

dotDefender for IIS

User Guide

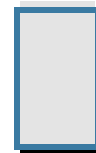


Table of Contents

Chapter 1	Introduction	5
1.1	Overview	5
1.2	Components	5
1.3	Benefits	6
1.4	Organization of this Guide	6
Chapter 2	Getting Started	9
2.1	System Requirements	9
2.1.1	<i>Windows 2008 Requirements.....</i>	<i>9</i>
2.1.1.1	<i>APPLICATION DEVELOPMENT:.....</i>	<i>9</i>
2.1.1.2	<i>SECURITY:.....</i>	<i>9</i>
2.1.1.3	<i>MANAGEMENT TOOLS:</i>	<i>9</i>
2.2	Installing dotDefender	10
2.3	Using the Administration Console.....	20
2.4	Stopping and Starting dotDefender	21
2.5	Applying Changes	22
2.6	Workflow	23
Chapter 3	Managing Logs.....	25
3.1	Overview	25
3.2	Managing dotDefender Events in the Windows Event Viewer	25
3.2.1	<i>dotDefender Windows Event logs Overview.....</i>	<i>26</i>
3.2.2	<i>Viewing Applicure Events.....</i>	<i>26</i>
3.2.3	<i>Viewing dotDefender Audit Events</i>	<i>28</i>
3.2.4	<i>Setting the Event Log Size</i>	<i>29</i>
3.2.5	<i>Saving the Applicure Windows Event Log</i>	<i>31</i>
3.2.6	<i>Clearing the Applicure Windows Event Log.....</i>	<i>31</i>
3.3	Viewing policy changes in the audit log file	31
3.4	Configuring the dotDefender Log Database	32
3.5	Viewing the dotDefender Log Database in the Log Viewer.....	33
3.5.1	<i>Opening the Log Viewer.....</i>	<i>34</i>
3.5.2	<i>Filtering the Log</i>	<i>35</i>
3.5.3	<i>Searching for an Event.....</i>	<i>39</i>
3.5.4	<i>Backing Up the dotDefender Event Database</i>	<i>40</i>
3.5.4.1	<i>Backup dotDefender Event Database.....</i>	<i>40</i>

3.5.4.2 Backup dotDefender Event log from the Windows Event Viewer	40
3.5.5 Viewing Archived Event Databases	40
3.5.6 Backing Up the dotDefender Configuration	41
3.6 Identifying False Positives	41
Chapter 4 Configuring Website Security Profiles	43
4.1 Website Security Profiles Overview	43
4.2 Modifying a Website Security Profile	44
4.2.1 Configuring Operating Mode	45
4.2.2 Configuring Session Protection	45
4.2.3 Configuring the Application Rule Set	46
4.2.4 Configuring the Error Page	47
4.2.5 Configuring Advanced Settings	49
Chapter 5 Configuring Patterns and Signatures	51
5.1 Patterns and Signatures Overview	51
5.2 Rule Categories	53
5.3 Enabling/Disabling a Rule Category	57
5.4 Configuring Patterns	57
5.4.1 Modifying Best Practices	58
5.4.2 Adding User-Defined Rules	60
5.4.2.1 Searching in Commonly Attacked Fields of HTTP Requests	63
5.4.2.2 Searching in Client Remote Address	66
5.4.2.3 Searching in URI	69
5.4.2.4 Searching in User-Agent	71
5.4.2.5 Searching in Custom Fields of HTTP Requests	74
5.4.2.6 Searching in Custom Parameters of XML/SOAP Elements	78
5.4.3 Managing the Rules	82
5.4.3.1 Viewing the User-Defined Rules	82
5.4.3.2 Enabling/Disabling a User-Defined Rule	83
5.4.3.3 Deleting a User-Defined Rule	83
5.4.3.4 Editing a User-Defined Rule	84
5.5 Managing Signatures	87
Chapter 6 Configuring Global Settings	88
6.1 Enabling / Disabling logging to Windows Event Logs	88
6.2 Enabling / Disabling NAT Support	89
Chapter 7 FAQs and Troubleshooting	90
7.1 FAQs	90
7.1.1 How do I allow an IP address, or a range of IP addresses?	91

7.1.2 How do I identify and control access to the Website, according to Windows users (using the Remote User field)?.....	92
7.1.3 How do I enable updates to work through a firewall?.....	95
7.1.4 How do I change the database size limit?	95
7.1.5 What is a "bad" User-Agent and why does dotDefender block certain browsers?	95
7.1.6 How do I let one "good" User-Agent pass through?.....	96
7.1.7 How do I remove the database when it is taking up too much space?..	97
7.1.8 What is a Proxy attack?.....	97
7.1.9 How do I turn a False Positive into a Whitelist Rule?.....	97
7.1.10 Does a User-Defined rule still undergo inspection?	97
7.1.11 I am upgrading. How do I back up the rule set?.....	98
7.1.12 How do I clear the Event Log?.....	98
7.1.13 I have scripts on a Website that are blocked for usage by end-users. How do I allow the scripts to run?	98
7.1.14 I have a content upload page, and I cannot upload new content.	99
7.2 Troubleshooting.....	99
7.2.1 System Requirements	99
7.2.2 Configuring dotDefender for IIS to work properly with IIS ISAPI Filters (SSL-encrypted sites).....	99
Chapter 8 Regular Expressions.....	101
8.1 POSIX Basic Regular Expressions.....	101
8.2 POSIX Extended Regular Expressions	102



Introduction

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

- [Overview](#)
- [Components](#)
- [Benefits](#)
- [Organization of this Guide](#)

1.1 Overview

dotDefender is a software-based web application firewall installed on Apache, IIS, or Microsoft ISA Server. dotDefender provides robust protection against attacks targeting web applications.

dotDefender utilizes three 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 security 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 leechers.

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](#)).
- 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](#)).

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 (Cookie Tampering)
- dotDefender (Session Protection)
- dotDefender (Main)

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.

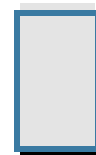
1.4 Organization of this Guide

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 - [Configuring Website Security Profiles](#)**, describes how to configure the Website profiles.
- **Chapter 5 - [Configuring Patterns and Signatures](#)**, describes how to configure the Patterns and Signatures.
- **Chapter 6 - [Configuring Global Settings](#)**, describes how to configure server wide settings.
- **Chapter 7 - [FAQs and Troubleshooting](#)**, details a variety of frequently asked questions and troubleshooting information.
- **Chapter 8 - [Regular Expressions](#)**, a brief tutorial on writing Regular Expressions.



Getting Started

This chapter contains the following sections:

- [System Requirements](#)
- [Installing dotDefender](#)
- [Using the Administration Console](#)
- [Stopping and Starting dotDefender](#)
- [Applying Changes](#)
- [Workflow](#)

2.1 System Requirements

dotDefender operation requires the following:

- Web Server: IIS 5.x, IIS 6.0, IIS 7.0
- Platform: Microsoft Windows 2000, Microsoft Windows 2003, Microsoft Windows XP, Windows 2008

2.1.1 Windows 2008 Requirements

The following role services should be installed (In addition to the default role services installed with IIS):

2.1.1.1 APPLICATION DEVELOPMENT:

- ISAPI Extensions
- ISAPI Filters

2.1.1.2 SECURITY:

- Windows Authentication

2.1.1.3 MANAGEMENT TOOLS:

- IIS6 Metabase Compatibility

Note: When selecting the parameters instructed in the steps below, leave other default definitions without changing.

1. Select **Start > Server Manager** to open the Server Manager window.
2. Select **Roles** in the left pane.
3. Select **Add Roles**.
4. Select **Web Server IIS**.
The Add Roles Wizard appears.
5. Click the **Add Required Features** button (default).
6. Click, **Next, Next**.
7. In the Select Role Services window select **Role Services** in the left panel.
8. Under Application Development in the right pane, select:
 - ◆ **ISAPI Extensions**
 - ◆ **ISAPI Filters**
9. Under Security select **Windows Authentication**.
10. Under Management Tools > IIS6 Management Compatibility, select **IIS6 Metabase Compatibility**.
11. Click **Next**, then click **Install**.

After installation, the Installation Results window appears with a message informing you that the Installation has succeeded.

This installs the Role Services for IIS.

2.2 Installing dotDefender

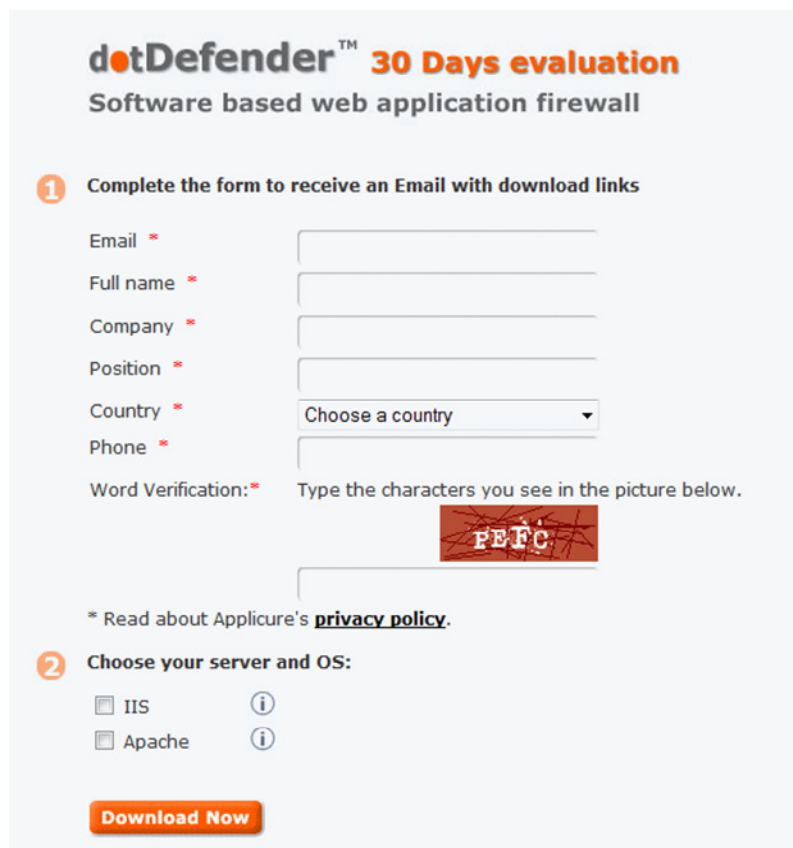
Note: The IIS web server will be automatically restarted during the installation process.

1. Open your browser and navigate to www.applicure.com. You are prompted to download a 30-day evaluation version. You can continue to use the trial version for up to 30 days and then purchase a license.



The advertisement features the dotDefender logo at the top left. Below it, a paragraph describes the Web Application Firewall's capabilities: "Web Application Firewall protects your websites and internal applications from defacement and hacker attacks, including SQL Injection, Session Hijacking and Cross-Site-Scripting." To the right of this text is a 3D rendering of the software's retail box, which includes the Applicure logo and the slogan "OUT-OF-THE-BOX Website Security". At the bottom left of the ad is an orange button labeled "30 Day Free Trial", and to its right is a blue link that says "Read more »".

2. Click **30 Days Evaluation**. You are prompted to provide your details, including your name, email address, server type, and operating system.

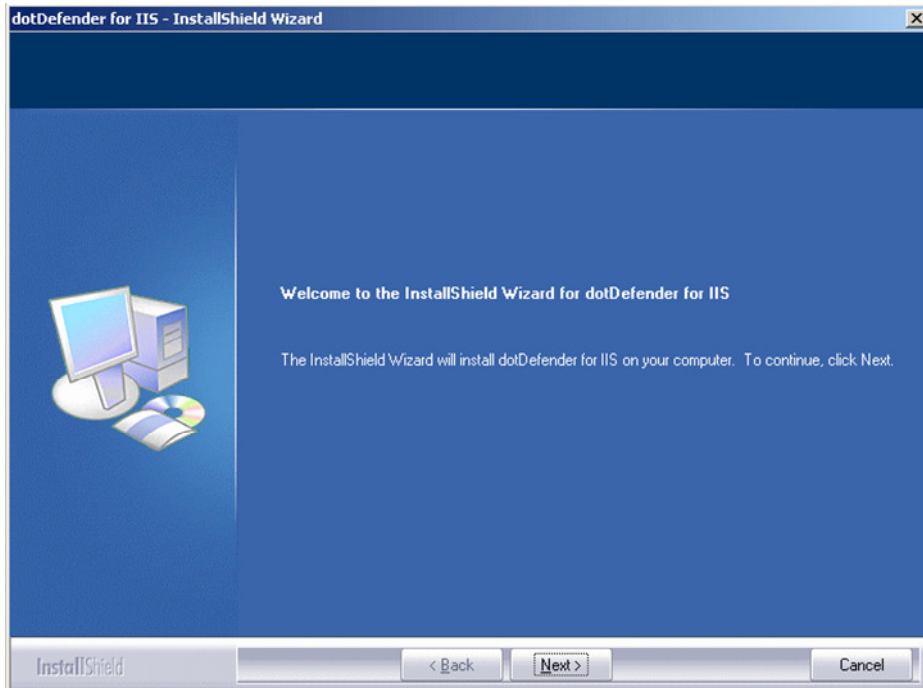


The registration form is titled "dotDefender™ 30 Days evaluation" and "Software based web application firewall". It is divided into two numbered sections. Section 1, "Complete the form to receive an Email with download links", contains input fields for Email, Full name, Company, Position, and Phone, each with a red asterisk indicating it is required. The Country field is a dropdown menu currently showing "Choose a country". Below these fields is a "Word Verification" section with a red asterisk and a small image of a red brick with the letters "PEFC" on it. A note below the form says "* Read about Applicure's [privacy policy](#)." Section 2, "Choose your server and OS:", has two radio button options: "IIS" and "Apache", each with an information icon (i) to its right. At the bottom of the form is an orange "Download Now" button.

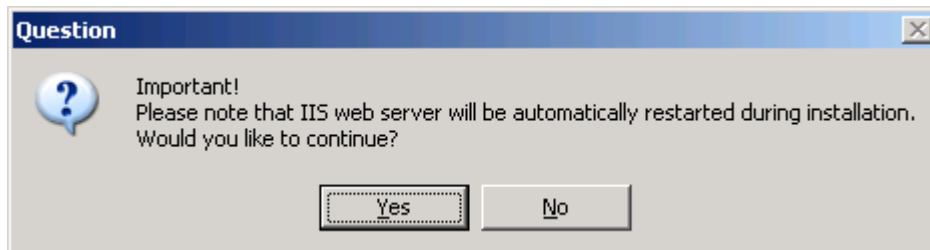
3. Select **IIS**.
4. Click **Download Now**. You are prompted to check your email for download instructions.
5. Follow the email instructions.

6. Double-click the downloaded file.

The InstallShield Wizard begins and the Welcome window appears.

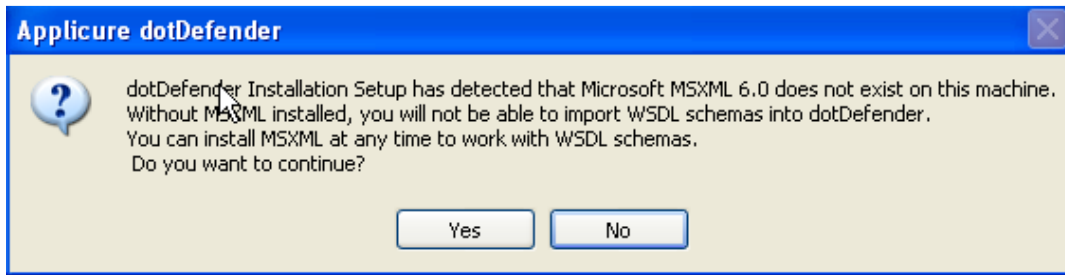


7. Click **Next** to continue.
8. A message appears warning you that the IIS web server will be automatically restarted during the installation. Click **Yes** to continue.



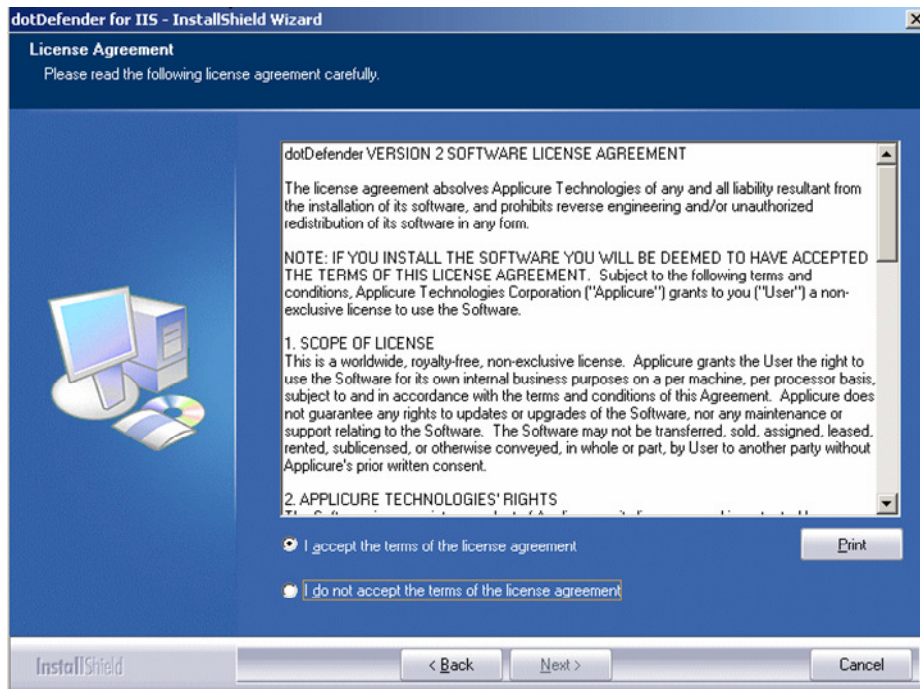
If you do not have MSXML installed on your system, a message appears informing you and also prompting you to continue with the installation.

You may continue with the installation of dotDefender successfully. However, if you need to inspect XML traffic you will need to eventually download and install MSXML 6.0 or higher.

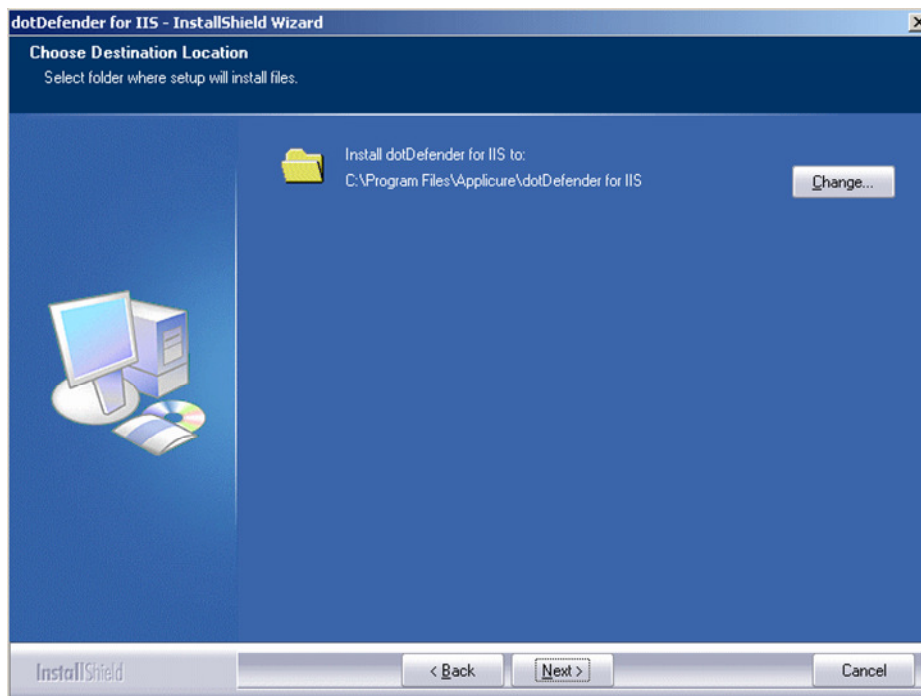


You can download **MSXML** from the Microsoft download website.

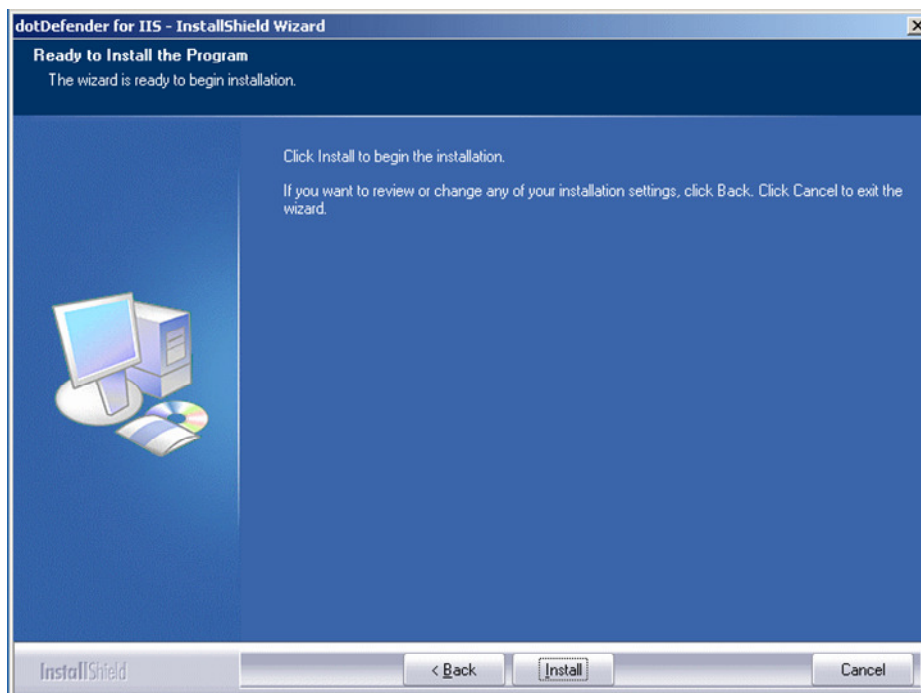
9. Click **Yes** to continue with the installation of dotDefender. You can install MSXML at any time later.
10. The License Agreement window appears.



11. Read the license and select **I accept the terms of the license agreement**. Click **Next**. The Choose Destination Location window appears.



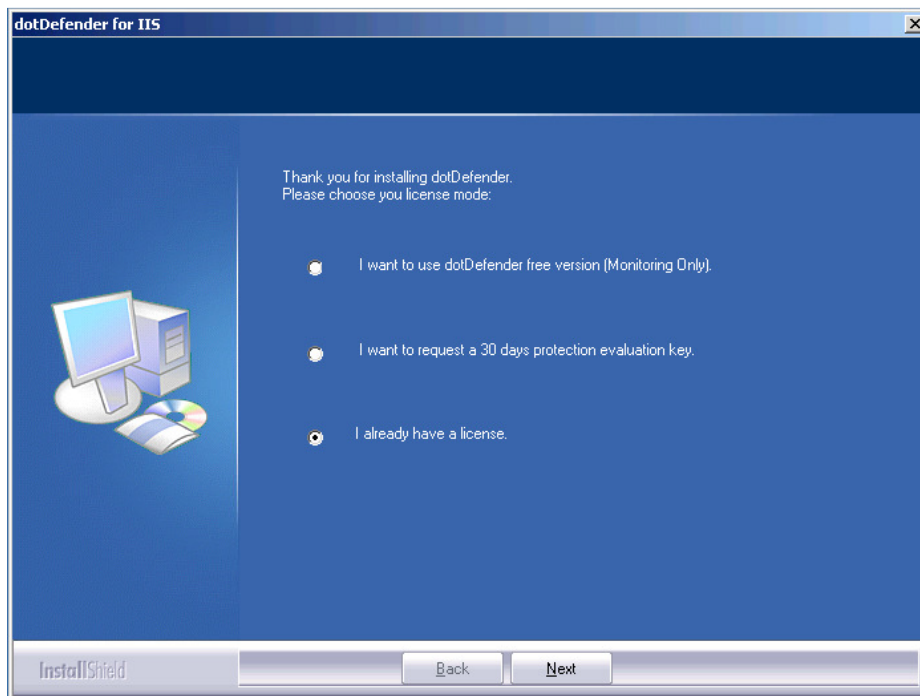
12. Use the default Destination Location or click **Change** to browse and select the directory in which you want to install the dotDefender files. Click **Next**. The Ready to Install the Program window appears.



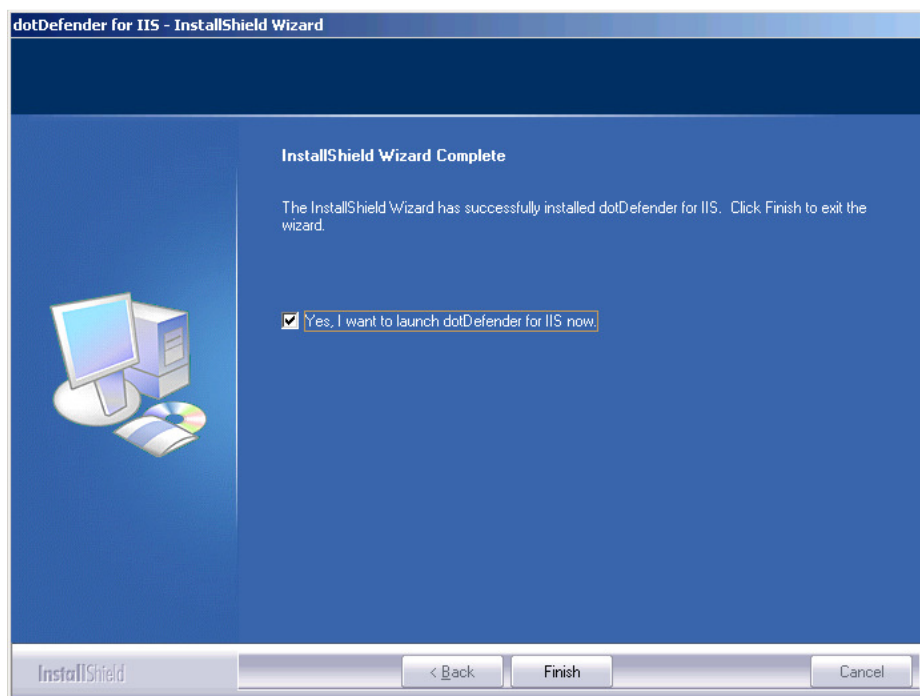
13. Click **Install** to begin installation.

14. Choose whether to install a license file, request a license file online or continue the installation without installing a license (Monitoring only). Click **Next**.

Note: Your websites are not protected until you install the license!



15. When the InstallShield Wizard is complete, click **Finish**.




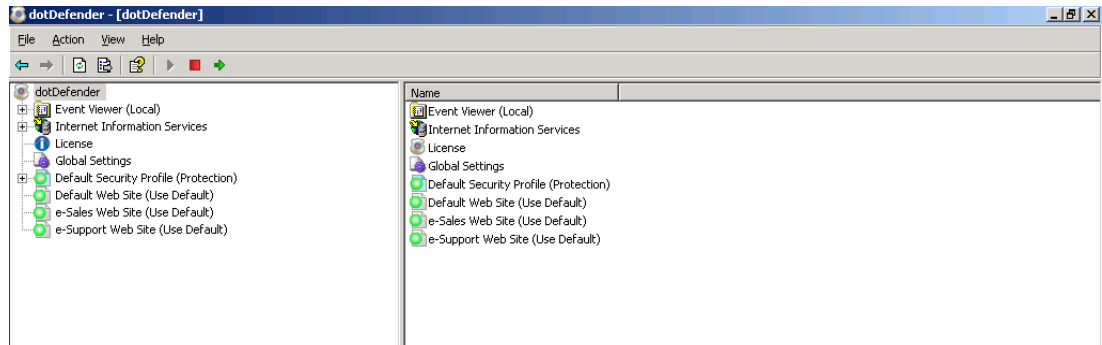
16. dotDefender is automatically launched and becomes active every time the web server starts. The Welcome to dotDefender window appears.



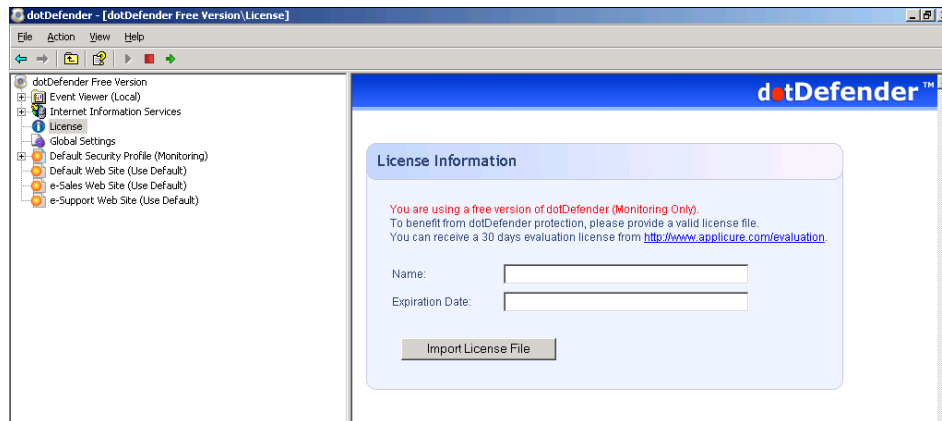
dotDefender icon

17. You can choose to display this window at each startup by leaving the tick mark at **Show this dialog at startup**. If you do not wish to see this window at every startup, remove the tick mark by clicking.
18. Click **Close**. The dotDefender icon appears on the task bar each time you start your web server.

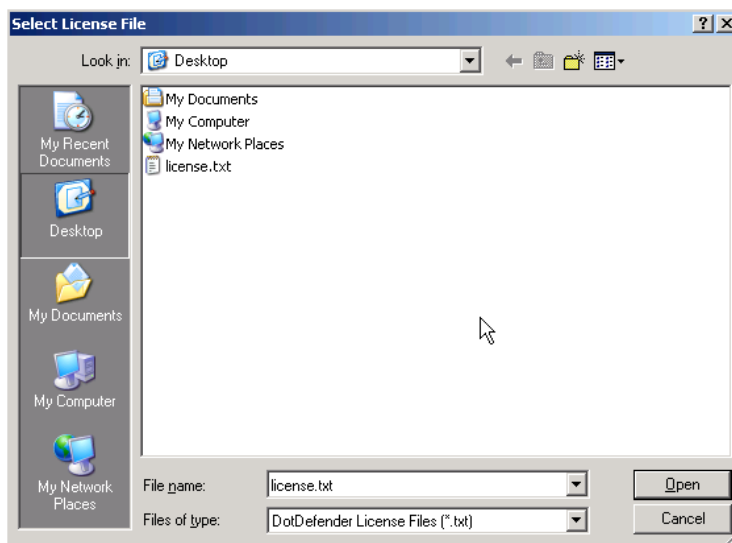
19. Right-click the  icon and select **Open dotDefender**. The dotDefender administration console appears.



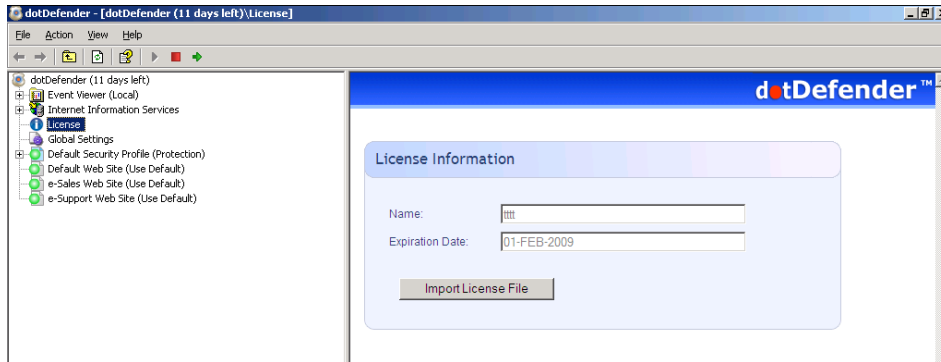
20. If a license has not been installed in the dotDefender installation process, Click **License**.




21. Click **Import License File**. The Select License File window appears.




22. Browse to and select the license file (**license.txt**), and click **Open**. The License Information appears.



23. Click  to apply the changes.

The installation is complete.

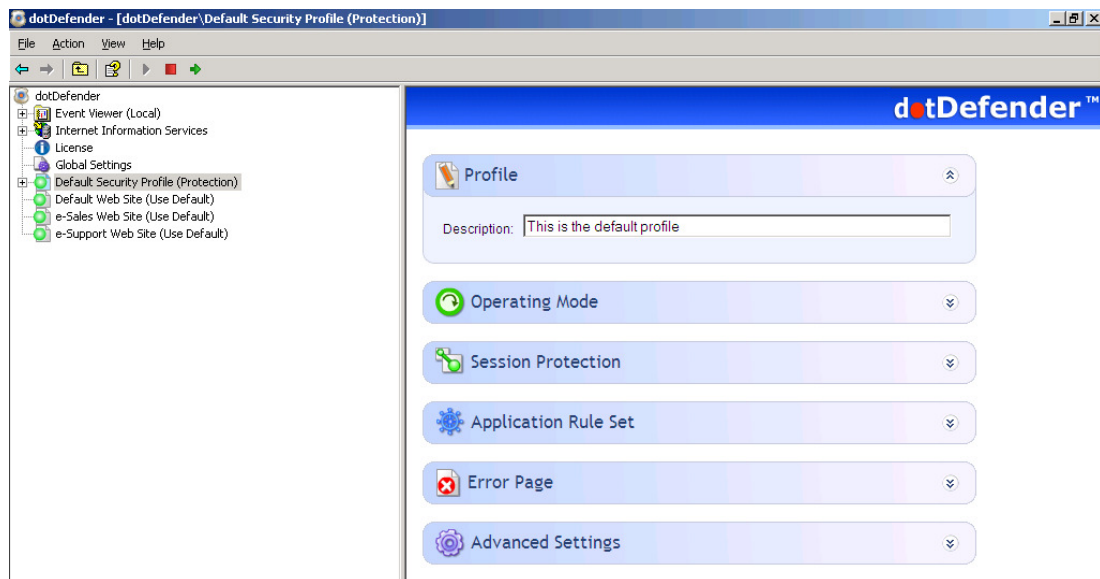
Note: Every time you use the Trial Mode, the number of days remaining for your trial period appears in dotDefender.  dotDefender (11 days left) To purchase the product, contact [Applicure](#) to get a quote.

2.3 Using the Administration Console






This section describes how to open the Administration Console and the toolbar. For additional information about the Administration Console, see [Configuring Website Security Profiles](#).

To open the Administration Console:

- Right-click the  icon and select **Open dotDefender**, or from the Start menu, select **Programs > Applicure dotDefender for IIS > dotDefender Administration Console**.



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
	Returns to the previous view
	Forwards to the next view
	Moves up one level in the tree
	Displays Help about dotDefender when one of the dotDefender branches is selected
	Starts dotDefender

Icon	Function
	Stops dotDefender
	Applies changes

2.4 Stopping and Starting dotDefender

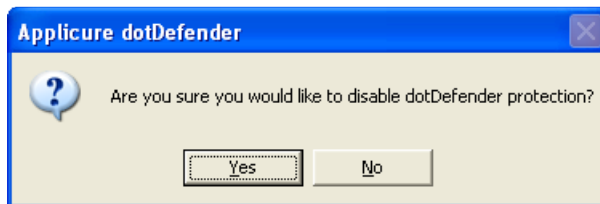
By default, dotDefender is active immediately upon installation (assuming that you have loaded your license and that the license has not expired). All websites and applications on the server are identified and assigned the [Default Security Profile](#) setting. The default **Operation Mode** setting 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.

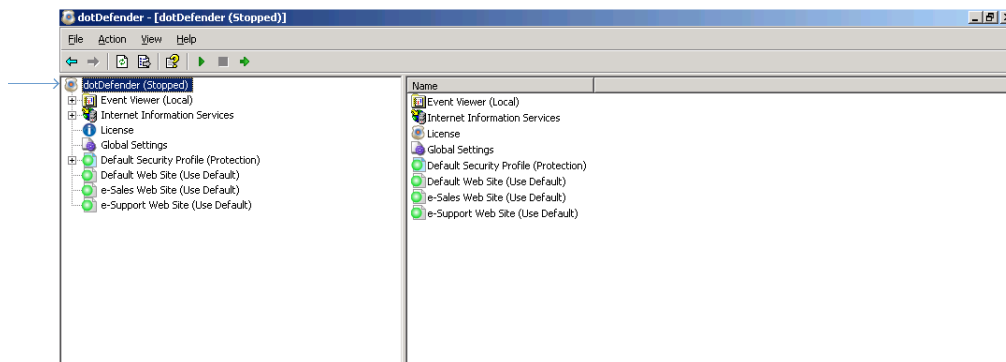
Note: When dotDefender stops, it becomes inactive on the web server where it is installed. Consequently, dotDefender does not perform application protection. When disabled, dotDefender does not use server resources and does not affect server performance.

To stop dotDefender:

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



2. Click **Yes**. You are prompted: Settings successfully submitted.
3. dotDefender is deactivated as indicated below.



To start dotDefender:

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




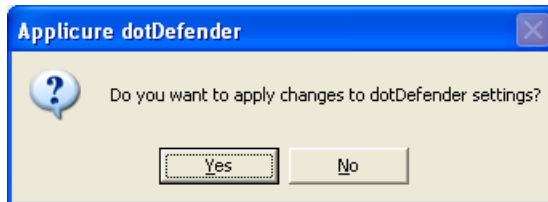
2. Click **OK**. dotDefender is active.

2.5 Applying Changes

If you make a change in the Administration Console, you need to apply the change in order for it to take effect.

To apply changes:

1. Click  in the dotDefender toolbar.
2. Alternatively, if you do not apply the changes and try to close Administration Console, a pop-up message prompts you to do so.



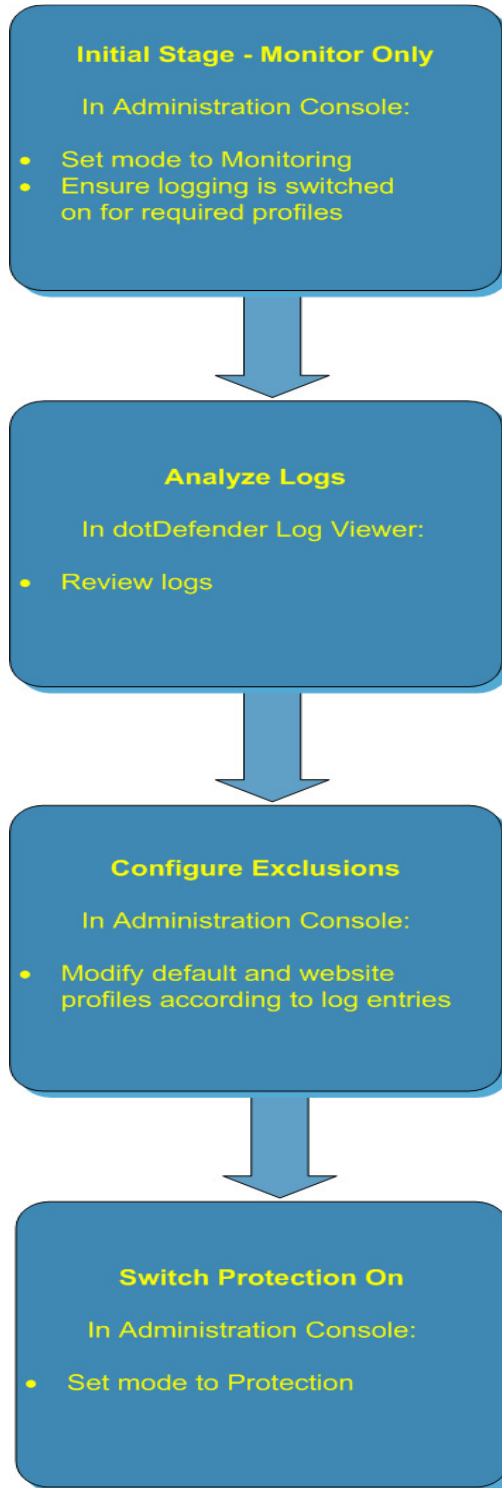
3. Click **Yes** to apply the changes. A pop-up message confirms successful submission of the settings.



4. Click **OK**.

2.6 Workflow

The following workflow is recommended:

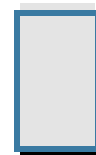


It is recommended that you initially use dotDefender with the default settings. In the Administration Console, set the mode to **Monitoring** and ensure that the dotDefender log is enabled.

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 and [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 to make the necessary adjustments to the configuration.



Managing Logs

This chapter contains the following sections:

- [Overview](#)
- [Managing dotDefender Events in the Event Viewer](#)
- [Viewing policy changes in the audit log file](#)
- [Configuring the dotDefender Log Database](#)
- [Viewing the dotDefender Log Database in Log Viewer](#)
- [Identifying False Positives](#)

3.1 Overview

There are three types of logs:

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

3.2 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](#)

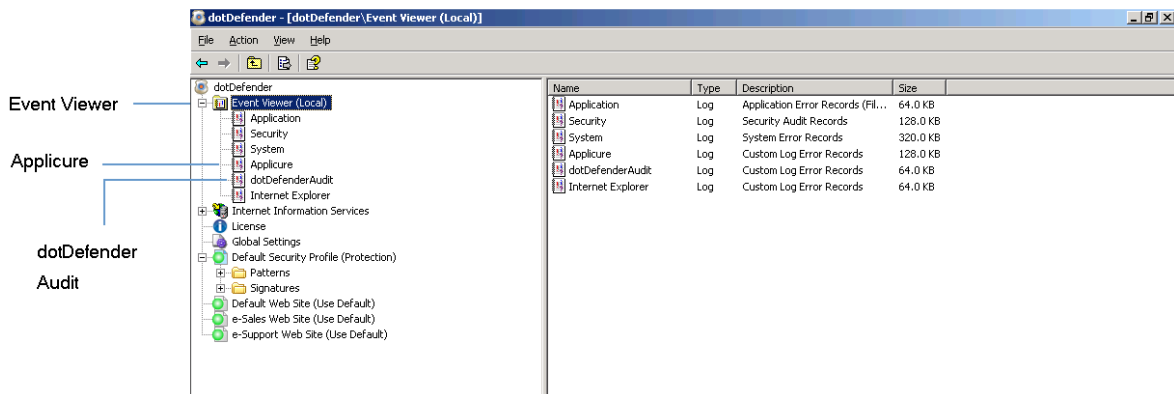
- [Saving the Appicure Windows Event Log](#)
- [Clearing the Appicure Windows Event Log](#)

3.2.1 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:

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

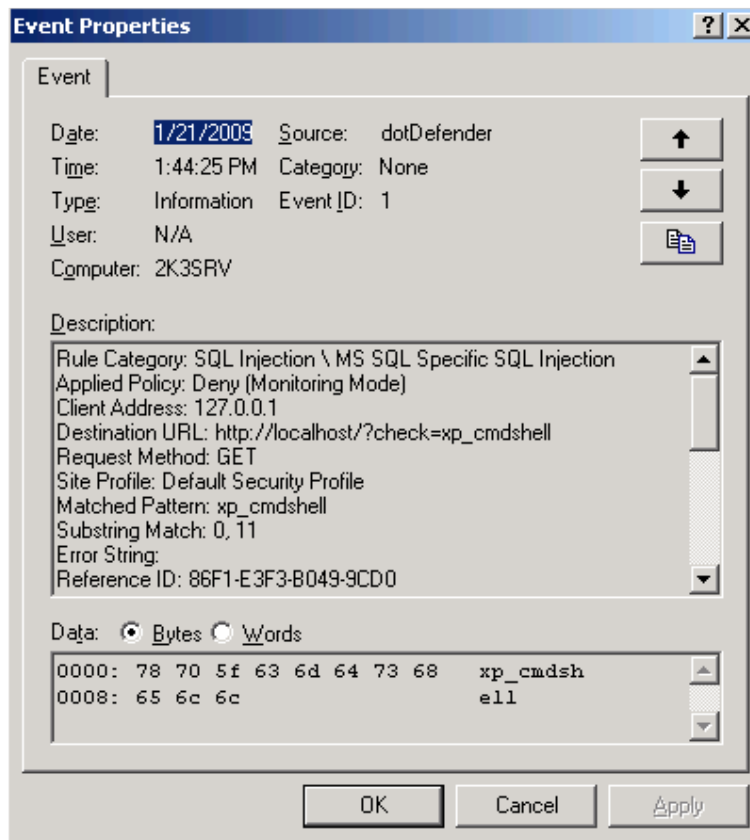


3.2.2 Viewing Appicure Events

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

To view Appicure events:

1. In the left pane of the Administration Console, expand **Event Viewer (Local)** and select **Appicure**.
2. 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

3.2.3 Viewing dotDefender Audit Events

Overview

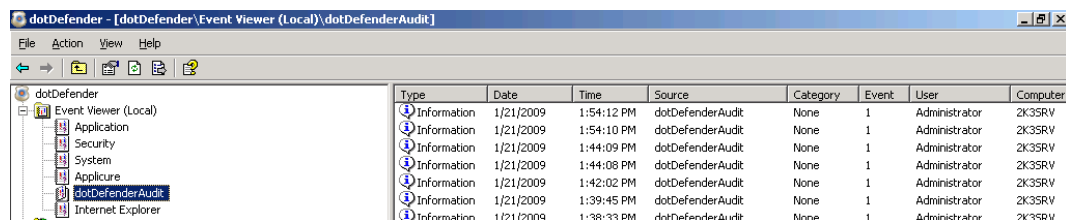
dotDefender keeps two audit trace logs that reflect the status and policy changes in the security policy of each website as required by the PCI regulation. These status messages are divided into two logs:

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](#))

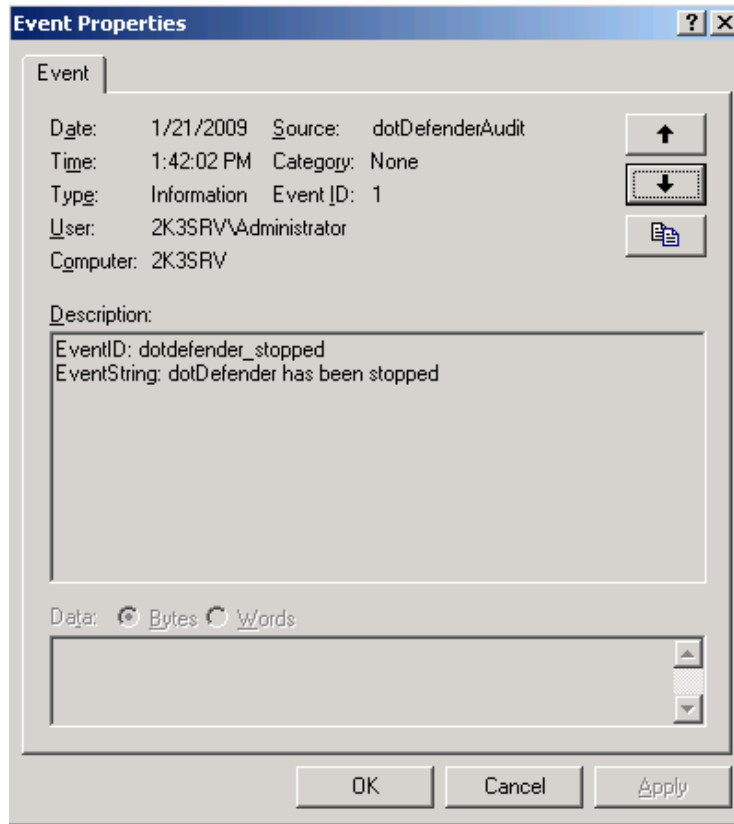
dotDefenderAudit is a watchdog service that polls dotDefender for any status changes. The information on any change in **Operating Mode** includes the date and time of change, designating dotDefenderAudit as the source, the Event ID, and the computer.

To view detailed dotDefenderAudit events:

1. In the left pane of the Administration Console, open **Event Viewer (Local)** and select **dotDefenderAudit**.



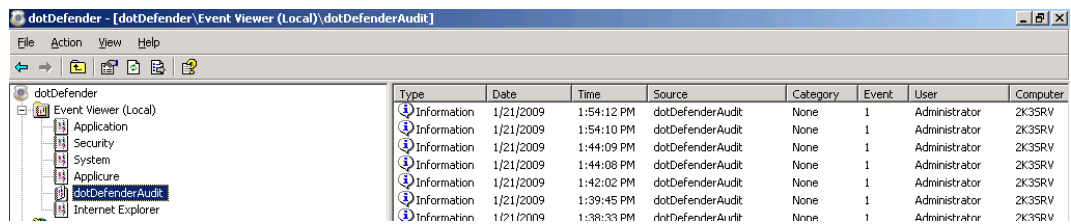
2. Double-click or right-click an event. The right pane expands to show the Audit events.
3. Select **Properties** to display an explanation of the event.



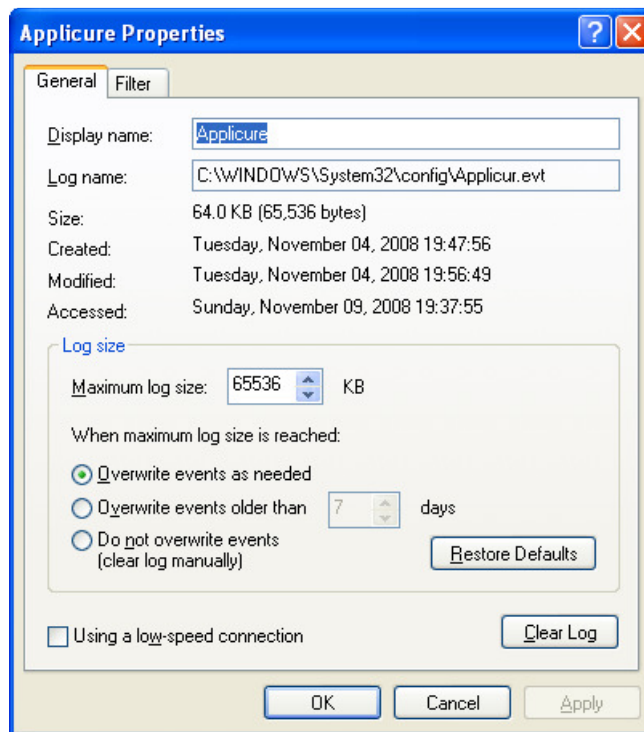
3.2.4 Setting the Event Log Size

To set the Event log size:

1. In the left pane of the Administration Console, open **Event Viewer (Local)**.



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



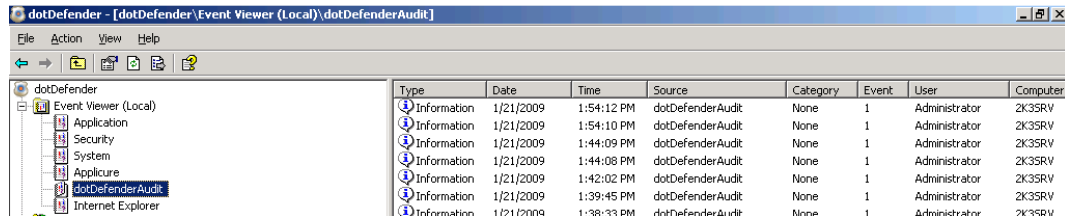
3. Set the **Maximum log size**.
4. The overwrite options in the **When maximum log size is reached** area specify what happens when the log size limit is reached. Select one of the following options:
 - ◆ **Overwrite events as needed:** When the log is full, the newest event replaces the oldest event.
 - ◆ **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.

3.2.5 Saving the Appicure Windows Event Log

You can export the log for troubleshooting purposes.

To save the Appicure Windows Event Log:

1. In the left pane of the Administration Console, open **Event Viewer (Local)**.

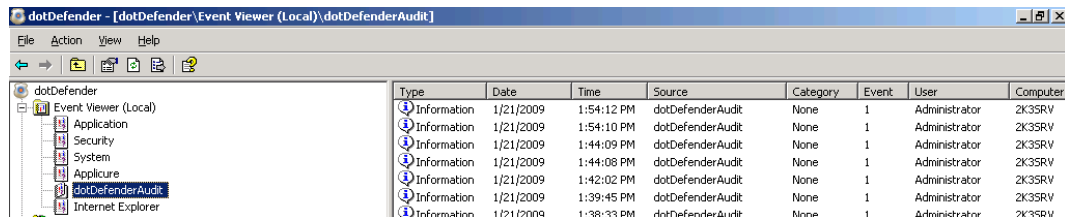


2. Right-click on **dotDefenderAudit** or **Appicure**, and select **Save Log File As....**
3. Enter a name for your file and set the file type to .evt (Event Log).

3.2.6 Clearing the Appicure Windows Event Log

To clear the Appicure Windows Event Log:

1. In the left pane of the Administration Console, open **Event Viewer (Local)**.



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

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 two tab-separated audit log files.

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

Both log files may be viewed under the following location:

\Program Files\Appicure\dotDefender for IIS\etc

3.4 Configuring the dotDefender Log Database

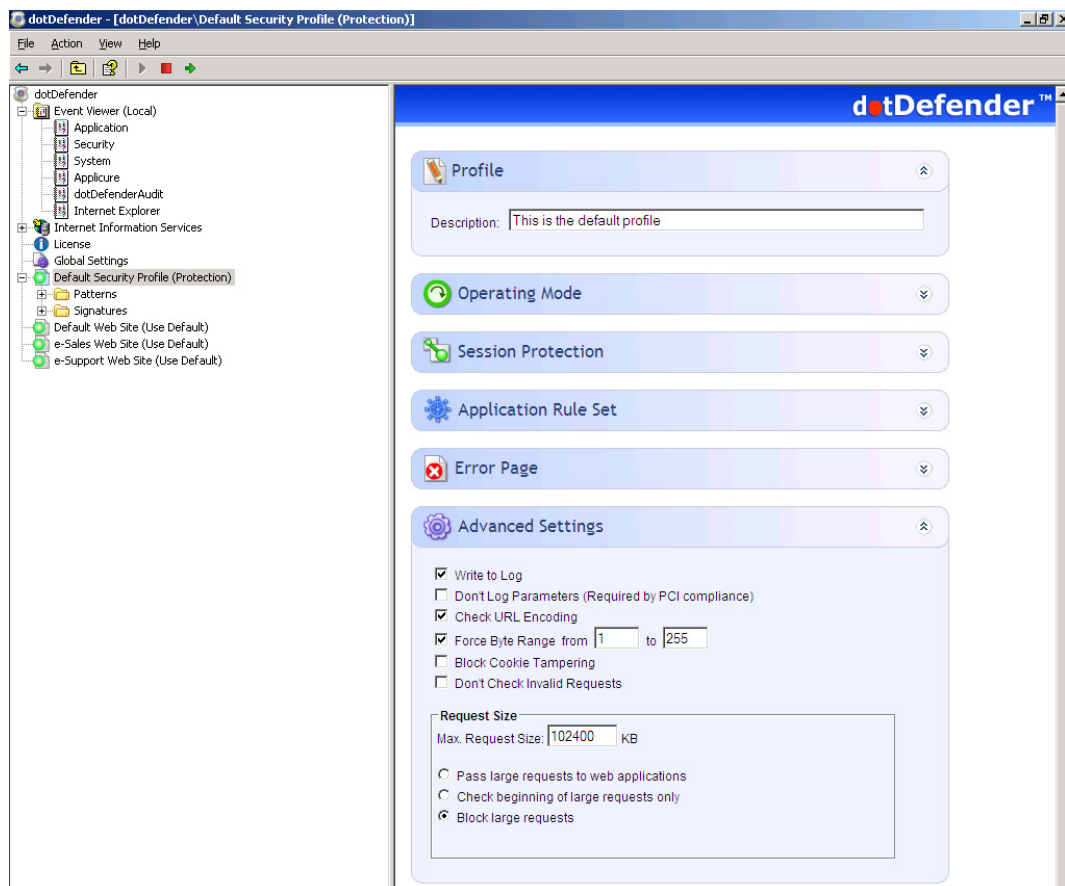
You can enable/disable the log for all of the websites using the Default Security Profile, and separately for each Website that does not use the Default Security Profile.

The **aclogsvc.ddb** log file is located in the following folder:
\Program Files\Applicure\dotDefender for IIS\etc


This file has a default maximum size of 1GB. The size of the database 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:

1. In the left pane of the Administration Console, select **Default Security Profile**. The Log Settings area appears in the right pane.

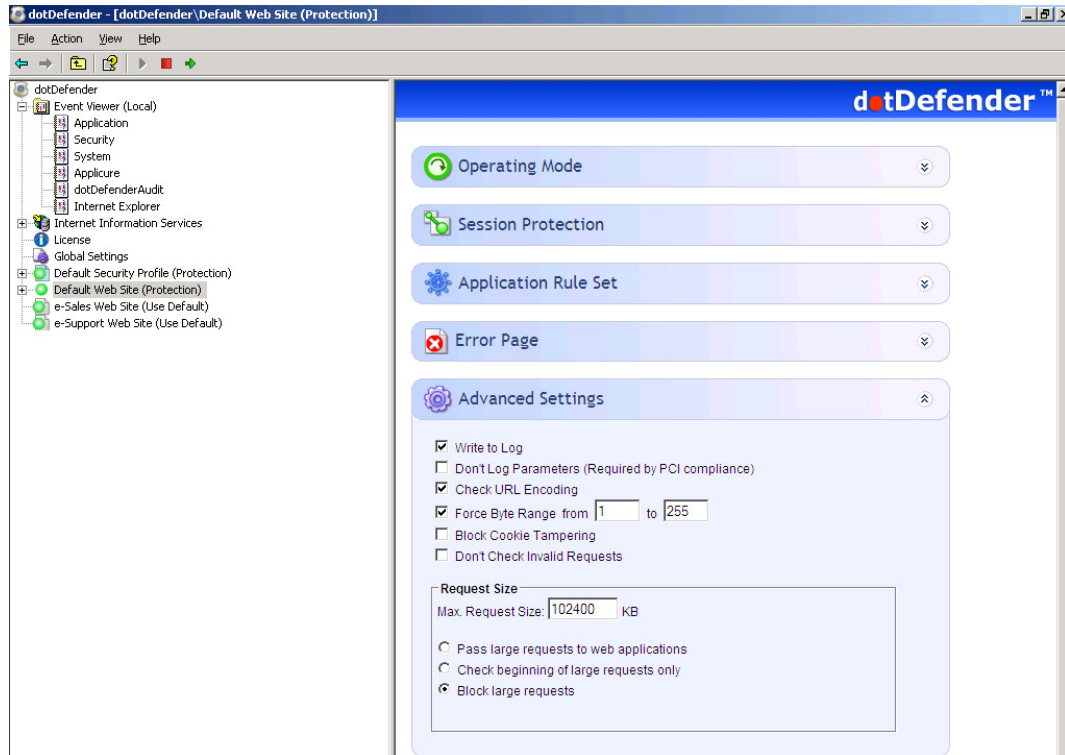



2. Expand the **Advanced Settings** area.

3. Select the **Write to Log** option to enable logging for all websites that use the Default Security Profile.
4. Click  to apply the changes.

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

1. In the left pane of the Administration Console, select required **Website Security Profile**. The right pane opens the Log Settings area.



2. Expand the **Advanced Settings** area.
3. Select the **Write to Log** option to enable logging for this Website.
4. 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:

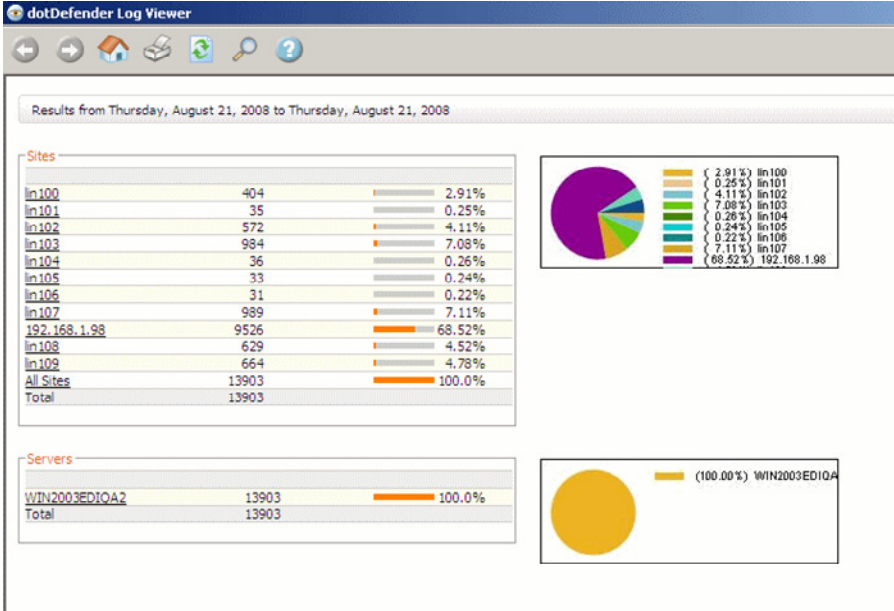
- [Opening the Log Viewer](#)
- [Filtering the Log](#)
- [Searching for an Event](#)
- [Deleting the dotDefender Log Database File](#)

3.5.1 Opening the Log Viewer

To open the Log Viewer:

- Right-click the  icon and select **Open Log Viewer**.
- OR -
- From the Start menu, select **Programs > Applicure dotDefender for IIS > dotDefender for IIS Log Viewer**.

The Log Viewer window appears. The log shows results for blocked sites and servers, which are displayed in a list and pie chart.



The screenshot shows the 'dotDefender Log Viewer' window. The main content area displays 'Results from Thursday, August 21, 2008 to Thursday, August 21, 2008'. It is divided into two sections: 'Sites' and 'Servers'. The 'Sites' section includes a table of attacks per site and a pie chart. The 'Servers' section includes a table of attacks per server and a pie chart.

Attacks per site

Site	Attacks	Percentage
lin100	404	2.91%
lin101	35	0.25%
lin102	572	4.11%
lin103	984	7.08%
lin104	36	0.26%
lin105	33	0.24%
lin106	31	0.22%
lin107	989	7.11%
192.168.1.98	9526	68.52%
lin108	629	4.52%
lin109	664	4.78%
All Sites	13903	100.0%
Total	13903	








Attacks per server

Server	Attacks	Percentage
WIN2003EDIQA2	13903	100.0%
Total	13903	

Note: Ensure that you are viewing the results for the correct dates. For additional information, see [Viewing the dotDefender Log](#).

The following icons appear on the Log Viewer toolbar:

Icon	Function

Icon	Function
	Previous view
	Next view
	Home view
	Print
	Refresh
	Search
	Help

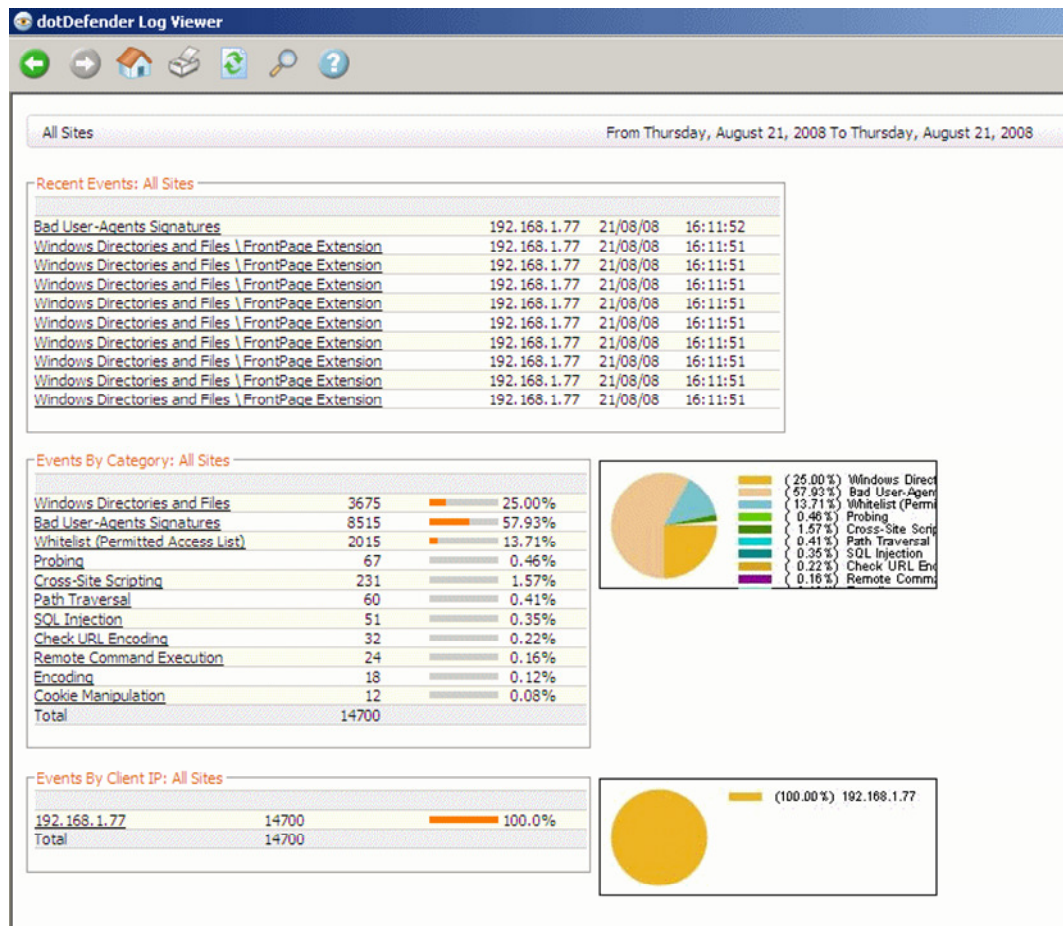
3.5.2 Filtering the Log

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

To filter the log:

1. In the Log Viewer window, click one of the following:
 - ◆ **All Sites:** To view all attack categories from all sites.
 - ◆ **Specific site/s:** To view all attack categories from a specific site.
 - ◆ **Servers:** To view all attack categories from all servers.
 - ◆ **Specific server/s:** To view all attack categories from a specific server.

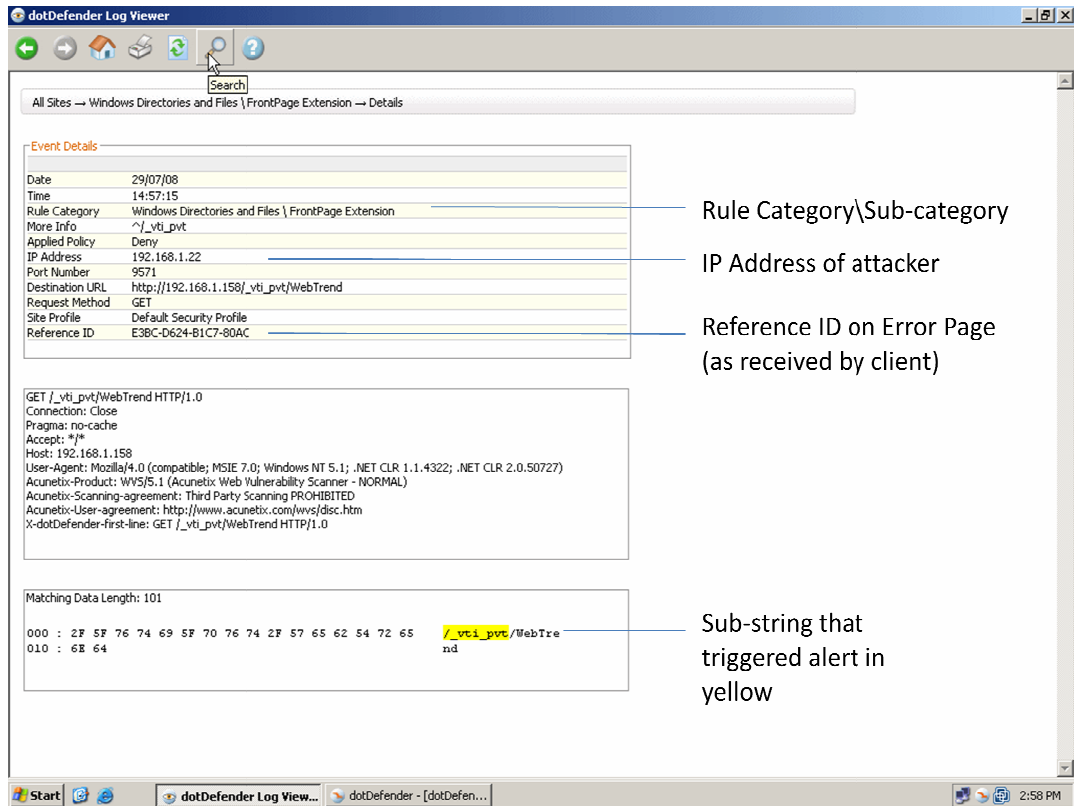
In each case, Log Viewer expands to show the 10 most recent events. It lists the attack category, sub-category, and event details including attacker IP address, date and time of attack, and URL.



2. To drill down and filter for greater detail, click one of the following:

- ◆ A specific event
- ◆ A specific category
- ◆ A specific IP address

3. 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 .
More Information	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 pass. 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.

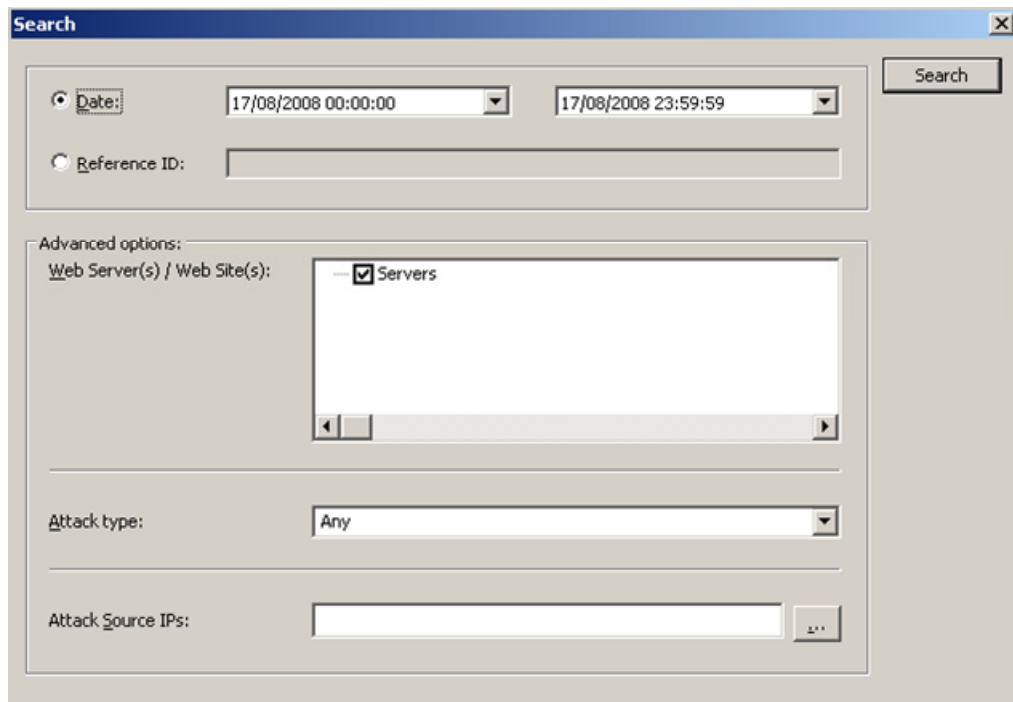
Name	Description
Site profile	The security profile of the website.
Reference ID	Unique identifier of the event (see Configuring the Error Page).
HTTP Headers	Details of the HTTP Headers of the HTTP request.
Matching Data Length	The hex dump of the string as it was captured on the wire. The matching substring 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.
3. Click **Search**.

3.5.4 Backing Up the dotDefender Event Database

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

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

3.5.5 Viewing Archived Event Databases

There are two methods of viewing dotDefender databases with dotDefender Log Viewer:

- Double-click on the archived Event Database

- Open the Event Database from the command line:

1. Run the command from the command line

**C:\Program Files\Applicure\dotDefender for IIS\bin\DDLogViewer.exe"
[event database file path]**

For example:

**"C:\Program Files\Applicure\dotDefender for IIS\bin\DDLogViewer.exe"
c:\backups\aclogsvc.ddb**

Note: Verify that the dotDefender log viewer is not open at the same time. You can open only one instance of the dotDefender Log Viewer at a time.

3.5.6 Backing Up the dotDefender Configuration

To backup the Default Security Profile rule settings:

1. Open the Windows registry
2. Browse to each of the following registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Applicure\dotDefender\Sites\0

HKEY_LOCAL_MACHINE\SOFTWARE\Applicure\dotDefender.effective\Sites\0

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

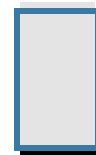
To backup the complete configuration of dotDefender:

1. Copy the file **C:\Program Files\Applicure\dotDefender for IIS\etc\aciisflt.amf** to a backup location of your choosing.

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 web applications 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](#).



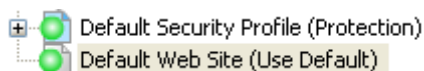
Configuring Website Security Profiles

This chapter contains the following sections:

- [Website Security Profiles Overview](#)
- [Modifying a Website Security Profile](#)

4.1 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.

Nonetheless, 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:

- Session Protection settings
- Selecting an application rule set.
- Specifying the error page.
- Modifying the advanced settings.
- Changing the Best Practices rule settings.

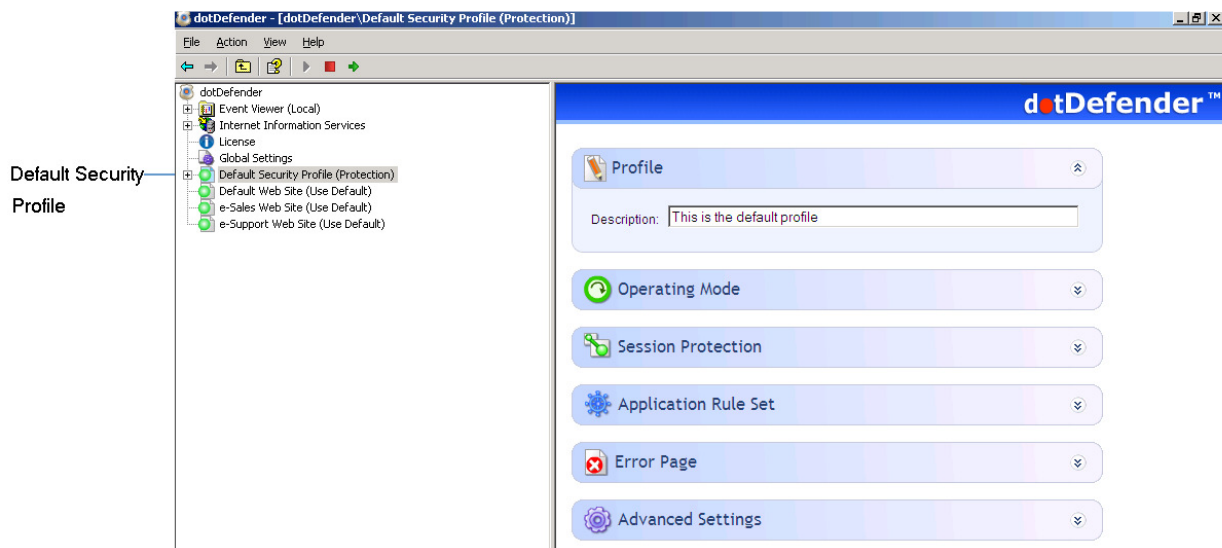
- Adding new user-defined rules.

4.2 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 **Profile Description** field, enter a description of the Profile.
3. (Optional) You can make changes in any of the following sections:
 - ◆ [Operating Mode](#)
 - ◆ [Session Protection](#)
 - ◆ [Application Rule Set](#)
 - ◆ [Error Page](#)
 - ◆ [Advanced Settings](#)

4.2.1 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.
 - ◆ **Protection:** This option 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 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, or if you select this option for Default Security Profile, for all Website Security Profiles that use the Default Security Profile.

Note: Confirmation is required when you between **operating modes**.

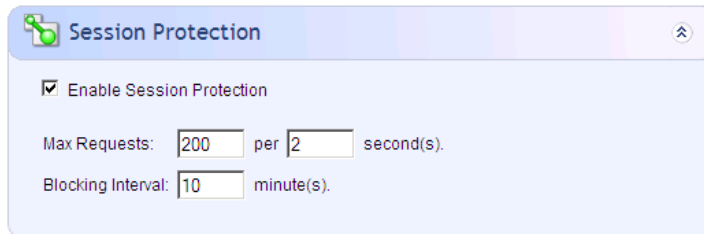
4.2.2 Configuring Session Protection

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.

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:

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




The screenshot shows a configuration panel titled "Session Protection" with a gear icon and an expand/collapse arrow. It contains the following settings:

- Enable Session Protection
- Max Requests: per second(s).
- Blocking Interval: minute(s).

2. 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.

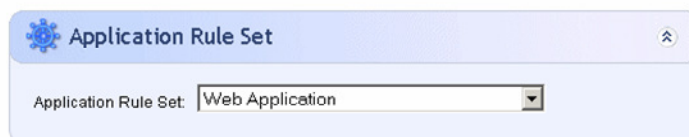
3. Click  to apply the changes.

4.2.3 Configuring the Application Rule Set

You can modify the Application Rule Set to provide targeted protection for Web Applications, Outlook Web Access or SharePoint Portal Servers.

To modify the Application Rule Set:

1. Expand the **Application Rule Set**. dotDefender for IIS provides several types of rule sets for each Website, based on the application that is protected.



The screenshot shows a configuration panel titled "Application Rule Set" with a gear icon and an expand/collapse arrow. It contains the following setting:

- Application Rule Set:

2. Select one of the following:

- ◆ **Web Application:** dotDefender uses generic rules for all websites and web applications.
- ◆ **Microsoft Outlook Web Access:** dotDefender provides targeted protection for Outlook Web Access.
- ◆ **SharePoint Portal Server 2003:** dotDefender provides targeted protection for SharePoint Portal Server 2003.
- ◆ **SharePoint Server 2007:** dotDefender provides targeted protection for SharePoint Server 2007.

4.2.4 Configuring the Error Page

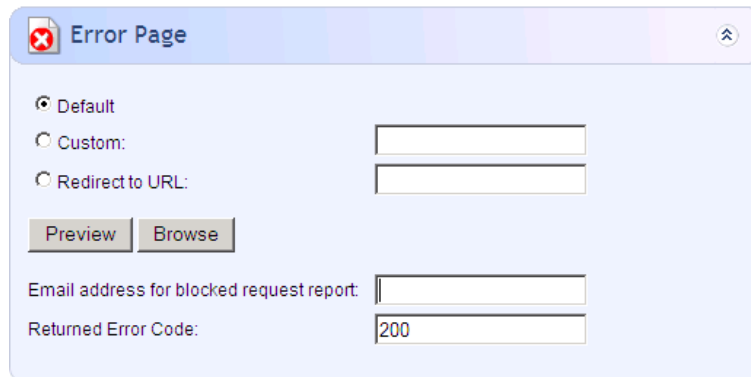
You can modify the Error Page settings to determine the page that is displayed as well as the email address to which valid users report when their requests are blocked.

You can add the following fields to a custom page:

- ◆ **%EMAIL%**
- ◆ **%RID%**
- ◆ **%IP%**
- ◆ **%DATE_TIME%**

To modify the Error Page:

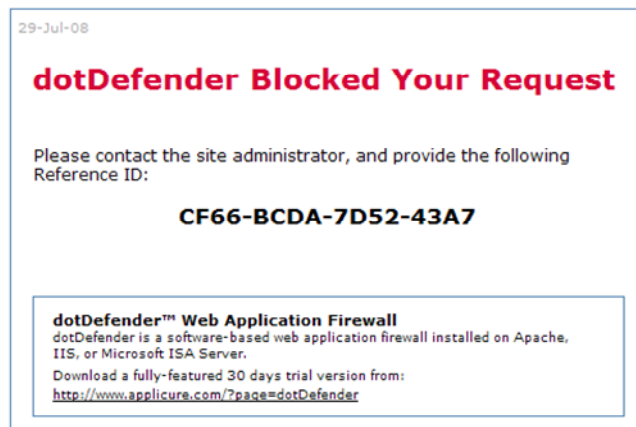
1. Expand the **Error Page**.



The screenshot shows a configuration window titled "Error Page" with a close button (X) and a maximize button (⌵). The window contains the following elements:

- Three radio buttons for selection: "Default" (selected), "Custom:", and "Redirect to URL:". The "Custom:" and "Redirect to URL:" options have corresponding text input fields.
- Two buttons: "Preview" and "Browse".
- Two text input fields: "Email address for blocked request report:" and "Returned Error Code:". The "Returned Error Code:" field contains the value "200".

2. Select one of the following:
 - ◆ **Default:** This option uses a 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.
 - ◆ **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.
3. (Optional) Click **Preview** to view the Error Page, or click **Browse** to navigate to the URL.
4. (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 default Error Page includes several variables, such as the Date and Reference ID.

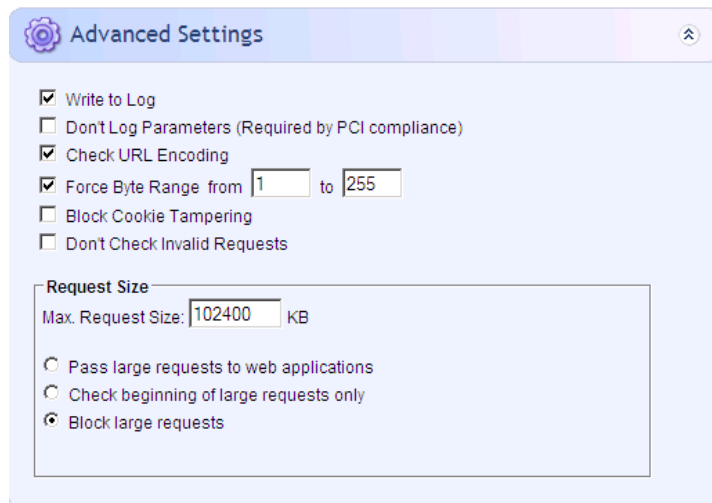
5. (Optional) Configure the HTTP status code returned to the client when a request has been denied by setting a status code number at the right-hand side of the **“Return Error Code:”** field according to the expected application behavior. Some examples for such status codes include: 200, 302, 400, 404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

4.2.5 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 Windows Event Log and 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.

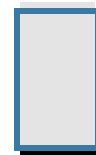
3. In the Request Size area, enter the maximum permitted request size (in KB) in the **Maximum Request Size** field. By default, a value higher than the maximum size results in blockage of traffic to the web server.

4. In the Request Size area, select one of the following options:

- ◆ **Pass Large Requests to Web Applications:** dotDefender allows HTTP requests that are larger than the maximum request size.
 - ◆ **Check Beginning of Large Requests Only:** dotDefender only checks the beginning of large HTTP requests (that are larger than the maximum request size).
 - ◆ **Block Large Requests:** dotDefender blocks HTTP requests that are larger than the maximum request size (default).
5. Click  to apply the changes. The following pop-up message appears.



6. Click **OK**.



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](#)

5.1 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:**
 - ◆ **Whitelist (Permitted Access List):** A Whitelist enables you to approve or deny specific users, pages, or actions that are not checked by default by dotDefender. You can configure, for example, rules to block access to server applications or, conversely, allow absolute access so they are not checked. You 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.
 - ◆ **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 screenshot shows the dotDefender Log Viewer interface. The 'Event Details' section contains the following information:

Date	29/07/08
Time	14:57:15
Rule Category	Windows Directories and Files \ FrontPage Extension
More Info	^/_vti_pvt
Applied Policy	Deny
IP Address	192.168.1.22
Port Number	9571
Destination URL	http://192.168.1.158/_vti_pvt/WebTrend
Request Method	GET
Site Profile	Default Security Profile
Reference ID	E3BC-D624-B1C7-80AC

The raw request text is:

```
GET /_vti_pvt/WebTrend HTTP/1.0
Connection: Close
Pragma: no-cache
Accept: */*
Host: 192.168.1.158
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm
X-dotDefender-first-line: GET /_vti_pvt/WebTrend HTTP/1.0
```

The matching data section shows a hex dump with the following text highlighted in yellow:

```
000 : 2F 5F 76 74 69 5F 70 76 74 2F 57 65 62 54 72 65  /_vti_pvt/WebTre
010 : 68 64                                             nd
```

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.

For example, in this example:

- The **Category** of the attack is **Windows Directories and Files**.
- The **Sub-category** is **FrontPage Extension**.
- The **IP Address** is **192.168.1.22**.
- The **Reference ID** is **E3BC-D624_B1C7-80AC**.
- The substring is **_vti_pvt**.

5.2 Rule Categories

The dotDefender software has the following predefined rule categories:

Pattern	Description
Whitelist (Permitted Access List)	<p>A Whitelist 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.</p> <p>Whitelist rules are evaluated before all other dotDefender protection rules and signatures.</p>
Paranoid	<p>A collection of rules that provides a more restrictive level of security, but may interfere with web application usability.</p> <p>You can use this category to tighten security for sensitive applications or functionalities (for example, login or credit card details).</p>
Encoding	<p>Encoding is a method of representing characters in different ways for use in computer systems.</p> <p>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.</p> <p>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.</p>

Pattern	Description
Buffer Overflow	<p>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.</p>
SQL Injection	<p>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.</p> <p>SQL injection aims at penetrating back-end database(s) to manipulate data, thus stealing or modifying information in the database.</p>
Cross-Site Scripting	<p>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.</p> <p>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.</p> <p>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.</p> <p>There are two categories of cross-site scripting:</p> <ul style="list-style-type: none"> • 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.

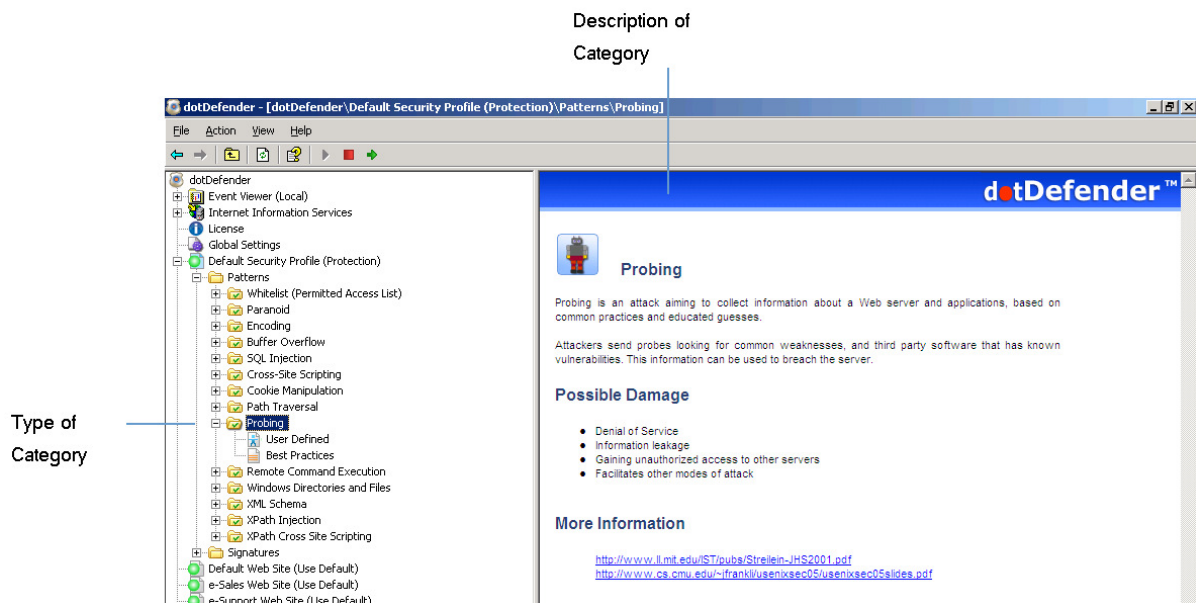
Pattern	Description
Cookie Manipulation	<p>Cookies are commonly used to store user and session identification information that serves as a means of authenticating users to the application. Cookie Manipulation refers to various methods of manipulation of cookie content. Using cookies, an attacker can obtain unauthorized access to the web server. CLRF Injection (Carriage Return/Line Feed) is an example of Cookie Manipulation.</p>
Path Transversal	<p>A URL is a web address translated into a path on the web server. A URL leads to specific directories and files residing on the web 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.</p> <p>Path traversal gains access to an organization's server files and directories that are otherwise inaccessible to external users.</p> <p>Path Traversing is implemented with common OS operations, such as using the characters <code>"../../../../"</code> for traversing between server directories and files.</p>
Probing	<p>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.</p>
Remote Command Execution	<p>A type of injection, similar to SQL Injection, except that it injects OS Shell commands into the Shell.</p>
Windows Directories and Files	<p>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.</p>
XML Schema	<p>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.</p> <p>Since the XML Schema describes all of the available service functions, hackers may use this information to discover vulnerabilities in the application.</p>

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**.
2. Select a pattern category. The description of the category is shown in the right pane.



5.3 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.

5.4 Configuring Patterns

To configure a pattern category:

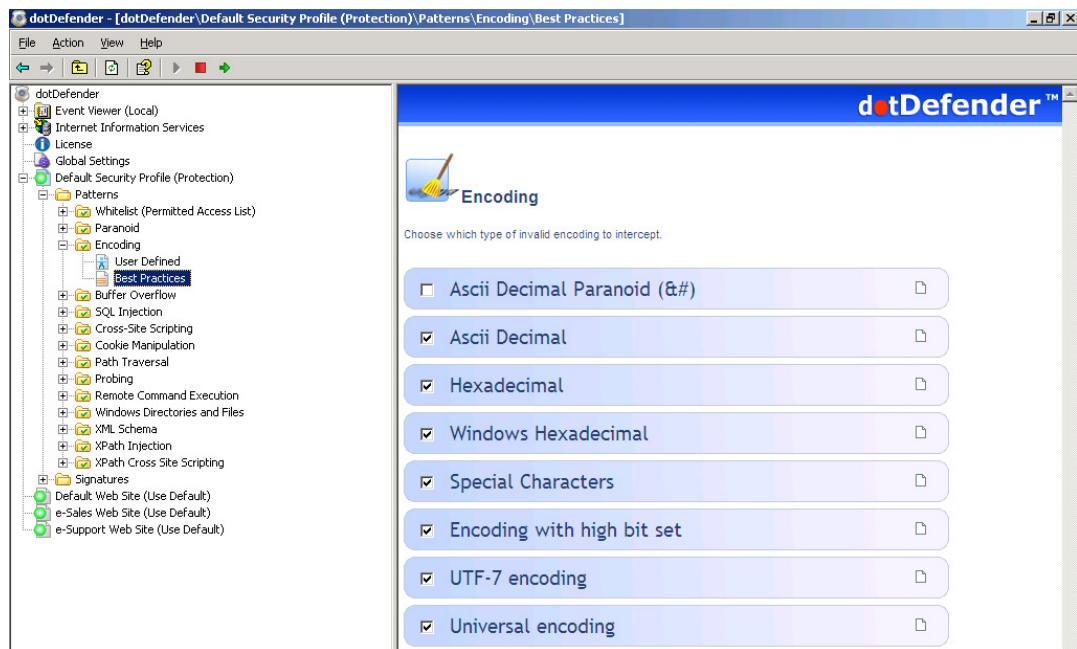
1. In the left pane of the Administration Console, select the required Profile.
2. Expand **Patterns**.
3. Expand the required pattern category.
4. Select one of the following:
 - ◆ [Modifying Best Practices](#)
 - ◆ [Adding User-Defined Rules](#)

5.4.1 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:

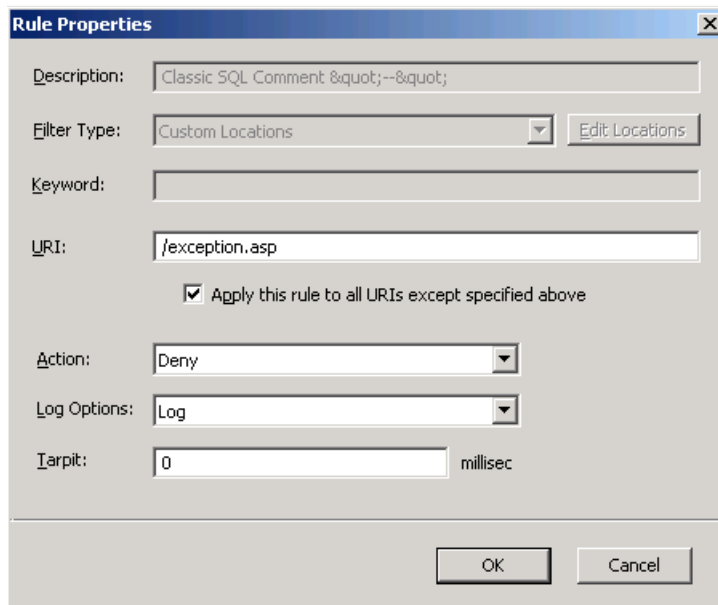
1. Select **Best Practices**. The sub-categories appear in the right pane.






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

Note: It is recommended to define the URI in the Rule Properties dialog box as “Allowed” rather than disable a rule.

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



4. In the **URI** field, enter a specific URI under which you want to apply a rule. By default, rules are applied to all URIs (all web pages). In the URI field, enter a specific URI under which you want to apply a rule.
 - ◆ To apply the rule to all URIs except the one you specified, select **Apply this rule to all URIs except specified above**.
5. From the **Action** drop-down list, select one of the following:
 - ◆ **Deny**: Denies this request.
 - ◆ **Allow**: Quits scanning at this sub-category after a pattern is matched.
 - ◆ **Monitor Only**: Monitors this sub-category after a pattern is matched.
6. From the **Log Options** drop-down list, select one of the following:
 - ◆ **Log**
 - ◆ **No Log**
7. 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.
8. Click **OK**. The  changes to .
9. Click  to apply the changes. The following window appears.



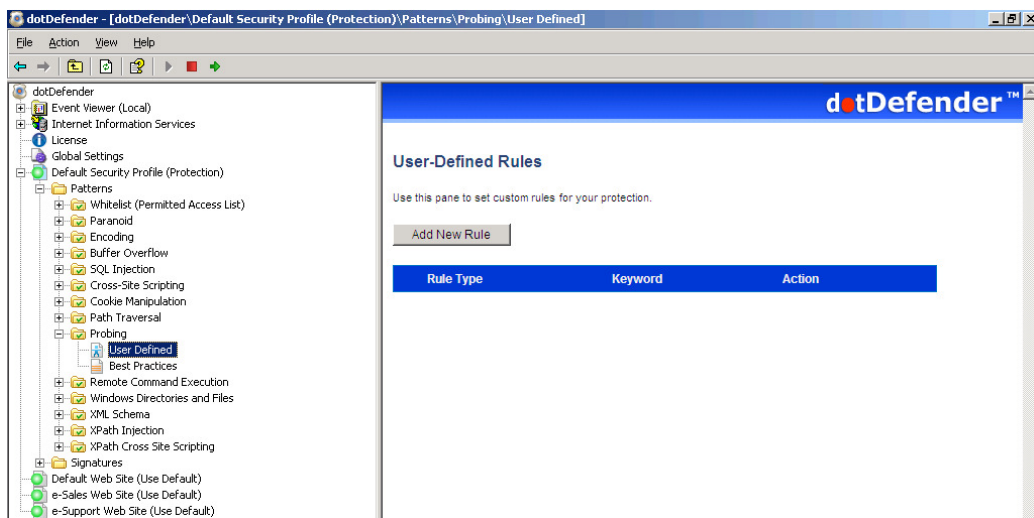
10. Click **OK**.

5.4.2 Adding User-Defined Rules

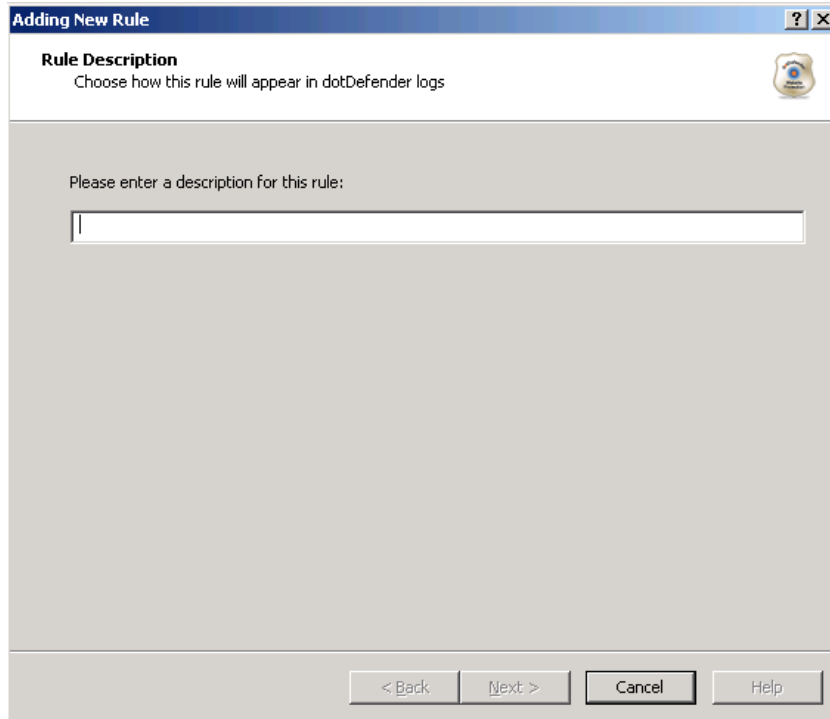
You can create new rules for dotDefender by using regular expressions to match a pattern that is to be blocked, allowed or monitored. Identify the pattern using the sub-string identified in the log. For further information, see [Managing Logs](#).

To add a new rule:

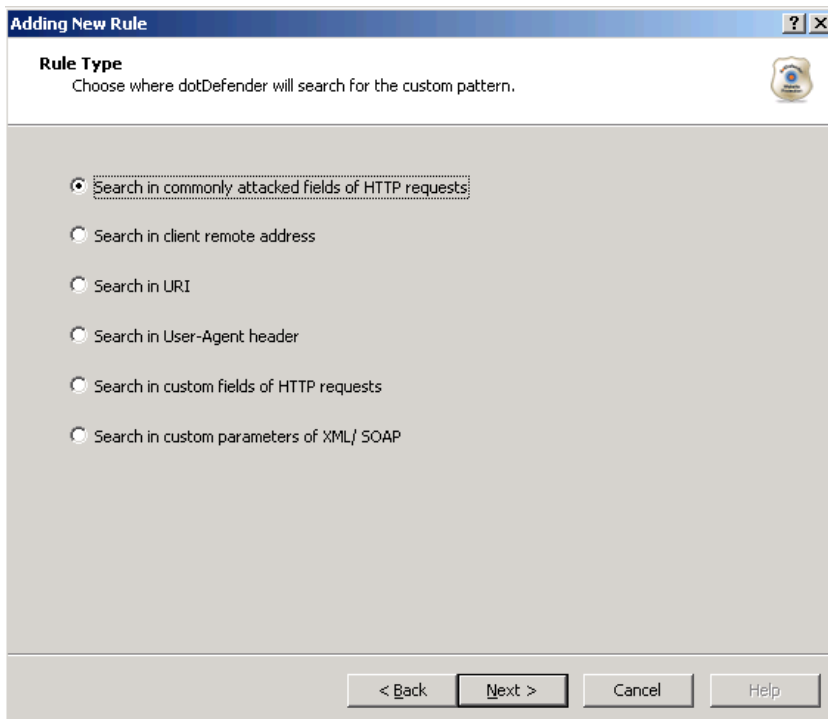
1. Click **User Defined** in any category. The User-Defined Rules list appears in the right pane.



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



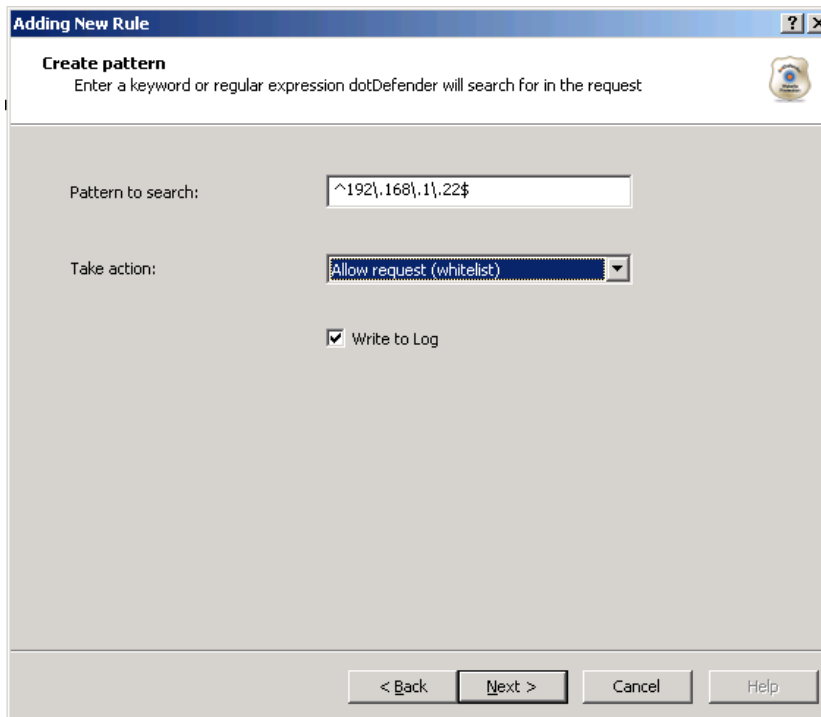
3. Type a description for the rule. Click **Next**.



4. 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 Commonly Attacked Fields of HTTP Request** – Search for pattern in the client’s IP address field. Click **Next** to continue. The Create pattern window appears.
 - ◆ **Searching in Commonly Attacked Fields of HTTP Request** - Search for pattern in the URI address. Click **Next** to continue. The Create pattern window appears.
 - ◆ **Searching in Commonly Attacked Fields of HTTP Request** – Search for pattern in the User-Agent client software identifier field. Click **Next** to continue. The Create pattern window appears.
 - ◆ **Searching in Client Remote Address**
 - ◆ **You can specify a pattern to search for in Client Remote Address.**

To search in Client Remote Address:

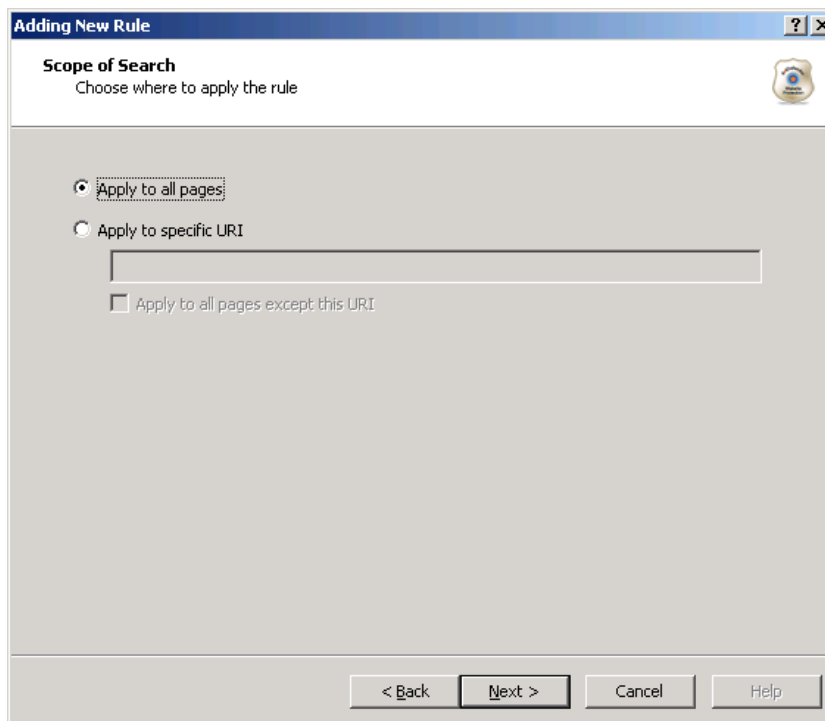
1. In the Create pattern window, in the **Pattern to Search** field, enter a regular expression for which dotDefender looks in the HTTP request. For further information, see **Regular Expressions**.



The screenshot shows a dialog box titled "Adding New Rule" with a "Create pattern" tab. The dialog contains the following elements:

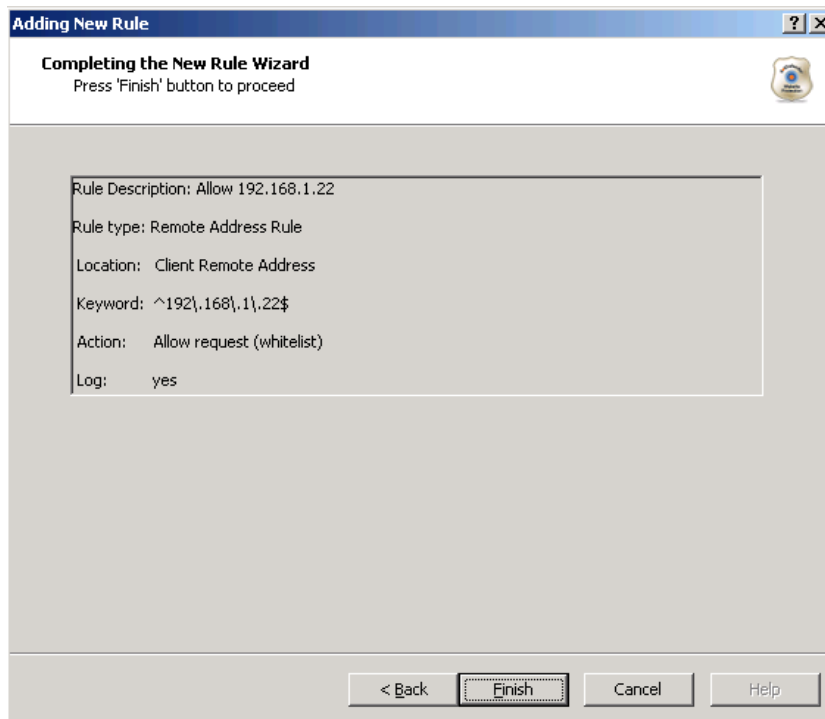
- Pattern to search:** A text input field containing the regular expression `^192\.,168\.,1\.,22$`.
- Take action:** A dropdown menu currently showing "Allow request (whitelist)".
- Write to Log:** A checked checkbox.
- Navigation:** Buttons for "< Back", "Next >", "Cancel", and "Help" are located at the bottom of the dialog.

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.

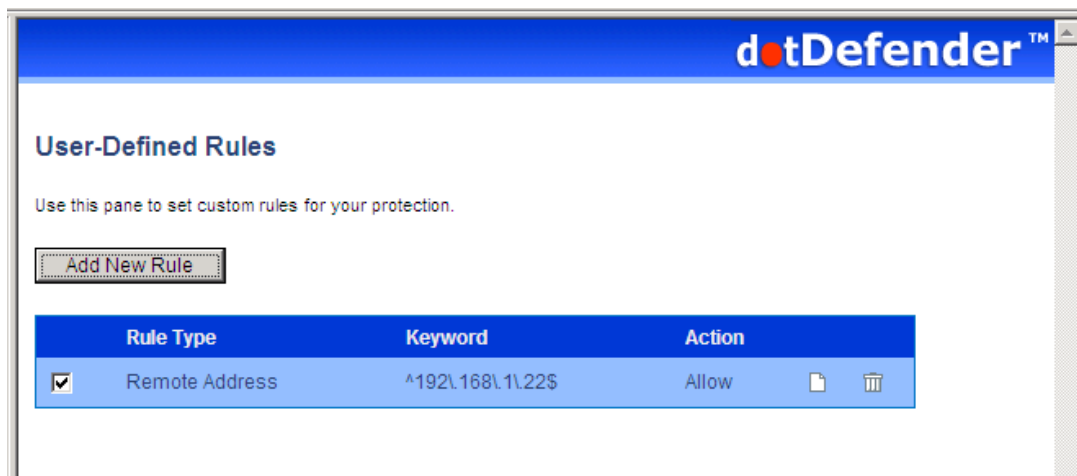


5. Select one of the following:
 - ◆ **Apply to all pages:** dotDefender applies the search to all HTTP pages.
 - ◆ **Apply to specific URI:** dotDefender applies the search to a specific URI. Enter the URI field.
 - ◆ **Apply to all pages except this URI:** dotDefender applies the search to all HTTP pages, excluding the specified URI.

- Click **Next**. 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.



- Click  to apply the changes. The following window appears.



9. Click **OK**.

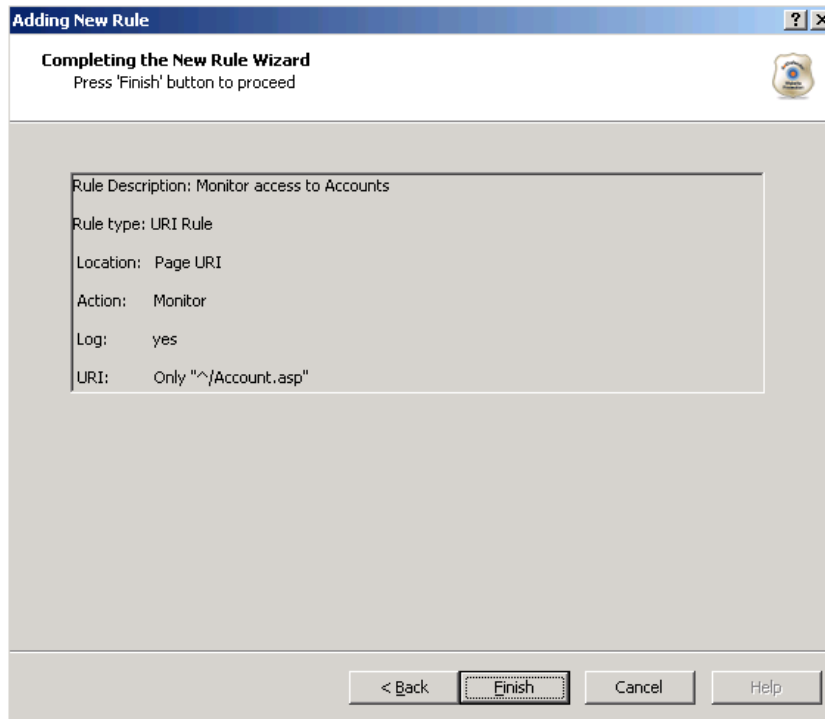
5.4.2.1 Searching in URI

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

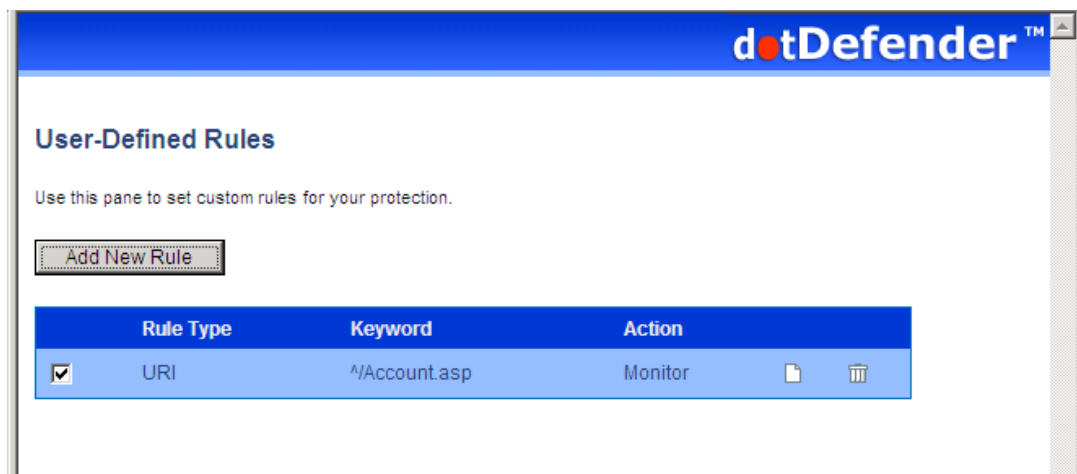
To search in URI:

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.

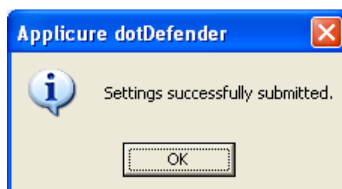
- Click **Next**. The **Completing the New Rule Wizard** window appears.



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



- Click  to apply the changes. The following window appears.



7. Click **OK**.

5.4.2.2 Searching in User-Agent

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

To search in User-Agent:

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**.

The screenshot shows a dialog box titled "Adding New Rule" with a "Create pattern" tab. Below the tab title is the instruction "Enter a keyword or regular expression dotDefender will search for in the request". The main area contains three fields: "Pattern to search:" with the text "olloBot" entered; "Take action:" with a dropdown menu showing "Block request"; and a checked checkbox labeled "Write to Log". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

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.

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

Adding New Rule [?] [X]

Scope of Search
Choose where to apply the rule

Apply to all pages

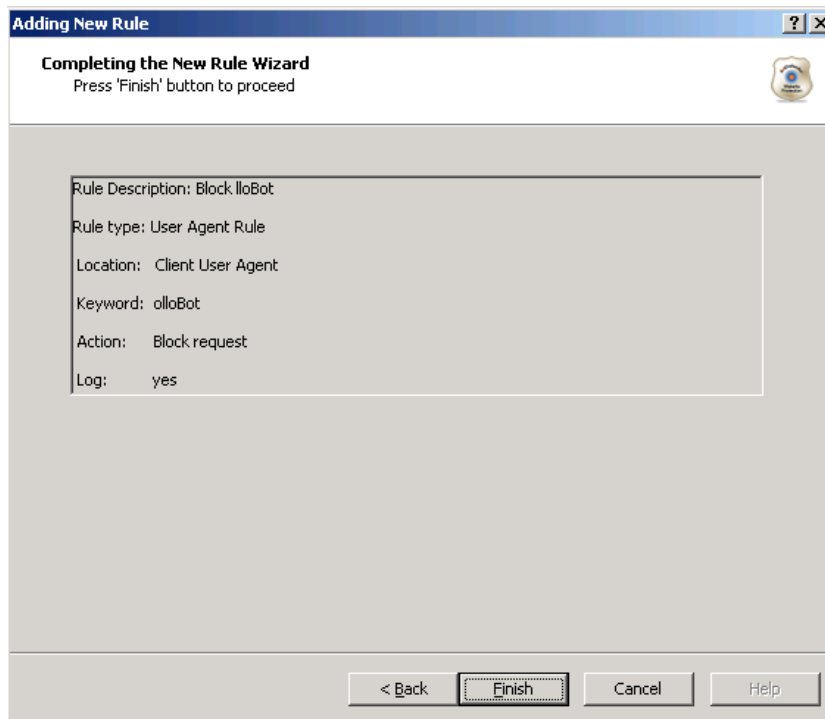
Apply to specific URI
/upload_content.asp

Apply to all pages except this URI

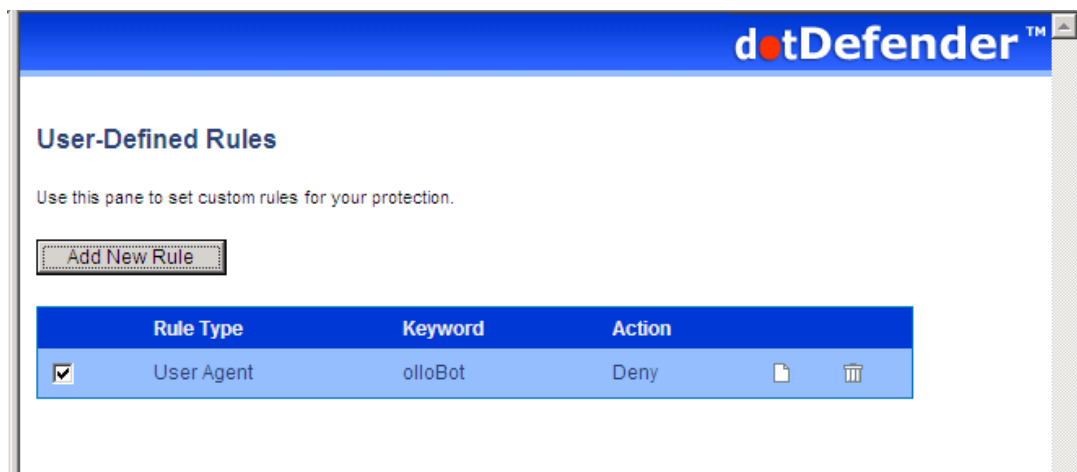
< Back Next > Cancel Help

- 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.

- Click **Next**. 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.



- Click  to apply the changes. The following window appears.



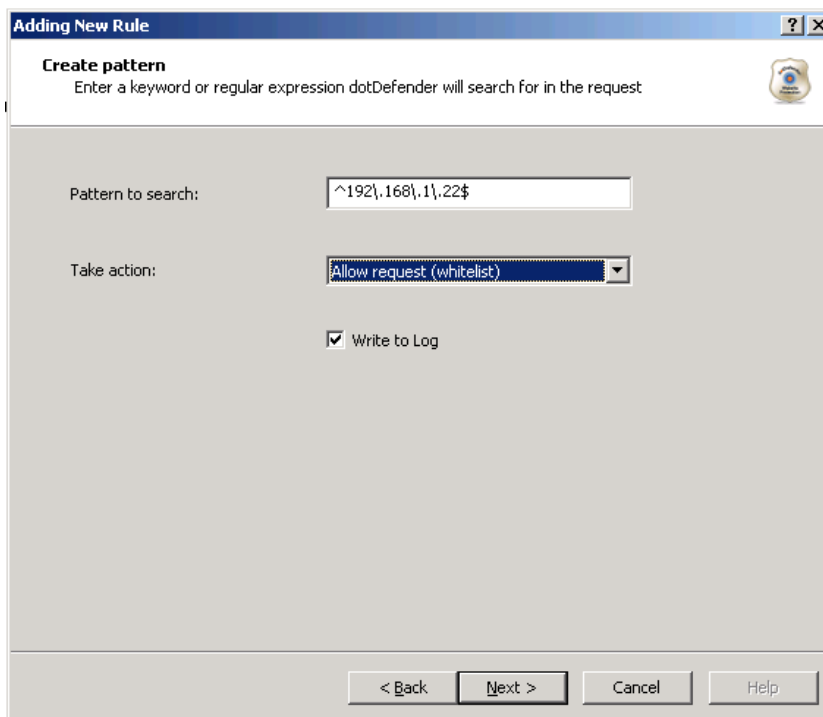
9. Click **OK**.

5.4.2.3 Searching in Custom Fields of HTTP Requests - Click Next to continue. The Custom Fields window appears. Continue with Searching in Client Remote Address

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

To search in Client Remote Address:

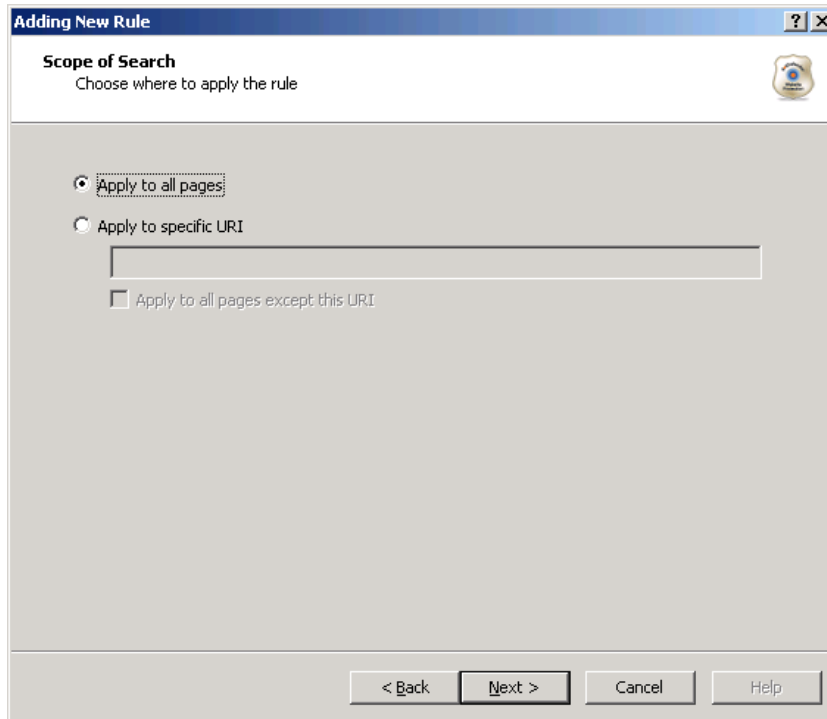
10. In the Create pattern window, in the **Pattern to Search** field, enter a regular expression for which dotDefender looks in the HTTP request. For further information, see **Regular Expressions**.



The screenshot shows a dialog box titled "Adding New Rule" with a "Create pattern" tab. The instruction reads: "Enter a keyword or regular expression dotDefender will search for in the request". The "Pattern to search:" field contains the regular expression `^192\.,168\.,1\.,22$`. The "Take action:" dropdown menu is set to "Allow request (whitelist)". The "Write to Log" checkbox is checked. At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

11. 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.
12. (Optional) Select the **Write to Log** checkbox if you want the events matching the rule to be logged.

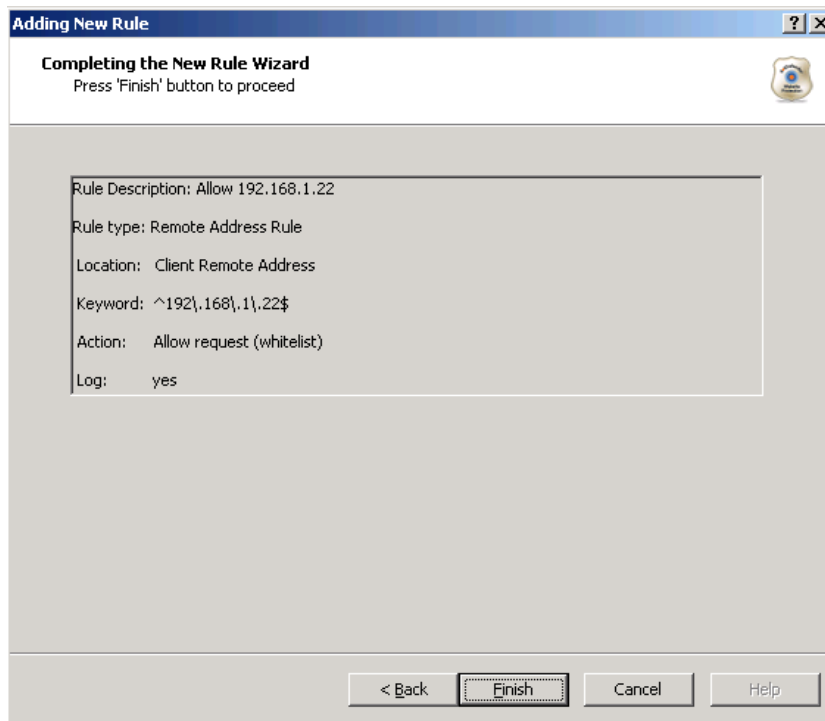
13. Click **Next** to continue. The Scope of Search window appears.



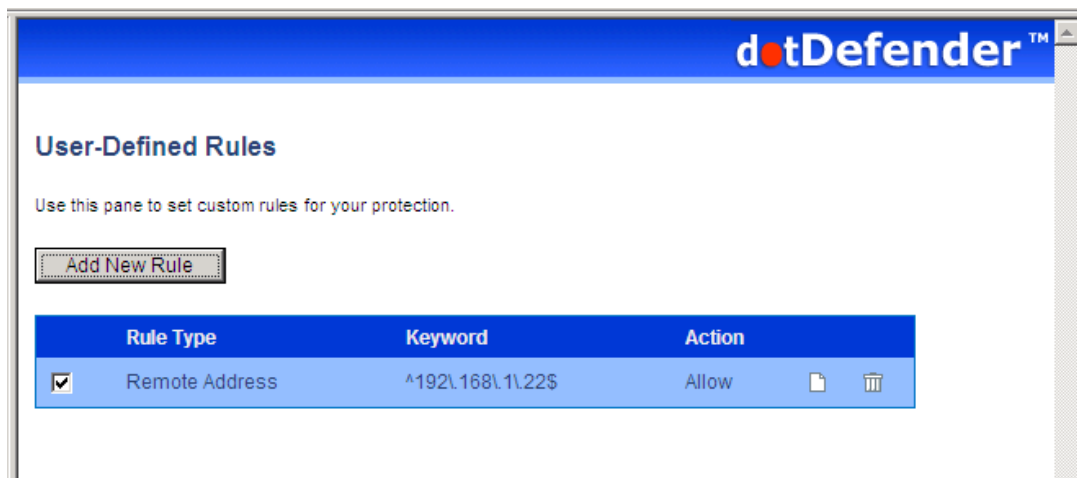
14. Select one of the following:

- ◆ **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.

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



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



17. Click  to apply the changes. The following window appears.



18. Click **OK**.

5.4.2.4 Searching in URI

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

To search in URI:

19. Select one of the following:

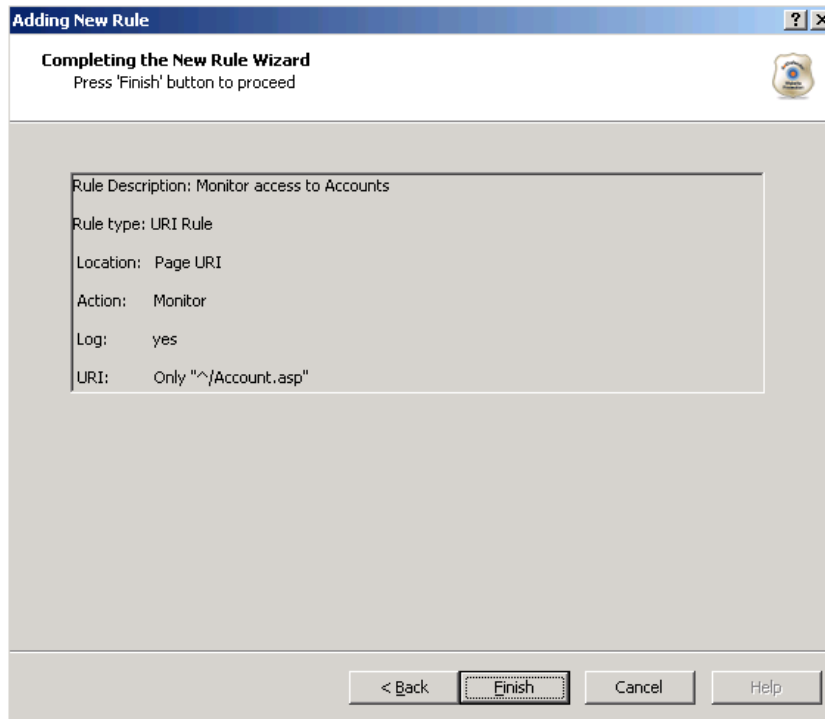
- ◆ **Apply to all pages:** dotDefender applies the search to all HTTP pages.
- ◆ **Apply to specific URI:** dotDefender applies the search to a specific URI. Enter the URI field.
- ◆ **Apply to all pages except this URI:** dotDefender applies the search to all HTTP pages, excluding the specified URI.

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

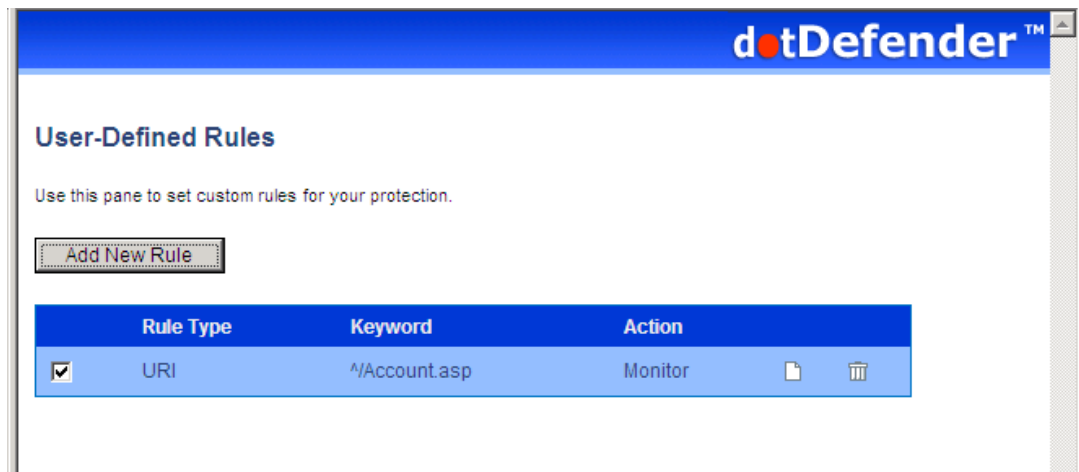
- ◆ **Block request:** dotDefender stops requests including this URI.
- ◆ **Allow request (Whitelist):** dotDefender allows requests including this URI.
- ◆ **Monitor:** dotDefender only logs HTTP requests including this URI.
- ◆ **Skip Category:** dotDefender excludes rules in this category for requests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

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

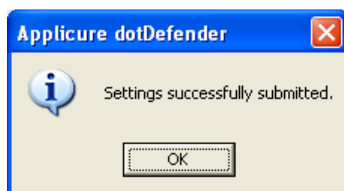
22. Click **Next**. The **Completing the New Rule Wizard** window appears.



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



24. Click  to apply the changes. The following window appears.



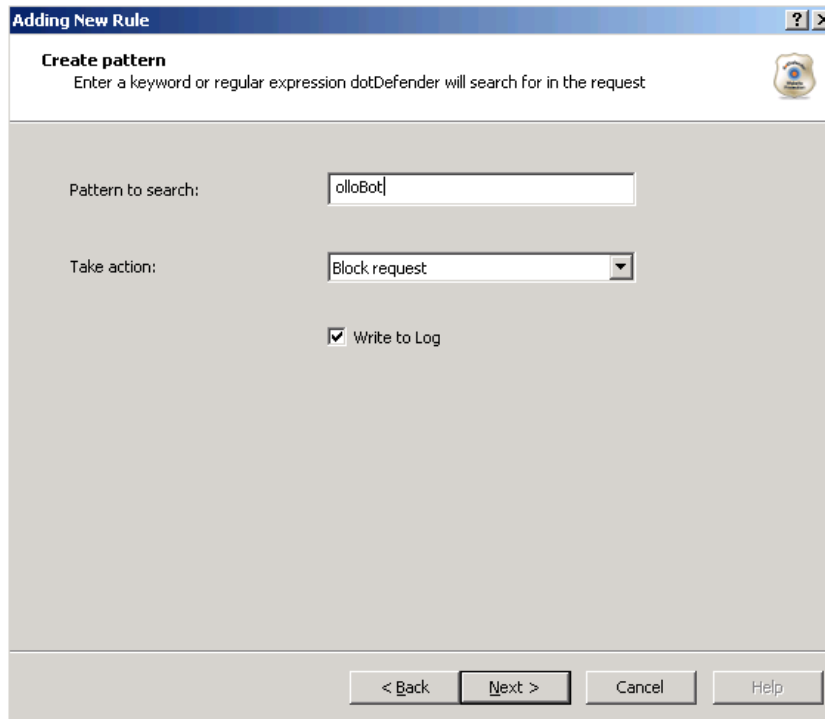
25. Click **OK**.

5.4.2.5 Searching in User-Agent

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

To search in User-Agent:

26. 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**.



27. 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.

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

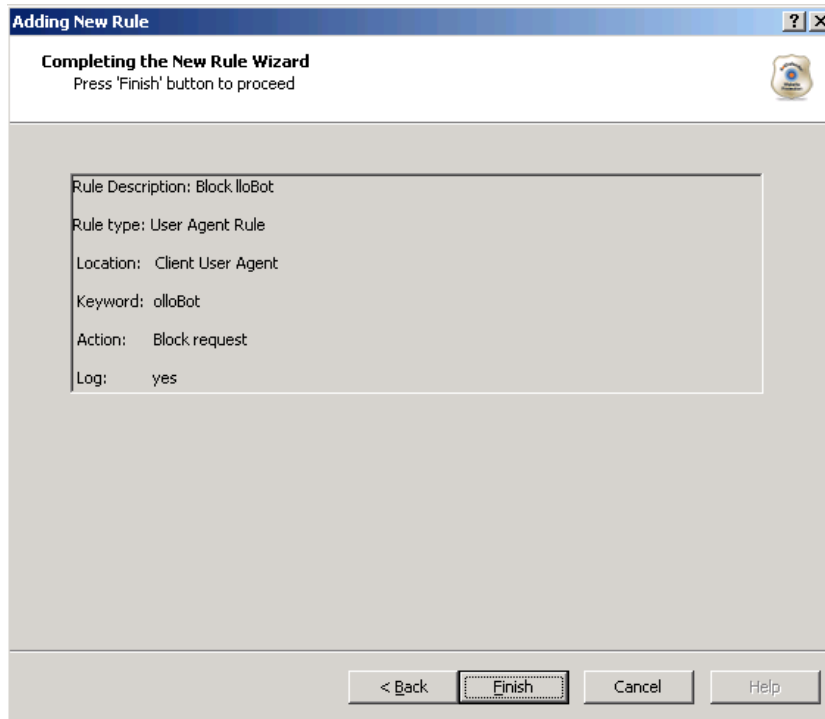
29. Click **Next** to continue. The Scope of Search window appears.

The screenshot shows a dialog box titled "Adding New Rule" with a sub-tab "Scope of Search". The instruction "Choose where to apply the rule" is displayed. There are three radio button options: "Apply to all pages", "Apply to specific URI", and "Apply to all pages except this URI". The "Apply to specific URI" option is selected, and a text input field below it contains the URI "/upload_content.asp". The "Apply to all pages except this URI" option is checked. At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

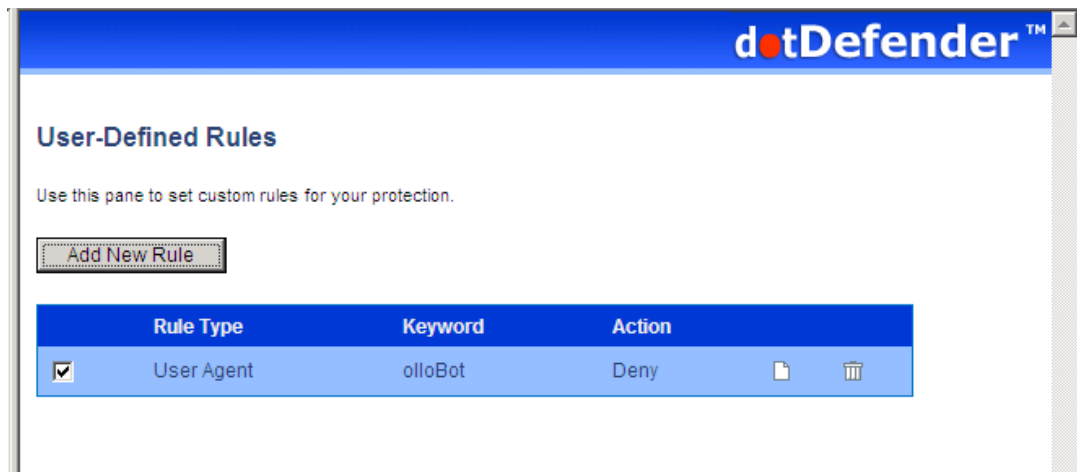
30. Select one of the following:

- ◆ **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.

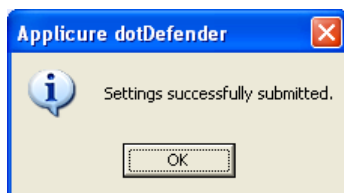
31. Click **Next**. The **Completing the New Rule Wizard** window appears.



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



33. Click  to apply the changes. The following window appears.



34. Click **OK**.

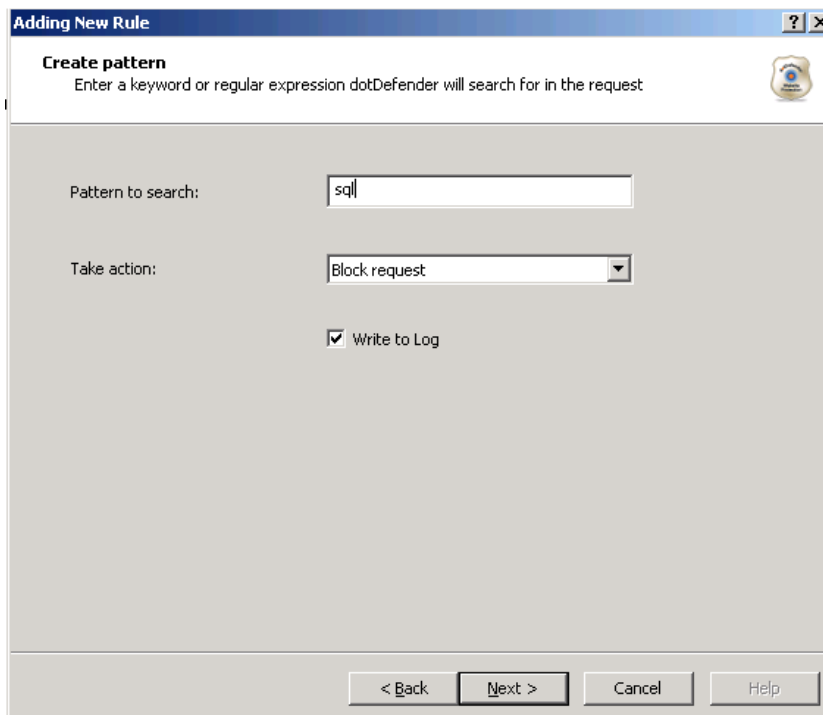
- ◆ Searching in Custom Fields of HTTP Requests
- ◆ **Search in custom parameters of XML/SOAP** - Click **Next** to continue. The Custom Fields window appears. Continue with [Searching in Custom Parameters of XML/SOAP](#).

5.4.2.6 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](#).

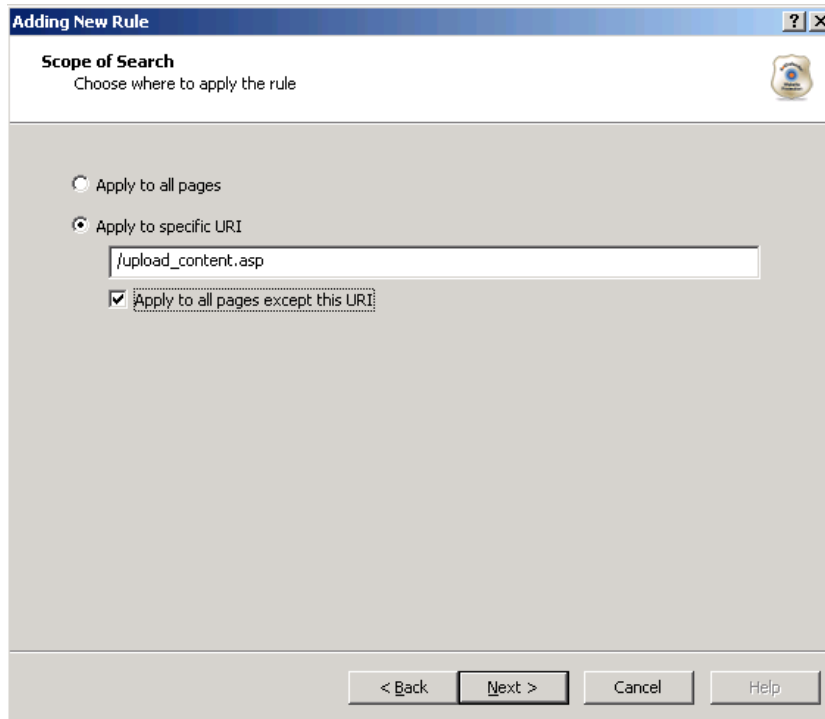


The screenshot shows a window titled "Adding New Rule" with a "Create pattern" tab. The window contains the following elements:

- A title bar with a question mark icon and a close button.
- A subtitle "Create pattern" and a description: "Enter a keyword or regular expression dotDefender will search for in the request".
- A text input field labeled "Pattern to search:" containing the text "sql".
- A dropdown menu labeled "Take action:" with "Block request" selected.
- A checked checkbox labeled "Write to Log".
- Four buttons at the bottom: "< Back", "Next >", "Cancel", and "Help".

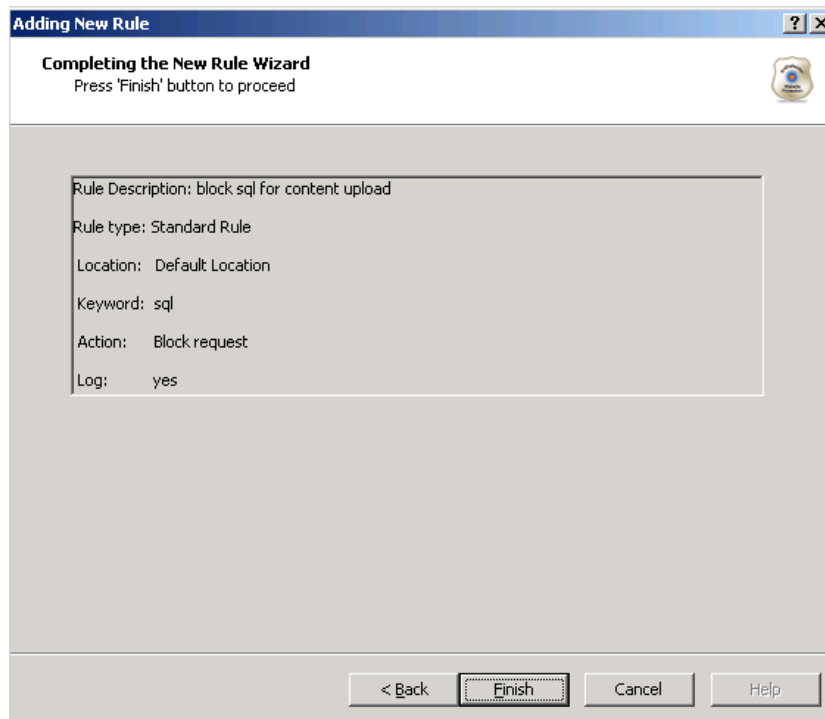
2. From the **Take action** drop-down list, select one of the following:
 - ◆ **Block request:** dotDefender stops requests containing the pattern.
 - ◆ **Allow request (Whitelist):** dotDefender allows requests containing the pattern.
 - ◆ **Monitor:** dotDefender only logs HTTP requests containing 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.

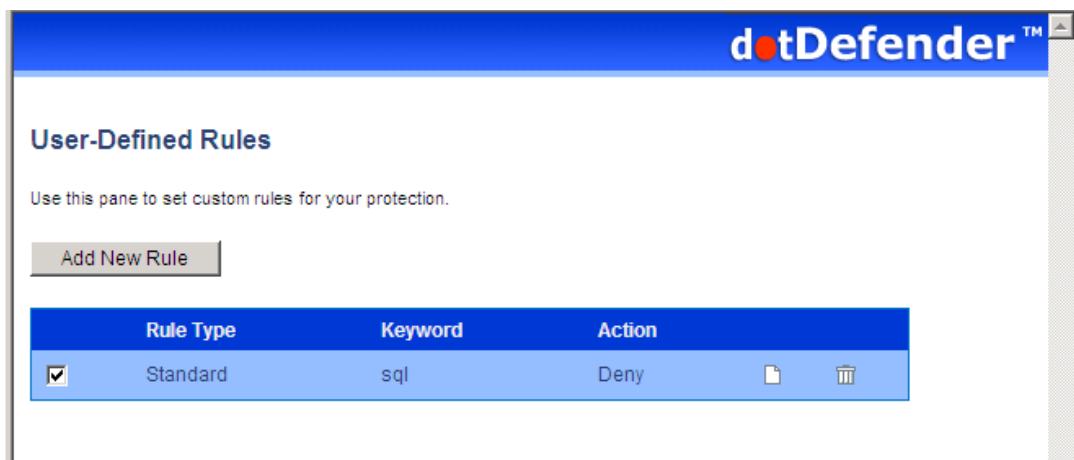


5. Select one of the following:
 - ◆ **Apply to all pages:** dotDefender applies the search to all HTTP pages.
 - ◆ **Apply to specific URI:** dotDefender applies the search to a specific URI. Enter the URI field.
 - ◆ **Apply to all pages except this URI:** dotDefender applies the search to all HTTP pages, excluding the specified URI.

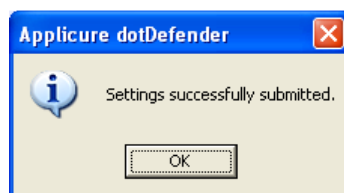
- Click **Next**. The **Completing the New Rule Wizard** window appears.



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



- Click  to apply the changes. The following window appears.



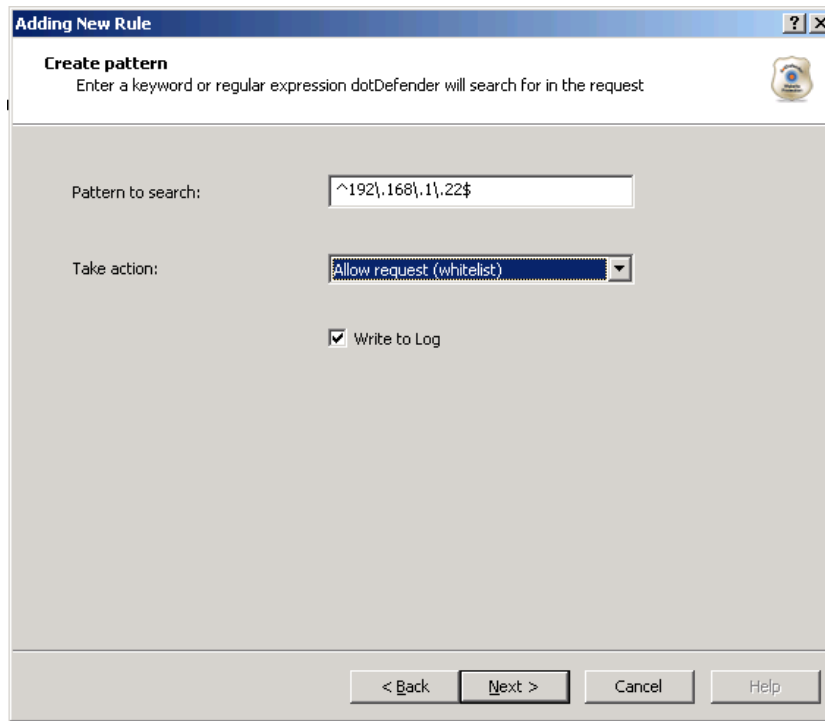
9. Click **OK**.

5.4.2.7 Searching in Client Remote Address

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

To search in Client Remote Address:

10. 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](#).

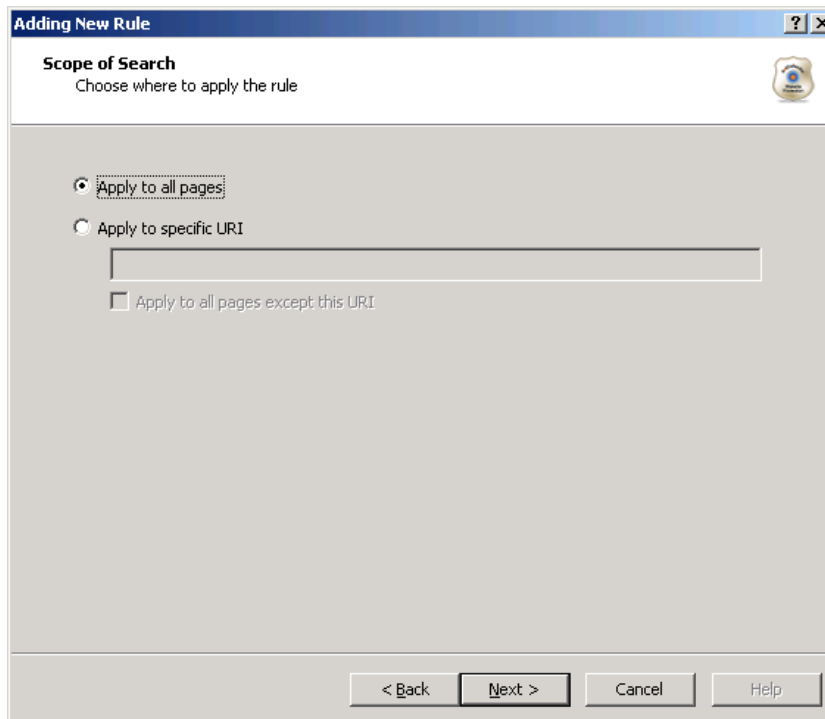


11. From the **Take action** drop-down list, select one of the following:

- ◆ **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.

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

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

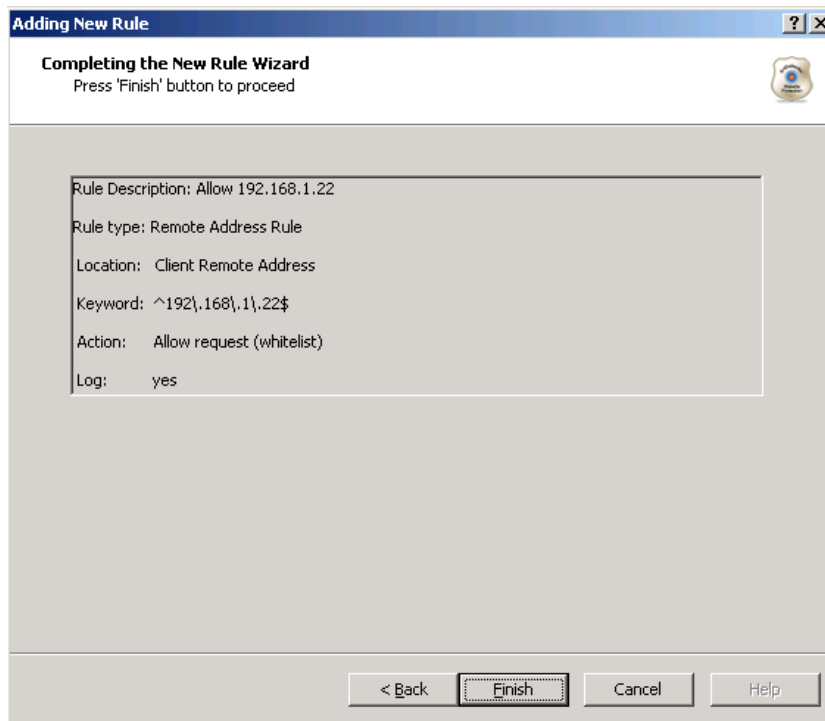


The screenshot shows a dialog box titled "Adding New Rule" with a "Scope of Search" tab. The subtitle is "Choose where to apply the rule". There are three radio button options: "Apply to all pages" (selected), "Apply to specific URI" (with an empty text input field below it), and "Apply to all pages except this URI" (with an unchecked checkbox). At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

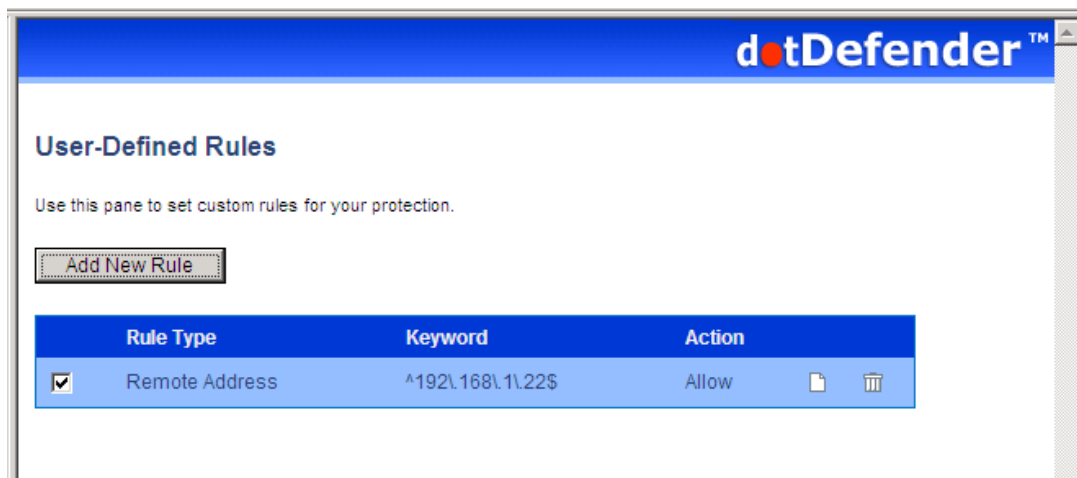
14. Select one of the following:

- ◆ **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.

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



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



17. Click  to apply the changes. The following window appears.



18. Click **OK**.

5.4.2.8 Searching in URI

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

To search in URI:

19. Select one of the following:

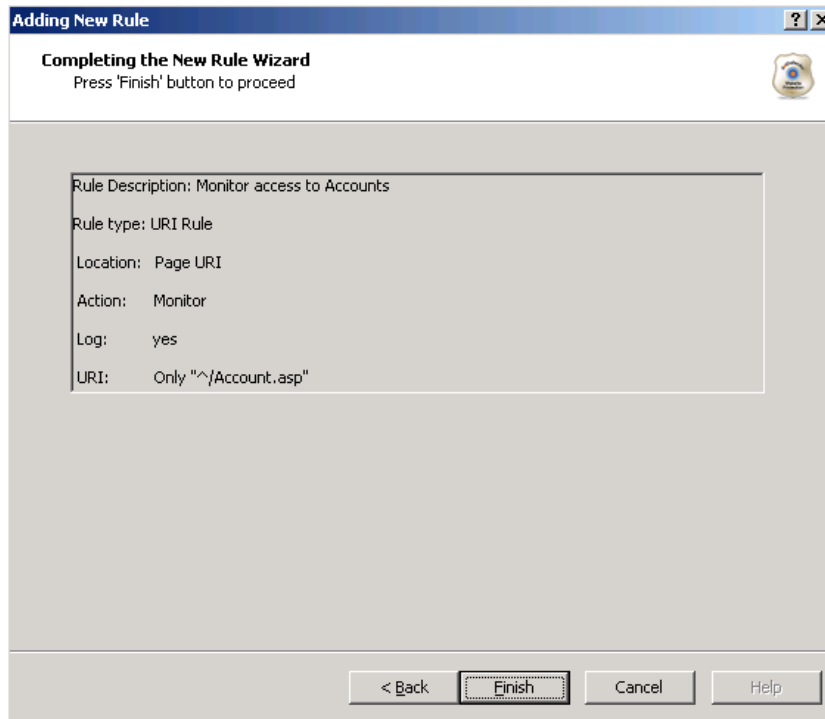
- ◆ **Apply to all pages:** dotDefender applies the search to all HTTP pages.
- ◆ **Apply to specific URI:** dotDefender applies the search to a specific URI. Enter the URI field.
- ◆ **Apply to all pages except this URI:** dotDefender applies the search to all HTTP pages, excluding the specified URI.

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

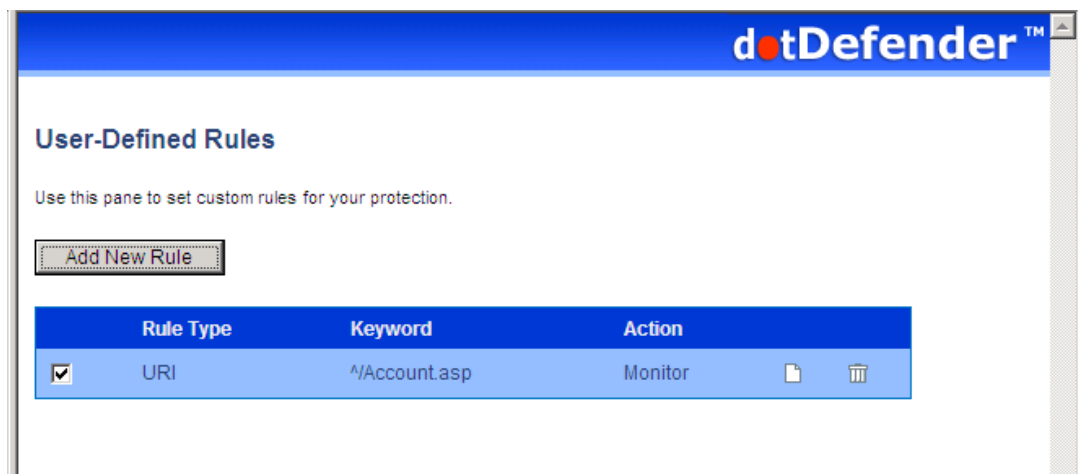
- ◆ **Block request:** dotDefender stops requests including this URI.
- ◆ **Allow request (Whitelist):** dotDefender allows requests including this URI.
- ◆ **Monitor:** dotDefender only logs HTTP requests including this URI.
- ◆ **Skip Category:** dotDefender excludes rules in this category for requests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

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

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



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



24. Click  to apply the changes. The following window appears.



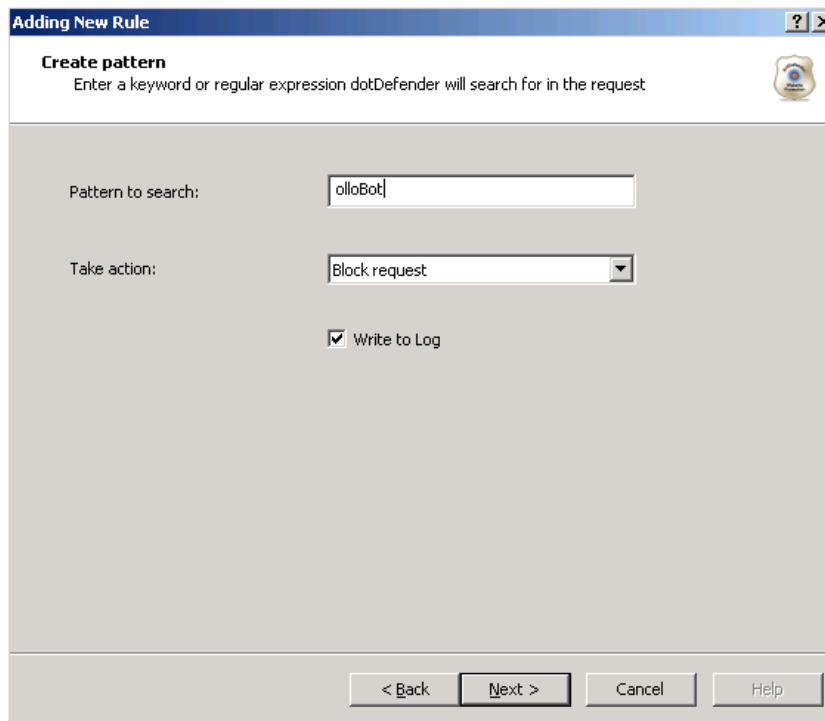
25. Click **OK**.

5.4.2.9 Searching in User-Agent

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

To search in User-Agent:

26. 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](#).



The screenshot shows a dialog box titled "Adding New Rule" with a "Create pattern" tab. The dialog contains the following elements:

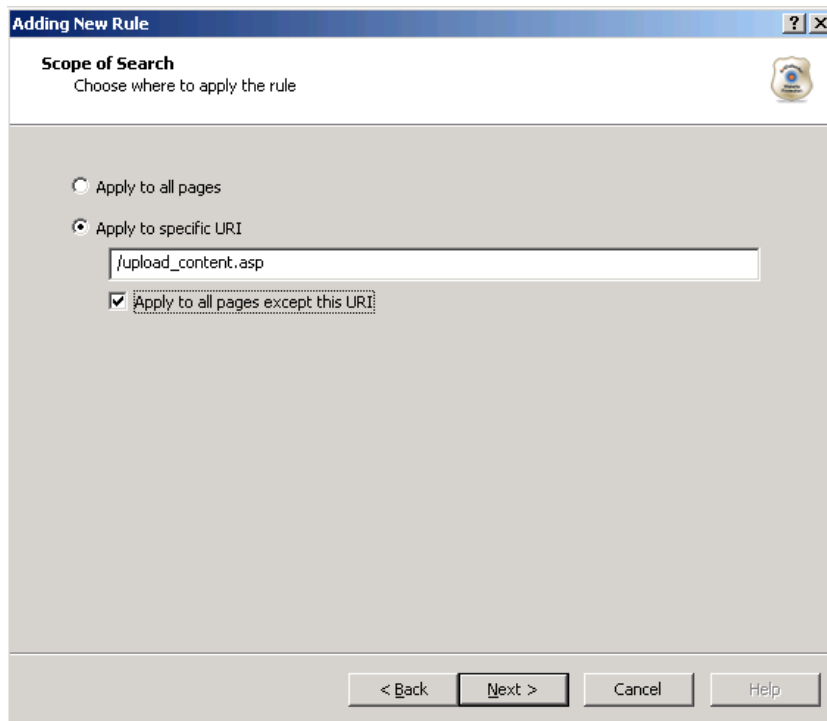
- Pattern to search:** A text input field containing the text "olloBot".
- Take action:** A dropdown menu with "Block request" selected.
- Write to Log:** A checked checkbox.
- Navigation buttons:** "< Back", "Next >", "Cancel", and "Help".

27. 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.

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

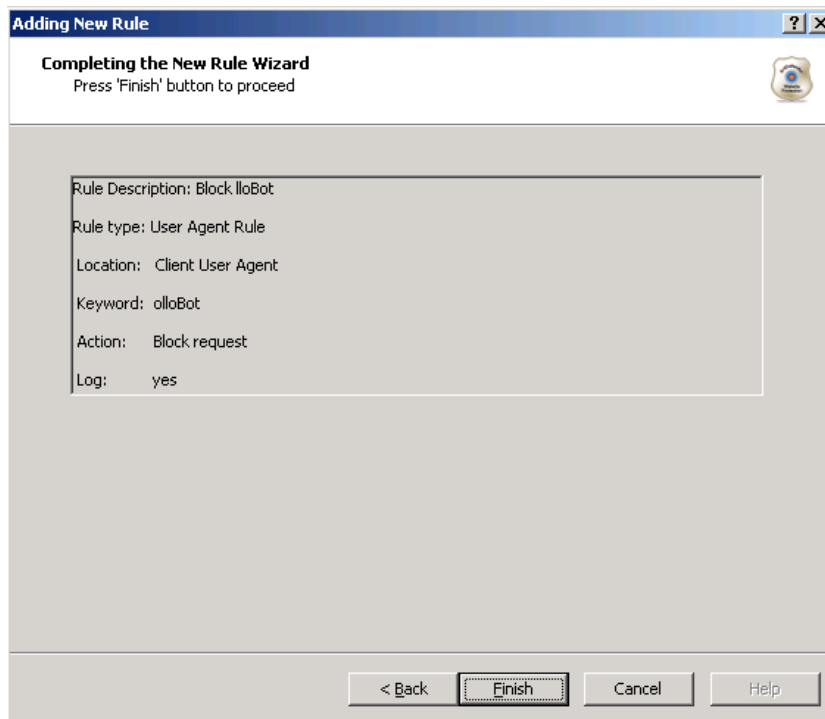
29. Click **Next** to continue. The Scope of Search window appears.



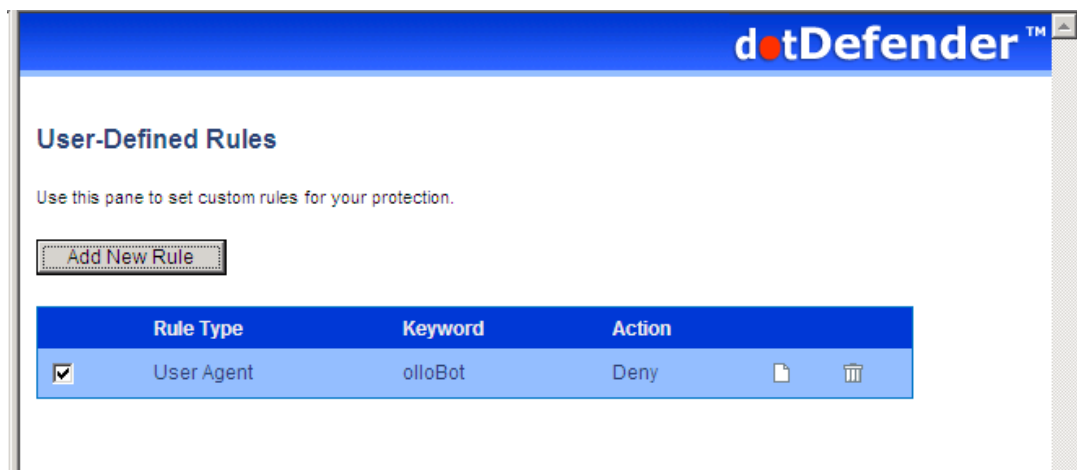
30. Select one of the following:

- ◆ **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.

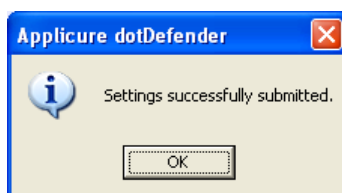
31. Click **Next**. The **Completing the New Rule Wizard** window appears.



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



33. Click  to apply the changes. The following window appears.



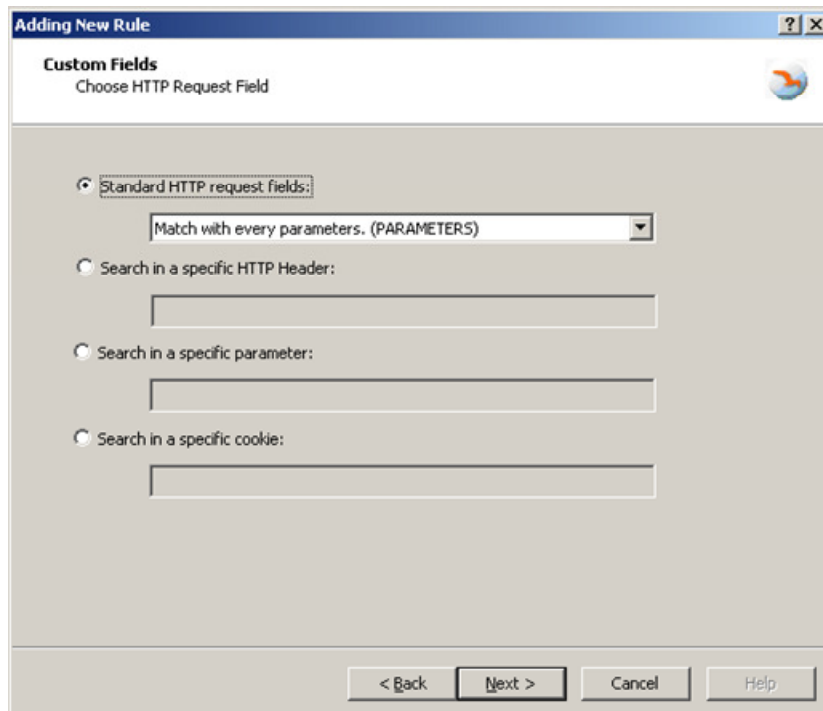
34. Click **OK**.

5.4.2.10 Searching in Custom Fields of HTTP Requests

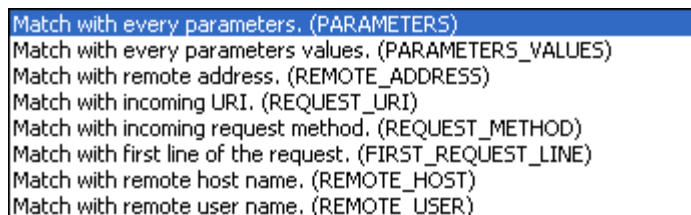
You can specify a pattern in specific fields of HTTP requests.

To search in custom fields of HTTP requests:

1. In the Adding New Rule window, select the type of HTTP request field for which you want to define a rule.

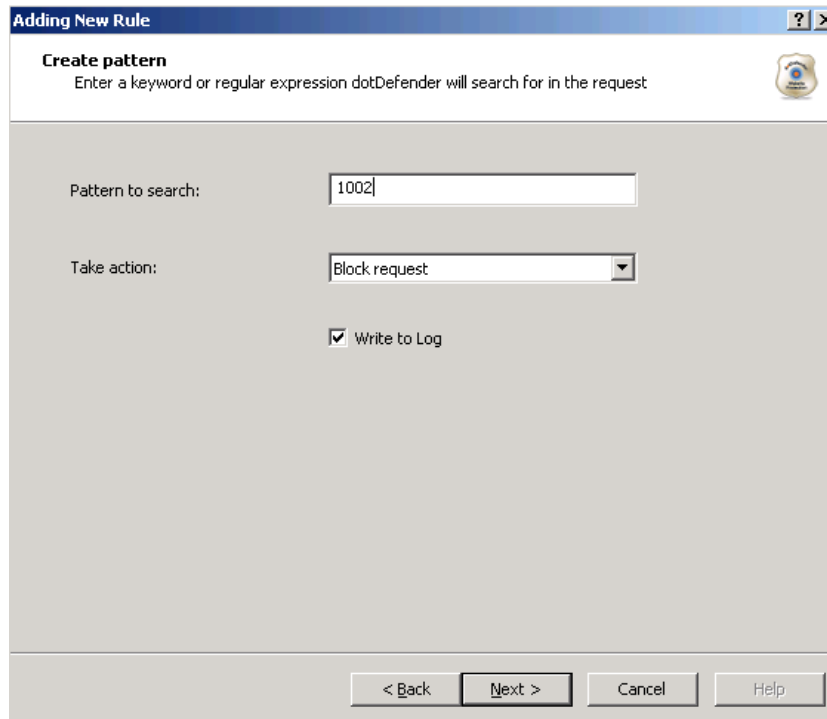


- ◆ **Standard HTTP request fields:** Applies the rule to a standard HTTP request field. Select an option from the drop-down list.



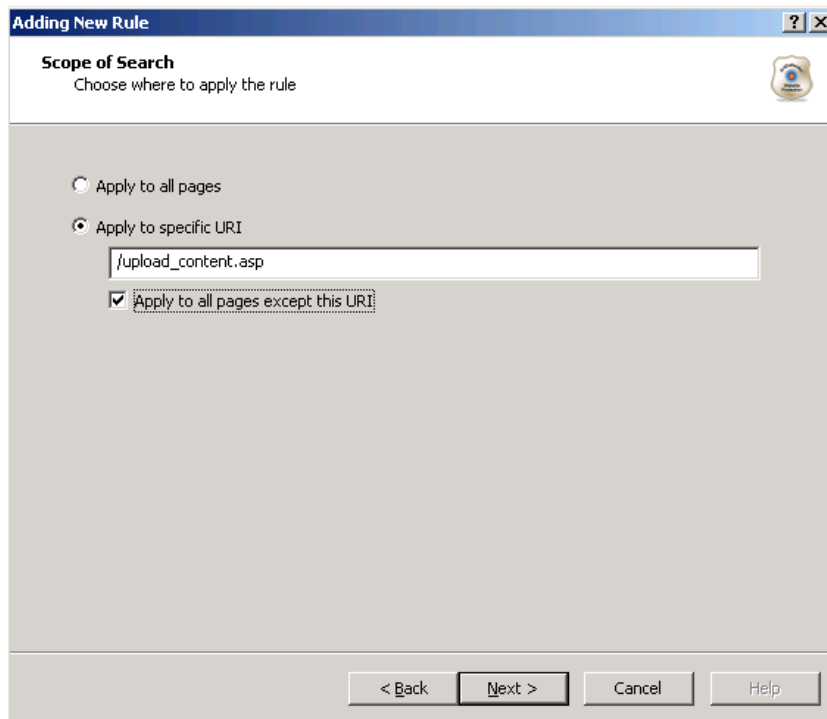
- **Search in a specific HTTP Header:** Applies the rule to a specific HTTP header. Enter the HTTP Header.
- **Search in a specific parameter:** Applies the rule to the specified GET or POST parameter. Enter the GET or POST parameter.

- **Search in a specific cookie:** Applies the rule to a specified cookie. Enter the cookie name.
2. Click **Next**. The Create pattern window is displayed.

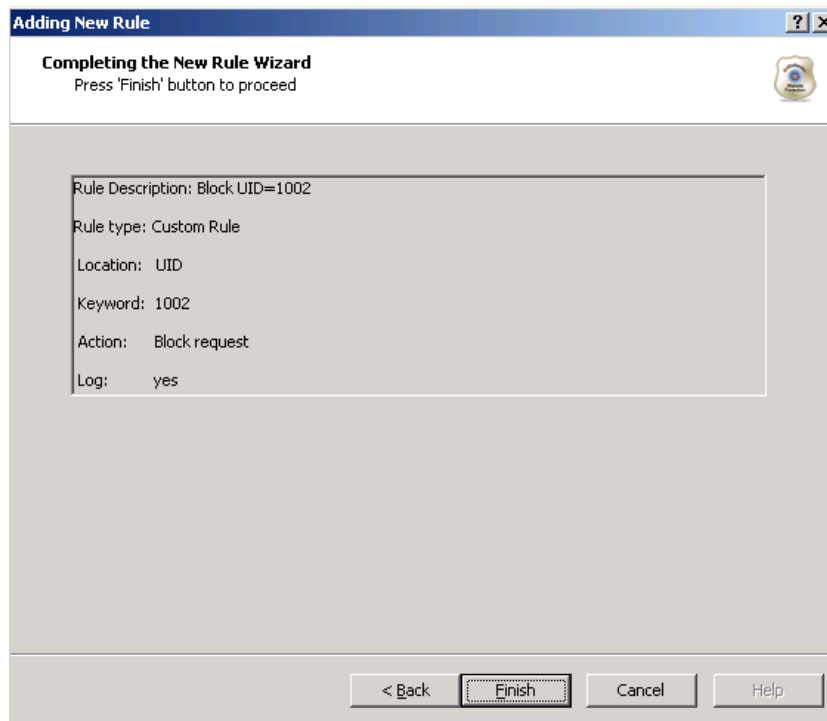


The screenshot shows a window titled "Adding New Rule" with a sub-header "Create pattern". Below the sub-header is the instruction "Enter a keyword or regular expression dotDefender will search for in the request". The main area contains three fields: "Pattern to search:" with the value "1002", "Take action:" with a dropdown menu showing "Block request", and a checked checkbox labeled "Write to Log". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

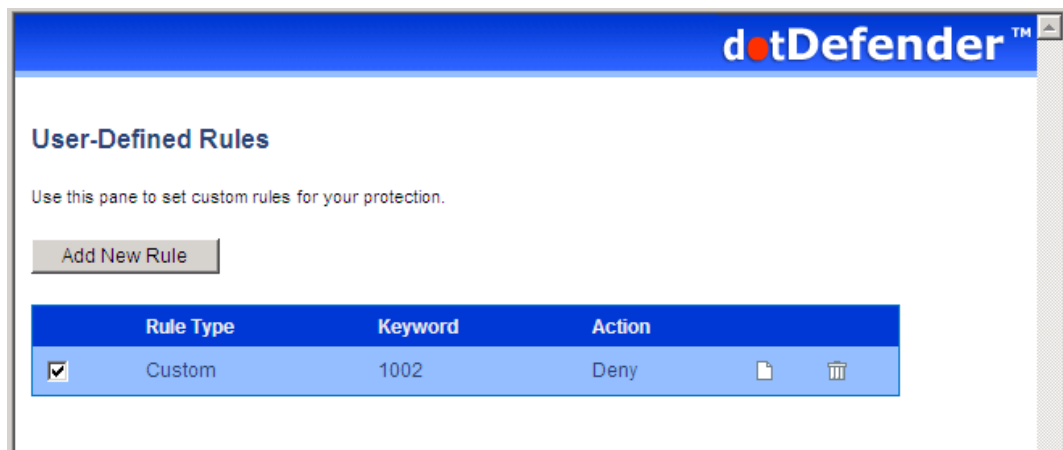
3. In the **Pattern to search** field, enter a regular expression for which dotDefender looks in the HTTP request. For further information, see [Regular Expressions](#).
4. From the **Take action** drop-down list, select the action to be taken when a pattern is matched:
 - ◆ **Block request:** dotDefender stops 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.
5. (Optional) Select the **Write to Log** checkbox if you want HTTP requests containing the pattern to appear as Log events.
6. Click **Next**. The Scope of Search window appears.



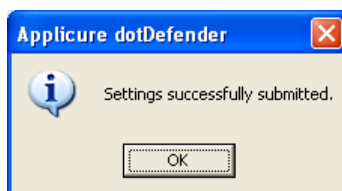
7. Select one of the following:
 - ◆ **Apply to all pages:** dotDefender applies the search to all HTTP pages.
 - ◆ **Apply to specific URI:** dotDefender applies the search to a specific URI. Enter the URI field.
 - ◆ **Apply to all pages except this URI:** dotDefender applies the search to all HTTP pages, excluding the specified URI.
8. Click **Next**. 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.



- Click  to apply the changes. The following window appears.



- Click **OK**.

5.4.2.11 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)

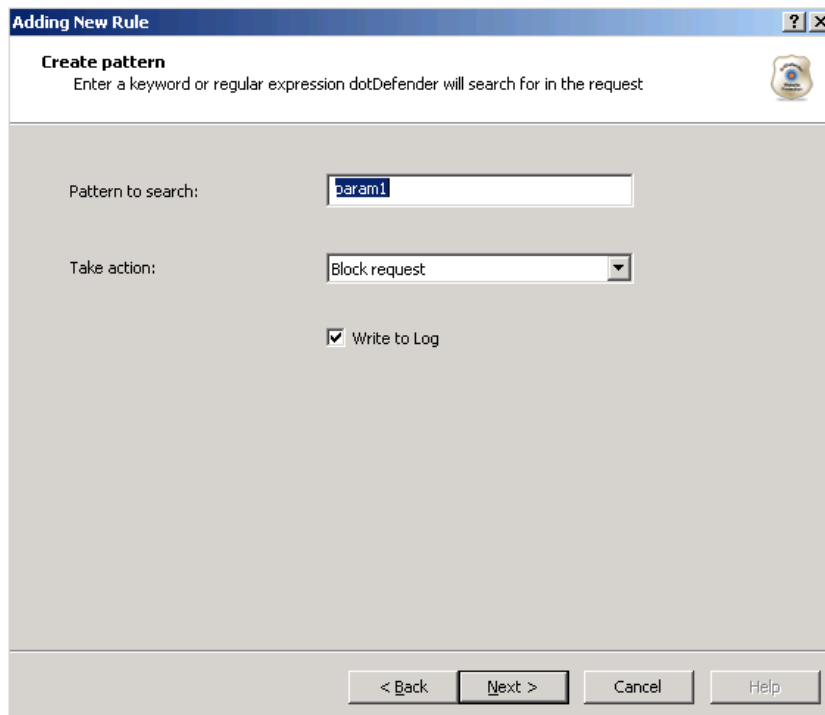
To search in custom parameters of XML/SOAP elements:

1. In the XML Parameters window, do one of the following:

- ◆ Select **Element from schema** and set the schema properties as follows:
 - a) Click **Import** to add a referable schema.
 - b) Select a **.wsdl** or **.xsd** file and click **Open**. The file is added to the **Schema** area.
 - c) Select the **Service** from the drop-down list.
 - d) Select the **Method** from the drop-down list.
 - e) Select the **Element**.
- ◆ 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.

2. Click **Next** to continue. The Create pattern window appears.

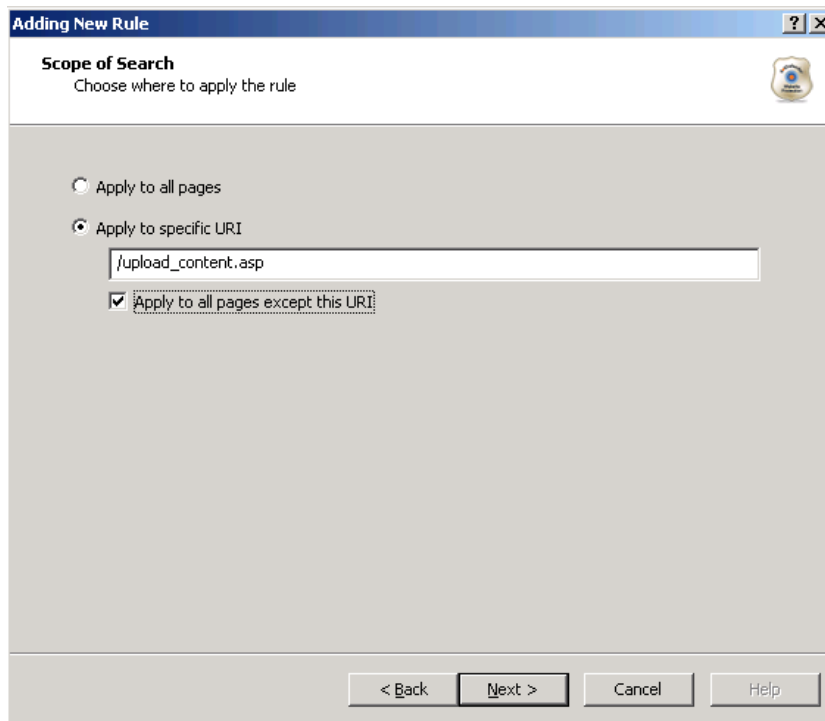


The screenshot shows a dialog box titled "Adding New Rule" with a sub-header "Create pattern". Below the sub-header is the instruction: "Enter a keyword or regular expression dotDefender will search for in the request". The dialog contains the following fields and controls:

- "Pattern to search:" text label followed by a text input field containing "param1".
- "Take action:" text label followed by a dropdown menu with "Block request" selected.
- A checked checkbox labeled "Write to Log".
- At the bottom, four buttons: "< Back", "Next >", "Cancel", and "Help".

3. 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.
4. Enter a regular expression for which dotDefender looks in the HTTP request. For further information, see [Regular Expressions](#).
5. 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.
6. (Optional) Select **Write to Log** so that HTTP requests containing the pattern appear as Log events.

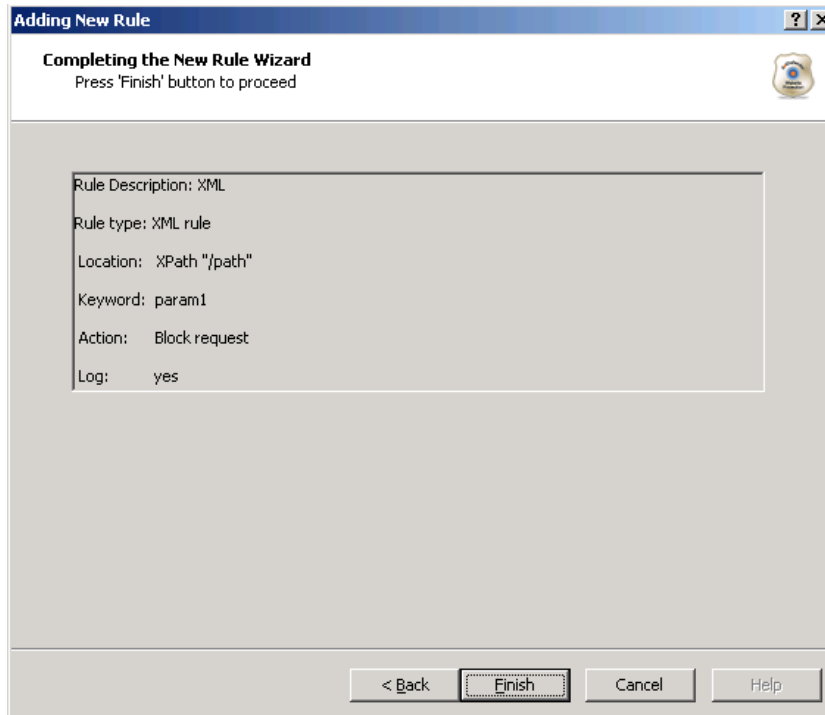
7. Click **Next**. The Scope of Search window appears.



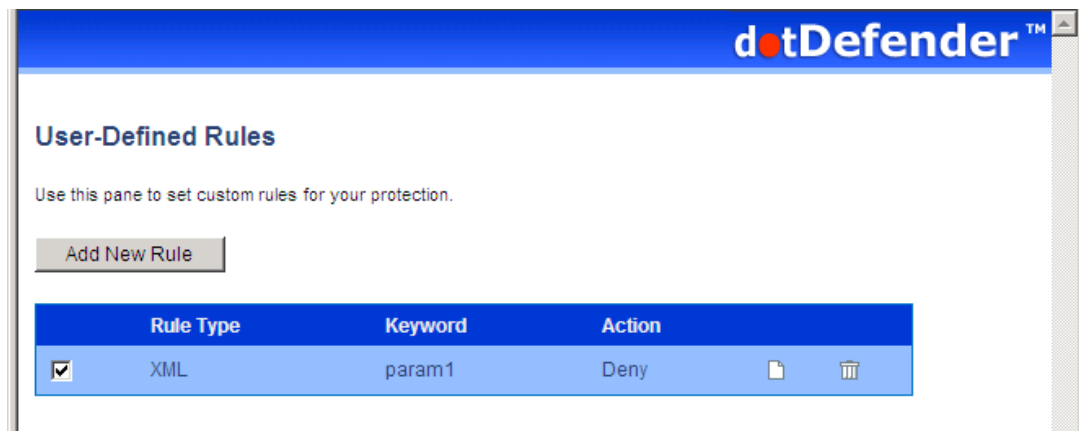
8. Select one of the following:

- ◆ **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.

- Click **Next**. 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.



- Click to apply the changes. The following window appears.



12. Click **OK**.

5.4.3 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](#)

5.4.3.1 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:




- **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.

5.4.3.2 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:

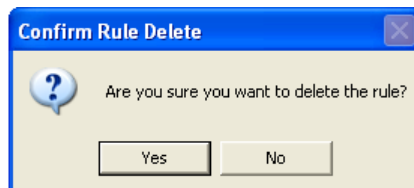
1. Click / to select/deselect a User-Defined Rule.
2. Click  for the changes to take effect. The following window appears.




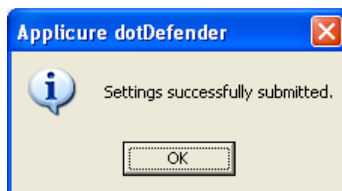
3. Click **OK**.

5.4.3.3 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.



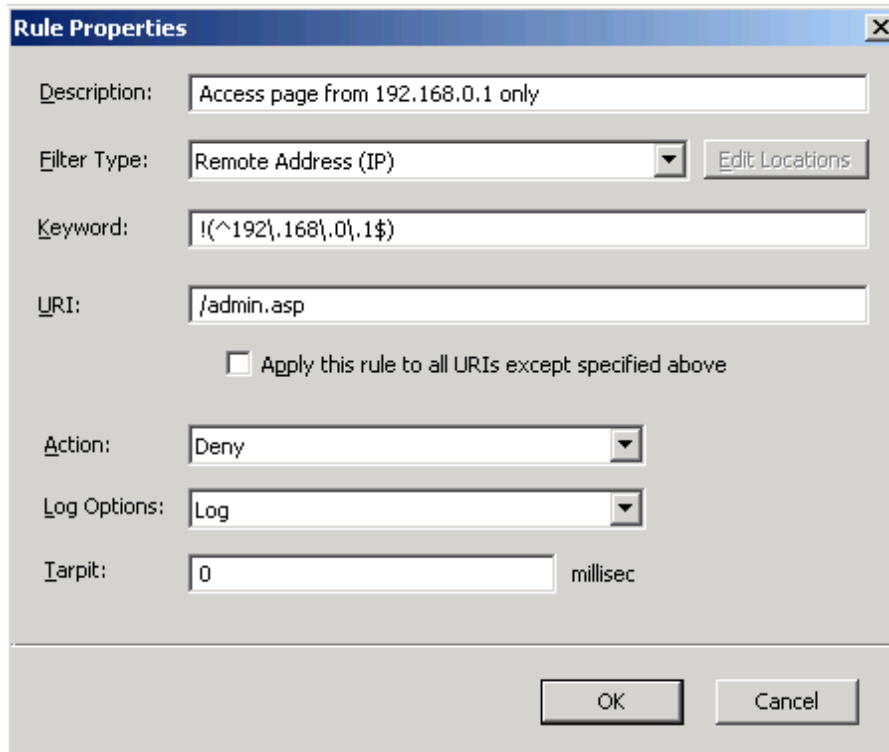
4. Click **OK**.

5.4.3.4 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:

- 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](#).

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

Rule Properties

Description: User Defined Rule

Filter Type: User Agent

Keyword: SpamBot

URI: /Sensitive_form.asp

Apply this rule to all URIs except specified above

Action: Deny

Log Options: Log

Tarpit: 10000 millisec

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.

- Select the required **Filter Type** from the list below:

Filter Type: Custom locations

Keyword: Recommended locations

URI: Remote Address (IP)

User Agent

Custom locations

Recommended Locations – Commonly attacked locations

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

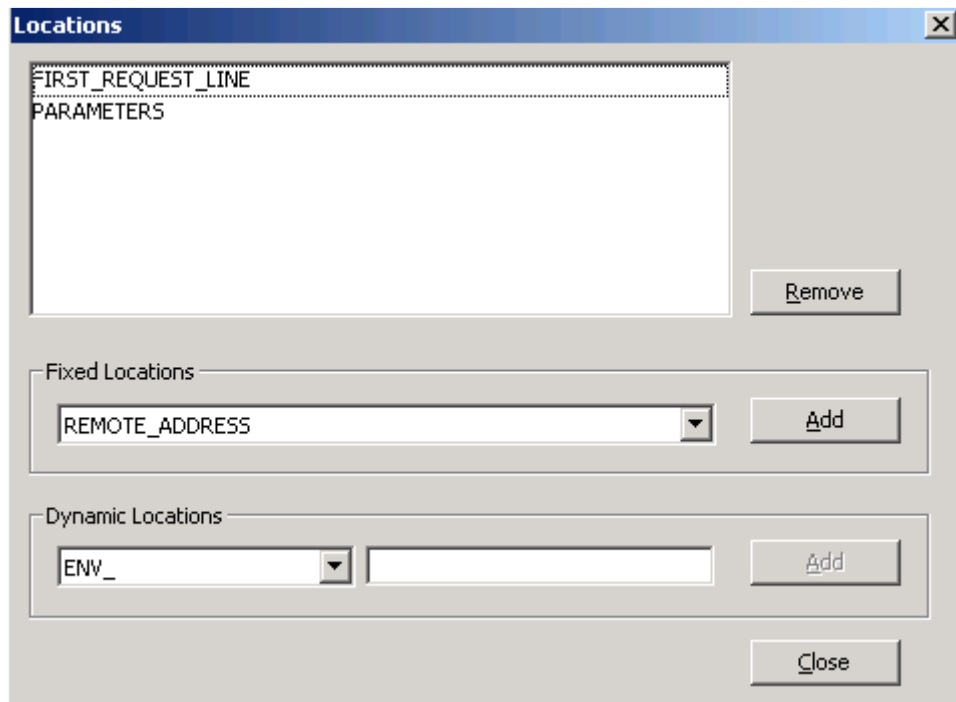
URI - The relative application URL address including parameters

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
AUTEXTYPE	HTTP authentication type. For example: Basic Authentication
SERVER_NAME	Host name as appears in the HOST header. For example: www.applicure.com
SERVER_SOFTWARE	Version of the IIS server
FIRST_REQUEST_LINE	The first line of the full HTTP request, as received by IIS
REQUEST_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

Field	Description
PARAMETERS_VALUES	Parameter values only
XML_VALUES	XML values only

- 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

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

5.5 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

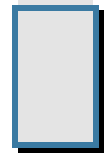
- MPack Protection

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.



Configuring Global Settings

This chapter explains the server wide settings available in dotDefender

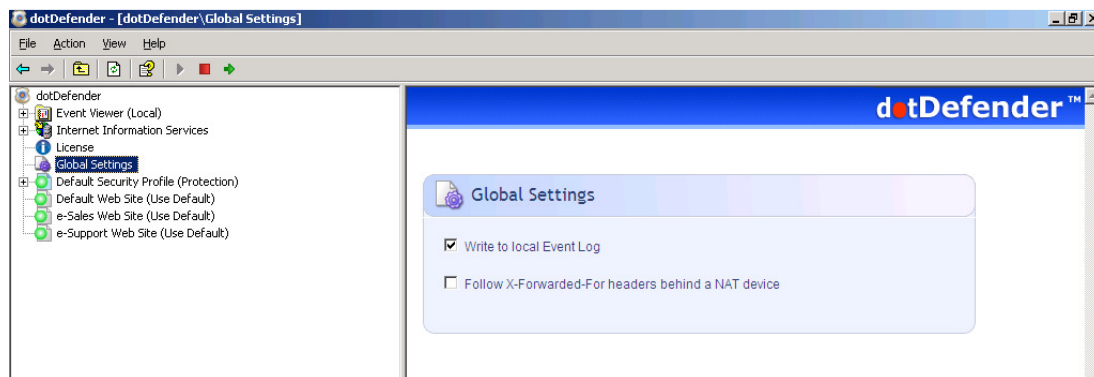
This chapter contains the following sections:


- [Enabling/Disabling logging to Windows Event Logs](#)
- [Enabling/Disabling NAT support](#)

6.1 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.



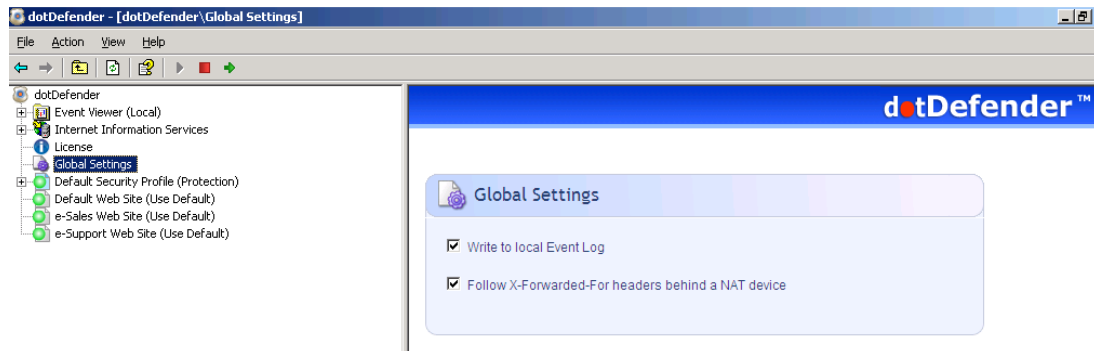
2. Select the **Write to Local Event Log** option to enable the logging globally.
3. Click  to apply the changes.


6.2 Enabling / Disabling NAT Support

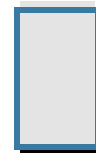
The NAT support feature allows dotDefender to properly identify client IP addresses while working behind a NAT device such as: load balancer, proxy, and firewall. Using the X-Forwarded-For HTTP header, the frontend device communicates the original client address as seen within the request.

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.



FAQs and Troubleshooting

This chapter contains the following sections:

- [FAQs](#) (Frequently Asked Questions)
- [Troubleshooting](#)

7.1 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?](#)
- [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?](#)
- [How do I remove the database when it 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?](#)
- [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 keep getting blocked at a content upload page, and I cannot upload new content.](#)

7.1.1 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.

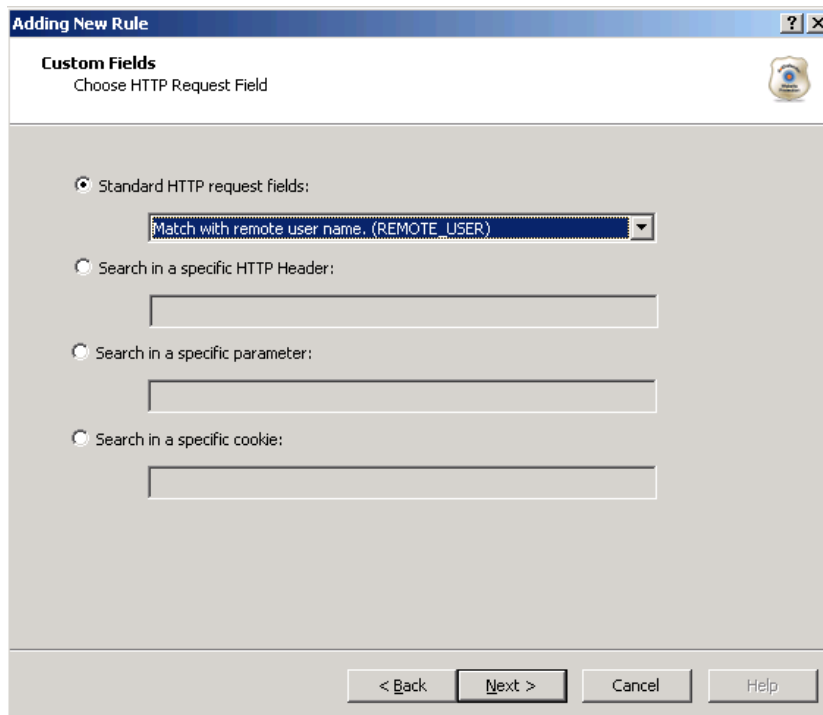
1. Open the dotDefender Administration Console.
2. Expand the required Profile.
3. Expand **Patterns**.
4. Expand **Whitelist**.
5. Select **User Defined**.
6. In the right pane, click **Add New Rule**.
7. In the Rule Type window, select **Search in client remote address** and click **Next**.
8. To white-list 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$`
9. To white-list a range of IP addresses, in the Create Pattern window, enter a regular expression representing the range. For example, to white-list the range 10.20.54.0-10.20.68.255, enter:
`^10\.20\.((5[4-9])|(6[0-8]))\.[([0-9])|([1-9][0-9])|(1[0-9][0-9])|(2[0-4][0-9])|(25[0-5]))$`
10. In the same window, in the **Take Action** field, select **white-list** and choose whether to log all events for the IP or not.
11. Click **Next**.
12. In the Scope to Search window, click **Next** and then click **Finish**.
13. Click  for the settings to take effect. The following window appears.



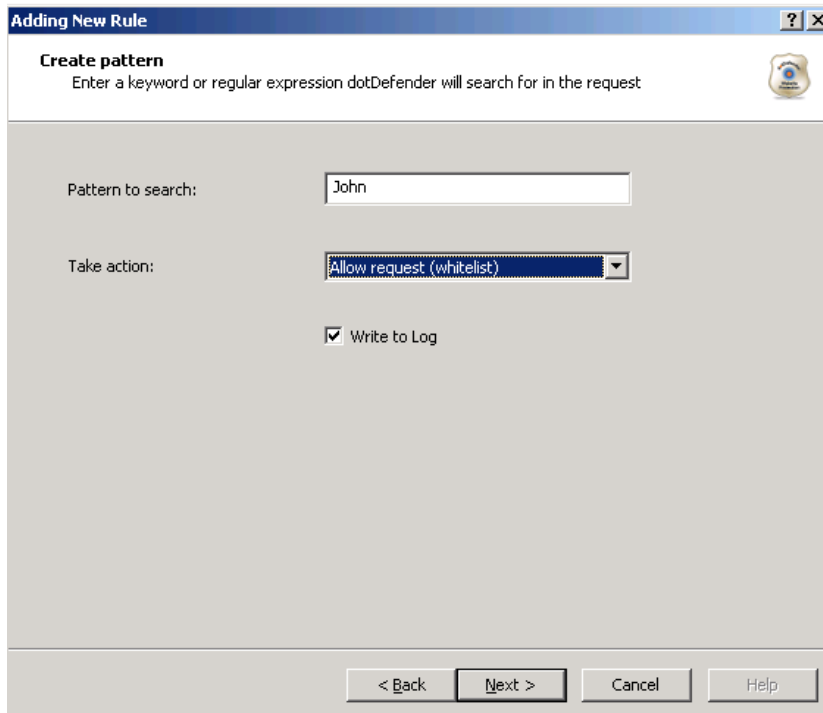
14. Click **OK**.

7.1.2 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.



Adding New Rule

Create pattern
Enter a keyword or regular expression dotDefender will search for in the request

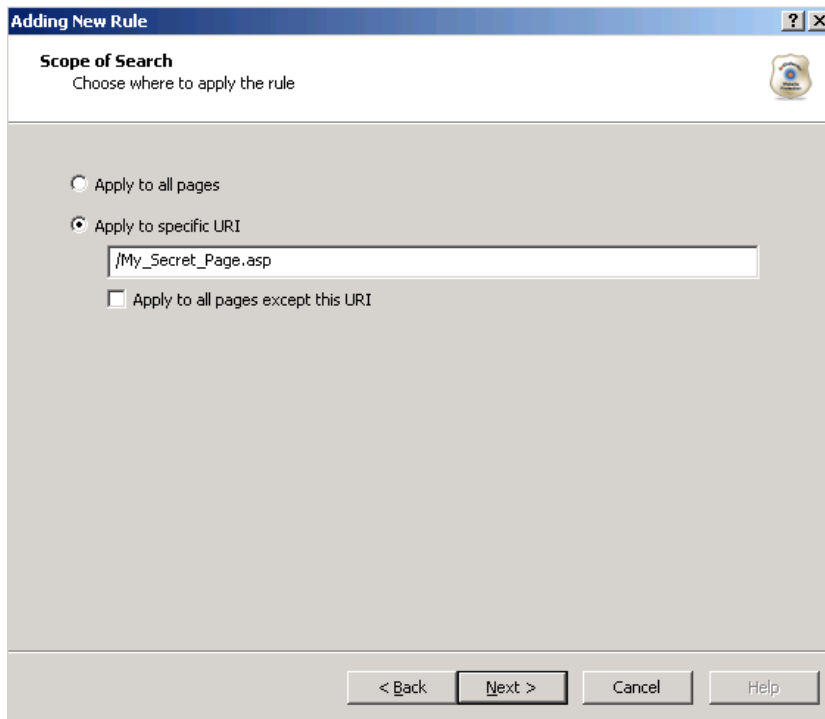
Pattern to search:

Take action:

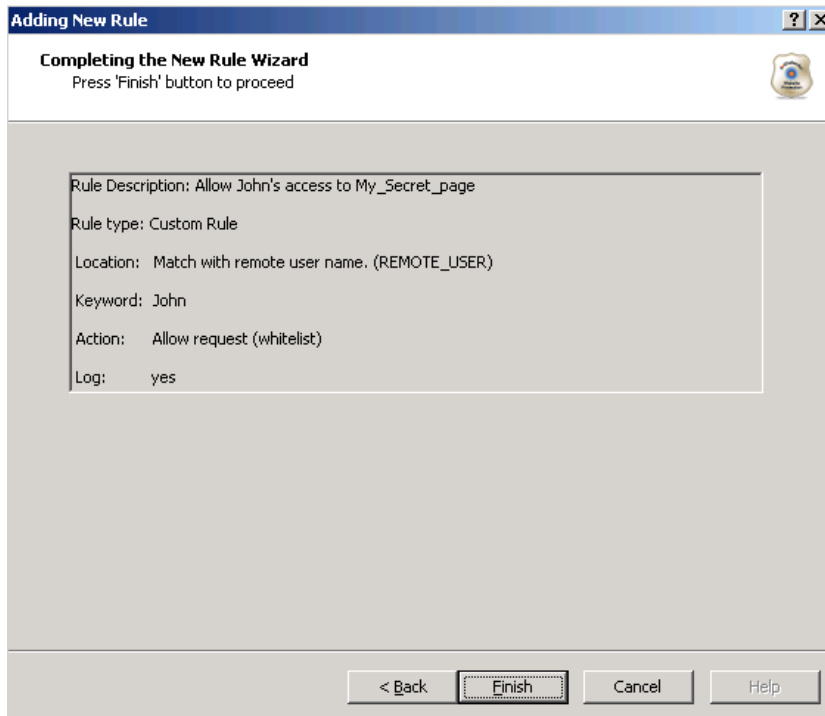
Write to Log

< Back Next > Cancel Help

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 [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 "John".

7.1.3 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**

7.1.4 How do I change the database size limit?

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

If the number of events reaches 100,000 (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: $64 \text{ KB} * 15,000 = \sim 1 \text{ GB}$.

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.

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

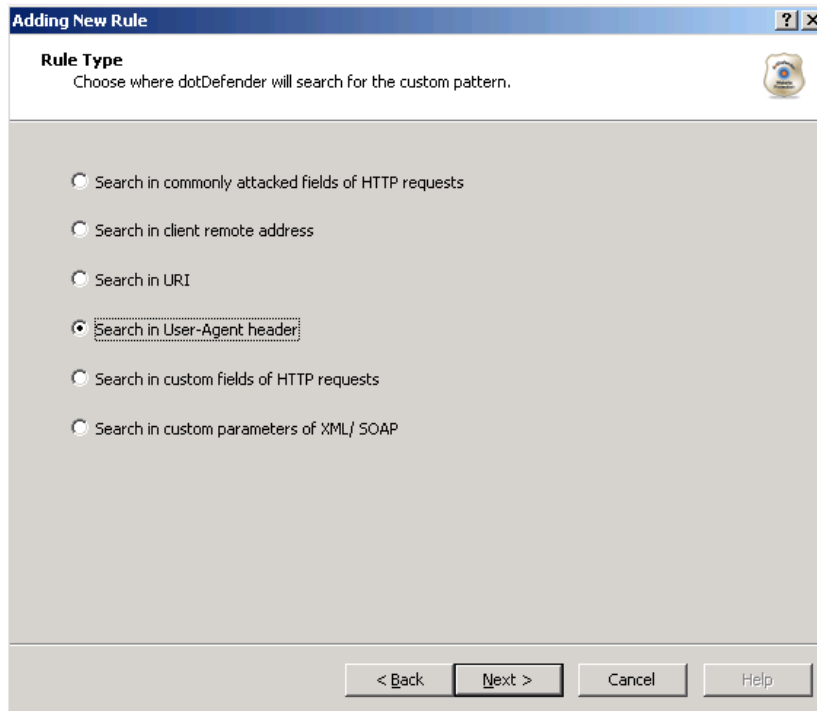
A User-Agent is an HTTP header, containing a string identifying the software being used by the client to connect to the Website. For example, this might be Internet Explorer, Mozilla Firefox, Nokia, or Motorola cellular phones. The Bad User-Agents database is a very effective mechanism for distinguishing 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?](#)

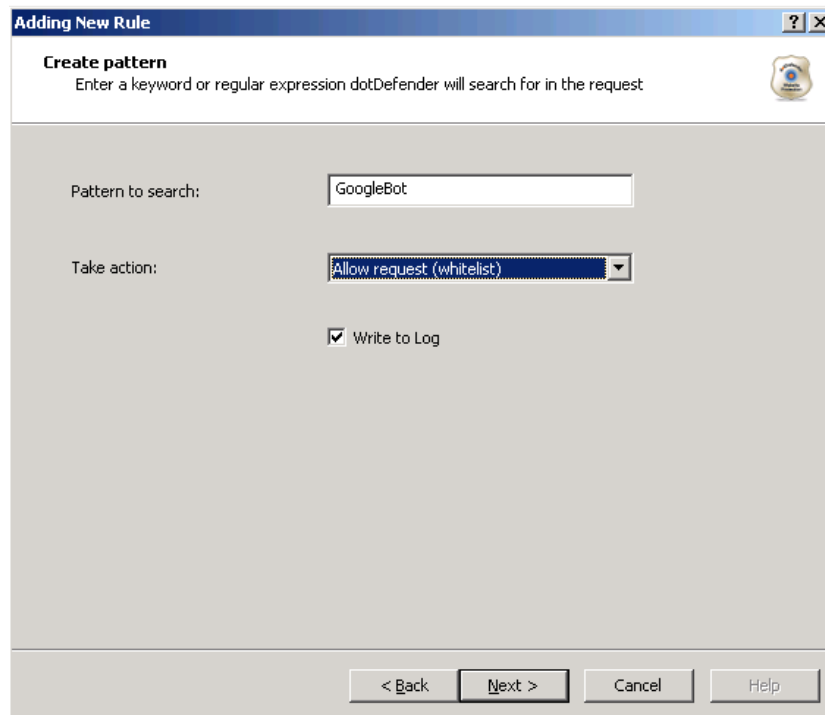
7.1.6 How do I let one "good" User-Agent pass through?

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).

7.1.7 How do I remove the database when it is taking up too much space?

See [Deleting the dotDefender Log Database File](#).

7.1.8 What is a Proxy attack?

A proxy attack is an attempt to use your web server as a jumping point to attack other sites. Your web server then attacks other sites.

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

See [Adding User-Defined Rules](#).

7.1.10 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.

- **Pass:** dotDefender for IIS monitors this request, without intervening.

7.1.11 I am upgrading. How do I back up the rule set?

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.effective > 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**.



7.1.12 How do I clear the Event Log?

See [Clearing the Applicure Windows Event Log](#).


7.1.13 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  to apply the changes.
7. Click **OK**.

7.1.14 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](#).

7.2 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.

7.2.1 System Requirements

- dotDefender supports IIS Servers web servers 5.x and higher.
- dotDefender supports the following operating systems:
 - ◆ Windows 2008
 - ◆ Windows 2003: Service Pack 1 and the latest Windows updates
 - ◆ Windows XP: Service Pack 2 and the latest Windows updates
 - ◆ Windows 2000: Service Pack 4 and the latest Windows updates

7.2.2 Configuring dotDefender for IIS to work properly with IIS ISAPI Filters (SSL-encrypted sites)

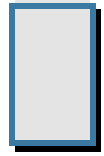
For dotDefender for IIS to work properly, the high-priority IIS ISAPI filters—sspfilt, Compression, and md5filt (IIS 6.0, Windows XP only)—should be executed before the three dotDefender for IIS ISAPI filters.

Note: If you have other high-priority ISAPI filters, make sure to also execute them before dotDefender for IIS ISAPI filters.

To execute the high-priority IIS ISAPI filters—sspifilt, Compression, and md5filt (IIS 6.0, Windows XP only):

Checks for IIS 5.0:

1. Verify that there are three dotDefender IIS ISAPI filters.
2. On the desktop, right-click **My Computer** and select **Manage**.
3. Click (to expand) **Services and Applications**.
4. Right-click **Internet Information Services** and select **Properties**. The Internet Information Services Properties dialog box is displayed.
5. Select the Internet Information Services tab.
6. In the Master Properties dialog box, select **WWW Services**.
7. In the Internet Information Services tab, click **Edit**.
8. In the WWW Service Master Properties dialog box, select **ISAPI Filters** tab.
9. Move the two high-priority sspifilt and Compression ISAPI filters to the top of the list, to be executed before the dotDefender for IIS ISAPI filters.
10. Verify that the dotDefender for IIS (Cookie Tampering), dotDefender for IIS (Session Protection) and dotDefender for IIS (Main) ISAPI filters appear in this order on the list, below the IIS ISAPI filters. If they do not, select the filter and use the up/down arrows (on left) to move it to the specified location.
11. Click **Apply** and then **OK**.



Regular Expressions

dotDefender supports regular and extended regular expressions.

This chapter contains the following sections:

- [POSIX Basic Regular Expressions](#)
- [POSIX Extended Regular Expressions](#)

8.1 POSIX Basic Regular Expressions

Expression	Description
.	Matches any single character. For example, <code>a.c</code> matches "abc", etc., but <code>[a.c]</code> matches only "a", ".", or "c".
[]	A bracket expression. Matches a single character that is contained within the brackets. For example, <code>[abc]</code> matches "a", "b", or "c". <code>[a-z]</code> specifies a range which matches any lowercase letter from "a" to "z". These forms can be mixed: <code>[abcx-z]</code> matches "a", "b", "c", "x", "y", or "z", as does <code>[a-cx-z]</code> .
[^]	Matches a single character that is not contained within the brackets. For example, <code>[^abc]</code> matches any character other than "a", "b", or "c". <code>[^a-z]</code> 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.

Expression	Description
\(\)	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", "xyzy", and so on. \ (ab\)* matches "", "ab", "abab", "ababab", and so on.
\{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".

8.2 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

POSIX	Perl	ASCII	Description
<code>[:graph:]</code>		<code>[\x21-\x7E]</code>	Visible characters
<code>[:lower:]</code>		<code>[a-z]</code>	Lowercase letters
<code>[:print:]</code>		<code>[\x20-\x7E]</code>	Visible characters and spaces
<code>[:punct:]</code>		<code>[- !"#\$%&'()*+,-./:;<=>? @[\\]_`{ }~]</code>	Punctuation characters
<code>[:space:]</code>	<code>\s</code>	<code>[\t\r\n\v\f]</code>	Whitespace characters
	<code>\S</code>	<code>[^\s]</code>	non-whitespace character
<code>[:upper:]</code>		<code>[A-Z]</code>	Uppercase letters
<code>[:xdigit:]</code>		<code>[A-Fa-f0-9]</code>	Hexadecimal digits