



**CxSAST v9.2.0**

## **Setup and Installation Guide**

This document is non-binding and for information purposes only

# Contents

<b>SETTING UP CXSAST .....</b>	<b>5</b>
SYSTEM ARCHITECTURE .....	5
<i>CxClient</i> .....	6
<i>CxServer</i> .....	6
<i>Architecture Types</i> .....	7
<i>Centralized Architecture</i> .....	7
<i>Distributed Architecture</i> .....	8
<i>High Availability Architecture</i> .....	9
HARDWARE & SOFTWARE REQUIREMENTS.....	10
<i>Server Host Requirements</i> .....	10
Required Software for all Scenarios .....	10
Centralized (POC) .....	11
Centralized (Production) .....	11
Distributed – CxEngine (Production) .....	11
Distributed – CxManager with Management and Orchestration Layer (Production) .....	12
Distributed – CxManager without Management and Orchestration Layer (Production) .....	12
Distributed – Database (Production).....	12
DB Latency.....	12
Server Hardening Checklist .....	13
Recommended Resolutions.....	13
<i>Supported Environments</i> .....	14
Supported Components and Operating Systems .....	14
<i>Supported SQL Servers</i> .....	15
<i>Supported Integrations and Plugins</i> .....	15
<i>Supported Browsers</i> .....	15
Chrome Support .....	16
<i>Preparing the Environment</i> .....	16
Installing IIS 10 on Windows 10 .....	18
Installing IIS 8 on Windows Server 2012 .....	19
Installing IIS 8.5 on Windows Server 2012 R2.....	22
Installing IIS 10 on Windows Server 2016 .....	23
Enabling Long Path Support in Windows 10 and Server 2016.....	26
INSTALLING CXSAST.....	27
<i>Installation Permissions</i> .....	28
SQL Database .....	28
AWS RDS.....	29
<i>Preparing for Installation</i> .....	29
Obtaining and Validating a License .....	29
Making the Installation Package Available .....	29
Prerequisites .....	30
<i>Installing CxSAST</i> .....	32
Prerequisites and Recommendations.....	32
Installation.....	32

Installed Services Check .....	45
General Settings .....	48
My Profile Settings .....	49
Engine Settings (in a distributed architecture) .....	50
Installation Verification .....	51
<i>Installing CxSAST in Silent Mode</i> .....	51
Prerequisites .....	51
Parameters .....	52
Remarks .....	54
Examples .....	54
UPGRADING CxSAST IN HIGH AVAILABILITY SOLUTIONS .....	55
MODIFYING CxSAST .....	56
<b>Before you Start</b> .....	56
BACKING UP AND RECOVERING CxSAST .....	64
<i>Backing up CxSAST</i> .....	64
<i>Recovering CxSAST</i> .....	66
UPGRADING CxSAST .....	68
<i>Upgrading CxSAST in High Availability Solutions</i> .....	72
<i>Access Control Data Migration Installer</i> .....	72
Access Control Data Migration Tool - Overview .....	72
Restoring Passwords .....	76
Using the Access Control Data Migration Tool .....	76
Access Control Data Migration Tool Troubleshooting .....	85
ADDING A CXENGINE SERVER .....	88
UNINSTALLING CxSAST .....	92
UPDATING THE CxSAST LICENSE .....	95
CxSAST UTILITIES .....	98
<i>CxZIP - Create a Smaller File for Upload</i> .....	98
Create a Smaller File for Upload .....	98
Create a Smaller File for Upload (Longpath Support) .....	98
<i>CxCMDLineCounter - Count Lines of Code</i> .....	99
CxSAST APPLICATION MAINTENANCE GUIDE .....	100
<i>Introduction</i> .....	100
<i>Backup</i> .....	101
Step 1. Stop the CxServices .....	101
Step 2. Stop the Web Server .....	101
Step 3. Back up the Checkmarx Folder .....	101
Step 4. Backup the Database .....	102
Step 5. Backup the Scanned Source Folder .....	102
Step 6. Restart the CxServices .....	102
Step 7. Restart the Web Server .....	102
<i>Recovery</i> .....	102
Step 1. Stop the CxServices .....	102
Step 2. Stop the Web Server .....	103
Step 3. Restore Checkmarx's Backed up Folders and configuration files .....	103
Step 4. Restore the Scanned Source Folder .....	103
Step 5. Restore the Database .....	103
Step 6. Restart the CxServices .....	103
Step 7. Restart the Web Server .....	103

Step 8. Check the Recovered Version.....	103
MAINTENANCE AND CLEANUP.....	104
<i>CxManager</i> .....	104
Sources.....	104
Logs.....	105
Reports.....	105
<i>CxEngine</i> .....	105
Sources.....	105
Logs.....	105
Scans.....	106
<i>CxWebPortal</i> .....	106
Logs.....	106
<i>CxAudit</i> .....	106
Sources.....	106
Logs.....	106
<i>Database</i> .....	107
APPENDIX A: COMPRESSING A FOLDER IN WINDOWS.....	107
<i>Trade-Offs</i> .....	107
<i>When to Use and When Not to Use NTFS Compression</i> .....	107
<i>How to Use NTFS Compression</i> .....	108
CXSAST DATABASE MAINTENANCE GUIDE.....	109
<i>Chapter 1 - Introduction</i> .....	109
<i>Chapter 2 - Checkmarx Tables Overview</i> .....	110
<i>Chapter 3 - Monitoring</i> .....	111
<i>Chapter 4 - Maintenance Options for Reducing Fragmentation</i> .....	113
CXSAST ENGINE SETTINGS.....	115
<i>Introduced Configuration Extensions</i> .....	115
<i>PROCESS_AFFINITY_MANAGER_SETTINGS</i> .....	115

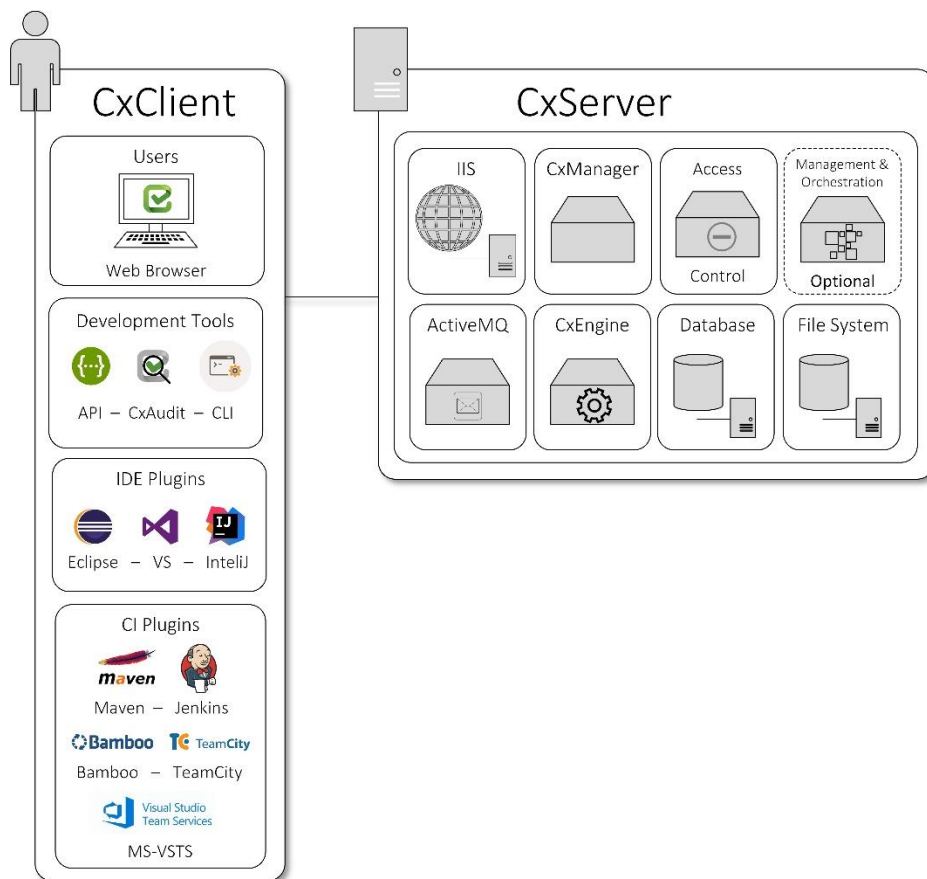
## Setting Up CxSAST

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

---

## System Architecture

The CxSAST system architecture overview 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** - provide scanning and integrated scan result navigation directly from the IDE development environment.
- **CI Plugins** - provide 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). Access Control manages roles and users.
- **CxManager** - manages and integrates system components, performs all system functions utilizing the IIS Web and Result services.
- **Management & Orchestration (Optional)** - manages security risk and orchestrates policy management, and includes remediation intelligence for unified findings, helping to drive decision across the organization based on actionable data.
- **ActiveMQ** – manages messaging queues.
- **CxEngine** - performs the code scans.
- **Database** - stores scan results and system settings.
- **File System** - controls how the data is stored and retrieved.

## Architecture Types

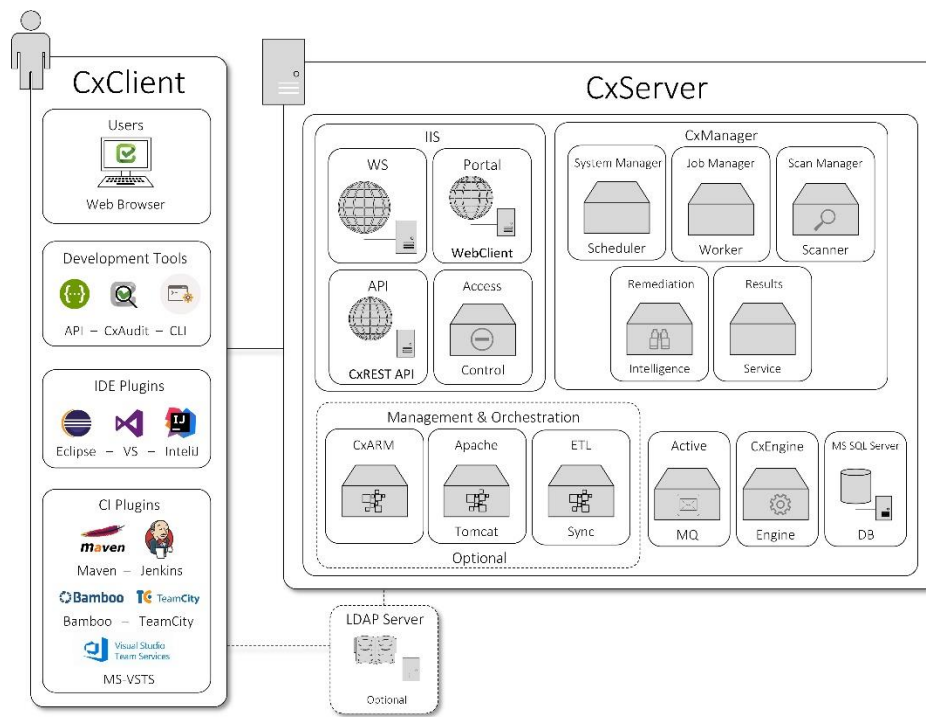
CxSAST supports the following architecture types:

- **Centralized Architecture** - where all server components are installed on the same host.
- **Distributed Architecture** - where any or some 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

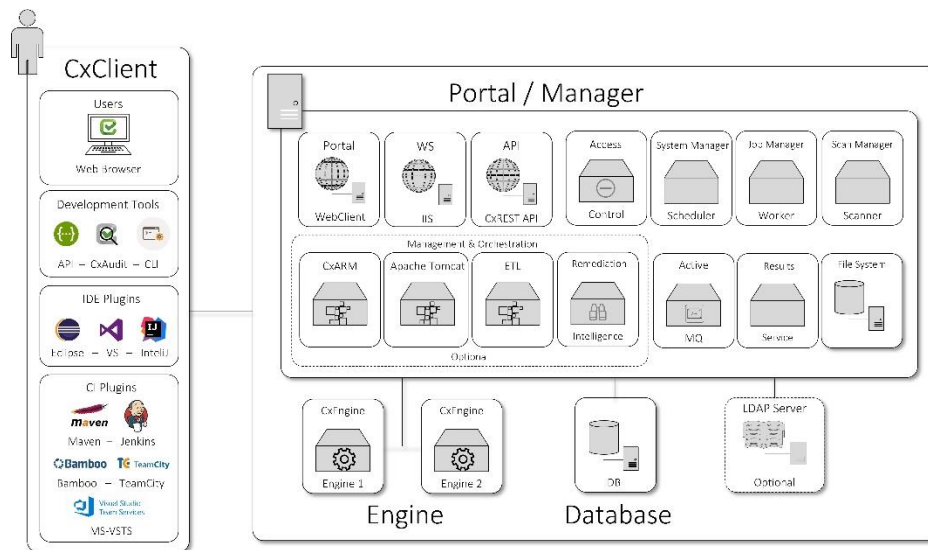
Centralized computing is a type of computing architecture where all or most of the processing/computing is performed on a central server. Centralized computing enables the deployment of all of a central server's computing resources, administration and management. CxSAST supports centralized architecture,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



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. The ActiveMQ is, by default, installed as part of the Manager, but can also be configured as an individual server, or as part of a cluster (node).

CxSAST also supports following architecture types:

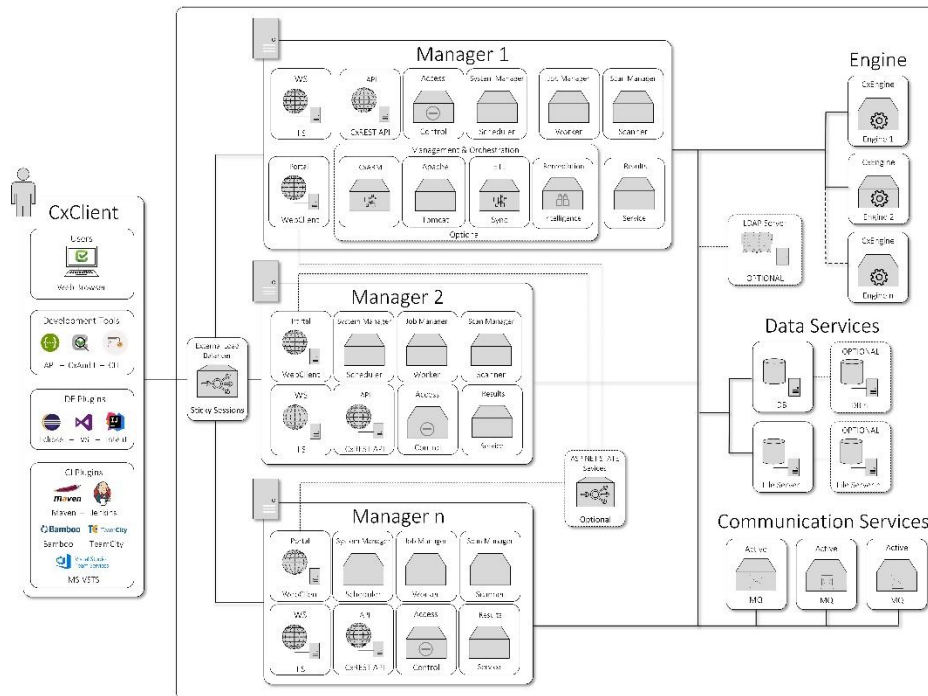
- **Centralized Architecture** - where all server components are installed on the same host.
- **High Availability Architecture** - where more than one manager is available to control system management, ensuring that in cases where one manager fails the system will continue to be fully operational.

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. The ActiveMQ can be configured as an individual server, or as part of a cluster (node).

- All CxManagers must be co-located in the 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** - All server components are installed on the same host.
- **Distributed Architecture** - Some or all 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.

---

## Hardware & Software Requirements

The following pages describe the hardware and software requirements for CxSAST:

---

### 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 the disk speed affects the scan time. For exact data for tested versions, refer to the CxSAST Release Notes.

The tables in the sections below list the requirements for the specific scenario.

### Required Software for all Scenarios

The following is required for all scenarios:

- Windows Installer 3.1 or above, run **msiexec** to check for the exact required version
- .NET Framework 4.7.1
- For distributed installation, the .NET Core 2.1 Runtime & Hosting is required for hosts on which CxManager is being installed.
- .NET Core 2.1.14 Runtime & Hosting
- Java 1.8 (Oracle or AdoptOpenJdk). The minimum version for Oracle is 8u241 and for AdoptOpenJdk, it is 8u242.
- **For Distributed Database (Production):** MS SQL Server 2012/2014/2016 (Express is not recommended).

### Centralized (POC)

LOC (Lines of Code)	RAM (GB)	Cores	CPU (GHz)	Disk (GB)	OS	Web Server
200K	8	6-8	2.8	80 (recommended)	Windows 10 Windows Server 2008R2, 2012, 2012R2, 2016	IIS 7/7.5/8/8.5/10
500K	16					

### Centralized (Production)

Centralized (Production) In addition to the listed resources, the following number of cores is required as follows:

- **One concurrent scan:** 8 cores.
  - **Each additional concurrent scan:** Additional 2 cores, up to max. of 12 cores. Recommended are 4, 6, or 8 cores.
  - **Max recommended concurrent scans:** 3
- For scans of 1M lines of code or more, it is recommended to limit the number of concurrent scans to one or run them on their own distributed server.

LOC (Lines of Code)	RAM (GB)	CPU (GHz)	Disk (GB)	OS	Web Server
200	10	2.8	250 (recommended)	Windows Server 2008R2, 2012, 2012R2, 2016	IIS 7/7.5/8/8.5/10
600	16				
1,200	24	2.8			
2,000	40				
3000	56				
4000	72				

### Distributed – CxEngine (Production)

For distributed CxEngine servers (for concurrent scans), each server must meet the listed requirements.

Centralized (Production) In addition to the listed resources, the following number of cores is required as follows:

- **One concurrent scan:** 4 cores.
- **Each additional concurrent scan:** Additional 2 cores. Recommended are 4, 6, or 8 cores.
- **Recommended socket configuration:** Single socket

LOC (Lines of Code)	RAM (GB)	CPU (GHz)	Disk (GB)	OS
200	6	2.8 (recommended)	100 (recommended)	Windows Server 2008R2, 2012, 2012R2, 2016
600	12			
1,200	20			
2,000	32			
3,000	48			
4,500	72			

### Distributed – CxManager with Management and Orchestration Layer (Production)

RAM (GB)	Cores	CPU (GHz)	Disk (GB)	OS	Web Server
14	8	2.5	250 (recommended)	Windows Server 2008R2, 2012, 2012R2, 2016	IIS 7/7.5/8/8.5/10

### Distributed – CxManager without Management and Orchestration Layer (Production)

RAM (GB)	Cores	CPU (GHz)	Disk (GB)	OS	Web Server
10	8	2.5	250 (recommended)	Windows Server 2008R2, 2012, 2012R2, 2016	IIS 7/7.5/8/8.5/10

### Distributed – Database (Production)

RAM (GB)	Cores	CPU (GHz)	Disk (GB)	OS
12	6-8	2.5	350-400 (recommended)	Windows Server 2008R2, 2012, 2012R2, 2016

- The required RAM and LOC resources for Javascript are higher.
- The Checkmarx Server requires dedicated memory allocation; features such as Memory Ballooning cannot be used.
- For Cloud Environment installations (AWS, etc.), these requirements may not exactly match the ones for Centralized or Distributed installations because you are choosing from predefined hardware packages and not defining your own specifications.
- To learn more about socket configuration, use our Engine Socket Configuration guide.

### DB Latency

	Acceptable Latency	Components
Network	<5ms, ideally <1ms	CxManager(s), SQL Server(s)
Network	<30ms	CxEngines
Disk I/O	<20ms avg	CxManager, CxEngine, SQL Server

## Server Hardening Checklist

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

### 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.

## Recommended Resolutions

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 pages outline the supported environments for CxSAST:

### Supported Components and Operating Systems

The following operations systems have been tested with CxSAST / CxOSA v9.0.0:

Operating Systems	CxSAST	CxOSA	Access Control	Management &Orchestration
Windows (64-bit) 10	V			
Windows Server 2008R2	V			
Windows Server 2012	V			
Windows Server 2012R2	V			
Windows Server 2016	V			

- Windows Server Core is not supported.

Java Version	CxSAST	CxOSA	Access Control	Management &Orchestration
Java 1.8 (Oracle or AdoptOpenJdk)	V			

- The lowest supported version for Oracle is 8u241. For AdoptOpenJdk it is 8u242.

Frameworks	CxSAST	CxOSA	Access Control	Management &Orchestration
Microsoft .NET Framework 4.7.1	V			
Microsoft .NET Core 2.1.16 Runtime & Hosting	V			

Web Server	CxSAST	CxOSA	Access Control	Management &Orchestration
IIS 7.5-10	V			

---

## Supported SQL Servers

The following SQL servers have been tested with CxSAST / CxOSA v9.0.0:

SQL Server	CxSAST	CxOSA	Access Control	Management &Orchestration
2012	V			
2012R2	V			
2014	V			
2016	V			
2017	V			

- AWS RDS can be used (see AWS RDS section in the Installing CxSAST guidelines).
- Azure Managed Instance DBaaS is supported from CxSAST 9.2.
- SQL Express not supported in production due to throughput and 10GB DB size limits imposed by Microsoft.
- For ideal performance we recommend applying MSSQL SP4 when working with MSSQL 2012

---

## Supported Integrations and Plugins

This page is not updated any further. For updated information on integrations and plugins, refer to the [SDLC Documentation](#)

---

## Supported Browsers

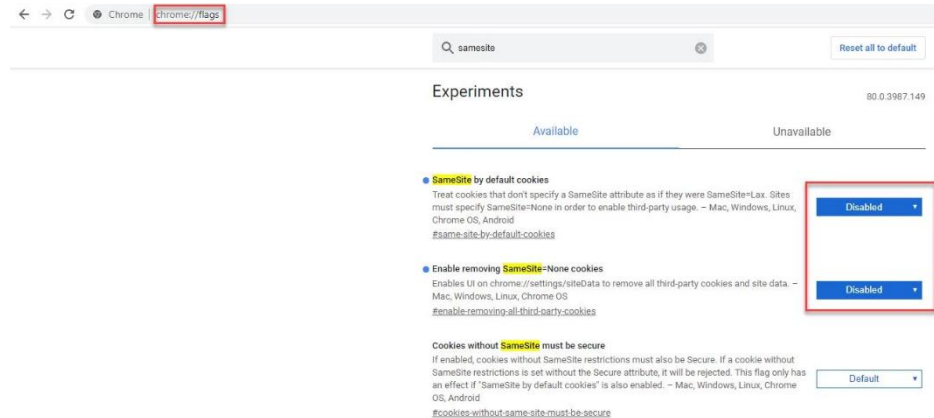
The following browsers have been tested with CxSAST / CxOSA v9.0.0 and Codebashing v3.2.0

SQL Server	CxSAST	CxOSA	Access Control	Management &Orchestration	Codebashing
Chrome	Latest				Latest
Edge	Latest				Latest
Safari	Latest				Latest
Firefox	Latest				Latest

- 'Latest' is defined by the browser vendors. Check with the respective browser vendor for the latest version available.
- If you are using Chrome version 80, refer to the section below.

## Chrome Support

In Chrome, Version 80, the SameSite options must be disabled as illustrated below, otherwise you are unable to log on to the CxSAST Portal.



---

## Preparing the Environment

The following sections include the environmental preparations:

Once you understand [CxSAST 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 2016/2017/2019 for Production.

4. If using **Management & Orchestration**, in order for it to be able to connect, make sure of the following:
  - The SQL Server Browser (Windows service) is enabled and running on the SQL Server for CxARM (**Management & Orchestration**)
  - The TCP/IP port is enabled (in the **SQL Server Configuration Manager > SQL Server Network Configuration** category)
  - Additional ports are opened for Apache Tomcat (HTTP-8080, HTTPS-8443), Remediation Intelligence (8082) and ActiveMQ (61616 for unsecured traffic over ActiveMQ and 61617 for secured traffic over ActiveMQ).
5. For **Access Control**, open the relevant port on the Manager for Engine-to-Manager communication using **Active MQ**:
  - For *unencrypted* TCP transfer, open port **61616**.
  - For TLS *encrypted* transfer, open port **61617**.
6. During the installation process excessive amount of disk read/write operations are performed. These operations can be significantly slowed down by any anti-virus software, and in some cases might even cause the installation process to fail. Therefore it is highly recommended to perform the following:  
On server component hosts:

- a) Stop the antivirus before installation, or prevent it from scanning the following:

**Checkmarx folders:**

C:\CxSrc, C:\ExtSrc, C:\CxReports

**Checkmarx installation directory, e.g.:**

C:\Program Files\Checkmarx\ - C:\Program Files\Checkmarx\

- b) Once installation is complete, restart the antivirus.

7. Install and configure Java.

- The Java installation should be located where permission fulfillment is possible (e.g. C:\Program Files) and not in personal users' folders such as the Desktop folder. The approved and recommended Java version is 1.8. The minimum version for Oracle is 8u241 and for AdoptOpenJdk, it is 8u242.
- In case Java JRE is automatically updated to a new version, you have to manually update the JRE folder path in the CX\_JAVA\_HOME environment variable, otherwise, CxSAST stops operating.

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

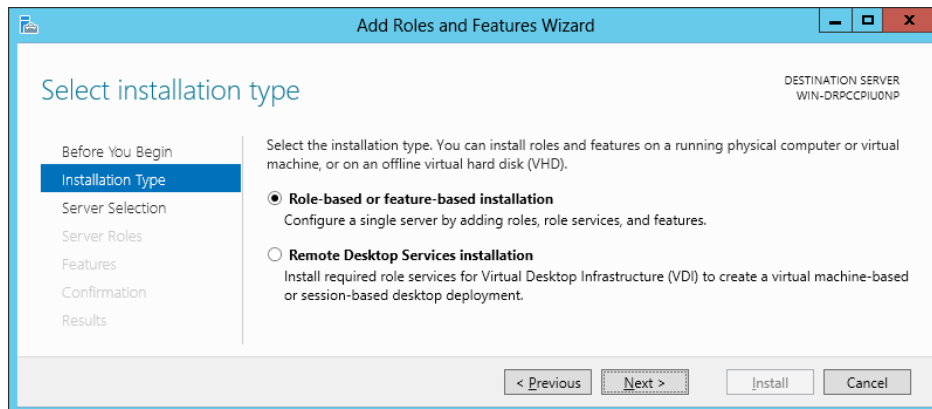
**Installing IIS 10 on Windows 10**

1. Open Control Panel.
2. In Control Panel, click **Programs** and then click **Turn Windows features on or off**.
3. In the Windows Features dialog box, click **Internet Information Services** and then click **OK**.
4. Make sure that the following role services are selected:
  - **IIS Management Console**
  - **IIS Metabase Compatibility**
  - **ASP.NET**
  - **Static Content**

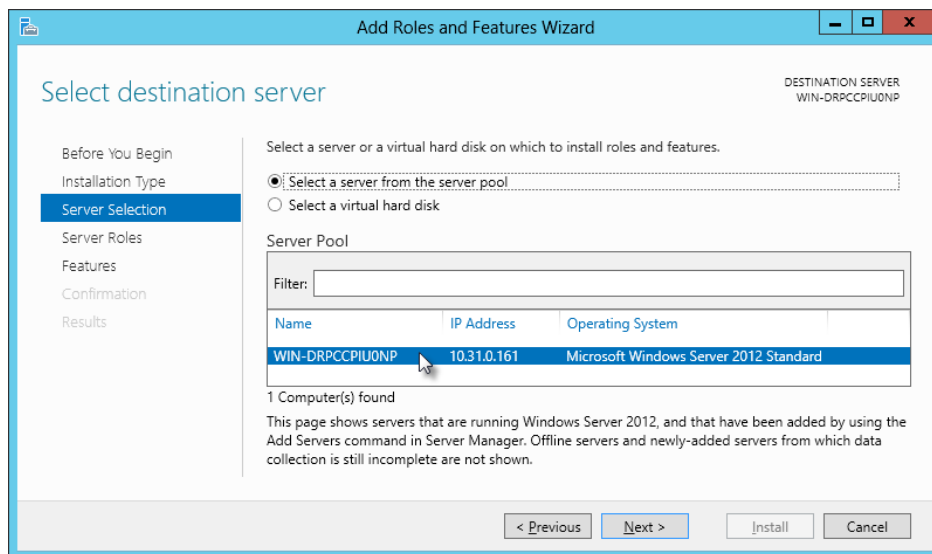
## Installing IIS 8 on Windows Server 2012

- For additional information, refer to <https://docs.microsoft.com/en-us/iis/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012>

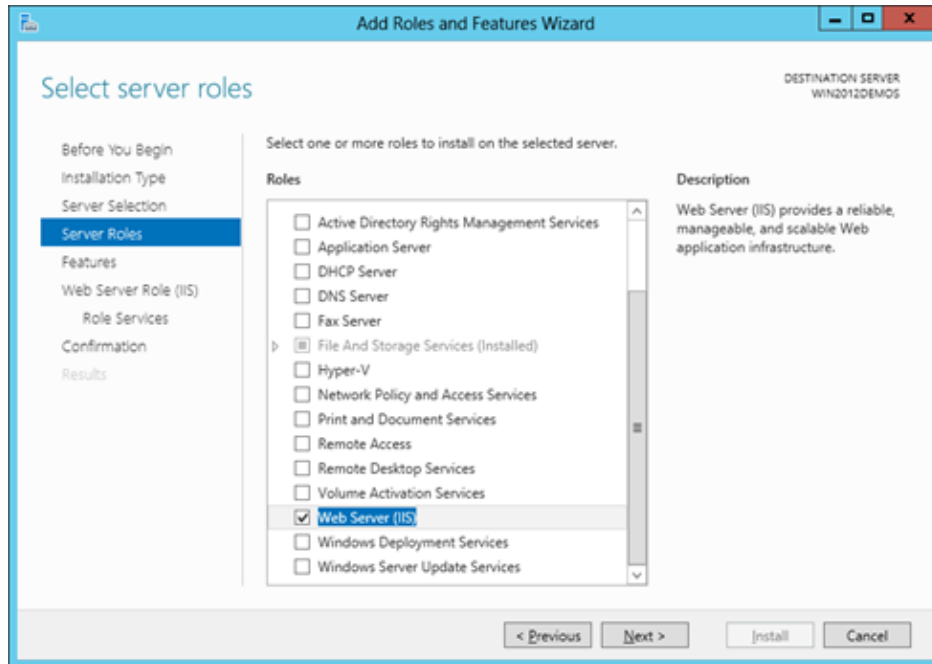
1. Open the **Server Manager > Manage menu > Add roles and features:**
2. Select **Installation Type > Role-based or feature-based Installation**, and click **Next:**



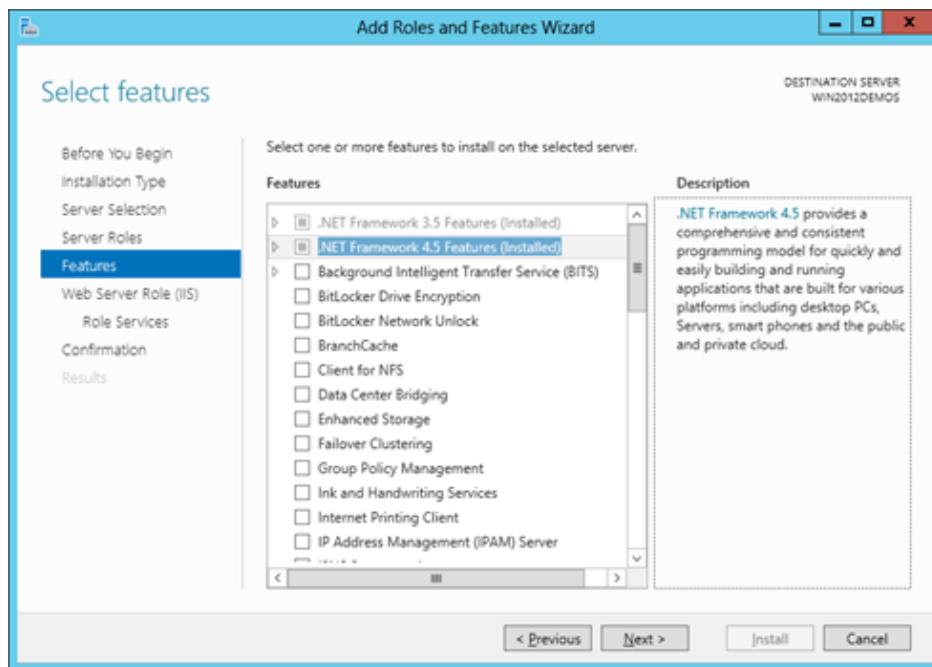
3. From the **Select destination server** window, select the appropriate server (local is selected by default), and click **Next:**



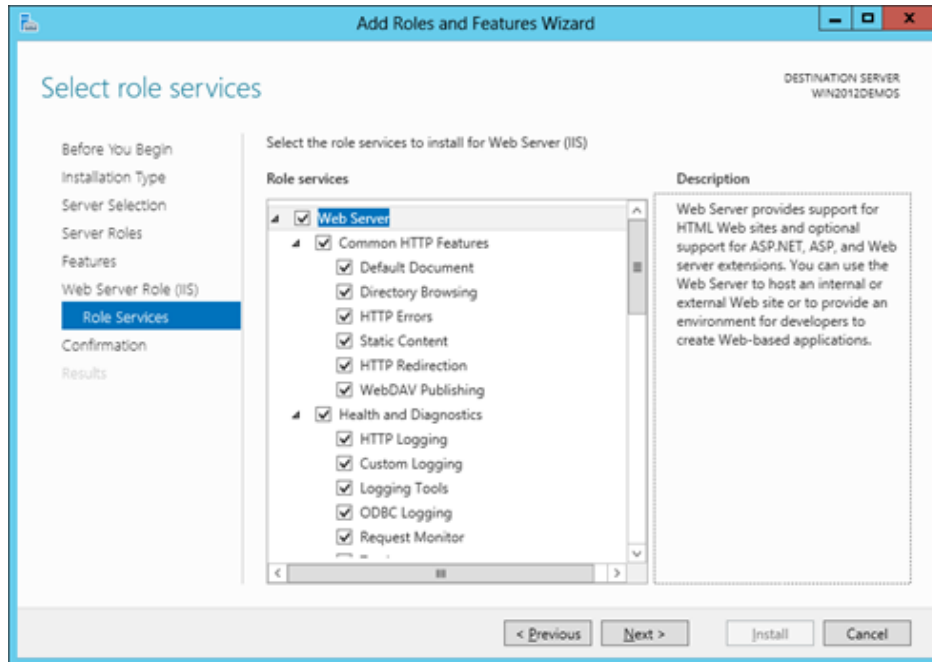
4. From **Select Server Roles** window, select **Web Server (IIS)**, and then click **Next:**



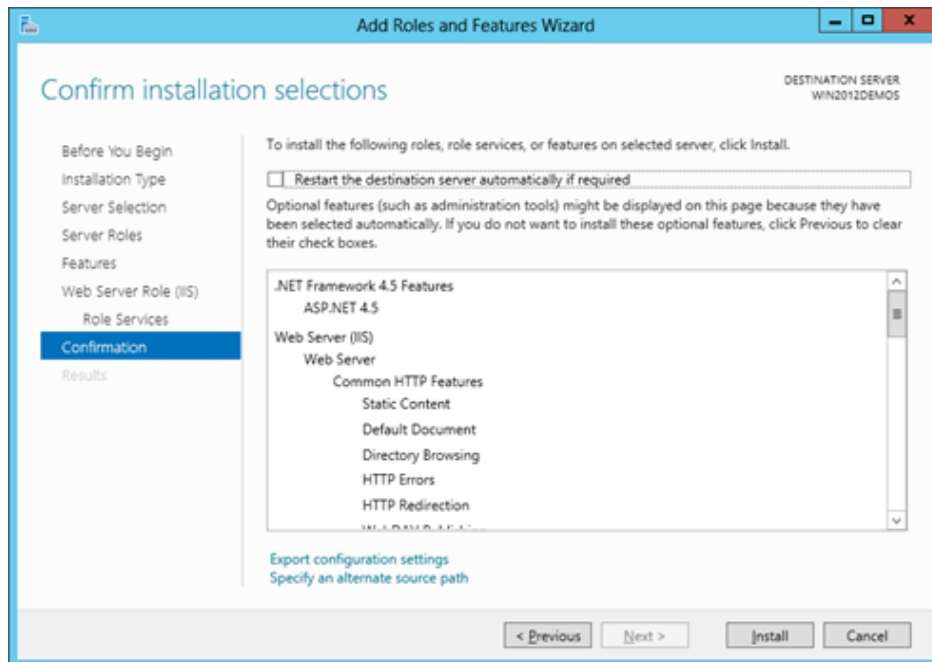
5. From the Select Features window, click **Next**.



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



7. Select the following role services:
  - 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
8. Click **Next**.
9. From **Confirm installation selections** window, review the selections. To edit selections, click **Previous**:



10. Click **Install**.
11. From the **Installation progress** window, view the installation progress.
12. Click **Close**.
13. Confirm that the Web server works by using <http://localhost>

#### Installing 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 this case, make sure to include IIS with the following:

- IIS Management Console
- Static Content
- ASP.NET 4.5 with all dependencies
- IIS 6 Metabase Compatibility
- .Net Framework 4.5 Features -> WCF Services -> HTTP Activation

- For additional information, refer to <https://docs.microsoft.com/en-us/iis/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2>

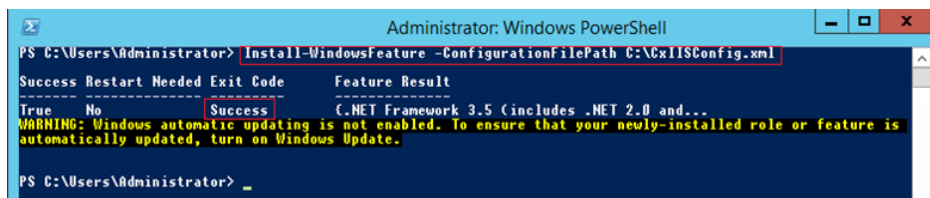
➤ **To configure IIS 8.5 using the Checkmarx configuration file:**

1. Download [CxIISConfig.xml](#).
2. Run **Windows PowerShell** as an Administrator:



3. In Windows PowerShell, run the following:

**Install-WindowsFeature –ConfigurationFilePath <path>\CxIISConfig.xml**  
 where <path> is the path to the directory where you put the configuration file.



```

Administrator: Windows PowerShell
PS C:\Users\Administrator> Install-WindowsFeature -ConfigurationFilePath C:\CxIISConfig.xml
Success Restart Needed Exit Code      Feature Result
-----
True     No           Success      (.NET Framework 3.5 (includes .NET 2.0 and...
WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is
automatically updated, turn on Windows Update.
PS C:\Users\Administrator> _
  
```

### Installing IIS 10 on Windows Server 2016

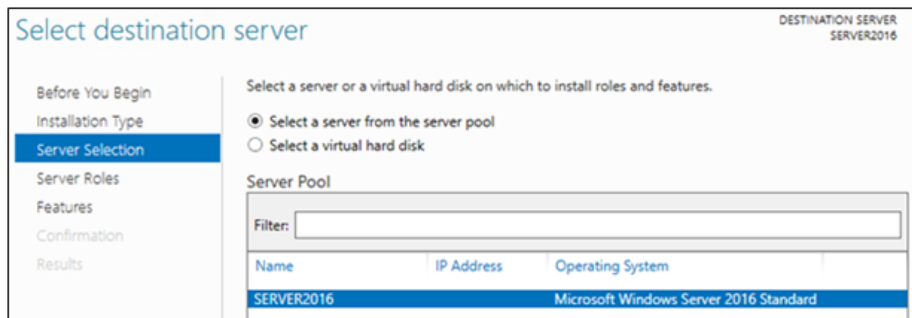
1. On your Server Manager Dashboard go to: **Manage > Add Roles and Features**. The Add Roles and Features wizard opens:



2. On the Before you Begin page click **Next**.
3. On the Select Installation Type page, select **Role-Based or feature-based installation**, and then click **Next**.

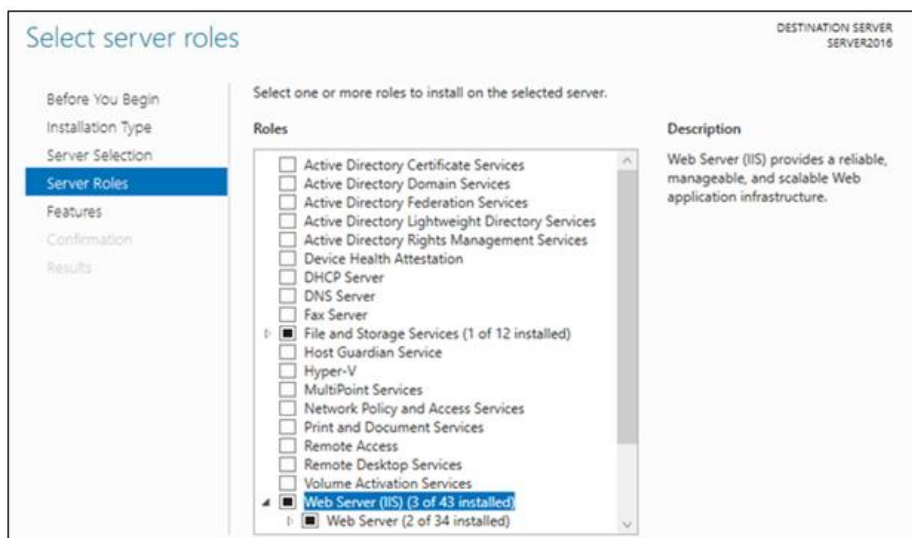


- On the Server Selection page, select the server to perform the installation, and then click **Next**.



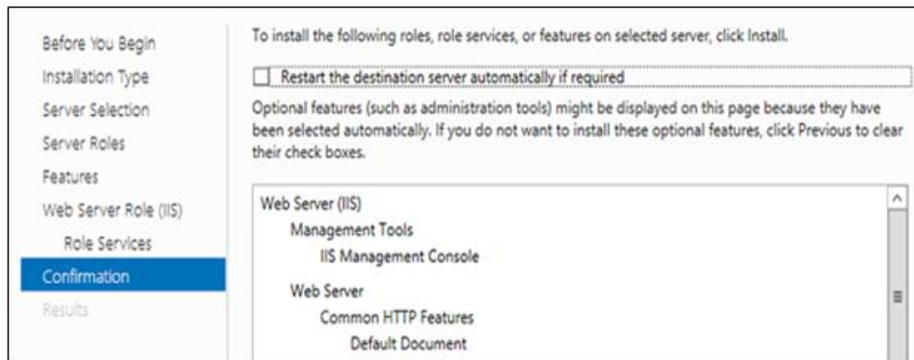
- On the Server Roles page, select **Web Server (IIS)** and the following role services:
  - IIS Management Console
  - IIS Metabase Compatibility
  - ASP.NET
  - Static Content

- Click **Next**.

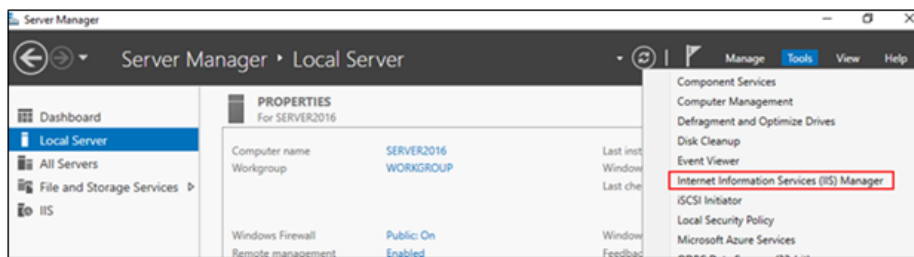




7. On the Features Page click **Next**.
8. On the Confirmation page, review and then click **Install** to complete the IIS installation.



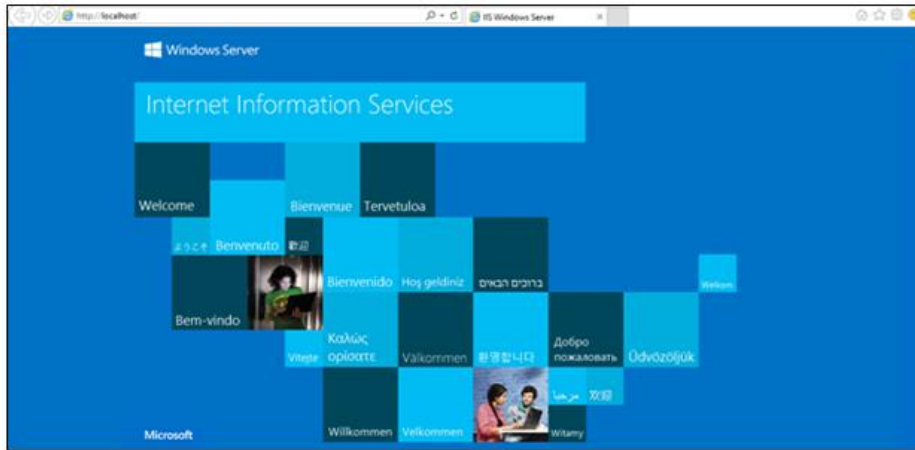
9. Once the Web Service Role (IIS) is installed, browse for the **IIS Manager** on the Start menu, or by clicking **Tools**.



10. Now you can utilize the IIS manager to navigate and create your new website.



11. Confirm that the Web server works by using <http://localhost>.



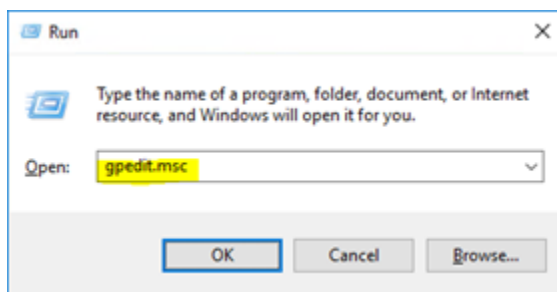
For correct synchronization the Checkmarx Server/CxAudit and the Database must be on the same time zone.

### Enabling Long Path Support in Windows 10 and Server 2016

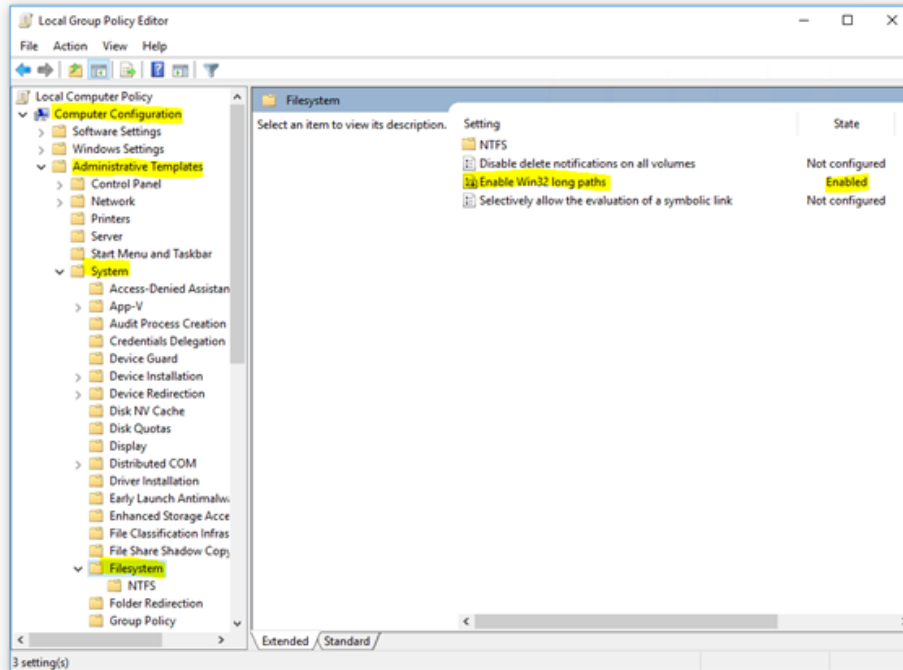
Traditionally, Windows operating system does not support path or file names with more than 260 characters. However, Windows 10 and Windows Server 2016 now provide support for these 'long paths'.

➤ **To enable long path support:**

1. In Windows 10/Server 2016, open the Run dialog (**Start > Programs > Accessories > Run**).



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



3. Navigate to: **Local Computer Policy > Computer Configuration > Administrative Templates > System > Filesystem.**
4. Enable the **Enabling Win32 long paths** key. The key updates instantly and no restart is required.

- Long Path support in Windows 10 starts with Build 14352.

## Installing CxSAST

The following pages describe the Installation procedures of releases of CxSAST:

Before installing CxSAST, make sure that you understand the [System Architecture](#) and that your server host(s) complies with the [Server Host Requirements](#). To install CxSAST, you have to download and extract the installation archive and install required third-party components.

- To install and configure high availability solutions, refer to the relevant instructions. A diagram that outlines the architecture for high availability solutions is available here.

---

## Installation Permissions

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

### SQL Database

If the database uses **Windows domain authentication**, the station 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, refer to [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. When installing SQL, you are asked to define a password to access the internal CxARM database. This password must not exceed 32 characters.

**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. Make sure that the SQL User's password does not consist of more than 32 characters. This may mean that you have to reset this password **before** you start upgrading.

To change the user credentials used for CxDB connectivity, refer to [Configuring User Credentials for CxDB Connectivity](#).

## AWS RDS

DBaaS is not supported natively, but AWS RDS can still be used. To run RDS, you need to create three databases, CxDB, CxActivity and CxARM. Provide the user with the Checkmarx dbo privileges for the newly created databases. Run the installer again and when the installation connects to the database and when a message appears that the three databases are already existing, click **Continue**. Once the installation is complete, the RDS starts running.

---

## Preparing for Installation

Follow the instructions below to obtain/validate your license and make the installation package available.

### Obtaining and Validating a License

It is recommended to obtain a license before you start your installation. This way you will be able to provide the license during the installation and be able to use the product immediately.

Your CxSAST license is tied to a specific station (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.

To receive your license, submit the Hardware ID to your technical contact or sales manager. If you are not sure whom to send the Hardware ID to, [open](#) a support ticket.

If CxSAST is already installed and you have not yet obtained a permanent CxSAST license, submit the Hardware ID to your Checkmarx sales representative or [open](#) a support ticket to obtain your production license file. The Hardware ID can be found at **Start > All Programs > Checkmarx > HardwareId**.

### Making the Installation Package Available

Follow the instructions below to make the installation package available on each server component host.

1. Download the [CxSAST installation package](#). The installation package downloads as a zip archive.
2. Copy the zip archive to each server component host and extract it there to a folder of your choice. To extract the zip archive, you may have to enter a password that has been provided by [Checkmarx support](#)
3. Install the required third-party components and then start installing CxSAST by running **CxSetup.exe** .

## Prerequisites

If not already installed on the server host, you have to make the third-party components listed below available before you can complete installing the CxSAST application. The required resources and installation packages are available in the extracted CxSAST installation package in a folder called **third\_party**.

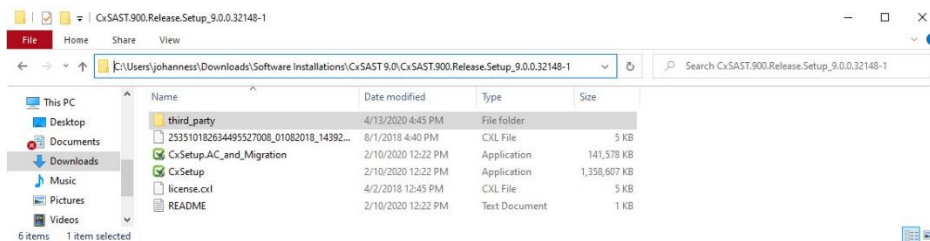
- **C++ Redist 2010 and 2015 SP3**
- **IIS v7.0 or higher**
- **NET Core 2.1.16 (or higher 2.1.x versions) Runtime & Hosting**
- **MS SQL**
- **Java JRE 1.8.0 (64-bit)**

For additional information, refer to [Server Host Requirements](#).

- The third-party components can be installed and made available as part of the CxSAST setup at the Prerequisite Check stage, although it is recommended to do it beforehand. Additional information on these third-party components are available under Preparing the Environment
- The approved and recommended Java version is 1.8. The minimum version for Oracle is 8u241 and for AdoptOpenJdk ,it is 8u242
- CxSAST requires the 64-bit version of Java. The 32-bit version results in an error during the installation.

## IIS

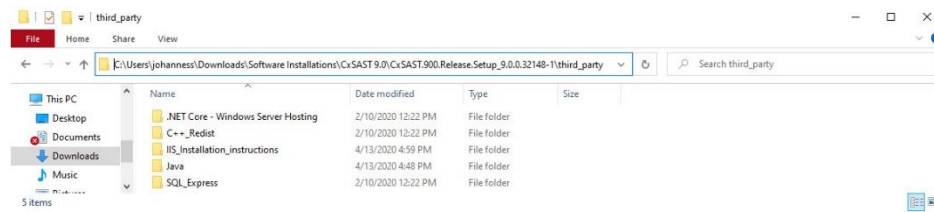
1. Navigate to the **third\_party** folder in the setup folder of your CxSAST installation package, for example **C:\Users\<<name>\Downloads\Software Installations\CxSAST 9.0\CxSAST.900.Release.Setup\_9.0.0.32148-1**.



2. Navigate to the **IIS\_Installation\_instructions** folder and refer to the instructions there on installing and enabling **IIS** for the Windows version in use.

## C++, .NET, MS SQL

1. In the **third\_party** folder, navigate to the folder with the first component to install.



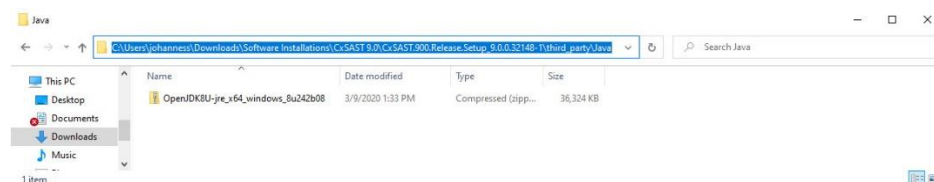
2. Run the setup and follow the onscreen instructions.
3. Repeat this for the remaining components that have to be installed yet.
  - When installing SQL, you are asked to define a password to access the internal CxARM database. This password must not exceed 32 characters.
  - If you upgrade, you may have to reset the existing password as passwords could exceed 32 characters in previous versions.

## Java

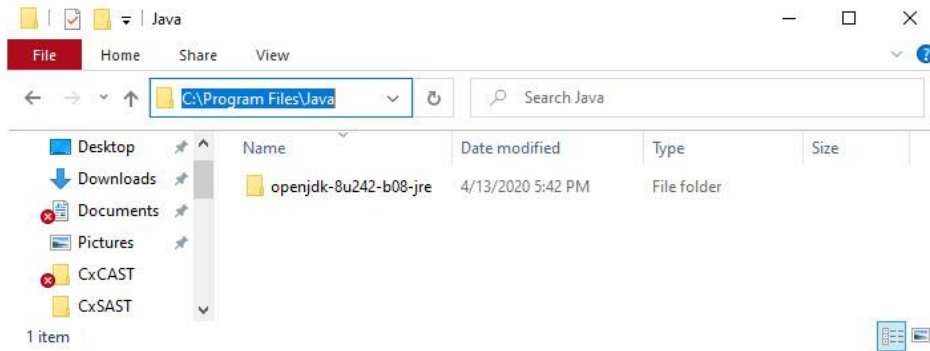
The files of the required Java Runtime Environment are available in a zip archive and are only copied into a new folder and not installed.

### ➤ To make the Java Runtime Environment available:

1. In the **third\_party** folder, navigate to the Java folder. In this folder, there is one zip file listed.



2. Open the zip archive and extract its content to a folder of your choice. It contains a folder called **openjdk-8u242-b08-jre** that accommodates all the required files for installing and operating CxSAST successfully. The **openjdk-8u242-b08-jre** folder is also referred to as the JRE folder throughout this document.
3. Copy the **openjdk-8u242-b08-jre** to a non-personal folder under a folder created for Java application. This folder may for example be **<root directory>:\Program Files** on your PC.



## Installing CxSAST

### Prerequisites and Recommendations

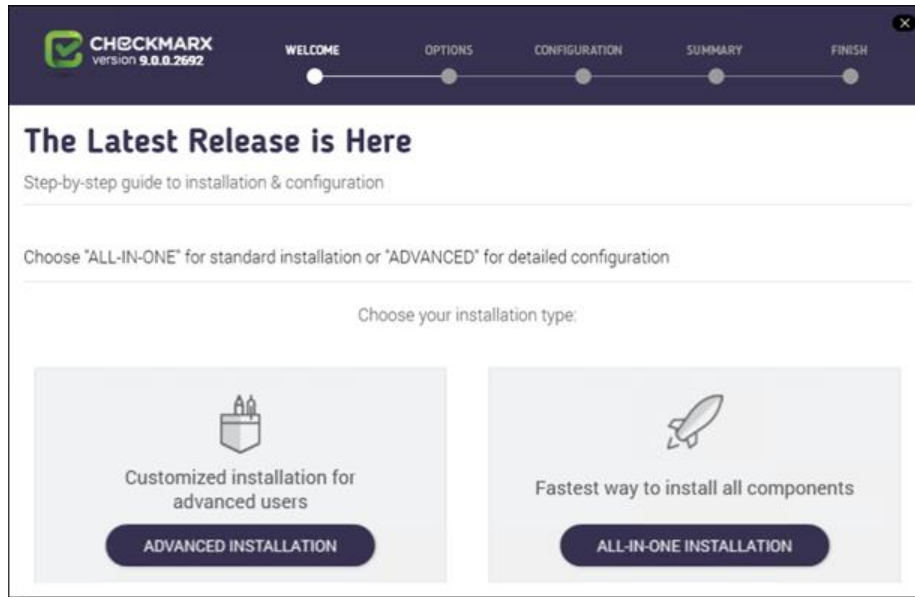
- The required Web Server for Checkmarx is **IIS Server**. If the IIS Server still missing, it is be installed by the CxSAST installer which requires the Windows installation media to be accessible.
- SQL 2012 Express SP2 is included with the CxSAST installer. It is installed in the event that no other version of SQL is already installed.

### Installation

- For upgrading from v8.7 or prior versions, you are first required to install v8.8/v8.9 and only then proceed with the v9.0 installation. For more information, refer to Installing CxSAST (v8.8.0 to v8.9.0).
- For upgrading from v8.8/v8.9 to v9.0 you are first required to perform the Access Control data migration procedure. For more information, refer to Access Control Data Migration Installer.

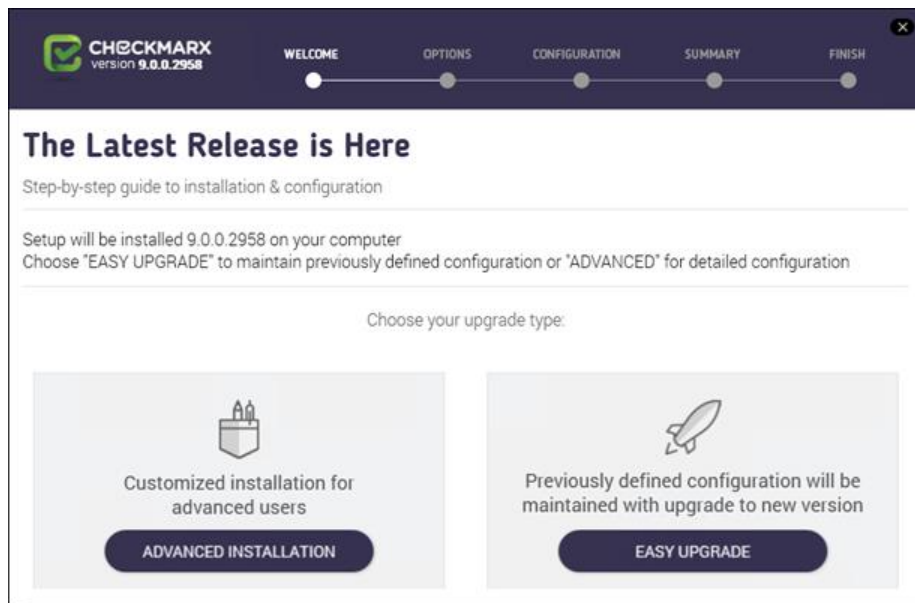
1. Once you have downloaded the CxSAST Installation package and made the third-party components available, run the **CxSetup.exe**. The **Checkmarx Welcome** window is displayed.



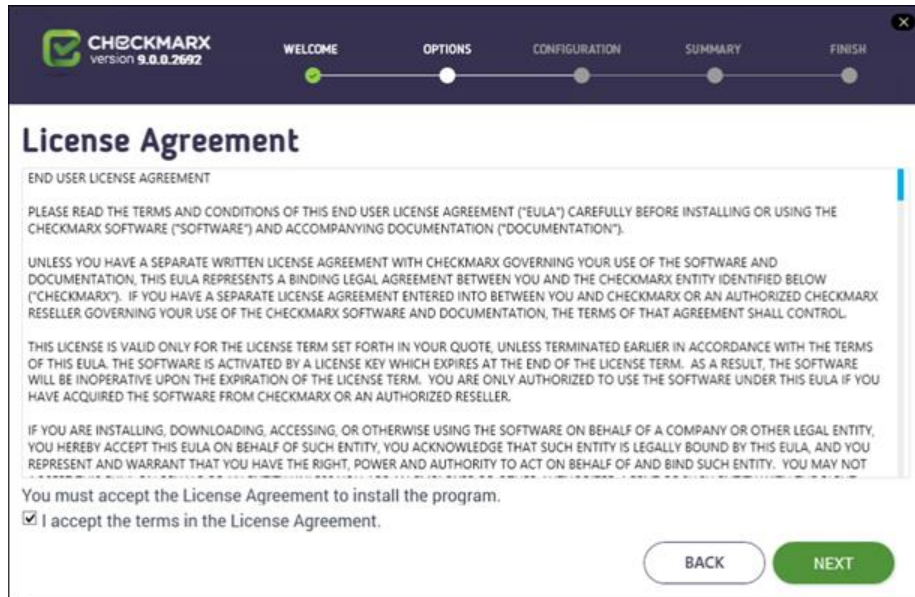


2. Click **ALL IN ONE** to continue, **ADVANCED** to define additional setup options, or **X** to exit.

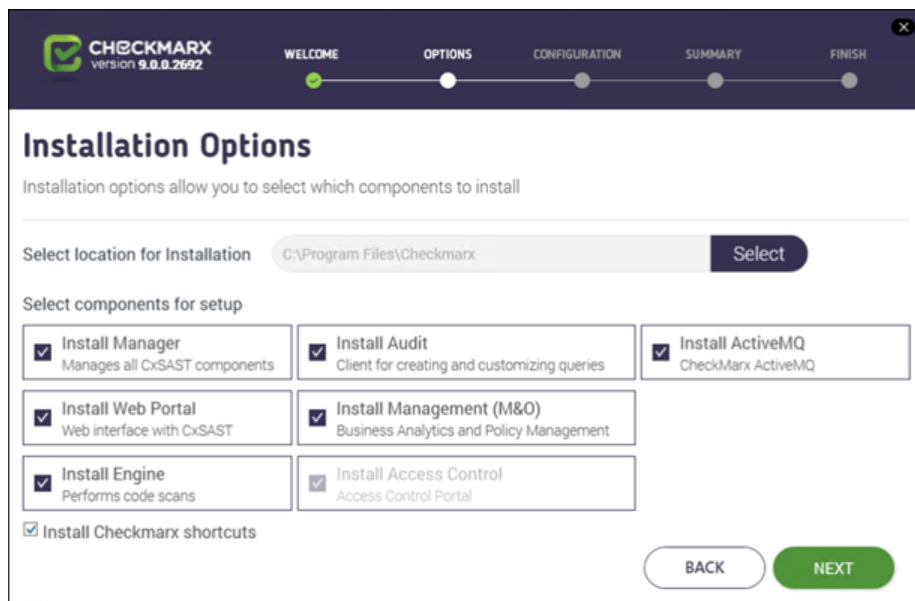
For upgrades, the options are **EASY UPGRADE** to continue or **ADVANCED** to define additional setup options.



In both instances, the **Checkmarx License Agreement** window is displayed.



3. Review and accept the license agreement by checking the '**I accept the terms in the License Agreement**' checkbox. Click **Next** to continue.
4. If you selected **ADVANCED**, the additional **Installation Options** window is displayed.



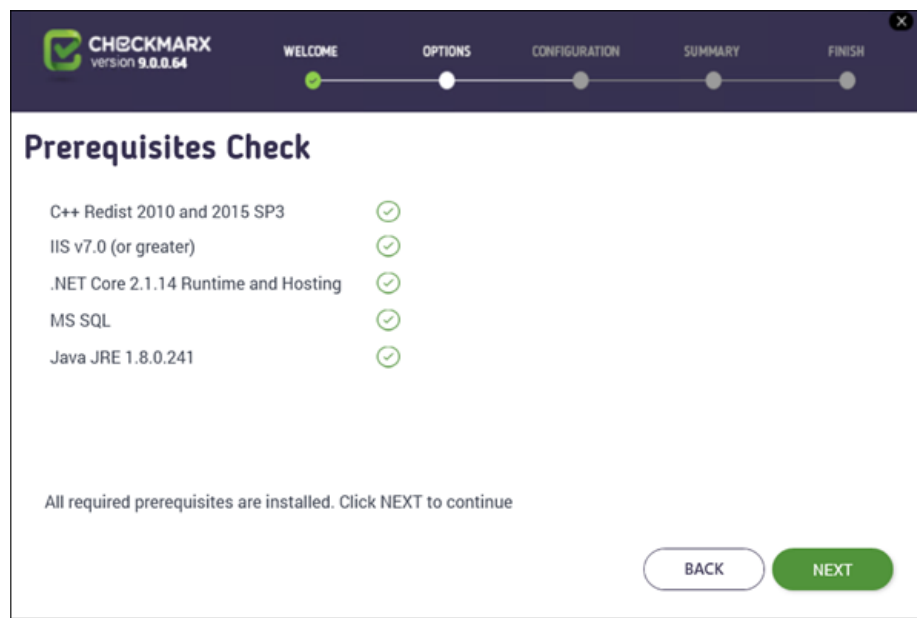
5. Click **Select** to define the CxSAST installation location.

- To avoid permission restrictions, install CxSAST in <root directory>:\Program Files .
- For upgrades, previously installed location settings and product components are loaded from the existing configuration and cannot be changed. You can however install or remove product components by using the Modify option. For more information, refer to **Modifying CxSAST**.

6. Select the required components for this installation from the available list.
  - **POC/Evaluation** - Select to install Audit, Engine, Manager, Management and Orchestration, ActiveMQ and Web Portal
  - **Distributed Architecture** - Select to install either Engine or Manager, Management and Orchestration, ActiveMQ and/or Web Portal

For upgrading Manager/Portal server in a distributed environment, the ActiveMQ component is automatically selected when using the 'Easy Upgrade' option.

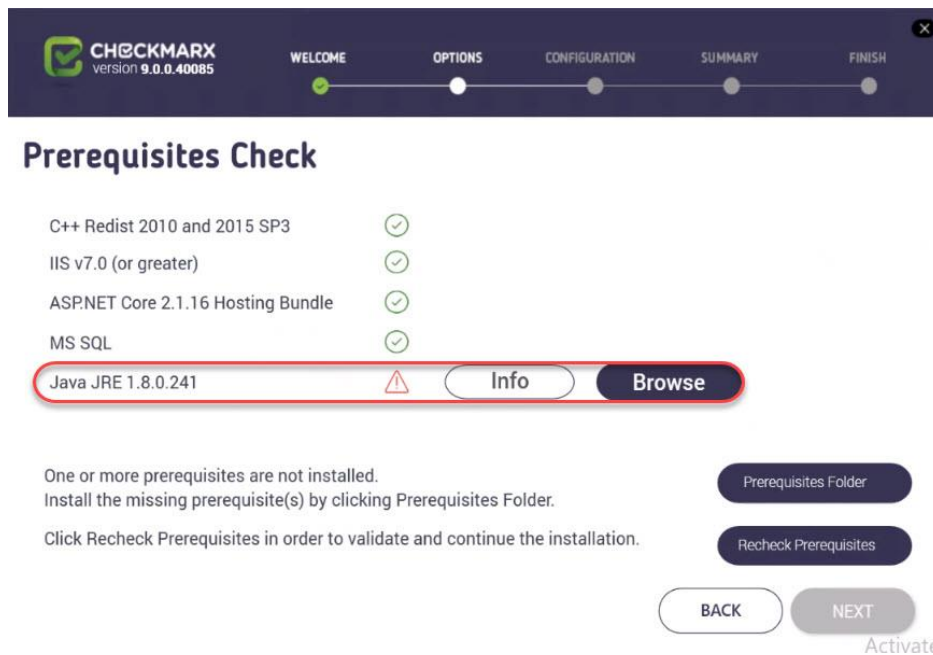
- **Centralized Architecture** - Select to install Engine, Manager, Management and Orchestration, ActiveMQ and Web Portal ([Audit](#), if you plan to create and customize queries on the host).
  - **CxEngine Server only** - Select to install Engine (see [Adding a CxEngine Server](#)).
7. To add related shortcuts on your desktop, check **Install Checkmarx Shortcuts**.
  8. Click **Next**. The **Prerequisites Check** window is displayed, indicating the status of all required third-party components.



Components that are already in place are labeled accordingly

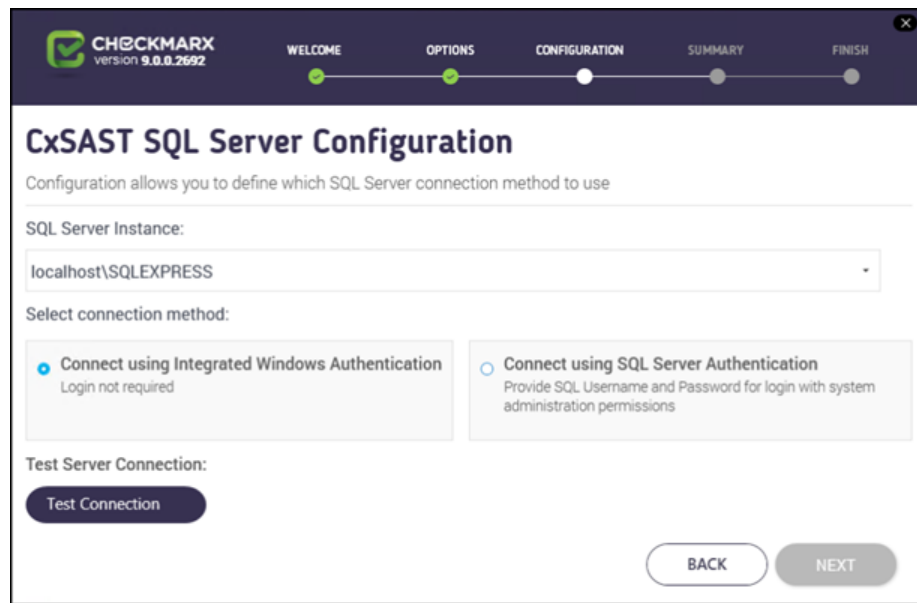
Missing component are labeled . To add them, do the following:

- For any missing component (except the Java Runtime Environment), click the Prerequisites Folder button to navigate to the supplied components and install each one separately. To do so, follow the on-screen instructions.
- For the required Java Runtime Environment (JRE), click **Browse** and select the entire JRE folder (and not only the bin folder) that you copied to your station (e.g. **C:\Program Files\openjdk-8u242-b08-jre**, **C:\Program Files\Java\jre1.8.0\_241** or **C:\Program Files\Java\jdk1.8.0\_241\jre**). These instructions assume that you have extracted and copied the content of the provided ZIP archive to the relevant location.  
If you did not make the Java files available, refer to the instructions at the top to do so and then click **Recheck Prerequisites** to repeat the validation process.
- All prerequisites must be labeled , otherwise the setup cannot be completed and CxSAST is not installed.



- The recommended Java version is 1.8. The minimum version for Oracle is 8u241. For AdoptOpenJdk, the minimum version is 8u242. Verify that the minimum version is installed on your server before continuing.
- In case Java JRE is automatically updated to a new version, you have to manually update the JRE folder path in the CX\_JAVA\_HOME environment variable, otherwise CxSAST stops operating.

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

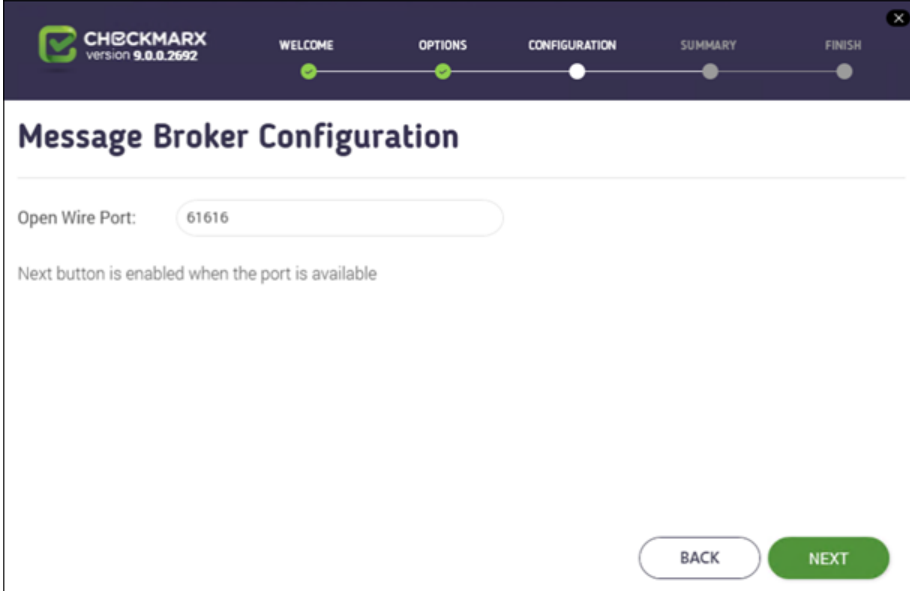


10. Select the Server from the SQL Server Instance list. If using a non-standard database port, provide the server name with a comma followed by the port number (e.g. LOCALHOST\SQLEXPRESS,25).

- For upgrades, previously defined SQL Server instance settings are loaded from the existing configuration and cannot be changed.

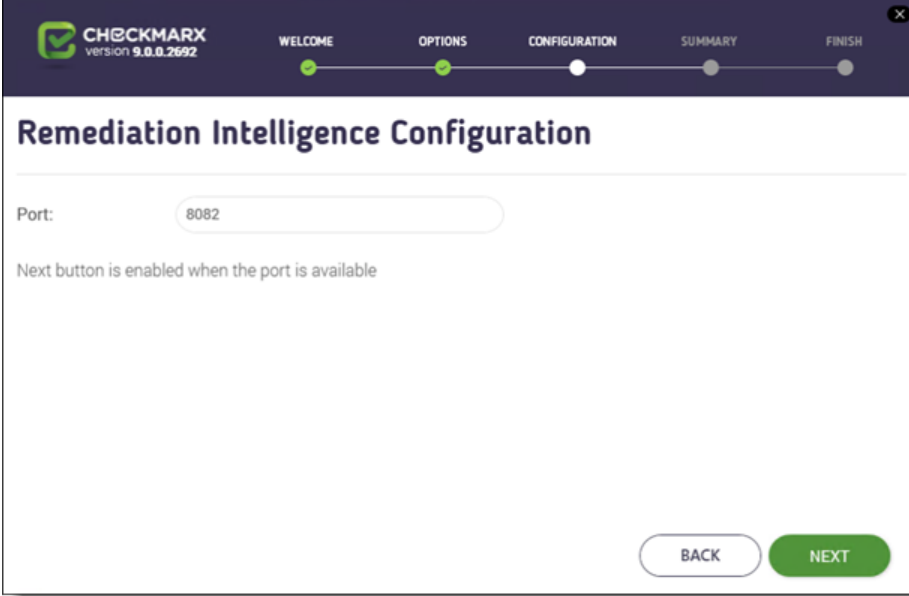
11. For **CxSAST**, define a connection to the installed SQL Server or to any other SQL server on your network, by selecting one of the following:
  - **Connect using Integrated Windows Authentication** (login not required)
  - **Connect using SQL Server Authentication** (provide SQL user name and password for login with SA permissions).
12. Click **Test Connection**. A "**Connection OK**" message is displayed upon confirmed connection to the CxSAST SQL Server.
13. If the "SQL Connection Test Results" message indicates that connection to the SQL Server has failed, verify the following:
  - Host, port and login credentials are correct.
  - The station is a member of a Windows domain (if not, either join the station 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).A notification displays, if existing SQL Express files are detected.

14. Click **OK** on the message, and then click **NEXT** to continue. The **Message Broker Configuration** window is displayed.



- The default OpenWire port is 61616.
- The NEXT button is enabled when the default port is available. If unavailable, define another available port.
- In case the ActiveMQ is uninstalled and reinstalled using a non-default port, a manual update in the DB is required to match the change - Databases > CxDB > Tables > CxComponentConfiguration > ActiveMessageQueueURL > Key Value (e.g. tcp://<AMQ\_URL>:<non-default\_port>)
- Make sure that port 61616 is open in all relevant firewalls between the ActiveMQ server and the following components:
  - CxManager servers (for Access Control, Scan Manager and Results Services). This includes high availability configurations with multiple CxManagers. For additional information on configuring Access Control and ActiveMQ for high availability, refer to Configuring Access Control for High Availability Environments and Configuring ActiveMQ for High Availability Environments.
  - CxEngine servers
  - M&O server

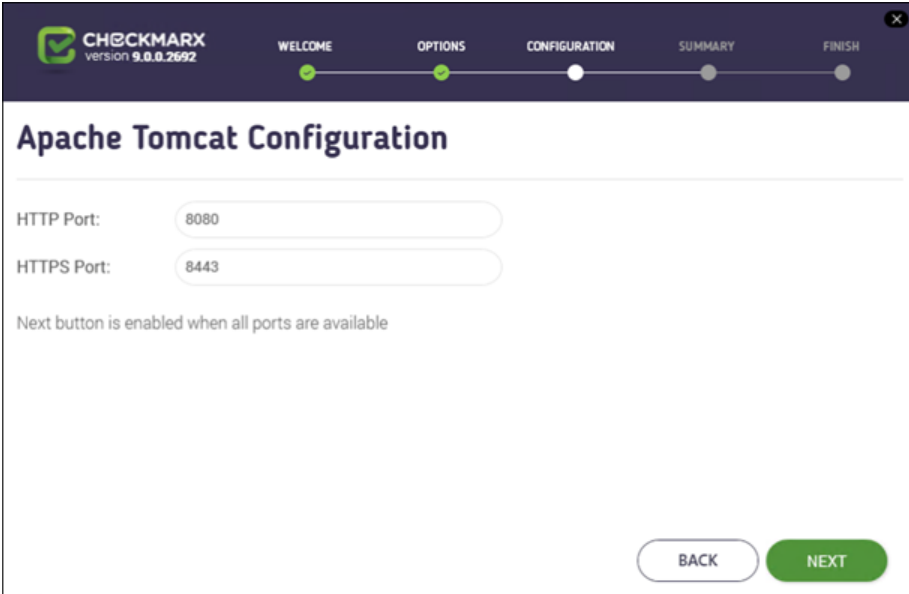
15. Click **Next**. If installing Management and Orchestration, the **Remediation Intelligence Configuration** window is displayed.



The screenshot shows a configuration window titled "Remediation Intelligence Configuration". At the top, there is a dark blue header with the Checkmarx logo and version "9.0.0.2692". A progress bar below the header has five steps: WELCOME, OPTIONS, CONFIGURATION (current), SUMMARY, and FINISH. The main content area has a "Port:" label followed by a text input field containing "8082". Below the input field, it says "Next button is enabled when the port is available". At the bottom right, there are two buttons: "BACK" (disabled) and "NEXT" (enabled).

- In older versions and previous builds of the current version of CxSAST, Automated Prioritization was called Remediation Intelligence. The screen image below still refers to this previous name.
- The default port is 8082.
- The NEXT button is enabled, if the default port is available. If unavailable, define another available port.

16. Click **Next**. If installing Management and Orchestration, the **Apache Tomcat Configuration** window is displayed.

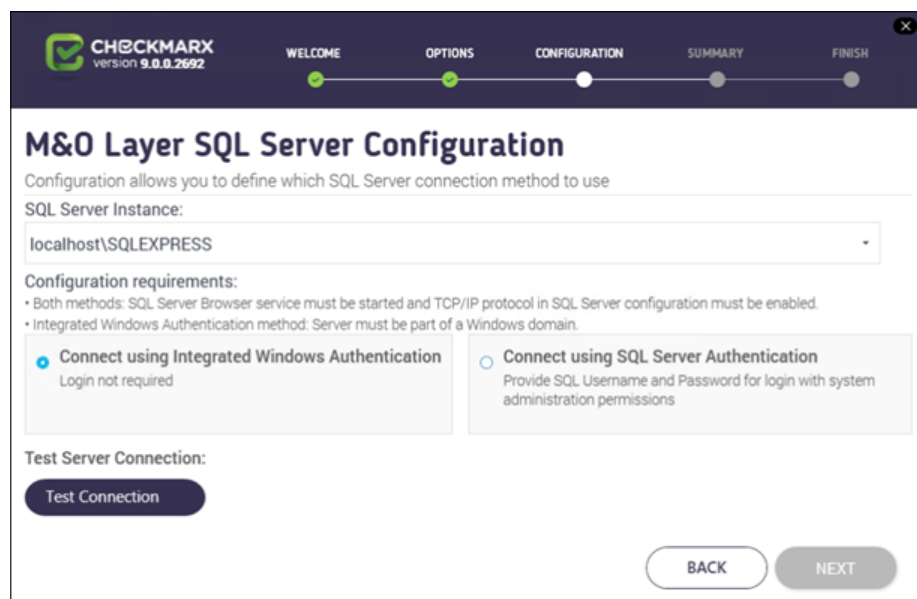


The screenshot shows a configuration window titled "Apache Tomcat Configuration". At the top, there is a dark blue header with the Checkmarx logo and version "9.0.0.2692". A progress bar below the header has five steps: WELCOME, OPTIONS, CONFIGURATION (current), SUMMARY, and FINISH. The main content area has two labels: "HTTP Port:" followed by a text input field containing "8080", and "HTTPS Port:" followed by a text input field containing "8443". Below the input fields, it says "Next button is enabled when all ports are available". At the bottom right, there are two buttons: "BACK" (disabled) and "NEXT" (enabled).

- Default ports (as displayed) are:
  - HTTP port is 8080
  - HTTPS port is 8443
- The NEXT button is enabled when the default port(s) are available. The installer verifies that ports are not blocked, but does not check, if ports are part of IIS bindings. If you suspect that one of the relevant ports is part of IIS bindings, open IIS and check it. You can only complete the installation, if ports are not blocked and if they are not part of IIS bindings. If port(s) are unavailable, define other available port(s) in the respective Port fields.

17. Click **NEXT**. If installing Management and Orchestration, the **M&O Layer SQL Server Configuration** window is displayed.

- If the M&O database resides on a separate server, SQL Server Instance must read <IP address of the M&O DB server>\SQLEXPRESS. If it reads localhost\SQLEXPRESS instead, cancel the setup and start it again.



18. Select the Server from the SQL Server Instance list. If using a non-standard database port, provide the server name with a comma followed by the port number (e.g. LOCALHOST\SQLEXPRESS,25).

- For upgrades, previously defined SQL Server instance settings are loaded from the existing configuration and cannot be changed, unless the Management and Orchestration component was only added in the latest upgrade.

19. For **Management and Orchestration**, define the SQL Server connection by selecting one of the following:



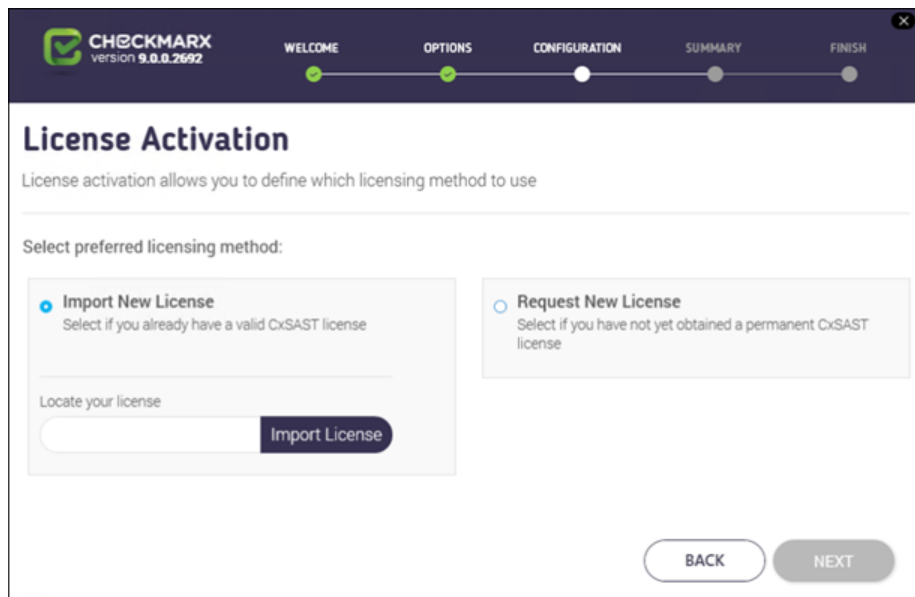
- **Connect using Integrated Windows Authentication** (login not required)
- **Connect using SQL Server Authentication** (provide SQL user name and password for login with SA permissions)

- For M&O Layer SQL Server connectivity, both Dynamic and Static port configurations are supported. For more information, refer to Configuring Management & Orchestration SQL Server for Dynamic and Static Port Connectivity.

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

- If the "SQL Connection Test Results" message indicates that connection to the SQL Server has failed, verify the following:
  - Host, port and login credentials are correct
  - The station is a member of a Windows domain (if not, either join the station 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).

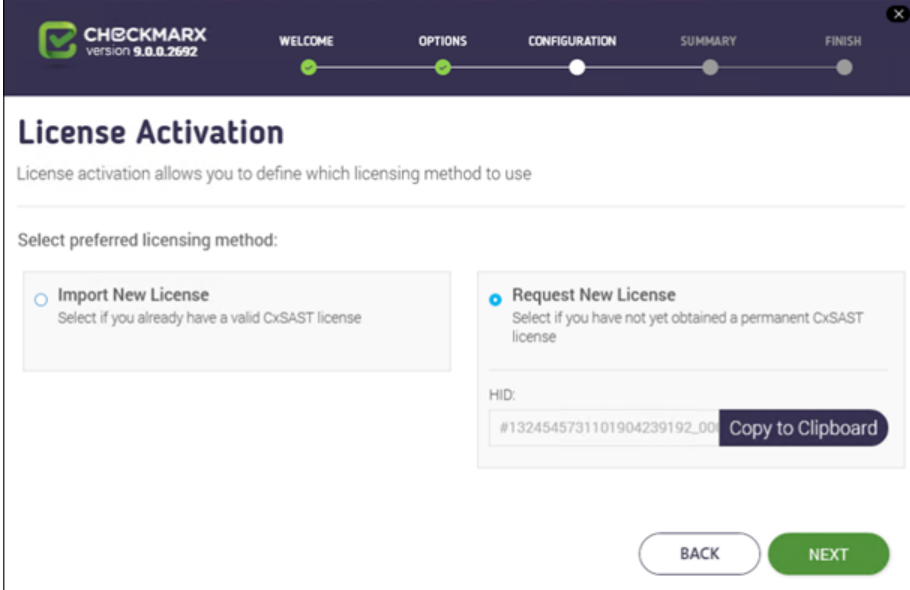
21. Click **OK** on the message, and then click **NEXT**. The **License Activation** window is displayed.



- For upgrades, the license information (if it exists and is valid) is automatically loaded from the existing configuration and the License Activation window is not displayed.

22. 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 and click **Open**.
- **Request New License:** If you have not yet obtained a permanent CxSAST license, select **Request New License** and then click **Copy to Clipboard**. Send the copied Hardware ID (HID) to your Checkmarx sales representative or [open a support ticket](#)



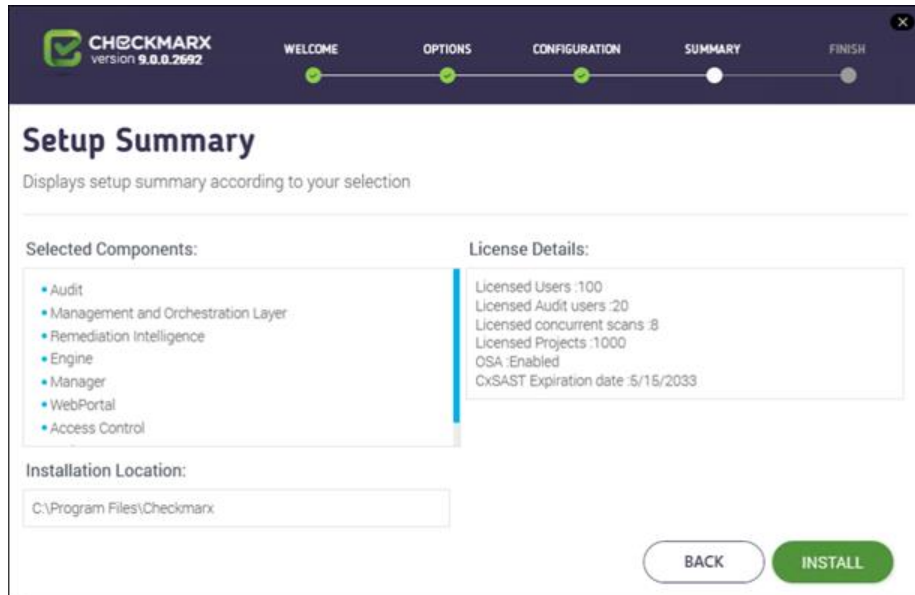
- Once you have obtained a new or updated Checkmarx license, you can use the license importer to import the license into CxSAST. For more information, refer to [Updating the CxSAST License](#).

23. Click **NEXT** to continue.

- If your license does not 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 [open a support ticket](#).
- If the default port 80 is occupied, the **Validate Port** window is displayed. If required, select another port and click **Validate Port**.
- 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.

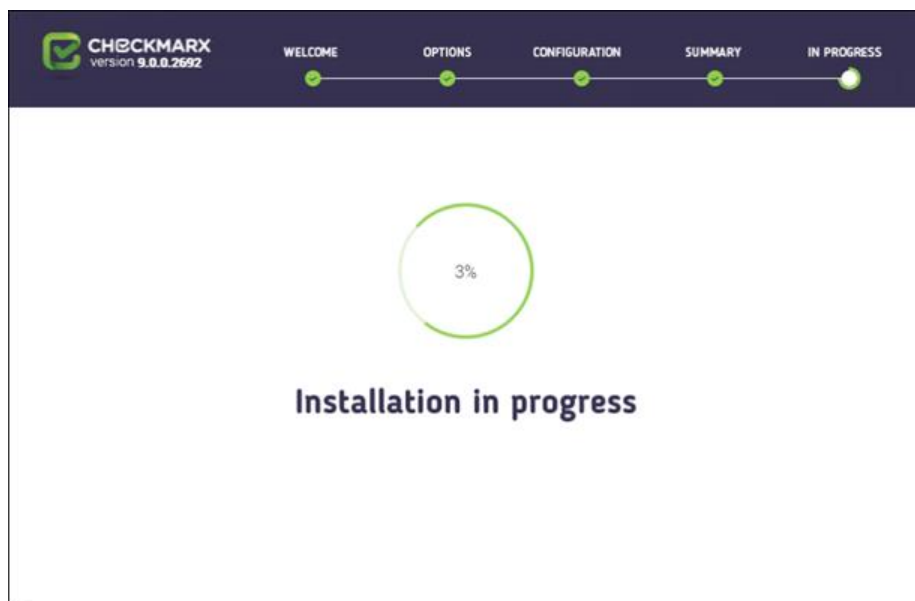
24. Click **NEXT** to continue. The **Setup Summary** window is displayed.



25. Check the setup summary according to your component selection and license details.

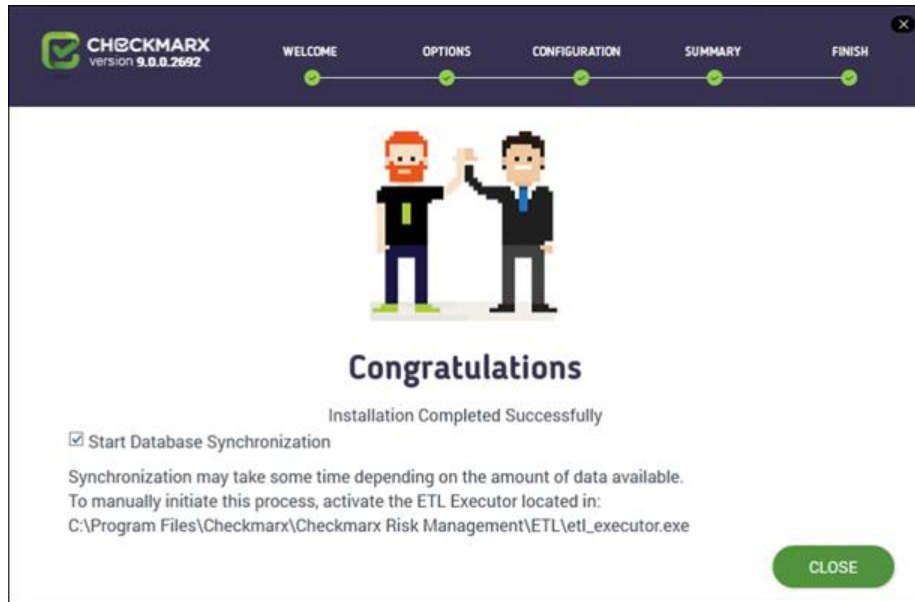
- For upgrades, the license information is not displayed because it has already been loaded from the existing configuration.

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



If the installation fails, the "**Setup failed**" message is displayed. For more information, see the installation logs. If you need further assistance, please [open a support ticket](#)

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



If you installed Management and Orchestration on the Congratulations window, the **Start Database Synchronization** checkbox is selected by default. This enables Management and Orchestration automatically by initializing the synchronization process. This process may take some time, depending on the amount of data being synchronized.

To perform the database synchronization at another time, clear the checkbox, and click **CLOSE**. At a later time, use the ETL tool to perform the synchronization, located at <Installation folder>\Checkmarx\Checkmarx Risk Management\ETL\etl\_executor.exe, for example C:\Program Files\Checkmarx\Checkmarx Risk Management\ETL\etl\_executor.exe

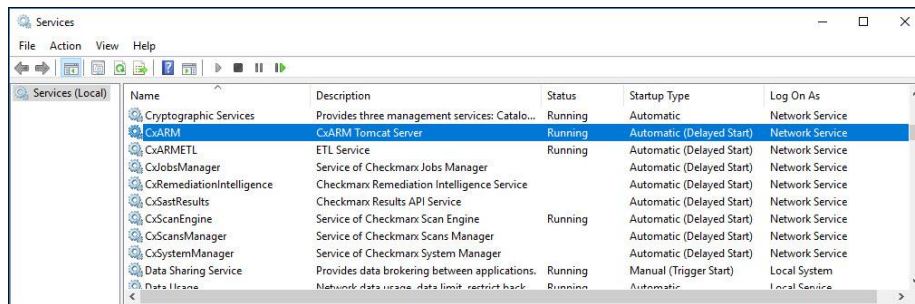
27. **To continue now with the database synchronization**, leave the checkbox checked and click **CLOSE**. If required, reboot the server (you receive a prompt, if rebooting is necessary). The database synchronization starts automatically.

For more information about installing Management and Orchestration, see [Installing Management and Orchestration](#).

- If attempting to install CxSAST with an existing Management and Orchestration database, the subsequent ETL DB sync will fail, due to a limitation in Management and Orchestration. Therefore, in order to reinstall CxSAST, either delete the existing Management and Orchestration database before re-installing, or reinstall with a new Management and Orchestration database.

## Installed Services Check

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



Make sure the following installed Checkmarx services and Web server are started:

### On a centralized host:

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxSastResults
- CxScanEngine
- Management and Orchestration:
  - CxARM
  - CxARMETL
  - CxRemediationIntelligence
- Shared services:
  - ActiveMQ

- Web server (run "iisreset /start" from elevated CMD or Start action for the server name in IIS Console):
  - World Wide Web Publishing Service
  - IIS Admin Service

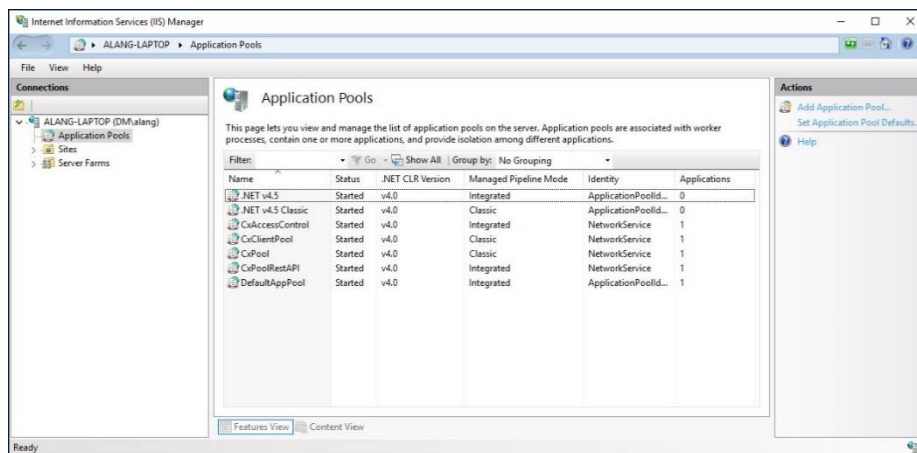
**On a CxEngine host (if applicable):**

- CxScanEngine

By default, all product services are installed and configured to run with Windows Network Service account. For updating or customizing non-default service accounts, please refer to [Configuring CxSAST for use with a non-default user \(Network Service\) - CxServices & IIS Application Pools](#).

➤ **To run the Pool Check for the installed application:**

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

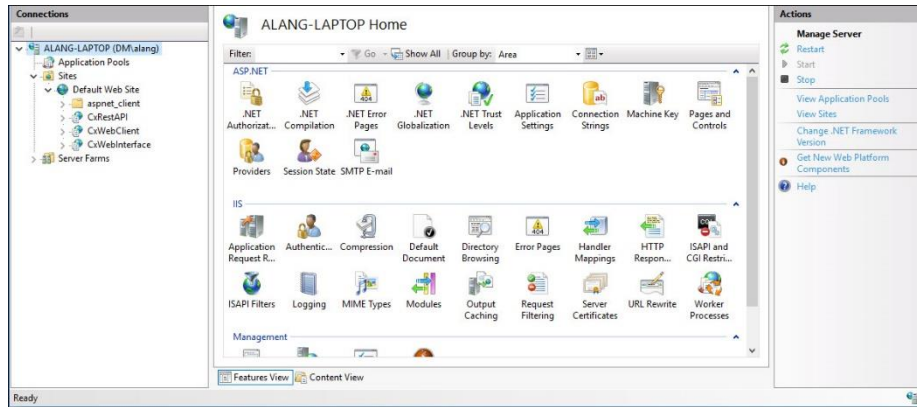


2. Make sure the following installed application pools are started:

**On a centralized host:**

- CxClientPool
- CxPool
- CxPoolRestAPI
- CxAccessControl

If any of the IIS Pools are not started automatically after installing, restart the station.



## 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 defined.

- This configuration should only be added on a station with .NET 4.6.2 or above installed, otherwise there will be issues in the application.

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: *<Installation folder>\Checkmarx\Checkmarx Web Services\CxWebInterface\web.config* , for example *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" />
```

## Login to the CxSAST Web Interface

Access the [CxSAST web interface](#) in one of the following ways:

- **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).
- **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.

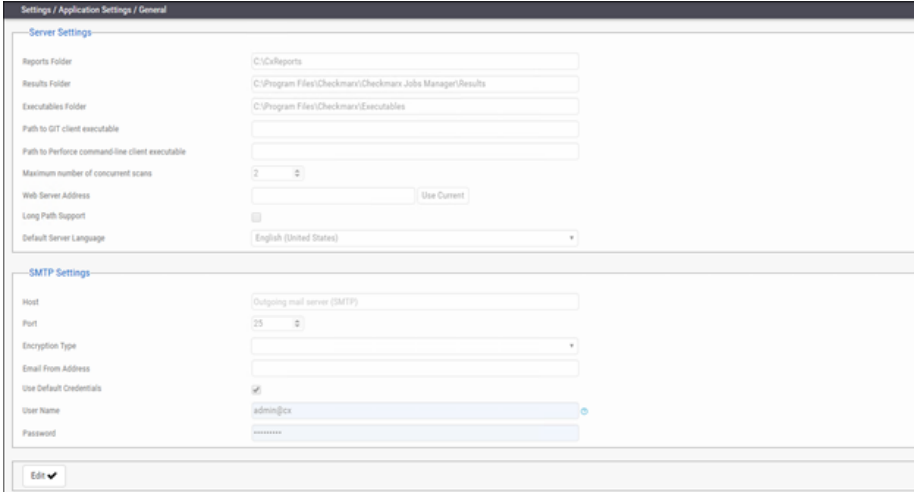
If '3rd party cookies' are disabled in your browser, you will not be able to log into the CxSAST Web Interface via 'http://localhost'. If this is the case you will need to use 'http://<FQDN>', where <FQDN> is the Fully Qualified Domain Name and consists of both the hostname and domain name (e.g. `http://mqserver.company.com:5555`).

Upon a clean installation, a single Administrator Account needs to be created using Access Control. For more information, refer to [Accessing the Access Control Web Interface](#).

## General Settings

To define general settings, do the following:

1. Go to **Settings > Application Settings > General**. The General Settings screen is displayed.



2. Click **Edit** to enable changes.

## 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

1. To enable the long path support in CxSAST, click **Edit** and check the **Long Path Support** checkbox.

- Confirm that all application servers support long paths, otherwise scans with long path files may fail.

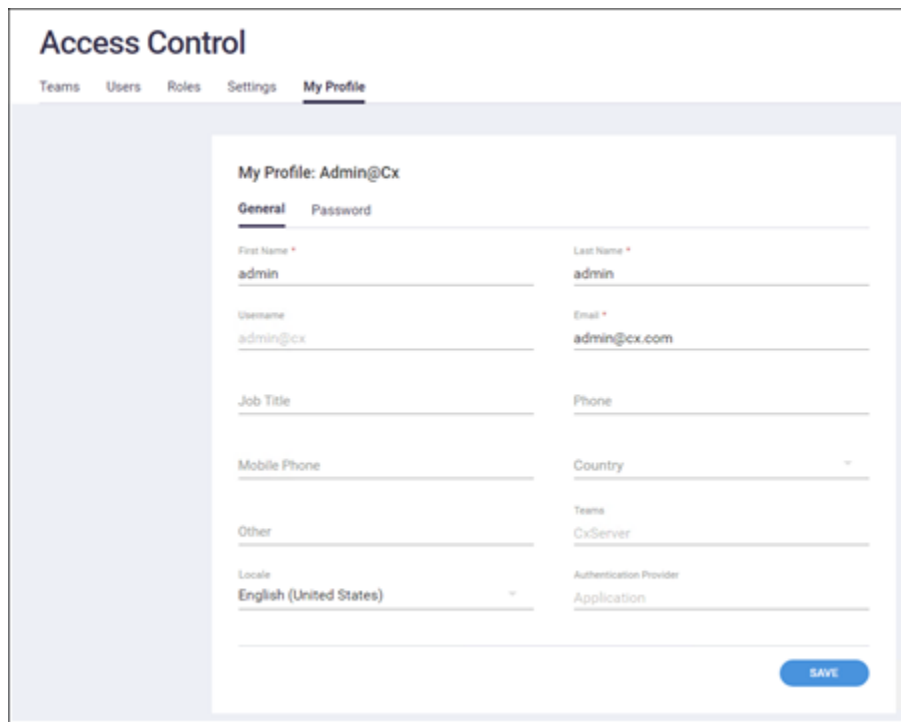
2. Click **Update** to save the changes.

## SMTP Settings

1. Provide the relevant **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.
2. Click **Update** to save changes.

## My Profile Settings

- Go to **My Profile > General**. The My Profile screen is displayed.



The screenshot shows the 'Access Control' interface with the 'My Profile' tab selected. The profile is for 'Admin@Cx'. The 'General' tab is active, showing a form with the following fields:

My Profile: Admin@Cx	
<b>General</b>	<b>Password</b>
First Name *	Last Name *
admin	admin
Username	Email *
admin@cx	admin@cx.com
Job Title	Phone
Mobile Phone	Country
Other	Teams
Locale	CxServer
English (United States)	Authentication Provider
	Application

A blue 'SAVE' button is located at the bottom right of the form.

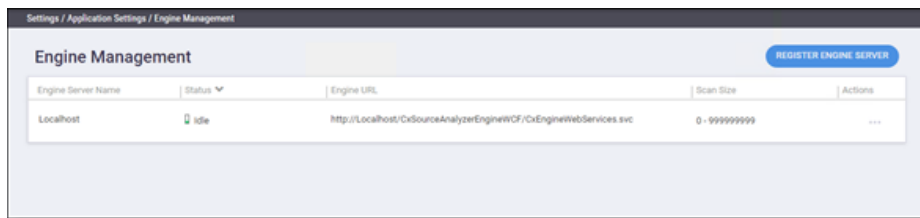
## Email Verification

- Verify that the email address in the CxSAST profile settings is valid, i.e. **John.Smith@example.com**, and not **John.Smith@example**. This step is required for Codebashing registration.


- You can subsequently change the Administrator password and add CxSAST users. For more information, refer to Access Control User Management.

### Engine Settings (in a distributed architecture)

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



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



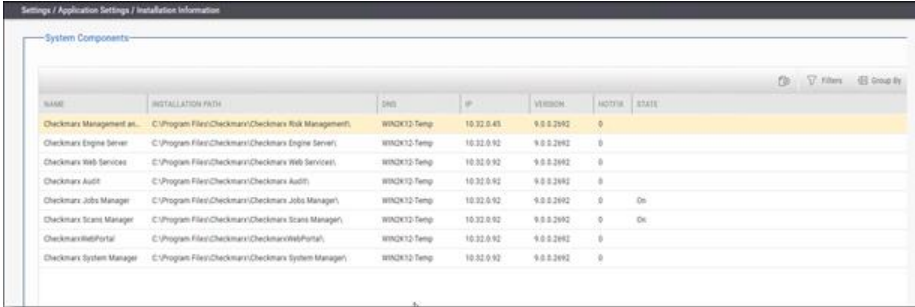
3. Assign a **Server Name** to the engine and provide the **Server URL** to enable CxManager to communicate with CxEngine. The URL looks similar to the following:
4. **http://<Server\_Name>/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc** where <Server\_Name> is the CxEngine host's IP address or resolvable name.
5. In addition, you can define **Scan LOC Limits** (maximum lines of code allowed). This setting is optional.

- It is recommended to validate the defined URL by opening it in a browser on the CxManager Server.
- If you have multiple CxEngine Servers, repeat this procedure for each Engine Server.

6. Click **Update**.

## Installation Verification

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



NAME	INSTALLATION PATH	OS	IP	VERSION	HOTFIX	STATE
Checkmarx Management Console	C:\Program Files\Checkmarx\Checkmarx Risk Management\	WINDOWS Temp	10.32.0.43	9.0.0.2042	0	
Checkmarx Engine Server	C:\Program Files\Checkmarx\Checkmarx Engine Server\	WINDOWS Temp	10.32.0.92	9.0.0.2042	0	
Checkmarx Web Services	C:\Program Files\Checkmarx\Checkmarx Web Services\	WINDOWS Temp	10.32.0.92	9.0.0.2042	0	
Checkmarx Audit	C:\Program Files\Checkmarx\Checkmarx Audit\	WINDOWS Temp	10.32.0.92	9.0.0.2042	0	
Checkmarx Jobs Manager	C:\Program Files\Checkmarx\Checkmarx Jobs Manager\	WINDOWS Temp	10.32.0.92	9.0.0.2042	0	OK
Checkmarx Scans Manager	C:\Program Files\Checkmarx\Checkmarx Scans Manager\	WINDOWS Temp	10.32.0.92	9.0.0.2042	0	OK
Checkmarx Portal	C:\Program Files\Checkmarx\Checkmarx Portal\	WINDOWS Temp	10.32.0.92	9.0.0.2042	0	
Checkmarx System Manager	C:\Program Files\Checkmarx\Checkmarx System Manager\	WINDOWS Temp	10.32.0.92	9.0.0.2042	0	

2. 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.

- After upgrading, if you need to modify a protocol, a station and/or port definitions for upgraded Cx components, please refer to [Changing the Server Name, IP or Port for Checkmarx Components](#) for further information and instructions.

---

## Installing CxSAST in Silent Mode

The CxSAST/CxOSA silent install / uninstall enables you to specify property values from the command line (CLI) and is ideal for large-scale enterprise deployments. This method gives you the ability to perform a clean install, upgrade and uninstall of the CxSAST/CxOSA application in silent mode, without constant interaction from GUI interface prompts.

### Prerequisites

The required prerequisites are listed below. For further information and instructions on installing and making them available, refer to the [installation guide](#).

- **C++ Redist 2010 and 2015 SP3**
- **IIS v7.0 (or higher)**
- **.NET Core 2.1.16 (or higher 2.1.x versions) Runtime & Hosting**
- **MS SQL**
- **Java 1.8 64-bit**

- The Java installation must reside where permission fulfillment is possible (e.g. C:\Program Files) and not in personal user folders such as the Desktop folder. The approved and recommended Java version is 1.8. The minimum version for Oracle is 8u241 and for AdoptOpenJdk, it is 8u242.

- Access Control Installation & Migration Setup is required for upgrading to CxSAST/CxOSA versions 9.0.0 and later from prior CxSAST/CxOSA versions 8.8.0 or 8.9.0
- Access Control and CxManager must be installed on the same server station.

### Syntax (Access Control Installation & Migration Setup)

```
CxSetup.AC_and_Migration.exe /quiet /install ACCESSCONTROL=1 ACCEPT_EULA=Y
INSTALLSHORTCUTS=1 SQLAUTH=1 SQLSERVER=SQL_SERVER_INSTANCE SQLUSER=SQL_USER
SQLPWD=SQL_PASSWORD PORT=ACCESS_CONTROL_PORT
CXSAAS_ADDRESS=CXSAAS_URL_ADDRESS
```

### Syntax (General CxSAST/CxOSA Setup)

```
CxSetup.exe /quiet /install BI=1 ACCEPT_EULA=Y CX_JAVA_HOME="C:\Program
Files\Java\jre1.8.0_241" ACTIVEMQ=1 VALIDATED_ACCESSCONTROL_MIGRATION=Y
SQLAUTH=1 SQLSERVER=SQL_SERVER_INSTANCE SQLUSER=SQL_USER SQLPWD=SQL_PASSWORD
CXARM_SQLAUTH=1 CXARM_DB_HOST=SQL_SERVER_INSTANCE CXARM_DB_USER=SQL_USER
CXARM_DB_PASSWORD=SQL_PASSWORD
```

To upgrade CxSAST 8.x to 9.0 and remove a service, you have to first install the new version of CxSAST and then run the silent installation wizard again to remove the relevant service. Attempts to install the new version of CxSAST and remove the relevant service in one step cause the entire process to fail.

### Parameters

The table below lists the and explains the various parameters.

Parameter	Description
/?	Opens the help dialog.
/install / uninstall / quiet	Installs or uninstalls CxSAST/CxOSA silently (Install is the default). Displays no UI and no prompts. By default, UI and all prompts are displayed.  If you only enter <b>/install</b> or <b>/uninstall</b> , the relevant wizard starts in GUI mode.
ACCEPT_EULA=	Sets EULA (End User License Agreement) variable with Y to accept, or N to not accept (ACCEPT_EULA=N is the default). Must be set to Y to run the installation.
CX_JAVA_HOME=	Path to the JRE folder (e.g. C:\openjdk-8u242-b08-jre, C:\Program Files\Java\jre1.8.0_241 or C:\Program Files\Java\jdk1.8.0_241\jre).  Refer to Java in the Prerequisites section of the installation guide for additional information and instructions on making the required Java version available.
INSTALLFOLDER=	Sets the installation directory path (e.g. INSTALLFOLDER="D:\TEMP DIR", INSTALLFOLDER=D:\TEMP).  "INSTALLFOLDER=D:\\" is supported.
MANAGER=	Sets Manager component variable with 1 to install, or 0 to remove\not install.  (MANAGER=1 is default)

Parameter	Description
WEB=	Sets Web component variable with 1 to install, or 0 to remove\not install (WEB=1 is the default).
ENGINE=	Sets Engine component variable with 1 to install, or 0 to remove\not install (ENGINE=1 is the default)
AUDIT=	Sets Audit component variable with 1 to install, or 0 to remove\not install (AUDIT=1 is the default).
BI=	Sets BI component (CxARM) variable with 1 to install, or 0 to remove\not install. (BI=1 is the default).
ACCESSCONTROL=	Sets Access Control component variable with 1 to install, or 0 to remove\not install (ACCESSCONTROL=1 is the default).
VALIDATED_ACCESSCONTROL_MIGRATION=	Sets the Access Control Migration manual validation with Y to yes, or N to no (e.g. VALIDATED_ACCESSCONTROL_MIGRATION=Y)
ACTIVEMQ=	Sets Active MQ component variable with 1 to install, or 0 to remove\not install (ACTIVEMQ=1 is the default).
INSTALLSHORTCUTS=	Sets application shortcuts variable with 1 to install shortcuts, or 0 to not install shortcuts (INSTALLSHORTCUTS=1 is the default).
SQLAUTH=	Sets the SQL authentication mode for CxSAST/CxOSA. Use 0 for Windows authentication or 1 for SQL authentication (SQLAUTH=0 is the default). When SQLAUTH is set to 0, the SQLUSER and SQLPWD settings are ignored.
SQLSERVER=	Sets the SQL server address and instance for CxSAST/ CxOSA (e.g. SQLSERVER= localhost\SQLEXPRESS)
SQLUSER=	Sets the SQL user credential for CxSAST/CxOSA (e.g. SQLUSER=sa)
SQLPWD=	Sets the SQL password credential for CxSAST/CxOSA (e.g. SQLPWD=12345)
CXSAST_ADDRESS=	Sets the CxSAST URL address (CXSAST_ADDRESS=http://localhost:80 is the default). Also validates that the defined URL address is reachable.
MQHTTPPORT=	Sets the MQ Admin console port definition (MQHTTPPORT=61616 is the default).
MQMANAGERHTTPPORT=	Sets the MQ operational port definition (MQMANAGERHTTPPORT=8161 is the default).
RIHTTPPORT=	Sets the Remediation Intelligence port definition (RIHTTPPORT=8082 is the default).
TOMCATHTTPPORT=	Sets Apache Tomcat HTTP port definition (TOMCATHTTPPORT=8080 is the default).
TOMCATHTTPSPORT=	Sets Apache Tomcat HTTPS port definition (TOMCATHTTPSPORT=8443 is the default).
CXARM_SQLAUTH=	Sets the SQL authentication mode for CxARM. Use 0 for Windows Authentication or 1 for SQL Authentication (CXARM_SQLAUTH=0 is the default). When SQLAUTH is set to 0, the CXARM_DB_USER and CXARM_DB_PASSWORD settings are ignored.
CXARM_DB_HOST=	Sets the SQL server address and instance for CxARM (e.g. CXARM_DB_HOST=localhost\SQLEXPRESS)
CXARM_DB_USER=	Sets the SQL user credential for CxARM (e.g. CXARM_DB_USER=sa)

Parameter	Description
CXARM_DB_PASSWORD=	Sets the SQL password credential for CxARM (e.g. CXARM_DB_PASSWORD=12345)
LIC=	Sets the license path (e.g. LIC="C:\Users\Administrator\Documents\license.cxl"). Note - If the license check fails, the license will not be installed.  The license can also be installed manually once the installation is complete.
PORT=	Sets the port definition (PORT=80 is the default for CxSAST/CxOSA, PORT=8081 is the default for Access Control)

## Remarks

- The default silent installation command is <Path-To-Installer-File> /install /quiet
- By default most options and components are set to 1 (enabled).
- The Access Control Installation & Migration Setup procedure is required for upgrading to CxSAST/CxOSA versions 9.0.0 and later from prior CxSAST/CxOSA versions 8.8.0 or 8.9.0 only. For a first-time CxSAST/CxOSA installation (v9.0.0 and up), simply perform the General CxSAST/CxOSA Setup procedure provided in this guide.
- SQL Server connection Requirements:
- For both SQL Server 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.
- When upgrading CxSAST/CxOSA using the silent install method, you should not change the existing port settings or the application will not function properly. Changing the port settings can be performed manually after the upgrade is complete.

## Examples

To perform the Access Control Installation & Migration Setup prior to the silent installation for upgrade to version 9.0.0: CxSetup.AC\_and\_Migration:

```
CxSetup.AC_and_Migration.exe /quiet /install ACCESSCONTROL=1 ACCEPT_EULA=Y
CX_JAVA_HOME="C:\Program Files\Java\jre1.8.0_241" INSTALLSHORTCUTS=1
SQLAUTH=1 SQLSERVER=192.168.0.0\SQLEXPRESS SQLUSER=sa SQLPWD=12345 PORT=8081
CX_SAST_ADDRESS=http://localhost:80
```

To perform a silent installation with all components using windows integrated authentication and creating shortcuts:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y CX_JAVA_HOME="C:\Program
Files\Java\jre1.8.0_241" LIC=C:\LIC\license.cxl BI=1 ENGINE=1 MANAGER=1 WEB=1
AUDIT=1 INSTALLSHORTCUTS=1
```

To perform a silent installation with only Manager Component to d:\Cx and without shortcuts created:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y CX_JAVA_HOME="C:\Program Files\Java\jre1.8.0_241" LIC=C:\LIC\license.cxl BI=0 ENGINE=0 MANAGER=1 WEB=0 AUDIT=0 INSTALLFOLDER="d:\Cx" INSTALLSHORTCUTS=0
```

To perform a silent installation to a default location with all components without a license (the license can be imported later) – using SQL authentication:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y CX_JAVA_HOME="C:\Program Files\Java\jre1.8.0_241" BI=1 SQLAUTH=1 SQLSERVER=192.168.0.0\SQLEXPRESS SQLUSER=sa SQLPWD=12345 CXARM_SQLAUTH=1 CXARM_DB_USER=test CXARM_DB_PASSWORD=Pass
```

To perform a silent install to a default location with only Manager Component – using SQL authentication:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y CX_JAVA_HOME="C:\Program Files\Java\jre1.8.0_241" ENGINE=0 MANAGER=1 WEB=0 AUDIT=0 BI=0 SQLAUTH=1 SQLSERVER=LOCALHOST\SQLEXPRESS SQLUSER=SqlUser SQLPWD=SqlPassword
```

To perform a silent install for engine only:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y ENGINE=1 MANAGER=0 WEB=0 AUDIT=0 BI=0
```

To perform a silent uninstall:

```
CxSetup.exe /uninstall /quiet
```

---

## Upgrading CxSAST in High Availability Solutions

To install and configure high availability solutions, refer to the relevant instructions. In addition, a diagram that outlines the architecture for high availability solutions is available here.

To edit any of the protocols in use, the station and/or port definitions for any of the upgraded Cx components, refer to Changing the Server Name, IP or Port for Checkmarx Components for further information and instructions.

By default all product services are installed and configured to run with Windows Network Service account. For updating or customizing non-default service accounts, please refer to [Configuring CxSAST for use with a non-default user \(Network Service\) - CxServices & IIS Application Pools](#).

---

## Modifying CxSAST

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

---

### Before you Start

If you are switching Java versions, for example due to upgrading or otherwise modifying your CxSAST installation in a way that it requires a newer Java installation, you have to update the newer Java location with the certificate from the previous Java location. This means, you have to copy the **cacerts** file from the previous Java location (`..\Checkmarx Risk Management\jre\lib\security\`) to the new Java location (`<install path>\openjdk-8u242-b08-jre\lib\security\`) and overwrite the existing **cacerts** file in the new location with your existing **cacerts** file.

Make sure there are no scans currently running.

Stop all Cx Windows services and Web servers (depending on the Checkmarx components installed on the server):

➤ **On a centralized host:**

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxSastResults
- CxScanEngine
- Management and Orchestration:
  - CxARM
  - CxARMETL
  - CxRemediationIntelligence
- Shared services:
  - ActiveMQ
- 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



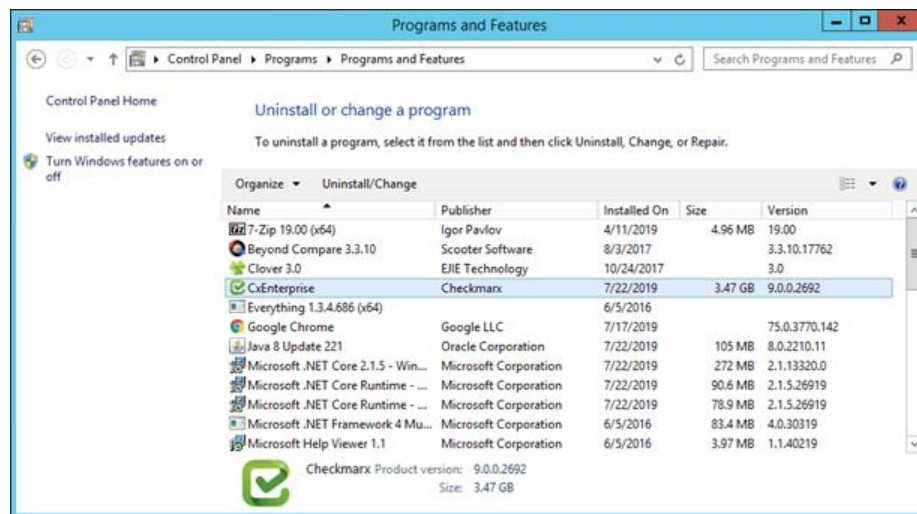
➤ On a CxEngine host (if applicable):

- CxScanEngine

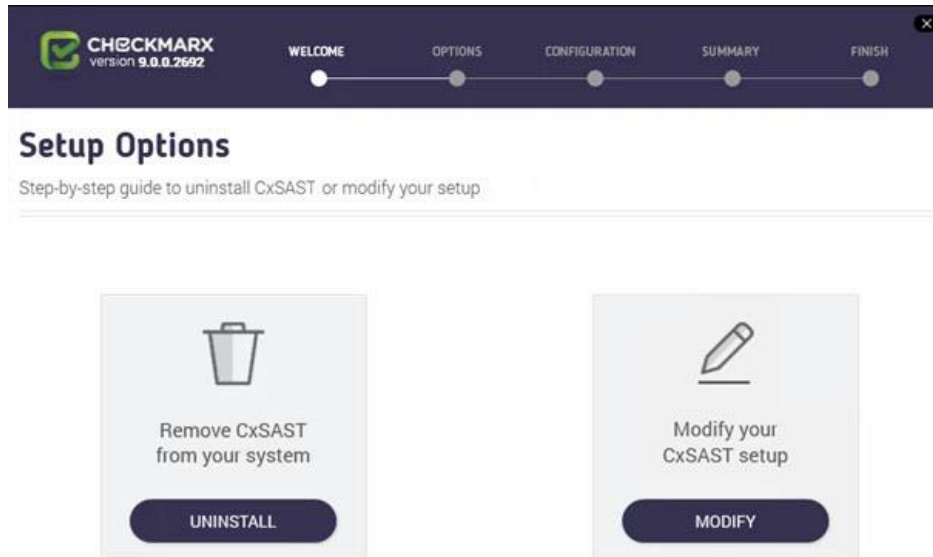
➤ To modify CxSAST:

1. Go to **Start > Control Panel > Programs > Programs and Features**. The **Programs and Features** screen is displayed.

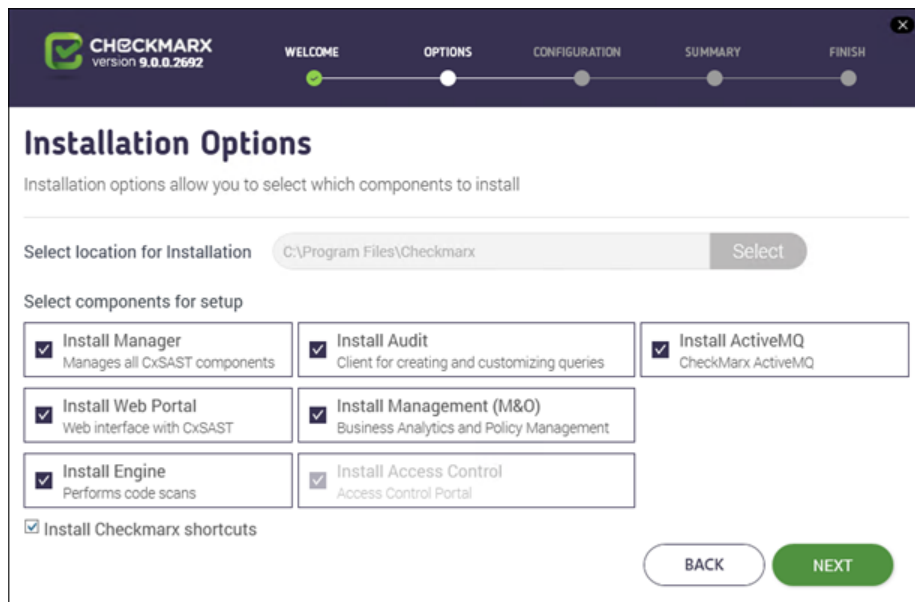
- As a precaution, you should backup all Cx databases (using standard SQL Server tools and make sure to give the files unique names and to include .bak.



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




3. Click **MODIFY**, then click **OK** on the warning message to acknowledge that selecting Modify will change any previously defined installation configuration back to the default setting. The additional **Installation Options** window is displayed.



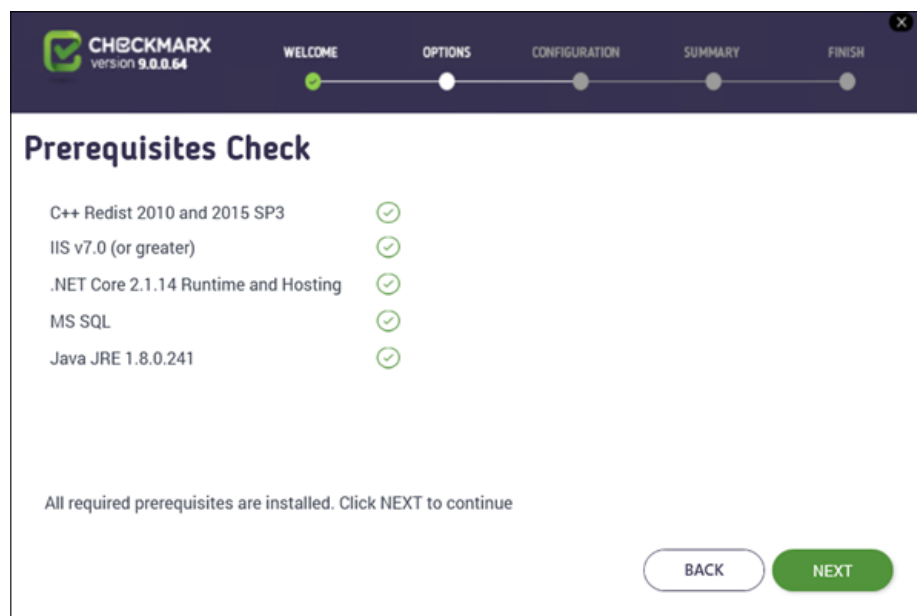
4. Select or deselect the required product features for this modification from the available list.

- Access Control is the only component that, by default, you cannot modify.

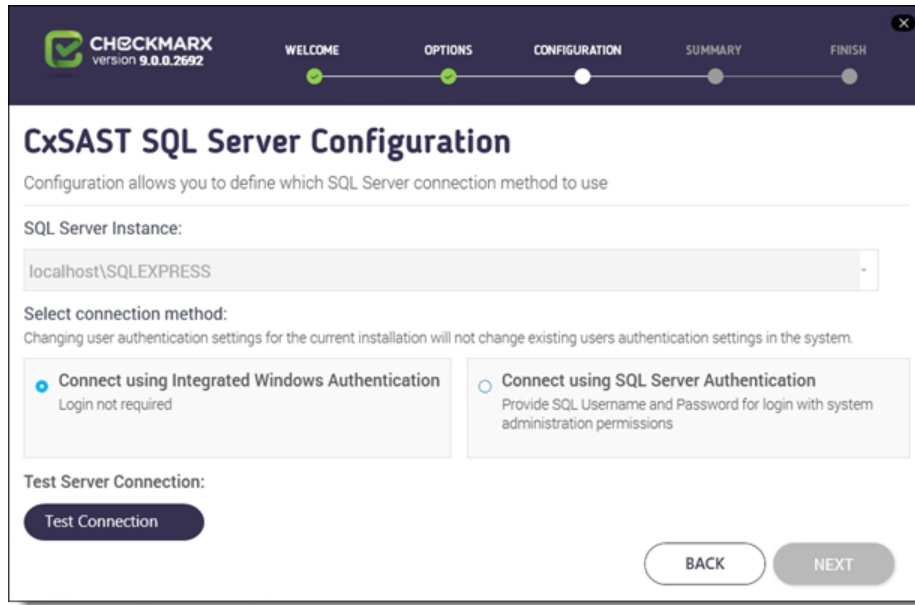
5. Click **Next** to continue. The **Prerequisites Check** window is displayed, showing the status of all prerequisite components.
6. For any prerequisite component yet installed (marked with ) , perform the following:
  - Click 'Browse' and select the JRE folder (e.g. `C:\openjdk-8u242-b08-jre` , `C:\Program Files\Java\jre1.8.0_241` or `C:\Program Files\Java\jdk1.8.0_241\jre`).

- The Java installation must be located where permission fulfillment is possible (e.g. C:\Program Files) and not in personal user's folders such as the Desktop folder. The approved and recommended Java version is 1.8. The minimum version for Oracle is **8u241** and for **AdoptOpenJdk** , it is **8u242**. Before you continue, verify that the minimum version is installed on your server.

7. Click the Prerequisites Folder button to navigate to the supplied components and install each one separately.
8. After all missing prerequisite component(s) has been installed, click 'Recheck Prerequisites' after making the necessary changes.

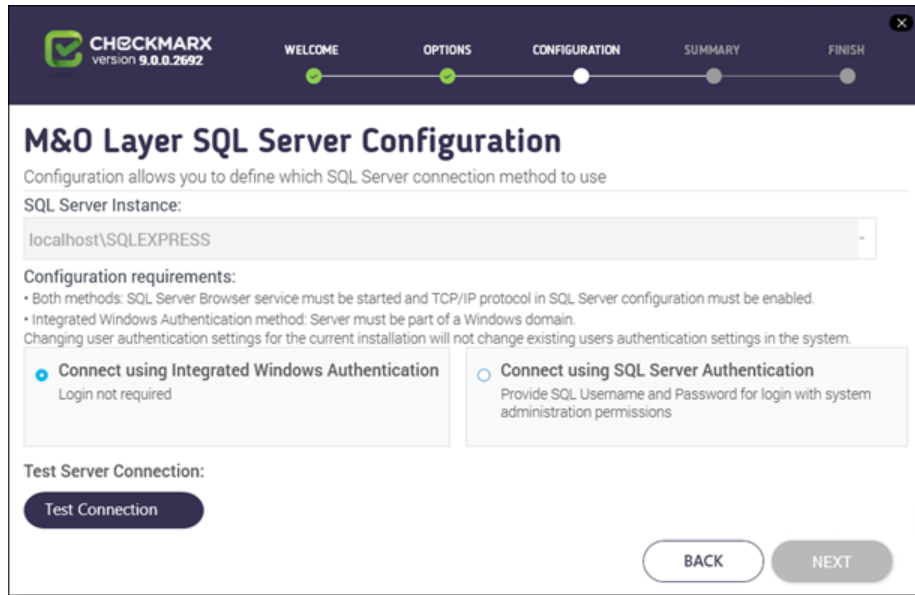


9. When all prerequisite components are installed, click **Next** to continue.  
The **CxSAST SQL Server Configuration** window is displayed.



10. 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).
11. Click **Test Connection**. A "**Connection OK**" message is displayed upon confirmed connection to the CxSAST SQL Server.
12. If the "SQL Connection Test Results" message indicates that connection to the SQL Server has failed, verify the following:
  - Host, port and login credentials are correct
  - The 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).
13. Once the connection has been successfully tested and the prerequisites are in place, click **OK** on the confirmation message, then click **NEXT**.

The **M&O Layer SQL Server Configuration** window is displayed.



14. For **Management and Orchestration Layer**, 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).

- For M&O Layer SQL Server connectivity, both Dynamic and Static port configurations are supported. For more information, refer to [Configuring Management & Orchestration SQL Server for Dynamic and Static Port Connectivity](#).

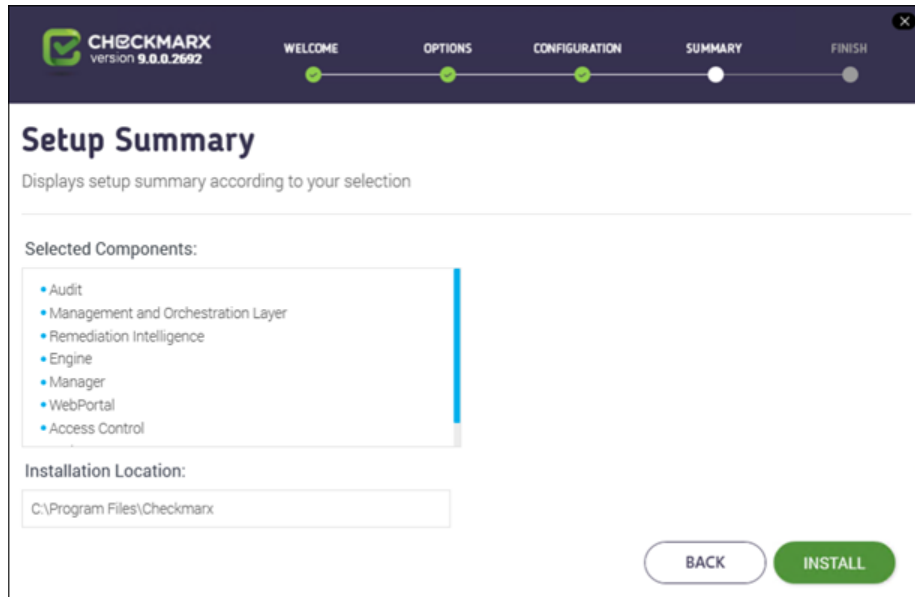
15. Click **Test Connection**. A "**Connection successful**" message is displayed upon confirmed connection to the SQL Server.

16. If the "SQL Connection Test Results" message indicates that connection to the SQL Server has failed, verify the following:

- Host, port and login credentials are correct
- The 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).

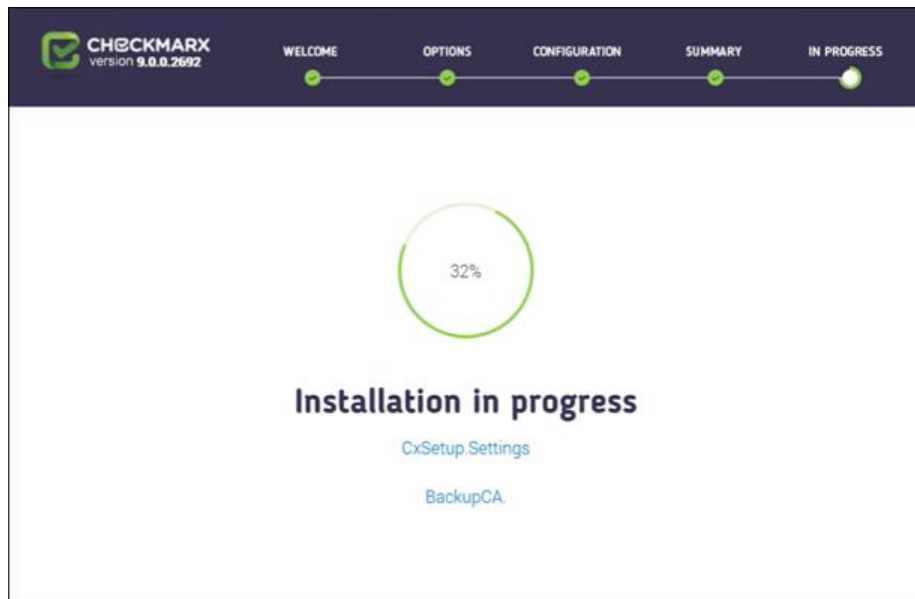
17. Click **OK** on the message, and then click **NEXT**.

The **Setup Summary** window is displayed.



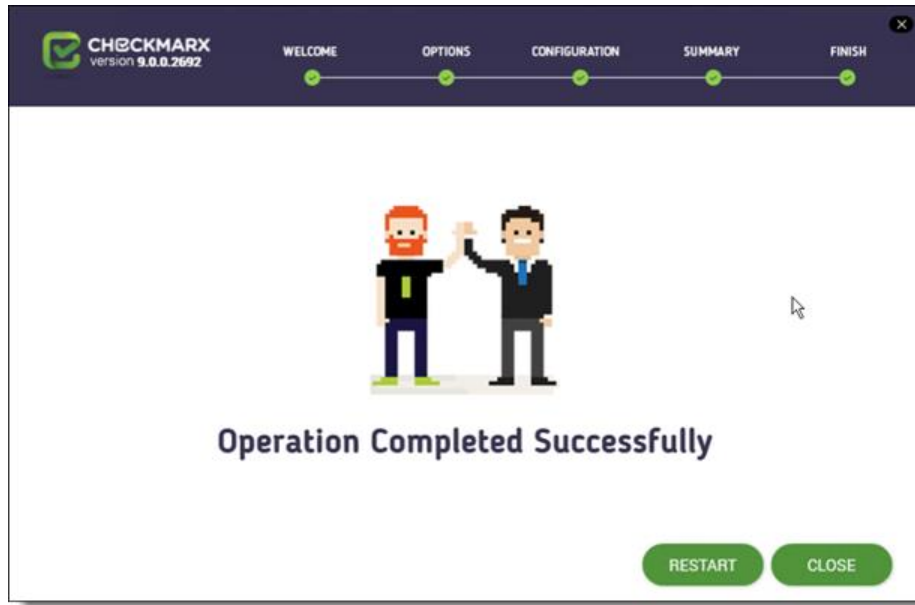
18. Check the setup summary according to your selection.

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



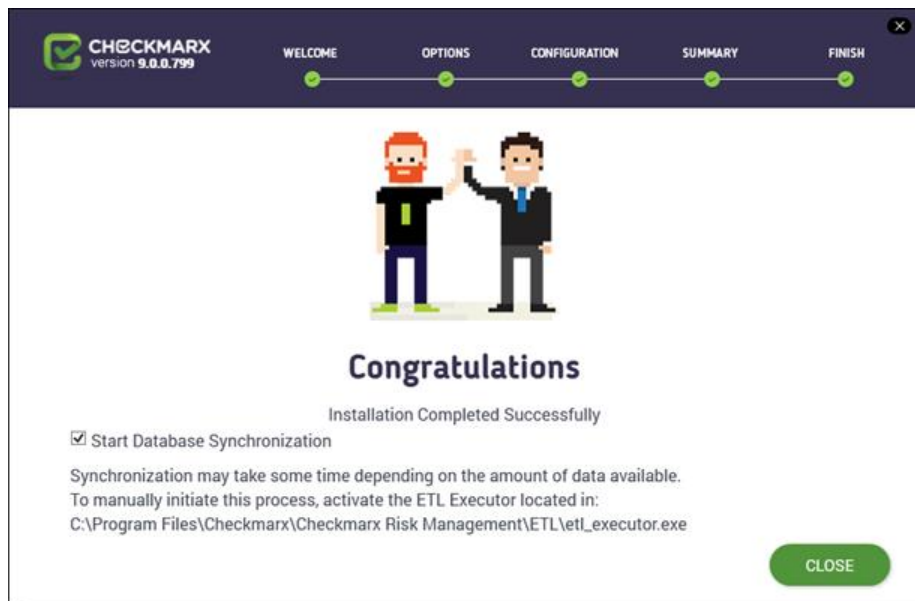
20. If the installation fails, the "Setup failed" message is displayed. Refer to the installation logs for additional information. If you need further assistance, please contact [Checkmarx support](#).

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



21. Click **RESTART** to complete the installation.

If part of the modification included selecting the Management and Orchestration component on the Congratulations window, the **Start Database Synchronization** window is displayed.



By default, **Start Database Synchronization** is checked. This enables Management and Orchestration by initializing the automatic synchronization process. This process may take some time, depending on the amount of data being synchronized.

22. **To continue now with the database synchronization**, leave the checkbox selected, and then click **CLOSE**. If required, reboot the server (you receive a prompt, if rebooting is necessary). The database synchronization process starts automatically.

For more information about installing Management and Orchestration, see [Installing Management and Orchestration](#).

23. **To perform the database synchronization at another time**, clear the checkbox, and click **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**

- If attempting to install CxSAST with an existing Management and Orchestration database, the subsequent ETL DB sync will fail, due to a limitation in Management and Orchestration. Therefore, in order to reinstall CxSAST, either delete the existing Management and Orchestration database before reinstalling, or reinstall with a new Management and Orchestration database.
- Validate that all Cx Windows services and Web servers (depending on the Checkmarx components installed on the server) have started.

By default all product services are installed and configured to run with Windows Network Service account. For updating or customizing non-default service accounts, please refer to [Configuring CxSAST for use with a non-default user \(Network Service\) - CxServices & IIS Application Pools](#).

---

## Backing Up and Recovering CxSAST

The following page describes the backup and recovery procedures for CxSAST

---

### Backing up CxSAST

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

In general, 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, do the following:

1. Make sure there are no scans currently running.
2. Stop all Cx Windows services and Web servers (depending on the Checkmarx components installed on the server):

➤ **On a centralized host:**

- CxSystemManager



- CxJobsManager
  - CxScansManager
  - CxSastResults
  - CxScanEngine
  - Management and Orchestration:
    - CxARM
    - CxARMETL
    - CxRemediationIntelligence
  - Shared services:
    - ActiveMQ
  - 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
3. **Back up the Checkmarx folder by copying it aside (Logs folder can be excluded)**  
Example: <Checkmarx Installation Path>\Checkmarx -> <Checkmarx Installation Path>\Checkmarx01012016
  4. **Back up the CxDB, CxActivity and CxARM SQL databases using standard Database tools**
  5. **Back up the CxSRC folder - scanned source folder - by creating a copy**  
Example: X:\CxSrc -> X:\CxSrc01012016
  6. Check that you have the CxSAST installation zip file for the current backed up version (can be requested from [Checkmarx support](#)).
  7. Start all Cx Windows services and Web servers (depending on the Checkmarx components installed on the server):

➤ **On a centralized host:**

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxSastResults
- CxScanEngine
- Management and Orchestration:
  - CxARM

- CxARMETL
- CxRemediationIntelligence
- Shared services:
  - ActiveMQ
- Web server (run "iisreset /start" from elevated CMD or Start action for the server name in IIS Console):
  - World Wide Web Publishing Service
  - IIS Admin Service

---

## Recovering CxSAST

The recovery procedure may be different based on the state of CxSAST server(s). If CxSAST exists and is working you can start from the second step.

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

1. **Install CxSAST with the same version as your backed up version to and install it to the same path as your previous CxSAST installation.**
2. Stop all Cx Windows services and Web servers (depending on the Checkmarx components installed on the server):

➤ **On a centralized host:**

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxSastResults
- CxScanEngine
- Management and Orchestration:
  - CxARM
  - CxARMETL
  - CxRemediationIntelligence
- Shared services:
  - ActiveMQ

- 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
  - 3. **Move/rename the Checkmarx folder**

Example: <Checkmarx Installation Path>\Checkmarx --> <Checkmarx Installation Path>\checkmarxNew01012016
  - 4. **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
  - 5. **Restore the database**

Restore the databases using the backup that you previously saved using the standard database tools.
  - 6. **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
  - 7. Start all Cx Windows services and Web servers (depending on the Checkmarx components installed on the server):
- **On a centralized host:**
- CxSystemManager
  - CxJobsManager
  - CxScansManager
  - CxSastResults
  - CxScanEngine
  - Management and Orchestration:
    - CxARM
    - CxARMETL
    - CxRemediationIntelligence
  - Shared services:
    - ActiveMQ

- Web server (run "iisreset /start" from elevated CMD or Start action for the server name in IIS Console):
  - World Wide Web Publishing Service
  - IIS Admin Service
- 8. Check the recovered version
- 9. 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

For any further assistance, contact Checkmarx support.

---

## Upgrading CxSAST

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

- Make sure to back up your Cx databases prior to running any software update. Schedule the database backup to create compressed files with unique file names in a separate folder from the main database files.
- For upgrading from v8.7 or prior versions, you are first required to install v8.8/v8.9 and only then proceed with the v9.0 installation. For more information, refer to [Installing CxSAST \(v8.8.0 to v8.9.0\)](#).
- For upgrading from v8.8/v8.9 to v9.0 you are first required to perform the Access Control data migration procedure. For more information, refer to [Access Control Data Migration Installer](#).
- Make sure that the SQL password does not exceed 32 characters. You may have to reset this password before upgrading as the SQL password could exceed 32 characters in previous versions. For further information, refer to [Installing CxSAST \(v9.0.0\)](#)
- If you are switching Java versions, for example due to upgrading or otherwise modifying your CxSAST installation in a way that it requires a newer Java installation, you have to update the newer Java location with the certificate from the previous Java location. This means, you have to copy the cacerts file from the previous Java location (`..\Checkmarx Risk Management\jre\lib\security\`) to the new Java location (`<install path>\openjdk-`

8u242-b08-jre\lib\security\) and overwrite the existing cacerts file in the new location with your existing cacerts file.

➤ **Before you start:**

1. Make sure there are no scans currently running.
2. Stop all Cx Windows services and Web servers (depending on the Checkmarx components installed on the server):

➤ **On a centralized host**

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxScanEngine
- Management and Orchestration:
  - CxARM
  - CxARMETL
- Web server: (run "iisreset /stop" from elevated CMD or Stop action for the server name in IIS Console)

➤ **On a CxEngine host (if applicable):**

- CxScanEngine

- Make sure to back your Cx databases up prior to running any software update. Schedule the database backup to create compressed files with unique file names in a separate directory from the main database files.

➤ **To upgrade CxSAST:**

1. Download the [CxSAST installation package](#).
2. Extract the downloaded ZIP archive, supplying the password provided by [Checkmarx support](#).
3. Run the **CxSetup.exe** on each server component host and perform the upgrade according to the [Installing CxSAST](#) procedure.

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\\AppData\Roaming\Checkmarx).

- The following files should be backed-up in case they need to be restored after an upgrade  
"<Drive>:\Program Files\Checkmarx\Checkmarx Audit\DefaultConfig.xml"
- "<Drive>:\Program Files\Checkmarx\Checkmarx Engine Server\DefaultConfig.xml"  
"<Drive>:\Program Files\Checkmarx\Executables\\*.\*\*"
- The following files should be backed up and used during the upgrade process:  
"<Drive>:\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:  
"<Drive>:\Program Files\Checkmarx\Configuration\DBConnectionData.config"

- To configure Access Control and ActiveMQ for High Availability, refer to Configuring Access Control for High Availability Environments and Configuring ActiveMQ for High Availability Environments.
- For upgrading Manager/Portal server in a distributed environment, the ActiveMQ component is automatically selected when using the 'Easy Upgrade' option.
- For high availability deployments, each manager (ScanManager, etc.) should be upgraded individually.

4. Validate that all Cx Windows services and Web servers (depending on the Checkmarx components installed on the server) have started:

➤ **On a centralized host:**

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxSastResults
- CxScanEngine
- Management and Orchestration:
  - CxARM
  - CxARMETL
  - CxRemediationIntelligence
- Shared services:
  - ActiveMQ

- Web server: (run "iisreset /start" from elevated CMD or Start action for the server name in IIS Console):
  - World Wide Web Publishing Service
  - IIS Admin Service

- If you have the IIS configured for both HTTP (80) and HTTPS (443), HTTPS (443) takes priority, and the system is configured accordingly.
- After upgrading to CxSAST 9.0, make sure that all external IIS bindings are defined at the ExternalListenUrls key in the appsettings json file. If, for example, port 80 (HTTP) and port 443 (HTTPS) were bound, the setting must look as follows: "ExternalListenUrls": http://\*:80;https://\*:443 . The appsettings json file resides in the Checkmarx Access Control folder.
- After upgrading to CxSAST 9.0, check the CxSASTManagerUri key located in the SQL [Cxdb].dbo.[CxComponentConfiguration] database table and verify that the protocol previously in use has been preserved. For example, if the protocol was HTTPS, it must still be set to HTTPS as follows: SET [VALUE]='https://{fqdn}'.  
{fqdn} stands for fully qualified domain name of your CxSAST Manager Server. The full queries to view and update the value:

- SQL QUERY VIEW CURRENT VALUE  
select \* from [CxDB].dbo.[CxComponentConfiguration] WHERE [Key] = 'CxSASTManagerUri'
- SQL QUERY TO UPDATE VALUE  
UPDATE [CxDB].dbo.[CxComponentConfiguration]
- SET [VALUE] = 'https://{fqdn}'  
WHERE [Key] = 'CxSASTManagerUri'

5. If required, start each one manually.

- By default all product services are installed and configured to run with Windows Network Service account. When upgrading from v8.8/8.9 to v9.0, any non-default accounts for new CxSAST Services (CxSASTResults, CxRemediationIntelligence, ActiveMQ) and IIS Application Pools (CxAccessControl) may need to be updated and customized according to your existing policy. You should also verify that all other previously existing CxSAST services and IIS Application Pools are still managed by your customized account. For updating non-default service accounts, please refer to Configuring CxSAST for use with a non-default user (Network Service) - CxServices & IIS Application Pools.

---

## Upgrading CxSAST in High Availability Solutions

To install and configure high availability solutions, refer to the relevant instructions. In addition, a diagram that outlines the architecture for high availability solutions is available [here](#).

To edit any of the protocols in use, the station and/or port definitions for any of the upgraded Cx components, refer to [Changing the Server Name, IP or Port for Checkmarx Components](#) for further information and instructions.

---

## Access Control Data Migration Installer

### Access Control Data Migration Tool - Overview

- This procedure applies to upgrading to CxSAST versions CxSAST versions 8.8.0 or 8.9.0 to version 9.0.0 and higher.
- For a first-time CxSAST installation (v9.0.0 and up), do not perform this procedure. Follow the instructions in the installation documentation for the respective CxSAST version.

For CxSAST versions 8.8.0 and 8.9.0, user management was an inseparable, platform-internal part of CxSAST – installed together with CxSAST and utilizing the same database.

When upgrading to CxSAST (v9.0.0 and up) from version v8.8.0 or v8.9.0, in order to retain all the previous CxSAST data (such as authorization and authentication definitions, configurations, teams, users and permissions), it is required to perform a procedure that first installs the new Access Control and then migrates the existing CxSAST data to it – followed by a manual verification of the data transferred – and then a separate installation for upgrading to the new CxSAST version.

If you wish to upgrade to CxSAST (v9.0.0 and up) from a CxSAST version **prior to v8.8.0**, you must first upgrade to version 8.8.0 or 8.9.0, and then perform the procedure in this guide.

- Any CxSAST version upgrade must be performed on the same station in order to preserve the existing CxSAST data on the CxDB.

For example:

- When upgrading to v8.8.0 / v8.9.0 - from a version prior to v8.8.0
- When upgrading to v9.0.0 and up - from v8.8.0 or v8.9.0



## Describing the Upgrade Process

When upgrading to CxSAST (v9.0.0 and up) from versions 8.8.0 or 8.9.0, the procedure consists of three phases:

**Phase 1:** The Access Control Migration installer will install the new Access Control module – a platform-external module, using the same CxDB database in a different scheme, and different set of APIs. After successful installation, the same installer runs the Data Migration Tool – which reads the existing CxSAST user data from the SAST-internal CxDB, and then populates the CxDB database for the new Access Control with the same data.

During this phase, user notification is provided upon any errors found – in the Access Control installation as well as the data migration. This helps to mitigate damage by enabling any problems to be dealt with immediately, while the data is still accessible and retrievable from the older CxSAST version still installed.

For more information about the procedure, refer to [Phase 1 – Running the Access Control Data Migration Tool Installer.](#)

**Phase 2:** After the data migration has completed successfully, this next phase allows the customer to manually cross-check and verify all transferred data (viewable in the new Access Control interface) against the data in CxSAST (viewable in the CxSAST interface) – to ensure successful data migration, and if needed, to rectify any problems **before** installing the new CxSAST (v9.0.0 and up).

Even though the Data Migration Tool may finish running without returning an error indication, there still remains the potential for error. For example, problems could stem from data that was – for whatever reason – incorrectly or erroneously altered in CxSAST prior to the migration, which, after being migrated, could result in lost user data, or render the product inaccessible.

Performing manual verification of migrated data is extremely beneficial to preempt problems that may only become apparent after the new CxSAST version has been installed – at which stage resolution becomes much more difficult.

For more information about the procedure, refer to [Phase 2 – Manually Verifying the Data after Migration.](#)

**Phase 3:** After manual validation of the data migration, run the CxSAST executable file to install the new CxSAST (v9.0.0 and up).

For more information about the procedure, refer to [Phase 3 – Installing the New CxSAST Version \(9.0.0 and up\).](#)

## Data Types Migrated

Some typical data types migrated are as follows:

- Users
- Teams
- Permissions
- Roles
- SMTP settings
- SAML settings
- LDAP settings

- **SMTP (mail) Settings Migration:** In case the SMTP “From address” field is empty in v8.8/v8.9, the migration will use the SMTP user name for that field. In case the username does not contain a valid email address, the migration will use ‘noreply@checkmarx.com’ as the “From address”. This setting is located [here](#).
- **LDAP SSO Domains:** Only domains mapped to the LDAP SSO and which are configured with a Fully Qualified Domain Name (FQDN) will be fully migrated.
- **Domains Migration:** Domains which are not associated with users will not be migrated

## New / Replacement CxSAST/CxOSA & Access Control Roles Available after Data Migration

The following compares the prior roles available in v8.8.0 and v8.9.0 to the new / replacement roles available after performing the Access Control Data Migration procedure and upgrading to v9.0.0 and up:

For more information, see [CxSAST / CxOSA Roles and Permissions \(v9.0.0 and up\)](#).

Former role before data migration & upgrade to v9.0.0 (and up)	New role(s) after data migration & upgrade to v9.0.0 (and up)
Reviewer	Reviewer
ReviewerWithSeverityStatus	Reviewer + Results Updater + Results Verifier
ReviewerAudit	Reviewer + Auditor
ReviewerWithSeverityStatusAudit	Reviewer + Results Updater + Results Verifier + Auditor
Scanner	Scanner + Reviewer + Results Updater + Data Cleaner + Security Risk Viewer
ScannerWithNEAndDelete	Scanner + Reviewer + Results Updater + Results Verifier + Data Cleaner
ScannerWithNE	Scanner + Reviewer + Results Updater + Results Verifier
ScannerWithDelete	Scanner + Reviewer + Results Updater + Data Cleaner
ScannerAudit	Scanner + Reviewer + Results Updater + Auditor

Former role before data migration & upgrade to v9.0.0 (and up)	New role(s) after data migration & upgrade to v9.0.0 (and up)
ScannerWithNEAndDeleteAudit	Scanner + Reviewer + Results Updater + Results Verifier + Data Cleaner + Auditor
ScannerWithNEAudit	Scanner + Reviewer + Results Updater + Results Verifier + Auditor
ScannerWithDeleteAudit	Scanner + Reviewer + Results Updater + Data Cleaner + Auditor
CompanyManager	Access Control Manager (AC role) + Scanner + Reviewer + Results Updater + Result Verifier
CompanyManagerAudit	Access Control Manager (AC role) + Scanner + Reviewer + Results Updater + Result Verifier + Auditor
SPManager	Access Control Manager (AC role) + Scanner + Reviewer + Results Updater + Result Verifier
SPManagerAudit	Access Control Manager (AC role) + Scanner + Reviewer + Results Updater + Result Verifier + Auditor
ServerManager	Access Control Manager (AC role) + SAST Admin
ServerManagerAudit	Access Control Manager (AC role) + SAST Admin + Auditor

### Default LDAP Role after Data Migration

LDAP configurations/sync settings, LDAP users, and mappings for group-to-role & group-to-team are migrated.

After migration, the former **default LDAP role** (in v8.8.0 / v8.9.0) will be migrated (in v9.0.0 and up) to a single default LDAP role, which will include permissions of all the role attributes (NE, delete project, etc.) - and which will be named (according to the permissions) as per **one** from the following examples:

Examples (2 sets of role variations):

<ul style="list-style-type: none"> <li>• SAST Scanner</li> <li>• SAST Scanner_With_NE</li> <li>• SAST Scanner_With_Delete</li> <li>• SAST Scanner_With_NE_And_Delete</li> </ul>	<ul style="list-style-type: none"> <li>• SAST Reviewer</li> <li>• SAST Reviewer_With_NE</li> <li>• SAST Reviewer_With_Delete</li> <li>• SAST Reviewer_With_NE_And_Delete</li> </ul>
---	---

### Default SAML Role after Data Migration

SAML configurations (including certificates) are migrated.

After migration, the former **default SAML role** (in v8.8.0 / v8.9.0) will be migrated (in v9.0.0 and up) to a single default SAML role, which will include permissions of all the role attributes (NE, delete project, etc.) - and which will be named (according to the permissions) as per **one** from the following examples:

Examples (2 sets of role variations):

<ul style="list-style-type: none"><li>• SAST Scanner</li><li>• SAST Scanner_With_NE</li><li>• SAST Scanner_With_Delete</li><li>• SAST Scanner_With_NE_And_Delete</li></ul>	<ul style="list-style-type: none"><li>• SAST Reviewer</li><li>• SAST Reviewer_With_NE</li><li>• SAST Reviewer_With_Delete</li><li>• SAST Reviewer_With_NE_And_Delete</li></ul>
--	--

### Future Benefits of the New Access Control Module

In the future the new Access Control module will simplify the login process by enabling Checkmarx users to perform a single login while utilizing multiple Checkmarx products, while delivering a fully featured user interface for unified access control and user management across the entire Checkmarx product offering.

### Restoring Passwords

During the upgrade, the **enc-credentials.properties** file is overwritten and a backup is created. As a result, the password property in the **credentials-enc.properties** file is removed and the password reset to the default.

➤ **To restore the password to your previous value:**

1. Open **credentials-enc\_backup.properties**, located in the same folder, and navigate to the Password property.
2. Copy the entire line of the Password property.
3. Paste it into the corresponding location of **credentials-enc.properties** and save the file.
4. Do not overwrite the newly created **credentials-enc.properties** with the backup file **credentials-enc\_backup.properties**. Doing so causes SAST to stop operating properly.

### Using the Access Control Data Migration Tool

#### Phase 1 – Running the Access Control Data Migration Tool Installer

- This procedure is only for upgrading to CxSAST v9.0.0 and later from v8.8.0 or v8.9.0. If you wish to upgrade from a CxSAST version prior to v8.8.0, you must first upgrade to v8.8.0 or v8.9.0, and then perform the following procedure for upgrading to CxSAST (v9.0.0 and up).
- For a clean CxSAST installation (first-time CxSAST installation of v9.0.0 or later), do not run the Access Control Migration installer – only run the CxSAST installer. Refer to the installation documentation for the CxSAST version.

After starting the Access Control Data Migration Tool Installer, stop using CxSAST, as any new data will not be migrated to the new CxSAST version.

Running the Access Control Migration installer between a few minutes and approximately half an hour, depending on the size of the database being migrated.

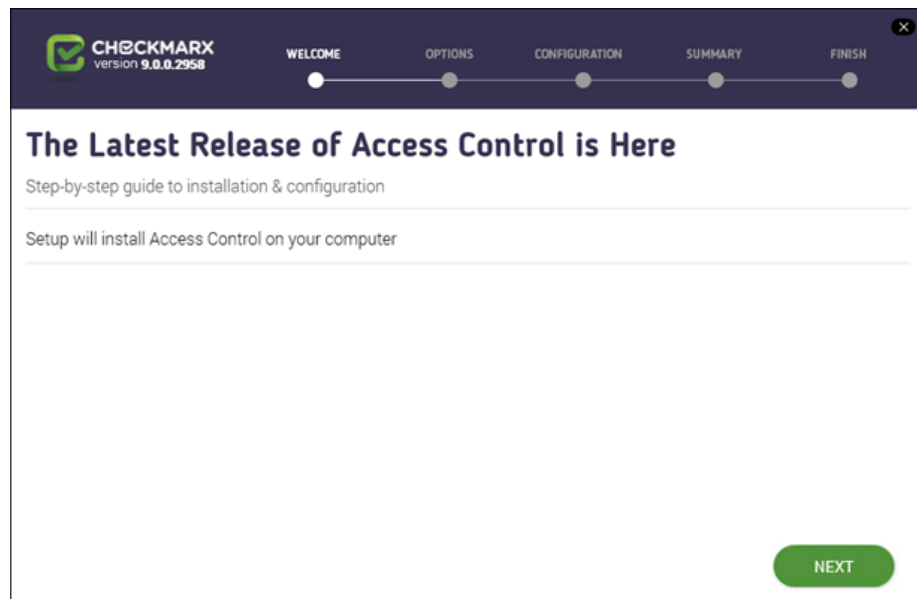
The Access Control Migration Tool should only be used once, even high-availability environments with multiple Manager servers.

Request the download link for the new release of CxSAST (v9.0.0 and up) from [here](#). You will receive two executable files:

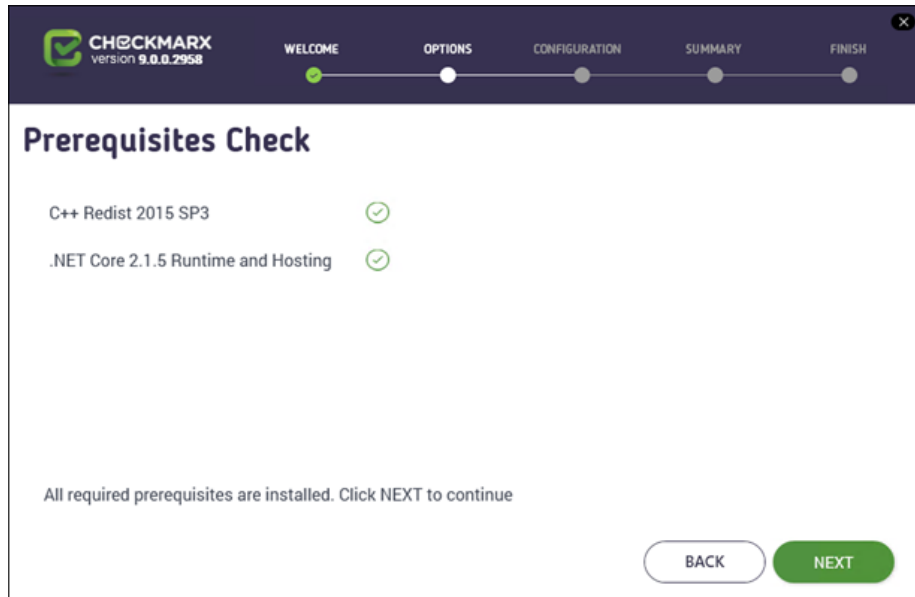
- **Access Control Migration installer** – for installing the new Access Control and performing data migration
- **CxSAST upgrade installer** – for upgrading to CxSAST (v9.0.0 and up)

Cx Windows services and Web servers (depending on the Checkmarx components installed on the server) must not be stopped, as recommended for the upgrade.

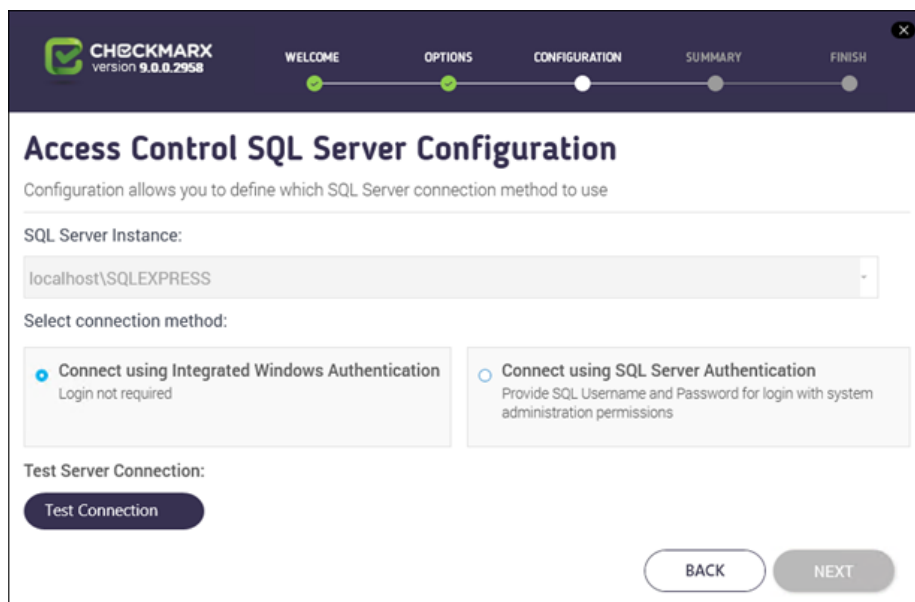
1. First, run the Access Control Migration installer as an **administrator**.



2. Click **Next**. The Prerequisites Check window is displayed, showing the status of all prerequisite components for Access Control.



3. For any prerequisite that shows as not yet installed, click the respective **INFO** button for additional installation information, and then click **Prerequisites Folder** to install the missing component(s).
4. Click **Recheck Prerequisites** to confirm the installation status.
5. When all prerequisite components are installed, click **Next** to continue. The **Access Control SQL Server Configuration** window is displayed.



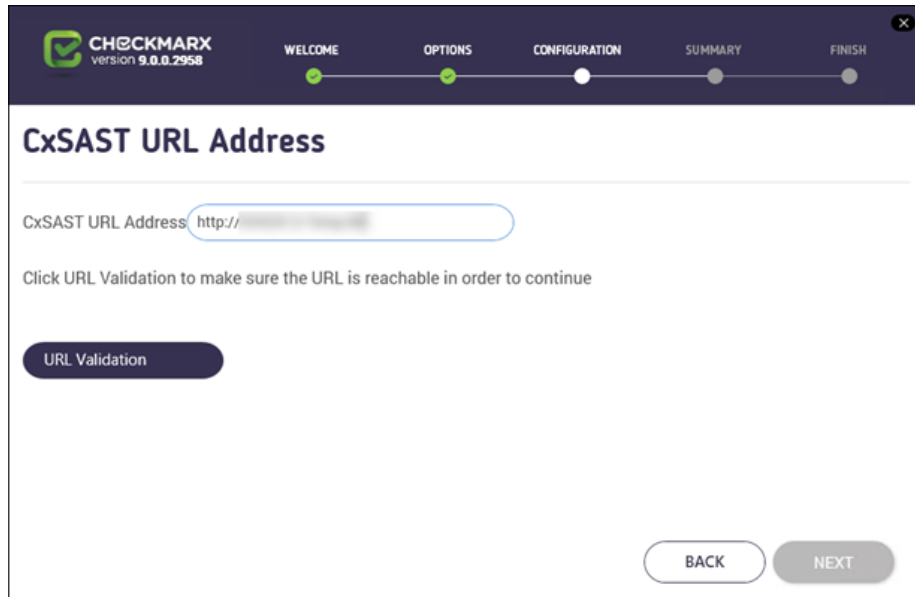
6. Define a connection to the installed SQL Server or to any other SQL server on your network, by selecting one of the following:

- **Connect using Integrated Windows Authentication** (login not required)
  - **Connect using SQL Server Authentication** (provide SQL user name and password for login with SA permissions).
7. Click **Test Connection**. A "**Connection Successful**" message is displayed upon confirmed connection to the SQL Server.

- If the "SQL Connection Test Results" message indicates that connection to the SQL Server has failed, verify the following:
  - Host, port and login credentials are correct
  - The 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).

- The migration tool installs and configures the Application Pool (CxAccessControl) to run with Windows Network Service, even if the previous CxSAST version had a different service account configuration. After installing Access Control, if the migration tool fails to run due to an SQL connection failure, navigate to the IIS Manager (inetmgr) and update your service account configuration for the Application Pool (CxAccessControl) in order to continue with the migration.
- Before the migration process begins, a message will appear, indicating that the user account for the CxAccessControl IIS Application Pool must be changed to the user that was used before, in order for the migration to succeed. Please notice: The migration tool continues with the migration without waiting for the 'OK' button to be pressed on the presented message. Hence, this change must be done in prior steps.

8. Click **OK** on the message, and then click **NEXT** to continue. The CxSAST URL Address window is displayed.

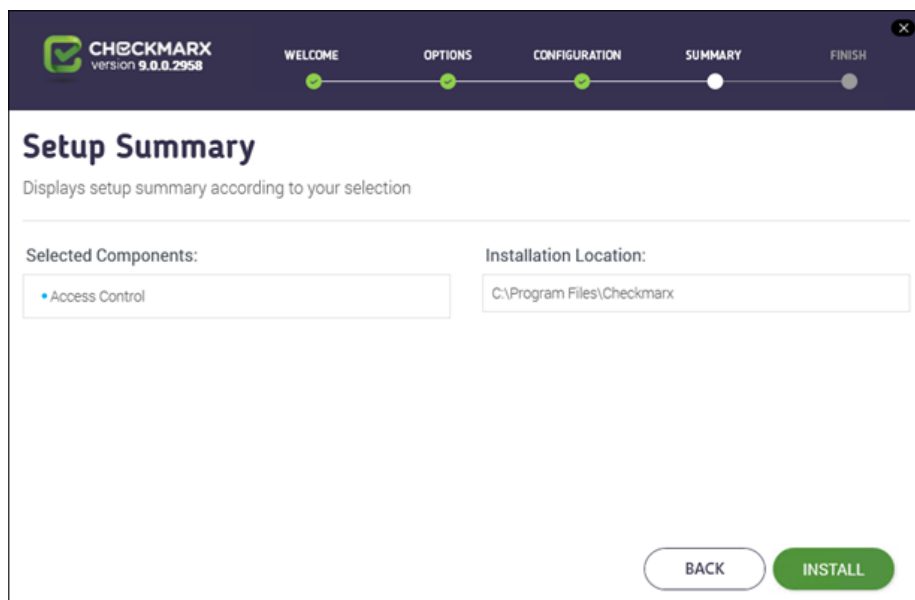


9. Click the URL Validation button to verify that the defined URL is reachable.

A "**URL Validation Passed**" message is displayed upon confirmed connection to the defined URL.

- If the "URL Validation" message indicates that connection to the defined URL has failed, redefine the URL and click the URL Validation button again.

10. Once the URL has been validated, click **OK** on the message, and then click **NEXT** to continue. The Setup Summary window is displayed.

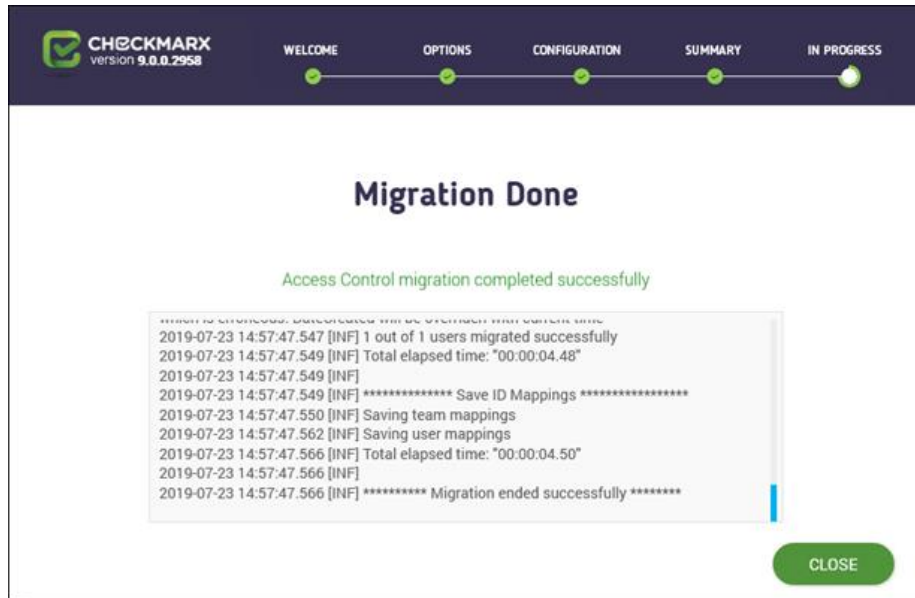


11. Check the setup summary according to your selection.



12. Click **INSTALL** to continue, **BACK** to return to the previous window, or **X** to exit. The migration process is started.

Once the migration process is complete, the Migration Complete window is displayed.



13. Click **CLOSE** to complete.

After running the Access Control Data Migration Tool Installer, you have to perform the recycling procedure for the AccessControl Application Pool from the IIS Manager.

### Examples of Error Notifications and Potential Fixes

If any error is encountered during either the Access Control installation or data migration stage, an error notification will be displayed.

For a full list of error notifications and potential fixes, see [Access Control Data Migration Tool Troubleshooting \(v9.0.0 and up\)](#).

#### Error found:

In this example, the error is due to an invalid character ( \ ) in the team name:

```
2018-11-07 07:59:29.999 [ERR] Failed to migrate team Team\C (Id: 88080c54-c92d-45a6-9fcb-ee60d9a7ceff). HTTP response status code: 400, content: {"Message": "Invalid character in team name."}
```

**Potential fix:**

The backslash (\) and colon (:) are not supported characters for a team name. In the SAST CxDB, change team name Team\C to **Team-C** for example, and rerun the data migration tool.

**Errors found:**

In this example, a problematic team GUID appears in the users-teams mapping table.

```
2018-11-07 08:06:44.985 [Fatal]
[ACMigrationTool.Infrastructure.SAST.SASTUsersRepository] Failed to read
SAST users-teams connections from the database
```

```
2018-11-07 08:06:44.986 [Fatal] [ACMigrationTool.MigrationRunner] Guid
should contain 32 digits with 4 dashes (xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxxxxxx) .
```

**Potential fix:**

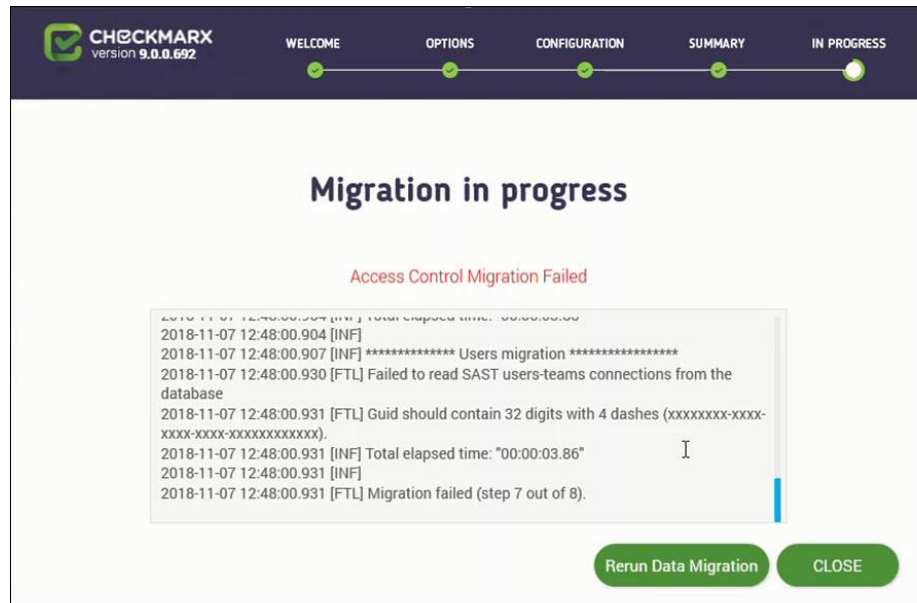
1. Find the problematic GUID in the users-team mapping table in the SAST CxDB
2. Remove the problematic entry.
3. Log into CxSAST and assign a team to the specific user.
4. Rerun the data migration tool.

### Errors Found During Access Control Installation

In case of an error found during the Access Control installation, the installer does not proceed to the data migration stage. In this case, contact [Checkmarx support](#).

After resolving the issues, rerun the Access Control Migration installer. If no further errors are found, after the Access Control installation stage is completed, the Data Migration Tool runs automatically.

## Errors Found During Data Migration

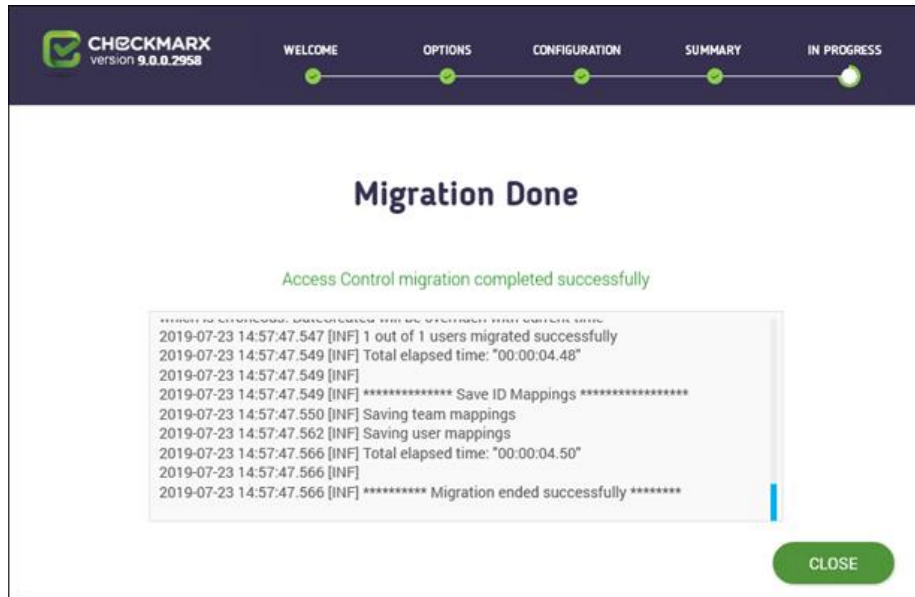


In the Data Migration phase, **disabled users** in v8.8.0 / v8.9.0 which belong to a **non-existing** authentication provider will not be migrated.

In case of an error found during the data migration stage, do the following:

1. Rectify the problem / discrepancy in the SAST CxDB.
2. In the installer, click the **Rerun Data Migration** button to perform the data migration again.
3. Alternatively, you can exit and restart the installer, which will also confirm the Access Control installation was successful, before rerunning the migration again.

Upon completion of the Access Control Migration installer without error notification, you receive a confirmation message:



Continue to the next phase, where you perform a manual data verification procedure to ensure the integrity of the data migration.

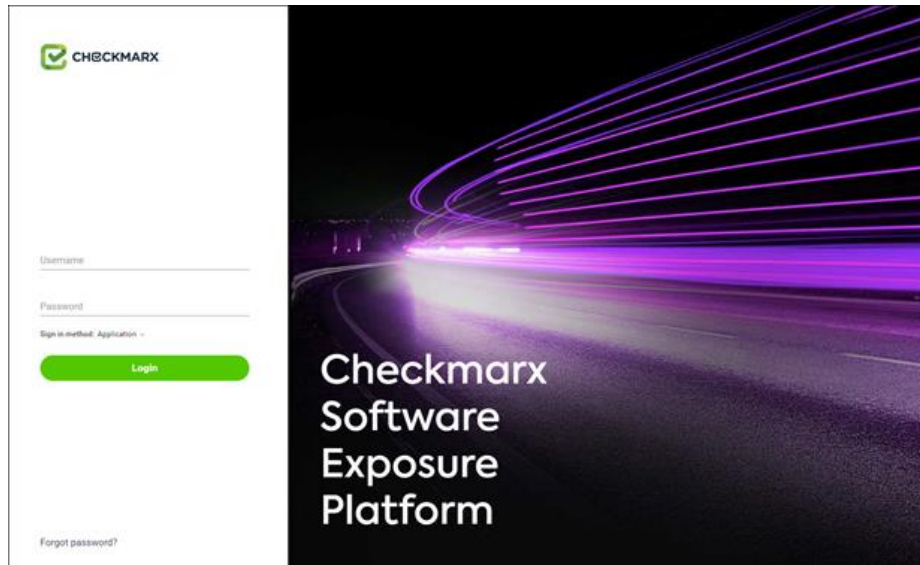
### Phase 2 – Manually Verifying the Data after Migration

Whether or not the prior phase returned any error messages during the Access Control setup or data migration, at this point – **before** upgrading the CxSAST version – you should manually verify the data that was migrated. Even without notification, errors in the migration of data may still exist for a variety of reasons – that may not even be connected to the data migration process – for example, data that was altered in CxSAST before the data migration, which could result in lost user data, or render the product inaccessible.

See [Access Control Data Migration Tool - Overview](#) for details about what data to verify after the migration.

Log in to the Access Control interface, and then cross check for any problems or discrepancies in the data – for example, by checking the data that was migrated against the data in CxSAST.

See the [Access Control user documentation](#) for details on working with the Access Control interface.



### Phase 3 – Installing the New CxSAST Version (9.0.0 and up)

- After upgrading SAST 9.0, make sure to modify the link for the Sign-On URL for the SAML server from `http{s}://{server}:{port}/CxRestAPI/auth/samlAcs` to `http{s}://{server}:{port}/CxRestAPI/auth/identity/samlAcs`. Otherwise the access link to the SAML server is broken as the login page of the SAML server cannot be reached.
- When starting the CxSAST version upgrade installation (after successful completion of the Access Control Data Migration procedure), a message appears confirming that you have manually validated the migrated data (phase 2). Select Validate to confirm, otherwise exit the installation.

After the migrated data has been manually verified, you can now start upgrading CxSAST by running the CxSAST installation file as an **administrator**.

Refer to the installation documentation for the CxSAST version for further information and instructions.

### Access Control Data Migration Tool Troubleshooting

This chapter provides troubleshooting information for typical errors that may be encountered when running the Access Control Migration Tool installer.

For any error encountered while running the Access Control Migration Tool installer (whether in the **Access Control installation** phase or the **data migration** phase), an error notification will be displayed.

Only upon completion of the Access Control Migration Tool installer without any error notification (you'll receive a confirmation message) will you then be able to continue to

the next phase (manual validation of migrated data), after which you can then run the CxSAST / CxOSA upgrade installation.

### Access Control Installation Errors

In case of an error found during the Access Control installation, the installer will not proceed to the data migration stage. In this case contact [Checkmarx support](#).

After resolution, rerun the Access Control Migration Tool installer. If no further errors are found in the Access Control installation stage, the data migration stage will then run automatically.

### Data Migration Errors

In case of an error found during the data migration stage:

1. Rectify the problem / discrepancy in the CxSAST CxDB.
2. In the installer, click the **Rerun Data Migration** button to perform the data migration again.
3. Alternatively, you can exit and restart the installer, which will also confirm the Access Control installation was successful, before rerunning the migration again.

### Data Migration Error Notifications and Potential Fixes

The following is a list of typical errors encountered and their potential fixes in the data migration phase:

**Error found:**

In the step *Checking Access Control API Connection*, the following error displays:

```
Failed to make an API call to Access Control. Verify that Access Control is up and running and rerun the migration.
```

**Potential fix:** Disable the Windows proxy configuration, and rerun the data migration tool.

**Potential fix:** Manually change the CxAccessControl account to have the same domain user as the remaining 8.x application pools.

**Error found:**

Error is due to an invalid character ( \ ) in the team name:

```
2018-11-07 07:59:29.999 [ERR] Failed to migrate team Team\C (Id: 88080c54-c92d-45a6-9fcb-ee60d9a7ceff). HTTP response status code: 400, content: {"Message": "Invalid character in team name."}
```

**Potential fix:**

The backslash (\) and colon (:) are not supported characters for a team name. In the SAST CxDB, change team name Team\C to **Team-C** for example, and rerun the data migration tool.

**Errors found:**

A problematic team GUID appears in the users-teams mapping table.

```
2018-11-07 08:06:44.985 [Fatal]
[ACMigrationTool.Infrastructure.SAST.SASTUsersRepository] Failed to read
SAST users-teams connections from the database
```

```
2018-11-07 08:06:44.986 [Fatal] [ACMigrationTool.MigrationRunner] Guid
should contain 32 digits with 4 dashes (xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxxxx) .
```

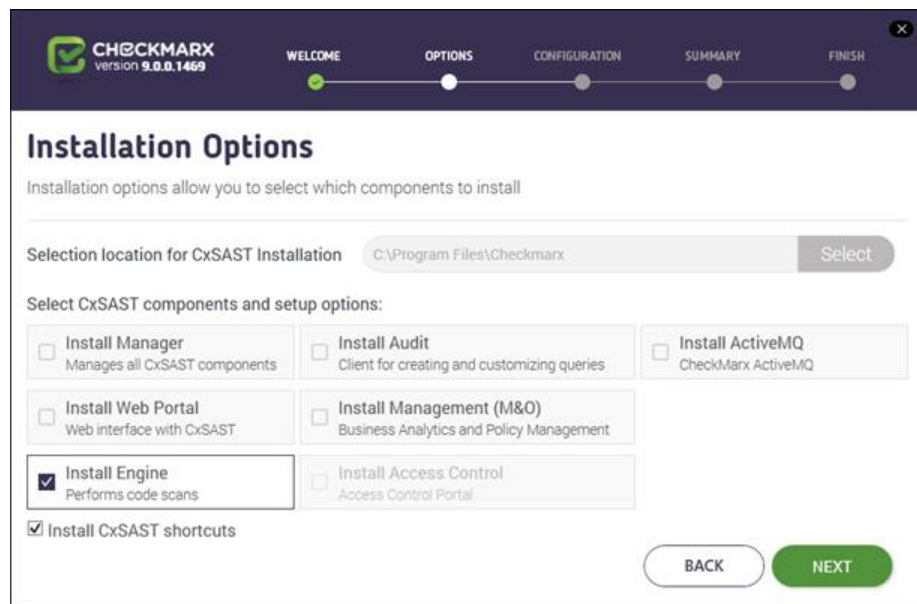
**Potential fix:**

1. Find the problematic GUID in the users-team mapping table in the SAST CxDB
2. Remove the problematic entry.
3. Log into CxSAST and assign a team to the specific user.
4. Rerun the data migration tool.

## Adding a CxEngine Server

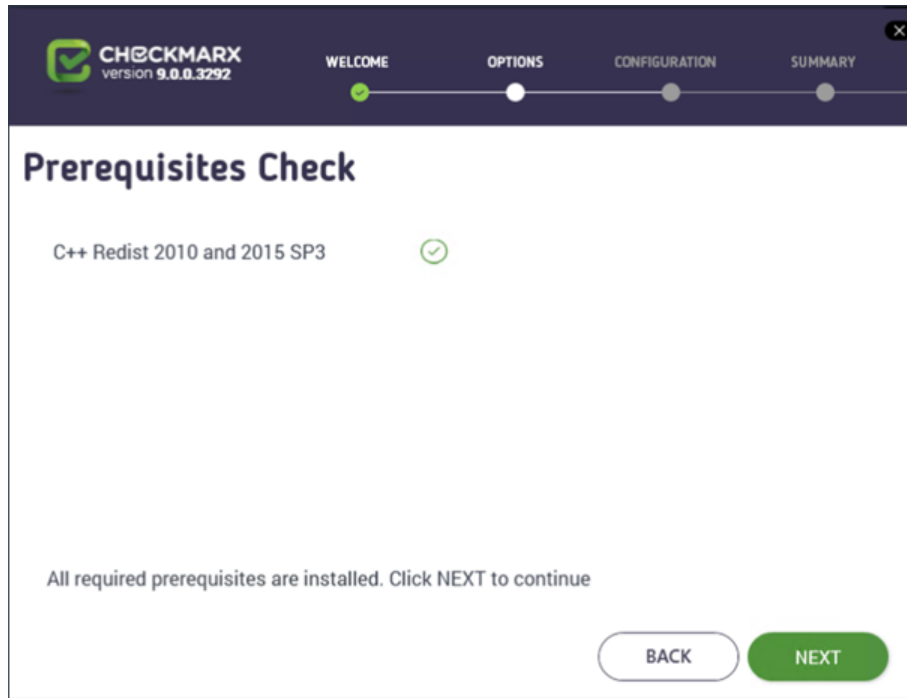
If you see that your scan load requires an additional Engine server, you can add one as follows:

1. [Prepare the environment](#) for the new CxEngine.
2. Perform the [Installing CxSAST](#) procedure, and once the **Installation Options** window is displayed, click **Select** to define the CxEngine installation location.
3. Select **Install Engine only**.



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



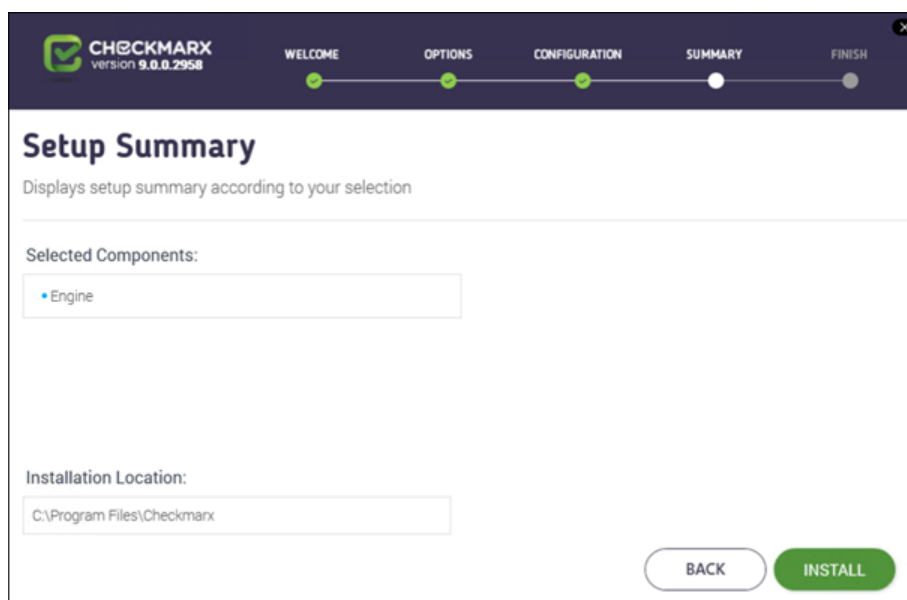


5. For any prerequisite component not installed, click the **Prerequisites Folder** button to browse for and install each missing prerequisite component.

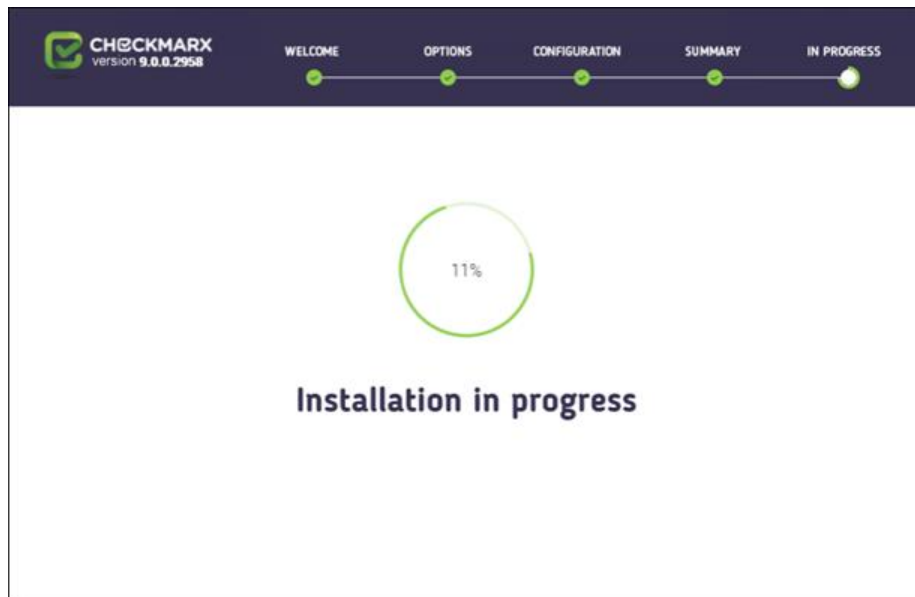
- C++ Redist Version 2015 is required in addition to version 2010

6. After the missing prerequisite component(s) have been installed, click **Recheck Prerequisites** to confirm the updated prerequisite status.

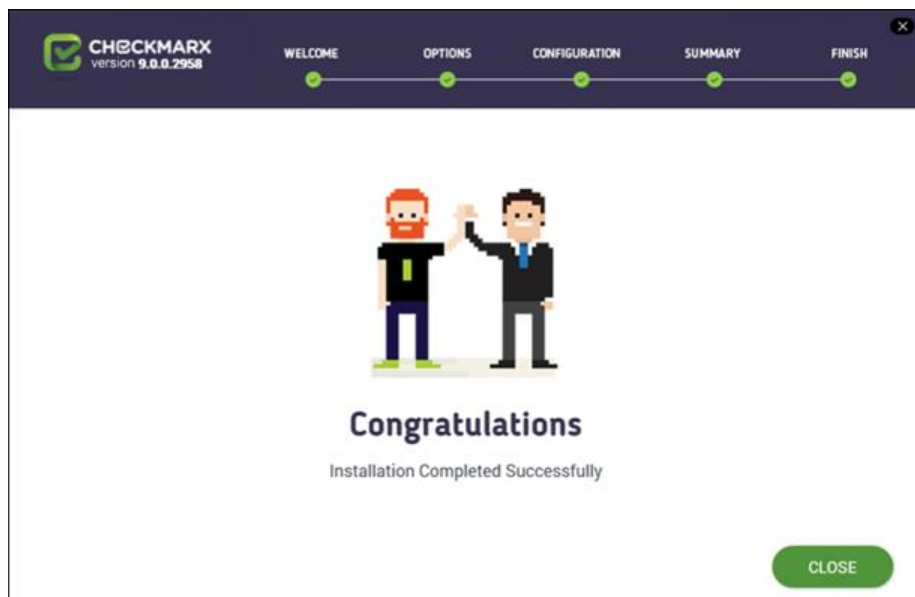
7. When all prerequisite components are installed, click **Next** to continue. The **Setup Summary** window is displayed.



8. Check the setup summary according to your selection.
9. Click **INSTALL** to continue, **BACK** to return to the previous window, or **X** to exit. The **Installation in Progress** window is displayed.



10. Once successfully installed, the **Installation Completed Successfully** window is displayed.

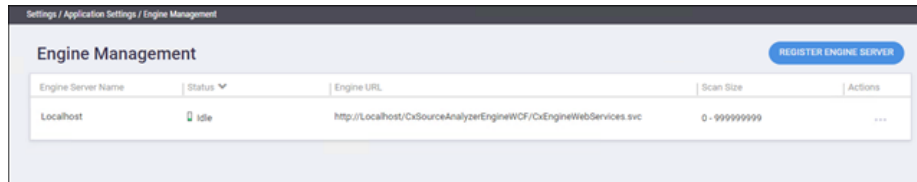


11. Click **CLOSE** to complete the installation.

- Engine Servers do not require a separate license. The existing CxSAST license should be copied from CxManager to each Engine using the License Importer tool (Start > Checkmarx > CxLicenseImporter.exe). For more information, refer to Updating the CxSAST License.

12. Log into the CxSAST web interface.

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



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



15. Assign a **Server Name** to the engine, 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).

16. Click **Update**.

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

- Increase the number of concurrent scans allowed (**Settings > Application Settings > General > 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.
17. 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:**

1. Copy your CxSAST license file to a safe location.
2. Make sure that there are no scans currently running.
3. Stop all Cx Windows services and Web server (depending on the Checkmarx components installed on the server):

➤ **On a centralized host:**

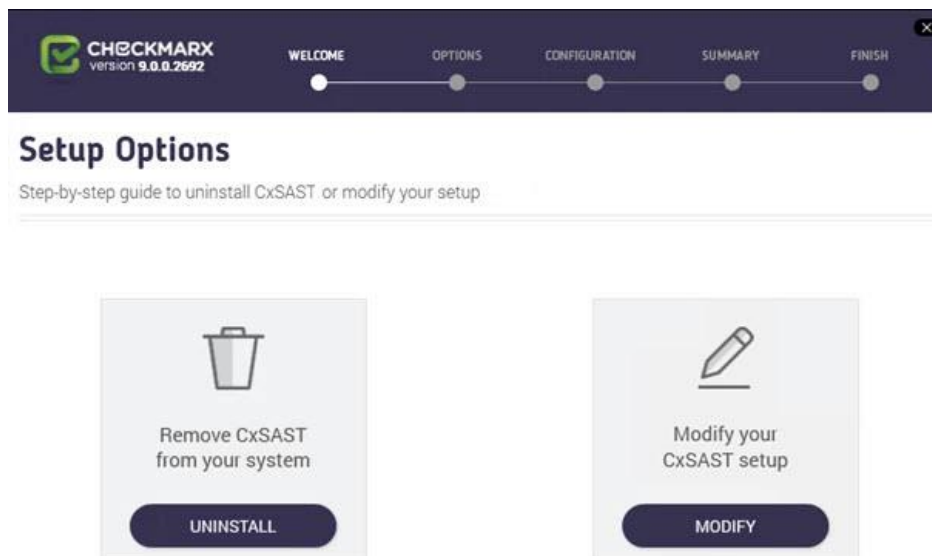
- CxSystemManager
- CxJobsManager
- CxScansManager
- CxSastResults
- CxScanEngine
- Management and Orchestration:
  - CxARM
  - CxARMETL
  - CxRemediationIntelligence
- Shared services:
  - ActiveMQ
- Web server: (run "iisreset /stop" from elevated CMD or Stop action for the server name in IIS Console):
  - World Wide Web Publishing Service
  - IIS Admin Service

➤ On a CxEngine host (if applicable):

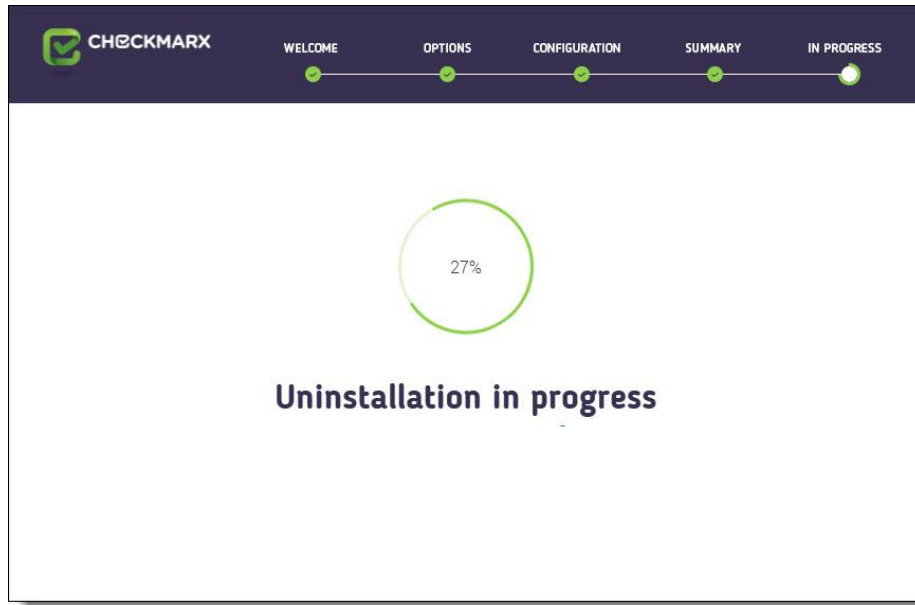
- CxScanEngine
4. Go to **Start > Control Panel > Programs > Programs and Features**. The **Programs and Features** screen is displayed.



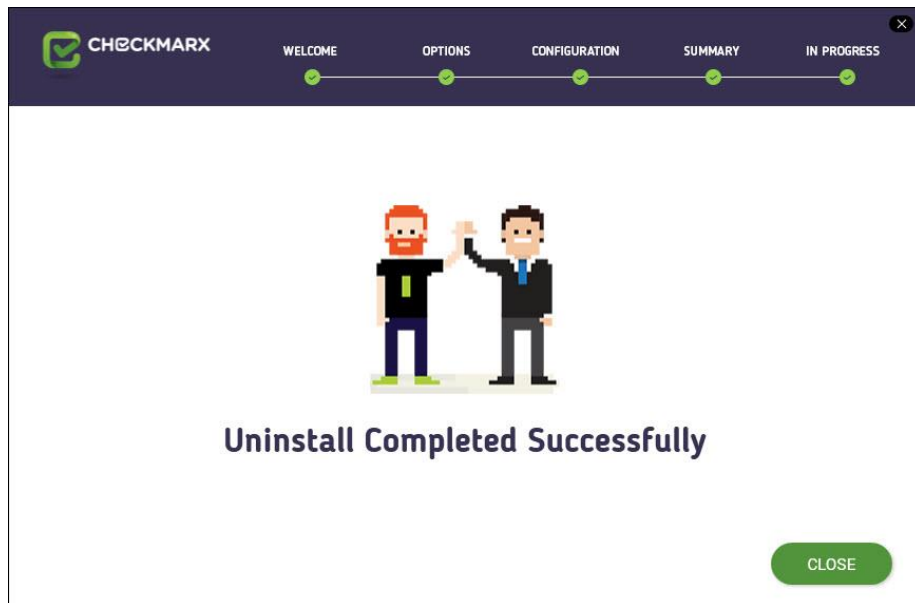
5. Double-click on **CxEnterprise**, or right click and select **Uninstall/Change**. The **Setup Options** window is displayed.



6. Click **UNINSTALL**, then click on the warning to confirm that you are about to remove CxSAST and all of its components. The **Uninstallation in Progress** window is displayed.



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



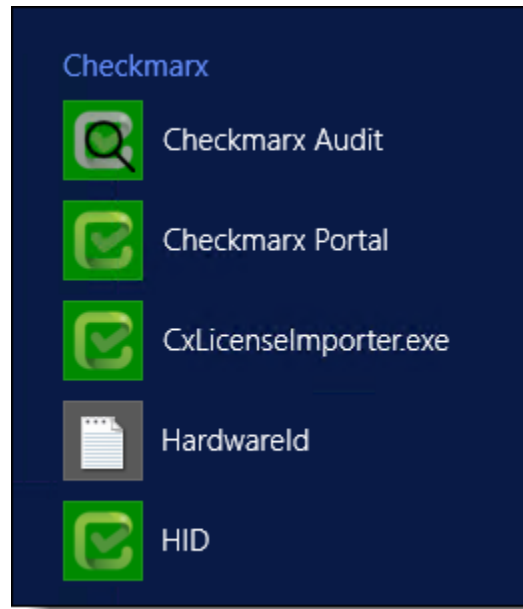
8. Click **Close** to complete the uninstall.

- Even though Uninstall removes most Checkmarx folders, the following folders are preserved for renewal at a later stage:
  - CxSrc
  - SQL DBs: CxDB, CxActivity and CxARM

## Updating the CxSAST License

➤ **To obtain a new or updated Checkmarx license for CxSAST:**

1. Go to **Start > All Programs > Checkmarx**, click **HID** to generate the Hardware ID.



2. 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.

- Updating the license on each CxManager is required in case of distributed or high availability architecture installations.

3. Close all Checkmarx Application windows.
4. Go to **Start > All Programs > Checkmarx**, and then click **CxLicenseImporter.exe**.

The Checkmarx License Importer is displayed.



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

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



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

6. Restart all Cx Windows services and Web server (depending on the Checkmarx components installed on the server):

➤ On a centralized host:

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxSastResults
- CxScanEngine
- Management and Orchestration:
  - CxARM
  - CxARMETL
  - CxRemediationIntelligence
- Shared services:
  - ActiveMQ
- Web server: (run "iisreset /start" from elevated CMD or Start action for the server name in IIS Console):
  - World Wide Web Publishing Service
  - IIS Admin Service

➤ On a CxEngine host (**if applicable**):

- CxScanEngine

---

## CxSAST Utilities

This section of the Checkmarx Knowledge Center includes information about the various utilities available for CxSAST.

---

### CxZIP - Create a Smaller File for Upload

#### Create a Smaller File for Upload

When uploading a project for scanning, 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, you can use Checkmarx's CxZip utility.

➤ **To create a smaller file for upload:**

1. Download and install the relevant 7-Zip application from [7-Zip](#)
2. Download and extract the zipped **CxZip.exe** from [Checkmarx Utilities](#).
3. Edit the extracted **CxExt.txt** file to specify extensions.
4. Limitation: The zip library is limited to 65534 entries (files) per zip archive.
5. Run the following command:

```
CxZip.exe <FolderToZip> <ZipFileToCreate.zip>
```

where <FolderToZip> is the source code folder, and <ZipFileToCreate.zip> is the path to the output zip file to be created.

For example:

```
CxZip.exe c:\Projects\TestProject c:\Projects\TestProject.zip
```

#### Create a Smaller File for Upload (Longpath Support)

When uploading a project for scanning, if the zip file is larger than 200 MB (due to a Microsoft default IIS implementation), you will not be able to upload it. To create a smaller zip file of only files with specified extensions, you can use Checkmarx's CxZip utility.

➤ **To create a smaller file for upload:**

1. Download and install the relevant 7-Zip application from [7-Zip](#)
2. Download and extract the zipped **CxZip.exe** from [Cx7Zip](#)

3. If 7-Zip was not installed in the default location C:\Program Files\7-Zip\7z.exe, then open Cx7Zip.exe.config and modify the path to 7z.exe accordingly:  
`<add key="7zipPath" value="<installation path>\7z.exe"/>`

Run the following command:

```
Cx7Zip.exe <FolderToZip> <ZipFileToCreate.zip>
```

where <FolderToZip> is the source code folder, and <ZipFileToCreate.zip> is the path to the output zip file to be created.

For example:

```
Cx7Zip.exe c:\Projects\TestProject c:\Projects\TestProject.zip
```

The default values can be modified in Cx7Zip.exe.config:

```
<add key="SourcePath" value="C:\longpath"/>  
<add key="DestPath" value="C:\7z.zip"/>
```

---

## CxCMDLineCounter - Count Lines of Code

When uploading a project for scanning, and you would like to know how many lines of code (LOC) are to be scanned, you can use Checkmarx's Cx CMD Line Counter utility.

Note that for JavaScript code the counted lines of code result may not be entirely accurate until after the first scan is performed.

- **To count the lines of code for a project:**
  1. Download and extract the zipped **CxCmdLineCounter.exe** from [Checkmarx Utilities](#).
  2. Open the Command Line Interface (CMD) window and navigate to the folder that contains the CxCmdLineCounter.exe

Run:

```
CxCmdLineCounter [Project Folder] [Result File Path]\[FileName.txt]  
where <Project Folder> is the source code folder, and [Result File  
Path]\[FileName.txt] is the path and file name to the output txt file to be  
created
```

For example:

```
CxCmdLineCounter.exe c:\Projects\TestProject c:\Projects\TestProject.txt
```

Using the above example will create a file named "TestProject.txt" under the projects folder that will have the number of counted lines of all the code under "C:\projects\TestProject".

---

## 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 3 <sup>rd</sup> 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 the following:

- 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 is 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\(v=sql.110\)](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 <b>external fragmentation</b> you have for the given objects. <b>The lower the number the better</b> - 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 ( <b>internal fragmentation</b> ). <b>The higher the number the better</b> 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 <b>heap</b> 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
<i>ALTER INDEX REORGANIZE</i>	> 10% and < = 30%	<p>Reorganizing an index is always executed <b>online</b> 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.</p> <p>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.</p> <p>Reorganize does NOT update statistics, this should be run manually.</p> <p>Single threaded only – regardless of edition</p>
<i>ALTER INDEX REBUILD WITH (ONLINE = ON)</i>	> 30%	<p>Rebuilding an index can be executed online or offline. To achieve availability similar to the reorganize option, you should rebuild indexes online.</p> <p>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.</p> <p>Defragments all levels of the index and update statistics.</p>

### 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 Engine Settings

The CxSAST engine supports single-socket and multi-socket stations. To optimize the CxSAST engine for both configurations, to utilize available cores and to improve the scan time, Checkmarx introduced configuration extensions to set the best policy to the CxSAST engine.

### Introduced Configuration Extensions

The added configuration extensions are the following:

Configuration Extension	Description
PROCESS_AFFINITY_MANAGER_SETTINGS	To be set while installing CxSAST
PARAMETER_VALUE_CORES_NUMBER	To be used after consulting with Technical Support only

### PROCESS\_AFFINITY\_MANAGER\_SETTINGS

This configuration selects the allocation scheme for CPU sockets and cores. It contains Microsoft's affinity setting for single-socket and multi-socket work stations.

- **To configure the Affinity setting:**

Enter the following:

```
"SingleSocket,[AffinitySettingX];MultiSocket,[AffinitySettingY]"
```

The possible values for **[AffinitySettingX]** and **[AffinitySettingY]** are listed in the table below:

AffinitySetting	Description
OldVersion	Operates as it did in early CxSAST versions up to version 8.9. The only issue is that the selected core is not from the optimal socket.
NoLimitation	Allows the operating system to allocate without any CxSAST engine logics. By default, both work station types (single-socket and multi-socket) are allowed.
NewVersion	The CxSAST engine is executed from the same socket. Depending on the engine phase, it runs on one or multiple cores that belong to that socket.

AffinitySetting	Description
NewVersionOneSocketOnly	The CxSAST engine is executed from one socket only. The number of cores must be defined before executing the engine.

➤ **To configure the Affinity setting to operate with CxSAST 9.0:**

Configure the Affinity setting as listed in the table below for the respective Windows operating systems.

Operating System	SingleSocket	MultiSocket	Syntax
Windows Server 2008R2	OldVersion	NoLimitation	SingleSocket, <b>OldVersion</b> ;MultiSocket, <b>NoLimitation</b>
Windows Server 2012R2	NoLimitation	NoLimitation	SingleSocket, <b>NoLimitation</b> ;MultiSocket, <b>NoLimitation</b>
Windows Server 2016	NoLimitation	NoLimitation	SingleSocket, <b>NoLimitation</b> ;MultiSocket, <b>NoLimitation</b>

➤ **To configure the Affinity setting for virtual machines (VM):**

If you prefer to avoid working on multi-socket/multi-core configurations, please note that CxSAST engines works best with the following configuration on Windows hosts:

- Single-socket
- Multi-core

This configuration provides better performance than the multi-socket/single-core configuration.