



3

Implementing a Security Policy for a Production Web Site or Application

- Implementing application security for a production web site or application
- Starting the Deployment Wizard
- Defining the web application properties
- Configuring an attack signatures set for the application systems
- Verifying that the application servers are receiving traffic
- Running the Policy Builder to automatically create the security policy
- Finalizing the new security policy configuration

Implementing application security for a production web site or application

In this implementation, we describe the process for automatically building a security policy that is based on untrusted traffic through a web site or web application. *Untrusted traffic* is traffic that can come from any source, and may or may not be malicious. You create this security policy by using the Deployment Wizard. The Deployment Wizard guides you through the following tasks:

- Defining the basic web application properties
- Configuring an attack signature set for the application systems
- Verifying that the application servers are receiving traffic and that Application Security Manager is logging the traffic
- Running the Policy Builder to automatically build the security policy
- Finalizing the newly-created security policy

Important

*This implementation assumes that you have already configured the network settings that are appropriate for your environment. Refer to Chapter 2, **Reviewing Network Configuration Tasks**, if you have not yet configured network connectivity.*

Starting the Deployment Wizard

Once you have completed the network configuration and updated the system-supplied attack signatures, you are ready to start the Deployment Wizard. The Deployment Wizard automates several essential configuration tasks, to expedite the initial configuration of a security policy.

When you start the Deployment Wizard, you select a deployment scenario. Each deployment scenario includes preset configuration options. The configuration options are tailored to address the needs of the environment or application for which you are creating a security policy. For this implementation, which uses the production site deployment scenario, the default security policy uses these settings:

- Sets the enforcement mode to **Transparent**.
- Adds wildcard match all (*) entities for object types, objects, and parameters.
- Enables tightening for object types and parameters.
- On the Blocking Policy screen, enables the Learn flag for all but a few of the available violations.
- On the Blocking Policy screen, enables the Alarm and Block flags, in addition to the Learn flag, for the following violations:
 - **Illegal object type**
 - **Non-existent object**
 - **Illegal parameter**
 - **HTTP protocol compliance failed**
 - **Illegal cookie length**
 - **Illegal header length**
 - **Illegal dynamic parameter value**

◆ Important

You can run the Deployment Wizard only for new, unconfigured web applications, so do not set the language encoding for a new web application if you want to use the Deployment Wizard.

◆ Note

*If you have not yet configured the basic local traffic settings, refer to Chapter 2, **Reviewing Network Configuration Tasks**, and perform those tasks. Once you have completed the tasks outlined in that chapter, you can proceed with this implementation.*

To start the Deployment Wizard

1. On the Main tab of the navigation pane, in the **Application Security** section, click **Web Applications**.
The Web Applications screen opens in a new browser session.
2. In the Name column, click the web application name that matches the application security class name.
The Web Application Properties screen opens.
3. In the Deployment Wizard area, click the **Run Deployment Wizard** button.
The Deployment Wizard starts.
4. For the Deployment Scenario setting, select **Production Site (Untrusted Traffic)**.
5. Click the **Next** button.
The Configure Web Application Properties screen opens.

Defining the web application properties

In this step, you configure the web application properties. Defining the web application properties includes selecting the web application language and, optionally, configuring a pattern for extracting dynamic session information from URLs. For additional information on web application configuration, see the *Working with Web Applications* chapter, in the *Configuration Guide for BIG-IP® Application Security Management*.

To configure web application properties

1. On the Configure Web Application Properties screen, for the **Application Language** setting, select one of the following options:
 - Leave the setting at the default value, **Auto detect**.
The Deployment Wizard determines the language encoding based on application data.
 - Select a specific language encoding from the list.
2. If the web application includes session information in its URLs, then you can enable the **Dynamic Sessions in URL** setting. See Chapter 7, *Extracting Dynamic Session Information from URLs*, for more information.
3. Click **Next**.
The Configure Attack Signatures screen opens.

Configuring an attack signatures set for the application systems

Attack signatures represent known attack patterns. In this step, you create an attack signatures set based on the systems that are in your configuration. The system then assigns the set to the security policy, and applies those signatures to the requests for the associated web application. There is also a set of generic attack signatures that is automatically assigned to the security policy.

In this step, you also configure whether the system activates signature staging. When signature staging is enabled, the system keeps track of how many times an attack signature detects an attack pattern, but does not activate blocking for that signature until the staging time has passed.

To configure an attack signatures set

1. On the Configure Attack Signatures screen, for the **Systems** setting, from the **Available Systems** list, select (by clicking) the systems that apply to your web application.

*Tip: Hold the **Ctrl** key to select more than one system in the list.*

2. Click the Move (<<) button to add the selected systems to the **Assigned Systems** list.
3. If you do not want the system to keep the signatures in the staging state, clear the **Enable Signatures Staging** check box. Otherwise, leave the box checked, which is the default setting.
4. For the **Staging Period** setting, specify the length of time for which the signatures are in the staging state. The default is **7** days. Note that this setting is not applicable if you have cleared the **Enable Signatures Staging** setting.
5. Click **Next**.
The Web Application Properties screen opens, and the Deployment Wizard verifies that the system is receiving traffic.

◆ Note

*For more information on attack signatures and signature staging, refer to the **Working with Attack Signatures** chapter in the **Configuration Guide for BIG-IP® Application Security Management**.*

Verifying that the application servers are receiving traffic

Before the Deployment Wizard starts the Policy Builder, the wizard verifies that the application servers are receiving traffic. In the messages and information area of the screen (near the top), you see a notification that the system is checking to see if Application Security Manager is logging requests. The Deployment Wizard moves to the next phase only after it has successfully logged at least one request.

To verify that the application servers are receiving traffic

1. Open a new browser session to the web application.
2. Browse the web application to generate several requests.
3. Return to the Application Security Manager browser session.
4. In the messages and information area of the screen, you see one of two messages:
 - **The ASM logging failed.**
If you see this message, then you need to review the networking configuration.
 - **ASM logging started successfully.**
If you see this message, then the Deployment Wizard starts the Policy Builder.

Running the Policy Builder to automatically create the security policy

After the Deployment Wizard has successfully tested the logging mechanism, the wizard automatically starts the Policy Builder. The **Policy Builder** is an automated tool that discovers and populates the security policy with the web application entities. As the Policy Builder runs, you see status messages or a progress bar in the messages and information area of the screen. The status messages include information on the number of parsed requests, and the number of found object types, objects, and parameters. Figure 3.1 shows an example of the status messages.

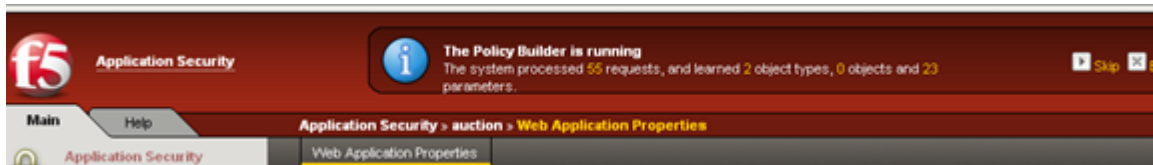


Figure 3.1 Policy Builder status messages

The progress bar displays the degree of completeness for the security policy. Figure 3.2 shows an example of the progress bar.

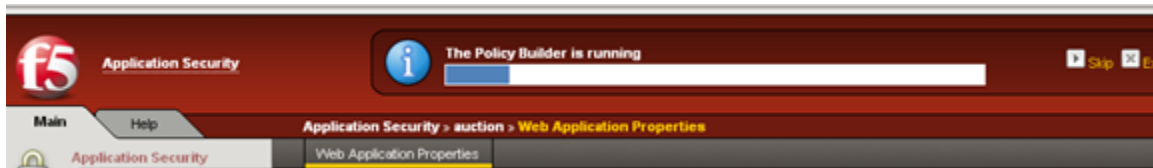


Figure 3.2 Policy Builder progress bar

The deployment scenario that you select when you first start the Deployment Wizard determines the Policy Builder settings. For this implementation, the Policy Builder uses the following settings:

- The **Traffic Source** option is set to **Live Traffic**.
- The **Continuous Mode** option is set to **Run continuously**.
- The **Track Site Changes** option is set to **On**.
- The **Security Template** option is set to **Basic**.

The Policy Builder runs until it determines that the new security policy is stable, that is, has little to no change. Depending on your web application, and the typical traffic flow, this process may take from a few hours up to several days. Once the Policy Builder determines that the security policy is stable, you finalize the security policy, and exit the Deployment Wizard.

◆ **Note**

*For more information on the Policy Builder, see the **Building a Security Policy with the Policy Builder** chapter of the **Configuration Guide for BIG-IP® Application Security Management**.*

Finalizing the new security policy configuration

The Deployment Wizard notifies you, in the messages and information area of the screen, when the Policy Builder has finished building the new security policy, and determines that the security policy is at a stable point. This point occurs when there are few or no new learning suggestions for period of time. Once the security policy is stable, you can finalize the security policy and finish the deployment process. You can also finalize the deployment at any time by clicking the **Skip** button in the messages and information area.

Important

*Finalizing the deployment by clicking the **Skip** button does not stop the Policy Builder. For information on stopping the Policy Builder, refer to the **Stopping the Policy Builder** section of the **Building a Security Policy Automatically with the Policy Builder** chapter, in the **Configuration Guide for BIG-IP® Application Security Management**.*

Understanding the available actions

When you finalize the Deployment Wizard, the Policy Builder takes a series of actions that are based on your selection in the finalization step. The possible actions are:

◆ **Go to the Traffic Learning page to fine-tune the automatically built security policy**

When you select this action, the system performs the following activities:

- Clears the wildcard match all (*) entities from the object types and parameters list.
- Retains the wildcard match all (*) entity in the objects list.
- Retains learning suggestions that the Policy Builder did not resolve.
- Opens the Traffic Learning screen, where you can evaluate the remaining learning suggestions, if any.

◆ **Exit the Deployment Wizard without fine-tuning the automatically built security policy. Learning suggestions are kept.**

When you select this action, the system performs the following activities:

- Retains the wildcard match all (*) entity in the object types, objects, and parameters lists.
- Retains learning suggestions that the Policy Builder did not resolve.

◆ **Exit the Deployment Wizard without fine-tuning the automatically built security policy. Learning suggestions are deleted.**

When you select this action, the system performs the following activities:

- Clears the wildcard match all (*) entities from the object types and parameters list.
- Retains the wildcard match all (*) entity in the objects list.
- Clears learning suggestions that the Policy Builder did not resolve.

Finishing the deployment

Once you have decided which action to take, you can finish the deployment process.

To finish the deployment process

1. In the Finish the Deployment area, for the **Actions** setting, select the action that you want the Deployment Wizard to take.
2. For the **Enable Signature Staging** setting, clear the check box if you do not want the system to put detected attack signature patterns in a staging period. Otherwise, leave the box checked, which is the default setting.
3. Click **Finish**.
The Deployment Wizard performs the action you specified, and exits. The wizard also takes the following actions:
 - Changes the web application logging profile from **Log all requests** to **Log illegal requests**.
 - Performs the **Apply Policy** action.

Working with learning suggestions

If there are learning suggestions that the Policy Builder could not resolve, you evaluate each individually, and decide which course of action you want to take.

- You can accept the learning suggestion, which updates the security policy. Click the **Apply Policy** button to put the updated security policy into effect.
- You can disable the learning suggestion, which clears the learning suggestion, and disables the Learn, Alarm, and Block flags on the Blocking Policy screen. Click the **Apply Policy** button to put the updated security policy into effect.
- You can clear the learning suggestion. The Learning Manager continues to generate learning suggestions for the violation.

For more information on the learning process and learning suggestions, refer to the *Refining the Security Policy Using Learning* chapter in the *Configuration Guide for BIG-IP® Application Security Management*.

Additional security policy options

You can configure any of the following additional options to further customize the security policy for your web site or application.

- ◆ **Custom blocking response page**
When the Policy Enforcer blocks a request, the system returns the blocking response page to the offending client. You can use the default

blocking response page, or you can customize the page as needed. For additional information, refer to *Configuring the response pages*, in the *Working with the Security Policy* chapter of the *Configuration Guide for BIG-IP® Application Security Management*.

◆ **Sensitive parameters**

If the web application includes parameters that contain sensitive information, such as passwords or user account numbers, you can configure them as sensitive parameters. For more information, see *Configuring sensitive parameters*, in the *Working with the Security Policy* chapter of the *Configuration Guide for BIG-IP® Application Security Management*.

◆ **Flow access to prevent forceful browsing**

For web applications that have login and logout screens, you can configure the valid access points for those screens, which prevents forceful browsing of the web application. For more information, see *Configuring flow access to prevent forceful browsing*, in the *Working with the Security Policy* chapter of the *Configuration Guide for BIG-IP® Application Security Management*.