Duo Policy Guide
Configuring Access via Duo’s Policy Engine

Released March 23, 2017
Revised May 2, 2017
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

User and Group Status
  Active Status
  Bypass Status
  Disabled Status
  Status Controls

Enrollment and 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 & Trusted Networks - Scenario 1
  Enrollment & Trusted Networks - Scenario 2
Overview

Why do I need this guide?
Duo’s policy engine is highly adaptable and designed to meet a diverse set of use-cases. The use of policies configured to reflect your specific needs will allow 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 what 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’s built-in and 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.
- Note: Duo MFA customers receive a subset of the Global Policy settings available in Duo Access and Duo Beyond.

Application Policies

- These policies apply to all users logging into the specific application.
- 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 overridden setting is crossed out in the Global Policy view. If there are no Custom Policies that apply to the application, then the Global Policy settings are shown.
- Note: Duo Access and Duo Beyond allow for policies to be shared between applications. Duo MFA only allows custom policies to be created on a per-application basis.

Group Policies

- Group Policies can be assigned to one or more Duo user groups.
- These policies will override both the Global and Application Policies.
- They can be assigned 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: This is only available in Duo Access and Duo Beyond.
Policies Illustration

Below is a simple illustration of how policies can be used (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 that 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:

![Diagram showing new user access being denied to unenrolled users.]

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:

![Diagram showing new users being prompted to complete Duo enrollment before accessing Salesforce.]

5 of 24
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:

**User Policy Settings**

- **User Location Policies** (i.e. policies that are enforced based on the geographical origin of the user’s device IP address) will 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 2FA.
- **The New User Policy** deals with enrollment options for usernames unknown to Duo or usernames without a 2FA device attached (i.e. partially enrolled, which is explained more below).
- **The Group Access Policy** deals with authentication behavior. **(Note:** In the MFA edition, the Group Access Policy can only be applied to an application policy, which will impact all users logging into the application.)
  - Changing the Group Access Policy setting from the default setting 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, i.e. there is no opportunity for self-enrollment.
    - Authentication to the application is blocked with the “deny” setting, 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 group access 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 for 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 a 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 usernames in this state.
  - The New User Policy does not apply for a user in this state.
    - If the New User Policy is set to “Allow access without 2FA”, users in this state will be prompted to enroll.
    - If the New User Policy is set to “Deny access”, users in this state will be denied access to the application until they enroll through another mechanism like an enrollment e-mail or through a Device Management Portal.
  - Users in this state do consume a license.
  - When the policy requires enrollment, if a user can’t enroll, a 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 Group Access Policy to handle these scenarios.
User and 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 the Bypass Status is enabled, Individual users or groups will bypass 2FA after successfully passing primary authentication.
- When the Bypass Status is disabled, individual users or groups will always fail 2FA, even if they are able to pass 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.
Enrollment and 2FA Enforcement Planning

There are 3 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 2 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 unenrolled users to pass through without two-factor authentication”.
   b. Set the Group Access Policy to “Allow users to pass through without two-factor authentication”.
3. Create another new policy (GP-Citrix-Pilot-Enforce).
   a. Set the New User Policy to “Prompt unenrolled users to enroll whenever possible”.
   b. Set the Group Access Policy to “No effect”.
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 e-mails and which can include a link to the DMP for enrollment. These e-mails can then originate from internal e-mail servers instead of Duo.

2. **AD Sync** of usernames into Duo with the option to send enrollment e-mails
3. **Bulk Import**
4. Create **Admin API** calls to **create users** and **send enrollment e-mails**
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 e-mail that originates from internal e-mail servers.

**Stage 3: Determine When to Enforce 2FA and 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 Group Access 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 Group Access Policy to “No Action”
   c. The final policy will look as follows:

<table>
<thead>
<tr>
<th>Group policies</th>
<th><strong>GP-Citrix-Pilot-Enforce</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This policy applies to 1 group: <em>Pilot-Group1</em>.</td>
<td></td>
</tr>
<tr>
<td>[User] New User Policy</td>
<td>Prompt unenrolled users to enroll whenever possible.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application policy</th>
<th><strong>AP-Citrix-Prod1</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This policy applies to all users accessing this application.</td>
<td></td>
</tr>
<tr>
<td>[User] New User Policy</td>
<td>Prompt unenrolled users to enroll whenever possible.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Global policy</th>
<th><strong>Global Policy</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This policy always applies to all applications.</td>
<td></td>
</tr>
<tr>
<td>[User] New User Policy</td>
<td>Deny access to unenrolled users.</td>
</tr>
</tbody>
</table>

**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 that 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):
   d. Set the New User Policy to “Deny Access”.
   e. Set the Group Access 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 Group Access Policy to “No Action”
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 Group Access Policy to “No effect.
   b. The policy will look as follows:

   ![Application Policy](attachment:application_policy.png)

   **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”.

---

13 of 24
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 “Prompt unenrolled users to enroll whenever possible”.
   b. Set the Group Access Policy to “Allow users to pass through without two-factor authentication”.
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 Group Access 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 unenrolled users to pass through without two-factor authentication”. This setting overrides the global policy.
   b. Set the Group Access Policy to “No effect”. This setting overrides the global policy.
   c. The effective policy should look like the following:

   ![Application Policy Diagram]

   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 2 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 unenrolled users to pass through without two-factor authentication”.
   b. Set the Group Access Policy to “Allow users to pass through without two-factor authentication”.
3. Create another new policy (*WebSDK-Enforce2FA*).
   a. Set the New User Policy to “Prompt unenrolled users to enroll whenever possible”.
   b. Set the Group Access Policy to “No effect”.
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:
### 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 Additional 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”.

   a. Set the New User Policy to “Deny access to unenrolled users”.
2. Your policy should look like the following:

   ![Policy Configuration]

   **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 Additional 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 2 policies: one Application Policy and one Group Policy.

1. Manually create or use AD Sync to bring in a group of users that you still want to prompt for enrollment when logging into the application (Straggler-Group).
2. Create and apply a new Application Policy (NewUser-Deny).
   a. Set the New User Policy to “Deny access to unenrolled users”.
   b. Set the Group Access Policy to “No effect”.
3. Create another new policy (Straggler-Enrollment).
   a. Set the New User Policy to “Prompt unenrolled users to enroll whenever possible”.
   b. Set the Group Access Policy to “No effect”.
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 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 & Trusted 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 “Prompt unenrolled users to enroll whenever possible”.
   b. Set the Group Access Policy to “No effect”.
   c. In the Trusted 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 Trusted 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 & Trusted 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 always want to require 2FA, regardless of where they log in from.

This setup requires 2 policies: one Application Policy and one Group Policy.

1. Manually create or use AD Sync to import a group of users that you still want to prompt for enrollment when logging into the application, regardless of location (ADSyncc-VPN-Adms).
2. Create and apply a new Application Policy (WebSDK-Application-Trusted-Network).
   a. Set the New User Policy to “Prompt unenrolled users to enroll whenever possible”.
   b. Set the Group Access Policy to “No effect”.
   c. In the Trusted 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 “Prompt unenrolled users to enroll whenever possible”.
   b. Set the Group Access Policy to “No effect”.
   c. Set the Trusted 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. The final policy should like similar to the following:

![Policy Configuration]

**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.