SimpleRisk API 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.

API Extra

By default, SimpleRisk will utilize the API for application functionality, but uses cookie-based authentication. This extra enables the ability to create, rotate, and invalidate API keys that can be used to automate interactions with the SimpleRisk API.

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 API 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 "API" 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

The API Extra can use two different forms of authentication. By default, it uses cookie-based authentication. When you are logged into the SimpleRisk instance, you can make API requests using cookie-based authentication, but it would be difficult to automate requests using cookies so we include key-based authentication as well.

Key-based authentication is enabled on a per-user basis. To get a user key, log in to your SimpleRisk instance, select your name at the top right, and select "My Profile" from the dropdown menu. If the API Extra has been enabled, you should see an option to "Generate API Key". When clicked, this will give you an API key that you can use to interact in an automated fashion with SimpleRisk as though you were that user. It will be a long (100 character) random (upper case, lower case, and digits) string. Write it down because your only options later will be to "Rotate API Key", which will cancel the current key and generate a new one, or "Invalidate API Key", which will simply cancel the current key.

Features

If you log into your SimpleRisk instance, you can see the list of API calls that are available by going to https://path_to_simplerisk/api. Here are some examples of GET calls that you can make to the SimpleRisk API:

Print the version of the API (JSON result)

GET https://path_to_simplerisk/api/version?key=your_simplerisk_api_key

Print the user associated with an API key (JSON result)

GET https://path_to_simplerisk/api/whoami?key=your_simplerisk_api_key

Print the information associated with a risk (JSON result)

GET https://path_to_simplerisk/api/management/risk/view?id=risk_id&key=your_simplerisk_api_key

Print the information associated with a risk mitigation (JSON result)

GET https://path_to_simplerisk/api/management/mitigation/view?id=risk_id&key=your_simplerisk_api_key

*** This doesn't seem to work currently ***

Print the information associated with a risk review (JSON result)

GET https://path_to_simplerisk/api/management/review/view?id=risk_id&key=your_simplerisk_api_key

*** This doesn't seem to work currently ***

Print a list of all users and their information (JSON result)

GET https://path_to_simplerisk/api/admin/users/all?key=your_simplerisk_api_key

Print a list of enabled users and their information (JSON result)

GET https://path_to_simplerisk/api/admin/users/enabled?key=your_simplerisk_api_key

Print a list of disabled users and their information (JSON result)

GET https://path_to_simplerisk/api/admin/users/disabled?key=your_simplerisk_api_key

Print the results from the Dynamic Risk Report (JSON result)

GET https://path_to_simplerisk/api/reports/dynamic?status=[0-2]&group=[0-14]&sort=[0-2]&key=your_simplerisk_api_key

Status: 0 = Open Risks; 1 = Closed Risks; 2 = All Risks

Group: 0 = None; 1 = Risk Level; 2 = Status; 3 = Site/Location; 4 = Risk Source; 5 = Category; 6 = Team; 7 = Technology; 8 = Owner; 9 = Owner's Manager; 10 = Risk Scoring Method; 11 = Control Regulation; 12 = Project ; 13 = Next Step; 14 = Month Submitted

Sort: 0 = Calculated Risk; 1 = ID; 2 = Subject

Here are some examples of POST requests that you can make to the SimpleRisk API:

Add a New Risk

URL: https://path_to_simplerisk/api/management/risk/add?key=your_simplerisk_api_key

Method: POST

Request params:

```
{
    "subject": "Subject",
    "category": "1",
    "location": "6",
    "reference_id": "",
    "regulation": "3",
```

"control_number": "",

"assets": "credit card data, google-public-dns-a.google.com, ",

"technology": "8",

"team": "3",

"owner": "16",

"manager": "15",

"source": "4",

"scoring_method": "1",

"likelihood": "2",

"impact": "2",

"AccessVector": "N",

"AccessComplexity": "L",

"Authentication": "N",

"ConfImpact": "C",

"IntegImpact": "C",

"AvailImpact": "C",

"Exploitability": "ND",

"RemediationLevel": "ND",

"ReportConfidence": "ND",

"CollateralDamagePotential": "ND",

"TargetDistribution": "ND",

"ConfidentialityRequirement": "ND",

"IntegrityRequirement": "ND",

"AvailabilityRequirement": "ND",

"DREADDamage": "10",

"DREADReproducibility": "10",

"DREADExploitability": "10",

"DREADAffectedUsers": "10",

"DREADDiscoverability": "10",

"OWASPSkillLevel": "10",

"OWASPMotive": "10",

"OWASPOpportunity": "10",

"OWASPSize": "10",

"OWASPEaseOfDiscovery": "10",

"OWASPEaseOfExploit": "10",

"OWASPAwareness": "10",

"OWASPIntrusionDetection": "10",

"OWASPLossOfConfidentiality": "10",

"OWASPLossOfIntegrity": "10",

"OWASPLossOfAvailability": "10",

"OWASPLossOfAccountability": "10",

"OWASPFinancialDamage": "10",

"OWASPReputationDamage": "10",

"OWASPNonCompliance": "10",

"OWASPPrivacyViolation": "10",

"Custom": "",

"assessment": "Assessment",

"notes": "Additional notes"

}

Response:

{

  "status": 200,

  "status_message": "Risk ID 3143 submitted successfully!",

  "data": {

    "risk_id": 3143

  }

}

Add a New Mitigation

URL: https://path_to_simplerisk/api/management/mitigation/add?key=your_simplerisk_api_key

Method: POST

Request params:

{

```
    "id": 2280,

    "planning_date": "03/02/2017",

    "tab_type": "1",

    "planning_strategy": "2",

    "mitigation_effort": "2",

    "mitigation_cost": "2",

    "mitigation_owner": "17",

    "mitigation_team": "2",

    "current_solution": "Current solution",

    "security_requirements": "Requirements",

    "security_recommendations": "Recommends"

}
```

Response:

```
{

    "status": 200,

    "status_message": "Success",

    "data": {

        "risk_id": "2280",

        "mitigation_id": "916"

    }

}
```

Add a New Management Review

URL: https://path_to_simplerisk/api/management/review/add?key=your_simplerisk_api_key

Method: POST

Request params:

```
{

    "id": "2280",

    "review": "1",

    "next_step": "1",

    "comments": "This is a comment",

    "custom_date": "no",
```

```
    "next_review": "06/11/2017"

}

Response:

{

  "status": 200,

  "status_message": "Success",

  "data": {

    "risk_id": "2280",

    "mitigation_id": "916"

  }

}
```