

AnyDesk Security Best Practises

User Guide

AnyDesk Software GmbH

Version 1.0

Legal Notice

Copyright © 2023 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

my.anydesk II management portal	4
Permission and User Management	4
Two-Factor Authentication (2FA)	5
AnyDesk Custom Client	6
Incoming and Outgoing Only AnyDesk Clients.....	6
Client Settings and Capabilities	6
Access Control List and Custom Namespace	7
Permission Profiles	7
Unattended Access	8
Two-Factor Authentication (2FA).....	8
Forced User Login.....	8
Example Use Case	9
Remote Support	9
Incoming-Only Client.....	9
Outgoing-Only Client.....	11

Revision history

Date	Version	Description
22.03.2023	1.0	Initial publication.

my.anydesk II Management Portal

Upon purchase or trial registration, your [my.anydesk II](#) account is created with the email address registered initially. This account has unrestricted access to all settings within my.anydesk II, including organization and IDP setup, but also review of connection history and other information.

It is recommended to use this account only for initial setup, and users should receive customized permissions for the portal according to their needs.

Permission and User Management

You can create a role with different permission sets and assign it to individual users or user groups. 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 user management console.

Custom permission sets and roles can also be created. It is recommended to grant the minimum permissions needed. For more information on **User Management** setup, see [here](#).

You can grant the following permissions (**No Access, View, View & Edit**) to the following sections in [my.anydesk II](#):

- Users
- Groups
- Roles
- Permission Sets
- Address Books
- Clients
- Sessions
- Builds
- Organization
- License
- Invoices
- Personal Profile

The preconfigured roles are following:

- **Accountant** – includes permission to view **Organization, License, Invoices** sections.
- **Admin** – includes permission to view and edit **Users, Groups, Roles, Permission Sets, Address Books, Clients, Sessions, Builds, Organization** sections. Includes permission to view **Invoices**.

- **Data Protection Officer** – includes permission to view **Users, Groups, Roles, Permission Sets, Address Books, Clients, Sessions, Organization, License,** and **Invoice** sections.
- **Owner** – includes permission to view and edit all options.
- **User** – includes permission to view **Clients** and **Buils** sections. Includes permission to view and edit **Personal Profile**.

Two-Factor Authentication (2FA)

If you want to add another layer of security to your AnyDesk account, you can activate multi-factor authentication. When signing into your account, you will have to provide your login, password, and an additional security code.

Common 2FA applications like the Microsoft Authenticator or Google Authenticator can be used. 2FA for the my.anydesk II profile is setup by the users themselves within **My Profile**.

AnyDesk Custom Client

AnyDesk offers the functionality to modify the functionality and capability of the AnyDesk Client before deployment, or after deployment with tools like Microsoft Group Policy and Mobile Device Management software. For more information on customizing the AnyDesk client, see [here](#).

Incoming and Outgoing Only AnyDesk Clients

Custom AnyDesk clients can support the following connections:

- Incoming only
- Outgoing only
- Bidirectional

For IT Supporters, Admins and other personnel that are supposed to use AnyDesk to connect to other endpoints, it is recommended to create **only outgoing** AnyDesk Clients if no incoming connection is needed. This ensures that no incoming connection can be requested.

In contrast, any personnel that receives support or any endpoint that is only supposed to be connected to, should have an **incoming client** only. This way, you ensure that no connection can be established from this endpoint while still applying your license to those AnyDesk Clients. For more information, see [here](#).

Client Settings and Capabilities

The AnyDesk security and connection settings are secured by UAC and require administrative rights to be modified. However, settings for the AnyDesk Client can be preset and locked so that the end-user cannot change any settings within the AnyDesk Client after deployment.

It is recommended to disable the settings as there is no need to modify the AnyDesk Client in a deployed stage. Only if 2FA is to be set up, the Security Settings need to be available.

Specific categories of settings can be disabled individually by using the Advanced Options. A list of all key values available to perform these actions can be found [here](#).

Additionally, it is recommended to disable the Address Book for Clients that are going to be deployed on endpoints that only receive connections. For more information on settings and capabilities, see [here](#).

Access Control List and Custom Namespace

With the **Access Control List**, you can ensure that the target endpoint can only receive session requests from whitelisted AnyDesk Clients. The Access Control List should be applied to any AnyDesk Client that will receive connections.

Having a custom Namespace allows to whitelist the entire Namespace over a wildcard (*@namespace). To receive an Alias within the Namespace, either a custom configuration package needs to be created that automatically assigns an Alias within the Namespace, or an Alias with the Namespace must be manually assigned in my.anydesk, in the **Clients** list.

For mass deployment, the automatic option is recommended. Only Clients that will initiate connections over AnyDesk should be part of the Namespace. For more information on the Access Control List, see [here](#).

Permission Profiles

Permission Profiles within the AnyDesk Client regulate what permissions the connecting user will have on the remote endpoint. The profiles are set for the AnyDesk Client on the remote endpoint, 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 [here](#).

It is also recommended to give the minimum permission needed

The following permissions are available:

- Hear my device's sound output
- Control my device's keyboard and mouse
- Restart my device
- Enable Privacy Mode
- CTRL+ALT+DEL
- Lock my device's keyboard and mouse
- Lock device on session end
- Show colored cursor if input is disabled
- Access my device's clipboard
- Access my device's clipboard to transfer files
- Use the file manager
- Request system information
- Draw on my device's screen

- Create TCP Tunnels
- Allow to record session

Unattended Access

Unattended Access should only be granted for endpoints 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 endpoint whenever a connection might be required.

Passwords for Unattended Access are set on a per 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 [here](#).

Two-Factor Authentication (2FA)

Additionally, a 2FA can be added to Unattended Access to secure access over password. In addition to Access Control List, which only allows access to whitelisted personnel and the password only known to those personnel, the request for a second authentication guarantees maximum security.

To set up 2FA, any common authenticator app like Microsoft Authenticator or Google Authenticator can be used. Setup must be done locally within the AnyDesk Clients Settings. For more information on 2FA setup, see [here](#).

Forced User Login

Forcing a user login is recommended for AnyDesk Clients that will be used to initiate connections. This option ensures that even if a user who is not authorized to use AnyDesk gets hold of a device that has a client installed, the user has no possibility to use AnyDesk.

To use this functionality, all employees who are supposed to initiate connections need to have a my.anydesk II account, which is used to login to the AnyDesk Client.

Example Use Case

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

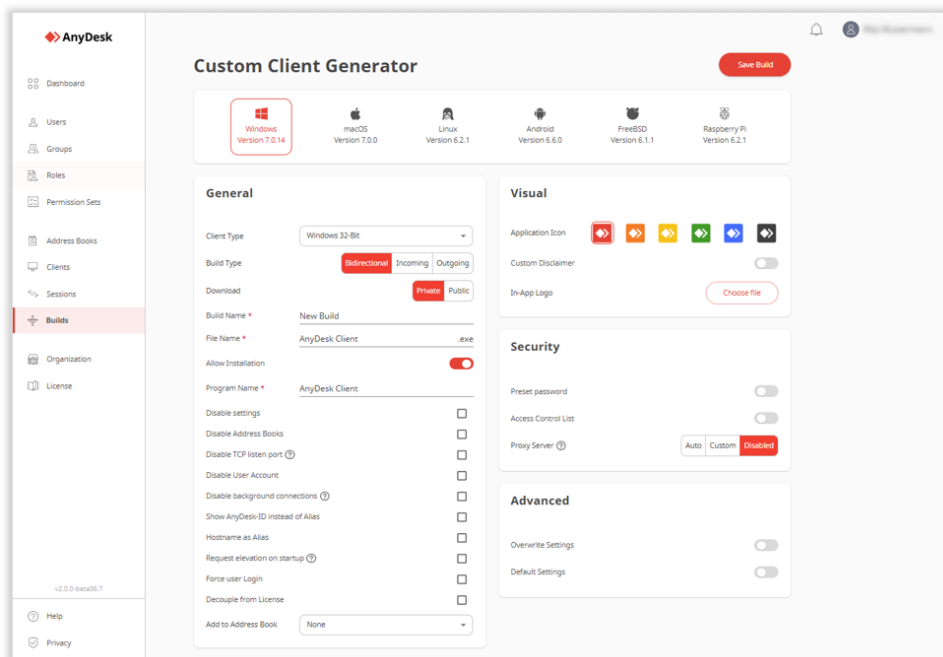
Note: This example is only to visualize a possible configuration. Permissions and access should always be given considering the specific use case. If you need assistance setting up the perfect configuration for your company, please reach out to us.

Remote Support

Requirements:

- 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 Namespace

Incoming-Only Client



Under the **Advanced** section, the following key-values to remove the preconfigured permission profiles were added:

```
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
```

Session Permission Profiles

Preset Permission Profiles Switch Permission Profile during Session

Remember Previous Session Permissions Show Permission Profiles in Accept Window

Creating new Permission Profiles in Client

Default Screen Sharing Full Access Unattended Access Profile 1 ✕ +

Permission Profile Status Unattended Access Not set Enabled Disabled

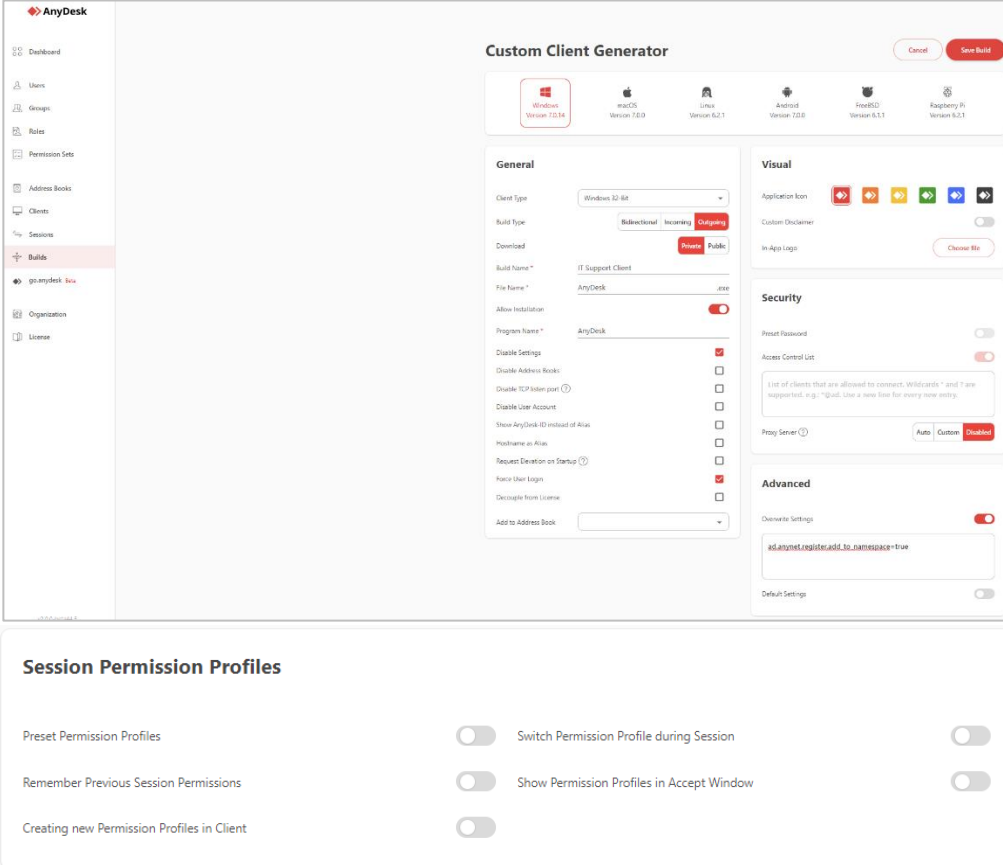
Custom Name Secure Profile

Profile Switching

Show in Accept Window

Feature	Enable	Editable in Settings	Editable in Accept Window
Hear my device's sound output	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Control my device's keyboard and mouse	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Restart my device	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enable Privacy Mode	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CTRL+ALT+DEL	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lock my device's keyboard and mouse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lock device on session end	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Show colored cursor if input is disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access my device's clipboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access my device's clipboard to transfer files	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Use the file manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Request system information	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Draw on my device's screen	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create TCP Tunnels	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Allow to record session	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Outgoing-Only Client



The screenshot shows the AnyDesk Custom Client Generator interface. The 'Outgoing' build type is selected. Under the 'Advanced' section, the key-value `ad.anynet.register.add_to_namespace=true` is entered in the 'Custom Settings' field. Below the generator, the 'Session Permission Profiles' section shows three settings: 'Preset Permission Profiles' (disabled), 'Remember Previous Session Permissions' (disabled), and 'Creating new Permission Profiles in Client' (disabled).

For the outgoing-only client, under the **Advanced** section, the following key-value for automatic registration of the Alias to the custom Namespace was added:

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

As for the permission profiles, since no incoming connection can be established those have been deactivated.

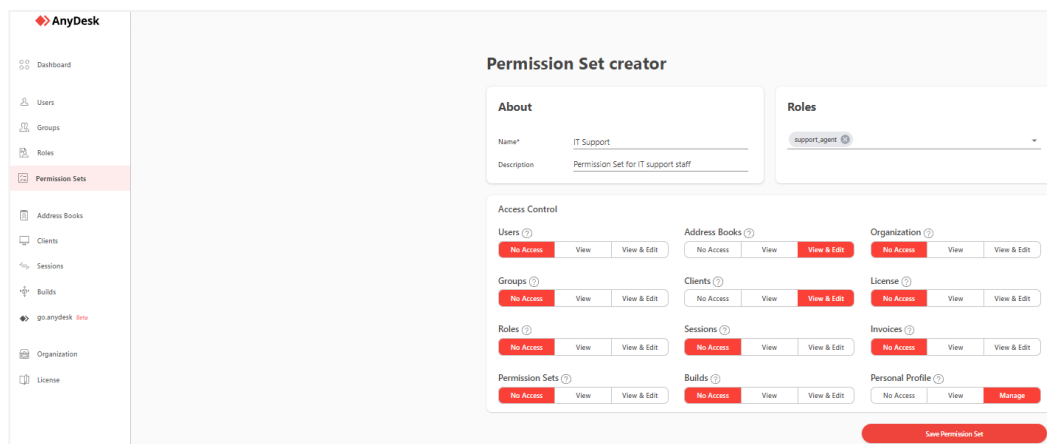
my.anydesk II Permission Sets

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

As a result, the IT supporter staff can only view and edit the Address Books, and the Clients list to be able to remove an AnyDesk Client from the license in case a device is decommissioned, for example.

Additionally, they also have access to view the session logs, making use of session notes left by colleagues, for example.

Permission to view and edit the personal profile is also given so that 2FA for the account can be set up.





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 AnyDesk features in Help Center](#)

Join our community

