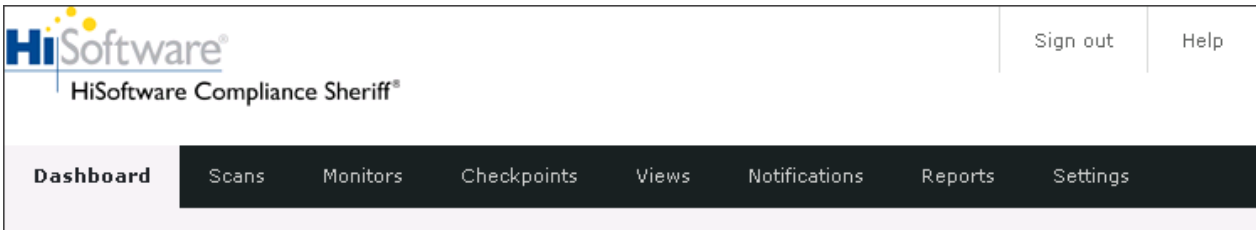
CSU Dominguez Hills ATI
COMPLIANCE SHERIFF
USER'S GUIDE

VERSION 4.2.x

Table of Contents

Table of Contents

Dashboard



The dashboard is the presentation area for the views you have defined. You can display one or more views on your dashboard.

Add a View to the Dashboard

1. Click the **Dashboard** tab.
2. Click **Add view**, and select a view from the drop-down list. (If you have not yet created any views, none will appear. See the Views section of this document for further instructions.)

A drop-down menu for **Panels**, **Tabs**, or **Vertical** is only shown if more than one view is added to the dashboard.

Rearrange Views on the Dashboard

1. Click the title bar of the view.
2. Drag the view to the preferred location.

Views can only be 'swapped' with an adjacent view, either horizontally or vertically. To the right of the Add View button is a drop-down menu, from which you can select **Panels** or **Tabs** for a left-to-right arrangement of your views, or **Vertical** for a top-to-bottom arrangement (see Presentation Mode for more details). If you have a large number of views in vertical mode and you want to move the top view to the bottom, it would be simpler to close it and re-add it. Otherwise, if you want to move the bottom view to the top, you will have to do it in multiple steps (this will require fewer steps in panels mode than in vertical mode).

Remove a View from the Dashboard

1. Click the **Dashboard** tab.
2. At the top right corner of the view you want to close, click the close button (**X**) .

To remove a view in tabs mode, highlight the view you want to remove, and click on the **X** next to the view's name.

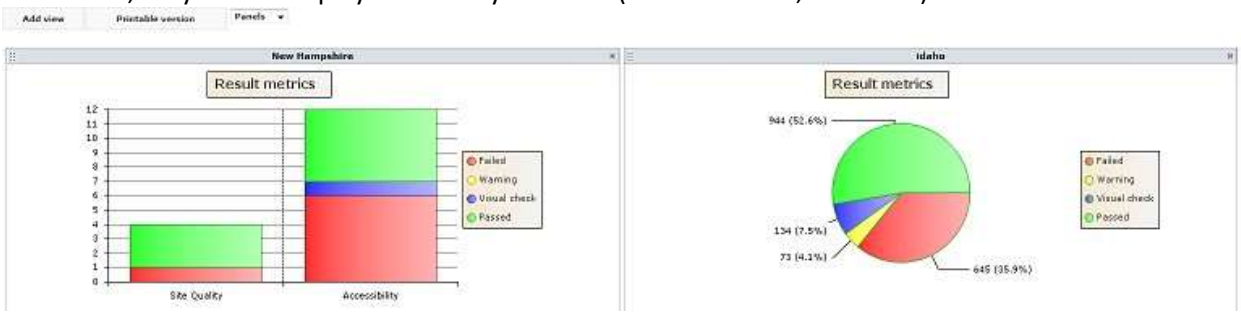
Presentation Mode

When there is more than one View, you have an option to change the presentation mode.

1. Click the **Dashboard** tab.
2. To the right of the Add View button, click on the drop-down menu.
3. Select the presentation mode you prefer.

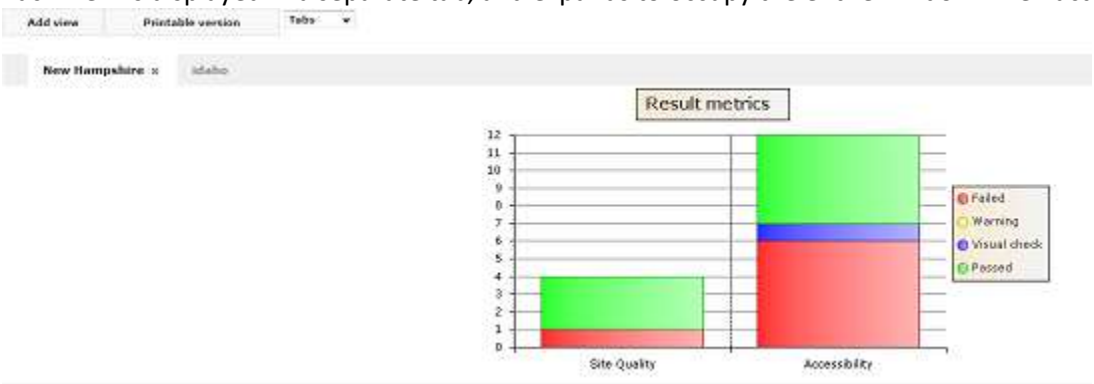
Panels

The views are arranged to be as square as possible. For example, if you add 4 views to your dashboard, they will be displayed in a 2 by 2 format (two columns, two rows). If you have 6 views on your dashboard, they will be displayed in a 3 by 2 format (three columns, two rows).



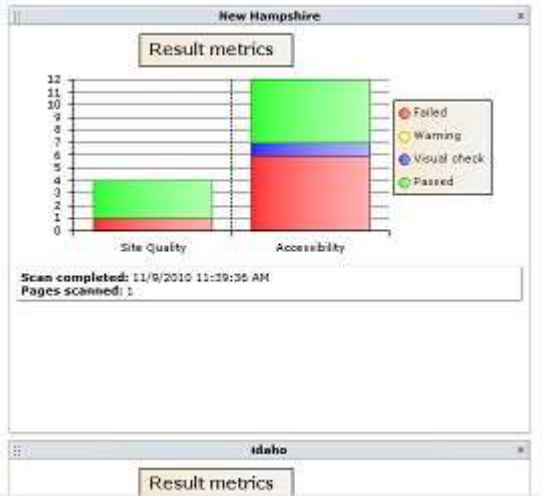
Tabs

Each view is displayed in a separate tab, and expands to occupy the entire window when active.



Vertical

The views are arranged down the window, one below the other.



Vertical mode is recommended for users employing screen readers (such as Jaws), since it allows each view to be read from top to bottom.

Printable Version

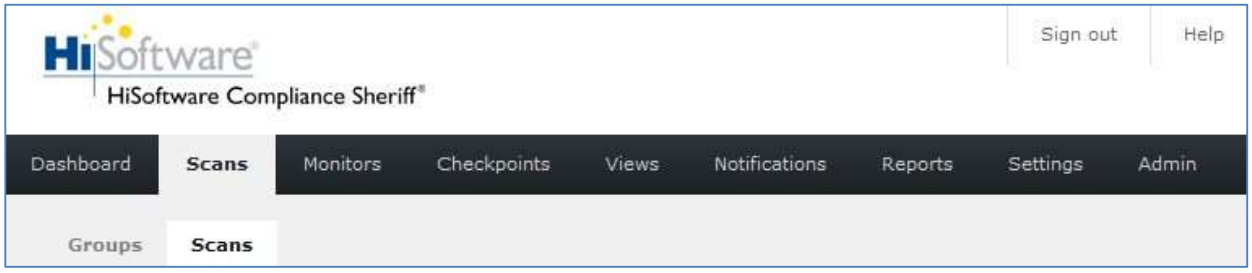
The printable version allows you to view the dashboard in a report form, by combining the report forms of each view on your dashboard together. In panels mode, the views are shown in two separate columns.

The printable report version only includes a summary (i.e. collapsed version) of any tables.

Printing

1. To customize the print out (for page size, orientation, etc), open your browser and click **File** -> **Page Setup**.
2. When ready to print, click **File** -> **Print**.

Scans



A scan is a collection of checkpoints that will be executed on the pages of a website. Once a scan has been run, you can use the scan results to create views and reports.

Scans allow you to run multi-level checks on your site for compliance issues. They can be scheduled by site users with valid permissions.

When you click on the **Scans** tab, a list of all the scans you've created will appear on the screen. The page defaults to the **Scans** sub-tab, but you can click the **Groups** sub-tab to see a list of all your scan groups. You can also select a scan group from the **Scan Group** pull-down menu in the upper right.
You can create a new scan by clicking **New**, or delete a scan by checking the appropriate box and clicking **Delete**. If you click **Toggle Filter**, text boxes will appear at the top of each column, and you can enter specific values into these boxes to filter your list. Check **Disable auto-update** if you don't want the page to refresh while you're selecting a range of scans.

Create a New Scan

To create a new scan, you must enter a Base URL and select at least one checkpoint group.

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Click on the **New** button.
3. In the **Display Name** field, type a name for the scan. You can use long descriptive names.
4. In the **Base URL** field, type the full path name of the site to be scanned.
5. By default, subgroups are not listed in the table. Put a check in the "Show subgroups" box to show all available subgroups in the list.
6. In the **Checkpoint groups** table on the right, select the **Checkpoint groups** or/and **Subgroups** to be used by the scan, then click on the **Add** button. You must select at least one checkpoint group. (A subgroup is any checkpoint group that is contained by another checkpoint group.)
7. If you would like the scan to begin from a specific site page, enter the address of this page in the **Start page** field.
8. If necessary, edit the transaction script by clicking on the **Edit** button beneath the **Transaction Script** heading. (For more information on transaction scripts, please go to the Transaction Scripts page.)
9. If a site requires a username and password to be scanned, or if you wish to specify the domain and/or the page limit of a scan, click on the **Edit** button beneath the **Options** heading.
10. Click on the **Save** button.

Edit a Scan

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Locate the scan you wish to edit, and click on its name.
3. Modify the scan properties as needed. To remove a checkpoint group, look for the checkpoint group's name in the left-side **Checkpoint groups** field, click in the box next to it, then click on the **Remove** button.
4. Click on the **Save** button.

 If you use the **Save as new** button to create a new Scan, you must change the **Display name** first.

Delete a Scan

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. If the scan you wish to delete is running, stop it first, using the **Stop** button on the far right.
3. Select the check box next to the scan's name.

You can select more than one scan to delete at a time.

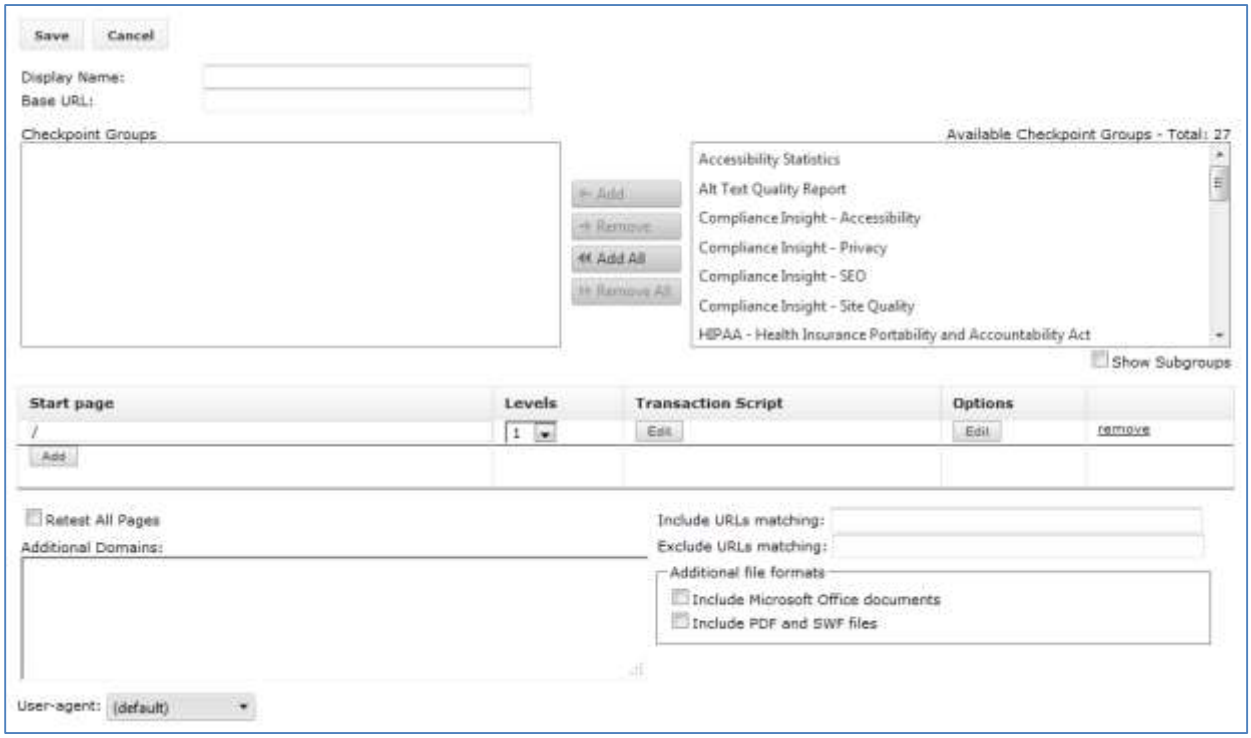
To select or de-select all scans, you can double-click on the header cell of the check box column, located at the top left.

4. Click on the **Delete** button.
5. A confirmation dialog box will appear. Select **OK** to confirm deletion.

 Any results that may have existed for the scan will be permanently deleted.

If you elect to delete a scan that has a view associated to it, a confirmation box will appear: "One or more views refer to the scan(s) you are deleting, and may not continue to function correctly." Choose **OK** to delete, or **Cancel** to abort.

Scan Properties



Add

Highlight one or more checkpoint groups in the right-hand table and click **Add** to include them in your scan.

Add All

To add all of the checkpoint groups in your system to a scan, click **Add All**.

Additional Domains

If your scan is set to scan http://www.mycompany.com/, a 'Search' link may be pointing to http://search.mycompany.com/, which will not be scanned by default. If this is the case, include the domain in the **Additional Domains** property of your scan. (The Additional Domains field is located near the bottom-left of the page when you're creating or editing a scan.)

Additional file formats

When **Additional file formats** is selected, the files are first converted to HTML and then processed against the checkpoints defined in the scan. Your scan may include the following non-HTML file types:

- Microsoft Office files: MS Office 2003 (Word, Excel and PowerPoint) documents.
- PDF and SWF files: Adobe Portable Document Files (PDF 1.4) and Shockwave Flash files (SWF 8 and below)

Available Checkpoint Groups

A checkpoint group is a set of checkpoints or checkpoint subgroups. Usually they are a related set, but a checkpoint group can be created for any purpose. The right-hand table, labeled **Available Checkpoint Groups**, lists the remaining checkpoint groups defined for your system. The left-hand table lists the checkpoint groups that will be used by the scan. Highlight one or more checkpoint groups in the right-hand table and click **Add** to include them in your scan. Highlight one or more checkpoint groups in the left-hand table and click **Remove** to take them out of your scan. To add or remove all of the checkpoint groups in your system to or from a scan, click **Add All** or **Remove All**.

Base URL

This defines the potential scope and limit of the scan. A valid http:// or https:// URL should be entered. If you do not type http://, it will be added automatically. A base URL must be defined for a scan.
A scan does not scan all pages in the domain. The number of pages is determined by the level defined in the start page, and by what can be reached via crawling links.

We recommend you do not define sub-directories in the base URL. For example, use http://mysite.com/, not http://mysite.com/en/, and use the start page option to specify the address relative to the site root.

File-based scans can be defined using the file:/// prefix (this is added automatically if required), but note that for such scans **Run locally** must be selected.

Checkpoint Groups

A checkpoint group is a set of checkpoints or checkpoint subgroups. Usually they are a related set, but a checkpoint group can be created for any purpose. The left-hand table lists the checkpoint groups that will be used by the scan. The right-hand table, labeled **Available Checkpoint Groups**, lists the remaining checkpoint groups defined for your system. Highlight one or more checkpoint groups in the right-hand table and click **Add** to include them in your scan. Highlight one or more checkpoint groups in the left-hand table and click **Remove All** to take them out of your scan. To add or remove all of the checkpoint groups in your system to or from a scan, click **Add All** or **Remove All**.

Dynamically generated fields

This is a comma-separated list of form fields that hold typically session-based IDs that change every time you attempt an interaction. For instance, after recording a number of steps with the script recorder, you may notice steps like:

POST http://mysite.com/myapp.cgi, cmd=addtocart&sessionid=267ga672fe7afdbc25c

Each page that is returned by the transaction script is tested to the number of levels specified for the relevant start page. If you only want the pages specifically returned by the script tested, make sure that levels is set to 0.

Display Name
This is the descriptive name for a scan. It will be displayed on the list of scans. The scan list can be sorted by name by clicking **scan** on the top title bar column.

Exclude all URLs matching
This is a regular expression for excluding all pages with names that conform to the expression.

Example:
\.txt will exclude all pages whose URLs end with .txt.

Include all URLs matching
This field will determine what pages are included for testing. The filter is a regular expression. If specified, pages will only be included in the scan if the URL matches the expression.

Example:
/Shop/

This means that only pages whose URL includes the value /Shop/ will be tested.

Levels
For a particular **Start page** you can specify how many levels the scan will track down. A scan will include any pages referenced by the current page, provided it does not exceed the number of levels defined. We recommend that you set the level to 1 when you create a new scan. This will reduce the number of pages that will be scanned while you are refining the scan properties. Later, when you are ready to scan all the pages of a website, you can increase the levels.

The maximum number of scan levels is 20.

Options
The **Options** menu can be accessed by clicking on the **Edit** button beneath the **Options** heading.
Username/Password/Domain

Use these options for sites requiring HTTP authentication (for example, when the browser displays a login dialog).

Page Limit
Use this to limit the maximum number of pages returned.

Remove
Highlight one or more checkpoint groups in the left-hand table and click **Remove** to take them out of your scan.

Remove All
To remove all of the checkpoint groups from a scan, click **Remove All**.

Retest All Pages
Previous scan results can be manually modified by importing a CSV file with updated results. When an update is detected, the page is not re-scanned, which preserves the results of the last scan. Turning this option on forces the scan to retest these pages and update the results.

Scan local content
The Toolbar from previous versions of HiSoftware Compliance Sheriff is no longer used to scan content on your local machine. Instead, by clicking the **Scan local content** check box, you can install the browser-agnostic local scan agent on your machine, and it will automatically upload local content to your Compliance Sheriff server for scanning. As such, most of the previous restrictions on local scans are now removed – you can schedule scans that check local content, results highlighting is supported, performance is increased, and logging is available to all users. However, please note that Transaction Scripts are now disabled when a local content scan is defined.

For more information, visit the Scan Local Content page.

Show Subgroups
The Checkpoint Groups available on your system are comprised of Checkpoint subgroups. If you put a check in the **Show Subgroups** box, the Checkpoint subgroups will appear in the right-hand column.

Start page
A **Start page** defines the starting URL. The default is "/" which means the root of the base URL. A Scan will begin at the first **Start page**, then when all links are exhausted, it will continue at the next start page.

Multiple **Start pages** can be defined/added, each with different attributes.

Transaction Script
A **Transaction script** is used to define user interactions required to access portions of a site. For example, to scan pages in a shopping cart site, you will need to log-in, select an item, and check out. To create a **Transaction script,** click on the **Edit** button beneath the "Transaction script" heading. A script can be typed in the field provided (see Transaction script commands in this chapter) or by using the recorder facility.

User-agent
This option may be used if your web server is configured to respond differently to different user agent strings. For instance, it may require that string include "IE" or "Firefox". HiSoftware Compliance Sheriff is configured with sample User-agent strings as listed in the drop-down list, along with a "default" option. To edit or add user-agent string to this list, see Chapter 10: User agents under the **Settings** tab.

You can find more information on User-gent strings at the MSDN library:
http://msdn2.microsoft.com/en-us/library/ms537503.aspx.

The default user-agent string is internally defined as: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; HiScan).

Transaction Scripts

A transaction script is used to define user interactions required to access portions of a site. For example, to scan pages in a shopping cart site you will need to log-in, select an item and checkout.

Create a Transaction Script

To create a transaction script, perform the following steps:

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Click on the **New** button.
3. In the **Transaction Scripts** field, click on the **Edit** button.
4. A script can be typed in the field provided or by using a recorder facility. For information on transaction script commands, visit the Transaction Script Commands page.

Transaction Script Commands

The transaction script recorder is only supported in Internet Explorer 7.0 or greater. If you are using an older version of IE, or a different browser, you can create the transaction script yourself. Beneath the "Transaction Script" heading, click the **Edit** button, and enter the transaction script manually.

GET <url>
The GET command causes a new page to be loaded.

POST <url>, <postdata>
This command issues an HTTP POST request for a specified resource.
The format of the <postdata> for the POST command is exactly as it is sent to the HTTP server.

If you use the script recorder, passwords are automatically encoded so that they can't be easily read by other users. You should **not** use sensitive username/password combinations for the transaction script recorder, as this is a testing tool, and every time you run a scan it will replay the script actions specified, which may involve logging in as a particular user and performing actions as though the scanning tool was that user.

TESTING ON|OFF
The "TESTING ON|OFF" command is available for cases where particular interactions are required as part of the transaction, but the pages that are returned do not need testing.
Example:

TESTING OFF
POST http://mysite.com/myapp.cgi, user=john&password=%43%42%46
GET http://mysite.com/myapp.cgi, cmd=addtocart&item=7e489232
TESTING ON
POST http://mysite.com/myapp.cgi, cmd=checkout
This will cause the first two steps – logging in, and adding an item to a cart – to be executed, but the pages returned will not be checked. Only the page returned by the final step – executing a 'checkout' – will be tested against the checkpoints, or included in the database results/report.

SLEEP <seconds>
This causes the scanner to pause before testing the page and continuing with the next step. This can allow the browser more time to complete the request, including executing any client-side scripts.

Dynamic generated fields
This is a comma-separated list of form fields that typically hold session-based IDs that change every time you attempt an interaction. For instance, after recording a number of steps with the script recorder, you may notice steps like:
POST http://mysite.com/myapp.cgi, cmd=addtocart&sessionid=267ga672fe7afdbc25c

The value of the 'sessionid' field identifies the session to the web server, and is different every time you use the web application. If the script was simply replayed as is, it would most likely fail, because the server is expecting a new session ID. If "sessionid" is listed as a dynamic generated field, then instead of simply sending the same value that was recorded initially, it finds the new value that was supplied by the server when the first step was executed, by looking for a hidden form field with that name.
When you use the script recorder, it attempts to determine likely session ID fields automatically. This is not always possible to do reliably, and so it should be checked after you finish recording.

Run a Scan

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Find the scan you wish to execute and click on the **Run** button, located at the far right of the row. **Run** launches the scan immediately. If the scan is marked as "local" in the **Base URL** column, it will run on your own machine. This option requires the HiSoftware Toolbar.
3. The status will change to "Running."

Scans can also be started automatically by setting up a Schedule.

Scan Status

The status of the scan will depend on its current state of activity, or the success of the most recent scan.

Icon	Status	Description
	None	The scan has not been run.
Pending	Pending	The scan has been launched, but is not able to run yet.
Running	Running	The scan is currently in progress.
82%	Passed	The scan completed successfully, and a health value generated.
52%	Passed with warnings	The scan completed with some warnings, and a health value generated.
9%	Failed	The scan completed, but one or more pages failed to pass all the checkpoints.
Aborted	Aborted	The scan failed to complete properly. See Troubleshooting for additional information.

You can view the results of the scan in detail by clicking on the status description (located beneath the "Status" heading), or using the ENTER key to activate the link.

Stop a Scan

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Check that the scan status shows as **Running**.
3. Click on the associated **Stop** button to stop the scan. The **Stop** button is located in the same place as the **Run** button, at the far right of the row.

View Scan Results

1. After a scan has been run, click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Click **More** in the row corresponding to your scan. The **More** link is located in the far-right column.
3. Additional fields will appear beneath the row. To view a scan result, click **Show Results**.
4. The properties for a view will be displayed. If you have previously specified a view, the view properties will be remembered. (For more information on view properties and how to manage them, please consult the Views section of this document.)

The view will only show the results of the current scan.

5. Click **Save** to save the results and view properties of this scan. To cancel, click on the **Cancel** button.

View Scan Log File

By combining time-stamped log messages from multiple scan runs, HiSoftware Compliance Sheriff V4.2 allows you to filter past and present results by category: Debug, Info, and Error. **Debug** refers to detailed information about scan progress, including an "Analyzing" message for every page processed. **Info** refers to information about the scan, including timings, IP address information, and redirections detected. **Error** refers to unexpected events, such as pages not being able to be downloaded or processed, or critical problems that prevent the scan from completing.

To access the log file, perform the following steps:

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Click on the status link in the corresponding row. Status links are located in the **Status** column.
3. The log file for the last run will be displayed. Click or un-click the Debug, Info, and Error boxes to determine which results are displayed. You can also click on the any of the column titles (Type, Timestamp, Message, and Stack trace) to sort the results according to that column.

Export Results

You can export the results of a scan to a CSV file.

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Find the scan you wish to export and click on the **More** link in the corresponding row. The **Export to CSV** field will appear. (PLEASE NOTE: The **More** link will not appear if the scan has not been run.)
3. From the drop-down menu in the **Export to CSV** field, select the type of data you wish to export. For more specific options, click **Advanced**.
4. Once you've selected a data type, click **Export**. You will be prompted to **Open** or **Save** the file.

Example:

You can export visual checks to a CSV, perform the visual checks, update the CSV, and then update the database.

Import and Update Results

You can update the database with previously exported CSV files that you have amended.
For example, you may perform a number of visual checks on items that were identified by one or more checkpoints, and change each result to "Fail" or "Pass" as appropriate. If you do not change the corresponding "message" column, it will be automatically changed to reflect the new result. In either case, your username will be automatically appended to the message text in square brackets so that anyone viewing the results will be able to confirm that the result has been manually adjusted, and by whom.

Because the results are in CSV format, you can use whatever tools your spreadsheet tool provides to make "batch" changes. For example, if you know that every page in your site must pass a particular checkpoint marked as 'visual,' you could filter the records to only show those pertinent to that checkpoint, and update all those records at once.

Before committing the changes to the database, you will be asked to confirm the operation, and you will be shown the number of records that will be updated. Note that this operation is irreversible and will permanently alter the database.

Subsequent runs of the same scan may or may not preserve any manual adjustments you have made; this is dependent on whether the crawler can determine that the page has not changed. When the records are updated through the Import facility, page results that were updated will be flagged accordingly. This flag is then used by the crawler to skip these pages during subsequent scans, preserving the result. If you want the scanner to re-scan the page, check on the "Retest all pages" option in the scan properties before you run the scan.

The alternative to using CSV import to update results is to use the Results Revision Wizard.
To use CSV import, perform the following steps:

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Find the scan you wish to update with a previously exported CSV file, and click on the **More** link in the corresponding row. The **Update from CSV** field will appear.
3. In the **Update from CSV** field, click **Select**, and locate the CSV file you wish to import. Once you've selected a file, click **Import**.
4. A result message will appear in the panel. To refresh the status panel, click **Refresh import**. To abort, click **Cancel import**.

Purge Scan Results

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Find the scan whose results you wish to purge and click on the **More** link in the corresponding row. The **Purge** field will appear.
3. Click on one of the purge buttons:
    a. **Purge all** deletes all runs, including the one most recently completed, so that no results will be available for this Scan.
    b. **Purge old** deletes all runs except the one most recently completed.
    c. **Purge latest** deletes only the most recently completed run.

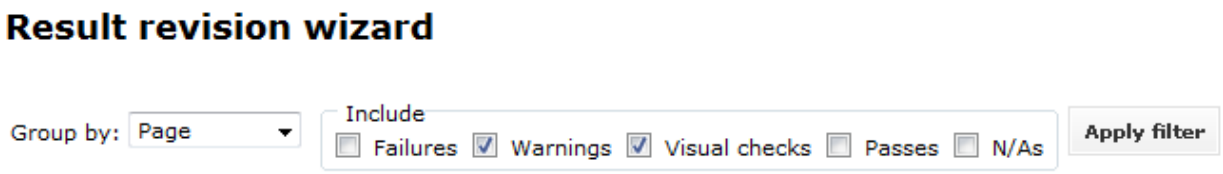
 Purging means that the results are PERMANENTLY deleted from the database. Deleted results cannot be recovered, so delete with care. In most cases, you will only need to do this if your database becomes cluttered with scan results that you no longer need.

Revise Scan Results

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Find the scan whose results you wish to revise, and click on the **More** link in the corresponding row. The **Results** field will appear.
3. In the **Results** field, click on the **Revise Results** button. You will be directed to the result revision wizard.

Result Revision Wizard

PURPOSE:
The result revision wizard allows you to manually modify the results generated by an automated scan. This is needed for checkpoints that require visual checking, and when checkpoints generate "false positives" - for example, when a failure is recorded but manual inspection determines that the page or element in question should have passed the checkpoint, usually because the checkpoint rule does not explicitly cover all possible exceptions.



ACTIONS:
The wizard displays all the results generated by a single scan, much like a report, with various grouping and filtering options. Each result is shown via a set of toggle buttons, one for each of the following: Failed, Warning, Visual Check, Pass, and N/A. The button associated with the generated result will be shown as depressed. The user may elect to leave the result as is, or to modify it by clicking any of the other buttons. Upon modifying a result, the user also has the opportunity to modify the result message as well, so that reference notes or comments explaining why a given result was modified can be added. Note that the user name of the user who modified the result is always stored as part of the comment, so that results modified through the revision wizard can always be detected easily when displaying views or reports. After examining or modifying a page of results, the user can click on the **Next** button to commit the changes to the database and continue to the next page. On the final page of results, the user would click on the **Finish** button.

The results revision wizard supports two methods of working - "by page" and "by checkpoint".

"By page" mode is suitable for smaller scans (for example, if there are fewer than 100 pages requiring manual checking). In this mode, the wizard steps through each web page one by one, showing the URL of the page, and listing any results for that page that match the current filter. By default, only "Warnings" and "Visual Checks" are shown, so if the user needs to revise any "Failed" results, they will need to click in the **Failures** check box in the **Include** field.

Clicking on the web page URL will open the relevant web page in a new window. There are also options to control how the page is displayed:

Grayscale: The page is displayed without colors. This can be useful when checking a page's suitability for colorblind users.
Disable CSS: The page is displayed with no styles. This can help determine how a page is viewed by visually impaired users, or users with limited interfaces.

Hide images: The page is displayed with no images. This can be useful to determine whether or not all necessary information is available in text form.

Linearize: The page is displayed so that all tables are shown with only one cell per row. This can help determine how information in tables is presented by screen readers.
Note that clicking on **Next** or **Previous** will cause the currently displayed web page to change automatically.

If there are more than 25 results for a particular web page, only the first 25 will be shown initially, and a box with the number [2] will be shown that allows the user to access the remaining results. If there are more than 50 results, there will boxes labeled [1], [2], [3] etc.

"By Checkpoint" mode is suitable for large scans in which a single checkpoint is likely to fail in the same manner across a large range of pages. For example, if a large number of pages are based off a template that uses a decorative image with blank ALT text, you are likely to get a large number of warnings about the same image. Instead of modifying each instance one by one, you can modify all such instances with a single click. Furthermore, if the checkpoint makes use of a user-variable to list exceptions to the general rule, then in many cases the user-variable can be automatically updated so that future scans will record the correct result.

When using "by Checkpoint" mode, the wizard steps through each checkpoint one at a time in numerical order. For each checkpoint, the results are grouped by the result message and the key attribute values. For example, if Checkpoint Accessibility 1.1.1 causes a warning "Non-decorative IMG element contains empty ALT attribute" for images "http://mysite.com/logo.gif" and "http://mysite.com/blank.gif", two separate entries will be shown. When a result is changed for an entry with an associated key attribute value, then the checkpoint rule is checked to look for a test with the following form:

```
If has attribute {key-attribute}
If attribute value [as absolute url] equals any of
%{uservarname}%
...
Else
Mark {existing-result-value}, with '{message}'
```

where *{key-attribute}*, *{existing-result-value}* and *{message}* match the result being modified. The [as absolute url] part is optional.

If such a test is found, then the key attribute value for the current result record is added to the User Variable *{uservarname}*, with the necessary comma separator. Note that for results where no key-attribute value is present (e.g. page-based checkpoints), no user-variables will be automatically updated. If there are more than 25 results for a particular checkpoint, the results are broken up into subsets as described previously.

If you are using spell-checking checkpoints, you can use the wizard to add custom words, including proper nouns (such as company and product names), so that these words don't fail the checkpoints in the future. A revision will need to be made to each individual spell-checking checkpoint you are using. Be sure to capitalize proper nouns, so that future scans will identify un-capitalized instances of these words as errors. For example, if you wanted "Firefox" to pass a spell-check, you use the Wizard to add "Firefox" only, because "firefox" is a spelling error. For more information on adding custom words, visit the User Dictionaries page.

CAPABILITIES:

The wizard supports several shortcut keys to make stepping through the results faster:

f: marks the current result as a "Failure" and steps to the next result
w: marks the current result as a "Warning" and steps to the next result
v: marks the current result as a "Visual check" and steps to the next result
p: marks the current result as a "Pass" and steps to the next result
n: marks the current result as a "N/A" and steps to the next result

To use these shortcut keys, you will need to ensure the focus is on one of the result buttons - this is true when each screen is shown initially, but it won't be true if, for example, you modify any of the grouping or filtering options. This method is most appropriate when there is no need to enter extra comments for each modification. After modifying the last result on a particular screen, the focus jumps to either a numbered-button that brings up the next subset of results for the current page or checkpoint, or if none, to the **Next** button. You will need to hit the return or space key to activate the button.

HOW TO USE:

Scenario 1 - page-based visual accessibility check

1. Run a Section 508 or WCAG 1.0 Priority 1 scan on 5-page sites containing an image.
2. When the scan finishes, click on the result shown under the **Status** column.
3. Click **Revise results**.
4. All warnings and visual checks for the first page of your web site will be shown.
5. Uncheck the **Warnings** check box and click **Apply Filter**.
6. Notice that only Visual check results are now shown.
7. Click on the page URL to open a new window displaying the page.
8. Check the **Grayscale** check box to show the page in monochrome.
9. Visually confirm that the page is readable with no color.
10. For the entry for Checkpoint 2.1 "Ensure that all information conveyed with color is also available without color", click on the **Passed** button.
11. Click **Next** to move to the next page, and commit your change to the database.
12. Repeat Steps 9-11 until you see the **Finish** button, then click on it. Your website is now accessible to color blind users.

Scenario 2 - Checkpoint-based false-positive revision

1. Ensure first that you are using the checkpoints shipped with version 4.2 - if you upgraded from a previous version, you may need to contact support.
2. Run a Section 508 or WCAG 1.0 Priority 1 scan on a site with several pages based on a template that contains a decorative image (e.g. a border or spacer image) with blank ALT text.
3. When the scan finishes, click on the result shown under the **Status** column.
4. Click the **Review results** button.
5. Change to **Group by Checkpoint**, and un-check the **Visual checks** checkbox.

6. Click **Apply Filter**, and note that all warnings generated by Checkpoint 1.1.1 are shown.
7. For the first entry, take note of the full URL of the IMG SRC attribute, and click on the **Passed** button.
8. Click on the **Next** button (or the **Finish** button if no other checkpoints generated warnings).
9. Navigate to the **Settings** tab, and click **User agents, variables & key attributes**.
10. Confirm that in the entry field labeled "List of user variables", the variable %DecorativeImageList% now includes the URL you noted in Step 7.
11. Create another scan of the same site (or edit the existing scan to ensure that "Retest all pages" is checked), and run it.
12. Repeat steps 3-6, and note that there is now no warning for the image URL that was added to the %DecorativeImageList% user-variable.

MISC:
If you change the grouping or any of the filter checkboxes, you must click on the "Apply Filter" button. Depending on what is currently displayed, the wizard may then need to change the currently displayed Checkpoint. To visually confirm that a Checkpoint has passed, you can click on the Checkpoint number, which will open a new window containing the information associated with the Checkpoint.

Scan Local Content

If you want scans to be able to access content that is only reachable from your machine, the HiSoftware local scan agent needs to be running. The local scan agent communicates with the Compliance Sheriff server to upload content accessed by your machine for scanning. This content may be local, but it may also be on the company intranet, or on a secure intranet site that requires special authentication only possible from your machine. If you want to run scans overnight, you'll need to make sure that the machine hosting the local scan agent won't be shut down, or placed in hibernation mode.

To enable local content scanning, please perform the following steps:

1. Click the "Scan local content" checkbox on the scan definition page. (If you have already done this and have arrived at this page, proceed to Step 2.)
2. Download and run the local scan agent installer. When the welcome prompt appears, click **Next**.
3. The installer will prompt you to select a folder path for the installation. Use the default folder path provided by the installer, and click **Next**.
4. Enter the URL path to Compliance Sheriff. This should be the address of the instance that you downloaded the Compliance Sheriff install from. (Do not include the "[active server page].aspx" suffix.) Click **Next**. (NOTE: If this is a "localhost" address, you don't need to use the local scan agent.)
5. Enter a user name and password. You need to do this because the local scan agent runs as a background task, and the credentials you supply are what will be used to fetch any content required for the scan. For security reasons, it's best not to provide the credentials of a domain user, but of a local user that only has access to the particular content you want to scan. Click **Next**.
6. Click **Install** to begin the installation.
7. When the installation completes, click **Finish**.
8. A page will load in your default browser, stating "You may now scan content on this machine with the current browser." (NOTE: The installer only allows the local scan agent to work for your default browser. If you are using your non-default browser to run HiSoftware Compliance Sheriff, and you run the local scan agent install, you'll notice that a post-install URL will open in your *default* browser, saying it is ready for use--your non-default browser has *not* been enabled. If you want to enable a non-default browser, you will need to copy and paste this post-install URL from your default browser into your non-default browser, and hit **Enter**.)
9. You may now create a local scan. In the **Base URL** field, enter the location of the local file content. For example: "file:///C:/FileDirectory1/FileDirectory2". Leave the "Scan local content" box checked.

Whether your browser can run local scans is based on a cookie set by the installer, containing the name of your machine. If this cookie isn't set, or if you turn off or clear the cookies in your browser, you'll have to re-run the installer. If you still have the post-install URL open, you can re-paste it into the browser you plan to use. Either way, you don't need to re-download the agent, you just need to re-run it.

Please note that you can only use the local scan agent for a single instance of Compliance Sheriff. If you are accessing multiple installations of Compliance Sheriff at different addresses from your machine, you can't have the local scan agent supporting them all. It can only support one of them.

Schedule Scans

A scan can be scheduled to run at predetermined intervals. Multiple schedules can be defined for a scan. If a scan has no schedule defined the text "schedule" will be displayed in the schedule column. If there are one or more schedules defined the date and time of the next run will be displayed.

Schedule a Scan

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Locate the **Scheduled** column (on the far right).
3. In the corresponding row, click on the text: It will either appear as "schedule" (meaning no schedule has been created yet), or it will show the date and time of the next scheduled run (meaning a schedule has already been created).
4. Click on the **Add** button to define a schedule.
5. Select the Schedule properties you require.
6. Click on the **Save** button.
7. When you return to the scans list, you will see the date and time of the next scheduled run.

If a scan is scheduled to run more than once per day, but the first run has not completed by the time the next run is scheduled to begin, then this next run will be skipped.

Example:

Schedules: Daily at 3:00pm, 3:30pm and 4:00pm.
If the scan takes 70 minutes to run, then there will be only 1 scan result per day.

Schedules use the time zone defined in the **User preferences** under **Settings**. The default time is based on the locale set on the server hosting HiSoftware Compliance Sheriff. Hence, if a user in a different time zone wants to set a schedule on the actual date/time defined for the server, the time difference should be taken in consideration.

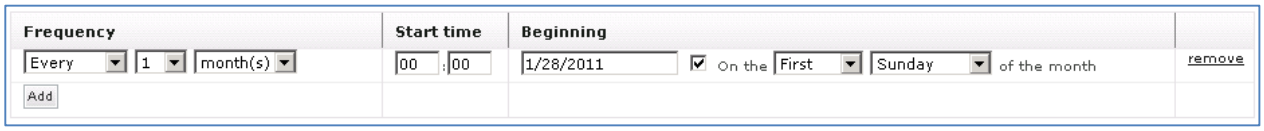
Edit a Scan Schedule

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Click on the current schedule defined for the scan under the **Scheduled** column.
3. You can edit the current Schedule properties defined: click **Add** to set another schedule for the scan, or click on the **Remove** link to remove a schedule.
4. Click **Add** to define a new schedule.
5. If you want to revert to a manual process, all schedules defined must be removed.
6. Click **Save**.
7. On returning to the scans list, you will see the date and time of the next scheduled run, as defined by the schedule you created.

Delete a Scan Schedule

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. Click on the current schedule defined for the scan under the **Scheduled** column.
3. Click on the **Remove** link in the far right column.
4. Click **Save**.
5. A confirmation dialog box will appear. Click on **OK** to confirm deletion.

Schedule Properties



Add
The **Add** button will create a schedule. Multiple schedules can be defined for a scan or monitor. The default start time is midnight on the following day.

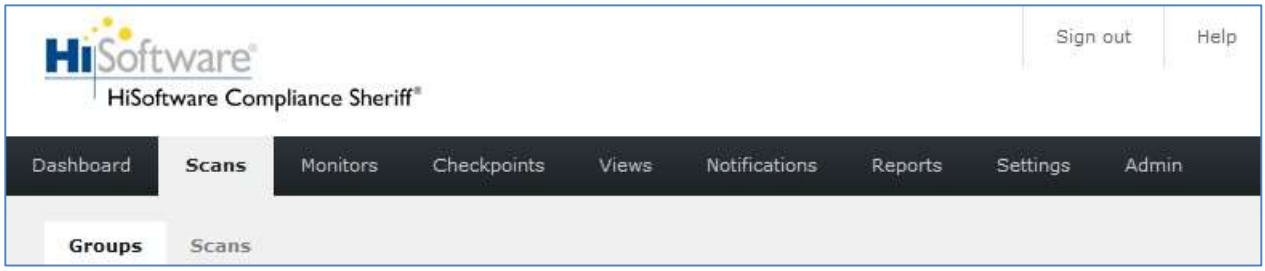
Beginning
Use the date field to specify the date the scan will commence.
If the frequency is set to **Month(s)**, check that the start date is not past the 28th of the month, or it will not run on months with fewer than 29 days.

Frequency
Use the three drop-down fields to define the interval between runs. The first drop-down contains two options: **Every**, for running a scan or monitor periodically, and **Run once**, for scheduling a single scan at some point in the future. If you choose **Every**, two further drop-down menus allow you to specify the number of days, weeks, or months between each run (**minutes** and **hours** are also available).

"On the" feature (for monthly scans only)
This feature allows the user to specify when a monthly scan should occur. Once **month(s)** has been selected from the third drop-down menu in the **Frequency** column, the **On the** check box will appear in the **Beginning** column, along with two drop-down menus. Put a check in the **On the** check box, and use the two drop-down menus to specify a time. If you wanted, for example, to schedule a monthly scan for the third Tuesday of every month, you would select **Third** from the first pull-down menu, and **Tuesday** from the second.

Start time
Use the **hour** and **minutes** fields to define the time of the day the scan or monitor will commence.

Scan Groups



If you have a high number of scans, creating scan groups can help you stay organized. By creating scan groups, you can easily access your scans by the matter they refer to, and you can combine the results of multiple scans into a single view or report.

Most customers choose to create scan groups based on regions of the world or business units. For example, if your organization uses different versions of its website in different regions, you could create a scan group for each region. You could also create different groups of scans for different departments in your organization.

When you click on the **Scans** tab and the **Groups** sub-tab, a list of all the scan groups you've created will appear on the screen. You can create a new scan group by clicking **New**, or delete a scan group by checking the appropriate box and clicking **Delete**. If you click **Toggle Filter**, text boxes will appear at the top of each column, and you can enter specific values into these boxes to filter your list. Check **Disable auto-update** if you don't want the page to refresh while you're selecting a range of scan groups.
For additional information, please choose one of the topics below.

Create a Scan Group

1. Click on the **Scans** tab, then click on the **Groups** sub-tab.
2. Click **New**.
3. In the **Display Name** field, type a name for the scan group. You can use long descriptive names.
4. In the **Group contains** field, select whether the scan group should include scans or subgroups (other scan groups). The available scans or subgroups will appear in the right-hand table. A scan group *cannot* include both scans and subgroups.
5. Put a check in the left-column box next to the scans or subgroups you would like to include in the scan group.
6. Click **Add** to add these scans or subgroups to your scan group.
7. If you've added a scan or subgroup in error and wish to remove it, put a check in the left-column box next to the scan or subgroup you wish to remove, and click **Remove**.
8. Click **Save**.

View the Contents of a Scan Group

1. Click on the **Scans** tab, then click on the **Scans** sub-tab.
2. In the **Group** field on the far right, select the scan group you wish to view from the pull-down menu.
3. The contents of the scan group will be displayed, and you may now run or schedule the individual scans in this scan group as needed. If your scan group contains other scan groups, the scans within the other scan groups will be displayed.
4. To create a view based on a scan group, follow these steps.

Edit a Scan Group

1. Click on the **Scans** tab, then click on the **Groups** sub-tab.
2. Locate the scan group you wish to edit, and click on its name.
3. To add additional scans or subgroups to a scan group, select **Scans** or **Subgroups** from the **Group contains** field. Then, on the right-hand table, put a check in the left-column box of the scans or subgroups you wish to add. Click **Add**. (A scan group *cannot* contain both scans and subgroups.)
4. To remove a scan or subgroup from a scan group, look for the scan or subgroups' name in the left-side **Display Name** field, click in the left-column box next to it, then click on the **Remove** button.
5. Click **Save**.

If you use the **Save as new** button to create a new scan group, you must change the **Display name** first.

Delete a Scan Group

1. Click on the **Scans** tab, then click on the **Groups** sub-tab.
2. Put a check in the left-column check box next to the scan group's name.

You can select more than one scan group to delete at a time.

To select or de-select all scan groups, you can double-click on the header cell of the check box column, located at the top left.

3. Click **Delete**.
4. A confirmation dialog box will appear. Select **OK** to confirm deletion.

If you elect to delete a scan group that has a view associated to it, a confirmation box will appear:

"One or more views refer to the scan group(s) you are deleting, and may not continue to function correctly." Choose **OK** to delete, or **Cancel** to abort.

View Scan Group Log File

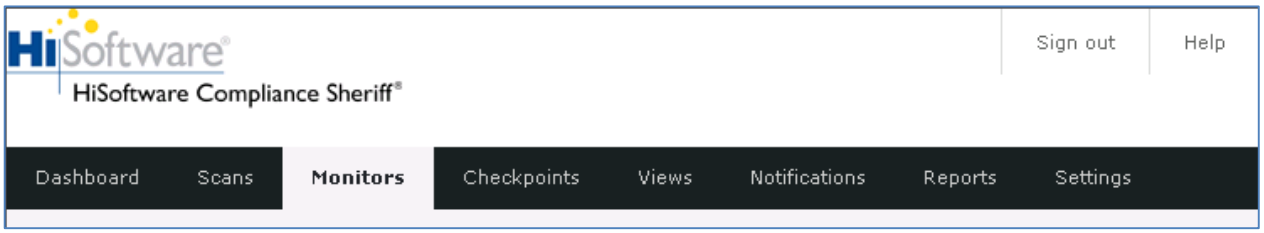
By combining time-stamped log messages from each scan contained with a group, HiSoftware Compliance Sheriff V4.2 allows you to filter past and present results by category: Debug, Info, and Error.

Debug refers to detailed information about a scan's progress, including an "Analyzing" message for every page processed. **Info** refers to information about a scan, including timings, IP address information, and redirections detected. **Error** refers to unexpected events, such as pages not being able to be downloaded or processed, or critical problems that prevent a scan from completing.

To access the log file, perform the following steps:

1. Click on the **Scans** tab, then click on the **Groups** sub-tab.
2. Click on the status link in the corresponding row. Status links are located in the **Status** column.
3. The log file for the last run will be displayed. Click or un-click the Debug, Info, and Error boxes to determine which results are displayed. You can also click on the any of the column titles (Type, Timestamp, Message, and Stack trace) to sort the results according to that column.

Monitors



A Monitor is a collection of Checkpoints that will be executed on the pages of a website. You can then use the Monitor results to create Views and reports from these results. By default, Monitors display Site Quality Checkpoints; however, a Monitor may use any Priority 1 Checkpoint.

Monitors protect specific pages of your site from serious threats. They are run more frequently than Scans, and are ideal for security issues. If you want a site page to have thorough protection, you want a Monitor.

When you click on the Monitors tab, a list of all the monitors you've created will appear on the screen. You can create a new monitor by clicking **New**, or delete a monitor by checking the appropriate box and clicking **delete**. if you click **toggle filter**, text boxes will appear at the top of each column, and you can enter specific values into these boxes to filter your list. check **disable auto-update** if you don't want the page to refresh while you are selecting a range of monitors.

Creating a new Monitor

1. Click on the **Monitors** tab.
2. Click **New**.
3. In the **Display Name** field, type a name for the monitor.

You can use long descriptive names.

4. In the **Base URL** field, type the path name of the site to be monitored, but do not enter sub-page name. For example, if you wanted to create a monitor on "http://mysite.com/en/", you would enter "http://mysite.com" in the **Base URL** field, and specify the sub-page "/en/" in the **Page** field. You can specify multiple sub-pages by clicking **Add** beneath the **Page** field.
5. In the **Checkpoint groups** table on the right, select the **Checkpoint groups** to be used by the monitor, then click **Add**. You must select at least one checkpoint.
6. If necessary, edit the transaction script by clicking **Edit** beneath the **Transaction Script** heading. (For more information, please visit the Transaction Scripts page.)
7. If a site requires a username and password to be monitored, or if you wish to specify the domain and/or the page limit of a monitor, click **Edit** beneath the **Options** heading.
8. The **Send alerts** field allows you to determine how you'll be notified of this monitor's results. Select the **Send alerts** type for this monitor in the **Send alerts** field. All options, except for **Never**, require a valid email address to be entered. You are required to select a **Send alerts** mode to create a new monitor.
9. At the bottom of the page, you will notice the **User-agent** field. Leave this at "(default)" unless your web server is configured to respond differently to different user-agent strings. For example, your web server may require that a string include Internet Explorer or Firefox.
10. Click **Save**.

Edit a Monitor

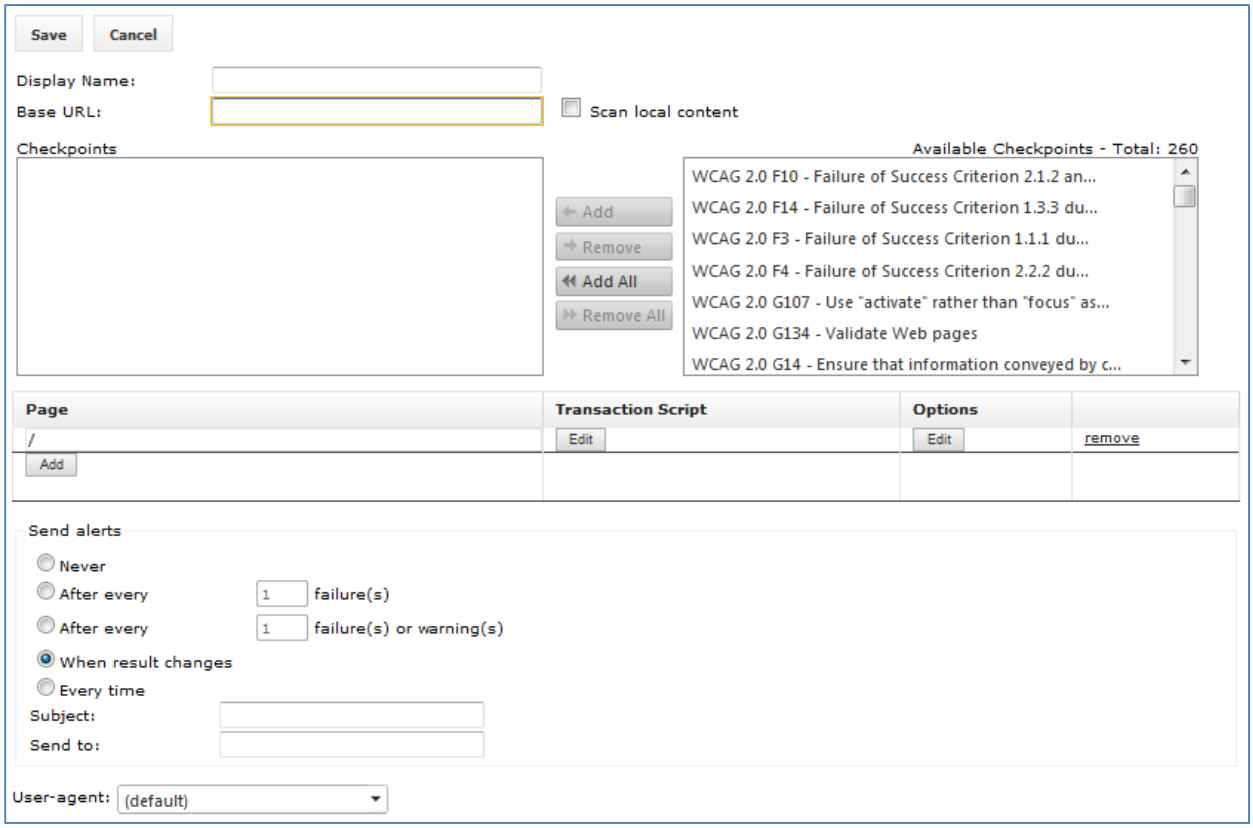
1. From the **Monitors** tab, locate the name of the monitor you wish to edit, and click on its name.
2. Modify the monitor properties as needed. To remove a checkpoint, look for the checkpoint's name in the left-side **Checkpoints** field, click in the box next to it, then click on the **Remove** button.
3. Click **Save**.

 If you use the **Save as new** button to create a new monitor, you must change the **Display name** first.

Delete a Monitor

1. Click the **Monitors** tab.
2. If the monitor you wish to delete is running, stop it first, using the **Stop** button on the far right.
3. Select the check box next to the monitor's name. You can select more than one monitor to delete at a time.
4. To select or de-select all monitors, you can double-click on the header cell of the check box column, located at the top left.
5. Click **Delete**.
6. A confirmation dialog box will appear. Select **OK** to confirm deletion.
7. Any results that may have existed for the monitor will be permanently deleted.
8. If you elect to delete a monitor that has a view associated to it, a confirmation box will appear: "One or more views refer to the monitor(s) you are deleting, and may not continue to function correctly." Choose **OK** to delete or **Cancel** to abort.

Monitor Properties



Add

Highlight one or more checkpoint groups in the right-hand table and click **Add** to include them in your monitor.

Add All

To add all of the checkpoint groups in your system to a monitor, click **Add All**.

Base URL

This defines the potential scope and limit of the monitor. A valid http:// or https:// URL should be entered. If you do not type http://, it will be added automatically. A Base URL must be defined for a monitor.

We recommend that you *do not* define sub-pages in the base URL. For example, use "http://mysite.com/" instead of "http://mysite.com/en/", and use the "Page" field to specify the "/en/" sub-page.

Checkpoints

A checkpoint is an instruction set that will check that a web page conforms to some predetermined rules or guidelines. A checkpoint must belong to a module, such as privacy, accessibility, or custom. See Modules in for more details. You can create new checkpoints within a module. You can also edit existing checkpoints; however, we recommend that you create a duplicate checkpoint and then edit the duplicate.

The right-hand table lists the remaining checkpoints defined for your system. The checkpoints included in the monitor can be changed by selecting one or more checkpoints on the left-hand or right-hand table, and clicking on the **Remove** or **Add** button, respectively.

Display name

This is the descriptive name for a monitor. It will be displayed on the list of monitors. The monitors list can be sorted by name by clicking **Monitors** on top title bar column.

Dynamically Generated Fields

This is a comma-separated list of form fields that hold typically session-based IDs that change every time you attempt an interaction. For instance, after recording a number of steps with the script recorder, you may notice steps like:

POST http://mysite.com/myapp.cgi, cmd=addtocart&sessionid=267ga672fe7afdbc25c

The value of the 'sessionid' field identifies the session to the web server, and is different every time you use the web application. If the script was simply replayed as is, it would most likely fail because the server is expecting a new session ID. If "sessionid" is listed as a dynamic generated field, then instead of simply sending the same value that was recorded initially, it finds the new value that was supplied by the server when the first step was executed (basically looking for a hidden form field with that name).

When you use the script recorder, it attempts to determine likely session ID fields automatically, but this is not always possible to do reliably. It should be checked after you finish recording.

Options

The **Options** menu can be accessed by clicking on the **Edit** button beneath the **Options** heading.

Username/Password/Domain

Use these options for sites requiring HTTP authentication (for example, when the browser displays a login dialog).

Page

Each entry defines the URL of the sub-page to be checked, relative to the base URL. The default is "/" which means the root or home page of your site. Multiple sub-pages can be defined.

Remove

Highlight one or more checkpoint groups in the left-hand table and click **Remove** to take them out of your monitor.

Remove All

To remove all of the checkpoint groups from a monitor, click **Remove All**.

Scan local content

The Toolbar from previous versions of HiSoftware Compliance Sheriff is no longer used to scan content on your local machine. Instead, by clicking the **Scan local content** check box, you can install the browser-agnostic local scan agent on your machine, and it will automatically upload local content to your Compliance Sheriff server for scanning. As such, most of the previous restrictions on local scans are now removed – you can schedule scans that check local content, results highlighting is supported, performance is increased, and logging is available to all users. However, please note that Transaction Scripts are now disabled when a local content scan is defined.

For more information, visit the Scan Local Content page.

Send Alerts

Alerts are text-only e-mail messages, sent when a Checkpoint returns a particular result. They contain only the information specified by the Checkpoint result message, rather than a full report. There are several options for how often a Monitor should send alerts:

- **Never**
- **After every *n* failure(s)**: If *n* is 1, an alert is sent every time a checkpoint returns a "Failed" result. For higher values of *n,* then at least *n* consecutive runs of the monitor must produce a "Failed' result before an alert is sent. For example, if a Monitor checks your website every 5 minutes to determine that the site is available, but you only wish to be alerted if the site is down for 15 minutes or greater, you would use an *n* value of '3'.
- **After every *n* failure(s) or warning(s)**: This is similar to the above, except that both "Failed" and "Warning" results are considered. For example, if you are using the default "Verify that page is available" Checkpoint for a Monitor that checks your website every 5 minutes, and you specify a value of '3', then you would be alerted if the first and second run determined that the site could not be accessed ("Failed"), and the third run determined that the site was available, but took longer than 10 seconds to download ("Warning").
- **When result changes**: This option causes alerts to be sent only when the result is different from the previous run. No alert will be sent the very first time the monitor runs.
- **Every time**

Subject

This allows you to customize the subject field of the notification e-mails you will receive.

Send to

Required setting that specifies the e-mail address to send the alert to. You may use a semi-colon to separate multiple addresses.

Transaction Script

A **Transaction script** is used to define user interactions required to access portions of a site. For example, to scan pages in a shopping cart site, you will need to log-in, select an item, and check out. To create a **Transaction script,** click on the **Edit** button beneath the "Transaction script" heading. A script can be typed in the field provided (see Transaction script commands in this chapter) or by using the recorder facility.

User-agent

This option may be used if your web server is configured to respond differently to different user agent strings. For instance, it may require that string include “IE” or “Firefox”. HiSoftware Compliance Sheriff is configured with sample User-agent strings as listed in the drop-down list, along with a “default” option. To edit or add user-agent string to this list, see Chapter 10: User agents under the **Settings** tab. You can find more information on User-gent strings at the MSDN library: http://msdn2.microsoft.com/en-us/library/ms537503.aspx

The default user-agent string is internally defined as: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; HiScan).

Run Monitors

Monitors can be run on demand or be scheduled to run at regular intervals.

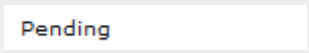
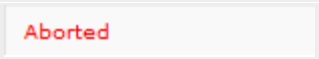
Run a Monitor

1. Click on the **Monitors** tab.
2. Find the monitor you wish to execute and click **Run**, located at the far right of the row. **Run** launches the monitor immediately. If the monitor is marked as "local" in the **Base URL** column, it will run on your own machine. This option requires the HiSoftware Toolbar.
3. The status will change to "Running".

Monitors can also be started automatically by setting up a Schedule.

Monitor Status

The status of the monitor will depend on its current state of activity, or the success of the most recent monitor.

Icon	Status	Description
	None	The monitor has not been run.
	Pending	The monitor has been launched, but is not able to run yet.
	Running	The monitor is currently in progress.
	Passed	The monitor completed successfully, and a health value generated.
	Passed with warnings	The monitor completed with some warnings, and a health value generated.
	Failed	The monitor completed, but one or more pages failed to pass all the checkpoints.
	Aborted	The monitor failed to complete properly. See Troubleshooting for additional information.

You can view the results of the monitor in detail by clicking on the status description (located beneath the "Status" heading), or using the ENTER key to activate the link.

Stop a Monitor

1. Click on the **Monitors** tab.
2. Check that the monitor status shows as **Running**.
3. Click on the associated **Stop** button to stop the Monitor. The **Stop** button is located in the same place as the **Run** button, at the far right of the row.

View Monitor results

1. Click on the **Status** field of a monitor.
2. The log file of that monitor will be displayed. Click on the **Show Results** field.
3. The properties for a view will be displayed. If you have previously specified a view, the view properties will be remembered. (For more information on view properties and how to manage them, please consult the Views section of this document.)

The view will only show the results of the current monitor.

4. Click **Save** to save the results and view properties of this monitor. To cancel, click **Cancel**.

View Monitor Log File

By combining time-stamped log messages from multiple monitor runs, HiSoftware Compliance Sheriff V4.2 allows you to filter past and present results by category: Debug, Info, and Error. **Debug** refers to detailed information about monitor progress, including an "Analyzing" message for every page processed. **Info** refers to information about the monitor, including timings, IP address information, and redirections detected. **Error** refers to unexpected events, such as pages not being able to be downloaded or processed, or critical problems that prevent the monitor from completing.

1. In the monitors tab, click on the status link in the corresponding row. Status links are located in the **Status** column.
2. The log file for the last monitor will be displayed.
3. The log file for the last monitor will be displayed. Click or un-click the Debug, Info, and Error boxes to determine which results are displayed. You can also click on the any of the column titles (**Type**, **Timestamp**, **Message**, and **Stack trace**) to sort the results according to that column.

Export Monitor Results

You can export the results of a monitor to a CSV file.

1. In the monitors tab, find the monitor you wish to export and click on the status link in the corresponding row. Status links are located in the **Status** column.
2. Navigate to the **Export to CSV** field.
3. From the drop-down menu, select the type of data you wish to export. For more specific options, click **Advanced**.
4. Once you've selected a data type, click **Go**.
5. You will be prompted to **Open** or **Save** the file.
   Example:
   You can export visual checks to a CSV, perform the visual checks, update the CSV, and then update the database.

Purge Monitor Results

1. Click on the **Monitors** tab.
2. Find the monitor whose results you wish to purge and click on the status link in the corresponding row. Status links are located in the **Status** column.
3. Click on one of the purge buttons:
   - **Purge all** deletes all runs, including the one most recently completed, so that no results will be available for this monitor.
   - **Purge old** deletes all runs except the one most recently completed.
   - **Purge latest** deletes only the most recently completed run.

 Purging means that the results are PERMANENTLY deleted from the database. Deleted results cannot be recovered, so use with care. Typically you should only need to use this if your database has become cluttered with “test” results that you are absolutely sure you no longer need.

Schedule Monitors

A monitor can be scheduled to run at predetermined intervals. Multiple schedules can be defined for a monitor. If a monitor has no schedule defined, the text "schedule" will be displayed in the schedule column. If there are one or more schedules defined, the date and time of the next run will be displayed.

Schedule a Monitor

1. Click the **Monitors** tab and locate the **Scheduled** column (on the far right).
2. In the corresponding row, click on the text: It will either appear as "schedule" (meaning no schedule has been created yet), or it will show the date and time of the next scheduled run (meaning a schedule has already been created).
3. Click on the **Add** button to define a schedule.
4. Select the Monitor Schedule properties you require.
5. Click **Save**.
6. When you return to the monitors list, you will see the date and time of the next scheduled run.

If a monitor is scheduled to run more than once per day, but the first run has not completed by the time the next run is scheduled to begin, then this next run will be skipped.

Example:

Schedules: Daily at 3:00pm, 3:05pm and 3:10pm.
If the monitor takes 7 minutes to run, then there will be only 2 monitor results per day.

Schedules use the time zone defined in the **User preferences** under **Settings**. The default time is based on the locale set on the server hosting HiSoftware Compliance Sheriff. Hence, if a user in a different time zone wants to set a schedule on the actual date/time defined for the server, the time difference should be taken in consideration.

Edit a Monitor Schedule

1. Navigate to the **Monitors** tab.
2. Click on the current schedule defined for the monitor under the **Scheduled** column.
3. You can edit the current Schedule properties defined: click **Add** to set another schedule for the scan, or click on the **remove** link to remove a schedule.
4. Click **Add** to define a new schedule.

If you want to revert to a manual process, all schedules defined must be removed.

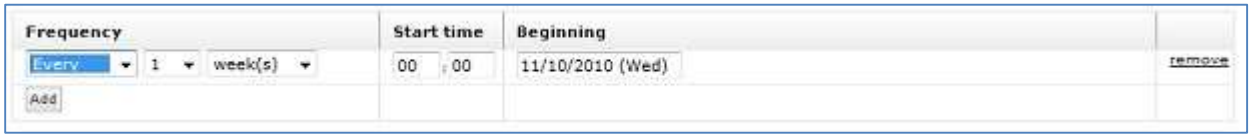
5. Click **Save**.

On returning to the monitors list, you will see the date and time of the next scheduled run, as defined by the schedule you created.

Delete a Monitor Schedule

1. Navigate to the **Monitors** tab.
2. Click on the current schedule defined for the Monitor under the **Scheduled** column.
3. In the far right column, click on the **Remove** link.
4. Click **Save**.
5. A confirmation dialog box will appear. Click **OK** to confirm deletion.

Monitor Schedule Properties



Add

The **Add** button will create a schedule. Multiple schedules can be defined for a monitor or scan.

The default start time is midnight on the following day.

Beginning

Use the date field to specify the date the monitor will commence.

If frequency is set to **Month(s)**, check that the start date is not past the 28th of the month, or it will not run on months with fewer than 29 days.

Frequency

Use the three drop-down fields to define the interval between runs. The first drop-down contains two options: **Every**, for running a scan or monitor periodically, and **Run once**, for scheduling a single monitor at some point in the future. If you choose **Every**, two further drop-down menus allow you to specify the number of days, weeks, or months between each run (**minutes** and **hours** are also available). For example, to schedule a monitor to check for changes every day, set the frequency to either **Every 24 hours** or **Every 1 day**.

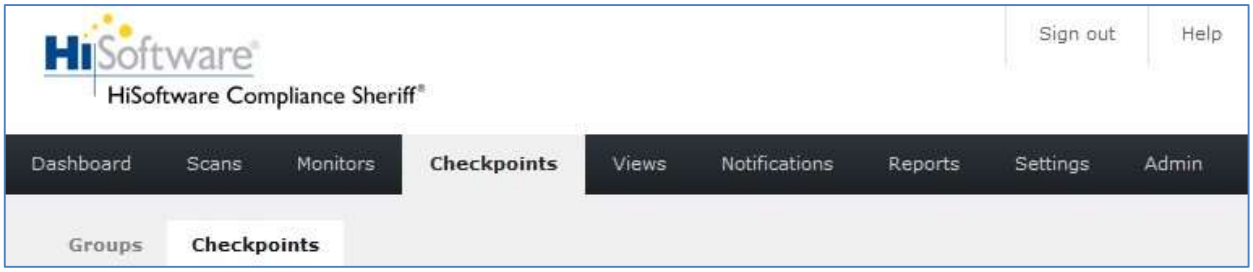
Start time

Use the **hour** and **minutes** fields to define the time of the day the monitor or scan will commence.

Weekday of the month

This option is only available if the **Frequency** period selected is **month(s)**. Click on the check box in the first column to define which weekday of the month the monitor will start.

Checkpoints

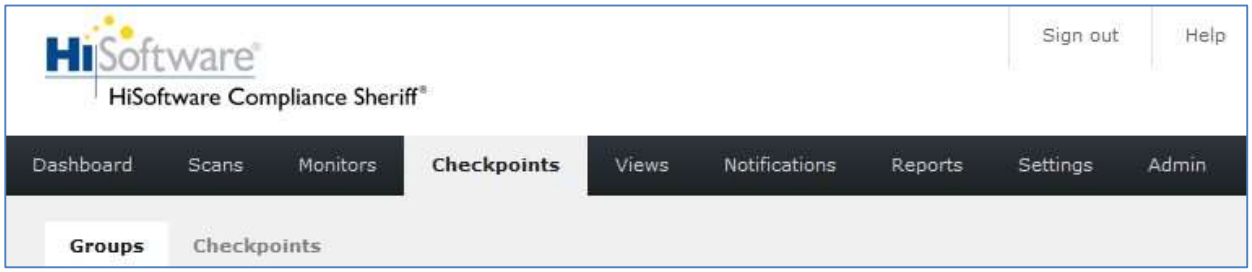


A checkpoint is an instruction set that will check that a web page conforms to predetermined rules or guidelines. A checkpoint must belong to a module, such as privacy, accessibility, or custom. On the checkpoints landing page, you can sort your checkpoints by module: make a selection from the **Module** pull-down menu to view only the checkpoints contained in that module. (See Modules for more information.)

Customize Checkpoints

Although the checkpoints provided with the software are designed to give useful results "out-of-the- box", it is recommend that you read this section to determine which checkpoints should be customized, and how. This will help you achieve more accurate results that are tailored to the design of your organization's website.

Checkpoint Groups

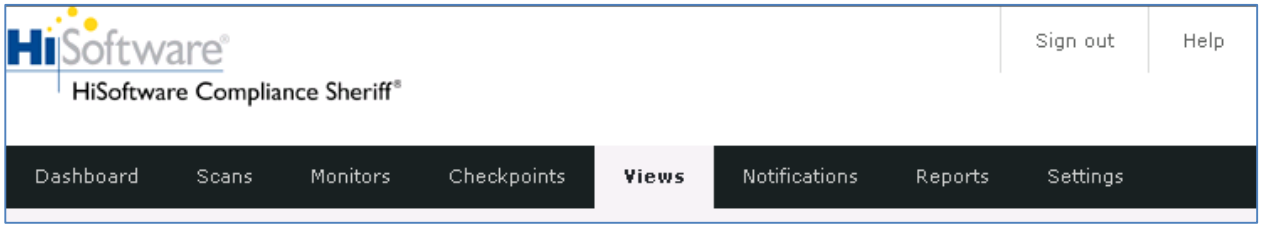


A checkpoint group is a collection of checkpoints, or a collection of other checkpoint groups. A checkpoint group contained within another checkpoint group is called a subgroup. A checkpoint group is not allowed to contain itself, and it cannot contain a checkpoint *and* a subgroup.

Checkpoint groups allow you to collect related checkpoints for easy assignment to scans. Checkpoint groups are also useful when constructing views of results. Being able to report by checkpoint group and subgroup will allow you to more effectively present the results of a scan or monitor.

All CSU campuses will be using the CSU ATI Checkpoints.

Views



A view is a presentation of data from the results database. A view may contain a graphical chart, a textual summary, or table of results.

When you click the **Views** tab, a list of the views you have created will appear, along with the date they were last modified. To see what a view looks like, click the **preview** icon in the appropriate row (the icon is a small magnifying glass). Similarly, you can also generate a report from any view. If you have created a long list of views, use the **Search** field to find the view you're looking for.

All dates and times displayed use the time zone specified in the user's preferences.

Create a View

1. Click the **Views** tab.
2. Click **New**.
3. In the **Name** field, enter a name for the view.
4. In the **Show results for** field, you will see three options: scans, scan groups, or monitors. Choose which category you want the view to show results for.
5. If you selected **scans** in Step 4, a Scans menu will appear in the field below. From this field, choose which scan or scans you would like to be associated with the view (you can select multiple items from each scroll-down menu by holding the CTRL button). If you selected **scan groups** on **monitors**, the process is the same. If you have already run the scan(s), scan group, or monitor(s) associated with this view, a preview of the view will appear in the preview pane as you make your selections. Click **Disable auto-update** if you don't want the preview pane to reload each time you make a change. If you choose this option, you can use the **Update** button to refresh the preview.
6. In the Checkpoint Groups field (or Checkpoints field, if you've selected a monitor), select which checkpoint groups should appear in the view. (PLEASE NOTE: You can open or close each field on this page by clicking the arrow buttons in the upper right of each field.)
7. In the Pages field, you can select the specific URLs that the view will display results for.
8. Modify the Chart, Summary, and Table fields as desired.
9. Click the **Save** button.

Edit a View

1. Click on the **Views** tab.
2. Locate the View you wish to edit and click on its name. This will take you to the editing page. Before selecting a View to edit, you can click on the preview command next to its name to display the View in the RHS pane.
3. Modify the View properties (see this chapter) as needed.
4. Click on the **Save** button.

 If you use the **Save as new** button to create a new view, you must change the name first.

Delete a View

1. Click on the **Views** tab.
2. Find the View you wish to delete and click in the checkbox to the left of its name, in the first column of the table.
3. Click on the **Delete** button.
4. A confirmation dialog box will appear. Select "OK" to confirm deletion.

If a View is being used in the Dashboard a different confirmation will appear: "One or more user dashboards refer to the View(s) you are deleting, and may not continue to function correctly." Choose **OK** to Delete, or **Cancel** to abort.
You can select more than one view to delete at a time.

Generate a Report

Views can be displayed in both a dynamic, expandable form (as per the Dashboard and the preview command) and in a static report form suitable for e-mailing, printing, or archiving.
To generate a report from a view definition:

1. Click on the **Views** tab.
2. Locate the view you wish to generate a report from. In the same row as this view, click the appropriate icon. You have two options:
   a. **Open report for "[View name]" in a new window**. (This will be an HTML page.)
   b. **Open PDF report for "[View name]" in a new window**.

You can create a Notification to schedule automatic creation and e-mailing of reports.

View Properties

Name
This is the display name of the view, used in the title bar for tabs or panels on the dashboard, and as the title for any generated reports.
Show results for
Use this option to determine whether your view will show results from scans, scan groups, or monitors. This option determines the remaining available properties.

Properties for views showing scan results

Scans
From this field, choose which scan or scans you would like to be associated with the view. You can select multiple scans by holding the CTRL button. If you have already run the scan(s) associated with this view, a preview of the view will appear in the preview pane as you make your selections. Click **Disable auto-update** if you don't want the preview pane to reload each time you make a change. If you choose this option, you can use the **Update** button to refresh the preview.

Checkpoint Groups
In the Checkpoint Groups field, select which checkpoint groups should appear in the view. You can select multiple checkpoint groups by holding the CTRL button.
By default, the results for all checkpoint groups (as selected in the scan definitions) are included in the view. However, you may choose to report on specific groups.

Pages
In the Pages field, you can select specific URLs that the view will display results for. (PLEASE NOTE: Depending on the scans you've selected, this field may be blank.)

Chart
In the Chart field, you can select a type of chart to display the data you have selected.

Summary
In the Summary field, you can enable or disable the display of information from the scan summary in your view. This information can include any (or none) of the following items:

- Date/Time scan started
- Date/Time scan completed
- Number of pages scanned
- Number of checkpoints tested
- Accessibility statistics

To show the complete set of accessibility statistics, ensure that you add the checkpoint group "Accessibility Statistics" to the scan property.

The summary information is always for the most recently completed scan.

Table
There are various types of tables available for display in the view. All table types show data for the last completed scan.

Properties for views showing scan group results

Scan Groups
From this field, choose which scan groups you would like to be associated with the view. You can select multiple scan groups by holding the CTRL button. If you have already run the scan group(s) associated with this view, a preview of the view will appear in the preview pane as you make your selections. Click **Disable auto-update** if you don't want the preview pane to reload each time you make a change. If you choose this option, you can use the **Update** button to refresh the preview.

Checkpoint Groups
In the Checkpoint Groups field, select which checkpoint groups should appear in the view. You can select multiple checkpoint groups by holding the CTRL button.
By default, the results for all checkpoint groups (as selected in the scan group definitions) are included in the view. However, you may choose to report on specific checkpoint groups.

Example:

> You have configured three scan groups on www.mysite.com, products.mysite.com and support.mysite.com, respectively, and have included all possible checkpoint groups in each scan group. If you only want to view privacy issues in the support area, then you would select "support.mysite.com" from the list of scan groups, and the checkpoint groups beginning with "Privacy -" from the list of checkpoint groups.

Pages
In the Pages field, you can select the specific URLs that the view will display results for. (PLEASE NOTE: Depending on the scan groups you've selected, this field may be blank.)

Chart
In the Chart field, you can select a type of chart to display the data you have selected.

Summary
In the Summary field, you can enable or disable the display of information from the scan group summary in your view. This information can include any (or none) of the following items:

- Date/Time scan started
- Date/Time scan completed
- Number of pages scanned
- Number of checkpoints tested
- Accessibility statistics

To show the complete set of accessibility statistics, ensure that you add the checkpoint group "Accessibility Statistics" to the scan group property.

The summary information is always for the most recently completed scan group.

Table
There are various types of tables available for display in the view. All table types show data for the last completed scan group.

Properties for views showing monitor results

Monitors
From the Monitors field, select which monitor(s) should appear in the view. You can select multiple monitors by holding the CTRL button. If you have already run the monitor(s) associated with this view, a preview of the view will appear in the preview pane as you make your selections. Click **Disable auto-update** if you don't want the preview pane to reload each time you make a change. If you choose this option, you can use the **Update** button to refresh the preview.

Checkpoints
In the Checkpoints field, select which checkpoints should appear in the view. You can select multiple checkpoints by holding the CTRL button.

By default, the results from all checkpoints are included. However, you may select individual checkpoints to report on if needed.

Example:

> You have configured three monitors on www.mysite.com, products.mysite.com and support.mysite.com, respectively, and have included all the checkpoints in every monitor. If you only want to view the link validation results for the support area, you should select "support.mysite.com" from the list of monitors, and "Validate all links" from the list of checkpoints.

Reporting Period

Length: The length of time for which the view is to show results.
Ending: The time point that defines how recent the results shown should be.

Example:

> A monitor has been running for a week, once every hour. You wish to view the results for a 12-hour period, but you do not wish to include the most recent 2 hours. You should set Length to "12 Hours", and the Ending to "2 hours ago".

Chart
You can select a chart to display the data you have selected.

Summary
In the Summary field, you can enable or disable the display of information from the monitor summary in your view. The summary can include any (or none) of the following items:

- Reporting period start Date/Time
- Reporting period end Date/Time
- Number of pages monitored
- Number of checkpoints tested

Table
Only a single table type, History, is available for views showing monitor results. See Tables for more information.

View Charts

Charts for views showing scan results

The chart types available for scan results are:

Health
A health chart shows the percentage of pages that passed the scan(s). Health charts can be displayed as a gauge or a line chart. (See below for more information on the display options.)

Page compliance
The page compliance chart shows the number of pages that pass or fail. You also have options to distinguish warnings and visual checks using the results of the most recently completed scan, or use detailed ALT text--this will make the ALT text show up in the text of the issue, and you can hover over an image to see the total text. Page compliance charts can be displayed as a gauge, pie chart, or bar chart.

Result metrics
Unlike page compliance charts, result metrics charts show the total number of failures and passes, but the results are not grouped by page. You still have options to distinguish warnings and visual checks using the results of the most recently completed scan, or use detailed ALT text. Result metrics charts can be displayed as pie charts or bar charts.

Failures by Priority
These charts show what percentage of failures were Priority 1 and what percentage were Priority 2. They can be displayed as pie charts or bar charts. (See Checkpoint Properties for more information on priority settings.)

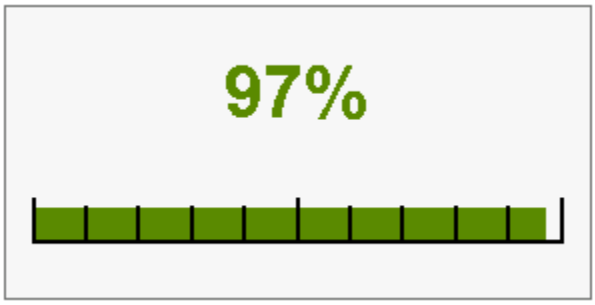
Failures by Group
These charts show what percentage of failures were associated with each checkpoint group. They can be displayed as pie charts or bar charts. They can also be filtered to display only Priority 1 checkpoint groups; Priority 1 and 2; or Priority 1, 2, and 3.

None
Select this option if you don't want a chart to be displayed.

As stated above, each chart type has different display options, which you select from the **Show as** field. These options are described below.

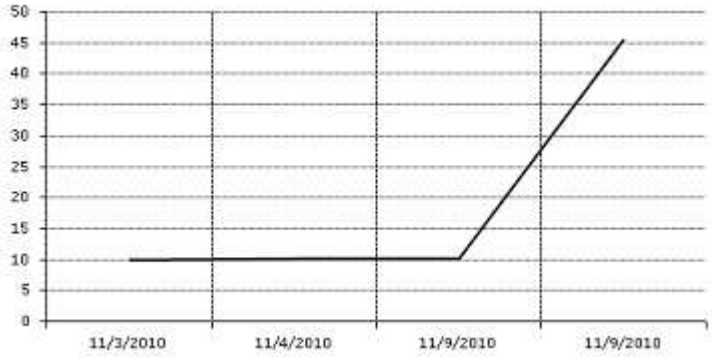
Gauge

A gauge shows the percentage of pages that passed all checkpoints. Warnings are not included.



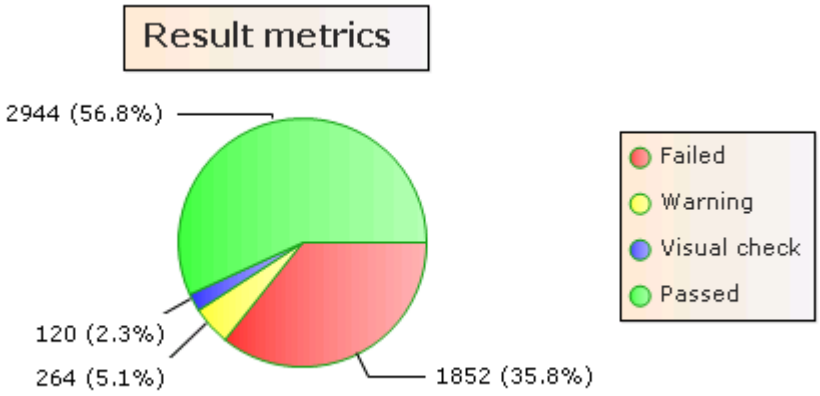
Line chart

A line chart shows the run progress over time.



Pie chart

A pie chart shows the percentages for "passed" and "failed" in the form of a pie chart. Additional slices can be shown for warnings and visual checks. Otherwise, they are rolled into the “passed” category.



Bar chart

A bar chart shows page compliance against a secondary (X) axis. See the **Bar chart options** link below for more information.

Charts for views showing scan group results

The chart types available for scan group results are:

Health
A health chart shows the percentage of pages that passed the scan group(s). Health charts can be displayed as a gauge or a line chart. (See below for more information on the display options.)

Page compliance
The page compliance chart shows the number of pages that pass or fail. You also have options to distinguish warnings and visual checks using the results of the most recently completed scan group, or use detailed ALT text--this will make the ALT text show up in the text of the issue, and you can hover over an image to see the total text. Page compliance charts can be displayed as a gauge, pie chart, or bar chart.

Result metrics
Unlike page compliance charts, result metrics charts show the total number of failures and passes, but the results are not grouped by page. You still have options to distinguish warnings and visual checks using the results of the most recently completed scan group, or use detailed ALT text. Result metrics charts can be displayed as pie charts or bar charts.

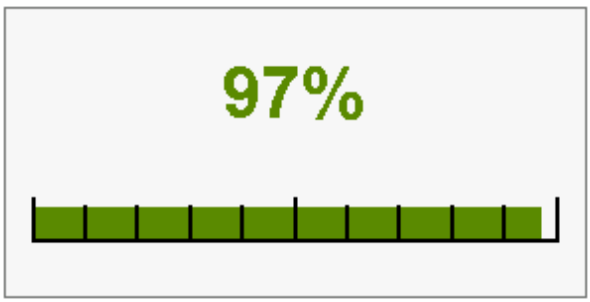
Failures by Priority
These charts show what percentage of failures were Priority 1 and what percentage were Priority 2. They can be displayed as pie charts or bar charts. (See Checkpoint Properties for more information on priority settings.)

Failures by Group
These charts show what percentage of failures were associated with each checkpoint group. They can be displayed as pie charts or bar charts. They can also be filtered to display only Priority 1 checkpoint groups; Priority 1 and 2; or Priority 1, 2, and 3.

None
Select this option if you don't want a chart to be displayed.

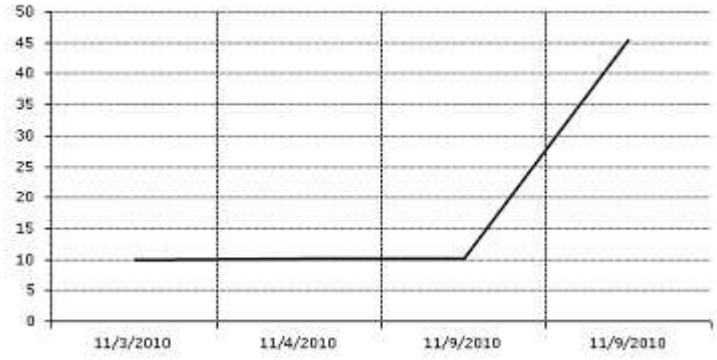
As stated above, each chart type has different display options, which you select from the **Show as** field. These options are described below.

Gauge
A gauge shows the percentage of pages that passed all checkpoints. Warnings are not included.



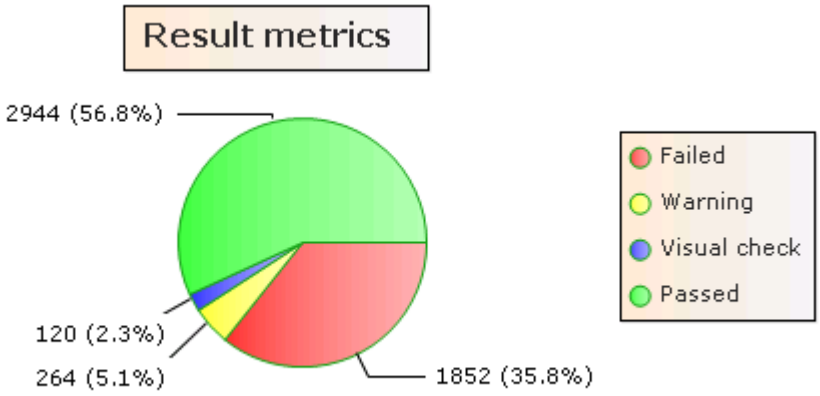
Line chart

A line chart shows the run progress over time.



Pie chart

A pie chart shows the percentages for "passed" and "failed" in the form of a pie chart. Additional slices can be shown for warnings and visual checks. Otherwise, they are rolled into the “passed” category.



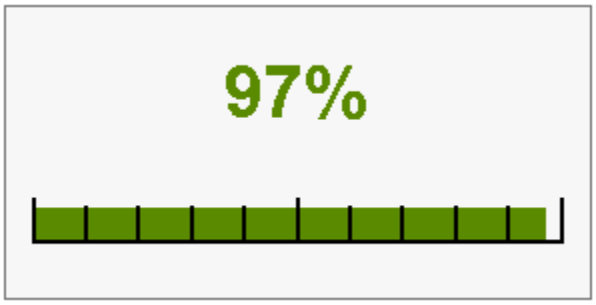
Bar chart

A bar chart shows page compliance against a secondary (X) axis. See the **Bar chart options** link below for more information.

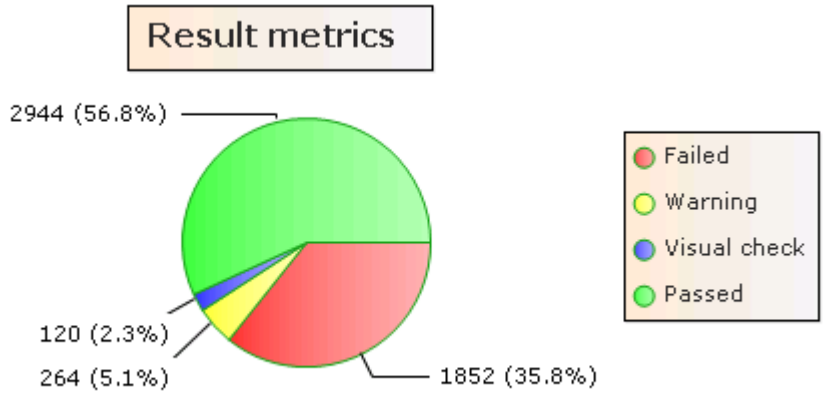
Charts for views showing monitor results

The chart types available for monitors are:

Health
Health charts display a gauge of the health index for the selected monitoring period. The health index is calculated from the number of failures and warnings encountered across the entire result set. Warnings have half the weighting of failures.



Result Metrics
Result metrics charts show all possible results as a pie chart. Additional slices can be shown for warnings and visual checks, which are otherwise considered a "pass" result.



None
Select this option if you don't want a chart to be displayed.

Bar chart options

All chart types other than **Health** can be plotted as a bar chart, with the X-axis being either:

- **Scan**
- **Checkpoint Group**
- **Time**

For the **Failures by checkpoint group** chart, you cannot select **checkpoint group** for the X-axis.

For **scan**, the names of each scan are displayed as labels on the X-axis (very long scan names are unsuitable for display).

Likewise, for **checkpoint group**, the names of each checkpoint group are displayed as labels on the X-axis.

The full checkpoint group is not necessarily displayed. If multiple groups are selected, and they start with the same text followed by a "-", that part from the chart (or the table) will be truncated.

Example:

WCAG 1.0 – SubGroup1
WCAG 1.0 – SubGroup2
The chart and table will show
SubGroup1
SubGroup2

For **Time**, you will need to specify what each X-axis point (and corresponding bar) represents, using the **Step by** field:

Step by Runs
Step by Months
Step by Quarters

You can then specify how many bars to draw, using the **Show Last** field.

When **Step by** is "Runs", each bar represents the result of a single run, no matter when they occurred. For example, if you had run your scan 5 times during the day, typing "3" in the "Show last" field will cause the final 3 of those runs to be shown.

When **Step by** is "Months", each bar represents the result of the final run of each month, including the current month.

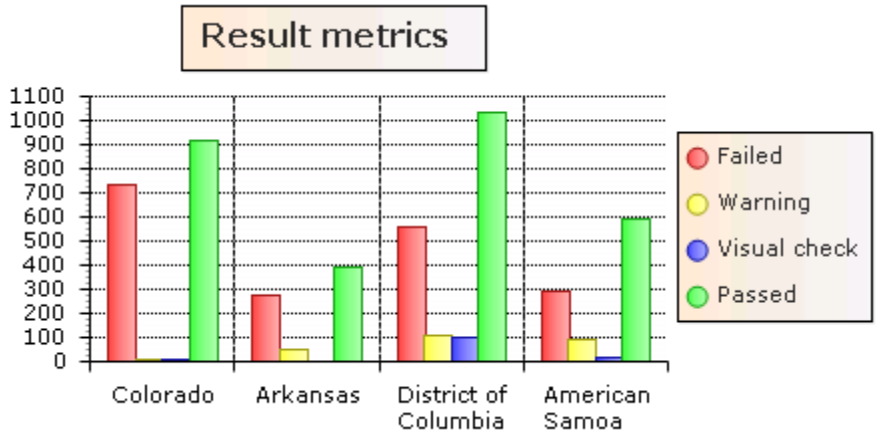
For example, if the current date is 2-Mar-2007, and your scan is scheduled to run on the first and 15th day of each month, typing "3" in the "Show last" field will cause the results for 15-Jan-2007, 15-Feb-2007, and 1-Mar-2007 to be shown. After March 15th, the third bar will show the result for that run.

When **Step by** is "Quarters", each bar represents the result of the final run for the preceding calendar quarters, not including the current quarter.

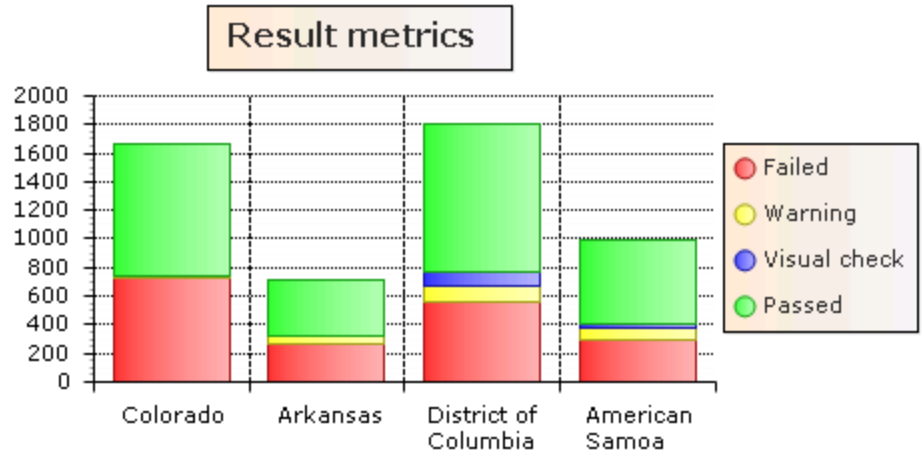
For example, if the current date is 2-Jul-2007, and your scan is scheduled to run on the first day of every month, typing "3" in the "Show last" field will only summon the results for 1-Mar-2007 (Q1) and 1-Jun-2007 (Q2). No result exists for the quarter before that, so there is no 3rd bar. The bar for Q3 will not be shown until 1-Oct-2007.

Lastly, you can choose to show the **Bars** as:

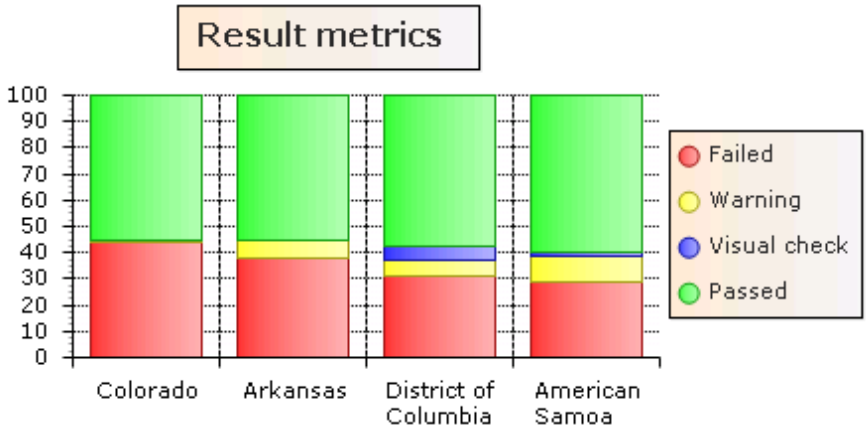
Clustered



Stacked



Full stacked



View Tables

Tables for views showing scan results

The following table types are available:

Page compliance
The page compliance table shows the individual checkpoint results in an expandable tree, and includes a page count and percentage for each result type (Failed, Warning, Visual, Passed and N/A).

By default, the results can be grouped as follows:

- By result value, then page, then checkpoint group, then checkpoint
- By result value, then page, then checkpoint
- By result value, then scan, then page, then checkpoint group, then checkpoint.

You can customize groupings by accessing Table groupings, located in the Settings tab. Note that the first level of the Page compliance table should always be "Result".

The sort order of the entries at each level is automatic: all entries are first sorted by the associated result value. Scans and pages are sorted by the order in which they were processed, checkpoints are sorted by their internal IDs (which, for standard checkpoints, corresponds to their Number property), and checkpoint groups are sorted according to the order they are defined within a scan.

Issue identification
The Issue Identification table shows the individual checkpoint results in an expandable tree, with columns for showing the number of failures in each top-level group.

By default, the table can be grouped as follows:

- By checkpoint group, then by checkpoint, then page
- By checkpoint group, then priority, then checkpoint, then page
- By scan, then by checkpoint group, then checkpoint, then page
- By scan, then page, then group, then checkpoint
- By checkpoint group, then priority, then page, then checkpoint
- By page, then checkpoint group, then checkpoint.

You can customize groupings by accessing Table groupings, located in the Settings tab.

See the entry for **Page Compliance** tables below for more information on the sort order of table entries.

Occurrences
The Occurrences table is designed to help track issues that reoccur across a large number of pages on a web site. Read more about occurrences tables here.

Links analysis
The links analysis table is designed to assist you in finding broken links, and to generate a basic site map of the link structure of your site.

For every page or resource found by the scan, you can view the status (typically an HTTP status code such as 404), the content-type, the size in bytes, the number of links in and out, and the last modified date/time.

The table can optionally be grouped by Status, Content-Type, Last Modified date, or "File Type", a user-definable grouping.

File types
This is a variation of the links analysis table that simply lists information about the files successfully accessed while crawling your website.

Score card
See How to Create a View for a Scorecard.

Scan summary
See How to Create a View for a Scan Summary.

None
Choose this option if you don't want a table to be displayed in your view.

Tables for views showing scan group results

The following table types are available:

Page compliance
The page compliance table shows the individual checkpoint results in an expandable tree, and includes a page count and percentage for each result type (Failed, Warning, Visual, Passed and N/A).

By default, the results can be grouped as follows:

- By result value, then page, then checkpoint group, then checkpoint
- By result value, then page, then checkpoint
- By result value, then scan, then page, then checkpoint group, then checkpoint.

You can customize groupings by accessing Table groupings, located in the Settings tab. Note that the first level of the Page compliance table should always be "Result".

The sort order of the entries at each level is automatic: all entries are first sorted by the associated result value. Scans and pages are sorted by the order in which they were processed, checkpoints are sorted by their internal IDs (which, for standard checkpoints, corresponds to their Number property), and checkpoint groups are sorted according to the order they are defined within a scan.

Issue identification
The Issue Identification table shows the individual checkpoint results in an expandable tree, with columns for showing the number of failures in each top-level group.

By default, the table can be grouped as follows:

- By checkpoint group, then by checkpoint, then page
- By checkpoint group, then priority, then checkpoint, then page
- By scan, then by checkpoint group, then checkpoint, then page

- By scan, then page, then group, then checkpoint
- By checkpoint group, then priority, then page, then checkpoint
- By page, then checkpoint group, then checkpoint.

You can customize groupings by accessing Table groupings, located in the Settings tab.

See the entry for **Page Compliance** tables below for more information on the sort order of table entries.

Occurrences
The Occurrences table is designed to help track issues that reoccur across a large number of pages on a web site. Read more about occurrences tables here.

Links analysis
The links analysis table is designed to assist you in finding broken links, and to generate a basic site map of the link structure of your site.
For every page or resource found by the scan, you can view the status (typically an HTTP status code such as 404), the content-type, the size in bytes, the number of links in and out, and the last modified date/time.
The table can optionally be grouped by Status, Content-Type, Last Modified date, or "File Type", a user-definable grouping.

File types
This is a variation of the links analysis table that simply lists information about the files successfully accessed while crawling your website.

Score card
See How to Create a View for a Scorecard.

Scan summary
See How to Create a View for a Scan Summary.

None
Choose this option if you don't want a table to be displayed in your view.

Tables for views showing monitor results

The History table is an expandable tree that shows all results as recorded over the reporting period, in chronological order.
The tree can grouped into levels, with the following groupings available by default:

- By checkpoint, then page
- By page, then checkpoint
- By monitor, then page, then checkpoint

You can customize groupings by accessing Table groupings, located in the Settings tab.

Below is an example of a table where the first level is checkpoint and the second level is page.

Show failures & warnings only: Use this option to hide any entries where the monitor result was 'Passed', 'Visual' or 'N/A'.

Show changes only: Use this option so that consecutive entries with the same result are compressed into a single entry. The timestamps in the table can be used to determine how long a particular result was relevant for.

Table options

Table options

Group by
Refer to the information above about various table types for an explanation of this field.

Show column for priority 1 issues
This option only applies to the **Issue Identification** table type. Uncheck this to hide the column that counts priority 1 failures for each top-level group.

Show only differences to previous run
This option (not available for **Links Analysis**) causes the tree to reflect only results that have changed since the previous runs of the scans involved. For example, if page `index.html` failed checkpoints Accessibility 1.1.1 but passed Accessibility 1.1.2 on run 1, but on run 2 it passed both checkpoints, then only the fact that it passed 1.1.1 would be taken into consideration. Hence, only this checkpoint would be included in the report for that page. If, however, on run 2, it failed both checkpoints, only the fact that Accessibility 1.1.2 has failed would be shown in the report, as the result had not changed for Accessibility 1.1.1.

Include (Failures, Warnings, Visual checks, Passes, N/As)
This set of options allows you to choose which result types are included in the table. For page compliance tables, this only affects which top-level entries are expandable to see the full details. For links analysis tables, "Failures" refers to links that could not be successfully accessed (i.e. did not return an HTTP 200 success code), "Passes" refers to links that were successfully accessed, and "N/A" refers to link types that cannot be tested (e.g. mailto: links).

Use Relative URLs
This option causes all URLs in the report to be displayed relative to the Base URL of the first scan selected.

Maximum list length

This option controls the maximum number of entries shown in any table group. This prevents the table from becoming too unwieldy when dealing with large result sets, but some of the reports may be truncated. Note that you can set different list lengths for different levels by separating values with commas: e.g. "50,5" means that the top level list should only be truncated if there are more than 50 entries, while each sub-list (and sub-sub-list below that) is kept to a maximum of 5 entries.

Table options (Occurrences Table only)

Show key attribute column

This option determines whether top-level entries of the table are based on key attribute information. See the Occurrences Table topic for more information.

Show container ID column

This option determines whether top-level entries of the table are based on container ID information. See the Occurrences Table topic for more information.

Table options (Links Analysis only)

Show 'linked to by' details

For each page, a list of other pages that link to it is shown.

Show 'links to' details

For each page, a list of pages and resources that are linked to it is shown.

Broken links are shown in red.

Table options (Links Analysis only when Group By is set to "File type")

Show external file type

This adds an extra file type category, "External Files", which includes all pages that are not at the same base URL of the scan, or part of the Additional Domains list.

Edit file types

This allows you to modify the file type map used to categorize pages into various file types. Each file type is specified by an entry enclosed with square brackets. You can then use either **Url=** or **Content-Type=** to specify a pattern, or comma-separated list of patterns, against which the pages are matched. Use '*' as a wildcard. Note that all spaces are ignored.

For example, the default file type "Web Pages" is specified as follows:

```
[Web Pages]
Url = *.htm,*.html Content-
Type = *html*
```

In this case, any page whose URL ends with `.htm` or `.html`, or whose HTTP Content-Type header value includes `html,` will be included in this file type. Note that each page is tested against the file types in the order they are specified, and is included in the first type it matches.

An empty header can be used to exclude pages and content type, for example:

```
[PDF]
Url = *.pdf
[]
Url = *
```

will exclude links to all file types except those ending with a PDF extension.

Save as default
This button modifies the default file type map that will be used for creating new views. This applies immediately, without any need to save the view you are working on.

Use default
This copies the default file type map into the current view's file type map. No permanent change is made until you save the view.

Occurrences Table

PURPOSE

The occurrences report is designed to help track issues that recur across a large number of pages on a website.

Many modern websites use scripts and templates to generate the final output. If there are compliance issues in the templates themselves, the issues will appear across large sections of the website, potentially on every page.

ACTIONS/CAPABILITIES

Occurrences reports allow the user to group together issues based on "key attribute values", and also (optionally) by the internal ID of the HTML `div` blocks that contain the elements triggering particular checkpoint results. Because the report is sorted by how many times the issue occurs, it allows the user to focus on frequently-occurring errors first.

For example, it may be that every page on a website includes an img element with a src attribute of "companylogo.png", where the alt tag is missing. In this case, the error "IMG element has no ALT text" will occur at least once on every page, making it a high-recurrence error that will most likely appear near the top of the report. Grouped under each entry, a list of occurrences for every page is available. Depending on whether the "key attribute" column is shown or not, the top-level items on the report can be based on this key attribute value. If the column is hidden, then all errors with the message "IMG element has no ALT text" are grouped together with a single count, and the key attribute values are only visible as sub-groups under each entry.

If the column is shown, then a separate entry for each key attribute value is created. For example, "IMG element has no ALT text" might occur 10,000 times with the src attribute value of "companylogo.png", but only 10 times with the src attribute value of "home.png". Depending on the report options, the latter entry might not even appear in the report.

There is an optional form of additional grouping, available for websites that make use of the ID attribute on HTML div elements. For each element-based checkpoint result recorded, the ID of the containing div is also recorded. This is called the "container ID". If, for example, your website was constructed from two or three different templates, all of which had the company logo image with no ALT text, but each template used a different ID for the div that contained the img element, then if you turned on the "container ID" column, you would see several entries for the error "IMG element has no ALT text"--one for each container ID. However, note that when this column is turned off, no information regarding container IDs is preserved in the report. (This is not the case for key attribute values, where turning off the column simply pushes the grouping one level down.)

Note that by default the occurrences report shows only failures and warnings. However, visual checks can be included. It is not recommended that "passes" and "n/a" results are included, as no detailed occurrence information is available for such results. Please also note that the sort order is primarily based on occurrence counts; hence, if the most common result message is a warning, it will be placed at the top, potentially above the other result messages for failures. If two entries have the same occurrence count, then failures will be sorted before warnings and visual check results. For the actual list of occurrences under each entry, the primary sort order is by source code line number.

The occurrences report will also show checkpoint results for elements that have no key attribute values (e.g. table elements), and even for results that are page-based rather than element-based, but this is typically less useful.

HOW TO USE

Scenario 1 - Accessibility

1. Scan a site with at least 10 pages based off the same template for WCAG 1.0 or Section 508 compliance, where the template includes an image with no ALT text.
2. Once the scan is finished, click on the "Failed" status, then click the "View results" link.
3. Change the table type to "Occurrences".
4. One of the top entries should be "IMG element contains no ALT attribute." In the key attribute, the URL of the image that is missing an ALT tag will be shown. The number in the right-hand column indicates how many times on your site an image using this URL was found without an ALT attribute.
5. Uncheck the "Show container ID column" option if your site does not use div IDs, or this does not provide a useful means of identifying recurring issues.
6. Uncheck the "Show key attribute column" option if you wish to see all cases of image elements not using ALT attributes grouped together with a single count.
7. You can now expand this entry to see a list of all the different URLs for which there are IMG elements with no ALT attributes.
8. Expand any one of those sub-entries to see a list of the pages and line/column positions where those IMG elements occur in the source. You can view the occurrences as they appear on a given page by clicking on the URL. When the HTML document opens, click on the "rendered page" link in the frame at the top of the page. Occurrences will be highlighted.
9. If you can see the same column number and very similar line numbers occur across a number of pages, the error is most likely in a template file on the web server.

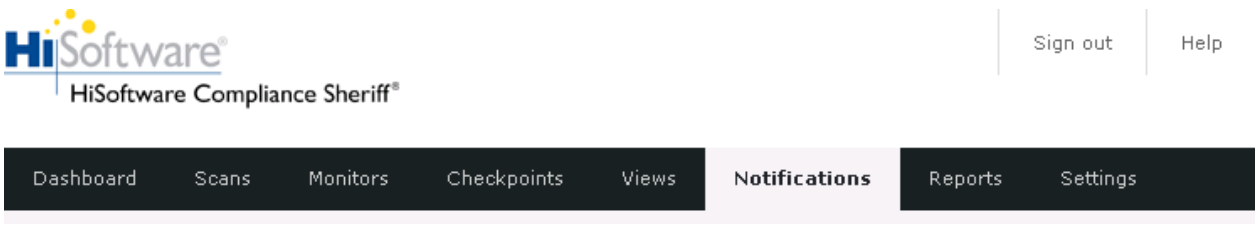
Scenario 2 - Site Quality

1. Scan a site with at least 10 pages all based off the same template for links analysis compliance, where that template includes a link to a non-existent file.
2. Once the scan is finished, click on the "Failed" status, then click the "View results" link.
3. Change the table type to "Occurrences".
4. One of the top entries should be "One or more broken links found: (404) Not Found ". In the key attribute, the URL of the link that is broken will be shown. The number in the right-hand column indicates how many times a link to this URL was found on your site.
5. Uncheck the "Show container ID column" option if your site does not use div IDs, or this does not provide a useful means of identifying recurring issues.
6. Uncheck the "Show key attribute column" option if you wish to see all cases of 404 errors grouped together with a single count.
7. You can now expand this entry to see a list of all the different URLs that caused 404 errors.
8. Expand any one of those sub-entries to see a list of the pages and line/column positions where those links elements occur in the source. You can view the occurrences as they appear on a given page by clicking on the URL. When the HTML document opens, click on the "rendered page" link in the frame at the top of the page. Occurrences will be highlighted.
9. If you can see the same column number and very similar line numbers occur across a number of pages, the error is most likely in a template file on the web server.

MISC

To get the most from an occurrences report, it may be necessary to customize what the key attributes are for each element type. The default list is designed to work specifically with the checkpoints that are shipped with the product, and should prove generally useful. An example of a possible customization would be to add the class attribute as a key attribute of the table element – if a company's website programming guidelines dictate use of the class attribute to distinguish different types of tables (for example, data vs. layout tables), then being able to group together checkpoint results for tables of different classes might assist them in determining the best way to fix any reported compliance issues. For information on editing key attributes, see the topic User agents, variables & key attributes. This screen is accessed via the Settings tab.

Notifications



A notification is an email message that is automatically sent at the end of a scan or monitor, or at scheduled intervals. For example, if you have a report that combines the result of Scan A and Scan B, where Scan A is run weekly and Scan B is run monthly, you may want to receive updates on this report each week after Scan A finishes, each month after Scan B finishes, or just once a quarter.

Create a Notification

1. Click the **Notifications** tab.
2. Click the **New** button.
3. From the **Send report based on view** drop-down menu, select a view. The views that appear will be views that you have created. (For more information, please visit the Views page.)
4. In the **Send to** field, type one or more email addresses. E-mail addresses should be separated by commas or semi-colons.
5. In the **Subject** field, type a subject line for the notification email.
6. If you do not wish to receive the full report in the notification email, select **Send as link**, which will send a link to the report, or **Table summary only (don't expand)**, which means that page details will not be sent. Make your selection by putting a check in the corresponding box.
7. Determine when the notification will be sent by selecting one of two options: **Send after each run of scan/monitor**, or **Send at scheduled intervals**. If you select **Send after each run of scan/monitor**, you will need to select a scan or monitor from the drop-down menu. You will receive a notification after this scan or monitor is run. If you select **Send at scheduled intervals**, you will need to click on the **Add** button and use the three drop-down fields to define the interval between notifications. The frequency can be set to minutes, hours, days, weeks, or months. Multiple schedules can be defined for a notification. (PLEASE NOTE: A 24-hour clock is used.)
8. Click on the **Save** button.

Edit a Notification

1. Click on the **Notifications** tab.
2. In the **Subject** column, locate the notification you wish to edit, and click on it.
3. Modify the notification properties as needed.
4. Click the **Save** button.

 If you use the **Save as new** button to create a new notification, you should change the notification's short description before doing so.

Delete a Notification

1. Click on the **Notifications** tab.
2. In the far-left column, select the check box that corresponds with the notification you wish to delete.
3. Click on the **Delete** button.
4. A confirmation dialog box will appear. Select **OK** to confirm deletion.

Notification Properties

Add

Clicking the **Add** button will cause open-ended schedule definitions to appear. Multiple schedules can be defined for a notification.

The default start-time is midnight on the following day.

Beginning

Use the date field to specify the date that the notification will be sent.

If the frequency is set to **Month(s)**, be sure that the start date is not set higher than "28". If it is, notifications will not be sent during February. This would also apply for months with 30 days, if the start date was set at "31".

Frequency

Use the three drop-down fields to define the interval between notifications. The frequency can be set to minutes, hours, days, weeks, or months.

Send after each run of scan/monitor

For this option, a notification is sent immediately after the associated scan or monitor defined in a view finishes running. If a view has multiple scans or monitors associated with it, you will need to choose which scan or monitor will determine when the notification is sent--the notification will be sent when this scan or monitor finishes running. In most cases, you should select the scan or monitor that you expect to finish last.

Send as link

This option means the report is not embedded in the email body; instead, the email will contain a link to the most current version of report. This option is not suitable if the e-mail recipient does not have access to the server hosting HiSoftware Compliance Sheriff, or if you wish to ensure that the version of the report created when the notification is sent is archived permanently.

Send at scheduled intervals

For this option, notifications will be sent according to the schedule you define. You can define multiple schedules for a notification by clicking on the **Add** button.

Send report based on view

The email notification contains a scan or monitor report, based on a view you've previously created. The body of the email can contain the report itself or a link to the report.

Send to

In this field, enter the email address where the notification should be sent. If a notification should be sent to multiple recipients, separate their email addresses with commas or semicolons.

Start time

Use the hour and minutes fields to define the time of the day that the notification will be sent. (PLEASE NOTE: A 24-hour UTC clock is used.)

Subject

This is what will appear in the subject line of the notification email.

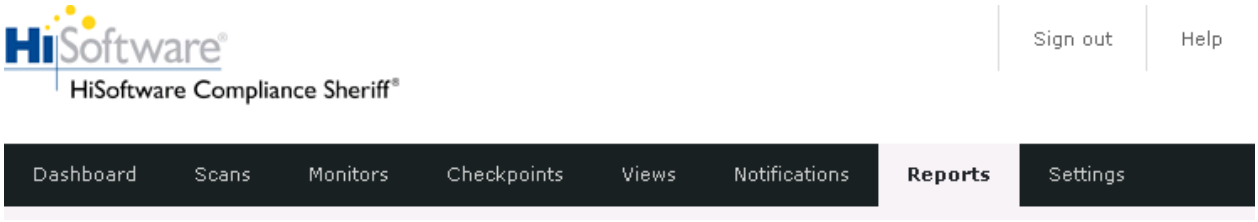
Table summary only (don't expand)

This option means that the report will not contain page details.

Weekday of the month

This option is only available if the **Frequency** period selected is **month(s)**. Click in the check box in the **Beginning** column, and use the drop-down menus to determine the weekday of the month on which the notifications will be sent.

Reports



A report in HiSoftware Compliance Sheriff V4.2 utilizes Compliance Insight, a new compliance performance management console. Compliance Insight provides executive management visibility into how your organization is performing with respect to compliance goals, and allows you to compare compliance performance among individuals and groups (business departments, geographical units, and others).

Scan Summaries

Scan summaries give you the complete results of a scan or monitor. From the scan summary main display page, you can find all the information you need on where to focus your future efforts at web compliance, and get a clear sense of how well your organization is meeting its unique web governance standards.

How to Access the Scan Summary Main Display page

The scan summary main display page can be accessed from the **Scans** tab or the **Reports** tab.

From the **Scans** tab:
Under the **Health** heading, click on the relevant numerical value (%) for the statistic you wish to see the full report on. (PLEASE NOTE: If you haven't run any scans, the table containing the Health heading will not appear.)

From the **Reports** tab:
The reports tab, when first accessed, will always display a scorecard for a particular scan group or set of scan groups. Each cell within the scorecard that displays a health value can be clicked on to view scan summary details. When a scan summary is accessed using this method, it will automatically filter the results to match the scan or checkpoint group selected in the scorecard cell.

How to Navigate the Scan Summary Main Display page

Once you've accessed the Main Display page, you can make use of the features listed below. To view the scan summary of an individual checkpoint group, select a checkpoint group from the **Checkpoint Group pull-down menu** near the top right.

Back to Scorecard

If you've arrived at the main display page via a scorecard, you'll see a fourth button in the top left, **Back to Scorecard**, which will take you back to the scorecard.

Create View

Create View, a button at the top left, will take you to the create a view page, where you can create a view for this scan. (Please visit the Views page for more information on how views work.)

Not Applicables

Not Applicables are issues that don't refer to a specific checkpoint category.

Priority 1 Checkpoints

Priority 1 Checkpoints refer to issues that most users consider very important (for example, checkpoints that locate social security numbers on a non-confidential part of the site would be considered Priority 1 checkpoints). In the Top 10 Issues field, Priority 1 checkpoints will appear first. Users can alter the priority status of a checkpoint in the checkpoint editor.

Revise Results

The **Revise Results** button takes you to the result revision wizard (RRW) page. On the RRW page, you can change the result title associated with each error, so that the next time the scan is run, a specific issue will be associated with the title you prefer (for example, a result with the title "Visual" could be changed to "Passed"). HiSoftware gives users this option because our checkpoints are rigorous, and the scans may identify issues that some users might consider low-priority. On the RRW page, the user can tell HiSoftware Compliance Sheriff to disregard certain issues, or to label them differently. To more quickly locate and re-label specific issues, try applying a filter on the RRW page, or grouping results by checkpoint or page. Don't forget to select the **Save** button after you've made a change. For more information on revising scan results, visit the Revise Scan Results page.

Top 10 Checkpoints

In the **Top 10 Checkpoints** field, you can view the ten checkpoints with the highest occurrence counts, by category (what the occurrence counts refer to depends on which category is selected). This is useful for finding out which checkpoints produce the largest set of results. From the pull-down menu, select **Failures**, **Warnings**, **Visuals**, **Passed**, or **N/A**. The ten checkpoints with the highest occurrence counts in that category will be displayed. Click on the text in the **Description** field to open the list of occurrences in the results revision wizard. If desired, you can change the title associated with any given violation. In the **Number** column, click on a checkpoint's number to open the checkpoint in the Checkpoint editor.

If you are viewing the results of a scan group summary, the same checkpoint may be listed more than once in the Top 10 Checkpoints table. This is due to the fact that the table makes distinctions between the individual scans that comprise the scan group. Repetition of a checkpoint means that multiple scans within the scan group found violations for this checkpoint.

Top 10 Checkpoints Changed via Results Revision

The **Top 10 Checkpoints Changed via Results Revision** field shows you the results associated with checkpoints you've modified in the results revision wizard. This field allows you to keep an eye on the

RRW changes you've made, and make sure that these changes are working for you.

Top 10 Issues

In the **Top 10 Issues** field, you will see a list of the ten results that HiSoftware recommends taking immediate action on. The icons in the left margin tell you what type of checkpoint each item refers to: Failure, Warning, or Visual. To view a checkpoint's violations as they appear on a site page, click on the text in the result field to open the show instances feature.

Top 10 Pages

The **Top 10 Pages** field shows the ten pages containing the highest number of checkpoint violations. While the Top 10 Checkpoints field reveals which checkpoints are consistently violated across your site collection, the Top 10 Pages field reveals which site pages consistently violate any number of checkpoints. Use the pull-down menu to view the top 10 pages for Failures, Warnings, or Visuals.

Trend

The **Trend** field breaks the Scan down into numerical results. You can see how many pages were scanned, how long the Scan took and the average time per page, and the total Checkpoints tested. You can also see the numerical totals for each item in the pie chart, along with the total **Priority 1 Failures** and **Not Applicables**. If this Scan has been run two or more times, a line graph will show you how the overall results have changed with each successive Scan.

View Full Details

View Full Details, a button at the top left, will take you a page that lists every single item that the scan detected. Note that clicking View Full Details may take a long time to generate, as it will be a fully expanded report with every item displayed.

How to Create a View for a Scan Summary

Once you've created a view for a scan summary, you can add it to your dashboard for handy reference.

1. Click the **Views** tab.
2. Click the **New** button.
3. In the Name field, enter a unique name for the view you're creating.
4. Click **Scans** to open the Scans field. Select the scans you wish to include in the view. Remember to hold the CTRL button if you want to select multiple scans. Once you've finished making your selections, click **Scans** again to collapse the field. (Collapsing the fields isn't required, but it keeps things tidy on your screen.)
5. Click on the **Checkpoint Groups** button to open the Checkpoint Groups field. Select the checkpoint groups you want to associate with the view. Remember to hold the **CTRL** button if you want to select multiple checkpoint groups. Once you've finished making your selections, click **Checkpoint Groups** again to collapse the field.
6. In the Charts field, click **Charts**. From the Chart type pull-down menu, select **None**. Once you've done so, collapse the field by clicking on the **Charts** button.
7. Click on the **Table** button to open the Table field. From the Table type pull-down menu, select **Scan summary**.
8. Click **Save**.
9. On the Views tab main page, you'll see a listing for the new View in the left-side column. In the right-side column, you'll see three small icons: Preview, Open report for <title of View> in a new window, and Open PDF report for <title of View> in a new window. Click the **Open report for <title of View> in a new window** icon.
10. If the scan summary displays as expected, close the window. You can now add this scan summary to your dashboard.

Show Instances

How to Use The Show Instances Feature

The show instances feature allows you to view scan or monitor results that pertain to content on a web page, *as the content appears* on the page. You can view the rendered page or the source code, and HiSoftware Compliance Sheriff will show you exactly where each issue occurs.

For a glossary of terms associated with the **Show Instances** feature, visit the Show Instances Properties page. If you have additional questions, visit the Show Instances FAQ page.

Access the Show Instances Feature From a Detailed Report

1. Click on the **Reports** tab.
2. In the table that appears, click on the relevant numerical value (%) for the issue you wish to see the full report on. (PLEASE NOTE: If you haven't run any scans or monitors, this table will not appear.)
3. In the report, you will see a **Top Ten Results** heading. Beneath this heading is a list of the ten checkpoints with the highest number of violations. (The number of checkpoints that appear beneath this heading will vary depending on how many checkpoints were included in the scan or monitor, and/or how many checkpoints were violated.)
4. Click one of these checkpoints to open the show instances feature for that checkpoint.
5. HiSoftware Compliance Sheriff will render the first page on which one or more violations occurred. A red square will appear around the violations.
6. To scroll through the individual violations on a page, use the arrows on the right side of the colored bar at the top of the page. These arrows have visual labels: **Next Occurrence** and **Previous Occurrence**.


Next Occurrence *Previous Occurrence*

7. To view the individual violations by number, click on the **Occurrences** pull-down menu and select a number. Select **All** to view all the violations on a page at once. (If more than one violation occurs on a page, show instances will default to **All** when opened.)

Occurrences pull-down menu

8. To scroll through the pages on which one or more violations occurred, use the arrows in the grey field at the top left. These arrows have visual labels: **Next Page** and **Previous Page**.


Next Page *Previous Page*

9. To see where the violations occur in the HTML, click on the **Code source** button, located at the right end of the colored bar at the top of the page. The source HTML of the page will appear, and red squares will appear around the violations. To see the rendered page again, click on the **Rendered**

view button, located in the same place the **Code source** button appeared earlier.

Code source

Rendered view

10. If a reference page has been set for the checkpoint, you can access it by clicking on the **How to fix?** button.

How to fix?

11. The URL of the page being rendered will appear at the top of the page. Click on it to open the page outside of HiSoftware Compliance Sheriff.

Access the Show Instances Feature From a Scan Summary

1. Click on the **Scans** tab.
2. Under the **Health** heading, click on the relevant numerical value (%) for the statistic you wish to see the full report on. (NOTE: If you haven't run any scans, the table containing the **Health** heading will not appear.)
3. In the report, you will see a **Top Ten Results** heading. Beneath this heading is a list of the ten checkpoints with the highest number of violations. (The number of checkpoints that appear beneath this heading will vary depending on how many checkpoints were included in the scan or monitor, and/or how many checkpoints were violated.)
4. Click on one of these checkpoints to open the show Instances feature for that checkpoint.
5. HiSoftware Compliance Sheriff will render the first page on which one or more violations occurred. A red square will appear around the violations.
6. To scroll through the individual violations on a page, use the arrows on the right side of the colored bar at the top of the page. These arrows have visual labels: **Next Occurrence** and **Previous Occurrence**.


Next Occurrence *Previous Occurrence*

7. To view the individual violations by number, click on the **Occurrences** pull-down menu and select a number. Select **All** to view all the violations on a page at once. (If more than one violation occurs on a page, show instances will default to **All** when opened.)

Occurrences pull-down menu

8. To scroll through the pages on which one or more violations occurred, use the arrows in the grey field at the top left. These arrows have visual labels: **Next Page** and **Previous Page**.


Next Page *Previous Page*

9. To see where the violations occur in the HTML, click on the **Code source** button, located at the right end of the colored bar at the top of the page. The source HTML of the page will appear, and red squares will appear around the violations. To see the rendered page again, click on the **Rendered view** button, located in the same place the **Code source** button appeared earlier.

Code source *Rendered view*

10. If a reference page has been set for the checkpoint, you can access it by clicking on the **How to fix?** button.

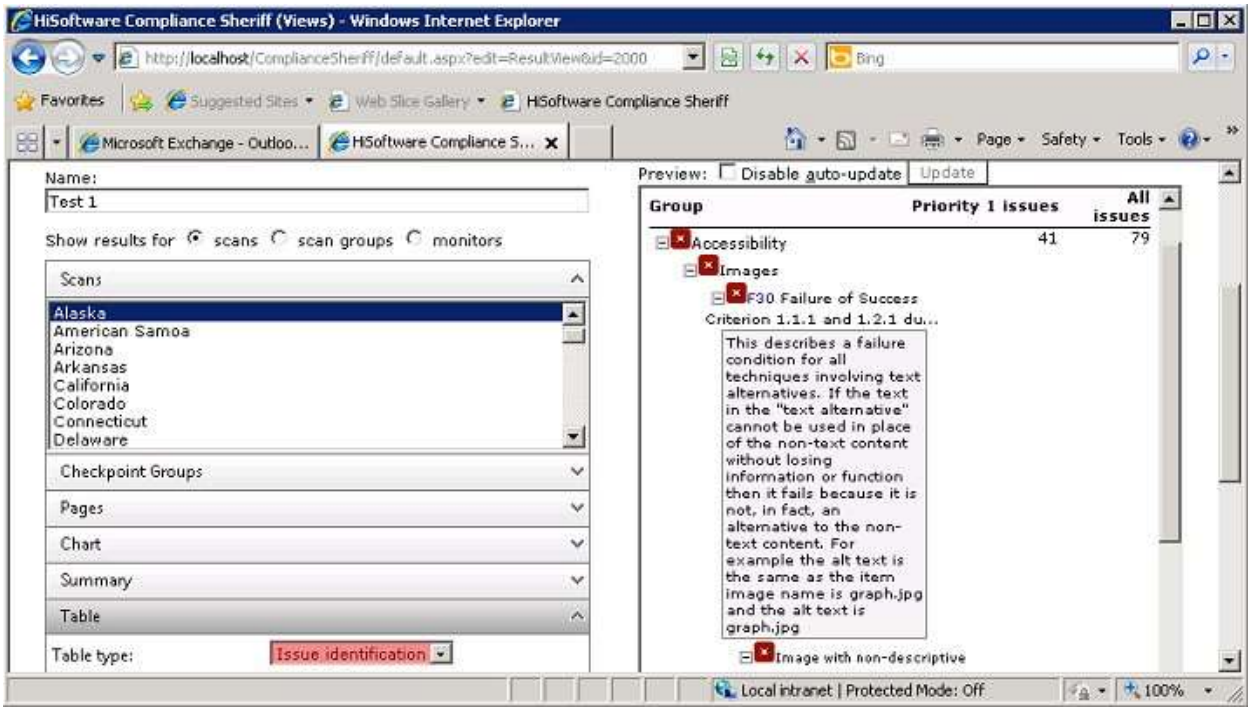
How to fix?

11. The URL of the page being rendered will appear at the top of the page. Click on it to open the page outside of HiSoftware Compliance Sheriff.

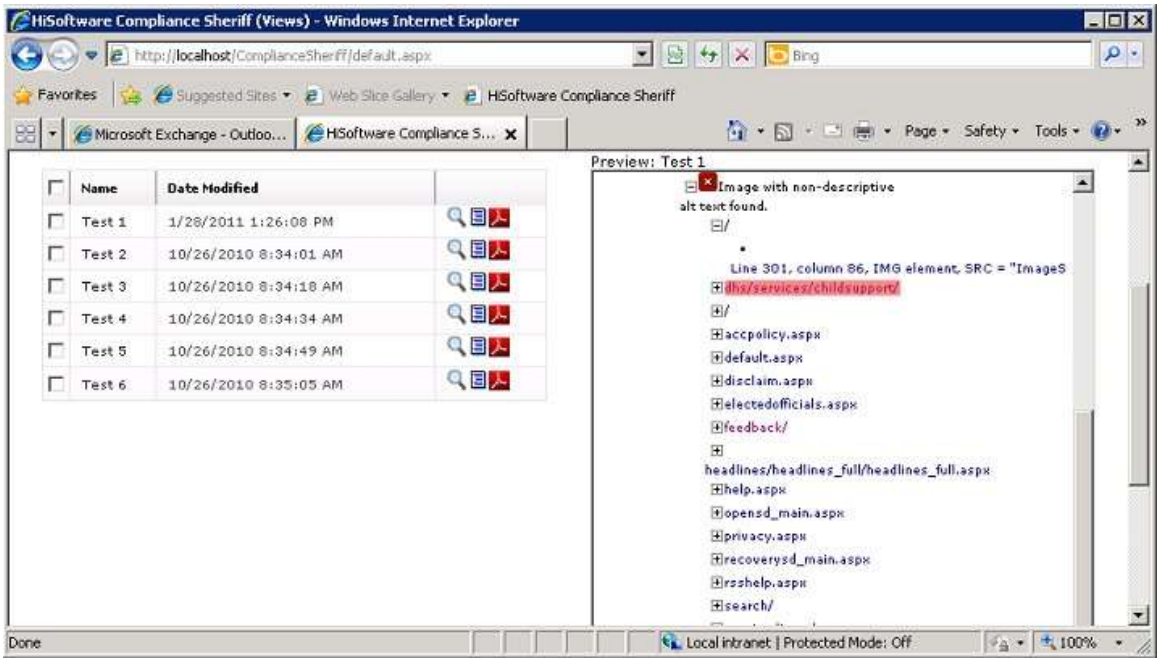
Access the Show Instances Feature From a View

The show instances feature can be accessed from a view, but the view must be set to table type **Issue identification** or **Occurrences**. To change a view to one of these two table types, follow the instructions below. If you have already created a view with this table type, skip ahead to Step 6. (For more information about the various table types, visit the Tables page.)

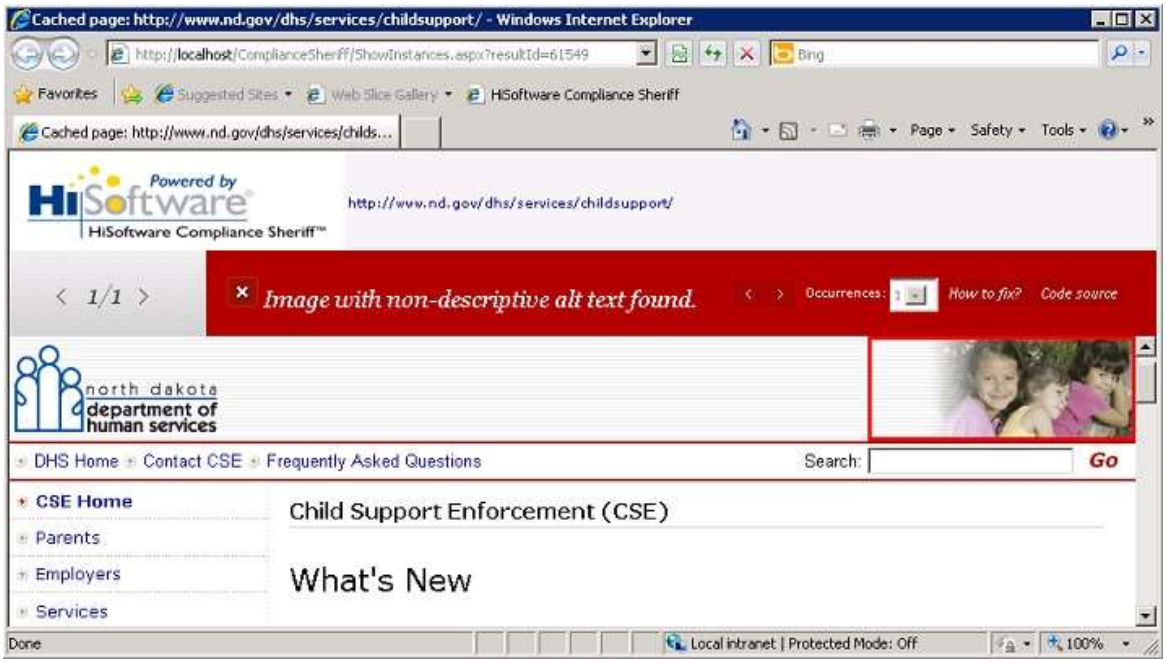
1. Click on the **Views** tab.
2. Click on the name of the View you wish to change.
3. Click on the gray **Table** bar to open the Tables pull-down menu.
4. From the **table type** pull-down menu, select "Issue identification" or "Occurrences". In the example shown below, "Issue identification" has been selected.



5. Click on the **Save** button.
6. Once the views main page has loaded, click on the preview icon (a magnifying glass) in the row associated with the view you want to examine.
7. Locate the link associated with the page you want to open in the show instances feature, and click on it.



8. The page will be opened in the show instances feature.



Access the Show Instances Feature From an API

Various integrations make use of the show instances feature to highlight issues found in their content. One example can be found here:
http://api.hisoftware.com/RadEditor/

Show Instances: Properties

Code source

To see where the violations occur in the HTML, click on the **Code source** button, located at the right end of the colored bar at the top of the page.

Code source

How to fix?

Clicking the **How to fix** button will load the reference page that has been set for the checkpoint, if a reference page has been set. To customize the reference page in a checkpoint, edit the **URL for further information** field in the checkpoint editor. For more information on checkpoints, visit the Checkpoints chapter.

How to fix?

List of Keyboard Shortcuts

ALT + = (next result)
ALT + - (previous result)
ALT+ [(next occurrence)
ALT+] (previous occurrence)

Next Occurrence

The **Next Occurrence** button allows you to scroll through the individual violations on a page, in the order they appear in the HTML.

Next Occurrence

Next Page

The **Next Page** button allows you to scroll to the next page on which one or more violations occurred.

Next Page

Occurrences

The **Occurrences** pull-down menu allows you to view the individual violations by number. Select **All** to view all the violations on a page at once. (If more than one violation occurs on a page, show instances will default to **All** when opened.)

Occurrences pull-down menu

Previous Page

The **Previous Page** button allows you to scroll to the previous page on which one or more violations occurred.

Previous Page

Previous Occurrence

The **Previous Occurrence** button allows you to scroll backwards through the individual violations on a page.

Previous Occurrence

Rendered view

If you've clicked on **Code source** and wish to see the rendered page again, click on the **Rendered view** button, located in the same place the **Code source** button appeared earlier.

Rendered view

Result

A result refers to the end product of a scan or monitor. Each checkpoint in HiSoftware Compliance Sheriff has the ability to produce multiple results. The most common two results for a checkpoint will be a PASS result or a FAIL result. When building a checkpoint in HiSoftware Compliance Sheriff the text that is placed in to the rule will be displayed as a message to the user.

Show Instances: FAQ

How do I access the show instances feature?

You can access the show instances feature from one of four places:

- From A Detailed Report
- From A Scan Summary
- From a View
- From an API
- From SharePoint

What types of content can be rendered?

The following types of content can be rendered:

- MSG
- TXT
- DOC
- DOCX
- PDF
- PPT
- PPTX
- XLS
- XLSX
- HTML

Why does the content rendered not look exactly like it does on the original page?

Some times certain scripts or css files are not available and the content will not display exactly as it does on the web site. In these instances, the user can navigate using the URL on show instances to inspect the live site. For PDF and Office file formats, the content is converted into a HTML representation of the original content.

What is a result?

A result refers to the end product of a scan or monitor. Each checkpoint in HiSoftware Compliance Sheriff has the ability to produce multiple results. The most common two results for a checkpoint will be a PASS result or a FAIL result. When building a checkpoint in HiSoftware Compliance Sheriff the text that is placed in to the rule will be displayed as a message to the user.

What is an occurrence?

An occurrence is a specific location within content where a compliance check was performed. If, for example, an error was found in two locations in the document, then two occurrences will be displayed.

What do the icons in the left margin of the Top Ten Results panel signify?

Please visit the Reports Properties page.

Why do some occurrences display extra text?

For checkpoints that use %value% in the result message, the occurrences will populate with the string recorded in the value parameter. An example would be checking for the presence of emails in the content.

How do I customize where the How to fix button links to?

Clicking the **How to fix** button will load the reference page that has been set for the checkpoint, if a reference page has been set. To customize the reference page in a checkpoint, edit the **URL for further information** field in the checkpoint editor. For more information on checkpoints, visit the Checkpoints chapter.

I don't understand the terms used in the show instances interface. Where can I find definitions?

Definitions of terms used in the show instances interface can be found on the Show Instances Properties page.

What keyboard shortcuts can be used to navigate the show instances feature?

- **ALT + =** (next result)
- **ALT + -** (previous result)
- **ALT+ [** (next occurrence)
- **ALT+]** (previous occurrence)

How do I remove the security popup in Internet Explorer?

If HiSoftware Compliance Sheriff is hosted on a secure site, and the show instances report links to a non-secure site, the Internet Explorer security settings for the internet zone will need to be adjusted.

1. From the Tools menu in Internet Explorer, select **Internet Options**.
2. Click the **Security** tab.
3. Click on the green check to add HiSoftware Compliance Sheriff to your list of trusted sites.
4. Once the green check has been selected, click **Custom level**.
5. In the Miscellaneous heading, under "Display mixed content," select **Enable**.
6. Click **OK** to exit the Internet Options menu.

Scorecards

A scorecard is a table that gives you a visual sense of how well your organization is meeting its unique web compliance standards. By allowing you to make side-by-side comparisons of several sites or groups of sites across your network, a scorecard allows you to see which areas of your site network are exceeding your goals, which areas need further attention, and which areas have improved or declined.

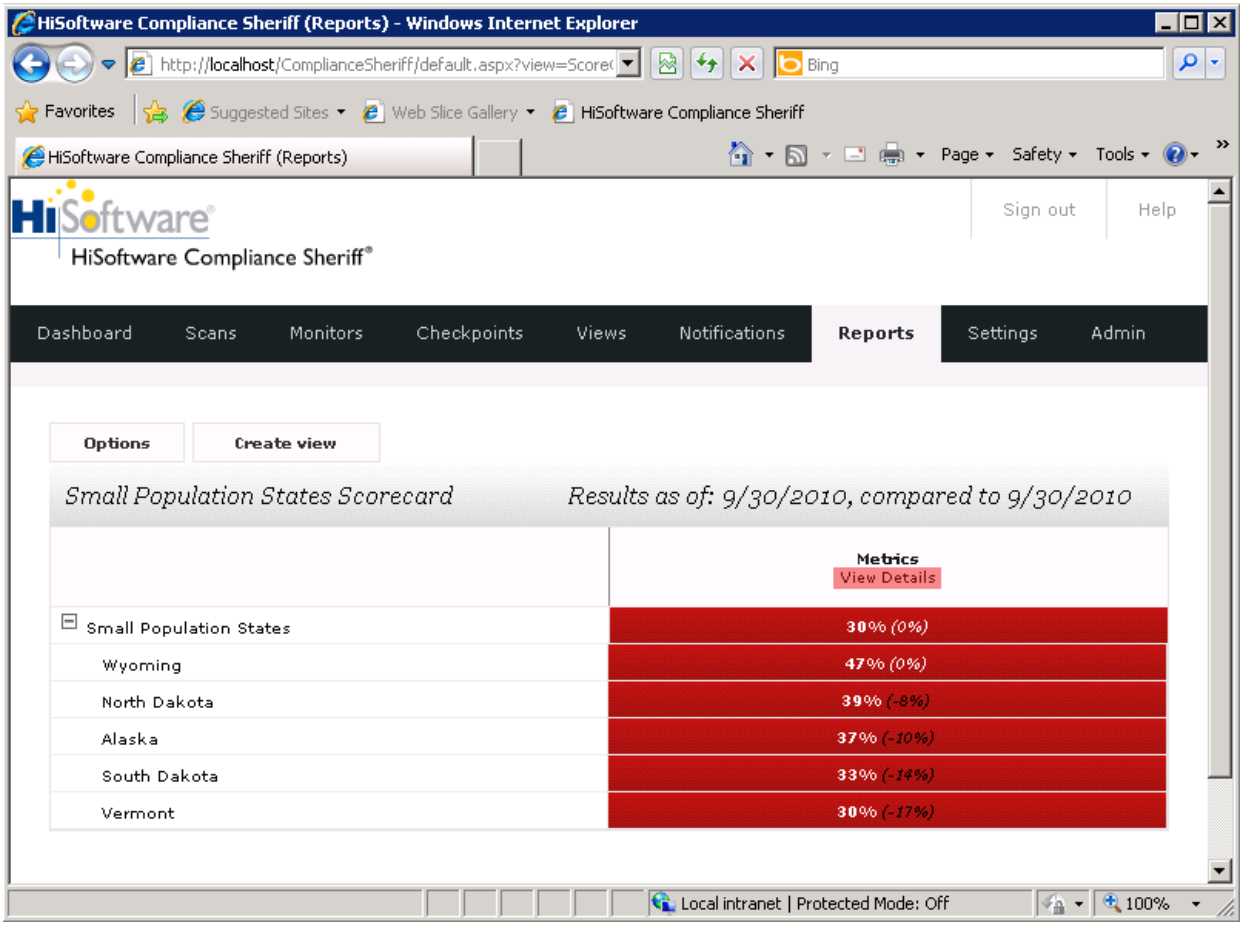
Scorecards: An Introduction

Before setting up a scorecard, HiSoftware recommends that you first determine how your organization wants to manage web compliance. What are your governance strategies? What areas of compliance—accessibility, privacy, site quality, or other areas—are most important to you? What divisions within your organization are the most relevant? (When comparing different areas of a site network, many organizations, for example, choose to compare the performance of different geographical regions, while others choose to compare business departments.) What divisions would *you* make? What areas of compliance would you enforce most strictly? Thinking about these questions will help ensure that your organization exceeds its web compliance goals, and that the scorecards you create are pertinent to these goals.

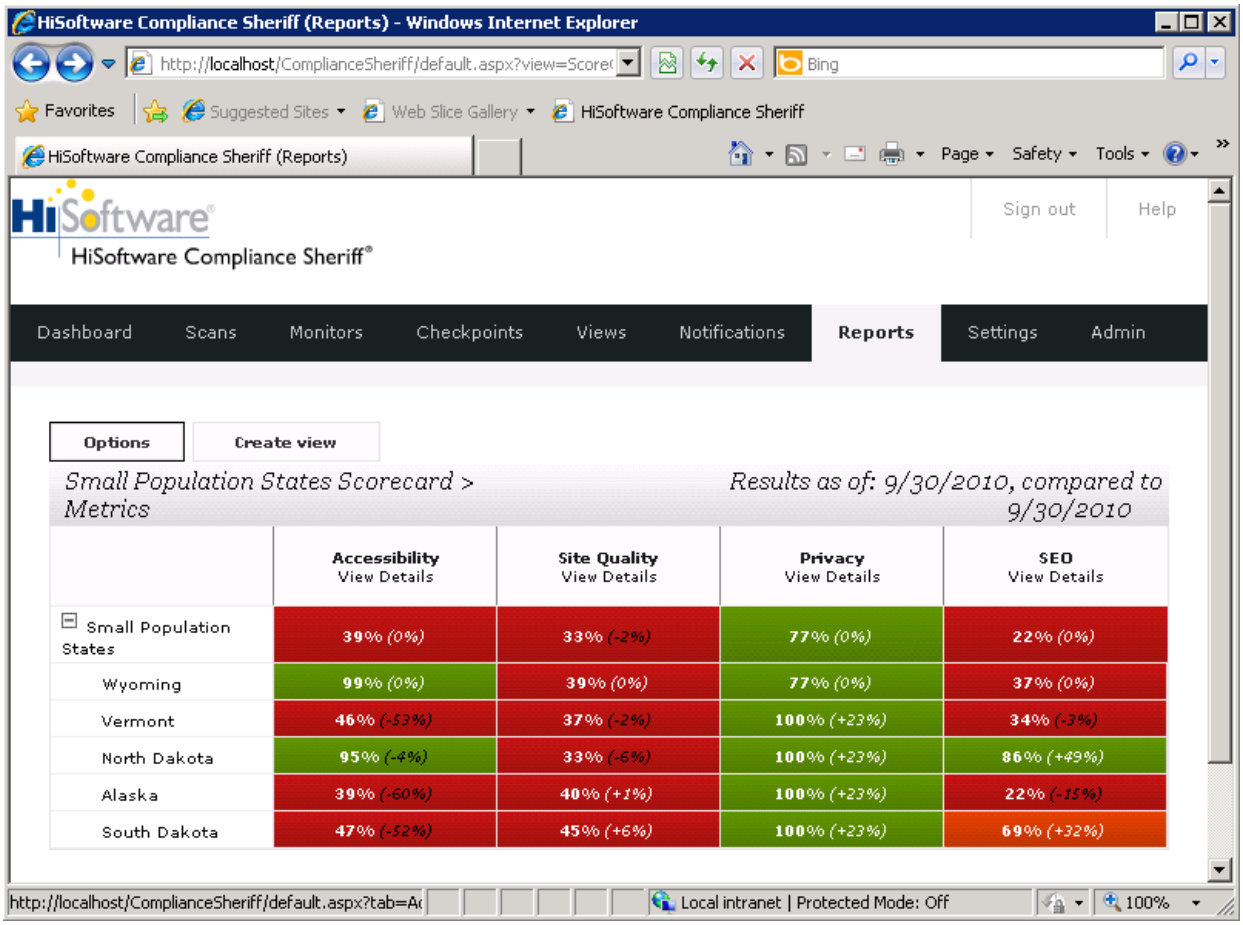
The steps below show you how set up a scorecard.

1. Determine which scans or scan groups you wish to compare. The unique URL of each scan will determined which site pages are compared in the scorecard.
2. Review the checkpoints or checkpoint groups associated with the scans or scan groups you wish to compare. Determine whether these are the compliance issues that you consider most important for comparison purposes. (If you're unsure where to start, HiSoftware recommends using the checkpoint group **Metrics** for each scan in your scorecard. **Metrics** tests a site's adherence to common standards for accessibility, site quality, privacy, and search engine optimization. Depending on your organization's license with HiSoftware Compliance Sheriff you may or may not have access to **Metrics**, but there are many other checkpoint groups you can use. If you don't have **Metrics**, you can create a checkpoint group.)
3. Once you've confirmed that the most appropriate checkpoints or checkpoint groups have been assigned to the **Scans** (i.e. site pages) that you want to compare, create a scan group.
4. On the scan groups main page (**Scans** tab, **Groups** sub-tab), and run your new **Scan Group** by clicking on the **Run** button in the relevant row.
5. Once all the sites have been scanned, a **Completed** message will appear beneath the **Status** heading for your scan group.
6. A percent value will appear beneath the **Health** column for your scan group, indicating what percentage of the sites scanned passed the checkpoints you selected. To access the scorecard, click on this percent value.

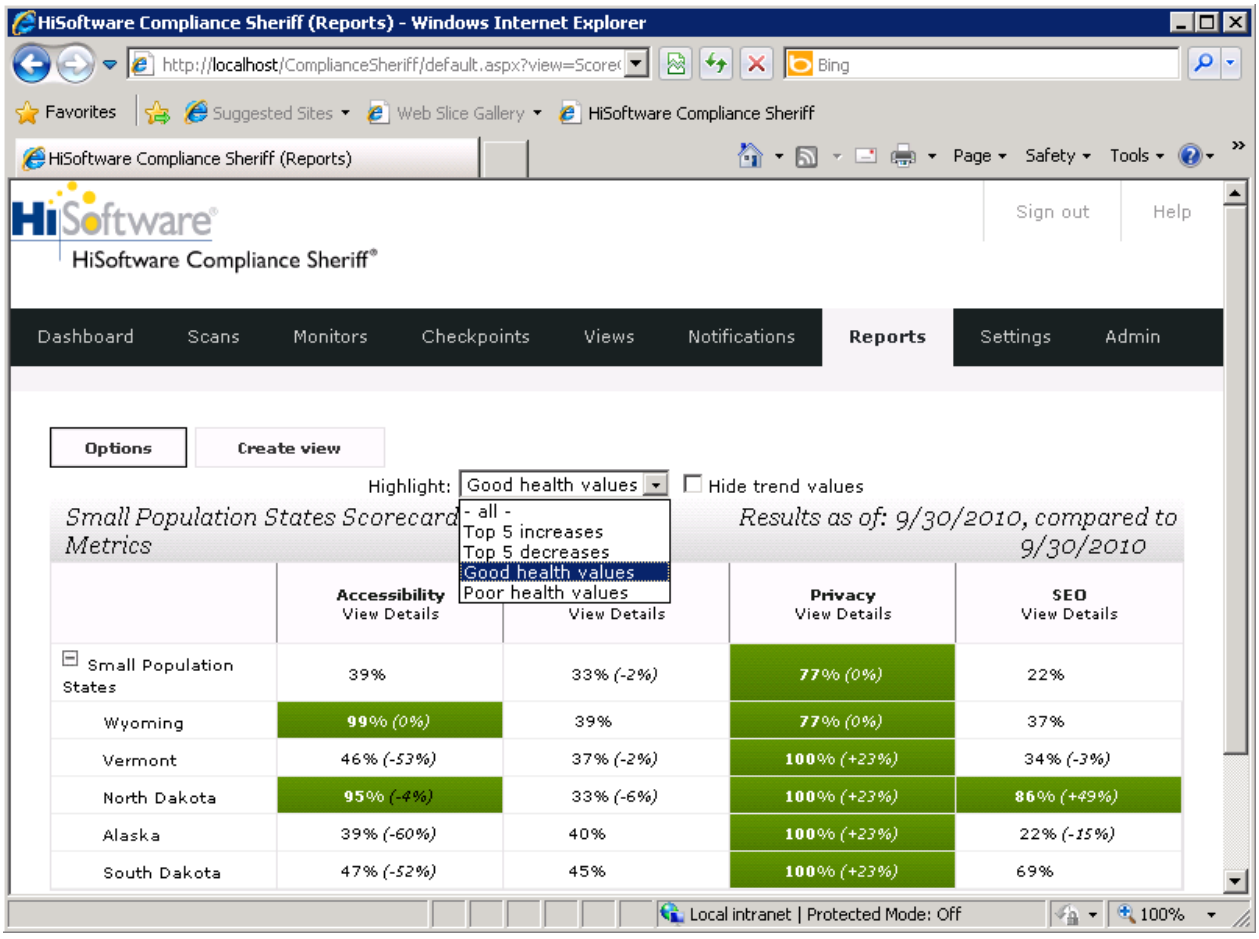
7. The scorecard will appear. The scan groups associated with this scorecard will be listed in the far-left column. To view or hide the individual scans of a scan group, click on the "+" or "–" signs next to the title of each scan group. To view the individual checkpoints in a checkpoint group, click on the **View Details** link beneath the checkpoint group title. In the example below, a scorecard comparing the government websites of small population states has been created. **Metrics** is the checkpoint group being used to compare them. The **View Details** link (highlighted) is selected.



8. If the scan group you created has been run only one time, you will see only one value listed in each cell. If this is the second time you have run the scan group (as in the example below), and if a specific page has improved or worsened in a given area since the previous run, you will see a second value listed in parenthesis beside the first. This second value indicates the percent increase or decrease in compliance since the previous run.



9. If you click on the **Options** button in the top left, a pull-down menu labeled **Highlight** will appear at the top center. You will notice it defaults to “all”, meaning all cells are highlighted. To highlight only the areas performing well, select “Good health values” from this pull-down menu. Select “Poor health values” to see only the areas performing badly. If you have run this scan group before, you can highlight the areas demonstrating greatest improvement by selecting “Top 5 increases”. You can also select “Top 5 decreases” to highlight the areas demonstrating the greatest decline. To hide the trend values (the percent of improvement or decline since the last run), check the **Hide trend values** box. In the example below, "Good health values" is selected from the **Highlight** pull-down menu.



10. To the view the report for an individual scan in the group, or to access the show instances feature, click on the percent value shown for the unique scan you wish to review.
11. In the future, you can access this same scorecard from the **Reports** tab. Go to the **Reports** main page, and select the checkpoint group title from the pull-down menu. You can also create a view for a scorecard (see link below).

Scorecards: How to Create a View

Creating a view for a scorecard allows you to see only the parts of a scorecard that are most essential to your web compliance goals. This is useful if you have a high number of checkpoints associated with a scan group, which can create a very large scorecard. Once you've created a unique view for a scorecard, you can add it to your dashboard for handy reference.

1. Click on the **Views** tab.
2. Click the **New** button.
3. In the **Name** field, enter a unique name for the view you're creating.
4. Click the **Scans** button to open the **Scans** field. Select the scans you wish to include in the view. Remember to hold the CTRL button if you want to select multiple scans. Once you've finished making your selections, click on the **Scans** button again to collapse the field. (Collapsing the fields isn't required, but it keeps things tidy on your screen.)
5. Click the **Checkpoint Groups** button to open the **Checkpoint Groups** field. Select the checkpoint groups you want to associate with the view. Remember to hold the CTRL button if you want to select multiple checkpoint groups. Once you've finished making your selections, click on the **Checkpoint Groups** button again to collapse the field.
6. In the **Charts** field, click the **Charts** button. From the **Chart type** pull-down menu, select **None**. Once you've done so, collapse the field by clicking on the **Charts** button.
8. Click the **Table** button to open the **Table** field. From the **Table type** pull-down menu, select **Scorecard**.
9. Click the **Save** button.
10. On the **Views** tab main page, you'll see a listing for the new view in the left-side column. In the right-side column, you'll see three small icons: "Preview," "Open report for <title of View> in a new window," and "Open PDF report for <title of View> in a new window." Click the "Open report for <title of View> in a new window" icon.
11. If the Scorecard displays as expected, close the window. You can now add this Scorecard to your Dashboard.

Scorecards: FAQ

How do I create a scorecard to compare business departments?

A scan should be created for each business department. Examples of business departments include:

- Marketing
- Contoso Product
- Acme Product
- HR
- Operations
- Professional Services

These scans can then be placed inside of a scan group, and the scan group can then be used to schedule and run a series of compliance checks. This scan group could be titled “Business Departments.”

Each business department can contain multiple scans that contribute to an overall score.

How do I create a scorecard to compare geographical regions?

A scan should be created for each region. For example:

- EMEA
- ASIA
- USA

These scans can then be placed inside of a scan group, and the scan group can then be used to schedule and run a series of compliance checks. This scan group could be titled “Regions.”
Each region can contain multiple scans that contribute to an overall score.

Do all scans within my scan group need to have the same checkpoint groups?

No, but HiSoftware recommends it. This will make the scorecard’s comparisons more helpful.

Can I put a scorecard on my dashboard?

Yes, but you will first need to Create a View for a Scorecard. When adding a scorecard to your dashboard, HiSoftware recommends that you display the scorecard in either “Vertical” mode or “Tabs” mode, so that the entire scorecard is visible in the UI.

How do I access the default scorecard for my scan group?

Navigate to the **Scans** tab and make sure the **Groups** sub-tab is selected.
By clicking on the **Health** percent value, the user will open the default scorecard for the scan group.

How do I change which checkpoint groups are displayed within the scorecard?

Click the **Configure** button on the scorecard you’ve opened. This will take you to the **Views** tab, where a scorecard can be configured. The checkpoint groups list allows you to select which checkpoint groups will be displayed. Only checkpoint groups contained within the scan on your scorecard will be available as options.

What happens if I view a scorecard for a scan group that has not been run?

The scorecard will display N/A for all checkpoint groups.

What happens if I view a scorecard and one of the scans did not run a particular checkpoint group?

The scorecard will display N/A in the column of the checkpoint group(s) that were not run. You may go back and add in the relevant checkpoint group, and re-run the scan to fully complete the scorecard.

How is the score calculated for a checkpoint group column on scorecard?

The scan group will display the lowest compliance score of all the scans within the group. If three scans have a compliance score of 93, and one has a score of 78, then the scan group will have a score of 78.

How is the compliance score calculated for a particular checkpoint group and scan?

This is the current calculation:
6 / ({# pages failing a Priority 1 checkpoint} + 9) + 2 / ({# pages failing a Priority 2 checkpoint} + 9) + 1 / ({# pages failing a Priority 3 checkpoint} + 9)

How many checkpoints should I use for KPI?

We recommend using no more than 10 checkpoints per checkpoint group.

How do I educate teams on performance measurements?

- Give each team documentation on what they're assessed on and compared with.
- Give training workshops to all teams.
- Explain past, present, and future performance indicators.

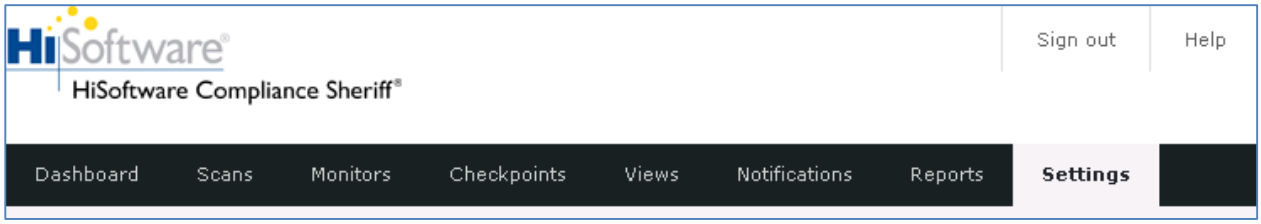
How do I export a scorecard to Excel, CSV, or PDF?

Once a scorecard has been saved as a view, it can be exported to any of these formats from the views tab. If the icons for these file formats do not appear in the views tab, additional installation steps may be required. Contact support@hisoftware.com for more information.

Can I shorten the names of checkpoints or checkpoint groups?

If you add the same prefix to several checkpoints or checkpoint groups contained within a larger checkpoint group, the scorecard will remove the prefix when you drill down from the larger checkpoint group. For example, the checkpoint group "Metrics" contains four checkpoint groups: Metrics - Accessibility, Metrics - Site Quality, Metrics - Privacy, and Metrics - SEO. In a scorecard, if you drill down from the "Metrics" Checkpoint Group, the contents will appear as Accessibility, Site Quality, Privacy, and SEO -- the "Metrics" prefix is removed.

Settings



The settings tab can be used to configure and customize HiSoftware Compliance Sheriff.

Change Your Password

1. Select the **Settings** tab.
2. Click on the **Change password** link.
3. In the **Current password** field, type in your current password.
4. In the **New password** field, type in your new password.
5. In the **Confirm password** field, type in your new password again.
6. Click on the **Save** button.

User Preferences

Time zone
Allows the user to select the local time zone.

Maximum text length for long descriptions and URLs
Determines how long a browser string or description can be before it's truncated. This can be adjusted according to screen resolution.

Use script editor when editing checkpoints
Allows users to modify checkpoint rules with a regular text editor. This is suitable for advanced or visually-impaired users.

Contact support@hisoftware.com for assistance with this feature.

Auto-update scans tab and view editor preview
If this option is unchecked, the scans tab will not refresh automatically. Also, when editing view definitions, the preview will not be updated automatically.
This can be useful for users with accessibility concerns.

Auto-update interval for Scans tab
This specifies the number of seconds between refreshes of the scans tab. The minimum refresh interval is 3 seconds.

UI Theme
This pull-down menu allows you to specify which UI theme you prefer: default or high contrast.

System Configuration

Web Application Settings

Ignore list limits in reports
This will ignore list limits in reports.

Include instance detail in report
Determines whether or not a report should include a list of individual instances and state the line number and column number for each. If this detail is not required, un-check this box to generate smaller reports.

Max report size
This specifies the maximum size in bytes for generated reports - reports larger than this value are truncated, and an alert message is added to the bottom of the report. You may use the suffixes "MB" or "KB" as appropriate. A maximum size must be specified; there is no way to specify an unlimited size.

Report header link URL
Will create a URL link in the header of a report.

Result Logging
If checked, every SQL query used to generate the charts and result tables is logged into Trace.log, located on the host server under the ...\Log directory.

Review wizard max image width
Determines the maximum image width in pixels for images shown in the review wizard. Images wider than the specified limit will be truncated.

Implied Permissions
HiSoftware Compliance Sheriff has an implied permissions feature, which means that If you give a user "edit" or "view" permissions to a specific scan group or checkpoint group, the user will automatically be granted "edit" or "view" permissions to the individual scans or checkpoints contained in that group. Additionally, if you give a user permission to create scans or checkpoints, and the user already has “edit” or “view” permissions for one or more scan groups or checkpoint groups, then when the user creates a new scan or checkpoint and adds it to one of the user's permissible groups, the user will automatically be granted “edit” or “view” permissions to it.

Please note that a "deny" permission, such as "deny edit" or "deny view", does *not* override an existing implied permission. The reason for this is that a "deny" permission already grants an implied permission: If you define a group with a "deny view" permission for the scan "Top Secret Scan", you are, by implication, giving the user permission to view all scans except "Top Secret Scan".

Please also note that if you do not specify a permission for an object type, then the users of that group will not see those objects.

Scanner Settings

Allow invalid SSL certificates
This option is checked by default, and users can access these sites if they choose to do so. When unchecked, sites using invalid SSL certificates (for example, sites with expired or non-trusted root certificates) will not be crawled.

Browser load retries
This value provides additional control over how long to wait for Internet Explorer to become responsive when executing client scripts or transaction scripts.

Browser load timeout
This sets the maximum time in milliseconds to wait for pages to load when "Execute client scripts" is used, or when the loading is part of a transaction. Setting this too long can cause scans to run very slowly; however, setting it too low can cause pages to be processed before all content has been processed and all scripts have finished running.

Cache all pages
Uncheck this to prevent the contents of scanned pages being saved on the HiSoftware Compliance Sheriff server, meaning that they must be re-downloaded when viewing source code highlighted with result detail information. Not suitable for scanning dynamic sites.

Http user agent
User agent string to use for scans that specify “default” for this setting.

Ignore script links
When selected, the crawler ignores potential URLs found inside JavaScript code, and ignores pages with URLs that are only found inside JavaScript code.

Link check exclude filter
Pages containing "logout" in the URL will not be scanned, because users may be unexpectedly logged out of a site whenever the scan runs. If you want to add additional filters to this field, use a regular expression. For a complete description of regular expressions, please visit the following page: http://www.regular-expressions.info/reference.html

Max page size
The maximum number of bytes that will be downloaded for any one page. Pages over the specified size will either be truncated (for text-based formats like HTML), or ignored (for binary formats like Office and PDF documents). The default is 1 MB (1048576).

Max threads
Maximum number of additional threads used to perform simultaneous downloads. Default is 10, the maximum recommended value is 20.

Purge after
Number of months after which to delete old database records.

Record all instances
Ensures that results from a scan are stored in the instances table. By default, the scanner only stores instances with a Failed/Warning or Visual result.

Resolve host aliases
Ensures that the crawler will cross over to the alias hosts if they've been configured.

Retries
Number of times to retry accessing any page after a failure. Default number of times is 3.

The time between retries is given by the Timeout parameter.

Certain failures will not cause retries, for example, 404 page not found.

Rollup after
Number of months after which to 'roll-up' old database records. It purges all except the last run for each month.

Timeout
Minimum number of milliseconds to wait before giving up on downloading a file. The default is 30000 (one half-minute).

It may wait longer than the specified time if simultaneous downloads are occurring.

Verbose
Check for detailed logging (default), un-check for errors and warnings only. A log file is created per scan or monitor, which is displayed when the scan/monitor status is opened. The log filename is based on the Scan ID, for example 2001.log, and is located in one of 2 areas:

- For normal scans/monitors - the host server's "logs" directory (the default location is C:\Program Files (x86)\HiSoftware\Compliance Sheriff\logs)
- For Scans run locally – in the following user's default directory on the machine where the scan was started:

%USERPROFILE%\Local Settings\Application Data\HiSoftware Toolbar\<Web location of HiSoftware Compliance Sheriff instance>\<Scan ID.log>

For example:
C:\Documents and Settings\Administrator\ Local Settings\Application Data\HiSoftware Toolbar\demo.hisoftware.com_HiCS\2001.log

Notification Settings

From
The 'from' address for all notifications. Default is no-reply@hisoftware.com.

Link notification text
This can be used to add additional text to the end of messages sent for notifications where **Send as link** is checked.

Retry delay
Number of milliseconds before retrying if initial attempt to send notification fails.

Send password
The password to use for SMTP authentication.

Send user name
The user name to use for SMTP authentication.

SMTP authenticate
Set to '1' if the SMTP server requires authentication.

SMTP server
The domain name or IP address of the SMTP server to use. The default is blank, which means to use the local server hosting HiSoftware Compliance Sheriff.

SMTP server port
The TCP/IP port used by the SMTP server.

SMTP use SSL
Check this box if the SMTP server requires authentication.

Web location
The web address of the HiSoftware Compliance Sheriff application. This is set dynamically by the web application and should not be edited.

Table Groupings for Views

Table groupings allows you to specify the order of results for various tables.

1. Click the **Settings** tab.
2. Click **Table Groupings for Views**.
3. Click the text field for the table you wish to customize.
4. Type the order you wish to see the results in.

Groupings must be separated by a comma and you can ONLY use groupings in the table selected. For example, you cannot use “Group” in the Result History table.

Groupings are case sensitive. For example, using “page” instead of “Page” will result in error when you attempt to display the views.

5. Specify the allowed groupings (Result, Scan, Monitor, Group, Checkpoint, Page).
6. Click **Save**.