SimpleRisk Custom Authentication Extra Installation and Administration Guide

Introduction

While the SimpleRisk Core product is free and open source in order to make risk management attainable for the masses, we have developed a series of "Extras" which provide additional "Enterprise" level functionality for your SimpleRisk installation. By purchasing these Extras, you add functionality to your installation, while at the same time providing financial support to see that the SimpleRisk Core product remains in active development for the long haul. It's a win-win!

License

The SimpleRisk Extras are offered on a per-installation basis and include support and updates for a full year from the date of purchase.

The Basics

Getting a SimpleRisk Extra up and running is designed to be as easy as possible. There are three basic steps:

1. **Installation** – This is the simple process of obtaining the Extra and placing the files in the proper directory.
2. **Activation** – This is the simple process of telling SimpleRisk that the Extra is ready to be used.
3. **Configuration** – This is the simple process of configuring any settings that change how the extra functions.

Custom Authentication Extra

By default, SimpleRisk uses locally defined user accounts to authenticate with the system. This extra provides support for users to authenticate with SimpleRisk using an LDAP or Active Directory repository. It also includes functionality for adding multi-factor authentication to your SimpleRisk installation using Duo Security. The plan is to eventually expand this Extra to include functionality for other multi-factor authentication vendors as well. If you have a specific one that you would like to use, please contact us at support@simplerisk.it.

Installation

All SimpleRisk Extras are delivered through the SimpleRisk services functionality. This is enabled automatically once you register your SimpleRisk instance. To register your SimpleRisk instance, go to Configure Register & Upgrade. Enter your organization's information and save it. This should generate

a unique instance id for your SimpleRisk instance and communicate with our servers to create a services API key. Once registered, SimpleRisk will download and install the Upgrade Extra for you. This provides buttons for upgrading and backing up the application as well as the Extra installation functionality. If you have issues, ensure that your "simplerisk" directory is writeable by the user the web server runs as (typically "www-data"). If your system is behind a dynamic NAT pool, you may need to contact support to remove the IP restriction for your instance. Once your payment has been received, your downloads will be enabled and will show up in the Configure ⍰ Register & Upgrade menu. You can simply click the button to download the Extra.

Activation

This next step is what tells SimpleRisk that the Email Notification Extra is installed and ready to use. Log in to your SimpleRisk instance and select "Configure" from the Navigation Menu at the top. Then, select "Extras" from the Configuration Menu at the left. You will see a list here of each of the Extras that are available for purchase. Find the row for the "Custom Authentication" Extra and click where it says "No" in the Enabled column. Click on the "Activate" button. Once activated, you should see the word "ACTIVATED" under the Extra name in green and the Extra configuration parameters will appear below.

Configuration

The Custom Authentication Extra has numerous configuration options that are available by selecting "Configure" from the Navigation Menu at the top. Then, select "Extras" from the Configuration Menu at the left. You will see a list here of each of the Extras that are available for purchase. Find the row for the "Custom Authentication" Extra and click where it says "Yes" in the Enabled column. Configurations are ordered here by "LDAP", "Duo Security", and "Toopher":

LDAP

This section contains the configurations necessary in order to authenticate users in SimpleRisk by LDAP instead of SimpleRisk's internal passwords. Once activated, you will have a new "LDAP" user type when adding a new user in "User Management". The specified username must match the LDAP username for the user.

- **BIND FIRST:** When checked, this tells the Custom Authentication Extra that you will need to use a special service account to bind to the LDAP server first in order to search for the full path to the user who is logging in. After checking, you will have the option to provide the BIND ACCOUNT and BIND ACCOUNT PASS.
- **BIND ACCOUNT:** This parameter specifies the full path to the service account that you would like to use to bind to LDAP.
- **BIND ACCOUNT PASS:** This parameter specifies the password to use with the BIND ACCOUNT to bind the LDAP.
- **TLS:** When checked, this tells PHP to use the ldap_start_tls function for the connection. This should be set to false unless you are trying to upgrade the security of a plain LDAP connection to

an encrypted channel. This is not the same as using ldaps:// on port 636 and the two methods should not be used together.

- **SASL:** When checked, this tells PHP to use the ldap_sasl_bind function which uses SASL to bind to the LDAP server. When unchecked, this tells PHP to use the regular ldap_bind function to bind to the LDAP server.
- **CHASE_REFERRALS:** This parameter specifies whether referrals should be followed by PHP when connecting to the LDAP server. As long as you are specifying the direct path to the User DN, you can leave this unchecked. If you need it to chase referrals, then go ahead and check it.
- **LDAP_VERSION:** This parameter specifies the LDAP protocol to be used by PHP when connecting to the LDAP server. PHP uses LDAP version 2 by default, but LDAP version 3 is preferable as long as your LDAP server supports it.
- **LDAPHOST:** This parameter specifies the LDAP server that you would like SimpleRisk to use to try to authenticate a user with. You can specify a server name without the protocol (i.e. "ldap.mydomain.com") or with the protocol included (i.e. "ldaps://ldap.mydomain.com").
- **LDAPPORT:** This parameter specifies the port that the LDAP server is running on. Typically this would be set to "389" for LDAP or "686" for LDAPS.
- **USERDN:** This parameter specifies the full path to where the users exist within your LDAP repository.

SAML

This section contains the configurations necessary in order to authenticate users in SimpleRisk by SAML/Shibboleth instead of SimpleRisk's internal passwords. Once activated, you will have a new "SAML" user type when adding a new user in "User Management".

If you would like to setup via a SAML metadata XML export from SimpleRisk to import into you IDP you can do so by going to the Configure menu at the top of SimpleRisk, then hit Extras on the left side, and finally click the "Yes/No" next to Custom Authentication.

Now click the SAML tab and enter the trusted domain value or the IDP's domain and save the value at the bottom of the page. Now you should be able to click the "Download SAML 2.0 Metadata" link near the top of the page. If you wish to manually configure the IDP please refer to the information below.

On your SAML identity provider (IdP), you will need to configure the following parameters:

- **Single Sign On URL:**
  https://your_simplerisk_domain/vendor/simplesamlphp/simplesamlphp/www/module.php/saml/sp/saml2-acs.php/default-sp
- **Recipient URL:**
  https://your_simplerisk_domain/vendor/simplesamlphp/simplesamlphp/www/module.php/saml/sp/saml2-acs.php/default-sp
- **Destination URL:**
  https://your_simplerisk_domain/vendor/simplesamlphp/simplesamlphp/www/module.php/saml/sp/saml2-acs.php/default-sp

- **Audience URI (SP Entity ID):** https://your_simplerisk_domain/vendor/simplesamlphp/simplesamlphp/www/module.php/saml/sp/metadata.php/default-sp
- **Default Relay State:** https://your_simplerisk_domain/extras/authentication/login.php

To finish the configuration of SimpleRisk for the Custom Authentication Extra, you will need to configure the following parameters if you have not already:

- **TRUSTED DOMAINS:** This a comma-separated list of domains that SimpleRisk will be allowed to authenticate with via SAML. Typically, this is just the domain name of your SAML identity provider (IdP).
- **METADATA URL:** This is the URL provided by your IdP containing the metadata for your SAML provider. If a metadata url is not available, you can paste the metadata directly into the metadata xml field instead. The major benefit to using a URL over the XML is that it will be dynamically updated if the configuration is changed.
- **METADATA XML:** This is the metadata provided by your IdP for your SAML provider. You may also select "Choose File" in order to upload a file containing the metadata. You do not need to provide this if you have provided a working metadata url.
- **USERNAME MATCH:** SimpleRisk can authenticate a user via two different methods. If you select the "Authenticated Username" method, SimpleRisk will compare the username authenticated at the IdP to the usernames configured in SimpleRisk. If you select the "Authenticated Attribute" method, SimpleRisk will compare the value of the attribute in the "Username Attribute" parameter to the usernames configured in SimpleRisk. This allows you to have a different username in SimpleRisk than in your SAML provider, but still authenticate properly. Most configurations will use the "Authenticated Username" method of authentication.
  Azure AD Users: You may need to use the following as your Username attribute "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress". This scheme may also apply to your other assertions as well.
- **USRNAME ATTRIBUTE:** This parameter is used only when the "Authenticated Attribute" method is selected for the "Username Match" parameter. It is used to specify the name of the attribute provided by the IdP that you will use to compare against the SimpleRisk usernames.

**** NOTE:** For those looking to integrate SimpleRisk with ADFS as the SAML provider, the ADFS IdP will not accept the NameID parameter provided by SimpleRisk by default because it is provided in transient format (urn:oasis:names:tc:SAML:2.0:nameid-format:transient). You will need to work with your AD team to create a custom rule to do a translation to transient NameIDs for the SimpleRisk application. The following document from Cisco nicely outlines how to do this (see step 11):

https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/118771-configure-samlsso-00.html

Duo Security

This section contains the configurations necessary in order to activate Duo Security's multi-factor authentication for SimpleRisk users. When adding new users or updating existing users, change the multi-factor authentication selector to "Duo Security" in order to take advantage of multi-factor authentication for that user.

- **IKEY:** This parameter specifies the Duo Security integration key that is passed to sign a request.
- **SKEY:** This parameter specifies the Duo Security secret key that is passed to sign a request.
- **HOST:** This parameter specifies the Duo Security host that is used to pass requests to for multi-factor authentication.

Toopher

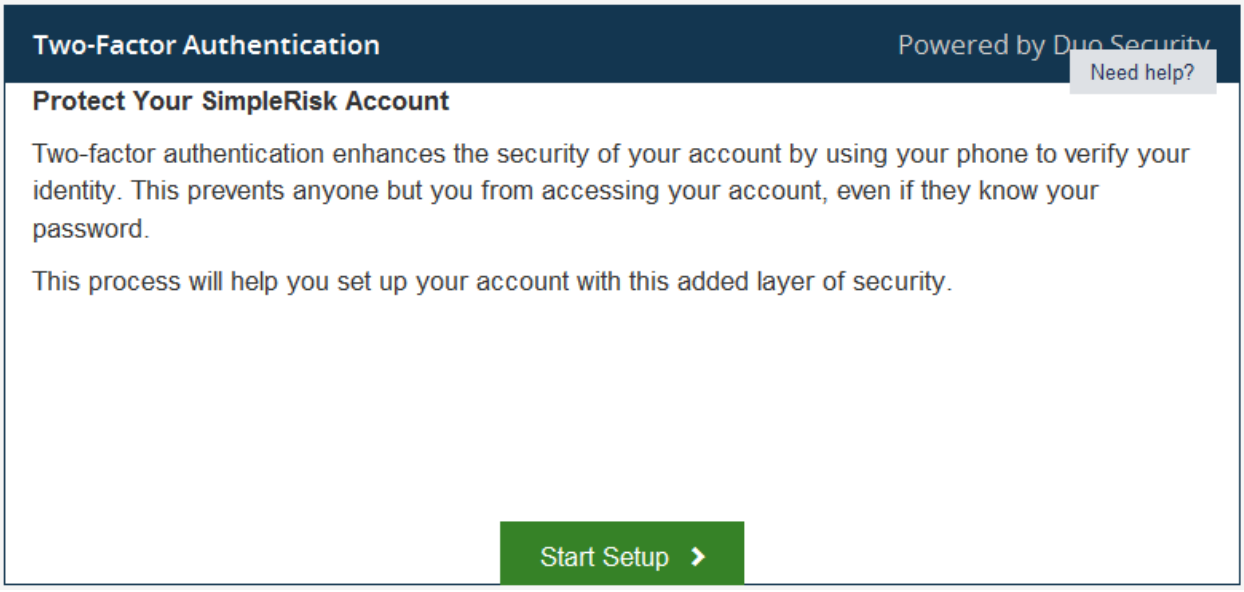
Toopher authentication is not yet implemented in the SimpleRisk Custom Authentication Extra, but if you need it, please send an e-mail to extras@simplerisk.it and we will do our best to prioritize it.

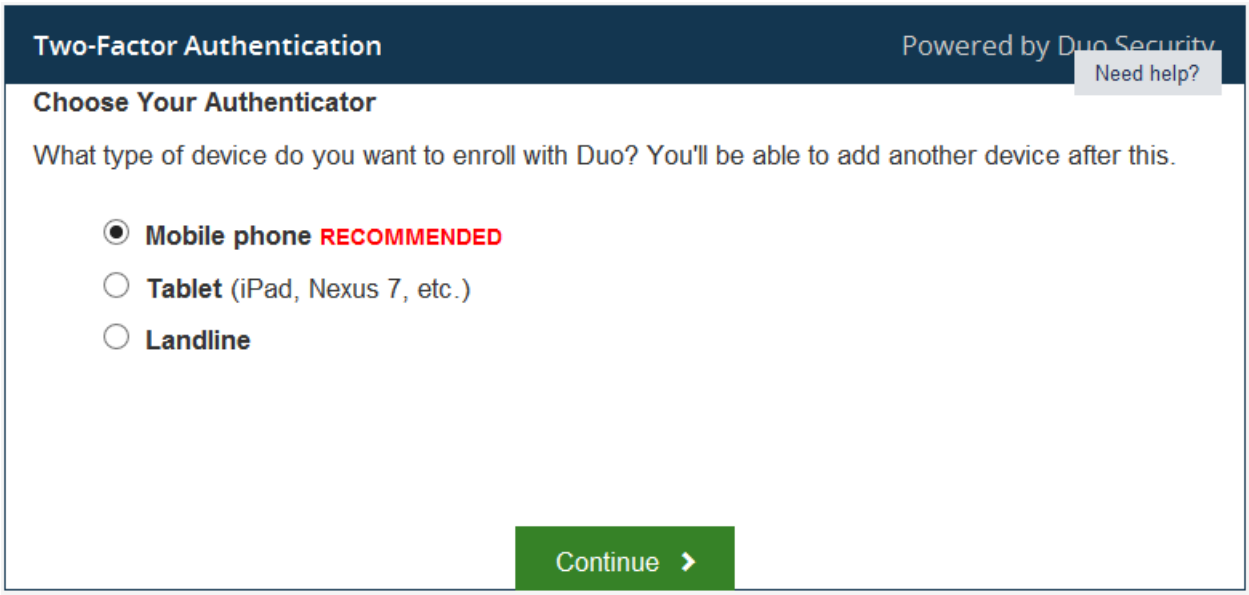
- **CONSUMER KEY:** N/A
- **CONSUMER SECRET:** N/A

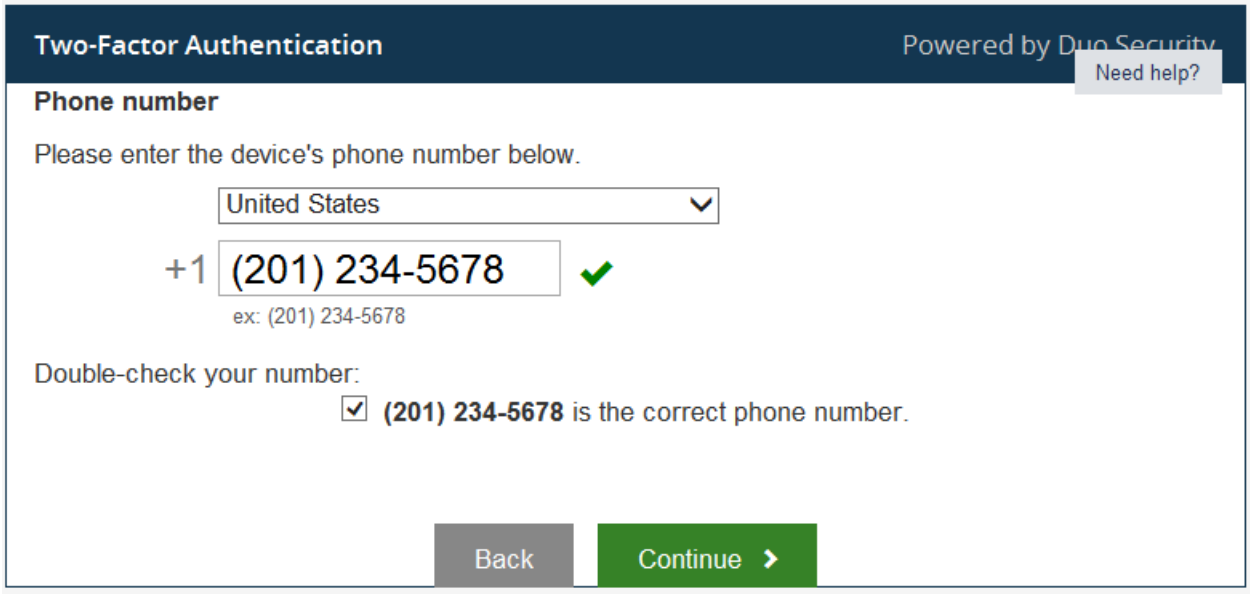
Features

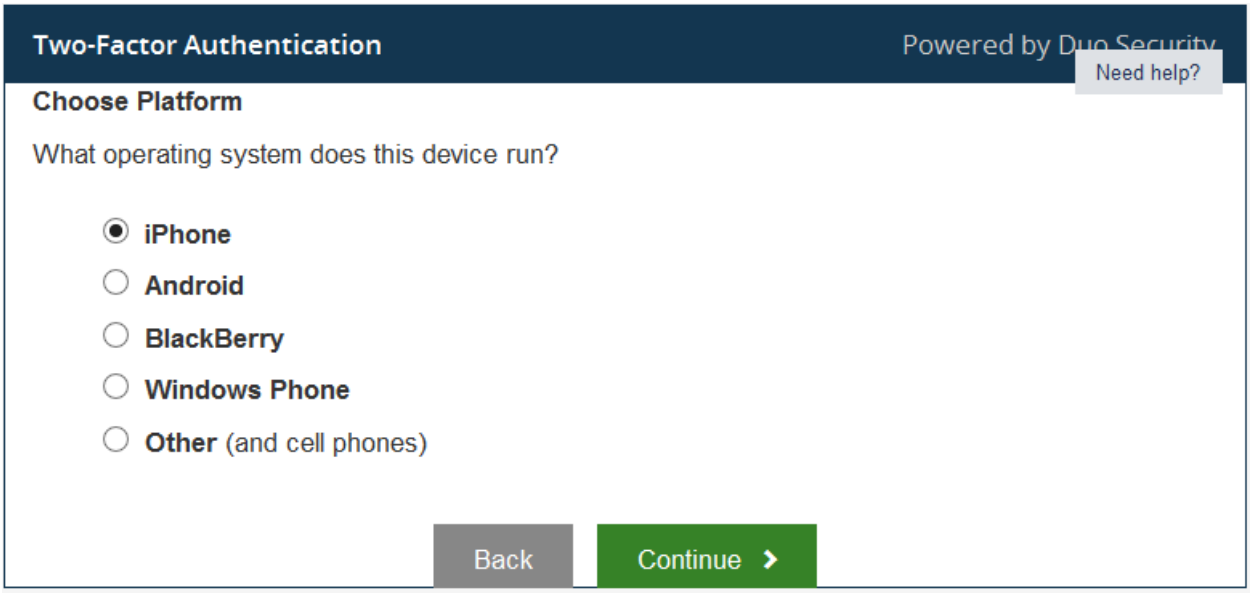
The changes from enabling this Extra are rather subtle in terms of the SimpleRisk user interface. First off, under the "Configure" menu select "User Management" and you will see a new "LDAP" type when adding a new user. The rest of the user setup is identical to adding a local user with the exception of not having to specify a password. Any users added with the "LDAP" type will attempt to bind to LDAP using the specified username and password entered at login. Local users and LDAP users can live side-by-side in SimpleRisk with no issues and we highly recommend that you keep around the local "admin" account as a backdoor just in case something happens with authenticating with LDAP.

The other subtle change that you will see is at the very bottom of the "Add a New User" section where there is a new "Duo Security" option for Multi-Factor Authentication. This can be enabled for any user in the system, but uses your businesses Duo Security account information so you will need to sign up with them first, and follow the configuration instructions above, before using it. Once set, the next time the configured user logs into the system, they will be presented with a series of steps to set up their multi-factor device:


Two-Factor Authentication
Powered by Duo Security
Need help?
Protect Your SimpleRisk Account
Two-factor authentication enhances the security of your account by using your phone to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.
This process will help you set up your account with this added layer of security.
Start Setup

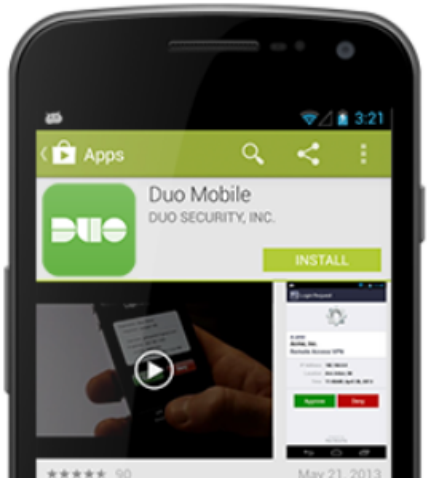

Two-Factor Authentication
Powered by Duo Security
Need help?
Choose Your Authenticator
What type of device do you want to enroll with Duo? You'll be able to add another device after this.
Mobile phone RECOMMENDED
Tablet (iPad, Nexus 7, etc.)
Landline
Continue


Two-Factor Authentication
Powered by Duo Security
Need help?
Phone number
Please enter the device's phone number below.
United States
+1
(201) 234-5678
ex: (201) 234-5678
Double-check your number:
(201) 234-5678 is the correct phone number.
Back
Continue


Two-Factor Authentication
Powered by Duo Security
Need help?
Choose Platform
What operating system does this device run?
iPhone
Android
BlackBerry
Windows Phone
Other (and cell phones)
Back
Continue

Two-Factor Authentication Powered by Duo Security

Need help?



Install Duo Mobile for Android

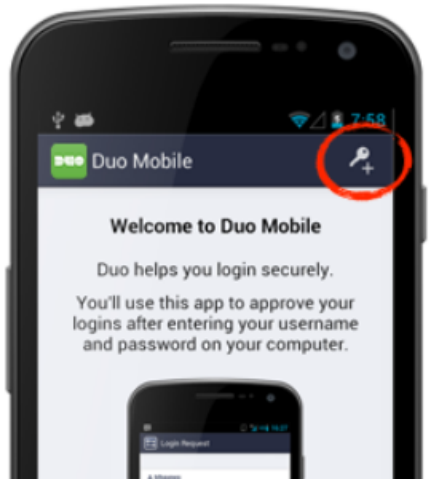
1. Launch the Google Play Store app and search for "Duo Mobile".
2. Tap "Install" to install the app.

☑ I have Duo Mobile installed

Back Continue ›

Two-Factor Authentication Powered by Duo Security

Need help?

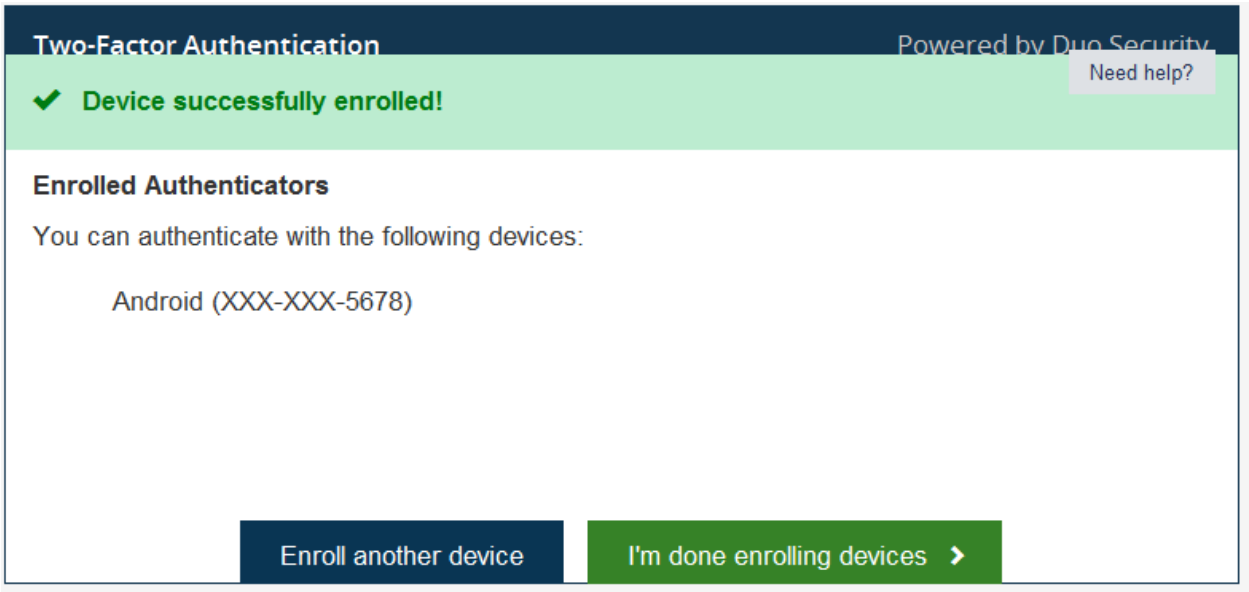


Activate Duo Mobile for Android

1. Open Duo Mobile.
2. Tap the "+" button. Then tap "Scan Barcode".
3. Scan this barcode.

Can't scan this barcode? Click here

Back Continue ›



You can disable the Duo Security multi-factor authentication at any time by setting the user back to “None”.