Some Help With

Configure AnyDesk with your MDM tool

TABLE OF CONTENT

Supported platform packages

Configure via MDM for macOS

- PayloadContent elements
- Additional profile properties
- Deploying the profile

Configure via MDM for Android

Configure via MDM for iOS

- Configuration keys for iOS

This article explains how to deploy and configure AnyDesk in your organization using Mobile Device Management (MDM) tools like Microsoft Intune.

Supported platform packages

AnyDesk offers several deployment formats:

- Windows (`.msi` , custom client only)
- macOS (`.pkg` , custom client only)
- Android (Google Play)
- iOS (App Store)

> 🦉 Check **Windows CLI installation guide** and **macOS CLI installation guide** for references.

> 🚨 **IMPORTANT**
>
> AnyDesk provides deployment packages (`.msi` for Windows, `.pkg` for macOS, Android via Google Play, and iOS via App Store), but we can't support every third-party MDM tool. For specific deployment instructions, consult your MDM vendor or refer to our example scripts for Windows and macOS.

Configure via MDM for macOS

To configure AnyDesk (version 6.4+) via MDM, you must upload a `.mobileconfig` XML profile. The profile contains the following required elements:

- `PayloadContent`
- `PayloadScope`
- `PayloadUUID`
- `PayloadDisplayName`
- `PayloadIdentifier`
- `PayloadType`
- `PayloadVersion`

PayloadContent elements

XML Tag	Description	Value Type	Example/Values
`PayloadContent`	This XML group contains the action MDM configuration. The following tags belong to this group.		`<dict>...</dict>`
`PayloadDisplayName`	Profile name shown in *System Preferences* > *Profiles* on the deployed macOS devices.	string	*Company A's AnyDesk Configuration*
`PayloadIdentifier`	Unique identifier for the AnyDesk configuration in reverse-domain notation.	string	`com.companya.config.anydesk`
`PayloadUUID`	Unique random UUID for the AnyDesk configuration. *Format:* `<8 characters>-<4 characters>-<4 characters>-<4 characters>-<12 characters>` * Number between 1-9 * Letter between A-F	string	`5D2F7682-3B17-43EC-B6F6-CB20696ED631`
`PayloadType`	Custom app ID that corresponds to your account prefix. You can find the prefix in my.anydesk II > *Builds* > select a custom client > custom client Details page. ⚠️ In this case, the reverse domain-notation created in `PayloadIdentifier` should not be used. Must follow the format: `com.philandro.anydesk-<prefix>`	string	`com.philandro.anydesk-<prefix>`
`PayloadVersion`	Integer version number of this configuration.	integer	`1`
`ad.*` keys	Key-value pairs from AnyDesk advanced options. All settings and permission sets here *overwrite*.	string	See the **Value Possibilities** columns in Advanced options.
`ad.features.connect`	Enable or disable initiating connections.	string	0: Disable **1: Enable**
`ad.features.accept`	Enable or disable receiving connection requests.	string	0: Disable **1: Enable**

Additional profile properties

XML Tag	Description	Value Type	Example/Values
`PayloadScope`	Determines the scope of the MDM profile. `System` needs to be used to apply AnyDesk configuration to all local user accounts and the global AnyDesk service.	string	`System`
`PayloadUUID` *(profile-level)*	Random UUID for the MDM profile from that is unique within the company. ⚠️ This UUID should be different from the one assigned to the AnyDesk configuration in `PayloadContent::PayloadUUID`	string	`A2A5828E-F98C-45BB-9BFE-E4E854B3AC45`
`PayloadDisplayName` *(profile-level)*	Name of the MDM profile. An MDM profile can contain enterprise configurations for multiple apps.	string	*Company A's MDM Profile*
`PayloadIdentifier` *(profile-level)*	MDM profile identifier in reverse-domain notation.	string	`com.companya.config`
`PayloadType` *(profile-level)*	Type of MDM profile. With an AnyDesk configuration, PayloadType `Configuration` needs to be used.	string	`Configuration`
`PayloadVersion` *(profile-level)*	Internal integer version of this MDM profile. It helps macOS distinguish between different versions of the same profile.	integer	`1`

Deploying the profile

This configuration can be deployed manually on each individual device or automatically deployed through the mobile device management tool.

Manually

via MDM

To deploy the profile on macOS device manually:

1. Copy the `.mobileconfig` file to each macOS device and install it.
2. In **System Preferences** > **Profiles**, confirm the unsigned/unverified configuration.

Changes take effect the next time the custom AnyDesk client launches on each device.

To deploy the profile on your enrolled macOS devices through your MDM tool:

1. Create a new macOS configuration profile.
2. Enter profile name (and optional description).
3. Upload the `.mobileconfig` file with the AnyDesk configuration (or create the XML within the MDM interface).
4. Assign to target users, groups, or devices.
5. Save and deploy.

Depending on your MDM deployment settings, after a few minutes, the MDM profile should be deployed on all connected enrolled devices. You can verify the installation in **System Preferences > Profiles**.

Changes take effect the next time the custom AnyDesk client launches on each device.

Configure via MDM for Android

Mobile device management (MDM) tools with app restriction features can deploy a modified version of the standard AnyDesk application from the Google Play Store.

> 💡 **NOTE**
>
> Configuring a custom AnyDesk client (APK) via MDM is not supported.

The standard AnyDesk client can be easily configured using the built-in Configuration Editor available in most MDM tools. To do so:

1. Add the AnyDesk app from the Google Play Store to your MDM.
2. For Managed Devices, create an app configuration policy.
3. The targeted application is the AnyDesk for Android app, you added in Step 1.
4. To customize the AnyDesk settings, use the built-in Configuration Editor/Designer. You can view a predefined list of available keys and values with descriptions:
    - If the keys starts with `defaults.*`, the user of the configured AnyDesk client can modify the settings.
    - If the keys starts with `overrides.*`, the user will **not** be able to change the settings.
5. Save.

Similar to macOS, once saved, the enrolled devices should automatically retrieve the configuration from the MDM solution and update the AnyDesk settings.

> 🚨 **IMPORTANT**
>
> If you're managing your AnyDesk application to connect to an AnyDesk On-Premises appliance server, the following keys are required:
>
> - `overrides.ad.license.register_key`
> - `overrides.ad.anynet.boot_addrs`
> - `overrides.ad.anynet.ca_certs`

Configure via MDM for iOS

Starting with AnyDesk 5.5.0 for iOS, administrators can now configure the standard version of AnyDesk from the App Store using mobile device management (MDM) solutions.

Similar to Android, the standard AnyDesk client for iOS can be easily configured using the built-in Configuration Editor available in many MDM tools. To do so:

1. Add the AnyDesk for iOS application to your MDM solution.
2. For Managed Devices, create an **Application Configuration Policy**.
3. The targeted application will be the AnyDesk for iOS app you added in Step 1.
4. To customize the settings of the AnyDesk client, use the built-in Configuration Editor/Designer. A full list of available keys and their descriptions can be found in the table below.
5. Save.

The configuration can then be deployed to iOS devices via Profiles linked to your AnyDesk configuration or Apple Configurator 2. For more information on enrolling your devices, please contact your IT administrator or MDM vendor directly.

Configuration keys for iOS

You must assign a key type (either `defaults` or `overrides`) to the beginning of each Configuration key listed below.

- If the key starts with `defaults`, the option will be configured as specified, but the user of the configured AnyDesk client will still have the ability to modify the setting if they choose to.
  For example:
  `defaults.ad.security.acl_enabled`
- If the key starts with `overrides`, the user will not be able to change the setting in the configured AnyDesk client.
  For example:
  `overrides.ad.discovery.hidden`

The default values for the standard AnyDesk client are indicated in **bold** in the **Value Possibilities** column.

Key	Description	Value Type	Value Possibilities
`ad.features.address_book`	Specifies whether the AnyDesk client has access to the Address Book feature. If set to `true`, a valid license key must be provided for the key: `ad.license.register_key`	boolean	**false**, true
`ad.license.register_key`	The license key, available in your my.anydesk management console or the WebUI of the On-Premises appliance server. It is required to connect the AnyDesk client to your On-Premises appliance server.	string	`A1S273JUEKSA87XN`
`ad.anynet.boot_addrs`	⚠️ Use this setting only if you want the AnyDesk client to connect to your AnyDesk On-Premises appliance server. It specifies the IP address or URL of the appliance server the AnyDesk client should connect to, using the following format (port is optional): `(ip	host):port;(ip	host):port;…)` This setting is required to connect the client to your On-Premises appliance server.
`ad.anynet.ca_certs`	⚠️ Use this setting only if you want the AnyDesk client to connect to your AnyDesk On-Premises appliance server. This specifies the public certificate of the appliance server. Note that MDMs like Microsoft Intune only allow single-line values. Since the certificate is multiline, you must manually replace all newline characters with `\n`. For	string	

Key	Description	Value Type	Value Possibilities
	example, if your certificate is formatted as: `abc qwe` Plain text Copy The MDM value for this key should be: `abc\nqwe` Plain text Copy This setting is required to connect the client to your On-Premises appliance server.		
`ad.ui.cfg_enabled`	Specifies whether the AnyDesk client has access to the settings.	boolean	false, **true**
`ad.ui.cfg_enable_audio`	Specifies whether the AnyDesk client has access to the Audio settings.	boolean	false, **true**
`ad.ui.cfg_enable_connection`	Specifies whether the AnyDesk client has access to the Connection settings.	boolean	false, **true**
`ad.ui.cfg_enable_privacy`	Specifies whether the AnyDesk client has access to the Privacy settings.	boolean	false, **true**
`ad.ui.cfg_enable_recording`	Specifies whether the AnyDesk client has access to the Recording settings.	boolean	false, **true**
`ad.security.auto_disconnect.mode`	Specifies whether the Auto-disconnect feature is enabled.	integer	**0: Disabled** 1: Enabled
`ad.security.auto_disconnect.timeout`	Specifies the inactivity timeout period (in seconds) before incoming sessions are automatically disconnected.	integer	Minimum: 60
`ad.security.hear_audio`	Specifies whether clients connecting to this AnyDesk client can hear the device's audio output.	boolean	false, **true**

Key	Description	Value Type	Value Possibilities
`ad.security.sysinfo`	Specifies whether clients connecting to this AnyDesk client can view the device's system information.	boolean	false, **true**
`ad.security.acl_enabled`	Specifies whether the Access Control List (ACL) feature is enabled for this AnyDesk client.	boolean	**false**, true
`ad.security.acl_list`	Specifies which AnyDesk IDs or aliases are included in the access control list (ACL) enabled above.	string	`123456789:true; mycomputer@ad:true;`
`ad.discovery.enabled`	Specifies whether the client can discover other AnyDesk clients on the same local area network.	boolean	false, **true**
`ad.discovery.hidden`	Specifies whether other AnyDesk clients can discover this client on the same local network.	boolean	false, **true**
`ad.input.auto_touch_to_touch_mode`	Specifies whether touch-to-touch mode is available when connected to remote Android devices.	boolean	**false**, true
`ad.input.touch_mode`	Specifies whether touchpad mode or touch mode is used.	integer	1: Touch **2: Touchpad**
`ad.image.follow_remote_cursor`	Specifies whether the view automatically switches when the remote mouse cursor moves to a different display.	integer	**0: Disabled** 1: Enabled
`ad.image.follow_remote_focus`	Specifies whether the view automatically switches when the remote	integer	**0: Disabled** 1: Enabled

Key	Description	Value Type	Value Possibilities
	foreground window moves to another display.		
`ad.image.quality_lossless`	Specifies whether outgoing sessions from this client use the lossless quality transmission setting.	boolean	**false**, true
`ad.image.quality_preset`	Specifies the transmission quality for outgoing sessions.	integer	0: Best quality **1: Balanced** 2: Optimize reaction time
`ad.image.show_remote_cursor`	Specifies whether the remote cursor is visible.	boolean	**false**, true
`ad.audio.playback_mode`	Specifies whether you can hear the audio from the device you're connecting to.	integer	0: Disable **1: Enable**
`ad.audio.transmit_mode`	Specifies whether others can hear the audio from your device when connected to you.	integer	0: Disable **1: Enable**
`ad.anynet.listen_port`	Specifies the listening port for incoming direct connections.	integer	`0`
`ad.anynet.proxy.mode`	Specifies the proxy mode.	integer	0: Never use a proxy server **1: Try to detect** 2: Use a specific proxy server
`ad.anynet.proxy.addr`	Specifies the proxy address.	string	`1.1.1.1`
`ad.anynet.proxy.port`	Specifies the proxy port.	integer	`10000`
`ad.anynet.proxy.auth`	Specifies whether authentication credentials are required to be sent to the proxy.	boolean	**false**, true
`ad.anynet.proxy.user`	Specifies the proxy username.	string	`myproxyuser`

Key	Description	Value Type	Value Possibilities
`ad.anynet.proxy.pass_plain`	Specifies the proxy password.	string	`myproxypassword`
`ad.recording.auto_start.incoming`	Automatically starts a screen recording when someone connects to your device.	integer	**0: Disabled** 1: Enabled
`ad.recording.auto_start.outgoing`	Automatically starts a screen recording when you connect to another device.	integer	**0: Disabled** 1: Enabled
`ad.session.remember_settings`	Specifies whether the client remembers settings, such as activating Privacy Mode, when reconnecting to the same remote device in the future.	boolean	false, **true**

A security feature that lets you define which AnyDesk IDs or Aliases are allowed to connect to a device. All devices outside of your Access Control List are automatically blocked.