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. Ongoing support and updates for the SimpleRisk Extras is 20% of the original cost per year.

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

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.

You may also need to install the LDAP module for PHP in order for everything to work properly. On a debian system, you would do this with the following command:

>   *sudo apt-get install php5-ldap*

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.

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

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

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

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

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 ❯

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