CxSAST v9.3.0

Setup and Installation Guide

This document is non-binding and for information purposes only

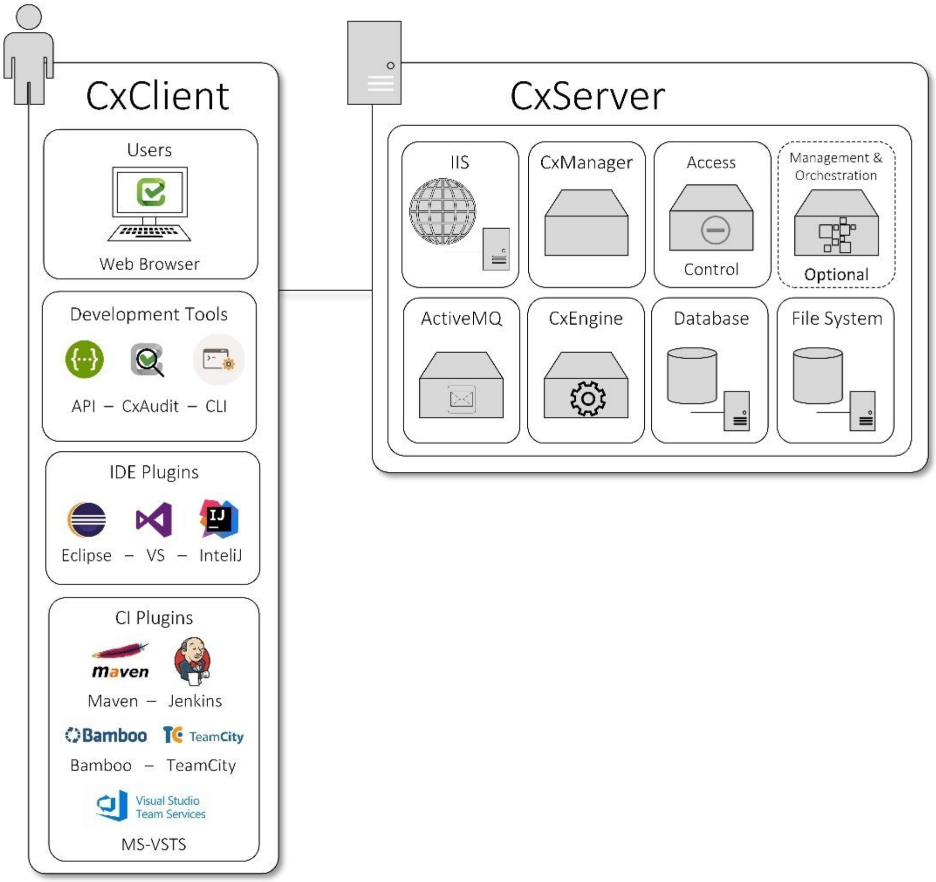
Contents

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 consists of the following components:



CxClient

CxSAST supports the following clients (user interfaces):

- **Web Portal** - provides an intuitive web interface to create, manage and analyze code scan projects in 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 the 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

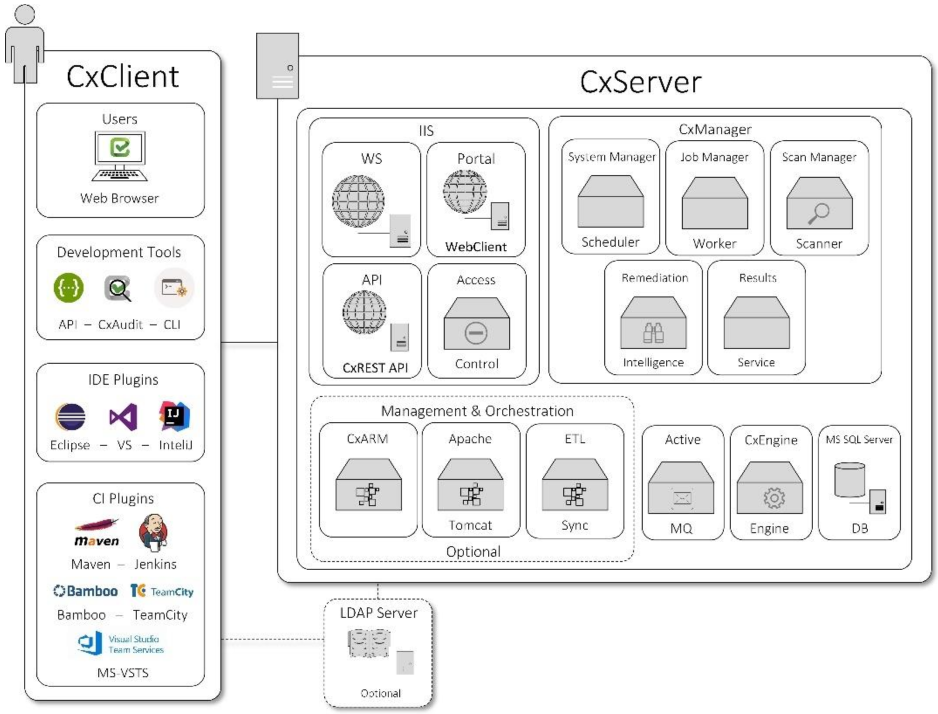
CxSAST supports the following:

- **Centralized Architecture** - all server components are installed on the same host.
- **Distributed Architecture** - some or all the server components are installed on dedicated hosts.
- **High Availability Architecture** - more than one manager is available to control the system management, ensuring that when one manager fails, the system continues to be fully operational.

The communication between CxClient and CxManager and between CxManager and the CxEngine is maintained via HTTP by default, but it can be configured to be maintained via HTTPS instead.

Centralized Architecture

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



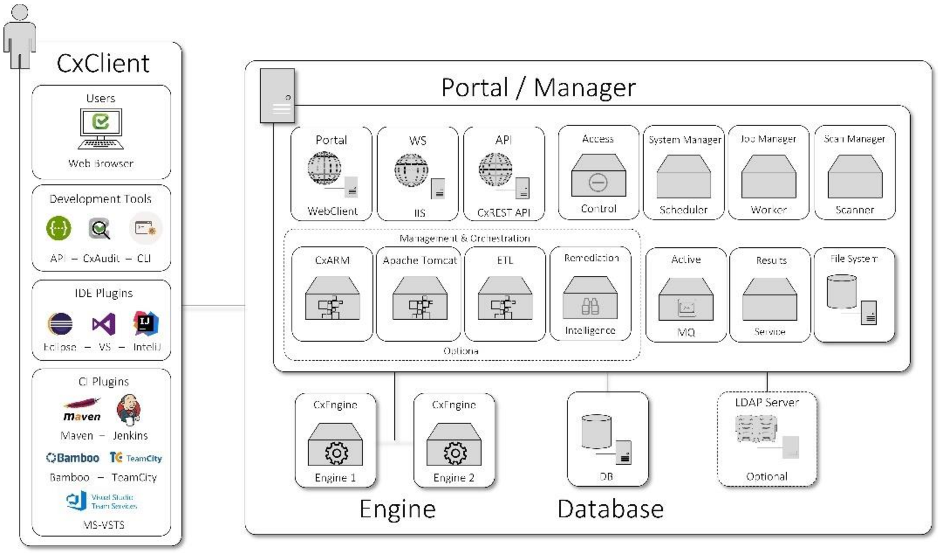
CxSAST also supports following architecture types:

- **Distributed Architecture** - where any or 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.

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).

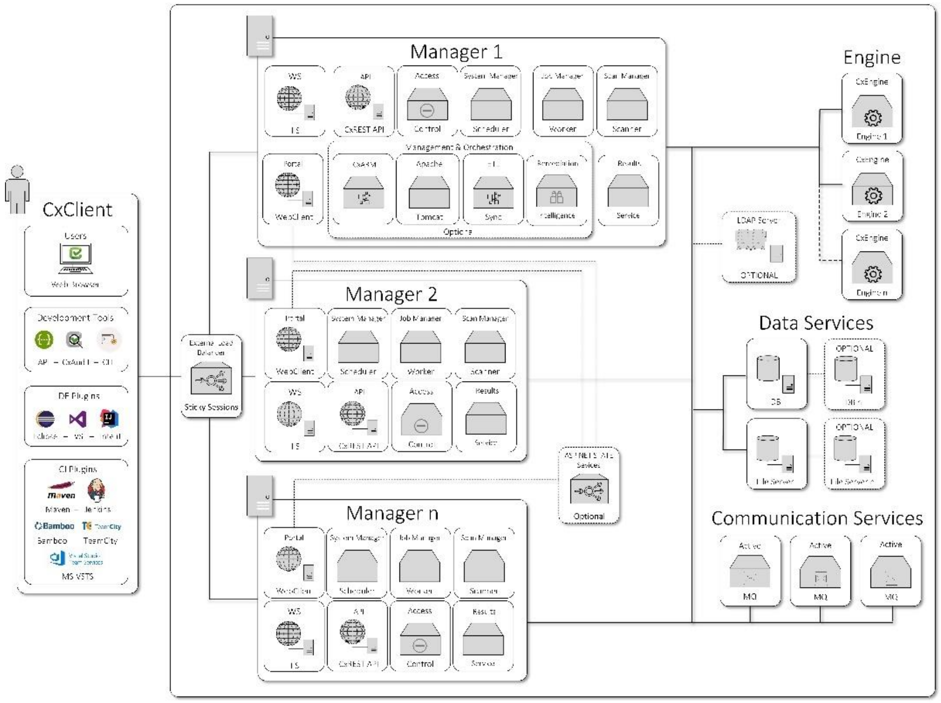
CxSAST also supports following architecture types:

- **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).

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

CxSAST also supports following architecture types:

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

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

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.x Runtime & Hosting is required for hosts on which CxManager is being installed.
- .NET Core 2.1.x 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 2012/2014/2016/2017/2019 (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, 2019	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, 2019	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, 2019
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, 2019	IIS 7/7.5/8/8.5/10

Distributed – CxManager without Management and Orchestration Layer (Production) or Web Portal (Apart of CxManager)

RAM (GB)	Cores	CPU (GHz)	Disk (GB)	OS	Web Server
10	4	2.5	250 (recommended)	Windows Server 2008R2, 2012, 2012R2, 2016, 2019	IIS 7/7.5/8/8.5/10

Distributed – ActiveMQ (Production

RAM (GB)	Cores	CPU (GHz)	Disk (GB)	OS	Web Server
8	4	2.5	250 (recommended)	Windows Server 2008R2, 2012, 2012R2, 2016, 2019	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, 2019

- 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), ActiveMQ
Network	<30ms	CxEngines
Disk I/O	<20ms avg	CxManager, CxEngine, SQL Server, ActiveMQ

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			

Operating Systems	CxSAST	CxOSA	Access Control	Management &Orchestration
Windows Server 2016	V			
Windows Server 2019	V			
Linux (CentOS, Ubuntu, Fedora, RHEL)	V			

- Windows Server Core is not supported.

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

SQL Server	CxSAST	CxOSA	Access Control	Management &Orchestration
2019	V			

- AWS RDS can be used (see AWS RDS secton 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.

Supported Integrations and Plugins

This page is not updated any further. For updated information on integrations and plugins, refer to the Integrations Documentation

Supported Browsers

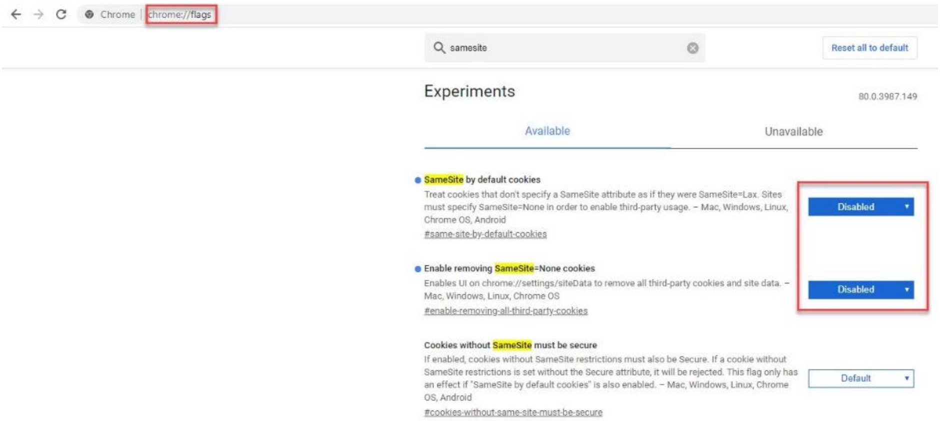
The following browsers have been tested with CxSAST / CxOSA v9.0.0 and Codebashing v3.2.0

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.



SameSite by default cookies
Treat cookies that don't specify a SameSite attribute as if they were SameSite=Lax. Sites must specify SameSite=None in order to enable third-party usage. – Mac, Windows, Linux, Chrome OS, Android
#same-site-by-default-cookies
Disabled

Enable removing SameSite=None cookies
Enables UI on chrome://settings/siteData to remove all third-party cookies and site data. – Mac, Windows, Linux, Chrome OS
#enable-removing-all-third-party-cookies
Disabled

Cookies without SameSite must be secure
If enabled, cookies without SameSite restrictions must also be Secure. If a cookie without SameSite restrictions is set without the Secure attribute, it will be rejected. This flag only has an effect if "SameSite by default cookies" is also enabled. – Mac, Windows, Linux, Chrome OS, Android
#cookies-without-same-site-must-be-secure
Default

Preparing the Environment

Once you understand CxSAST System Architecture Overview, before installing CxSAST, make sure that 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):

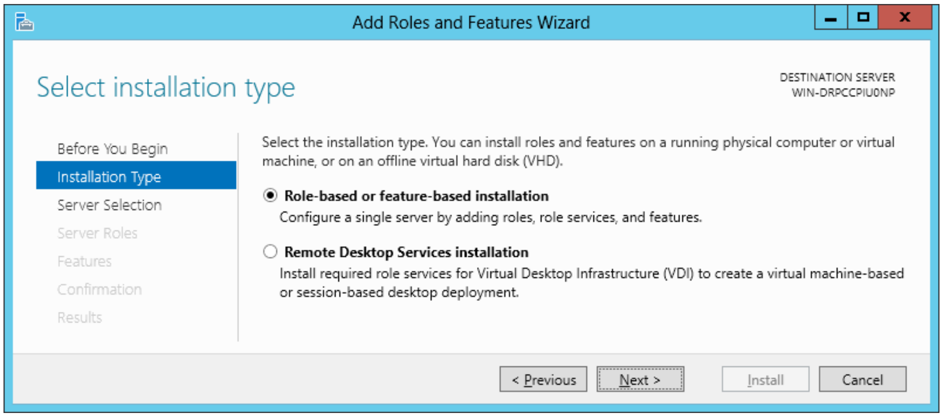
Installing IIS 10 on Windows 10

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. Ensure the following role services are selected:
    - IIS Management Console
    - IIS Metabase Compatibility
    - ASP.NET
    - Static Content

Installing IIS 8 on Windows Server 2012

For further 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:

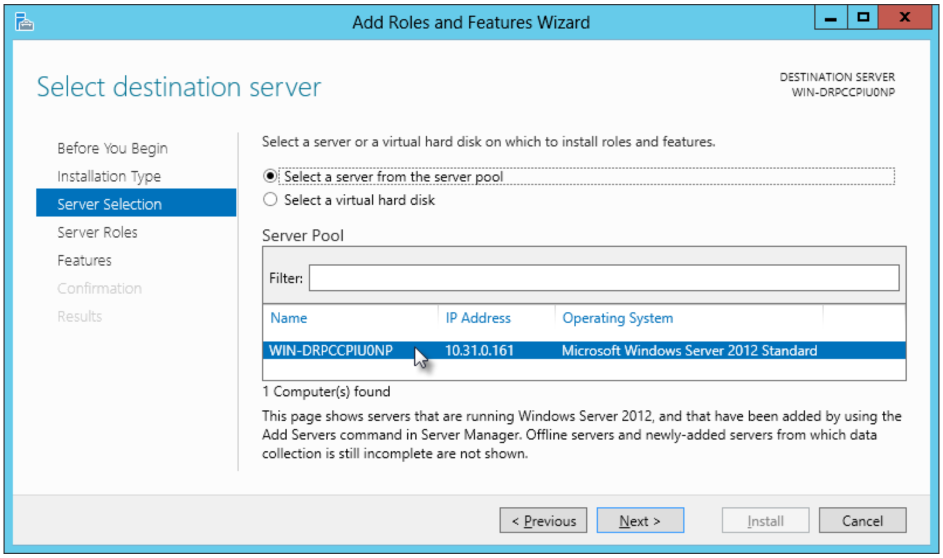


Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

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



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-DRPCCPIUONP

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

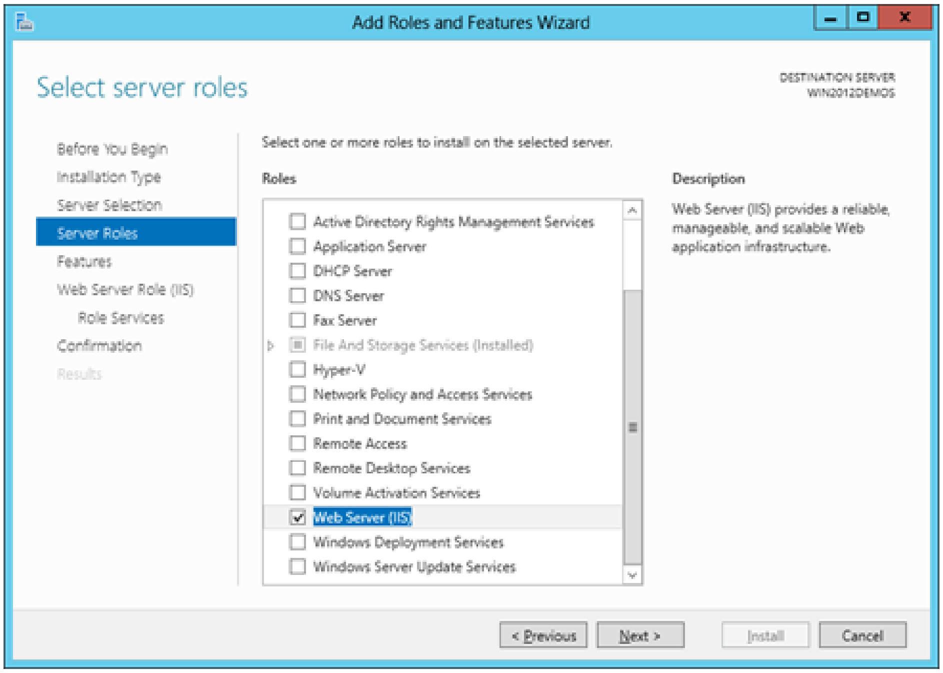
Filter:

Name	IP Address	Operating System
WIN-DRPCCPIUONP	10.31.0.161	Microsoft Windows Server 2012 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

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



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN2012DEMOS

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

Select one or more roles to install on the selected server.

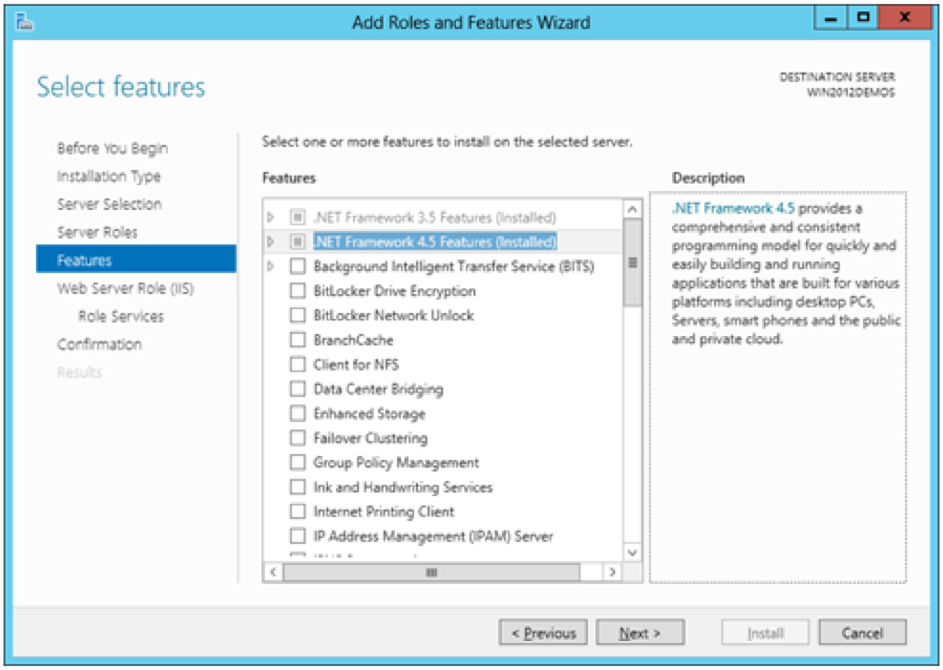
Roles

□ Active Directory Rights Management Services
□ Application Server
□ DHCP Server
□ DNS Server
□ Fax Server
▷ ▣ File And Storage Services (Installed)
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
☑ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

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



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN2012DEMOS

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

Select one or more features to install on the selected server.

Features

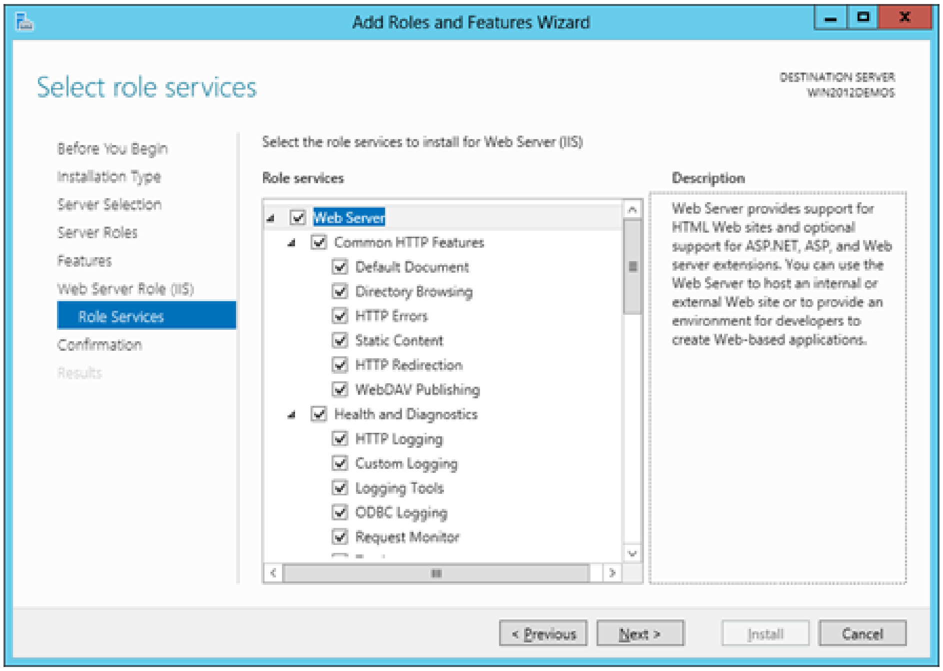
- ▣ .NET Framework 3.5 Features (Installed)
- ▣ .NET Framework 4.5 Features (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ Ink and Handwriting Services
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server

Description

.NET Framework 4.5 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.

< Previous | Next > | Install | Cancel

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



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN2012DEMOS

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Web Server (IIS)

Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☑ HTTP Redirection
    - ☑ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - ☑ Custom Logging
    - ☑ Logging Tools
    - ☑ ODBC Logging
    - ☑ Request Monitor

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

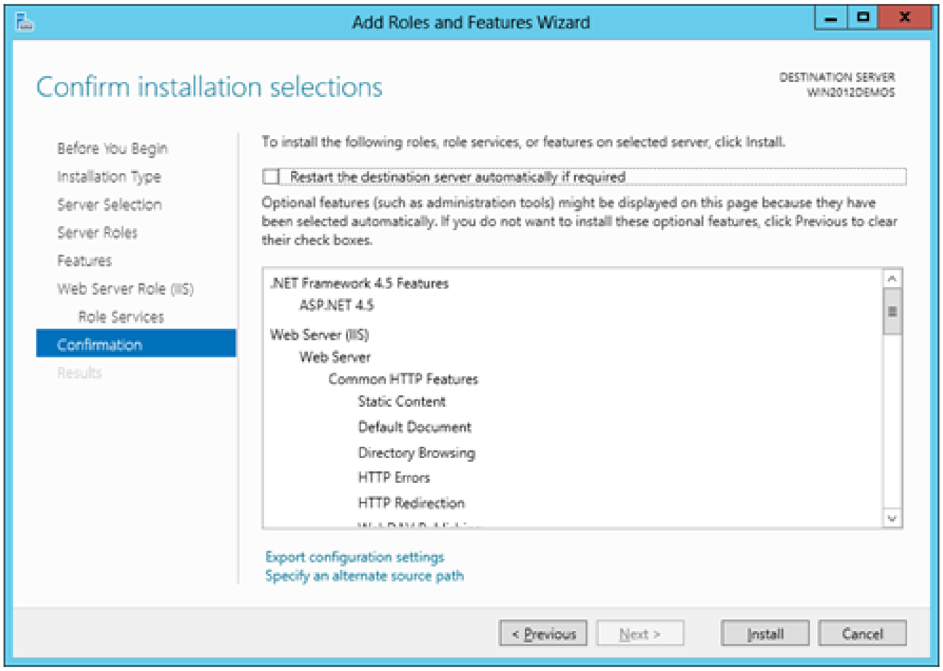
< Previous | Next > | Install | Cancel

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:**



Confirm installation selections

DESTINATION SERVER
WIN2012DEMOS

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
.NET Framework 4.5 Features
    ASP.NET 4.5
Web Server (IIS)
    Web Server
        Common HTTP Features
            Static Content
            Default Document
            Directory Browsing
            HTTP Errors
            HTTP Redirection
```

Export configuration settings
Specify an alternate source path

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 which case make sure to include IIS with:

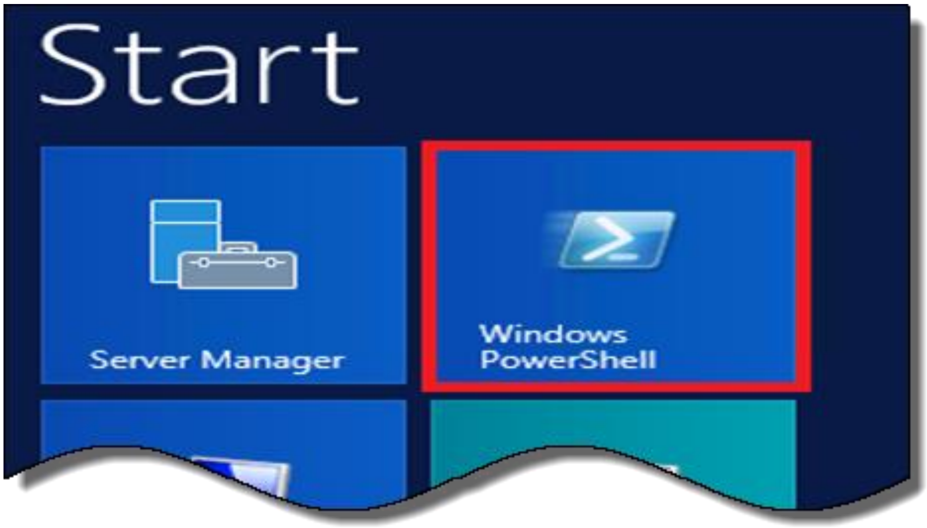
- IIS Management Console
- Static Content
- ASP.NET 4.5 with all dependencies
- IIS 6 Metabase Compatibility
- .Net Framework 4.5 Features -> WCF Services -> HTTP Activation

Installing IIS 8.5 on Windows Server 2012 R2

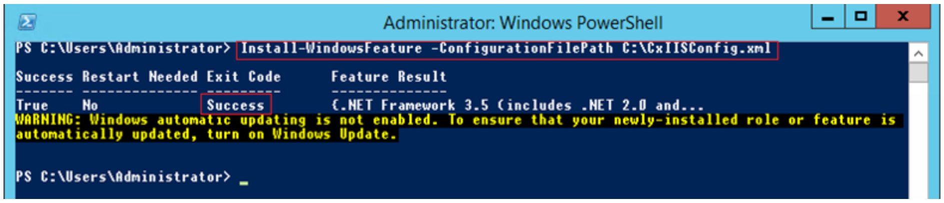
For additional information, refer to https://docs.microsoft.com/en-us/iis/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2

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



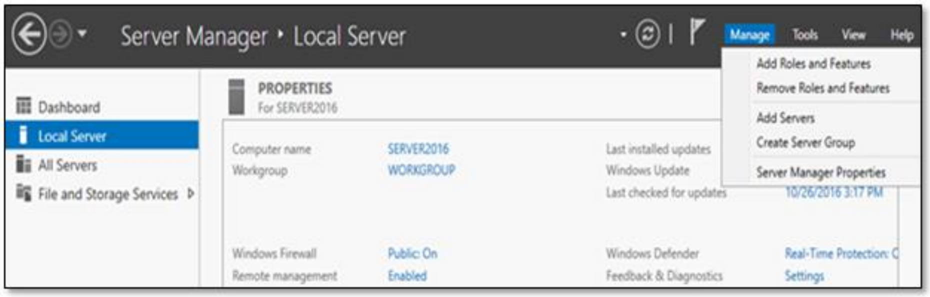
```
PS C:\Users\Administrator> Install-WindowsFeature -ConfigurationFilePath C:\CxIISConfig.xml

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> _
```

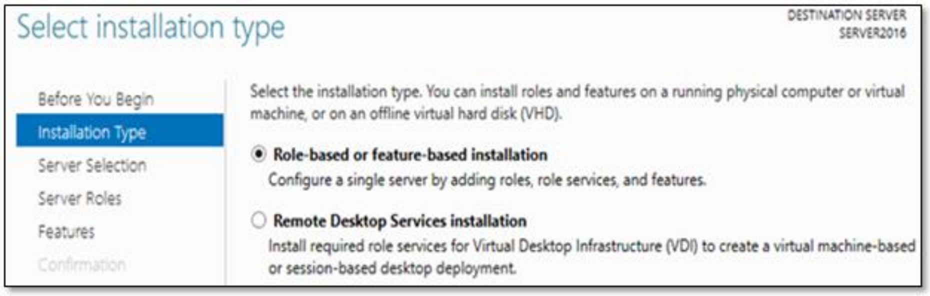
Installing IIS 10 on Windows Server 2016

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



Computer name SERVER2016
Workgroup WORKGROUP
Last installed updates
Windows Update
Last checked for updates 10/26/2016 3:17 PM
Windows Firewall Public: On
Remote management Enabled
Windows Defender Real-Time Protection: O
Feedback & Diagnostics Settings

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

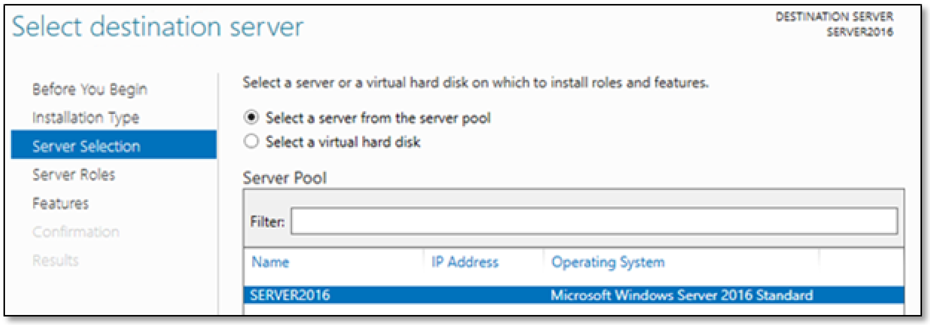


Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

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



Select a server or a virtual hard disk on which to install roles and features.

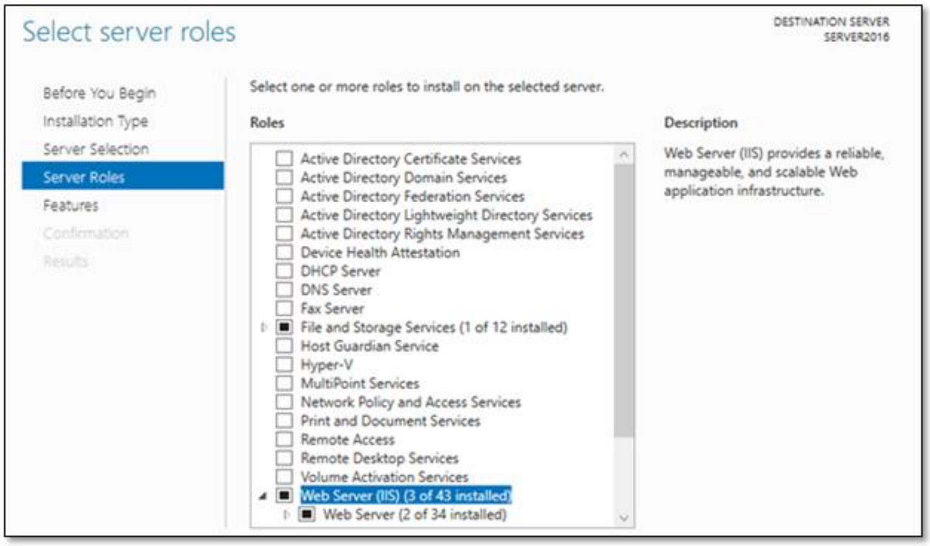
● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
SERVER2016		Microsoft Windows Server 2016 Standard

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



Select server roles

DESTINATION SERVER
SERVER2016

Select one or more roles to install on the selected server.

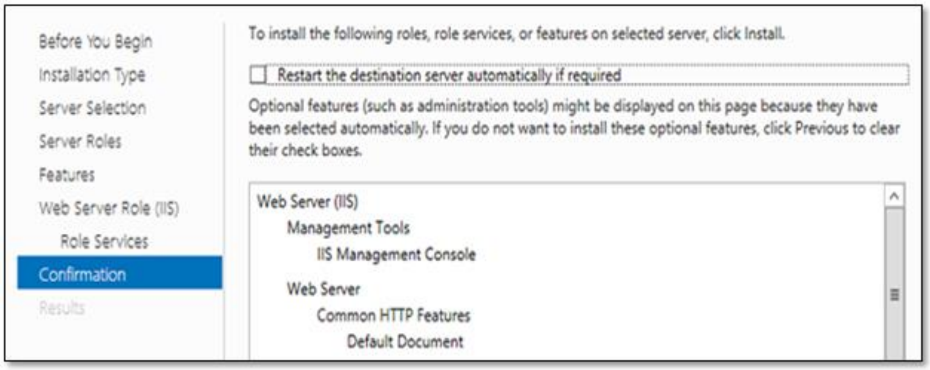
Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (3 of 43 installed)
  - ■ Web Server (2 of 34 installed)

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

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



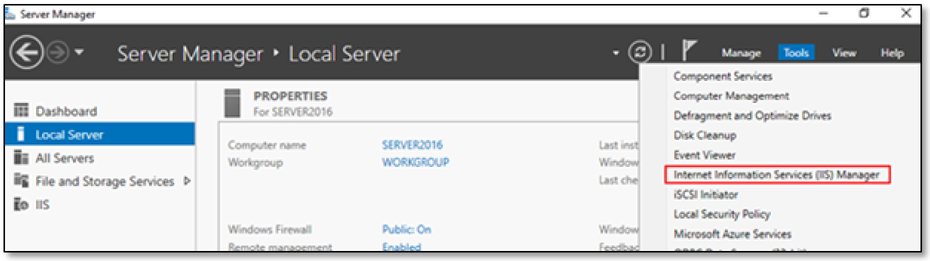
To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Web Server (IIS)
  Management Tools
    IIS Management Console
  Web Server
    Common HTTP Features
      Default Document

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

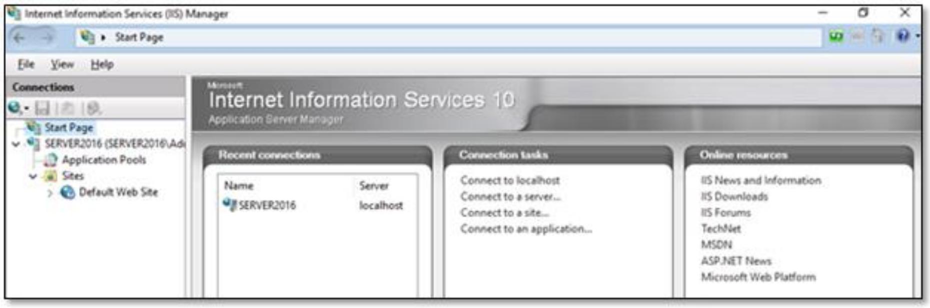


PROPERTIES
For SERVER2016

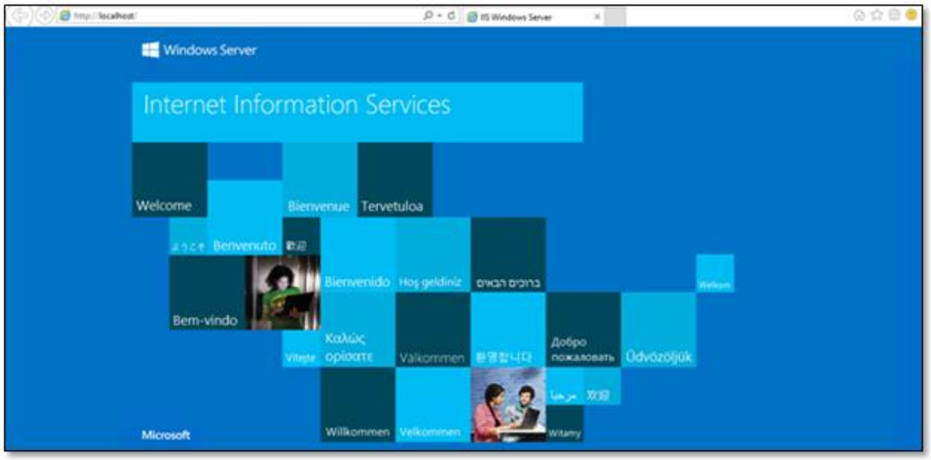
Computer name SERVER2016
Workgroup WORKGROUP

Windows Firewall Public: On
Remote management Enabled

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



9. Confirm that the Web server works by using http://localhost.

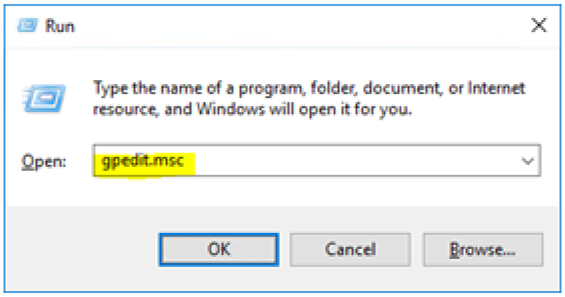


For correct synchronization, the Checkmarx Server/CxAudit and the database must be on the same time zone.

Enabling Long Path Support in Windows 10 and Server 2016

Traditionally, Windows operating systems do not support path or filenames with more than 260 characters. However, Windows 10 and Windows Server 2016 now provide support for these 'long paths'.

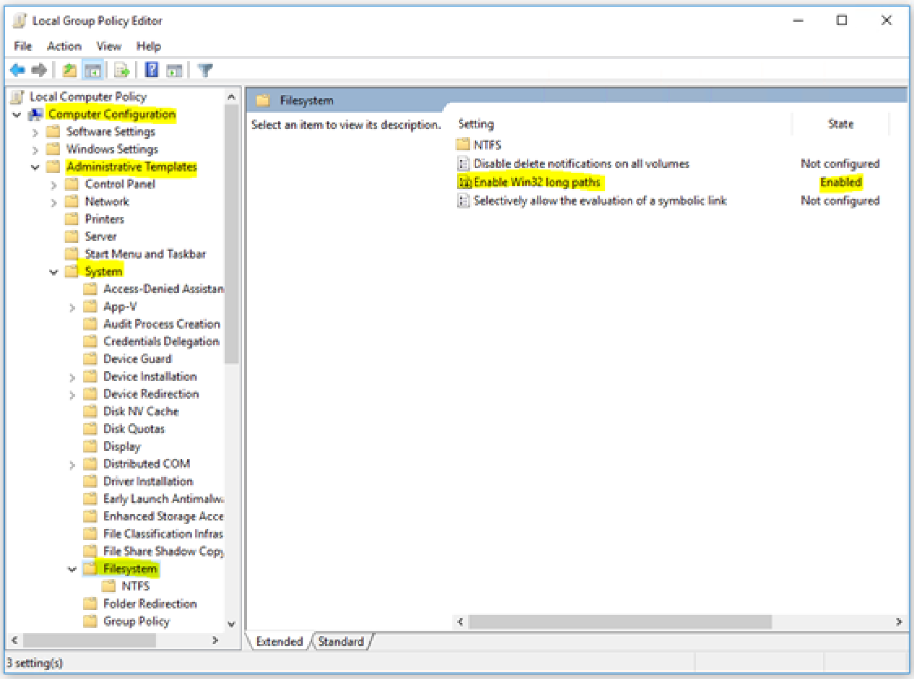
1. In Windows 10/Server 2016, open the Run dialog (**Start** > **Programs** > **Accessories** > **Run**).



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

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



Select an item to view its description.

Setting	State
NTFS	
Disable delete notifications on all volumes	Not configured
Enable Win32 long paths	Enabled
Selectively allow the evaluation of a symbolic link	Not configured

3 setting(s)

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

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 the archive, extract the installation executable **CxSetup.exe** 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.

Installing CxSAST in a Centralized Environment

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

Installation Permissions

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

SQL Server 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 a login User for Windows 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 is unavailable, certain prerequisites must be fulfilled prior to the installation.

- Build three SQL databases using the names CxDB, CxActivity, and CxARM.
- Create a 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 be used - To make RDS work you need to create three databases, CxDB, CxActivity, and CxARM. Give the user that you created for Checkmarx dbo privileges to the newly created databases. Run the installer again and when the installation connects to the Database and you see a message about the three databases already existing, just click continue. Once the installation is complete the RDS should work.

Preparing for Installation

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 the archive, extract the installation executable **CxSetup.exe** 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.

Obtaining and Validating a License

1. It is recommended to obtain a license before you start your installation. This way you are able to provide the license during the installation and are able to use the product immediately.
2. Your CxSAST license is tied to a specific station (server); so all you have to do is to run the Cx HID Generator and an HID (hardware identification number) is provided. The HID Generator can be downloaded from the Cx Utilities page.
3. 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

➢ **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**.

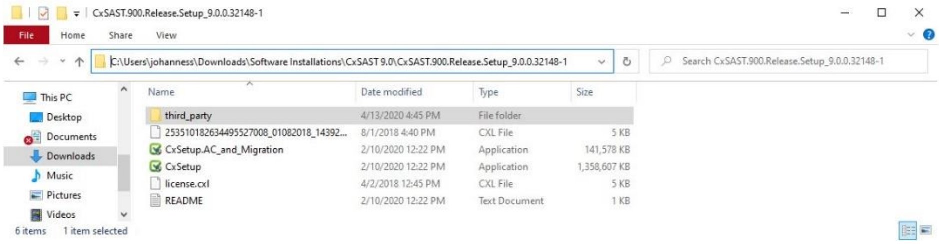
- **C++ Redist 2010 and 2015 SP3**
- **IIS v7.0 or higher**
- **ASP.NET Core 2.1.16 (or higher 2.1.x versions) Runtime & Hosting**
- **MS SQL**
- **Java JRE 1.8.0 (64-bit)**

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.
- 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.

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**.



C:\Users\johanness\Downloads\Software Installations\CxSAST 9.0\CxSAST.900.Release.Setup_9.0.0.32148-1

Search CxSAST.900.Release.Setup_9.0.0.32148-1

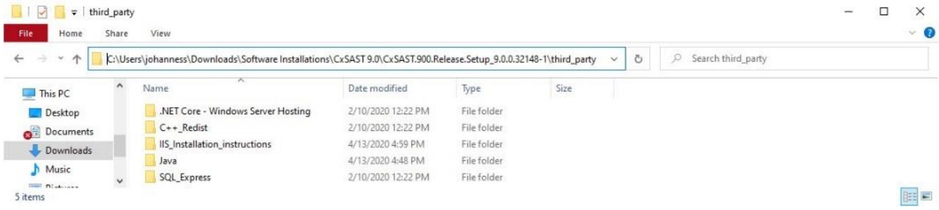
Name	Date modified	Type	Size
third_party	4/13/2020 4:45 PM	File folder	
253510182634495527008_01082018_14392...	8/1/2018 4:40 PM	CXL File	5 KB
CxSetup.AC_and_Migration	2/10/2020 12:22 PM	Application	141,578 KB
CxSetup	2/10/2020 12:22 PM	Application	1,358,607 KB
license.cxl	4/2/2018 12:45 PM	CXL File	5 KB
README	2/10/2020 12:22 PM	Text Document	1 KB

6 items 1 item selected

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.



C:\Users\johanness\Downloads\Software Installations\CxSAST 9.0\CxSAST.900.Release.Setup_9.0.0.32148-1\third_party

Search third_party

Name	Date modified	Type	Size
.NET Core - Windows Server Hosting	2/10/2020 12:22 PM	File folder	
C++_Redist	2/10/2020 12:22 PM	File folder	
IIS_Installation_instructions	4/13/2020 4:59 PM	File folder	
Java	4/13/2020 4:48 PM	File folder	
SQL_Express	2/10/2020 12:22 PM	File folder	

5 items

2. Run the setup and follow the onscreen instructions.
3. Repeat this for the remaining components that have to be installed yet.

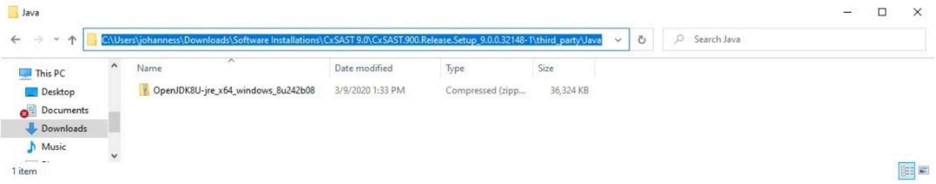
- When installing SQL, you are asked to define a password to access the internal CxARM database. This password must not exceed 32 characters.
- If you upgrade, you may have to reset the existing password as passwords could exceed 32 characters in previous versions.

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.



C:\Users\johanness\Downloads\Software Installations\CxSAST 9.0\CxSAST.900.Release.Setup_9.0.0.32148-1\third_party\Java

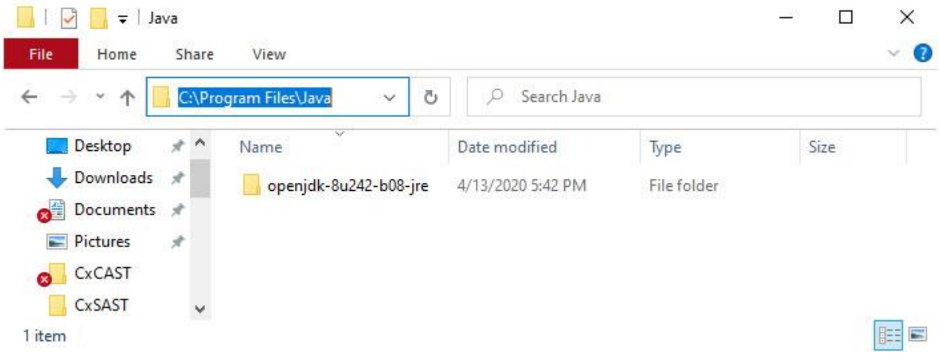
Name	Date modified	Type	Size
OpenJDK8U-jre_x64_windows_8u242b08	3/9/2020 1:33 PM	Compressed (zipp...	36,324 KB

2. Open the zip archive and extract its content to a folder of your choice.

- The zip archive 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.

- 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.



C:\Program Files\Java

Name	Date modified	Type	Size
openjdk-8u242-b08-jre	4/13/2020 5:42 PM	File folder	

Installing CxSAST

Prerequisites and Recommendations

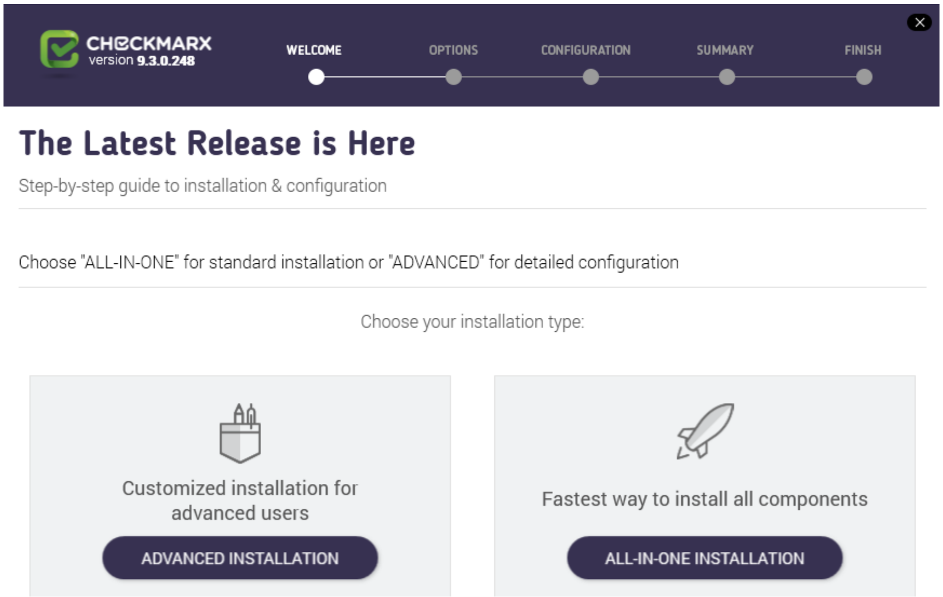
- The required Web Server for Checkmarx is Microsoft IIS Server.
- SQL 2012 Express SP2 is included with the CxSAST installer. It is installed, if there is no other version of SQL already installed.

Installation

- You can directly upgrade to CxSAST 9.3 from version 9.2 or 9.0.
- For upgrading from version 8.8 or 8.9, you have to first upgrade to version 9.0, which requires migrating the Access Control data as explained in Access Control Data Migration Installer.

1. Once you have downloaded the CxSAST Installation package and made the third-party components available, run **CxSetup.exe**.

If you install CxSAST without any previous installations of CxSAST on your host



The Latest Release is Here

Step-by-step guide to installation & configuration

Choose "ALL-IN-ONE" for standard installation or "ADVANCED" for detailed configuration

Choose your installation type:

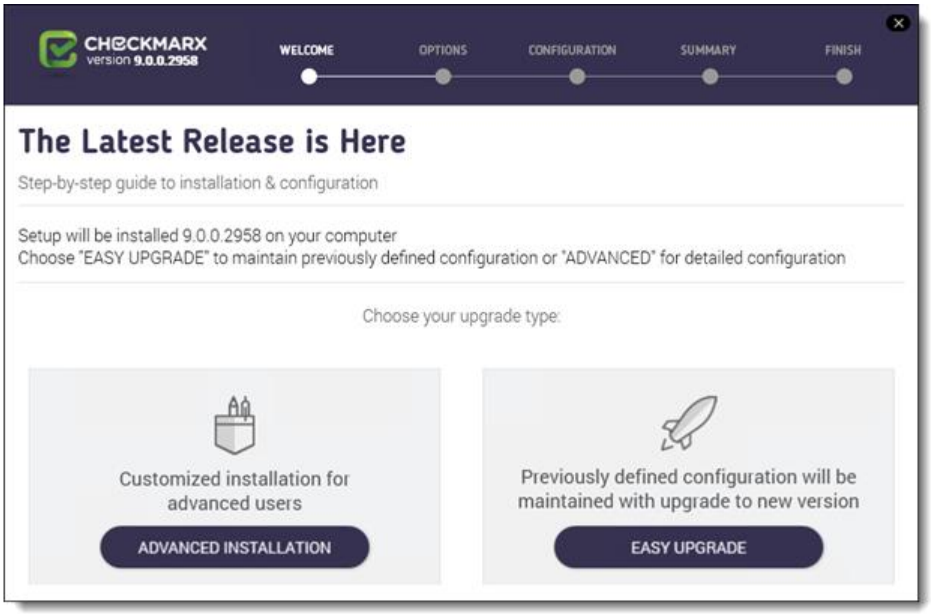
Customized installation for advanced users

Fastest way to install all components

- Click <**ALL-IN-ONE-INSTALLATION**> to continue the centralized installation, or click <**X**> to exit.

- By default, all components including Management & Orchestration install with CxSAST. To exclude Management & Orchestration, click <**ADVANCED INSTALLATION**> and then clear **Install Management (M&O)** when you are asked to select the installation options.

If you install a newer build or upgrade from version 9.02 or 9.2, click here to continue



The Latest Release is Here

Step-by-step guide to installation & configuration

Setup will be installed 9.0.0.2958 on your computer
Choose "EASY UPGRADE" to maintain previously defined configuration or "ADVANCED" for detailed configuration

Choose your upgrade type:

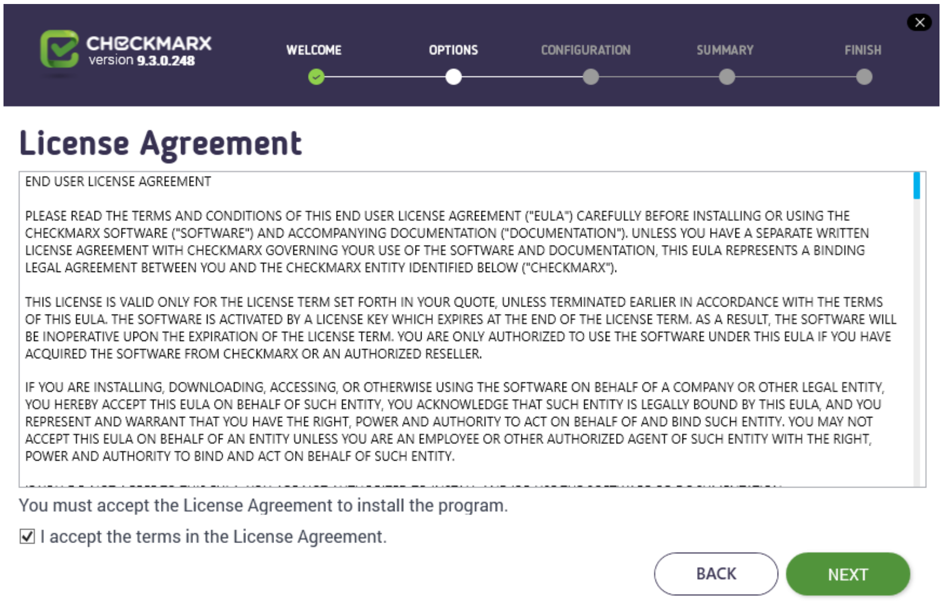
Customized installation for advanced users

Previously defined configuration will be maintained with upgrade to new version

- To upgrade while preserving your current configuration, click <**EASY UPGRADE**> to continue.
- To modify the current configuration, for example to include or exclude Management & Orchestration, click <**ADVANCED INSTALLATION**> and then select or clear **Install Management (M&O)** respectively.

- If you wish to install components on more than one host, refer to Installing CxSAST in a Distributed Environment for further information and instructions.

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



License Agreement

END USER LICENSE AGREEMENT

PLEASE READ THE TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE INSTALLING OR USING THE CHECKMARX SOFTWARE ("SOFTWARE") AND ACCOMPANYING DOCUMENTATION ("DOCUMENTATION"). UNLESS YOU HAVE A SEPARATE WRITTEN LICENSE AGREEMENT WITH CHECKMARX GOVERNING YOUR USE OF THE SOFTWARE AND DOCUMENTATION, THIS EULA REPRESENTS A BINDING LEGAL AGREEMENT BETWEEN YOU AND THE CHECKMARX ENTITY IDENTIFIED BELOW ("CHECKMARX").

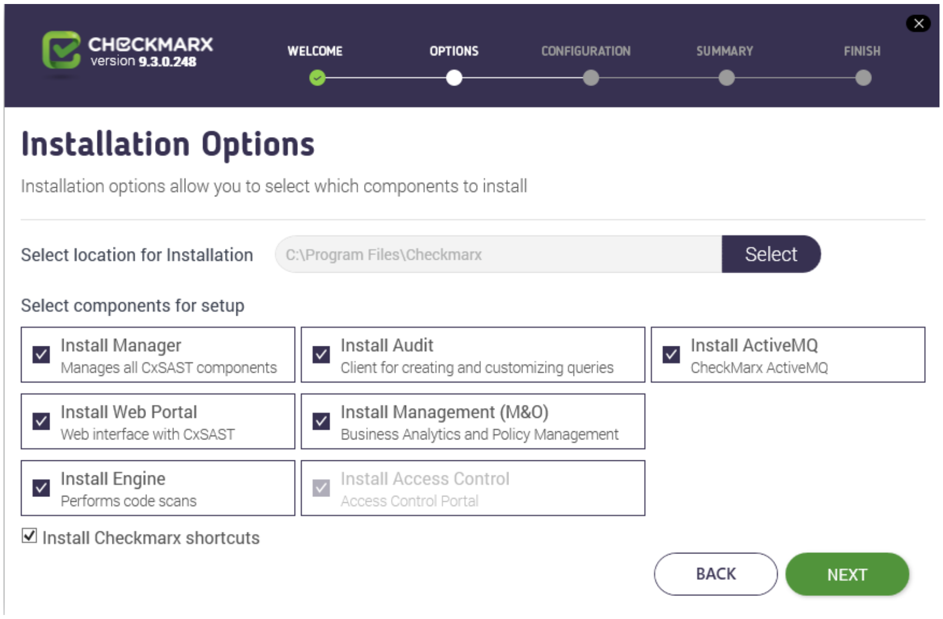
THIS LICENSE IS VALID ONLY FOR THE LICENSE TERM SET FORTH IN YOUR QUOTE, UNLESS TERMINATED EARLIER IN ACCORDANCE WITH THE TERMS OF THIS EULA. THE SOFTWARE IS ACTIVATED BY A LICENSE KEY WHICH EXPIRES AT THE END OF THE LICENSE TERM. AS A RESULT, THE SOFTWARE WILL BE INOPERATIVE UPON THE EXPIRATION OF THE LICENSE TERM. YOU ARE ONLY AUTHORIZED TO USE THE SOFTWARE UNDER THIS EULA IF YOU HAVE ACQUIRED THE SOFTWARE FROM CHECKMARX OR AN AUTHORIZED RESELLER.

IF YOU ARE INSTALLING, DOWNLOADING, ACCESSING, OR OTHERWISE USING THE SOFTWARE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU HEREBY ACCEPT THIS EULA ON BEHALF OF SUCH ENTITY, YOU ACKNOWLEDGE THAT SUCH ENTITY IS LEGALLY BOUND BY THIS EULA, AND YOU REPRESENT AND WARRANT THAT YOU HAVE THE RIGHT, POWER AND AUTHORITY TO ACT ON BEHALF OF AND BIND SUCH ENTITY. YOU MAY NOT ACCEPT THIS EULA ON BEHALF OF AN ENTITY UNLESS YOU ARE AN EMPLOYEE OR OTHER AUTHORIZED AGENT OF SUCH ENTITY WITH THE RIGHT, POWER AND AUTHORITY TO BIND AND ACT ON BEHALF OF SUCH ENTITY.

You must accept the License Agreement to install the program.

☑ I accept the terms in the License Agreement.

2. Review and accept the license agreement by checking **I accept the terms in the License Agreement.**
3. Click <**NEXT**> to continue. If you clicked <**ADVANCED INSTALLATION**> before, the additional **Installation Options** window is displayed with all components selected.



Installation Options

Installation options allow you to select which components to install

Select location for Installation: C:\Program Files\Checkmarx

Select components for setup

☑ Install Manager – Manages all CxSAST components
☑ Install Audit – Client for creating and customizing queries
☑ Install ActiveMQ – CheckMarx ActiveMQ
☑ Install Web Portal – Web interface with CxSAST
☑ Install Management (M&O) – Business Analytics and Policy Management
☑ Install Engine – Performs code scans
☑ Install Access Control – Access Control Portal

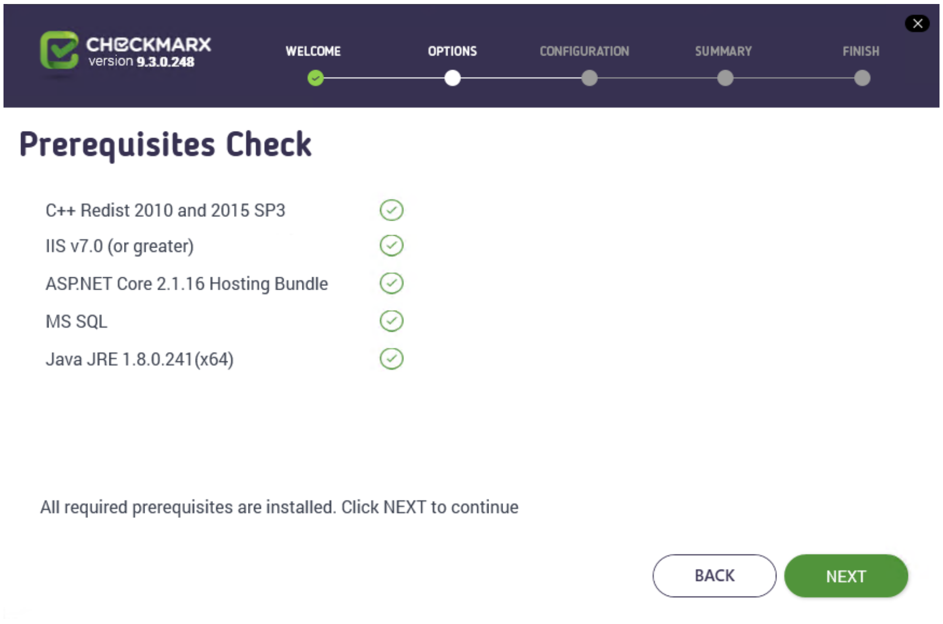
☑ Install Checkmarx shortcuts

4. 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 feature. For further information and instructions, refer to Modifying CxSAST.

5. Click <**NEXT**>. The **Prerequisites Check** window is displayed, indicating the status of all required third-party components.



Prerequisites Check

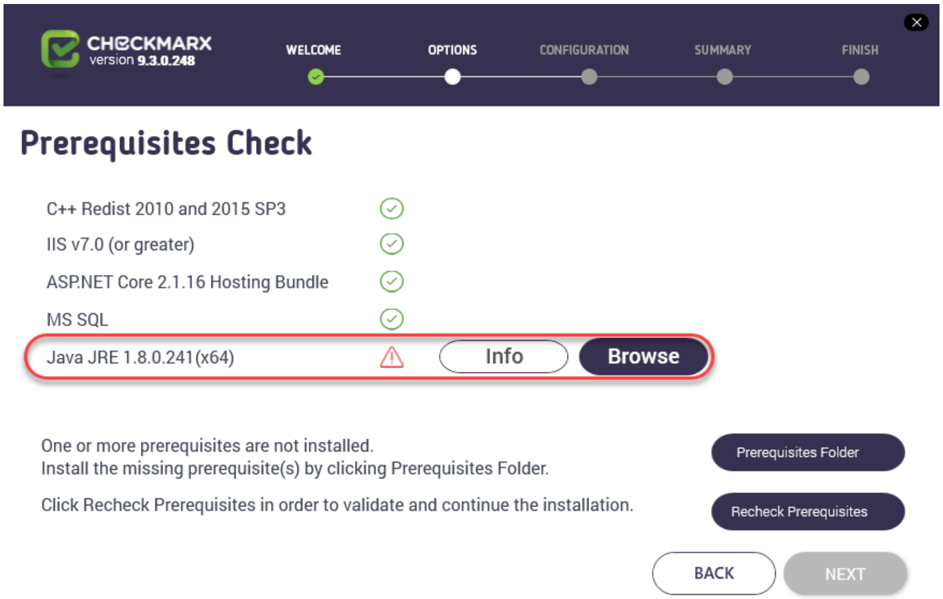
C++ Redist 2010 and 2015 SP3	✓
IIS v7.0 (or greater)	✓
ASP.NET Core 2.1.16 Hosting Bundle	✓
MS SQL	✓
Java JRE 1.8.0.241(x64)	✓

All required prerequisites are installed. Click NEXT to continue

- Available components are labeled ✓. All prerequisites must be available, otherwise the setup cannot be completed and CxSAST is not installed.
- 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.



Prerequisites Check

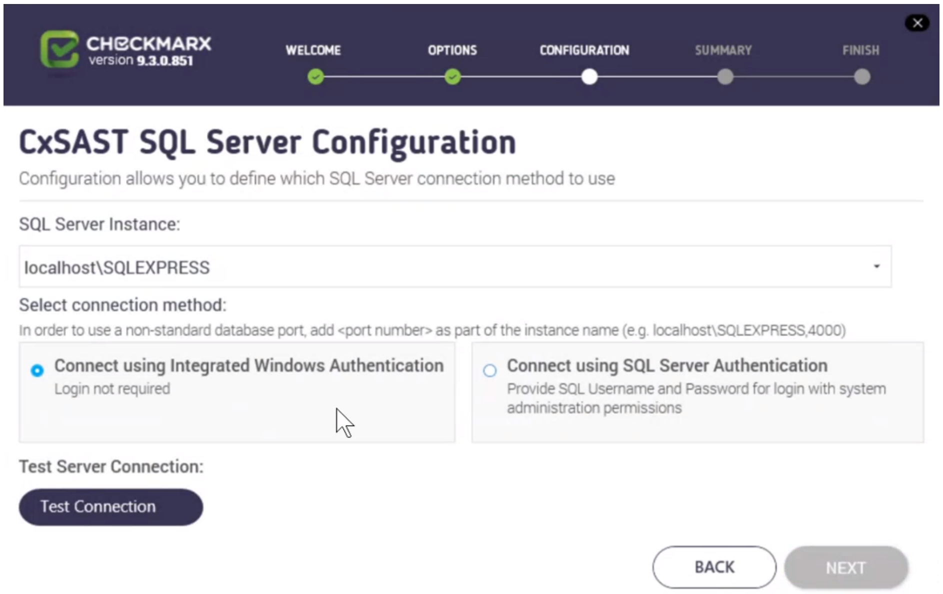
C++ Redist 2010 and 2015 SP3	✓
IIS v7.0 (or greater)	✓
ASP.NET Core 2.1.16 Hosting Bundle	✓
MS SQL	✓
Java JRE 1.8.0.241(x64)	⚠

One or more prerequisites are not installed.
Install the missing prerequisite(s) by clicking Prerequisites Folder.

Click Recheck Prerequisites in order to validate and continue the installation.

- 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.

6. Once all prerequisite components are installed, click <**NEXT**> to continue. The **CxSAST SQL Server Configuration** window is displayed.



CxSAST SQL Server Configuration

Configuration allows you to define which SQL Server connection method to use

SQL Server Instance:

localhost\SQLEXPRESS

Select connection method:

In order to use a non-standard database port, add <port number> as part of the instance name (e.g. localhost\SQLEXPRESS,4000)

● Connect using Integrated Windows Authentication
Login not required

○ Connect using SQL Server Authentication
Provide SQL Username and Password for login with system administration permissions

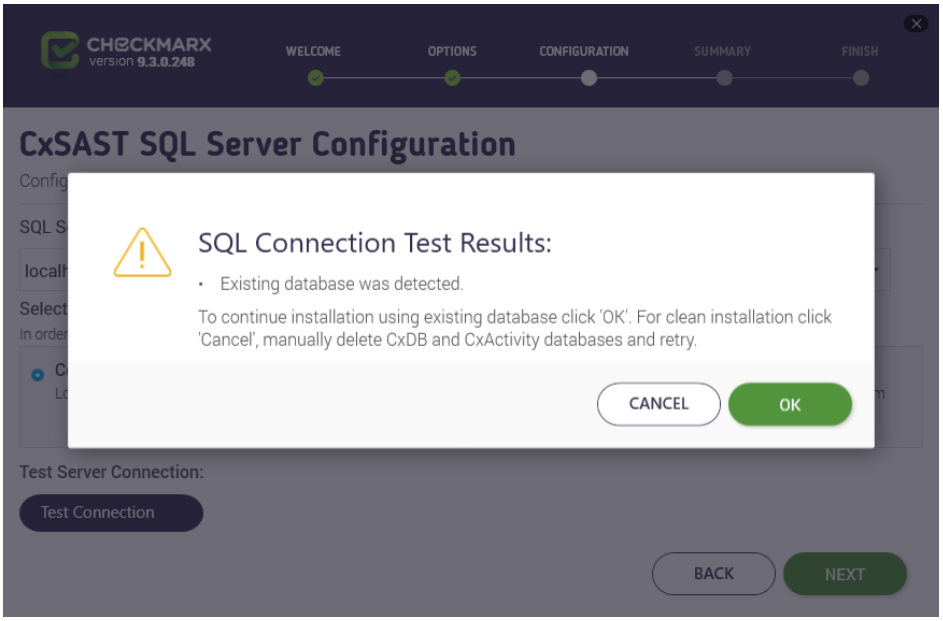
Test Server Connection:

7. 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.

8. 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 to log in with SA permissions).
9. Click **<Test Connection>**.
   - If the database was not in use, a message appears that indicates that the connection was successful.
   - If a previously used database exists, A message appears that a database was detected. In this case, you may continue using the database or re-install it as explained in the message.

- 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 host is a member of a Windows domain. If is not part of a Windows domain, either join the host to a domain and restart it, or connect using SQL Server Authentication.
- The SQL Server Browser Windows service is running. If it is not running, enable and start it.



CxSAST SQL Server Configuration

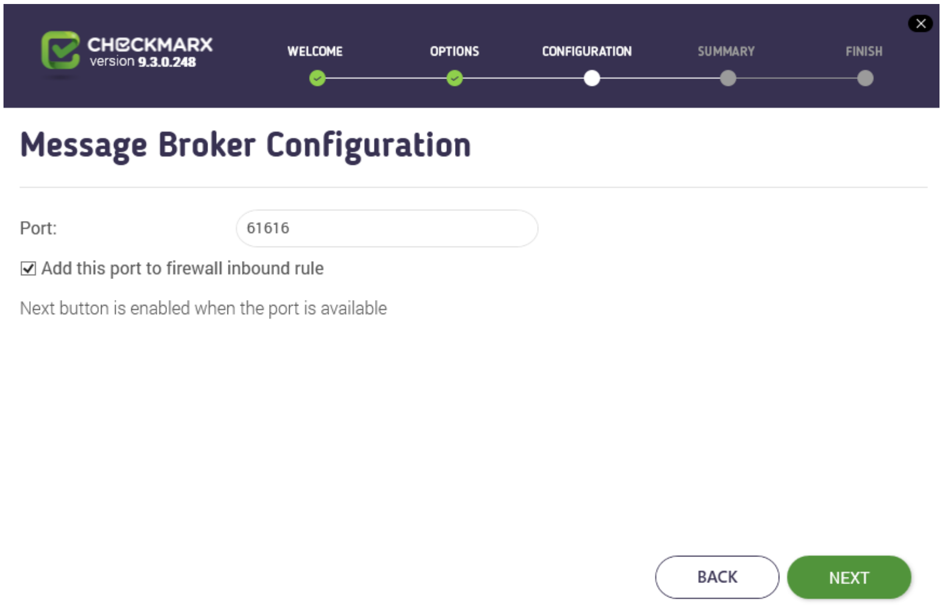
SQL Connection Test Results:

- Existing database was detected.

To continue installation using existing database click 'OK'. For clean installation click 'Cancel', manually delete CxDB and CxActivity databases and retry.

Test Server Connection:

10. Click <**OK**>, and then click <**NEXT**>to continue. The **Message Broker Configuration** window is displayed.



Message Broker Configuration

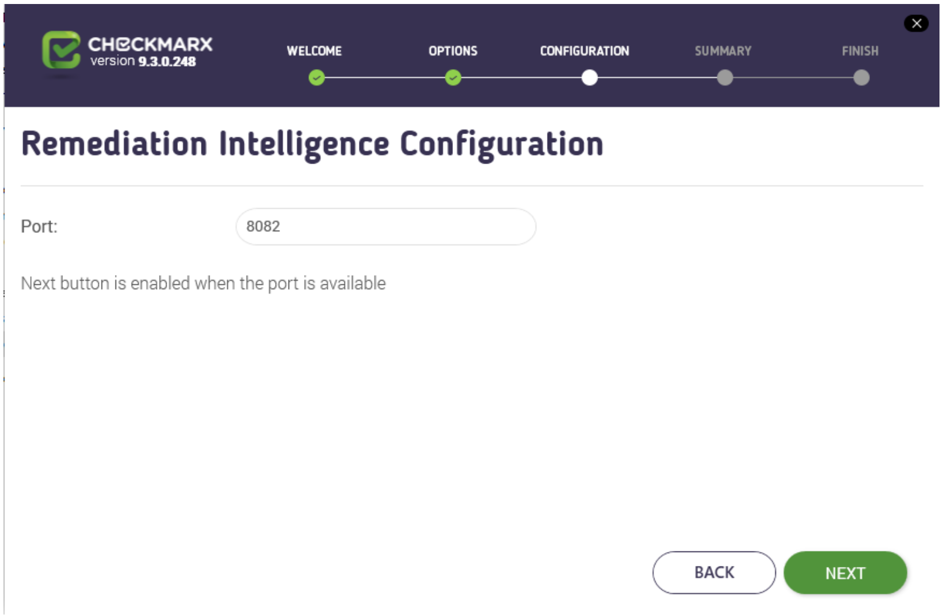
Port: 61616

☑ Add this port to firewall inbound rule

Next button is enabled when the port is available

- The default ActiveMQ port is **61616**.
- <**NEXT**> 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

11. Click **<NEXT>**. If installing Management and Orchestration, the **Remediation Intelligence Configuration** window is displayed.



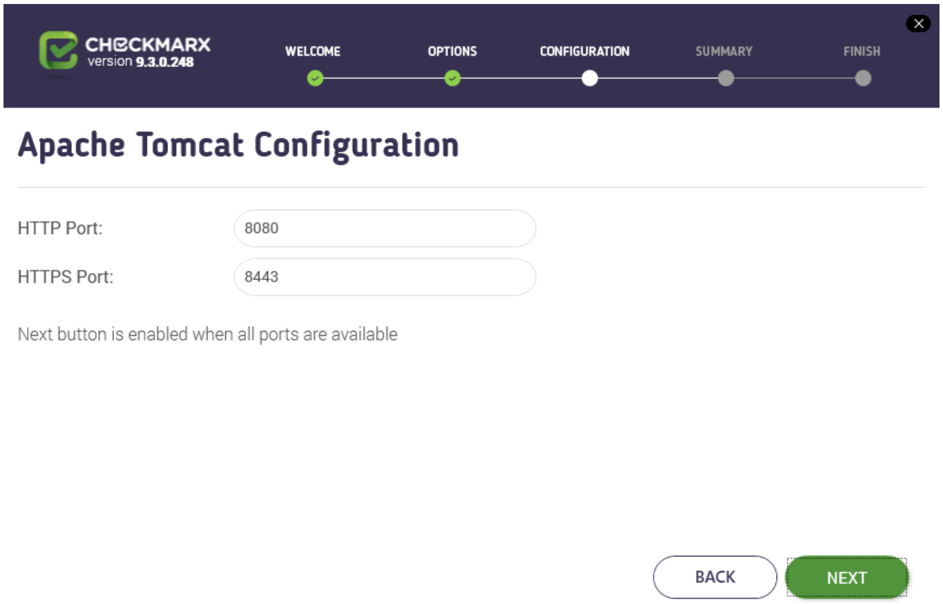
Remediation Intelligence Configuration

Port: 8082

Next button is enabled when the port is available

- 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**.
- <**NEXT**> is enabled, if the default port is available. If unavailable, define another available port.

12. Click <**NEXT**>. If installing Management and Orchestration, the **Apache Tomcat Configuration** window is displayed.



Apache Tomcat Configuration

HTTP Port: 8080

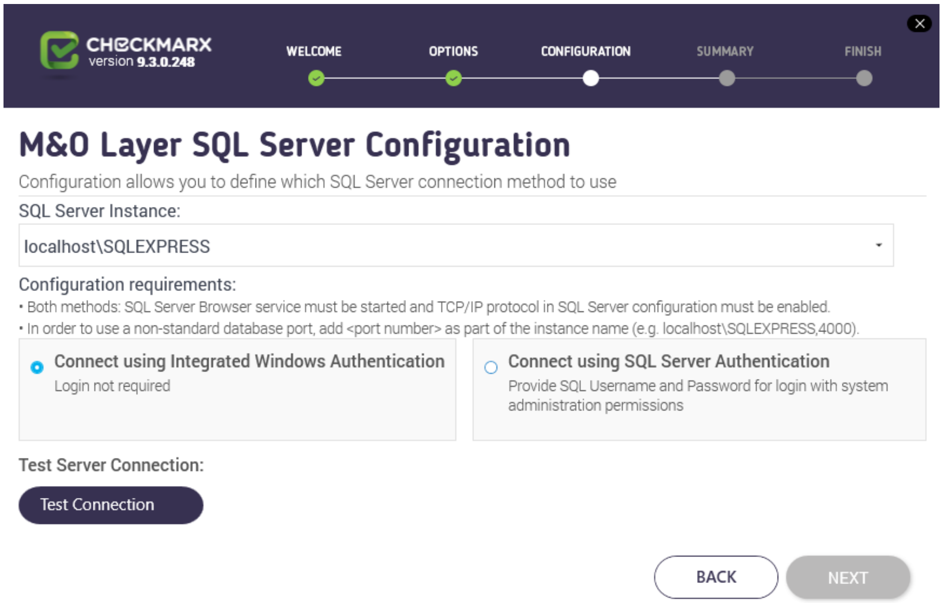
HTTPS Port: 8443

Next button is enabled when all ports are available

- Default ports (as displayed) are:
  - HTTP port is 8080
  - HTTPS port is 8443
- <NEXT> is enabled, if 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.

13. 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.



M&O Layer SQL Server Configuration

Configuration allows you to define which SQL Server connection method to use

SQL Server Instance: localhost\SQLEXPRESS

Configuration requirements:

- Both methods: SQL Server Browser service must be started and TCP/IP protocol in SQL Server configuration must be enabled.
- In order to use a non-standard database port, add <port number> as part of the instance name (e.g. localhost\SQLEXPRESS,4000).

● Connect using Integrated Windows Authentication
Login not required

○ Connect using SQL Server Authentication
Provide SQL Username and Password for login with system administration permissions

Test Server Connection:

14. 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.

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

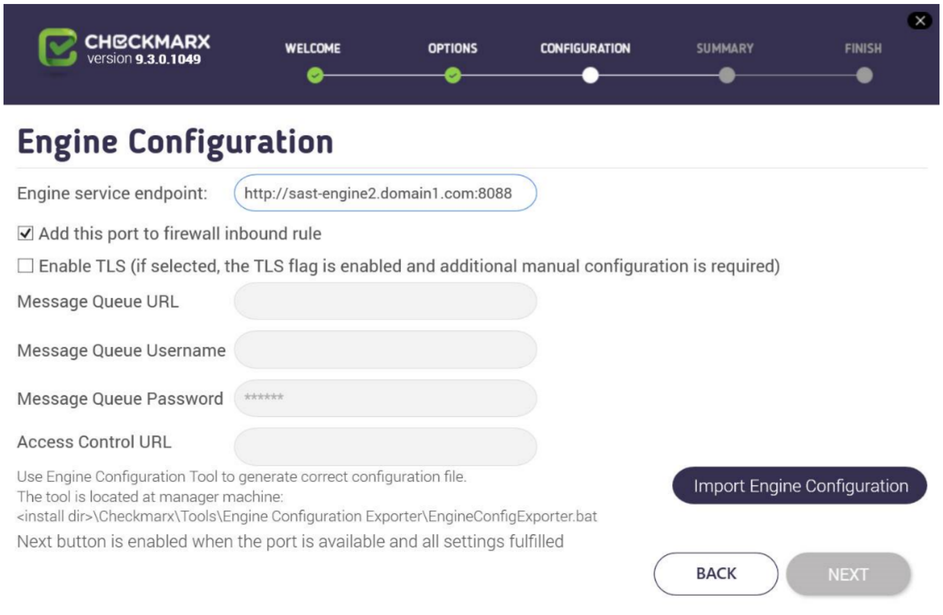
- **Connect using Integrated Windows Authentication** (login not required)
- **Connect using SQL Server Authentication** (provide SQL user name and password for login with SA permissions)

> - 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.

16. 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 an existing database has been detected, follow the onscreen instructions to either continue with that database or install a new one.
> - If the database belongs to a previous version of CxSAST, you have to remove it and install a new one, otherwise CxSAST does not operate. If you uninstall CxSAST, the database is not removed automatically.
> - 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 it is not part of a Windows domain, either join the station to one and restart it, or connect using SQL Server Authentication.
>   - The SQL Server Browser Windows service is running. If it is not running, enable and start it.

17. On the message, click <**OK**>, and then click <**NEXT**>. The **Engine Configuration** window is displayed.



Engine Configuration

Engine service endpoint: http://sast-engine2.domain1.com:8088

☑ Add this port to firewall inbound rule

□ Enable TLS (if selected, the TLS flag is enabled and additional manual configuration is required)

Message Queue URL

Message Queue Username

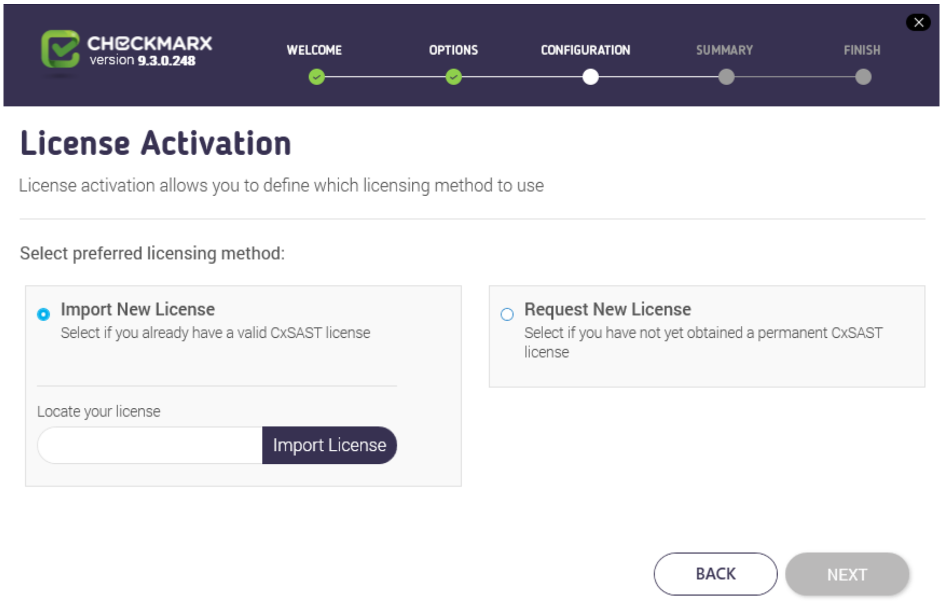
Message Queue Password ******

Access Control URL

Use Engine Configuration Tool to generate correct configuration file.
The tool is located at manager machine:
<install dir>\Checkmarx\Tools\Engine Configuration Exporter\EngineConfigExporter.bat

Next button is enabled when the port is available and all settings fulfilled

18. If **Enable TLS** is checked, TLS flag is enabled and additional manual configuration is required.
19. Click <**NEXT**>. The **License Activation** window is displayed.



License Activation

License activation allows you to define which licensing method to use

Select preferred licensing method:

● Import New License
Select if you already have a valid CxSAST license

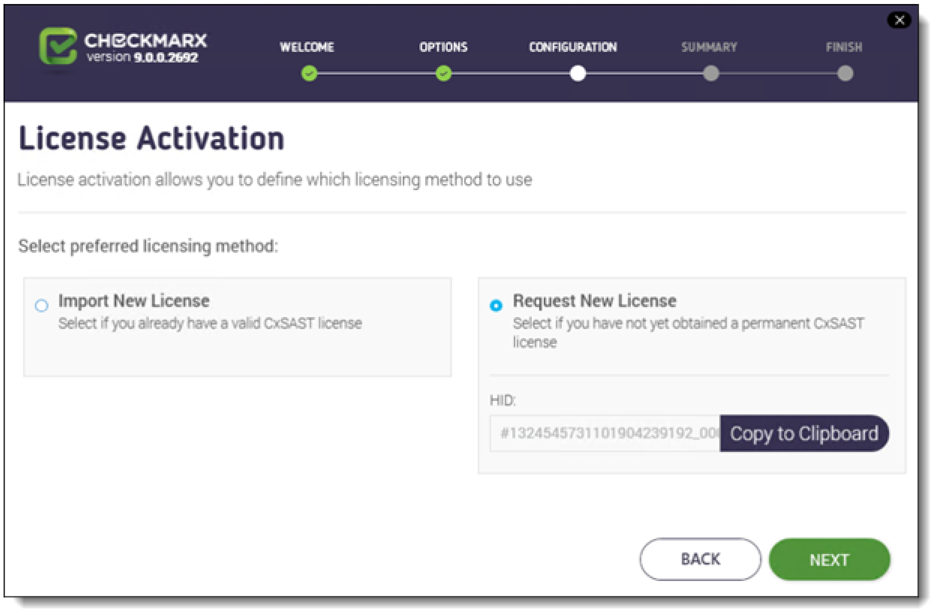
Locate your license

○ Request New License
Select if you have not yet obtained a permanent CxSAST license

- If you already have a valid license from your previous installation, the license information is automatically loaded from the existing configuration and the License Activation window is not displayed.
- If the License Activation window appears while installing or upgrading, you have to provide an updated license file. Any existing license file from a previous installation will be rendered invalid.

20. 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



License Activation

License activation allows you to define which licensing method to use

Select preferred licensing method:

○ Import New License
Select if you already have a valid CxSAST license

● Request New License
Select if you have not yet obtained a permanent CxSAST license

HID: #132454573110190423919 2_00

- To update the license at a later stage with an updated license file, use the License Importer utility as explained.

21. Click <**NEXT**> to continue.

- If your license does not match your current Hardware ID (HID), a warning message is displayed. In this case, obtain the proper license from your Checkmarx sales representative and use the License Importer utility to import it as explained once you received it.

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

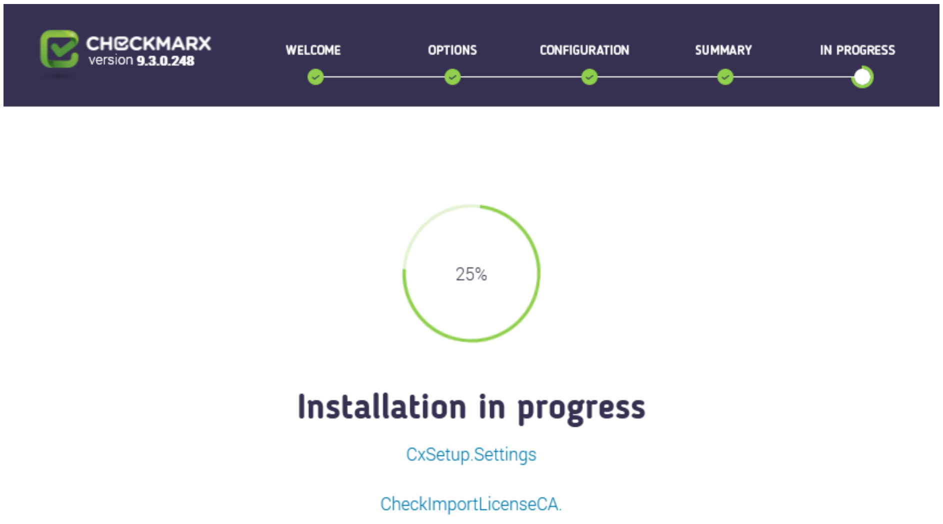
- Default website does exist (occupies a different port) and port 80 is occupied by another application or website.

- If port **80** is occupied, the **Validate Port** window is displayed. In this case, select another port and click <**Validate Port**>.

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

- If your license remains valid after upgrading according to your license agreement with Checkmarx or you upgrade your CxSAST version with a newer build of the same version, the license information is not displayed because it has already been loaded from the existing configuration.

23. Click <**INSTALL**> to continue. The **Installation in Progress** window is displayed and the application is installed and configured.
    - To return to the previous window, click <**BACK**>.
    - To exit, click <**X**>.

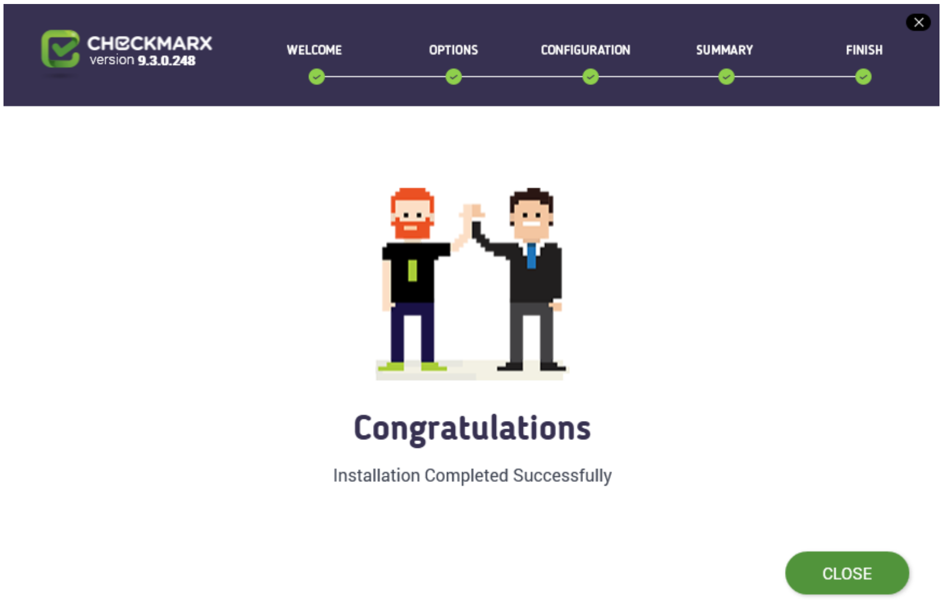


Installation in progress

CxSetup.Settings

CheckImportLicenseCA.

- Once the installation is complete the **Installation Completed Successfully** window is displayed.
- If the installation fails, the "**Setup failed**" message is displayed. For more information, refer to the installation logs. If you need further assistance, please [open a support ticket]



- If you install CxSAST with Management and Orchestration, the Congratulations window appears with the **Start Database Synchronization** checkbox and the installation must be completed with synchronizing the database.

Completing the CxSAST Installation with Management and Orchestration

If you install CxSAST with Management and Orchestration, the database must synchronize. You may start the synchronization process immediately after installing CxSAST or synchronize at a later stage. In this case, the Congratulations window appears with the **Start Database Synchronization** checkbox selected by default.

➢ **To start synchronizing the database immediately:**

- Leave the checkbox selected and click <**CLOSE**>. Restart the server, if you are asked to do so. The database synchronization process starts.
- For additional information and instructions about installing Management and Orchestration, refer to Installing Management and Orchestration.

➢ **To synchronize the database at a later stage:**

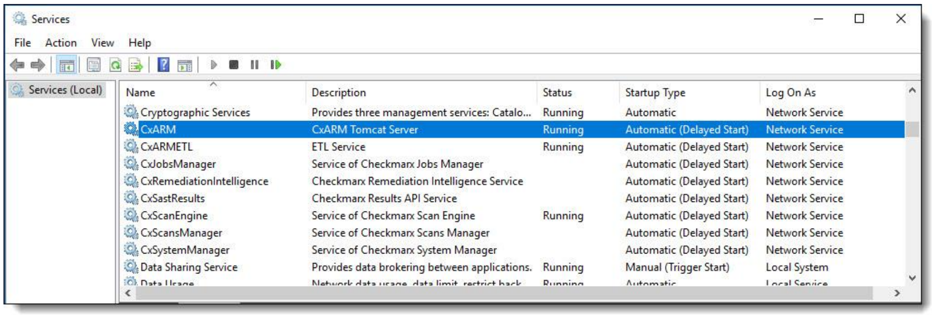
- Clear the checkbox and click <**CLOSE**>.
- When desired, close all Checkmarx applications and use the ETL tool to perform the synchronization. The ETL_tool is located at **<Installation folder>\Checkmarx\Checkmarx Risk Management\ETL\etl_executor.exe**, for example **C:\Program Files\Checkmarx\Checkmarx Risk Management\ETL\etl_executor.exe**

- The synchronization may take a long time, depending on the amount of data being synchronized. During that time, you cannot access the web portal.
- If attempting to install CxSAST with an existing Management and Orchestration database, the subsequent ETL DB sync fails due to a limitation in Management and Orchestration. Therefore, when reinstalling CxSAST, either delete the existing Management and Orchestration database before reinstalling or reinstall CxSAST with a new Management and Orchestration database.

Checking Installed Services

➢ **To check the status of installed services and if they have been installed:**

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



Name	Description	Status	Startup Type	Log On As
Cryptographic Services	Provides three management services: Catalo...	Running	Automatic	Network Service
CxARM	CxARM Tomcat Server	Running	Automatic (Delayed Start)	Network Service
CxARMETL	ETL Service	Running	Automatic (Delayed Start)	Network Service
CxJobsManager	Service of Checkmarx Jobs Manager		Automatic (Delayed Start)	Network Service
CxRemediationIntelligence	Checkmarx Remediation Intelligence Service		Automatic (Delayed Start)	Network Service
CxSastResults	Checkmarx Results API Service		Automatic (Delayed Start)	Network Service
CxScanEngine	Service of Checkmarx Scan Engine	Running	Automatic (Delayed Start)	Network Service
CxScansManager	Service of Checkmarx Scans Manager		Automatic (Delayed Start)	Network Service
CxSystemManager	Service of Checkmarx System Manager		Automatic (Delayed Start)	Network Service
Data Sharing Service	Provides data brokering between applications.	Running	Manual (Trigger Start)	Local System
Data Usage	Network data usage, data limit, restrict back	Running	Automatic	Local Service

2. 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):

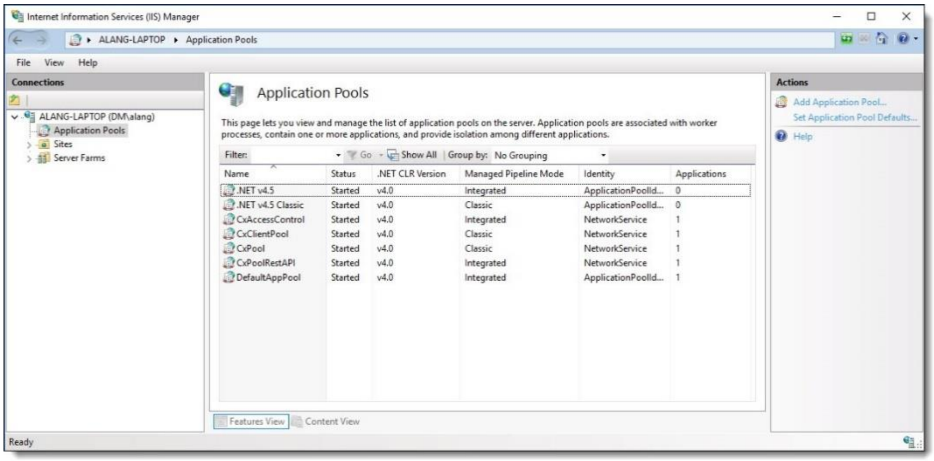
- CxScanEngine

> - 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.

Checking the Installed Application Pools

➢ **To check the status of the application pools and if they are installed:**

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



This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

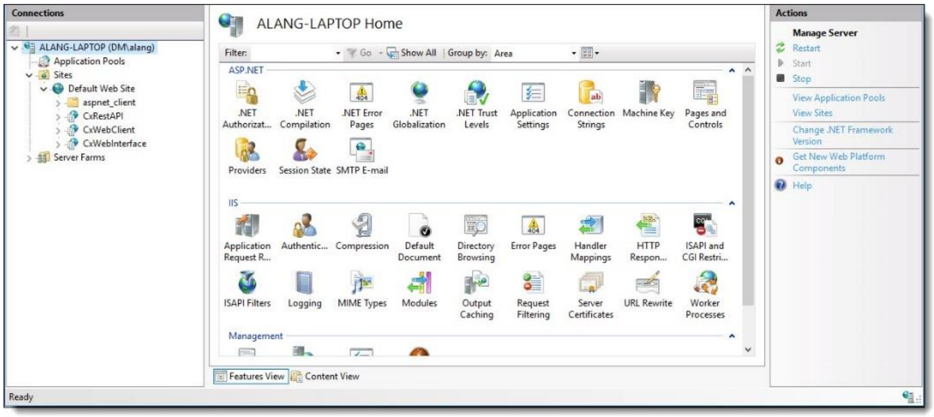
Name	Status	.NET CLR Version	Managed Pipeline Mode	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
CxAccessControl	Started	v4.0	Integrated	NetworkService	1
CxClientPool	Started	v4.0	Classic	NetworkService	1
CxPool	Started	v4.0	Classic	NetworkService	1
CxPoolRestAPI	Started	v4.0	Integrated	NetworkService	1
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	1

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.



Enabling 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 must 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 Servces\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:

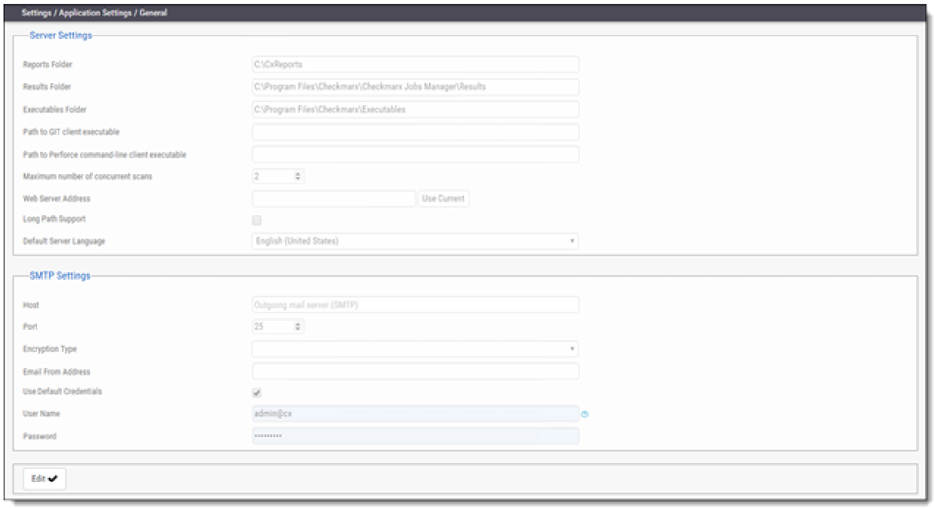
- **Access CxSASTlocally (from the server host):** Use the **Checkmarx Portal** shortcut on the Desktop or navigate to the Checkmarx folder (**Start > All Programs > Checkmarx > Checkmarx Portal**).
- **Access CxSAST from any other computer:** Make sure that organizational routing and firewall configuration 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 the 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 have 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

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



Settings / Application Settings / General

Server Settings

Reports Folder	C:\CxReports
Results Folder	C:\Program Files\Checkmarx\Checkmarx Jobs Manager\Results
Executables Folder	C:\Program Files\Checkmarx\Executables
Path to GIT client executable	
Path to Perforce command-line client executable	
Maximum number of concurrent scans	2
Web Server Address	Use Current
Long Path Support	□
Default Server Language	English (United States)

SMTP Settings

Host	Outgoing mail server (SMTP)
Port	25
Encryption Type	
Email From Address	
Use Default Credentials	☑
User Name	admin@cx
Password	••••••••••

4. 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. In order for the long path support to be fully enabled 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.

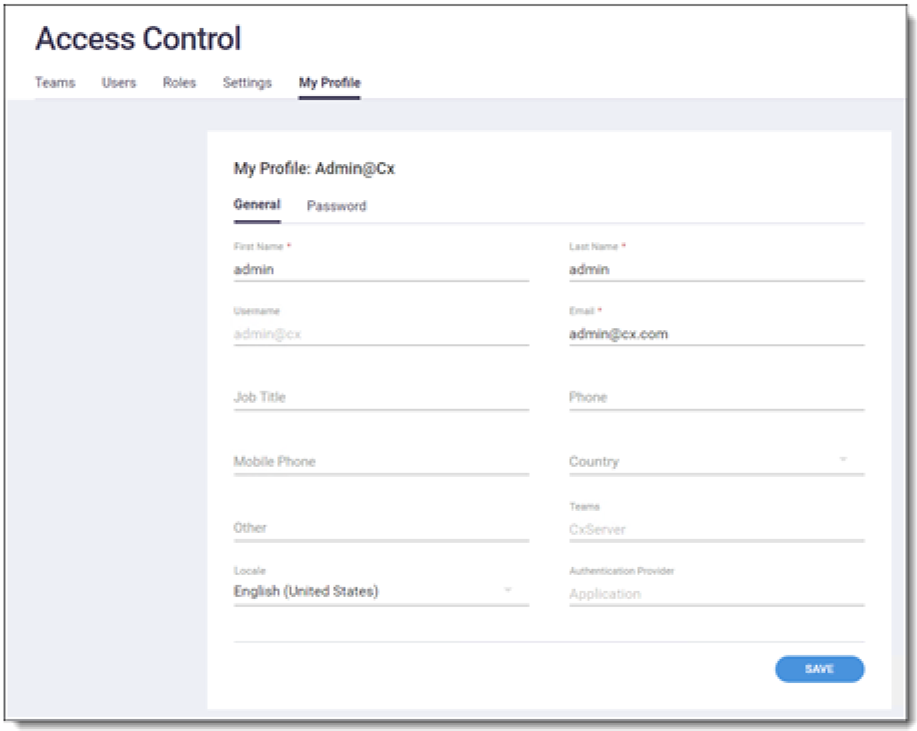
2. Click **Update** to save the changes.

SMTP Settings

1. Provide the relevant **SMTP** settings. Other settings should usually be left as they are.
2. Optionally, you can configure the "From" field of emails. If you don't configure it, it is left empty.
3. Click **Update** to save changes.

My Profile Settings

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



Access Control

My Profile: Admin@Cx

First Name * admin

Last Name * admin

Username admin@cx

Email * admin@cx.com

Job Title

Phone

Mobile Phone

Country

Other

Teams CxServer

Locale English (United States)

Authentication Provider Application

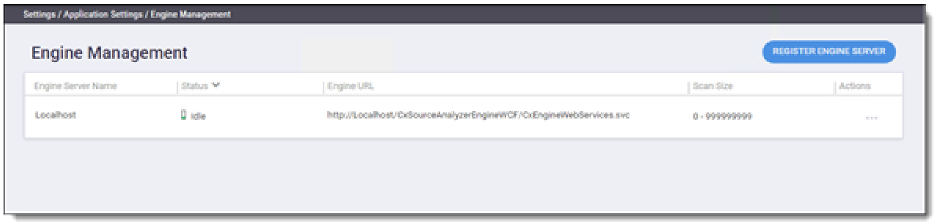
Email Verification

- Verify that the email address in the CxSAST profile settings is of a valid format, i.e. **John.Smith@example.com**, and not **John.Smith@example**. This 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.

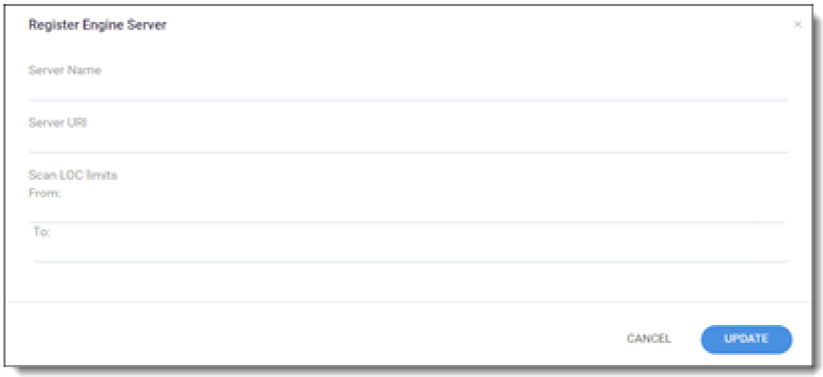
Engine Settings (in a distributed architecture)

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



Engine Server Name	Status	Engine URL	Scan Size	Actions
Localhost	Idle	http://Localhost/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc	0 - 999999999	...

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**, so that CxManager is able to communicate with CxEngine.

   The URL should be as follows:
   http://<Server_Name>:{port}
   where **<Server_Name>** is the CxEngine host's IP address or resolvable name. The default port is 8088.

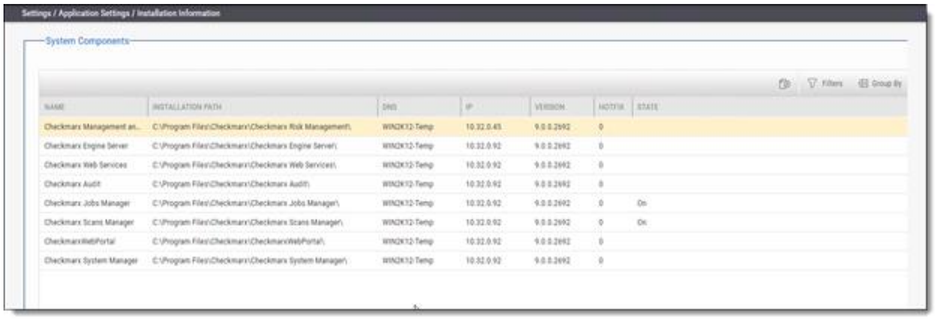
   Optionally you can define Scan LOC Limits (maximum lines of code allowed).
4. If you have multiple CxEngine Servers, repeat this procedure for each Engine Server.

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

5. Click <**UPDATE**>.

Installation Verification

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



Settings / Application Settings / Installation Information

System Components

NAME	INSTALLATION PATH	DNS	IP	VERSION	HOTFIX	STATE
Checkmarx Management an...	C:\Program Files\Checkmarx\Checkmarx Risk Management\	WIN2K12-Temp	10.32.0.45	9.0.0.2692	0	
Checkmarx Engine Server	C:\Program Files\Checkmarx\Checkmarx Engine Server\	WIN2K12-Temp	10.32.0.92	9.0.0.2692	0	
Checkmarx Web Services	C:\Program Files\Checkmarx\Checkmarx Web Services\	WIN2K12-Temp	10.32.0.92	9.0.0.2692	0	
Checkmarx Audit	C:\Program Files\Checkmarx\Checkmarx Audit\	WIN2K12-Temp	10.32.0.92	9.0.0.2692	0	
Checkmarx Jobs Manager	C:\Program Files\Checkmarx\Checkmarx Jobs Manager\	WIN2K12-Temp	10.32.0.92	9.0.0.2692	0	On
Checkmarx Scans Manager	C:\Program Files\Checkmarx\Checkmarx Scans Manager\	WIN2K12-Temp	10.32.0.92	9.0.0.2692	0	On
CheckmarxWebPortal	C:\Program Files\Checkmarx\CheckmarxWebPortal\	WIN2K12-Temp	10.32.0.92	9.0.0.2692	0	
Checkmarx System Manager	C:\Program Files\Checkmarx\Checkmarx System Manager\	WIN2K12-Temp	10.32.0.92	9.0.0.2692	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 a Distributed Environment

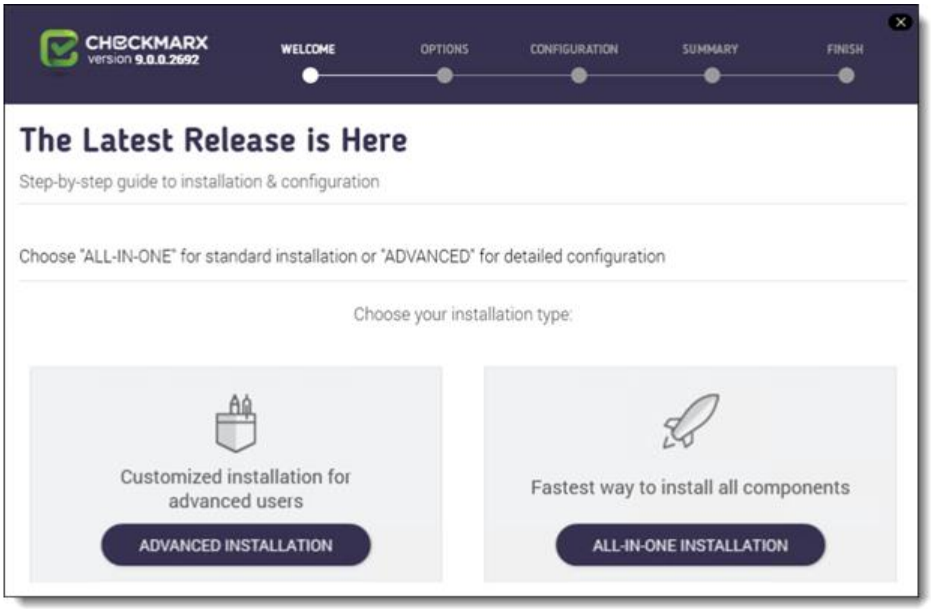
A distributed architecture refers to a scenario where the server components are 'distributed' over multiple dedicated servers as explained in System Architecture Overview. To install the CxSAST Server in a distributed environment (on different dedicated hosts), you have to install each CxSAST Server component specified below on the respective host in the outlined order.

- The installation or upgrade of each component must be performed from the same setup file (**CxSetup.exe**) as all components must be of the same version and build.

Workflow

➢ **To start installing a component of CxSAST:**

1. Verify that you downloaded the CxSAST installation package and that the third-party components have been made available as explained under Preparing CxSAST for Installation.
2. Run **CxSetup.exe.** The **Checkmarx Welcome** window is displayed.



The Latest Release is Here

Step-by-step guide to installation & configuration

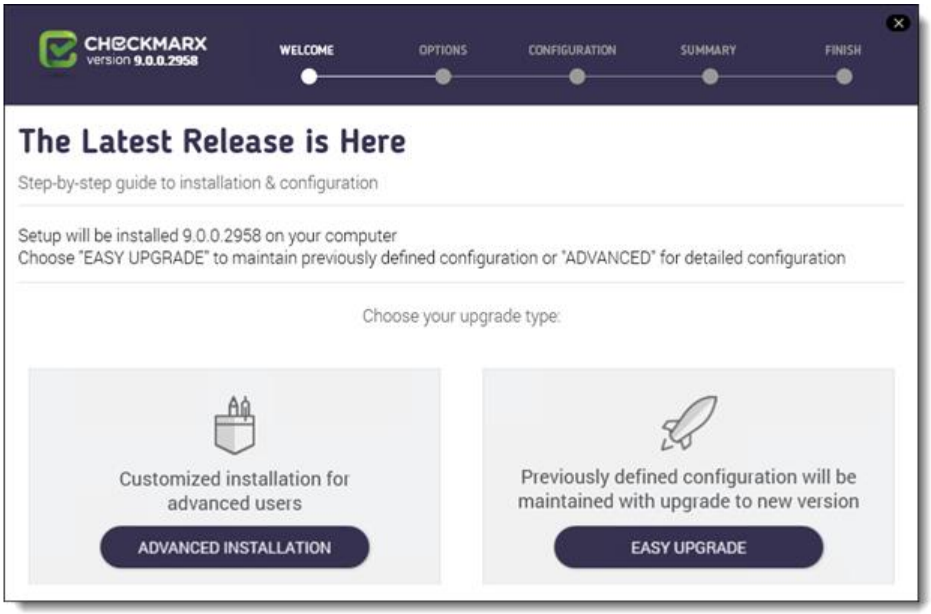
Choose "ALL-IN-ONE" for standard installation or "ADVANCED" for detailed configuration

Choose your installation type:

Customized installation for advanced users

Fastest way to install all components

3. Click <**ADVANCED INSTALLATION**> to continue, or **X** to exit.
   For upgrades, use <**ADVANCED INSTALLATION**> as well and select the required setup options to continue as explained below.



The Latest Release is Here

Step-by-step guide to installation & configuration

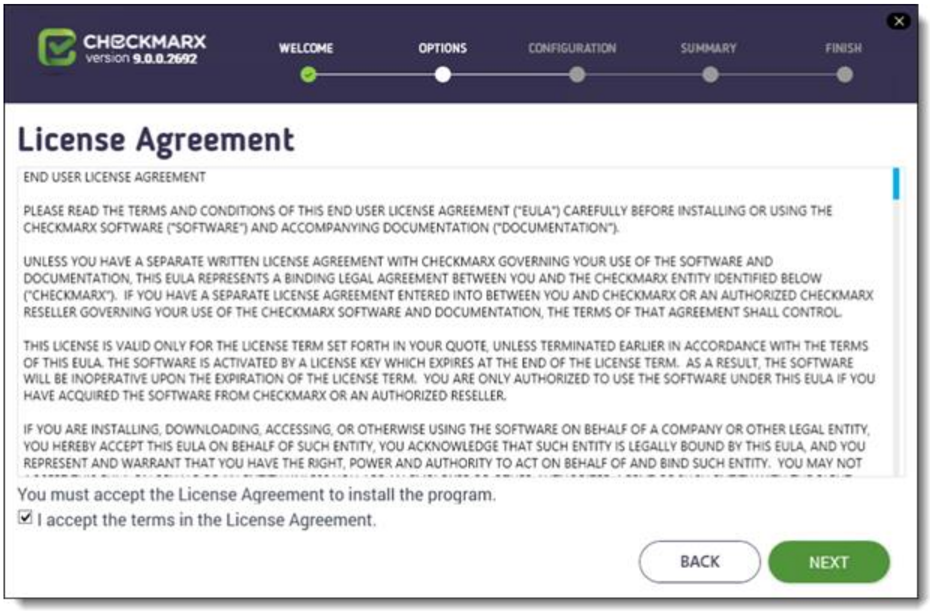
Setup will be installed 9.0.0.2958 on your computer
Choose "EASY UPGRADE" to maintain previously defined configuration or "ADVANCED" for detailed configuration

Choose your upgrade type:

Customized installation for advanced users

Previously defined configuration will be maintained with upgrade to new version

4. For both scenarios, the **Checkmarx License Agreement** window is displayed.



License Agreement

END USER LICENSE AGREEMENT

PLEASE READ THE TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE INSTALLING OR USING THE CHECKMARX SOFTWARE ("SOFTWARE") AND ACCOMPANYING DOCUMENTATION ("DOCUMENTATION").

UNLESS YOU HAVE A SEPARATE WRITTEN LICENSE AGREEMENT WITH CHECKMARX GOVERNING YOUR USE OF THE SOFTWARE AND DOCUMENTATION, THIS EULA REPRESENTS A BINDING LEGAL AGREEMENT BETWEEN YOU AND THE CHECKMARX ENTITY IDENTIFIED BELOW ("CHECKMARX"). IF YOU HAVE A SEPARATE LICENSE AGREEMENT ENTERED INTO BETWEEN YOU AND CHECKMARX OR AN AUTHORIZED CHECKMARX RESELLER GOVERNING YOUR USE OF THE CHECKMARX SOFTWARE AND DOCUMENTATION, THE TERMS OF THAT AGREEMENT SHALL CONTROL.

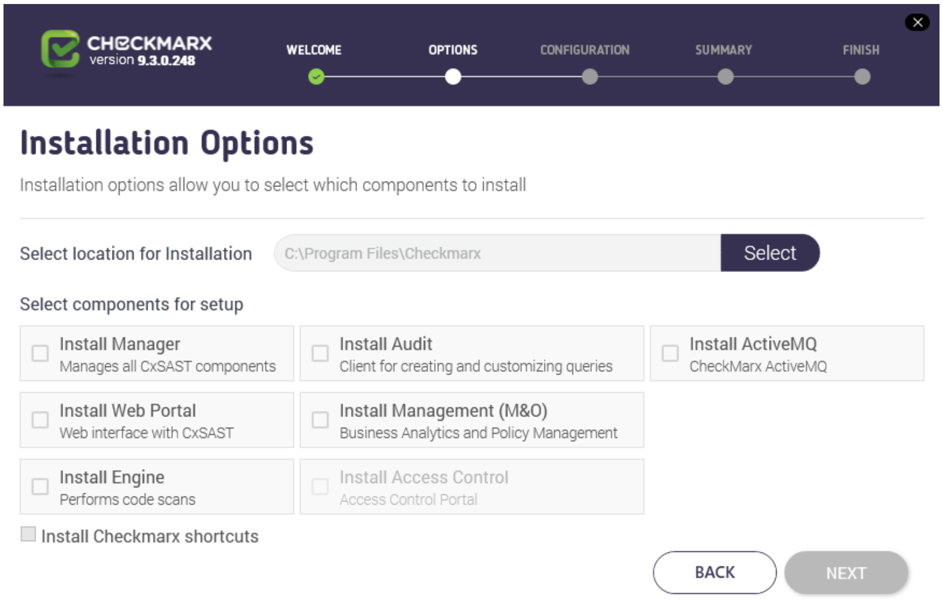
THIS LICENSE IS VALID ONLY FOR THE LICENSE TERM SET FORTH IN YOUR QUOTE, UNLESS TERMINATED EARLIER IN ACCORDANCE WITH THE TERMS OF THIS EULA. THE SOFTWARE IS ACTIVATED BY A LICENSE KEY WHICH EXPIRES AT THE END OF THE LICENSE TERM. AS A RESULT, THE SOFTWARE WILL BE INOPERATIVE UPON THE EXPIRATION OF THE LICENSE TERM. YOU ARE ONLY AUTHORIZED TO USE THE SOFTWARE UNDER THIS EULA IF YOU HAVE ACQUIRED THE SOFTWARE FROM CHECKMARX OR AN AUTHORIZED RESELLER.

IF YOU ARE INSTALLING, DOWNLOADING, ACCESSING, OR OTHERWISE USING THE SOFTWARE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU HEREBY ACCEPT THIS EULA ON BEHALF OF SUCH ENTITY, YOU ACKNOWLEDGE THAT SUCH ENTITY IS LEGALLY BOUND BY THIS EULA, AND YOU REPRESENT AND WARRANT THAT YOU HAVE THE RIGHT, POWER AND AUTHORITY TO ACT ON BEHALF OF AND BIND SUCH ENTITY. YOU MAY NOT

You must accept the License Agreement to install the program.

☑ I accept the terms in the License Agreement.

5. Review and accept the license agreement by checking **I accept the terms in the License Agreement.**
6. Click <**NEXT**> to continue. The **Installation Options** window is displayed.



Installation Options

Installation options allow you to select which components to install

Select location for Installation C:\Program Files\Checkmarx

Select components for setup

☐ Install Manager — Manages all CxSAST components
☐ Install Audit — Client for creating and customizing queries
☐ Install ActiveMQ — CheckMarx ActiveMQ
☐ Install Web Portal — Web interface with CxSAST
☐ Install Management (M&O) — Business Analytics and Policy Management
☐ Install Engine — Performs code scans
☐ Install Access Control — Access Control Portal

☐ Install Checkmarx shortcuts

- For new installations, click <**Select**> to define the CxSAST installation location.
- 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 feature. For further information, refer to Modifying CxSAST.

- To avoid permission restrictions, install CxSAST in **<root directory>:\Program Files** .

7. Check the required component(s), for example **Install CxManager**, on the respective host where you start installing.

➢ **To continue installing the respective components on the respective dedicated hosts:**

1. Install the components in the order outlined below.
2. Follow the links for further information and instructions on installing each component.

   a) **Installing CxManager**. CxManager manages and integrates system components and contributes the JSON file with the engine settings that you need at a later stage.
   b) **Installing and Configuring ActiveMQ**. The ActiveMQ manages the messaging queues and contributes the Message Queue parameters that are going to be loaded together with the engine configuration.
   c) **Installing and Configuring the Web Portal**. The Web Portal is required to access and interact with CxSAST through the web.
   d) **Installing CxEngine**. The CxEngine performs the code scans.

- When you install the **CxEngine**, you import the engine configuration settings stored in a JSON file that you retrieve from **CxManager**.
- If **CxManager** and **ActiveMQ** are not available to the **CxEngine** installation, the installation cannot be completed.
- When installing in Silent Mode, you have to use Silent Reconfigure option to complete the installation. For further information, refer to Silent Installation.

Required Prerequisites for Installing CxSAST in a Distributed Environment

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 **CxSAST.exe** to every relevant host and install the required third-party components for the CxSAST component to be installed on the respective host. For information and instructions on preparing for installing CxSAST and making the required prerequisites available, refer to Preparing CxSAST for Installation.

This document outlines, which prerequisites are required for which component.

Prerequisite	**Required for…**			
C++ Redist 2010 and 2015 SP3	CxManager		Web Portal	CxEngine

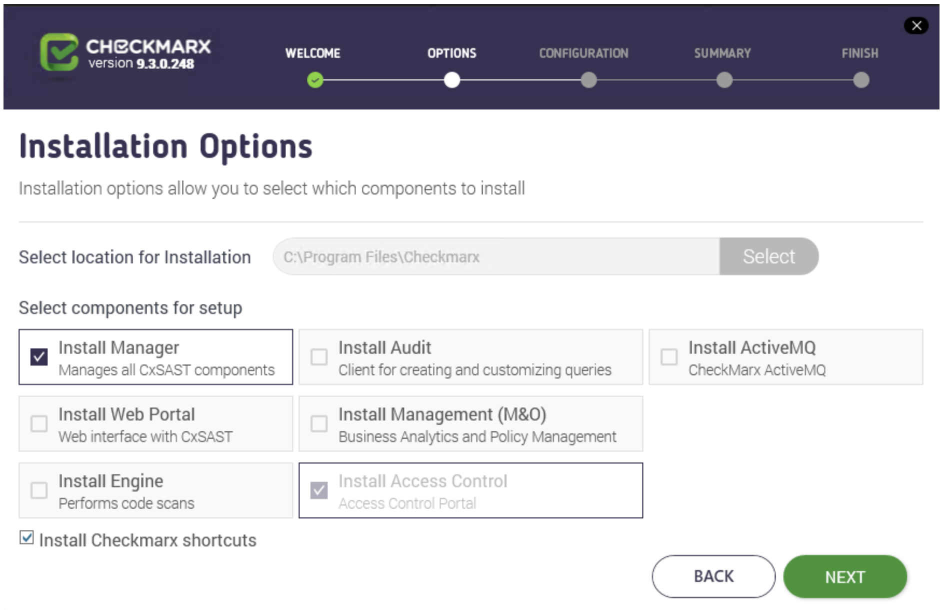
Prerequisite	Required for…			
IIS v7.0 or higher	CxManager		Web Portal	
ASP.NET Core 2.1.16 (or higher 2.1.x versions) Runtime & Hosting	CxManager			CxEngine
MS SQL	CxManager	ActiveMQ		
Java JRE 1.8.0 (64-bit)	CxManager	ActiveMQ		

Installing the CxManager

The first component to install in this sequence is the CxManager.

➢ **To install CxManager:**

1. Select **Install Manager** only.



Installation Options

Installation options allow you to select which components to install

Select location for Installation: C:\Program Files\Checkmarx

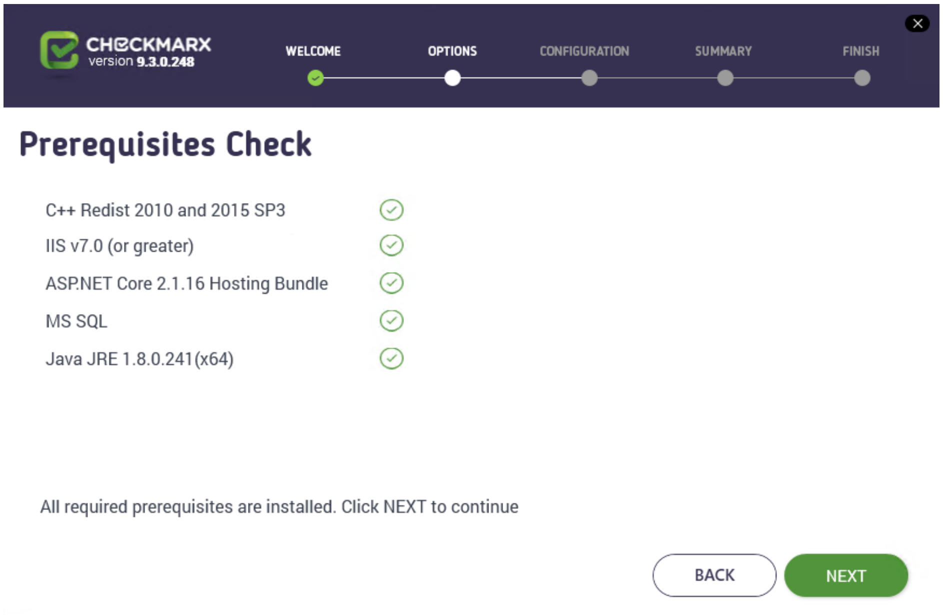
Select components for setup

- ☑ Install Manager – Manages all CxSAST components
- □ Install Audit – Client for creating and customizing queries
- □ Install ActiveMQ – CheckMarx ActiveMQ
- □ Install Web Portal – Web interface with CxSAST
- □ Install Management (M&O) – Business Analytics and Policy Management
- □ Install Engine – Performs code scans
- ☑ Install Access Control – Access Control Portal

☑ Install Checkmarx shortcuts

- **Access Control** is selected by default as it installs together with **CxManager**.

2. Click **Next** to continue. The **Prerequisites Check** window is displayed, showing the status of the required components to install CxManager. For additional information and instructions on installing and preparing required software, refer to Preparing to Install CxSAST.



Prerequisites Check

C++ Redist 2010 and 2015 SP3	✓
IIS v7.0 (or greater)	✓
ASP.NET Core 2.1.16 Hosting Bundle	✓
MS SQL	✓
Java JRE 1.8.0.241(x64)	✓

All required prerequisites are installed. Click NEXT to continue

3. Once all components are indicated to be available ✓ , click **<NEXT>**. The **CxSAST SQL Server Configuration** window is displayed.
4. 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).

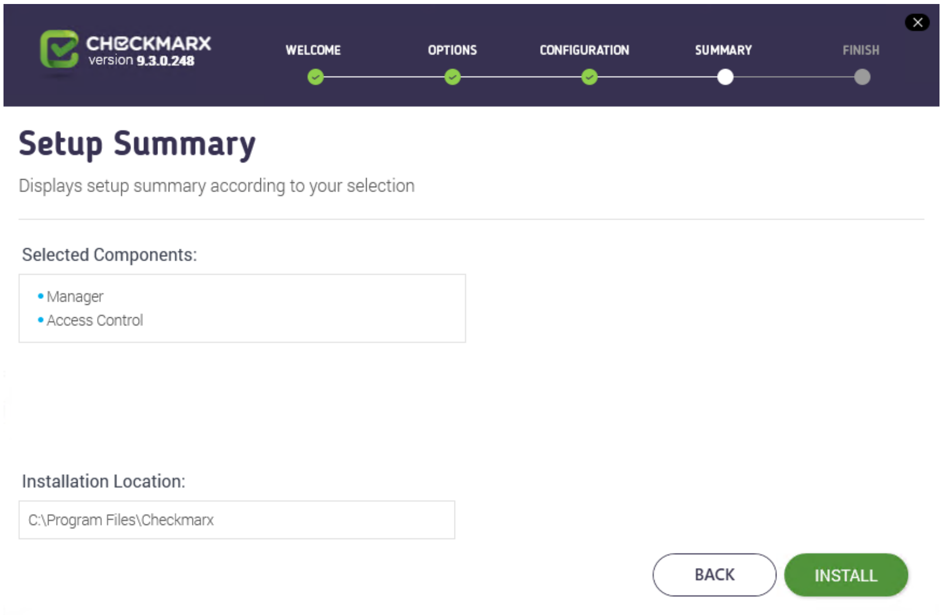
- For upgrades, previously defined SQL Server instance settings are loaded from the existing configuration and cannot be changed.

5. 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).
6. Click **Test Connection.**
    - If the database was not in use, a message appears that indicates that the connection was successful.
    - If a previously used database exists, A message appears that a database was detected. In this case, you may continue using the database or re-install it as explained in the message.

- 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).

Once the SQL connection has been successfully tested, the Setup summary appears.



Setup Summary

Displays setup summary according to your selection

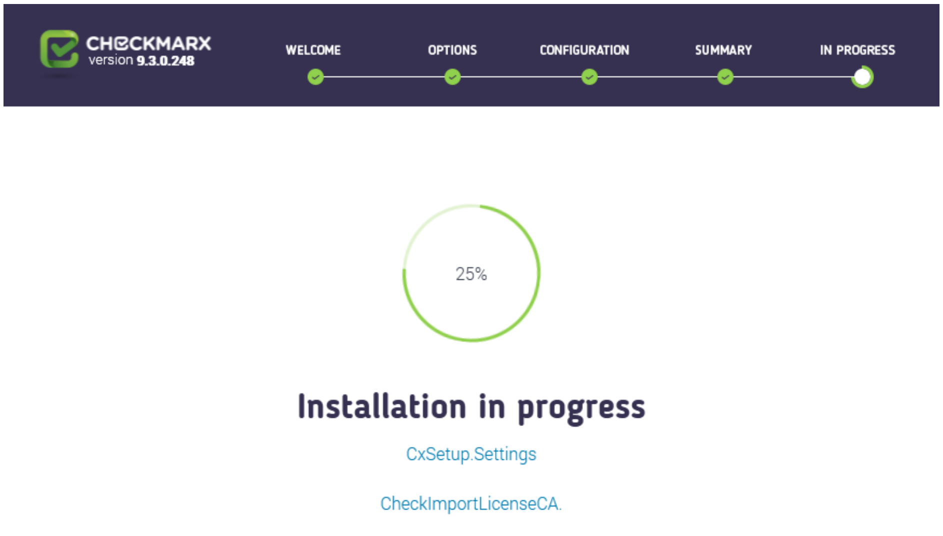
Selected Components:

- Manager
- Access Control

Installation Location:

C:\Program Files\Checkmarx

7. Check the setup summary according to your selection.
8. Click <**INSTALL**> to continue. The **Installation in Progress** window is displayed and the installation proceeds, which may take a few minutes.
    - To return to the previous window, click <**BACK**>.
    - To exit, click <**X**>.

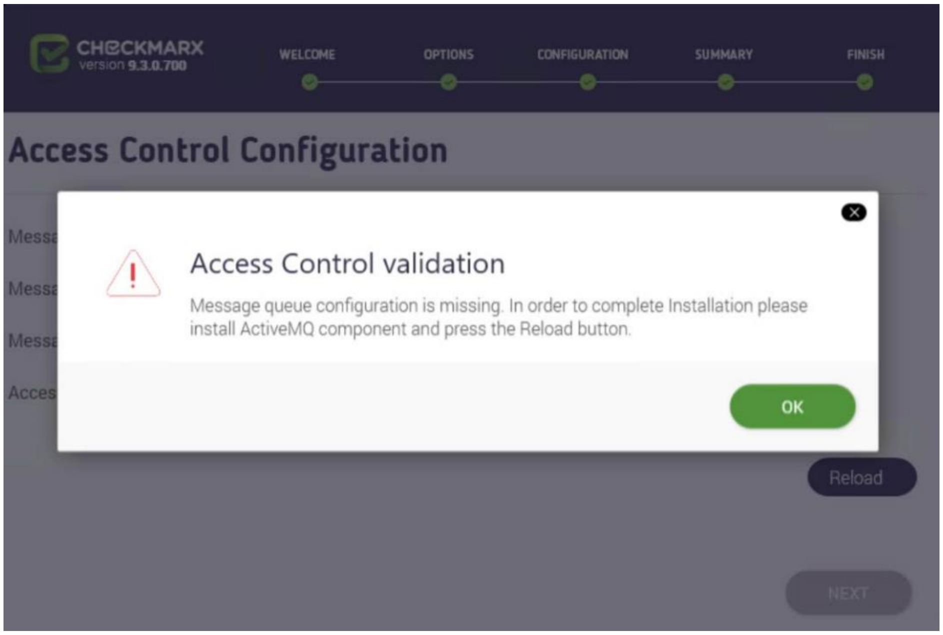


Installation in progress

CxSetup.Settings

CheckImportLicenseCA.

9. Once installed, you are notified that Access Control validation is not yet complete and that you must install **ActiveMQ**.



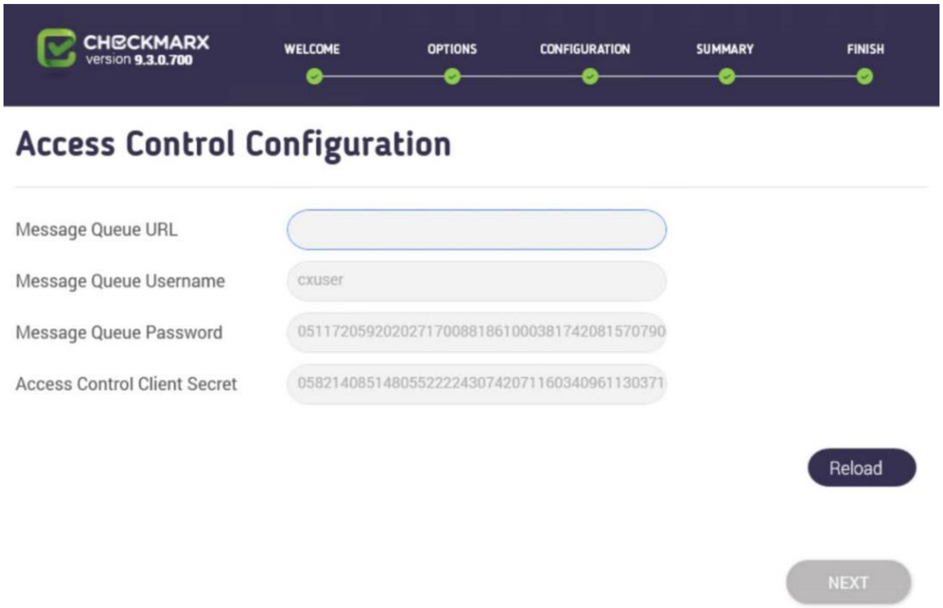
Access Control Configuration

Access Control validation

Message queue configuration is missing. In order to complete Installation please install ActiveMQ component and press the Reload button.

10. Click <**OK**> to acknowledge the Access Control Validation message. The Access Control Configuration window appears with the Message Queue URL field empty.

- The Message Queue URL becomes available once the ActiveMQ is installed and you reload the Access Control configuration.



Access Control Configuration

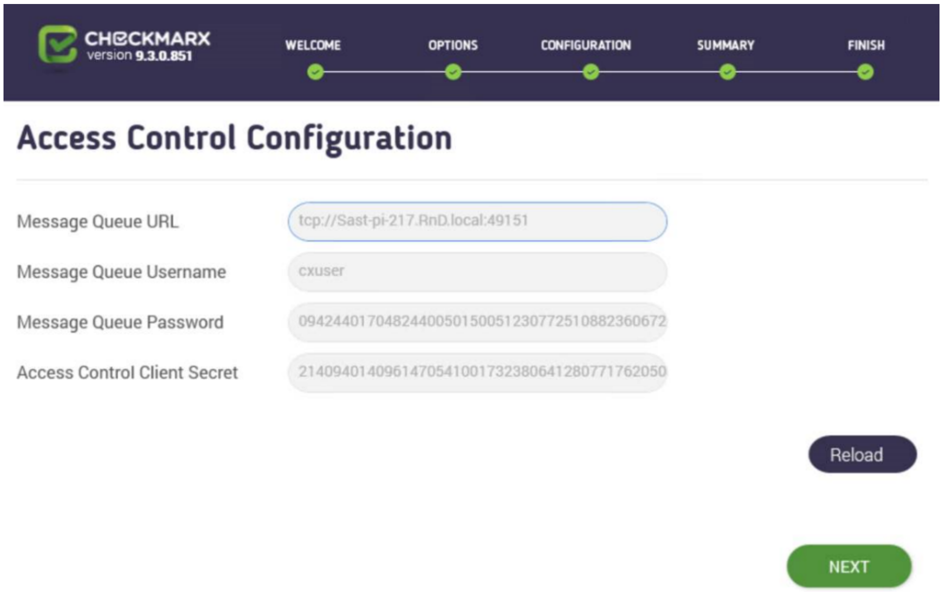
Message Queue URL

Message Queue Username: cxuser

Message Queue Password: 05117205920202717008818610003817420815707900

Access Control Client Secret: 0582140851480552222430742071160340961130371

11. Switch to the ActiveMQ station and install **ActiveMQ** there as explained.
12. Once the ActiveMQ installation has been successfully completed, return to the CxManager station and click <**Reload**>. The Message Queue URL field now displays the address of the ActiveMQ server.



Access Control Configuration

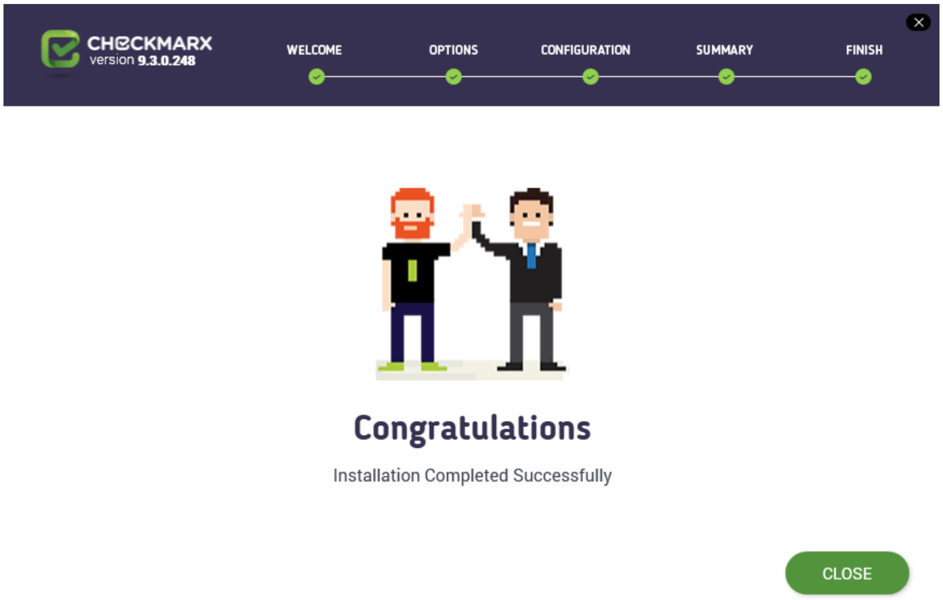
Message Queue URL: tcp://Sast-pi-217.RnD.local:49151

Message Queue Username: cxuser

Message Queue Password: 0942440170482440050150051230772510882360672

Access Control Client Secret: 2140940140961470541001732380641280771762050

13. Click <**Next**>. A message indicates that the installation has been completed successfully.



Congratulations

Installation Completed Successfully

14. Click <**CLOSE**> to complete the installation.

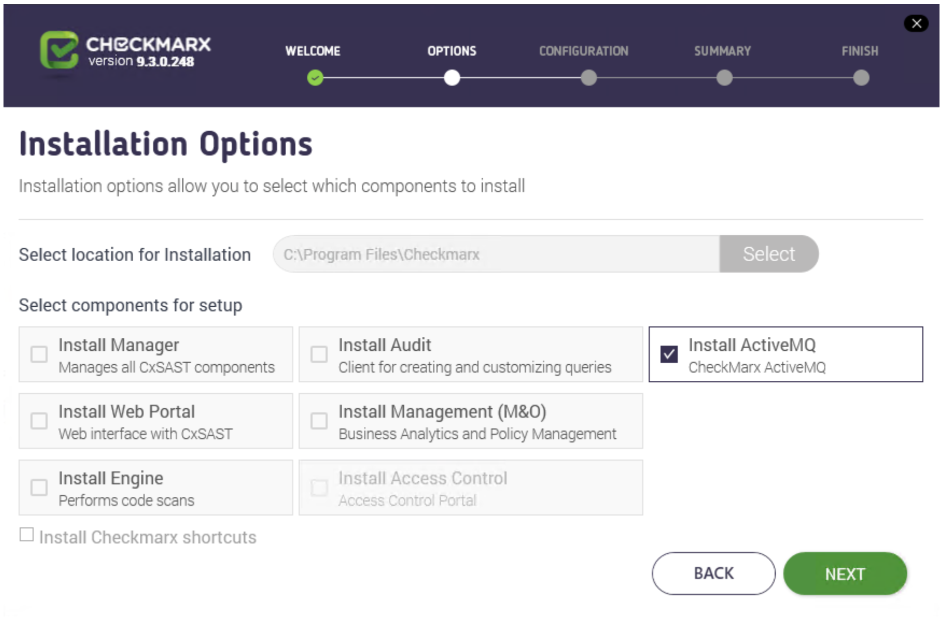
Installing the ActiveMQ

The second component to install in this sequence is the ActiveMQ.

- Installing ActiveMQ requires CxManager installed as explained.

➢ **To install ActiveMQ:**

1. Select **Install ActiveMQ** only.



Installation Options

Installation options allow you to select which components to install

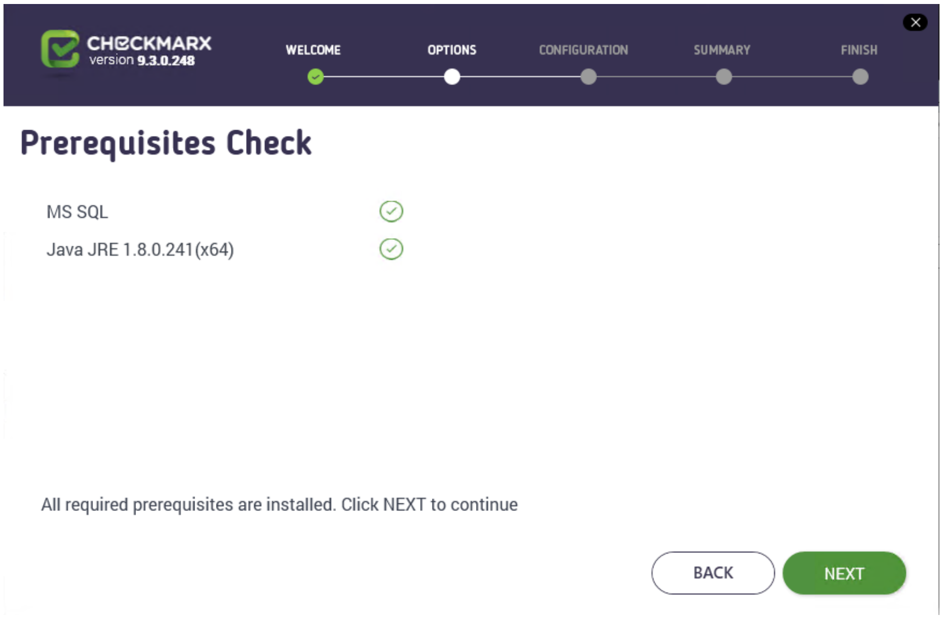
Select location for Installation: C:\Program Files\Checkmarx

Select components for setup

- □ Install Manager – Manages all CxSAST components
- □ Install Audit – Client for creating and customizing queries
- ☑ Install ActiveMQ – CheckMarx ActiveMQ
- □ Install Web Portal – Web interface with CxSAST
- □ Install Management (M&O) – Business Analytics and Policy Management
- □ Install Engine – Performs code scans
- □ Install Access Control – Access Control Portal

□ Install Checkmarx shortcuts

2. Click <NEXT> to continue. The **Prerequisites Check** window is displayed, showing the status of the required components to install ActiveMQ. For additional information and instructions on installing and preparing the required software, refer to Preparing to Install CxSAST.

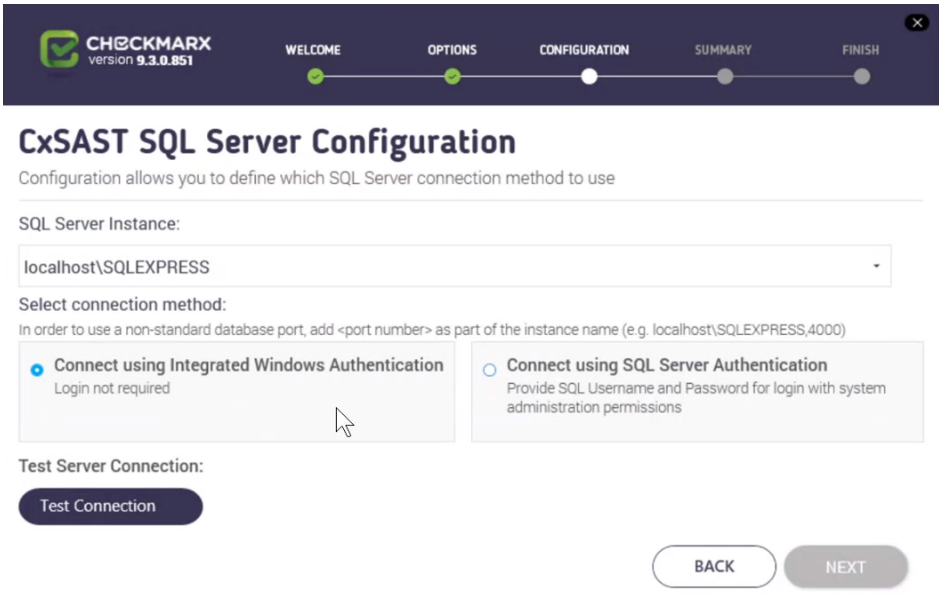


Prerequisites Check

MS SQL	✓
Java JRE 1.8.0.241(x64)	✓

All required prerequisites are installed. Click NEXT to continue

3. Once all components are indicated to be available ✓, click <NEXT>. The **CxSAST SQL Server Configuration** window is displayed with default settings.



CxSAST SQL Server Configuration

Configuration allows you to define which SQL Server connection method to use

SQL Server Instance: localhost\SQLEXPRESS

Select connection method:

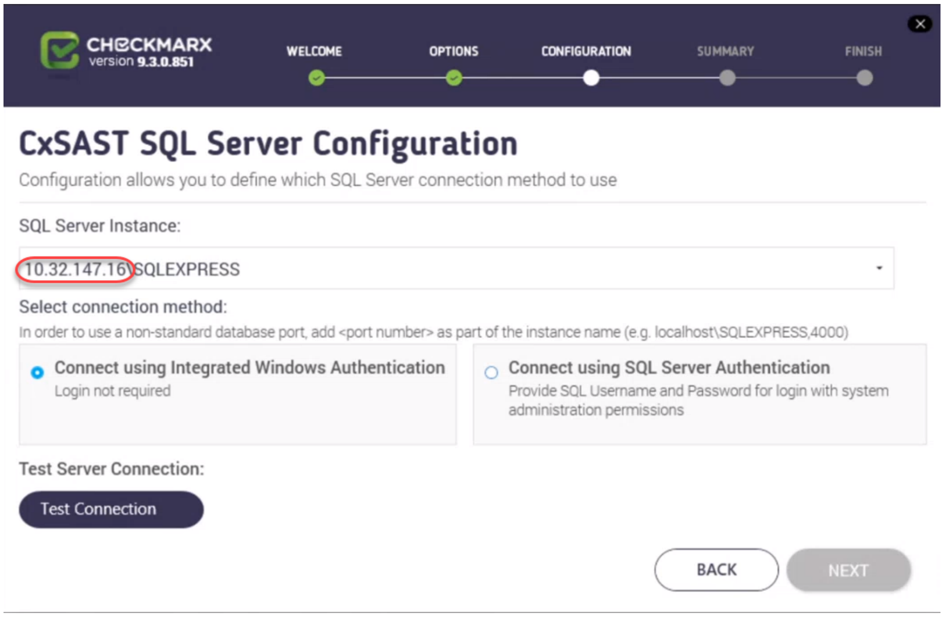
In order to use a non-standard database port, add <port number> as part of the instance name (e.g. localhost\SQLEXPRESS,4000)

● Connect using Integrated Windows Authentication
Login not required

○ Connect using SQL Server Authentication
Provide SQL Username and Password for login with system administration permissions

Test Server Connection:

4. Select the Server from the SQL Server Instance list.
5. Since you install the components on different stations, you have to replace **localhost** with the IP address or host name of the CxManager server or the relevant database server. In this example, the CxManager and the SQL server are installed on the station with the IP address **10.32.147.16** .



CxSAST SQL Server Configuration

Configuration allows you to define which SQL Server connection method to use

SQL Server Instance: 10.32.147.16\SQLEXPRESS

Select connection method:

In order to use a non-standard database port, add <port number> as part of the instance name (e.g. localhost\SQLEXPRESS,4000)

● Connect using Integrated Windows Authentication
Login not required

○ Connect using SQL Server Authentication
Provide SQL Username and Password for login with system administration permissions

Test Server Connection:

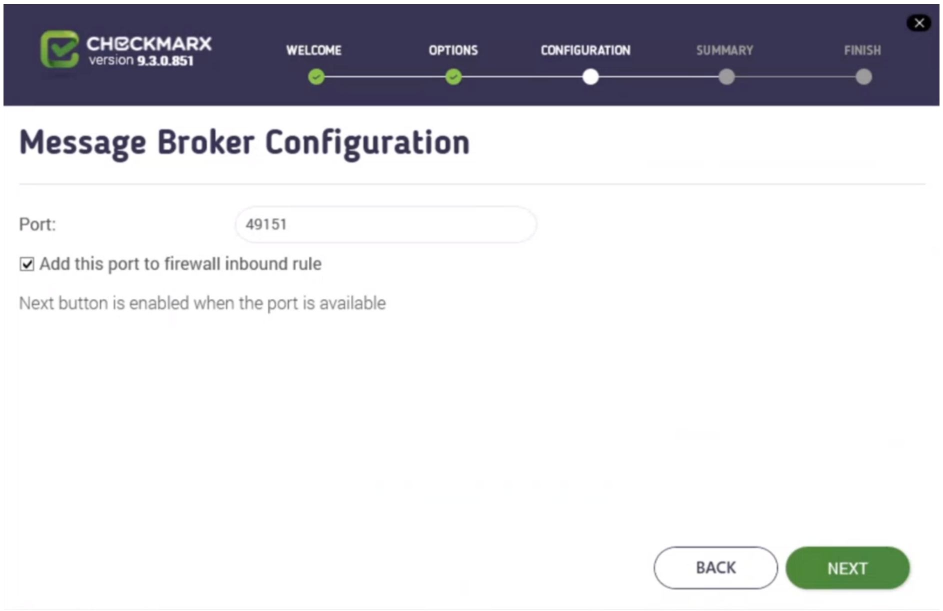
6. If using a non-standard database port, provide the server name with a comma followed by the port number, for example port **25**, which looks as follows: **10.32.147.16\SQLEXPRESS,25.**

- The SQL server can also be installed on a different station. It does not have to be installed on the CxManager station as explained here.
- For upgrades, previously defined SQL server instance settings are loaded from the existing configuration and cannot be changed.

7. 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**. This option does not require login credentials.
   - **Connect using SQL Server Authentication**. This option requires providing an SQL user name and password for login with SA permissions.
8. Click **<Test Connection>**.
   - If the database was not in use, a message appears indicating that the connection was successful.
   - If a previously used database exists, a message appears indicating that a database has been detected. In this case, you may continue using the database or re-install it as explained in the message that appeared.

- 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).

9. To add the displayed port in the **Message Broker Configuration** window to the firewall inbound rules, check **Add This Port to Firewall Inbound Rules**.



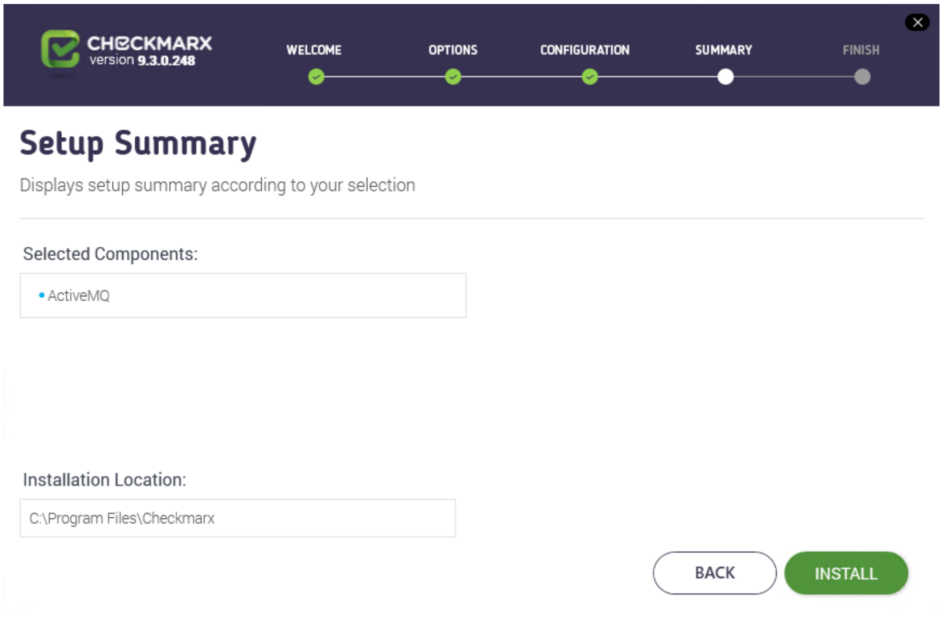
Message Broker Configuration

Port: 49151

☑ Add this port to firewall inbound rule

Next button is enabled when the port is available

10. Click <**NEXT**>. The setup summary appears.



Setup Summary

Displays setup summary according to your selection

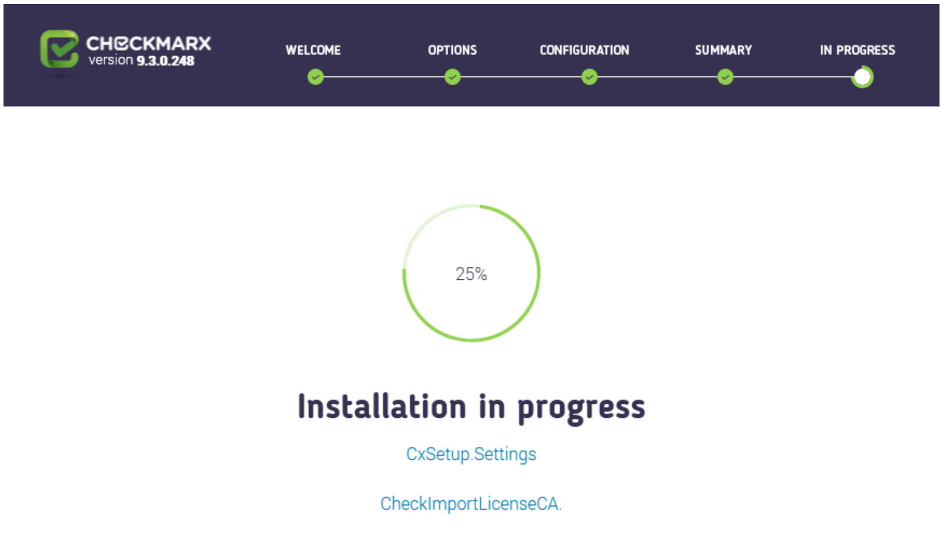
Selected Components:

- ActiveMQ

Installation Location:

C:\Program Files\Checkmarx

11. Click <**INSTALL**> to continue. The **Installation in Progress** window is displayed and the installation proceeds, which may take a few minutes.
    - To return to the previous window, click <**BACK**>.
    - To exit, click <**X**>.

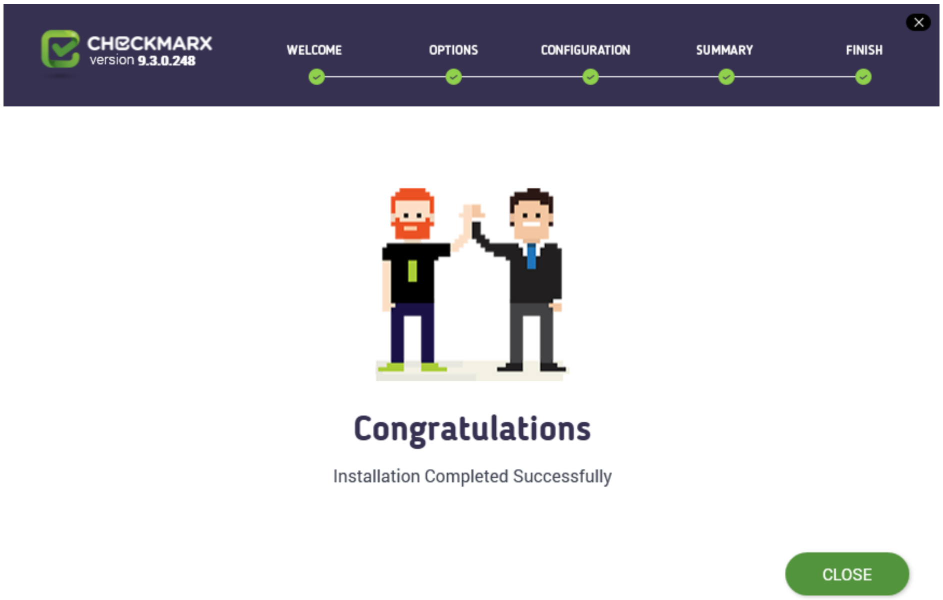


Installation in progress

CxSetup.Settings

CheckImportLicenseCA.

12. Once successfully installed, the **Installation Completed Successfully** window is displayed.
13. After the installation has been completed successfully, return to the CxManager Installation and complete the Access Control configuration by reloading and thus refreshing the parameter set.



Congratulations

Installation Completed Successfully

14. Click <**CLOSE**> to complete the installation.

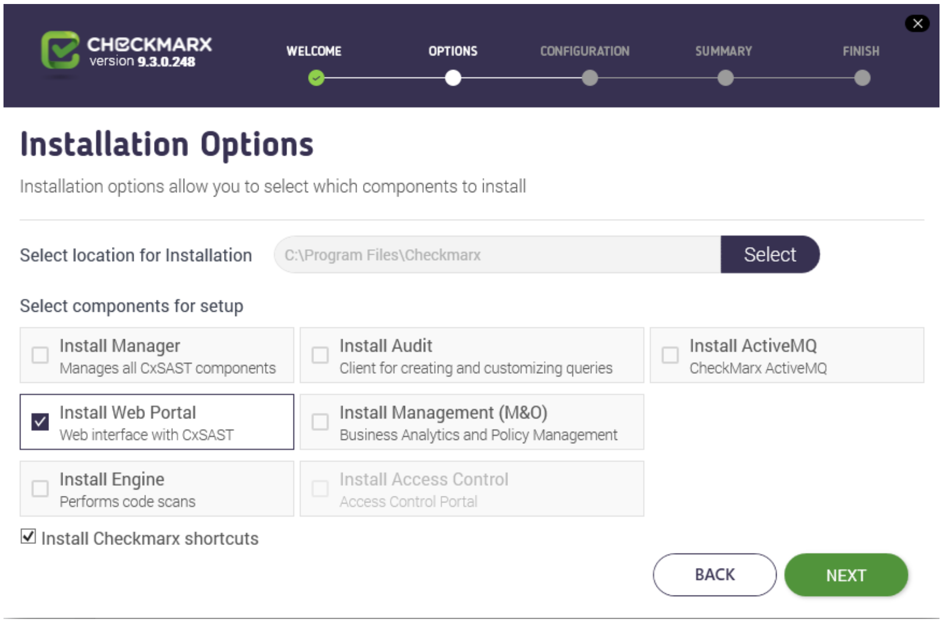
Installing and Configuring the Web Portal

The third component to install in this sequence is the Web Portal. Once the Web Portal has been installed, you have to configure it.

You have to install the Web Portal before installing CxEngine as part of installing CxEngine is logging on to and registering the new engine via the web portal.

➢ **To install the Web Portal:**

1. Select **Install Web Portal** only.



Installation Options

Installation options allow you to select which components to install

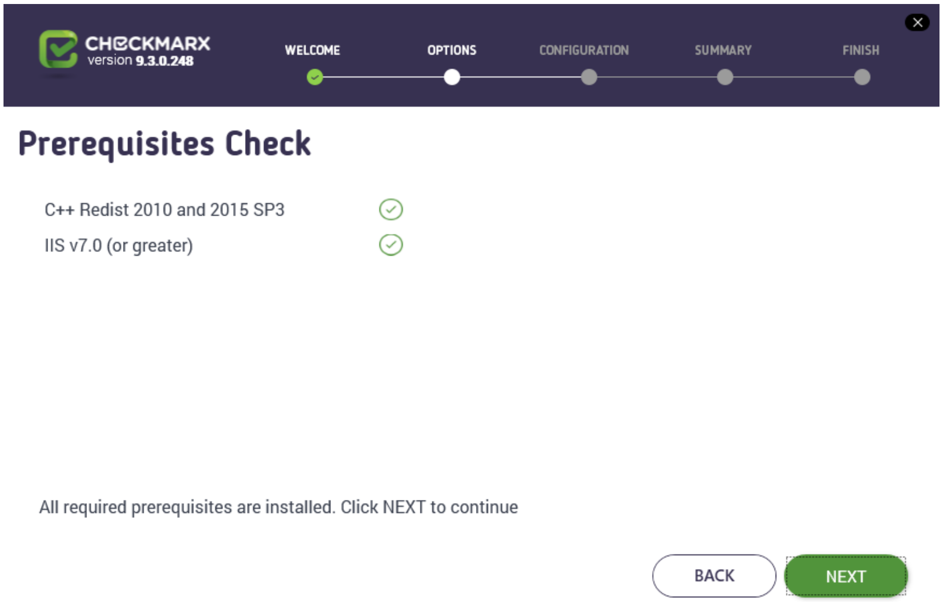
Select location for Installation: C:\Program Files\Checkmarx

Select components for setup

- □ Install Manager – Manages all CxSAST components
- □ Install Audit – Client for creating and customizing queries
- □ Install ActiveMQ – CheckMarx ActiveMQ
- ☑ Install Web Portal – Web interface with CxSAST
- □ Install Management (M&O) – Business Analytics and Policy Management
- □ Install Engine – Performs code scans
- □ Install Access Control – Access Control Portal

☑ Install Checkmarx shortcuts

2. Click **Next** to continue. The **Prerequisites Check** window is displayed, showing the status of the required components to install the Web Portal. For additional information and instructions on installing and preparing the required software, refer to Preparing to Install CxSAST.



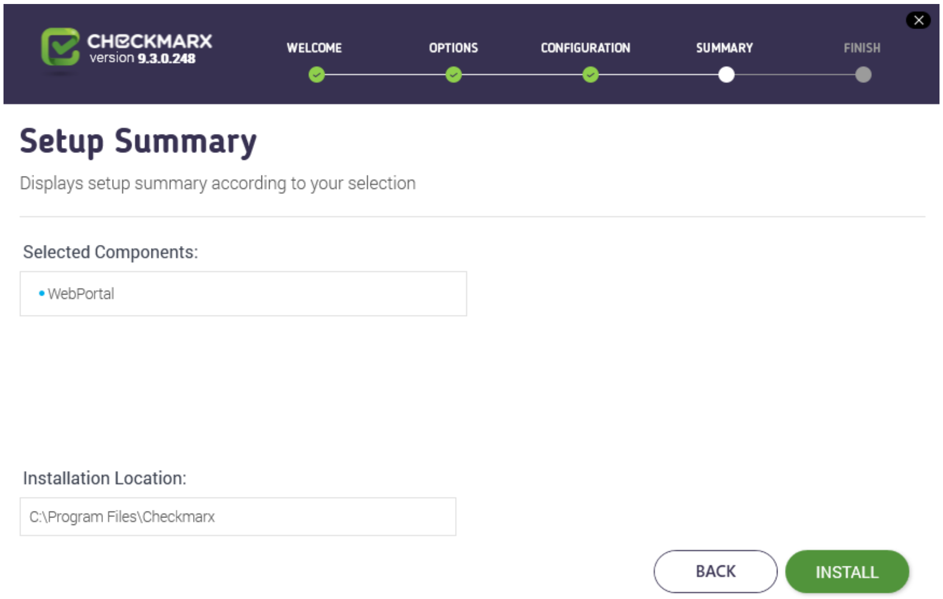
Prerequisites Check

C++ Redist 2010 and 2015 SP3 ✓

IIS v7.0 (or greater) ✓

All required prerequisites are installed. Click NEXT to continue

3. Once all components are indicated to be available ✓, click <**NEXT**>. The setup summary appears.



Setup Summary

Displays setup summary according to your selection

Selected Components:

- WebPortal

Installation Location:

C:\Program Files\Checkmarx

4. Click <**INSTALL**> to continue. The **Installation in Progress** window is displayed and the installation proceeds, which may take a few minutes.
   - To return to the previous window, click <**BACK**>.
   - To exit, click <**X**>.
5. Once successfully installed, the **Installation Completed Successfully** window is displayed.
6. Click <**CLOSE**> to complete the installation.

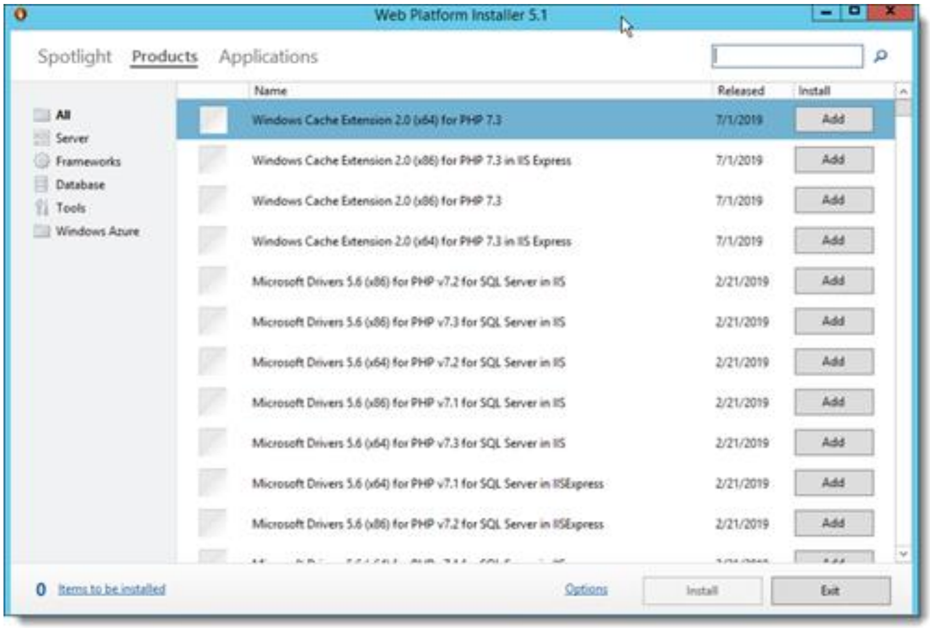
Configuring the Web Portal

To secure communications between all Checkmarx Software Exposure Platform components, we recommend that you install a signed certificate and enable SSL on the CxManager to enforce SSL security (HTTPS). This instruction defines the procedure for enabling SSL support on the CxManager.

The Checkmarx web portal can be configured using the Microsoft Web Platform Installer and the IIS Management console on the Checkmarx Web Portal server. The configurations steps can be performed manually from the Checkmarx Web Portal server. Once you have installed the IIS application components of the Checkmarx Software Exposure Platform setup, you can start configuring the Web Portal as explained below.

➢ **To configure the Web Portal:**

1. Go to the Microsoft Web Platform Installer and click **Install this extension to download the installation file.**
2. Run the **Microsoft Web Platform Installer** on the Checkmarx Web Portal server station. The Microsoft Web Platform Installer is displayed.



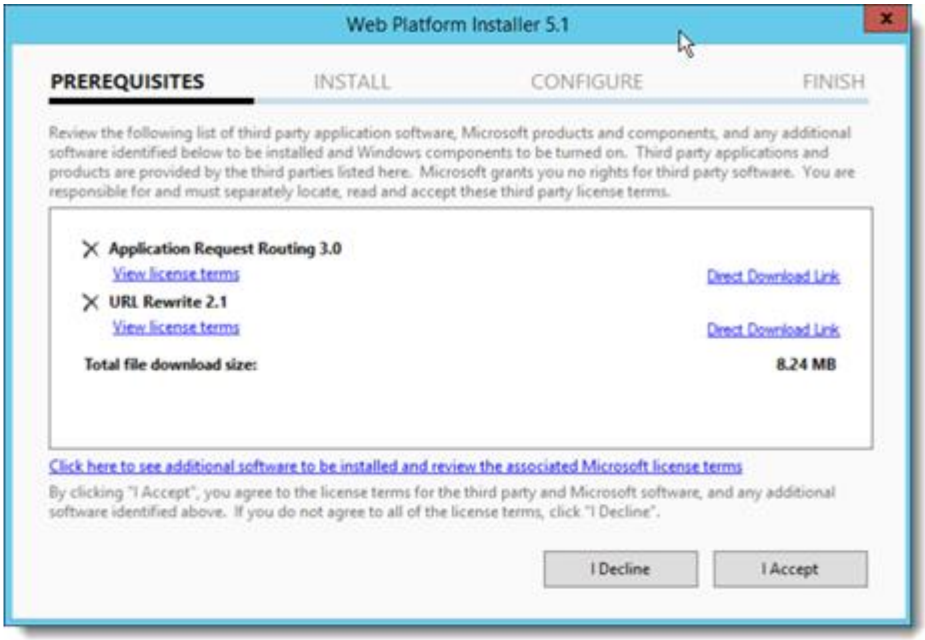
Name	Released	Install
Windows Cache Extension 2.0 (x64) for PHP 7.3	7/1/2019	Add
Windows Cache Extension 2.0 (x86) for PHP 7.3 in IIS Express	7/1/2019	Add
Windows Cache Extension 2.0 (x86) for PHP 7.3	7/1/2019	Add
Windows Cache Extension 2.0 (x64) for PHP 7.3 in IIS Express	7/1/2019	Add
Microsoft Drivers 5.6 (x86) for PHP v7.2 for SQL Server in IIS	2/21/2019	Add
Microsoft Drivers 5.6 (x86) for PHP v7.3 for SQL Server in IIS	2/21/2019	Add
Microsoft Drivers 5.6 (x64) for PHP v7.2 for SQL Server in IIS	2/21/2019	Add
Microsoft Drivers 5.6 (x86) for PHP v7.1 for SQL Server in IIS	2/21/2019	Add
Microsoft Drivers 5.6 (x64) for PHP v7.3 for SQL Server in IIS	2/21/2019	Add
Microsoft Drivers 5.6 (x64) for PHP v7.1 for SQL Server in IISExpress	2/21/2019	Add
Microsoft Drivers 5.6 (x86) for PHP v7.2 for SQL Server in IISExpress	2/21/2019	Add

3. Open the **Products** tab and do the following:

   a) Search for the **URL Rewrite 2.1** module and click <**Add**>.

   b) Search for the **Application Request Routing 3.0** module and click <**Add**>.

4. Click <**Install**>. The prerequisites for Web Platform Installer is displayed.



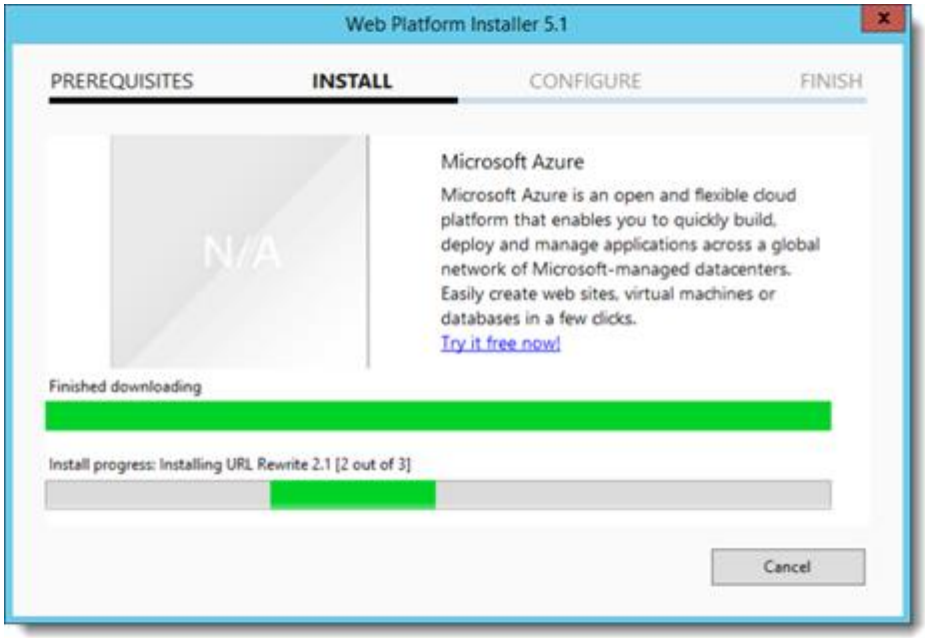
Review the following list of third party application software, Microsoft products and components, and any additional software identified below to be installed and Windows components to be turned on. Third party applications and products are provided by the third parties listed here. Microsoft grants you no rights for third party software. You are responsible for and must separately locate, read and accept these third party license terms.

✕ Application Request Routing 3.0 View license terms	Direct Download Link
✕ URL Rewrite 2.1 View license terms	Direct Download Link
Total file download size:	8.24 MB

Click here to see additional software to be installed and review the associated Microsoft license terms

By clicking "I Accept", you agree to the license terms for the third party and Microsoft software, and any additional software identified above. If you do not agree to all of the license terms, click "I Decline".

5. Click <**I Accept**>. The installation progress is displayed. You are notified once the installation completed successfully.



Microsoft Azure

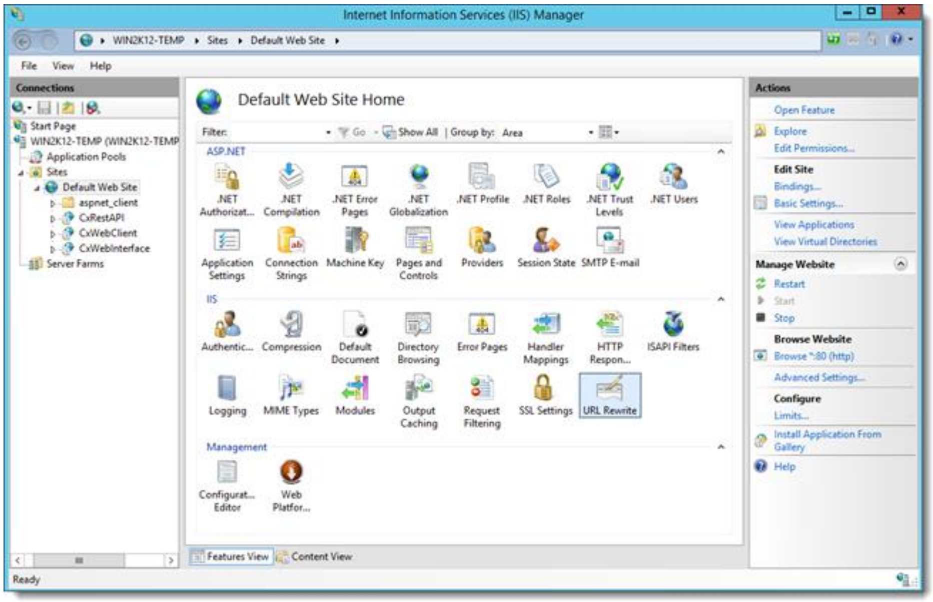
Microsoft Azure is an open and flexible cloud platform that enables you to quickly build, deploy and manage applications across a global network of Microsoft-managed datacenters. Easily create web sites, virtual machines or databases in a few clicks.

Try it free now!

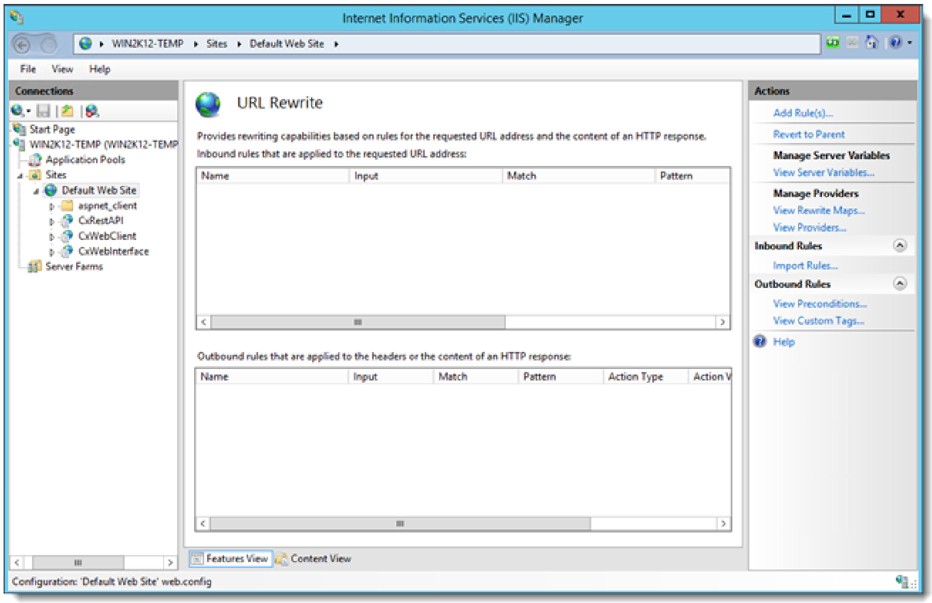
Finished downloading

Install progress: Installing URL Rewrite 2.1 [2 out of 3]

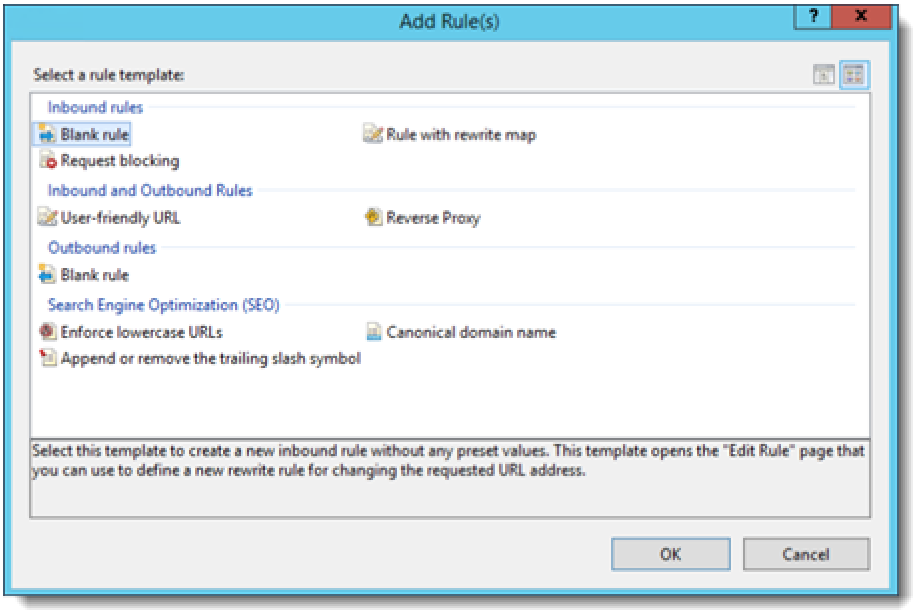
6. Click <**Finish**>.
7. Open the **Internet Information Services (IIS) Manager** on the Checkmarx Web Portal server (**IIS Manager > Sites > Default Web Site > IIS > URL Rewrite**).



8. Right click on **URL Rewrite** and select **Open Feature**. The URL Rewrite Rule option is displayed.

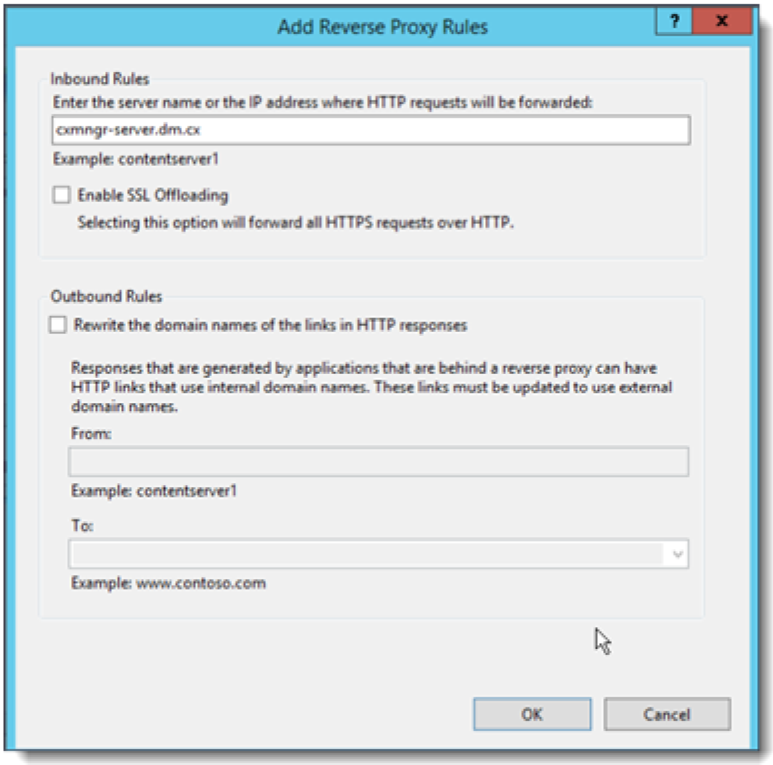

Internet Information Services (IIS) Manager
WIN2K12-TEMP ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
WIN2K12-TEMP (WIN2K12-TEMP
Application Pools
Sites
Default Web Site
aspnet_client
CxRestAPI
CxWebClient
CxWebInterface
Server Farms
URL Rewrite
Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.
Inbound rules that are applied to the requested URL address:
Name Input Match Pattern
Outbound rules that are applied to the headers or the content of an HTTP response:
Name Input Match Pattern Action Type Action V
Features View
Content View
Actions
Add Rule(s)...
Revert to Parent
Manage Server Variables
View Server Variables...
Manage Providers
View Rewrite Maps...
View Providers...
Inbound Rules
Import Rules...
Outbound Rules
View Preconditions...
View Custom Tags...
Help
Configuration: 'Default Web Site' web.config

9. From the **Action** panel, select **Add Rule(s)**. The Rule Templates List is displayed.



Select this template to create a new inbound rule without any preset values. This template opens the "Edit Rule" page that you can use to define a new rewrite rule for changing the requested URL address.

10. From **Inbound and OutBound Rules**, select **Reverse Proxy** and click <**OK**>. The Add Reverse Proxy Rule dialog is displayed.



Inbound Rules

Enter the server name or the IP address where HTTP requests will be forwarded:

cxmngr-server.dm.cx

Example: contentserver1

☐ Enable SSL Offloading

Selecting this option will forward all HTTPS requests over HTTP.

Outbound Rules

☐ Rewrite the domain names of the links in HTTP responses

Responses that are generated by applications that are behind a reverse proxy can have HTTP links that use internal domain names. These links must be updated to use external domain names.

From:

Example: contentserver1

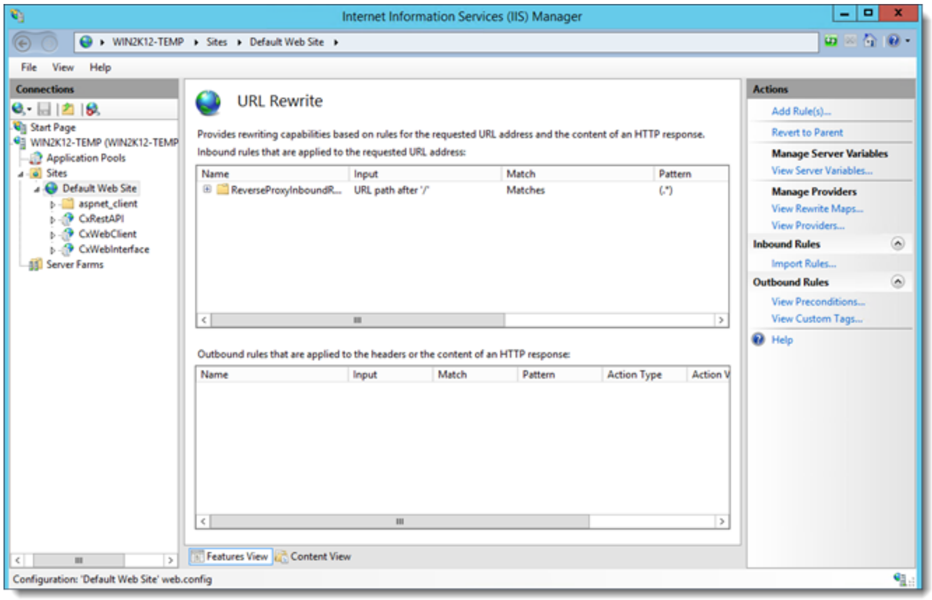
To:

Example: www.contoso.com

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

12. Disable the **SSL Offloading** option.

13. Click <**OK**> to save the changes. The new rule is displayed.



Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

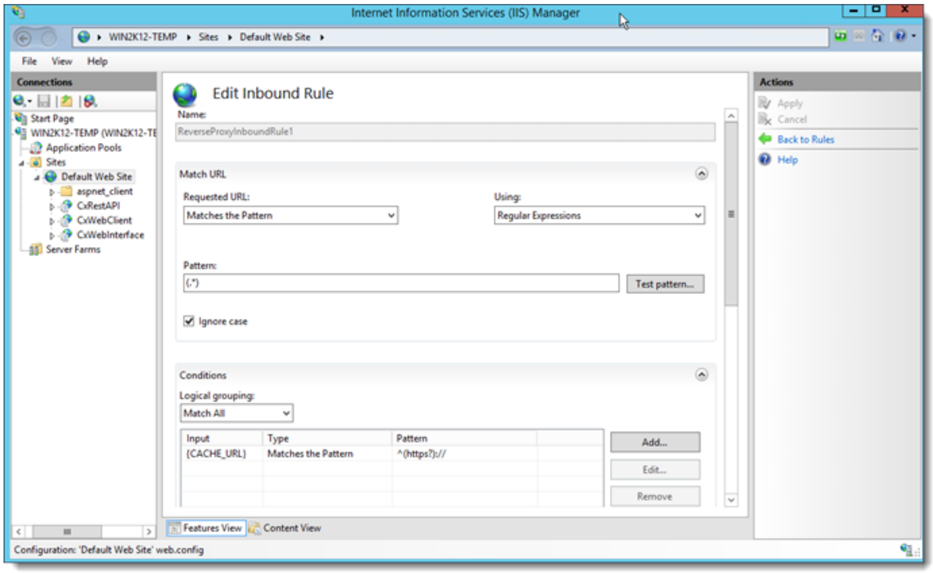
Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern
ReverseProxyInboundR...	URL path after '/'	Matches	(.*)

Outbound rules that are applied to the headers or the content of an HTTP response:

Name	Input	Match	Pattern	Action Type	Action V

14. Select the newly created Rule and from the **Inbound Rules** panel (right) and click <**Edit**>. The Edit Inbound Rule window is displayed.



Name: ReverseProxyInboundRule1

Requested URL: Matches the Pattern

Using: Regular Expressions

Pattern: (.*)

☑ Ignore case

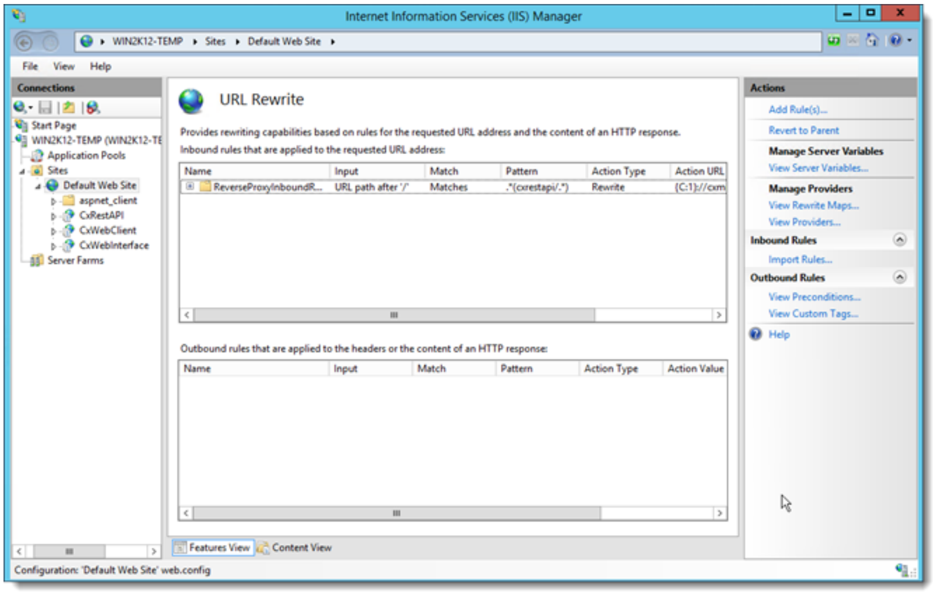
Logical grouping: Match All

Input	Type	Pattern
{CACHE_URL}	Matches the Pattern	^(https?)://

15. Add/change the following:

- **Pattern**: .*(cxrestapi/.*)
- **Action Type**: Rewrite

16. Click <**Apply**> and verify the changes in the URL Rewrite rule.



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

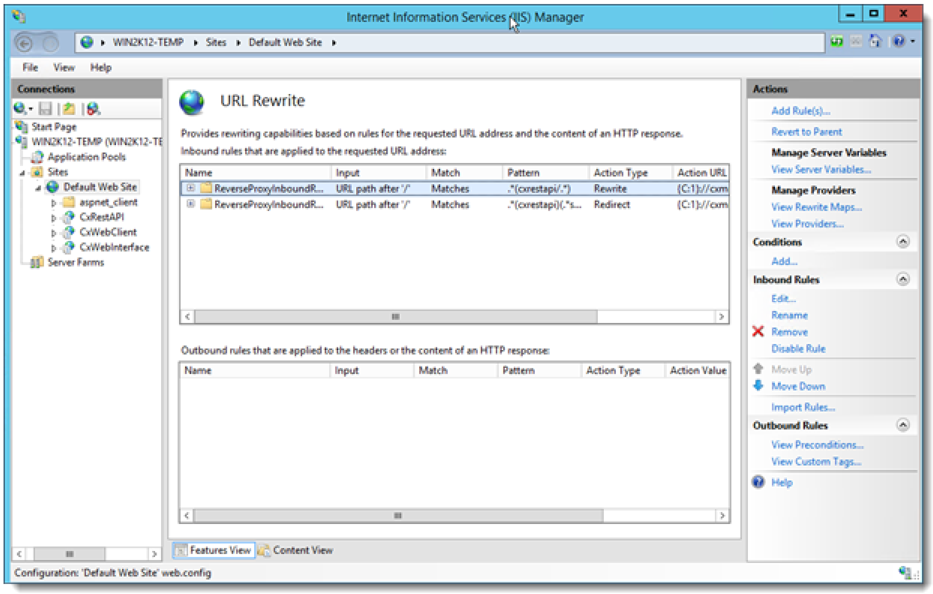
Name	Input	Match	Pattern	Action Type	Action URL
ReverseProxyInboundR...	URL path after '/'	Matches	.*(cxrestapi/.*)	Rewrite	{C:1}://cxm

Outbound rules that are applied to the headers or the content of an HTTP response:

Name	Input	Match	Pattern	Action Type	Action Value

Configuration: 'Default Web Site' web.config

17. If you are using SAML, add a second rule, add/change the following:
    - **Pattern**: .*(cxrestapi)(.*samlLogin).*
    - **Action Type**: Redirect
18. Click <**Apply**> and verify the changes in the URL Rewrite rule.
19. Once both rules should be displayed, select the new rule and click 'move up'.



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern	Action Type	Action URL
ReverseProxyInboundR...	URL path after '/'	Matches	.*(cxrestapi/.*)	Rewrite	{C:1}://cxm
ReverseProxyInboundR...	URL path after '/'	Matches	.*(cxrestapi)(.*s...	Redirect	{C:1}://cxm

Outbound rules that are applied to the headers or the content of an HTTP response:

Name	Input	Match	Pattern	Action Type	Action Value

Configuration: 'Default Web Site' web.config

20. On the Cx Web Portal server, under **C:\Program Files\Checkmarx\CheckmarxWebPortal\Web**, open the '**web.config**' file in the editor and update the following for the value of '**CxWSResolver.CxWSResolver**' with the CxManager server IP/domain name.

Example:

from....

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

to....

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

21. Open the command line interface (CMD) as Administrator and enter the following command:

```
appcmd.exe set config -section:system.webserver/proxy -preserveHostHeader:true /commit:apphost
```

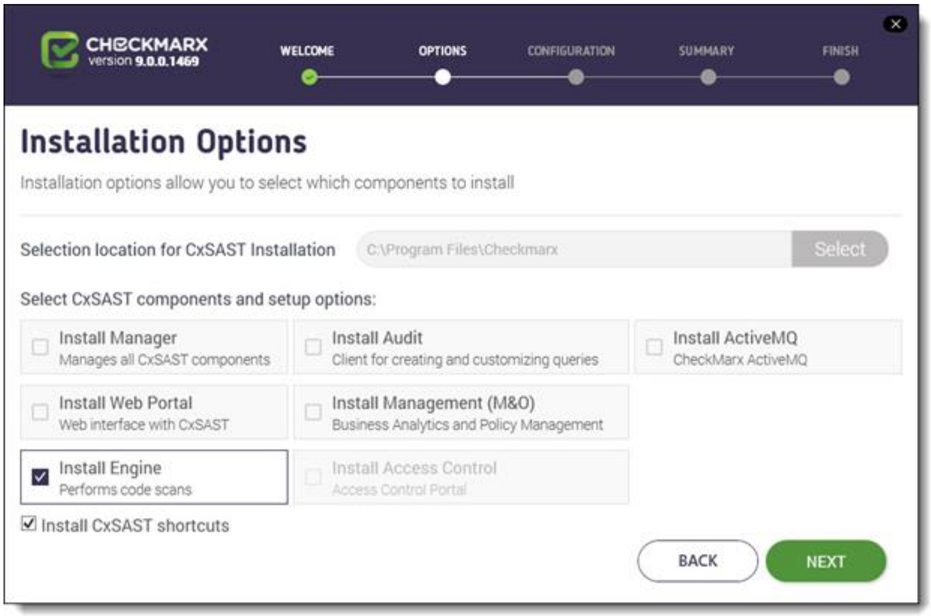
22. Test the Checkmarx Web Portal and Software Exposure Platform. The system is now ready for **CxEngine** to be installed.

Installing the CxEngine Server

The fourth and final component to install in this sequence is the CxEngine.
In order to be able to log on to the CxSAST web interface, you must have the Web Portal installed before installing CxEngine.

➢ **To install CxEngine:**

1. Select **Install Engine** only.



Installation Options

Installation options allow you to select which components to install

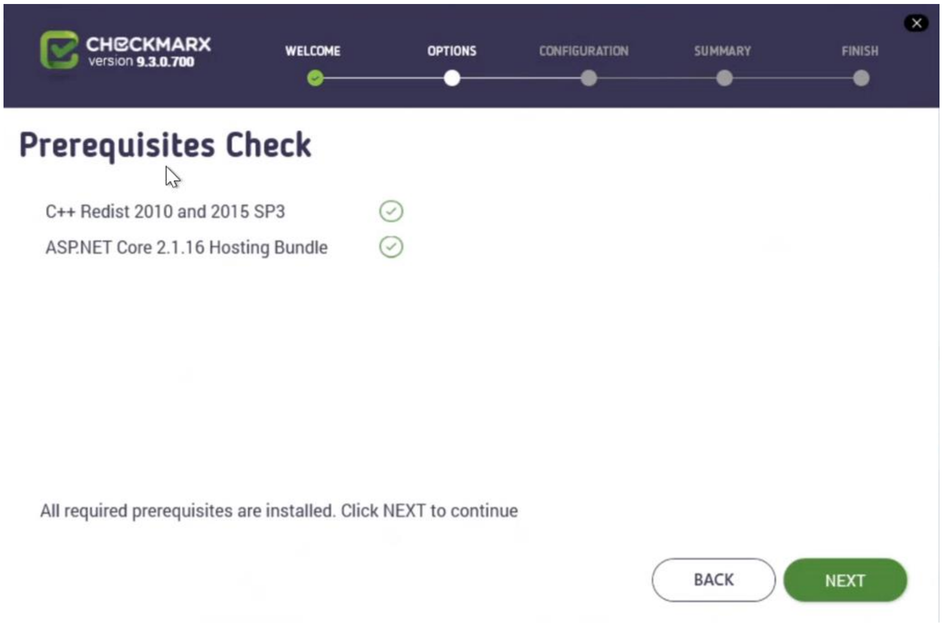
Selection location for CxSAST Installation: C:\Program Files\Checkmarx

Select CxSAST components and setup options:

- □ Install Manager — Manages all CxSAST components
- □ Install Audit — Client for creating and customizing queries
- □ Install ActiveMQ — CheckMarx ActiveMQ
- □ Install Web Portal — Web interface with CxSAST
- □ Install Management (M&O) — Business Analytics and Policy Management
- ☑ Install Engine — Performs code scans
- □ Install Access Control — Access Control Portal

☑ Install CxSAST shortcuts

2. Click <**Next**> to continue. The **Prerequisites Check** window is displayed, showing the status of the required components to install the CxEngine server.



Prerequisites Check

C++ Redist 2010 and 2015 SP3 ✓

ASP.NET Core 2.1.16 Hosting Bundle ✓

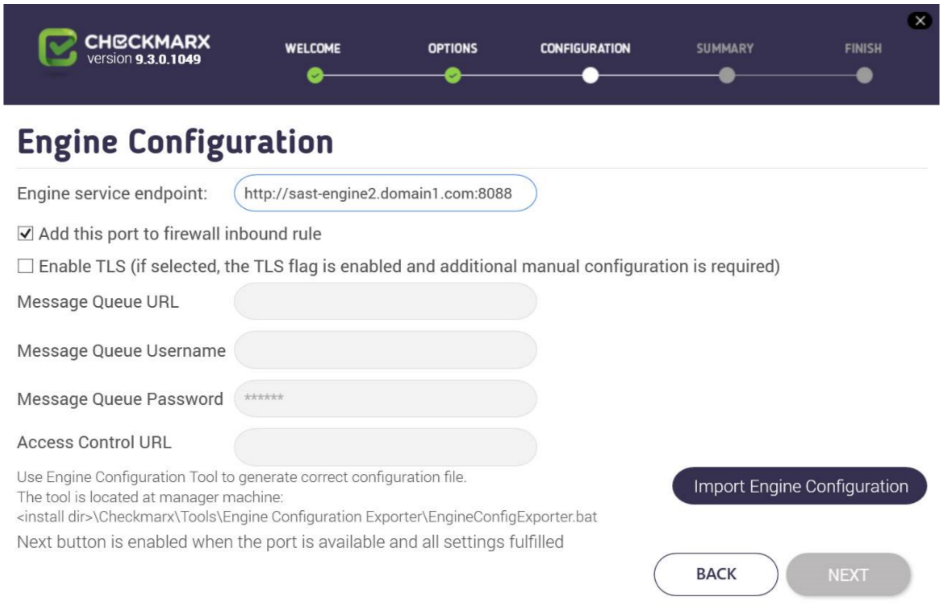
All required prerequisites are installed. Click NEXT to continue

3. For any prerequisite component not installed, click <**Prerequisites Folder**> to browse for and install each missing prerequisite component.

   In addition to version 2010, the CxEngine Server requires C++ Redist Version 2015.

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

5. When all prerequisite components are installed, click <**Next**> to display the Engine Configuration window.



Engine Configuration

Engine service endpoint: http://sast-engine2.domain1.com:8088

☑ Add this port to firewall inbound rule

☐ Enable TLS (if selected, the TLS flag is enabled and additional manual configuration is required)

Message Queue URL

Message Queue Username

Message Queue Password ******

Access Control URL

Use Engine Configuration Tool to generate correct configuration file.
The tool is located at manager machine:
<install dir>\Checkmarx\Tools\Engine Configuration Exporter\EngineConfigExporter.bat

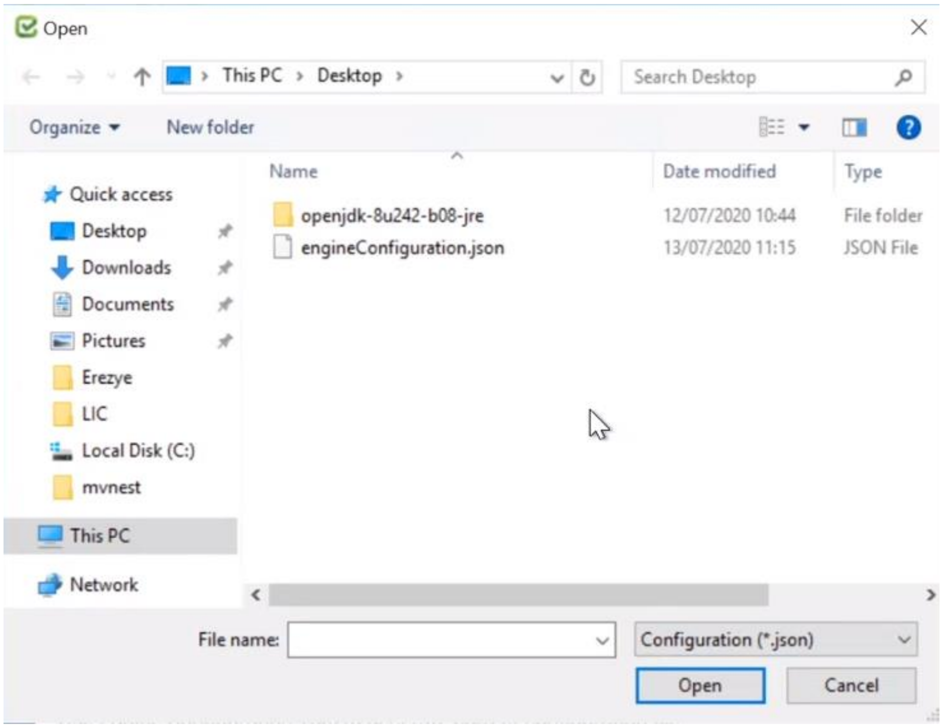
Next button is enabled when the port is available and all settings fulfilled

➢ **To set up the CxEngine:**

1. Enter the service endpoint URL in the Engine Service Endpoint field (http://{IP or FQDN}:{port}). If you use a domain name, it reads looks similar to http://<engine name>.<location.domain>:<port number>, for example http://engine1.checkmarx.com:8088

- Errors in the URL such as an illegal port result in an error indication ⊗ and you cannot continue the process until the error is corrected.
- The CxEngine Server uses port **8088** by default. You can also use a different port, although it is not recommended.
- All the CxEngine Server environment variables can be viewed and edited in the Windows Properties once the engine is configured and running.

2. To open the required port in the Windows firewall, check Add this Port to Firewall Inbound Rule.
3. To enable encryption via TLS, check Enable TLS. This switches the TLS variable to true in the environment variables under Windows Properties.
4. On the station hat has CxManager installed, open the file explorer and navigate to the installation folder, for example C:\Program Files and from there to ..\Checkmarx\Tools\Engine Configuration Exporter.
5. Run EngineConfigExporter.bat. Two new folders are created, Logs and Output. The engine configuration file engineConfiguration.json is generated in the Output folder.
6. Go to the Output folder and copy engineConfiguration.json to a location of your choice on the CxEngine station.
7. To invoke the engine parameters, click <Import Engine Configuration>. The file explorer opens.



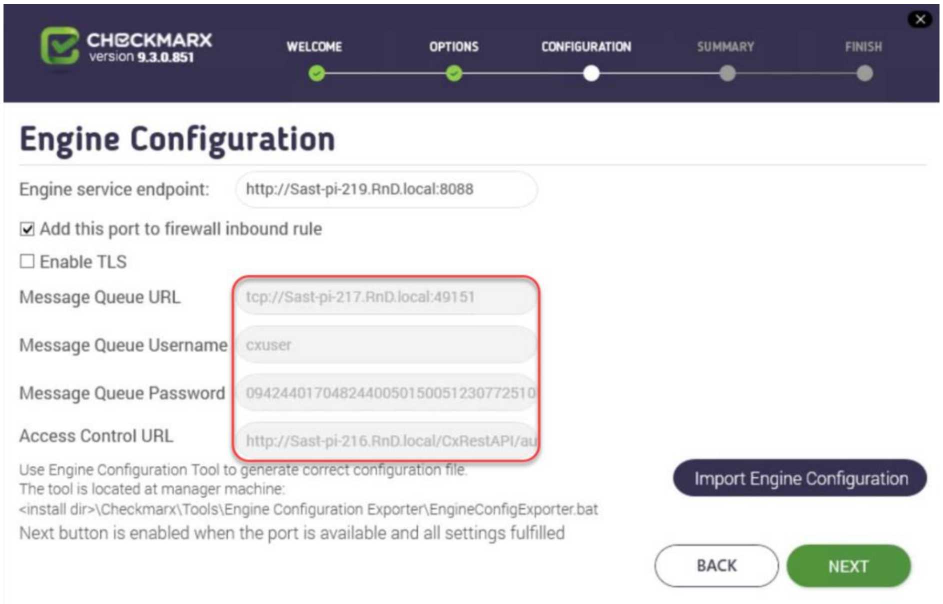
Name	Date modified	Type
openjdk-8u242-b08-jre	12/07/2020 10:44	File folder
engineConfiguration.json	13/07/2020 11:15	JSON File

File name:

Configuration (*.json)

8. Navigate to the file location **engineConfiguration.json** file's location and click <**Open**>.
9. The Engine configuration is imported and displayed in the relevant fields of the Engine Configuration window.

- The imported parameters cannot be entered or edited manually in the Engine Configuration dialog box.
- The engine configuration is available for editing as Windows Environment Variables. For additional information, refer to the relevant page.



Engine Configuration

Engine service endpoint: http://Sast-pi-219.RnD.local:8088

☑ Add this port to firewall inbound rule

☐ Enable TLS

Message Queue URL: tcp://Sast-pi-217.RnD.local:49151

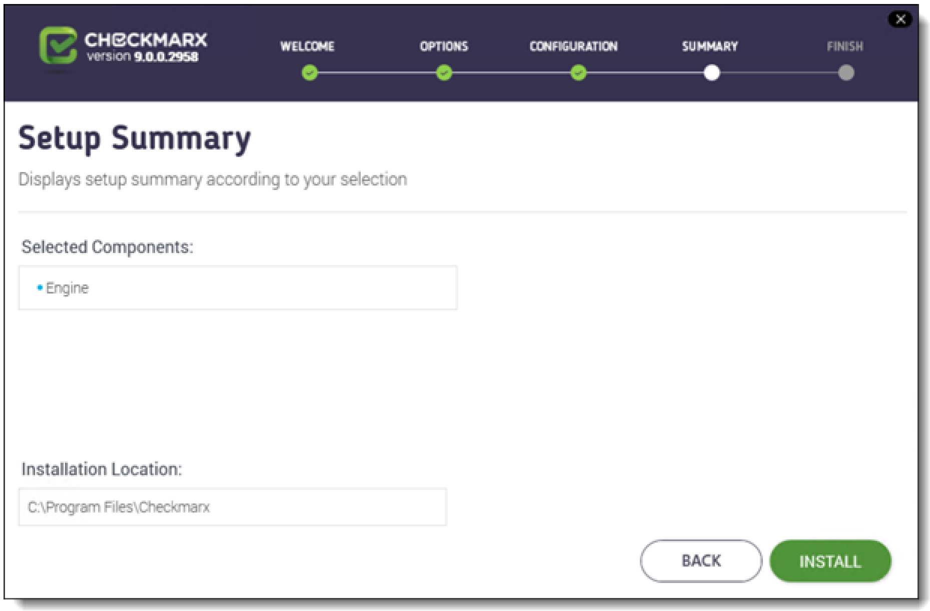
Message Queue Username: cxuser

Message Queue Password: 094244017048244005015005123077251O

Access Control URL: http://Sast-pi-216.RnD.local/CxRestAPI/au

Use Engine Configuration Tool to generate correct configuration file.
The tool is located at manager machine:
<install dir>\Checkmarx\Tools\Engine Configuration Exporter\EngineConfigExporter.bat
Next button is enabled when the port is available and all settings fulfilled

10. Click <**Next**>. The **Setup Summary** window is displayed.



Setup Summary

Displays setup summary according to your selection

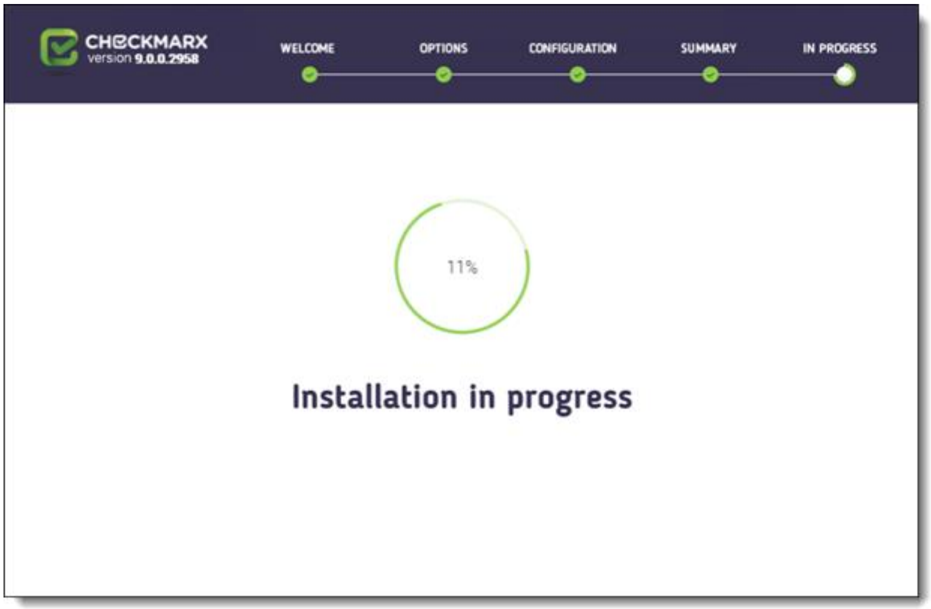
Selected Components:

- Engine

Installation Location:

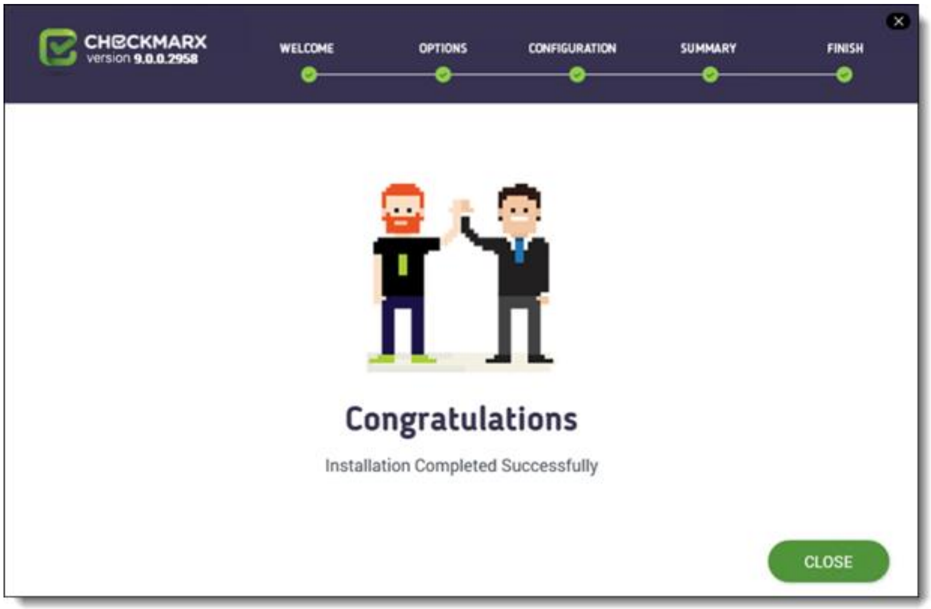
C:\Program Files\Checkmarx

11. Check the setup summary according to your selection.
12. Click <**INSTALL**> to continue. The **Installation in Progress** window is displayed and the installation proceeds, which may take a few minutes.
    - To return to the previous window, click <**BACK**>.
    - To exit, click <**X**>.



Installation in progress

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



Congratulations

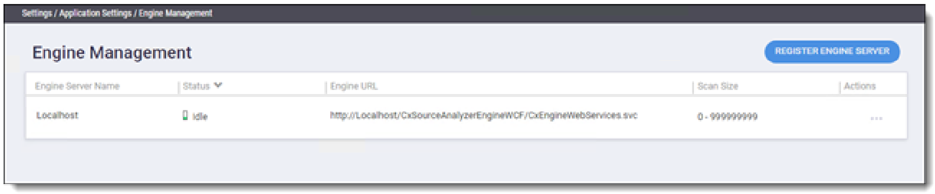
Installation Completed Successfully

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

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

15. Log into the CxSAST web interface.

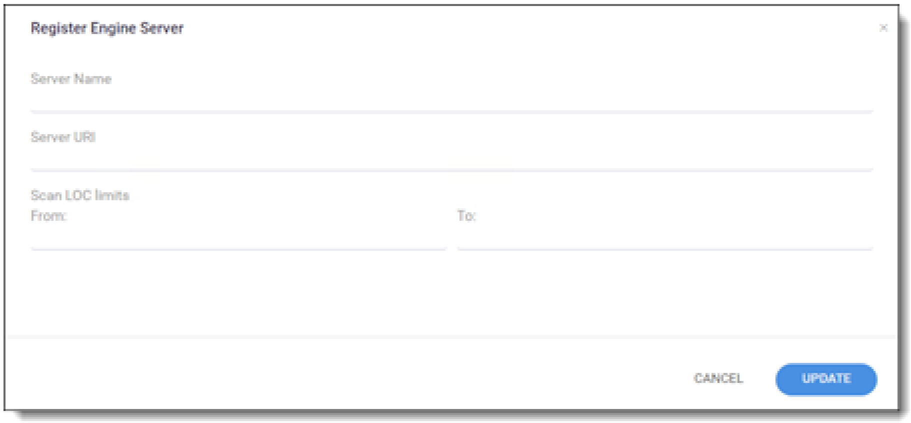
16. Go to **Settings > Application Settings > Engine Management.** The **Engine Management** window is displayed.



Engine Management

Engine Server Name	Status	Engine URL	Scan Size	Actions
Localhost	Idle	http://Localhost/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc	0 - 999999999	...

17. Click <**Register Engine Server**>. The **Register Engine Server** window is displayed.



18. Assign a **Server Name** to the engine, and provide the **Server URL** to enable CxManager to communicate with CxEngine.

    The URL is something like **http://{IP or FQDN}:{port}**. {IP or FQDN} refers to the IP address or the host name.

19. Click <**Update**>.

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

- 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.

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

Installing and Configuring CxEngine under Linux

Starting with CxSAST 9.3, CxEngine supports both Windows and Linux, thus becoming a cross-platform. These pages explain how to install CxEngine under Linux, transition to Linux and establish a secure connection between CxEngine and CxManager.

Before you start installing CxEngine, refer to Preparing the System for Cross-Platform Query Support for additional information.

Starting with CxSAST 9.3, CxEngine is supported by the common Linux distributions, which are the following:

- CentOS
- RHEL (Red Hat Enterprise Linux)
- Ubuntu
- Amazon Linux

Some Amazon Linux images are pre-configured with a limited number of file-descriptors, which may render the EngineService unstable. In these cases, the following message is returned: **No file descriptors available**

Required Prerequisites for Installing CxEngine

- Linux host, equipped with either an x64 or arm64 processor.
- Docker engine, available from https://docs.docker.com/engine/install/
- **For Amazon Linux images**: Increased limit of file descriptors as explained below.

➢ **To increase the limit of file descriptors in Linux, enter the following into the console:**

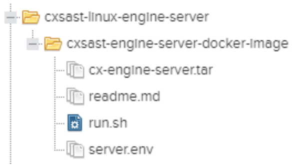
1. Run: **ulimit**
   Verify that there is no limit to max number of files
2. Run: **ps ~A**
   Find the process number of dotnet (proc#)
3. Run: **cat /proc/proc#/limits**
   Check the Max open files (soft/hard) - it should be 4096/65535 at least
4. If the current limit is below the expected values, edit **/etc/security/limits.conf**,
   Add these lines:
   ```
   * soft nofile 4096
   * hard nofile 65535
   ```
5. Restart the machine for the changes to take effect
6. Repeat steps 1-3 and verify the limits have changed.
   If the problem persists - edit **run.sh**
   Add this parameter to the docker run command:
   --ulimit nofile=4096:65535
   ```
   docker run --ulimit nofile=4096:65535
   ```

Package Content

The CxEngine package for Linux contains the following files:

- cx-engine-server.tar (CxEngine image)
- readme.md
- run.sh
- server.env

The package is provided with the following directory structure:



cxsast-linux-engine-server
cxsast-engine-server-docker-image
cx-engine-server.tar
readme.md
run.sh
server.env

Installation and Configuration

These instructions assume that the prerequisites are in place and you downloaded the installation package.

➢ **To install CxEngine**

1. Create a new directory.
2. Copy the three installation files into the new directory:
   cx-engine-server.tar
   server.env
   run.sh
3. Retrieve the AMQ Password and the URL. The AMG is usually deployed as part of the CxManager component.

1. To retrieve the AMQ password, connect to the CxSAST database, and execute the following SQL query:

```
SELECT TOP (1000) [Id]
,[Key]
,[Value]
,[Description]
FROM [CxDB].[dbo].[CxComponentConfiguration]
WHERE [Key] = 'MessageQueuePassword'
```

2. To retrieve the AMQ URL, connect to the CxSAST database and execute the following SQL query:

```
SELECT TOP (1000) [Id]
,[Key]
,[Value]
,[Description]
FROM [CxDB].[dbo].[CxComponentConfiguration]
WHERE [Key] = 'ActiveMessageQueueURL'
```

4. Open server.env and update the following environment variables with the required data as follows:
   ES_MESSAGE_QUEUE_PASSWORD={retrieve from database}
   ES_MESSAGE_QUEUE_URL=tcp://{client host address as explained below}:{port}
   CX_ES_ACCESS_CONTROL_URL=http://{client host address}/CxRestAPI/auth
   CX_ES_END_POINT={cx-server host address - example - http://x.x.x.x:8088}
5. Enter **sh run.sh** to install CxEngine. The image (cx-engine-server.tar) is extracted and loaded. The container is established.

- **run.sh** uses port 8088 by default, which must be entered in the **server.env** variables as relevant. To use a different port, follow the instructions below and use that new port where entering the port is required.

- Unlike Windows services, the CxSAST Linux container does not restart automatically by default.
  To configure the CxSAST Linux Engine containers to restart automatically, open run.sh with your text editor and, in the “docker_run_args=” section, add or uncomment “—restart=always” (as needed).

Changing the Port for the Command run.sh

It is recommended to use the default port (port 8088). If you have to use a different port, for example **port 8090**, change the port as follows:

1. Run the “docker run” command **0.0.0.0:{exposed port}:8090**
2. Save the new setting.

Verifying that the Server with CxEngine is Running

The syntax below assumes that you use the default port (port 8088).

1. Run the “docker ps” command. The following is returned, if the container is running:
   ```
   * IMAGE: cx-engine-server
   * PORTS: 0.0.0.0:8088->8088/tcp
   ```
2. Run the command "docker logs -f {container ID}”. The following is returned if the server is running.
   ```
   * Now listening on: <http://[::]:8088> |Application started
   ```

➢ **To connect CxEngine to the Application:**

- In the web portal, go to **Settings > Application Settings > Engine Management** and connect to the new engine as explained under Engine Management.

Preparing the System for Cross-Platform Query Support

There are differences between Windows and Linux with respect to file names and new line characters. Therefore, CxSAST queries have been adjusted to run run on Windows and Linux. User custom queries must follow the same adaptations to support both platforms as explained below.

Required Adjustments

There are two differences between Linux and Windows:

1. File names:

    a) Windows – *\temp\config.xml
    b) Linux – */temp/config.xml

2. New Line characters:

    a) Windows - `\r\n`
    b) Linux - `\n`

Solution

Already starting with CxSAST 9.2, an additional CxQL API has been introduced, the cxEnv. By using this API variable, queries can be written in a cross-platform format in order to support both operating systems.

There are 6 properties to be used in **cxEnv**:

- cxEnv.Path.DirectorySeparatorChar
- cxEnv.Path.AltDirectorySeparatorChar
- cxEnvPath.InvalidPathChars
- cxEnv.Path.PathSeparator
- cxEnv.Path.VolumeSeparatorChar
- cxEnv.NewLine

For a full description of each variable, refer to the latest CxQL API guide.

All custom queries must use the above-listed variables rather than the actual values to run on both platforms and all their flavors.

Examples

The following section illustrates two examples.

Directory Separator

This string:

```
string[] path = fileName.Split('\\');
```

Must be replaced with the following:

```
string[] path = fileName.Split(cxEnv.Path.DirectorySeparatorChar);
```

New Line in Regex

This string:

```
elseIfs.FindByRegex(@"[\W]if[^;\{]*{[^\}]*}[(\s)(\r\n)]*else[(\s)(\r\n)]*{[^\
}]*?[(/\*)(//)]");
```

Must be replaced with the following:

```
elseIfs.FindByRegex(@"[\W]if[^;\{]*{[^\}]*}[(\s)(" + cxEnv.NewLine +
@")]*else[(\s)(" + cxEnv.NewLine + @")]*{[^\}]*?[(/\*)(//)]");
```

Centos 8 Installation Notes

This note addresses users who use Centos 8 and did not set up a Docker engine yet.

RHEL switched from iptables to nftables, which means that there are no more iptables running on the Centos 8 level and all the firewall functionality is provided by nftables.

The migration from iptables to nftables requires one of the following:

- Configuring **firewalld** to use iptable configurations.
- Enabling masquerading.

Configuring Firewalld to use Iptable Configurations

This section explains how to provide an interface to firewalld to add iptables. To do so, do the following:

1. At the prompt, enter **- sudo vi /etc/firewalld/firewalld.conf**
2. Change **- FirewallBackend=nftables** to **- FirewallBackend=iptables**
3. Save the change and reload **firewalld**. To do so, enter **- sudo systemctl restart firewalld.service** at the prompt.

Enabling Masquerading

1. Check what interface docker is using (default is 'docker0').
   ip link show
2. Check available firewalld zones, e.g. 'public'.
   - sudo firewall-cmd --get-active-zones
3. Check what zone the docker interface it bound to, most likely 'no zone' yet.
   - sudo firewall-cmd --get-zone-of-interface=docker0
4. Add the 'docker0' interface to the 'public' zone. Changes take effect once firewalld is reloaded.
   - sudo nmcli connection modify docker0 connection.zone public
5. Add masquerading. It allows for docker ingress and egress.
   - sudo firewall-cmd --zone=public --add-masquerade –permanent
6. Optionally open required incoming ports (optional).
   - sudo firewall-cmd --zone=public --add-port=443/tcp
7. Reload firewalld.
   - sudo firewall-cmd –reload
8. Reload dockerd.
   - sudo systemctl restart docker

Configuring TLS (SSL) between CxManager and CxEngine

CxSAST supports a secure communication between CxManager and CxEngine based on TLS (SSL) certificates. These instructions take Windows and Linux support for CxEngine into consideration.

The Cx Engine is working on a Rest service that is not managed via the IIS console. The steps below explain how to configure the secure connection on both the CxManager and the CxEngine servers.

The secure connection is established between two servers only, it can be configured with Self Signed Certificates or real CA`s certificates. For additional information and instructions, refer to Configuring TLS (SSL) between CxManager and CxEngine (v9.3.0 and up).

Best Practices to Maintain Docker Security

This document provides tips for best best practice on the optimal security measures to be taken when running the Engine on Linux Docker.

Docker Image

The provided docker image uses the following protection:

1. Uses a limited Linux version (.NET Core 2.1 and .NET Core 3.1 alpine).
2. Creates a dedicated user (not root) to operate the respective docker.

Docker Orchestrators

When working with multiple docker orchestrators, each of them provides a default set of capabilities.

To optimize security, the customer can remove all capabilities. The Engine doesn’t require any special permission or capability in order to run.

To drop all capabilities when using Docker Compose, you can use the following command:

```
 cap_drop:
-all
```

Frequently Asked Questions on CxEngine

What does the run.sh file do? Does it create the docker every time?

- **run.sh** creates an image and then a container from that image, even if there is already one running. For additional information on **run.sh,** refer to the run.sh section.

If a client accesses the container and gets off, why is the container created again when the client accesses it again?

- It is the best practice for using Docker.

How do you rename the Docker container?

- It is a standard Docker run argument. Refer to the Docker site for more information.

Installing CxSAST in Silent Mode

Installing in ‘Silent mode’ refers to run the installation using the CLI interface instead of the GUI. You can install CxSAST in a Centralized architecture or a Distributed architecture as explained in this section.

Preparing CxSAST for Installation

To perform a distributed installation in Silent mode, first, perform and complete the installation and then run **Silent Reconfigure**.

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 the archive, extract the installation executable **CxSetup.exe** and make the required third-party components available. For further information regarding installation permissions and making third-party components available, refer to Preparing for Installation.

The required prerequisites are the following:

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

- Java installation should be located 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**.
- 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 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 Preparing for Installation.
- **Access Control** and **CxManager** must be installed on the same host.

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.

Installing/Uninstalling CxSAST in a Centralized Environment

Installing CxSAST in a centralized environment refers to installing all CxSAST components on the same host.

The CxSAST silent install/uninstall path enables you to specify property values from the command line (CLI) and is ideal for large-scale enterprise deployments. This method provides you with the ability to perform a clean installation, upgrade, and uninstallation of CxSAST in silent mode, without having to continuously interact with GUI prompts.

➢ **To install CxSAST**

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
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
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
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
```

Common CxSAST Installation Scenarios

➢ **To install CxManager unsafe-only to D:\Cx and without creating shortcuts**

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
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
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
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 install all components to a default location without a license using the SQL authentication**

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
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
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
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
```

The license can be imported at a later stage.

➢ **To install CxManager unsafe-only to a default location using SQL authentication**

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
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
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
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 install CxEngine unsafe-only**

- Enter or copy the syntax into the CLI interface without forced line breaks:

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

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

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

- For a table of available variables and parameters, refer to the Parameters page.

Uninstalling CxSAST

➢ **To uninstall CxSAST**

To uninstall CxSAST, enter the following:

```
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 the 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.

Installing CxSAST in a Distributed Environment

A distributed architecture refers to a scenario where the server components are 'distributed' over multiple dedicated servers as explained in System Architecture Overview. To install the CxSAST Server in a distributed environment (on different dedicated hosts), you have to install each CxSAST Server component specified below on the respective host in the outlined order.

The installation or upgrade of each component must be performed from the same setup file (**CxSetup.exe**) as all components must be of the same version and build.

Workflow

Before you can start installing the components, you have to make the third-party components for the respective CxSAST Server component available as explained under Preparing CxSAST for Installation. For a list of the required third-party components for each CxSAST Server component, refer to the list of required third-party components.

Once you have downloaded the CxSAST Installation package and made the third-party components available, open the command line interface on each relevant host and enter the required syntax as specified in the relevant topics below. The CxSAST server components must be installed in the following order:

1. **CxManager**. CxManager manages and integrates system components and contributes the JSON file with the engine settings that you need at a later stage.
2. **ActiveMQ**. The ActiveMQ manages the messaging queues and contributes the Message Queue parameters that are going to be loaded together with the engine configuration.
3. **Web Portal**. The Web Portal is required to access and interact with CxSAST through the web.

4. **CxEngine**. The CxEngine performs the code scans.

- To avoid permission restrictions, install each CxSAST Server component in **<root directory>:\Program Files** .
- When you install the **CxEngine**, you import the engine configuration settings stored in a JSON file that you retrieve from **CxManager**.
- **CxManager** and **ActiveMQ** must be available to the **CxEngine** installation, otherwise the application cannot operate once installed. To make these components available, you have to use **Reconfigure** to complete the installation.

Required Prerequisites for Installing CxSAST in a Distributed Environment

For required pre-requisites, refer to the section Required Prerequisites for Installing CxSAST in a Distributed Environment

Installing the CxSAST Manager

The first component to install in this sequence is the CxManager.

Prerequisites

The required prerequisites are listed below. For further information and instructions on installing and making them available, refer to Preparing for Installation.

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

- Java installation should be located 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**.
- 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 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 (v9.3.0)
- If you perform a silent installation in a Distributed environment, you cannot stop the installation before it is complete and you have to run **Reconfigure** to properly configure the setup after ActiveMQ has been installed.
- Access Control and CxManager must be installed on the same server station.

Installing CxSAST Manager

➢ **To install CxManager**

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y INSTALLFOLDER=”C:\Program
Files\Checkmarx” LIC=C:\LIC\license.cxl INSTALLSHORTCUTS=0
CX_JAVA_HOME="C:\"Program Files\Java\jre1.8.0_241" BI=0 MANAGER=1 ACTIVEMQ=0
SQLAUTH=1 SQLSERVER=SQL_SERVER_INSTANCE  QLUSER=SQL_USER SQLPWD=SQL_PASSWORD
WEB=0 ENGINE=0 AUDIT=0
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
CxSetup.exe /install /quiet
ACCEPT_EULA=Y
INSTALLFOLDER=”C:\Program Files\Checkmarx”
LIC=C:\LIC\license.cxl
INSTALLSHORTCUTS=0
CX_JAVA_HOME="C:\"Program Files\Java\jre1.8.0_241"
BI=0
MANAGER=1
ACTIVEMQ=0
SQLAUTH=1
SQLSERVER=SQL_SERVER_INSTANCE
SQLUSER=SQL_USER
SQLPWD=SQL_PASSWORD
WEB=0
ENGINE=0
AUDIT=0
```

➢ **To install CxManager to a default location using SQL authentication**

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y INSTALLFOLDER=”C:\Program
Files\Checkmarx” LIC=C:\LIC\license.cxl INSTALLSHORTCUTS=0
CX_JAVA_HOME="C:\"Program Files\Java\jre1.8.0_241" BI=0 MANAGER=1 ACTIVEMQ=0
SQLAUTH=1 SQLSERVER=SQL_SERVER_INSTANCE SQLUSER=SQL_USER SQLPWD=SQL_PASSWORD
WEB=0 ENGINE=0 AUDIT=0
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
CxSetup.exe /install /quiet
ACCEPT_EULA=Y
INSTALLFOLDER=”C:\Program Files\Checkmarx”
LIC=C:\LIC\license.cxl
INSTALLSHORTCUTS=0
CX_JAVA_HOME="C:\"Program Files\Java\jre1.8.0_241"
BI=0
MANAGER=1
ACTIVEMQ=0
SQLAUTH=1
SQLSERVER=SQL_SERVER_INSTANCE
SQLUSER=SQL_USER
SQLPWD=SQL_PASSWORD
WEB=0
ENGINE=0
AUDIT=0
```

- Access Control installs together with CxManager as both components must reside on the same host.
- For a table of parameters with additional information on them, refer to the Parameter page.

Installing ActiveMQ

The second component to install in this sequence is ActiveMQ.

Prerequisites

The required prerequisites are listed below. For further information and instructions on installing and making them available, refer to Preparing for Installation.

- MS SQL
- Java 1.8 64-bit

- Java installation should be located 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**.
- 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 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 (v9.3.0)
- If you perform a silent installation in a Distributed environment, you cannot stop the installation before it is complete.
- To properly configure the setup, you have to return to the CxManager installation and run **Reconfigure** as explained there.

Installing ActiveMQ

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y INSTALLFOLDER=”C:\Program
Files\Checkmarx” INSTALLSHORTCUTS=0 CX_JAVA_HOME="C:\"Program
Files\Java\jre1.8.0_241" BI=0 MANAGER=0 ACTIVEMQ=1 SQLAUTH=1
SQLSERVER=SQL_SERVER_INSTANCE SQLUSER=SQL_USER SQLPWD=SQL_PASSWORD WEB=0
ENGINE=0 AUDIT=0
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
CxSetup.exe /install /quiet
ACCEPT_EULA=Y
INSTALLFOLDER=”C:\Program Files\Checkmarx”
INSTALLSHORTCUTS=0
CX_JAVA_HOME="C:\"Program Files\Java\jre1.8.0_241"
BI=0
MANAGER=0
ACTIVEMQ=1
SQLAUTH=1
SQLSERVER=SQL_SERVER_INSTANCE
SQLUSER=SQL_USER
SQLPWD=SQL_PASSWORD
WEB=0
ENGINE=0
AUDIT=0
```

Reconfiguring CxManager after Installing ActiveMQ

Before you continue, you have to run **Reconfigure** to update the Environment Variables for Access Control.

- Do not run **Reconfigure** before ActiveMQ has been installed.

```
CxSetup.exe /install /quiet RECONFIGURE_ACCESS_CONTROL=1
```

Access Control parameters can be viewed and edited via Environment Variables that are available under Windows Properties.

Installing the Web Portal

The third component to install in this sequence is the Web Portal. Once the Web Portal has been installed, you have to configure it.

You have to install the Web Portal before installing CxEngine as part of installing CxEngine is logging on to and registering the new engine via the web portal.

Prerequisites

The required prerequisites are listed below. For further information and instructions on installing and making them available, refer to Preparing for Installation.

- C++ Redist 2010
- IIS v7.0 (or higher)

If you perform a distributed installation as Silent CLI_Installation, you cannot stop the installation before it is complete and you have to run **Reconfigure** to properly configure the setup once it has been installed.

Installing the Web Portal

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y INSTALLFOLDER=”C:\Program
Files\Checkmarx” INSTALLSHORTCUTS=0 BI=0 MANAGER=0
ACTIVEMQ=0 SQLAUTH=0 WEB=1 ENGINE=0 AUDIT=0
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
CxSetup.exe /install /quiet
ACCEPT_EULA=Y
INSTALLFOLDER=”C:\Program Files\Checkmarx”
INSTALLSHORTCUTS=0
BI=0
MANAGER=0
ACTIVEMQ=0
SQLAUTH=0
WEB=1
ENGINE=0
AUDIT=0
```

Installing the CxEngine Server

The fourth and final component to install in this sequence is the CxEngine Server.

Prerequisites

The required prerequisites are listed below. For further information and instructions on installing and making them available, refer to Preparing for Installation.

- C++ Redist 2010 and 2015 SP3
- ASP.NET Core 2.1.16 Hosting Bundle

If you perform a distributed installation as Silent CLI_Installation, you cannot stop the installation before it is complete and you have to run **Reconfigure** to properly configure the setup once it has been installed.

Installing the CxEngine

- Enter or copy the syntax into the CLI interface without forced line breaks:

```
CxSetup.exe /install /quiet ACCEPT_EULA=Y INSTALLFOLDER=”C:\Program
Files\Checkmarx” INSTALLSHORTCUTS=0 BI=0 MANAGER=0 WEB=0 ENGINE=1 AUDIT=0
```

The syntax is illustrated below with forced line breaks to show the required content and parameters. Do not copy the syntax with forced line breaks, otherwise, errors are returned.

```
CxSetup.exe /install /quiet
ACCEPT_EULA=Y
INSTALLFOLDER=”C:\Program Files\Checkmarx”
INSTALLSHORTCUTS=0
BI=0
MANAGER=0
WEB=0
ENGINE=1
AUDIT=0
```

Reconfiguring the CxEngine Parameters

For information and instructions on reconfiguring the CxEngine parameters, refer to Reconfiguring CxEngine.

Parameters for Installing CxSAST in Silent Mode

The table below displays all parameters and variables for silent installation of CxSAST in Centralized and Distributed environment.

Parameter	Settings	Description
/?		Opens the help dialog.
/install /uninstall /quiet		Installs or uninstalls CxSAST silently (Install is the default). Displays no GUI and no prompts. By default, GUI and all prompts are displayed. If you only enter /install or /uninstall, the relevant wizard starts in GUI mode.
ACCEPT_EULA=	**Y**: Accept **N**: Don't accept (default)	Sets the EULA (End User License Agreement) variable. Must be set to Y to run the installation. If you keep ACCEPT_EULA=N, the installation does not proceed.
CX_JAVA_HOME=	Path to the JRE folder	For example **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=	Folder where the installation files reside	For example **INSTALLFOLDER=”D:\TEMP DIR”**, **INSTALLFOLDER=D:\TEMP**. "**INSTALLFOLDER=D:\**" is supported.
MANAGER=	1: Install (default) **0**: Remove/do not install	Sets the Manager component variable: If CxManager is installed, Access Control is installed automatically as well.
WEB=	**1**: Install (default) **0**: Remove/do not install	Sets the Web component variable.

Parameter	Settings	Description
ENGINE=	**1**: Install (default) **0**: Remove/do not install	Sets the Engine component variable
AUDIT=	**1**: Install (default) **0**: Remove/do not install	Sets Audit component variable.
BI=	**1**: Install (default) **0**: Remove\do not install	Sets the BI component (CxARM) variable.
ACCESSCONTROL=	**1**: Install (default) **0**: Remove\do not install	Sets the Access Control component variable. Access Control must be installed on the same host as CxManager and ACCESSCONTROL must be set to 1.
VALIDATED_ACCESSCONTROL_MIGRATION=	**Y**: Yes **N**: No	Sets the Access Control Migration manual validation.
ACTIVEMQ=	**1**: Install (default) **0**: Remove\do not not install	Sets Active MQ component variable.
INSTALLSHORTCUTS=	**1**: Install shortcuts (default) **0**: Do not install shortcuts	Sets application shortcuts variable.
SQLAUTH=	**1**: Windows authentication (default) **0**: SQL authentication	Sets the SQL authentication mode for CxSAST: When SQLAUTH=1, the SQLUSER and SQLPWD settings are ignored.
SQLSERVER=	server location	Sets the SQL server address and instance for CxSAST (e.g. SQLSERVER= localhost\SQLEXPRESS)
SQLUSER=	user name	Sets the SQL user credential for CxSAST (e.g. SQLUSER=sa)
SQLPWD=	password	Sets the SQL password credential for CxSAST (e.g. SQLPWD=12345) The SQL passwords may consist of up to 32 characters.
CXSAST_ADDRESS=	**http://localhost:80** (default)	Sets the CxSAST URL address. Also validates that the defined URL address is reachable.
MQHTTPPORT=	**61616** (default)	Sets the MQ Admin console port definition.
MQMANAGERHTTPPORT=	**8161** (default)	Sets the MQ operational port definition.
RIHTTPPORT=	**8082** (default)	Sets the Remediation Intelligence port definition.
TOMCATHTTPPORT=	**8080** (default)	Sets the Apache Tomcat HTTP port definition.
TOMCATHTTPSPORT=	**8443** (default)	Sets the Apache Tomcat HTTPS port definition .
CXARM_SQLAUTH=	**0**: Windows authentication (default) **1**: SQL authentication	Sets the SQL authentication mode for CxARM. If **SQLAUTH=0**, the CXARM_DB_USER and CXARM_DB_PASSWORD settings are ignored.
CXARM_DB_HOST=	location	Sets the SQL server address and instance for CxARM (e.g. CXARM_DB_HOST=localhost\SQLEXPRESS)
CXARM_DB_USER=	user name	Sets the SQL user credential for CxARM (e.g. CXARM_DB_USER=sa)
CXARM_DB_PASSWORD=	password	Sets the SQL password credential for CxARM (e.g. CXARM_DB_PASSWORD=12345)
LIC=	The path to the license file	Sets the license path (e.g. LIC="C:\Users\Administrator\Documents\license.cxl"). If the license check fails, the license will not be installed.

Parameter	Settings	Description
		The license can also be installed manually once the installation is complete.
PORT=	**8081** (default for Access Control) **80** (default for CxSAST)	Sets the port definition.
ENGINE_TLS_ENABLE=	**true**: TLS enabled **false**: TLS disabled (default)	Enables/disables the encryption protocol TLS. If set to true, TLS is enabled and additional manual configuration is required. Set ENGINE_TLS_ENABLE=true and manually configure TLS once the installation is complete.
ENGINE_SERVICE_END_POINT=	**http://<fqdn>:8088** (default)	URL of the CxEngine host. This URL contains the following components: http://<engine name>.<location.domain>:<port number>and could be for example something like http://engine1.checkmarx.com:8088
ENGINE_HTTP_PORT=	**8088** (default)	Sets the port used by CxEngine.
ENGINE_SETTINGS_FILE=	The path to the engine settings file (JSON)	Sets the path to the JSON file.
ENGINE_FIREWALL_RULE=	**1**: Enabled (firewall rules apply) **0**: Disabled	Defines whether firewall rules apply.
ENGINE_CERTIFICATE_SUBJECT_NAME=	**CN=CxEngine** (default)	Defines name of the certificate for the TLS engine..
ENGINE_MESSAGE_QUEUE_DISABLE=	**None** (default)	Defines the engine message queue.
ENGINE_MESSAGE_QUEUE_TTL=	**60** (default)	Sets the TTL of the message queue.
ENGINE_EA_ENABLED_QUEUES=	**ResultQueue;IncrementalFilesQueue** (default)	Defines the Engine EA enabled queues.
ENGINE_EA_PUBLISHING_METHOD=	**MessageQueue** (default)	Defines the method of publishing scan results.
RECONFIGURE_ENGINE=	**1**: Reconfigure CxEngine	Reconfigures CxEngine. For additional customized ENGINE parameters, refer to Reconfiguring Access Control and CxEngine.
RECONFIGURE_ACCESS_CONTROL=	**1**: Reconfigure Access Control	Reconfigures Access Control related environment variables. For additional information on reconfiguring Access Control, refer to Reconfiguring Access Control and CxEngine.

- The default silent installation command is **<Path-To-Installer-File> /install /quiet**
- By default most options and components are set to 1 (enabled).
- 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 in Silent mode, do not change the existing port settings or the application will not function properly. You may change port settings once the upgrade is complete.

Reconfiguring Access Control and CxEngine

Environment variables can be reconfigured either by using the Reconfigure command or by entering the Environment Variables section under Windows Properties. Some parameters can be configured either via **Silent Reconfigure** or via the Environment Variables. In addition, the Environment Variables include parameters that are not related to **Reconfigure** such as the hostname and the IP address of the relevant host, and database parameters such as **TLS**.

Once you install **ActiveMQ**, you have to reconfigure Access Control as mentioned here. In addition, you may reconfigure the CxEngine parameters as mentioned here.

Reconfiguring Access Control

Once you complete installing ActiveMQ, you have to return to the CxManager installation and run Reconfigure to update Access Control.

To reconfigure Access Control, run the following command:

```
CxSetup.exe /install /quiet RECONFIGURE_ACCESS_CONTROL=1
```

Access Control parameters can be viewed and edited via Environment Variables that are available under **Windows Properties**.

Configuring CxEngine

After installing the CxEngine, you have to run Reconfigure to set the CxEngine parameters as illustrated and explained below. These parameters are available as Environment Variables for editing from the Windows Properties once they are set.

To rset the CxEngine parameters to the default parameters, run the following command:

```
CxSetup.exe /install /quiet RECONFIGURE_ENGINE=1
```

The default settings can be viewed in the Reconfigure Parameter table below.

To reconfigure selected settings to customized parameters and leave the remaining parameters at their default:

Use the syntax to reconfigure the CxEngine parameters to their default and list the ENGINE parameters with a different setting than the default. The example below illustrates setting the Engine settings to default, but with **TLS** enabled, which is disabled by default.

```
CxSetup.exe /install /quiet
RECONFIGURE_ENGINE=1

ENGINE_TLS_ENABLE=true
```

To reconfigure all settings to customized parameters:

Use the syntax and list all ENGINE settings with their parameter settings as illustrated below. For this option, **RECONFIGURE_ENGINE** must be set to **0** and all ENGINE parameters must be listed.

```
CxSetup.exe /install /quiet
RECONFIGURE_ENGINE=0

ENGINE_SERVICE_END_POINT=http://<fqdn>:8080
ENGINE_HTTP_PORT=8080
ENGINE_TLS_ENABLE=false
ENGINE_SETTINGS_FILE=<path to the JSON file 'engineConfiguration.json'>
ENGINE_FIREWALL_RULE=1
ENGINE_CERTIFICATE_SUBJECT_NAME=CxEngine
ENGINE_MESSAGE_QUEUE_DISABLE=none
ENGINE_MESSAGE_QUEUE_TTL=60
ENGINE_EA_ENABLED_QUEUES=ResultQueue;IncrementalFilesQueue
ENGINE_PUBLISHING_METHOD=MessageQueue
```

- Errors in the URL such as an illegal port cause an error indication ⊗ and you cannot continue the process until the error is corrected.
- The CxEngine Server uses port 8080 by default. You can also use a different port, although it is not recommended.
- All the CxEngine Server environment variables can be viewed and edited in the Windows Properties once the engine is configured and running.

Parameter Overview

Some of the values can be found as well among the Environment Variables.

Parameter	Settings	Description
ENGINE=	**1**: Installs CxEngine (default) **0**: Remove or does not install CxEngine	Defines whether or not to install CxEngine.
ENGINE_SERVICE_ENDPOINT=	**http://localhost:8088** (default)	URL of the CxEngine host. It contains the following components: **http://<engine name>.<location.domain>:<port number>** and could be for example something like **http://engine1.checkmarx.com:8088**
ENGINE_HTTP_PORT=	**8088** (default)	The port used by CxEngine.
ENGINE_TLS_ENABLE=	**true** **false** (default)	Set **ENGINE_TLS_ENABLE=true** and manually configure TLS once the installation is complete.
ENGINE_SETTINGS_FILE=	Location of **engineConfiguration.json**	This file has to be generated on the CxManager host and copied to the CxEngine host as follows: On the host with CxManager installed, open the file explorer and navigate to the installation folder, for example **C:\Program Files** and from there to **..\Checkmarx\Tools\Engine Configuration Exporter**. Run **EngineConfigExporter.bat**. Two new folders are created, **Logs** and **Output**. The engine configuration file **engineConfiguration.json** is generated in the Output folder. Go to the Output folder and copy engineConfiguration.json to a location of your choice on the CxEngine station. Use the location of the JSON file for the Engine Settings file parameter, for example "C:\Users\<username>\config files\engineConfiguration.json"
ENGINE_FIREWALL_RULE=	**1**: The installer creates a new firewall inbound rule for the CxEngine port (default). **0**: No new rules are created. New needed firewall rules must be created manually.	Creates a firewall inbound rule for the CxEngine port, depending on the setting.
ENGINE_CERTIFICATE_SUBJECT_NAME=	**CN=CxEngine** (default)	The engine certificate subject name.
ENGINE_MESSAGE_QUEUE_DISABLE=	**none** (default)	States which queues are disabled for the EngineService.
ENGINE_MESSAGE_QUEUE_TTL=	**60**	TTL = Time To Live The max. lifetime (in seconds) of the message in the message queue.
ENGINE_EA_ENABLED_QUEUES=	**ResultQueue;IncrementalFilesQueue**	
ENGINE_PUBLISHING_METHOD=	**MessageQueue**	Method of publishing scan results.

Common Use Cases

There are two commonly used scenarios for distributed installations:

- Installing ActiveMQ after installing CxManager
- Changing the host name of ActiveMQ

Installing ActiveMQ after CxManager

- To install ActiveMQ after CxManager, refer to Installing ActiveMQ.
- Return to the host with CxManager installed.
- Reconfigure Access Control as explained under Installing CxManager.

Changing the Host Name of ActiveMQ

- After changing the host name of ActiveMQ, you have to reconfigure both the Access Control and CxEngine as explained above.

CxSAST Environment Variables

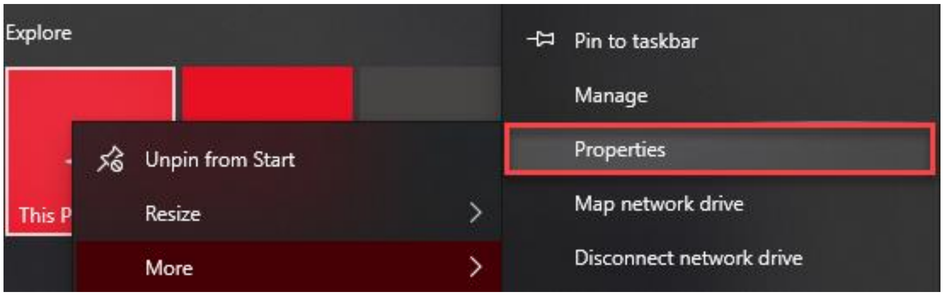
Starting with CxSAST v9.3.0, Access Control and CxEngine parameters in use are now available for viewing and editing via Environment Properties under Windows Properties. This approach provides an interface for reconfiguring Access Control and CxEngine parameters at a later stage for users who wish to do so.

Change any of these settings for troubleshooting purposes only according to instructions from Technical Support.

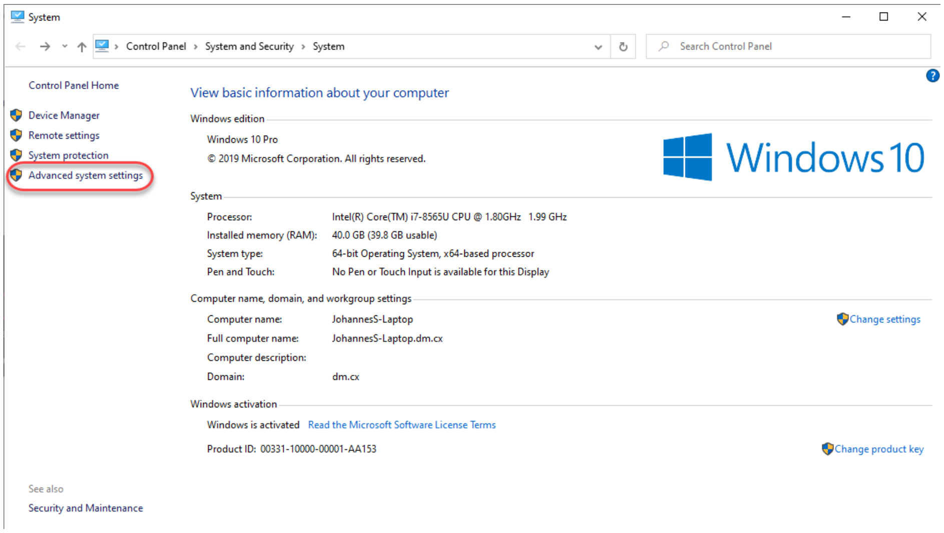
Accessing Environment Variables

➢ **To access the Environment Variables under Windows Properties**

1. Right-click **This PC** and then navigate to **Properties** to open the **Control Panel**.



2. From the Control Panel, select **Advanced System Settings** to open the **System Properties**.



View basic information about your computer

Windows edition

Windows 10 Pro

© 2019 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz 1.99 GHz
Installed memory (RAM):	40.0 GB (39.8 GB usable)
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

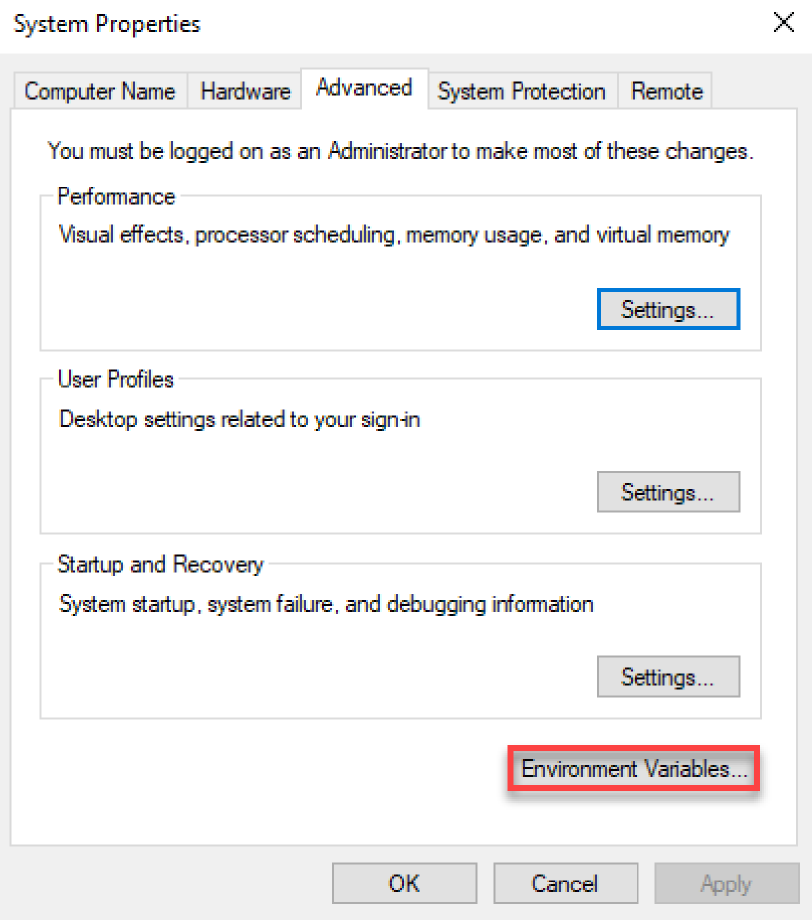
Computer name:	JohannesS-Laptop
Full computer name:	JohannesS-Laptop.dm.cx
Computer description:	
Domain:	dm.cx

Windows activation

Windows is activated Read the Microsoft Software License Terms

Product ID: 00331-10000-00001-AA153

3. From the System Properties page, enter **Environment Variables** and display system variables.



You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

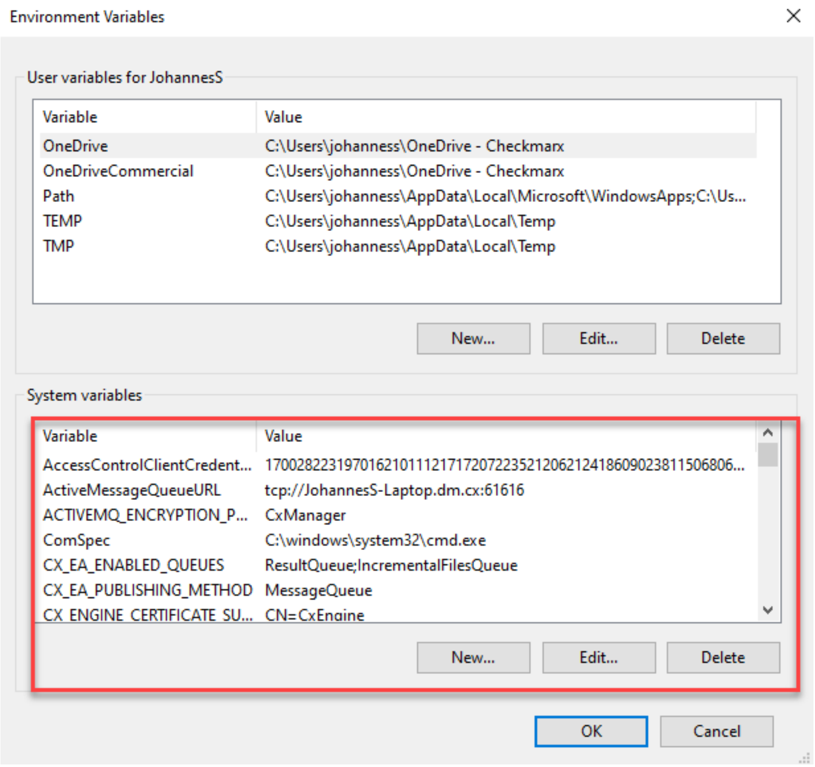
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

4. To add, delete, or edit system variables use the relevant buttons, and follow the onscreen instructions.



Environment Variables

User variables for JohannesS

Variable	Value
OneDrive	C:\Users\johannes\OneDrive - Checkmarx
OneDriveCommercial	C:\Users\johannes\OneDrive - Checkmarx
Path	C:\Users\johannes\AppData\Local\Microsoft\WindowsApps;C:\Us...
TEMP	C:\Users\johannes\AppData\Local\Temp
TMP	C:\Users\johannes\AppData\Local\Temp

System variables

Variable	Value
AccessControlClientCredent...	17002822319701621011121717207223521206212418609023811506806...
ActiveMessageQueueURL	tcp://JohannesS-Laptop.dm.cx:61616
ACTIVEMQ_ENCRYPTION_P...	CxManager
ComSpec	C:\windows\system32\cmd.exe
CX_EA_ENABLED_QUEUES	ResultQueue;IncrementalFilesQueue
CX_EA_PUBLISHING_METHOD	MessageQueue
CX_ENGINE_CERTIFICATE_SU...	CN=CxEngine

List of Available Environment Variables

The table below lists all Access Control and CxEngine system environment variables relevant for CxSAST. In addition, it lists available options and briefly explains each variable.

Variable	Default Settings	Description and Settings
Access Control		
Database__Type	**MsSql**	The only database format supported at present is Microsoft’s SQL Server.
Database__ConnectionString	**Data Source=localhost\SQLEXPRESS;Initial Catalog=CxDB;Integrated Security=True;Password=** **Data Source=localhost\SQLEXPRESS;Initial Catalog=CxDB;Integrated Security=False;User ID=test;Password="dRWVg0cv2wR+4PI9OSuJww==";Pooling=True**	Displays the path to the database, the database catalog and the password that you have to add in order to connect seamlessly.
Database__ConnectionStringHash		The encryption key for the entire CxSAST application.
Database__ConnectionStringSalt		Additional parameter (Salt) for encryption.
ActiveMessageQueueURL	**tcp://localhost:61616**	The location where CxSAST messages are stored.
MessageQueueUsername	**cxuser**	User name.

Variable	Default Settings	Description and Settings
MessageQueuePassword	**158219190118106154183187084097247236091137123199**	Password (encrypted).
AccessControlClientCredentialsSecret	**1082431311900690982130280271381240971521242370162021902221481160351912002360861390070040191410011782070310412191971430**On the Cx Web Portal server**072042131037132230220034**	Security key for encryption.
CxEngine		
CX_ENGINE_PORT	**8088**	The port used by CxEngine.
CX_ENGINE_TLS_ENABLE	**false**	Set ENGINE_TLS_ENABLE=true and manually configure TLS once the installation is complete.
CX_ENGINE_CERTIFICATE_SUBJECT_NAME	**CN=CxEngine**	Name of the certificate for the TLS engine. Make sure that this variable is added, if you intend to use TLS.
CX_ES_MESSAGE_QUEUE_TTL	**60**	TTL = Time To Live The max. lifetime (in seconds) of the message in the message queue.
CX_EA_ENABLED_QUEUES	**ResultQueue;IncrementalFilesQueue**	
CX_EA_PUBLISHING_METHOD	**MessageQueue**	Method of publishing scan results.
CX_ES_END_POINT	**http://localhost:8088**	URL of the CxEngine host. This URL contains the following components: http://<engine name>.<location.domain>:<port number>and could be for example something like http://engine1.checkmarx.com:8088
CX_ES_MESSAGE_QUEUE_URL	**tcp://localhost:61616**	The location where CxSAST messages are stored.
CX_ES_MESSAGE_QUEUE_USERNAME	**cxuser**	User name
CX_ES_MESSAGE_QUEUE_PASSWORD	**158219190118106154183187084097247236091137123199**	Password (encrypted)
CX_ES_ACCESS_CONTROL_URL	**http://localhost/CxRestAPI/auth**	The location of the Access Control server.
SCANS_PARENT_PATH		
CX_ES_ENGINE_WORKER_PATH	**C:\Program Files\Checkmarx\Checkmarx Engine Service\Engine Server**	The full path of the CxEngine server folder
CX_ES_ENGINE_WORKER_RELATIVE_PATH	**Engine Server**	Relative path to the CxEngine server folder. Effective only, if CX_ES_ENGINE_WORKER_PATH is not set, or the path does not exist.
CX_ES_ENGINE_SCANS_PARENT_PATH	**C:\EngineServiceScans**	The location of the engine scan logs
CX_VERSION	**9.3.0.248**	The product version.

Variable	Default Settings	Description and Settings
CX_JAVA_HOME	**C:\Program Files\Java\jdk1.8.0_241**	The path to the Java JRE.
CX_ES_MESSAGE_QUEUE_DISABLE	none	States which queues are disabled for the EngineService.

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

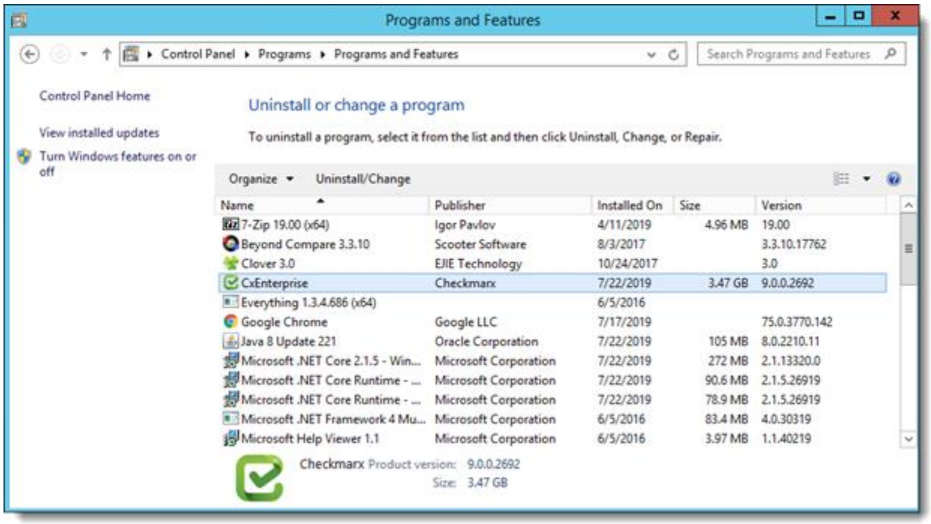
On a CxEngine host (if applicable):

- 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.



Programs and Features
Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize ▾
Uninstall/Change

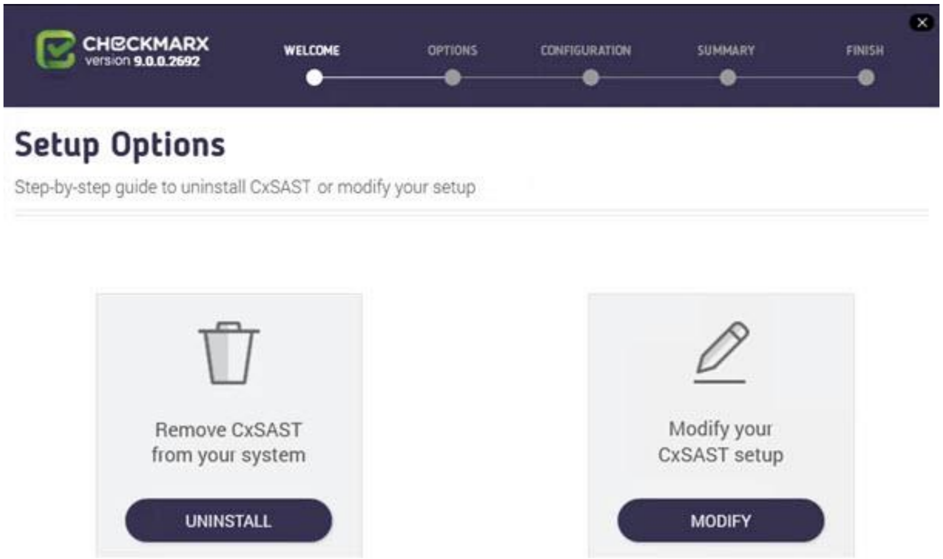
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
7-Zip 19.00 (x64)	Igor Pavlov	4/11/2019	4.96 MB	19.00
Beyond Compare 3.3.10	Scooter Software	8/3/2017		3.3.10.17762
Clover 3.0	EJIE Technology	10/24/2017		3.0
CxEnterprise	Checkmarx	7/22/2019	3.47 GB	9.0.0.2692
Everything 1.3.4.686 (x64)		6/5/2016		
Google Chrome	Google LLC	7/17/2019		75.0.3770.142
Java 8 Update 221	Oracle Corporation	7/22/2019	105 MB	8.0.2210.11
Microsoft .NET Core 2.1.5 - Win...	Microsoft Corporation	7/22/2019	272 MB	2.1.13320.0
Microsoft .NET Core Runtime - ...	Microsoft Corporation	7/22/2019	90.6 MB	2.1.5.26919
Microsoft .NET Core Runtime - ...	Microsoft Corporation	7/22/2019	78.9 MB	2.1.5.26919
Microsoft .NET Framework 4 Mu...	Microsoft Corporation	6/5/2016	83.4 MB	4.0.30319
Microsoft Help Viewer 1.1	Microsoft Corporation	6/5/2016	3.97 MB	1.1.40219

Checkmarx Product version: 9.0.0.2692
Size: 3.47 GB

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



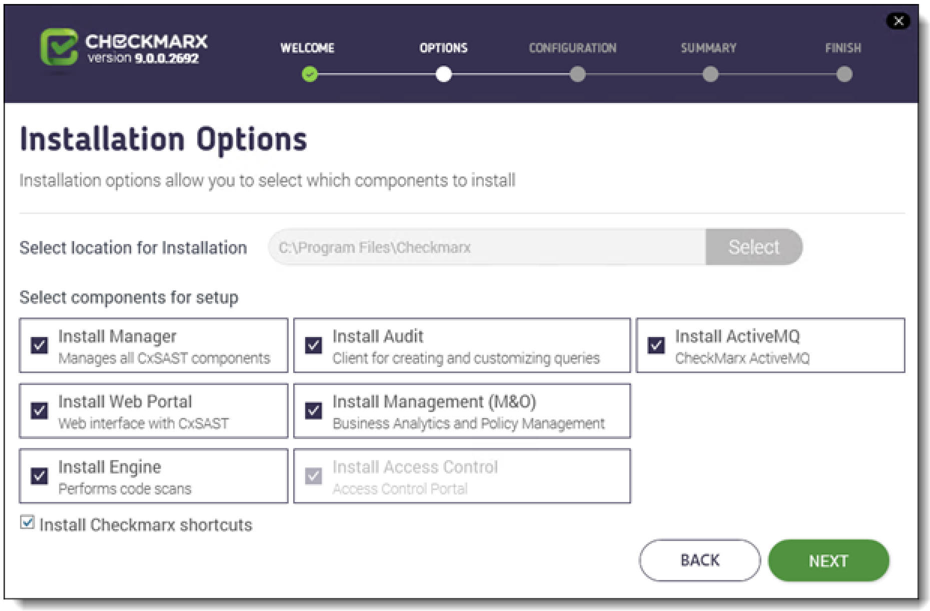
Setup Options

Step-by-step guide to uninstall CxSAST or modify your setup

Remove CxSAST from your system

Modify your CxSAST setup

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



Installation Options

Installation options allow you to select which components to install

Select location for Installation: C:\Program Files\Checkmarx

Select components for setup

☑ Install Manager – Manages all CxSAST components

☑ Install Audit – Client for creating and customizing queries

☑ Install ActiveMQ – CheckMarx ActiveMQ

☑ Install Web Portal – Web interface with CxSAST

☑ Install Management (M&O) – Business Analytics and Policy Management

☑ Install Engine – Performs code scans

☑ Install Access Control – Access Control Portal

☑ Install Checkmarx shortcuts

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.

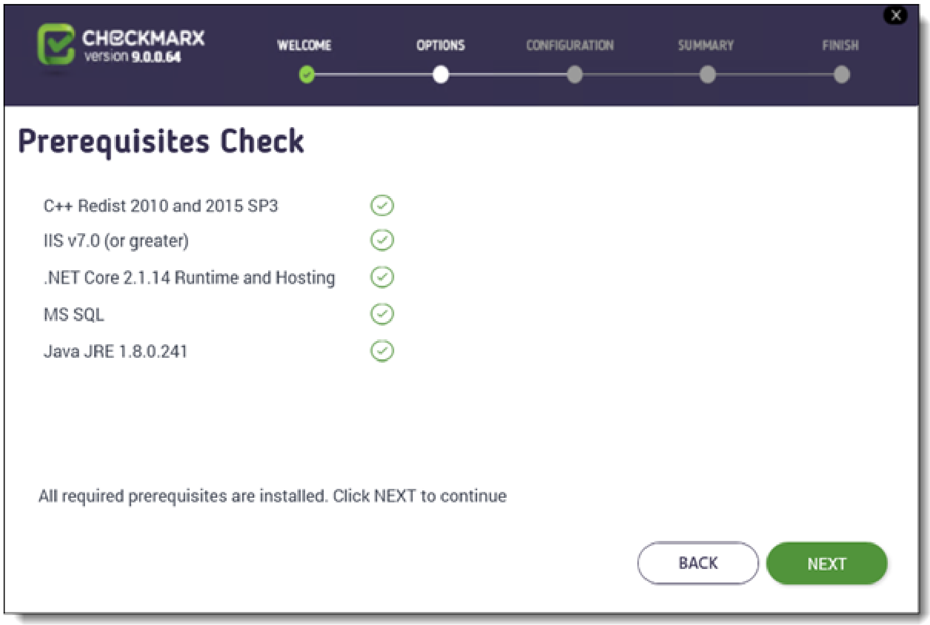
6. For any prerequisite component not yet installed (marked with ⚠), perform the following:

    - 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 should 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.

    - Click the Prerequisites Folder button to navigate to the supplied components and install each one separately.

7. After all missing prerequisite component(s) has been installed, click <**Recheck Prerequisites**> after making the necessary changes.

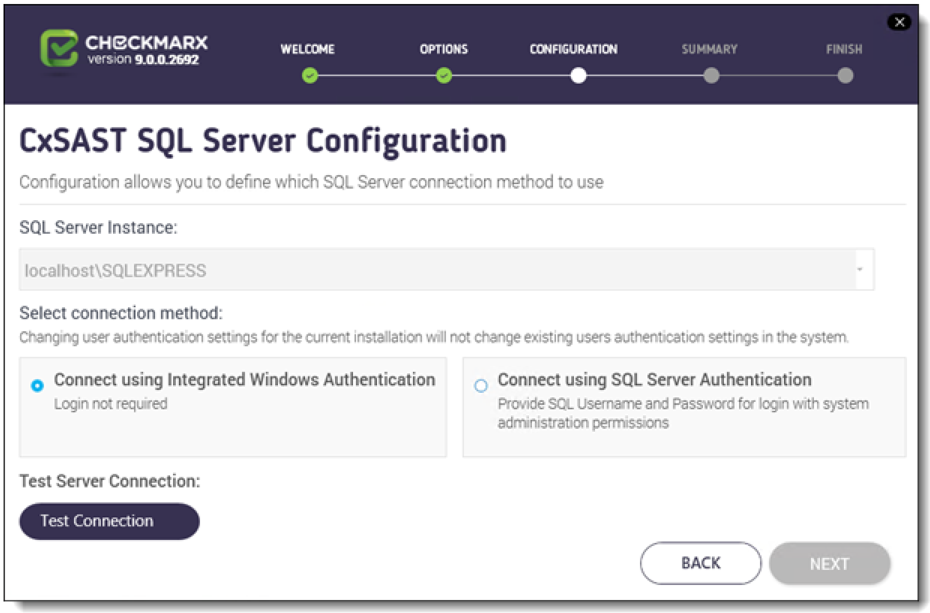


Prerequisites Check

C++ Redist 2010 and 2015 SP3 ✓
IIS v7.0 (or greater) ✓
.NET Core 2.1.14 Runtime and Hosting ✓
MS SQL ✓
Java JRE 1.8.0.241 ✓

All required prerequisites are installed. Click NEXT to continue

8. When all prerequisite components are installed, click <**NEXT**> to continue. The **CxSAST SQL Server Configuration** window is displayed.



CxSAST SQL Server Configuration

Configuration allows you to define which SQL Server connection method to use

SQL Server Instance:

localhost\SQLEXPRESS

Select connection method:

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

● Connect using Integrated Windows Authentication
Login not required

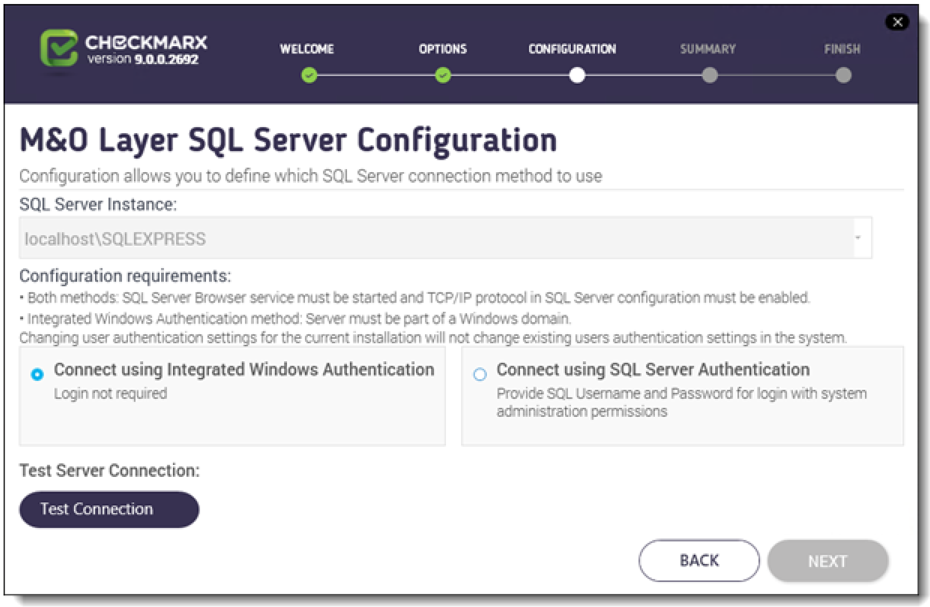
○ Connect using SQL Server Authentication
Provide SQL Username and Password for login with system administration permissions

Test Server Connection:

9. 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).
10. Click **<Test Connection>**. A "**Connection OK**" message is displayed upon confirmed connection to the CxSAST 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).

11. Click <**OK**> on the confirmation message, then click <**NEXT**>. The **M&O Layer SQL Server Configuration** window is displayed.



M&O Layer SQL Server Configuration

Configuration allows you to define which SQL Server connection method to use

SQL Server Instance:

localhost\SQLEXPRESS

Configuration requirements:

• Both methods: SQL Server Browser service must be started and TCP/IP protocol in SQL Server configuration must be enabled.

• Integrated Windows Authentication method: Server must be part of a Windows domain.

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

● Connect using Integrated Windows Authentication
Login not required

○ Connect using SQL Server Authentication
Provide SQL Username and Password for login with system administration permissions

Test Server Connection:

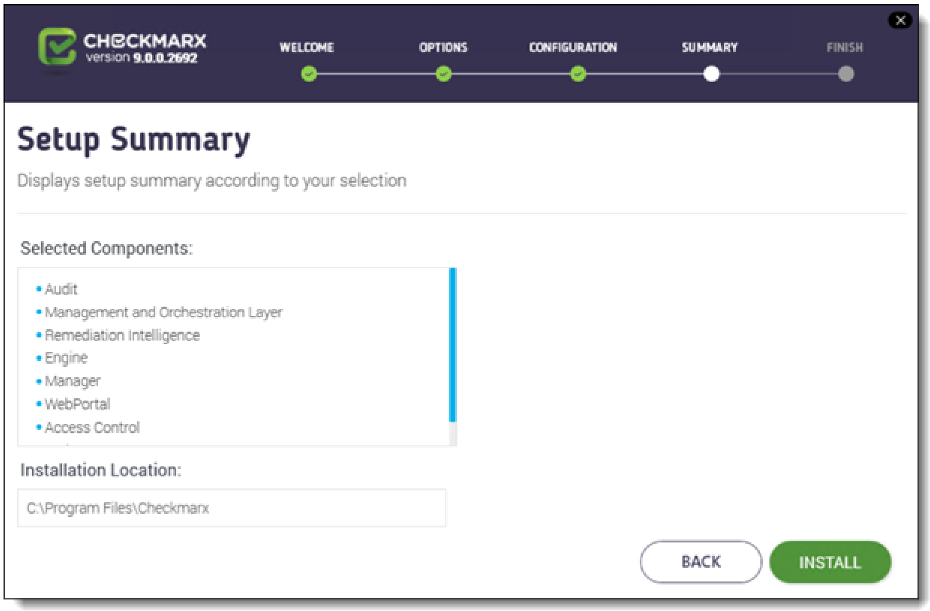
12. For **Management and Orchestration Layer,** define the SQL Server connection by selecting one of the following:
    - **Connect using Integrated Windows Authentication** (login not required)
    - **Connect using SQL Server Authentication** (provide SQL user name and password for login with SA permissions).

- 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**.

13. 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).

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



Setup Summary

Displays setup summary according to your selection

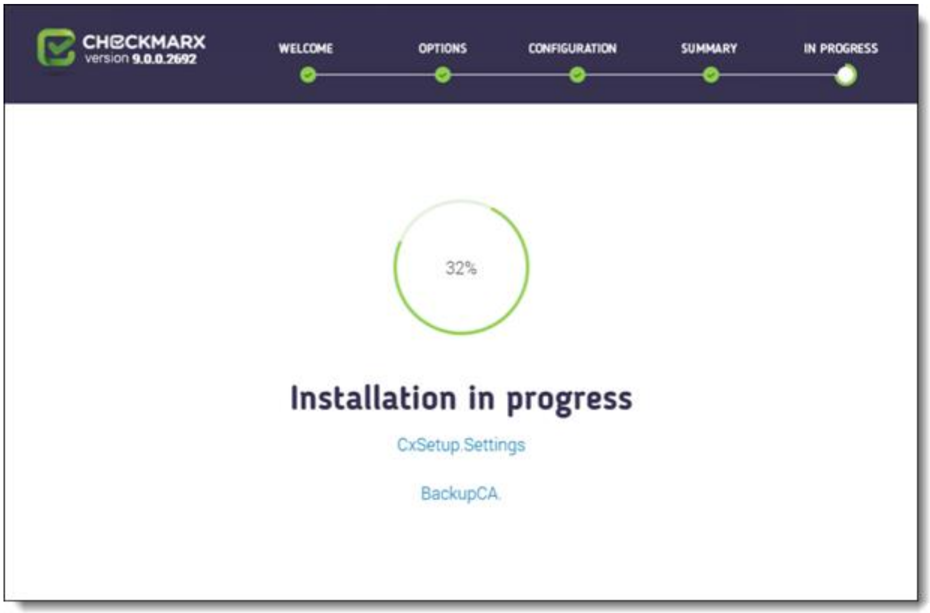
Selected Components:

- Audit
- Management and Orchestration Layer
- Remediation Intelligence
- Engine
- Manager
- WebPortal
- Access Control

Installation Location:

C:\Program Files\Checkmarx

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



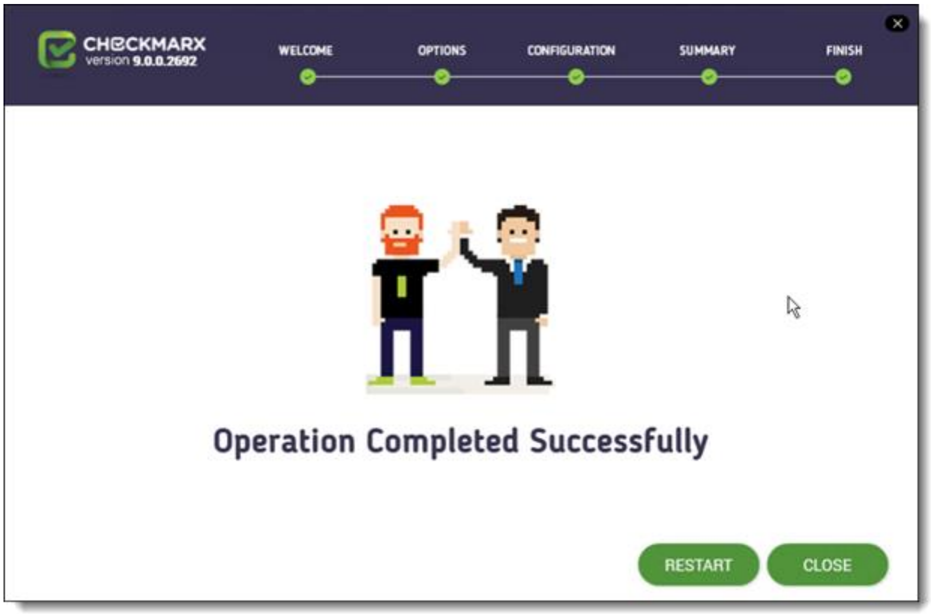
Installation in progress

CxSetup.Settings

BackupCA

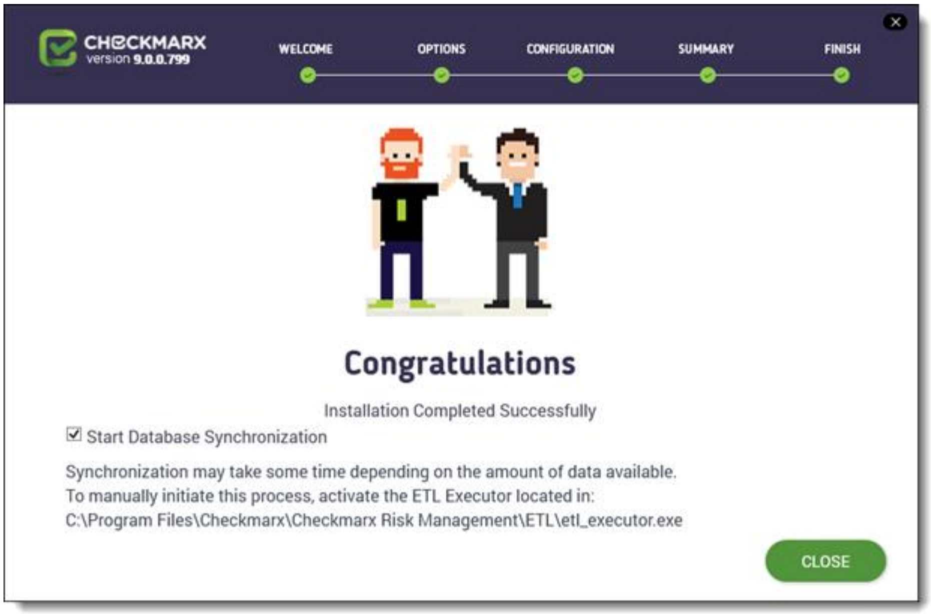
- If the installation fails, the "Setup failed" message is displayed. For more information, see the installation logs. If you need further assistance, please contact Checkmarx support.

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



Operation Completed Successfully

18. Click <**RESTART**> to complete the installation.
19. If part of the modification included selecting the Management and Orchestration component on the Congratulations window, the **Start Database Synchronization** window is displayed.



Congratulations

Installation Completed Successfully

☑ Start Database Synchronization

Synchronization may take some time depending on the amount of data available.
To manually initiate this process, activate the ETL Executor located in:
C:\Program Files\Checkmarx\Checkmarx Risk Management\ETL\etl_executor.exe

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

- **To continue now with the database synchronization**, leave the checkbox selected, and then click <**CLOSE**>. If required, reboot the server (you will receive a prompt if rebooting is necessary). The database synchronization process starts automatically.
- For more information about installing Management and Orchestration, see Installing Management and Orchestration.
- **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 re-installing, or reinstall with a new Management and Orchestration database.

20. 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 & 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.

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

If the Snapshots option is not available, 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. Backup 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

- Check that you have the CxSAST installation zip file for the current backed up version (can be requested from Checkmarx support).

6. 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) must be rebuilt, do the following:

1. Install CxSAST with same version as your backed up version to the same path as your former 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
4. Example: <Checkmarx Installation Path>\Checkmarx --> <Checkmarx Installation Path>\checkmarxNew01012016
5. Restore the Checkmarx folder
6. 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
7. Restore the database

   Restore the databases using the backup that you previously saved using the standard database tools.
8. Restore the scanned source folder,
9. Move the old scanned source folder that you previously saved back to the original folder location.

   Example: X:\CxSrc01012016 --> X:\CxSrc
10. 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

11. Check the recovered version
12. Perform a basic test on the restored installation to check that everything is up and running.
    - Login
    - View older scan results
    - Run a small new scan
    - View the new scan results

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

Upgrading CxSAST

This page applies only to full upgrades and not to hotfixes. CxSAST supports upgrades from up to the two previous versions.

- 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 v8.8 or v8.9, you have to first install v9.0 and only then proceed with installing v9.3. If you use an earlier version of CxSAST, contact Checkmarx Support before you start upgrading.
- Make sure that the SQL password does not exceed 32 characters.
- If you are switching Java versions, for example, due to upgrading or otherwise modifying your CxSAST installation in a way that 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.
- Some environment variables are renamed, but the names are not updated in the list of Environment Variables list. Therefore, you have to manually verify that the environment variable names match the respective listed ones. If they do not match, you have to manually update them under Windows Properties as explained once the upgrade is complete. Incompatible environment variable names cause CxSAST to fail.
- If you intend to use TLS,
  - follow the guide under Configuring SSL between CxManager and CxEngine v9.3.0 and verify the certificate's installation location as mentioned in the guide.
  - make sure to add **CX_ENGINE_CERTIFICATE_SUBJECT_NAME** as environment variable as explained, if it is not listed already.

Before you start:

1. Make sure there are currently no scans 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**: Stop Internet Information Services (IIS). To do so, open Internet Information Services (IIS) and click ■ Stop under Manage Server or open a command-line shell (CMD) as Administrator and enter "iisreset /stop".

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 **CxSetup.exe** on each server component host and perform the upgrade according to the Installing CxSAST procedure.
4. During the upgrade, the Checkmarx installer automatically performs a backup copy of configuration files. The Checkmarx backup files are located at **%appdata%\checkmarx** (usually **C:\Users\<user>\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 the 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.) must be upgraded individually.

5. 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: Stop Internet Information Services (IIS). To do so, open Internet Information Services (IIS) and click ■ **Stop** under **Manage Server** or open a command-line shell (CMD) as Administrator and enter "**iisreset /stop**".
     - 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 9.3, you have to reconnect the new engines using a different URL.**
  - The URL of the CxSAST engines until CxSAST 9.2 used to be http://{IP or FQDN}/CxSourceAnalyzerEngineWCF/CxEngineWebServices.svc
  - The new URL for the new engine for **CxSAST 9.3** and up is **http://{IP or FQDN}:{port}**.

6. 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, any non-default accounts for new CxSAST Services (CxSASTResults, CxRemidiationIntelligence, 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.

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.

Adding a CxEngine Server

This section explains how to install a CxEngine Server on a separate station. This can be as part of a distributed installation or simply to add an additional CxEngine server to an existing installation later on.

Workflow

If you add a CxEngine to an existing CxSAST system, pre-requisites are already in place. If you install CxEngine as part of a new distributed installation, you must install the components in the order outlined below. A distributed architecture refers to a scenario where the server components are 'distributed' over multiple dedicated servers and not installed all on the same server as explained here.

1. **Installing CxManager**. CxManager manages and integrates system components and contributes the JSON file with the engine settings that you need at a later stage.
2. **Installing and Configuring ActiveMQ**. The ActiveMQ manages the messaging queues and contributes the Message Queue parameters that are going to be loaded together with the engine configuration.

3. **Installing and Configuring the Web Portal**. Must be installed before installing CxEngine as part of installing CxEngine is logging on to and registering the new engine via the web portal.
4. **Installing CxEngine**. The CxEngine performs the code scans.

- When installing in Silent Mode, you have to use the Silent Reconfigure option to complete the installation. For further information, refer to Silent Installation.

When you install the CxEngine Server, you import the engine configuration settings stored in a JSON file that you retrieve from CxManager.

- If CxManager and ActiveMQ are not available to the CxEngine installation, the installation cannot complete.

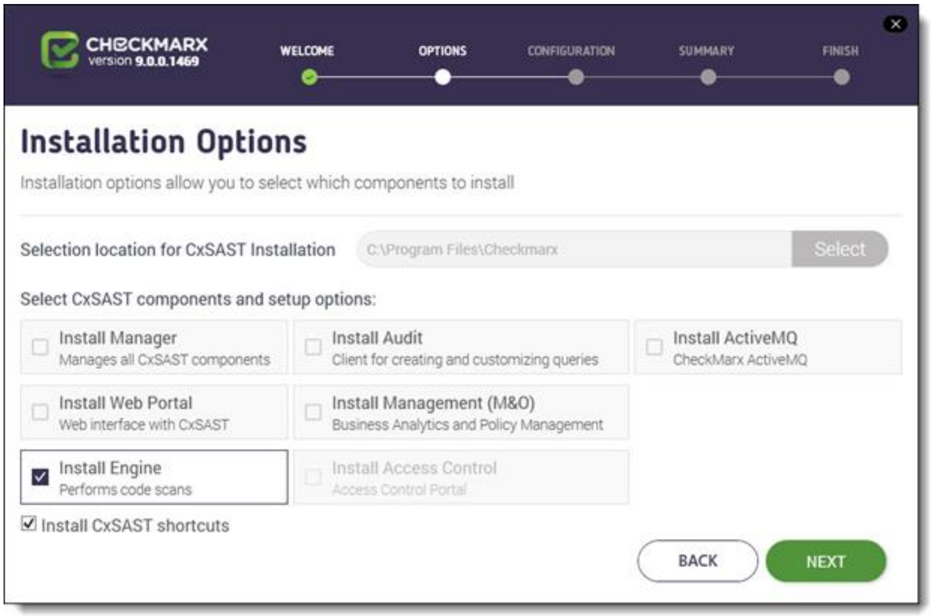
Installing the CxEngine Server

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

- Prepare the environment for the new CxEngine.
- Verify that the pre-requisites are in place and start the CxSAST installation. Once the Installation Options window is displayed, click Select to define the CxEngine installation location.

➢ **To start installing the CxEngine:**

1. Select **Install Engine** only.



Installation Options

Installation options allow you to select which components to install

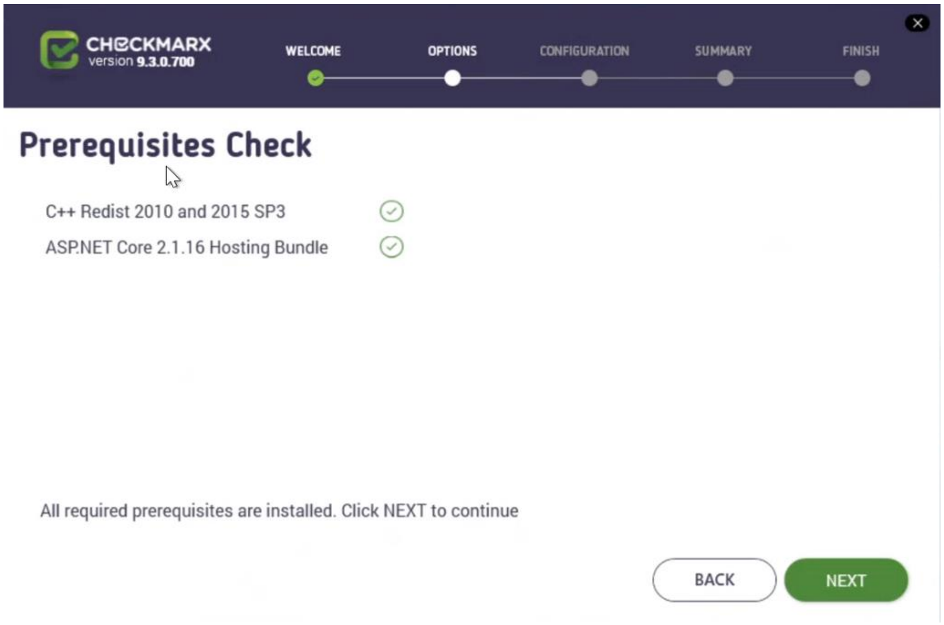
Selection location for CxSAST Installation: C:\Program Files\Checkmarx [Select]

Select CxSAST components and setup options:

□ Install Manager Manages all CxSAST components	□ Install Audit Client for creating and customizing queries	□ Install ActiveMQ CheckMarx ActiveMQ
□ Install Web Portal Web interface with CxSAST	□ Install Management (M&O) Business Analytics and Policy Management	
☑ Install Engine Performs code scans	□ Install Access Control Access Control Portal	

☑ Install CxSAST shortcuts

2. Click <**Next**> to continue. The **Prerequisites Check** window is displayed, showing the status of the required components to install the CxEngine server.



Prerequisites Check

C++ Redist 2010 and 2015 SP3 ✓

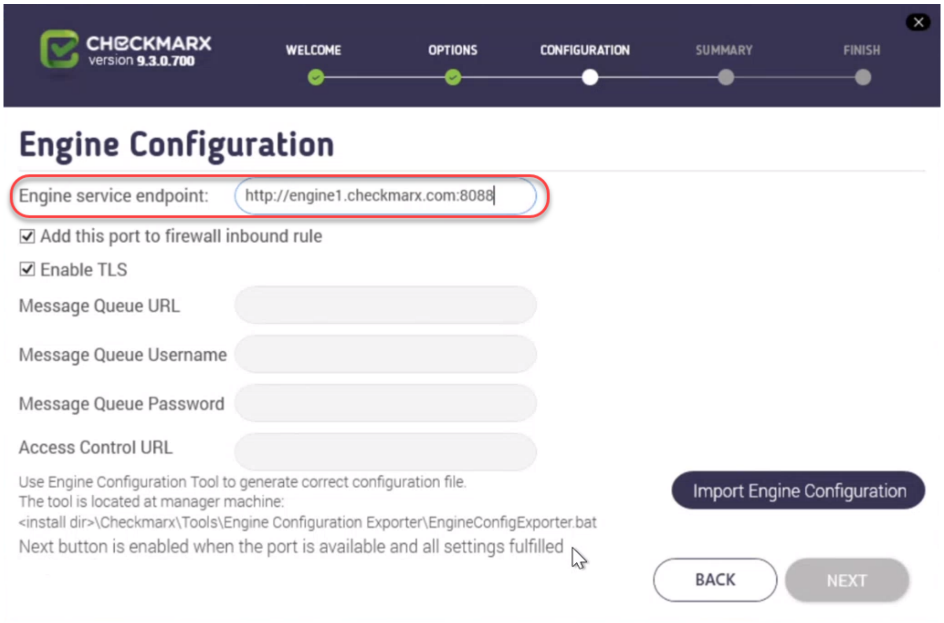
ASP.NET Core 2.1.16 Hosting Bundle ✓

All required prerequisites are installed. Click NEXT to continue

3. For any prerequisite component not installed, click <**Prerequisites Folder**> to browse for and install each missing prerequisite component.

   In addition to version 2010, the CxEngine Server requires C++ Redist Version 2015.

4. After the missing prerequisite component(s) have been installed, click <**Recheck Prerequisites**> to confirm the updated prerequisite status.
5. When all prerequisite components are installed, click <**Next**> to display the Engine Configuration window.



Engine Configuration

Engine service endpoint: http://engine1.checkmarx.com:8088

☑ Add this port to firewall inbound rule

☑ Enable TLS

Message Queue URL

Message Queue Username

Message Queue Password

Access Control URL

Use Engine Configuration Tool to generate correct configuration file.
The tool is located at manager machine:
<install dir>\Checkmarx\Tools\Engine Configuration Exporter\EngineConfigExporter.bat

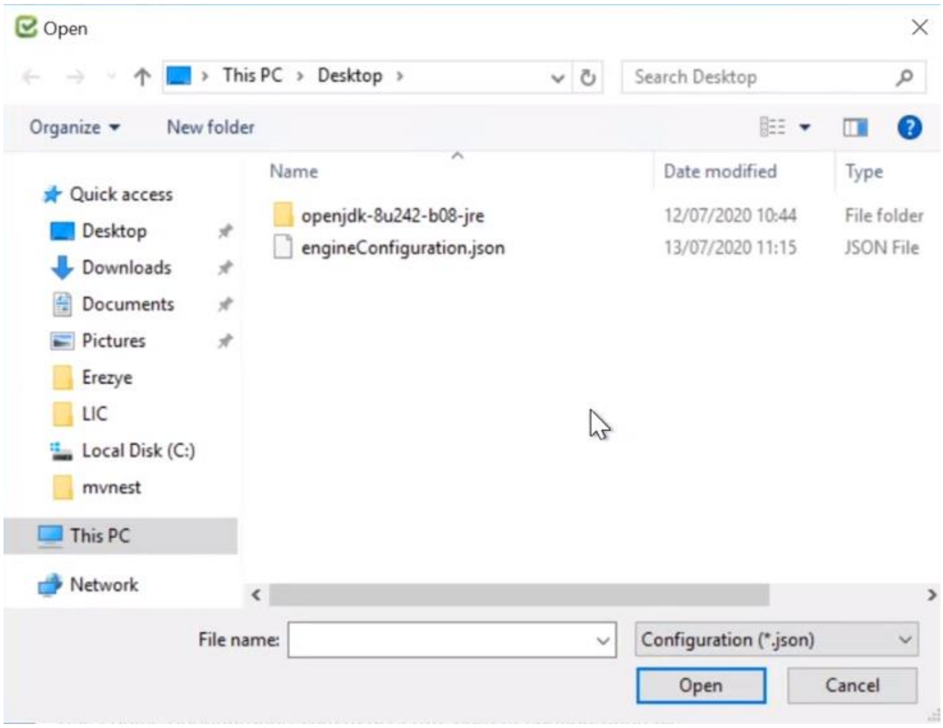
Next button is enabled when the port is available and all settings fulfilled

➢ **To set up the CxEngine:**

1. Enter the service endpoint URL in the **Engine Service Endpoint** field, which reads something like **http://<engine name>.<location.domain>:<port number>**, for example **http://engine1.checkmarx.com:8088**.

- Errors in the URL such as an illegal port result in an error indication ⊗ and you cannot continue the process until the error is corrected.
- The CxEngine Server uses port 8088 by default. You can also use a different port, although it is not recommended.
- All the CxEngine Server settings can be viewed and edited in the Windows Properties once the engine is configured and running.

2. To open the required port in the Windows firewall, check **Add this Port to Firewall Inbound Rule**.
3. To enable encryption via TLS, check **Enable TLS**.
4. On the host with CxManager installed, open the file explorer and navigate to the installation folder, for example **C:\Program Files** and from there to **..\Checkmarx\Tools\Engine Configuration Exporter**.
5. Run **EngineConfigExporter.bat**. Two new folders are created, **Logs** and **Output**. The engine configuration file **engineConfiguration.json** is generated in the Output folder.
6. Go to the Output folder and copy **engineConfiguration.json** to a location of your choice on the CxEngine station.
7. To invoke the engine parameters, click <Import Engine Configuration>. The file explorer opens.

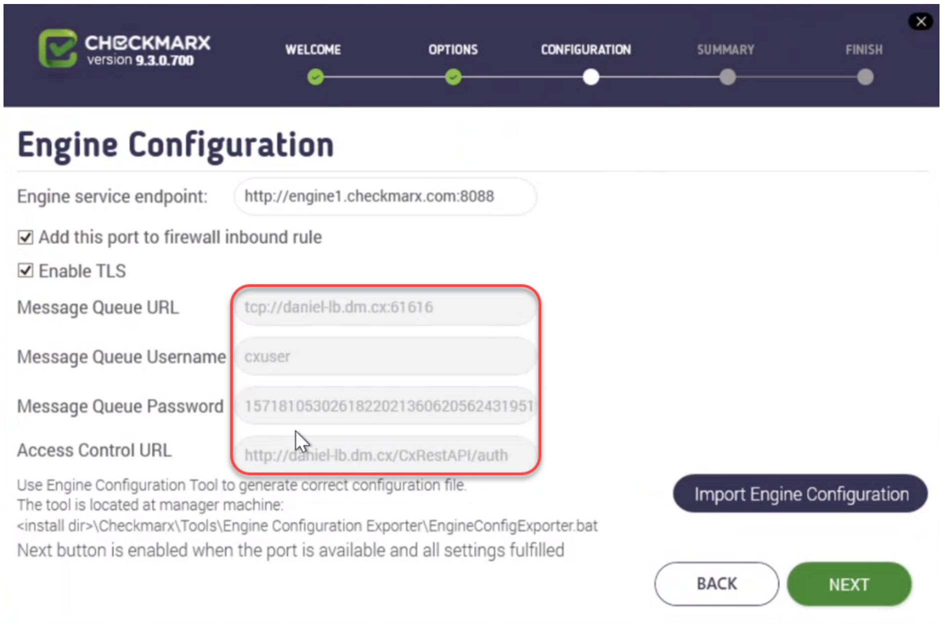


Name	Date modified	Type
openjdk-8u242-b08-jre	12/07/2020 10:44	File folder
engineConfiguration.json	13/07/2020 11:15	JSON File

File name:
Configuration (*.json)

8. Navigate to the file location **engineConfiguration.json** file's location and click <**Open**>. The Engine configuration is imported and displayed in the relevant fields of the Engine Configuration dialog box.

- The imported parameters cannot be entered or edited manually in the Engine Configuration dialog box.
- The engine configuration is available for editing as Windows Environment Variables. For additional information, refer to the relevant page.



Engine Configuration

Engine service endpoint: http://engine1.checkmarx.com:8088

☑ Add this port to firewall inbound rule

☑ Enable TLS

Message Queue URL: tcp://daniel-lb.dm.cx:61616

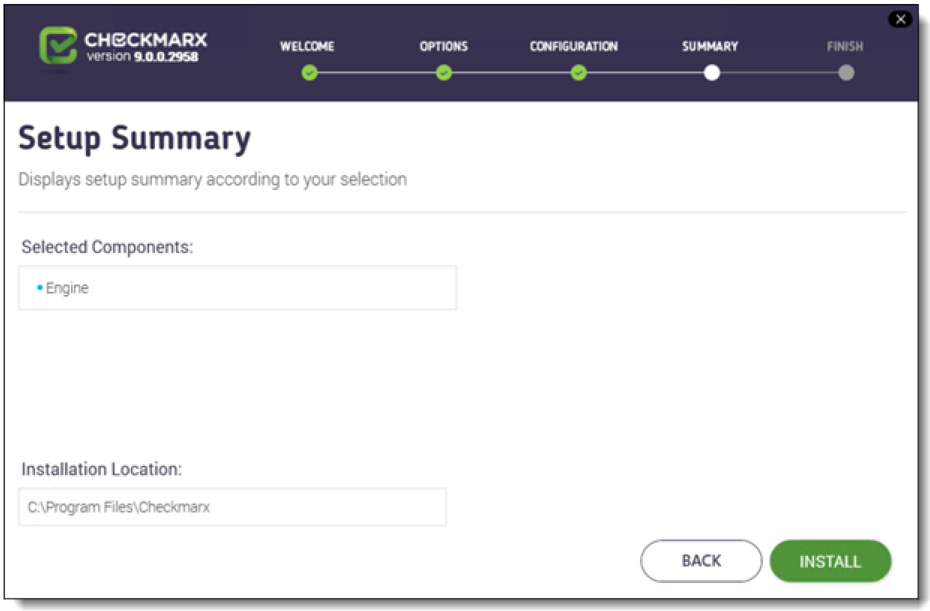
Message Queue Username: cxuser

Message Queue Password: 157181053026182202136062056243195

Access Control URL: http://daniel-lb.dm.cx/CxRestAPI/auth

Use Engine Configuration Tool to generate correct configuration file.
The tool is located at manager machine:
<install dir>\Checkmarx\Tools\Engine Configuration Exporter\EngineConfigExporter.bat
Next button is enabled when the port is available and all settings fulfilled

9. Click <**Next**>. The **Setup Summary** window is displayed.



Setup Summary

Displays setup summary according to your selection

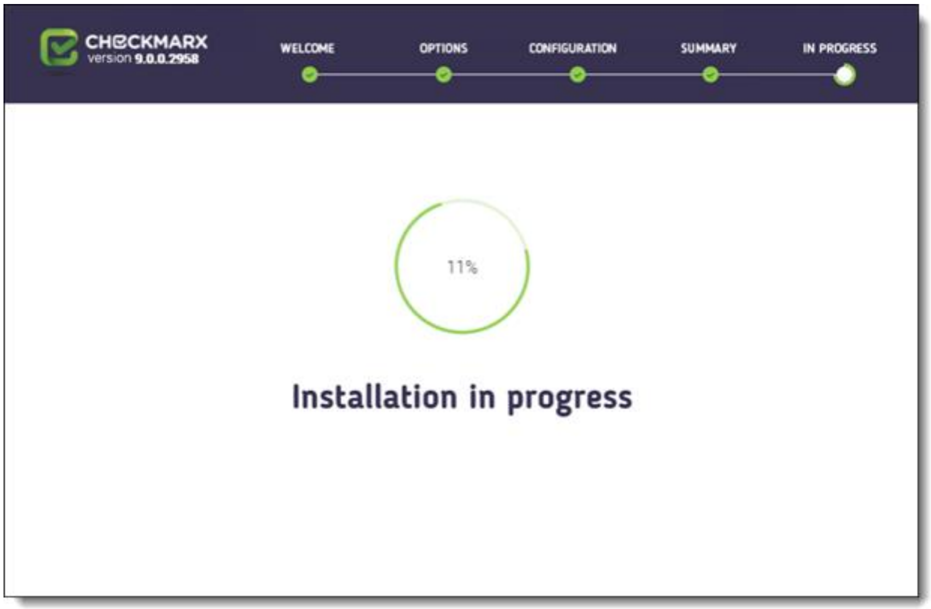
Selected Components:

- Engine

Installation Location:

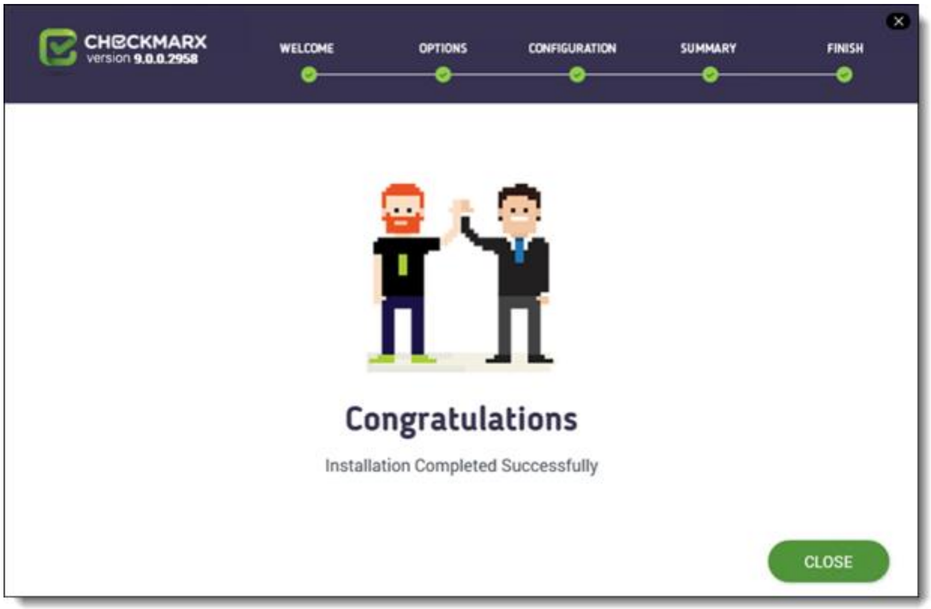
C:\Program Files\Checkmarx

10. Check the setup summary according to your selection.
11. Click <**INSTALL**> to continue, The **Installation in Progress** window is displayed and the installation proceeds, which may take a few minutes.
    - To return to the previous window, click <**BACK**>.
    - To exit, click <**X**>.



Installation in progress

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



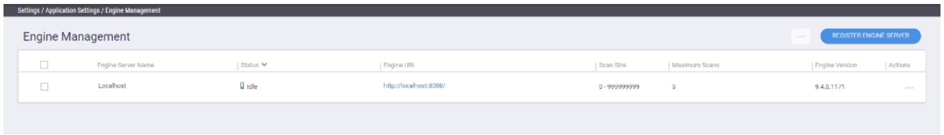
Congratulations

Installation Completed Successfully

13. Click <**CLOSE**> to complete the installation.

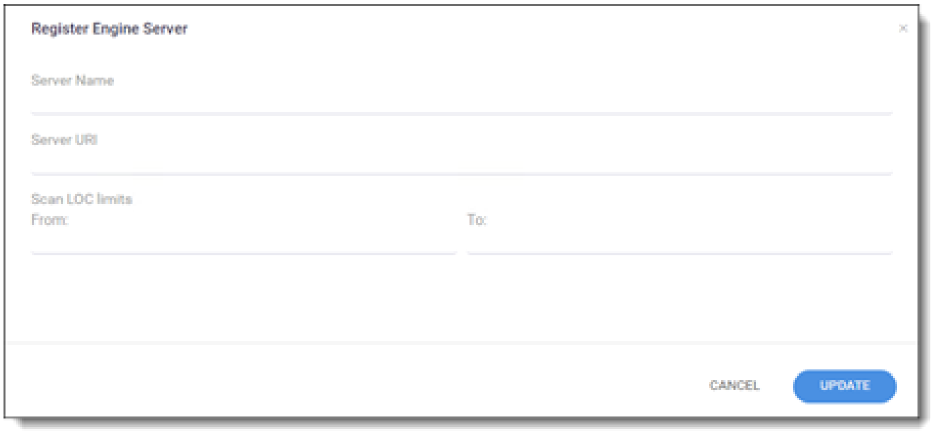
- Engine servers do not require a separate license. The existing CxSAST license must be copied from CxManager to each CxEngine host using the License Importer tool (Start > Checkmarx > CxLicenseImporter.exe). For more information, refer to Updating the CxSAST License.

14. Log into the CxSAST web interface.
15. Go to **Settings > Application Settings > Engine Management.** The **Engine Management** window is displayed.



□	Engine Server Name	Status	Engine URL	Scan Size	Maximum Scans	Engine Version	Actions
□	Localhost	Idle	http://localhost:8088/	0 - 999999999	3	9.4.0.1171	...

16. Click <**Register Engine Server**>. The **Register Engine Server** window is displayed.



17. Assign a **Server Name** to the engine, and provide the **Server URL** to enable CxManager to communicate with CxEngine. The URL is something like **http://<server>:<port>** (where <server> is the CxEngine host's IP address or a resolvable name), for example **http://engine1:8088**.
18. Click <**Update**>.

- Once the new engine is installed, you may have to:
    - 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.

19. 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:**

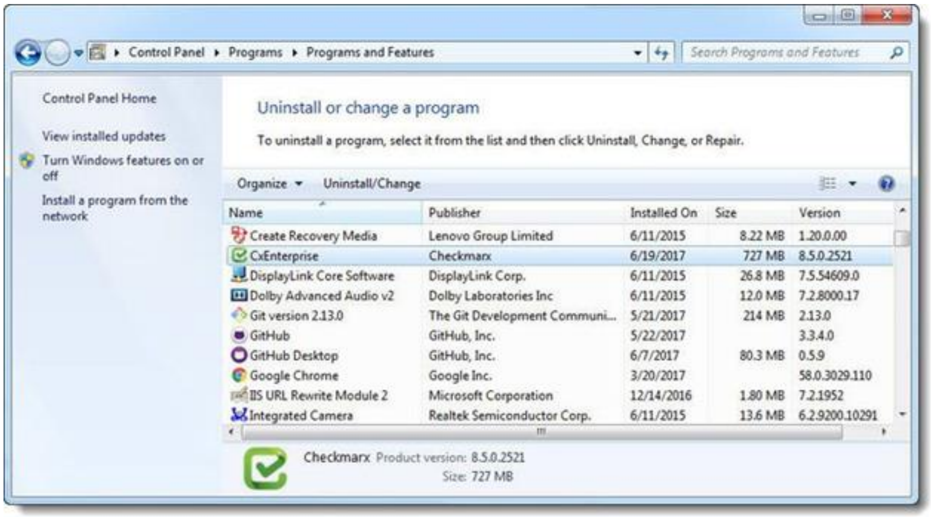
1. Copy your CxSAST license file to a safe location.
2. Make sure that there are no scans currently running.
3. Stop all Cx Windows services and Web server (depending on the Checkmarx components installed on the server):

   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.



Control Panel ▸ Programs ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize ▾
Uninstall/Change

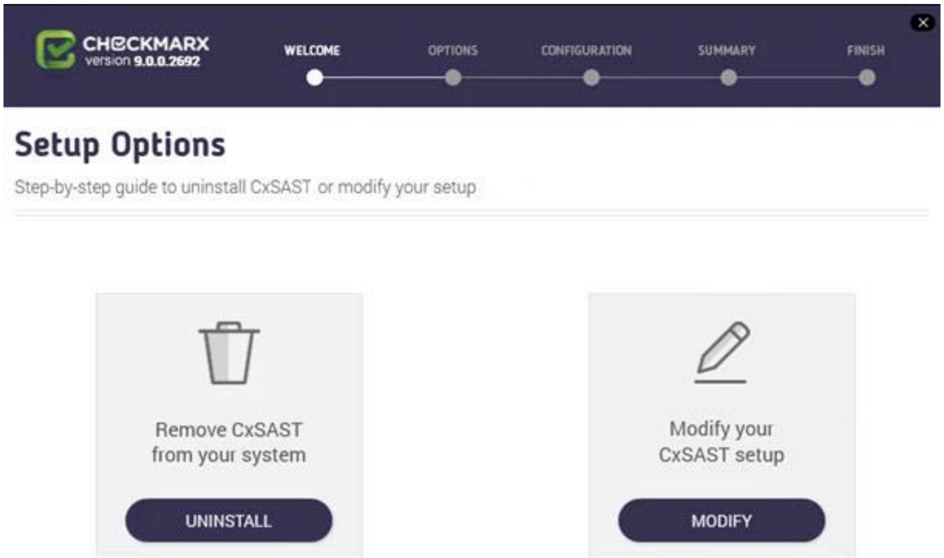
Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Create Recovery Media	Lenovo Group Limited	6/11/2015	8.22 MB	1.20.0.00
CxEnterprise	Checkmarx	6/19/2017	727 MB	8.5.0.2521
DisplayLink Core Software	DisplayLink Corp.	6/11/2015	26.8 MB	7.5.54609.0
Dolby Advanced Audio v2	Dolby Laboratories Inc	6/11/2015	12.0 MB	7.2.8000.17
Git version 2.13.0	The Git Development Communi...	5/21/2017	214 MB	2.13.0
GitHub	GitHub, Inc.	5/22/2017		3.3.4.0
GitHub Desktop	GitHub, Inc.	6/7/2017	80.3 MB	0.5.9
Google Chrome	Google Inc.	3/20/2017		58.0.3029.110
IIS URL Rewrite Module 2	Microsoft Corporation	12/14/2016	1.80 MB	7.2.1952
Integrated Camera	Realtek Semiconductor Corp.	6/11/2015	13.6 MB	6.2.9200.10291

Checkmarx Product version: 8.5.0.2521
Size: 727 MB

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



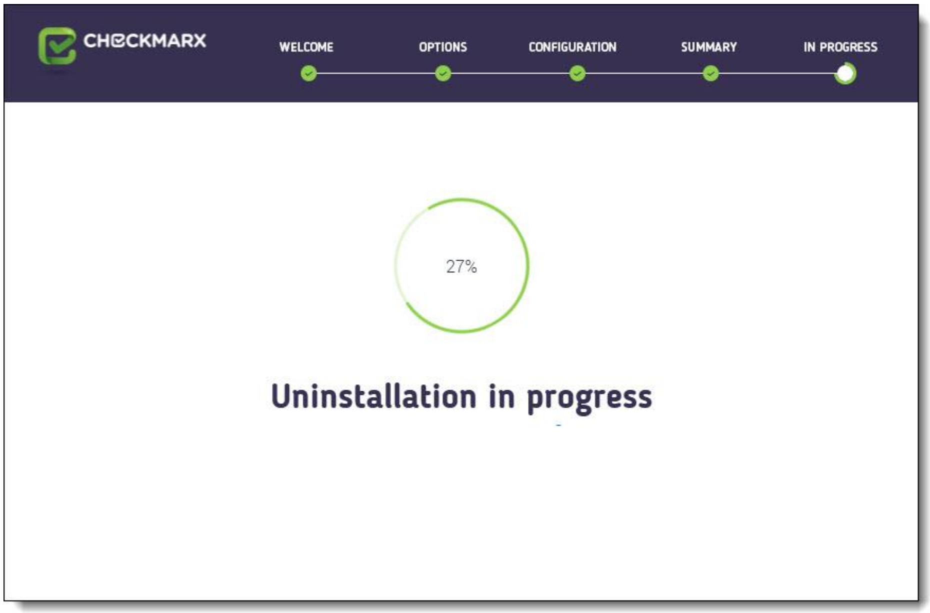
Setup Options

Step-by-step guide to uninstall CxSAST or modify your setup

Remove CxSAST from your system

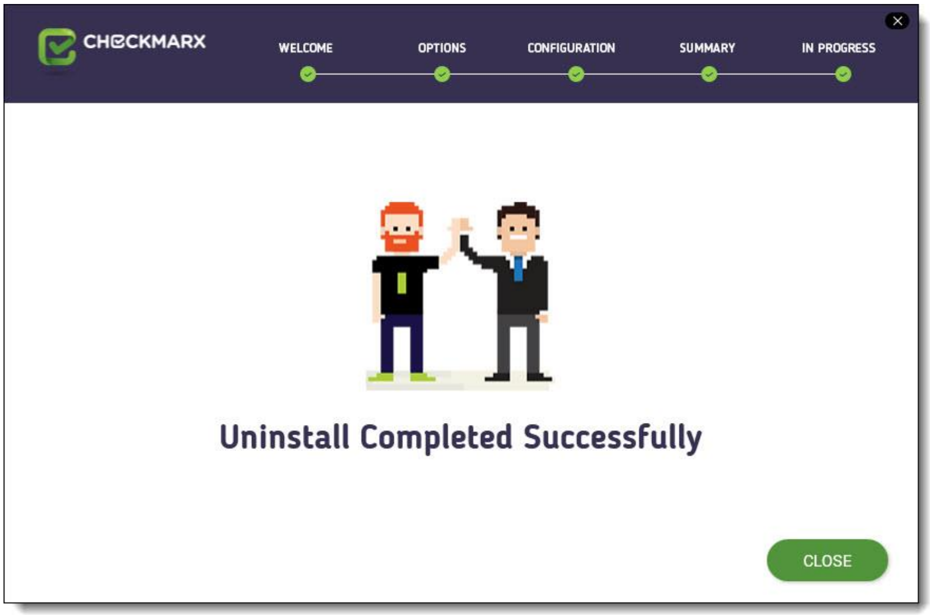
Modify your CxSAST setup

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.



Uninstallation in progress

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



Uninstall Completed Successfully

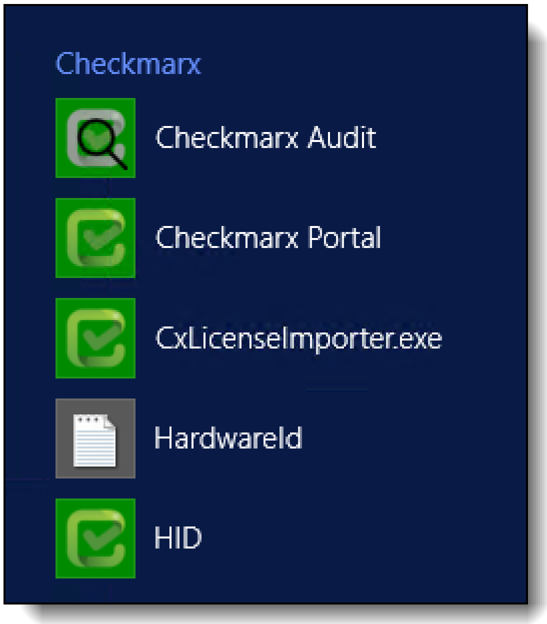
8. Click <**CLOSE**>to complete the uninstall.

- Even though uninstall removes most Checkmarx folders, for renewal purposes, the following folders are not deleted:
  - CxSrc
  - SQL DBs: CxDB, CxActivity and CxARM

Updating the CxSAST License

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

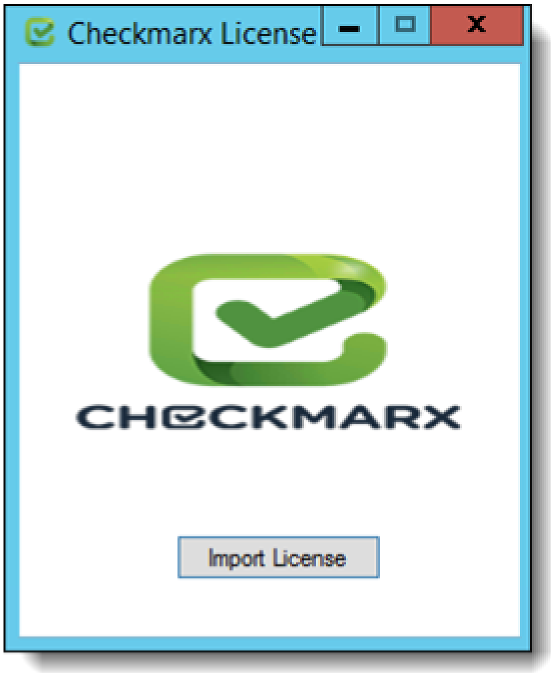
1. Go to **Start** > **All Programs** > **Checkmarx**, click **HID** to generate the Hardware ID.



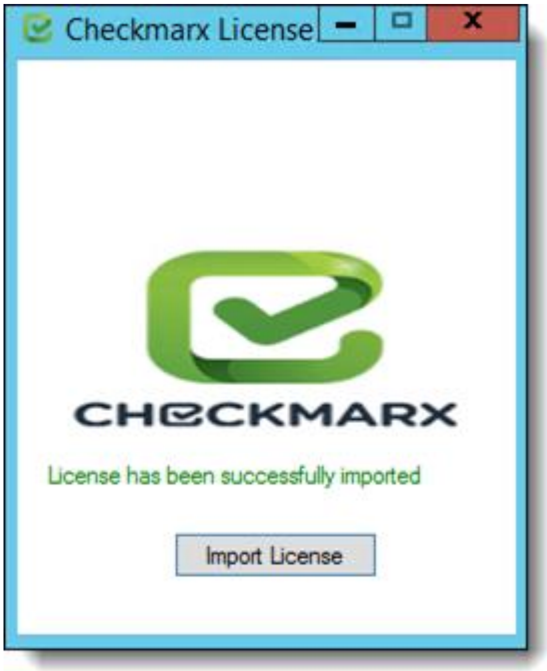
2. Go to: **<Checkmarx directory>HID>HardwareId**, then copy the **HardwareId** and send it to your Checkmarx sales representative or Checkmarx support to obtain a new or updated license.

- For Distributed and High Availability Installations, updating the license on each CxManager host is required.

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.



License has been successfully imported

- If your license doesn't match your current hardware ID (HID), a warning message is displayed.

Import a different license or request a new one from your Checkmarx sales representative or contact Checkmarx support.

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

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

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.

The CxZIP Utility

This section provides the available options for creating a smaller file for upload using the CxZIP utility.

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 specifiy extensions.
4. 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

- 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"/>

3. 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
3. Run the following script:

```
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 example above creates a file named "**TestProject.txt**" in the projects folder that has the number of counted lines of the entire 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 3rd party systems
Web Portal	Web interface with CxSAST
Audit	Client for creating and customizing queries
Database	Stores scan results and system settings

Backup

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

Step 1. Stop the CxServices

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

Step 2. Stop the Web Server

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

Step 3. Back up the Checkmarx Folder

1. Create a new Checkmarx backup folder (recommended to include backup date). Example: **C:\Program Files\Checkmarx - > C:\Program Files\Checkmarx15052016**
2. 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

- Back up 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**> in 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**> in 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 has been previously backed up by overwriting the databases 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**> in 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.

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

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

CxAuditSrc

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

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

Logs

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

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

Database

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

Appendix A: Compressing a Folder in Windows

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

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

Trade-Offs

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

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

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

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

When to Use and When Not to Use NTFS Compression

NTFS compression is ideal for:

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

NTFS compression should not be used for:

- Windows system files and other program files. Using NTFS compression here can reduce your computer's performance and potentially cause other errors.
- Servers where the CPU is getting heavy use. On a modern desktop or laptop, the CPU sits in an idle state most of the time, which allows it to decompress the files quickly. If you use NTFS compression on a server with a high CPU load, the server's CPU load will increase and it will take longer to access files.
- Files in compressed format. (You won't see much of an improvement by compressing your music or video collections).
- Computers with slow CPUs, such as laptops with low-voltage power-saving chips. However, if the laptop has a very slow hard disk, it's unclear whether compression would help or hurt performance.

How to Use NTFS Compression

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

1. To get started, right-click the file, folder, or drive you want to compress and select **Properties**.
2. Under **Attributes**, click <**Advanced**>.
3. Check **Compress contents to save disk space** and click <**OK**> twice.

4. If you enabled compression for a folder, Windows asks you whether you also want to encrypt subfolders and files.
5. 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.
6. Compare the Size on disk field to see how much space you saved.
7. Compressed files and folders are identified by their blue names in Windows Explorer.
8. To extract these files in the future, go back to their advanced attributes and clear **Compress.**

CxSAST Database Maintenance Guide

Chapter 1 - Introduction

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

There are basically two types of fragmentation:

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

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

Logical scan (or external/extent) fragmentation is caused by an operation called a page split. This occurs when a record has to be inserted on a specific index page (according to the index key definition) but there is not enough space on the page to fit the data being inserted. The page is split in half and roughly 50% of the records moved to a newly allocated page. This new page is usually not physically contiguous with the old page and therefore is refered 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 additional information, refer to https://technet.microsoft.com/en-us/library/2008.08.database.aspx.

Chapter 2 - Checkmarx Tables Overview

The CxSAST application has two databases:

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

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

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

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

Tables from the two first categories carry a high risk of fragmentation.

Instead of rebuilding or reorganizing all indexes on a regular basis (e.g. daily/weekly/monthly) the

more sophisticated approach involves using the dynamic management function (DMF) sys.dm_db_index_physical_stats to periodically determine which indexes are fragmented, and then choosing whether and how to operate on those. This function accepts parameters such as the database, database table, and index for which you want to find fragmentation. An example of the function usage is as follows:

```
SELECT
                OBJECT_NAME(ips.object_id)                "TblName"
                ,ips.object_id
                ,ips.index_id
     ,(select i.name from sys.indexes i where ips.object_id = i.object_id AND ips.index_id =
i.index_id and ips.index_level = 0) "IndexName"
                ,ips.index_type_desc                   "IndexType"
               ,ips.avg_fragmentation_in_percent
                ,ips.fragment_count
                ,ips.avg_fragment_size_in_pages
                ,ips.forwarded_record_count
                ,ips.alloc_unit_type_desc
                ,ips.page_count
                ,ips.index_depth
                ,ips.avg_page_space_used_in_percent
                ,ips.record_count
                ,ips.ghost_record_count
                ,ips.version_ghost_record_count
                ,ips.min_record_size_in_bytes
                ,ips.max_record_size_in_bytes
                ,ips.avg_record_size_in_bytes
                ,ips.compressed_page_count
FROM sys.dm_db_index_physical_stats(DB_ID('CxDB'),NULL,NULL,NULL,'<Scanning
Mode>') AS ips WHERE (1=1)
                and index_level=0
ORDER BY OBJECT_NAME(ips.object_id),ips.index_id;
```

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

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

The default (NULL) is LIMITED.

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

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

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

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

Returned Column	Description
	avg_fragment_size_in_pages value, the better the range scan performance.
forwarded_record_count	Number of records in a heap that have forward pointers to another data location. (This state occurs during an update, when there is not enough room to store the new row in the original location.) NULL for any allocation unit other than the IN_ROW_DATA allocation units for a heap. NULL for heaps when mode = LIMITED.

Chapter 4 - Maintenance Options for Reducing Fragmentation

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

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

- 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.
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,OldVersion;MultiSocket,NoLimitation
Windows Server 2012R2	NoLimitation	NoLimitation	SingleSocket,NoLimitation;MultiSocket,NoLimitation
Windows Server 2016	NoLimitation	NoLimitation	SingleSocket,NoLimitation;MultiSocket,NoLimitation

➢ **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.