

SimpleRisk Team Separation 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.

Team Separation Extra

By default, all SimpleRisk users are able to see all risks entered into the system. This extra enables functionality creating virtual walls so that risks assigned to a team are only viewable by members of that team.

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

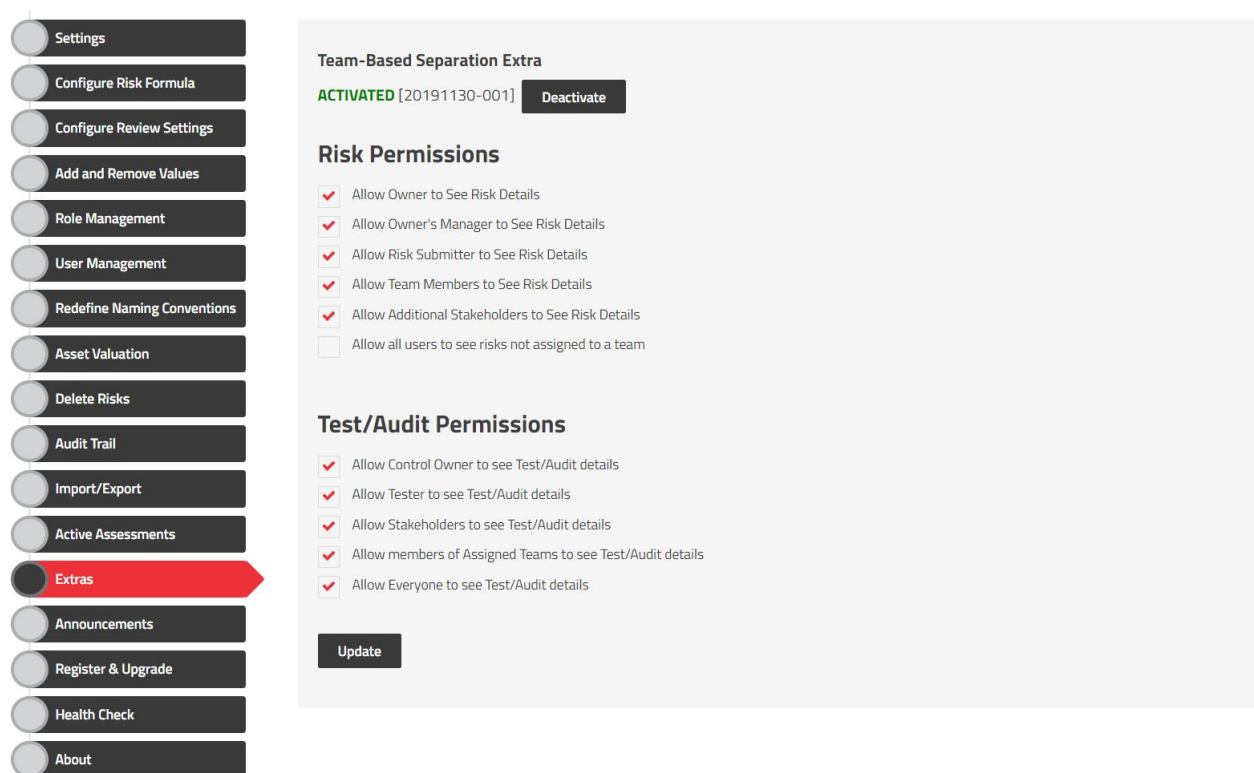
functionality. If you have issues, ensure that your “simplerisk” directory is writeable by the user the web server runs as (typically “www-data”). If your system is behind a dynamic NAT pool, you may need to contact support to remove the IP restriction for your instance. Once your payment has been received, 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 Team Separation 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 “Team-Based Separation” 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.

Configuration

There are a few ways we can edit how the Team-Based Separation works . A screenshot of the configuration page found by using “Configure” at the top followed by “Extras” on the left and finally clicking the button (yes/no) in the same row as Team-Based Separation is shown below.



The screenshot shows the SimpleRisk configuration interface. On the left is a vertical navigation menu with 18 items: Settings, Configure Risk Formula, Configure Review Settings, Add and Remove Values, Role Management, User Management, Redefine Naming Conventions, Asset Valuation, Delete Risks, Audit Trail, Import/Export, Active Assessments, Extras (highlighted in red), Announcements, Register & Upgrade, Health Check, and About. The main content area is titled "Team-Based Separation Extra" and shows the status "ACTIVATED [20191130-001]" with a "Deactivate" button. Below this are two sections: "Risk Permissions" and "Test/Audit Permissions".

Team-Based Separation Extra
ACTIVATED [20191130-001] Deactivate

Risk Permissions

- ☒ Allow Owner to See Risk Details
- ☒ Allow Owner's Manager to See Risk Details
- ☒ Allow Risk Submitter to See Risk Details
- ☒ Allow Team Members to See Risk Details
- ☒ Allow Additional Stakeholders to See Risk Details
- ☐ Allow all users to see risks not assigned to a team

Test/Audit Permissions

- ☒ Allow Control Owner to see Test/Audit details
- ☒ Allow Tester to see Test/Audit details
- ☒ Allow Stakeholders to see Test/Audit details
- ☒ Allow members of Assigned Teams to see Test/Audit details
- ☒ Allow Everyone to see Test/Audit details

Update

Each of these permissions are set on the basis that as long as you satisfy one condition then you will be able to view said risks. Permission to see overrides anything that would otherwise make it seem as though you couldn't view a particular risk or test. Just as an example a user who does not belong to the team a risk is assigned to can still see that risk with the currently pictured permissions as long as they submitted that risk or are named as the Owner, Owner's Manager, and/or Additional Stakeholder. Any one of those will work and you do not need to satisfy them all to gain access to the risk.

Features

You should notice no difference in SimpleRisk's user interface when this Extra is enabled other than seeing it marked as "Enabled" when selecting "Configure" from the menu at the top, followed by "Extras" in the menu at the left. However, once enabled, all risks with a "Team" assigned to them will only be viewable by users who are members of that team.

To check the "Team" that a risk belongs to, select the risk ID of the risk that you would like to view from any report view. Look under the "Details" section for an entry named "Team". A risk can only be assigned to a single team.

To check the teams that a user has access to, select "Configure" from the top navigation menu followed by "User Management" from the left-side menu. Scroll down to the "View Details for User" section. Select the user that you would like to check on and click the "Select" button. You will see a "Team(s)" configuration for the user where any currently enabled teams will be highlighted. If a highlighted team name matches with the team assigned to a risk, then the user should have access. If a team is not highlighted, you can configure a user to be a member of multiple teams via this configuration and select "Update" when you are ready to save your configuration.