dotDefender v4.2

User Guide

Applicure Web Application Firewall

Table of Contents

1

Introduction

This chapter introduces the Applicure dotDefender application. It contains the following sections:

1.1 Overview

dotDefender is a software-based Web Application Firewall installed on Apache or Microsoft IIS Server. dotDefender provides robust protection against attacks targeting Web applications. dotDefender utilizes multiple security engines to achieve optimal protection:

- Pattern Recognition: This engine uses rules to detect certain patterns that could indicate an attack and deals with the attack according to configuration.
- Session Protection: The Session Protection engine focuses on the user session level, dealing with session spoofing and flooding of the server with HTTP requests (Denial of Service).
- Signature Knowledgebase: This engine uses signatures to detect known attacks, such as vulnerability scanners, bots, site-scrapers, email harvesters, and leeches.
- Malicious File Upload: Protects upload folders on the server against malicious file uploads.
- Server Masking & Information Leakage: Camouflages server and application against sensitive information leakage.

1.2 Components

dotDefender includes the following applications:

- Administration Console - Enables you to configure and manage dotDefender:
  - Global Settings (see **Configuring Global Settings**)

- Session Protection (see **Configuring Session Protection**)
- Website Security Profiles (see **Configuring Website Security Profiles**)
- Upload Folders Protection (see **Upload Folders Protection**)
- Outgoing (egress) Inspection (see **Preventing Information Leakage**)
- Patterns and Signatures (see **Configuring Patterns and Signatures**)

- Logs (see **Managing Logs**).
  - Log Viewer - Displays information about detected attacks, such as originating IP, timestamp, type of attack, and target locations (see **Managing Logs**).

1.2.1 Specific Windows components

dotDefender writes security events to the following file:

- **aclogsvc.ddb**. Typically located in: C:\Program Files\Applicure\dotDefender for IIS\etc\

dotDefender adds the following branches to the Windows Event log:

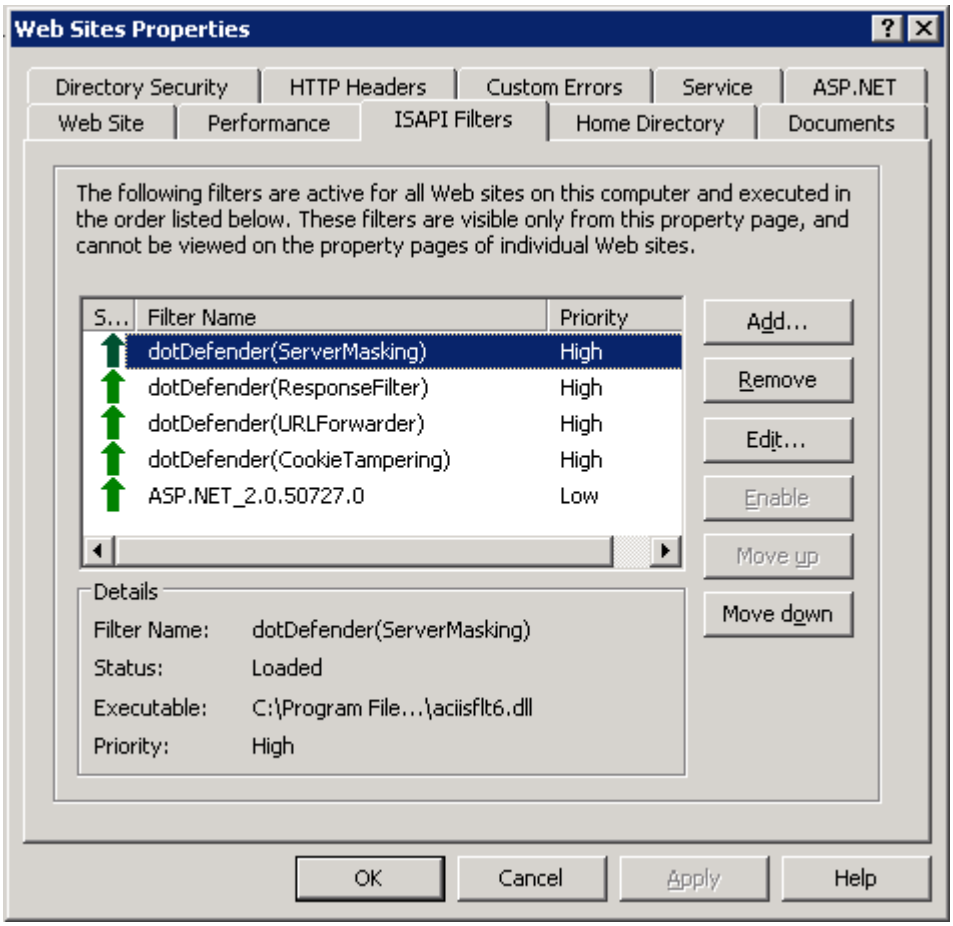
- **Applicure:** Records security events.
- **dotDefender Audit:** Records dotDefender ISAPI filter status.

dotDefender comprises the following services:

- **dotDefender Audit Service:** Watchdog that polls the filters and writes their current status.
- **dotDefender Log Service:** Manages the logs.

dotDefender installs the following ISAPI filters:

- dotDefender(ServerMasking)
- dotDefender(ResponseFilter)
- dotDefender(URLForwarder)
- dotDefender(CookieTampering)



1.2.2 Specific Linux components

dotDefender writes security events to the following file:

- **dotDefender_db.sqlite**. Located in: /usr/local/APPCure/log/

dotDefender comprises the following daemons:

- **dotDefender License daemon:** Manages the license.
- **dotDefender Log daemon:** Manages the logs.

dotDefender installs the following module:

- **dotDefender Apache module**

1.3 Benefits

dotDefender provides the following features and benefits:

- Lightweight and non-intrusive.
- Detailed verbose logs, yet enabling you to see the big picture.

- Cross-platform IIS and Apache.
- Centrally managed.
- Rapidly deployed and minimal maintenance required.
- Scalable and suited to shared hosting environments.
- Full-blown Web Services API.

1.4 Organization of this Guide

This guide provides the installation and operation instructions for dotDefender, and serves as a resource for types of web attacks and troubleshooting procedures.
It is composed of the following chapters:

- **Chapter 1 - Introduction** (this chapter), introduces dotDefender.
- **Chapter 2 - Getting Started**, describes the system requirements, download and installation process, how to stop and start dotDefender and the typical dotDefender workflow.
- **Chapter 3 - Managing Logs**, describes the types of logs, the log settings and how to view logs. It also discusses the handling of false positives.
- **Chapter 4 – Preventing Information Leakage**, describes how dotDefender protects your sensitive data from proliferation.
- **Chapter 5 - Configuring Website Security Profiles**, describes how to configure the Website profiles.
- **Chapter 6 - Configuring Patterns and Signatures**, describes how to configure the Patterns and Signatures, and how to update them.
- **Chapter 7 - Configuring Global Settings**, describes how to configure server wide settings.
- **Chapter 8 - FAQs and Troubleshooting**, details a variety of frequently asked questions and troubleshooting information.
- **Chapter 9 - Regular Expressions,** a brief tutorial on writing Regular Expressions.
- **Chapter 10 – Appendix**, Operating System specific files and features

2

Getting Started

This chapter contains the following sections:

2.1 Using the Administration Console

This section describes how to access the Administration Console and the toolbar. For additional information about the Administration Console, see Configuring Website Security Profiles.

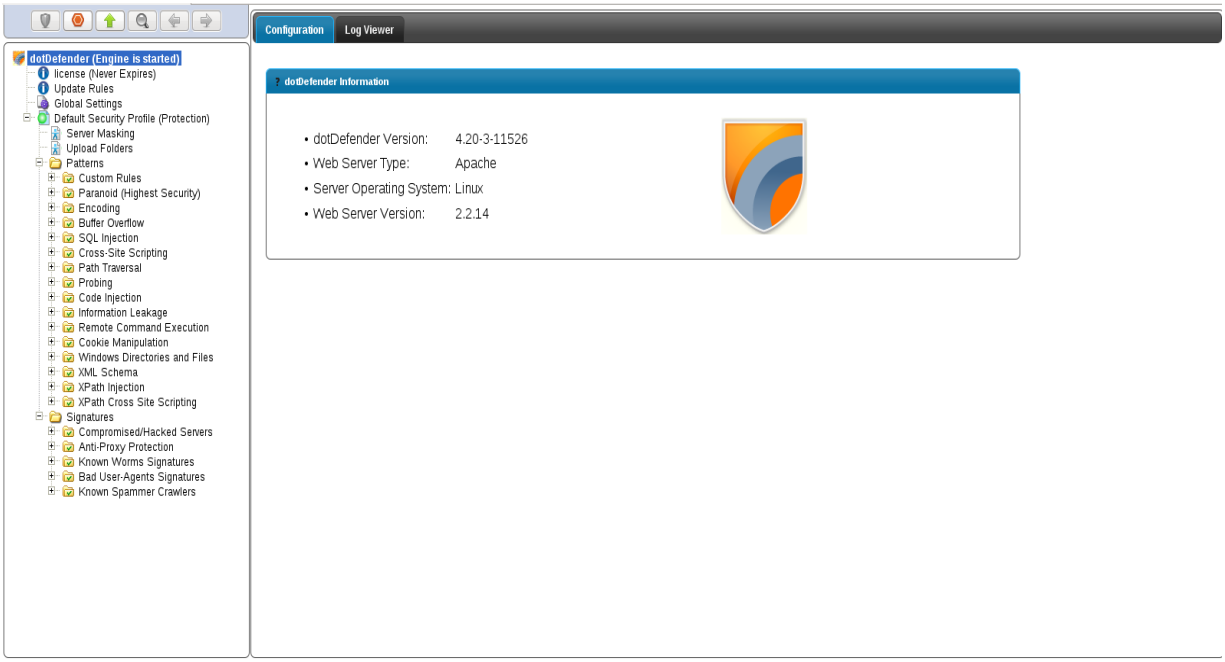
Linux/Unix: In the installation process, an alias is created in the Apache configuration file. The dotDefender Administration Console will be accessible through all sites at the Alias specified in the installation process.

Windows: In the installation process, a virtual directory is created in the Default Website. The dotDefender Administration Console will be accessible at the Default Website under the dotDefender directory. To modify the virtual directory location, or create the directory manually, see **Manually creating dotDefender virtual directory**.

To access the Administration Console:

- **Linux/Unix:** Browse to **http://Any_Site_On_Server/Alias/** (Default user name is 'admin'. Password is created in the installation process)
- **Windows:** Browse to **http://Default_site/dotDefender/**

Note: If the dotDefender Administration Console is not accessible, browse to the file **dotDefender.html** in the dotDefender/Alias directory



The dotDefender Administration Console window appears. The left pane shows a tree structure where you can select various branches.

The right pane shows configuration options for each branch. The following icons appear in the top toolbar:

Icon	Function
	Applies changes
	Starts dotDefender
	Stops dotDefender
	Opens the Log Viewer
	Go to previous page
	Go to next page

2.2 Stopping and Starting dotDefender

By default, dotDefender is active immediately upon installation (assuming that you have loaded a valid license). All websites and applications on the server are identified and assigned the **Default Security Profile** setting. The default **Operation Mode** setting is **Protection**, and thus active protection is applied to all websites configured on the Web server. There may be some occasions where you need to stop dotDefender.

Note: When dotDefender stops, it becomes inactive on the Web server where it is installed. Consequently, dotDefender does not perform application protection. When disabled, dotDefender does not use server resources and does not affect server performance.

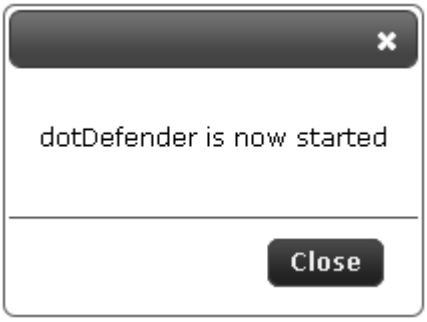
To stop dotDefender:

- Click  in the dotDefender toolbar. The following window appears.

- Click **Close**.
- dotDefender is deactivated as indicated by the grayed-out Stop button:

To start dotDefender:

- Click  in the dotDefender toolbar. The following window appears.



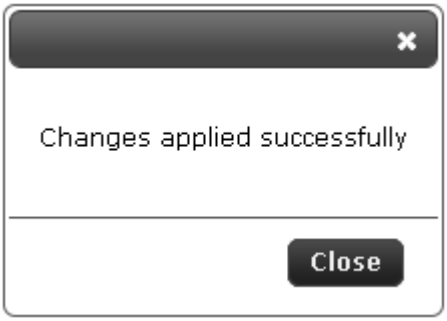
- Click **OK**. dotDefender is now active.

2.3 Applying Changes

If you modify settings in the Administration Console, the modifications will take effect only after applying the changes.

To apply changes:

- Click  in the dotDefender toolbar.
- A pop-up message confirms successful submission of the settings.

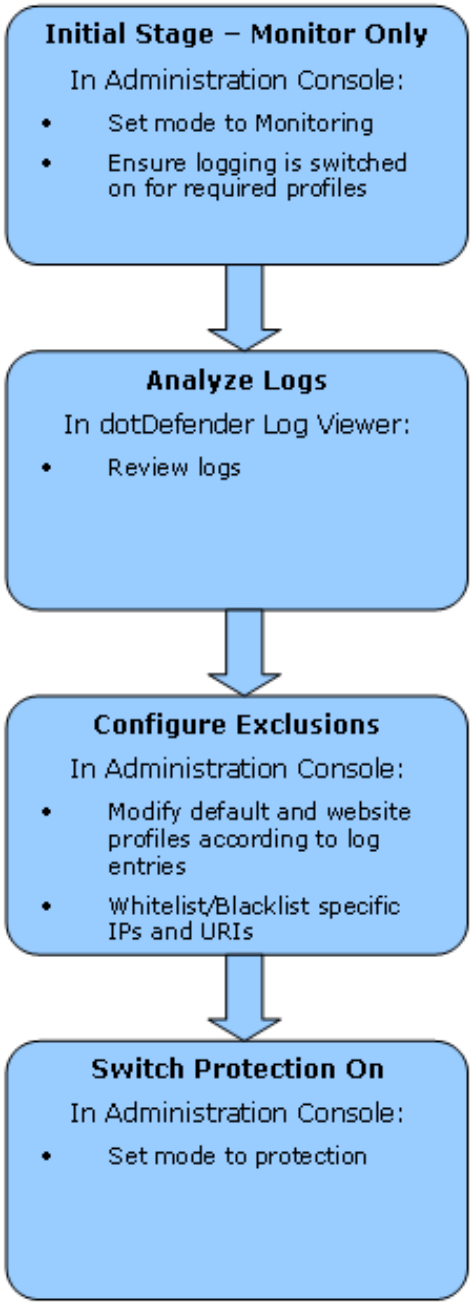


- Click **Close**.

Note: If you do not apply the changes and close the Administration Console, the new settings will be ignored and deleted.

2.4 Workflow

The following workflow is recommended:



It is recommended that you initially use dotDefender with the default settings. In the Administration Console, set the mode to **Monitoring** and ensure that the dotDefender log is enabled.
Allow dotDefender to run in **Monitoring** stage for 3-6 days, depends on the traffic.
After time has elapsed, analyze the logs. If you believe that the cause of a triggered alert is a legitimate application activity, follow the instructions in **Identifying False Positives.**
In the Administration Console, set the mode to **Protection**.
This is an iterative process. Continue to monitor logs and **Reference IDs** received by the users on an ongoing basis, and make the necessary adjustments to the configuration.

3

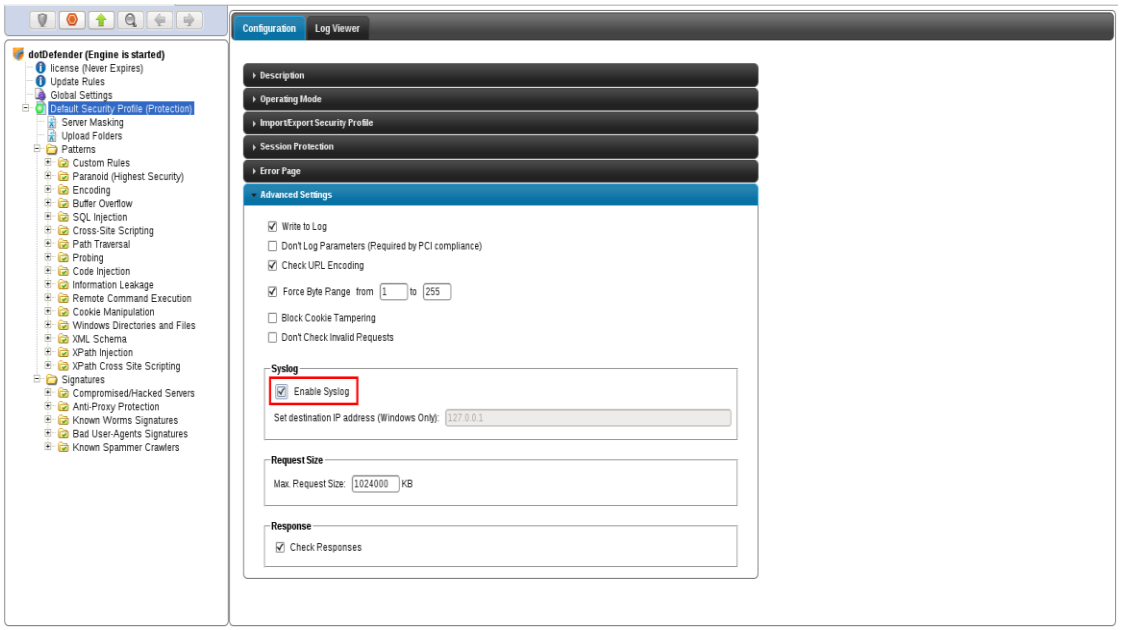
Managing Logs & Alerts

This chapter contains the following sections:

3.1 Configuring Syslog Alerts

In order to configure Syslog alert sending on dotDefender:

- Under the **Configuration** tab, select the relevant website profile for which you require Syslog alerts
- In the right-hand side pane, select **Advanced Settings**
- Check the **Syslog** checkbox
- Fill in the Syslog server IP address under **Set destination IP address**
- Click the "Apply Changes" button



Note: **Set Destination IP address** is to be used from WINDOWS machine (on which dotDefender is installed) to another WINDOWS machine.

dotDefender on Linux machine: Events will be written to LOCAL Syslog.

3.2 Log Overview

There are three types of logs:

- **Applicure log database:** Security events, viewed in the dotDefender Log Viewer.

- **Policy change log:** Records all changes made to policies via the Administration Console
- (Windows only): Events logged in two branches in the Windows Event Viewer:
  - **Applicure:** Records security events.
  - **dotDefenderAudit:** Records dotDefender filter status.

3.3 Viewing policy changes in the audit log file

The changes made via dotDefender Administration Console are recorded in detail, according to the PCI regulation, within tab-separated audit log files.
Windows:

- "submit.log" contains the most recent change made
- "submit.bak" contains the last 1000 changes.

Linux:

- audit.log

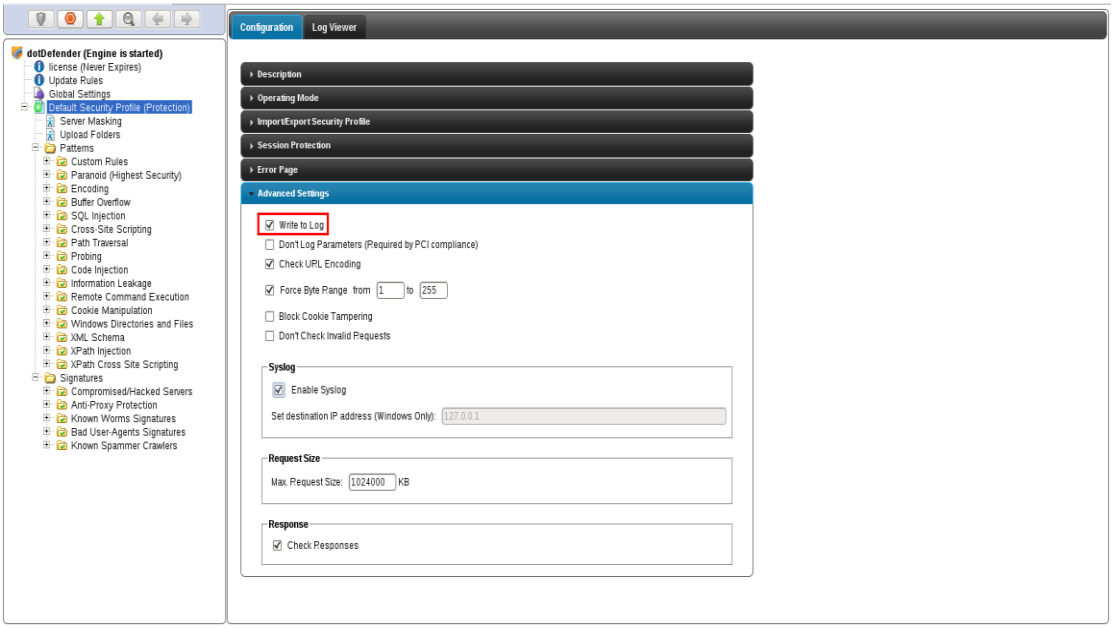
The files may be viewed under the following location:
Windows: \Program Files\Applicure\dotDefender for IIS\etc
Linux/Unix: /usr/local/APPCure/log/

3.4 Configuring the dotDefender Log Database

You can enable/disable the log for all of the websites using the Default Security Profile, and separately for each wbsite that does not use the Default Security Profile.
Windows: The **aclogsvc.ddb** log file is located in the following folder:
\Program Files\Applicure\dotDefender for IIS\etc
Linux/Unix: The **dotDefender_db.sqlite** log file is located in the following directory:
/usr/local/APPCure/etc
This file has a default maximum of 60,000 events for Linux/Unix and 15,000 event for Windows. This value is user-definable. A user-configurable threshold size can trigger a user-defined action (see **How do I change the database size limit?**).The database can be copied or moved to a different location and opened in the Log Viewer.

To enable the log for the websites using the Default Security Profile:

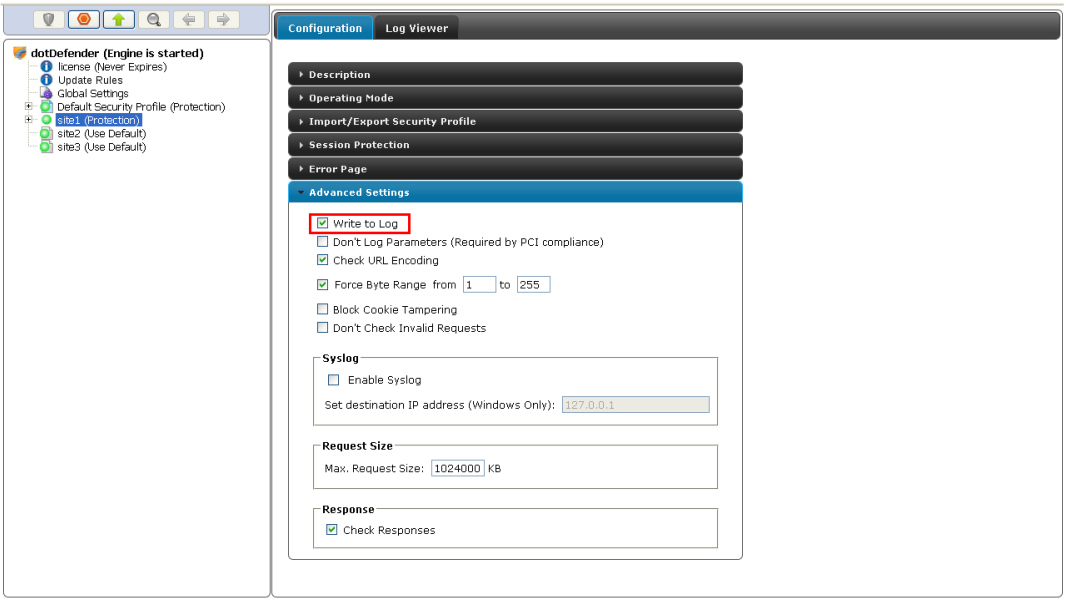
In the left pane of the Administration Console, select **Default Security Profile**. The profile settings appear in the right pane.



1. Expand the **Advanced Settings** section.
2. Select the **Write to Log** option to enable logging for all websites that use the Default Security Profile.
3. Click  to apply the changes.

To enable the log for a Website not using the Default Security Profile:

In the left pane of the Administration Console, select required **Website Security Profile**. The right pane opens the profile settings area.



1. Expand the **Advanced Settings** area.
2. Select the **Write to Log** option to enable logging for this Website.
3. Click  to apply the changes.

3.5 Viewing the dotDefender Log Database in the Log Viewer

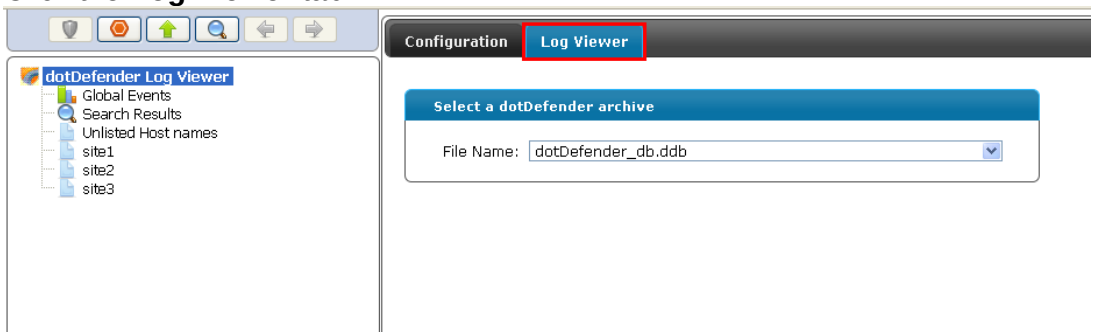
The Log Viewer displays information about countered attacks. You can drill down for more detailed information.
This section includes the following sections:

- Opening the Log Viewer
- Filtering the Log
- Searching for an Event
- Deleting the dotDefender Log Database File

3.5.1 Opening the Log Viewer

To open the Log Viewer:

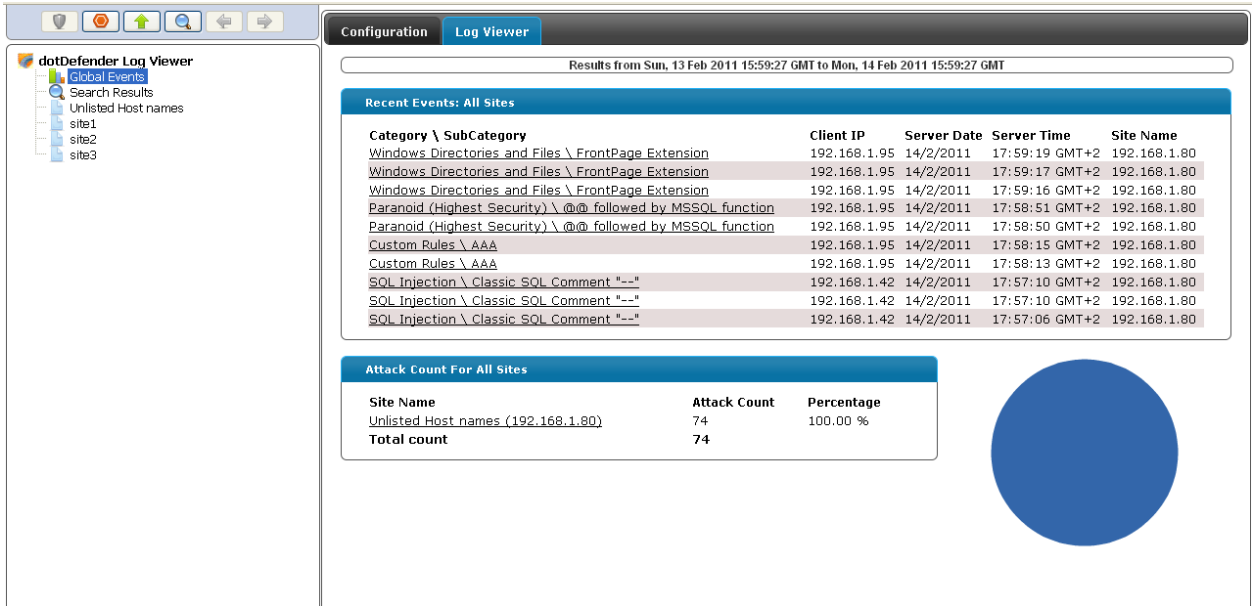
- Click the **Log Viewer** tab.



The Log Viewer window appears.

Select a site in the left pane to see site specific events or select Global Events to see all events for the server.

The log shows results for blocked sites, which are displayed in two lists: Recent Events for all sites and Total Attack Count for all sites.



Note: Ensure that you are viewing the results for the correct dates. For additional information, see **Viewing the dotDefender Log**.

The following icons are available on the Log Viewer toolbar:

Icon	Function
	Previous view
	Next view
	Search for events

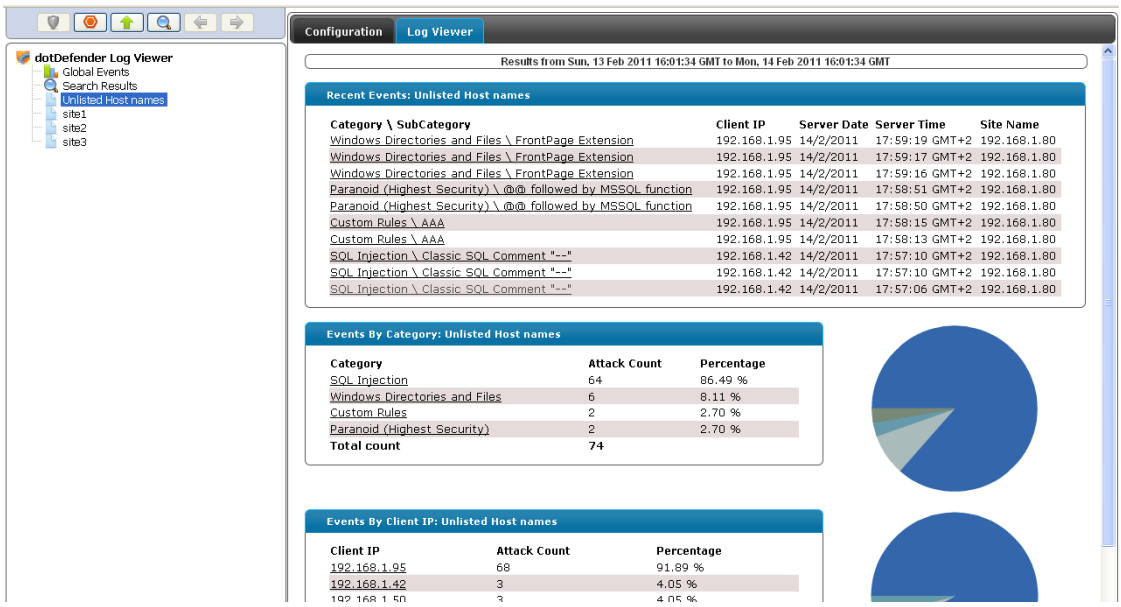
3.5.2 Filtering the Log

You can filter the view for countered attacks per site or view all sites.

To filter the log:

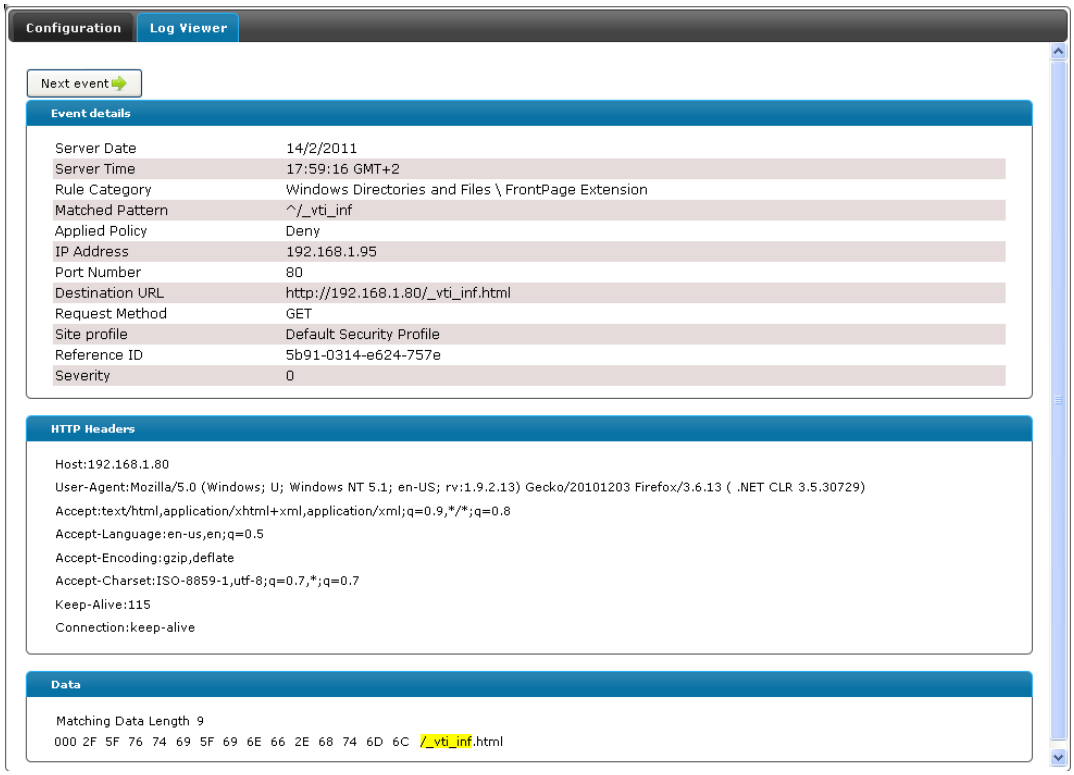
In the Log Viewer window, under each security profile in the left pane, click one of the following:

- **Events by category**: To view all attack categories for a specific site.
- **Events by IP Address**: To view all client IP addresses which were blocked by dotDefender.



- To drill down and filter for greater detail, click one of the following:
  - A specific category
  - A specific client IP address

- Click a specific event to display event details.



The following table describes the event details:

Name	Description
Date	The date of the event.
Time	The time when the event occurred.
Rule Category	Attack category and sub-category intercepted. See **Configuring Patterns and Signatures**.
Matched Pattern	The pattern matching the rule that detected the attack. See **Adding User-Defined Rules**.
Applied Policy	**Deny**: dotDefender denied this HTTP request. **Allow**: dotDefender stopped checking the HTTP request, and allowed it to reach the server. **Pass**: dotDefender skipped this rule and continued inspection using the rest of the rules.
IP Address	The source IP address of the request sender.
Port Number	Port number of the request sender.
Destination URL	The URL targeted by the sender.
Request Method	HTTP method, such as GET, POST, HEAD.

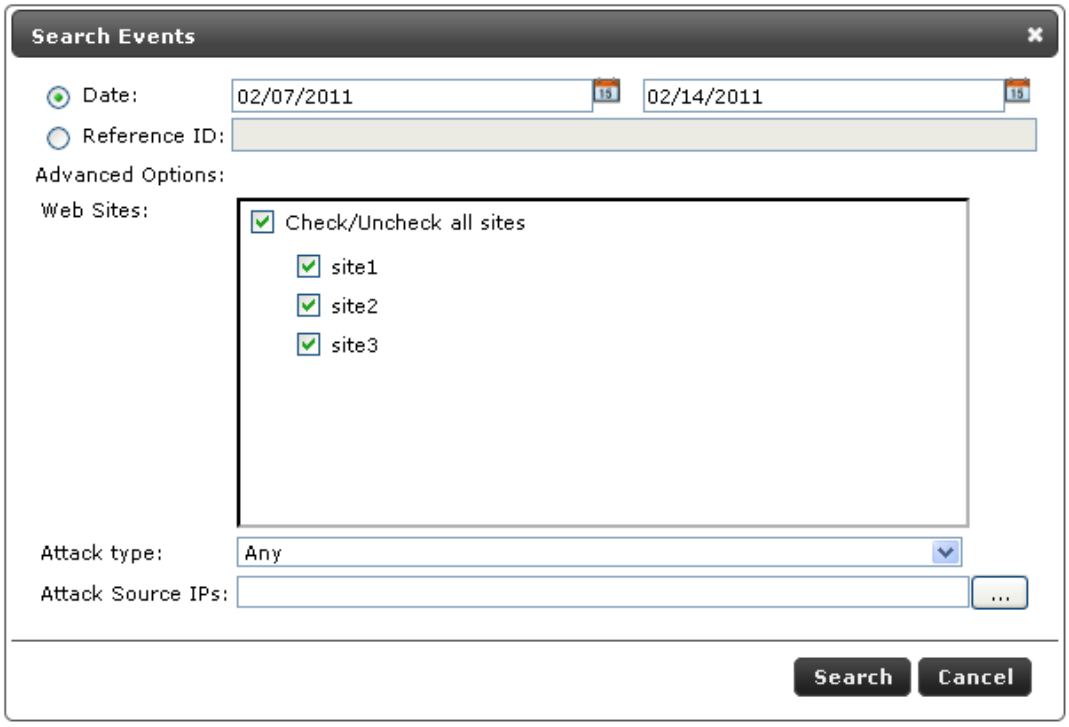
Name	Description
Site profile	The security profile of the website.
Reference ID	Unique identifier of the event (see **Configuring the Error Page**).
Severity	Attack severity level from 0 to 100.
HTTP Headers	Details of the HTTP Headers of the HTTP request.
Matching Data Length	The hex dump of the string as it was captured on the wire. The matching substring that triggered the alert is highlighted in yellow.

3.5.3 Searching for an Event

When troubleshooting, you may want to search for a specific event according to the key characteristics of the attack, such as Date, Reference ID, or Attack Category.

To search for an event:

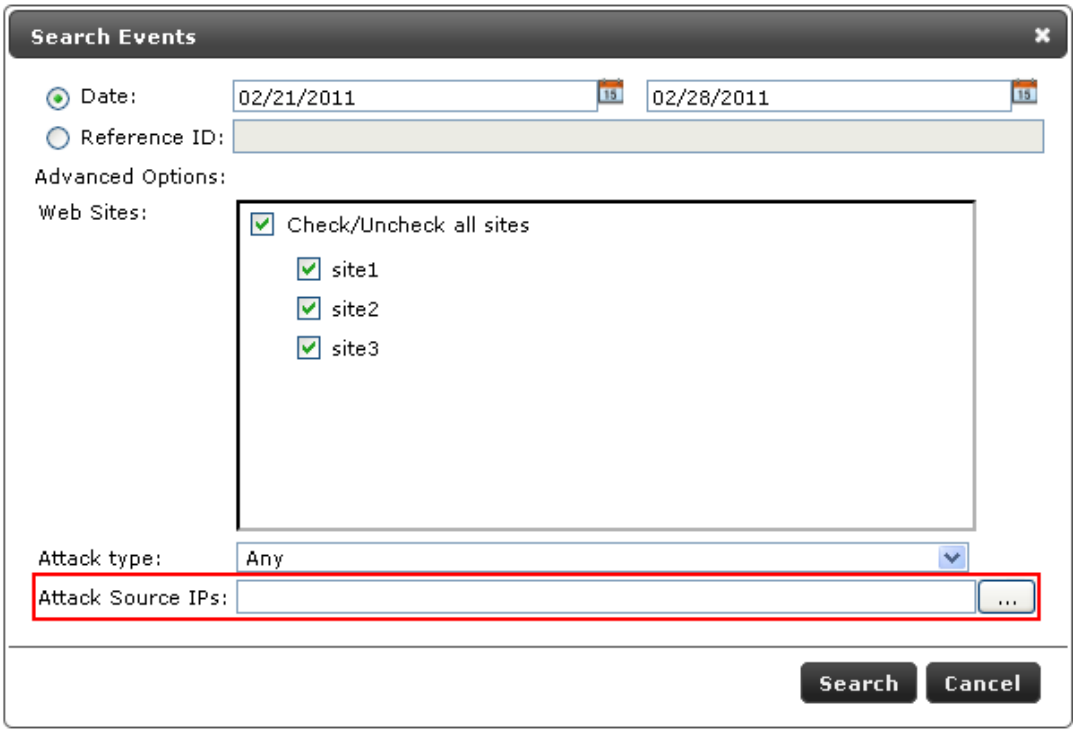
1. Click the **Search** icon  in the Log Viewer. The Search window appears.

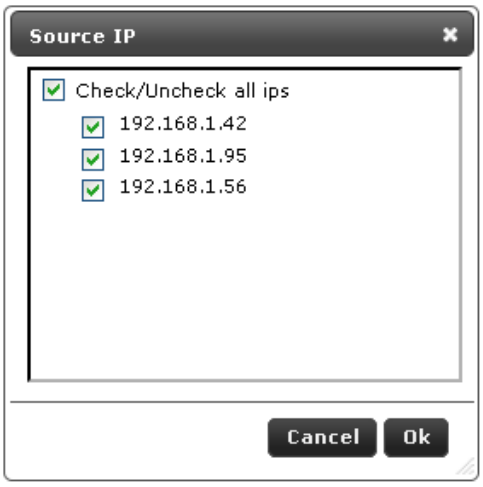


2. Set one or more of the search criteria as follows:

- Select **Date**, and select the Date range from the drop-down calendars.
- Select **Reference ID**, and enter the Reference ID you received on the Error Page (see **Configuring the Error Page**)
- In the **Advanced options** area, select Web Server or Website.

- From the **Attack type** drop-down list, select one of the recorded attack types.
- In the **Attack Source IPs** area, click ... to select an IP address from the list of IP addresses that have been logged.





- Click **Search**.

3.5.4 Backing Up the dotDefender Event Database (Windows)

To backup the dotDefender Event Database, you can do one or both of the following:

3.5.4.1 Backup dotDefender Event Database

- Stop the **dotDefender Log Service.**
- Copy the file:
  C:\Program Files\Applicure\dotDefender for IIS\etc\aclogsvc.ddb
  to a backup location of your choosing.
- Start the **dotDefender Log Service.**

3.5.4.2 Backup dotDefender Event log from the Windows Event Viewer

- Open the Windows Event Viewer
- Right click the Applicure branch
- Select "**Save log file as...**"
- Save in a backup location of your choosing.

Note: The dotDefender Log Viewer can only open event databases (*.ddb files).

To move the dotDefender log database file

- Stop the **dotDefender Log Service**.
- Copy or move the **aclogsvc.ddb** log file located in the following folder:
  \Program Files\Applicure\dotDefender for IIS\etc
- Start the **dotDefender Log Service**.
- The Log Service initializes. If the old event database has been deleted, a new database will be automatically generated

3.5.5 Backing Up the dotDefender Event Database (Linux)

To backup the dotDefender Event Database, copy the file
/usr/local/APPCure/log/dotDefender_db.ddb

3.5.6 Backup of dotDefender configuration/rules (Linux)

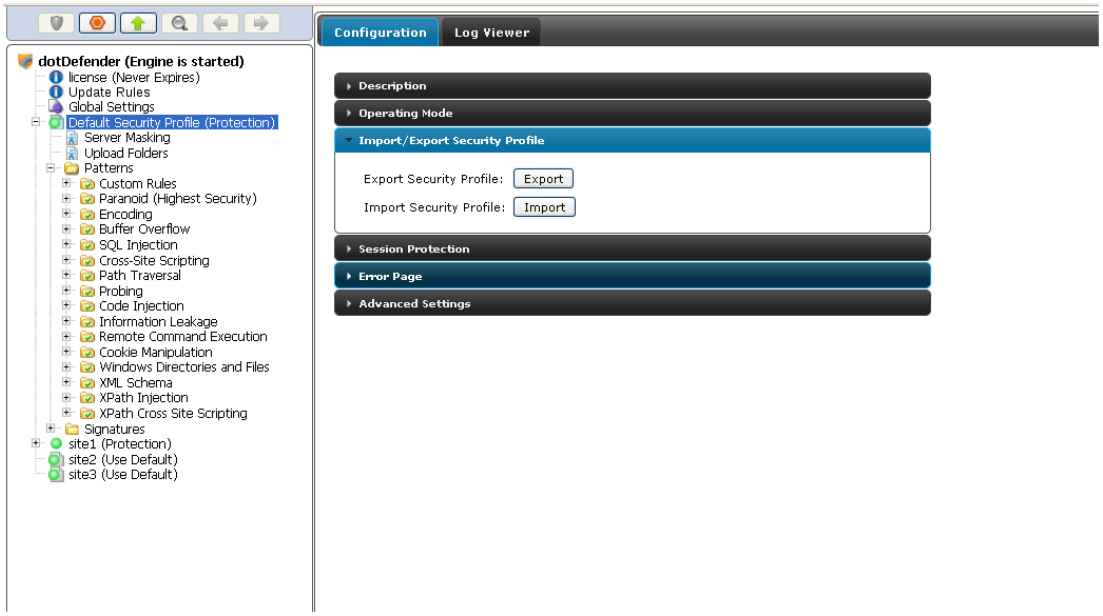
There are two methods for dotDefender configuration backup

1. Export security profiles to XML files
2. Backup dotDefender files

- **To export security profiles to XML files**

Select a security profile.

On the right pane, in the **Import/Export Security Profile** section, click the Export button.



Save the XML file to a backup location.

Follow this procedure to each security profile to backup.

- **To backup configuration via file backup**

Backup the directory /usr/local/APPCure/

3.5.7 Backup of dotDefender Configuration/rules (Windows)

There are two methods for dotDefender configuration backup:

1. Export security profiles to XML files
2. Backup registry keys and files

- **To backup the dotDefender configuration via registry and file backup:**

1. Open the Windows registry
2. Browse to the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Applicure

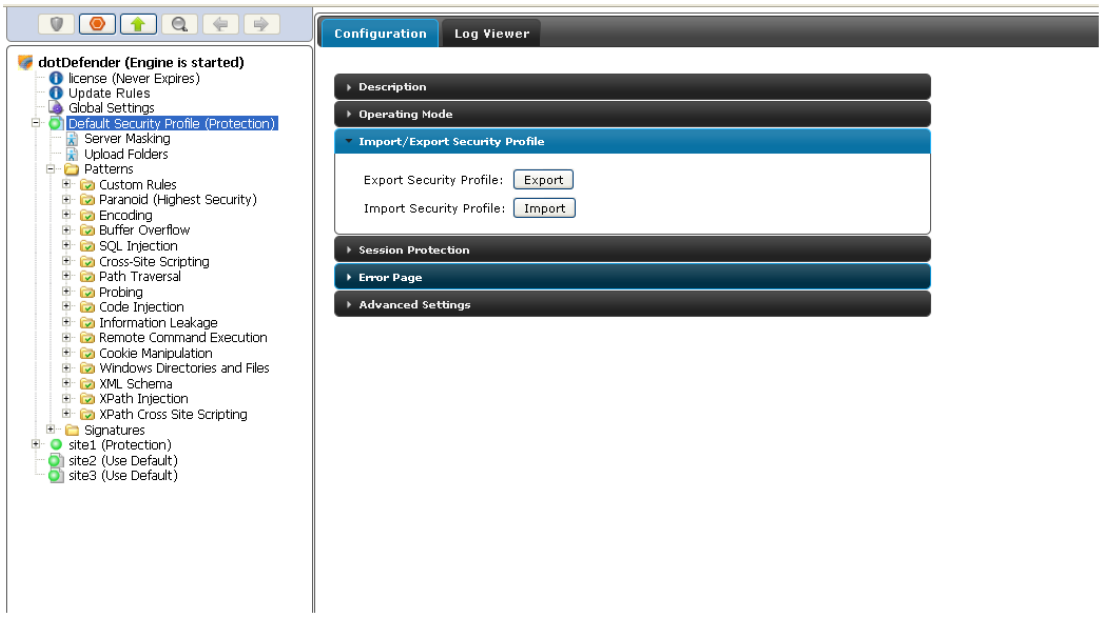
3. Right click the key, select Export and save in a backup location

4. Backup the Applicure directory, typically located in C:\Program Files\Applicure\

To backup security profiles to XML files

Select a security profile.

On the right pane, in the **Import/Export Security Profile** section, click the Export button.



Save the XML file to a backup location.

Follow this procedure to each security profile to backup.

3.6 Identifying False Positives

The Website administrator may need to customize dotDefender. As Web applications tend to differ in the way they are designed, some activities may appear as attacks and be blocked as a result of dotDefender's default rule settings, even though they originate from valid and legitimate sites. You can use the Reference ID (RID) on the Error Page as a filter in your search in order to find the required request.
dotDefender customization enables users to investigate and identify the security problem via the Log Viewer or Event Log. You can then modify the Default Security Profile or Website Security Profiles and create user-defined rules for Patterns, or configure Signatures: see **Configuring Patterns and Signatures**.

4

Preventing Information Leakage

This section includes the following sections:

- Information Leakage Overview
- Leakage Prevention – Best Practice Rules
- Leakage Prevention – Custom Rules

4.1 Information Leakage Overview

“Applications can unintentionally leak information about their configuration or internal workings, or violate privacy through a variety of application problems. Applications can also leak their internal state via how long they take to process certain operations or via different responses to differing inputs, such as displaying the same error text with different error numbers. Web applications will often leak information about their internal state through detailed or debug error messages. Often, this information can be leveraged to launch or automate more powerful attacks.
Applications frequently generate error messages and display them to users. Many times these error messages are quite useful to attackers, as they reveal implementation details or information that is useful in exploiting vulnerabilities.
There are several common examples of this:

- Detailed error handling, where inducing an error displays too much information, such as stack traces, failed SQL statements, or other debugging information
- Functions that produce different results based upon different inputs. For example, supplying the same username but different passwords to a login function should produce the same text for no such user and bad password. However, many systems produce different error codes

4.2 Leakage Prevention – Best Practices Rules

dotDefender offers outgoing HTTP inspection rules as part of the Best-Practices Rule set on the Web server, protecting against, for example:

- Credit card exposure

- Social Security Number exposure
- Application & database error proliferation

4.3 Leakage Prevention – Custom Rules

dotDefender allows the administrator to write custom HTTP outgoing inspection rules. Leakage prevention can be obtained in two methods:

- Adding custom (User-Defined) rules to block responses such as error messages from the application. These rules are written in a similar manner as the incoming traffic rules (See **Adding User-Defined rules for responses**)
- Adding Server Masking rules to hide server response headers or change their values for each server response. For example, the server header can be modified from Apache to IIS. For more information, see **Server Masking**.

5

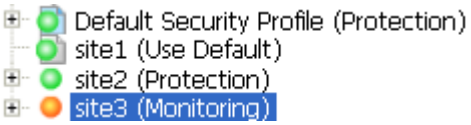
Configuring Website Security Profiles

This chapter contains the following sections:

5.1 Website Security Profiles Overview

Applicure has created best practice rules to detect possible Web attacks. These are defined in the **Default Security Profile**. Initially, all websites use the Default Security Profile (DSP) settings. Any changes to the Default Security Profile (DSP) are propagated to all Website Security Profiles that are configured to use the Default Security Profile (DSP). This is indicated by the **(Use Default)** following the Website Security Profile.

Always start by using the Default Security Profile.
You may decide to configure a Website Security Profile for a specific website. When you select a Website Security Profile and choose either the **Protection**, **Monitoring** or **Disabled** mode, it no longer uses the Default Security Profile. This mode is indicated in ( ) after the Website Security Profile name.



Once you have selected an operating mode other than Use Default Security Profile, you can modify the Website Security Profile by:

- Importing an application rule set template
- Exporting an application rule set template
- Configuring Session Protection settings
- Specifying the error page
- Modifying the advanced settings

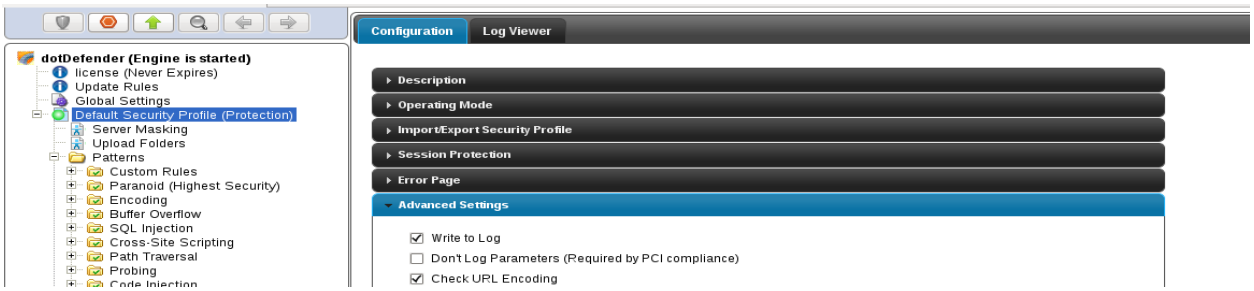
- Changing the Best Practices rule settings.
- Adding new user-defined rules.

5.2 Modifying a Website Security Profile

You can modify the Default Security Profile or any of the Website Security Profiles.

To modify a Profile:

1. In the left pane of the Administration Console, select the required Profile. The right pane displays the Profile settings:



2. (Optional) In the **Description** field, enter a description of the Profile.
3. (Optional) You can make changes in any of the following sections:

- **Operating Mode**
- **Session Protection**
- **Import/Export Security Profile**
- **Error Page**
- **Advanced Settings**

5.2.1 Configuring Operating Mode

You can modify how dotDefender protects your site, monitors attacks, and writes logs.

To modify the Operating Mode:

1. Expand **Operating Mode**. The Operating Mode section opens.

2. Select one of the following operating modes:

- **Use Default Security Profile**: This option can be used to apply the Default Security Profile to the Website Security Profile. If the Default Security Profile is in Protection operating mode, this mode blocks and sends an error message to the attack source when an attack is detected. The event is automatically recorded in the Log.
- **Protection:** This option applies a default template to the specified site. Rules can be applied specifically to this site and the Default Security Profile rules are not applied. This mode blocks and sends an error message to the attack source when an attack is detected. The event is automatically recorded in the Log.
- **Monitoring:** This option applies a default template to the specified site without providing protection while monitoring only. Rules can be applied specifically to this site and the Default Security Profile rules are not applied. This option can be used to monitor and write events in the Log, without providing protection - it does not block attacks.
- **Disabled:** This option disables dotDefender so that it does not monitor or write events in the Log for this Profile. If this option is selected for the Default Security Profile, all Website Security Profiles using the Default Security Profile will not be protected by dotDefender.

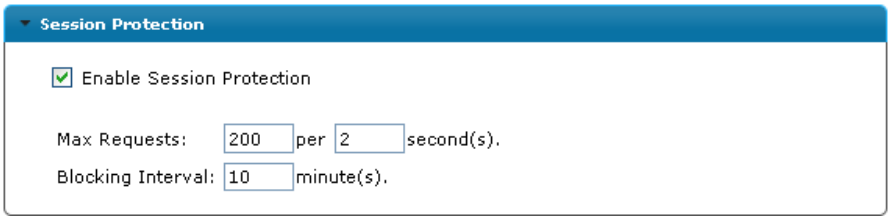
5.2.2 Configuring Session Protection

dotDefender implements a **Session Protection** mechanism that prevents an attacker from sending a large number of HTTP requests in a short period of time. When an attack attempt is detected, dotDefender bans the IP addresses for a preconfigured interval.
Configuration of **Session Protection** is described below.

Note: It is recommended to leave the default **Session Protection** parameters as defined by Applicure. If necessary, make specific minor (narrow) adjustments.

To configure Session Protection:

Expand **Session Protection**. The Session Protection section appears:



In the right pane, edit one or more parameters, as follows:

- **Enable Session Protection**: Enables the Session Protection feature.
- **Max. Requests per seconds**: Defines the maximum allowed number of HTTP requests sent from the same IP address to your Web server, per specified number of seconds. A user sending requests at a higher rate is blocked.
- **Blocking interval**: Sets the time period dotDefender blocks access from the suspected attacker's IP address, counting from the latest request.
- **Write to Log**: Allows session protection events to be written to the Log Viewer.

Click  to apply the changes.

5.2.3 Import/Export security profile

Security Profiles rule sets are stored in an XML file. Application rule sets for known applications and content management systems (CMS) can be imported from a prepared template.
Security Profiles can be transferred from one profile to another by exporting and importing. It does not matter if the Security Profiles are located on the same server or on different servers running on different platforms.

To export an Application Rule Set:

- Expand the **Import/Export security profile** section

- Click on the Export button
- Save the XML file

To import an Application Rule Set:

1. Expand the **Import/Export security profile** section

2. Click on the Import button
3. Browse to an XML file containing a security profile rule set
4. Click  to apply the changes

Note: All old configuration settings will be removed and the new XML settings will apply.

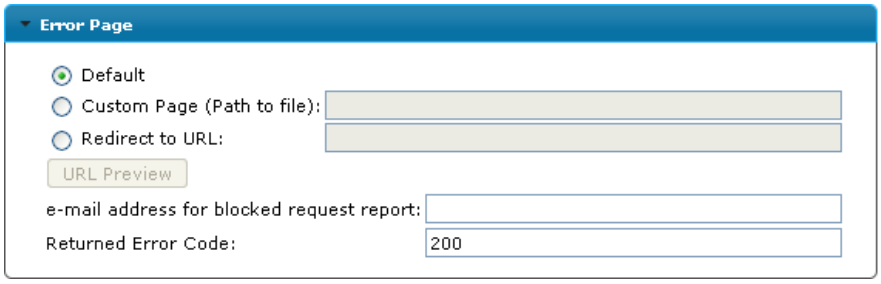
5.2.4 Configuring the Error Page

You can modify the Error Page settings to determine the page that is displayed as well as the email address to which valid users report when their requests are blocked.
To view the resultant error page, the following request can be sent to the server and should be blocked when security profile is set to Protection: **http://www.company.com/?a=xp_cmdshell** (Where **www.company.com** is the URL to one of the websites on the server)
You can add the following variables to the body of a custom page:

- **%MAILTO_BLOCK% -** Email entered in the "Email address for blocked request report" field. Adding this variable creates an active link to send an email to the Website Administrator. The email includes the Reference ID, Client IP address and Date. On **Linux/Unix** platforms, this variable is named %EMAIL% and must be closed with brackets, like so **<%EMAIL%>**
- **%RID% -** Reference ID. On **Linux/Unix** platforms, this variable must be closed with brackets, like so **<%RID%>**
- **%IP% -** Server's IP address. On **Linux/Unix** platforms, this variable must be closed with brackets, like so **<%IP%>**
- **%DATE_TIME% -** Date of blocked request. On **Linux/Unix** platforms, this variable must be closed with brackets, like so **<%DATE_TIME%>**

To modify the Error Page:

1. Expand the **Error Page** section:



2. Select one of the following:

   - **Default**: This option uses the default Error Page.
   - **Custom**: This option enables you to enter the path to an error page file, to be displayed by dotDefender in the attacker's browser. For example:

IIS: C:\Inetpub\wwwroot\custom_deny.html

Apache: /var/www/custom_deny.html

   - **Redirect to URL**: This option instructs dotDefender to redirect a user to a full URL path (for example, a web page). In this case, no error page is displayed. For Example: **http://www.company.com**. (Optional) Click **URL Preview** to view the page.

3. (Optional) Enter an email address in the **Email address for blocked request report** to create an active link to send an email to the Website Administrator. Note: The **%MAILTO_BLOCK%** variable (Or **<%EMAIL%>** for Linux/Unix) should be added manually to the body of a custom error page.

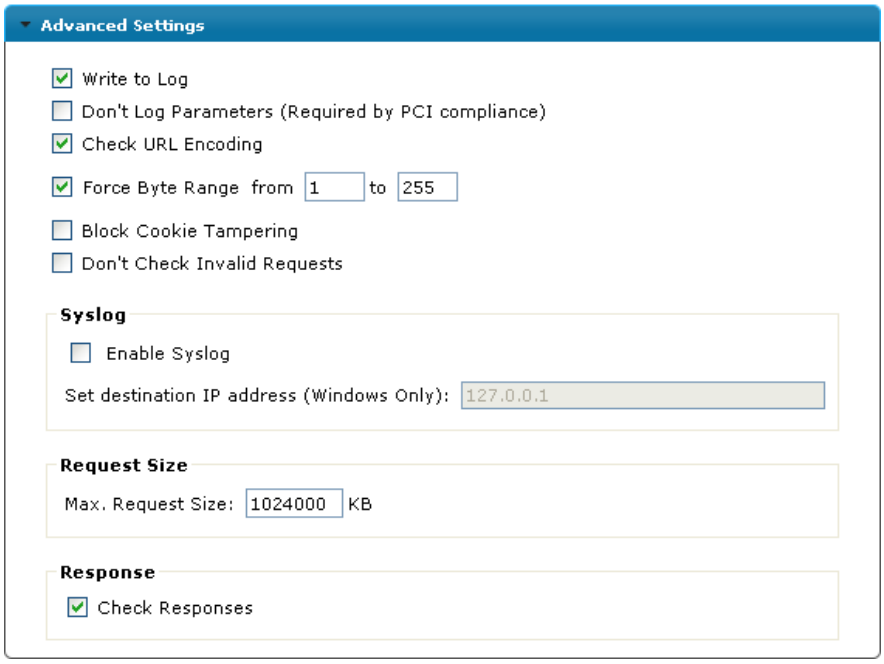
4. (Optional) Configure the HTTP status code returned to the client when a request has been denied by setting a status code number at the right-hand side of the **"Return Error Code:"** field according to the expected application behavior. Some examples for such status codes include: 200, 302, 400, 404 and 500.
   This is especially useful when using automatic Vulnerability Assessment software that expects a pre-defined status code in order to differentiate between successful and unsuccessful vulnerability detection.

5.2.5 Configuring Advanced Settings

You can modify the Advanced Settings for various options, such as writing to the log, checking URL encoding, and managing large requests.

To modify the Advanced Settings:

1. Expand the **Advanced Settings**.



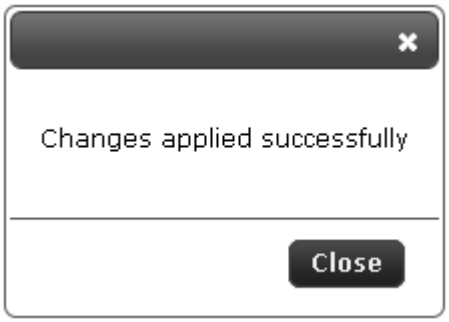
2. Select one or more of the following options:

   - **Write to Log**: dotDefender writes the attack events to the dotDefender database.
   - **Don't Log Parameters (Required by PCI compliance):** dotDefender will not log parameter strings. Instead, what will be visible in the event's details are only the detected attack patterns.
   - **Check URL Encoding**: dotDefender checks that the URL is RFC compliant.
   - **Force Byte Range from (minimum value) to (maximum value)**: dotDefender limits the range of byte values that it will pass.
   - **Block Cookie Tampering**: dotDefender blocks tampering by cookies. It checks that the cookie was not changed from the time it was issued to the user to the time the user returns the cookie with the next request.
   - **Don't Check Invalid Requests**: This option instructs dotDefender to ignore invalid HTTP requests, such as non-standard headers, BOT files, HTTP requests originating from Proxy Servers, or syntax missing in the structure.

3. In the Request Size area, enter the maximum permitted request size (in KB) in the **Maximum Request Size** field. By default, a value higher than the maximum size results in blockage of traffic to the Web server.

4. In the **Response** area, select the **Check Responses** option to apply egress (Outgoing) traffic inspection and filtering. Once this option is selected, all HTTP response rules will be applied.

- Click  to apply the changes. The following pop-up message appears:



- Click **OK**.

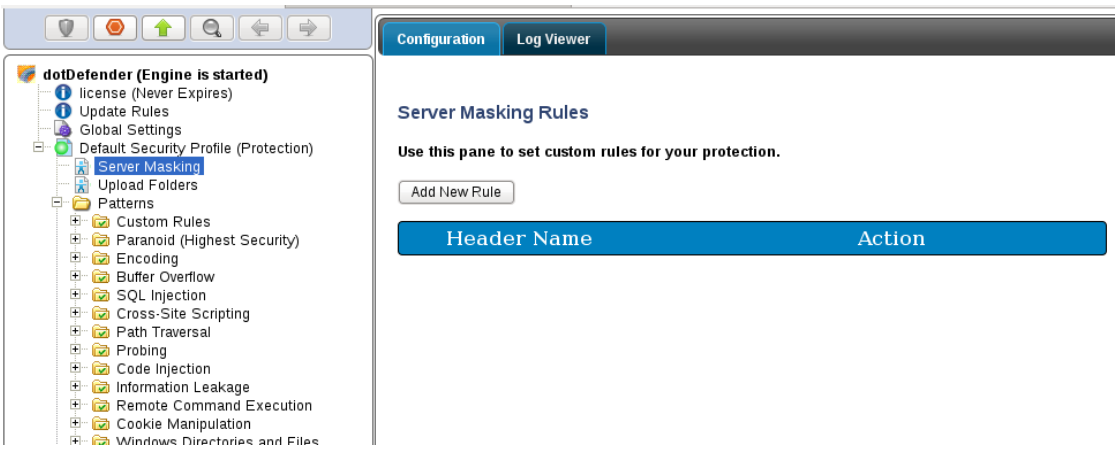
5.3 Server Masking

The server masking function allows you to conceal sensitive infrastructure fingerprint information. This is achieved using HTTP response header removal, replacement or addition.

Examples:

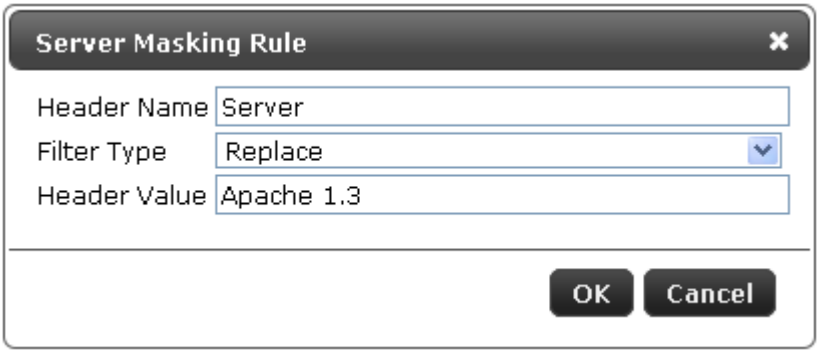
- **Masking Server header** - In order to mask an IIS 6.0 web server, perform the following:

1. Expand a security profile.
2. Select **Server Masking**:



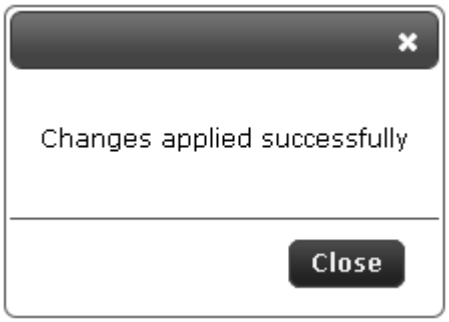
3. In the right pane, click the **Add New Rule** button.
4. In the **Header Name** field, type: **Server.**

5. **In the Filter Type, select Replace:**



6. **In the Header Value, type: Apache 1.3.**

- Click **OK**. The new rule appears in the **Server Masking Rules** list.
- Click  to apply the changes. The following pop-up message appears:

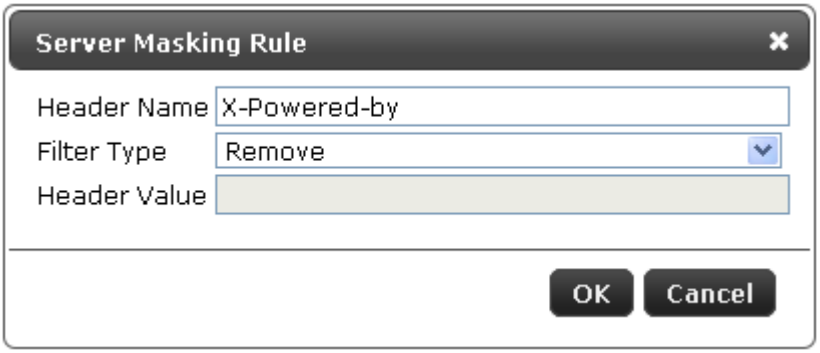


- Click **OK**.

- **Removing X-Powered-by header** - In order to remove the X-Powered-by header, perform the following:

1. Expand a security profile.
2. Select **Server Masking**.

3. In the right pane, click the **Add New Rule** button.
4. In the Header Value, type: X-Powered-by:



5. In the Filter Type, select **Remove**.
6. Click **OK**. The new rule appears in the **Server Masking Rules** list.
7. Click  to apply the changes. The following pop-up message appears:

8. Click **Close**.

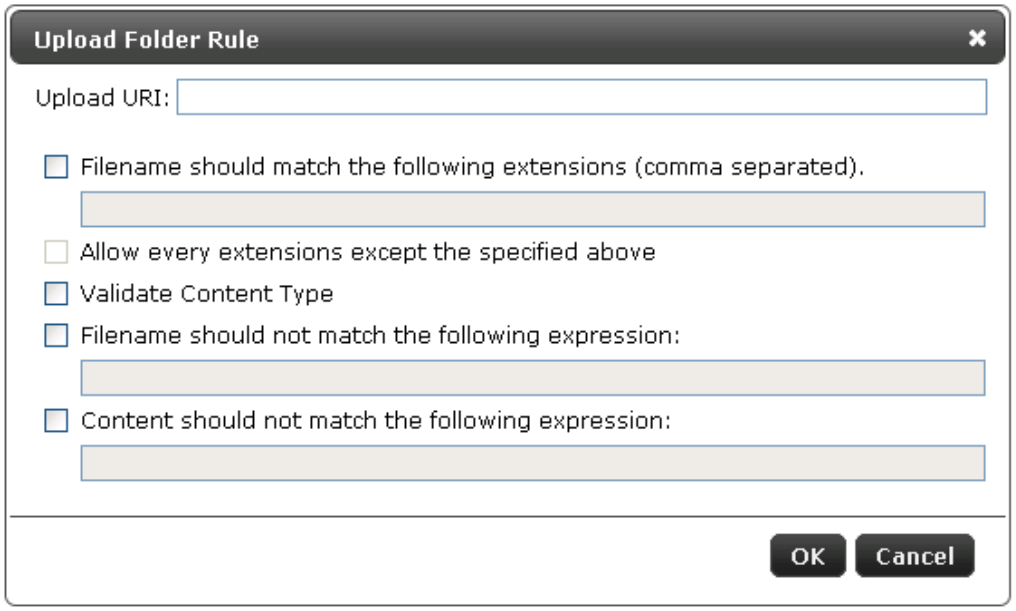
5.4 Upload Folders Protection

In order to validate uploaded file types and content, use **Upload Folder Protection** to define fine-grained rules to define allowed/disallowed file extensions, MIME types and content patterns. This mechanism allows protection against malicious file uploads using such public interfaces as image and content management systems. Unvalidated file uploads often lead to complete server compromise using Web-shell backdoors masquerading as innocent picture/document files.

To create a custom rule to validate uploaded file types and content

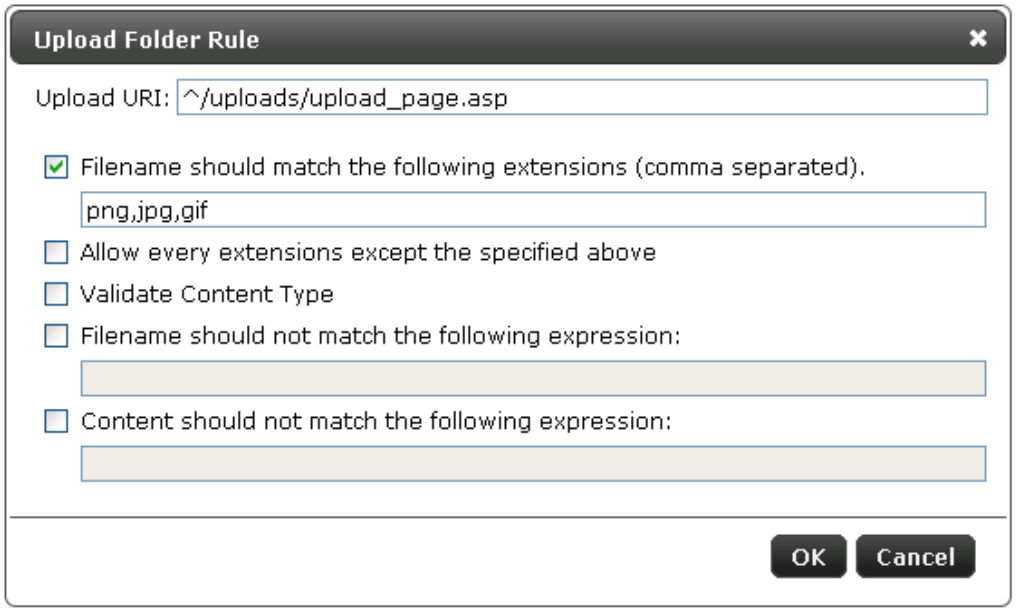
1. Expand a security profile
2. Select **Upload Folders**:

3. In the right pane, click the **Add New Rule** button

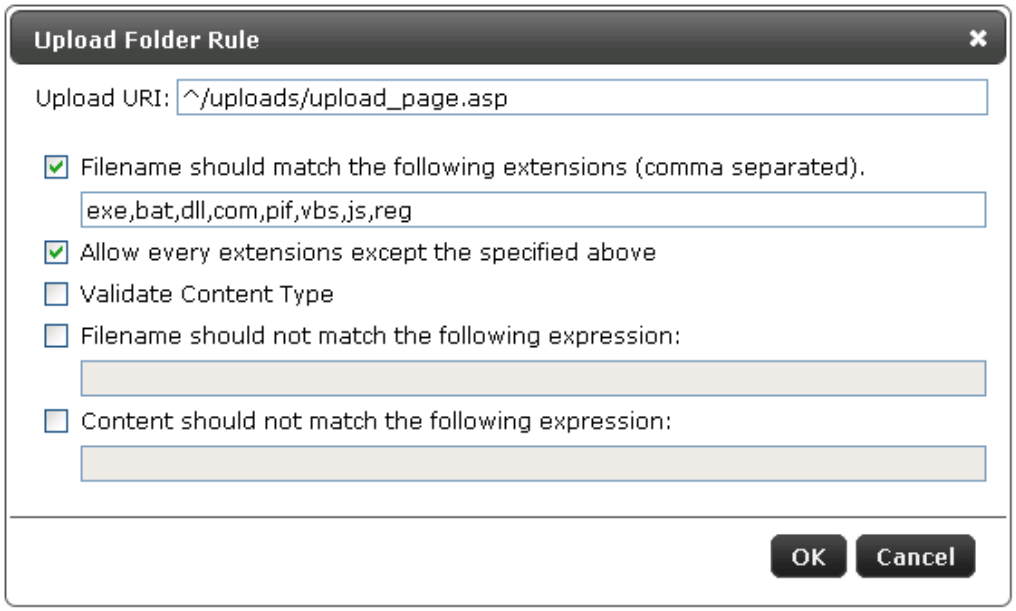


4. In the **Upload URI** field, type the URI of the upload page. For example: /Content_Upload/upload_form.asp

5. Select **Filename should match the following extensions (comma separated)** and type the extensions which should be allowed for upload. For example: **png,jpg,gif**



6. To create a list of extensions that should not be allowed to be uploaded, select **Allow every extension except specified above** and follow paragraph 5 above while typing file extensions which should not be allowed:



- Select **Validate Content Type** to validate content type of the file and ensure that a malicious script is not attempted to be uploaded using a false extension.
- (Optional) Select **Filename should not match the following expression** to block specific filenames. Type a pattern representing the names of files to be blocked.
- (Optional) Select **Content should not match the following expression** to block specific patterns in the content of the files. Type a string representing the content to be blocked.

7. Click **OK**
8. The new rule appears in the **Upload Folders Rules** list.
9. Click  to apply the changes. The following pop-up message appears:

10. Click **Close**.

6

Configuring Patterns and Signatures

Web application hacking attempts are classified by distinct patterns or signatures.
This chapter contains the following sections:

- Patterns and Signatures Overview
- Rule Categories
- Enabling/Disabling a Rule Category
- Configuring Patterns
- Managing Signatures
- Update Rules

6.1 Patterns and Signatures Overview

When blocking attacks, dotDefender tries to identify threats based on pattern-matching rules and behavior signatures. The Default Security Profile and Website Security Profiles include:

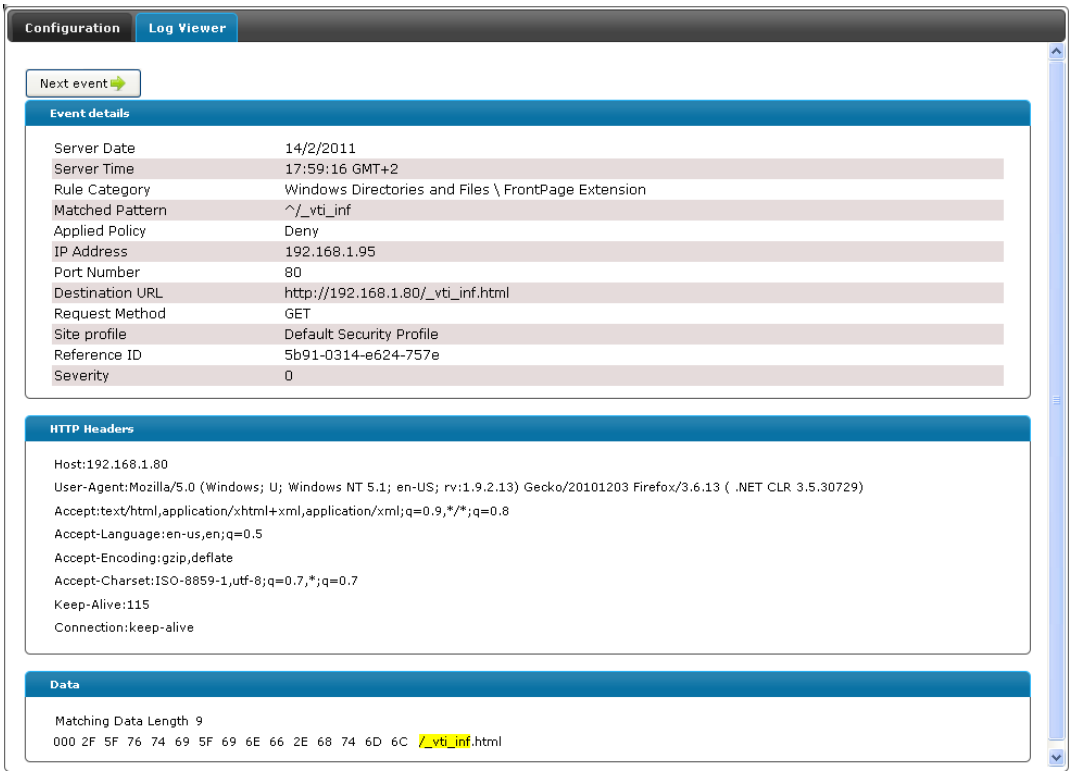
- **Patterns:**
  - **Rule Categories** that include:
    - **User-defined rules:** Custom rules for this rule category.
    - **Best practices:** A predefined set of best practice sub-categories (rules) defined by Applicure.
- **Signatures:** Predefined signature categories**.**

To modify the behavior of dotDefender, for example, to allow false positives, you can do one of the following:

- Define a Whitelist rule. See **Configuring Patterns**.
- Disable/enable a rule category. See **Enabling/Disabling a Rule Category**.
- Create a user-defined category rule. See **Configuring Patterns**.
- Disable/enable a Best Practice category (rule). See **Configuring Patterns**.
- Enable/disable a signature category. See **Managing Signatures**.

dotDefender Log Viewer displays the category/sub-category of the attack, as well as the

substring that caused the alert to be triggered. An example of an attack is displayed in the Event Details window:



The fields displayed include:

- Date
- Time
- Category of attack
- Sub-category of attack
- IP address of attacker
- Reference ID
- The hex dump of the string as it was captured on the wire: the matching substring that triggered the alert is highlighted in yellow.

In the example above:

- The **Category** of the attack is **Windows Directories and Files**.
- The **Sub-category** is **FrontPage Extension**.
- The **IP Address** is **192.168.1.4**.
- The **Reference ID** is **d011-6496-42c4-91ee**.
- The substring is **_vti_pvt**.

6.2 Rule Categories

The dotDefender software has the following predefined rule categories:

Pattern	Description
Custom Rules (Permitted Access List)	The Custom Rules category enables you to approve or deny specific users, pages, or actions that are not checked by default by dotDefender. dotDefender users can configure, for example, rules to block access to server applications or, conversely, allow absolute access so they are not checked. dotDefender users can also define certain application web pages or directories not to be checked at all. **Whitelist rules are evaluated before all other dotDefender protection rules and signatures.**
Paranoid (Highest Security)	A collection of rules that provides a more restrictive level of security, but may interfere with Web application usability. You can use this category to tighten security for sensitive applications or functionalities (for example, login or credit card details.
Encoding	Encoding is a method of representing characters in different ways for use in computer systems. ASCII (American Standard Code for Information Interchange), and UTF (Unicode Transformation Format) are examples of encoding, where the same text is encoded in various ways, so that a Web server can interpret it. An Encoding attack harms the application by implementing obfuscation to ensure that suspect packets are camouflaged by, for example, UTF or HEX (Hexadecimal) encoding. This results in a disguised injection of malicious phrases in URLs, parameters or metadata.
Buffer Overflow	When an application sends more data to a buffer than the buffer is designed to hold, the overflow can cause a system crash or create a vulnerability that enables unauthorized system access.
SQL Injection	An SQL injection is an attack method that targets the database via a Web application. This method exploits the application by injecting malicious queries, causing the manipulation of data. SQL injection aims at penetrating back-end database(s) to manipulate data, thus stealing or modifying information in the database.

Pattern	Description
Cross-Site Scripting	Scripts comprise of a set of programming language instructions executed by another program (such as a browser). Scripting is used to create dynamic pages in Web applications. Cross-site scripting is a client-side attack method that occurs when an attacker uses a Web-based application to send malicious code to another user who uses the same application. This attack is most common in dynamically-generated application pages, where embedded application forms are built. This attack is automatically executed when the client's browser opens an HTML web page. As a result of cross-site scripting, a user's browser mistakenly identifies the script as having originated from a trusted source. As a result, the maliciously injected code can access cookies, session tokens, or any other sensitive information. There are two categories of cross-site scripting: • Stored attacks: These occur when the injected malicious code is stored on a target server such as a bulletin board, a visitor log, or a comment field. The victim retrieves and executes the malicious code from the server, when interacting with the target server. • Reflected attacks: These occur when the user is tricked into clicking a malicious link, or submitting a manipulated form (crafted by the attacker). The injected code travels to the vulnerable Web server which reflects the cross-site attack back to the user's browser. The browser then executes the malicious code, assuming it comes from a trusted server.
Path Traversal	A URL is a Web address translated into a path on the Web server. It leads to specific directories and files residing on the server. Path traversal is an attack mechanism that changes the original path to the path desired by an attacker, in order to gain access to internal libraries and folders. Path traversal gains access to an organization's server files and directories that are otherwise inaccessible to external users. Path Traversing is implemented with common OS operations, such as using the characters "/../../../.." for traversing between server directories and files.

Pattern	Description
Probing	Probing is an attack aim at collecting information about a Web server and applications, based on common practices and educated guesses. Attackers send probes looking for common weaknesses and third-party software that has known vulnerabilities. This information can be used to breach the server.
Code Injection	Remote File Inclusion attacks supply the application with an external script to be automatically interpreted by the running application, possibly resulting in server compromise. Code Injection can result in local OS access, sabotage / theft of data and remote access to servers. Code Injection is commonly used by hackers to install backdoors written in ASP and PHP, being the de-facto interpreted languages supported by Web servers.
Information Leakage	This protection category prevents leakage of sensitive information (e.g. Credit card data, Healthcare…). Disclosing either personal or system infrastructure information. In case such data is detected within HTTP responses, it will be blocked or removed.
Remote Command Execution	A type of injection, similar to SQL Injection, except that it injects OS Shell commands into the Shell.
Cookie Manipulation	Cookies are commonly used to store user and session identification information that serves as a means of authenticating users to the application. Cookie Manipulation refers to various methods of manipulation of cookie content. Using cookies, an attacker can obtain unauthorized access to the Web server. CLRF Injection (Carriage Return/Line Feed) is an example of Cookie Manipulation.
Windows Directories and Files	Windows directories and files are default components created during the installation of IIS and related applications, such as FrontPage, IIS sample page, and more. These default components contain known weaknesses, which an attacker may use to breach the server.
XML Schema	XML Schema is a document that describes, in a formal way, the syntax elements and parameters of predefined XML structures and files. It is used in Web Services and XML-based applications. Since the XML Schema describes all of the available service functions, hackers may use this information to discover vulnerabilities in the application.

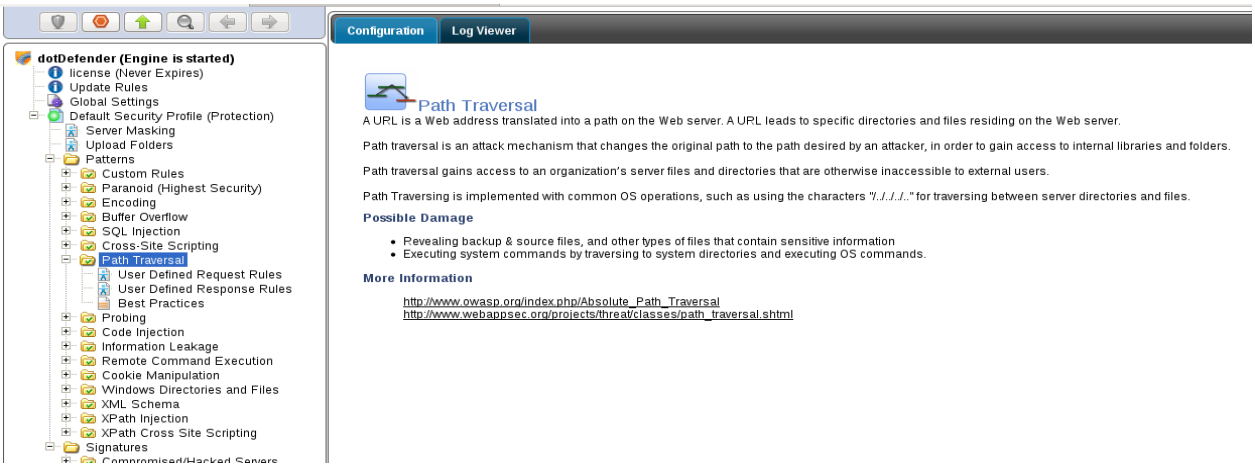
Pattern	Description
XPath Injection	XPath is a language used to access parts of an XML document. Hackers may insert malicious code into XML parameters to gain access to the Web server, or retrieve information from the database, much like SQL Injection.
XPath Cross-Site Scripting	Inserts cross-site scripting attacks into sections of XML. For further information, see **Cross-site Scripting**.

These descriptions can also be viewed online in dotDefender.

To view an explanation of a pattern category:

1. In the left pane of the Administration Console, expand the **Default Security Profile (Protection)**, and then expand **Patterns**.

- Select a pattern category. The description of the category is shown in the right pane:



6.3 Enabling/Disabling a Rule Category

You can enable or disable a rule category.

To enable/disable a rule category:

1. In the left pane of the Administration Console, select the required profile.
2. Expand **Patterns**.
3. Right-click on the rule category and select **Disable/Enable**. The rule category is enabled or disabled, accordingly.
4. Click  to apply the changes.

6.4 Configuring Patterns

To configure a pattern category:

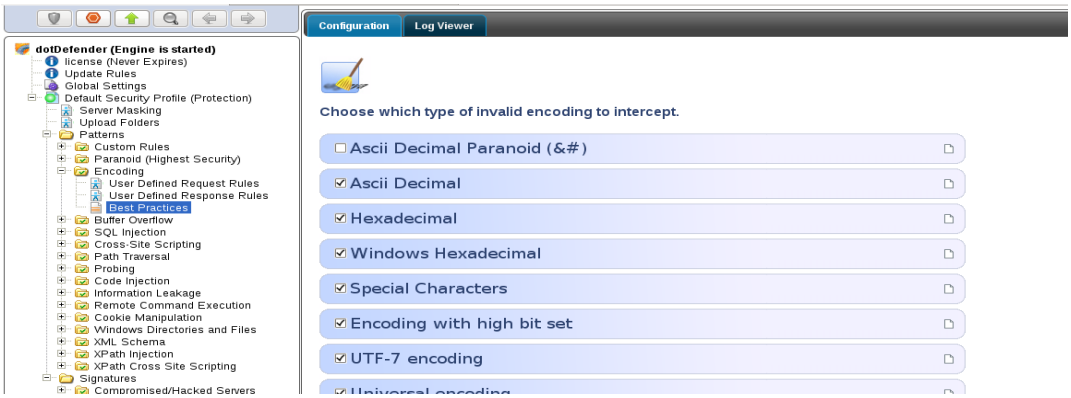
1. In the left pane of the Administration Console, select the required Profile.
2. Expand **Patterns**.
3. Expand the required pattern category.
4. Select one of the following:
   - **Modifying Best Practices**
   - **Adding User-Defined Rules**

6.4.1 Modifying Best Practices

dotDefender supplies a series of **best practice** rules to block attacks. You can modify the rule properties or enable/disable the rule.

To modify Best Practices sub-categories:

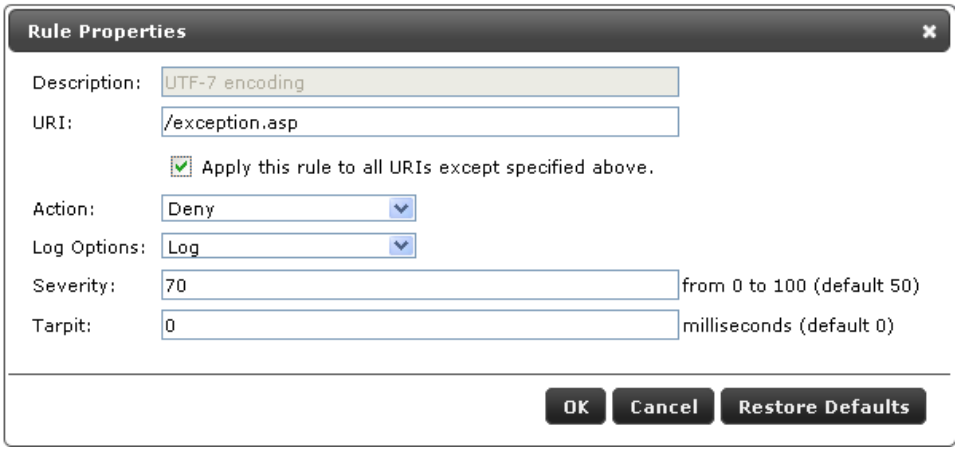
1. Select **Best Practices**. The sub-categories appear in the right pane:



- (Optional) Click ☐ / ☑ to enable/disable the sub-category (rule).

Note: It is recommended to define a URI in the Rule Properties dialog box and select the "Apply this rule to all URIs except specified above" checkbox rather than disable a rule.

2. Select a sub-category (rule) and click 🗋. The Rule Properties window appears:



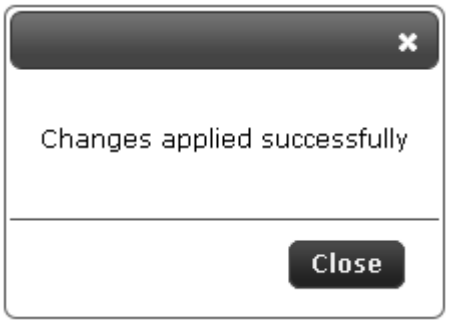
3. In the **URI** field, enter a specific URI under which you want to apply or exclude a rule. By default, rules are applied to all URIs (all Web pages).

- To apply the rule to all URIs except the one you specified ("Exclude"), select **Apply this rule to all URIs except specified above**.

4. From the **Action** drop-down list, select one of the following:
   - **Deny:** Denies the request when the pattern is matched.
   - **Allow:** Quits scanning the request at this sub-category after the pattern is matched. (Not recommended for Best Practice rules)**.**
   - **Monitor Only:** Monitors this sub-category when a pattern is matched.
5. From the **Log Options** drop-down list, select one of the following:
   - **Log**
   - **No Log**

- In the **Severity** field, the severity can be modified to any value from 0 to 100, where 100 is the highest severity. The value of the severity is used in the Central Management reporting feature, which enables the filtering of events by their severity.
- In the **Tarpit** field, choose the required response latency by defining a value in milliseconds next to Tarpit. This option enables delaying rapid attacks, offloading the Web server.

6. Click **OK**. The changes to .
7. Click to apply the changes. The following window appears:



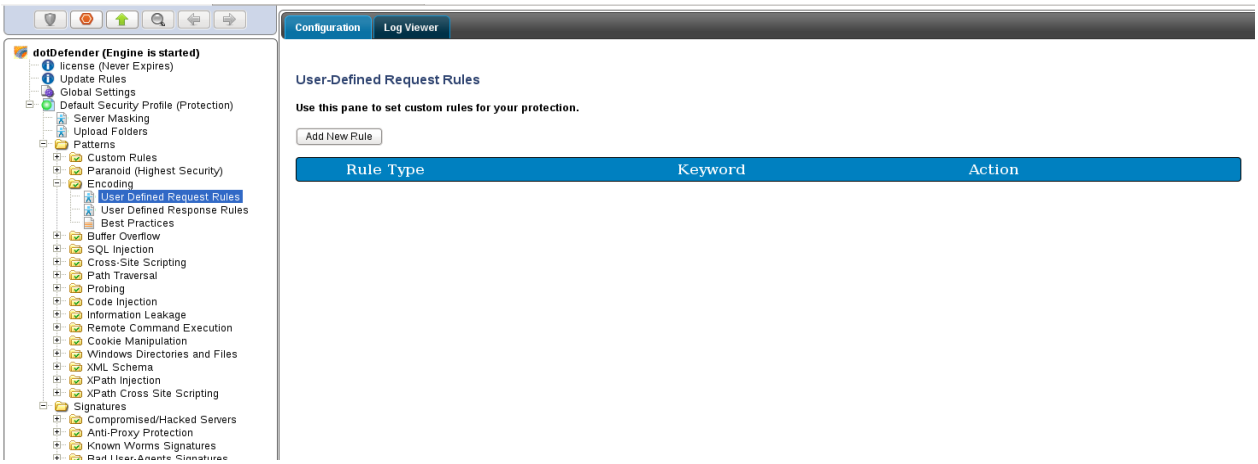
8. Click **Close**.

6.4.2 Adding User-Defined Rules for incoming requests

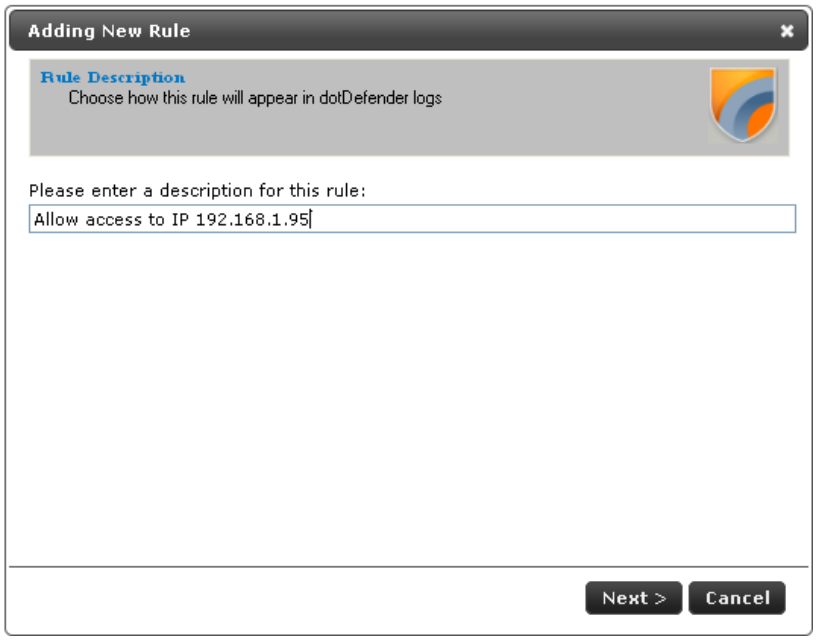
You can create new rules for dotDefender by using regular expressions to match a pattern that is to be blocked, allowed or monitored. The following instructions explain how to create a rule to block, allow, or monitor incoming HTTP requests to the server. (Optional: identify the pattern using the sub-string identified in the log. For further information, see **Managing Logs**.)

To add a new rule:

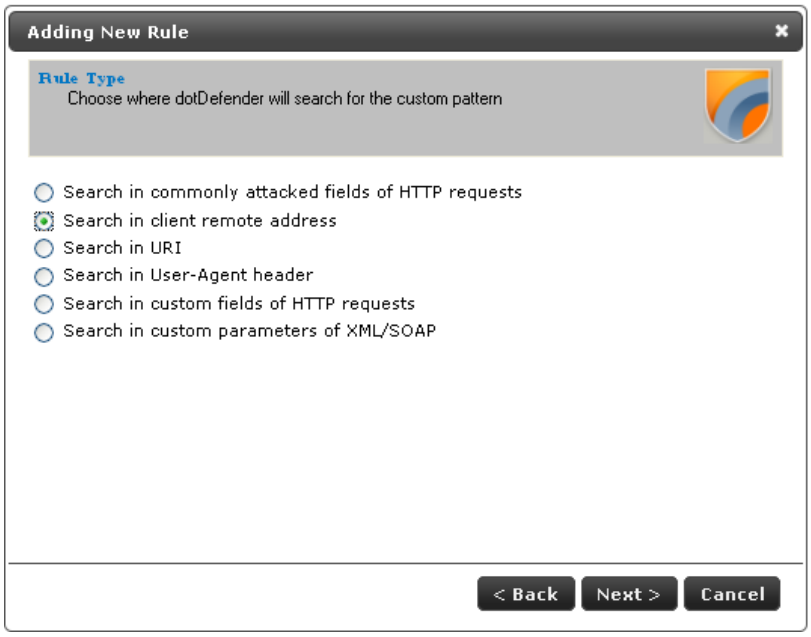
Click **User Defined Request rules** in any category. The User-Defined Rules list appears in the right pane:



Click **Add New Rule**. The New Rule wizard appears:



Type a description for the rule. Click **Next**:



To determine where in the HTTP request dotDefender searches for the custom pattern, select one of the following options:

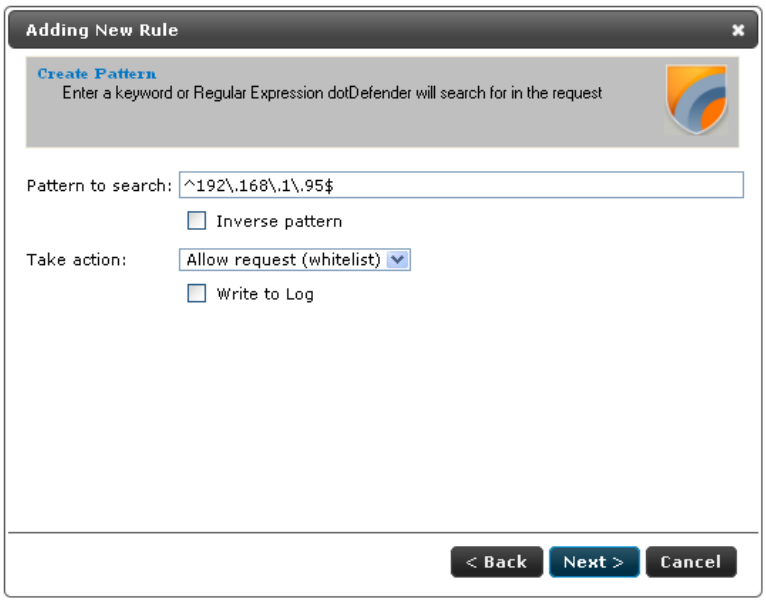
- **Searching in Commonly Attacked Fields of HTTP Requests** - Click **Next** to continue. The Create pattern window appears. Continue with Searching in Commonly Attacked Fields of HTTP Requests.
- **Searching in Client Remote Address** – Search for pattern in the client's IP address field. Click **Next** to continue. The Create pattern window appears.
- **Searching in URI** - Search for pattern in the URI of the request. Click **Next** to continue. The Scope of search window appears.
- **Searching in User-Agent header** – Search for pattern in the User-Agent client software identifier field. Click **Next** to continue. The Create pattern window appears.
- **Searching in Custom Fields of HTTP Requests** - Click **Next** to continue. The Custom Fields window appears. Continue with Searching in Client Remote Address
- **Searching in custom parameters of XML/SOAP** - Click **Next** to continue. The Custom Fields window appears. Continue with Searching in Custom Parameters of XML/SOAP.

6.4.2.1 Searching in Client Remote Address

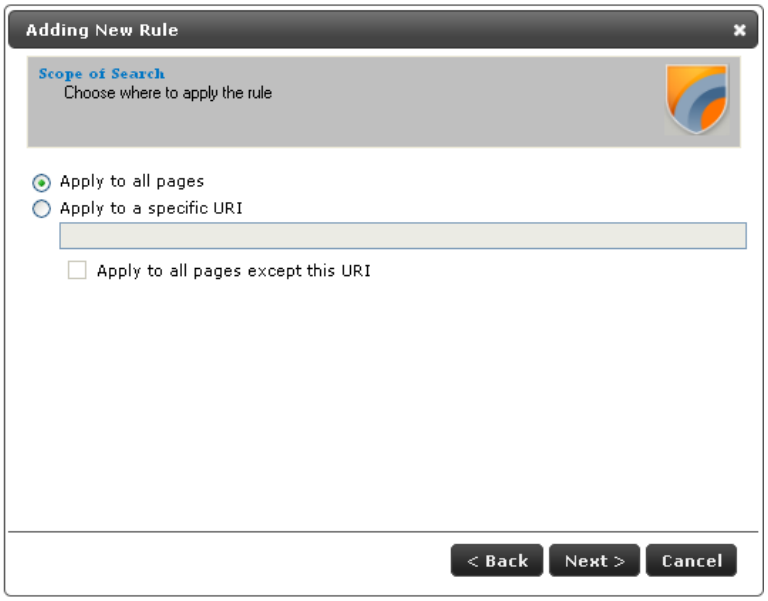
You can specify a pattern to search for in Client Remote Address.

To search in Client Remote Address:

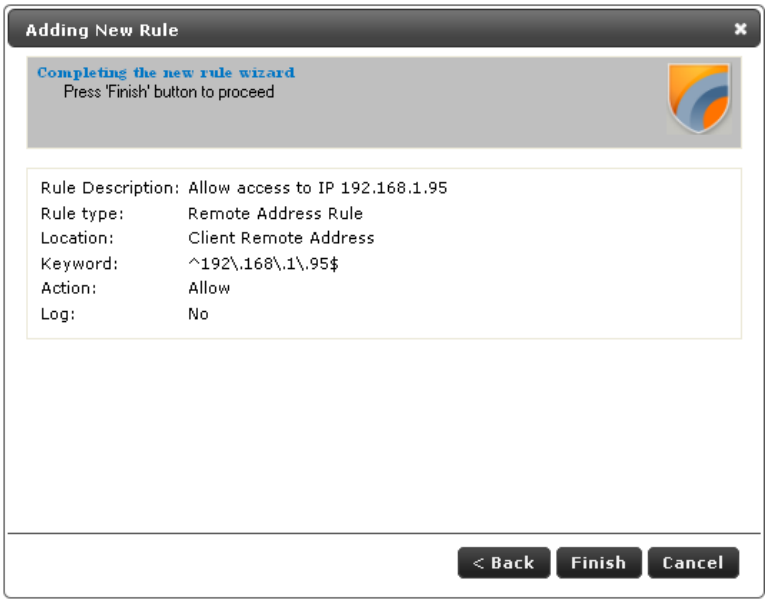
1. In the Create pattern window, in the **Pattern to Search** field, enter a regular expression for which dotDefender looks in the HTTP request. For further information, see **Regular Expressions**.



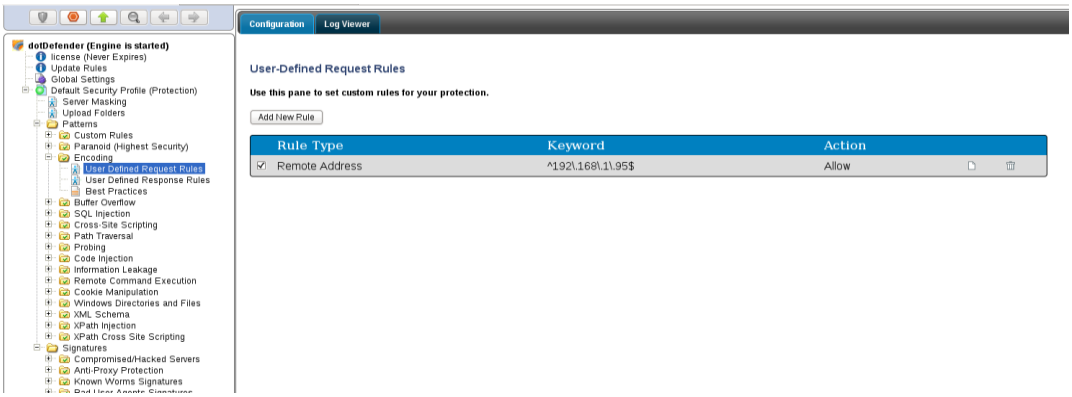
2. From the **Take action** drop-down list, select one of the following:
   - **Block request:** dotDefender blocks requests containing the pattern.
   - **Allow request (Whitelist):** dotDefender allows requests containing the pattern.
   - **Monitor:** dotDefender only logs HTTP requests containing the pattern.
   - **Skip Category:** dotDefender excludes rules in this category for requests containing the pattern.
3. (Optional) Select the **Write to Log** checkbox if you want the events matching the rule to be logged.
4. Click **Next** to continue. The Scope of Search window appears:



5. Select one of the following:
   - **Apply to all pages**: dotDefender applies the search to all HTTP pages.
   - **Apply to specific URI**: dotDefender applies the search to a specific URI. Enter the URI field.
   - **Apply to all pages except this URI**: dotDefender applies the search to all HTTP pages, excluding the specified URI.
6. Click **Next**. The **Completing the New Rule Wizard** window appears:



7. Review the summary of the new rule. Click **Finish**. The new rule appears in the list of User-Defined Rules:



8. Click  to apply the changes. The following window appears:

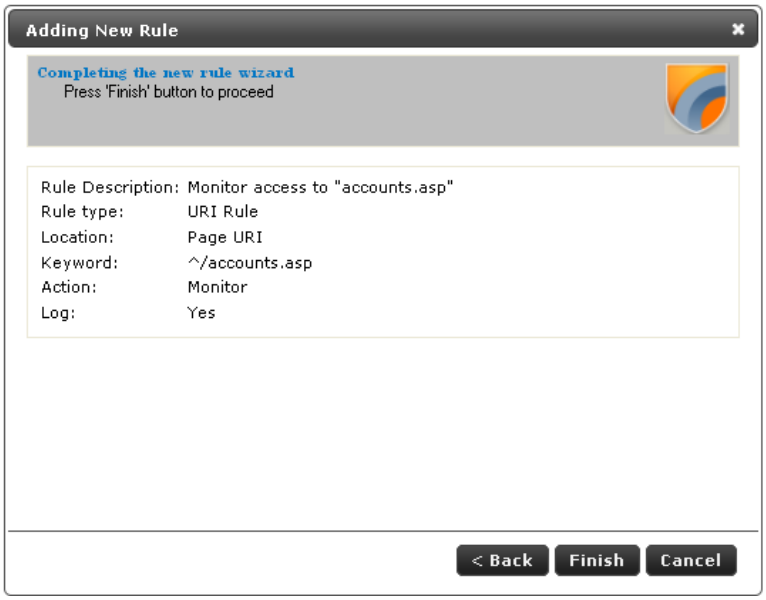
9. Click **Close**.

6.4.2.2 Searching in URI

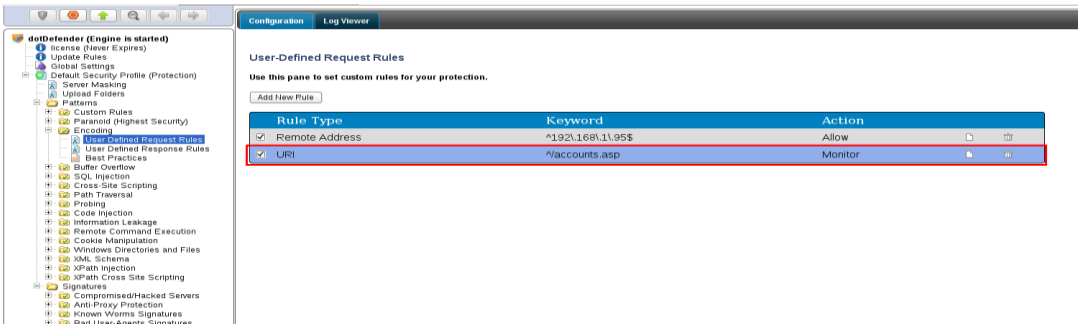
You can specify a URI for which an action will be applied.

To search in URI:

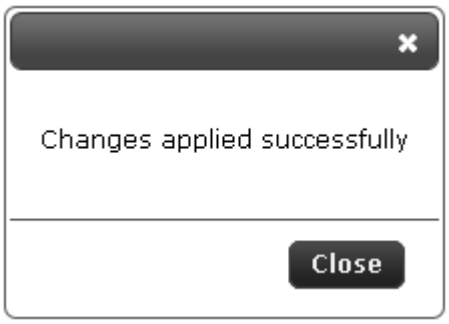
1. Select one of the following:
   - **Apply to all pages:** dotDefender applies the search to all HTTP pages.
   - **Apply to specific URI:** dotDefender applies the search to a specific URI. Enter the URI field.
   - **Apply to all pages except this URI:** dotDefender applies the search to all HTTP pages, excluding the specified URI.
2. From the **Take action** drop-down list, select one of the following:
   - **Block request:** dotDefender stops requests including this URI.
   - **Allow request (Whitelist):** dotDefender allows requests including this URI.
   - **Monitor:** dotDefender only logs HTTP requests including this URI.
   - **Skip Category:** dotDefender excludes rules in this category for requests containing this URI.
3. (Optional) Select the **Write to Log** checkbox if you want the events matching the rule to be logged.
4. Click **Next**. The **Completing the New Rule Wizard** window appears:



5. Review the summary of the new rule. Click **Finish**. The new rule appears in the list of User-Defined Rules:



6. Click  to apply the changes. The following window appears:



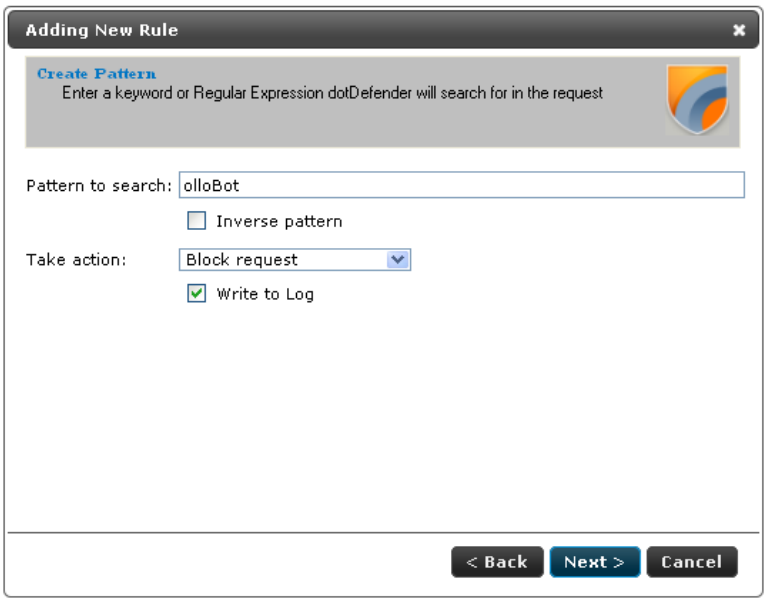
7. Click **Close**.

6.4.2.3 Searching in User-Agent header

You can specify a pattern to search for in User-Agent client software identifier field.

To search in User-Agent header:

1. In the Create pattern window, in the **Pattern to Search** field, enter a regular expression for which dotDefender looks in the HTTP request. For further information, see **Regular Expressions**.

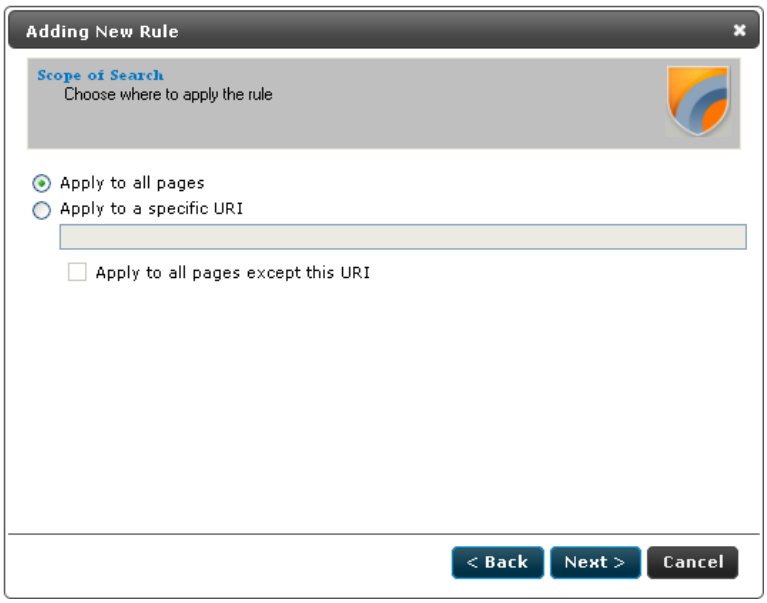


2. From the **Take action** drop-down list, select one of the following:

   - **Block request:** dotDefender stops requests containing the pattern.
   - **Allow request (Whitelist):** dotDefender allows requests containing the pattern.
   - **Monitor:** dotDefender only logs HTTP requests containing the pattern.
   - **Skip Category:** dotDefender excludes rules in this category for requests containing the pattern.

3. (Optional) Select the **Write to Log** checkbox if you want the events matching the rule to be logged.

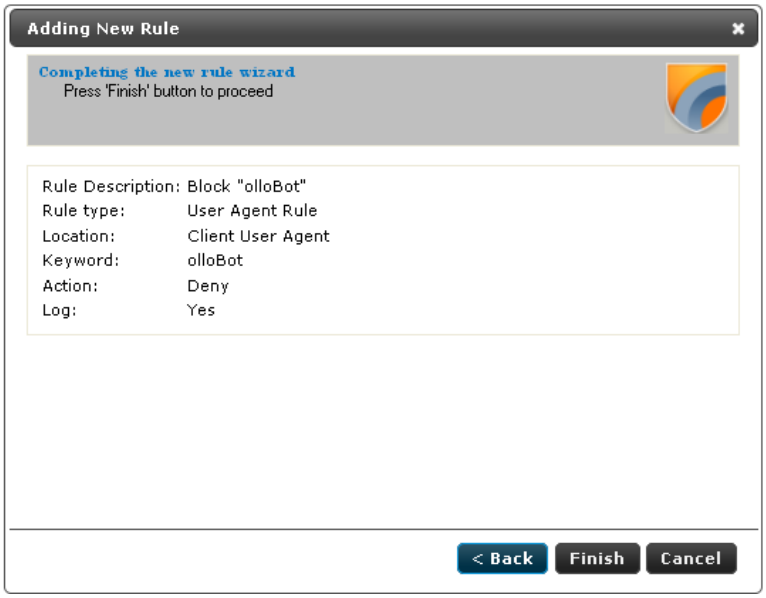
4. Click **Next** to continue. The Scope of Search window appears:



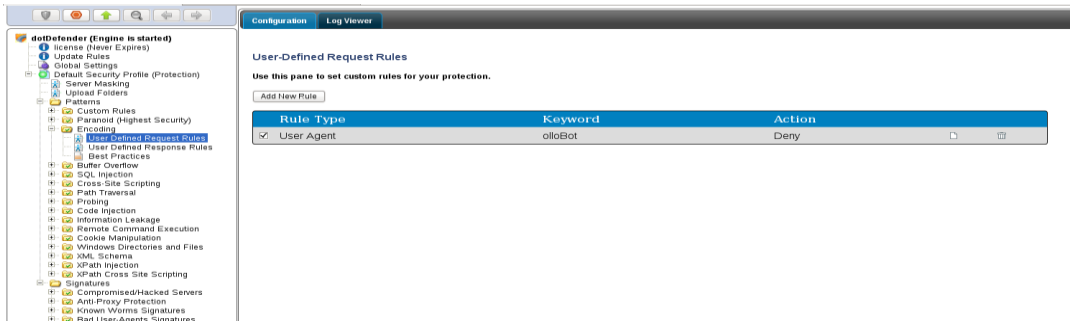
5. Select one of the following:

- **Apply to all pages**: dotDefender applies the search to all HTTP pages.
- **Apply to specific URI**: dotDefender applies the search to a specific URI. Enter the URI field.
- **Apply to all pages except this URI**: dotDefender applies the search to all HTTP pages, excluding the specified URI.

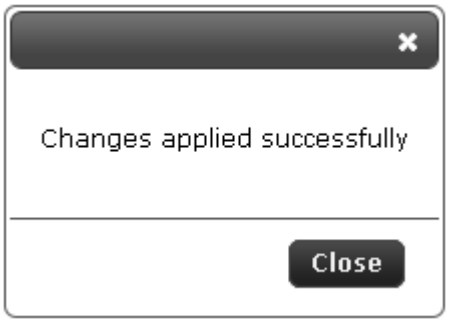
6. Click **Next**. The **Completing the New Rule Wizard** window appears:



7. Review the summary of the new rule. Click **Finish**. The new rule appears in the list of User-Defined Rules:



8. Click  to apply the changes. The following window appears:



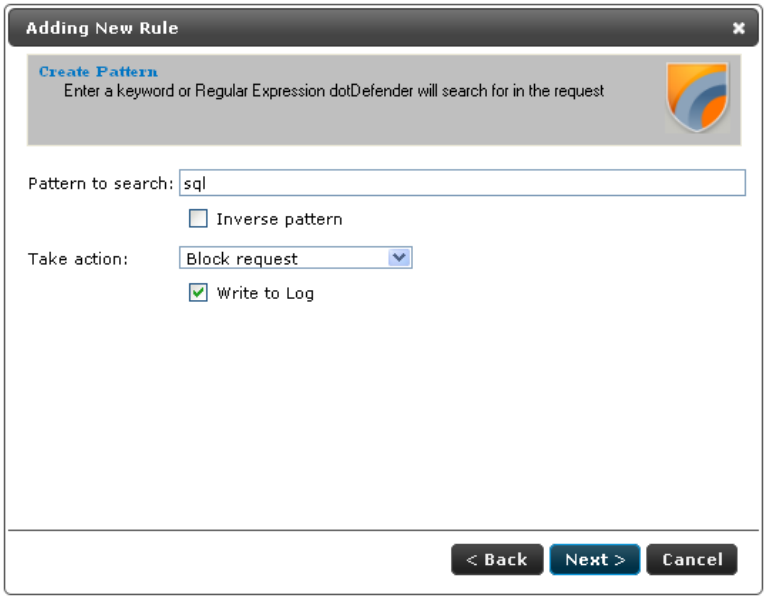
9. Click **Close.**

6.4.2.4 Searching in Commonly Attacked Fields of HTTP Requests

You can specify a pattern to search for in commonly attacked fields of HTTP requests.

To search in commonly attacked fields:

1. In the Create pattern window, in the **Pattern to Search** field, enter a regular expression for which dotDefender looks in the HTTP request. For further information, see **Regular Expressions**.

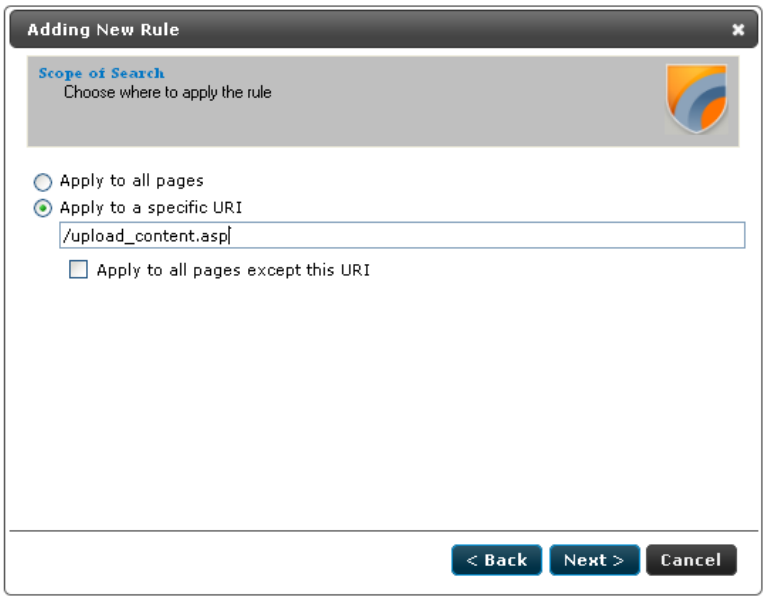


2. From the **Take action** drop-down list, select one of the following:

- **Block request:** dotDefender stops requests containing the pattern.
- **Allow request (Whitelist):** dotDefender allows requests containing the pattern.
- **Monitor:** dotDefender only logs HTTP requests containing the pattern.
- **Skip Category:** dotDefender excludes rules in this category for requests containing the pattern.

3. (Optional) Select the **Write to Log** checkbox if you want the events matching the rule to be logged.

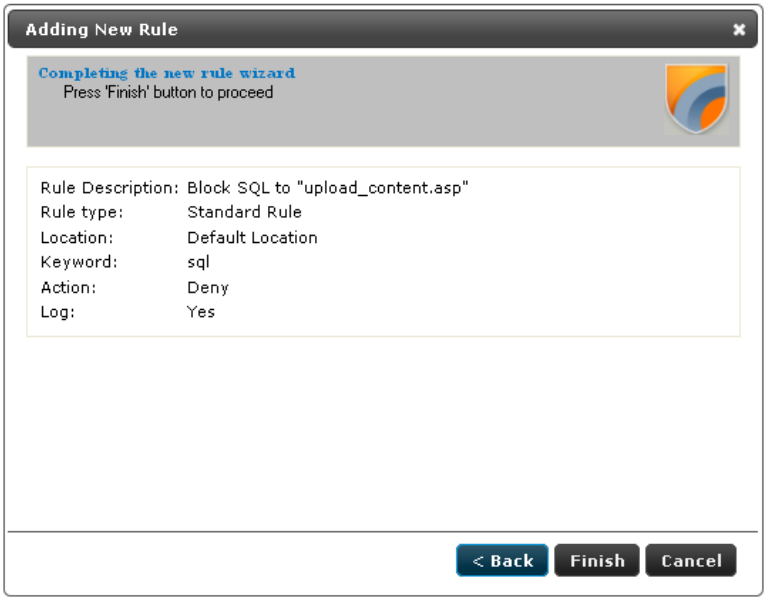
4. Click **Next** to continue. The Scope of Search window appears:



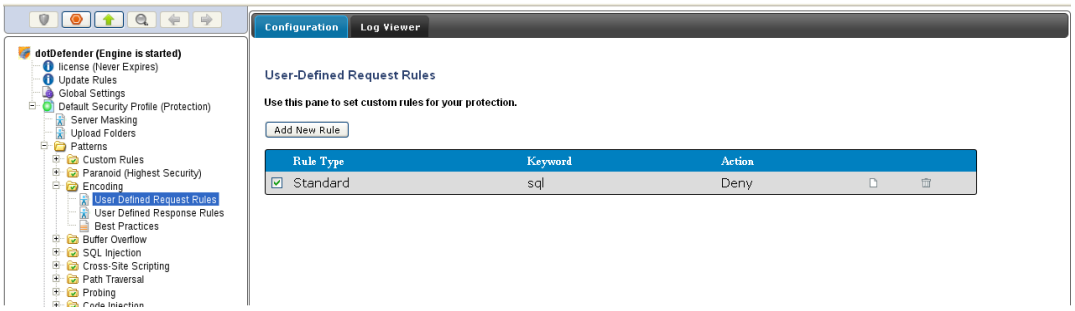
5. Select one of the following:

- **Apply to all pages**: dotDefender applies the search to all HTTP pages.
- **Apply to specific URI**: dotDefender applies the search to a specific URI. Enter the URI field.
- **Apply to all pages except this URI**: dotDefender applies the search to all HTTP pages, excluding the specified URI.

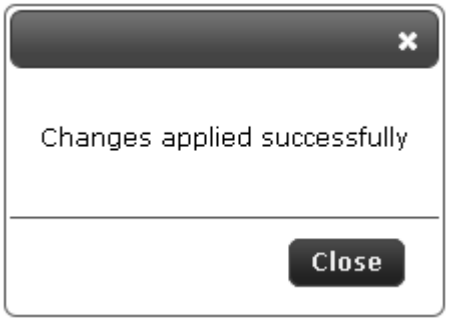
6. Click **Next**. The **Completing the New Rule Wizard** window appears:



7. Review the summary of the new rule. Click **Finish**. The new rule appears in the list of User-Defined Rules:



8. Click  to apply the changes. The following window appears:



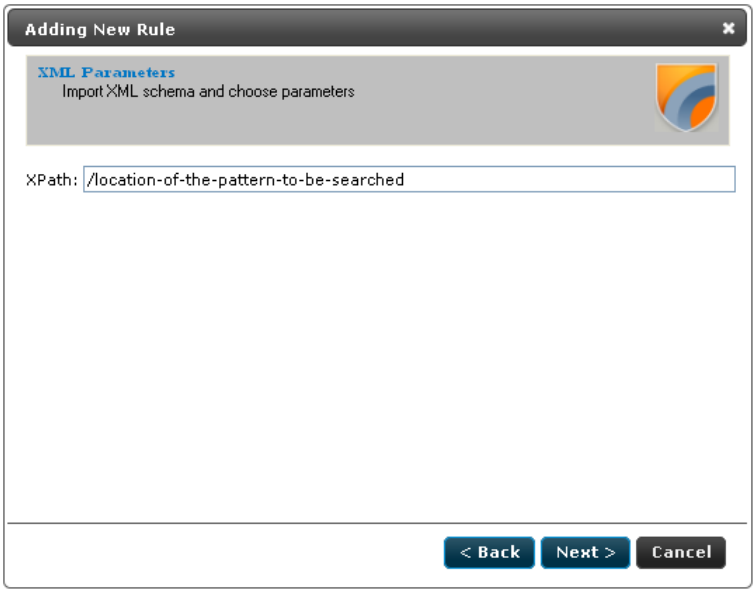
9. Click **Close**.

6.4.2.5 Searching in Custom Parameters of XML/SOAP Elements

Simple Object Access Protocol (SOAP) is a protocol for communication between applications and a format for sending messages via the Internet. SOAP is based on XML; it is platform and language independent, and it is a W3C recommendation.
A schema serves as a map of an XML structure. dotDefender recognizes two types of schemas: .XSD (commonly used for XML file structure maps) and .WSDL (used as an interface menu for Web Services)

To search in custom parameters of XML/SOAP elements:

1. The XML Parameters window appears:



2. Select **Element from schema** and set the schema properties as follows:

   ♋◑ Click **Import** to add a referable schema.

   ♌◑ Select a **.wsdl** or **.xsd** file and click **Open**. The file is added to the **Schema** area.

   ♍◑ Select the **Service** from the drop-down list.

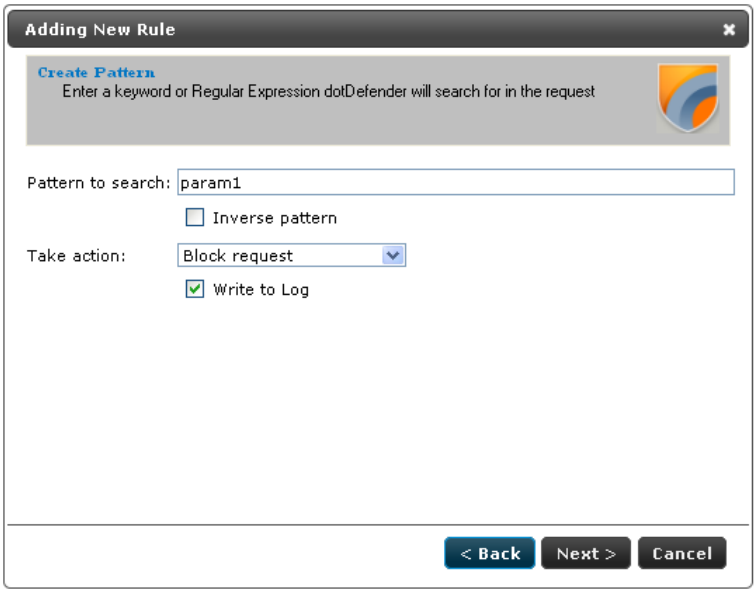
   ♎◑ Select the **Method** from the drop-down list.

   ♏◑ Select the **Element**.

3. Select **XPath** and enter the location of the pattern to be searched. This is an alternative to pointing out the location in the schema.

Note: When this option is selected, all **Element from Schema** fields are disabled.

4. Click **Next** to continue. The Create pattern window appears:



5. In the **Pattern to search** field, enter a regular expression representing a value to be blocked/allowed for the location selected in the **Adding New Rule – Completing the New Rule Wizard** window. For example, if REMOTE_ADDRESS has been selected, a regular expression representing the IP address to block or allow should be typed here.

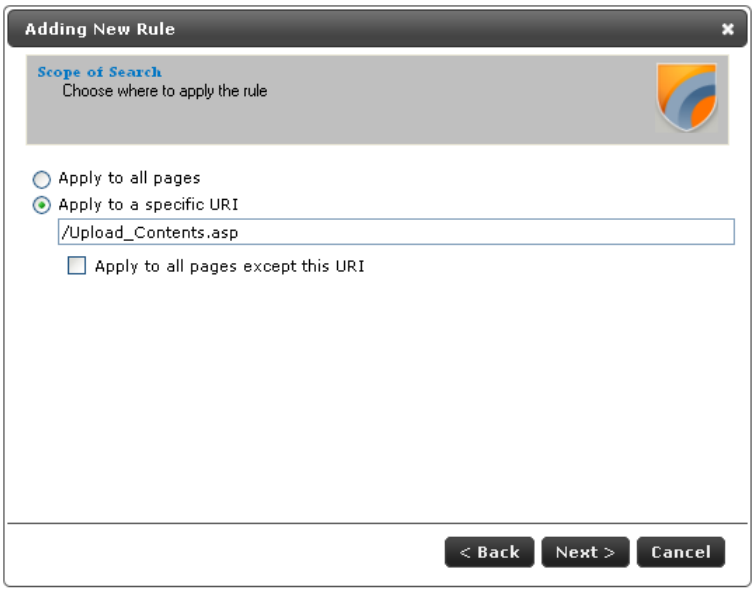
6. Enter a regular expression for which dotDefender looks in the HTTP request. For further information, see **Regular Expressions.**

7. From the **Take action** drop-down list, select the action to be taken when a pattern is matched:

   - **Block request:** dotDefender blocks HTTP requests containing the pattern.
   - **Allow request (Whitelist):** dotDefender allows requests containing the pattern.
   - **Monitor:** dotDefender only logs HTTP requests containing the pattern.
   - **Skip Category:** dotDefender excludes rules in this category for requests containing the pattern.

8. (Optional) Select **Write to Log** so that HTTP requests containing the pattern appear as Log events.

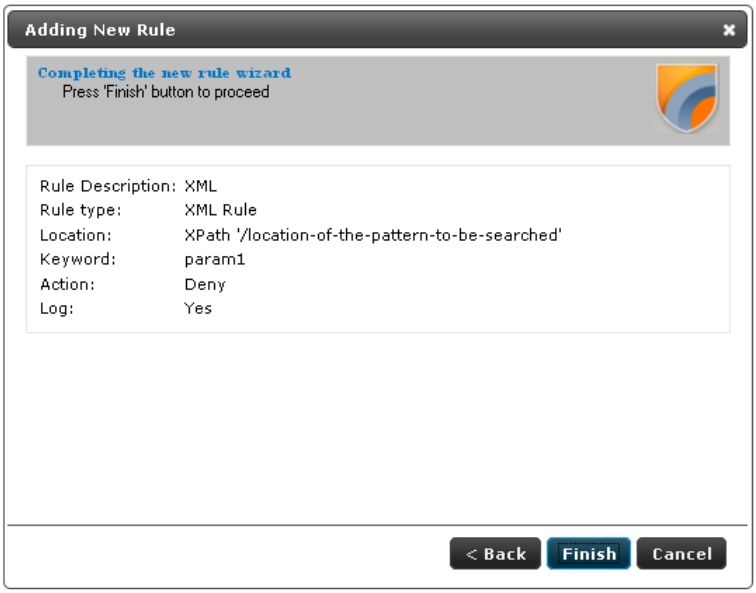
9. Click **Next**. The Scope of Search window appears:



10. Select one of the following:

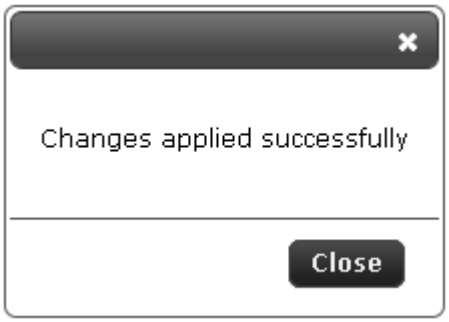
- **Apply to all pages**: dotDefender applies the search to all HTTP pages.
- **Apply to specific URI**: dotDefender applies the search to a specific URI. Enter the URI field.
- **Apply to all pages except this URI**: dotDefender applies the search to all HTTP pages, excluding the specified URI.

11. Click **Next**. The Completing the New Rule Wizard window appears:



Review the summary of the new rule. Click **Finish**.

12. Click  to apply the changes. The following window appears:



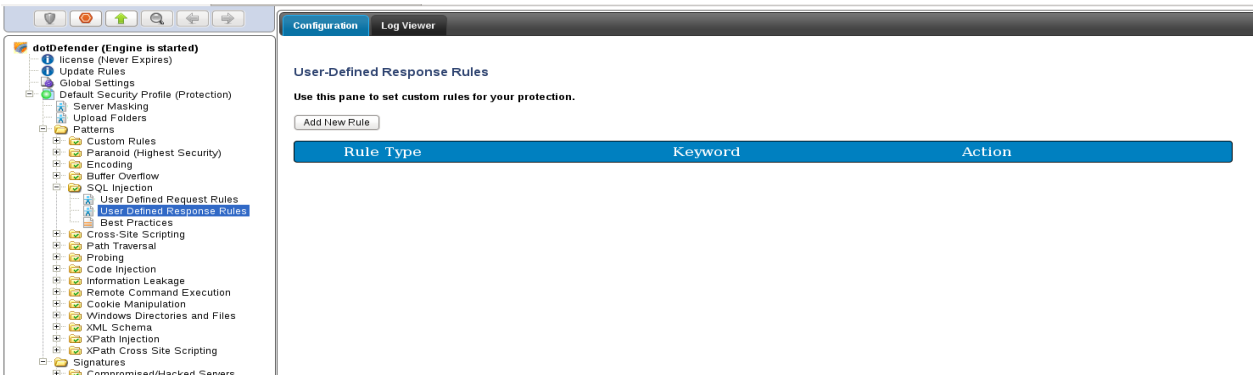
13. Click **Close**.

6.4.3 Adding User-Defined Rules for responses

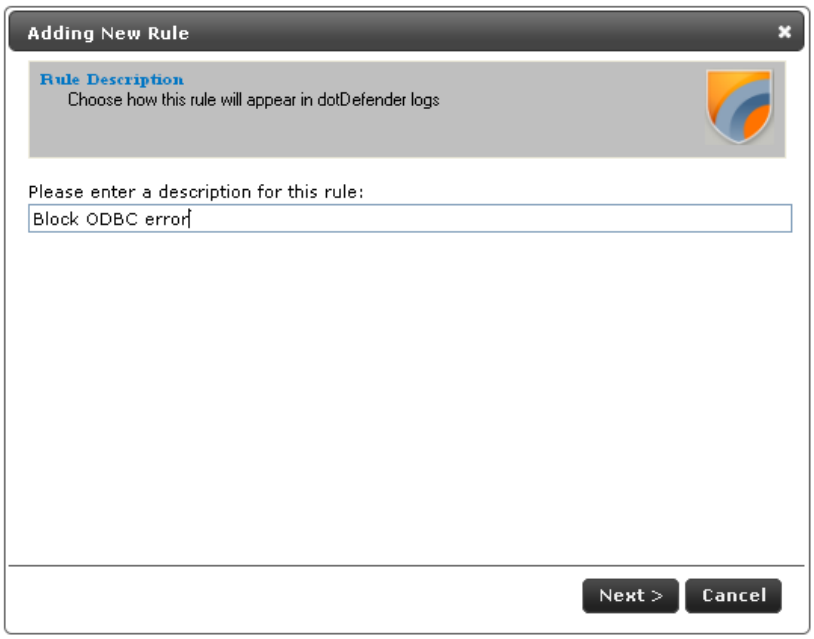
You can create new rules for dotDefender by using regular expressions to match a pattern that is to be blocked, allowed or monitored. The following instructions explain how to create a rule to block, allow, or monitor outgoing responses from the server.

To add a new rule:

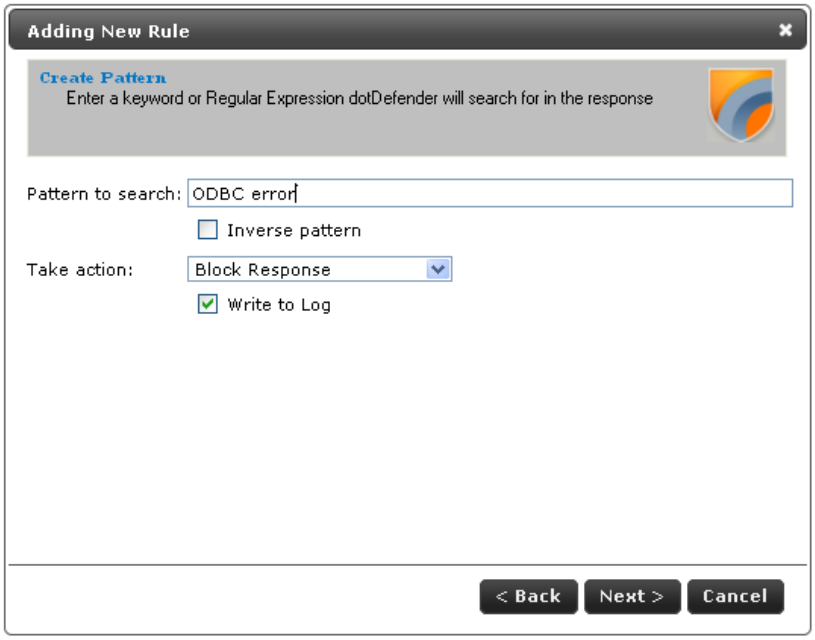
1. Click **User Defined Response Rules** in any category. The User-Defined Reponse Rules list appears in the right pane:



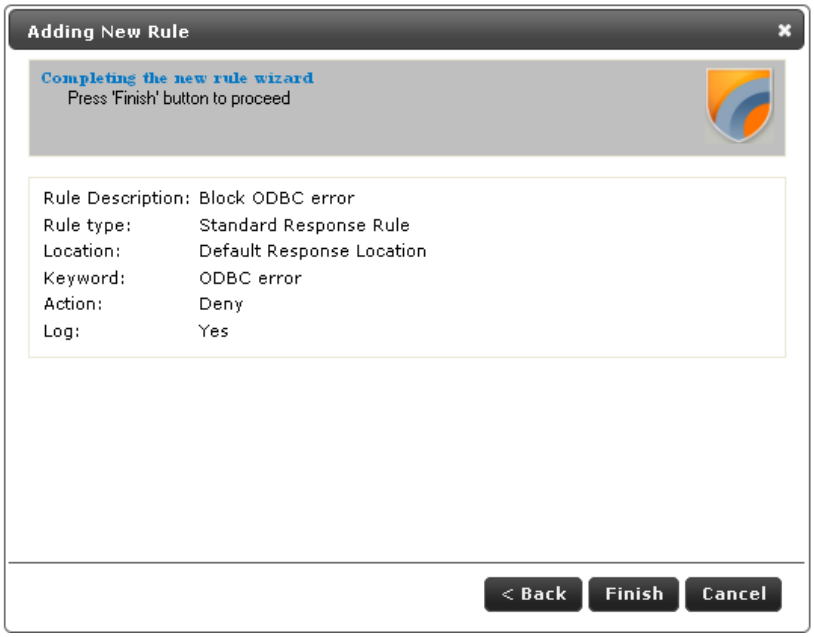
2. Click **Add New Rule**. The New Rule wizard appears:



3. Type a description for the rule. Click **Next**.

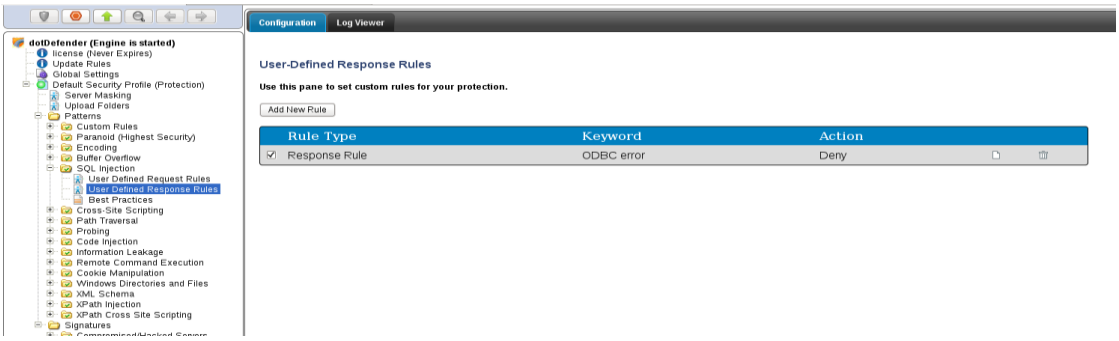


4. In the **Pattern to search** field, enter a regular expression representing a value to be blocked or allowed in the response. Click **Next**.

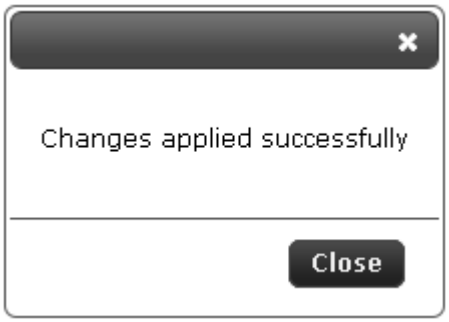


5. The Completing the New Rule Wizard window appears. Review the summary of the new rule. Click **Finish**.

- The new rule appears in the list of User-Defined Rules:



6. Click  to apply the changes. The following window appears:



7. Click **Close**.

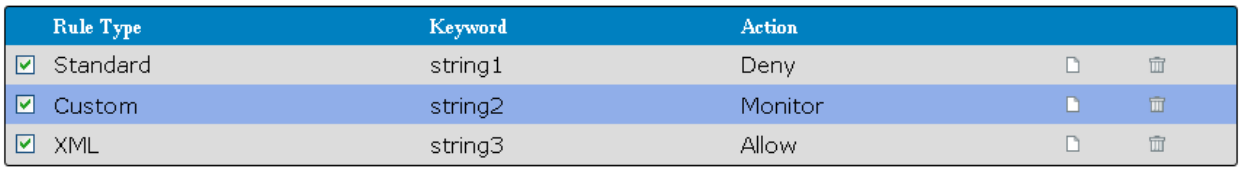
6.4.4 Managing the Rules

This section includes:

- Viewing the User-Defined Rules
- Enabling/Disabling a User-Defined Rule
- Deleting a User-Defined Rule
- Editing a User-Defined Rule

6.4.4.1 Viewing the User-Defined Rules

The User-Defined Rules appear in the right pane of the Administration Console. An example of three new Rule Types is shown below:



Rule Type	Keyword	Action
Standard	string1	Deny
Custom	string2	Monitor
XML	string3	Allow

- **Standard**: Created when the **Search in commonly attacked fields of HTTP requests** option is selected.
- **Custom**: Created when the **Search in custom fields of HTTP requests** option is selected.
- **XML**: Created when the **Search in custom parameters of XML/SOAP elements** option is selected.

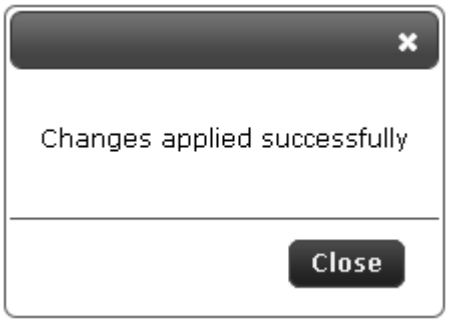
6.4.4.2 Enabling/Disabling a User-Defined Rule

You can enable or disable a User-Defined Rule.

Note: By default, every new rule defined is enabled (checkbox is selected).

To enable/disable a User-Defined Rule:

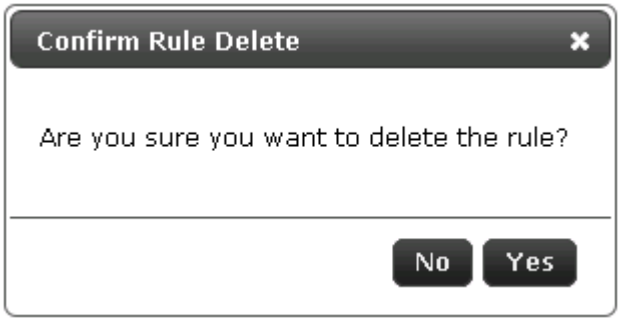
1. Click ☐/☑ to select/deselect a User-Defined Rule.
2. Click  for the changes to take effect. The following window appears:



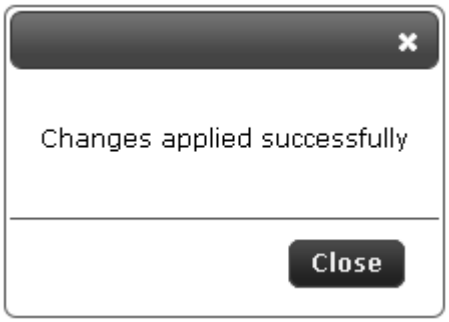
3. Click **Close**.

6.4.4.3 Deleting a User-Defined Rule

1. Click  to delete a User-Defined Rule. The following window appears:



2. Click **Yes**.
3. Click  for the changes to take effect. The following window appears:



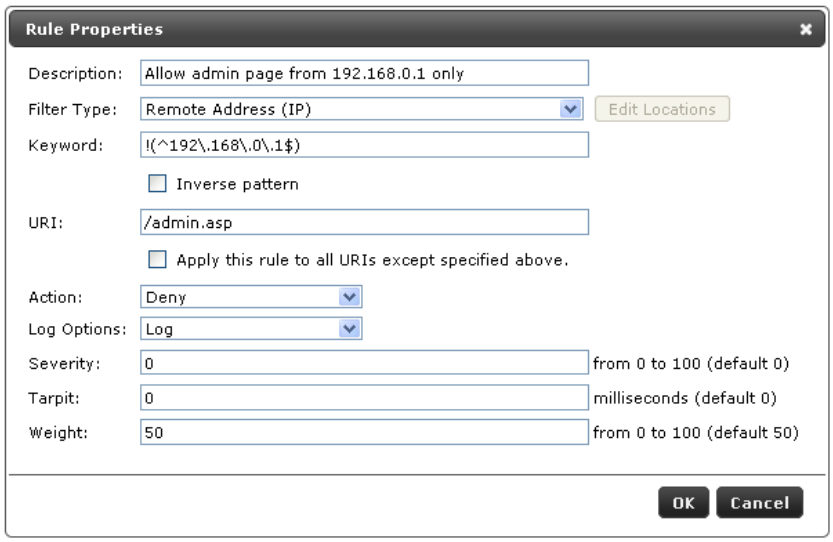
4. Click **OK**.

6.4.4.4 Editing a User-Defined Rule

This enables you to add additional fixed and dynamic locations and define Tarpit response latency.

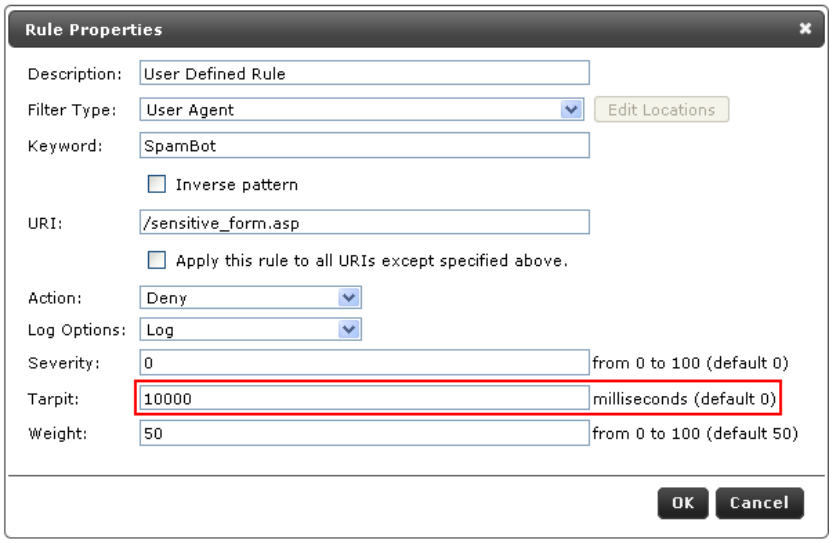
To edit a User-Defined Rule:

1. Click  next to the User-Defined Rule. The Rule Properties window appears:



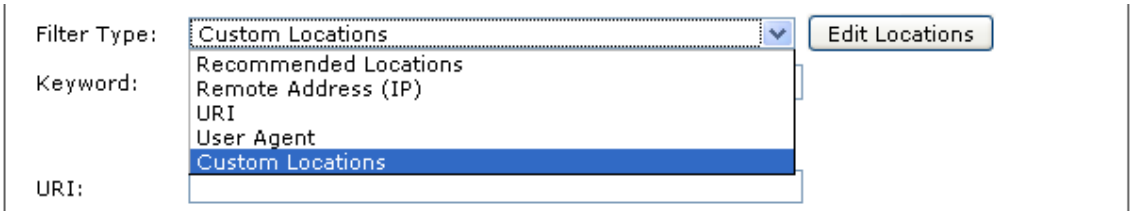
The example above demonstrates how to deny any IP address, excluding 192.168.0.1, from accessing a sensitive Web page. For additional information, see **Adding User-Defined Rules.**

2. Choose the required response latency by defining a value in milliseconds next to **Tarpit**. This option enables delaying rapid attacks, offloading the Web server.



The example above demonstrates how to slow down automatic spam bots from overloading a Web form. In the case that the bot is identified via the User-Agent header, it is denied access, while the response arrives 10 seconds (10,000 milliseconds) after the request has been received at the server side.

3. Select the required **Filter Type** from the list below:



Recommended Locations – Commonly attacked locations

Remote Address (IP) – The IP address of the connecting user

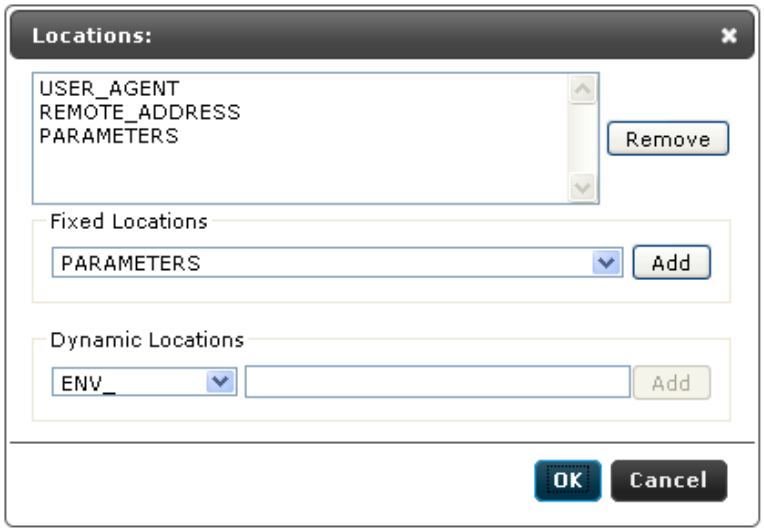
URI - The relative application URL address including parameters

User Agent – The client software identifier string

Custom Locations – Locations specified in the Edit Locations menu

- To edit and/or add specific locations, click Edit Locations. The Locations window appears, enabling you to add multiple locations.

Note: This option is available only when **Custom Locations** is selected.



- The Fixed Locations pre-defined fields are parsed for HTTP incoming requests. In the **Fixed Locations** area, select one of the following:

Field	Description
REMOTE_ADDRESS	IP address of the connecting user
REMOTE_HOST	Host of the connecting user
REMOTE_USER	Authenticated username on IIS
REQUEST_METHOD	HTTP request method. For example: GET, POST
PATH_INFO	The relative application URL address without parameters. For example: /registration/forms/register.asp
AUTH_TYPE	HTTP authentication type. For example: Basic Authentication
SERVER_NAME	Host name as appears in the HOST header. For example: www.applicure.com
SERVER_PROTOCOL	Name and revision of the information protocol via which the page was requested. For example: 'HTTP/1.1'.
FIRST_REQUEST_LINE	The first line of the full HTTP request, as received by IIS
UNPARSED_URI	The relative application URL address including parameters. For example: /registration/forms/register.asp?Form=reg
PARAMETERS	The string containing the parameter names and values
PARAMETERS_VALUES	Parameter values only
REQUESTED_ XML_VALUES	XML values only

Field	Description
USER_AGENT	A string identifying a browser or agent accessing a web page. For example: "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13 (.NET CLR 3.5.30729)" , "curl/7.15.5 (x86_64-redhat-linux-gnu) libcurl/7.15.5 OpenSSL/0.9.8b zlib/1.2.3 libidn/0.6.5"
SCRIPT_NAME	A variable that should be a part of a URI path (not URL-encoded) which could identify the CGI script (rather than the script's output).
URI	A URI is the way to identify any of those points of content, whether it be a page of text, a video or sound clip, a still or animated image, or a program. A URI typically describes The mechanism used to access the resource, specific computer that the resource is housed in and specific name of the resource (a file name) on the computer.
RECOMMENDED	Commonly attacked locations.

4. Click **Add**. The fixed location is added. Repeat this step to add more fixed locations.

- The Dynamic Locations are environment variables. In the **Dynamic Locations** field, select one of the following:

Field	Description
ENV	OS environment variable, such as Path, Computer Name, Home Directory, Current User, Windows Directory
HEADER	HTTP Header Name
PARAMETER	GET or POST parameter name
COOKIE	Name of cookie
XML	One of the XML parameters

5. Enter the required dynamic location information.
6. Click **Add**. The dynamic location is added. Repeat steps 6 and 7 to add more dynamic locations.
7. Click **Close**. The Rule Properties window appears.
8. Click **OK**.
9. Click  to apply the changes.

6.5 Managing Signatures

You can enable or disable a Signature category. Rules are not created for Signatures. The Signatures that dotDefender inspects include the following:

- Comprised/Hacked Servers
- Anti-Proxy Protection
- Known-Worms Signatures
- Bad User-Agents Signatures
- Known Spammer Crawlers
- MPack Protection

To view an explanation of a signature category:

1. In the left pane of the Administration Console, expand the required profile.
2. Expand **Signatures**.
3. Select a Signature category. The description appears in the right pane.

To enable/disable a signature category:

1. In the left pane of the Administration Console, select the required Profile.
2. Expand **Signatures**.
3. Right-click on the signature category and select **Disable/Enable**. The signature category is either enabled or disabled.

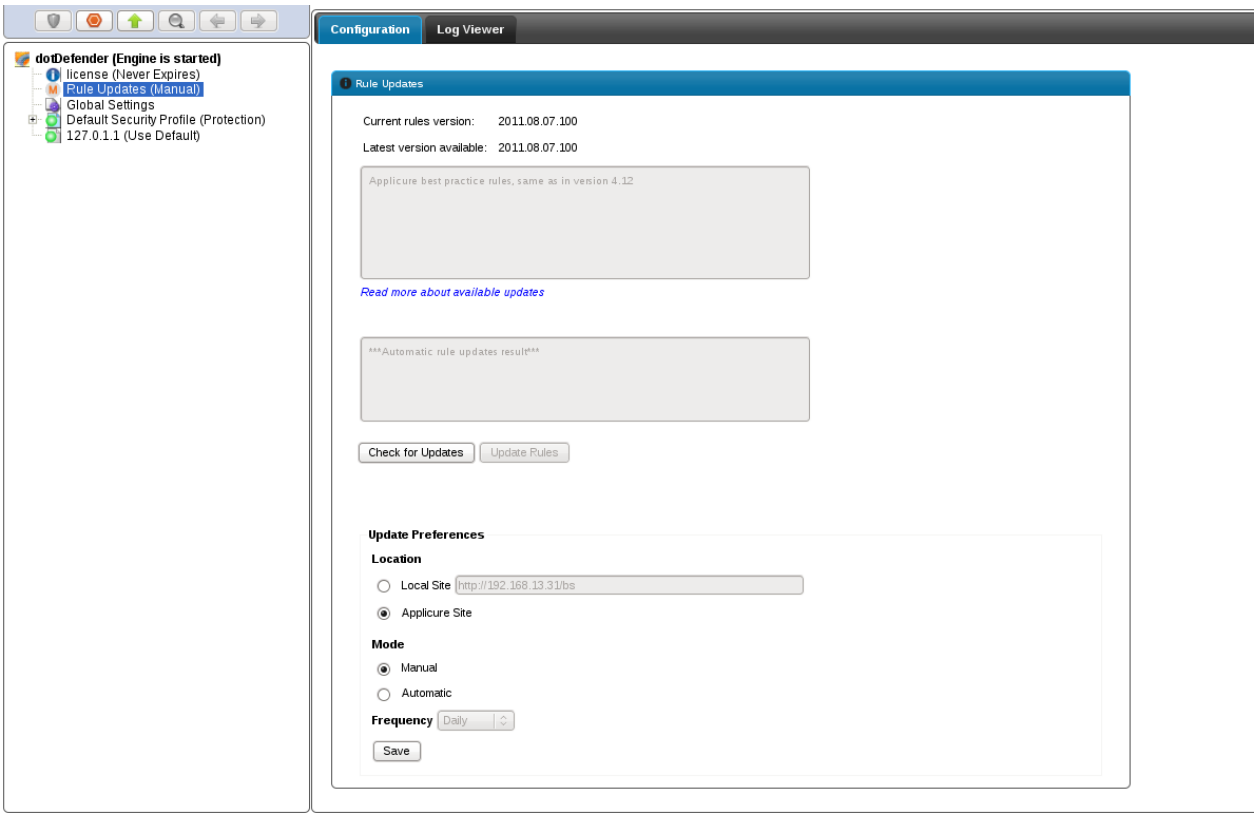
6.6 Rule Updates

The “Rule Updates” feature provides the ability to have dotDefender's Best Practices up-to-date with the latest available version of Rule Updates, without the need of upgrading dotDefender.

New security rules for strengthening protection will be available for download from either Applicure's website or a specific URL (for servers with limited access).

In addition, this feature provides the ability to select whether to update dotDefender's Best Practices automatically or manually.

In order to see the Rule Updates screen, click on “Rule Updates”in the tree on the left-hand side pane.
Each icon next to “Rule Updates” has a special meaning 



In the left-hand side pane, select **Rule Updates**.
The right pane opens the Rule Updates area.

- **Rule Updates** (upper section):

Current Rules Version – Shows the current version number of Rule Updates.

Latest Version Available– Shows the latest Rule Updates version available.

- **Update Preferences:**

Location: Local Site – Download from a custom location.

This option will probably be required for servers will limited access to internet.

Location: Applicure Site – Download from Applicure's website.

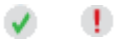
Mode: Manual – Checks for updates by clicking the button “Check for Updates”.

When this option is selected, the Rule Updates icon on the left-hand side pane will show

Users will click the “Check for Updates” button to check for the latest version available.

If the “Update Rules” button is ***enabled*** - click it to download the latest version.

Mode: Automatic – Checks for updates are being done automatically. Users will choose from the drop-down box the **frequency** of these checks (every one day, three days, one week, one month or three months).



When this option is selected, the Rule Updates icon on the left-hand side pane will show either or

- If dotDefender is up-to-date, the icon will show 
- If dotDefender is not up-to-date, or failed to download the latest available version, the icon will show

- After changes have been made, click “**Save**” for changes to take effect.

7

Configuring Global Settings

This chapter explains the server wide settings available in dotDefender
This chapter contains the following sections:

- (Windows)Enabling/Disabling logging to Windows Event Logs
- Enabling/Disabling NAT support
- Updates

7.1 (Windows) Enabling / Disabling logging to Windows Event Logs

To enable the global logging across websites:

1. In the left pane of the Administration Console, select **Global Settings**. The right pane opens the Global Settings area:

2. Select the **Write to Local Event Log** option to enable the logging globally.

3. Click  to apply the changes.

7.2 Enabling / Disabling NAT Support

The NAT support feature allows dotDefender to properly identify client IP addresses while working behind a NAT device such as a load balancer, proxy, or firewall. Using the X-Forwarded-For HTTP header, the frontend device communicates the original client address as seen within the request.

To enable NAT support:

1. In the left pane of the Administration Console, select **Global Settings**. The right pane opens the Global Settings area:

2. Select the **Follow X-Forwarded-For headers behind a NAT device** option to enable global identification of all remote client addresses behind NAT.

3. Click  to apply the changes.

8

FAQs and Troubleshooting

This chapter contains the following sections:

- FAQs (Frequently Asked Questions)
- Troubleshooting

8.1 FAQs

The following list includes some of the questions that are frequently addressed to technical support:

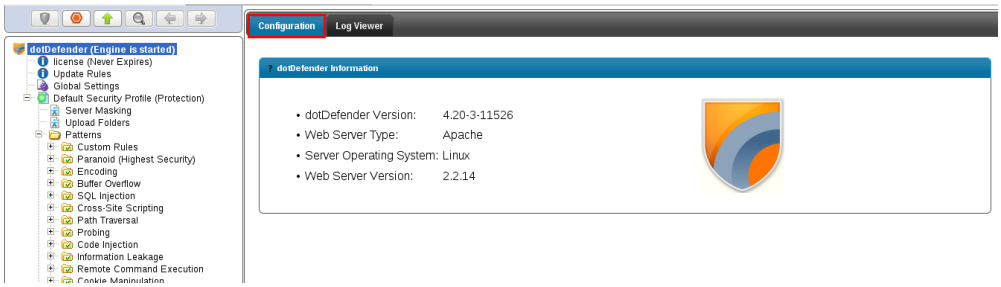
- How do I allow an IP address, or a range of IP addresses?
- How do I identify and control access to the website, according to Windows users (using the Remote User field)?
- How do I enable updates to work through a firewall?
- How do I change the database size limit (Windows)?
- How do I change the database size limit (Linux)?
- What is a “bad” User-Agent and why is dotDefender blocking some browsers for it?
- How do I let one "good" User-Agent pass through?
- What can I do if the database is taking up too much space?
- What is a Proxy attack?
- How do I turn a False Positive into a Whitelist Rule?
- Does a user-defined rule still undergo inspection?
- How do I back up the rule set (Windows)?
- What should I backup for upgrade (Linux)?
- How do I clear the Event Log?
- I have scripts on a website that are blocked for usage by end-users. How do I allow the scripts to run?
- After I installed dotDefender, I am getting blocked at a content upload page, and I cannot upload new content.

8.1.1 How do I allow an IP address, or a range of IP addresses?

To allow an IP address or a range of IP addresses, add a User-Defined Rule. For further information on the regular expressions, see **Regular Expressions.**

Note: This IP address or range of IP addresses will be white-listed for all rules.

1. Click the Configuration tab on the right pane.



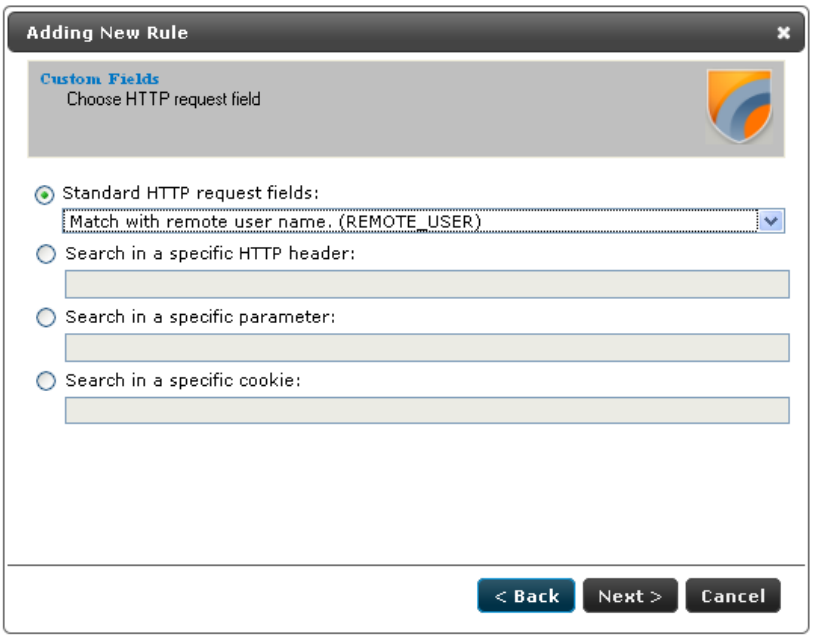
2. Expand the required Profile.
3. Expand **Patterns**.
4. Expand **Custom Rules**.
5. Click **User Defined Request Rules**.
6. In the right pane, click **Add New Rule**.
7. In the Rule Description window, enter a description for the rule and click **Next**.
8. In the Rule Type window, select **Search in client remote address** and click **Next**.
9. To white-list one IP address, in the Create Pattern window, enter the IP address beginning with the caret sign and ending with the dollar sign and add backslashes before each dot (since this is a regular expression field). For example, to white-list the IP 192.168.200.100, enter:
   ^192\.168\.200\.100$
10. To white-list a range of IP addresses, in the Create Pattern window, enter a regular expression representing the range. For example, to white-list the range 10.20.54.0-10.20.68.255, enter:
    ^10\.20\.((5[4-9])|(6[0-8]))\.(([0-9])|([1-9][0-9])|(1[0-9][0-9])|(2[0-4][0-9])|(25[0-5]))$
11. In the same window, in the **Take Action** field, select **Allow** and choose whether to log all events for the IP or not.
12. Click **Next**.
13. In the Scope of Search window, click **Next** and then click **Finish**.

14. Click  for the settings to take effect. The following window appears:

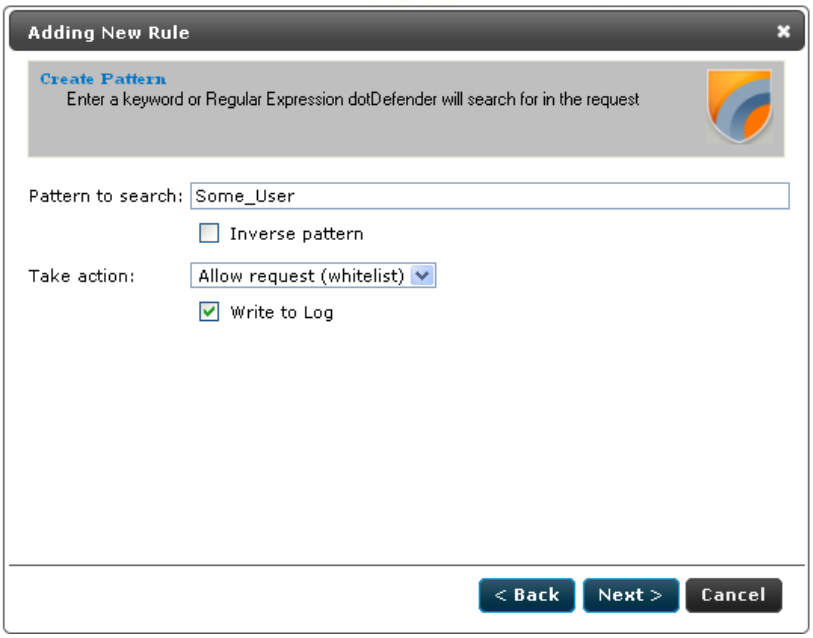
15. Click **OK**.

8.1.2 How do I identify and control access to the website, according to Windows users (using the Remote User field)?

1. Create a new rule (see **Adding User-Defined Rules**).
2. From the **Standard HTTP request fields** drop-down list, select **Match with Remote user name**:



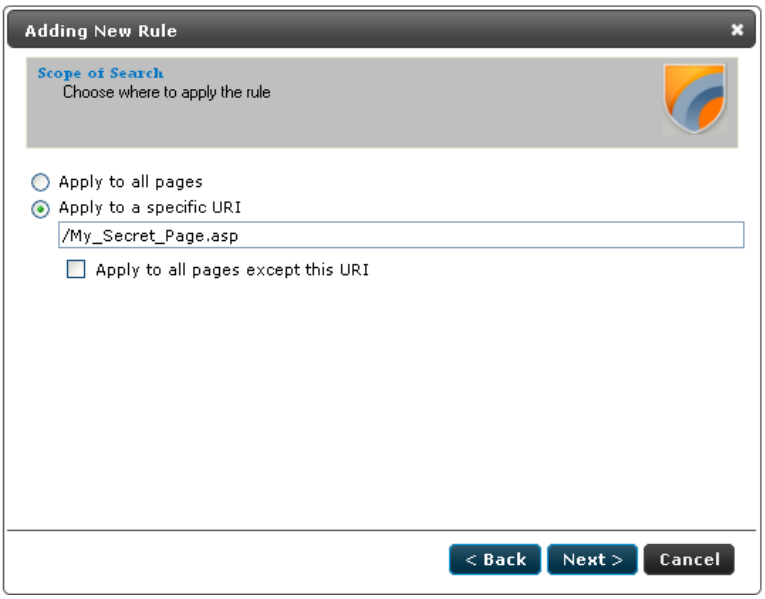
3. Click **Next**. The Create pattern window appears:



4. In the **Pattern to search** field, enter the name of the Windows user who should have access to the site.

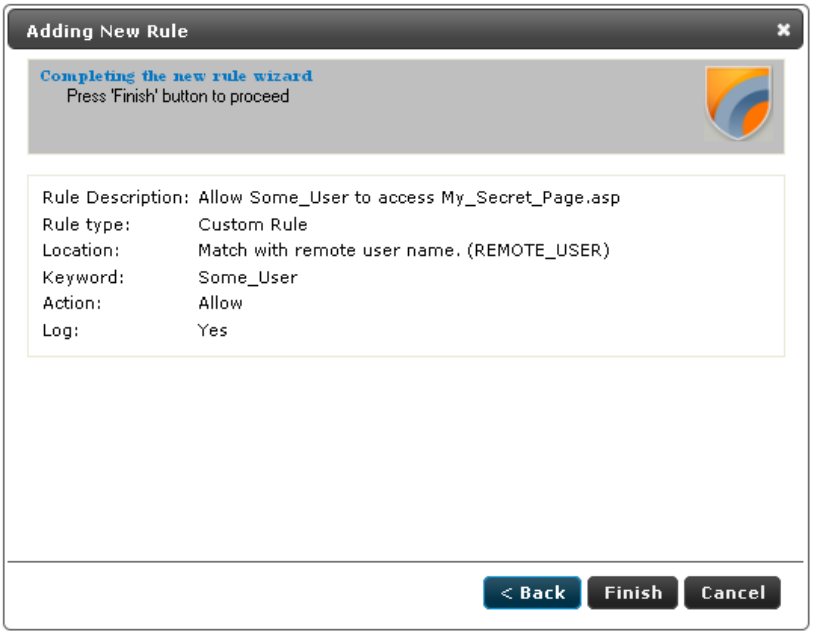
5. From the **Take action** drop-down list, select **Allow request (Whitelist)**. This removes protection for this user.

6. Click **Next**. The Scope of Search window appears:



7. In the **Apply to specific URI** field, enter the page or path that this user can access. This is defined using a regular expression. For further information, see **Regular Expressions**.

8. Click **Next**. The Completing the New Rule Wizard window appears:



This rule allows access to **My_Secret_Page.asp** to the Windows user "**Some_user**".

8.1.3 How do I enable updates to work through a firewall?

- Open port 80 in the firewall for the following addresses:
  - **services.installshield.com**
  - **updates.applicure.com**

8.1.4 How do I change the database size limit (Windows)?

The dotDefender Log Service (**aclogsvc**), checks the database (**aclogsvc.ddb**) every 500 events (Registry key: **LogTruncateCheckFrequency**).

If the number of events reaches 15,000 (Registry key: **LogTruncateMaxCount**) it deletes 10% of the items in the database (Registry key: **LogTruncateCountDivider**), while using the First In First Out method (deleting old events first).

Each event (Record) logged in the database is limited to approximately 64 KB.

Potentially the size of the database can reach approximately 1 GB, when using the default values: 64 KB * 15,000 = ~ 1 GB.

The parameters are configurable in the registry:

[HKEY_LOCAL_MACHINE\SOFTWARE\Applicure\dotDefender\aclogsvc]

"LogTruncateCheckFrequency"=500

"LogTruncateMaxCount"=15000

"LogTruncateCountDivider"=10

Make these changes in the registry and then restart dotDefender Log Service for the settings to take effect.

8.1.5 How do I change the database size limit (Linux)?

dotDefender log service checks the database(dotDefender_db.sqlite) every 500 events. If the number of events reaches 60,000, retains 90% of the items in the database (54,000 events), while using the First In First Out method (deleting old events first). This values can be edited in the /usr/local/APPCure/etc/dotDefender_logd.conf file, Where **"HIGH"** stands for maximal number of events, **"LOW"** for number of events retained after deletion, and **"SLEEP"** for time (In seconds) to wait before checking database limit.

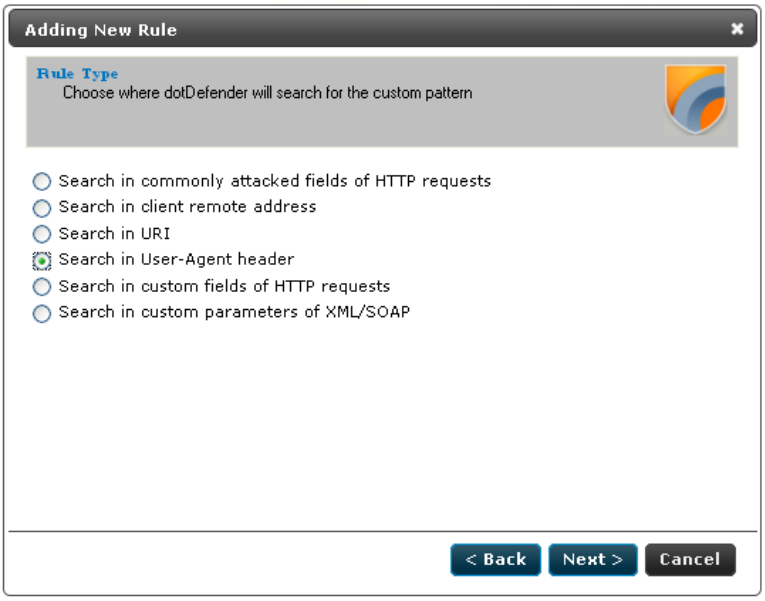
8.1.6 What is a "bad" User-Agent and why does dotDefender block certain browsers?

A User-Agent is an HTTP header, containing a string identifying the software being used by the client to connect to the website. For example, this might be Internet Explorer, Mozilla Firefox, Nokia, or Motorola cellular phones. The Bad User-Agents database is a very effective mechanism for distinguishing legitimate surfers from automatic, malicious tools meant for scanning and attacking the website. There are borderline situations where a component that has been used by malicious software is also used in legitimate software, especially in auto scripts and bots, for example, Indy library. In this case, see **How do I let one "good" User-Agent pass through?**

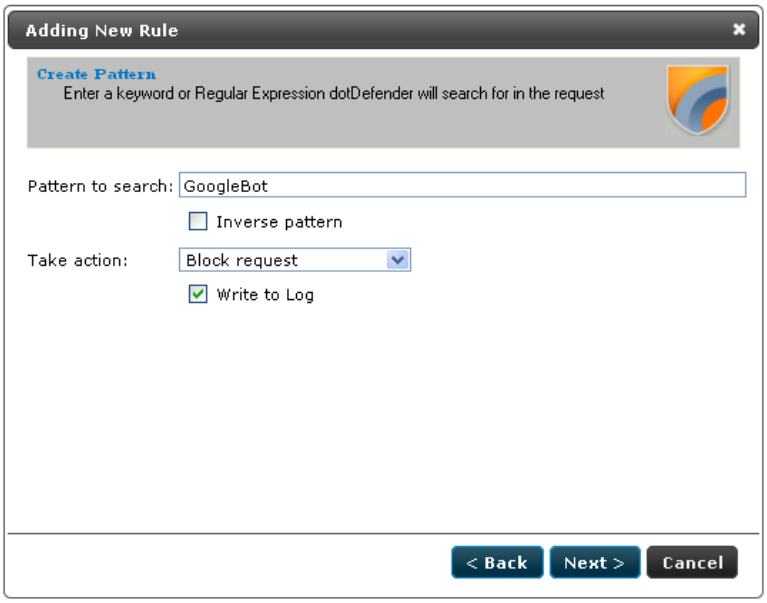
8.1.7 How do I let one "good" User-Agent pass through?

Sometimes there is a borderline situation where an automatic tool is essential and harmless to the Website. In this case, you can use the Whitelist to allow a specific User-Agent through by defining this User-Agent string under **User-Agent header**.

1. Create a new rule (see **Adding User-Defined Rules**). The Rule Type window appears:



2. Select **Search in User-Agent header**, and click **Next**. The Create pattern window appears:



3. In the **Pattern to search** field, enter the User-Agent string (preferably under a specific URL only).

8.1.8 What can I do if the database is taking up too much space?

See **Deleting the dotDefender Log Database File**.

8.1.9 What is a Proxy attack?

A proxy attack is an attempt to use your Web server as a jumping point to attack other sites.

8.1.10 How do I turn a False Positive into a Whitelist Rule?

See **Adding User-Defined Rules**.

8.1.11 Does a User-Defined rule still undergo inspection?

In the Create Pattern window, you can define the policy as:

- **Deny**: dotDefender for IIS denies this HTTP request.
- **Allow**: dotDefender for IIS stops checking the HTTP request, and allows it to enter the server.
- **Monitor**: dotDefender for IIS monitors this request, without intervening.

8.1.12 I am upgrading. How do I back up the rule set (Windows)?

You can only back up the Default Security Profile. Central Management allows Default Security Profile replication between different servers.

1. In the Registry, HKEY_LOCAL_MACHINE\SOFTWARE\Applicure\dotDefender > Sites > 0. 0 represents the Default Security Profile.
2. Right-click and select **Export**.
3. Save the file as type **.backup**.
4. After you have upgraded, double-click the backup file, and when prompted to export the file, click **Yes**.

8.1.13 I am upgrading. What should I backup (Linux)?

Simply copy the folder /usr/local/APPCure/etc, which contains all the information needed, including configuration files, logs and license file. After the upgrade, copy the backup to the same directory on the server.

8.1.14 How do I clear the Event Log?

See **Clearing the Applicure Windows Event Log**.

8.1.15 I have scripts on a website that are blocked for usage by end-users. How do I allow the scripts to run?

See **Modifying Best Practices**.

Note: If this method does not work, select **Patterns > Windows Directories and Files > Best Practices > Test Scripts**, and select **Disable**.

1. In the required profile, select Patterns > Windows Directories and Files > Best Practices > Test Scripts.
2. Click **Edit**  . The Rule Properties window appears.
3. In the **URI** field, enter the directory (URI) that should not be blocked.
4. From the **Action** drop-down list, select **Allow**.
5. Select **No log**.
6. Click **OK**.
7. Click  to apply the changes.

8.1.16 I have a content upload page, and I cannot upload new content.

1. In the Log Viewer, click the **Search** icon  .
2. Select **Reference ID** and enter the Reference ID that you received on the Error Page.
3. Click **Search**. The URL of the upload page appears.
4. Focus specifically on the categories **Classic SQL**, **SQL Comments**, and any category of **Cross Site Scripting**.
5. Examine the Log Viewer for any alerts for these categories.
6. Notice the URL of the content upload page.
7. Create a User-Defined rule for **SQL** and **Cross Site Scripting** for this site. See **Adding User-Defined Rules**.

8.2 Troubleshooting

This section describes errors and how to solve them. The action(s) to be taken to resolve each problem are provided in the order of priority. To resolve each problem, start with step one and continue to the next until the problem is solved.

8.2.1 System Requirements

- dotDefender supports IIS Servers Web servers 6.x and higher.
- dotDefender supports the following operating systems:
  - Windows 2008
  - Windows 2003: Service Pack 1 and the latest Windows updates

9

Regular Expressions

dotDefender supports regular and extended regular expressions.
This chapter contains the following sections:

- POSIX Basic Regular Expressions
- POSIX Extended Regular Expressions

9.1 POSIX Basic Regular Expressions

Expression	Description
.	Matches any single character. For example, a.c matches "abc", etc.
[ ]	A bracket expression. Matches a single character that is contained within the brackets. For example, [abc] matches "a", "b", or "c". [a-z] specifies a range which matches any lowercase letter from "a" to "z". These forms can be mixed: [abcx-z] matches "a", "b", "c", "x", "y", or "z", as does [a-cx-z].
[^]	Matches a single character that is not contained within the brackets. For example, [^abc] matches any character other than "a", "b", or "c". [^a-z] matches any single character that is not a lowercase letter from "a" to "z".
^	Matches the starting position within the string.
$	Matches the ending position of the string or the position just before a string-ending newline.
\(\)	Defines a marked subexpression. The string matched within the parentheses can be recalled later (see the next entry, \n).
\n	Matches what the nth marked subexpression matched, where n is a digit from 1 to 9.
*	Matches the preceding element zero or more times. For example, ab*c matches "ac", "abc", "abbbc", etc. [xyz]* matches "", "x", "y", "z", "zx", "zyx", "xyzzy", and so on. \(ab\)* matches "", "ab", "abab", "ababab", and so on.

Expression	Description
\{m,n\}	Matches the preceding element at least m and not more than n times. For example, a\{3,5\} matches only "aaa", "aaaa", and "aaaaa".

9.2 POSIX Extended Regular Expressions

POSIX	Perl	ASCII	Description
[:alnum:]		[A-Za-z0-9]	Alphanumeric characters
[:word:]	\w	[A-Za-z0-9_]	Alphanumeric characters plus "_"
	\W	[^\w]	non-word character
[:alpha:]		[A-Za-z]	Alphabetic characters
[:blank:]		[\t]	Space and tab
[:cntrl:]		[\x00-\x1F\x7F]	Control characters
[:digit:]	\d	[0-9]	Digits
	\D	[^\d]	non-digit
[:graph:]		[\x21-\x7E]	Visible characters
[:lower:]		[a-z]	Lowercase letters
[:print:]		[\x20-\x7E]	Visible characters and spaces
[:punct:]		[-!"#$%&'()*+,./:;<=>?@[\\\]_`{|}~]	Punctuation characters
[:space:]	\s	[\t\r\n\v\f]	Whitespace characters
	\S	[^\s]	non-whitespace character
[:upper:]		[A-Z]	Uppercase letters
[:xdigit:]		[A-Fa-f0-9]	Hexadecimal digits

10

Appendix

This chapter contains the following sections:

- Specific Windows files and features
- Specific Linux/Unix files and features

10.1 Specific Windows files and features

10.1.1 Managing dotDefender Events in the Windows Event Viewer

This section includes the following topics:

- dotDefender Windows Event logs Overview
- Viewing Applicure Events
- Viewing dotDefender Audit Events
- Setting the Event Log Size
- Saving the Applicure Windows Event Log
- Clearing the Applicure Windows Event Log

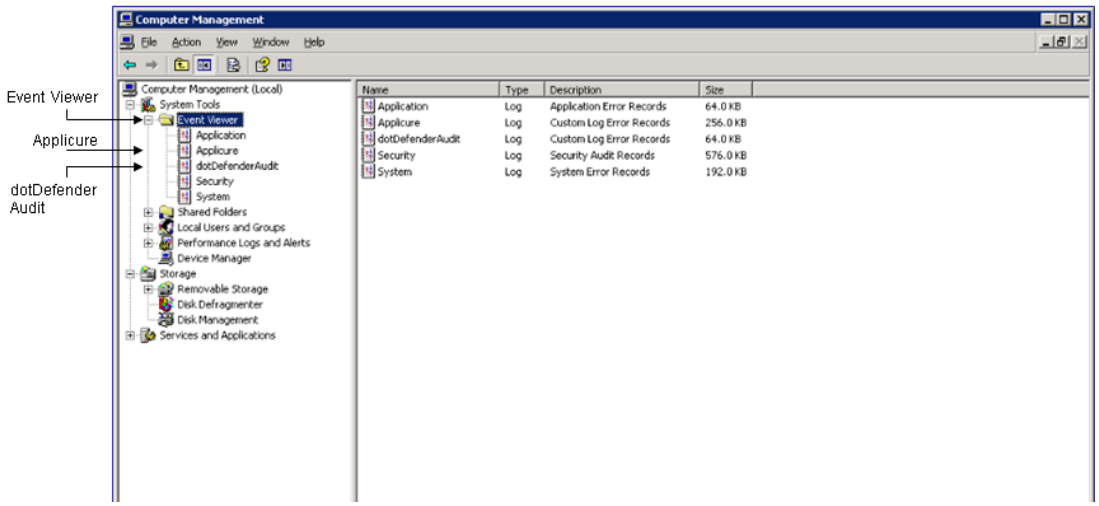
dotDefender Windows Event logs Overview

Note: To enable server wide logging to Windows Event Logs, see **Enabling / Disabling Logging to Windows Event Logs**

dotDefender adds the following branches to the Windows Event Viewer:

- **Applicure:** Records security events.
- **dotDefender Audit:** Records dotDefender filter status.

Right-click on "**My Computer**" and select "**Manage**".
The **Computer Management** window appears:



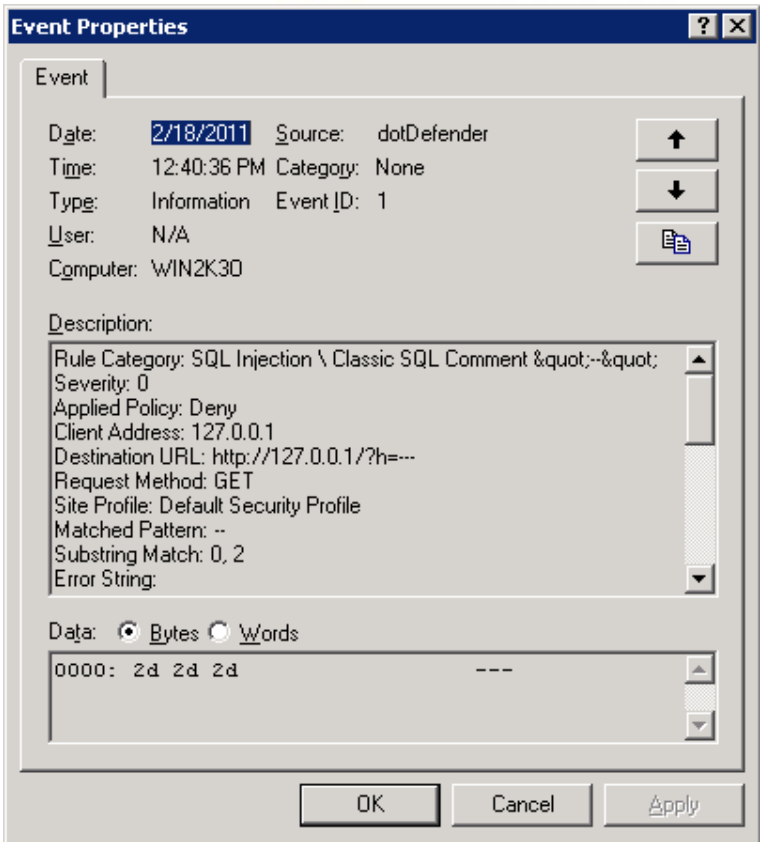
10.1.1.1 Viewing Applicure Events

The **Applicure** branch contains dotDefender security events.

To view Applicure events:

In the left pane of the **Computer Management** window, expand **System Tools,** expand **Event Viewer** and select **Applicure**.

Double-click or right-click an event and select **Properties**. The **Information** Properties window appears:



The information for each attack includes the following:

- Date and Time
- Source of event
- Category and type of event
- Event ID
- User
- Computer (server)
- Description of attack with Rule Category and sub-category
- IP address of attack
- Destination URL
- Request Method
- Name of Security Profile
- Matched Pattern
- Substring that caused error

- HTTP Headers, such as User Agent and Cookie
- HTTP Body

10.1.1.2 Viewing dotDefender Audit Events

Overview

dotDefender keeps two audit trace logs that reflect the status and policy changes in the security policy of each website as required by the PCI regulation. These status messages are divided into two logs:

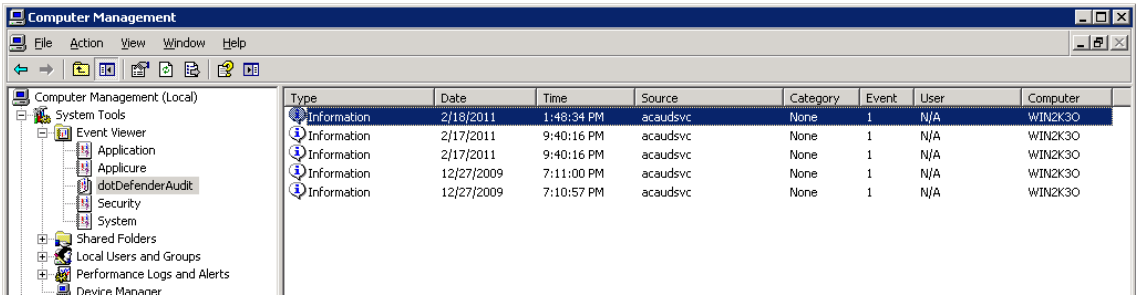
1. **dotDefenderAudit Windows Event Log** – ISAPI filter status

2. **Policy Change Log** – All changes made via dotDefender Administration Console (See **Viewing policy changes in the audit log file**)

dotDefenderAudit is a watchdog service that polls dotDefender for any status changes. The information on any change in **Operating Mode** includes the date and time of change, designating dotDefenderAudit as the source, the Event ID, and the computer.

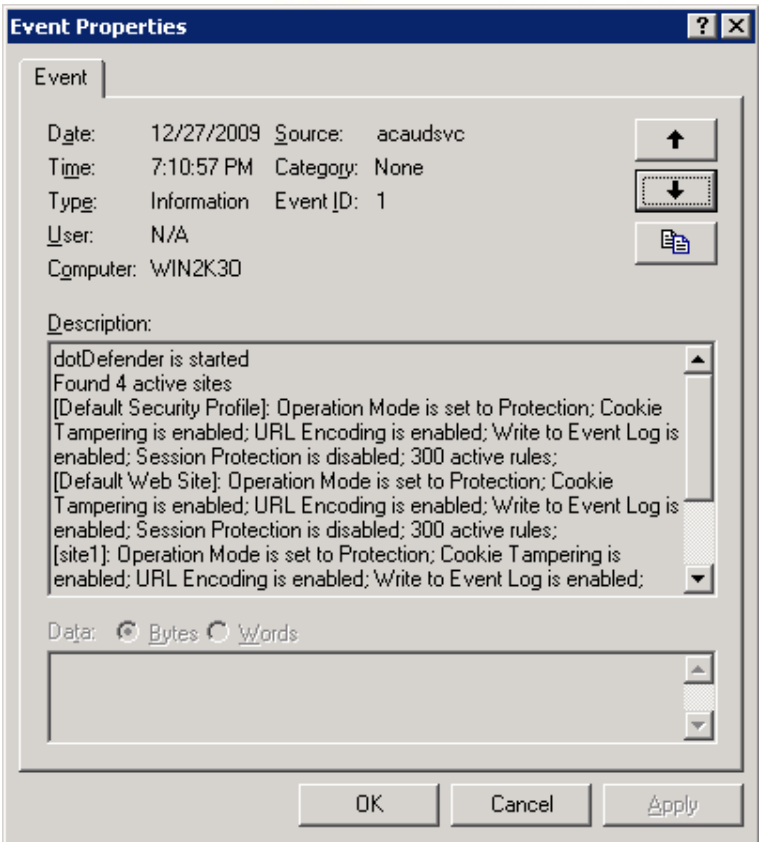
To view detailed dotDefenderAudit events:

In the left pane of the **Computer Management** window, expand **System Tools,** expand **Event Viewer** and select **dotDefenderAudit**:



Double-click or right-click an event. The right pane expands to show the Audit events.

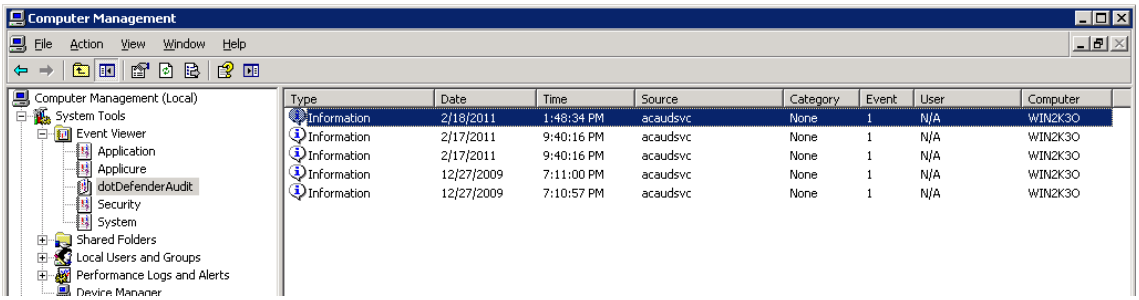
Select **Properties** to display an explanation of the event:



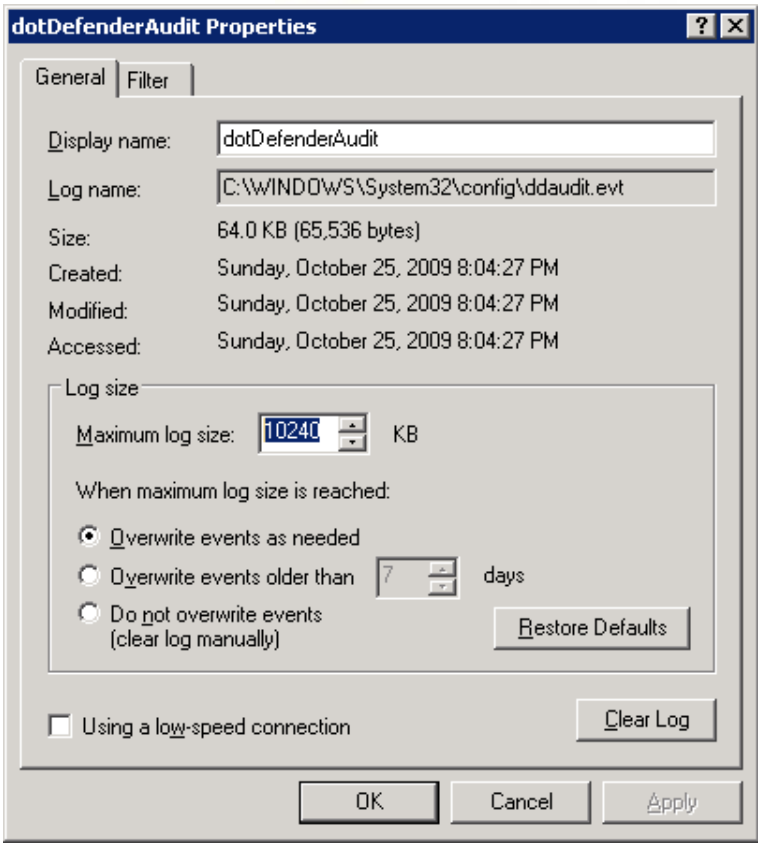
10.1.1.3 Setting the Event Log Size

To set the Event log size:

1. In the left pane of the **Computer Management** window, expand **System Tools** and expand **Event Viewer**:



2. Right-click on **dotDefenderAudit** or **Applicure**, and select **Properties**:



3. Set the **Maximum log size**.

4. The overwrite options in the **When maximum log size is reached** area specify what happens when the log size limit is reached. Select one of the following options:

   - **Overwrite events as needed:** When the log is full, the newest event replaces the oldest event.
   - **Overwrite events older than days:** Specifies the number of days before a log can be overwritten.
   - **Do not overwrite events (clear log manually):** If the maximum log file is reached, new events are discarded**.**

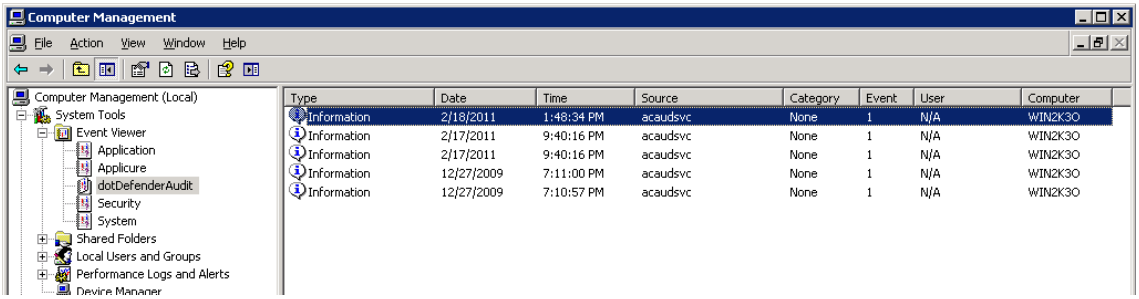
5. Click **OK**. The log file settings are changed.

10.1.1.4 Saving the Applicure Windows Event Log

You can export the log for troubleshooting purposes.

To save the Applicure Windows Event Log:

In the left pane of the **Computer Management** window, expand **System Tools** and expand **Event Viewer**:



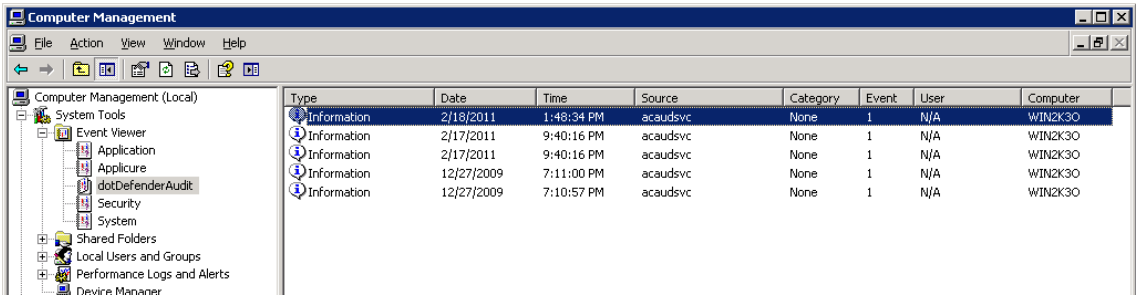
Right-click on **dotDefenderAudit** or **Applicure**, and select **Save Log File As...**.

Enter a name for your file and set the file type to .evt (Event Log).

10.1.1.5 Clearing the Applicure Windows Event Log

To clear the Applicure Windows Event Log:

In the left pane of the **Computer Management** window, expand **System Tools** and expand **Event Viewer**:



Right-click on **dotDefenderAudit** or **Applicure** and select **Clear all Events**. The events are cleared and the right pane no longer displays events.

10.1.2 Manually creating dotDefender virtual directory

When installing dotDefender, the installation attempts to create a virtual directory under the Default Web Site. If the Default Web Site does not exist, the virtual directory should be created manually, by following the procedure below.
This procedure contains the following sections:

- Creating dotDefender virtual directory under Windows 2003
- Creating dotDefender virtual directory under Windows 2008

10.1.2.1 Creating dotDefender virtual directory under Windows 2003

1. Navigate to the IIS Manager window.
2. Go to “Web Sites” →
3. Select the site you wish to create the VD under.

(Point at the selected site) → Right click → New... → Virtual Directory

4. In the Wizard:
   Click NEXT
   Alias: type: “dotDefender” and NEXT
   Path: Browse and navigate to:
   “$:\Program Files\Applicure\dotDefender for IIS\cgi-bin”, and NEXT
   Make sure both “Read” and “Execute” are checked and NEXT
   Click FINISH
5. (Point at the newly created dotDefender's VD) → Right click → Properties:

Under the “Virtual Directory” tab:
Select “Configuration...”:
In the “Application Configuration” window, under the “Mapping” tab, click “Add...”:
Executable: Browse and select (from within the “cgi-bin” directory):
dotDefenderWS.exe
Once you have selected the file, add quotations to the entire path!
(“$:\Program Files\Applicure\dotDefender for IIS\cgi-bin\dotDefenderWS.exe”)
Extension: type: “.exe”
Make sure to uncheck “Script engine”.
Click OK.
In the “Application Configuration” window, click OK.

6. Under the “Directory Security” tab:
   In the “Authentication and access control” section, click “Edit...”
   In the “Authentication Methods” section:
   Uncheck “Enable anonymous access”.
   In the “Authenticated Access” section:
   Make sure to check “Integrated Windows authentication”.
   Click OK.
7. Under the “Documents” tab:
   Click “Add...”
   Type in the field: “dotDefender.html”.
8. Click OK (to close the Properties window).
9. Go to “Web Service Extensions” →
10. Right click in the list (below the records) → “Add a new Web service extension...”
    In the “New Web Service Extension” window:

Extension name: type: “dotDefender WS”
Click “Add...” and in the next window click “Browse...”
Select (from within the “cgi-bin” directory): “dotDefenderWS.exe” and “Open”
Click OK.
Make sure to check “Set extension status to Allowed”.
Click OK.

Now you may close all windows and reload the dotDefender GUI.

10.1.2.2 Creating dotDefender virtual directory under Windows 2008

1. Navigate to the IIS Manager window.
2. Go to “Sites” →
3. Select the site you wish to create the VD under.

(Point at the selected site) → Right click → Add Virtual Directory...

4. In the “Add virtual directory” window:
   Alias: type “dotDefender”
   Physical path: Browse and navigate to:
   “$:\Program Files\Applicure\dotDefender for IIS\cgi-bin”, and OK.
5. Select the newly created dotDefender's virtual directory and go to “Handler Mappings”:
   On the right-hand side pane select “Add Script Map...”
   Request path: type “dotDefenderWS.exe”.
   Executable: Browse and select (from within the “cgi-bin” directory):
   dotDefenderWS.exe.
   Once you have selected the file, add quotations to the entire path!
   (“$:\Program Files\Applicure\dotDefender for IIS\cgi-bin\dotDefenderWS.exe”)
   Name: type “dotDefender”.
   Click on “Request Restrictions...”
   In the “Request Restrictions” window:
   Under the “Mapping” tab:
   Check “Invoke handler only if request is mapped to:”
   (Make sure “File” is selected)
   Under the “Verbs”: Make sure “All verbs” is selected.
   Under the “Access” tab: Select “Execute”.
   Click OK.
   Click OK and then YES.
   Select the newly created resource “dotDefenderWS”.
   On the right-hand side pane select “Edit Feature Permissions...”
   In the “Edit Feature Permissions” window:
   Make sure to check all boxes, and click OK.
6. Select the newly created dotDefender's virtual directory and go to “Authentication”:
   DISABLE “Anonymous Authentication”.
   ENABLE “Windows Authentication”.
7. Select the newly created dotDefender's virtual directory and go to “Default Document”:
   On the right-hand side pane select “Add...”
   In the “Add Default Document” window:
   Name: type “dotDefender.html”
   Click OK.

Now you may close all windows and reload the dotDefender GUI.

10.2 Specific Linux files and features

10.2.1 Adding websites to server

When a new website is added to the Apache server, it will be automatically protected by dotDefender, assuming that the Default Security Profile is set to Protection mode. To be able to see the new website in the dotDefender Administration Console and be able to configure a specific profile for the website:
Execute the script /usr/local/APPCure/webservice/bin/generate_sites.sh

If you need assistance or have any questions during the deployment process,
please feel free to contact us at: **support@applicure.com**

Applicure Technologies Ltd.
www.applicure.com