A Guide: Migrating to Windows 11 in the cloud with IGEL

Author: Andy Prior

Change Log

Author	Date	Change	Version
Andy Prior	21/06/2024	Initial Draft	1.0
Andy Prior	06/08/2024	Updated UMS Images on page 8, minor changes to formatting	1.1

Contents

NOTICE

Copyright

Trademarks

Disclaimer

The specifications and information contained in this manual are intended for information use only, are subject to change at any time without notice and should not be construed as constituting a commitment or obligation on the part of IGEL Technology GmbH. IGEL Technology GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including any pertaining to the products and software described in it. IGEL Technology GmbH makes no representations or warranties with respect to the contents thereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

A Guide: Migrating to Windows 11 in the cloud with IGEL

IGEL OS12 Deployment options for Endpoints & automated device configuration to deliver a seamless user experience when connecting to Windows 11 in the Cloud.

Microsoft Windows 365 Cloud PC, Microsoft Azure Virtual Desktop and IGEL provide a robust solution to a modern hybrid cloud strategy with SaaS, Daas and VDI workloads. Streamline migration to Windows 11 by optimizing existing devices with IGEL OS, improving endpoint security, simplifying management and reducing costs.

As organizations prepare for the end of Windows 10 support in October 2025, the migration to Windows 11 on the endpoint presents challenges, particularly with hardware compatibility, financial impact, and environmental concerns. IGEL OS, Microsoft AVD and Windows 365 provide a robust solution to these challenges, enhancing Windows 11 capabilities through improved security, cost efficiency, simplified management, and environmental sustainability.

In this guide we look at IGEL OS provisioning options; how to enroll the device using the IGEL Onboarding service, apply OS settings, something we call Profiles, deploy the IGEL AVD client and automatically connect to a Microsoft AVD Desktop.

Here is a video of the user experience from boot, discovery, configuration and connect to Microsoft AVD in less than three minutes.

Let’s build this! https://youtu.be/GMMSC8bHj1k

Assumptions

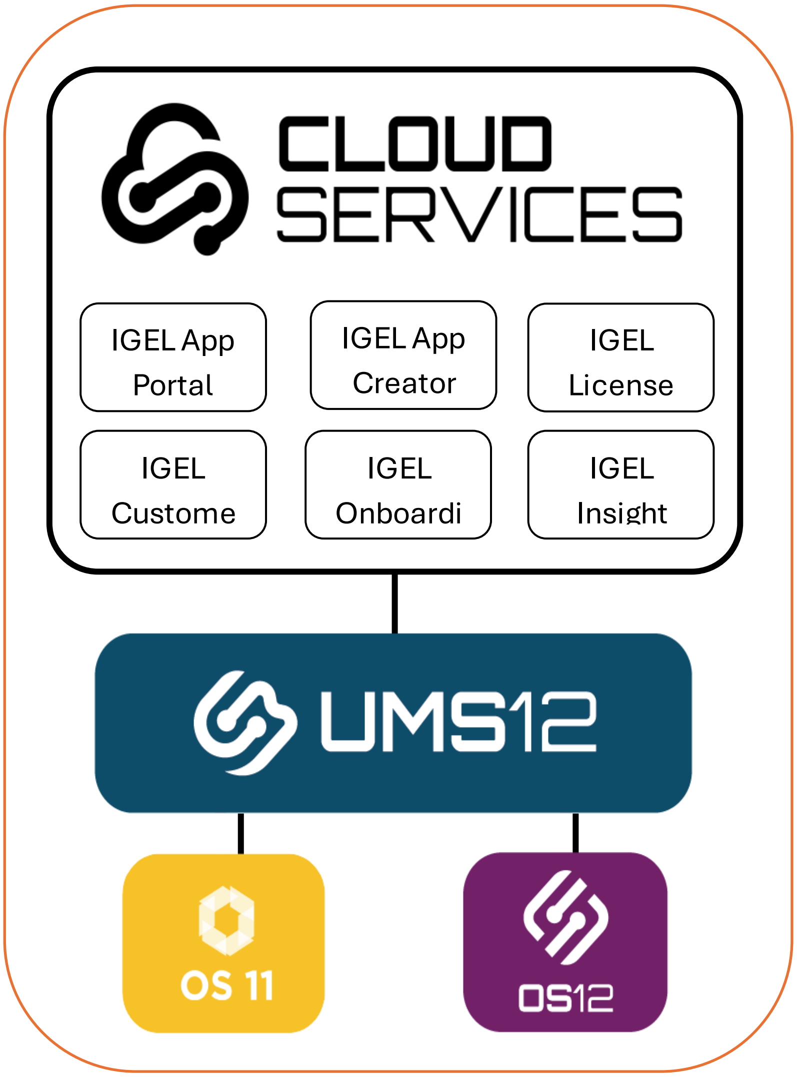
There are a few assumptions when using this guide to deploy IGEL OS and connecting to Microsoft AVD.

- You have a working Microsoft EntraID and AVD environment running Windows 11 hosts.
- UMS is installed and licensed.
- Customer Portal Admin user already created.
- The IGEL OS12 device can communicate with the UMS server and has Internet access.
- UMS server has internet access.
- You are running OS12 on the target device.
- If you don't have these pre-requirements in place, you can find details on these here:
    - https://kb.igel.com/en/how-to-start-with-igel/current/

IGEL Overview

There are three main components which make up IGEL's next gen secure edge operating system.

OS12	a lightweight secure endpoint operating system.
Universal Management Suite (UMS)	allows for the remote configuration and control of IGEL operating systems.
Cloud Services	A set of Cloud based services used to manage, deploy and maintain your IGEL environment.



Cloud Services

IGEL Cloud Services is an End User Computing platform that includes several cloud services allowing for better flexibility, managing authentication options, managing applications and OS image versions, automatic provisioning, license management, RBAC and insights.

IGEL Cloud Services comprises of the following components:

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.

UMS Registration Service is used to register and authenticate your UMS instance. This will allow UMS to communicate with the IGEL Cloud Services.

IGEL Onboarding Service allows your users to easily onboard IGEL OS 12 devices and users using only their corporate email, this service has a related service: IGEL OS idp, this is used for identifying your users using an external identity provider using OpenID and OAuth 2.0 authorization protocols.

IGEL App Portal where you can find all applications and base OS images currently available for IGEL OS 12.

IGEL Insight Service which collects analytical and usage data to improve IGEL products and services and provide a better customer experience.

IGEL License Portal is where you can manage licenses for your IGEL OS devices.

Universal management Suite (UMS)

IGEL Universal Management Suite (UMS) is the management software for the secure central remote administration of IGEL OS devices. With the UMS, you can configure endpoint devices in the same way as locally on the device. Typical areas of use would be; automatic provisioning of devices, configuring devices software clients, tools, authentication options, corporate look and feel, distributing updates, diagnostics and support.

OS12

IGEL OS 12 is the latest version of IGEL's managed endpoint OS designed for secure, high-performance access to any digital workspace.

It standardizes diverse endpoints onto a unified platform and provides adaptive configuration and granular control, while giving users a familiar, trouble-free workspace. Supporting more remote display protocols and attached peripheral devices than any alternative solution, IGEL OS 12 is purpose-built for enterprise access to virtual environments of all types.

IGEL OS12 Deployment Options

What options are available for me to convert my existing x86 64 hardware to IGEL OS12?

I'll not be covering the actual deployment of the IGEL OS in detail in this article. I think it is important to cover the various deployment options available to you and any pre-requisites needed to run the IGEL OS.

OS Creator (OSC)

With the IGEL OS Creator (OSC), you can install IGEL OS 12 on any supporting device. Moreover, you can use the IGEL OS Creator to recover a broken installation of IGEL OS that cannot boot anymore. The OSC is used to create a bootable USB drive containing the IGEL image.

PXE

The Preboot Execution Environment or PXE (commonly pronounced as pixie) is a client-server environment that enables network computers to boot over the network interface card.

IGEL SCCM Add-on

IGEL OS 12 SCCM Add-on facilitates deploying IGEL OS via Microsoft SCCM. The package contains IGEL OS Base System as a dd image (dd is a command used to capture a Linux image) that will be booted using a Windows PE boot file customized for this purpose.

With the installation of IGEL OS SCCM Add-on, a customized Windows PE image and a task sequence for deploying IGEL OS are created, and the IGEL OS Image Manager is installed.

UD Pocket

UD Pocket boots IGEL OS on your computer. However, it does not make any changes to the operating system already installed on the device's storage – UD Pocket runs entirely from the USB stick.

To facilitate booting your UD Pocket, you can use the IGEL UD Pocket Starter. The IGEL UD Pocket Starter creates a boot option for the UD Pocket so that there is no need to change the boot settings manually. You can install the IGEL UD Pocket Starter easily on an endpoint device running Microsoft Windows 10 or 11 - provided Microsoft BitLocker is not active on the device. When you uninstall the IGEL UD Pocket Starter, it is removed without any trace on the device.

The minimum system requirements for IGEL OS12 are listed below:

- CPU: 64-bit dual core 1.5Ghz
- Memory: 4GB If you intend to run high resolutions, multiple monitors or unified communications, higher specifications are recommended.
- Storage: 8GB
- Graphics: Intel ATI\AMD Nvidia
- Network Card: Ethernet or wireless

Whilst OS12 will run on any hardware with the above specification a List of tested and supported devices can be found here: https://kb.igel.com/hardware/en/devices-supported-by-igel-os-12-81496425.html

Software Downloads: https://www.igel.com/software-downloads/igel-os-12-secure-endpoint/

IGEL Ready

Want to know if your device is compatible? The IGEL Ready program authorizes technology companies to partner with IGEL to integrate and certify their products with IGEL OS. https://www.igel.com/ready/

Let’s build it!

Now that we have covered all the components which make up the IGEL OS ecosystem it’s time to configure things. In this section I’ll be detailing how to configure the IGEL Cloud services, register your UMS, configure the onboarding service and setting up EntraID as an Identity Provider (idp), configure UMS profiles to deploy the IGEL AVD client and configure the IGEL OS.

Cloud Services Configuration

Onboarding Service

IGEL Onboarding Service configuration

For onboarding your users and devices, IGEL Cloud Services needs to know your UMS and your users. The UMS is identified and authenticated by its fully qualified domain name (FQDN) or IP address and its root certificate. The users are authenticated by an external identity provider (IdP). For that, we are using the OpenID Standard to obtain user information and the standardized OAuth 2.0 authorization protocols.

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

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

Activating the Onboarding Service (OBS)

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

1. Log in to the IGEL Customer Portal .

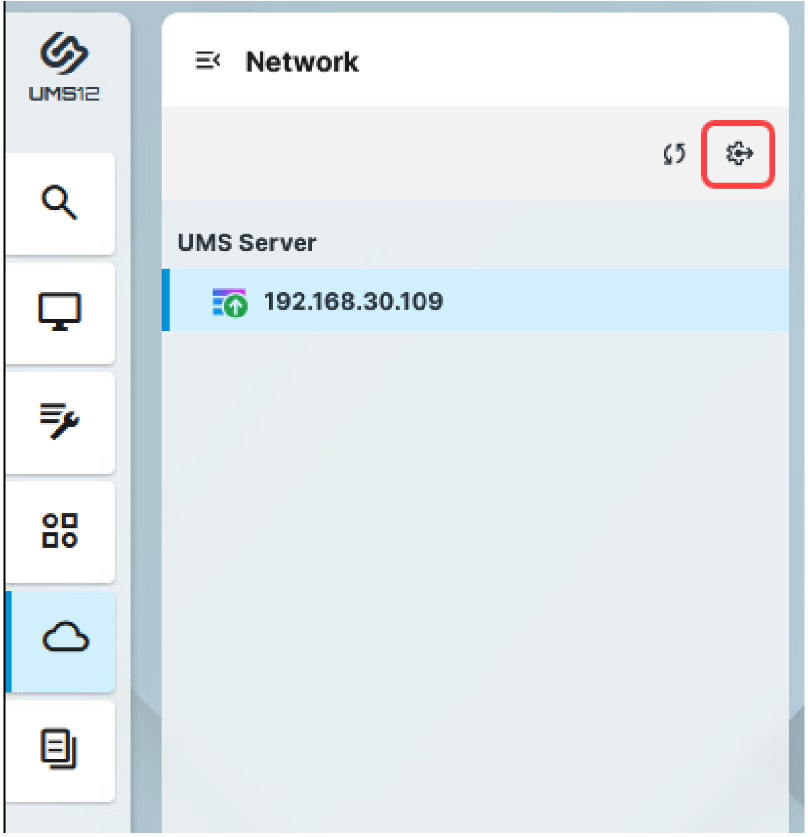
2. From the menu, select **Activate IGEL OS Onboarding**.

Downloading the Root Certificate Chain

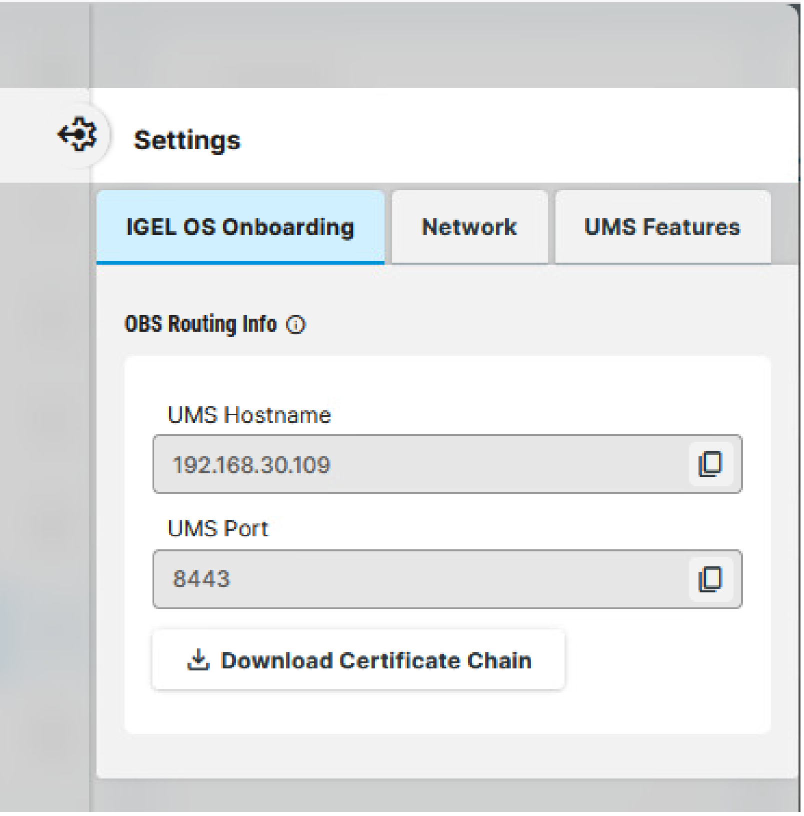
▶ In the web browser, open the URL https://<server>:8443/webapp/#/login

If your UMS is to be connected directly to your endpoint devices, you download the certificate chain of the UMS.

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



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



UMS Hostname: 192.168.30.109

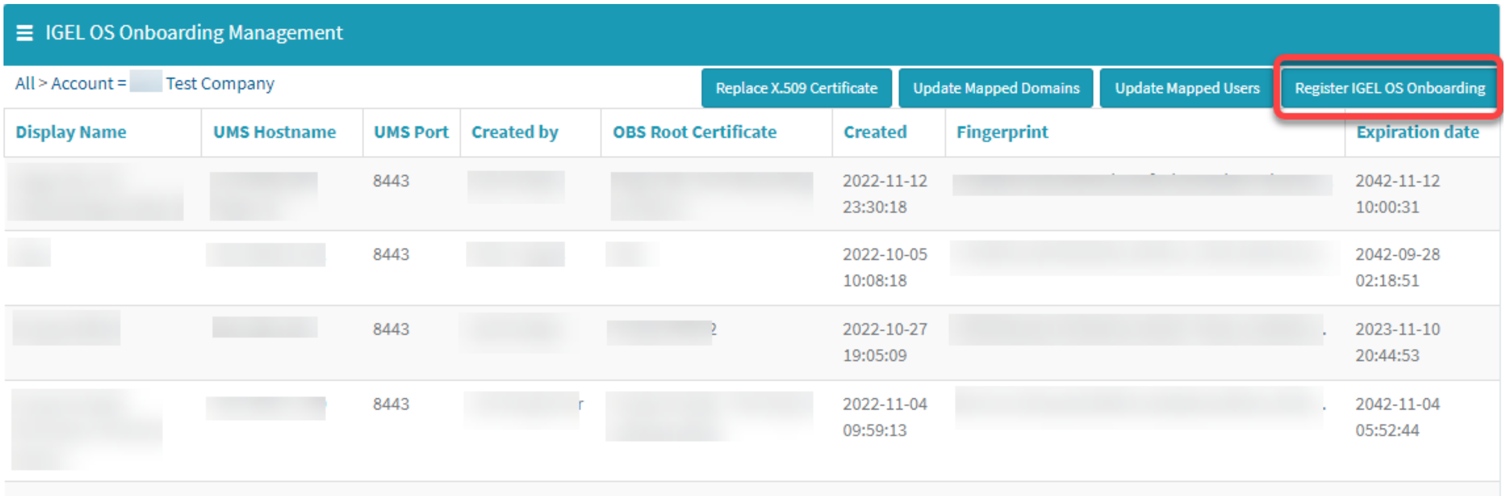
UMS Port: 8443

2. Click **Download Certificate Chain**.
   The certificate file is downloaded to your file system. In the following step, we will use it for the OBS routing.

Creating the Record Set for the OBS Routing

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

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


IGEL OS Onboarding Management
Replace X.509 Certificate
Update Mapped Domains
Update Mapped Users
Register IGEL OS Onboarding

All > Account = [redacted] Test Company

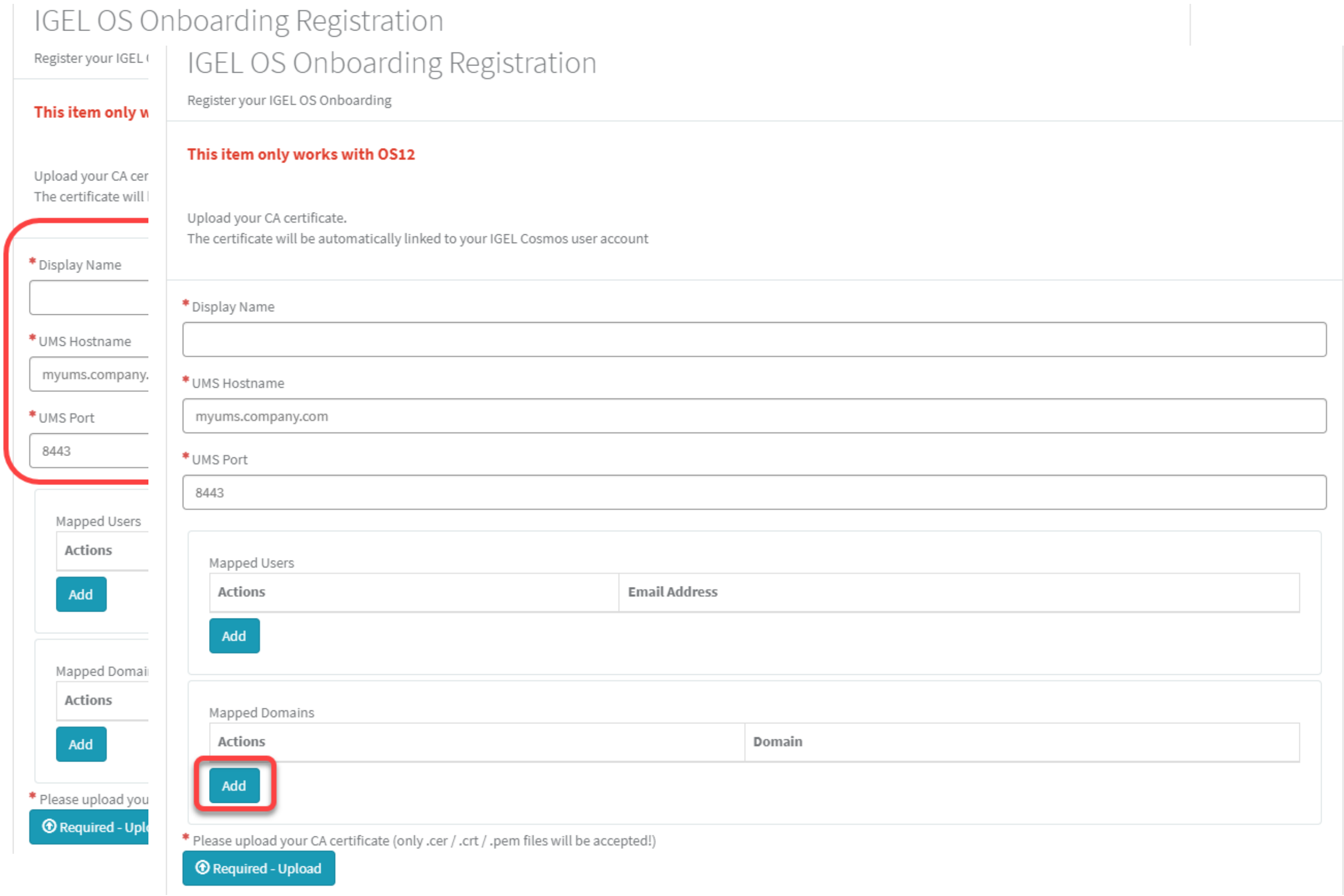
Display Name	UMS Hostname	UMS Port	Created by	OBS Root Certificate	Created	Fingerprint	Expiration date
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-11-12 23:30:18	[redacted]	2042-11-12 10:00:31
[redacted]	[redacted]	8443	[redacted]	[redacted]	2022-10-05 10:08:18	[redacted]	2042-09-28 02:18:51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

3. Enter the following data:

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

     > **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.



IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name

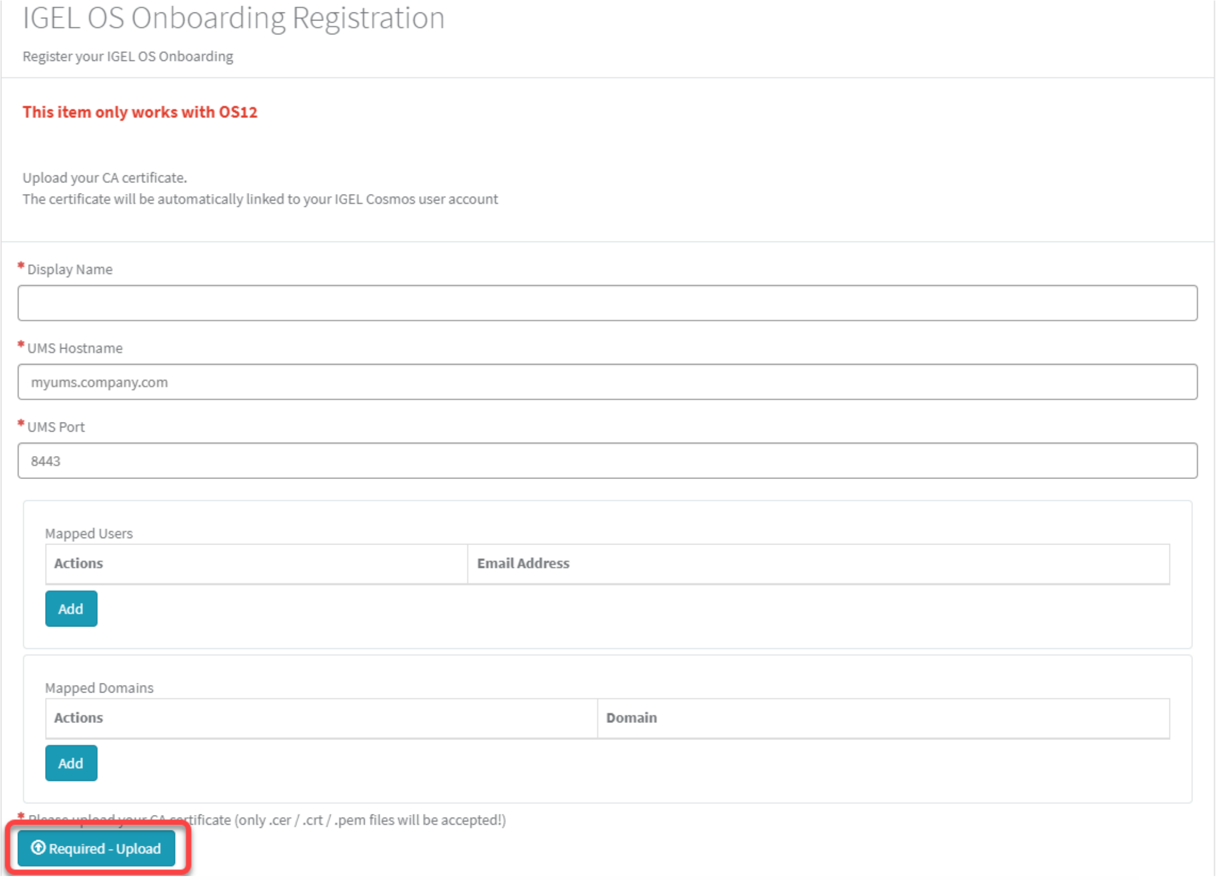
* UMS Hostname: myums.company.com

* UMS Port: 8443

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

4. Proceed by adding individual users or one or more domains that include all e-mail addresses of these domains.
   - To add an individual user, click **Add** in the area **Mapped Users**.
   - To add a domain, click **Add** in the area **Mapped Domains**.
5. In the dialog, enter the e-mail address of the user we have created in Microsoft Entra ID or the relevant domain and click **Add**.

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



IGEL OS Onboarding Registration

Register your IGEL OS Onboarding

This item only works with OS12

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

* Display Name

* UMS Hostname

myums.company.com

* UMS Port

8443

Mapped Users

Actions	Email Address

Add

Mapped Domains

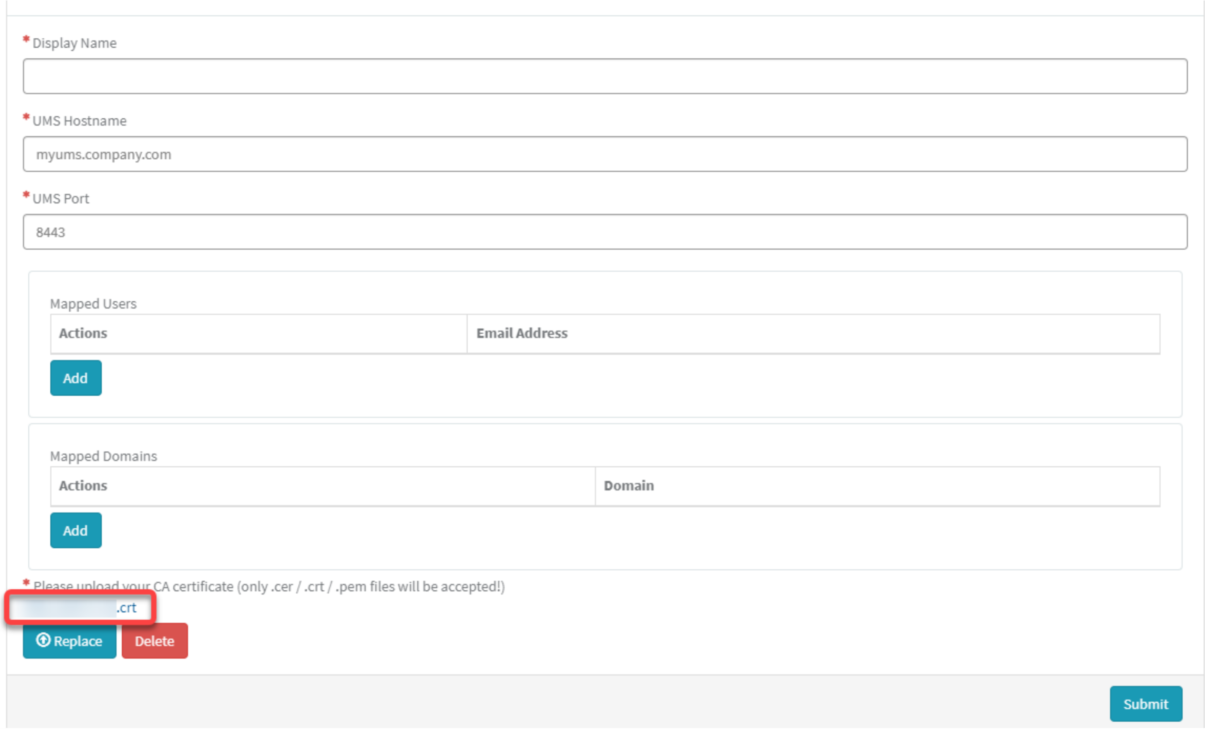
Actions	Domain

Add

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

Required - Upload

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



* Display Name

* UMS Hostname

myums.company.com

* UMS Port

8443

Mapped Users

Actions	Email Address

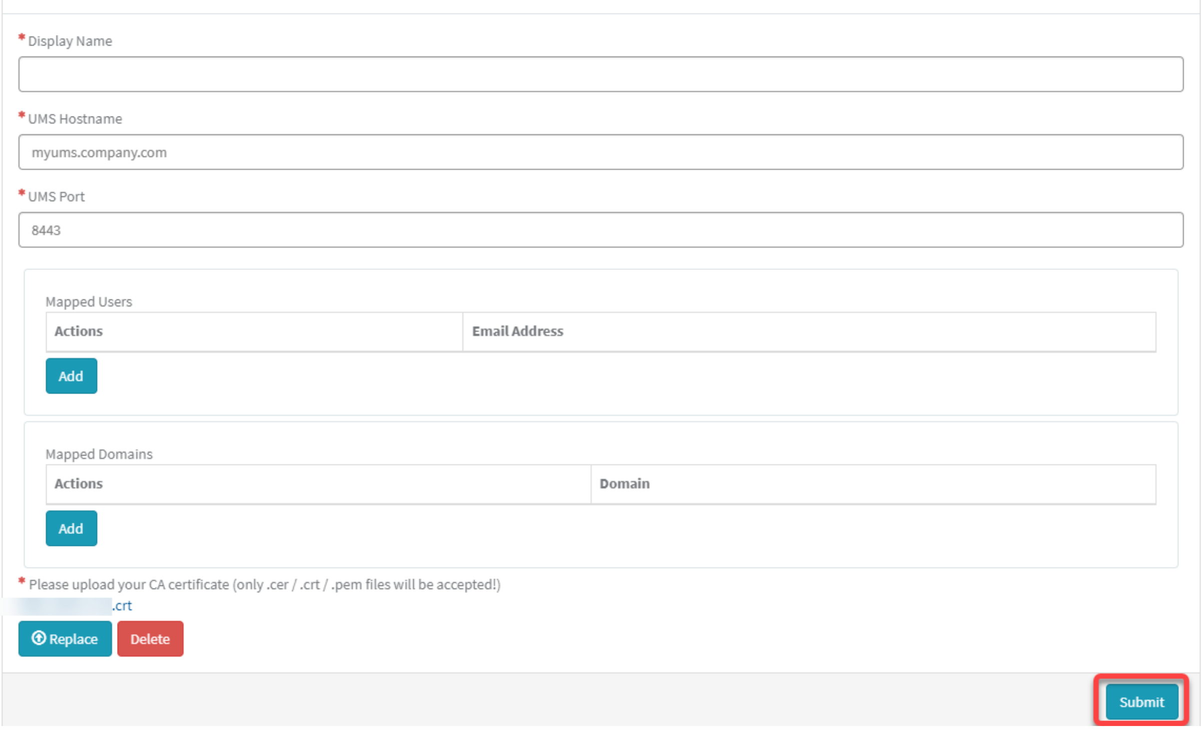
Mapped Domains

Actions	Domain

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

[redacted].crt

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



* Display Name

* UMS Hostname

myums.company.com

* UMS Port

8443

Mapped Users

Actions	Email Address

Mapped Domains

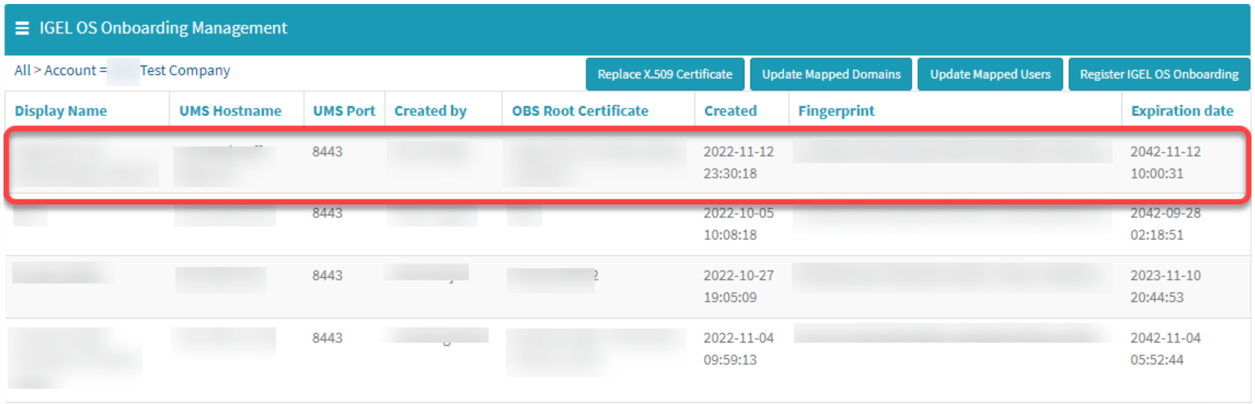
Actions	Domain

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

[redacted].crt

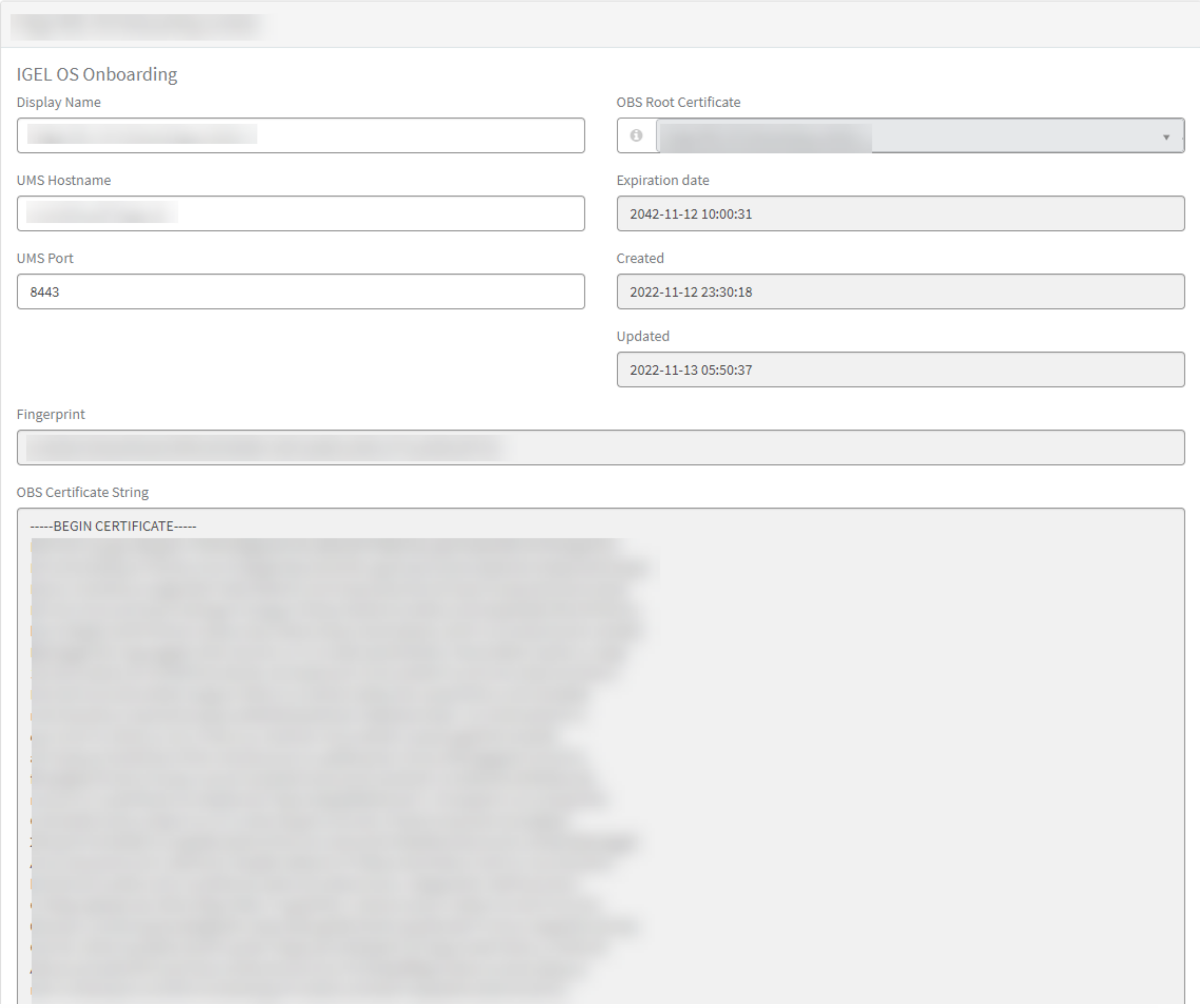
After a few seconds, the new data record is ready.

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


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

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

The details are displayed.



[redacted]

IGEL OS Onboarding

Display Name	[redacted]
OBS Root Certificate	[redacted]
UMS Hostname	[redacted]
Expiration date	2042-11-12 10:00:31
UMS Port	8443
Created	2022-11-12 23:30:18
Updated	2022-11-13 05:50:37
Fingerprint	[redacted]

OBS Certificate String

```
-----BEGIN CERTIFICATE-----
```

[redacted]

Authentication

Configuring Microsoft Entra ID as an Identity Provider

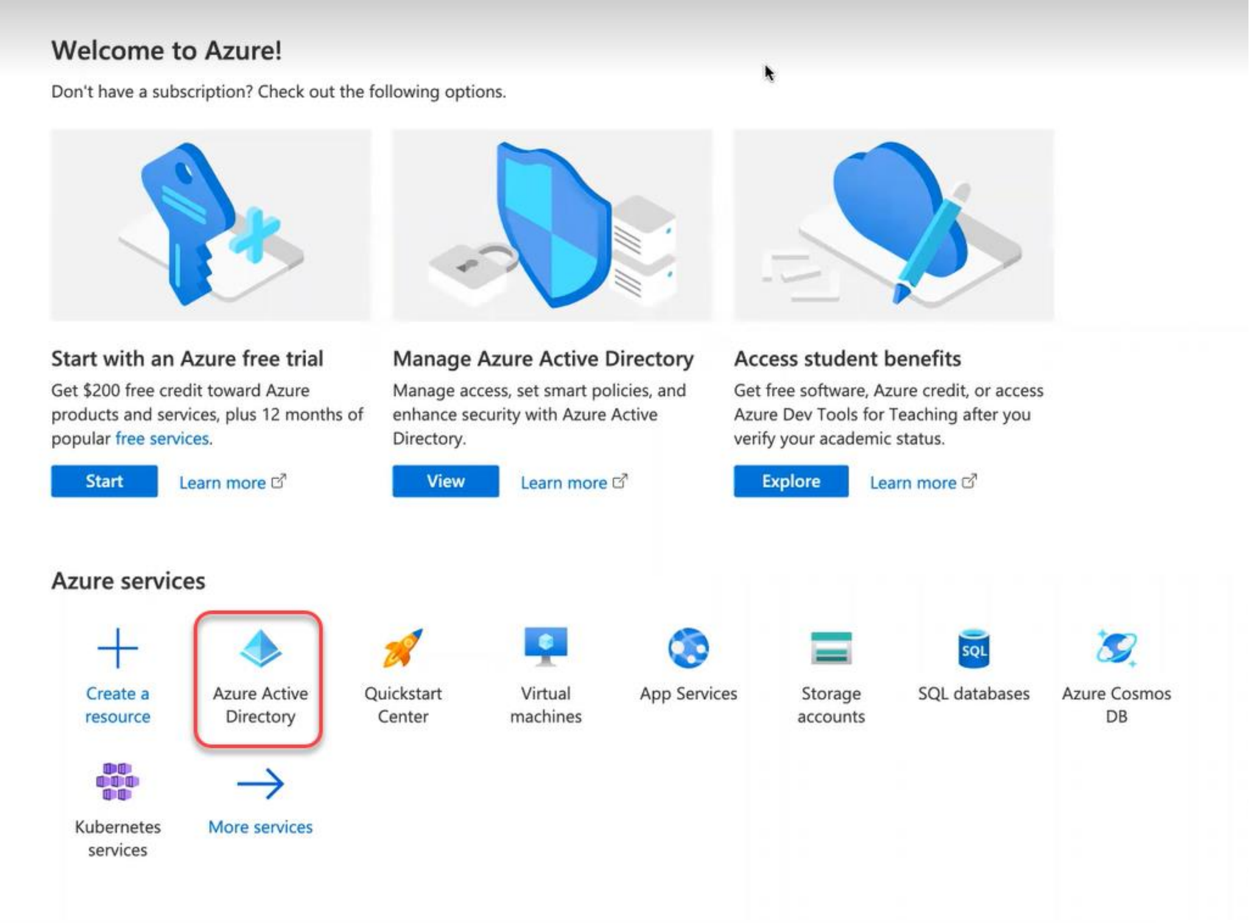
To configure Microsoft Entra ID as the identity provider, you need to do the following:

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

Creating a Web Application That Will Serve as Identity Provider

Azure Portal: https://portal.azure.com/#home

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



Welcome to Azure!

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

Start with an Azure free trial

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

Manage Azure Active Directory

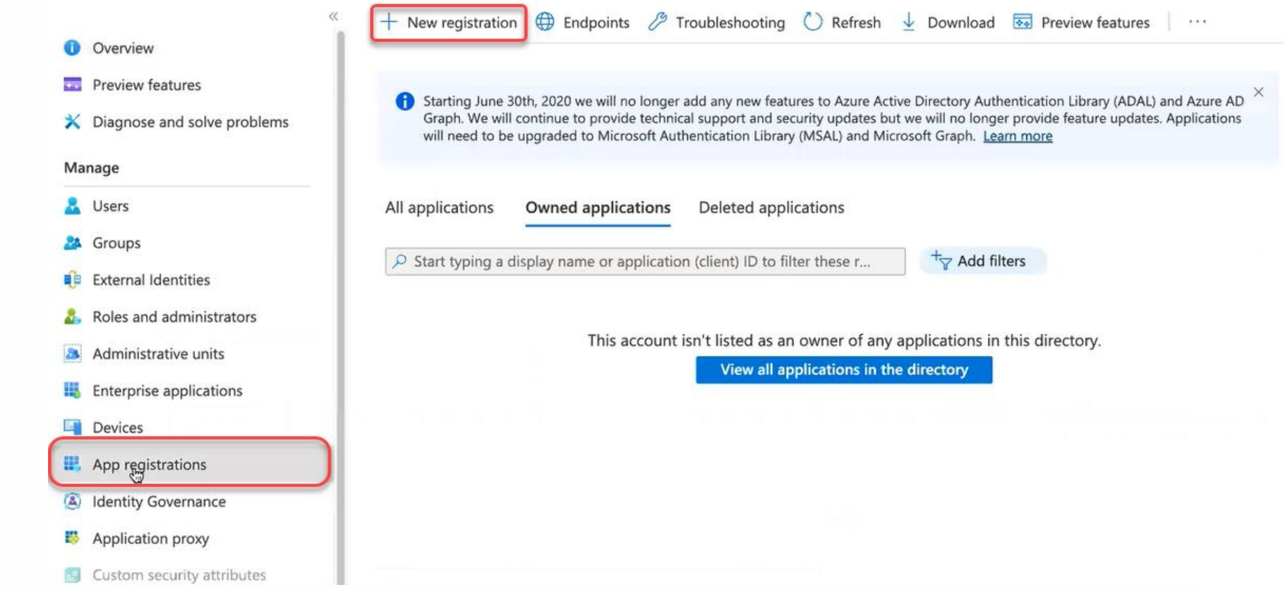
Manage access, set smart policies, and enhance security with Azure Active Directory.

Access student benefits

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

Azure services

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

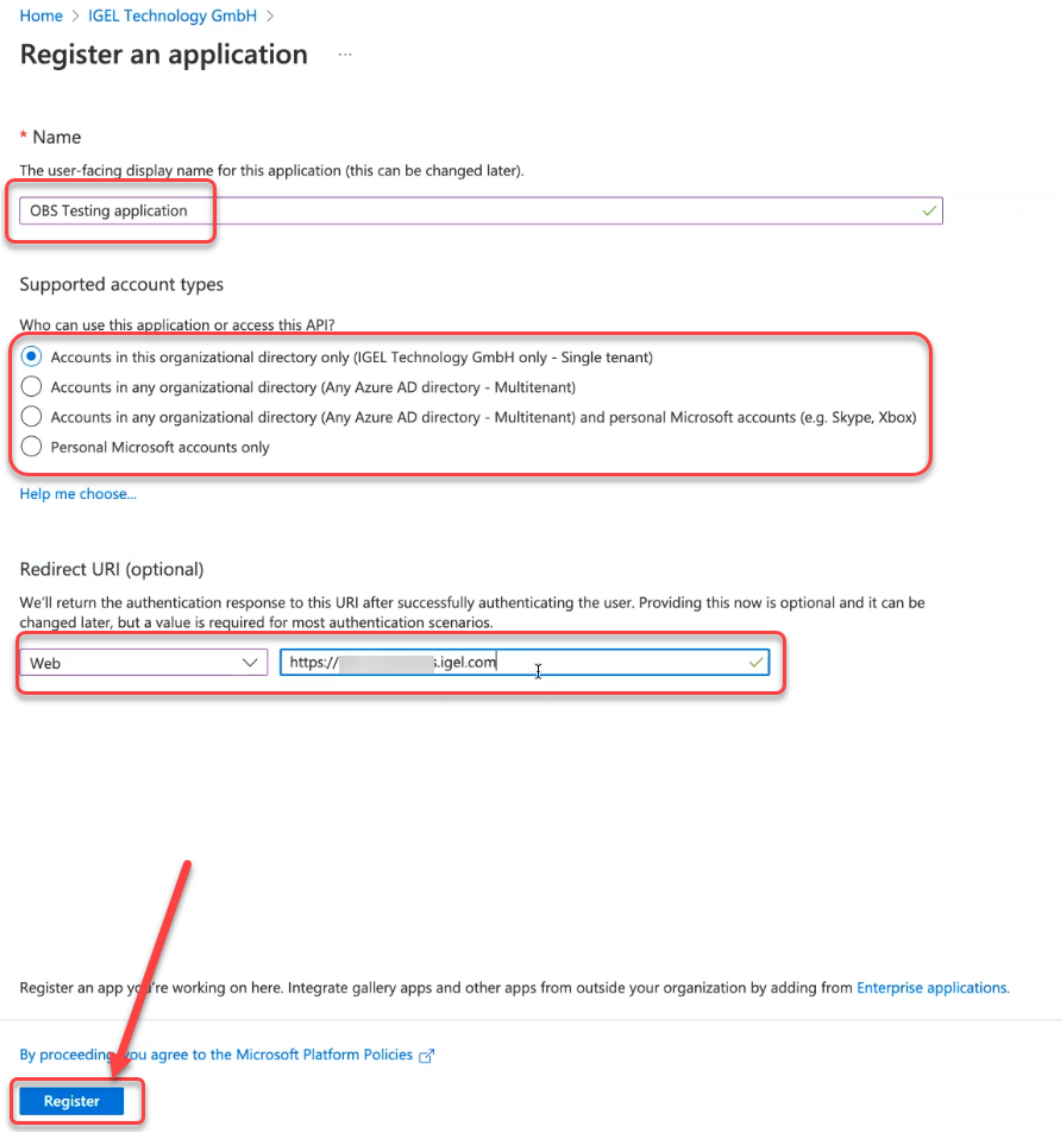


Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft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

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

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

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



Home > IGEL Technology GmbH >

Register an application ...

* Name

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

OBS Testing application

Supported account types

Who can use this application or access this API?

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

Help me choose...

Redirect URI (optional)

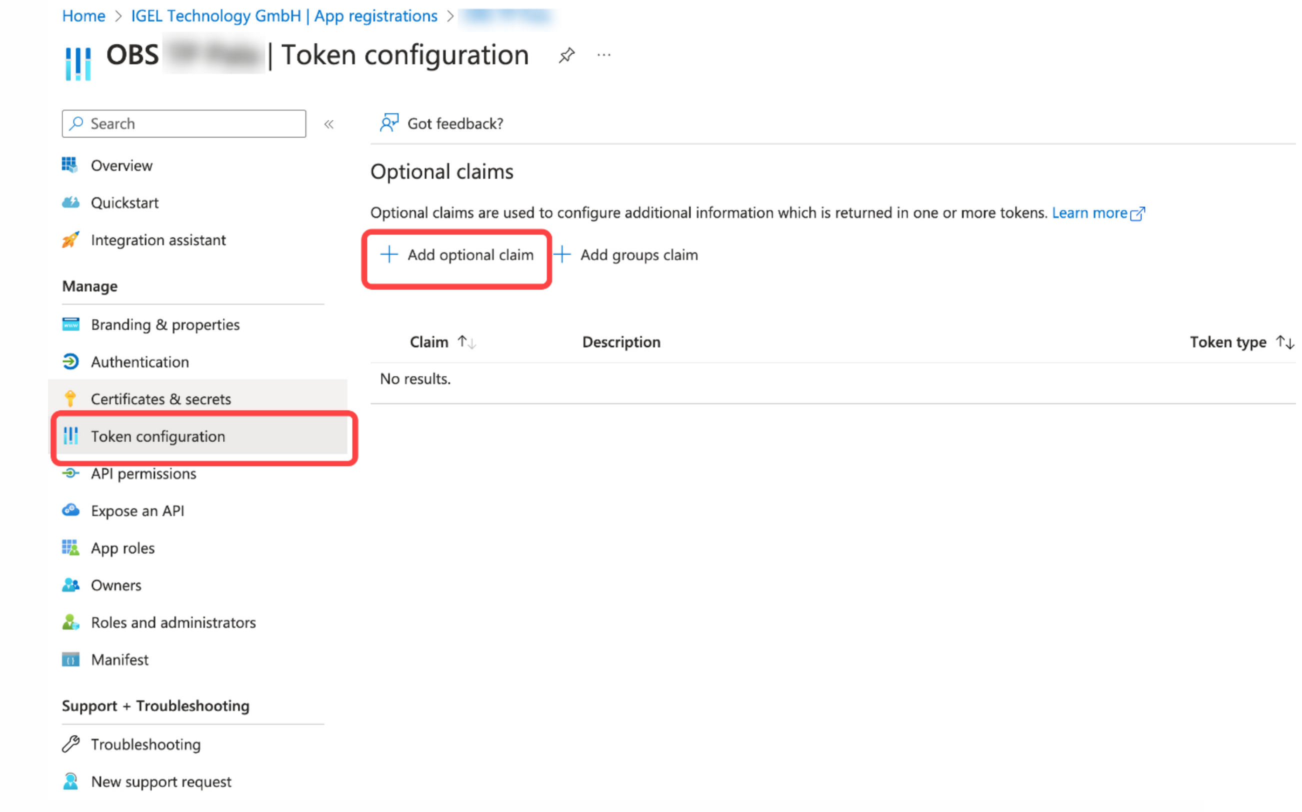
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ˅ https://[redacted].igel.com

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

By proceeding, you agree to the Microsoft Platform Policies

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



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

OBS [redacted] | Token configuration

Optional claims

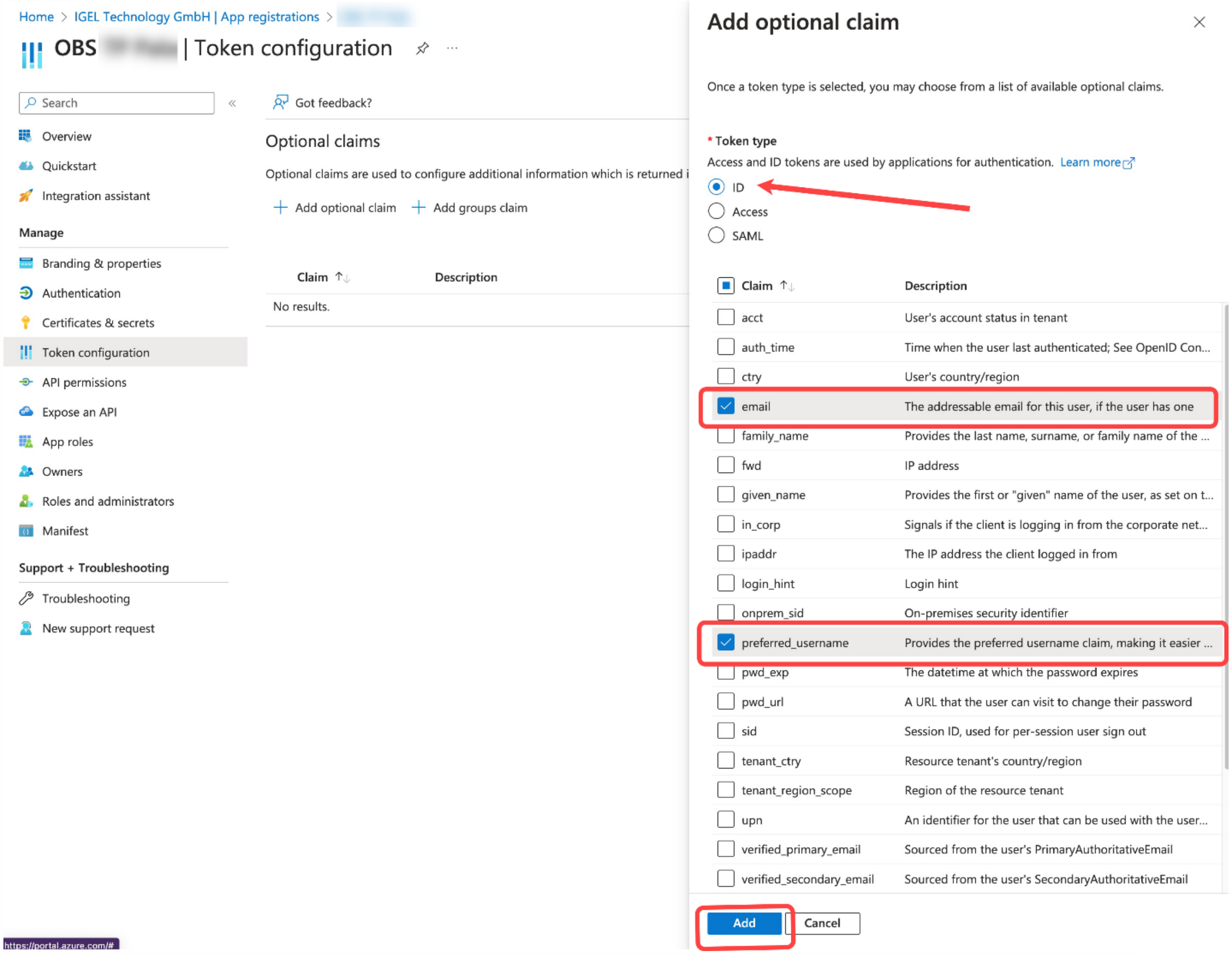
Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

Claim	Description	Token type
No results.		

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

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

6. Click **Add**.



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

OBS [redacted] | Token configuration

Optional claims

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

+ Add optional claim + Add groups claim

Claim	Description
No results.	

Add optional claim

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

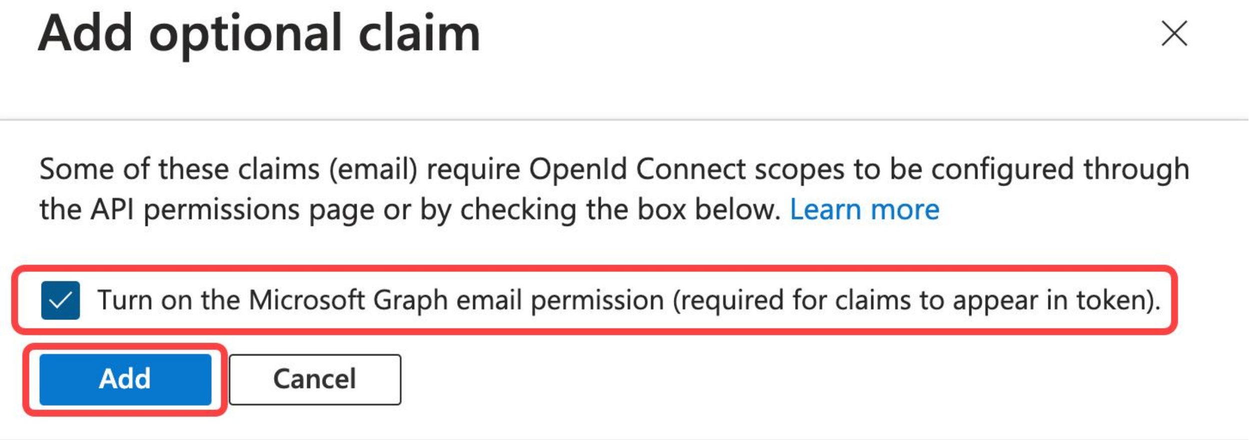
* Token type

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

● ID
○ Access
○ SAML

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

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

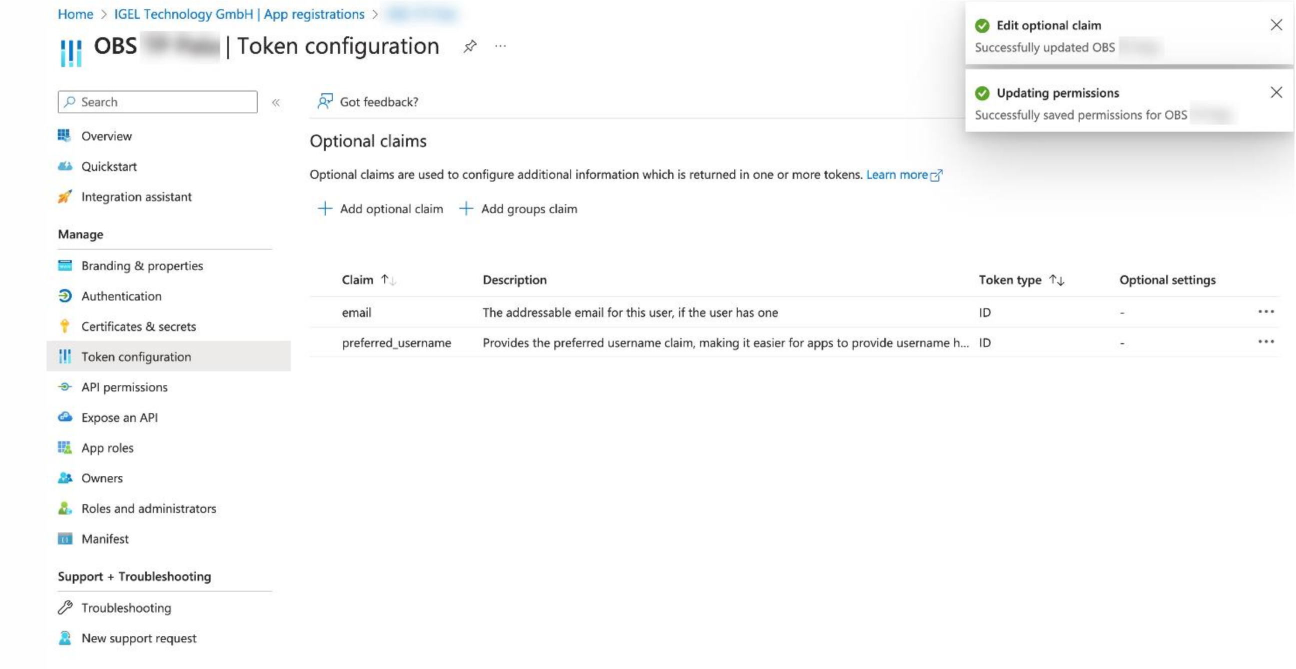


Add optional claim

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

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

The token configuration is completed:



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

OBS [redacted] | Token configuration

Optional claims

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

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

Edit optional claim
Successfully updated OBS [redacted]

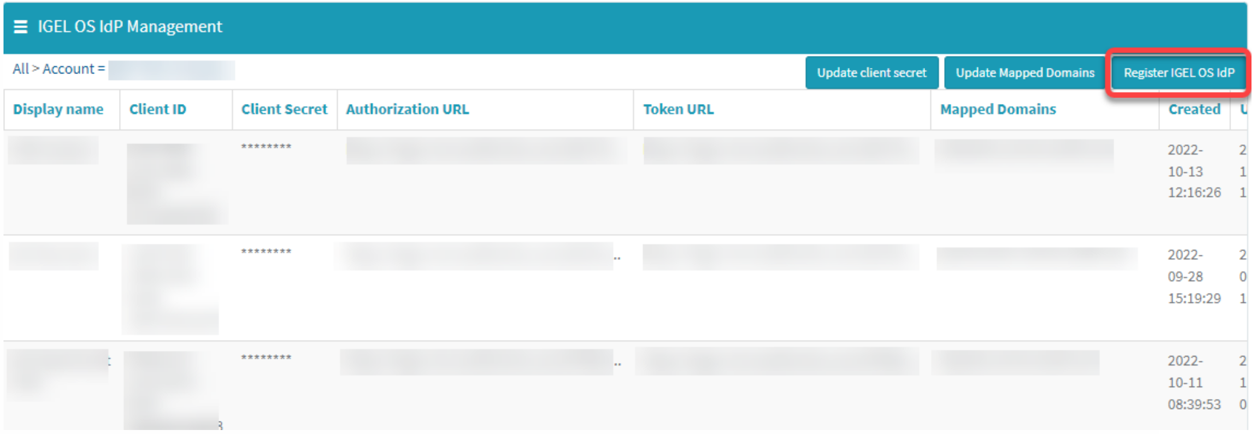
Updating permissions
Successfully saved permissions for OBS [redacted]

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

Registering our Entra App in the IGEL Customer Portal

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

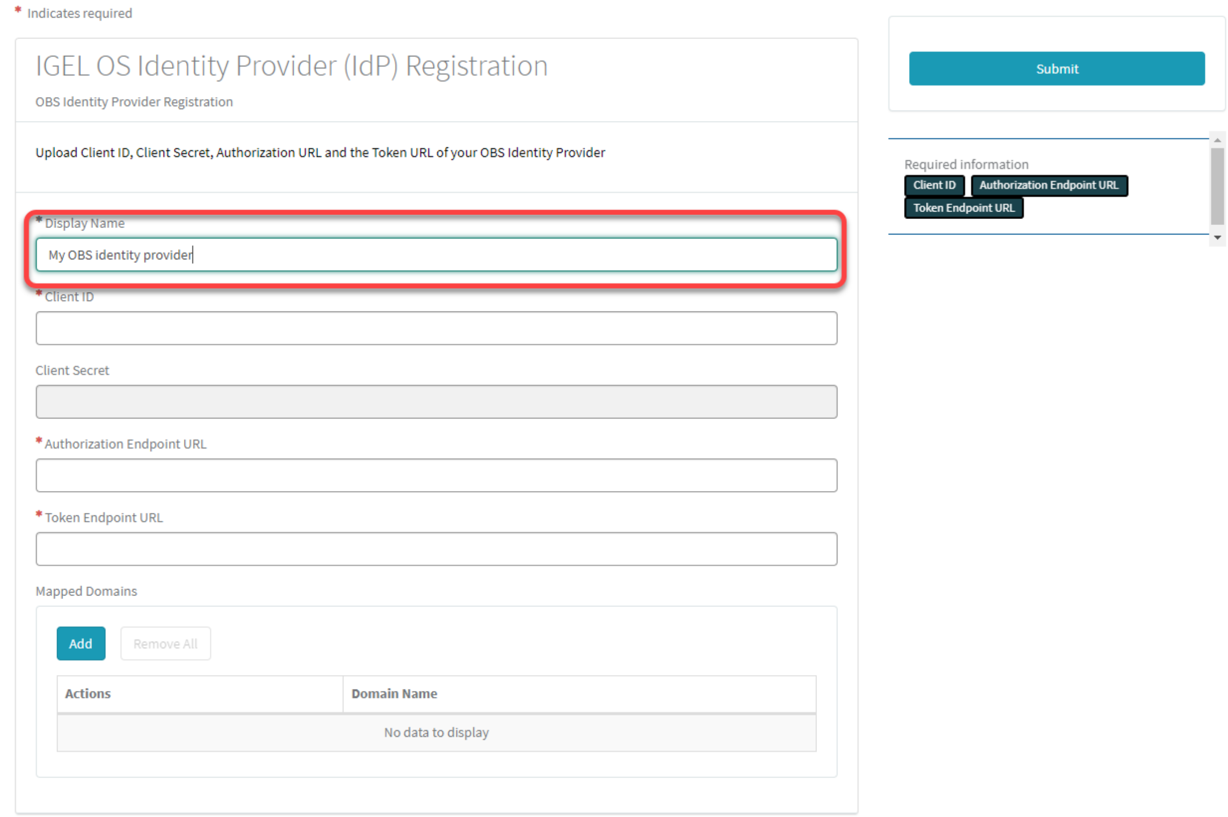
2. Click **Register IGEL OS IdP**.



All > Account = [redacted]

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

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



* Indicates required

IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name: My OBS identity provider

* Client ID

Client Secret

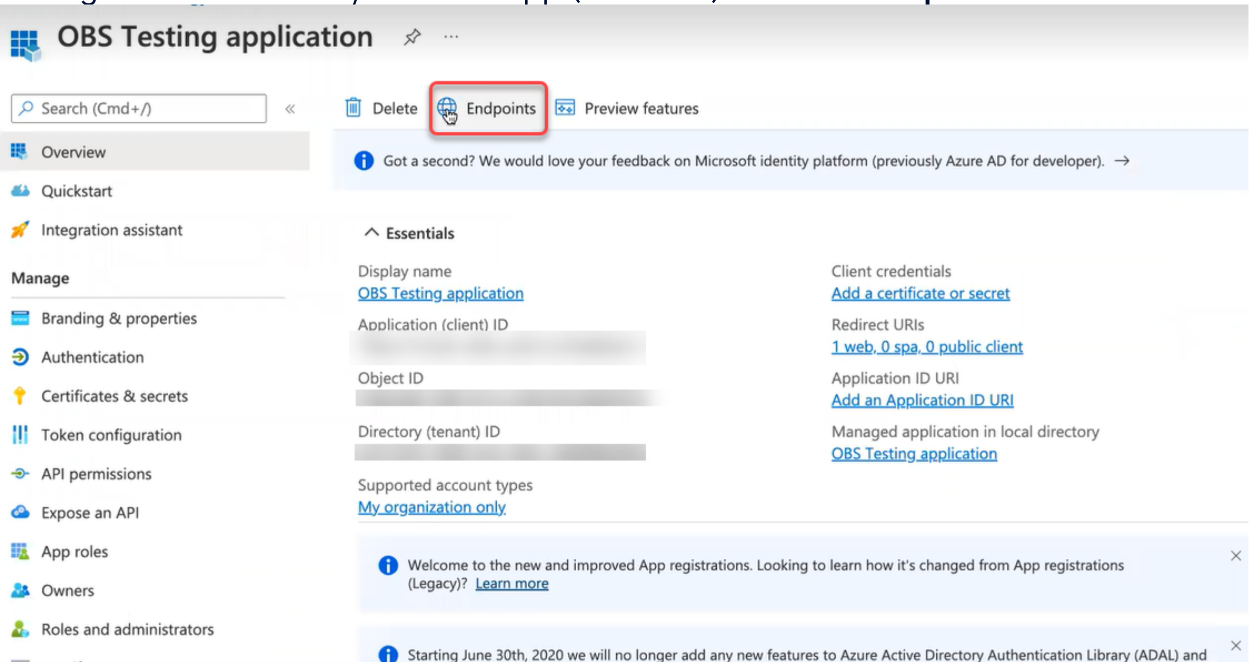
* Authorization Endpoint URL

* Token Endpoint URL

Mapped Domains

Actions	Domain Name
No data to display	

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



OBS Testing application

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

Essentials

Display name: OBS Testing application

Application (client) ID: [redacted]

Object ID: [redacted]

Directory (tenant) ID: [redacted]

Supported account types: My organization only

Client credentials: Add a certificate or secret

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

Application ID URI: Add an Application ID URI

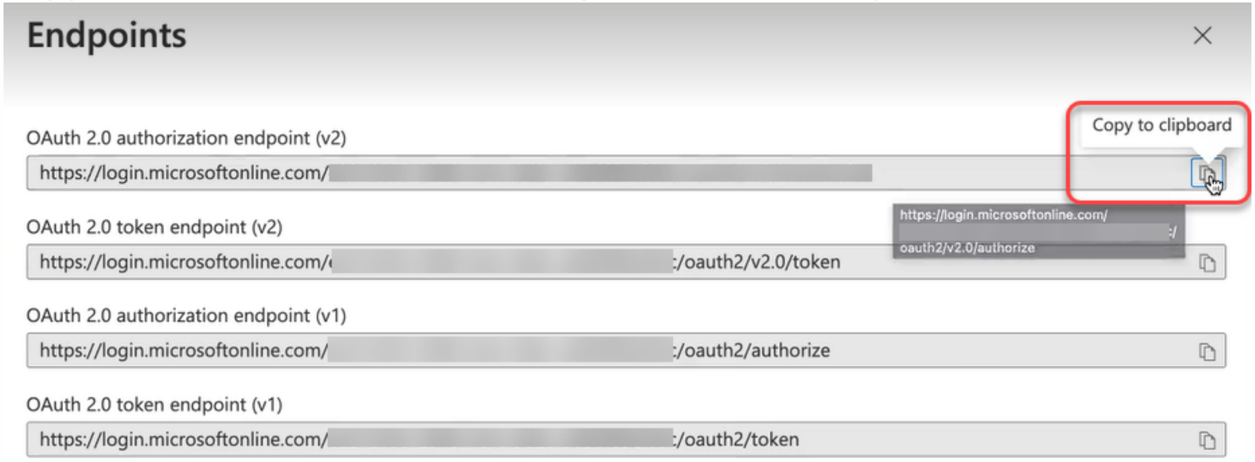
Managed application in local directory: OBS Testing application

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

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

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

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



Endpoints

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

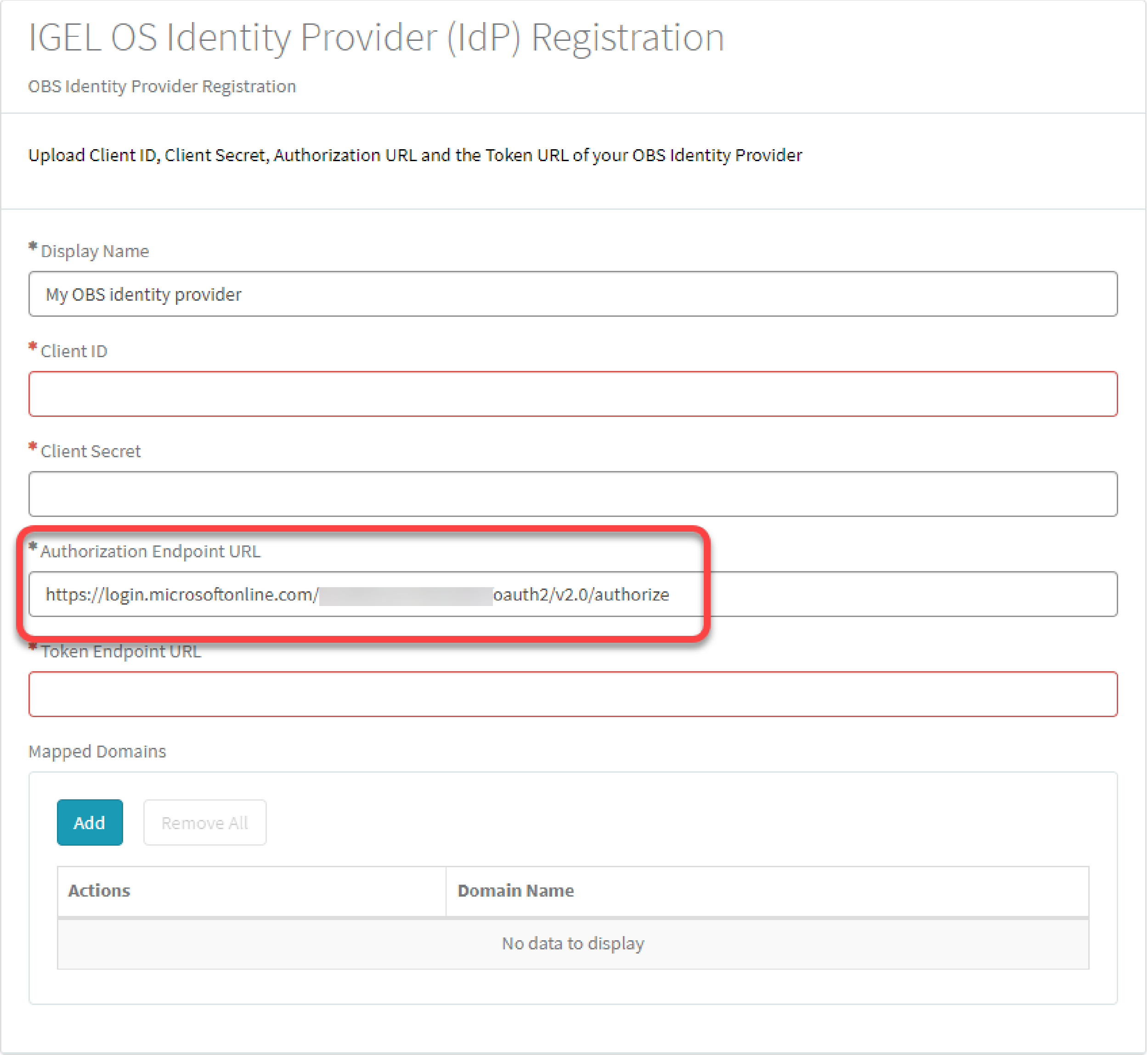
https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

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

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

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

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

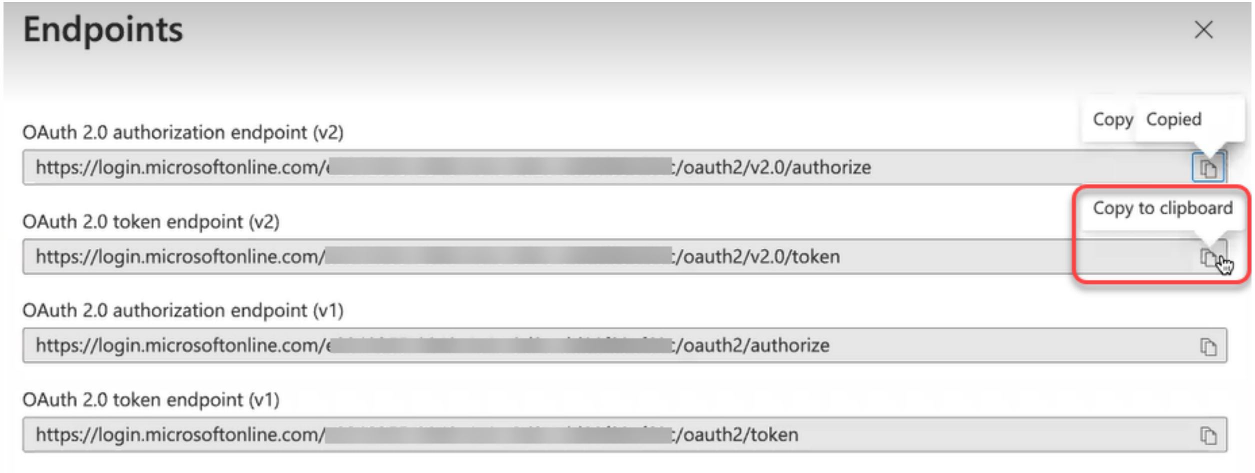
Upload Client ID, Client Secret, Authorization URL and the Token URL of your OBS Identity Provider

* Display Name	My OBS identity provider
* Client ID	
* Client Secret	
* Authorization Endpoint URL	https://login.microsoftonline.com/[redacted]oauth2/v2.0/authorize
* Token Endpoint URL	

Mapped Domains

Actions	Domain Name
No data to display	

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



Endpoints

OAuth 2.0 authorization endpoint (v2)

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

OAuth 2.0 token endpoint (v2)

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

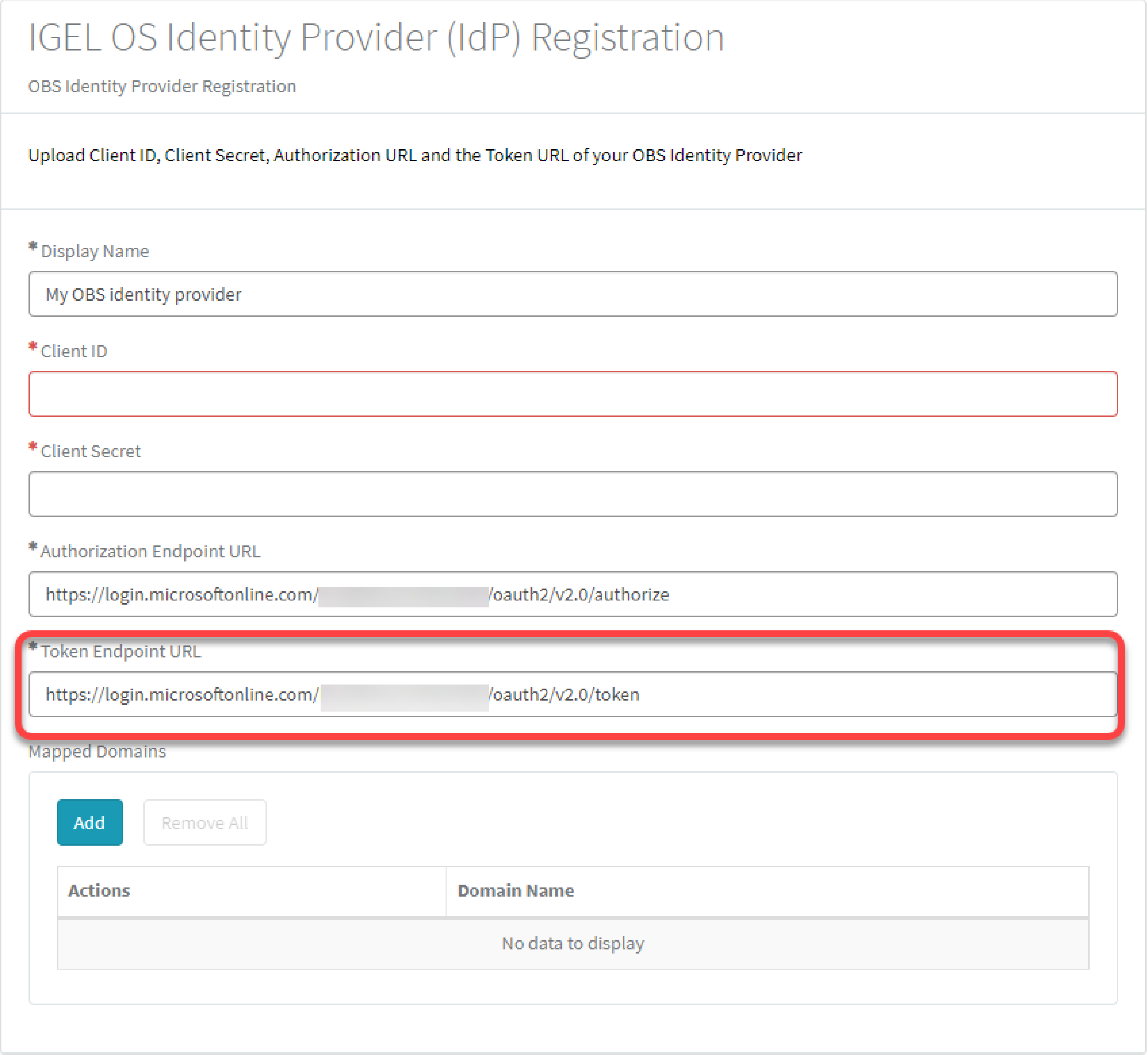
OAuth 2.0 authorization endpoint (v1)

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

OAuth 2.0 token endpoint (v1)

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

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name

My OBS identity provider

* Client ID

* Client Secret

* Authorization Endpoint URL

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

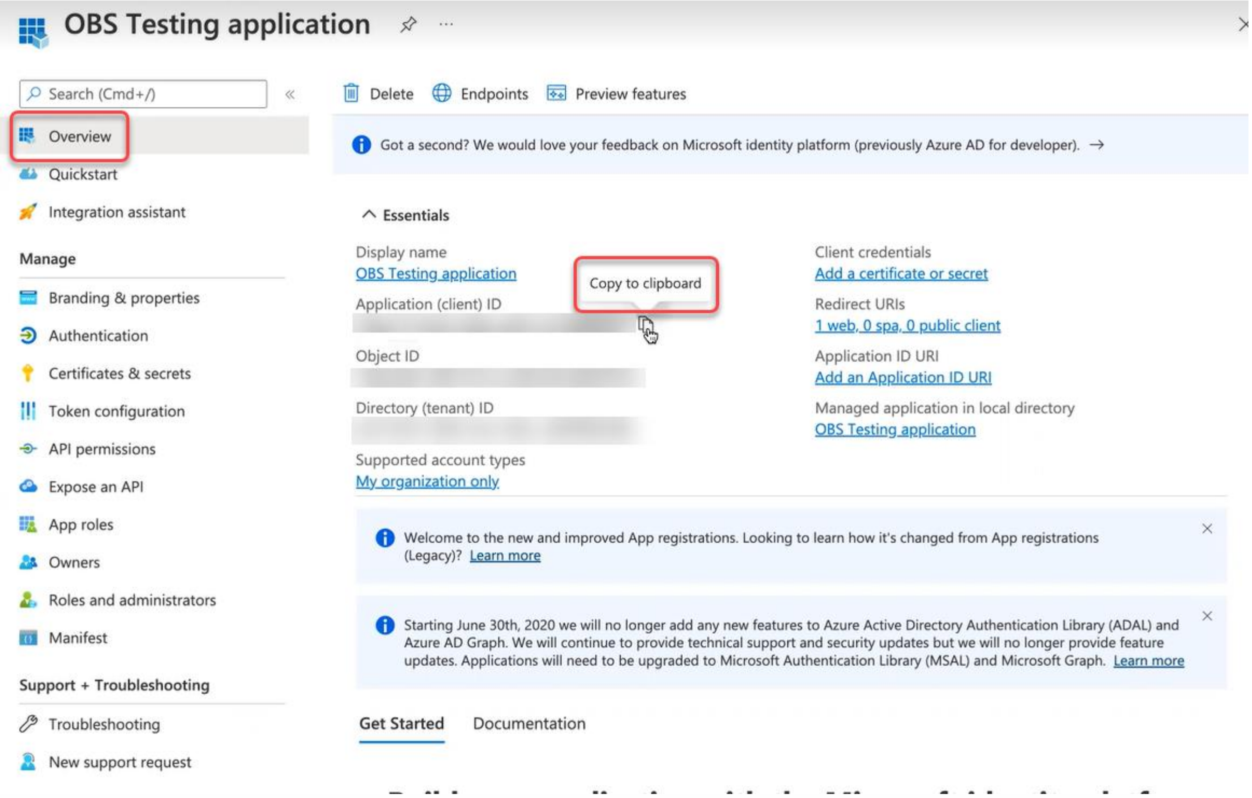
* Token Endpoint URL

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

Mapped Domains

Actions	Domain Name
No data to display	

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



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

Display name: OBS Testing application

Application (client) ID: [redacted]

Object ID: [redacted]

Directory (tenant) ID: [redacted]

Supported account types: My organization only

Client credentials: Add a certificate or secret

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

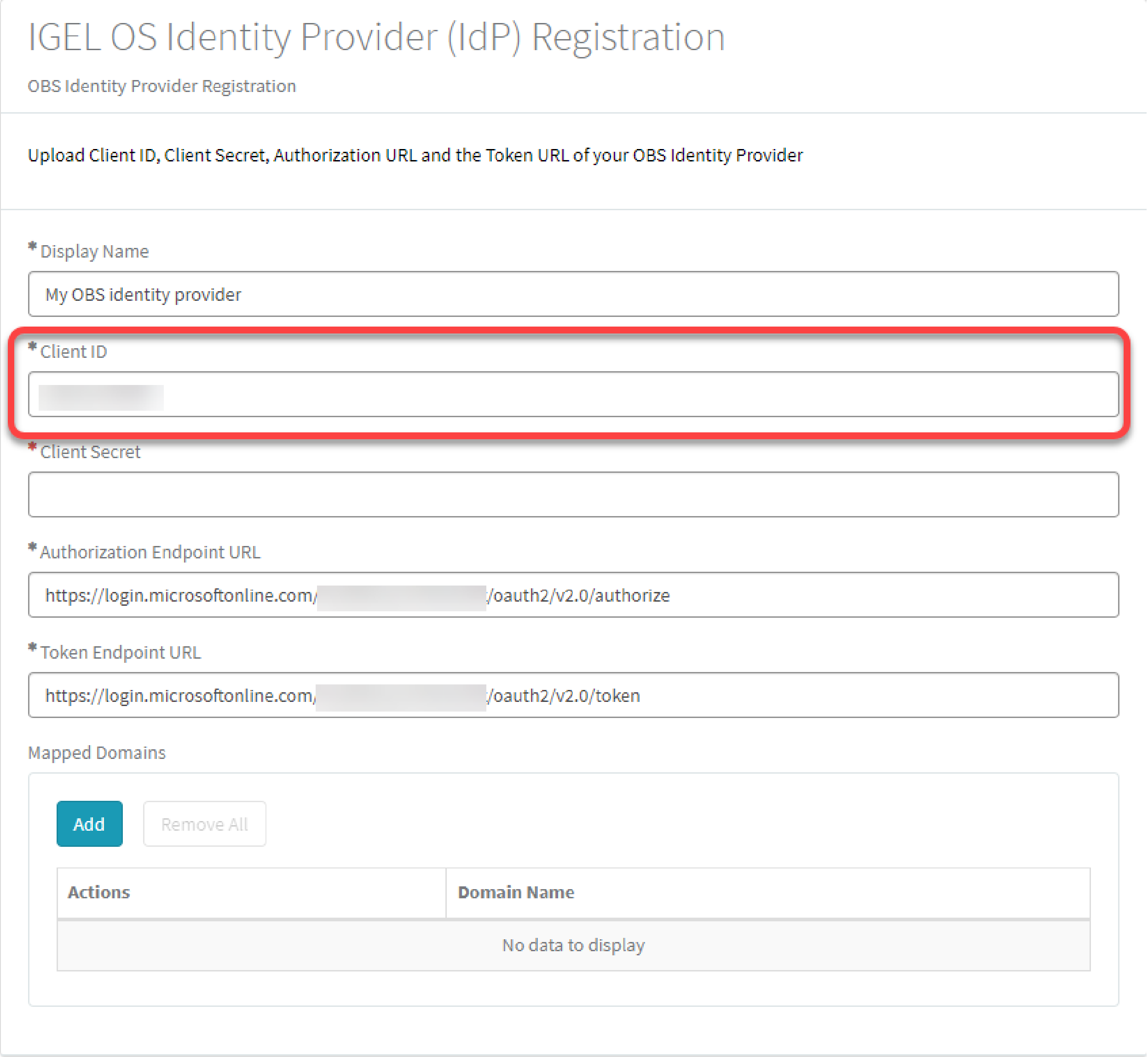
Application ID URI: Add an Application ID URI

Managed application in local directory: OBS Testing application

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

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

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name: My OBS identity provider

* Client ID: [redacted]

* Client Secret:

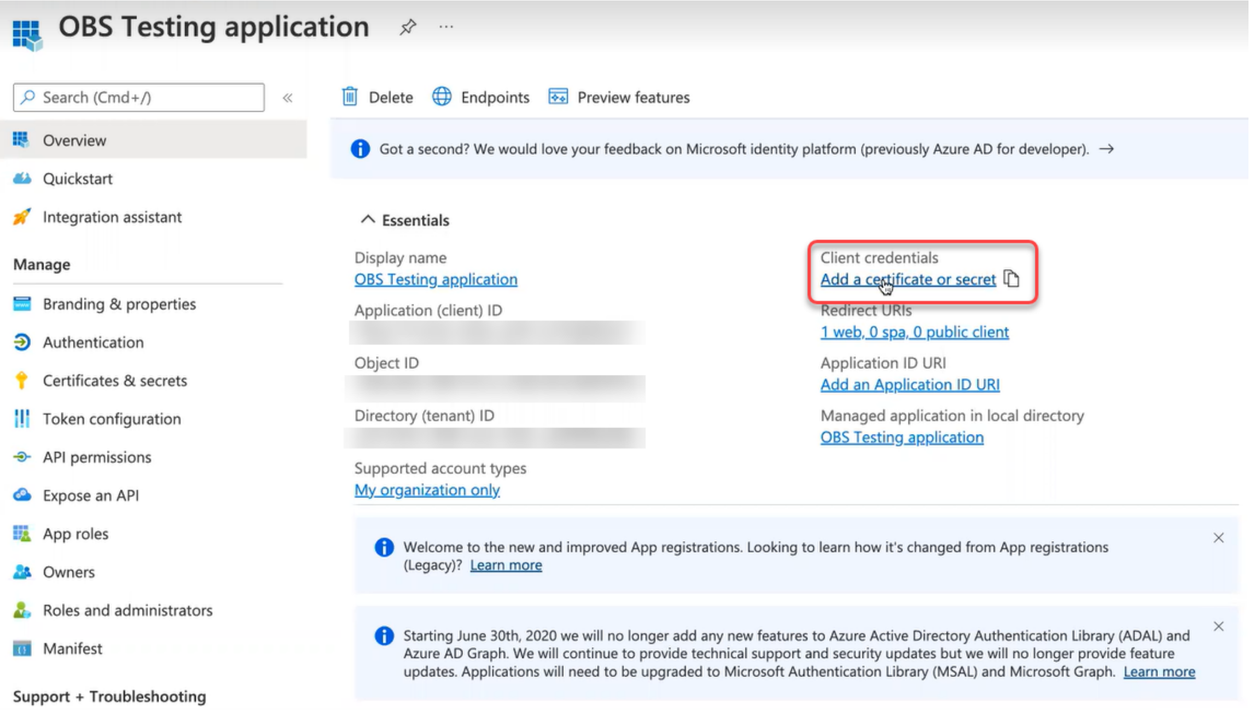
* Authorization Endpoint URL: https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

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

Mapped Domains

Actions	Domain Name
No data to display	

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



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

Display name
OBS Testing application

Application (client) ID
[redacted]

Object ID
[redacted]

Directory (tenant) ID
[redacted]

Supported account types
My organization only

Client credentials
Add a certificate or secret

Redirect URIs
1 web, 0 spa, 0 public client

Application ID URI
Add an Application ID URI

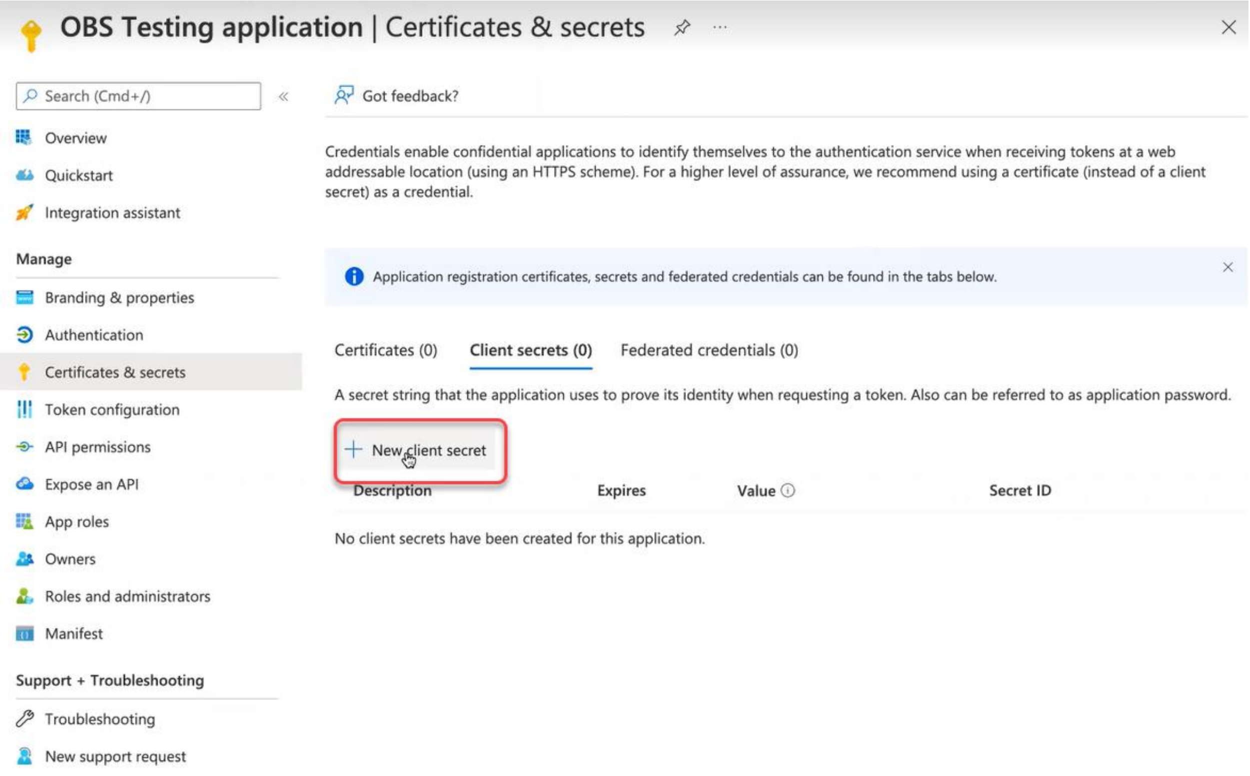
Managed application in local directory
OBS Testing application

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

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

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

12. Click **New client secret**.



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

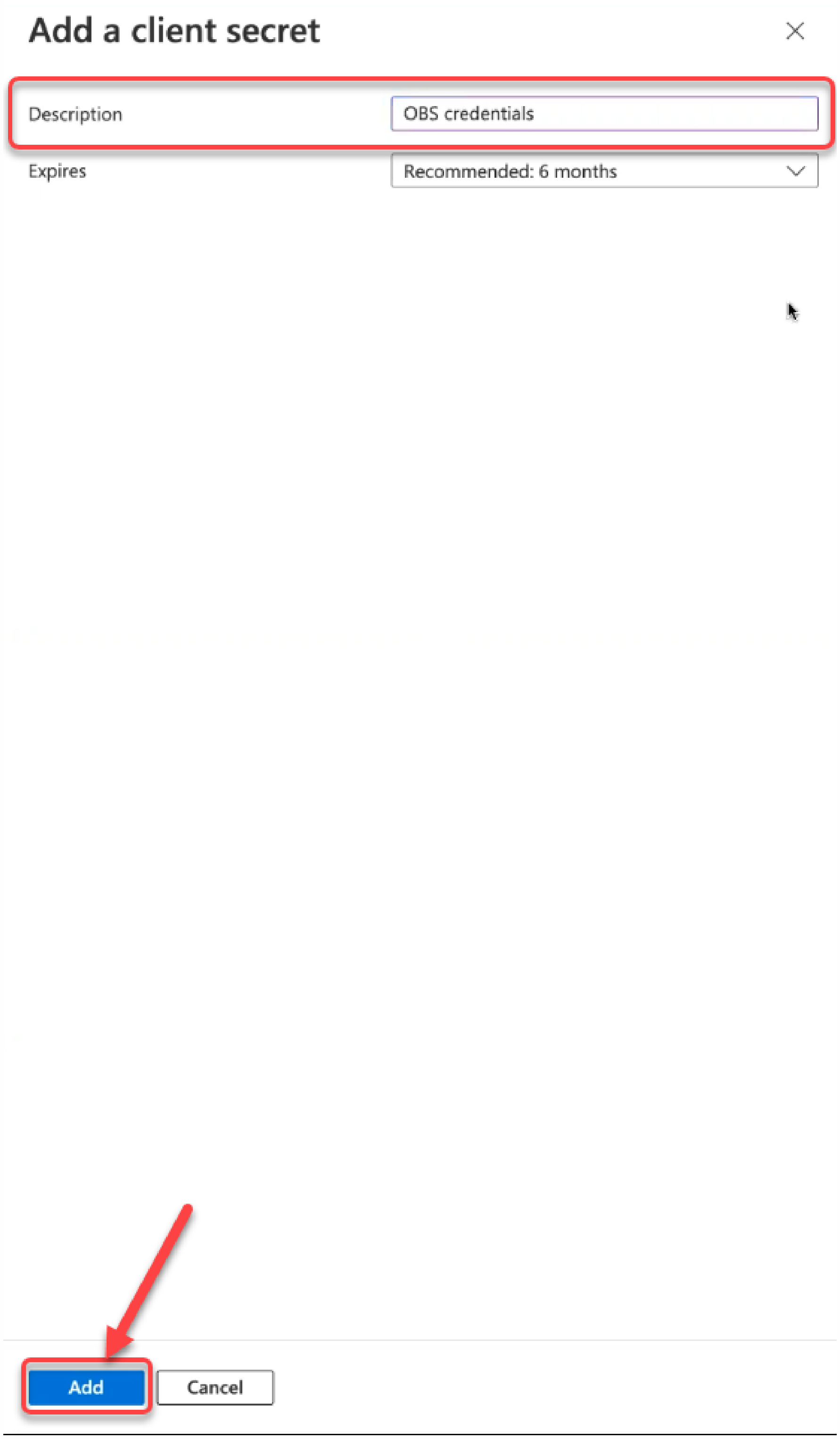
Application registration certificates, secrets and federated credentials can be found in the tabs below.

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

No client secrets have been created for this application.

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

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

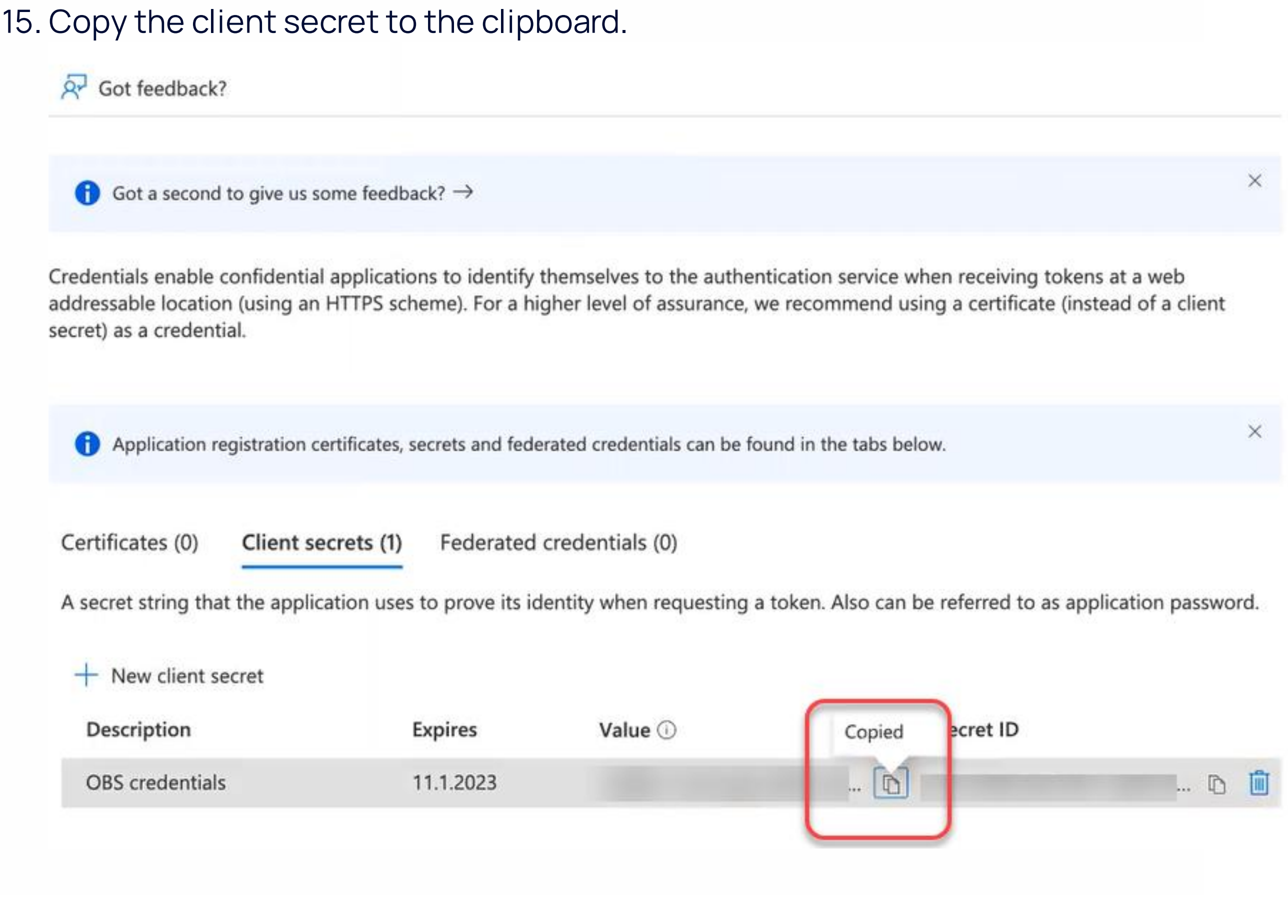


Add a client secret

Description: OBS credentials

Expires: Recommended: 6 months

15. Copy the client secret to the clipboard.



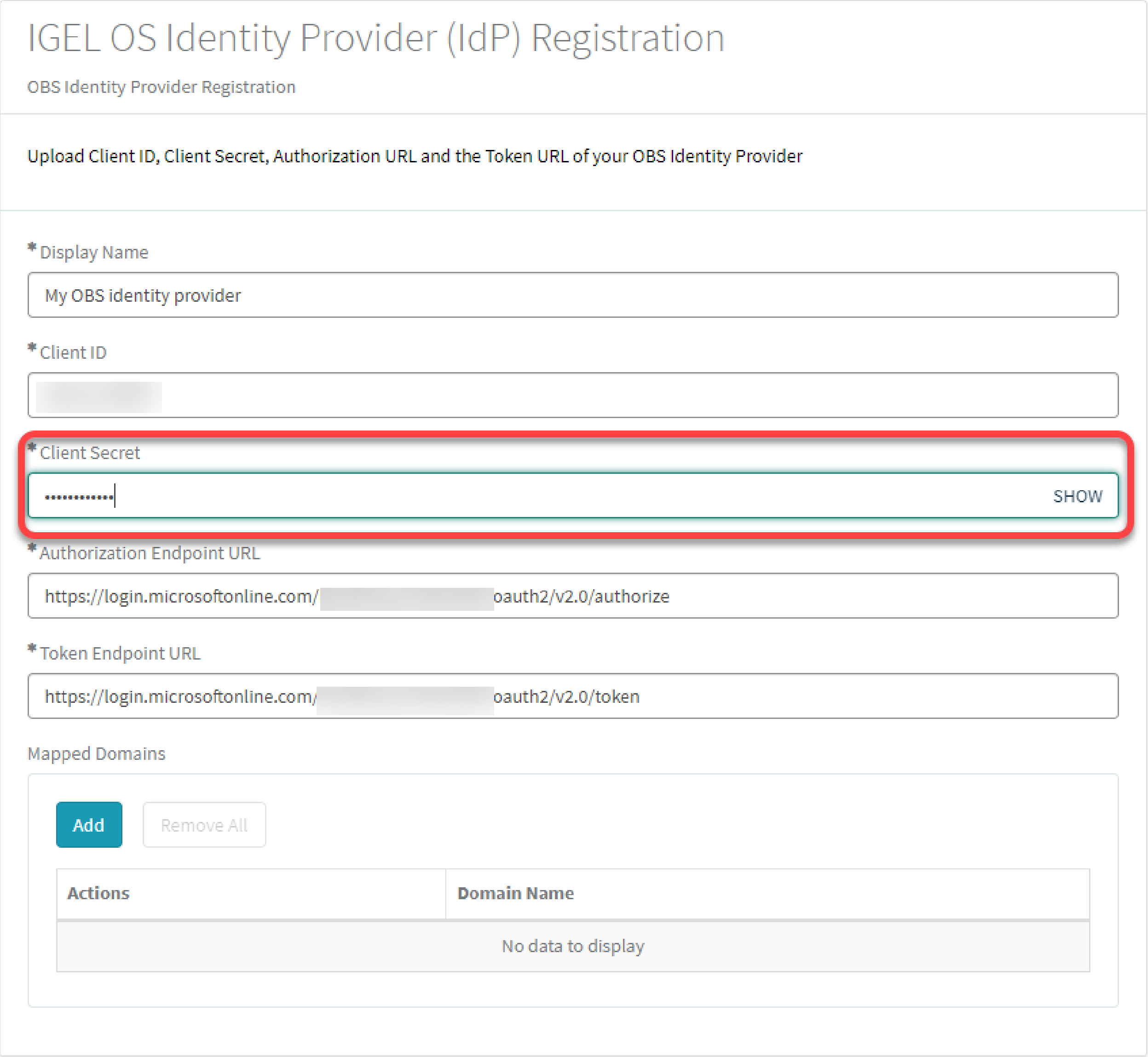
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

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

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

Description	Expires	Value ⓘ	ecret ID
OBS credentials	11.1.2023	...	...

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



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

*Display Name

My OBS identity provider

*Client ID

[redacted]

*Client Secret

•••••••••••• SHOW

*Authorization Endpoint URL

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

*Token Endpoint URL

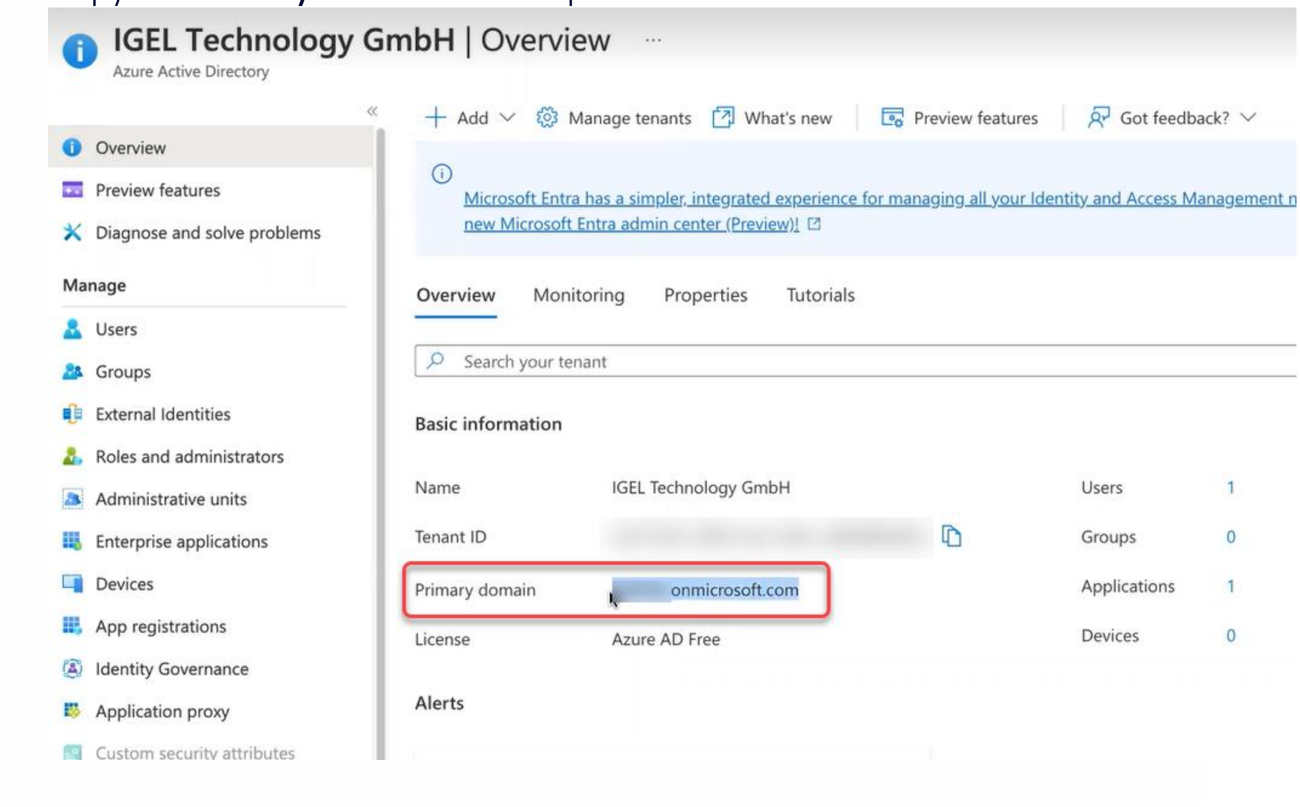
https://login.microsoftonline.com/[redacted]oauth2/v2.0/token

Mapped Domains

Actions	Domain Name
No data to display	

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

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



IGEL Technology GmbH | Overview

Azure Active Directory

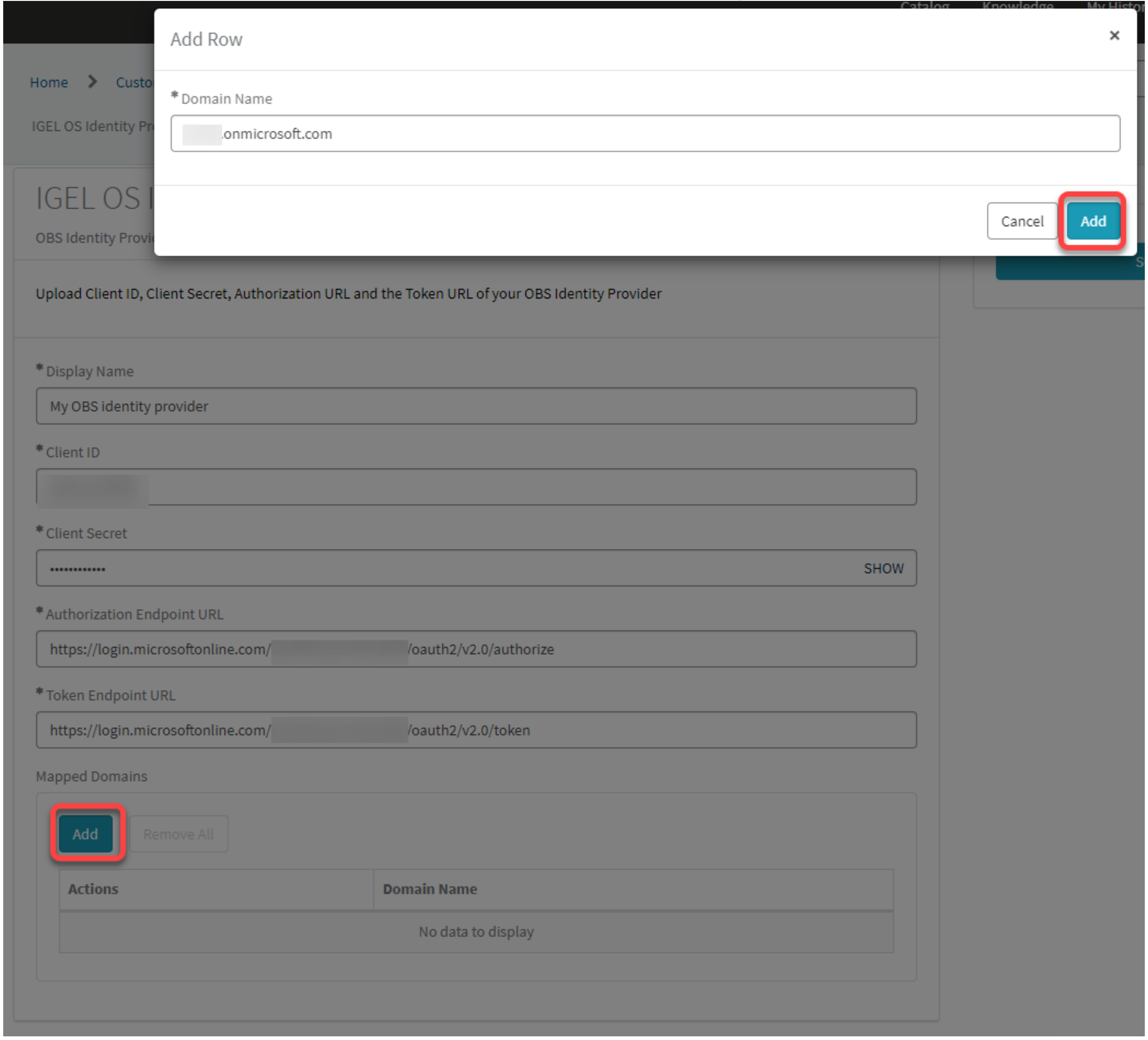
Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management n new Microsoft Entra admin center (Preview)!

Basic information

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

Alerts

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



Add Row

* Domain Name

[redacted].onmicrosoft.com

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

* Display Name

My OBS identity provider

* Client ID

[redacted]

* Client Secret

••••••••••••

* Authorization Endpoint URL

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

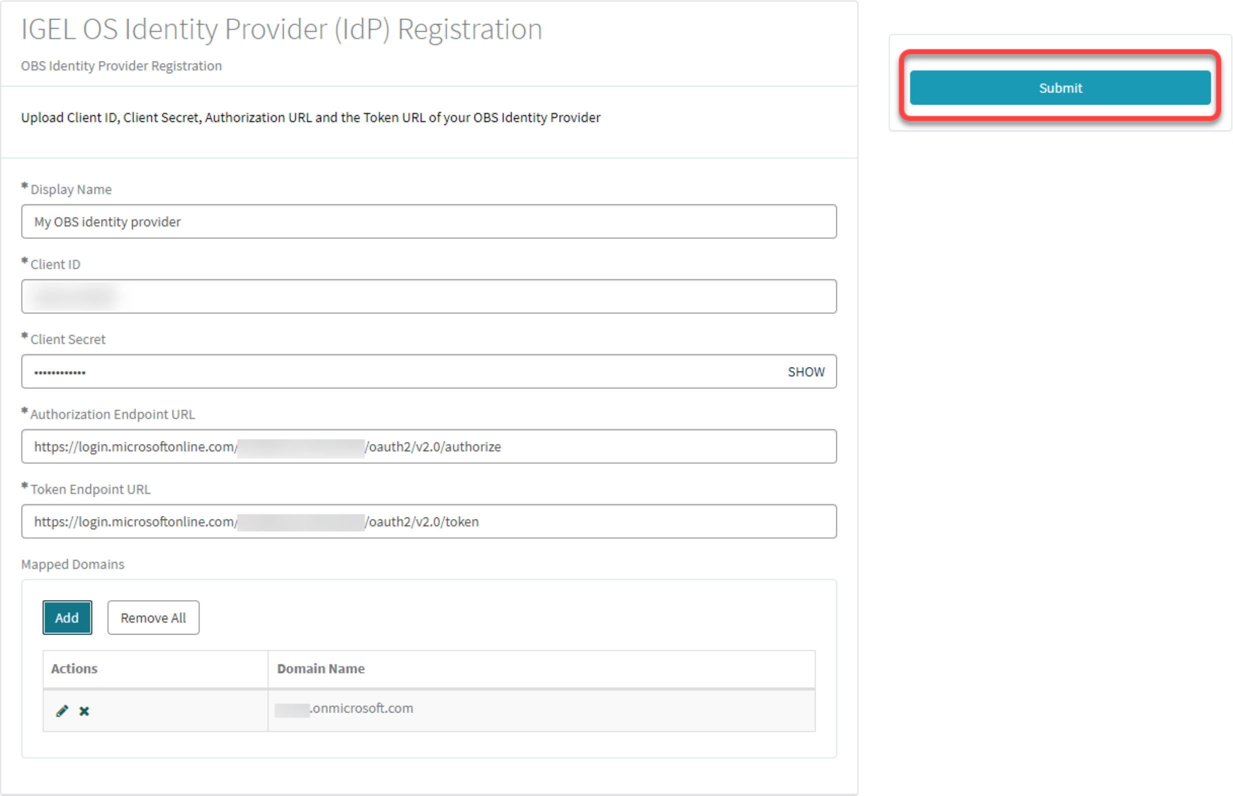
* Token Endpoint URL

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

Mapped Domains

Actions	Domain Name
No data to display	

20. Click **Submit**.



IGEL OS Identity Provider (IdP) Registration

OBS Identity Provider Registration

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

* Display Name: My OBS identity provider

* Client ID: [redacted]

* Client Secret: •••••••••••• SHOW

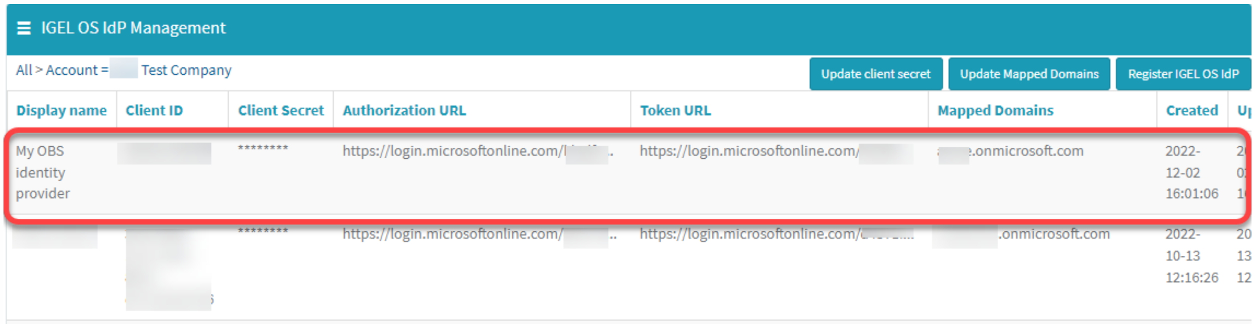
* Authorization Endpoint URL: https://login.microsoftonline.com/[redacted]/oauth2/v2.0/authorize

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

Mapped Domains

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

The data record is created.



☰ IGEL OS IdP Management

All > Account = [redacted] Test Company

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

EntraID is now configured as your identity provider, all we need to do is configure some profiles in UMS to install the IGEL AVD client and configure it to auto launch.

UMS Configuration

Connect UMS to the App Portal or Registering the UMS allows the UMS to authenticate to the IGEL Cloud Services and will allow the UMS (and devices if configured) to connect to and download IGEL and partner applications from the App portal. https://apps.igel.com

Registering the UMS

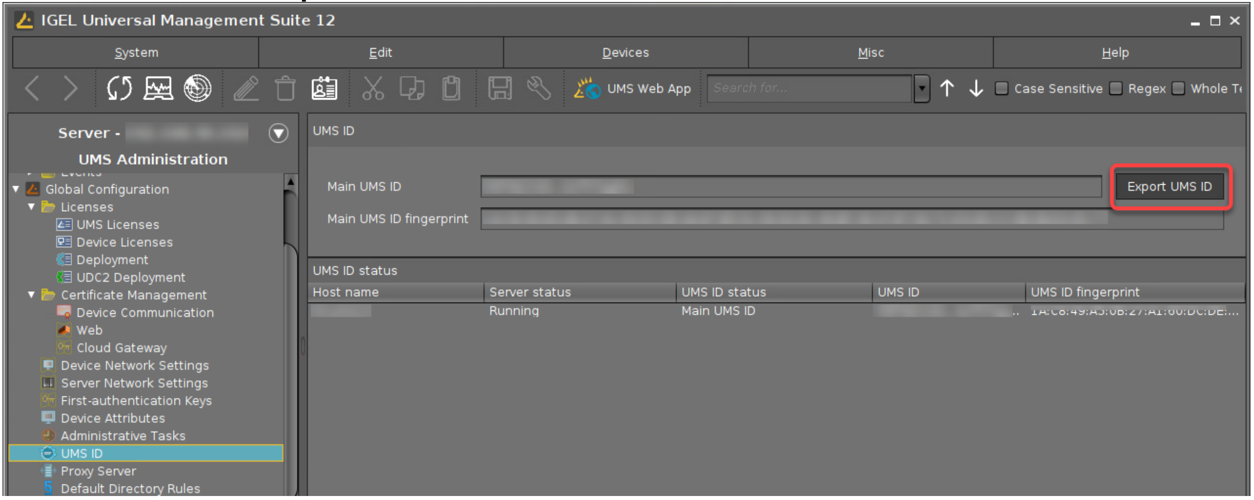
To authenticate your UMS to the IGEL Cloud Services, you must register your UMS. This involves uploading the UMS ID, which is essentially a certificate of your UMS, to the IGEL Customer Portal.

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

Exporting the UMS ID

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

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

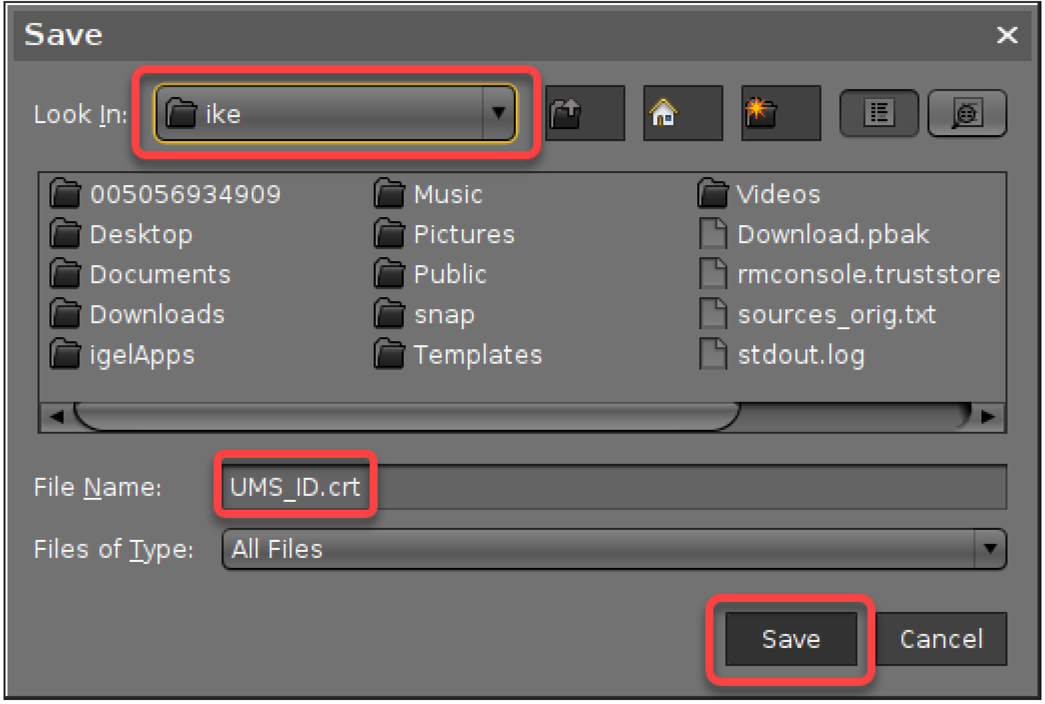


Main UMS ID: [redacted]

Main UMS ID fingerprint: [redacted]

Host name	Server status	UMS ID status	UMS ID	UMS ID fingerprint
[redacted]	Running	Main UMS ID	[redacted]	1A:C8:49:A5:0B:27:A1:60:DC:DE:...

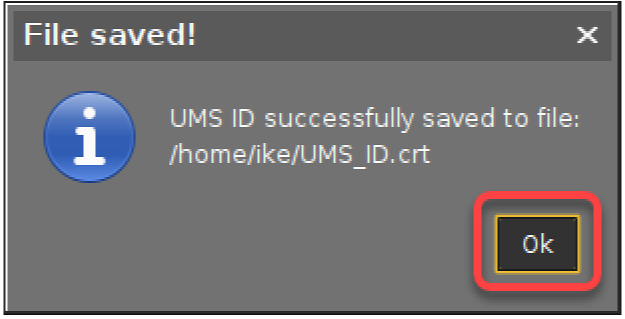
2. Select a storage location and click **Save**.



File Name: UMS_ID.crt

Files of Type: All Files

3. Close the confirmation dialog.



File saved!

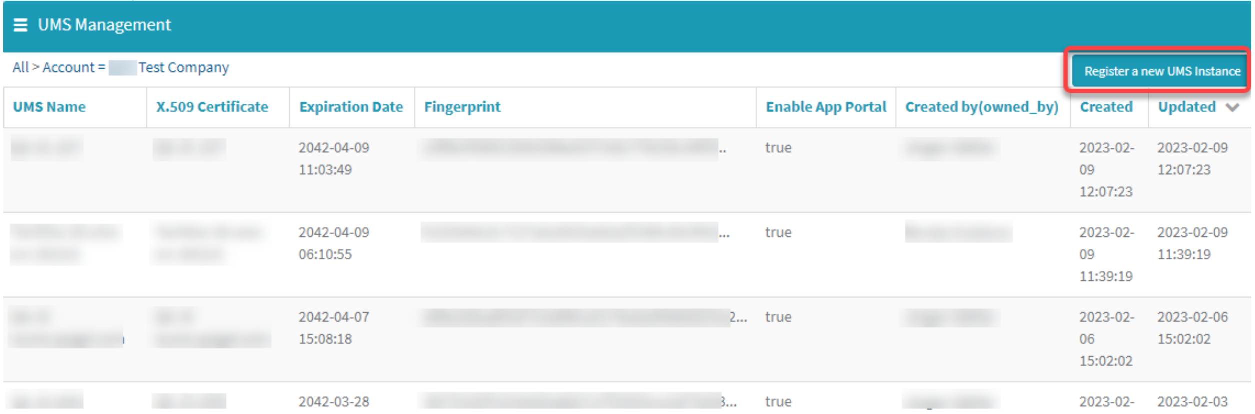
UMS ID successfully saved to file:
/home/ike/UMS_ID.crt

Registering the UMS

1. Open the IGEL Customer Portal in your browser and log in to your admin account.

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

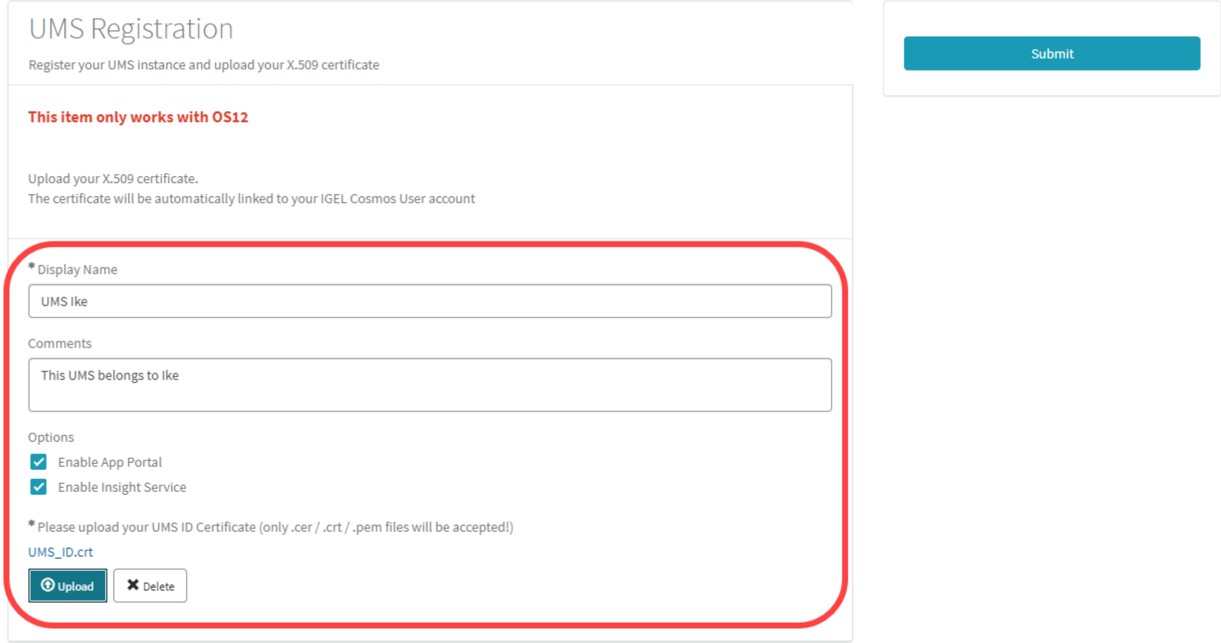
3. Click **Register a new UMS Instance**.



All > Account = [redacted] Test Company

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

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



UMS Registration

Register your UMS instance and upload your X.509 certificate

This item only works with OS12

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

* Display Name: UMS Ike

Comments: This UMS belongs to Ike

Options

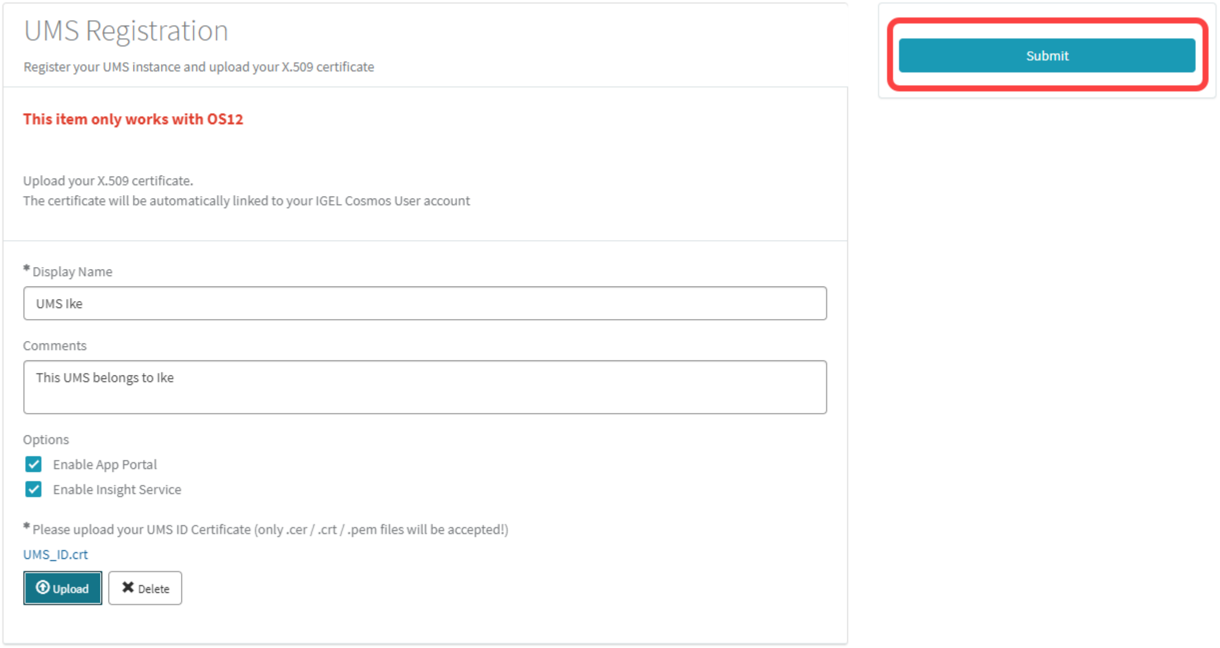
☑ Enable App Portal

☑ Enable Insight Service

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

UMS_ID.crt

5. Click **Submit**.



UMS Registration

Register your UMS instance and upload your X.509 certificate

This item only works with OS12

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

* Display Name: UMS Ike

Comments: This UMS belongs to Ike

Options

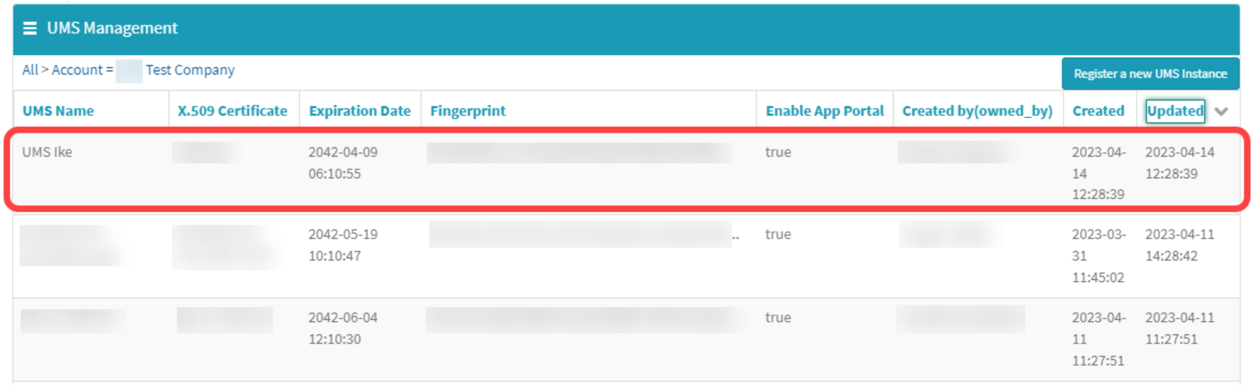
☑ Enable App Portal

☑ Enable Insight Service

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

UMS_ID.crt

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



UMS Management

All > Account = [redacted] Test Company

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

Overview of UMS WEB App and UMS Profiles

IGEL UMS Web App

The IGEL Universal Management Suite (UMS) Web App is a web-based user interface to the UMS Server. The installation of the UMS Web App is handled via the UMS installer, see IGEL UMS Installation.

The UMS Web App can currently be used only in addition to the Java-based UMS Console. Some features are currently available only in the UMS Web App, others only in the UMS Console; see the feature matrix under Overview of the IGEL UMS.

The range of functions available in the UMS Web App will constantly be expanded.

All features that are already available in the UMS Web App are fully supported.

The main features of the UMS Web App include:

- managing device configuration and creating profiles
- shadowing of devices and various device commands (power control, update, sending/receiving settings, reset to factory defaults, etc.)
- assigning objects to devices and device directories
- importing and managing IGEL OS Apps and their versions
- monitoring the status of the UMS network
- configurable search functionality
- logging of actions

To open the IGEL UMS Web App:

▶ In the web browser, open the URL https://<server>:8443/webapp/

Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can create and manage profiles. **Profiles** are predefined configurations that can be assigned globally to managed devices via the UMS.

Menu path: **UMS Console › Profiles**

When Is It a Good Idea to Use Profiles?

You can achieve the following using profiles:

- Setting identical configurations for a number of devices
- Defining different usage scenarios for devices (or groups of devices) in an abstract manner
- Significantly reducing administrative outlay
- Reducing configuration options on the device

You have the option of creating directories for saving profiles and can add, delete, and change the profiles in this part of the structure.

Creating Profiles for IGEL OS 12 Devices

Before creating profiles for IGEL OS 12 devices, you have to import the required apps from the IGEL App Portal; see How to Import IGEL OS Apps from the IGEL App Portal.

Alternatively, at least one IGEL OS 12 device with the required apps has to be already registered with the UMS Server. IGEL OS base system as well as all locally installed apps are then automatically recognized by the UMS. See e.g. Installing IGEL OS Apps Locally on the Device.

As soon as there are apps listed under **UMS Web App › Apps**, you can create a profile to configure settings for your devices.

There are two methods to create a profile:

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

Profiles cannot currently be deleted in the UMS Web App. Use the UMS Console, instead.

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

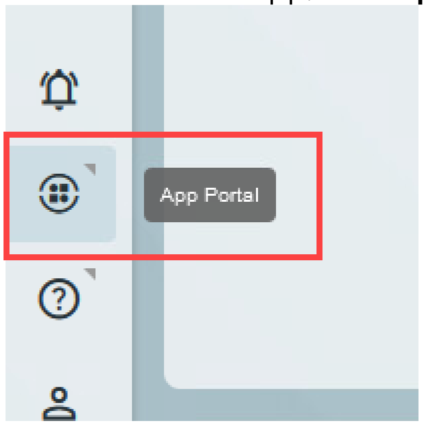
Import the AVD Client App

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

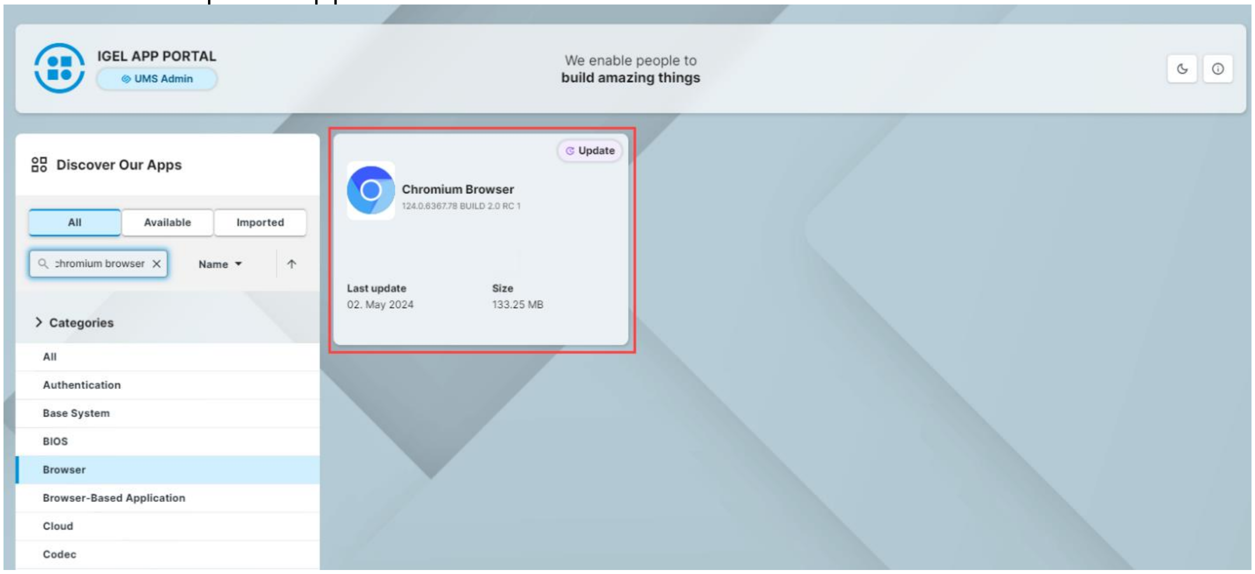
As we've registered the UMS server to IGEL Cloud Services the UMS Server will automatically authenticate with the App Portal allowing you to directly import apps into the UMS Server.

To import apps to the IGEL UMS, proceed as follows:

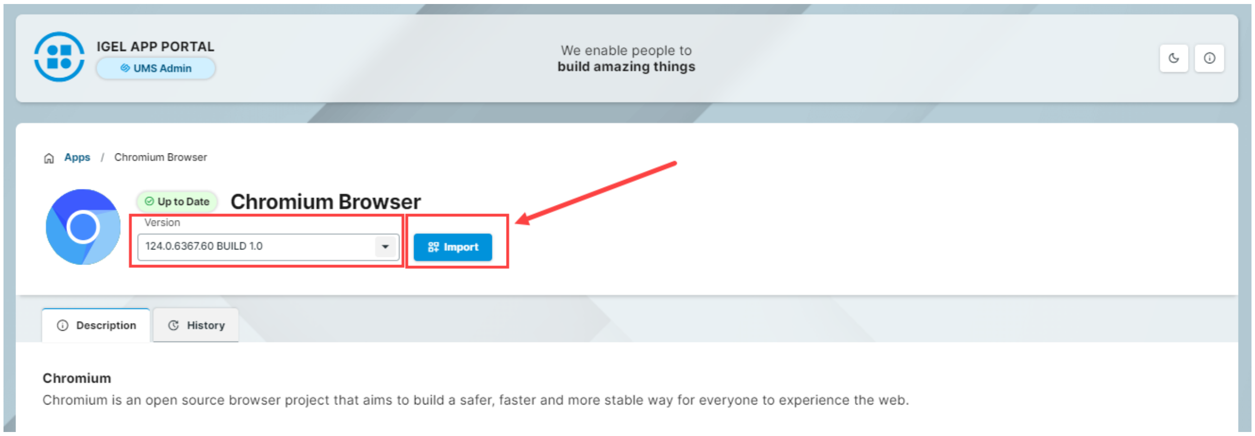
1. In the UMS Web App, click **App Portal**.



2. Select the required app.



3. Select the required version and click **Import**.



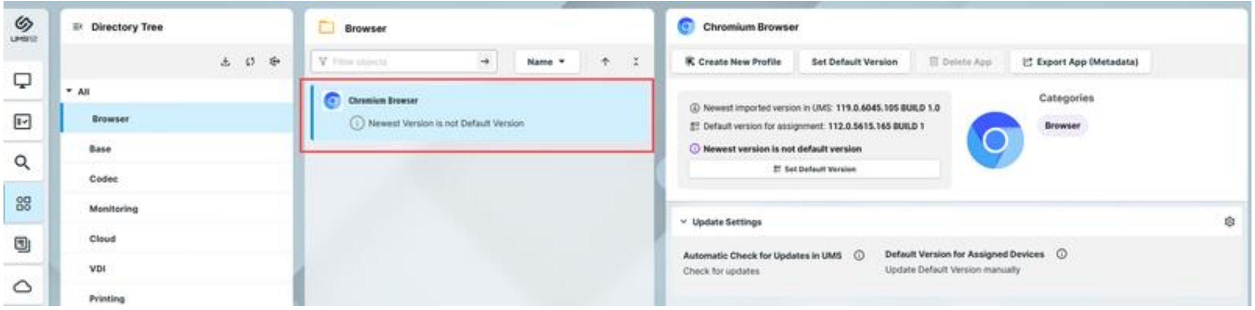
Version: 124.0.6367.60 BUILD 1.0

Chromium

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

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

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



Chromium Browser: Newest Version is not Default Version

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

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

Newest version is not default version

Automatic Check for Updates in UMS: Check for updates

Default Version for Assigned Devices: Update Default Version manually

Profiles in the IGEL UMS

In the IGEL Universal Management Suite (UMS), you can create and manage profiles. **Profiles** are predefined configurations that can be assigned globally to managed devices via the UMS.

Menu path: **UMS Console › Profiles**

When Is It a Good Idea to Use Profiles?

You can achieve the following using profiles:

- Setting identical configurations for a number of devices
- Defining different usage scenarios for devices (or groups of devices) in an abstract manner
- Significantly reducing administrative outlay
- Reducing configuration options on the device

You have the option of creating directories for saving profiles and can add, delete, and change the profiles in this part of the structure.

Creating Profiles for IGEL OS 12 Devices

Before creating profiles for IGEL OS 12 devices, you have to import the required apps from the IGEL App Portal; see How to Import IGEL OS Apps from the IGEL App Portal.

Alternatively, at least one IGEL OS 12 device with the required apps has to be already registered with the UMS Server. IGEL OS base system as well as all locally installed apps are then automatically recognized by the UMS. See e.g. Installing IGEL OS Apps Locally on the Device.

As soon as there are apps listed under **UMS Web App › Apps**, you can create a profile to configure settings for your devices.

There are two methods to create a profile:

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

Profiles cannot currently be deleted in the UMS Web App. Use the UMS Console, instead.

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

Set the Corporate Identity

Firmware Customizations in the IGEL UMS

You can customize the user interface of your IGEL OS devices to suit your corporate design using the firmware customization function in the IGEL Universal Management Suite (UMS). The configuration takes place in a dedicated wizard; for a minimal configuration, only a name and a file object need to be specified.

Menu path: **UMS Console › Firmware Customizations**

Mode of Action

A firmware customization can be assigned to a device or a directory.

Firmware customizations override standard profiles but in turn can be overridden by priority profiles. They are therefore between priority profiles and standard profiles in terms of their priority. Further information regarding the prioritization of profiles can be found under Prioritization of Profiles in the IGEL UMS.

If several use cases of the same type are assigned to a device, e.g. a background image, only the use case with the highest priority will be effective. The priority is determined by how direct or indirect the assignment to the device is: A firmware customization assigned directly to the device has a higher priority than one which is assigned to the device directory. If both firmware customizations have the same priority, the firmware customization with the higher ID will be effective.

In order to obtain the ID of a firmware customization, move the mouse pointer over the relevant object in the structure tree

Firmware Customization Options

There are several options available to you in order to customize the look and feel of the device. These include:

- Start Button
- Start Menu
- Taskbar Background
- Screensaver
- Screensaver (Custom Partition)
- Bootsplash
- Background Image

For our deployment we'll look to change the device background imager or wallpaper.

Changing the background Image

- **Name**: "Background image"
- **Use case**: "Background image"
- **Background monitor 1-8**: Name of an image file for up to 8 monitors
    - **Choose file**: All files registered in the UMS in a suitable format (*.jpg, *bmp, *png) and for which your have authorizations are shown here.
    - **Upload file**: Select a file from a local directory or from the UMS server.

      For the background image, the device obtains the selected file from the UMS via HTTPS as soon as it is required.

    - **Clear**: Deletes the image file shown under **Background monitor 1-8**.

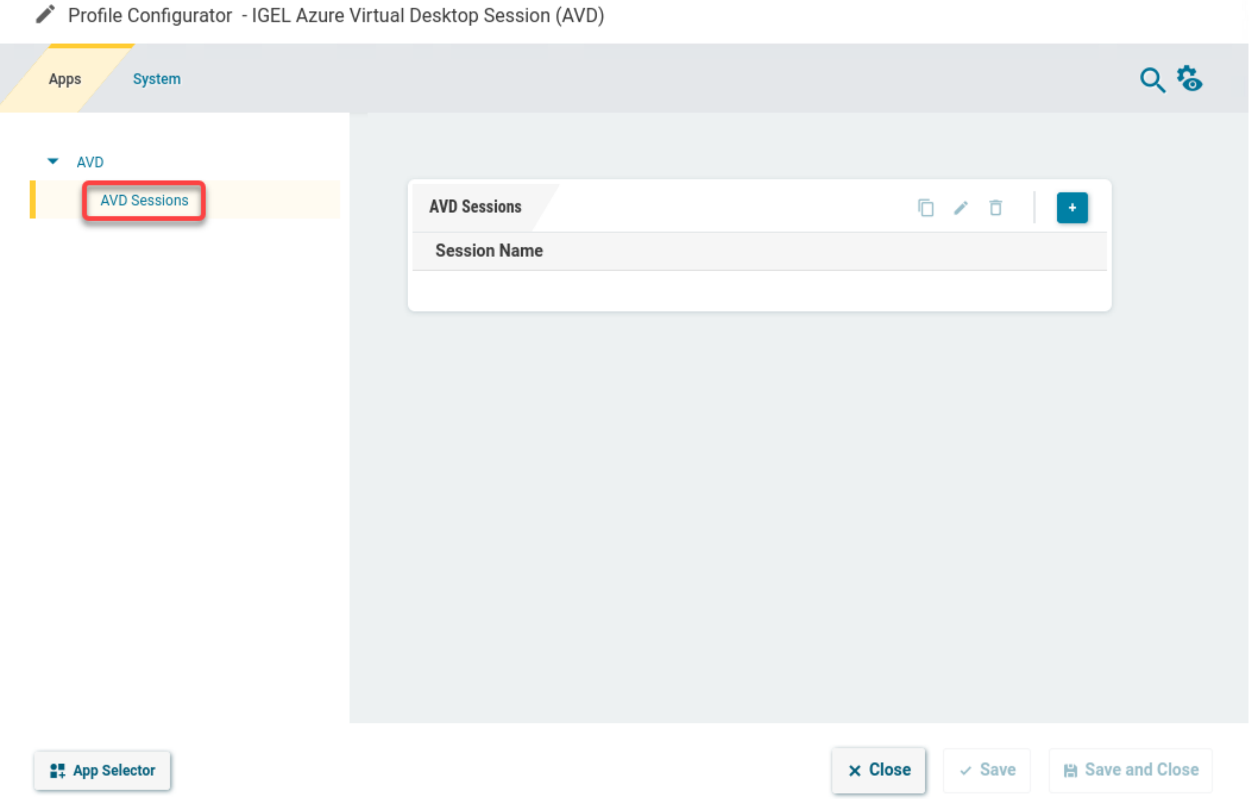
Deploy AVD client

When the IGEL Azure Virtual Desktop client is installed, the following app with the required version is also installed automatically:

- IGEL Remote Desktop Core

Create a Session

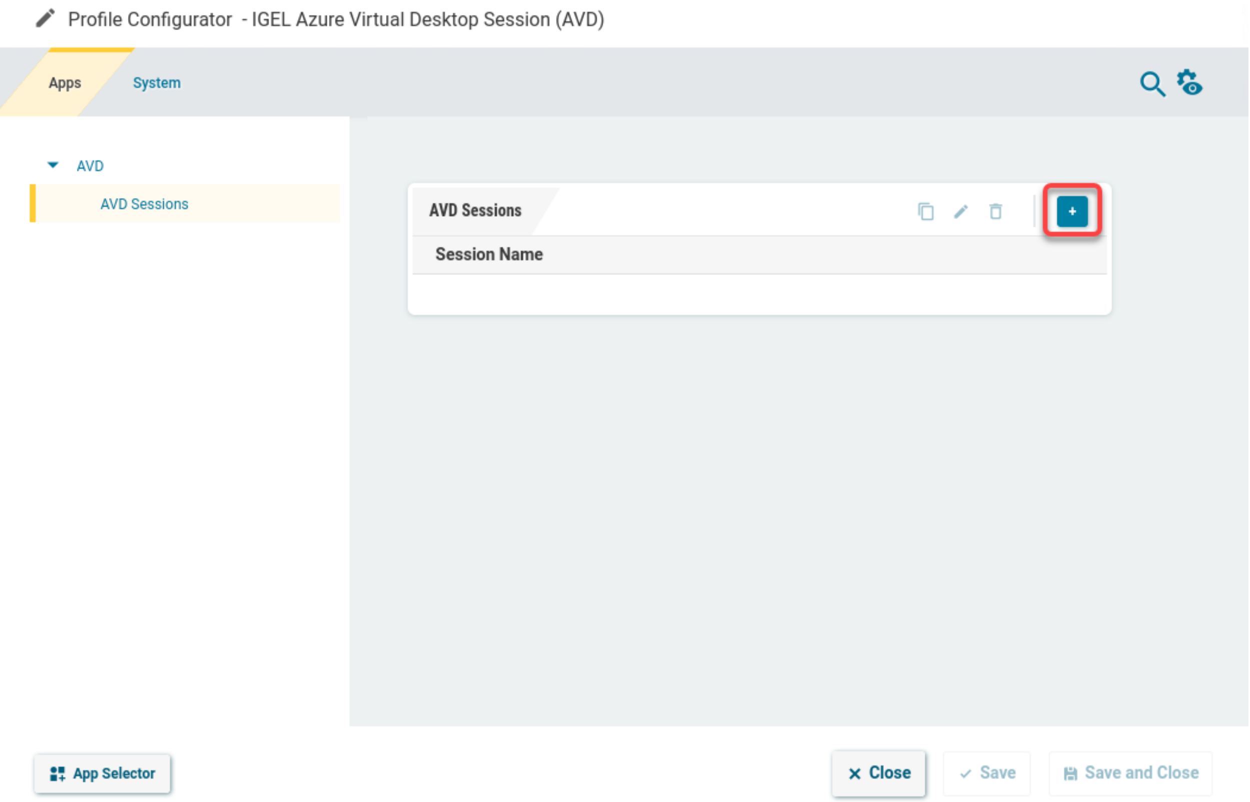
1. In the profile configurator, go to **Apps › AVD › AVD Sessions**.



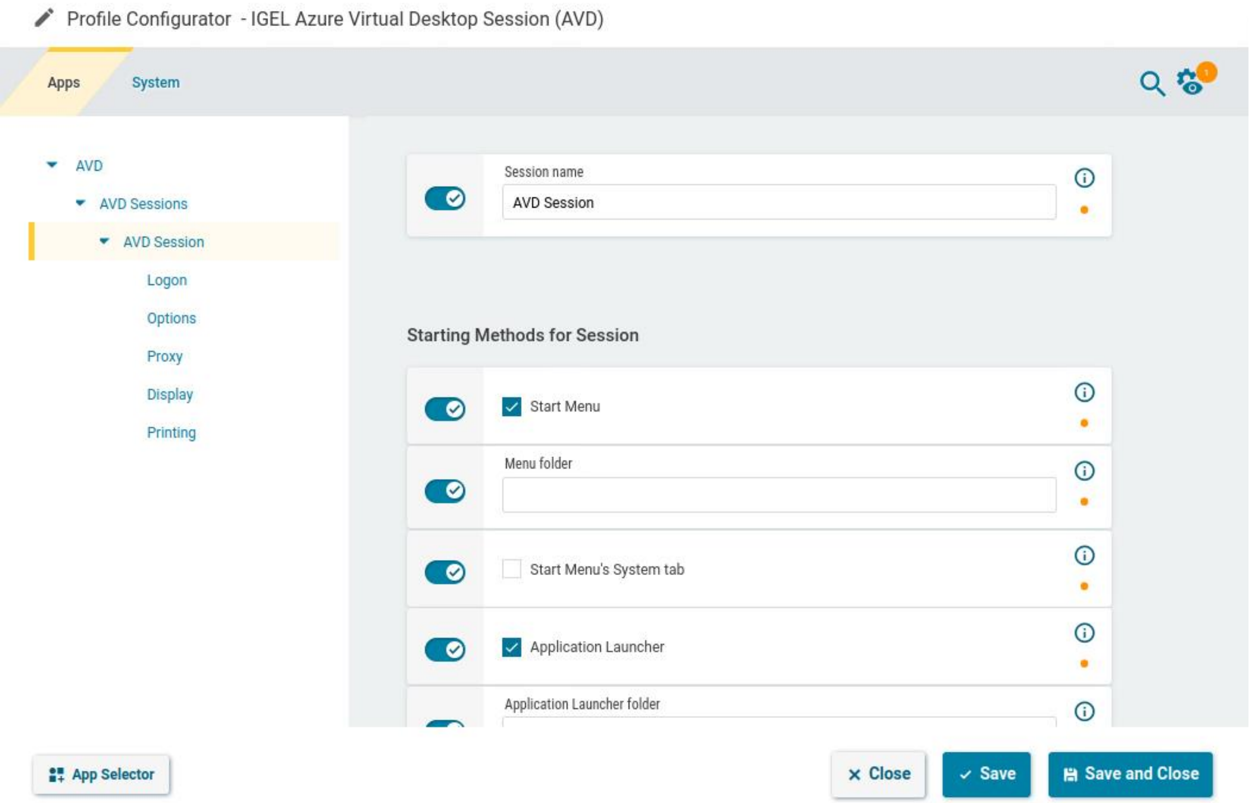
Profile Configurator - IGEL Azure Virtual Desktop Session (AVD)

2. Click

.



The session is created.



Profile Configurator - IGEL Azure Virtual Desktop Session (AVD)

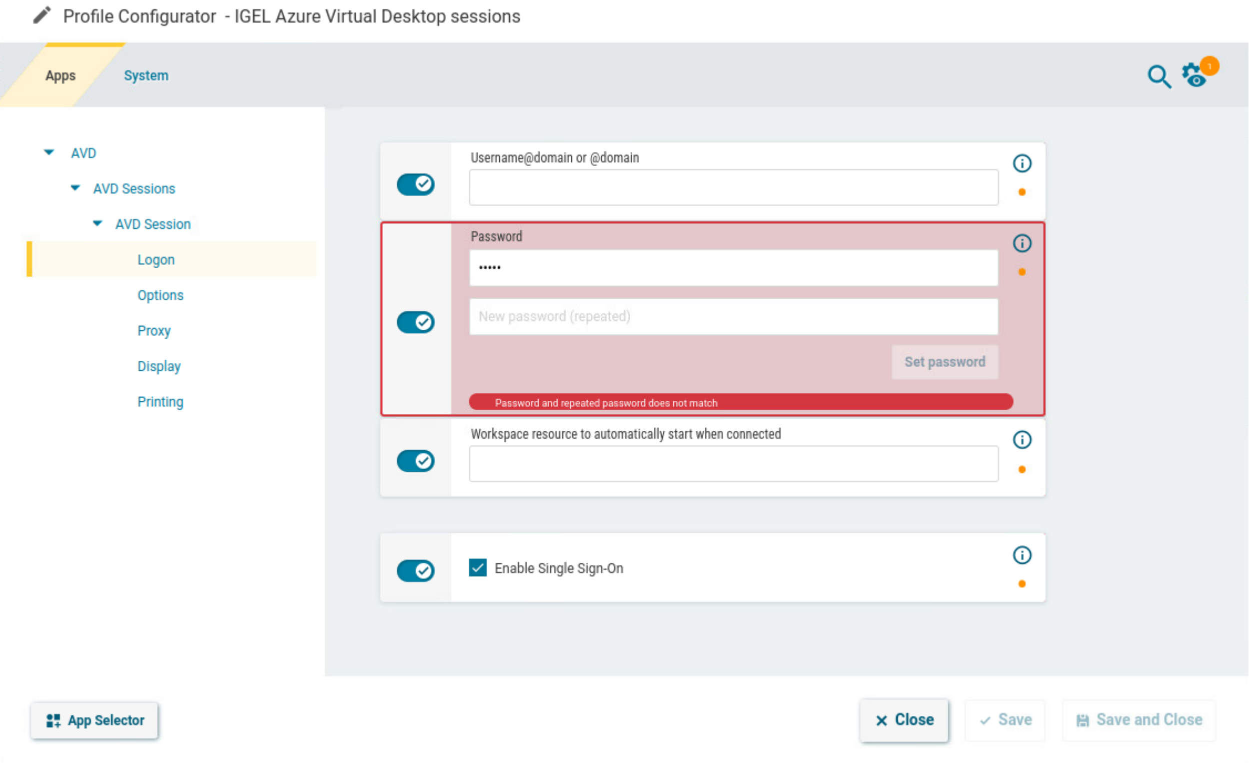
Session name: AVD Session

Starting Methods for Session

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

Configuring the Logon

1. In the profile configurator, go to **Apps** › **AVD** › **AVD Sessions** › **[session name]** › **Logon**.



Profile Configurator - IGEL Azure Virtual Desktop sessions

Username@domain or @domain

Password: •••••

New password (repeated)

Password and repeated password does not match

Workspace resource to automatically start when connected

☑ Enable Single Sign-On

2. Edit the settings according to your needs. The parameters are described in the following.

Username@domain or @domain

The user name or a preset domain name that will be used for the automatic connection to the AVD session. The string after "@" is taken as a preset domain name.

Example:

avd@your.domain.com: To log in, the user does not need to enter the username and the domain name.

@your.domain.com: To log in, the user only needs to enter the username, e.g. avd. The preset domain – your.domain.com – will automatically be appended.

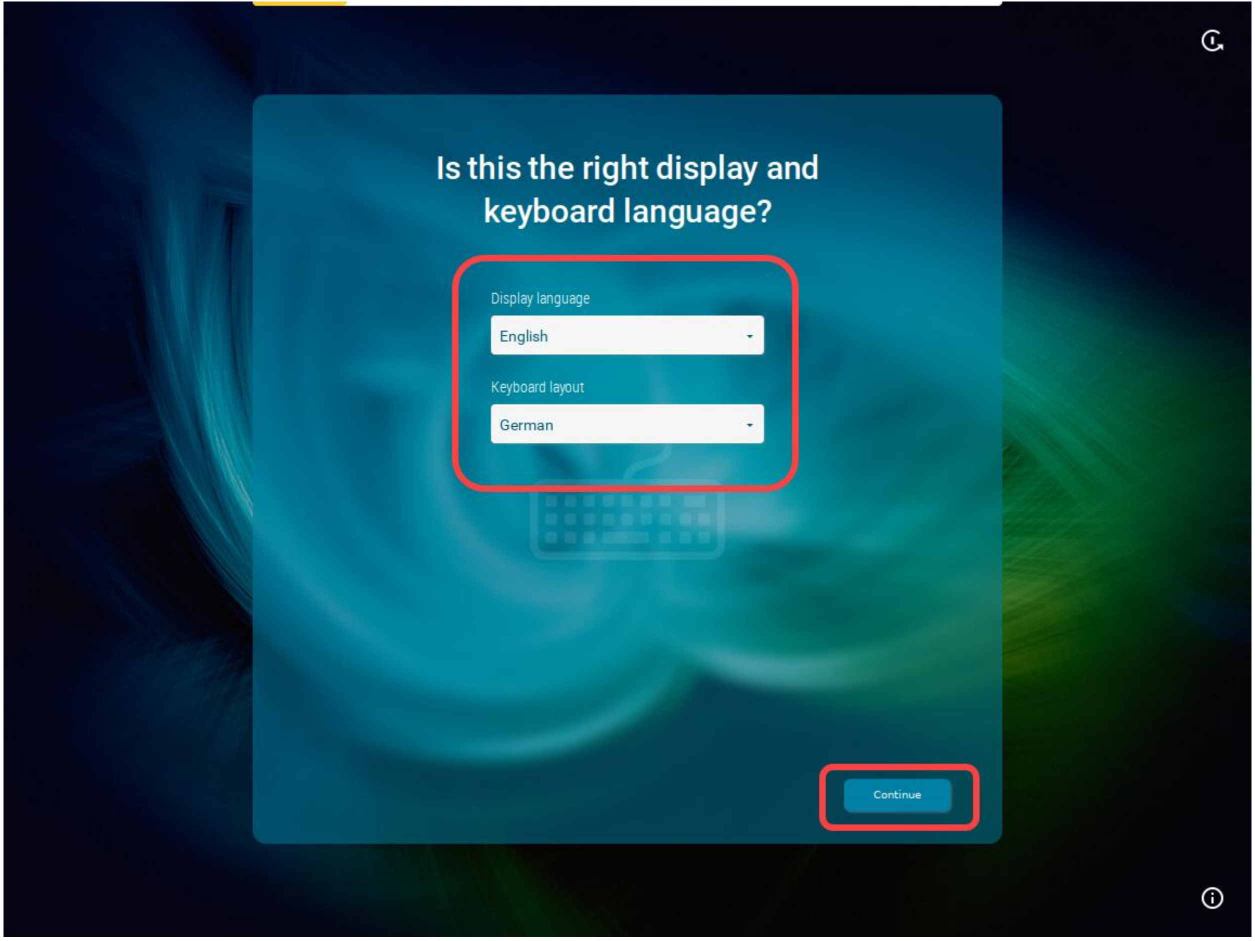
Connect a Device and Test!

Time to switch to the device and get it registered with UMS using your EntraID identity.

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

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

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

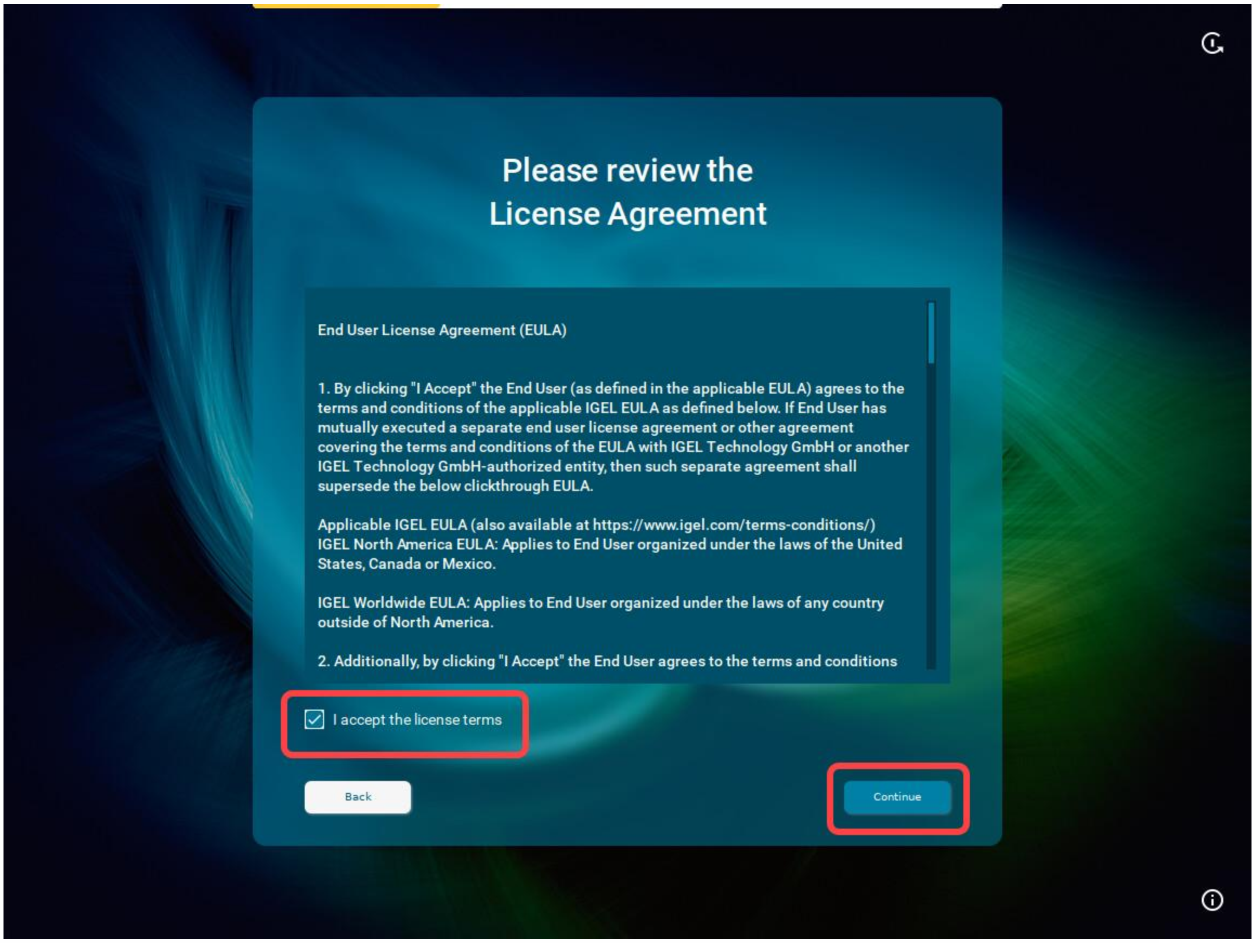


Is this the right display and keyboard language?

Display language: English

Keyboard layout: German

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



Please review the License Agreement

End User License Agreement (EULA)

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

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

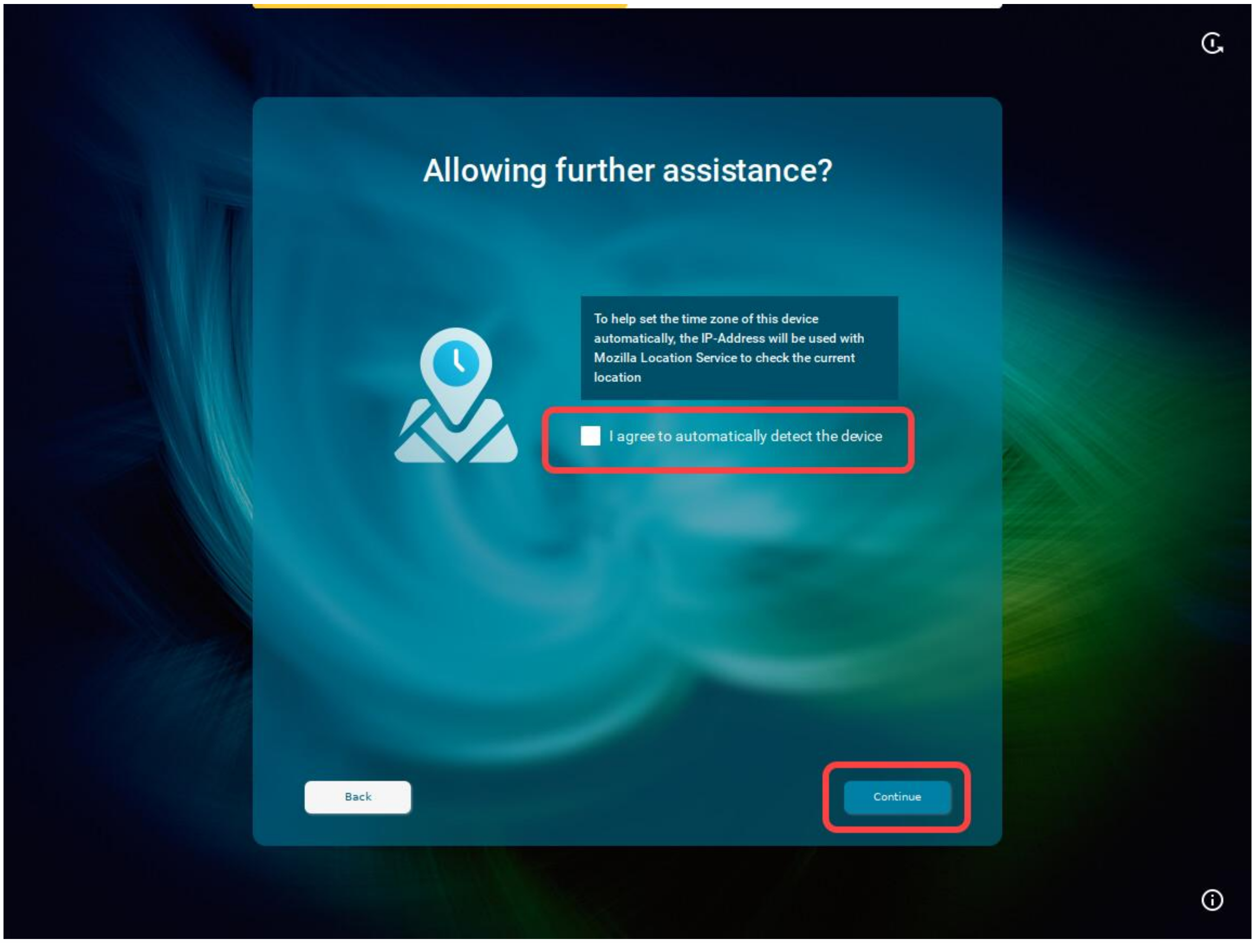
IGEL Worldwide EULA: Applies to End User organized under the laws of any country outside of North America.

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

☑ I accept the license terms

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

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



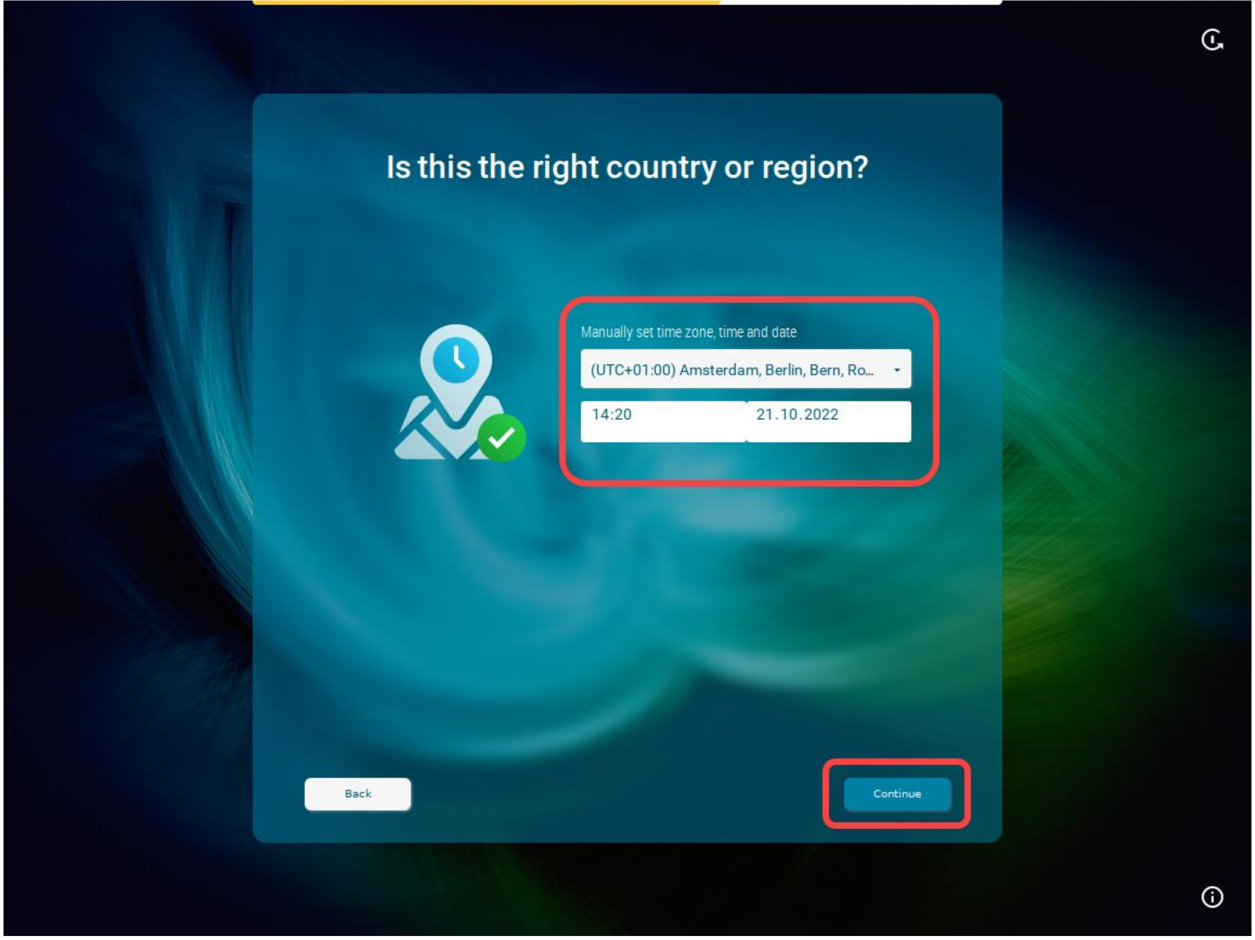
Allowing further assistance?

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

□ I agree to automatically detect the device

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

   TIP! *– Make sure you do set the time & Date correctly, misconfiguration can lead to device licensing issues!*



Is this the right country or region?

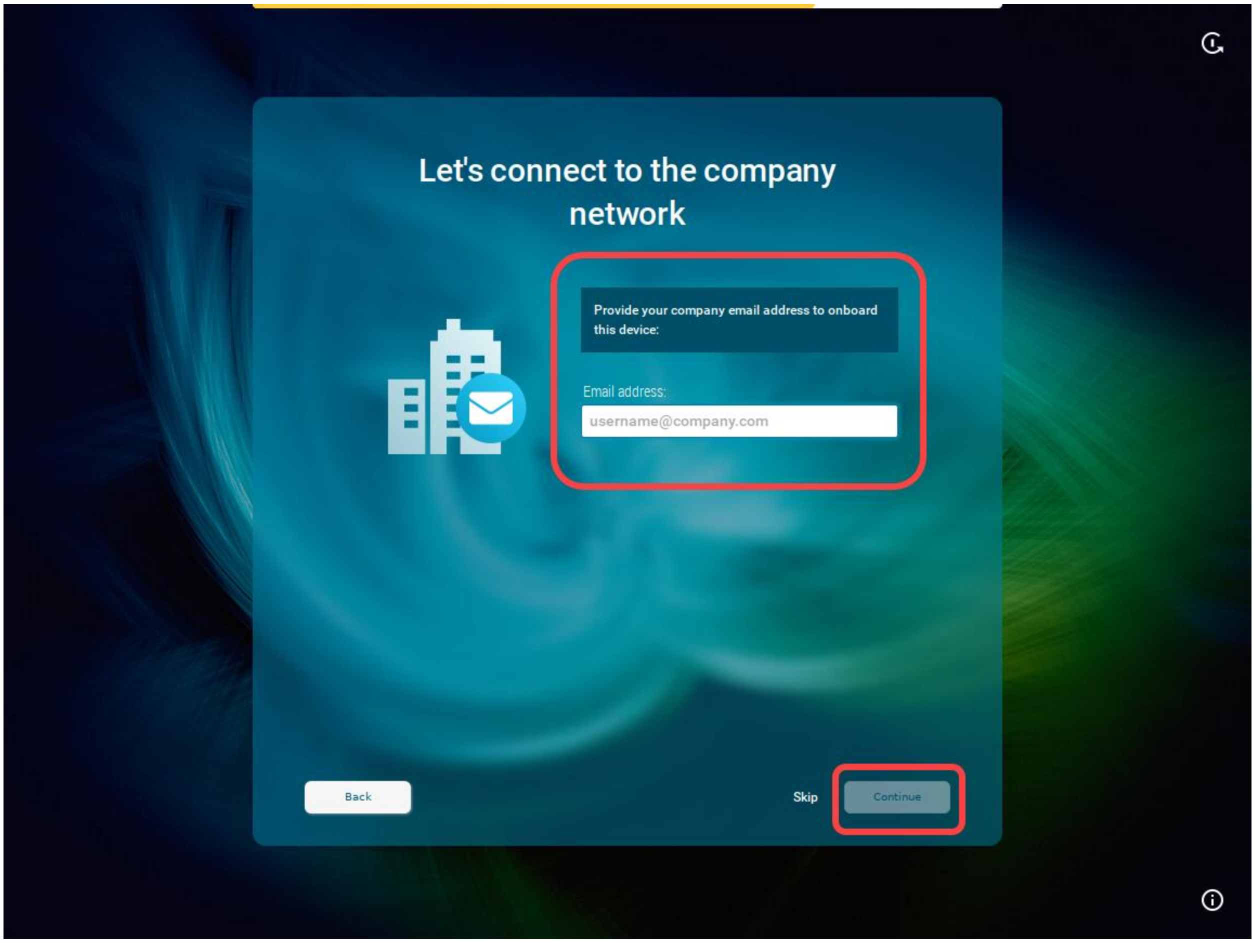
Manually set time zone, time and date

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

14:20

21.10.2022

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

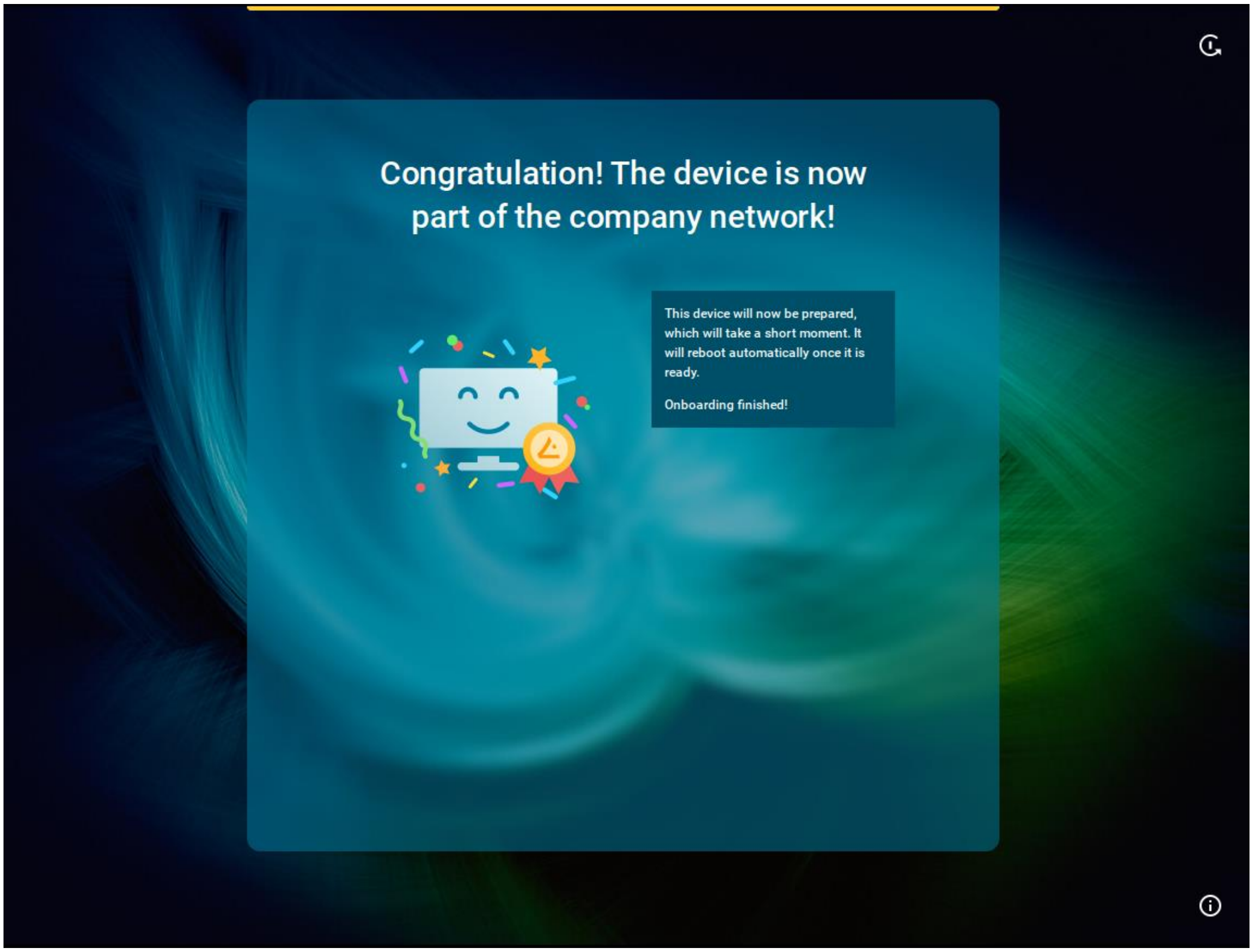


Let's connect to the company network

Provide your company email address to onboard this device:

Email address: username@company.com

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



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

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

Onboarding finished!

Once the device has be successfully registered with the UMS the default profile will apply to the device, updating the firmware (if required) downloading the custom wallpaper, installing the IGEL AVD client and configuring a connection to automatically star on boot and once there is a network available.

Congratulations you now have a configured device!

https://www.youtube.com/watch?v=iqgOy_4hUIA

References:

IGEL OS12 UMS and Cloud services overview

https://kb.igel.com/howtocosmos/en/how-to-start-with-igel-cosmos-77865726.html

https://kb.igel.com/howtocosmos/en/using-the-igel-customer-portal-81509885.html

IGEL OS12 Deployment Options

OS Creator Utility - https://kb.igel.com/base_system/12.4/en/how-to-deploy-igel-os-12-with-igel-os-creator-osc-122896320.html

PXE - https://kb.igel.com/base_system/12.4/en/how-to-deploy-igel-os-12-with-pxe-122896396.html

SCCM - https://kb.igel.com/base_system/12.4/en/how-to-deploy-igel-os-12-with-igel-os-12-sccm-add-on-122896414.html

UD Pocket - https://kb.igel.com/base_system/12.4/en/how-to-use-igel-os-12-with-ud-pocket-122896456.html

Supported H\W - https://kb.igel.com/hardware/en/devices-supported-by-igel-os-12-81496425.html

Software Downloads: https://www.igel.com/software-downloads/igel-os-12-secure-endpoint/

Let's build it!

Discovery

IGEL Onboarding Service configuration

https://kb.igel.com/howtocosmos/en/initial-configuration-of-the-igel-onboarding-service-obs-77865754.html

Authentication

EntraID as an idp configuration

https://kb.igel.com/howtocosmos/en/initial-configuration-of-the-igel-onboarding-service-obs-77865754.html

https://kb.igel.com/base_system/12.3.0/en/how-to-configure-single-sign-on-sso-on-igel-os-12-112731582.html

UMS Configuration

Connect UMS to the App Portal, download OS12, download the AVD Client ap, import a wallpaper. Create Profiles to deploy the AVD client, set it to auto start and fill out a pre-configured Domain name.

https://kb.igel.com/howtocosmos/en/igel-app-portal-77865794.html

https://kb.igel.com/howtocosmos/en/igel-ums-12-basic-configuration-77865800.html

https://kb.igel.com/en/igel-apps/current/configuring-igel-azure-virtual-desktop-client

https://kb.igel.com/en/universal-management-suite/12.04.120/configuration-centralized-management-of-device-set

https://kb.igel.com/endpointmgmt-12.04.120/en/igel-ums-web-app-126852399.html

https://kb.igel.com/endpointmgmt-12.04.120/en/create-firmware-customization-126851579.html