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 are good in perpetuity. You pay once and never have to worry about re-upping your license ever again. See if any of those other risk management vendors will give you that kind of a deal. With each Extra we also include one year of complimentary upgrades and e-mail support.

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. **Configuration** – Some of our Extras have settings that can change how the extra functions.
3. **Activation** – By hitting the proper URL you will tell SimpleRisk that the Extra is ready to be used.

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

Once your payment has been received, you will be provided with a tarball containing the Custom Authentication Extra code via e-mail. Transfer that file on to the server where SimpleRisk has been

installed and place it inside the SimpleRisk root directory (i.e. where you find the index.php file). Then run the following command:

tar xvzf custom_authentication_extra.tgz

This will create a new "extras" directory if it didn't already exist and place an "authentication" directory inside it that contains the code. The Extra is now installed.

Configuration

You will see a special config.php file for the Custom Authentication Extra under the following path:

/your/path/to/simplerisk/extras/authentication/includes/config.php

Open that file in your favorite text editor and you will see the parameters that are currently configurable. The following is a list of the current parameters along with a brief description of what each does.

- **TLS:** Set this parameter to either "true" or "false". When set to "true", 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.
- **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.
- **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 as "0". If you need it to chase referrals, then set it to "1" instead.
- **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.
- **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.

Once you have properly set each of these parameters, then your last step is to activate the Custom Authentication Extra.

Activation

This last step is what tells SimpleRisk that the Custom Authentication Extra is installed and ready to use. It also generates the unique application key that Duo Security will use if you enable it for mutli-factor authentication. Use your favorite web browser and go to the following URL:

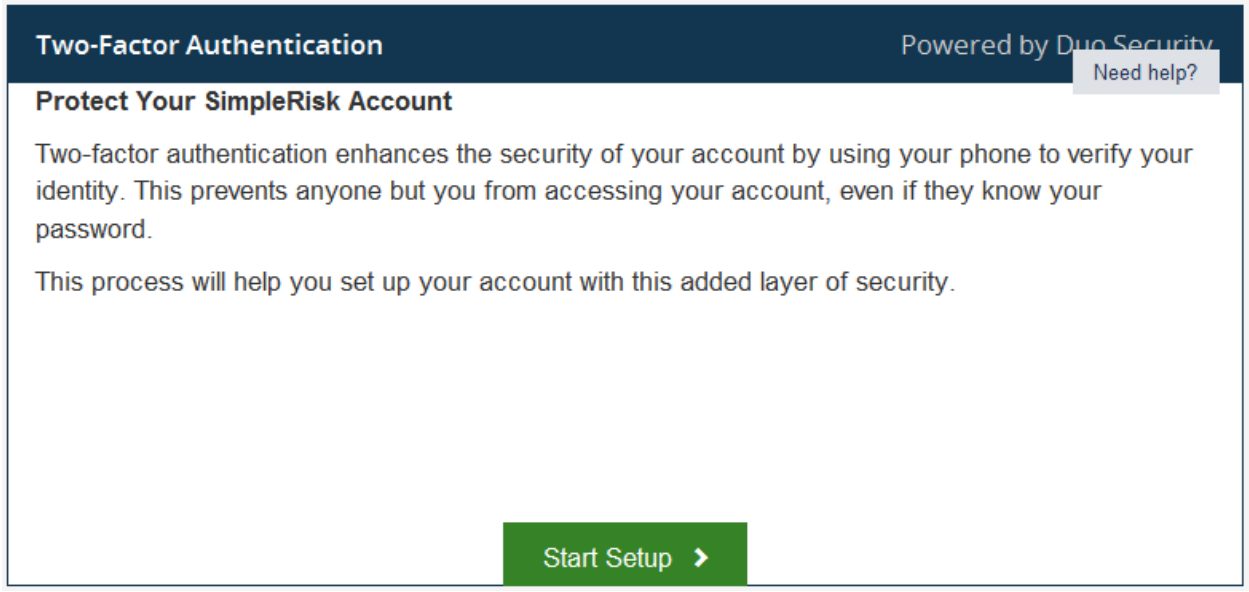
http://your_simplerisk_host/extras/authentication

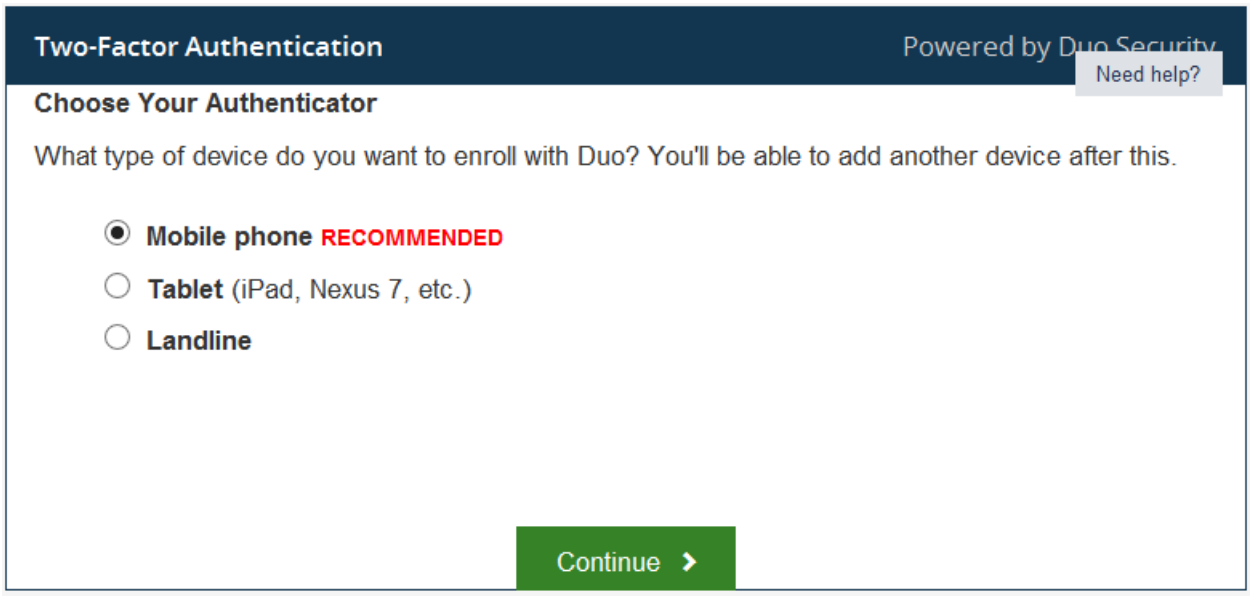
If you have HTTPS installed, then use https:// instead of http://. The "your_simplerisk_host" should be substituted for whatever the host name is for the system SimpleRisk is installed on. If you've installed SimpleRisk in some location other than the web root, you will want to specify that as well. If it works, you should just see a blank page with no error messages.

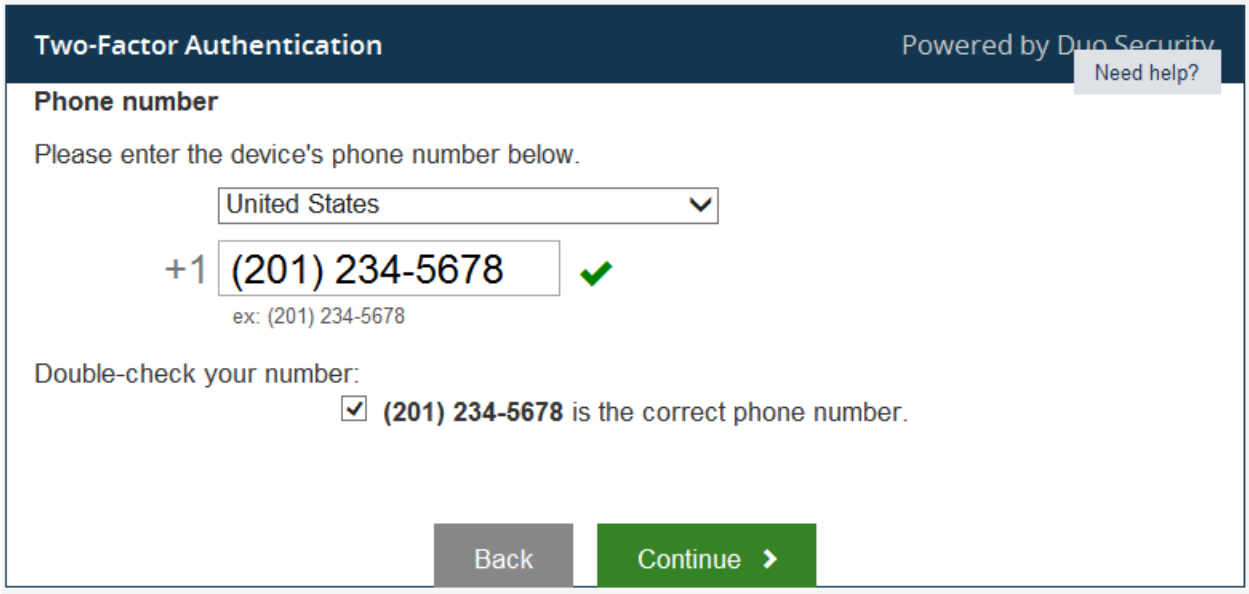
Features

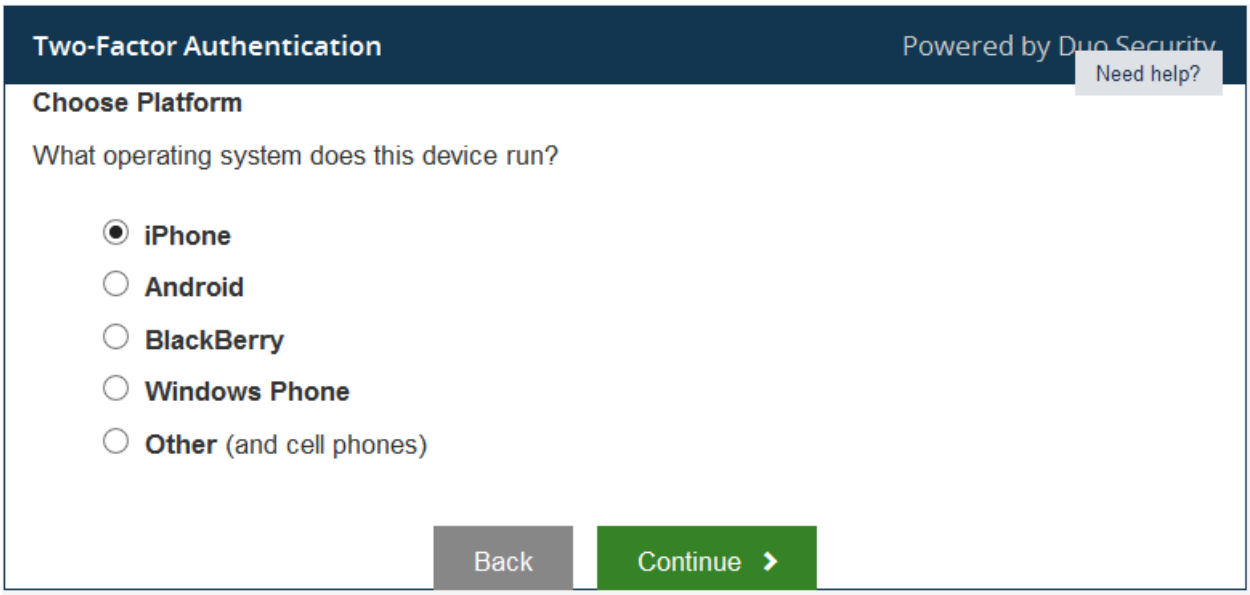
The changes from enabling this Extra are rather subtle in terms of the SimpleRisk user interface. First off, under the "Configure" menu select "User Management" and you will see a new "LDAP" type when adding a new user. The rest of the user setup is identical to adding a local user with the exception 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

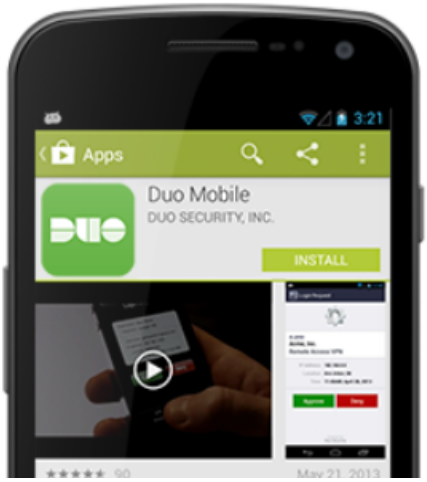

Two-Factor Authentication
Powered by Duo Security
Need help?
Choose Your Authenticator
What type of device do you want to enroll with Duo? You'll be able to add another device after this.
Mobile phone RECOMMENDED
Tablet (iPad, Nexus 7, etc.)
Landline
Continue


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

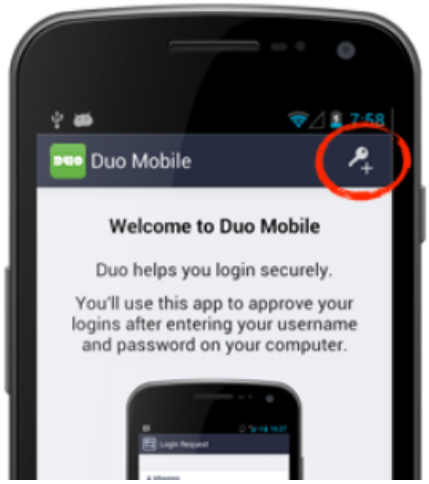
1. Launch the Google Play Store app and search for "Duo Mobile".
2. Tap "Install" to install the app.

☑ I have Duo Mobile installed

Back Continue ›

Two-Factor Authentication Powered by Duo Security

Need help?

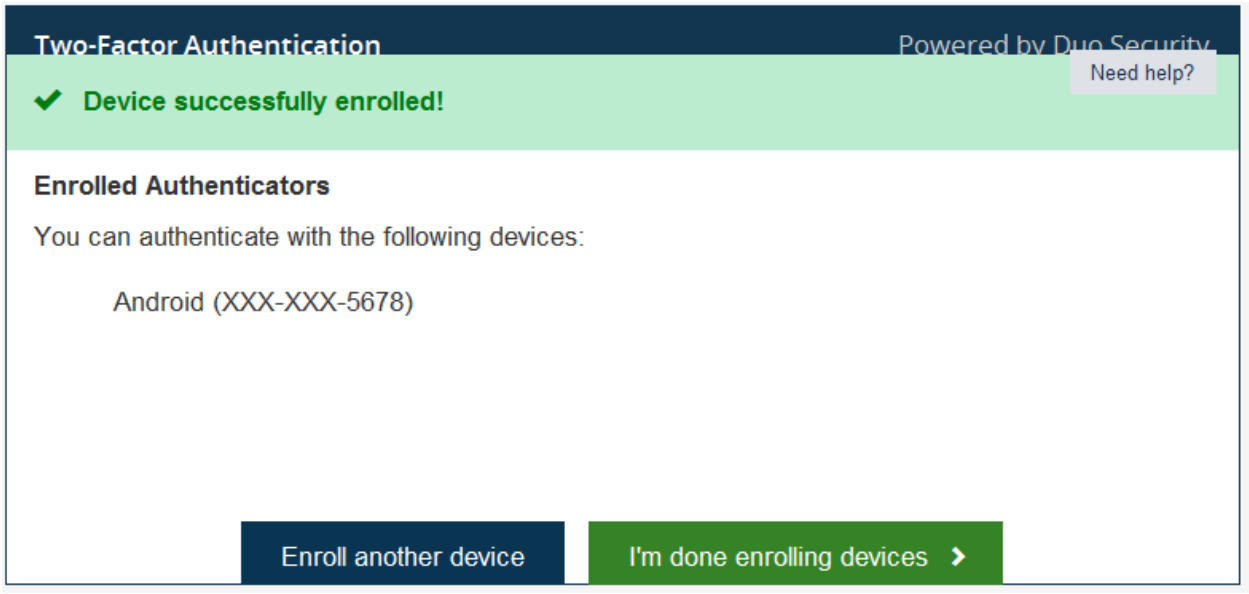


Activate Duo Mobile for Android

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”.