Copyright © 2016, 2019, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any
loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.
CONTENTS

CHAPTER 1 About Oracle Dyn Web Application Security ........................................... 7
  Prefer Online Help? .................................................................................................. 8
  Need API Documentation? ..................................................................................... 8

CHAPTER 2 Getting Started Guide .......................................................................... 9
  Web Application Security Service Components .................................................. 9
  Ways to Access the Web Application Security Service ....................................... 10
  Identity, Authentication and Authorization .......................................................... 10
  Service Capabilities and Limits ............................................................................ 10
  Getting Started ...................................................................................................... 11

CHAPTER 3 Partner Admin ...................................................................................... 12
  Partner Admin Overview ....................................................................................... 12
  Set Up and Manage Companies .......................................................................... 14
  Invite and Manage Users and Access Policies ...................................................... 16
  Set Up Email Notifications ................................................................................... 20
  Manage Partner Templates .................................................................................... 23
  Run a Company Usage Report ............................................................................. 26
  Partner Branding ................................................................................................... 27
  Manage Services .................................................................................................... 30
  Partner Policies ..................................................................................................... 31
  Single Sign-On (SSO) ............................................................................................. 32
# Table of Contents

## CHAPTER 4 Administration ................................................................. 35
- Administration .............................................................................. 35
- Create and Manage Web Apps ....................................................... 37
- Add and Manage Company Services ............................................ 56
- Inviting Users and Access Policies .............................................. 59
- Enabling Two-Factor Authentication ............................................ 64
- Managing Custom WAF Rules ..................................................... 65
- Managing IP Lists (Administration) ............................................. 69
- Manage a Company Profile ......................................................... 72
- Managing Templates ................................................................. 74
- Setting Up Notifications ............................................................. 77
- SSL Certificates .......................................................................... 85
- Resetting Your Password ........................................................... 90

## CHAPTER 5 Access Control ............................................................... 95
- Access Control ............................................................................ 95
- Access Control Dashboard ......................................................... 95
- Access Rules ............................................................................... 96
- IP Lists ....................................................................................... 101
- IP Whitelist .............................................................................. 105
- Threat Intelligence ..................................................................... 108

## CHAPTER 6 Bot Manager ................................................................. 110
- Bot Manager ............................................................................... 110
- Bot Manager Dashboard ............................................................. 110
- Captcha Challenge .................................................................... 112
- Device Fingerprinting Challenge (DFC) .................................... 116
- Human Interaction Challenge (HIC) .......................................... 118
- IP Rate Limiting .......................................................................... 121
- Javascript Challenge (JSC) ......................................................... 122
- Advanced Rate Limiting ............................................................. 124
- Good Bot Whitelist .................................................................... 128
# Table of Contents

## CHAPTER 7 API Security

- API Security .............................................. 130
- Configure API Security .............................. 130

## CHAPTER 8 Caching Policies

- Caching Policies Module ............................. 134
- Caching Dashboard .................................... 134
- Purge Cache ............................................ 136
- Caching Rules .......................................... 138
- Zentags .................................................. 141

## CHAPTER 9 Web Application Firewall

- Web Application Firewall ......................... 147
- WAF Dashboard ....................................... 147
- Set Up and Tune the WAF .......................... 150
- Recommendations .................................... 155
- WAF Rules ............................................. 158
- WAF Protection Rule IDs ............................ 165
- WAF Settings ......................................... 194
- Transferring Web Application Security WAF to Oracle Cloud Infrastructure WAF .. 196

## CHAPTER 10 DDoS Mitigation Manager

- DDoS Dashboard ........................................ 201
- DDoS Alerts ............................................. 202
- DDoS Profiles .......................................... 204

## RELEASE NOTES

...
CHAPTER 1 About Oracle Dyn Web Application Security

Oracle Dyn Web Application Security’s platform provides you the ability to implement and manage various applications to mitigate traffic to your domains, such as bot traffic, DDoS traffic, and other forms of abusive traffic.

If you're ready to manage traffic using policies, access rules, and IP white lists, this guide is right for you. It provides the following information about using Oracle Dyn Web Application Security:

<table>
<thead>
<tr>
<th>Section</th>
<th>What's Covered</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Using the Access Control module.</td>
<td>Access Control</td>
</tr>
<tr>
<td>Partner Admin</td>
<td>Using the Partner Admin tab.</td>
<td>Partner Admin</td>
</tr>
<tr>
<td>Administration</td>
<td>Using the Administration tab.</td>
<td>Administration</td>
</tr>
<tr>
<td>Bot Manager</td>
<td>Using the Bot Manager module.</td>
<td>Bot Manager</td>
</tr>
<tr>
<td>API Security</td>
<td>Using the API Security module.</td>
<td>API Security</td>
</tr>
<tr>
<td>Caching Policies</td>
<td>Using the Caching Policies module.</td>
<td>Caching Policies</td>
</tr>
<tr>
<td>DDoS Mitigation</td>
<td>Using the DDoS Mitigation Manager.</td>
<td>DDoS Mitigation Manager</td>
</tr>
<tr>
<td>Web Application</td>
<td>Using the Web Application Firewall module.</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Prefer Online Help?
The information in this guide is also available in the online help at http://web-securityhelp.dyn.com.

Need API Documentation?
For general information, see About the API. For links to the detailed service API documentation, see the online help at http://websecurityhelp.dyn.com.
CHAPTER 2 Getting Started Guide

The Web Application Security Service provides users the ability to manage traffic to web applications, such as, bot traffic, DDoS traffic, and other forms of abusive traffic in accordance with a custom security profile. The Web Application Security portal provides real-time analytics and alerting to display what enforcement measures are taking place to maintain the availability and integrity of your domains.

Web Application Security Service Components

The following list describes the components of the Oracle Dyn Web Application Security.

**WEB APPS**

Web applications (web apps) are sets of configurations that can be applied to your domain, such as activating Bot Manager or Web Application Firewall rules.

**WEB APPLICATION FIREWALL (WAF)**

A custom security profile that allows you to monitor, manage, and block traffic.

**BOT MANAGER**

A bot mitigation service that allows you to block, whitelist, or challenge incoming bot traffic to your domain.

**API SECURITY**

Determines the legitimacy of API requests, and eliminates API attacks at the edge of the network based on unique hash identifiers received from the edge servers.

**ACCESS CONTROL**

Gives users the ability to define granular access rules to control traffic based on geolocation, threat intelligence feeds, UserAgent, and IP addresses. Access Control tab allows users to create and review rules, enable and disable threat feeds, manage IP lists, and manage whitelists.
CACHING POLICIES
Configure policies that allow you to cache frequently used content on edge servers to increase application performance.

DDOS MITIGATION
Monitor and filter out malicious traffic patterns from your IP prefixes.

Ways to Access the Web Application Security Service
You can access Oracle Dyn Web Application Security service using the UI (a browser-based interface) or the REST API. To access the UI, you must use a supported browser. You can go to the sign-in page, enter your user name and your password, to begin using the UI. Accessing the REST API requires adding an API application to the account at an administrative level and configuring it for your users. For more information about adding an API application, please see Using the API.

Identity, Authentication and Authorization
Each organization's account is defined as a "company" on the Oracle Dyn Web Application Security platform, and a user requires "company permissions" to invite and manage users of a company. Permissions at the company and web app levels are granular and can be adjusted for each authorized users. Users can be onboarded and off boarded by a designated company administrator. Accessing the Oracle Dyn Web Application Security REST API requires the generation of an authorization token by passing the API a client ID and client secret key. Access to the API limited to a set of IP addresses defined by the administrator.

Service Capabilities and Limits
The number of users that can be assigned to an account is limited. If you require more users, please contact support.
Getting Started

To begin using the service, you will need to create your first web app. Please see, Create and Manage Web Apps. If you have purchased the DDoS Mitigation Manager service, please see DDoS Mitigation Manager to learn about the DDoS dashboard.
CHAPTER 3 Partner Admin

This chapter explains how to configure settings in the Partner Admin tab.

Partner Admin Overview

The Partner Admin section lets authorized users manage partner-wide settings. The Partner Admin section provides access to the following tabs:

- Companies
- Users
- Notifications
- Templates
- Reports
- Branding
- Services
- Partner Policies
- Single sign-on (SSO)

To view the details of a specific company and manage company settings, including SSL certificates, custom WAF rules, IP lists, and templates, click Manage for the company you want to manage. See Administration.
To view consumption data for a specific time range, select an option from the time range drop-down list. Options include:

- **Last 6h** - (Default) Displays data for the last six hours.
- **Last 24h** - Displays data for the last 24 hours.
- **Last 2d** - Displays data for the last two days.
- **Last 7d** - Displays data for the last seven days.
- **Last 30d** - Displays data for the last 30 days.
- **Custom Range** - Select a start date and an end date within the past 60 days, and then click Apply.
Set Up and Manage Companies

The Partner Admin Companies tab is where you can set up and manage a company, and configure the company’s settings and services. You can also remove a company from the partner’s company list.

In Partner Admin, select **Companies** to view a list of companies associated with the partner.

To add a company

1. Click **Add company**.
2. Enter the company details.

3. Click **Save**.

4. Once you have added a company, you can add and manage the company's services. For more information, see [Managing Services](#).

To view and manage company settings

Click **Manage** for a company to open the company's Administration section. For more information, see [Administration](#).

To add and manage company services

You can add and configure the services available through the partner.
Click **Services** for a company to open the Services page in the company’s Administration section. For more information, see [Managing Services](#).

**To edit a company’s profile**

Click **Edit** for the company to open the Company Profile page in the company's Administration section. For more information, see [Company Profile](#).

**To delete a company**

Click **Delete** for the company you want to delete.

---

### Invite and Manage Users and Access Policies

The Users tab in the Partner Admin dashboard allows authorized users to manage existing and create new users. You can invite a new user and manage permissions of existing users.

To access the Partner Users tab, click the **Partner Admin** tab and then select **Users**.
Inviting Users

In the Users tab you can add new users and define permissions based on role. A new user can be invited (a unique email account is required) with the list of accessible web apps. If an email account is already registered in the Oracle Dyn WAF portal for any other companies, it cannot be used for a new invitation. The invite is sent by email from a Oracle Dyn email address. An account can be disabled or an invitation can be resent for an account which has never logged in.

To add a new user

1. From the Users tab, click + Invite User.
   a. In the Invite new user dialog, specify the new user settings:

   ![Invite new user dialog](image)

   b. Enter the email address for the new user in the Email field.
   c. (Optional) Enter a message that will be sent to the new user's email address.

2. Click Invite.
   The new user must accept the email invitation to begin using the portal.

3. (Optional) To resend the invite, select Resend invite from the actions drop-down menu.
4. Once the user accepts the invitation, click **Edit** to manage user permissions, such as defining password requirements and enabling two-factor authentication.

**Managing Users**

User profile settings include the ability to manage permissions and other identity-related settings. You can update the user’s name, contact information, and password. Security settings let you enable two-factor authentication, which adds an extra layer of security to the account.

**To update a user**

1. Click **Edit** for the user you want to update.

2. Update the user profile by clicking the tabs on the left.


- **Account information** - Edit the user’s name and phone number and then click Apply.
- **Change password** - Enter a new password and then click Apply.
- **Security settings** - Enable two-factor authentication.

The avatar that appears in the user profile is managed through Gravatar ([gravatar.com](http://gravatar.com)). A Gravatar account lets you associate email addresses with your account. Any service that uses Gravatar will match the email address and use the corresponding avatar for the profile picture.
Set Up Email Notifications

The Partner Admin Notifications tab allows an authorized user to create and edit email-based notifications for various events and actions. Notifications include:

- **Web app changes published** - Notifies users when changes are published to the EDGE nodes for selected web applications.
- **Web app created or deleted** - Notifies users when a web app is created or deleted.
- **Web app CNAME status changed** - Notifies users when a web app DNS CNAME changes are made for selected web apps.
- **Web app RPS changed** - Notifies users when web app RPS (requests per second) changes by more than the specified threshold value.
- **EDGE IP changed** - Notifies users when the IP addresses for the EDGE nodes are added or removed.

To access the Notifications tab, click the Partner Admin tab, and then click Notifications.

To add a notification

1. From the Notifications tab, click **Add notification**.
2. In the select notification type dialog box, select the type of notification you want to add and then click **Next**.

3. Specify the notification details based on your selection. Each user will receive a separate email.
   a. **Subscriptions**
      - **Name** - Enter a unique name for the notification.
      - **Services** - Select the services to watch changes for.
      - **Subscription Actions** - Select the actions that will trigger the notification.
      - **Users** - Select the users who will receive the notification.
CHAPTER 3 Partner Admin

b. Web app changes published
   - **Name** - Enter a unique name for the notification.
   - **Webapps** - Select the web apps for notifications.
   - **Users** - Select users to send notifications to.

c. Web app created or deleted
   - **Name** - Enter a unique name for the notification.
   - **Users** - Select users to send notifications to.

d. Web app CNAME status changed
   - **Name** - Enter a unique name for the notification.
   - **Webapps** - Select the web apps for notifications.
   - **Users** - Select users to send notifications to.

e. Web app RPS changed
   - **Name** - Enter a unique name for the notification.
   - **RPS change threshold** - Enter the threshold value for the change period.
   - **RPS change period** - Enter the time period to compare the change.
   - **Max notifications** - Enter the maximum number of notifications to send during the max period.
   - **Max period** - Enter the time period for max notifications.
   - **Webapps** - Select the web apps for notifications.
   - **Users** - Select users to send notification to.

f. EDGE IP changed
   - **Name** - Enter a unique name for the notification.
   - **Users** - Select users to send notification to.

4. Click **Save**.

To edit a notification
CHAPTER 3 Partner Admin

1. Click **Edit** for the notification you want to update.
2. Make changes to the notification and then click **Save**.

To delete a notification

1. Click **Delete** for the notification you want to delete.
2. In the confirmation dialog box, type **delete** and click **YES, I understand the consequences, delete this notification**.

Manage Partner Templates

You can save and manage a frequently used web app configuration as a template. A partner user can create a template and apply it to companies.

To access Templates, click the **Partner Admin** tab, and then select **Templates**.

You can add templates that can be applied to web apps. You can also update and delete templates.
To add a template

1. Click + **Add webapp template**. The Add Template window opens.
2. Enter the template name.

3. Enter a description of the template.
4. Select the web app containing the settings you want to use for the template.
5. Select the settings from the web app that you want to save to the template.
6. Click **Create**.

**To update template**
1. In the Actions column, click **Edit** for the template you want to update.
2. Change the name and/or the description as needed.
3. Click **Update**.

**To apply a template to a web app**
1. Click **Apply** for the template you want to apply.
2. Select the web app where you want to apply the template.
3. Click **Apply**.
   
   ![Tip] The template will override current web app settings.

**To delete a template**
1. In the Actions column, click **Delete** for the template you want to delete.
2. Click **OK** to confirm that you want to delete the template.

**Run a Company Usage Report**

The Company Usage Report shows the combined usage for all of a company's webapps.
To run the Company Usage Report

1. In Partner Admin, select Reports, and then click Company Usage.
2. Enter the date range for the report.
3. Click Create report.

Partner Branding

You can customize the branding for a partner, including the logo and user interface colors. The partner branding settings will also appear for the company portals associated with the partner.
To configure branding settings

1. In Partner Admin, select **Branding**.
2. Enter the branding settings.
3. Click **Apply**.
## Branding Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner name</td>
<td>Displays the partner's name.</td>
</tr>
<tr>
<td>Product brand name</td>
<td>The brand name to be used instead of Zenedge.</td>
</tr>
<tr>
<td>Header logo</td>
<td>Logo displayed in the top left header.</td>
</tr>
<tr>
<td>Custom favicon</td>
<td>You can select the icon to be associated with the partner's URL.</td>
</tr>
<tr>
<td>Footer text</td>
<td>Custom text to display in the footer, such as the copyright.</td>
</tr>
<tr>
<td>Support link</td>
<td>Custom link to support, which is used in the portal profile menu.</td>
</tr>
<tr>
<td>Header color</td>
<td>The color for the header panel.</td>
</tr>
<tr>
<td>Header text color</td>
<td>The color for header panel text.</td>
</tr>
<tr>
<td>Header active item color</td>
<td>The color for header active item.</td>
</tr>
<tr>
<td>Header active item text color</td>
<td>The color for header active item text.</td>
</tr>
<tr>
<td>Sidebar color</td>
<td>The color for the sidebar.</td>
</tr>
<tr>
<td>Sidebar item text color</td>
<td>The color for the sidebar item text.</td>
</tr>
<tr>
<td>Sidebar active item color</td>
<td>The color for the sidebar selected menu group item.</td>
</tr>
<tr>
<td>Sidebar active item text color</td>
<td>The color for the sidebar selected menu group item text.</td>
</tr>
<tr>
<td>Reset to default colors</td>
<td>Click to reset all colors to the default color settings.</td>
</tr>
</tbody>
</table>
Manage Services

You can add, edit, and deactivate the services that are available for companies.

To add a service

1. In Partner Admin, select **Services**.
2. Click **Add service**.
3. Select the base service, and then click **Next**.
4. Enter the settings for the service you selected.

5. Click Save.

To edit a service

1. Click Edit for the service you want to edit.
2. Update the service settings.
3. Click Save.

To deactivate a service

1. Click Deactivate for the service you want to deactivate.
2. Type deactivate to confirm that you want to deactivate the service.
3. Click I understand the consequences, deactivate the service.

Partner Policies

The partner policy contains the default values for the external data to be stored together with the company profile. The data is shown only to the partner users and is not available to company users.
To configure partner policies

1. In Partner Admin, select **Partner Policies**.
2. Enter the policy values.
3. Click **Save**.

**Single Sign-On (SSO)**

The Partner Admin SSO tab lets you configure single sign-on for your users.
To configure partner SSO

1. In Partner Admin, select **Single sign-on (SSO)**.
2. Select the **Enable Single sign-on** check box.
3. Enter the SSO settings.
4. Click **Save**.

### Single Sign-on Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Single sign-on</td>
<td>Select the check box to enable SSO.</td>
</tr>
<tr>
<td>SAML SSO URL</td>
<td>The URL that is invoked to redirect users to your identity provider.</td>
</tr>
<tr>
<td>Remote logout URL</td>
<td>The URL that is returned to your users after they log out.</td>
</tr>
<tr>
<td>Certificate fingerprint</td>
<td>The SHA1 fingerprint of the SAML certificate. Obtain this from your SAML identity provider.</td>
</tr>
<tr>
<td>SAML User ID</td>
<td>The SAML attribute for SSO user ID.</td>
</tr>
<tr>
<td>Custom error message (optional)</td>
<td>The error message displayed when a user’s SSO login attempt is unsuccessful.</td>
</tr>
</tbody>
</table>
CHAPTER 4 Administration

This chapter explains how to configure settings in the Administration tab.

Administration

The Administration section allows authorized users to manage company-wide settings. The Administration section provides access to the following tabs:

- Users
- Web apps
- Notifications
- Services
- SSL Certificates
- Custom WAF rules
- Templates
- IP Lists
- Company Profile
- API
The dashboard summarizes the list of web applications that are associated with a given company and protected by Oracle Dyn Web Application Security WAF. It also includes consumption statistics.

You can export the consumption summary as PDF, CSV, and printable formats. To view consumption data for a specific time range, select an option from the time range drop-down list. Options include:

- **Last 6h** - (Default) Displays data for the last six hours.
- **Last 24h** - Displays data for the last 24 hours.
- **Last 2d** - Displays data for the last two days.
Create and Manage Web Apps

Web apps allow you to add and apply Zenedge's products to your domains, including WAF rules, Bot Manager, and Access Control. Groups of domains using the same endpoint can be managed by one web app with a shared security profile for easier management. Each web app generates a custom CNAME record needed to route your domain's traffic through Zenedge's platform.

Creating a Web App

1. From the Administration dashboard, select Web Apps. A new window appears.
2. In the Add web application window, fill in the fields pertaining to your domain and origin servers as needed.
   - **Domain** - Your fully qualified domain or hostname. It is highly recommended that you use a domain with a label, such as "www.example.com", instead of a root domain or "naked" domain such as "example.com".
   - **Name** - A unique name for your application.
   - **Origin servers** - The IP address or domain of your origin servers. The web app will route traffic from your domains to these servers. Zenedge uses ports 80 or 443. Click + Add another to add additional origin servers, and use the weight function to load balance the traffic to your servers as desired. Warning: It is highly recommended to avoid using domains as origin servers.
   - **Base domain redirect** - Redirect requests from your "base" domain to its full domain.
Additional domains - Add any additional domains you would like routed through your web app. Note: Any additional domains must have the same origins servers as.

Enable HTTPS support - Add HTTPS support to your web app.

3. Click Save.

Accessing Your Web App
Once your web app has been created, you can access and manage the web using the following steps.

1. From the Administration dashboard, select Web Apps. A new window appears.
2. Click Manage beside the web app you would like to access.
3. From the dashboard, you can add and manage various modules, such as WAF rules, Bot Manager, and Access Control.

Web App Staging
Zenedge allows you to create a staging environment for your web app to test your configuration without impacting production traffic.

1. From the Administration dashboard, select Web apps. A new window appears.
2. In the Actions column, click the three dots beside web app you want to stage and select Create Staging from the drop-down menu. A new window appears.
3. Note the IP address in the Your staging EDGE server IP field. You will need to point the web application to the staging EDGE server. All customers share the same IP address.
4. Click Create. You will be notified by email when the staging environment has been created.

Deleting a Web App
Use the following steps to remove a web app from your account.
1. From the Administration dashboard, select Web Apps. A new window appears.
2. In the Actions column, click the three dots beside web app you want to remove. A drop-down menu appears.
3. Select Delete from the drop-down menu.
4. Type "delete" into the confirmation field, and then click **YES, I understand the consequences, delete this webapp.**

**Viewing Alerts**

The Alerts dashboard shows all web application alerts on one page. Alerting is used to understand what rules and countermeasures are triggered by requests and are used as a basis to move request handling into block mode. An alert is registered in the portal and the request is still proxied to the origin. You can search through alerts and review the log entries associated with alerts. Only traffic that is alerted, not blocked, is displayed in the Alerts dashboard.

To access the Alerts dashboard, from the Web app dashboard, select **Alerts.**
The following information is displayed in the dashboard:

- **Alerts Raised** - Displays alert data over time by the alert source (for example, WAF or JS Challenge).

- **Recent Alerts** - Displays the recent alerted requests. Use the Alerts drop-down list to filter the results by the type of alert.

- **Top IPs Alerted** - Displays the top IP addresses from alerted requests during the selected date period. Use the Alerts drop-down list to filter the results by the type of alert.

- **Top Alerted User Agents** - Displays the top user agents from alerted requests during the selected date period. Use the Alerts drop-down list to filter the results by the type of alert.
To download the dashboard view as an image, click **Save**. To view alerts data for a specific time range, select an option from the time range drop-down list. Options include:

- **Last 6h** - (Default) Displays data for the last six hours.
- **Last 24h** - Displays data for the last 24 hours.
- **Last 2d** - Displays data for the last two days.
- **Last 7d** - Displays data for the last seven days.
- **Last 30d** - Displays data for the last 30 days.
- **Custom Range** - Select a start date and an end date within the past 30 days, and then click **Apply**.

**Viewing Changes**

The **Changes** tab provides access to a list of web app changes in various publishing states. Change views include:

- **Changes to be published** - Displays web application configuration changes waiting to be published to the edge servers. You can revert or publish changes from this view.
- **Changes publishing now** - Displays changes for web application configuration which are currently being published to the edge servers.
- **Recently published** - Displays recently published changes. If no changes were published within the past 30 days, the date and time of the most recent change displays. Use the filters to display changes by feature type and a specified time range.
To access web app changes

1. From the Administration dashboard, select **Web apps**.
2. Click **Manage** beside the web app you would like to change.
3. From the Web app dashboard, select **Changes**.

To revert pending changes

Before publishing a change, you can revert the change to its current published state. Once a
CHAPTER 4 Administration

change is published, it cannot be reverted.

1. Click Revert beside the change you want to remove from the To Be Published list.

2. In the confirmation dialog box, type revert and then click YES, I understand the consequences, revert this change.

To publish pending changes

When you make web application configuration changes, the changes appear in the list to be published.

1. Click Publish for the change you want to publish, or click the Publish button to publish all changes in the list.

2. The published change is added to the Being published now list. Changes take approximately seven to ten minutes to be published to the edge servers.

Logs

You can find a specific log using predefined filters. The details of each logged event are provided.
To access Logs

1. From the Administration dashboard, select Web apps.
2. Click Manage beside the web app you would like to view.
3. From the Web app dashboard, select Logs.

Viewing Logs

To view log activity data for a specific time range, select an option from the time range drop-down list. Options include:

- **Last 15 min** - Displays data for the last 15 minutes.
- **Last 30min** - Displays data for the last 30 minutes.
- **Last 1hr** - Displays data for the last hour.
- **Last 6h** - (Default) Displays data for the last six hours.
- **Last 24h** - Displays data for the last 24 hours.
- **Custom Range** - Select a start date and an end date within the past 60 days, and then click Apply.

Logs are retained for 7 days.
To filter results

1. Enter the field name you want to use as the filter, or select a field name from the list.
2. Enter or select the information you want to apply to the filter.
   a. To find all logs within the specified time period that contain the specified information, click the filter icon.
   b. To exclude the specified information from the log results, click the exclude icon.

You can use information from a specific log as an applied filter.

1. Click a log to expand the log details.
2. Click the filter or exclude icon for a specific field.

This creates an applied filter using the information in the field. The results display or exclude logs containing the specified information.
To export the log to a spreadsheet

Click the to Excel button to export up to 250 log lines to a spreadsheet.

Web App Settings

This chapter explains how to use the Settings tab.

Settings

The Settings tab provides access to components of service delivery, such as SSL/TLS encryption. You can manage the configuration of a web application, including the origin servers and list of domains that share the security settings.

To access Settings

1. From the Administration dashboard, select Web apps.
2. Click Manage beside the web app you would like to view.
3. From the Web app dashboard, select Settings.

Advanced Settings

Advanced settings include cache headers, indicating that the platform is deployed behind a CDN and to respect the Real ClientIP in the correct header.
To configure advanced settings

1. Click the **Settings** tab, and then select **Advanced**.
2. Select **Enable HTTPS support**.
3. Configure the following settings:
   a. **HTTP/2 Support** - Contact Support for changes. HTTP/2 is the first major upgrade to the HTTP protocol. The main focus of HTTP/2 is performance, especially latency as perceived by the end-user while using a browser.
   b. **Respect caching headers** - Automatically cache content based on the request HTTP headers. Caching rules may override caching policy.
   c. **Behind CDN** - Enable if web application uses CDN which allows to better define the client IP address and other useful information.
   d. **WebSocket Support** - For specified URLs the WAF is disabled. All challenges,
like JSC, HIC and etc., remain active. To disable challenges for specific URL, use the bypass action in the access control for the WebSocket URLs.

4. Click **Save**.

The updated settings are added to the list of changes to be published.

See [Viewing Changes](#) for information on reverting or publishing changes.

**HTTPS Support**

HTTPS encrypts your visitors' personal data to and from your web application.
To configure HTTPS support

1. Click the Settings tab, and then select HTTPS Support.
2. Select Enable HTTPS support.
3. Configure the following settings:

a. **SSL certificate** - Select the SSL certificate to assign to the current web application, or click + Add SSL Certificate to create a new SSL certificate for the web application. See SSL Certificates for more information.

b. **SSL Cypher Group** - Contains a list of supported cyphers that help secure a network connection that uses TLS or SSL.

c. **OCSP stapling** - OCSP stapling is an alternative approach to the original Online Certificate Status Protocol (OCSP) for determining whether an SSL certificate is valid.

d. **HTTP to HTTPS redirect** - When enabled, all HTTP traffic is automatically redirected to HTTPS.

e. **HTTPS Origin servers** - The IP addresses of the HTTPS web app hosts servers. Click + Add HTTPS origin server to add another server.

f. **HTTPS for additional domains** - Add the HTTPS support to the additional domains, in addition to the primary. Additional domains can be added in the Name and Domains tab.

   ![Tip](lightbulb) Adding additional domains with HTTPS support requires SNI support in the origin.

4. Click **Save**.

The updated settings are added to the list of changes to be published.

See Viewing Changes for information on reverting or publishing changes.

**Names and Domains**

The Names and Domains menu option provides an overview of domain settings, including redirect and which CNAME is assigned.
To view and update names and domains settings

1. Click the **Settings** tab, and then select **Names and Domains**.

2. Update the following settings (some information is managed at the Administration level):

   a. **Name** - The web app app name, used in lists and selection.
   
   b. **CNAME assigned** - The CNAME record assigned to web app (managed at the Administration level).
   
   c. **Domain** - The main domain name. The main domain cannot be changed, but you can create a new web app with the new domain name.
   
   d. **Base domain redirection (APEX redirect)** - If enabled, redirects requests from your "base" domain to its full domain (e.g., from http://example.com/home to http://www.example.com/home)
to http://www.example.com/home).

e. **Additional domains** - Add each domain on the separate line.

3. Click **Save**.

The updated settings are added to the list of changes to be published.

See [Viewing Changes](#) for information on reverting or publishing changes.

### Origin and Backup Servers

You can designate a backup server and configure round robin load balancing. Custom headers can be used to further validate requests, in addition to Total Origin Lockdown.
To configure origin servers

1. Click the **Settings** tab, and then select **Origin Servers**.
2. Select **Enable HTTPS support**.
3. Configure the following settings:

   a. **Origin servers** - The IP addresses of the web app hosts servers. All requests load balanced across all origin servers based on the weight field. It’s highly recommended to avoid using domain names as origin servers.

   b. **Health checks** -
      - **URL** - Enter the URL of the origin servers being monitored.
      - **Expected response code** - Select the HTTP response codes to be returned when the origin servers are healthy.
      - **Expected response text** - Enter the response text for the health check to search for to determine whether the health check will pass or fail.
      - **Check interval** - Select the period of time between health checks of the instance.
      - **Response timeout** - Select the maximum time to wait for a reply before marking the health check as failed.
      - **Healthy/unhealthy threshold** - Enter the number of successful and failed health checks before the server is marked down/up.

   c. **Load balance method** -
      - **IP Hash** - All incoming requests from the same client IP address will go to the same content origination server.
      - **Round Robin** - Forwards requests sequentially to the available origin servers. After a request is sent to the last origin server, the process starts again with the first origin server.
      - **Sticky Cookie** - Adds a session cookie to the first response from the origin server and identifies the server that sent the response. The client’s next
request contains the cookie value, and nginx routes the request to the origin server that responded to the first request.

d. **Backup servers** - The backup servers to be used when all origin servers fail.

e. **GZIP compression** - When enabled, supports GZIP compressed content, improving performance.

f. **Custom headers** - The custom HTTP headers to set or override in requests to origin servers. You can use these headers to help validate that the requests made to your origin server were sent from EDGE. You can configure your origin server to only allow requests that contain the custom header values that you specify.

4. Click **Save**.

The updated settings are added to the list of changes to be published.

See [Viewing Changes](#) for information on reverting or publishing changes.

**Response Headers**

You can add response headers to further contextualize the response on the client side. Response headers contain the date, size, and type of file that the server sends back to the client, as well as information about the server.
To add a response header

1. Click the Settings tab, and then select Response Headers.
2. Click + Add response header.
3. Enter the following information:
   a. Name - Unique name for the header.
   b. HTTP header field name - The name to set for HTTP header.
   c. HTTP value field name - The value to set for HTTP header.
4. Click Save.

The response header is added to the list of changes to be published.

See Viewing Changes for information on reverting or publishing changes.
To edit a response header

1. Click **Edit** for the response header you want to update.
2. Make the changes, and then click **Save**.

The updated response header is added to the list of changes to be published. See [Viewing Changes](#) for information on reverting or publishing changes.

To delete a response header

1. Click **delete** for the response header you want to delete.
2. Type **Delete**, and then click **Yes, I understand the consequences, delete this response header**.

The deleted response header is added to the list of changes to be published.

**Note**
Response headers can only be deleted from the origin.

See [Viewing Changes](#) for information on reverting or publishing changes.

**Add and Manage Company Services**

You can add, update, or deactivate services that are available through the company's partner.

To access Services, click the **Administration** tab, and then select **Services**.
To add a service

1. Click **Add Service**, and then select the service. The Add Service window for the specific service opens.
2. Configure the service settings.
3. Click **Save**.

**To edit a service**

1. Click **Edit** for the service you want to edit.
2. Enter your changes, and then click **Save**.
To deactivate a service

1. Click **Deactivate** for the service you want to deactivate.
2. Type **deactivate** to confirm that you want to deactivate the service.
3. Click **I understand the consequences, deactivate the service**.

Inviting Users and Access Policies

The Users tab in the Administration dashboard allows authorized users to manage existing and create new users. You can invite a new user, manage permissions of existing users, and disable a user. It is important to note that the same user cannot belong to two different companies. Users can belong to either the company or web application levels, with different permission types. Oracle Dyn Web Application Security features fine grain permissions and access as well as two-factor authentication based on SMS.

To access the Users tab, click the Administration tab and then select **Users**.
Inviting Users

In the Users tab you can add new users and define permissions based on role. A new user can be invited (a unique email account is required) with the list of accessible web apps. If an email account is already registered in the Oracle Dyn WAF portal for any other companies, it cannot be used for a new invitation. The invite is sent by email from a Oracle Dyn email address. An account can be disabled or an invitation can be resent for an account which has never logged in.

To add a new user

1. From the Users tab, click + **Invite User**.
a. In the Invite new user dialog, specify the new user settings:

```
Invite new user

Email

A message from you (optional)

Web app permissions
Please select web apps to which user needs access to.
You can limit user permissions later.

OFF  www.example.com

OFF  www.example2.com

OFF  www.example1.com
```

b. Enter the email address for the new user in the Email field.

c. (Optional) Enter a message that will be sent to the new user’s email address.

d. Select the webapps that the user needs access to.

2. Click Invite.
The new user must accept the email invitation to begin using the portal.

3. (Optional) To resend the invite, select **Resend invite** from the actions drop-down menu.

**Managing Users**

User profile settings include the ability to manage permissions and other identity-related settings. You can also force a password change when managing a user. A user’s permissions to access web applications’ settings is fine grain and can be restricted based on job function. If company-level permissions include full control, then no further definition is required. The user will have full access to all web application settings. Company level permissions can be further defined to include access to various functions at the administrative level of control.

**To update a user**

1. Click **Manage** for the user you want to update.

![User Management Table]

You can use the Filter by list to sort emails or names alphabetically in ascending or descending order.

2. Update the user profile by clicking the tabs on the left.
**Account information** - Edit the user's name and phone number and then click Apply.

**Change password** - Enter a new password and then click Apply.

**Webapps permissions** - Select the access level for each application and then click Apply.

**Company permissions** - Select the check box for the permission you want to allow the user to access and then click Apply.

**System settings** - Update the Email, SSO User ID, or Phone number and then click Apply.

**Partner settings** - Update the SSO User ID and then click Save.

To delete a user

1. Click **Delete** for the user you want to delete.
2. In the confirmation dialog box, type delete and then click **YES, I understand the consequences, delete this user.**

Enable Two-Factor Authentication

When enabled, the user is required to use two-factor authentication.

To enable two-factor authentication

1. In the drop-down list next to your user name, select **My Profile.**

2. Select the **Security settings** tab, and then set the **Two-factor authentication** toggle to **On.**

3. Complete the steps to enable two-factor authentication.

Enabling Two-Factor Authentication

When enabled, all company users are required to use two-factor authentication.
The two-factor authentication methods that are supported include SMS, as well as any two-factor authentication app, such as Google Authenticator.

💡 Two-factor authentication can also be configured for an individual user. See Inviting Users and Access Policies.

To access two-factor authentication, click the Administration tab, and then select Company Profile.

To enable two-factor authentication

1. Click the Company Profile tab.
2. Set the Enable two-factor authentication policy toggle to On.
3. Click Apply.

Managing Custom WAF Rules

You can create custom rules in addition to the WAF rulesets that are already provided. The syntax of the custom rule is based on the regular expression and fully compatible with mod_security. You can display the list of web apps that are using a specific custom ruleset.

To access Custom WAF rules, click the Administration tab, and then select Custom WAF rules.

You can add, update, and delete custom WAF rules.

Note

Rules that are not proprietary to other companies can be imported (e.g., trustwave rules).
To add a custom WAF rule

1. Click **Add Custom WAF Rule**.
2. Enter a name and description for the rule.

3. The rule template must include two variables. These variables will be replaced during publishing:
   - \{\{\text{mode}\}\} - rule action, defined by the user in the UI, such as Alert only or Block. For example: `ctl:ruleEngine=\{\{\text{mode}\}\}`
   - \{\{\text{id\_1}\}\} - unique rule id. It is possible to use multiple IDs in one rule by using different variables, such as `\{\{\text{id\_2}\}\}`, `\{\{\text{id\_3}\}\}` and so on. For example: `id=\{\{\text{id\_1}\}\}`. The numbering is automatically generated by the portal.

4. Click Save.
To update a custom WAF rule

1. In the Actions column, click **Edit** for the rule you want to update.
2. Make the changes, and then click **Save**.

   You cannot edit a custom WAF rule that is enabled in a web app.

To delete a custom WAF rule

1. In the Actions column, click **Delete** for the rule you want to delete.
2. Click **OK** to confirm that you want to delete the rule.

   You cannot delete a custom WAF rule that is enabled in a web app.

To manage custom rules currently in use

The values displayed in the Used By column indicate whether the action for the rule is an alert or block. When a custom rule is in use, an icon appears in the Used By column.
1. Click the icon to open a popup window displaying the web apps where the custom rule is in use.

   ![Sample rule used by](sample_rule.png)

2. Click **Manage** in the popup window to open the WAF rules for the web app and update the actions for the custom rule.

### Managing IP Lists (Administration)

You can configure and manage company IP lists that are used by all web applications. Company IP lists are also displayed in each web application's IP list section, but are managed at the administration level.

To access IP Lists, click the **Administration** tab, and then select **IP Lists**.

IP Lists can be added and removed at the Administration level. Each IP should be on a separate line.
To add IP lists

1. Click + **Add IP List**. The Add IP List window opens.
2. Enter a name for the IP list.
3. Enter each IP address on a separate line.
4. Click **Save**.

**Note:** IP lists created at the company or administration level are inherited by web apps, but IP lists created at the web app level are not inherited between web apps.
The IPs column shows the number of IPs in the IP list. Click the icon to view the IPs.

**To update an IP list**
1. Click **Edit** for the IP list you want to update.
2. Enter your changes, and then click **Save**.

**To delete an IP list**
1. Click **Delete** for the IP list you want to delete.
2. Type **delete** to confirm you want to delete the IP list.
3. Click **Yes, I understand the consequences, delete this IP list**.

**Manage a Company Profile**
The Company Profile page is where you manage a company's contacts, authentication options, and billing information.
To add or update a company profile

1. Click the **Company Profile** tab.
2. Enter the company profile settings.
3. (Optional) To add another company profile, click **Add Another**.
4. Click **Apply**.
Company Profile Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company name</td>
<td>Enter the name of the company.</td>
</tr>
<tr>
<td>Company country</td>
<td>The company's country, which will also be used in the billing address.</td>
</tr>
<tr>
<td>Company phone</td>
<td>The company contact phone number.</td>
</tr>
<tr>
<td>Enable two factor authentication policy (2A)</td>
<td>When enabled, all company users are required to configure the two factor authentication.</td>
</tr>
<tr>
<td>Billing currency</td>
<td>The currency used for billing.</td>
</tr>
<tr>
<td>Billing address (optional)</td>
<td>The address used for billing.</td>
</tr>
<tr>
<td>Tax ID (optional)</td>
<td>The Taxpayer Identification Number (TIN).</td>
</tr>
<tr>
<td>Billing contact (optional)</td>
<td>The contact for billing questions or requests.</td>
</tr>
<tr>
<td>Technical contact (optional)</td>
<td>The contact person for technical questions or requests.</td>
</tr>
<tr>
<td>External Data</td>
<td>The data from any external systems to be stored together with company profile. This information is shown only to the partner users and customer support. Company users do not have access to this information.</td>
</tr>
</tbody>
</table>

Managing Templates

You can save and manage a frequently used web app configuration as a template. A template can be applied to a specific web app, and a specific configuration of a web app can be exported as a template.

To access Templates, click the Administration tab, and then select Templates.
You can add templates that can be applied to web apps. You can also update and delete templates.

To add a template

1. Click **Add webapp template**. The Add Template window opens.
2. Enter the template name.
3. Enter a description of the template.
4. Select the web app containing the settings you want to use for the template.
5. Select the settings from the web app that you want to save to the template.
6. Click **Create**.

**To update template**
1. In the Actions column, click **Edit** for the template you want to update.
2. Change the name and/or the description as needed.
3. Click **Update**.

**To apply a template to a web app**
1. Click **Apply** for the template you want to apply.
2. Select the web app where you want to apply the template.
3. Click **Apply**.

   🟡 The template will override current web app settings.

**To delete a template**
1. In the Actions column, click **Delete** for the template you want to delete.
2. Click **OK** to confirm that you want to delete the template.

**Setting Up Notifications**
The Notifications tab allows an authorized user to create and edit email-based notifications for various events and actions. Notifications include:
- **Network alerts** - Notifies users when a network alert is received for network profiles.
- **Node error occurred** - Notifies when an error occurs at an edge node during the processing of a node task.
- **Node status changed** - Notifies when the node status changes.
- **Subscriptions** - Notifies when a subscription event occurs.
- **Traffic lost or appeared** - Notifies when traffic is lost or appears for a web app.
- **Web app changes published** - Notifies users when changes are published to the EDGE nodes for selected web applications.
- **Web app created or deleted** - Notifies users when a web app is created or deleted.
- **Web app CNAME status changed** - Notifies users when a web app DNS CNAME changes are made for selected web apps.
- **Web app RPS changed** - Notifies users when web app RPS (requests per second) changes by more than the specified threshold value.
- **Web app daily report** - Sends a report daily.
- **Web app summary report** - Sends a summary report daily.
- **Origin status changed** - Notifies when the origin server status changes.

To access the Notifications tab, click the Administration tab, and then click Notifications.
To add a notification

1. From the Notifications tab, click **Add notification**.

2. In the select notification type dialog box, select the type of notification you want to add and then click **Next**.
# CHAPTER 4 Administration

## Step 1: select notification type

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network alerts</td>
<td>Notify once network alert is received for network profiles</td>
</tr>
<tr>
<td>Node error occurred</td>
<td>Notify when error occurs at edge node during node tasks processing.</td>
</tr>
<tr>
<td>Node status changed</td>
<td>Notify when node status changes.</td>
</tr>
<tr>
<td>Subscriptions</td>
<td>Notify when some subscription event occurs.</td>
</tr>
<tr>
<td>Traffic lost or appeared</td>
<td>Notify when traffic is lost or appear for some web application.</td>
</tr>
<tr>
<td>Web app changes published</td>
<td>Notify when some changes are published for selected web applications.</td>
</tr>
<tr>
<td>Web app created or deleted</td>
<td>Notify when a web application is created or deleted.</td>
</tr>
<tr>
<td>Web app CNAME status changed</td>
<td>Notify when CNAME is changed for selected web applications.</td>
</tr>
<tr>
<td>Web app RPS changed</td>
<td>Notify when RPS changes by more than N% for selected web applications.</td>
</tr>
<tr>
<td>Web app daily report</td>
<td>Send report every day at chosen time.</td>
</tr>
<tr>
<td>Web app summary report</td>
<td>Send report every day at chosen time.</td>
</tr>
<tr>
<td>Origin Status changed</td>
<td>Notify when the origin server status changed.</td>
</tr>
</tbody>
</table>
3. Specify the notification details based on your selection. Each user will receive a separate email.

   a. Network alerts
      * Name - Enter a unique name for the notification.
      * Network profiles - Select the network profiles for notifications.
      * Users (optional) - Select users to receive notifications.
      * Web hook URL (optional) - Set the URL to send POST requests to the URL.
      * Payload JSON - Customize payload JSON to be sent with a request.

   b. Node error occurred -
      * Name - Enter a unique name for the notification.
      * Users (optional) - Select users to receive notifications.
      * Web hook URL (optional) - Set the URL to send POST requests to the URL.
      * Payload JSON - Customize payload JSON to be sent with a request.

   c. Node status changed -
      * Name - Enter a unique name for the notification.
      * Users (optional) - Select users to receive notifications.
      * Web hook URL (optional) - Set the URL to send POST requests to the URL.
      * Payload JSON - Customize payload JSON to be sent with a request.

   d. Subscriptions -
      * Name - Enter a unique name for the notification.
      * Services - Select the services to monitor.
CHAPTER 4 Administration

- **Subscription actions** - Select the action that will trigger the notification.
- **Users** - Select users to receive notifications.

e. Traffic lost or appeared
   - **Name** - Enter a unique name for the notification.
   - **Traffic threshold** - Enter the threshold value for requests before an alert is sent.
   - **Users** - Select users to receive notifications.

f. Web app changes published
   - **Name** - Enter a unique name for the notification.
   - **Webapps** - Select the web apps for notifications.
   - **Users** - Select users to send notifications to.

g. Web app created or deleted
   - **Name** - Enter a unique name for the notification.
   - **Users** - Select users to send notifications to.

h. Web app CNAME status changed
   - **Name** - Enter a unique name for the notification.
   - **Webapps** - Select the web apps for notifications.
   - **Users** - Select users to send notifications to.

i. Web app RPS changed
   - **Name** - Enter a unique name for the notification.
   - **RPS change threshold** - Enter the threshold value for the change period. If needed, you can adjust the threshold to reduce notifications.
   - **RPS change period** - Enter the time period to compare the change. If needed, you can adjust the time period to reduce notifications.
   - **Max notifications** - Enter the maximum number of notifications to send
during the max period.

- **Max period** - Enter the time period for max notifications.
- **Webapps** - Select the web apps for notifications.
- **Users** - Select users to send notification to.

**Note**
You can adjust the RPS change threshold, RPS change period, max notifications, and max period to reduce the number of notifications that are sent.

j. Web app daily report -

- **Name** - Enter a unique name for the notification.
- **Send report at** - Select the time of day when you want the report to be sent.
- **Webapps** - Select the web apps to be included in the notification.
- **Users** - Select users to send notification to.

k. Web app summary report -

- **Name** - Enter a unique name for the notification.
- **Send report at** - Select the time of day when you want the report to be sent.
- **Webapps** - Select the web apps to be included in the notification.
- **Users** - Select users to send notification to.

l. Origin status changed -

- **Name** - Enter a unique name for the notification.
- **Change status to trigger notification** - Select the change status that will trigger the notification.
CHAPTER 4 Administration

- **Web apps to trigger notification** - Select the web apps that you want to trigger notifications when their origin status changes.
- **Users** - Select users to send notification to.
- **Web hook URL (optional)** - Set the URL to send POST requests to the URL.
- **Payload JSON** - Customize payload JSON to be sent with a request.

4. Click **Save**.

**To edit a notification**

1. Click **Edit** for the notification you want to update.

2. Make changes to the notification and then click **Save**.

**To delete a notification**

1. Click **Delete** for the notification you want to delete.

2. In the confirmation dialog box, type **delete** and click **YES, I understand the consequences, delete this notification.**
SSL Certificates

Oracle Dyn Web Application Security terminates SSL connections to inspect requests in runtime, and then re-encrypts requests before sending them to the origin for fulfillment. To use SSL with your web app, you must add a SSL certificate bundle to the system using the SSL Certificates tab. The certificate bundle you upload includes the public certificate and the corresponding private key. Self-signed certificates can be used for the internal communication within the suite. SSL certificates are applied at the company level, and every web app will have access to the SSL certificate.

To access the SSL Certificates tab, click the Administration tab, and then select SSL Certificates.

Working with SSL Certificates

Oracle Dyn Web Application Security accept third-party and self-signed certificates in PEM format only. The following is an example PEM encoded certificate:

```
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
```
Obtaining Third-Party SSL Certificates

You can purchase an SSL certificate from a trusted Certificate Authority such as Symantec, Thawte, RapidSSL, or GeoTrust. The certificate issuer will provide an SSL certificate that includes a certificate, intermediate certificate, and private key. Use this information, including the intermediate certificate, when adding an SSL certificate to Oracle Dyn Web Application Security.

An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, through the intermediate and ending with the SSL certificate issued to you.

Converting to PEM format

If you receive your certificates and keys in formats other than PEM, you must convert them before you can upload them to the system. You can use OpenSSL to convert certificates and keys to PEM format.

Uploading Certificate Chains

If you have multiple certificates that form a single certification chain, you must include all relevant certificates in one file before you upload them to the system. The following example of a certificate chain file includes four certificates:

```
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Base64_encoded_certificate>
-----END CERTIFICATE-----
```
Submitting Private Keys

If your private key submission returns an error, the most common reasons are your private key is malformed or the system does not recognize the encryption method used for your key.

Private key consistency

If you receive an error related to the private key, you can use OpenSSL to check its consistency:

```
openssl rsa -check -in <private_key>.pem
```

This command verifies that the key is intact, the passphrase is correct, and the file contains a valid RSA private key.

Decrypting a private key

If the system does not recognize the encryption technology used for your private key, decrypt the key. Upload the unencrypted version of the key with your certificate bundle. You can use OpenSSL to decrypt a private key:

```
openssl rsa -in <private_key>.pem -out <decrypted_private_key>.pem
```

To add an SSL certificate

1. Click + Add SSL certificate.
CHAPTER 4 Administration

Add SSL Certificate

**Name**
Name of SSL certificate

**Certificate**
Insert the certificate including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- statements. Must be in PEM format.

Must also include intermediate certificates (the website certificate must be first).

**Private key**
Insert the private key including the -----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY----- statements.

Must be in PEM format and not protected by a passphrase.

**Self-Signed Certificate**
Self-signed certificates will show an SSL warning in the browser and it is highly recommended to avoid using it for production web apps.

[Save button]
2. In the **Add SSL Certificate** dialog box, enter the following:

   - **Name**: Specify the **Name** of the self-signed or chain SSL certificate.
   - **Certificate**: Paste the certificate, in PEM format, in this field. You must also include intermediate certificates (the website certificate must be first). The following is an example:

   ```
   -----BEGIN CERTIFICATE-----
   <Base64_encoded_certificate>
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   <Intermediate_Base64_encoded_certificate>
   -----END CERTIFICATE-----
   ```

   - **Private key**: Paste the private key for the certificate, in PEM format, in this field. The private key cannot be protected by a passphrase. The following is an example:

   ```
   -----BEGIN PRIVATE KEY-----
   <Base64_encoded_private_key>
   -----END PRIVATE KEY-----
   ```

   - **Self-Signed Certificate**: Optional. Enable this field when using a self-signed certificate to show an SSL warning in the browser for the web app.

   ![](warning_icon) Disabling SSL certificate trust verification is not recommended for web apps in production.

3. Click **Save**.

4. To assign the SSL certificate to a web app, from the Web app dashboard, select **Settings** and then follow the instructions to configure [HTTPS Support](#).

### To view SSL certificate details

1. Click **Info** for the SSL certificate you want to view details for.
2. In the dialog box, click **Close** to return to the portal.

**To delete an SSL certificate**

⚠️ Use caution when removing an SSL certificate; unintentional deletion will result in downtime. Manage SSL certificate changes during change windows only.

1. Click **Delete** for the SSL certificate you want to delete.

2. In the confirmation dialog box, type **delete** and click **YES, I understand the consequences, delete this certificate.**

**Resetting Your Password**

Use the instructions below to reset your password.
Changing your password

1. From the User menu, click **My Profile**.

2. Click **Change password**.

3. Enter a new password that meets all of the requirements.

4. Click **Apply**.
Resetting your password if you forgot it

1. In the Zenedge login screen, click **Forgot your password?**

2. Enter your email address in the field and click **Reset Password**.
If you forgot the email address you used to create your account, contact Oracle + Dyn Technical Support.

3. If there is an account associated with your email, you will receive an email with instructions on resetting your password. In the Password reset instructions email, click **Reset my password**.

4. Enter a new password in the **new password** field and then click **Change password**.
You can now use your new password to log into the system.
CHAPTER 5 Access Control

This chapter explains how to set up and configure Access Control.

Access Control

The Access Control module provides the ability to define granular access rules to control traffic based on geo-location, threat intelligence feeds, UserAgent, IP, etc. You can create and review rules, enable and disable threat feeds, manage IP lists, and manage whitelists.

To open the Access Control module

1. From the Administration dashboard, select Web apps.
2. Click Manage beside the web app you would like to view.
3. From the Web app dashboard, select Access Control.

Access Control Dashboard

The Access Control dashboard displays widgets and graphs related to the actions taken by access rules for requests during the specified time period.

To save a snapshot of the current dashboard, click Save.

To view blocking and alerting activity data for a specific time range, select an option from the time range drop-down list. Options include:

- Last 6h - (Default) Displays data for the last six hours.
- Last 24h - Displays data for the last 24 hours.
- Last 2d - Displays data for the last two days.
- Last 7d - Displays data for the last seven days.
- Last 30d - Displays data for the last 30 days.
- Custom Range - Select a start date and an end date within the past 60 days, and then click Apply.
CHAPTER 5 Access Control

- **Blocked by Access Control** - Displays the number of requests blocked per access rule for the selected time period.
- **Top Blocked IP Address** - Displays the top IP addresses with blocked requests per access rule for the selected time period.
- **Alerted by Bot Manager** - Displays the Access Rules alerts for the selected time period.
- **Threat Feeds Alerts** - Displays the top threat feeds for alerts during the selected time period.

Access Rules

Access rules provide granular control over the web properties. Web property owners can create custom detailed rules.

The order of access rules determines how rules are applied to each request. When a request meets all conditions of a rule, the action for the rule is taken.

Uses for access rules include:

- Country
- URL
- IP
- HTTP Header

There are numerous conditions that can be used to create a new access control rule. Users can add a single access rule with multiple conditions.

⚠️ The request must match all conditions in order for the action to be taken.

Rule condition options include:

- **URL is** - match the URL address provided. URL is case-sensitive.
- **URL is NOT** - match all other URLs except the one provided. URL is case-sensitive.
CHAPTER 5 Access Control

- **URL starts with** - match the beginning of the URL. URL is case-sensitive.
- **URL ends with** - match only the end of the URL. URL is case-sensitive.
- **URL contains** - match the part of the URL address provided.
- **URL regex** - match the URL regular expression provided.
- **IP in** - the request IP address is in the list defined.
- **IP not in** - the request IP address is not in the list defined.
- **IP in list** - the request IP address is in the specified IP list.
- **IP not in list** - the request IP address is not in the specified IP list.
- **HTTP Header contains** - the HTTP Header contains the specified name and value.
- **HTTP Header regex** - the HTTP Header contains the specified HTTP regular expression.
- **Country in** - match all requests that originate from the specified country.
- **Country not in** - match requests from all countries except the specified country.
- **User Agent is** - matches the User Agent header specified.
- **User Agent is not** - match all other user agents except the one specified.

Action options include:

- **Log and Allow** - The request is logged, and no further action is taken.
- **Alert only** - The alert is triggered on all requests matching the rule conditions. Alerts are displayed on the Alerts dashboard.
- **Block with error page** - The error page appears with additional details, such as error description, IncidentID, and error code. Users can customize the error page text for a specific access rule.
- **Block with response code** - Only the selected response code appears in the response.
- **Show CAPTCHA** - Show a CAPTCHA challenge page instead of a requested page.
- **Redirect** - Redirects the matched request to the URL entered in the Redirect URL field.
Select the status code that you want to display upon redirect.

- **Bypass** - Bypass the selected handlers for all matching requests.

To open Access Rules, select **Access Rules** in the Access Control Module.

To add an access rule

1. Click **+ Add access rule**. The Add Access Rule window opens.
2. Enter a name for the access rule.
3. Select the access rule condition that must be met before the rule action is taken.
4. (Optional) Click **+ Add another** to add more rule conditions.
5. Select the rule action to be taken when the request matches the rule condition.
6. Add, replace, or remove an HTTP header condition.
7. (Optional) Click **+ Add another** to add more HTTP header conditions to the rule.
8. Click **Save**.

The rule is added to the Access Rules list. The access rule appears in the list of changes to be published.

See [Viewing Changes](#) for information on reverting or publishing changes.

To reorder access rules

Access rules will be applied to each request in the specified order.

1. Click **Reorder**. The Reorder window opens.

2. Click and drag the access rules to reorder the list.

3. Click **Save**.

The reordered access rule appears in the list of changes to be published.
To edit an access rule

1. Click **Edit** for the rule you want to edit.
2. Update the access rule.
3. Click **Save**.

The updated access rule appears in the list of changes to be published.
See [Viewing Changes](#) for information on reverting or publishing changes.

To duplicate an access rule

1. Click **Duplicate** for the access rule you want to copy.
2. Enter any additional details for the new access rule.
3. Click **Save**.

The duplicated access rule appears in the list of changes to be published.
See [Viewing Changes](#) for information on reverting or publishing changes.

A drop-down menu in the Actions column provides additional options.

To view the log for a specific access rule

1. In the list of access rules, click the arrow in the Actions column for the rule you want to view.
2. Click **View Logs**.
The Logs dashboard opens, displaying the log for the access rule.

**To delete an access rule**

You can delete a specific access rule. When you delete an access rule, the access rule is added to the list for publication.

1. In the list of access rules, click the arrow in the Actions column for the rule you want to delete.
2. Click **Delete**.

The rule is removed from the Access Rules list. The deleted access rule appears in the list of changes to be published.

See **Viewing Changes** for information on reverting or publishing changes.

**IP Lists**

The IP List option lets you add and manage lists of IPs for a specific web application. IP lists can be used in a blacklist or whitelist (such as a company scanner can be whitelisted if it runs from static IPs).

IP Lists for all web applications are managed at the Administration level.

To access IP Lists for the web app, select **IP Lists** in the Access Control Module.
To add IP lists

1. Click *Add IP List*.

The Add IP List window opens.
2. Enter a name for the IP list.
3. Enter each IP address on a separate line.

   Duplicate IPs are not allowed in a single IP list.

4. Click **Save**.

   The IP list appears in the list of changes to be published.
CHAPTER 5 Access Control

See Viewing Changes for information on reverting or publishing changes.

- The IPs column shows the number of IPs in the IP list. Click the icon to view the IPs in the IP list.
- The Used by column shows the number of IP whitelists currently using the IP list. Click the icon to view the IP whitelists where the IP list is currently in use.

To edit IP lists

1. Click Edit for the IP list you want to update.

  💡 A "?” indicates a company IP list and is managed at the Administration level.

2. Enter your changes.
3. Click Save.

The updated IP list appears in the list of changes to be published.

See Viewing Changes for information on reverting or publishing changes.

To delete IP lists

1. Click Delete for the IP list you want to delete.
2. Type delete to confirm you want to delete the IP list. This field is case sensitive.
3. Click Yes, I understand the consequences, delete this IP list.

The deleted IP list appears in the list of changes to be published.

See Viewing Changes for information on reverting or publishing changes.
IP Whitelist

The IP Whitelist allows you manage which IP addresses appear on the IP whitelist. Requests from the whitelisted IP addresses bypass all challenges, such as DDoS policies and Web Application Firewall (WAF).

To access the IP whitelist, select **IP Whitelist** in the Access Control Module.

To add IPs to the IP whitelist

1. Click **+ Add IP whitelist**.

   The Add IPs to whitelist window opens.
2. Enter the name of the whitelist.
3. Select IP lists you want to include in the whitelist.
4. Enter the IP addresses you want to add to the whitelist. Add individual IP address on a separate line.
5. Click Save.

The IP whitelist appears in the list of changes to be published.
See Viewing Changes for information on reverting or publishing changes.

- The IP addresses column shows the number of IP addresses in the IP whitelist. Click the icon to view the IPs included in the whitelist.
- The IP Lists column shows the number of IP lists included in the IP whitelist. Click the icon to view the IP lists currently in use (note: You can also update a web app IP list associated with the whitelist).

To edit IP whitelists

1. Click Edit for the IP whitelist you want to update.
2. Enter your changes.
3. Click Save.

The updated IP whitelist appears in the list of changes to be published.

See Viewing Changes for information on reverting or publishing changes.

To delete IP whitelists

1. Click Delete for the IP whitelist you want to delete.
2. Type delete to confirm you want to delete the IP whitelist.
3. Click Yes, I understand the consequences, delete this IP whitelist.

The deleted IP whitelist appears in the list of changes to be published.

See Viewing Changes for information on reverting or publishing changes.
Threat Intelligence

Access control that is based on the reputation of IPs protects a web application. Threat Intelligence receives feeds from several sources, including commercial data and open source project data to block or alert IPs based on reputation.

To configure Threat Intelligence feeds

1. In the Access Control Module, select **Threat Intelligence**.
2. For each threat feed, choose from the following settings, and then click **Apply**:
   - **Off** - Take no action on requests from matched IP addresses.
   - **Log only** - All requests from matched IP addresses trigger an alert, which will appear on the Alerts dashboard.
3. **Block** - Blocks all requests from the matched IP address with a 403 response code.

Each threat feed setting is added to the list of changes to be published.

See [Viewing Changes](#) for information on reverting or publishing changes.
CHAPTER 6 Bot Manager

This chapter explains how to set up and manage the Bot Manager.

Bot Manager

Non-human traffic makes up the majority of traffic to most sites. Bot Manager is designed to detect and block, or otherwise direct, non-human traffic that may interfere with site operations. The Bot Manager features mitigate bots that conduct content and price scraping, vulnerability scanning, comment spam, brute force attacks, and application-layer DDoS attacks. You can also whitelist good bots.

To access the Bot Manager

1. From the Administration dashboard, select Web apps.
2. Click Manage beside the web app you would like to view.
3. From the Web app dashboard, select Bot Manager.

Bot Manager Dashboard

The Bot Management dashboard provides an overview of the various countermeasures and their request handling ratios.
To save a snapshot of the current dashboard, click **Save**.

To view blocking and alerting activity data for a specific time range, select an option from the time range drop-down list. Options include:

- **Last 6h** - (Default) Displays data for the last six hours.
- **Last 24h** - Displays data for the last 24 hours.
- **Last 2d** - Displays data for the last two days.
- **Last 7d** - Displays data for the last seven days.
- **Last 30d** - Displays data for the last 30 days.
- **Custom Range** - Select a start date and an end date within the past 60 days, and then click **Apply**.

Select the check box next to the challenge(s) you want to display in each section of the Dashboard.
CHAPTER 6 Bot Manager

**Blocked by Bot Manager** - Displays the number of requests blocked per challenge for the selected time period.

**Top Blocked IP Address** - Displays the top IP addresses with blocked requests per challenge for the selected time period.

**Alerted by Bot Manager** - Displays the Bot Manager alerts for the selected time period.

**Top Alerted IP Addresses** - Displays the top IP addresses for alerts during the selected time period.

**Top Alerted User-Agents** - Displays the top User-Agents from alerts for each challenge during the selected time period.

**Bot Categories** - Displays Bot Policies requests by category.

**Captcha Challenge**

If a specific URL should be accessed only by a human, you can control it with Captcha protection. You can customize the comments for the Captcha Challenge for each URL.
To add a Captcha Challenge

1. In the Bot Manager, select **Captcha Challenge**.
2. Click + **Add Captcha**.
Add Captcha

**CAPTCHA title**
CAPTCHA page title text.

**CAPTCHA URL**
URL challenged by CAPTCHA.

**Session duration**
How many seconds we would not allow to resubmit CAPTCHA to the same user.

**CAPTCHA header**
CAPTCHA page header text, shown before CAPTCHA image.

**Footer text**
Text would be shown just after edit box and before submit button.

**Incorrect CAPTCHA text**
Text would be shown when incorrect text is entered.

**Submit button**
Text of the submit button.

We have detected an increased number of attempts to access this website. To help us keep this site secure, please let us know that you are not a robot by entering the text from the image below.

Enter the letters and numbers as they are shown in the image above.

The CAPTCHA was incorrect. Try again.

Yes, I am human
3. Enter the Captcha Challenge settings.
4. (Optional) Click **Preview Captcha** to preview the Captcha Challenge before you save it.
5. Click **Save**.

The Captcha Challenge is added to the list of changes to be published.

See **Viewing Changes** for information on reverting or publishing changes.

**To edit a Captcha Challenge**

1. Click **Edit** for the Captcha Challenge you want to edit.
2. Update the Captcha Challenge.
3. Click **Save**.

The updated Captcha Challenge is added to the list of changes to be published.

See **Viewing Changes** for information on reverting or publishing changes.

**To delete a Captcha Challenge**

- In the list of Captcha Challenges, click **Delete** for the challenge you want to delete.

The deleted Captcha Challenge is added to the list of changes to be published.

See **Viewing Changes** for information on reverting or publishing changes.
Captcha Challenge Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captcha Title</td>
<td>Enter the text for the Captcha page title.</td>
</tr>
<tr>
<td>Captcha URL</td>
<td>Enter the URL challenged by Captcha.</td>
</tr>
<tr>
<td>Session duration</td>
<td>Enter the number of seconds after which the Captcha challenge cannot be resubmitted to the same user.</td>
</tr>
<tr>
<td>Captcha header</td>
<td>Enter the text that will appear before the Captcha image (e.g., &quot;I am not a robot&quot;).</td>
</tr>
<tr>
<td>Footer text</td>
<td>Enter the text that will appear after the edit box and before the Submit button (e.g., &quot;Enter the letters and numbers as they are shown in the image above.&quot;).</td>
</tr>
<tr>
<td>Incorrect Captcha text</td>
<td>Enter the text that will appear when incorrect text is entered (e.g., &quot;The Captcha was incorrect. Please try again.&quot;).</td>
</tr>
<tr>
<td>Submit button</td>
<td>Enter the text for the Submit button (e.g., &quot;Yes, I am human.&quot;).</td>
</tr>
</tbody>
</table>

Device Fingerprinting Challenge (DFC)

Device Fingerprinting Challenge (DFC) generates a hashed signature of both virtual and real browsers based on 50+ attributes. These proprietary signatures are then leveraged for real-time correlation to identify and block malicious bots. The signature is based on a library of attributes detected via JavaScript listeners; the attributes include OS, screen resolution, fonts, UserAgent, IP, etc. We are constantly making improvements and considering new libraries to include in our DFC build. We can also exclude attributes from the signature as needed.
DFC collects attributes to generate a hashed signature about a client – if a fingerprint is not possible, then it will result in a block or alert action. If the same fingerprint is shared across multiple devices, these can also be enforced (e.g. blocked, alerted, redirected).

To configure DFC settings

1. In the Bot Manager, select **Device Fingerprinting Challenge**.
2. Select the **Enable Device Fingerprinting Challenge** check box.
3. Enter the details of the DFC.
4. (Optional) To preview the error message, click **Preview error page**.
5. Click **Save**.

The DFC is added to the list of changes to be published.
See Viewing Changes for information on reverting or publishing changes.

**DFC Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Fingerprinting Challenge</td>
<td>Enables an advanced countermeasure that generates a unique hashed signature based on a device’s attributes such as browser, screen resolution, OS, and more.</td>
</tr>
<tr>
<td>Actions to be taken for detected bots</td>
<td>Choose appropriate actions to take for any detected bots which fail the DFC (requests without device fingerprints). The options include: Alert - raising the alert and allow the request i.e. no block. Block with response code - block the requests with specified response code.</td>
</tr>
<tr>
<td>Action threshold</td>
<td>Specify the number of failed requests before taking action.</td>
</tr>
<tr>
<td>Threshold expiry period</td>
<td>Number of seconds before threshold expires.</td>
</tr>
<tr>
<td>Action expiry period</td>
<td>Number of seconds between challenges to the same IP address.</td>
</tr>
<tr>
<td>Max IPs allowed</td>
<td>Maximum number of IP addresses with the same device fingerprint.</td>
</tr>
<tr>
<td>Max IPs expiry period</td>
<td>Number of seconds before Max IPs expires.</td>
</tr>
</tbody>
</table>

**Human Interaction Challenge (HIC)**

Human Interaction Challenge (HIC) is an advanced countermeasure that allows the proxy to check various event listeners in the user's browser to determine if there is a human user making a request. Event listeners are essentially behavior markers for human users. Humans interact with the browser canvas differently than bots. A bot cannot present a behavior, or
would do so with a highly predictable pattern (such as clicking a single place on a webpage repetitively).

- The challenge is presented using an inserted JavaScript.
- If the user passes the challenge, a cookie is generated. The name and value are preset prior to the challenge. The value is a time stamp of the interaction.
- The user session is based on the IP and Fingerprint (such as UserAgent), if enabled.
- The challenge can block with a custom page or custom captcha, or can alert the origin with an additional custom header field. The origin can then make a determination of what to do with an alerted request (such as redirect).
- The challenge can be customized based on several features and thresholds.
- Whitelisted IPs are not subject to this challenge.
To configure HIC settings

1. In the Bot Manager, select **Human Interaction Challenge**.
2. Select the **Enable Human Interaction Challenge** check box to enable and configure the HIC settings.
3. Click **Save**.

The HIC change is added to the list of changes to be published.

See [Viewing Changes](#) for information on reverting or publishing changes.

### HIC Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Interaction Challenge</td>
<td>Enables an advanced countermeasure that looks for natural human interactions, such as mouse movements, time on site, and page scrolling to identify bots.</td>
</tr>
<tr>
<td>Actions to be taken for detected bots</td>
<td>Choose appropriate actions to take for any bots detected utilizing Human Interaction Challenge.</td>
</tr>
<tr>
<td>Action threshold</td>
<td>Specify the number of failed requests before taking action.</td>
</tr>
<tr>
<td>Threshold expiry period</td>
<td>Number of seconds before threshold expires.</td>
</tr>
<tr>
<td>Action expiry period</td>
<td>Number of seconds between challenges to the same IP address.</td>
</tr>
<tr>
<td>Interactions threshold</td>
<td>The number of interactions required for passing the challenge.</td>
</tr>
</tbody>
</table>
### Parameter | Description
--- | ---
Recording period | The number of seconds to record the interactions from the users.
Set header for failed requests | Allows you to add an additional HTTP header to requests that fail the challenge.

### IP Rate Limiting
IP Rate Limiting allows you to configure a threshold for the number of requests from a unique IP for the given period. You can also define the response code for the requests from the same IP that exceed the threshold.
To configure IP Rate Limiting settings

1. In the Bot Manager, select **IP Rate Limiting**.
2. Select the **Enable IP Rate Limiting** check box.
3. Enter the IP Rate Limiting settings.
4. Click **Save**.

The IP Rate Limiting change is added to the list of changes to be published.

See [Viewing Changes](#) for information on reverting or publishing changes.

**IP Rate Limiting Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Rate Limiting</td>
<td>Enables IP Rate Limiting and allows you to configure IP Rate Limiting parameters.</td>
</tr>
<tr>
<td>Rate limiting threshold</td>
<td>Enter the number of requests allowed from one IP address per one second.</td>
</tr>
<tr>
<td>Delayed threshold</td>
<td>Enter the maximum number of delayed requests before a request is blocked.</td>
</tr>
<tr>
<td>Block response code</td>
<td>Select the status code to return in response to blocked requests.</td>
</tr>
</tbody>
</table>

**Javascript Challenge (JSC)**

Javascript Challenge (JSC) filters abnormal/malicious bots and allows access only from real clients. Additional functionality, such as detecting NAT’d traffic, can mitigate the risk of blocking legitimate user traffic from users behind a shared IP. JSC settings include the ability to identify traffic that may be coming from a common IP (such as ISP, corporate web proxy), so enforcement does not apply to legitimate users.
To configure JSC settings

1. In the Bot Manager, select **Javascript Challenge**.
2. Click the **Enable Javascript Challenge** box to display **Yes**.
3. Enter the details of the JSC.
4. Click **Save**.

The JSC change is added to the list of changes to be published.

See **Viewing Changes** for information on reverting or publishing changes.
**CHAPTER 6 Bot Manager**

**JSC Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable JavaScript challenge</td>
<td>Enables the JSC to detect bot traffic and generate a series of responses based on the JSC settings.</td>
</tr>
<tr>
<td>JS Challenge Action</td>
<td>Action to take against failed JSC requests.</td>
</tr>
<tr>
<td>Action threshold</td>
<td>Specify the number of failed requests before taking action.</td>
</tr>
<tr>
<td>Action expire time</td>
<td>How many seconds between challenges to the same IP address.</td>
</tr>
<tr>
<td>Follow redirects</td>
<td>When enabled, the requests with 301/302 response will be challenged.</td>
</tr>
<tr>
<td>Enable NAT Support</td>
<td>When enabled, a unique hash is added to the IP Address expiration time, which prevents the blocking of visitors with shared IPs.</td>
</tr>
<tr>
<td>Block action</td>
<td>Action to take against failed JSC requests.</td>
</tr>
<tr>
<td>Block response code</td>
<td>The status code to return in response to blocked requests.</td>
</tr>
</tbody>
</table>

**Advanced Rate Limiting**

Advanced Rate Limiting allows you prevent excessive requests in a given time frame, per EDGE region.
There are numerous conditions that can be used to create a new rate limiting rule. Users can add a single rule with multiple conditions.

⚠️ Delay rules should appear at the top of the list and Block rules should appear at the bottom of the list. Also, "wider net" rules should appear at the bottom of the list to confirm that more specific rules are caught prior to less specific ones.

Limiting rule condition options include:

- **URL is** - match the URL address provided. URL is case-sensitive.
- **URL is NOT** - match all other URLs except the one provided. URL is case-sensitive.
- **URL starts with** - match the beginning of the URL. URL is case-sensitive.
- **URL ends with** - match only the end of the URL. URL is case-sensitive.
- **URL contains** - match the part of the URL address provided.
- **URL does not start with** - The start of the URL is not in the list defined.
- **URL does not end with** - The end of the URL is not in the list defined.
- **URL does not contain** - Match all other URLs except URLs containing the specified information.
- **URL matches regex** - Match the URL regular expression provided.
- **URL does not match regex** - Match all other URL regular expressions except for the regular expression provided.
- HTTP Method is - Match the HTTP method request.
- HTTP Method is not
- HTTP method in -
- HTTP method not in

Action options include:

- **Alert** - The alert is triggered on all requests matching the rate rule conditions. Alerts are displayed on the Alerts dashboard.
- **Block with page** - The error page appears with additional details, such as error description, IncidentID, and error code. Users can customize the error page text for a specific access rule.
- **Block with response code** - Only the selected response code appears in the response.
- **Delay** - Requests are delayed by the specified interval.

**To add an advanced rate limiting rule**

1. In the Bot Manager, select **Advanced Rate Limiting**.
2. Click **+ Add Rate Limiting Rule**. The Add rate limiting rule window opens.
3. Enter the rate limiting threshold.
4. Select the rate limiting condition that must be met before the rate limiting action is taken.
5. (Optional) Click **+ Add another** to add more rate limiting conditions.
6. Select the rate limiting action to be taken when the request matches the condition.
7. Click **Save**.
The rate limiting rule is added to the Rate Limiting Rules list. The rate limiting rule appears in the list of changes to be published.

See Viewing Changes for information on reverting or publishing changes.

To reorder advanced rate limiting rules

Rules will be applied to each request in the specified order.

1. Click Reorder. The Reorder window opens.

2. Click and drag the rules to reorder the list.

3. Click Save.

The reordered rule appears in the list of changes to be published.
Good Bot Whitelist

The Good Bot Whitelist list shows bots that are managed by known providers, such as Baidu or Google. You can allow the access from a specific good bot, or block a bot if it serves no business purpose. Allowed good bots from this menu are whitelisted.

The list of good bots is managed and continuously updated. You can also add good bots as an access control rule. See Access Rules.

To manage the Good Bots whitelist

1. In the Bot Manager, select Good Bot Whitelist.
2. Set the toggle to Yes for each bot you want to designate as a good bot.
3. Click Save.
CHAPTER 6 Bot Manager

The Good Bots whitelist is added to the list to be published.

See Viewing Changes for information on reverting or publishing changes.
CHAPTER 7 API Security

This chapter explains how to set up and manage API Security.

API Security

API Security uses advanced techniques to vet API requests, determine their legitimacy, and eliminate API attacks at the edge of the network based on unique hash identifiers received from the edge servers. Malicious activity is blocked by the web application security proxy while authorized traffic passes through seamlessly.

The solution works for both authenticated and un-authenticated API calls.

To access API Security

1. From the Administration dashboard, select Web apps.
2. Click Manage beside the web app you would like to view.

Configure API Security

The following information will guide you through configuring API Security. The process includes:

1. Enabling the security token challenge
2. Adding changes in your API clients
3. Checking logs to confirm integration
4. Enabling the challenge in block mode

Note

Before getting started, generate the private and public RSA keys, which are used for the token request encryption.
To open the Security Token Challenge, select **Security Token Challenge** in the API Security Module.

To enable the security token challenge

1. Select the **Enable Security Token Challenge** check box.
2. For **Action to be taken for failed requests**, select **Alert**.
3. In the **API path** field, enter the URI for the api (for example, `/api/`).
4. In the **Encryption private key** field, enter the RSA private key in PEM format.

**To add changes in your API clients**

- Ensure that you can receive a 418 response code from API calls, which is used for the challenge.
- Generate a message with the following parameters: unique user data:timestamp:20 symbols of sha256_hash(unique user data:timestamp)
- Encrypt the message with the given public key using RSAES-OAEP schema
- Send a POST request to the /__zenedge/a url with the encrypted message in the `ze-d` and `ze_d` headers, and receive the security token in the response in the `ze-a` or `ze_a` header.
- Include the security token in the `ze-a` and `ze_a` http header.

**Sample python code**

```python
# the message formulation
timestamp = int(time.time())

message = UNIQUE_USER_DATA+':'+str(timestamp)

message_hash = SHA256.new()
message_hash.update(message)

full_message = message+':{:.20}'.format(message_hash.hexdigest())

# scheme RSAES-OAEP

cipher = PKCS1_OAEP.new(public_key)
ciphertext = cipher.encrypt(full_message)

send_data = ciphertext.encode("hex")

# request to get token

connection.request("POST", "/__zenedge/a", ", {"Host": HOST_HEADER, "ze-d": send_data, "ze_d": send_data})
```
To check logs to confirm integration

1. View the logs.

2. Find access logs with the 418 response code. This is the code used when the challenge is first presented.

To enable the challenge in block mode

When the number of users reaches your predefined limit, change the action from Alert to Block. This will prevent unauthenticated connections to the API.
CHAPTER 8 Caching Policies

This chapter explains how to set up and manage Caching Policies.

Caching Policies Module

The platform offers advanced caching abilities to deliver content via its global network and accelerate application page load and execution time. Additional caching configurations are available through advanced templates that can be activated by the Security Operations team.

Caching helps improve efficiency by storing frequently used data. Cached content is served from the edge server(s) without the need to fetch it from the origin. Caching rules can be created and managed in the Caching Policies module.

To access the Caching Policies module

1. From the Administration dashboard, select Web apps.
2. Click Manage beside the web app you would like to change.
3. From the Web app dashboard, select Caching Policies.

Caching Dashboard

The Caching dashboard provides an overview of all current caching policies for a specific web application. Dashboard widgets allow users to understand how current caching functions are being used and what eligible objects are not being cached. Use the date range option to view activity for different periods of time. The following information is displayed in the dashboard:

- **Savings** - Displays the percentage of requests and GB's saved.
- **Caching by Countries** - Displays the top caching traffic by country. Hover over
- **Caching Requests** - Displays caching requests over a period of time.
- **Caching State** - Displays a caching status chart.
- **Top Not Cached** - Displays the top requests not cached.
To download the dashboard view as an image, click **Save**. To view blocking and alerting activity data for a specific time range, select an option from the time range drop-down list. Options include:

- **Last 6h** - (Default) Displays data for the last six hours.
- **Last 24h** - Displays data for the last 24 hours.
- **Last 2d** - Displays data for the last two days.
- **Last 7d** - Displays data for the last seven days.
- **Last 30d** - Displays data for the last 30 days.
- **Custom Range** - Select a start date and an end date within the past 30 days, and then click **Apply**.
CHAPTER 8 Caching Policies

Purge Cache

⚠️ It is strongly recommended to avoid purging the entire cache as the cache storage would be immediately invalidated. This will result in all new requests going back to the origin until the cache storage is full again. The purge cache function can be granular or global. Schedules can be established using the API.
To purge a specific resource

1. Select an option from the URL is drop-down menu.

2. Enter a URL in the **URL of resource to purge** field. Use the guidelines below to purge different resources.

   - **A specific resource**: Enter the resource’s URL.
   - **A home (root) page**: Enter /
   - **An entire cache**: Enter /* or click Purge entire cache.
   - **A specific directory only**: Enter /example
   - **A specific directory and everything underneath it**: Enter /example*
   - **A home (root) page for the additional domain**: Enter domain/
   - **An entire cache for the additional domain**: Enter domain/*
   - **A specific directory only for the additional domain**: Enter domain/example
CHAPTER 8 Caching Policies

- **A specific directory and everything underneath it for the additional domain:** Enter `domain/example`

3. Click **Purge now**.
   The resource is purged from all Edge nodes in approximately seven to ten minutes.

Caching Rules

It is important to note that rules are implemented in the sequence they are added. Add the most aggressive rules first to help prioritize the caching. A general approach can be to add "do not cache" rules before caching rules. A rule can be based on URL, File Type, or other resource.

![Caching Rules Table]

To add a new rule

1. Click **+ Add caching rule**.
2. In the **Select the rule type** dialog box, select the type of content you want to cache and click **Next**.
3. Specify URL caching rule settings:
   a. Add a new Caching URL rule.
      - **Name**: Enter the name of the caching rule.
      - **Expire after**: Select the expire time for files.
      - **Browser expire**: Optional. Select this option to enable the browser cache-control header.
      - **Browser expire after**: This option is only available if the Browser expire option is enabled.
      - **URLs to be cached**: Select a URL option from the drop-down menu. Enter the URL in the field and then click Add.
CHAPTER 8 Caching Policies

b. Add a new Caching file rule.
   - **Name**: Enter the Name of the caching rule.
   - **Expire after**: Select the expire time for files.
   - **Browser expire**: Optional. Select this option to enable the browser cache-control header.
   - **Browser expire after**: This option is only available if the Browser expire option is enabled.
   - **File types**: Enter file types separated by a space.

c. Add a new Never caching URL rule.
   - **Name**: Enter the name of the caching rule.
   - **URLs to be cached**: Select a URL option from the drop-down menu. Enter the URL in the field and then click Add.

d. Add a new Never caching file rule.
   - **Name**: Enter the name of the caching rule.
   - **File types**: Enter file types separated by a space.

4. Click **Save**.

   The caching rule appears in the list of changes to be published. See **Viewing Changes** for information on reverting or publishing changes.

**To edit a rule**

1. Click **Edit** for the rule you want to update.

   ![Edit and Delete buttons]

2. In the **Edit rule** dialog box, make changes to the rule and then click **Save**.
The edited rule appears in the list of changes to be published. See Viewing Changes for information on reverting or publishing changes.

To delete a rule

1. Click **Delete** for the notification you want to delete.

2. The deleted rule appears in the list of changes to be published. See Viewing Changes for information on reverting or publishing changes.

Zentags

Zentags allow web pages on your website to load faster. With Zentags, first "base" pages load from the cache, followed by the dynamic/personalized page content. Zentags provide the ability to tag static components in a dynamic page and cached; when called, dynamic components are rendered after to give the impression of fast load time so the user starts to perceive the page. The personalized sections in your html code need to be surrounded with Zentags.
CHAPTER 8 Caching Policies

To add a zentag

1. Click + Add zentag.
2. In the **Add zentag** dialog:
   a. Enter the **Name**.
   b. Select the **Zen type**.
   c. Enter an **ID**.
   d. Select an **Expire time**.

3. Click **Save**.

The Zentag appears in the list of changes to be published. See [Viewing Changes](#) for information on reverting or publishing changes.

**To edit a zentag**

1. Click **Edit** for the zentag you want to update.

2. In the **Edit Zentag** dialog box, make changes to the zentag and then click **Save**.

   The edited Zentag appears in the list of changes to be published. See [Viewing Changes](#) for information on reverting or publishing changes.

**To delete a zentag**

1. Click **Delete** for the zentag you want to delete.
2. In the confirmation dialog box, type **delete** and click **YES, I understand the consequences, delete this Zentag**.
   The deleted Zentag appears in the list of changes to be published. See [Viewing Changes](#) for information on reverting or publishing changes.

### Integrating Zentags with a Web App

**Add Zentags to the web app HTML code**

Zentags must surround the personalized sections in your HTML code. Zentag names are not case sensitive. For example, woodcutter, WOODcutter and woodCUTter represent identical Zentag names.

**Example:**

```
<!- ZENTAG:BEGIN:ZentagName --> your HTML code <!- ZENTAG:END:ZentagName" -->
```

To integrate Zentags with JavaScript, add a JavaScript callback function that would be called after the Zentag is loaded on the page. Callback function has to be present in the global namespace after Zentags are fetched.

**Example:**

```
<!- ZENTAG:BEGIN:ZentagName[:<JavaScript callback function name>] your HTML code!- ZENTAG:END:ZentagName" -->
```
CHAPTER 8 Caching Policies

Verify Zentag Integration

1. Verify that page is processed and cached by Oracle Dyn Web Application Security.
2. After the page loads, locate the "X-Cache-Status" response header.
   - If caching rules were set and configured properly, it should say "HIT". If it does not say "HIT", refresh your page. If refreshing does not work, make sure your caching rules are configured and enabled. Use the browser's developer tools to examine Network/Headers section of the request. This section should contain "X-Cache-Status" response header.
3. Verify that Zentags are processed by Oracle Dyn Web Application Security. Zentags are replaced with JavaScript code during the first request, so it's possible to see those in the source of the page using the browser's built-in functionality.
   - If you see the following HTML code, the Zentags were not processed. Make sure that Zentags are specified, properly described and enabled, and Zentag names match your HTML code.
     
     ```html
     <!-- ZENTAG:BEGIN:ZentagName -->
     your HTML code
     <!-- ZENTAG:END:ZentagName" -->
     ```
     - If you see the following HTML code, the Zentags were processed successfully. Upon subsequent requests, Zentags should be replaced directly with their content (instead of the placeholders). Content will be without Zentag's HTML code wrapper.
     ```html
     <div id="_zentag_ZentagName" style="display:none;"></div>
     ```
   - (Optional) Using your browser's developer tools, open the **Network** section and click **Filter**. Click **XHR** (Xml Http Request). This will display only ajax requests. There should be a "fetch_tags?..." request. In the query string you should find a
list of tags containing personalized content and to be fetched from the origin.
CHAPTER 9 Web Application Firewall

This chapter explains how to set up and manage Web Application Firewall.

Web Application Firewall

Configured as a reverse proxy, the Oracle Dyn Web Application Firewall (WAF) inspects all traffic destined to your web application origin and identifies and blocks all malicious traffic. WAF provides a custom security profile for each web application under protection based on more than 250 rules. Developing the security profile involves proxying traffic to establish a baseline, tuning, and moving into block mode.

To Access the Web Application Firewall Module

1. From the Administration dashboard, select Web apps.
2. Click Manage beside the web app you would like to change.
3. From the Web app dashboard, select Web Application Firewall.

WAF Dashboard

The WAF dashboard provides an overview of blocking and alerting activity for a specific web application. Dashboard widgets provide the ability to dive deeper into a specific IP, date range or rule set to understand the underlying threats and potential vulnerabilities. Use the date range option to view activity for different periods of time. The following information is displayed in the dashboard:

- **WAF Rules by Type** - Displays the top triggering rules that are disabled or are in alert or block mode.
- **Blocks by Rule** - The traffic that has been blocked by rule type. Click Off to disable blocking. Click Alert Only to turn on alerts and disable blocking. Click View logs to view the requests in detail. The information can be filtered by Rule ID number or by number of alerts.
• **Blocked Requests** - Displays a graph of blocked requests over time.

• **Alerts by Rule** - The suspicious traffic that has been alerted by rule type. Click **Off** to disable alerts. Click **Block** to turn on blocking and disable alerts. Click **View logs** to view the requests in detail. The information can be filtered by Rule ID number or by number of alerts. See **Logs** for more information.

• **Requests by IP Address** - Displays the top malicious IPs by number of requests. Click **View Logs** to view the requests in detail.

• **Requests Alerted** - Displays a graph of suspicious traffic over time.

• **WAF Requests by Country** - Displays the top malicious locations. The information can be filtered by Country, Alerts, and Blocks.
To download the dashboard view as an image, click **Save**. To view blocking and alerting activity data for a specific time range, select an option from the time range drop-down list. Options include:

- **Last 6h** - (Default) Displays data for the last six hours.
- **Last 24h** - Displays data for the last 24 hours.
- **Last 2d** - Displays data for the last two days.
- **Last 7d** - Displays data for the last seven days.
- **Last 30d** - Displays data for the last 30 days.
- **Custom Range** - Select a start date and an end date within the past 30 days, and then click **Apply**.

### Set Up and Tune the WAF

The following information will guide you through setting up and tuning the WAF. The process includes:

1. [Add a Web App](#)
2. [Test the Web App Functionality with Web Application Security](#)
3. [Point Your DNS to the Web Application Security CNAME](#)
4. [Tune the WAF](#)
5. [Advanced WAF Tuning](#)

### Requirements

To successfully complete the process, you must have the following:

- Public certificate for the fully qualified domain name of the web app.
- Corresponding private key for the web app in PEM format.
- IP Address of the web app (public IP address of the host server).
- Ability to update DNS records for the domain.

### Add a Web App

**To add a web app**

1. Log into [dojo.zenedge.com](http://dojo.zenedge.com).
2. Click the **Administration** tab, and then select **Web apps**.
3. Click + Add web app.

4. In the Add web application window, fill in the fields pertaining to your domain and origin servers as needed.

   - **Domain** - Your fully qualified domain or hostname. It is highly recommended that you use a domain with a label, such as "www.example.com", instead of a root domain or "naked" domain such as "example.com".

   - **Name** - A unique name for your application.

   - **Origin servers** - The IP address or domain of your origin servers. The web app will route traffic from your domains to these servers. Web Application Security uses ports 80 or 443. Click + Add another to add additional origin servers, and use the weight function to load balance the traffic to your servers as desired. Warning: It is highly recommended to avoid using domains as origin servers.

   - **Base domain redirect** - Redirect requests from your "base" domain to its full domain.

   - **Additional domains** - Add any additional domains you would like routed through your web app. Note: Any additional domains must have the same origins servers as

   - **Enable HTTPS support** - Add HTTPS support to your web app.

5. Click **Save**.

**Test the Web App Functionality with Web Application Security**

Before pointing your DNS to Web Application Security, you must test the functionality of the web app with Web Application Security to make sure requests are successfully sent through Web Application Security. You can do this by changing your host file to point to the web app’s IP address, which will force traffic for the domain to the IP address.

**To find the web app's IP address**

1. To find the web app’s CNAME, click the **Administration** tab, and then select **Web**
CHAPTER 9 Web Application Firewall

apps.

2. Click the web app to expand the web app details and find the CNAME.

3. Open Terminal (Mac and Linux) or Command Prompt (Windows), and type dig for the web app's CNAME.
   For example:
   
   dig www-example-com.zenedgerc.net
   
   You can find the IP address in the answer section.

4. Locate your /etc/hosts file and change the host file to point to the IP address.
CHAPTER 9 Web Application Firewall

To test the web app functionality

Do one of the following to test the web app functionality:

- Open the web app in a browser. Requests will be sent through Web Application Security, and the web app will function as if the DNS is pointing to the Web Application Security CNAME.

- Open Developer Tools in the browser, and then click the **Networks** tab. Click the request, and then check the response headers to verify that there is a X-Zen-Fury header with a long value (for example: X-Zen-Fury: 2da0ca5db26769b176b037bb157b04512099073).

- You can also check the web app’s Logs to see traffic that was routed through Web Application Security. If there are logs in the portal, then traffic went through Web Application Security. It may take a few minutes for the logs to show traffic. To check the web app’s Logs for web traffic, click the tab for the web app service (next to the **Administration** tab), and then select **Logs**.

  A 200 OK code indicates that the request was routed through Web Application Security. If you do not see a 200 OK code in the Log, contact Support.

Point Your DNS to the Web Application Security CNAME

After you test the web app, you can change your DNS to point to the Web Application Security CNAME to direct traffic to Web Application Security.

Tune the WAF

WAF Tuning enables you to block rules that were not triggered during the initial 7-10 days of monitoring.

Once traffic is routed to the Web Application Security network, recommendations will appear in the dojo portal after a few days. The WAF Recommendations engine aids in the optimization
of your WAF security profile. The Security Operations team proactively monitors all events to provide recommendations about the action of a specific ruleset. The Rule ID, WAF rule, and recommended action is displayed in this panel.

**To tune the WAF**

1. From the **Administration** tab, select **Web apps**.
2. Click **Web Application Firewall**, and then select **Recommendations**.
3. In the **Filter By** list, select **Block Recommendations**, and then click **Filter**.
4. Click **Accept Recommendations**.

Detailed information about the change appears in the list of changes to be published. See [Viewing Changes](#) for information on reverting or publishing changes.
Advanced WAF Tuning

Advanced WAF Tuning is available for customers with the appropriate subscription.

Once the action for these rules has been set to Block, the Security Operations Center (SOC) will proceed with the Advanced Tuning process. This process will analyze the last seven days of logs for triggered rules, which appear in Alert mode, and checks whether these rules are false positives (legitimate requests that triggered the rule) or true positives (malicious requests). This will reduce the number of false positives by tuning the rules that remained in Alert mode from the initial WAF tuning process. It will also enforce security by setting the action to Block for the rules that caught true positives.

Recommendations

The WAF Recommendations engine aids in the optimization of your WAF security profile. The Security Operations team proactively monitors all events to provide recommendations about the action of a specific ruleset. The Rule ID, WAF rule, and Recommended action is displayed in this panel.
To accept a recommended action

1. (Optional) Select All Recommendations, Alert Recommendations, Block
CHAPTER 9 Web Application Firewall

Recommendations, or Hidden Recommendations from the Filter by list and then click Filter.

2. Review the Rule ID, WAF Rule, and Recommended Action in the list.
3. Click Accept for the recommended action you want to accept.

![Rule ID, WAF rule, Recommended action table]

Detailed information about the change appears in the list of changes to be published. See Viewing Changes for information on reverting or publishing changes.

To accept all recommendations

1. Click Accept {number} Recommendations.

![WAF RECOMMENDED ACTIONS]

2. Detailed information about the changes appear in the list of changes to be published. See Viewing Changes for information on reverting or publishing changes.
To hide a recommendation

1. (Optional) Select All Recommendations, Alert Recommendations, or Block Recommendations from the Filter by list and then click Filter.

2. Review the Rule ID, WAF Rule, and Recommended Action in the list.

3. Click Hide for the recommended action you want to hide.

The recommended action is added to the Hidden Recommendations.

💡 You can view recommendations that have been hidden by selecting Hidden Recommendations.

WAF Rules

WAF Rules provide visibility of the rulesets used for a web app. The rule ID, Name/Description, Settings, and Actions of each rule set are displayed.

For a list of WAF protection rules and their intended purpose, see Protection Rule IDs.
Filtering the Displayed List of Rules

To help you locate a rule, you can filter the list that is displayed. Filters include: Rule ID, Rule action, Rule Types, OWASP 2013, Application Specific, Compliance, and Other.

- Enter a rule ID number in the Rule ID field and then click Add. The filter is added to the Applied filters and the rule list is updated to reflect the applied filter.
• Click a filter option to apply the filter to the list. The filter is added to the Applied filters and the rule list is updated to reflect the applied filter.

💡 Applied filters can be removed by clicking the x beside the filter name.

Managing Exclusions

Exclusions are the key to reducing false positives; Oracle Dyn Web Application Security permits a variety of exclusion types as per the figure below. The Oracle Dyn Security Operations team will design and test these exclusions following a review of the tuning report and in concurrence with the client’s approvals and change management practices. A visibility of the details for each ruleset helps to understand the actual behavior of each ruleset. All rulesets are based on regular expression.

To add a rule exclusion

1. Click Exclusions beside the rule you want to manage.

2. In the Rule exclusions dialog box, enter a value in the Request field beside the request you want to add. The values you add will be ignored by the rule.

   • Request cookie value - Specify exact cookie name for cookie value to be ignored.
- **Request cookie names** - Specify exact cookie *name* for cookie *name* to be ignored.
- **Request parameters** - Specify exact argument *name* for its *value* to be ignored.
- **Request parameter names** - Specify exact argument *name* for its *name* to be ignored.
### Rule 970901 exclusions

<table>
<thead>
<tr>
<th><strong>Request cookie values</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add request cookies to be ignored by the rule. This variable is a collection of all of request cookies (values only).</td>
<td>Request cookie value</td>
</tr>
<tr>
<td></td>
<td>+ Add another</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Request cookie names</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add request cookie names to be ignored by the rule. This variable is a collection of the names of all request cookies.</td>
<td>Request cookie name</td>
</tr>
<tr>
<td></td>
<td>+ Add another</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Request parameters</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add request parameters to be ignored by the rule. This variable is a collection of the names and values of all request parameters.</td>
<td>Request parameter</td>
</tr>
<tr>
<td></td>
<td>+ Add another</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Request parameter names</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add request parameter names to be ignored by the rule. This variable is a collection of the names of all request parameters.</td>
<td>Request parameter name</td>
</tr>
<tr>
<td></td>
<td>+ Add another</td>
</tr>
</tbody>
</table>

3. (Optional) Click **Add another** to add more values.
4. Click **Save**.

---

### Viewing Templates

Templates display rule details including the regular expression.
To view a template

1. Click **Template** beside the rule you want to view details for.

2. The template details window appears.
3. Click **Cancel** to return to the list of WAF rules.
CHAPTER 9 Web Application Firewall

Viewing Logs
Logs display the details of request events and incident responses. Click View logs beside the rule you want to view details for. See Logs for more information.

Applying an Action to a Rule
Ruleset actions can be managed in WAF Rules by selecting one of the action options beside a rule and clicking Save. Actions include:

- **Off** - The rule is disabled.
- **Block** - Matching requests are blocked.

**Warning:** It is recommended that you contact the Security Operations team to get expert advice before switching rules to Block mode.

- **Alert** - Matching requests generate an alert, and the request is proxied.

WAF Protection Rule IDs
The Oracle Dyn Web Application Security WAF service supports many protection rule types. The following list provides a brief explanation of the purpose of each protection rule type.
### Protection Rules

<table>
<thead>
<tr>
<th>Rule ID/Key</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90001</td>
<td>Filter Profanity</td>
<td>Detects profanity used in request headers and body.</td>
</tr>
<tr>
<td>90002</td>
<td>United States Social Security Number Leakage</td>
<td>Detects leakage of US SSN in response body and headers.</td>
</tr>
<tr>
<td>90004</td>
<td>Executable File Upload Attempt</td>
<td>Detects attempts to upload executable files through input forms.</td>
</tr>
<tr>
<td>90005</td>
<td>Brazilian Social Security Number (CPF) Leakage</td>
<td>Detects leakage of Brazilian CPF in response body and headers</td>
</tr>
<tr>
<td>90006</td>
<td>Credit Card Leakage in Request: GSA SmartPay</td>
<td>Detects GSA SmartPay credit card numbers in user input.</td>
</tr>
<tr>
<td>90007</td>
<td>Credit Card Leakage in Request: MasterCard</td>
<td>Detects MasterCard credit card numbers in user input.</td>
</tr>
<tr>
<td>90008</td>
<td>Credit Card Leakage in Request: Visa</td>
<td>Detects Visa credit card numbers in user input.</td>
</tr>
<tr>
<td>90009</td>
<td>Credit Card Leakage in Request: American Express</td>
<td>Detects American Express credit card numbers in user input.</td>
</tr>
<tr>
<td>90010</td>
<td>Credit Card Leakage in Request: Diners Club</td>
<td>Detects Diners Club credit card numbers in user input.</td>
</tr>
<tr>
<td>90011</td>
<td>Credit Card Leakage in Request: enRoute</td>
<td>Detects enRoute credit card numbers in user input.</td>
</tr>
</tbody>
</table>

**CHAPTER 9 Web Application Firewall**

Web Application Security User Guide 166
<table>
<thead>
<tr>
<th>Rule ID/Key</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90012</td>
<td>Credit Card Leakage in Request: Discover</td>
<td>Detects Discover credit card numbers in user input.</td>
</tr>
<tr>
<td>90013</td>
<td>Credit Card Leakage in Request: JCB</td>
<td>Detects JCB credit card numbers in user input.</td>
</tr>
<tr>
<td>90014</td>
<td>Credit Card Leakage in Request: GSA SmartPay</td>
<td>Detects GSA SmartPay credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90015</td>
<td>Credit Card Leakage in Request: MasterCard</td>
<td>Detects MasterCard credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90016</td>
<td>Credit Card Leakage in Request: Visa</td>
<td>Detects Visa credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90017</td>
<td>Credit Card Leakage in Request: American Express</td>
<td>Detects American Express credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90018</td>
<td>Credit Card Leakage in Request: Diners Club</td>
<td>Detects Diners Club credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90019</td>
<td>Credit Card Leakage in Request: enRoute</td>
<td>Detects enRoute credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90020</td>
<td>Credit Card Leakage in Request: Discover</td>
<td>Detects Discover credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90021</td>
<td>Credit Card Leakage in Request: JCB</td>
<td>Detects JCB credit card numbers sent from site to user.</td>
</tr>
<tr>
<td>90022</td>
<td>Credit Card Track 1 Data Leakage</td>
<td>Detects credit card track 1 data in the response body.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>90023</td>
<td>Credit Card Track 2 Data Leakage</td>
<td>Detects credit card track 2 data in the response body.</td>
</tr>
<tr>
<td>90024</td>
<td>Credit Card PAN Leakage</td>
<td>Detects credit card primary account number in the response body.</td>
</tr>
<tr>
<td>90025</td>
<td>visitorTracker_isMob Malware Detection</td>
<td>Detects and/or blocks visitorTracker_isMob malware.</td>
</tr>
<tr>
<td>120133</td>
<td>Canadian Social Identification Number (SIN) Leakage</td>
<td>Detects leakage of Canadian SIN in response body and headers.</td>
</tr>
<tr>
<td>900032</td>
<td>HTTP Parameter Polution (HPP) Detection</td>
<td>Detects requests that have multiple arguments with the same name indicative of an HPP attack.</td>
</tr>
<tr>
<td>911100</td>
<td>Restrict HTTP Request Methods</td>
<td>Allows only request methods specified by the configurable &quot;Allowed http methods&quot; parameter.</td>
</tr>
<tr>
<td>920100</td>
<td>Invalid HTTP Request Line</td>
<td>Detects an invalid HTTP request line.</td>
</tr>
<tr>
<td>920280</td>
<td>Missing/Empty Host Header</td>
<td>Detects a missing/empty host header.</td>
</tr>
<tr>
<td>920350</td>
<td>Invalid HTTP Request Line</td>
<td>Detects invalid HTTP request lines.</td>
</tr>
<tr>
<td>941100</td>
<td>Cross-Site Scripting (XSS) Attempt: Libinjection - XSS Detection</td>
<td>Detects XSS Libinjection attempt.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>941101</td>
<td>Cross-Site Scripting (XSS) Attempt: SS Attack Detected via libinjection</td>
<td>Detects an SS attack via libinjection.</td>
</tr>
<tr>
<td>941110</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 1</td>
<td>Detects script tag based XSS vectors, for example, <code>&lt;script&gt; alert(1)&lt;/script&gt;</code>.</td>
</tr>
<tr>
<td>941120</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 2</td>
<td>Detects XSS vectors making use of event handlers like onerror, onload etc, for example, <code>&lt;body onload=&quot;alert(1)&quot;&gt;</code>.</td>
</tr>
<tr>
<td>941130</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 3</td>
<td>Detects XSS vectors making use of attribute vectors.</td>
</tr>
<tr>
<td>941140</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 4</td>
<td>Detects XSS vectors making use of javascript URI and tags, for example, <code>&lt;p style=&quot;background:url(javascript:alert(1))&quot;&gt;</code>.</td>
</tr>
<tr>
<td>941150</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters - Category 5</td>
<td>Detects HTML attributes - <code>src</code>, <code>style</code> and <code>href</code>.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>941180</td>
<td>Cross-Site Scripting (XSS) Attempt: Blacklist Keywords from Node-Validator</td>
<td>Detects Blacklist Keywords from Node-Validator.</td>
</tr>
<tr>
<td>941190</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941200</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941210</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941220</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941230</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941240</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941250</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>941260</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941270</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941280</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941300</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941320</td>
<td>Cross-Site Scripting (XSS) Attempt: HTML Tag Handler</td>
<td>Cross-Site Scripting (XSS) Attempt: HTML Tag Handler</td>
</tr>
<tr>
<td>941330</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>941340</td>
<td>Cross-Site Scripting (XSS) Attempt: XSS Filters from Internet Explorer</td>
<td>Detects XSS Filters from IE.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>941350</td>
<td>Cross-Site Scripting (XSS) Attempt: UTF-7 encoding XSS filter evasion for IE</td>
<td>Cross-Site Scripting (XSS) Attempt: UTF-7 encoding XSS filter evasion for IE.</td>
</tr>
<tr>
<td>950002</td>
<td>Common System Command Access Attempt</td>
<td>Detects access attempts to common system commands, such as map, telnet, ftp, rcmd, cmd.</td>
</tr>
<tr>
<td>950005</td>
<td>Common System Files Access Attempt</td>
<td>Detects access attempts to common system files, such as access, passwd, groupm global.asa, httpd.conf, boot.ini, /etc.</td>
</tr>
<tr>
<td>950006</td>
<td>Injection for Common System Commands</td>
<td>Detects injections for common system commands such as telnet, map, biocalgroup, ftp, rcmd, echo, cmd, chmod, passwd, mail.</td>
</tr>
<tr>
<td>950007</td>
<td>Blind SQL Injection</td>
<td>Detects common blind SQL injection attacks.</td>
</tr>
<tr>
<td>950009</td>
<td>Session Fixation</td>
<td>Detects Session Fixation, an attack technique that forces a user's session ID to an explicit value. Depending on the functionality of the target website, a number of techniques can be utilized to &quot;fix&quot; the session ID value. These techniques range from Cross-site Scripting exploits to peppering the website with previously made HTTP requests. After a user's session ID has been fixed, the attacker will wait for that user to log in. Once the user does so, the attacker uses the predefined session ID value to assume the same online identity.</td>
</tr>
<tr>
<td>950010</td>
<td>LDAP Injection</td>
<td>Detects common LDAP data constructions injections.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>950011</td>
<td>SSI Injection</td>
<td>Detects common Server-Side-Include format data injections.</td>
</tr>
<tr>
<td>950012</td>
<td>HTTP Request Smuggling</td>
<td>Detects specially crafted requests that under certain circumstances could be seen by the attacked entities as two different sets of requests. This allows certain requests to be smuggled through to a second entity without the first one realizing it.</td>
</tr>
<tr>
<td>950018</td>
<td>UPDF XSS Injection</td>
<td>Detects submitted links that contain the # fragment in a query_string.</td>
</tr>
<tr>
<td>950019</td>
<td>Email Injection</td>
<td>Detects mail command injections targeting mail servers and webmail applications that construct IMAP/SMTP statements from user-supplied input that is not properly sanitized.</td>
</tr>
<tr>
<td>950103</td>
<td>Path/Directory Traversal</td>
<td>Detects path traversal attempts, also known as directory traversal or &quot;../&quot; attacks.</td>
</tr>
<tr>
<td>950107</td>
<td>URL Encodings Validation</td>
<td>Detects URL encoding inconsistencies, encoding abuse, and invalid formatting.</td>
</tr>
<tr>
<td>950110</td>
<td>Trojan, Backdoor, and Webshell Access Attempts</td>
<td>Detects when an attacker attempts to access trojan, backdoor, or webshell web page.</td>
</tr>
<tr>
<td>950116</td>
<td>Unicode Encoding/Decoding Validation</td>
<td>Blocks full-width Unicode encoding as decoding evasions could be possible.</td>
</tr>
<tr>
<td>950117</td>
<td>URL Contains an IP Address</td>
<td>Detects a common RFI attack, when a URL contains an IP address.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>950118</td>
<td>PHP Include() Function</td>
<td>Detects a common RFI php include() function attacks.</td>
</tr>
<tr>
<td>950119</td>
<td>Data Ends with Question Mark (s) (?)</td>
<td>Detects a common RFI attack, when data ends with question mark(s) (?).</td>
</tr>
<tr>
<td>950120</td>
<td>Host Doesn't Match Localhost</td>
<td>Detects a common RFI attack, when host doesn't match localhost.</td>
</tr>
<tr>
<td>950801</td>
<td>UTF Encoding Validation</td>
<td>Detects UTF encoding inconsistencies and invalid formatting.</td>
</tr>
<tr>
<td>950907</td>
<td>OS Command Injection</td>
<td>Detects OS command injection in an application to elevate privileges, execute arbitrary commands, compromise the underlying operating system and install malicious toolkits such as those to participate in botnet attacks.</td>
</tr>
<tr>
<td>950910</td>
<td>HTTP Response Splitting</td>
<td>Detects Carriage Return + Linefeed characters in the response header that could cause attacked entities to interpret it as two separate responses instead of one.</td>
</tr>
<tr>
<td>958000</td>
<td>Addimport XSS Attack</td>
<td>Detects usage of addimport in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958001</td>
<td>document Cookie XSS Attack</td>
<td>Detects usage of document.cookie in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958002</td>
<td>execscript XSS Attack</td>
<td>Detects usage of execscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958003</td>
<td>fromcharcode XSS Attack</td>
<td>Detects usage of fromcharcode in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958004</td>
<td>innerhtml XSS Attack</td>
<td>Detects usage of innerhtml in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958005</td>
<td>cdata XSS Attack</td>
<td>Detects usage of cdata in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958006</td>
<td>body background XSS Attack</td>
<td>Detects usage of &lt;body background in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958007</td>
<td>onload XSS Attack</td>
<td>Detects usage of onload in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958008</td>
<td>input type image XSS Attack</td>
<td>Detects usage of &lt;input type image in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958009</td>
<td>import XSS Attack</td>
<td>Detects usage of import in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958010</td>
<td>activexobject XSS Attack</td>
<td>Detects usage of activexobject in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958011</td>
<td>background-image: XSS Attack</td>
<td>Detects usage of background-image: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958012</td>
<td>copyparentfolder XSS Attack</td>
<td>Detects usage of copyparentfolder in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958013</td>
<td>createtextrange XSS Attack</td>
<td>Detects usage of createtextrange in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958016</td>
<td>getparentfolder XSS Attack</td>
<td>Detects usage of getparentfolder in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958017</td>
<td>getspecialfolder XSS Attack</td>
<td>Detects usage of getspecialfolder in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958018</td>
<td>href javascript: XSS Attack</td>
<td>Detects usage of href javascript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958019</td>
<td>href schell XSS Attack</td>
<td>Detects usage of href schell in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958020</td>
<td>href vbscript: XSS Attack</td>
<td>Detects usage of href vbscript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958022</td>
<td>livescript: XSS Attack</td>
<td>Detects usage of livescript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958023</td>
<td>lows rc javascript: XSS Attack</td>
<td>Detects usage of lows rc javascript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958024</td>
<td>lows rc shell XSS Attack</td>
<td>Detects usage of lows rc shell in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958025</td>
<td>lows rc vbscript XSS Attack</td>
<td>Detects usage of lows rc vbscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958026</td>
<td>mocha: XSS Attack</td>
<td>Detects usage of mocha: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958027</td>
<td>onabort XSS Attack</td>
<td>Detects usage of onabort in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958028</td>
<td>settimeout XSS Attack</td>
<td>Detects usage of settimeout in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958030</td>
<td>src http: XSS Attack</td>
<td>Detects usage of src http: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958031</td>
<td>javascript: XSS Attack</td>
<td>Detects usage of javascript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958032</td>
<td>src and shell XSS Attack</td>
<td>Detects usage of src and shell in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958033</td>
<td>vbscript: XSS Attack</td>
<td>Detects usage of vbscript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958034</td>
<td>style bexpression XSS Attack</td>
<td>Detects usage of style bexpression in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958036</td>
<td>type application x-javascript XSS Attack</td>
<td>Detects usage of type application x-javascript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958037</td>
<td>type application x-vbscript XSS Attack</td>
<td>Detects usage of type application x-vbscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958038</td>
<td>type text ecmascript XSS Attack</td>
<td>Detects usage of type text ecmascript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958039</td>
<td>type text javascript XSS Attack</td>
<td>Detects usage of type text javascript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958040</td>
<td>type text jscript XSS Attack</td>
<td>Detects usage of type text jscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958041</td>
<td>type text vbscript XSS Attack</td>
<td>Detects usage of type text vbscript in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958045</td>
<td>url javascript: XSS Attack</td>
<td>Detects usage of url javascript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958046</td>
<td>url shell XSS Attack</td>
<td>Detects usage of url shell in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958047</td>
<td>url vbscript: XSS Attack</td>
<td>Detects usage of url vbscript: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958049</td>
<td>?meta XSS Attack</td>
<td>Detects usage of ?meta in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958051</td>
<td>?script XSS Attack</td>
<td>Detects usage of &lt; ?script in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958052</td>
<td>alert XSS Attack</td>
<td>Detects usage of alert in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958054</td>
<td>lowsrc and http: XSS Attack</td>
<td>Detects usage of lowsrc and http: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958056</td>
<td>iframe src XSS Attack</td>
<td>Detects usage of iframe src in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958057</td>
<td>?iframe XSS Attack</td>
<td>Detects usage of ?iframe in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958059</td>
<td>asfunction: XSS Attack</td>
<td>Detects usage of asfunction: in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958291</td>
<td>Range Header Validation</td>
<td>Detects range header inconsistencies and invalid formatting.</td>
</tr>
<tr>
<td>958295</td>
<td>Connection Header Validation</td>
<td>Detects connection header inconsistencies and invalid formatting.</td>
</tr>
<tr>
<td>958404</td>
<td>onerror XSS Attack</td>
<td>Detects usage of onerror in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958405</td>
<td>onblur XSS Attack</td>
<td>Detects usage of onblur in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958406</td>
<td>onchange XSS Attack</td>
<td>Detects usage of onchange in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958407</td>
<td>onclick XSS Attack</td>
<td>Detects usage of onclick in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958408</td>
<td>ondragdrop XSS Attack</td>
<td>Detects usage of ondragdrop in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958409</td>
<td>onfocus XSS Attack</td>
<td>Detects usage of onfocus in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958410</td>
<td>onkeydown XSS Attack</td>
<td>Detects usage of onkeydown in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958411</td>
<td>onkeypress XSS Attack</td>
<td>Detects usage of onkeypress in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958412</td>
<td>onkeyup XSS Attack</td>
<td>Detects usage of onkeyup in request, cookies, or arguments.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>958413</td>
<td>onload XSS Attack</td>
<td>Detects usage of onload in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958414</td>
<td>onmousedown XSS Attack</td>
<td>Detects usage of onmousedown in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958415</td>
<td>onmousemove XSS Attack</td>
<td>Detects usage of onmousemove in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958416</td>
<td>bonmouseout XSS Attack</td>
<td>Detects usage of bonmouseout in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958417</td>
<td>bonmouseover XSS Attack</td>
<td>Detects usage of bonmouseover in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958418</td>
<td>onmouseup XSS Attack</td>
<td>Detects usage of onmouseup in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958419</td>
<td>onmove XSS Attack</td>
<td>Detects usage of onmove in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958420</td>
<td>onresize XSS Attack</td>
<td>Detects usage of onresize in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958421</td>
<td>onselect XSS Attack</td>
<td>Detects usage of onselect in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958422</td>
<td>onsubmit XSS Attack</td>
<td>Detects usage of onsubmit in request, cookies, or arguments.</td>
</tr>
<tr>
<td>958423</td>
<td>onunload XSS Attack</td>
<td>Detects usage of onunload in request, cookies, or arguments.</td>
</tr>
</tbody>
</table>
## CHAPTER 9 Web Application Firewall

<table>
<thead>
<tr>
<th>Rule ID/Key</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>959151</td>
<td>php Code Injection</td>
<td>Detects a common injections attack, when request contain any php code e.g. &quot;&lt;?&gt;&quot;.</td>
</tr>
<tr>
<td>960000</td>
<td>File Name Validation</td>
<td>Detects multipart/form-data file name evasion attempts.</td>
</tr>
<tr>
<td>960007</td>
<td>Missing Host Header</td>
<td>Detects missing request host header.</td>
</tr>
<tr>
<td>960009</td>
<td>Missing User-Agent Header</td>
<td>Detects missing request user-agent header.</td>
</tr>
<tr>
<td>960011</td>
<td>GET/HEAD Requests Validation</td>
<td>Detects if GET/HEAD requests contain request body since it is not a common practice.</td>
</tr>
<tr>
<td>960012</td>
<td>Content-Length Header Validation</td>
<td>Detects if content-length header is provided with every POST request.</td>
</tr>
<tr>
<td>960013</td>
<td>Require Content-Length to be provided with every HTTP/1.1 POST request that has no Transfer-Encoding header</td>
<td>Detects HTTP/1.1 requests that do not comply with HTTP 1.1 spec by having no content-length header when transfer-encoding is also absent.</td>
</tr>
<tr>
<td>960014</td>
<td>URI Validation</td>
<td>Ensures that URI and canonical server name are matching.</td>
</tr>
<tr>
<td>960015</td>
<td>Missing Accept Header</td>
<td>Detects missing request accept header.</td>
</tr>
<tr>
<td>960016</td>
<td>Content-Length Header Validation</td>
<td>Detects if content-length HTTP header is not numeric.</td>
</tr>
<tr>
<td>960017</td>
<td>Host Header Is IP Address</td>
<td>Detects if host header is a numeric IP address as it could be indicative of automated client access.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>960020</td>
<td>Pragma Header Validation</td>
<td>Ensures that pragma, cache-control headers and HTTP protocol version supplied by the client are matching.</td>
</tr>
<tr>
<td>960022</td>
<td>Expect Header Validation</td>
<td>Ensures that expect header and HTTP protocol version supplied by the client are matching.</td>
</tr>
<tr>
<td>960024</td>
<td>Repeatative Non-Word Chars</td>
<td>Attempts to identify when 4 or more non-word characters are repeated in sequence.</td>
</tr>
<tr>
<td>960208</td>
<td>Values Limits</td>
<td>Detects HTTP requests with value length exceeding the configurable &quot;Max length of argument&quot; parameter.</td>
</tr>
<tr>
<td>960209</td>
<td>Arguments Limits</td>
<td>Detects HTTP requests with argument name length exceeding the 100 symbols.</td>
</tr>
<tr>
<td>960335</td>
<td>Number of Arguments Limits</td>
<td>Detects HTTP requests with number of arguments exceeding the configurable &quot;Max amount of arguments&quot; value.</td>
</tr>
<tr>
<td>960341</td>
<td>Total Arguments Limits</td>
<td>Detects HTTP requests with total length of all arguments exceeding the configurable &quot;Max total argument length&quot; parameter.</td>
</tr>
<tr>
<td>960901</td>
<td>Character Set Validation</td>
<td>Ensures that only a specific character set(s) is used.</td>
</tr>
<tr>
<td>960902</td>
<td>Content-Encoding Header Validation</td>
<td>Ensures that identity is not specified in content-encoding header.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>960904</td>
<td>Missing Content-Type Header</td>
<td>Detects missing content-type header or if combination of content-length and content-type headers is invalid.</td>
</tr>
<tr>
<td>960911</td>
<td>Request Line Format Validation Against the HTTP RFC</td>
<td>Uses rule negation against the regex for positive security. The regex specifies the proper construction of URI request lines such as: &quot;http:&quot; &quot;//&quot; host [ &quot;:&quot; port ] [ abs_path [ &quot;:&quot; query ]]. It also outlines proper construction for CONNECT, OPTIONS, and GET requests.</td>
</tr>
<tr>
<td>960912</td>
<td>Malformed request bodies</td>
<td>Checks for request body parsing errors.</td>
</tr>
<tr>
<td>960914</td>
<td>Strict Multipart Parsing Checks</td>
<td>Uses strict checks for what is accepted in the multipart/form-data request body. If the rule proves to be too strict for your environment consider changing it to Off.</td>
</tr>
<tr>
<td>960915</td>
<td>Multipart Unmatched Boundary Check</td>
<td>Checks for signs of evasions during file upload requests.</td>
</tr>
<tr>
<td>970002</td>
<td>Statistics Pages Information Leakage</td>
<td>Detects statistics pages information leakage.</td>
</tr>
<tr>
<td>970003</td>
<td>SQL Errors Information Leakage</td>
<td>Detects SQL errors information leakage.</td>
</tr>
<tr>
<td>970004</td>
<td>IIS Errors Information Leakage</td>
<td>Detects IIS errors information leakage.</td>
</tr>
<tr>
<td>970007</td>
<td>Zope Information Leakage</td>
<td>Detects Zope information leakage.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>970008</td>
<td>ColdFusion Information Leakage</td>
<td>Detects ColdFusion information leakage.</td>
</tr>
<tr>
<td>970009</td>
<td>PHP Information Leakage</td>
<td>Detects PHP information leakage.</td>
</tr>
<tr>
<td>970010</td>
<td>ISA Server Existence Revealed</td>
<td>Detects if ISA server existence is revealed.</td>
</tr>
<tr>
<td>970011</td>
<td>File and/or Directory Names Leakage</td>
<td>Detects file and/or directory names leakage.</td>
</tr>
<tr>
<td>970012</td>
<td>MS Office Document Properties Leakage</td>
<td>Detects MS Office document properties leakage.</td>
</tr>
<tr>
<td>970013</td>
<td>Directory Listing Information Leakage</td>
<td>Detects directory listing information leakage.</td>
</tr>
<tr>
<td>970014</td>
<td>ASP/JSP Source Code Leakage</td>
<td>Detects ASP/JSP source code leakage.</td>
</tr>
<tr>
<td>970015</td>
<td>PHP Source Code Leakage</td>
<td>Detects PHP source code leakage.</td>
</tr>
<tr>
<td>970016</td>
<td>ColdFusion Source Code Leakage</td>
<td>Detects ColdFusion source code leakage.</td>
</tr>
<tr>
<td>970018</td>
<td>IIS Default Location Revealed</td>
<td>Detects if IIS default location is revealed.</td>
</tr>
<tr>
<td>970021</td>
<td>Weblogic Information Leakage</td>
<td>Detects Weblogic information leakage.</td>
</tr>
<tr>
<td>970118</td>
<td>Microsoft OLE DB Provider Error Page Leakage</td>
<td>Detects Microsoft OLE DB Provider for SQL Server error page.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>970901</td>
<td>5XX Status Code Information Leakage</td>
<td>Detects if an application generates 500-level status code. For example, 500 Internal Server Error, 501 Not Implemented...505 HTTP Version Not Supported.</td>
</tr>
<tr>
<td>973300</td>
<td>Common Direct HTML Injection</td>
<td>Detects tags that are the most common direct HTML injection points.</td>
</tr>
<tr>
<td>973306</td>
<td>Embedded JavaScript in Style Attribute</td>
<td>Detects embedded JavaScript in style attribute.</td>
</tr>
<tr>
<td>973307</td>
<td>Embedded Scripts Within JavaScript Fragments</td>
<td>Detects common JavaScript fragments like fromcharcode, alert, eval that can be used for attacks.</td>
</tr>
<tr>
<td>973309</td>
<td>CSS Fragments Attacks</td>
<td>Detects common CSS fragments attacks like &lt;div style=&quot;background-image: url(java- script:...)&quot;&gt; or &lt;img style=&quot;x:expression(document.write(1))&quot;&gt;.</td>
</tr>
<tr>
<td>973310</td>
<td>Embedded Scripts Within Alert Fragments</td>
<td>Detects attacks like alert('xss'), alert(&quot;xss&quot;), alert(/xss/).</td>
</tr>
<tr>
<td>973312</td>
<td>&quot;;</td>
<td>--&quot;&lt;XSS&gt;==&amp;{()} Attacks</td>
</tr>
<tr>
<td>973313</td>
<td>&amp;{alert('xss')} Attacks</td>
<td>Detects &amp;{alert('xss')} attacks.</td>
</tr>
<tr>
<td>973314</td>
<td>Doctype Entity Inject</td>
<td>Detects Doctype Entity inject attacks.</td>
</tr>
<tr>
<td>973331</td>
<td>Internet Explorer XSS Filters</td>
<td>Detects common IE XSS attacks.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 973336     | Embedding Scripts Within Scripts     | Detects script tag based XSS vectors. For example, `<script> alert(1)</script>`.
| 973337     | Embedded Scripts Within Event Handlers | Detects event handler based XSS vectors. For example, `<body onload="alert(1)">`.
| 973338     | Embedded Scripts Within URI Schemes  | Detects "data", "javascript", "src" or other URI schemes/attributes based XSS vectors. For example, `<p style="background:url(javascript:alert(1))">`.
<p>| 981004     | Potential Obfuscated Javascript, fromCharCode | Detects excessive fromCharCode JavaScript in output.                                           |
| 981005     | Potential Obfuscated Javascript, Eval+Unescape | Detects potential Eval+Unescape in response.                                                                                               |
| 981006     | Potential Obfuscated Javascript, Unescape | Detects potential Unescape in response.                                                                                                     |
| 981007     | Potential Obfuscated Javascript, Heap Spray | Detects potential Heap Spray in response.                                                                                                   |
| 981136     | Generic XSS Attacks                  | Detects common XSS attacks embedded within non-script elements. For example, jscript onsubmit copyparentfolder document javascript meta onchange onmove onkeydown onkeyup activexobject onerror onmouseover ecmaexpression onmouseover vbscript. |</p>
<table>
<thead>
<tr>
<th>Rule ID/Key</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>981172</td>
<td>SQL Character Anomaly Scoring</td>
<td>Attempts to gauge when there is an excessive use of meta-characters within a single parameter payload.</td>
</tr>
<tr>
<td>981177</td>
<td>IFrame Injection</td>
<td>Detects iframe injections that could execute malicious code to steal data, redirect to malware infected sites, load malware, etc.</td>
</tr>
<tr>
<td>981227</td>
<td>Request URI Validation</td>
<td>Detects invalid URI in request.</td>
</tr>
<tr>
<td>981242</td>
<td>Classic SQL Injection Probings</td>
<td>Detects classic SQL injection probings.</td>
</tr>
<tr>
<td>981244</td>
<td>SQL Authentication Bypass Attempts</td>
<td>Detects basic SQL authentication bypass attempts.</td>
</tr>
<tr>
<td>981245</td>
<td>SQL Authentication Bypass Attempts</td>
<td>Detects basic SQL authentication bypass attempts.</td>
</tr>
<tr>
<td>981246</td>
<td>SQL Authentication Bypass Attempts</td>
<td>Detects basic SQL authentication bypass attempts.</td>
</tr>
<tr>
<td>981272</td>
<td>SQL Injection Using sleep() or benchmark()</td>
<td>Detects blind SQL injection tests using sleep() or benchmark() functions.</td>
</tr>
<tr>
<td>981300</td>
<td>SQL Keyword Anomaly Scoring</td>
<td>Detects common SQL keywords anomalies.</td>
</tr>
<tr>
<td>981318</td>
<td>String Termination/Statement Ending</td>
<td>Identifies common initial SQLi probing requests where attackers insert/append quote characters to the existing normal payload to see how the app/db responds.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>1000000</td>
<td>Shellshock Exploit Attempt</td>
<td>Detects the ability to unintentionally execute commands in Bash (CVE-2014-6271).</td>
</tr>
<tr>
<td>2100019</td>
<td>/_layouts/scriptresx.ashx sections Parameter XSS</td>
<td>Detects Microsoft SharePoint /_layouts/scriptresx.ashx sections parameter XSS attacks.</td>
</tr>
<tr>
<td>2100023</td>
<td>/owssrv.dll List Parameter XSS</td>
<td>Detects Microsoft SharePoint /owssrv.dll List Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100026</td>
<td>/_layouts/Chart/WebUI/WizardList.aspx skey Parameter XSS</td>
<td>Detects Microsoft SharePoint /_layouts/Chart/WebUI/WizardList.aspx skey Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100027</td>
<td>/_layouts/themeweb.aspx XSS</td>
<td>Detects Microsoft SharePoint /_layouts/themeweb.aspx ctl00$PlaceHolderMain$ctl82$customizeThemeSection$accent6 Parameter XSS attacks.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>2100032</td>
<td>owssrv.dll View Parameter XSS</td>
<td>Detects Microsoft SharePoint owssrv.dll View Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100033</td>
<td>NewForm.aspx TextField_spSave Parameter XSS</td>
<td>Detects Microsoft SharePoint NewForm.aspx TextField_spSave Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100034</td>
<td>/Lists/Calendar/calendar.aspx CalendarDate Parameter XSS</td>
<td>Detects Microsoft SharePoint /Lists/Calendar/calendar.aspx CalendarDate Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100035</td>
<td>_layouts/Picker.aspx XSS</td>
<td>Detects Microsoft SharePoint _layouts/Picker.aspx ctl00$PlaceHolder-DialogBodySection$ctl04$hiddenSpanData Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100048</td>
<td>_layouts/help.aspx cid0 Parameter XSS</td>
<td>Detects Microsoft SharePoint _layouts/help.aspx cid0 Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100062</td>
<td>_layouts/ScriptResx.ashx name Parameter LFI</td>
<td>Detects Microsoft SharePoint _layouts/ScriptResx.ashx name Parameter LFI attacks.</td>
</tr>
<tr>
<td>2100063</td>
<td>_layouts/OSSSearchResults.aspx k Parameter XSS</td>
<td>Detects Microsoft SharePoint _layouts/OSSSearchResults.aspx k Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100069</td>
<td>wiki pages multiple Parameter XSS</td>
<td>Detects Microsoft SharePoint wiki pages multiple Parameter XSS (CVE-2013-3180) attacks.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>2100070</td>
<td>/Lists/Links/AllItems.aspx XSS</td>
<td>Detects Microsoft SharePoint /Lists/Links/AllItems.aspx ctl00$m$g_2085a7 32_4692_4d3e_99d2_4d90ea5108d2$ctl00$ctl05$ctl00$ctl00$ctl00$ctl00$urlFieldUrl Parameter XSS attacks.</td>
</tr>
<tr>
<td>2100082</td>
<td>Drupal - pre-auth SQL Injection Vulnerability</td>
<td>Detects Drupal pre-auth SQL injection vulnerability. A malicious user can inject arbitrary SQL queries and thereby control the complete Drupal site. This leads to a code execution as well. Drupal 7.32 fixed this bug.</td>
</tr>
<tr>
<td>2100083</td>
<td>Gerber WebPDM XSS Vulnerability</td>
<td>Detects cross-site scripting vulnerability in Gerber WebPDM Product Data Management System.</td>
</tr>
<tr>
<td>2100084</td>
<td>Gerber WebPDM SQL Injection Vulnerability</td>
<td>Detects SQL Injection Vulnerability in Gerber WebPDM Product Data Management System.</td>
</tr>
<tr>
<td>2100085</td>
<td>High X-SharePointHealthScore</td>
<td>Detects Microsoft SharePoint High X-SharePointHealthScore - potential DoS attack-availability risk.</td>
</tr>
<tr>
<td>2100086</td>
<td>Response Header Found</td>
<td>Detects Microsoft SharePoint SharePointError Response Header Found.</td>
</tr>
<tr>
<td>2100087</td>
<td>x-virus-infected Response Header Found</td>
<td>Detects x-virus-infected Response Header Found.</td>
</tr>
<tr>
<td>2100088</td>
<td>Rights Management (IRM) Error Response Header Found</td>
<td>Detects Microsoft SharePoint Information Rights Management (IRM) Error Response Header Found.</td>
</tr>
</tbody>
</table>
## CHAPTER 9 Web Application Firewall

<table>
<thead>
<tr>
<th>Rule ID/Key</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2200924</td>
<td>IRC Botnet Attacks</td>
<td>Detects common IRC Botnet attack commands.</td>
</tr>
<tr>
<td>2200925</td>
<td>Detects HOIC DoS Tool Requests</td>
<td>Detects HOIC DoS tool requests.</td>
</tr>
<tr>
<td>2250117</td>
<td>Common RFI Attacks</td>
<td>Detects common types of Remote File Inclusion (RFI) attacks.</td>
</tr>
<tr>
<td>2250120</td>
<td>Local File Inclusion Attacks</td>
<td>Detects common local file inclusion attacks like <code>my $dir = &quot;../../../../../../../../../../../&quot;;</code> or <code>&quot;http://&quot;.$site.$bug.$dir.&quot;/proc/self/environ%0000&quot;;</code>.</td>
</tr>
<tr>
<td>2250121</td>
<td>Local File Inclusion ENV Attack in User-Agent</td>
<td>Detects Local File Inclusion ENV Attack in User-Agent</td>
</tr>
<tr>
<td>2250122</td>
<td>PHP Injection Attack</td>
<td>Detects common php injection attacks like <code>&quot;send-contactus=1&amp;author_name=[php]eval(base64_decode(&quot;$.code.'&quot;'))%3Bdie%28%29%3B%5B%2Fphp-%5D&quot;</code></td>
</tr>
</tbody>
</table>
## CHAPTER 9 Web Application Firewall

<table>
<thead>
<tr>
<th>Rule ID/Key</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2250123</td>
<td>XML-RPC PHP Injection Attack</td>
<td>Detects common XML-RPC PHP Injections like $exploit .= &quot;echo'j13mb0t';&quot;.$code.&quot;echo'j13mb0t';exit;/*-&lt;name&gt;&lt;/value&gt;&lt;/param&gt;&lt;/params&gt;&lt;/methodCall&gt;&quot;;</td>
</tr>
<tr>
<td>2250125</td>
<td>osCommerce File Upload</td>
<td>Detects osCommerce file upload attacks like &quot;http://&quot;.$site.&quot;admin/file_manager.php/login.php&quot;;</td>
</tr>
<tr>
<td>2250127</td>
<td>e107 Plugin my_gallery Exploit</td>
<td>Detects e107 Plugin my_gallery Exploit &quot;http://&quot;.$site.&quot;e107_plugins/my_gallery/image.php?file=././e107_config.php&quot;.</td>
</tr>
<tr>
<td>2250128</td>
<td>Opencart Remote File Upload Vulnerability</td>
<td>Detects Opencart remote file upload vulnerability.</td>
</tr>
<tr>
<td>2250129</td>
<td>Zen Cart Local File Disclosure Vulnerability</td>
<td>Detects Zen Cart local file disclosure vulnerability.</td>
</tr>
<tr>
<td>201821375</td>
<td>CVE-2012-0209, Remote Execution Backdoor Attempt Against Horde</td>
<td>Detects remote execution backdoor attempt against Horde.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>201822063</td>
<td>CVE-2012-1823, CVE-2012-2311, CVE-2012-2335, CVE-2012-2336, PHP-CGI Remote File Include Attempt</td>
<td>Detects PHP-CGI remote file include attempts.</td>
</tr>
<tr>
<td>Rule ID/Key</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
</tbody>
</table>

**WAF Settings**

WAF Settings for the entire ruleset are managed from this dashboard. Block actions can be further defined in terms of response code, redirect, allowed HTTP methods, response body inspection, and more. The WAF Settings dashboard defines the parameters for enforcement any time a WAF rule is triggered.
The following table displays the parameters that can be configured.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block action</td>
<td>The action taken on malicious requests blocked by WAF. Options include: <strong>Response code</strong> or <strong>Block page</strong>.</td>
</tr>
<tr>
<td>Block response code</td>
<td>The response code to set to blocked requests. It is recommended that this option be set to <strong>403 Forbidden</strong>.</td>
</tr>
</tbody>
</table>
### Parameter | Description
---|---
Max amount of arguments | The maximum number of allowed arguments for HTTP policy rules. It is recommended that this option be set to **255**.
Max length of an argument | The maximum length of an argument used by HTTP policy rules. It is recommended that this option be set to **400** symbols.
Max total argument length | The maximum argument length for all arguments used at HTTP policy rules. It is recommended that this option be set to **64000** symbols.
Recommendations period | The period in days to analyze for recommended actions. It is recommended that this option be set to a period of **10 or 30** days.
Allowed HTTP methods | The list of allowed HTTP methods, which are used by HTTP policy rules. The most used options are GET, HEAD, POST, PUT, DELETE.
Enable response body inspection | Enable or Disable WAF rules related to HTTP response data.

---

**Transferring Web Application Security WAF to Oracle Cloud Infrastructure WAF**

Use the instructions below to transfer your Web Application Security WAF service to Oracle Cloud Infrastructure WAF.

**Sign Up for an Oracle Cloud Account**

Before transferring your Web Application Security WAF, you need to sign up for an Oracle Cloud account. For more information about signing up for a free Oracle Cloud account, see [Sign Up for the Free Oracle Cloud Promotion](#).

1. Visit the [account signup page](#).
2. Enter the necessary information.
You will receive a "Get Started with Oracle Cloud" email within 15 minutes with your credentials that you will use to log into your account. You can use the $300 promotional credit you receive to run your WAF service. For information about getting started with Oracle Cloud Infrastructure, see Welcome to Oracle Cloud Infrastructure.

Upgrade Your Oracle Cloud Infrastructure Account

Upgrading is required in order to continue your WAF service after the 30 day promotional period is over. If not, your WAF services (and any other Oracle Cloud services) will be deactivated.

To upgrade your account

1. Open the navigation menu. Under Governance and Administration, go to Billing and click Payment Method to upgrade to a paid (Pay As You Go) account and continue your service post-trial.
2. Select and confirm the Pay As You Go option. You will be billed monthly based on Oracle’s price list and your actual usage of cloud services. For more information about Pay As You Go, see Upgrade to Pay As You Go. For information about WAF service limits, see Service Limits.

Contact the Oracle Dyn Migration Team with Questions

For any questions regarding steps for migration please contact migrations@dyn.com and include the following information:

- Company Name.
- Web Application Firewall Applications to be migrated.
- The OCID for your Oracle Cloud Infrastructure tenancy. See Where to Find Your Tenancy's OCID.
- Any other pertinent information or questions.
Review Existing Web Application Security Settings to Prepare for Migration

Reviewing existing WAF traffic settings is critical to a successful migration when the policies are recreated in Oracle Cloud Infrastructure. To review existing settings, refer to Web Application Firewall. Please ensure you take note of current configuration settings to be used later on upon policy creation in Oracle Cloud Infrastructure.

Route Off the Web Application Security WAF Service

Routing off the service is required in order to prevent downtime to your web application while you create your policies in OCI. To route off your WAF service, update your hostname to point to your origin. You can accomplish this by navigating to your DNS provider, removing the target CNAME for Oracle Cloud Security, and adding in your origin hostname or IP addresses directly.

Delete the Existing Web App

Use the following steps to remove the web app from your account.

To delete your web app

1. From the Administration dashboard, select Web Apps. A new window appears.
2. Click the actions icon beside the web app you want to remove. A drop-down menu appears.
3. Select Delete from the drop-down menu.
4. Type "delete" into the confirmation field, and then click YES, I understand the consequences, delete this webapp.
Create a WAF Policy in Oracle Cloud Infrastructure

To create a WAF policy

1. Open the navigation menu. Under Solutions, Platform and Edge, go to Edge Services and click WAF Policies.

2. Click Create WAF Policy.

3. In the Create WAF Policy dialog box, enter the following:
   
   - **Policy Name:** A unique name for the policy. Avoid entering confidential information.
   
   - **Domains:**
     - **Primary Domain:** The fully qualified domain name (FQDN) of the application where the policy will be applied.
     - **Additional Domains:** (Optional) Subdomains where the policy will be applied.
   
   - **WAF Origin:** The host or IP address of the public internet facing application that is being protected by the application.
     - **Origin Name:** A unique name for the origin. Avoid entering confidential information.
     - **URI:** The IPv4 address or fully qualified domain name (FQDN) of the origin. The URI can be a full URI, not just a host/IP.
     - **HTTPS Port:** The port used for secure HTTP connection. The default port is 443.
     - **HTTP Port:** The HTTP port the origin listens on. The default port is 80.
     - **Header(s):** (Optional)
       - **Header Name:** The name displayed in the HTTP request header and the header value that can be added and passed to the origin server
CHAPTER 9 Web Application Firewall

with all requests.

- **Header Value:** Specifies the data requested by the header.

- **Tags:** Optionally, you can apply tags. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure if you should apply tags, skip this option (you can apply tags later) or ask your administrator.

4. **Click Create WAF Policy.** The WAF Policy overview appears. You can access Origin Management, Access Control, WAF, Bot Management, Alerts, and any unpublished changes. While the policy is being created, no changes can be made until the process has completed. Expect the policy to become active within 15 minutes of creation.

   A CNAME target is generated for each policy. The CNAME target is a hyphenated version of your FQDN within the Oracle Cloud Infrastructure domain (for example, myapp-mydomain-com.oraclecloud.net).

5. In your DNS zone, update the CNAME record entry with the value of the CNAME target that is generated. This enables traffic to be routed through the WAF before the application. This value is presented soon after you publish your policy the first time on the main page of the policy.

For more information on managing your WAF service, see [Managing WAF Policies](#).

**Cancel Dyn Web Application Security Service**

Please send an email to [customersuccess@dyn.com](mailto:customersuccess@dyn.com) notifying Dyn that you want to cancel your accounts.
CHAPTER 10 DDoS Mitigation Manager

This chapter explains how to set up and manage DDoS Mitigation Manager.

DDoS Dashboard

The DDoS dashboard gives you an overview of alerts that have been triggered by suspicious traffic patterns to your IP prefixes. To view specific details about an alert and their various types, please see Alerts.

To save a snapshot of the current dashboard, click **Save**.

To view traffic activity data for a specific time range, select an option from the time range drop-down list. Options include:
DDoS Mitigation Manager

- **Last 6h** - (Default) Displays data for the last six hours.
- **Last 24h** - Displays data for the last 24 hours.
- **Last 2d** - Displays data for the last two days.
- **Last 7d** - Displays data for the last seven days.
- **Last 30d** - Displays data for the last 30 days.
- **Custom Range** - Select a start date and an end date within the past 30 days, and then click **Apply**.

Alerts older than 30 days will be deleted from the system.

**Alerts by Importance** - Displays the number of alerts and their level of importance over the past 30 days.

**Recent Alerts** - Displays the 10 most recent alerts, including the date, the IP address the alert was triggered from, the alert's importance, and the type of alert. For more information on types of alerts, please see **Alerts**.

**Top Alerts by IP** - The most important alerts for your IP addresses as determined by the number and severity of alerts an IP has received.

**Alerts by Profile** - Displays alerts for each network profile. For more information about profiles, please see **Profiles**.

**Traffic by Profile** - Displays traffic for each network profile. For more information about profiles, please see **Profiles**.

**IP Prefixes** - A list of your IP prefixes that are being monitored by Oracle + Dyn.

**DDoS Alerts**

In the Alerts tab, you can view and sort your alerts by various parameters, including date, profile, and alert importance.
To view traffic and alert activity for a specific time range, select an option from the time range drop-down list. Options include:

- **Last 7d** - Displays data for the last seven days.
- **Last 30d** - Displays data for the last 30 days.
- **Custom Range** - Select a start date and an end date within the past 30 days, and then click Apply.

Alerts older than 30 days will be deleted from the system.

**Filtering Alerts**

You can apply filters to sort your alerts. When you apply a filter, a tag appears at the top of the screen. Remove filters from your results by clicking the X button beside the filter you wish to remove.
**Importance** - Use the Importance filter to sort alerts by various degrees of importance. For more information about alert importance.

**IP** - Type in an IP address to add or remove from your results.

**Profile** - Filter your results by a profile of IP prefixes.

**DDoS Profiles**

DDoS network profiles allow you to group IP prefixes together to more easily monitor specific sets of prefixes, such as all of the IP prefixes for a specific data center. Profiles are built during the provisioning of the DDoS Mitigation Manager service. If you need additional profiles or changes to your current profiles, please contact support.

The Profiles view allows you to view your available network profiles and page through the IP prefixes contained within each profile.
You can find the Oracle Dyn Web Application Security Release Notes online.