



AnyDesk Setup Guide

Introduction manual for IT administrators

AnyDesk Software GmbH

Version 2.0

01.04.2024

Legal Notice

Copyright © 2024 AnyDesk Software GmbH

Technical specifications are subject to change without notice. Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization from AnyDesk are prohibited. Offenders will be held liable for payment of damages. All rights are reserved.

This document is for informational purposes. It represents Any Desk's current product and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AnyDesk's products or services. This document does not create any warranties, representations, contractual commitments, conditions, or assurances from AnyDesk, its affiliates, suppliers, or licensors. The responsibilities and liabilities of AnyDesk to its customers is controlled by agreements, and this document is not part of, nor does it modify, any agreement between AnyDesk and its customers.

AnyDesk is designed to be connected to and to communicate via a network interface. Customer shall establish and maintain any appropriate measures (*such as but not limited to the application of authentication measures, encryption of data, etc.*) to protect the product, the network, its system, and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. AnyDesk is not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

To protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. AnyDesk provides such concept. You are responsible for preventing unauthorized access to your systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (*e.g., firewalls and/or network segmentation*) are in place. For additional information, please visit <https://anydesk.com>. AnyDesk recommends applying updates and to use the latest available version. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats.

Contents

Document Overview	4
Getting Started	5
Step 1. Set up the administrator account	5
Step 2. Set up your Team or Organization	6
Set up an organization and create users.....	6
Set up a team and invite other users	6
Step 3. Assign permissions to other users	7
Step 4. Create shared Address Books	8
Create shared Address Book	8
Add contacts to Address Book	9
Step 5. Create a custom AnyDesk client	10
Step 6. View sessions and clients details	10
my.anydesk II	12
User Providers.....	12
Admin user provider type.....	12
IDP user provider type.....	13
LDAP user provider type.....	15
User accounts creation and invitation	18
Create users	18
Invite users to your team	18
User management	19
Manage users	19
Manage user roles	20
Manage groups.....	21
Manage permission sets.....	21
Address Books.....	22
Clients management.....	23
Custom Clients	23
Builds overview	24
Central Management.....	25
License management.....	26
my.anydesk API.....	27
my.anydesk I	28

Revision history

Date	Version	Description
April 1 st , 2024	2.0	Updated the whole document.
March 1 st , 2023	1.0	Initial publication.

Document Overview

This guide is designed for IT administrators and others who are responsible for setting up the AnyDesk software. This guide provides information on how to configure the [my.anydesk II](#) management portal before using the AnyDesk application.

The document consists of the following chapters:

- [Getting started](#) – includes the first steps that must be done after purchasing AnyDesk license.
- [my.anydesk II](#) – provides a detailed information on [my.anydesk II](#) features.
- [my.anydesk I](#) – provides an overview on [my.anydesk I](#) management portal.

Getting Started

As an IT administrator, you first need to configure the [my.anydesk II](#) management portal so that you and your team can start using all AnyDesk features.

In this chapter, you will learn how to:

- [Set up the administrator account](#)
- [Set up your Team or Organization](#)
- [Assign permissions to other users](#)
- [Create shared Address Book](#)
- [Generate a custom AnyDesk clients](#)
- [View sessions and clients details](#)

Step 1. Set up the administrator account

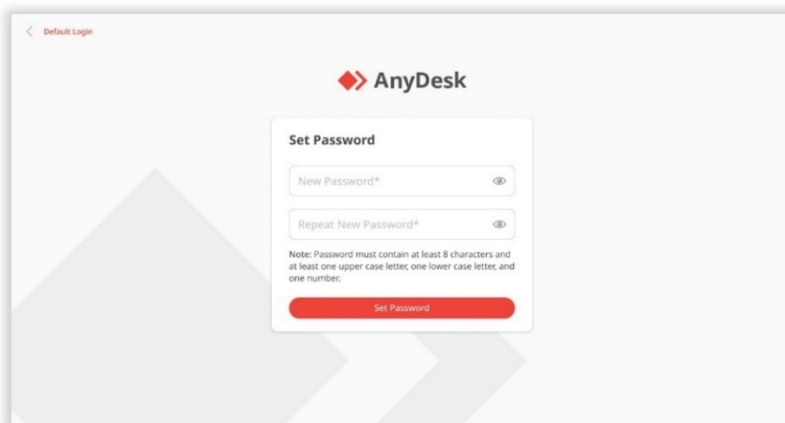
When you buy or sign up for a trial, your [my.anydesk II](#) account is automatically generated using the registered email address. The **Admin** account grants full access to all settings within [my.anydesk II](#) management portal, such as organization/team setup, as well as the ability to review sessions history and other data.

It is recommended to use this account only for the initial setup process. Afterwards, you can add users and grant them tailored permissions based on their specific requirements.

You receive two emails allowing you to set up your credentials to [my.anydesk](#).

To set up the administrator account:

- 1 Open the **Welcome to my.anydesk** email and select **Click here**.
- 2 On the opened page, set up your password. You will use it to log in to [my.anydesk II](#) with your account.
- 3 Click **Set Password**.



Step 2. Set up your Team or Organization

In [my.anydesk II](#), you can configure your team or organization (depending on the license you have), and only those users that you invite will be able to sign into the management portal, be part of your team/organization, and use the license features.

Set up an organization and create users

Note

Available for Ultimate (Cloud) license only.

As a license owner, you get to configure your organization, add users to the organization, and grant users access to different features within [my.anydesk II](#).

To set up an organization:

- 1 Log in to [my.anydesk II](#) with your administrator account which you have set up in [Step 1](#).
- 2 On initial login, you will be prompted to set up your organization. To do so, in the **Set Organization Name** window, enter the organization name you wish to use.
Note: The organization's name cannot be changed later.
- 3 Click **Set Organization Name**. Review the organization name provided and click **Continue**.

You will receive an email with the link to your organization shortly after. For more information, see the [Set up an Organization](#) article in Help Center.

To create users and add them to your organization, see the [User Providers](#) chapter in this document or refer to the [User Providers](#) article in Help Center.

Set up a team and invite other users

Note

Available for Standard and Advanced license only.

As a license owner, you get to configure your team and manage licensed users in the [my.anydesk II](#) management portal.

To set up a team:

- 1 Log in to [my.anydesk II](#) with your administrator account which you have setup in [Step 1](#).
- 2 On initial login, you will be prompted to setup your team. To do so, in the **Team Setup** window, enter the team name you wish to use and provide a short description.
Note: The team's name cannot be changed later.
- 3 Click **Create team**.

You can now invite users to your team. They will become part of your license. To invite users, please follow the instructions in this Help Center [article](#).

Step 3. Assign permissions to other users

Assigning roles to users helps you improve your productivity and security by reducing the threat that users have access to functionality they should not have access to.

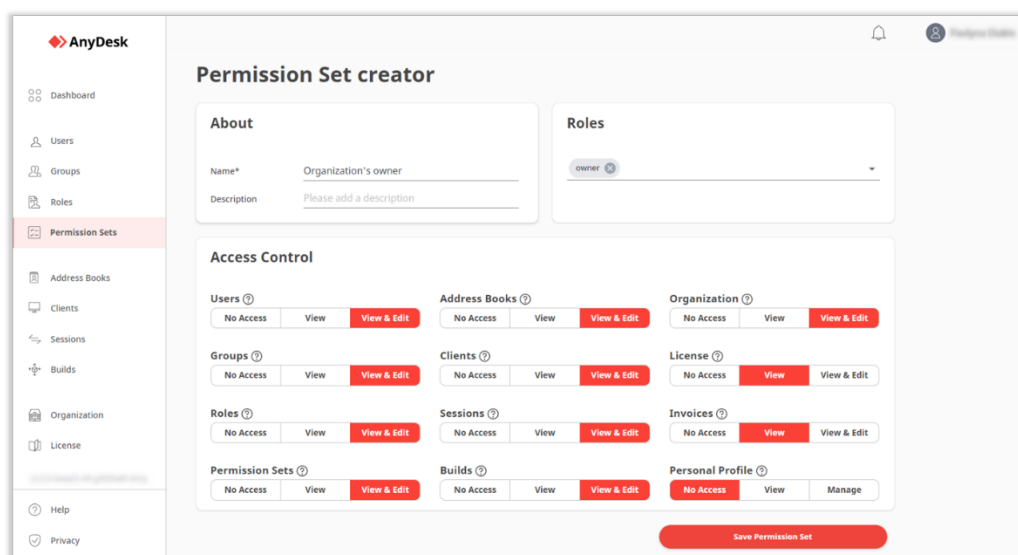
Once you have added all users to your team or organization, you can assign roles with different permissions to individual users or user groups in your license.

Each role has different sets of permissions that define what users can see and do within the management portal. Depending on the role the user is assigned to, they can either only view, view and edit, or have no access at all to different sections of [my.anydesk II](#) management portal.

In [my.anydesk II](#) management portal, there are the following preconfigured roles for the **Ultimate (Cloud)** license:

- **Owner** - a role is designed for a license owner. With this role, they can view and edit every section of the management portal and delete the Organization.
- **Admin** - a role that allows the user to view and edit all the sections of the management portal except for *License, Invoices, and personal profile*.
- **Support agent** - a role that allows the user to view the *Users, Groups, Address Books, and Clients* sections of my.anydesk II management portal. It is designed for IT support staff.
- **Accountant** - a role for a person within your organization that deals with invoices. The role grants the access to only view the *Organization, License, and Invoices* sections.
- **Data protection officer** - a role that allows the user to view all the sections of my.anydesk II management portal except for *Builds* and *personal profile*.
- **User** - the default role for every user. With this role, they can view and edit their *personal profile* and view the *Clients* and *Builds* sections.

You can also create custom permissions and roles. It is recommended to grant the minimum permissions needed. For more information on user and role management setup, see [this page](#).



Permission Set creator in my.anydesk II

In the table below, can check the roles available for Ultimate license and the permissions each role has in [my.anydesk II](#).

my.ad sections	Roles					
	Owner	Admin	Support agent	Data protection officer	Accountant	User
Personal profile	view & edit	x	x	x	x	view & edit
License	view & edit	view	x	view	view	x
Invoices	view & edit	view	x	view	view	x
Users	view & edit	view & edit	view	view	x	x
Roles	view & edit	view & edit	x	view	x	x
Groups	view & edit	view & edit	view	view	x	x
Permission Sets	view & edit	view & edit	x	view	x	x
Address Books	view & edit	view & edit	view	view	x	x
Clients	view & edit	view & edit	view	view	x	view
Sessions	view & edit	view & edit	x	view	x	x
Builds	view & edit	view & edit	x	x	x	view
Organization	view & edit	view & edit	x	view	view	x

Step 4. Create shared Address Books

Shared Address Book is a list of contacts (devices you connect to). By adding tags to contacts, you can filter the devices. You can create, view, and edit shared Address Books in [my.anydesk II](#). Users with the right permissions can also manage shared Address Books. For more information about Address Books, see [this article](#) in Help Center.

Create shared Address Book

To create a shared address book:

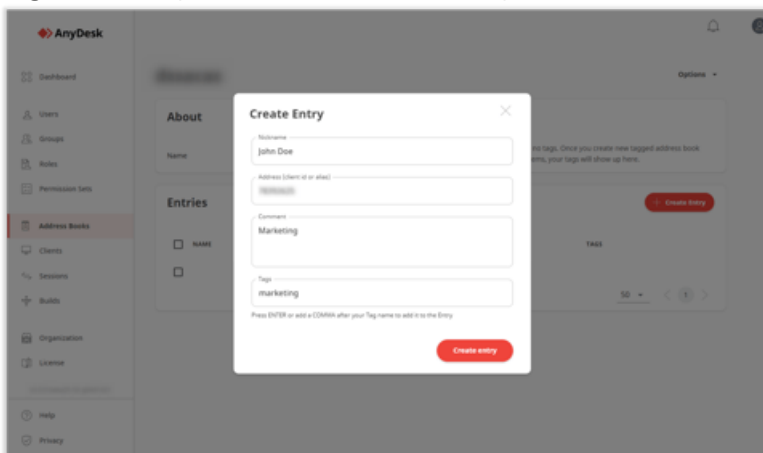
- 1 In your [my.anydesk II](#) account, go to **Address Books**.
- 2 In the **Organization** tab, click **Create Address Book**.
- 3 In the pop-up window, enter the name for the organization address book.
- 4 Click **Create address book**.

After that, you can add contacts to the shared address book.

Add contacts to Address Book

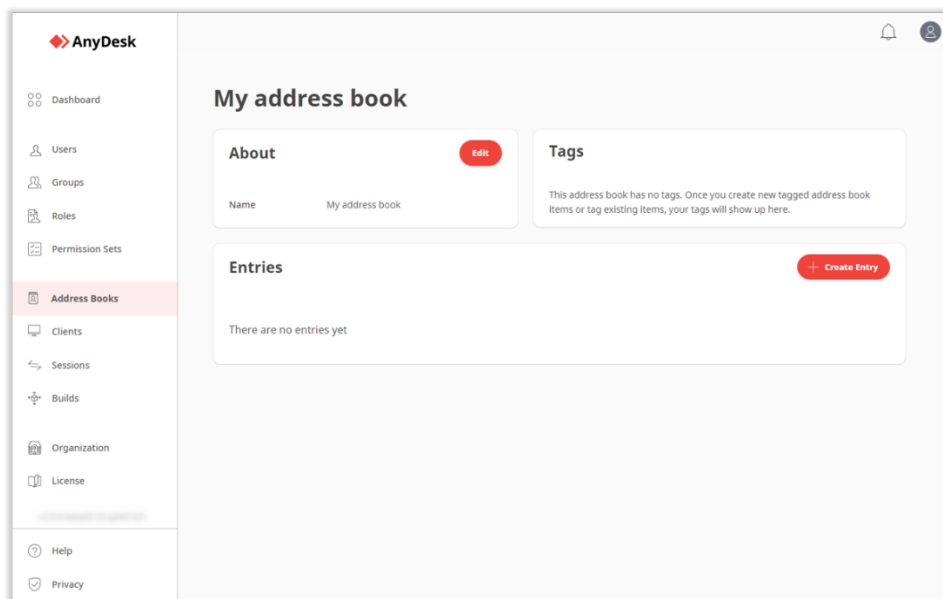
To add contacts to a shared address book:

- 1 In your [my.anydesk II](#) account, go to **Address Books**.
- 2 In the **Organization** tab, open the address book you wish to edit.
- 3 On the next page, go to the **Entries** section and click **Create Entry**.
- 4 In the pop-up window, provide the following details:
 - a **Nickname** - Enter the name for the contact.
 - b **Address** - Provide AnyDesk ID or Alias of the contact.
 - c **Comment** - Enter a description for the contact you are adding.
 - d **Tags** - Add a tag for further contact filtering.



- 5 Click **Create Entry**.

Additionally, users can set up personal Address Books within their account.



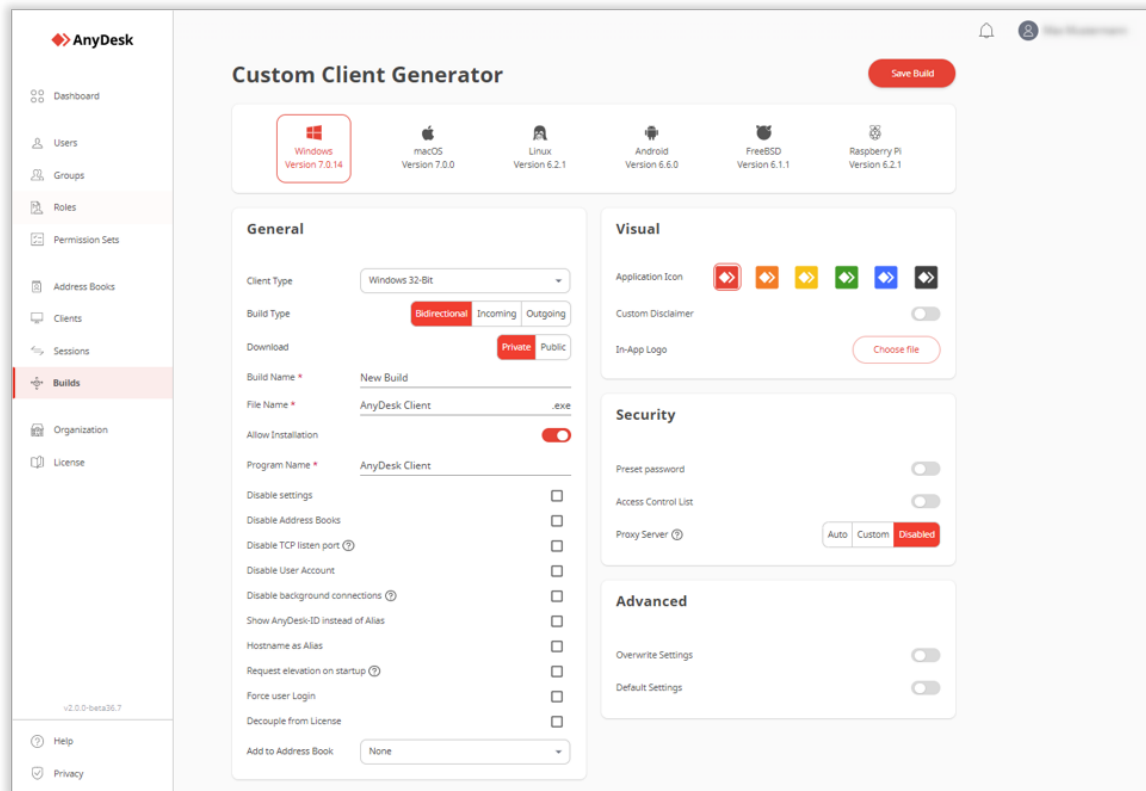
Personal Address Book page in my.anydesk II

Step 5. Create a custom AnyDesk client

The **Custom Client Generator** in my.anydesk.com allows you to create custom AnyDesk clients tailored to your needs. You can create incoming-only clients, for example, which are deployed to users' devices to allow IT admins to connect to those devices for troubleshooting. Users cannot start outgoing sessions with incoming-only clients. Moreover, you can set up the **Access Control List** security feature for advanced access control.

To open the Custom Client Generator:

- 1 Log in to my.anydesk.com with your administrator account.
- 2 Go to the **Builds** tab and click **Create Build**.
- 3 On the opened page, customize AnyDesk client according to your needs.



Note: For detailed instructions on how to use Custom Client Generator in my.anydesk.com, see [Create a Custom Client](#) in Help Center.

- 4 Click **Save Build**.

The custom AnyDesk client can be deployed directly. Alternatively, you can share a link with users, so they can download and install the custom client.

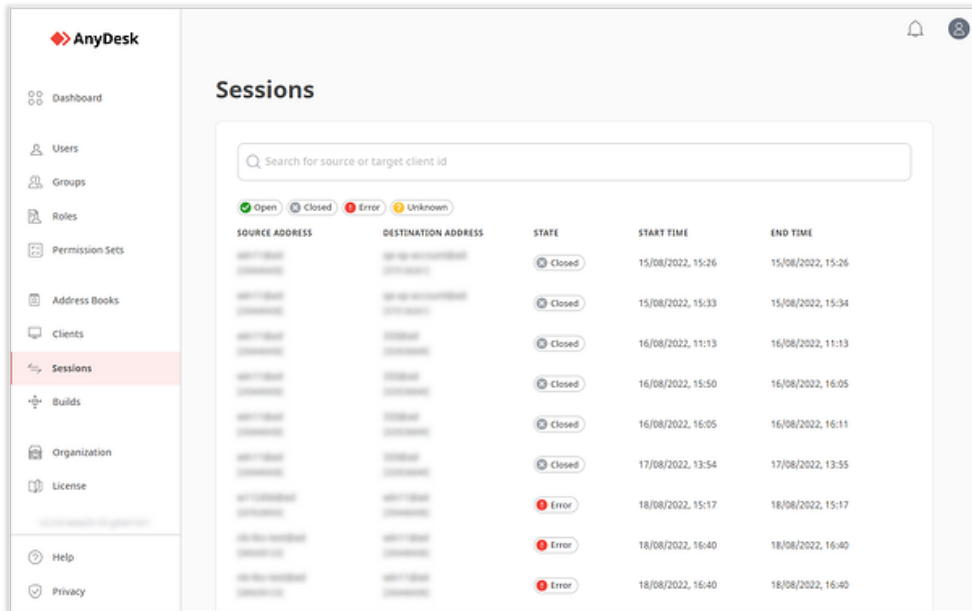
For more information, see [Custom Client Generator](#) chapter in this document.

Step 6. View sessions and clients details

Admins can view sessions' details in my.anydesk.com, review and edit session comments and close active sessions.

To access **Sessions** page:

- Log in to [my.anydesk II](#) with your administrator account and go to the **Sessions** tab.

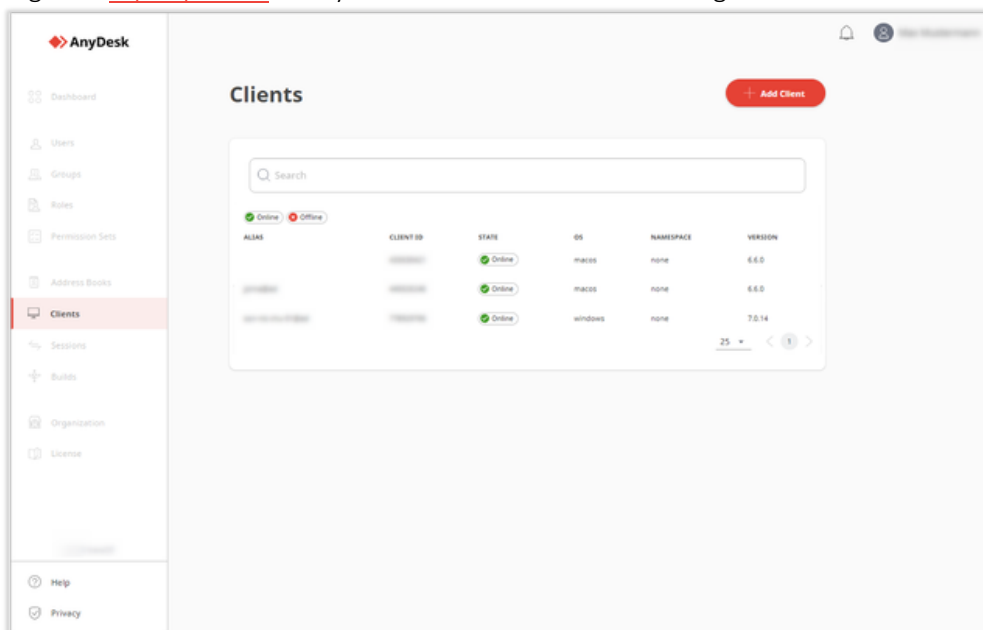


For more information about managing sessions, see [Sessions](#) in Help Center.

In the **Clients** page, you can see a detailed overview of all deployed clients assigned to your license. By selecting one of the clients from the list, the client's overview page will open.

To access **Clients** page:

- Log in to [my.anydesk II](#) with your administrator account and go to the **Clients** tab.



For more information about managing clients, see [Clients](#) in Help Center.

my.anydesk II

[my.anydesk II](#) is a user management portal which offers a wide range of possibilities for IT Support staff, administrators, license owner.

With [my.anydesk II](#), you can view sessions details, create personal or shared Address Books, view your license details, invite other users, create users, manage permission sets for users, and other.

User Providers

Within the [my.anydesk II](#) management console, you, as a license and organization owner, can set up a signup procedure for your users. The User Provider type defines how new users for your organization are created. This feature is exclusive to our Ultimate (Cloud) license.

[my.anydesk II](#) management portal supports three mutually exclusive user provider options:

- **Admin** – creating users in my.anydesk II manually.
- **IDP** – creating users via third-party identity provider. When selected, it allows the owner of the organization to create users for that organization using an identity management system that supports OpenID Connect (e.g., Microsoft Azure Active Directory). This way, Single Sign-On is set up and users can sign in with SSO using the organization's ID and company credentials.
- **LDAP** – users are synchronized with an LDAP system, and administrators can manage user, role, group and permission mappings. When selected, it allows the owner of the organization to set up a user authentication process which validates a username and password combination with a directory server, such as Microsoft Active Directory, OpenLDAP, or OpenDJ.

To access the user provider settings:

- 1 Sign in to [my.anydesk II](#) and go to the **Settings > User Providers** page.
- 2 On the opened page, select the preferred user provider and configure it.

Admin user provider type

The **Admin** user provider type allows the owner or administrator of the [my.anydesk II](#) organization to manually add one or more users to their main license account. As a result, you can create users one by one or add multiple users at once.

To select the Admin user provider type:

- 1 Sign in to [my.anydesk II](#) and go to the **Settings > User Providers** page.
- 2 On the opened page, select **Admin**.
- 3 In the **Switch active provider** window, select **Proceed**.

To learn how to create users, see [User account creation and invitation](#) in this document.

IDP user provider type

Note

Available for Ultimate (Cloud) license only.

The IDP user provider allows the owner of an organization to create users for that organization using a third-party identity provider that supports OpenID Connect (e.g., *Microsoft Azure Active Directory or Keycloak Active Directory*). Users from your organization will then be able to log in with SSO using the organization's ID and their company credentials.

Note

You will not be able edit users in [my.anydesk II](#) created through the IDP since they are synchronized with the identity provider.

The IDP user provider setup consists of the following steps:

- 1 [Select the IDP user provider in my.anydesk II.](#)
- 2 [Set up your identity provider.](#) You can use any third-party identity provider that supports OpenID Connect, such as Microsoft Azure Active Directory.
- 3 [Configure the IDP in my.anydesk II to connect my.anydesk II to the identity provider.](#)
- 4 Map your organization roles to the users in my.anydesk II. This way, you do not need to assign roles to users manually. For more information about IDP mapper, see [Set up IDP mapper](#) in Help Center.

Select IDP user provider

To select IDP user provider:

- 1 Sign in to [my.anydesk II](#) and go to the **Settings > User Providers** page.
- 2 On the opened page, select **IDP**.
- 3 In the **Switch active provider** window, select **Proceed**.

After that you will be able to configure IDP user provider.

Set up identity provider

Before configuring IDP in [my.anydesk II](#), you need to set up your identity provider first. You can use any third-party identity provider that supports OpenID Connect, such as Microsoft Azure Active Directory.

For IDP configuration in my.anydesk II, you will need the following data:

- **Client Secret.** Copy and paste the URL to the **Client Secret** field when configuring IDP Setup.
- **Application (Client ID).** Copy and paste the URL into the **Client ID** field.
- **Authorization endpoint.** Copy and paste the URL into the **Authentication URL** field.
- **Token endpoint.** Copy and paste the URL into the **Token URL** field.

Configure IDP

To configure IDP:

- 1 Sign in to [my.anydesk II](#) and go to the **Settings > Organization** page.
- 2 Scroll down to the **Import Roles** section, click **Edit** and provide the following information:
 - a **Roles DN** – type the LDAP DN where roles of this tree are saved. For example, `ou=roles,dc=example,dc=org` or `ou=finance,dc=example,dc=org`.
 - b **Redirect URI** – generated automatically when the IDP setup is completed. Copy the Redirect URI value after finishing the setup and paste it to your respective identity provider.
 - c **Client ID** – copy the **Application (Client ID)** value from your IDP and paste it here. It is used to register my.anydesk as an OIDC client with your provider.
 - d **Client Secret** – copy the **Client Secret** value from your IDP and paste it here. It is used to register my.anydesk as an OIDC client with your provider.
 - e **Token URL** – copy the **Token endpoint** value from your IDP and paste it here. It returns the access tokens, ID tokens, and refreshes tokens to the client (my.anydesk).
 - f **Authorization URL** – copy the **Authorization endpoint** value from your IDP and paste it here. It is used for authentication and authorization of my.anydesk client.
 - g **Trust Email** – turn the toggle off to let users verify their email address via my.anydesk II. Turn the toggle on to disable my.anydesk II email verification.
 - h **Backchannel Logout** – turn on the toggle to enable the support of backchannel logout by configured IDP. If enabled, the **Logout URL** field must be provided.
 - i **Logout URL** – provide the endpoint to log out users from external IDP. **Backchannel Logout** must be enabled.
 - j **Allowed Clock Skew** – provide value in seconds (the default value is *0*). It determines the acceptable skew when validating IDP tokens.
 - k **Default Scopes** – the scopes included when requesting authorization. The default is *openid*. Provide a comma-separated list of additional scopes you want to request.
 - l **Validate Signatures** – turn on the toggle to enable signature validation of configured IDP. If enabled, the **JWKS URL** field must be provided.
 - m **JWKS URL** – URL where my.anydesk II can retrieve the keys for the configured IDP. **Validate Signatures** must be enabled.
- 3 Click **Finish edit**.
- 4 After saving the identity provider, copy the assigned **Redirect URI**.
- 5 Open your identity provider and go to **Authentication**.

Note: Microsoft Azure AD identity provider is used in this example to showcase the procedure. You can use any other third-party identity provider.
- 6 Click **Add a platform**, select **Web**, and paste the **Redirect URI** you copied after saving the identity provider in my.anydesk II.
- 7 Click **Configure**.

For more information about IDP setup, see [Configure IDP](#) in Help Center.

LDAP user provider type

Note

Available for Ultimate (Cloud) license only.

The LDAP user provider refers to the protocol to synchronize or mass import users, groups, and roles from an Active Directory. An Active Directory is a database of hierarchically organized users, groups, roles, and permissions, as well as attributes for each of them (e.g., first name, group description, etc.).

The [my.anydesk II](#) management portal can connect to the Windows server-based Active Directories, and via LDAP, information can be fetched out of the Active Directory and used for the user management setup within my.anydesk.

The LDAP user provider setup consists of the following steps:

- 1 [Select the LDAP user provider in my.anydesk II.](#)
- 2 [Add Organization Certificates](#) – lists all certificates added to the organization. A certificate is a so-called PEM file that encrypts the communication between the [my.anydesk II](#) service and the Active Directory.
- 3 [Configure LDAP](#) – needs to be filled out to create a connection between my.anydesk and the Active Directory.
- 4 [Import Roles](#) – enables the possibility to import several roles from the Active directory.
- 5 [Set up LDAP Mapper](#) – enables to map roles from your organization to users in my.anydesk II. This way, you do not need to assign roles to users manually.

Select LDAP user provider

To select the LDAP user provider:

- 1 Sign in to [my.anydesk II](#) and go to the **Settings > User Providers** page.
- 2 On the opened page, select **LDAP**.
- 3 In the **Switch active provider** window, select **Proceed**.

After that you will be able to configure the LDAP user provider.

Add Organization certificate

The **Organization certificates** section lists all certificates added to the organization. A certificate is typically stored in .pem file and used to encrypt the communication between my.anydesk II and your LDAP identity provider.

To add a certificate to your organization:

- 1 Sign in to [my.anydesk II](#) and go to the **Settings > Organization** page.
- 2 Go to the **Organization certificates** section and click **Add new certificate**.
- 3 In the **Add new Organization certificate** window, paste the contents of the certificate file in .pem format.
- 4 Click **Add new certificate**.

Configure LDAP

You need to configure your LDAP-based identity provider to create a connection to [my.anydesk II](#).

To configure LDAP:

- 1 Sign in to [my.anydesk II](#) and go to the **Settings > Organization** page.
- 2 Scroll down to the **LDAP Setup** section, click **Edit** and provide the following information:
 - a **RDN LDAP Attribute** – type the name of LDAP attribute, which is used as RDN (top attribute) of typical user DN. Most often, this optional attribute is the same as the Username LDAP attribute. For example, for Windows Active Directory, it is common to use cn as RDN attribute when username attribute might be sAMAccountName.
 - b **UUID LDAP Attribute** – type the name of LDAP attribute, which is used as unique object identifier (UUID) for objects in LDAP. For Windows Active Directory, it should be objectGUID. If your LDAP server does not support the notion of UUID, you can use any other attribute that is unique among LDAP users in the tree. For example, uid or entryDN.
 - c **User Object Classes** – type all values of LDAP objectClass attribute for users in LDAP divided by comma. For example, inetOrgPerson,organizationalPerson. Newly created users will be synchronized to LDAP with all those object classes and existing LDAP user records can only be found if they contain all those object classes.
 - d **Connection URL** – paste a connection URL to your LDAP server.
 - e **Users DN** – type the full DN of the LDAP tree where your users are. This DN is the parent of LDAP users. For example, ou=users,dc=example,dc=com if your typical user has a DN like uid=john,ou=users,dc=example,dc=com.
 - f **Bind DN** – type the DN of the LDAP admin. This will be used by my.anydesk II to access the LDAP server.
 - g **Bind Credential** – type the password of the LDAP admin.
 - h **User Search Filter** – type the name of the LDAP filter used to search for users. Leave this empty if no additional filtering is needed and you want to retrieve all roles from LDAP. Otherwise, make sure the filter name starts with (and ends with), for example, (filtername).
 - i **Batch Size** – type the number of LDAP users that should be imported from LDAP to my.anydesk II per transaction.
 - j **Periodic Full Sync** – turn on the toggle to perform periodic full synchronization of LDAP users to my.anydesk II. If enabled, the Full Sync Period field must be provided.
 - k **Full Sync Period** – enter the time (in seconds) that should pass before my.anydesk II attempts to synchronize with the LDAP server again. Periodic Full Sync should be enabled.
 - l **Periodic Changed Users Sync** – turn on the toggle to perform periodic synchronization of changed or newly created LDAP users. If enabled, the Changed Sync Period field must be provided.
 - m **Changed Sync Period** – enter the time (in seconds) that should pass before my.anydesk II requests the LDAP server for changed or newly created LDAP users. Periodic Changed Users Sync should be enabled.
- 3 Click **Finish edit**.

Afterwards, all (potentially filtered) users from your LDAP server will be able to sign in to [my.anydesk II](#) with SSO using the organization's ID.

Import roles

You can import roles to [my.anydesk II](#) from your LDAP server. This way, you do not need to assign roles to users manually.

To import roles:

- 1 Sign in to [my.anydesk II](#) and go to the **Settings > Organization** page.
- 2 Scroll down to the **Import Roles** section, click **Edit** and provide the following information:
 - a **Roles DN** – type the LDAP DN where roles of this tree are saved. For example, ou=roles,dc=example,dc=org or ou=finance,dc=example,dc=org.
 - b **Role Name LDAP Attribute** – type the name of the LDAP attribute that is used in role objects for the name and RDN of the role. Usually, it will be cn. In this case typical role object may have DN like cn=Group1,ou=groups,dc=example,dc=org or cn=role1,ou=finance,dc=example,dc=org.
 - c **Role Object Class** – type the object class(es) of the role object. If more classes are needed, please separate them with commas. In a typical LDAP deployment, it would be groupOfNames. With Windows Active Directory, it is usually group.
 - d **LDAP Filter** – enter a custom filter to query for specific LDAP roles. Leave this empty if no additional filtering is needed and you want to retrieve all roles from LDAP. Otherwise, make sure the filter name starts with (and ends with), for example, (filtername).
 - e **User Roles Retrieve Strategy** – select one of the following ways of retrieving user roles:
 - **Load roles by 'member' attribute** – roles of users will be retrieved by sending an LDAP query to retrieve all roles where 'member' is the user.
 - **Get roles from user 'memberOf' attribute** – roles of users will be retrieved from the 'memberOf' attribute of the user or from the Member-Of LDAP Attribute.
 - f **Membership Attribute Type** – there are 3 different options that are dependent on the User Roles Retrieve Strategy:
 - **DN** – only available with the User Roles Retrieve Strategy – Load roles by role 'member' attribute. LDAP role has its cn members declared in form of their full DN. For example, member:uid=john,ou=users,dc=example,dc=com.
 - **UID** – only available with the User Roles Retrieve Strategy – Load roles by role 'member' attribute. LDAP role has its groupOfNa members declared in form of pure user uids. For example, memberUid:john.
 - **memberOf** – only available with the User Roles Retrieve Strategy – Get roles by role 'memberOf' attribute. It specifies the name of the LDAP attribute on the LDAP user that contains the roles the user is a member of. By default, it is 'memberOf'.
- 3 Click **Finish edit**.

Set up LDAP mapper

There are certain predefined *User-attribute-ldap-mappers* to ease up the setup procedure. These mappers make sure that user-specific attributes are correctly mapped. They include:

- Username
- Lastname

- Firstname
- Createtimestamp
- Modifytimestamp
- Email

User accounts creation and invitation

As a license administrator, you can add users to your organization or invite users to your team, depending on the license you have.

Note

For the Ultimate (Cloud) license, you can create users manually only if you set your user provider type to **Admin**. To learn how to manage user providers, see [Admin user provider type](#) in this document.

Create users

Multiple users that are assigned to your Ultimate (Cloud) license are called an organization. You can create users in [my.anydesk](#) and this way add them to your organization.

To create a user:

- 1 Log in to [my.anydesk II](#) with your administrator account and navigate to **Users**.
- 2 On the opened page, click **Create User** and in the pop-up window, enter the user's first and last names and provide their email.
- 3 Click **Create**.

The user will receive an email to verify their email address. After verification, the user can sign in to [my.anydesk II](#) using the organization ID which was provided in the email. You can also create multiple users at once.

To create multiple users:

- 1 Log in to [my.anydesk II](#) with your administrator account and navigate to **Users**.
- 2 Click **Create User** and in the pop-up window, click **Advanced**.
- 3 On the next page, type the email addresses of users you want to add into the text box.
Note: You can also drop a CSV with a list of users into the text box.
- 4 Click **Proceed**.

All users will receive an email to verify their email addresses. After verification, users can sign in to [my.anydesk II](#) using the organization ID which was provided in the email.

Invite users to your team

Multiple users that are assigned to your Standard or Advanced license are called a team. You can invite users to join your team.

The user invitation can go one of the following ways:

- The user does not exist yet and is created via invitation.
- The user already exists and is reassigned to the new license. If the invitation is accepted, a user is now part of the team.

To invite users to your team:

- 1 Log in to [my.anydesk II](#) with your administrator account and navigate to **Users**.
- 2 On the opened page, click **Invite User** and in the pop-up window, enter the user's first and last names and provide their email.
- 3 Click **Invite**.

After that, the user will receive an invitation email to their email address with a request to join your team.

User management

In [my.anydesk II](#), after you add or invite users to your license, you can manage users, assign roles to them and grant permissions on what they can do and see within **my.anydesk II** management portal.

Manage users

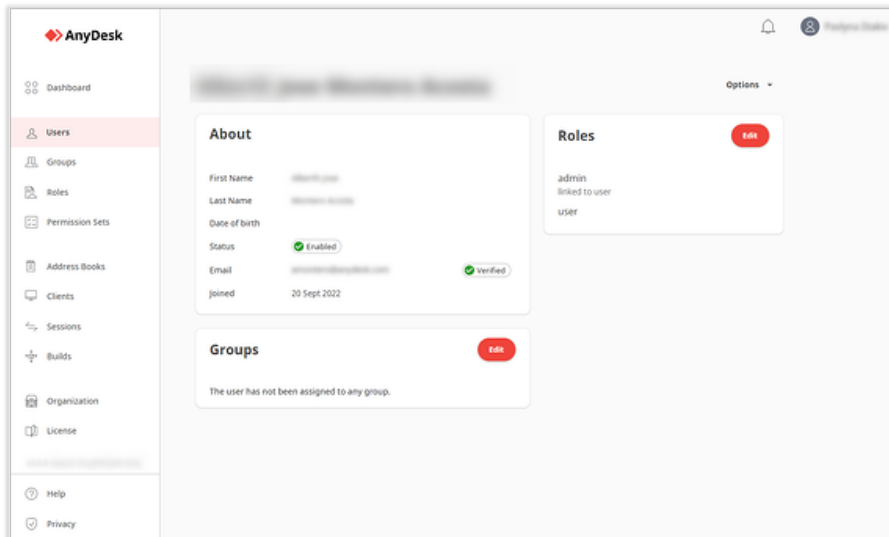
Note

Available for Standard, Advanced, or Ultimate (Cloud) license.

You can view the detailed information of each user when opening the user overview page. As an Admin, you can edit, delete, add new users, and assign different roles to the users and add them to groups.

To open the user overview page:

- In [my.anydesk II](#) account, go to **Users** and open the needed user from the list.



You can also delete or disable the user by clicking **Options** in the upper-right corner of the page and selecting either **Delete User** or **Disable User** depending on what you need.

By *deleting a user*, you also delete their personal address book. This action cannot be reversed.

If you *disable a user*, the user will no longer be able to log in and access [my.anydesk II](#).

Users can be disabled or deleted by administrators or users with the appropriate permissions.

Manage user roles

Note

Available for Advanced and Ultimate (Cloud) licenses only.

User roles are entities that contain one or more permission sets. You can assign a role with different permission sets to a user or a group. Depending on the role the user is assigned to, user can either only view, view and edit, or have no access at all to different sections of [my.anydesk II](#) management portal.

In [my.anydesk II](#) management portal, there are the following preconfigured roles for the *Ultimate (Cloud)* license:

- **Owner** - a role is designed for a license owner. With this role, they can view and edit every section of the management portal and delete the Organization.
- **Admin** - a role that allows the user to view and edit all the sections of the management portal except for *License, Invoices, and personal profile*.
- **Support agent** - a role that allows the user to view the *Users, Groups, Address Books, and Clients* sections of my.anydesk II management portal. It is designed for IT support staff.
- **Accountant** - a role for a person within your organization that deals with invoices. The role grants the access to only view the *Organization, License, and Invoices* sections.
- **Data protection officer** - a role that allows the user to view all the sections of my.anydesk II management portal except for *Builds* and *personal profile*.
- **User** - the default role for every user. With this role, they can view and edit their *personal profile* and view the *Clients* and *Builds* sections.

In the table below, can check the roles available for Ultimate license and the permissions each role has in [my.anydesk II](#).

my.ad sections	Roles					
	Owner	Admin	Support agent	Data protection officer	Accountant	User
Personal profile	view & edit	x	x	x	x	view & edit
License	view & edit	view	x	view	view	x
Invoices	view & edit	view	x	view	view	x
Users	view & edit	view & edit	view	view	x	x
Roles	view & edit	view & edit	x	view	x	x
Groups	view & edit	view & edit	view	view	x	x

Permission Sets	view & edit	view & edit	x	view	x	x
Address Books	view & edit	view & edit	view	view	x	x
Clients	view & edit	view & edit	view	view	x	view
Sessions	view & edit	view & edit	x	view	x	x
Builds	view & edit	view & edit	x	x	x	view
Organization	view & edit	view & edit	x	view	view	x

You can also create custom permissions and roles. It is recommended to grant the minimum permissions needed. For more information on user and role management setup, see [this page](#).

Manage groups

Note

Available for Ultimate (Cloud) license only.

Individual users can be organized and segmented by roles and groups. These two segmentation tools can be created manually or via mappers and importers through the user provider setup.

If you want to assign roles to several users, you can do that by creating a group. Groups are a list of users with the same permission sets. You can create a group with one or multiple roles assigned to it, and then add users to that group. This way, all members of the group will have the same roles. A user can be part of multiple groups.

To create a new group:

- 1 In [my.anydesk II](#) account, go to **Groups**.
- 2 Click **Create group** and in the pop-up window, provide the following information:
 - a **Group name** - type the name for your group.
 - b **Description** - type a short description for the group.
- 3 Click **Save group**.

After that, you can add users to the group and assign roles to it.

Manage permission sets

Note

Available for Ultimate (Cloud) license only.

Permission sets are sets of grants that define what users can see and do within **my.anydesk II** management portal. It is used to restrict access to **my.anydesk II** features and pages for certain users. This means that permission sets are used to give administrators the ability to restrict and monitor other users' access to features and pages.

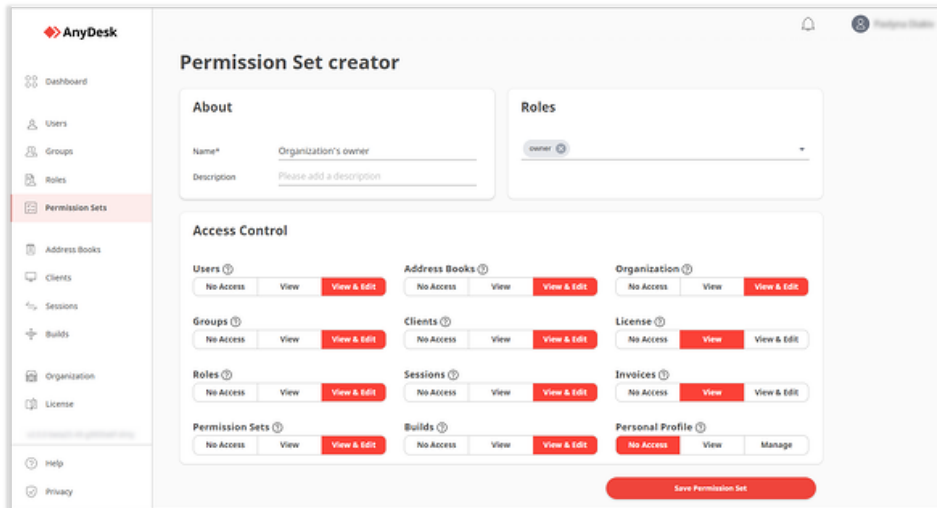
Multiple permission sets can be assigned to a single role.

Multiple roles can be assigned to groups or users. Permissions cannot be taken away once they are assigned.

You can view the list of all permission sets by navigating to the **Permission Sets** tab.

To create a permission set:

- 1 In [my.anydesk II](#) account, go to **Permission Sets** and click **Create Permission Set**.
- 2 On the opened page, provide the following information:
 - a **Name** – type the name for your permission set.
 - b **Description** – type a short explanation of the permission set.
 - c **Roles** – from the drop-down list, select roles to which you wish to assign this permission set.
Note: You can also assign a permission set to a role later in the **Roles** section.
 - d **Access Control** - for each section, select either **No Access**, **View**, or **View & Edit** depending on what you want users within the assigned role to have access to.



- 3 Click **Save Permission Set**.

Address Books


Address Book is a list of your contacts (devices you connect to). By adding tags to contacts, you can filter the devices.

Each user has a personal Address Book. If the user is a part of an organization or a team, they can also have access to organization's/team's Address Book. Organization's or team's Address Books can be summarized as shared Address Books. The shared Address Book can be visible to all licensed users.

The personal Address Book is an address book that is directly linked to a user account. This means that only the owner of the personal address book can view and edit it. The personal Address Book is automatically created after every user account creation.

Address Books are synchronized with the AnyDesk client. Whenever you make changes to the contacts or the Address Book itself in the [my.anydesk II](#) management portal or the AnyDesk client, it will be updated across both platforms.

To access the personal address book in [my.anydesk II](#), go to the **Address Book** section and select the **Personal** tab. You can add and edit Address Book entries and set and delete tags.

To access the address book in the AnyDesk client, in the upper-right corner of the client, click  > **Address Book**.

Clients management

A client is an AnyDesk application installed on your device. Within [my.anydesk II](#) management portal, you can view, filter, and manage clients that are linked to your license.

To access clients:

- Log in to [my.anydesk II](#) with your administrator account and navigate to **Clients**.

Here, you can see details of the clients deployed and assigned to your license.

Clicking on one of the clients will display the client details. Here, you can remove the client from the license, change the Alias, and view the session history.

Custom Clients

Note

Available for Standard, Advanced, and Ultimate (Cloud) licenses.

AnyDesk offers two types of clients (applications) that you can install on your devices:

- **Default AnyDesk client** – an AnyDesk application with default settings and configurations available to all users. You can download it from our [website](#).
- **Custom AnyDesk client** – an AnyDesk application fully customized by the user in [my.anydesk II](#) management portal using *Custom Client Generator*. You can customize the settings and permissions of the application according to your needs.

The **Custom Client Generator** in [my.anydesk II](#) management portal provides a wide range of possibilities to customize the AnyDesk application to fit individual needs.

You can access the **Custom Client Generator** by going to the **Builds** tab and clicking **Create Build**. On the opened page, it is split up into six sections:

- **OS** – defines for which operating system the client is meant for.
- **General** – defines naming and the most common features.
- **Visual** – defines the application icon and custom texts.
- **Security** – defines the access control list and proxy server.
- **Advanced** – input fields to enter further key values. Differentiates overwrite & default.
- **Session Permission Profiles** – defines the session permission profile presets.

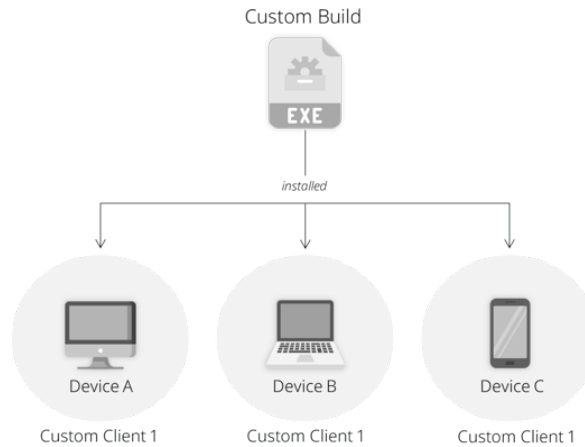
In our Help Center, you can find further information on [how to create custom clients](#) and [install](#) them.

The following configuration options for custom AnyDesk clients are supported:

- [Mobile Device Management](#)
- [Windows Group Policies](#)
- [Command Line Interface](#) (Windows, Linux, macOS)


Builds overview


Builds are custom clients, or custom AnyDesk applications, which you can create using the Custom Client Generator. It can be installed on one or multiple devices. This ensures that each device within your organization will have an AnyDesk client configured to your needs.

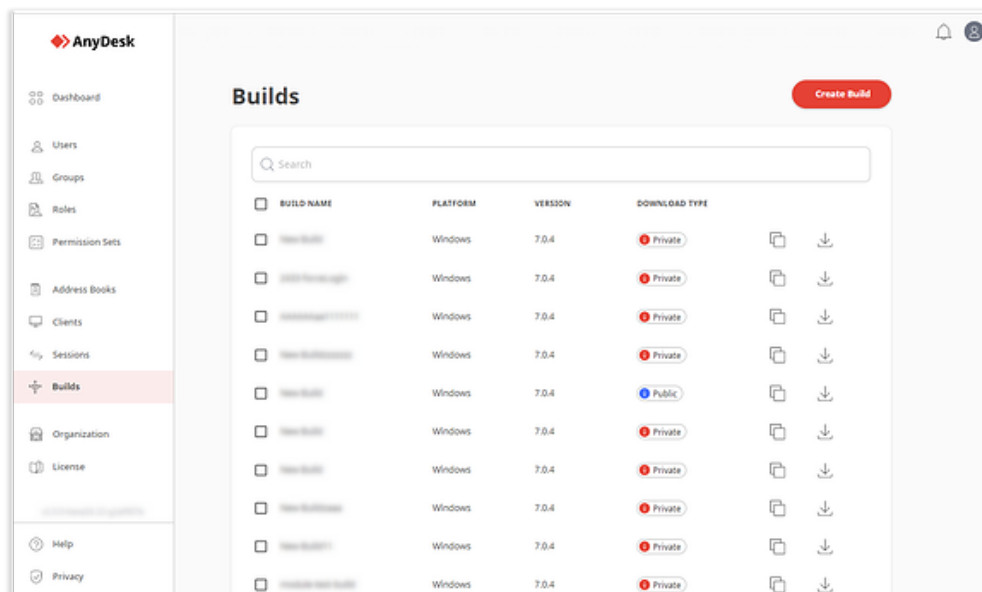


You can view all builds that you created, or others in your license that have the permission to do so, in the **Builds** tab. On the **Builds** page, view the following information for each configuration:

- **Build name** – the name of the created build.
- **Platform** – the operating system for which the build was created.
- **Version** – the version number of the created build.
- **Download type** – a type of the download link for the build. It can be either Private or Public.

You can copy the URL of that custom client configuration by clicking  and then share it with others. If the **Download type** is *Private*, then people using the URL will need to log into an account linked to your license to download it. If the **Download type** is set to *Public*, then anyone with the link can download that custom client.

To download the custom client with that configuration to your device, click .



Builds overview page

Manage Builds

Once you have created a Build (Custom Client), you can share it with your colleagues and install it on one or multiple devices. This means that the build can have multiple clients linked to it.

If you want to adjust the settings of all clients linked to the build, such as security settings, add or remove access to certain features, you can easily do that in [my.anydesk II](#).

Changes to build can be applied in two ways, depending on the build type you selected during creation. There are two types of builds:

- **Static** – a build that requires client reinstallation on every device after each customization.
- **Dynamic** – a build that can be customized in real-time without the need to reinstall it on all devices after each change. Updates will instantly apply to all linked clients. To use the dynamic builds, you need to [Activate Central Management](#) first.

For detailed instructions on how to make changes to the builds, see [this article](#) in our Help Center.

Central Management

Central Management allows you to quickly adjust client settings in real time. This means that you can customize already installed clients from [my.anydesk II](#) and see the changes in clients right away, without reinstalling them. For more information about Central Management, see [this article](#) in Help Center.

The feature is useful for IT admins who provide support to their colleagues in their organization and need effortless client customization in real time.

With Central Management you get access to the following features:

- **Dynamic Builds** – make changes to the specific Build and those changes will automatically apply to all clients linked to that Build.
- **Dynamic Client Configuration** – ability to edit individual clients dynamically and manage their set of features.

All changes made from [my.anydesk II](#) to authorized clients are securely signed using a Private Key.

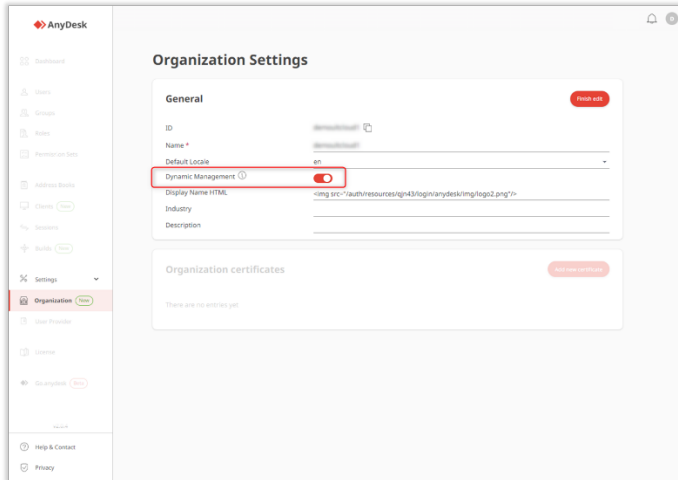
To unlock all Central Management features, first, you need to generate a Private Key, download and copy it, and then provide the Private Key in [my.anydesk II](#) after every login when you want to use the features. For more information about the Private Key, see [this article](#).

Activate Central Management

To activate Central Management:


- 1 Log in to [my.anydesk II](#) and go to the **Organization**.

- 2 In the **General** section, click **Edit** and then turn on the **Dynamic Management** toggle.



- 3 Go to **Dashboard**, click **Generate Private Key**.
- 4 In the **Save Private Key** window, download and copy the **Private Key**, select the checkbox, and then click **Continue**.

Note: The Private Key is only generated once and cannot be recovered if lost. Please make sure it's securely stored.
- 5 Go to the **Activate Client Management** window, click **Provide Private Key**.
- 6 In the opened window, paste the **Private Key** and click **Continue**.

After the Central Management was successfully activated, you will see  in the upper-right corner of the **Dashboard**. You will need to provide the Private Key each time you log in to my.anydesk.it and want to use Central Management features.

License management

You can manage your current license in my.anydesk.it management portal.

To access license management:

- 1 Log in to my.anydesk.it with your administrator account and navigate to **License**.
- 2 On the opened page, you can do the following actions:
 - a Upgrade license
 - b Reset license key
 - c Edit billing information
 - d Add, remove, and manage payment methods
 - e Activate or deactivate auto-renewal
 - f Download and pay invoices

my.anydesk API

my.anydesk REST-API can be used to retrieve and export license and client information from your my.anydesk account. The API is currently available for my.anydesk I. A new API for [my.anydesk II](#) with extended functionality is currently being developed.

For more information about API, refer to this [article](#) in Help Center.

my.anydesk I

[my.anydesk I](#) is our legacy customer portal. It is still available for customers to use. The [my.anydesk I](#) portal does not include user management. Only a single account can be created there.

Note

Configurations for custom clients done in [my.anydesk I](#) will not be synced to my.anydesk II. [my.anydesk I](#) management portal will eventually be discontinued.

When purchasing AnyDesk license, you will receive two emails with credentials to both management portals. Open the **Your AnyDesk Credentials** email and find there your username and password for [my.anydesk I](#).

Once logged in to your [my.anydesk I](#) account, you have five main tabs:

- **License:** View your license details, such as license key or expiration date and manage your license.
- **Clients:** View all licensed AnyDesk clients deployed on devices. Change their Alias, remove them from your license, or leave a comment.
- **Sessions:** View session history, view and edit session comments, end active sessions, and export the information.
- **Files:** View the list of your custom AnyDesk clients. You can also create new custom clients here.
- **Settings:** Change your general settings, payment options, customer, and company information. View and pay your invoices.

More information and helpful guides for the [my.anydesk I](#) portal can be found in our [Help Center](#).



About **AnyDesk**

AnyDesk is a remote desktop software that allows users to access and control a computer from a remote location. It was first released in 2014 and has since gained popularity as a reliable and secure remote desktop solution.

Resources

[Learn more about how to get started with AnyDesk in our Help Center](#)

[Watch our tutorial videos on how to use AnyDesk](#)

[Discover interesting use cases](#)

Join our community

