree' shows a folder named 'Devices (3)' containing 'Augsburg (2)' and 'Bremen (1)', with 'Augsburg (2)' highlighted and a red box around it. The main panel shows a list of devices under 'Augsburg'. To the right, a details panel for 'Augsburg' is open, showing buttons for 'Assign object' (highlighted with a red box), 'Reboot', 'Shutdown', 'Wake up', 'Suspend', and 'Send settings'. Below this is a 'Properties' section and a 'Assigned Objects' section.

A screenshot of the "Assign Object to Directory" dialog in the IGEL UMS Web App. The dialog shows a list of assignable objects on the left and assignments on the right. A red box highlights the "IGEL OS" entry in the list, and a red arrow points to the "Default Ver..." dropdown next to it. A red box also highlights the blue "→" button between the two panes. At the bottom are "Cancel" and "Save" buttons.

The screenshot shows the "Assign Object to Directory" dialog. On the left, under "Assignable Objects", there are three items: "IGEL OS", "CUPS printing app", and "zoom Zoom Media Plugins for VDI". Each item has a "Default Ver..." dropdown. On the right, under "Assignments", there is a large empty area. Between the two panes is a blue "→" button. At the bottom 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 213).

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



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 118).

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.

The screenshot shows the IGEL UMS 12 web interface. On the left, a sidebar lists categories like 'All', 'Browser', 'Cloud', 'VDI', etc. The main area shows a list of apps under 'IGEL OS'. One item, 'Chromium Browser', is highlighted with a red box. To the right, a detailed view for 'Chromium Browser' is shown. It includes a 'Create new profile' button, a 'Set Default Version' button, and a 'Delete App' button. Below these are buttons for 'Import newest version from App Portal' (highlighted with a red box) and 'Update Settings'. The 'Update Settings' section contains options for 'Automatic check for updates in UMS', 'Check for updates', and 'Default Version for assigned Devices'.

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 113).
- 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 118).

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

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

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' sidebar 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). The 'Test Update Chromium' row is highlighted with a red box. To its right is a detailed view of the profile: 'Test Update Chromium' with a shield icon, 'Edit Configuration' button (also highlighted with a red box), and 'Properties' section showing 'Name: Test Update Chromium', 'Directory Path: Profiles / Test App Updates', and 'Id: 19320'. A status bar at the bottom indicates '1 - 1 of 1'.

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

A screenshot of the 'Profile Configurator - Test Update Chromium' dialog. At the top is a title bar with a pencil icon and the text 'Profile Configurator - Test Update Chromium'. Below it is a navigation bar with 'Apps' (highlighted in yellow) and 'System' tabs, and a search icon. The main area shows a tree view with a single node 'chromium' under the 'Apps' tab. At the bottom are three buttons: 'Close' (with a red box around it), 'Save' (with a checkmark icon), and 'Save and Close' (with a disk icon).



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

6. Save the changes.

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

The new app version will be downloaded by the device.

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

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

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



Triggering the Mass Update

- 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 web interface. The top navigation bar includes 'UMS 12', 'Devices', 'Configuration', 'Apps' (which is selected), and '3 more'. Below the navigation is a sidebar with categories like 'All', 'Browser', 'Cloud', 'VDI', etc. The main content area shows a 'Browser' folder with one item, 'Chromium Browser'. To the right of the item is a 'Chromium Browser' card with a 'Set Default Version' button highlighted by a red box.

- Select the required version.

The screenshot shows the 'Set Default Version' dialog box overlying the main UMS interface. The dialog has a 'Version' dropdown menu with several options: '111.0.5563.64 BUILD 1 RC 1' (selected and highlighted by a red box), '108.0.5359.94 BUILD 3', '108.0.5359.94 BUILD 1 RC 1', and '111.0.5563.64 BUILD 1 RC 1' (repeated at the bottom).

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

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

The new version will be downloaded by the devices.

By default, apps / app versions assigned to the device will be automatically activated at the next reboot. By default, the reboot is performed automatically after the timeout of 60 seconds after the app download if the user does not postpone the device restart, see [IGEL OS Notification Center](#)(see [page 213](#)).

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



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



Installing the Base System via IGEL OS Creator (OSC)

Installation Requirements and Devices Supported by IGEL OS 12

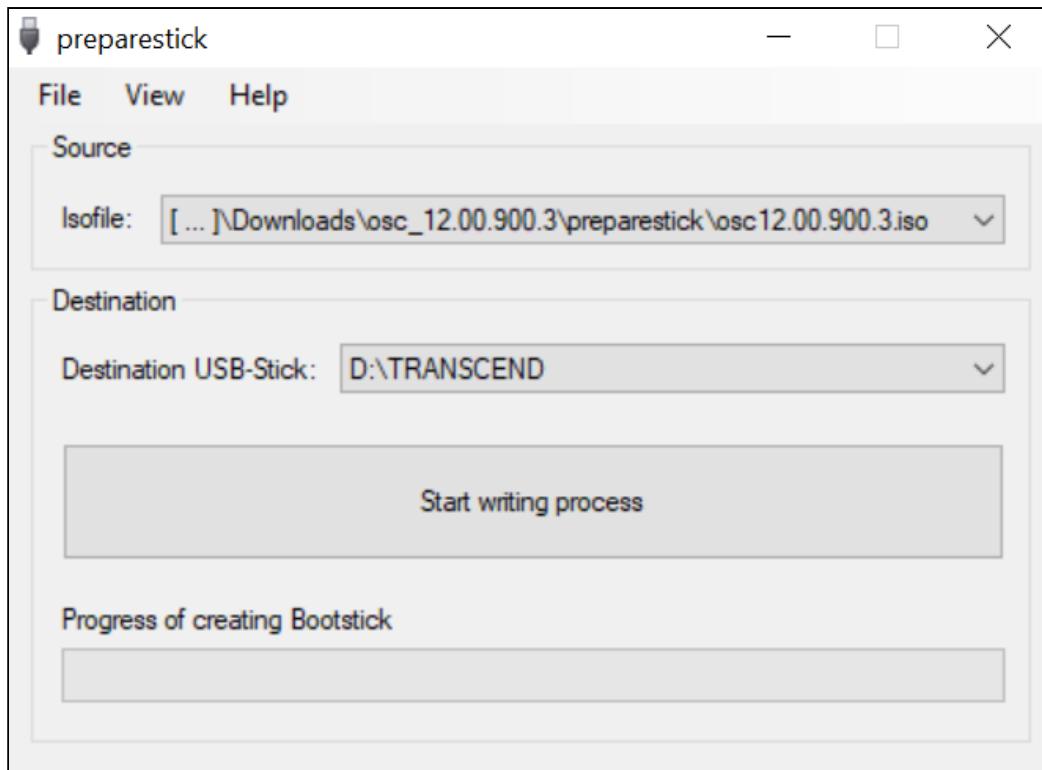
For the requirements for IGEL OS 12 and the list of the officially supported devices, see <https://kb.igel.com/os12-supported-hardware>.

Create USB Installation Medium

Windows

1. Download the ZIP archive for OS Creator from the [IGEL Download Server¹⁹](#):
 - For new devices, use the standard installer (e.g. `osc_12.01.110.zip`).
 - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e.g. `osc_12.01.110_legacy.zip`).
2. Unzip the contents into a local directory.
3. Connect a USB memory stick with at least 4 GB capacity to the computer.
All existing data on the USB memory stick will be destroyed.
4. Double-click the `preparestick.exe` file from the unzipped directory.
If you are in the "administrators" group, the program will start after you have confirmed a dialog. If you are not in the "administrators" group, you must enter the administrator password to start the program.

¹⁹ <https://www.igel.com/software-downloads/cosmos/>



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

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



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

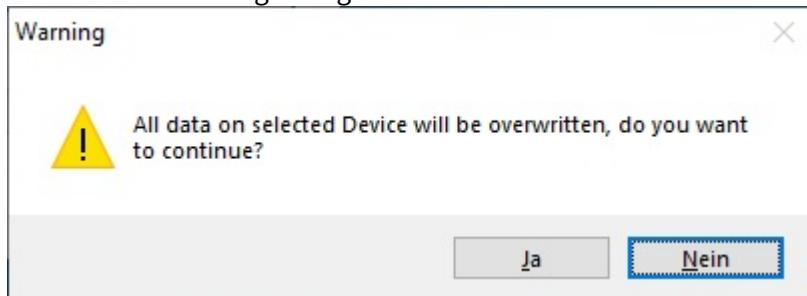
It is recommended that you only have one USB storage medium connected during this procedure. If you accidentally select the wrong medium, all data on it will be lost.

Generally speaking, the list of available USB storage media is refreshed automatically. If, however, you would like to refresh it manually, click on **View > Refresh USB Device List**.

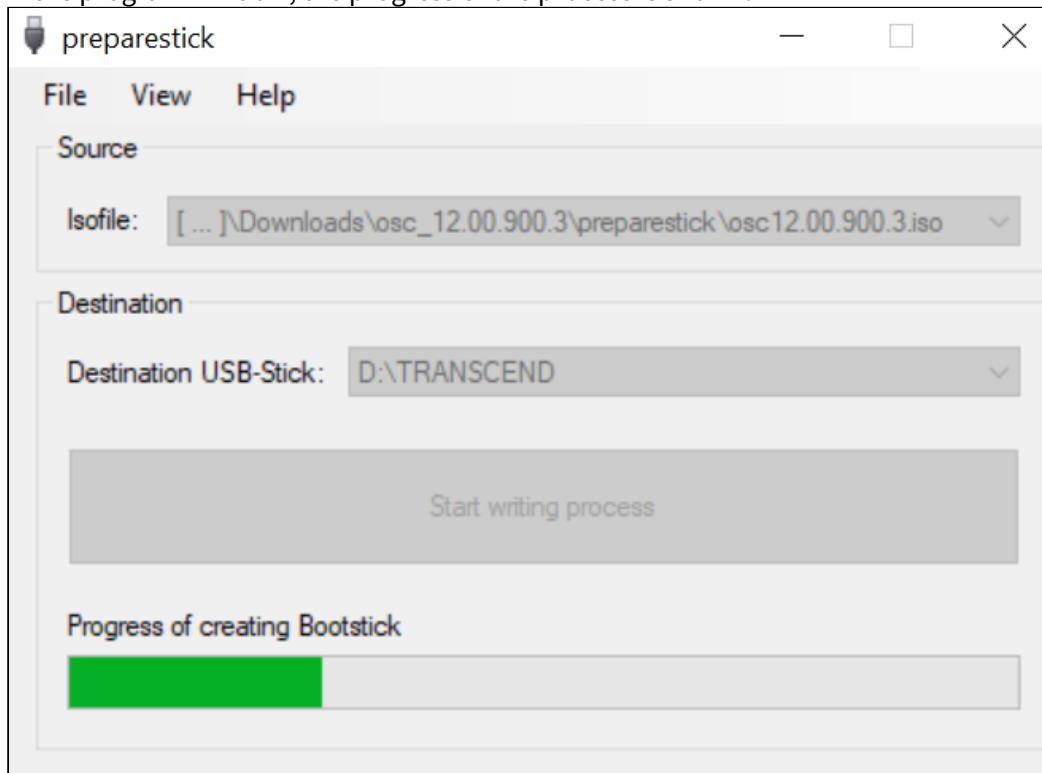
7. Click **Start writing process**.



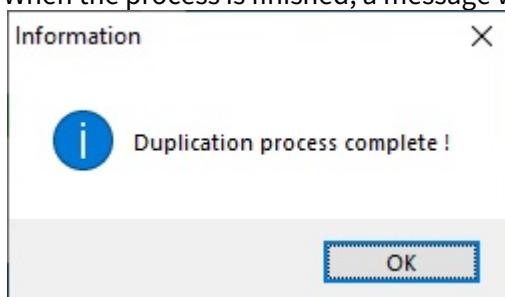
8. Confirm the following dialog:



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



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





9. Close the message window and the program.
10. After about 3 seconds, remove the USB memory stick.

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

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

Linux

1. Download the ZIP archive for OS Creator from the [IGEL Download Server](#)²⁰:
 - For new devices, use the standard installer (e.g. `osc_12.01.110.zip`).
 - For older devices or if you haven't been able to boot the installer at all, use the legacy installer (e.g. `osc_12.01.110_legacy.zip`).
2. Unzip the contents into a local directory.
3. From this directory, you will need the ISO file (e.g. `osc12.01.110.iso` or `osc12.01.110_legacy.iso`) to create a bootable medium.
4. Connect a USB memory stick with at least 4 GB capacity to the computer.

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

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

Example output:

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

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

²⁰ <https://www.igel.com/software-downloads/cosmos/>



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

6. The following command writes the installation data to the USB memory stick:

```
dd if=osc12.01.110.iso of=/dev/sdX bs=1M oflag=direct
```

Replace `sdX` with the device name of the USB memory stick that you have determined.

When the `dd` command has terminated, you can see the terminal emulator input prompt again.

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

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

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

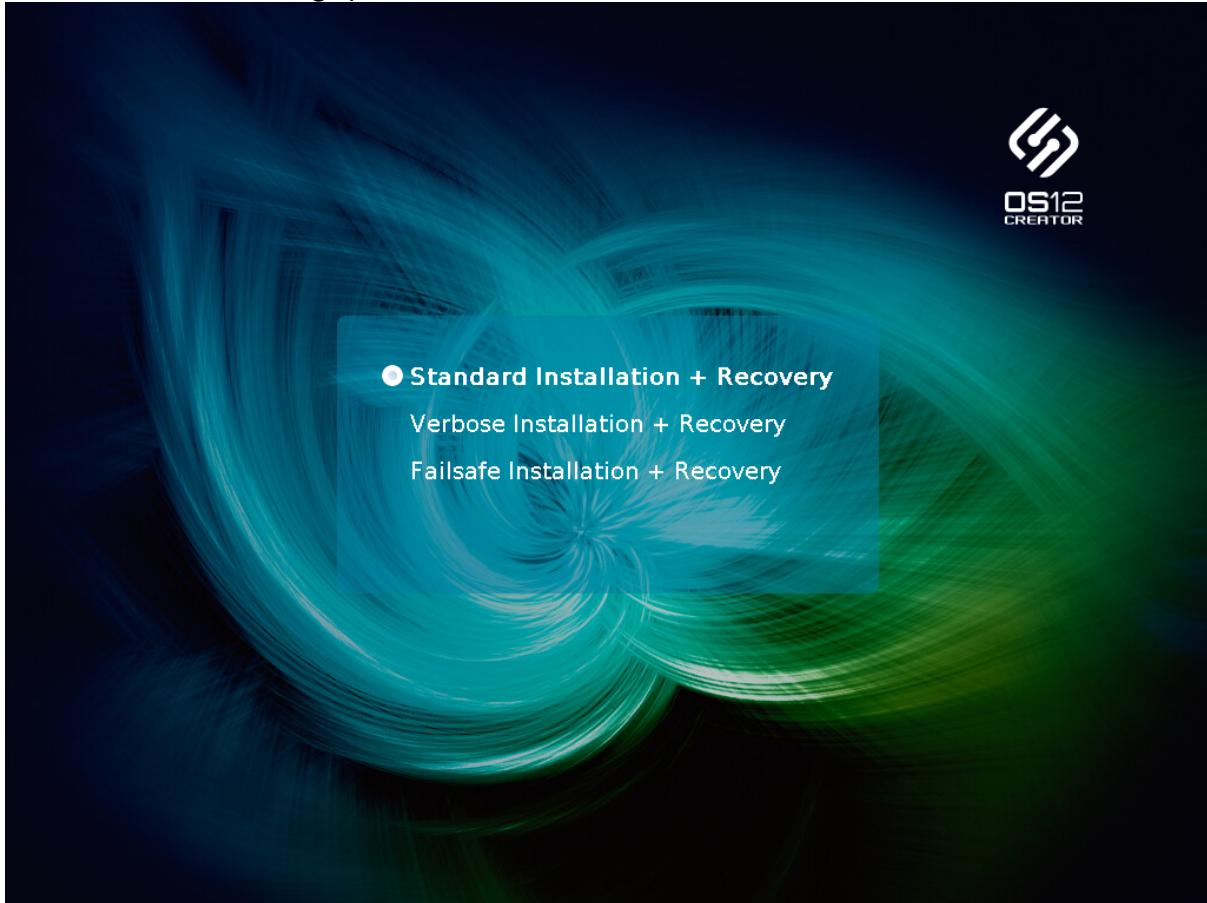
Installation Procedure

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

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



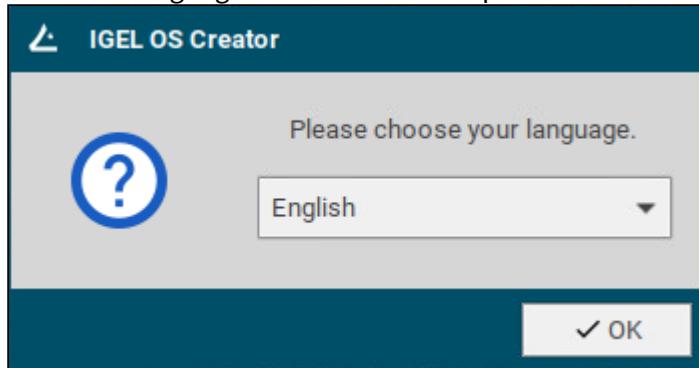
2. Select one of the following options from the boot menu:



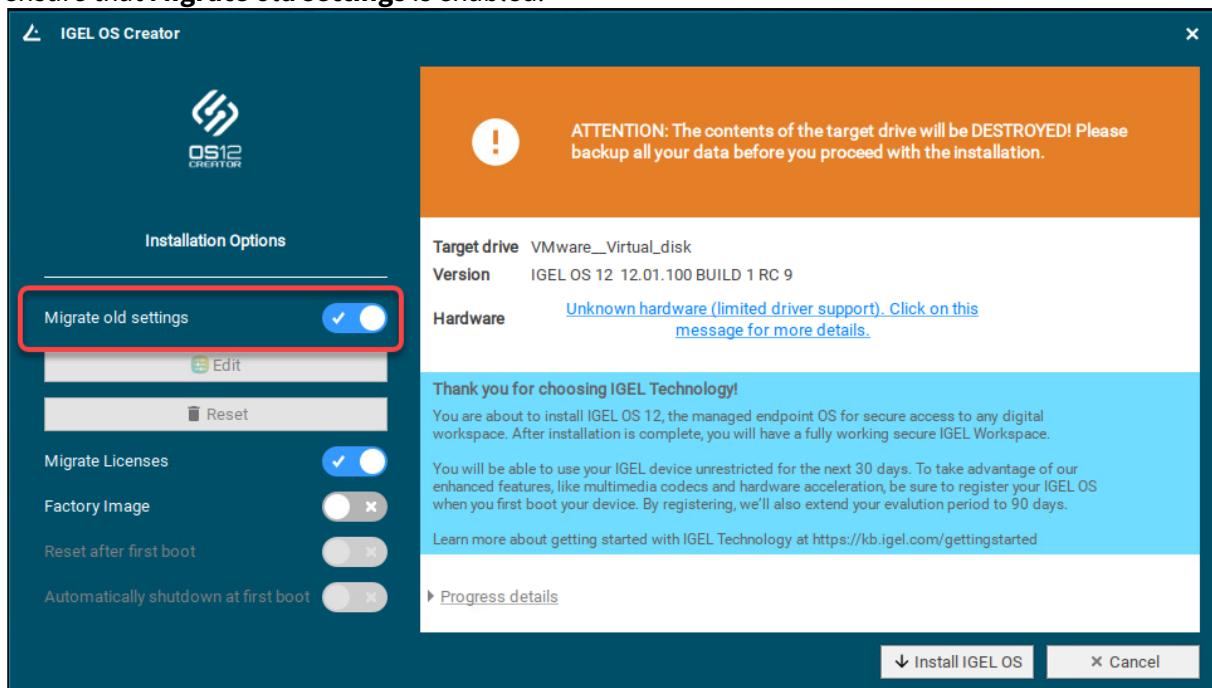
- **Standard Installation + Recovery:** Boots the system with just a few messages from the USB memory stick and launches the installation program. (Default)
- **Verbose Installation + Recovery:** Boots the system from the USB memory stick and shows the Linux boot messages in the process.
- **Failsafe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



3. Select the language for the installation process.



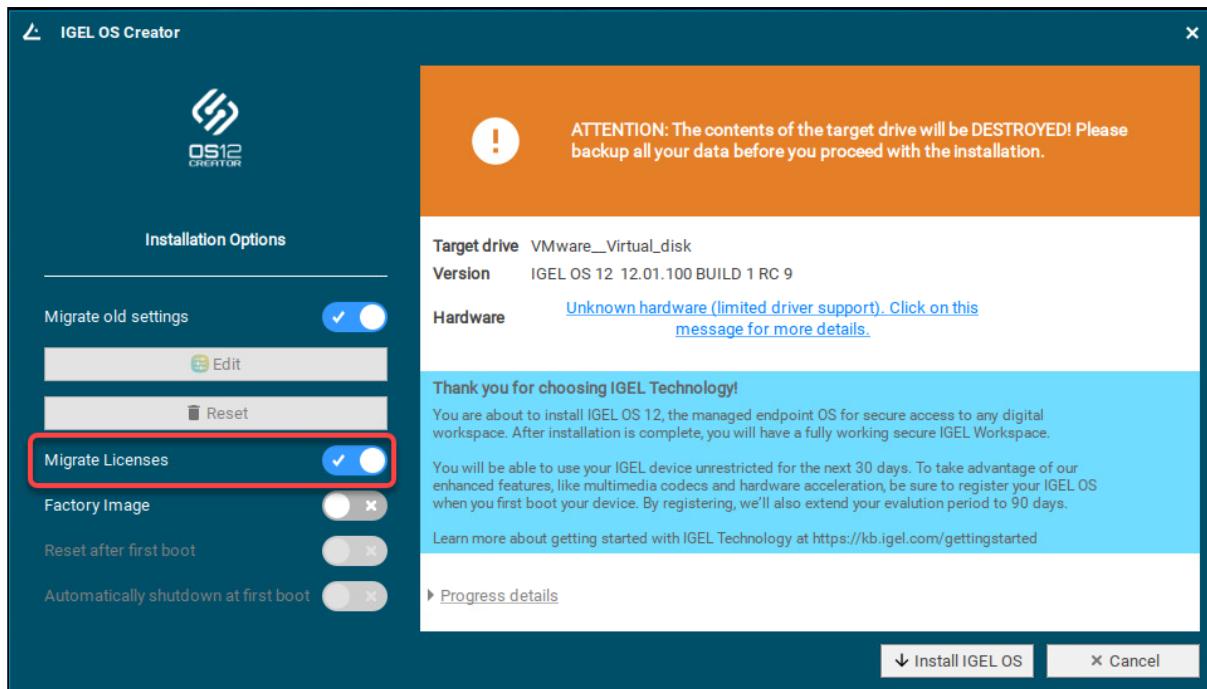
4. If IGEL OS 12 has been running on the device before and you want to preserve the device's settings, ensure that **Migrate old settings** is enabled.



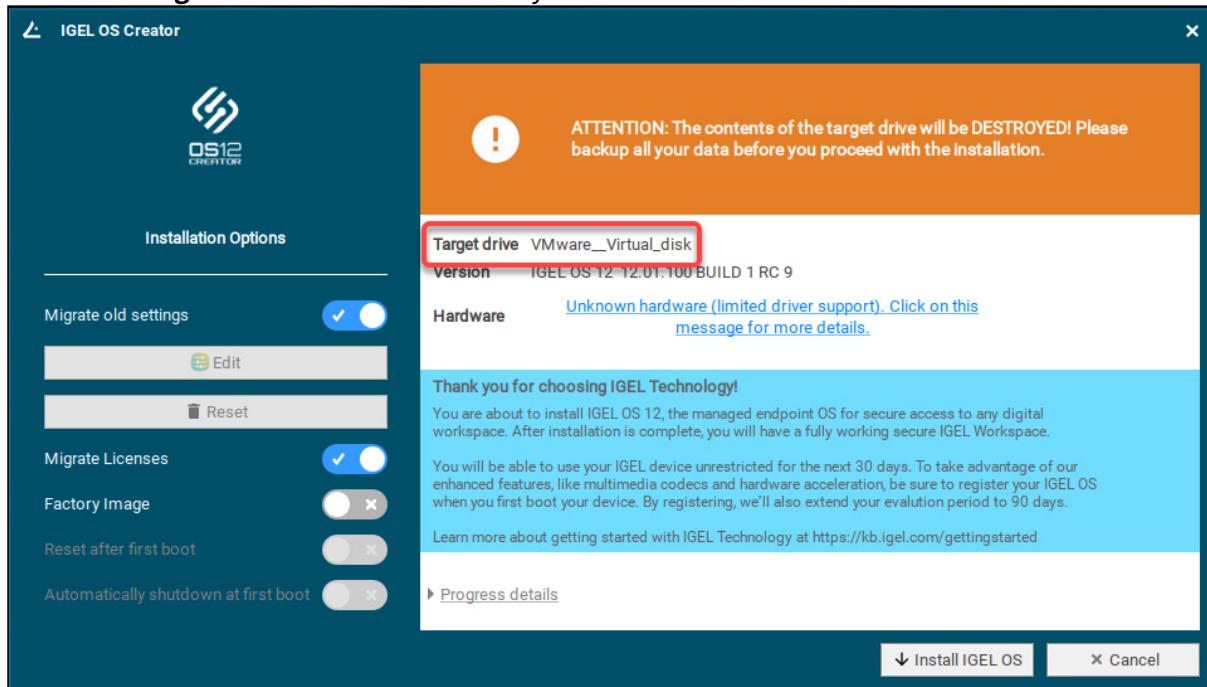
5. If one of the following is the case, make sure that **Migrate licenses** is enabled:

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

Installing the Base System via IGEL OS Creator (OSC)

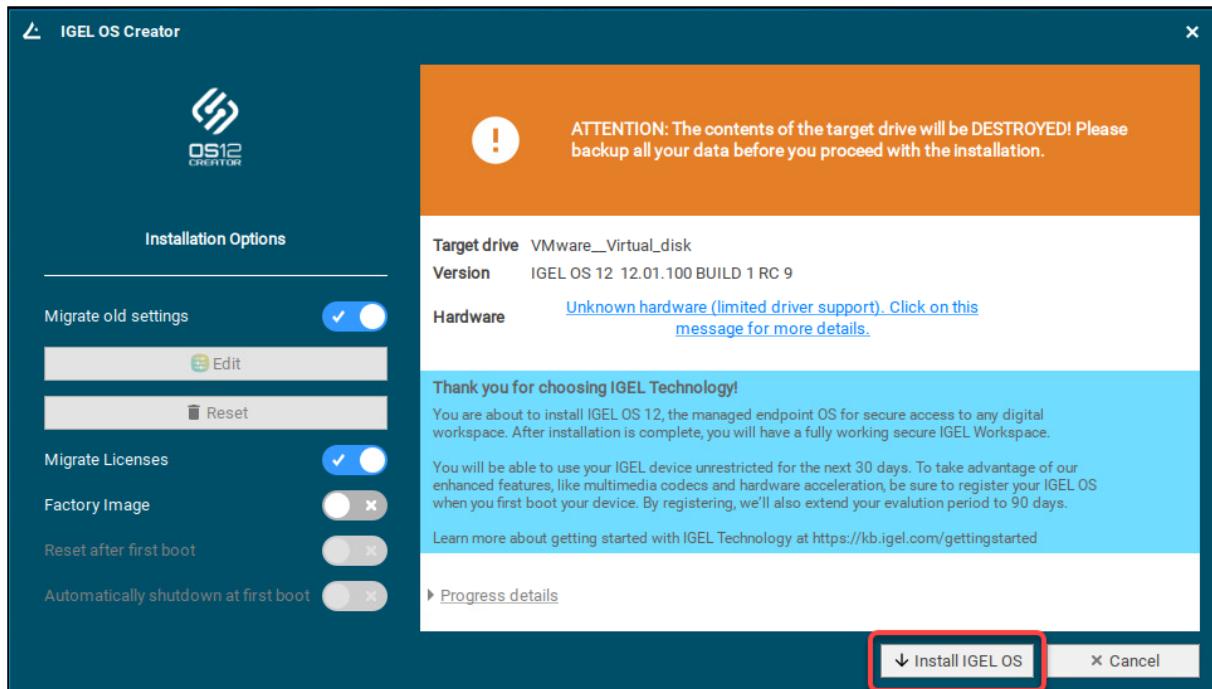


6. Check the **Target drive** to ensure that the system is installed on the desired drive.



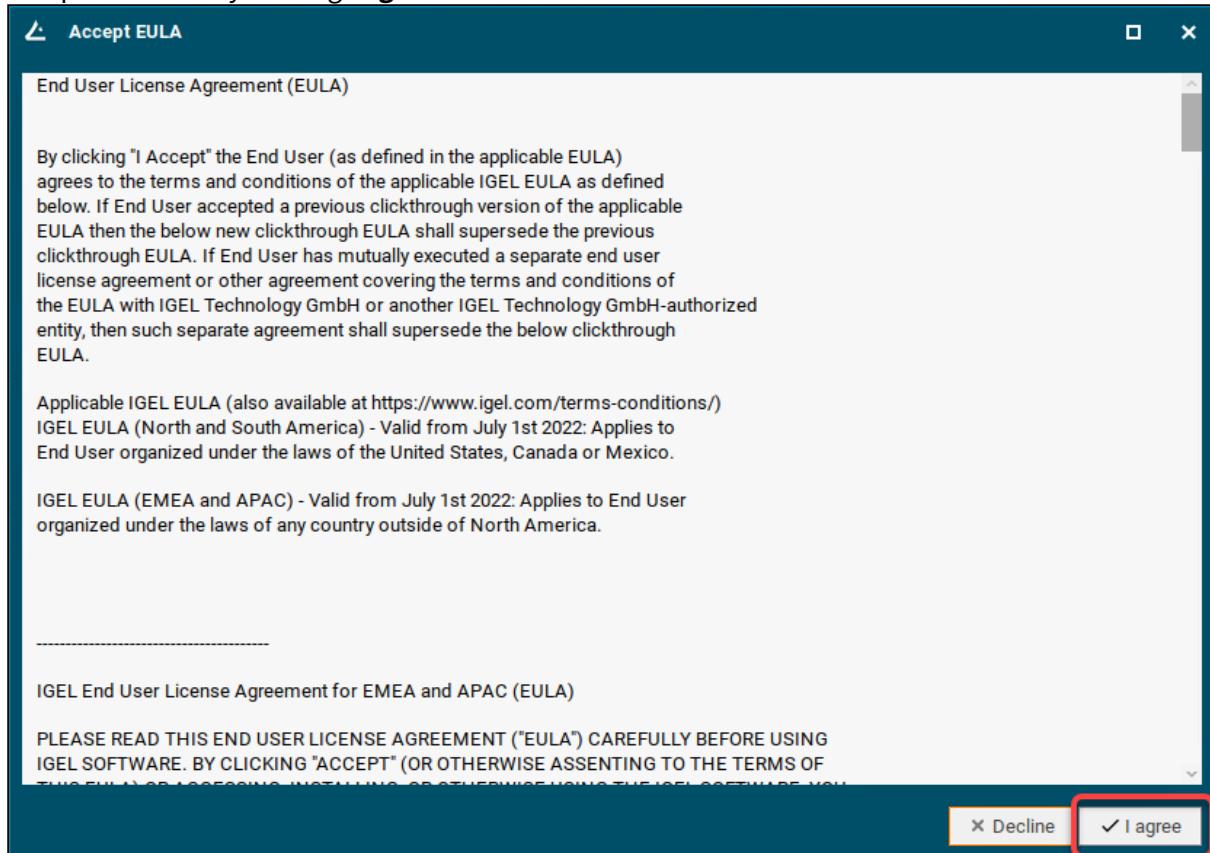


7. Click **Install IGEL OS**.



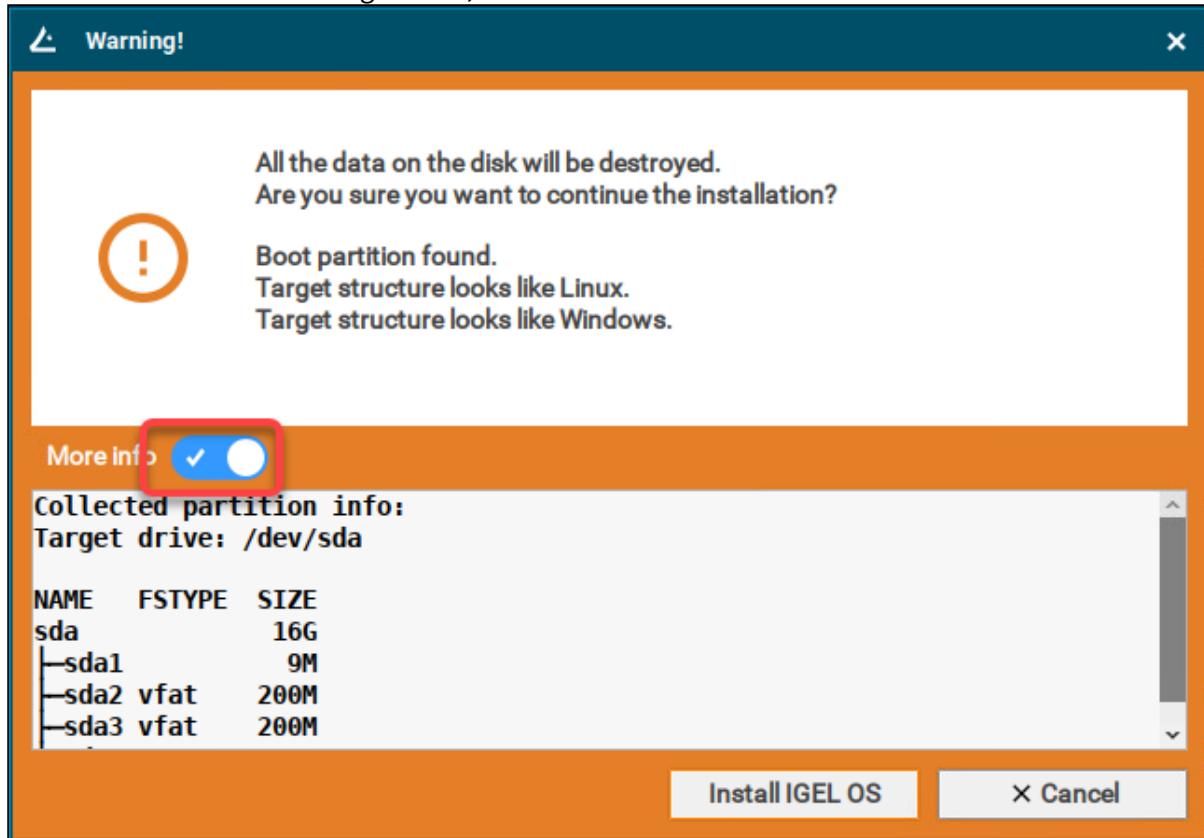


8. Accept the **EULA** by clicking **I agree**.



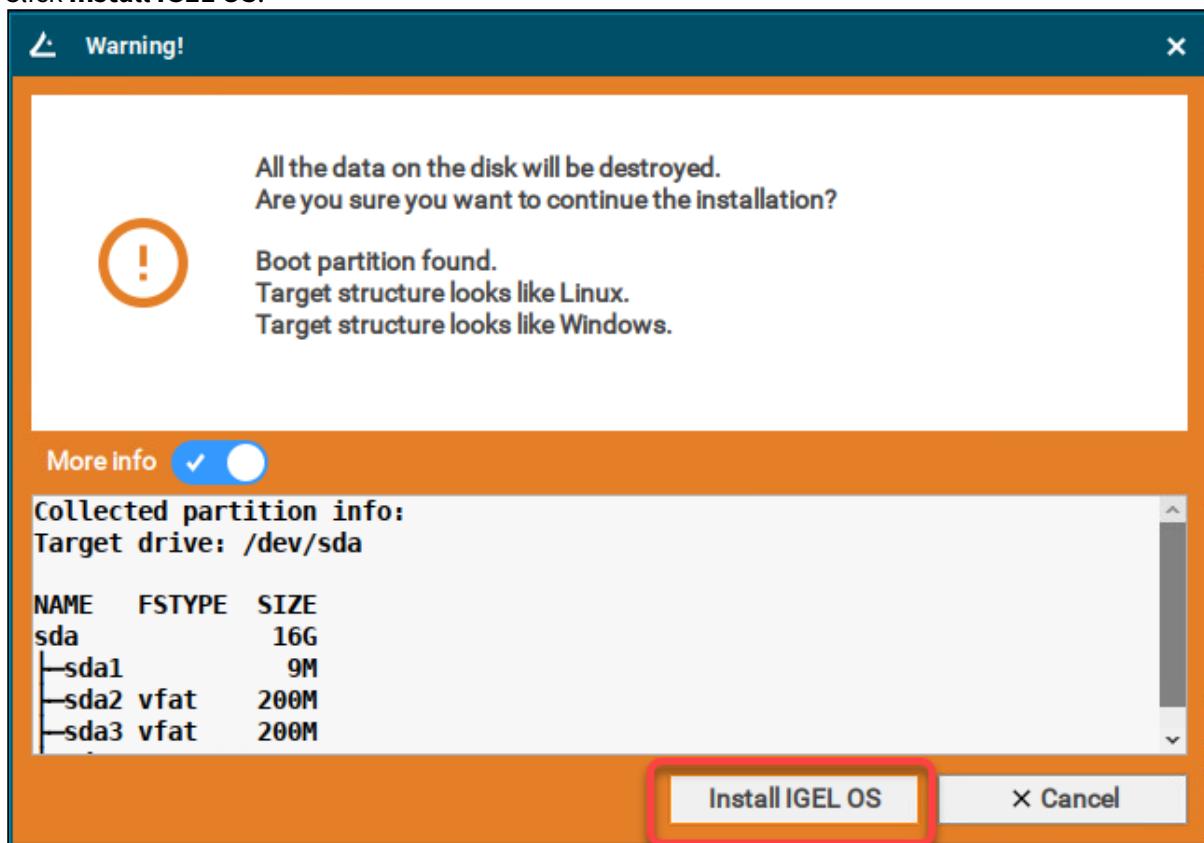


9. To view the details for the target drive, click **More Info**.



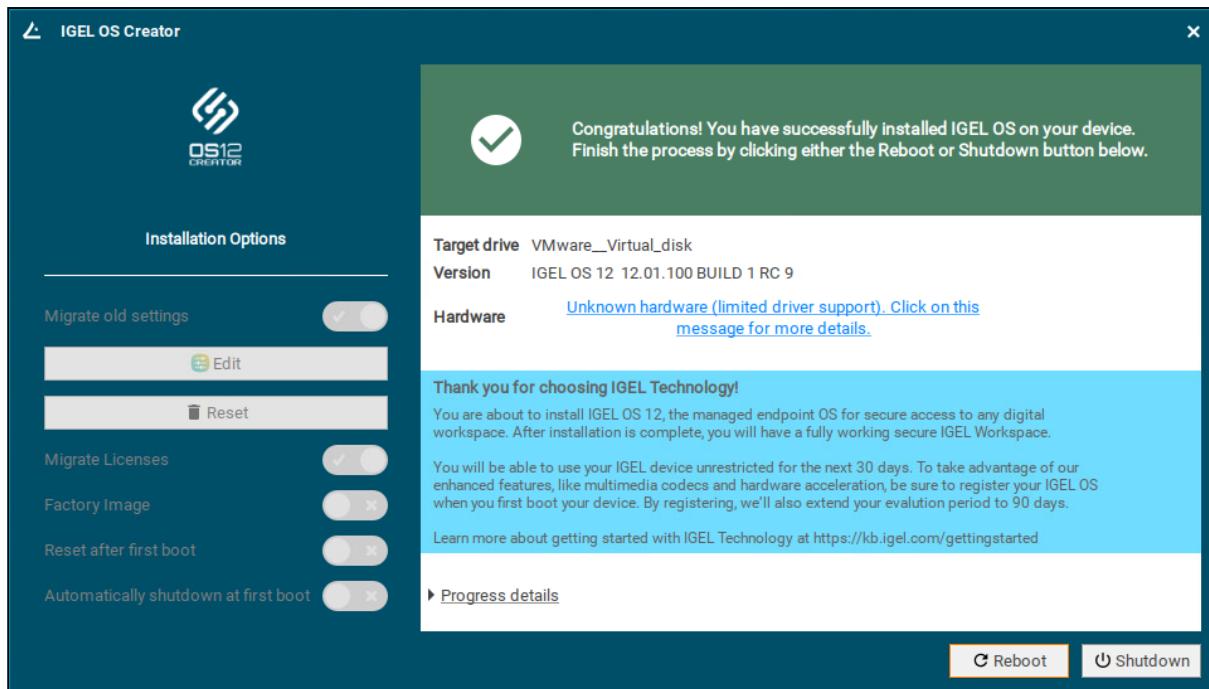


10. Click **Install IGEL OS**.

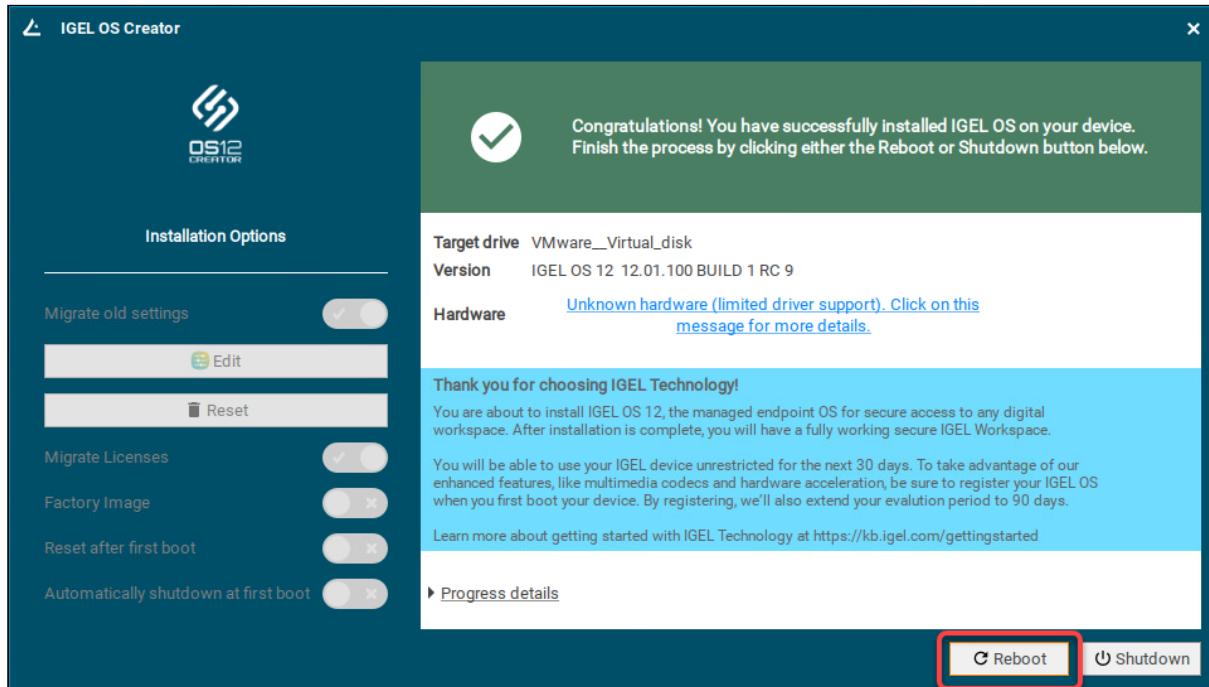


The installation program will install IGEL OS 12 on the target drive. If you see the success message, the installation is complete.

Installing the Base System via IGEL OS Creator (OSC)



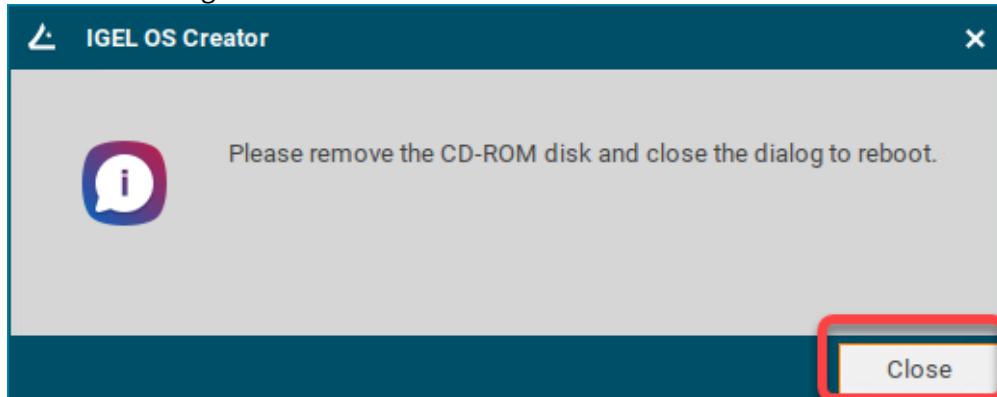
11. Click Reboot.



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 158).



Licensing

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

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

⚠ EULA Must Be Accepted

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

Starter License, Demo Licenses, and Limitations on Expiry

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

Endpoint Device / Apps

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

*Only if the device is managed by the UMS

Remote Management (UMS)

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



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

Onboarding Service (OBS)

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

Getting Your Licenses Ready for Deployment

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

²¹ <https://activation.igel.com/>



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

The image consists of two screenshots. The top screenshot shows a navigation sidebar with the following items: Home, Orders, UMS ID (which is highlighted with a red box), Search hardware, Multi-licensed hardware, Subscription Keys, Product Packs, Archived packs, and IGEL Knowledge Base. The bottom screenshot shows a circular interface with several icons: a pencil inside a circle, a trash can, a star, a file, a cube labeled '1', a plus sign inside a circle (which is highlighted with a red box), and a minus sign. The text 'td-ums12' is visible near the bottom left of the circular area.



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 checked="" type="checkbox"/>	WE-E	WE		0/10	EULA NOT ACCEPTED

The search bar at the top contains "we-e" and the selected row ("WE-E", "WE") is highlighted with a red box.

- 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.

A sidebar menu with the following items:

- Profile icon: [REDACTED]@igel.com ▾
- Home
- Orders
- UMS ID
- Search hardware
- Multi-licensed hardware
- Subscription Keys
- Product Packs** (This item is highlighted with a red box)
- Archived packs



Product Packs

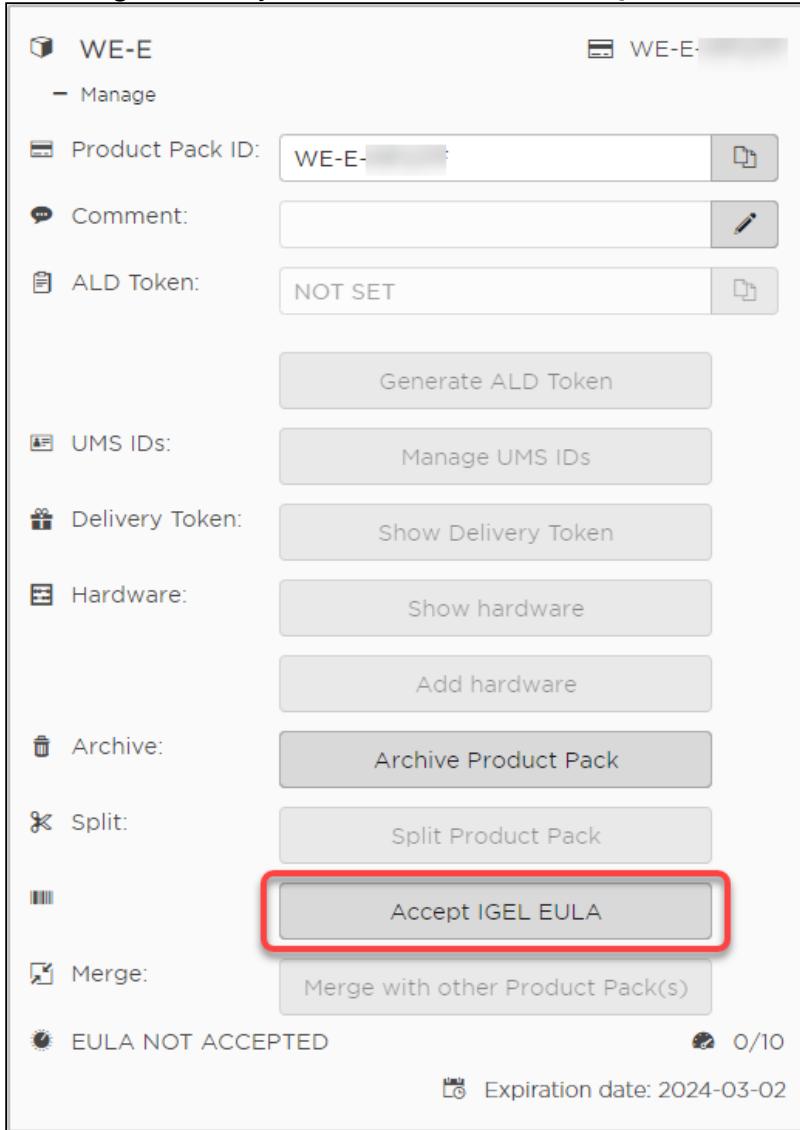
All WE-E Product Packs registered to IGEL Technology

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
+	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 navigation bar with 'WE-E-' and a 'Manage' link. Below it are fields for 'Product Pack ID' (WE-E-), 'Comment' (empty), and 'ALD Token' (NOT SET). There are three buttons: 'Generate ALD Token', 'Manage UMS IDs', and 'Show Delivery Token'. Under 'Hardware', there are 'Show hardware' and 'Add hardware' buttons. In the 'Archive' section, there's a 'Archive Product Pack' button. The 'Split' section has a 'Split Product Pack' button. The 'Merge' section has a 'Merge with other Product Pack(s)' button. At the bottom left, it says 'EULA NOT ACCEPTED'. On the right, there's a progress bar showing '0/10' and an expiration date of '2024-03-02'. The 'Accept IGEL EULA' button is highlighted with a red box.



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

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

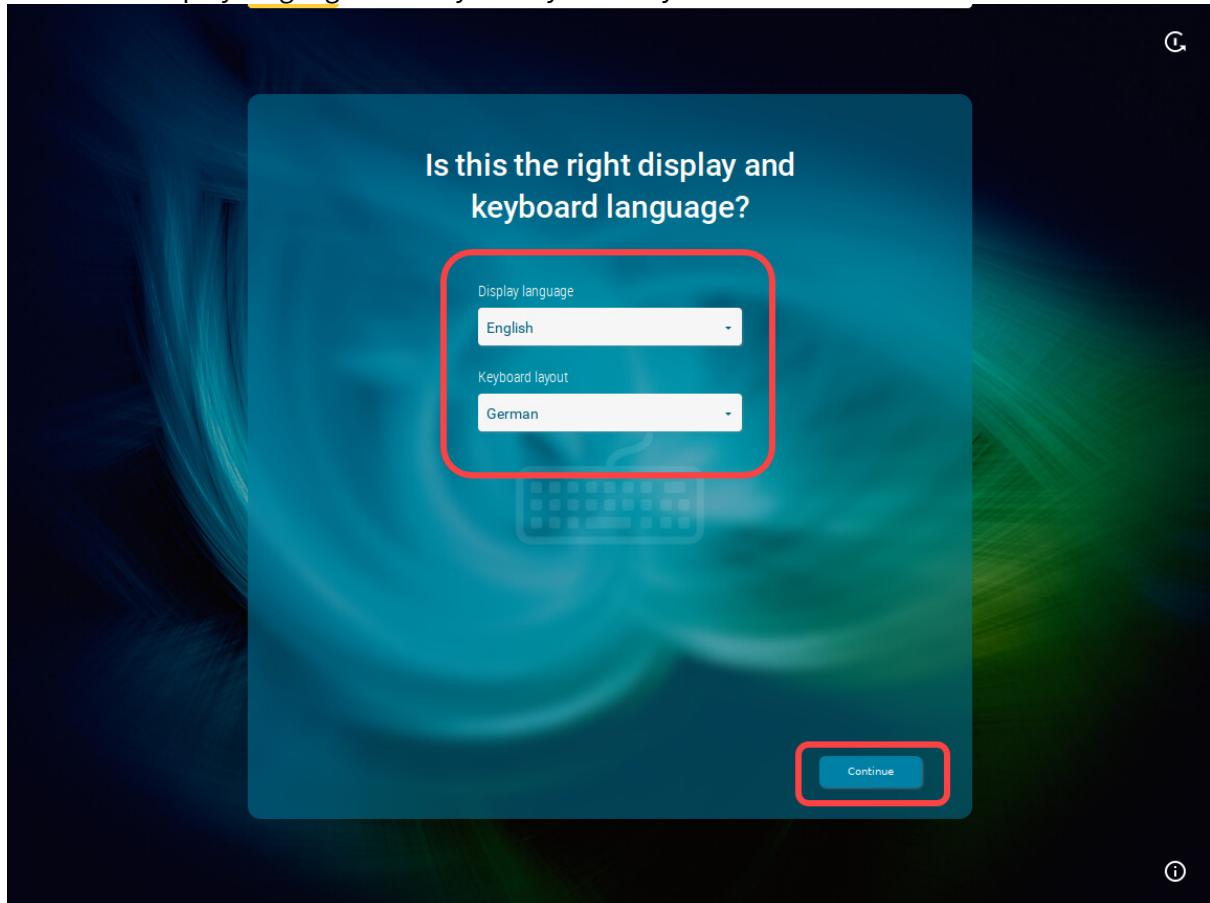
- ⓘ If you decide for some reason not to use the IGEL Onboarding Service or the one-time password method, you can skip the corresponding steps in the Setup Assistant. Your IGEL OS 12 device will start with a [Starter license](#)(see page 151).
To register this device with the UMS Server, you can use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

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

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

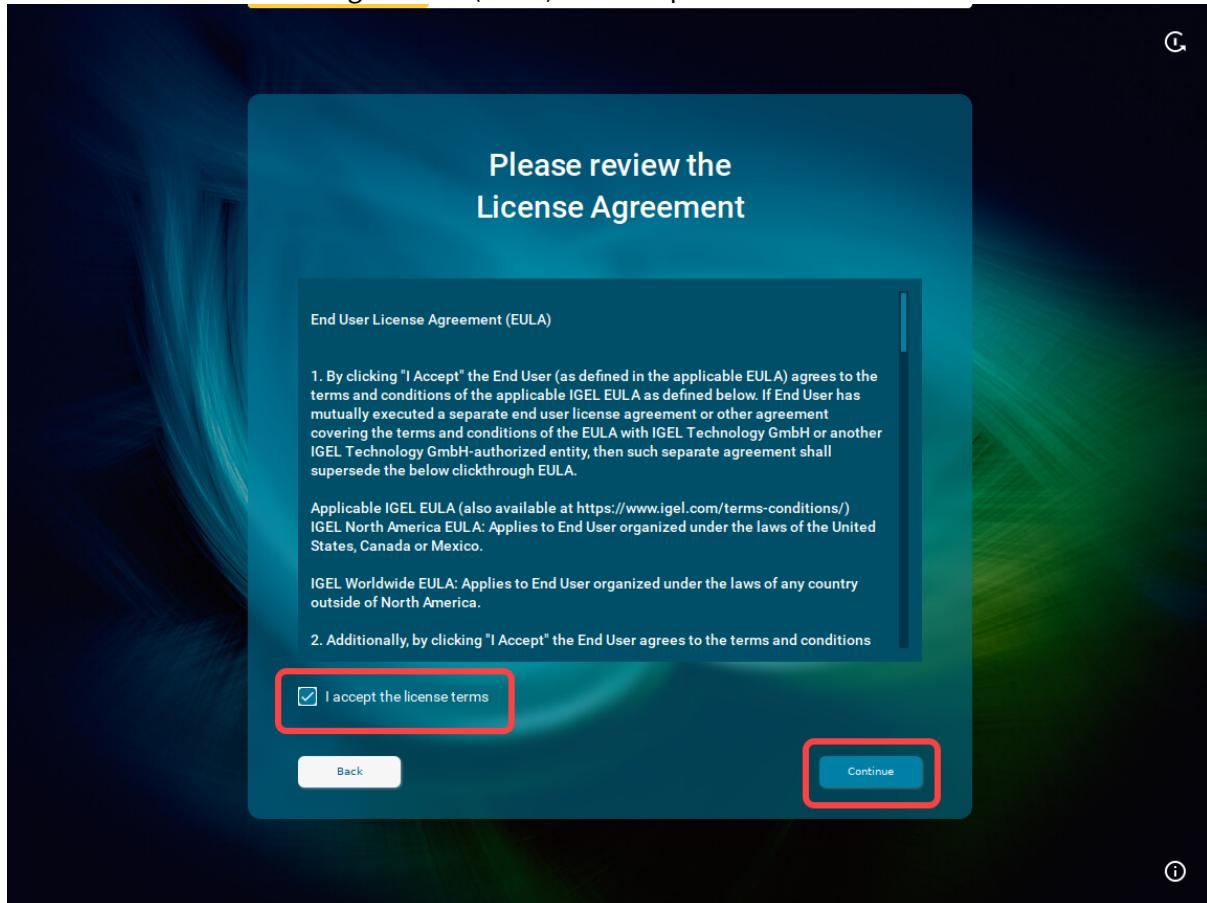


2. Choose the display language and set your keyboard layout. Click **Continue**.

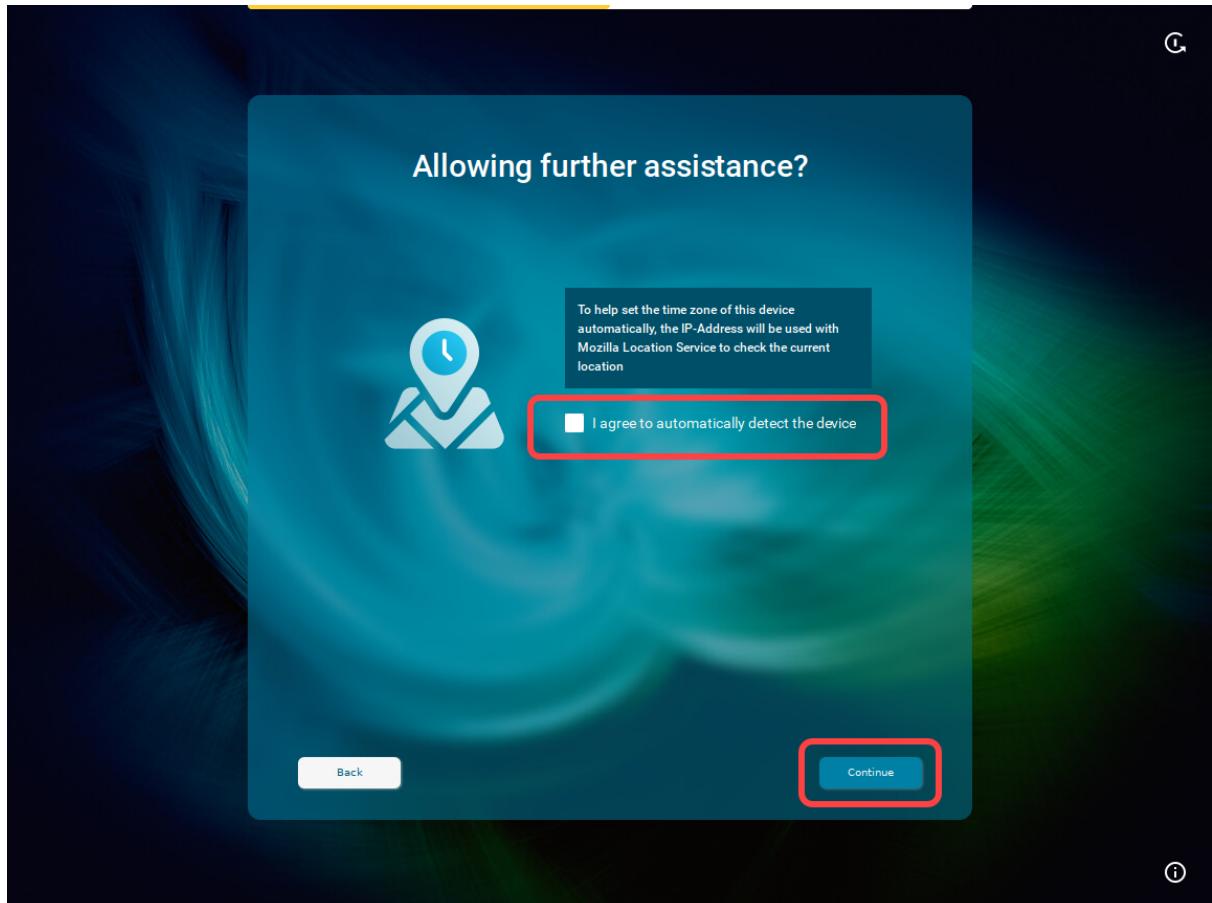




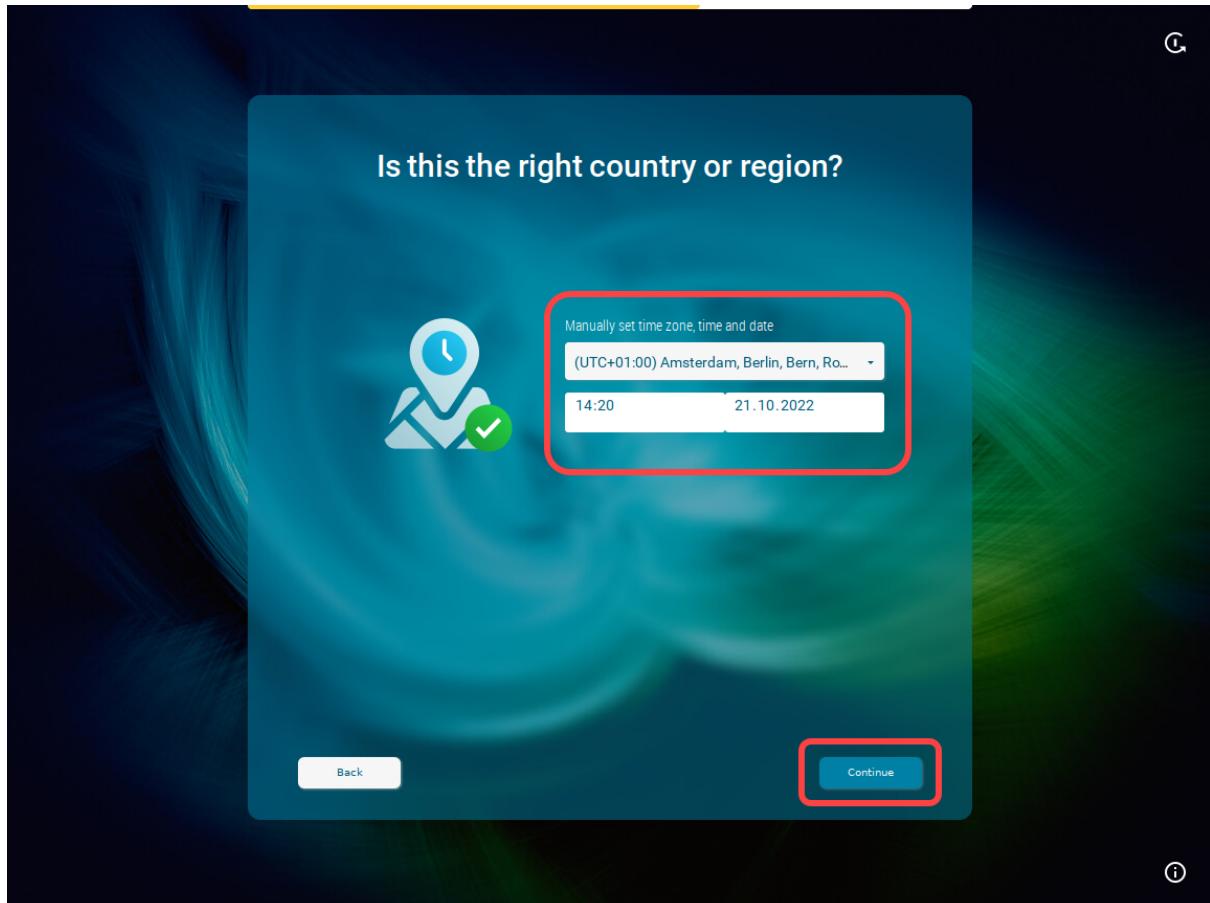
3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.



4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under [Troubleshooting: Configuring a Network during the Onboarding](#)(see page 174).
5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.

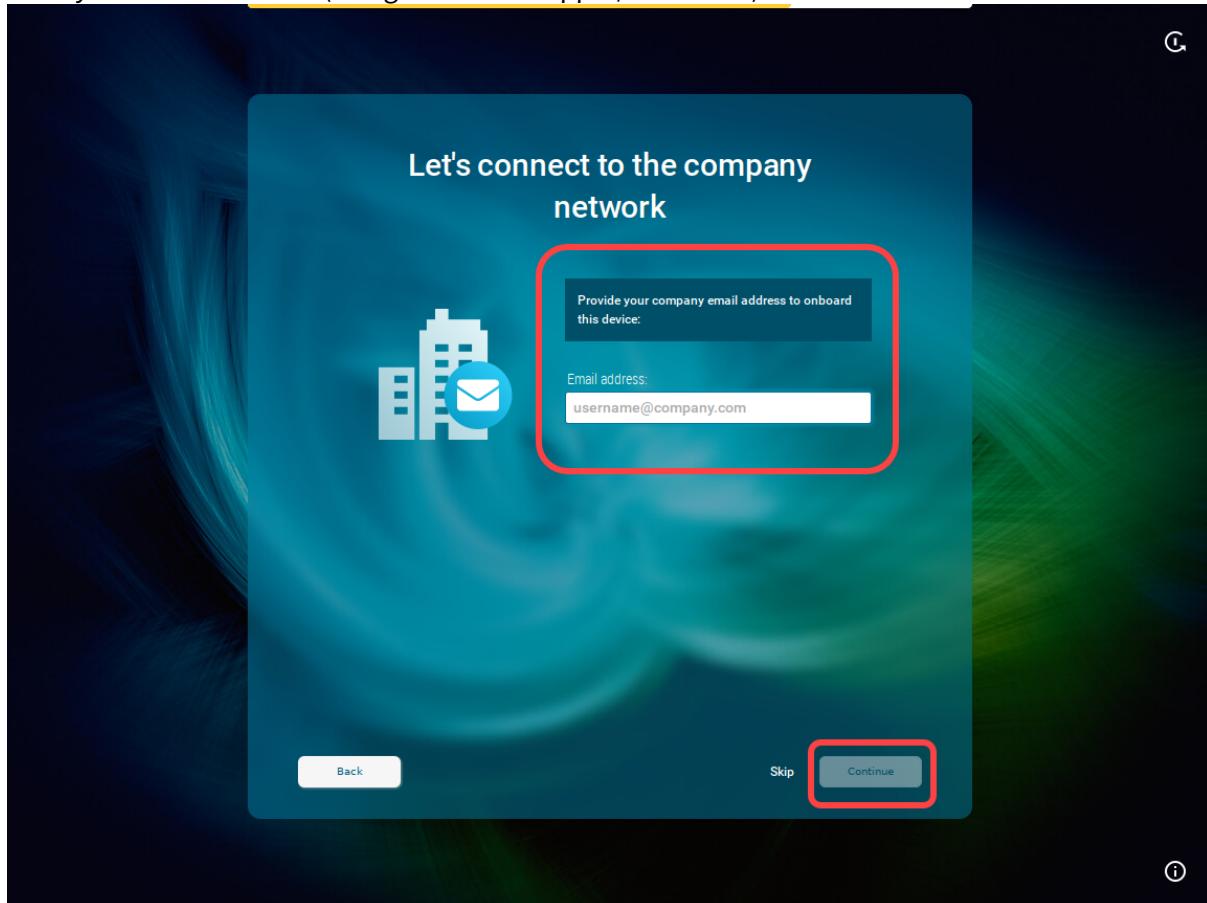


Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.





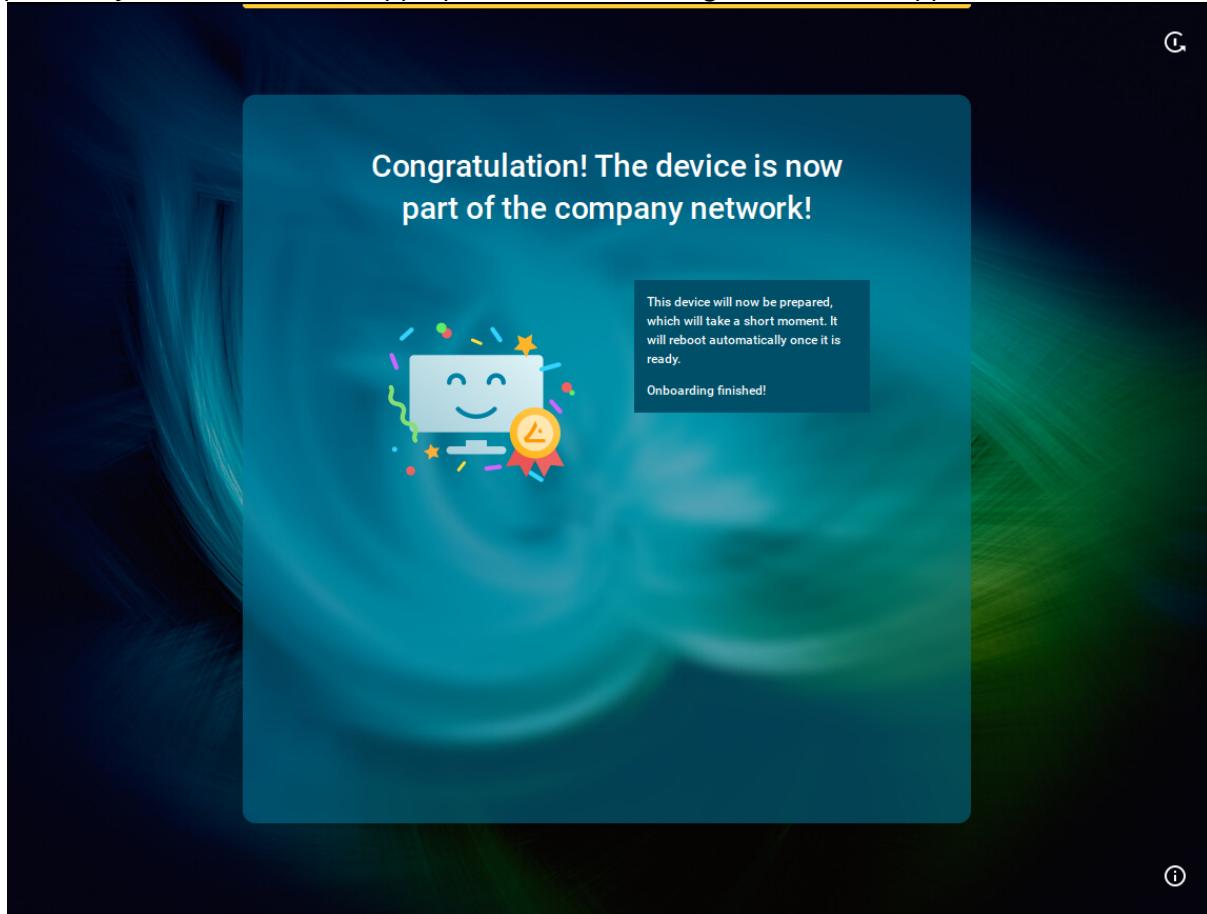
6. Enter your e-mail address (using the correct upper/lowercase) and click **Continue**.



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**.

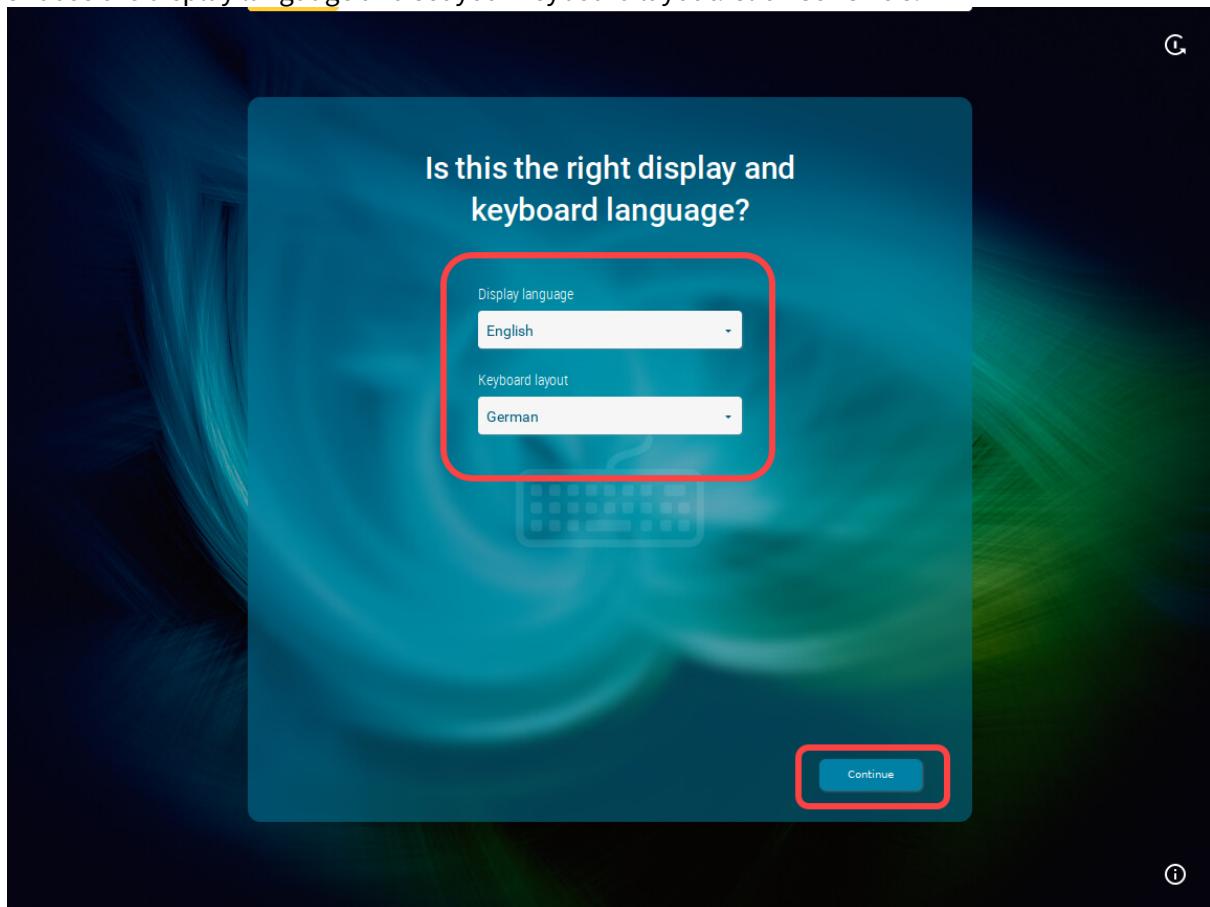
A screenshot of the UMS Web App interface. The top navigation bar includes tabs for "Devices", "Configuration", "Apps", and "Search". The main area shows a "Devices" list with one item named "renata". On the right, there's a detailed view for "ITC00E0C51A75F4" with various buttons like "Edit Configuration", "Shadow", "Assign object", "Reboot", and "Shutdown". Under "Custom Properties", the "System Information" tab is selected, showing fields for "Version" (12.1.100-1.rc.10+1), "Directory Path" (Devices /), and "Onboarded by" (IGEL US base system). Red arrows point from the bottom of the question text to the "Onboarded by" field in the UMS interface. The bottom of the screenshot shows a "Assigned Objects" section with a "System Information" tab highlighted.



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

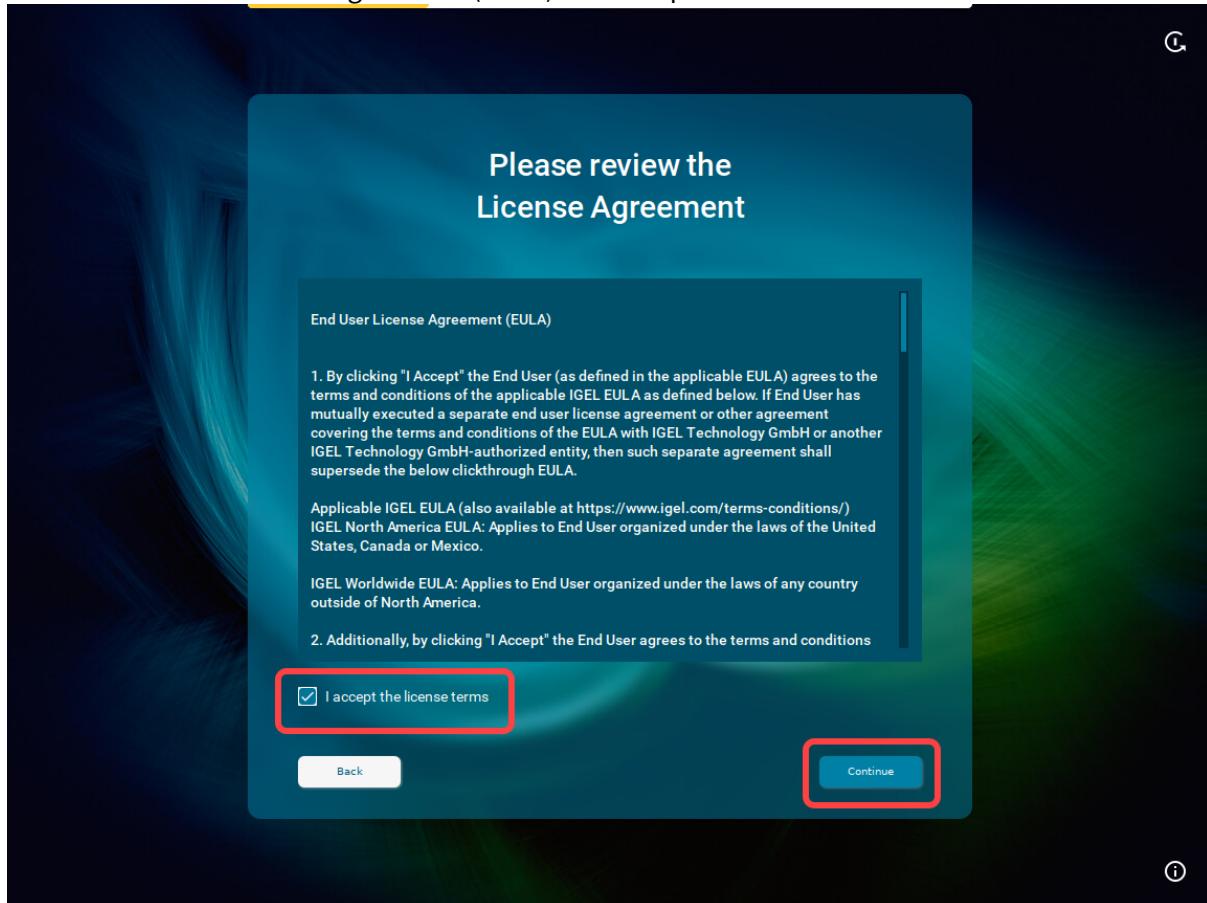
If you decided not to use IGEL Onboarding Service for the registration of your IGEL OS 12 devices, you can use a one-time password method as an alternative.

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

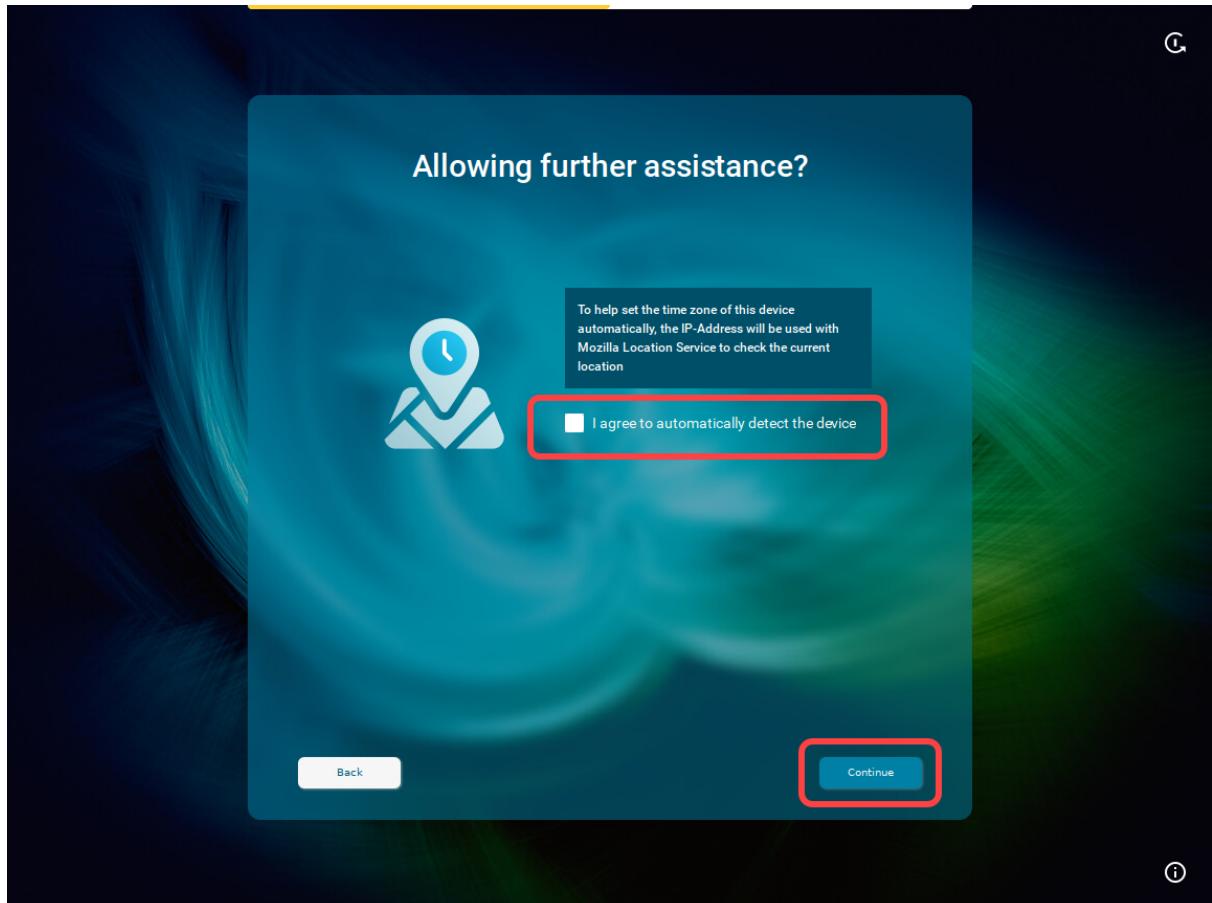




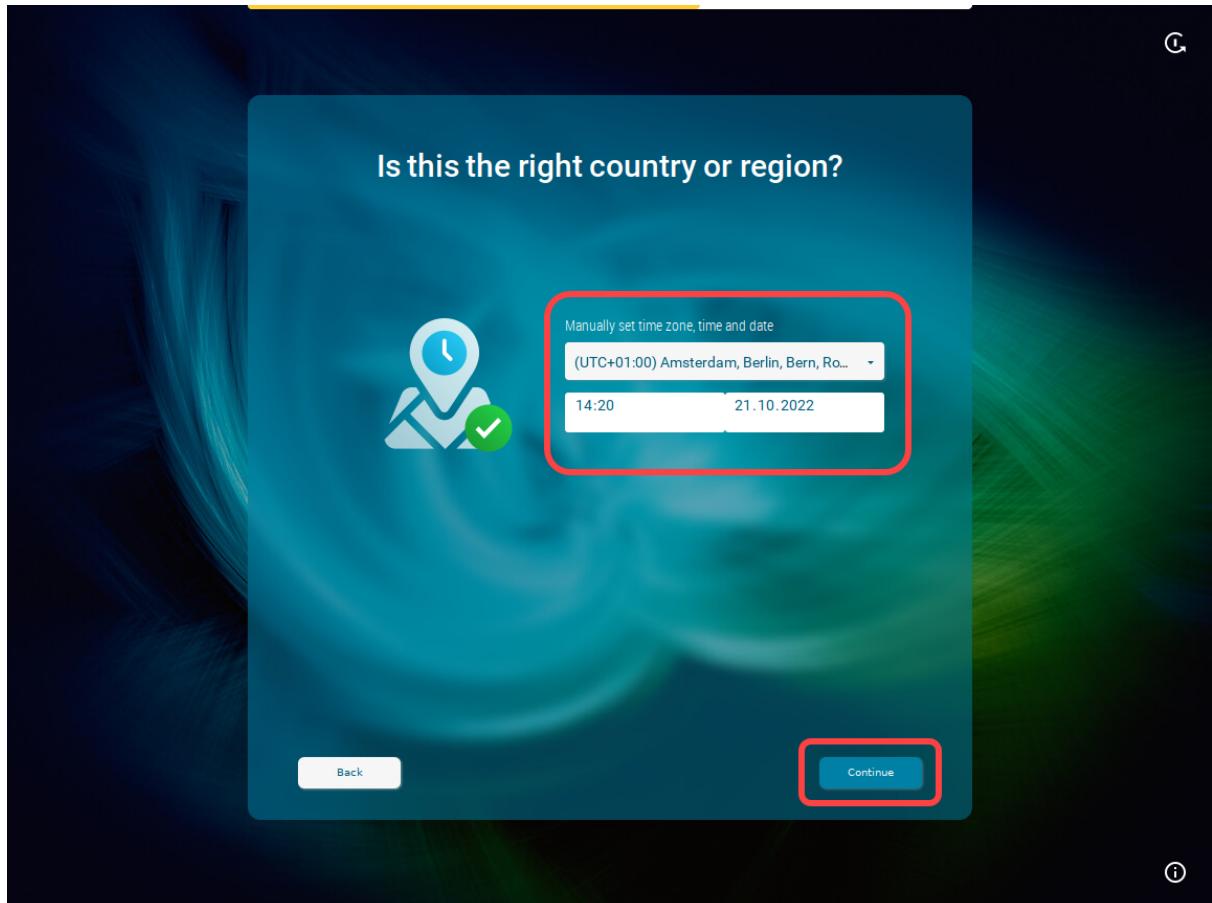
3. Read the End User License Agreement (EULA) and accept the license terms. Click **Continue**.



4. If you are not connected to a LAN, a network configuration screen is displayed. In this case, follow the instructions under [Troubleshooting: Configuring a Network during the Onboarding](#)(see page 174).
5. To automatically set the time zone, activate **I agree to automatically detect the device** and click **Continue**.

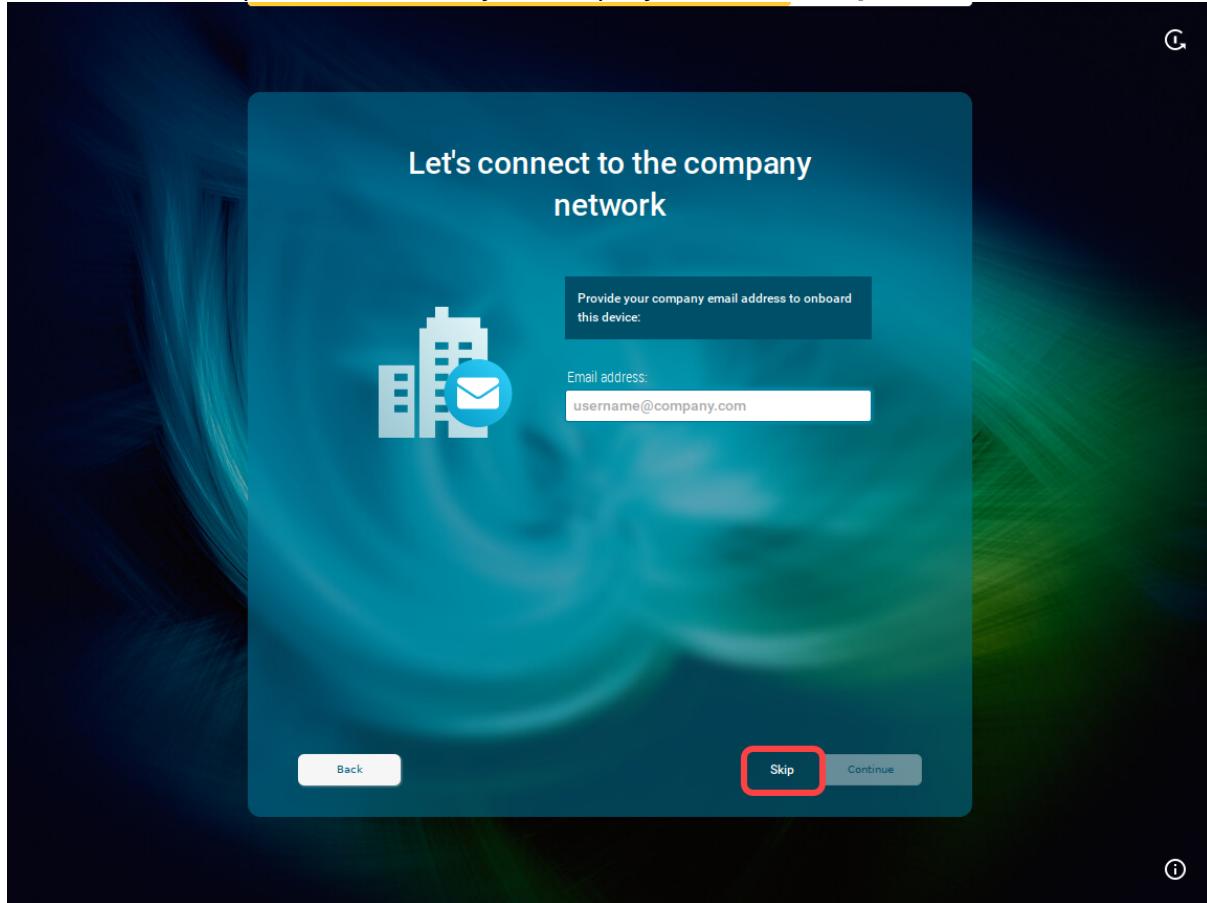


Or click **Continue** and set your time zone, time, and date manually, then click **Continue**.

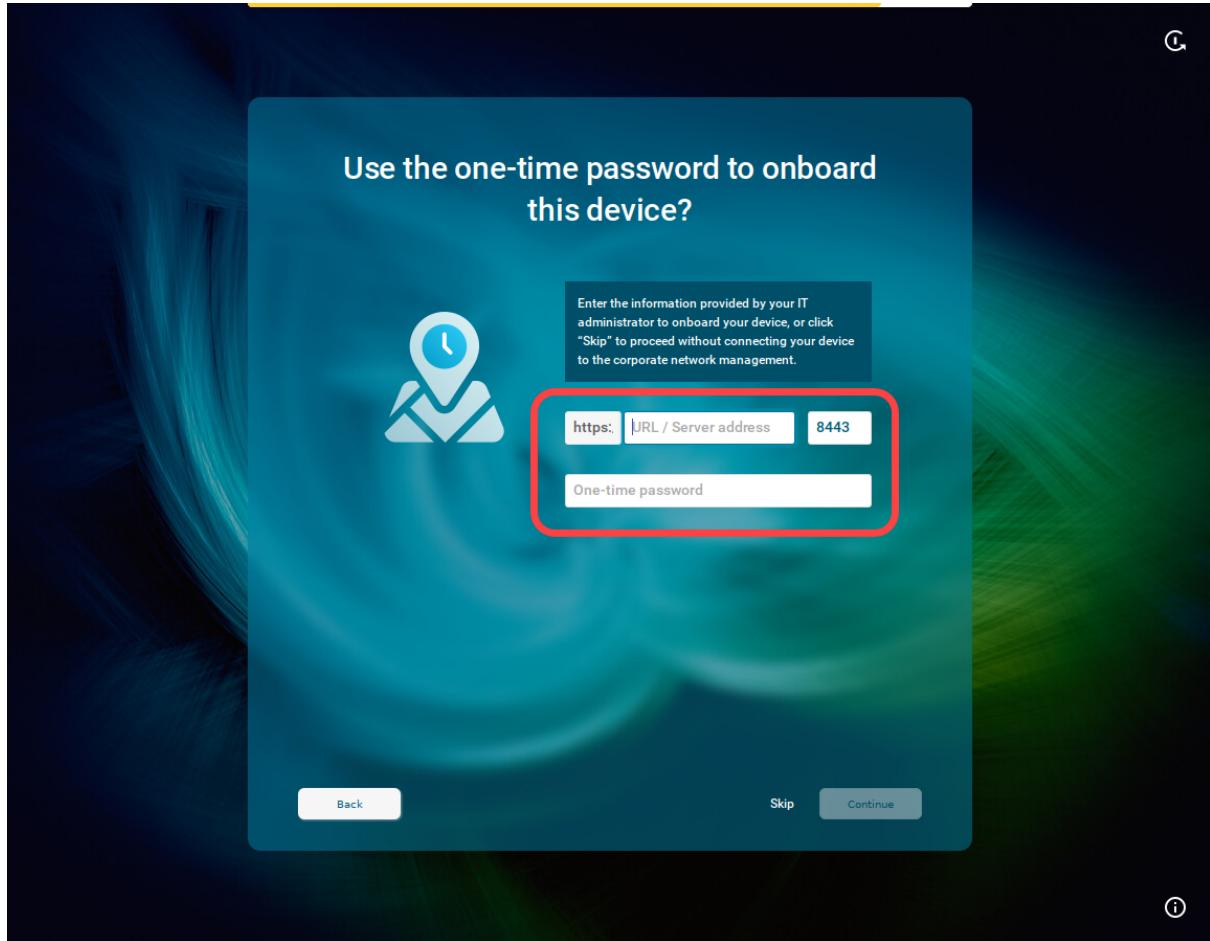




6. When the IGEL Setup Assistant asks for your company e-mail, click **Skip**.



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

You can create the following first-authentication keys:

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



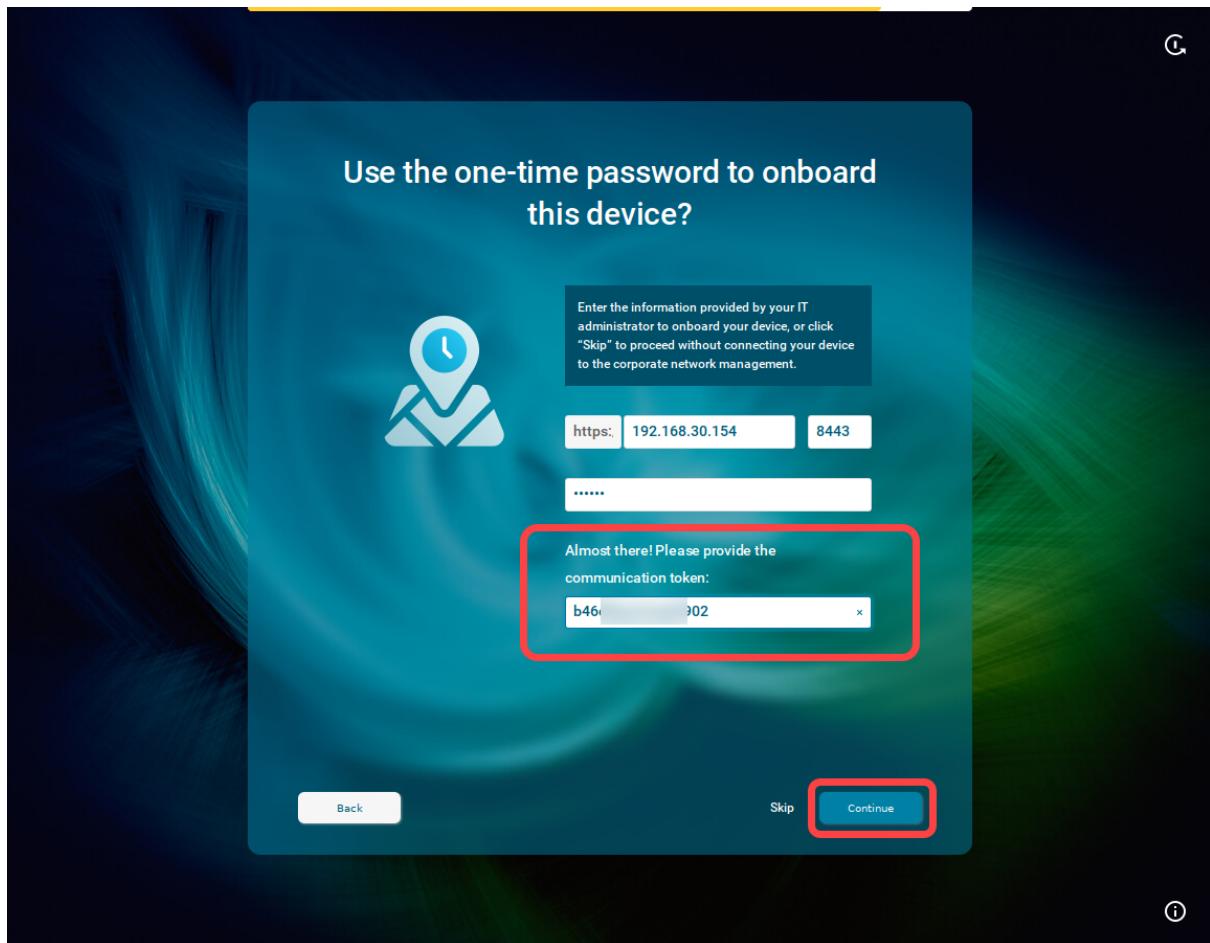
- Mass-deployment keys: Multiple-time keys that can be used by any device and will remain valid after use. If you choose to create a mass-deployment key, there is a possibility to set your own password.

The screenshot shows the UMS Administration interface. The left sidebar has 'First-authentication Keys' selected. A modal window titled 'Create new first-authentication keys' is open, containing four options: 'Create new one-time keys', 'Create new one-time keys', 'Create new one-time keys associated with a device', and 'Create new mass-deployment key'. A red box highlights the 'Create new mass-deployment key' option. A red arrow points from the 'Ok' button at the bottom right of the modal to the 'Ok' button at the bottom right of the main window.

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

The screenshot shows the UMS Administration interface with 'First-authentication Keys' selected in the sidebar. The table lists a single key entry: Unit ID '*****', First-authentication key '*****', Status 'Active', Usage date, Usage count '0', Type 'Mass-deployment key', and Comment. A red box highlights the 'First-authentication Keys' menu item. A red arrow points from the 'Show key' button in the top toolbar to the '*****' value in the 'First-authentication key' column. Another red arrow points from the 'Copy' icon in the top toolbar to the clipboard icon in the same row.

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 .



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 (highlighted with red arrow)

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-49687-1665998487122-2-0
Operating System: Microsoft Windows Server 2019 Standard
Host Name: review-UMS12
Process Type: UMS_SERVER
Port: 30001
Version: 12.00.900.rc3
Cert. Fingerprint - Part 1
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 (highlighted with red box)
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:

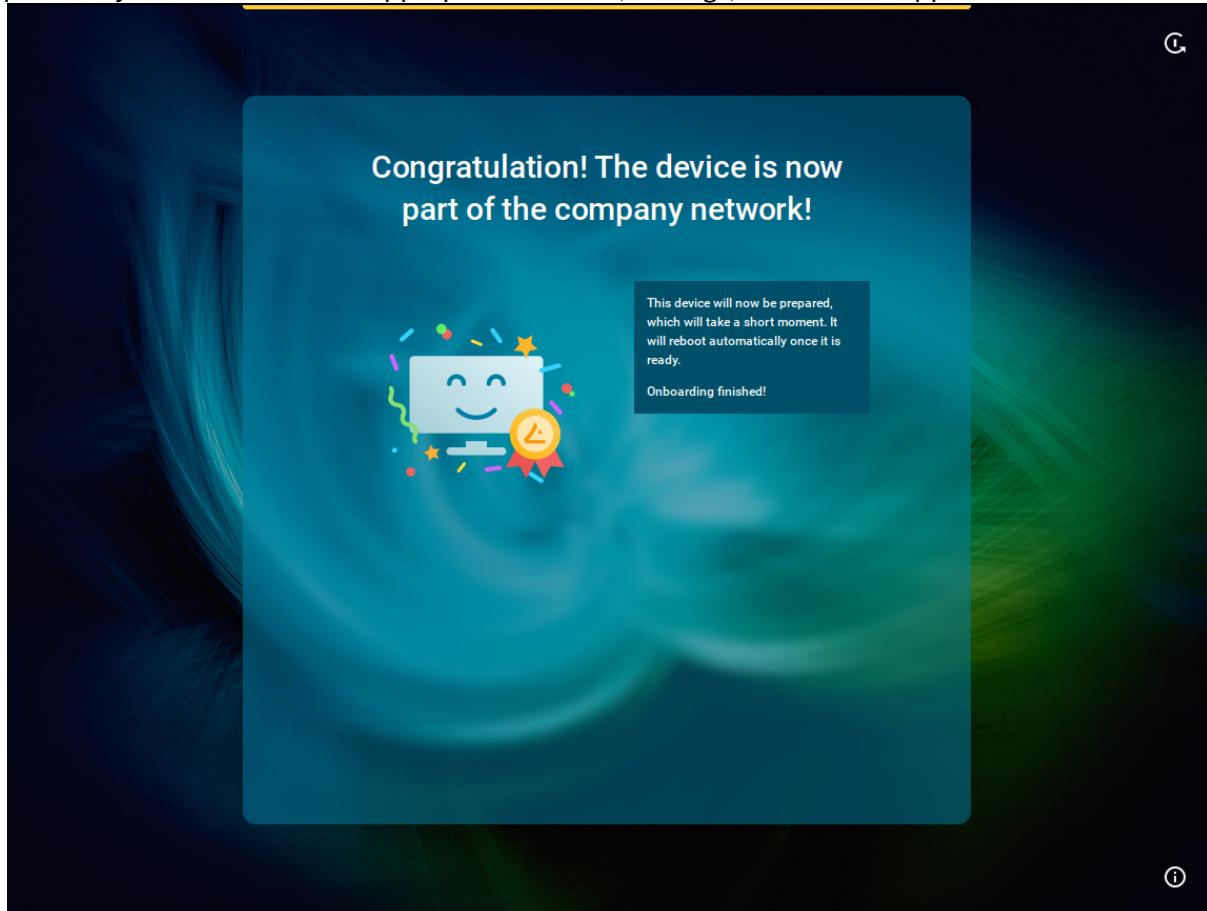
URL / Server address: Host name or IP address of the ICG server

Port: ICG port (Default: 8443)

One-time password: First-authentication key created as described above. You may find it also interesting to read Generating and Distributing First-Authentication Keys for Devices.

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

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



Troubleshooting: Configuring a Network during the Onboarding

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

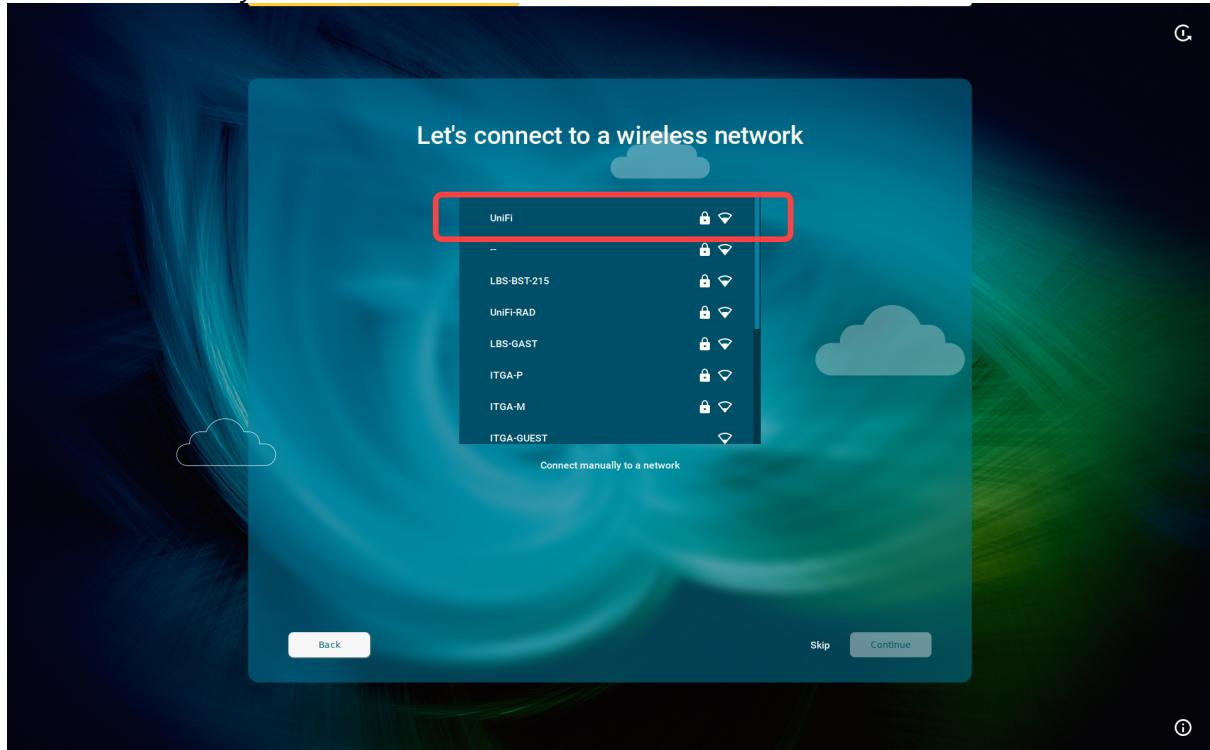


Connecting to a Wireless Network That Is Visible

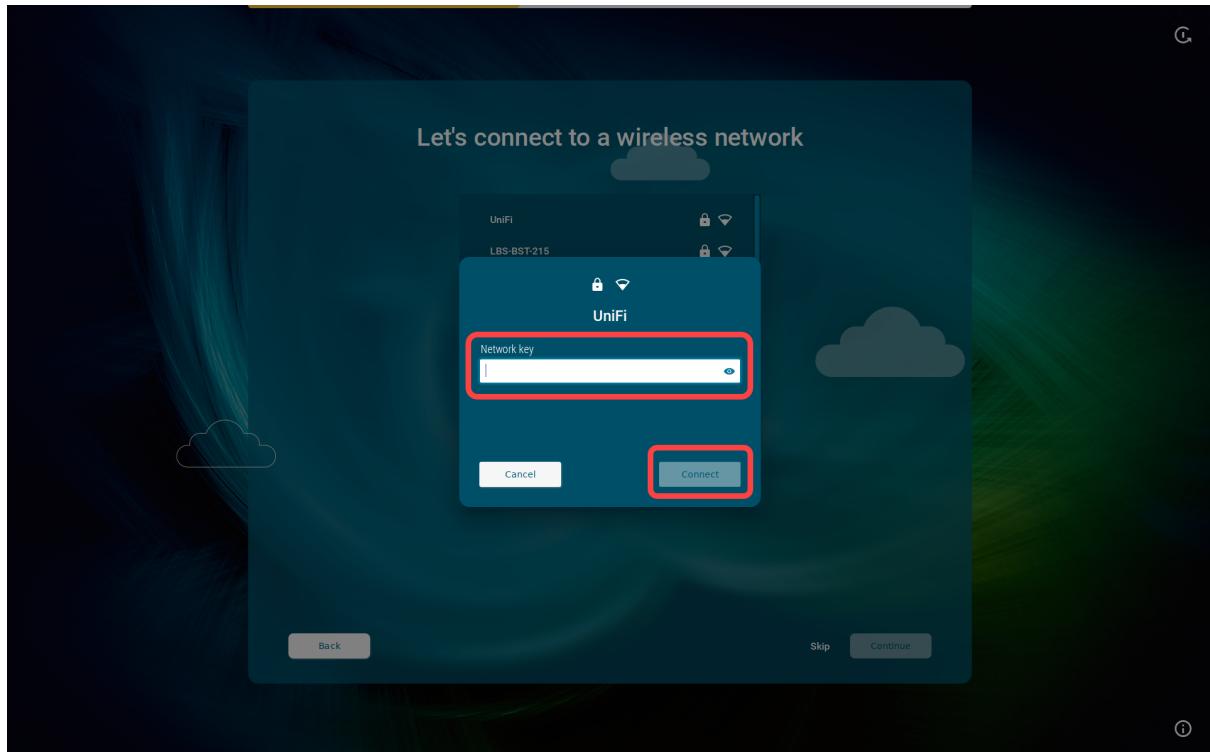
- i Wi-Fi networks with certificates are not supported in the Setup Assistant.

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**.



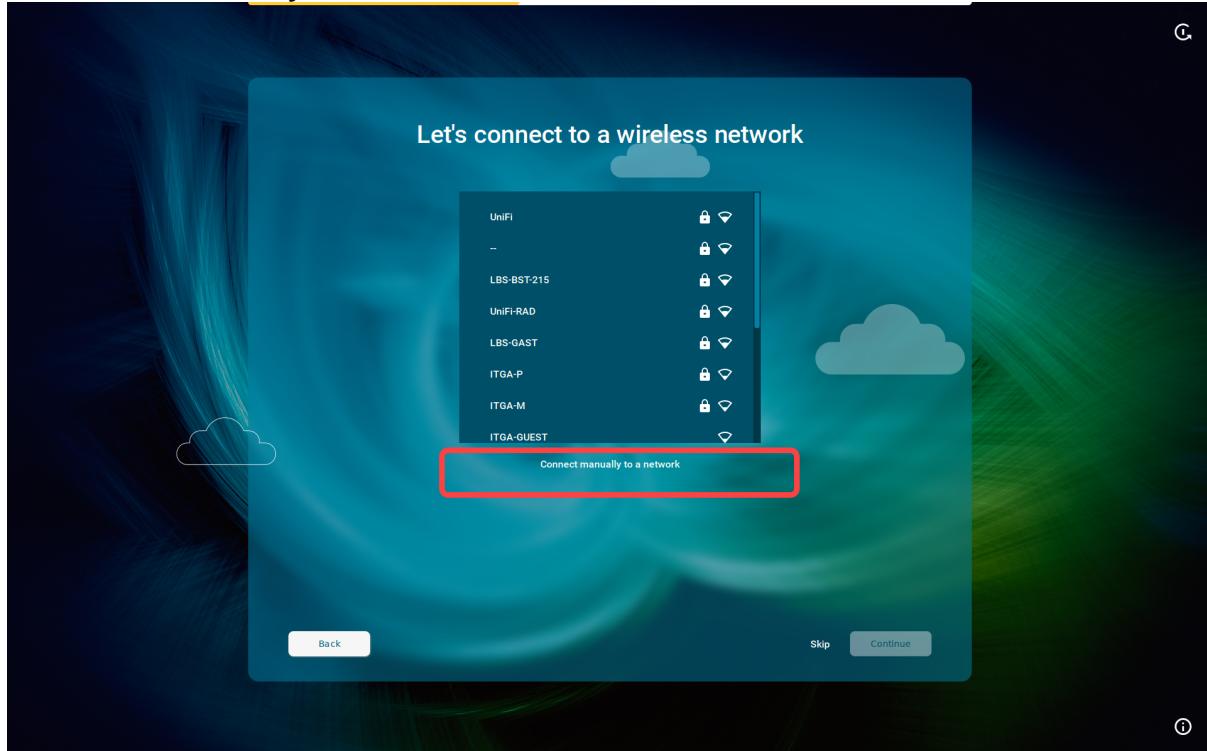
3. Click **Connect**.

- 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**.



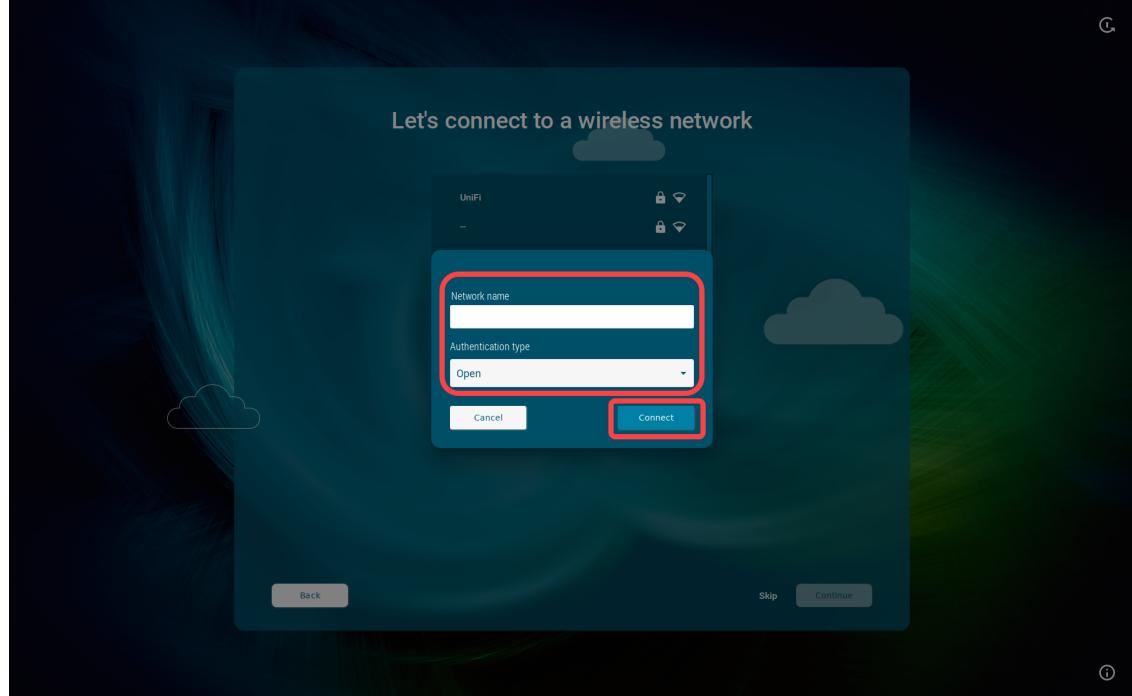
2. Select the **Authentication type** and enter the required authentication data.

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**.

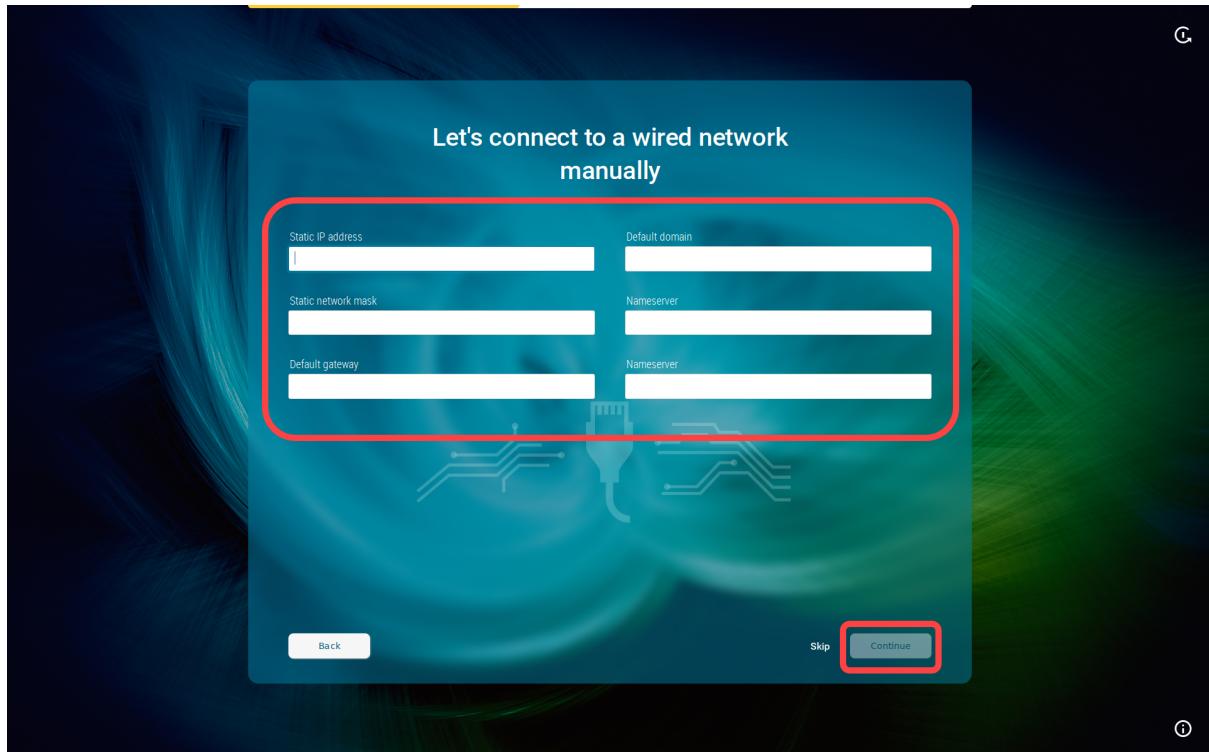


3. Click **Connect**.

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

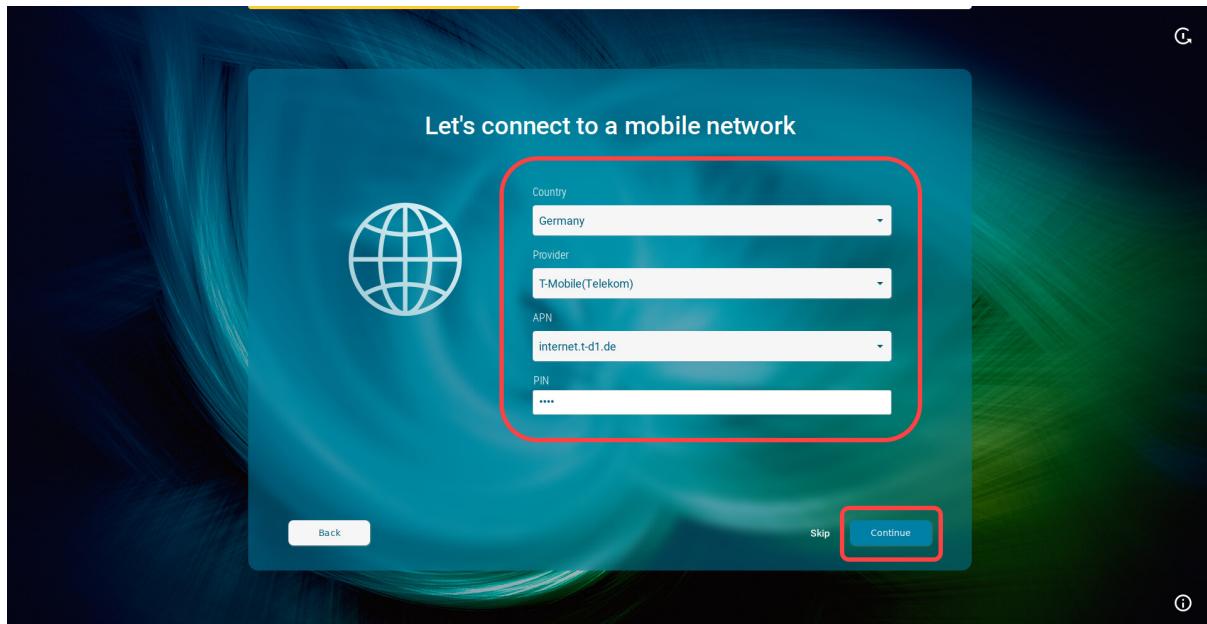
Provider: Provider (the possible options depend on what you choose for **Country**)

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 For information on the solution, see Troubleshooting: Error 38 during the Onboarding of an IGEL OS 12 Device (see page 182).



Error Code	Meaning
39	Failed to retrieve the enrolled certificate
40	Failed to convert the enrolled certificate to PEM
41	Failed to save the enrolled certificate
42	Failed to create a TLS context
43	Failed to create a TLS handle
44	Failed to establish a TCP connection
45	Failed to establish a TLS connection
46	Failed to verify TLS certificate chain
47	Failed to load system trust store

- 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 217) and contact IGEL Support.



Troubleshooting: Error 38 during the Onboarding of an IGEL OS 12 Device

During the onboarding with the IGEL Onboarding Service or with the one-time password method, you get the following error message: " Could not manage your device because of an internal error (<38>) ". Error 38 indicates that the device was unable to register the certificate from the UMS Server(s).

Problem

Possible causes for error 38 may be:

1. The device already exists on the UMS Server.
Typical use case: the device was once registered in the UMS, but was deleted, but not permanently, and remained in the UMS in the recycle bin.
2. Uncommon FQDN of the UMS Server
3. The Public Address is not resolvable by the endpoint devices, or it is not set, and the devices cannot resolve the internal address.
4. Multiple UMS Servers are behind a single external address / load balancer.

Solution

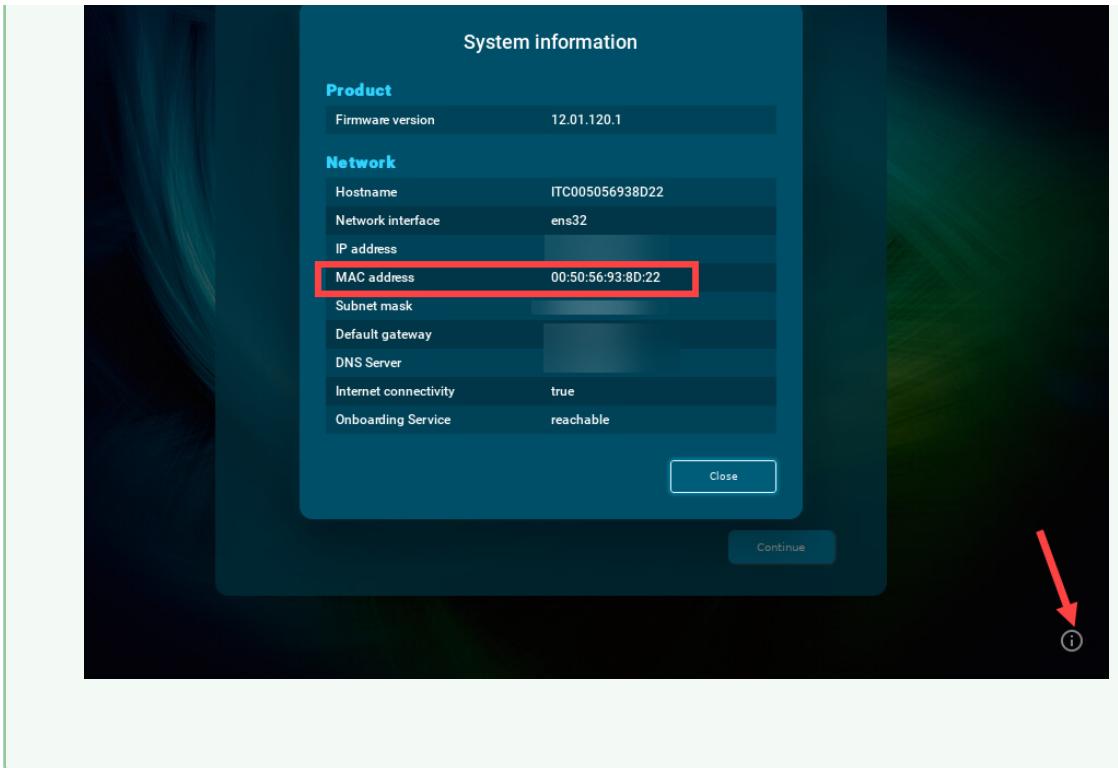
The Device Already Exists on the UMS Server

If you get error 38 during the device onboarding, the first thing to check is if the device has already been registered on the UMS Server. To do this, we will find out the current Unit ID of the device, search for it in the UMS, and will remove the device from the UMS:

1. To find out the Unit ID of the device:
 - If you are still in the IGEL Setup Assistant: Press anytime [CTRL+ALT+F12] or [CTRL+ALT+F11] to enter the command line interface (CLI) and then press [Enter] to log in as root.
 - If you skipped all steps in the IGEL Setup Assistant and started the device with a Starter license: In the **IGEL Setup > Accessories > Terminals**, add a terminal session and log in to the local terminal as root (by default, the password is empty on new devices).

Tip

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



2. Execute the following command:

```
echo $(get_unit_id)
```

This returns the Unit ID of the device:

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

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

Attribute	Value
Unit ID	005056938D22
MAC address	00:50:56:93:8D:22
Last IP	
Product	IGEL OS Base System
Product ID	UIC-LX
Version	12.1.120+1
Firmware Description	

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



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

The device will be moved to the recycle bin. See Recycle Bin - Deleting Objects in the IGEL UMS.

This screenshot shows the IGEL UMS interface. On the left, the navigation tree under 'Server' includes 'IGEL Universal Management Suite 12', 'Profiles (13)', 'Template Keys and Groups (0)', 'Firmware Customizations (1)', and 'Devices (2)'. Under 'Devices', there is a folder 'Augsburg (1)' containing 'td-RD01'. The main panel displays 'td-RD01' with sections for 'System Information' and 'Advanced System Information'. In the bottom right corner of the main panel, there is a message: 'review-UMS12 Jun 27, 2023 11:13 AM'. On the far right, there are two panels: 'Assigned objects' and 'Indirectly assigned objects'. A red box highlights the context menu for 'td-RD01', which includes options like 'Edit Configuration', 'Rename', and 'Delete'. The 'Delete' option is selected.

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

This screenshot shows the IGEL UMS interface with the 'Recycle Bin' selected in the navigation tree. The main panel displays the contents of the recycle bin, which include 'VMware' and 'td-RD01'. At the bottom of the main panel, there are two buttons: 'Restore recycle bin content' and 'Clear recycle bin'. A red box highlights the 'Clear recycle bin' button.

Now, when the device was permanently removed from the UMS, you can repeat the onboarding procedure.

Checking Host Names, FQDNs, and Public Address of the UMS Server

Having incorrect host or public names defined in the UMS can cause issues with devices identifying the UMS and installing the UMS certificates properly, thus resulting in error 38 during the device onboarding.



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

The hostname of the UMS must match the DNS name or SAN name for your UMS web certificate.

- i** The best practice is to use the common / routable FQDN and not the automatically generated name for the hostname. It is generally recommended to check for hostname oddities. For example, such names as `ums00.dci3rsbtpeunizc5g5ggfhwg.ux.internal.cloudapp.net` are common for cloud-hosted servers and generated automatically when creating a VM, e.g. in Azure – they should be renamed to simpler FQDNs such as `ums00.igel-demo.com`. Note that the maximal length of the FQDN is restricted to 255 characters.

If the hostnames do not meet these requirements, you need to update them:

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

The screenshot shows the UMS Administration interface. On the left, a tree view under 'UMS Network' shows 'Server' expanded, with 'UMS00' and 'UMS01' listed. On the right, a table titled 'Service is running' displays server details. The 'Host' attribute for 'UMS00' is highlighted with a red box. The table also lists other attributes like Process ID, Cluster ID, Version, Last Known IP, Public Address, Direct Communication Port, Web Port, Public Web Port, and Operating System.

Attribute	Value
Process ID	b05ed1f2-ac6f-4075-9e31-e22ae57e0f49
Cluster ID	UMS-CLUSTER-39415-1637260546688-2
Version	12.01.110
Host	UMS00
Last Known IP	10.1.1.10
Public Address	ums.
Direct Communication Port	50001
Web Port	8443
Public Web Port	8443
Operating System	Ubuntu 22.04.2 LTS

2. Change the hostname:

- via your operating system

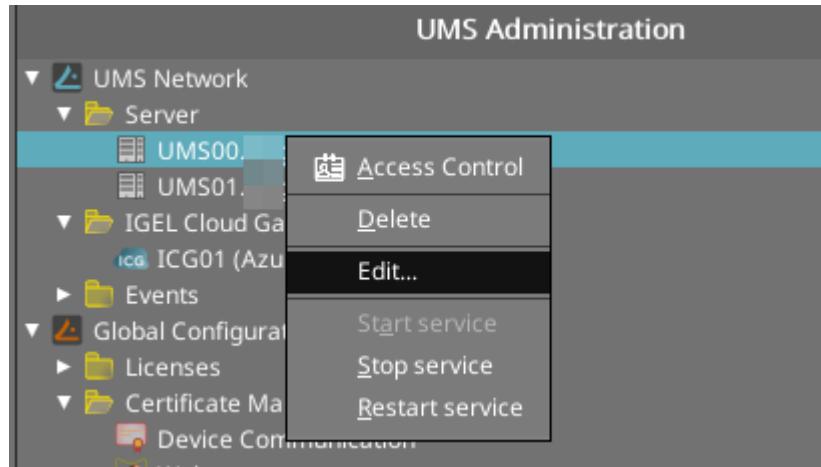
The proper way is to update the hostname of the UMS Server itself. To do this, simply follow your OS vendor's instructions for changing the hostname, and then reboot the server. After that, you should see the changes reflected in the UMS (see step 1).

OR

- via the UMS

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

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



2. Update the **Display Name** to easily resolvable FQDN of the server.
3. If you have a different external name for the server, enter it under **Public Address**. For more information on the Public Address, see Server - View Your IGEL UMS Server Information.

Process Configuration

Display Name	UMS00.igel-demo.com
Public Address	ums.igel.com
Public Web Port	8443

Save Process Configuration Cancel

4. Restart the UMS Server service. For details on how you can do it, see IGEL UMS HA Services and Processes.
5. Validate that you can resolve the **Display Name** or **Public Address** of the UMS Server(s) from your IGEL OS devices.

Specifying the Cluster Addresses of the UMS Server

If you are using multiple UMS Servers and they share a single external address, then you will need to update the FQDN of the UMS cluster; see "Cluster Address" section under Server Network Settings in the IGEL UMS. To do this, you can follow the steps below:

1. Confirm you can resolve / ping the unified FQDN and that it resolves to the correct IP(s) for your UMS cluster.



2. In the UMS Console, go to **UMS Administration > Global Configuration > Server Network Settings** and activate **Enable common cluster address for all UMS Servers**.

The screenshot shows the UMS Administration interface with the 'Server Network Settings' tab selected. The 'Cluster Address' section is highlighted with a red box. It contains the following settings:

- Enable common cluster address for all UMS servers (checked)
- Devices and other external services can reach the UMS cluster at <https://ums.igel.com>
- FQDN of the cluster: ums.igel.com
- Port: (empty input field)

3. Under **FQDN of the cluster**, enter the FQDN that your devices can use to resolve the UMS cluster.
4. If you have configured the custom port, specify it under **Port**.
5. Save the settings.
6. Configure a web certificate for all servers as described under Server Network Settings in the IGEL UMS.
7. Restart the UMS Server service on all servers. For details on how you can do it, see **IGEL UMS HA Services and Processes**.



Installing IGEL OS Apps Locally on the Device

You can install / uninstall apps on your devices not only via the IGEL Universal Management Suite (UMS), but also via the App Portal application on your devices. This is possible if **Permit local app installation** is enabled under **Security > Update**:

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 main panel shows a "Permit local app installation" checkbox with a blue checkmark, also enclosed in a red box. At the bottom left of the main panel is another red box around the "Update" button.

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

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

How to Locally Install Apps

To install apps, proceed as follows:

1. Open the App Portal locally on the device.





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

APP PORTAL OS12

All Apps

Discover Our Apps

ALL AVAILABLE INSTALLED

Categories All Sort by Name

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

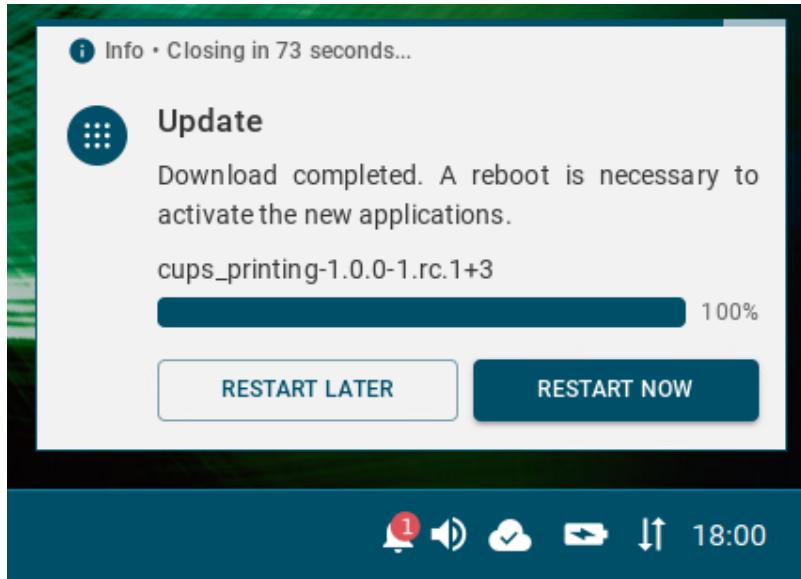
If the selected app / app version has already been installed, the **Uninstall** icon is shown.

- Accept the End User License Agreement (EULA).

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



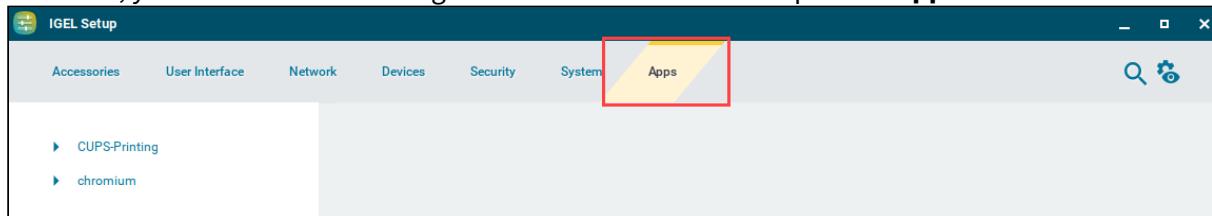
shown:



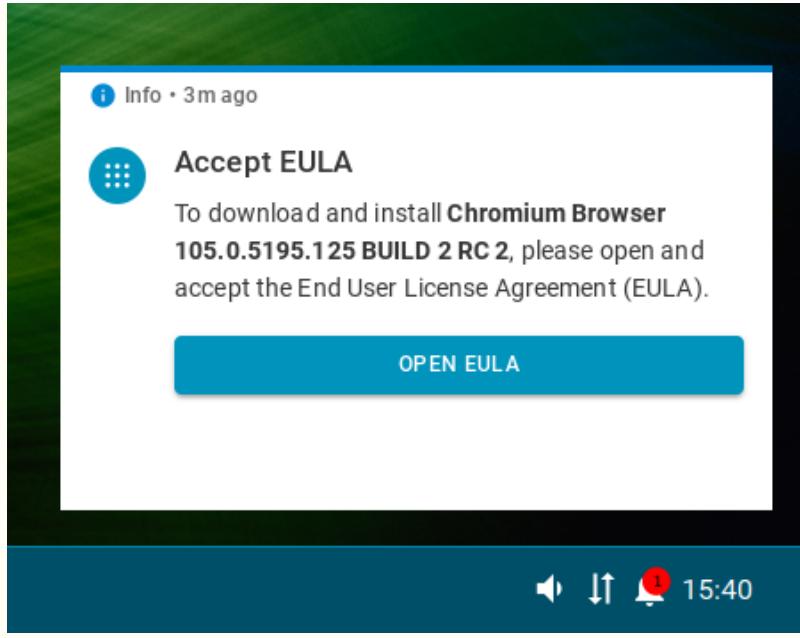
- i** Dependant apps and codecs (e.g. Chromium Multimedia Codec, Fluendo libva for Chromium, Citrix Multimedia Codec) are automatically installed on the device during the installation of the main app (e.g. Chromium Browser app, Citrix Workspace app).

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):



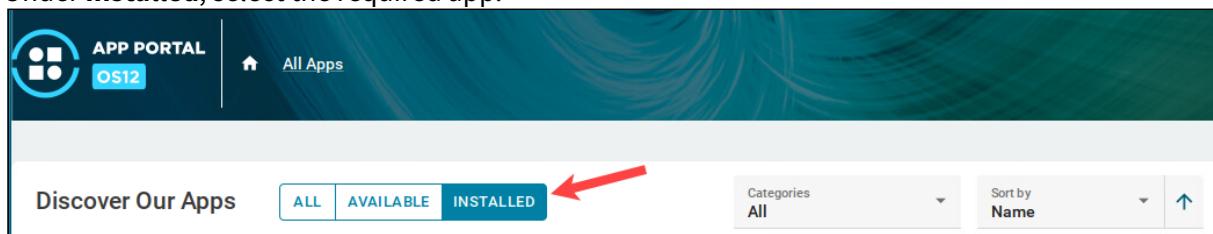
How to Locally Uninstall Apps

To uninstall apps on the device, proceed as follows:

1. Open the App Portal locally on the device.

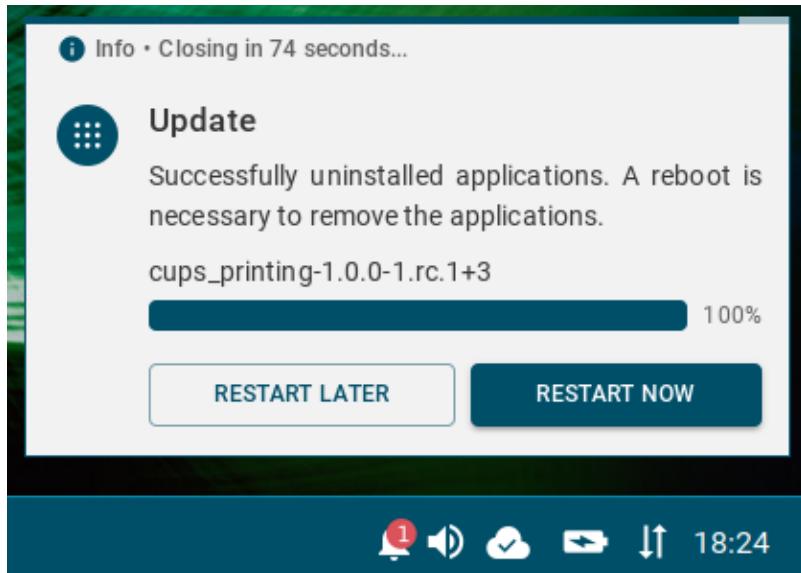


2. Under **Installed**, select the required app.



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 113).

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

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

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

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



Configuring SSO with Okta

Registering an Application in Okta

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

A screenshot of the Okta web interface. On the left, there's a sidebar with a red box around the 'Applications' section. In the main area, there's another red box around the 'Create App Integration' button, which is blue with white text. Other buttons include 'Browse App Catalog' and 'Assign Users to App'. Below these buttons is a table with columns for 'STATUS' (ACTIVE and INACTIVE), followed by several application entries with icons and names like 'Okta Admin Console', 'Okta Browser Plugin', and 'Okta Dashboard'.

STATUS	
ACTIVE	4
INACTIVE	4

Okta Admin Console
Okta Browser Plugin
Okta Dashboard

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



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

The screenshot shows the Okta interface for creating a new app integration. The left sidebar has options like Dashboard, Directory, Customizer, Application (selected), Applications, Self Service, Security, Workflow, Reports, and Settings. The main window title is 'Create a new app integration'. Under 'Sign-in method', 'OIDC - OpenID Connect' is selected. In the 'Application type' section, 'Native Application' is selected. The 'Next' button is highlighted with a red box.

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

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



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

A screenshot of the Okta interface showing the configuration of a new native app integration. The 'App integration name' field is set to 'IGEL OS Single sign-on'. Under 'Grant type', 'Authorization Code' is selected. In the 'Sign-in redirect URIs' section, the URL 'http://localhost/callback' is entered into the input field. Both fields are highlighted with red boxes.

The app integration is created.



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

A screenshot of the Okta application configuration interface. At the top, there's a search bar and navigation links for "Back to Applications", "IGEL OS Single sign-on" (which is active, indicated by a blue background), "Active", and "View Logs". Below this is a tabs menu with "General" (highlighted with a red box and underlined), "Sign On", "Mobile", "Assignments", and "Okta API Scopes".

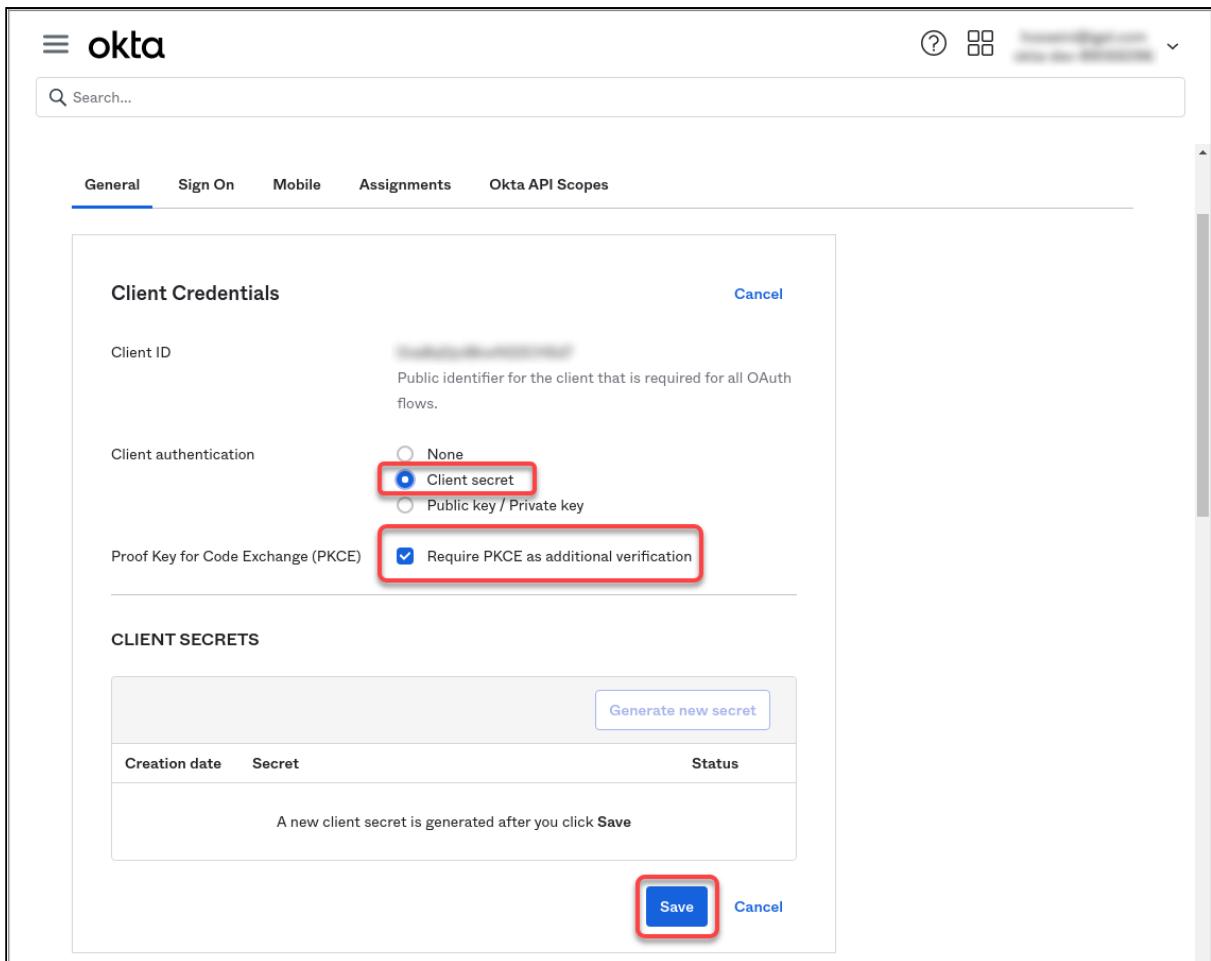
The main content area is titled "Client Credentials". It shows a "Client ID" field with a blurred value and an "Edit" button to its right, also highlighted with a red box. A tooltip below the field explains it as a "Public identifier for the client that is required for all OAuth flows".

Under "Client authentication", there are three radio button options: "None" (selected), "Client secret", and "Public key / Private key".

At the bottom, there's a checkbox for "Proof Key for Code Exchange (PKCE)" with the sub-instruction "Require PKCE as additional verification" checked.

A vertical scrollbar on the right side of the page indicates more content is available.

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

A screenshot of the Okta Client Credentials configuration page. The page has tabs at the top: General (selected), Sign On, Mobile, Assignments, and Okta API Scopes. The General tab shows the "Client Credentials" section. It includes fields for "Client ID" (disabled) and "Client authentication" (set to "Client secret"). A checkbox for "Require PKCE as additional verification" is checked and highlighted with a red box. Below this is the "CLIENT SECRETS" section, which contains a table with columns for "Creation date", "Secret", and "Status". A note says "A new client secret is generated after you click Save". At the bottom are "Save" and "Cancel" buttons, with "Save" highlighted with a red box.

Client ID

Client authentication

Client secret

Require PKCE as additional verification

CLIENT SECRETS

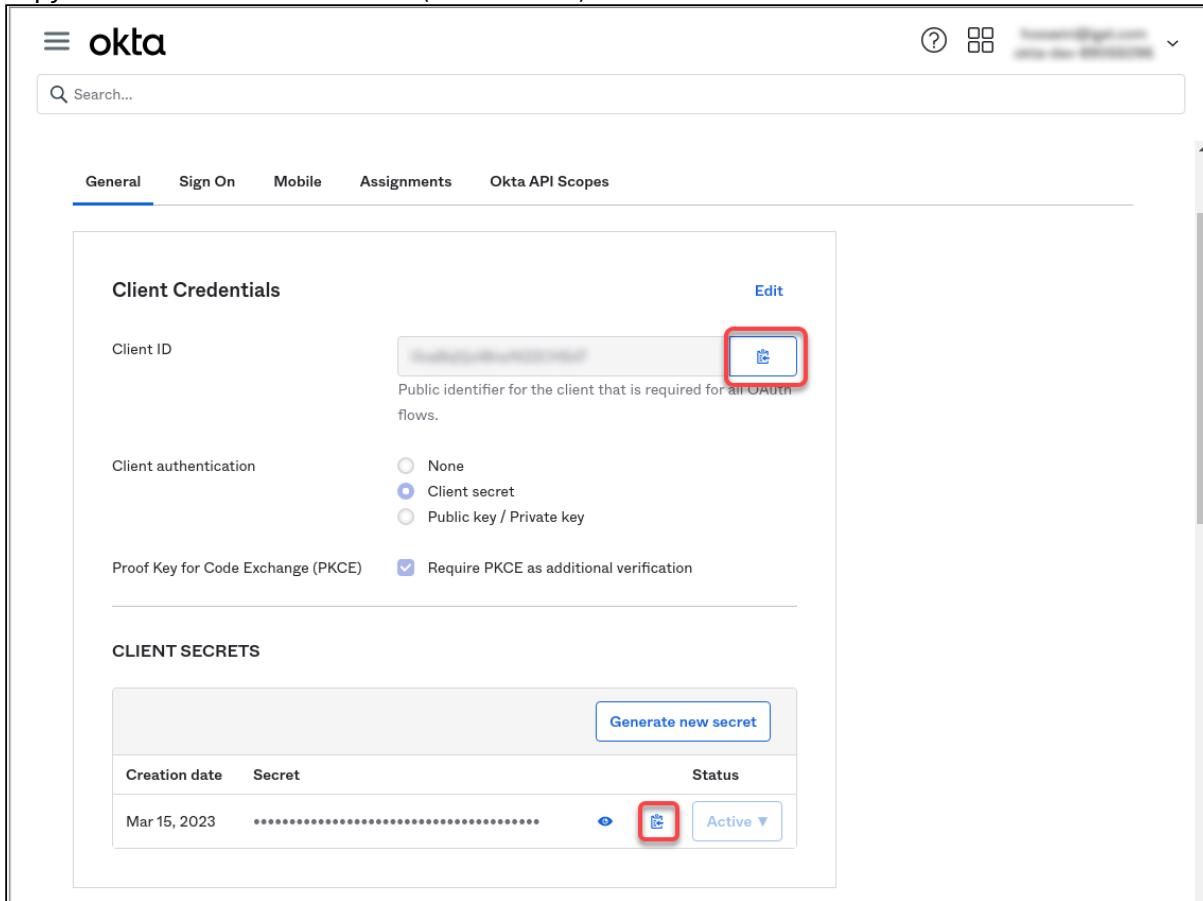
Generate new secret

Creation date Secret Status

A new client secret is generated after you click Save

Save Cancel

The client secret will be created.

6. Copy the **Client ID** and the **Secret** (client secret).A screenshot of the Okta interface showing the "Client Credentials" section. The "General" tab is selected. Under "Client Credentials", there is a "Client ID" field with a copy icon (a blue square with a white "C") highlighted with a red box. Below it is a description: "Public identifier for the client that is required for all OAuth flows." Under "Client authentication", the "Client secret" option is selected. There is also a checkbox for "Require PKCE as additional verification". Under "CLIENT SECRETS", there is a table with one row. The row shows "Mar 15, 2023" in the "Creation date" column, a long secret string in the "Secret" column, and an "Active" status with a dropdown arrow. A copy icon in the "Secret" column is also highlighted with a red box.

Configuring IGEL OS for SSO with Okta

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



- Provide the **Client secret**.

The screenshot shows the 'Single Sign-On with Identity Provider' configuration dialog. On the left, a sidebar lists various logon methods: Device Encryption, Password, Logon (Taskbar, Active Directory/Kerberos, Single Sign-On, Local User), Active Directory/Kerberos, Smartcard, Change password, and Update. 'Single Sign-On' is selected. The main panel shows the 'Identity Providers' configuration with Okta selected as the Identity Provider. The 'Client ID' and 'Client secret' fields are highlighted with a red box.

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

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

Setting up SSO with Azure AD

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

Registering an Azure Application

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

Configuring Single Sign-On (SSO)



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

Home > App registrations > Register an application ... X

* 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 (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.
http://localhost/callback ✓

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 [↗](#)

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

The screenshot shows the Microsoft Azure portal interface for managing API permissions. The left sidebar has a tree view with 'API permissions' selected and highlighted by a red box. The main content area shows a table of permissions under 'Configured permissions'. A single row is visible, representing the 'User.Read' permission from Microsoft Graph. This row is also highlighted by a red box. The 'Type' column indicates it is 'Delegated', and the 'Description' column says 'Sign in and read user p...'. The 'Admin consent req...' column shows 'No'.

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

4. Click **Add a permission**.

The screenshot shows the Microsoft Azure portal interface for managing API permissions. The URL in the address bar is [Home > \[redacted\] | App registrations > IGEL OS Single sign-on](#). The main title is "IGEL OS Single sign-on | API permissions".

The left sidebar has a "Manage" section with the following options: Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions (which is selected and highlighted in grey), Expose an API, App roles, Owners, Roles and administrators, and Manifest.

The right pane has a heading "Configured permissions" with a note: "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](#)".

A callout box highlights the "Add a permission" button, which is located next to a checkmark and the text "Grant admin consent for IGEL SSO".

The table below lists the configured permission:

API / Permissions name	Type	Description	Admin consent req...	Status
User.Read	Delegated	Sign in and read user profile	No	...

At the bottom, there is a note: "To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#)".



5. Select Microsoft Graph.

Screenshot of the "Request API permissions" dialog in the Azure portal, showing the selection of Microsoft Graph.

The dialog title is "Request API permissions". The left sidebar shows the navigation path: Home > App registrations > IGEL OS Single sign-on > API permissions. The "API permissions" section is selected.

The main area displays "Commonly used Microsoft APIs" with a highlighted box around the "Microsoft Graph" card:

- 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.
- Azure DevOps**: Integrate with Azure DevOps and Azure DevOps server.
- Azure Service Management**: Programmatic access to much of the functionality available through the Azure portal.
- Office 365 Management APIs**: Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs.

The "More Microsoft APIs" section contains the following cards:

- Azure Batch**: Schedule large-scale parallel and HPC applications in the cloud.
- Azure Communication Services**: Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams.
- Azure Cosmos DB**: Fast NoSQL database with open APIs for any scale.
- Azure Data Catalog**: Programmatic access to Data Catalog resources to register, annotate and search data assets.
- Azure Data Explorer**: Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions.
- Azure Data Explorer (with Multifactor Authentication)**: Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions.
- Azure Data Lake**: Access to storage and compute for big data analytic scenarios.
- Azure Import/Export**: Programmatic control of import/export jobs.
- Azure Key Vault**: Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults.



6. Select **Delegated permissions**.

The screenshot shows the 'Request API permissions' page for the 'IGEL OS Single sign-on' application in the Microsoft Azure portal. The left sidebar lists various management options like Overview, Quickstart, Integration assistant, and API permissions, which is currently selected. The main area shows the 'Microsoft Graph' API selected from the 'All APIs' list. It asks 'What type of permissions does your application require?' with two options: 'Delegated permissions' (selected) and 'Application permissions'. A red box highlights the 'Delegated permissions' section, which states: 'Your application needs to access the API as the signed-in user.' The 'Application permissions' section is also visible, stating: 'Your application runs as a background service or daemon without a signed-in user.'

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

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



- profile

The screenshot shows the 'Request API permissions' dialog in the Microsoft Azure portal. The left sidebar shows the 'IGEL OS Single sign-on' app registration with the 'API permissions' section selected. The main area displays the 'Microsoft Graph' API with its documentation link. It asks for 'Delegated permissions' (needed for signed-in users) and 'Application permissions' (needed for background services). Under 'Select permissions', three OpenID permissions are listed: 'email', 'openid', and 'profile'. The first two are highlighted with red boxes, and the third is also highlighted with a red box. At the bottom are 'Add permissions' and 'Discard' buttons, with 'Add permissions' also highlighted with a red box.

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



8. Check if the permissions are correct.

Screenshot of the Microsoft Azure portal showing the API permissions for the "IGEL OS Single sign-on" application. The "API permissions" section is selected in the left sidebar. A red box highlights the list of permissions under "Microsoft Graph (4)".

API / Permissions name	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 **Certificates & secrets** and click **New client secret**.A screenshot of the Microsoft Azure portal interface. The title bar says "IGEL OS Single sign-on | Certificates & secrets". On the left, there's a sidebar with "Manage" and "Support + Troubleshooting" sections. Under "Manage", several items are listed: Overview, Quickstart, Integration assistant, Certificates & secrets (which is highlighted with a red box), Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, and Manifest. The main content area has tabs for Certificates (0), Client secrets (0) (which is selected and highlighted with a red box), and Federated credentials (0). Below the tabs, it says "A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password." There's a button labeled "+ New client secret" with a red box around it. A tooltip above the table says "Application registration certificates, secrets and federated credentials can be found in the tabs below." A table below shows columns for Description, Expires, Value (with a help icon), and Secret ID. A note at the bottom says "No client secrets have been created for this application."

Description	Expires	Value ⓘ	Secret ID



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

A screenshot of the Microsoft Azure portal showing the 'App registrations' section for 'IGEL OS Single sign-on'. The 'Certificates & secrets' tab is selected. A modal window titled 'Add a client secret' is open, prompting for a 'Description' (with a placeholder 'Enter a description for this client secret') and an 'Expires' date ('Recommended: 180 days (6 months)'). Both fields are highlighted with a red box. At the bottom of the modal, the 'Add' button is also highlighted with a red box.



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

The screenshot shows the 'Certificates & secrets' tab selected in the left sidebar. Under 'Client secrets (1)', there is one entry for 'IGEL OS SSO client secret'. The 'Value' column for this entry is highlighted with a red box. The 'Secret ID' column also has a red box around its value.

Description	Expires	Value	Secret ID
IGEL OS SSO client secret	9/19/2023	[Redacted Value]	[Redacted Secret ID]

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

The screenshot shows the 'Overview' page for the application. The 'Display name' is 'IGEL OS Single sign-on'. The 'Client credentials' section shows the 'Application (client) ID' and 'Add a certificate or secret'. The 'Redirect URLs' section shows '0 web, 0 spa, 1 public client'. The 'Application ID URI' section shows 'Add an Application ID URI'. The 'Managed application in local directory' section shows 'IGEL OS Single sign-on'. The 'Object ID' and 'Directory (tenant) ID' fields are highlighted with red boxes.

Client credentials
Add a certificate or secret

Redirect URLs
0 web, 0 spa, 1 public client

Application ID URI
Add an Application ID URI

Managed application in local directory
IGEL OS Single sign-on



Configuring IGEL OS for SSO with Azure ID

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

The screenshot shows the 'Single Sign-On' configuration page in the IGEL COSMOS web interface. The 'Identity Providers' section is highlighted with a red box. It contains the following fields:

- Identity Provider:** Azure AD
- Azure AD Tenant Name/ID:** [REDACTED]
- Application (client) ID:** [REDACTED]
- Client secret:** [REDACTED] (with a 'Change password' button below it)

At the bottom of the page are three buttons: 'Close', 'Save', and 'Save and Close'. The 'Save and Close' button is highlighted with a blue box.

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

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

You can now use the [apps and utilities for IGEL OS 12 that support SSO with Azure AD](#)(see page 193).

For details on importing apps from the IGEL App Portal and installing them on IGEL OS devices,

see [IGEL UMS 12: Basic Configuration](#)(see page 106) and [Assignment of Apps and Profiles](#)(see page 118).

All methods of multi-factor authentication are available except the hardware token.

Enabling Local Login (Optional)

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

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

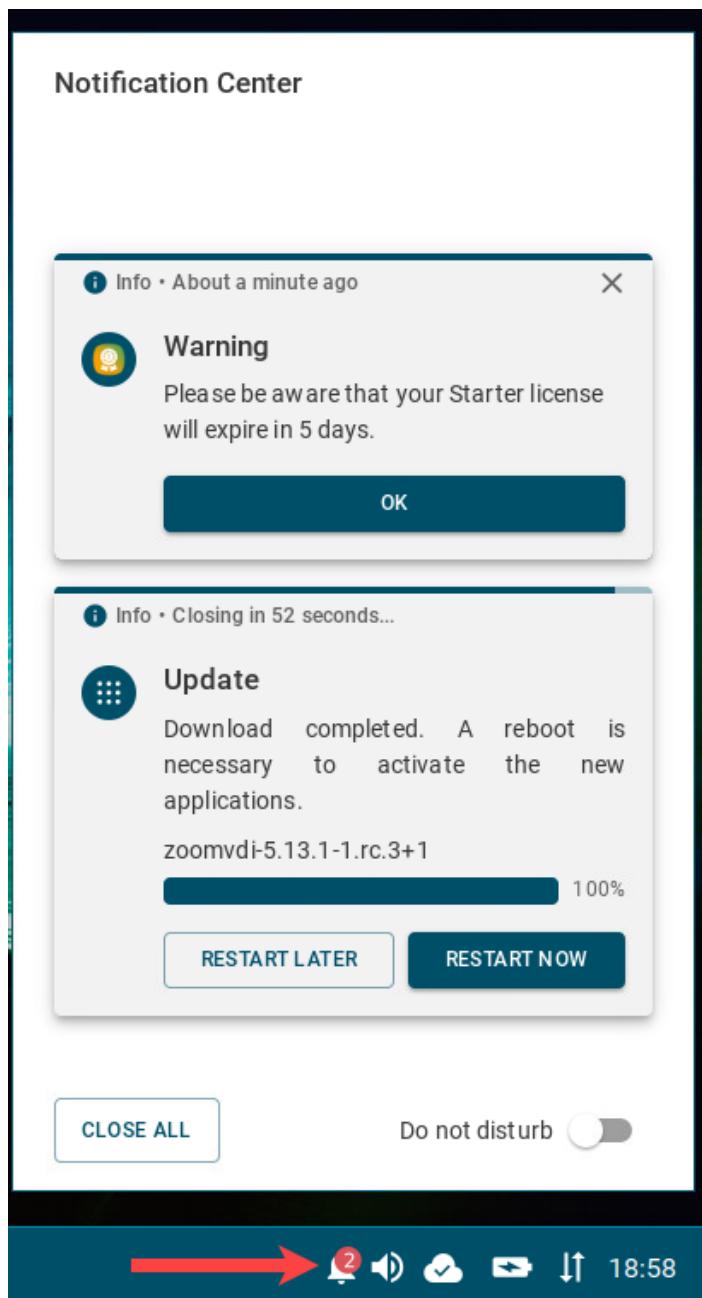
2. Activate **Login with local user password** and enter a password.

The screenshot shows the 'Profile Configurator - Default Profile' interface. The top navigation bar has tabs: Accessories, User Interface, Network, Devices, Security (which is highlighted in yellow), and System. On the left, a sidebar menu includes Device Encryption, Password, Logon (with Taskbar, Active Directory/Kerberos, Single Sign-On, Local User selected), Active Directory/Kerberos, Smartcard, Change password, and Update. At the bottom left is an App Selector button. The main area shows a configuration dialog for 'Login with local user password'. This dialog has a checked checkbox labeled 'Login with local user password' and two password input fields, both containing '.....'. Below these fields is a button labeled 'Set password' and a note 'Password not yet set'. To the right of this dialog is another section titled 'Logout Shortcut Locations' with three items: 'Start Menu' (disabled), 'Menu folder' (disabled), and 'Start Menu's System tab' (disabled). At the bottom right of the dialog 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 112).
- Messages sent by the UMS administrator
- Warnings, e.g. about license expiration, and errors
- Other notifications, e.g. about a new configuration the system has received



IGEL Insight Service

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

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

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

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

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

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

For more information, please refer to IGEL's [privacy policy](#)²².

- ⓘ **Where Are the IGEL COSMOS Cloud Services Data Stored?**

Currently, the IGEL COSMOS Cloud Services and apps available in the IGEL App Portal are stored in Azure Region West-Europe, location Amsterdam. The associated app metadata are stored in Frankfurt (Germany west central).

The Insight Service data are currently also stored in Frankfurt (Germany west central).

All data centers and their operators are fully ISO/IEC 27001 certified.

Data Collected by the IGEL Insight Service

- Company identifier
- UMS identifier
- Pseudonymized device identifier
- Name of the application
- Version of the application
- Manufacturer of the device
- Model of the device
- CPU of the device
- RAM of the device
- Mainboard of the device
- GPU of the device

²² <https://www.igel.com/privacy-policy/>



- Storage hardware of the device
- Network / Wi-Fi hardware information of the device
- Peripheral hardware information of the device
- Timestamp
- Client type (Insight Service Data Collector)
- Client version (Insight Service Data Collector)

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



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

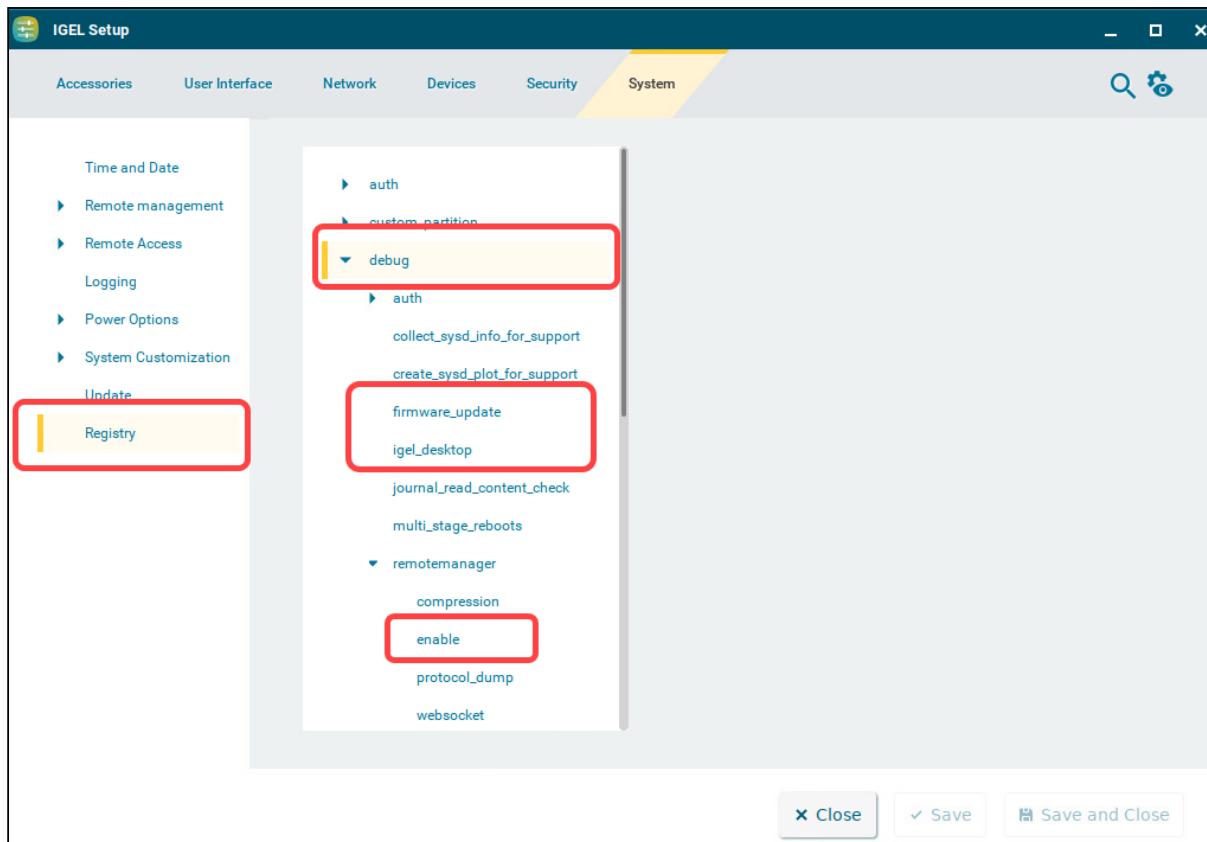
To collect the log files from the IGEL UMS Server, UMS Console, etc., you can use the Support Wizard: **UMS Console** > **Menu bar > Help > Save support information**. See Support Wizard in the IGEL UMS.

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

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

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

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



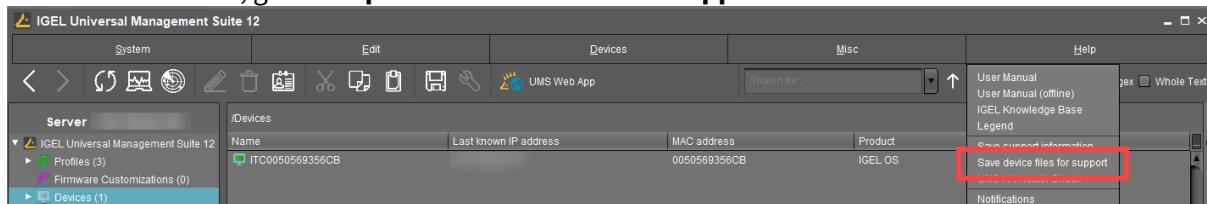
2. Click **Save or Apply**.

- 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:

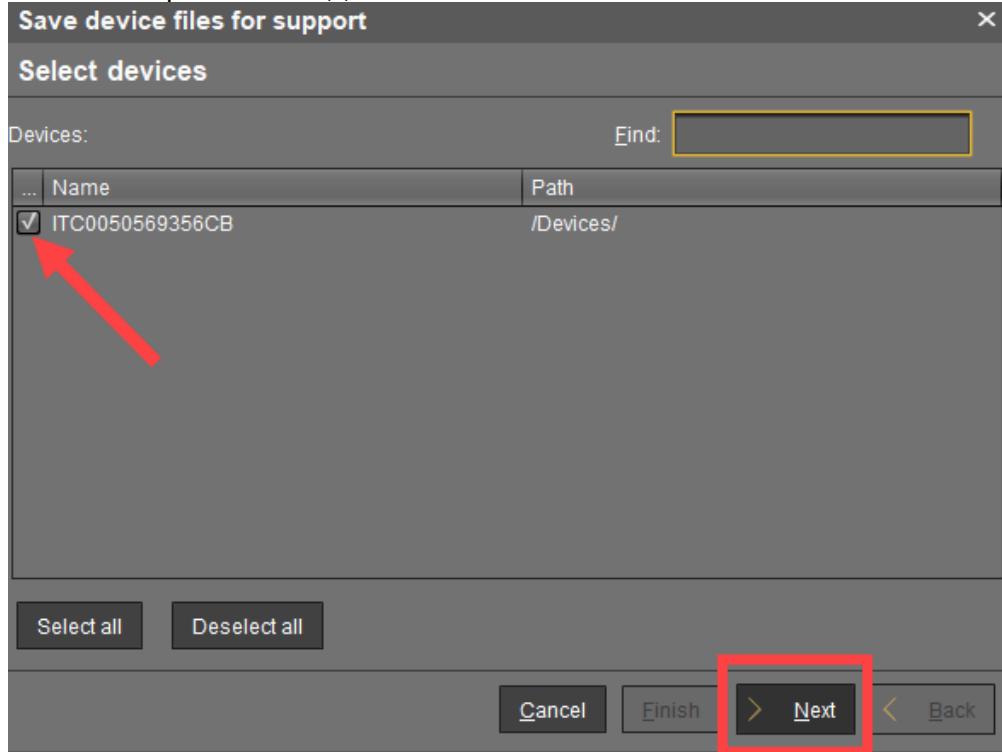
1. In the UMS Console, go to **Help > Save device files for support**.





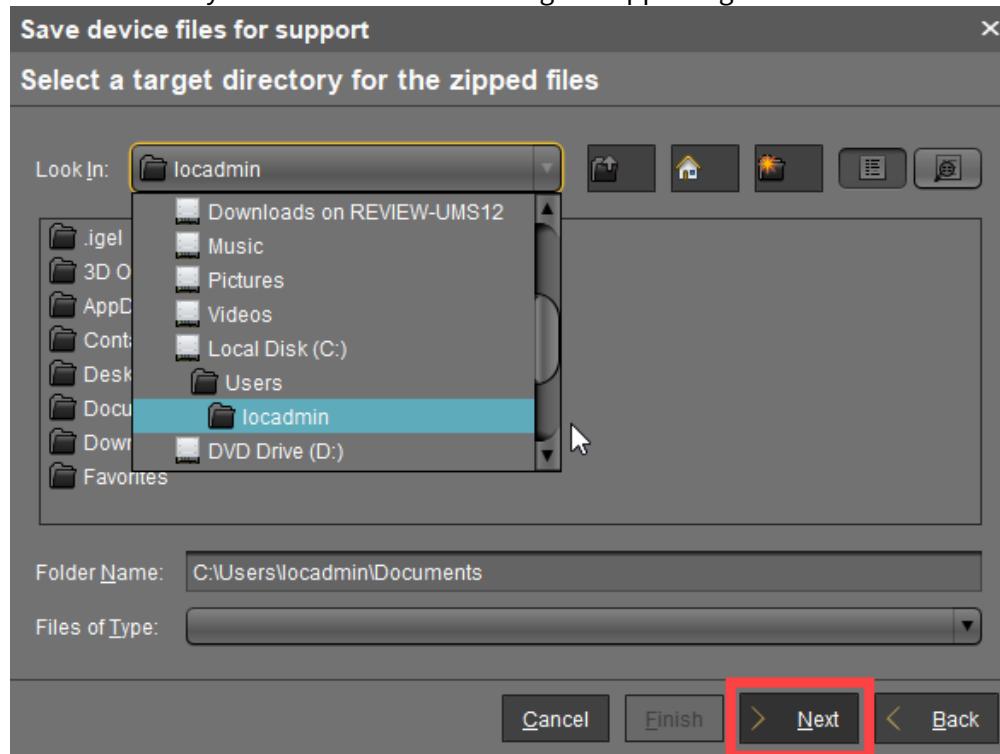
The dialog **Save device files for support** opens.

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



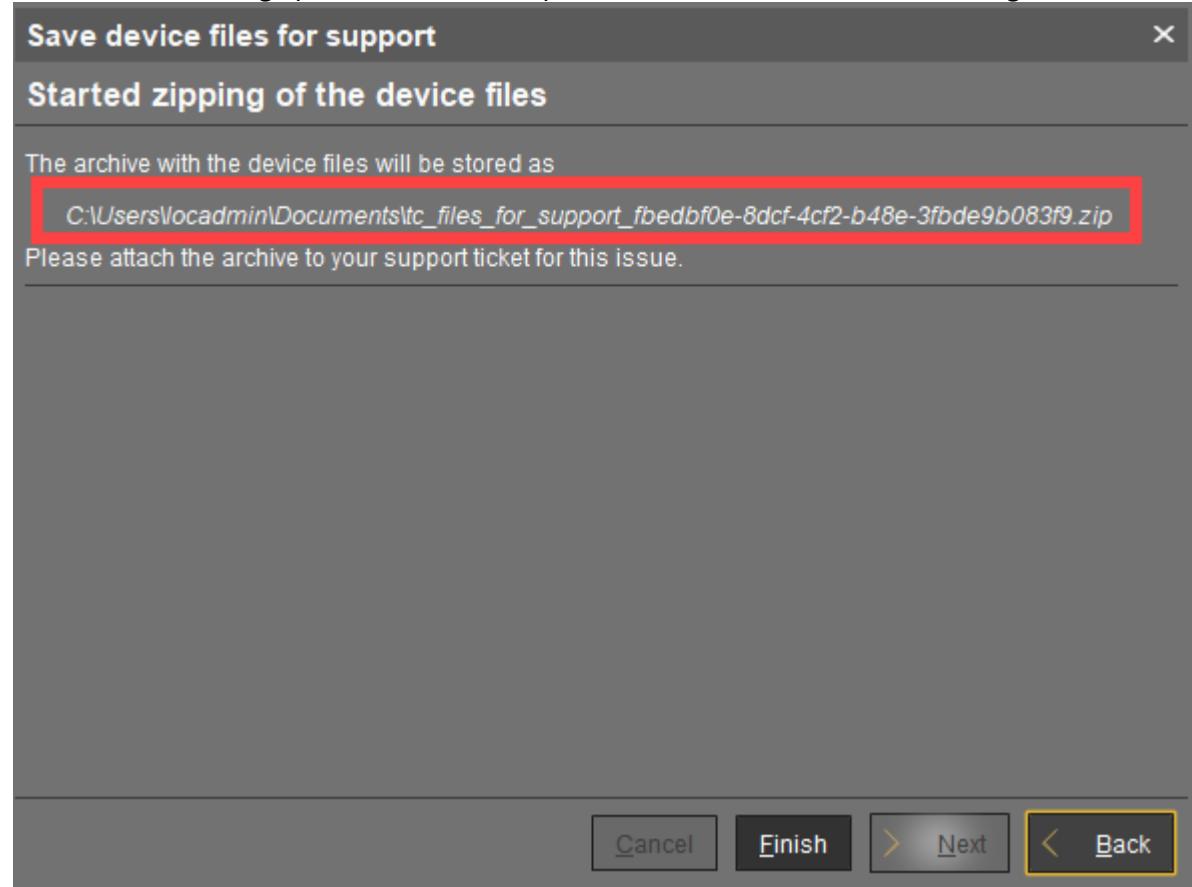


3. Select a directory which is suitable for saving the zipped log files and click **Next**.





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 ²³GEL Support via the [IGEL Customer Portal](#)²⁴.

Collecting Device Logs without the UMS

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

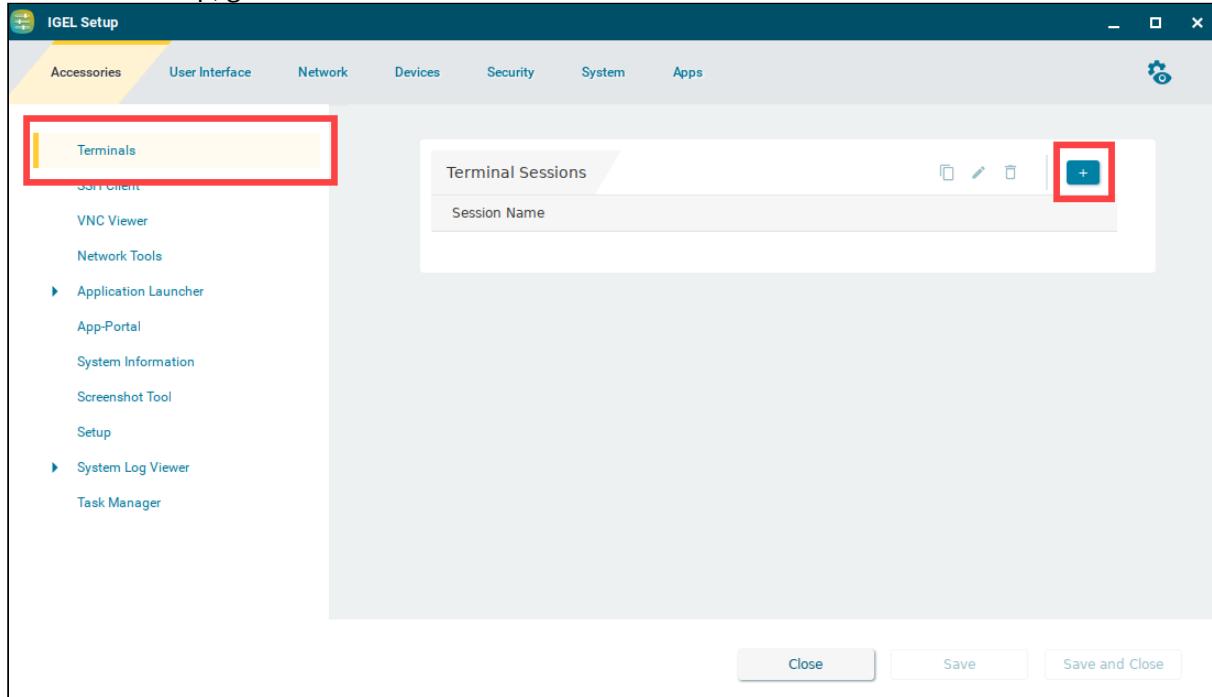
²³mailto:eap@igel.com

²⁴<https://cosmos.igel.com/>



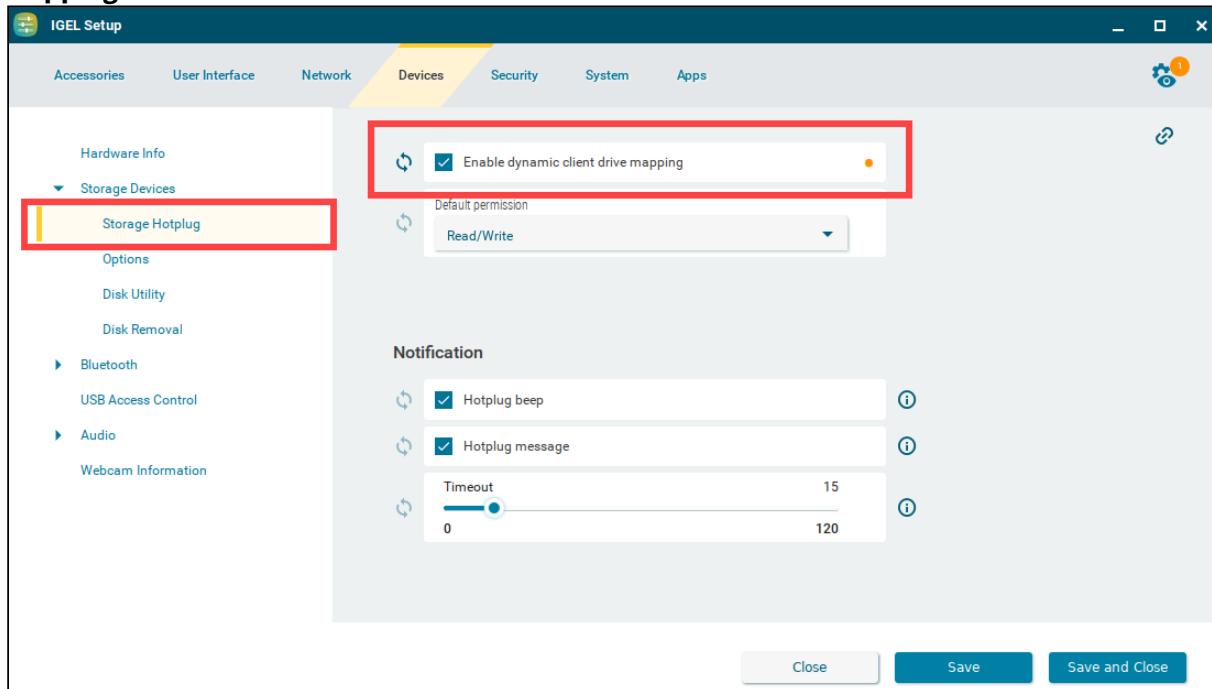
Option 1: Via Local Terminal

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





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



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

```
Local Terminal
login as "user" or "root": root
root@ITC00E0C561FAF7:~# /config/bin/create_support_information
warning: cannot stat '/var/lib/systemd/journalctl': 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%) 
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 ²⁵GEL Support via the [IGEL Customer Portal](#)²⁶.

Option 2: Via CLI

You can collect log files also via command line interface (CLI). This method can be useful, for example, if you experience problems on the stage of device onboarding.

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

²⁵mailto:eap@igel.com

²⁶<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](https://cosmos.igel.com/)²⁷.

²⁷ <https://cosmos.igel.com/>