DOCUMENTATION

Duo Authentication for Windows Logon and RDP

Last Updated: July 6th, 2023

Duo integrates with Microsoft Windows client and server operating systems to add two-factor authentication to Remote Desktop and local logons and credentialed UAC elevation prompts.

> Be sure to read through these instructions before you download and install Duo for Windows Logon.

Overview

Duo Authentication for Windows Logon adds Duo two-factor authentication to these Windows and Windows Server logon scenarios:

- Local or domain account logins
- Logins at the local console and/or incoming Remote Desktop (RDP) connections
- Credentialed User Access Control (UAC) elevation requests (e.g. Right-click + "Run as administrator") in v4.1.0 and later

Duo's Windows Logon client does not add a secondary authentication prompt to the following logon types:

- Shift + right-click "Run as different user"
- PowerShell "Enter-PSSession" or "Invoke-Command" cmdlets
- Non-interactive logons (i.e. Log on as a Service, Log on as Batch, Scheduled Tasks, drive mappings, etc.)
- Pre-Logon Access Providers (PLAPs) such as Windows Always On VPN

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

Reject Accept Manage cookie settings >

Important Notes

Please review all these compatibility and installation notes before proceeding.

- Installing Duo Authentication for Windows Logon adds two-factor authentication to **all** interactive user Windows login attempts, whether via a local console or over RDP, unless you select the "Only prompt for Duo authentication when logging in via RDP" option in the installer. If two-factor is enabled for both RDP and console logons, it may be bypassed by restarting Windows into Safe Mode (e.g. in case of a configuration error). If you wish to protect local console logons with Duo, please see the FAQ for some guidance on securing your Windows installation appropriately.
- Additional configuration may be required to log in using a Microsoft attached account. See Can I Use Duo with a Microsoft Account? for more information.
- Windows users must have passwords to log in to the computer. Users with blank passwords may not login after Duo Authentication installation.
- It's a good idea to have your BitLocker recovery key available in the event you need to boot into safe mode to uninstall Duo.
- This application doesn't support Surface Pro X or other devices with ARM processors. Installing Duo for Windows Logon on these devices may block logins, requiring uninstallation from Safe Mode.
- Review these Duo Knowledge Base articles for additional security recommendations:
  - How can I prevent an attacker with compromised administrative credentials from disabling Duo for Windows Logon and bypassing MFA?
  - Guide to Duo Authentication for Windows Logon and RDP Integration Security
  - Can Duo protect local console logins in Windows?
- Duo application features like failmode, offline access, and UAC protection may be configured during installation or post-installation via Regedit or Group Policy. Please see our FAQ for more information.

> **Connectivity Requirements**
> This application communicates with Duo's service on SSL TCP port 443.
>
> Firewall configurations that restrict outbound access to Duo's service with rules using destination IP addresses or IP address ranges aren't recommended, since these may change over time to maintain

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

TLS Requirements

Effective June 30, 2023, Duo no longer supports TLS 1.0 or 1.1 connections or insecure TLS/SSL cipher suites.

The current version of Duo for Windows Authentication supports TLS 1.2 when installed on a version of Windows that also supports and uses TLS 1.2 or higher.

See the article Guide to TLS support for Duo applications and TLS 1.0 and 1.1 end of support for more information.

System Requirements

Windows Versions

Duo Authentication for Windows Logon supports both client and server operating systems.

Clients:

- Windows 10 (as of v1.1.8)
- Windows 11 (as of v4.2.0)

Servers (GUI and core installs):

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016 (as of v2.1.0)
- Windows Server 2019 (as of v4.0.0)
- Windows Server 2022 (as of v4.2.0)

Ensure your system's time is correct before installing Duo.

System Processor

Duo Authentication for Windows Logon does not support devices with ARM processors, like the Surface Pro X

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

Duo Factor Support

Duo for Windows Logon supports these factor types for online two-factor authentication:

- Duo Push (Duo Mobile)
- Duo Mobile Passcodes
- SMS Passcodes
- Hardware Token OTP passcodes (including Yubikey OTP)
- Phone Call
- Bypass Codes

U2F security key support is limited to Offline Access only.

Enroll Users Before Installation

Duo Authentication for Windows Logon doesn't support **inline** self-service enrollment for new Duo users. Unenrolled users, that is, users that do not yet exist in Duo with an attached 2FA device, must be created manually by an administrator, imported by an administrator or self-enrolled through another application which supports Duo's self-service enrollment (see Test Your Setup) before those users can log in with Duo for Windows Logon.

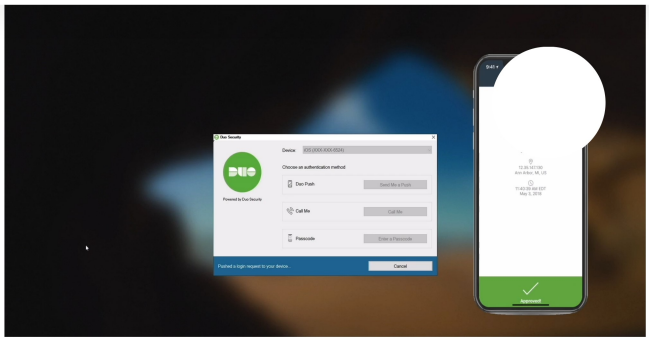
The Duo username (or username alias) should match the Windows username. When you create your new RDP application in Duo the username normalization setting defaults to "Simple", which means that the if the application sends the usernames "jsmith," "DOMAIN\jsmith," and "jsmith@domain.com" to Duo at login these would all resolve to a single "jsmith" Duo user.

Duo for Windows Logon supports Duo Push, phone callback or SMS passcodes, and passcodes generated by Duo Mobile or a hardware token as authentication methods. Duo users must have one of these methods available to complete 2FA authentication.

If the user logging in to Windows after Duo is installed does not exist in Duo, the user may not be able to log in to the system.

Read the enrollment documentation to learn more about enrolling your users in Duo.

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.



9:59

First Steps

Before moving on to the deployment steps, it's a good idea to familiarize yourself with Duo administration concepts and features like options for applications, available methods for enrolling Duo users, and Duo policy settings and how to apply them. See all Duo Administrator documentation.

1. Sign up for a Duo account.
2. Log in to the Duo Admin Panel and navigate to **Applications**.
3. Click **Protect an Application** and locate the entry for **Microsoft RDP** in the applications list. Click **Protect** to the far-right to configure the application and get your **integration key**, **secret key**, and **API hostname**. You'll need this information to complete your setup. See Protecting Applications for more information about protecting applications in Duo and additional application options.
4. We recommend setting the New User Policy for your Microsoft RDP application to **Deny Access**, because no unenrolled user may complete Duo enrollment via this application.
5. If you'd like to enable offline access with Duo MFA you can do that now in the "Offline Access Settings" section of the Duo application page, or return to the Admin Panel later to configure offline access after first verifying logon success with two-factor authentication.
6. Download the Duo Authentication for Windows Logon installer package. View checksums for Duo downloads here.

> **Treat your secret key like a password**

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

Remembered Devices for Windows Logon

Available in: Duo Essentials, Duo Advantage, and Duo Premier

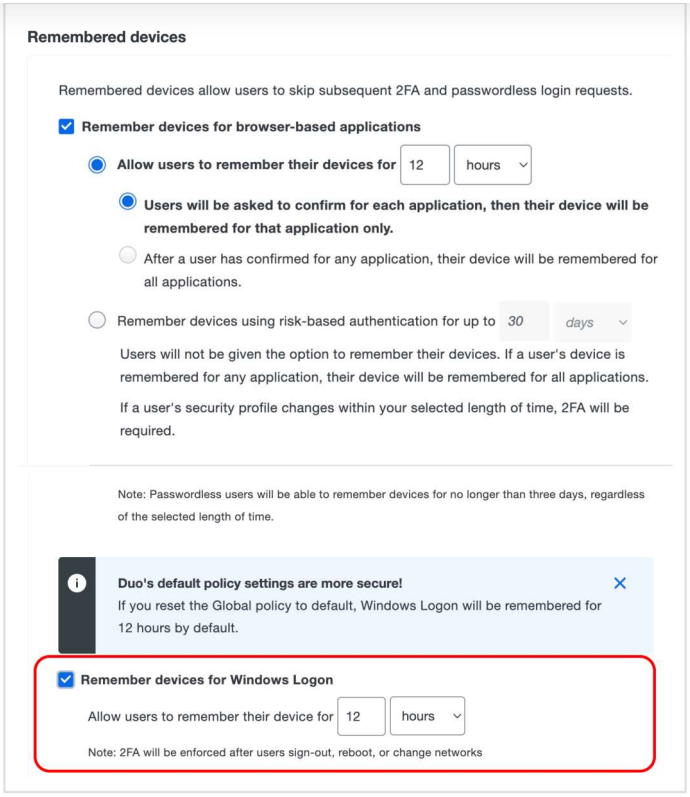
Version 4.2.0 of Duo Authentication for Windows Logon adds support for local trusted sessions, reducing how often users must repeat Duo two-factor authentication. The Remembered Devices policy now includes a setting for Windows logon sessions, which when enabled offers users a "Remember me" checkbox during local console login for the duration specified in the policy.

When users check this box and complete Duo authentication, they aren't prompted for Duo secondary authentication when they unlock the workstation after that initial authentication until the configured trusted session time expires. If the user changes networks, authenticates with offline access while the workstation is disconnected, logs out of Windows, reboots the workstation, or clicks the "Cancel" button during workstation unlock, Duo for Windows Logon invalidates the current trusted session and the next Windows logon or unlock attempt will require Duo authentication again.

To enable remembered devices for Windows Logon:

1. Create a new custom policy or update an existing policy for remembered devices which enables the **Remember devices for Windows Logon** option, and enter the number of hours or days you want a trusted Windows logon session to last. Click **Save Policy** when done.

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.



2 Apply the custom policy to your Microsoft RDP Duo application as a group or application policy. If you made the change in your global policy then the setting applies to all your Microsoft RDP Duo applications, unless any of them have a policy assigned with conflicting remembered Windows Logon device settings.

   The policy setting takes immediate effect — there is no need to reinstall the Duo Authentication for Windows Logon application after updating the remembered device policy as long as clients have already installed v4.2.0 or later. Systems with older versions of Duo for Windows Logon must upgrade to 4.2.0 or later to see the new option.

With this policy setting applied, users who log on to the local Windows console see an additional option on the Duo for Windows Logon prompt for remembering the device. This option will not display for RDP/remote logins to Windows systems with Duo Authentication for Windows Logon installed, regardless of the effective remembered devices policy setting for Windows Logon.

Administrators may revoke the Windows local trusted Duo session by unassigning a remembered devices policy for Windows Logon from a Microsoft RDP application, editing the policy attached to a Microsoft RDP application to disable the Windows Logon remembered devices setting, or by deleting the registry entry for the user session from the Windows client. Learn more about this in the Windows Logon FAQ.

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

If you want to deploy Duo to your Windows systems but have no users complete 2FA until a specific date (after all user enrollment is complete), set the New User Policy to "Allow Access" and set the Authentication Policy to "Bypass 2FA". With these two policy settings in place users who have and who have not enrolled in Duo log in to the Windows system as usual without experiencing Duo.

If you chose to enable offline access on your application, then enrolled users who bypass 2FA due to the effective Authentication Policy would still be prompted to complete offline enrollment. To avoid confusion, we recommend leaving offline access off until you require users to complete Duo 2FA while online.

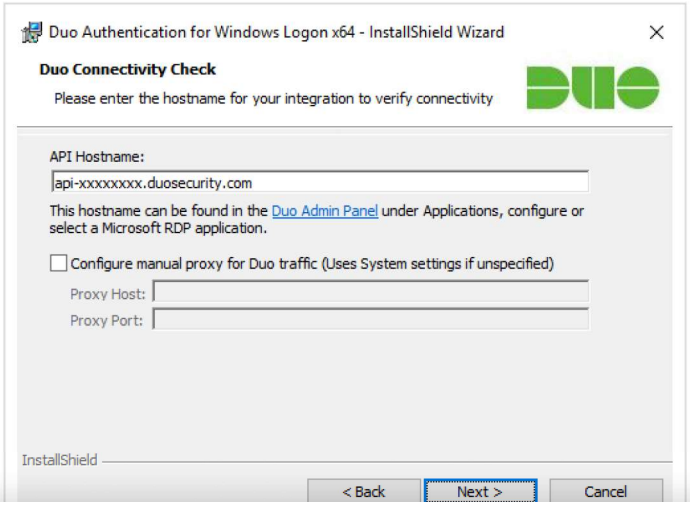
When you're ready to require Duo authentication for all users of the target Windows system, change the "New User Policy" to "Deny access" and change the "Authentication Policy" to "Enforce 2FA". This will prompt all enrolled users to perform Duo 2FA after they type in their usernames and passwords, and prevent users who have not enrolled in Duo from logging in without 2FA.

Run the Installer

1. Run the Duo Authentication for Windows Logon installer with administrative privileges.

   If you receive an "Installation stopped" error from the Duo installer please refer to Duo KB article 6462 for remediation steps.

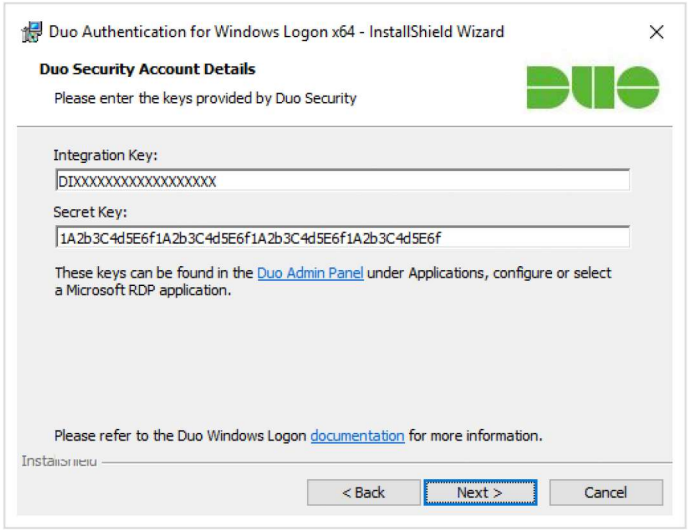
2. When prompted, enter your **API Hostname** from the Microsoft RDP application's details page in the Duo Admin Panel and click **Next**. The installer verifies that your Windows system has connectivity to the Duo service before proceeding.



Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

If you need to use an outbound HTTP proxy in order to contact Duo Security's service, enable the **Configure manual proxy for Duo traffic** option and specify the proxy server's hostname or IP address and port here.

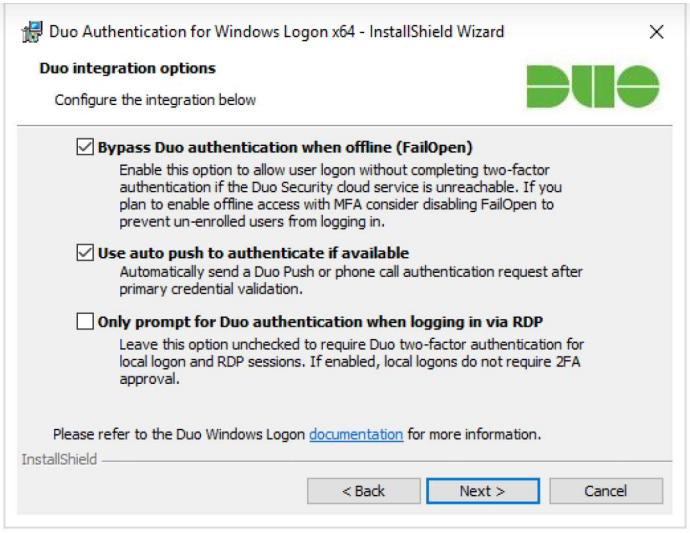
3 Enter your **integration key** and **secret key** from the Microsoft RDP application in the Duo Admin Panel and click **Next** again.



4 Select your integration options:

Setting	Description
Bypass Duo authentication when offline (FailOpen)	Enable this option to allow user logon without completing two-factor authentication if the Duo Security cloud service is unreachable. Checked by default. If you plan to enable offline access with MFA consider disabling FailOpen.
Use auto push to authenticate if available	Automatically send a Duo Push or phone call authentication request after primary credential validation to the first capable device attached to the user. Checked by default and applies to all users of the target system.
Only prompt for Duo authentication when logging in via RDP	Leave this option unchecked to require Duo two-factor authentication for console and RDP sessions. If enabled, console logons do not require 2FA approval. If you want to enforce protected offline access to laptop logins, be sure you don't check this box. If you do, laptop console logins won't require any form of Duo MFA.

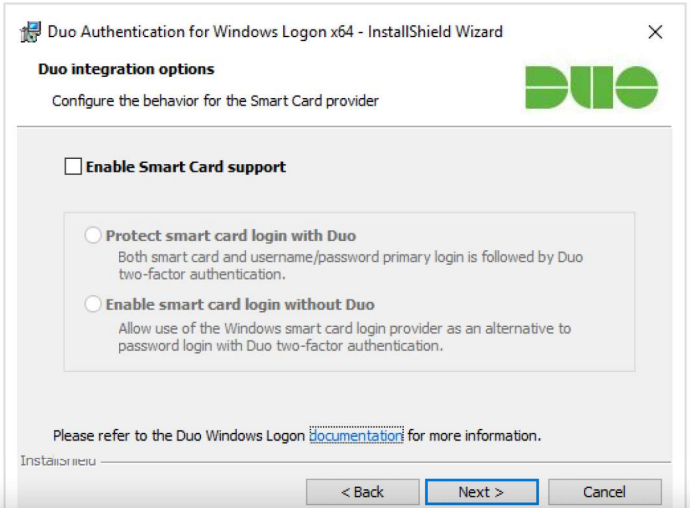
Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.



5 If you plan to use smart cards on the systems where you install Duo, click to **Enable Smart Card Support** and select your smart card options:

Setting	Description
Protect smart card login with Duo	Select this option to require Duo authentication after primary login with username and password or primary authentication with a smart card. Supported for local console logins.
Enable smart card login without Duo	Select this option to permit use of the Windows smart card login provider as an alternative to Duo authentication. Smart card logins won't require 2FA.

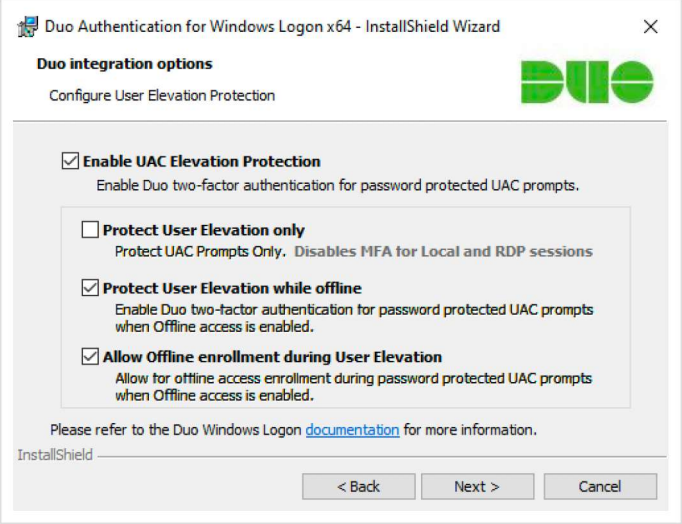
These options only support the Windows native smart card provider. Available in version 3.1.1 and later.



Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

Setting	Description
Protect User Elevation only	Enable Duo two-factor authentication at password-protected UAC prompts only. If you check this box Duo will **not** prompt for 2FA at local or RDP login or workstation unlock.
Protect User Elevation while offline	Permit offline access authentication for password-protected UAC prompts if offline access is also enabled.
Allow offline enrollment during User Elevation	Allow and prompt for offline access enrollment during UAC password elevation if offline access is also enabled.

Available in version 4.1.0 and later.



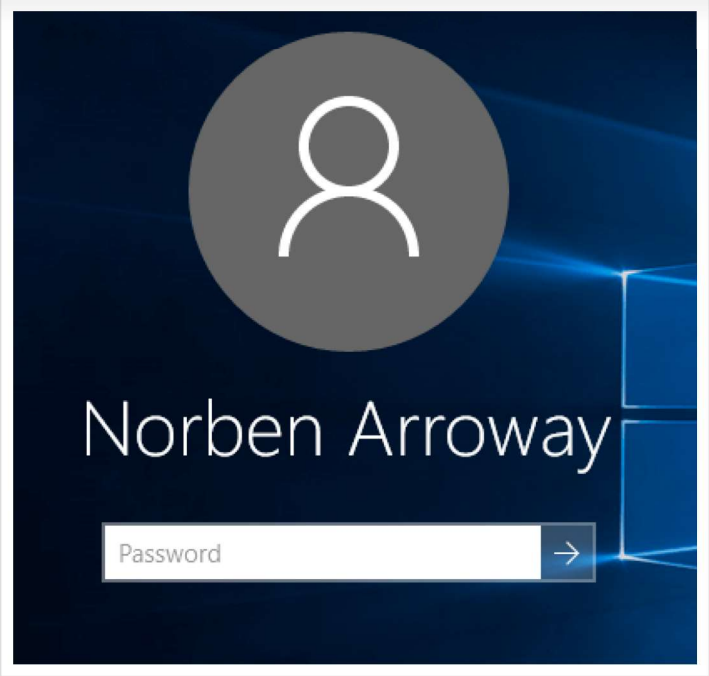
7 Click **Next** and then **Install** to complete Duo installation.

If you need to change any of your chosen options after installation, you can do so by updating the registry. See the Duo for Windows Logon FAQ for instructions on how to update the settings.

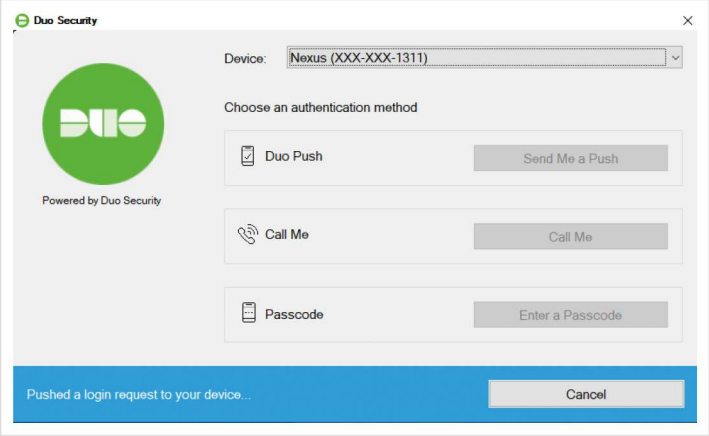
Test Your Setup

To test your setup, attempt to log in to your newly-configured system as a user enrolled in Duo.

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.



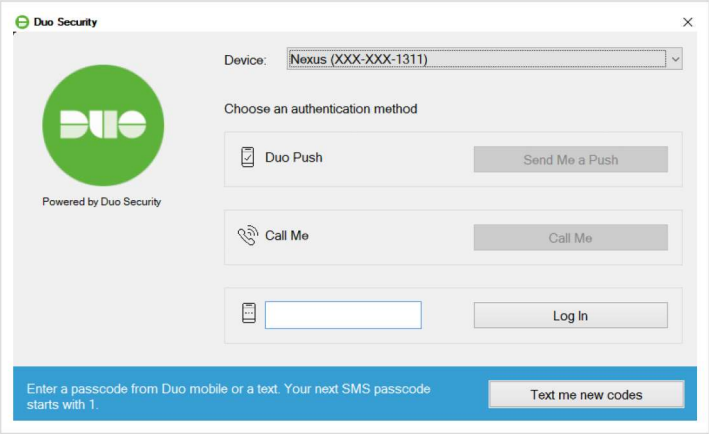
The Duo authentication prompt appears after you successfully submit your Windows credentials. With automatic push enabled (the default installation option), the prompt indicates that Duo pushed an approval request to your phone. Duo sends the push request to the first phone activated for Duo Push and associated with that Duo user.



With automatic push disabled, or if you click the Cancel button on the Duo authentication prompt after a 2FA request was sent, you can select a different device from the drop-down at the top (if you've enrolled more than one) or select any available factor to verify your identity to Duo:

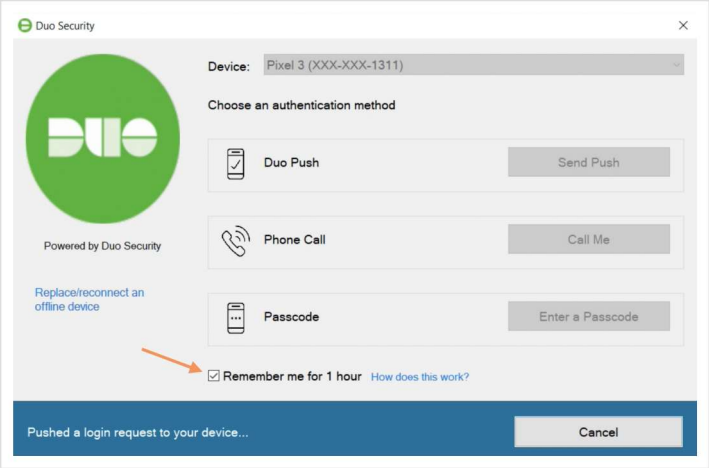
Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

Send me new codes button. You can then authenticate with one of the newly-delivered passcodes.



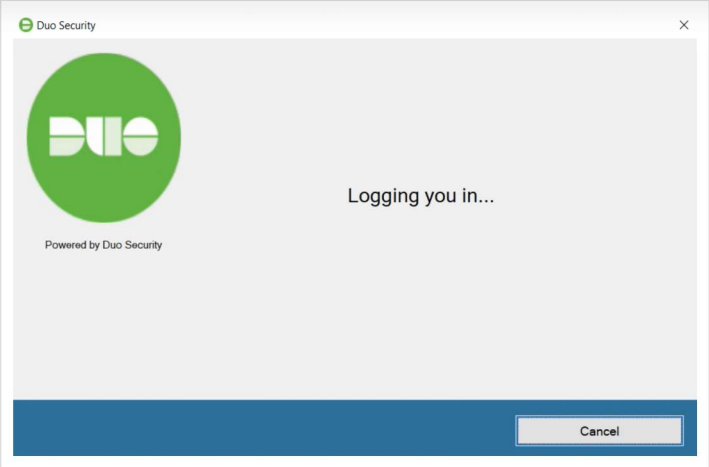
Remembered Device

If you applied a policy to your Microsoft RDP application that enables remembered devices for Windows Logon, then during Duo authentication at the local system's console you'll see the **Remember me for...** option, reflecting the number of hours or days you set in the policy.



If you check this box when authenticating you won't need to perform Duo second-factor authentication again for the duration specified on the prompt the next time you unlock the workstation to continue the logged-in Windows session.

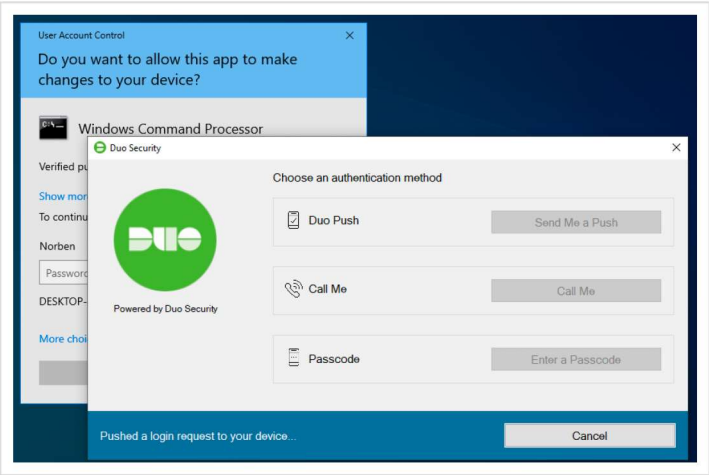
Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.



Duo will prompt you to complete two-factor authentication at the next Windows logon or unlock after the remembered device session ends, and at that time you can choose to begin a new trusted logon session.

UAC Elevation

If you enabled User Elevation in Duo for Windows Logon v4.1.0 or later, you'll see the Duo authentication prompt after you enter your password for a credentialed elevation request. The application you were trying to launch runs after you approve the Duo two-factor request. If you chose to remember the device at the Windows desktop login, then you won't need to approve Duo authentication for UAC elevations made by the **same logged-in account** either until the trusted Duo session ends.



Remember: if you find that Duo Authentication for Windows Logon has locked you out of your Windows system

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

Offline Access Video Overview

Offline Access Requirements

- Duo Essentials, Advantage, or Premier plan subscription (learn more about Duo's different plans and pricing)
- Duo Authentication for Windows Logon version 4.0.0 or later
  - Disable the **Bypass Duo authentication when offline (FailOpen)** option. If you enabled FailOpen during installation, you can change it in the registry.
  - Disable the **Only prompt for Duo authentication when logging in via RDP** option to use offline access with laptop or desktop local console logins. If you enabled Duo for RDP logins only during installation, you can change it in the registry.

Users must have either:

- Duo Mobile for Android or iOS version 3.22 or later (no Windows Phone support)
- A supported U2F security key - ensure the key you plan to use **does not** require extended length encoding. Some options we've tested:
  - Yubico brand keys supporting U2F/FIDO2
  - Google Titan
  - Feitian ePass FIDO
  - Thetis FIDO

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

Note these functional limitations for offline access authentication devices:

- Users may only register **one** authenticator for offline access, so it is not possible to register backup devices for approving offline login. Registering a second offline device deactivates the first one.
- U2F security keys for offline authentication only work for local system console logins. It is not possible to use a security key attached to your local RDP client system to perform offline authentication at a remote Windows server. You can use a Duo Mobile offline passcode with a remote system.
- Remembered devices policy settings and local trusted sessions do not apply to offline access. If you choose to remember the device when you log in while online, and then unlock the Windows workstation while offline, the previously created trusted session ends and you will need to complete offline access authentication. When the workstation is back online, you will need to complete online Duo authentication to begin a new remembered device session.

Offline Access Configuration

1. Return to your "Microsoft RDP" application page in the Duo Admin Panel. You may have given the RDP application a different name when you created it, but the "Type" will always be shown as "Microsoft RDP" on the Applications page.

2. Scroll down to the bottom of the RDP application's page to locate the **Offline Access Settings**. Check the box next to **Enable offline login and enrollment** to turn on offline access.

3. Check the **Only allow offline login from users in certain groups** to specify a group or groups of Duo users permitted to use offline access. Users who are not members of the groups you select here won't be able to enroll in offline access or login in with MFA when the Windows system is unable to contact Duo, and instead are subject to your fail mode configuration (let in without MFA if you enabled fail open, or prevented from logging in if you disabled fail open).

   After you configure this option, when a user logs into a Windows system while it's online and can reach Duo and it has been greater than 24-30 hours since the last online authentication, Duo for Windows Logon will update the offline policies for all users on the system, including deprovisioning them for offline access if they are no longer members of the offline groups selected for offline login in the Duo Admin Panel.

   If you also configured permitted groups on your RDP application, users need to be members of both the permitted and the offline login groups to use offline access.

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

next time they perform an online Duo authentication, the computer's offline counter resets.

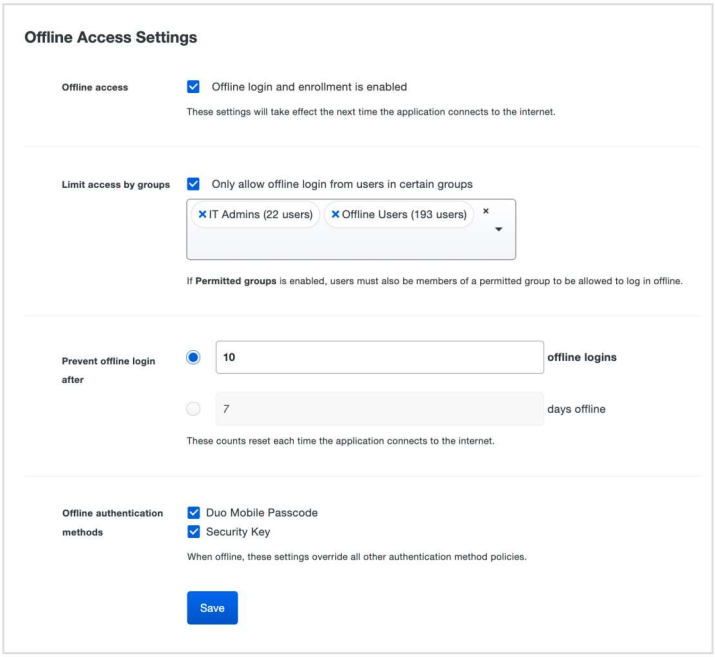
- Enter the maximum number of days offline, up to 365. With this option, there is no limit to the number of times a user logs in while offline during the allowed period.

  Users need to reconnect their offline computer to the internet upon reaching the end of the period you define here. The next time they perform an online Duo authentication, the computer's offline expiration date resets. If the user does not perform online Duo authentication before the maximum number of days specified here is reached, **they can no longer log in offline**, and so must connect to Duo's service in order to log in at all.

5 Users may activate offline access using either the Duo Mobile application for iOS or Android, or a U2F security key. Both offline authentication methods are allowed unless you uncheck one in the **Offline authentication methods** setting. You may not uncheck both options.

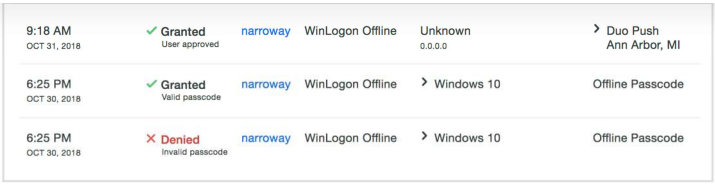
Any authentication method enabled for offline access is always permitted, overriding any other policy setting restricting authentication methods for the RDP application.

6 Click the **Save** button.



Offline Access Logging

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.



Advanced Configuration

Change How Many Users May Use Offline Access

By default, five (**5**) users may enroll in offline access. To increase or reduce the number of users that may activate offline access on a given Windows client, use the Registry Editor (regedit.exe) with administrator privileges to create or update the following registry value:

Location: **HKLM\SOFTWARE\Duo Security\DuoCredProv**:

Registry Value	Type	Description
`OfflineMaxUsers`	DWORD	Create this value and set to the number of users you would like to have the ability to enroll in offline access on a given Windows system. Minimum value: **1**; Maximum value: **50**. If not set the default is **5**.

Once the maximum number of users have activated offline access, the next user receives an error when attempting to enroll in offline access.

Force Offline Reactivation for a User

To force offline reactivation for a previously activated user on a given Windows system, use the Registry Editor (regedit.exe) with administrator privileges to delete the entire registry key that includes the username from **HKLM\SOFTWARE\Duo Security\DuoCredProv\Offline**.

Prevent Offline Access Use on a Client

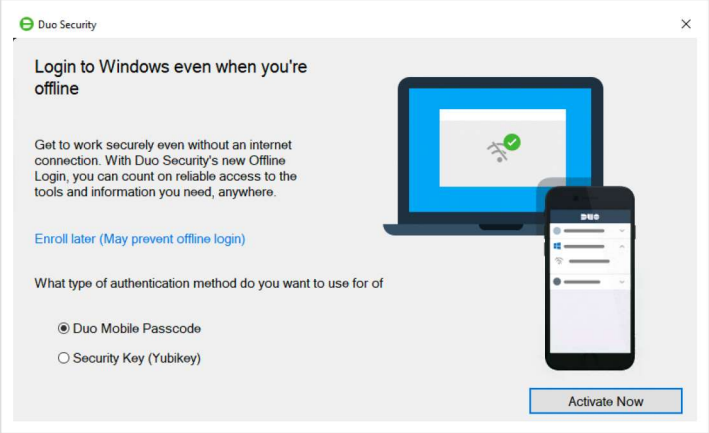
You may have Windows systems where no users should log in using offline access, regardless of the application setting in the Duo Admin Panel. To prevent offline authentication for any user on a given Windows client, use the Registry Editor (regedit.exe) with administrator privileges to create or update the following registry value:

Location: **HKLM\SOFTWARE\Duo Security\DuoCredProv**:

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

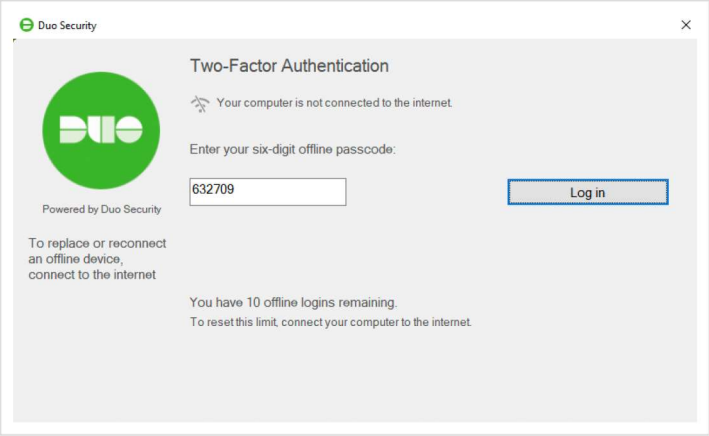
Offline Access Activation and Login

The next time you (or your end user) logs in to or unlocks the workstation while it's online and able to contact Duo, the offline activation prompt displays after successful two-factor authentication.



Step through the guided activation process to configure Duo Mobile or a U2F security key for offline MFA.

Once you've activated offline access for your account, when your computer isn't able to contact Duo's cloud service you'll automatically be offered the option to login with an offline code or security key after successfully submitting your Windows username and password.



You can also reactivate offline access from the online Duo prompt. Note that only **one authentication device** — a single phone with Duo Mobile or a single security key — may be activated for offline login. Activating a second

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

Updating Duo Authentication for Windows Logon

You can upgrade your Duo installation over the existing version; there's no need to uninstall first. The installer maintains your existing application information and configuration options.

1. Download the most recent Duo Authentication for Windows Logon installer package. View checksums for Duo downloads here.
2. Run the installer with administrator privileges and follow the on-screen prompts to complete the upgrade installation.

If you're upgrading to a version that includes new installer options, the configuration screen for those options won't be shown during an upgrade install. You'll need to configure those new options via Regedit or GPO update. See the Configuration section of the FAQ to learn how to enable and configure Duo for Windows Logon options in the registry, or the Group Policy documentation to learn how to configure options with GPO.

Uninstalling Duo

If you'd like to remove Duo Authentication for Windows Logon from your system, open the Windows Control Panel "Programs and Features" applet, click on the "Duo Authentication for Windows Logon" program in the list, and then click **Uninstall**.

Do not delete the Microsoft RDP application from the Duo Admin Panel until you have uninstalled the Duo application from all Windows systems using that application. If you delete the Admin Panel application before uninstalling the Duo software you may block users from logging in to Windows.

Advanced Deployment and Configuration using Group Policy

Please see our Duo Authentication for Windows Logon Group Policy documentation.

Troubleshooting

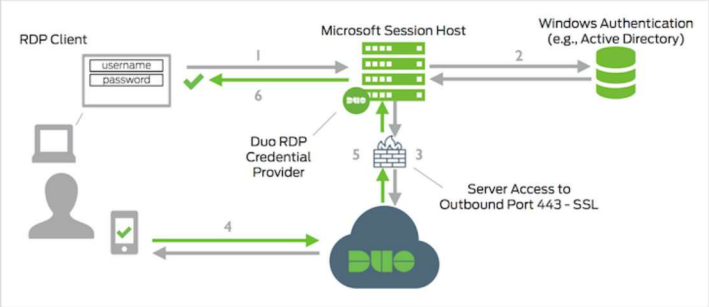
Need some help? Take a look at the Windows Logon Frequently Asked Questions (FAQ) page or try searching our Windows Logon Knowledge Base articles or Community discussions. For further assistance, contact Support.

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.

if the blocked users do not exist in Duo. Refer to these articles to learn more about user enrollment states and how they combine with policy settings to affect user logins.

- Why are Duo users being prompted to enroll or denied access when my New User Policy is set to allow access without 2FA?
- Guide to Duo User Enrollment States

Network Diagram



1. RDP connection, console logon, or UAC elevation initiated
2. Primary authentication of Windows credentials (domain or local user)
3. Duo Windows Logon credential provider connection established to Duo Security over TCP port 443
4. Secondary authentication via Duo Security's service
5. Duo Windows Logon credential provider receives authentication response
6. RDP or console session logged in

Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our Privacy Statement and Cookie Notice for more information.