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

Version 4.3 Published November 27, 2019
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

Enrollment States
   Fully Enrolled
   Partially Enrolled

More About New User Policy
   New User Policy & Enrollment States
   New User Policy & Trusted Endpoints

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 Additional Security to an Application - Scenario 1
   Adding Additional 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
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.
Policy Definitions & Guidelines

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

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 MFA customers receive a subset of the Global Policy settings available in Duo Access and Duo Beyond.

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 will appear crossed out in the Global Policy section of that Application page. 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.
- **Note:** Paid Duo editions allow for the custom policies available on those editions to be shared between applications.

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 Global Policy is overridden by a Group 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. Instructions on how to change the order of policies can be found [here](#).
- **Note:** [Custom policies for groups](#) are only available in Duo Access and Duo Beyond. [Authentication Policy](#), which overrides the New User Policy and controls whether users are required to 2FA or prompted to enroll, is available on all editions.
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 have 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 set-up 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 have 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, clicks 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:

![Diagram showing policy settings and user groups]

**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 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 controls enrollment options for usernames unknown to Duo or usernames without a 2FA device attached (i.e. partially enrolled, which is explained further below).

- The Authentication Policy controls authentication behavior. **(Note: In Duo MFA edition, the Authentication Policy can only be applied to an application policy, which will impact all users logging into that application.)**
  - Changing the Authentication Policy setting from the default setting (“No action”) prevents new users from completing in-line self-enrollment.
    - When set to “allow,” users not enrolled in Duo will bypass the frame entirely when accessing the application, so there is no opportunity for self-enrollment.
    - The “deny” setting blocks authentication to the application, so new 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.
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 through 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:
    - 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.
More About New User Policy

New User Policy & Enrollment States

As mentioned previously, the New User Policy controls authentication for users not yet enrolled in Duo. There are three options for configuring New User Policy: Require Enrollment, Allow Access Without 2FA, and Deny Access. The following table explains expected 2FA behavior for users in the different enrollment states with each New User Policy option enabled:

<table>
<thead>
<tr>
<th>New User Policy</th>
<th>User State</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Enrollment</td>
<td>Fully Enrolled</td>
<td>2FA Required</td>
</tr>
<tr>
<td>Require Enrollment</td>
<td>Partially Enrolled</td>
<td>Prompted to Enroll*</td>
</tr>
<tr>
<td>Require Enrollment</td>
<td>Unknown to Duo</td>
<td>Prompted to Enroll*</td>
</tr>
<tr>
<td>Allow Access</td>
<td>Fully Enrolled</td>
<td>2FA Required</td>
</tr>
<tr>
<td>Allow Access</td>
<td>Partially Enrolled</td>
<td>Prompted to Enroll*</td>
</tr>
<tr>
<td>Allow Access</td>
<td>Unknown to Duo</td>
<td>Bypass 2FA/Enrollment</td>
</tr>
<tr>
<td>Deny Access</td>
<td>Fully Enrolled</td>
<td>2FA Required</td>
</tr>
<tr>
<td>Deny Access</td>
<td>Partially Enrolled</td>
<td>Denied Access</td>
</tr>
<tr>
<td>Deny Access</td>
<td>Unknown to Duo</td>
<td>Denied Access</td>
</tr>
</tbody>
</table>

*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.

New User Policy & Trusted Endpoints

You can configure Duo’s Trusted Endpoints functionality to either block untrusted (unmanaged) devices from gaining access or to inventory which connecting devices are currently trusted or untrusted.

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 require all endpoints to be trusted.

Learn more about the Trusted Endpoints feature, including policy configuration recommendations.
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 which 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 that is 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:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Applies to Access Devices</th>
<th>Applies to Authentication Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Endpoints</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Remembered Devices</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Browsers</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Plugins</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tampered Devices</td>
<td>No*</td>
<td>Yes</td>
</tr>
<tr>
<td>Screen Lock</td>
<td>No*</td>
<td>Yes</td>
</tr>
<tr>
<td>Full Disk Encryption</td>
<td>No*</td>
<td>Yes</td>
</tr>
<tr>
<td>Mobile Device Biometrics</td>
<td>No*</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*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. If this user attempts to access a Duo-protected internal wiki from this laptop, 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 operating system policy on the access device.
Enrollment & 2FA Enforcement Planning

There are three stages that make up a typical enrollment and enforcement strategy.

Stage 1: Targeting of Pilot Users on a Specific Application

The goal of this stage is 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.

![Apply a Policy](image)

**c.** The final policy should look similar to the following:
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. Device Management Portal
   - Using this method, any valid user ID/password can login 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.

2. **AD Sync** of usernames into Duo with the option to send enrollment emails
3. **Bulk Import**
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 then 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 or not 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: these settings can always be overridden 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:
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:

**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:

   ![Application Policy Diagram]

   - **Global Policy**
     - **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.

   - **Group Policy**
     - **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.

   - **Application Policy**
     - **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.

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.

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

```
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](image)

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

   ![Policy Interface]

   **Results:**
   - Fully enrolled users will 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 like similar to the following:
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.

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:
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 for 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.