Hewlett Packard
Enterprise

HPE Security Fortify Runtime Application Protection

Software Version: 17.3

Operator Guide

Document Release Date: April 2017
Software Release Date: April 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The software is restricted to use solely for the purpose of scanning software for security vulnerabilities that is (i) owned by you; (ii) for which you have a valid license to use; or (iii) with the explicit consent of the owner of the software to be scanned, and may not be used for any other purpose.

You shall not install or use the software on any third party or shared (hosted) server without explicit consent from the third party.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Contents

Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products: http://www.hpe.com/software/fortify

About the Documentation Set

The HPE Security Fortify Software documentation set contains installation, user, and deployment guides for all HPE Security Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following HPE Security user community website:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will need to register for an account.

Change Log

The following table lists changes made to this document. Revisions to this document are published only if the changes made affect product functionality.

Software Release / Document Version	Change
17.3	Updated: Minor update for 17.3 release; no significant change to content.
16.8	Updated: Minor update for 16.8 release; no significant content changes.
16.3	Updated: Minor update for 16.3 release; no significant content changes. HP to HPE rebranding.

Chapter 1: Introduction

This guide contains information and procedures that enable you to run and monitor the operation of HPE Security Fortify Runtime Application Protection (RTAP).

Intended Audience

This guide is intended for use by enterprise security leads, development team managers, or someone who is responsible for ongoing maintenance of a Runtime system. Runtime Application Protection protects programs running under a supported Java Virtual Machine (JVM) or .NET CLR. The program can be a web application container or any other Java or .NET CLR program.

Related Documents

This topic describes documents that provide information about HPE Security Fortify Runtime Application Protection.

Note: The Protect724 site location is https://www.protect724.hpe.com/community/fortify/fortify-product-documentation.

All Products

The following documents provide general information for all products.

Document / File Name	Description	Location
HPE Security Fortify Software System Requirements HPE_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of HPE Security Fortify Software.	Included with product download and on the Protect724 site
HPE Security Fortify Software Release Notes HPE_FortifySW_RN_<*version*>.txt	This document provides an overview of the changes made to HPE Security Fortify Software for this release and important information not included elsewhere in the product documentation.	Included on the Protect724 site

Document / File Name	Description	Location
What's New in HPE Security Fortify Software <version> HPE_Whats_New_<*version*>.pdf	This document describes the new features in HPE Security Fortify Software products.	Included on the Protect724 site
HPE Security Fortify Open Source and Third-Party License Agreements HPE_OpenSrc_<*version*>.pdf	This document provides open source and third-party software license agreements for software components used in HPE Security Fortify Software.	Included with product download and on the Protect724 site
HPE Security Fortify Glossary HPE_Glossary.pdf	This document provides definitions for HPE Security Fortify Software terms.	Included with product download and on the Protect724 site

HPE Security Fortify Runtime

The following documents provide information about Fortify Runtime.

Document / File Name	Description	Location
HPE Security Fortify Runtime .NET Edition Designer Guide HPE_RT_DotNet_Design_Guide_<*version*>.pdf PDF only; no help file	This document provides information to aid in the configuration and customization of Fortify Runtime for a given application that operates on a .NET platform. The audience for this guide includes an HPE Security Fortify Runtime Solution Designer who often creates event handlers and chooses values for settings, sometimes writes rules, and occasionally creates a monitor. The HPE Security Fortify Runtime Solution Designer must understand both software and security.	Included with product download and on the Protect724 site

Document / File Name	Description	Location
HPE Security Fortify Runtime Java Edition Designer Guide HPE_RT_Java_Design_Guide_<*version*>.pdf PDF only; no help file	This document provides information to aid users in the configuration and customization of Fortify Runtime for a given application that operates on a Java platform. The audience for this guide includes HPE Security Fortify Runtime Solution Designers who often create event handlers and choose values for settings, sometimes write rules, and occasionally create a monitor. The Fortify Runtime Solution Designer must understand both software and security.	Included with product download and on the Protect724 site
HPE Security Fortify Runtime Application Protection (RTAP) .NET Installation Guide HPE_RTAP_DotNet_Install_<*version*>.pdf HPE_RTAP_DotNet_Install_Help_<*version*>	This document describes how to install the Fortify Runtime Agent for applications running under a supported .NET Framework on a supported version of IIS.	Included with product download and on the Protect724 site
HPE Security ArcSight Application View Runtime Agent Installation Guide HPE_AppView_RT_Agent_Install_<*version*>.pdf HPE_AppView_RT_Agent_Install_Help_<*version*>	This document describes how to install the Fortify Runtime Agent for applications running under a supported Java Runtime Environment (JRE) on a supported application server or service and applications running under a supported .NET Framework on a supported version of IIS.	Included with product download and on the Protect724 site
HPE Security Fortify Runtime Application Protection	This document provides information and procedures	Included with product download and on the

Document / File Name	Description	Location
Operator Guide HPE_RTAP_Oper_Guide_<*version*>.pdf HPE_RTAP_Oper_Help_<*version*>	that enable you to run and monitor the operation of HPE Security Fortify Runtime Application Protection.	Protect724 site
HPE Security ArcSight Application View Quick Start HPE_AppView_Quick_Start_<*version*>.pdf PDF only; no help file	This document provides brief instructions about how to get started with installing and configuring HPE Security ArcSight Application View.	Included with product download and on the Protect724 site
HPE Security Fortify RTAP Rulepack Kit Guide HPE_RTAP_Rulepack_Kit_<*version*>.pdf PDF only; no help file	This document describes the detection capabilities of HPE Security Fortify Runtime Application Protection (RTAP) and the HPE Security Fortify RTAP Rulepacks. Each category of attack, vulnerability, or audit event detected by RTAP is described in this document.	Included with product download and on the Protect724 site
HPE Security Fortify RTAL Rulepack Kit Guide HPE_RTAL_Rulepack_Kit_<*version*>.pdf PDF only; no help file	This document describes the capabilities of the HPE Security Fortify Runtime Application Logging (RTAL) Rulepack Kit. The HPE Security Fortify RTAL Rulepack is a special Runtime Kit for HPE Security Fortify Runtime. It provides information about web application internal activities to ArcSight analysis servers so that these events can be correlated with other existing ArcSight event information.	Included with product download and on the Protect724 site
HPE Security Fortify Runtime	This document recommends	Included with product

Document / File Name	Description	Location
Performance Tuning Guide HPE_RT_Perf_Tuning_<*version*>.pdf PDF only; no help file	ways to address performance bottlenecks a user might encounter in HPE Security Fortify Runtime. It is meant to supplement, not replace, the HPE Fortify Runtime Installation and Configuration guides. It is intended for users who are familiar with and can correctly install and run HPE Security Fortify Runtime.	download and on the Protect724 site

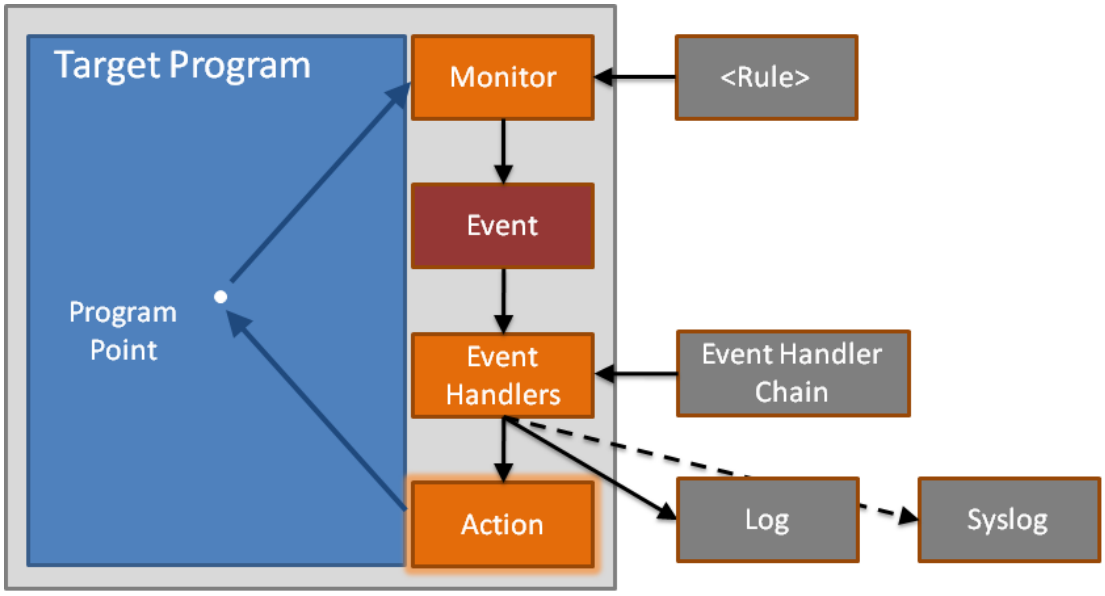
Chapter 2: Overview of HPE Security Fortify Runtime Application Protection

This chapter discusses the following RTAP Rulepacks and Rules.

About RTAP at Work

RTAP protects programs running under a supported Java Virtual Machine (JVM) or .NET CLR. The Java program can be a web application container or any other program.

The following figure provides an overview of RTAP components.



Protections are Defined by Rules

RTAP protections are defined by rules. A Rulepack serves as a container for one or more rules. HPE Security Fortify supplies an RTAP Rulepack for protecting against common types of attacks. You can also create your own custom Rulepacks.

A single rule specifies one or more program points that declare where to monitor a target program and one or more monitors that define what to watch for at a given program point. When a monitor detects the specified behavior in the target program, it creates an event.

Event Handlers Define Response to Events

An event is a collection of attributes. Attributes provide information such as category of problem that has been detected and the location in the code where the problem was detected.

RTAP evaluates the ongoing stream of events with a set of event handlers. An event handler matches against event attributes and specifies the way RTAP should respond. A response might include a passive activity such as logging the event or sending out a syslog notification, or it might include an action: a change to the state of the target program. An action could throw an exception or display a special error message to the user.

Event handlers are organized in an event handler chain. By default, RTAP stops evaluating the event handler chain after it finds the first matching event handler. The event handler chain enables the Runtime Solution Designer to organize event handlers into a sequence that provides the optimal action to take to protect the target program

About RTAP Modes of Operation

RTAP has two modes of operation: *Standalone mode* and *Federated mode*.

Standalone Mode

In Standalone mode, RTAP reads its configuration (including rules, event handlers, and other settings) from disk.

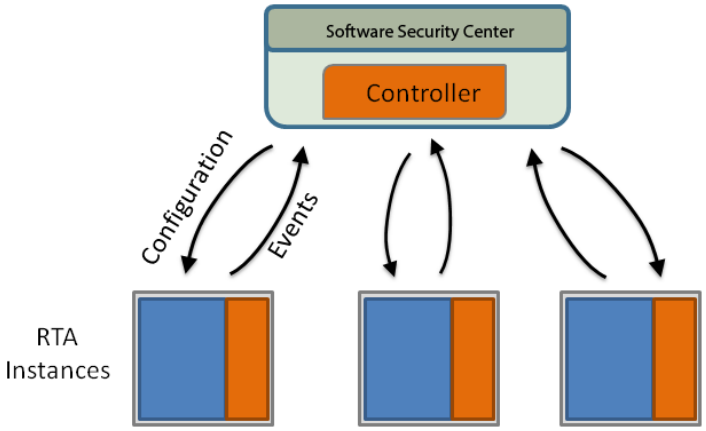
Federated Mode

In Federated mode, multiple computers running RTAP work in concert. They use the network to share a common source of configuration information and common event repository.

In Federated mode, an instance of RTAP:

- Operates as a Host member of an RTAP Federation
- Receives its configuration from a Federation Controller
- Transmits security events to its Federation Controller

The following figure shows the relationship of three hosts to an instance of HPE Security Fortify Software Security Center running as those hosts' Federation Controller.



After an RTAP Host receives a configuration from its Federation Controller, the Host caches the configuration. The Host uses that cached configuration until the Federation Controller sends a new configuration. The Host preserves the most recent cached configuration across program restart. This enables a RTAP Host running in Federated mode to resume operation without waiting for the Federation Controller to re send the Host's configuration.

About RTAP User Roles

Deploying, configuring, customizing, and monitoring the runtime platform often involves more than one person within an organization. In this section the three conceptual roles for runtime platform users is described. A single individual may fulfill more than one role, or duties for a single role may be spread across a team.

The Runtime platform conceptual roles may be classified as:

- RTAP Analyst
- RTAP Operator
- RTAP Solution Designer

HPE Security Fortify RTAP Analyst

This person is responsible for monitoring RTAP on an ongoing basis and for making limited configuration changes. An RTAP Analyst looks at RTAP output and makes decisions. An RTAP Analyst might modify event handlers or adjust settings within the structure established by the RTAP Solution Designer. This is principally a security role.

HPE Security Fortify RTAP Operator

This person is responsible for installation, basic configuration, and ongoing maintenance of the runtime system. An RTAP Operator expects the RTAP Solution Designer to provide a configuration for a particular application. With the configuration in hand, the HPE Security Fortify Runtime Operator can deploy RTAP. An RTAP Operator has skills which are similar to a system administrator.

HPE Security Fortify RTAP Solution Designer

This person is responsible for configuring and customizing RTAP for a given application. An RTAP Solution Designer often creates event handlers and chooses values for settings, sometimes writes Rules, and occasionally creates a Monitor. The RTAP Solution Designer must understand both software and security.

HPE Security Fortify RTAP User Role Examples

These roles may be fulfilled in different ways to meet the needs of different organizations.

Example 1: Business unit in a large enterprise

- RTAP Analyst: Central security team
- RTAP Solution Designer: Central security team working with developers
- RTAP Operator: Operations team

Example 2: Small team

- RTAP Analyst: Data center Network Operations Center (NOC)
- RTAP Solution Designer: Software architect
- RTAP Operator: Development team

Example 3: Outsourced data center

- Analyst: Central security team
- Solution Designer: Fortify Global Services
- Operator: outsourced data center operations

Chapter 3: Running HPE Security Fortify Runtime Application Protection in Standalone Mode

This chapter contains the following topics:

About the Standalone Mode Security Events Log

In Standalone mode, RTAP writes security events to a security events log file.

The following example shows the general form of an RTAP security event.

Example: RTAP event for the reflected cross-site scripting attack

```
[2009-09-29T09:51:04,680 EVENT]
Cross-Site Scripting
{
timestamp: 1254243064680
category: Cross-Site Scripting
subcategory: Reflected
.
.
.
}
name*: errorMsg
values*: </font><script>alert('exploited');</script><font>
Trigger*: name = errorMsg, values = </
font><script>alert('exploited');</script><font>
```

```
action: display (default)
dispatch: log (8)
}
```

In Federated mode, use the Runtime tab options to view security events.

Viewing Standalone Mode Security Events

In Standalone mode, RTAP writes security events to a security events log file.

By default, RTAP running in Standalone mode creates security event log file in `<install_dir>/log`.

To view the default RTAP security events log file, go to `<install_dir>/log`, and open `event.log` in a text editor. Scroll to the bottom of the security events log file to view the most recent events.

Managing Standalone Mode Security Event Log Files

In the RTAP Standalone mode configuration file, you can use the following configuration elements to control the size and number of RTAP security event log files:

- EventLogFile
- EventLogFileMaxBackups
- EventLogFileMaxSize

About RTAP System Messages in Standalone and Federated Mode

In Standalone mode, RTAP writes operational messages to a system log file.

In Federated mode, use the Runtime tab options to view system messages.

Viewing Standalone Mode System Messages

To view the default RTAP system log file, navigate to the `<install_dir>/log`, and open the `system.log` file in a text editor.

Managing Standalone Mode System Event Log Files

In the RTAP Standalone mode configuration file, you can use the following configuration elements to control the size and number of RTAP system event log files:

- `SystemLogFile`
- `SystemLogFileMaxBackups`
- `SystemLogFileMaxSize`

Chapter 4: Configuring HPE Security Fortify Runtime Application Protection in Standalone Mode

This chapter contains the following topics:

About RTAP Standalone Mode Configuration

You can configure RTAP to run in Standalone mode. In Standalone mode, RTAP:

- Reads its configuration from a configuration file
- Writes security events to an event log or to syslog
- Performs protective actions on an application

Updating Configuration File Settings

If RTAP is protecting a running target program, and RTAP is running in Standalone mode, then RTAP periodically scans its configuration file for changes. If RTAP detects changes in the configuration file, then RTAP loads and applies those changes.

For information about the frequency at which RTAP scans its configuration file for changes, see the table `ConfigurationPollInterval` parameter in the "RTAP Global Configuration Settings" on the next page table.

Standalone Mode Configuration File Sections

For RTAP running in Standalone mode, the Standalone mode configuration file contains three major sections:

- Global Settings
- Rules
- Event handlers

Summary of Standalone Configuration Options

The following table lists the RTAP Standalone configuration file options.

RTAP Global Configuration Settings

Global Configuration Setting	Description
`ConfigurationPollInterval`	Specifies the integer number of seconds between scans of the active configuration file. If zero or negative, RTAP does not periodically scan its configuration file for changes. Default: `2`
`DisplayDefaultForwardUrl`	If an RTAP rule does not specify an action, and RTAP detects the security condition specified by that rule, then RTAP displays the HTML page at the location specified by `DisplayDefaultForwardUrl`. Default value: No default value
`DisplayDefaultHtml`	The default HTML used with the display action. Used if no settings are supplied on the action. Default: `<!--'"--><html><table border=0 width=100% height=100% bgcolor=black><tr><td valign=center align=center><font face=Arial color=white>Protected by<h1>HPE SecurityFortify</h1></font></td></tr></table></html>`
`DisplayDefaultHttpStatusCode`	If an `action` specifies no HTTP status code, then RTAP transmits the HTTP status code specified by `DisplayDefaultHttpStatusCode`. Default: No default value.
`DisplayDefaultText`	If an action specifies no text display, then RTAP displays the text specified `DisplayDefaultText`. Default: `Protected by HPE Security Fortify`
`EnableActions`	If `true`, RTAP performs the actions defined in event handlers. If `false`, RTAP ignores actions defined in event handlers.

RTAP Global Configuration Settings, continued

Global Configuration Setting	Description
	Default: `true`
`Enabled`	Controls whether RTAP watches the target program If `Enabled` equals `true`, RTAP monitors the target program. If `Enabled` equals `false`, RTAP does not monitor the target program. The `Enabled` setting provides a single parameter to enable or disable RTAP. If `Enabled` equals `false`, the JVM runs as if RTAP was not installed. Default: `true`
`EventDispatchQueueSize`	The maximum capacity of the event dispatch queue. Normally, event dispatching is handled asynchronously. This setting controls the number of events that can be queued for dispatch before the application is blocked. If this value is too large, it can lead to memory problems if a very large number of events are generated in a short amount of time. A value of zero means that the queue is unbounded. Default: `100`
`EventLogFile`	Full path to the RTAP security events log file. If `EventLogFile` specifies `stdout`, RTAP writes security events to the system console rather than to a log file. If `EventLogFile` specifies a name that ends with `.gz`, RTAP will compress the log file using the same compression algorithm used by the gzip utility. If more than one concurrent RTAP instance writes to the same log file, the second process writes to `event1.log`, the third to `event2.log`, and so on. Default: `${FortifyHome}/log/event.log`
`EventLogFileMaxBackups`	The maximum number of event log file backups RTAP creates before overwriting existing log data. Default: `9`

RTAP Global Configuration Settings, continued

Global Configuration Setting	Description
`EventLogFileMaxSize`	The maximum size of the event log file before moving log data to a backup file. RTAP appends the number of the backup file to a given backup file's name. For example, RTAP names the first backup file `event.log.1`, the second `event.log.2`, and so on. Default: `100MB`
`FortifyHome`	The root directory of the RTAP files hierarchy. Default: The RTAP installation directory
`FortifyLicenseFile`	The path to the HPE Security Fortify license file. RTAP requires an up to date license in order to run. Default: If unspecified, then look for `fortify.license` in `${FortifyHome}`, then search recursively in parent directories of `${FortifyHome}` until found.
`MaxUntrustedAttributeLength`	The maximum permitted length, in octets, of an untrusted event attribute. If RTAP encounters an untrusted attribute that exceeds the value of `MaxUntrustedAttributeLength`, RTAP truncates that untrusted attribute. Default: 10240
`SyslogDefaultPicture`	The format for `syslog` messages. RTAP forwards all event attributes. For information about formatting RTAP output strings, see About String Formatting Picture Parameters. Default: `%all`
`SyslogDefaultSeverity`	The default severity of `syslog` messages. If the RTAP dispatcher does not specify a severity, then RTAP uses the severity specified by `SyslogDefaultSeverity`. Default: `error`

RTAP Global Configuration Settings, continued

Global Configuration Setting	Description
`SyslogPort`	The default `syslog` port number. Default: `514`
`SyslogServer`	The default `syslog` host. Default: No default value.
`SystemLogFile`	Name of the RTAP system events log file. If more than one concurrent RTAP instance writes to the same log file, the second RTAP instance writes to `system1.log`, the third instance to `system2.log`, and so on. Default: `${FortifyHome}/log/system.log`
`SystemLogFileMaxBackups`	Maximum number of system log file backups RTAP creates before overwriting existing security events log data. Default: `9`
`SystemLogFileMaxSize`	Maximum size of the system log file before RTAP begins writing log data to a backup file. If RTAP creates a backup log file, RTAP names the first backup file `system.log.1`, the second `system.log.2`, and so on. Default: `100MB`
`SystemLogLevel`	The minimum severity of system messages written to the log file. Valid values are `trace`, `debug`, `info`, `warn`, `error`, or `fatal`. Default: `info`
`SysLogMessageLength`	Determines the length of the message RTAP sends to `Syslog`. Default: `1024`
`TmpDirectory`	The directory where the RTAP writes temporary files. Default: `${FortifyHome}/tmp`

Chapter 5: Managing RTAP Configuration Files

This chapter contains the following topics:

Specifying Configuration Files When Starting RTAP

When you add RTAP protection to a JVM, you can also specify the location of a non‑default RTAP configuration file. To do this, add the full path of the configuration file to the -javaagent option, for example:

```
-javaagent:<install_dir>/lib/FortifyAgent.jar=<full path to configuration file>
```

Defining Configuration Settings

This chapter contains the following topics:

Overview of Configuration File Variables

In addition to the default set of RTAP configuration elements, you can also create configuration file variables. Configuration file variables specify settings or values that can then be referenced throughout the configuration file in which the variable was defined.

Defining Configuration File Variables

To define an RTAP configuration file variable, you create a new configuration Setting element, then specify that new element's attributes.

The following illustrates the general form of a configuration file variable definition:

```
<Setting name="MyAction">display</Setting>
```

In the preceding example:

- The `Setting` XML element defines the XML element that will contain the new configuration file variable.

- The `name` attribute specifies the name value pair (`MyValue`, equal to `display`) of the new configuration file variable.

Referencing a Configuration File Variable

After defining a variable named `MyAction`, you can reference the variable in an event handler's action. The following illustrates the general form of a configuration file variable reference:

```
<Action name="${MyAction}"/>
```

You can also use RTAP configuration file variables to control the behavior of a particular category of configuration file settings.

For example, for all rule `category` attributes, a configuration variable named `all_protected` equal to `true` could define a configuration in which all rule actions equal `rewrite` and `display`. Changing the value of `all_protected` to `false` would then change the rule actions to `log`.

Using Configuration Variables to Reference System Variables

You can also use RTAP configuration file variables to access system environment variables. To reference a system environment variable, preface the system variable name with `env`.

For example, to access the environment variable PWD, reference a configuration file as `${env.PWD}`.

Chapter 6: About String Formatting Picture Parameters

The `SyslogDefaultPicture` configuration setting described in "RTAP Formatting Variables" below allows you to use formatting statements to control how RTAP formats log files output.

The following table lists the string formatting variables supported by `SyslogDefaultPicture` configuration setting.

RTAP Formatting Variables

Formatting Parameter	Description
`%all`	All event attributes
`%hostname`	The name of the host computer
`%location`	The first line of the target program stack where the event was created
`%n`	A newline character
`%timestamp`	The time and date formatted per the ISO8601 standard
`%variable`, `%{variable}`	An RTAP event attribute other than the ones defined in the preceding table rows RTAP treats `%%` as a single `%` character

Chapter 7: HPE Security Fortify Runtime Application Protection Rulepacks and Rules

This chapter discusses the following RTAP Rulepacks and Rules.

About the Default RTAP Rules Set

RTAP rules specify how RTAP monitors and protects a target program.

An RTAP rule specifies one or more program points, and one or more monitors that

connect one or more rules to those program points.

By default, RTAP running in Standalone mode loads rules from both:

- The `<rules>` section in the configuration file `<install_dir>/config/rt_config.xml`
- The default Rulepack file `<install_dir>/rules/rules.rpr`

RTAP running in Federated mode receives its Rulepacks from its Federation Controller.

About RTAP Rulepacks

An RTAP Rulepack is an XML document that conforms to the schema defined by `<install_dir>/sdk/schema/rules.xsd`.

In its simplest form, a Rulepack contains a preamble with information about the Rulepack, followed by a list of RTAP rules. More typically, an RTAP Rulepack contains multiple rules.

RTAP DisableRules Element Example:

```
<DisableRules>
<Not><MatchAttribute name="vulnerability"/></Not>
</DisableRules>
```

About Importing an RTAP Rulepack

In the RTAP configuration file (by default `<install_dir>/config/rt_config.xml`), use the rules section to:

- Specify one or more additional rules files
- Enable or disable individual rules or groups of rules

Specifying the Location of Rulepack Files

To include a rules file named `my_rules.xml`, in the RTAP configuration file, add the line shown in the following example.

Commands used to specify the location of a Rulepack file Example:

```
<RulesFile>my_rules.xml</RulesFile>
```

In the preceding example, `my_rules.xml` specifies the full pathname to an external rules file.

Enabling RTAP Rules

By default, RTAP enables all rules. To explicitly enable an individual rule, use the `<EnableRules>` and `<MatchAttribute>` elements.

The following example illustrates the use of the `EnableRules` and `MatchAttribute` elements to enable a rule with a particular GUID.

RTAP EnableRules Element Example:

```
<EnableRules>
<MatchAttribute name="RuleID">dd6bb321-d25c-4797-843c-926a486d12be \
</MatchAttribute>
</EnableRules>
```

Disabling RTAP Rules

To disable one or more rules, use the `<DisableRules>` and `<MatchAttribute>` elements.

The following example illustrates the general form of the `DisableRules` and `MatchAttribute` elements to disable all rules where the category attribute equals `Privacy Violation`.

RTAP DisableRules Element Example:

```
<DisableRules>
<MatchAttribute name="category">Privacy Violation
</MatchAttribute>
</DisableRules>
```

Disabling Rules that Do Not Detect Vulnerabilities

You can use the `<DisableRules>` tag to disable all rules that do not detect vulnerabilities.

The following example illustrates the general form of the `Disable Rules` and `MatchAttribute` elements to disable all rules that do not include the attribute `vulnerability`.

RTAP DisableRules Element Example:

```
<DisableRules>
<Not><MatchAttribute name="vulnerability"/></Not>
</DisableRules>
```

Chapter 8: Operating HPE Security Fortify Runtime Application Protection in Federated Mode

This chapter contains the following topics:

About the Fortify Software Security Center Runtime Tab Options

The Fortify Software Security Center **Runtime** tab options enable you to perform monitoring and configuration of one or more instances of RTAP running in Federated mode. In addition to the **Runtime** tab, the Fortify Software Security Center Dashboard includes information about RTAP Hosts and events.

Two of the primary ways you will perform monitoring and configuration are:

- Viewing and responding to Runtime events
  For information about Runtime events, see "About Runtime Events" on the next page.
- Adding, modifying, or disabling a given Runtime Host's Event Handlers
  For information about working with Event Handlers, see "Managing a Configuration's Event Handlers" on page 37.

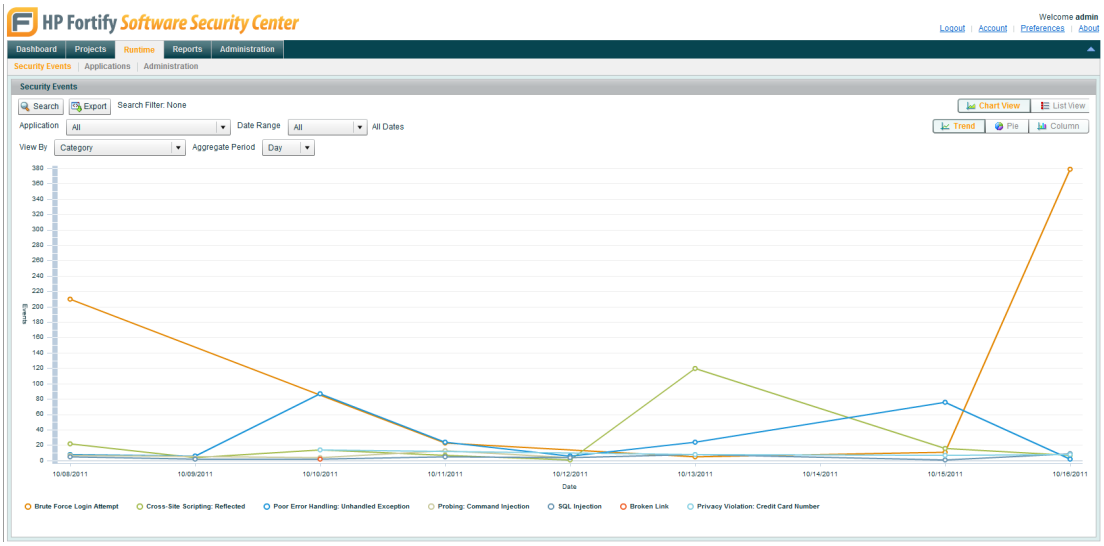
Displaying Runtime Features

To access the **Runtime** tab and associated tools, you will need a Fortify Software Security Center account.

Perform the following procedure to display RTAP features.

To display RTAP features:

1. Log on to Fortify Software Security Center.
   By default, Fortify Software Security Center displays the Dashboard.
2. In Fortify Software Security Center, click **Runtime**.
   By default, Fortify Software Security Center displays the RTAP Security Events page.



For more information about RTAP security events, see "About Runtime Events" on the next page.

About Fortify Software Security Center Runtime Tab Sections

In the **Runtime** tab, Fortify Software Security Center organizes RTAP features into three top level categories. Each category provides access to one or more functionally related tools.

The following table summarizes the three feature sections and tells you where in this chapter you can find more information about that section's tools and operations.

Runtime Tab Section	Description
Security Events	Use the Runtime tab's Security Events section to view RTAP security events as: • A list • A trend, pie, or bar chart For more information about working with see "About Runtime Events" below.
Applications	Use the Runtime tab's **Applications** section to view and manage Runtime Applications. In the **Runtime** tab, **Applications** provide a way to characterize an application program or group of related programs for purposes of configuring, managing, and reporting. For more information about working with Runtime Applications, see "About Creating and Managing Runtime Configurations" on page 48.
Administration	Use the Runtime tab's Administration section to create and manage Runtime Hosts, Applications, Federations, and Configurations. For information about specific features available in the tab's Administration page, see the following sections: • "About Runtime Host Creation and Management" on page 39 • "Creating and Managing Application Assignment Rules" on page 46 • About Runtime Federations

About Runtime Events

The Fortify Software Security Center provides two primary ways to display RTAP security events:

- **Chart View** allows you to display security events as a trend, pie, or bar chart.
- **List View** displays security events as a customizeable list.

Both methods of viewing RTAP security events enable you to filter events on the basis of time, type, or Runtime Application.

Viewing Event Details

Perform the procedure in this section to view multiple categories of detail about a Runtime security event.

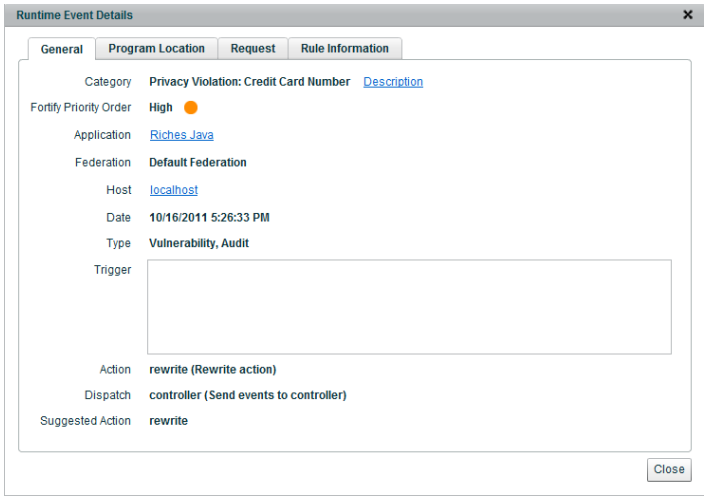
The Runtime features provide more than one way to access many of its tools and options. As you acquire more experience with the Runtime features, you will discover different ways to access options and perform tasks.

To view the Runtime Event Details dialog box:

1. Display the **Security Events** page in **List View**.
   a. Log on to Fortify Software Security Center.
   All Fortify Software Security Center account privilege levels can view RTAP security events if application access has been granted to that account. For more information about granting access to a Fortify Software Security Center user account, see the Fortify Software Security Center User Guide.
   b. In the **Runtime** tab, click **Security Events**.
   The Fortify Software Security Center displays the **Security Events** page. By default, the page lists events in the **Trend** chart view.
   c. In the upper right of the **Security Events** page, click **List View**.
   Current security events are listed in column form.
2. Display the details for a Security Event.

   In the Security Events page, in List View, choose an event then in the left side Security Event area click **View Details**.

   The Fortify Software Security Center displays the Runtime Event Details dialog box.



   The **Runtime Event Details** dialog box contains tabs that provide information about a specific aspect of the selected Security Event.
3. In the Runtime Event Details dialog box:
   - To view details about the security event, including what triggered the event, choose the **General** tab.
   In the **Runtime Event Details** dialog box, the Fortify Software Security Center displays only the tabs that are applicable to the selected event.

     To view details about the event, in **Category** click **Description**. Depending on your installation's security requirements, you may be asked to accept a temporary security certificate from the HPE Security Fortify content site, or abandon the request.

     To access the Runtime Application associated with the selected security event, click the **Default Application** link to display the Runtime Application page in the background, then click **Close** to close the Runtime Event Details dialog box. The Default Application link will actually appear as

whatever the name of the application is. For more information about the Runtime Application page, see "About Creating and Managing Runtime Configurations" on page 48.

To access the Runtime Host associated with the selected security event, click the **Host** link to display the Runtime Hosts page in the background, then click **Close** to access the Hosts page. For more information about the Runtime Hosts page, see "About Runtime Host Creation and Management" on page 39.

- If this event is associated with an Alert Notification, then the Fortify Software Security Center displays the **Alert** tab. To view details about the selected alert, choose the **Alert** tab.
- To view a trace of the events that preceded the security event, choose the **Program Location** tab.
- If this event has an associated stack trace, then the Fortify Software Security Center displays the **Exception** tab. To view the stack trace for the selected alert, choose the **Exception** tab.
- If this event has additional attributes, then the Fortify Software Security Center displays the **Other Attributes** tab.
- To view the stack trace for the selected alert, choose the **Additional Attributes** tab.
- To view details about the rule that detected the security event, choose the Rule Information tab. For information about Runtime rules and Rulepacks see "About Runtime Configuration Attributes" on page 56.

  To view details about the HTTP request that caused the security event, choose the Request tab.

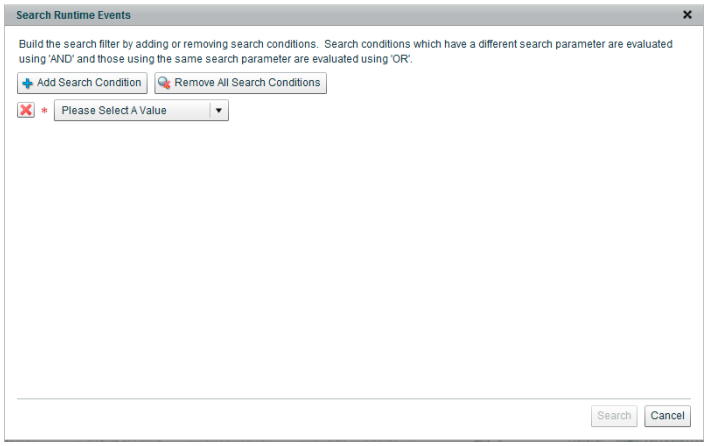
4. To exit the **Runtime Event Details** dialog box, click **Close**.

Searching Runtime Events

Use the Runtime Search tool to search for Runtime events.

To search Runtime events:

1. Display the **Security Events** page.
2. In the **Security Events** page, click **Search**.
   The Fortify Software Security Center displays the **Search Runtime Events** dialog box.



3. Specify the type of Runtime Events to search for. In the **Search Runtime Events** dialog box:
   a. Click Add Search Condition.
   The **Search Runtime Events** adds search attribute tools to the new search condition specifier.
   b. In the search condition list, select a type of event, then choose the values of the selected event attribute.
   c. Click **Add Search Condition** to specify additional search conditions.
   Click **Remove all Search Conditions** to remove all condition selectors from the search.
4. Click **Search**.
   The Fortify Software Security Center lists the Runtime Events that match the specified search conditions.

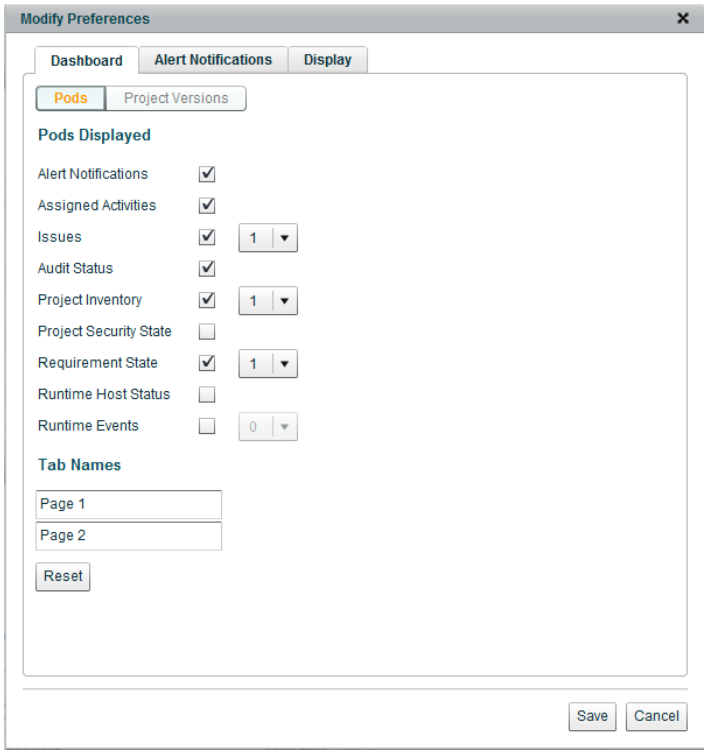
Configuring Runtime Preferences in the Dashboard

Perform the procedure in this section to configure how Fortify Software Security Center:

- Displays Runtime events in the Fortify Software Security Center Dashboard
- Sends Runtime Alert notifications to the email address specified in your Fortify Software Security Center user profile

To configure your Runtime preferences in Fortify Software Security Center:

1. In the Fortify Software Security Center Dashboard, click **Preferences**.
   Fortify Software Security Center displays the Modify Preferences dialog box. By default, the Modify Preferences dialog box opens on the Dashboard tab.



2. To display Runtime pods in the Fortify Software Security Center Dashboard, go to the **Dashboard**

tab, select **Preferences**, the select **Runtime Events**. Choose the number of Runtime Event pods to display in the Fortify Software Security Center Dashboard.

3. To enable email notification of Alert Events, click the **Alert Notifications** tab, then ensure Delivery Options is selected. Select **Email Alert Notifications**.
4. In the **Modify Preferences** dialog box, select the **Alert Notifications** tab, then click **Runtime Alerts**. Select **Receive Runtime Alert Notifications** to enable Runtime Alert notifications in the Fortify Software Security Center Dashboard.
5. Then in the **Applications** area, select whether you want to receive Runtime alert notifications from All applications you have access to or a specific Selected set of applications. If you clicked **Selected**, click **Add** to select the desired applications from the list in the Select Applications dialog box and then click **OK**.
6. Click **Save** to apply your changes and return to the Fortify Software Security Center Dashboard.

Managing a Configuration's Event Handlers

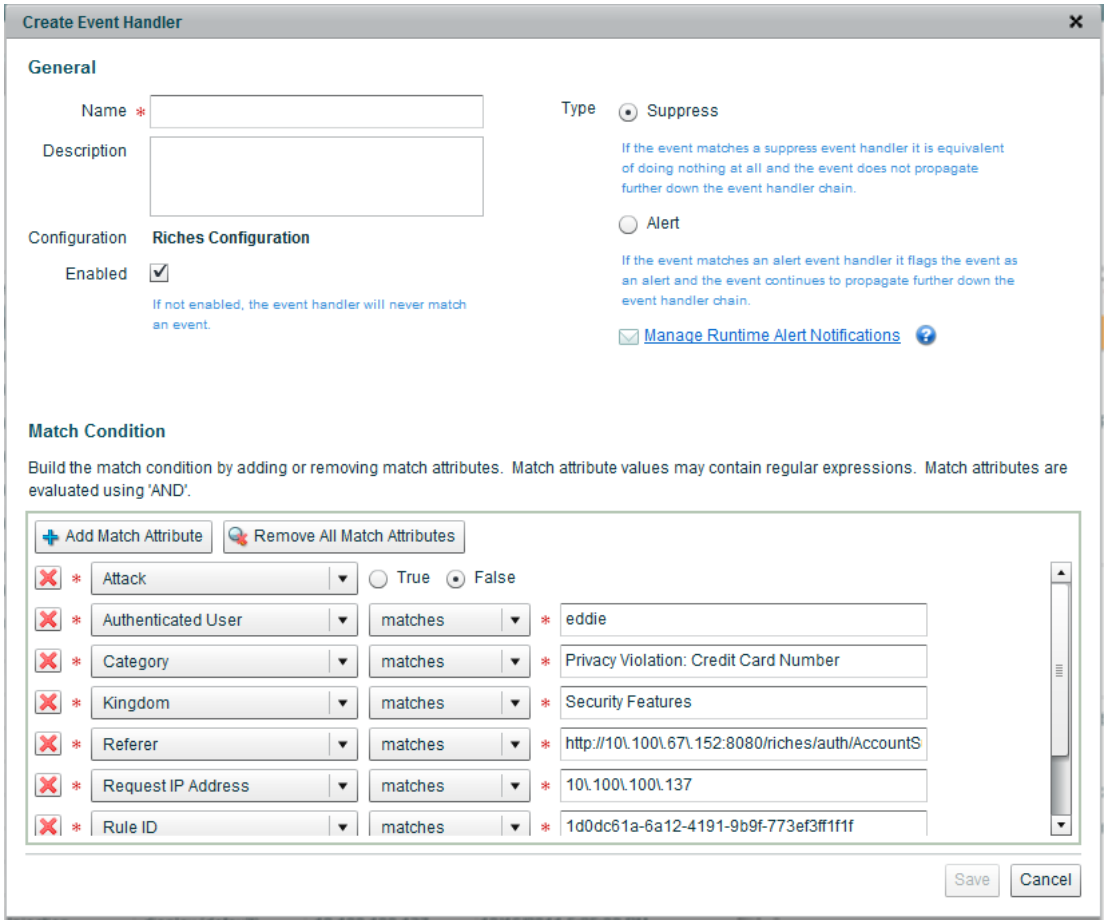
Runtime features include a GUI tool you can use to create new Event Handlers.

One Runtime features provides multiple ways to access the Create Event Handler tool. One way is to use an RTAP security event as the basis for a new Event Handler.

To use a security event as the basis for a new RTAP Event Handler:

1. Display the **Security Events** page in **List View**.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to create or edit an Event Handler.
   b. In the **Runtime** tab, click **Security Events** then in the top right of the page click **List View**. The Fortify Software Security Center displays the Security Events page.
2. Create a new Event Handler.
   In the **Security Events** page, in the list of events, select a security event then click **Add Event Handler**.

   The Fortify Software Security Center displays the **Create Event Handler** page.



In the **Create Event Handler** dialog, the **Match Condition** area contains the match attributes from the RTAP Rule that generated the Security Event.

3. To configure the new **Event Handler**, in the **Create Event Handler** dialog box:
   a. In the **Name** text entry area, type the name of the new Event Handler.
   b. To enable this event handler, select **Enabled**.
   c. To use this Event Handler to terminate RTAP event handler processing, in the **Type** area click **Suppress**.
   Do not click **Save**.
   d. To use this Event Handler to generate an alert, in the **Type** area click **Alert**.
4. Update the Event Handler's match conditions. In the **Match Condition** area:
   a. To add a new match attribute, click **Add Match Attribute**.
   The Create Event Handler dialog box adds a Please Select A Value placeholder attribute to the list of match attributes.
   b. To modify a match attribute, select a match attribute then in the shortcut list choose a type of match attribute.
   The **Create Event Handler** dialog box guides you through configuration of the match attribute by enabling and disabling options for that choice.
   c. To delete a match attribute, in the left of the list of attributes click the red X.
5. Click **Save**.

About Runtime Host Creation and Management

A Runtime *Host* is a computer running one or more federated instances of RTAP.

If RTAP has been configured to run in Federated mode, then when a given Runtime Host first starts, it attempts to contact the Fortify Software Security Center specified in its configuration file. After connecting to Software Security Center the Host receives its configuration from and reports its events to that server.

For any Host that has not yet been associated with a Federation, the Fortify Software Security Center transmits the Default Federation and associated configuration.

For more information about Runtime Applications, see "About Creating and Managing Runtime Configurations" on page 48.

Managing Undefined Hosts

To help ensure secure deployment of RTAP and the Runtime features, by default the Fortify Software Security Center refuses connections from undefined Hosts.

You can enable new Hosts to connect to the Fortify Software Security Center in either of two ways:

- Enable the Fortify Software Security Center to accept new connection requests from all RTAP instances.
  For information about enabling connections for all Hosts, see "Enabling Connections For all Undefined Hosts" below.
- Create a new Runtime Host definition before that Host issues a connection request to the Fortify Software Security Center.
  For information about creating a new Host definition, see "Adding a New Runtime Host" on the next page.

Enabling Connections For all Undefined Hosts

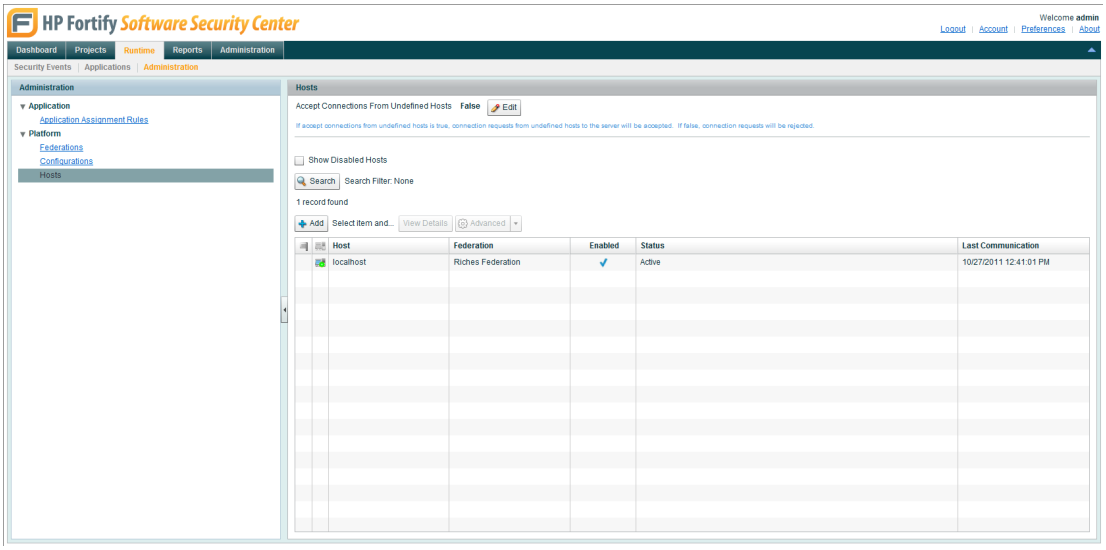
Perform the procedure in this section to enable or disable connection requests from undefined Hosts.

Before enabling connection requests from undefined Hosts, consider what security implications might apply in your network.

To enable or disable connections from undefined Runtime Hosts:

1. Log on to Fortify Software Security Center with Administrator or Security Lead privileges.
   You must have at least Security Lead privileges to change the Fortify Software Security Center's Hosts connection setting.
2. Display the **Hosts** page.
3. In the Runtime tab, click **Administration**, and then in the left side navigation pane click **Hosts**.

   The Fortify Software Security Center displays the **Hosts** page.



In the top of the **Hosts** page, the **Accept Connections from Unknown Hosts** area displays the current setting of the control: **True** equals accept connections from undefined Hosts.

In the **Active** column, the Fortify Software Security Center displays a colored icon for active Hosts; for disabled Hosts, the Fortify Software Security Center displays a light gray icon. For information about enabling or disabling Hosts, see "Enabling and Disabling Runtime Hosts" on the next page.

4. In the **Accept Connections from Unknown Hosts** area, click **Edit** and then click **Yes** or **No**.

   The Fortify Software Security Center applies the new setting and updates the status indicator.

Adding a New Runtime Host

If the Fortify Software Security Center is configured to refuse connections from undefined hosts, and Fortify Software Security Center receives a new connection request from a Host that is not defined in the Fortify Software Security Center then Fortify Software Security Center will refuse that connection request.

To enable a particular new Host to connect to the Fortify Software Security Center, create a new Runtime Host definition for that Host. This authorizes the Fortify Software Security Center to accept that newly defined Host's connection request.

Perform the procedure in this section to add a new Host definition to Fortify Software Security Center's list of Runtime Hosts.

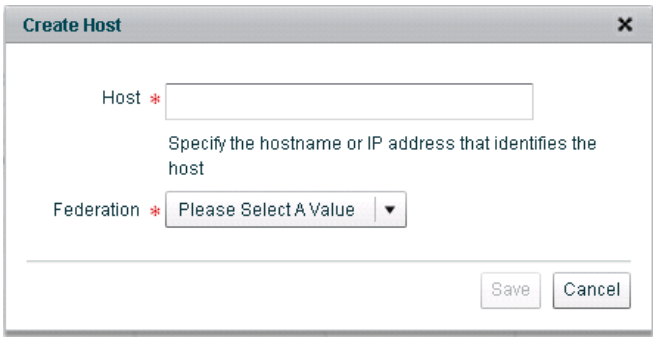
Before You Begin

Before performing the procedure in this section, note that the Fortify Software Security Center permits you to disable and edit Host definitions, but not delete Host definitions for hosts which have connected and sent data to the server.

To add a Runtime Host definition to the Runtime:

1. Log on to Fortify Software Security Center with Administrator or Security Lead privileges.
   You must have at least Security Lead privileges to add a Host definition to the Runtime.

2. Display the **Hosts** page.
3. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Hosts**.
   The Fortify Software Security Center displays the Hosts page.
4. In the Hosts page, click **Add**.
   The Fortify Software Security Center displays the **Add Host** dialog box.



5. Configure the new Runtime Host definition. In the **Add Host** dialog box:
   a. In the **Host** text entry area, type the network name for the Host or the Host's IP address.
      In general, if you have defined the host in your networks DNS, type the URL of the Host.
   b. In the **Federation** list, choose the Federation.

      For more information about creating Runtime Federations, see *About Runtime Federations* on page 46.

      After you supply all required information, the Fortify Software Security Center enables the Save button.
6. Click **Save**.

   The Fortify Software Security Center adds the new Host definition to the list of definitions.

   The newly defined Host is now known to Fortify Software Security Center. If the Fortify Software Security Center is configured to refuse undefined Host connections, and the new Host attempts to connect to Fortify Software Security Center, Fortify Software Security Center will accept the connection from this host.

Enabling and Disabling Runtime Hosts

You can disable a Runtime Host only after you stop the associated target application.

Fortify Software Security Center will not accept connection requests for disabled Runtime Hosts.

To enable or disable a Runtime Host:

1. Log on to Fortify Software Security Center.
2. Display the **Hosts** page.
3. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Hosts**.
   The Fortify Software Security Center displays the Hosts page.
4. To change the enabled state of a Runtime Host, in the list of Runtime Hosts, select a Host, click **Advanced**, then click **Enable** or **Disable**.
   Fortify Software Security Center changes the Host state.

Customizing Host List Headings

You may customize the way the Runtime Console lists Hosts.

To customize the Runtime Console's Hosts list:

1. Log in to Fortify Software Security Center with Administrator or Security Lead privileges.
   You must have at least Security Lead privileges to enable or disable a Fortify RTA Host.
2. Display the **Hosts** page.
3. In the **Runtime** tab, click **Administration** then in the left side navigation pane click **Hosts**.
   The Runtime Console displays the Hosts page.
4. In the **Hosts** page, above and to the right of the list of hosts, click the column tool, then choose which columns to display or suppress.
   The Runtime Console refreshes the list of RTAP Hosts. The list includes the new column selections.

Resetting Host Authentication

In the event there is an authentication failure between the RTAP Host and Fortify Software Security Center and you no longer have access to the original certificate, you may click a button in the Fortify Software Security Center UI to reset the host authentication.

The conditions under which an authentication failure may occur would be when either there is no certificate present or an invalid certificate.

To reset host authentication:

1. Display the **Hosts** page.
2. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Hosts**.
   The Fortify Software Security Center displays the Hosts page.
3. To reset the authentication of a Runtime Host, in the list of Runtime Hosts, select a Host, click **Advanced**, then click **Reset Host Authentication**.

It is also recommended the auth directory on the RTAP Host side should be deleted.

Responding to Host Log Messages That Require Attention

In the Hosts page in the left side of the list of the Hosts, Fortify Software Security Center displays a Host Log Messages Require Attention flag.

To view a Host's log messages:

1. In the **Hosts** page, select a Host then click **View Details**.
   The Fortify Software Security Center displays the selected Host's details.

2. In the selected Host's details page, click **Log**.
   Fortify Software Security Center displays a list of log messages. In the list, click a column heading to sort the list.

Chapter 9: Configuring HPE Security Fortify Runtime Applications in Federated Mode

This chapter discusses creating and managing HPE Security Fortify Runtime Applications in Federated mode in the following sections.

About Runtime Applications

In the Runtime, *Applications* are user supplied programs running under the control of an application server.

Applications provide a way to group and associate security events for purposes of management and reporting. This enables you to manage multiple applications that run under the same Runtime Host and report to the same Runtime Federation controller.

Runtime Applications interact with Application Assignment Rules. For information about Application Assignment Rules, see "Creating and Managing Application Assignment Rules" on page 46.

About the Default Application

HPE Security Fortify Software Security Center includes a non deletable Application definition named **Default Application**.

If the Fortify Software Security Center receives a security event from a Runtime Host, and the RTAP has no Application Assignment Rule that associates the event to a Runtime Application definition or application context path, then the RTAP associates the incoming event with the Default Application.

Creating a New Runtime Application

Perform the procedure in this section to create a new Runtime Application definition.

Runtime's Create Application feature consists of a series of three panels. Each of the three panels collects a particular category of required or optional information about the Application.

In the case of required information, the Create Application tool highlights required information in red. You must supply all required information to enable the Create Application tool's **Next** or **Finish** buttons.

To create a new Runtime Application:

1. Display the **Applications** page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to add or edit an Application definition.
   b. In the **Runtime** tab, click **Applications**.
   The Fortify Software Security Center displays the **Applications** page. The page lists all currently defined Applications.
2. In the **Applications** page, click **Add**.
   The Fortify Software Security Center displays the **Create Application feature's Application** panel.
3. In the **Application** panel:
   a. In the **Name** text entry area, type the name of the new Runtime Application.
   You must type a name to enable the Application panel's **Next** button.
   b. If you want to copy the Attributes set from an existing Runtime Application, in the select **Copy Application Attributes**, and then choose a Runtime Application.
   After you supply all required information, the **Application** panel enables the **Next** button.
   c. Click **Next**.
   The Fortify Software Security Center displays the **Create Application** tool's **Business Attributes** panel.
4. In the **Business Attributes** panel choose the optional and required business attributes for the new Runtime Application, then click **Next**.

   The **Business Attributes** panel does not enable the **Next** button until you have chosen all required business attributes.

   Click **Next** to display the **Technical Attributes panel**.
5. In the **Technical Attributes** panel choose the optional and required Technical attributes for the new Runtime Application, and then click **Finish**.

   The **Business Attributes** panel does not enable the **Finish** until you have chosen any required business attributes.

   The Fortify Software Security Center displays the **Applications** page. In the page, the list includes the new Runtime Application definition.

Customizing Business and Technical Attribute Definitions

In Fortify Software Security Center, you can use the **Administration** features to customize the Business and Technical Attributes presented by the **Create Application** feature. For information about managing Fortify Software Security Center Attribute Definitions, see the *HPE Security Fortify Software Security Center User Guide*.

Creating and Managing Application Assignment Rules

This section contains the following topics:

About Application Assignment Rules

Application Assignment Rules specifies the criteria the Fortify Software Security Center uses to associate security events received from RTAP with a particular Runtime Application.

By default, the Fortify Software Security Center associates security events from a Runtime Host with the Default Application. For more information about the Default Application, see "About the Default Application" on page 44

Application Assignment Rules provide the means of logically identifying and categorizing a given Host's security events for purposes of management and reporting.

Application Assignment Rules associate security events to a Runtime Application. An Application Assignment Rule can examine any event attribute on the Host that generated the event. The Fortify Software Security Center can associate Host events to a Runtime application in either or both of two ways:

- If you create an Application Assignment Rule that specifies one or more Runtime Hosts, the rule associates events with the Runtime Application.
- You can add to the Application Assignment Rule condition by adding or removing Runtime event conditions. You may match conditions which have a different Runtime event attribute and are evaluated using AND. Those using the same Runtime event attribute are evaluated using OR. A typical Application Assignment Rule may examine a distributed group security event from an application by examining the request path event attribute.

When the Fortify Software Security Center receives a security event, the console sequentially evaluates Application Assignment Rules definitions for a match to a particular Runtime Host definition or application request path specifier.

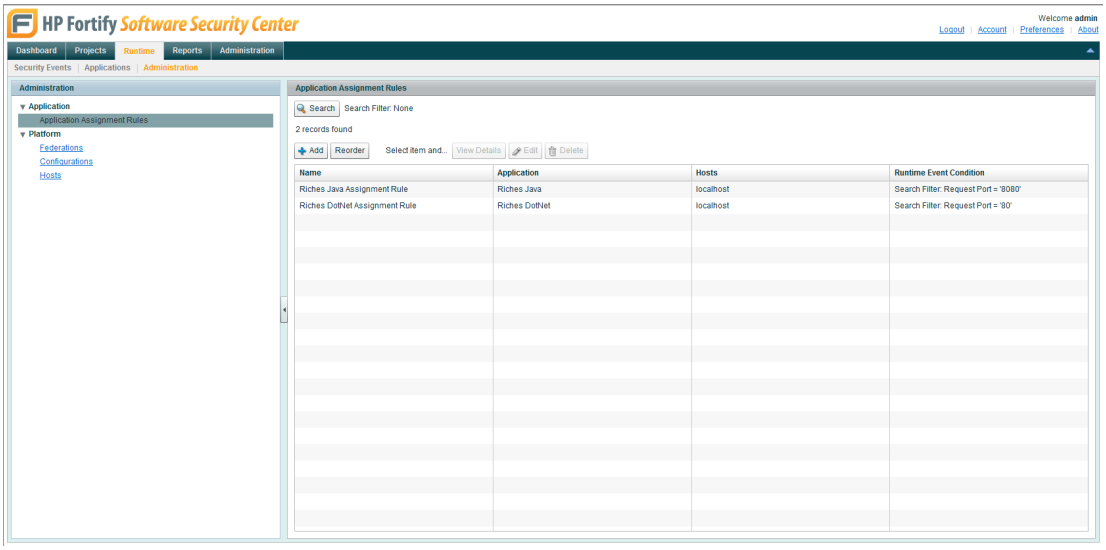
When the Fortify Software Security Center finds a match, the console stops evaluating Application Assignment Rules.

Creating an Application Assignment Rule

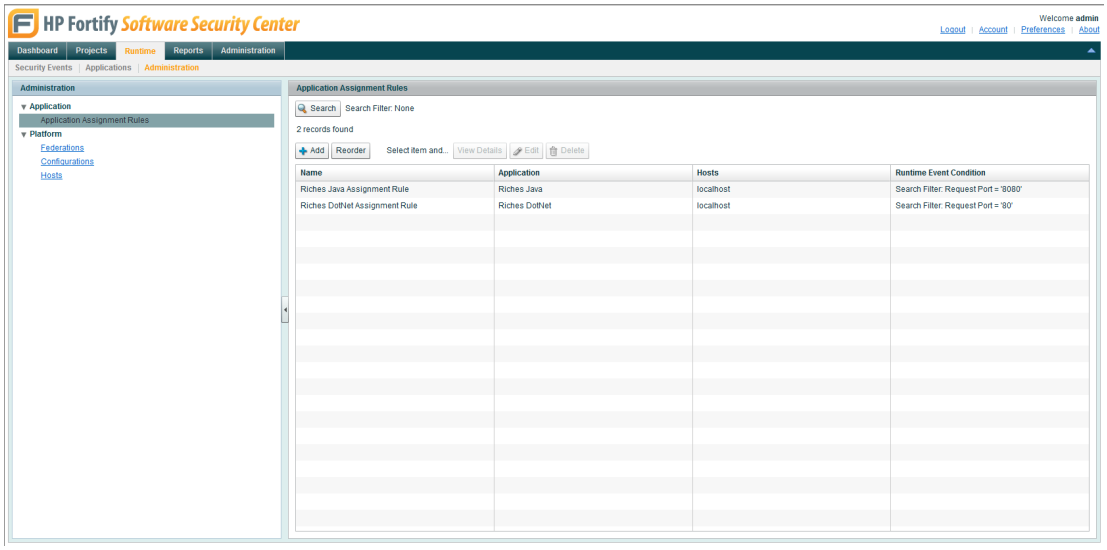
Perform the procedure in this section to create a new Application Assignment Rule.

To create a Runtime Application Assignment Rule:

1. Display the **Application Assignment Rules** page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to create or edit Application Assignment Rules.
   b. In the **Runtime** tab, click **Administration** then in the left side navigation pane click **Application Assignment Rules**.
   The Fortify Software Security Center displays the **Application Assignment Rules** page.



2. Create a new Application Assignment Rule. In the **Application Assignment Rules** page, click **Add**.
   The Fortify Software Security Center displays the **Create Application Assignment Rule** dialog box.



3. Configure the new Application Assignment Rule. In the **Create Application Assignment Rule** dialog box.
   - In the **Name** text entry area, type the name of the new Application Assignment Rule.
   - In the **Application** list, choose a Runtime Application.

   For information about Runtime Applications, see "About Creating and Managing Runtime Configurations" below.
4. Perform one or both of the following.
   - To create an Application Assignment Rule that associates RTAP security events with a Runtime Host, in the **Hosts** area, use the **Add** button to choose one or more Runtime Hosts.
   - To create an Application Assignment Rule condition by adding or removing Runtime Event conditions, use the request path area at the bottom of the Create Application Assignment Rule dialog box.

   After you supply all required information, the **Create Application Assignment Rule** dialog box enables the **Save** button.
5. Click **Save**.

About Creating and Managing Runtime Configurations

Use Runtime Configurations to manage the configuration settings used by a Runtime Federation.

Adding a New Runtime Configuration

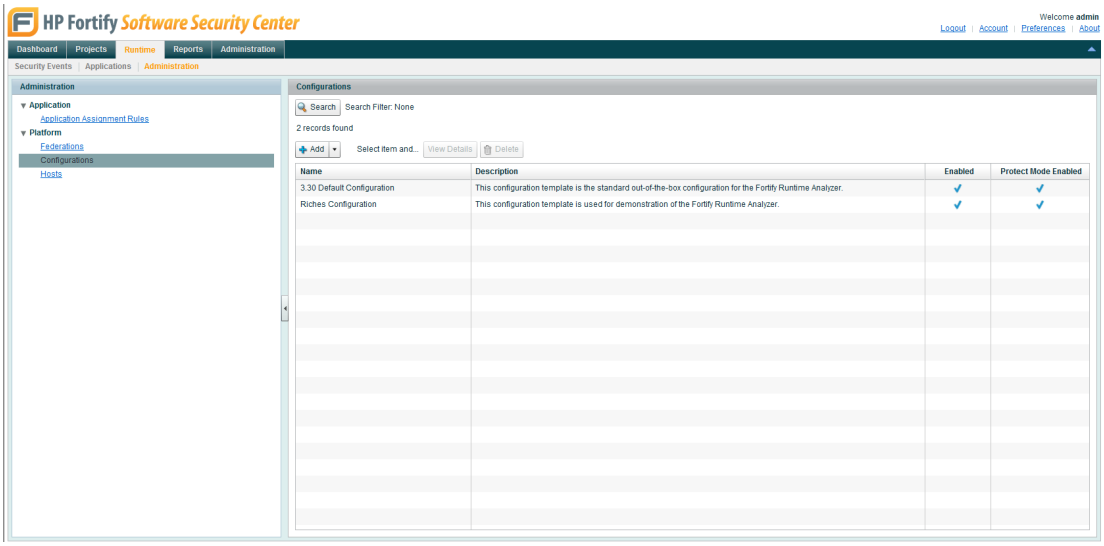
Perform the procedure in this section to add a new Runtime Configuration to Runtime's list of Configurations.

When you add a Runtime Configuration, you use an existing Runtime Configuration as a starting point for the new configuration, then customize the newly created configuration. The Fortify Software Security Center allows you to specify the existing Configuration in either of two ways:

- Clone an existing Runtime Configuration definition
- Upload a Configuration Template file (.xml filename extension)

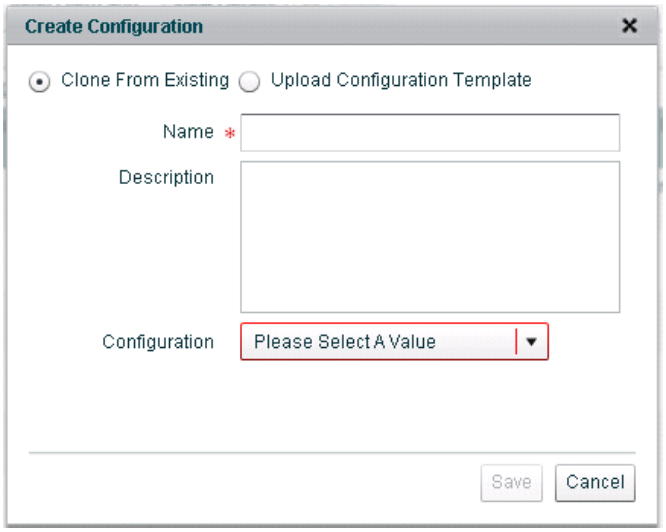
To create a Runtime Configuration:

1. Display the **Configurations** page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to create or edit Runtime Configurations.
   b. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Configurations**.
   The Fortify Software Security Center displays the Configurations page.

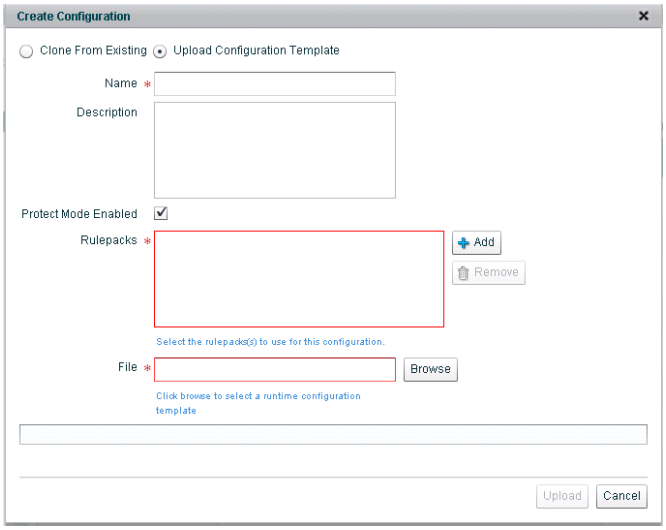


By default, the Fortify Software Security Center includes a non deletable default configuration named *HPE Security Fortify Runtime Configuration*. This ensures that there is always at least one Runtime Configuration to use as a starting point for a new configuration.

2. Create a new Configuration. In the Configurations page, click **Add**
   By default, the Fortify Software Security Center displays the Create Configuration dialog box's Clone from Existing dialog box.



3. To "clone" a copy of a an existing Runtime Configuration, in the **Create Configuration** dialog box:
   a. In the **Name** text entry area, type a name for the new Configuration instance.
   b. In the **Configuration** list, choose an existing configuration to clone.
   c. Click **Save**.
4. To create a Runtime Configuration by uploading a configuration template, select **Upload Configuration Template**.
   The Fortify Software Security Center displays the Create Configuration panel.



a. In the **Create Configuration** panel, in **Name** text entry area, type the name of the new configuration.
b. To make RTAP actively block detected attacks, select **Protect Mode** Enabled.
To log attacks but take no protective action, clear **Protect Mode Enabled**.
c. In the Rulepacks area, click **Add**, then select at least one Rulepack definition.
d. In the **File**area, click **Browse** then select a Runtime Configuration Template file (.xml filename extension).
You must specify a name, at least one Rulepack, and specify the location of a Runtime Configuration file to enable the Save button.
e. Click **Upload**.
The Fortify Software Security Center displays the Global Settings page.

5. At the top of the **Global Settings** page, click the **Configurations** link to return to the RTAP Configuration page.

About Configuration Templates

You can use the Fortify Software Security Center to export and import Runtime Configuration Templates as (.xml filename extension) files. They may be both uploaded and downloaded.

Configuration Templates:

- Provide the basis of the configuration the Federation controller sends to a Runtime Host.
- Provide a way to configure advanced Runtime features by enabling to download, edit, then editing the template's XML.

Uploading or Downloading a Runtime Configuration Template

To upload or download a Runtime Configuration Template:

1. Display the **Configuration Details** page.
   a. To upload a Configuration Template, log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to upload a Runtime Configuration Bundle.
   b. To download a Configuration Template, log on to Fortify Software Security Center with Administrator, Security Lead, or Manager privileges. You must have at least Manager privileges to download a Runtime Configuration Bundle.
   c. In the **Runtime** tab, click **Administration** then in the left side navigation pane click **Configurations**. The Fortify Software Security Center displays the Configurations page.
   d. In the **Configurations** page, in the list of Runtime Configurations select a configuration, then click **View Details**.
2. To upload the Configuration Template of the selected Runtime Configuration, in the top right of the configuration details page, click **Advanced** then choose **Upload Configuration Template**. Use the **Upload Configuration Template** dialog box to locate the XML file containing the Runtime Configuration Template.
3. To download the Configuration Template of the selected Runtime Configuration, in the top right of the page, click **Advanced** then choose **Download Configuration Template**. Use the **Select Location** dialog box to specify where to save the XML file containing the Runtime Configuration Template.

About Runtime Configuration Bundles

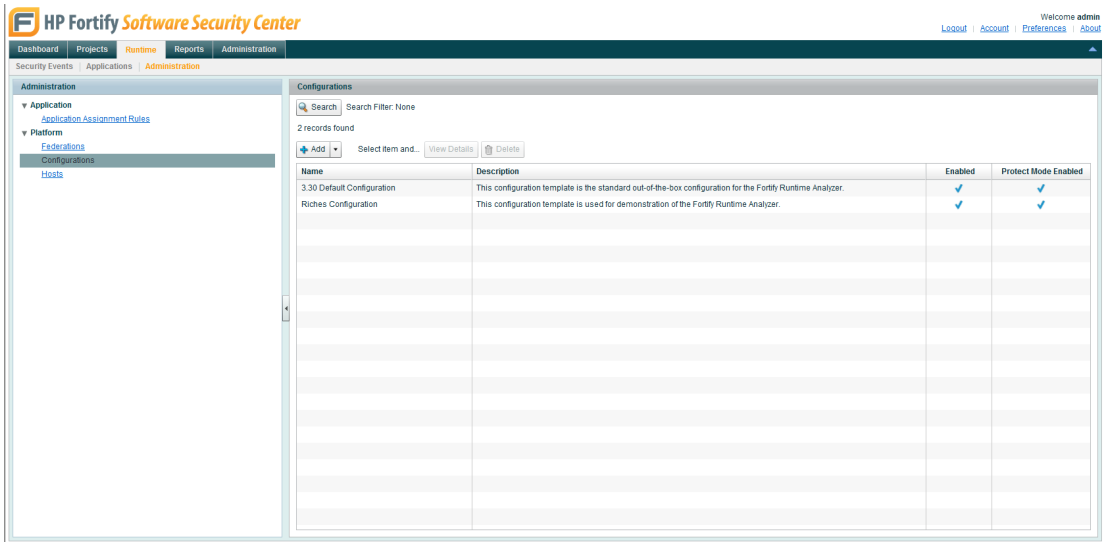
You can use the Fortify Software Security Center to export and import Runtime Configuration Bundles as a package (`.fpc` filename extension).

Configuration Bundles are completely self contained and thus portable. A given Configuration Bundle contains the complete set of global settings, rule packs, event handlers, general settings, and configuration information required to transfer a complete Runtime Configuration from one Fortify Software Security Center to another. Runtime configuration bundles may be imported and exported.

Exporting a Runtime Configuration Bundle

To export a Runtime Configuration Bundle:

1. Display the **Configuration Details** page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to export a Runtime Configuration Bundle.
   b. In the **Runtime** tab, click **Administration** then in the left side navigation pane click **Configurations**.
   The Fortify Software Security Center displays the **Configurations** page.
   c. In the **Configurations** page, in the list of Runtime Configurations select a configuration, then click **View** Details.
   The Fortify Software Security Center displays the **Configurations** page.



2. In the top right of the configuration details page, click Advanced then choose Export Configuration Bundle.
   Use the Select Location tool to choose the location and name of the exported Configuration Bundle as an FPC file.

Importing a Runtime Configuration Bundle

To import a Runtime Configuration Bundle:

1. Display the **Configuration Details** page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges.
      You must have at least Security Lead privileges to import a Runtime Configuration Bundle.
   b. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Configurations**.
      The Fortify Software Security Center displays the configuration details page.
2. Import the Configuration Bundle for the selected Runtime Configuration.
   In the **Configurations** page, click the **Add** drop down, then choose **Import Configuration Bundle**.

   Use the **Select Location** tool to choose the location and name of the exported Configuration Bundle as an FPC file.

About the Runtime Configuration's System-defined Settings

Fortify Software Security Center organizes Configuration system-defined settings into multiple tabs and pages.

The following table summarizes the System-defined configuration pages and describes the settings available on each of those pages.

System defined configuration settings

Settings Tab	Setting	Description
System Defined, General	Enable	Select Enable to enable RTAP. The Enable option provides a “master switch” for RTAP.
	Protect Mode Enabled	Select Protect Mode Enabled to enable protect mode. If Protect Mode Enable is selected, RTAP actively blocks attacks.
System Defined, Display	Display Default Forward Path	Specifies the default URL for the RTAP “Protected By” page
	Display Default HTML	Specifies the appearance of the HTML page located at Display Default Forward URL, described in the preceding table row.
	Display Default HTTP Status Code	Specifies the HTTP status code returned when RTAP displays the HTML page specified by Display Default Forward URL, described earlier in this table.
	Event Log file Max Size	Size threshold at which RTAP closes an event log file and begins a new file
	Log Default Picture	Default format of event log entries
	Syslog Server, Port	The URL and port number of an optional Syslog server. If no Syslog server and port are specified, then by default: • RTAP running in Standalone mode outputs security events to its event log • RTAP running in Federated mode outputs security events to its Federation controller. Default: No default value
	Syslog Default	Default Syslog event severity level Default: `error`

System defined configuration settings, continued

Settings Tab	Setting	Description
	Severity	
	Syslog Default Picture	Default format of Syslog entries.
	System Log File	Name of the log file where system messages are written If more than one concurrent Runtime process is configured to write to the same log file, the second process writes to `system1.log`, the third to `system2.log`, and so on. Default: `${FortifyHome}/log/system.log`
	System Log File Max Backups	Maximum number of system log file backups made before log data is overwritten Default: `9`
	System Log File Max Size	Maximum size of the system log file before moving log data to a backup For example, the first backup file will be named `system.log.1`, the second `system.log.2`, and so on. Default: `100MB`
	System Log Level	The minimum severity of system messages written to the log file Options are trace, debug, info, warn, error, and fatal. Default: `info`
	Event Log file Max Size	Size threshold at which RTAP closes an event log file and begins a new file

Editing a Runtime Configuration's System-defined Settings

To edit a Runtime Configuration's System defined settings:

1. Display the **Global Settings** page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to create or edit Configuration Settings.
   b. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Configurations**.
   The Fortify Software Security Center displays the Configurations page.

c. In the **Configurations** page, in the list of Configurations, select a configuration then click **View Details**.
By default, the Fortify Software Security Center displays the System Defined page for the configuration in the "System defined configuration settings" on page 53 table.

2. In the **System Defined** page, edit one or more System Defined Settings.
   a. Use the "System defined configuration settings" on page 53 table as a guide to selecting the tab (Global Settings, Rulepacks, Event Handlers, General) that provides access to the Configuration setting you want to modify.
   b. After selecting the appropriate Configuration tab, click **Edit**.
   c. After modifying the Configuration setting, click **Save**.

About Template Defined Configuration Settings

The Fortify Software Security Center provides single page access to the Runtime Configuration settings defined on that Configuration's Configuration Template.

The following table lists the default set of template defined configuration settings.

Default set of RTAP Template defined Configuration Settings

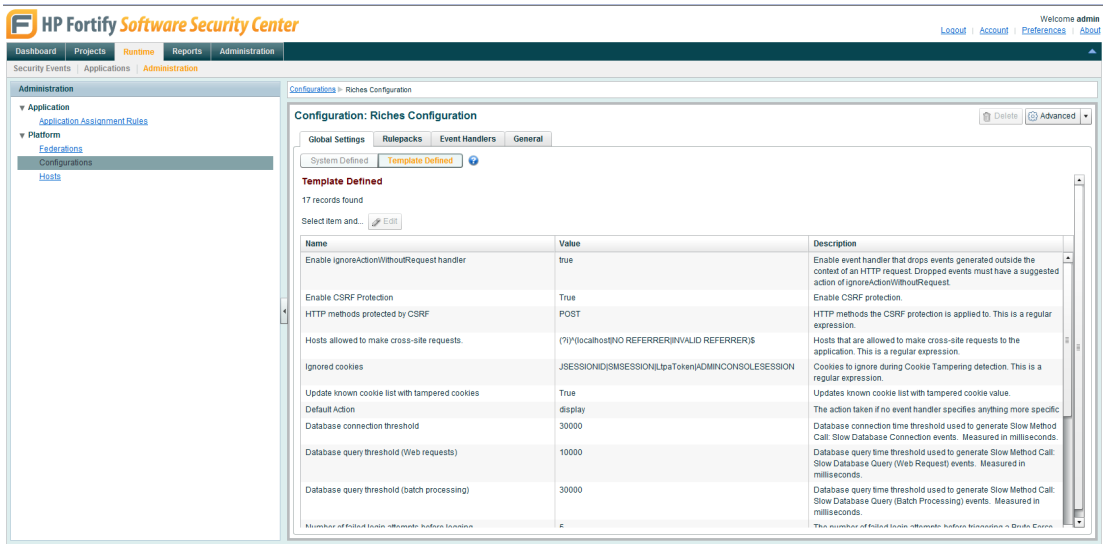
Template defined Setting	Description
disableCSRF	Disables CSRF protection.
CSRFProtectedMethods	A regular expression that specifies the HTTP methods RTAP applies to CSRF protection
CookieTampering IgnoredCookies	A regular expression that specifies the browser cookies ignored by RTAP during Cookie Tampering detection
CookieTampering UpdateWithTampered	Updates known cookie list with tampered cookie value
default_action	If no event handler specification exists, the default action taken by RTAP
DatabaseConnection TimeThreshold	The integer number of milliseconds before RTAP creates a `Slow Method Call: Slow Database Connection` events
WebSQLTimeThreshold	The integer number of milliseconds before RTAP creates a `Slow Method Call: Slow Database Query (Web Request)`event
SQLTimeThreshold	The integer number of milliseconds before RTAP creates a `Slow Method Call: Slow Database Query (Batch Processing)` event

Viewing or Editing a Configuration's Template Defined Settings

View or edit the Runtime Configuration's template defined settings to verify the configuration's settings and modify those settings.

To edit a Runtime Configuration's template defined settings:

1. Display the Global Settings page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to create or edit Template defined Configuration Settings.
   b. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Configurations**.
   Fortify Software Security Center displays the **Configurations** page.
   c. In the Configurations page, in the list of Configurations, select a configuration then click **View Details**.
   By default, Fortify Software Security Center displays the System Defined page for the configuration.
   d. In the **Configurations** page, select the **Template Defined** area.
   Fortify Software Security Center displays the Template Defined page for the configuration.



2. In the **Template Defined** page, edit one or more Template Defined settings by selecting a Template and clicking **Edit**.
3. After modifying the Configuration settings, click **Save**.

About Runtime Configuration Attributes

Fortify Software Security Center organizes Runtime Configuration attributes into multiple tabs and pages.

The following table summarizes the system defined configuration pages and describes the settings available on each of those pages.

Settings Tab	Setting	Description
Rulepacks	Add / View / Remove	Use to view and manage RTAP Rulepacks.
Event Handlers	Add / Edit / Delete	For more information about Event Handlers, see "Managing a Configuration's Event Handlers" on page 37.
General	Edit Name / Description	View or edit the selected Configuration's Name or Description text entry areas.

Adding Runtime Rulepacks to a Configuration

You can add Runtime Rulepacks that have been defined to Fortify Software Security Center.

To add a Rulepack to a configuration:

1. Display the **Rulepacks** page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges. You must have at least Security Lead privileges to add Rulepacks to a configuration.
   b. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Configurations**.
   Fortify Software Security Center displays the **Configurations** page.
   c. In the **Configurations** page, in the list of Configurations, select a configuration then click **View Details**.
   By default, the Fortify Software Security Center displays the **System Defined Settings** page for the configuration.
2. In the **Configurations** page, click **Rulepack**, then click **Add**.
   Fortify Software Security Center displays the **Add Rulepacks** dialog box. The dialog box lists the Rulepacks that can be added to the selected Runtime Configuration.
3. In the **Add Rulepack** dialog box, in the list of Rulepacks select one or more Rulepacks then click **Save**.
   Fortify Software Security Center adds the Rulepacks to the configuration.

Viewing Host Configuration Settings

The Fortify Software Security Center provides single page access to a Runtime Host Configuration's settings. This enables you to review or troubleshoot the configuration be sent to the Host.

To view a Host Configuration:

1. Display the **Global Settings** page.
   a. To upload a Configuration Template, log on to Fortify Software Security Center with Administrator, Security Lead, or Manager privileges.
   You must have at least Manager privileges to view a Runtime Host Configuration.
   b. In the **Runtime** tab, click **Administration** then in the left side navigation pane click Configurations. Fortify Software Security Center displays the **Configurations** page.
   c. In the **Configurations** page, in the list of Runtime Configurations select a configuration, then click **View Details**.
   Fortify Software Security Center displays the Global Settings page for the configuration.
2. To view the Host Configuration, in the top right of the **Global Settings** page, click **Advanced**, and then choose **View Host Configuration**.
   Fortify Software Security Center displays the View Host Configuration panel.

About Runtime Federations

A Federation is a group of Runtime Hosts that share the same configuration.

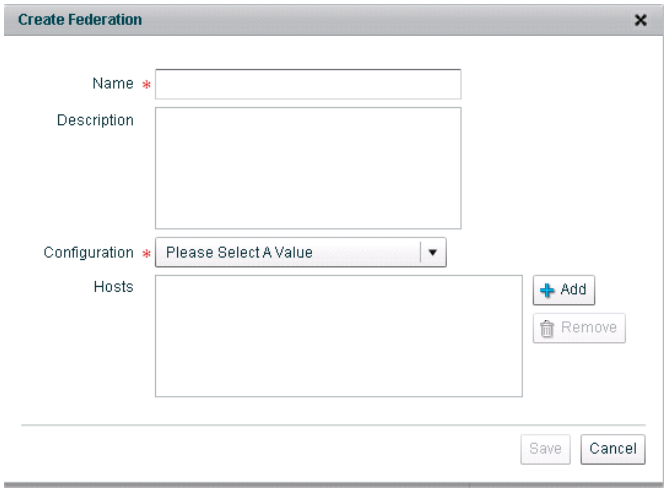
By definition, Federated mode means that RTAP receives its configuration (and reports its security events) to a Runtime Host running in an instance of Fortify Software Security Center.

A Runtime Host can belong to only one Runtime Federation.

Adding a New Runtime Federation

To add a Runtime Federation:

1. Display the **Federations** page.
   a. Log on to Fortify Software Security Center with Administrator or Security Lead privileges.
   You must have at least Security Lead privileges to create or edit Runtime Federations.
   b. In the **Runtime** tab, click **Administration**, and then in the left side navigation pane click **Federations**.
   Fortify Software Security Center displays the Federations page.
2. Create a new Federation. In the **Federations** page, click **Add**.
   Fortify Software Security Center displays the Create Federation dialog box.



3. Configure the new Federation. In the **Create Federation** dialog box:
   a. In the **Name** text entry area, type the name of the new Federation.
   b. In the **Configuration** area, choose the Runtime Configuration definition that the Fortify Software Security Center will apply to all Runtime Hosts in this Federation.
   You must specify a name and a configuration to enable the **Save** button.
   c. In the **Hosts** area, click **Add** then add one or more Hosts to the new Federation.
   You can use the Federation page's **Edit** button to add additional hosts to an existing Runtime Federation.
   d. Click **Save**.
   Fortify Software Security Center displays the new Federation's details page.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Operator Guide (HPE Security Fortify Runtime Application Protection 17.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to HPFortifyTechpubs@hpe.com.

We appreciate your feedback!