AnyDesk

Security Best Practices

User Guide

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**

my.anydesk II **5**

Permission and user management 5

Two-factor authentication for my.anydesk II 6

AnyDesk Custom Client **8**

Incoming- and outgoing-only clients 8

Settings 8

Access Control List and custom Namespace 10

Permissions for the connection 11

Unattended Access 12

Two-factor authentication for Unattended Access 12

Force user login 12

Use Case **13**

AnyDesk setup for remote support 13

Incoming-only client 13

Outgoing-only client 14

Revision history

Date	Version	Description
March 14th, 2024	2.0	Updated the whole document.
August 1st, 2023	1.1	Updated the ***Example Use Case*** chapter.
March 3rd, 2023	1.0	Initial publication.

Document Overview

This guide is tailored for IT administrators and users alike, offering practical advice on optimizing AnyDesk setup for heightened security.

The document consists of the following chapters:

- my.anydesk II – learn the basic roles and permissions that can be assigned to users.
- AnyDesk Custom Client – learn how to configure custom AnyDesk clients to make them more secure.
- Use Case – check the example setup of custom AnyDesk client.

my.anydesk II

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 and IDP 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.

Permission and user management

After purchasing the license, sign in to my.anydesk II management portal and add users to your license. Once you have added all users, 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.

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.

In my.anydesk II management portal, there are the following preconfigured roles for the Ultimate 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

Note

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.

Two-factor authentication for my.anydesk II

You can add another layer of security by setting up a two-factor authentication for **my.anydesk** account. When signing into your account, you will have to provide your login, password, and an additional security code.

Note

Before activating the two-factor authentication, you should first download an authenticator app to your mobile device. The recommended apps are Google Authenticator or Microsoft Authenticator.

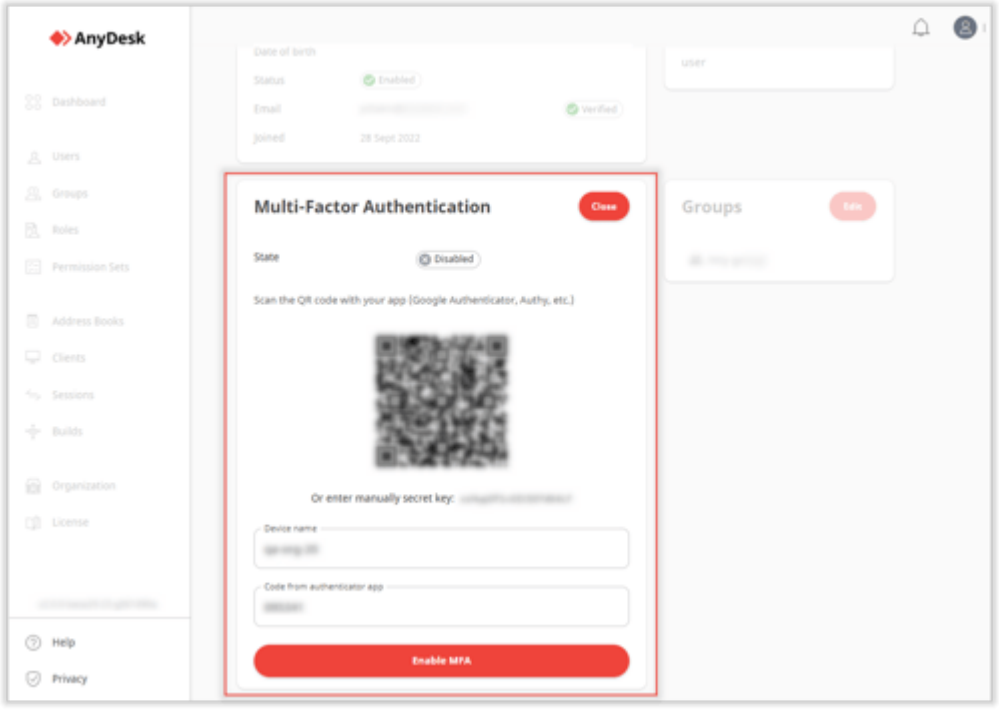
To activate two-factor authentication:

1. Sign in to my.anydesk II with your AnyDesk account credentials.
2. In the upper-right corner of the page, click your name and then select **My profile**.
3. In the **Multi-Factor Authentication** section, click **Edit**.

4 Open the authenticator app on your mobile device, scan the QR code and do the following:

a Specify the **Device Name**.

b Enter the **Code from authenticator app**.



5 Click **Enable MFA**.

AnyDesk Custom Client

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. You can customize the settings and permissions of the application according to your needs.

For more information on customizing the AnyDesk client, see this page.

Incoming- and outgoing-only clients

Depending on the users' need, you can set your AnyDesk client to be one of the following:

- **Incoming-only** – a client that can ***only receive*** a connection from another device.
- **Outgoing-only** – a client from which you can ***only create an outgoing connection***.
- **Bidirectional** – a client from which you can create connections to another device and receive incoming connection requests to your device.

To streamline the process for IT Support, Admins, and other personnel who use AnyDesk for device connections, it is recommended to configure ***outgoing-only AnyDesk clients***. This approach is particularly beneficial because IT Support typically does not require incoming connections from external sources. Since they only need to connect to employees' devices, this prevents incoming connection requests, making the process more secure and efficient.

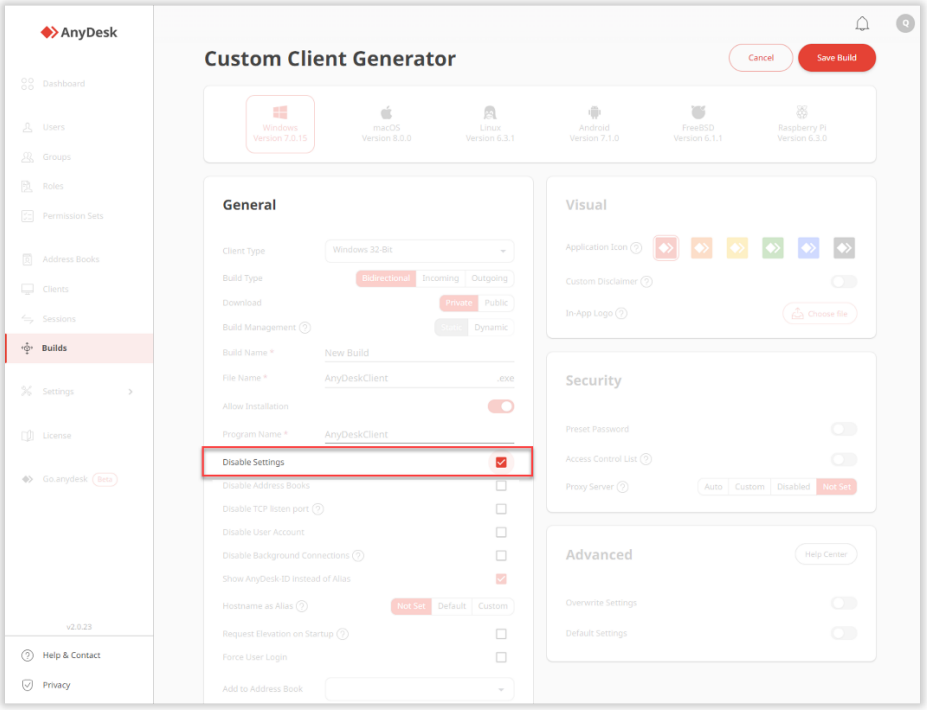
In contrast, the employees who receive support should have an ***incoming-only AnyDesk client***. This way, you ensure that no connection can be established from the employees devices. For more information, see this page.

Settings

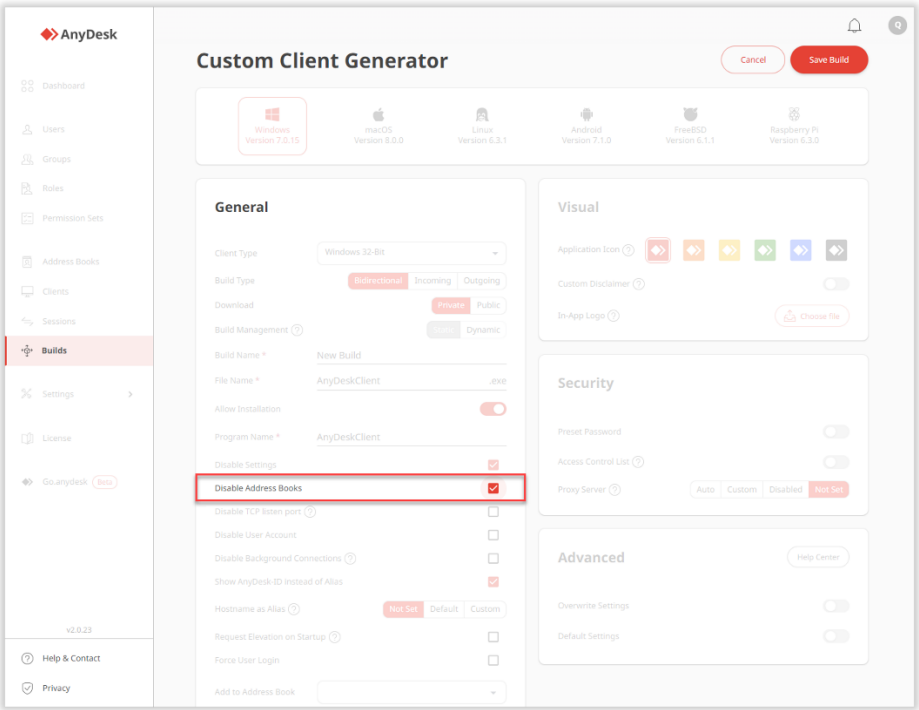
The security and connection settings in the AnyDesk client are secured by User Account Control (UAC) and require administrative rights to be modified. However, you can preset and locked so that the user cannot change any settings within the AnyDesk client after installation.

When creating a custom AnyDesk client in my.anydesk II management portal, it is recommended to disable access to the following section of AnyDesk client:

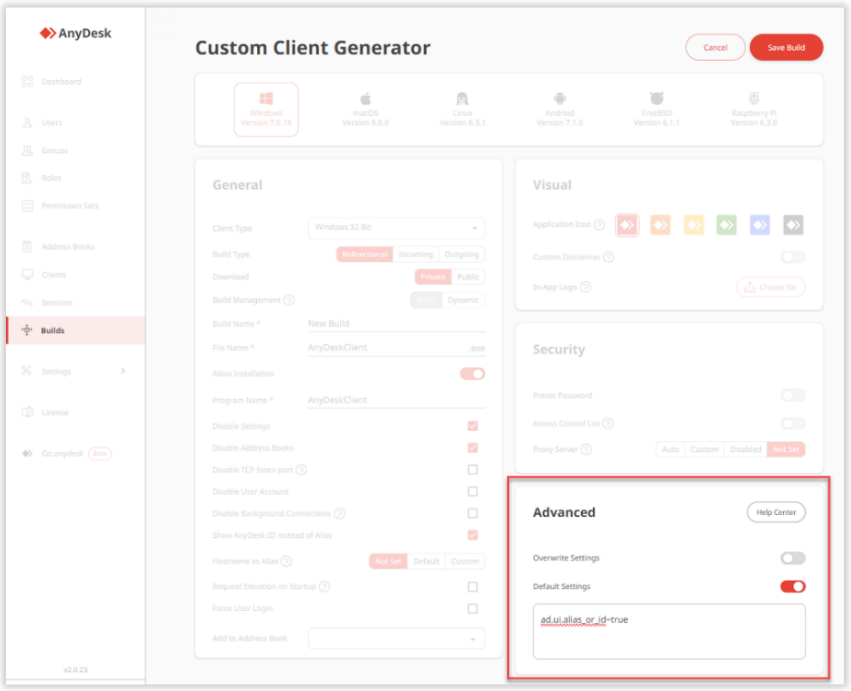
- **Settings**. It is recommended to disable the access to settings in the client since there is no need to modify the AnyDesk client when it is already installed. Only if two-factor authentication is to be set up,



- **Address Book for incoming-only clients**. Disable the Address Book for clients that are going to be installed on devices that only receive connections.



- **Specific categories**. You can disable specific features or sections of AnyDesk client by adding key values in the *Advanced* section. A list of all key values available can be found here.



Access Control List and custom Namespace

With the **Access Control List**, you can ensure that the device can only receive connection requests from whitelisted AnyDesk clients. The Access Control List should be applied to any AnyDesk client that will receive connections.

To connect to remote devices with AnyDesk, you need to know the ID or Alias (AnyDesk Address) of the remote device. AnyDesk Alias consists of your device's username and a Namespace, for example, *John@ad*.

The default Namespace is *@ad*, referring to **A**ny**D**esk, and it is assigned to all users who have installed the AnyDesk application. AnyDesk portable (not installed) only has an ID.

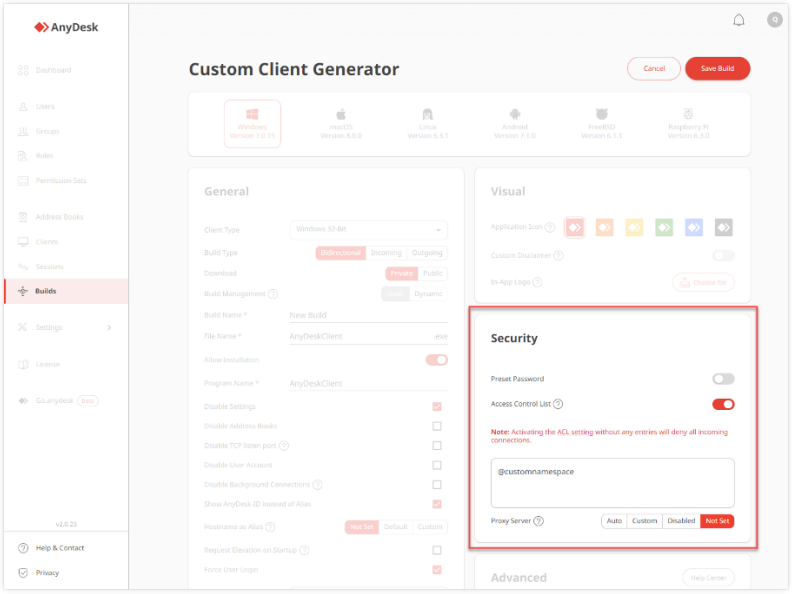
The custom Namespace option allows you to specify an individual name available only to you, for example, *YourName@CompanyName*. By having a custom Namespace allows to whitelist the entire Namespace over a wildcard (**@namespace*).

Your personal AnyDesk domain enhances device identification and security. You may whitelist the custom namespace in the Access Control List settings and only devices registered to your Namespace will be able to connect to you.

To set up Access Control List:

1. In the **Custom Client Generator**, go to **Security** section and turn on the **Access Control List** toggle.
2. In the text field, provide the list of clients that are allowed to connect to this custom client. You can provide just your custom namespace (*e.g., @companyname*) and

only users inside your organization will be able to request a connection.

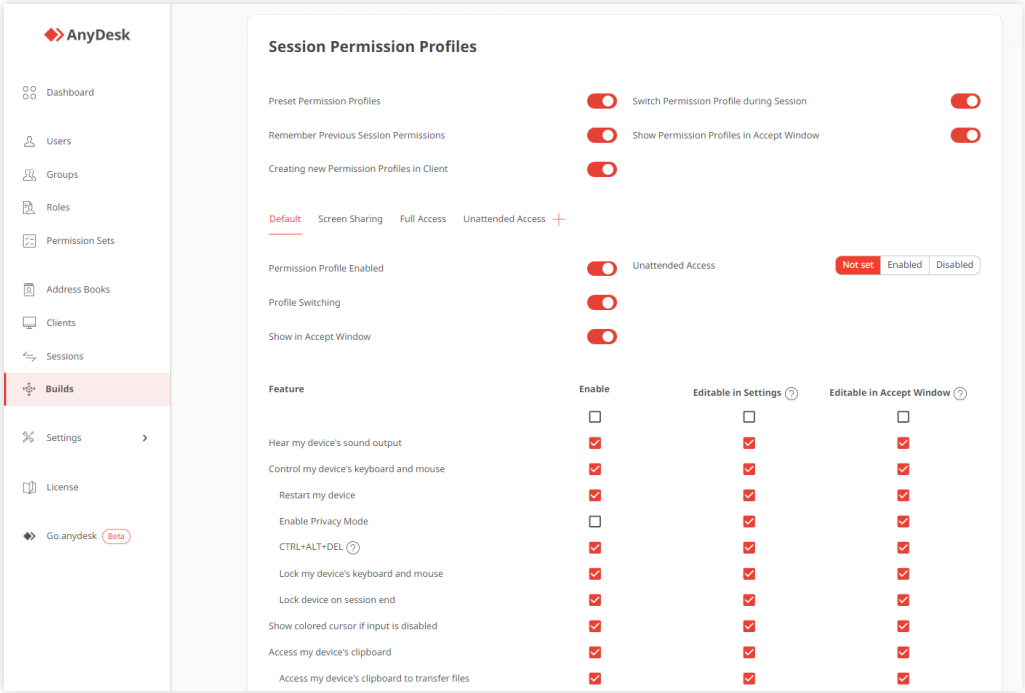


Permissions for the connection

You can control what the user who is connecting to the remote device can access on the remote device.

To access session permission management:

- In the **Custom Client Generator**, go to **Session Permission Profiles.**



The profiles are set for the AnyDesk client on the remote device, not the AnyDesk client used to connect.

It is recommended to delete all existing profiles and set up a custom one if none of the preset profiles fit the needs. For more information on Permission Profiles, see this page.

Unattended Access

Unattended Access should only be granted for devices that are monitored or if the remote work / home office use case applies to connect using a password.

> **Note**
>
> It is not needed to set up Unattended Access if a user is in front of the device whenever a connection might be required.

Passwords for Unattended Access are set on a permission profile basis, allowing to create multiple permission profiles with different passwords to grant different levels of access and permissions depending on the connecting personnels' needs. For more information on Unattended Access, see this page.

Two-factor authentication for Unattended Access

A two-factor authentication can be added to Unattended Access to secure access over password. When connecting to the remote device using Unattended Access, you will be asked to provide an Unattended Access password and an additional security code.

To set up 2FA, any common authenticator app like Microsoft Authenticator or Google Authenticator can be used. Setup must be done locally in Settings of the AnyDesk client. For more information on how to set up 2FA for Unattended Access, see this page.

Force user login

It is advised to enable the **Force user login** option for AnyDesk clients that will be used to create connections to remote devices. This feature ensures that every employee who has to establish remote connections will have to log in to their account in the AnyDesk client. If an unauthorized person gets access to a device with the AnyDesk client, they will not be able to connect to other devices in this case.

To use this functionality, all employees who are supposed to initiate connections need to have my.anydesk II account.

Use Case

To demonstrate possible configurations with the above-mentioned options, see the remote support use case below.

> **Note**
>
> The example is only to visualize a possible configuration. Permissions and access should always be given considering the specific use case. If you need assistance setting up the perfect configuration for your company, please reach out to us.

AnyDesk setup for remote support

The requirements for the remote support use case are the following:

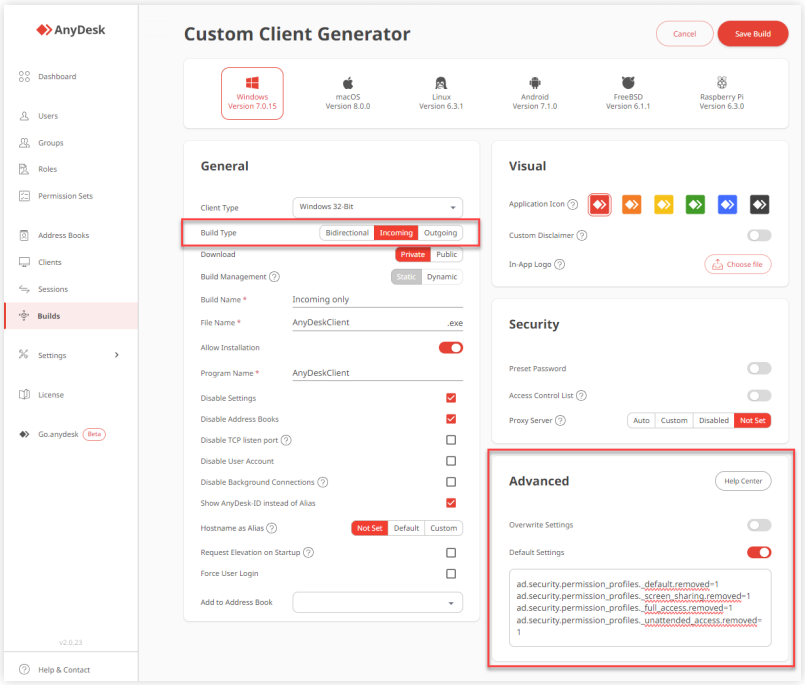
- Incoming-only AnyDesk client for all end users.
- Outgoing-only AnyDesk client for IT support staff.
- my.anydesk II accounts for all IT support staff.
- Access Control List with custom Namespace.

Incoming-only client

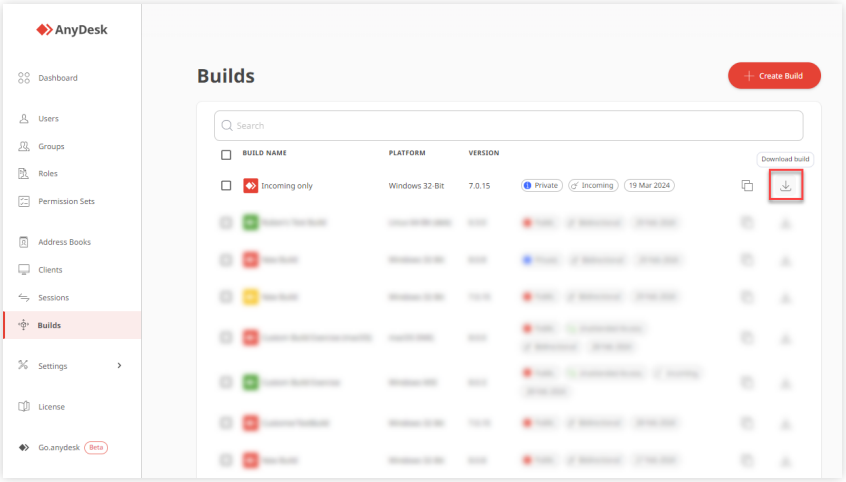
To create an incoming-only AnyDesk client:

1. Sign in to my.anydesk II and go to the **Builds** tab.
2. Click **Create Build** and provide the following information:
   a. Select the operating system.
   b. In the **Build Type** field, select **Incoming**.
   c. In the **Advanced** section, remove the preconfigured permission profiles by adding the following key-values:

```
ad.security.permission_profiles._default.removed=1
ad.security.permission_profiles._screen_sharing.removed=1
ad.security.permission_profiles._full_access.removed=1
ad.security.permission_profiles._unattended_access.removed=1
```



3 Click **Save**, download the build, and install it on all end users' devices.



Outgoing-only client

To create an outgoing-only AnyDesk client:

1 Sign in to my.anydesk II and go to the **Builds** tab.

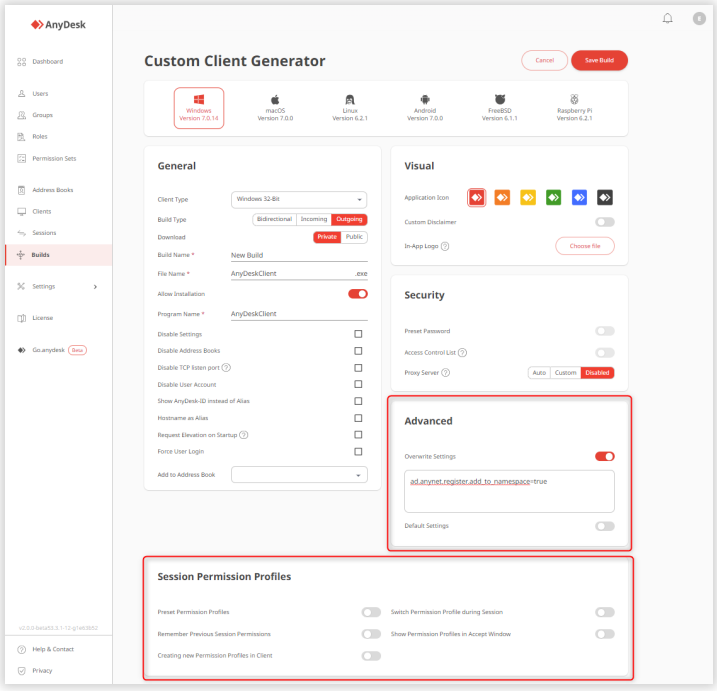
2 Click **Create Build** and provide the following information:

- **a** Select the operating system.
- **b** In the **Build Type** field, select **Outgoing**.
- **c** Select the **Force User Login** check box.

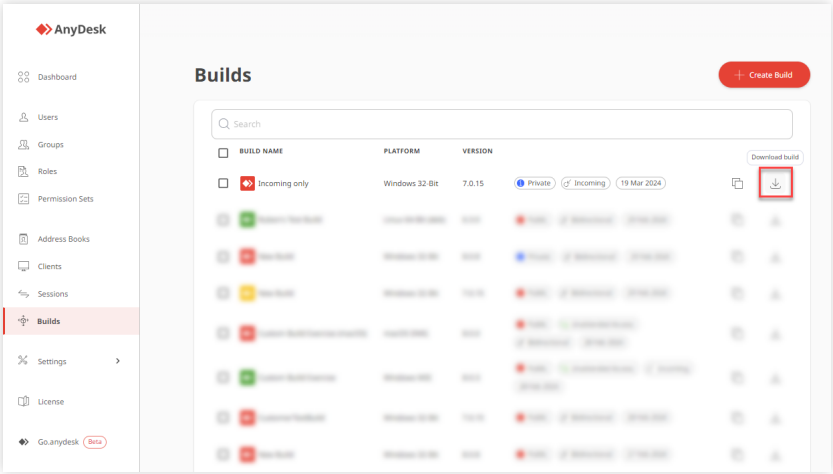
d In the **Advanced** section, add the following key-value for automatic registration of the Alias to the custom Namespace.

```
ad.anynet.register.add_to_namespace=true
```

e In the **Session Permission Profiles**, deactivate all permissions since no incoming connection can be established.



3 Click **Save**, download the build, and install it on all end users' devices.

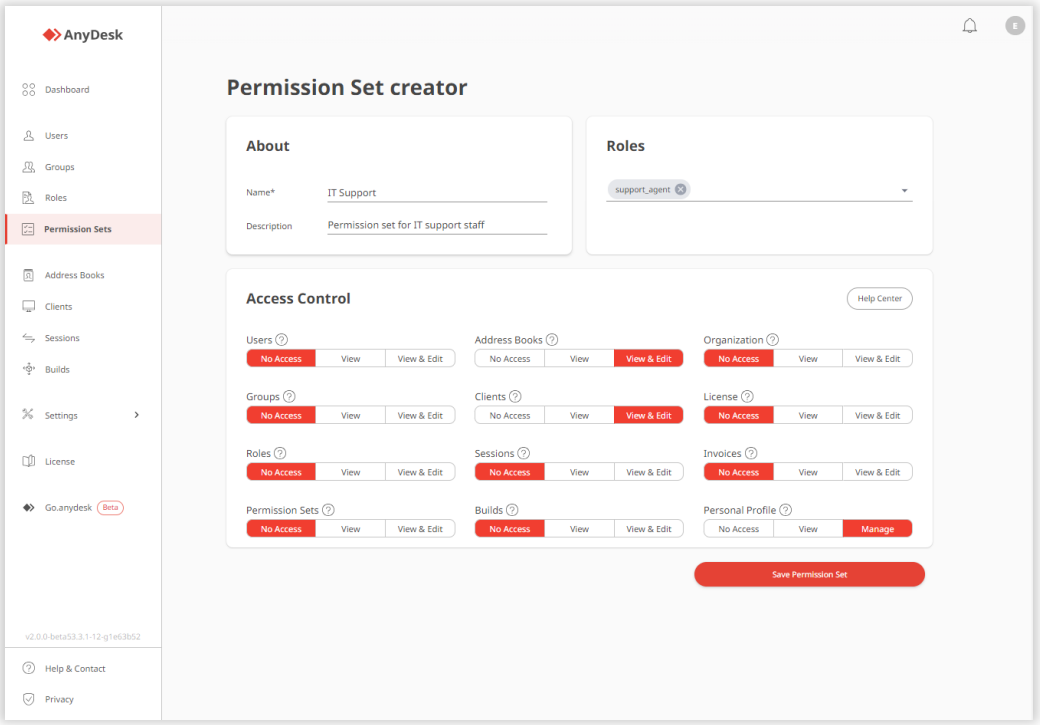


Permissions in my.anydesk II

Permissions given to users for my.anydesk II management portal vary depending on the responsibilities the employees have. In this case, we assume that the IT Support staff should have minimum access to my.anydesk II management portal as they mainly only use AnyDesk to remotely connect to end-users' devices.

The Admin or the owner of the license can create a specific permission set and assign it to the IT Support staff. As a result, the IT Support staff can have the following permissions in my.anydesk II management portal:

- View and edit the Address Books.
- View and edit the list of clients to be able to remove an AnyDesk client from the license in case a device is decommissioned, for example.
- View and edit personal profile to be able to set up two-factor authentication for the account.
- View session history, making use of session notes left by colleagues, for example.



AnyDesk

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

Copyright © 2024 **AnyDesk Software GmbH.** All rights reserved.