CxSAST v8.9.0

Setup, Installation and User Guide

Contents

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

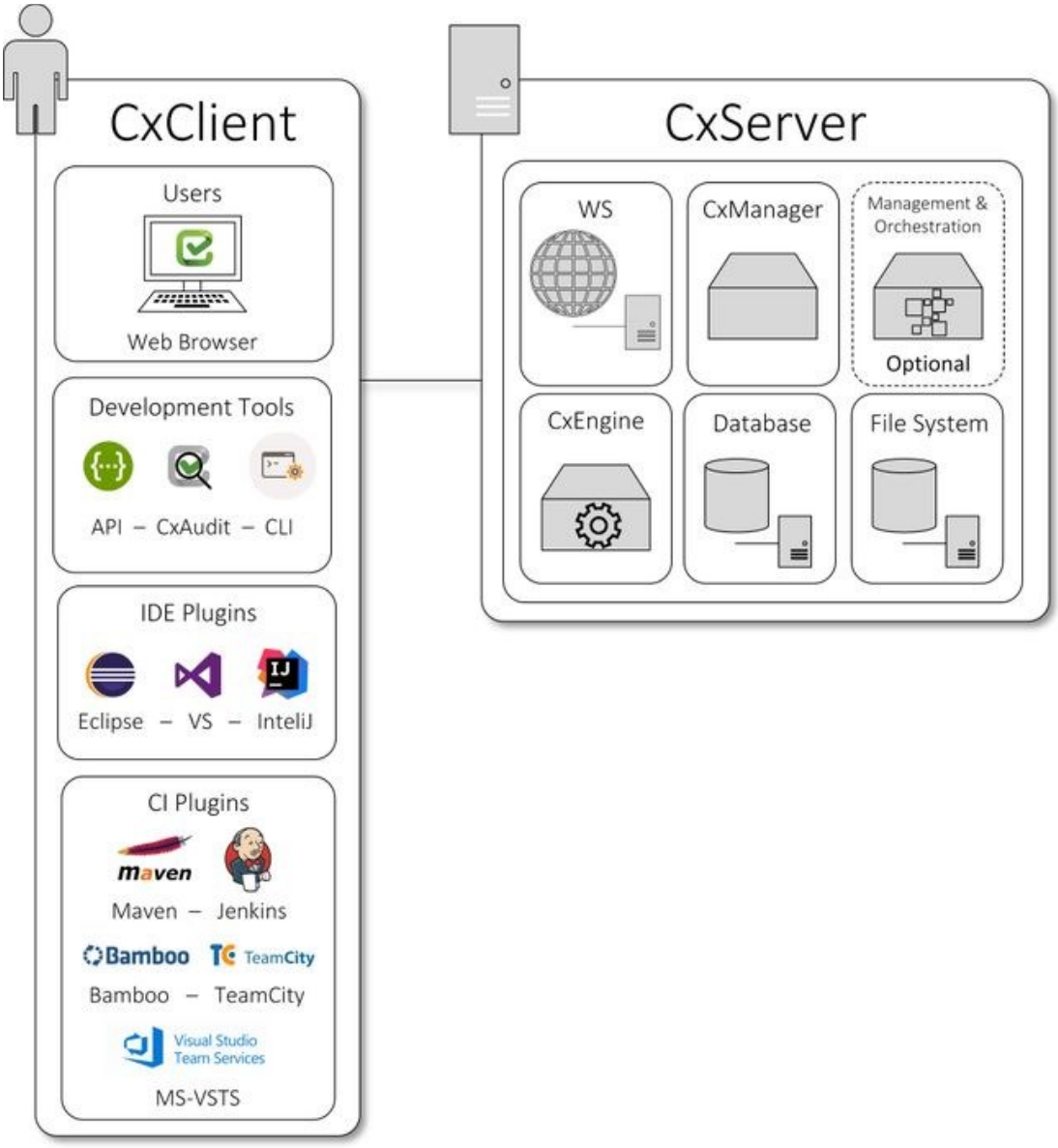
Setting Up CxSAST

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

In this section

System Architecture Overview

CxSAST includes the following components:



CxClient

CxSAST supports following clients (user interfaces)

- Web Portal - provides an intuitive web interface for managing and analyzing code scan projects for CxSAST.

- CxAudit - provides the capability to create or customize analysis queries for use in CxSAST.
- API - provides the capability for developers to create unique client implementations using the available APIs.
- CLI - provides a command line interface for CxSAST functionality and CI scenarios.
- IDE Plugins - provides scanning and integrated scan result navigation directly from the IDE development environment.
- CI Plugins - provides integration to CxSAST compatible plugins (e.g. Jenkins) for CI/CD scenarios.

CxServer

CxSAST includes the following server components:

- WS (IIS Web Service) - controls CxManager actions (i.e. initiating scans, viewing results and generating reports).
- CxManager - manages and integrates system components, performs all system functions utilizing the IIS Web Service.
- Management & Orchestration (Optional) - manages security risk and orchestrates policy management, helping to drive decision across the organization based on actionable data.
- CxEngine - performs the code scans.
- Database - stores scan results and system settings.
- File System - controls how the data is stored and retrieved.

Architecture Types

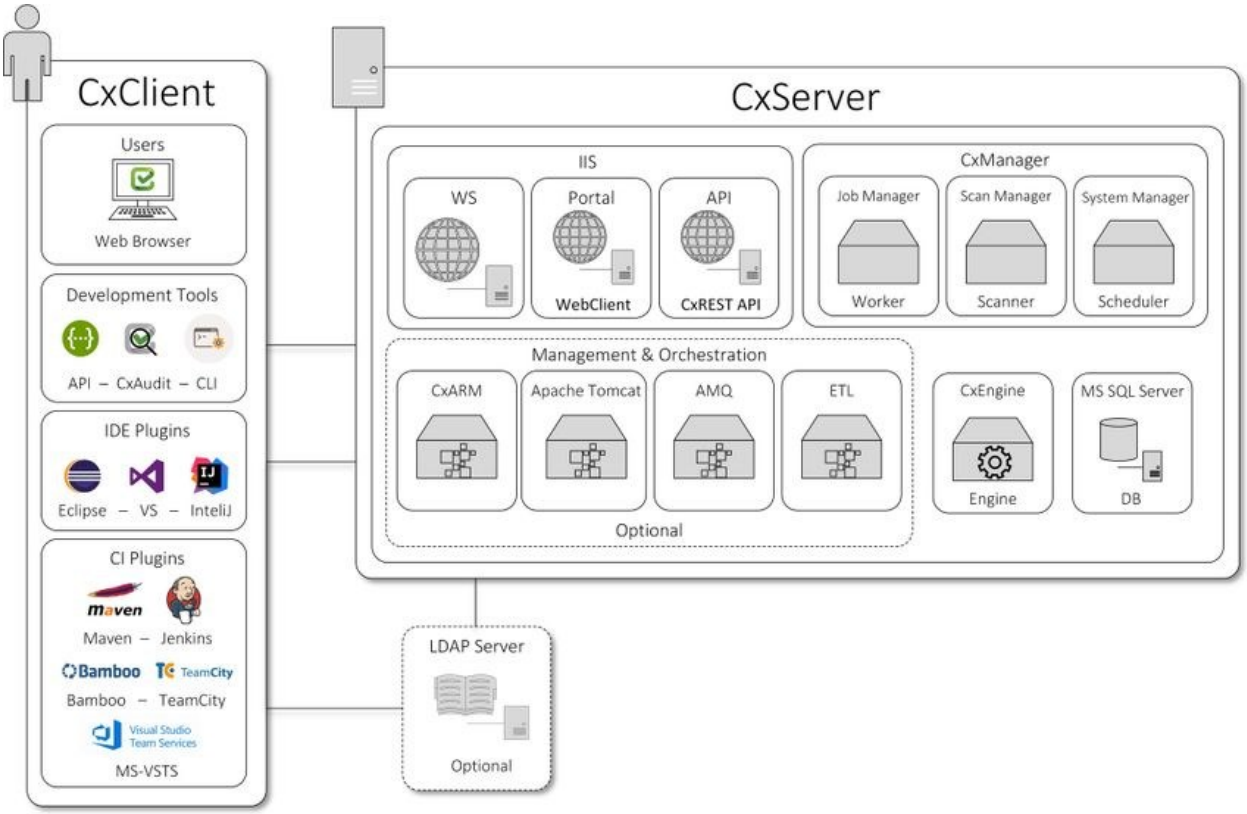
CxSAST supports following architecture types:

- Centralized Architecture - where all server components are installed on the same host.
- Distributed Architecture - where any or all of the server components are installed on dedicated hosts.
- High Availability Architecture - where more than one manager is available to control system management, ensuring that in cases where one manager fails the system will continue to be fully operational.

Communication between the CxClient 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.



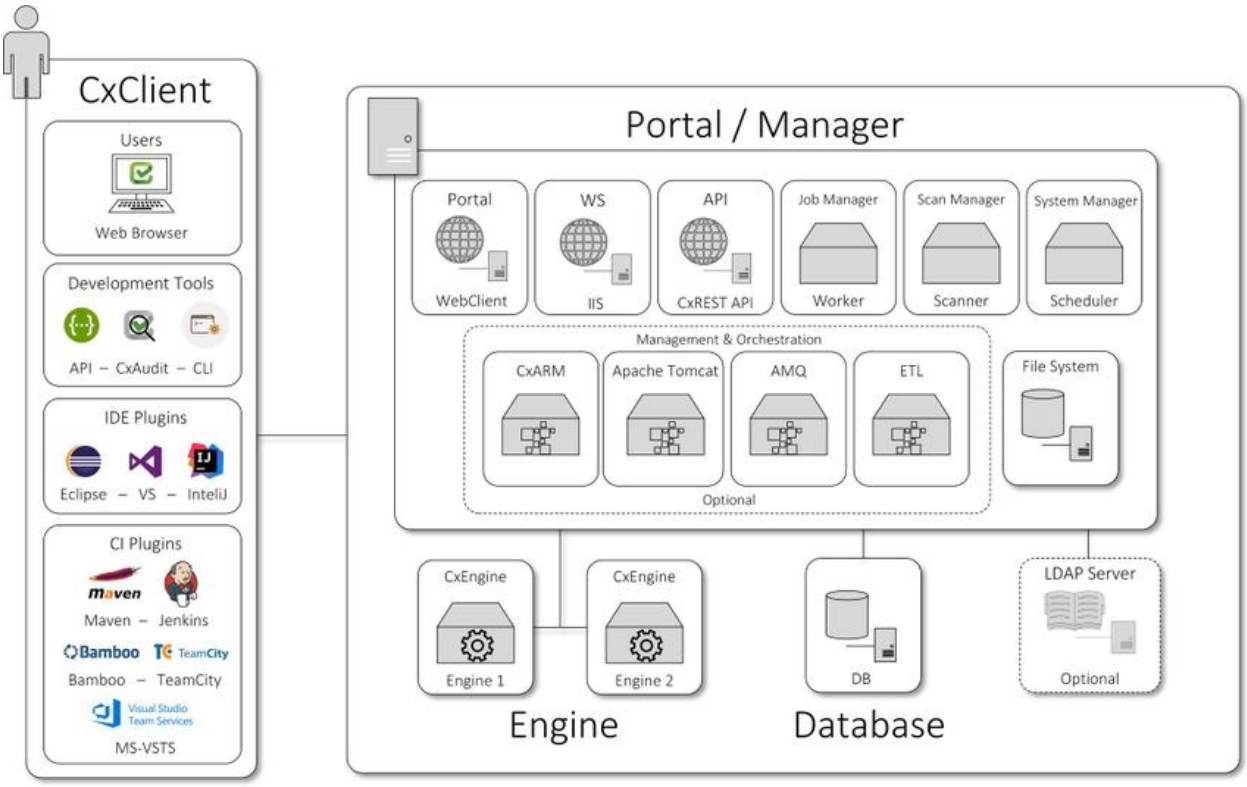
CxSAST also supports following architecture types:

- Distributed Architecture - where any or all of the server components are installed on dedicated hosts.
- High Availability Architecture - where more than one manager is available to control system management, ensuring that in cases where one manager fails the system will continue to be fully operational.

Communication between the CxClient and CxManager as well as communication between the CxManager and the CxEngine are via HTTP (by default). HTTPS can also be configured.

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.

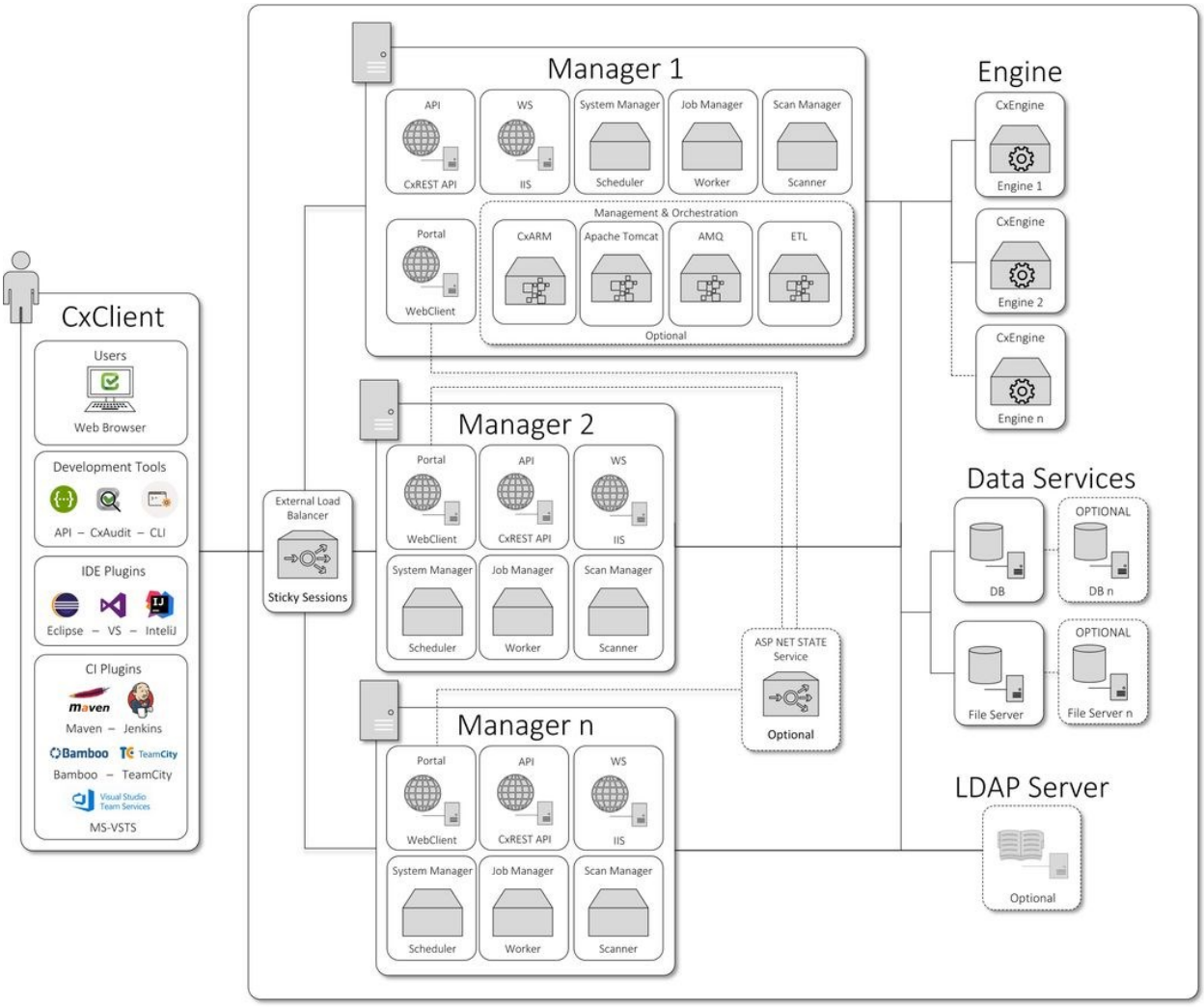
CxSAST also supports following architecture types:

- Centralized Architecture - where all server components are installed on the same host.
- High Availability Architecture - where more than one manager is available to control system management, ensuring that in cases where one manager fails the system will continue to be fully operational.

Communication between the CxClient and CxManager as well as communication between the CxManager and the CxEngine are via HTTP (by default). HTTPS can also be configured.

High Availability Architecture

High availability architecture is an approach of defining the components, modules or implementation of services of a system that ensures optimal operational performance, better load balance and easier versioning for upgrades. CxSAST supports high availability architecture, where two or more CxManager servers (in active-active mode) are installed and can access the same database. This ensures that in cases where one CxManager fails the system will continue to be 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.

CxSAST also supports following architecture types:

- Centralized Architecture - where all server components are installed on the same host.
- Distributed Architecture - where any or all of the server components are installed on dedicated hosts.

Communication between the CxClient and CxManager as well as communication between the CxManager and the CxEngine are via HTTP (by default). HTTPS can also be configured.

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.

<table>
<tr><th>Purpose</th><th>Lines of Code</th><th>Installed RAM**</th><th>Cores</th><th>CPU Speed</th><th>Disk</th><th>OS</th><th>Web Server</th><th>Other Software</th></tr>
<tr><td rowspan="2">Centralized (POC)</td><td>200K</td><td>8 GB</td><td rowspan="2">6-8</td><td rowspan="2">2.8 GHz</td><td rowspan="2">80 GB (recommended)</td><td rowspan="2">Windows 7,8,8.1,10 Windows Server 2008R2 2012, 2012R2, 2016</td><td rowspan="2">IIS 7/7.5/8/ 8.5/10</td><td rowspan="8">Windows Installer 3.1 or above (Run msiexec to check) .NET framework 4.7.1</td></tr>
<tr><td>500K</td><td>16 GB</td></tr>
<tr><td rowspan="6">Centralized (Production)</td><td>200K</td><td>10 GB</td><td rowspan="6">Minimum: 8 for 1 concurrent scan.
Additional 2 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.</td><td rowspan="2">2.8 GHz</td><td rowspan="6">250 GB (recommended)</td><td rowspan="7">Windows Server 2008R2 2012, 2012R2, 2016</td><td rowspan="6">IIS 7/7.5/8/ 8.5/10</td></tr>
<tr><td>600K</td><td>16 GB</td></tr>
<tr><td>1.2M</td><td>24 GB</td><td rowspan="4">2.8 GHz</td></tr>
<tr><td>2M</td><td>40 GB</td></tr>
<tr><td>3M</td><td>56 GB</td></tr>
<tr><td>4M</td><td>72 GB</td></tr>
<tr><td rowspan="2">Distributed - CxEngine (Production) For multiple</td><td>200K</td><td>6 GB</td><td rowspan="2">4 (for 1 concurrent scan)
Additional 2 cores for each additional</td><td rowspan="2">Recommended: 2.8 GHz</td><td rowspan="2">100 GB (recommended)</td><td rowspan="2">NA</td></tr>
<tr><td>600K</td><td>12 GB</td></tr>
</table>

Purpose	Lines of Code	Installed RAM**	Cores	CPU Speed	Disk	OS	Web Server	Other Software
CxEngine servers (for concurrent scans), each server should meet the requirements	**1.2M**	20 GB	concurrent scan (Recommended: 4, 6, or 8 cores)	Recommended: 2.8 GHz				
	2M	32 GB						
	3M	48 GB						
	4.5M	72 GB						
Distributed - CxManager with Management & Orchestration Layer (Production)		14 GB	8	2.5 GHz	250 GB (recommended)		IIS 7/7.5/8/8.5/10	
Distributed - CxManager without Management & Orchestration Layer (Production)		10 GB	4	2.5 GHz	250 GB (recommended)		IIS 7/7.5/8/8.5/10	
Distributed - Database (Production)		12 GB	6-8	2.5 GHz	350-400 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.

Server Hardening Checklist

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.
The following security hardening recommendations for the Checkmarx installation are:

Checkmarx Application -

- Configure Checkmarx System Admin login from dedicated IP`s only
- Use SSL for HTTPS based browsing – prohibit using HTTP
- Use SAML based authentication for the system (replacing local users)
- If applicable – enable 2FA/MFA through the SAML IDP (Checkmarx does not support that as a feature)
- Install the Checkmarx application in a distributed mode exposing the least Checkmarx components to users as possible.

Application Hosting Servers -

- Follow NIST standard
- Use - https://www.ssllabs.com/ssltest/analyze.html for checking general security of the implementation.

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

Supported Environments

The following section describes the supported environments:

In this section

Supported Operating Systems

The following operations systems have been tested with CxSAST / CxOSA:

Windows (64-bit)	7, 8, 8.1, 10	**Windows Server**	2008R2, 2012, 2012R2, 2016 Windows Server Core is not supported

Java Version

Java	7 - 8

Frameworks

Microsoft .NET Framework	4.7.1

Webserver

IIS	7.5 - 10

Supported SQL Servers

The following SQL servers have been tested with CxSAST / CxOSA:

SQL Server

SQL	2008, 2008R2, 2012, 2012R2, 2014, 2016 * DBaaS is not supported natively; AWS RDS can be used (see AWS RDS secton in the Installing CxSAST guidelines). ** SQL Express not supported in production due to throughput and 10GB DB size limits imposed by Microsoft.

Supported Browsers

The following browsers have been tested with CxSAST / CxOSA and Codebashing:

Browsers (CxSAST & CxOSA)

Microsoft Internet Explorer	10, 11, Edge	**Safari**	6 and up
Google Chrome	43 and up	**Mozilla Firefox**	38 and up

Browsers (Codebashing)

Microsoft Internet Explorer	Edge	**Safari**	11 and up
Google Chrome	62 and up	**Mozilla Firefox**	56 and up

Supported Integrations and Plugins

The following integrations and plugins have been tested with CxSAST / CxOSA:

IDE Plugins

Eclipse	4.6 (Neon), 4.7 (Oxygen), 4.8 (Photon)	**IntelliJ**	11 - 16, 2017, 2018, 2018.2.3 (Community Edition) Windows, Mac OS X (El Capitan and greater)
Visual Studio	2012, 2013, 2015, 2017, 2017 (Enterprise)		

Build Servers

Jenkins	2.60 – 2.165
Jenkins (Pipelines)	2.x or later (1.6 - 2.0 not supported)
TFS / VSTS (Azure DevOps)	2013, 2015, 2017, 2018 Update 3 (Supports Windows agents only)
Bamboo	5.9 - 6.8
TeamCity	2017.1.1 and up, 2018.1.2

Integration

Jira	5.0 - 7.0
SonarQube (Widget)	4.5.4 - 6.1
SonarQube (Plugin)	6.3 - 6.7
Apache Maven	3.0 - 3.25, 3.3.9

Preparing the Environment for Releases

The following sections include the environmental preparations needed for releases:

In this section

- Preparing the Environment
- CxSAST Server Components Installed on Dedicated Hosts

Preparing the Environment for CxSAST

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 for CxSAST, make sure the following services are running:
    - SQL Server (for CxSAST)
    - SQL Server Browser

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

4. If using SQL Server for CxSAST, make sure the following services are running:
    - SQL Server (for CxSAST)

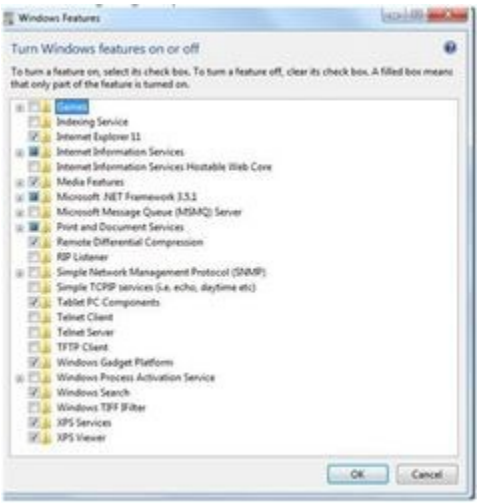
- SQL Server Browser

5. On server component hosts, prevent antiviruses from scanning the Checkmarx folder, usually:
   - **C:\CxSrc, C:\ExtSrc, C:\CxReports**
   - Checkmarx installation directory: **C:\Program Files\Checkmarx** - **C:\Program Files(x86)\Checkmarx**
6. 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 7

1. Open the Control Panel.
2. In **Programs**, click **Uninstall a program**.
3. Click **Turn Windows features on or off**:



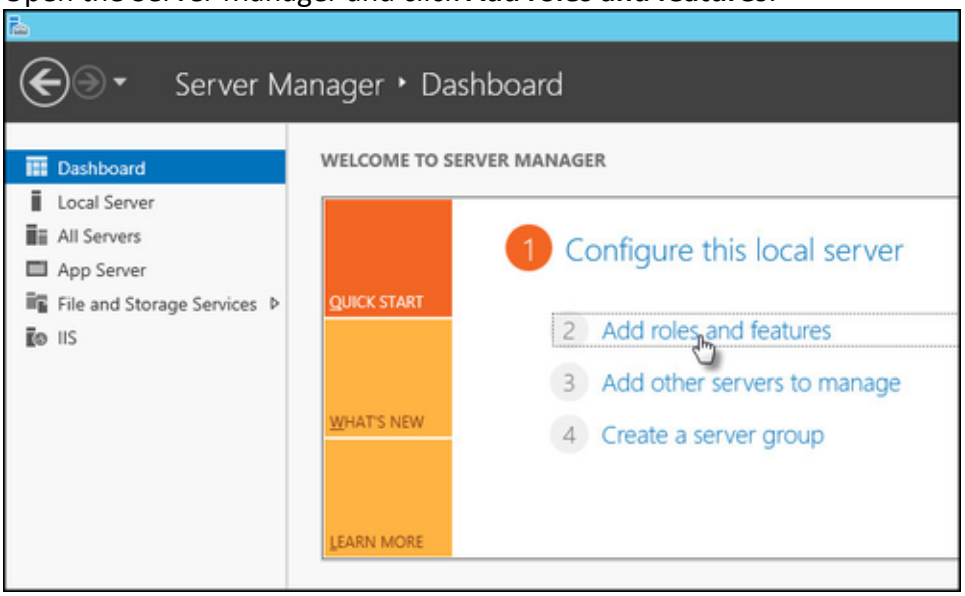
4. In **Internet Information Services**, select the following:
   - In **Web Management Tools**:
     - **IIS Metabase and IIS 6 Configuration Compatibility**
     - **IIS Management Console**
   - **World Wide Web Services** > Application Development Features > **ASP.NET** (Click OK to approve all dependent features)
   - **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:

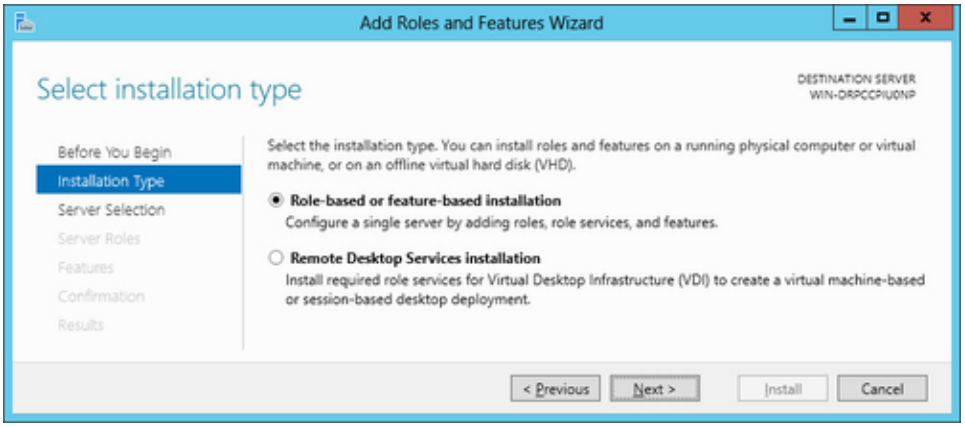
```
ServiceModelReg.exe -ia
```

Configure IIS 8 on Windows Server 2012

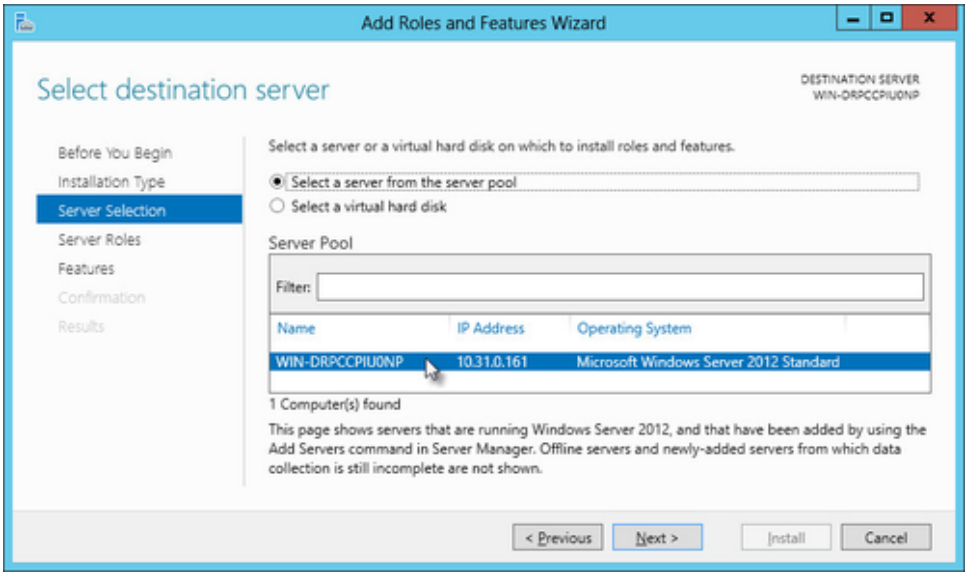
1. Open the Server Manager and click **Add roles and features**:



2. Select **Installation Type**, and select **Role-based or feature-based Installation**:

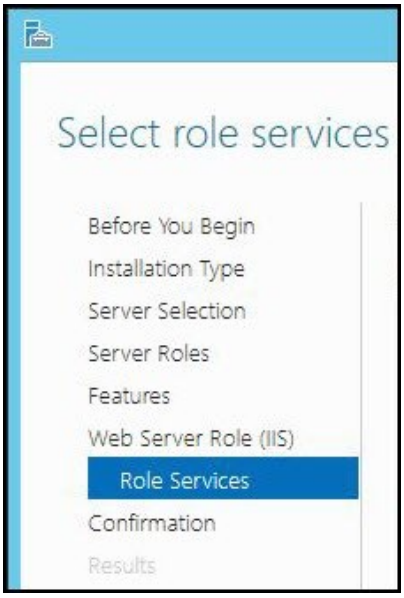


3. Click **Next**.
4. Select the server:



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:

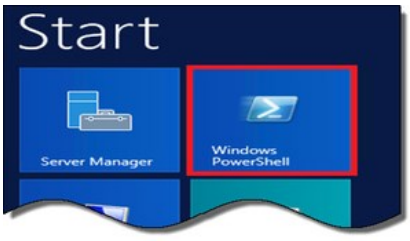
   - Common HTTP Features **> Static Content**
   - Application Development > **ASP.NET 4.5**
   - Management Tools > **IIS Management Console**
   - Management Tools > IIS 6 Management Compatibility > **IIS 6 Metabase Compatibility**
10. **Finish** the wizard, confirm and **Install**.

Configure IIS 8.5 on Windows Server 2012 R2

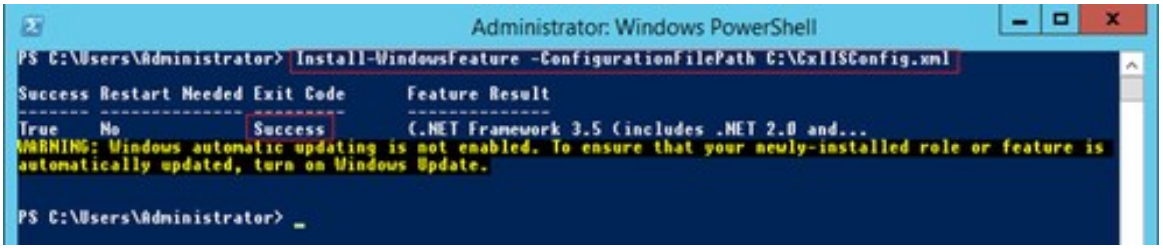
For IIS 8.5, Checkmarx provides a configuration file that can be used to automatically perform all necessary configuration. Alternatively, you can manually install IIS, in which case make sure to include IIS with - IIS Management Console, Static Content, ASP.NET 4.5 with all dependencies, IIS 6 Metabase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

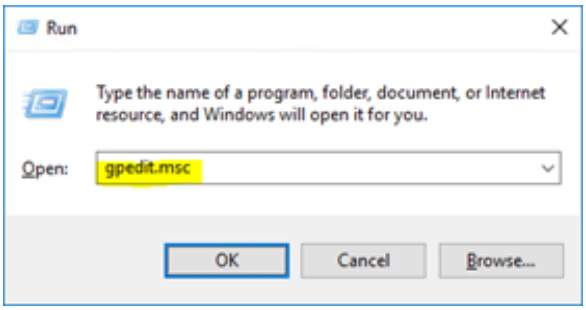


- For correct synchronization the Checkmarx Server/CxAudit and the Database must be on the same time zone.

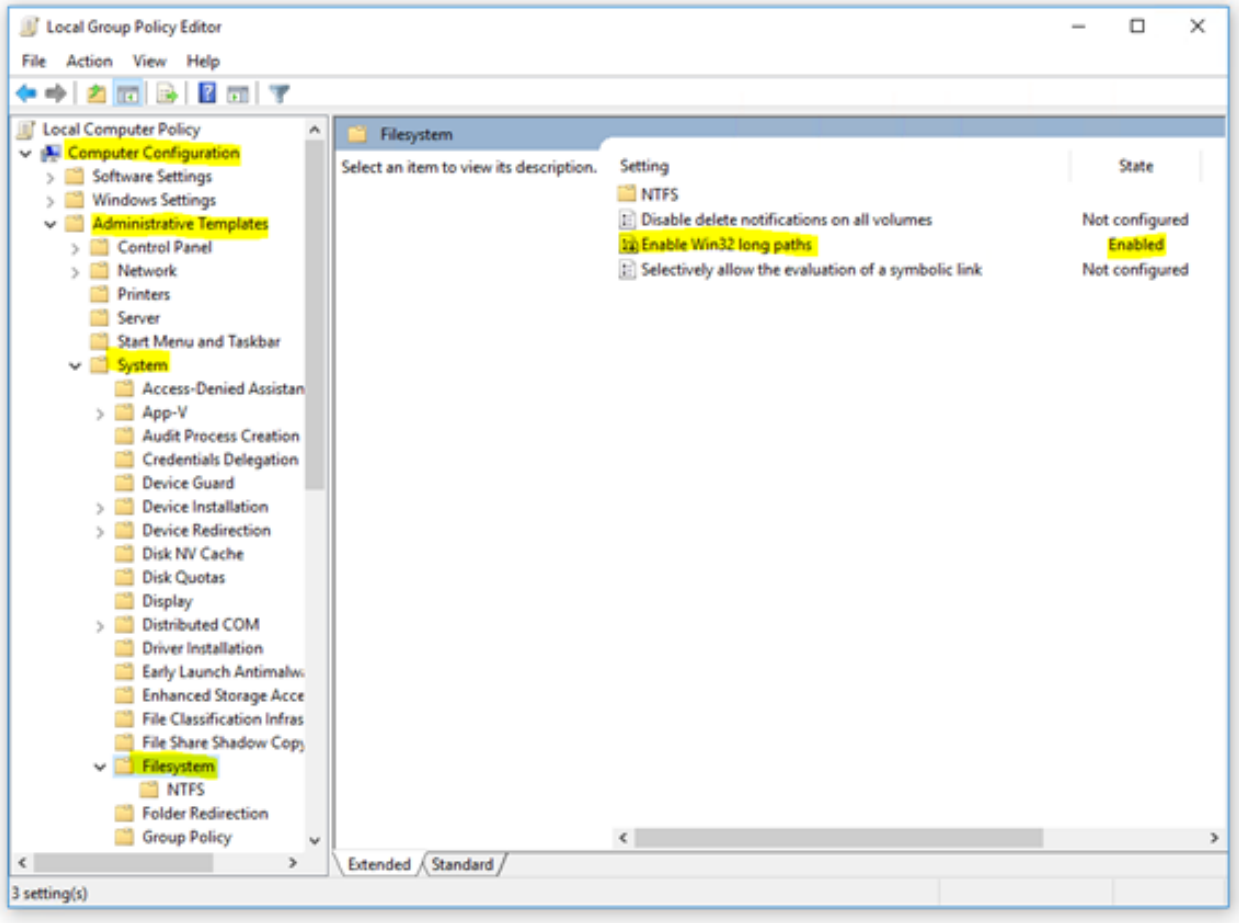
Enable Long Path Support in Windows 10 and Server 2016

Traditionally, Windows operating system didn't support path or filename with more than 260 characters. However, Windows 10 and Windows Server 2016 now present support for this issue.

In Windows 10/Server 2016, open the Run dialog (Start > Programs > Accessories > Run). The Run dialog is displayed.



Open the Local Group Policy settings by the typing gpedit.msc in the Run dialog. The Group Policy Editor is displayed.



Navigate to: Local Computer Policy > Computer Configuration > Administrative Templates > System > Filesystem.

Enable the Enabling Win32 long paths key. The key updates instantly and no restart is required.

■ Long Path support in Windows 10 starts from build 14352 or higher.

Preparing the Environment for CxOSA

Definitions for preparing the environment are currently dependent on the requirements defined for the CxSAST installation. For more information specific CxOSA requirements, see Preparing the Environment for CxOSA.

CxSAST Server Components Installed on Dedicated Hosts

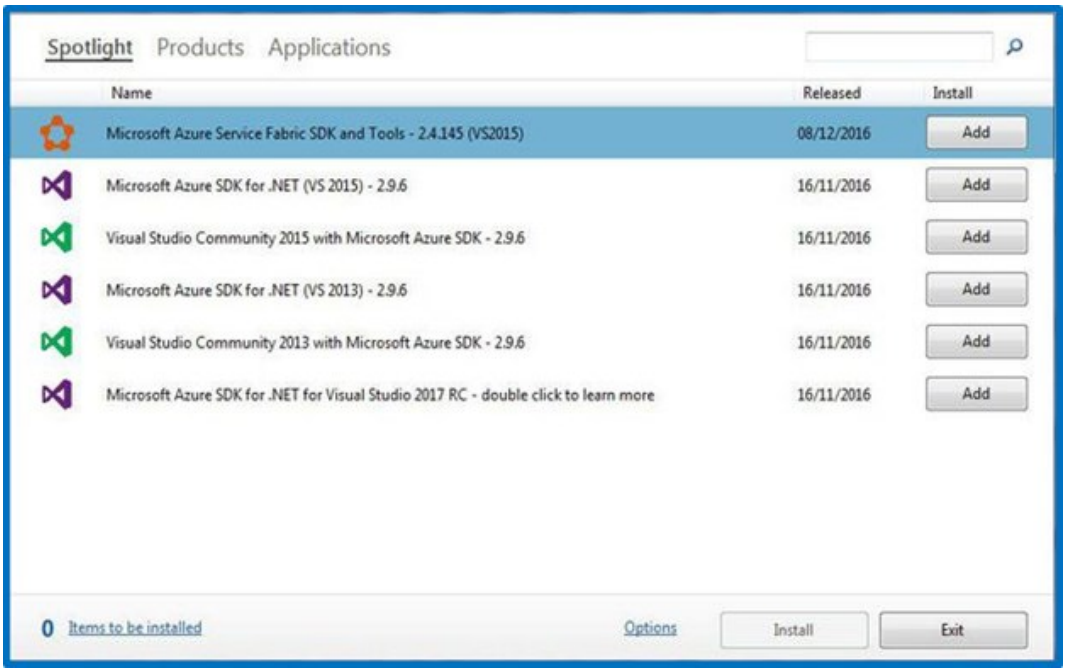
CxSAST supports Distributed Architecture, where any or all of the CxSAST server components are installed on dedicated hosts.

The following procedure should be implemented in all installations or upgrades to any version that includes the new IIS application (8.1.0 and up).

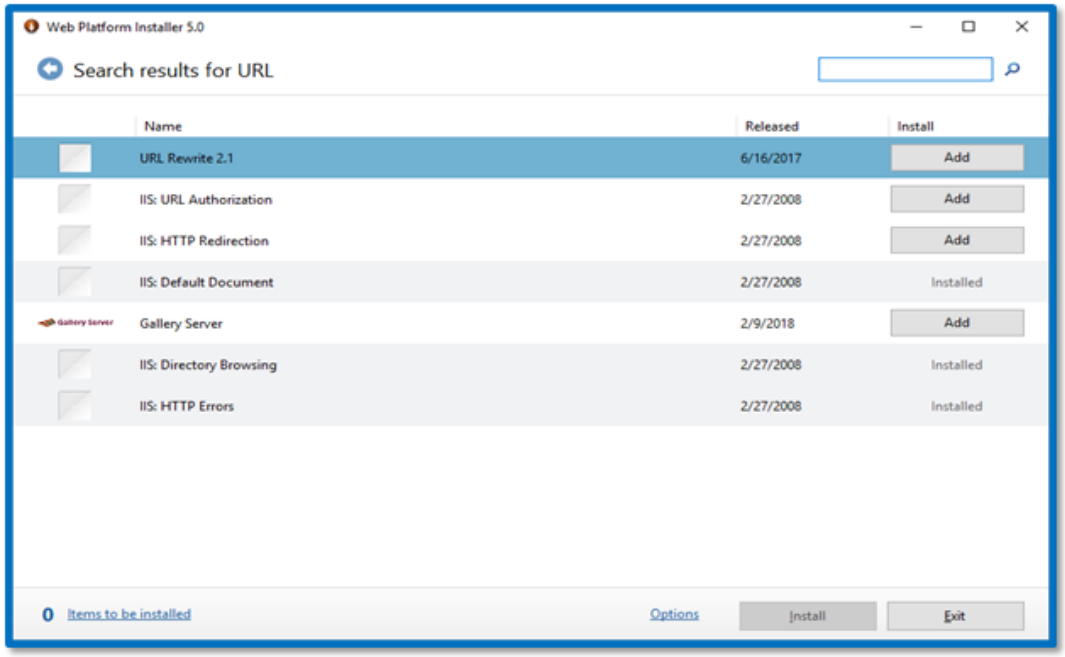
Once the IIS application components of the CxSAST setup have been installed, perform the following procedures:

Go to the Microsoft Web Platform Installer and click Install this extension to download the installation file.

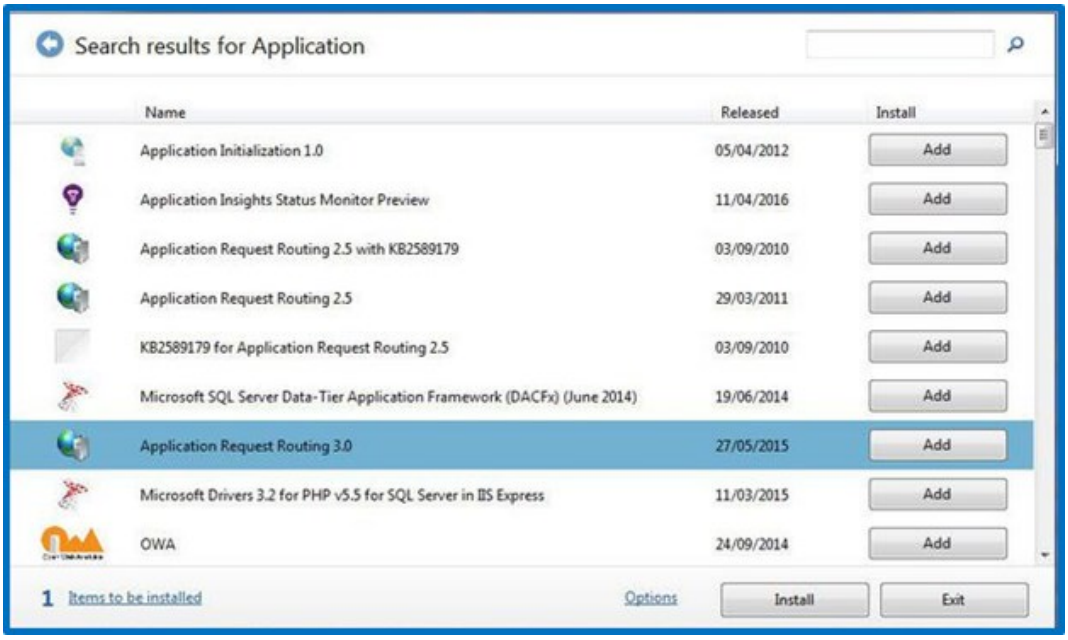
Run the Microsoft Web Platform Installer 5.0 on the Portal Server. The Microsoft Web Platform Installer is displayed.



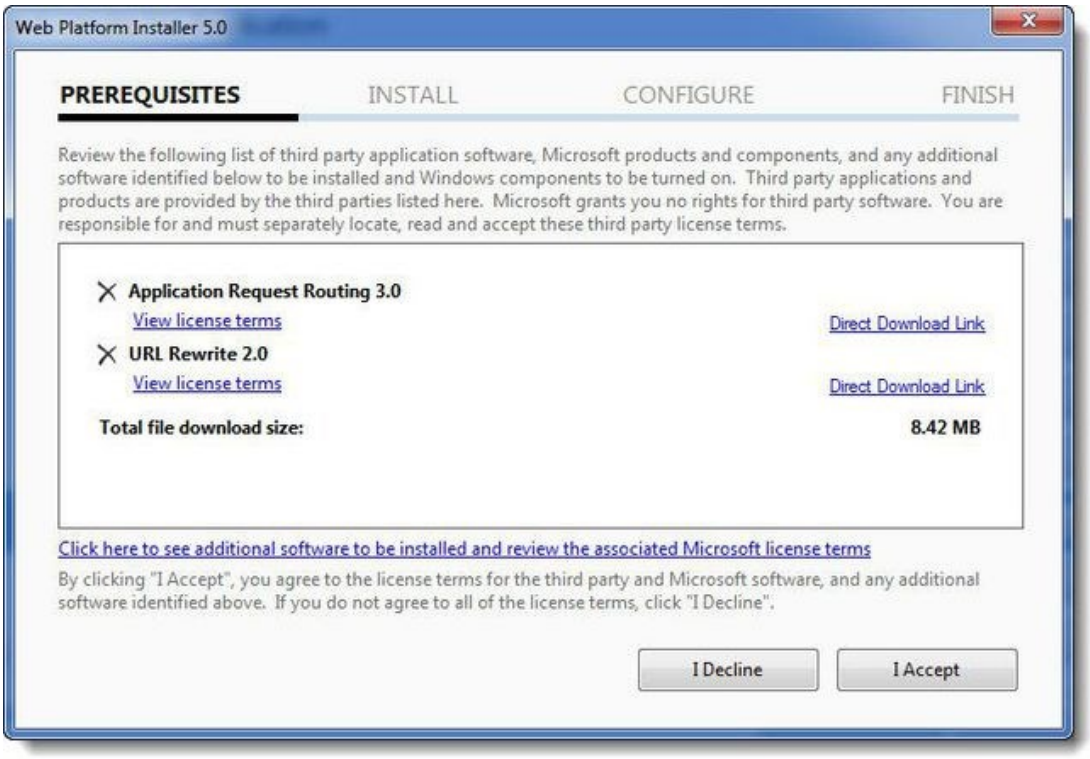
Search for the **Add URL Rewrite 2.0** module and click **Add**.



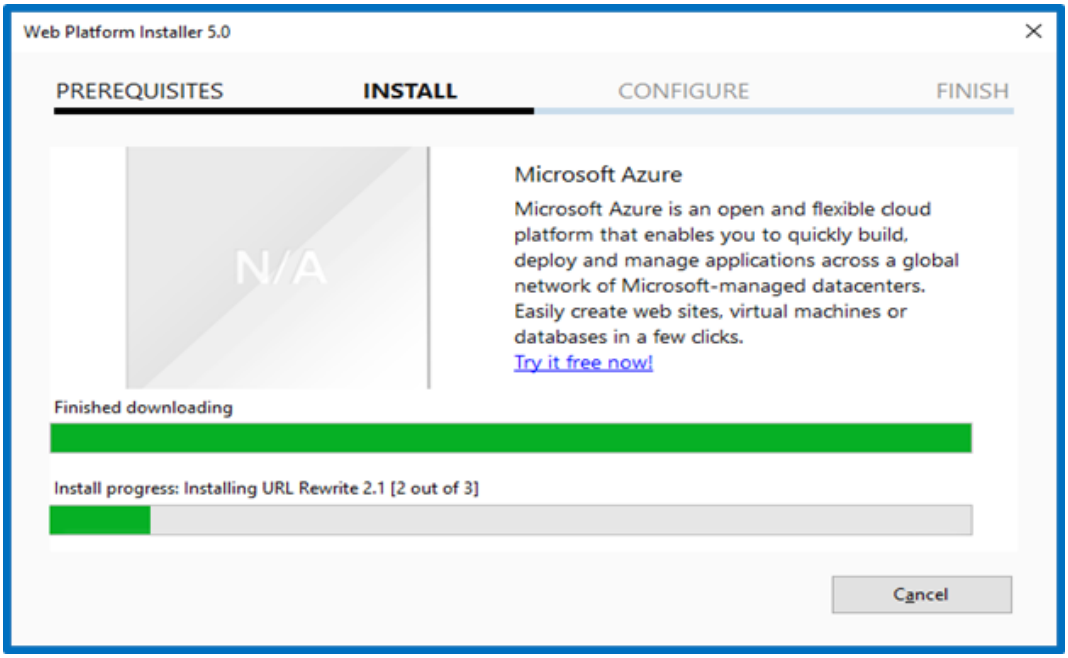
Search for the **Application Request Routing 3.0** module and click **Add**.



Click Install. The prerequisites for Web Platform Installer 5.0 are displayed.

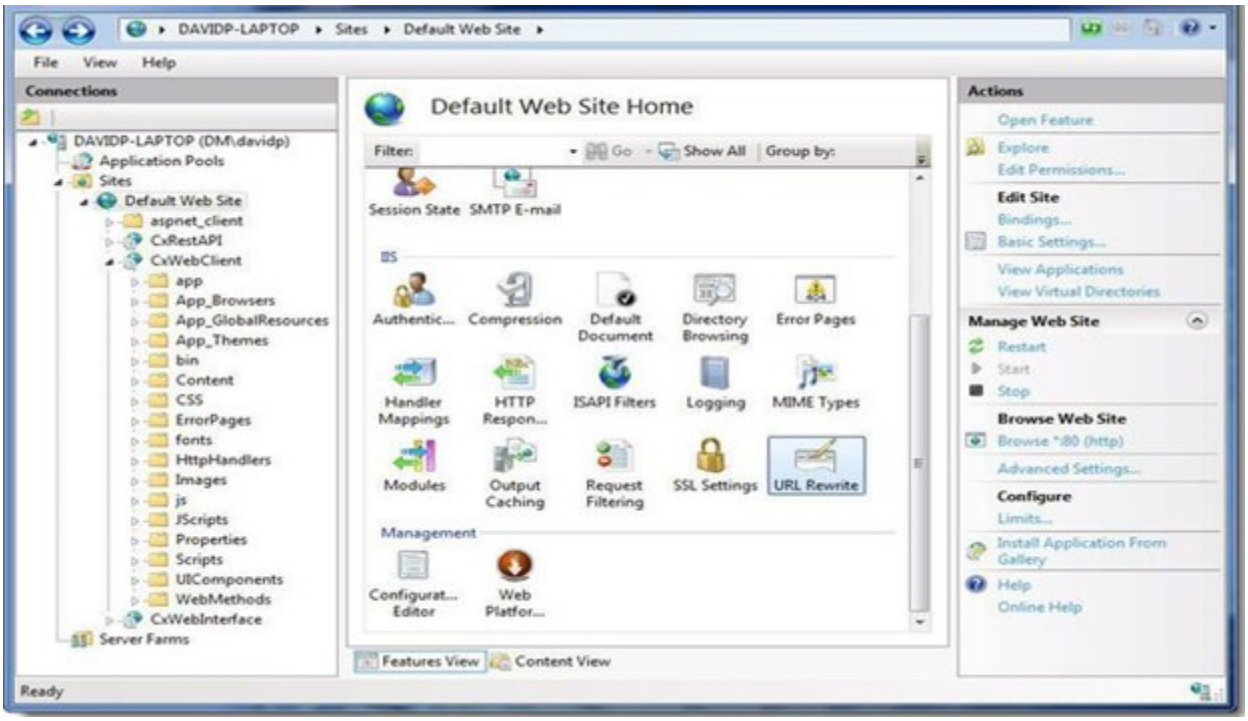


Click I Accept. The installation progress is displayed. You are notified upon successful installation.

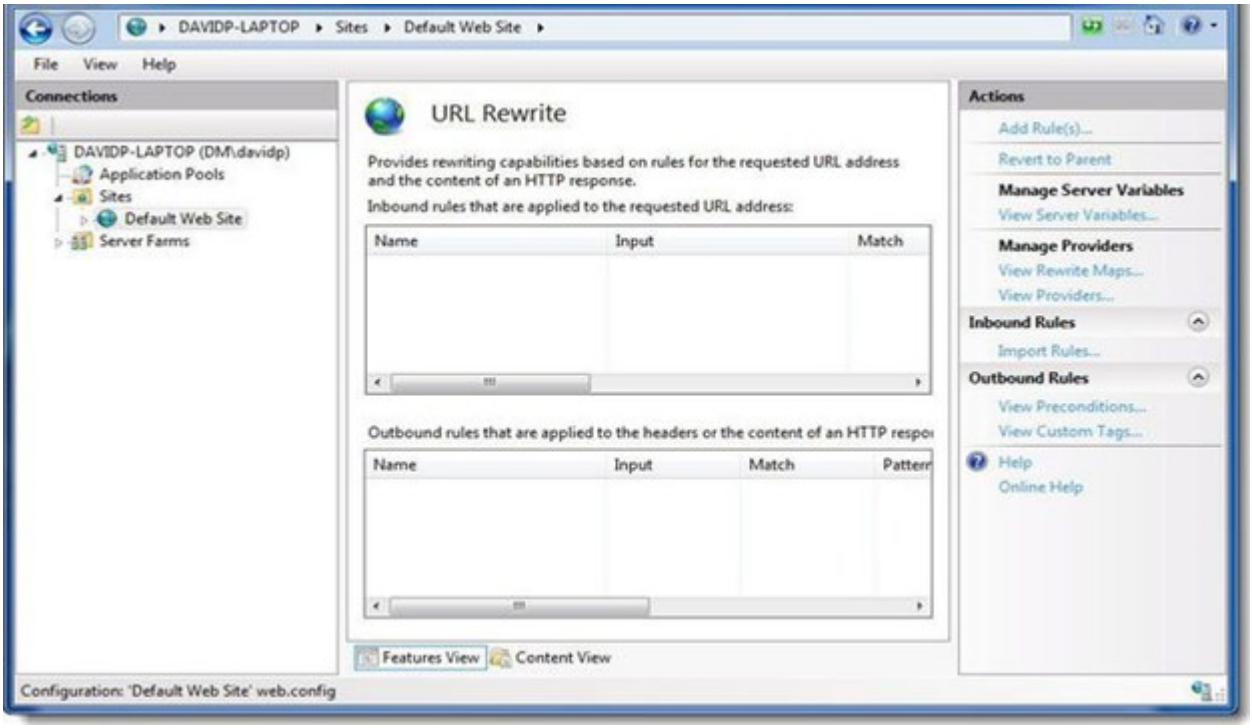


Click Finish.

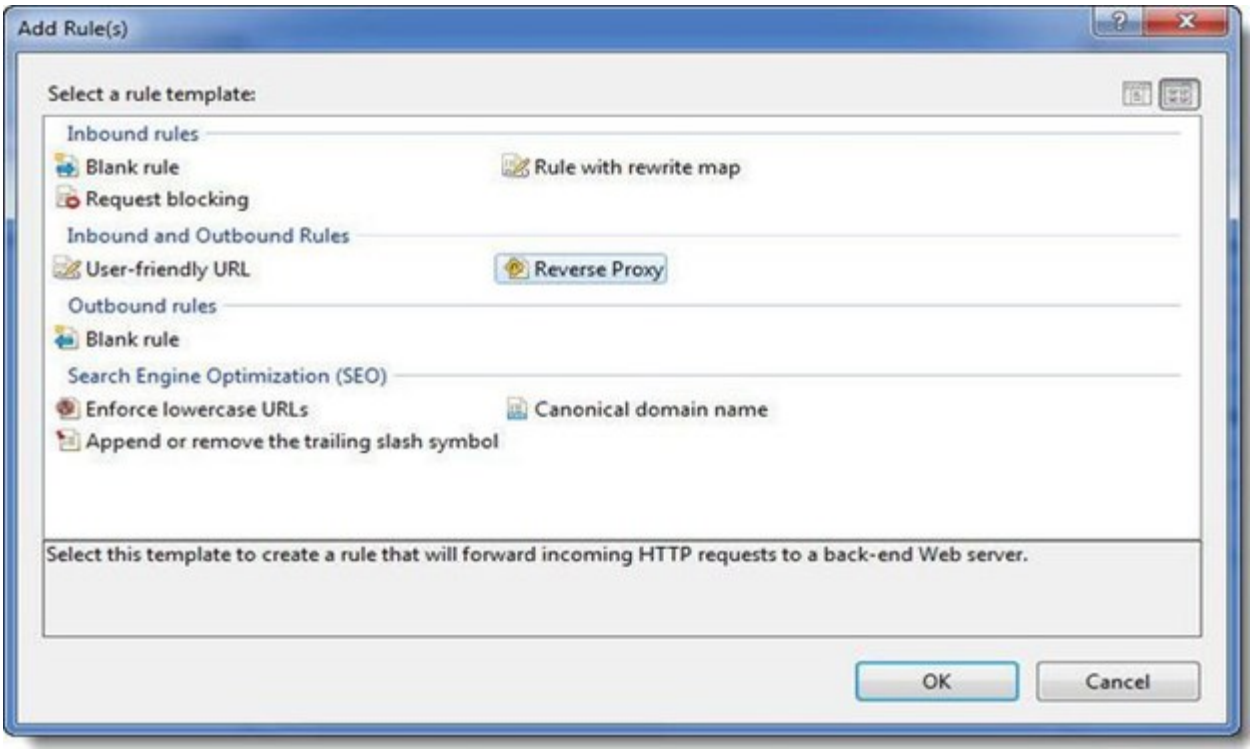
Open the Internet Information Services (IIS) Manager on the Portal Server (IIS Manager > Sites > Default Web Site > IIS > URL Rewrite).



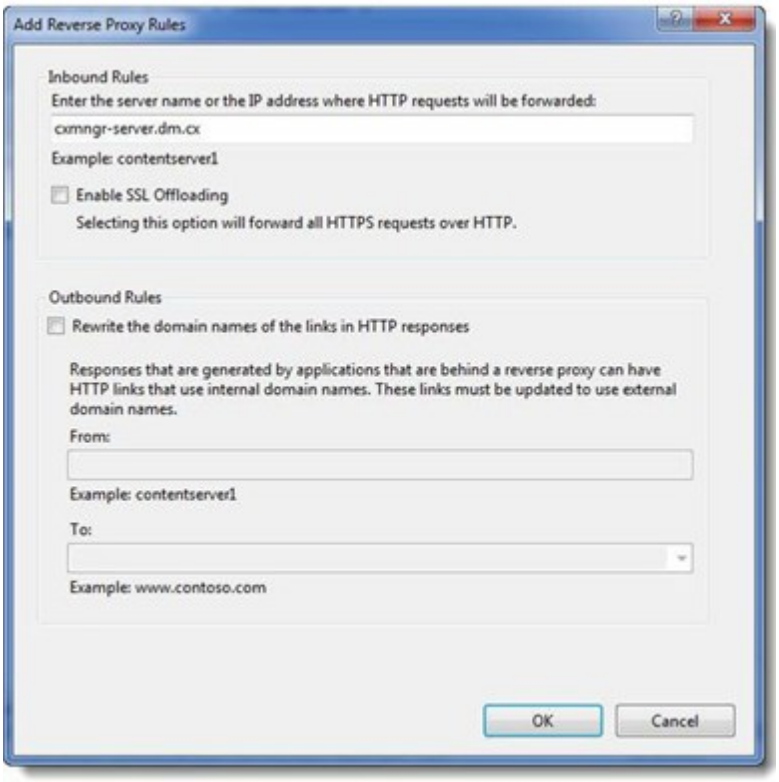
Select **Open Feature**. The **URL Rewrite Rule** is displayed.



Select **Add Rule(s)**. The **Rule Templates List** is displayed.



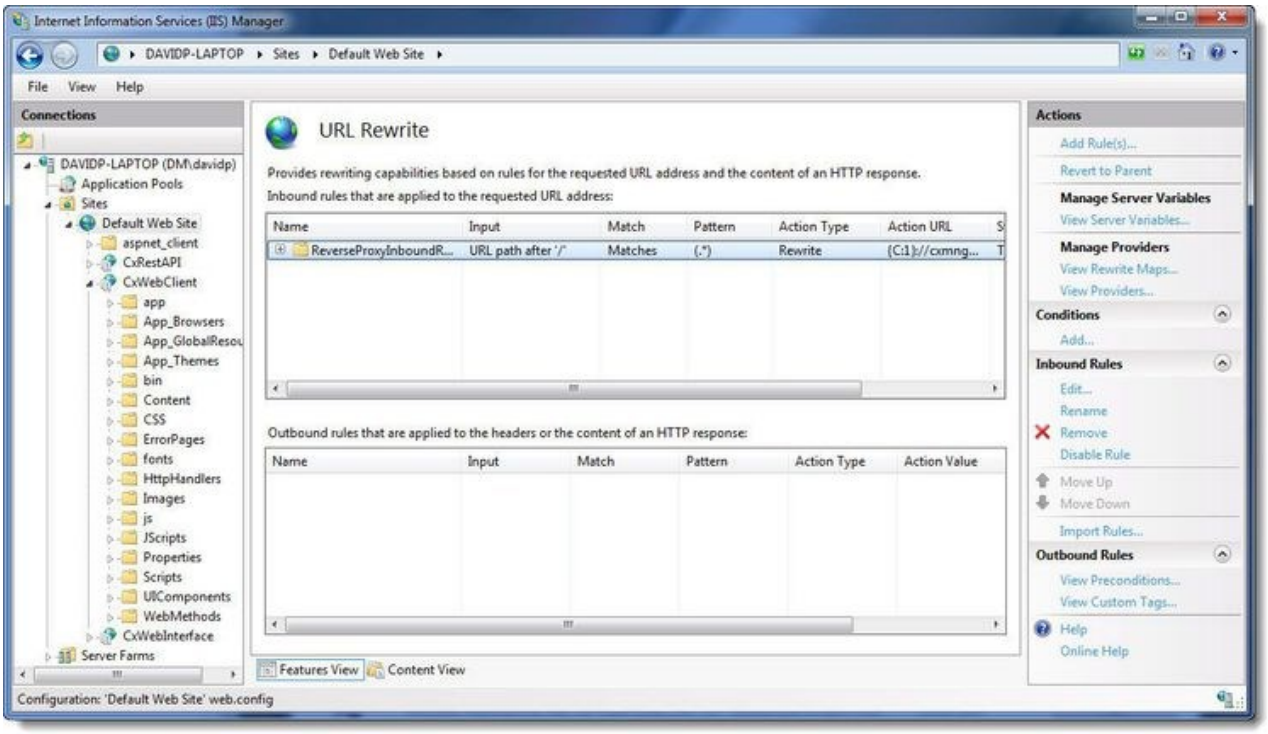
Select **Reverse Proxy**. The **Rule Template** is displayed.



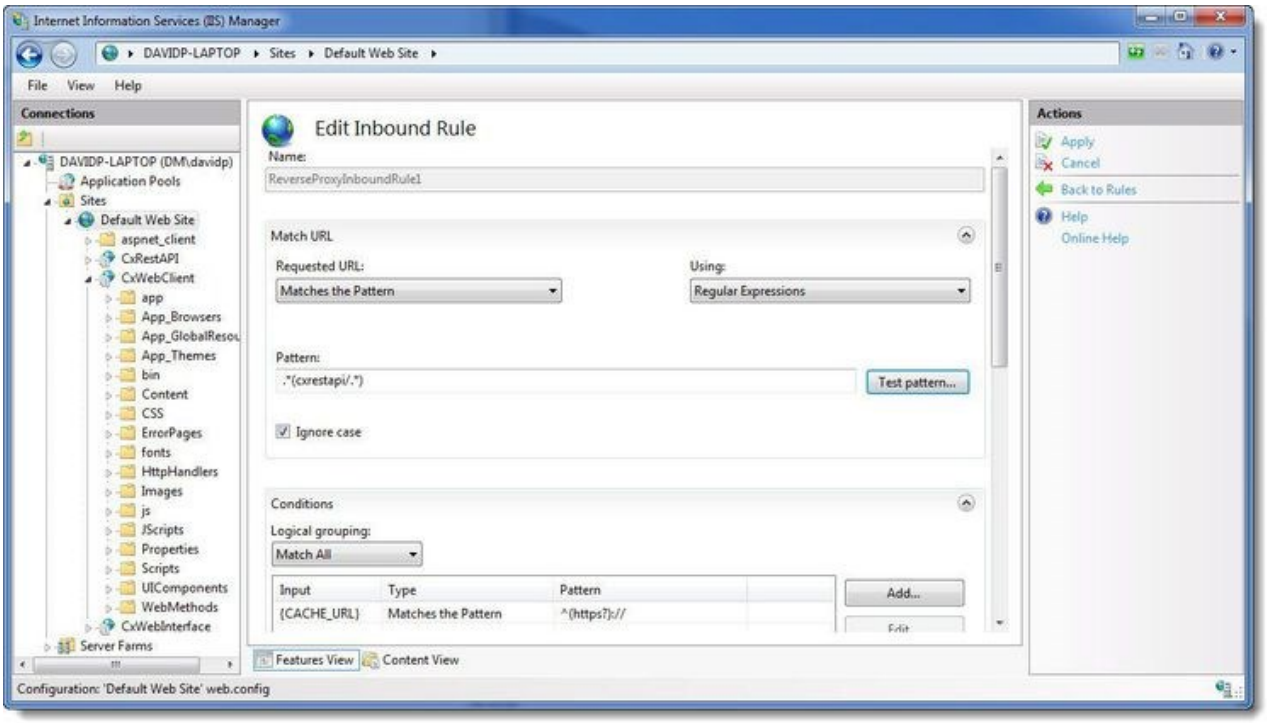
Enter the **CX Manager Server** name into the **Inbound Rules** field (e.g. cxmngr-server.dm.cx).

Disable the **SSL Offloading** option.

Click **OK** to save the changes.

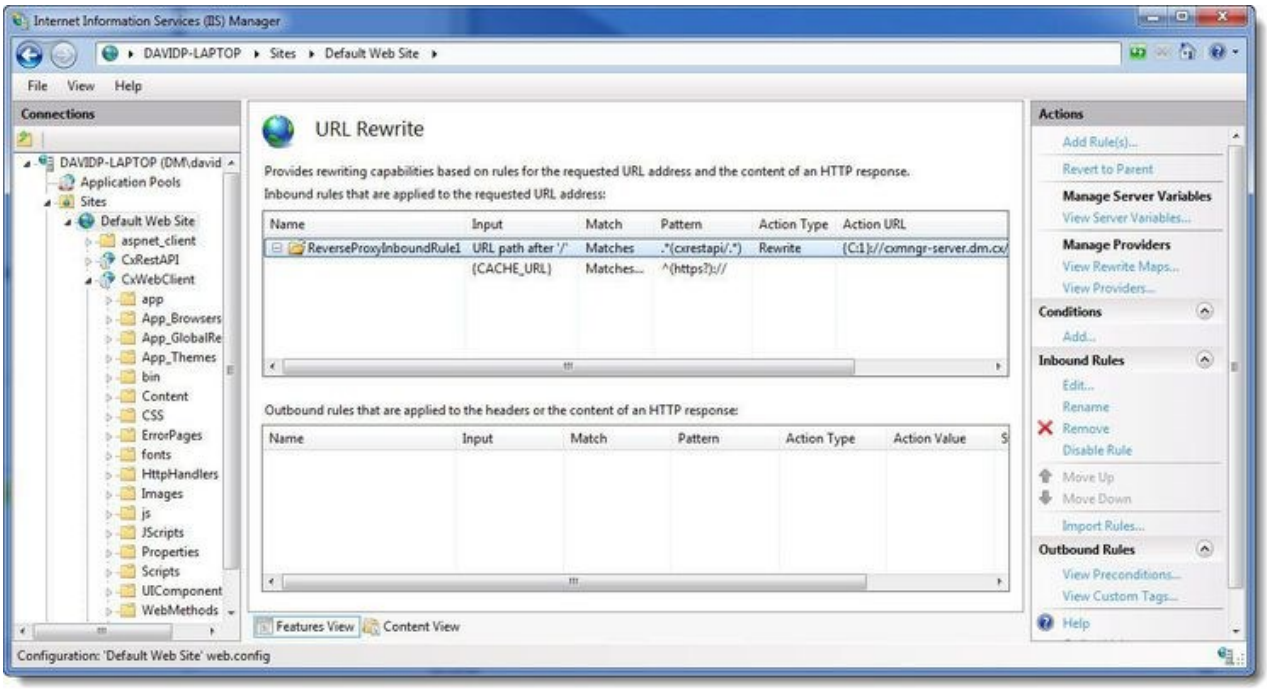


Select the newly created Rule and under Inbound Rules (right pane), click Edit. The Edit Inbound Rule window is displayed.



Change the **Pattern** to .*(cxrestapi/.*) and click **Apply**.

Verify the changes in the URL Rewrite rule.



On the Web portal machine (directory: C:\Program Files\Checkmarx\CheckmarxWebPortal\Web) open ‘web.config’ file in editor and update the

following the value of “CxWSResolver.CxWSResolver”with the Manager server IP/domain name.

Example:

from....

<add key="CxWSResolver.CxWSResolver" value="http://localhost:80/Cxwebinterface/CxWSResolver.asmx" />

to....

<add key="CxWSResolver.CxWSResolver" value="http://manager-domain-name.com/Cxwebinterface/CxWSResolver.asmx" />

```
<add key="CxPortalDefaultCulture" value="en-US" />
<add key="CxEnableIncrementalScan" value="true" />
<add key="CxUnicodeFont" value="Arial Unicode MS" />
<add key="CxWSResolver.CxWSResolver" value="http://[redacted]/Cxwebinterface/CxWSResolver.asmx" />
<add key="EnableIssueTracking" value="true" />
<add key="enableScriptBundleAndMinification" value="true" />
<add key="appSecCoachEnabled" value="true" />
```

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 installation environment.

Prior to installing CxSAST, if not already installed on the server host, install the following prerequisites, which are included in the installation zip file ("third party" folder):

- IIS (Windows 7 or greater) - see the OS-specific instructions (IISInstallationProcess.rtf file)
- MS SQL
- VC++ Runtime Redistributable

For more information, see server host requirements.

■ If you're interested in configuring a High Availability solution contact Checkmarx support.

■ If your portal is installed on a separate machine from manager, please perform the procedure **CxSAST Server Components Installed on Dedicated Hosts.**

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 machine with the product installed on it must be added to a Windows domain. In addition, 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 three SQL databases using the names; CxDB, CxActivity and CxARM.
- Create login for Windows User and associate it with DB_owner permission for CxDB, CxActivity and CxARM. This user should be a dedicated Service user and the same user must perform the installation, see **Configuring CxSAST for use with a non-default user (Network Service) - CxServices & IIS Application Pools** 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 three SQL databases using the names CxDB, CxActivity and CxARM.
- Create login for SQL User and associated it with the DB_owner permission for CxDB, CxActivity and CxARM. 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, CxActivity and CxARM.

■ **AWS RDS**

DBaaS is not supported naively. but AWS RDS can be used - To make RDS work you need to create three databases, CxDB, CxActivity and CxARM. Give the user that you created for Checkmarx dbo privileges to the newly created databases. Run the installer again and when the installation connects to the Database and you see a message about the three databases already existing, just click continue. Once the installation is complete the RDS should work.

Setting Up CxSAST

License Validation

It is recommended to obtain a license before you start your installation. This way you will not have to stop the installation in order to retrieve a license.

Your CxSAST license is tied to a specific machine (server); so all you have to do is to run the Cx HID Generator and a HID (hardware identification number) is provided. The HID Generator can be downloaded from the Cx Utilities page.

Please send the Hardware ID number to your technical contact or your sales manager. They will send you back your license. If you do not know who to send the Hardware ID to, please send it to support@checkmarx.com.

> If you have already installed CxSAST and have not yet obtained a permanent CxSAST 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:
    a. Extract the downloaded ZIP archive, supplying the password provided by Checkmarx support.
    b. Run **CxSetup.exe** and begin the installation.

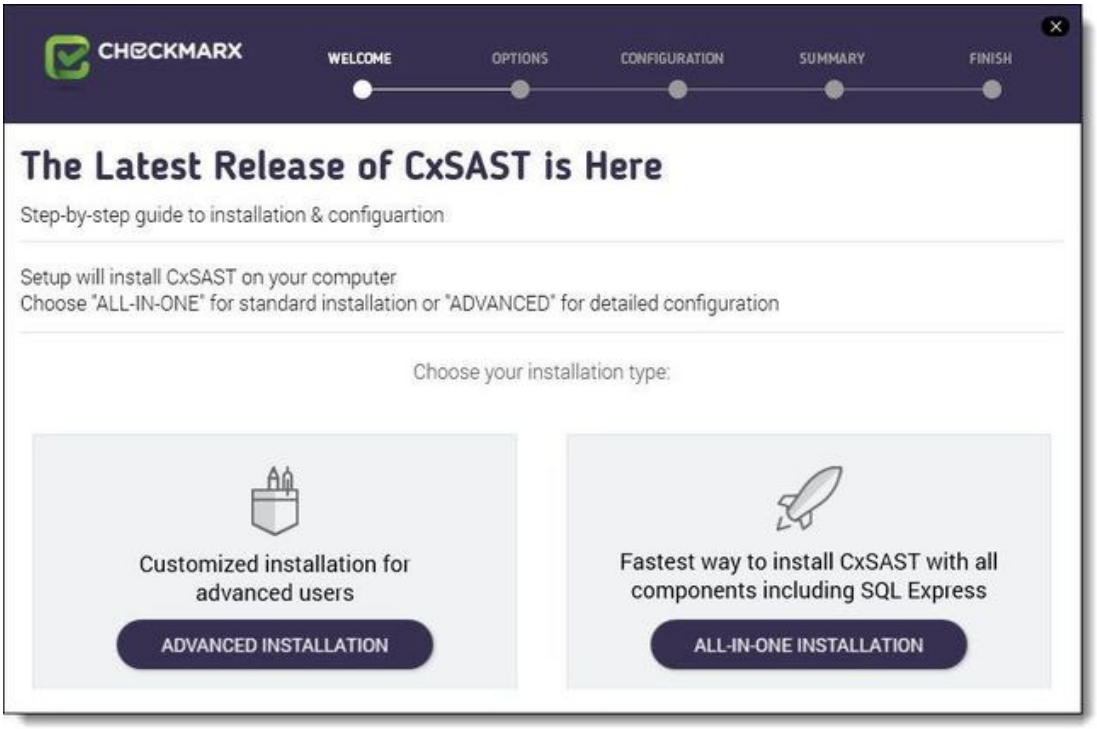
Installing CxSAST

Prerequisites and Recommendations

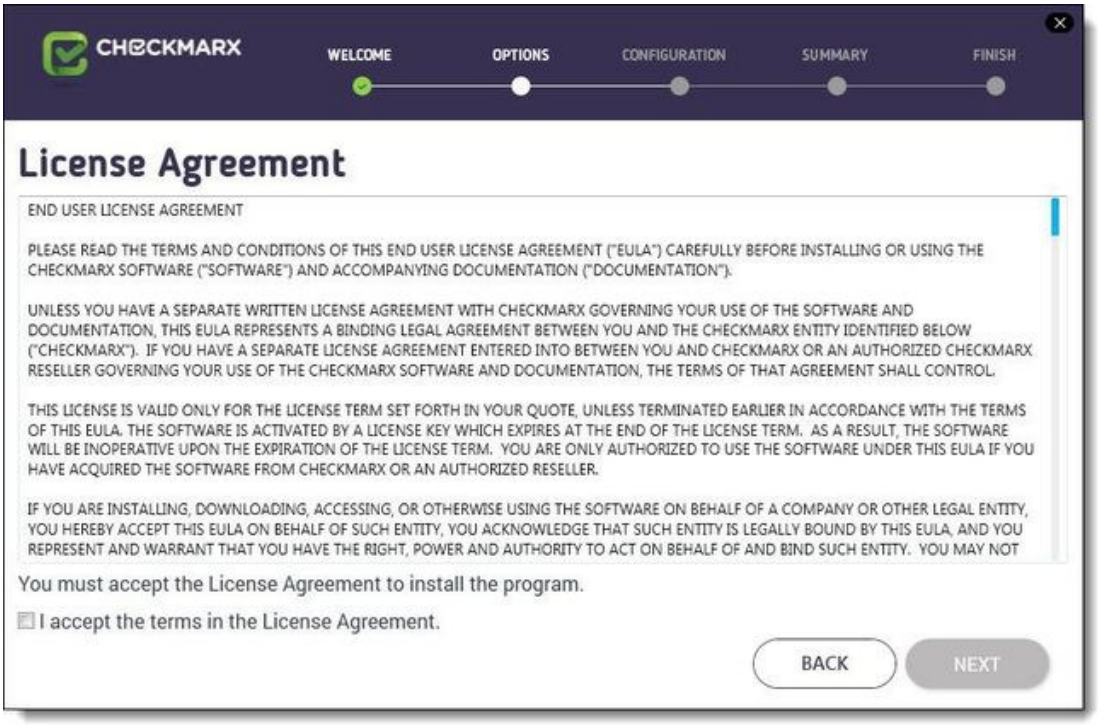
- The installer requires .Net 4.5.1 Framework installed on your server (If missing, it will be installed by the CxSAST installer).
- The required Web Server for Checkmarx is IIS Server (if missing, it will be installed by the CxSAST installer on the condition that the Windows installation media is accessible).
- SQL 2012 Express is included with 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.

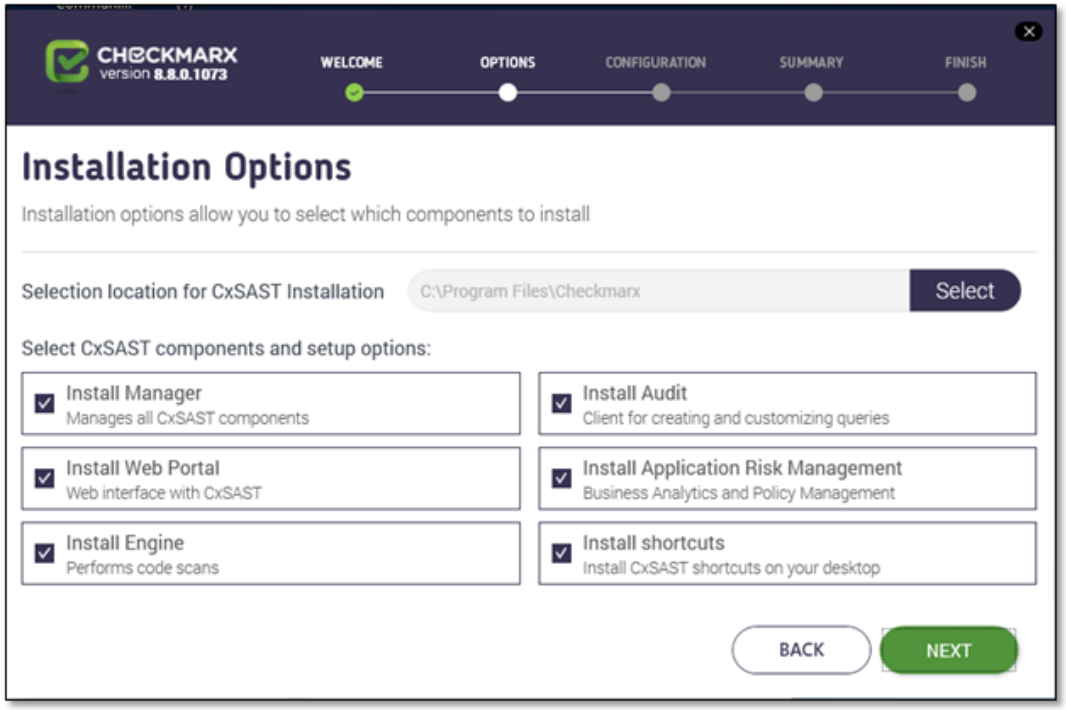


Click **ALL IN ONE** to continue, **ADVANCED** to define additional setup options, or **X** to exit. The **Checkmarx License Agreement** window is displayed.



Review and accept the license agreement by checking the '**I accept the terms in the License Agreement**' checkbox. Click **Next** to continue.

If you selected ADVANCED, the additional Installation Options window is displayed.



Click Select to define the CxSAST installation location.

Upgrade and Modify

For upgrades, previously installed location and product feature settings are loaded from the existing configuration and cannot be changed. You can however install or remove product features by using the modify feature.

Select the required product features for this installation from the available list. You can also select the option to install related shortcuts on your desktop.

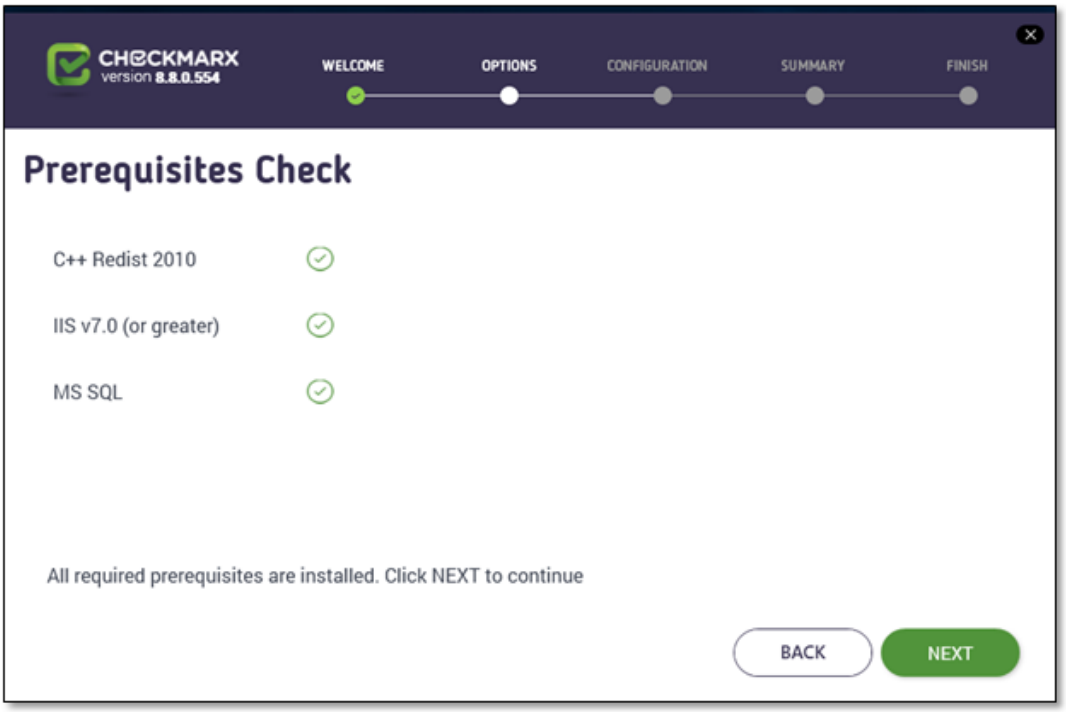
Product Feature Selection

- POC/Evaluation - Select to install Audit, Engine, Manager, Application Risk Management and WebPortal
- Distributed Architecture - Select to install either Engine or Manager, Application Risk Management and/or WebPortal
- Centralized Architecture - Select to install Engine, Manager, Application Risk Management and WebPortal (select Audit, if you plan to create and customize queries on the host)
- CxEngine Server only - Select to install Engine (see Adding a CxEngine Server).

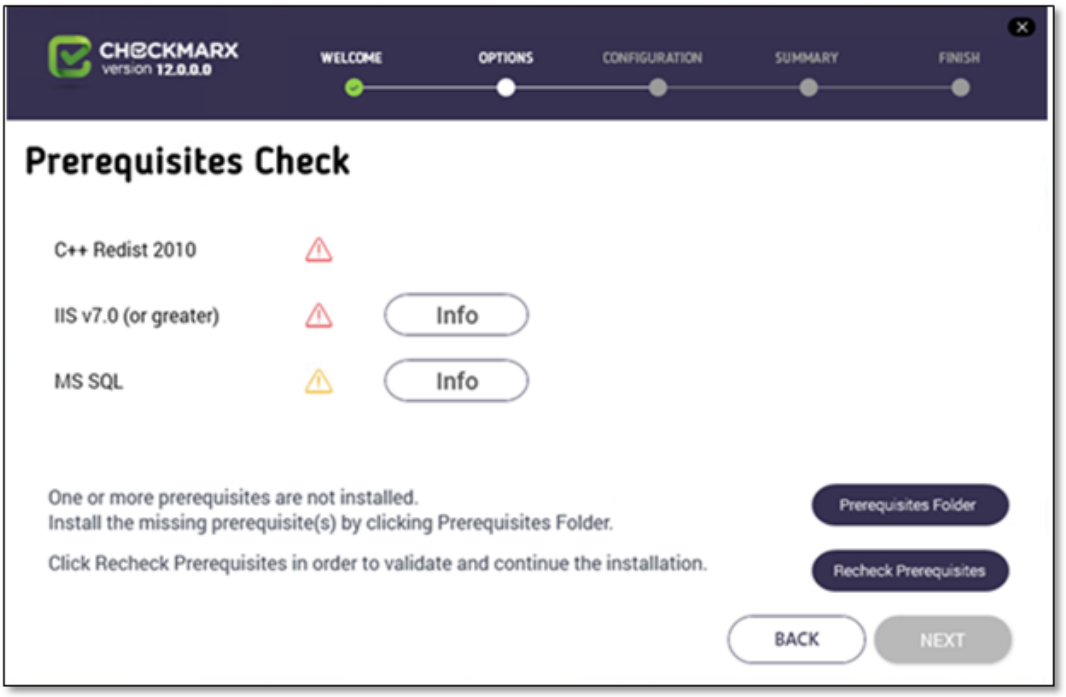
Install Application Risk Management

Checkmarx Application Risk Management (CxARM) – an application security risk management solution comprised of **CxARM Analytics** and **CxARM Policy Management** – for defining, tracking, evaluating and enforcing an organization's unified AppSec security policies, risks and status with a high level of visibility.

Click Next. The Prerequisites Check window is displayed, showing the status of all prerequisite components.

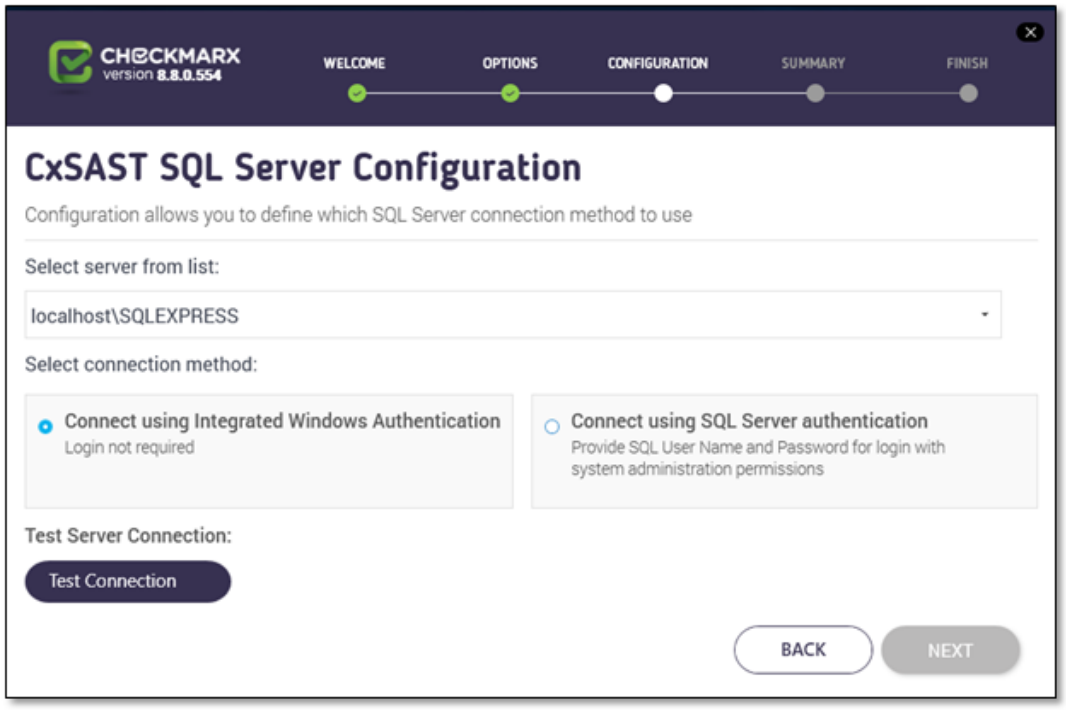


For any prerequisite not installed, click the respective INFO button for additional installation information, and then click Prerequisites Folder to install the missing component(s).



Click Recheck Prerequisites to confirm the installation status.

When all prerequisite components are installed, click Next to continue. The CxSAST SQL Server Configuration window is displayed.



For CxSAST, define a connection to the installed SQL Server or to any other SQL server on your network, by selecting one of the following:

- Connect using integrated Windows authentication (login not required)
- Connect using SQL Server authentication (provide SQL user name and password for login with SA permissions).

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

SQL Server Connection Failure

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

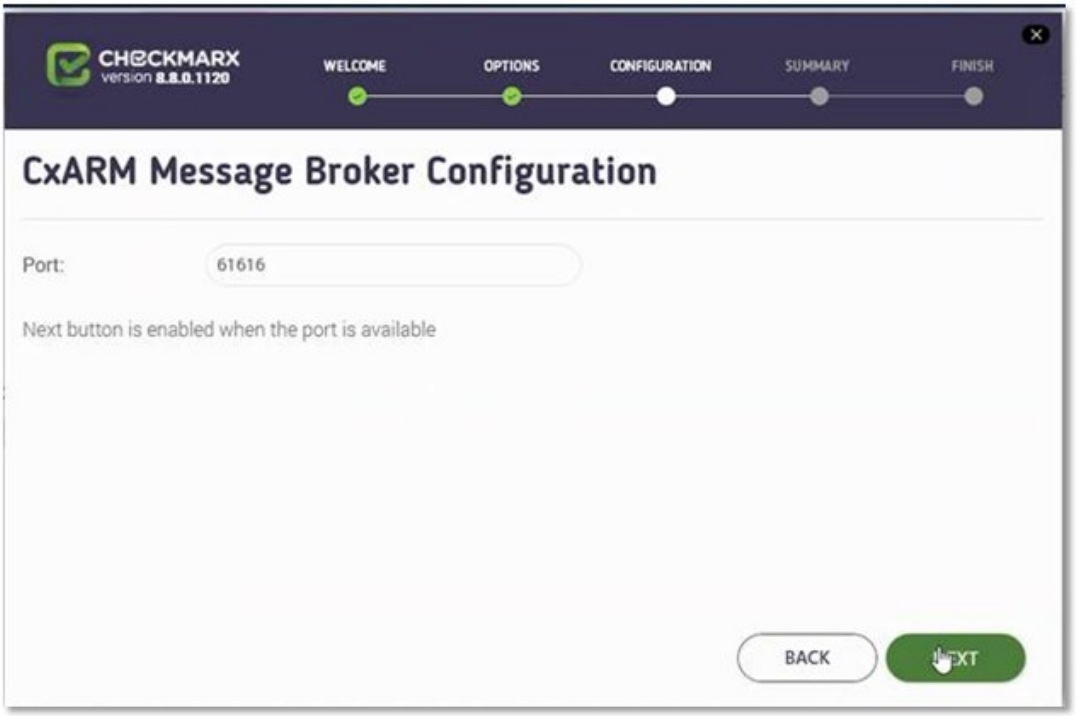
A notification displays if existing SQL Express files are detected.

Existing database detected

To continue the installation using existing SQL Server databases (CxDB and CxActivity), click OK.
To perform a clean installation of SQL Server Express, click CANCEL and manually delete the existing CxDB and CxActivity databases

Click OK on the message, and then click NEXT to continue.

If installing CxARM, the CxARM Message Broker Configuration window is displayed.

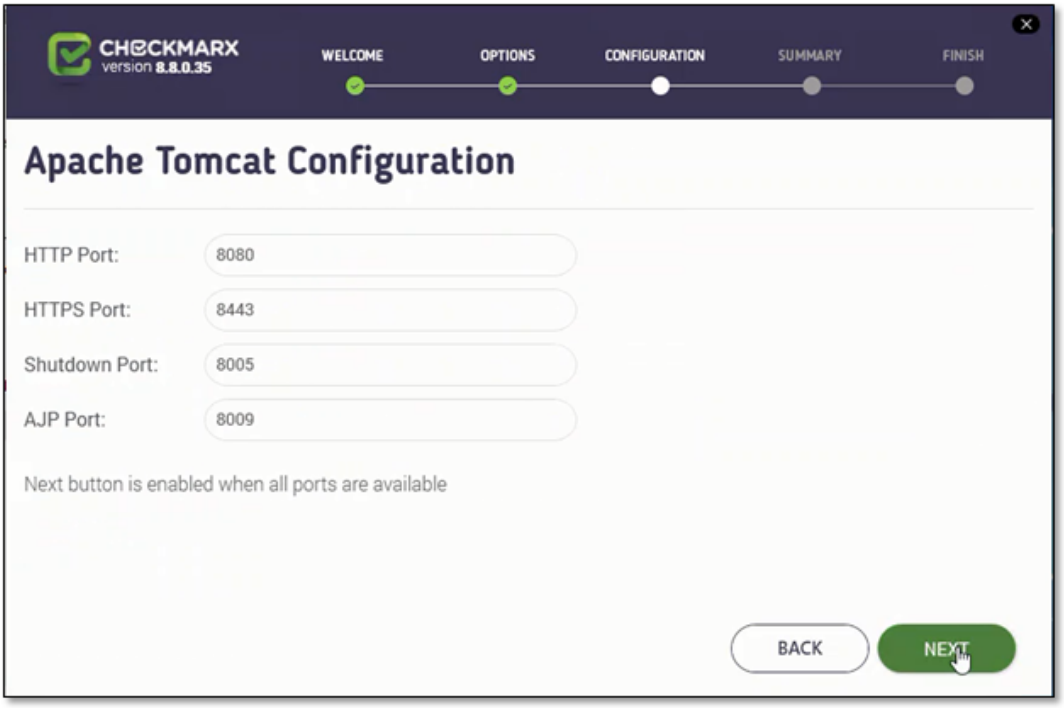


CxARM Message Broker Configuration

Default port is 61616
The NEXT button is enabled when the default port is available. If unavailable, define another available port.

Click Next.

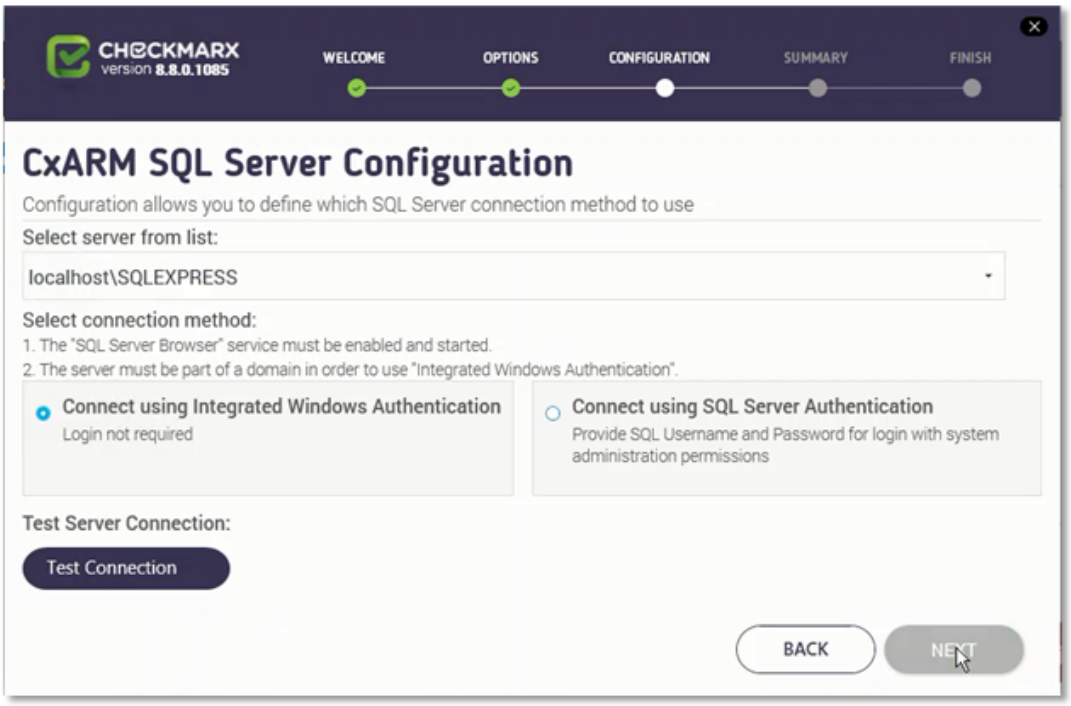
If installing CxARM, the Apache Tomcat Configuration window is displayed.



■ Apache Tomcat
Default ports are displayed The NEXT button is enabled when the default ports are available. If unavailable, define another available port in the respective Port field.

Click **Next.**

If installing CxARM, the **CxARM SQL Server Configuration** window is displayed.



For CxARM, define the SQL Server connection by selecting one of the following:

- Connect using Integrated Windows Authentication (login not required)
- Connect using SQL Server Authentication (provide SQL user name and password for login with SA permissions)

Connection Requirements

For M&O Layer SQL Server connectivity, both Dynamic and Static port configurations are now supported. See Configuring Management & Orchestration SQL Server for Dynamic and Static Port Connectivity for additional information.

The following prerequisites and recommendations are required:

- For both connection methods the SQL Server and the SQL Browser, services must be enabled and started
- For the Integrated Windows Authentication method, the server must be part of a Windows domain

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

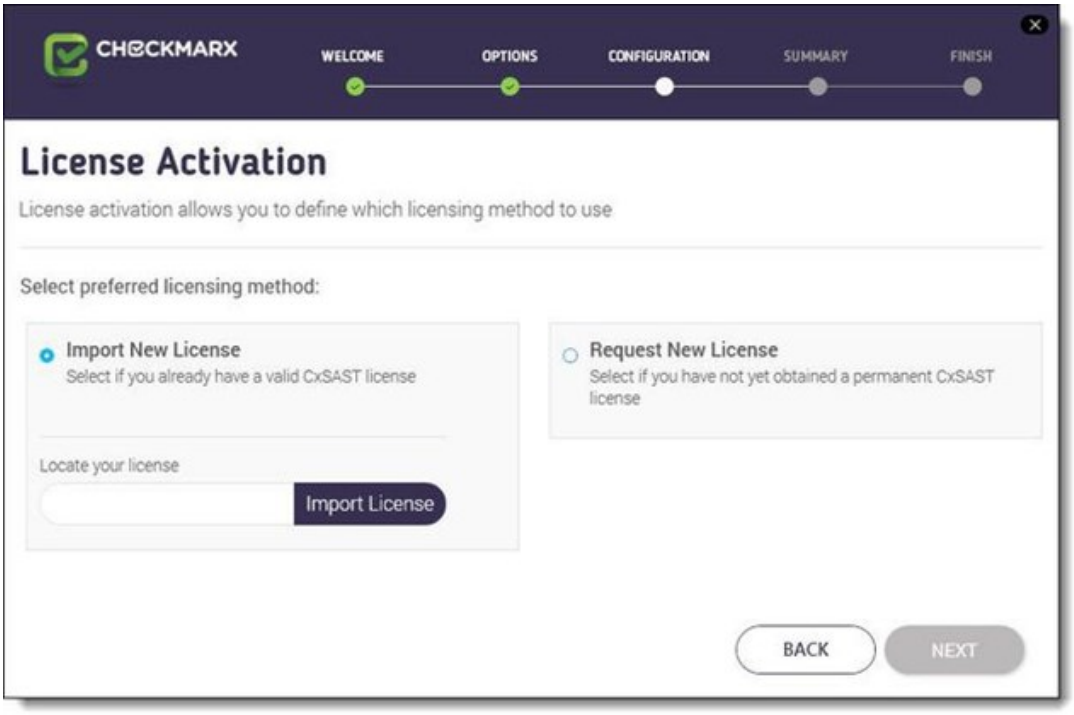
CxARM DB Connection Failure

If connection to the CxARM database fails, in order to continue with the installation, a confirmed connection is required.
If the "SQL Connection Test Results" message indicates that connection to CxARM database has failed, verify the following:

- Host, port and login credentials are correct
- The CxARM machine is a member of a Windows domain (if not, either join the machine to a domain and perform a restart, or connect using SQL Server Authentication)
- The SQL Server Browser Windows service is running (if not, enable and start it)

Click OK on the message, and then click NEXT.

The License Activation window is displayed.

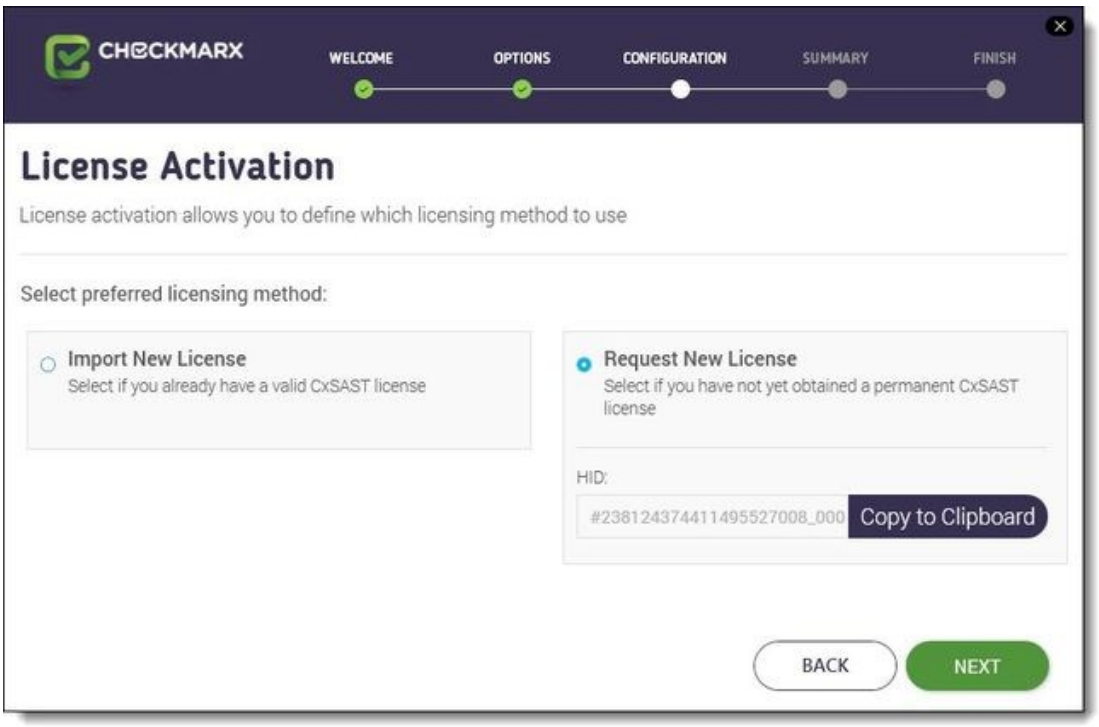


Upgrade and Existing License

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 the preferred licensing method by selecting one of the following:

- **Import new license**: If you already have a valid CxSAST license file, select the Import New License option and then click Import License Browse to the file location.
- **Request new license**: If you have not yet obtained a permanent CxSAST license. Select the Request New License option and then click Copy to Clipboard. Send the copied Hardware ID to your Checkmarx sales representative or contact Checkmarx support.



License Importer

Once you have obtained a new or updated Checkmarx license, you can use the license importer to import the license into CxSAST (see **Updating the CxSAST License**).

Click **NEXT** to continue.

HID Mismatch

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

If the default port 80 is occupied, the **Validate Port** window is displayed.

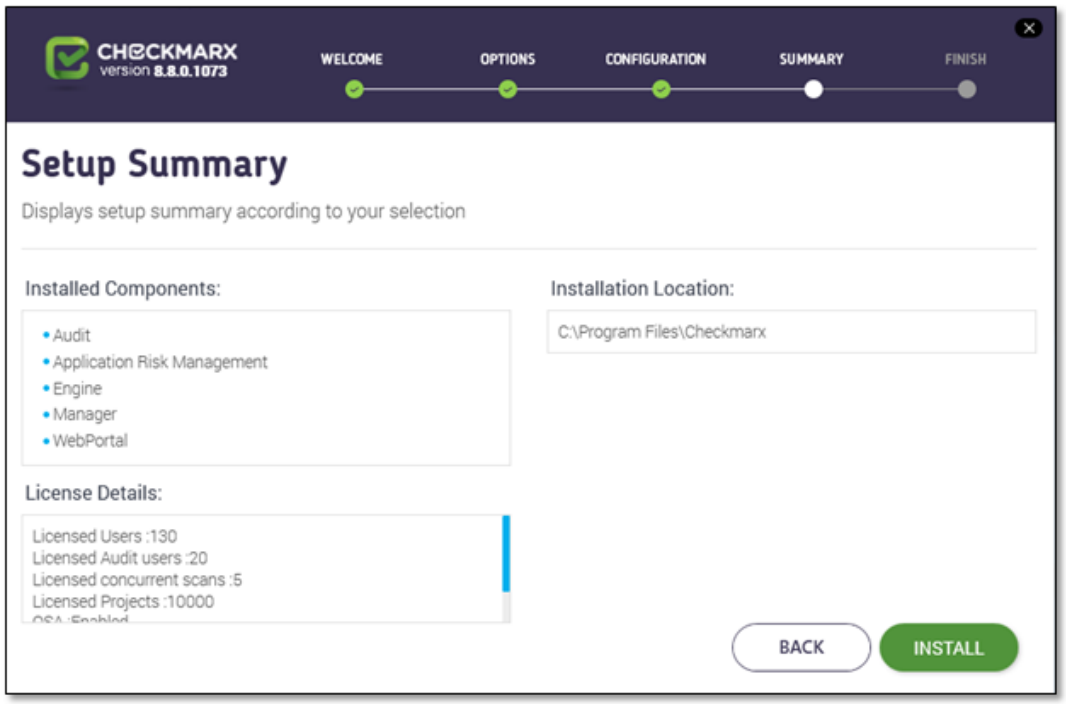
Default Port 80 Validation

Port 80 is allocated as the default port for Checkmarx applications. In clean installations the Validate Port window is displayed only if one of the following occurs:

- Port 80 is occupied by a non-default website or application
- Default website does not exist and port 80 is occupied by another application or website
- Default website does exist (occupies a different port) and port 80 is occupied by another application or website.

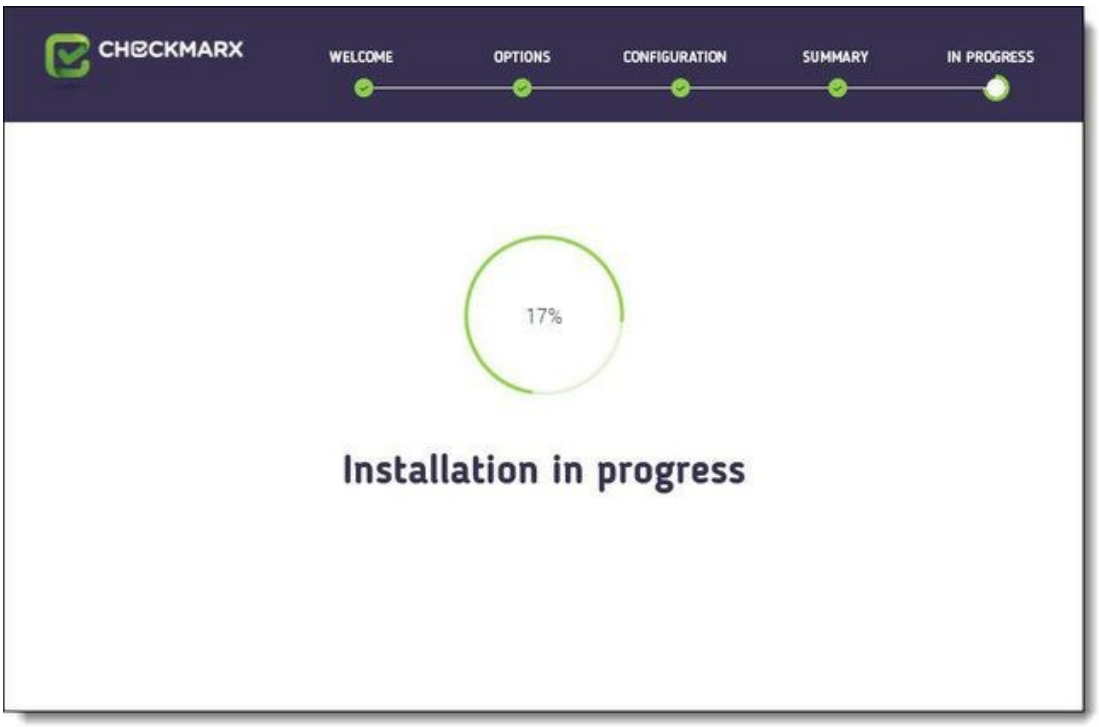
If required, select another port and click **Validate Port**.

Click **NEXT** to continue. The **Setup Summary** window is displayed.



Check the setup summary according to your selection.

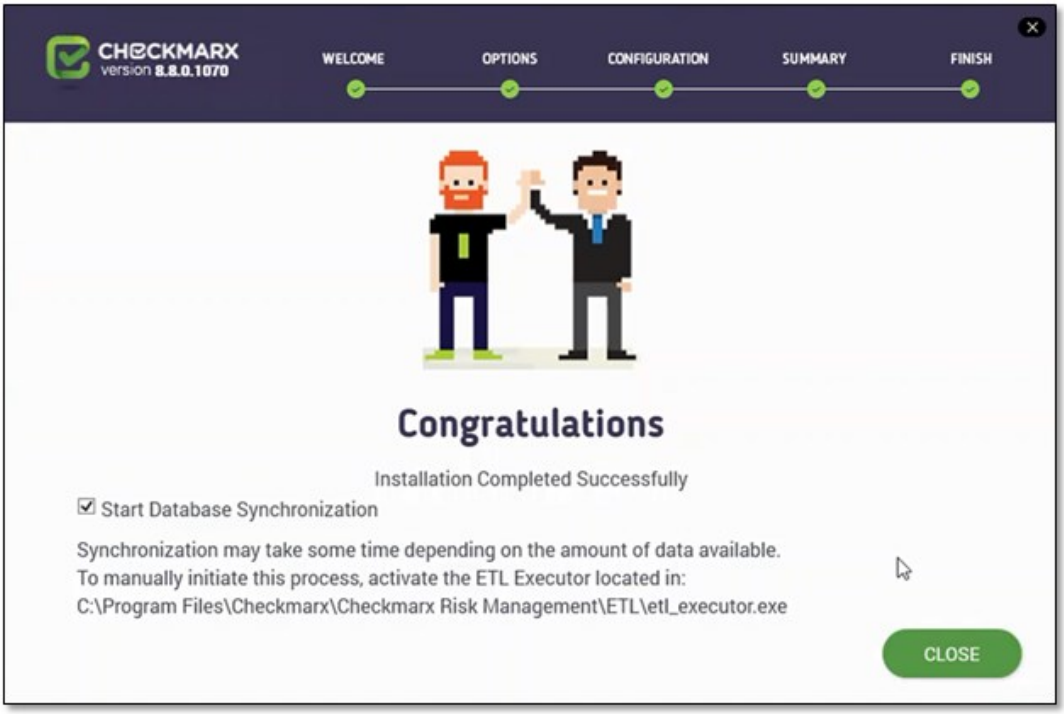
Click **INSTALL** to continue, **BACK** to return to the previous window, or **X** to exit. The **Installation in Progress** window is displayed.



Setup Failed

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.

Once complete the **Installation Completed Successfully** window is displayed.



Start Database Synchronization

If you have installed Management and Orchestration, according to the Congratulations window, by default the Start Database Synchronization checkbox is selected. This enables Management and Orchestration (CxARM) and initializes the automatic synchronization process that extracts data from the CxSAST database to the CxARM database. This process may take a while, depending on the amount of data being synchronized.

You can either perform the database synchronization now, or manually at a later time using the ETL Executor located in: C:\Program Files\Checkmarx\Checkmarx Risk Management\ETL\etl_executor.exe

NOTE: This folder may vary according to the selected Checkmarx installation folder.

For more information about Management and Orchestration prerequisites and recommendations, see Setting Up Management and Orchestration.

For more information about installing Management and Orchestration, see Installing Management and Orchestration.

Reinstalling CxSAST with an Already Existing CxARM DB

If attempting to install CxSAST with CxARM and connect to an existing CxARM DB, the subsequent ETL DB sync will fail, due to a limitation in CxARM. Therefore, in order to reinstall CxSAST with CxARM, either delete the existing CxARM DB before reinstalling, or reinstall with a new CxARM DB.

To continue now with the database synchronization:

Leave the checkbox selected, and then click **CLOSE.** If required, reboot the server (you will receive a prompt if rebooting is necessary). The database synchronization process starts automatically.

To perform the database synchronization at another time:

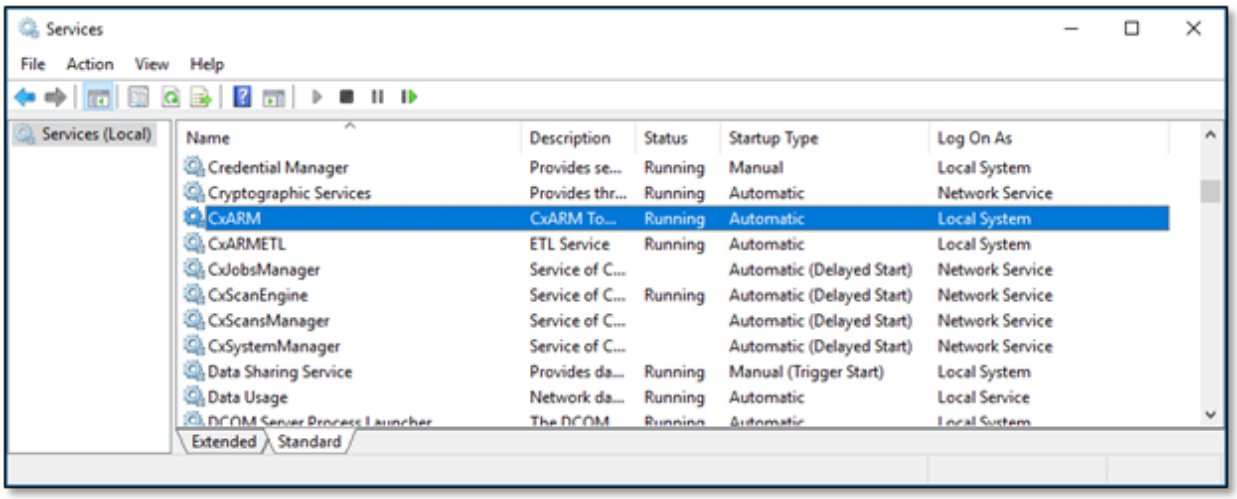
Alternatively, you can manually initiate the synchronization process at a later time by clearing the checkbox now, and clicking **Close.** At a later time use the ETL tool to perform the synchronization, located at: **C:\Program Files\Checkmarx\Checkmarx Risk Management\ETL\etl_executor.exe**

NOTE: This folder may vary according to the selected Checkmarx installation folder.

For more information on Application Risk Management, see Installing CxARM.

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 Checkmarx services are started:

On a centralized host:

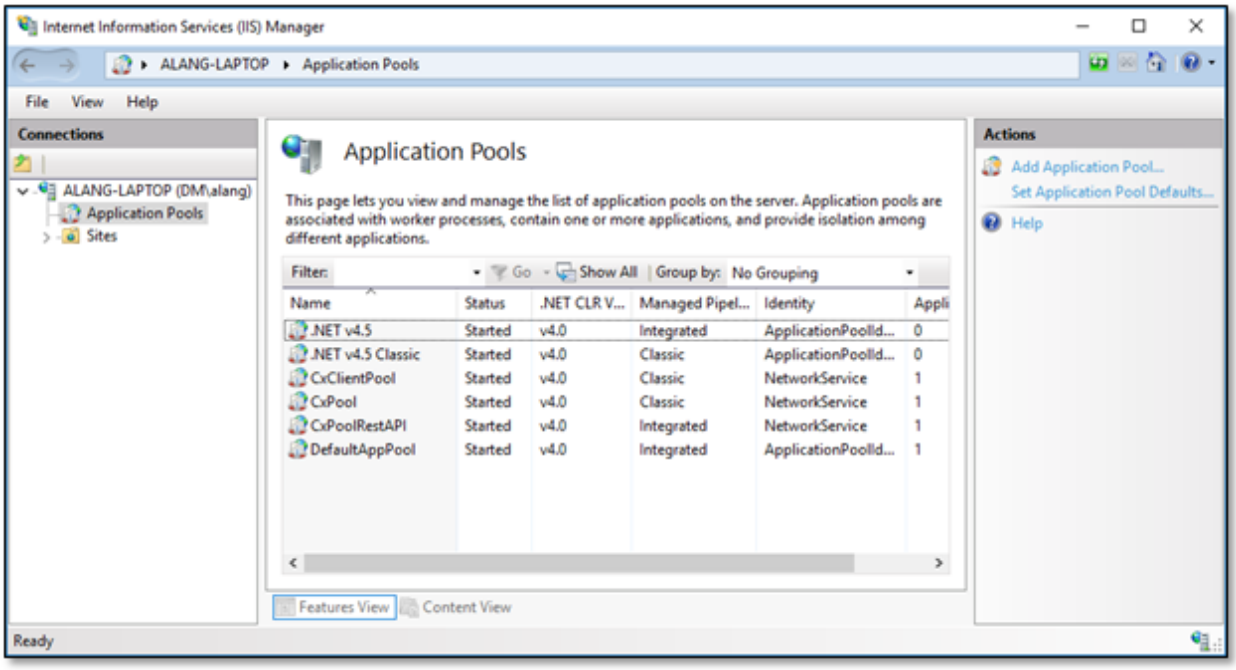
- CxJobsManager
- CxScansManager
- CxSystemManager
- CxScanEngine
- Web Server:
  - IIS Admin Service
  - World Wide Web Publishing Service
- Application Risk Management:
  - CxARM
  - CxARMETL

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
- CxPoolRestAPI

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

Enable Long Path Support in CxSAST Application

.NET framework 4.6.2 and above supports the Long Path feature by default. The following actions should be taken in order for the Long Path feature to be enabled.

The following configuration should be added to the Web Service and REST API:

<httpRuntime targetFramework="4.6.2" />

> The *web.config* file is usually located in the following path: *c:\Program Files\Checkmarx\Checkmarx Web Services\CxWebInterface\web.config*

For example:

```
<system.web>
    <httpRuntime targetFramework="4.6.2" />
    <compilation targetFramework="4.5.1" debug="true"/>
</system.web>
```

> If the httpRuntime already exists, add the targetFramework attribute as follows:
>
> <httpRuntime maxRequestLength="2097151" executionTimeout="36000" **targetFramework="4.6.2"** />

> Keep in mind that this configuration should only added on a machine that has .NET 4.6.2 or above installed, otherwise there will be issues in the application.

Login to the Web Interface

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

- Access CxSAST locally (from the server host) by using 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**

Password Complexity

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:

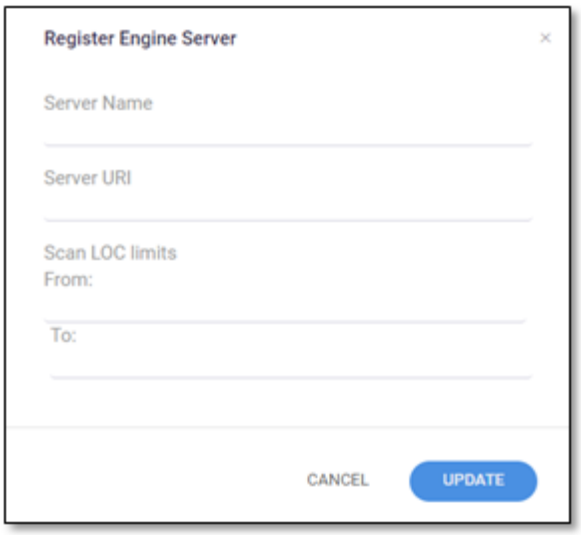
Go to Management > Application Settings > Engine Management. The Engine Management window is displayed.

Click Register Engine Server. The Register Engine Server window is displayed.

Give the Engine a Server Name, and provide the Server URL, so that CxManager will be able to communicate with CxEngine. The URL should be:
http://<Server_Name>/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc

(where <Server_Name> is the CxEngine host's IP address or resolvable name).

Optionally define Scan LOC Limits (maximum lines of code allowed).



URL Check

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

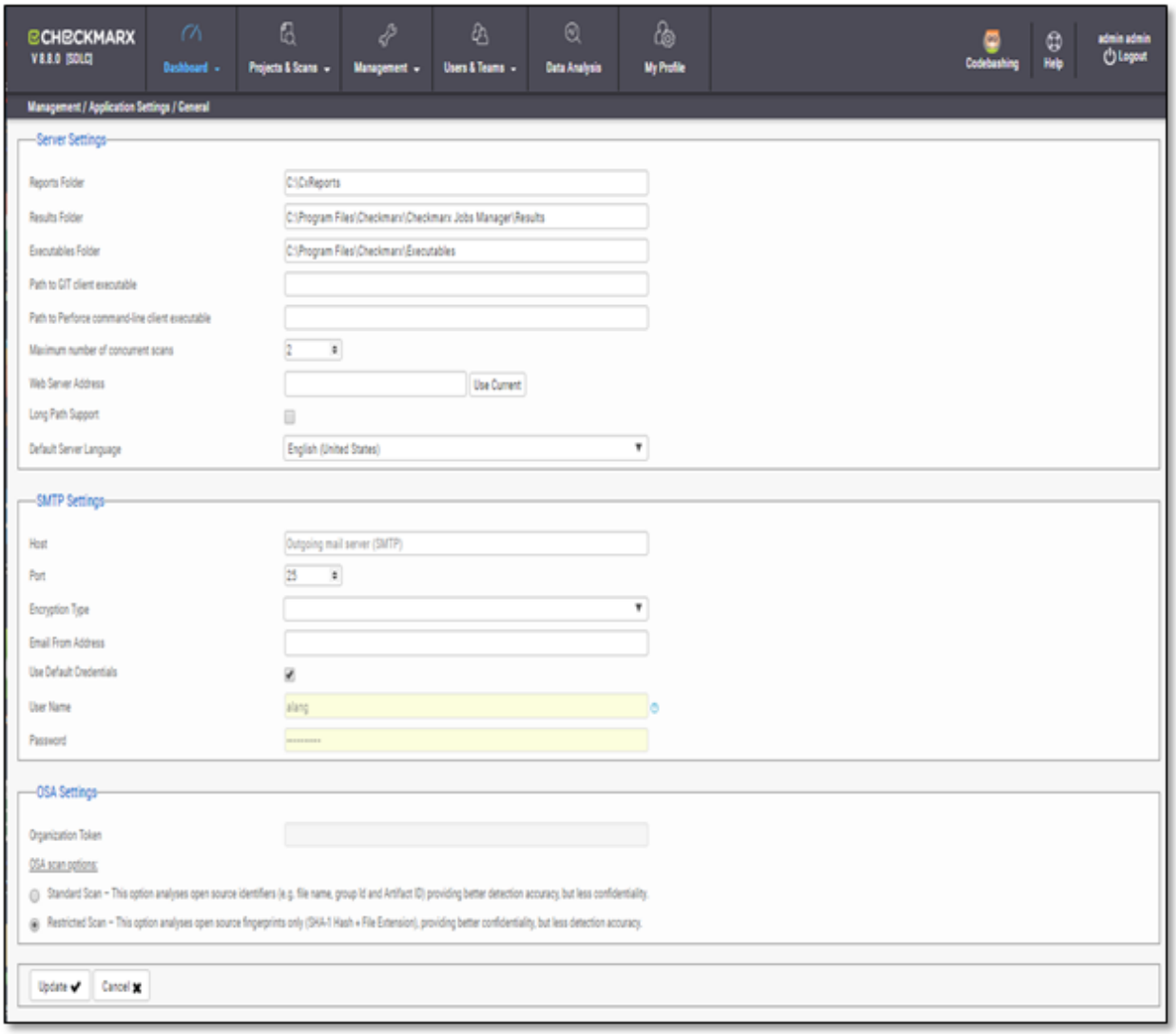
Click Update.

Multiple CxEngine Servers:

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

Go to Management > Application Settings > General.

After updating the information, at the bottom of the page, click Update:



Server Settings

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

Enable Long Path Support in Server Settings

In order for the long path feature to be fully supported in CxSAST, click Edit and check the Long Path Support checkbox.

Long Path Support

Click Got It on the message window to confirm your understanding that all application servers must support long paths, otherwise scans with long path files may fail.

Click Update to save the changes.

SMTP Settings

Provide SMTP settings. 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.

Click Update to save changes.

OSA Settings

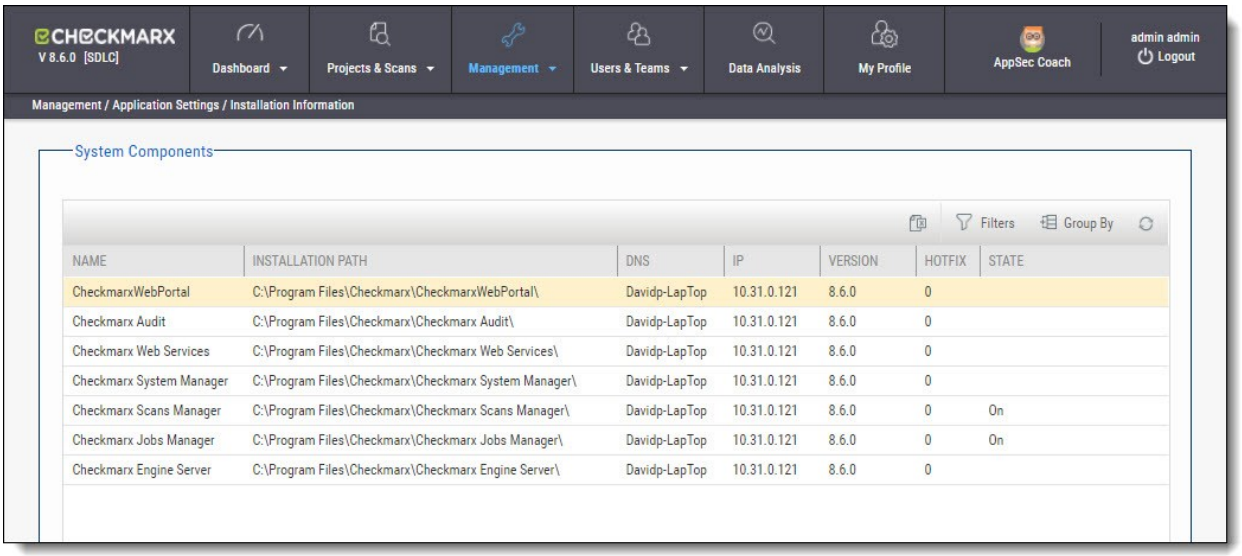
If licensed for CxOSA, select the OSA (Open Source Analysis) scan option and click Update.

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. This is required for AppSec Coach registration.

Installation Verification

Go to **Management** > **Application Settings** > **Installation Information.**



Validate that you have successfully installed the correct version and/or hot-fix and review all CxSAST system components ensuring that they are all of the same version.

Modifying CxSAST

Modify allows you to add or remove features for the currently installed version of the CxSAST application.

To modify CxSAST:

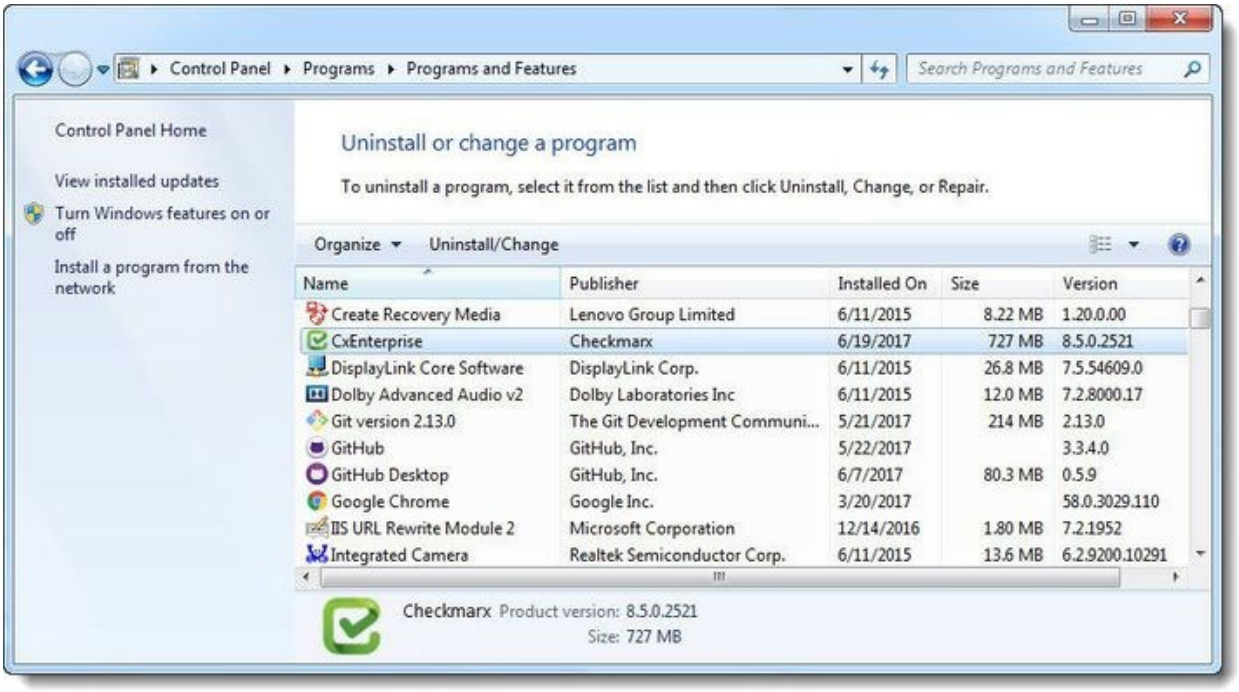
Make sure there are no scans currently running.

Stop all Cx Windows services:

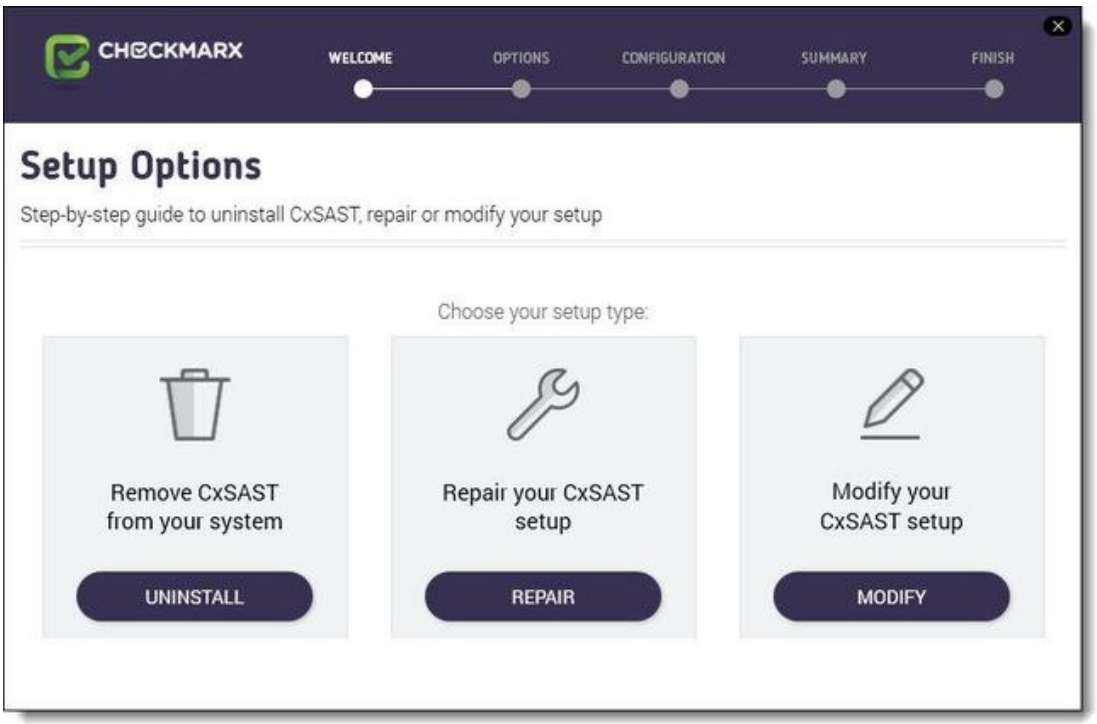
- CxSystemManager
- CxJobsManager
- CxScansManager
- CxScanEngine
- Web server:
  - World Wide Web Publishing Service
  - IIS Admin Service
- Application Risk Management:
  - CxARM
  - CxARMETL

> **Backup**
>
> As a precaution you should backup both Cx databases (using standard SQL Server tools and make sure to give the files unique names and to include **.bak.**

Go to **Start** > **Control Panel** > **Programs** > **Programs and Features**.

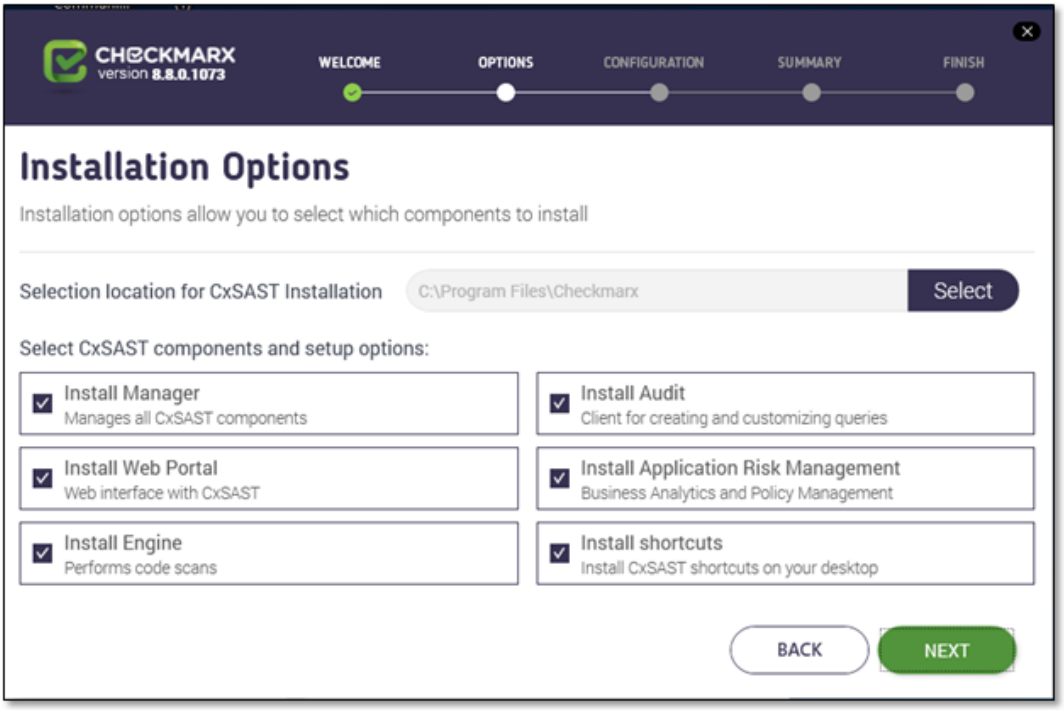


Double-click on **CxEnterprise**.or right-click and select **Uninstall/Change**. The **Setup Options** window is displayed.



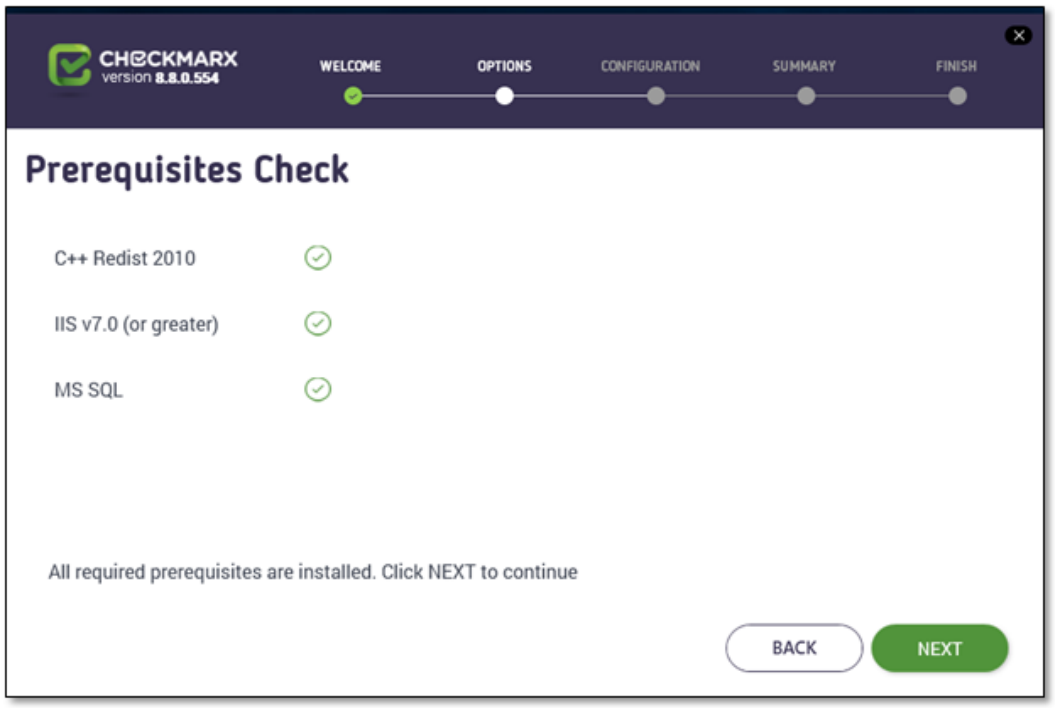
Click MODIFY, then click OK on the warning message to acknowledge that selecting Modify or Repair will change any previously defined installation configuration back to the default setting.

The additional Installation Options window is displayed.

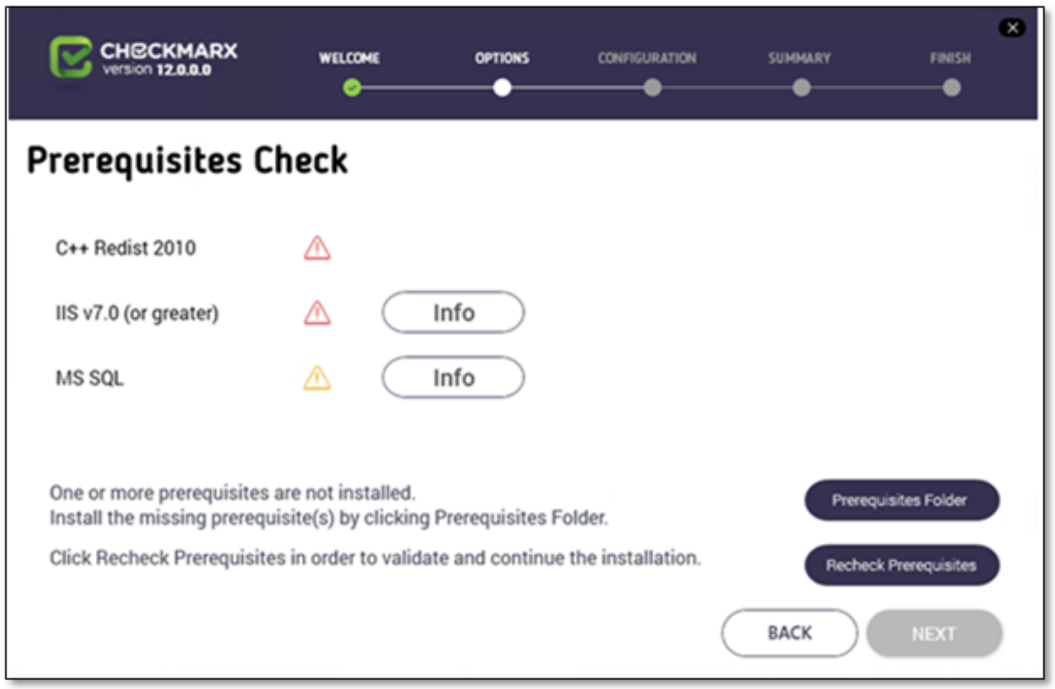


Select or deselect the required product features for this modification from the available list.

Click **Next** to continue. The Prerequisites Check window is displayed, showing the status of all prerequisite components.

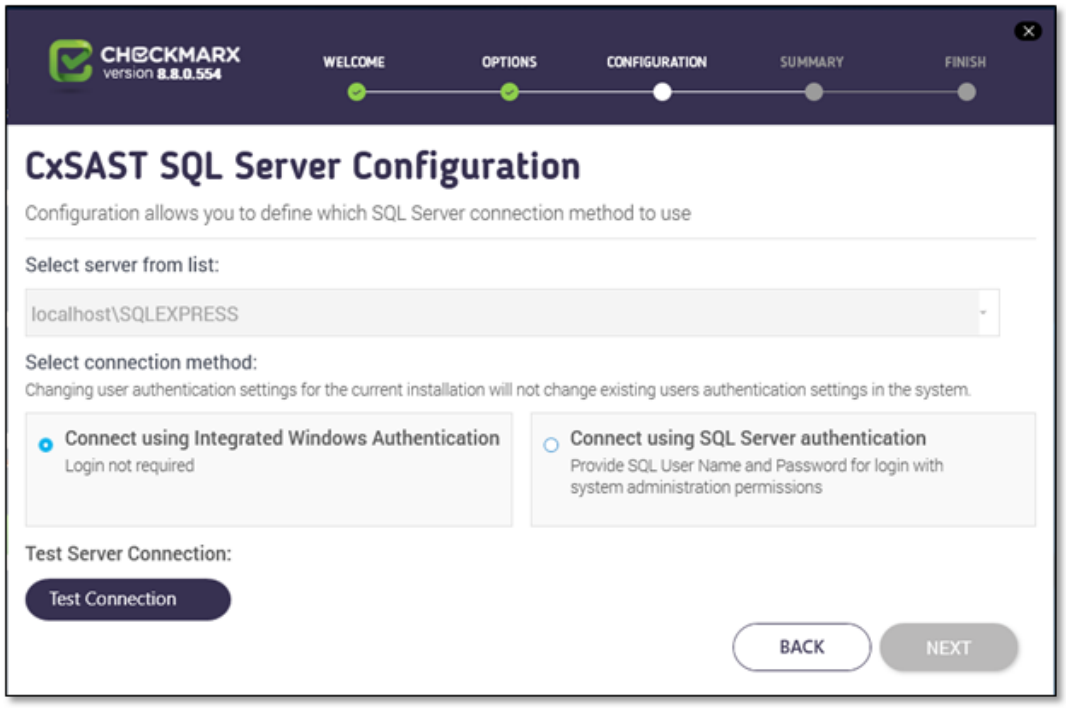


For any prerequisites not installed, click the respective INFO button for additional installation information, and then click Prerequisites Folder to install the missing component(s).



Click Recheck Prerequisites to confirm the installation status.

When all prerequisite components are installed, click Next to continue. The CxSAST SQL Server Configuration window is displayed.



For CxSAST, define a connection to the installed SQL Server or to any other SQL server on your network, by selecting one of the following:

- Connect using Integrated Windows Authentication (login not required)
- Connect using SQL Server Authentication (provide SQL user name and password for login with SA permissions).

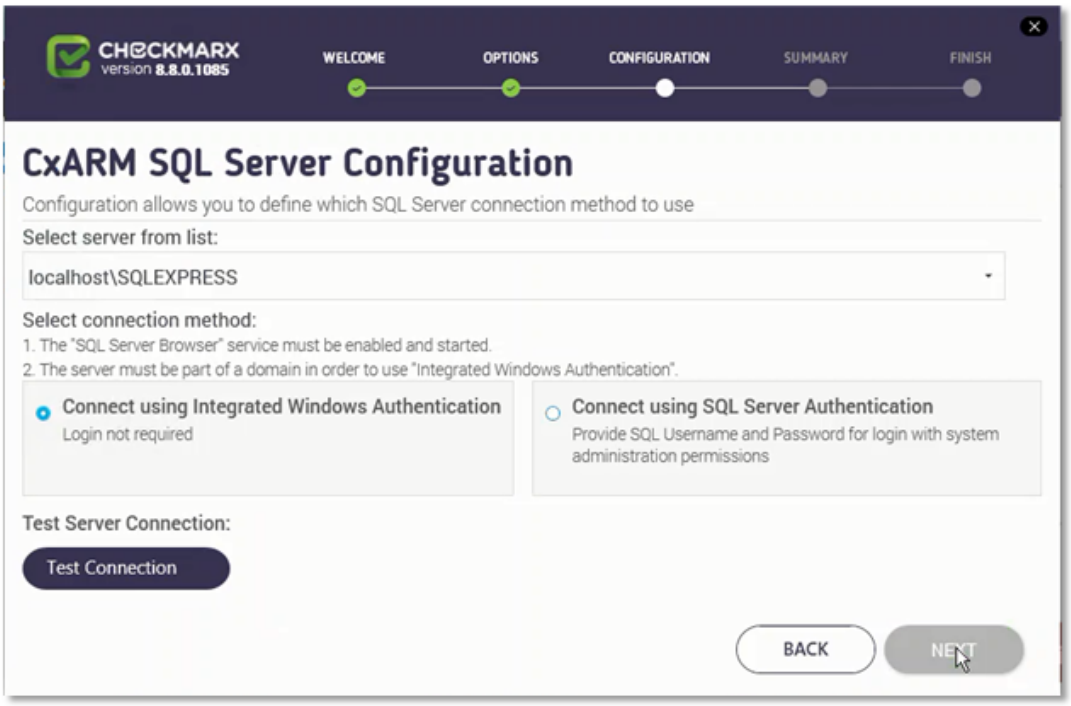
■ Changing user authorization settings for the current installation will not change existing users' authentication settings in the system.

Click Test Connection. A confirmation message is displayed upon successful connection to the CxSAST SQL Server.

■ **SQL Server Connection Failure**

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

Click OK on the confirmation message, then click NEXT. The CxARM SQL Server Configuration window is displayed.



For CxARM, define the CxARM SQL Server connection by selecting one of the following:

- Connect using Integrated Windows Authentication (login not required)
- Connect using SQL Server authentication (provide SQL user name and password for login with SA permissions).

Connection Requirements

For both connection methods: The SQL Server Browser Windows service must be enabled and started.
For the Integrated Windows Authentication method: The server must be part of a Windows domain.

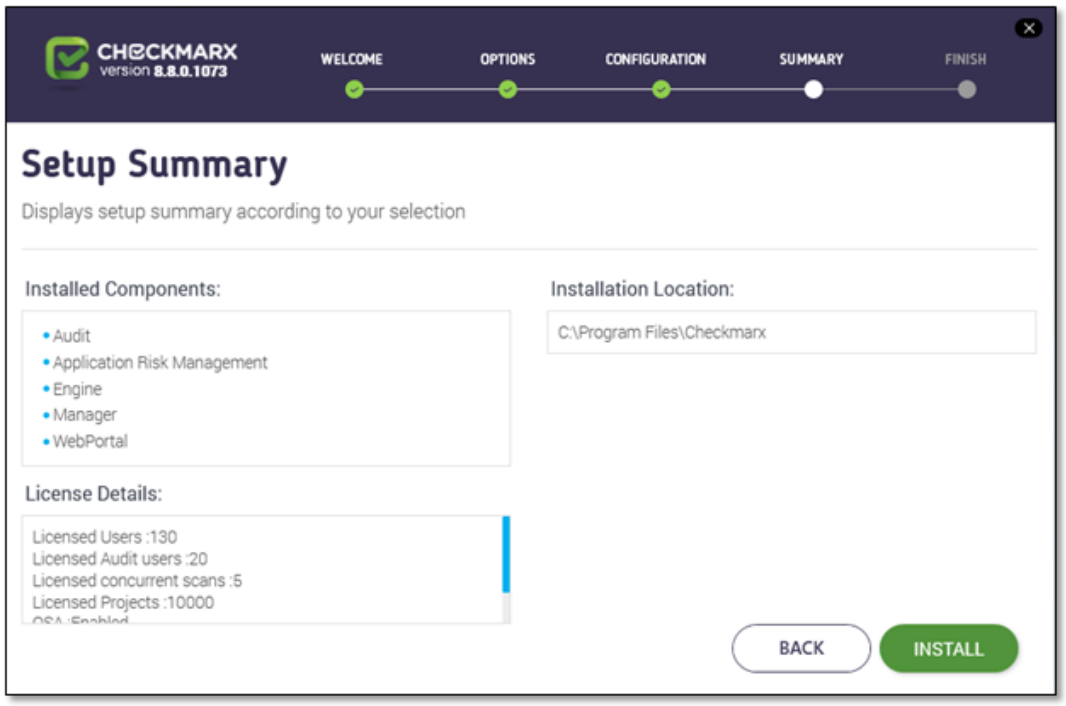
Click Test Connection. A "Connection successful" message is displayed upon confirmed connection to the SQL Server.

CxARM DB Connection Failure

If connection to the CxARM database fails, in order to continue with the installation, a confirmed connection is required.
If the "SQL Connection Test Results" message indicates that connection to CxARM database has failed, verify the following:

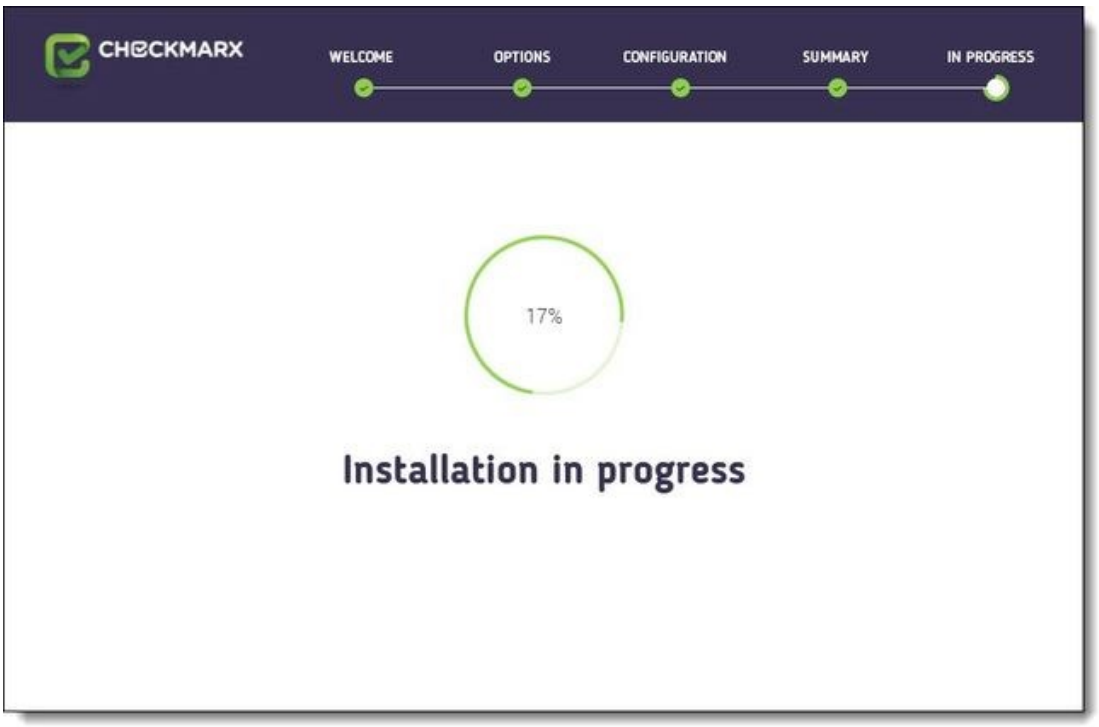
- Host, port and login credentials are correct
- The CxARM machine is a member of a Windows domain (if not, either join the machine to a domain and perform a restart, or connect using SQL Server Authentication)
- The SQL Server Browser Windows service is running (if not, enable and start it)

Click OK on the message, and then click NEXT. The Setup Summary window is displayed.



Check the setup summary according to your selection.

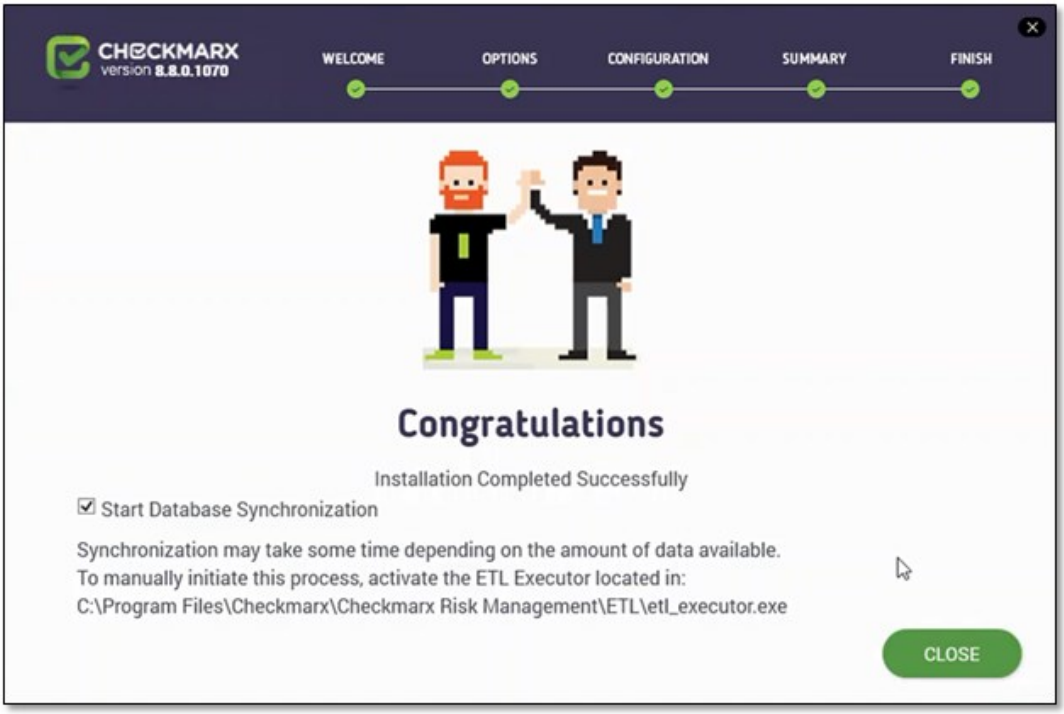
Click INSTALL to continue, BACK to return to the previous window, or X to exit. The Installation in Progress window is displayed.



Setup Failure

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.

Once complete, the Installation Completed Successfully window is displayed.



Start Database Synchronization

If you have installed Application Risk Management, on the Congratulations window, by default the Start Database Synchronization checkbox is selected. This enables Application Risk Management (CxARM) by initializing an automatic synchronization process that extracts data from the CxSAST database to the CxARM Analytics database. This process may take a while, depending on the amount of data being synchronized.
You can either perform the database synchronization now, or manually at a later time using the ETL Executor located in: C:\Program Files\Checkmarx\Checkmarx Risk Management\ETL\etl_executor.exe
NOTE: This folder may vary according to the selected Checkmarx installation folder.
For more information on Application Risk Management, see Installing CxARM.

To continue now with the database synchronization:

Leave the checkbox selected, and then click CLOSE. If required, reboot the server (you will receive a prompt if rebooting is necessary). The database synchronization process starts automatically.

To perform the database synchronization at another time:

Alternatively, you can manually initiate the synchronization process at a later time by clearing the checkbox now, and clicking Close. At a later time use the ETL tool to perform the synchronization, located at: C:\Program Files\Checkmarx\Checkmarx Risk Management\ETL\etl_executor.exe

NOTE: This folder may vary according to the selected Checkmarx installation folder.

For more information on Application Risk Management, see Installing CxARM.

Repairing CxSAST

Repair allows you to re-install any corrupted or missing files and restore the currently installed CxSAST application to an operational state.

To repair CxSAST:

Make sure there are no scans currently running.

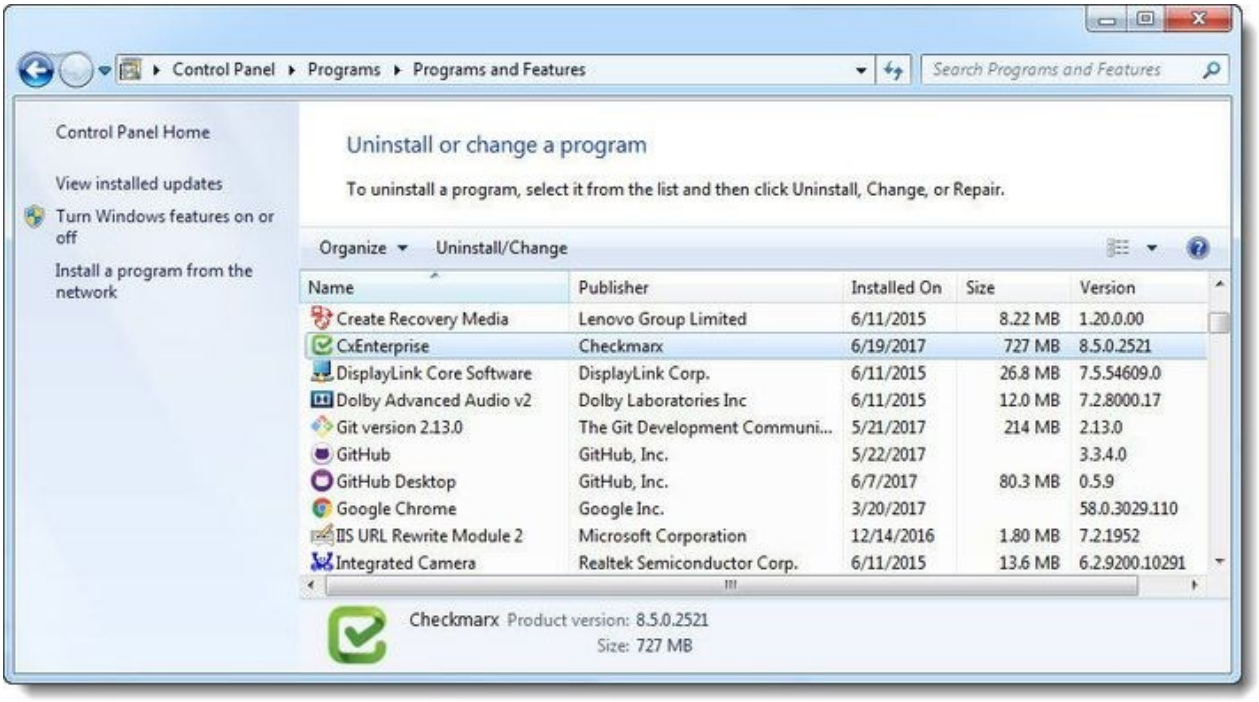
Stop all Cx Windows services:

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxScanEngine
- Web server:
  - World Wide Web Publishing Service
  - IIS Admin Service
- Application Risk Management:
  - CxARM
  - CxARMETL

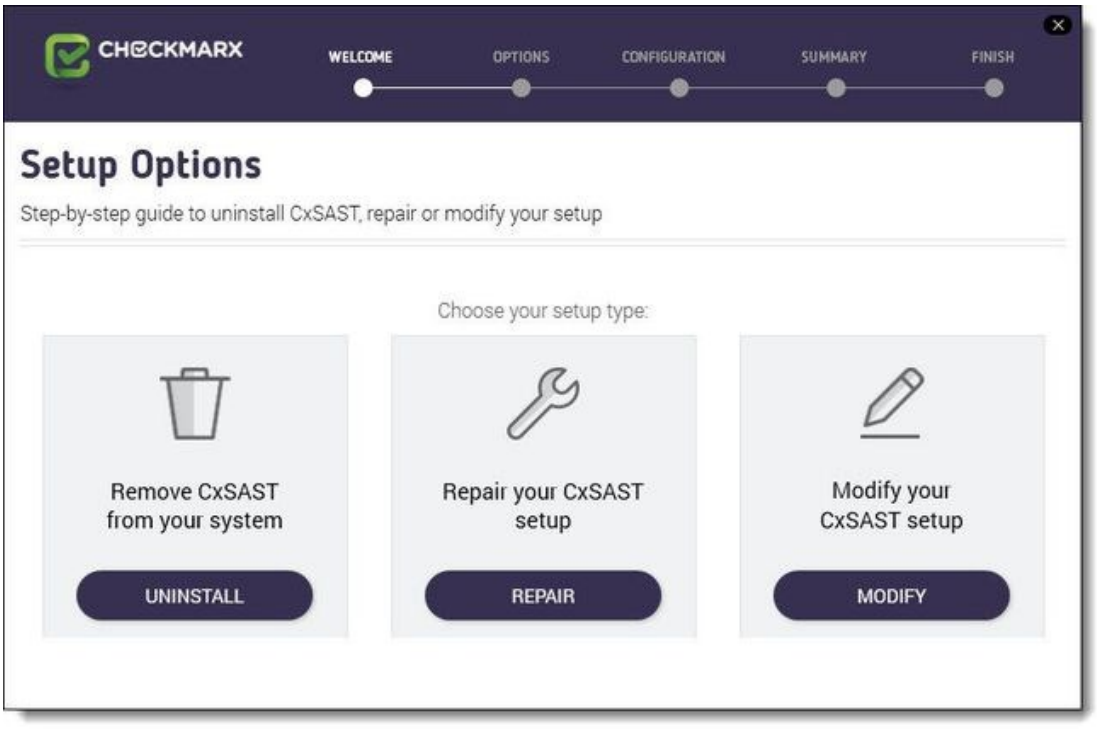
Backup

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**.

Go to **Start** > **Control Panel** > **Programs** > **Programs and Features**.

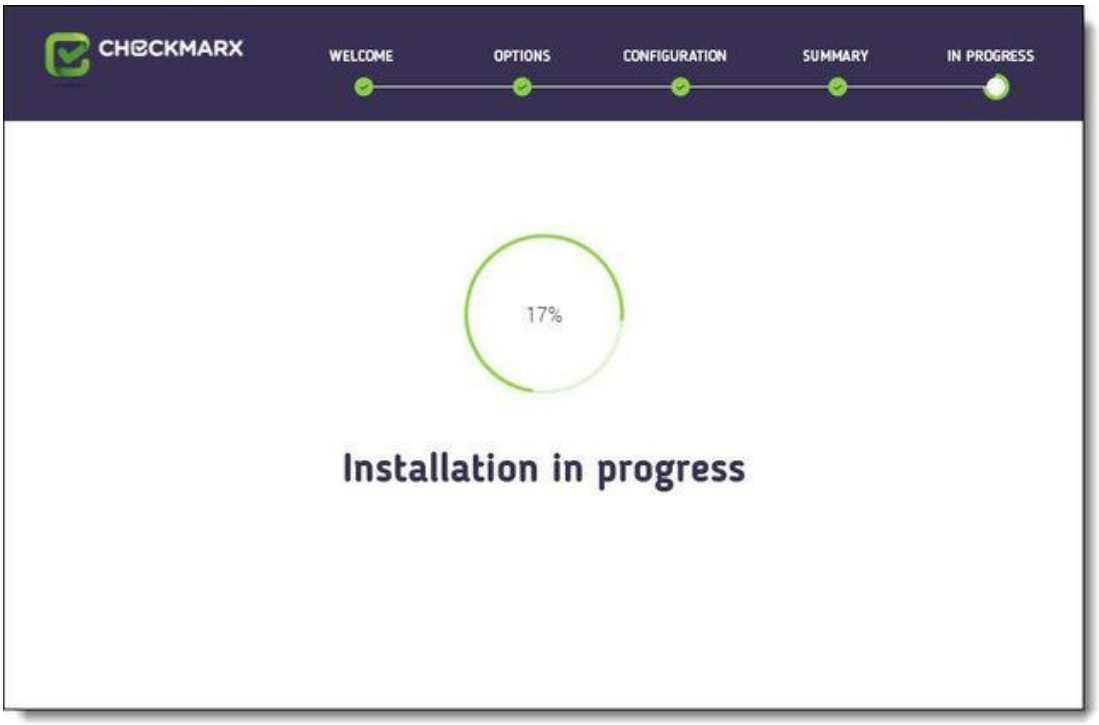


Double-click on **CxEnterprise**.or right-click ans select **Uninstall/Change**. The **Setup Options** window is displayed.



Click REPAIR, then click OK on the warning message to acknowledge that selecting Modify or Repair will change any previously defined installation configuration back to the default setting.

The Installation in Progress window is displayed.



Once complete the **Operation Completed Successfully** window is displayed.

Click **CLOSE** to complete the installation.

Backing Up CxSAST

The following page describes the backup and recovery procedures for CxSAST

Backing up CxSAST

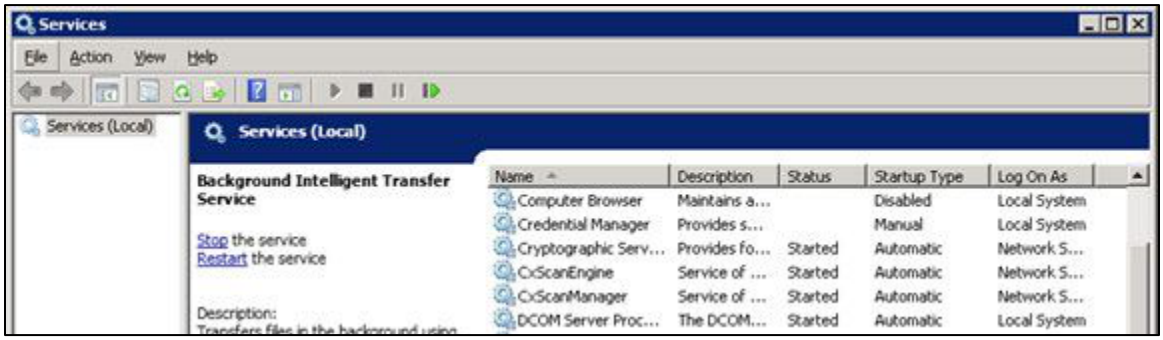
CxSAST Enterprise Edition is composed of application files, configuration files and two SQL databases.

Generally the best backup method (available only for virtual machines) would be a daily snapshot of the CxSAST machine(s) and restoration when needed.

If the Snapshots option is not available, please use the following instructions:

Stop the following services (depending on the Cx components installed on the server):

- CxJobsManager
- CxScansManager
- CxSystemManager
- CxScanEngine
- CxARM
- CxARMETL



Stop the IIS Web Server

Backup the Checkmarx folder by copying it aside (Logs folder can be excluded)

Example: <Checkmarx Installation Path>\Checkmarx -> <Checkmarx Installation Path>\Checkmarx01012016

Backup the CxDB and CxActivity SQL databases using standard Database tools

Backup the CxSRC folder - scanned source folder - by creating a copy

Example: X:\CxSrc -> X:\CxSrc01012016

> ■ Please check that you have the CxSAST installation zip file for the current backed up version (can be requested from Checkmarx support).

Start the following services (depending on the Cx components installed on the server):

- CxJobsManager
- CxScansManager
- CxSystemManager
- CxScanEngine
- CxARM
- CxARMETL

Start the IIS Web Server

Recovering CxSAST

The recovery procedure may be different based on the state of CxSAST server(s).

If the CxSAST server(s) needs to be rebuilt please follow the instructions:

> ■ If CxSAST exists and is working please start from the second step.

Install CxSAST with same version as your backed up version to the same path as your former CxSAST installation

Stop the following services (depending on the Cx components installed on the server):

- CxJobsManager
- CxScansManager
- CxSystemManager
- CxScanEngine
- CxARM
- CxARMETL

Stop the IIS Web Server

Move/rename the Checkmarx folder

Example: <Checkmarx Installation Path>\Checkmarx --> <Checkmarx Installation Path>\checkmarxNew01012016

Restore the Checkmarx folder

Move the old Checkmarx folder that you previously saved back to the original Checkmarx folder location.

Example: <Checkmarx Installation Path>\checkmarx0101216 --> <Checkmarx Installation Path>\Checkmarx

Restore the database

Restore the databases using the backup that you previously saved using the standard database tools.

Restore the scanned source folder

Move the old scanned source folder that you previously saved back to the original folder location.

Example: X:\CxSrc01012016 --> X:\CxSrc

Start the following services (depending on the Cx components installed on the server):

- CxJobsManager
- CxScansManager
- CxSystemManager
- CxScanEngine
- CxARM
- CxARMETL

Start the IIS Web Server

Check the recovered version

Perform a basic test on the restored installation to check that everything is up and running.

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

- Should you need any further assistance, please don't hesitate to contact Checkmarx support.

Upgrading CxSAST

CxSAST only supports upgrades for two earlier versions. If your current version is older, please contact support prior to the upgrade process.

> This page applies only to full upgrades (it does not apply to hotfixes).

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

To upgrade CxSAST:

Make sure that there are no scans currently running.

Although Cx Installer will stop and start services as needed – Due to different permission issues we recommend to manually stop all Cx Windows services and the Web server:

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxScanEngine
    - Web server (run "iisreset /stop" from elevated CMD or Stop action for the server name in IIS Console)
    - World Wide Web Publishing Service
- IIS Admin Service
- Application Risk Management:
    - CxARM
    - CxARMETL

> 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)**.

Install CxSAST.

During upgrade the Checkmarx installer automatically performs a backup copy of configuration files. To locate the Checkmarx backup files go to **Start** > **Search** > and type **"%appdata%" (**C:\Users\<user>\AppData\Roaming\Checkmarx).

Install CxSAST with CxARM

■ Upgrading CxSAST with Management & Orchestration (CxARM)

For v8.9.0 only, when performing an upgrade for CxSAST that includes Management and Orchestration, all manual changes performed within the Tomcat Server .xml file (see format below) will be reverted on upgrade. The installer will need to manually recreate the changes. A copy of the previous file will be kept in the folder (e.g. C:\Program Files\Checkmarx\Checkmarx Risk Management\Tomcat\conf\) for manual comparison by the installer.
The Tomcat ('Server.xml') file is backed up in the following format: serveryyyy.MM.dd.HH.mm.ss.xml (e.g. server2019.03.13.13.56.01.xml)

When upgrading CxSAST, in order to install CxARM, select the 'advanced' installation option. Selecting the 'easy' option will not install CxARM, unless you are installing on a clean environment - where it will be installed by default.

■ The following files should be backed-up in case they need to be restored after an upgrade "X:\Program Files\Checkmarx\Checkmarx Audit\DefaultConfig.xml"

"X:\Program Files\Checkmarx\Checkmarx Engine Server\DefaultConfig.xml"
"X:\Program Files\Checkmarx\Executables*.*"

The following files should be backed up and used during the upgrade process:
"X:\Program Files\Checkmarx\Licenses\License.cxl"

The following files should be backed-up and used if you are unable to find or connect to the database during installation:
"X:\Program Files\Checkmarx\Configuration\DBConnectionData.config"

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

Please validate and (if required), start all Cx Windows services and the Web server:

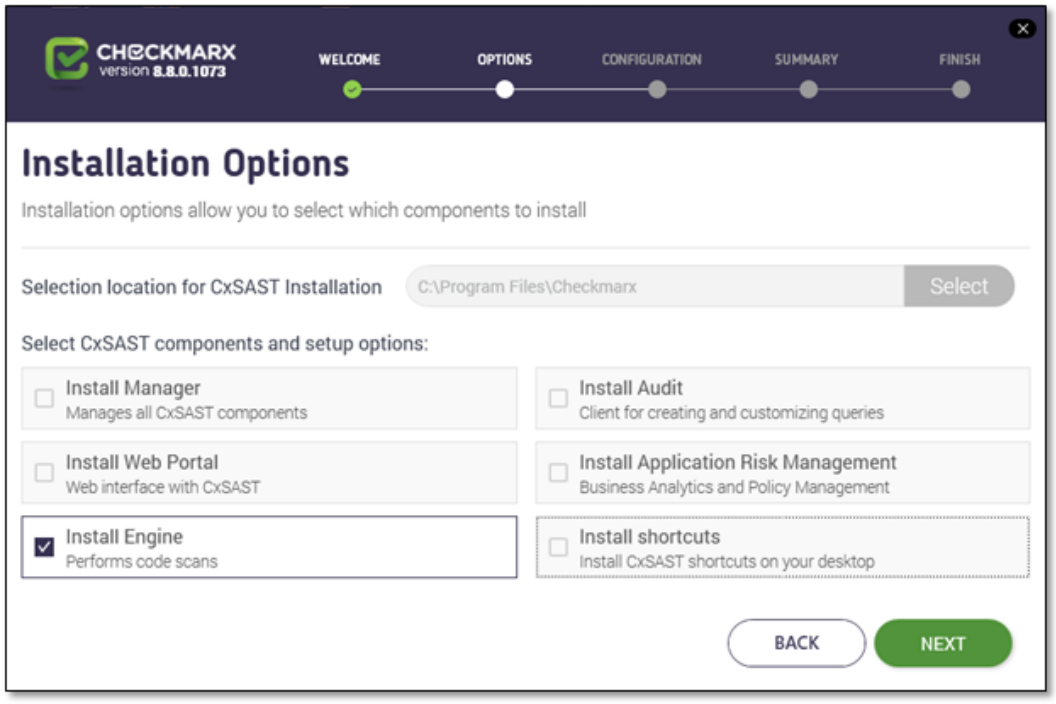
- CxSystemManager
- CxJobsManager
- CxScansManager
- CxScanEngine
- Web server (run "iisreset" from elevated CMD or Start action for the server name in IIS Console)
    - World Wide Web Publishing Service
    - IIS Admin Service
- Application Risk Management:
    - CxARM
    - CxARMETL

Adding a CxEngine Server

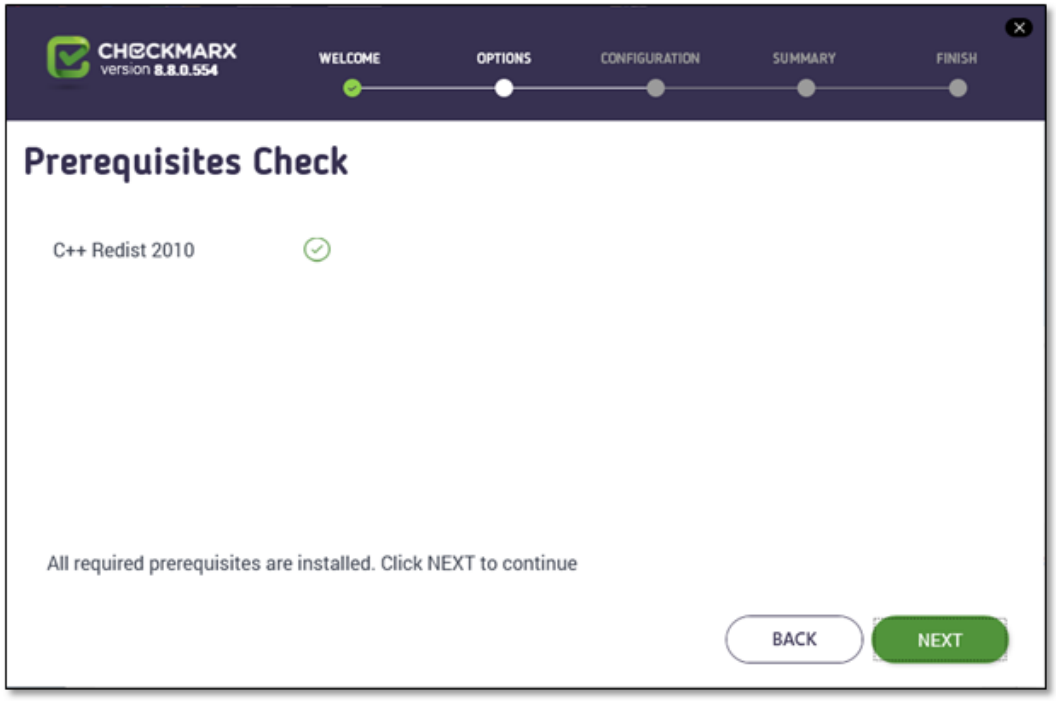
If you see that your scan load requires an additional Engine server, you can add one as follows:

Prepare the environment for the new CxEngine

Perform a server installation and under installation options, select **Install Engine** only.



Click Next. The Prerequisites Check window is displayed.



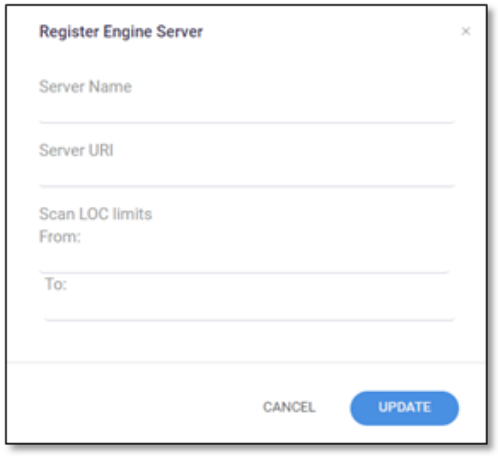
If the Prerequisites Check window indicates that any prerequisite component(s) are not installed on your computer, perform the installation(s) before proceeding.

When all prerequisite components are installed, click Next to continue.

- For a CxEngine only installation, the Checkmarx license and HID validation is no longer required.

Log into the CxSAST web interface.

Go to Management > Application Settings > Engine Management. The Engine Management window is displayed.



Give the Engine a **Server Name**, and provide the **Server 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 Update.

■ Once the new engine is installed, you may need to:

- Increase the number of concurrent scans allowed (**Application Settings** > **Application Management** > **Server Settings** > **Maximum number of concurrent scans**). See **Application Management** for more information.
- Change the max_scans_per_machine value for each engine ({installation folder} > Checkmarx > Checkmarx Engine Server > CxSourceAnalyzerEngine.WinService.exe.config).
  - and/or -
- If you install CxAudit on the server, you may need to import a new license with more scans (Start > All Programs > Checkmarx > HID). See Updating the CxSAST License for more information.

Restart the CxScansManager service so that the new engines can be placed into the rotation.

Uninstalling CxSAST

Uninstall allows you to remove the currently installed version of the CxSAST application.

To uninstall CxSAST from a server host:

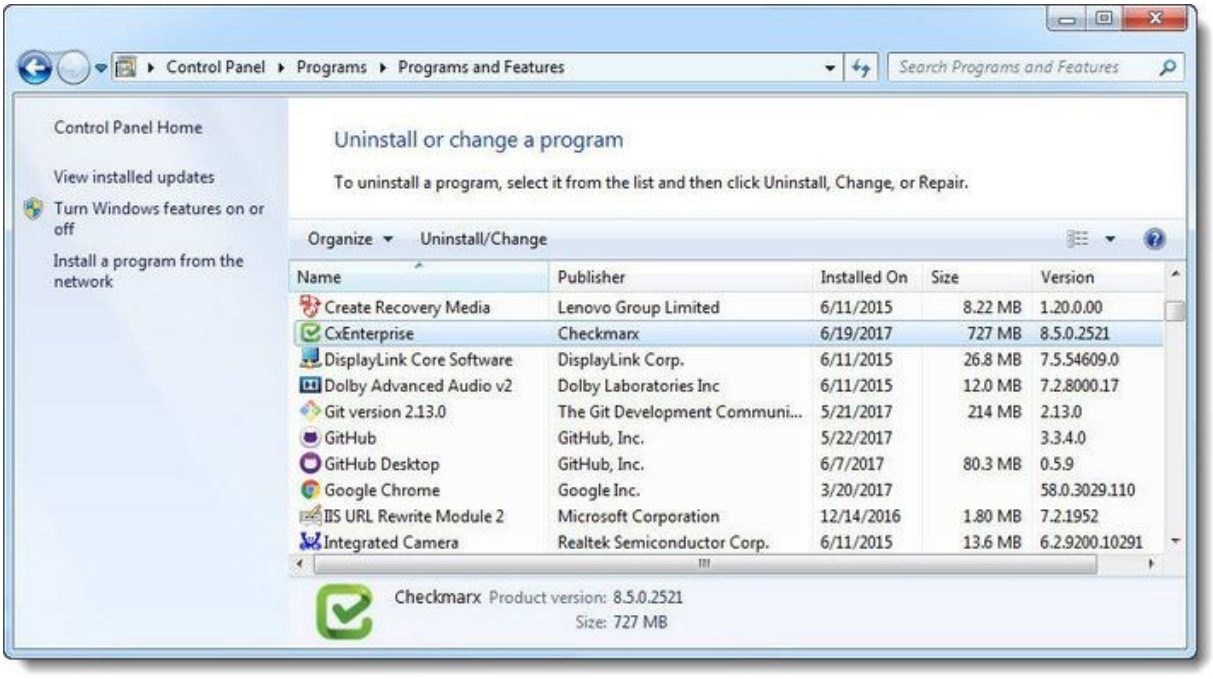
Copy your CxSAST license file to a safe location.

Make sure that there are no scans currently running.

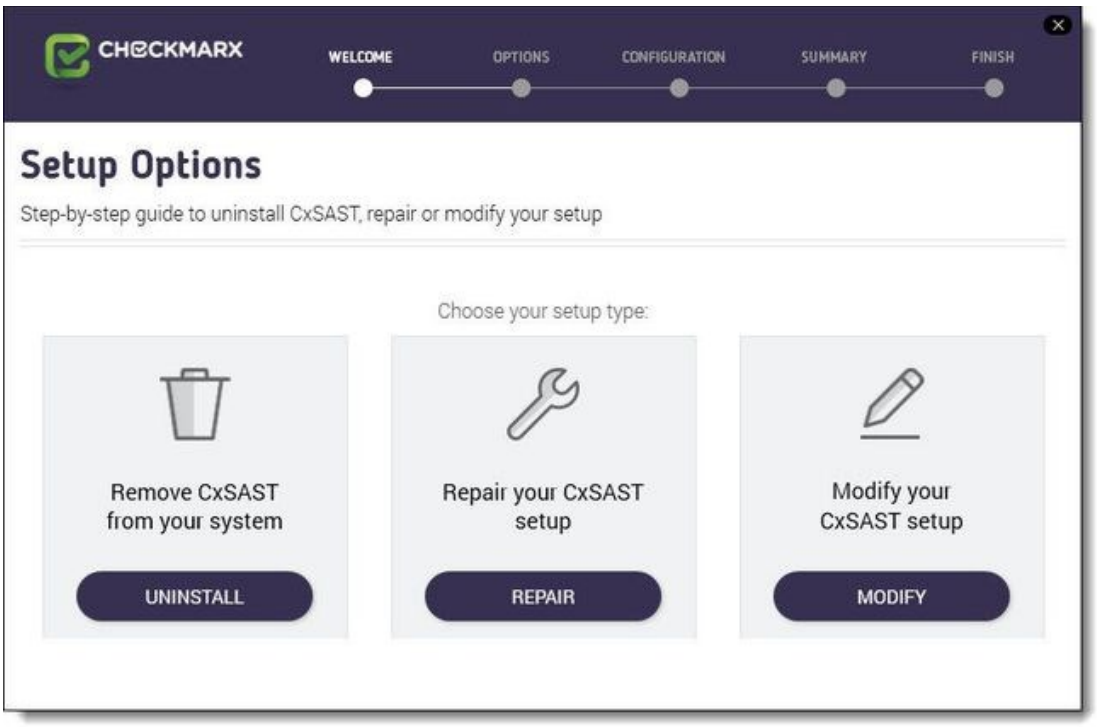
Stop all Cx Windows services:

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxScanEngine
- Web server:
  - World Wide Web Publishing Service
  - IIS Admin Service
- Application Risk Management:
  - CxARM
  - CxARMETL

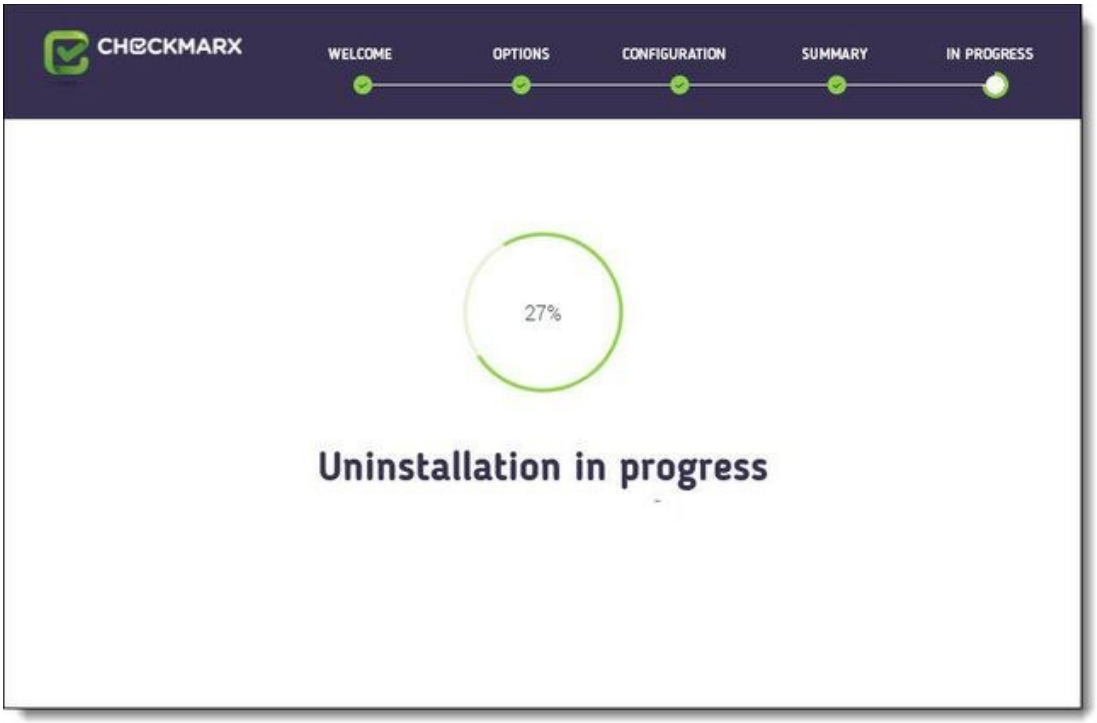
Go to **Start** > **Control Panel** > **Programs** > **Programs and Features**.



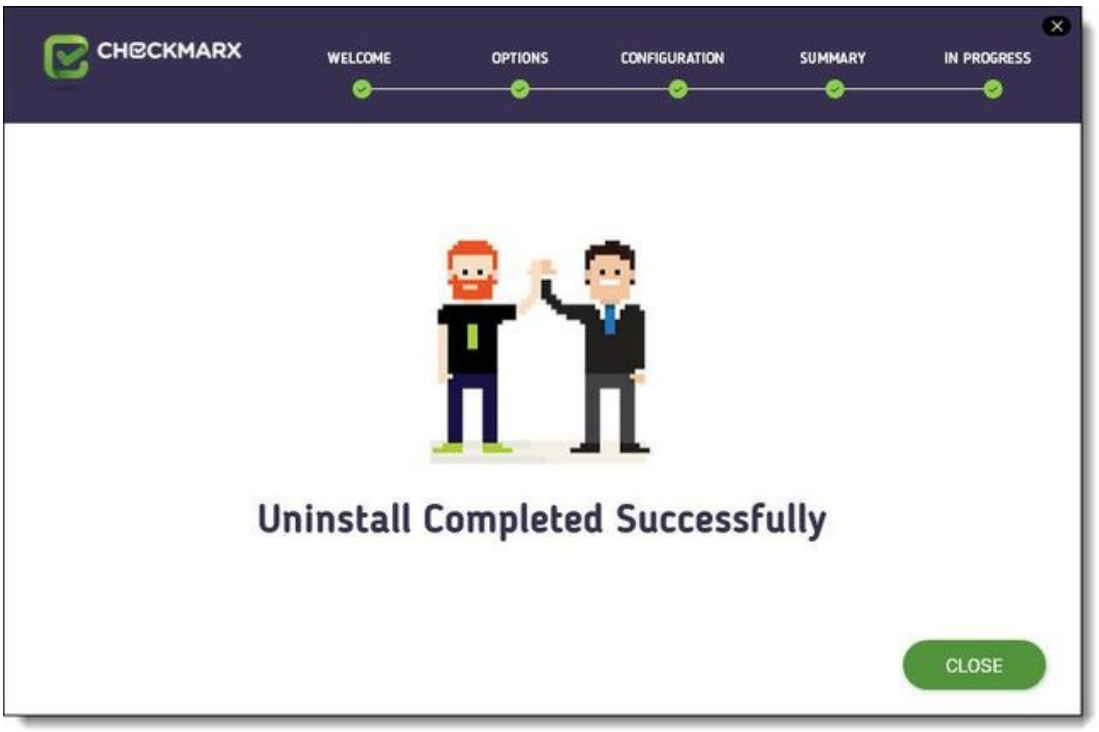
Double-click on **CxEnterprise**, or right click and select **Uninstall/Change**. The **Setup Options** window is displayed.



Click **UNINSTALL**. The **Uninstall in Progress** window is displayed.



Once complete, the **Uninstall Successfully Completed** window is displayed.



Click **Close** to complete the uninstall.

Renewal

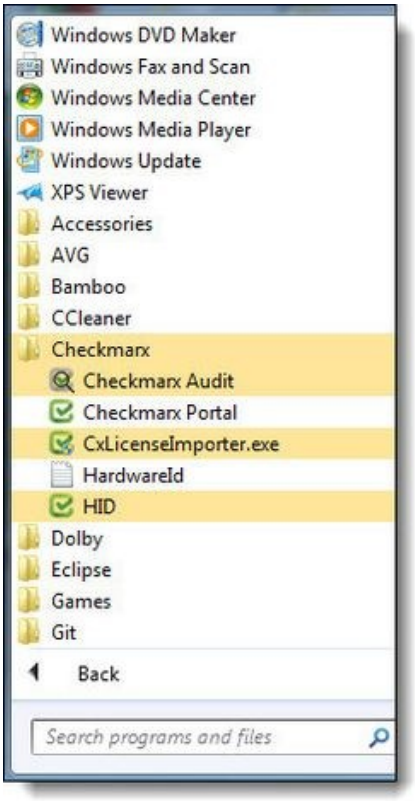
Even though uninstall removes most Checkmarx folders, for renewal purposes, the following folders are not deleted:

- **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 to generate the Hardware ID.



Go to: <Checkmarx directory>HID>HardwareId, then 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 then click CxLicenseImporter.exe, The Checkmarx License Importer is displayed.

Click Import License, navigate to your Checkmarx license file and click Open. If successful, a message displays notifying of the license import.

■ **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.

CxSAST Application Maintenance Guide

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 persistency
- **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.

Chapter 3 - Monitoring

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.

Chapter 4 - Maintenance Options for Reducing Fragmentation

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.

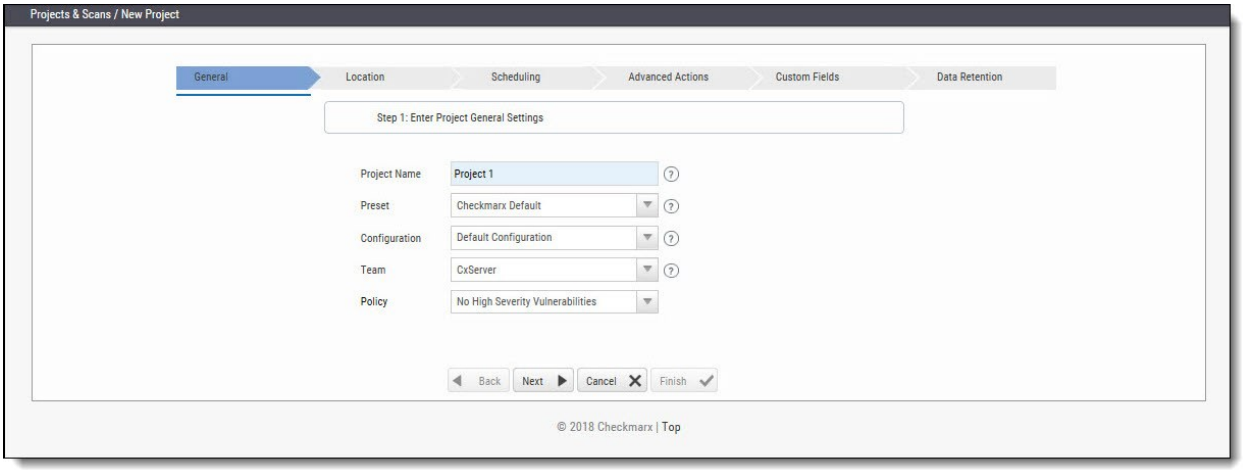
Setting Up

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

Step 1: Enter Project General Settings

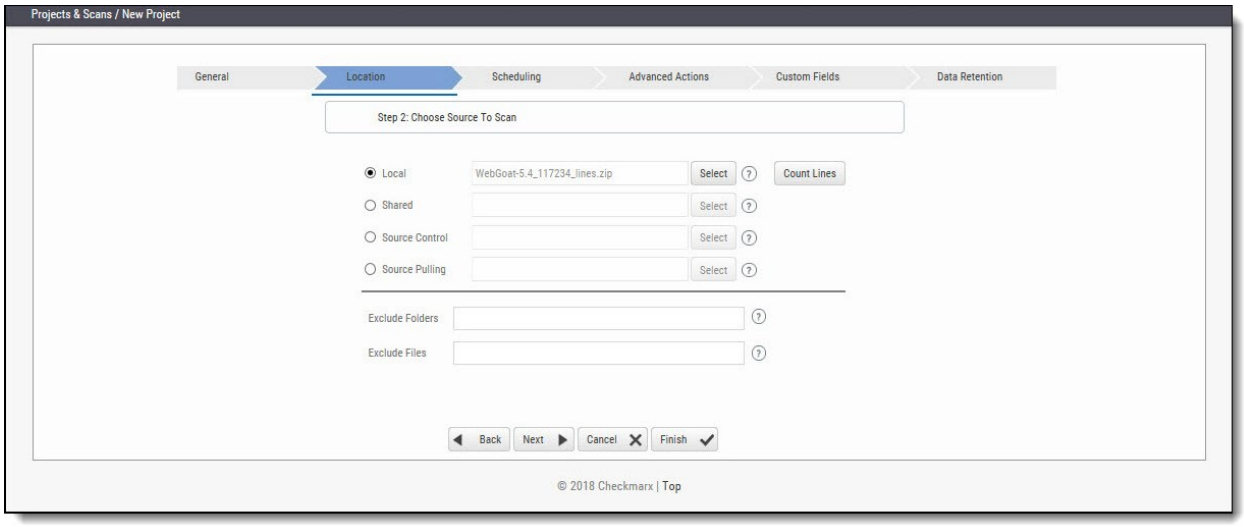
1. **Project Name**: Provide an appropriate Project Name for the project.
2. **Preset**: The Preset will determine the scan rules for the project. Select the appropriate scanning Preset from the drop-down list.
3. **Configuration**: Select the Configuration for the new project. For the trial version, 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.



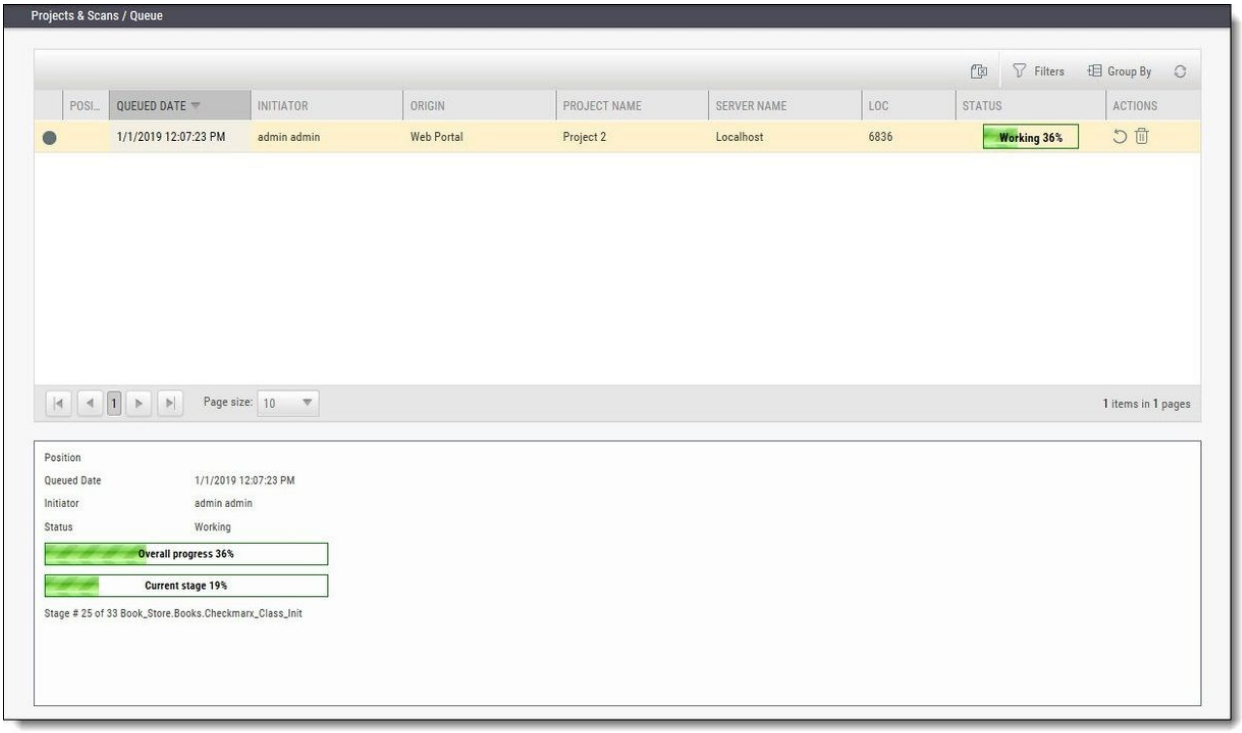
■ Note that you can scan the "**OWASP Benchmark Project**" code; go to https://github.com/OWASP/benchmark, click the **Clone or download** button and select your preferred option.

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

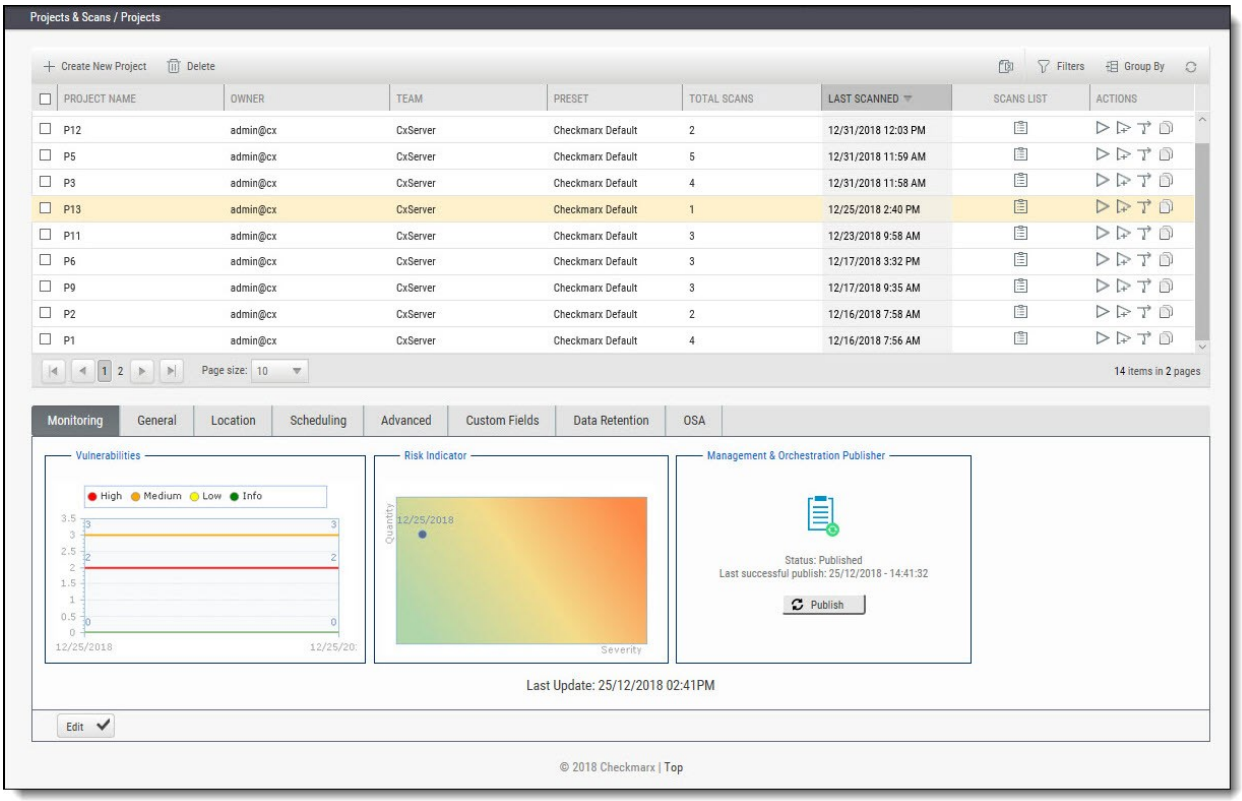
- In **Projects & Scans > Queue**, monitor the scan progress by clicking the project line in the queue table.



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

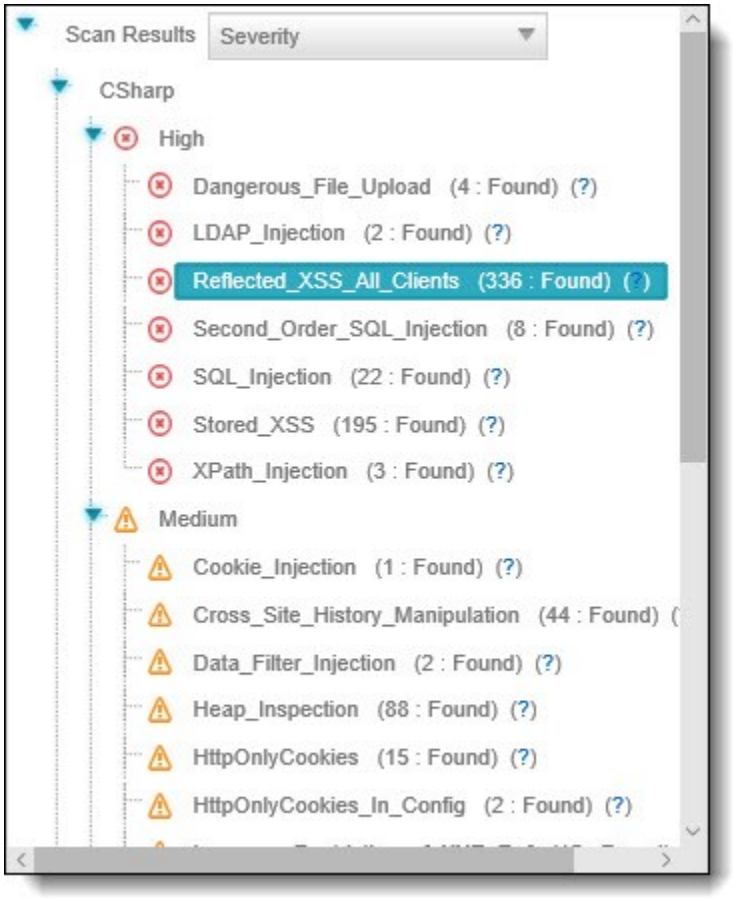
View detailed scan results within the Source Code. Vulnerabilities and navigated attack path are highlighted.

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

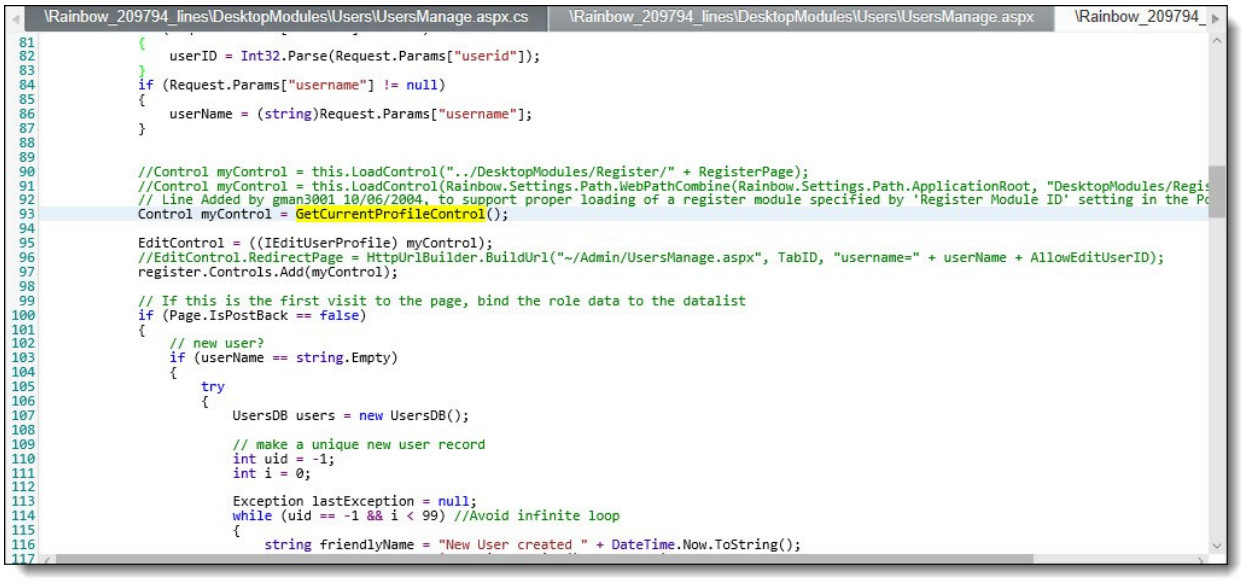
- Scan Results Summary by vulnerability,
- Results table or Graph,
- Attack Vector
- Source code

Scan Result Summary

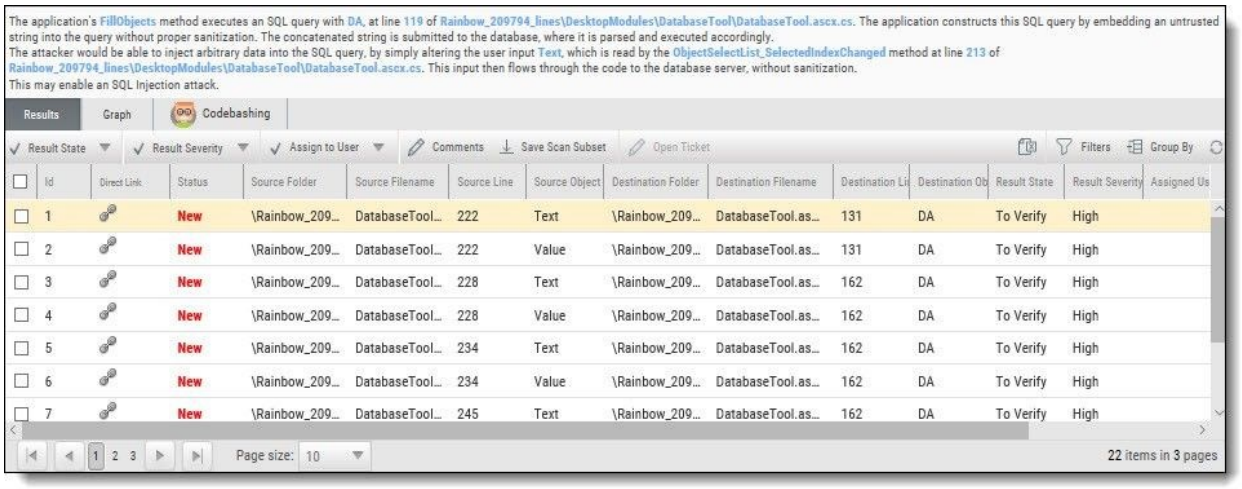
- **Scan Results Summary pane**: Summary of vulnerabilities detected, grouped by High, Medium and Low titles. The summary shows the number of instances of those vulnerability appearances in the code. The “tool tip” displays more information about the specific vulnerability and best practice technique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



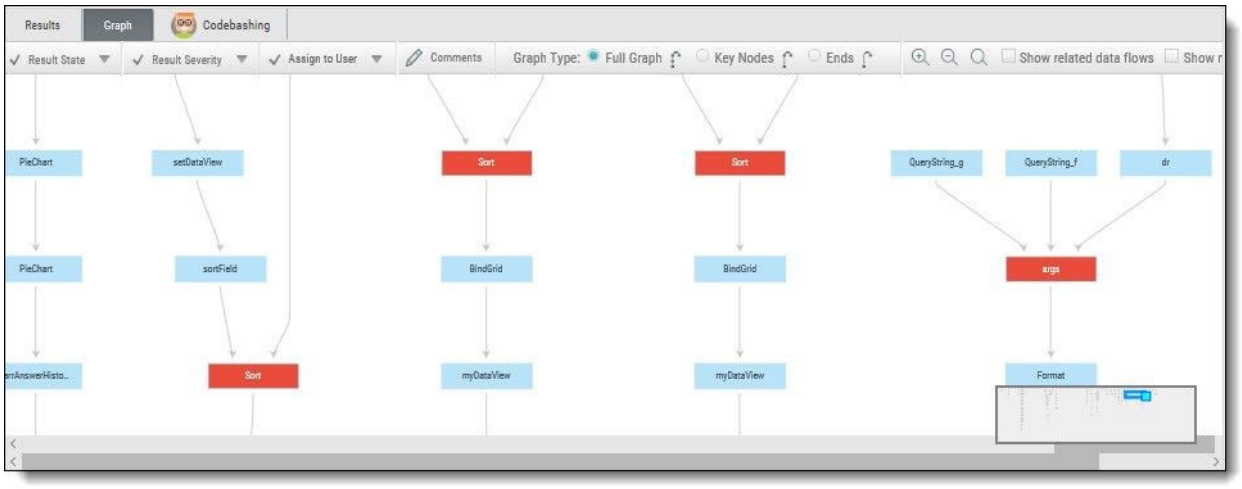
- **Source Code pane**: View specific points of vulnerabilities detected within the Source Code.



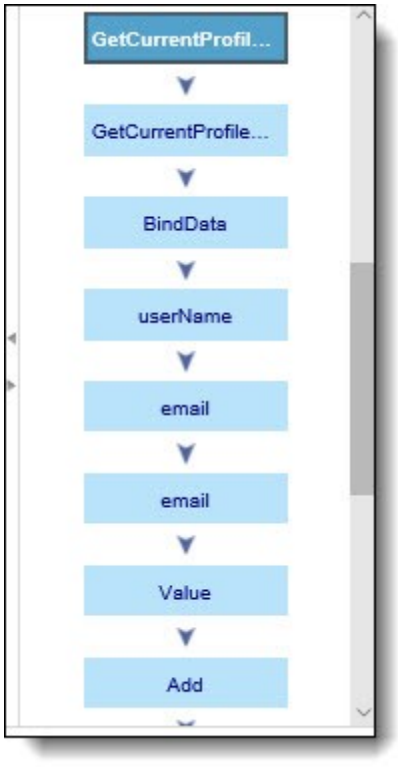
- **Results Table**: A listing of each vulnerability instance and detail. Manage results by using the Filter button to organizes data and saves results.



- **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.

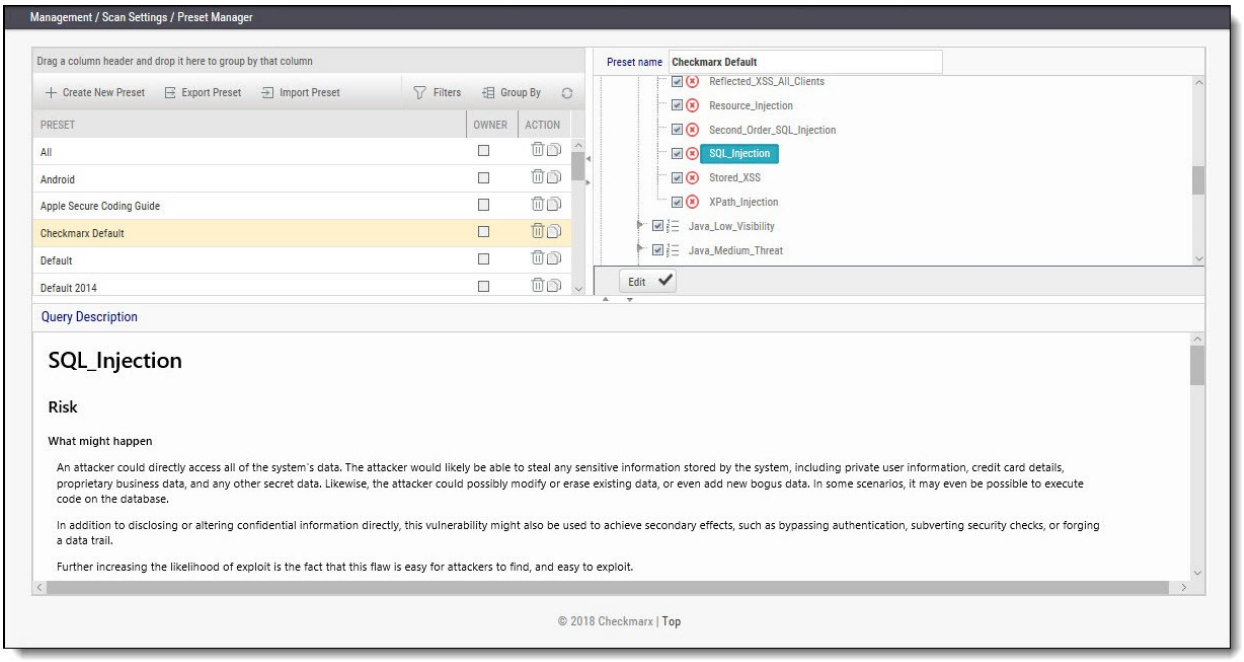


For more information on Working with Scan Results, see *Working with Scan Results*.

Preset Manager: Overview

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

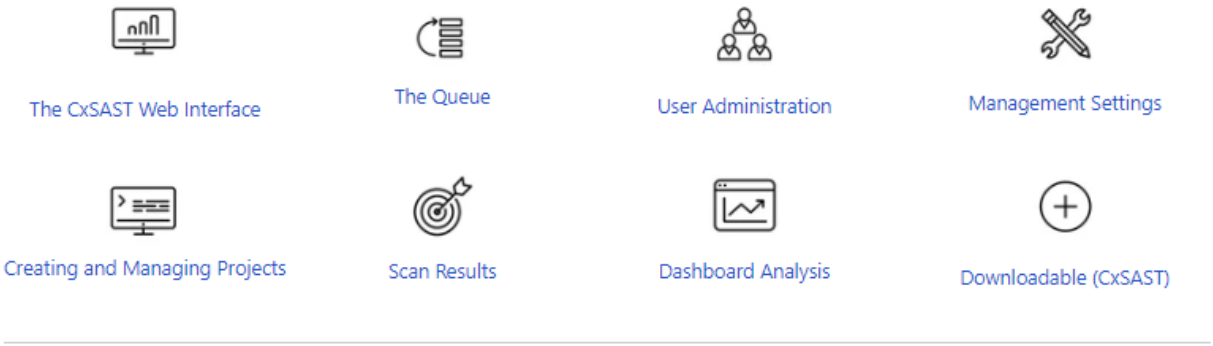
To access the Preset Manager go to **Management > Scan Settings > Preset Manager**. Queries contained inside the preset are presented in the right pane and description of vulnerability discovered by each query are described in **Query Description** below.



For more information on Managing Presets see *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

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

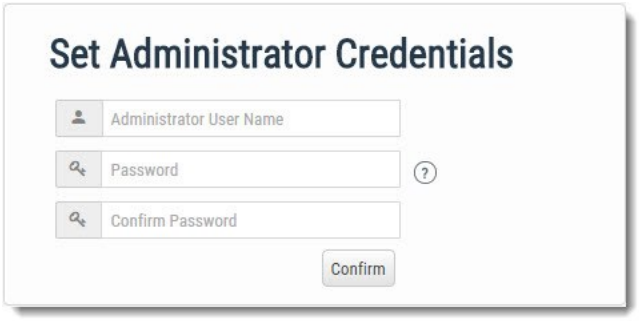
Access the CxSAST web interface in either of the following ways:

- 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.

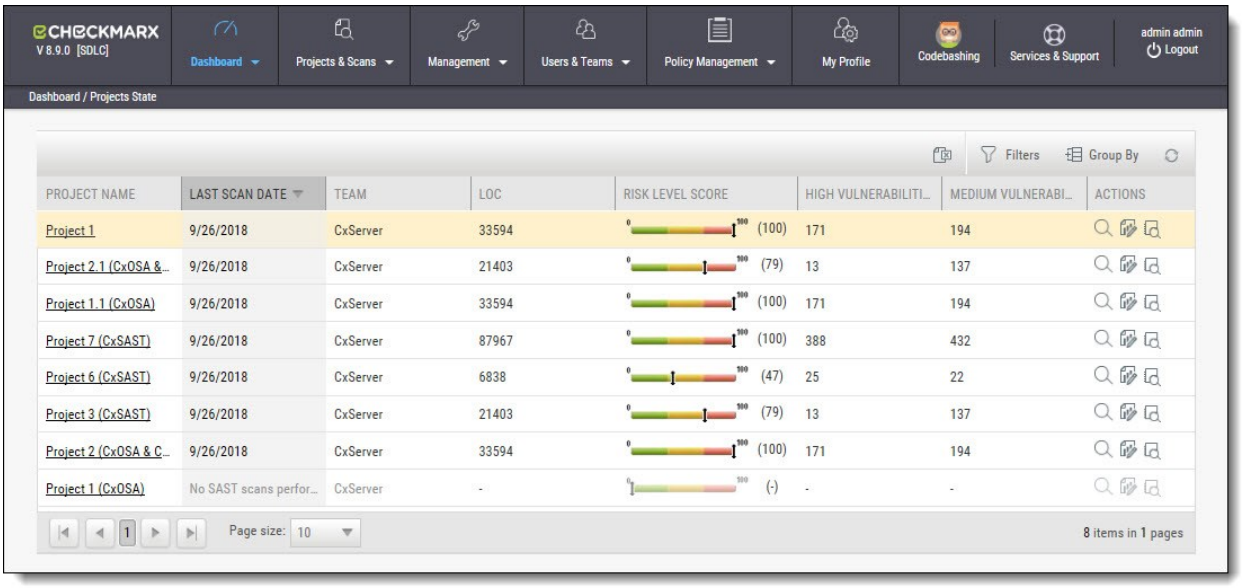
You can subsequently change the Administrator password and add CxSAST users.

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 Services &Support button allows CxSAST users to navigate to available support resources on our new Checkmarx Customer Center portal. This portal enables the option to open tickets and also provides access to useful Checkmarx links.

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**: Configure SAML for your environment.
- **Issue Tracking Settings**: Configure issue tracking

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.
- **External Services:** Define settings for external services (e.g. Codebashing).
- **Engine Management:** Manage single/multiple engines.

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

Unified Policy Management

- **Policy Manager:** Manage policies
- **Policy Violations:** View policy violations

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*.

Codebashing

Codebashing in-context eLearning platform. Codebashing is fully integrated into CxSAST so when developers encounter a security vulnerability they can activate the appropriate learning module at a single click. Once they have run through the hands-on training they get straight back to work equipped with the new knowledge to resolve the problem.

Services and Support

Checkmarx Customer Center with ticketing capabilities, access to the Checkmarx knowledge center and useful links to plugins, utilities and version updates.

Dashboard Menu

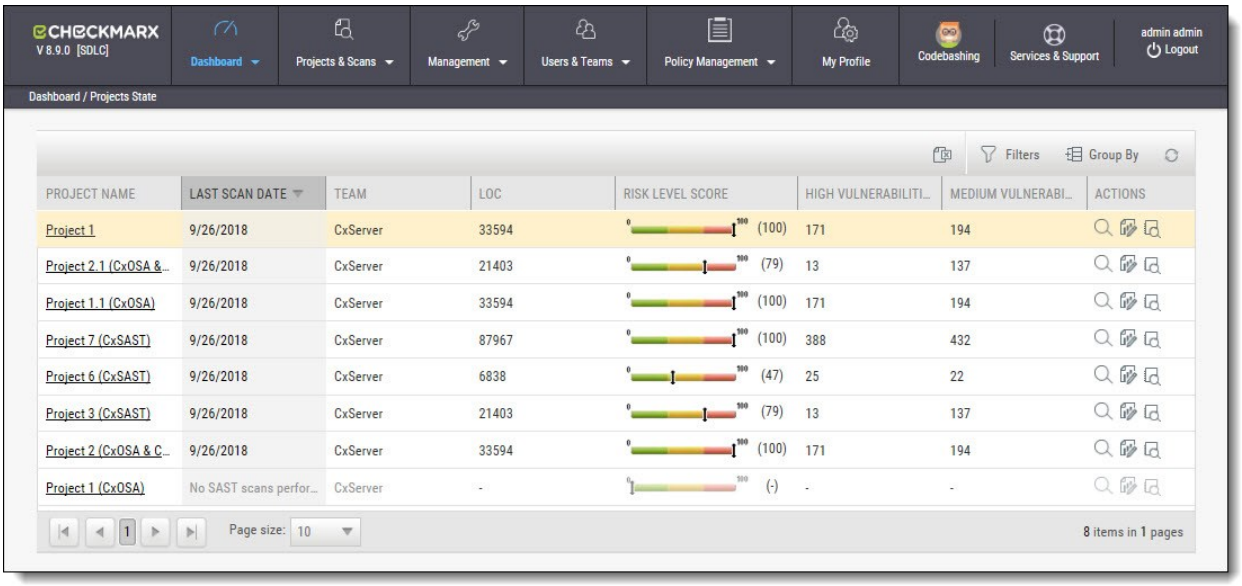
As a manager (Server, Company or Service Provider manager) you can view high-level information such as the state of your engines, project status, scans and queues in the Dashboard Menu.

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** (View results, Create report, Download scan logs)

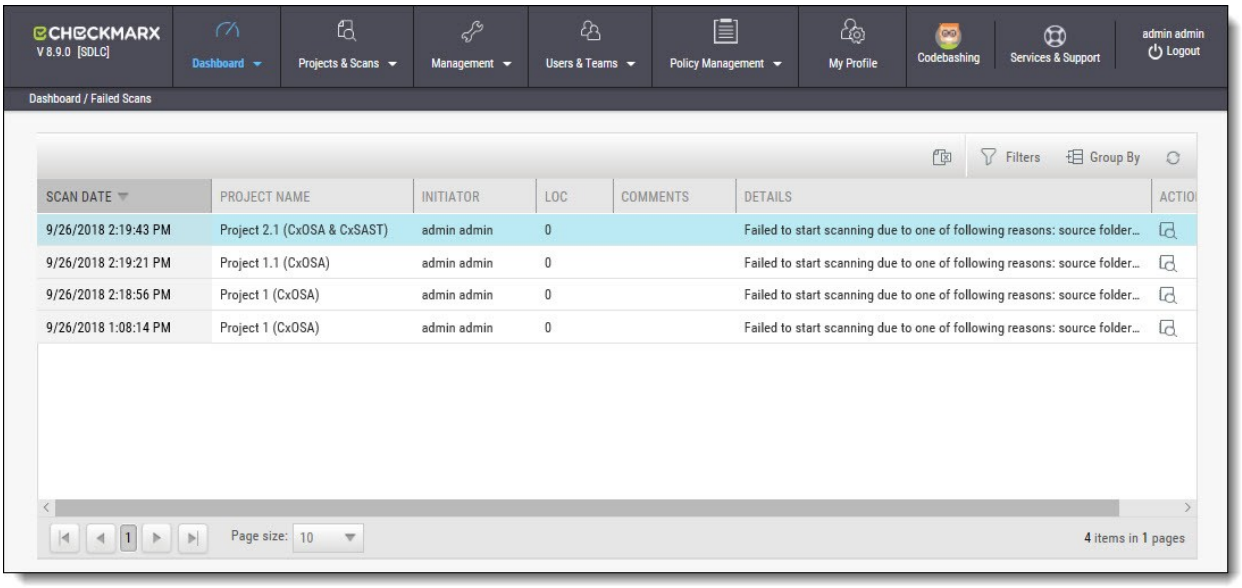
You can Export as CSV File , use the Filter and Group By tools as well as Refresh the current view.

■ 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:

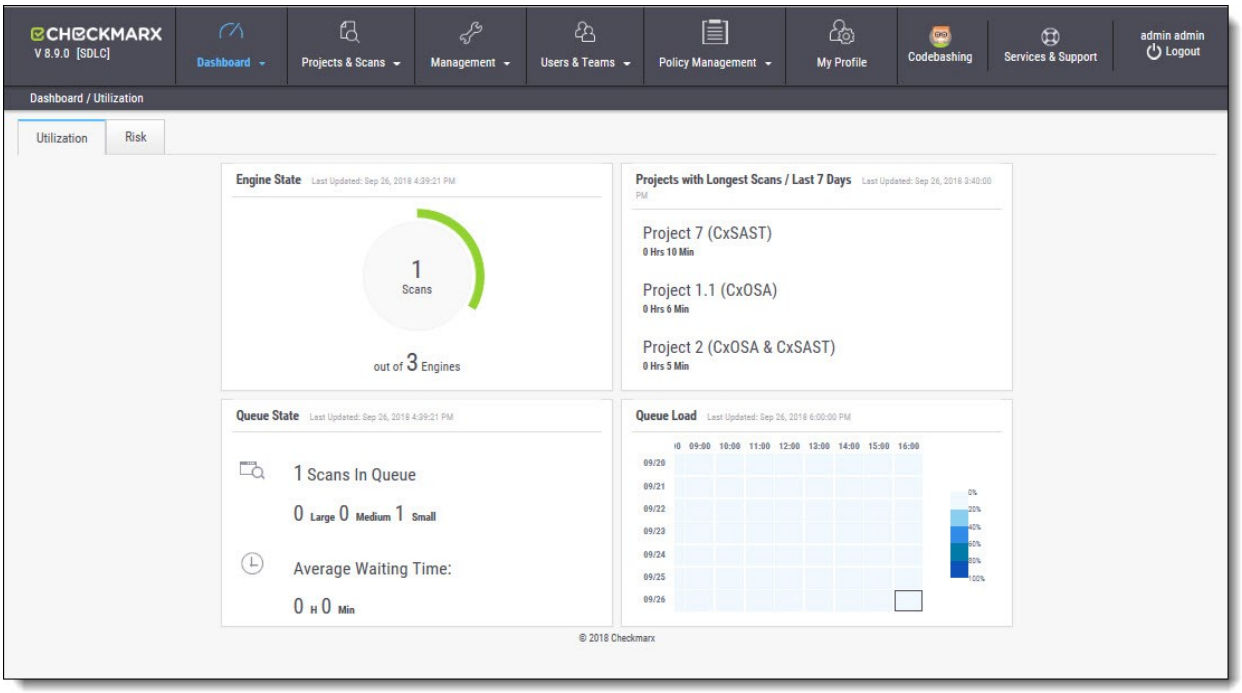
- **Scan Date**
- **Project Name**
- **Initiator**
- **LOC**
- **Comments** (as in The Queue)
- **Details**
- **Actions** (Download scan logs)

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:

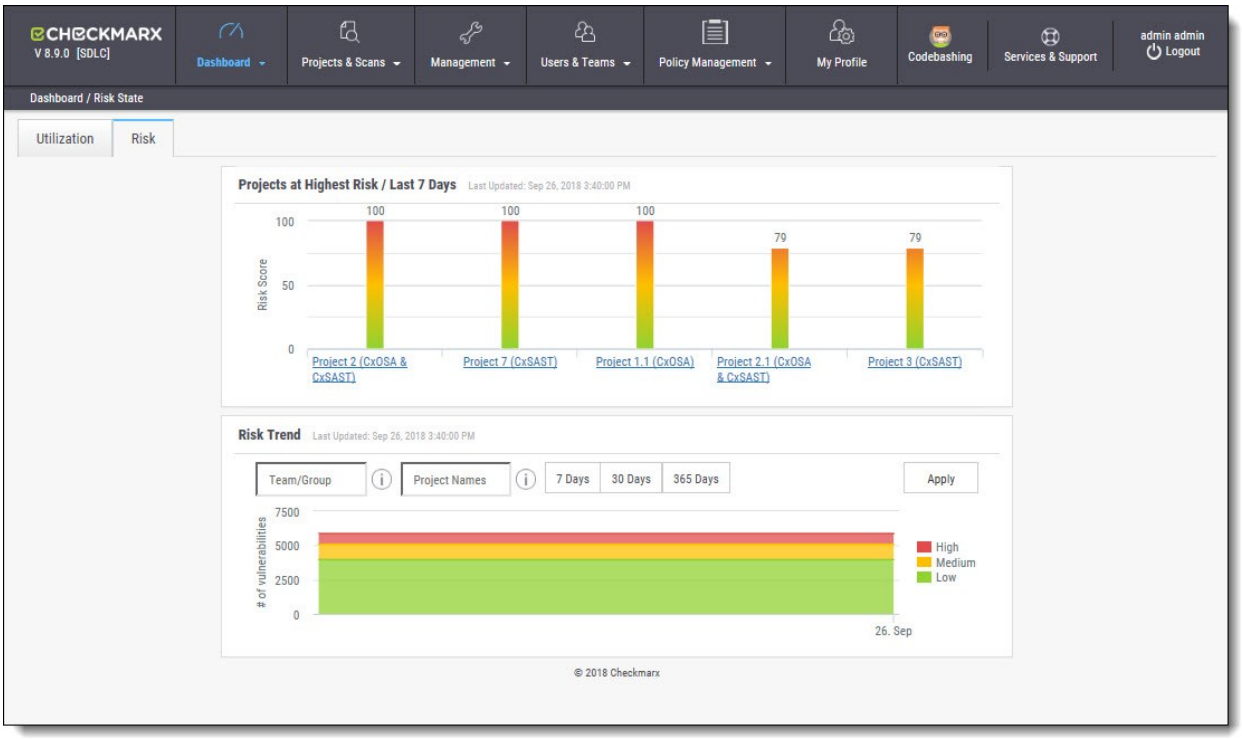
- **Engine State** - number of scans to engine ratio
- **Queue State** - number of scans in the queue and their LOC size / average waiting time
- **Projects with Longest Scans** - top 3 scans in the longest waiting time category
- **Queue Load** - queue load over a 7 day period:
    - The darker the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

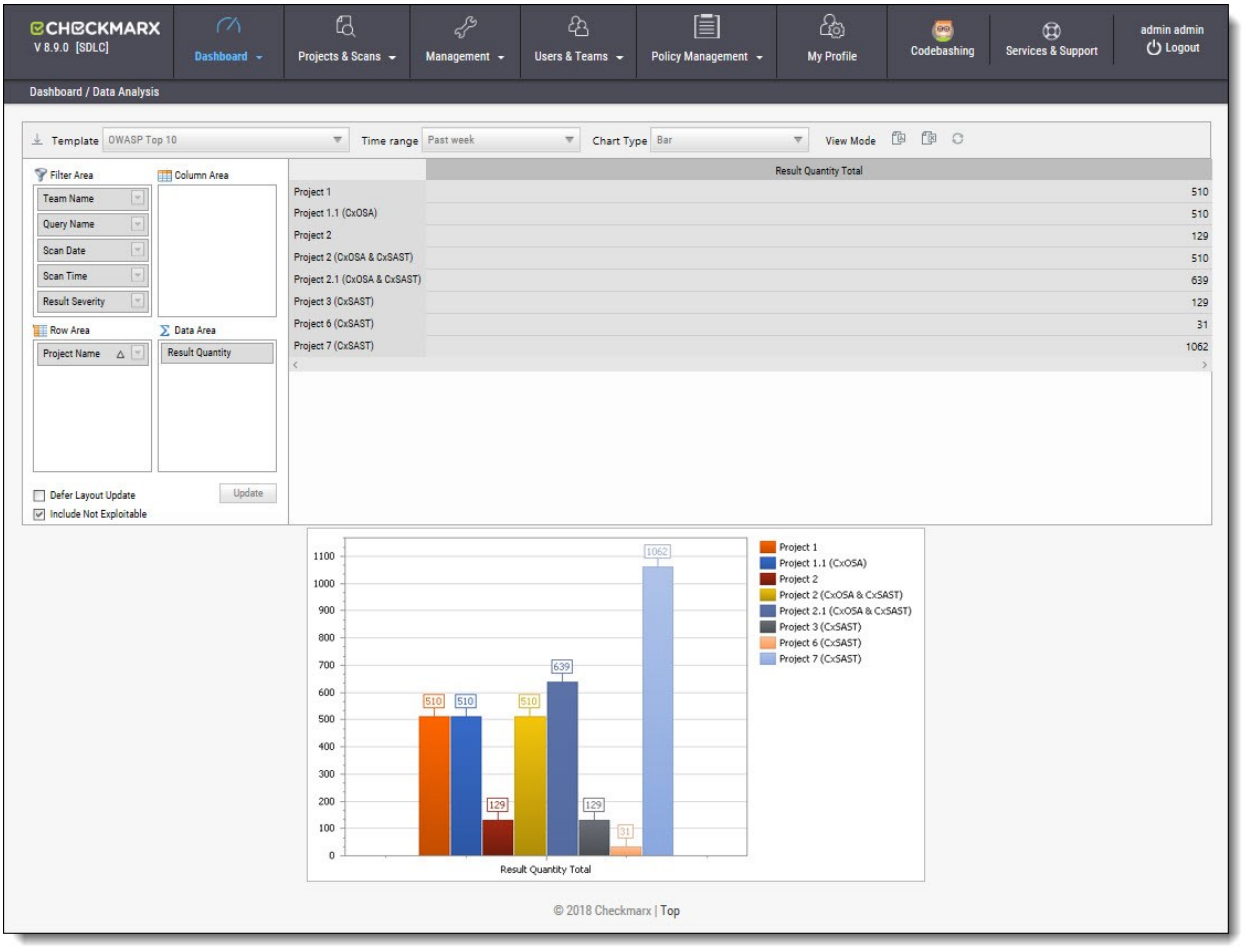
Click the legend to display/hide respective vulnerabilities (High, Medium, Low).

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

Data Analysis

The Data Analysis window displays a summary analysis of multiple projects. The data can be presented in several predefined configurations and you can also create your own tables.

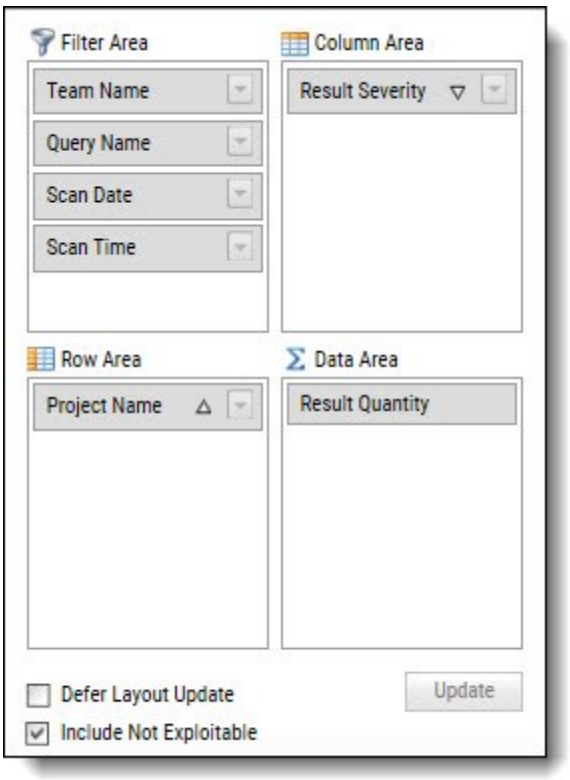
Go to **Dashboard > Data Analysis**. The Data Analysis window is displayed.



The data can be presented in several predefined configurations and you can also create your own tables.

In Template, select one of the following table configurations:

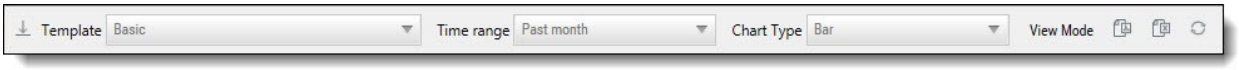
- Project Status: Displays data for most recent projects
- High & Medium: Displays data for projects with High or Medium severity
- Last week OWASP Top 10: Displays all projects last week results for OWASP Top 10 queries
- Basic: Create a pivot table from scratch. Drag and drop the relevant tab from 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**.

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



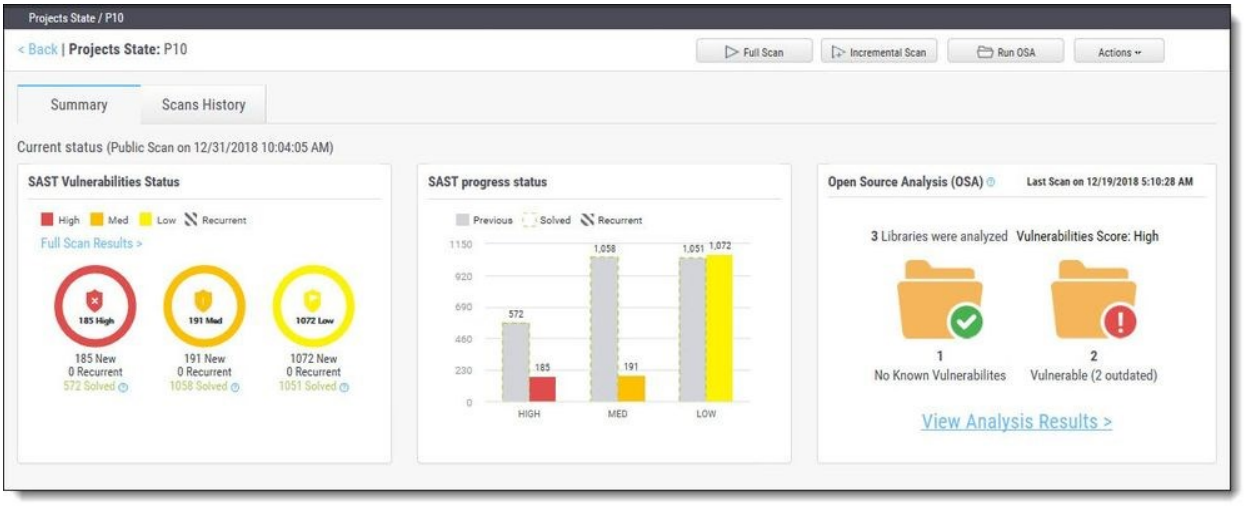
To save a custom table as a template, click **Save**.

Consolidated Project State

The Consolidated Project State window provides a high level summary of the status of each project.

To display the Consolidated Project State window:

Go to **Dashboard > Project State** and click the link on the **Project Name**. The Consolidated Project State window is displayed.



Summary

You can perform the following actions from the Consolidated Project State window:

- **Full Scan - p**erform a SAST scan for the whole project
- **Incremental Scan** - perform a SAST scan for only new and modified files since the last scan.
- **Run OSA** - perform Open Source Analysis on predefined open source libraries associated with this project.

> Note that a purchased or trial CxOSA license is required in order to run CxOSA projects. Please contact your Checkmarx Administrator.

> CI/Build plugins now use new core library with better compatibility and increased result accuracy. The new capability extracts dependencies resolving manifest files on the customer side. In order to avoid inconsistency between CxServer results and plugins - Run OSA from the Cx Web Interface was hidden in this version.

- **Additional Actions:**
  - **Edit Project** - displays the projects details
  - **Open Scan Summary** - displays the scan summary
  - **Open Viewer** - displays the scan results viewer
  - **CxOSA Viewer** - displays the CxOSA scan results viewer (see **CxOSA Viewer**).

> Action options on the Consolidated Project State window are available according to the user's permissions.

Current Status - Includes the time/date stamp indicating the date and time of the last SAST scan.

SAST Vulnerabilities Status

Provides a graph with the status of each vulnerability severity.

 ,  , - All new vulnerability instances discovered according to severity (high, medium and low)

 - Recurring vulnerability instances from previous scan

Solved is defined as vulnerabilities fixed/solved since last scan

> If no scans have yet been performed a "No Scans Performed" message is displayed. For more details about projects and scans, refer to *Creating and Configuring Projects*.
>
> If a new scan is currently in progress a "New Scan in Progress "message is displayed. For more details about the status of the scan, refer to the *Queue*.

Click the **Full Scan Results** link to display the **Scan List** for this project.

SAST Progress Status

Provides a graph with the progress status of each vulnerability severity.

 , , - All new vulnerability instances discovered according to severity (high, medium and low)

 - Vulnerability instances from previous scan

 - Fixed/solved vulnerability instances from previous scan

 - Recurring vulnerability instances from previous scan

Open Source Analysis (CxOSA)

Open Source Analysis (OSA) helps you manage the security risk involved in using open source libraries in your applications. This provides open source analysis results for predefined open source libraries associated with this project. Includes a stamp indicating the date and time of the last analysis.

- **No Known Vulnerable Libraries** - Number of libraries without any known security vulnerabilities.
- **Vulnerable Libraries -** Distribution of the vulnerable libraries:
  - **Vulnerable** - number of libraries that have at least one security vulnerability
  - **Outdated** - number of vulnerable libraries for which a newer version is available (major vs minor release).

■ If the Open Source Analysis license has not yet been enabled for this project a warning message is displayed. Please contact your Checkmarx Administrator.

Click the Run Analysis Now link to perform an Open Source Analysis. A "New Open Source Analysis is in progress" indicator is displayed.

■ If the Open Source Library directory location has not yet been configured and you try to run CxOSA, a warning message is displayed. Click on the link and define the Open Source Libraries location before continuing with the analysis.

For more information about Open Source Analysis (CxOSA), please see the *CxOSA Viewer*.

Scan History

Click the Scans History tab to display the scan results for the project.

CxOSA Viewer

Getting to Know the CxOSA Viewer

Once you have logged into the CxSAST application, the CxSAST web interface is displayed. To access the CxOSA Viewer, select a project from the Consolidated Project State screen, click the Actions button and select Open CxOSA Viewer from the drop-down. The CxOSA web interface includes navigation icons for each of the relevant modules:

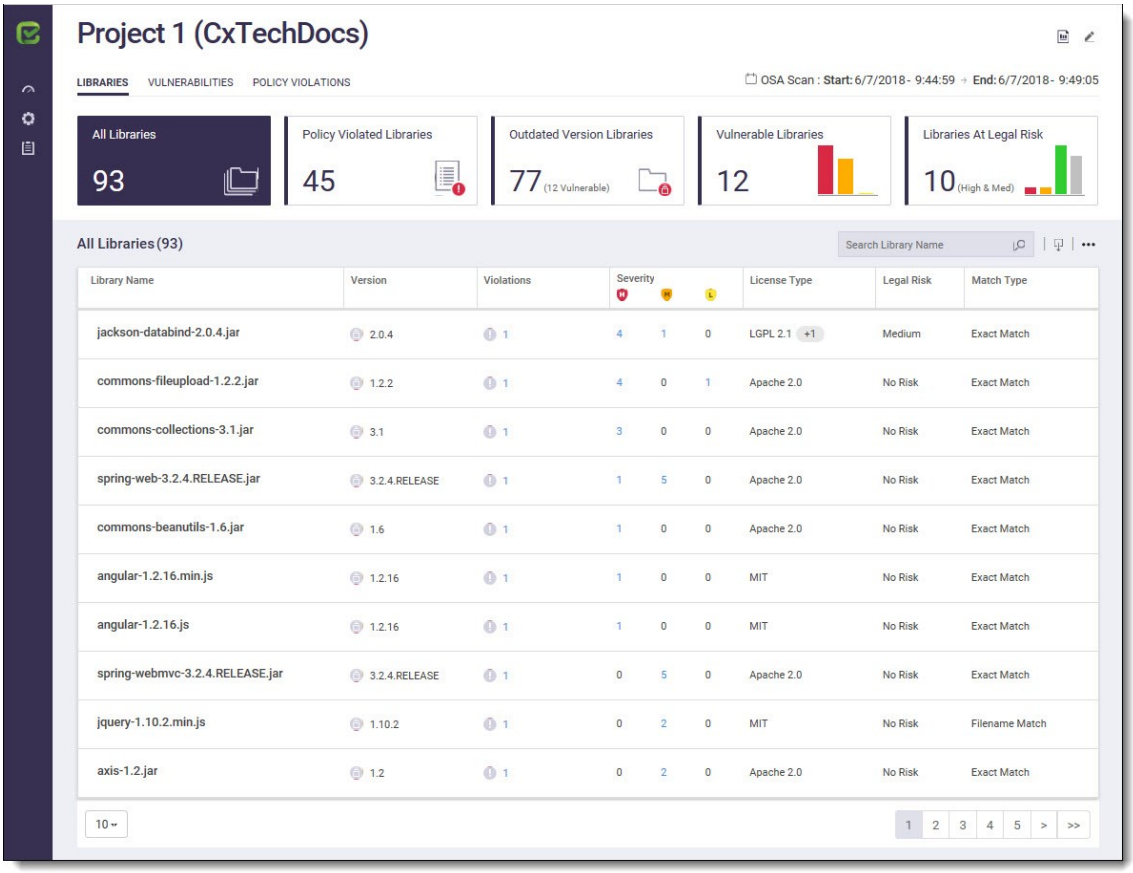
Project State – Provides access to the Consolidated Project State (see Consolidated Project State)

Application Settings – Provides access to Application Settings (see Application Settings)

Policy Management – Provides access to CxARM Policy Management (see CxARM Policy Management)

CxOSA Project View

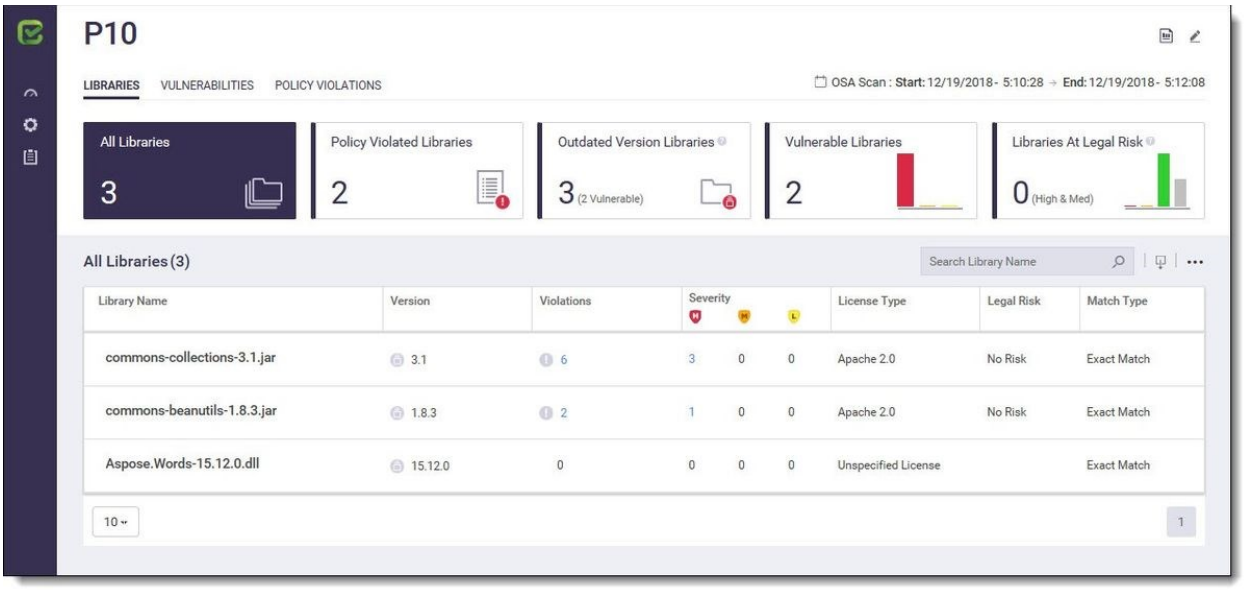
The CxOSA Project view displays the unique project name (top left), the scan type and the date and time the displayed scan started and ended (top right). An open Source Analysis report can be viewed by clicking on the Open Report icon (top right). See Open Source Analysis Report. You can edit the current project by clicking on the Edit Project icon (top right). See Editing a Project.



The Project view contains of the following two information tabs: Libraries and Vulnerabilities. Clicking on a tab displays the relevant view.

Libraries View

The Libraries view allows you to explore all the project's libraries. The Libraries list provides a list of all those libraries associated with the project. You can filter libraries in the Libraries list by All Libraries, Policy Violated Libraries, Outdated Version Libraries, Vulnerable Libraries and Libraries At Legal Risk by clicking on the relevant Dashboard Filter.



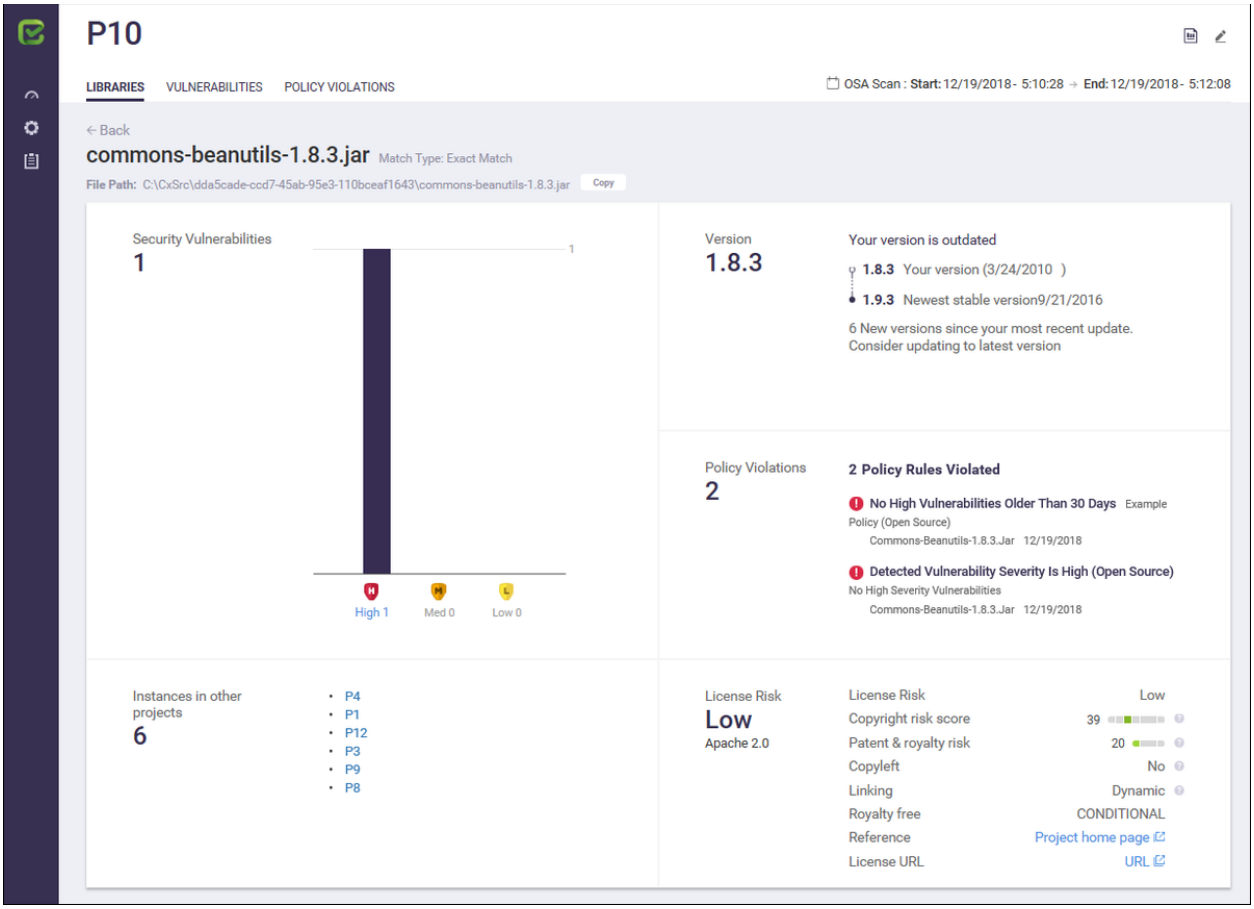
The Libraries List includes the following project libraries information:

Item	Description
Library Name	Name of the library. Clicking on the library link displays additional library status information (see *Library Status*)
	This allows you to export the scan results to a CSV format file for analysis purposes (see Exporting the Scan Results).
	This allows you to display only undetected libraries in the Libraries list.
	You can search for a specific library using the Search Library Name tool.

Item	Description
Version	This represents the library version being used. The icon indicates that the current library version is outdated. Mousing over the area provides additional information about the latest stable version available with release dates and the number of stable versions released in between both versions. No icon indicates the library version is up to date.
Violations	This represents the number of policy rule violated libraries. The icon indicates the policy violated library. Mousing over the area provides additional information about the policy violated library. No icon indicates that the library is not policy violated.
Severity	Distribution of the vulnerable libraries by severity.
	High – Vulnerable libraries stated with a high severity.
	Medium – Vulnerable libraries stated with a medium severity.
	Low – Vulnerable libraries stated with a low severity.
	Clicking on a severity link displays, the vulnerabilities associated with this library (see Project Vulnerabilities).
License Type	This represents the license type associated to the library. The icon indicates that there is more than one license type. If there are no license types associated to the library, 'No License' is indicated.
Legal Risk	This represents the possible legal risk level with regards to Copyright, Copyleft, Patent and Royalty, Linking and OSD Compliance. Possible risk states are high, medium, low or no risk. Additional information about legal risk is provided when drilling down to a specific library.
Match Type	Libraries that were not found using the SHA-1 Hash, will be matched by the provided filename. Possible values are: • Filename Match – Where match is done only by name • Exact Match – Where match is done by finger print

Library Status

Clicking on the library link in the Project Libraries list displays additional library status information (see *Project Libraries*).



The Library Status includes the following information:

Item	Description
Library File Name	Name of the library file
Match Type	Libraries that were not found using the SHA-1 Hash, will be matched by the provided filename. Possible values are: • Filename Match – Where match is done only by name • Exact Match – Where match is done by finger print
Security Vulnerabilities	This represents the severity (High Medium, Low) of security vulnerabilities discovered in the library.

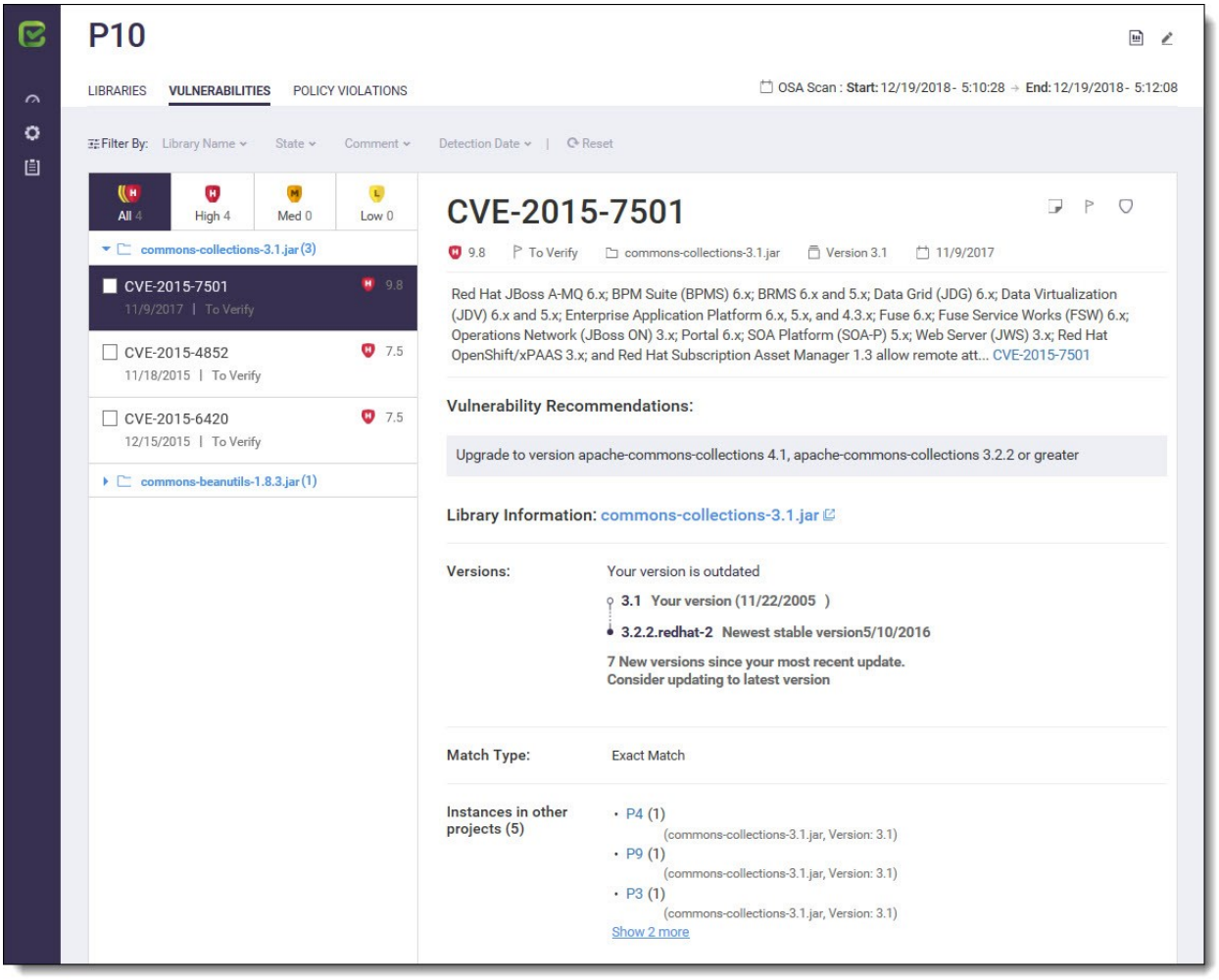
Item	Description
	Clicking on a severity link displays the vulnerability(s) associated with this library (see Project Vulnerabilities).
Instances in other projects	This represents instances of the same library being used in other projects. Provides an active link to the other project.
Version	Details regarding the version being used and the latest stable version available with release dates and the number of stable versions released in between both versions. A 'version is up to date' label is displayed when the version is up to date.
Policy Violations	This represents the policy violation associated with the library status. Information includes the number of policy violations, the rule that triggered the policy violation and the detection date of the policy violation.
License Risk	This represents the possible legal risk level with regards to licensing. Possible license risk states are: High, Medium, Low or No Risk. Also displayed is the following license compliance information:
	License Risk - Low, Medium, High or Unknown

Item	Description
	Copyright Risk Score - range according to score level (0 – 100%) • 13% - Licensee may use code without restriction • 26% - Anyone who distributes the code must retain any attributions included in original distribution. • 39% - Anyone who distributes the code must provide certain notices, attributions and/or licensing terms in documentation with the software. • 52% - Anyone who distributes a modification of the code may be required to make the source code for the modification publicly available at no charge. • 65% - Anyone who distributes a modification of the code or a product that is based on or contains part of the code may be required to make publicly available the source code for the product or modification, subject to an exception for software that dynamically links to the original code (example: LGPL). • 78% - Anyone who distributes a modification of the code or a product that is based on or contains part of the code may be required to make publicly available the source code for the product or modification (example: GPL). • 91% - Anyone who develops a product that is based on or contains part of the code, or who modifies the code, may be required to make publicly available the source code for that product or modification if s/he (a) distributes the software or (b) enables others to use the software via hosted or web services (example: Affero).
	Patent & Royalty Risk - range according to score level (0 – 100%) • 20% - Royalty free and no identified patent risks • 40% - Royalty free unless litigated. • 60% - No patents granted • 80% - Specific identified patent risks
	Copyleft - Full (CopyLeft on modifications as well as own code that uses the OSS), Partial (CopyLeft applies only to modifications) or No (not a CopyLeft license).
	Linking – Viral (will substantially infect the code linked to this OSS), Non Viral (will not affect the licensing of the linking code) or Dynamic (dynamic linking will not infect).
	Royalty Free - Yes, No or Conditional
	Mouse over each compliance result to display information about the risk factor

Item	Description
	Clicking on the Reference link provides a downloadable reference, e.g. XML file (.pom)
	License URL - Clicking on the License URL link takes you directly to the official license web page.

Vulnerabilities View

Clicking on the Vulnerabilities tab displays the Vulnerabilities view. The Vulnerabilities view allows you to explore all the vulnerable libraries associated with the selected project.



The Vulnerabilities view includes the following vulnerable libraries information:

Item	Description
Filter By	Using the filtering tool allows you to filter vulnerabilities according to single or multiple selections.
	Library Name – Filter by library name
	State – Filter by vulnerability state. Filtering options: To Verify, Not Exploitable, Confirmed, Urgent, Propose Not Exploitable
	Comment – Filter by user defined comment
	Detection Date – Filter by specific date
	Reset – Reset the filter to its pre-defined state
Vulnerable Libraries List	Lists all the vulnerable libraries according to the selected severity type
	All – All vulnerable libraries regardless of severity
	High – Vulnerable libraries stated with high severity
	Medium – Vulnerable libraries stated with medium severity
	Low – Vulnerable libraries stated with low severity
	Clicking on a severity type displays only those vulnerable libraries associated with the selected severity. All vulnerabilities listed here are in relation to the vulnerable library selected.
Vulnerability Actions	Clicking on one of the Action options (far right) or selecting a check-box in the Vulnerable Libraries List enables you to perform certain actions on the selected libraries/vulnerabilities.
	Add Comment – Add a comment to the selected vulnerability(s). See *Adding a Comment to a Vulnerability(s)*.
	Change State – Change the state of the selected vulnerability(s). See *Changing the State of a Vulnerability(s).*
	Change Severity – Change the severity of the selected vulnerability(s). See *Changing the State of a Vulnerability(s).*

Item	Description
Vulnerability Status	Represents the vulnerability according to the current selection and includes all related information about the vulnerability.
	Vulnerability – This represents the name of the vulnerability (e.g. CVE-2015-4852).
	Severity – This represents the severity of the vulnerability:
	 **High** – Vulnerabilities stated with high severity
	 **Medium** – Vulnerabilities stated with medium severity
	 **Low** – Vulnerabilities stated with low severity.
	7.5 – This represents vulnerability score.
	 – This represents the state of the vulnerability. Possible states are: To Verify (default), Confirmed, Suspicious, Not a Problem, Remediated.
	 – This represents name of the vulnerable library
	 – This represents the current version of the vulnerable library
	 – This represents the date and time and that the vulnerability was first discovered.
Description	Displays comprehensive information about the selected vulnerability, including risk details, a description of the cause and mechanism and may provide, if available, an active link to additional information about the vulnerability.
Vulnerability Recommendations	Displays recommendations for avoiding the vulnerability.
Library Information	Provides an active link to additional information about the vulnerable library (see Project Libraries).
Versions	Provides details regarding the library version being used and the latest stable version available with release dates and the number of stable versions released in between versions.

Item	Description
Match Type	Libraries that were not found using the SHA-1 Hash, will be matched by the provided filename. Possible values are: • Filename Match – Where match is done only by name • Exact Match – Where match is done by finger print
Instances in other projects	This represents instances of the same library being used in other projects. Provides an active link to the other project.

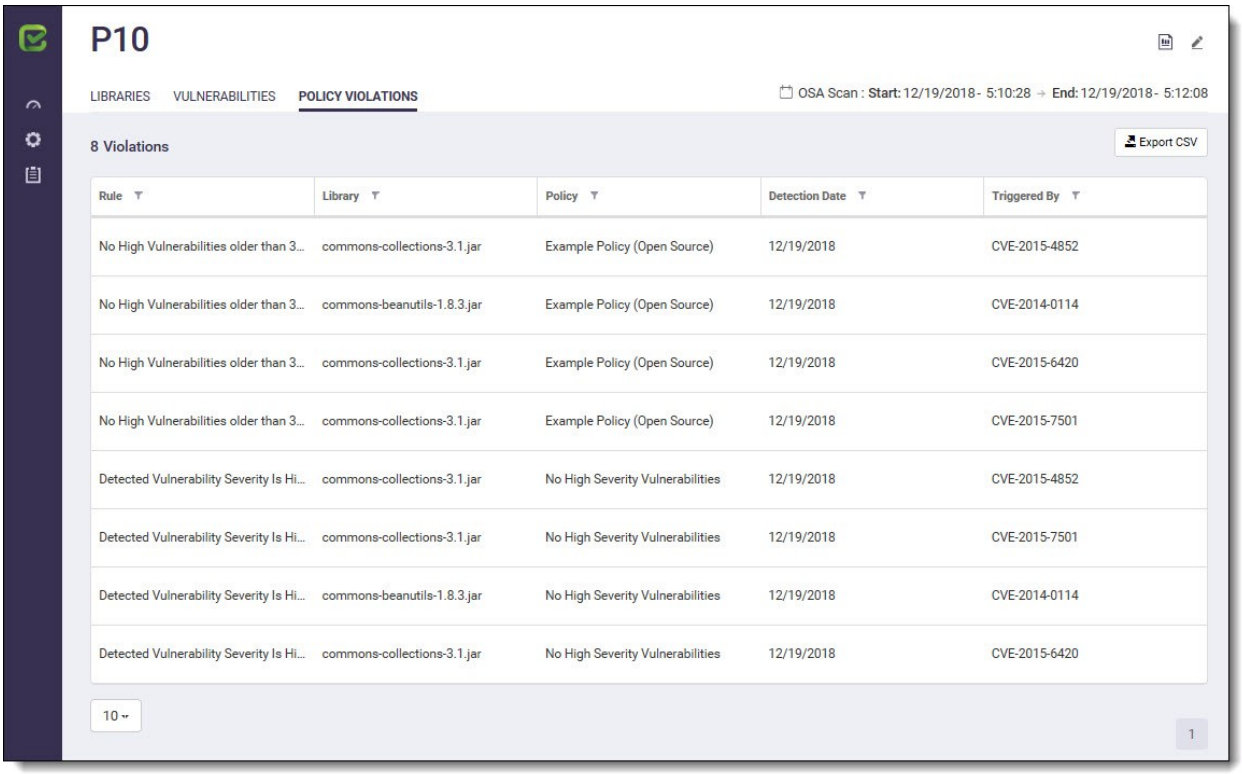
Policy Violations View

Policy Management provides a centralized management console for defining, managing and tracking an organization's acceptable security risk across all its applications and projects, using unified application security policies across customer/proprietary code and open source components.

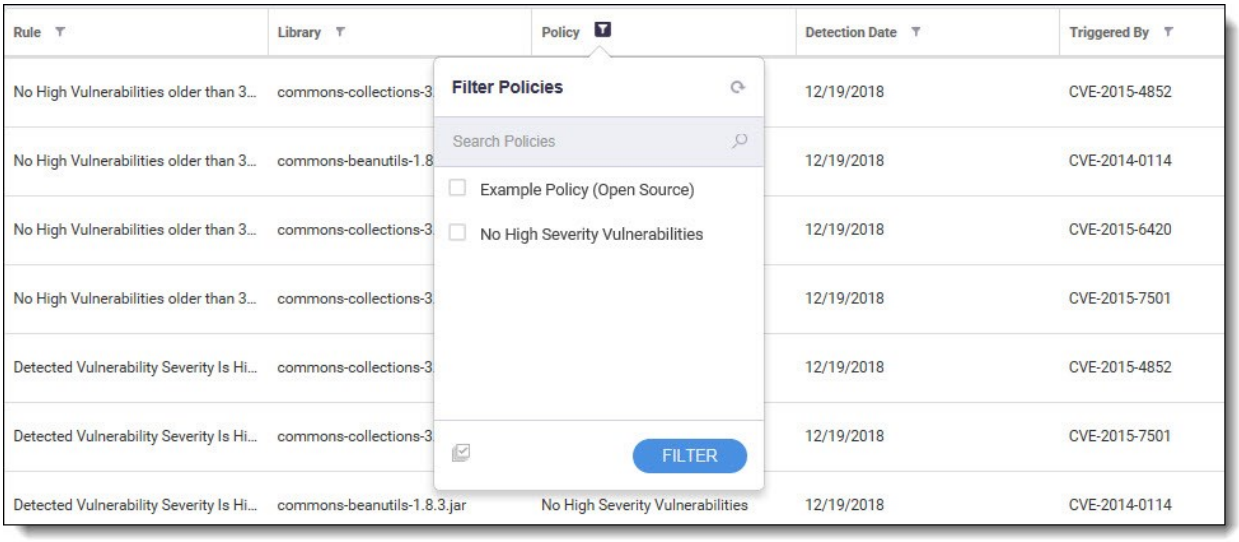
A security policy is comprised of customer-defined rules that serve to define compliance, and against which violations occur. After a policy is created, it can then be assigned to one or more projects. Multiple policies can also be defined per project.

Policy Management supports CxOSA rules pertaining to the library, license and vulnerabilities. For more information about this subject, see Policy Management.

Clicking on the Policy Violations tab displays the Policy Violations view. The Policy Violations view allows you to explore all the policy violations associated with the selected project.



You can filter policy violations in the Violations List by Rule, Library, Policy (example below), Detection Date and Triggered By, by clicking on the filter and selecting the relevant search option(s).



The Violations List includes the following policy violation information:

Item	Description
# Violations	Number of policy violation associated with the selected project.
Export to CSV	This allows you to export the policy violation results to a .CSV format file for analysis purposes (see Exporting the Results).
Rule	The rule currently being used in the policy. See CxARM Policy Management for more information about defining policy violation rules.
Library	This represents the policy violated library
Policy	The policy currently being used in the project. See CxARM Policy Management for more information about defining policies.
Detection Date	Detection date of the policy violation
Triggered By	The library that triggered the policy violation

Adding a Comment to a Vulnerability(s)

Selecting a check-box in the Vulnerable Libraries List enables you to add a comment to a vulnerability. This is useful for defining how to handle the vulnerability.

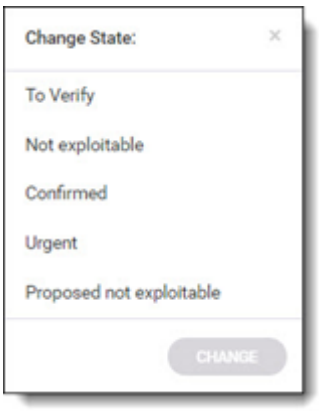
Once the vulnerability checkbox is selected, click the Add Comment icon. The Add Comment dialog is displayed.

Type in your comment and click Add. The Comment is displayed in the Vulnerabilities List.

Changing the State of a Vulnerability(s)

Selecting a check-box in the Vulnerable Libraries List enables you to change the state of a vulnerability. This is useful for disregarding false positives or just for defining what vulnerabilities to handle and how to handle them.

Once the checkbox is selected, click the Change State icon. The Change State dialog is displayed.



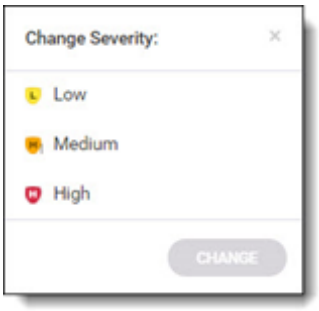
Select the state. The following states can be defined:

State	Description
To Verify (default)	Vulnerability requires verification, for example, by an authorized user
Not Exploitable	Vulnerability has been confirmed as not exploitable (i.e. false positive)
Confirmed	Vulnerability has been confirmed as exploitable and requires handling
Urgent	Vulnerability has been confirmed as exploitable and requires urgent handling
Proposed Not Exploitable	Vulnerability has been proposed as not exploitable, for example, as a potential false positive. Vulnerabilities defined with this state remain a potential threat until such a time that the state is changed to 'Confirmed' or 'Not Exploitable'

Changing the Severity of a Vulnerability(s)

Selecting a check-box in the Vulnerable Libraries List enables you to change the severity of a vulnerability. This is useful for defining a new severity to the vulnerability during handling.

Once the checkbox is selected, click the Change Severity icon. The Change Severity dialog is displayed.



Select the Severity. The following severities can be defined:

Severity	Description
Low	Vulnerabilities stated with low severity
Medium	Vulnerabilities stated with medium severity
High	Vulnerable libraries stated with high severity

Click Change. The severity of the vulnerability is changed and is displayed in the Vulnerabilities List.

Exporting the Scan Results (.csv)

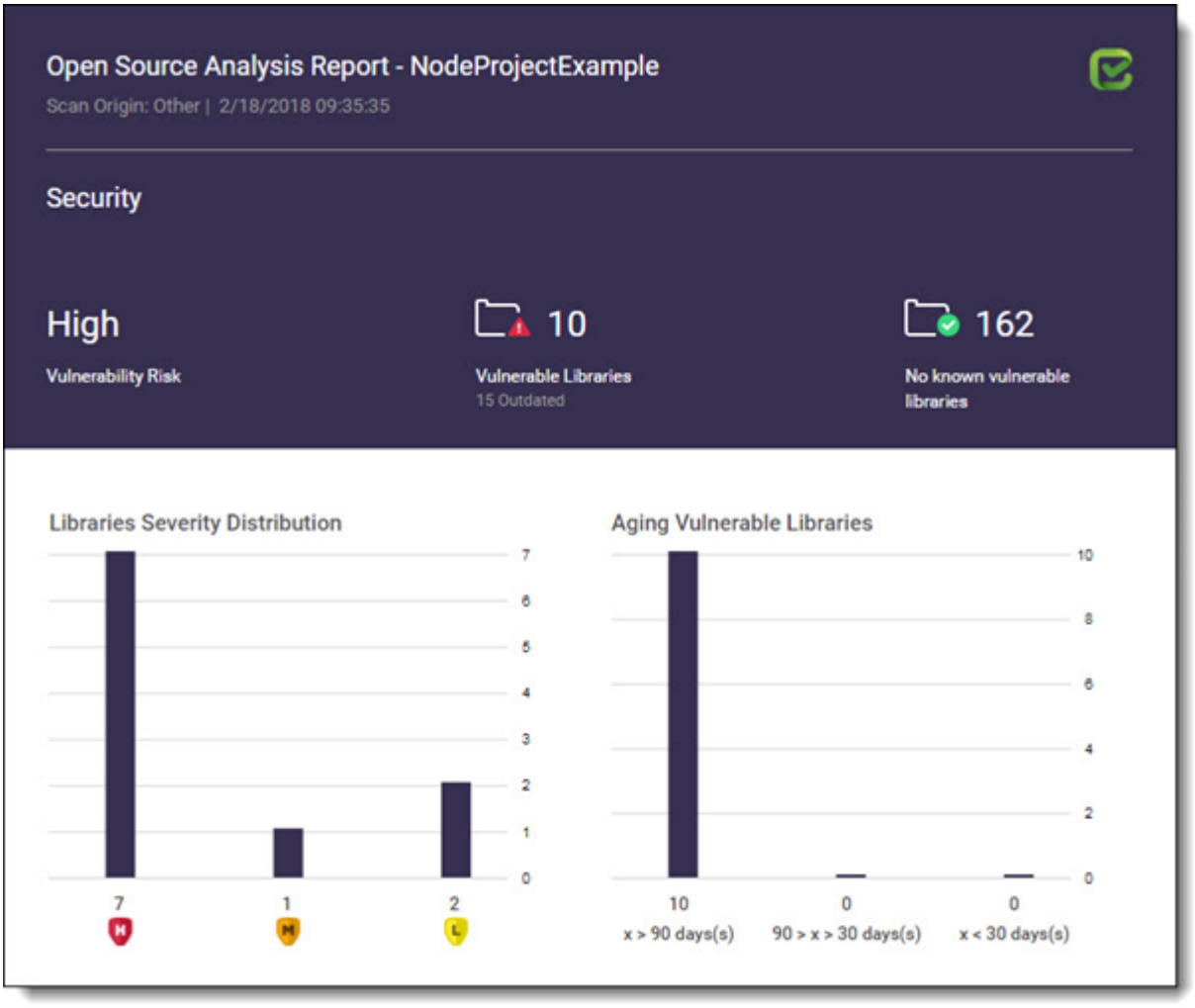
Once the scan results become available you have the capability to export the library table to a comma-separated values (.csv) file.

Open Source Analysis Report

The Open Source Analysis report can be viewed by clicking on the Open Report icon in the CxOSA Project view (top right) regardless of which tab you are currently viewing. For information about the CxOSA Report, see *Open Source Analysis Report*.

Open Source Analysis Report

The Open Source Analysis report can be viewed by clicking on the Open Report icon in the CxOSA Project view (top right) regardless of which tab you are currently viewing.



The **Open Source Analysis Report i**ndicates the scan origin from which the the analysis was performed. Also includes the time/date stamp indicating the date and time of the last analysis.

Security

Security panel provides information about the distribution of security issues for the project and is divided into the following major categories:

Vulnerability Risk

The maximum security severity across all security vulnerabilities found - High, Medium or Low

Vulnerable Libraries

Distribution of the vulnerable libraries:

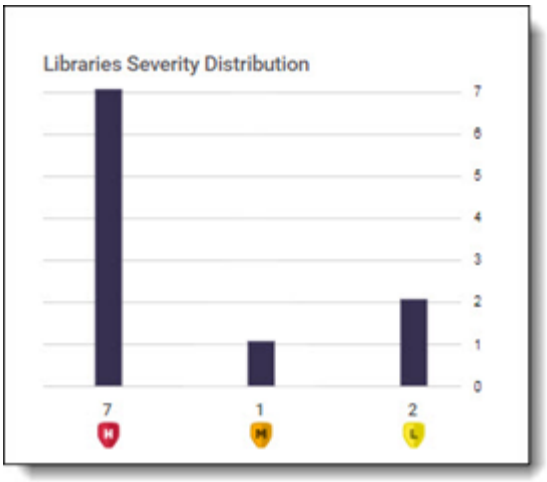
- **Vulnerable**- number of libraries that have at least one security vulnerability
- **Outdated** - number of vulnerable libraries for which a newer version is available (major vs minor release)

No Known Vulnerable Libraries

Number of libraries without any known security vulnerabilities.

Library Severity Distribution

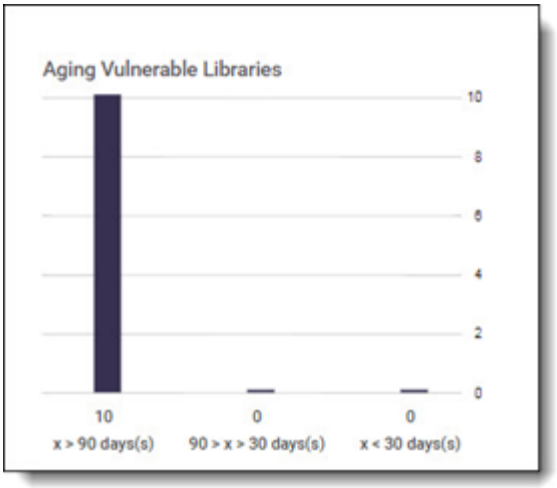
Distribution of the vulnerable libraries by severity. Indicates the number of libraries that have at least one security vulnerability with severity - High, medium or Low.



Aging Vulnerable Libraries

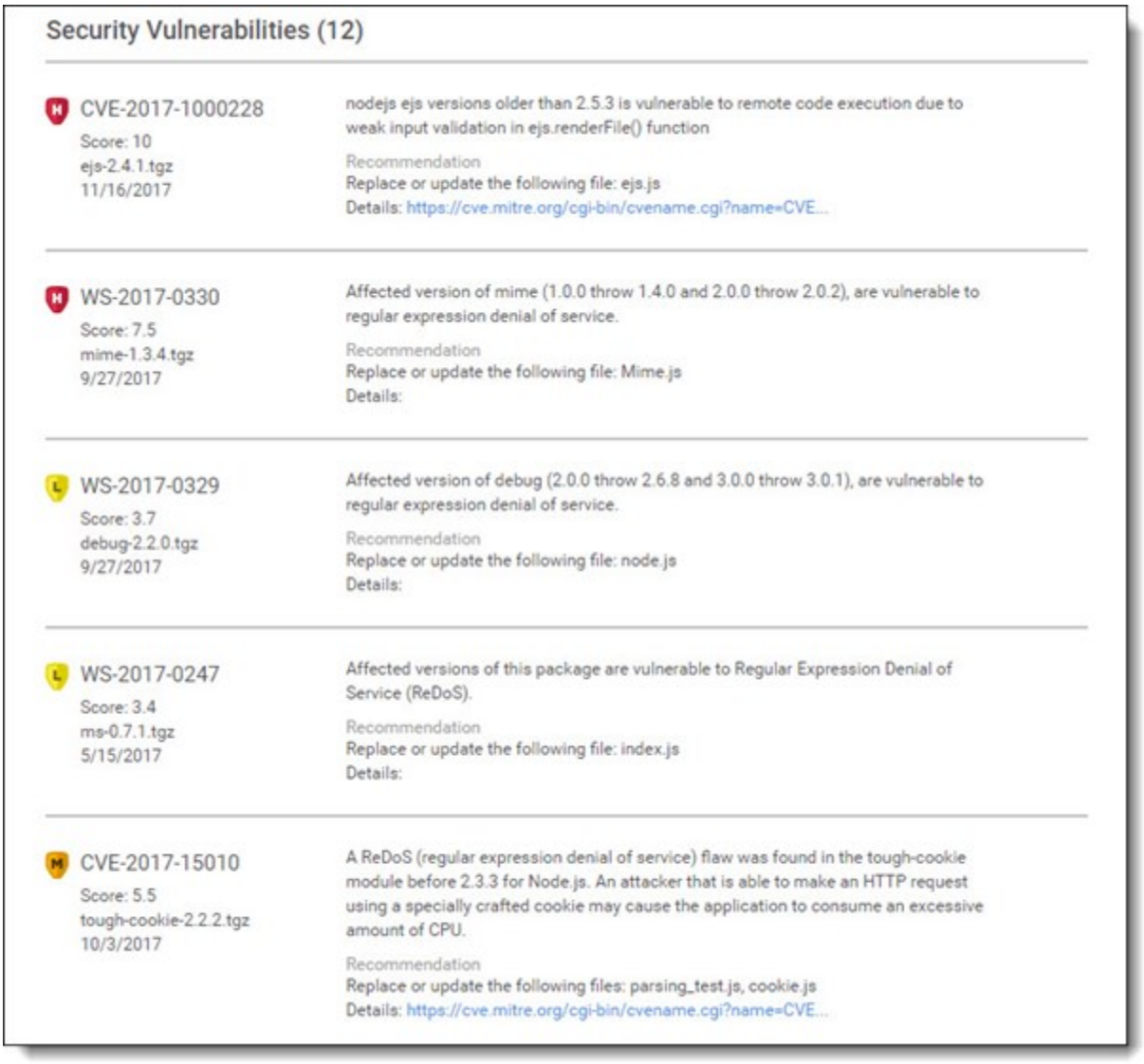
Distribution of vulnerable libraries by timeline:

- **X > 90 day(s)** - number of libraries that have at least 1 security vulnerability that was exposed more than 90 days ago
- **90 > x > 30 day(s)** - number of libraries that have at least 1 security vulnerability that was exposed between the last 30 and 90 days
- **X < 30 day(s)** - number of libraries that have at least 1 security vulnerability that was exposed in the last 30 days.



Security Vulnerabilities

The Security Vulnerabilities panel provides a list of security vulnerabilities ordered by vulnerability score. The number in parenthesis is the number of vulnerabilities.



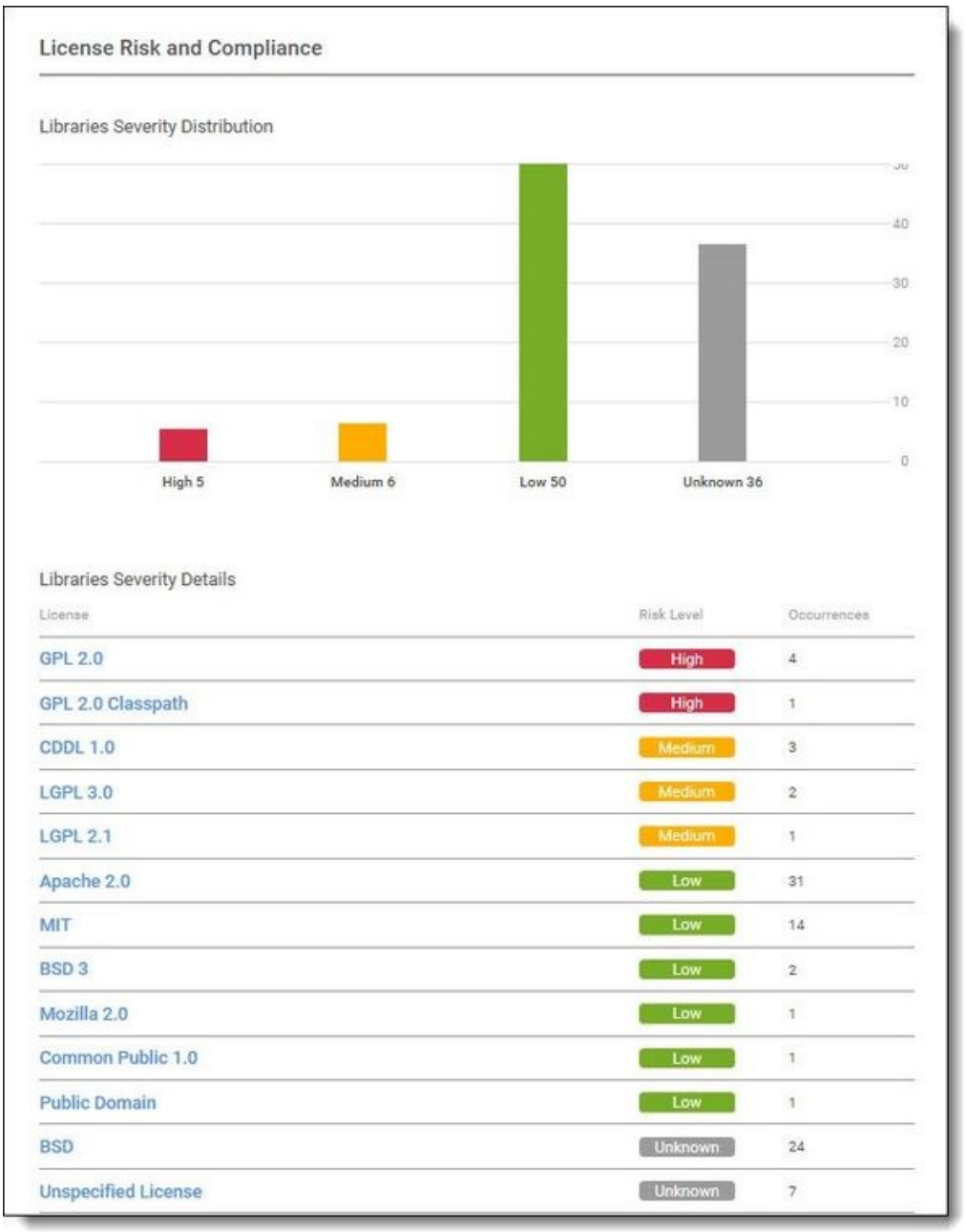
The Security Vulnerabilities list includes the following information:

- **Vulnerability** - the security vulnerability severity (High / Medium / Low) name, score (0 - 10) and publish date.
- **Library** - name of the library that has this security vulnerability
- **Description** - detailed description of the security vulnerability
- **Recommendation** - list of references to possible fixes, patches and further information regarding the security vulnerabilities. Includes a link to the CVE reference (i.e. CVE-2013-4316), if available.

- In some cases the CVE reference is not provided for security vulnerabilities. The vulnerability database is based on data from multiple official sources like NVD, Node Security etc. CxOSA detects vulnerabilities by searching the database and only displays a detection if there is a match for specific components or sub-components. This procedure eliminates "false-positive" detection and ensures that the user is only provided with the most accurate and reliable information. Not all security vulnerabilities have a specific CVE reference ID. In these cases we use our own internal identifier.

License Risk and Compliance

The License Risk and Compliance panel provides the distribution of project's open source libraries by type of license and the level of risk associated with each license.



Libraries Severity Distribution

Distribution of project's open source libraries by severity

Libraries Severity Details

Distribution of project's open source libraries by type of license, level of risk and occurrence:

- **License** - the name of the license
- **Risk Level** - this represents the possible legal risk level with regards to Copyright, Copyleft, Patent and Royalty, Linking and OSD Compliance:
    - **Low** - number of libraries licensed under Low ranking licenses
    - **Medium** - number of libraries licensed under Medium ranking licenses
    - **High** - number of libraries licensed under High ranking licenses
    - **Unknown** - number of libraries licensed under Unknown ranking licenses
- **Occurrences** - number of libraries with the given license

Outdated Libraries

A list of outdated libraries with recommendations regarding newer versions available.

The Outdated Libraries list includes the following information:

- **Library** - artifact id of the library, the library display name in parenthesis. For example "Struts 2 Core" is the official display name of the library and "struts2-core" is the artifact id.
- **Match Type** - Libraries that were not found using the SHA-1 Hash, will be matched by the provided filename.

  Possible values are:

  - **Filename Match** - with confidence level 70%
  - **Exact Match** - with confidence level 100%

- **Versions** - details regarding the version being used and the latest stable version available with release dates and the number of stable versions released in between both versions.
- **Recommendations** - recommended steps that may contain links to the library's homepage with possible links and information regarding newer stable release versions.

High-Medium Risk Licenses

A list of libraries with high or medium risk licenses, ordered by license risk score.

High-Medium Risk Licenses(11)

Library Name	License	Copyleft	Copyright	Pattent	Linking	Royaltyfree
html5shiv-3.7.0.js	GPL 2.0	Full	78	60	Viral	No
j2h-1.3.1.jar	GPL 2.0	Full	78	60	Viral	No
WebGoat6-v6.0.1	GPL 2.0	Full	78	60	Viral	No
main-webgoat-5.1@270	GPL 2.0	Full	78	60	Viral	No
mail-1.4.2.jar	GPL 2.0 Classpath	Full	78	60	Non_Viral	No
mailapi-1.4.2.jar	CDDL 1.0	Partial	65	60	Non_Viral	Conditional
jstl-1.2.jar	CDDL 1.0	Partial	65	60	Non_Viral	Conditional
mail-1.4.2.jar	CDDL 1.0	Partial	65	60	Non_Viral	Conditional
jquery.form-3.51.js	LGPL 3.0	Partial	65	20	Dynamic	Yes
jtds-1.2.2.jar	LGPL 3.0	Partial	65	20	Dynamic	Yes
jackson-databind-2.0.4.jar	LGPL 2.1	Partial	65	20	Dynamic	Conditional

The High- Medium Risk Licenses list includes the following information:

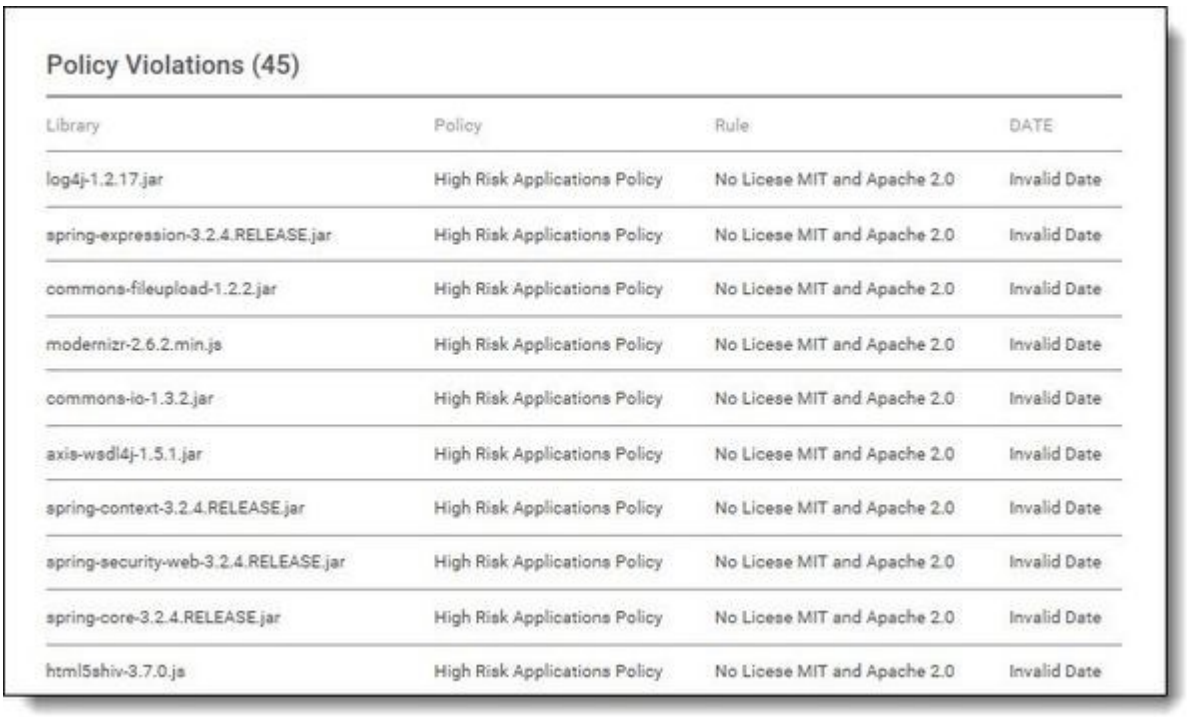
- **Library Name**- name of the file
- **License**- name of the high risk scored license
- **Copyleft**- Full (CopyLeft on modifications as well as own code that uses the OSS), Partial (CopyLeft applies only to modifications) or No (not a CopyLeft license)
- **Copyright**- score range according to color code and score level (0 - 100)
    - Licensee may use code without restriction
    - Anyone who distributes the code must retain any attributions included in original distribution

- Anyone who distributes the code must provide certain notices, attributions and/or licensing terms in documentation with the software
- Anyone who distributes a modification of the code may be required to make the source code for the modification publicly available at no charge
- Anyone who distributes a modification of the code or a product that is based on or contains part of the code may be required to make publicly available the source code for the product or modification, subject to an exception for software that dynamically links to the original code (e.g. LGPL)
- Anyone who distributes a modification of the code or a product that is based on or contains part of the code may be required to make publicly available the source code for the product or modification (e.g. GPL)
- Anyone who develops a product that is based on or contains part of the code, or who modifies the code, may be required to make publicly available the source code for that product or modification if s/he (a) distributes the software or (b) enables others to use the software via hosted or web services (e.g. Affero)

- **Patent**- score range according to color code  and score level (0 - 100)
  - Royalty free and no identified patent risks
  - Royalty free unless litigated
  - No patents granted
  - Specific identified patent risks
- **Linking**- Viral (will substantially infect the code linked to this OSS), Non Viral (will not affect the licensing of the linking code) or Dynamic (Dynamic linking will not infect)
- **Royalty Free** - Yes, No or Conditional.

Policy Violations

A list of policy violated libraries with policy violation, the rule that triggered the policy violation and the policy violation date.



Policy Violations (45)

Library	Policy	Rule	DATE
log4j-1.2.17.jar	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
spring-expression-3.2.4.RELEASE.jar	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
commons-fileupload-1.2.2.jar	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
modernizr-2.6.2.min.js	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
commons-io-1.3.2.jar	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
axis-wsdl4j-1.5.1.jar	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
spring-context-3.2.4.RELEASE.jar	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
spring-security-web-3.2.4.RELEASE.jar	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
spring-core-3.2.4.RELEASE.jar	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date
html5shiv-3.7.0.js	High Risk Applications Policy	No Licese MIT and Apache 2.0	Invalid Date

The Policy Violations list includes the following information:

- **Library Name** - name of the library file
- **Policy** - name of the policy that the library violated
- **Rule** - name of the rule that triggered the policy violation
- **Date** – date that the policy violation was triggered

Inventory Libraries

A list of the libraries names and their licenses.

Inventory Libraries (93)

Library Name	License	Match Type
spring-core-3.2.4.RELEASE.jar	Apache 2.0	Exact Match
commons-beanutils-1.6.jar	Apache 2.0	Exact Match
commons-lang3-3.3.2.jar	Apache 2.0	Exact Match
theme-tomorrow_night_eighties-1.1.3.js	BSD	Exact Match
axis-saaj-1.2.jar	Apache 2.0	Exact Match
modernizr-2.6.2.min.js	MIT	Exact Match
theme-clouds-1.1.2.js	BSD	Exact Match
angular-animate-1.2.16.min.js	MIT	Exact Match
mailapi-1.4.2.jar	CDDL 1.0, CDDL or GPLv2 with exceptions	Exact Match
theme-idle_fingers-1.1.3.js	BSD	Exact Match
commons-fileupload-1.2.2.jar	Apache 2.0	Exact Match

The Inventory list includes the following information:

- **Library** - name of the library file
- **License** - name of the license
- **Match Type** - Libraries that were not found using the SHA-1 Hash, will be matched by the provided filename.

  Possible values are:

  - Filename Match - with confidence level 70%
  - Exact Match - with confidence level 100%

- If an inventory is marked as "Requires Review", it simply means that the automatic analysis process wasn't able to assign a license to the library. The main reasons for this could be:
  - The file extension is not supported
  - The original open source file was modified and the SHA-1 was changed
  - The file is in-house
  - The file is not in the database and needs to be added
  - The file is not in the database and is not open source (commercial).

Best practice, in this case, is to perform a manual review (please contact Checkmarx support)

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.

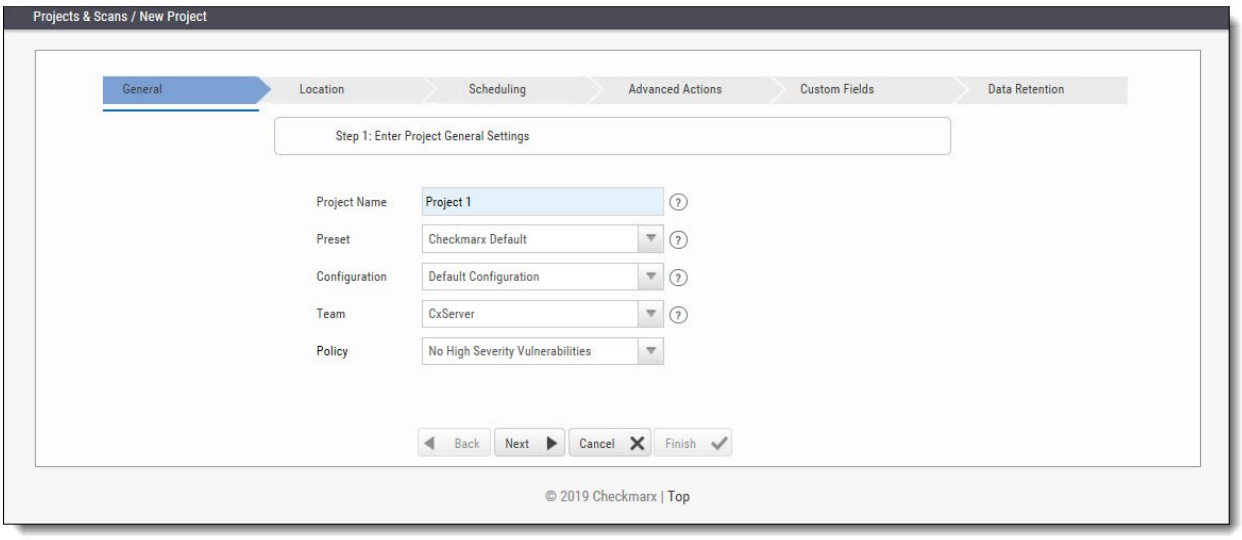
> ■ For Continuous Integration development methodology, if a new branch is created for each iteration, update the code location within the existing project (rather than creating a new project) so that all the results will reside within a single project. Scanning of projects that include multiple code 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.**

Creating and Configuring a CxSAST Project

To create a CxSAST project:

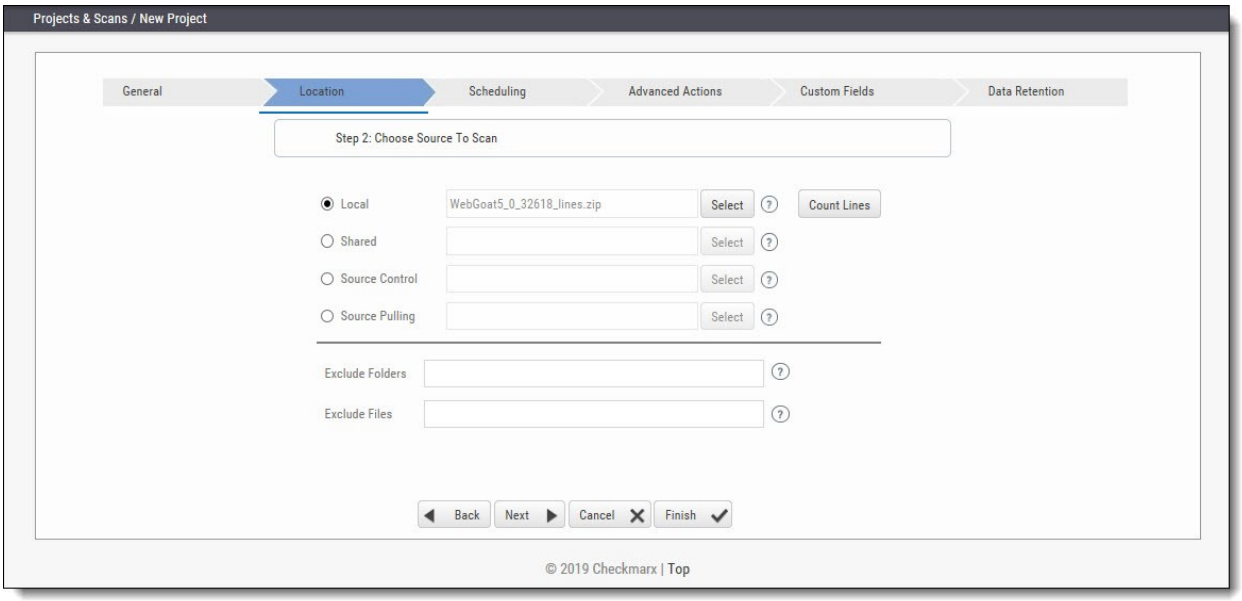
Select **Project & Scans > Create New Project**.



Configure the following **General** project properties:

- **Project Name -** should indicate the source code to be scanned and tracked.
- **Preset -** 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.
- **Configuration -** Apart from the default configuration setting, additional configuration selection traditionally for advanced users, can be used for scanning double-byte encoded source code. There is also the possibility to select a multi-language configuration. This means that all files will be scanned, regardless of language type. If there is a need, a threshold parameter can be adjusted in the database.
    - **Default configuration** will scan the primary language (e.g., java, C#, python, etc.) with the most files and all secondary languages (e.g., JavaScript, PL-SQL, vb-script, etc.). For example, a project with 100 java files, 50 python files, and 60 JavaScript files, will have only the java and JavaScript scanned with the Default configuration.
    - The **Multi-language configuration** will scan all languages including multiple primary languages. If the same project with 100 java files, 50 python files, and 60 JavaScript files is scanned, all languages – java, python, and JavaScript will be scanned.
- **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.
- **Policy** - select a predefined violation policy from the Policy drop-down. Refer to Policy Management for more information about defining violation policies and rules.

Click **Next**.



Configure the following source code **Location** properties:

- **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*).

  ■ CxSAST does not scan two files with the same name or files with special characters that are not supported in Windows.

  ■ 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 *CxSAST Utilities Guide*).

  Zip files generated in a Linux environment may not function properly.

  ■ 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.

  ■ If the zip file contains another zip file inside, the internal zip file will not be sent for scanning. Unzip the contents to the main zip file before scanning.

- **Shared -** project code that is maintained on a network server accessible from the CxSAST Server. Click **Select,** provide your Windows domain credentials in order for CxSAST to access the network (username format: domain_name\user name), and select one or more network folders containing the project code.

  ■ Zipped source code is not supported for shared location scans. Unzip the contents of the zip file before scanning.

  ■ CxSAST does not scan two files with the same name or files with special characters that are not supported in Windows.

- **Source Control -** project code that is maintained in either TFS , SVN , GIT or PerForce source control systems. Click **Select.** See *Configuring the Connection to a Source Control System (v8.6.0 and up)* in the *CxSAST Configuration Guide.*

  ■ Files inside a zip file that are located inside a repository will not be sent for scanning. Unzip the contents of the zip file to the repository before scanning.

> CxSAST does not scan two files with the same name or files with special characters that are not supported in Windows.

- **Source Pulling -** an extension to "Shared" option above, "Source Pulling" activates a configurable script to pull source code from a source control system into the Shared location specified. Note: this script must be set previously configured in the CxSAST Windows client application. For any issues, please review:
  Network and Shared dialogs may not work on "Localhost.
- Optionally, you can **Exclude Folders** and/or **Exclude Files** from being scanned.

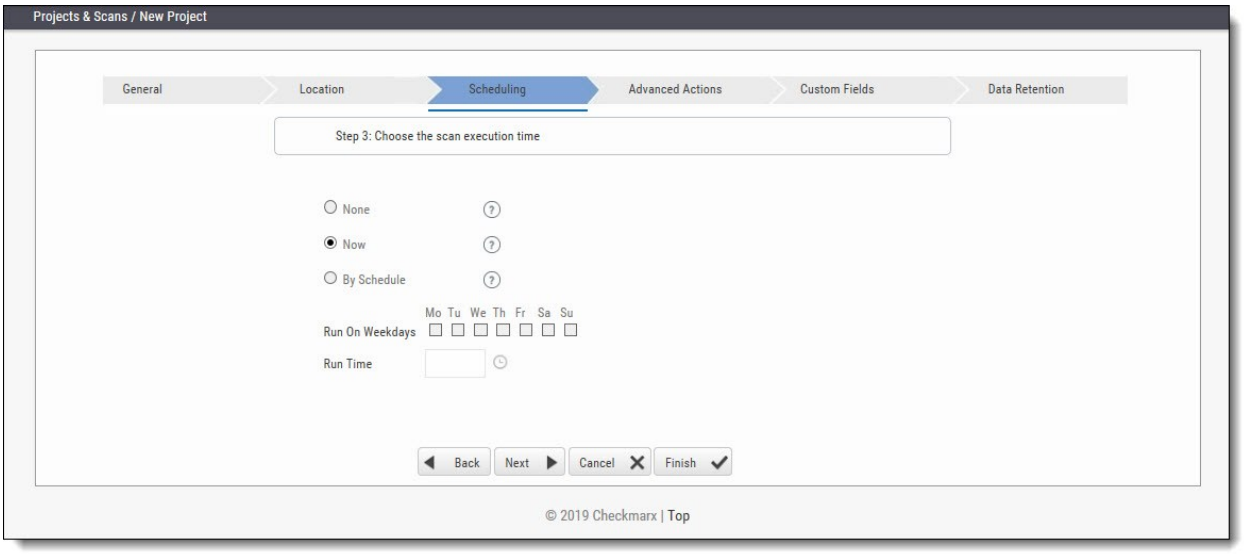
> Type a comma-separated list of folders or files, including wildcards to exclude. For example, consider the following archive, any file/folder name typed into the Exclude File/Folder fields will exclude the file or folder in the project with that name. Also, typing {file name}, for example, 'readme.txt', 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
> ```

> CxSAST does not scan two files with the same name or files with special characters that are not supported in Windows.

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 larger than the result that will be shown from the **Count Lines** option or the Cx CMD Line Counter.

Click **Next**. The following steps of the wizard are optional. You can click **Finish** to skip them.



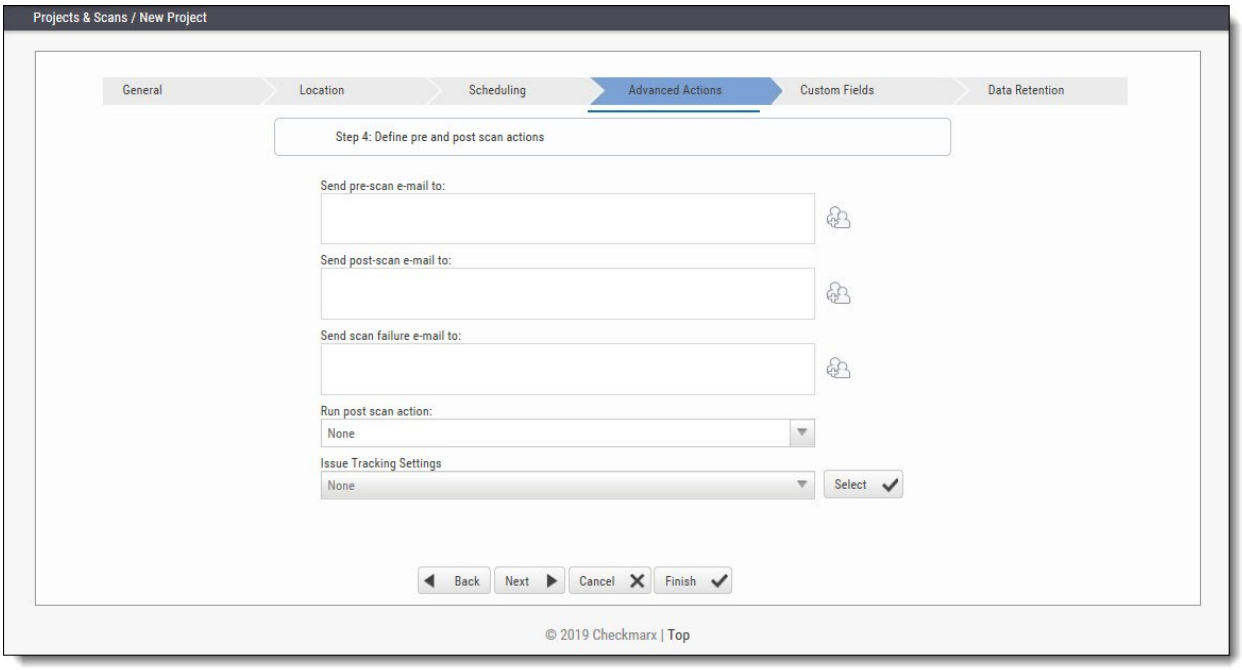
> Scheduling is not applicable to a **Local** source code location, since the CxSAST Server cannot automatically access the local source. You will need to periodically manually upload a new zip file.

Configure the following scan execution **Scheduling** properties:

- **None** - defines no scheduling
- **Now** - defines an immediate scan
- **By Schedule** - define an automatic weekly scan according to the specified time
    - **Run on Weekdays** - define which day to run the periodic scan
    - **Run Time** - define what time to run the periodic scan.

> 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 the CLI in the Build file, but it does not have to be done this way because CxSAST scans source code and does not require building or compiling the source code.

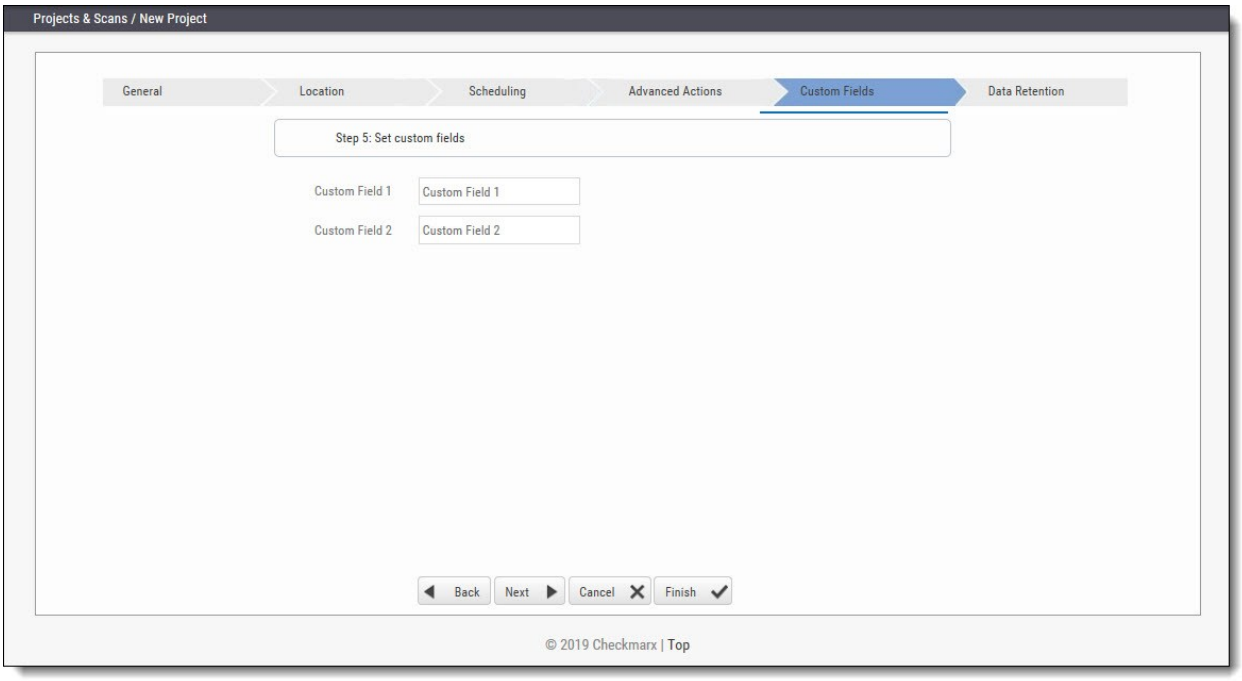
Click **Next**. The following steps of the wizard are optional. You can click **Finish** to skip them.



Configure the following **Advanced Action** properties:

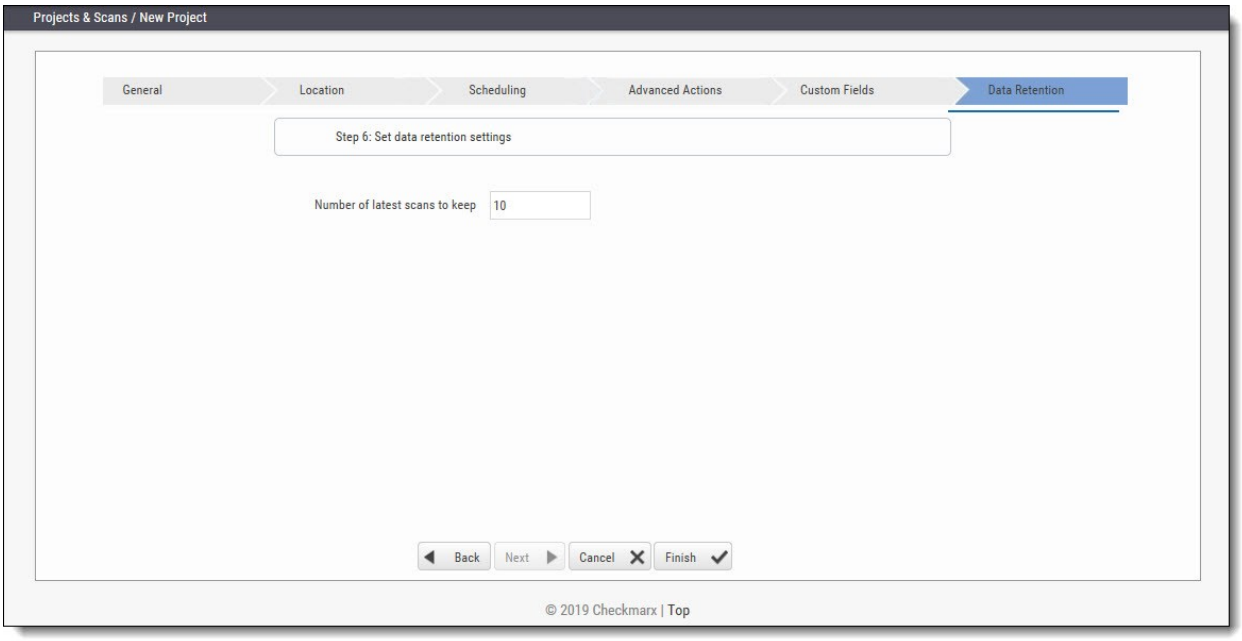
- **Send pre-scan email to** - define to which e-mail to send a pre-scan notification
- **Send post-scan e-mail to** - define to which e-mail to send a post-scan notification
- **Send scan failure e-mail to** - define to which e-mail to send a scan failure notification
- **Run post scan action** - define which post scan action to run (see *Configuring an Executable Action*)
- **Issue Tracking Settings** - define to which issue tracking system to integrate (see *Setting Up JIRA Integration* in the *CxSAST Plugin and Integration Guide*).

Click **Next**. The following steps of the wizard are optional. You can click **Finish** to skip them.



Configure the **Custom Field** properties according to the available custom fields (see *Managing Custom Fields*).

Click **Next**. The following steps of the wizard are optional. You can click **Finish** to skip them.



Configure the **Data Retention** properties:

- **Number of latest scans to keep** - Define the number of latest scans to be kept (see *Data Retention Management*).

Click **Finish** and check the scan status (see *The Queue*).

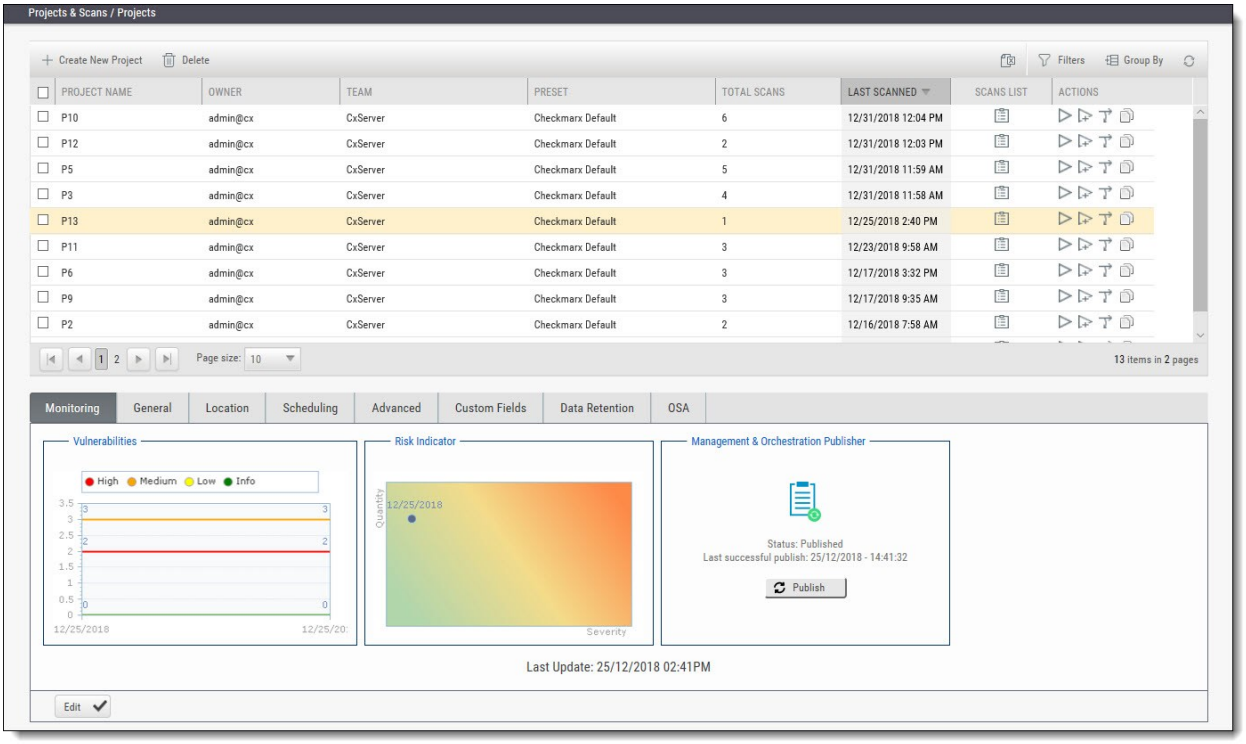
Configuring Open Source Analysis

CxOSA allows you to manage, control and prevent the security risks and legal implications introduced by open source components used as part of the development effort. CxOSA supports all the most common programming languages, enabling you to secure all their open source components in addition to the in-house developed code analysis coverage. For more information about code coverage, refer to Supported Code Languages in the CxOSA Release Notes.

Creating a project is currently dependent on CxSAST and is achieved as part of the CxSAST project creation. You can add CxOSA to any CxSAST project performing a scan. For more information about this subject, refer to Creating and Configuring Projects.

To configure a CxOSA project:

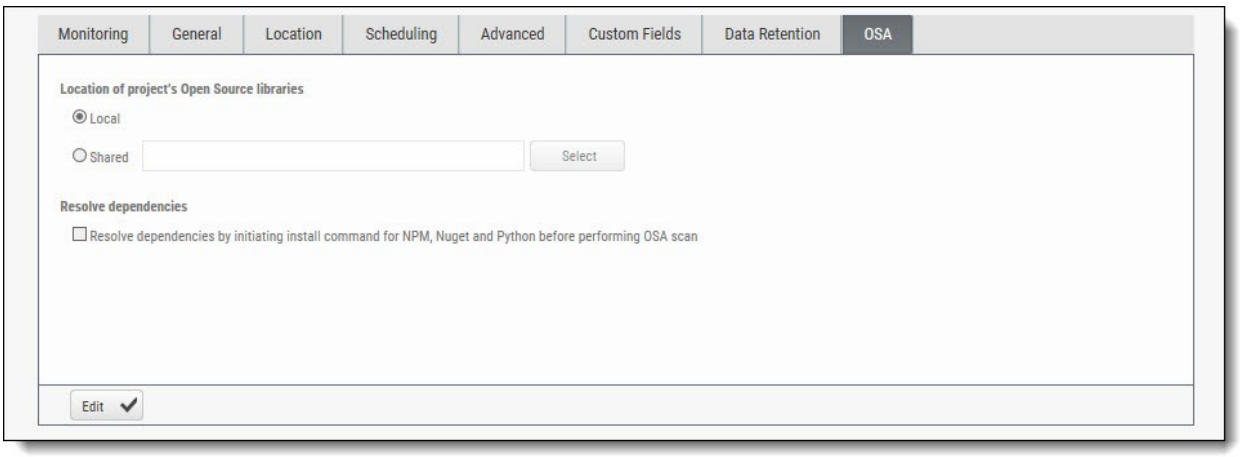
Click Projects & Scans > Projects. The Projects View is displayed.



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

Select an existing project from the Projects list, or click Create New Project and define the new project configuration as you would if you were creating and configuring a project for CxSAST. For more information about this subject, see Creating and Configuring Projects.

Click the OSA tab. The CxOSA properties are displayed.



The OSA tab provides the option to define the location of the open source libraries for scanning as well as resolve dependencies by initiating the install command for NPM and Nuget before performing OSA scan.

In order to use this functionality, you should install the pre-requisite installations specific to the dependencies you would like to resolve. For more information about this subject, refer to Preparing the Environment for CxOSA.

Click **Edit** and configure the following CxOSA properties:

- **Local -** open source code libraries that are maintained locally. Go to *Consolidated Project State (up to v8.7.0)* in order to access the local directory and select a compressed file (.zip) containing the project open source libraries.
- **Shared** - open source code libraries that are maintained on a network server accessible from the CxSAST Server. Click **Select,** provide your Windows domain credentials in order for CxSAST to access the network (username format: domain_name\user name), and select one or more network folders containing the project open source libraries

> Note that there is no limitation to the OSA file size for analysis.

- **Resolve dependencies** - select the checkbox to resolve dependencies by initiating install command for NPM before performing OSA scan

Click **Update**.

Performing scans from the CxServer, and based on your environment and language, additional package managers should also be installed, see Supported Languages and Package Managers for more information.

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.

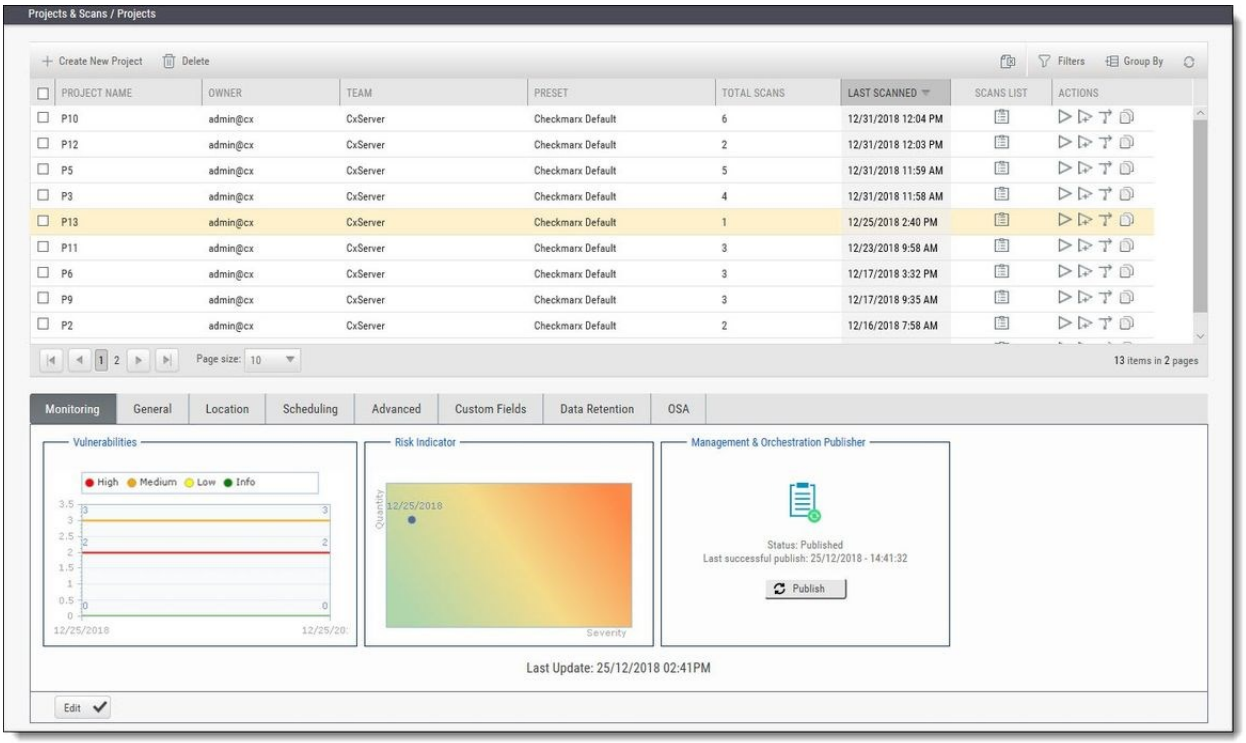
- **Branch Project** - similar to copy project, except it copies the following set of properties: Preset, Team and the Last scan from the source project with all results and remarks.

  Note that when branching a project, the branch should be started from the last successful scan. Successful scan meaning the 'last real scan' that was performed, instead of the attempted scan which changed the date of scan start date, but was actually never performed due to there being no change in the code.

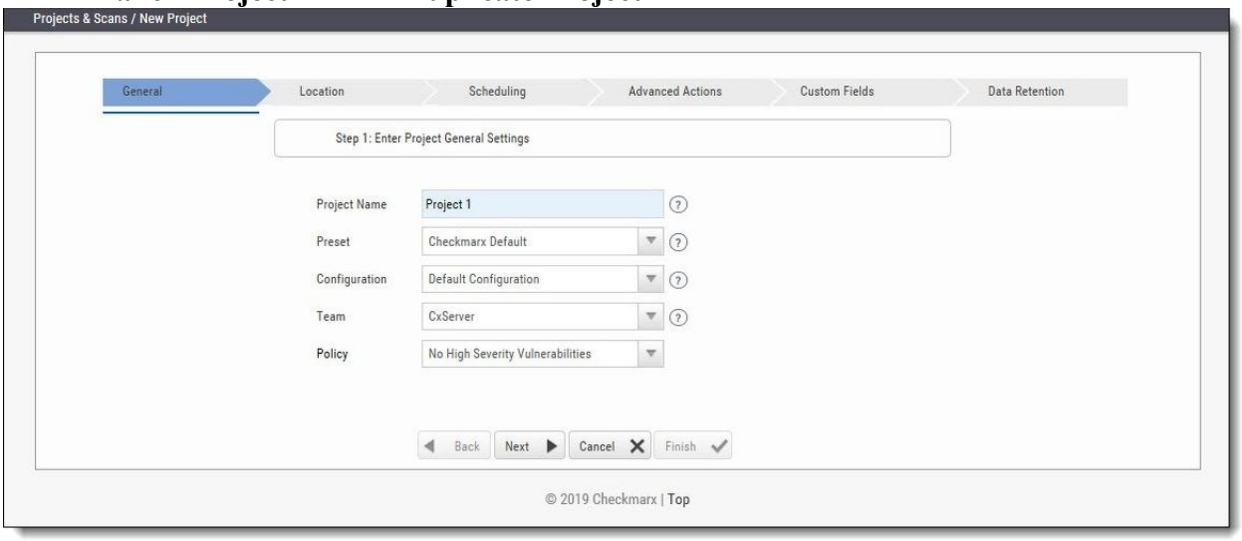
  Duplicate Project - creates a new project based on the settings of the existing one and also copies the following set of properties: Preset, Team, Exclusions, Scheduling, Pre-scan, Post-scan and Scan failure emails.

To branch or duplicate an existing project:

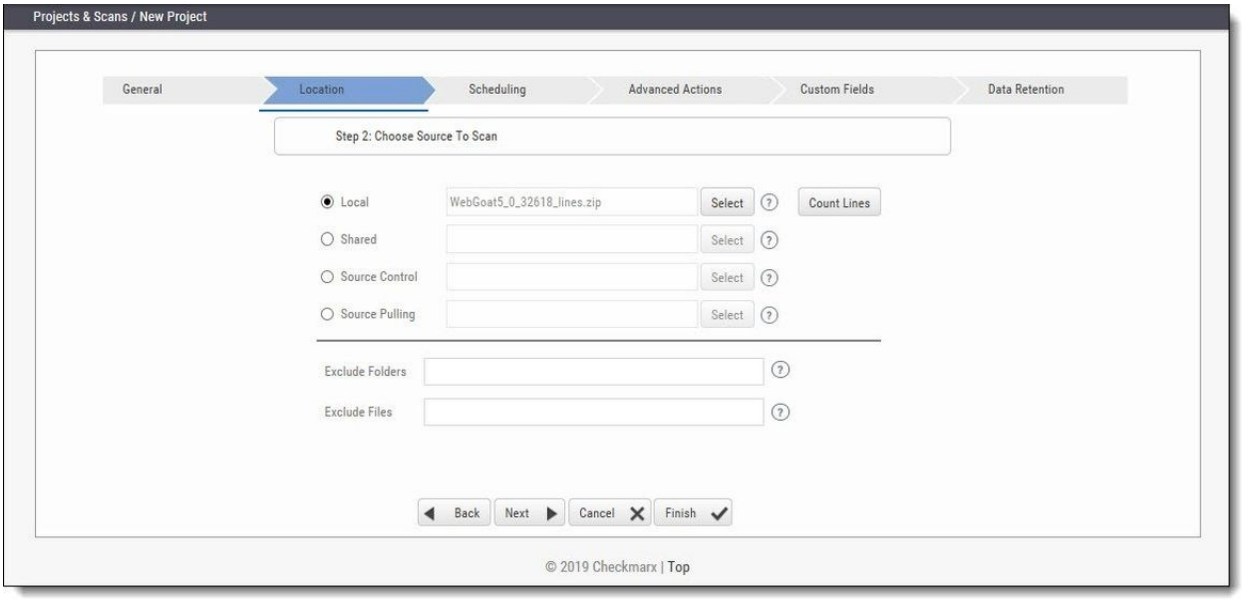
Go to **Projects & Scans and** select **Projects**.



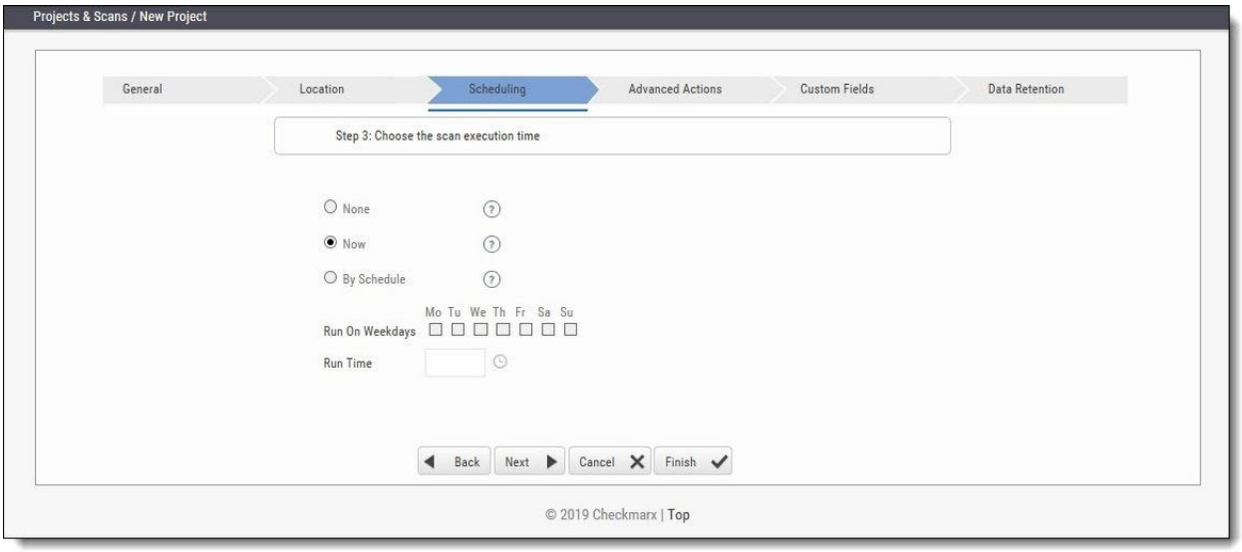
Click **Branch Project**  or **Duplicate Project**  .



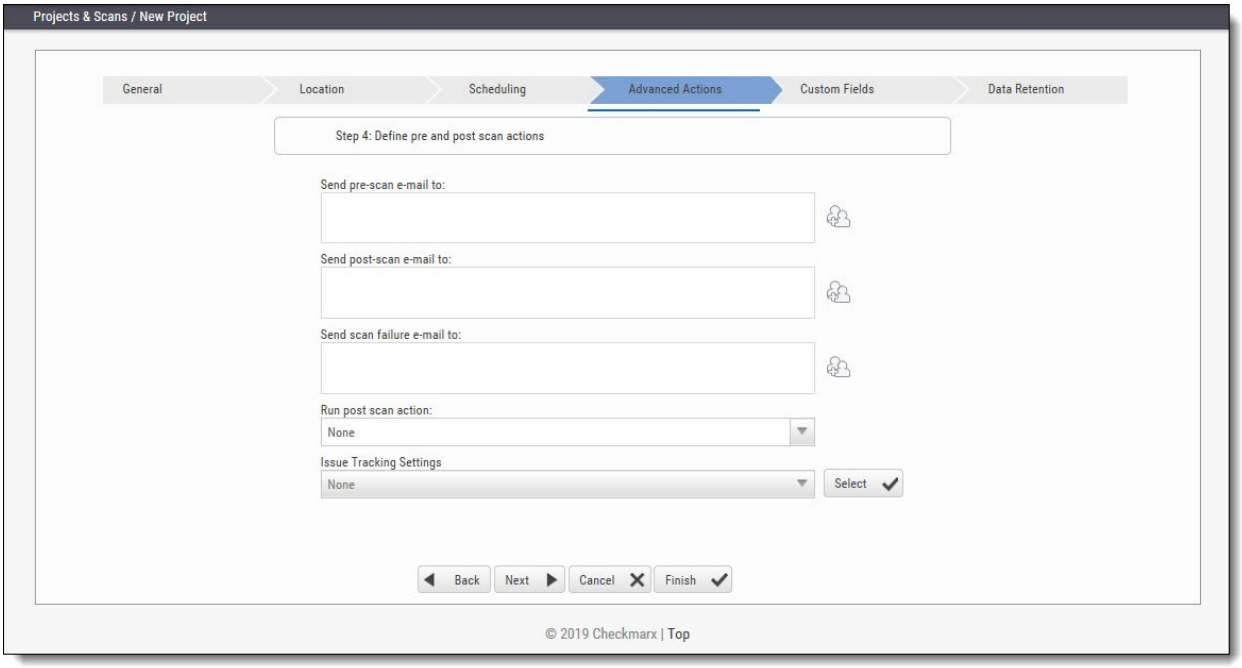
Define **General** settings and click **Next**.



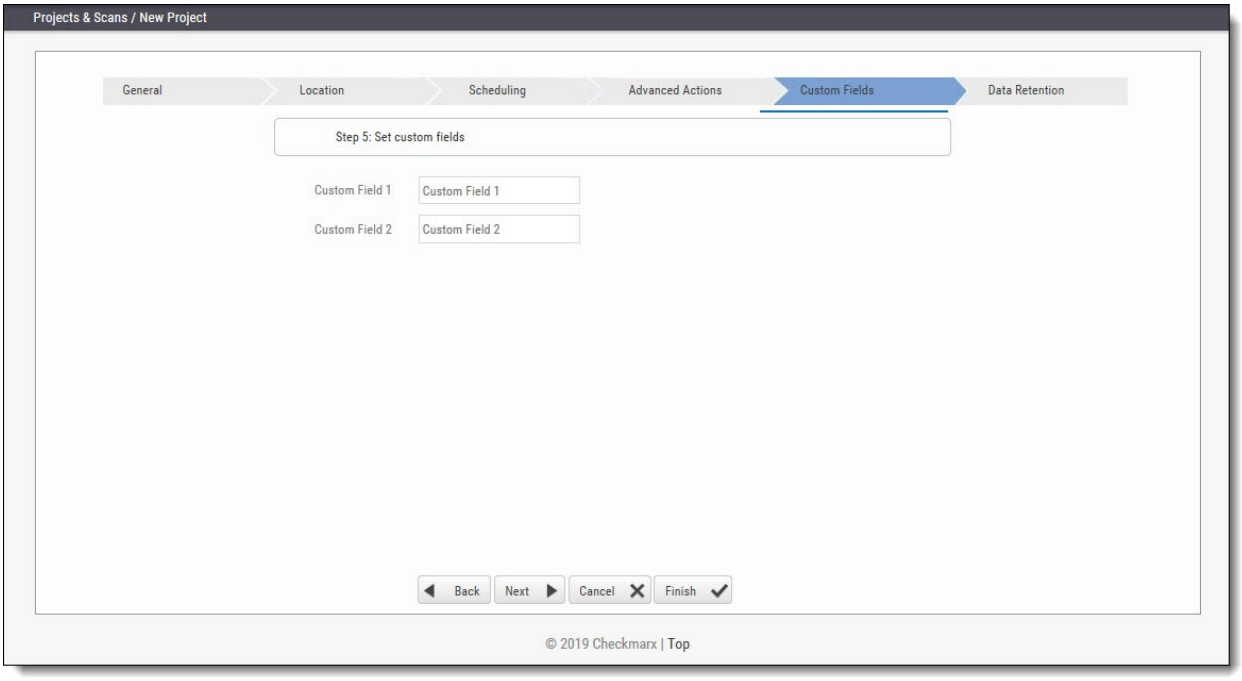
Define the **Location** of the source code and click **Next**.



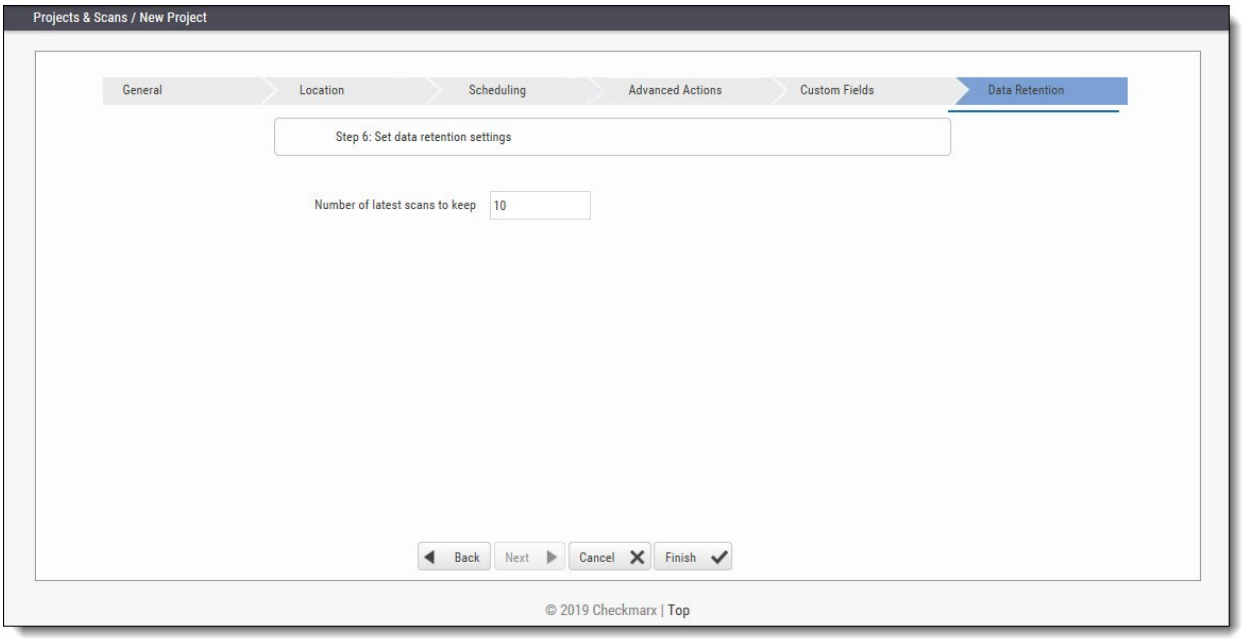
Define scan **Scheduling** options and click **Next**.



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



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



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

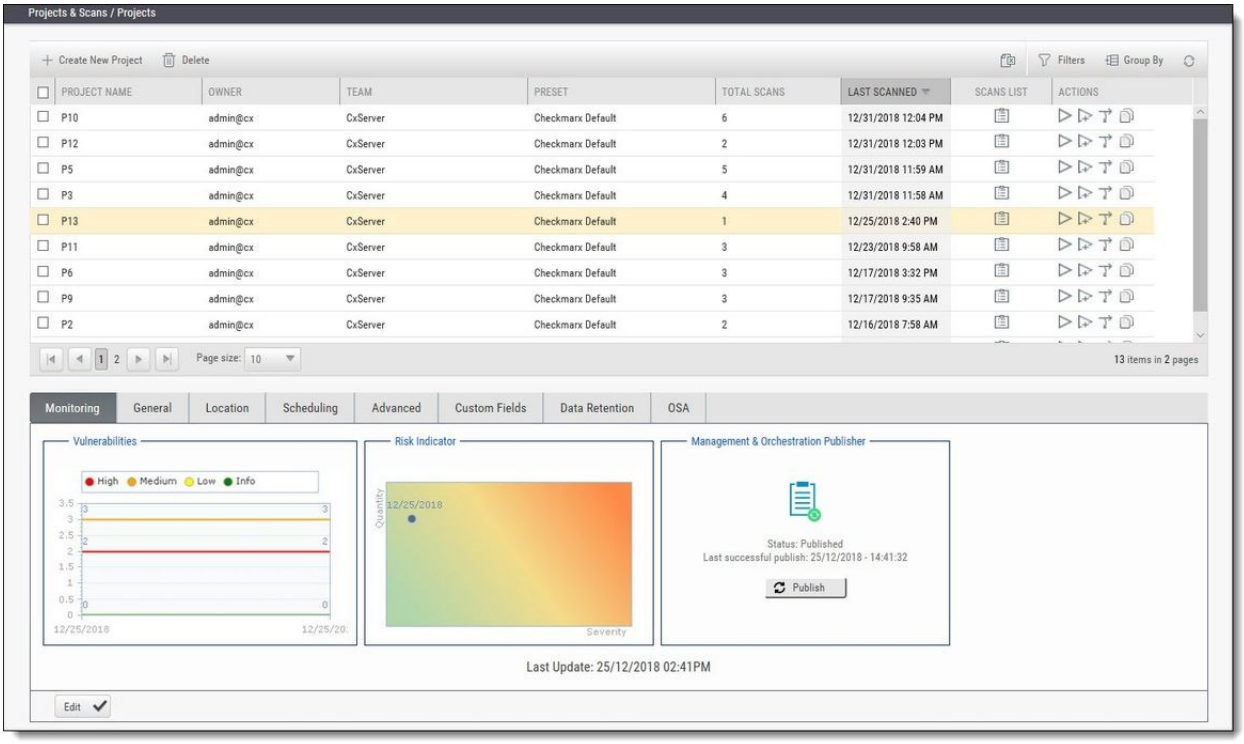
Once complete, click **Save**. The following message is displayed: "Branching may take a few minutes, would you like to proceed?"

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

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

- Branched projects are not counted as additional projects according to the Checkmarx licensing structure. This means that you are not allowed to create new projects once you have reached the maximum project threshold, however, you will be able to open branches of existing projects without forfeiting additional licenses.

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.

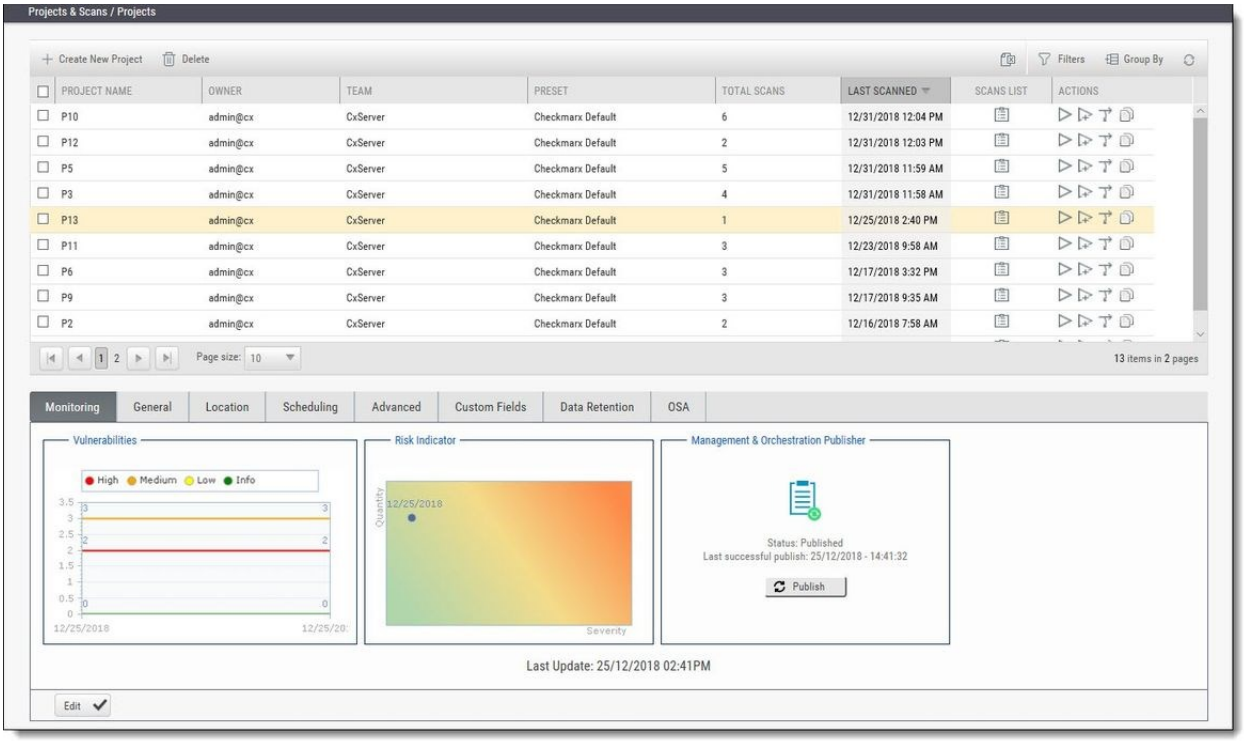
	**Incremental Scan**	Incremental scan is used to increase the scanning speed of the project. It works by scanning only the code that has changed since the last full scan was performed. During the incremental scan, the system takes each file that was sent to be incrementally scanned and creates a hash 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. • The following configuration keys are available: ○ INCREMENTAL_SCAN_THRESHOLD Defines the maximum percentage of files changed to allow the incremental scan. Valid values: 1-19, Default value: 7 ○ INCREMENTAL_SCAN_THRESHOLD_ACTION Defines the action to be taken when the threshold exceed in incremental scan. FAIL – fail the scan, FULL – switch to full scan. Valid values: FAIL or FULL. Default value: FAIL

■ 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.

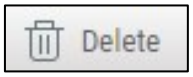
	**Branch Project**	The Branch Project operation is similar to copy project, but it copies a different set of properties: Preset, Team and the Last scan from the source project with all results and remarks.
	**Duplicate Project**	Duplicate Project creates a new project based on the setting of an existing 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:



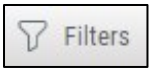
The following actions are available from the table's header bar:

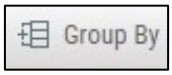
- **Delete** -  Delete rows

> ■ 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.

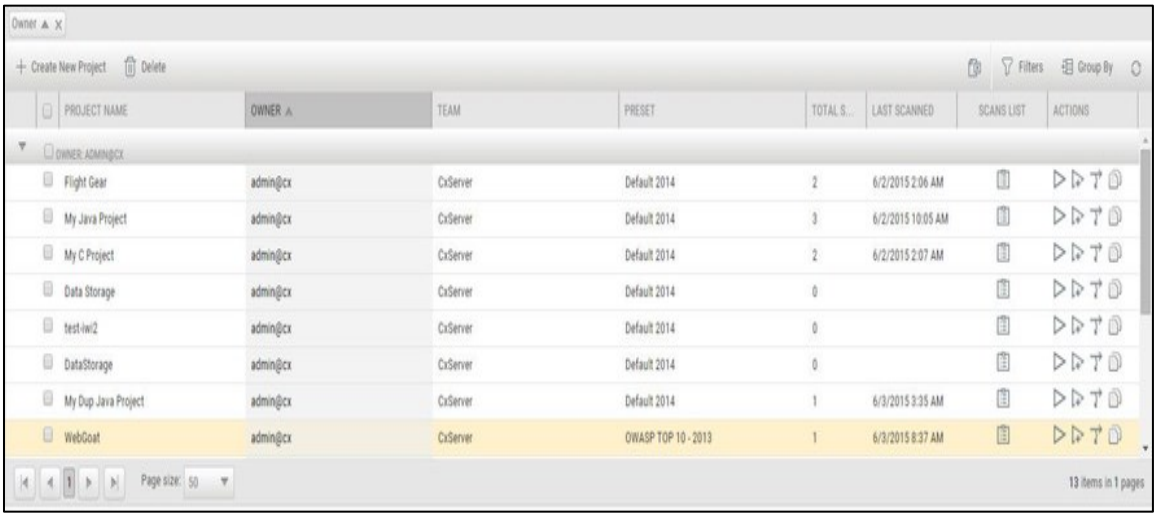
> ■ When the user deletes a project, the project is not deleted from the database. Instead, the project is marked as "deprecated". All scans under the deleted project are also marked as "deprecated". This deprecated data can be ultimately be removed as part of the Data Retention Management process.

- **Export** -  Export to CSV

- **Filters -** 

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

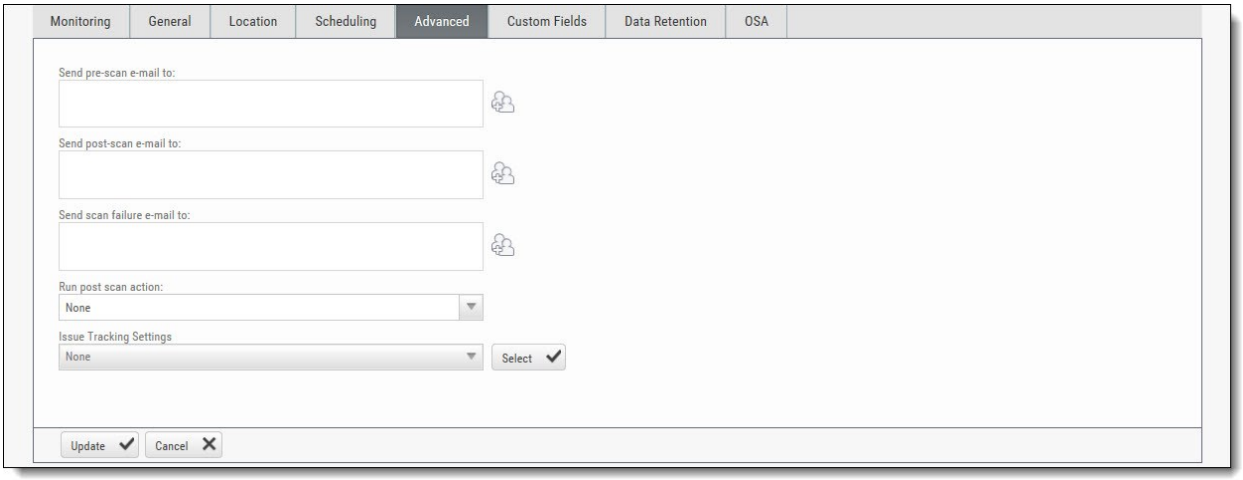
- Send an email message
- Run an executable

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

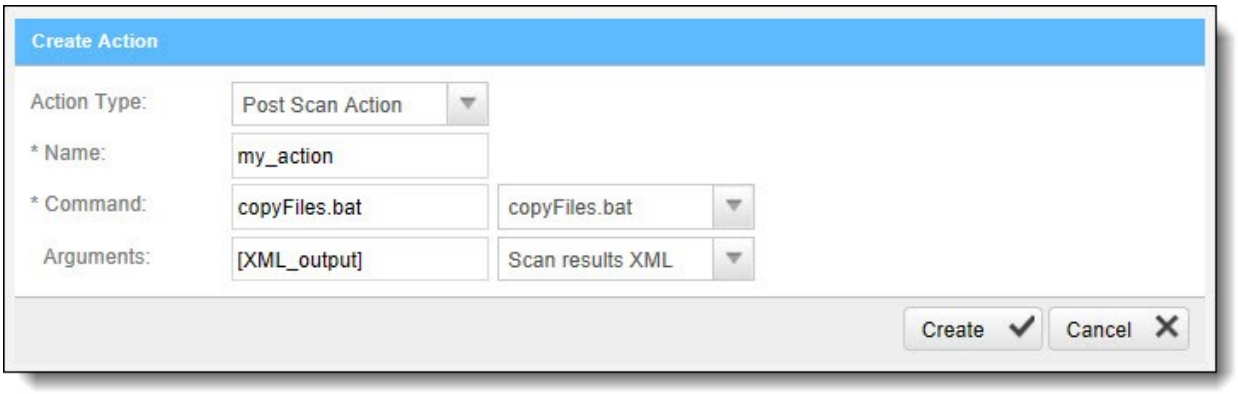
Configuring an Executable Action

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:

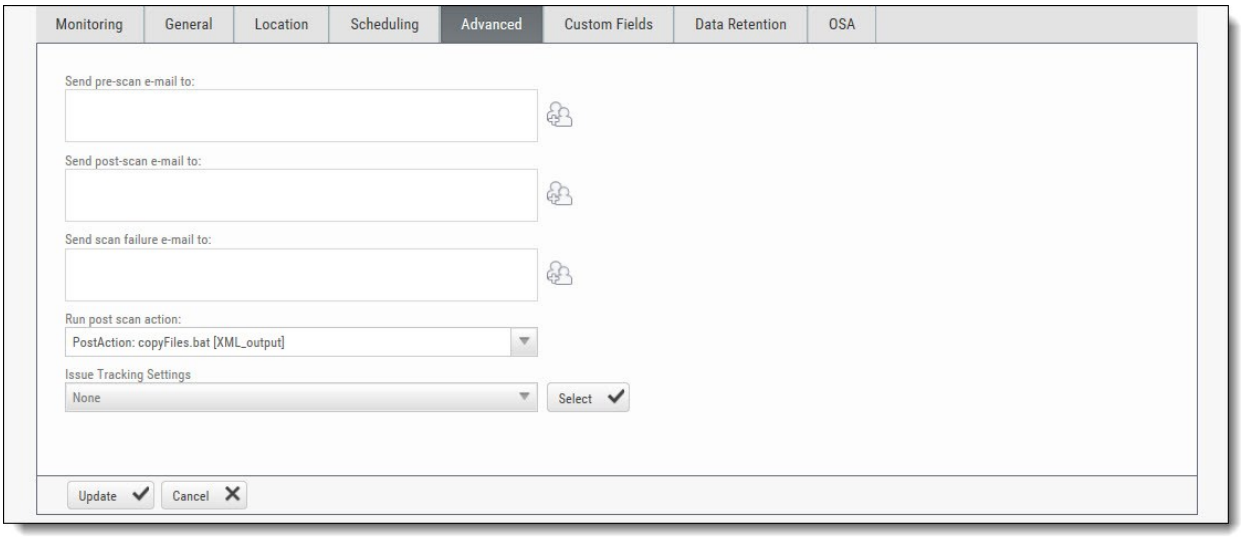


- **Action Type: Pre-scan** or **Post-scan**.
- **Name:** This will appear in a drop-down list when assigning the actions to a project.
- **Command:** Use the syntax as required by the executable or select from the list.

> 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**.

- **Arguments:** Enter arguments required by the command.
- 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:

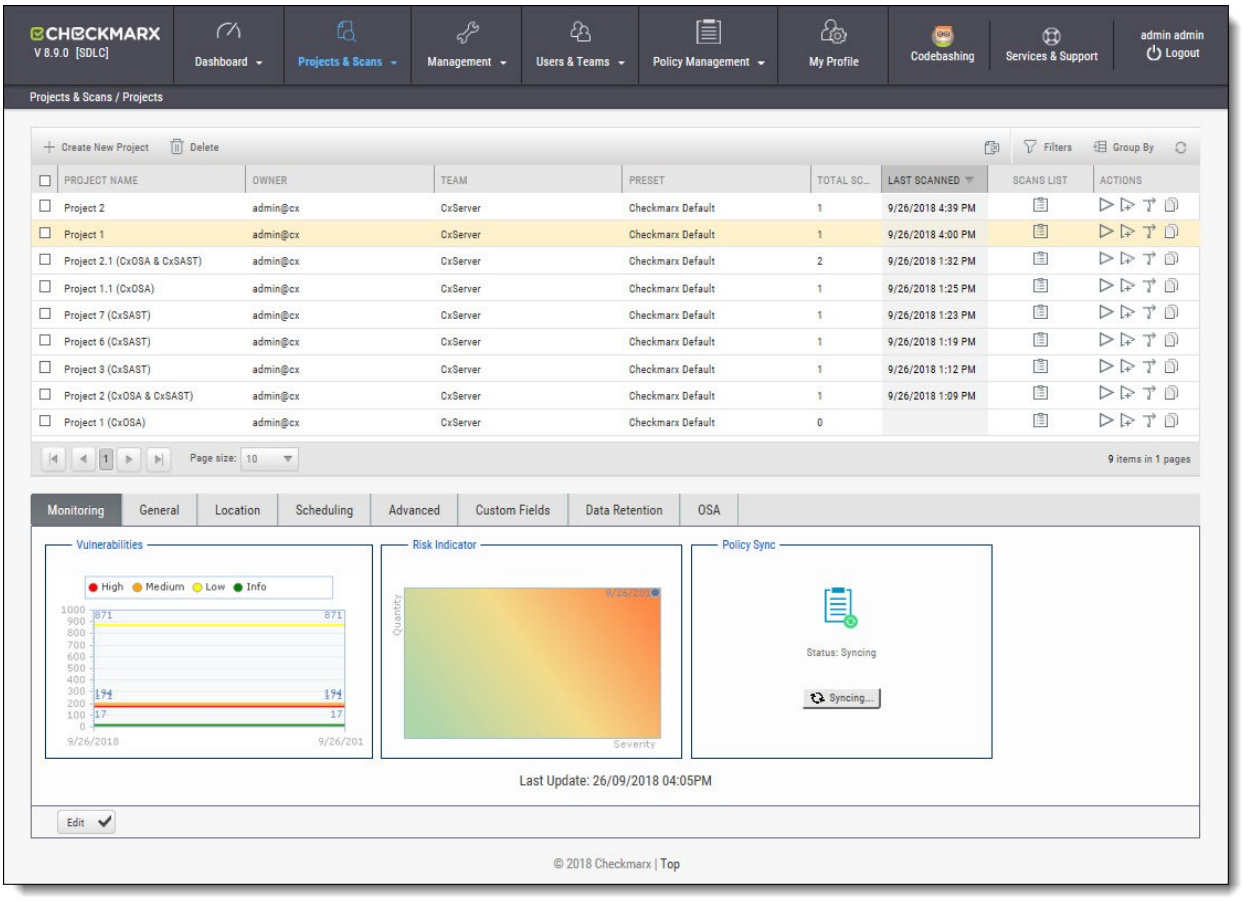


4. Click **Finish**.

Viewing Project Details

You can view detailed information about a particular project from the Projects window.

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

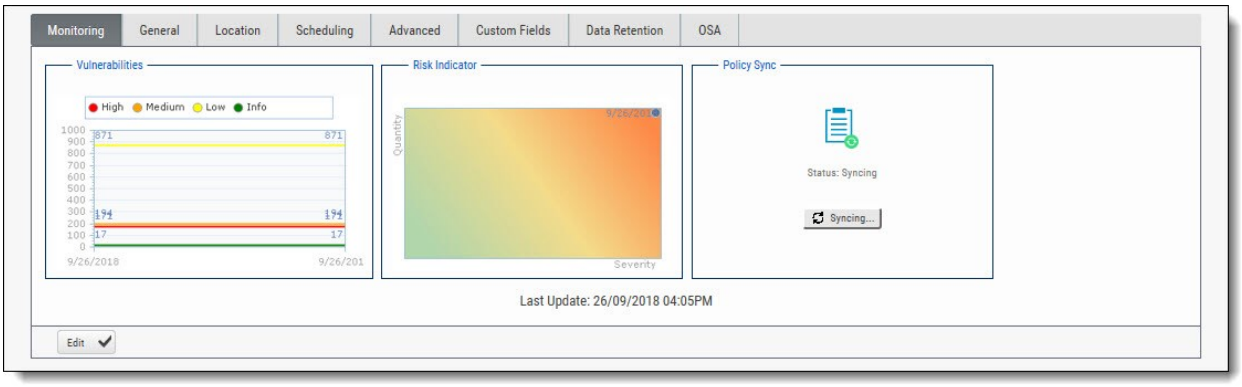


The Projects window lists all the projects that are configured for groups where the logged-on user is a member. You can also manage the table (see *Managing Tables*).

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 (see *Managing Projects and Running Scans*).

Selecting a project displays its details in the tabbed panel below.



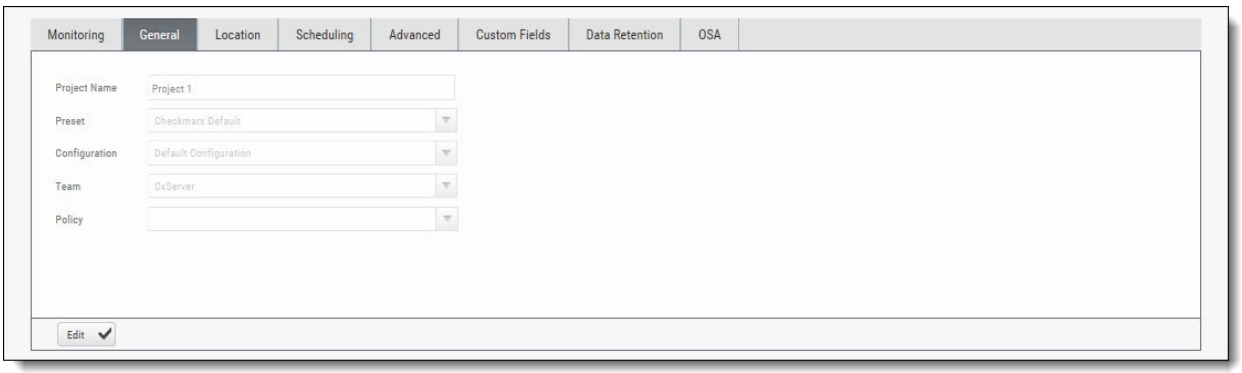
The Monitoring tab represents the evolution of the project last 10 scans focusing on the numbers of found vulnerabilities and overall risk.

- 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).
- The **Risk Indicator** chart represents each scan result combining quantity and severity of found vulnerability instances.
- The **Policy Sync** indicator provides the capability to manually synchronize the latest scan for a specific project to the latest policy definition. This provides you with the most updated policy status for your project. The 'Unsynced' status indicates that synchronization has not yet been processed. 'Syncing' means that its currently in-process. Once synchronization is complete, the status changes to 'Synced' with the last sync date and time displayed.

Click **Edit** to change settings and then click **Update** to save the changes.

General Properties

Click the **General** tab to display its properties.



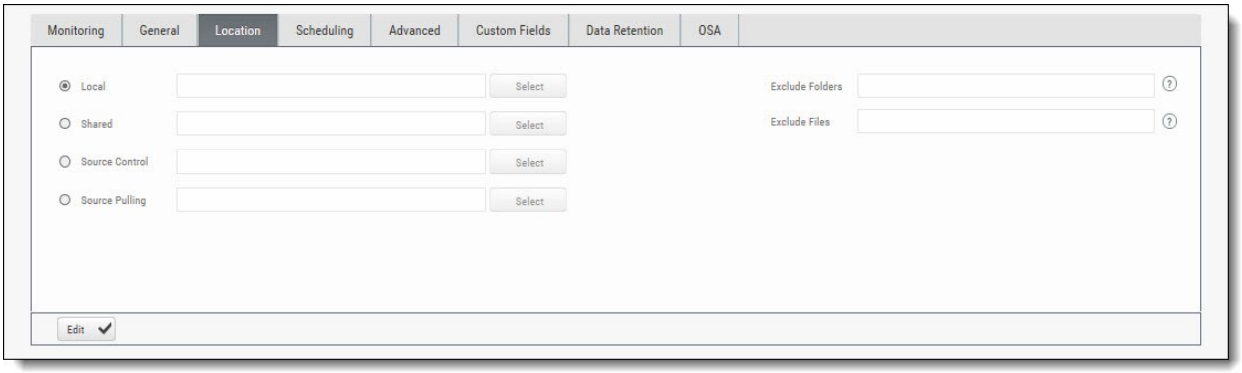
The General tab represents the project name, defined preset, configuration and team associated with the project.

For more information about defining these properties refer to section about General properties in *Creating and Configuring Projects*.

Click **Edit** to change settings and then click **Update** to save the changes.

Location Properties

Click the **Location** tab to display its properties.



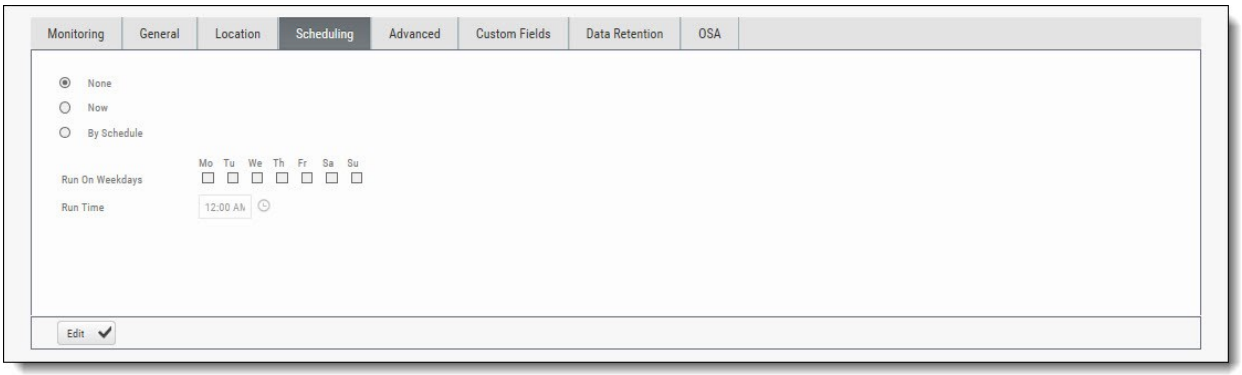
The Location tab represents the various options for locating and pulling the source code for scanning.

For more information about defining these properties refer to section about Location properties in *Creating and Configuring Projects*.

Click **Edit** to change settings and then click **Update** to save the changes.

Scheduling Properties

Click the **Scheduling** tab to display its properties.



The Scheduling tab represents the various options for scheduling the automatic scans.

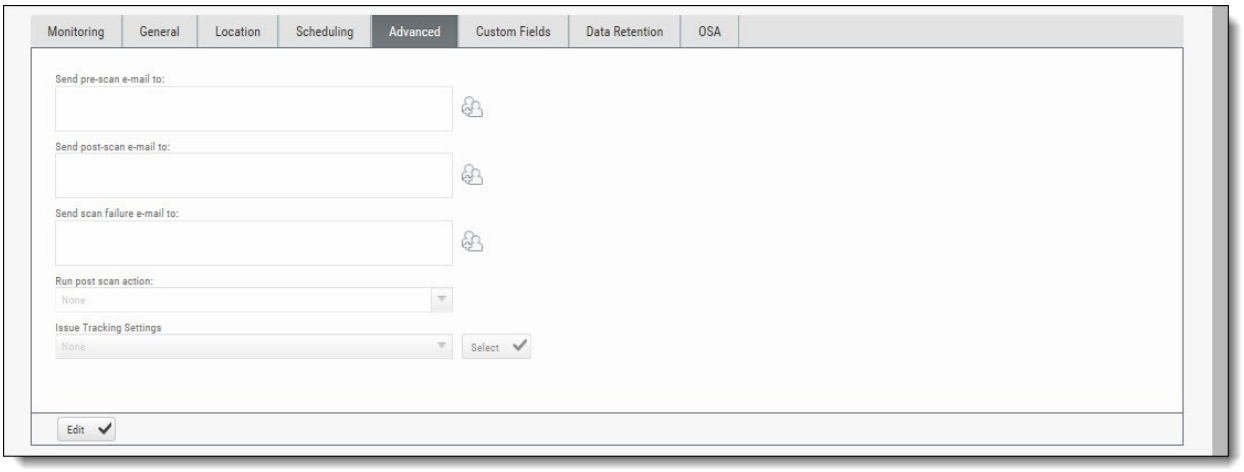
> ■ Scheduling is not available for Local source code location, since the CxSAST Server cannot automatically access the local source. You will need to periodically manually upload a new zip file.

For more information about defining these properties refer to section about Scheduling properties in *Creating and Configuring Projects*.

Click **Edit** to change settings and then click **Update** to save the changes.

Advanced Properties

Click the **Advanced** tab to display its properties.



The Advanced tab represents the various options for pre/post scan actions and issue tracking settings.

For more information about defining these properties refer to section about Advanced properties in *Creating and Configuring Projects*.

Click **Edit** to change settings and then click **Update** to save the changes.

Custom Fields Properties

Click the **Custom Fields** tab to display its properties.

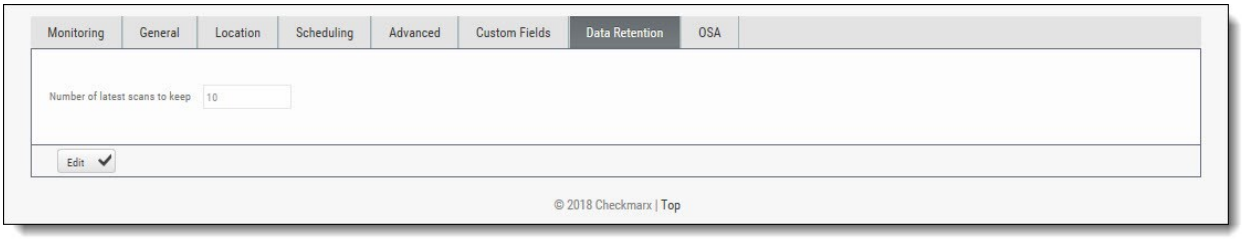
The Custom Fields tab represents the option to define additional project properties using the predefined custom fields.

For more information about defining these properties refer to section about Custom Field properties in *Creating and Configuring Projects*.

Click **Edit** to change settings and then click **Update** to save the changes.

Data Retention Properties

Click the **Data Retention** tab to display its properties.



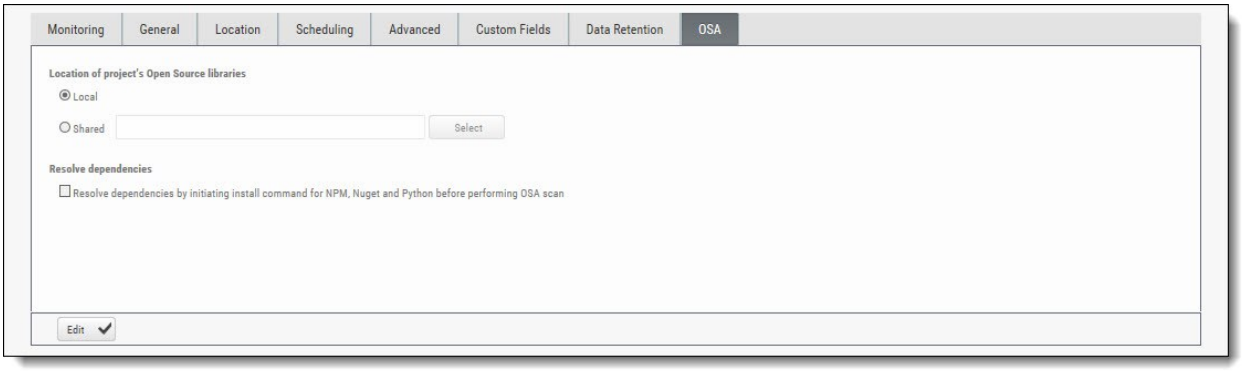
The Data Retention tab represents the option to define the number of last scans to be kept for the project. This helps to manage data storage consumption.

For more information about defining these properties refer to section about Data Retention properties in *Creating and Configuring Projects*.

Click **Edit** to change settings and then click **Update** to save the changes.

CxOSA Properties

Click the **OSA** tab to display its properties.



The OSA tab represents the option to define the location of the open source code libraries for analysis, resolve dependencies as well as select a redefined violation policy for the project. Please refer to CxARM Policy Management for more information about defining violation policies and rules.

For more information about defining these properties refer to section about Open Source Analysis properties in Creating and Configuring Projects.

Click **Edit** to change settings and then click **Update** to save the changes.

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:

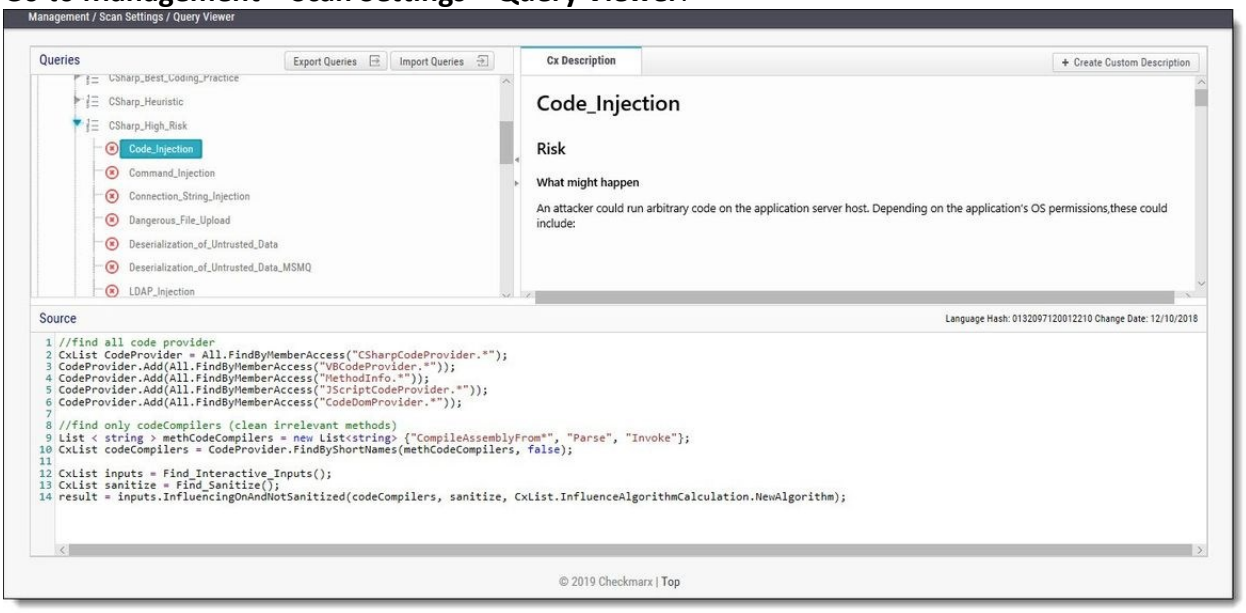
- Viewing, Importing, and Exporting Queries
- Managing Query Presets

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:

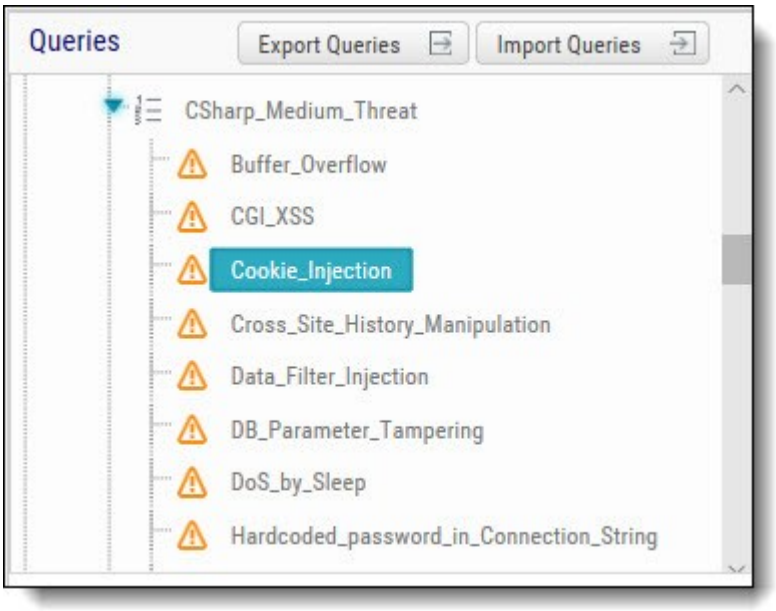
1. Go to **Management** > **Scan Settings** > **Query Viewer**:



   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.

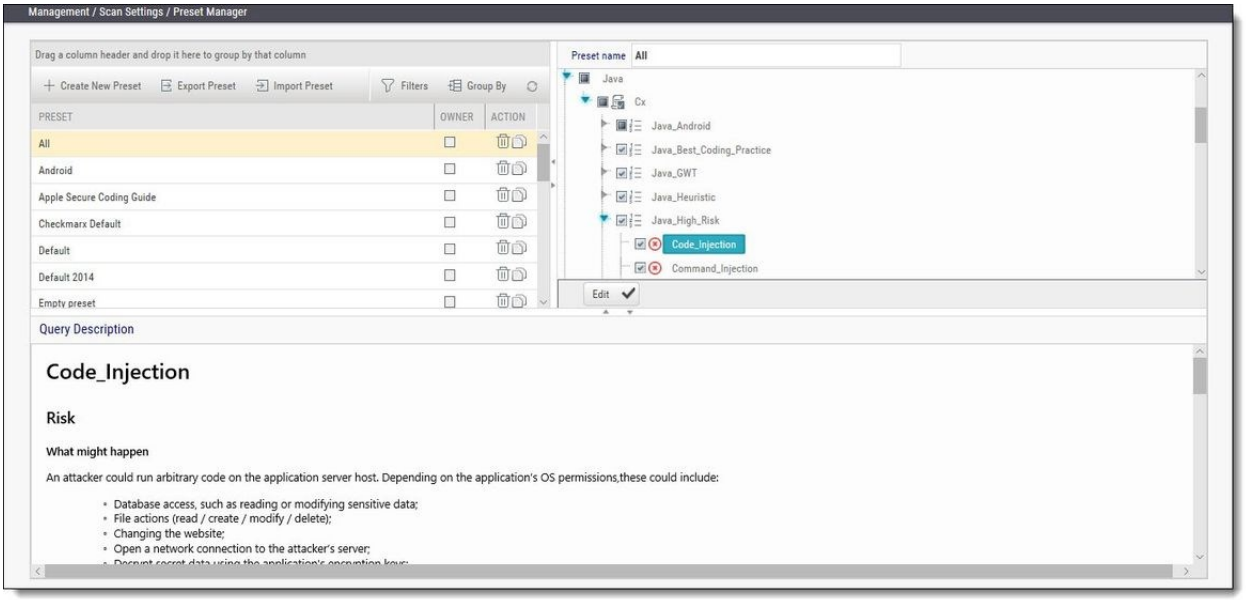
■ If the imported query has the same name as an existing one, the existing query will be overridden.

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.

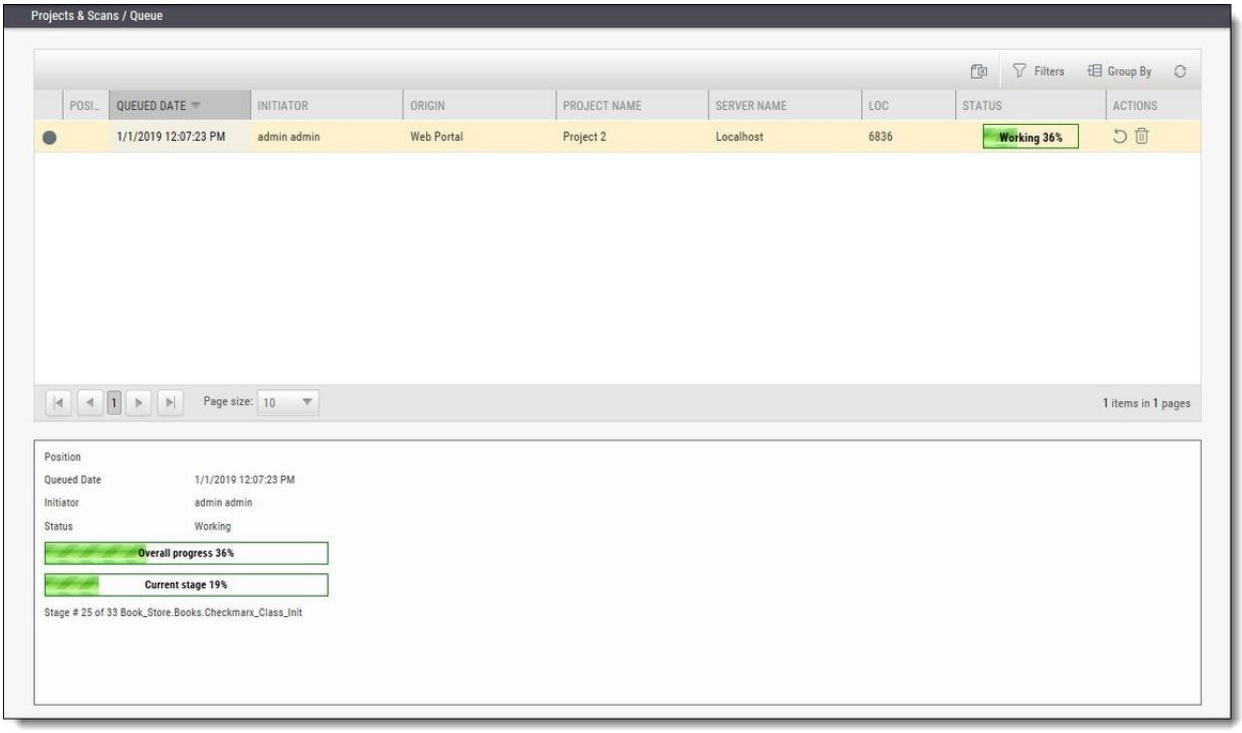
To import a preset:

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.



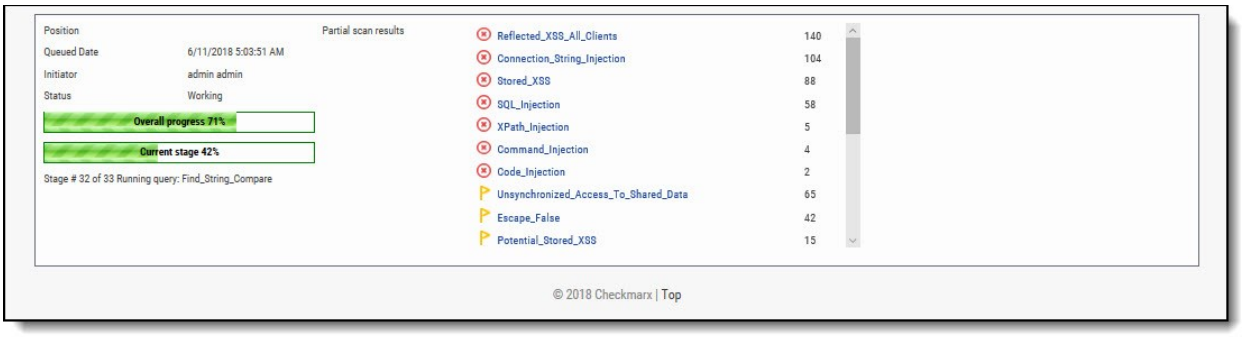
c

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  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  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

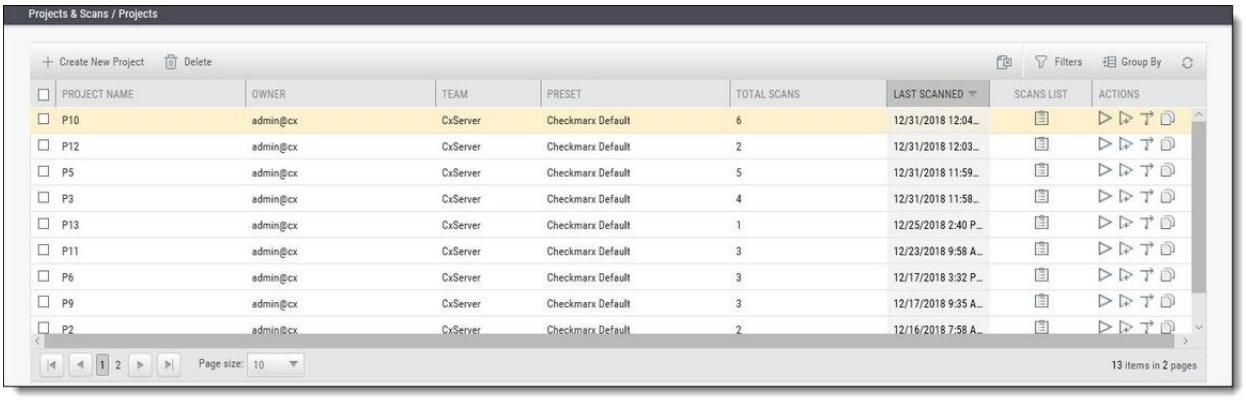
To view scan results, you can view either of the following tables:

- 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 and Actions

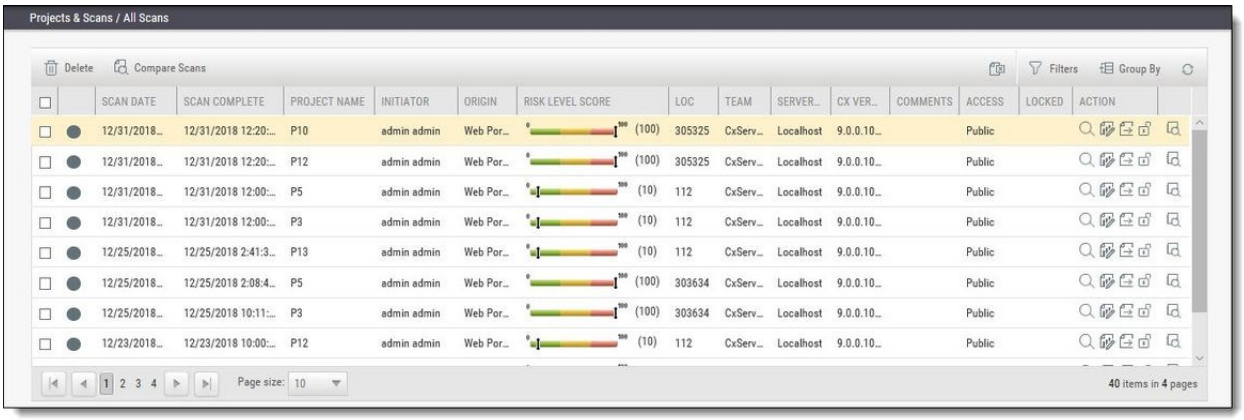
In Projects & Scans > Projects, various scans and action lists are available (see *Creating and Configuring Projects*).



Column	Action	Description
Scan List	 View Project Scans	Displays the project in the individual project path, for example, Projects & Scans/View Project Scans/My Java Projects.
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. **NOTE:** 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 (see *Managing Tables*), including sorting by Scan Date, Scan Complete date, Project Name, or Risk Level Score.



- indicates scan in process
- indicates a full scan
- indicates an incremental scan

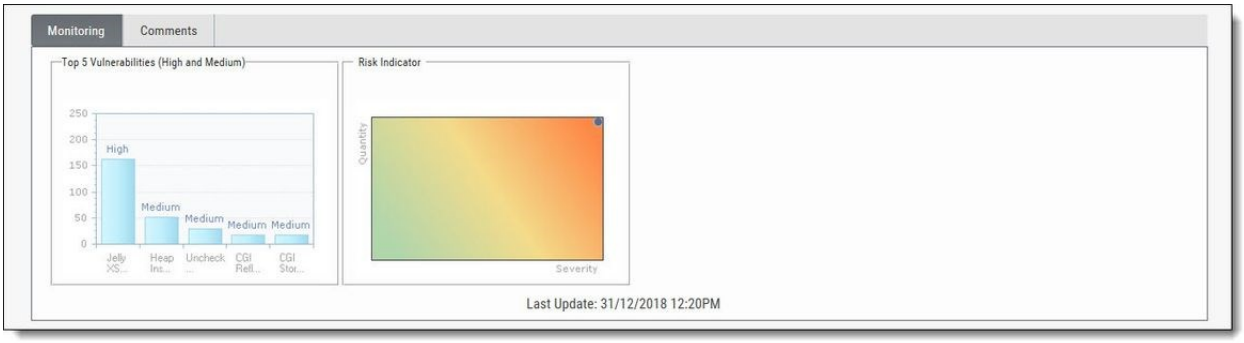
Additionally indicates a partial scan. Information about why only a partial scan was performed is provided in Scan Summary. For more information about partial scans, refer to the FAQ section.

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 See *Scan Result Actions (v8.6.0 and up).*

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:

Select the rows of the requested scans.

Click the Delete button. A prompt appears, requesting you to confirm the deletion operation.

Click **OK**.

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

Clicking the Export as CSV File options downloads the DeleteErrors.csv file, which displays the details of the locked scans.

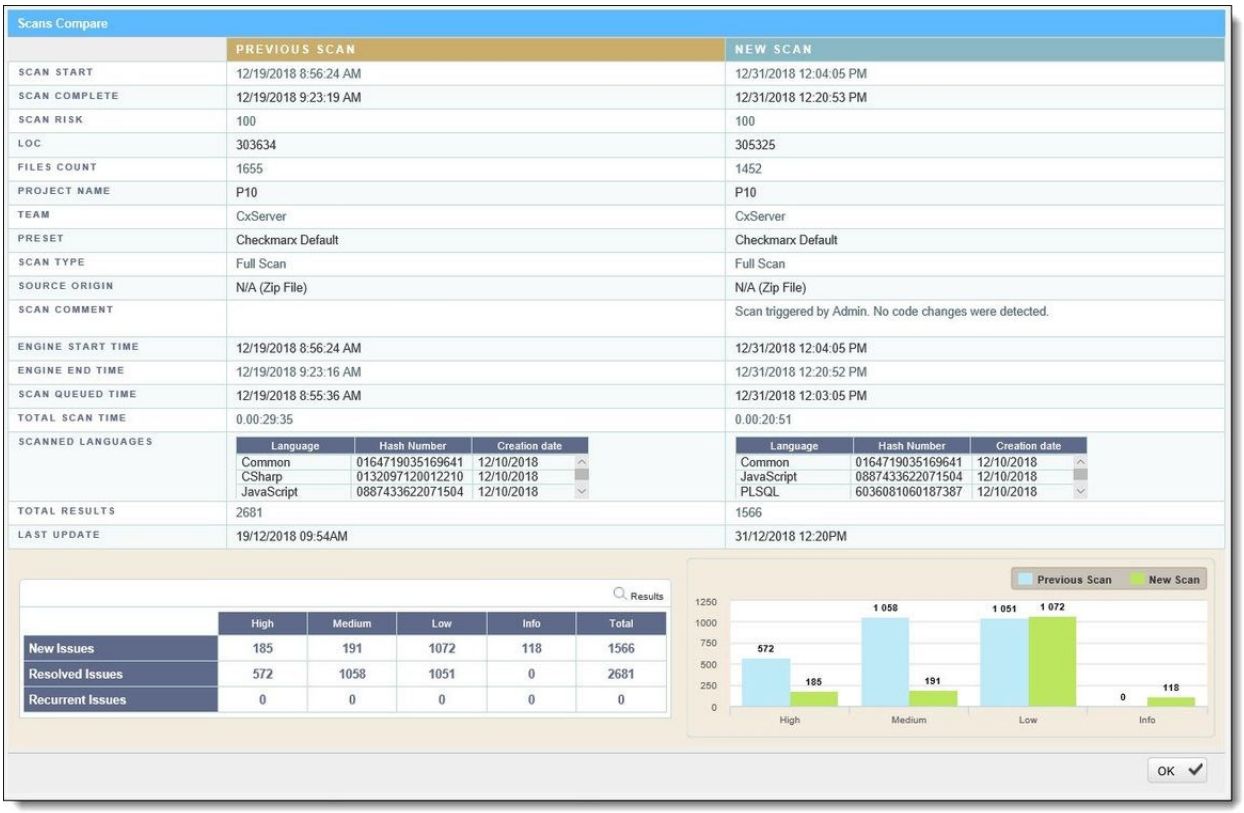
Unlocking all scans indicated in the report enables full deletion of the project.

Comparing Scans

To compare scans:

In Projects & Scans > All Scans, select two scans to compare.

Click the Compare Scans option. The Scans Compare screen is displayed.

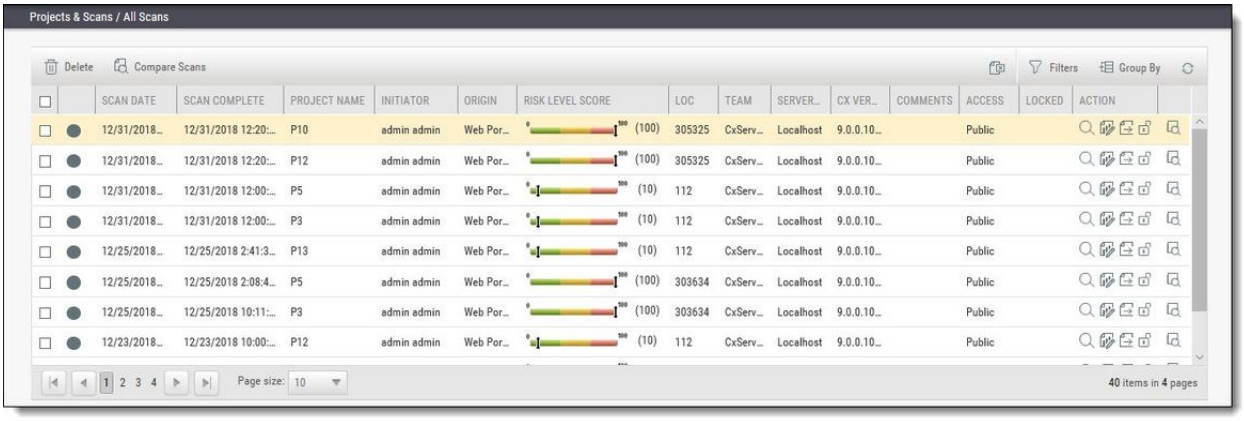


Click on the Results button in order to see a 'file compare' showing the code differences in each file, grouped by vulnerability/scan result.

Scan Result Actions

Navigating All Scans

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

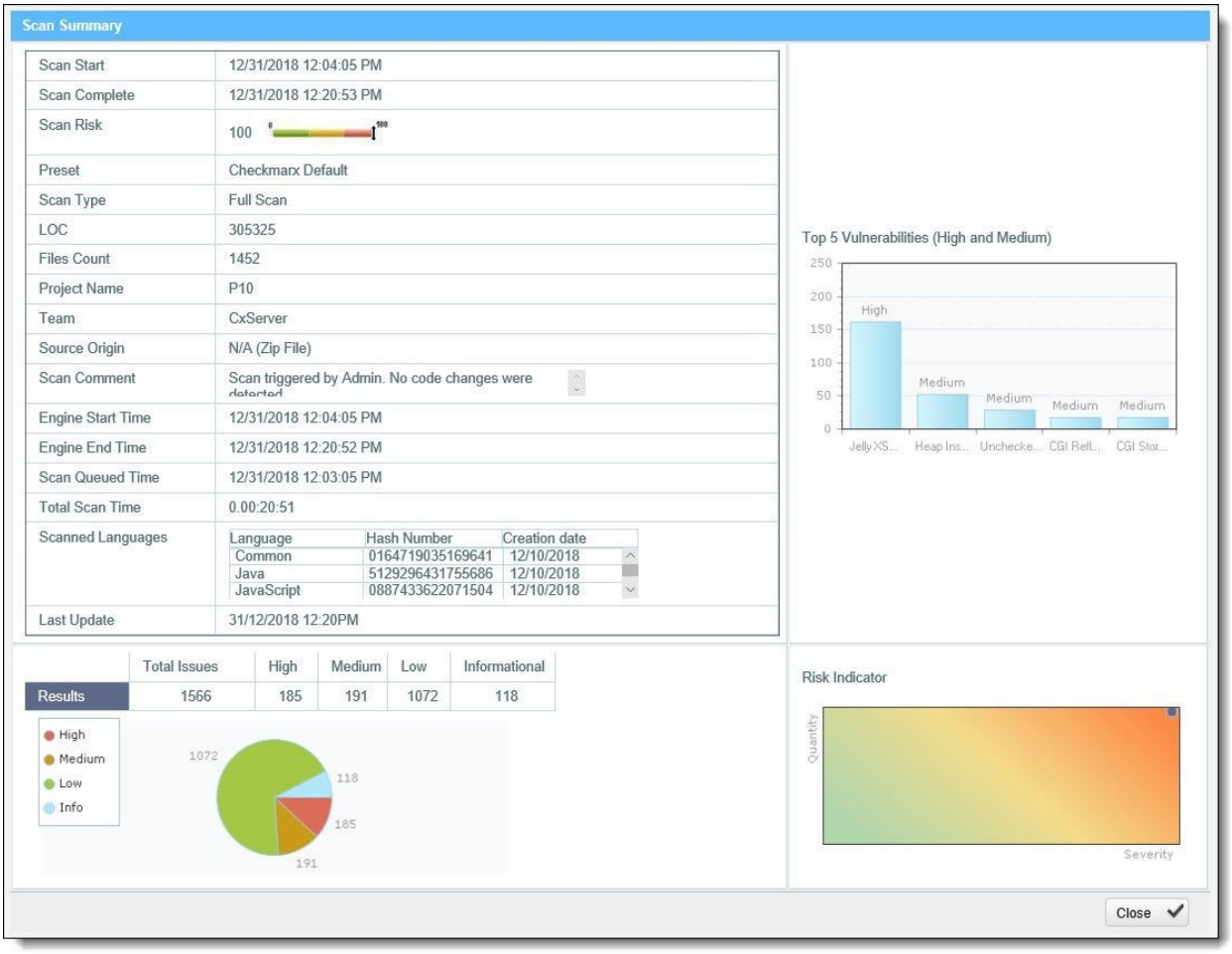


Column	Action	Description
Action		View Scan Results
		Create Report
		Open Scan Summary
		Download Scan Logs

Viewing the Scan Summary

To view the Scan Summary:

In Projects & Scans > All Scan, click the Open Scan Summary  option. The Scan Summary window is displayed.



The Scan Summary window includes the following scan information:

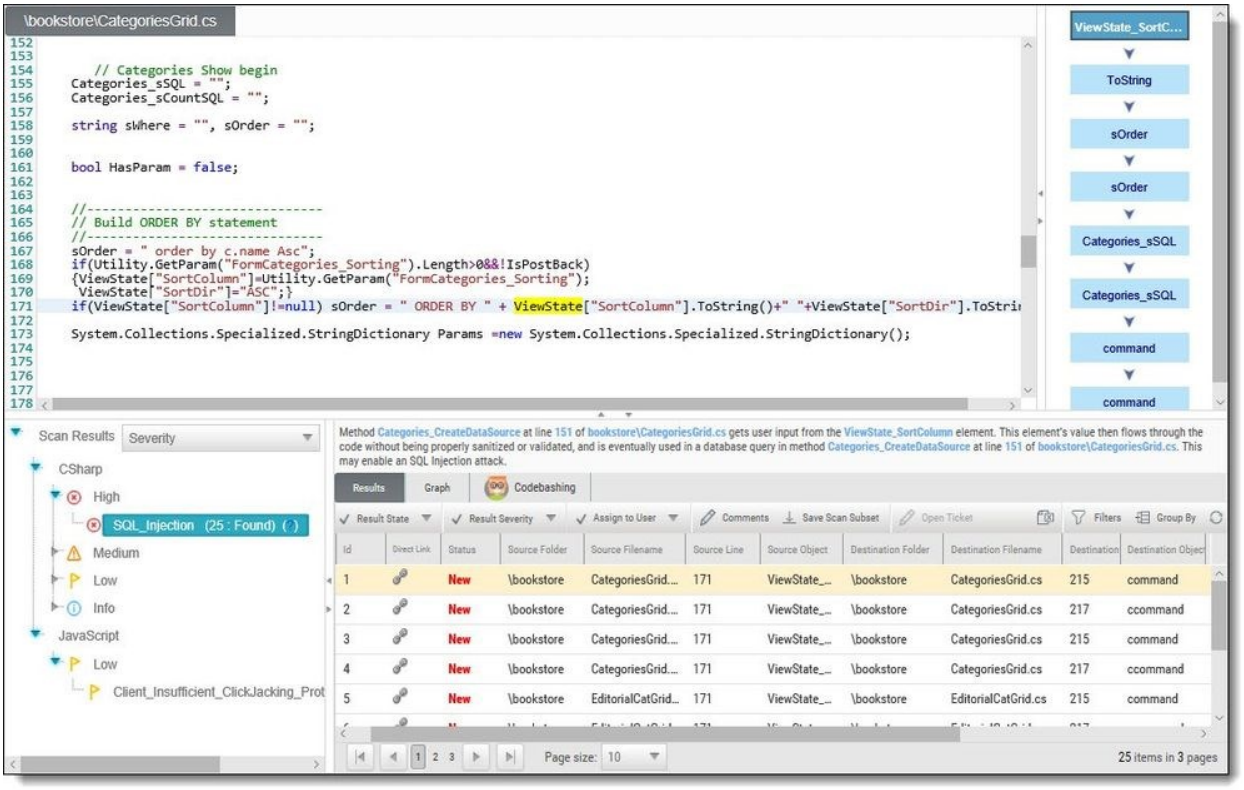
- Scan details table: Shows the scan start and finish dates, risk level, LOC (Lines of Code in project), number of files, preset (query set), source origin, and comment.
- The Top 5 High and Medium Vulnerabilities chart shows the five most common high and medium vulnerabilities found in this scan.
- 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.

Click the Download Scan Logs option to download all server logs related to this scan.

■ This action is available to CxSAST Administrators, SP Managers, Company Managers, and Scanners.

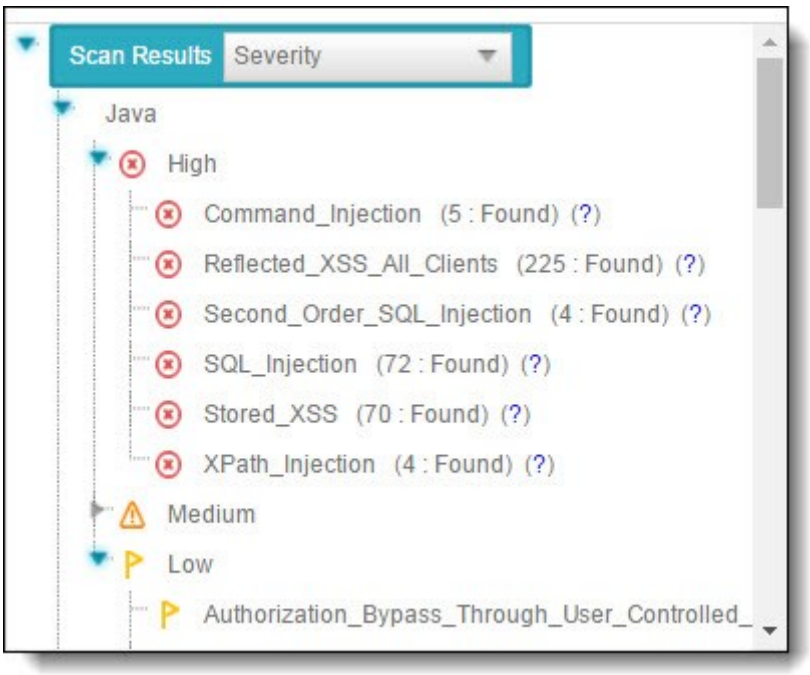
Navigating Scan Results

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 ( ) takes you to the **Codebashing™**, our interactive learning platform, where you can learn about code vulnerabilities, why they happen, and how to eliminate them. Once there, select a tutorial and start sharpening your skills.

■ Codebashing provides developers with a new in-context learning platform that sharpens the skills they need to fix vulnerabilities and write secure code. This new approach makes AppSec learning an engaging experience, more effective, with a fast learning curve.

Codebashing is currently available as a free limited edition to all users. This version includes a free edition of Codebashing covering:

- **Lessons**: SQL Injection (SQLi), Cross-site scripting (XSS), XML Injection (XXE)
- **Languages**: Java, .Net, PHP, Node.JS, Ruby, Python

The full and paid version will include over 20+ lessons and additional languages:

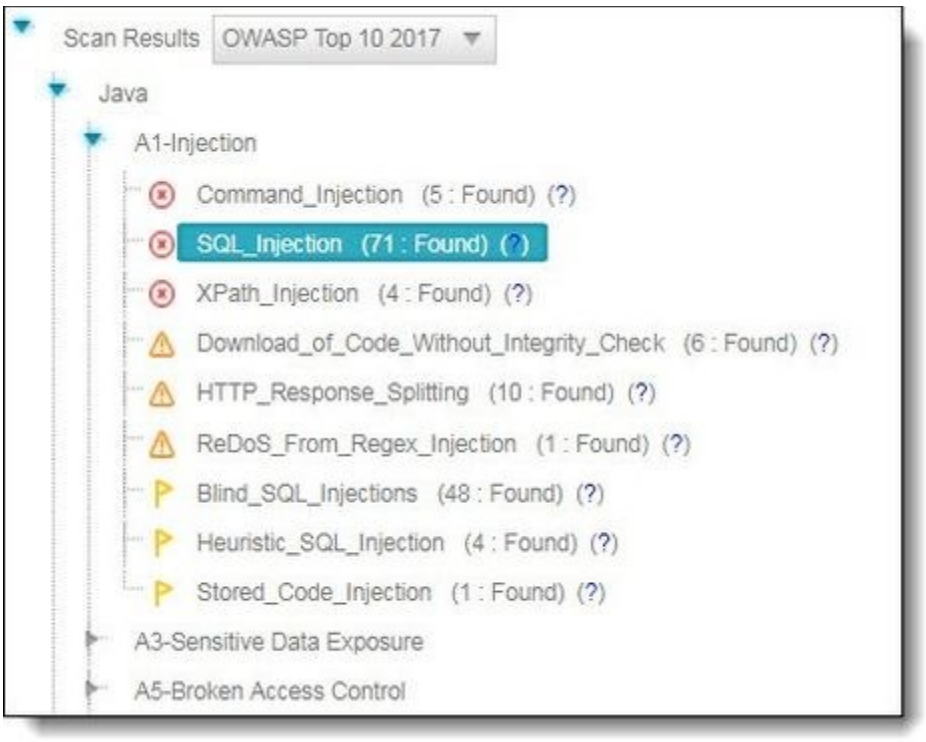
- **Lessons**: Session fixation, Use of insufficiently random values, Reflected XSS, Command Injection, DOM XSS, Directory (Path) Traversal, Privileged Interface Exposure, Leftover Debug Code, Session Exposure in URL, User Enumeration, Horizontal Privilege Escalation, Vertical Privilege Escalation, Authentication Credentials in URL, Cross Site Request Forgery (POST), Cross Site Request Forgery (GET), Click Jacking, Insecure URL Direct.
- **Languages**: Scala, C/C++.

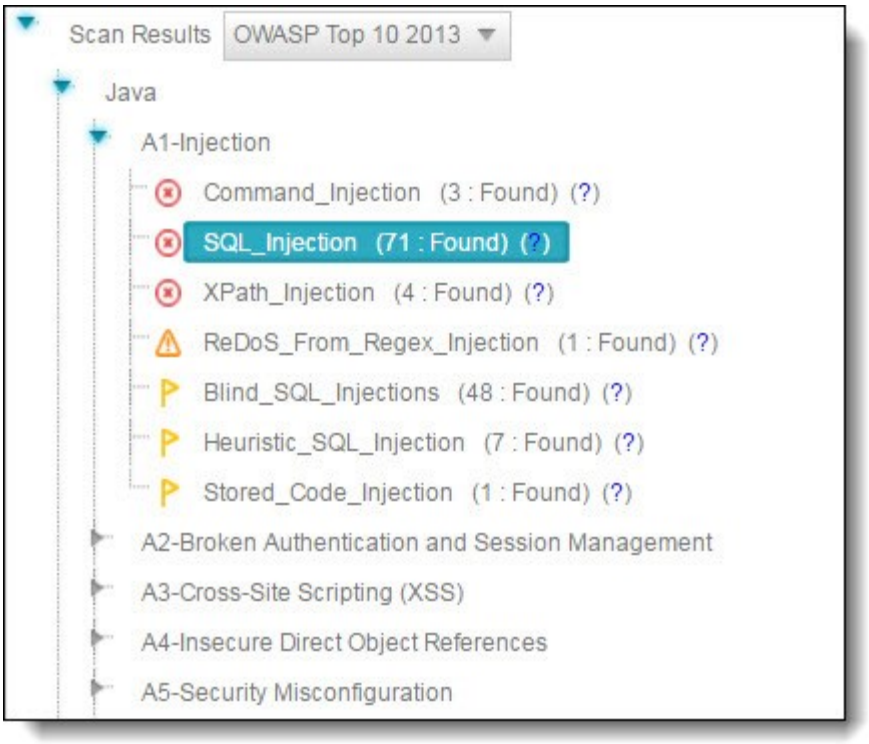
Clicking **(?)** displays comprehensive information about this vulnerability type, including risk details, a description of the cause and mechanism, recommendations for avoiding the vulnerability and source code examples.

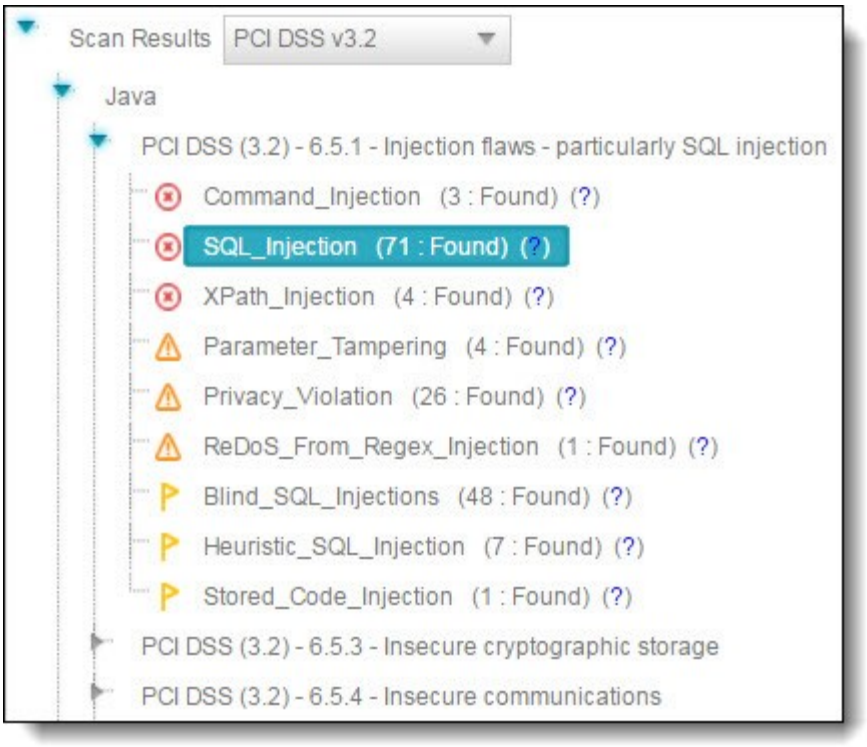
The Severity drop-down list provides the following methods for displaying the detected vulnerabilities:

- **Severity** - displays application security risks (vulnerabilities) by severity (High, Medium and Low)
- **OWASP Top 10 2017** - displays the vulnerabilities associated with categories (A1 to A10) that appear in the list of the 10 most serious risks, as defined by OWASP (Open Web Application Security Project). All vulnerabilities that do not fall into any of the OWASP Top 10 2017 categories are grouped under un-categorized.
- **OWASP Top 10 2013** - displays the vulnerabilities associated with categories (A1 to A10) that appear in the list of the 10 most serious risks, as defined by OWASP (Open Web Application Security Project). All vulnerabilities that do not fall into any of the OWASP Top 10 2013 categories are grouped under un-categorized.
- **PCI** - displays the vulnerabilities associated with categories (DSS v3.2), as defined by PCI (Payment Card Industry). All vulnerabilities that do not fall into any of the PCI categories are grouped under un-categorized.
- **FISMA** - displays the vulnerabilities associated with categories (2014), as defined by FISMA (Federal Information Security Modernization Act). All vulnerabilities that do not fall into any of the FISMA categories are grouped under un-categorized.
- **NIST** - displays the vulnerabilities associated with categories (SP 800-53), as defined by NIST (National Institute of Standards and Technology). All vulnerabilities that do not fall into any of the NIST categories are grouped under un-categorized.
- **OWASP Mobile Top 10 2016** - displays the vulnerabilities associated with categories (M1 to M10) that appear in the list of the 10 most serious risks, as defined by OWASP (Open Web Application Security Project). All vulnerabilities that do not fall into any of the OWASP Mobile Top 10 2017 categories are grouped under un-categorized.
- **Custom** - a user-defined method for rating the security levels. Using the Custom method requires integrating the user's severity rating method with CxSAST. For more details, please contact Checkmarx support.

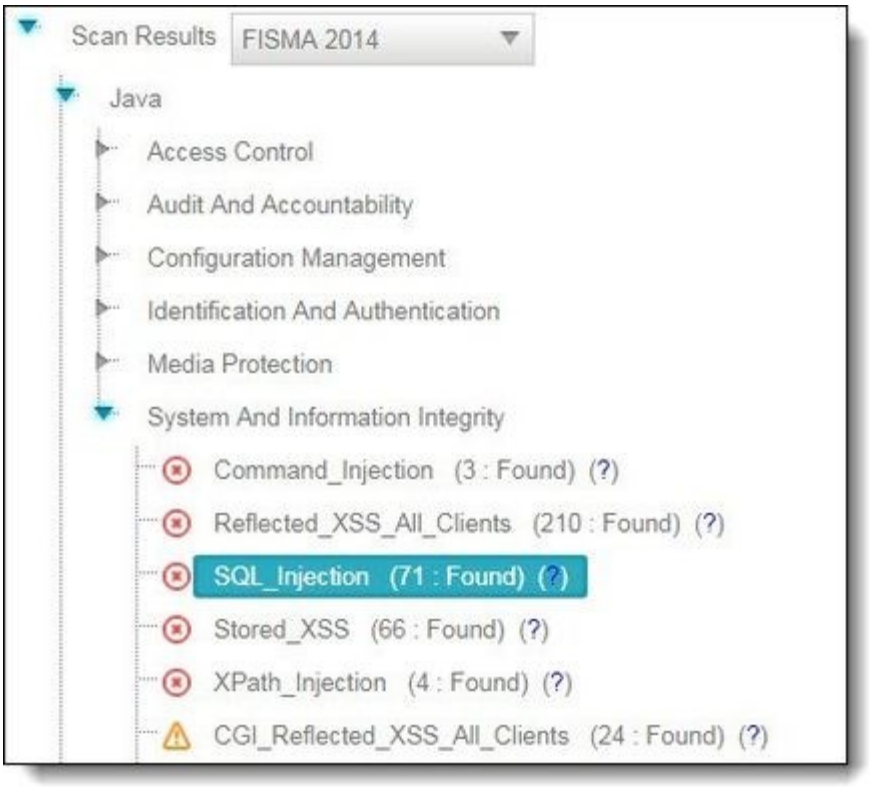
The following images show the Severity drop-down list opened after selecting OWASP (2017 or 2013) and PCI for the first, second and third image, respectively.

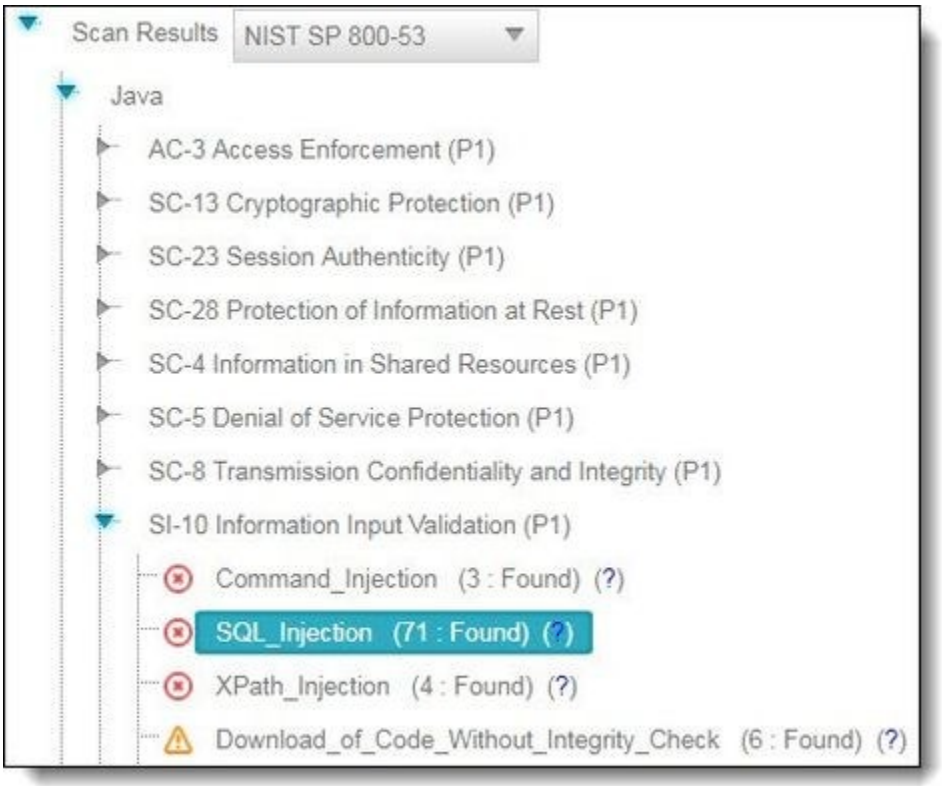






The following images show the Severity drop-down list opened after selecting FISMA and NIST for the first and second image, respectively.

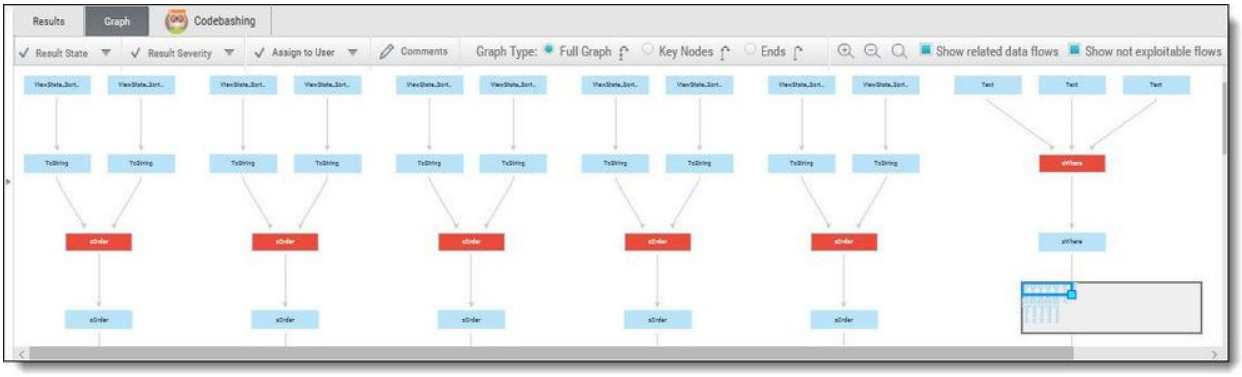




Select a query to view found instances in the **Results** pane:

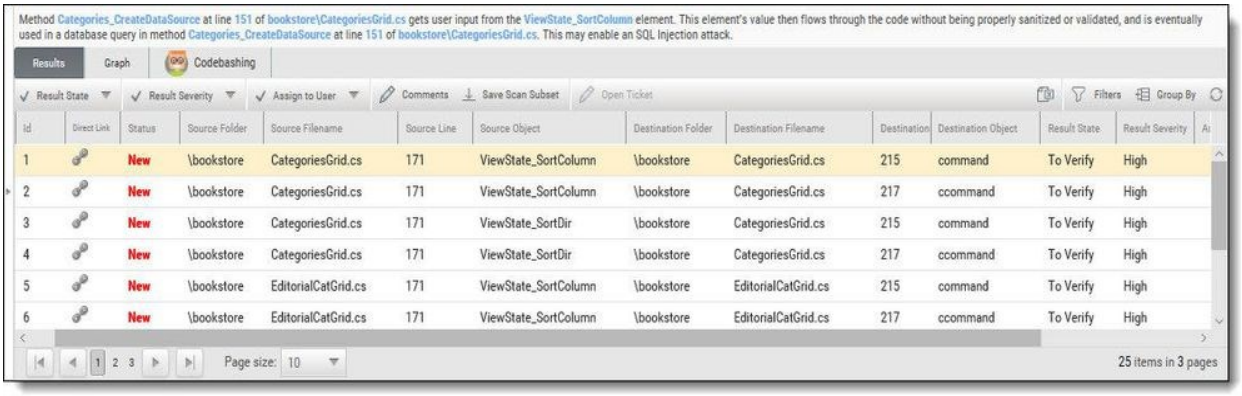
Results (lower-right pane) - Displays the found instances of the query that is selected in the **Queries** pane in the following two formats:

- **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 (see *CxSAST Plugin and Integration Guide*), the Graph pane displays full paths of the code elements that constitute the found instances together with

- **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 (See *Managing Tables*).



Id	Direct Link	Status	Source Folder	Source Filename	Source Line	Source Object	Destination Folder	Destination Filename	Destination	Destination Object	Result State	Result Severity
1		New	\bookstore	CategoriesGrid.cs	171	ViewState_SortColumn	\bookstore	CategoriesGrid.cs	215	command	To Verify	High
2		New	\bookstore	CategoriesGrid.cs	171	ViewState_SortColumn	\bookstore	CategoriesGrid.cs	217	ccommand	To Verify	High
3		New	\bookstore	CategoriesGrid.cs	171	ViewState_SortDir	\bookstore	CategoriesGrid.cs	215	command	To Verify	High
4		New	\bookstore	CategoriesGrid.cs	171	ViewState_SortDir	\bookstore	CategoriesGrid.cs	217	ccommand	To Verify	High
5		New	\bookstore	EditorialCatGrid.cs	171	ViewState_SortColumn	\bookstore	EditorialCatGrid.cs	215	command	To Verify	High
6		New	\bookstore	EditorialCatGrid.cs	171	ViewState_SortColumn	\bookstore	EditorialCatGrid.cs	217	ccommand	To Verify	High

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 permission 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.

Result 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.

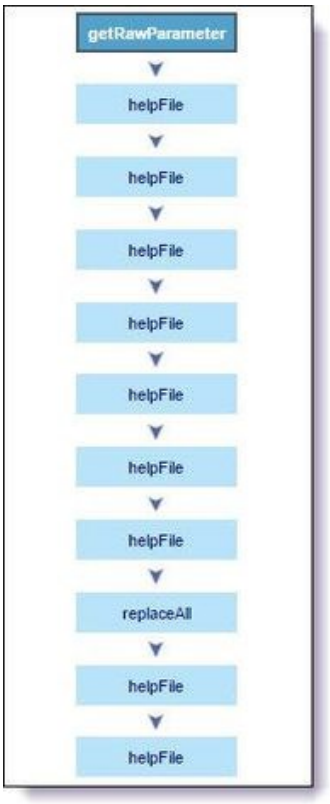
Click **Save Scan Subset** for selected instances to appear in the results list as an independent result set.

If configured, tickets can be opened in a bug tracking system (e.g. Jira) by clicking **Open ticket**.

Click the link icon 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.

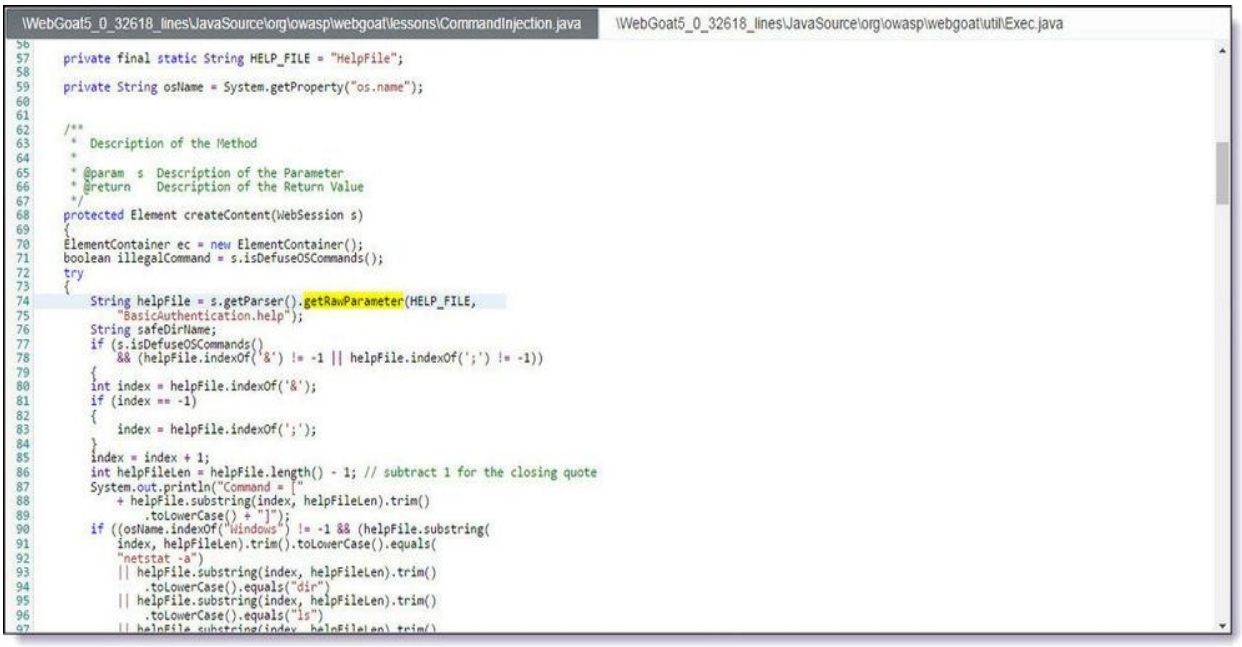


Number of Nodes

The Number of Nodes column in the Results panel provides the number of nodes in the attack vector provided by each result. Sorting, filtering and grouping options are available. This column is disabled by default and can be made available from the Columns selection tool.

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.

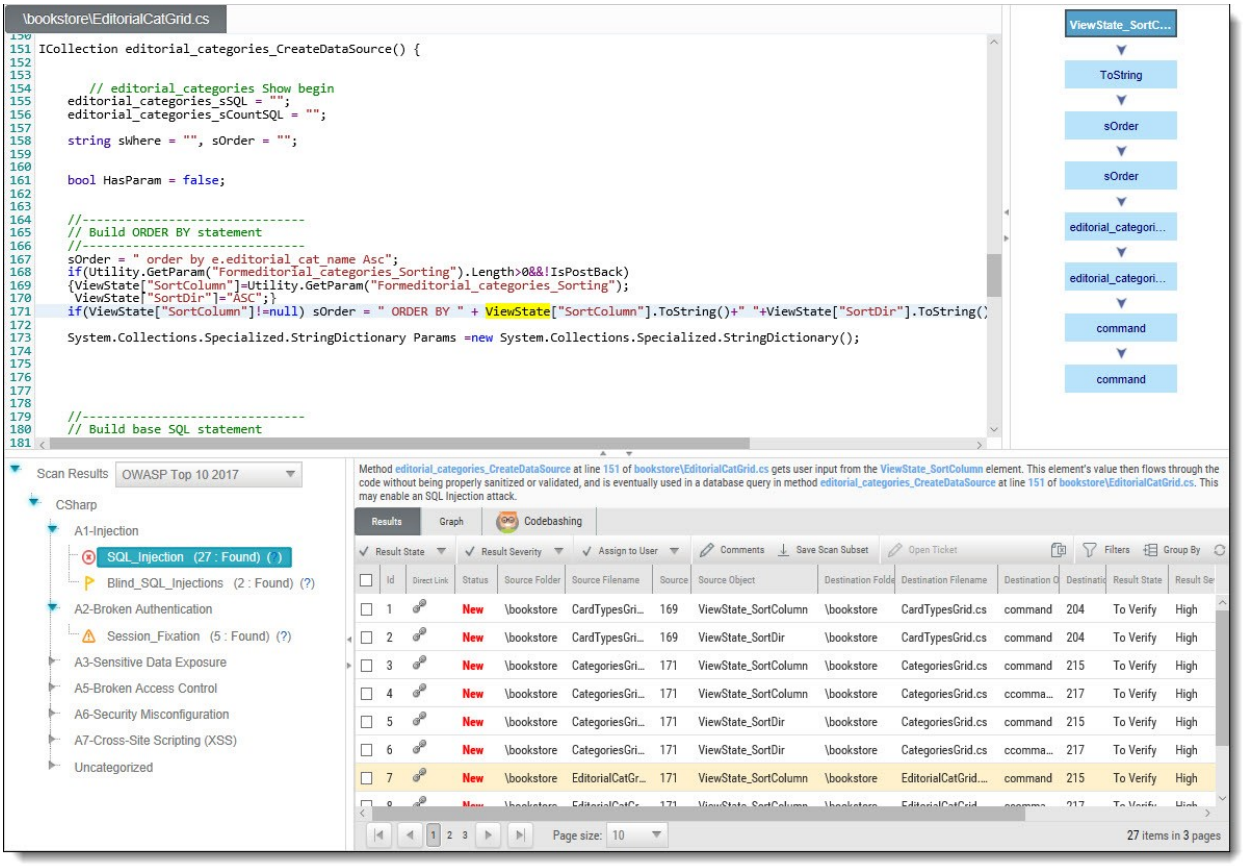


Highlights the code line containing the element that is selected in the **Path** pane.

■ When using the CxSAST IDE plugins (see *CxSAST Plugin and Integration Guide*) you can immediately fix the code in place!

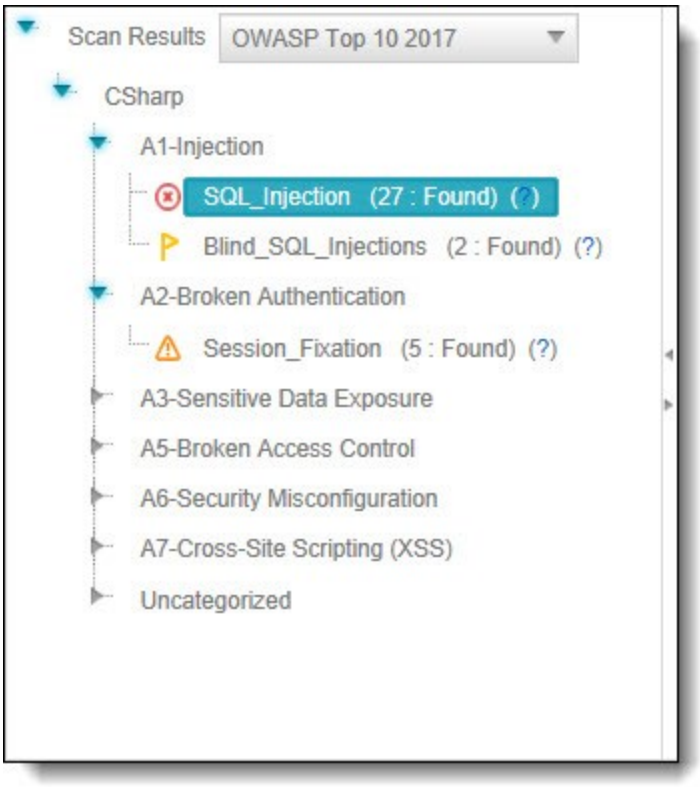
Scan Results Example

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



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.

The Queries pane (bottom-left) shows that 27 instances of the SQL_Injection vulnerability were found.



Clicking **(**  **)** takes you to the **Codebashing**, where you can learn more about the selected vulnerability, why it happens, and how to eliminate it.

CoachCodebashing™

AppSec Coach provides developers with a new in-context learning platform that sharpens the skills they need to fix vulnerabilities and write secure code. This new approach makes AppSec learning an engaging experience, more effective, with a fast learning curve.

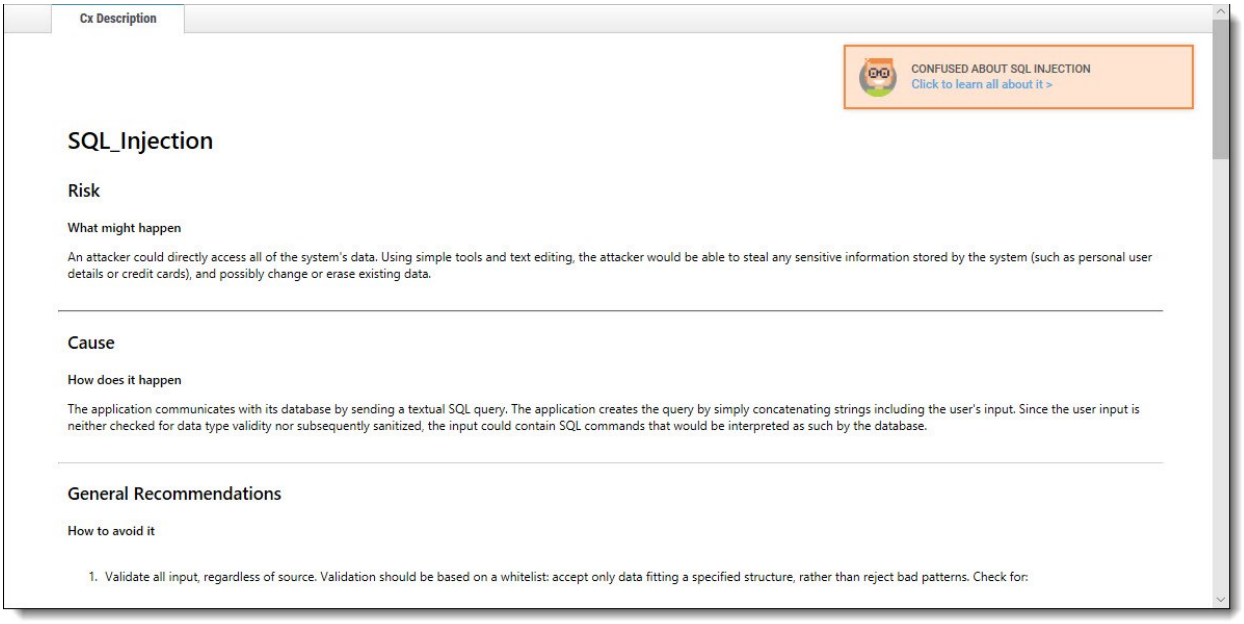
AppSec Coach is currently available as a free limited edition to all users. This version includes a free edition of AppSec Coach covering:

- **Lessons**: SQL Injection (SQLi), Cross-site scripting (XSS), XML Injection (XXE)
- **Languages**: Java, .Net, PHP, Node.JS, Ruby, Python

The full and paid version will include over 20+ lessons and additional languages:

- **Lessons**: Session fixation, Use of insufficiently random values, Reflected XSS, Command Injection, DOM XSS, Directory (Path) Traversal, Privileged Interface Exposure, Leftover Debug Code, Session Exposure in URL, User Enumeration, Horizontal Privilege Escalation, Vertical Privilege Escalation, Authentication Credentials in URL, Cross Site Request Forgery (POST), Cross Site Request Forgery (GET), Click Jacking, Insecure URL Direct.
- **Languages**: Scala, C/C++.

Clicking **(?)** displays full general information for the SQL_Injection, including risk, cause and recommendations with code examples.



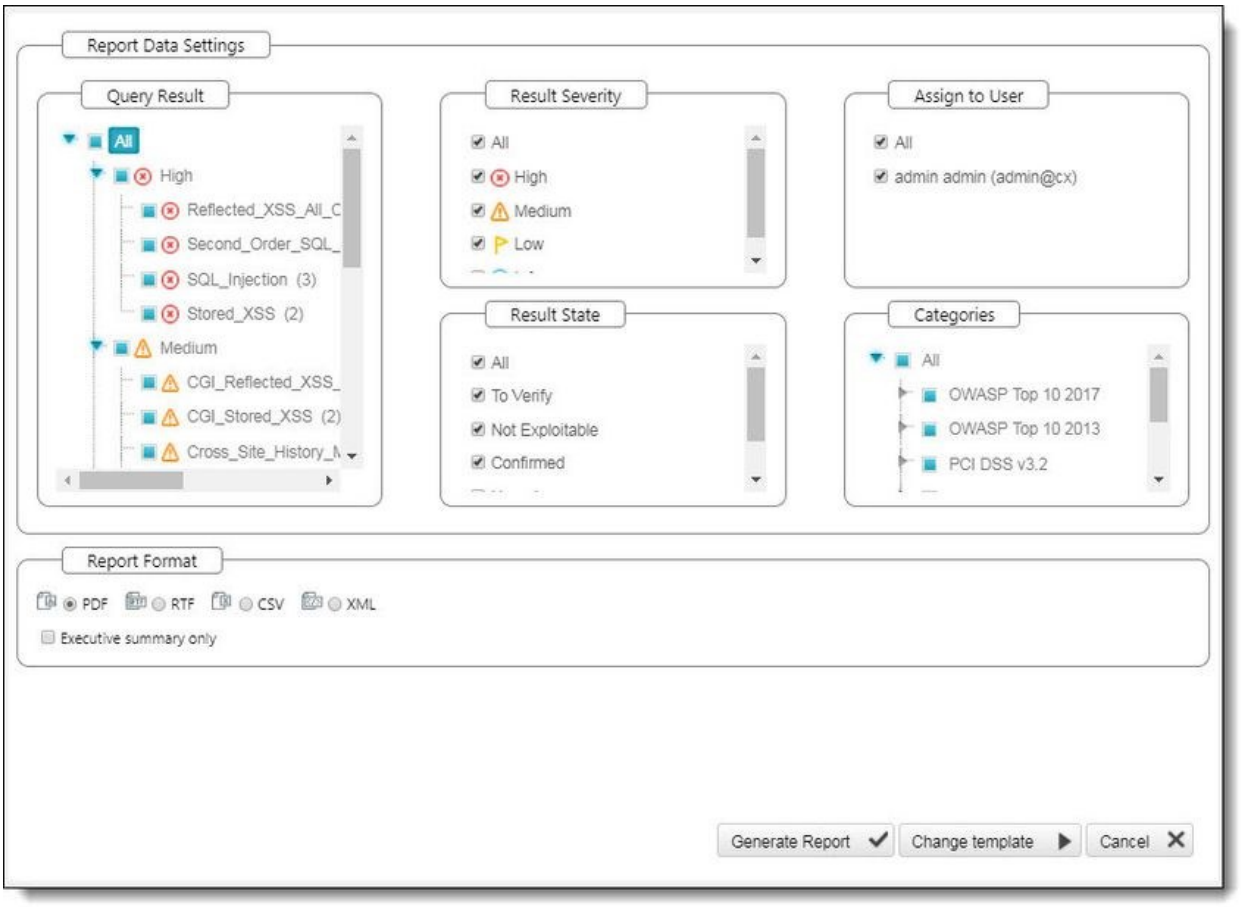
Selecting a specific instance of the vulnerability in the **Results** pane (bottom, center and right) displays the instance's code details at the top of the pane, and displays the path of component code elements in the **Path** pane (top-right). The Path pane shows all the code elements leading from 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.

Generating Scan Result Reports

You can generate a report containing detailed scan results, in any of the following formats: PDF (default), RTF, CSV or XML.

To generate a scan results report:

In the All Scans table (for all projects or for an individual project), click **Create Report**  . The report settings are displayed.



Filter results for the generated report and select the report file format.

By default, all categories are selected to be included in the report.

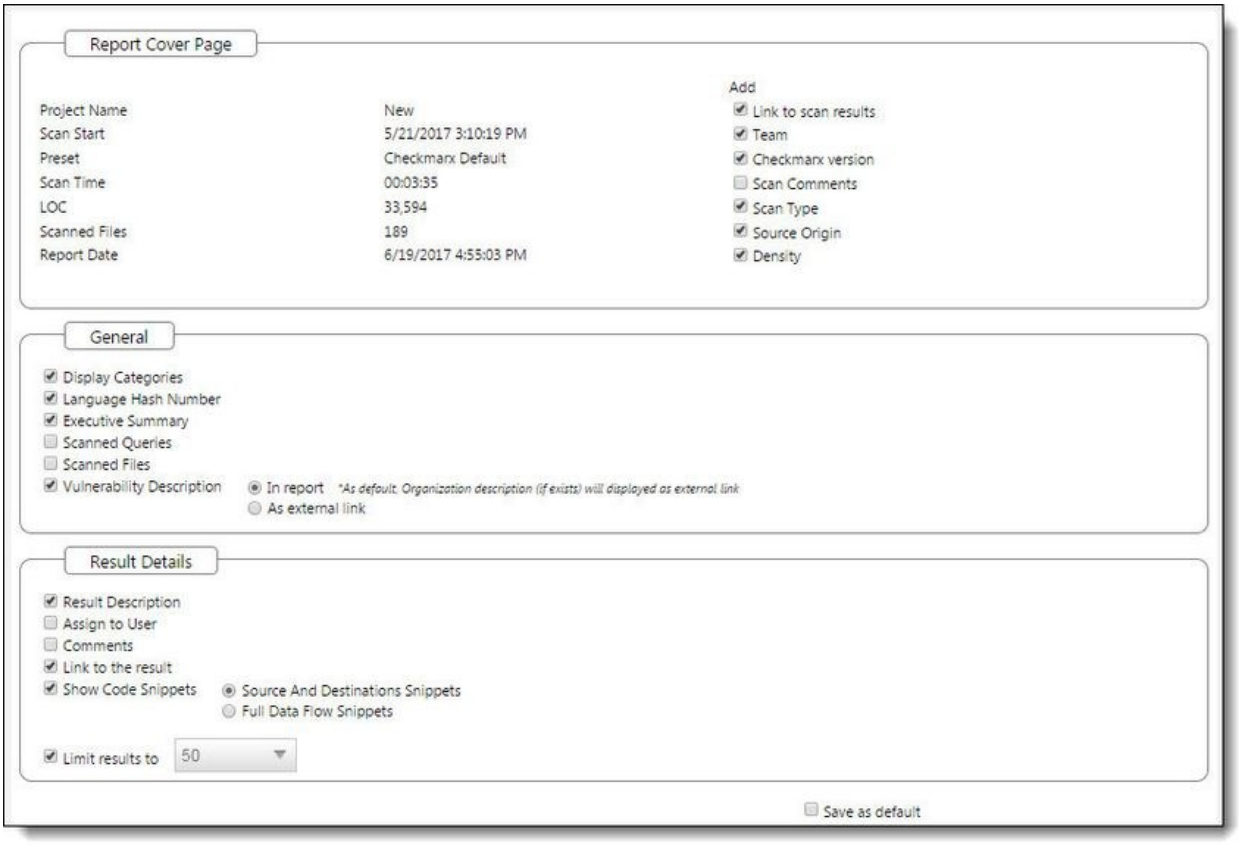
To customize categories:

Go to the relevant group under the Categories section, click the group to expand it and 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. Otherwise, follow the procedure below to save the modifications you make as an updated report template.

To change the report template:

Select **Change template**. The template setting are displayed.



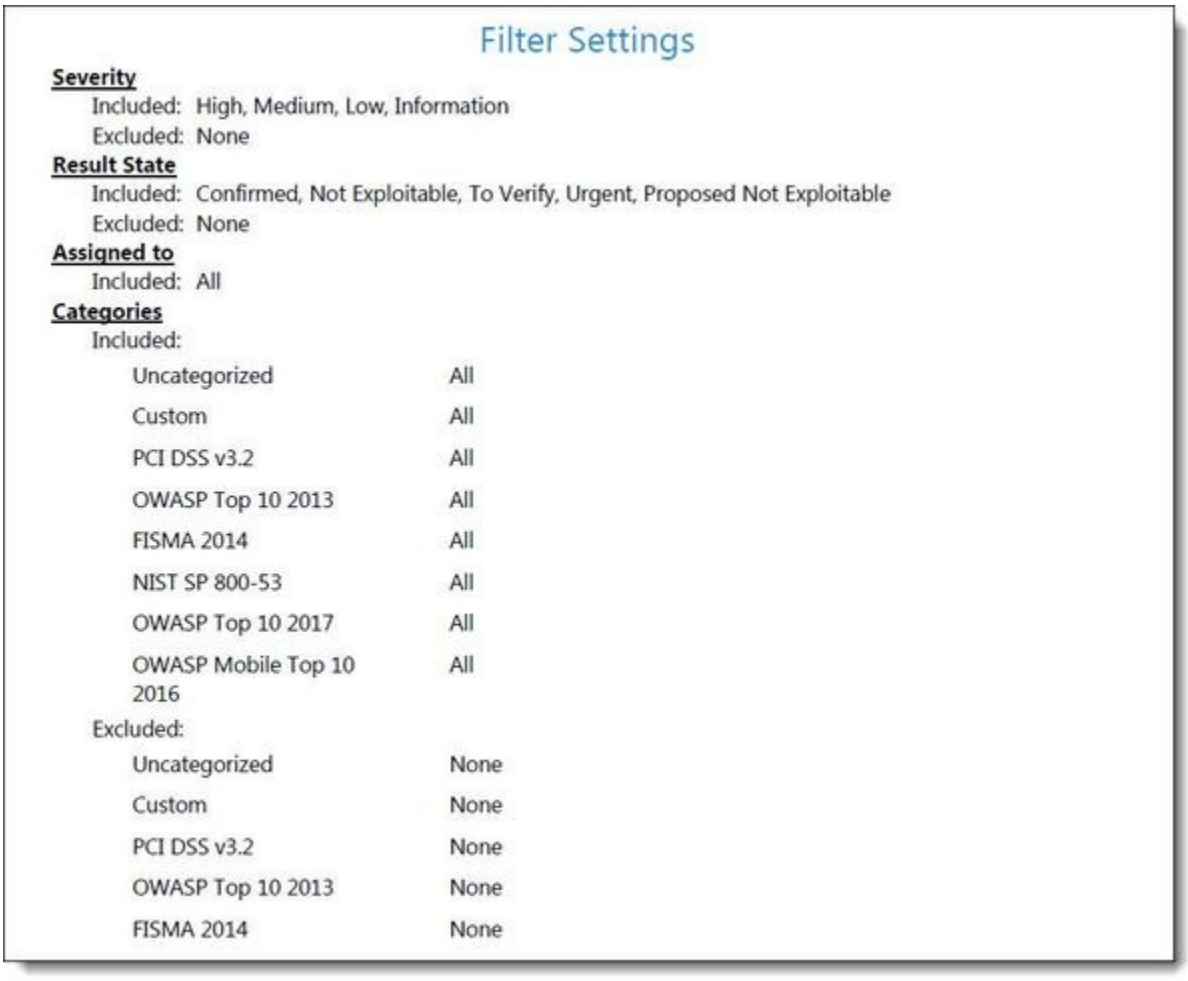
Select which details should be presented on the report cover page, in the report itself and what details to show for each result.

Select the **Save as default** check-box to save the modified template as the default report template.

Click **Back** and review all settings you defined.

Click **Generate Report**. The report starts generating.

The exclusions that were made are displayed on the Filter Setting section at the beginning of the PDF file, as shown below.



Filter Settings

Severity
Included: High, Medium, Low, Information
Excluded: None

Result State
Included: Confirmed, Not Exploitable, To Verify, Urgent, Proposed Not Exploitable
Excluded: None

Assigned to
Included: All

Categories
Included:

Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2	None
OWASP Top 10 2013	None
FISMA 2014	None

Parameters that were selected to be displayed will appear in the report even if none of these parameters (for example, OWASP A-6 category) were detected in the scan, in which case they will appear with the count "0".

The OWASP (2017, 2013 & Mobile 2016), PCI, FISMA and NIST 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).

Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection*	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	83	51
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A3-Sensitive Data Exposure*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	3	3
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	13	3
A6-Security Misconfiguration *	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	73	73
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	10	4
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	0	0
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

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	Business Impact	Issues Found	Best Fix Locations
A1-Injection*	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	83	51
A2-Broken Authentication and Session Management*	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	48	48
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	10	4
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	73	73
A6-Sensitive Data Exposure*	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	3	3
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	11	2
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	36	35
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	26	24

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	9	3
PCI DSS (3.2) - 6.5.2 - Buffer overflows	0	0
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage*	24	24
PCI DSS (3.2) - 6.5.4 - Insecure communications*	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	73	73
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	60	28
PCI DSS (3.2) - 6.5.8 - Improper access control*	26	24
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	2	1
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	24	24

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

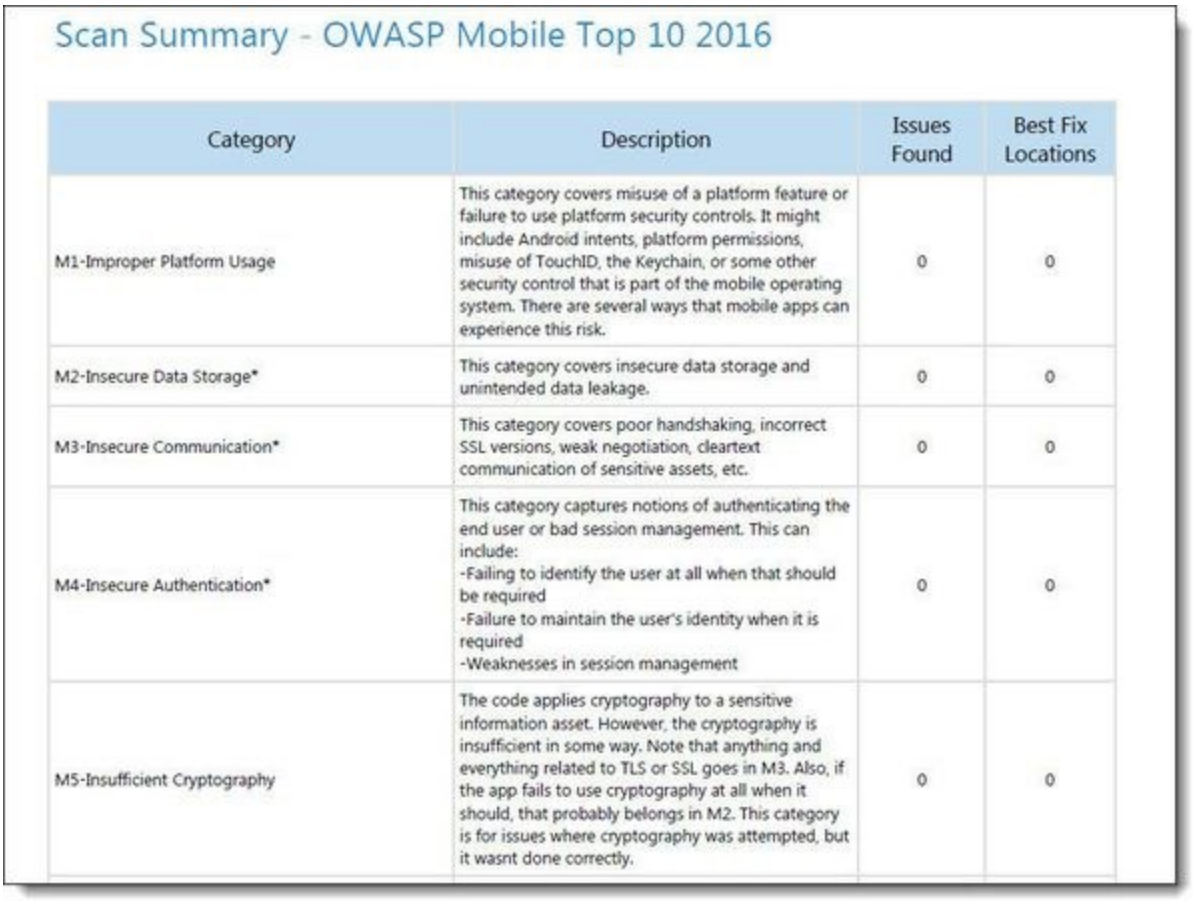
Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control*	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	11	2
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management*	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	73	73
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	84	84

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)*	71	62
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	2	1
SC-28 Protection of Information at Rest (P1)*	24	24
SC-4 Information in Shared Resources (P1)	3	3
SC-5 Denial of Service Protection (P1)*	71	47
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	109	75
SI-11 Error Handling (P2)*	73	73
SI-15 Information Output Filtering (P0)	10	4
SI-16 Memory Protection (P1)*	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.



Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage*	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication*	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication*	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0

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.

.CSV Report Results

The following is a basic description of the fields provided in the .csv report result, which is generated by the create report feature if the selected format is .csv:

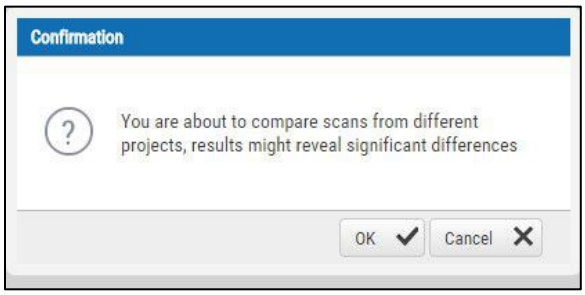
- **SrcFileName** – file name of the first node of the result
- **Line** – line of the first node of the result
- **Column** – column of the first node of the result
- **NodeId** – internal id to be able to identify the query in the first node
- **Name** – text of the first node of the result
- **DestFileName** – file name of the last node of the result
- **DestLine** – line of the last node of the result
- **DestColumn** – column of the last node of the result
- **DestNodeId** – internal id to be able to identify the query in the last node
- **DestName** – text of the last node of the result

Comparing Scan Result Sets

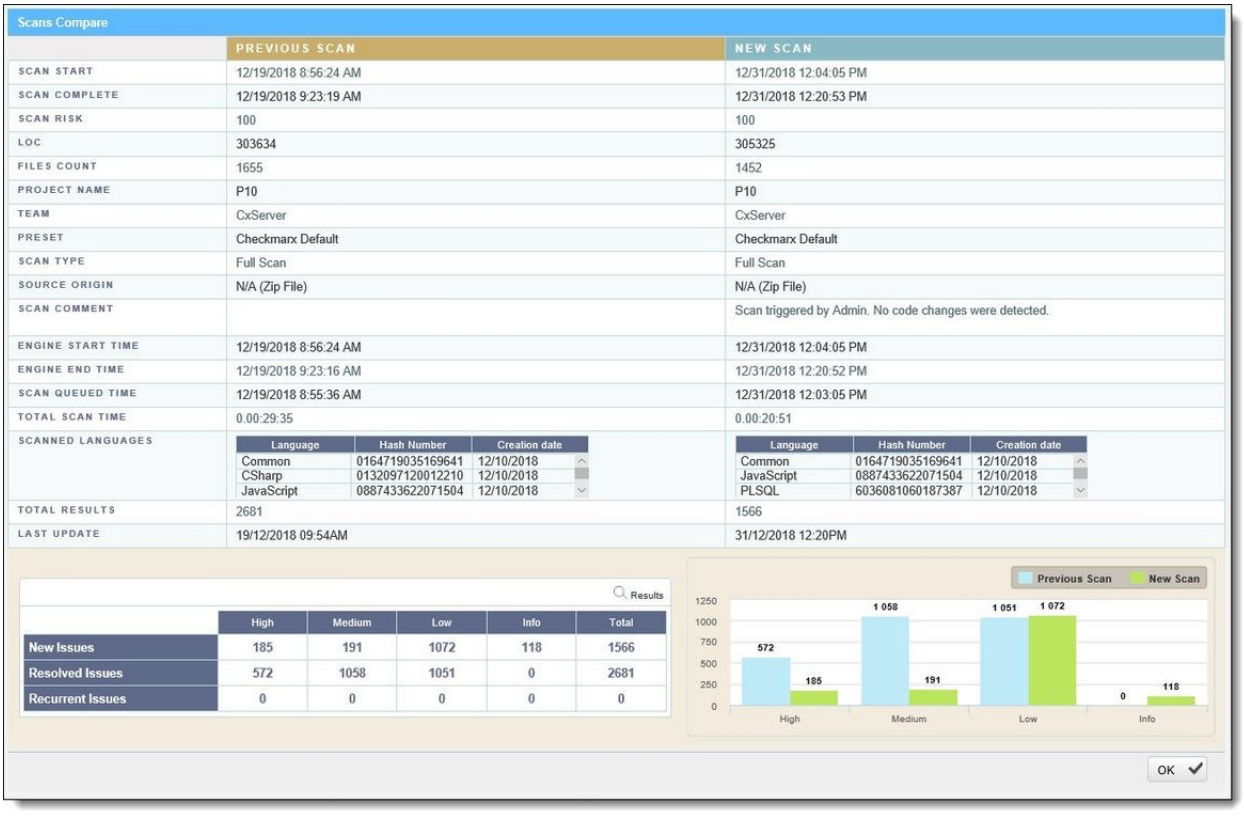
You can now compare the results of two scans in separate projects. CxSAST provides a summary of differences, and an interactive interface similar to the interface for results of single scan.

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"



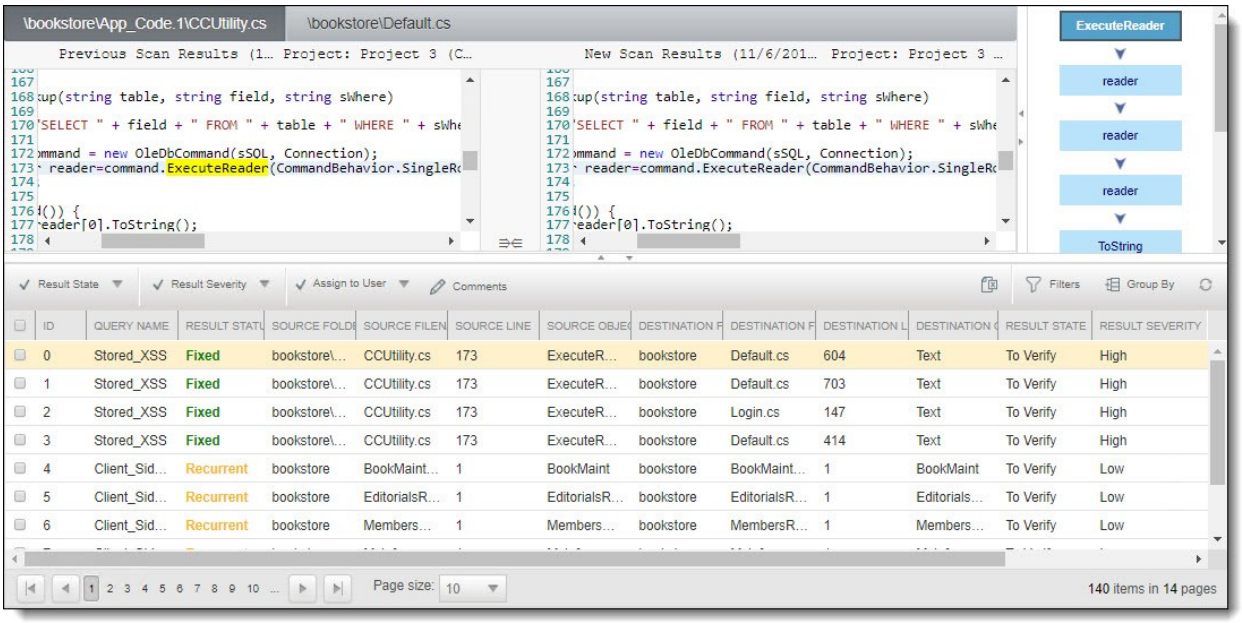
A comparison summary is displayed:



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:
    - **New Issues**: Issues that were found only in the newer scan
    - **Resolved Issues**: Issues that were found only in the older scan
    - **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, click Results. A code comparison is displayed:

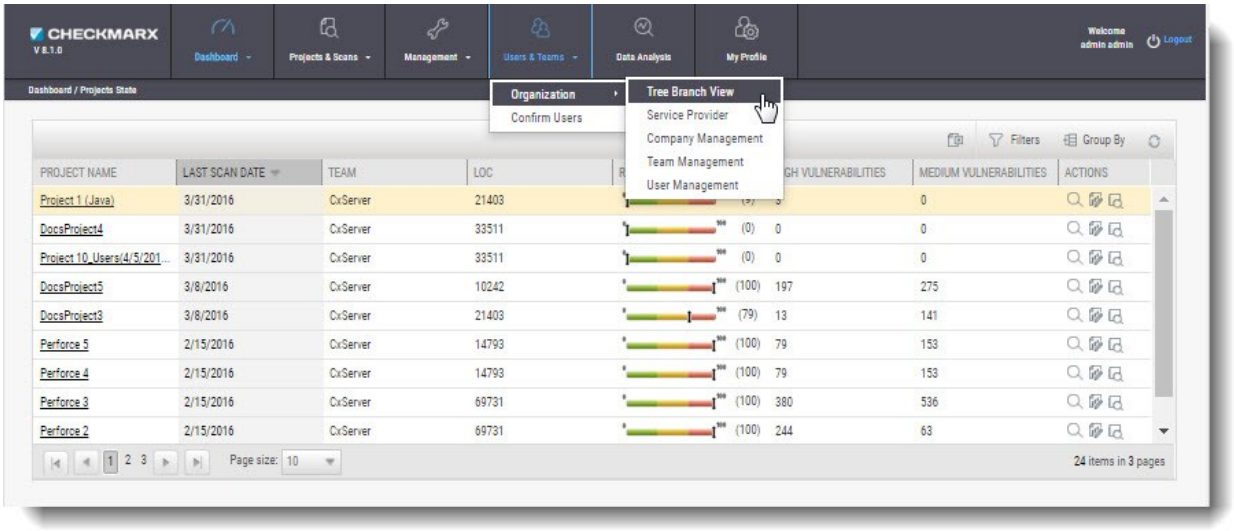


User Administration

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.

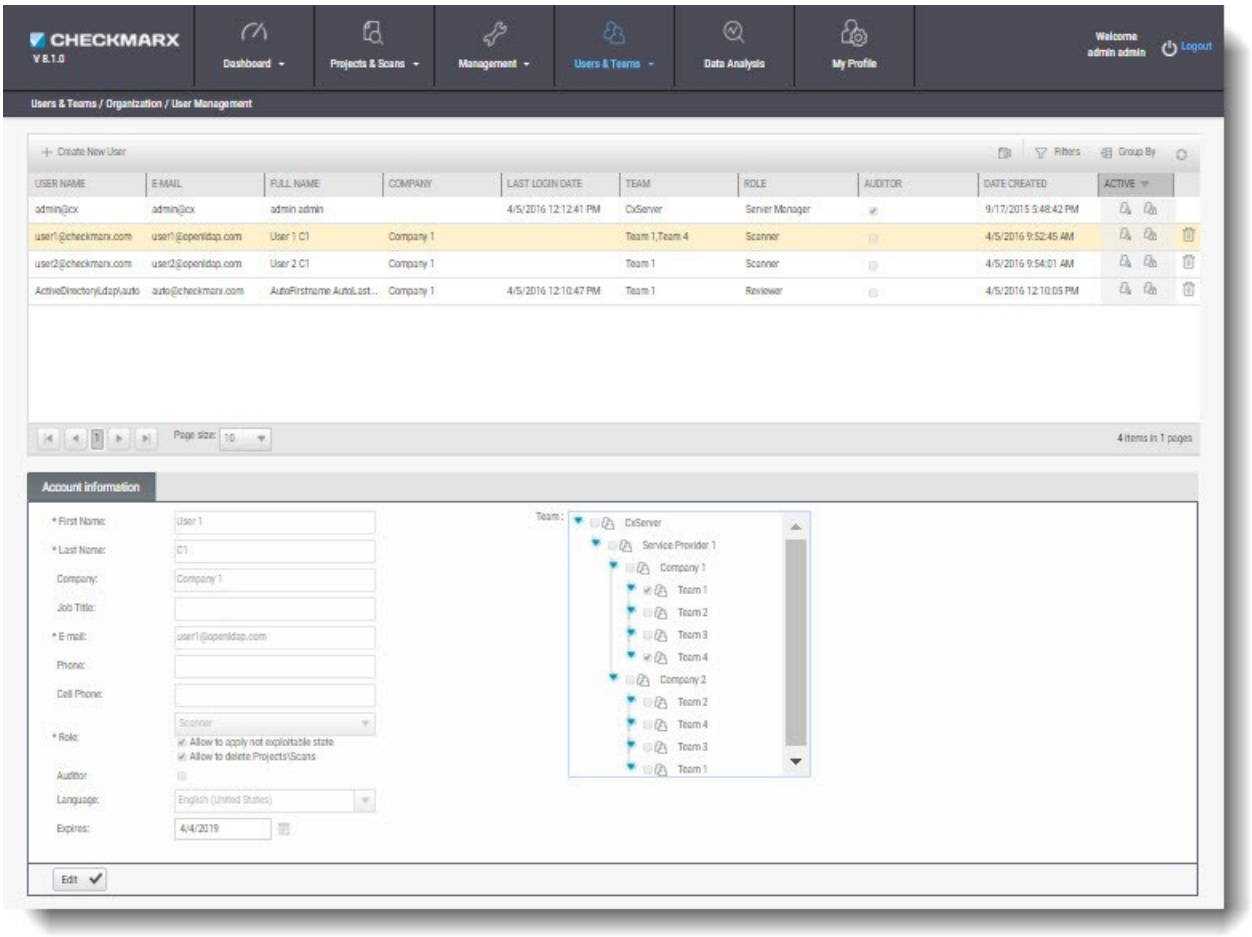
In This Section:

Creating User Accounts in the Web Interface

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:

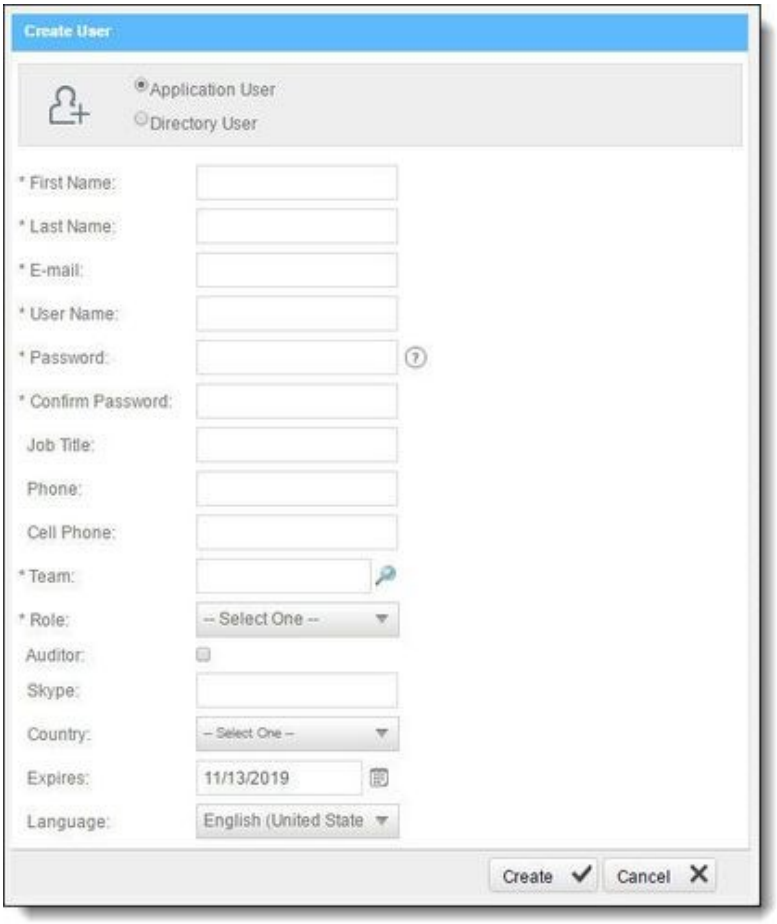
Go to **Users & Teams** > **Organization** > **User Management**. The User Management window is displayed.



Click **Create New User**.

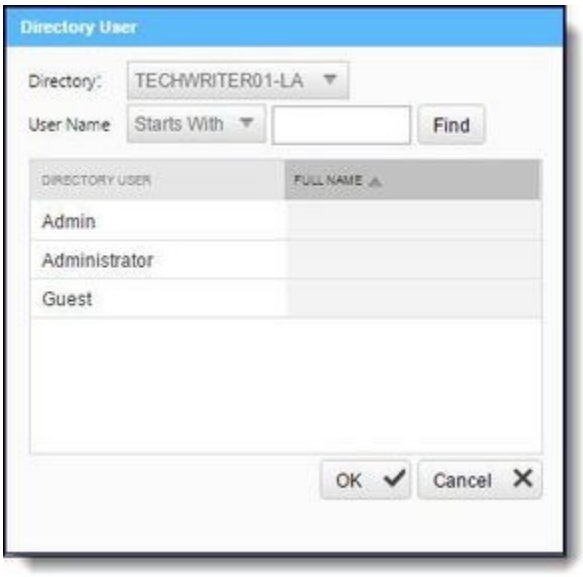
Once the Create User Window is displayed, select **Application User** (password is mandatory) or **Directory User** (authentication is managed by the selected Directory, e.g. LDAP / SAML Server).

■ The information fields in the Create User window are displayed according to the selected User type.



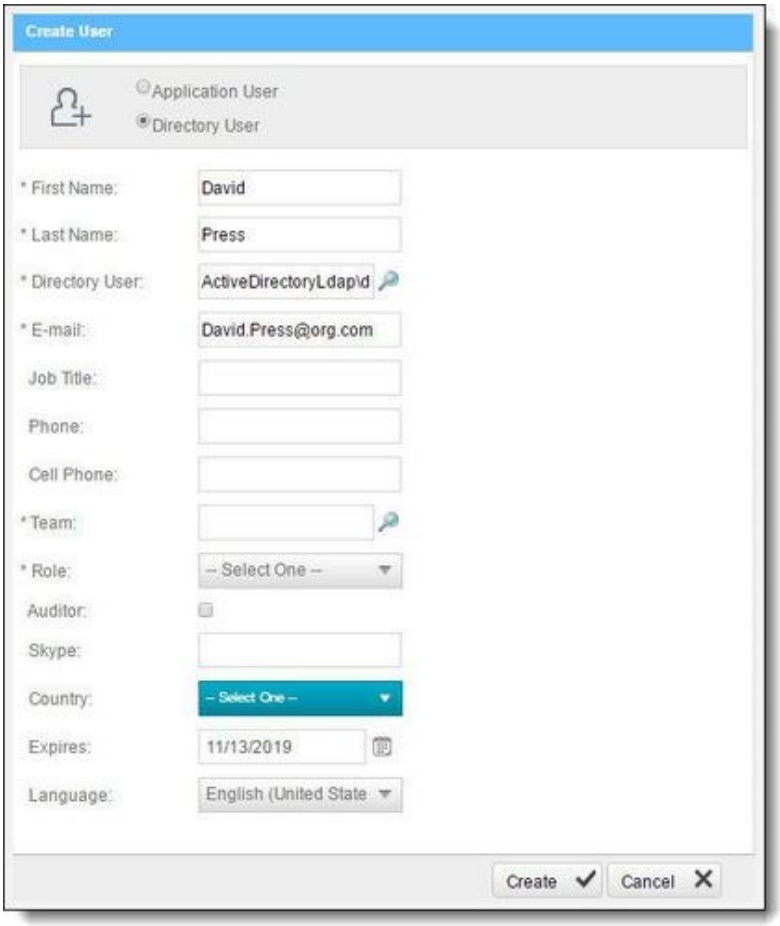
If you selected **Directory User**, the Directory User dialog window is displayed.

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 (see *CxAudit Guide*).
- **Language** defines the UI language for each user according to list of supported languages.

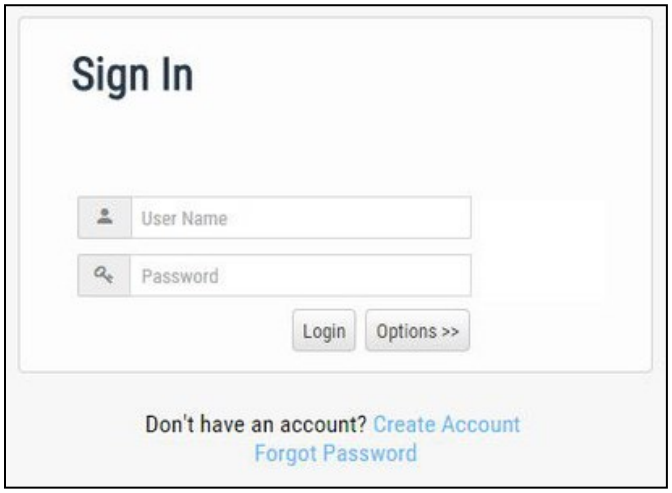
Click **Create**.

Creating User Accounts via User Registration

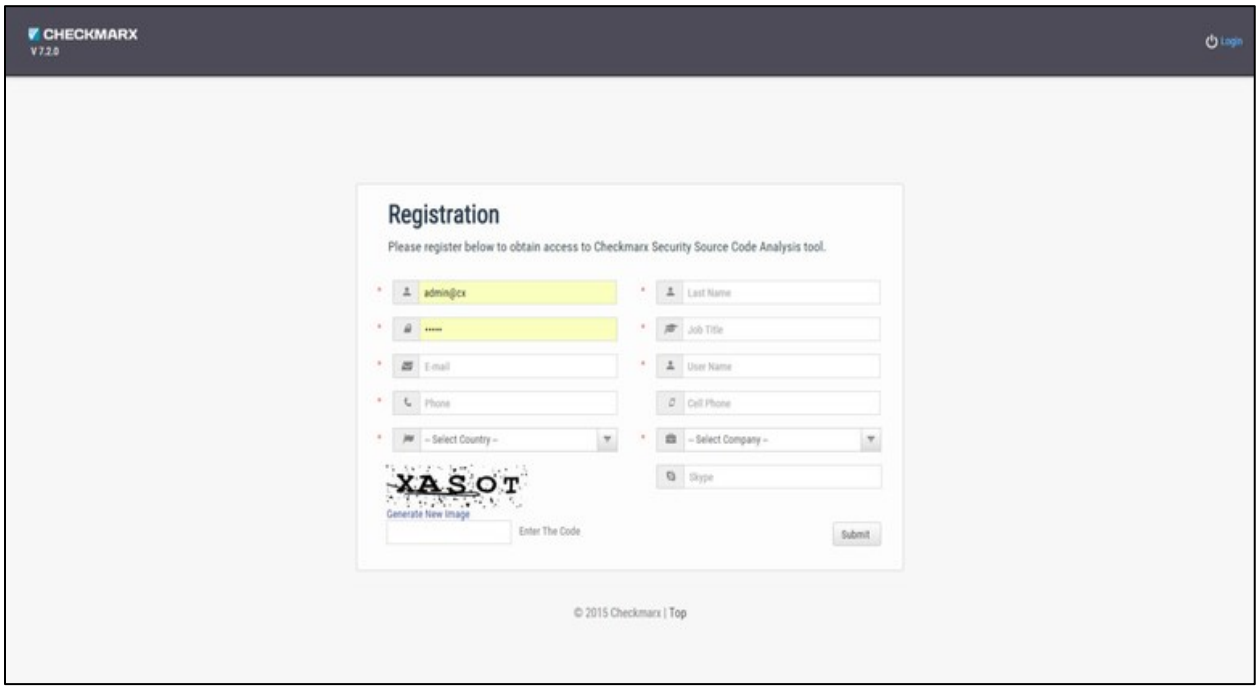
Organizational members can sign up for a user account to be confirmed by their Manager. At sign-up, the user specifies the company, and the user that appears in the CxSAST web interface for confirmation by the Company Manager, SP Manager, or Server Manager. Upon confirmation, the user is notified by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

To sign up for a user account:

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



In the Create Account window, fill in the personal details. The E-mail will be used as the user name for login.



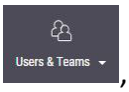
■ The required password complexity is as follows:

- 9 to 400 characters
- At least 1 uppercase letter
- At least 1 lower case letter
- At least 1 special character
- At least 1 digit

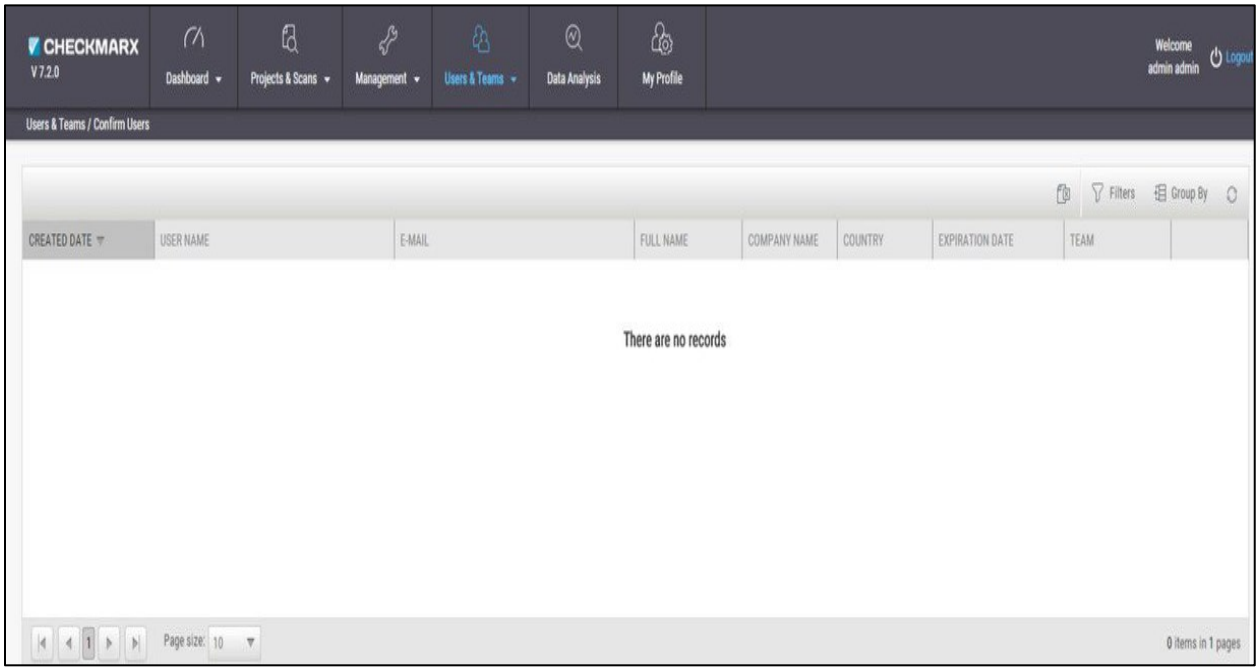
Type the captcha text, and click **Submit**.

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

To confirm a user account:

In **Users & Teams** 

, select **Confirm Users**. The Confirm Users window is displayed.



In the table, select the user account request to be confirmed.

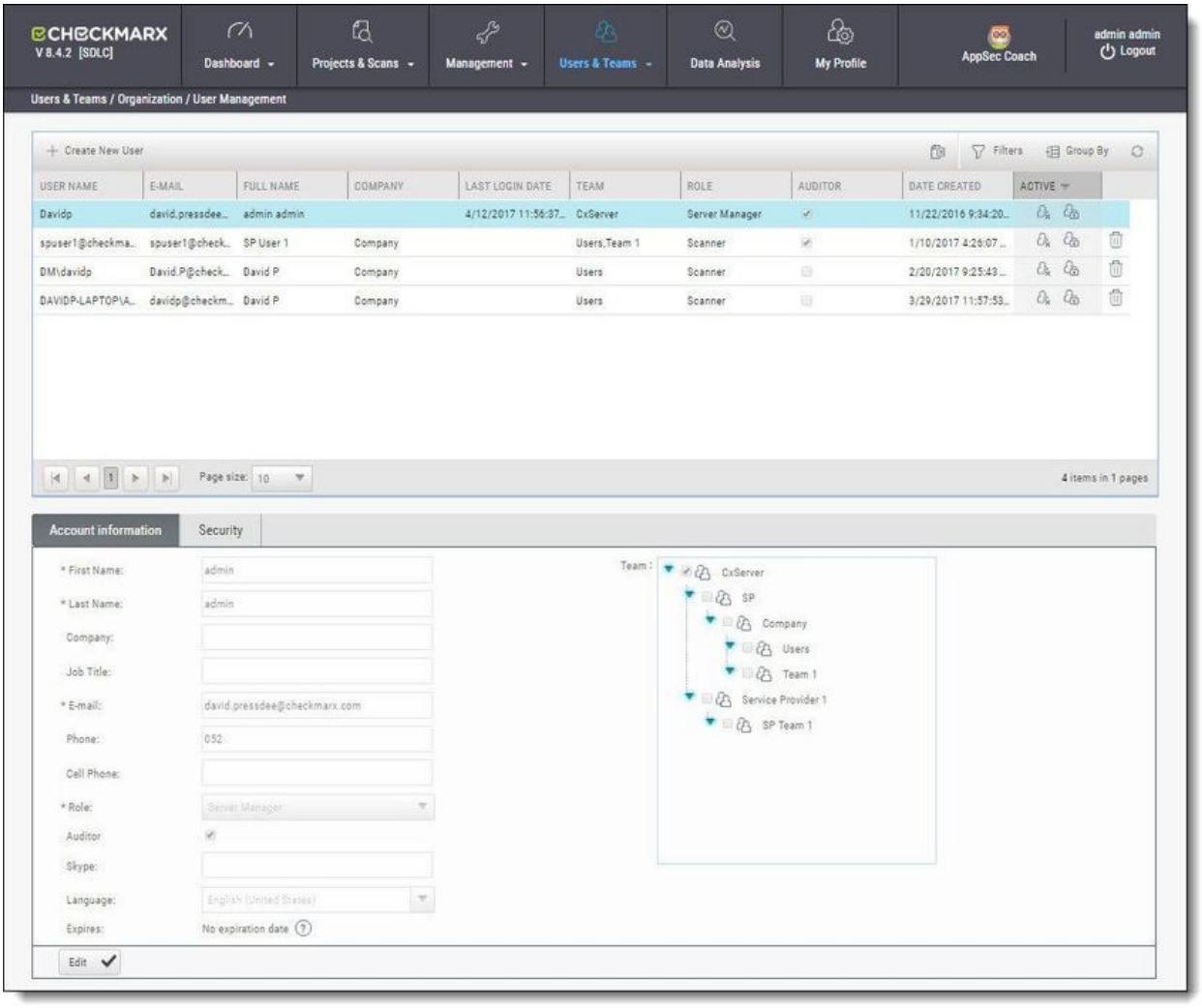
You can view additional information about the user by hovering over the  . You can delete the request.

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

Click  to confirm the request.

Managing Existing Users

Open **Users & Teams > Organization > User Management**, the following window is displayed.



You can export the existing user list as a CSV file , use the filter tool to search for a specific user, separate users into groups as well as refresh the current view.

To change a user's group (Team, Company, or SP) membership and/or Role:

Select the user in the table to display below the table their personal **User Details**.

Below the User Details, click **Edit**.

Select the desired group: SP, Company, or Team.

Select the appropriate Role for the desired level of authorization. Click **Update**.

In the table, Server, SP, and Company Managers can deactivate users (). Only Server Manager (admin) users can reset passwords ().

Users can edit some of their own details from the Update Profile menu (see *Getting to know the System Dashboard*).

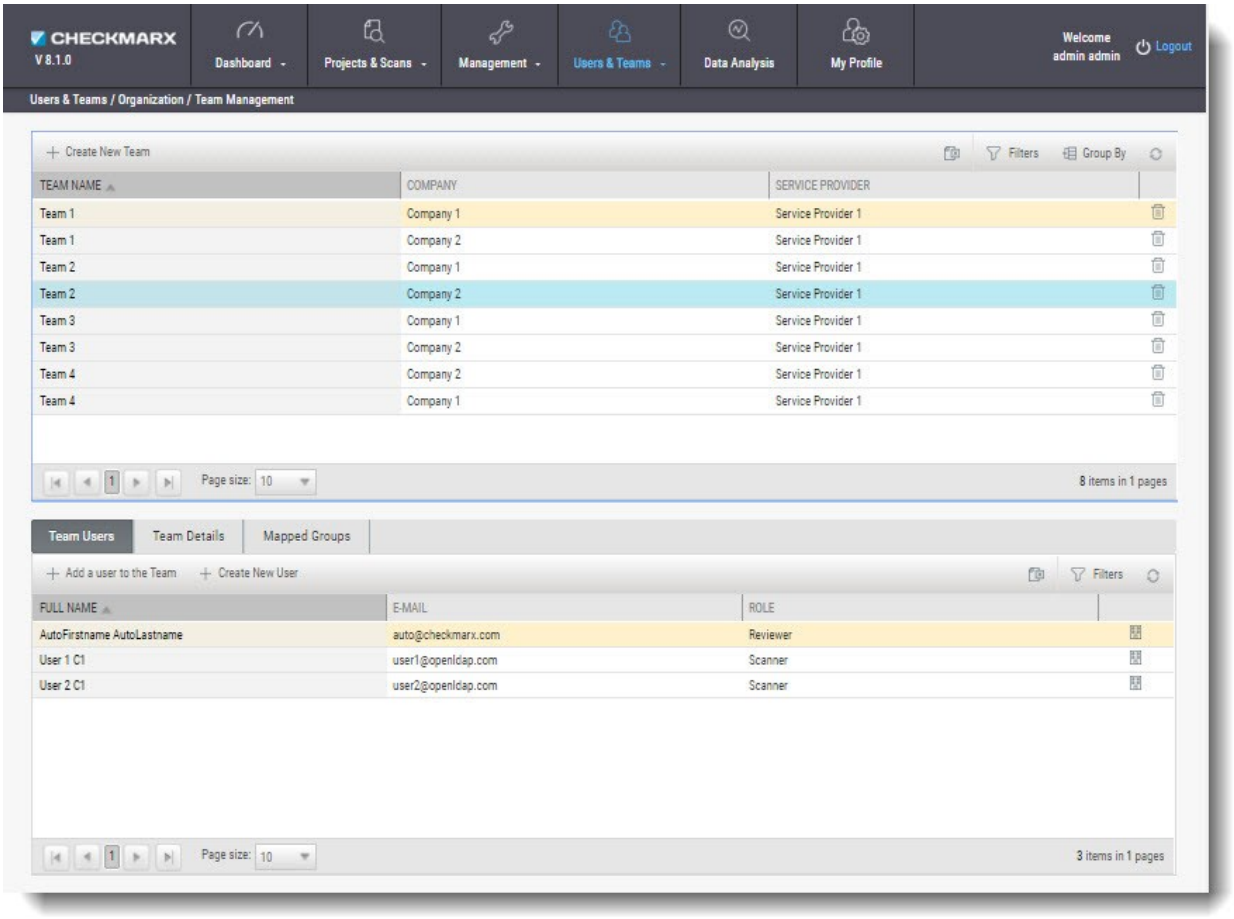
Parameters in the Security tab can be used to restrict user access by IP address (IP security is currently limited to admin users only).

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 and 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:

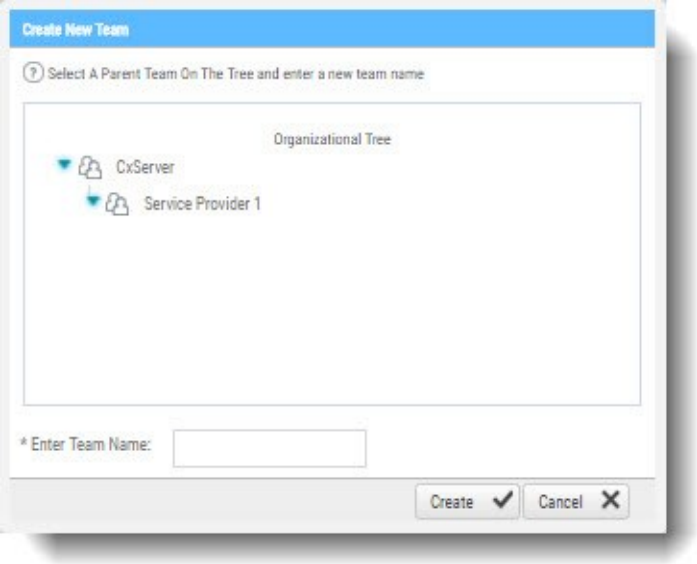
Go to **Users & Teams > Organization > Team Management**, the Team Management window is displayed.



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.

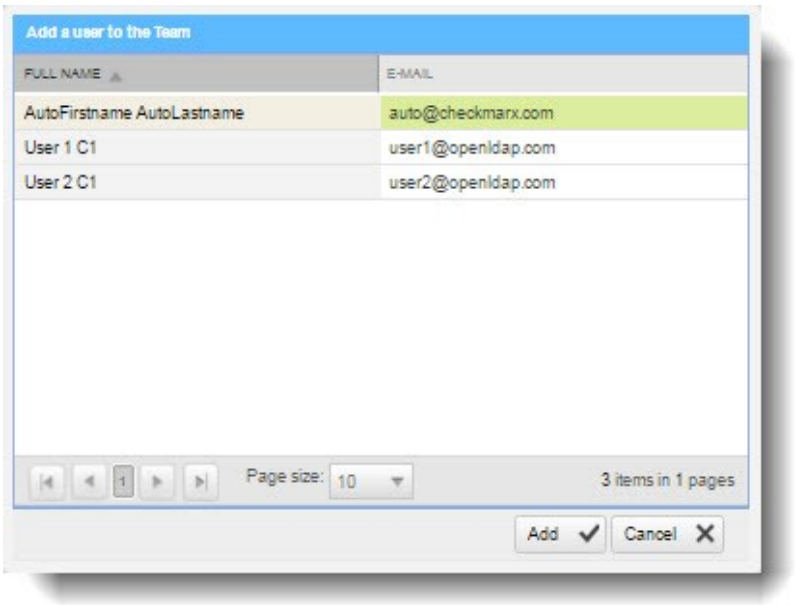
You can now add User to the Team.

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.

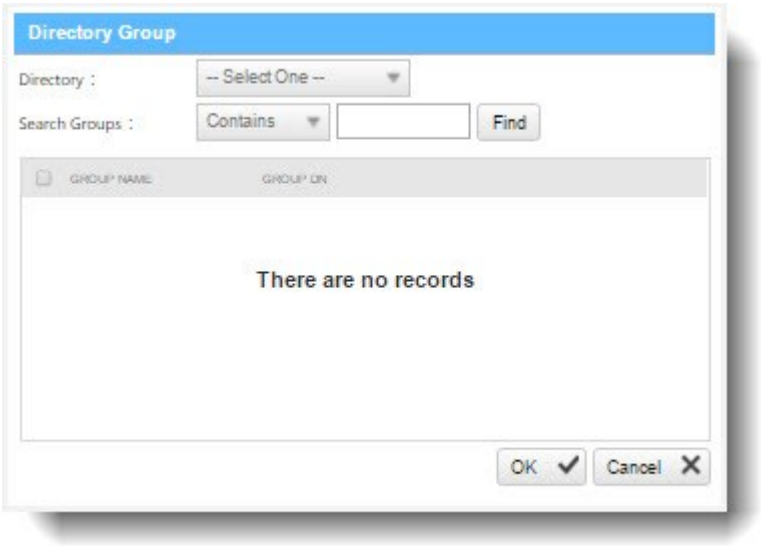
Mapping LDAP Directory User Groups to CxSAST Teams

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*).

Changing SAML User Teams and Roles in the CxSAST

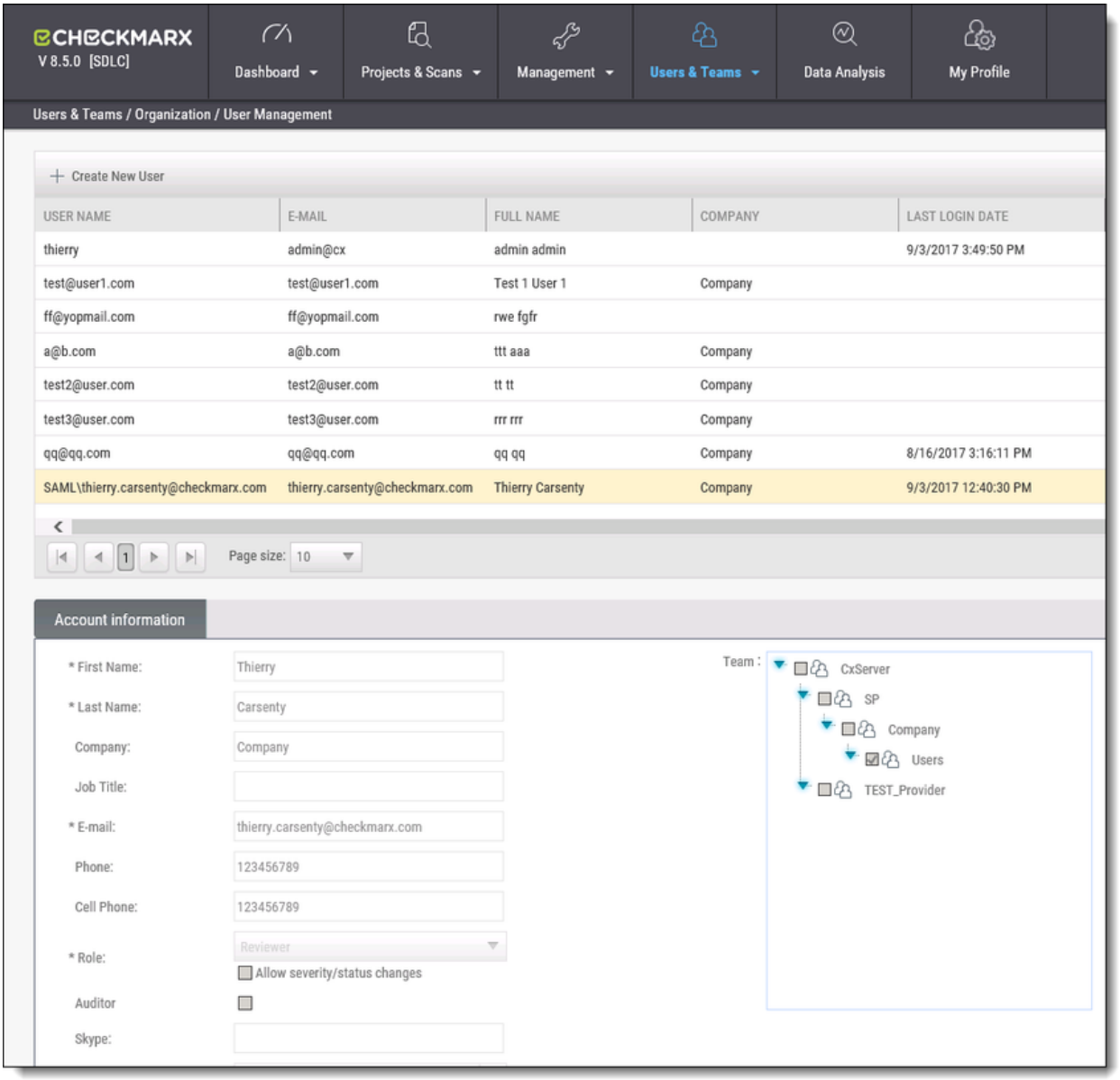
If the IdP Authentication method is used, SAML users' will be defined according to their predefined attributes in the SAML IdP. This means that the team and the role are setup automatically in CxSAST according to the definitions in the SAML IdP and this step is not required.

If the Manual Authentication method is used (default), SAML users' will be defined upon login according to the default settings in CxSAST (either a scanner or reviewer). You can, if required, change a logged in user's Team and Role from the User Management.

- When SAML is enabled, SAML users do not need to be added manually by the Cx admin; they are able to automatically log in once the SAML login is available and attributed to the roles as per this page.

To change a SAML User's Team and Role in the CxSAST:

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



■ Once logged in to CxSAST, all SAML users are shown in the **User Management** screen with 'SAML\' preceding their User Name (e.g. SAML\david.press@checkmarx.com).

Select a **SAML User** from the **User List** and click **Edit**.

Update the **Team** and **Role** accordingly and then click **Update** to confirm the change.

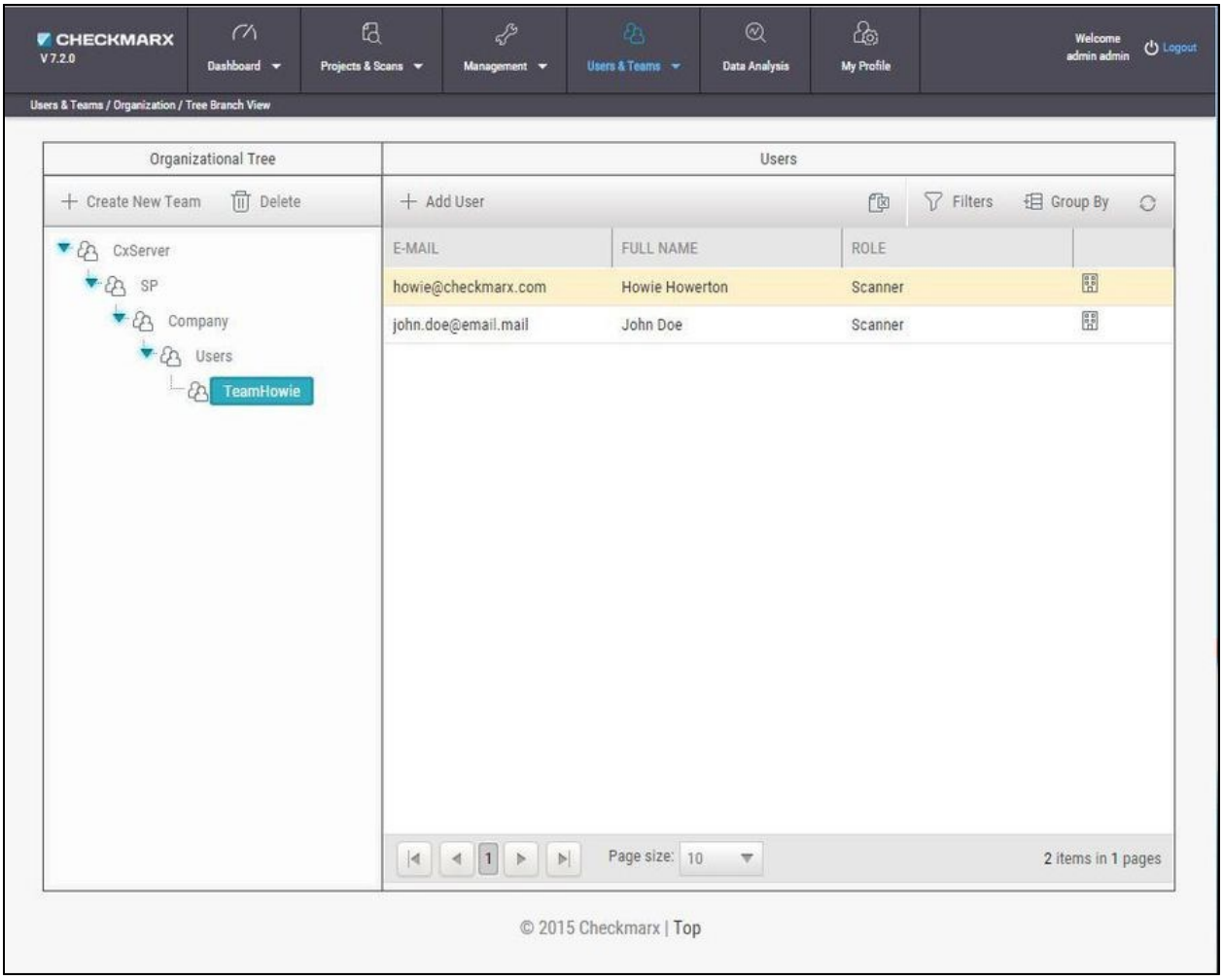
Managing the Organizational Hierarchy

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

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

Tree Branch View

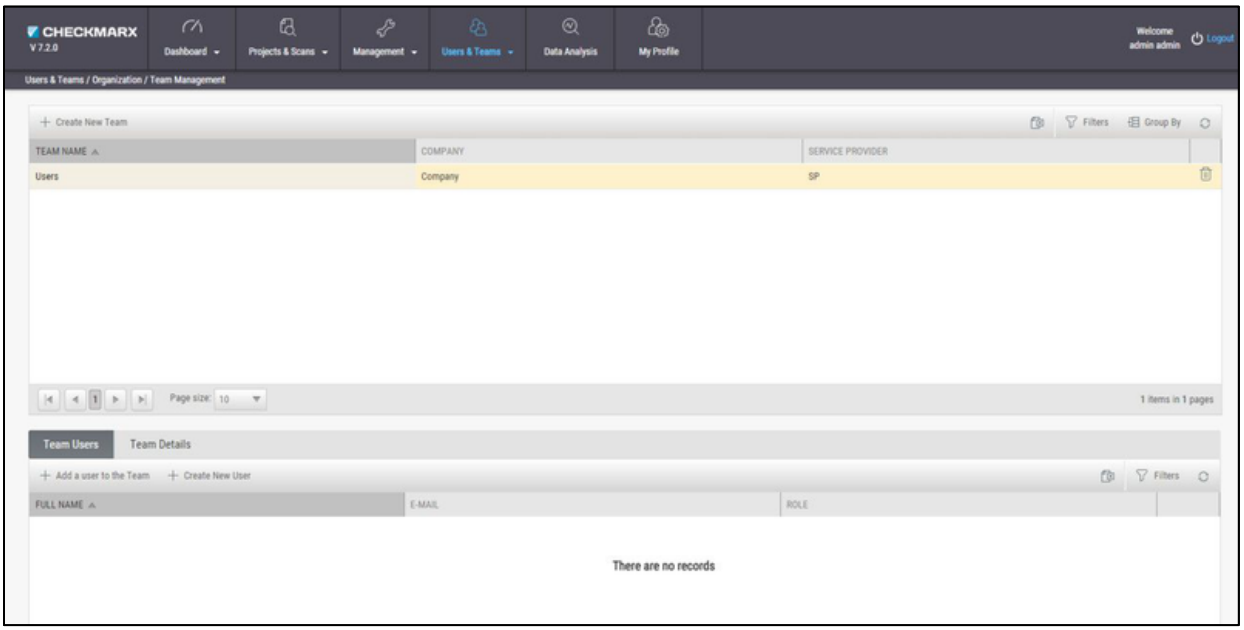
Tree Branch View provides a high-level view of the organizational hierarchy.



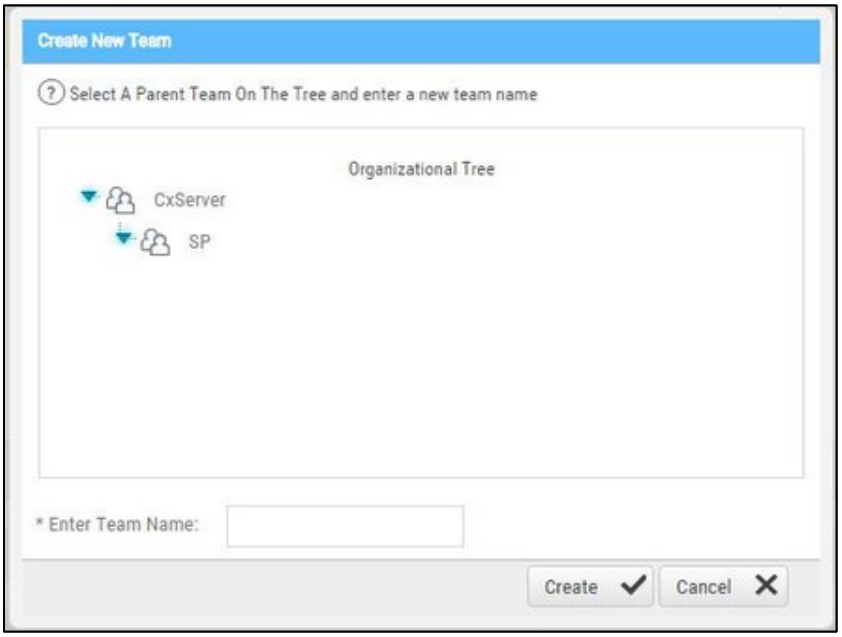
In Tree Branch View, you can + Create New Team under the selected one. You can + Add User to a Team. You can also drag any team to move it under a different Company or Team (to become a child Team). All the Team's relevant child teams, users, projects, scans, and queries will be moved along with it.

Team Management

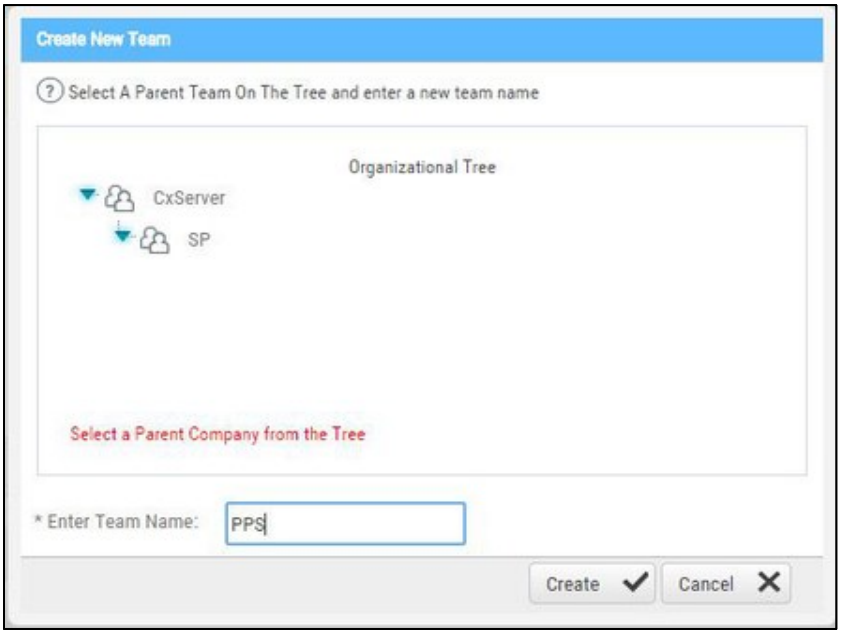
Manage various levels of Teams (Teams, Companies, and Service Providers - SPs) in **Team Management**.



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.

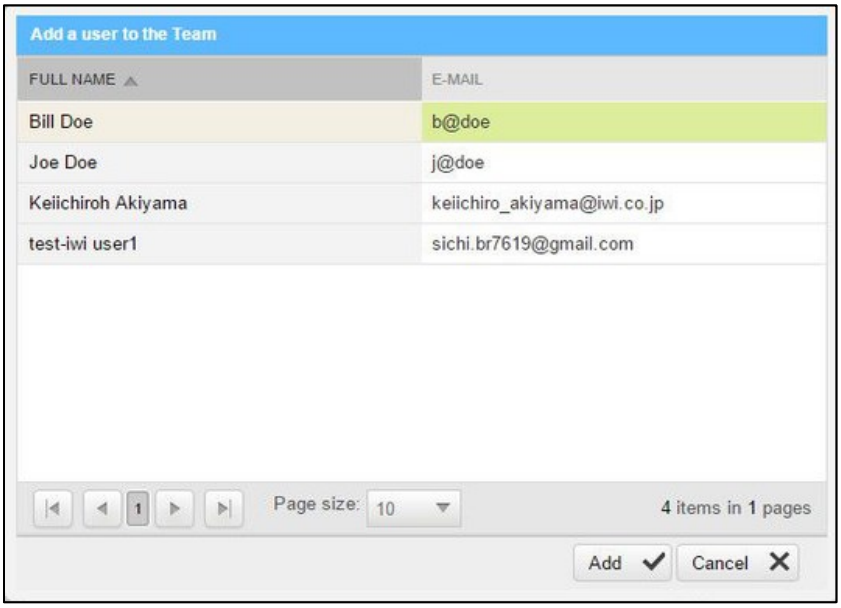


Select a parent group, and type a name for the new group, and click **Create.**



In the Team Management window, click 

to add a new user to the Team. The Add a user to the Team window is displayed.

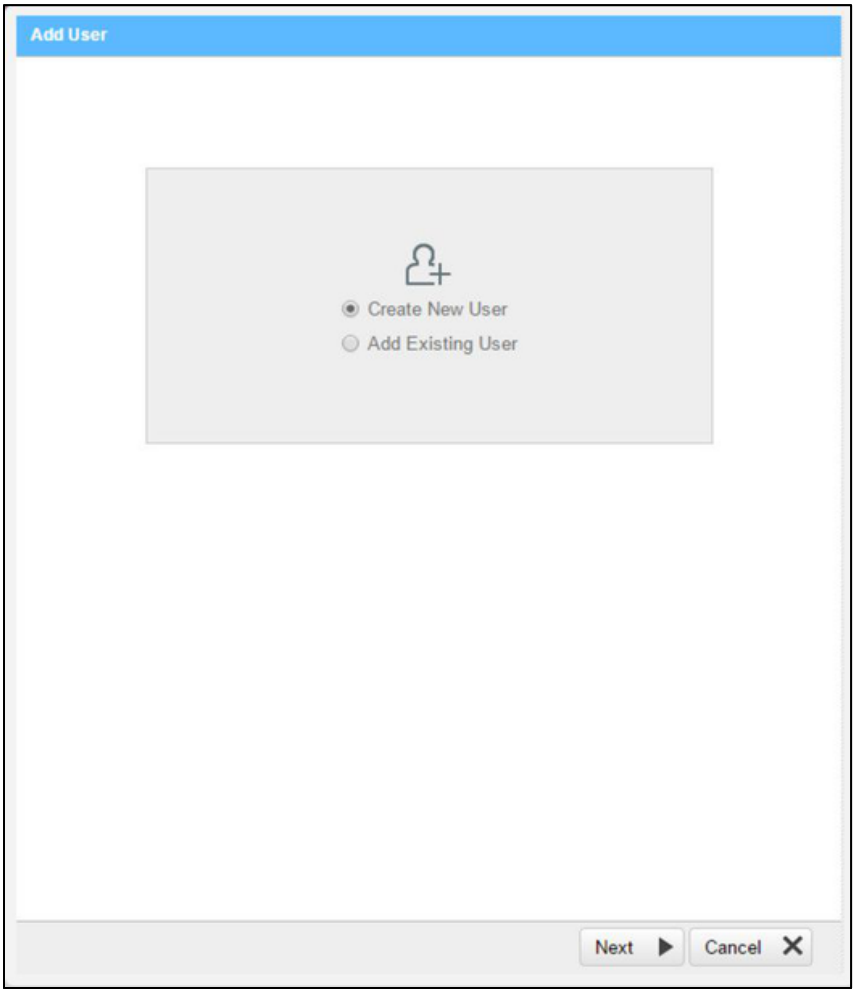


Select a user and click **Add**. The Team member will be added in the Team Users tab.

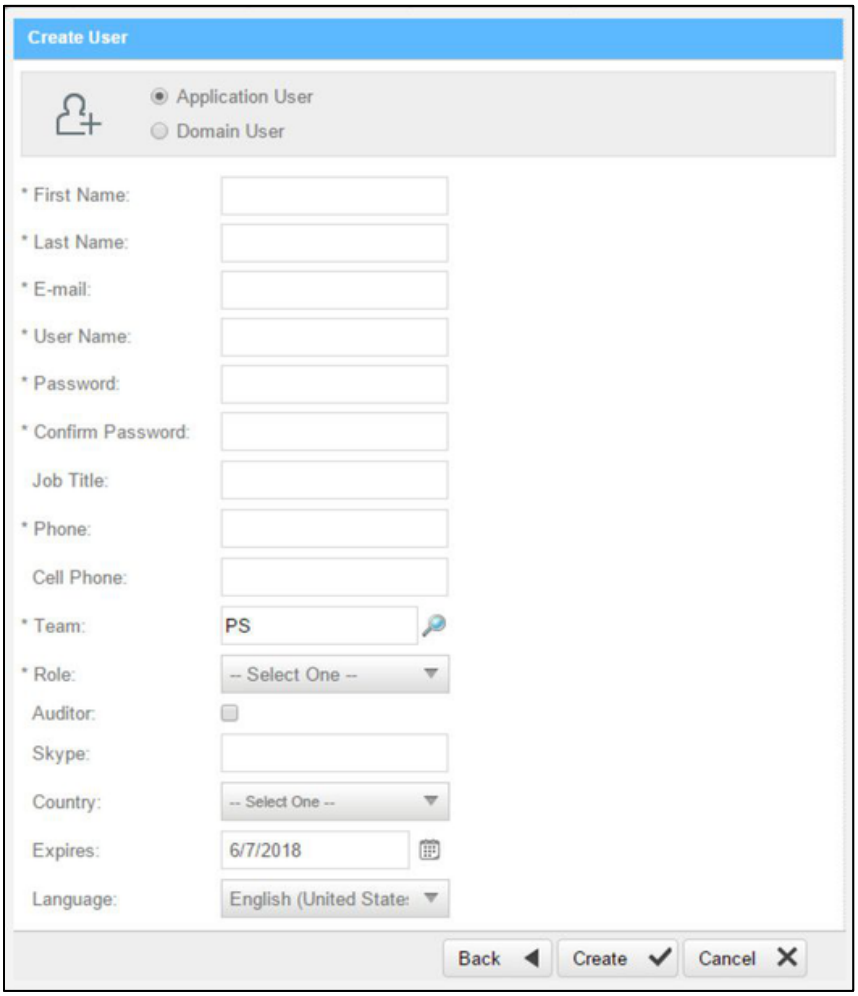
Note: Once the team member has been added to the Team User window they will no longer appear on the list as they can only be added once.

To create a new user, click 

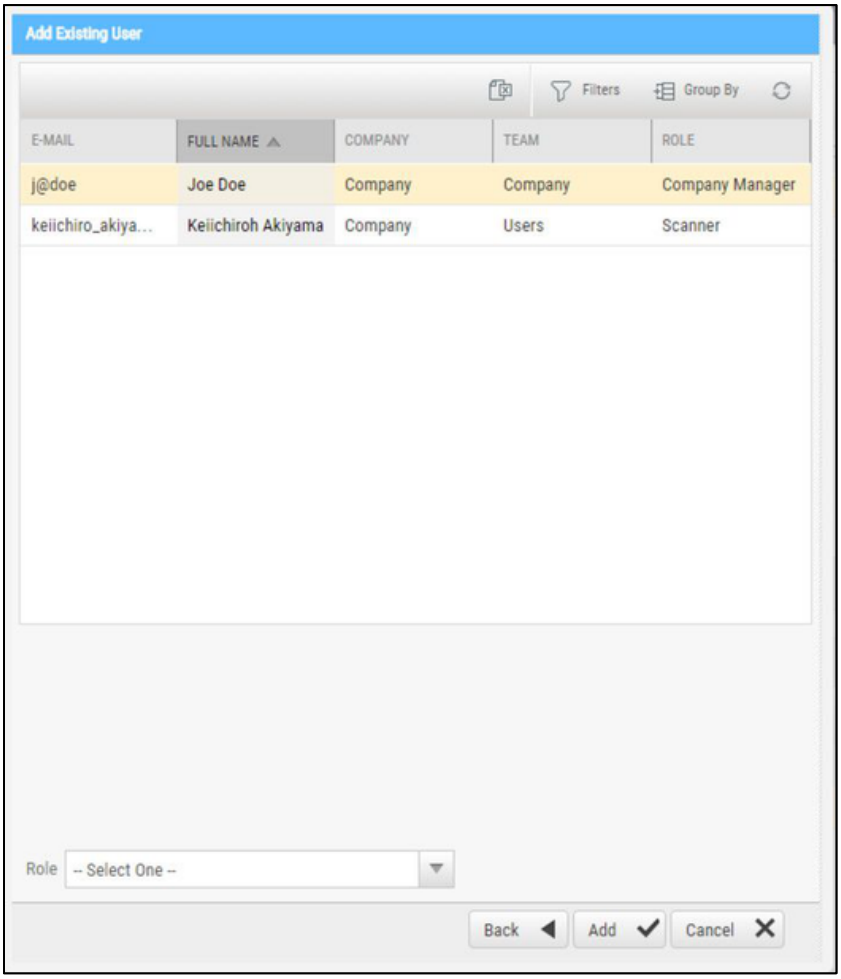
. The following window is displayed:



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:

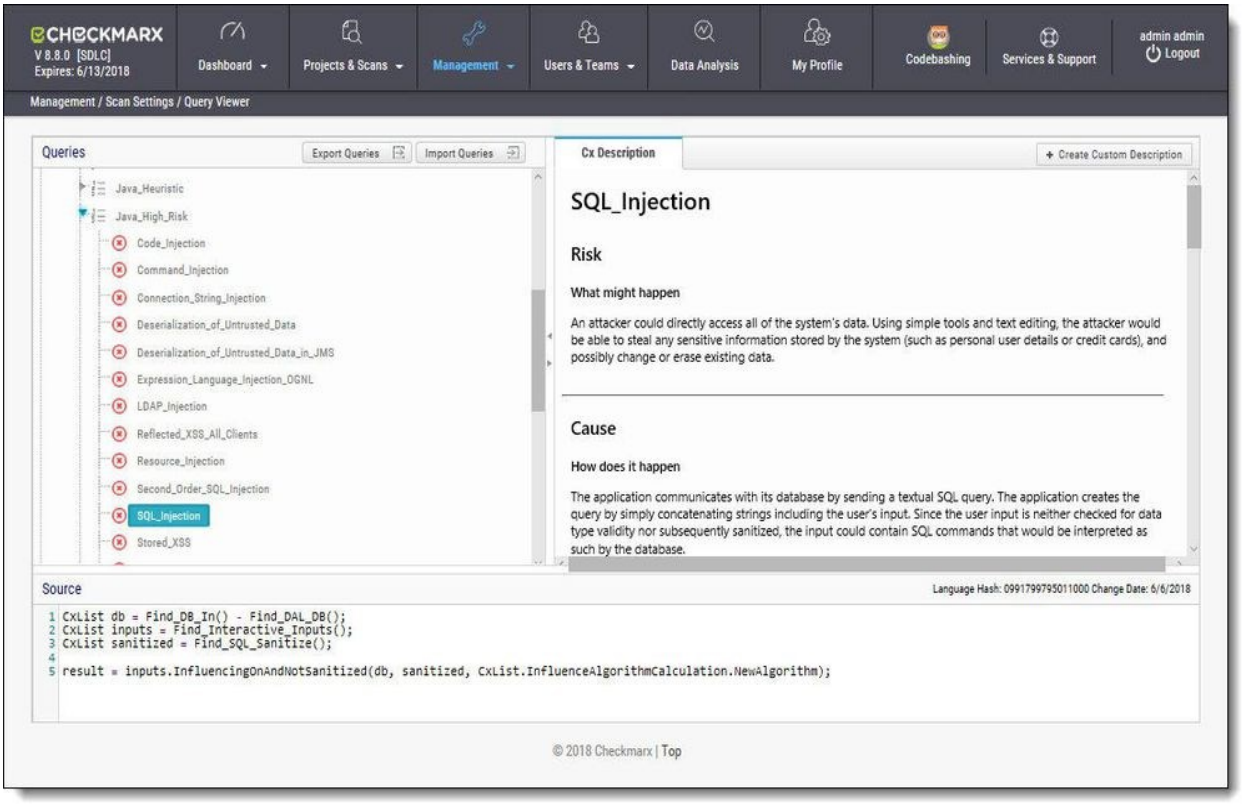
Scan Settings

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.



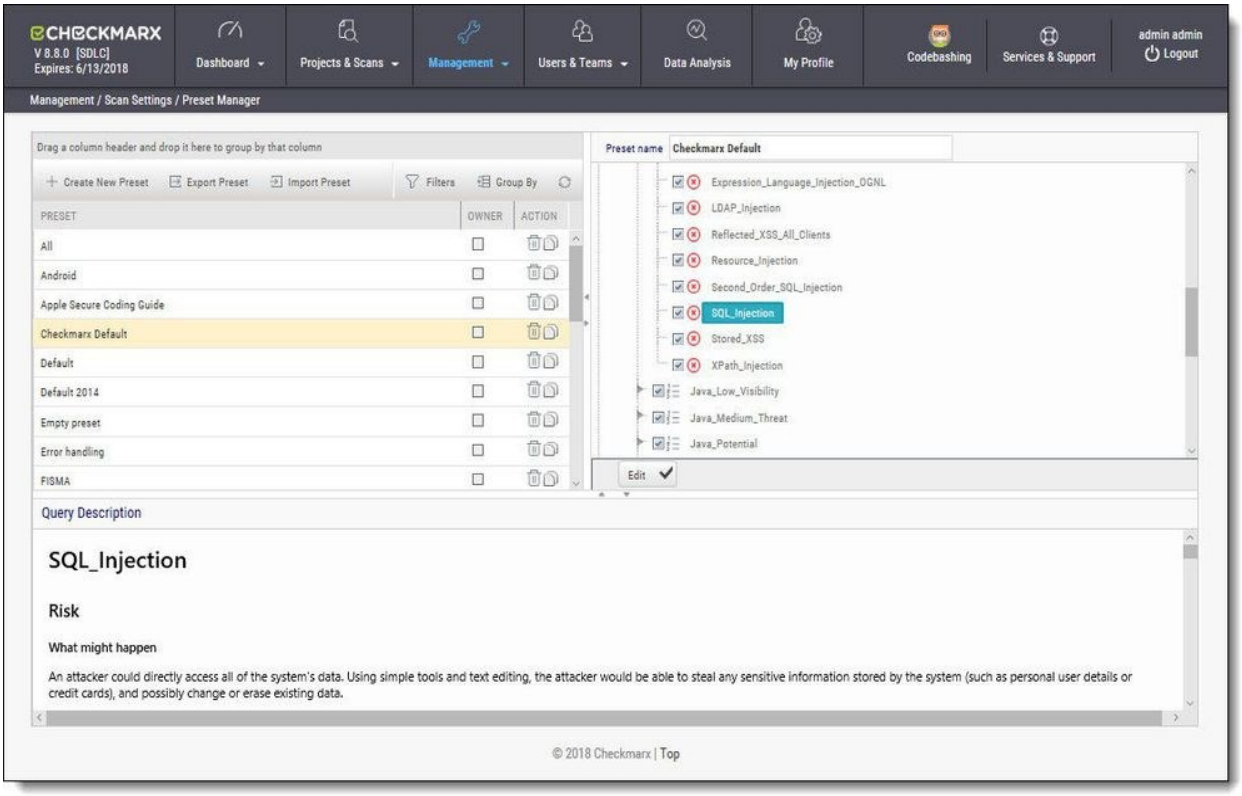
Select a **Query** in the **Queries** pane. A description is provided in the **Description** pane with a full explanation of the risk. The source code for the query is displayed in the **Source** pane at the bottom of the window.

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.

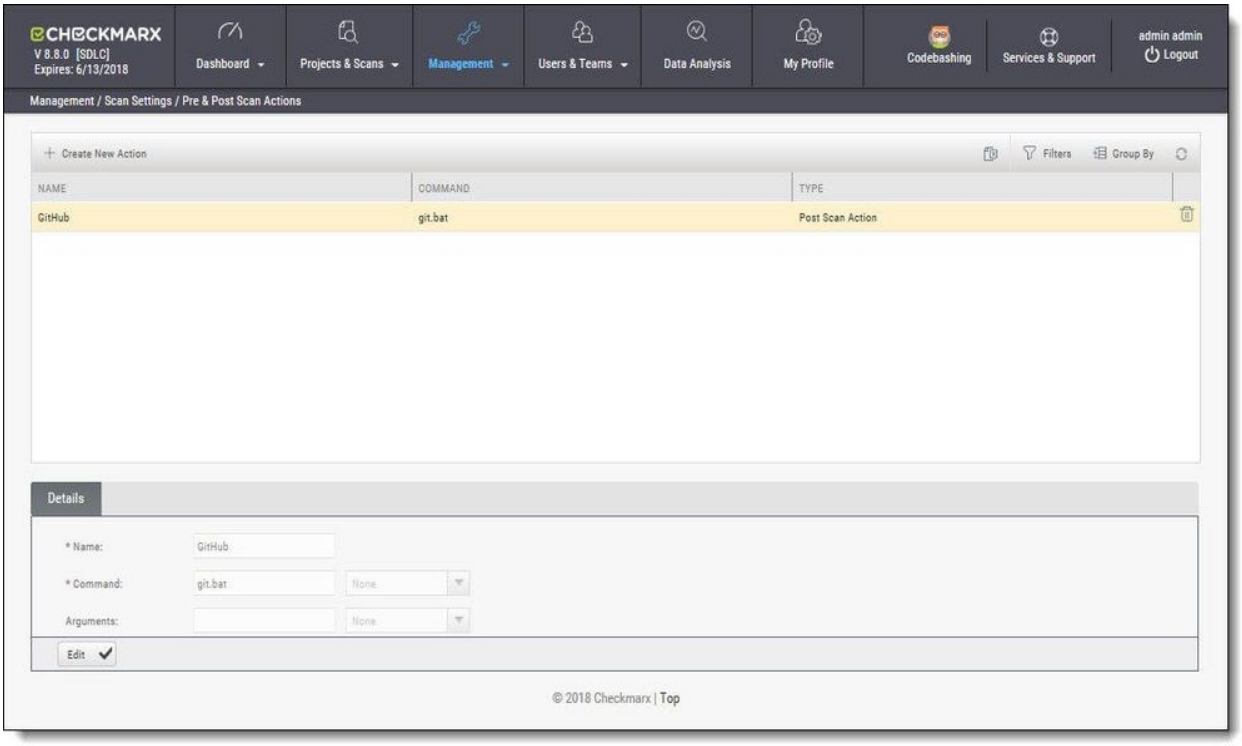
Click **Create New Preset** to create a new preset.

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.

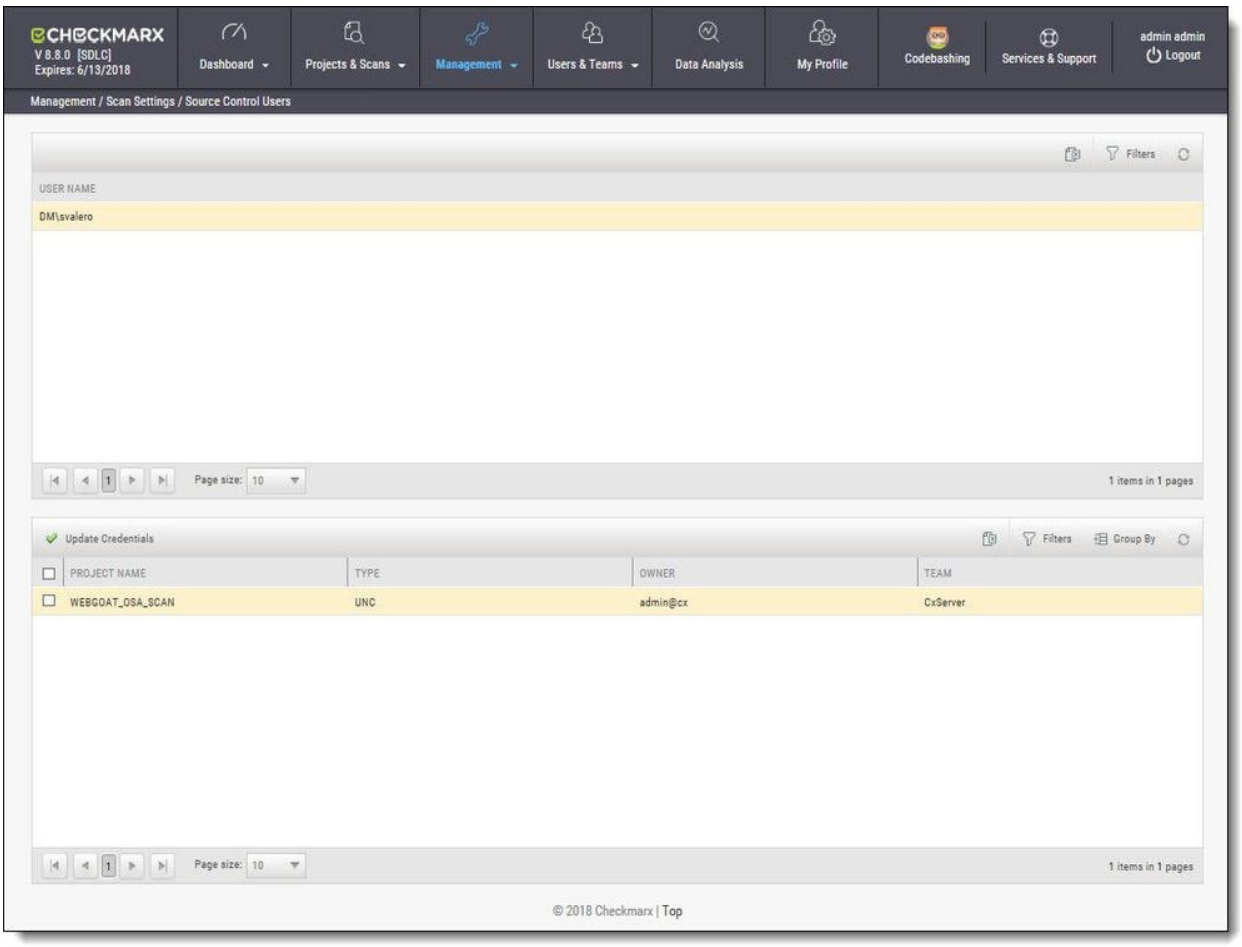
Click **Edit** to update the selected action details.

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.

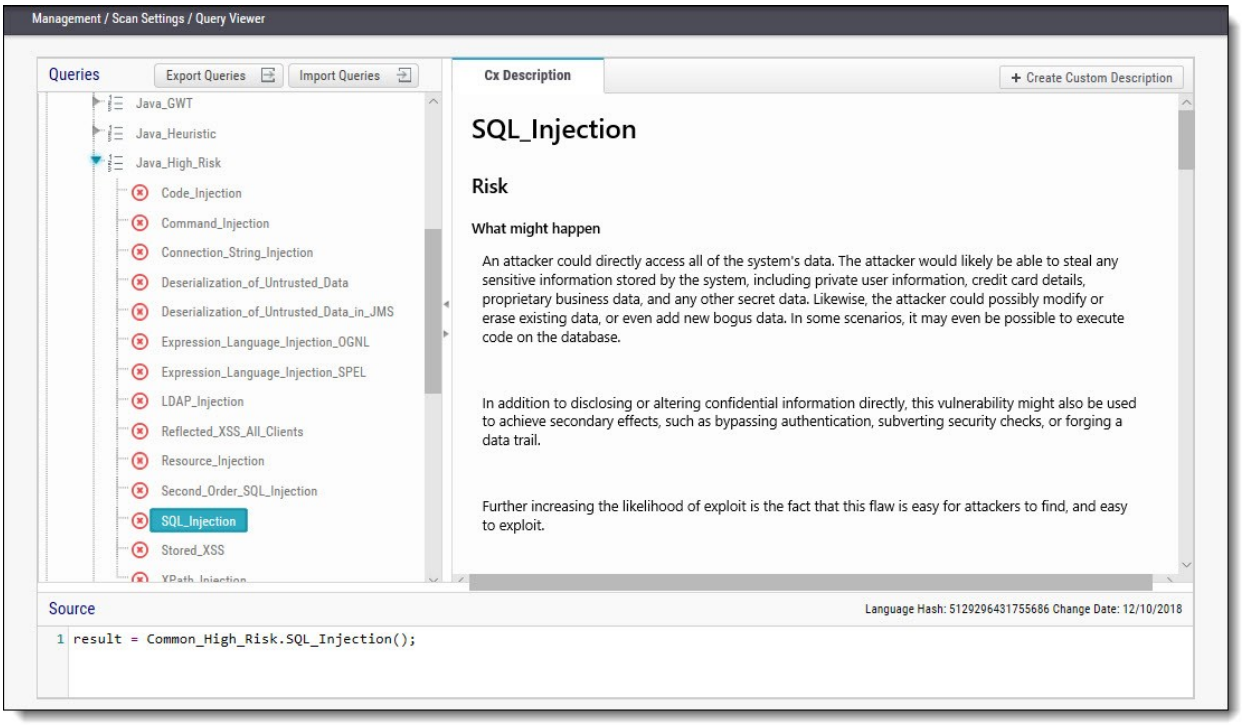
Click **Update Credentials** to update the selected user credentials.

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

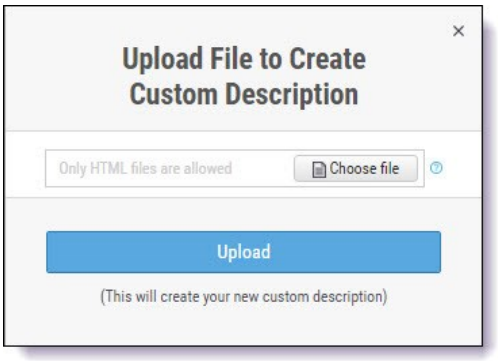
You can create a Custom Description to best suit your own organizations procedures and best practices.

- 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.



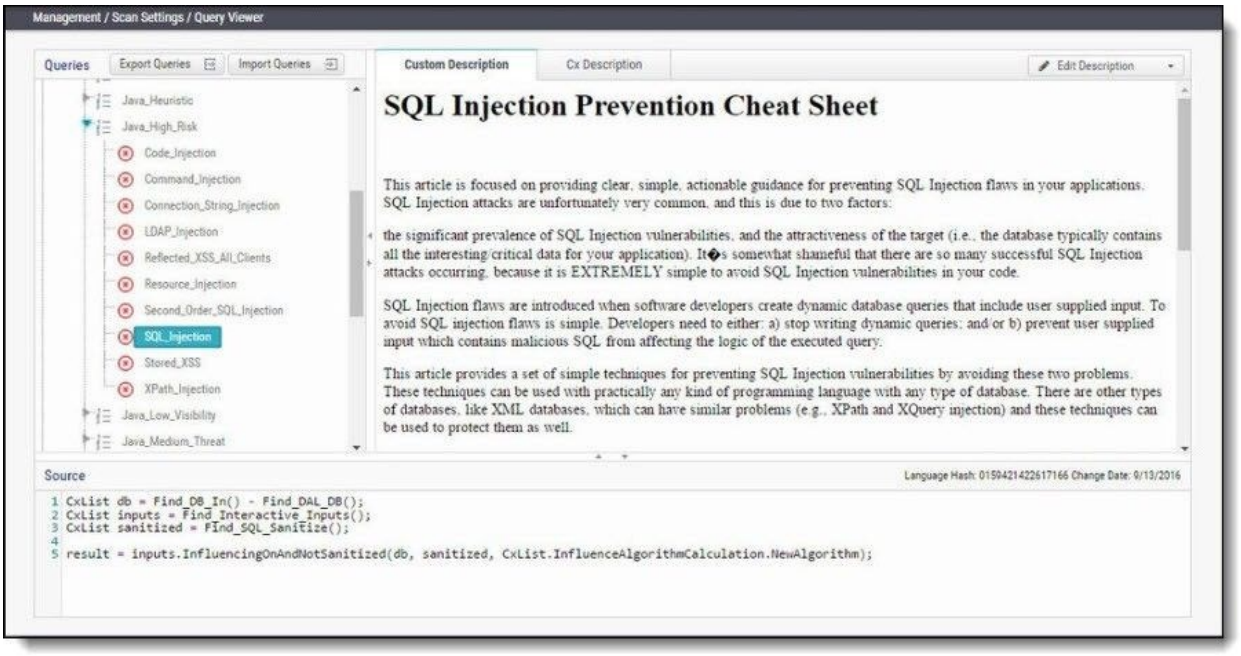
Click **Choose File,** navigate to the custom description file (.HTML) and click **Open**.

■ 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.



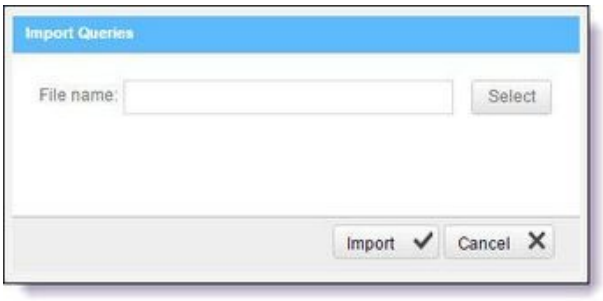
You can replace or delete the custom description by clicking **Edit Description** and selecting **Update Description** or **Delete Description** accordingly.

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.



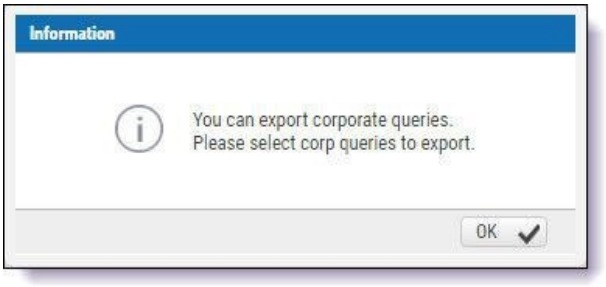
Click **Import,** navigate to the query file (.XML) and click **Open**. The query is displayed in the **Queries** pane.

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.



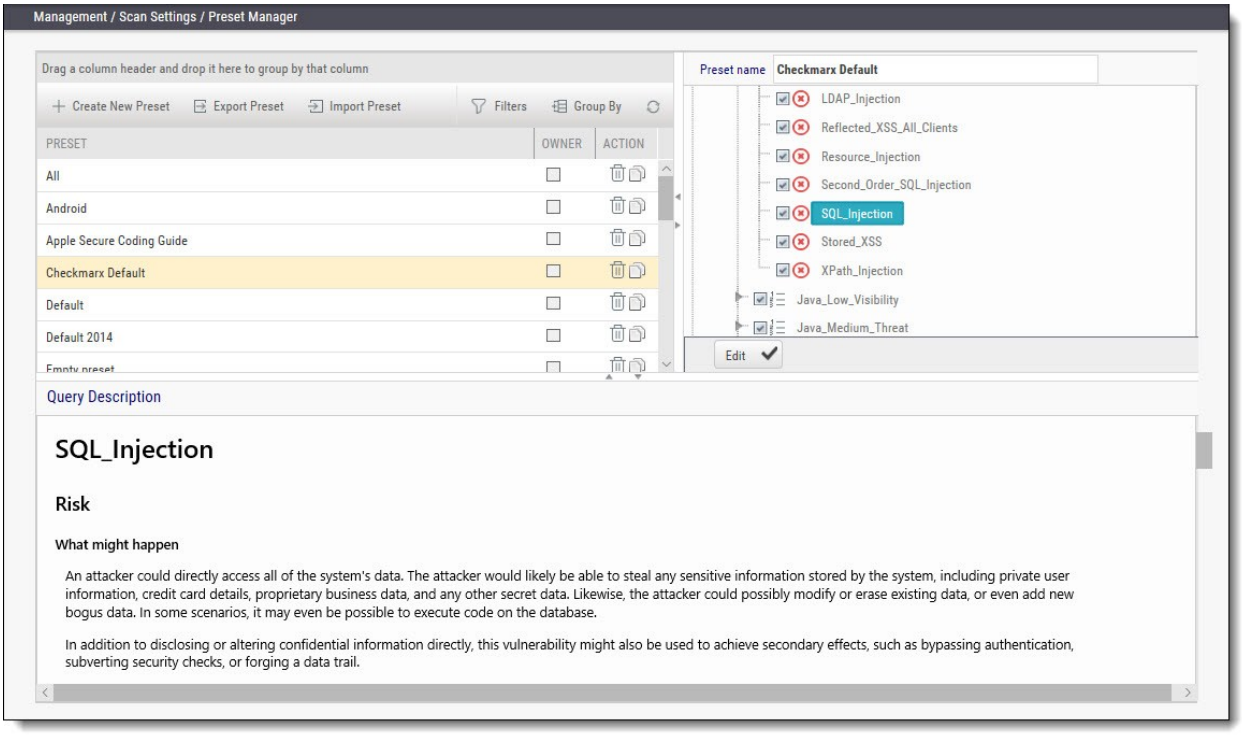
Click **OK**.

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.

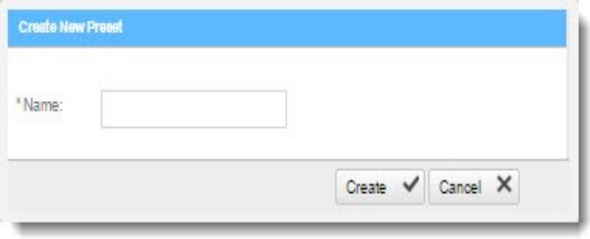


- You can quickly create a new preset based on an existing one (duplicate) by selecting a Preset from the Preset pane and clicking  .

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.

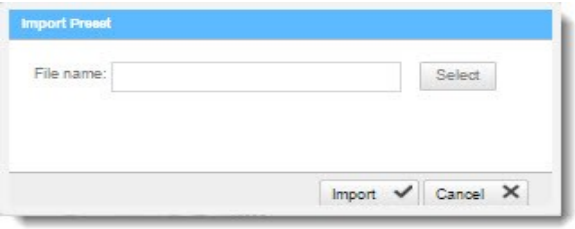
> ■ You can edit a single language, such as Java, selecting and deselecting the queries as needed, and then press Synchronize in order for all related queries in all languages to be selected.

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, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
Android	For Android related application security risks	Groovy, Java and Kotlin coding languages
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, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
Default	Default preset (soon to be discontinued)	Apex, ASP, CPP, CSharp, Groovy, Java, JavaScript, ObjectiveC, 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....
FISMA	For homeland security application risks according to the 'Federal Information Security Modernization Act' compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
High and Medium	For high and medium related application security risks	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
High, Medium and Low	For high, medium and low related application security risks	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, 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, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Typescript, VB6, VbNet and VbScript coding languages
JSSEC	For Android related application security risks according to the JSSEC (Japan's Smartphone Security Association) compliance guidelines	Groovy and Java coding languages
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, Groovy, Java, JavaScript, Kotlin and ObjectiveC coding languages

Preset	Usage	Includes vulnerability queries for....
NIST	For the application security risks according to the 'National Institute of Standards and Technology' compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript 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, Groovy, Java, JavaScript, Kotlin and ObjectiveC coding languages
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, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Typescript, 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, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
OWASP TOP 10-2017	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2017	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, 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, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet, and VbScript coding languages

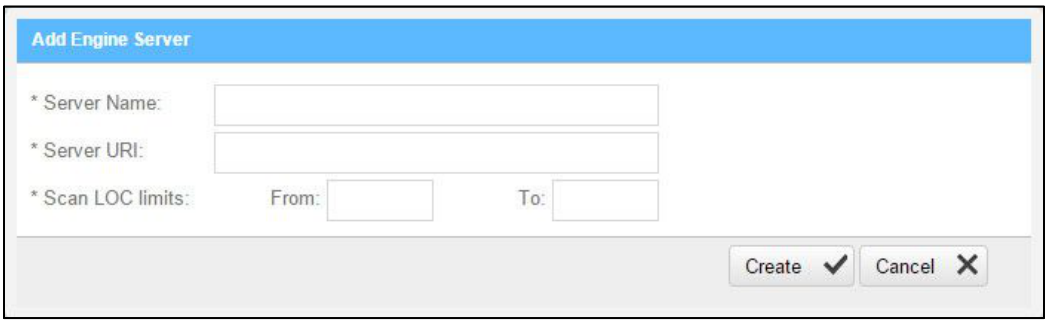
Preset	Usage	Includes vulnerability queries for....
SANS Top 25	For the top 25 web application security risks according the SANS Technology Institute's compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet 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
XSS and SQLi only	Recommended best practice when starting to scan a new project in order to focus on the most important vulnerabilities first.	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala VB6, VbNet and VbScript coding languages

Limiting Engine Scans

To Limit Engine Scans:

In **Management > Server Setting > Installation Information**, click 

.
The Add Engine Server window is displayed.

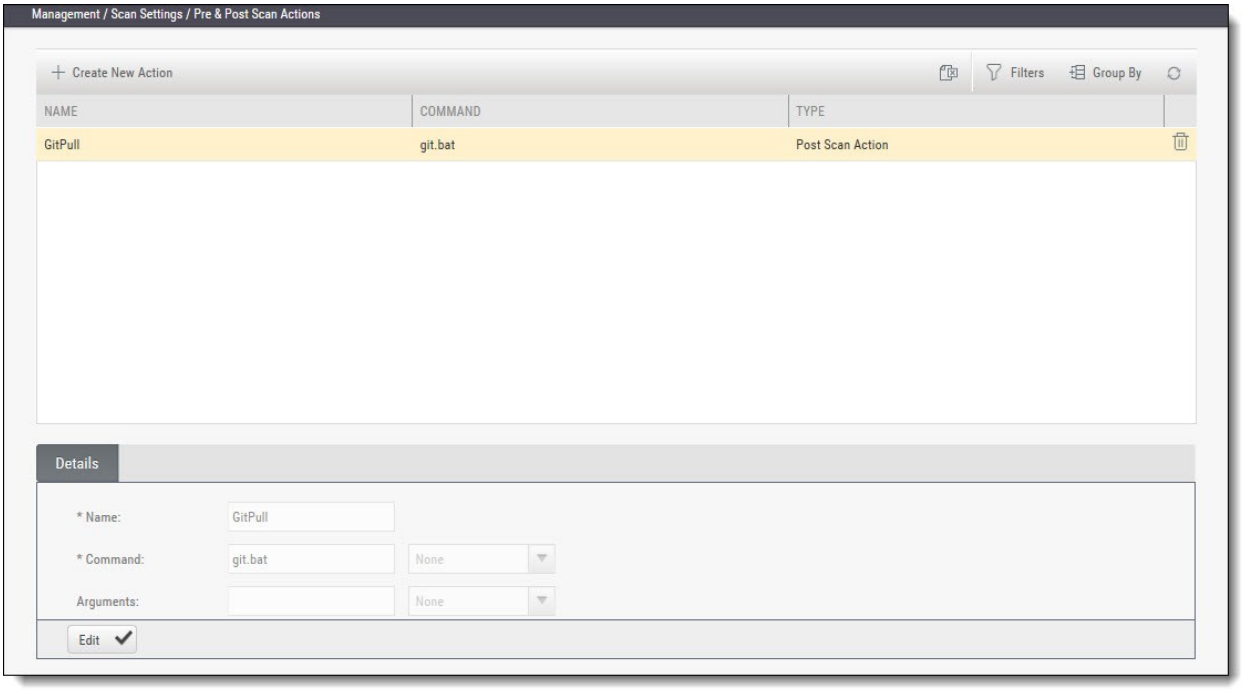


The Adding Engine Server window includes the following properties:

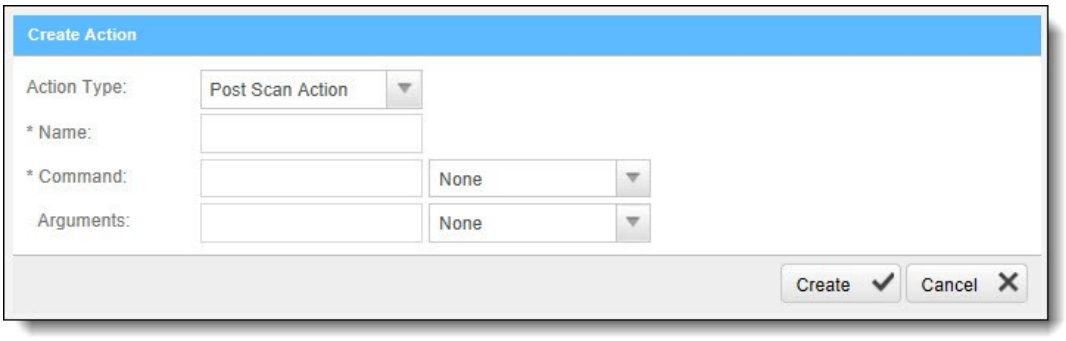
- **Server Name**: The name of the server you are appointing as Engine Server
- **Server URI**: The address of the server
- **Scan LOC limits**: The Scan limits is not a mandatory field, in the event the fields are left empty assume the value From to include: All to: All. Define the lower and higher 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.

Configuring Pre & Post Scan Action

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



Click Create New Action. The Create Action window is displayed.



Configure the following parameters:

- Action Type - select Pre-scan Action / Post Scan Action
- Name - enter the Pre/Post scan Action name
- Command - enter the command (e.g. pull batch file's exact name)
- Arguments - leave empty

Click Create and Finish.

Connection Settings.

In this section:

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

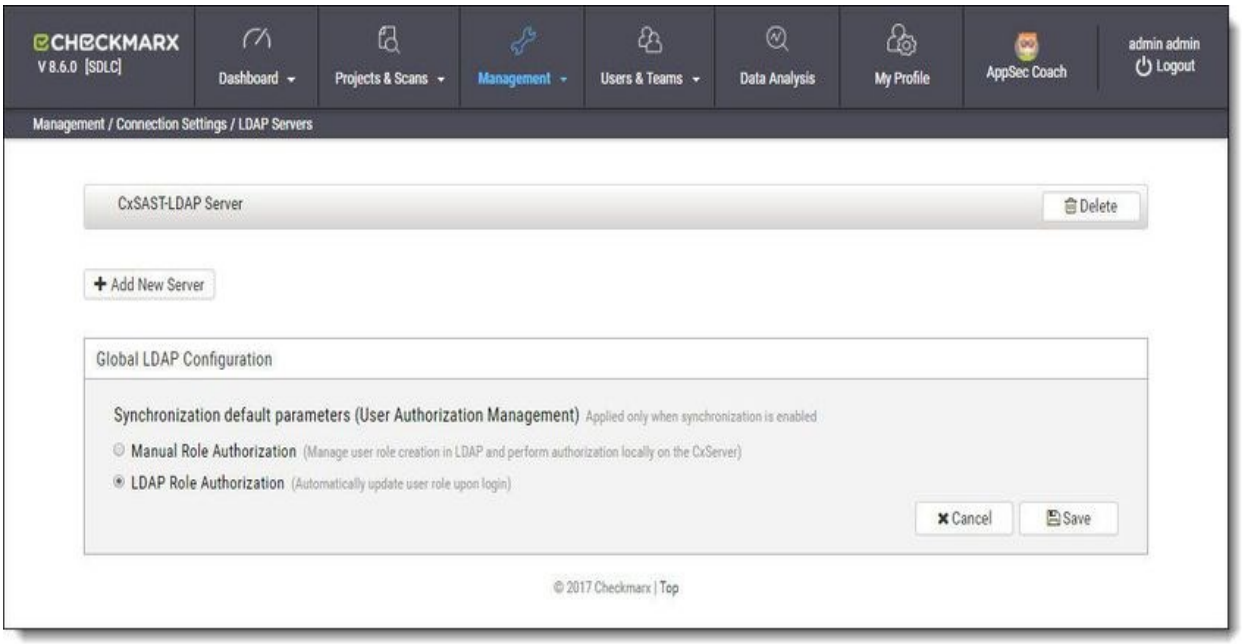
LDAP Management

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.



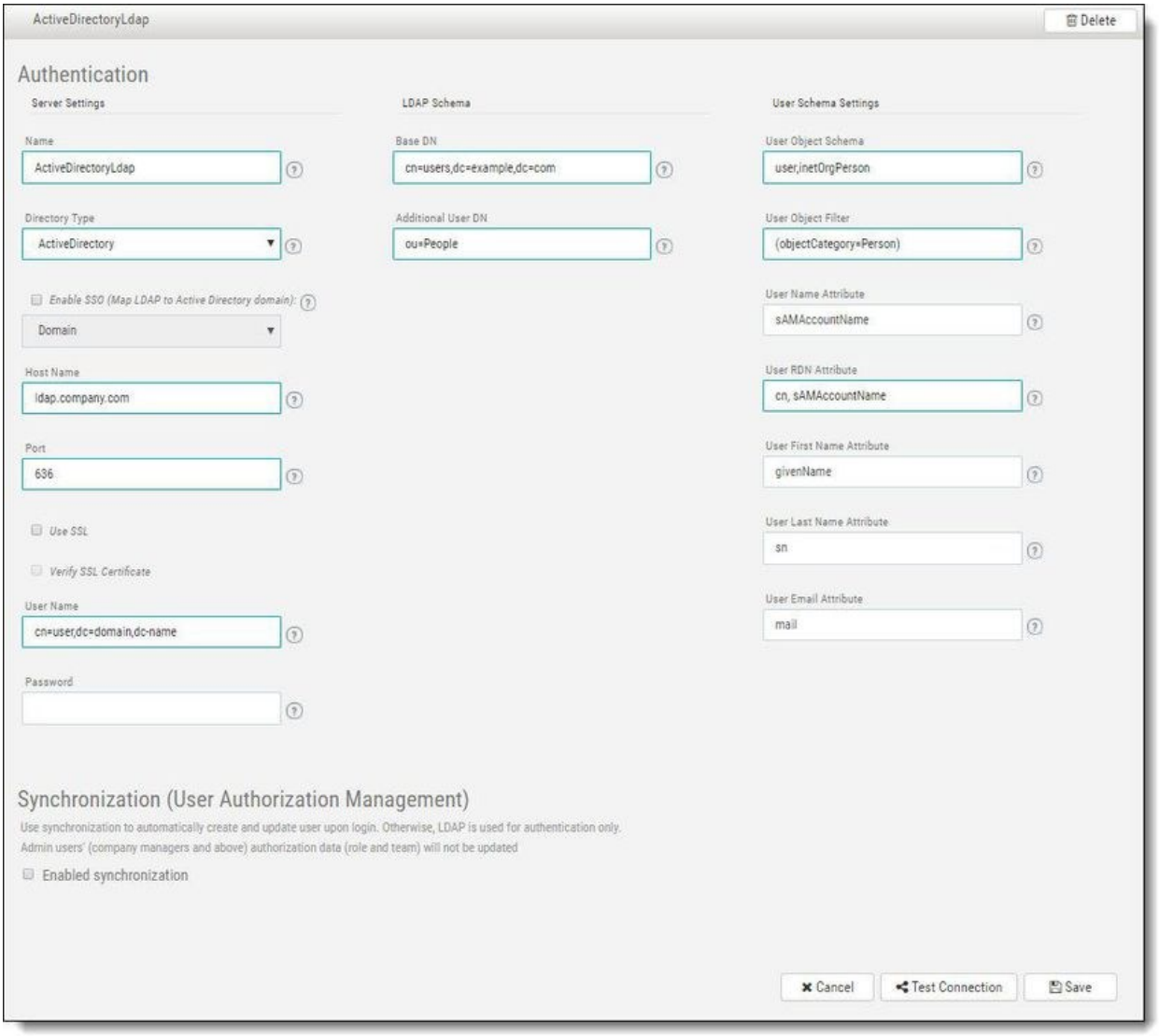
Click + **Add New Server**. The LDAP Server Authentication window is displayed (see *Defining LDAP Authentication Settings*, below).

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

Configuring LDAP Authentication Settings

To configure LDAP Authentication settings:

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



Define the following Authentication parameters:

Parameter	Description
Name	Server name
Directory Type	Provides auto selection for server parameters according to default settings (ActiveDirectory, OpenLDAP, or LDAP Server) • **Enable SSO (Map LDAP to Directory Domain)** - Selecting this option ensures that SSO users are automatically created upon login and synchronized as LDAP users • **Domain** - Select the relevant domain for this LDAP configuration. **NOTE:** SSO and domain selection is only enabled for ActiveDirectory users.
Host Name	LDAP server hostname (e.g. ldap.company.com)
Port	Port of the LDAP server (e.g. 389, 636 (for SSL)) • **Use SSL** - Selecting this option ensures that all information passed between the server and the client remains private • **Verify SSL Certificate** - Selecting this option ensures SSL certificate verification
User Name	Name of the user that the application uses when connecting to the LDAP server (e.g. user@domain.name or cn=user,dc=domain,dc=name) **NOTE:** 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
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 Object Schema	LDAP user object class type to use when loading users (e.g. user, inetOrgPerson)

Parameter	Description
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 user first name (e.g. givenName)
User Last Name Attribute	Attribute field to use when loading the user last name (e.g. sn)
User Email Attribute	Attribute field to use when loading the user email (e.g. mail)

Click **Save** to save the changes.

Click **Test Connection**.

■ Note that you can save the LDAP settings without having to perform and validate the connection test first. Validating the connection can be performed at a later stage.

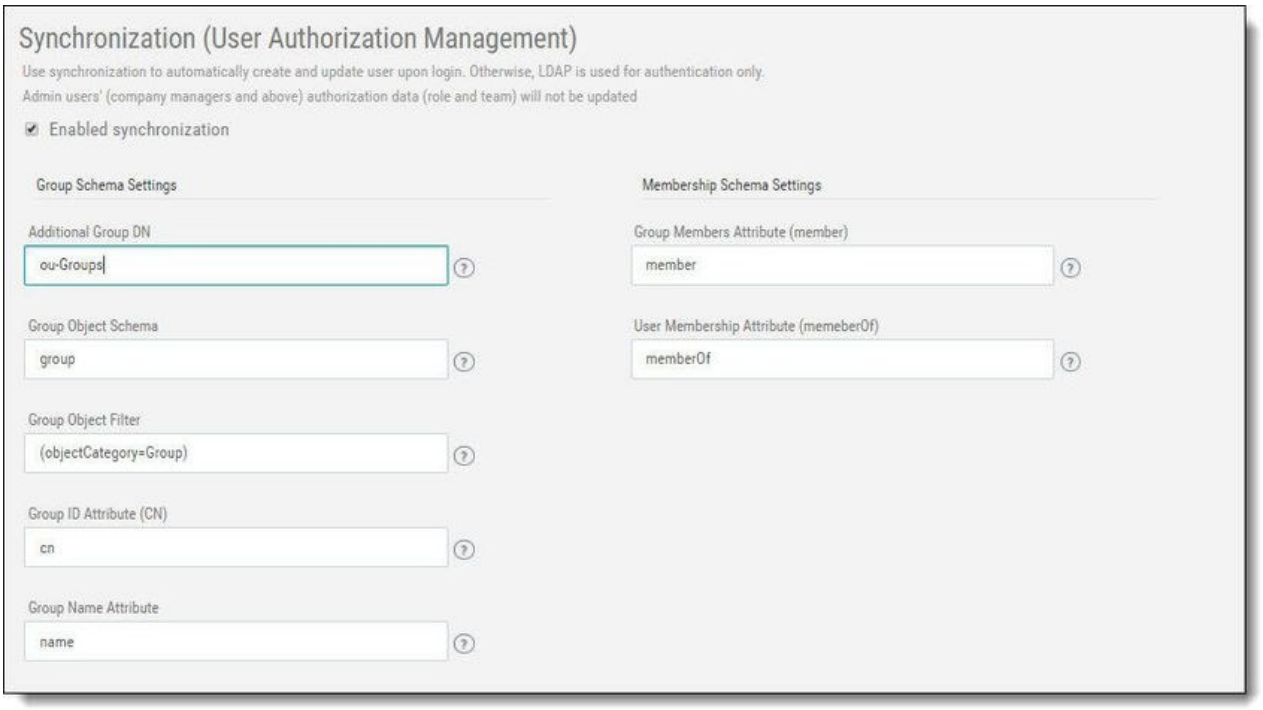
Configuring LDAP Synchronization Settings

Synchronization, once enabled, can be used to automatically create and update LDAP users upon login. If disabled, LDAP is used for authentication only.

■ Note that, even with LDAP synchronization enabled, there is still an ability to manually change the account status of a user from CxSAST. Any changes will be overridden by the LDAP server on the next synchronization.

To configure LDAP Synchronization settings:

Check **Enable Synchronization.** The LDAP Synchronization window is displayed.



■ Even with LDAP synchronization enabled, there is still an ability to manually change the account status of a user from CxSAST. Any changes will be overridden by the LDAP server on the next synchronization.

Define the following Synchronization parameters:

Parameter	Description
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)
Group Members Attribute (member)	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 Membership Attribute (memberOf)	LDAP membership attribute is a multi-valued attribute that contains groups of which the user is a direct member (e.g. memberOf)

Defining User Management (Synchronization)

User Management (Synchronization) supports the retrieving of users from LDAP and defining them in CxSAST. Synchronization default parameters only apply when the Synchronization option is enabled (see **Configuring LDAP Synchronization Settings**).

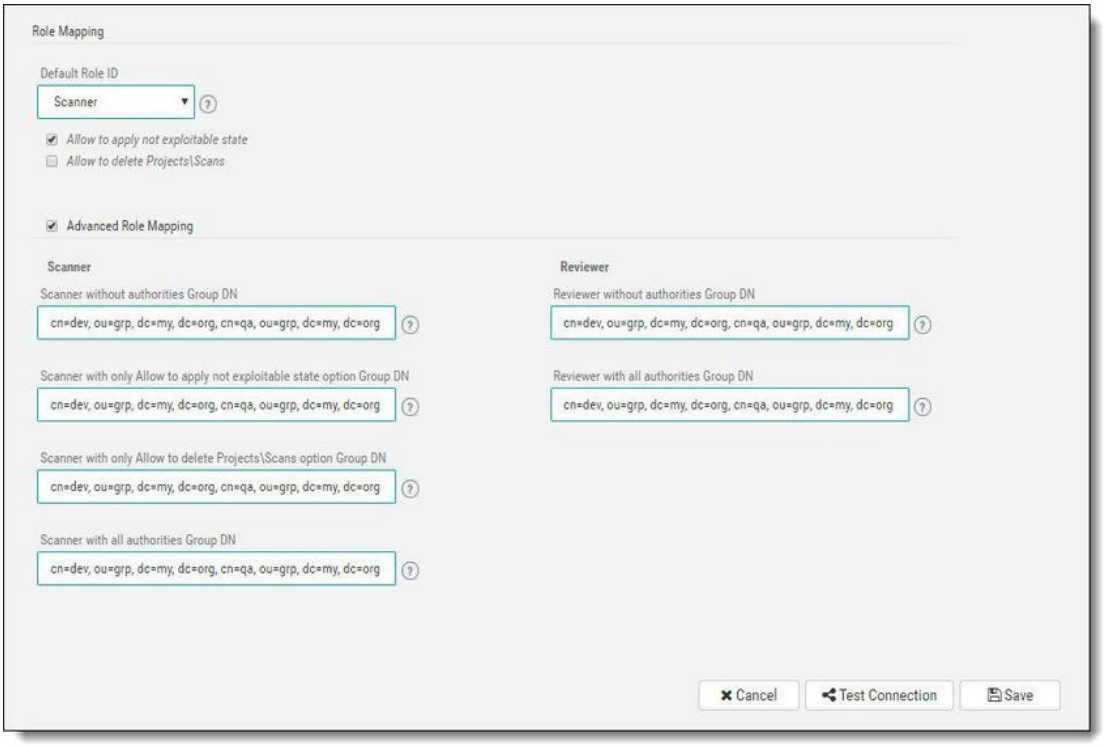
Select the preferred Synchronization Default Parameters:

Method	Description
Manual Role Authorization	User creation managed by LDAP and authorization performed manually by CxSAST user management. By default, LDAP users belong to one team and are either defined as scanners or reviewers upon login. You can manually change a logged in user's Team and Role from CxSAST (see *Mapping LDAP Directory User Groups to CxSAST Teams*).
LDAP Role Authorization	Role authorization is managed by LDAP and automatically updated upon login to CxSAST. Role authorization and management definitions are defined during the creation and mapping of user attributes in LDAP.

Click **Save** to save the changes.

Defining Role Mapping Settings

Role mapping settings are used to determine the role of users (e.g. Scanner, Reviewer) who were created in LDAP and otherwise not assigned roles in CxSAST. Role Mapping parameters only apply when the Manual Role Authorization option is enabled - see *Defining User Management (Synchronization*).



Define the following Role Mapping parameters:

Parameter	Description
Default Role ID	Used to determine the CxSAST role of users who have otherwise not been assigned roles (e.g. Scanner, Reviewer) • **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 • **Reviewer** - can make changes to the status or severity of found instances if the checkbox is selected
Advanced Role Mapping	Role mapping in CxSAST can be managed by checking the Advanced Role Mapping checkbox and the defining the parameters below. **NOTE:** Roles managed by LDAP are automatically updated upon login to CxSAST.

Parameter	Description
Scanner without authorities Group DN	Used to define a list of LDAP Group DNs. Members of these groups will be assigned the scanner role without Apply Not Exploitable State and Delete Projects\Scan options (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Scanner with only Allow to apply not exploitable state option Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the scanner role with only Apply Not Exploitable State option (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Scanner with only Allow to delete Project\Scans option Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the scanner role with only Delete Project\Scans option (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Scanner with all authorities Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the scanner role with Apply Not Exploitable State and Delete Projects\Scan options (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Reviewer without authorities Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the reviewer role without Allow Severity/Status Change options (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Reviewer with all authorities Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the reviewer role with Allow Severity/Status Change options (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).

Click **Save** to save the changes.

In order for users to automatically log in using Synchronization, complete *Mapping LDAP Directory User Groups to CxSAST Teams (*see *Managing Teams).*

SAML Management

Security Assertion Markup Language (SAML) is an XML-based format for exchanging authentication and authorization data between an identity provider and a service provider. Checkmarx's Static Analysis Security Solution (CxSAST) has just become SAML 2.0 aware and can now be configured to act as a SAML 2.0 Service Provider. SAML supports the user lifecycle by retrieving users from the Identity Provider (IdP) and defining them in CxSAST. This allows for more centralized and enhanced user management.

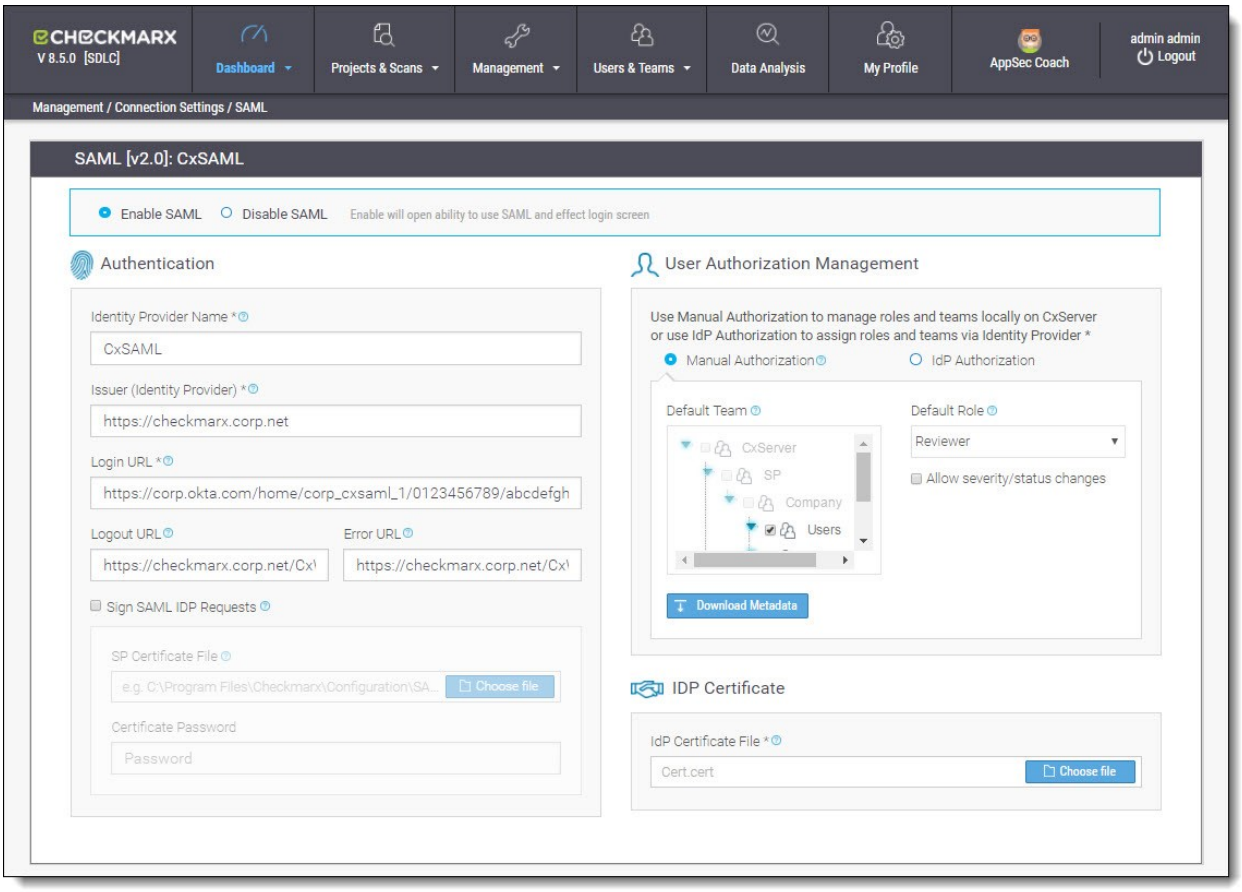
- SAML login for CxAudit is currently not supported.

Configuring SAML in CxSAST

Before you start with Configuring SAML in CxSAST, see *Enabling HTTPS on the CxSAST Server* and also *Configuring the Identity Provider* (in the *CxSAST Plugin and Integration Guide*) – these are required in order to proceed.

- Make sure that the property in the Web Server Address field (Management -> Application Settings -> General) is set and valid.

From the **CxSAST** application, go to **Management** > **Connection Settings** > **SAML**. The **SAML Configuration** screen is displayed.



Select **Enable SAML** in order to activate the **SAML Configuration** screen.

■ The SAML Single Sign-In option won't be available in the CxSAST Login screen unless SAML is enabled.

Fill the following Authentication parameter fields:

Parameter	Description
Identity Provider Name	Name given to the SAML Identity Provider (e.g. CxSAML)
Issuer (Identity Provider)	Element which contains the unique identifier of the IdP, and will usually contain the URL of the IdP and a hash (e.g.: http://www.okta.com/exkac5ylseLJUQLeZ0h7). This parameter is provided by the Identity Provider setup information (see *Retrieving Identity Provider Setup Information* in the *CxSAST Plugin and Integration Guide)*.

Parameter	Description
Login URL	Identity Provider login location where SAML requests will be sent (e.g. https://corp.okta.com/home/corp_cxsaml_1/0123456789/abcdefghij). This parameter is provided by the Identity Provider setup information (see *Retrieving Identity Provider Setup Information* in the *CxSAST Plugin and Integration Guide*).
Logout URL	Location where logout instances will be redirected (e.g. https://checkmarx.corp.net/CxWebClient).
Error URL	Location where error instances will be redirected (e.g. https://checkmarx.corp.net/CxWebClient/ErrorPages/Default_Error.aspx).
Issuer (Audience)	The local server name is the issuer by default. Changing the default is done in the database: [CxDB].[dbo].[CxComponentConfiguration], [Key] = 'SamlServiceProviderIssuer', [Value]= '<SP Issuer>'
CxSAST Login URL	The local server name is the host name by default. Changing the default is done in the database: [CxDB].[dbo].[CxComponentConfiguration], [Key] = 'WebServer', [Value]= '<Host name>'
Sign SAML IdP Requests	Select to enable the Sign SAML IdP Requests option. This assures that every request sent to the IdP server is signed with a Service Provider certificate.
SP Certificate File	Click Choose File and navigate to the relevant certificate file (.p12 or .pfx formats only). The uploaded certificate file should contain a private key.
Certificate Password	Enter the unique password for the certificate file. Password is only required when a certificate is added or updated.

Select the preferred Authorization method:

Method	Description

Manual Authorization	User creation managed by the SAML Identity Provider and authorization performed manually by CxSAST user management.
	• **Default Team** - All new users will be added to selected default team
	• **Default Role** - All new users will be added to selected default role (scanner or reviewer)
	  ○ **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
	  ○ **Reviewer** - can make changes to the status or severity of found instances if the checkbox is selected
	NOTE: By default SAML users belong to one team and are either defined as scanners or reviewers upon login. You can manually change a logged in user's Team and Role from the CxSAST (see *Changing the SAML User's Team and Role in the CxSAST*).

IdP Authorization	Teams and roles managed by the SAML Identity Provider are automatically updated upon login to CxSAST. The definitions for the update are defined during the creation and mapping of user attributes in the SAML IdP (see *Creating and Mapping User Attributes in OKTA* in the *CxSAST Plugin and Integration Guide*.
Download Metadata	The Metadata file may be required for troubleshooting by the IdP admin, or for defining missing attributes (see *Configuring the Identity Provider*). Click **Export Metadata**. The metadata file is downloaded to the default download directory. See *Exporting the Metadata File from CxSAST* in *SAML Management (v8.5.0 and up)*. **NOTE:** The information provided in the downloaded metadata file will depend on the Manual or IdP Authentication method currently selected.

Importing the SAML Certificate into CxSAST

In order for CxSAST to validate the authentication token, the IdP certificate (.cert) needs to be imported and installed on CxSAST (CxManager location).

From **IDP Certificate**, click **Choose File** and navigate to the same IdP certificate file (.cert) that was downloaded to the default download directory during the configuration of the Identity Provider (see *Retrieving Identity Provider Setup Information* in the *CxSAST Plugin and Integration Guide*).

- For instances where there is no other choice but to manually install the IdP certificate file on the CxSAST server trusted root certification authority (see *Manually Installing a SAML Certificate on the CxSAST Server* in the *CxSAST Plugin and Integration Guide*).

Click **Save** to save the changes. The **SAML setup confirmation** message is displayed.

- If the Configuration is not saved (no clear confirmation message), check the log file at: <Checkmarx manager installation>\Logs\WebAPI\WebAPI.log

Exporting the Metadata File from CxSAST

The **Metadata** file may be required for troubleshooting by the IdP admin, or for defining missing attributes (see *Configuring the Identity Provider* in the *CxSAST Plugin and Integration Guide*).

Click **Export Metadata**. The **metadata file** is downloaded to the default download directory.

- The information provided in the downloaded metadata file will depend on the Manual or IdP Authentication method currently selected (see *Configuring SAML in CxSAST*).

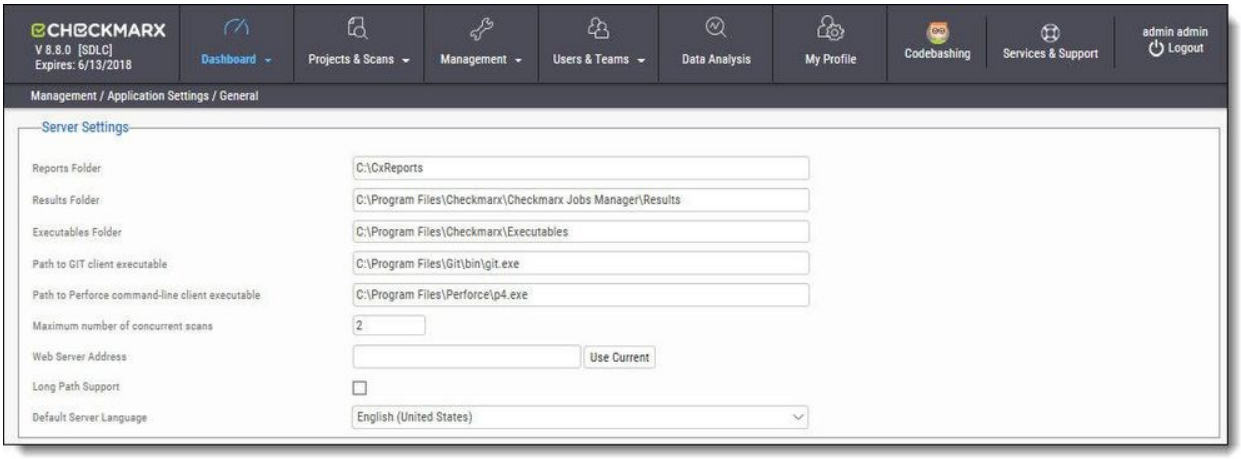
Application Management

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 panel, you can set folder locations, maximum number of scans, default settings and automatic sign in.



Click **Edit**. The setting fields are enabled.

The panel 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 (e.g. 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).

> The validation of 'git.exe' and 'p4.exe' is no longer mandatory in CxSAST when defining the 'Path to GIT client executable' and the 'Path to Perforce command-line client executable' parameters.

- **Path to P4 command line client executable** - Set the Perforce client executable path (e.g. 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. CxScansManager service must be restarted before any changes to this setting will go into effect.
- **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.
- **Long Path Support** - Enables long path support for the CxSAST application.
- **Default Server Language** - Set the default server language.
- **Allow Auto Sign In** - Enable/Disable auto sign in.

SMTP Settings

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

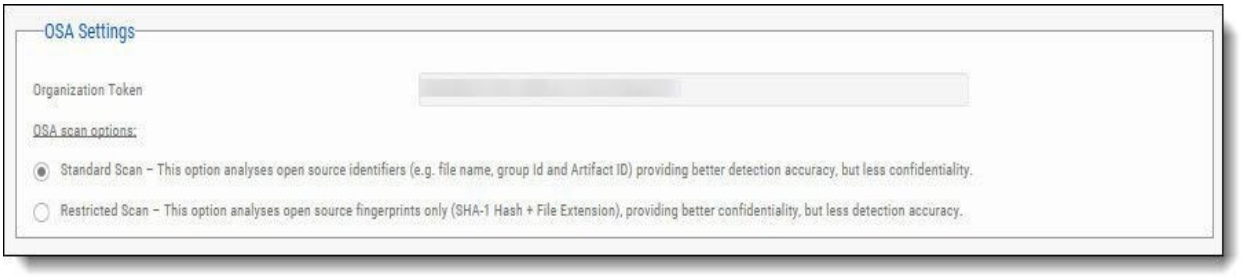
Click **Edit**. The setting fields are enabled.

This panel includes the following settings:

- **Host** - Type in the host domain
- **Port** - Select a port number
- **Encryption Type** - Select the encryption type
- **Email from Address** - Notification by E-mail address
- **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

OSA Settings

The OSA settings panel enables you to set the CxOSA settings for the system.



Click **Edit**. The setting fields are enabled.

This panel includes the following settings:

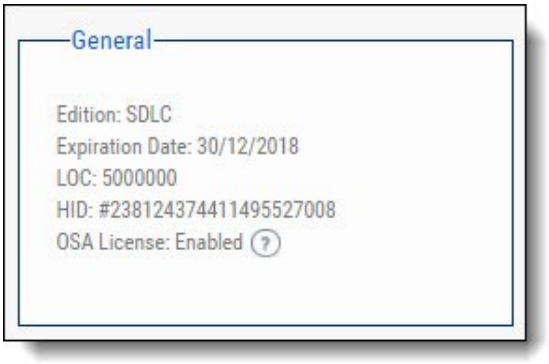
- **Organization Token** - Displays the organization token provided by WS (read-only)
- **OSA Scan Options:**
  - **Standard Scan** – This option analyses open source identifiers (e.g. file name, group Id and Artifact ID) providing better accuracy, but less confidentiality (Default for new installations).
    Restricted Scan – This option analyses open source fingerprints only, providing better security, but less confidentiality (Default for upgrades on existing installations).

License Details

The License Details screen is divided into the following windows:

General

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



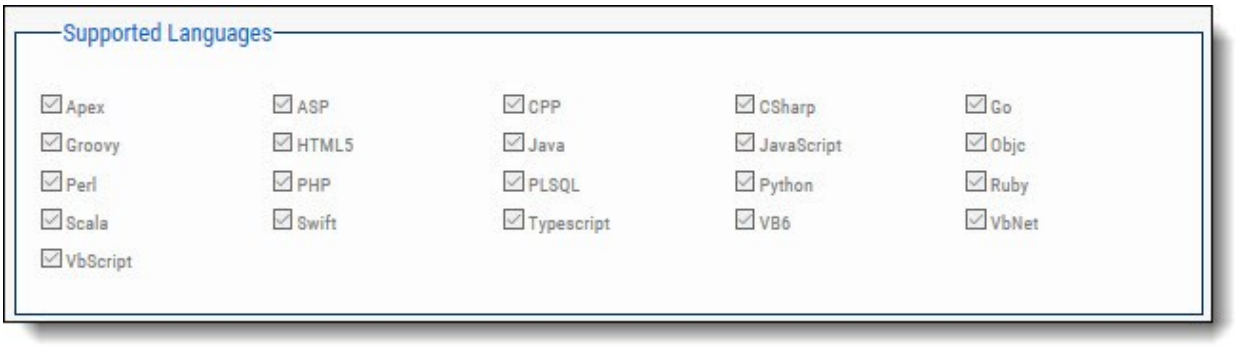
This includes the following information:

- **Edition -** CxSAST license edition (SDLC or Security Gate)
- **Expiration Date** - CxSAST license expiry date
- **LOC** - The number of lines of code the license was bought for
- **HID** - Hardware identification number
- **CxOSA License -** Open Source Analysis license status (Enabled, Disabled or Conditional with expiration date for Conditional version).

■ 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.

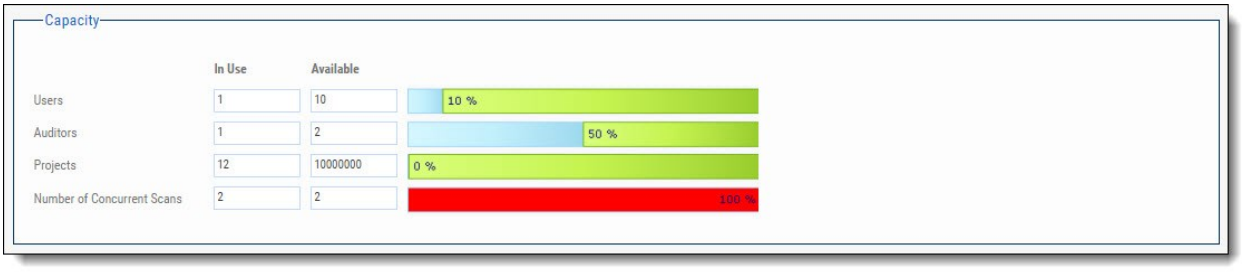
Supported Languages

The **Supported Languages** panel includes the supported languages used in default queries.



Capacity

The Capacity panel provides information about the number of users (combined roles), projects and engines available and in use in the system according to the current license.



The **Capacity** panel includes the following information:

- **Users** - Number of users available in the system (i.e. Server Managers, Service Provider Managers, Company Managers, Scanners and Reviewers)
- **Auditors** - Number of users available in the system that have auditing permissions and can run CxAudit (i.e Auditors Users)
- **Projects** - Number of projects available in the system
- **Number of Concurrent Scans** - Number of concurrent scans available in the system.

License Expiration Notification

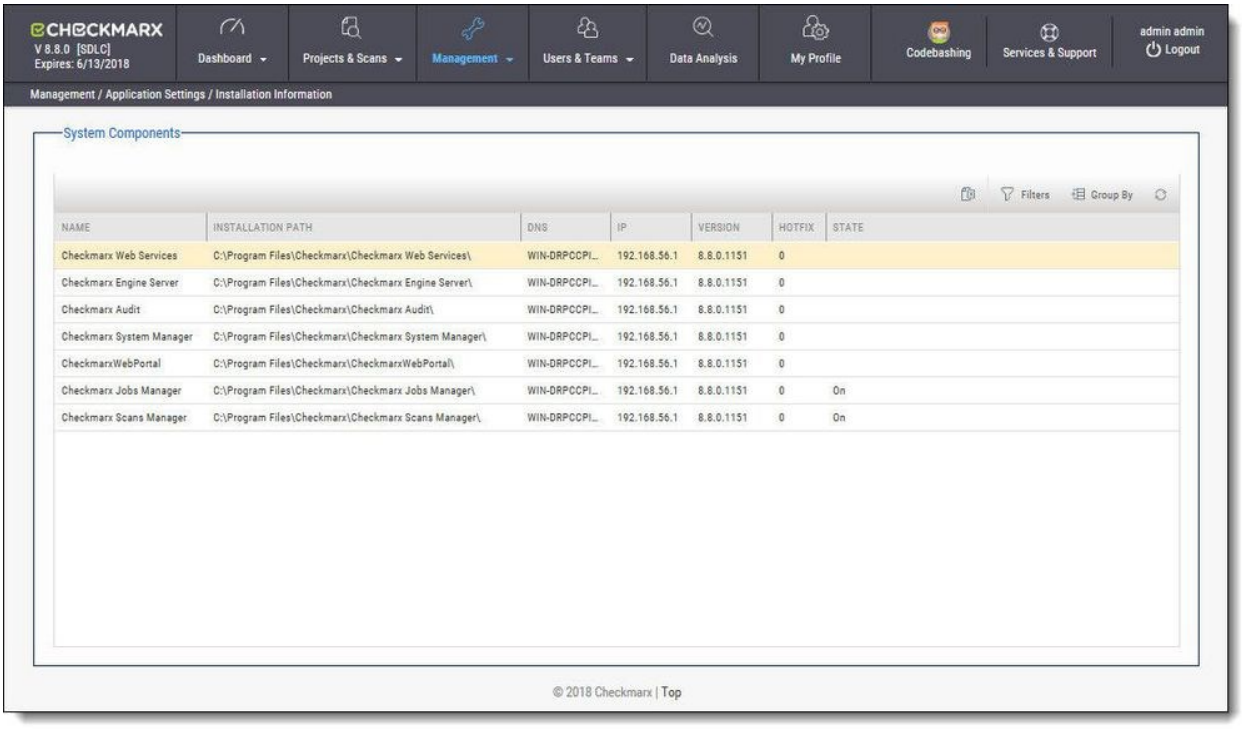
The **License Expiration Notification** panel provides notification behavior settings for when your CxSAST license is about to expire.

- **Notification by E-mail** - If checked, a notification email is automatically sent to the CxSAST Administrator User on a weekly basis, starting 90 days (defined in the database) before the actual license is set to expire.

> ■ The Notification by E-mail address is defined under the E-mail Notifications parameter in Server *SMTP Setting*.

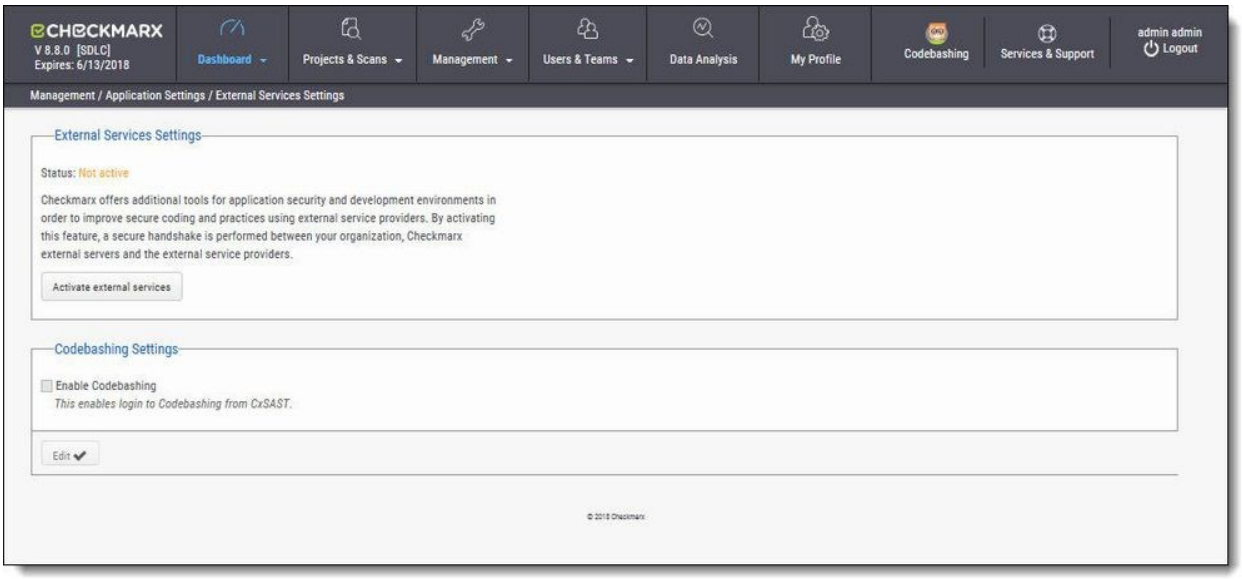
Installation Information

The Installation Information screen provides a list of all the Cx components installed, the Installation Path, Version (with build), DNS, IP, Hotfix, and State.



External Services Settings

CxSAST offers additional tools for application security and development environments in order to improve secure coding and practices using external service providers. By activating this feature, a secure handshake is performed between your organization, Checkmarx external servers and the external service providers.



Click the **Activate/Reactivate External Services** button to activate or reactivate (if deactivated) a secure communication path between your organization, CxSAST and the service provider.

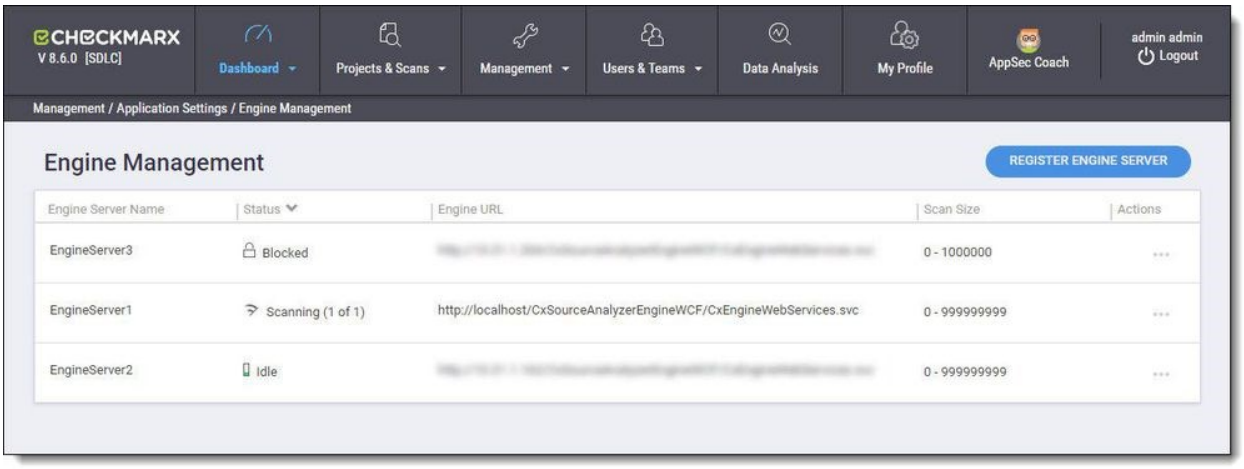
> In cases where the automatic activation process doesn't perform as expected, you may need to request a manual activation. Please contact Checkmarx support.

Click **Edit**. The **Codebashing Settings** fields are enabled.

- **Enable Codebashing** - If selected, enables **anonymous data collection** in order to provide user analytics. The second checkbox, enables **non-anonymous data collection** in order to provide user analytics.If selected, sends the user details (email) to Codebashing for Analytics View.

Engine Server Management

Engine Server Management enables an interface for viewing real-time engine server status information that includes the number of engine servers in the system (active and offline), status of each engine server (scanning, idle, blocked, etc.) and location (URL) and scan size of each engine server. Direct action options (single) include register, edit, unregister and block/unblock engine servers.



> The Engine Server Management screen automatically refreshes itself every 20 seconds.

Engine Sever Management provides real-time information about the status of each engine server in the system. Each engine server is listed according to its status. The engine server list includes the following information:

Field	Description
Engine Sever Name	Name of the engine server
Status	Status of the engine server: • Scanning • Idle (engine server waiting to receive scan requests • Blocked (engine server unable to receive scan requests) • Offline (engine server unable to communicate to system, e.g. machine down, service stopped, connectivity issues, etc.) • Scanning and Blocked (engine server running scans already requested from the system, before the engine server was blocked)
Engine URL	URL of the engine server
Scan Size	Engine server scan size
Actions	Single actions: edit, unregister and block/unblock engine server

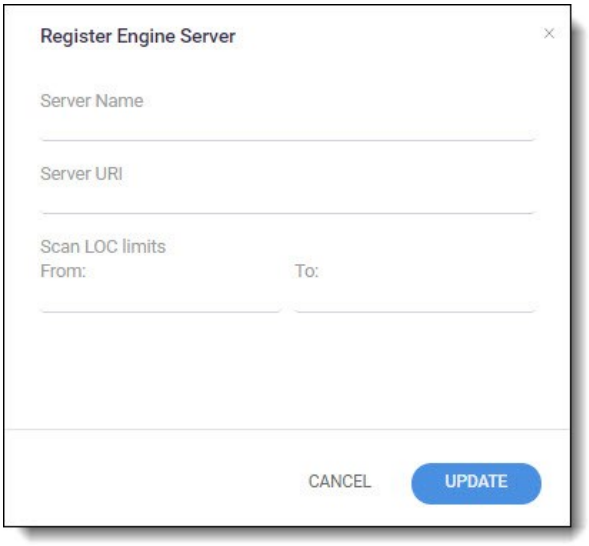
Performing Engine Sever Management Actions

Once the Engine Management screen is displayed you can perform single actions.

Register a New Engine Server

You can register a new engine server to the system.

To register a new engine server, click the Register Engine Server button. The Register Engine Server dialog is displayed.



Define the following attributes:

Parameter	Description
Server Name	Enter the name of the engine server. Each engine server should have a unique name.
Server URI	Enter the URI address of the engine server. URI address must start with the http(s):// prefix.
Scan LOC Limit	Enter the scan LOC (lines of code) limit. The 'From' and 'To' definition must be a whole number between 0 - 999,999,999.

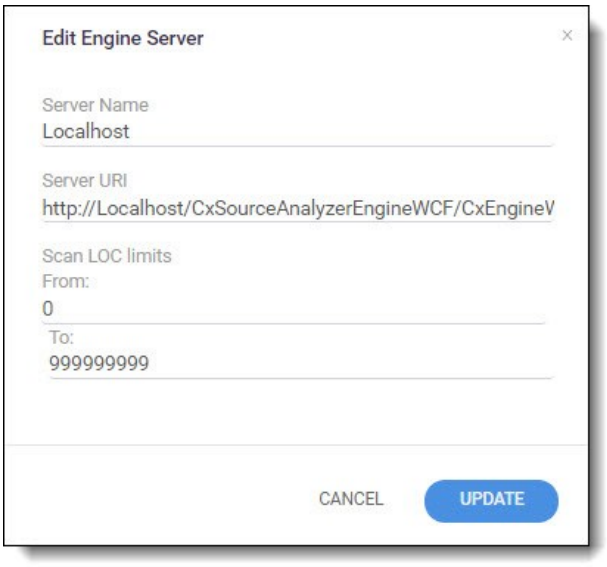
Click Update to save the changes. The new engine server is added to the engine List.

Edit an Existing Engine Servers Attributes

You can edit an existing engine server's attributes in the system.

To edit an existing engine server's attributes:

Click the Actions  icon in line with the engine server that you would like to edit and select Edit. The Edit Engine Server dialog is displayed.



Change the engine server's attributes accordingly (see Register a New Engine Server for more information about the available attributes).

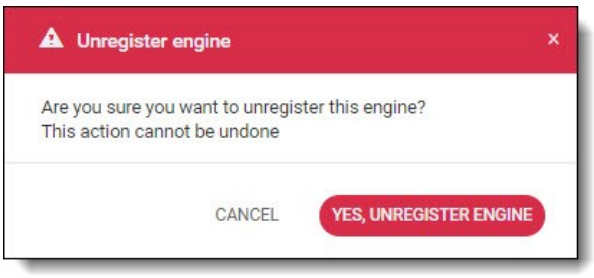
Click Update to save the changes.

Unregister an Engine Server

You can unregister an existing engine server in the system.

To unregister an existing engine server:

Click the Actions  icon in line with the engine server that you would like to unregister and select Unregister. The Unregister Engine Server dialog is displayed.



Click Unregister Engine to continue, or click Cancel. The engine server is removed from the engine list.

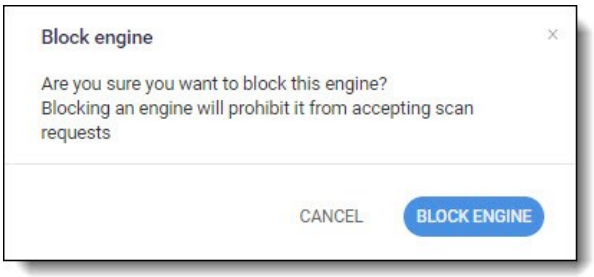
> ■ You cannot unregister an engine server that is currently running a scan.

Block/unblock an Engine Server

You can block an engine server in the system. Blocking prevents the engine server from accepting any new scan requests from the system. Scans already requested from the system, before the engine server was blocked, will continue uninterrupted until completion.

To block an engine server in the system:

Click the Actions  icon in line with the engine server that you would like to block and select Block. The Block Engine Server dialog is displayed.



Click Block Engine to continue, or click Cancel. The status of the engine server is changed to Blocked in the engine list.

To unblock an engine server in the system, perform the same procedures, as above, and select Unblock until completed. Once the engine server is unblocked it can start to except new scan requests from the system.

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*).

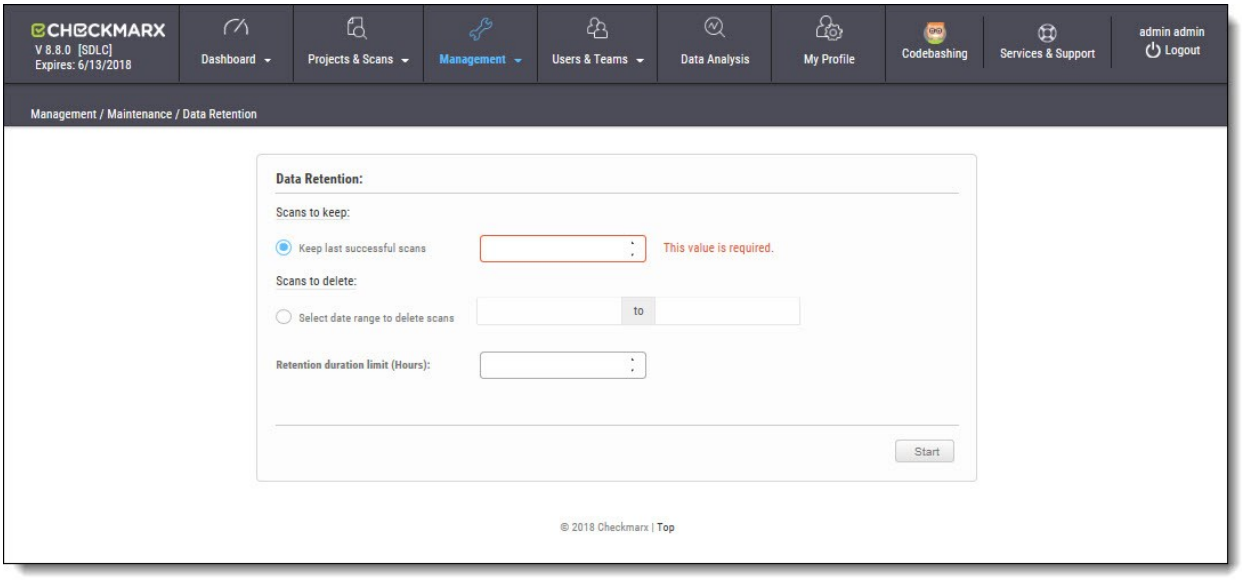
Specific scans may be marked as “Locked” to avoid automated purging of important scan data.

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:

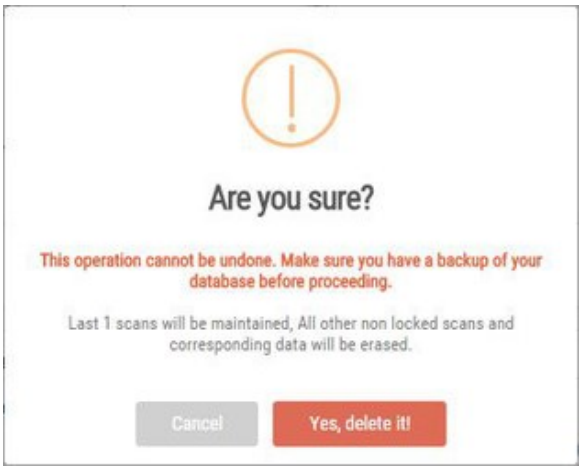
Scans to keep:

- **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.

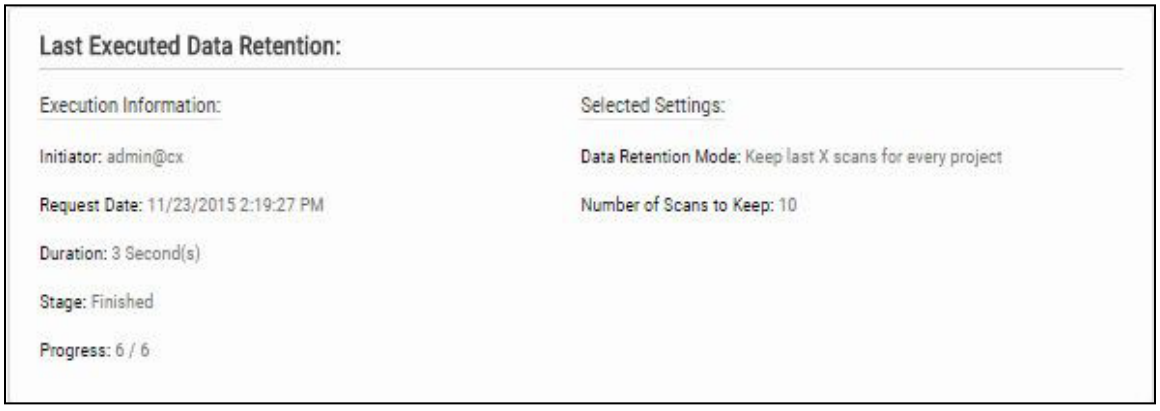
Click **Start**. The following message appears:



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

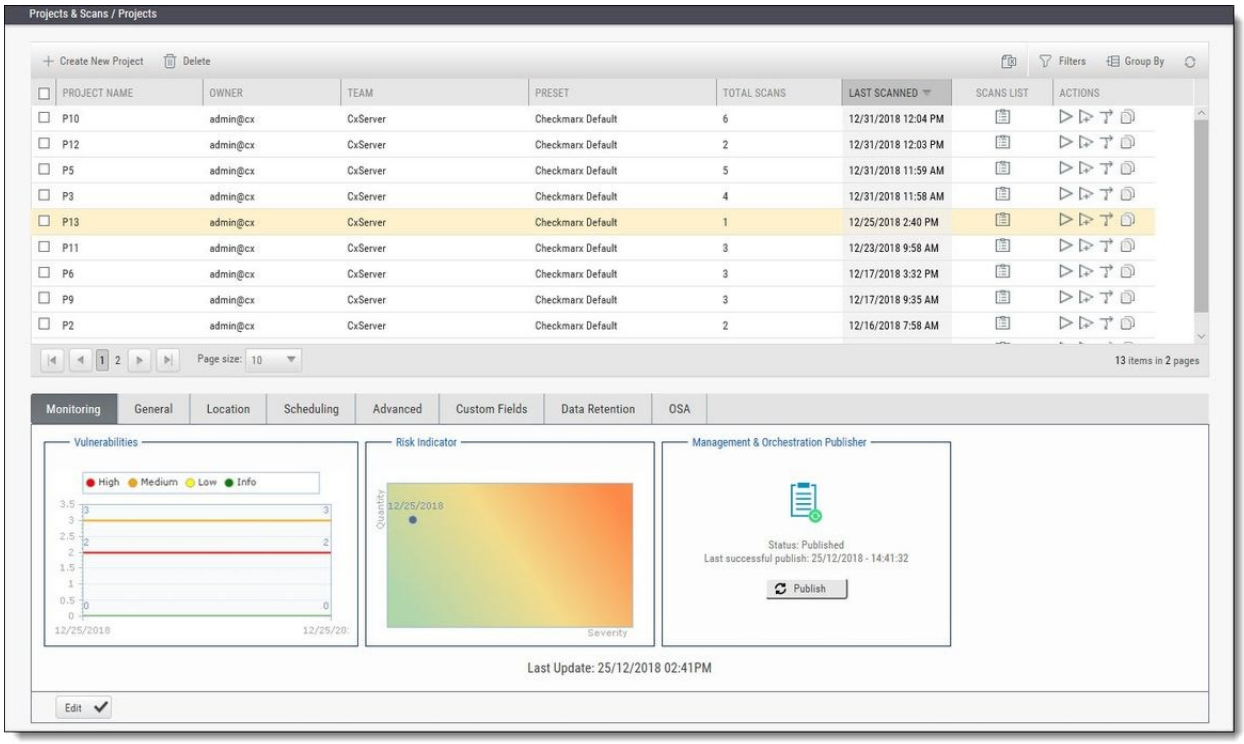
- CxSRC folder – This folder holds the extracted source files which are being scanned. Files and folders inside the CxSrc folder are deleted as part of data retention except for the following scenario:
  In case the exact same sources (ZIP, remote location..) are uploaded to the same existing scan, the 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:

Go to **Projects & Scans** > **Projects**.



Select the requested project. If many projects exist, find the project by using the following steps:

Click **Filters** on the right.
Type one or more identifying criteria for the project, such as the project name, owner, and team.
Click **Enter**.

Go to the column **Scans List**.

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.

Go to the **Locked** column. See if one or more of the scans is locked.

Use the **Unlock scan** button ( ) to remove the lock.

Custom Field Management

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:

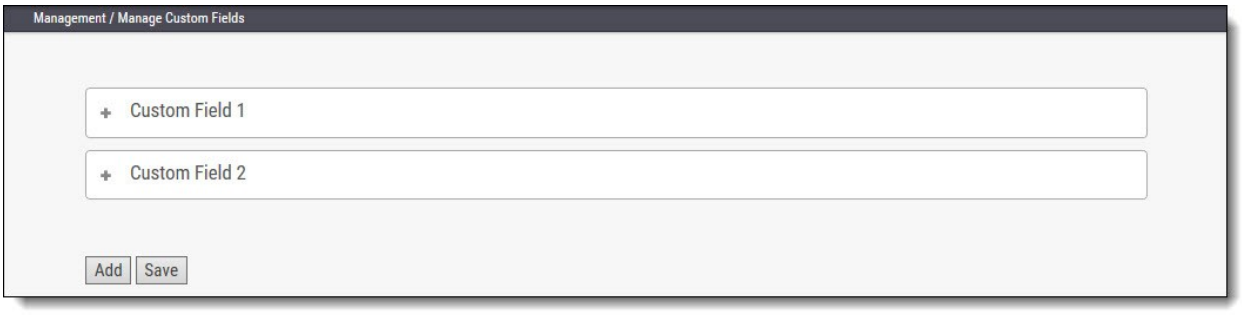
Go to **Management > Manage Custom Fields.**

Click **Add**.

Enter a unique custom field name in the designated field.

Click **Save**.

Each newly added custom field (up to 10) is displayed on the list and can be edited or deleted.



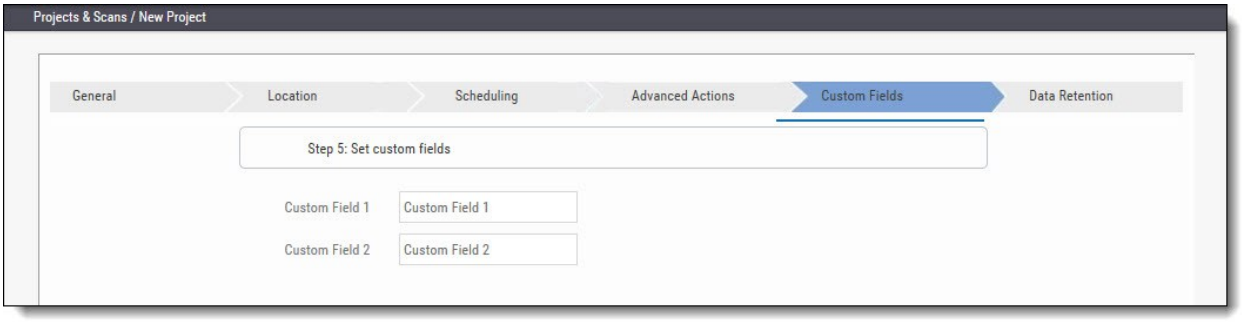
To edit the custom field's name:

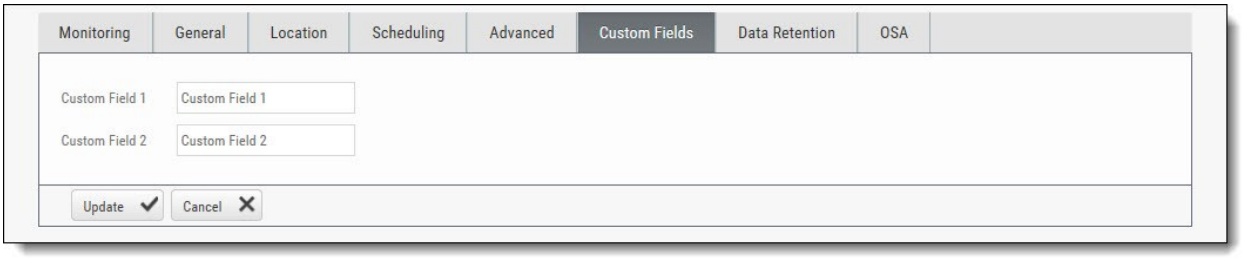
Click the "+" sign to the left of the field name.

Perform the requested change in the editable row that appears.

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.



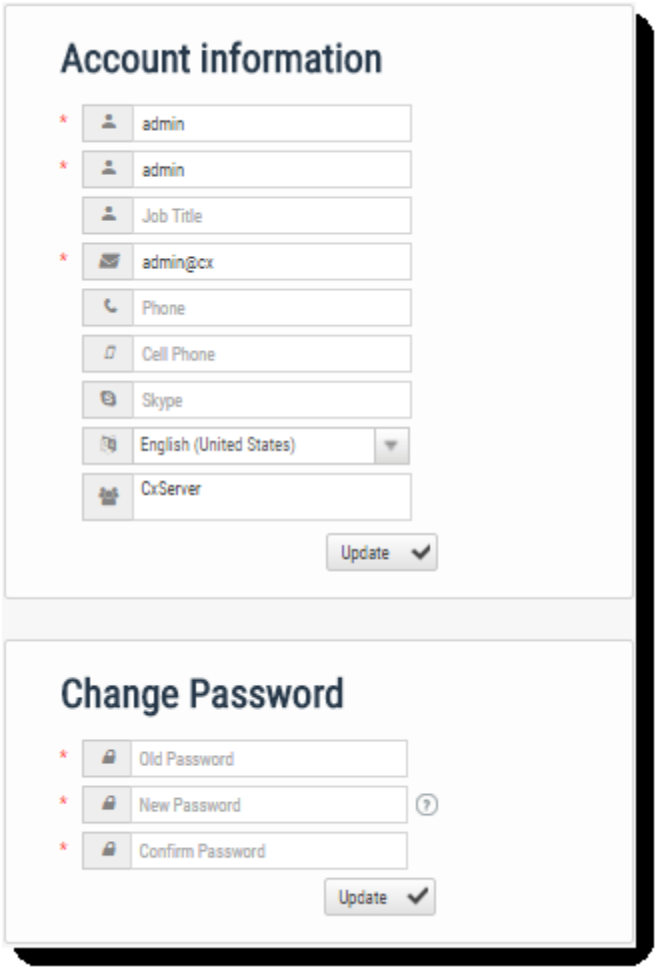


My Profile Settings

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)
  - French (France)
  - Spanish (Spain)
  - Portuguese (Brazil)
  - Russian (Russia)
  - 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**.