



# INSTALLATION & USER GUIDE

Version 5.1

## Copyright information

Copyright © 2016 Cryptzone North America Inc. All rights reserved.

Information in this document is subject to change without notice and does not represent a commitment on the part of the vendor or its representatives. Permission to use, distribute, or copy not granted without written approval. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, without the written permission of Cryptzone North America Inc. Complying with all applicable copyright laws in the US and other countries is the responsibility of the user.

The Cryptzone logo, Security Sheriff, Compliance Sheriff, and Compliance Deputy are trademarks of Cryptzone North America Inc. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other product names mentioned herein are trademarks of their respective owners.

## Technical support

For licensing or technical support information, please submit your requests via the Cryptzone Help Center at <http://support.cryptzone.com> using your Service Cloud account. For more information, visit [www.cryptzone.com](http://www.cryptzone.com).

## Table of contents

<b>1. About Compliance Deputy</b>	<b>1</b>
<b>2. Installation and configuration</b>	<b>2</b>
2.1 Requirements	2
2.2 Installation summary	3
2.3 Compliance Deputy Configuration	3
2.4 Installing Compliance Deputy	5
2.5 Upgrading Compliance Deputy	11
<b>3. Using Compliance Deputy</b>	<b>12</b>
3.1 Scanning a page	12
3.2 Scan using a different checkpoint group	13
3.3 Scan with a different scan definition	13
3.4 Help and support	13
<b>Appendix A: Administration</b>	<b>14</b>
A.1 Allow anonymous access to scan results	14
A.2 Changing the scan timeout	14
A.3 Displaying completed Deputy scans	15
A.4 Deleting Deputy scans	15
A.5 Show Usage	16

# 1. About Compliance Deputy

Designed to work with Compliance Sheriff®, Compliance Deputy is an on-demand browser-based solution that allows developers and content providers to test and repair content prior to publishing them into the production environment. It leverages the checkpoints and rules designed in Compliance Sheriff to test page content as it is being created to ensure only compliant content is published to live sites. Address web governance issues including privacy factors like personally identifiable information (PII) and protected health information (PHI), Web accessibility, site quality, offensive content and more.

## 2. Installation and configuration

### 2.1 Requirements

- Compliance Sheriff 5.1 and above
- Compliance Deputy CAL license
- Browsers
  - Internet Explorer 9.0 and above
  - Google Chrome 40.0 and above
  - Safari 7.0 (Mac OS X 10.9) and above
  - Mozilla Firefox 38.0 and above
- Operating Systems: As per OS that supports the above Browser versions
- .Net Framework v4.0 and above.

**Note:** .Net Framework v4.5 is required if your web server does not allow clients to connect using TLS (Transport Layer Security) protocol 1.0. i.e. Connection can only be established through TLS 1.1 and/or 1.2.

#### Additional requirements

- Internet Explorer
  - Installed using the msi installer is provided
  - Enhanced Security Configuration (IE ESC) to be turned off.
- Google Chrome
  - For all clients, this is installed through the Chrome Web Store
  - Alternatively, for developers, the extension is also provided in the Compliance Deputy install zip file.
  - If Compliance Sheriff is installed and configured on a non-HTTPS environment, attempting to scan secure/HTTPS sites with Deputy may be aborted (timeout).
  - Refer to the Chrome POST-INSTALLATION section below on how this can be resolved.
- Safari (Mac)
  - Extension is provided in the zip file for manual installation.
  - Support for Safari (Mac) is limited to scanning pages that are accessible by the Compliance Sheriff worker agent. Unlike the IE and Chrome versions, the Local Scan Agent is currently NOT available for Safari (Mac) which means local content, such as CSS files referenced by the page being scanned, will not be available to the remote Worker server for processing.
- Mozilla Firefox
  - Extension is provided in the zip file for manual installation.

## 2.2 Installation summary

**Note:** If a previous version of Compliance Deputy is already installed, uninstall this version before proceeding.

To install and configure Compliance Deputy:

1. Add Compliance Deputy CALs to the Compliance Sheriff license
2. Create the Compliance Deputy configuration file
3. Install and configure Compliance Sheriff on each client for the browsers supported. Note that this process varies across the different browsers.

## 2.3 Compliance Deputy Configuration

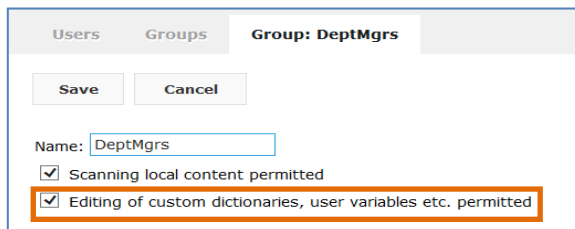
The configuration file contains information that will be used by Compliance Deputy when a scan is submitted.

- Connection details to Compliance Sheriff
- Compliance modes/Checkpoint group(s) that will be available to the user when submitting a page scan
- Scan group that the Deputy scan will belong to when created in Compliance Sheriff.

### Creating a configuration file

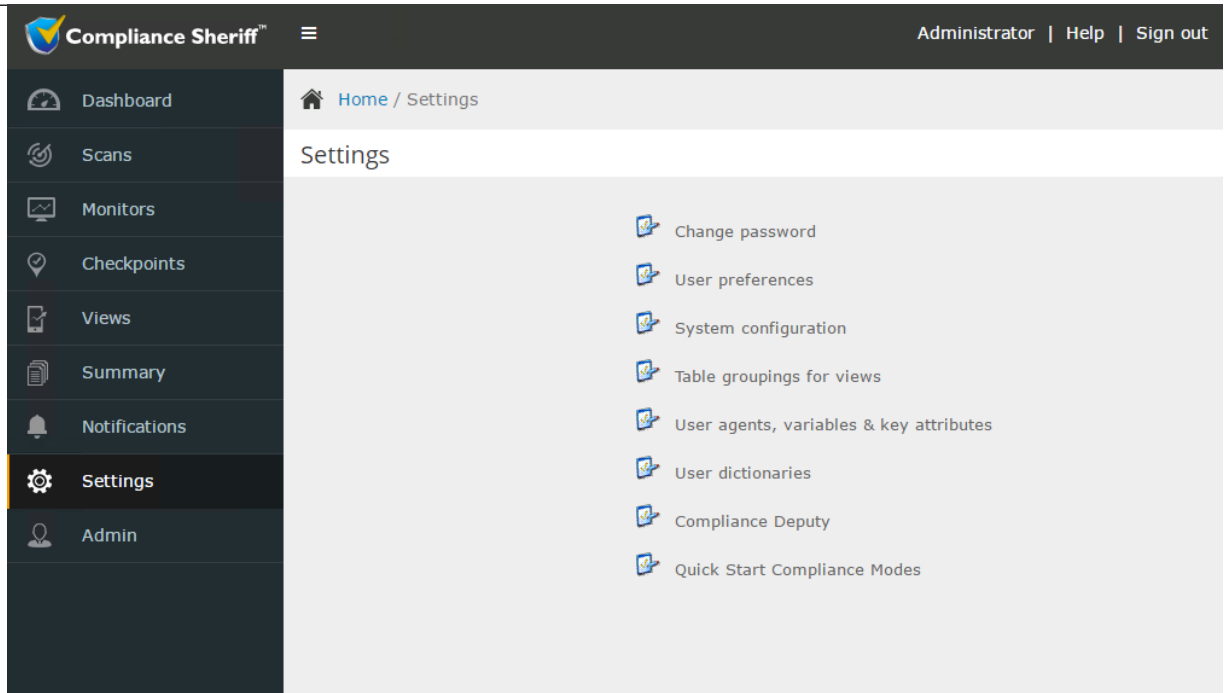
**Note:** Access to the Compliance Deputy setting requires:

- The Compliance Sheriff license includes CAL licenses for Compliance Deputy AND
- The logged in user is a member of a Compliance Sheriff group with the option “Editing of custom dictionaries, user variables etc. permitted” selected.



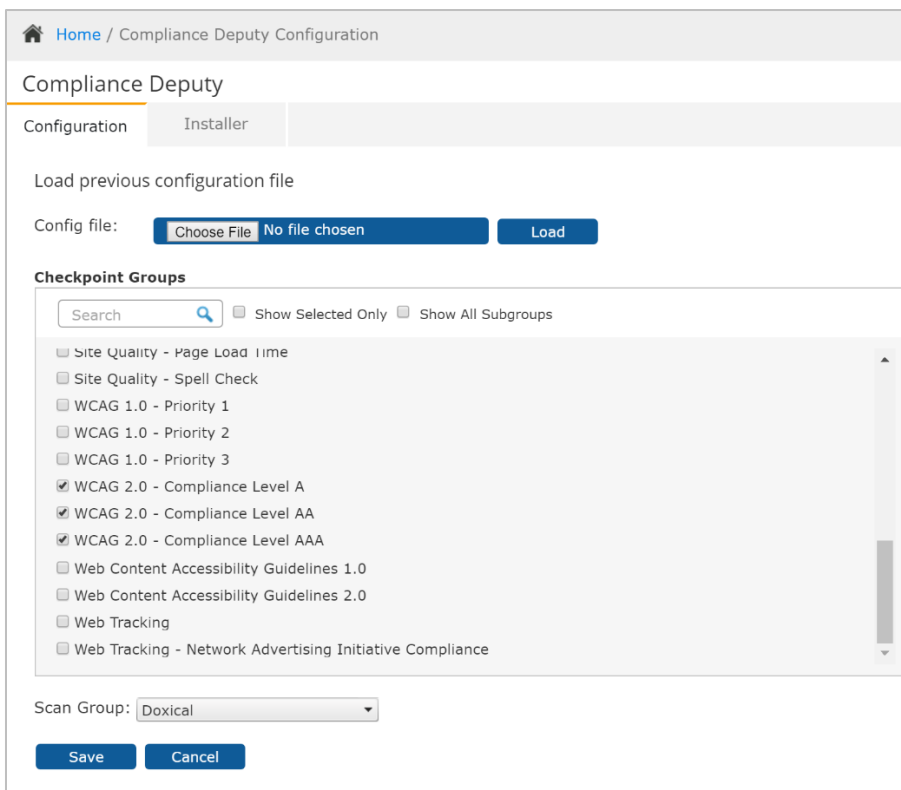
The screenshot shows the 'Groups' tab in the Compliance Sheriff interface. The group 'DeptMgrs' is selected. Below the group name, there are two checkboxes: 'Scanning local content permitted' and 'Editing of custom dictionaries, user variables etc. permitted'. Both checkboxes are checked. The 'Editing of custom dictionaries, user variables etc. permitted' checkbox is highlighted with an orange border.

1. Login to Compliance Sheriff
2. Go to Settings Tab and click on “Compliance Deputy”



The Compliance Deputy screen contains the following tabs:

- **Configuration:** Allows the options for the configuration file to be defined and saved.
- **Installer:** Allows the user to download a zip file contain the four versions of Compliance Deputy to a location that can be accessed by your users. This should be the same location where you saved the configuration file into.



1. Select the Checkpoint groups or subgroups that the users can scan their page against. These are the same groups available in the Checkpoint Groups list.
2. Select the Group that scans from Compliance Deputy will be assigned to. If a scan group does not exist, create one from the Scan tab. For new V5.1 installations, a group called "Temporary scans" is provided.

**Note:** Deputy scans are considered "Temporary scans". By default, they will not be displayed in the scan list (even when selecting "--All--" in the Scan group filter). To display the Deputy scans, change the scan group filter.

3. Save the configuration file to a location accessible by your users.
4. Go to the Installer tab and click on "Download" to copy the zip file containing the installers, into the same location where you saved the configuration file into.

**Note:** Once installed, the end user has the option of using the Compliance Deputy to browse and load the configuration file.

## 2.4 Installing Compliance Deputy

Refer to the sections below on how to installation/configure Compliance Deputy on different browsers:

- Internet Explorer
- Google Chrome
- Safari (Mac OS)
- Mozilla Firefox

The installers and extensions for these four browsers are included in the Compliance Deputy v5.1 zip file. This can be downloaded by logging into Cryptzone's distribution server (<https://HiVe.HiSoftware.com>) or from the Installer tab in the [Compliance Deputy configuration](#) page in Compliance Sheriff. The Google Chrome extension is also available from the Chrome Web Store (CSW).

### 2.4.1 Internet Explorer

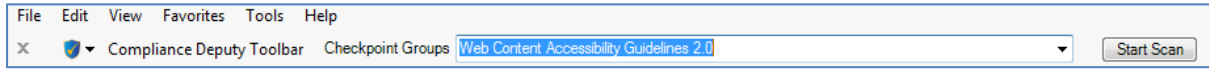
The Compliance Deputy installer for Internet Explorer is provided as a Windows installer (msi) which can be run interactively through the install wizard or in silent mode via the command line.


#### Using the install wizard

1. Close all Internet Explorer sessions.
2. From the downloaded zip file, extract the installer "ComplianceDeputySetup.msi" into your local directory.
3. Copy the Deputy configuration file created previously (e.g. "ComplianceDeputy.config") and pasted/moved it to the same local directory
4. Run the installer and follow the on-screen prompts.
5. When completed, start Internet Explorer.
6. The user may be prompted to allow the add-on to be enabled. When prompted, click on 'Allow' or 'Enable' for the add-on to be enabled.



7. Compliance Deputy will then be displayed in the toolbar.



8. If the Checkpoint group drop down list is empty, the installer may have failed to copy the configuration file into the install directory selected during the install process (for example, you may have executed the installer from a network share).
9. You can manually browse for and load the configuration file using the drop down list provided in the toolbar by clicking on the icon .

### Install in silent mode

Using the msi parameters, Compliance Deputy can be installed from a command line using `msiexec`. For more information on using `msiexec`, in a command prompt, type in `c: />msiexec /?`

1. Close all Internet Explorer sessions
2. From the downloaded zip file, extract the installer "ComplianceDeputySetup.msi" into your local directory.
3. Copy the Deputy configuration file created previously (eg "ComplianceDeputy.config") and pasted/moved it to the same local directory
4. Open a command prompt and set it to the directory containing the Compliance Deputy installer and configuration file.
5. Run the following command

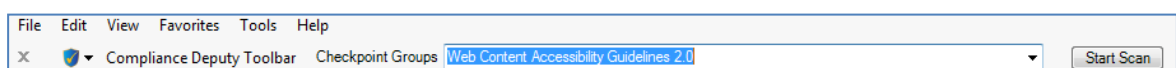
```
c:/> msiexec /i ComplianceDeputySetup.msi /q
```


where:

`/q` = quiet mode (suppresses all install windows) and uses the default install options (installation directory). The default directory is `C:/> Program files (x86)\Cryptzone\Compliance Deputy` To install Compliance Deputy into a different directory:

```
c:/> msiexec TARGETDIR="C:\<mytargetdir>" /i
ComplianceDeputySetup.msi /q
```

6. During the install process, Deputy will automatically load the configuration file (ComplianceDeputy.config) found in the same location as the msi installer.
7. When completed, start Internet Explorer.
8. The user may be prompted to allow the add-on to be enabled. When prompted, click on 'Allow' or 'Enable' for the add-on to be enabled.
9. Compliance Deputy will then be displayed in the toolbar:



10. If the Checkpoint group drop down list is empty, the installer may have failed to copy the configuration file into the install directory selected during the install process (for example, you may have executed the installer from a network share).
11. You can manually browse for and load the configuration file using the drop down list provided in the toolbar by clicking on the icon .

**Note:** For both install options above, the Compliance Sheriff local scan agent, which allows local content (such as the local CSS file referenced by a web page) to be scanned by the remote Worker server, is installed automatically with Compliance Deputy.

### Disable or uninstall

Compliance Deputy can be deactivated and/or removed by performing the following steps:

1. **To disable the Add-in:** go to **Tools menu > Manage Add-ons**. From the list of Toolbars and Extensions, locate and select one of the Compliance Deputy entries in the list. Click on the Disable button and when prompted, click Disable again, ensuring that Compliance Deputy is selected.
2. **To Uninstall the Add-in:** go to **Control panel > Programs and Features**. From the “Uninstall or change a program” list, double click on Compliance Deputy and follow the prompts.

### 2.4.2 Google Chrome




Google Chrome extensions can be loaded directly in the Extensions window when the Developer mode session is checked. However, the current version of Chrome enforces the policy that extensions must be downloaded and installed from the Chrome Web Store (CWS).

If you manually add the extension into Chrome using the Developer mode option, the extension will be disabled when you next start a browser session, requiring you to repeatedly remove and add the extension each time.

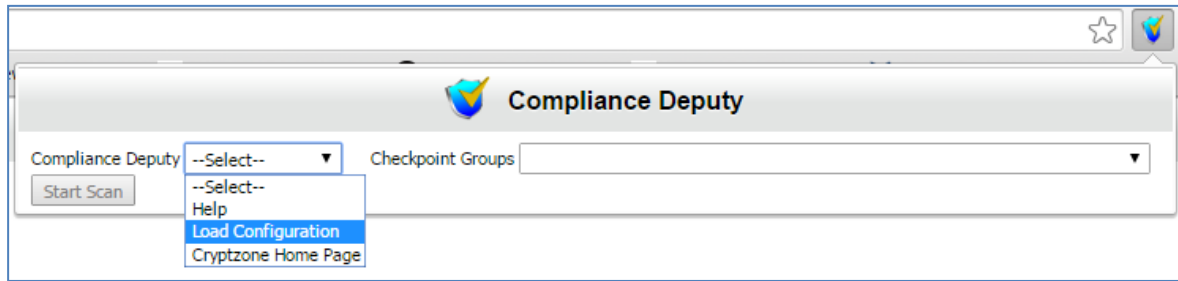
To ensure that the extension is retained, you need to add it from the Chrome Web Store.

### Adding the extension from CWS

To install Compliance Deputy on Chrome from the Chrome Web Store (CWS):

1. Open a Chrome browser session.
2. Go to the Chrome Web Store by clicking on the Show Apps toolbar(  ), or enter the following URL: [https://chrome.google.com/webstore/category/apps?utm\\_source=chrome-ntp-icon](https://chrome.google.com/webstore/category/apps?utm_source=chrome-ntp-icon)
3. Search the Web Store for “Compliance Deputy” or enter the following URL: [https://chrome.google.com/webstore/detail/compliance-deputy-toolbar/lefgkpbepgkeffnmjahndmdlfdjmka?utm\\_source=chrome-ntp-icon](https://chrome.google.com/webstore/detail/compliance-deputy-toolbar/lefgkpbepgkeffnmjahndmdlfdjmka?utm_source=chrome-ntp-icon)
4. Click on the ‘Add to Chrome’ button .
5. When prompted to confirm, click Add to continue.
6. Compliance Deputy should now be available in the toolbar .
7. Click on the toolbar icon to display the options and configuration menus.

8. From the Compliance Deputy drop down list, select "Load configuration".



9. A new browser tab is displayed to allow you to load the configuration file. In this browser tab, along with the option to load a config file, one more option is given to enter the username which will be displayed under show usage.
10. Click on Browse and select the Compliance Deputy configuration file eg "ComplianceDeputy.config". This is the configuration file created from Compliance Sheriff and made available to the users.
11. Once selected, click Upload. Compliance Deputy is now configured and you can start scanning any public pages.

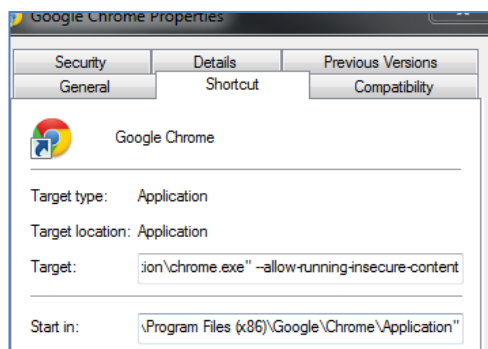
**Note:** For both install options above, the Compliance Sheriff local scan agent, which allows local content (such as the local CSS file referenced by a web page) to be scanned by the remote Worker server, is installed automatically with Compliance Deputy.

### Post installation: scanning a secure (HTTPS) site

If Compliance Sheriff is installed and configured on a non-HTTPS environment, attempting to scan a secure (HTTPS) page with Deputy may be aborted (timeout). This is because by default, Chrome will block insecure content on secure pages. In order for Compliance Deputy to scan secure pages, ensure that Chrome does not block such content. This can be resolved by using one of the following options:

- Ensure that the Compliance Sheriff instance (that Deputy is configured with) is set up in a secure/HTTPS (SSL) environment, OR
- Allow the Chrome browser to always load insecure content (not recommended). This can be done by starting Chrome with the switch: "--allow-running-insecure-content" or add this to Chrome's shortcut to load insecure content automatically:

"...\application\chrome.exe --allow-running-insecure-content"



For more information, refer to: <https://support.google.com/chrome/answer/1342714?hl=en>

## Disable or remove the extension

The Chrome extension can be deactivated/remove from the “Customize and Control Google Chrome” drop down list

1. Select More tools > Extensions
2. Locate Compliance Deputy from the list
3. Uncheck “Enabled” or click on the Trash icon to remove the extension.

### 2.4.3 Safari (Mac OS)

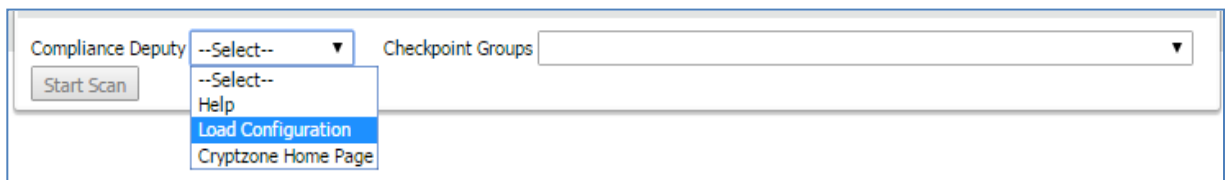
Compliance Deputy is offered as an extension to Safari on the Mac OS X platform.

#### Adding the extension

1. Ensure you have access to the location where the Compliance Deputy configuration file (created from Compliance Sheriff) and the zip file containing the Deputy extension as per section 2.3 above.
2. Close all Safari sessions
3. From the Compliance Deputy installers zip file, extract the Safari extension “Safari\_ComplianceDeputy.safariextz” into a folder in your Mac client.
4. Start Safari and drag/drop the extension into the browser window.
5. When prompted, click Install. The Compliance Deputy extension will now be available in Safari as a grey ‘shield’ toolbar button:



6. Compliance Deputy should now be available in the toolbar
7. Click on the toolbar icon to display the options and configuration menus.



8. From the Compliance Deputy drop down list, select “Load configuration”
9. A new browser tab will be displayed to allow you to load the configuration file.
10. Click on Browse and select the configuration file eg “ComplianceDeputy.config” that was created from Compliance Sheriff and made available to the users.
11. Once selected, click Upload. Compliance Deputy is now configured and you can start scanning any public pages.


**Note:** Unlike Compliance Deputy for Internet Explorer and Google Chrome, the Compliance Sheriff Local Scan Agent is not available for Safari. Support for the Local Scan Agent on Safari will be reviewed in future releases. As a consequence, the following features are not available for Deputy on Safari:

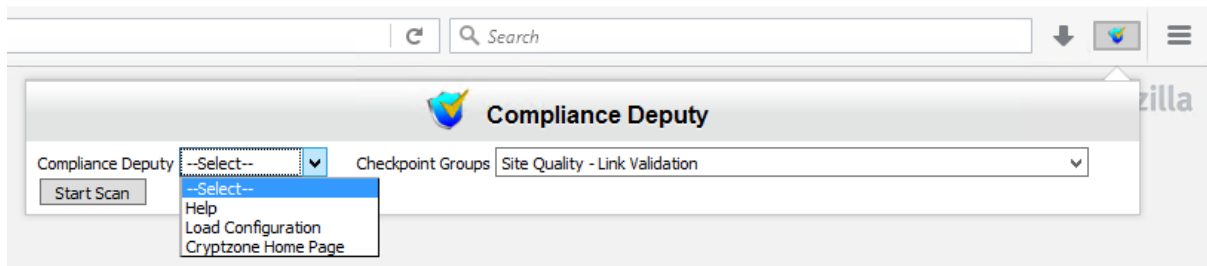
- Scanning of content required by the loaded page that is inaccessible from the remote worker server, such as CSS files stored on the local machine that is referenced by the loaded page.
- Display of <client machine>\<username> in the Show Usage screen in the Compliance Sheriff Admin tab.

#### 2.4.4 Mozilla Firefox

Compliance Deputy is available as an extension to Firefox.

##### Adding the extension

1. Ensure you have access to the location where the Compliance Deputy configuration file (created from Compliance Sheriff) and the zip file containing the Deputy extension as per section 2.3 above.
2. Close all Firefox sessions.
3. From the Compliance Deputy installers zip file, extract the Firefox extension "Firefox\_ComplianceDeputy.xpi" into a folder in your PC client.
4. Start Firefox and install the Compliance Deputy extension file (Open Menu>Add Ons>Extensions>Tools>Install Add-on From File).
5. Compliance Deputy should now be available in the toolbar 
6. Click on the toolbar icon to display the options and configuration menus.
7. From the Compliance Deputy drop down list, select "Load configuration".



8. A new browser tab is displayed to allow you to load the configuration file. In this browser tab, along with the option to load a config file, one more option is given to enter the username which will be displayed under show usage.
9. Click on Browse and select the configuration file eg "ComplianceDeputy.config" that was created from Compliance Sheriff and made available to the users.
10. Once selected, click Upload.
11. After the installation completes, the following changes need to be made to the IIS settings before a scan can be run:
  - a) Open IIS.
  - b) Select ComplianceSheriff website.
  - c) Open "Request Filtering" and click "HTTP Verbs".
  - d) Add new Verb "OPTIONS" by clicking on "Allow Verb".
  - e) Open Handler Mapping.
  - f) Click "View Ordered List".

- g) Find and select "OPTIONSVerbHandler".
  - h) Click "Move UP" in Actions pane until "OPTIONSVerbHandler" is at the top.
  - i) Restart Server.
12. Compliance Deputy is now configured and you can start scanning any public pages.

## 2.5 Upgrading Compliance Deputy

If you are currently using an older version of Compliance Deputy, this version needs to be disabled or removed prior to downloading and installing a later version.

### Internet Explorer

The installer for Compliance Deputy will automatically check if version is currently installed. If found, it will automatically uninstall it, then proceed with installing the new version.

Note that in version Compliance Deputy 4.2, the default install directory was "...\\HiSoftware". This has been change to make the default directory to "Cryptzone".

### Chrome, Safari, and Firefox












These browsers were not supported in Compliance Deputy v4.2.

## 3. Using Compliance Deputy

With the Compliance Deputy toolbar, you can quickly scan the current browser page against a selected Checkpoint Group.

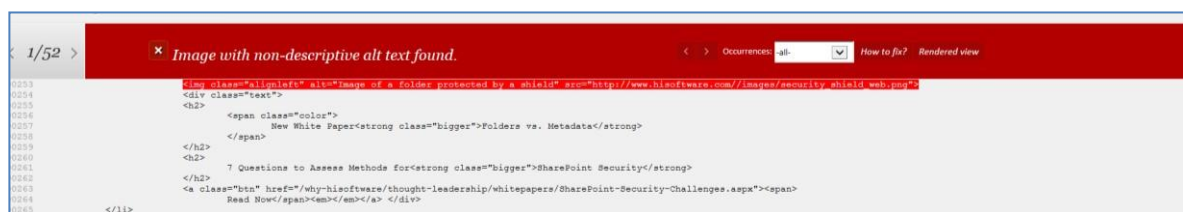
### 3.1 Scanning a page

1. In the browser, type the address of the page you want to scan.
2. In Compliance Deputy, select the Checkpoint group you want to scan the page against.
3. Click Start Scan. A scan status of “Scan running” will be displayed. When the scan is completed, a new tab is opened to display the scan result, and the status changes to “Complete”.

WCAG 2.0 - Compliance Level A scan for http://www.hisoftware.com/		
Result	Checkpoint	Message
	Failure of Success Criterion 1.1.1 and 1.2.1 due to using text alternatives that are not alternatives.	Image with non-descriptive alt text found.
	Use h1-h6 to identify headings	Page does not use headers according to specification.
	Making the DOM order match the visual order	Elements displayed with absolute positioning may be out of logical DOM order
	Failure of Success Criterion 2.1.2 and Conformance Requirement 5 due to combining multiple content formats in a way that traps users inside one format type	Verify that focus is not trapped when using keyboard to navigate application
	Failure of Success Criterion 1.3.3 due to identifying content only by its shape or location	Verify page does not use shape or location to explain instructions
	Failure of Success Criterion 1.1.1 due to using CSS to include images that convey important information	Ensure that image used in background-url for element is not conveying information
	Validate Web pages	Verify page has been run through W3C validator
	Ensure that information conveyed by color differences is also available in text	Page references an external style-sheet. Visual check required.
	Ensure that no component of the content flashes more than three times in any 1-second period	Page may contain elements that cause flickering.
	Provide text descriptions to identify required fields that were not completed	Verify that all required fields are exposed to assistive technology.
	Provide expected data format and example	Verify that instructions are provided for input that requires specially formatted data

**Note:** If you're prompted to log in to Compliance Sheriff when attempting to open the scan result page, Compliance Sheriff may have been upgraded from an earlier version. See Appendix A.1.

4. To view the scan status, click the status message in the toolbar.
5. To view the highlights of issues identified by the Checkpoint, click on the message link. Click on ‘Source’ to display the page source, or ‘Rendered view’ to show the actual web page.



6. The result allows you to review the page you're currently developing, make the necessary changes, save and deploy the page, and re-run the same scan.

### 3.2 Scan using a different checkpoint group

1. When the issue has been identified and corrected, open the same page and re-run the scan against the same checkpoint group to confirm the fixes.
2. Alternatively, from the Deputy toolbar drop down list, you can select another checkpoint group to scan the page against.
3. If the checkpoint group is not available in the list, notify your Compliance Sheriff administrator. The administrator will need to create or edit the Compliance Deputy configuration file to include the appropriate Checkpoints group(s). Once provided, use the Load configuration option in the Deputy toolbar to browse for and reload the new/updated configuration file.

### 3.3 Scan with a different scan definition

- To use a different scan group or scan definition, you will need to create and deploy additional configuration files. For example, to check accessibility on mobile devices, you will need to create a configuration file that specifies mobile checkpoints and a scan group containing a scan definition for each user-agent string you want to test.

### 3.4 Help and support

Additional information on Compliance Deputy can be obtained from the following options.

- Open the Help page. Select “Help” from the Compliance Deputy drop-down list in the toolbar. This will open the Compliance Deputy section on the Compliance Sheriff User Guide.

Note that this requires the Compliance Deputy configuration file, created in Compliance Sheriff, to be loaded into Compliance Deputy.

- Cryptzone web site. Select “Cryptzone Home Page” from the Compliance Deputy drop-down list in the toolbar.
- Cryptzone Help Centre. Submit your requests via the Cryptzone Help Center (<http://support.cryptzone.com>) using your Service Cloud account.



## Appendix A: Administration

### A.1 Allow anonymous access to scan results

If Compliance Sheriff has been upgraded from an earlier version, the user may be prompted to log in to Compliance Sheriff when attempting to open the scan results. To allow anonymous users to run ad-hoc scans and view the results, the following configuration can be added into the Compliance Sheriff web.config file.

- Go to the Compliance Sheriff Web Front End (WFE) installation directory  
e.g. C:\Program Files (x86)\Cryptzone\Compliance Sheriff\web
- Edit 'Web.config' and insert the following after </System.web>:

```
<location path="ShowResults.aspx">
  <system.web>
    <authorization>
      <allow users="*" />
    </authorizati
      on>
    </system.web>
  </location>
```

### A.2 Changing the scan timeout

When a page scan is submitted by Compliance Deputy, Compliance Sheriff will scan the page against the checkpoint group(s) selected. Compliance Sheriff will then wait for a set period for the scan to be completed before submitting the result back to Compliance Deputy. This timeout period ensures that Compliance Deputy does not wait indefinitely should a delay occur in Compliance Sheriff.

Scenarios where this may occur:

- Compliance Sheriff is currently processing a large number of jobs and there are no available workers to process the new requests (refer to your Compliance Sheriff User Guide)
- If you're scanning a large page against a large number of checkpoints.

By default, this timeout period is set to 180 seconds. This can be increased or reduced through the following configuration:

- In the server where the Controller for Compliance Sheriff is installed, locate and edit the Compliance Sheriff configuration file:  
C:\programdata\Cryptzone\ComplianceSheriff\Customers\<Customername>\ComplianceSheriff.config.xml
- Under the <appSettings> group, insert the following:

```
<add key="SinglePageScanMaxSecondsToWait" value="x" />
```

Where: x = timeout in seconds (default is 180 seconds)

- Once entered, the field will be available in Compliance Sheriff: Settings tab > System Configuration > Web Application Settings

### A.3 Displaying completed Deputy scans

When scans are submitted, it will go through several statuses: From Pending -> Running -> Completed or Aborted.

To ensure that the scan list in Compliance Sheriff is not heavily populated by temporary or ad-hoc scans submitted by various users, such as those from Compliance Deputy or a Quick Start scan from the Dashboard, Compliance Sheriff will only display 'Completed' scans when selecting the appropriate scan group from the scan group filter.

To display completed Deputy scans:

1. Ensure that a scan group is created and selected in the Compliance Deputy configuration file
2. Load this configuration file into Compliance Deputy and submit a Deputy Scan
3. When completed, from the Compliance Sheriff Scan list, change the Scan group filter to the Scan group that the Deputy Scan was set to.

#### Notes:

- Temporary/ad-hoc scans are removed, regardless of its status, after a certain time based (see A.4 below)
- The above apply to Quick Start scans from the Dashboard. Ensure that the Quick Start configuration file is set with a scan group.
- Scans created when saving Quick Start scan results are considered permanent scans are excluded from the above rule. i.e. they are displayed as per normal scans.

### A.4 Deleting Deputy scans

When a new page scan is submitted by Compliance Deputy, a housekeeping trigger will be issued to detect and then delete previous scans.

By default, temporary scans (Deputy and Quick Start scans) older than 10 minutes, from the date/time-stamp of the new scan, will be deleted.

This default can be changed through the following configuration:

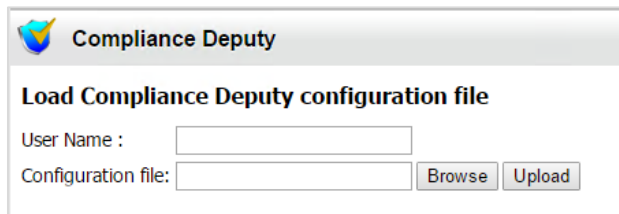
1. In the server where the Controller for Compliance Sheriff is installed, locate and edit the Compliance Sheriff configuration file:  
`C:\programdata\Cryptzone\ComplianceSheriff\Customers\<Customername>\ComplianceSheriff.config.xml`
2. Under the <appSettings> group, insert the following:  
`<add key="DeleteAdhocScansOlderThan" value="x" />`  
 Where:  
`x` = scan age in seconds (default is 600 seconds) 0 = Do not delete
3. Once entered, the field will be available in Compliance Sheriff: Settings tab > System Configuration > Web Application Settings

**Support tip:** For troubleshooting purposes, if a Deputy scan is aborted, use the above setting to preserve the scan and its results whilst working with Cryptzone support to identify the issue. Alternatively, when a scan is aborted, click on its status then "Export files" to package up the scan definition, which will include the scan log file and resources used by the scan.

## A.5 Show Usage

For administrators, history of all scans, including scans submitted through Compliance Deputy, will be listed in the Show Usage screen in Compliance Sheriff

1. Log in to Compliance Sheriff as an administrator
2. Go to the Admin Tab and click on the 'Show usage' button
3. A page will be displayed showing a table containing the list of
  - scans performed
  - Its base URL
  - Start and Finish date/time
  - Pages scanned (1 page)
  - Number of Checkpoints used (defined by the Checkpoint group selected)
  - Client machine\username will be displayed for IE. Username entered while loading the config file will be displayed under show usage for Chrome and Firefox.



The screenshot shows a window titled "Compliance Deputy" with a logo on the left. Below the title bar, the text "Load Compliance Deputy configuration file" is displayed. There are two input fields: "User Name :" followed by a text box, and "Configuration file:" followed by a text box. To the right of the "Configuration file:" text box are two buttons: "Browse" and "Upload".