



Duo Policy Guide: Configuring Access via Duo's Policy Engine

Version 5.2 released May 1, 2023

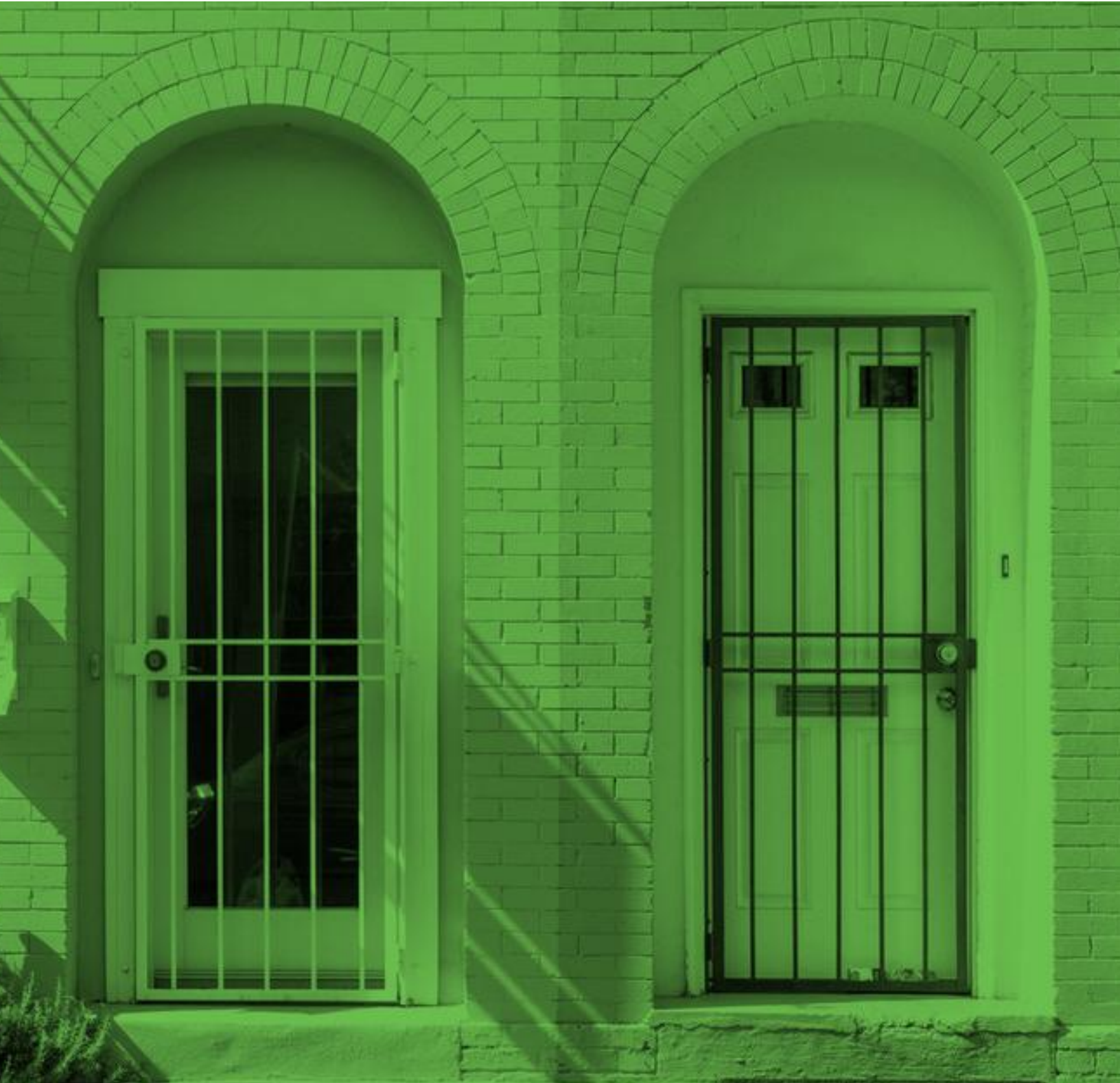


Table of Contents

Overview

[Why Do I Need This Guide?](#)

[Planning for Success](#)

Policy Definitions & Guidelines

[Global Policy](#)

[Application Policies](#)

[Group Policies](#)

[Policies Illustration](#)

[User Policy Settings](#)

[Device Policy Settings](#)

Enrollment States

[Fully Enrolled](#)

[Partially Enrolled](#)

[Unenrolled / New User](#)

More About New User Policy and Authentication Policy

[New User Policy & Enrollment States](#)

[How are they different?](#)

User & Group Status

[Active Status](#)

[Bypass Status](#)

[Disabled Status](#)

[Status Controls](#)

Administrative Roles & Units

Access vs. Authentication Devices

Enrollment & 2FA Enforcement Planning

Policy Example Scenarios

[Enrollment - Scenario 1](#)

[Enrollment - Scenario 2](#)

[Enrollment - Scenario 3](#)

[Adding More Security to an Application - Scenario 1](#)

[Adding More Security to an Application - Scenario 2](#)

[Enrollment & Authorized Networks - Scenario 1](#)

[Enrollment & Authorized Networks - Scenario 2](#)

[Enrollment & User Location - Scenario](#)

[Remembered Devices - Adding More Granular Restrictions - Scenario](#)

[Device Health application - Enforce Device Health Checks - Scenario](#)

[Operating System Policy - Block out-of-date Windows Devices - Scenario](#)

Overview

Why Do I Need This Guide?

Duo's policy engine is highly adaptable and designed to meet a diverse set of use cases. Configuring policies to reflect your specific needs allows you to get the most value out of the Duo edition you purchased. As your trusted access provider, we want to make sure you're equipped to leverage all the capabilities available to you.

Planning for Success

Duo lets you reduce risk by enforcing precise policies and controls. Learn how to define and enforce rules for **who can access which applications and under which conditions**. Being adept at defining and implementing policies will ultimately ensure a better experience with Duo.

This guide will help you understand:

- The three types of policies
- The relationship and rules between active policies
- Key terms related to user enrollment
- Example scenarios that can be extended or replicated for your own use cases

This guide serves as a supplement for the [documentation on policy and controls](#) found on our website and our [Policy & Access Control for Everyone course](#) available on our free education platform, Duo Level Up.

Policy Definitions & Guidelines

Duo gives administrators the power to create policies with granular levels of enforcement. Any of the policies available in your Duo deployment can be applied at the Global, Application, and Group level.

Policies allow you to segment access by defining who can access your Duo-protected applications and under which conditions. When an end-user attempts to access a Duo-protected application, your policy settings are checked as part of the authentication workflow. Depending on how your policies are configured, Duo can validate the user, network, access device, and authentication device before allowing access to an application.

In terms of hierarchy, think of policies in this way: Group > Application > Global, i.e., Application and Group Policies override the Global Policy; and Group Policies override Application Policies.

Find additional explanations and illustrations for how Policy & Access Control works in our free education platform, [Level Up](#).

Global Policy

- This policy applies to all applications and all users.
- It cannot be deleted (but can be edited).
- Since this applies to all applications, be sure to note the default Global Policy settings and modify the Application or Group Policies where appropriate for your use cases.
- Global Policy is configurable via the top-level “Policies” tab in the Duo Admin Panel.
- **Note:** Duo Essentials customers receive a subset of the Global Policy settings available in Duo Advantage and Duo Premier.

Application Policies

- These policies can be assigned to multiple applications and apply to all users logging into those applications.
- Application Policies are relevant when you need controls that differ from the Global Policy.
- They’re created as a “Custom Policy” and only need to specify the settings you wish to override from the Global Policy.
 - When this is the case, the text appears crossed out in the Application page’s Global Policy section. There will also be an (i) information icon specifying that rule is overridden for all users accessing that application.
- You can create and assign Application Policies to an application via the application’s properties page.

Group Policies

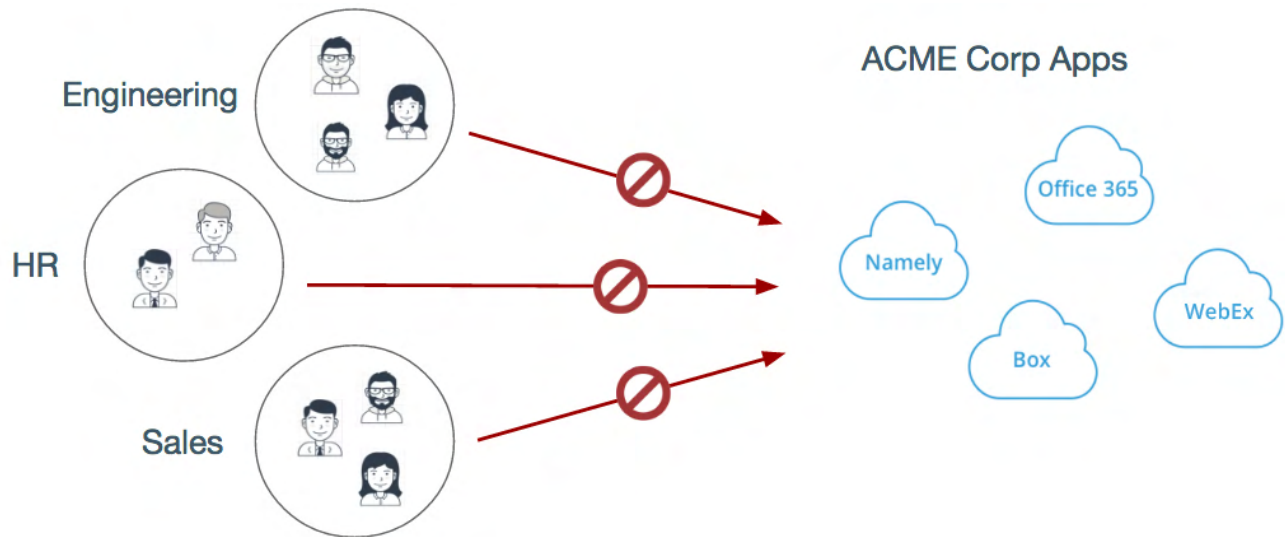
- You can assign Group Policies to one or more Duo user groups.
- These policies will override both the Global **and** Application Policies.
 - When a Group Policy overrides a Global Policy, the text will **not** appear crossed out in the Global Policy section of an application page, but you will see an (i) information icon specifying the rule is overridden for some groups of users accessing that application.
- You can create and assign Group Policies from each application’s properties page.
- An application can have multiple Group Policies applied. The policy framework applies custom Group Policy settings in the order they are listed in an application’s policy properties. When Group Policy settings conflict, the first policy listed takes precedence. You can find instructions on how to change the order of policies in our [Reorder Policies documentation](#).

Note on custom policy options by edition: Paid Duo editions allow for custom policies for all policy options included in the edition to be shared between applications or groups. Custom policy on Duo Free edition is limited to controlling a New User Policy with a shared Application Policy between applications.

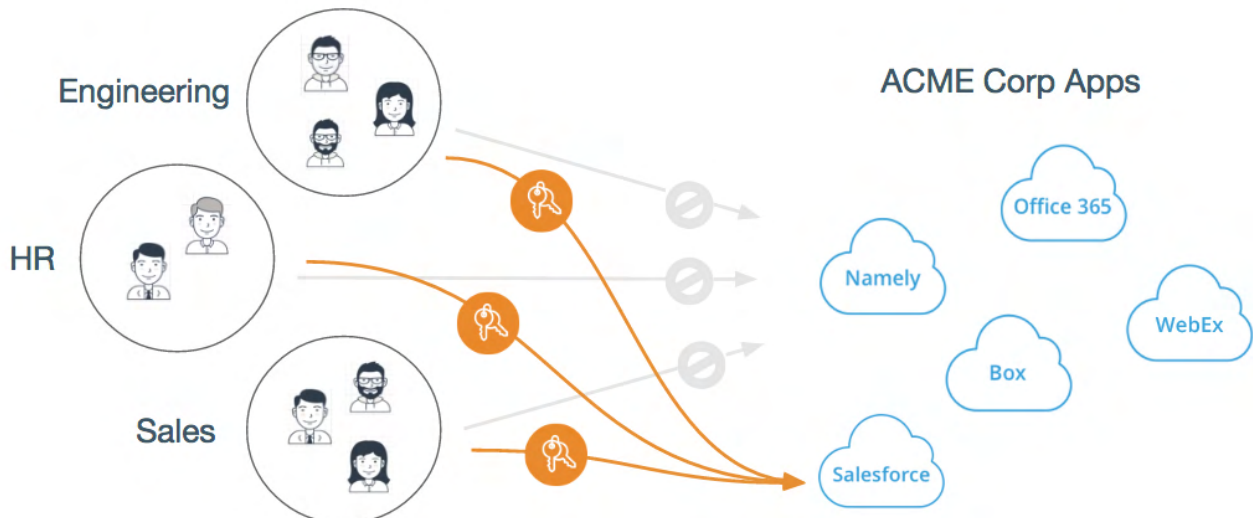
Policies Illustration

Below is a simple illustration of how you can use policies (in this instance, we are using the New User Policy and the Remembered Devices Policy). As you'll see in the diagrams, Application Policies override Global Policies, and Group Policies will override both Application and Global Policies.

Imagine ACME Co. starts by utilizing a **Global Policy** where they set the **New User Policy** to **Deny Access to Unenrolled Users** and **Remembered Devices** to **Do Not Remember Devices**. This means only users who have already enrolled with Duo 2FA can authenticate and access the applications; new users cannot. An illustration of that setup for new users could look something like the following diagram:

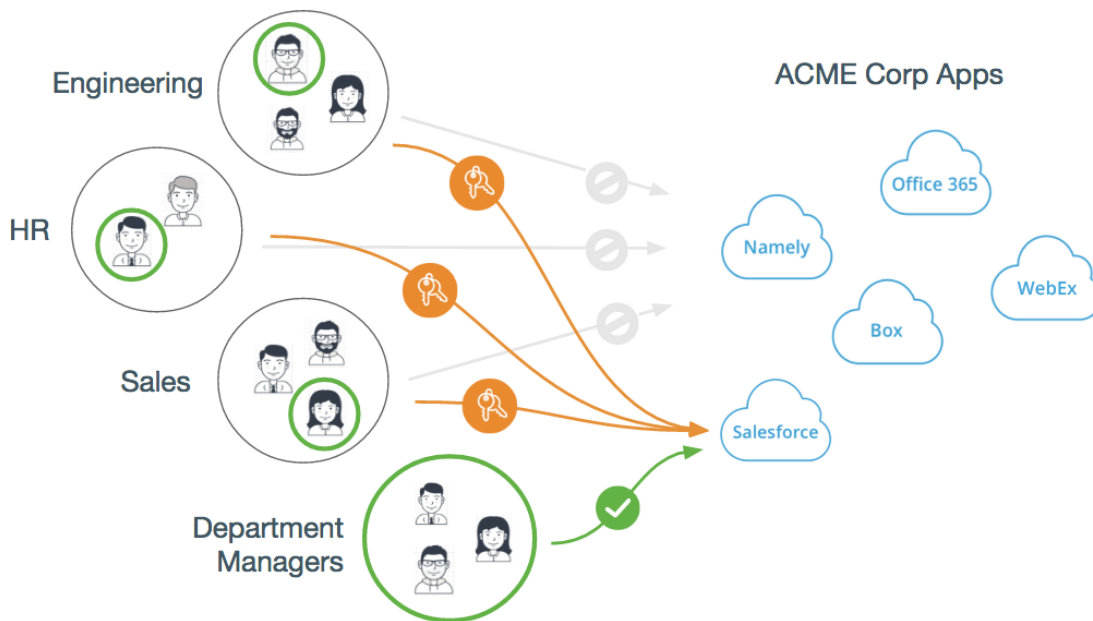


ACME then decides to protect their Salesforce application and knows there will be instances when new team members will need to access Salesforce. As a result, they've created and applied a new policy to the **Application** where they set the **New User Policy** to **Require Enrollment**. Now, **all new users** logging into the Salesforce application will see the Duo in-line enrollment workflow, which they will need to complete before gaining access to the Salesforce application. Previously enrolled users will still be required to complete 2FA, and the illustration above for new users would change to look like the following:

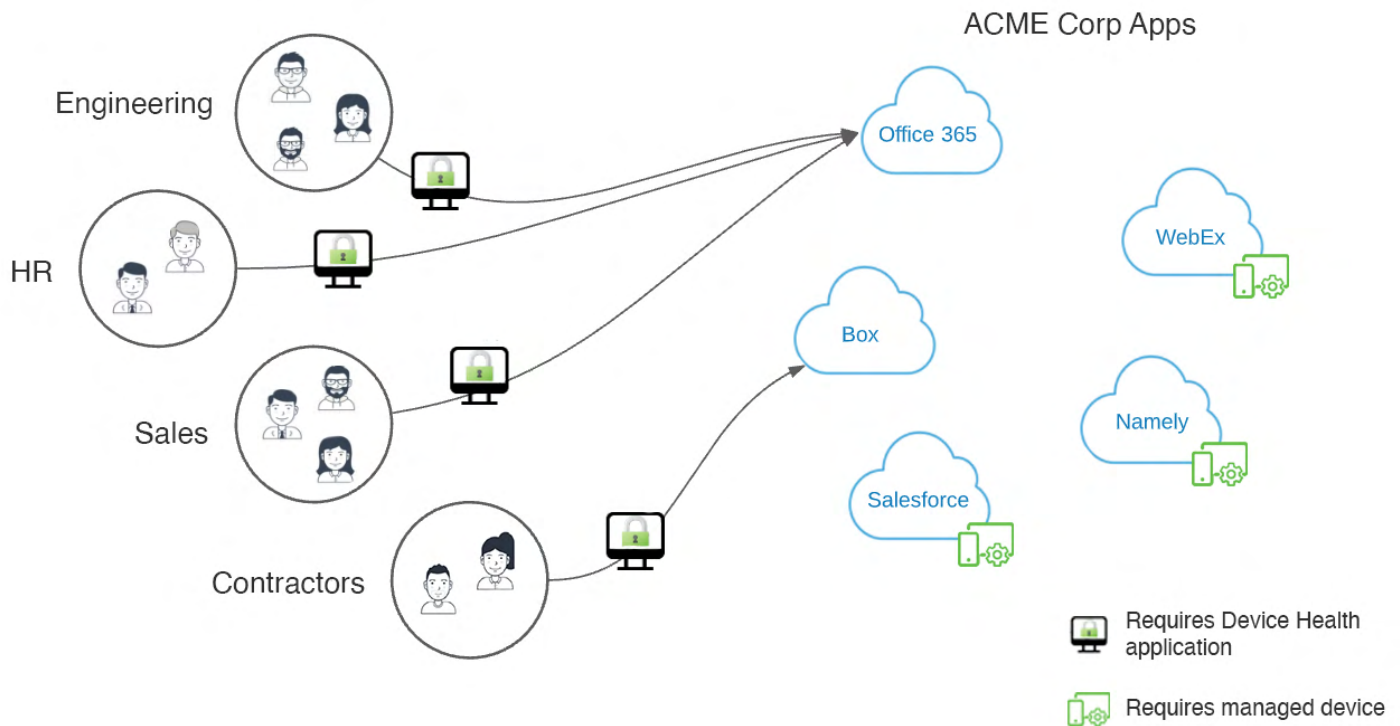


Because ACME department managers log into Salesforce several times a day, ACME decides to leverage the **Remembered Devices** policy for that specific user group. ACME can import groups and user membership using the AD Sync process or manually create groups and specify members manually from the Admin Panel.

Once the group exists in Duo, ACME creates a new policy with the **Remembered Devices** policy set to **9 hours**. The ACME admin then modifies the application, selects the **“Apply Policy to a Group of Users”** option, and chooses the new policy and the target group mentioned above. With this policy in place, only Department Managers logging into the Salesforce app will have the Remembered Devices option. The diagram below illustrates this scenario:



ACME allows employees to access Microsoft 365 and allows contractors to access Box file sharing on personal devices. For all other applications, ACME requires employees to use corporate-managed devices. To enable secure access for unmanaged devices, ACME creates a new policy for Microsoft 365 and Box using Duo’s **Device Health application** and requires the client to be installed and running before granting application access. The ACME admin then enforces device health check for up-to-date OS, password and disk encryption status. Next, the ACME admin creates a **Trusted Endpoints** policy for other applications to require only **managed devices** to be granted application access. With these policies in place, only trusted devices that meet ACME’s security requirements are granted access to business applications. The diagram below illustrates this scenario:



User Policy Settings

- [User Location Policies](#) (i.e., policies that are enforced based on the geographical origin of the user's device IP address) override Remembered Devices and Trusted Networks policies.
 - Example: Geo IP Policy is set to require 2FA from the United States and the policy also contains a trusted network CIDR block that is registered to the U.S. Users in that trusted network CIDR block will still be required to complete 2FA.
- The [New User Policy](#) is used to determine enrollment behavior when end-users not known to Duo log in to a Duo-protected application. This policy controls whether end-users are prompted to self-enroll or are blocked from accessing protected applications. The New User Policy applies to all usernames unknown to Duo (i.e. there is no information about them in the Admin Panel) or usernames without a 2FA device attached (i.e., partially enrolled, which is explained further in the Enrollment States section below).
- The [Authentication Policy](#) determines whether or not your fully and partially enrolled users are prompted to complete two-factor authentication (2FA) when they access a protected application. Users who have at least some information about them in the Duo Admin Panel are subject to the Authentication Policy.

Because only enrolled users can complete 2FA, partially enrolled end-users are instead prompted to complete the enrollment process when this policy is configured to enforce 2FA.

- Changing the Authentication Policy setting from the default setting (“Enforce 2FA”) prevents new users from completing in-line self-enrollment.
 - When set to “Bypass 2FA” users will bypass the authentication prompt when accessing the application, so there is no opportunity for self-enrollment. Fully and partially enrolled users may log in without completing 2FA unless another policy requires it.
 - The “deny access” setting blocks authentication to the application, so new or partially enrolled users cannot self-enroll in that scenario either.
 - End-users who receive enrollment links via email may complete the Duo enrollment process via the emailed link regardless of the Authentication Policy setting.

Device Policy Settings

- [Remembered devices](#): Duo's remembered devices feature is similar to the "remember my computer" or "keep me logged in" options users are accustomed to seeing during primary authentication on many websites. With the remembered devices feature enabled and the users checking this box, they will not be challenged for secondary authentication again when they log into that application from that device for the specified period of time.
- [Operating systems](#), [Browsers](#), and [Plugins](#): Use these policy settings to:
 - Restrict access and authentication from specific operating systems and versions.
 - Inform your users when their web browser or select plugins are out of date.
 - Optionally block access to applications protected with Duo from devices with outdated software.
- [Duo Device Health application](#) helps you control access to your applications through the policy system by restricting access when devices do not meet particular security requirements.

Administrators can [distribute the application for installation](#) on user’s devices in three ways:

- **User Self-install During Authentication** - The easiest way to distribute the Device Health application is to apply a Device Health policy to a web-based application that features Duo's authentication prompt and then let users self-install the client when prompted during Duo authentication.
- **Send Download Links to Users** - Notify your users of the new Device Health application requirement and give them the chance to install the application ahead of time. You can send these client download links to your users:
 - **macOS**: <https://dl.duosecurity.com/DuoDeviceHealth-latest.dmg>
 - **Windows 10**: <https://dl.duosecurity.com/DuoDeviceHealth-latest.msi>
- **Scripted or Managed Deployment** - Deploy the Device Health application via a [scripted install or an endpoint management tool](#), download the installers using the links above, and use the following syntax to automate installation:

- **macOS**: Extract the .pkg installer file from the downloaded .dmg file first.

```
sudo installer -pkg
/Volumes/DuoDeviceHealth/Install-DuoDeviceHealth.pkg -target /
```

- **Windows 10**: Replace the example MSI file name with your actual MSI filename.

```
msiexec /i /path/to/installer DuoDeviceHealth-2.4.0.msi
```


- Note that installation requires administrator privileges on both Windows and macOS.

Duo Device Health application has three operating modes:

- **Don't require users to have the app:** When this option is selected, the policy is not in effect and has no impact on end-user access.
 - **Require users to have the app:** When this option is selected, but none of the "Block access" options below it are selected, having the Device Health application installed and reporting information to Duo is required for access.
 - **Require users to have the app and "Block access":** When this option is selected and one or more of the "Block access" options are selected, the Device Health application must be installed and the device must satisfy the specified health requirements for access.
 - Block access if firewall is off.
 - Block access if disk encryption is off.
 - Block access if system password is not set.
 - Block access if an endpoint security agent is not running.
Note: For a list of supported endpoint security agents, click [here](#).
Endpoint security agent policy is available for Premier edition.
 - Use a combination of Device Health application policy and other Duo policies, including Browsers, Plugins, and Operating Systems policies.
 - Note: When an operating system policy and Device Health policy are both enabled, the Device Health application will be the preferred and a more trusted source of information about the endpoint OS over a user agent.
- **Trusted Endpoints** policy allows you to configure and either block untrusted (unmanaged) devices from gaining access *or* to inventory which connecting devices are currently trusted or untrusted. This policy tracks whether devices accessing the applications are verified via device certificates, application verification, or management status. Learn more in our [Getting Started with Trusted Endpoints course](#) on our free education platform, Duo Level Up.
 - **Certificate-based Trusted Endpoint verification will reach end-of-life in a future release.** Read more on Trusted Endpoints End-of-Life in the [Duo Trusted Endpoints Certificate Migration Guide](#).
 - Note that if you have a Trusted Endpoints policy in place set to "Require endpoints to be trusted," users who cannot complete Trusted Endpoints attestation will be blocked and unable to enroll or authenticate. Alternatively, you can elect to "Allow all endpoints," which will provide trustworthiness information in reporting but allow non-trusted endpoints until you are ready to change the policy to require all endpoints to be trusted. [Learn more about the Trusted Endpoints feature and policy configuration recommendations](#).
 - If you use Cisco Secure Endpoint as your endpoint security agent, you can [integrate Duo](#) with the agent using a connector application. This enables Duo and Cisco Secure Endpoint to have shared visibility into a Windows or macOS endpoint, and Duo can block access to protected applications by Duo from devices deemed as compromised by Cisco Secure Endpoint.

Enrollment States

Fully Enrolled



- A user is fully enrolled when a username exists in Duo **and** has at least one 2FA device attached.
 - The New User Policy **does not** apply to a user in this state.
 - Enrolled users who have not activated a smartphone or other Duo Push-capable device can authenticate using phone calls, SMS passcodes, and hardware tokens.
 - Enrolled users who have activated Duo Mobile can authenticate into Duo-protected applications using Duo Push notifications and generate passcodes with that device.

Partially Enrolled



- A user is partially enrolled when their username exists in Duo **but has no 2FA devices attached**.
 - An AD Sync process may have imported usernames without phone numbers. These users are **not** considered fully enrolled. Admins should consider how the New User Policy settings will impact users in this state.
 - **Please note the effect the New User Policy has on partially-enrolled users:**
 - If the New User Policy is set to “Allow access without 2FA,” users in a partially-enrolled state will be prompted to enroll.
 - If the New User Policy is set to “Deny access,” users in a partially-enrolled state will be denied access to the application until they enroll through another mechanism like an enrollment email or a Device Management Portal.
 - Users in this state **do** consume a license.
 - If the policy requires enrollment, but a user can’t enroll, that user can’t authenticate:
 - This can happen if conflicting application Policy settings require the user to self-enroll using an application that does not actually support the authentication prompt.
 - Check your RDP and thick clients like AnyConnect, Citrix Receiver, etc. Users will silently fail authentication with no feedback or error messages.
 - NOTE: There is an exception with WinLogon, which has an error message for unenrolled users (i.e., “The username you have entered is not enrolled with Duo Security”).
 - You will need to use the Authentication Policy to handle these scenarios.

Unenrolled / New User



- If a username is not listed in the Duo Admin Panel at all, the user is not enrolled. Their information will not appear in the Admin Panel and they will be considered a new user when they attempt to access Duo-protected applications.

More About New User Policy and Authentication Policy

New User Policy & Enrollment States

As mentioned previously, the [New User Policy](#) controls authentication for all users who are not fully or partially enrolled in Duo, also known as **unenrolled users**. There are three options for configuring New User Policy: Require Enrollment, Allow Access Without 2FA, and Deny Access.

Authentication Policy & Enrollment States

The [Authentication Policy](#) determines whether or not your fully and partially enrolled end-users are prompted to complete two-factor authentication (2FA) when they access a protected application. Users who have at least some information about them in the Duo Admin Panel are subject to the Authentication Policy.

How are they different?

Both New User and Authentication policy control enrollment behavior, but have one important difference; while New User policy targets only unenrolled users, the Authentication Policy applies to fully and partially enrolled end-users. By configuring both of these policies together, you can control how all of your employees experience authentication and enrollment.

The following table explains the expected required authentication experience for users in the different enrollment states with each New User Policy option enabled:

New User Policy	User State	Result
Require Enrollment	Fully enrolled	2FA required
Require Enrollment	Partially enrolled	Prompted to enroll*
Require Enrollment	Unknown to Duo	Prompted to enroll*
Allow Access without 2FA	Fully enrolled	2FA required
Allow Access without 2FA	Partially enrolled	Prompted to enroll*
Allow Access without 2FA	Unknown to Duo	Bypass 2FA/enrollment

Deny Access	Fully enrolled	2FA required
Deny Access	Partially enrolled	Denied access
Deny Access	Unknown to Duo	Denied access

*Thick clients like Cisco AnyConnect, Citrix Receiver, and the Duo Winlogon/RDP module will be denied access as they cannot display an enrollment prompt to the user.

User & Group Status

Active Status

- 2FA is required for a successful login unless overridden by other policy options.
 - It does not mean a user has activated Duo Mobile.

Bypass Status

- When a user is in bypass status, individual users or groups will bypass 2FA after successfully passing primary authentication.

Disabled Status

- The user is not permitted to use Duo two-factor authentication, and access is denied.

Status Controls

- Status can be controlled at both the user level and the group level, but keep in mind the following:
 - Status cannot be controlled at the user level for users that belong to a synced group; however, it is still possible to change the status of the entire synced group.
 - If the user status is set to active but the user belongs to one or more disabled groups, the user will remain in a disabled state until **all** groups the user belongs to are in an active state.

Administrative Roles & Units

All Duo administrators have an assigned role that determines what they can view and which actions they can perform in the Duo Admin Panel. They can also be provisioned into groups, or Administrative Units (AUs), that restrict which objects (e.g. users, applications) they can see and perform actions on.

Please see our documentation to learn more about Administrative Roles and Units:

- Administrative Roles: <https://duo.com/docs/admin-roles>
- Administrative Units: <https://duo.com/docs/administrative-units>

Access vs. Authentication Devices

It is important to distinguish between access and authentication devices and understand how they interact with policy.

Access Device: a mobile or desktop device an end-user uses to **access** an application.

Authentication Device: a mobile or desktop device an end-user uses to **perform authentication** with Duo.

Access and authentication devices must both meet all policy requirements; if there is any policy that the devices do not meet, the user will be denied access. This is also true for a device acting as **both** an access device and an authentication device (a smartphone, for example).

Below is an explanation of how policy configuration applies to devices:

Policy Type	Applies to Access Devices	Applies to Authentication Devices
Trusted Endpoints	Yes	No
Remembered Devices	Yes	No
Device Health Application	Yes	No
Operating Systems	Yes	Yes
Browsers	Yes	No
Plugins	Yes	No
Host Firewall	Yes	No
System Password	Yes	No
Full Disk Encryption	Yes*	Yes
Anti Virus Agent	Yes	No
Tampered Devices	No*	Yes
Screen Lock	No*	Yes
Mobile Device Biometrics	No*	Yes

*Note that these policy types can be enforced on access devices when using [the Duo Mobile Trusted Endpoints configuration](#).

Example (Operating Systems):

- Your organization has a Duo Operating Systems policy that blocks Windows Phones. If a user attempts to access a Duo-protected application by sending the 2FA request using Push or a Duo Mobile passcode from a Windows Phone, that user will be denied access to the application. This is

because the Operating Systems policy that denies access from Windows Phones is being applied to the authentication device.

Example (Browsers):

- Your organization has a Duo policy that requires browsers to be no more than 2 weeks out of date. A user's laptop has a version of Google Chrome that is long out of date. Suppose this user attempts to access a Duo-protected internal wiki from this laptop. In that case, they will be denied access until they can update Google Chrome to a version that satisfies the policy.

Example (Browsers + Device Encryption):

- Your organization has two Duo policies in place: one that requires browsers to be no more than 2 weeks out of date and another for authentication devices to have full-disk encryption enabled. A user's Android phone has full-disk encryption enabled, but Google Chrome is long out of date. If this user goes to access their Duo-protected internal wiki on this Android phone, they will be restricted from access until they update Google Chrome on the phone. In this case, their phone would have satisfied policy requirements as an authentication device but failed as an access device.

Example (Screen Lock + Operating System):

- Your organization has multiple policies in place: one that requires an operating system of Windows 8 or later, a screen lock policy, and no Android OS restrictions. If a user attempts to access a Duo-protected application with a Windows 10 desktop (access device) but attempts to approve the 2FA request using Push or Duo Mobile passcode from an Android authentication device that does NOT have screen lock enabled, that user will be denied access to the application. This is because the authentication device did not meet the policy requirement despite the user meeting the access device's operating system policy.

Example (Device Health Application + Operating System + Disk Encryption):

- Your organization has multiple policies in place: one that requires Device Health application to be installed, an operating system of Windows 10.0 xxxx (build version) or later, and disk encryption (Microsoft Bitlocker) must be enabled. If a user attempts to access a Duo-protected application with a Windows 10 desktop (access device) that has Duo Device Health Application installed but does not have the right Windows 10 build or disk encryption enabled, then that user will be denied access to the application until they can remediate device security status to satisfy the policy.

Enrollment & 2FA Enforcement Planning

Three stages make up a typical enrollment and enforcement strategy.

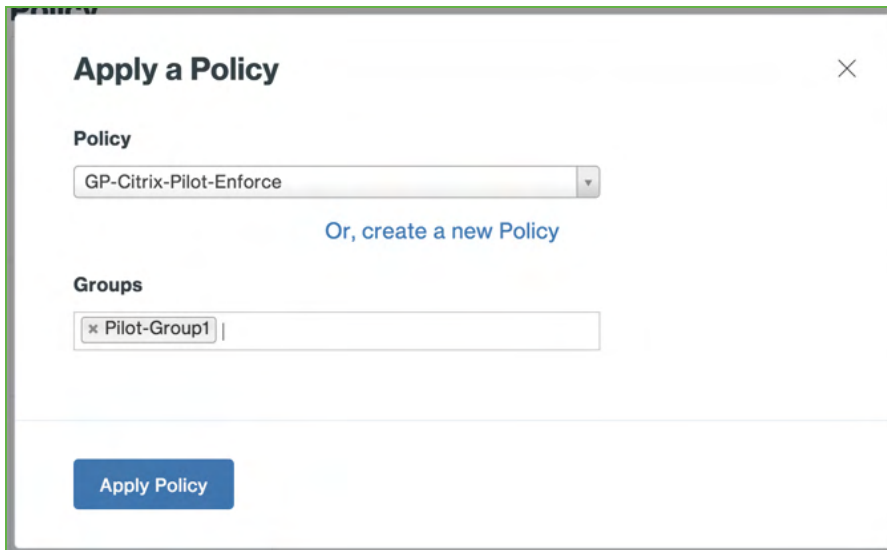
Stage 1: Targeting of Pilot Users on a Specific Application

This stage aims to enforce Duo 2FA and enrollment, potentially on a production application, to only specific groups of pilot users.

Important Note: AD Sync can be configured, but at this stage, we ONLY want to sync AD groups that contain pilot users.

This setup requires two policies: one Application Policy and one Group Policy.

1. Create a new group for the users you want to enforce 2FA/enrollment (*Pilot-Group1*).
 - a. Add users to this group.
2. Create and apply a new application policy (*AP-Citrix-Prod1*).
 - a. Set the New User Policy to “Allow access without 2FA.”
 - b. Set the Authentication Policy to “Bypass 2FA.”
3. Create another new policy (*GP-Citrix-Pilot-Enforce*).
 - a. Set the New User Policy to “Require enrollment.”
 - b. Set the Authentication Policy to “Enforce 2FA.”
4. Edit the application configuration.
 - a. Apply a Group Policy.
 - b. Select the policy created in step 3 and the group(s) created in step 1.



The screenshot shows a dialog box titled "Apply a Policy" with a close button (X) in the top right corner. Under the "Policy" section, a dropdown menu is set to "GP-Citrix-Pilot-Enforce". Below this is a blue link that says "Or, create a new Policy". Under the "Groups" section, a text input field contains "Pilot-Group1" with a small 'x' icon to its left. At the bottom of the dialog is a blue button labeled "Apply Policy".

- c. The final policy should look similar to the following:

Group policies

GP-Citrix-Pilot-Enforce Edit | Replace | Unassign

This policy applies to 1 group: [Pilot-Group1](#).

Enabled	New User Policy	Prompt unenrolled users to enroll whenever possible.
Enabled	Authentication Policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

[Apply another group policy](#)

Application policy

AP-Citrix-Prod1 Edit | Replace | Unassign

This policy applies to all users accessing this application.

Enabled	New User Policy	Allow unenrolled users to pass through without two-factor authentication.
Enabled	Authentication Policy	Skip two-factor authentication and enrollment, unless there is a superseding policy configured.

Global policy

Global Policy Edit Global Policy

This policy always applies to all applications.

Enabled	New-User-Policy	Prompt unenrolled users to enroll whenever possible. ⓘ
	Authentication-Policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured. ⓘ

Results:

- Fully and partially enrolled users that do not belong to the groups specified in the Group Policy will **not** be prompted to 2FA or enroll.
- Users unknown to Duo will log into the application without 2FA.
- Only partially and fully enrolled users that belong to the group(s) specified in the Group Policy **will** be prompted to 2FA or enroll.

Stage 2: Open Enrollment Period

At this stage, admins have several methods available to allow users to begin enrolling their devices with Duo.

1. [AD Sync](#) of usernames into Duo with the option to send enrollment emails
2. [Bulk Import](#)
3. [Device Management Portal](#) (not compatible with the Universal Prompt or the v4 Duo Web SDK)
 - Using this method, any valid user ID/password can log in to the Device Management Portal and walk through the enrollment process.

- Does not require that usernames pre-exist in Duo (AD Sync). Usernames will organically appear in Duo as users take the initiative to login to the DMP and complete the enrollment process.
 - Can create and customize enrollment emails that can include a link to the DMP for enrollment. These emails can then originate from internal email servers instead of Duo.
4. Create [Admin API](#) calls to [create users](#) and [send enrollment emails](#)
 5. Create an Auth API call to create the user and [generate an activation link](#).
 - The API response can be consumed/scripted for inclusion in a customized email that originates from internal email servers.

Stage 3: Determine When to Enforce 2FA & Enrollment

As the policies stand now, newly and partially enrolled users are NOT prompted for 2FA or enrollment when logging into the application unless they belong to the pilot group. This is due to the Authentication Policy setting.

Depending on the desired end-user experience, we can control whether newly enrolled users will see the Duo 2FA challenge when logging into the application immediately after completing enrollment or suppressing the 2FA prompt until a specific enforcement date.

Option 1: Big Bang Enforcement

On the go-live day, change the following Application Policy settings to begin enforcement of 2FA and enrollment on all users logging into the application (Note: you can always override these settings for specific users/groups by applying additional group policies):

1. On the application policy (*AP-Citrix-Prod1*):
 - a. Set the New User Policy to “Require Enrollment.”
 - b. Set the Authentication Policy to “Enforce 2FA.”
 - c. The final policy will look as follows:

Group policies

GP-Citrix-Pilot-Enforce Edit | Replace | Unassign

This policy applies to 1 group: [Pilot-Group1](#).

✔ Enabled	New User Policy	Prompt unenrolled users to enroll whenever possible.
✔ Enabled	Authentication Policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

[Apply another group policy](#)

Application policy

AP-Citrix-Prod1 Edit | Replace | Unassign

This policy applies to all users accessing this application.

✔ Enabled	New User Policy	Prompt unenrolled users to enroll whenever possible.
✔ Enabled	Authentication Policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Global policy

Global Policy Edit Global Policy

This policy always applies to all applications.

✔ Enabled	New-User-Policy	Prompt unenrolled users to enroll whenever possible. ⓘ
	Authentication Policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured. ⓘ

Results:

- Partially enrolled users will be prompted to enroll (AD Sync).
- Users unknown to Duo will be prompted to enroll.
- Fully enrolled users will be prompted for 2FA.
- Fully enrolled and partially enrolled users that belong to the group(s) specified in the group policy will still be prompted to 2FA or enroll.
- The group policy we created in stage 1 for the pilot group is no longer necessary and can be removed.

Option 2: Strict Big Bang Enforcement

A slight twist on the previous option, this method will deny authentication and enrollment to users who do not belong to groups specified in the group policy.

On the go-live day, change the following Application and Group Policy settings to begin enforcement of 2FA and enrollment on specific users logging into the application:

1. On the Application Policy (*AP-Citrix-Prod1*):
 - a. Set the New User Policy to “Deny Access.”
 - b. Set the Authentication Policy to “Deny Access.”

2. On the Group Policy (*GP-Citrix-Pilot Enforce*):
 - a. Set the New User Policy to “Require Enrollment.”
 - b. Set the Authentication Policy to “Enforce 2FA.”
3. Apply the Group Policy created above to a group that contains all users (*All-Duo-Enforced-Users*).
4. The policy will look as follows:

The screenshot displays the Duo policy configuration interface, organized into three sections: Group policies, Application policy, and Global policy.

Group policies: The main policy is **GP-Citrix-Pilot-Enforce**, which applies to 1 group: *All-Duo-Enforced-Users*. It includes two active policies:

- New User Policy:** Enabled. Prompt unenrolled users to enroll whenever possible.
- Authentication Policy:** Enabled. Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

A button labeled "Apply another group policy" is visible below the group policy details.

Application policy: The main policy is **AP-Citrix-Prod1**, which applies to all users accessing this application. It includes two active policies:

- New User Policy:** Enabled. Deny access to unenrolled users.
- Authentication Policy:** Enabled. Deny authentication to all users.

Global policy: The main policy is **Global Policy**, which always applies to all applications. It includes two active policies:

- New User Policy:** Enabled. Prompt unenrolled users to enroll whenever possible.
- Authentication Policy:** Enabled. Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

An "Edit Global Policy" button is located to the right of the Global Policy header.

Results:

- Fully enrolled and partially enrolled users that belong to the group(s) specified in the Group Policy will still be prompted to 2FA or enroll.
- Any partially enrolled or fully enrolled users that **do not belong** to the group(s) specified in the Group Policy will be denied access.
- Users unknown to Duo will be denied access.

Option 3: Immediate Opt-in Enforcement of 2FA

Making the policy changes below will immediately begin prompting users who complete enrollment using the Device Management portal for 2FA when logging into the application.

NOTE: With this option, admins should wait to perform AD Sync for the general user population until just before the enforcement deadline or even afterwards. This is because the AD Sync process creates

“partially enrolled” users and the policy change below would begin prompting all users in this state for 2FA and enrollment when logging into the application.

1. On the application policy (*AP-Citrix-Prod1*):
 - a. Set the Authentication Policy to “Enforce 2FA.”
 - b. The policy will look as follows:

The screenshot displays the Duo policy configuration interface, organized into three main sections: Group policies, Application policy, and Global policy.

- Group policies:** Shows a policy named "GP-Citrix-Pilot-Enforce" applied to the group "All-Duo-Enforced-Users". It lists two enabled policies:
 - New User Policy:** Prompt unenrolled users to enroll whenever possible.
 - Authentication Policy:** Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
- Application policy:** Shows a policy named "AP-Citrix-Prod1" applied to all users accessing this application. It lists three enabled policies:
 - New User Policy:** Allow unenrolled users to pass through without two-factor authentication.
 - Authentication Policy:** Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
 - Device Health Application:** Don't require users to have the app.
- Global policy:** Shows the "Global Policy" which always applies to all applications. It lists two enabled policies:
 - New-User-Policy:** Prompt unenrolled users to enroll whenever possible.
 - Authentication-Policy:** Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Results:

- Partially enrolled users will be prompted to enroll.
- Users unknown to Duo will pass through to the application after passing primary authentication without 2FA.
- Fully enrolled users will be prompted for 2FA.
- Fully enrolled and partially enrolled users that belong to the group(s) specified in the Group Policy **will** still be prompted to 2FA or enroll.

On the Go-Live Day:

- Perform AD sync on the general user groups.

- Change the following Application Policy settings to begin enforcement of 2FA and enrollment on **all users** logging into the application. This will then capture and enforce users who did not enroll during the open enrollment period:
 - On the Application Policy (*AP-Citrix-Pilot Enforce*), set the New User Policy to “Require Enrollment.”

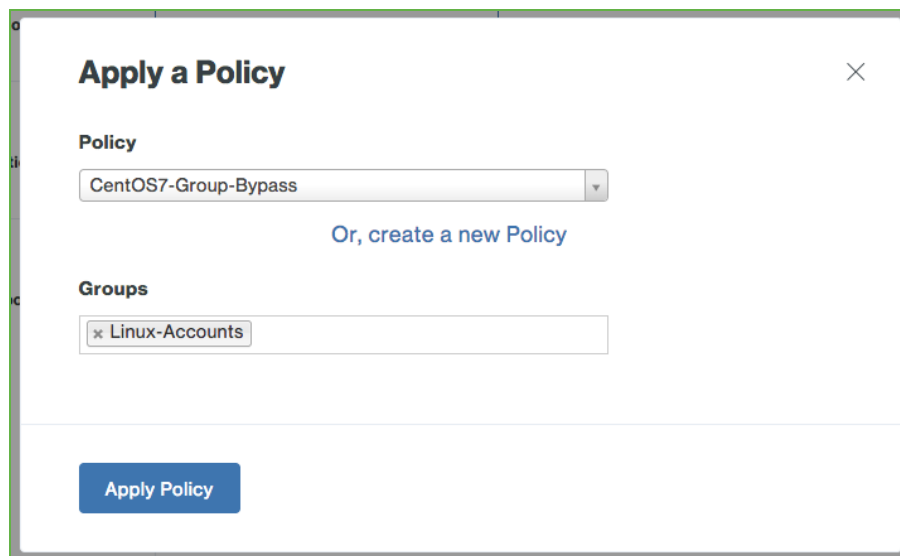
Policy Example Scenarios

There are common use cases for policies that admins often want to configure. These example scenarios take you through these use cases step-by-step to get your policies implemented quickly and easily.

Enrollment - Scenario 1

I want to enforce 2FA and enrollment on a specific application but still allow specific groups of users to bypass 2FA.

1. Create or AD sync a group of users that you want to bypass 2FA (*Linux-Accounts*).
2. Create a new policy (*CentOS7-Group-Bypass*).
 - a. Set the New User Policy to “Require enrollment.”
 - b. Set the Authentication Policy to “Bypass 2FA.”
3. Edit the application configuration.
 - a. Apply a Group Policy.
 - b. Select the policy created in Step 2 and the group(s) created in Step 1.



The screenshot shows a dialog box titled "Apply a Policy" with a close button (X) in the top right corner. Under the "Policy" section, a dropdown menu is set to "CentOS7-Group-Bypass". Below this, there is a link that says "Or, create a new Policy". Under the "Groups" section, there is a text input field containing a tag for "Linux-Accounts". At the bottom of the dialog, there is a blue button labeled "Apply Policy".

4. Your final policy should look similar to the following:

Group policies

CentOS7-Group-Bypass Edit | Replace Unassign

This policy applies to 1 group: Linux-Accounts.

Enabled	New User Policy	Prompt unenrolled users to enroll whenever possible.
Enabled	Authentication Policy	Skip two-factor authentication and enrollment, unless there is a superseding policy configured.

[Apply another group policy](#)

Application policy

[Apply a policy to all users](#)

Global policy

Global Policy Edit Global Policy

This policy always applies to all applications.

Enabled	New User Policy	Prompt unenrolled users to enroll whenever possible. ●
	Authentication Policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured. ●

Results:

- Fully enrolled and partially enrolled users who **are** a member of the “Linux-Accounts” group will **not** be prompted for enrollment or 2FA because of the Authentication Policy.
- Fully enrolled and partially enrolled users who are **not** a member of the “Linux-Accounts” group **will** be prompted for enrollment and 2FA.
- Users unknown to Duo will be prompted to enroll.

Enrollment - Scenario 2

I want all users to bypass 2FA on a specific application EXCEPT for fully enrolled users. I still want to prompt partially enrolled users for enrollment.

1. Create and apply a new Application Policy (*WebSDK-App-Policy*).
 - a. Set the New User Policy to “Allow access without 2FA.” This setting overrides the Global Policy.
 - b. Set the Authentication Policy to “Enforce 2FA.” This setting overrides the Global Policy.
 - c. The effective policy should look like the following:

The screenshot displays the Duo policy configuration interface, divided into three sections: Group policies, Application policy, and Global policy.

- Group policies:** Contains a button labeled "Apply a policy to groups of users".
- Application policy:** Shows the "WebSDK-App-Policy" which applies to all users accessing this application. It includes "Edit", "Replace", and "Unassign" actions. Below the title, two policies are listed:
 - New User Policy:** Enabled. Description: "Allow unenrolled users to pass through without two-factor authentication."
 - Authentication Policy:** Enabled. Description: "Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured."
- Global policy:** Shows the "Global Policy" which always applies to all applications. It includes an "Edit Global Policy" button. Below the title, two policies are listed:
 - New-User-Policy:** Enabled. Description: "Deny access to unenrolled users."
 - Authentication-Policy:** Enabled. Description: "Deny authentication to all users."

Results:

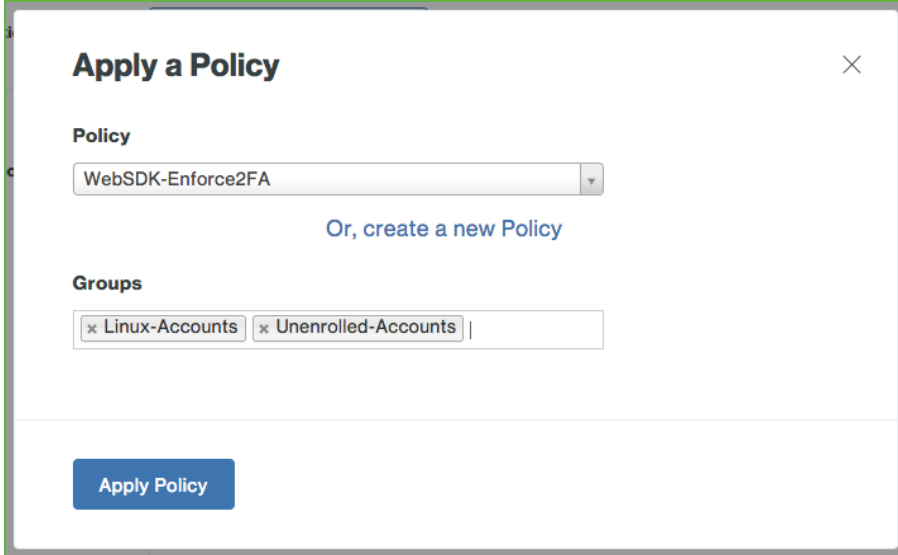
- Partially enrolled users will be prompted to enroll.
- Users unknown to Duo will pass through to the application after passing primary authentication without 2FA.
- Fully enrolled users will be prompted for 2FA.

Enrollment - Scenario 3

I want all users to bypass 2FA/enrollment on a specific application EXCEPT for specific groups of users. In addition, I don't want to prompt partially enrolled users for enrollment unless they belong to the group(s) previously mentioned.

This setup requires two policies: one Application Policy and one Group Policy.

1. Create a new group for the users you want to enforce 2FA/enrollment (*Linux-Accounts, Unenrolled Accounts*).
 - a. Add users to this group.
2. Create and apply a new Application Policy (*WebSDK-App-Policy*).
 - a. Set the New User Policy to "Allow access without 2FA."
 - b. Set the Authentication Policy to "Bypass 2FA."
3. Create another new custom policy (*WebSDK-Enforce2FA*).
 - a. Set the New User Policy to "Require enrollment."
 - b. Set the Authentication Policy to "Enforce 2FA."
4. Edit the application configuration.
 - a. Apply a Group Policy.
 - b. Select the policy created in step 3 and the group(s) created in step 1.



Apply a Policy ×

Policy

WebSDK-Enforce2FA ▾

[Or, create a new Policy](#)

Groups

× Linux-Accounts × Unenrolled-Accounts |

Apply Policy

- c. The final policy should look similar to the following:

Group policies

WebSDK-Enforce2FA Edit | Replace | Unassign

This policy applies to 2 groups: [Linux-Accounts](#), [Unenrolled Accounts](#).

Enabled	New User Policy	Prompt unenrolled users to enroll whenever possible.
Enabled	Authentication Policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

[Apply another group policy](#)

Application policy

WebSDK-App-Policy Edit | Replace | Unassign

This policy applies to all users accessing this application.

Enabled	New User Policy	Allow unenrolled users to pass through without two-factor authentication.
Enabled	Authentication Policy	Skip two-factor authentication and enrollment, unless there is a superseding policy configured.

Global policy

Global Policy Edit Global Policy

This policy always applies to all applications.

Enabled	New-User-Policy	Prompt unenrolled users to enroll whenever possible. Ⓢ
	Authentication-Policy	Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured. Ⓢ

Results:

- Partially enrolled users that do not belong to the groups specified in the Group Policy will **not** be prompted for enrollment and will bypass 2FA.
- Users unknown to Duo will log into the application without 2FA.
- Only partially and fully enrolled users that belong to the group(s) specified in the Group Policy **will** be prompted to 2FA or enroll.

Adding More Security to an Application - Scenario 1

I have most of my users enrolled in Duo, and I now want to change my New User Policy on a specific application to a more secure option: “Deny Access.”

1. Create and apply a New Application Policy (*New-User-Deny*).
 - a. Set the New User Policy to “Deny access to unenrolled users.”
2. Your policy should look like the following:

The screenshot displays the Duo policy configuration interface. At the top, under 'Group policies', there is a button labeled 'Apply a policy to groups of users'. Below this, the 'Application policy' section shows a policy named 'New-User-Deny' with the description 'This policy applies to all users accessing this application.' and actions 'Edit', 'Replace', and 'Unassign'. The policy is 'Enabled' and has a 'New User Policy' of 'Deny access to unenrolled users.' Below the application policy, the 'Global policy' section shows a 'Global Policy' that 'always applies to all applications.' with an 'Edit Global Policy' button. The global policy is 'Enabled' and has a 'New-User-Policy' of 'Prompt-unenrolled-users-to-enroll-when-ever-possible.' and an 'Authentication Policy' of 'Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.'

Results:

- Fully enrolled users will be able to log into the application and will be challenged for 2FA.
- Partially enrolled users will **not** be able to log into the application.
 - The user can still enroll by clicking the link contained in the enrollment email.
 - The user can still call the help desk and have a 2FA device manually attached to the account.
- Users unknown to Duo will **not** be able to log into the application.

Adding More Security to an Application - Scenario 2

I have most of my users enrolled in Duo, and I now want to change my New User Policy on a specific application to a more secure option: “Deny Access.” However, I have a specific group of stragglers I would still like to prompt for enrollment upon first logging into the application.

This setup requires two policies: one Application Policy and one Group Policy.

1. Manually create or use AD Sync to bring in a group of users you still want to prompt for enrollment when logging into the application (*Straggler-Group*).
2. Create and apply a new Application Policy (*New-User-Deny*).
 - a. Set the New User Policy to “Deny access.”
 - b. Set the Authentication Policy to “Enforce 2FA.”
3. Create another new custom policy (*Straggler-Enrollment*).
 - a. Set the New User Policy to “Require enrollment.”
 - b. Set the Authentication Policy to “Enforce 2FA.”
4. Edit the application configuration.
 - a. Apply a Group Policy.
 - b. Select the policy created in step 3 and the group(s) created in step 1.
 - c. The final policy should look similar to the following:

The screenshot displays the Duo policy configuration interface, organized into three sections: Group policies, Application policy, and Global policy.

- Group policies:** A policy named "Straggler-Enrollment" is applied to the "Straggler-Group". It includes two enabled policies:
 - New User Policy:** Prompt unenrolled users to enroll whenever possible.
 - Authentication Policy:** Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
- Application policy:** A policy named "New-User-Deny" is applied to all users accessing the application. It includes two enabled policies:
 - New User Policy:** Deny access to unenrolled users.
 - Authentication Policy:** Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
- Global policy:** A policy named "Global Policy" is applied to all applications. It includes two enabled policies:
 - New-User-Policy:** Prompt-unenrolled-users-to-enroll-when-ever-possible.
 - Authentication-Policy:** Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

Results:

- Fully enrolled users will be able to log into the application and will be challenged for 2FA.
- Partially enrolled users that do **not** belong to the group specified in the Group Policy will **not** be able to log into the application.
 - The user can still enroll by clicking the link contained in the enrollment email.
 - The user can still call the help desk and have a 2FA device manually attached to the account.
- Partially enrolled users that belong to the “Stragglers” group specified in the policy will be prompted to enroll.
- Users unknown to Duo will **not** be able to log into the application.

Enrollment & Authorized Networks - Scenario 1

I have an application where I only want to prompt users for 2FA when accessing the application from external networks. I want my internal users to bypass 2FA and enrollment.

1. Create and apply a new Application Policy.
 - a. Set the New User Policy to “Require enrollment.”
 - b. Set the Authentication Policy to “Enforce 2FA.”
 - c. In the Authorized Networks section of the policy, enter the IP ranges of the internal networks. Be sure to uncheck the “Require enrollment from these networks” option. Networks listed here will bypass 2FA and enrollment.

The screenshot displays the Duo Policy Editor interface. At the top, under 'Group policies', there is a button 'Apply a policy to groups of users'. Below this, the 'Application policy' section shows a policy named 'Bypass-Internal-Users' with options to 'Edit', 'Replace', or 'Unassign'. The policy description is 'This policy applies to all users accessing this application.' It lists three settings: 'New User Policy' (Enabled) with the value 'Prompt unenrolled users to enroll whenever possible.', 'Authentication Policy' (Enabled) with the value 'Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.', and 'Authorized Networks' (Enabled) with the value 'Allow access without 2FA for these networks: 192.0.2.8, 198.51.100.0.'. The 'Global policy' section shows a 'Global Policy' that 'always applies to all applications' with an 'Edit Global Policy' button. It lists two settings: 'New-User-Policy' (Enabled) with the value 'Prompt unenrolled users to enroll whenever possible.' and 'Authentication-Policy' (Enabled) with the value 'Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.'.

Results:

- Any user logging into the application from an IP in the Authorized Networks list will bypass 2FA and enrollment. This includes fully enrolled users, partially enrolled users, and users unknown to Duo.
- Fully enrolled users logging into the application from an untrusted IP will be required to 2FA.
- Partially enrolled users logging into the application from an untrusted IP will be prompted to enroll.
- Users unknown to Duo logging into the application from an untrusted IP will be prompted for enrollment.

Enrollment & Authorized Networks - Scenario 2

I have an application where I only want to prompt users for 2FA when accessing the application from external networks. I want my internal users to bypass 2FA and enrollment when logging into the application, except for a specific group of privileged users that I always want to require 2FA, regardless of where they log in from.

This setup requires two policies: one Application Policy and one Group Policy.

1. Manually create or use AD Sync to import a group of users you still want to prompt for enrollment when logging into the application, regardless of location (*ADSync-VPN-Admins*).
2. Create and apply a new Application Policy (*WebSDK-Application-Authorized-Network*).
 - a. Set the New User Policy to “Require enrollment.”
 - b. Set the Authentication Policy to “Enforce 2FA.”
 - c. In the Authorized Networks section of the policy, enter the IP ranges of the internal networks. Be sure to uncheck the “Require enrollment from these networks” option. Networks listed here will bypass 2FA and enrollment.
3. Create another new policy (*Power-Users-Always2FA*).
 - a. Set the New User Policy to “Require enrollment.”
 - b. Set the Authentication Policy to “Enforce 2FA.”
 - c. Set the Authorized Networks list to “None.”
4. Edit the application configuration.
 - a. Apply a Group Policy.
 - b. Select the policy created in step 3 and the group(s) created in step 1.
 - c. Apply an Application policy.
 - d. Select the policy created in step 2.
 - e. The final policy should look similar to the following:

The screenshot displays two policy configuration panels. The top panel is for a Group Policy named "Power-Users-Always2FA", which applies to the group "ADSync-VPN-Admins". It has three settings: "New User Policy" (Enabled, "Prompt unenrolled users to enroll whenever possible."), "Authentication Policy" (Enabled, "Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured."), and "Authorized Networks" (Enabled, "No networks."). Below this panel is a button labeled "Apply another group policy". The bottom panel is for an Application Policy named "WebSDK-Application-Authorized-Network", which applies to all users. It also has three settings: "New User Policy" (Enabled, "Prompt unenrolled users to enroll whenever possible."), "Authentication Policy" (Enabled, "Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured."), and "Authorized Networks" (Enabled, "Allow access without 2FA for these networks: 192.0.2.8.").

Policy Type	Policy Name	Applies To	Settings
Group Policy	Power-Users-Always2FA	ADSync-VPN-Admins	<ul style="list-style-type: none">New User Policy: Enabled, Prompt unenrolled users to enroll whenever possible.Authentication Policy: Enabled, Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.Authorized Networks: Enabled, No networks.
Application Policy	WebSDK-Application-Authorized-Network	All users	<ul style="list-style-type: none">New User Policy: Enabled, Prompt unenrolled users to enroll whenever possible.Authentication Policy: Enabled, Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.Authorized Networks: Enabled, Allow access without 2FA for these networks: 192.0.2.8.

Results:

- Fully and partially enrolled users that belong to the “Power-Users” group will be prompted for 2FA and enrollment, regardless of location.
- Users logging into the application from an IP in the Trusted Networks list **and** do not belong to the “Power-Users” group will bypass 2FA and enrollment. This includes: fully enrolled users, partially enrolled users, and users unknown to Duo.
- All fully enrolled users logging into the application from an untrusted IP will be required to 2FA.
- All partially enrolled users logging into the application from an untrusted IP will be prompted for enrollment.
- All users unknown to Duo logging into the application from an untrusted IP will be prompted for enrollment.

Enrollment & User Location - Scenario

I have an application where I want to deny access to a group of privileged users if they are in a specified location.

1. Manually create or use AD Sync to import a group of users you will want to deny access to based on their location (*Power-Admins*).
2. Create and apply a new Group Policy (*Deny-Based-on-User-Location*)
 - a. In the User Location section of the policy, enter the country you want to take action on and select "Deny access."
3. Edit the application configuration.
 - a. Apply a Group Policy.
 - b. Select the policy created in step 2 and the group(s) created in step 1.

Results:

- Any user in the group *Power-Admins* who is logging into the application from an IP in the country specified in the User Location policy will be denied access.

Remembered Devices - Adding More Granular Restrictions - Scenario

I want the majority of our applications to allow users to choose to remember their devices for a 30-day timeframe without being re-prompted to authenticate but require that two particularly sensitive applications have a timeframe of only 4 hours.

1. Edit your Global Policy.
 - a. In the Remembered Devices section of the policy, select the options “**Users may choose to remember their devices for 30 days for all protected web applications.**”
2. Create and apply a new Application Policy (*AP-Remember-Device-4-Hours*)
 - a. In the Remembered Devices section of the policy, select the options “**Users may choose to remember their devices for 4 hours for all protected web applications.**”
3. Edit the application configuration for the first application for which you want to require the 4-hour timeframe.
 - a. Apply an Application Policy.
 - b. Select the policy created in step 2.
4. Repeat step 3 for the second application for which you want to require the 4-hour timeframe.

Results:

- Any users accessing either of the two particularly sensitive applications to which the Application Policy *AP-Remember-Device-4-Hours* has been applied will be able to choose to have their device remembered for 4 hours.
- All other applications affected by the Global Policy will be linked with a shared Remembered Devices session cookie, allowing users to only be re-prompted once every 30 days when accessing any of these applications.
- The Remembered Devices session cookie is not shared between the global 30-day policy and the application-level 4-hour policy. Because the Application Policy overrides the Global Policy, applications configured with the Application Policy will require Duo authentication at the end of any 4-hour Remembered Devices session.

Device Health Application - Enforce Device Health Checks - Scenario

I have an application where I want to deny users access if the access device does not have disk encryption enabled.

1. Create and apply a new Application Policy (*DHA-Disk-Encryption-Off-Deny*)
 - a. Go to the **Applications** tab in the Admin Panel.
 - b. Select the application you want the policy to apply to.
 - c. In the Policy section, click on “**Apply a policy to all users**” to create an Application Policy.
 - d. Select “**Create a new policy**”.
 - e. Click **Device Health Application** under the Devices section of the policy.
 - i. Select **Require users to have the app** on the OS(s) of your choice.
 - ii. Check **Block access if Bitlocker / FileVault is off**.
 - f. Create and apply the policy.

The screenshot displays the Duo Admin Panel configuration for a Device Health application. On the left, a sidebar lists various policy categories: Policy name (DHA-Disk-Encryption-), Users (New User policy, Authentication policy, User location), Devices (Trusted Endpoints, Device Health application, Remembered devices, Operating systems, Browsers, Plugins), Networks (Authorized networks, Anonymous networks), and Authenticators (Authentication methods, Duo Mobile app). The main panel, titled "Device Health application", contains the following settings:

- Policy name: DHA-Disk-Encryption-
- Users: New User policy, Authentication policy, User location
- Devices: Trusted Endpoints, **Device Health application**, Remembered devices, Operating systems, Browsers, Plugins
- Networks: Authorized networks, Anonymous networks
- Authenticators: Authentication methods, Duo Mobile app

The "Device Health application" configuration includes:

- macOS: Enforcing
- Windows: Enforcing
- Options for requiring users to have the app:
 - Don't require users to have the app
 - Require users to have the app** ⓘ
- Block access if BitLocker is off: (When the user is blocked, the app will provide remediation. See what it looks like ⓘ)
- Block access if firewall is off:
- Block access if system password is not set:
- Block access if an endpoint security agent is not running:
- Select which Duo supported endpoint security agent(s) are allowed: Select one or more endpoint security agents
- Enter remediation instructions for your end users. This will appear on the Device Health application remediation screen when your end user has been blocked. (Max. 700 characters)
- Learn more ⓘ

Results:

- Users accessing the protected application for the first time since enforcing this policy will need to download and install the Device Health Application. There are three options available to distribute the client application:
 - Let users [self-install the client when prompted during Duo authentication](#).
 - Notify your users of the new Device Health application requirement and give them the chance to install the application ahead of time by sending client download links:
 - **macOS**: <https://dl.duosecurity.com/DuoDeviceHealth-latest.dmg>
 - **Windows 10**: <https://dl.duosecurity.com/DuoDeviceHealth-latest.msi>
 - Deploy the Device Health application via a scripted install or an endpoint management tool

- Any user that logs into the application from a device that does not have the Device Health Application installed or has the disk encryption turned off will be denied access and guided with the remediation steps to turn the disk encryption ON.

Operating System Policy - Block out-of-date Windows Devices - Scenario

I want to encourage users to update their Operating System (OS) on Windows devices two weeks after Microsoft’s latest build version is available. I also want to block access to all applications from any device that is not running the latest version after a month.

- Edit your Global Policy.
 - In the Operating Systems section of the policy, check **“Allow Windows Devices”**.
 - Under the “Encourage users to update” section, from the first drop-down menu, select **“If less than the latest”** and from the second drop-down menu, select **“After 2 weeks”**.
 - Under “Block versions” section, from the first drop-down menu, select **“If less than the latest”** and from the second drop-down menu, select **“After 1 month”**.

The screenshot shows the configuration for the "Allow Windows devices" policy. It is divided into two main sections: "Encourage users to update" and "Block versions".

Encourage users to update:

- The checkbox "Allow Windows devices" is checked.
- The first drop-down menu is set to "If less than the latest".
- The second drop-down menu is set to "After 2 weeks".

Block versions:

- The first drop-down menu is set to "If less than the latest".
- The second drop-down menu is set to "After 1 month".

Informational text on the right:

- If Device Health Application policy is not enabled, less than latest will fall back to Windows 10.** (with a "Learn more" link)
- If a version becomes out of date**
 - Day 1 - 14**: no message to update is shown
 - Day 14 - 1 month**: If Device Health application is installed, then Windows 10 devices will be encouraged to update to: **10.0 2004 (19041.450) or 10.0 1909 (18363.1016) or 10.0 1903 (18362.1016) or 10.0 1809 (17763.1397)** (with a "Windows release information" link)
 - After 1 month**: users are blocked

- In the Device Health application section of the policy, check **Require users to have the app.**
 Note: If the Duo Device Health application is not enabled, then the policy engine will fall back to simply “Windows 10” when assessing the Windows version of the device accessing a Duo-protected application.
- Click **“Save Policy”**.

Results:

- Users accessing any protected application from Windows devices will be notified via an alert and encouraged to update their OS to the latest version 2 weeks after Microsoft makes it available.
- One month after the new Windows build version is available from Microsoft, all access devices that are not running the latest version will be blocked.