

Assessment Management Platform QuickStart Guide



The Assessment Management Platform (AMP) is a distributed network of HP scanners (WebInspect, DevInspect, or QAInspect) controlled by a system manager with a centralized database.

Enterprise users in various locations can control any number of HP devices scanning Web applications or Web services. The resulting risk assessment data is gathered in a central SQL database to provide advanced reporting and trending capabilities.

Configuration Requirements

Before installing AMP version 9, make sure that your system meets the following minimum requirements:

All Products

- Microsoft .NET 3.5 SP1
- Microsoft Internet Explorer 7.0 or 8.0, or FireFox 2.x or 3.x
- An active Internet or intranet connection

AMP Server

- 4 GB of RAM
- 5 GB (remote database) or 20 GB of free disk space (local database)
- 2.5 GHz processor or better
- Microsoft IIS 6.0, 7.0, or 7.5
- Windows Server 2003 SP2 or 2008 SP2 or 2008 R2

AMP Console/Client

- 1 GB of memory
- 2 GB of free disk space
- 1.5 GHz processor or better
- Windows XP Professional SP3 32-bit or Windows Server 2003 SP2 32-/64-bit or Windows Vista SP2 32-/64-bit or Windows 7 32-/64-bit or Windows Server 2008 SP2 32-/64-bit
- Microsoft SQL Server Express Edition 2005 SP3 or 2008 SP2 (required only if you want to edit policies, compliance templates, or audit inputs)
- Microsoft Silverlight Runtime v3 (required only if you want to use the Scan Linkage Analyzer and Attachments)

AMP Sensor (WebInspect 9.0)

- 2 GB of RAM
- 2 GB of free disk space
- 1.5 GHz processor or better
- Windows XP Professional SP3 32-bit or Windows Server 2003 Standard SP2 32-bit or Windows Vista SP2 32-/64-bit or Windows 7 32-/64-bit or Windows Server 2008 SP2 or R2 32-/64-bit
- Microsoft SQL Server Express Edition 2005 SP3 or SQL Server 2005 SP4 or SQL Server Express 2008 SP2 or SQL Server 2008 SP2 or R2
- The minimum screen resolution for WebInspect is 1024 x 768. For best performance, use a screen display of 1280x1024.

AMP Database

- 2 GB of RAM
- 20 GB of free disk space
- 2.5 GHz processor or better
- Microsoft SQL Server Standard Edition 2005 SP4 or 2008 SP2 or R2
- Windows Server 2003 SP2 32-/64-bit or Windows Server 2008 SP2 or R2 32-/64-bit

For an AMP environment to support Internet Protocol version 6 (IPv6), the IPv6 protocol must be deployed on each AMP Console, AMP Sensor, and the AMP Server.

AMP Components

AMP comprises the following:

- The AMP server/manager
- The AMP console (which provides the graphical user interface to the system manager)
- The AMP Web console (a browser-based interface designed specifically for non-administrative functions)
- AMP Quality Center service (if integrating with HP Quality Center)
- Scanners. Two types of scanners are supported:
 - Sensor - This is the WebInspect application when connected to AMP for the purpose of performing remotely scheduled or requested scans with no direct user interaction through its graphical user interface. It receives instructions exclusively from the configurable connection to an AMP Manager.

- Client - A client is any HP scanner (WebInspect or QALInspect) that connects to AMP to receive license, permissions, updates or scan data, and which also presents a user interface through which scans may be conducted. AMP controls permissions for a client and also provides the policies and compliance templates used by clients.

AMP Software Installation

Apply all available service pack upgrades and patches to all operating systems. For an AMP environment to support Internet Protocol version 6 (IPv6), the IPv6 protocol must be deployed on each AMP Console, AMP Sensor, and the AMP Manager.

Typical installations will have one SQL server, one or more consoles, and multiple sensors. These components can be distributed across your network in any way you like, but you must configure at least one of each. The AMP console connects to the AMP server via HTTP/S. This connection must be reachable by the AMP console and the AMP sensor.

Save the installation program to your hard drive and copy it to a CD, or save it to a network location that can be accessed by each machine on which you expect to install a component.

When installing components on different machines, begin with the one on which the server will be installed. **Install the server on one machine only.**

Note: Before installing the sensor or the manager, make sure the Microsoft Administrative Tools/Services window is not open.

Server/Manager Installation

1. Start the installation program.
2. On the *Welcome* page, click **Next**.
3. Review the license agreement. If you accept, select the check box and click **Next**; otherwise click **Exit**.
4. Select the folder into which you want to install the software and click **Next**.
5. When ready to install, click **Install**.
6. After installation, click **Finish**.
7. When the Initialization Wizard appears, click **Next**.
8. On the *Activate AMP License* window, enter the Activation ID sent to you by HP. If using a proxy server, select **Use Proxy Server** and provide the requested information.
9. Click **Next**.

The *AMP License User Information* window displays user information as submitted to HP.

10. Click **Next**.

This form is submitted to an HP server, which accesses a corporate database to retrieve and download license information.

11. When the *AMP License Information* window appears, click **Next**.
12. On the *SQL Server Information* panel, enter the name of the SQL Server and select the authentication method that will be used. If you are upgrading from a previous version of AMP, you must have at least "read access" to the database. If you are installing AMP 9 for the first time, then you must have privileges to create a database (or your database administrator must create a blank database and assign ownership to you).
13. Click **Next**.
14. On the *Database Selection* window, choose one of the following:
 - To use a new database, select **Create new database** and enter the database name. You must have privileges to create this database.
 - To upgrade from an AMP 8 database, select **Use existing database** and select one from the list. You must have owner privileges for that database.
15. Click **Next**.
16. For an existing database only, the *AMP Database Upgrade* window appears. Enter a name for the new database and click **Next**.
17. On the *Setup AMP Manager WebService* window, enter the root Web site and the name of the IIS virtual directory. If you are upgrading, do not choose the same IIS Virtual Directory name used previously.

If you select **Require Secure Channel (SSL)**, add and/or select an SSL certificate. Note: SSL is highly recommended.

These entries create the URLs for the following components.

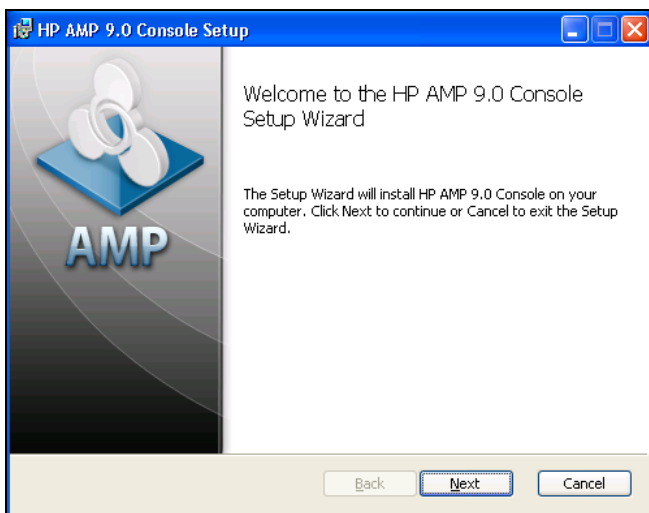
- AMP Console: `http(s)://<AMP server computer name>/<virtual directory name>/`.
- AMP Web Console: `http(s)://<AMP server computer name>/<virtual directory name>/WebConsole`

18. Click **Next**.
19. On the *Setup the AMP Manager User* window, enter the local or domain user account that you want to associate with the AMP Manager Web Service. For AMP to work properly, this account must be a local administrator. This enables the AMP Manager to install service packs and patches released by HP.
20. Click **Next**.

21. On the *Setup AMP Database User* window, specify how the AMP Manager should connect to the AMP database.
 - **Windows Authentication** - The name and password specified in the AMP Manager's user account is used to authenticate to the database. When working in a domain environment, the AMP Manager's user account should be a domain account. When working in a workgroup environment, you must have the exact same user name and password on both the AMP Server and the database computers.
 - **SQL Authentication** - Enter the SQL server user name and password.
22. Click **Next**.
23. On the *Ready To Start* window, verify your previous choices.
 - To change settings, click **Back**.
 - To begin configuration, click **Next**. The program creates and populates the database, and initializes other database and system components.
24. When the program displays the initialization results, click **Next**.
25. On the *Sensor Users* window, click **Add** and enter the user accounts that will be associated with the sensors (WebInspect installations).
26. Click **Next**.
27. When installation is complete, the following window appears. Click **Finish**.

Console Installation

1. Start the installation program.



2. On the Welcome page, click **Next**.
3. Review the license agreement. If you accept, click **Next**; otherwise click **Cancel**.

4. Select the folder into which you want to install the software and click **Next**.
5. Click **Next**.
6. When the process is complete, click **Finish**.

WebInspect (Sensor) Installation

1. Start the installation program.
2. On the Welcome page, click **Next**.
3. Review the license agreement. If you accept, click **Next**; otherwise click **Cancel**.
4. Select the folder into which you want to install the software and click **Next**.

The *WebInspect Setup* dialog appears.

5. Select **Configure WebInspect as an AMP Sensor**.
6. On the *AMP Sensor Configuration* window, specify the URL of the AMP manager.
7. In the **Sensor Authentication** group, enter the Windows account credentials for this sensor. Be sure to add this account to the list of sensor users using the AMP Administration module. See above.
8. Click **Next**.
9. Click **Install**.
10. When the process is complete, click **Finish**.

Quality Center Service Installation

If you plan to integrate AMP with an HP Quality Center installation (which would allow you to submit vulnerabilities to Quality Center as defects), you must install the Quality Center service. The AMP QC service must be installed on a machine that also has the Quality Center client application installed.

Note: Beginning with version 11, HP Quality Center has been renamed HP Application Lifecycle Management (ALM). If you are integrating ALM with AMP, you must also install the Connectivity Add-in as part of the ALM installation; select Add-Ins Page from the ALM main window.

AMP QC Service installation can be launched from AMP Server installation wizard.

Configuration information is maintained in a file named *QualityCenterService.conf*, which is stored on the machine on which the service is installed. The default location is *C:\Documents and Settings\All Users\Application Data\HP\AMP\8.0\QualityCenterService*.

Refer to the AMP user Guide for configuration information.

Upgrade Considerations

Observe the following guidelines if you are upgrading from AMP 8.1.

- You cannot upgrade to AMP 9 from versions previous to 8.10.
- AMP 9 does not support versions of WebInspect prior to 7.0 and requires WebInspect 8.0, 8.10, or 9.0 to support AMP's new scan visualization feature.
- Make a back-up copy of your database.
- The AMP 9 database must be installed on the same database server used by AMP 8.10.
- Before upgrading, use your SQL Server configuration tools to confirm that the hard drive on your database server contains free space equal to at least 3-4 times the size of your existing database. This is because you need to have room for the new database and about 2-3 times the database size for the SQL Server transaction log. For example, if you have a 30 GB AMP 8.10 database, then you will need at least 90-120 GB of free disk space for the upgrade to succeed. Once the upgrade has succeeded, you should be able to shrink your new database's transaction log to a more reasonable size.

Start the AMP Console

1. At a machine on which you have installed the AMP Console, click **Start > All Programs > HP > HP AMP 9.0 Console > AMP 9.0 Console**.
2. On the **Log On** tab, select or enter the URL of the AMP manager.
3. Select one of the following logon options:
 - To log on using your Windows user account, select **Log on as the current Windows user**.
 - To use a different account, select **Log on as**, then enter the user name and password for an account that has permission to access the console. For new installations, use the account name and password of the user who installed the AMP server software. This user is permitted to perform all restricted functions.
4. To use a proxy server to reach the AMP manager, click the **Proxy** tab and select one of the following:
 - **Use the Internet Explorer proxy** (to use the proxy server specified in Tools/Internet Options/Connections/LAN Settings).
 - **Use the proxy below**, and then provide the requested information.
5. Click **OK**.

Note: If you see the message "The AMP Server refused the request," you may have entered your user name and

password incorrectly, or your account has not been assigned to a role.

Create Organizations and Projects

Administrative authority within AMP is distributed across three levels: system, organization, and project. Each level has at least one administrator. The person who installed the AMP software is, by default, the system administrator. If this person does not intend to perform the initial configuration, he must explicitly designate another user as administrator for the default organization and default project.

Note: If you are upgrading from AMP 8.0 and want to migrate your database to AMP 9.0, the AMP Initialize program ports all your sites, roles, and objects to the AMP 9.0 default project.

1. Click the **Administration** group.
2. Click the **Roles and Permissions** shortcut.
3. Select **AMP System** in the Hierarchy pane.
4. Click **Action** and select **Add Organization**.
Every system must have at least one organization.
5. On the *Create Organization* dialog, type a name for the organization and click **OK**.
6. In the Hierarchy pane, select the organization you just added.
7. Click **Action** and select **Add Project**.
Each organization can have one or more projects.
8. On the *Create Project* dialog:
 - a. Type a name for the project in the **Name** box.
 - b. Select **Allow access to all of the organization's current resources**.
 - c. In the **Scan Permissions** group, click **Add**.
 - d. Type a host name (wild cards allowed), IP address, or IP address range, and click **OK**.
 - e. Click **OK** to close the *Create Project* dialog.

Notice that users who create an organization or project are automatically assigned as administrators of that organization or project.

Select Organization Resources


You can specify which resources are available to an organization. For example, the AMP system contains 17 scanning policies. Your organization may choose to allow only 10 of them.

1. In the Project Hierarchy pane, select the organization you created.

2. Click the **Resources** tab.

3. Select an item in the **Object Type** list.

All instances of those object types are displayed in the **Available** column.

4. Click  to move all object types to the **Allowed** column.

Note: The project administrator may further restrict which resources are available to a project.

5. Repeat Steps 3-4 until all resources are in the **Allowed** column.

Define Project Roles

A role is a named collection of permissions. You can allow other users to access the AMP console and perform functions you specify by assigning them to a role, based on their Windows user accounts.

1. In the Project Hierarchy pane, select the project you created.
2. Click the **Roles** tab.
3. Click **Add**.
4. On the *New Role* dialog:
 - a. Type "Tester" in the **Name** box.
 - b. From the **Default** list, select the permission that will be assigned, by default, to each activity associated with this role. For this demonstration, click **Allowed**.
 - c. Click **OK**.
5. In the Permissions area, expand the nodes to view the activities associated with each category. You can change permission for an individual activity by clicking "Allowed" and then clicking the associated drop-down arrow.

Assign Users to Roles

Note: If you are upgrading to AMP 9.0, the installation program assigns your users to the same roles enumerated for 8.0. If you are upgrading with a database migrated from another domain, users will appear in Roles as <unknown>.

1. Select "Tester" from the **Role name** list.
2. Click **Add** (to the right of the **Group or user names** list).
3. On the *Select Users or Groups* dialog, select a domain or work group in the **From this location** list.
4. In the text box below, type a Windows account name.
5. To verify the name, click **Check Names**.
6. Click **OK**.


Select Project Resources

Note: If you are upgrading from AMP 8.0, the installation program automatically assigns all resources to the AMP 9.0 default project.

You can specify which resources are available to projects within an organization. For example, the AMP system contains 17 scanning policies. Your organization may choose to allow only 10 of them. Of those 10 available, you might choose to allow only 5 to be used in your project.

1. Click the **Resources** tab.
2. Select an item in the **Object Type** list.

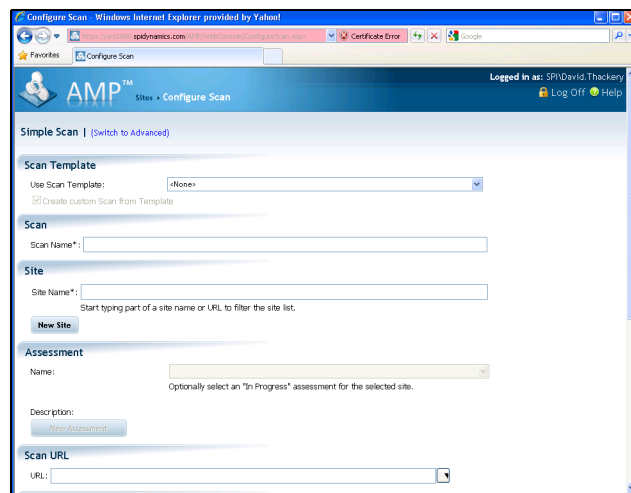
All object types permitted by the organization to be used by the project are displayed in the **Available** column.

3. Click  to move all object types to the **Allowed** column.

Note: The project administrator may further restrict which resources are available to a project.

Start a Scan

1. On the AMP console toolbar, click **Web Console**.
2. If necessary, click **Continue to this website**.
3. On the AMP Welcome page, click **Log On**.
4. Enter your credentials and click **OK**.
5. On the AMP Web Console navigation pane, click **New Scan**.



6. Provide the requested information. For detailed assistance, click **Help**.
7. After supplying all options, click **Scan Now**.

An assessment is a virtual workspace for your scans and vulnerability information, allowing you to bring together all the results of your web application investigation into one

Assessment Management Platform

Using Assessments



centralized location. Within an assessment, you can combine data from multiple scans, remove duplicate vulnerabilities, add manually found vulnerabilities, and attach documentation such as notes and screenshots. This new concept in AMP v.9 shifts the Quality Assurance focus from individual scans to a repository of findings that are accumulated during the entire testing phase and throughout the life cycle development process.

Correlation between Scans in an Assessment

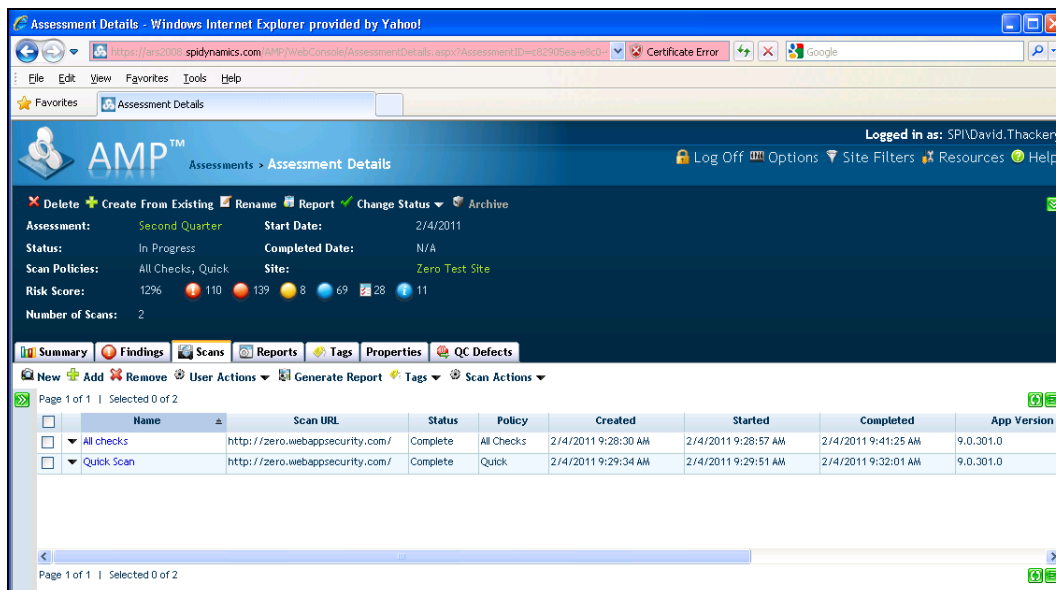
AMP v9 can compare the results of several dynamic scans and determine which vulnerabilities are actually multiple occurrences of the same issue. It performs this correlation by comparing the location of the vulnerability (URL, parameters, etc.), the nature of the vulnerability (cross-site scripting, SQL injection, etc.) and other attributes. This correlation occurs automatically when a scan is added to an assessment. Matched vulnerabilities are grouped into a “finding.”

Create an Assessment

- 1 In the Filtered Views group on the navigation pane, click **Sites**.
- 2 Select a site that has multiple scans.
- 3 Click the drop-down arrow next to the site name and select **Add an Assessment**.
- 4 Enter an assessment name (such as “*Second Quarter*”) and click **Finish**.

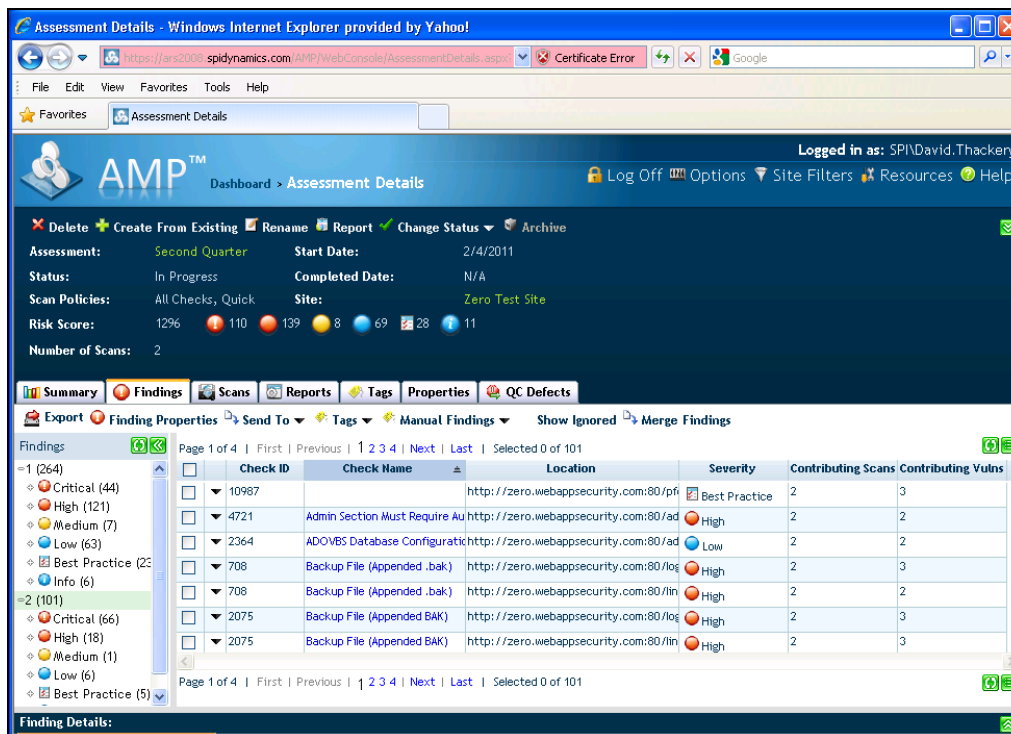
Add Scans to the Assessment

- 1 On the Assessment Details form, click the **Scans** tab and click **Add**.
- 2 Select two or more scans. In this example, two scans were added to the assessment. Both were conducted against the same site, but one scan used the Quick Scan policy and the other used the All Checks policy (which is more thorough and should uncover additional vulnerabilities).



- 3 Click the **Findings** tab.

When assessments are updated by adding scans, AMP automatically correlates the scan results into findings, as depicted in the following illustration.



The findings in the left column are grouped by contributing scans. Notice that both scans found 66 critical vulnerabilities and one scan found an additional 44 critical vulnerabilities. The Risk Score shows that the assessment contains 110 unique critical vulnerabilities, reflecting that correlation has eliminated the 66 duplicates.



The **Summary** tab on the Assessment Details form also illustrates successful correlation. The dotted bar on the “Finding to Severity” chart represents the total uncorrelated vulnerabilities as compared with the solid bar representing correlated (or unique) vulnerabilities.

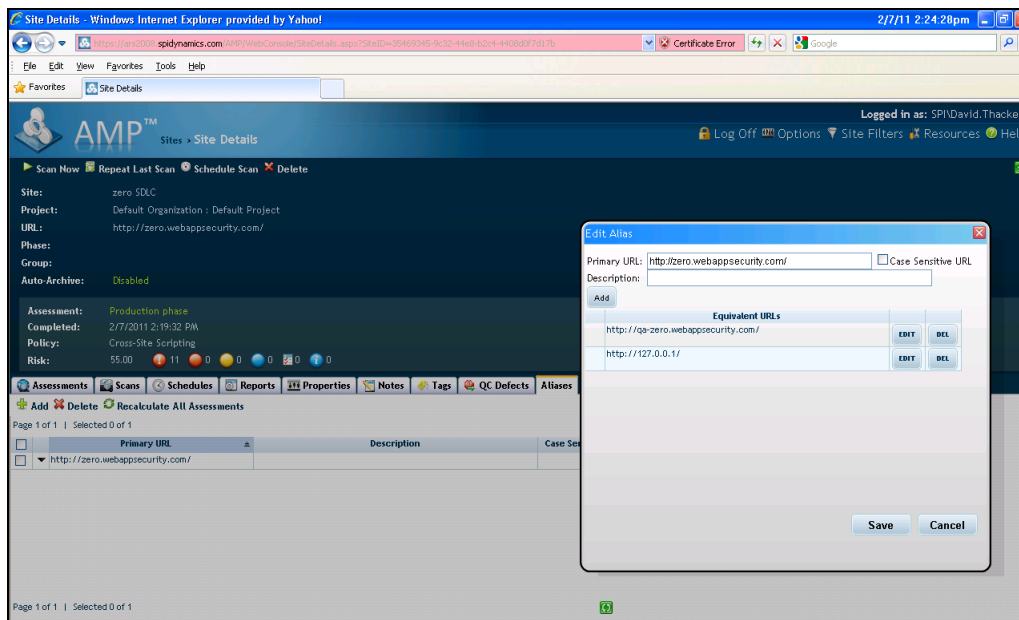
Correlation across Assessments

The following example illustrates how false positives can be carried over from one assessment to the next without any user intervention. It also illustrates AMP's new "alias" feature, which allows you to combine scan results from multiple URLs.

We have created three assessments for testing our site at different stages of the standard development process. For demonstration purposes, each assessment contains only one scan (although in practice, each assessment would typically contain multiple scans conducted over a period of time). The Development host is <http://127.0.0.1/>; the QA host is <http://qa-zero.webappsecurity.com/>; the Production host is <http://zero.webappsecurity.com/>. Because the hosts are different, AMP normally would not correlate the vulnerabilities and findings across the assessments. However, if we designate one of the URLs as the primary and then specify that the other two URLs are equivalent to the primary (thus creating an "alias" for the related URLs), AMP can correlate findings, false positives, and ignored vulnerabilities across all three assessments.

Create a Site

- 1 In the navigation pane, under Actions, click **New Site**.
- 2 For the site name, enter Zero SDLC.
- 3 For the URL, enter <http://zero.webappsecurity.com>
- 4 On the Site Details form, click the **Aliases** tab and then click **Add**.
- 5 On the *Add New Alias* dialog, enter <http://zero.webappsecurity.com> as the primary URL and click **Add**.
- 6 In the **Equivalent URLs** box, enter <http://127.0.0.1> and click **UPD** (update).
- 7 Click **Add** again, enter <http://qa-zero.webappsecurity.com> and click **UPD**.



- 8 Click **Save**.

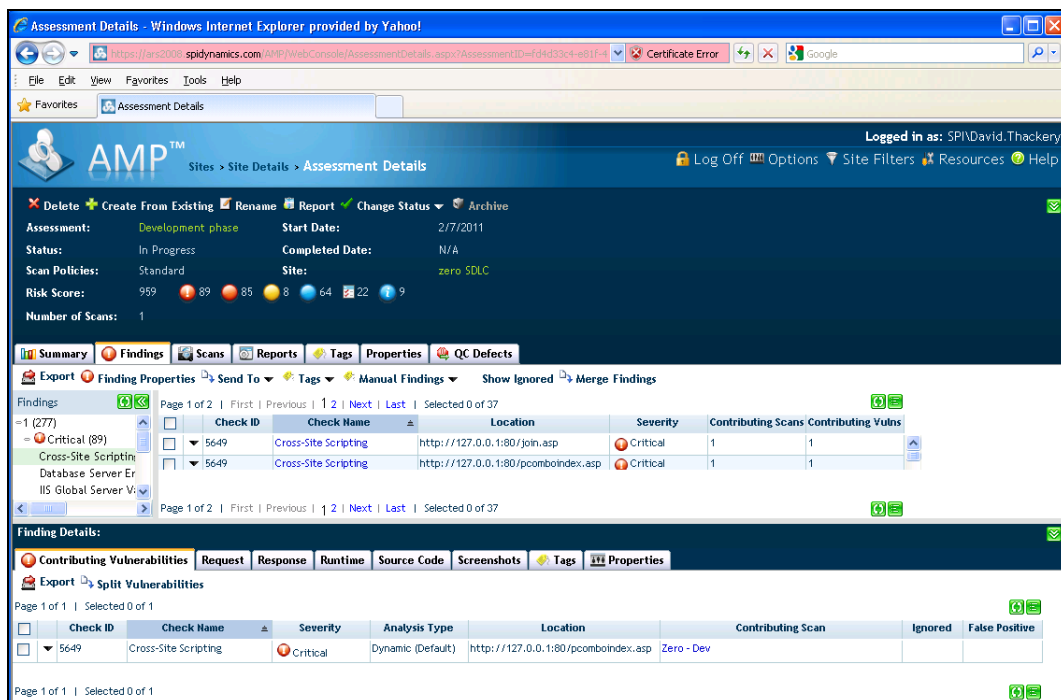
Create Assessment

- 1 In the navigation pane, under Actions, click **New Assessment**.
- 2 For the site name, enter Zero SDLC.
- 3 For the assessment name, enter Development Phase.
- 4 Click **Finish**.

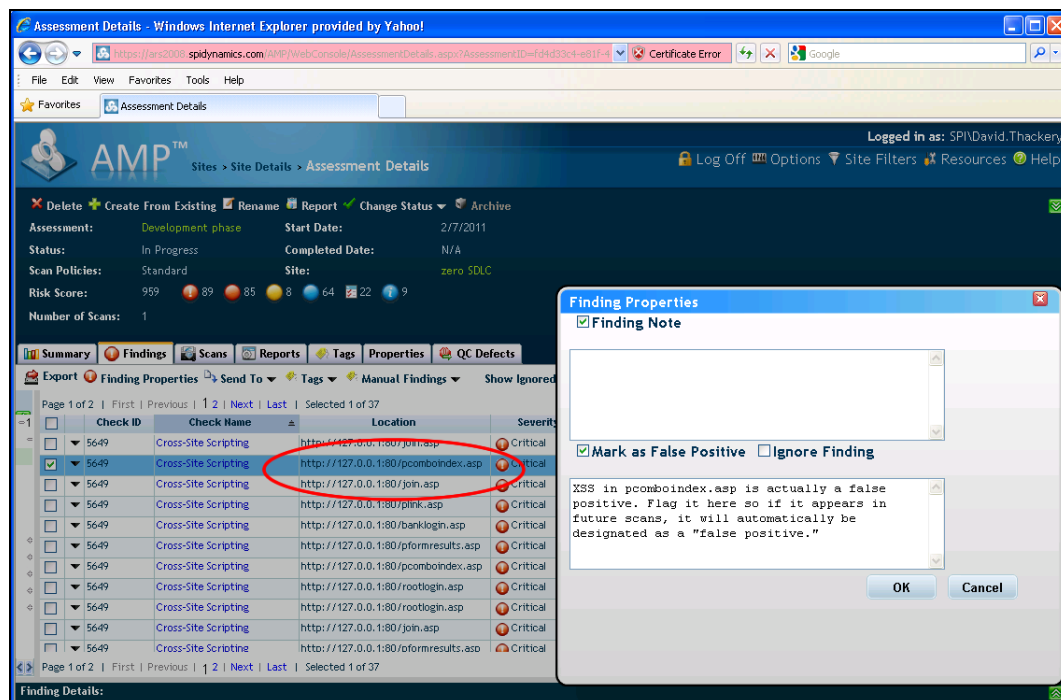
Conduct Scans

- 1 From the Assessment Details form, click the **Scans** tab and then click **New**. Note: if you had already conducted a scan, you could click **Add** to assign an existing scan to the assessment.

- 2 Configure the scan and click **Scan Now** (or **Finish**).
- 3 When the scan is complete, navigate to the Assessment Details form.
- 4 Click on the cross-site scripting check name in the Findings tree view (at left).
- 5 Click the pcomboindex.asp cross-site scripting finding to reveal (at the bottom) the list of vulnerabilities that contributed to this finding. Note that the False Positive column is not checked.

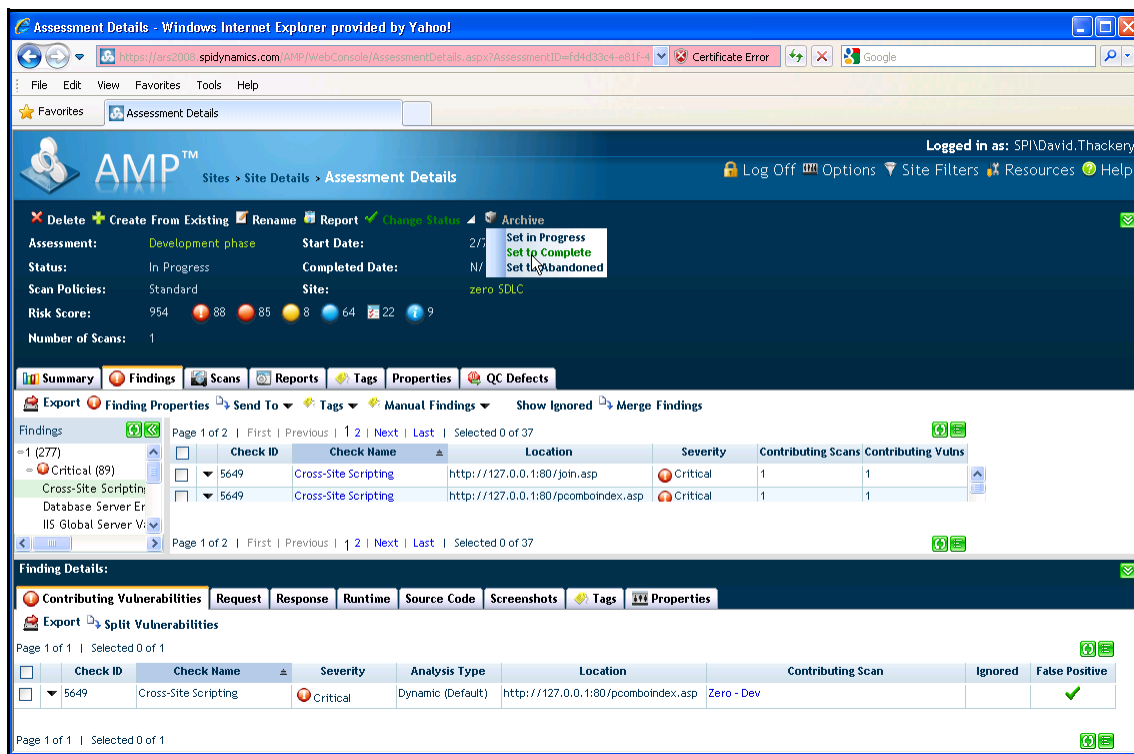


- 6 On the **Findings** tab, check the box next to the Check ID for cross-site scripting at pcomboindex.asp.
- 7 Click **Finding Properties**.



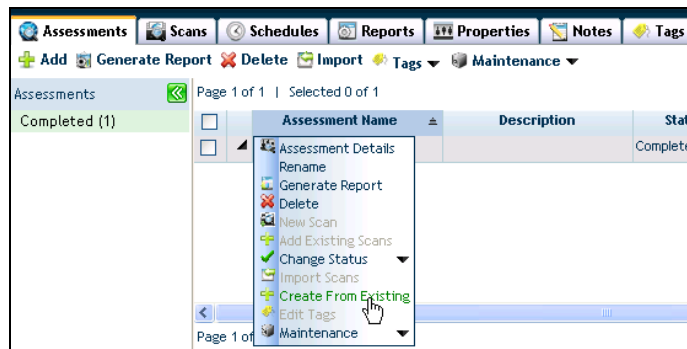
- 8 On the Finding Properties dialog, select **Mark as False Positive** and (optionally) add a note that explains the reason for your conclusion. Note: you can select multiple findings and mark them as false positive.
- 9 Click **OK**.

In real-world scenarios, you may conduct additional assessments while in the development phase. Then, when moving on to a new assessment, you would mark the previous assessment as complete.



In this example, the QA assessment represents the stage gate at the end of the QA process before moving on to the Production phase. We now need to create a second assessment for the QA phase.

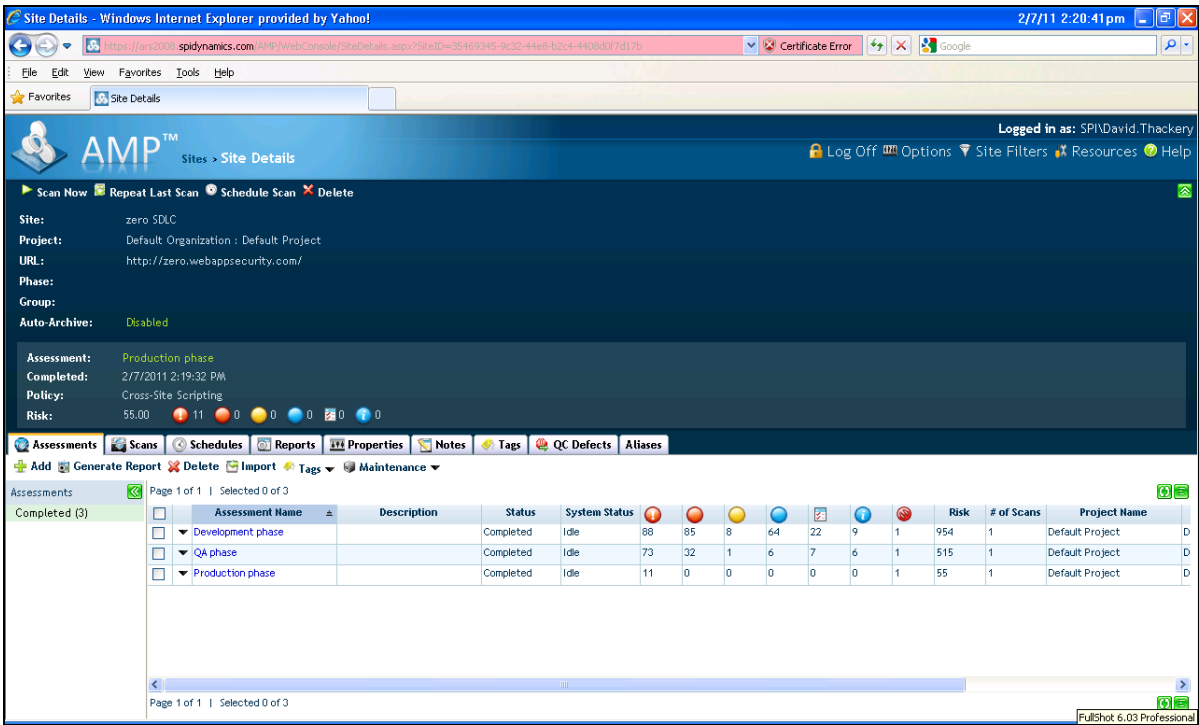
- 10 In the Site Details form, on the **Assessments** tab, click the drop-down arrow next to the Development Phase assessment and select **Create from Existing**.



This opens the settings page (not shown).

- 11 Enter QA Phase as the name for the new assessment.
- 12 In the Carry Over Information section, select **False Positives** and **Ignored Vulnerabilities**.
- 13 Click **Finish**.
- 14 Conduct a scan of <http://qa-zero.webappsecurity.com> and then mark the assessment as complete.
- 15 Create a third assessment named Production Phase, conduct a scan of <http://zero.webappsecurity.com/>, and then mark the assessment as complete.

So now we have three assessments, each marked complete, as illustrated on the Site Details form depicted in the following illustration.



- 16 In the navigation pane under Filtered Views, click **Assessments**.
- 17 Click the Production Phase assessment name to navigate to the Assessment Details form.
- 18 Click on the cross-site scripting check name in the Findings tree view (at left).
- 19 Click the pcomboindex.asp cross-site scripting finding to reveal (at the bottom) the list of vulnerabilities that contributed to this finding. Note that the False Positive column is checked because this vulnerability was flagged as a false positive in the first assessment (Development Phase) and was carried over through the QA phase and into the Production phase.

