CxSAST v8.0.0

Setup, Installation and User Guide

Contents

Version Release Notes

For version-specific CxSAST release notes, go to:

https://checkmarx.atlassian.net/wiki/spaces/KC/pages/9142278/CxSAST+Release+Notes

Checkmarx CxSAST Overview

Checkmarx CxSAST is a unique source code analysis solution that provides tools for identifying, tracking, and repairing technical and logical flaws in the source code, such as security vulnerabilities, compliance issues, and business logic problems.

Without needing to build or compile a software project's source code, CxSAST builds a logical graph of the code's elements and flows. CxSAST then queries this internal code graph. CxSAST comes with an extensive list of hundreds of preconfigured queries for known security vulnerabilities for each programming language. Using the CxSAST Auditor tool, you can configure your own additional queries for security, QA, and business logic purposes.

CxSAST provides scan results either as static reports, or in an interactive interface that enables tracking runtime behavior per vulnerability through the code, and provides tools and guidelines for remediation. Results can be customized to eliminate false positives, and various types of workflow metadata can be added to each result instance. These metadata are maintained through subsequent scans, as long as the instance continues to be found.

The input to CxSAST's scanning and analysis is the source code, not binaries, so no building or compiling is required, and no libraries need to be available. The code doesn't even need to be able to compile and link properly. Consequently, CxSAST can run scans and generate security reports at any given point in a software project's development life cycle.

CxSAST supports Open Source Analysis (CxOSA) enabling licensing and compliance management, vulnerabilities alerts, policy enforcement and reporting. CxOSA supports all the most common programming languages, enabling organizations to secure all their open source components in addition to the in-house developed code analysis coverage: (see Supported Code Languages and Frameworks).

You can integrate CxSAST into several aspects of your development cycle, such as with software build automation tools (Apache Ant and Maven), software development version control systems (GIT), issue tracking and project management software (JIRA), repository hosting services (GitHub), application vulnerability management platforms (ThreadFix), continuous integration platforms (Bamboo and Jenkins), continuous code quality inspection platforms (SonarQube) and source code management tools (TFS).

CxSAST scans can be manually activated, periodically scheduled, or initiated upon build by one of our integrated build systems.

CxSAST also supports a wide range of OS platforms, programming languages and frameworks.

CxSAST is deployed on a server and accessed by users via our web interface or one of our IDE plugins (Eclipse, Visual Studio and IntelliJ).

Please contact us with any issues, questions or comments, at: support@checkmarx.com

Setting Up CxSAST

This setup guide includes information on setting up CxSAST for trial, proof of concept (POC) and in production environments.

Setting Up CxSAST

- System Architecture Overview
- Server Host Requirements
- Preparing the Environment for Releases
- Installing CxSAST
- Modifying CxSAST
- Repairing CxSAST
- Backing Up CxSAST
- Upgrading CxSAST
- Adding a CxEngine Server
- Removing CxSAST
- Updating the CxSAST License

System Architecture Overview

CxSAST includes the following components:
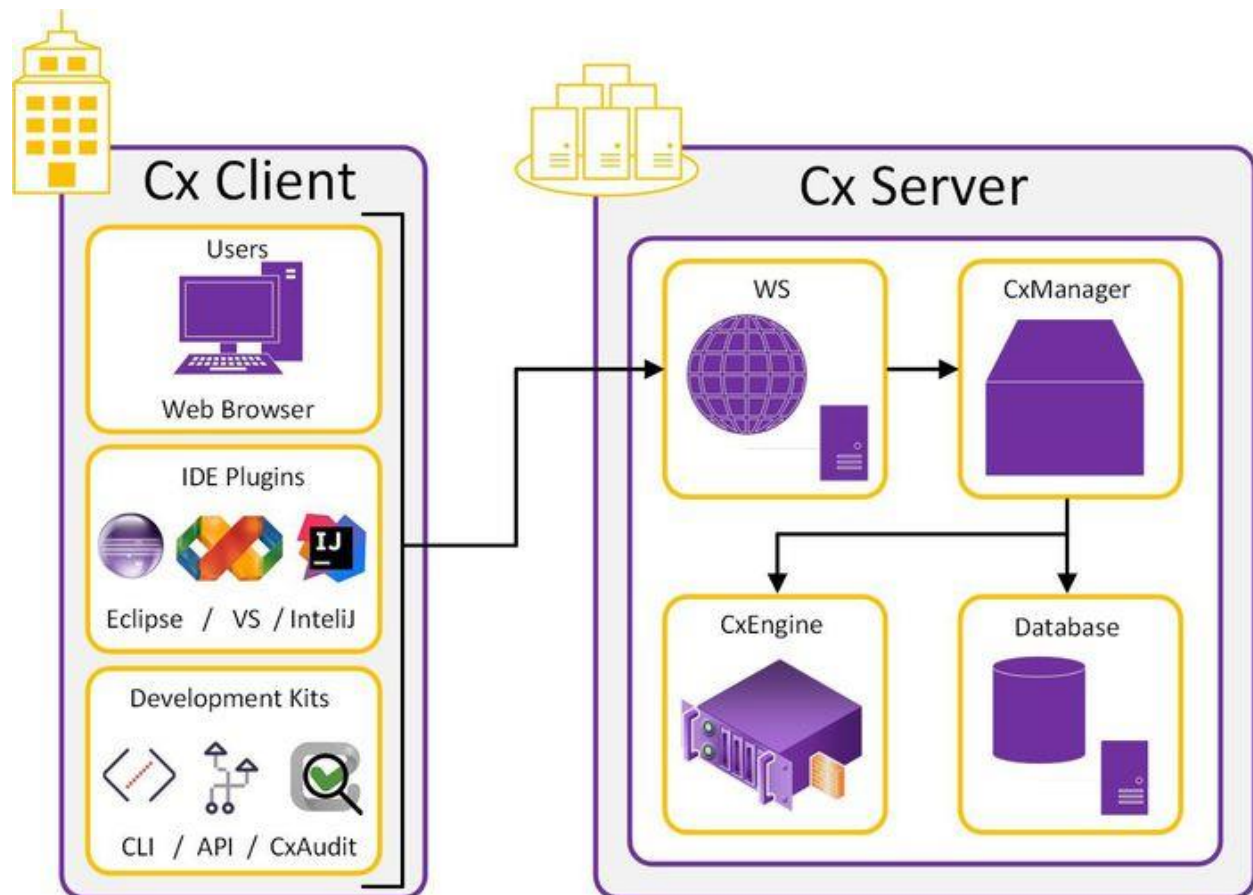
CxSAST Server Components

- **CxEngine**: Performs code scans
- **Database**: Stores scan results and system settings. Can be a new/existing commercial MS SQL Server, or for POC (Proof of Concept), SQL 2012 Express can be used. This is installed with CxSAST installer (if defined) when any version of SQL is not already installed
- **CxManager**: Manages systems, performs all system functions and integrates system components. Uses the IIS web server and is installed by the CxSAST installation, if not already installed
- **CxSAST Web Client -** The main interface for controlling CxManager actions (i.e. initiating scans, view results and generating reports).

CxSAST Clients (user interfaces):

- IDE Plugins
- CxAudit
- CxSAST CLI
- CxSAST API

CxSAST supports a Centralized Architecture, where all server components are installed on the same host, or a Distributed Architecture, where any or all of the server components are installed on dedicated hosts.

CxSAST also supports High Availability Architecture, where more than one CxManager is available to control system management, ensuring that in cases where one CxManager fails the system will continue to be fully operational.

Communication between clients and the CxSAST Web Client and CxManager as well as communication between the CxManager and the CxEngine, are via HTTP (by default). HTTPS can also be configured.

Centralized Architecture

Centralized computing is a type of computing architecture where all or most of the processing/computing is performed on a central server. Centralized computing enables the deployment of all of a central server's computing resources, administration and management. CxSAST supports centralized architecture, where all server components are installed on the same host.
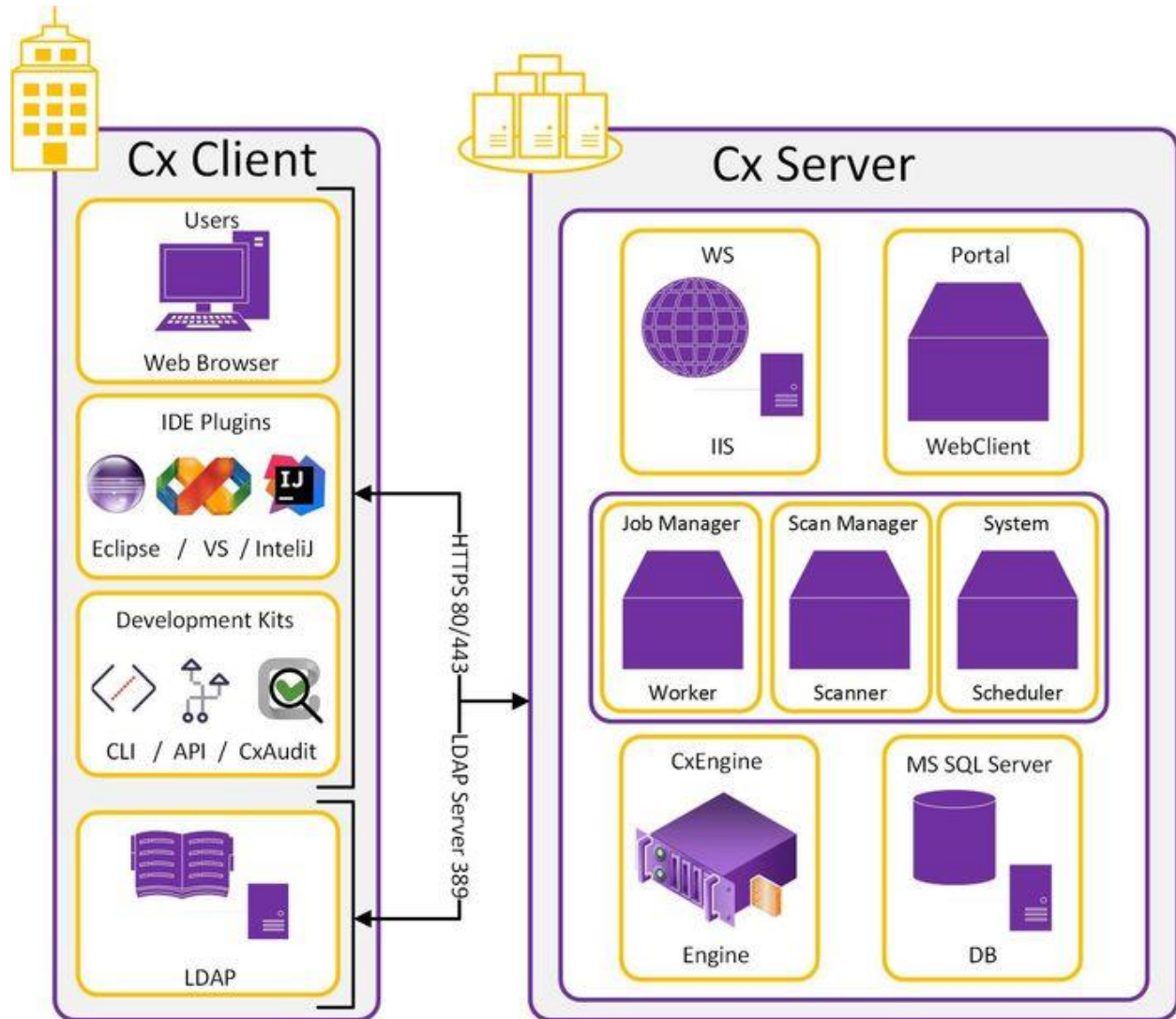
Distributed Architecture

In distributed architecture, components are presented on different platforms and several components can cooperate with one another over a communication network in order to achieve a specific objective or goal. CxSAST supports distributed architecture, where any or all of the server components are installed on dedicated hosts.
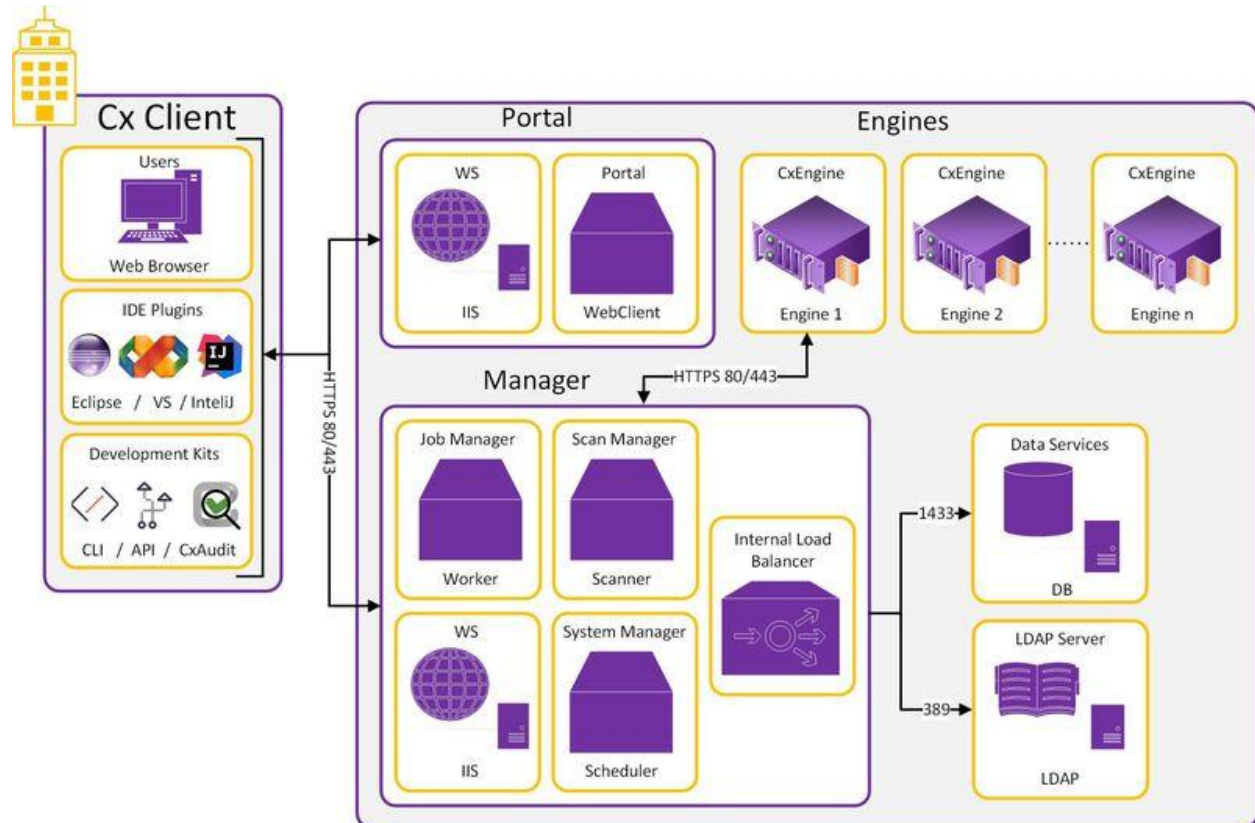
The basis of a distributed architecture is its transparency, reliability, and availability. Distributed architecture is the most recommended method for CxSAST deployment because all Cx components function at their most optimized capacity.

High Availability Architecture

High availability architecture is an approach of defining the components, modules or implementation of services of a system which ensures optimal operational performance, even at times of high loads. CxSAST supports high availability architecture, where two or more CxManager servers (in active-active mode) are installed behind an internal load balancer and can access the same database. This ensures that in cases where one CxManager fails the system will continue to be fully operational.
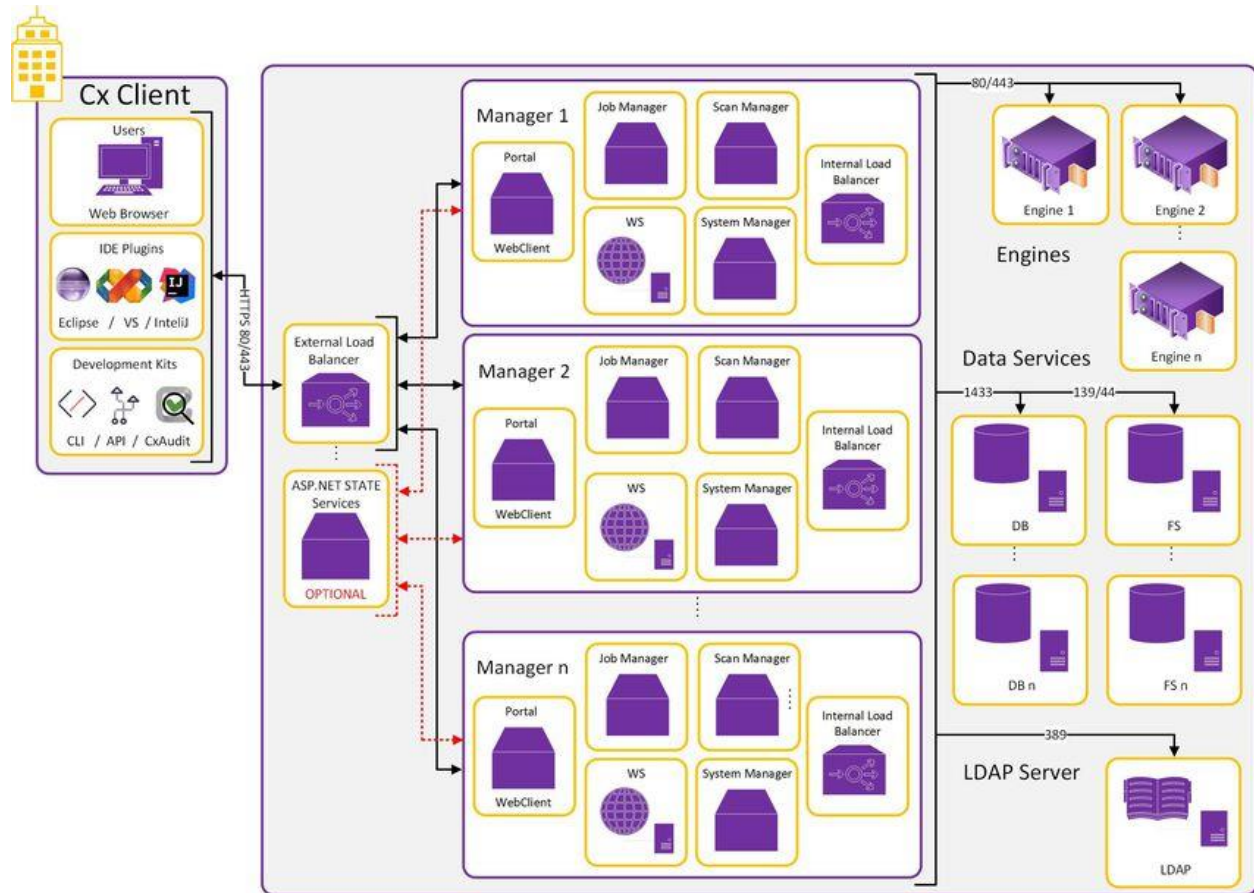
The main objective of implementing High Availability is to make sure CxSAST is always available for the systems users and clients.

ⓘ Please note that all CxManagers must be co-located in same data center. If you are interested in configuring a High Availability solution please contact Checkmarx support.

Server Host Requirements

Server host requirements depend on whether the installation is Centralized or Distributed, and on how many lines of code will need to be scanned. These requirements are also applicable for CxAudit.

> ⓘ For **POC**, Microsoft SQL Express (pre-installed with CxSAST) can be used. For **Production**, we recommend working with a commercial version of Microsoft SQL Server. The version used will depend on your scalability and performance needs. For more details about features supported by the different editions of SQL Server, please use the following link.

In addition to the requirements in the table below, in general, CPU clock speed and disk speed will affect scan time. For exact tested versions, see the CxSAST Release Notes.

Purpose	Lines of Code	Installed RAM**	Cores	CPU Speed	Disk	OS	Web Server	Other Software
Centralized (POC)	200K	6 GB	Recommended: 4 up to a maximum of 12 cores	2.8 GHz	50 GB (recommended)	Windows 7,8,8.1,10 Windows Server 2008R2 2012, 2012R2, 2016	IIS 7/7.5/8/ 8.5/10	Windows Installer 3.1 or above (Run msiexec to check) .NET framework 4.5.1 or above (Windows 7/8 will need .NET framework 3.5 as well because of IIS version)
	500K	8-16 GB						
Centralized (Production)	200K	6 GB	Minimum: 6 for 1 concurrent scan. Additional 4 cores for each additional concurrent scan, up to a maximum of **12** cores, (Recommended: 4, 6, or 8 cores) Max recommended concurrent scans: **3*** * Scans of 1M LOC or more are recommended to limit concurrency or run on their own distributed server.	2.8 GHz	250 GB (recommended)		IIS 7/7.5/8/ 8.5/10	
	600K	10 GB						
	1.2M	16 GB						
	2M	25 GB		2.8 GHz				
	3M	40 GB						
	4M	50 GB						
Distributed - CxEngine (Production) For multiple CxEngine servers (for concurrent scans), each server should meet the requirements	200K	5 GB	4 (per concurrent scan) up to a maximum of **12** cores (Recommended: 4, 6, or 8 cores)	Recommended: 2.8 GHz	100 GB (recommended)	Windows Server 2008R2 2012, 2012R2, 2016	NA	
	600K	9 GB						
	1.2M	15 GB						
	2M	24 GB		Recommended: 2.8 GHz				
	3M	36 GB						
	4.5M	50 GB						
Distributed - CxManager (Production)		8 GB	4	2.5 GHz	250 GB (recommended)		IIS 7/7.5/8/8. 5/10	
Distributed - Database (Production)		8 GB	4	2.5 GHz	250 GB (recommended)		NA	MS SQL Server (Express not recommended) 2008/2012/2014/ 2016

** Note: GB RAM / LOC numbers for Javascript are higher.

ⓘ	Note that the Checkmarx Server requires dedicated memory allocation; features such as Memory Ballooning cannot be used.

ⓘ	**Cloud Environments** Note that for Cloud environment installations (AWS, etc.), these requirements may not be exactly the same as for Centralized or Distributed installations because you are choosing from predefined hardware packages and not defining your own specifications.

For the CxSAST application, it is recommended to use a display with any one of the following resolutions; 1280x720, 1280x800, 1366x768, 1920x1080.

Preparing the Environment for Releases

The following sections include the environmental preparations needed for releases:

> **Contents**
> - Preparing the Environment
> - CxSAST Server Components Installed on Dedicated Hosts

Preparing the Environment

Once you understand System Architecture Overview, before installing CxSAST, make sure server hosts conform to server requirements, and prepare the following:

1. Make sure that the Centralized or CxManager host name does not contain any non-alphanumeric characters such as "_" . This is to avoid issues described here.

2. Make sure that organizational firewalls allow:
   - HTTP (TCP port 80):
     - From client hosts to the Centralized or CxManager host
     - Between CxManager and CxEngine (in a distributed architecture)
   - SQL Server traffic (by default, TCP port 1433) from CxManager to SQL Server (If using SQL Server, in a distributed architecture)
   - SQL Browser (UDP port 1434) - this will allow machines (i.e. on installation wizard) to scan for SQL Servers on the network

     > - If an SQL Server is not displaying in the Installation window, you can try typing the machine name or IP address directly into the Wizard
     >
     > - If an SQL Server uses a custom port, use a "," between the machine name/IP and port number, e.g. "10.199.76.1,65391" or "SSMACHINE,65391".

3. If using SQL Server, make sure the following services are running:
   - SQL Server
   - SQL Browser

     > SQL Express for POC can be installed by CxSAST installer, or use SQL Web/Standard/Enterprise 2008/2012/2014 for Production.

4. On server component hosts, prevent anitviruses from scanning the checkmarx folder, usually:
   - **C:\CxSrc**
   - Checkmarx installation directory: **C:\Program Files\Checkmarx** - **C:\Program Files(x86)\Checkmarx**

5. Configure IIS (except on database-only component server in a distributed deployment):

     > Turn off Compatibility Mode for the Windows IE 11 browser to work with CxSAST as an intranet site.

Configure IIS 7 on Windows Server 2008

1. Open the Server Manager by right-clicking **Computer** and selecting **Manage**.

2. In the left-hand navigation pane select **Roles**, and click **Add Role Services**:
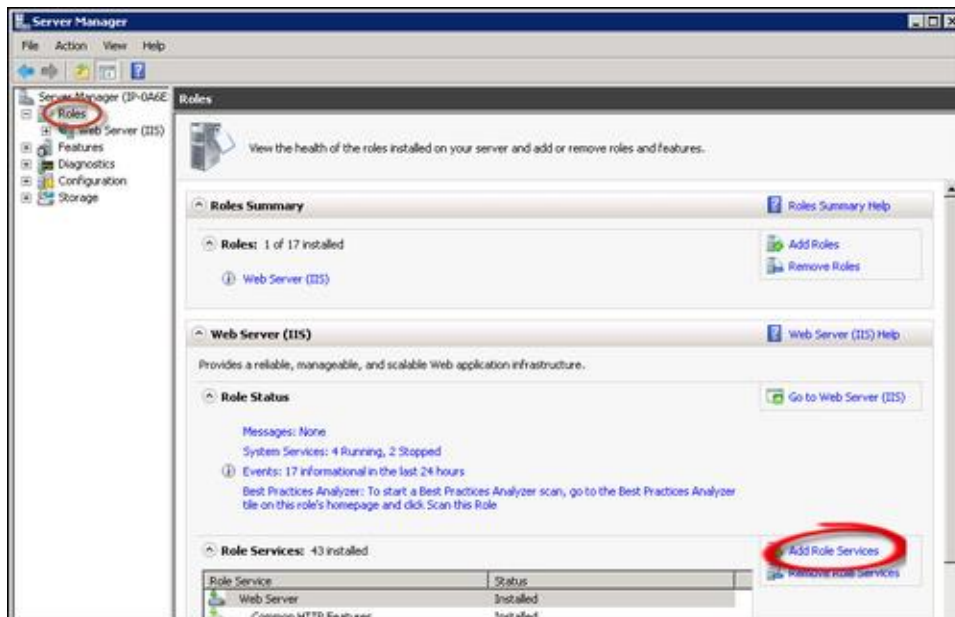
3. Scroll down and select the following:
   - **Static Content**
   - **World Wide Web Services** > **Application Development Features** > **ASP.NET**
     (Click OK to approve all dependent features)
   - In **Management Tools**:
     - **IIS Management Console**
     - **IIS 6 Metabase Compatibility**.
   - Click **Next**, and **Install**.

4. **Close** the window.

5. Download and install **.Net Framework 4.5.2** and all its updates.

6. Open a command prompt as an Administrator, and go to C:\Windows\Microsoft.NET\Framework64\v4.0.30319.

7. Run:
   ```
   ServiceModelReg.exe –ia
   ```

   NOTE: If the IIS Pools are not started automatically after the CxSAST installation, you should restart the machine.

Configure IIS 7 on Windows 7

1. Open the Control Panel.

2. In **Programs**, click **Uninstall a program**.

3. Click **Turn Windows features on or off**:
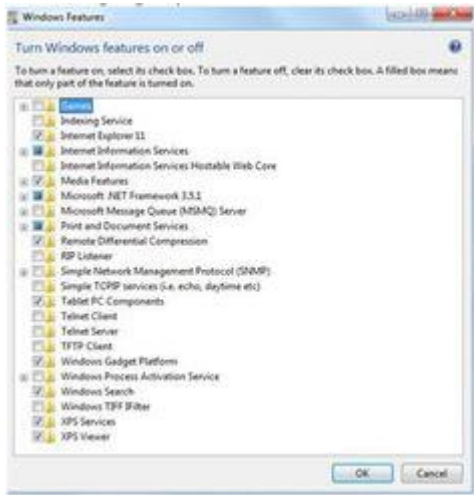
4. In **Internet Information Services**, select the following:

   o In **Web Management Tools**:

      ▪ **IIS Metabase and IIS 6 Configuration Compatibility**

   ▪ **IIS Management Console**

   o **World Wide Web Services** > Application Development Features > **ASP.NET** (Click OK to approve all dependent features)

   o **World Wide Web Services** > **Common HTTP Features** > **Static Content**

5. Click **OK**.

6. Download and install **.Net Framework 4.5.2** and all its updates.

7. Open a command prompt as an Administrator, and go to C:\Windows\Microsoft.NET\Framework64\v4.0.30319.

8. Run:

   ```
   ServiceModelReg.exe –ia
   ```
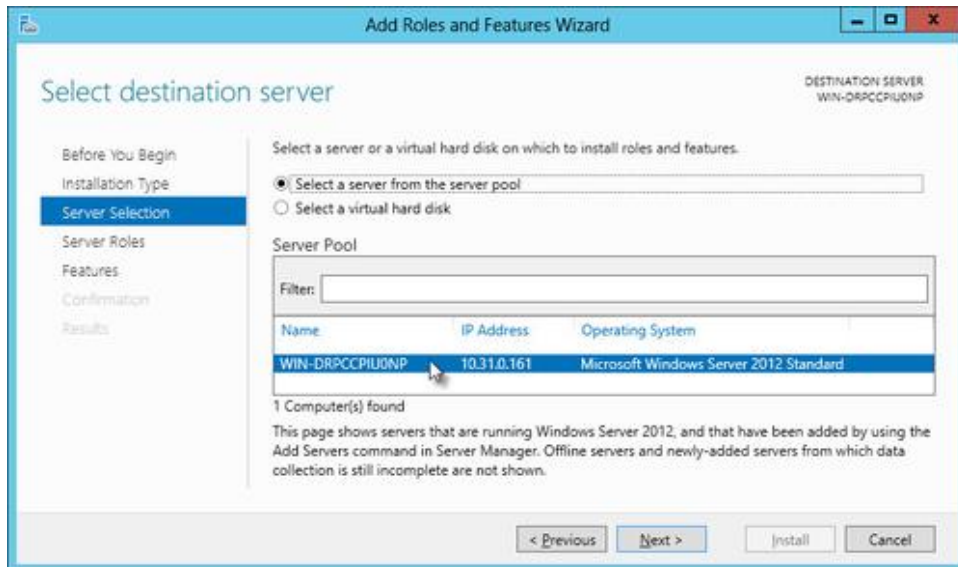
Configure IIS 8 on Windows Server 2012

1. Open the Server Manager and click **Add roles and features**:
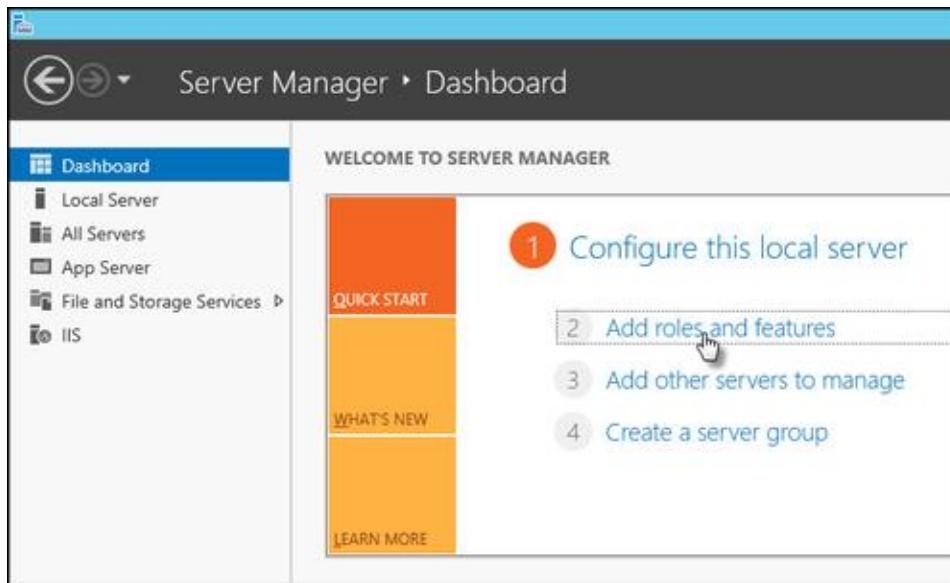
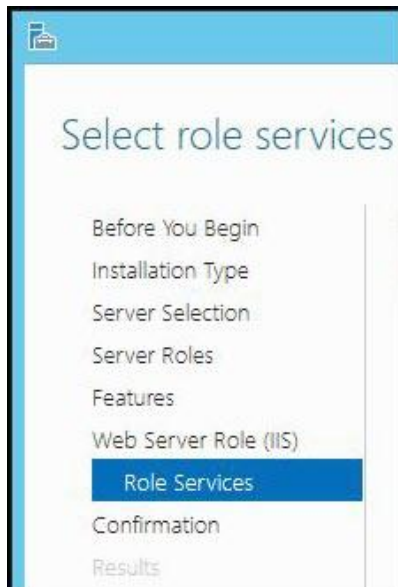2. Select **Installation Type**, and select **Role-based or feature-based Installation**:
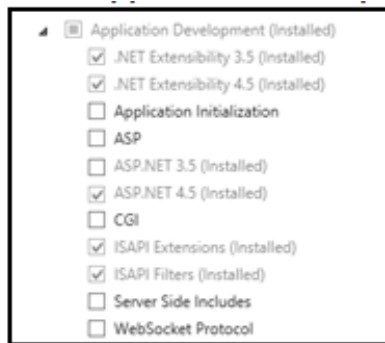

3. Click **Next**.

4. Select the server:

5. Click **Next**.

6. For Server Roles - Select **Web Server (IIS)** and Click **Next**

7. For Features - Select - .Net Framework 4.5 Features > WCF Services > **HTTP Activation** and click **Next**

8. Continue through the wizard until the **Web Server Role (IIS)** > **Role Services** page:

9. Select the following:

- o Common HTTP Features **> Static Content**
- o Application Development > **ASP.NET 4.5**
- o Management Tools > **IIS Management Console**
- o Management Tools > IIS 6 Management Compatibility > **IIS 6 Metabase Compatibility**

10. **Finish** the wizard, confirm and **Install**.
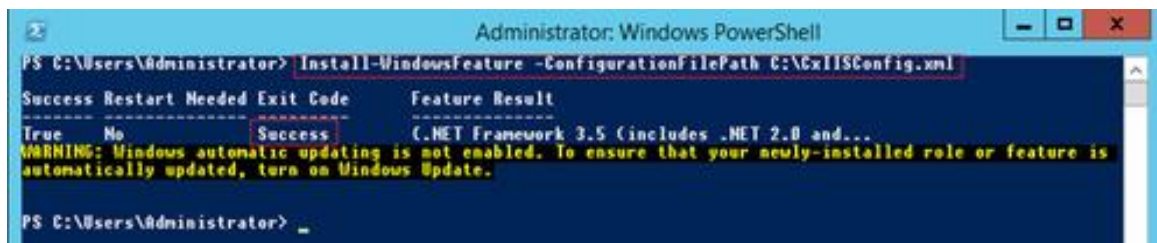
Configure IIS 8.5 on Windows Server 2012 R2

For IIS 8.5, Checkmarx provides a configuration file that can be used to automatically perform all necessary configuration. Alternatively, you can manually install IIS, in which case make sure to include IIS with - IIS Management Console, Static Content, ASP.NET 4.5 with all dependencies, IIS 6 Metabase Compatibility and .Net Framework 4.5 Features -> WCF Services -> HTTP Activation

To configure IIS 8.5 using the Checkmarx configuration file:

1. Download **CxIISConfig.xml.**
2. Run **Windows PowerShell** as an Administrator:

3. In PowerShell, run:
   Install-WindowsFeature –ConfigurationFilePath <path>**\CxIISConfig.xml**
   where <path> is the path to the directory where you put the configuration file.

ⓘ For correct synchronization the Checkmarx Server/CxAudit and the Database must be on the same timezone.
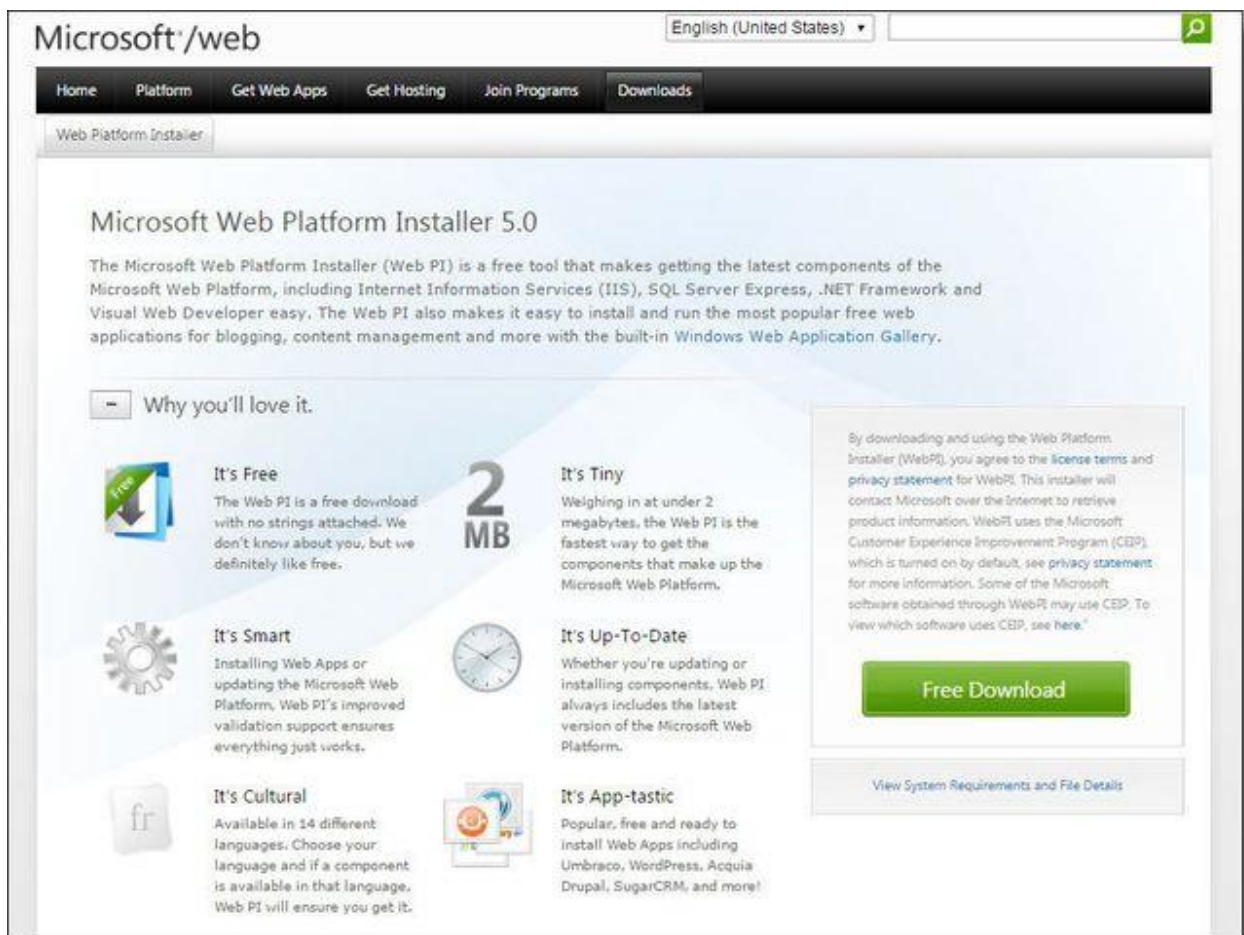
CxSAST Server Components Installed on Dedicated Hosts

CxSAST supports Distributed Architecture, where any or all of the CxSAST server components are installed on dedicated hosts.

The following procedure should be implemented in all installations or upgrades to any version that includes the new IIS application.

Once the IIS application components of the CxSAST setup have been installed, perform the following procedures:

Go to the Microsoft Web Platform Installer and click **Download**.

Run the **Microsoft Web Platform Installer** on the **Portal Server**. The **Microsoft Web Platform Installer** is displayed.
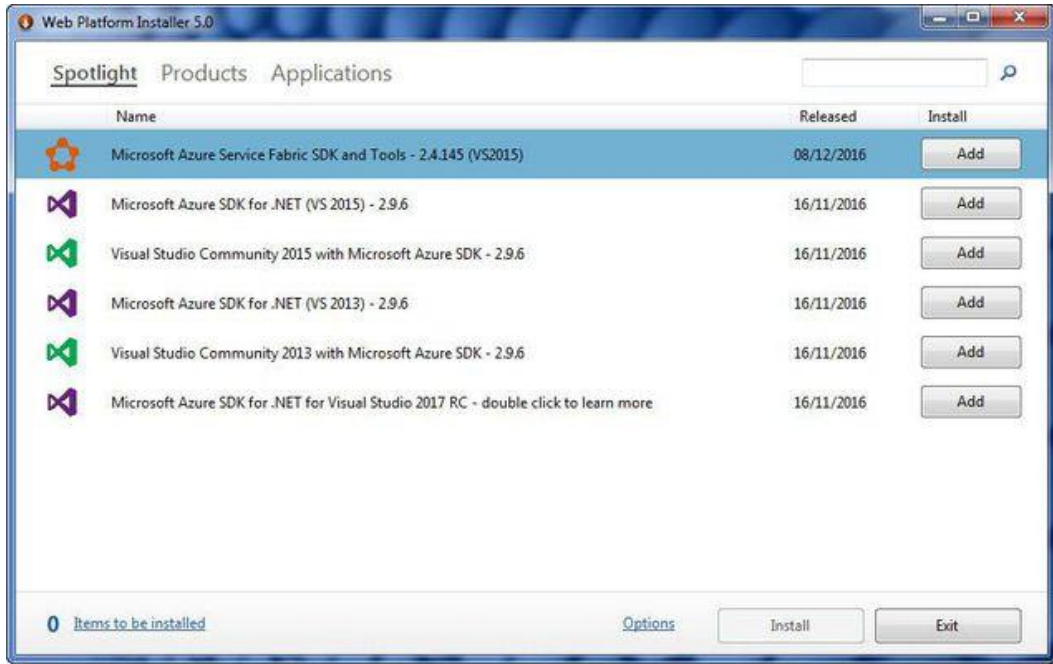
Search for the **Add URL Rewrite 2.0** module and click **Add**.
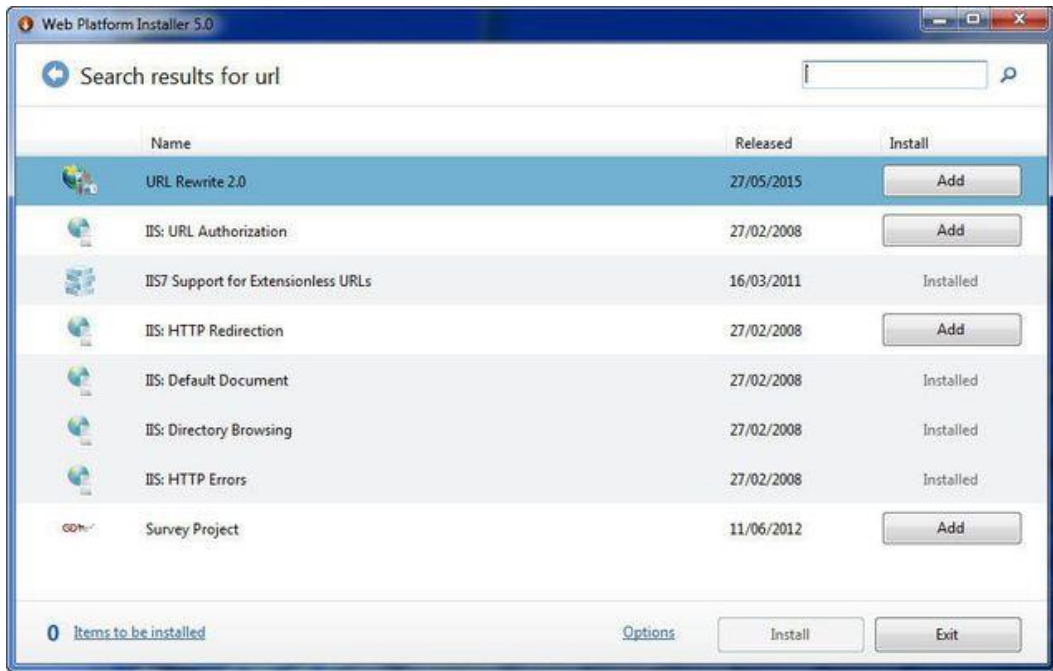
Search for the **Application Request Routing 3.0** module and click **Add**.
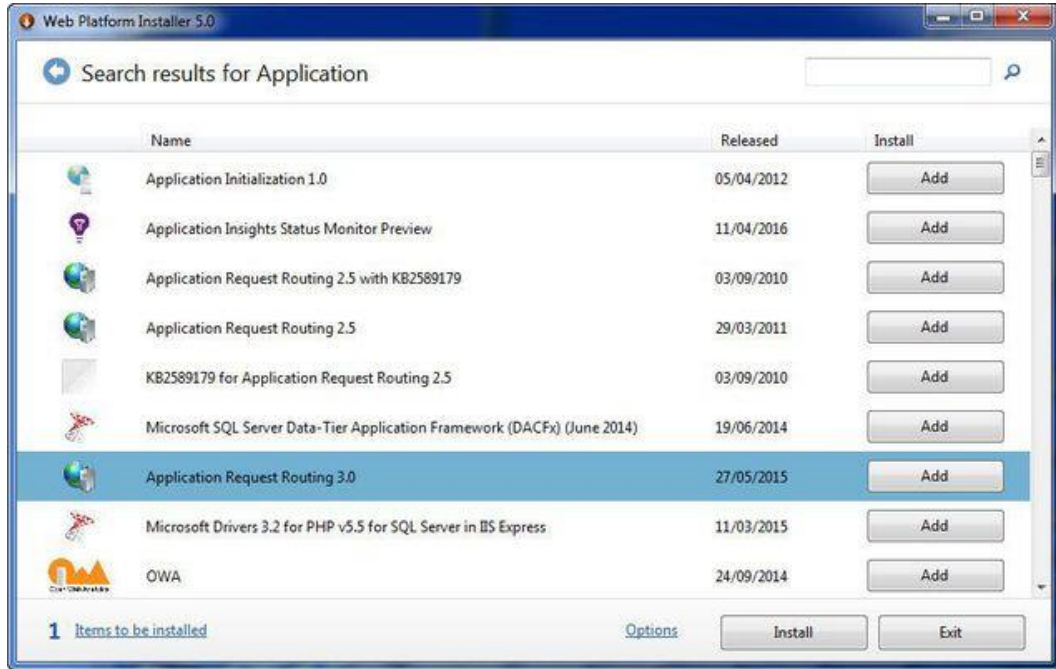
Click **Install**. The **Microsoft Web Platform Installer Prerequisites** are displayed.
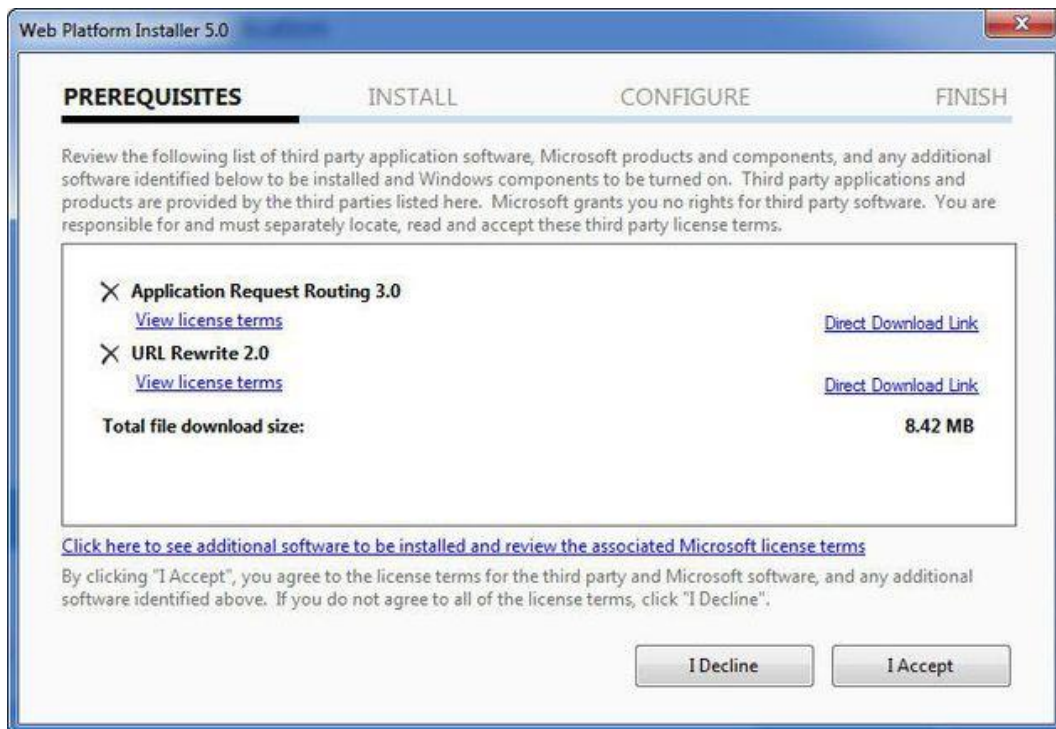
Click **I Accept**. The **Microsoft Web Platform Installer Confirmation** is displayed.
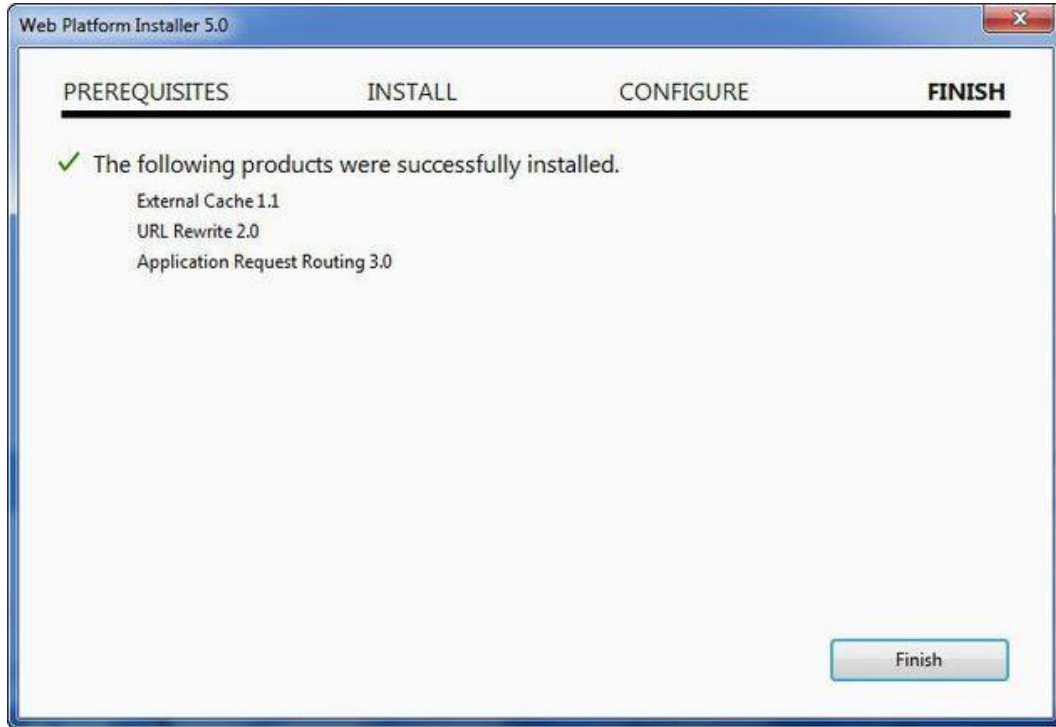
Click **Finish** to finalize.

Open the **Internet Information Services (IIS) Manager** on the Portal Server (**IIS Manager > Sites > Default Web Site > IIS > URL Rewrite**).
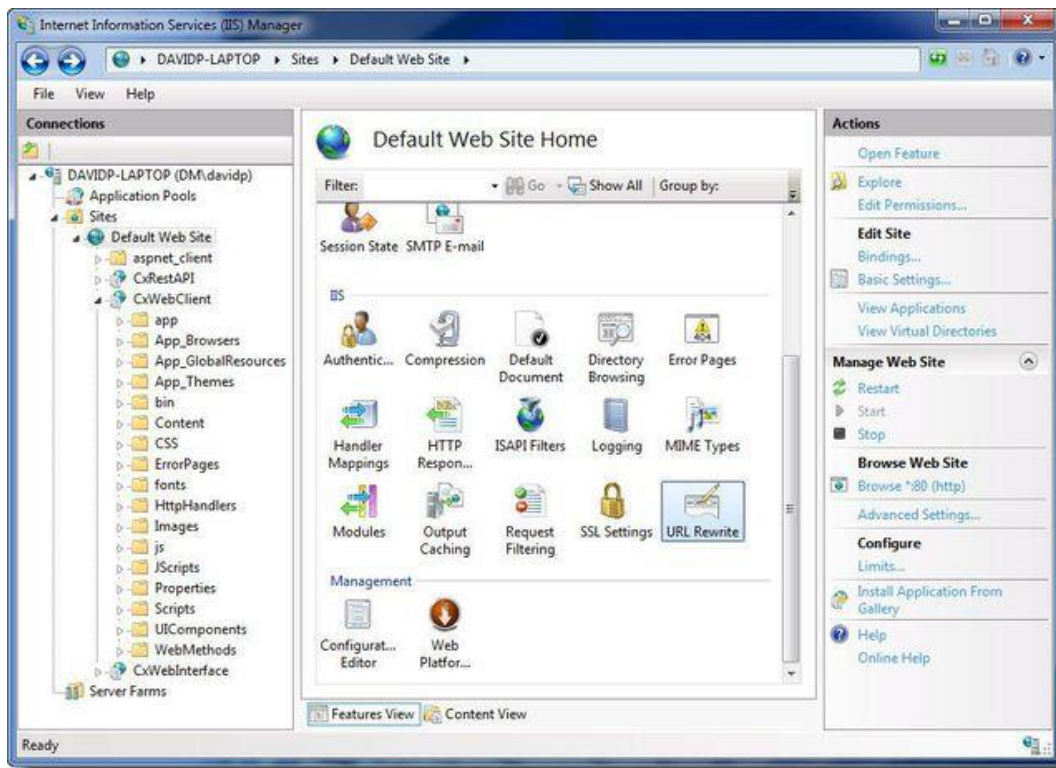
Select **Open Feature**. The **URL Rewrite Rule** is displayed.
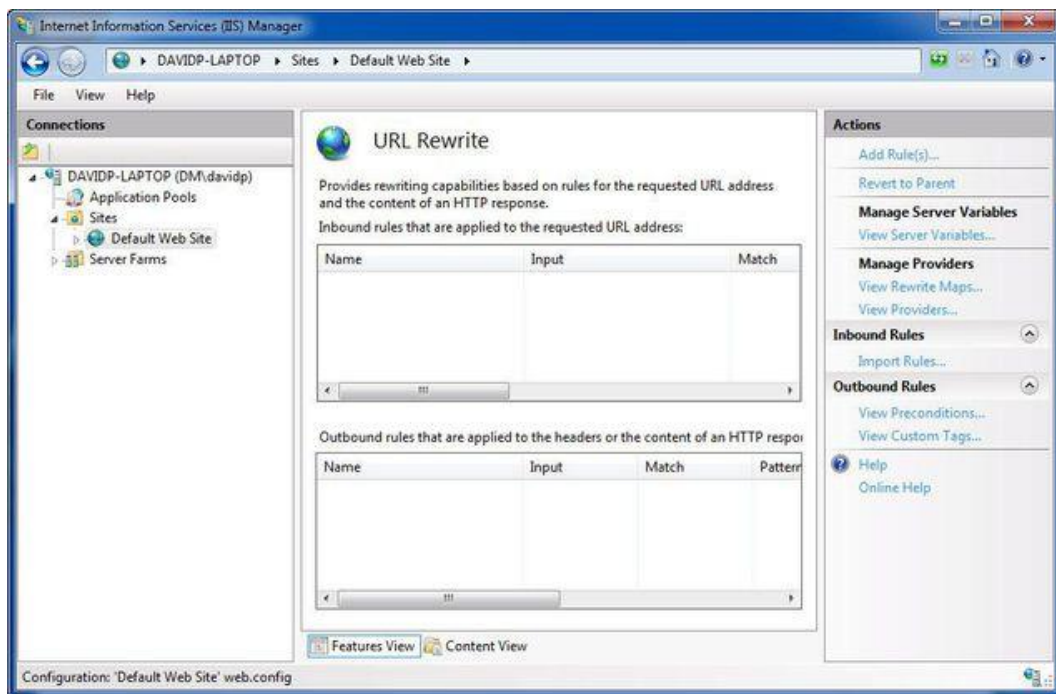
Select **Add Rule(s)**. The **Rule Templates List** is displayed.
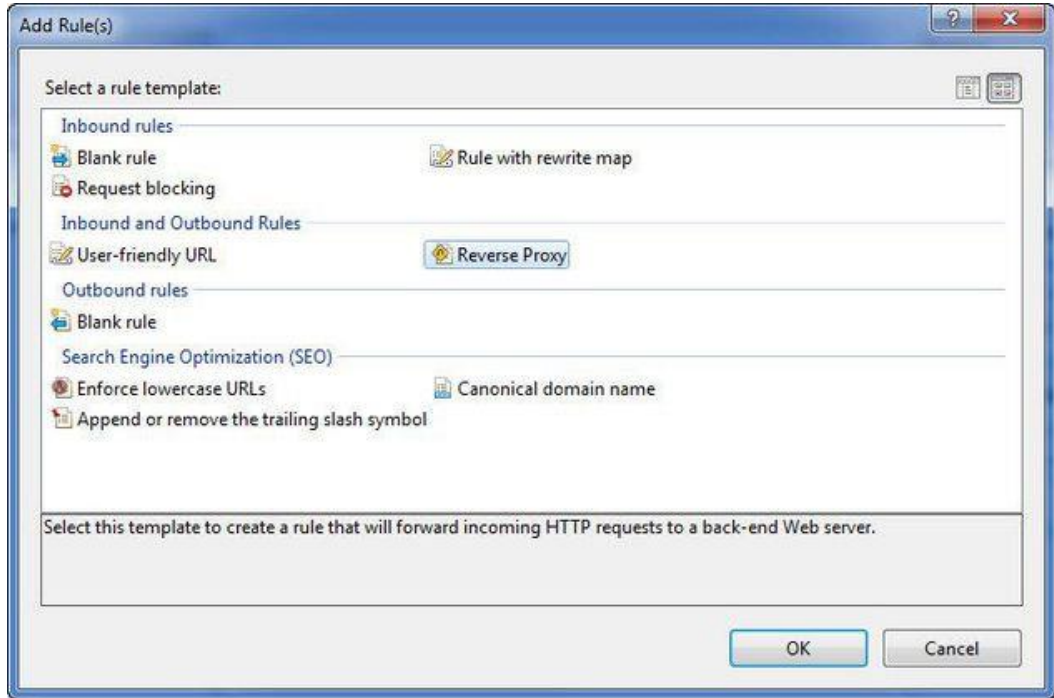
Select **Reverse Proxy**. The **Rule Template** is displayed.
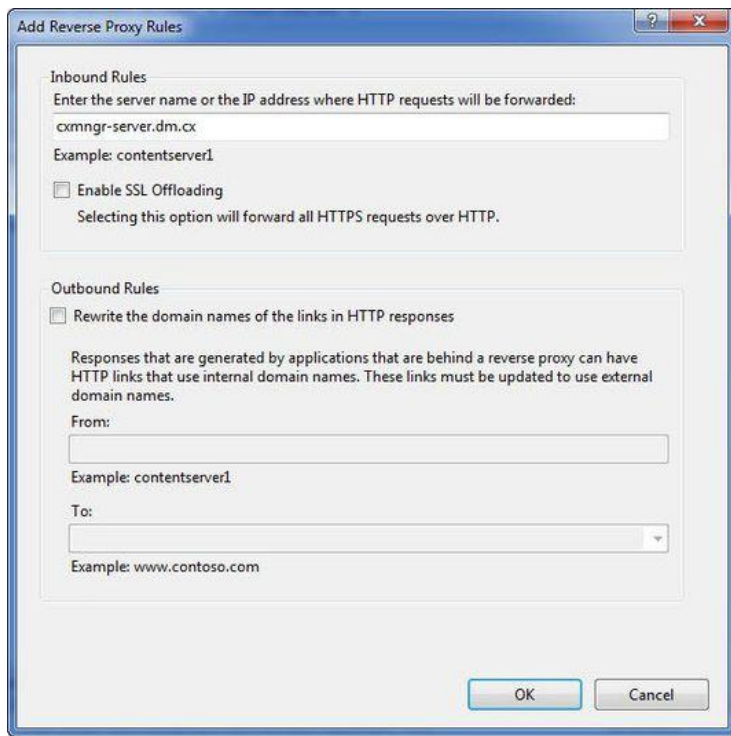
Enter the **CX Manager Server** name into the **Inbound Rules** field (e.g. cxmngr-server.dm.cx).

Disable the **SSL Offloading** option.

Click **OK** to save the changes.
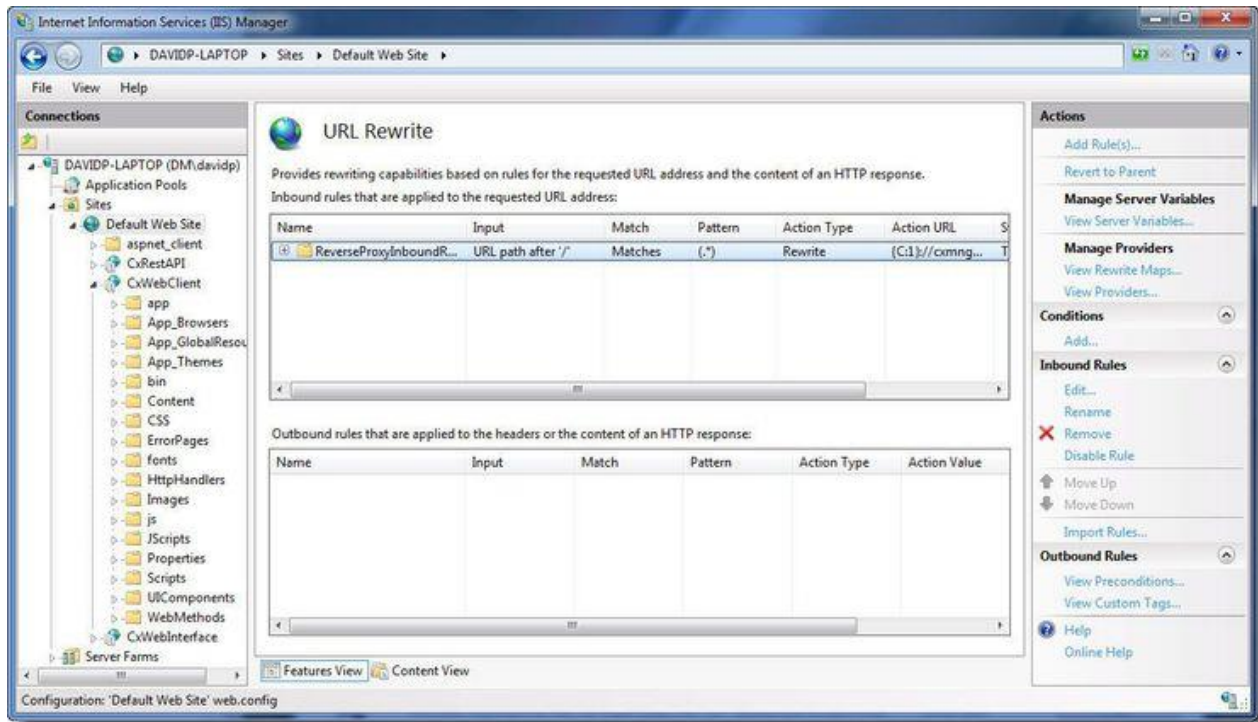
Select the newly created **Rule** and click **Edit**. The **Edit Inbound Rule** is displayed.
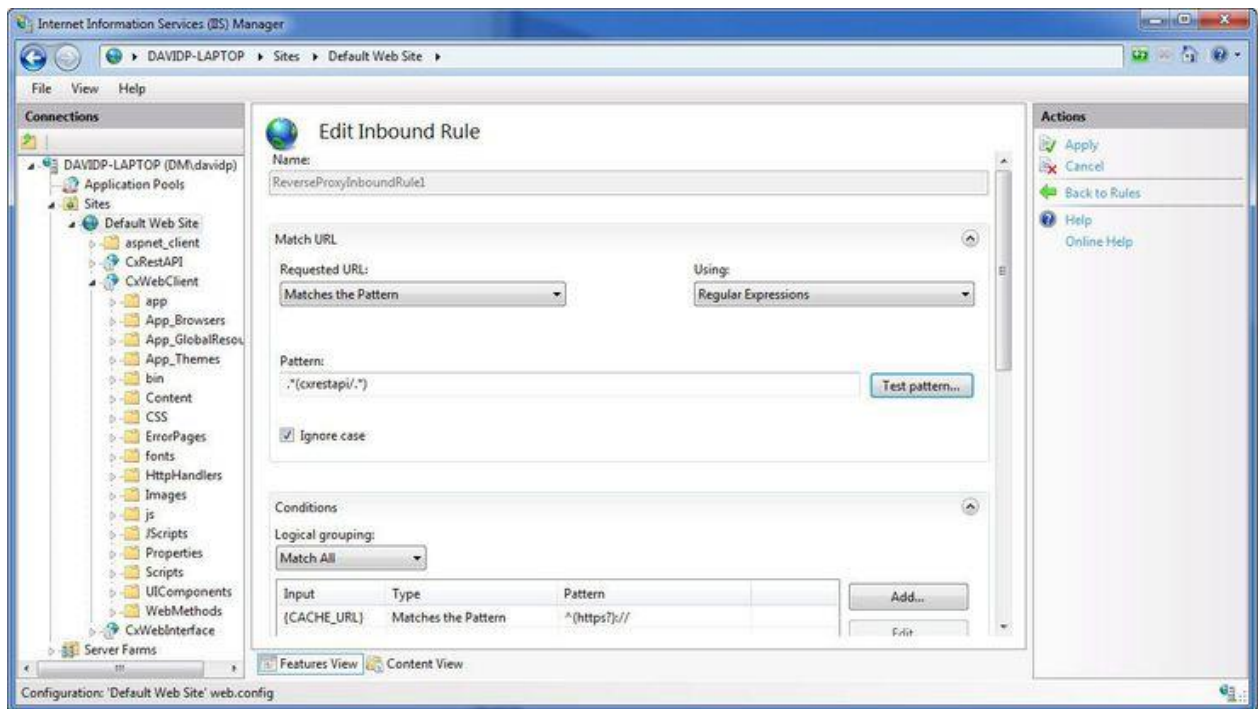
Change the **Pattern** to .*(cxrestapi/.*) and click **Apply**.

Verify the changes in the URL Rewrite rule.
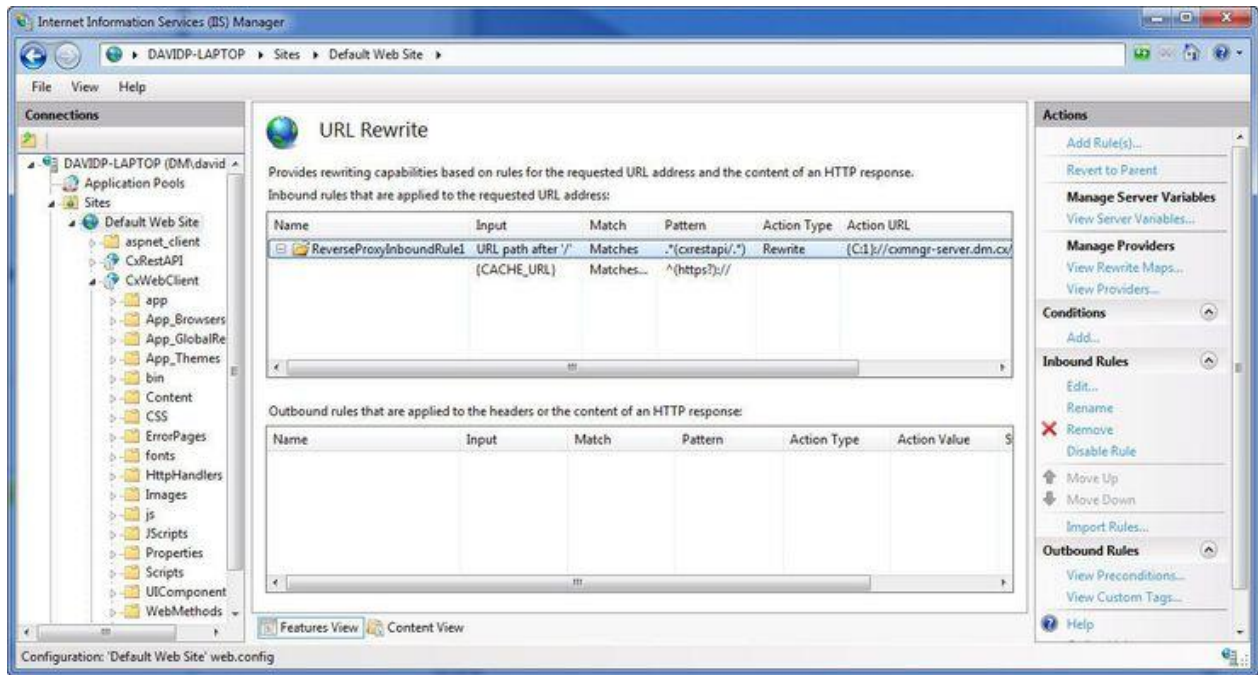
Test the **CxSAST** application.

Installing CxSAST

Before installing CxSAST, make sure that you understand the System Architecture, that your server host(s) complies with the Server Host Requirements, and that you have properly prepared the Environment.

ⓘ If some or all CxSAST server components are to be installed on different hosts, please perform the following procedure.

Installation Permissions

The user performing the installation must have administrative network permissions (user name and password) for the computer/server running CxSAST Services.

ⓘ For SQL Server database:

If the database uses Windows domain authentication, the user account performing the installation (Centralized or CxManager) must have SA permission on the database server for the duration of the installation process. If SA permission is unavailable, certain prerequisites must be fulfilled prior to the installation:

- Build two SQL databases using the names; CxDB and CxActivity
- Create login for Windows User and associate it with DB_owner permission for CxDB and CxActivity. This user should be a dedicated Service user and the same user must perform the installation, see Link for additional information.

If the database uses SQL Server native authentication, prepare an SQL Server user account. This account must have SA permissions for the duration of the installation process. If SA permission are unavailable, certain prerequisites must be fulfilled prior to the installation.

- Build two SQL databases using the names CxDB and CxActivity
- Create login for SQL User and associated it with the DB_owner permission for CxDB and CxActivity. Define this user in the CxSAST installation.

For upgrades, all previously defined SQL connection parameters are loaded from the existing configuration. If Windows authentication is being used, run the installer with the same user that is defined for the CxServices or any other Windows authenticated user with DB owner permission on CxDB and CxActivity.

Setting Up CxSAST

License Validation

If you have not yet obtained a permanent Checkmarx license, send your hardware ID (**Start** > **All Programs** > **Checkmarx** > **HardwareId**) to your Checkmarx sales representative or Checkmarx support to obtain a Production license file.

Installation Package

1. Download the CxSAST installation package.
2. On each server component host:
    1. Extract the downloaded ZIP archive, supplying the password provided by Checkmarx support.
    2. Run **CxSetup.exe** and begin the installation.

Installing CxSAST

Prerequisites and Recommendations

- The installer requires .Net 4.5.1 Framework installed on your server (If missing, it will be installed by CxSAST Installer).
- The required Web Server for Checkmarx suite is IIS server (if missing, it will be installed by the CxSAST Installer on the condition that the Windows installation media is accessible).
- SQL 2012 Express is included inside the CxSAST installer and is installed (if defined) in the event that no other version of SQL is already installed.

Installation

Once you have downloaded the CxSAST Installation package, run the **CxSetup.exe.** The Checkmarx Welcome window is displayed.
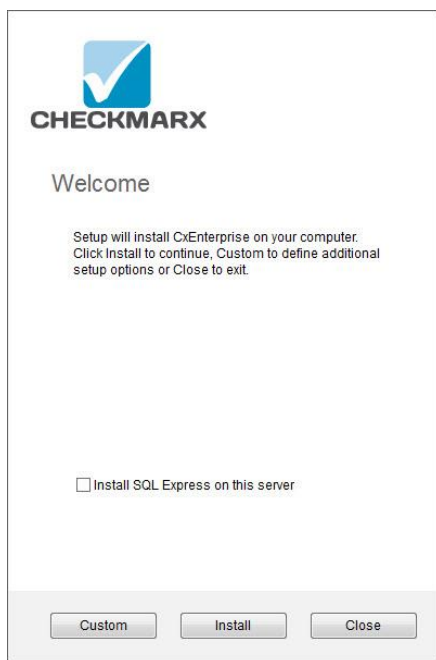
If SQL Server is not already installed and you want to install SQL Express, select the **Install SQL Express on this server** check-box.

> ⓘ For upgrades, previously installed SQL parameters are loaded from the existing configuration and the Install SQL Express option is not displayed.

Click **Install** to continue, **Custom** to define additional setup options, or **Close** to exit.

If you selected **Custom**, the Additional Setup Options window is displayed.

Define the Checkmarx setup installation location and select whether to install related shortcuts on your desktop.

> ⓘ For upgrades, previously installed location and product features are loaded from the existing configuration and cannot be changed. You can however install product features that haven't already been installed.
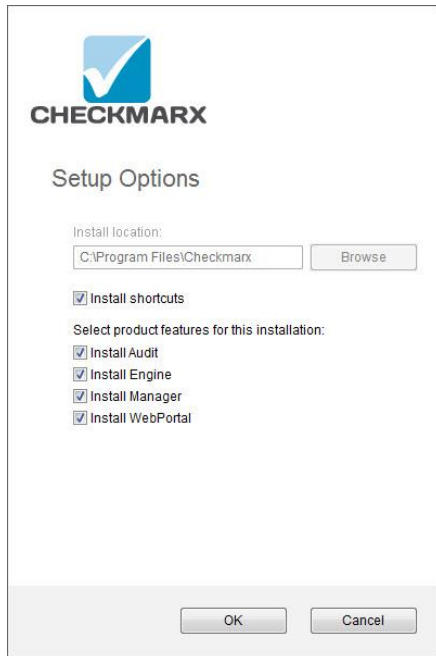
Select the required product features for this installation from the available list.

> ⓘ Tip for installation type selection:
>
> - **POC/Evaluation** - Select **Audit**, **Engine**, **Manager** and **WebPortal**
> - **Distributed Architecture** - Select either **Engine** or **Manager** and/or **WebPortal**
> - **Centralized Architecture** - Select **Engine**, **Manager** and **WebPortal** (select **Audit**, if you plan to customize queries on the host)
> - **CxEngine Server only** - Select **Engine** (see **Adding a CxEngine Server**).

Once you have made your selection, click **OK**. The Checkmarx Welcome window is displayed.
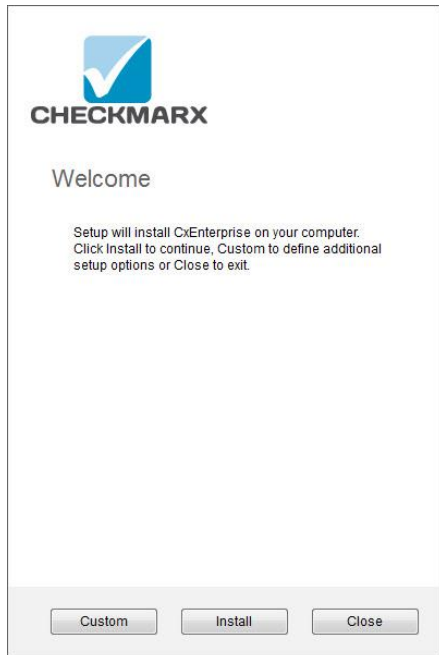
Click **Install** to continue, or **Close** to exit.

If you selected **Install**, the setup procedure starts. The Set SQL Server Configuration window is displayed.

> ⓘ If you selected "Install SQL Express on this server" option in the initial Checkmarx Welcome window, the Set SQL Server Configuration window will not be displayed.
>
> For upgrades the SQL Server parameters are loaded from the existing configuration and cannot be changed.

In the Set SQL Server Configuration window, define a connection to the installed SQL Server or to any other SQL server on your network, by selecting either:

- **Connect using integrated Windows authentication** (login not required)
- **Connect using SQL Server authentication** (provide SQL User Name and SQL Password for login with SA permissions).

Click **Test Connection**. A "Connection OK" message is displayed upon confirmed connection to the SQL Server.

> ⓘ In order to continue with the installation confirmed connection to the SQL Server is required.
>
> If connection to the SQL Server fails a "Connection failure" message with the required action is displayed.

Click **Next**. The setup procedure continues.
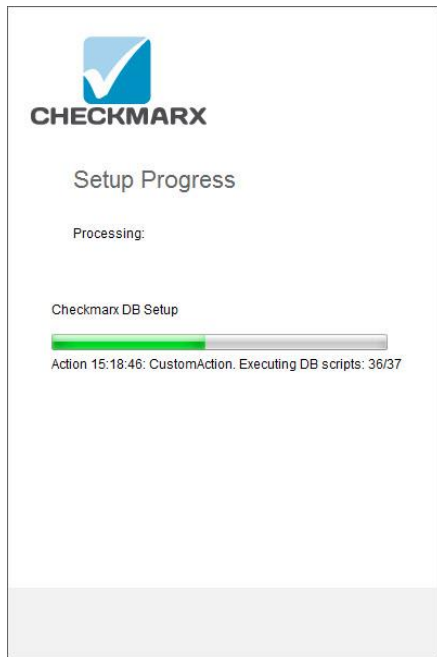
Once complete, the License Activation window is displayed.
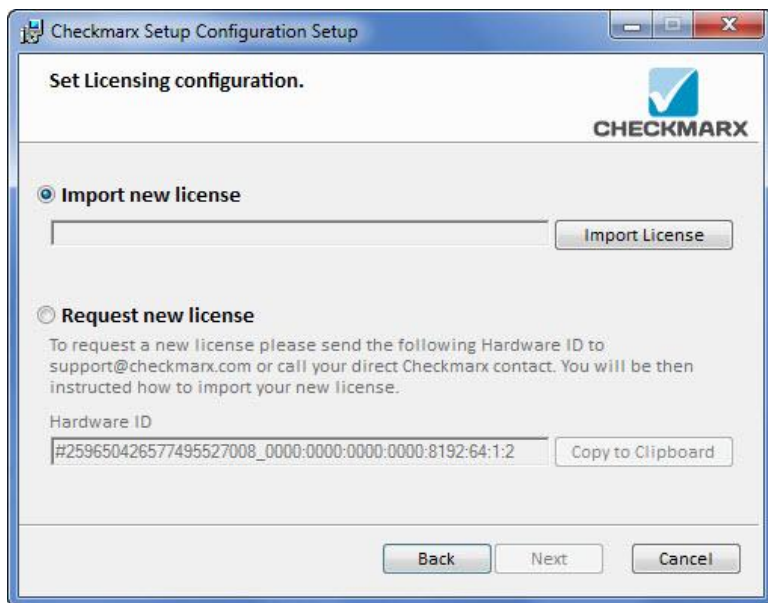
> ⓘ   For upgrades, the license information (if exists and is valid) is automatically loaded from the existing configuration and the License Activation window is not displayed.

Select a **License Activation** option.

ⓘ Tip for license type selection:

- **Import new license:** Select and click **Import License** if you already have a valid license file.
- **Request new license:** Select if you have not yet obtained a permanent Checkmarx license. Click **Copy to Clipboard** and send the Hardware ID to your Checkmarx sales representative or contact Checkmarx support

Click **Next**.

ⓘ If your license doesn't match your current hardware ID (HID) a warning message is displayed. Please import a different license or request a new one from your Checkmarx sales representative or contact Checkmarx support.

The Validate Port window is displayed if:

- The default website exists, the selected port is not part of the default website's port bindings list and the port is occupied by another application or website
- The default website does not exist and the selected port is occupied by another application or website.

Select another available port and click **Validate Port**.

ⓘ Port 80 is the default port for Checkmarx applications.

Once the port has been validated, click **Next**. The setup procedure continues.

Once the setup procedure is complete, click **Next**.
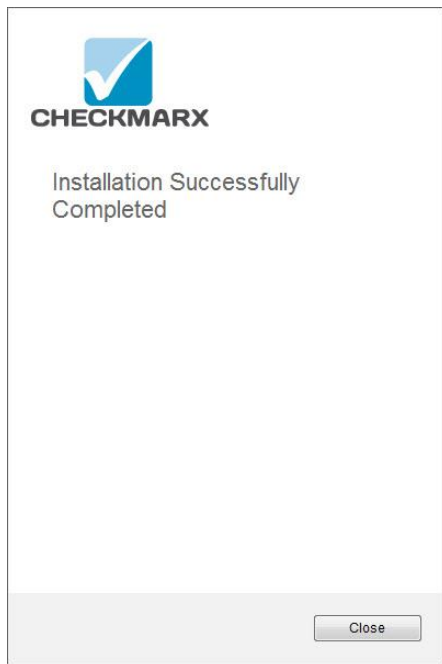
Once the Setup Successful Completed window is displayed, click **Close** to complete the installation.

> ⓘ If the installation fails, the "Setup failed" message is displayed. For more information, see the installation logs. If you need further assistance, please contact Checkmarx support.

Installed Services Check

Go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**
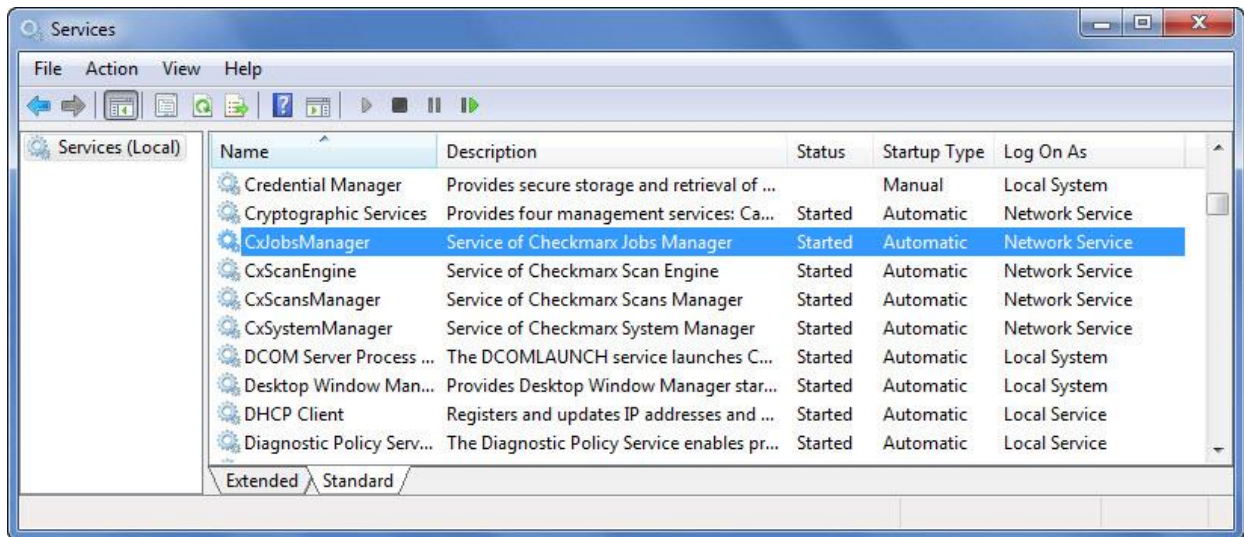

> ⓘ The database (DB) is required to be up and running in order for Checkmarx services to be able to run.

Make sure the following installed services are started:
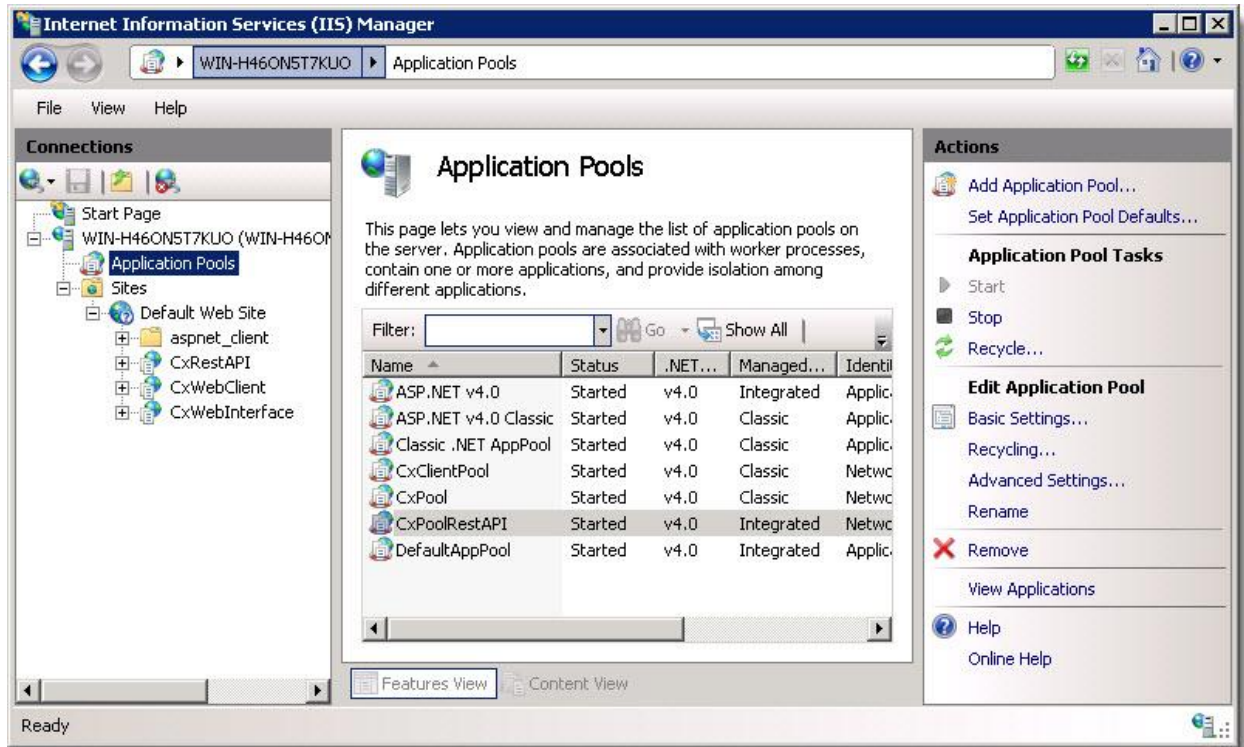
On a centralized host:

- CxJobsManager
- CxScansManager
- CxSystemManager
- CxScanEngine
- Web Server - IIS Admin Service & World Wide Web Publishing Service

On a CxEngine host:

- CxScanEngine

Installed Application Pool Check

Go to **Start** > **Control Panel** > **All Control Panel Items** > **Administrative Tools** > **Internet Information Services (IIS) Manager**

Make sure the following installed application pools are started:

On a centralized host:

- CxClientPool
- CxPool

> ⓘ If the IIS Pools are not started automatically after installation, you should restart the machine.

Login to the Web Interface

Access the CxSAST web interface in either of the following ways:

- To access CxSAST locally (from the server host), use the **Checkmarx Portal** shortcut on the Desktop or navigate to the Checkmarx folder (**Start** > **All Programs** > **Checkmarx** > **Checkmarx Portal**).
- To access CxSAST from any other computer, make sure that organizational routing and firewall configuration allow the client computer to access the CxSAST server. Point your browser to: http://<server>/cxwebclient/login.aspx where <server> is the IP address or resolvable hostname of the CxSAST server.

Upon a fresh installation, a single Administrator Account needs to be created.

Once the Set Administrator Credentials window is displayed, add the following credentials:

- **Administrator User Name**
- **Password**
- **Confirm Password**

> ⓘ The required password complexity is as follows:
>
> - 9 to 400 characters
> - At least 1 uppercase letter
> - At least 1 lower case letter
> - At least 1 special character
> - At least 1 digit

Click **Confirm** to complete.

You can subsequently change the Administrator password and add CxSAST users.

In a distributed architecture:

In the web interface, go to **Management** > **Application Settings** > **Installation Information**, and click **Add Engine Server**.

Give the CxEngine server a **Name**, provide its URL, so that CxManager will be able to communicate with CxEngine and optionally define LOC limits.

The URL should be:
http://<Server_Name>**/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc**
where < Server_Name> is the CxEngine host's IP address or resolvable name.
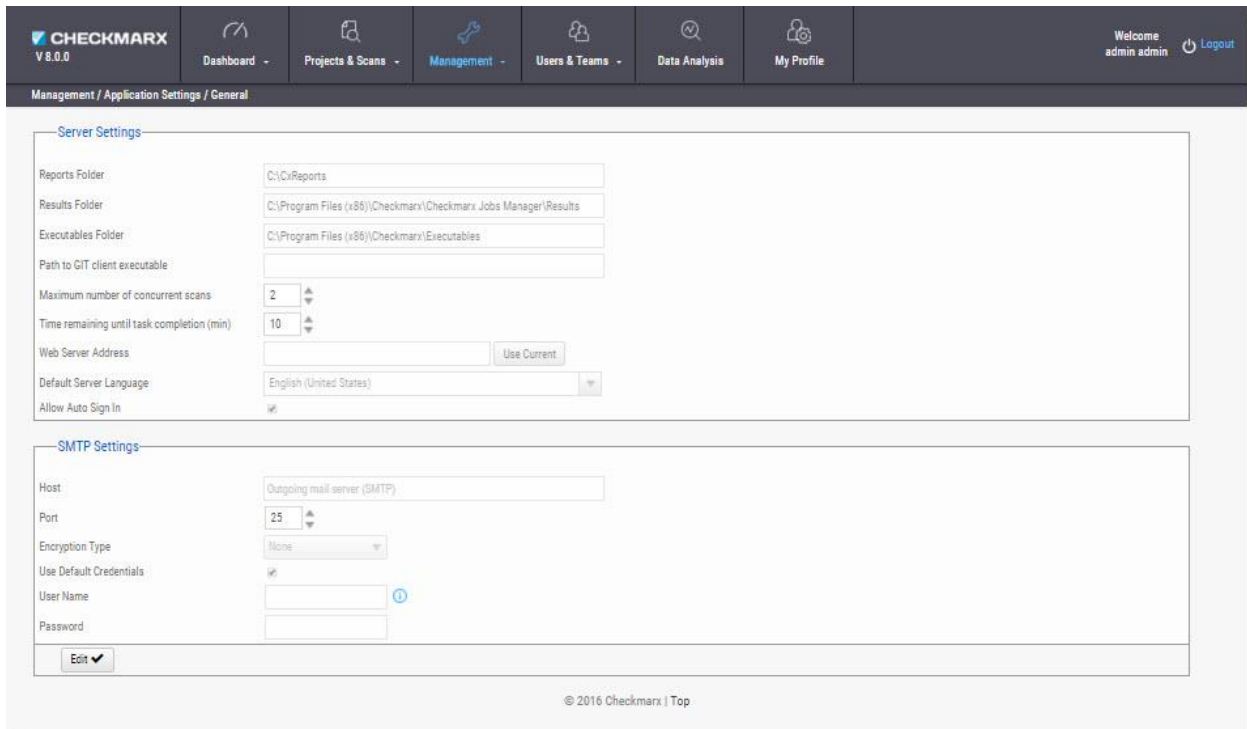

ⓘ It is recommended to check the defined URL by opening it in a browser on the CxManager
   server to validate.

Click **Create**.

Multiple CxEngine Servers:

If you have multiple CxEngine Servers, repeat the above step for each one.

In the web interface, go to **Management** > **Application Settings** > **General**.

Click **Edit.**

If permitted by your Checkmarx license, set the "Maximum number of concurrent scans" to the
desired number for all the CxEngine Servers.

Provide **SMTP** settings and click **Update**. Other settings should usually be left as they are.
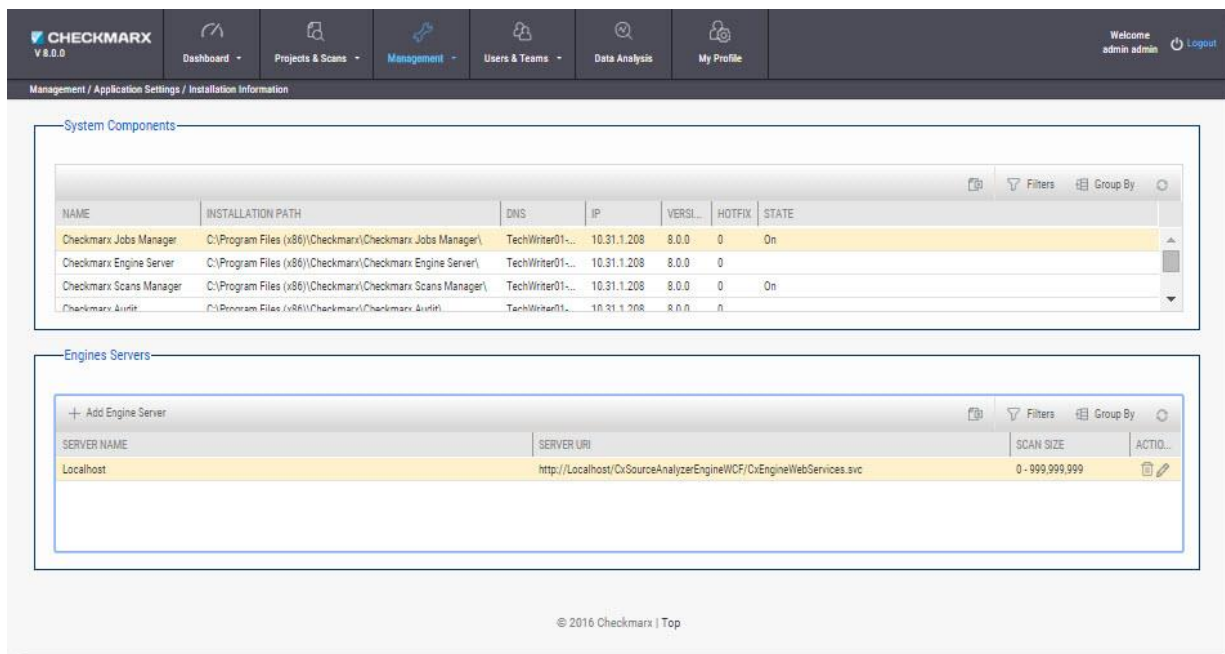
Optionally, you can configure the "From" field of emails. If you don't configure it, it will be left
empty."

Email Verification

Verify that the email address in the CxSAST profile settings (My Profile > Account Information) is of a valid format, i.e. John.Smith@example.com, and not John.Smith@example.

Installation Verification

Validate that you have successfully installed the correct version and/or hot-fix by clicking **Management** > **Application Settings** > **Installation Information** and reviewing all Checkmarx system components ensuring that they are all of the same version.

Upgrading CxSAST

> ⓘ This page applies only to full upgrades (it does not apply to hotfixes).
>
> CxSAST only supports upgrades for two earlier versions. If your current version is older, please contact support prior to the upgrade process.

In a distributed deployment, you must upgrade all components. Perform the following on the CxManager and on each CxEngine as relevant.

To upgrade CxSAST:

1. In the IIS Manager, navigate to **Application Pools**, and check if the user **Identity** of either of the following is anything other than the default **NetworkService**, in which case make sure you know the user account's full credentials.

   - **CxClientPool**
   - **CxPool**

2. In the Service Manager (services.msc), check the **Log On As** user accounts of each of the following. If any of them is anything other than the default **Network Service**, make sure you know the user account's full credentials.

   - CxJobsManager
   - CxScanEngine
   - CxScansManager
   - CxSystemManager

3. Make sure that no scans are currently running.

4. Stop all Cx Windows services and the Web server:

   - CxSystemManager
   - CxJobsManager
   - CxScansManager
   - CxScanEngine
   - Web server (run "iisreset /stop" from CMD):
     - World Wide Web Publishing Service
     - IIS Admin Service

5. As a precaution you should backup both Cx databases (using standard SQL Server tools - Make sure to give the files unique names and to include **.bak)**.

6. Install CxSAST.

7. If in steps 1-2 you found any non-default user accounts, reconfigure them as follows:

   - For application pool accounts, in the IIS Manager, navigate to **Application Pools**, and for each of **CxPool** and **CxClientPool**:

     a. Select the pool.
     b. Go to **Actions** > **Advanced Settings** > **Process Model** > **Identity**.
     c. Change the Identity value to the correct one.

   - For service accounts, in the Service Manager, for each of the services listed in step 2:

     a. Right-click the service and select **Properties**.
     b. In the **Log On** tab, configure the correct account.
     c. Click **OK**.

8. During upgrade the Checkmarx installer automatically performs a backup copy of the following files:

   - Checkmarx Audit\CxAudit.exe.config

   - Checkmarx Audit\Config.xml

   - Checkmarx Audit\ExtensionsConfig.xml

   - Checkmarx Audit\Log4Net.config

   - Checkmarx Engine Server\CxEngineAgent.exe.config

   - Checkmarx Engine Server\CxSourceAnalyzerEngine.WinService.exe.config

   - Checkmarx Engine Server\ExtensionsConfig.xml

   - Checkmarx Engine Server\CxEngineLog4Net.config

   - Checkmarx Engine Server\Logs4Net.config

   - Checkmarx Jobs Manager\bin\CxJobsManagerWinService.exe.config

   - Checkmarx Jobs Manager\bin\CxJobsManagerLog4Net.Build.config

   - Checkmarx Jobs Manager\bin\CxJobsManagerLog4Net.config

   - Checkmarx Scans Manager\bin\CxScansManagerWinService.exe.config

   - Checkmarx Scans Manager\bin\CxScansManagerLog4Net.config

   - Checkmarx System Manager\bin\CxSystemManagerService.exe.config

   - Checkmarx System Manager\bin\CxSystemManagerLog4Net.config

   - Checkmarx Web Services\CxWebInterface\Web.config

   - Checkmarx Web Services\CxWebInterface\Log4Net.config

   - Checkmarx WebPortal\Web\Web.config

   - Checkmarx WebPortal\Web\Log4Net.config

   - Configuration\ExtensionsConfig.xml

To locate the Checkmarx backup files go to **Start** > **Search** > and type "**%appdata%**" (C:\Users\<user>\AppData\Roaming\Checkmarx).

ⓘ The database (DB) is required to be up and running in order for Checkmarx services to be able to run.

Restart all Cx Windows services and the Web server:

- **CxSystemManager**

- **CxJobsManager**

- **CxScansManager**

- **CxScanEngine**

- **Web server** (run "iisreset" from CMD)**:**

  o World Wide Web Publishing Service

  o IIS Admin Service

Adding a CxEngine Server

If you see that your scan load requires an additional Engine server, you can add one as follows:

Prepare the new CxEngine host.

Perform a server installation. Under Product Feature selection, select only **Install Engine**.
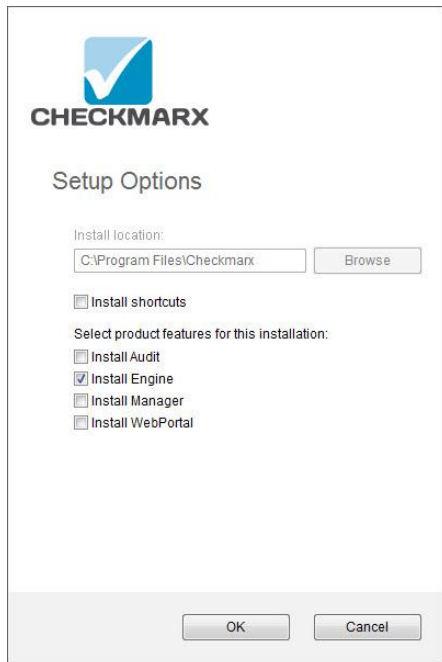
Log into the CxSAST web interface, go to **Management** > **Application Settings** > **Installation Information**, and click **Add Engine Server**. The Add Engine Server window is displayed.

Give the Engine server a **Name**, and provide its URL, so that CxManager will be able to communicate with CxEngine. The URL should be:

http://<server>**/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc**
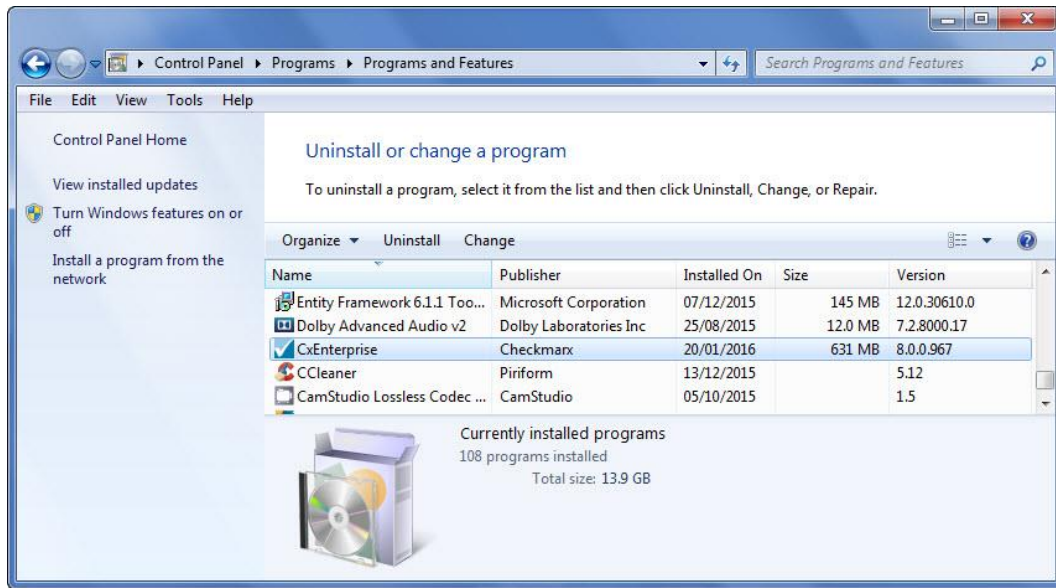where <server> is the CxEngine host's IP address or resolvable name.
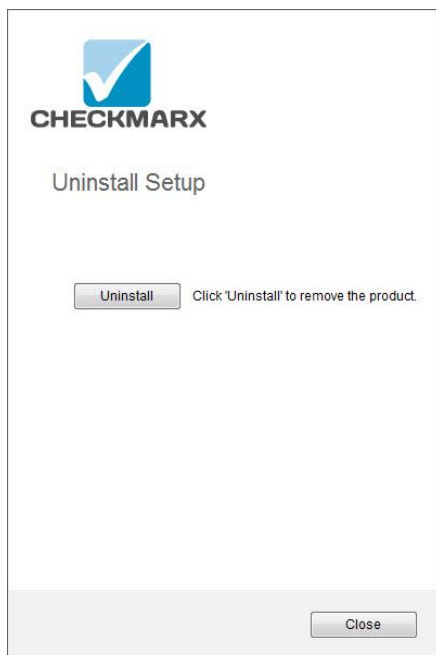
Click **Create**

Uninstalling CxSAST

To uninstall CxSAST from a server host:

Copy your Checkmarx license file to a safe location.
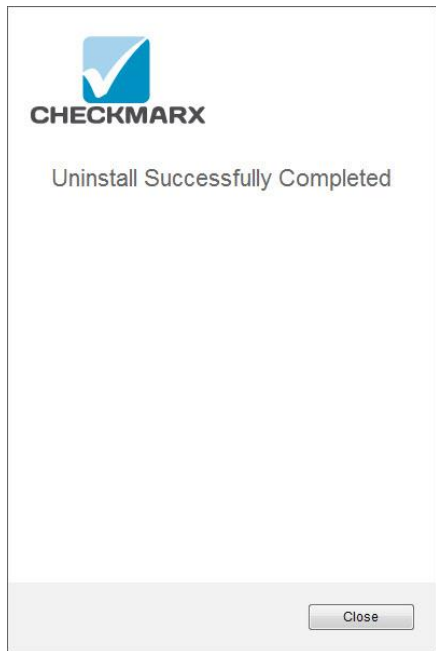
Go to **Start** > **Control Panel** > **Programs** > **Programs and Features.**

Double-click on **CxEnterprise**. The Uninstall Setup window is displayed.

Once complete the Uninstall Successfully Completed window is displayed.

Click **Close** to complete the uninstall.

> ⓘ Even though uninstall removes most Checkmarx folders, for consolidation purposes, the following folders are not deleted:
>
> - **CxSrc**
> - **CxDB (SQL)**

Updating the CxSAST License

To obtain a new or updated Checkmarx license for CxSAST:

Go to **Start** > **All Programs** > **Checkmarx**, click **HID**
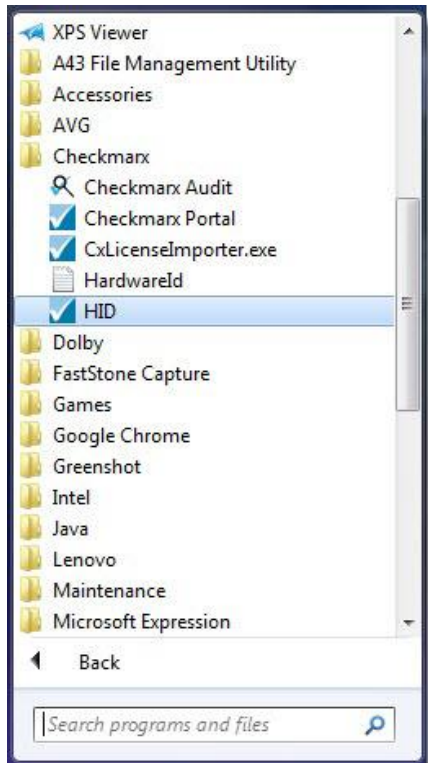
Once the Hardware ID is generated, copy the **HardwareId** and send it to your Checkmarx sales representative or Checkmarx support to obtain a new or updated license.

ⓘ **Distributed Installations**

Updating the license on each machine is required in case of distributed architecture installations.

Close all Checkmarx Application windows.

Go to **Start** > **All Programs** > **Checkmarx** and click **CxLicenseImporter.exe**, The Checkmarx License Importer is displayed.

Click **Import License,** navigate to your Checkmarx license file and click **Open**.

> ⓘ **HID Mismatch**
> If your license doesn't match your current hardware ID (HID) a warning message is displayed.
> Import a different license or request a new one from your Checkmarx sales representative or
> contact Checkmarx support.

The Import License Successful message might take a few seconds to appear.

> ⓘ The database (DB) is required to be up and running in order for Checkmarx services to be
> able to run.

Restart all Cx Windows services:

- **CxSystemManager**
- **CxJobsManager**
- **CxScansManager**
- **CxScanEngine**
- **Web server:**
  - o World Wide Web Publishing Service
  - o IIS Admin Service

CxSAST Application Maintenance Guide

- Introduction
- Backup
    - Step 1. Stop the CxServices
    - Step 2. Stop the Web Server
    - Step 3. Back up the Checkmarx Folder
    - Step 4. Backup the Database
    - Step 5. Backup the Scanned Source Folder
    - Step 6. Restart the CxServices
    - Step 7. Restart the Web Server
- Recovery
    - Step 1. Stop the CxServices
    - Step 2. Stop the Web Server
    - Step 4. Restore the Scanned Source Folder
    - Step 5. Restore the Database
    - Step 6. Restart the CxServices
    - Step 7. Restart the Web Server
- Maintenance and Cleanup
    - CxManager
        - Sources
            - CxSrc
            - ExtSrc
        - Logs
        - Reports
    - CxEngine
        - Sources
            - CxSrc
        - Logs
        - Scans
    - CxWebPortal
        - Logs
    - CxAudit
        - Sources
            - CxAuditSrc
        - Logs
    - Database
- Appendix A: Compressing a Folder in Windows
    - Trade-Offs
    - When to Use and When Not to Use NTFS Compression
    - How to Use NTFS Compression

Introduction

Checkmarx CxSAST collects sources, logs and sensitive information and stores it in files and the database. This document describes the backup and recovery, maintenance and cleanup procedures for CxSAST.

CxSAST is comprised of the following main components:

System Manager	Manages the system services: cleanup, monitoring, etc.
Jobs Manager	Runs all long management tasks: creates reports, prepares sources, etc.
Scans Manager	Manages all scans
Engine Server	Performs the scans
Web Services	Connects the web clients with the 3rd party systems
Web Portal	Web interface with CxSAST
Audit	Client for creating and customizing queries
Database	Stores scan results and system settings

Backup

CxSAST is composed of files and the database, both should be backed up.

Step 1. Stop the CxServices

Stop the CxJobsManager, CxScansManager, CxSystemManager and CxScanEngine services by opening **Services**, selecting the **CxService** and clicking **Stop** for each one (this depends on your Checkmarx distributed installation).

Step 2. Stop the Web Server

Stop the IIS Web server by opening the **IIS Manager**, selecting the <**server name**> and clicking **Stop** on the **Actions** menu.

Step 3. Back up the Checkmarx Folder

Create a new Checkmarx backup folder (recommended to include backup date).
Example: C:\Program Files\Checkmarx - > C:\Program Files\Checkmarx15052016

Copy the following items from the Checkmarx folder:

- **Configuration**, **Executable** and **Licenses** folders and the following configuration files:
- Checkmarx Audit\CxAudit.exe.config

- Checkmarx Audit\Config.xml
- Checkmarx Audit\ExtensionsConfig.xml
- Checkmarx Audit\Log4Net.config
- Checkmarx Engine Server\CxEngineAgent.exe.config
- Checkmarx Engine Server\CxSourceAnalyzerEngine.WinService.exe.config
- Checkmarx Engine Server\ExtensionsConfig.xml
- Checkmarx Engine Server\CxEngineLog4Net.config
- Checkmarx Engine Server\Logs4Net.config
- Checkmarx Jobs Manager\bin\CxJobsManagerWinService.exe.config
- Checkmarx Jobs Manager\bin\CxJobsManagerLog4Net.Build.config
- Checkmarx Jobs Manager\bin\CxJobsManagerLog4Net.config
- Checkmarx Scans Manager\bin\CxScansManagerWinService.exe.config
- Checkmarx Scans Manager\bin\CxScansManagerLog4Net.config
- Checkmarx System Manager\bin\CxSystemManagerService.exe.config
- Checkmarx System Manager\bin\CxSystemManagerLog4Net.config
- Checkmarx Web Services\CxWebInterface\Web.config
- Checkmarx Web Services\CxWebInterface\Log4Net.config
- Checkmarx WebPortal\Web\Web.config
- Checkmarx WebPortal\Web\Log4Net.config
- Configuration\ExtensionsConfig.xml

Step 4. Backup the Database

Backup the database using the standard database tools.

Step 5. Backup the Scanned Source Folder

Copy the CxSrc folder and rename it as the backup (recommended to include backup date).
Example: C:\CxSrc - > C:\CxSrc15052016

Step 6. Restart the CxServices

Restart the CxJobsManager, CxScansManager, CxSystemManager and CxScanEngine services by opening **Services**, selecting the **CxService** and clicking **Restart** for each one (this depends on your Checkmarx distributed installation).

Step 7. Restart the Web Server

Restart the IIS Web server by opening the IIS manager, selecting the <server name> and clicking Start on the Actions menu.

Recovery

The recovery steps below take into consideration the following; a new installation of CxSAST on your server using the same installation path and CxSAST version that was previously installed when the backup was performed.

Step 1. Stop the CxServices

Stop the CxJobsManager, CxScansManager, CxSystemManager and CxScanEngine services by opening **Services**, selecting the **CxService** and clicking **Stop** for each one (this depends on your Checkmarx distributed installation).

Step 2. Stop the Web Server

Stop the IIS Web server by opening the **IIS Manager**, selecting the <**server name**> and clicking **Stop** on the **Actions** menu.

Step 3. Restore Checkmarx`s Backed up Folders and configuration files

Restore the Checkmarx folders and configuration files that were previously backed up by copying the files from the backup folder to your newly created folder overwriting the original files:
Example: C:\Program Files\ Checkmarx15052016 - > C:\Program Files\Checkmarx

Step 4. Restore the Scanned Source Folder

Copy the CxSrc folder from the backup overwriting the new empty folder:

Example: C:\CxSrc15052016 - > C:\CxSrc

Step 5. Restore the Database

Restore the database that was previously backed up overwriting the db's that were created by the new installation.

Step 6. Restart the CxServices

Restart the CxJobsManager, CxScansManager, CxSystemManager and CxScanEngine services by opening **Services**, selecting the **CxService** and clicking **Restart** for each one (this depends on your Checkmarx distributed installation).

Step 7. Restart the Web Server

Restart the IIS Web server by opening the **IIS Manager**, selecting the <**server name**> and clicking **Start** on the **Actions** menu.

Step 8. Check the Recovered Version

Perform a basic test on the new version to check that everything is up and running:

- Login
- View older scan results
- Run a new small scan
- View the new scan results

Maintenance and Cleanup

Maintenance and cleanup of Checkmarx CxSAST refers to the following types of data:

Sources	Source files that are scanned are stored in several locations during the scan
Logs	Old logs that can simply be deleted, moved or compressed as needed
Reports	All reports are saved on the disk. If deleted, a new report can be created on request

CxManager

Includes the System Manager, Jobs Manager, Scans Manager and Web Services.

Sources

CxSrc

Default location: C:\CxSrc

This is the main sources location - after the scan is complete CxSAST leaves one copy of the sources to be used by the project viewer and for creating code samples in reports.

The recommended method to clean the CxSrc folder is to use CxSAST's built-in data retention feature. This allows retention of scanned files in the CxSrc folder (and the DB).

It is also possible to delete old sources from the Checkmarx folder, if required. Deleting the sources will not affect the statistical information saved in the database. Opening the project viewer that does not have sources anymore will only result in an empty code area.

It is also possible to use the Microsoft compressed folder option to save disk space (see Appendix A: Compressing a Folder in Windows) Compressing a folder for a project will save about 90% of the space and only affect performance when accessing the project's viewer.

ExtSrc

Default location: C:\ExtSrc

This is used as a temporary folder to extract the content of Zip files. Any files that remain in this location can be deleted with no implications.

Logs

Default location: C:\Program Files\Checkmarx\Logs

All logs are saved on the disk. Old logs can simply be deleted or compressed as needed

Reports

Default location: C:\CxReports

All reports are saved on the disk. If deleted, a new report can be created on request.

As all created logs are created to this folder but sent to requesting client – the reports that are saved in this folder can be deleted with no implications.

CxEngine

Sources

CxSrc

Default location: C:\CxSrc

Only if the CxEngine is installed on a separate server this folder should be cleaned separately from the CxManager. If it is separate, and only after scans are completed and there are any files that remain in this location, they can be deleted with no implications.

Logs

Default location: C:\Program Files\Checkmarx\Checkmarx Engine Server\Logs
C:\Program Files\Checkmarx\Checkmarx Engine Server\Logs\Trace

All logs are saved on the disk. Old logs can simply be deleted, moved or compressed as needed.

Scans

Default location: C:\Program Files\Checkmarx\Checkmarx Engine Server\Scans
C:\Program Files\Checkmarx\Checkmarx Engine Server\Logs\ScanLogs

All scans are saved on the disk. While the engine is not running, old scans can simply be deleted, moved or compressed as needed.

CxWebPortal

Logs

Default location: C:\Program Files\Checkmarx\Logs\WebClient
C:\Program Files\Checkmarx\Logs\WebClient\Trace

All logs are saved on the disk. Old logs can simply be deleted, moved or compressed as needed.

CxAudit

Sources

CxAuditSrc

Default location: Cx8.4.2 and below: C:\CxAuditSrc
Cx8.5 and up:%AppData%\..\local\Checkmarx\CxAudit\CxAuditSrc

All sources are saved on the disk. Old sources can simply be deleted, moved or compressed as needed.

Logs

Default location: C:\Program Files\Checkmarx\Checkmarx Audit\Logs

All logs are saved on the disk. Old logs can simply be deleted, moved or compressed as needed.

Database

Checkmarx CxSAST uses two main databases (CxDB and CxActivity). In order to keep the log size small, both databases can be set to Recovery Model = Simple.

Appendix A: Compressing a Folder in Windows

The NTFS file system used by Windows has a built-in compression feature known as NTFS compression. With a few clicks, you can compress files, making them take up less space on your hard drive. Best of all, you can still access the files normally.

Using NTFS compression involves a trade-off between CPU time and disk activity. Compression will work better in certain types of situations and with certain types of files.

Trade-Offs

NTFS compression makes files smaller on your hard drive. You can access these files normally – no need for cumbersome zipping and unzipping. Like with all file compression systems, your computer must use additional CPU time for decompression when it opens the file.

However, this doesn't necessarily mean it will take any longer to open the file. Modern CPUs are very fast, but disk input/output speeds haven't improved nearly as much. Consider a 5 MB uncompressed document – when you load it, the computer must transfer 5 MB from the disk to your RAM. If that same file were compressed and took up 4 MB on the disk, the computer would transfer only 4 MB from the disk. The CPU would have to spend some time decompressing the file, but this will happen very quickly – it may even be faster to load the compressed file and decompress it because disk input/output is so slow.

On a computer with a slow hard disk and a fast CPU – such as a laptop with a high-end CPU but a slow, energy efficient physical hard disk, you may see faster file loading times for compressed files.

This is especially true as NTFS compression isn't very aggressive in its compression. A test by Tom's Hardware found that it compressed much less than a tool like 7-Zip, which reaches higher compression ratios by using more CPU time.

When to Use and When Not to Use NTFS Compression

NTFS compression is ideal for:

- Files you rarely access. (If you never access the files, the potential slow-down when accessing them is unnoticeable).
- Files in uncompressed format. (Office documents, text files, and PDFs may see a significant reduction in file size, while MP3s and videos are already stored in a compressed format and won't shrink much, if at all).
- Saving space on small solid state drives. (Warning: Using compression will result in more writes to your solid state drive, potentially decreasing its life span. However, you may gain some more usable space.)
- Computers with fast CPUs and slow hard disks.

NTFS compression should not be used for:

- Windows system files and other program files. Using NTFS compression here can reduce your computer's performance and potentially cause other errors.

- Servers where the CPU is getting heavy use. On a modern desktop or laptop, the CPU sits in an idle state most of the time, which allows it to decompress the files quickly. If you use NTFS compression on a server with a high CPU load, the server's CPU load will increase and it will take longer to access files.

- Files in compressed format. (You won't see much of an improvement by compressing your music or video collections).

- Computers with slow CPUs, such as laptops with low-voltage power-saving chips. However, if the laptop has a very slow hard disk, it's unclear whether compression would help or hurt performance.

How to Use NTFS Compression

Now that you understand which files you should compress, and why you shouldn't compress your entire hard drive or your Windows system folders, you can start compressing some files. Windows allows you to compress an individual file, a folder, or even an entire drive (although you shouldn't compress your system drive).

To get started, right-click the file, folder, or drive you want to compress and select Properties.

Click the Advanced button under Attributes.

Enable the Compress contents to save disk space check box and click OK twice.

If you enabled compression for a folder, Windows will ask you whether you also want to encrypt subfolders and files.

In this example, we saved some space by compressing a folder of text files from 356 KB to 255 KB, about a 40% reduction. Text files are uncompressed, so we saw a big improvement here.

Compare the Size on disk field to see how much space you saved.

Compressed files and folders are identified by their blue names in Windows Explorer.

To un-compress these files in the future, go back into their advanced attributes and uncheck the Compress checkbox.

CxSAST Database Maintenance Guide

Chapter 1 - Introduction

The purpose of the document to provide specific information about Checkmarx SAST (CxSAST) tables regarding their maintenance. It doesn't replace MS SQL Server guidelines and best practices published by official database providers. It refers to sole aspects (key area) of database maintenance: Index and Tables fragmentation.

There are basically two types of fragmentation:

- Fragmentation within individual data and index pages (sometimes called **internal fragmentation**)
- Fragmentation within index or table structures consisting of pages (called **logical scan fragmentation** and extent scan fragmentation)

More commonly, **internal fragmentation** results from data modifications, such as inserts, updates, and deletes, which can leave empty space on a page. Depending on the table/index schema and the application's characteristics, this empty space may never be reused once it is created and can lead to ever-increasing amounts of unusable space in the database. Wasted space on data/index pages can therefore lead to needing more pages to hold the same amount of data. Not only does this take up more disk space, it also means that a query needs to issue more I/Os to read the same amount of data. All these extra pages occupy additional space in the data cache, therefore taking up more server memory.

Logical scan (or external/extent) fragmentation is caused by an operation called a page split. This occurs when a record has to be inserted on a specific index page (according to the index key definition) but there is not enough space on the page to fit the data being inserted. The page is split in half and roughly 50% of the records moved to a newly allocated page. This new page is usually not physically contiguous with the old page and therefore is referred to as fragmented. Extent scan fragmentation is similar in concept. Fragmentation within the table/index structures affects the ability of the SQL Server to do efficient scans, whether over an entire table/index or bounded by a query WHERE clause (range scan).

For more details see https://technet.microsoft.com/en-us/library/2008.08.database.aspx.

Chapter 2 - Checkmarx Tables Overview

The CxSAST application has two databases:

- **CxActivity** – contains tables serving auditing persistancy
- **CxDB** – primary database serving ongoing usage

CxSAST inserts data in CxActivity tables without deleting or updating them in the future. Therefore, the risk of fragmentation and as result performance degradation is low.

CxDB database has tables for various functionalities working in different ways. From now, the discussion will be related to the tables dynamic having relatively massive data. These tables are divided to three categories:

	Tables List	Description/Purpose
1	dbo.PathResults, dbo.NodeResults, dbo.ResultsLabels, dbo.ResultsLabelsHistory, dbo.Auxiliary_*	Ongoing growing tables having purging policy as default application behavior
2	CxBi.*, dbo.QueryVersion, dbo.ScanRequests, dbo.ScanStatistics, dbo.TaskScans, dbo.LoggedinUser	They serve for analyzing/calculation with removing data at the end of processing
3	dbo.Libraries, dbo.ScannedLibraries, dbo.ScannedVulnerabilities, dbo.Scans, dbo.Vulnerabilities	Ongoing growing tables

Tables from the two first categories have high risk of fragmentation.

Instead of rebuilding or reorganizing all indexes on a regular basis (e.g. daily/weekly/monthly) the more sophisticated approach involves using the dynamic management function (DMF) sys.dm_db_index_physical_stats to periodically determine which indexes are fragmented, and then choosing whether and how to operate on those. This function accepts parameters such as the database, database table, and index for which you want to find fragmentation. An example of the function usage is as follows:

```
SELECT

            OBJECT_NAME(ips.object_id)              "TblName"

            ,ips.object_id

            ,ips.index_id

    ,(select i.name from sys.indexes i where ips.object_id = i.object_id AND ips.index_id = i.index_id and ips.index_level = 0) "IndexName"

            ,ips.index_type_desc              "IndexType"

            ,ips.avg_fragmentation_in_percent

            ,ips.fragment_count

            ,ips.avg_fragment_size_in_pages

            ,ips.forwarded_record_count

            ,ips.alloc_unit_type_desc

            ,ips.page_count

            ,ips.index_depth

            ,ips.avg_page_space_used_in_percent

            ,ips.record_count

            ,ips.ghost_record_count

            ,ips.version_ghost_record_count

            ,ips.min_record_size_in_bytes
```

,ips.max_record_size_in_bytes

,ips.avg_record_size_in_bytes

,ips.compressed_page_count

FROM sys.dm_db_index_physical_stats(DB_ID('CxDB'),NULL,NULL,NULL,'<Scanning

Mode>') AS ips WHERE (1=1)

and index_level=0

ORDER BY OBJECT_NAME(ips.object_id),ips.index_id;

Scanning Mode - the mode in which the function is executed determines the level of scanning performed to obtain the statistical data that is used by the function. *Mode* is specified as

- LIMITED - fastest mode and scans the smallest number of pages (min info)
- SAMPLED - returns statistics based on a 1% sample of all the pages in the index or heap. If the index or heap has fewer than 10,000 pages, DETAILED mode is used instead of SAMPLED.
- DETAILED – heaviest mode and scans all pages and returns all statistics (max info)

The default (NULL) is LIMITED.

For more details see https://msdn.microsoft.com/en-us/library/ms188917(v=sql.110).

Returns size and fragmentation information for the data and indexes of the specified table or view. For an index, one row is returned for each level of the B-tree in each partition. For a heap, one row is returned for the IN_ROW_DATA allocation unit of each partition. For large object (LOB) data, one row is returned for the LOB_DATA allocation unit of each partition. If row-overflow data exists in the table, one row is returned for the ROW_OVERFLOW_DATA allocation unit in each partition.

Along with other information, the following columns are most important for detecting fragmentation:

Returned Column	Description
avg_fragmentation_in_percent	This indicates the amount of **external fragmentation** you have for the given objects. **The lower the number the better** - as this number approaches 100% the more pages you have in the given index that are not properly ordered. For **heaps**, this value is actually the percentage of extent fragmentation and not external fragmentation.
avg_page_space_used_in_percent	This indicates how dense the pages in your index are, i.e. on average how full each page in the index is (**internal fragmentation**). **The higher the number the better** speaking in terms of fragmentation and read-performance. To achieve optimal disk space use, this value should be close to 100% for an index that will not have many random inserts. However, an index that has many random inserts and has very full pages will have an increased number of page splits. This causes more fragmentation. Therefore, in order to reduce page splits, the value should be less than 100%.
fragment_count	A fragment is made up of physically consecutive leaf pages in the same file for an allocation unit. An index has at least one fragment. The maximum fragments an index can have are equal to the number of pages in the leaf level of the index. So the less fragments the more data is stored consecutively.
avg_fragment_size_in_pages	Larger fragments mean that less disk I/O is required to read the same number of pages. Therefore, the larger the avg_fragment_size_in_pages value, the better the range scan performance.
forwarded_record_count	Number of records in a **heap** that have forward pointers to another data location. (This state occurs during an update, when there is not enough room to store the new row in the original location.) NULL for any allocation unit other than the IN_ROW_DATA allocation units for a heap. NULL for heaps when mode = LIMITED.

Decision which defragmentation method to use should be based on the degree of fragmentation and table type (as result of running sys.dm_db_index_physical_stats, see the previous chapter). There are two main methods:

Method	When	Comments
ALTER INDEX REORGANIZE	> 10% and < = 30%	Reorganizing an index is always executed **online** and uses minimal system resources. It defragments the leaf level of clustered and non-clustered indexes on tables and views by physically reordering the leaf-level pages to match the logical, left to right order of the leaf nodes. Reorganizing also compacts the index pages. Reorganizing a specified clustered index compacts all LOB columns that are contained in the clustered index. Reorganizing a non-clustered index compacts all LOB columns that are non-key (included) columns in the index. Reorganize does NOT update statistics, this should be run manually. Single threaded only – regardless of edition
ALTER INDEX REBUILD WITH (ONLINE = ON)	> 30%	Rebuilding an index can be executed online or offline. To achieve availability similar to the reorganize option, you should rebuild indexes online. The ONLINE option and parallelism are available for Enterprise Edition only! When performed offline, the entire table is unavailable for the duration of the operation. Defragments all levels of the index and update statistics.

Important notes:

- There are other methods (e.g. drop and recreate cluster index), but are more complicated and less recommended.

- Fragmentation alone is not a sufficient reason to reorganize or rebuild an index. The main effect of fragmentation is that it slows down page read-ahead output during index scans. This causes slower response times. If the query workload on a fragmented table or index does not involve scans, because the workload is primarily singleton lookups, removing fragmentation may have no effect.

- These values (in **When** column compared with **avg_fragmentation_in_percent**) provide a rough guideline for determining the point at which you should switch between ALTER INDEX REORGANIZE and ALTER INDEX REBUILD. However, the actual values may vary from case to case. It is important that you experiment to determine the best threshold for your environment. Very low levels of fragmentation (less than 5%) should not be addressed by either of these commands because the benefit from removing such a small amount of fragmentation is almost always vastly outweighed by the cost of reorganizing or rebuilding the index. The decision should be take into consideration SQL Server Edition.

- In general, fragmentation on small indexes is often not controllable. The pages of small indexes are stored on mixed extents. Mixed extents are shared by up to eight objects, so the fragmentation in a small index might not be reduced after reorganizing or rebuilding the index.

CxSAST Quick Start

This Quick Start includes information on setting up first project scans and an overview of presets.

ⓘ **Page Contents**

- Setting Up
  - o   Step 1: Enter Project General Settings
  - o   Step 2: Select Source To Scan
  - o   Step 3: Scan Execution
- Reviewing Scan Results
  - o   Step 1 – Projects & Scans
  - o   Step 2 – Review Scan Results in the Source Code
- Preset Manager: Overview

Setting Up
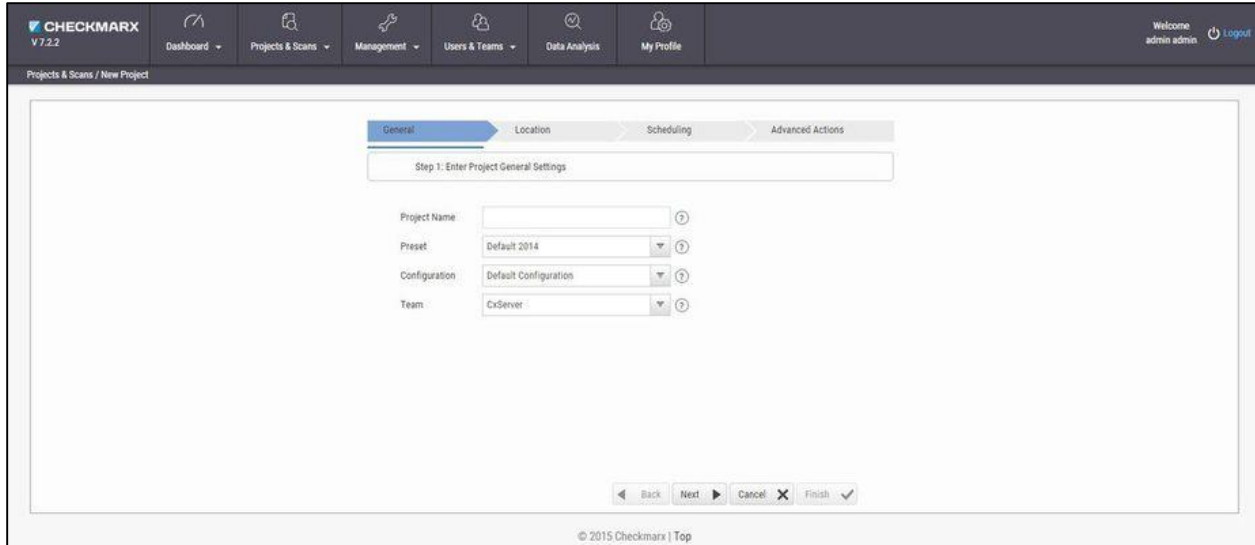
In the **Projects & Scans > Create New Project** window perform the following procedure:

Step 1: Enter Project General Settings

1. **Project Name**: Provide an appropriate Project Name for the project.
2. **Preset**: The Preset will determine the scan rules for the project. Select the appropriate scanning Preset from the drop-down list.
3. **Configuration**: Select the Configuration for the new project. For the trial version, it is advised to perform the default selection.
4. **Team**: Select the Team for the new project. For the trial version, it is advised to perform the default selection.
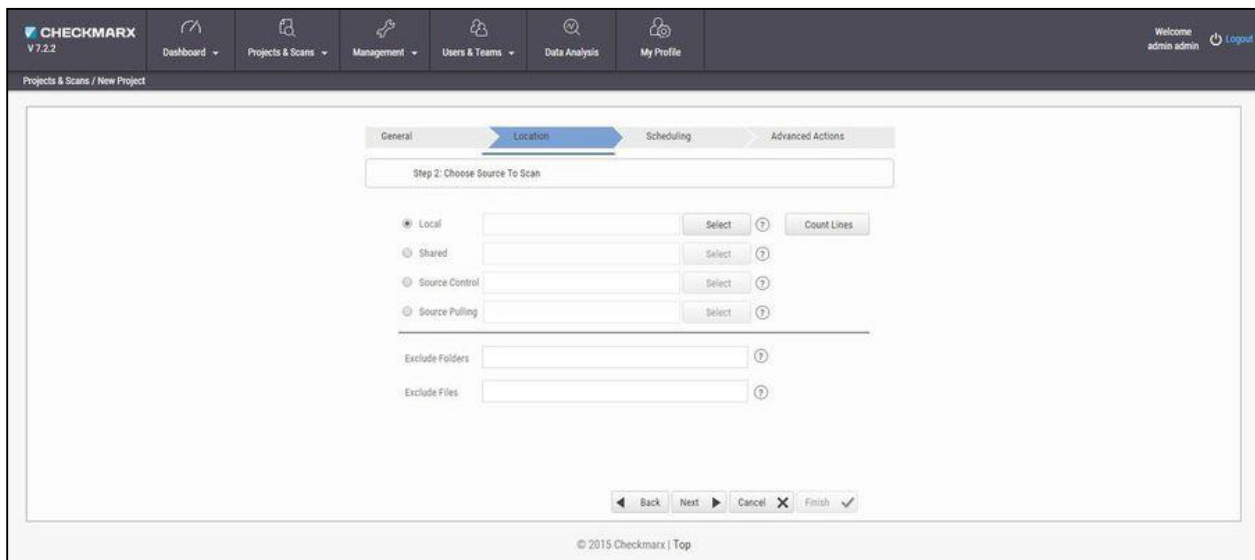
⚠ It is advised to leave the fields **Configuration** and **Team** unchanged in the trial.

Step 2: Select Source to Scan

1. Select **Local** to upload code as a ZIP file. The code must be zipped by MS zip. The test account is limited to 350,000 Lines of Code (LOC).
2. Select **Shared**, **Source Control** or **Source Pulling**, and upload the code in any other format.
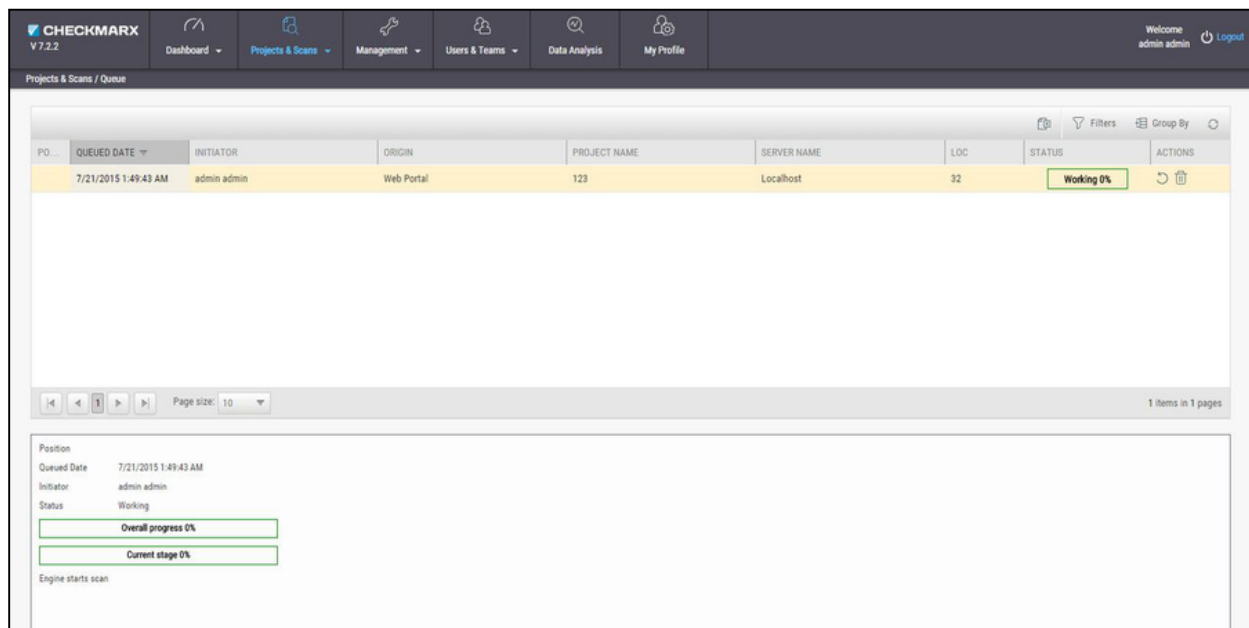
ⓘ Note that you can scan the "**OWASP Benchmark Project**" code; go to **https://github.com/OWASP/benchmark**, click the **Clone or download** button and select your preferred option.

---

3. Other sample code for scanning include:

   Bookstore.Net; **Bookstore.Java**; **Bookstore.php4**; **WebGoat5.0**; **WebGoat6.0**; **CPP Example**; **iGoat**; **Samples**; **Android**.

4. . If using a Browser/ Eclipse/ Visual Studio/ IBM RAD, please start with the browser option.

5. . When the Finish button becomes active, click **Finish** to place the project into a queue.

Step 3: Scan Execution

- In **Projects & Scans > Queue**, monitor the scan progress by clicking the project line in the queue table.

Reviewing Scan Results

Step 1 – Projects & Scans

- In **Projects & Scans > Projects**, click Scans List to view the high level summary of scan results and account activity.

For more information on Dashboards see **Getting to Know the System Dashboard.**

Step 2 – Review Scan Results in the Source Code

View detailed scan results within the Source Code. Vulnerabilities and navigated attack path are highlighted.

The View Results page is divided into four (4) sections:

- Scan Results Summary by vulnerability,
- Results table or Graph,
- Attack Vector
- Source code

Scan Result Summary

- **Scan Results Summary pane**: Summary of vulnerabilities detected, grouped by High, Medium and Low titles. The summary shows the number of instances of those vulnerability appearances in the code. The "tool tip" displays more information about the specific vulnerability and best practice technique for removal.
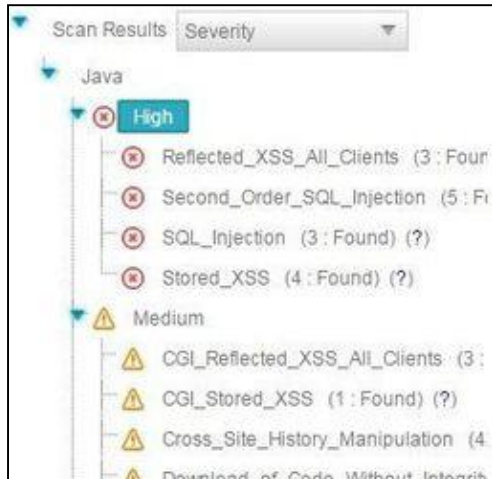
- **Source Code pane**: View specific points of vulnerabilities detected within the Source Code.

- **Results Table**: A listing of each vulnerability instance and detail. Manage results by using the Filter button to organizes data and saves results.

- **Graph**: Gain a macro chart perspective vulnerabilities found in code, see correlations and identify the optimal points for fix (red buttons).
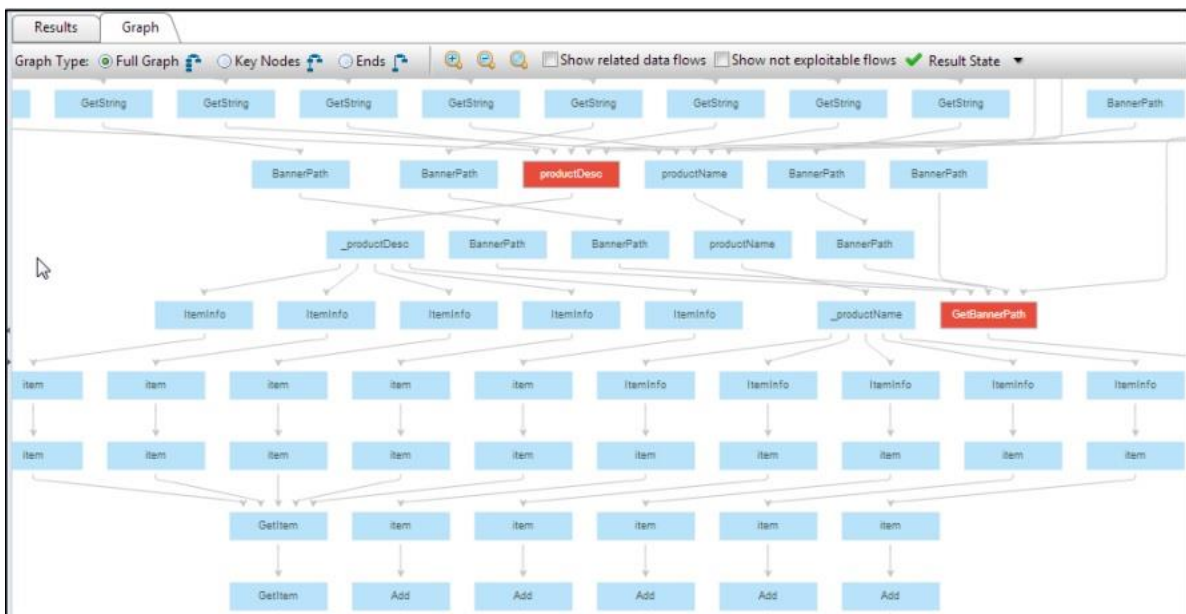
- **Attack Vector**: Note the full path of code elements that constitute the vulnerability instance selected in the Results pane.

For more information on Working with Scan Results, see **Working with Scan Results.**

Preset Manager: Overview

A Preset Setting consists of a group of queries. The Preset Manager enables the viewing of query details in each Preset.

To access the Preset Manager go to **Management > Scan Settings > Preset Manager**.
Queries contained inside the preset are presented in the right pane and description
of vulnerability discovered by each query are described in **Query Description** below.
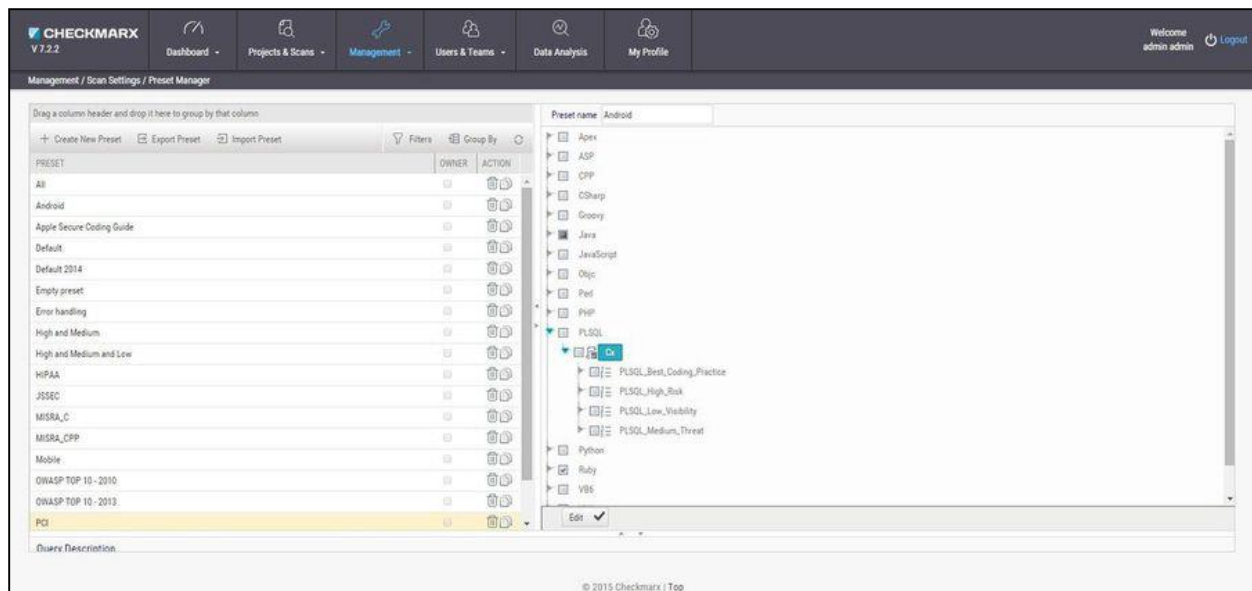
For more information on Managing Presets **Managing Query Presets**.

CxSAST User Guide

This guide provides information about CxSAST usage, once it has already been set up in your environment.

The CxSAST Web Interface
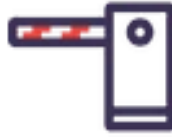
The Queue

User Administration

Management Settings

Creating and Managing Projects

Scan Results

Dashboard Analysis

The CxSAST Web Interface

CxSAST provides an intuitive web interface for managing and analyzing code scan projects and the CxSAST system.

In This Section:

- Accessing the Web Interface
- Getting to Know the System Dashboard

Accessing the Web Interface

Access the CxSAST web interface in either of the following ways:

- To access CxSAST locally (from the server host), use the **Checkmarx Portal** shortcut on the Desktop or navigate to the Checkmarx folder (**Start** > **All Programs** > **Checkmarx** > **Checkmarx Portal**).
- To access CxSAST from any other computer, make sure that organizational routing and firewall configuration allow the client computer to access the CxSAST server. Point your browser to: http://<server>/cxwebclient/login.aspx where <server> is the IP address or resolvable hostname of the CxSAST server.

Upon a fresh installation, a single Administrator Account needs to be created.

Once the Set Administrator Credentials window is displayed, add the following credentials:

- Administrator User Name
- Password
- Confirm Password

ⓘ The required password complexity is as follows: 9 to 400 characters, at least 1 uppercase letter, at least 1 lower case letter, at least 1 special character, at least 1 digit.

Click **Confirm** to complete.

You can subsequently change the Administrator password and add CxSAST users.

Getting to Know the System Dashboard

Overview

The CxSAST web interface includes drop-down navigation menus for each relevant module, as follows:

Dashboard | Projects & Scans | Management Settings | Users & Teams | Data Analysis | My Profile Settings

---

ⓘ Visual indicators are displayed just underneath the Checkmarx logo/version and may include:

- Type of product edition currently installed - SDLC or Security Gate
- Expiry date of the current CxSAST license. The indicator appears 90 days (defined in the DB) before the actual license expiry date and, if defined, an email notification is automatically sent to the CxSAST System Administrator.

The Help button allows CxSAST users to navigate to available support resources on our new Checkmarx Customer Center portal. This portal holds a restricted area, available for activated users only.

CxSAST web interface menu items are described below.

Dashboard Menu

View the state of your engines, scans and queues:

Project State: The current project state, including project information such as Risk level score, High/Medium vulnerabilities, LOC, and Last scan date.

Failed Scans: Log of failed scans, including reason or partial explanation such as "failed to start scanning due to one of the following reasons: source folder is empty, all source files are of an unsupported language or file format".

Utilization: A graphic interface divided into the following four quadrants:

- **Engine State:** Provides information about the number of scans to engine ratio.
- **Queue State**: Provides information about the number of scans in the queue and their LOC size/ Average waiting time.
- **Projects with Longest Scans**: Provides information about the Top 3 scans in the Longest Waiting Time category.
- **Queue Load**: Provides perspective about the queue load over a 7 day period. The darker the blue the more in the queue; whereas the empty cell with the black outline is the queue running now.

Risk: The Risk graph at the upper half of the window displays the High Risk projects over the last 7 day period, while the lower half displays the Risk Trend of selected projects and Time periods.

Projects and Scans

View projects scans and queues:

- **Create New Project**: Starts the New Project wizard.
- **Queue**: View statuses of currently running scans.
- **Projects**: All projects configured for groups in which the logged-on user is a member.
- **All Scans**: Existing scan results of projects configured for groups in which the logged-on user is a member.

Management Settings

Manage Scan and Server settings:

Scan Settings:

- **Query Viewer:** View and manage queries used in the system.
- **Preset Manager:** Create and manage sets of queries according to your needs.
- **Pre & Post Scan Actions:** Allows defining actions, based on preloaded scripts that will run prior or post scan.
- **Source Control Users:** View and modify details of user accounts for accessing source control repositories.

Connection Settings:

- **LDAP Servers**: Define an LDAP Server for your environment.
- **SAML Management**: Configure SAML for your environment.

Application Settings:

- **General:** Folder locations, SMTP, and other settings.
- **License Details:** The installed license details, including supported languages, roles, and number of companies and service providers.
- **Installation Information:** Locations of server components.

Maintenance:

- **Data Retention**: Set the requested policy for deleting scans from all projects in the system.

Manage Custom Fields:

- **Manage Custom Fields**: Define project attributes (metadata) by using custom fields

Users & Teams

Manage users and the user hierarchy:

- **Organization**: Configure the organizational hierarchy
- **Confirm Users**: Confirm users who self-registered

Data Analysis

View and analyze scan-related data.

My Profile

Change personal details (for all user types) and password (only for Application local users, not Windows domain users) of logged-on user.

See also **Managing Tables.**

Dashboard Menu
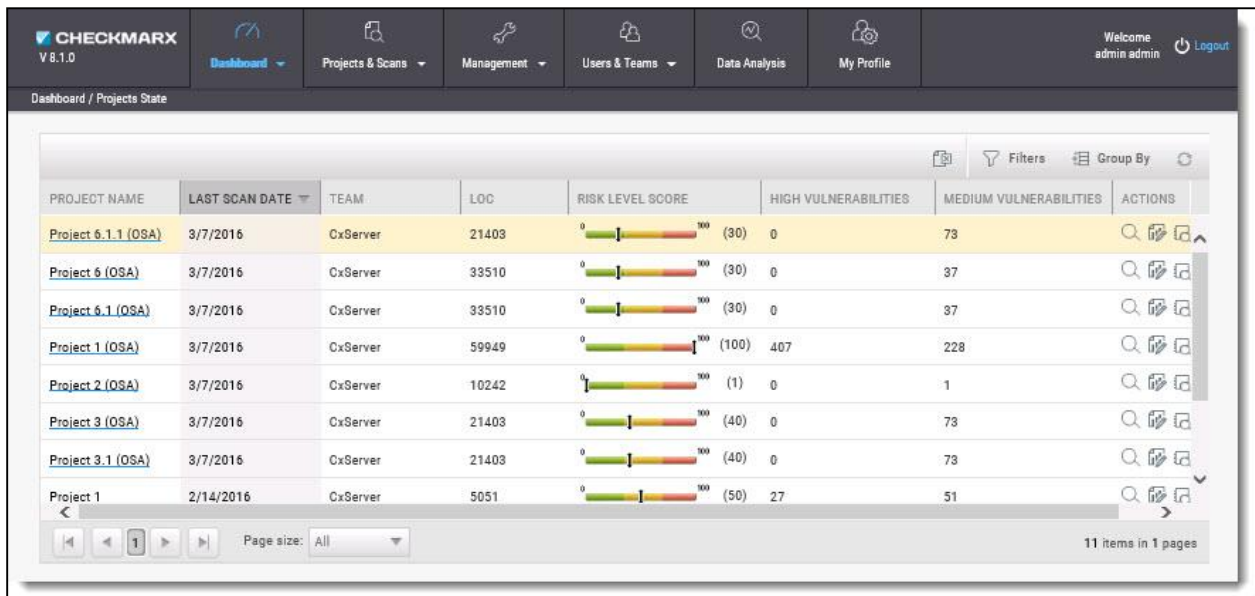
As a manager (Server, Company or Service Provider manager) you can view high-level information such as the state of your engines, project status, scans and queues in the Dashboard Menu.

To enter the Dashboard Menu click **Dashboard** and select the relevant sub-menu.

Project State

The Project State window displays the status of all current projects.

Go to **Dashboard > Project State**. The Project State window is displayed.

The Project State window includes the following information:

- **Project Name** - click on the **Project Name** link to view the Consolidated Project State
- **Last Scan Date**
- **Team**
- **LOC**
- **Risk Level Score**
- **Vulnerabilities** (High and Medium)
- **Actions** ([icon] View results, [icon] Create report, [icon] Download scan logs)

You can Export as CSV File [icon], use the [icon] Filter and [icon] Group By tools as well as [icon] Refresh the current view.

> ⓘ Projects that have not yet had scans performed on them are displayed in the Project State window the "No SAST Scans performed" message.

Failed Scans

The failed scans window displays the status of all failed scans.

Go to **Dashboard > Failed Scans**. The Failed Scans window is displayed.

The Failed Scans window includes the following information:

- **Scan Date**
- **Project Name**
- **Initiator**
- **LOC**
- **Comments** (as in The Queue)
- **Details**
- **Actions** (⬚ Download scan logs)

You can ⬚ Export as CSV File, use the ⬚ Filter and ⬚ Group By tools as well as ⬚ Refresh the current view.

Utilization

The Utilization window displays the status of all completed and running scans.

Go to **Dashboard > Utilization**. The Utilization window is displayed.
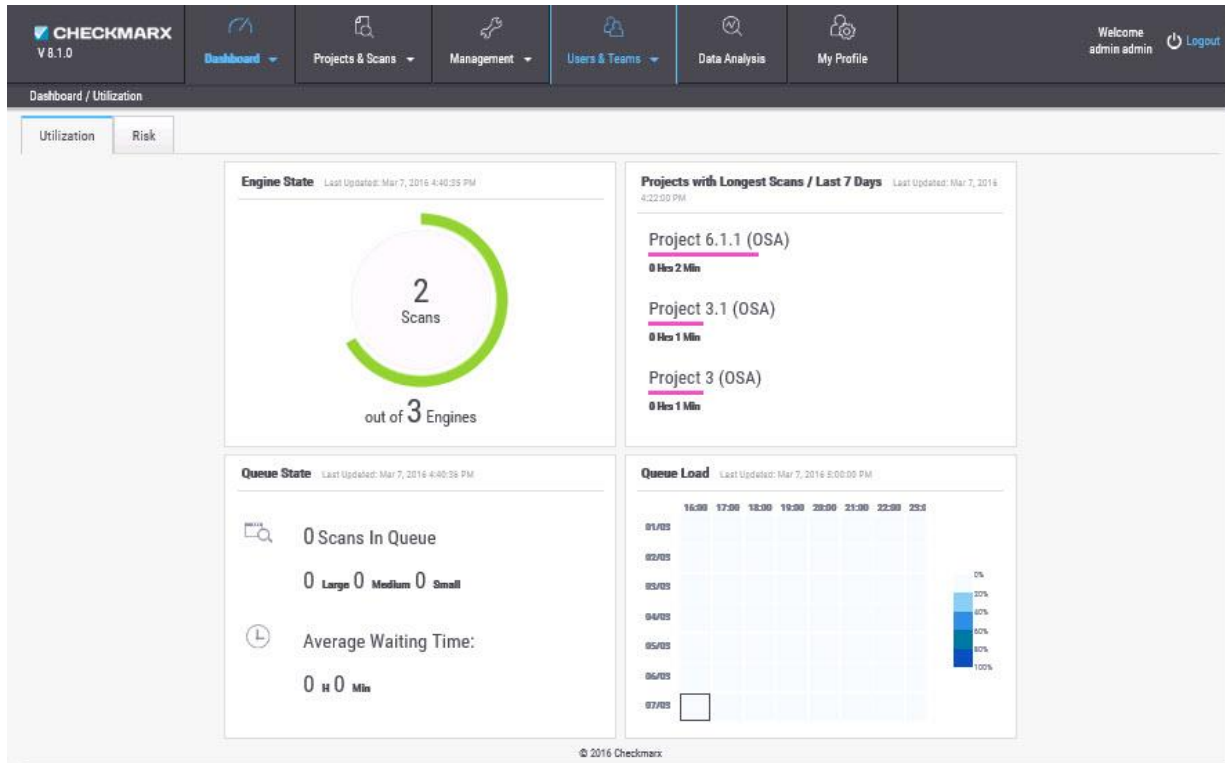
The Utilization window includes the following information:

- **Engine State** - number of scans to engine ratio
- **Queue State** - number of scans in the queue and their LOC size / average waiting time
- **Projects with Longest Scans** - top 3 scans in the longest waiting time category
- **Queue Load** - queue load over a 7 day period:
    - The darker the blue the more in the queue
    - Empty cell with the black outline indicates currently running queue

Each widget in the Utilization window includes a time-stamp indicating the last date and time the data was last updated.

Risk State

The Risk State window displays the number of vulnerabilities and the risk score for each project.

Go to **Dashboard > Risk State**. The Risk State window is displayed.

The Risk State window includes the following information:

- **Projects at Highest Risk / Last 7 Days** - risk score for each project by filtering option
- **Risk Trend** - number of vulnerabilities by filtering option

You can filter by Team/Group, Project Name and Number of Days. Click Apply to confirm.

Roll-over the graph to get the project risk and vulnerabilities scores according to date.

Click Project Name link to view Project State Summary

Click the legend to display/hide respective vulnerabilities (High, Medium, Low).

Each widget in the Risk State window includes a time-stamp indicating the last date and time the data was last updated.

Creating and Managing Projects

A CxSAST project defines the source to be scanned, scan scheduling, and notification settings. Normally, a CxSAST project should correspond to a software development project, or to part of one. Any time a scan is run (manually or scheduled), the scan results remain associated with the CxSAST project.

> ⓘ For Continuous Integration development methodology, if a new branch is created for each iteration, update the code location within the existing project (rather than creating a new project) so that all the results will reside within a single project. Scanning of projects that include multiple code languages is supported. To enable this feature, please contact Checkmarx professional services.

Open Source Analysis (CxOSA) can be added to an existing CxSAST project in cases where open source components are used as part of the development effort. When CxOSA is activated, CxSAST sends the open source fingerprint (SHA-1 hash plus file extension) to the CxOSA service. Using this fingerprint, the CxOSA service maps the open source libraries, identifies any vulnerabilities, analyses license risk and compliance, builds inventory and detects outdated libraries. A comprehensive report can be generated from the **Consolidated Project State.**

In This Section:
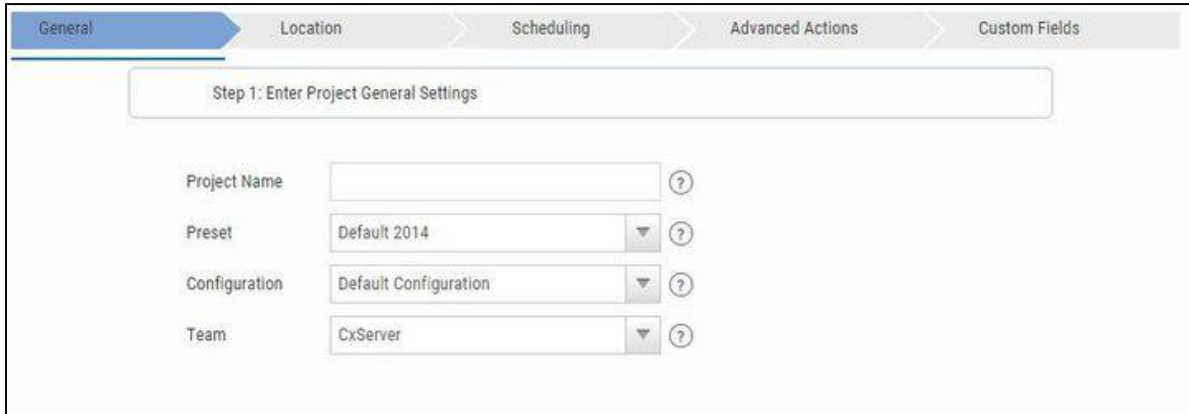
Contents
- Creating and Configuring Projects
- Branching / Duplicating Existing Projects
- Managing Projects and Running Scans
- Advanced Actions
- Viewing Project Details
- Managing Queries

Creating and Configuring a CxSAST Project
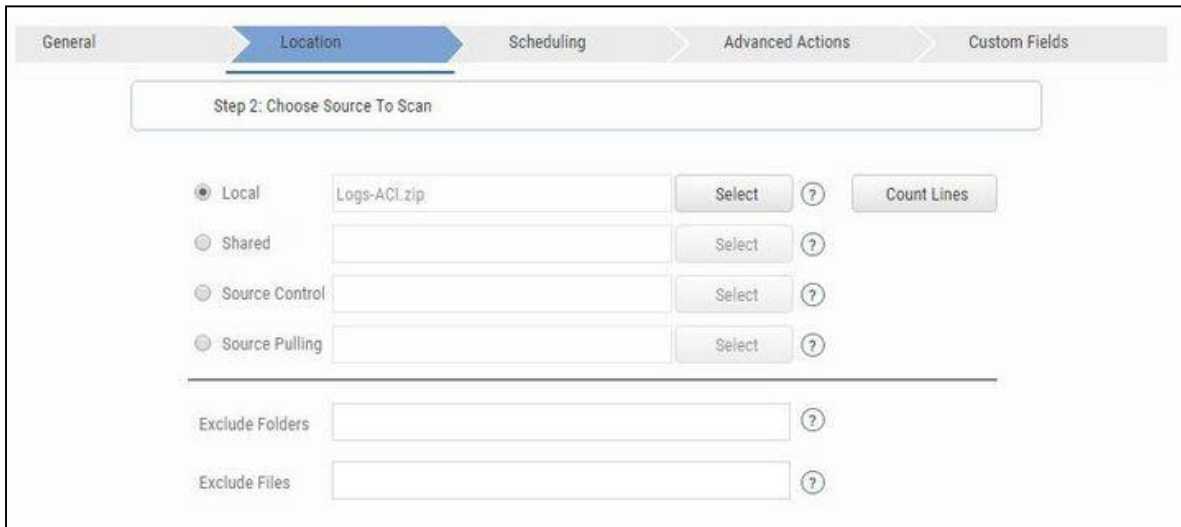
To create a CxSAST project:

1. Select **Project & Scans > Create New project**.

2. Configure the following **General** project properties:

- o **Project Name**: Should indicate the source code to be scanned and tracked.
- o **Preset**: The set of queries to be run on the code scan. **Default** includes a set of queries recommended by Checkmarx for most projects. For all coding best practices, select **All**. For example, for an Android project select **Android**. For a full list of executed queries, see the Vulnerability Queries section in the release notes.
- o **Configuration**: Advanced users only, for scanning double-byte encoded source code.
- o **Team**: Determines who will be able to view your project and its scan results. Available options depend on the permissions of the logged-on user. Selecting **CxServer** allows access only to the server Administrator. If you're working as a single user, leave the default option.

3. Configure the source code's **Location**:
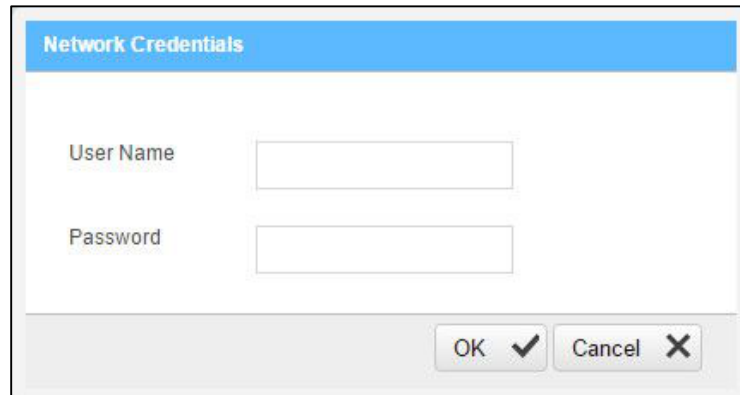
o **Local**: Click **Select** to browse to a local zip file containing the code. Future scans to the project are also via local upload (see **Managing Projects and Running Scans**).

⚠ **Notes**
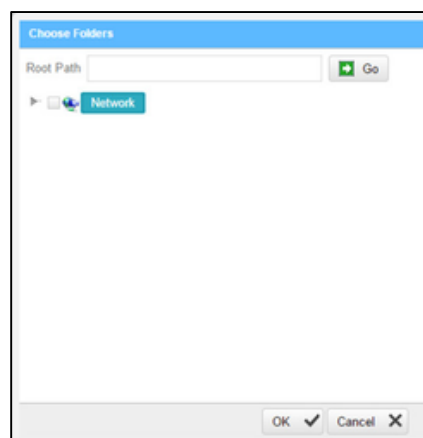
- Since the CxSAST server cannot automatically access the local source, Local projects do not have automatic scheduled scans. You will need to periodically manually upload a new zip file.
- Zip files generated in a Linux environment may not function properly.
- **Count Lines** counts lines in the source code to be scanned.
- If the zip file is larger than 200 MB, you will not be able to upload it. To create a smaller zip file of only files with specified extensions, use the CxZip utility.
- See also: Troubleshooting

- o **Shared**: The project code is maintained on a network server accessible from the CxSAST server. Click **Select** to configure details:

    a. Provide Windows domain credentials, with which CxSAST will access the network:

The username should be in format: domain name\user name.

    b. Click **OK**, and select one or more network folders containing the project code:

    c. Click **OK**.

- o **Source Control**: The project code is maintained in a TFS , SVN , PerForce, or GIT source control system. Click **Select** to configure the connection to a source control system.
- o **Source Pulling**: Activates a configurable script to pull source code from a source control system, available here only if previously configured in the CxSAST Windows client application. Depending on script configuration, you'll be able to select a script and/or location.

4. Optionally, you can **Exclude Folders** and/or **Files** from being scanned. Type a comma-separated list of folders or files, including wildcards to exclude. For example, consider the following archive, any file/folder name typed into the Exclude File/Folder fields will exclude the file or folder in the project with that name. Also, typing {file name}, for example, 'readme.txt', will exclude everything in the location of the project with this name:

```
|-- add-ons
| |-- connectors
| | |-- cvc3.js
| | |-- spass.js
| | `-- z3.js
| |-- lib
| |-- readme.txt
| |-- smt_solver.js
| `-- src
|-- doc
| `-- readme.txt
`-- src
`-- lib
|-- find_sql_injections.js
|-- jquery.js
`-- logic.js
```

5. Optionally, click **Count Lines** to display the number of lines in the current project.

Please note that as the Java Script is being enhanced in the scan process – the real count of lines might be bigger than the result that will be shown from the Count Lines option (as well as from the Cx CMD Line Counter).
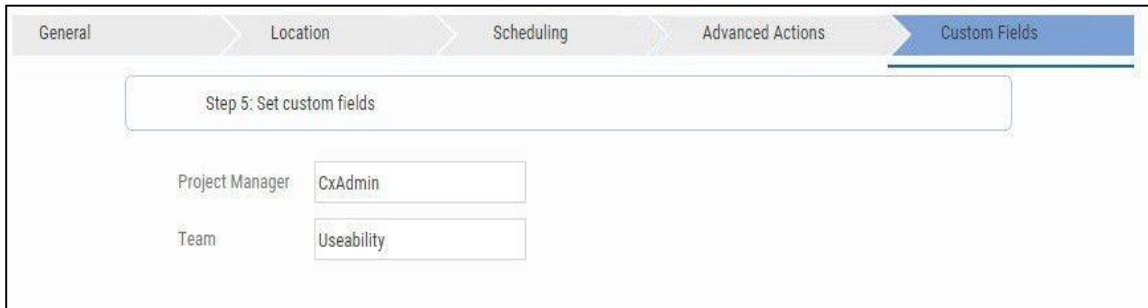
The following steps of the wizard are optional. You can click **Finish** to skip them.

1. Click **Next** and configure **Scheduling** (not applicable to a **Local** source code location):
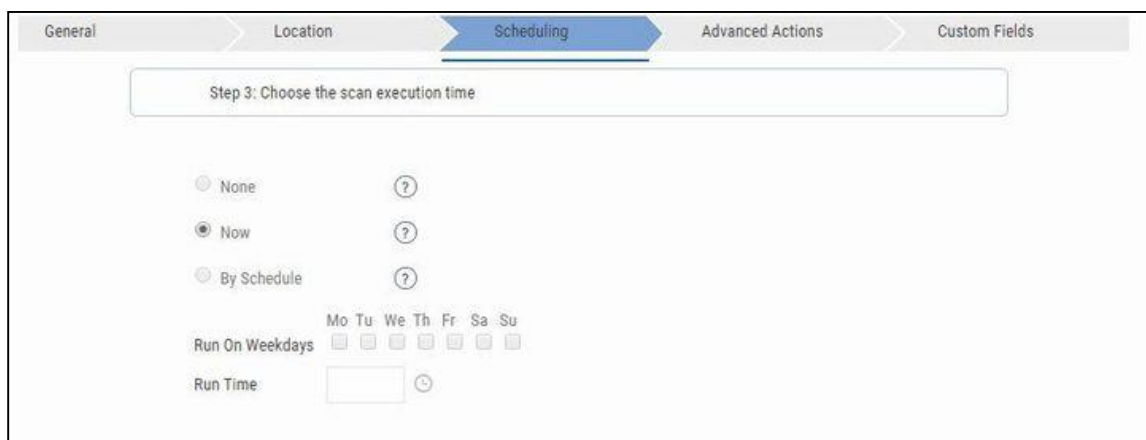
> ⚠ To support Continuous Integration development methodology, it is recommended to schedule periodic scanning of source files, so they can be checked after modifications. This can be automated via CLI in the Build file, but it does not have to be done this way because CxSAST scans source code and does not require

2. Click **Next**, and optionally configure **Advanced Actions.**
3. Click **Next**, and optionally configure **Managing Custom Fields.**

General	Location	Scheduling	Advanced Actions	Custom Fields

Step 5: Set custom fields

Project Manager   CxAdmin

Team   Useability

4. **Finish** the wizard. It may take some time for the scan to begin running.

Branching / Duplicating Existing Projects
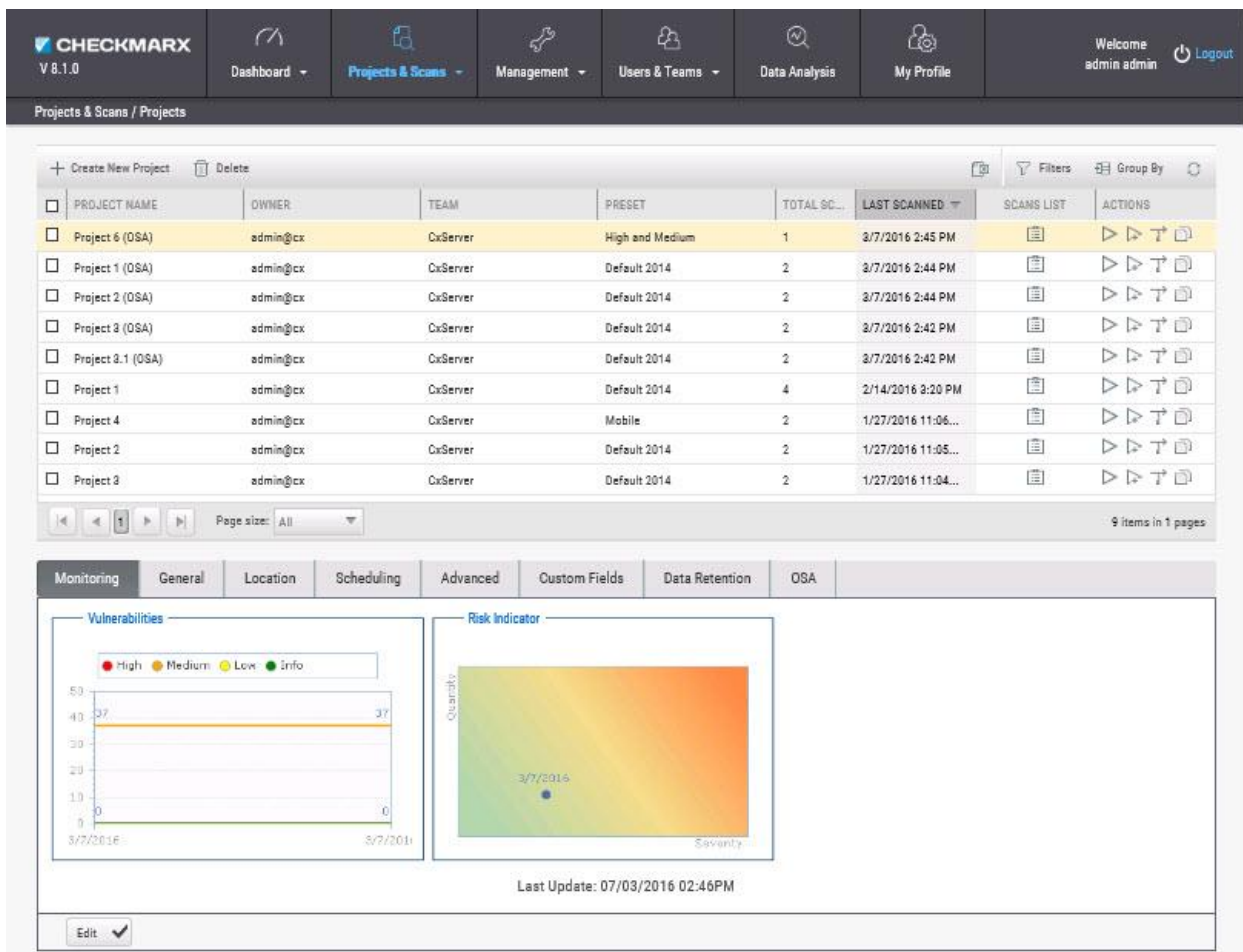
CxSAST gives you the capability to branch / duplicate an existing project and have the new project inherit all of the issues, comments and dispositions from the source project. Once the project has been branched / duplicated you can treat it as a separate project with separate issues to manage.

> ⓘ **Branch Project** - similar to copy project, except it copies the following set of properties: Preset, Team and the Last scan from the source project with all results and remarks.
>
> **Duplicate Project** - creates a new project based on the settings of the existing one and also copies the following set of properties: Preset, Team, Exclusions, Scheduling, Pre-scan, Post-scan and Scan failure emails.

To branch or duplicate an existing project:

Go to **Projects & Scans and** select **Projects**.

Click **Branch Project** [icon] or **Duplicate Project** [icon] .

Define **General** settings and click **Next**.

Define the **Location** of the source code and click **Next**.

Define scan **Scheduling** options and click **Next**.

Define **Advanced Action** settings and click **Next**.

Define **Custom Field** settings and click **Next**.

Define Data Retention settings and click **Next**.

Once complete, click **Save**. The following message is displayed: "Branching may take a few minutes, would you like to proceed?"

Click **OK**. The "Branching successfully ended" message is displayed.

The branched/duplicated project is displayed in the Projects window.

Managing Projects and Running Scans
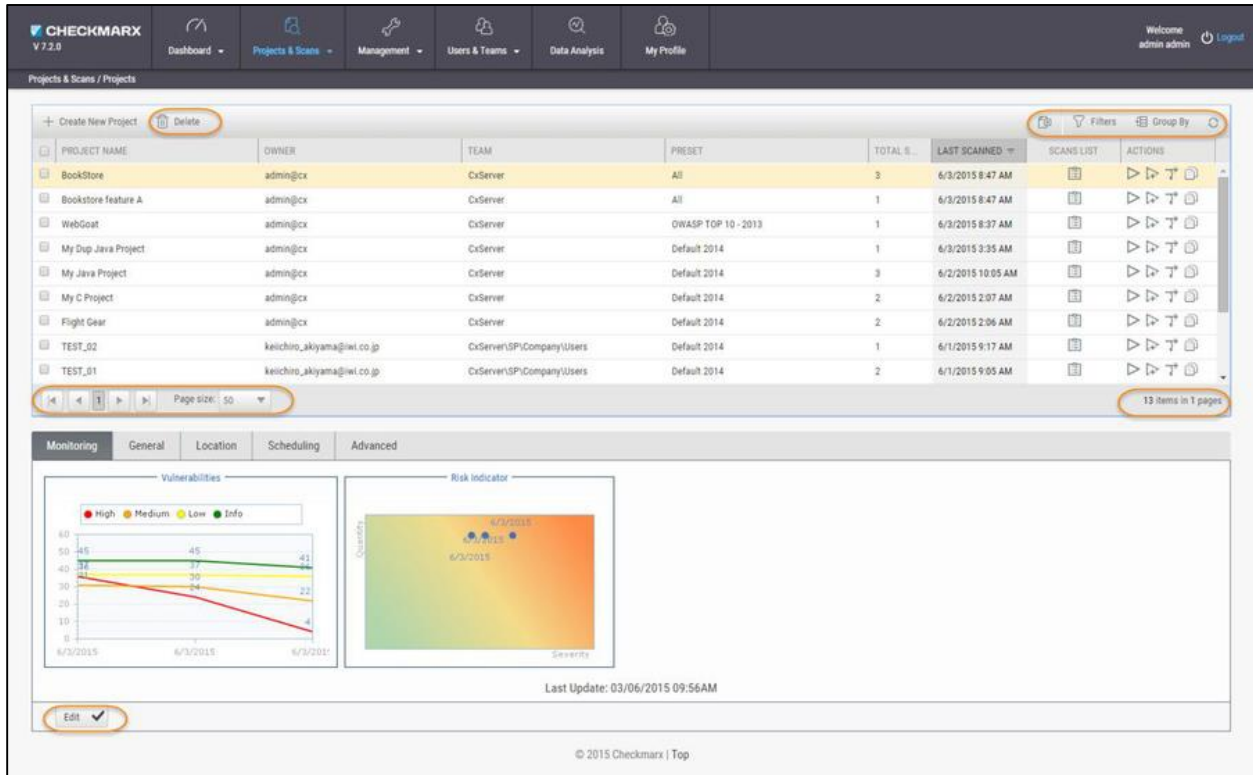
Scan List/Actions

In **Projects & Scans > Projects**, various scans and action lists are available (see **Creating and Configuring Projects**).

	Scan List	Displays the project in the individual project path, e.g. Projects & Scans/View Project Scans/My Java Projects.
	Full Scan	A scan of the whole project. If the project is configured for a local location, this will require uploading a zip file with the updated source code.
	Incremental Scan	Incremental scan is used to increase the scanning speed of the project. It works by scanning only the code that has changed since the last full scan was performed. During the incremental scan, the system takes each file that was sent to be incrementally scanned and creates a hash of its code. It then compares the value of the hash with the value of the hash of the files with the same name that was scanned on the last full scan. ⓘ • Incremental scan needs to be performed on all of the code, not only on the changed code. • Incremental scan is recommended only if the regular scan takes more than 45 minutes. • When using incremental scan as part of CI/CD (for example as part of a build process) you need to make sure that a full scan is performed every X amount of incremental scans. Otherwise the changes will aggregate and when more than 7% of the code has changed CxSAST will either run a full scan or fail the scan, depending on the configuration.

> ⓘ If a zip file is uploaded that contains file path greater than 255 characters, the file will not be sent for scanning. Shorten the file path and try again.

	Branch Project	The Branch Project operation is similar to copy project, but it copies a different set of properties: Preset, Team and the Last scan from the source project with all results and remarks.
	Duplicate Project	Duplicate Project creates a new project based on the setting of an existing one. From the existing project it will copy the following: Preset, Team, Exclusions, Scheduling, Pre-scan emails, Post-scan emails and Scan failure emails.

Managing Tables

The various tables in the web interface provide navigation and pagination controls:
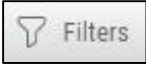
The following actions are available from the table's header bar:

- **Delete** - Delete rows

  > ⓘ A project can contain one or more scans that are locked, or whose deletion requires authorization that the current user does not have. In such cases, all objects that can be deleted are removed, and a message is displayed to notify the user about the objects that could not be deleted.

  > ⓘ When the user deletes a project, the project is not deleted from the database. Instead, the project is marked as "deprecated". All scans under the deleted project are also marked as "deprecated". This deprecated data can be ultimately be removed as part of the Data Retention Management process.

- **Export** - Export to CSV

- **Filters** - ▽ Filters Display a filtering field for each column heading. After typing a filter text (not case-sensitive), press **Enter** to filter.

- **Group By** - ⊞ Group By Group values by dragging the column header to the top bar. For example, a manager could group projects by user.

- To re-order the rows by the values of a column, without grouping, just click the column heading (toggle between ascending and descending order).

- **Refresh** - ↻ Refresh the table.

Advanced Actions

CxSAST can automatically perform configurable actions with each scan. The available types of **Advanced Actions** are:

- Send an email message
- Run an executable

In This Section:
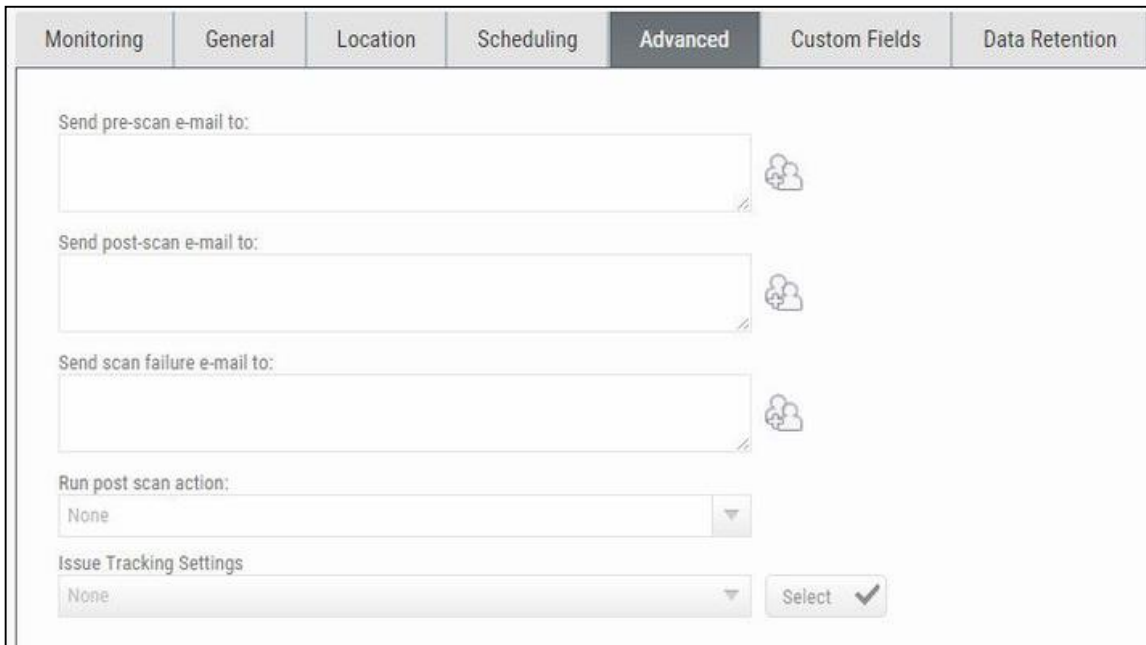
- Configuring an Email Action
- Configuring an Executable Action

Configuring an Email Action

You can configure CxSAST to automatically send an email before or after a scan.

To configure an automatic email:

1. In a project's Advanced Actions tab, enter the requested email address under the relevant event:

2. Click and add recipients. Separate email addresses with semicolons (;).
3. Click **Finish**.

> ⚠ Email actions require SMTP settings
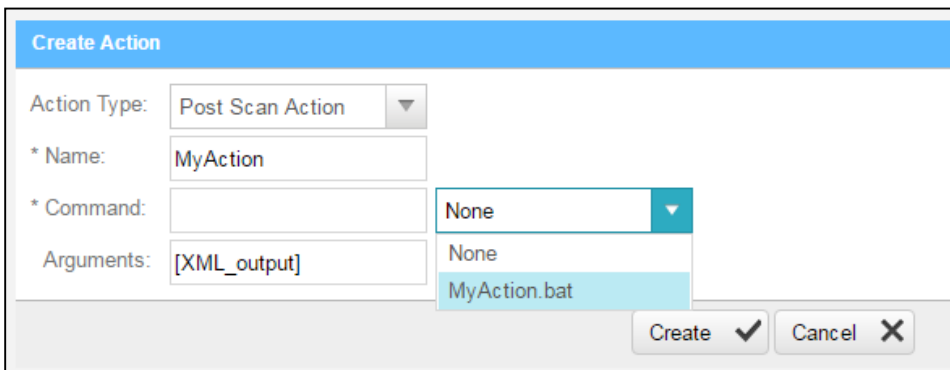
Configuring an Executable Action

To configure CxSAST to run an executable before or after a scan:

1. Upload an executable: To ensure the integrity of the system and to restrict access, executable files must be uploaded manually by approved personnel.

> ⓘ The location used by CxSAST for executable files appears in **Management > Application Settings > General > Executables Folder**.

2. Define an Action for the executable: Go to **Management > Scan Settings > Pre & Post Scan Actions > Create New Action**, and configure the following:
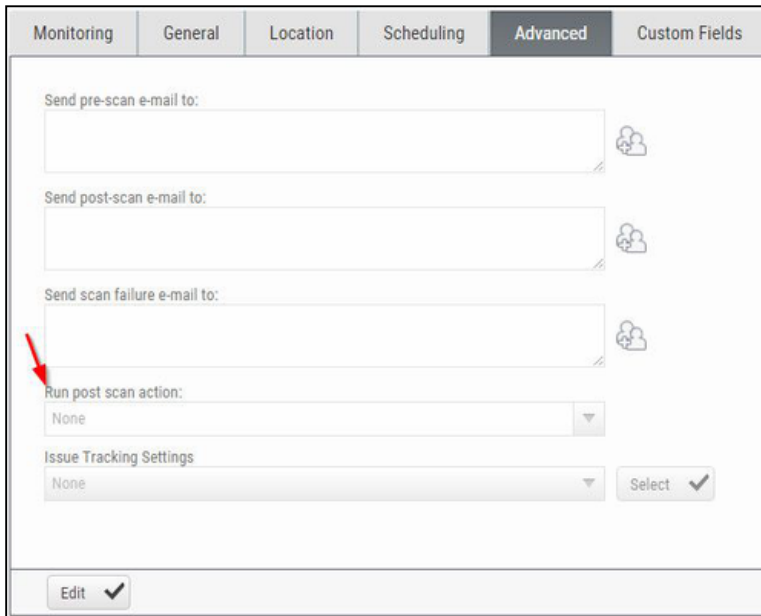
- o **Action Type: Pre-scan** or **Post-scan**.
- o **Name:** This will appear in a drop-down list when assigning the actions to a project.
- o **Command:** Use the syntax as required by the executable or select from the list.

> ⓘ |Note that the command should use the same name that is used for the file located in the 'Executables' folder (files present in that folder will show up in the drop-down list), as defined in **Management > Application Settings > General > Executables Folder**.

- o **Arguments:** Enter arguments required by the command.
- o For post-scan actions you can also select whether the scan results should be XML or CSV.

3. Assign the action to a project: In a project's Advanced Actions tab, select an action from the list:

4. Click **Finish**.

Viewing Project Details

To open the projects table, go to **Projects & Scans > Projects**. The Projects window is displayed.

The Projects table lists all the projects that are configured for groups where the logged-on user is a member. You can manage the table.

For a non-Local project (or, for an Incremental scan of a Local project), **Total Scans** counts only scans when the code had changes relative to the previous scan.

For each project, you can view its scans or perform other actions.

Selecting a project in the table displays its details at the bottom of the window:

- The Monitoring tab represents the evolution of the project last 10 scans focusing on the numbers of found vulnerabilities and overall risk.

  o The **Vulnerabilities** chart includes a graph for vulnerabilities of each severity level (High, Medium, Low, and Info). Each graph presents numbers of found vulnerability instances (y axis) for progressive scans by date (x axis).

  o The **Risk Indicator** chart represents each scan result combining quantity and severity of found vulnerability instances.

- The next four tabs are the same as when Creating and Configuring a CxSAST Project. Click **Edit** to change settings; when you're done, click **Update**.

Managing Queries

You can import and export CxSAST code queries as XML files. You can manage sets of queries known as **Presets** to be selected per-project to be used.

In This Section:

- Viewing, Importing, and Exporting Queries
- Managing Query Presets

Viewing, Importing, and Exporting Queries

The **Query Viewer** displays all Checkmarx default queries and custom queries, with their descriptions and source code. You can import and export custom queries as XML files.

To export queries:

1. Go to **Management** > **Scan Settings** > **Query Viewer**:
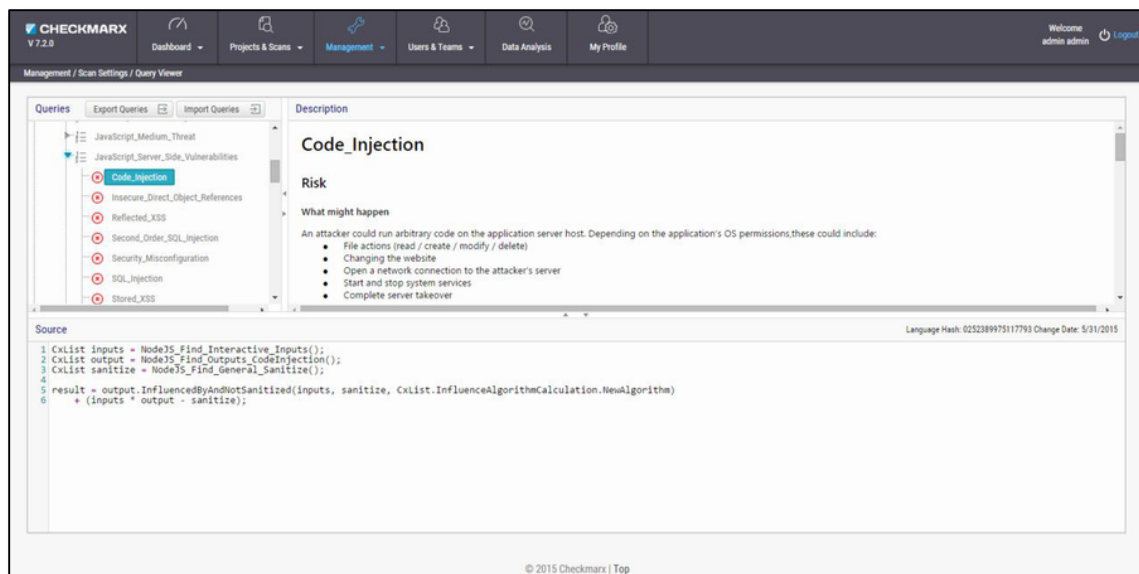
To keep track of changes to query sets, you can select a language (or one of its child items) and view the **Hash** and **Change Date** of the last changes to the language's query set.

To view a query's **Description** and **Source** code, select the query.

2. Select organizational custom queries to be exported.
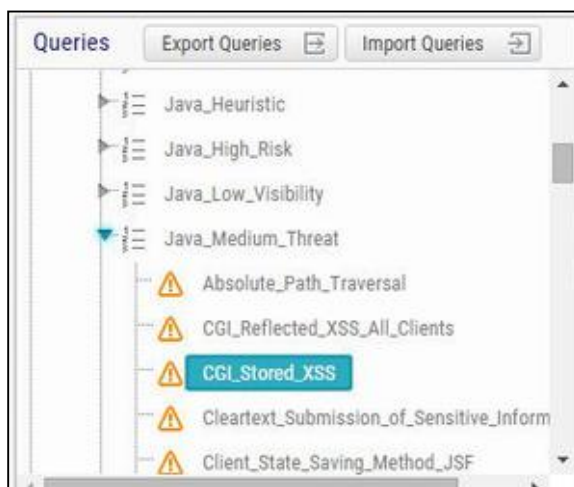
3. Click **Export Queries**.
4. Save the exported XML file.

To import queries:

1. Click **Import Queries**.
2. Select the XML file to be imported.

> ⓘ **If the imported query has the same name as an existing one, the existing query will be overridden.**

Managing Query Presets

Presets are sets of queries that you can select when Creating and Configuring a CxSAST Project to be used when scanning. Predefined presets are provided, and you can configure your own. You can also import and export presets.

To create a new preset:

1. Go to **Management** > **Scan Settings** > **Preset Manager**, and click **Create New Preset**:
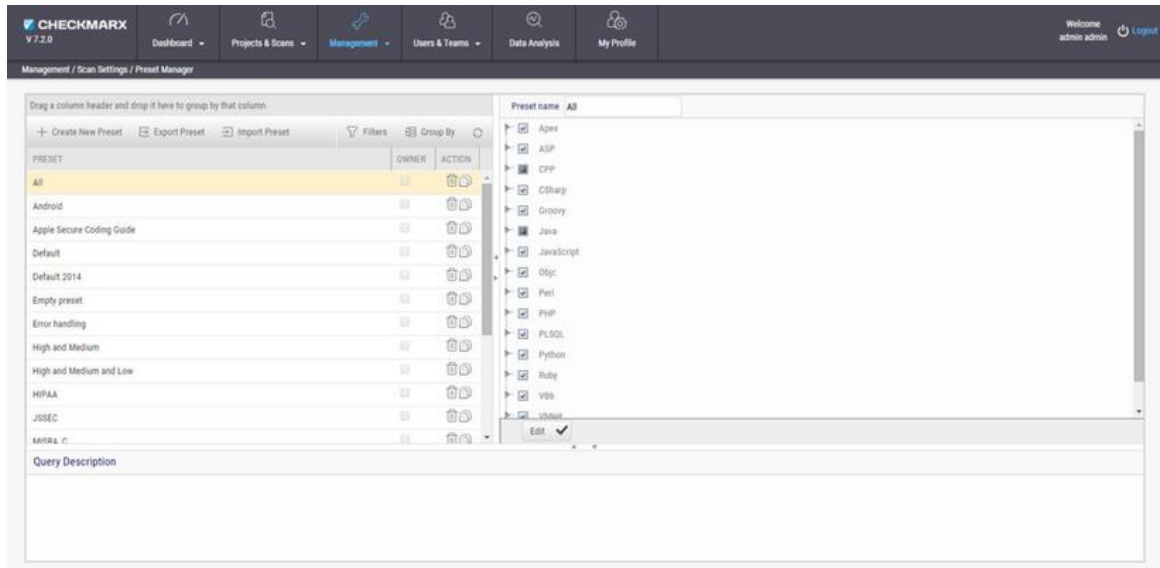
2. Type a preset **Name** and click **OK**.
3. Select a code language.
4. Select queries to be included in the preset.
5. Click **Save**.

To export a preset:

1. Go to **Management** > **Scan Settings**, and select the preset to be exported.
2. Click **Export Preset**.
3. Save the exported XML file.
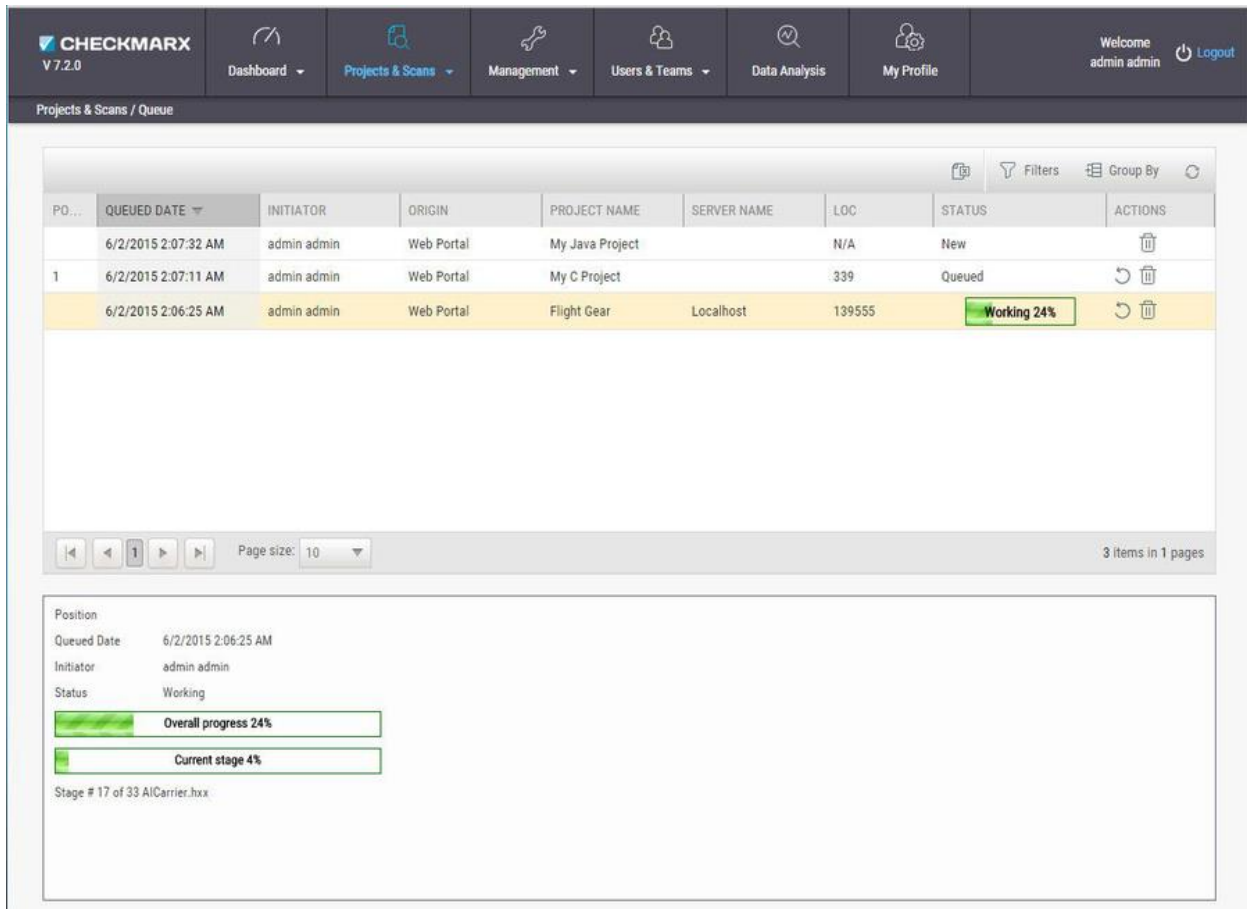
To import a preset:

1. Go to **Management** > **Scan Settings**, and click **Import Preset**.
2. Choose the preset XML file to be imported.

> ⓘ   If the imported preset includes a query that has the same name as an existing one, the existing query will be overridden.

The Queue

The Queue is accessed via **Projects & Scans > Queue**. It lists the scan that is currently running and the order in which the following scans will be executed. You can manage the table.

For each scan, the Queue table displays details including Date and time, the initiating user, the originating system, the Server name (the CxEngine server performing the scan), the number of Lines Of Code (LOC), scan status (see below), and available actions (see below).

Click [icon] to postpone a scan. Postpone will stop the current scan and move it to the end of the scan queue. Once the scan gets to the top of the queue, it will start scanning again.

Click [icon] to delete a scan. Delete will remove the current scan from the queue.

Selecting a scan displays its details, and a progress bar indicating the percentage of scan completion, below the table. Once the first query is completed (usually at about 50% of the scan), a summary of partial results appears, with links to the actual results:

In the table, each scan shows one of the following in the **Status** column:

- **Progress bar**: Shows the percentage of scan completion
- **Pending**: Scan request submitted, but still performing preparatory tasks, such as uploading or extracting
- **Queued**: Ready to scan but waiting for system resources
- **Finished**: Completed scans remain in the Queue window for a configurable time period (by default, 10 minutes)
- **Failed**: When the scan fails it disappears from the queue and reappears in the failed scans page in the Dashboard

The Queue window refreshes every minute. If an active scan (showing a progress bar) is selected, the window refreshes every 10 seconds.

⚠ Multiple projects may be run in parallel, assuming the proper license is installed and system resources availability. Each scan requires its own processing core, and 1GB RAM for every 150,000 lines of code. If system resources are in use but will be available, the project is queued; if total system resources are not sufficient for the scan, an error message is displayed.

Scan Results

Contents

- Viewing Results from All Scans
- Scan Result Actions
- Navigating Scan Results
- Scan Results Example
- Generating Scan Results Report
- Comparing Scan Result Sets

Viewing Results from All Scans

In this Section:

- Projects Scan List/Actions
  - Scan List
  - Scan Actions
- All Scans
  - Deleting Scans
  - Comparing Scans

To view scan results, you can view either of the following tables:

- In **Projects & Scans > Projects,** view an individual project scan results.
- In **Projects & Scans > All Scans**, view the results from all scans.
  To see one project scan results using the All Scans table, in the project's row, click **Open Viewer** (🔍).

Projects Scan List/Actions

In **Projects & Scans > Projects**, various scans and action lists are available (see **Creating and Configuring Projects**).

SCANS LIST	ACTIONS
▤	▷ ▷ ⊤ ▯

Scan List	▤	Displays the project in the individual project path, for example, Projects & Scans/View Project Scans/My Java Projects.
Scan Actions	▷ **Full scan**	A scan of the whole project. If the project is configured for a local location, this will require uploading a zip file with the updated source code.
	▷ **Incremental scan**	A scan of only new and modified files since the last previous scan.
⚠ **Incremental scan significantly shortens the scan time, but it is not recommended for projects with significant amounts of changes**		
	⊤ **Branch Project**	The Branch Project operation is similar to copy project, but it copies a different set of properties: Preset, Team and the Last scan from the source project with all results and remarks.
	▯ **Duplicate Project**	Duplicate Project creates a new project based on the setting of an existing one. From the existing project it will copy the following: Preset, Team, Exclusions, Scheduling, Pre-scan emails, Post-scan emails and Scan failure emails.

All Scans

All Scan results appear in a table with each row representing an individual scan result set. You can manage the table, including sorting by **Scan Date**, **Scan Complete** date, **Project Name**, or **Risk Level Score**.

Result sets marked with represent partial results saved by a user from a complete result set.

Each row of the scan results table includes a **Risk Level Score** and a risk indicator bar, showing the overall risk calculation of all vulnerabilities found in this scan. Some of the other columns are:

- **Initiator**: The user who activated the scan
- **Origin**: The system from which the scan was activated
- **LOC**: The number of Lines of Code in the project
- **Team**: Team that the scan is assigned to
- **Server Name**: The CxEngine server that performed the scan
- **Cx Version**: The CxSAST version number at scan time.
- **Comments**: Indicates any comments maintained for the project, for future scans and for instances that continue to be found.
- **Access**: Defines whether the scan is a private scan (not visible to others, but can be viewed by immediate managers) or a public scan.
- **Locked**: Specific scans may be marked as "Locked" to avoid automated purging of important scan data. Locked scans cannot be deleted.
- There are also additional available Actions.

If a scan was initiated for a non-local project (or, for an Incremental scan for a local project) with no code changes since the previous scan, the **Comments** indicate that the scan was not actually performed.

Selecting a scan in the table displays its details at the bottom of the window:

The **Monitoring** tab provides two graphical summaries of found vulnerabilities:

- The **Top 5 High and Medium Vulnerabilities** chart shows the five most common High and Medium vulnerabilities found in this scan.
- The **Risk Indicator** chart represents the correlation between the severity and the quantity of the results.
  - Severity - Axis X (value between 0 and 100) is calculated according to the number of High, Medium and Low severity results
  - Quantity - Axis Y (value between 0 and 100) is calculated according to the number of High, Medium and Low severity results

The **Comments** tab allows you to write comments on the scan results.

Deleting Scans

To delete one or more scans:

1. Select the rows of the requested scans.
2. Click the Delete button.
   A prompt appears, requesting you to confirm the deletion operation.
3. Click **OK**.

If the user does not have the authorization required for deleting scans, no scan will be deleted.

If one or more of the scans is locked, a message similar to the following one appears:
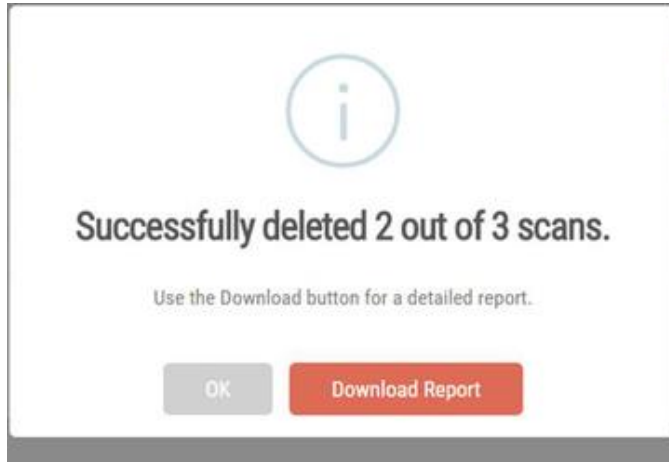
Clicking Download Report downloads the DeleteErrors.csv file, which displays the details of the locked scans.

D	C	B	A	
Error	Scan Start Time	Team Full Path	Project Name	1
The scan is locked. Unlock the scan before deleting it	11/5/2015 2:59:10 PM	CxServer\SP\Company\Users	MyProject	2

Unlocking all scans indicated in the report enables full deletion of the project.

Comparing Scans

Enables Comparing Scan Result Sets.

To compare scans:

In **Projects & Scans > All Scans**, select two scans to compare, and then click the Compare Scans button.

When comparing scans from different projects: "You are about to compare scans from different projects, results might reveal significant differences".

The following information is displayed:

	PREVIOUS SCAN	NEW SCAN
SCAN START	5/19/2015 11:32:23 AM	5/19/2015 11:34:24 AM
SCAN COMPLETE	5/19/2015 11:33:24 AM	5/19/2015 11:35:24 AM
SCAN RISK	15	42
LOC	1338	339
FILES COUNT	4	3
PROJECT NAME	My Java Project	My C Project
TEAM	CxServer	CxServer
PRESET	Default 2014	Default 2014
SCAN TYPE	Full Scan	Full Scan
SOURCE ORIGIN	N/A (Zip File)	N/A (Zip File)
SCAN COMMENT		
ENGINE START TIME	5/19/2015 11:32:23 AM	5/19/2015 11:34:24 AM
ENGINE END TIME	5/19/2015 11:33:24 AM	5/19/2015 11:35:24 AM
SCAN QUEUED TIME	5/19/2015 11:32:02 AM	5/19/2015 11:34:06 AM
TOTAL SCAN TIME	00:01:37.0170000	00:01:31.5060000

SCANNED LANGUAGES

Language	Hash Number	Creation date		Language	Hash Number	Creation date
Java	0113095717627047	5/19/2015		CPP	2074580126042165	5/19/2015

	PREVIOUS SCAN	NEW SCAN
TOTAL RESULTS	50	82
LAST UPDATE	19/05/2015 11:33AM	19/05/2015 11:35AM

	High	Medium	Low	Info	Total
New Issues	3	20	6	53	82
Resolved Issues	23	1	26	0	50
Recurrent Issues	0	0	0	0	0

Results 🔍

Click on the **Results** button in order to see a 'file compare' showing the code differences in each file, grouped by vulnerability/scan result.

Scan Result Actions

In this Section:

- Navigating the All Scans table

Navigating the All Scans table

In the All Scans table you can implement the following scan result actions .

	View Scan Results icon
	Create Report icon
	Open Scan Summary icon
	Download Scan Logs icon

Viewing Scan Summaries

To view the Scan Summary:

In **Projects & Scans > All Scan**, click . The Scan Summary window is displayed.
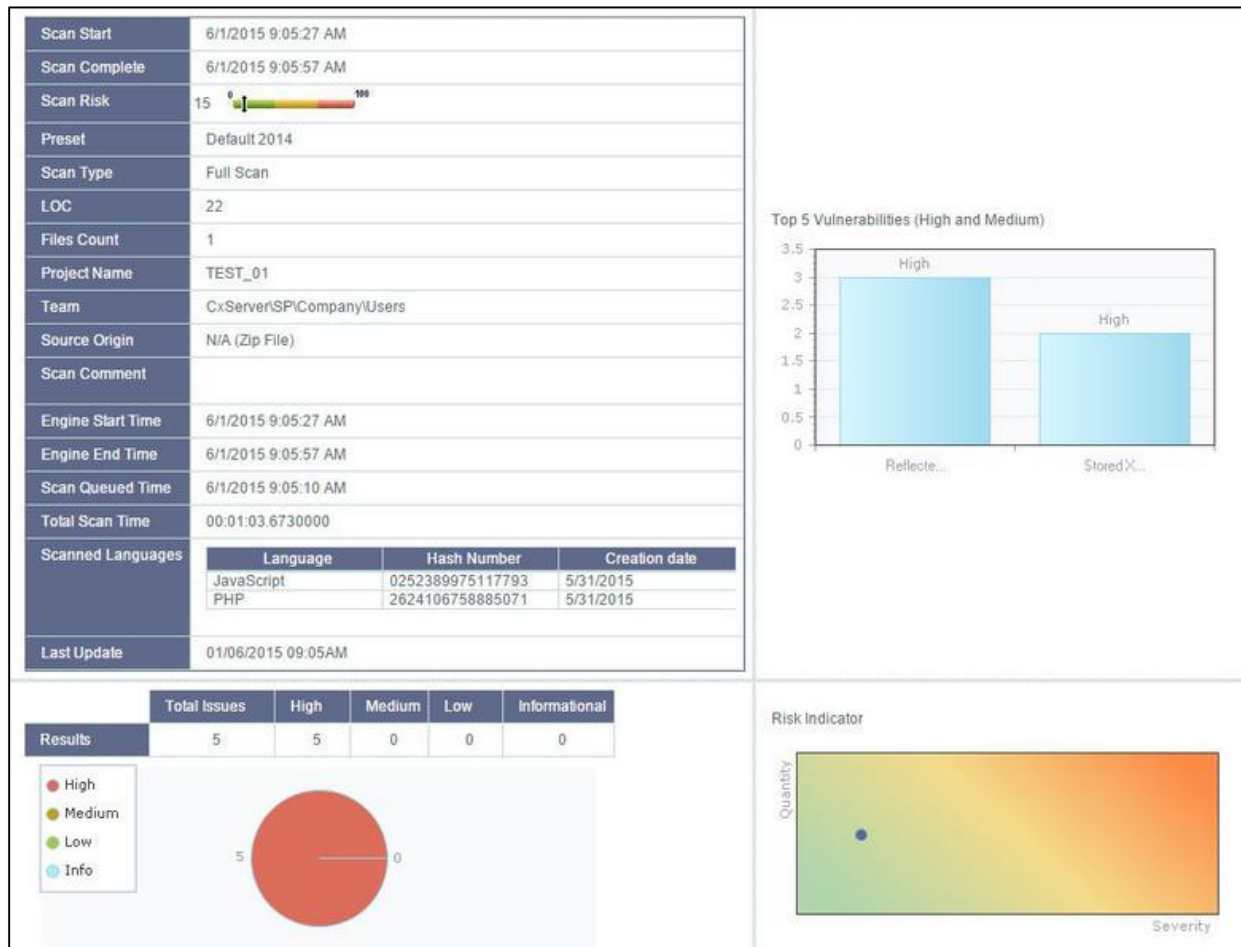
The Scan Summary window includes:
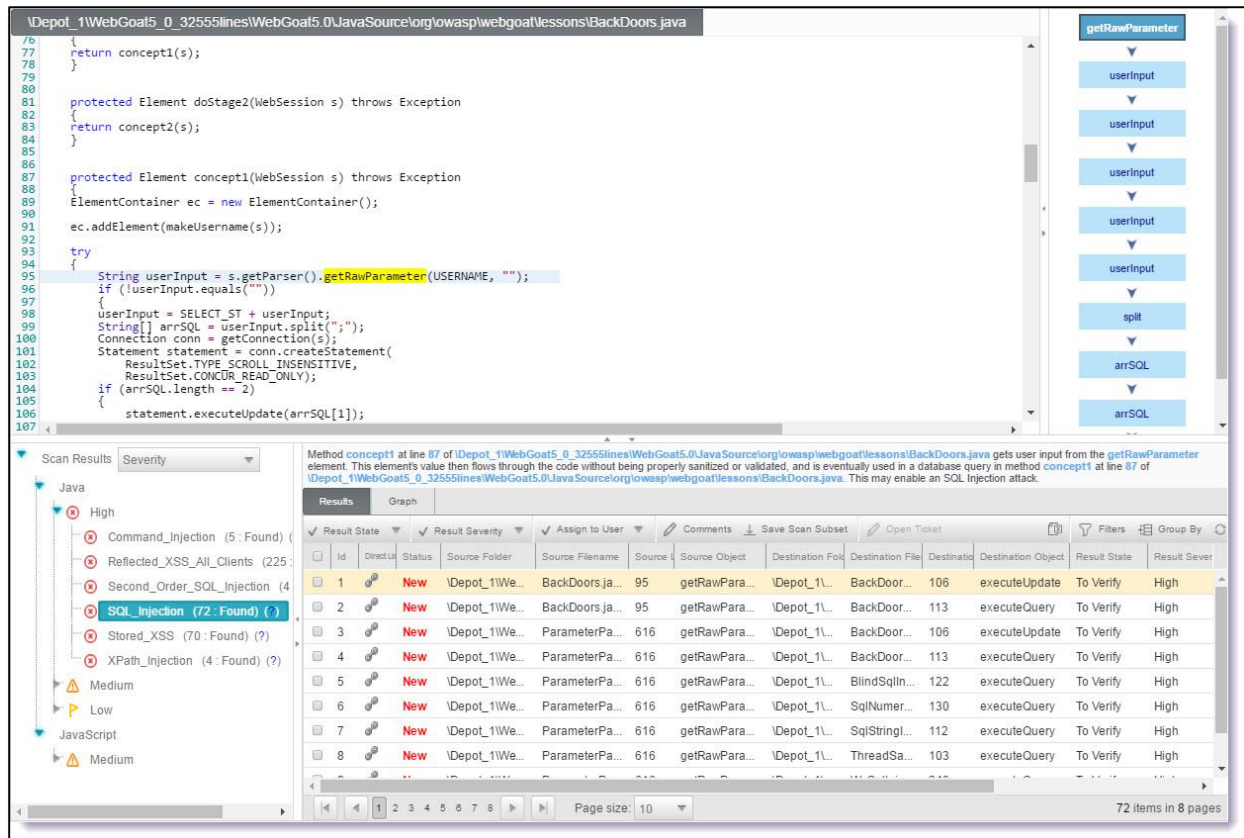
- Scan details table: Shows the scan start and finish dates, risk level, LOC (Lines of Code in project), number of files, preset (query set), source origin, and comment.
- The **Top 5 High and Medium Vulnerabilities** chart shows the five most common high and medium vulnerabilities found in this scan.
- The Pie chart shows the number of found vulnerabilities of each severity level as a percentage of all found vulnerabilities.
- The **Risk Indicator** chart presents the scan status as combination of quantity and severity of found vulnerabilities.

- Download all server logs related to this scan. This action is available to CxSAST Administrators, SP Managers, Company Managers, and Scanners.

Navigating Scan Results

When viewing full **Scan Results** in the web interface, you can interactively navigate through the results:

The interface includes four panes with different levels of information. You can drill down from a comprehensive list all the way down to the actual code elements, by moving through the panes in the following order:

Queries (lower-left pane) - Each item in the list is a specific type of vulnerability for which CxSAST queries the scanned code, with the number of found instances of that vulnerability. The queries are sorted by code language, category, and severity.

Clicking (?) displays comprehensive information about this vulnerability type, including risk details, a description of the cause and mechanism, recommendations for avoiding the vulnerability, and source code examples.

Select a query to view found instances in the **Results** pane:

Results (lower-right pane) - Displays the found instances of the query that is selected in the **Queries** pane in the following two formats:

- **Graph** (right tab in **Results** pane) - Graphical display of first and last code elements of each found instance, with the relationships between them.
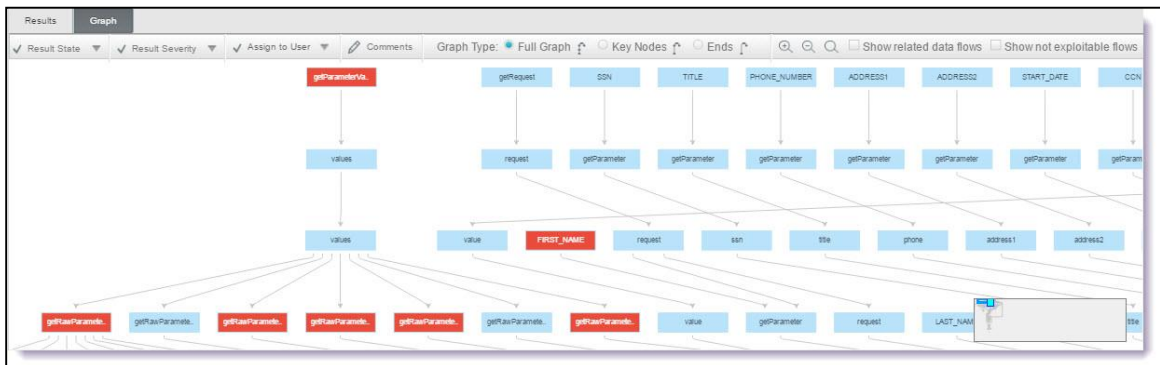
> ⓘ In the CxSAST IDE plugins, the Graph pane displays full paths of the code elements that constitute the found instances, with the relationships between them.

- **Results** (left tab in **Results** pane) - Tabular list of found instances and details. The highlighted instance's code element details appear at the top. You can navigate the results using pagination controls.

Select an instance node (Graph tab) or an instance check-box (Results tab) enabling you to change the following states (user permission dependent):

Results State - useful for disregarding false positives or just for planning what issues to handle

- **To Verify** (default) – instance requires verification (i.e. authorized user)
- **Not Exploitable** – instance has been confirmed as not exploitable (i.e. false positive). Instances defined with this state are not represented in the scan summary, graph, reports or dashboard, etc.

> ⓘ Depending on your user permissions you may not be able to select the "Not Exploitable" state. If this is the case select the "Proposed Not Exploitable" state and then escalate the instance to an authorized user for confirmation.

- **Proposed Not Exploitable** – instance has been proposed as not exploitable (i.e. potential false positive). Instances defined with this state are represented in the scan summary, graph, reports or dashboard, etc. until such a time that the state is changed to "Not Exploitable"
- **Confirmed** – instance has been confirmed as exploitable and requires handling
- **Urgent** – instance has been confirmed as exploitable and requires urgent handling

> ⓘ It is also possible to customize result states to your own preferences. Contact Checkmarx customer support for more information.

Severity (High, Medium, Low and Info) - useful for defining the priority level of the selected issue.

> ⓘ When the state of an instance is changed (i.e. to Not Exploitable), all other instances with same similarity ID are automatically marked with the newly changed state. A popup window is displayed (if enabled) listing all the affected instances including the project name, scan date and a direct link to the affected instance.

**Assign to User** - useful for planning who should handle the selected issue.

Click **Comments** to add a comment to an instance. This metadata is maintained for the project when performing future scans and for instances that continue to be found.

Click **Save Scan Subset** for selected instances to appear in the results list as an independent result set.

Click the link to obtain a URL to this results interface with the instance immediately selected.
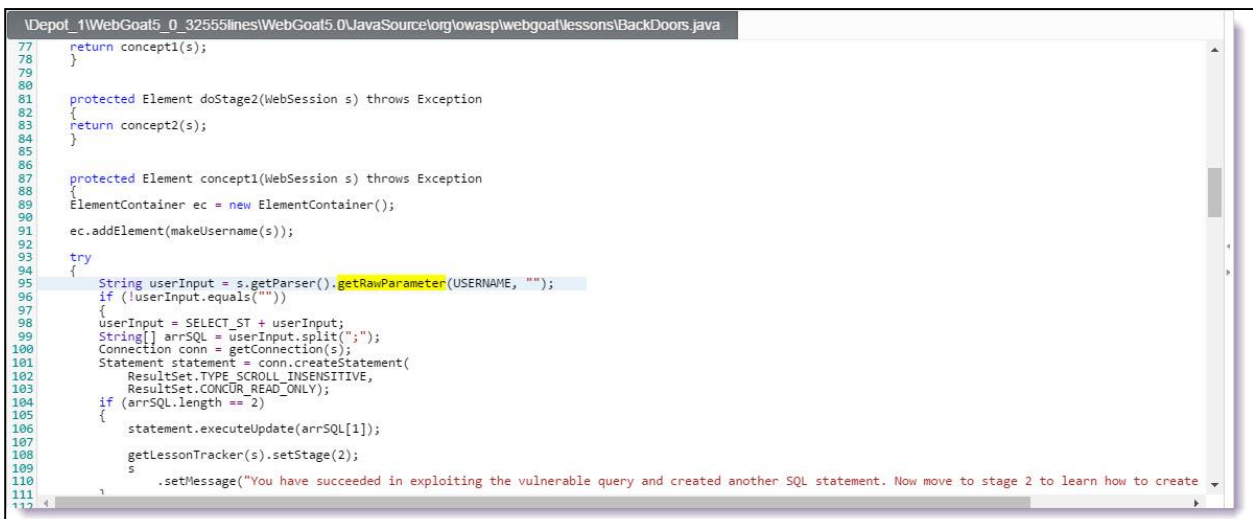
Path (upper-right pane) - Displays the full path of code elements that constitute the vulnerability instance that is selected in the **Results** pane. This path represents the full attack vector for the vulnerability instance.

Select an instance in the **Results** pane (**Results** or **Graph** tab) and view its attack vector in the **Path** pane.
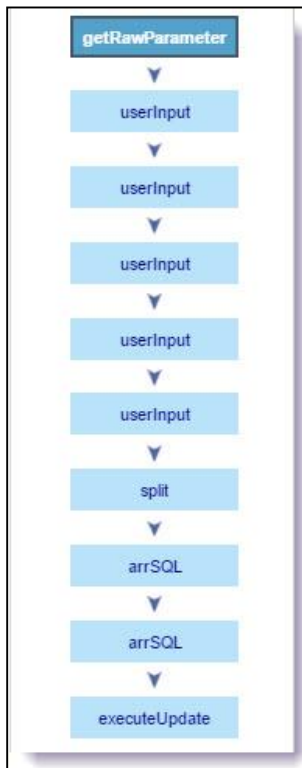
Select a code element in the **Path** pane to view it in its code context, in the **Source Code** pane (see below).

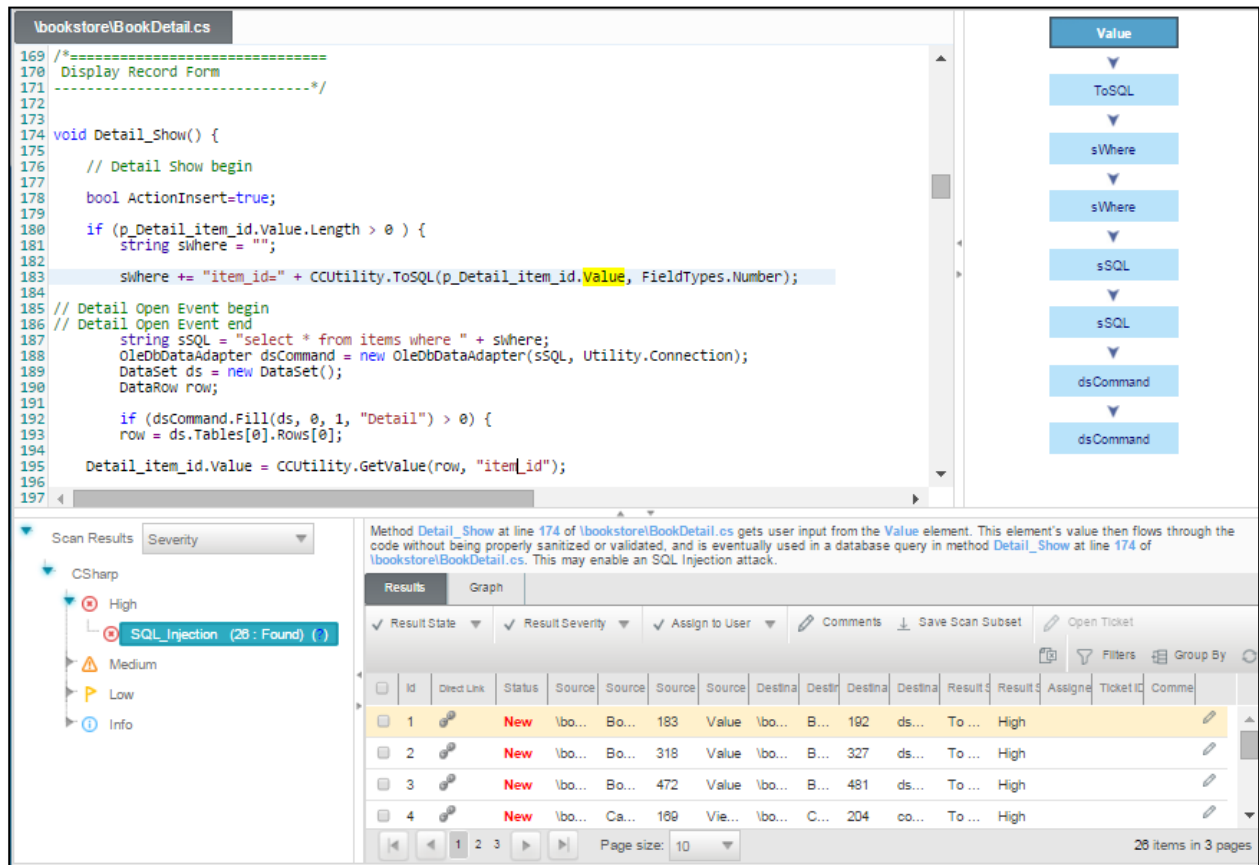**Source Code** (upper-left pane): Displays the source code files.

Highlights the code line containing the element that is selected in the **Path** pane.

> ⓘ When using the CxSAST IDE plugins, you can immediately fix the code in place!
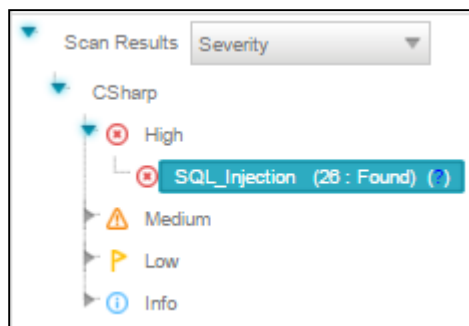
Scan Results Example

The following is an example of scan results showing an SQL Injection vulnerability.

The **Queries** pane (bottom-left) shows that 26 instances of the **SQL_Injection** vulnerability were found:

Clicking **(?)** displays full general information for SQL Injection, including recommendations and code examples. Briefly, an SQL Injection vulnerability exists when user input is used in the syntax of an SQL query. Since those inputs could be interpreted as SQL syntax rather than user input, a user could manipulate the input in such a way as to alter query logic, potentially bypassing security checks and modifying the database, including execution of system commands.

Selecting a specific instance of the vulnerability in the **Results** pane (bottom, center and right) displays the instance's code details at the top of the pane, and displays the path of component code elements in the **Path** pane (top-right). The Path pane shows all the code elements leading from the user input to the SQL query. Selecting each element in turn displays and highlights the element in the code context in the **Source Code** pane (top, left and center). The vulnerability needs to be eliminated somewhere along that path.

The drop-down list **Severity** allows selecting one of the methods listed below for displaying the detected vulnerabilities: by This estimation is based on various factors, such as the likelihood of the vulnerability to be exploited for security attack and the estimated impact of the attack.

- Severity - the severity of application security risk, namely: the estimated associated risk to the business if the path the vulnerability provides through your application is exploited. Possible values are: High, Medium, Low.

- Custom - a user-defined method for rating the security levels*.*

- PCI - displays the vulnerabilities that belong to categories of the PCI (Payment Card Industry). All vulnerabilities that do not fall into any of the PCI categories are grouped under **Uncategorized.**

- OWASP Top 10 2013 - displays the vulnerabilities belonging to categories (A1 to A10) that appear in the list of the 10 most serious risks, as determined by the Open Web Application Security Project (OWASP). All vulnerabilities that do not fall into any of the OWASP Top 10 2013 categories are grouped under **Uncategorized.**

Note: Using the Custom method requires integrating the user's severity rating method with Checkmarx system. For details, contact Checkmarx support team.

The images below show the Severity drop-down list opened after selecting PCI and OWASP for the first and second image, respectively.
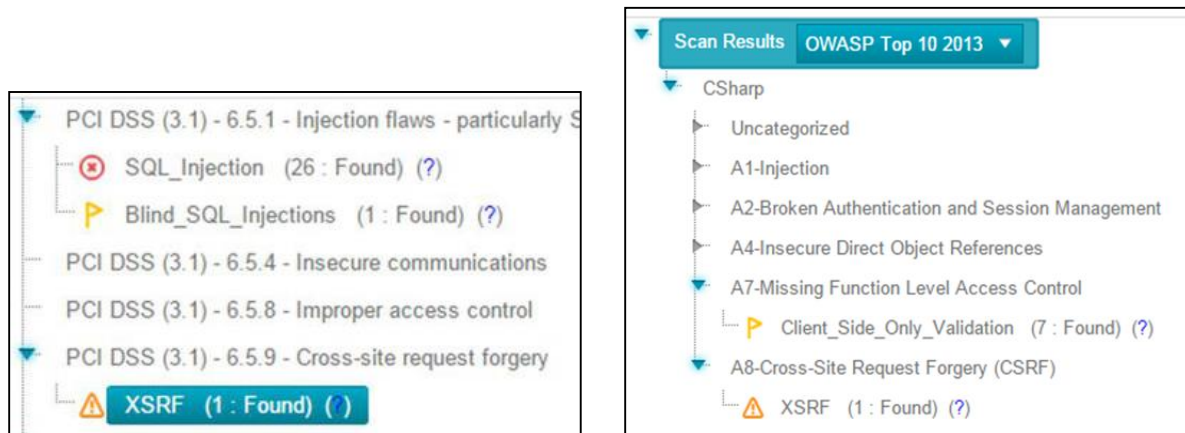
Generating Scan Result Reports

You can generate a report containing detailed scan results, in any of the following formats:

- PDF (default)
- RTF
- CSV
- XML

To generate a report:

1. In the All Scans table (for all projects or for an individual project), click [icon] .

2. Filter results in the generated report and report file format:

3. By default, all categories are selected to be included in the report. To customize the category groups:

   a. Go to the relevant group under the Categories section.

   b. Click the group to expand it.

   c. Clear the vulnerabilities that you do not want to display in the report, as shown below.

If these changes are only relevant for a specific need and do not need to be saved as a different template, click Generate to generate the report (see below). Otherwise, follow the procedure below to save the modifications you make as an updated report template.

To change the report template:

1. Select **Change template** and click **Next**.
2. Select which details should be presented on the report cover page and in the report itself, and what details to show for each result:

3. Select the check-box *Save as default* to save the modified template as a default.
4. Click Back and review all settings you defined. In the example shown below, several changes have been made in the settings.
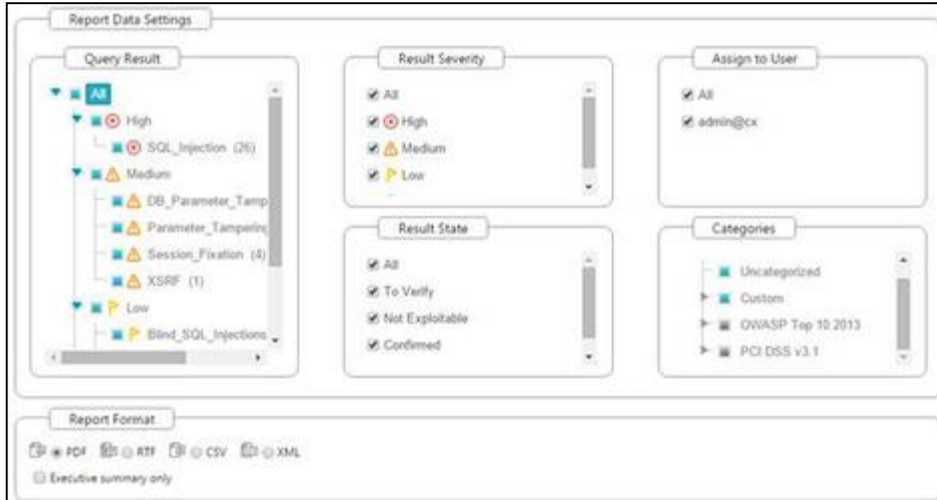
5. Click **Generate Report**.

The exclusions you made are displayed on the Filter Setting section at the beginning of the PDF file, as shown below. Parameters that were selected to be displayed will appear in the report even if none of these parameters (for example, OWASP A-6 category) was detected in the scan, in which case they will appear with the count "0".

The OWASP and PCI summary sections in the scan report include a column named Best Fix Locations, which indicates the number of locations in the flow map that have been found as the best locations to fix the issues that belong to the selected category (for example, A1-Injection). The Best fixed location is an absolute number that cannot be filtered and always displays all of the values. As a result, it is quite probable that while in effect the number of vulnerabilities far exceeds the number of best fix locations for a specified category (for example, 8000 and 600 respectively), the filtered report may display 350 issues and 300 best fix locations.

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Buisness Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	72	27
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	2	2
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	1	1
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	190	19
A9-Using Components with Known Vulnerabilities	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

Scan Summary - PCI DSS v3.1

Further details and elaboration about vulnerabilities and risks can be found at: PCI DSS v3.1

| Category	Issues Found	Best Fix Locations
PCI DSS (3.1) – 3.0 - Protect stored cardholder data	0	0
PCI DSS (3.1) – 3.2 - Don`t store sensitive authentication data after authorization	0	0
PCI DSS (3.1) – 3.4 - Render PAN unreadable anywhere it is stored	0	0
PCI DSS (3.1) – 3.6 - Encryption of key-management cardholder data with cryptographic keys	0	0
PCI DSS (3.1) – 4.0 - Encrypt transmission of cardholder data	0	0
PCI DSS (3.1) – 4.1 - Use strong cryptography and security protocols	0	0
PCI DSS (3.1) – 6.2 - Install critical security patches within one month of release	0	0
PCI DSS (3.1) – 6.3 - Secure authentication and logging	50	62
PCI DSS (3.1) – 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.1) – 6.5.2 - Buffer overflows	0	0
PCI DSS (3.1) – 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.1) – 6.5.4 - Insecure communications	0	0
PCI DSS (3.1) – 6.5.5 - Improper error handling	50	62
PCI DSS (3.1) – 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.1) – 6.5.8 - Improper access control	0	0
PCI DSS (3.1) – 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.1) – 6.5.10 - Broken authentication and session management	7	7

Comparing Scan Result Sets

You can now compare the results of two scans in separate projects. CxSAST provides a summary of differences, and an interactive interface similar to the interface for results of single scan.

To view a comparison, select two rows in the table and click **Compare Scans**.

The following message is displayed when comparing scans from different projects: "You are about to compare scans from different projects, results might reveal significant differences"
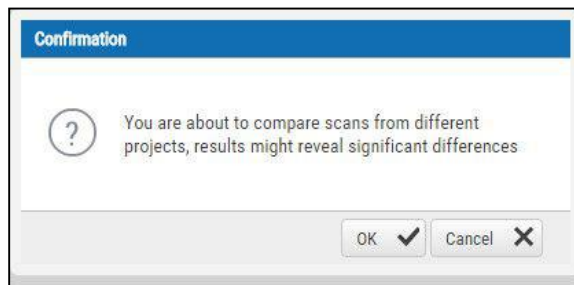
A comparison summary is displayed:
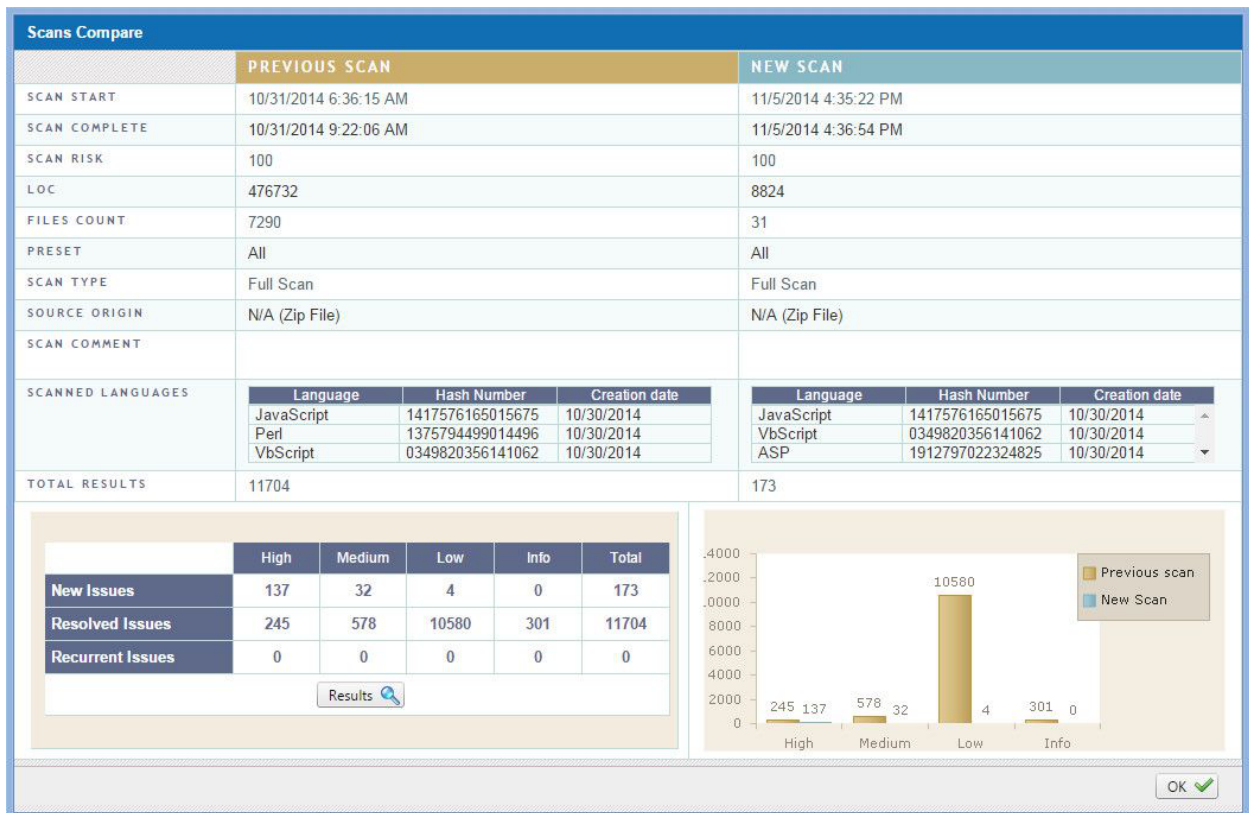
The comparison summary includes:

- The scan details table, showing the scan start and finish dates, risk levels, LOC (Lines of Code scanned), number of files, query set, source code origin, comments, code language details (including unique identifier and date of last change to the language queries), and total vulnerabilities found.

- The bottom-left table displays changes from the earlier scan to the newer one, in number of issues of each severity level:

  o **New Issues**: Issues that were found only in the newer scan

  o **Resolved Issues**: Issues that were found only in the older scan

  o **Recurring Issues**: Issues that were found in both scans

- The bottom-right chart graphically compares the number of found vulnerabilities in both scans, for each severity level.

To view a code comparison, at the bottom-left of the above summary window, click **Results**. A code comparison is displayed:

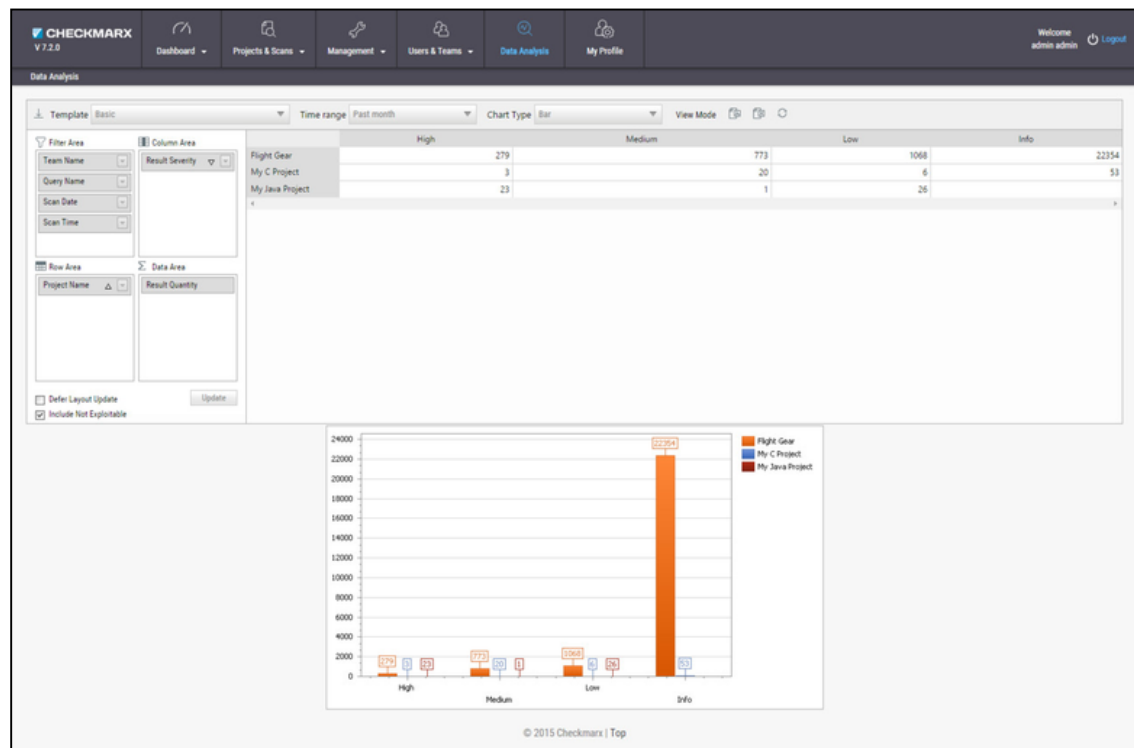# Dashboard Analysis

In This Section:

- Dashboard Menu
- Data Analysis

Data Analysis

The Data Analysis page displays a summary analysis of multiple projects. The data can be presented in several predefined configurations, and you can create your own tables. To view the data analysis window:

1. Click **Data Analysis** . The Data Analysis window is displayed.

In **Template**, select one of the following table configurations:

- **Project Status:** Displays data for most recent projects
- **Last Month's Scans:** Displays data for projects in the past month with High or Medium severity
- **Last week OWASP Top 10:** Displays all projects last week results for OWASP Top 10 queries.
- **Basic:** Create a pivot table from scratch. Drag and drop the relevant tab from Filter area to Column, Row or Data area

Filter parameters by selecting **Defer Layout Update** to disable filtering.

Decide whether to **Include** result instances that have been marked as **Not Exploitable**.

2. Use the top bar to alter the **Chart Type**, **View Mode** or to **Export** the chart and the table to PDF or Excel file.
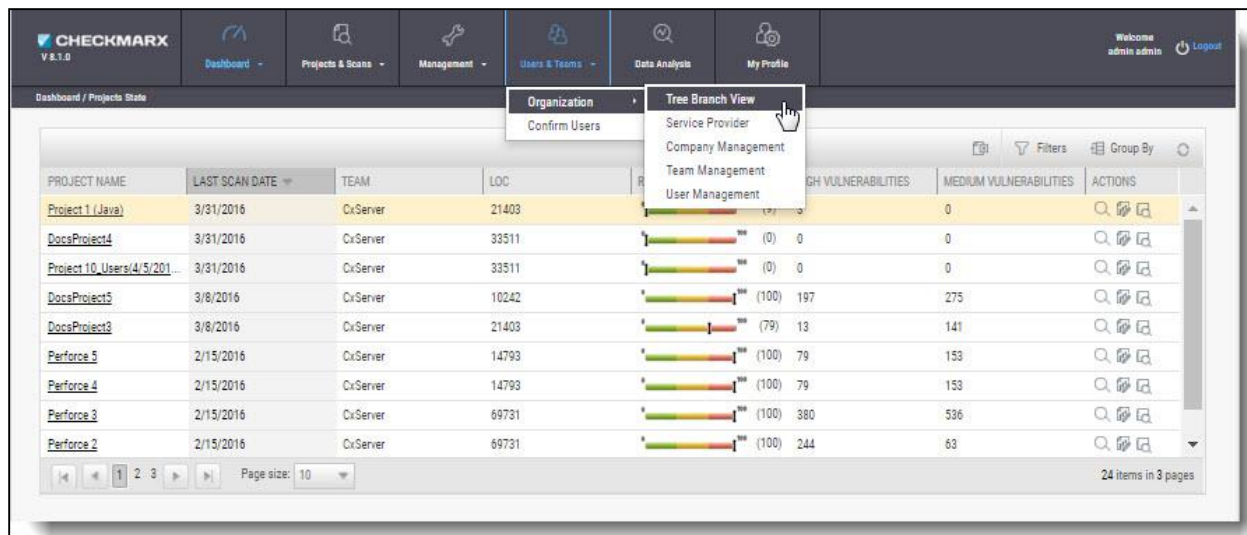

To save a custom table as a template, click **Save**.

User Administration

In This Section:

- Role and Permission Overview
- Creating and Managing User Accounts
- Managing the Organizational Hierarchy

In **Users & Teams > Organization** menu, you can add, edit and delete users and roles in the system.

The Users & Teams menu includes the following options:

- **Organization**: Add, edit and delete roles of the system at the various organizational levels.
  - ○ **Tree Branch View** - View the organizational tree (upper window), and create new service providers and new users (lower window).
  - ○ **Service Provider** - View service provider list (upper window), and create service provider companies, new teams, and new users, and view service provider details (lower window).
  - ○ **Company Management** - View company list (upper window), and create new teams and new users and view company details (lower window).
  - ○ **Team Management** - View team list (upper window), and add new users to the team and view team details (lower window).
  - ○ **User Management** - Create new user (upper window), and manage account details (lower window).
- **Confirm Users**: Confirm users enrolled to the system at various authorization/organization levels.

Role and Permission Overview

The availability of CxSAST projects and their associated scan results depends on project configuration, and on users' permissions as defined by their CxSAST roles. CxSAST roles also determine permissions for user management.

A CxSAST user can have one of the following CxSAST roles:

- Regular **Users** belong to one or more Teams, and have one of the following roles:
  - **Scanners** can create projects for their own team, and scan and view results of their Team's existing projects.
  - **Reviewers** can view scan results of projects created for their Team, but cannot create projects or scan existing projects.
- **Company Manager**: Can create and manage projects for any of the teams in the Company, create and manage the Company's Teams and Users. Company manager can also be defined as an Auditor.
- **Service Provider (SP) Manager**: Can create and manage projects for any of the teams in the SP's Companies, and create and manage the SP's Companies, Teams, and Users.
- **Server Manager**: The default admin user account is the Server Manager. The Server Manager has complete permissions for the whole system, including all of the above permissions, and server settings.

This section explains how to create and manage user accounts, and how to manage Teams, Companies, and SPs (see **Managing the Organizational Hierarchy**).

Creating and Managing User Accounts

CxSAST recognizes users with two types of authentication:

- **Directory User**: A user in the Windows Domain, registered with CxSAST. Authentication is managed by the User Directory, e.g. LDAP Server - ActiveDirectoryLdap.
- **Application User**: A user account created and managed only in CxSAST.

Both types of user accounts can be created by a Server Manager, from within the Web Interface. In addition, an Application User account can be created via user registration. All user accounts can be subsequently managed.

To create an account for a Manager (SP or Company), first create a regular user account (Scanner or Reviewer) using either of the two methods, and then set the user to be a Manager.

In This Section:
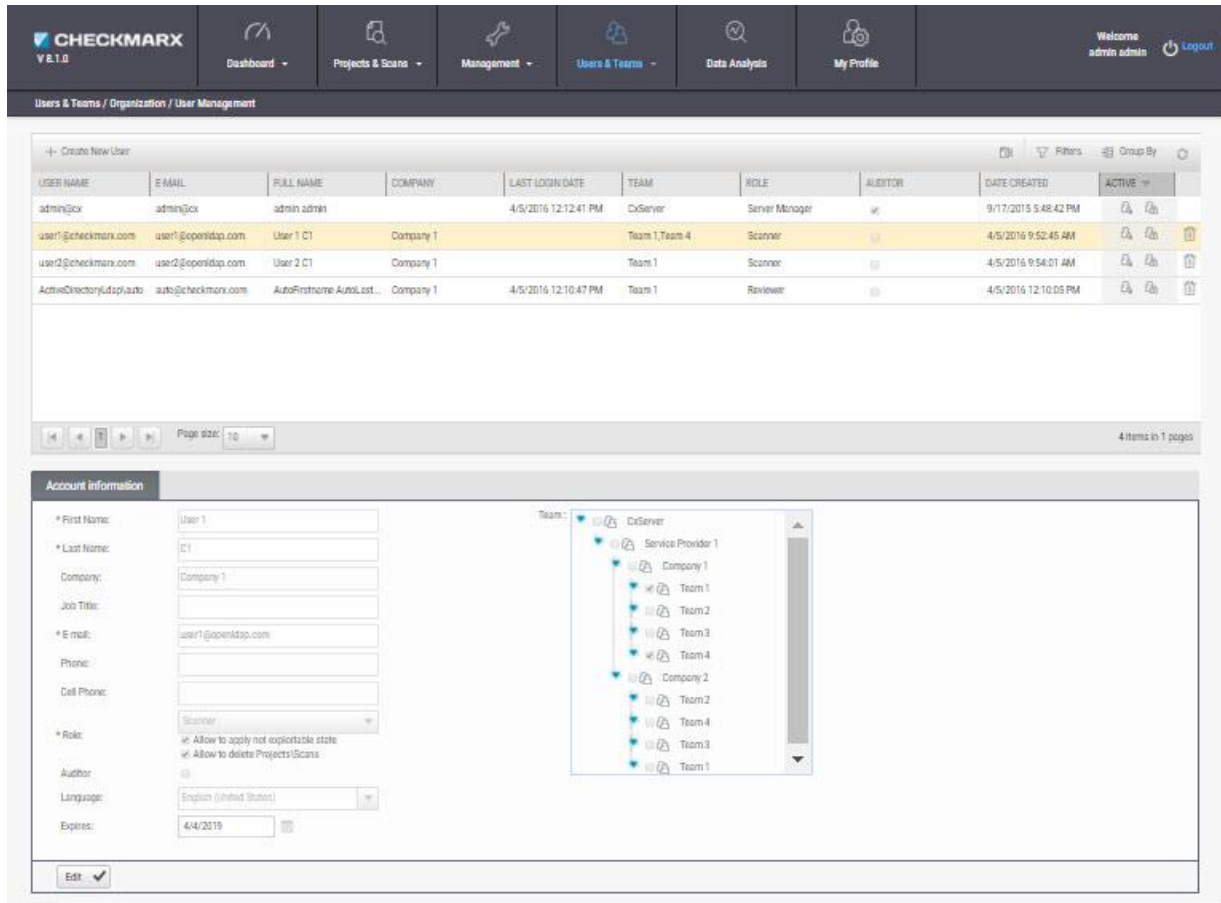
- Creating User Accounts in the Web Interface
- Creating User Accounts via User Registration
- Managing Existing Users

Creating User Accounts in the Web Interface

Regular users may belong to one or more teams and can be defined as a scanner or reviewer. A user may also be turned into a manager at a later stage.

To create a User account:

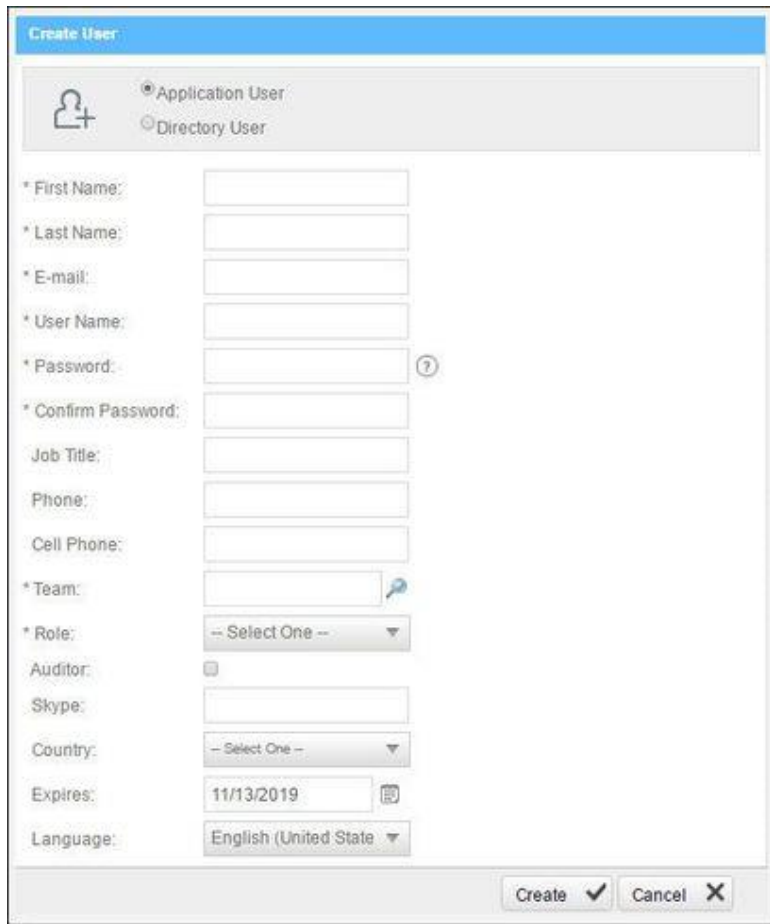Go to **Users & Teams** > **Organization** > **User Management**. The User Management window is displayed.

Click **Create New User**.

Once the Create User Window is displayed, select **Application User** (password is mandatory) or **Directory User** (authentication is managed by the selected Directory, e.g. LDAP / SAML Server).

> ⓘ   The information fields in the Create User window are displayed according to the selected User type.
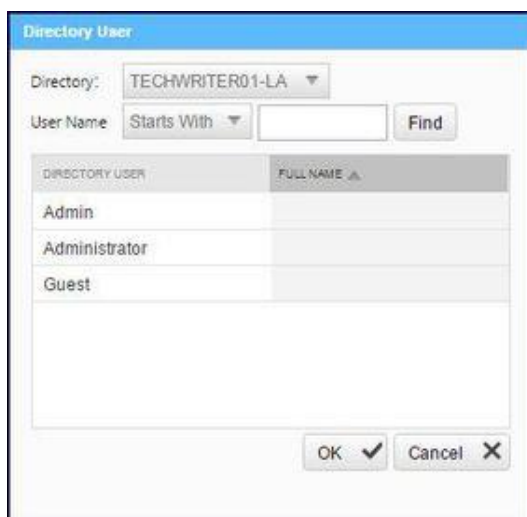
If you selected **Directory User**, the Directory User dialog window is displayed.

Select a **Directory** from the drop-down (e.g. ActiveDirectoryLdap) and click **Find**. All the available Directory Users associated with the selected directory are displayed.
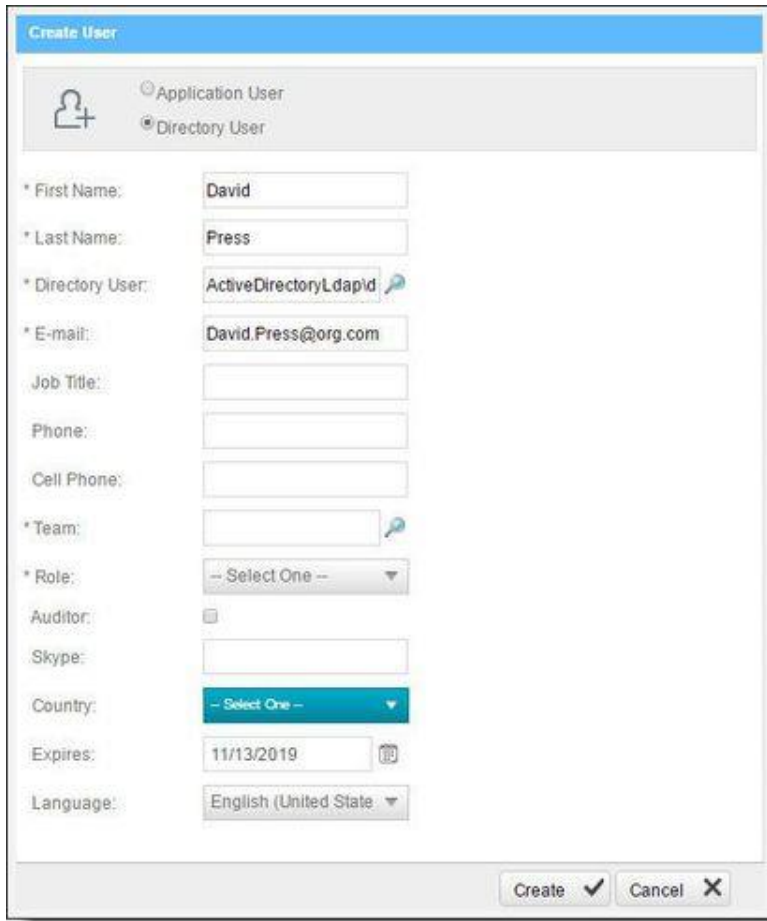
ⓘ If there are no LDAP Directory Users displayed in the Directory User dialog window, check your LDAP connection settings (see **Connection Settings in LDAP Server Management**).

Select a **Directory User** from the list and Click **OK**. Directory User information is automatically filled by the User Directory.

For both user types, fill in the user's details in the available fields (fields marked with * are mandatory):

- **First Name / Last Name** is the user's full name (automatically filled by the User Directory).
- **E-mail** / **User Name** is the user's email address, which is used as the name for logging in (automatically filled by the User Directory).

- For **Team**, click and then drill down the displayed organizational navigation tree to select one or more Teams to which this user will belong. If the user is to be a Company or SP Manager, just select a Team under the Company or SP; User may be turned into a Manager at a later stage.

- **Role** is either **Scanner** or **Reviewer**, at this point. User may be turned into a Manager at a later stage (by managing the Organizational Hierarchy; or, by using Organizational Tree mode).

  - A **Scanner** can delete projects\scans if the checkbox is selected. Select the **Not Exploitable state** checkbox to provide authorization to apply not exploitable state to instances.

  - A **Reviewer** can make changes to the status or severity of found instances if the checkbox is selected.

- **Auditor**: Reviewers can be turned into Auditors. Permissions to use CxAudit.

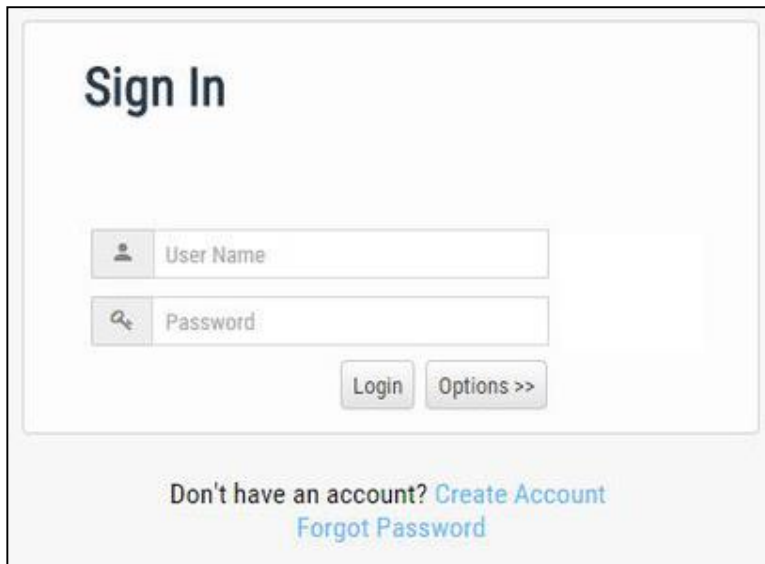- **Language** defines the UI language for each user according to list of supported languages.

Click **Create**.

Creating User Accounts via User Registration

Organizational members can sign up for a user account to be confirmed by their Manager. At sign-up, the user specifies the company, and the user that appears in the CxSAST web interface for confirmation by the Company Manager, SP Manager, or Server Manager. Upon confirmation, the user is notified by email.
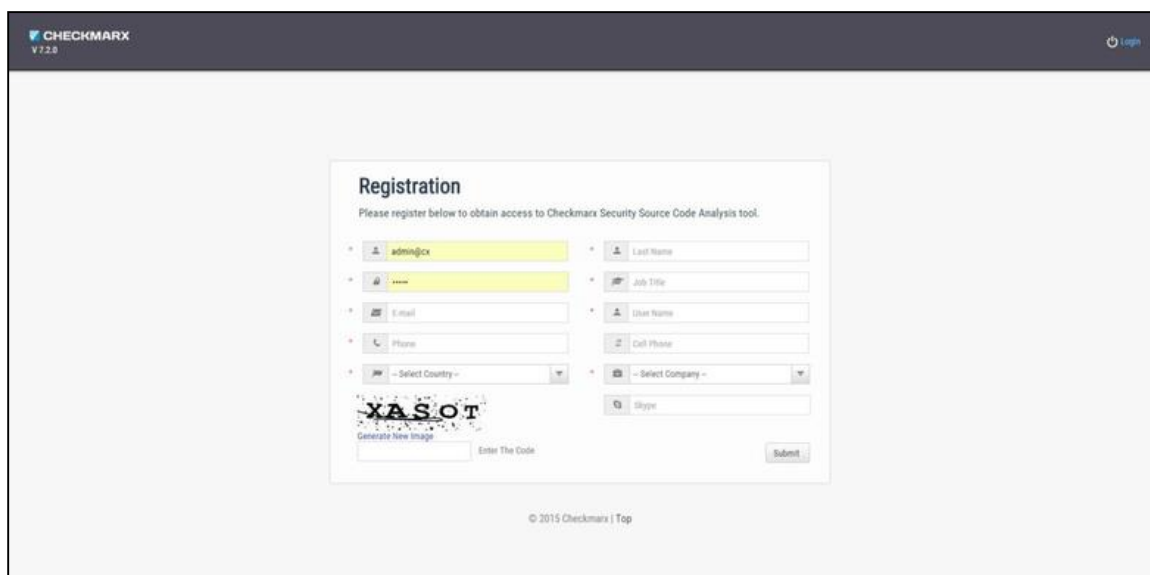
To sign up for a user account:

1. In the CxSAST Sign In, click **Create Account**.

2. In the Create Account window, fill in the personal details. The E-mail will be used as the user name for login.
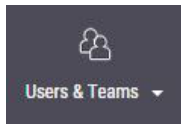
> ⓘ The required password complexity is as follows:
>
> - 9 to 400 characters
> - At least 1 uppercase letter
> - At least 1 lower case letter
> - At least 1 special character
> - At least 1 digit

3. Type the captcha text, and click **Submit**.

The Company, SP, or Server Manager can subsequently confirm the user account.

To confirm a user account:

1. In **Users & Teams** , select **Confirm Users**. The Confirm Users window is displayed.
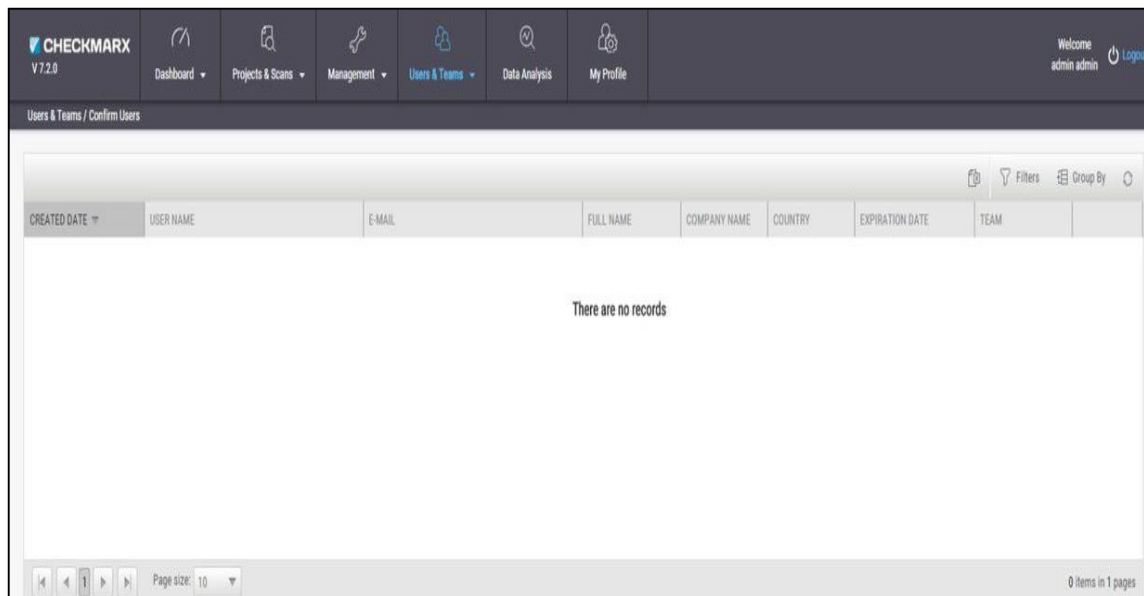
2. In the table, select the user account request to be confirmed.

   You can view additional information about the user by hovering over the ⓘ. You can delete the request.

3. Optionally, change the **Expiration date** and/or **Group** (Team).

4. Click ✔ to confirm the request.

Managing Teams

Regular **Users** belong to one or more Teams and can be defined as **Scanners** (permissions to create projects for their own team, and scan a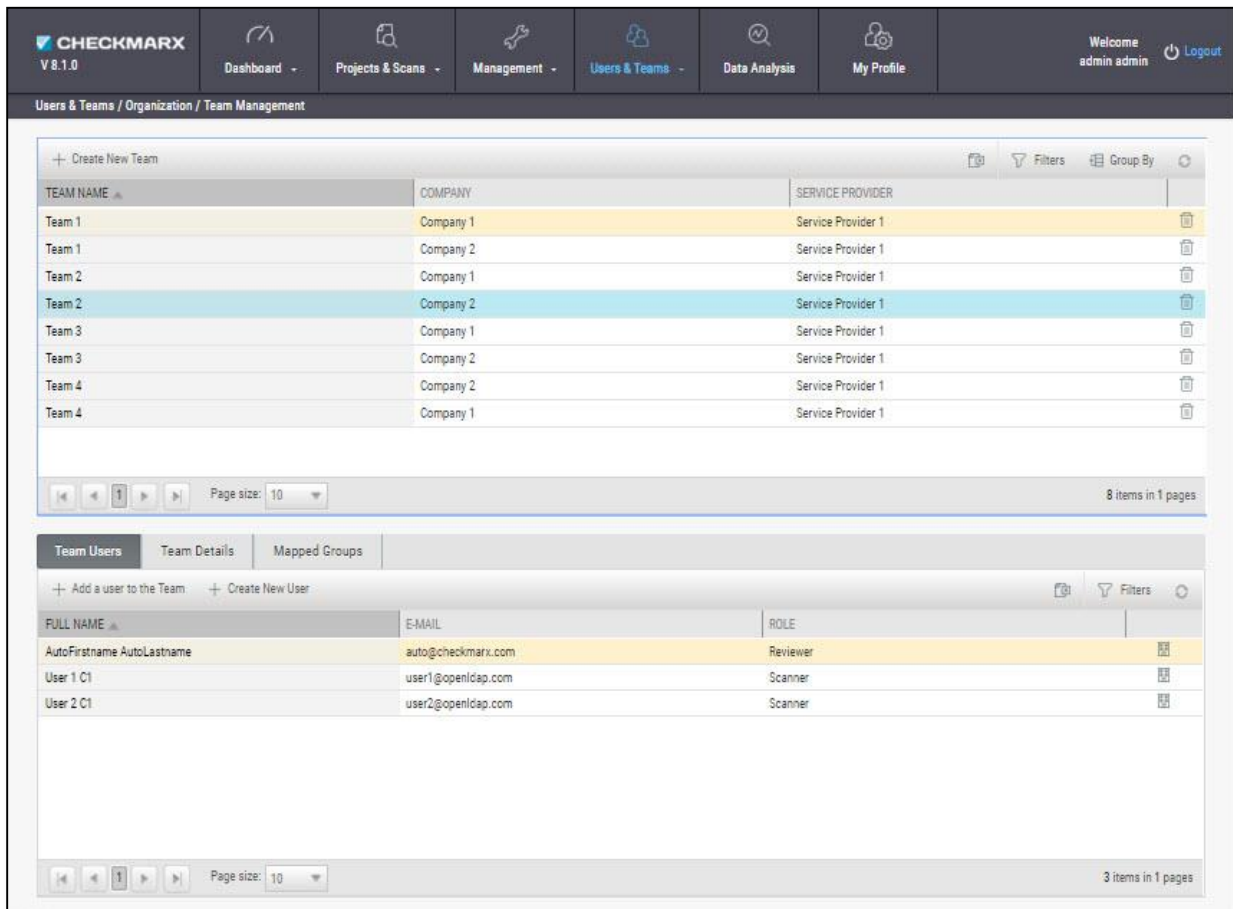nd view results of their Team's existing projects) or **Reviewers** (permissions to view scan results of projects created for their Team, but cannot create projects or scan existing projects).

To manage these Teams:

Go to **Users & Teams > Organization > Team Management**, the Team Management window is displayed.

Creating a Team

To create a new Team:

Click **Create New Team**. The Create New Team window is displayed.
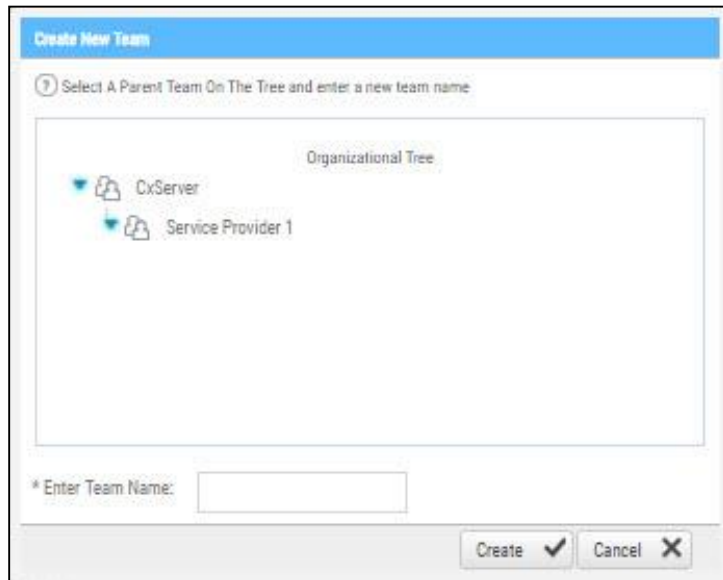
Select a **Parent Company** on the Organizational Tree and enter a new **Team Name** into the field.

Click **Create**. The new Team is displayed in the Team list.
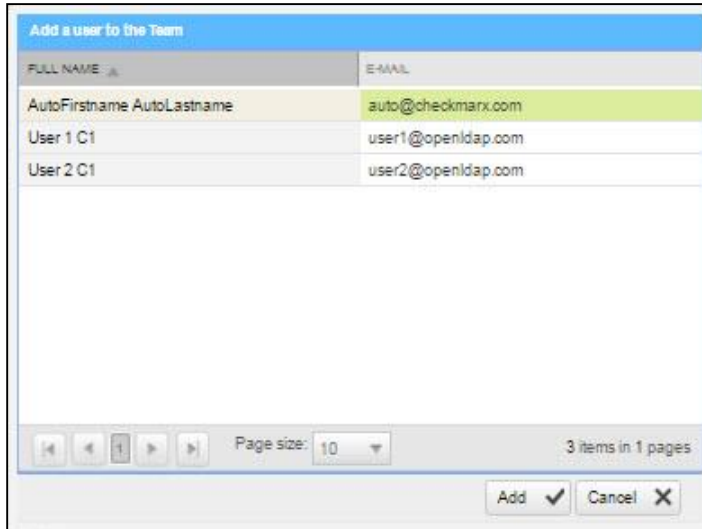
You can now add User to the Team.

Adding a User to a Team

To add a User to a Team:

Select the Team from the Team list.

Click **Add a New User to the Team**. The Add a User to the Team window is displayed.

Select a **User** from the list and click **Add**. The selected user is displayed in the Team Users tab.

> ⓘ   In certain cases you may need to create a new user (see **Creating and Managing User Accounts**).

Click on the Team Details tab to view Team information.

Mapping LDAP Directory User Groups to CxSAST Teams

A Directory User may have been created in an LDAP Directory, unrelated to CxSAST (e.g. LDAP Server - ActiveDirectoryLdap). This Directory User is associated to an LDAP User Group and therefore authentication is managed by the relevant LDAP Sever. In order for the Directory User to login and be visible in CxSAST, the LDAP User Group that the Directory User is associated to needs to be mapped to a CxSAST Team.

To map an LDAP User Group to a CxSAST Team:

Select the **Team** from the Team list and click the **Mapped Groups** tab.

Click **Add Group Mapping**. The Directory Group window is displayed.
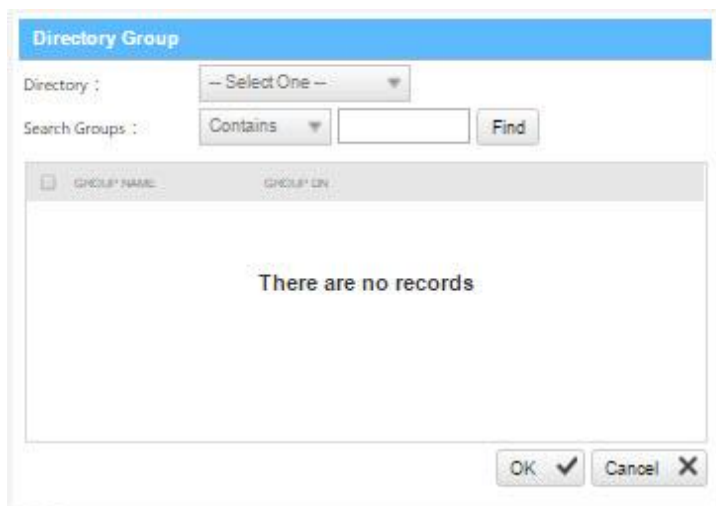
Select an **LDAP Directory** from the drop-down (e.g. ActiveDirectoryLdap) and click **Find**.

Select the **LDAP User Group** from the list (e.g QA) and Click **OK**. The LDAP User Group is displayed in the Mapped Group tab.

From this point on, all LDAP Group Users that login (first time) to CxSAST with their LDAP credentials are automatically created in the CxSAST Team that the LDAP Group User is mapped to. On subsequent logins, the user details and CxSAST Teams will be automatically synchronized.

You can also create LDAP users (see **Creating User Accounts in the Web Interface**).
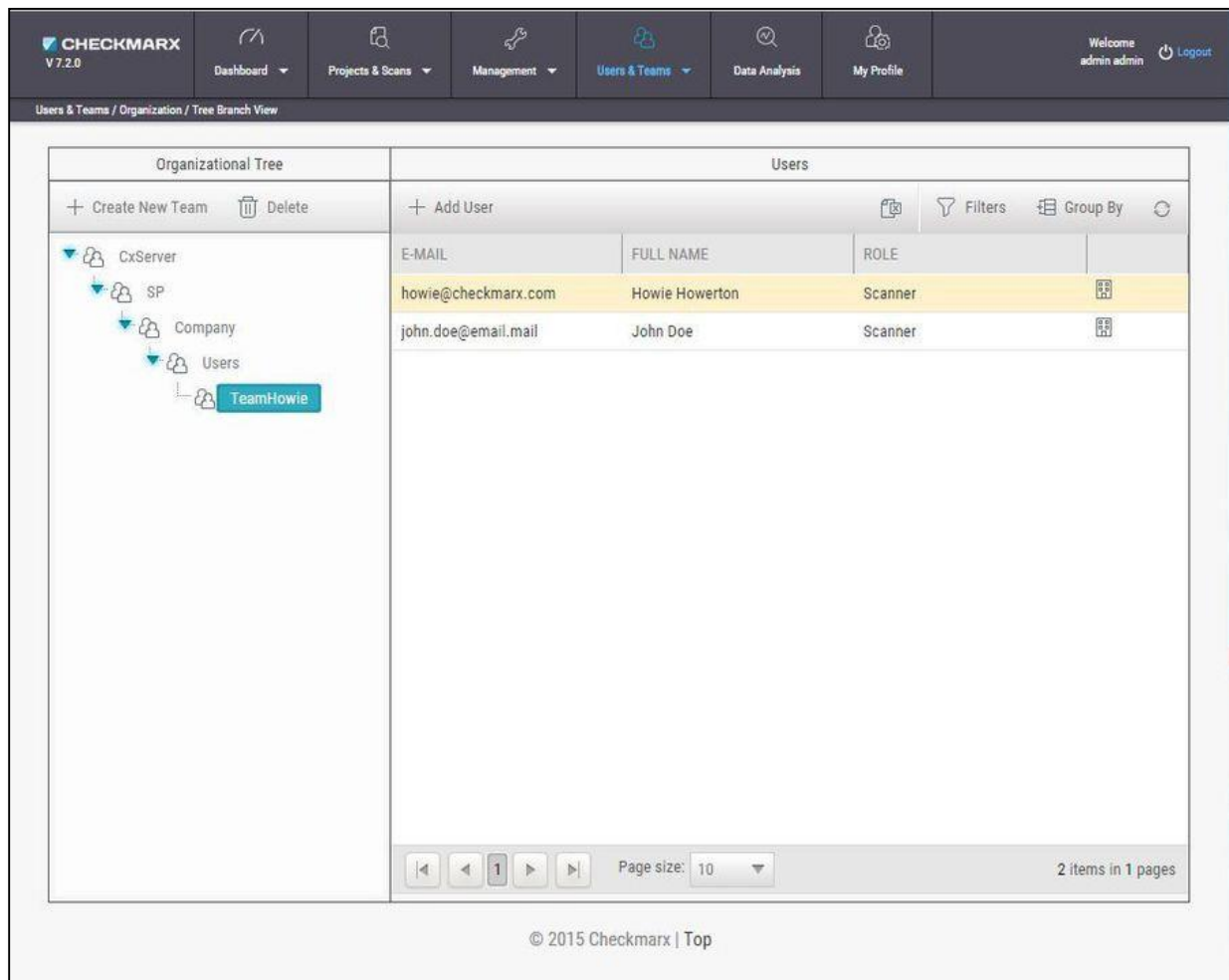
Managing the Organizational Hierarchy

To manage the organizational hierarchy, go to **Users & Teams** > **Organization**.

Available actions depend on the permissions of the logged-in user.

Tree Branch View

Tree Branch View provides a high-level view of the organizational hierarchy.

In Tree Branch View, you can [+ Create New Team] under the selected one. You can [+ Add User] to a Team. You can also drag any team to move it under a different Company or Team (to become a child Team). All the Team's relevant child teams, users, projects, scans, and queries will be moved along with it.

Team Management

Manage various levels of Teams (Teams, Companies, and Service Providers - SPs) in **Team Management**.
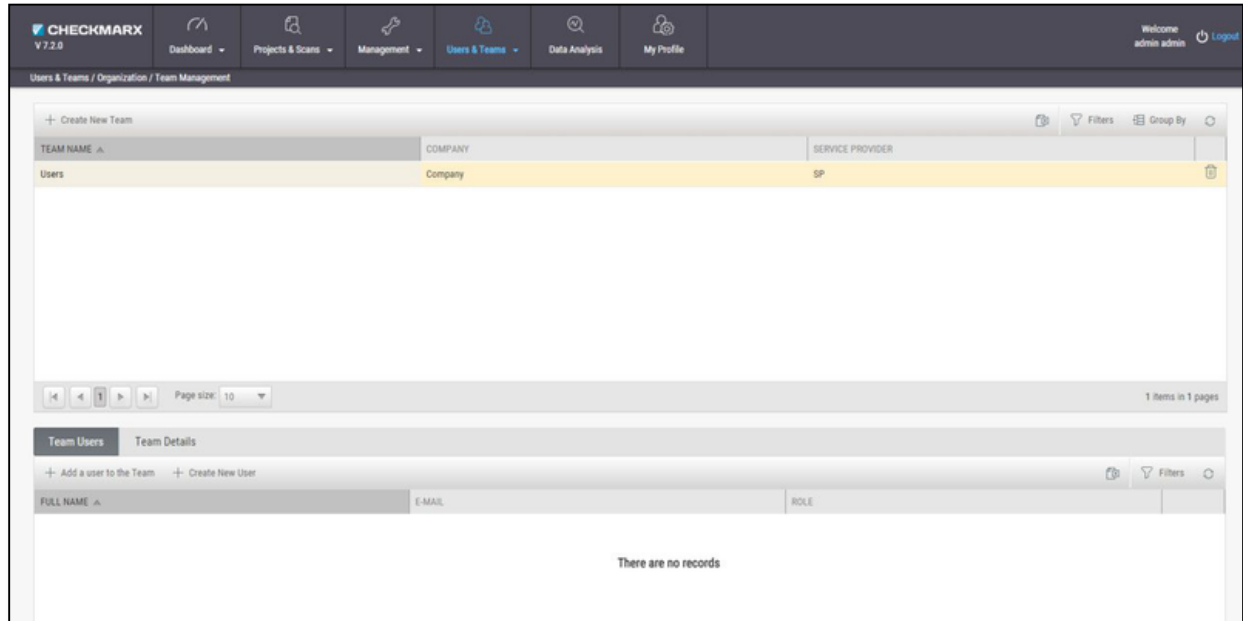
Each team-management window includes a table listing all the existing team of that level. To create a new team at the managed level (for example, in SP Management, to create a new SP), click ⊞ Create New Team . The Create New Team window is displayed.
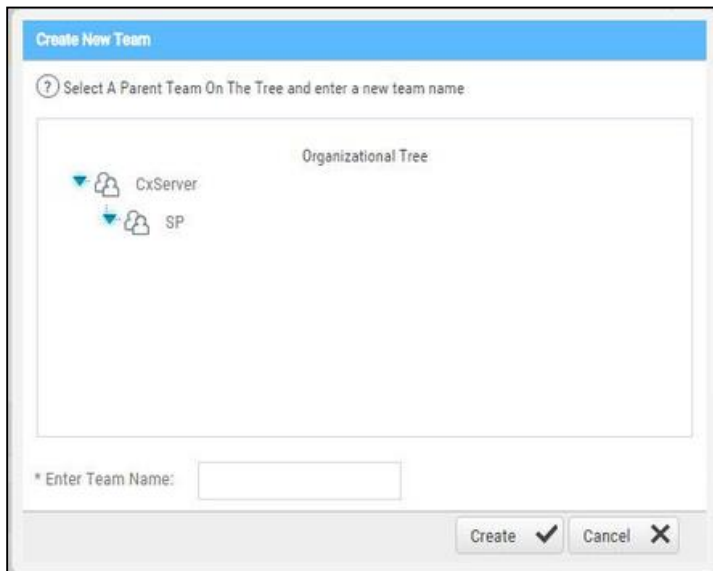
Select a parent group, and type a name for the new group, and click **Create.**
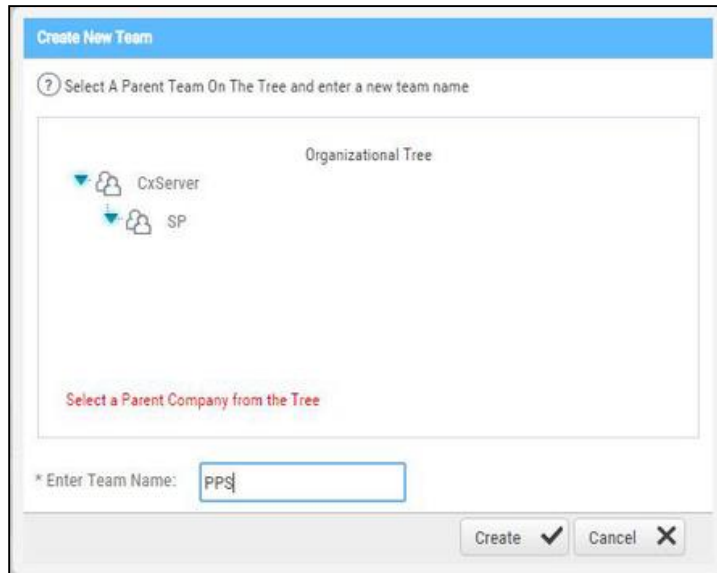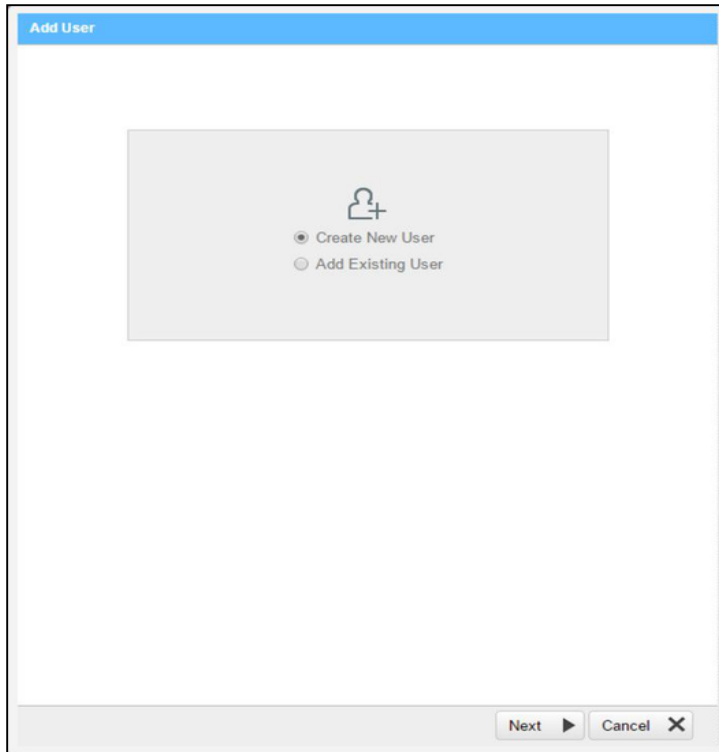
In the Team Management window, click ![Add a user to the Team] to add a new user to the Team. The Add a user to the Team window is displayed.
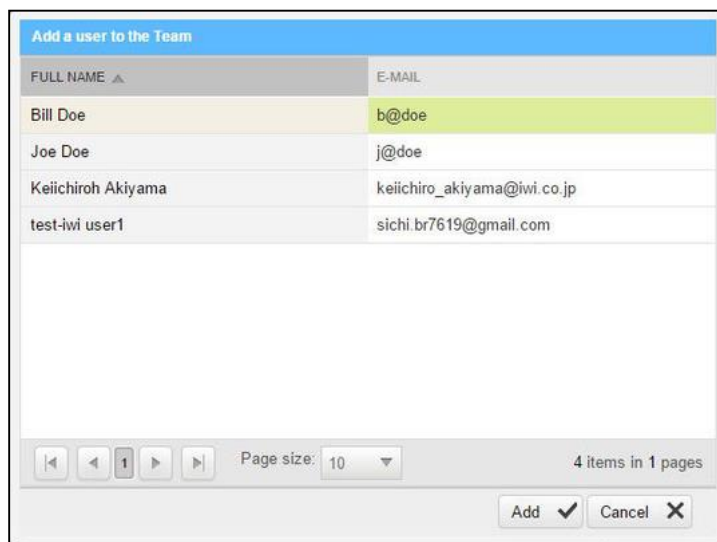
Select a user and click **Add**. The Team member will be added in the Team Users tab.
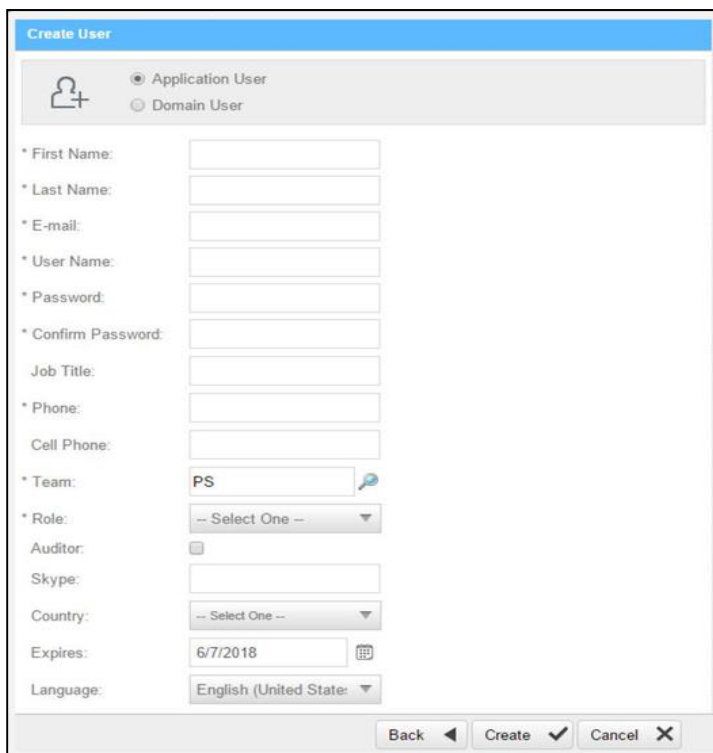
Note: Once the team member has been added to the Team User window they will no longer appear on the list as they can only be added once.

To create a new user, click ![Create New User]. The following window is displayed:

When selecting Create New User, the following window is displayed. Fill in the new user details, and click create.

When selecting Add Existing User, the following window is displayed.
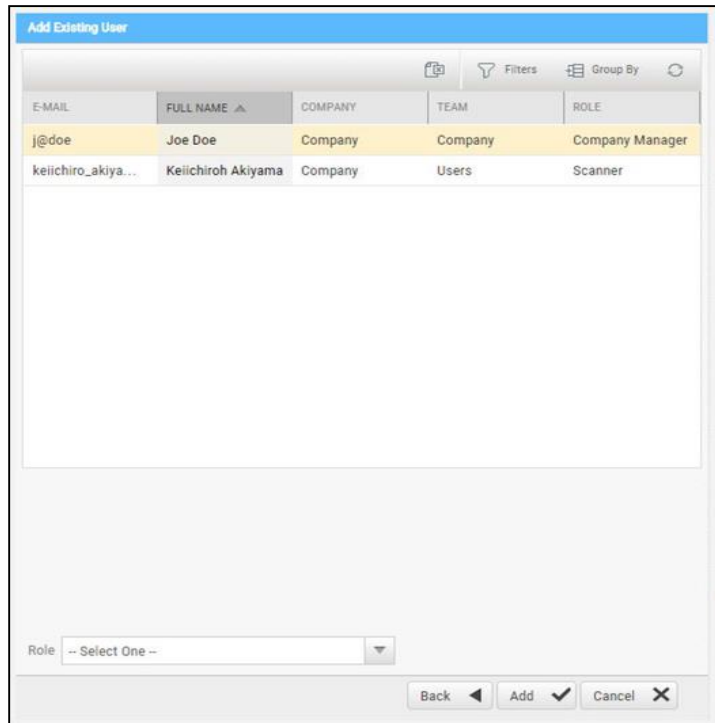
Select the user and click **Add**.

Management Settings

In this section:

- Scan Settings
- Connection Settings.
- Application Settings
- Maintenance Settings
- Managing Custom Fields
- My Profile Settings

Scan Settings

Query Viewer

The **Query Viewer** displays all default queries in CxSAST. A Query is a set of predefined source code used when scanning for vulnerabilities.

To open the **Query Viewer**:

Go to **Management** > **Scan Settings** > **Query Viewer**, . The **Query Viewer** window is displayed.
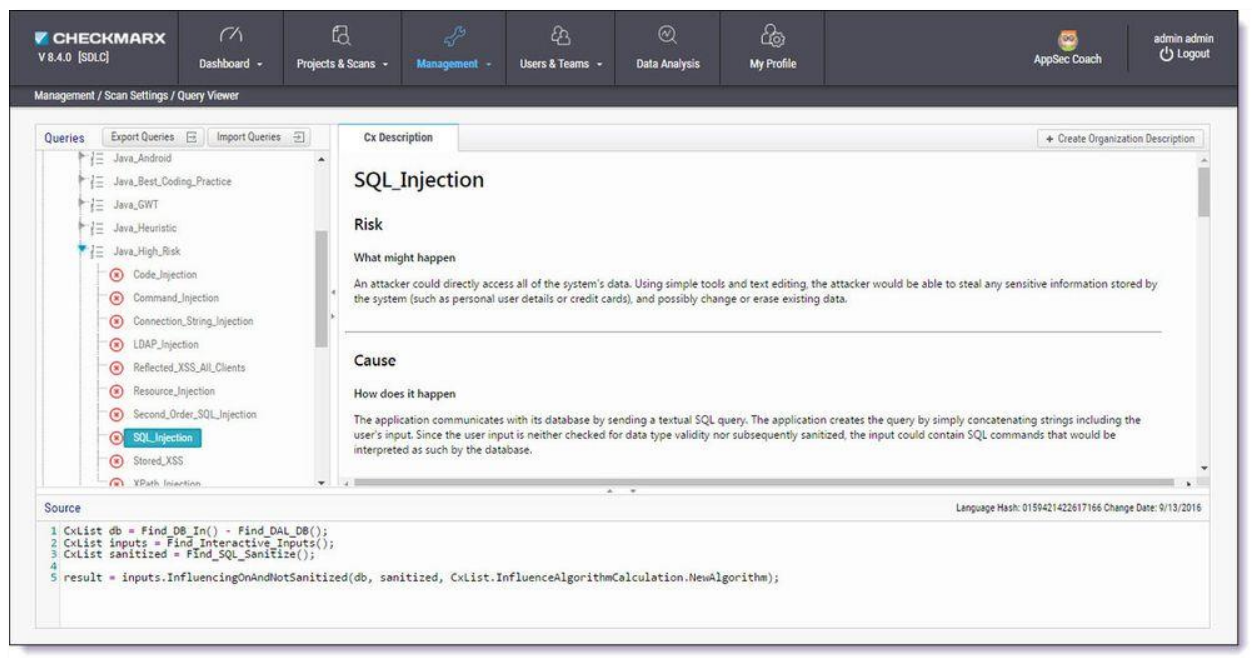
Select a **Query** in the **Queries** pane. A description is provided in the **Description** pane with a full explanation of the risk. The source code for the query is displayed in the **Source** pane at the bottom of the window.

Preset Manager

Presets in CxSAST are predefined sets of queries that can be selected when creating and managing projects. CxSAST provides predefined presets and you can create and configure your own.

To open the **Presets Manager**:

Go to **Management** > **Scan Settings** > **Preset Manager**. The **Preset Manager** window is displayed.

Select a **Preset** in the **Presets** pane. Select a **Query** from the **Queries** pane. A description is provided in the **Description** pane with a full explanation of the risk.

Click **Create New Preset** to create a new preset.

Pre & Post Scan Actions

CxSAST can be configured to perform automatic predefined actions before and after a scan, for example, sending a confirmation email or performing an executable action.

To open **Pre & Post Scan Actions**:

Go to **Management** > **Scan Settings** > **Pre & Post Scan Actions**. The **Pre & Post Scan Actions** window is displayed.

Select an **Action** from the **Actions** pane. The definitions of the selected action are displayed in the **Details** pane at the bottom of the window.
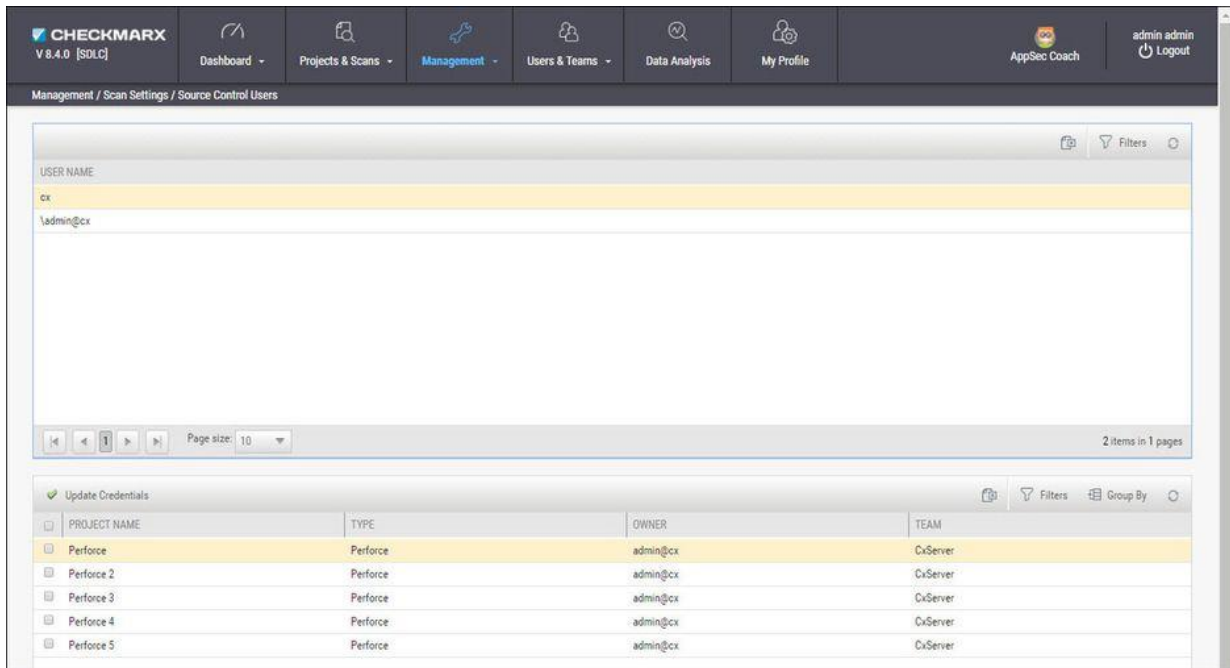
Click **Edit** to update the selected action details.

Source Control Users

CxSAST can be configured to connect to a source code control repository (i.e. TFS, SVN, GIT or Perforce) for creating projects. The **Source Control User** window can be used to view and modify the details of the authorized users that have access to these source code control repositories.

To open **Source Control Users**:

Go to **Management** > **Scan Settings** > **Source Control Users**. The **Source Control User** window is displayed.

Select the **User** from the **Users** pane. The credentials of the selected user are displayed in the **Credentials** pane at the bottom of the window.

Click **Update Credentials** to update the selected user credentials.

Query Viewer

The **Query Viewer** displays all default queries in CxSAST. A Query is a set of predefined source code used when scanning for vulnerabilities. Conventionally descriptions are provided for each query with an explanation of the associated risk, a description of the cause and mechanism, recommendations for avoiding the vulnerability, and source code examples. Custom descriptions can be created to best suit your organizations procedures and best practices, therefore shortening the remediation time for your developers and improving the quality of your code. You can also import and export queries.

To open the **Query Viewer**:

Go to **Management > Scan Settings > Query Viewer**. The **Query Viewer** window is displayed.
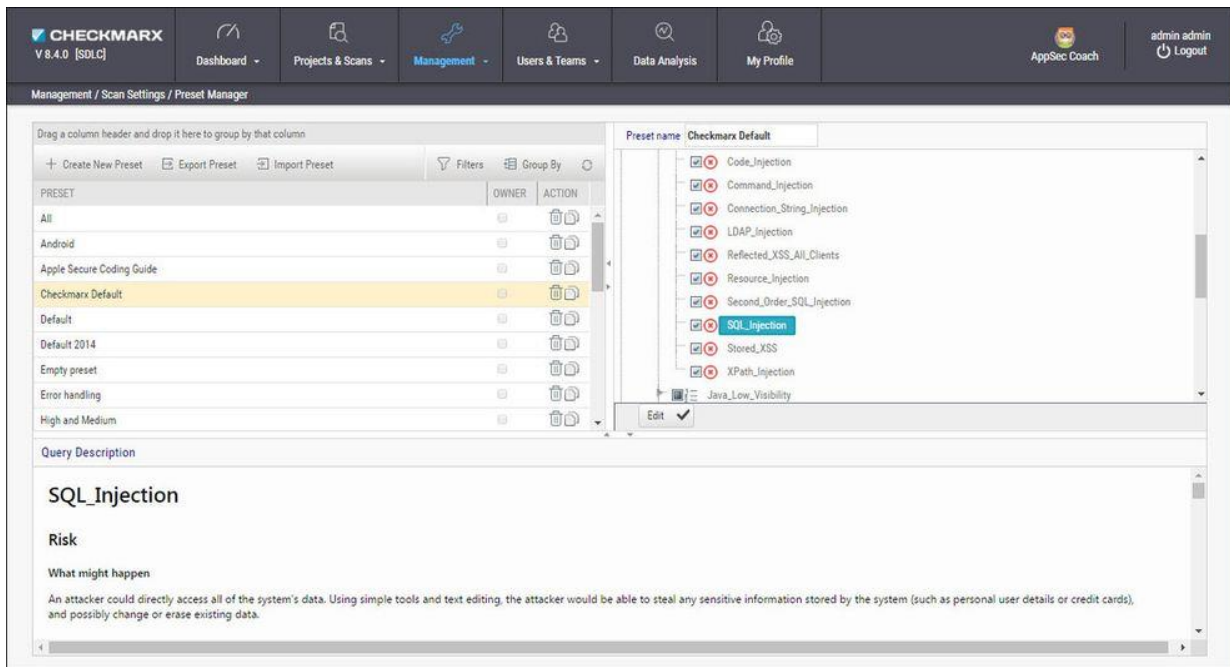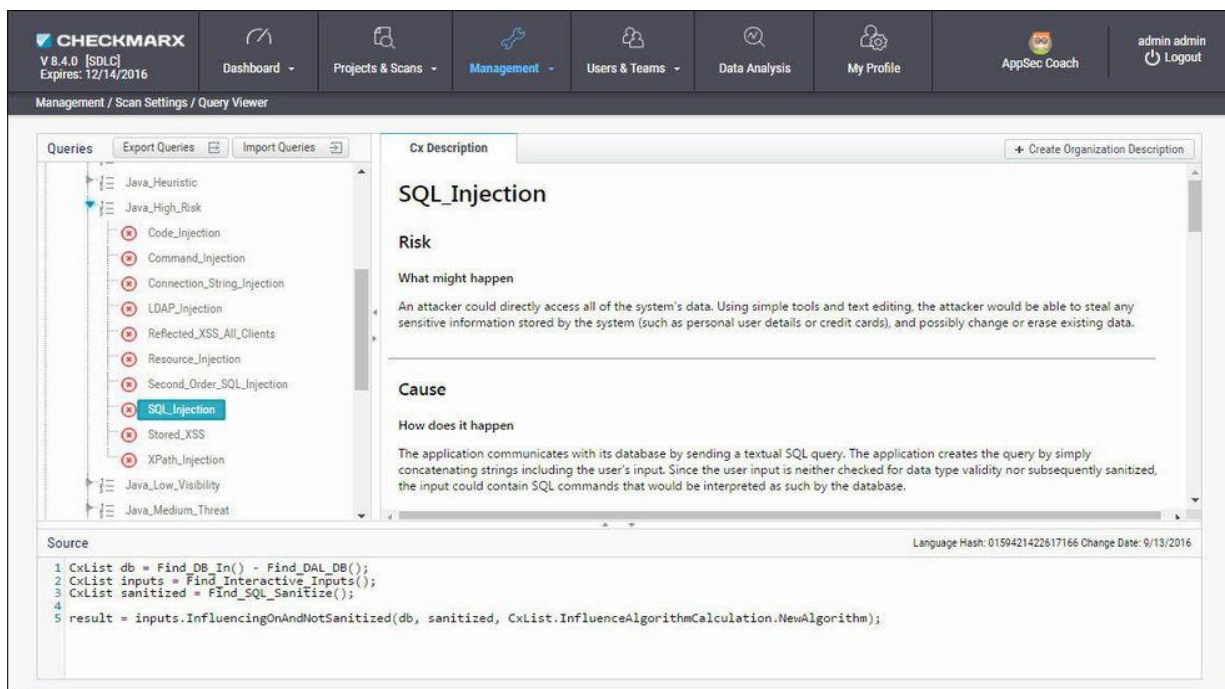

Select a **Query** in the **Queries** pane. A description is provided in the **Description** pane with a full explanation of the risk. The source code is displayed in the **Source** pane at the bottom of the window.
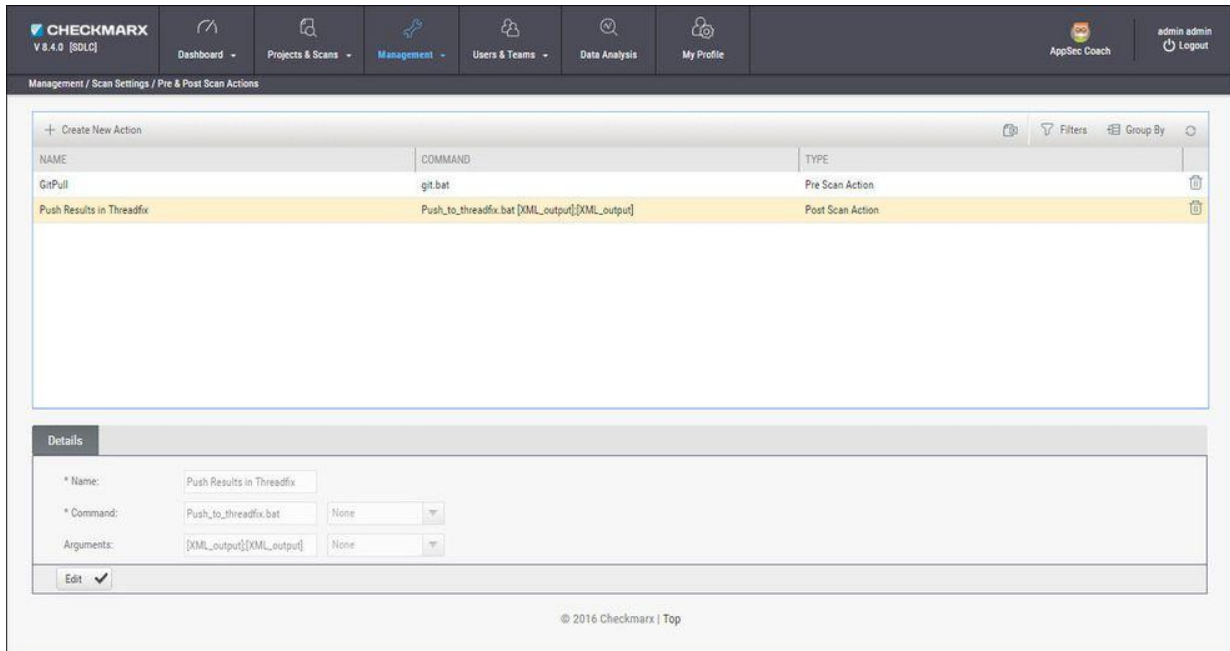
Creating a Custom Description

You can create a Custom Description to best suit your own organizations procedures and best practices.

> ⓘ The custom description creation option is enabled by default for Auditor and Admin users only.

To create a custom description:

From the **Query Viewer**, select a **Query** in the **Queries** pane. A description is provided in the **Description** pane.

Click **Create Custom Description**. The **Upload File to Create Custom Description** window is displayed.
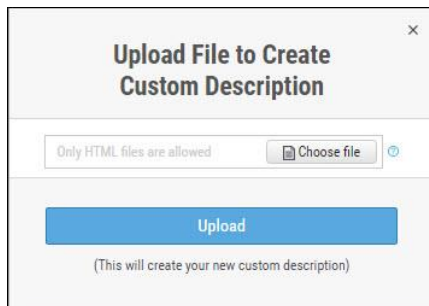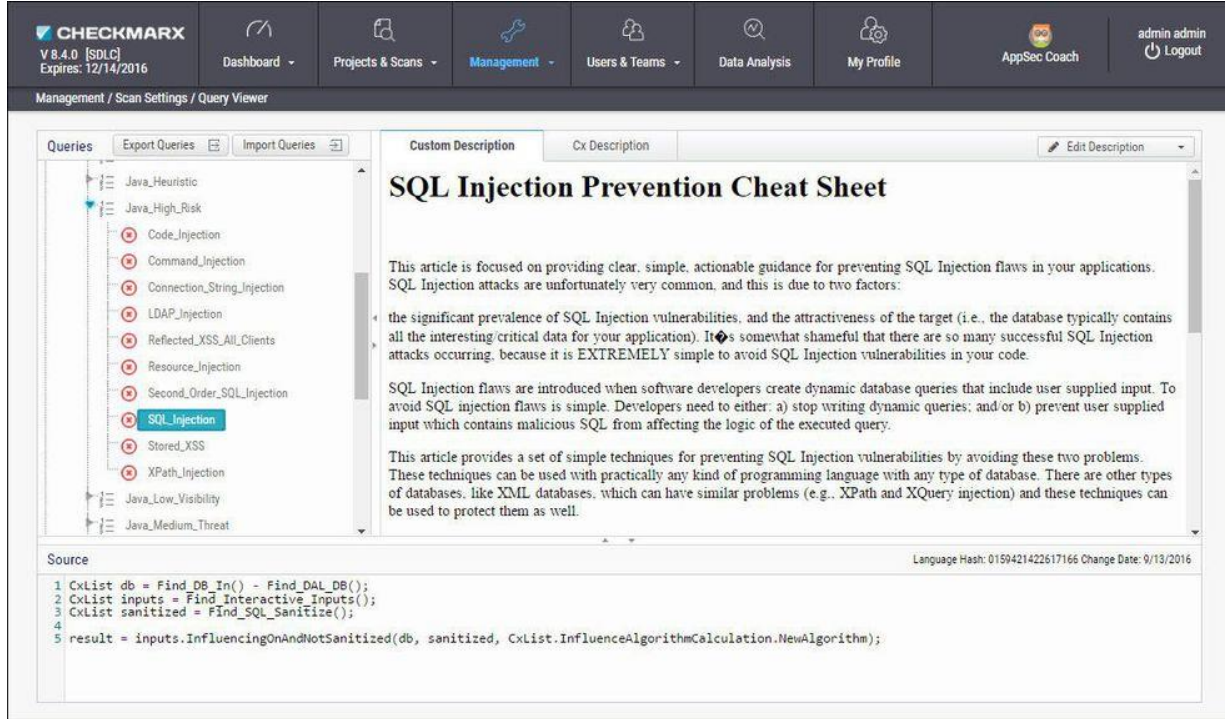
Click **Choose File,** navigate to the custom description file (.HTML) and click **Open**.

> ⓘ For security reasons CxSAST only supports the following HTML tags, attributes and inline styles:
>
> - **Tags** - b, br, caption, center, col, colgroup, dir, div, dl, dt, em, fieldset, font, footer, h1, h2, h3, h4, h5, h6, header, hr, i, li, ol, p, pre, span, strike, strong, table, tbody, td, tfoot, th, thead, tr, u, ul,
> - **Attributes** - align, alt, bgcolor, border, cellpadding, cellspacing, charset, color, cols, colspan, dir, height, lang, list, nowrap, radiogroup, rows, rowspan, selected, size, span, style, title, valign, value, vspace, width, wrap
> - **Styles (CSS values)** - background, background-color, background-position, background-repeat, border, border-bottom, border-bottom-color, border-bottom-style, border-bottom-width, border-collapse, border-color, border-left, border-left-color, border-left-style, border-left-width, border-right, border-right-color, border-right-style, border-right-width, border-spacing, border-style, border-top, border-top-color, border-top-style, border-top-width, border-width, bottom, caption-side, clear, clip, color, content, counter-increment, counter-reset, cursor, direction, display, empty-cells, float, font, font-family, font-size, font-style, font-variant, font-weight, height, left, letter-spacing, line-height, list-style, list-style-image, list-style-position, list-style-type, margin, margin-bottom, margin-left, margin-right, margin-top, max-height, max-width, min-height, min-width, orphans, outline, outline-color, outline-style, outline-width, overflow, padding, padding-bottom, padding-left, padding-right, padding-top, page-break-after, page-break-before, page-break-inside, quotes, right, table-layout, text-align, text-decoration, text-indent, text-transform, top, unicode-bidi, vertical-align, white-space, widows, width, word-spacing, z-index.
>
> If you try to upload a file with anything else other than what is listed above, the description will not be saved.

Click **Upload**. The **Custom Description** tab is displayed in the **Description** pane.

You can replace or delete the custom description by clicking **Edit Description** and selecting **Update Description** or **Delete Description** accordingly.

Importing Queries

You can import queries into CxSAST to best suit your own organizations procedures and best practices.

To import queries:

From the **Query Viewer**, click **Import Queries**. The **Import Queries** window is displayed.

Click **Import,** navigate to the query file (.XML) and click **Open**. The query is displayed in the **Queries** pane.

Exporting Queries

You can export queries from CxSAST to use in other departments.

To export queries:

From the **Query Viewer**, click **Export Queries**. The **Export Queries** window is displayed.
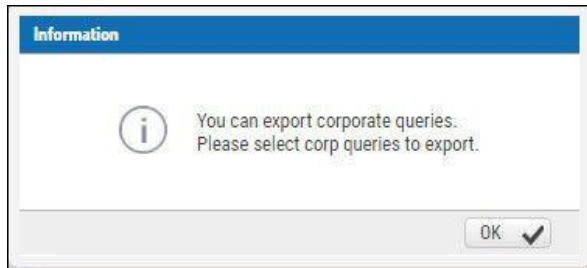
Click **OK**.

Preset Manager

Presets are predefined sets of queries that you can select when Creating, Configuring and Branching Projects. Predefined presets are provided by Checkmarx and you can configure your own. You can also import and export presets.

To open the Preset Manager:

Go to **Management > Scan Settings > Preset Manager**. The Presets Manager window is displayed.
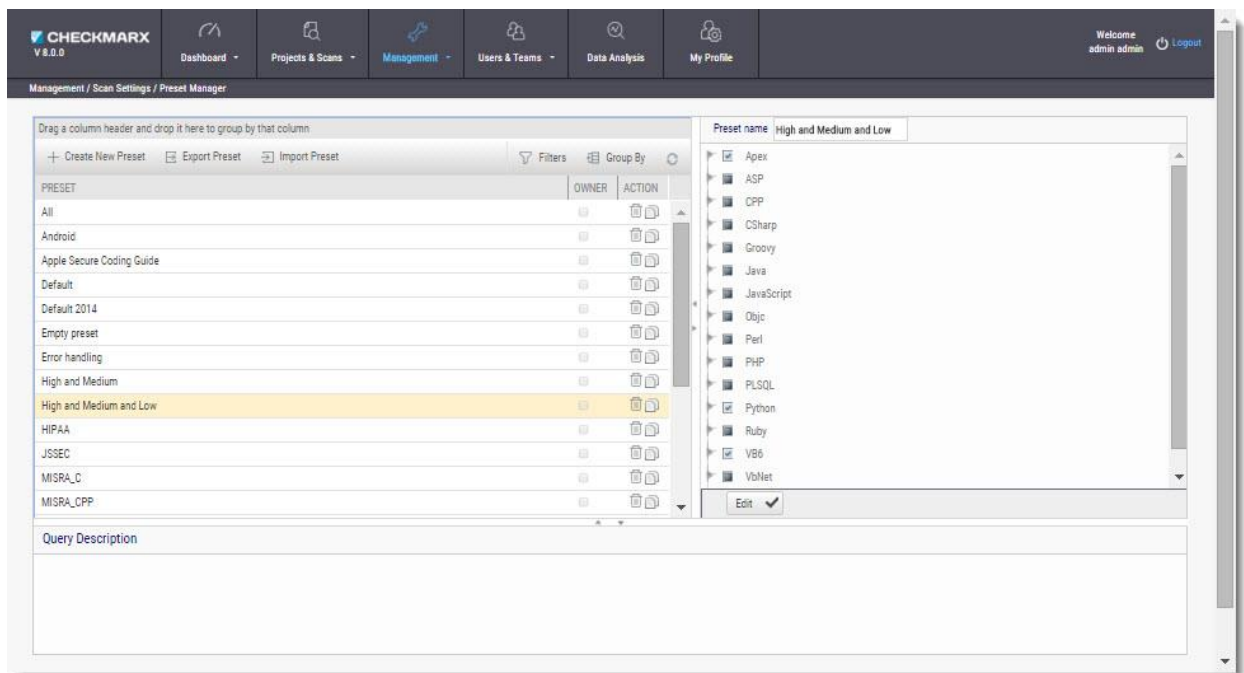
ⓘ	You can quickly create a new preset based on an existing one (duplicate) by selecting a Preset from the Preset pane and clicking ▢.

Creating a New Preset

To create a new preset:

From the **Preset Manager**, click **Create New Preset**. The Create New Presets window is displayed.
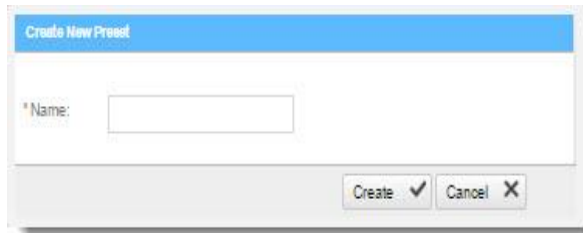
Enter a preset **Name** and click **Create**.

Select a **Coding Language**.

Select the **Queries** to be included in the preset.

Click **Save**.

Modifying an Existing Preset

To modify an existing preset:

From the **Preset Manager**, select a **Preset** from the Preset pane and click **Edit**.

Select a **Coding Language**.

Select the **Queries** to be included in the preset.

> ⓘ You can edit a single language, such as Java, selecting and deselecting the queries as needed, and then press Synchronize in order for all related queries in all languages to be selected.

Click **Save**.

Importing a Preset

To import a preset:

From the **Preset Manager**, click **Import Preset**. The Import Preset window is displayed.
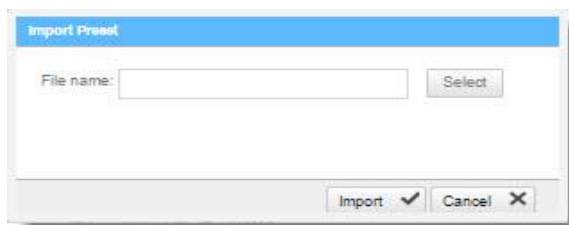
Click **Select**, navigate to the preset (.XML file) and click **Open**.

ⓘ If the imported preset has the same name as an existing one, the existing preset will be overridden.

Click **Import**.The Preset is displayed in the Preset pane.

Exporting a Preset

To export a preset:

From the **Preset Manager**, click **Export Preset** and save the exported preset (.XML file).

Deleting a Preset

To delete a preset:

From the **Preset Manager**, select a **Preset** from the Preset pane and click .

Predefined Presets

The following is a list of all the predefined presets provided by Checkmarx with the recommended usage and which vulnerability queries are included:

Preset	Usage	Includes vulnerability queries for….
All	For all application security risks	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
Android	For Android related application security risks	Java coding language
Apple Secure Coding Guide	For IOS related application security risks	ObjectiveC coding language
Checkmarx Default	The Checkmarx Default preset essentially contains all the vulnerabilities that Checkmarx recommends to scan in cases when you are unsure about which preset to use.	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, Objc, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
Default	Default preset (soon to be discontinued)	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, Objc, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
Default 2014	Default preset for 2014 (soon to be discontinued)	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
Empty Preset	Empty preset with no vulnerability queries. This can be used to create a new preset from scratch	Empty
Error Handling	For error handling related application security risks	Apex, ASP, CPP, CSharp, Java, Perl, PHP, Ruby and VbNet coding languages

Preset	Usage	Includes vulnerability queries for....
High and Medium	For high and medium related application security risks	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
High, Medium and Low	For high, medium and low related application security risks	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
HIPAA	For sensitive patient data related security risks according to the HIPAA (Health Insurance Portability and Accountability Act) compliance guidelines	Apex, ASP, CPP, CSharp, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Ruby, VB6, VbNet and VbScript coding languages
JSSEC	For Android related application security risks according to the JSSEC (Japan's Smartphone Security Association) compliance guidelines	Java coding language
MISRA_C	For C related application security risks according to the MISRA (Motor Industry Software Reliability Association) compliance guidelines	C++ coding language
MISRA_CPP	For C++ related application security risks according to the MISRA (Motor Industry Software Reliability Association) compliance guidelines	C++ coding language
Mobile	For mobile related application security risks	CSharp, Java, JavaScript and ObjectiveC coding languages
OWASP Mobile TOP 10-2016	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2016	CSharp, Java, JavaScript and ObjectiveC coding languages

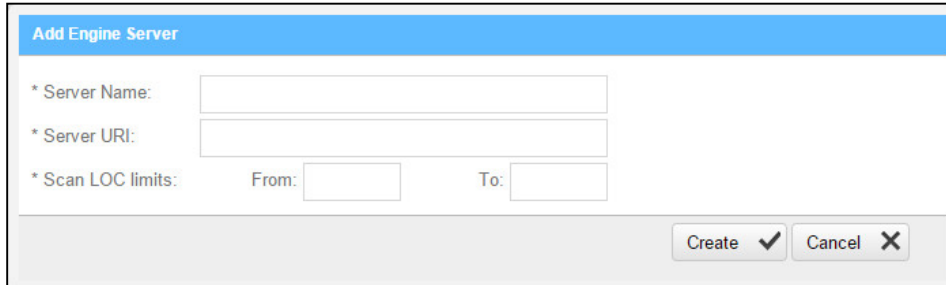| Preset	Usage	Includes vulnerability queries for....
OWASP TOP 10-2010	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2010	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
OWASP TOP 10-2013	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2013	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
PCI	For credit card payment application security risks according to the PCI (Payment Card Industry) compliance guidelines	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet, and VbScript coding languages
SANS Top 25	For the top 25 web application security risks according the SANS Technology Institute's compliance guidelines	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, VB6, VbNet and VbScript coding languages
WordPress	For WordPress related web application security risks	PHP coding language
XS	For XS SAP related application security risks	JavaScript coding language

Limiting Engine Scans

To Limit Engine Scans:

In **Management > Server Setting > Installation Information**, click .
The Add Engine Server window is displayed.

The Adding Engine Server window includes the following properties:

- **Server Name**: The name of the server you are appointing as Engine Server

- **Server URI**: The address of the server

- **Scan LOC limits**: The Scan limits is <u>not</u> a mandatory field, in the event the fields are left empty assume the value From to include: All to: All. Define the lower and higher limits for size of projects that this engine can accept for scanning.

    - When the range is defined and the user clicks OK, the system performs a check of range continuity. In the event there is no continuity between ranges of all engines defined at that moment, a pop-up message is displayed: "Line 1: "Notice: Projects including the following ranges: line 2 : XXX – YYY line 3: more then 1000 Line 4: Will not be scanned."

    - In the event the scan size falls out of defined engine ranges, the scan fails and the following message is displayed: "Scan has failed due to falling outside of the defined engines scan ranges".

    - After defining the scan engine range, in order to activate the user has to Restart the scan manager service.

Connection Settings.

In this section:

- LDAP Management
- SAML Management
- Issue Tracking Management (New)

LDAP Management

LDAP (Lightweight Directory Access Protocol) is an Internet protocol that web applications can use to look up information about those users and groups from the LDAP server. You can connect the CxSAST application to an LDAP directory for authentication, user and group management. CxSAST provides built-in connectors for the most popular LDAP directory servers; Active Directory, OpenLDAP and Custom LDAP Server. Connecting to an LDAP directory server is useful if user groups are stored in a corporate directory. Synchronization with LDAP allows the automatic creation, update and deletion of users and groups in CxSAST according to any changes being made in the LDAP directory.

Adding an LDAP Server

To add a new LDAP Server:

Select **Management** > **Connection Settings** > **LDAP Servers**. The LDAP Server window is displayed.
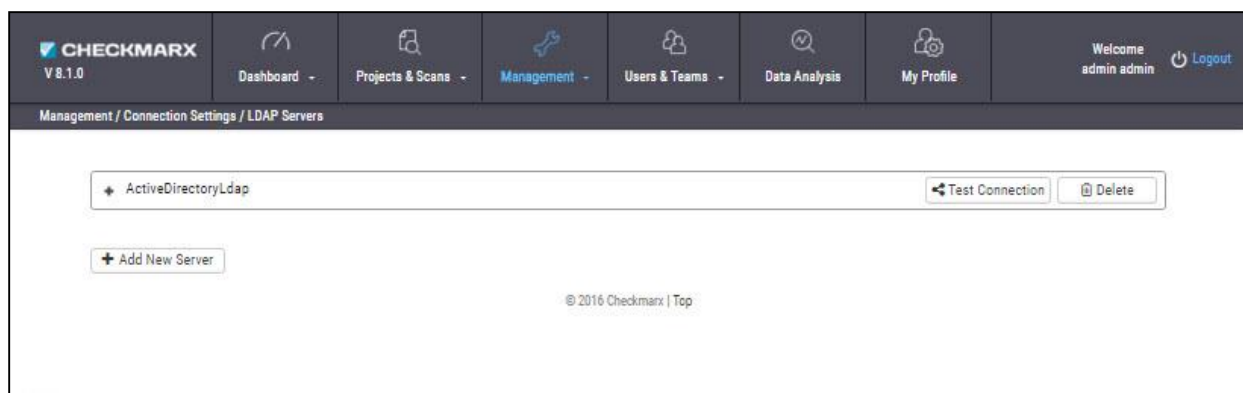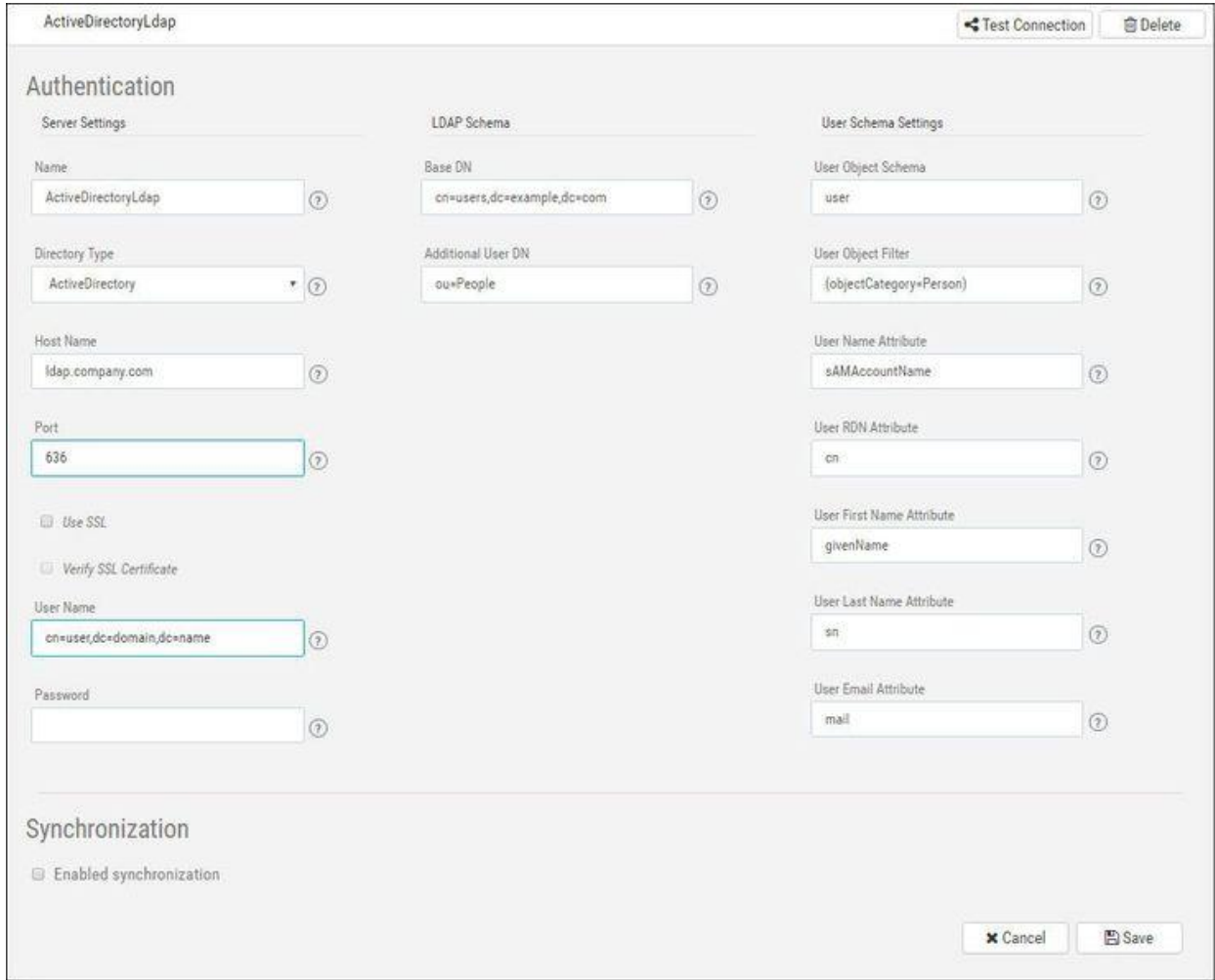
Click + **Add New Server**. The LDAP Server Authentication window is displayed (see **Defining LDAP Authentication Settings,** below).

To delete an existing LDAP Server, click **Delete**.

Defining LDAP Authentication Settings

To define LDAP Server authentication settings:

Click + (active directory) to expand an existing LDAP server settings, or click + **Add New Server**. The LDAP Server Authentication window is displayed.

The LDAP Server Authentication window includes the following settings:

Server Settings

- **Name** - Server name
- **Directory Type** - Provides auto selection for server parameters according to default settings (ActiveDirectory, OpenLDAP, or LDAP Server)
- **Host Name** - LDAP server hostname
- **Port** - LDAP server port
  - **Use SSL** - Used to ensure that all data passed between the server and the client remains private and integral
  - **Verify SSL Certificate** - Used to verify SSL certificates
- **User Name** - Distinguished name (DN) of the user that the application uses when connecting to the LDAP server (e.g. cn=user,dc=domain,dc=name)

> ⓘ You can enable or disable the use of the LDAP control extension for paging of search results. If paging is enabled (default), the search will retrieve sets of data rather than all of the search results at once. Therefore, if you are searching for a specific user then the definition in the User Name field should also be specific (using full user DN, e.g. dn=myuser,ou=people,dc=company,dc=com).

- **Password** - Password of the user specified above

LDAP Schema

- **Base DN** - Used to search for users (e.g. cn=users, dc=example, dc=com)
- **Additional User DN** - Used to limit users search to specific DN (e.g. ou=People)

User Schema Settings

- **User Object Schema** - LDAP user object class type to use when loading users (e.g. user)
- **User Object Filter** - Filter expression to use when searching user objects (e.g. (objectCategory=Person))
- **User Name Attribute** - Attribute field to use on the user object (e.g. cn=sAMAccountName)
- **User RDN Attribute** - Attribute field to use when loading the user distinguished name (e.g. cn)
- **User First Name Attribute** - Attribute field to use when loading the first user name (e.g. givenName)
- **User Last Name Attribute** - Attribute field to use when loading the last user name (e.g. sn)
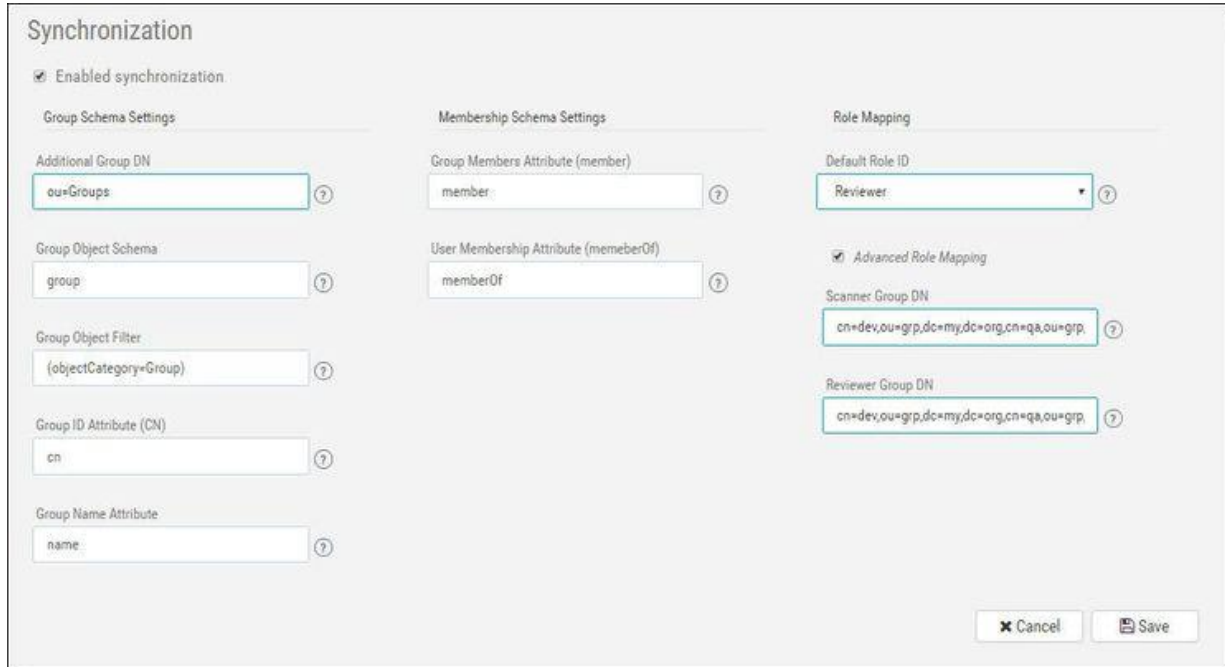- **User Email Attribute** - Attribute field to use when loading email (e.g. mail)

Click **Test Connection**.

Click **Save**.

Defining LDAP Synchronization Settings

To define LDAP Server synchronization settings:

Click **Enable Synchronization.** The LDAP Server Synchronization window is displayed.

The LDAP Server Synchronization window includes the following settings:

Group Schema Settings

- **Additional Group DN** - Used to limit groups search to specific DN (e.g. ou=Groups)
- **Group Object Schema** - LDAP group object type (e.g. group)
- **Group Object Filter** - LDAP filter expression to use when searching the groups (e.g. (objectCategory=Group))
- **Group ID Attribute (CN)** - Attribute in LDAP defining the group's id (e.g. cn)
- **Group Name Attribute** - Attribute in LDAP defining the group's name (e.g. name)

Membership Schema Settings

- **Group Members Attribute** - LDAP member attribute is a multi-value attribute that contains the list of distinguished names for the user, group, and contact objects that are members of the group (e.g. member)
- **User MemberOf Attribute** - LDAP memberOf attribute is a multi-valued attribute that contains groups of which the user is a direct member (e.g. memberOf)

Role Mapping

- **Default Cx Role** - Used to determine the CxSAST role of users who are otherwise not assigned roles (e.g. Scanner, Reviewer)

  Advanced Role Mapping - Select **Advanced Role Mapping** checkbox to activate advanced role mapping options

  - **Scanner Group** - List of LDAP group DNs. Members of these groups will be assigned the Scanner role (e.g. cn=dev,ou=grp,dc=my,dc=org ; cn=qa,ou=grp,dc=my,dc=org)
  - **Reviewer Group** - List of LDAP group DNs. Members of these groups will be assigned the Reviewer role (e.g. cn=dev,ou=grp,dc=my,dc=org ; cn=qa,ou=grp,dc=my,dc=org)

Click **Save**.

You can now create LDAP users (see **Creating User Accounts in the Web Interface**) and map LDAP user groups to CxSAST teams (see **Managing Teams**).
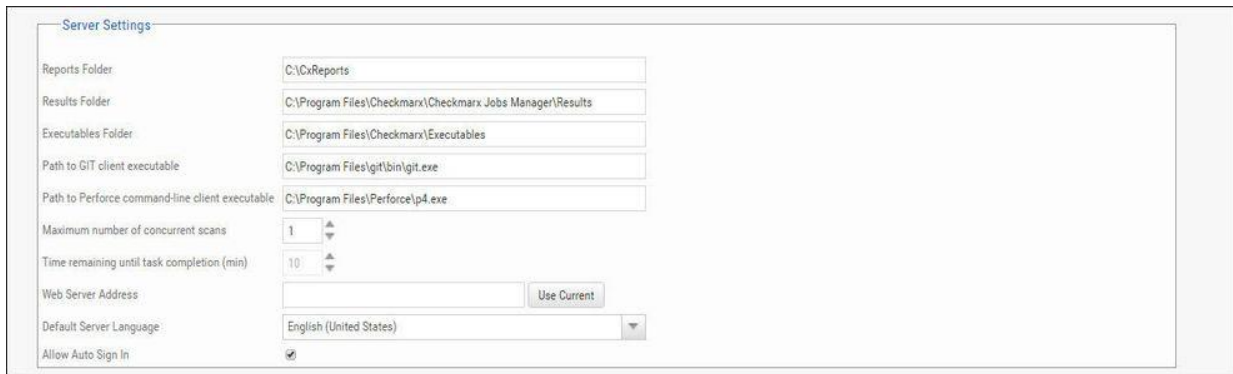
Application Management

General

The General screen enables you to set the paths, folders, web server address, and language as well as other Application specific settings and SMTP.

Server Settings

In the Server settings window, you can set folder locations, maximum number of scans, default settings and automatic sign in.

The Server Settings window includes the following settings:

- **Reports Folder** - Set the reports folder to save reports in (e.g. C:\CxReports)
- **Results Folder** - Set the results folder to save results in (e.g. C:\Program Files\Checkmarx\Checkmarx Jobs Manager\Results)
- **Executables Folder** - Set the executables folder to save executables in (C:\Program Files\Checkmarx\Executables)
- **Path to GIT client executable** - Set the GIT client executable path (e.g. C:\Program Files\git\bin\git.exe)
- **Path to P4 command line client executable** - Set the Perforce client executable path (C:\Program Files\Perforce\p4.exe)

> ⓘ If you haven't already done so, download the P4 command line executable (HELIX P4: COMMAND-LINE) from: https://www.perforce.com/downloads/helix, run the .exe file making sure the installed files are placed into a directory that CxSAST can access (i.e. C:\Program Files\Perforce)". Use this same directory to fill the Path to P4 command line client executable parameter field.

- **Maximum number of concurrent scans** - Set the maximum number of concurrent scans a CxManager can run. This cannot exceed the licensed number of concurrent scans. The default is 2.

- **Time remaining until task completion (min)** - Set the time remaining until task completion (timer).
- **Web Server Address** - Set the web server address in order to access links in generated report from outside the organization.
- **Default Server Language** - Set the default server language.
- **Allow Auto Sign In** - Enable/Disable auto sign in.

SMTP Settings

The SMTP settings window enables you to set the host settings and default credentials of your SMTP.

The SMTP Settings window includes the following settings:

- **Host** - Type in the host domain.
- **Port** - Select a port number.
- **Encryption Type** - Select the encryption type.
- **Use Default Credentials** - Enable/disable default credentials. If enabled the default credentials of the host machine are used.
- **User Name** - Type in the user name.
- **Password** - Type in the password.

License Details

The License Details screen is divided into the following windows:

General

**The General window** provides general license information.

The General window includes the following properties:

- **Expiration Date** - CxSAST license expiry date
- **Engines** - The number of engines the license was bought for
- **LOC** - The number of lines of code the license was bought for
- **HID** - Hardware identification number
- **OSA License -** Open Source Analysis license status - Enabled, Disabled or Conditional (with expiration date for Conditional version)

Note: To request a new license, if you have not yet obtained a permanent license, copy your **Hardware ID**, which you will need in order to obtain a license from Checkmarx. Or, you can later obtain your hardware ID by using the shortcut in the Windows / Start menu Checkmarx folder.

Supported Languages

The Supported Languages window includes the supported languages used in default queries.
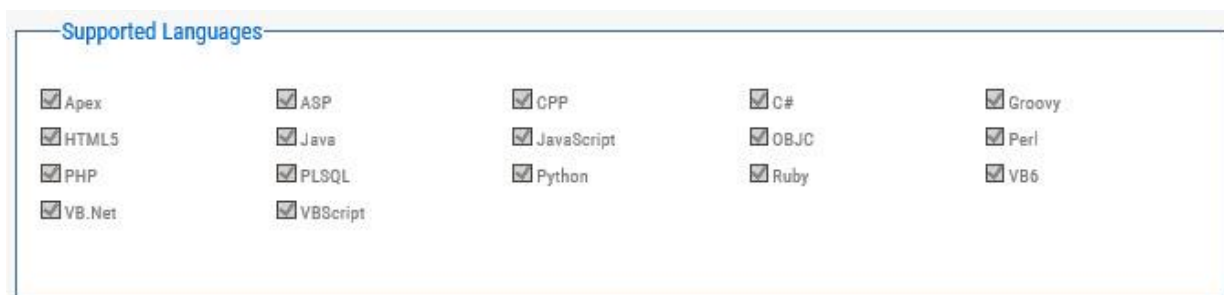
Roles

The Roles window describes the number of users with roles in used/available which are licensed in the system.


The Roles window includes the following user types:

- **Server Managers** - The default administrator user account. The Server Manager has complete permissions for the whole system, including server settings.
- **Service Provider Managers** - Users can create and manage projects for Companies, Teams, and Users.
- **Company Managers** - Users can create and manage projects for Company's Teams and Users.
- **Scanners** - Users can create projects for their own team, and scan and view results of their Team's existing projects.
- **Auditors** - Users have auditing permissions and can run the CxAudit.
- **Reviewers** - Users can review data reports at the management level.

Number of Companies and Service Providers

The number of companies/service providers who have licenses in use/available in the system.
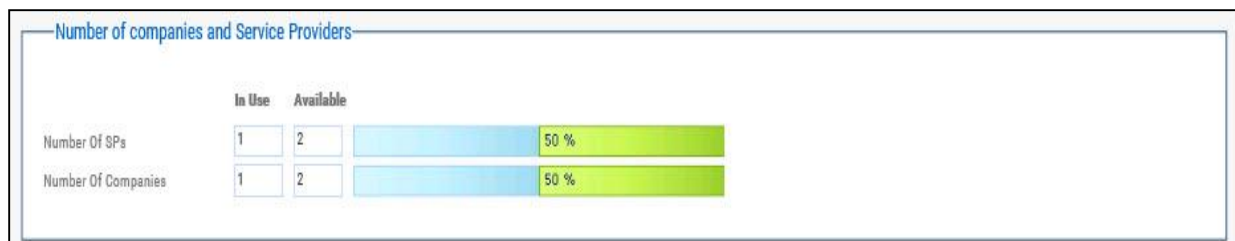
The Number of Companies and Service Providers window includes licenses in use/available in the system:

- **Number Of SP's** - The number of Service Providers in the system
- **Number Of Companies** - The number of Companies in the system.

Installation Information

The Installation Information screen provides the number of system components and engines installed.

The Installation Information screen is divided into the following two windows:

- **System Components** - Provides a list of components installed with Cx, the Installation Path, Version, DNS, IP, Hotfix, and State.

- **Engine Servers** - Provides the Server name, Server URL, Scan size and Action.

Maintenance Settings

In this section:

- Data Retention Management

Data Retention Management

In order to properly manage data storage consumption, CxSAST allows for the manual purging of old scan data. An administrator can define the desired storage policy by date range or by defining a minimal number of scans to retain overriding the date range.

> ⓘ **Warning** - Scanned data is purged from the file system as well as the database, therefore, once deleted cannot be reversed. See **Data Retention Purged Data**, below.

Using SOAP API and Windows Tasks, data retention can be automated.

> ⓘ Data retention settings apply globally to all projects within the system. This global configuration can be overridden for a specific project, either during the project creation or by editing the project's setting through the Data Retention tab (see **Creating and Configuring a CxSAST Project** and **Viewing Project Details**).
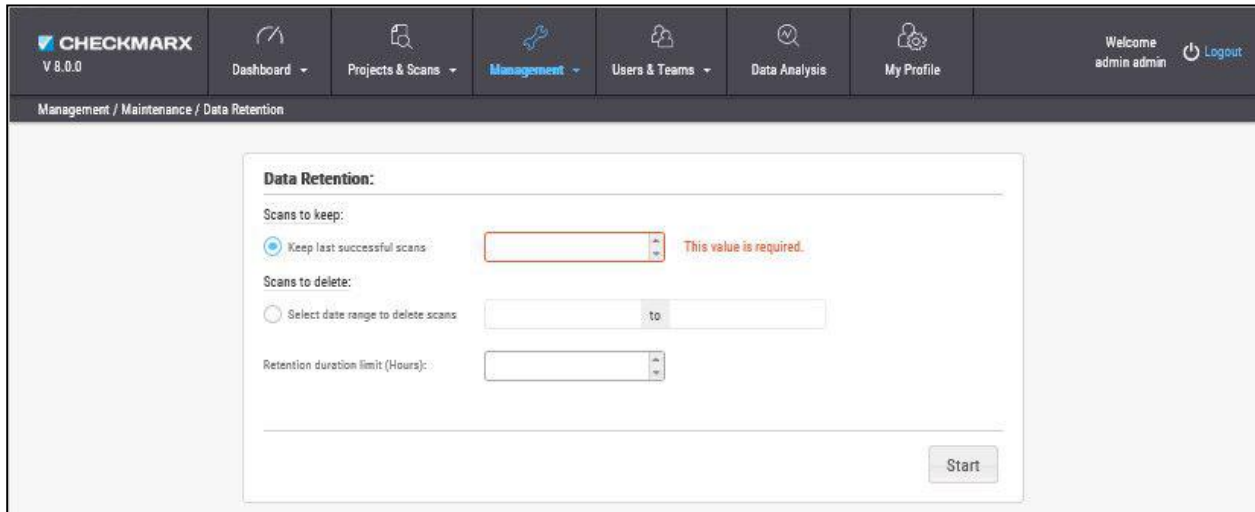
Specific scans may be marked as "Locked" to avoid automated purging of important scan data.

> ⓘ Locked scans cannot be deleted, and will be skipped in the data retention process. If you would like to delete all scans within the range defined for deletion, it is highly important to ensure that no locked scans are included within this range. If the range does include locked scans, unlock the scans before executing the Data Retention command (see **Unlocking Scans**).

Defining Data Retention Settings

To define the data retention settings:

Select **Management** > **Maintenance** > **Data Retention**. The Data Retention window is displayed.

The Data Retention window includes the following settings:

Scans to keep:

- **Keep last successful scans** - Set the requested number of scans to be kept. This setting leaves only the specified number of recent successful last scans and deletes all other scans.

Scans to delete:

- **Select date range to delete scans** - Enter a start and an end date. This setting deletes all scans within a predefined time range.
- **Retention duration limit (hours)** - Set a limit to the amount of time the operation should take. If set to 10, then after 10 hours the operation automatically stops, regardless of whether the operation is complete.

Click **Start**.The following message appears:
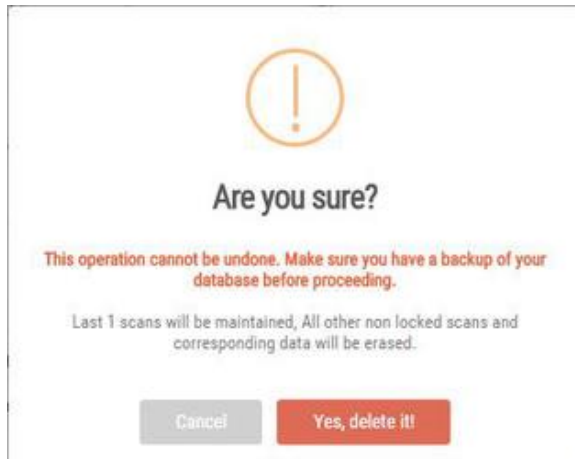
If you are unsure whether you have backed up your database, or if the range you defined for deletion includes locked scans, click **Cancel** to postpone the deletion.

If you want to continue, click **Yes, delete it.** The following message is displayed "**Data retention is now in progress**" and the progress of the data retention process is represented in the Stages panel.
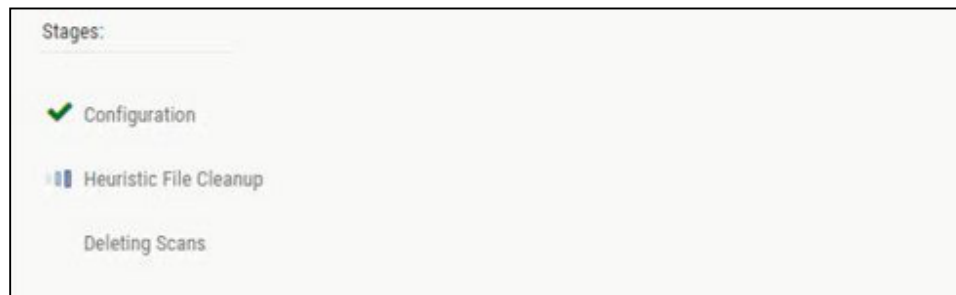
Once the data retention process is complete, status information about last deletion is displayed in the **Last Executed Data Retention** panel.
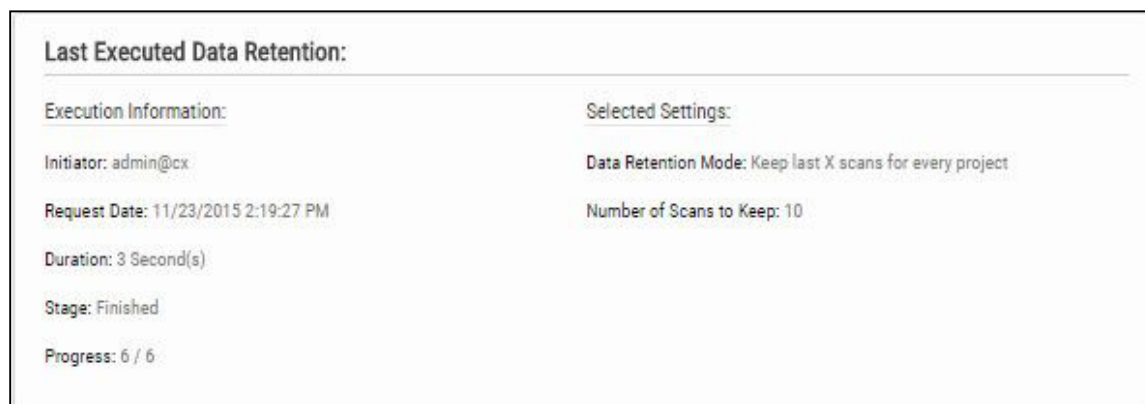
Data Retention Purged Data

Scanned data is purged from the file system as well as the database, therefore, once deleted cannot be reversed. The following data is purged as part of the data retention:

Database Tables

Selected data from the following tables is purged as part of the data retention:

- All Scans
- TaskScans
- CancelledScans
- TaskScanEnvironment
- ScanReports
- FailedScans
- PathResults
- NodeResults

File System

- CxSRC folder – This folder holds the extracted source files which are being scanned. Files and folders inside the CxSrc folder are deleted as part of data retention except for the following scenario:
  In case the exact same sources (ZIP, remote location..) are uploaded to the same existing scan, the extracted folder will be excluded from further data retention cleaning tasks.
- CxReports folder - This folder holds the following:
  - Reports requested by the customer and created in the CxSAST reports page. These reports are deleted as part of the data retention
  - Eclipse IDE reports created after each developer scan request. These reports are not deleted as part of the data retention.

Unlocking Scans

One of the most common reasons for having no scans deleted is that one or more of the scans are locked. This can be modified by unlocking the scans.

To unlock the scans:

1. Go to **Projects & Scans** > **Projects**.
2. Select the requested project. If many projects exist, find the project by using the following steps:
   a. Click **Filters** on the right.
   b. Type one or more identifying criteria for the project, such as the project name, owner, and team.
   c. Click **Enter**.
3. Go to the column **Scans List**.
4. Click the button **View project scans**.
   A list of all scans belonging to the selected project appears. If the list contains more than one page, use the directional arrows on the left to move to the next or previous page.
5. Go to the **Locked** column.
6. See if one or more of the scans is locked.
7. Use the **Unlock scan** button (🔒) to remove the lock.

Managing Custom Fields

It is now possible to define project attributes (metadata) by using custom fields.

Implementing and consuming project attributes - using the new Custom Fields capability - is a 3 steps process:

1. Creating new custom fields
2. Filling up the custom fields per project
3. Consuming custom fields using the OData REST APIs.

To define custom fields:

1. Go to **Management > Manage Custom Fields.**
2. Click **Add**.
3. Enter a unique custom field name in the designated field.
4. Click **Save**.

Each newly added custom field (up to 10) is displayed on the list and can be edited or deleted.
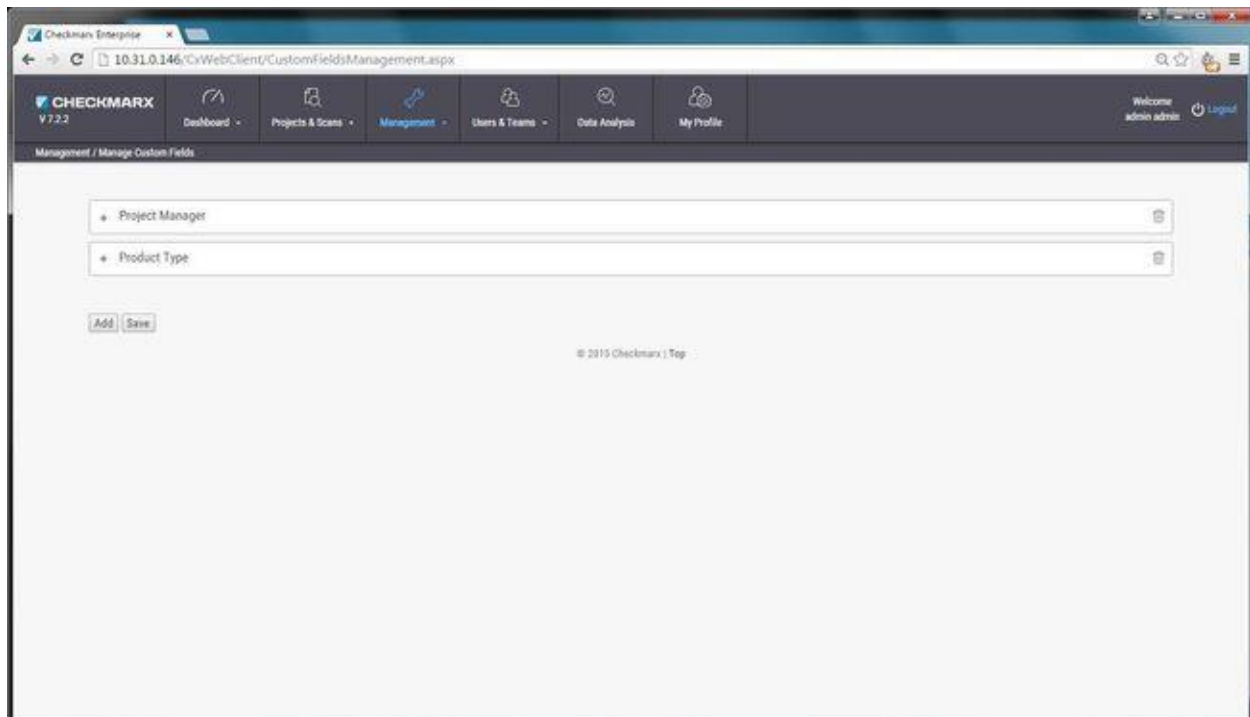
To edit the custom field's name:

1. Click the "+" sign to the left of the field name.
2. Perform the requested change in the editable row that appears.
3. Click **Save**.

Custom field are available for fill-out in the project attributes screen, both when you create new project and later when you edit an existing project.
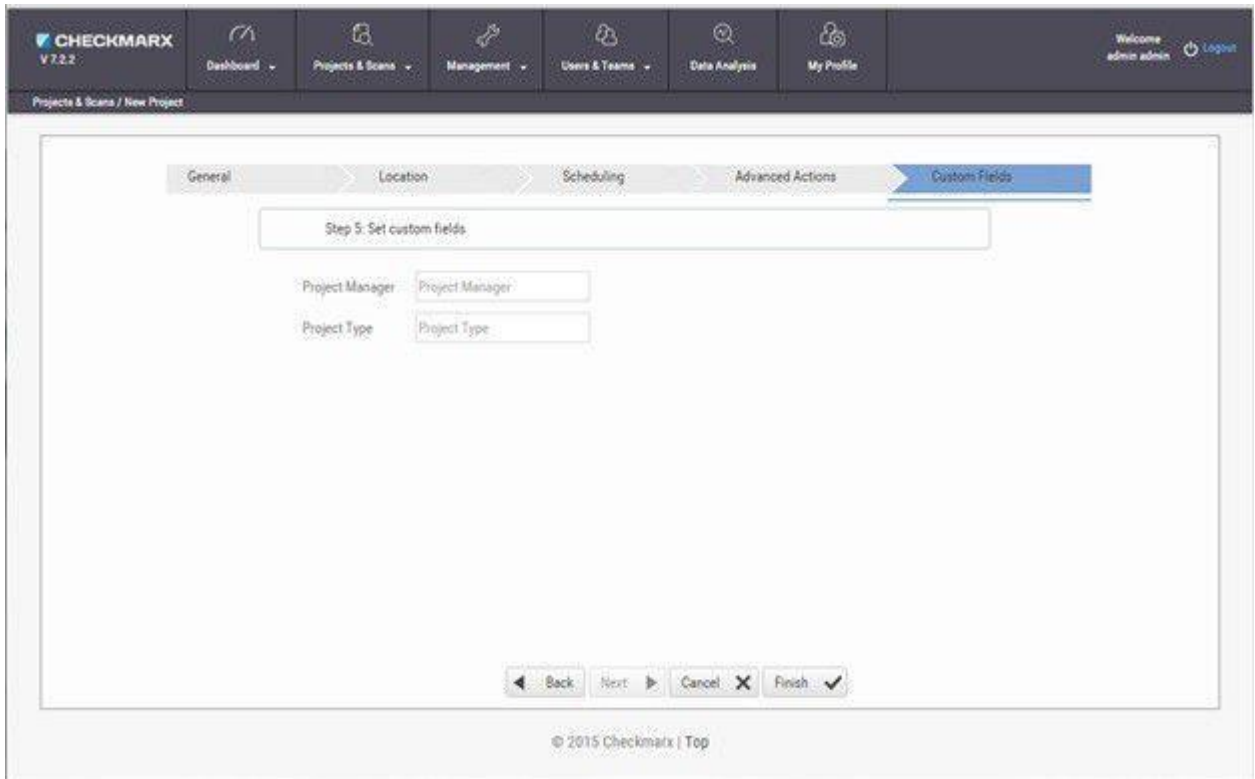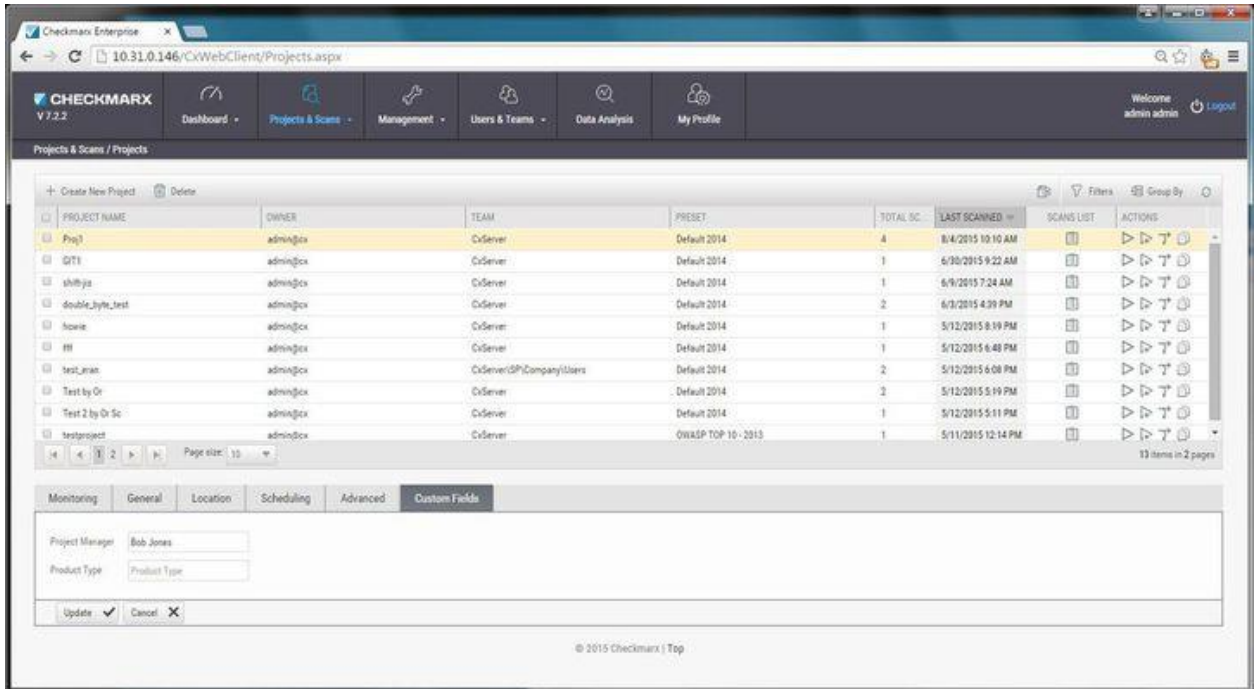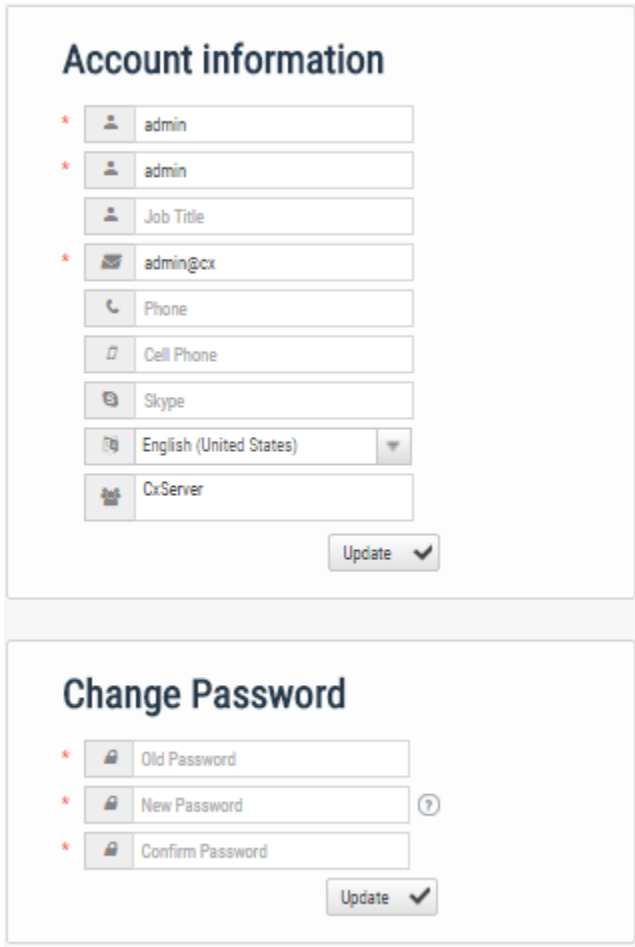
My Profile Settings

Accessing My Profile Settings

To access My Profile settings:

In the System Dashboard, click **My Profile**. The My Profile window is displayed.

* Indicates a mandatory field

Defining Profile Account Information

The Account information window includes the following parameters:

Account Information:

- *** First Name**
- *** Last Name**
- **Job Title**
- *** Email** - the email address used (must be of valid format, i.e. John.Smith@example.com, and not John.Smith@example).
- **Phone** - the user's landline phone number
- **Cell Phone** - the user's cellular phone number
- **Skype** - the user's skype name
- **Language** - can be one of the following options:
  - English (United States)
  - Chinese (Traditional, Taiwan)
  - Japanese (Japan)
  - Korean (Korea)
  - Chinese (Simplified, PRC)
- **User Teams** - Server name used by the user teams

Click **Update**.

Changing Profile Password

The Change Password panel allows replacing the user's current password, by providing the following parameters:

Change Password:

- *** Old Password**
- *** New Password**
- *** Confirm Password**

> ⓘ The required password complexity is as follows: 9 to 400 characters, at least 1 uppercase letter, at least 1 lower case letter, at least 1 special character and at least 1 digit.

Click **Update**.