

CxSAST v8.6.0

Setup, Installation and User Guide

This document is non-binding and for information purposes only



Contents

VERSION RELEASE NOTES	8
CHECKMARX CXSAST OVERVIEW	9
SETTING UP CXSAST	
System Architecture Overview	11
CxSAST Server Components	
CxSAST Clients (user interfaces):	
CENTRALIZED ARCHITECTURE	13
DISTRIBUTED ARCHITECTURE	14
HIGH AVAILABILITY ARCHITECTURE	15
Server Host Requirements	16
PREPARING THE ENVIRONMENT FOR RELEASE	19
Preparing the Environment	20
Configure IIS 7 on Windows Server 2008	21
Configure IIS 7 on Windows 7	
Configure IIS 8 on Windows Server 2012	23
Configure IIS 8.5 on Windows Server 2012 R2	
Enable Long Path Support in Windows 10 and Server 2016	
CxSAST Server Components Installed on Dedicated Hosts	29
INSTALLING CXSAST	
Installation Permissions	
Setting Up CxSAST	
License Validation	
Installation Package	
Installing CxSAST	
Prerequisites and Recommendations	
Installation	
Installed Services Check	
Installed Application Pool Check	
Enable Long Path Support in CxSAST Application	
Login to the Web Interface	
Enable Long Path Support in Server Settings	
	54
Suntay	54
Parameters	54
Remarks	55
Fyamales	56
	57
REDAIDING CYSAST	
	60
Backing un CVCAST	۵۵. دم
Recovering (VSAST	
	ייייייע 70
	72
ADDING A CAENGINE SERVER	



UNINSTALLING CXSAST	70
UPDATING THE CXSAST LICENSE	
CXSAST APPLICATION MAINTENANCE GUIDE	8
Introduction	8.
Backup	8.
Step 1. Stop the CxServices	
Step 2. Stop the Web Server	
Step 3. Back up the Checkmarx Folder	
Step 4. Backup the Database	
Step 5. Backup the Scanned Source Folder	
Step 6. Restart the CxServices	
Step 7. Restart the Web Server	
Recovery	84
Step 1. Stop the CxServices	8
Step 2. Stop the Web Server	
Step 3. Restore Checkmarx's Backed up Folders and configuration files	8
Step 4. Restore the Scanned Source Folder	
Step 5. Restore the Database	
Step 6. Restart the CxServices	8
Step 7. Restart the Web Server	
Step 8. Check the Recovered Version	
Maintenance and Cleanun	-
CxManager	8
Reports	
CxEngine	
Sources	
Logs	
Scans	
CxWebPortal	
Logs	
CxAudit	
Sources	
Logs	
Database	8
Appendix A: Compressing a Folder in Windows	
Trade-Offs	
When to Use and When Not to Use NTFS Compression	
How to Use NTFS Compression	
XSAST DATABASE MAINTENANCE GUIDE	89
Chapter 1 - Introduction	
Chapter 2 - Checkmarx Tables Overview.	9
Chapter 3 - Monitorina	
Chapter 4 - Maintenance Options for Reducing Fragmentation	9,
SAST QUICK START	Qi
Stan 1. Enter Project Conoral Sattings	
Step 1: Enter Project General Settings	



Step 2: Select Source to Scan	97
Step 3: Scan Execution	
REVIEWING SCAN RESULTS	
Step 1 – Projects & Scans	
Step 2 – Review Scan Results in the Source Code	
Scan Result Summary	
Preset Manager: Overview	
CXSAST USER GUIDE	
THE CXSAST WEB INTERFACE	
ACCESSING THE WEB INTERFACE	
GETTING TO KNOW THE SYSTEM DASHBOARD	
Overview	
Dashboard Menu	
Projects and Scans	
Management Settings	
Scan Settings:	
Connection Settings:	
Application Settings:	
Maintenance:	
Manage Custom Fields:	
Users & Teams	
Data Analysis	
My Profile	
Dashboard Menu	
Project State	
Failed Scans	
Utilization	
Risk State	
Consolidated Project State	
Summary	
SAST Vulnerabilities Status	
SAST Progress Status	
Open Source Analysis (CxOSA)	
CxOSA (Open Source Analysis) Report	
Scan History	
VIEWING THE OPEN SOURCE ANALYSIS REPORT	
Security	
Vulnerability Score	
Vulnerable Libraries	
Severity Distribution	
Aging Vulnerable Libraries	
Security Vulnerabilities	
License Risk and Compliance	
License Distribution	
License Risk Distribution	
Outdated Libraries	

CH©CKMARX choose what developers use

High-Medium Risk Licenses	
Inventory	
Unresolved Libraries	
GENERATING THE OPEN SOURCE ANALYSIS REPORT TO PDF	
CREATING AND MANAGING PROJECTS	
CREATING AND CONFIGURING A CXSAST PROJECT	
CONFIGURING OPEN SOURCE ANALYSIS	
BRANCHING / DUPLICATING EXISTING PROJECTS	
MANAGING PROJECTS AND RUNNING SCANS	
Scan List/Actions	
MANAGING TABLES	
Advanced Actions	
CONFIGURING AN EMAIL ACTION	
CONFIGURING AN EXECUTABLE ACTION	
VIEWING PROJECT DETAILS	
General Properties	
Location Properties	
Scheduling Properties	
Advanced Properties	
Custom Fields Properties	
Data Retention Properties	
CxOSA Properties	
MANAGING QUERIES	
VIEWING, IMPORTING, AND EXPORTING QUERIES	
MANAGING QUERY PRESETS	
ТНЕ QUEUE	
SCAN RESULTS	
VIEWING RESULTS FROM ALL SCANS	
Projects Scan List/Actions	
Scan List	
Actions	
All Scans	
Deleting Scans	
Comparing Scans	
SCAN RESULT ACTIONS	
Navigating the All Scans table	
Viewing the Scan Summaries	
NAVIGATING SCAN RESULTS	
SCAN RESULTS EXAMPLE	
GENERATING SCAN RESULT REPORTS	
COMPARING SCAN RESULT SETS	
DASHBOARD ANALYSIS	
DATA ANALYSIS	
USER ADMINISTRATION	
ROLE AND PERMISSION OVERVIEW	
CREATING AND MANAGING USER ACCOUNTS	

CHECKMARX choose what developers use

CREATING USER ACCOUNTS IN THE WEB INTERFACE	202
CREATING USER ACCOUNTS VIA USER REGISTRATION	206
MANAGING EXISTING USERS	208
MANAGING TEAMS	210
Creating a Team	211
Adding a User to a Team	211
MAPPING LDAP DIRECTORY USER GROUPS TO CXSAST TEAMS	213
CHANGING SAML USER TEAMS AND ROLES IN THE CXSAST	215
MANAGING THE ORGANIZATIONAL HIERARCHY	217
Tree Branch View	217
Team Management	218
MANAGEMENT SETTINGS	222
SCAN SETTINGS	223
Query Viewer	223
Preset Manager	224
Pre & Post Scan Actions	225
Source Control Users	226
QUERY VIEWER	227
Creating a Custom Description	228
Importing Queries	230
Exporting Queries	231
PRESET MANAGER	232
Creating a New Preset	233
Modifying an Existing Preset	233
Importing a Preset	234
Exporting a Preset	234
Deleting a Preset	234
Predefined Presets	235
LIMITING ENGINE SCANS	239
CONNECTION SETTING	240
LDAP MANAGEMENT	241
Adding an LDAP Server	241
Configuring LDAP Authentication Settings	242
Configuring LDAP Synchronization Settings	245
Defining User Management (Synchronization)	247
Defining Role Mapping Settings	248
SAML MANAGEMENT	250
Configuring SAML in CxSAST	250
Importing the SAML Certificate into CxSAST	253
Exporting the Metadata File from CxSAST	253
APPLICATION MANAGEMENT.	254
General	254
Server Settings	
SMTP Settings	
OSA Settings	
License Details	257

CH©CKMARX choose what developers use

General	
Supported Languages	
Capacity	
License Expiration Notification	
Installation Information	259
External Services Settings	
Engine Server Management	
Performing Engine Sever Management Actions	
Register a New Engine Server	
Edit an Existing Engine Servers Attributes	
Unregister an Engine Server	
Block/unblock an Engine Server	
MAINTENANCE SETTINGS	265
DATA RETENTION MANAGEMENT	
Defining Data Retention Settings	
Scans to keep:	
Scans to delete:	
Data Retention Purged Data	
Database Tables	
File System	
UNLOCKING SCANS	270
MANAGING CUSTOM FIELDS	271
MY PROFILE SETTINGS	273
Accessing My Profile Settings	
Defining Profile Account Information	
Account Information:	
Changing Profile Password	
Change Password:	



Version Release Notes

For version-specific CxSAST release notes, go to:

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



Checkmarx CxSAST Overview

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

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

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

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

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

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

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

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

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

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



Setting Up CxSAST

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

In this section:

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



System Architecture Overview

CxSAST includes the following components:



CxSAST Server Components

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



CxSAST Clients (user interfaces):

- IDE Plugins
- CxAudit
- CxSAST CLI
- CxSAST API

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

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

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



Centralized Architecture

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





Distributed Architecture

In distributed architecture, components are presented on different platforms and several components can cooperate with one another over a communication network in order to achieve a specific objective or goal. CxSAST supports distributed architecture, where any or all of the server components are installed on dedicated hosts.



The basis of a distributed architecture is its transparency, reliability, and availability. Distributed architecture is the most recommended method for CxSAST deployment because all Cx components function at their most optimized capacity.



High Availability Architecture

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



The main objective of implementing High Availability is to make sure CxSAST is always available for the systems users and clients.

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



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.

(i) 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 <u>link</u>.

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



Purpose	Lines of Code	Installed RAM**	Cores	CPU Speed	Disk	os	Web Server	Other Software
	200K	6 GB			50 GB	Windows 7,8,8.1,10 Windows	IIS	
(POC)	500K	8-16 GB	Recommended: 4 up to a maximum of 12 cores	2.8 GHz	(recommended)	Server 2008R2 2012, 2012R2, 2016	7/7.5/8/ 8.5/10	
	200K	6 GB	Minimum: 6 for 1 concurrent scan.	2.0 CH				
	600K	10 GB	Additional 4 cores for each additional concurrent scan,	2.8 GHZ				Windows Installer 3.1 or above (Run msiexec to check)
Centralized	1.2M	16 GB	up to a maximum of 12 cores, (Recommended: 4, 6, or 8 cores.)		250 GB		IIS	
(Production)	2M	25 GB	Max recommended concurrent scans: 3 *	2.8 GHz	(recommended)		8.5/10	
	3М	40 GB	more are recommended to limit concurrency or					
	4M	50 GB	run on their own distributed server.					.NET framework 4.5.1 or above (Windows 7/8
Distributed - CxEngine	200K	5 GB		Recommended:		Windows		will need .NET framework 3.5 as well because of
(Production) For multiple CxEngine	600K	9 GB		2.8 GHz		Server 2008R2 2012.		IIS version)
servers (for	1.2M	15 GB	4 (per concurrent scan) up to a maximum of 12		100 GB	2012R2, 2016	NA	
concurrent scans), each server	2M	24 GB	(Recommended: 4, 6, or 8 cores)	Recommended:	(recommended)	recommended)		
should meet the	3М	36 GB		2.8 0112				
requirements	4.5M	50 GB						
Distributed - CxManager (Production)		8 GB	4	2.5 GHz	250 GB (recommended)		IIS 7/7.5/8/8. 5/10	
Distributed - Database (Production)		8 GB	4	2.5 GHz	250 GB (recommended)		NA	MS SQL Server (Express not recommended) 2008/2012/2014/ 2016

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



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

i Cloud Environments

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

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



Preparing the Environment for Release

The following sections include the environmental preparations needed for releases:

In this section:

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



Preparing the Environment

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

- 1. Make sure that the Centralized or CxManager host name does not contain any nonalphanumeric characters such as "_". This is to avoid issues described <u>here</u>.
- 2. Make sure that organizational firewalls allow:
 - HTTP (TCP port 80):
 - From client hosts to the Centralized or CxManager host
 - Between CxManager and CxEngine (in a distributed architecture)
 - SQL Server traffic (by default, TCP port 1433) from CxManager to SQL Server (If using SQL Server, in a distributed architecture)
 - SQL Browser (UDP port 1434) this will allow machines (i.e. on installation wizard) to scan for SQL Servers on the network

- If an SQL Server is not displaying in the Installation window, you can try typing the machine name or IP address directly into the Wizard

- If an SQL Server uses a custom port, use a "," between the machine name/IP and port number, e.g. "10.199.76.1,65391" or "SSMACHINE,65391".

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

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

- 4. On server component hosts, prevent anitviruses from scanning the Checkmarx folder, usually:
 - C:\CxSrc
 - Checkmarx installation directory: C:\Program Files\Checkmarx\ C:\Program Files(x86)\Checkmarx\
- 5. Configure IIS (except on database-only component server in a distributed deployment):

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



Configure IIS 7 on Windows Server 2008

- 1. Open the Server Manager by right-clicking **Computer** and selecting **Manage**.
- 2. In the left-hand navigation pane select Roles, and click Add Role Services:

E. Server Manager			
File Action View Help			
** 2 10 12			
Roles H Grand Server (IIS) H Grand Server (IIS) H Diagnostics	Roles Vew the health of the roles ind	alled on your server and add or remove roles and features.	
Configuration Storage	Roles Summary		Roles Summary Help
	 Rolest 1 of 17 installed Web Server (IIS) 		Add Roles
	• Web Server (IIS)		Web Server (IIS) Heb
	Provides a reliable, manageable, and scal	able Web application infrastructure.	
	 Role Status Messages: None System Services: 4 Running, 2 S Events: 17 Informational in the lateral 	topped et 24 hours	Go to Web Server (IIS)
	Best Practices Analyzer: To start tile on this role's homepage and	a Best Practices Analyzer scan, go to the Best Practices Analyzer did. Scan this Role	Add Role Services
	Role Service	Satus	Po Remover Role Services
	Web Server	Installed	

- 3. Scroll down and select the following:
 - Static Content
 - World Wide Web Services > Application Development Features > ASP.NET (Click OK to approve all dependent features)
 - In Management Tools:
 - IIS Management Console
 - IIS 6 Metabase Compatibility.
 - Click Next, and Install.
- 4. **Close** the window.
- 5. Download and install .Net Framework 4.5.2 and all its updates.
- 6. Open a command prompt as an Administrator, and go to C:\Windows\Microsoft.NET\Framework64\v4.0.30319.
- 7. Run:

ServiceModelReg.exe -ia

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



Configure IIS 7 on Windows 7

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



- 4. In Internet Information Services, select the following:
 - o In Web Management Tools:
 - IIS Metabase and IIS 6 Configuration Compatibility
 - IIS Management Console
 - World Wide Web Services > Application Development Features > ASP.NET (Click OK to approve all dependent features)
 - World Wide Web Services > Common HTTP Features > Static Content
- 5. Click **OK**.
- 6. Download and install .Net Framework 4.5.2 and all its updates.
- 7. Open a command prompt as an Administrator, and go to C:\Windows\Microsoft.NET\Framework64\v4.0.30319.
- 8. Run:

```
ServiceModelReg.exe -ia
```



Configure IIS 8 on Windows Server 2012

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

🗩 Ə 🔹 Server Ma	anager • Dashboard
Dashboard Local Server All Servers App Server File and Storage Services ▷ IIS	WELCOME TO SERVER MANAGER QUICK START QUIC

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

elect installatio	on type	DESTINATION SERVE WIN-ORPCOPIUON
Before You Begin	Select the installation type. You can install roles and features on machine, or on an offline virtual hard disk (VHD).	a running physical computer or virtua
Installation Type	C Data barred and the stand of the stand	
Server Selection	 Kole-based or reature-based installation Configure a signale server by adding roles role services and fe 	ATURA
	consigning a single server by booking totes, the services, and te	
	Remote Desktop Services installation	
	Install required role services for Virtual Desktop Infrastructure or session-based desktop deployment.	(VDI) to create a virtual machine-bas

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



elect destination	ON SERVER DESTINATION SERVER
Before You Begin	Select a server or a virtual hard disk on which to install roles and features.
Installation Type	Select a server from the server pool
Server Selection	Select a virtual hard disk
Server Roles	Server Pool
Features Confirmation	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.
	< Previous Next > Install Cancel

- 5. Click Next.
- 6. For Server Roles Select Web Server (IIS) and Click Next
- For Features Select .Net Framework 4.5 Features > WCF Services > HTTP Activation and click Next
- 8. Continue through the wizard until the **Web Server Role (IIS)** > **Role Services** page:

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



- 9. Select the following:
 - Application Development (Installed)
 NET Extensibility 3.5 (Installed)
 NET Extensibility 4.5 (Installed)
 Application Initialization
 ASP
 ASP.NET 3.5 (Installed)
 CGI
 ISAPI Extensions (Installed)
 ISAPI Filters (Installed)
 Server Side Includes
 WebSocket Protocol
 - Common HTTP Features > Static Content
 - Application Development > ASP.NET 4.5
 - Management Tools > IIS Management Console
 - Management Tools > IIS 6 Management Compatibility > IIS 6 Metabase Compatibility
- 10. Finish the wizard, confirm and Install.



Configure IIS 8.5 on Windows Server 2012 R2

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

To configure IIS 8.5 using the Checkmarx configuration file:

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



3. In PowerShell, run:

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



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



Enable Long Path Support in Windows 10 and Server 2016

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

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

💷 Run	×
0	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	gpedit.msc ~
	OK Cancel Browse

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

Local Group Policy Editor			-		×
File Action View Help					
🔶 🤿 🙇 🚾 🔒 📓 📷 🝸					
Local Computer Policy A	📔 Filesystem				
Computer Configuration Software Settings	Select an item to view its description.	Setting		State	
> Windows Settings		NTFS			
Administrative Templates		Disable delete notifications on all volumes	Not	configur	ed
> Control Panel		Enable Win32 long paths	- 1	Enabled	
> 🛄 Network		E Selectively allow the evaluation of a symbolic link	Not	configur	ed
Printers					
Server					
Start Menu and Taskbar					
V System					
Access-Denied Assistan					
> App-v					
Credentials Delenation					
Device Guard					
> Device Installation					
> Device Redirection					
Disk NV Cache					
Disk Quotas					
Display					
> Distributed COM					
Driver Installation					
Early Launch Antimalw					
Ella Classification Infras					
File Share Shadow Com					
Filesystem					
T NTFS					
Folder Redirection					
🧰 Group Policy 🗸 🗸		٢			>
< >	Extended Standard				
3 setting(s)					



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

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

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



CxSAST Server Components Installed on Dedicated Hosts

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

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

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

Go to the Microsoft Web Platform Installer and click Download.



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



oper	ingine Products Preprietations			
_	Name		Released	Install
Ô,	Microsoft Azure Service Fabric SDK and Tools - 2.4.145 (VS2015)		08/12/2016	Add
1	Microsoft Azure SDK for .NET (VS 2015) - 2.9.6		16/11/2016	Add
1	Visual Studio Community 2015 with Microsoft Azure SDK - 2.9.6		16/11/2016	Add
A	Microsoft Azure SDK for .NET (VS 2013) - 2.9.6		16/11/2016	Add
A	Visual Studio Community 2013 with Microsoft Azure SDK - 2.9.6		16/11/2016	Add
A	Microsoft Azure SDK for .NET for Visual Studio 2017 RC - double click t	o learn more	16/11/2016	Add
0 Iter	ms to be installed	Options	Install	Fxit

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

Sea	rch results for url		ډ [] ،
	Name	Released	Install
¢.,	URL Rewrite 2.0	27/05/2015	Add
•	IIS: URL Authorization	27/02/2008	Add
52	IIS7 Support for Extensionless URLs	16/03/2011	Installed
e.	IIS: HTTP Redirection	27/02/2008	Add
e.	IIS: Default Document	27/02/2008	Installed
e	IIS: Directory Browsing	27/02/2008	Installed
e	IIS: HTTP Errors	27/02/2008	Installed
COM-	Survey Project	11/06/2012	Add
heres	to be installed	Onting	



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

Sear	ch results for Application		
	Name	Released	Install
2	Application Initialization 1.0	05/04/2012	Add
9	Application Insights Status Monitor Preview	11/04/2016	Add
Q	Application Request Routing 2.5 with KB2589179	03/09/2010	Add
	Application Request Routing 2.5	29/03/2011	Add
	KB2589179 for Application Request Routing 2.5	03/09/2010	Add
ye.	Microsoft SQL Server Data-Tier Application Framework (DACFx) (June 2014)	19/06/2014	Add
	Application Request Routing 3.0	27/05/2015	Add
No.	Microsoft Drivers 3.2 for PHP v5.5 for SQL Server in IIS Express	11/03/2015	Add
	OWA	24/09/2014	Add
Items t	o be installed Option	15 Install	Exit

Click Install. The Microsoft Web Platform Installer Prerequisites are displayed.

PREREQUISITES	INSTALL	CONFIGURE	FINISH
Review the following list of thi oftware identified below to b products are provided by the t esponsible for and must sepa	rd party application software, e installed and Windows com hird parties listed here. Micro rately locate, read and accept	Microsoft products and components ponents to be turned on. Third party isoft grants you no rights for third par these third party license terms.	, and any additional applications and ty software. You are
× Application Request	Routing 3.0		
View license terms		1	Direct Download Link
X URL Rewrite 2.0			
View license terms		1	Direct Download Link
Total file download size:	r.		8.42 MB
<mark>Tick here to see additional sol</mark> By clicking "I Accept", you agr oftware identified above. If y	ftware to be installed and revi ree to the license terms for the ou do not agree to all of the li	ew the associated Microsoft license te third party and Microsoft software, a icense terms, click "I Decline".	erms and any additional



Click I Accept. The Microsoft Web Platform Installer Confirmation is displayed.

PREREQUISITES The following products v External Cache 1.1	INSTALL	CONFIGURE	FINITELL
The following products v External Cache 1.1			FINISH
External Cache 1.1	were successfully in	nstalled.	
	20		
URL Rewrite 2.0			
Application Request Routi	ing 3.0		
			Finish

Click Finish to finalize.

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



e View Help		
inections	Default Web Site Home	Actions
 DAVIDP-LAPTOP (DM\davidp) Application Pools Stes Default Web Site Stes CxRestAPI CxRestAPI CxRestAPI App_GlobalResources App_ClobalResources App_Themes Some From Pages Some From Pages HttpHandlers 	Filter:	Open Feature Depen Feature Edit Permissions Edit Site Bindings Basic Settings View Applications View Virtual Directories Manage Web Site Restart Stop Browse Web Site Browse Ya0 (http) Advanced Settings
O - III Images O - III Images O - III Is O - III IS O - III IS O - IIII IS O - IIII IS O - IIII IS O - IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Modules Output Request SSL Settings URL Rewrite Management Configurat Editor Platfor	Configure Limits Configure Distall Application From Gallery Confine Help Confine Help

Select Open Feature. The URL Rewrite Rule is displayed.

File View Help						
onnections		write			Actions	
	OKL KE	write			Add Rule(s)	
DAVIDP-LAPTOP (DM\davidp)	Provides rewriting ca	apabilities based on rules	for the requested URL	address	Revert to Parent	
Sites Gefault Web Site	and the content of a Inbound rules that a	Manage Server Variables View Server Variables				
p - jjj] Server Farms	Name	Input		Match	Manage Providers View Rewrite Maps View Providers	
					Inbound Rules	
					Import Rules	
	۰ (m				Outbound Rules	6
	Outbound rules that	are applied to the header	s or the content of an	HTTP respon	View Preconditions View Custom Tags	8
	Name	Input	Match	Patterr	😧 Help	
	<i>.</i>	ш		•	Gnime Help	



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

Select a rule template:		
Inbound rules		
😝 Blank rule	Rule with rewrite map	
😼 Request blocking		
Inbound and Outbound Rules		
😹 User-friendly URL	🛞 Reverse Proxy	
Outbound rules		
🗧 Blank rule		
Search Engine Optimization (SEO)		
Enforce lowercase URLs	🔝 Canonical domain name	
Mappend or remove the trailing sla	ish symbol	
elect this template to create a rule th	at will forward incoming HTTP requests to a back-end W	eb server.
	N	100 B

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

And the server name or the IP address where HTTP requests will be forwarded:	Enter the server name or the IP address where HTTP requests will be forwarded: cxmngr-server.dm.cx	
commgr-server.dm.cx xample: contentserver1 Enable SSL Offloading Selecting this option will forward all HTTPS requests over HTTP. hutbound Rules 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	cxmngr-server.dm.cx	
Example: contentserver1 Example: contentserver1 Example: contentserver1 Example: www.contoso.com Example: www.contoso.com Example: www.contoso.com Example: contentserver1 Find the final sector of the sect		
Enable SSL Offloading Selecting this option will forward all HTTPS requests over HTTP. Nutbound 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	Example: contentserver1	
Selecting this option will forward all HTTPS requests over HTTP.	Enable SSL Offloading	
Dutbound 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	Selecting this option will forward all HTTPS requests over HTTP.	
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	Outbound Rules	
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	Rewrite the domain names of the links in HTTP responses	
Example: contentserver1 To: Example: www.contoso.com	From:	
To: Example: www.contoso.com	Example: contentserver1	
Example: www.contoso.com	To:	
Example: www.contoso.com		
	Example: www.contoso.com	

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



Disable the SSL Offloading option.

Click **OK** to save the changes.

Internet Information Services (IIS) Mar	nager.			APRIL 1				actar all of	×
O O DAVIDP-LAPTOP	Sites Default Web Site							😡 × 🟠	
File View Help									
Connections								Actions	
21	URL Rewrite							Add Rule(s)	
DAVIDP-LAPTOP (DM\davidp)	Provides rewriting capabilities ba	Revert to Parent							
Application Pools	Inbound rules that are applied to	the requested URL add	dress:					Manage Server Variable	es
🖌 😝 Default Web Site	Name	Input	Match	Pattern	Action Type	Action URL	s	View Server Variables	
aspnet_client	🛞 🧾 ReverseProxyInboundR	URL path after '/'	Matches	(.*)	Rewrite	{C:1}://comng	T	Manage Providers	
CXRestAPI								View Rewrite Maps View Providers	
> App Browsers								Conditions	۲
App_GlobalResou								Add	
App_Themes	201							Inbound Rules	0
o - Din Content	< ()	EN.				1	7	Edit	
CSS	Outbound rules that are applied t	o the headers or the c	ontent of an Hi	TP response:				Rename X Remove	
p 🚰 fonts	Name	input N	Aatch	Pattern	Action Type	Action Value		Disable Rule	
 HttpHandlers Images 								 Move Up Move Down 	
b - is is is in the second								Import Rules	
6 - C Properties								Outbound Rules	•
 Scripts UlComponents 								View Preconditions View Custom Tags	
> - WebMethods	•	m			1		F	B Help	
Server Farms							2	Online Help	
(m))	Features View 👫 Content View	N							
onfiguration: 'Default Web Site' web.com	nfig								61

Select the newly created **Rule** and click **Edit**. The **Edit Inbound Rule** is displayed.

Internet Information Services (IIS) Mar	ager	
CO O HAVIDP-LAPTOP	Sites Default Web Site	<u>a</u> ≈ <u>b</u> ⊛
File View Help		
Connections	Edit Inbound Rule	Actions
DAVIDP-LAPTOP (DM\davidp)	Name ReverseProxyInboundRule1	Ex Cancel
	Match URL 🛞	 Help Online Help
	Matches the Pattern Regular Expressions	
	Pattern: ·*(cxrestapi/*) Ignore case	
 Images js JScripts Properties 	Conditions Cogical grouping: Match All	
 scripts UlComponents WebMethods CxWebInterface Server Farms 	Input Type Pattern {CACHE_URL} Matches the Pattern ^@https?jc// Add	
	Features View 💦 Content View	
onfiguration: 'Default Web Site' web.com	fig	9



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

Verify the changes in the URL Rewrite rule.

DAVIDP-LAPTOP	Sites Default Web Site						100 (100	(i) (i)	
ile View Help									
nnections		Actions							
	URL Rewrite	Add Rule(s)							
DAVIDP-LAPTOP (DM\david	Provides rewriting capabilities base	Revert to Parent Manage Server Variables							
Application Pools	Inbound rules that are applied to th								
Default Web Site Site Site Software client Software client Software client Software client	Name	Input	Match	Pattern	Action Type	Action URL	View Server Variables		
	😑 🥁 ReverseProxyInboundRule1	URL path after '/'	Matches	.*(crrestapi/.*)	Rewrite	{C:1}://cxmngr-server.dm.cx/	Manage Providers		
		{CACHE_URL} Matches^(https?)://					View Rewrite Maps View Providers		
> - app							Conditions	۲	
App_GlobalRe							Add		
App_Themes App_Themes App_Content Content CSS CSS ForroPages c	×(Inbound Rules	۲	
	Outbound rules that are applied to	Edit Rename							
	Name	Input	Match	Pattern	Action T	ype Action Value S	X Remove Disable Rule		
 HttpHandlers Images 							 Move Up Move Down 		
> js							Import Rules		
Properties Scripts							Outbound Rules View Preconditions	۲	
UIComponent WebMethods	Land M						View Custom Tags		
an k	Features View 💦 Content View						😯 Help		

Test the **CxSAST** application.


Installing CxSAST

Before installing CxSAST, make sure that you understand the system architecture, that your server host(s) complies with the <u>server host requirements</u>, and that you have properly prepared the installation <u>environment</u>.

- If you are interested in configuring a High Availability solution please contact <u>Checkmarx support</u>.
- (i) If your portal is installed on a separate machine from manager, please perform the following <u>procedure</u>.

Installation Permissions

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

(i) SQL Server database:

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

- Build two SQL databases using the names; CxDB and CxActivity
- Create login for Windows User and associate it with DB_owner permission for CxDB and CxActivity. This user should be a dedicated Service user and the same user must perform the installatio. For additional information, see CxSASTConfiguration Guide > Configuring CxSAST for use with a non-default user (Network Service) CxServices & IIS Application Pools.

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

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

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



i AWS RDS

DBaaS is not supported naively. but AWS RDS can be used - To make RDS work you need to create two databases, CxDB, and CxActivity. 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 two databases already existing, just click continue. Once the installation is complete the RDS should work.

Setting Up CxSAST

License Validation

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

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

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

(i) If you have already installed CxSAST and have not yet obtained a permanent CxSAST license, send your hardware ID (Start > All Programs > Checkmarx > HardwareId) to your Checkmarx sales representative or <u>Checkmarx support</u> to obtain a Production license file.

Installation Package

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



Installing CxSAST

Prerequisites and Recommendations

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

Installation

Once you have downloaded the CxSAST Installation package, run the CxSetup.exe. The Checkmarx Welcome window is displayed.

			SUMMARY	FINISH	8
The Latest Release of CxS Step-by-step guide to installation & configuration	SAST is	Here			
Setup will install CxSAST on your computer Choose "ALL-IN-ONE" for standard installation or "A	ADVANCED" for	detailed configuratio	n		
Choo	se your installa	tion type:			
			D		
Customized installation for advanced users		Fastest way to components i	install CxSAST ncluding SQL E	with all xpress	
ADVANCED INSTALLATION		ALL-IN-O	NE INSTALLATION		

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



		OPTIONS		SUMMARY	FINISH
License Agreem	ient				
END USER LICENSE AGREEMENT					1
PLEASE READ THE TERMS AND CONDI CHECKMARX SOFTWARE ("SOFTWARE	TIONS OF THIS END USE ") AND ACCOMPANYING	ER LICENSE AGREEME S DOCUMENTATION	NT ("EULA") CAREFULLY BE ("DOCUMENTATION").	FORE INSTALLING OR L	ISING THE
UNLESS YOU HAVE A SEPARATE WRIT DOCUMENTATION, THIS EULA REPRES ("CHECKMARX"). IF YOU HAVE A SEPA RESELLER GOVERNING YOUR USE OF T	FEN LICENSE AGREEMEN ENTS A BINDING LEGAL RATE LICENSE AGREEME THE CHECKMARX SOFTW	IT WITH CHECKMAR) AGREEMENT BETWEI ENT ENTERED INTO B VARE AND DOCUMEN	GOVERNING YOUR USE O EN YOU AND THE CHECKM ETWEEN YOU AND CHECKI ITATION, THE TERMS OF TI	F THE SOFTWARE AND ARX ENTITY IDENTIFIED MARX OR AN AUTHORI HAT AGREEMENT SHALI	BELOW ZED CHECKMARX L CONTROL.
THIS LICENSE IS VALID ONLY FOR THE OF THIS EULA. THE SOFTWARE IS ACTI WILL BE INOPERATIVE UPON THE EXPI HAVE ACQUIRED THE SOFTWARE FRO	LICENSE TERM SET FOR VATED BY A LICENSE KE RATION OF THE LICENSE M CHECKMARX OR AN A	TH IN YOUR QUOTE, Y WHICH EXPIRES AT E TERM, YOU ARE ON AUTHORIZED RESELLI	UNLESS TERMINATED EARI THE END OF THE LICENSE ILY AUTHORIZED TO USE T IR.	JER IN ACCORDANCE V TERM. AS A RESULT, TH HE SOFTWARE UNDER	VITH THE TERMS HE SOFTWARE THIS EULA IF YOU
IF YOU ARE INSTALLING, DOWNLOAD YOU HEREBY ACCEPT THIS EULA ON B REPRESENT AND WARRANT THAT YOU	ING, ACCESSING, OR OT EHALF OF SUCH ENTITY, J HAVE THE RIGHT, POW	HERWISE USING THE YOU ACKNOWLEDG /ER AND AUTHORITY	SOFTWARE ON BEHALF OF E THAT SUCH ENTITY IS LEC TO ACT ON BEHALF OF AN	A COMPANY OR OTHE GALLY BOUND BY THIS ID BIND SUCH ENTITY.	ER LEGAL ENTITY, EULA, AND YOU YOU MAY NOT
You must accept the License	Agreement to inst	all the program.			
I accept the terms in the Lic	cense Agreement.		(ВАСК	NEXT

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

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



				SUMMARY	FINISH
Installation Opt	to select which co	omponents to in:	stall		
Selection location for CxSAST Select CxSAST components a	Installation	\Program Files\C	heckmarx		Select
Manages all CxSAST compon	ents		Install Audit Client for creating and	customizing queries	
Web Install Web Portal Web Interface with CxSAST			Install shortcuts Install CxSAST shortcu	uts on your desktop	
Performs code scans					
			(васк	NEXT

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

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

Select the required product features for this installation from the available list.

Ì	Product Feature Selection:

- POC/Evaluation Select to install Audit, Engine, Manager and WebPortal
- Distributed Architecture Select to install either Engine or Manager and/or WebPortal
- Centralized Architecture Select to install Engine, Manager and WebPortal (select Audit – see the <u>CxAudit Guide</u>, if you plan to create and customize queries on the host)
- **CxEngine Server only** Select to install Engine (see <u>Adding a CxEngine Server</u>).

Click NEXT to continue. The SQL Server Configuration window is displayed.



		OPTIONS		SUMMARY	FINISH
SQL Server Con Configuration allows you to de	figuration efine which SQL Serve	r connection i	nethod to use		
Select server from list: localhost\SQLEXPRESS					
Select connection method:					
 Connect using Integrate Login not required 	d Windows Authentic	ation	Connect using SQL Provide SQL User Name system administration p	Server authentica and Password for log ermissions	tion in with
Test Server Connection: Test Connection					
			(ВАСК	NEXT

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).



		options		SUMMARY	FINISH
SQL Server Con Configuration allows you to de	figuration	er connection :	method to use		
Select server from list:					
localhost\SQLEXPRESS					
Select connection method:					
Connect using Integrated Login not required	l Windows Authentic	ation o	Connect using SQL Provide SQL User Name system administration p	Server authenticat and Password for log vermissions	ion in with
Test Server Connection:		SQL	. User Name:	SQL Passwor	d:
Test Connection		Sé	1	*****	
			(ВАСК	NEXT

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

i SQL Server Connection Failure

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

Click **NEXT** to continue.

If previously installed SQL Express files are found in the system, an additional **SQL Server Configuration** window is displayed.

i Existing SQL Express Files

Define an SQL Express installation type by selecting one of the following:

- Install SQL Server Express using existing files
- Perform clean installation of SQL Server Express

Once complete, the License Activation window is displayed.



		OPTIONS		SUMMARY	FINISH
License Activat	to define which lice	nsing method to	use		
Select preferred licensing me	ethod:				
• Import New License Select if you already have a v	alid CxSAST license	С	Request New Lice Select if you have not license	nse yet obtained a perma	inent CxSAST
Locate your license	Import License				
			(ВАСК	NEXT

i Upgrade and Existing License

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

Select the preferred licensing method by selecting one of the following:

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



		OPTIONS		SUMMARY	FINISH
License Activat	to define which lice	nsing method to	use		
Select preferred licensing me	thod:				
O Import New License Select if you already have a v	alid CxSAST license	Q	Request New Licen Select if you have not y license	nse yet obtained a perma	nent CXSAST
		н	D:	1	
			#23812437441149552	7008_000 Copy t	o Clipboard
			(ВАСК	NEXT

i License Importer

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

Click **NEXT** to continue.

(i) HID Mismatch

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

Please import a different license or request for a new one from your Checkmarx sales representative or contact <u>Checkmarx support</u>.

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



i Default Port 80 Validation

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

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

If required, select another port and click Validate Port.

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

		OPTIONS		SUMMARY	FINISH
Setup Summary	y	54			
Displays setup summary acco	ording to your selec	tion			
Installed Components:		In	stallation Location:		
• Audit		С	:\Program Files\Checkm	arx	
• Engine • Manager • WebPortal					
License Details:					
Licensed Users :10 Licensed Audit users :2 Licensed concurrent scans :2 Licensed Projects :1000000 OSA :Enabled CxSAST Expiration date :12/30/20	018				
			(васк	INSTALL

Check the setup summary according to your selection.

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



	OPTIONS		SUMMARY	
	17%			
	17%			
Instal	lation in	progress		

Once complete the Installation Completed Successfully window is displayed.





i) Setup Failed

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

Click **Close** and perform a restart to complete the installation.

Installed Services Check

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

File Action View	/ Help					
🔶 🌒 🗐 🗐	Q 🛃 🛛 📷 🕨 🔳 I	L D				
Services (Local)	Name	Description	Status	Startup Type	Log On As	
	Credential Manager	Provides secure storage and retrieval of Provides four management services: Ca	Started	Manual Automatic	Local System Network Service	
	🙀 CxlobsManager	Service of Checkmarx Jobs Manager	Started	Automatic	Network Service	
	🕼 CxScanEngine	Service of Checkmarx Scan Engine	Started	Automatic	Network Service	-
	CxScansManager	Service of Checkmarx Scans Manager	Started	Automatic	Network Service	
	🔍 CxSystemManager	Service of Checkmarx System Manager	Started	Automatic	Network Service	
	DCOM Server Process	The DCOMLAUNCH service launches C	Started	Automatic	Local System	
	🔍 Desktop Window Man	Provides Desktop Window Manager star	Started	Automatic	Local System	
	DHCP Client	Registers and updates IP addresses and	Started	Automatic	Local Service	
	Diagnostic Policy Serv	The Diagnostic Policy Service enables pr	Started	Automatic	Local Service	
	Extended Standard					

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

Make sure the following installed services are started:

On a centralized host:

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

On a CxEngine host:

• CxScanEngine



Installed Application Pool Check

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



Make sure the following installed application pools are started:

On a centralized host:

- CxClientPool
- CxPool
- CxPoolRestAPI

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

Enable Long Path Support in CxSAST Application

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

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

<httpRuntime targetFramework="4.6.2" />



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

For example:

<system.web>

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

(i) If the httpRuntime already exists, add the targetFramework attribute as follows:

```
<httpRuntime maxRequestLength="2097151"
executionTimeout="36000" targetFramework="4.6.2" />
```

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

Login to the Web Interface

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

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

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

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

- Administrator User Name
- Password
- Confirm Password



2	Administrator User Name	
04	Password	\odot
a,	Confirm Password	

i Password Complexity

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

Click **Confirm** to complete.

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

In a distributed architecture:

Go to Management > Application Settings > Installation Information, and click Add Engine Server.

Give the CxEngine a **Server Name**, provide the **Server URL**, so that CxManager will be able to communicate with CxEngine and optionally define **Scan LOC Limits** (maximum lines of code allowed).

Server URI;			C 4 1 2 20 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
			Server URI;
* Scan LOC limits: from: to:	to:	from:	Scan LOC limits:

The URL should be:

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



i URL Check

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

Click Create.

Multiple CxEngine Servers:

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

Go to **Management** > **Application Settings** > **General**.

CHECKMARX V 8.6.0 [SDLC] Dashboard -	ि Projects & Scans →	چ Management +	යිලා My Profile	Coach AppSec Coach	admin admin U Logout		
Management / Application Settings / General							
Server Settings							
Reports Folder	C:\CxReports						
Results Folder	C:\Program F	C:\Program Files\Checkmarx\Checkmarx Jobs Manager\Results					
Executables Folder	C:\Program F	C:\Program Files\Checkmarx\Executables					
Path to GIT client executable	C:\Program F	C:\Program Files\Git\bin\git.exe					
Path to Perforce command-line client executable	C:\Program F	iles\Perforce\p4.exe					
Maximum number of concurrent scans	2 \$						
Web Server Address			Use Current				
Long Path Support							
Default Server Language	English (Unit	ed States)			v		

Click Edit.

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

Provide **SMTP** settings and click **Update**. Other settings should usually be left as they are.

Optionally, you can configure the "From" field of emails. If you don't configure it, it will be left empty."

Enable Long Path Support in Server Settings

In order for the long path feature to be fully supported in CxSAST, the following Long Path parameter needs to be enabled in the CxSAST Server Settings.

To enable the Long Path parameter in CxSAST:



Go to Management > Application Settings > General > Server Settings.

Click Edit and check the Long Path Support checkbox.

Click Update to save the changes.

Email Verification

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

Installation Verification

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

.0 [SDLC])ashboard 🛨	hboard 👻 Projects & Scans 👻 Management 👻		hboard 👻 Projects & Scans 👻 Management 👻 Users & Teams 👻 Data Analysis My Pro		My Prof	ìle	AppSec Coach	С,
ement / Application Settings	: / Installation Inf	ormation		0		d.			
-System Components									
sjoten osniponento									
							0 V	Filters 🖽 Group	By O
NAME	INSTALLA	TION PATH		DNS	IP	VERSION	HOTFIX	STATE	
CheckmarxWebPortal	C:\Progra	m Files\Checkmarx\Check	marxWebPortal\	Davidp-LapTop	10.31.0.121	8.6.0	0	1,2	
Checkmarx Audit	C:\Program	m Files\Checkmarx\Check	marx Audit\	Davidp-LapTop	10.31.0.121	8.6.0	0		
Checkmarx Web Services	C:\Program	m Files\Checkmarx\Check	marx Web Services\	Davidp-LapTop	10.31.0.121	8.6.0	0		
Checkmarx System Manag	er C:\Program	m Files\Checkmarx\Check	marx System Manager\	Davidp-LapTop	10.31.0.121	8.6.0	0		
Checkmarx Scans Manage	r C:\Program	m Files\Checkmarx\Check	marx Scans Manager\	Davidp-LapTop	10.31.0.121	8.6.0	0	On	
Checkmarx Jobs Manager	C:\Program	m Files\Checkmarx\Check	marx Jobs Manager\	Davidp-LapTop	10.31.0.121	8.6.0	0	On	
Checkmarx Engine Server	C:\Program	m Files\Checkmarx\Check	marx Engine Server\	Davidp-LapTop	10.31.0.121	8.6.0	0		

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.



CxSAST Silent Install / Uninstall

The CxSAST silent install / uninstall enables you to specify property values from the command line (CLI) and is ideal for part of a large-scale enterprise deployment. This method gives you the ability to perform a clean install, upgrade and uninstall of CxSAST silently (without constant interaction or prompts).

Syntax

CxSetup.exe /install /quiet ENGINE=1 MANAGER=1 WEB=1 AUDIT=1 INSTALLFOLDER="d:\Cx" INSTALLSHORTCUTS=1 SQLAUTH=1 SQLSERVER=192.168.0.0\SQLEXPRESS SQLUSER=sa SQLPWD=12345

Parameters

Parameter	Description
/?	Opens the help dialog.
/install /quiet	Installs CxSAST silently (Install is the default).
/uninstall /quiet	Uninstalls CxSAST silently.
INSTALLFOLDER=	Sets the installation directory path (e.g. INSTALLFOLDER="D:\TEMP DIR", INSTALLFOLDER=D:\TEMP)
ENGINE=	Sets Engine component variable with 1 to install, or 0 to remove\not install (ENGINE=1 is the default)
MANAGER=	Sets Manager component variable with 1 to install, or 0 to remove\not install. (MANAGER=1 is default)
WEB=	Sets Web component variable with 1 to install, or 0 to remove\not install (WEB=1 is the default).
AUDIT=	Sets Audit component variable with 1 to install, or 0 to remove\not install (AUDIT=1 is the default).
INSTALLSHORTCUTS=	Sets application shortcuts variable with 1 to install shortcuts, or 0 to not install shortcuts (INSTALLSHORTCUTS=1 is the default).



MSSQLEXP=	Sets whether to install MS SQL express on the local machine (assuming external SQL server is used) with 1 to install, or 0 not to install (MSSQLEXP=0 is the default).
	NOTES:
	 When defining 1 (Install), if CxActivity and CxDB already exists on the file system. Installation will reinstall CxDB and CxActivity and all existing data will be erased. MS SQL express will not be installed even if the variable is set to 1 when an existing deployment is found.
SQLSERVER=	Sets the SQL server address (e.g. SQLSERVER= localhost\SQLEXPRESS)
SQLAUTH=	Sets the SQL authorization credential. (e.g. SQLAUTH=1) NOTE: When SQLAUTH is not set to 1 SQLUSER and SQLPWD are ignored.
SQLUSER=	Sets SQL user credential (e.g. SQLUSER=sa)
SQLPWD=	Sets the SQL password credential (e.g. SQLPWD=12345)
LIC=	Sets the license path (e.g. LIC="C:\Users\Administrator\Documents\license.cxl"). Note - If the license check fails, the license will not be installed.
PORT=	Sets the port definitions (PORT=80 is the default)

Remarks

- The default silent installation command is <Path-To-Installer-File> /install /quiet
- By default most options and components are set to 1 (enabled).
- By default Microsoft SQL Express will not be installed (MSSQLEXP=0).



Examples

To perform a silent install with all components and with shortcuts to d:\Cx

CxSetup.exe /install /quiet ENGINE=1 MANAGER=1 WEB=1 AUDIT=1
INSTALLFOLDER="d:\Cx" INSTALLSHORTCUTS=1

To perform a silent install with only Manager Component and with no shortcuts to d:\Cx

CxSetup.exe /install /quiet ENGINE=0 MANAGER=1 WEB=0 AUDIT=0
INSTALLFOLDER="d:\Cx" INSTALLSHORTCUTS=0

To perform a silent install to a default location with all components – using SQL authentication:

CxSetup.exe /install /quiet SQLAUTH=1 SQLSERVER=192.168.0.0\SQLEXPRESS SQLUSER=sa SQLPWD=12345

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

CxSetup.exe /install /quiet ENGINE=0 MANAGER=1 WEB=0 AUDIT=0 SQLAUTH=1 SQLSERVER=192.168.0.0\SQLEXPRESS SQLUSER=sa SQLPWD=12345

To perform a silent uninstall:

CxSetup /uninstall /quiet



Modifying CxSAST

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

To modify CxSAST:

Make sure there are no scans currently running.

Stop all Cx Windows services:

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

i) Backup

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

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



Control Panel Home View installed updates Turn Windows features on or	Uninstall or change a program To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.					
off	Organize - Uninstall/Chan)EE 🔹 🌘			
Install a program from the network	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)
	CitHub	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	
	•	m			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	۶

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

		OPTIONS		summary	FINISH
Setup Options Step-by-step guide to uninstall	CxSAST, repair or	modify your setu	p		
	(Choose your setu	p type:		
Ū		Þ		Ø	
Remove CxSAST from your system		Repair your Cx setup	SAST	Modify yo CxSAST se	ur tup
UNINSTALL		REPAIR		MODIFY	



Click **MODIFY**. The additional **Setup Options** window is displayed.

				SUMMARY	FINISH			
Installation Opl	tions	emponents to in	stall					
Selection location for CxSAST Select CxSAST components a	r Installation	\Program Files\C	heckmanx		Select			
Manages all CxSAST compor	ients		Install Audit Client for creating and	customizing queries				
Install Web Portal Web interface with CxSAST	Install Web Portal Web interface with CxSAST			Install shortcuts Install CxSAST shortcuts on your desktop				
Install Engine Performs code scans								
			(BACK	NEXT			

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

Click **NEXT** to continue. The **SQL Server Configuration** window is displayed.



		OPTIONS		SUMMARY	FINISH
SQL Server Con	figuration	reconnection	method to use		
Select server from list:	nne which SQL Serve	Connection	metriod to use		
Select connection method:					
 Connect using Integrated Login not required 	l Windows Authentic	ation _O	Connect using SQL Provide SQL User Name system administration p	Server authentica and Password for log ermissions	tion jin with
Test Server Connection:					
			(ВАСК	NEXT

In the SQL Server Configuration window, 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).



				SUMMARY	FINISH		
SQL Server Con	figuration						
Configuration allows you to def	fine which SQL Server o	connection i	method to use				
Select server from list:							
localhost\SQLEXPRESS					•		
Select connection method:							
O Connect using Integrated	Windows Authenticati	ion o	• Connect using SQL Server authentication Provide SQL User Name and Password for login with system administration permissions				
Test Server Connection:		SQL	User Name:	SQL Passwor	rd:		
Test Connection		sa		•••••			

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

i SQL Server Connection Failure

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

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



		OPTIONS		SUMMARY	FINISH
Setup Summary Displays setup summary account	rding to your selec	tion			
Installed Components:		In	stallation Location:		
• Audit • Manager • WebPortal		С	\Program Files\Checkm	arx	
			(васк	INSTALL

Check the setup summary according to your selection.

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



			SUMMARY	
	17%)		
	C			
Instal	lation in	progress		

i Setup Failure

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

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





Click **RESTART** to complete the installation.



Repairing CxSAST

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

To repair CxSAST:

Make sure there are no scans currently running.

Stop all Cx Windows services:

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

(i) Backup

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

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



Control Panel Home View installed updates Turn Windows features on or	Uninstall or change a program To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.					
off	Organize 👻 Uninstall/Change					2
Install a program from the network	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	
	CitHub	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	
	1	III				F

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

		OPTIONS		SUMMARY	FINISH
Setup Options Step-by-step guide to uninstall	CxSAST, repair or	modify your setu	p		
	(Choose your setu	p type:		
		ß		Ø	
Remove CxSAST from your system		Repair your Cx setup	SAST	Modify yo CxSAST se	ur tup
UNINSTALL		REPAIR		MODIFY	



Click **REPAIR**. The **Repair in Progress** window is displayed.



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





Click **CLOSE** to complete the installation.



Backing Up CxSAST

The following page describes the backup and recovery procedures for CxSAST

Backing up CxSAST

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

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

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

Stop the CxJobsManager, CxScansManager, CxSystemManager and CxScanEngine services (this depends on the Cx components installed on the server)

Q Services							
Ele Action View	Help						
(+ +) 🔽 🔛	G 🔒 🚺 📷 🕨 🖩 II 🕪						
Services (Local)	Q. Services (Local)	3					
	Background Intelligent Transfer	Name +	Description	Status	Startup Type	Log On As	
	Service	Computer Browser	Maintains a	10	Disabled	Local System	
	AND CARD TO STATE	Credential Manager	Provides s		Manual	Local System	
	Stop the service Restart the service	Cryptographic Serv	Provides fo	Started	Automatic	Network S	11
	CONSTANCE OF AND	CriscanEngine	Service of	Started	Automatic	Network S	
	And the second se	CoScanManager	Service of	Started	Automatic	Network S	
	Description: Transferr flat is the backets ad using	DCOM Server Proc	The DCOM	Started	Automatic	Local System	

Stop the IIS Web Server

Internet Information Servi	ces (IIS) Manager	
00		i a ≥ 5 i 0 •
Ele Yew Help		
Connections	ATH TRAINDENVIL Home	Actions
Q- [] [] []	WIN-TRAINFSIVON Home	Manage Server
Sart Page	Filter:	C Restart
Application Pools	ASPINET	Start
	MET NET NETError NET NET Fruit Application Connection	View Application Pools View Sites
	Authorizati Compliation Pages Globalization Levels Settings Strings	1 Help

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

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

Backup the CxDB and CxActivity SQL databases using standard Database tools

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

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



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

Start the CxJobsManager, CxScansManager, CxSystemManager and CxScanEngine services

Start the IIS Web Server

Recovering CxSAST

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

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

(i) If CxSAST exists and is working please start from the second step.

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

Stop the CxJobsManager, CxScansManager, CxSystemManager and CxScanEngine services (this depends on the Cx components installed on the server)

Stop the IIS Web Server

Move/rename the Checkmarx folder

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

Restore the Checkmarx folder

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

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

Restore the database

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



Restore the scanned source folder

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

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

Start the CxJobsManager, CxScansManager, CxSystemManager and CxScanEngine services (this depends on the Cx components installed on the server)

Start the IIS Web Server

Check the recovered version

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

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

(i) Should you need any further assistance, please contact <u>Checkmarx support</u>.



Upgrading CxSAST

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

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

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

To upgrade CxSAST:

Make sure that there are no scans currently running.

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

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

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

Installing CxSAST

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


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

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

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

The following files should be backed-up and used if you are unable to find or connect to the database during installation:

"X:\Program Files\Checkmarx\Configuration\DBConnectionData.config"

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

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

- CxSystemManager
- CxJobsManager
- CxScansManager
- CxScanEngine
- Web server (run "iisreset" from elevated CMD or Start action for the server name in IIS Console).



Adding a CxEngine Server

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

Prepare the environment for the new CxEngine

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

				SUMMARY	FINISH
Installation Opt	tions	omponents to in	stall		
Selection location for CxSAST Select CxSAST components a	Finstallation	:\Program Files\C	heckmarx		Select
Install Manager Manages all CxSAST compon	ients	C	Install Audit Client for creating and	customizing queries	
U Install Web Portal Web interface with CxSAST		C	Install shortcuts	uts on your desktop	
Install Engine Performs code scans					
50		.97	(ВАСК	NEXT

Engine Servers do not require a separate license. You should continue the installation without importing the license. The existing CxSAST license should then be copied from CxManager to each Engine using the License Importer tool (Start > Checkmarx > CxLicenseImporter.exe).

Log into the <u>CxSAST web interface</u>.

Go to **Management** > **Application Settings** > **Installation Information**, and click **Add Engine Server**. The Add Engine Server window is displayed.



Server Name:				
Server URI:				
Scan LOC limits:	from:	to:		

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

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

Click Create.

i) On	ce the new engine is installed, you may need to:
•	Increase the number of concurrent scans allowed (Application Settings > Application Management > Server Settings > Maximum number of concurrent scans). See
	Application Management for more information.
	- and/or -
•	Import a new license with more scans (Start > All Programs > Checkmarx > HID). See <u>Updating the CxSAST License</u> for more information.

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



Uninstalling CxSAST

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

To uninstall CxSAST from a server host:

Copy your CxSAST license file to a safe location.

Make sure that there are no scans currently running.

Stop all Cx Windows services:

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

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

Control Panel	 Programs Programs and Feat 	ures	▼ *† Se	arch Programs o	and Features	ş.
Control Panel Home View installed updates	Uninstall or change a To uninstall a program, sele	program ct it from the list and then click Uninst	all, Change, or	Repair.		
Turn Windows features on or off						
Install a program from the	Organize 🔹 Uninstall/Change 🛛 🔠 💌					2
network	Name	Publisher	Installed On	Size	Version	
	Screate 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	
	oit 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	
	1	m				,



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

		OPTIONS		SUMMARY	FINISH
Setup Options Step-by-step guide to uninstall	CxSAST, repair or	modify your setu	p		
	c	Choose your setu	p type:		
Ū		Þ		\mathcal{O}	
Remove CxSAST from your system		Repair your Cx setup	SAST	Modify you CxSAST setu	ц ц
UNINSTALL		REPAIR		MODIFY	

Click UNINSTALL. The Uninstall in Progress window is displayed.





Once complete, the Uninstall Successfully Completed window is displayed.



Click **Close** to complete the uninstall.

i Renewal

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

- CxSrc
- CxDB (SQL)



Updating the CxSAST License

To obtain a new or updated Checkmarx license for CxSAST:

Go to Start > All Programs > Checkmarx, click HID

0	Windows DVD Maker		
	Windows Fax and Scan		
8	Windows Media Center		
0	Windows Media Player		
P	Windows Update		
-	XPS Viewer		
Accessories			
	AVG		
	Bamboo		
	CCleaner		
34	Checkmarx		
	🔍 Checkmarx Audit		
	🕑 Checkmarx Portal		
	😪 CxLicenseImporter.exe		
	📋 HardwareId		
	🕑 HID		
	Dolby		
	Eclipse		
	Games		
	Git		
1	Back		
٢	Search programs and files		

Once the Hardware ID is generated, copy the **HardwareId** and send it to your Checkmarx sales representative or <u>Checkmarx support</u> to obtain a new or updated license.

i Distributed Installations

Updating the license on each machine is required in case of <u>distributed architecture</u> installations.

Close all Checkmarx Application windows.

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





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

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

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

① The database (DB) is required to be up and running in order for Checkmarx services to be able to run.

Restart all Cx Windows services:

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



CxSAST Application Maintenance Guide

- Introduction
- Backup
 - Step 1. Stop the CxServices
 - Step 2. Stop the Web Server
 - Step 3. Back up the Checkmarx Folder
 - Step 4. Backup the Database
 - Step 5. Backup the Scanned Source Folder
 - Step 6. Restart the CxServices
 - Step 7. Restart the Web Server
- Recovery
 - Step 1. Stop the CxServices
 - Step 2. Stop the Web Server
 - Step 4. Restore the Scanned Source Folder
 - Step 5. Restore the Database
 - Step 6. Restart the CxServices
 - Step 7. Restart the Web Server

• Maintenance and Cleanup

- CxManager
 - Sources
 - CxSrc
 - ExtSrc
 - Logs
 - Reports
- CxEngine
 - Sources
 - CxSrc
 - Logs
 - Scans
- CxWebPortal
 - Logs
- o **CxAudit**
 - Sources
 - CxAuditSrc
 - Logs
- Database
- Appendix A: Compressing a Folder in Windows
 - o Trade-Offs
 - \circ $\;$ When to Use and When Not to Use NTFS Compression
 - How to Use NTFS Compression



Introduction

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

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

CxSAST is comprised of the following main components:

Backup

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

Step 1. Stop the CxServices

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

Step 2. Stop the Web Server

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



Step 3. Back up the Checkmarx Folder

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

Copy the following items from the Checkmarx folder:

- Configuration, Executable and Licenses folders and the following configuration files:
- Checkmarx Audit\CxAudit.exe.config
- Checkmarx Audit\Config.xml
- Checkmarx Audit\ExtensionsConfig.xml
- Checkmarx Audit\Log4Net.config
- Checkmarx Engine Server\CxEngineAgent.exe.config
- Checkmarx Engine Server\CxSourceAnalyzerEngine.WinService.exe.config
- Checkmarx Engine Server\ExtensionsConfig.xml
- Checkmarx Engine Server\CxEngineLog4Net.config
- Checkmarx Engine Server\Logs4Net.config
- Checkmarx Jobs Manager\bin\CxJobsManagerWinService.exe.config
- Checkmarx Jobs Manager\bin\CxJobsManagerLog4Net.Build.config
- Checkmarx Jobs Manager\bin\CxJobsManagerLog4Net.config
- Checkmarx Scans Manager\bin\CxScansManagerWinService.exe.config
- Checkmarx Scans Manager\bin\CxScansManagerLog4Net.config
- Checkmarx System Manager\bin\CxSystemManagerService.exe.config
- Checkmarx System Manager\bin\CxSystemManagerLog4Net.config
- Checkmarx Web Services\CxWebInterface\Web.config
- Checkmarx Web Services\CxWebInterface\Log4Net.config
- Checkmarx WebPortal\Web\Web.config
- Checkmarx WebPortal\Web\Log4Net.config
- Configuration\ExtensionsConfig.xml

Step 4. Backup the Database

Backup the database using the standard database tools.

Step 5. Backup the Scanned Source Folder

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

Step 6. Restart the CxServices

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

Step 7. Restart the Web Server

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



Recovery

Step 1. Stop the CxServices

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

Step 2. Stop the Web Server

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

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

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

Step 4. Restore the Scanned Source Folder

Copy the CxSrc folder from the backup overwriting the new empty folder: Example: C:\CxSrc15052016 - > C:\CxSrc

Step 5. Restore the Database

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

Step 6. Restart the CxServices

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

Step 7. Restart the Web Server

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

Step 8. Check the Recovered Version

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

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



Maintenance and Cleanup

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

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

CxManager

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

Sources

CxSrc

Default location: C:\CxSrc

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

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

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

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

ExtSrc

Default location: C:\ExtSrc

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

Logs

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

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





Default location: C:\CxReports

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

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

CxEngine

Sources

CxSrc

Default location: C:\CxSrc

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

Logs

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

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

Scans

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

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

CxWebPortal

Logs

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

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



CxAudit

Sources

CxAuditSrc

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

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

Logs

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

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

Database

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

Appendix A: Compressing a Folder in Windows

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

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

Trade-Offs

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

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

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

This is especially true as NTFS compression isn't very aggressive in its compression. <u>A test by</u> <u>Tom's Hardware</u> 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 <u>solid state drives</u>. (Warning: Using compression will result in more writes to your solid state drive, potentially decreasing its life span. However, you may gain some more usable space.)
- Computers with fast CPUs and slow hard disks.

NTFS compression should not be used for:

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

How to Use NTFS Compression

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

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

Click the Advanced button under Attributes.

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

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

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

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

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

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



CxSAST Database Maintenance Guide

In this guide:

- Chapter 1 Introduction Maintenance
- Chapter 2 Checkmarx Tables Overview
- Chapter 3 Monitoring
- Chapter 4 Maintenance Options for Reducing Fragmentation

Chapter 1 - Introduction

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

There are basically two types of fragmentation:

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

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

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

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



Chapter 2 - Checkmarx Tables Overview

The CxSAST application has two databases:

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

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

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

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

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

Chapter 3 - Monitoring

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



SELECT

OBJECT_NAME(ips.object_id)

"TblName"

,ips.object_id

,ips.index_id

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

,ips.index_type_desc "IndexType" ,ips.avg_fragmentation_in_percent ,ips.fragment_count ,ips.avg_fragment_size_in_pages ,ips.forwarded_record_count ,ips.alloc_unit_type_desc ,ips.page_count ,ips.index_depth ,ips.avg_page_space_used_in_percent ,ips.record_count ,ips.ghost_record_count ,ips.version_ghost_record_count ,ips.min_record_size_in_bytes ,ips.max_record_size_in_bytes ,ips.avg_record_size_in_bytes ,ips.compressed_page_count



FROM sys.dm_db_index_physical_stats(DB_ID('CxDB'),NULL,NULL,'<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 <u>https://msdn.microsoft.com/en-us/library/ms188917(v=sql.110)</u>.

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			
	This indicates the amount of external fragmentation you have for the given objects.			
avg_fragmentation_in_percent	The lower the number the better - as this number approaches 100% the more pages you have in the given index that are not properly ordered.			
	For heaps , this value is actually the percentage of extent fragmentation and not external fragmentation.			
	This indicates how dense the pages in your index are, i.e. on average how full each page in the index is (internal fragmentation).			
avg_page_space_used_in_percent	The higher the number the better speaking in terms of fragmentation and read-performance. To achieve optimal disk space use, this value should be close to 100% for an index that will not have many random inserts. However, an index that has many random inserts and has very full pages will have an increased number of page splits. This causes more fragmentation. Therefore, in order to reduce page splits, the value should be less than 100%.			
fragment_count	A fragment is made up of physically consecutive leaf pages in the same file for an allocation unit. An index has at least one fragment. The maximum fragments an index can have are equal to the number of pages in the leaf level of the index. So the less fragments the more data is stored consecutively.			
avg_fragment_size_in_pages	Larger fragments mean that less disk I/O is required to read the same number of pages. Therefore, the larger the avg_fragment_size_in_pages value, the better the range scan performance.			
forwarded record count	Number of records in a heap that have forward pointers to another data location. (This state occurs during an update, when there is not enough room to store the new row in the original location.)			
v <u> </u>	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
		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.
ALTER INDEX REORGANIZE	> 10% and < = 30%	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
		Rebuilding an index can be executed online or offline. To achieve availability similar to the reorganize option, you should rebuild indexes online.
ALTER INDEX REBUILD WITH (ONLINE = ON)	> 30%	The ONLINE option and parallelism are available for Enterprise Edition only! When performed offline, the entire table is unavailable for the duration of the operation.
		Defragments all levels of the index and update statistics.



Important notes:

- There are other methods (e.g. drop and recreate cluster index), but are more complicated and less recommended.
- Fragmentation alone is not a sufficient reason to reorganize or rebuild an index. The main effect of fragmentation is that it slows down page read-ahead output during index scans. This causes slower response times. If the query workload on a fragmented table or index does not involve scans, because the workload is primarily singleton lookups, removing fragmentation may have no effect.
- These values (in **When** column compared with **avg_fragmentation_in_percent**) provide a rough guideline for determining the point at which you should switch between ALTER INDEX REORGANIZE and ALTER INDEX REBUILD. However, the actual values may vary from case to case. It is important that you experiment to determine the best threshold for your environment. Very low levels of fragmentation (less than 5%) should not be addressed by either of these commands because the benefit from removing such a small amount of fragmentation is almost always vastly outweighed by the cost of reorganizing or rebuilding the index. The decision should be take into consideration SQL Server Edition.
- In general, fragmentation on small indexes is often not controllable. The pages of small indexes are stored on mixed extents. Mixed extents are shared by up to eight objects, so the fragmentation in a small index might not be reduced after reorganizing or rebuilding the index.



CxSAST Quick Start

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

In this s	In this section:									
•	Setting	ς Up								
	0	Step 1: Enter Project General Settings								
	0	Step 2: Select Source To Scan								
	0	Step 3: Scan Execution								
•	Reviewing Scan Results									
	0	Step 1 – Projects & Scans								
	0	Step 2 – Review Scan Results in the Source Code								
•	Preset	Manager: Overview								



Setting Up

Δ

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

Step 1: Enter Project General Settings

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

.xpiica. 0/10/2010	 Projects & Scans - 	Management +	Users & Teams 👻	Data Analysis	یجی۔ My Profile	Codebashing	Services & Support	
ojects & Scans / New Project	91	o Al-			19	1		
General	Location	scheduling	Advan	Iced Actions	Custom Fields	Data Ki	etention	
	Step 1: Enter	Project General Settings						
	Project Name	Project 3 (CxOSA)		0				
	Preset	Checkmarx Default		0				
	Configuration	Default Configuration	n 🔻	0				
	Team	CxServer	v	0				

Step 2: Select Source to Scan

- 1. Select **Local** to upload code as a ZIP file. The code must be zipped by MS zip. The test account is limited to 350,000 Lines of Code (LOC).
- 2. Select **Shared**, **Source Control** or **Source Pulling**, and upload the code in any other format.



CHBCKMARX V 8.8.0 [SDLC] Expires: 6/13/2018	C/ Dashboard +	[]_ Projects & Scans →	Management +	د Users & Teams →	📿 Data Analys	is	Cos My Profile	Services & Supp	admin admin bort 🖒 Logout
Projects & Scans / New Proje	ct				1				
G	eneral	Location	Scheduling	a Advar	nced Actions	5	Custom Fields	Data Retention	
		Step 2: Choose	Source To Scan						
		Local	WebGoat-5.4_	117234_lines.zip	Select	0	Count Lines		
		O Shared			Select	0			
		O Source Contro	d		Select	0			
		O Source Pulling	1		Select	0			
		Exclude Folders				(?)			
		Exclude Files							
			a Date New	. Dennel X	Elaish a				
			Back Nex	t V Cancel	Finish V				
				© 2018 Checkmarx	Тор				

- Note that you can scan the "OWASP Benchmark Project" code; go to <u>https://github.com/OWASP/benchmark</u>, click the Clone or download button and select your preferred option.
 - 3. Other sample code for scanning include:

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

- 4. If using a Browser/ Eclipse/ Visual Studio/ IBM RAD, please start with the browser option.
- 5. When the Finish button becomes active, click **Finish** to place the project into a queue.



Step 3: Scan Execution

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

CHBCKMARX V 8.8.0 [SDLC] Expires: 6/13/2018	CA Dashboard -	C. Projects & Scans 👻	لمرجع Management -	کے Users & Teams 🗕	⊘ Data Analysis	යි My Profile	🤓 Codebashing	G Services & Support	admin admin U Logout
Projects & Scans / Queue									
POSIQUEUED DA1 6/11/2018 4 6/11/2018 4 6/11/2018 4	E T INITIAT 59:23 AM admin a 59:00 AM admin a 57:37 AM admin a	OR OF dmin Wi dmin Wi dmin Wi	RIGIN eb Portal eb Portal eb Portal	PROJECT NAME Project 1 (CxTecht Project 2 (CxTecht Project 3 (CxOSA)	SERVI Docs) Local Local	ER NAME host host	[LOC ST 6864 6838 0 21403 Fir	Filters T	Croup By O ACTIONS D 111 D 111 E C
	Page size: 10	×							3 items in 1 pages
Position									
Queued Date	6/11/2018 4:59:23 AM								
Initiator	admin admin								
Dverall ; Curren Stage # 24 of 83 DefaultCons	rogress 34%								
				© 2018 Checkman	с Тор				



Reviewing Scan Results

Step 1 – Projects & Scans

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

8.8.0 [SDLC] xpires: 6/13/2018	Dashboard -	C) Projects & Scans 🕞	کرچ Management –	요 Users & Teams 🕞	📿 Data Analysis	Co My Profile Co	odebashing	G Services & Support	admin admin U Logout
ojects & Scans / Projects									
+ Create New Project	Jelete						ß	√ Filters	Group By
PROJECT NAME	OWNER	TEAM	PRESET	TOTAL SCAN	LAST SCANNED -	SCANS LIST	ACTIONS		
Project 2 (CxTechDocs)	admin@cx	CxServer	Checkmarx Default	r 1	6/10/2018 7:05 AM		$\triangleright \triangleright \top$, D	
Project 1 (CxTechDocs)	admin@cx	CxServer	Checkmarx Default	с <u>1</u>	6/10/2018 6:09 AM		$\triangleright \triangleright \top$	0	
Billing	admin@cx	CxServer	Checkmarx Default	6 010	6/7/2018 4:23 AM	1	$\triangleright \triangleright \top$	• 🖻	
WEBGOAT_OSA_SCAN	admin@cx	CxServer	Default	0			$\triangleright \triangleright \forall$, D	
Project 3 (CxOSA)	admin@cx	CxServer	Checkmarx Default	t 0			$\triangleright \triangleright \forall$	• 🗅	
	'age size: 10 ▼								5 items in 1 pages
Monitoring General	age size: 10 💌	Scheduling Adv	anced Custom Fi	ields Data Retentic	n OSA				5 items in 1 pages
Monitoring General Vulnerabilities Vulnerabilities in high Medium (90 30 30 30 30 30 30 30 30 30 50 30 50 30 50 50 50 50 50 50 50 50 50 50 50 50 50	Location	Scheduling Adv	anced Custom Fi Risk Indicator	ields Data Retentio	n OSA				5 items in 1 pages
Monitoring General Vulnerabilities Vulnerabili	Page size: 10 Location Locw Info	Scheduling Adv	anced Custom Fi Risk Indicator ———— Last U	ields Data Retentio	n OSA				5 items in 1 pages

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

Step 2 – Review Scan Results in the Source Code

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

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

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



Scan Result Summary

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



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





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

/ Result St	tate 🔻	√ Result Se	verity 🖤	✓ Assign to Us	er 🔻 🖉 Com	ments 🛓 Sa	ve Scan Subset							D 7 Filter
] 1d		Query Name	Status	Source Folder	Source Filename	Source Line	Source Object	Destination Fold	Destination Files	Destination Line	Destination Obj	e Result State	Result Severity	Assigned User
0 1	P	Reflected	New	\admin_p	BookDetai	154	paramName	\admin_pa	BookDetai	858	print	To Verify	High	
2	00	Reflected	New	\admin_p	BookDetal	154	paramName	\admin_pa	BookDetai	1119	print	To Verify	High	
3	00	Reflected	New	\admin_p	BookDetai	154	paramName	\admin_pa	BookDetai	637	print	To Verify	High	
1	P	SQL_Injec	New	\admin_p	BookDetai	154	paramName	\admin_pa	BookDetai	49	executeQ	To Verify	High	
5	P	SQL_Injec	New	\admin_p	BookDetai	154	paramName	\admin_pa	BookDetai	731	executeUp	To Verify	High	
6	00	SQL_Injec	New	\admin_p	BookDetai	154	paramName	\admin_pa	BookDetai	958	executeUp	To Verify	High	
0 7	d ⁰	Second	New	\admin_p	Login_jsp	49	executeQ	\admin_pa	BookDetai	731	sSQL	To Verify	High	

• **Graph**: Gain a macro chart perspective vulnerabilities found in code, see correlations and identify the optimal points for fix (red buttons).





• **Attack Vector**: Note the full path of code elements that constitute the vulnerability instance selected in the Results pane.

getParameter	
٧	
param	
٧	
param	
٧	
getParam	
٧	
sSQL	
٧	
sSQL	
٧	
executeUpdate	

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



Preset Manager: Overview

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

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

CHBCKMARX V 8.8.0 [SDLC] Expires: 6/13/2018	(🔨 Dashboard 🖌	C) Projects & Scans 🗸	چې Management –	උදු Users & Teams	⊘ s → Data Analysis	යිා My Profile	Codebashing	G Services & Support	admin admin 🖒 Logout
Management / Scan Settings	/ Preset Manager			1		9			
Drag a column header and dro	p it here to <mark>group</mark> by tha	t column		F	Preset name Checkmarx Defau	lt			
+ Create New Preset E PRESET All Android Apple Secure Coding Guide Checkmarx Default Default 2014 Empty preset Error handling FISMA	2 Export Preset 2	Import Preset C	✓ Filters E Group OWNER □ □ □	by C ACTON Image: Comparison of the compariso	Image: Second_time I	n_Language_Injection_O ection _Injection order_SQL_Injection ttion SS ection ibility _Threat I	GNL .		
Query Description SQL_Injectio Risk What might happen An attacker could direct credit cards), and possib <	n Iy access all of the sy: Iy change or erase ex	stem's data. Using simple disting data.	e tools and text editin	ig, the attacker w	• ould be able to steal any se eckmarx Top	sitive information sto	red by the system (suc	ch as personal user detai	ls or

For more information on Managing Presets, see Managing Query Presets.



CxSAST User Guide

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



The CxSAST Web Interface



The Queue







Managing Projects

Creating and Scan Results





Page 105



The CxSAST Web Interface

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

In this section:

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



Accessing the Web Interface

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

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

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

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

- Administrator User Name
- Password
- Confirm Password

÷	Administrator User Name	
a.	Password	0
a,	Confirm Password	

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

Click **Confirm** to complete.

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



Getting to Know the System Dashboard

Overview

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

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

CHECKMARX V 8.8.0 [SDLC] Expires: 6/13/2018	(7/) Dashboard +	C3 Projects & Scans →	رچ Management -	요 Users & Teams 👻	📿 Data Analysis	N	کی Ay Profile		🛱 Services & Support	admin admin U Logout
Dashboard / Projects State	15 - 1316 -					.h.				
								1	0 ⊽ Filters €	Group By
PROJECT NAME	LAST SCAN DATE 🔻	TEAM	LOC	F	IISK LEVEL SCORE	1	HIGH VULNERAB	ILITIES MEDI	UM VULNERABILITIES	ACTIONS
Project 4 (CxOSA)	6/11/2018	CxServer	87967	10	[³⁰⁰	(100)	401	486		Q 🖗 🖪
Project 1 (CxTechDocs)	6/11/2018	CxServer	6864			(55) 5	5	20		QBQ
Project 2 (CxTechDocs)	6/11/2018	CxServer	6838			(47) 2	25	22		0, 🕼 🖪
Project 3 (CxOSA)	6/11/2018	CxServer	21403	6	¹⁰⁰	(79) 1	13	143		Q 🕼 🖪
Billing	6/7/2018	CxServer	10242	3	I***	(100) ;	384	300		QBD
WEBGOAT_OSA_SCAN	No SAST scans perform	ed CxServer	82	2	J ³⁰⁰	(-) -		12		Q. 🖗 🖪
	Page size: 10 🔻									6 items in 1 pages
				© 2018 Checkmarx	Тор					

- ① Visual indicators are displayed just underneath the Checkmarx logo/version and may include:
 - Type of product edition currently installed SDLC or Security Gate
 - Expiry date of the current CxSAST license. The indicator appears 90 days (defined in the DB) before the actual license expiry date and, if defined, an email notification is automatically sent to the CxSAST System Administrator.

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

CxSAST web interface menu items are described below.


Dashboard Menu

View the state of your engines, scans and queues:

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

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

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

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

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

Projects and Scans

View projects scans and queues:

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

Management Settings

Manage Scan and Server settings:

Scan Settings:

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



Connection Settings:

- LDAP Servers: Define an LDAP Server for your environment.
- **SAML Management**: Configure SAML for your environment.
- Issue Tracking Settings: Configure issue tracking.

Application Settings:

- **General:** Folder locations, SMTP, and other settings.
- License Details: The installed license details, including supported languages, roles, and number of companies and service providers.
- Installation Information: Locations of server components.
- External Services: Define settings for external services (e.g. Codebashing).
- Engine Management: Manage single/multiple engines

Maintenance:

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

Manage Custom Fields:

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

Users & Teams

Manage users and the user hierarchy:

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

Data Analysis

View and analyze scan-related data.

My Profile

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



Dashboard Menu

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

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

Project State

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

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

CHECKMARX V 8.8.0 [SDLC] Expires: 6/13/2018	(7) Dashboard +	Ca. Projects & Scans 🕞	رچ Management +	ے Users & Teams 🗕	☑ Data Analysis		යිනු My Profile	😇 Codebashing	Servic	😧 es & Support	admin admin U Logout
Dashboard / Projects State)t)/				<u>h</u> :		(3				
									(D) 7	Filters 🗄	Group By 🔘
PROJECT NAME	LAST SCAN DATE 🔻	TEAM	LOC		RI <mark>S</mark> K LEVEL SCORE		HIGH VULNERAB		EDIUM VULN	ERABILITIES	ACTIONS
Project 4 (CxOSA)	6/11/2018	CxServer	87967		°[¹⁰⁰	(100)	401	4	86		Q 🕼 Q
Project 1 (CxTechDocs)	6/11/2018	CxServer	6864		"""	(55)	5	2	0		QBQ
Project 2 (CxTechDocs)	6/11/2018	CxServer	6838		° ¹⁰	(47)	25	2	2		Q 🖗 🖪
Project 3 (CxOSA)	6/11/2018	CxServer	21403		° ¹⁰⁰	(79)	13	1	43		Q 🕼 🖪
Billing	6/7/2018	CxServer	10242		°I***	(100)	384	3	00		0.68 6
WEBGOAT_OSA_SCAN	No SAST scans performe	ed CxServer	82		°I	(-)	22	2			0. 🐼 🖪
(d d 1 b b)	Page size: 10 💌										6 items in 1 pages
				© 2018 Checkmarx	Тор						

The Project State window includes the following information:

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

You can Export as CSV File [19], use the [17] Filter and [19] Group By tools as well as

Refresh the current view.

① Projects that have not yet had scans performed on them are displayed in the Project State window the "No SAST Scans performed" message.



Failed Scans

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

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

CAN DATE =	PRO JECT NAME		100	COMMENTS	DETAILS			gi li rinters 18 d		NG
/11/2018 5:52:15 AM	WEBGOAT OSA SCAN	admin admin	0	COMMENTS	Failed to start scanning	due to one of following	reasons: source folde	r is empty, all source files a	. 6	110
/10/2018 6:26:21 AM	WEBGOAT_OSA_SCAN	admin admin	0		Failed to start scanning	due to one of following	reasons: source folde	r is empty, all source files a.	. 6	
/10/2018 6:22:58 AM	WEBGOAT_OSA_SCAN	admin admin	0		Failed to start scanning	due to one of following	reasons: source folde	r is empty, all source files a.	. G	
/7/2018 1:29:59 AM	Project 1 (CxTechDocs)	admin admin	18033		Scan failed due to insuff	icient memory. Engine s	erver has a total 4098	5 MB out of which only 0 MB	. B.	
/7/2018 1:27:36 AM	Project 1 (CxTechDocs)	admin admin	6836		Scan failed due to insuff	icient memory. Engine s	erver has a total 4098	5 MB out of which only 0 MB	G	

The Failed Scans window includes the following information:

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

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



Utilization

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

Go to **Dashboard > Utilization**. The Utilization window is displayed.



The Utilization window includes the following information:

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

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



Risk State

The Risk State window displays the number of vulnerabilities and the risk score for each project. Go to **Dashboard > Risk State**. The Risk State window is displayed.



The Risk State window includes the following information:

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

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

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

Click Project Name link to view Project State Summary

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

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



Consolidated Project State

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

To display the Consolidated Project State window:

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

CHECKMARX V 8.1.0 Expires: 5/30/2016	(7) Dashboard -	C). Projects & Scens -	🖉 Management 👻	C) Lisers & Teams -+	🕑 Data Analysis	Co My Profile			Welcome admin admin
Projects State / My Project 2			2						
< Back Projects Stat	te: MY PROJE	CT 2			⊳ Full	Scan	Incremental Scan	😁 Run OSA	Actions -
Summary	OSA (1)	Scans H	istory						
Current status (Public	Scan on 12/14/	2015 1:49:05 PM)							
SAST Vulnerabilities S	Status		SAST pr	ogress status			Open Source Ana	alysis (OSA) 🗇	Last Scan on 4/14/2016 1:49:05 PM
Hign Med Full Scan Results>	Low N Recur Base Made 834 New 0 Recurring	2824 New O Recurring	3000 2400 1800 1200 600	Previous 501ved	N Recurrent 1, 834	2,824	1 No Known Vi	ulnerabilites	1 Vulnerable & Outdated
To ouried (y)	HAT GUARDE (J)	Tank annan ()		13 . HISH	MED	LOW		Total 2 Li View Analysis	braries s Results >
				0.2	16 Checkmark				

Summary

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

- Full Scan perform a SAST scan for the whole project
- Incremental Scan perform a SAST scan for only new and modified files since the last scan
- **Run OSA** perform Open Source Analysis on predefined open source libraries associated with this project
 - (i) Note that a purchased or trial CxOSA license is required in order to run CxOSA projects. Please contact your Checkmarx Administrator.



- Additional Actions:
 - Edit Project displays the projects details
 - **Open Scan Summary** displays the scan summary
 - **Open Viewer** displays the scan results viewer

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

 ${\bf Current\ Status}$ - Includes the time/date stamp indicating the date and time of the last SAST scan

SAST Vulnerabilities Status

Provides a graph with the status of each vulnerability severity.

All new vulnerability instances discovered according to severity (high,

medium and low)

N - Recurring vulnerability instances from previous scan

Solved is defined as vulnerabilities fixed/solved since last scan

(i) If no scans have yet been performed a "No Scans Performed" message is displayed. For more details about projects and scans, refer to **Creating and Configuring Projects**.

If a new scan is currently in progress a "New Scan in Progress "message is displayed. For more details about the status of the scan, refer to the **Queue**.

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

SAST Progress Status

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

- All new vulnerability instances discovered according to severity (high,

medium and low)





N - Recurring vulnerability instances from previous scan



Open Source Analysis (CxOSA)

Provides open source analysis results for predefined open source libraries associated with this project. Includes a stamp indicating the date and time of the last analysis

(i) In cases where the open source analysis license has not yet been enabled, by clicking on the available link, you can view a sample of the Open Source Analysis report. Once the sample is displayed another link provides navigation to additional information about Open Source Analysis (<u>https://www.checkmarx.com/Open-Source-Analysis</u>).

Vulnerability Libraries - total number of libraries analyzed and a breakdown of the vulnerabilities recorded.

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

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

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

CxOSA (Open Source Analysis) Report

Click the OSA tab to display the Open Source Analysis Report. This report can also be generated to PDF format for download and print.

(i) The OSA tab is not available until after the first open source analysis has been completed.

Scan History

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



Viewing the Open Source Analysis Report

Once the Open Source Analysis has been performed, you can view the Open Source Analysis report. This report provides a high level summary of the status of the project.

To view the Open Source Analysis report:

Go to **Dashboard > Project State** and click the **View Analysis Results** link or select the **OSA** tab. The Open Source Analysis report is displayed.

CHECKMARX V 8.4.2 HF6 [SDLC]	(74) Dashboard +	C. Projects & Scans 👻	Management →	요 Users & Tearns ㅋ	🕢 Data Analysis	යි My Profile	Sec Coach	admin admin U Logout
Projects State / Project 3 (Cxt	DSA)		1					
Back Projects State: F	PROJECT 3 (CXO	SA)		> Full Scan	Incrementa	al Scan	Run OSA Acti	ons 🔻
Summary	OSA 🔊	Scans History						
pen Source Analysis	Report							
en Source Path: Analyzed fro	om portal						🕹 Dow	nload PDF
IST Analyzed On: 7/3/2017 2.1	9.15 PM							
Security								
Vulnerability Score		Vulnerable Libra	ries	Severity Di	stribution	Ag	ging Vulnerable Librar	es
	_	F	F	High 2			2	
нісі	ц			Med 0		_		
IIIG		0	2	Low 0				
		No Known Vulnerabilities	Vulnerable (2 Outdated)	23	/ulnerable Libraries		0	0 < 20 Dave
		- attraction theo	(a cardeted)				so bujo - so bays	- oo bays

CxOSA Report - Indicates the open source path and for which libraries the analysis was performed. Also includes the time/date stamp indicating the date and time of the last analysis.

Click the **Download PDF** button to generate and download a PDF version of the Open Source Analysis report. An "Open Source Analysis Report download is in progress" indicator is displayed.

(i) It is highly recommended that you generate the PDF version straight after creating the Open Source Analysis report in order to ensure consistency.

For information about performing the other available actions, i.e. Full Scan, Incremental Scan, Run OSA, Additional Actions, see <u>Consolidated Project State</u>.



Security

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

Vulnerability Score

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



Vulnerable Libraries

Distribution of the vulnerable libraries:

vunerable Libra	nes
	Đ
0	2
No Known Vulnerabilities	Vulnerable (2 Outdated)

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



Severity Distribution

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

High	2	
Med	0	
LOW	0	
		2 Vulnerable Libraries

Aging Vulnerable Libraries

Distribution of vulnerable libraries by timeline:

- > 90 days number of libraries that have at least 1 security vulnerability that was exposed more than 90 days ago
- < 90 days number of libraries that have at least 1 security vulnerability that was exposed in the last 90 days
- < 30 days number of libraries that have at least 1 security vulnerability that was exposed in the last 30 days



Security Vulnerabilities

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

Security Vulnerabilities (9)		
Vulnerability	Library	Description	Top Fix
High 10.0 CVE-2014-9495 10-01-2015	libpng-v1.5.10 (File: pngrutil.c)	Heap-based buffer overflow in the png_combine_row function in libpng before 1.5.21 and 1.6.x before 1.6.16, when running on 64- bit systems, might allow context-dependent attackers to execute arbitrary code via a "very wide interlaced" PNG image.	All libping 1.6 users should upgrade to the latest version >= libping-1.6.16 All libping 1.5 users should upgrade to the latest version >= libping-1.5.21 https://security.gentoo.org/glsa/201502-10
High 7.5 CVE-2013-0156 13-01-2013	activesupport-3.2.1.gem	active_support/core_ext/hash/conversions.rb in Ruby on Rails before 2.3.15, 3.0.x before 3.0.19, 3.1.x before 3.1.10, and 3.2.x before 3.2.11 does not properly restrict casts of string values, which allows remote attackers to conduct object-injection attacks and execute arbitrary code, or cause a denial of service (memory and CPU consumption) involving nested XML entity references, by leveraging Action Pack support for (1) YAML type conversion or (2) Symbol type conversion.	All Ruby on Rails 2.x users should upgrade to the latest version >= rails-2.3.18 https://security.gentoo.org/glsa/201412-28
High 7.5 CVE-2015-0973 18-01-2015	libpng-v1.5.10 (File: pngrutil.c)	Buffer overflow in the png_read_IDAT_data function in pngrutil.c in libpng before 1.5.21 and 1.6.x before 1.6.16 allows context- dependent attackers to execute arbitrary code via IDAT data with a large width, a different vulnerability than CVE-2014-9495.	
Medium 5.8 CVE-2013-1856 19-03-2013	activesupport-3.2.1.gem	The ActiveSupport::XmIMini_JDOM backend in lib/active_support/xmI_mini/jdom.rb in the Active Support component in Ruby on Rails 3.0.x and 3.1.x before 3.1.12 and 3.2.x before 3.2.13, when JRuby is used, does not properly restrict the capabilities of the XML parser, which allows remote attackers to read arbitrary files or cause a denial of service (resource consumption) via vectors involving (1) an external DTD or (2) an external entity declaration in conjunction with an entity reference.	All Ruby on Rails 2.x users should upgrade to the latest version >= rails-2.3.18 https://security.gentoo.org/glsa/201412-28
Medium 5.0 CVE-2015-3227 26-07-2015	activesupport-3.2.1.gem	The (1) jdom.rb and (2) rexml.rb components in Active Support in Ruby on Rails before 4.1.11 and 4.2.x before 4.2.2, when JDOM or REXML is enabled, allow remote attackers to cause a denial of service (SystemStackError) via a large XML document depth.	

The Security Vulnerabilities list includes the following information:

- **Vulnerability** the security vulnerability severity (High / Medium / Low) and score (0 10), name with a link to the CVE reference (i.e. <u>CVE-2013-4316</u>) and publish date
- Library name of the library that has this security vulnerability
- Description detailed description of the security vulnerability
- **Recommendations** list of references to possible fixes, patches and further information regarding the security vulnerabilities.
- In some cases the CVE reference is not provided for security vulnerabilities. The vulnerability database is based on data from multiple official sources like NVD, Node Security etc. CxOSA detects vulnerabilities by searching the database by SHA-1 and only displays a detection if there is a match for specific components or sub-components. This procedure eliminates "false-positive" detection and ensures that the user is only provided with the most accurate and reliable information. Not all security vulnerabilities have a specific CVE reference ID. In these cases, we use our own internal identifier.



License Risk and Compliance

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

License Distribution				License	Risk Distrib	ution	
License	Rink Level	Occurrences		162			1
GPL 3.0	High	1					
Microsoft	Medium	8.8					
LGPL 2.1	Medium	1					
Apache 2.0	Low	18					
MIT .	Low	-8					
BSD 2	Low	3 1					
BSD 3	Low	1				-	
Microsoft SQL Server Compact 4.0	Unknown	16		28	9	1	50
Microsoft SQL Server Compact 3.5 SP2	Unknown	-11		Low	Med	High	Unknown
GPL 2.0	Unknown	7	•				

License Distribution

Distribution of project's open source libraries by type of license:

- License the name of the license
- **Risk Level** this represents the possible legal risk level with regards to Copyright, Copyleft, Patent and Royalty, Linking and OSD Compliance - High, medium, low or unknown
- Occurrences number of libraries with the given license

License Risk Distribution

Distribution of project's open source libraries by level of risk associated with each license:

- Low number of libraries licensed under Low ranking licenses
- **Medium** number of libraries licensed under Medium ranking licenses
- High number of libraries licensed under High ranking licenses
- **Unknown** number of libraries licensed under Unknown ranking licenses



Outdated Libraries

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

Library	Versions	Recommendations	Match Type	Confidence Level
activesupport-3.2.1.gem	Your version: 3.2.1, Released: 26-01-2012 Newest stable version: 5.1.0, Released: 27-04-2017 187 new versions since your most recent update	Consider updating to latest version	Filename Match	70%
libpng-v1.5.10	Your version: v1.5.10, Released: 29-03-2012 Newest stable version: v1.6.9, Released: 06-02-2014 20 new versions since your most recent update	Consider updating to latest version	Exact Match	85%

The Outdated Libraries list includes the following information:

- **Library** artifact id of the library, the library display name in parenthesis. For example "Struts 2 Core" is the official display name of the library and "struts2-core" is the artifact id.
- **Versions** details regarding the version being used and the latest stable version available with release dates and the number of stable versions released in between both versions.
- **Recommendations** recommended steps that may contain links to the library's homepage with possible links and information regarding newer stable release versions.
- **Match Type** Libraries that were not found using the SHA-1 Hash, will be matched by the provided filename. Possible values are:
 - Filename Match with confidence level 70%
 - Exact Match with confidence level 100%
- **Confidence Level** anything below 100% indicates that there is a possibility that identification of the library is not accurate.
 - o **100%** File Type: Binary files (e.g. jar, dll). Match Type: SHA-1 Hash
 - **75-85%** File Type: Files Mapping to libraries (e.g. js, c). Source files exist in multiple source libraries and there are several possibilities to match them. Match Type: SHA-1 Hash
 - 70% File Types: All. Match Type: Match by Name (disabled by default). When enabled, libraries that were not found using the SHA-1 Hash, will be matched by the provided filename (starting from v8.4.2 hotfix).



- (i) For confidence level, the following should be noted:
 - Binary files always provide 100% confidence level
 - In some cases, when the confidence level is less than 100%, it maybe because some source files exist in multiple source libraries. During analysis, one of several possible matches are chosen and the origin source file may not be from where the user downloaded it.

High-Medium Risk Licenses

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

				Risk Inc	licators	
Library	License	Copyleft	Copyright	Patent	Linking	Royalty Free
0.6-master_2011-10-14	LGPL 3.0	Partial	65	20	Dynamic	Yes
DVWA-1.9-master_2016-05-20	GPL 3.0	Full	78	20	Viral	Yes
dvwa-master_2011-10-14	GPL 3.0	Full	78	20	Viral	Yes
htmlpurifier-1.0rc	LGPL 2.1	Partial	65	20	Dynamic	Conditional
htmlpurifier-v3.1.1	LGPL 2.1	Partial	65	26	Dynamic	Conditional
PHPIDS-0.6.3	GPL 3.0	Full	78	20	Viral	Yes
phpids-master_2010-03-07	LGPL 3.0	Partial	65	28	Dynamic	Yes

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

- Library name of the file
- License name of the high risk scored license
- **Copyleft** Full (CopyLeft on modifications as well as own code that uses the OSS), Partial (CopyLeft applies only to modifications) or No (not a CopyLeft license)
- **Copyright** score range according to color code and score level (0 100)
 - Licensee may use code without restriction
 - Anyone who distributes the code must retain any attributions included in original distribution
 - Anyone who distributes the code must provide certain notices, attributions and/or licensing terms in documentation with the software
 - Anyone who distributes a modification of the code may be required to make the source code for the modification publicly available at no charge
 - Anyone who distributes a modification of the code or a product that is based on or contains part of the code may be required to make publicly available the source code for the product or modification, subject to an exception for software that dynamically links to the original code (e.g. LGPL)



- Anyone who distributes a modification of the code or a product that is based on or contains part of the code may be required to make publicly available the source code for the product or modification (e.g. GPL)
- Anyone who develops a product that is based on or contains part of the code, or who modifies the code, may be required to make publicly available the source code for that product or modification if s/he (a) distributes the software or (b) enables others to use the software via hosted or web services (e.g. Affero)
- **Patent** score range according to color code and score level (0 100)
 - Royalty free and no identified patent risks
 - Royalty free unless litigated
 - No patents granted
 - Specific identified patent risks
- Linking Viral (will substantially infect the code linked to this OSS), Non Viral (will not affect the licensing of the linking code) or Dynamic (Dynamic linking will not infect)
- Royalty Free Yes, No or Conditional

Inventory

A list of the libraries names and their licenses.

Inventory (13)			
Library	Licenses	Match Type	Confidence Level
0.6-master_2011-10-14	LGPL 3.0	Exact Match	75%
cakephp-0.6.3	GPL 2.0	Exact Match	85%
cakephp-master_2011-10-14	GPL 2.0	Exact Match	75%
civicrm-master_2009-11-02	AGPL 3.0, GPL 2.0	Exact Match	75%
DVWA-1.9-master_2016-05-20	GPL 3.0	Exact Match	75%
dvwa-master_2011-10-14	GPL 3.0	Exact Match	75%
htmlpurifier-1.0rc	LGPL 2.1	Exact Match	85%
htmlpurifier-v3.1.1	LGPL 2.1	Exact Match	85%
ispCP-omega-1.0.0-rc6	Unspecified License	Exact Match	85%
monast-0.2b	BSD 3	Exact Match	85%
PHPIDS-0.6.3	GPL 3.0	Exact Match	85%
phpids-master_2010-03-07	LGPL 3.0	Exact Match	75%
sfXssSafePatchedPlugin-master_2009-12-14	MIT	Exact Match	75%



The Inventory list includes the following information:

- Library name of the file
- License name of the license
- **Match Type** Libraries that were not found using the SHA-1 Hash, will be matched by the provided filename. Possible values are:
 - Filename Match with confidence level 70%
 - Exact Match with confidence level 100%
- **Confidence Level** anything below 100% indicates that there may be cases in which identification of the library is not accurate.
 - **100%** File Type: Binary files (e.g. jar, dll). Match Type: SHA-1 Hash
 - **75-85%** File Type: Files Mapping to libraries (e.g. js, c). Source files exist in multiple source libraries and there are several possibilities to match them. Match Type: SHA-1 Hash
 - **70%** File Types: All. Match Type: Match by Name (disabled by default). When enabled, libraries that were not found using the SHA-1 Hash, will be matched by the provided filename (starting from v8.4.2 hotfix).
- (i) If an inventory is marked as "Requires Review", it simply means that the automatic analysis process wasn't able to assign a license to the library. The main reasons for this could be:
 - The file extension is not supported
 - The original open source file was modified and the SHA-1 was changed
 - The file is in-house
 - The file is not in the database and needs to be added
 - The file is not in the database and is not open source (commercial).

In this case the best practice is to perform a manual review (please contact Checkmarx support).



Unresolved Libraries

A list of the libraries that were not detected by CxOSA.

Unresolved Libraries (1)	
Library	
someFile.log.2011	

The unresolved libraries list includes the following information:

- Library name of the file
 - (i) Undetected libraries only report files in binary format (such as .dll & .jar) other files will not be reported. Saving all file formats will infect the database, therefore CxOSA saves undetected files only in binary format.



Generating the Open Source Analysis Report to PDF

Once the Open Source Analysis report is displayed, you can generate a PDF version for download or print.

To generate the Open Source Analysis report to PDF:

Go to **Dashboard > Project State** and click the **View Analysis Results** link or select the **OSA** tab.

Click the **Download PDF** button. An "Open Source Analysis Report download is in progress" indicator is displayed.

Once complete, the PDF version of the Open Source Analysis report is generated (similar to the example below) and automatically displayed.

sis Report		
portal AM		
Vulnerable Libraries	Severity Distribution	Aging Vulnerable Libraries
0 1 Vetkoren	High 1 Med 0 Low 0	
	ysis Report portal AM	ysis Report a portal AM Vulnerable Libraries Vulnerable Libraries Severity Distribution High 1 Med 0 Low 0 Low 0 Libraries





Security Vulnerabilities (4)

Vulnerability	Library	Description	Top Fix
High 10.0 CVE-2014-9495 2015-01-10	libpng-v1.5.10 (File: pngrutil.c)	Heap-based buffer overflow in the png_combine_row function in libpng before 1.5.21 and 1.6.x before 1.6.16, when running on 64-bit systems, might allow context-dependent attackers to execute arbitrary code via a "very wide interlaced" PNG image.	All libpng 1.6 users should upgrade to the latest version >= libpng-1.6.16 All libpng 1.5 users should upgrade to the latest version >= libpng-1.5.21 Details: https://security.gentoo.org/glsa/201502-10
High 7.5 CVE-2015-0973 2015-01-18	libpng-v1.5.10 (File: pngrutil.c)	Buffer overflow in the png_read JDAT_data function in pngrutil.c in libpng before 1.5.21 and 1.6.x before 1.6.16 allows context-dependent attackers to execute arbitrary code via IDAT data with a large width, a different vulnerability than CVE-2014-9495.	
Medium 5.0 CVE-2013-7353 2014-05-06	libpng-v1.5.10 (File: pngset.c)	Integer overflow in the png_set_unknown_chunks function in libpng/pngset.c in libpng before 1.5.14beta08 allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a crafted image, which triggers a heap- based buffer overflow.	All libpng users should upgrade to the latest version >= libpng-1.6.10 Details: https://security.gentoo.org/glsa/201408-06
Medium 5.0 CVE-2013-7354 2014-05-06	libpng-v1.5.10 (File: pngset.c)	Multiple integer overflows in libpng before 1.5.14rc03 allow remote attackers to cause a denial of service (crash) via a crafted image to the (1) png_set_sPLT or (2) png_set_text_2 function, which triggers a heap-based buffer overflow.	All libpng users should upgrade to the latest version >= libpng-1.6.10 Details: https://cecurity.costop.com/oles/201408-06

	277. 17		License F	Risk Distribution	
MIT	Risk Level	1			
Libpng	Unknown	1			

			CH choose	Se what developer
Outdated Librarie	as (2)			
* Confidence level < 100% ind Library	icates that there may be cases in which the identification of Versions	of the library is not accurate.	Match Type	Confidence Level
* Confidence level < 100% ind Library activesupport-3.2.1.gem	icates that there may be cases in which the identification of Versions Your version: 3.2.1, Released: 2012-01-26 Newest stable version: 5.1.0, Released: 2017-04-27 187 new versions since your most recent update	Pecommendations	Match Type Filename Match	Confidence Level



High-Medium Risk Licenses (7)

Carefully review the licenses and the way in which each library is used. We recommend that you consult with a specializing legal expert.

				Risk Indica	tors	
Library	License	Copyleft	Copyright	Patent	Linking	Royalty Free
PHPIDS-0.6.3	GPL 3.0	Full	78	29	Viral	Yes
dvwa-master_2011-10-14	GPL 3.0	Full	78	20	Viral	Yes
DVWA-1.9-master_2016-05-20	GPL 3.0	Full	78	20	Viral	Yes
0.6-master_2011-10-14	LGPL 3.0	Partial	65	29	Dynamic	Yes
htmlpurifier-v3.1.1	LGPL 2.1	Partial	65	20	Dynamic	Conditional
phpids-master_2010-03-07	LGPL 3.0	Partial	16	20	Dynamic	Yes
htmlpurifier-1.0rc	LGPL 2.1	Partial	65	29	Dynamic	Conditional



Inventory (13)

Library	Licenses	Match Type	Confidence Level
0.6-master_2011-10-14	LGPL 3.0	Exact Match	75%
cakephp-0.6.3	GPL 2.0	Exact Match	85%
cakephp-master_2011-10-14	GPL 2.0	Exact Match	75%
civicrm-master_2009-11-02	AGPL 3.0, GPL 2.0	Exact Match	75%
DVWA-1.9-master_2016-05-20	GPL 3.0	Exact Match	75%
dvwa-master_2011-10-14	GPL 3.0	Exact Match	75%
htmlpurifier-1.0rc	LGPL 2.1	Exact Match	85%
htmlpurifier-v3.1.1	LGPL 2.1	Exact Match	85%
ispCP-omega-1.0.0-rc6	Unspecified License	Exact Match	85%
monast-0.2b	BSD 3	Exact Match	85%
PHPIDS-0.6.3	GPL 3.0	Exact Match	85%
phpids-master_2010-03-07	LGPL 3.0	Exact Match	75%
sfXssSafePatchedPlugin-master_2009-12-14	MIT	Exact Match	75%





Unresolved Libraries (1)

Library

someFile.log.2011

You can now print the report.



Creating and Managing Projects

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

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

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

In this section:

- Creating and Configuring Projects
- Branching / Duplicating Existing Projects
- Managing Projects and Running Scans
- Advanced Actions
- Viewing Project Details
- Managing Queries



Creating and Configuring a CxSAST Project

To create a CxSAST project:

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

CHECKMARX	(7) Dashboard - Proj	Ca 🎝 ects & Scans - Management -	ے۔ Users & Teams -	🔍 Data Analysis	Co My Profile	admin adm AppSec Coach 🖒 Logo
ojects & Scans / New Projec	t	- 44	-			
General	Location	Scheduling	Advanced Act	tions Ci	ustom Fields	Data Retention
-	Step 1: E	nter Project General Settings				
	Project Nam	Project 1	0			
	Preset	Checkmarx Default	• 0			
	Configuratio	Default Configuration	* 🧿			
	Team	CxServer	* ?			
		◀ Back Next ►	Cancel X Finish	~		

Configure the following **General** project properties:

- **Project Name** should indicate the source code to be scanned and tracked.
- Preset set of queries to be run on the code scan. Default includes a set of queries recommended by Checkmarx for most projects. For all coding best practices, select All. For example, for an Android project select Android. For a full list of executed queries, see the Vulnerability Queries section in the release notes.
- **Configuration** Apart from the default configuration setting, additional configuration selection traditionally for advanced users, can be used for scanning double-byte encoded source code. There is also the possibility to select a multi-language configuration. This means that all files will be scanned, regardless of language type. If there is a need, a threshold parameter can be adjusted in the database.
- **Team** determines who will be able to view your project and its scan results. Available options depend on the permissions of the logged-on user. Selecting **CxServer** allows access only to the server Administrator. If you're working as a single user, leave the default option.

Click Next.



	CA Dashboard -	Projects & Scans -	رج Management +	දියි Users & Teams -	🔍 Data Analy	rsis My Profile	a AppSec Coach	dmin ac () Log
cts & Scans / New Projec	t i		1	а. — — — — — — — — — — — — — — — — — — —		N.	dil -	
General	Location	s	icheduling	Advanced Action		Custom Fields	Data Retention	
	Stej	p 2: Choose Source To S	Scan					
	• Lo	cal		Se	lect 🧿	Count Lines		
	© Sh	ared		Se	lect 🧿			
	⊚ So	urce Control		Se	lect 🧿			
	⊚ So	urce Pulling		Se	lect (?)			
	Exclud	le Folders			0			
	Exclud	le Files			0			
		- Bac	k Next L C	ancel ¥				
		a pac						

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

• Local - Click Select to browse to a local zip file containing the code. Future scans to the project are also via local upload (see <u>Managing Projects and Running Scans</u>).

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

(i) If the zip file is larger than 200 MB, you will not be able to upload it. To create a smaller zip file of only files with specified extensions, use the **CxZip utility** (see the **CxSAST Utilities Guide**).

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

- (i) If a zip file is uploaded that contains file path greater than 255 characters, the file will not be sent for scanning. Shorten the file path and try again.
- (i) If the zip file contains another zip file inside, the internal zip file will not be sent for scanning. Unzip the contents to the main zip file before scanning.



- Shared project code that is maintained on a network server accessible from the CxSAST Server. Click Select, provide your Windows domain credentials in order for CxSAST to access the network (username format: domain_name\user name), and select one or more network folders containing the project code.
 - (i) Zipped source code is not supported for shared location scans. Unzip the contents of the zip file before scanning.
- Source Control project code that is maintained in either TFS, SVN, GIT or PerForce source control systems. Click Select. See Configuring the Connection to a Source Control System (v8.6.0 and up) in the CxSAST Configuration Guide.
 - (i) Files inside a zip file that are located inside a repository will not be sent for scanning. Unzip the contents of the zip file to the repository before scanning.
- **Source Pulling** an extension to "Shared" option above, "Source Pulling" activates a configurable script to pull source code from a source control system into the Shared location specified. Note: this script must be set previously configured in the CxSAST Windows client application.
- Optionally, you can **Exclude Folders** and/or **Exclude Files** from being scanned.



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

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

Click **Count Lines** to display the number of lines in the current project.

(i) Please note that as the Java Script is being enhanced in the scan process, the real count of lines might be larger than the result that will be shown from the **Count Lines** option or the <u>Cx CMD Line Counter</u>.



CHECKMARX	C√\ Dashboard +	Projects & Scans -	ے Management –	کے Users & Teams 🕞	⊘ Data Analysis	Co My Profile	ee AppSec Coach	admin admir U Logout
rojects & Scans / New Projec	t		lan.					
General	Location	s	cheduling	Advanced Action	s Cu	istom Fields	Data Reten	tion
	Ste	p 3: Choose the scan ex	ecution time					
	© N	one	0					
	• N	ow	0					
	😐 Bj	y Schedule	(1)					
	Run O	Mo Tu V In Weekdays 🔲 🗐	Ve Th Fr Sa Su					
	Run T	ìme	0					
		▲ Back	k Next 🕨 C	ancel 🗙 Finish 🤸	/			

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

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

- None defines no scheduling
- Now defines an immediate scan
- By Schedule define an automatic weekly scan according to the specified time
 - Run on Weekdays define which day to run the periodic scan
 - **Run Time** define what time to run the periodic scan.
- (i) To support continuous integration development methodology, it is recommended to schedule periodic scanning of source files, so they can be checked after modifications. This can be automated via the CLI in the Build file, but it does not have to be done this way because CxSAST scans source code and does not require building or compiling the source code.



cts & stans / New Project						
General	Location	Scheduling	g Adva	nced Actions	Custom Fields	Data Retention
	Step 4: D	efine pre and post scan act	ions			
	Send pre-sca	in e-mail to:				
					2	
	Send post-so	an e-mail to:				
					<u>&</u>	
	Send scan fa	ilure e-mail to:				
					<u>&</u>	
	Run post sca	n action:				
	None Issue Tracki	no Settings			•	
	None	ig octorige			▼ Select ✓	

Configure the following **Advanced Action** properties:

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



CHOCKMARX	(7) Dashboard +	Projects & Scans -	ے Management –	کے Users & Teams 🕞	🕢 Data Analysis	Co My Profile	Coach	admin admin () Logout
Projects & Scans / New Projec			1.					
General	Location St Custo	step 5: Set custom fields m fields are not defined	icheduling	Advanced Action	s Cu	stom Fields	Data Reter	ation
		d Bac	k Next 🕨 C	ancel 🗙 Finish 🕻	1			

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



	C/ Dashboard -	C. Projects & Scans -	ے۔ Management -	دی Users & Teams	⊘ Data Analysis	Co My Profile	Sec Coach	admin admi U Logout
rojects & Scans / New Project								
General	Locatio	n 🔰	Scheduling	Advanced Actio	ins C	ustom Fields	Data Retentio	n
		Step 6: Set data retention	settings					
	Num	ther of latest scaps to kee	•					
	NUT	iber of latest scans to kee	p					
		4.0		0				
		◀ Ba	ck Next 🕨	Cancel X Pinish	~			

Configure the **Data Retention** properties:

• Number of latest scans to keep - Define the number of latest scans to be kept (see <u>Data</u> <u>Retention Management</u>).

Click **Finish** and check the scan status (see <u>The Queue</u>).



Configuring Open Source Analysis

Checkmarx Open Source Analysis (CxOSA) allows you to manage, control and prevent the security risks and legal implications introduced by open source components used as part of the development effort. CxOSA supports all the most common programming languages, enabling you to secure all their open source components in addition to the in-house developed code analysis coverage (see **Supported Code Languages and Frameworks** in the **CxSAST Release Notes**).

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

Configuration for CxOSA is performed from within CxSAST and you can add CxOSA to any project performing a scan.

To configure an open source analysis:

Select **Projects & Scans > Projects**. The **Projects View** is displayed.

CHECKMARX 8.4.0 [SDLC] kpires: 12/14/2016	C / Dashboard +	Projects &	Scans -	ے Management -	요 Users & Teams + Da	🕢 ta Analysis	යි My Profile	Ą	opSec Coach	admin admin U Logout
ojects & Scans / Projects							1			
+ Create New Project	Delete							r b	\[Filters I I	Group By 🕜
PROJECT NAME	0	WNFR	TEAM	PRESET	TOTAL SCANS	LAST SCAN	INED	SCANS LIST	ACTIONS	
DocsProject	ad	min@cx	CxServer	Default 2014	1	12/10/201	9:04 AM	[]		r n
DocsProject2	ad	lmin@cx	CxServer	Default 2014	0					r D
DocsProject3	ad	lmin@cx	CxServer	Default 2014	4	3/8/2016 1	1:11 AM	1	\triangleright	70
DocsProject4	ad	lmin@cx	CxServer	Default 2014	4	3/16/2016	4:05 PM		$\triangleright \triangleright \neg$	r D
DocsProject5	ad	lmin@cx	CxServer	Default 2014	4	3/8/2016 1	1:12 AM	Ē		7 🗋
	Page size: 10 T								5	items in 1 pages
Monitoring General	Page size: 10 T	Scheduling	Advance	d Custom Field	ds Data Retention	OSA			5	items in 1 pages
Monitoring General	Page size: 10 T	Scheduling	Advance	d Custom Field	ds Data Retention	OSA			5	items in 1 pages
Monitoring General	Page size: 10 Location Jonerabilities	r Scheduling	Advance	d Custom Field Risk India 2/10/201	ds Data Retention cator 6 2/10/2010 2/20/2010 3/6/2011	OSA			5	items in 1 pages
Monitoring General Monitoring General Vi High Medium 2500 2000 1644 1500 1000 500 500 500 2/10/2016 2/10/2	Page size: 10 Location Jnerabilities	Scheduling	Advance	d Custom Field Risk Indi	ds Data Retention cator 6. 2/14/2010 3/0/2014 3/0/2014 Seventy	OSA			5	items in 1 pages
Monitoring General Monitoring General Vi High Medium 2500 2000 1644 1500 1644 1500 1644 1500 2000 1644 1500 1644 1644 1644 1644 1644 1644 1644 16	Page size: 10 Location Junerabilities Low Info	Scheduling 2855 3/8/20:	Advance	d Custom Field Risk Indi 2/10/201 Last Update: 0	ds Data Retention cator 6 2/10/2010 2/24/2055 3/0/2020 Sevenity 11/06/2016 04:33PM	OSA			5	items in 1 pages



Select an existing project from the Projects list.

(i) You can also click **Create New Project** and define the new project configuration as you would if you were <u>Creating and Configuring a CxSAST Project</u>.

Click the **OSA** tab. The CxOSA properties are displayed.

onitoring	General	Location	Scheduling	Advanced	Custom Fields	Data Retention	OSA	
ocation of proj	ect's Open Sourc	e libraries						
Shared				5	Select			

Click Edit and configure the following CxOSA properties:

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

(i) Note that there is no limitation to the OSA file size for analysis.

Click Update.

Run the open source analysis and check the analysis results. See Consolidated Project State.



Branching / Duplicating Existing Projects

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

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

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

To branch or duplicate an existing project:

Go to Projects & Scans and select Projects.

CHECKMARA	CA Dashboard 👻	Projects & Scans 💂	کرچ Management –	요 Users & Teams 👻	⊘ Data Analysis	Co My Profile Co	odebashing	G Services & Support	admin admin U Logout
rojects & Scans / Projects									
+ Create New Project 📋 [Jelete						¹	🖓 Filters ∉	Group By
PROJECT NAME	OWNER	TEAM	PRESET	TOTAL SCANS	LAST SCANNED	SCANS LIST	ACTIONS		
Project 2 (CxTechDocs)	admin@cx	CxServer	Checkmarx Default	6 010	6/10/2018 7:05 AM	1		• D	
Project 1 (CxTechDocs)	admin@cx	CxServer	Checkmarx Default	r 1	6/10/2018 6:09 AM	Ē	DDT	* D	
Billing	admin@cx	CxServer	Checkmarx Default	6 01	6/7/2018 4:23 AM	1		• 🗅	
WEBGOAT_OSA_SCAN	admin@cx	CxServer	Default	0		ř.		• D	
Project 3 (CxOSA)	admin@cx	CxServer	Checkmarx Default	t 0		Ē		• 🗅	
(4 4 1) (1)	Page size: 10 💌								5 items in 1 pages
Monitoring General	Page size: 10 V	Scheduling Adva	anced Custom Fi	ields Data Retentio	o OSA				S items in 1 pages
Monitoring General Vulnerabilities Vulnerabilities Vulnerabilities Vulnerabilities Vulnerabilities 0 0 0 0 0 0 0 0 0 0 0 0 0	Location S	Scheduling Adv	anced Custom Fi	ields Data Retentio	o OSA				S Items in 1 pages
Monitoring General	Dage size: 10 V Location S Low Info	Scheduling Adv 80 36 23 0 6/10/201	anced Custom Fi Risk Indicator ————————————————————————————————————	ields Data Retentio	1 OSA				5 Items in 1 pages



	-2				(23)
Click Branch Project		or Du	plicate	Project	1

and a second	_				
	Step 1: Enter	Project General Settings			
	Project Name		3		
	Preset	High and Medium	* 0		
	Configuration	Default Configuration	* (?		
	Team	CxServer	* (?		
		Carrow Discover and Carrow and Car			

Define General settings and click Next.

seneral	Location	scheduling	Advanceo Actions		Custom Fields	Uata Ketention
	Step 2: Choose Source Ti	o Scan				
	Local		Select]0	Count Lines	
	O Shared		Select	0		
	O Source Control		Select	0		
	O Source Pulling		Select	0		
	Exclude Folders		0	0		
	Exclude Files		0	0		
	4 0	with News In Council	V Datas			


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

General	Location	Scheduling Advanced Actions	Custom Fields	Data Retention
	Step 3: Choose the scar	execution time]
	O Nome	•		
	Now	0		
	O By Schedule	0		
	Mo Tu Run On Weekdays 🔲 🛙	u We Th Fr Sa Su		
	Run Time	0		
	4	and New Monte X Finish and		

Define scan Scheduling options and click Next.

Seneral	Location	Scheduling Advi	anced Actions	Custom Fields	Data Retention
	Step 4: Define	e pre and post scan actions			
	Send pre-scan e	-mail to:			
				8	
	Send post-scan	e-mail to:			
	Send scan failur	e e-mail to:			
				2	
	Run post scan a	ction:	11		
	None		-		
	Issue Tracking S	Settings		1 (
	None		7	Select 🖌	



Define Advanced Action settings and click Next.

General	Location	Scheduling	Advanced Actions	Custom Fields	Data Retention
	Step 5: Set cu:	stam fields]
	Project Manager	Project Manager			
	Project Type	Project Type			

Define Custom Field settings and click Next.

aciicrai	Location	scheduling	Advanced Actions	Custom Fields	Data Retention
	Step 6: Set di	ata retention settings]
	Number of latest	scans to keep			

Define Data Retention settings and click Next.

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

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

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



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



Managing Projects and Running Scans

Scan List/Actions

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

iiid	Scan List	Displays the project in the individual project path, e.g. Projects & Scans/View Project Scans/My Java Projects.
\triangle	Full Scan	A scan of the whole project. If the project is configured for a local location, this will require uploading a zip file with the updated source code.
		Incremental scan is used to increase the scanning speed of the project. It works by scanning only the code that has changed since the last full scan was performed. During the incremental scan, the system takes each file that was sent to be incrementally scanned and creates a hash of its code. It then compares the value of the hash with the value of the hash of the files with the same name that was scanned on the last full scan.
		 Incremental scan needs to be performed on all of the code, not only on the changed code.
		 Incremental scan is recommended only if the regular scan takes more than 45 minutes.
<u>/+</u>	Incremental Scan	 When using incremental scan as part of CI/CD (for example as part of a build process) you need to make sure that a full scan is performed every X amount of incremental scans. Otherwise the changes will aggregate and when more than 7% of the code has changed CxSAST will either run a full scan or fail the scan, depending on the configuration.
		The following configuration keys are available:
		 INCREMENTAL_SCAN_THRESHOLD Defines the maximum percentage of files changed to allow the incremental scan. Valid values: 1-19, Default value: 7 INCREMENTAL_SCAN_THRESHOLD_ACTION Defines the action to be taken when the threshold exceed in incremental scan. FAIL – fail the scan, FULL – switch to full scan. Valid values: FAIL or
(i) If	a zip file is up or scanning. Sh	loaded that contains file path greater than 255 characters, the file will not be sent orten the file path and try again.



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



Managing Tables

CHECKMARX	CA CA Dashboard - Projects & Scans -	🖉 👸 Management + Users & Teams +	ල දු Data Analysis My Profile				Welcome admin admin 🖞 Logo
Projects & Scans / Projects							
+ Create New Project	Delete					D Filter	s 🗐 Group By 🔿
PROJECT NAME	OWNER	TEAM	PRESET	TOTAL S.	LAST SCANNED =	SCANS LIST	ACTIONS
BookStore	admin@cx	CxServer	All	3	6/3/2015 8:47 AM		
Bookstore feature A	admin@cx	CxServer	Al	1	6/3/2015 8:47 AM	(1)	
WebGoat	admin@cx	CxServer	OWASP	TOP 10 - 2013 1	6/3/2015 8:37 AM	(¹	
My Dup Java Project	admin@cx	CrServer	Default :	1014	6/3/2015 3:35 AM	1	
My Java Project	admin@cx	CxServer	Default	1014 3	6/2/2015 10:05 AM	1	$\triangleright \triangleright 7 \oslash$
My C Project	admin@cx	CxServer	Default :	2	6/2/2015 2:07 AM		
Flight Gear	admin@cx	CxServer	Default	2	6/2/2015 2:06 AM	<u>(1)</u>	
TEST_02	kelichiro_akiyamaj	Siwi.co.jp CxServer\SP\Co	mpany\Users Default :	1014 1	6/1/2015 9:17 AM		
TEST_01	kelichiro_akiyama	liwi.co.jp CxServer\SP\Co	mpany\Users Default :	2	6/1/2015 9:05 AM	自	DDTO.
Monitoring General	Page size: 50 v	Advanced					13 items in 1 pages
V High @ High @ Hedum 50 145 50 15 10 0 6/3/2015	Vierabilies 45 42 37 22 34 22 4/W2015 6/W2021	Autoritation	Severa				
			Last Update: 03/06/2015 09:564	м			
Edit 🗸							
			© 2015 Checkmark Top				

The various tables in the web interface provide navigation and pagination controls:

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

• Delete - Delete rows

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

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



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



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

Owner 🔺	x							
+ Creat	New Project 📋 Delete						() 7 Filter	🗄 Group By 🔘
0	PROJECT NAME	OWNER A	TEAM	PRESET	TOTALS	LAST SCANNED	SCANS LIST	ACTIONS
¥ ()	awee stampes							
G	Flight Gear	admin@cx	CrServer	Default 2014	2	6/2/2015 2:06 AM	<u>iii</u>	DDTD
0	My Java Project	admin@cx	Criserver	Default 2014	3	6/2/2015 10:05 AM	1	$\triangleright \triangleright \uparrow \odot$
8	My C Project	admin@cx	CrServer	Default 2014	2	6/2/2015 2:07 AM	1	DDTD
.0	Data Storage	admin@cx	CxServer	Default 2014	0		1	DDTD
0	test-iwi2	admin@cx	Criserver	Default 2014	0		1	DDTD
0	DataStorage	admin@cx	CriServer	Default 2014	0		(1)	$\triangleright \triangleright \land \oslash$
0	My Dup Java Project	admin@cx	CxServer	Default 2014	1	6/3/2015 3:35 AM	1	DDTO
0	WebGoat	admin@cx	CriServer	OWASP TOP 10 - 2013	1	6/3/2015 8:37 AM		DATO .
(4) (4)	Page size 50 T							13 items in 1 pages

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



Advanced Actions

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

- Send an email message
- Run an executable

In this section:

- Configuring an Email Action
- Configuring an Executable Action



Configuring an Email Action

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

To configure an automatic email:

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

Monitoring	General	Location	Scheduling	Advanced	Custom Fields	Data Retention
Send pre-scan	e-mail to:					
				2	<u>4</u> 2	
Send post-scar	n e-mail to:					
					69	
Send scan faile	ure e-mail to:					
					<u>4</u> 2	
Run post scan	action:					
None				V		
Issue Tracking	Settings					
None				\forall	Select 🗸	

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





Configuring an Executable Action

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

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

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

 Define an Action for the executable: Go to Management > Scan Settings > Pre & Post Scan Actions > Create New Action, and configure the following:

Create Action			
Action Type:	Post Scan Action		
* Name:	MyAction		
* Command:		None	•
Arguments:	[XML output]	None	
		MyAction.bat	
			Create 🗸 Cancel 🗙

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

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

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



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

Monitoring	General	Location	Scheduling	Advanced	Custom Fields
Send pre-scan	e-mail to:				
				1.	42
Send post-scar	n e-mail to:				
					<u>6</u> 2
Send scan failu	ure e-mail to:			10	
					<u>4</u> 2
Run post scan	action:				
None				∇	
Issue Tracking	Settings				
None				Ŧ	Select 🗸
Edit 🗸					

4. Click Finish.



Viewing Project Details

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

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

7 8.4.0 [SDLC] Expires: 12/14/2016	(🔨 Dashboard -	C. Projects & Se	cans - Mai	्री nagement - Us	은 ers & Teams 구	📿 Data Analysis	ැති My Profile	e AppS	ec Coach	admin adm U Logou
rojects & Scans / Projects										
+ Create New Project] Delete							6 V	Filters 🗐 Gro	оир Ву 🛛 🔿
PROJECT NAME	OV	VNER	TEAM	PRESET	TOTAL SCAN	IS LAST SCAN	INED	SCANS LIST	ACTIONS	
DocsProject	ad	min@cx	CxServer	Default 2014	1	12/10/2015	5 9:04 AM		$\triangleright \triangleright \uparrow$	D
DocsProject2	ad	min@cx	CxServer	Default 2014	0			<u> </u>	$\triangleright \triangleright \uparrow$	\square
DocsProject3	ad	min@cx	CxServer	Default 2014	4	3/8/2016 1	1:11 AM		$\triangleright \triangleright \uparrow$	\square
DocsProject4	ad	min@cx	CxServer	Default 2014	4	3/16/2016	4:05 PM		$\triangleright \triangleright \uparrow$	D
DocsProject5	ad	min@cx	CxServer	Default 2014	4	3/8/2016 1	1:12 AM		$\triangleright \triangleright \uparrow$	
	Page size: 10 🐨	•							5 ite	ems in 1 pages
Monitoring General	Page size: 10 T	Scheduling	Advanced	Custom Fields	Data Retention	OSA			5 ite	ems in 1 pages
Monitoring General	Page size: 10 Location /ulnerabilities	Scheduling	Advanced	Custom Fields	Data Retention	OSA			5 ite	ems in 1 pages
Monitoring General	Page size: 10 Location /ulnerabilities n Low Info	Scheduling	Advanced	Custom Fields Risk Indicat 2/10/2016	Data Retention	OSA			5 ite	ems in 1 pages
Monitoring General	Page size: 10 Location Location n Low Info	Scheduling	Advanced	Custom Fields Risk Indicat 2/10/2016	Data Retention	OSA			5 ite	ems in 1 pages
Monitoring General	Page size: 10	Scheduling	Advanced	Custom Fields Risk Indicat 2/10/2016	Data Retention	OSA			5 ite	ems in 1 pages

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

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

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

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



lonitoring	General	Location	Scheduling	Advanced	Custom Fields	Data Retention	OSA
	Vulner	abilities —		3.07	Risk Indicator		7
• High 2500 2000 1644 1500 1000 500 882 0	• Medium •	Low Info	205	Quantity	2/10/2016	2/10/2010 2/54/2016 3/6/2016	
2/10/2016	2/10/2016	2/24/2016	3/8/201			Severity	
					Last Update: 01/06	/2016 04:33PM	

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

- The **Vulnerabilities** chart includes a graph for vulnerabilities of each severity level (High, Medium, Low, and Info). Each graph presents numbers of found vulnerability instances (y axis) for progressive scans by date (x axis).
- The **Risk Indicator** chart represents each scan result combining quantity and severity of found vulnerability instances.

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

General Properties

Click the General tab to display its properties.

Monitoring	General	Location	Scheduling	Advanced	Custom Fields	Data Retention	OSA	
Project Name	DocsProje	ct5						
Preset	Default 20)14		*				
Configuration	Default Co	onfiguration		~				
Team	CxServer							
Update 🗸	Cancel X	•						

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

For more information about defining these properties refer to section about General properties in <u>Creating and Configuring a CxSAST Project</u>.

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



Location Properties

Custom Fields Data Retention OSA Monitoring General Location Scheduling Advanced Local Select Shared Select Source Control Select Source Pulling Select 0 Exclude Folders Exclude Files 0 Update 🗸 Cancel 🗙

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

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

For more information about defining these properties refer to section about Location properties in <u>Creating and Configuring a CxSAST Project</u>.

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

Scheduling Properties

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

Monitoring	General	Location	Scheduling	Advanced	Custom Fields	Data Retention	OSA	
an News								
None								
Ry Sched	le							
Run On Weeko Run Time	lays D 12:0	Tu We Th Fr	Sa Su					
Update 🗸	Cancel X	:						

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

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



For more information about defining these properties refer to section about Scheduling properties in <u>Creating and Configuring a CxSAST Project.</u>

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

Advanced Properties

Click the Advanced tab to display its properties.

Nonitoning	General	Location	Scheduling	Advanced	Custom Fields	Data Retention	OSA	
Send pre-scan e-	-mail to:							
					<u>4</u> 2			
Send nost-scan	e-mail to:			1				
ound post sound	e manto.				20			
				11	420			
Send scan failur	re e-mail to:							
				1	<u>6</u> 2			
Run post scan a	ction:							
None				Ψ.				
Issue Tracking S	Settings							
None				Ψ.	Select 🖌			

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

For more information about defining these properties refer to section about Advanced properties in <u>Creating and Configuring a CxSAST Project.</u>

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

Custom Fields Properties

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

Monitoring	General	Location	Scheduling	Advanced	Custom Fields	Data Retention	OSA	
Program Manager	Program M	snager						
Product Manager	Product Ma	nager						
Project Manager	Project Mar	iager						
		•						
Update 🗸	Cancel >							

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



For more information about defining these properties refer to section about Custom Field properties in <u>Creating and Configuring a CxSAST Project.</u>

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

Data Retention Properties

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

Monitoring	General	Location	Scheduling	Advanced	Custom Fields	Data Retention	OSA
Number of latest sc	cans to keep						
Update 🗸	Cancel X						

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

For more information about defining these properties refer to section about Data Retention properties in <u>Creating and Configuring a CxSAST Project</u>.

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

CxOSA Properties

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

Monitoring	General	Location	Scheduling	Advanced	Custom Fields	Data Retention	OSA	
Location of proj	ect's <mark>O</mark> pen Sourc	e libraries						
Local								
Shared				S	elect			
G	36							
Update 🗸	Cancel 🗙	C						

The OSA tab represents the option to define the location of the open source code libraries for analysis.

For more information about defining these properties refer to section about Open Source Analysis properties in <u>Creating and Configuring a CxSAST Project</u>.

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



Managing Queries

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

In this section:

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



Viewing, Importing, and Exporting Queries

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

To export queries:

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

V7.2.0 Dashboard - Projects & Scans	چ • Management • Users & Teams •	ල දි _{ලි} Data Analysis My Profile	Welcome admin admin 🕁 Logoz
Management / Scan Settings / Query Viewer Queries Export Queries () Import Queries ()	Description Code Injection		
JavaScipt, Server, Side, Vulnerabilities Code, Injection Secure, Direct, Object, References O Reflected, XSS Security, Misconfiguration Sol, Injection Sol, Injection Stored, XSS	Risk What might happen An attacker could run arbitrary code on the - File actions (read / create / modi - Changing the website - Open a network connection to th - Start and stop system services - Complete server takeover	e application server host. Depending or fy / delete) he attacker's server	the application's OS permissions,these could include:
Source 1 CxList inputs = Node35 Find Interactive Ing 2 CxList output = Node35 Find Outputs CodeIng 3 CxList sanitize = Node35_Find General_Sanit 4 5 result = output.InfluencedByAndNotSanitized 6 + (inputs * output - sanitize);	uts(); jection(); iire(); ś(inputs, sanitize, CxList.Influence	eAlgorithmCalculation.NewAlgor	Language Hash: 0252389975117793 Change Date: 5/31/2015
		© 2015 Checkmarx Top	

To keep track of changes to query sets, you can select a language (or one of its child items) and view the **Hash** and **Change Date** of the last changes to the language's query set.

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

2. Select organizational custom queries to be exported.





- 3. Click Export Queries.
- 4. Save the exported XML file.

To import queries:

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

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



Managing Query Presets

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

To create a new preset:

1. Go to Management > Scan Settings > Preset Manager, and click Create New Preset:

CHECKMARX	(^/ Deshboard -	Projects & Scare -	j) Management -	2) Users & Teams -	🔍 Data Analysis	ے My Profile	Welcome admin.admin.dbl.ogand
Management / Scan Settings / F	Preset Manager						
Crosp a column feader and do	React Manager	y that column	∑ Filtes		Preset name All ▶ Ø Aper ▶ Ø Churp ▶ Ø Goory ▶ Ø JavaScript ▶ Ø Objc ▶ Ø Pel ▶ Ø Pel ▶ Ø PelØ ▶ Ø PelØ		
High and Medium High and Medium and Low HIPAA JISEC AMRRA C Query Description					E Python E Ruby E Vito Source Edt		

- 2. Type a preset **Name** and click **OK**.
- 3. Select a code language.
- 4. Select queries to be included in the preset.
- 5. Click Save.

To export a preset:

- 1. Go to Management > Scan Settings, and select the preset to be exported.
- 2. Click Export Preset.
- 3. Save the exported XML file.

To import a preset:

- 1. Go to Management > Scan Settings, and click Import Preset.
- 2. Choose the preset XML file to be imported.
- (i) If the imported preset includes a query that has the same name as an existing one, the existing query will be overridden.



The Queue

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

V 8.8.0 [SDLC Expires: 6/13/	KMARX (2] 12018 Dash	∽∕ board -	Projects & Scans -	√ Management →	د Users & Teams 🕞	⊘ Data Analysis	Co My Profile	Codebashing	G Services & Support	admin admin O Logout
Projects & Sca	ns / Queue									
POSI_	QUEUED DATE == 6/11/2018 4:59:23 AM 6/11/2018 4:59:00 AM 6/11/2018 4:57:87 AM	INITIATO admin a admin a admin a	DR dmin dmin dmin	ORIGIN Web Portal Web Portal Web Portal	PROJECT NAME Project 1 (CxTecht Project 2 (CxTecht Project 3 (CxOSA)	SERVEI Docs) Localho Docs) Localho Localho	R NAME Ost Ost	(LOC 5T 6864 6538 21403 Fir		Group By 〇 ACTIONS う団 こ団 信 伝
Position	1 > Page	size: 10	T							3 items in 1 pages
Queued Date	6/11/20	8 4:59:23 AM								
Initiator	admin ad	lmin								
Status	Working									
Stage # 24 of 3	Overall progress 34% Current stage 79% 33 DefaultConstructor:Login									
					© 2018 Checkman	к Тор				

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

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

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

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



018 5:03:51 AM admin 9	 Connection_String_Injection Stared_XSS 	104 88	
admin 9	Stored_XSS	88	
9			
211	SQL_Injection	58	
\$	XPath_Injection	5	
	Command_Injection	4	
ng Compare	Code_Injection	2	
	Unsynchronized_Access_To_Shared_Data	65	
	P Escape_False	42	
	Potential_Stored_X88	15 ~	
1	fra	XPath_Injection Compare Compare Visynchronized_Access_To_Shared_Data Escape_False Potential_Stored_XSS	* * XPath_Injection S * * * * ring_Compare * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

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

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

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

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



Scan Results

In this section:

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



Viewing Results from All Scans

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

- In **Projects & Scans > Projects**, view an individual project scan results.
- In **Projects & Scans > All Scans**, view the results from all scans.

To see one project scan results using the All Scans table, in the project's row, click **Open** Viewer $(\bigcirc$).

Projects Scan List/Actions

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

₽C V 8.0	HECKMARX	C∕∕ Dashboard →	C. Projects & Scans -	√ Management →	دی Users & Teams 🔸	⊘ Data Analysis	And the second s	Sec C	admin bach Ú	n admin Logout
Proje	cts & Scans / Projects			_						
+	Create New Project	Delete						D 7 Filte	rs 🖽 Group By	0
D.	PROJECT NAME	OWNER	TEAM		PRESET	TOTAL SC.	LAST SCANNED -	SCANS LIST	ACTIONS	
۵	Project 5	admin@cx	CxServer		Checkmarx Default	4	11/27/2017 6:04 PM	Ē	DDTD	2
1	Project 6	admin@cx	CxServer		Checkmarx Default	1	11/20/2017 3:01 PM		DDTD	
۲	Project 1 (GitHub)	admin@cx	CxServer		Checkmarx Default	1	11/20/2017 2:56 PM	Ē		
	Project 4	admin@cx	CxServer		Checkmarx Default	1	11/20/2017 2:49 PM	1	DDTO	- 11
0	Project 1 (Branch 2)	admin@cx	CxServer		Checkmarx Default	1	11/20/2017 2:41 PM			
0	Project 2.1	admin@cx	CxServer		Checkmarx Default	1	11/20/2017 2:27 PM	(<u></u>		
	Project 1.1	admin@cx	CxServer		Checkmarx Default	1	11/20/2017 2:23 PM	1		- 11
	Project 6.1	admin@cx	CxServer		Checkmarx Default	1	11/20/2017 2:22 PM			
	Project 1 (Branch 1)	admin@cx	CxServer		Checkmarx Default	3	11/20/2017 2:19 PM	Ē	DDT0	
6	Project 2 (Jenkins)	admin@cx	CxServer		Checkmarx Default	2	10/17/2017 4:36 PM	1	DDTO	*
H		Page size: 10	Ŧ					1994	12 items in 2 p	oages



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

All Scans

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

3		SCAN D_	SCAN C_	PROJE	INITIAT	ORIGIN	RISK LEVEL SCORE		LOC	TEAM	SERVER_	CX VER.	COMME_	ACCESS	LOCKED	ACTION	
1	0	11/27/2_	11/27/2	Project 5	admin a,	Web Por	' <u> </u>	(79)	21403	CxServer	Localhost	8.6.0	Attempt_	Public		QGGCC	G.
9		11/26/2_	11/26/2	Project 5	admin a	Web Por	·*	(79)	21403	CxServer	Localhost	8.6.0		Public		QGEd	G.
3	•	11/20/2_	11/20/2_	Project 5	admin a	Web Por_	·*	(55)	6864	CxServer	Localhost	8.6.0		Public		0.6266	G.
8		11/20/2	11/20/2	Project 6	admin a,	Web Por	··	(64)	6836	CxServer	Localhost	8.6.0		Public		0.6260	G.
9		11/20/2_	11/20/2	Project_	admin a_	Web Por	' <u> </u>	(100)	33594	CxServer	Localhost	8.6.0		Public		QBEd	G.
9	•	11/20/2_	11/20/2_	Project 5	admin a	Web Por_	·***	(73)	18033	CxServer	Localhost	8.6.0		Public		0.6260	G,
1		11/20/2_	11/20/2	Project 4	admin a	Web Por	·*	(79)	21403	CxServer	Localhost	8.6.0		Public		0.6660	G.
9		11/20/2_	11/20/2	Project_	admin a_	Web Por	*I**	(100)	33594	CxServer	Localhost	8.6.0		Public		0.6060	G.
1		11/20/2_	11/20/2_	Project _	admin a	Web Por	'I**	(100)	87967	CxServer	Localhost	8.6.0		Public		QGGGd	G.



indicates a full scan
 indicates an incremental scan

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

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

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

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





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

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

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

Scan triggered by admin. No code changes were detected.		
•	× (

Deleting Scans

To delete one or more scans:

- 1. Select the rows of the requested scans.
- 2. Click the Delete button. A prompt appears, requesting you to confirm the deletion operation.
- 3. Click **OK**.
- (i) If the user does not have the authorization required for deleting scans, no scan will be deleted.

If one or more of the scans is locked, a message appears indicating, for example, that only 2 of the 3 scans were deleted successfully.

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

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



Comparing Scans

To compare scans:

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

Click the Compare Scans Compare Scans Compare screen is displayed.

cans Compare													
	PREVIO						NEW SCAN						
CAN START	11/20/2017	7:20:47 PM					11/26/2017 8:52:41 AM						
CAN COMPLETE	11/20/2017	7:21:49 PM					11/26/2017 8:54:44 AM						
CAN RISK	55						79						
oc	6864						21403						
LES COUNT	34						28						
ROJECT NAME	Project 5						Project 5						
EAM	CxServer					CxServer							
RESET	Checkmarx	Default					Checkmarx Del	ault					
CAN TYPE	Full Scan						Full Scan						
OURCE ORIGIN	N/A (Zip Fil	le)					N/A (Zip File)						
CAN COMMENT													
NGINE START TIME	11/20/2017	7:20:47 PM				11/26/2017 8:52:41 AM							
NGINE END TIME	11/20/2017	7:21:48 PM					11/26/2017 8:54:42 AM						
CAN QUEUED TIME	11/20/2017	7:20:27 PM					11/26/2017 8:5	2:22 AM					
OTAL SCAN TIME	0.00:01:40						0.00:02:23						
CANNED LANGUAGES	Lang Common CSharp JavaScript	usge H 01075 12207 t 01395	ash Number 29819410380 42574124002 95324901015	Creation da 11/20/2017 11/20/2017 11/20/2017	te V		Language Hash Number Creation date Common 0107529819410380 11/20/2017 Java 0181425764607500 11/20/2017						
OTAL RESULTS	109						552						
AST UPDATE	20/11/2017	07:21PM					26/11/2017 08:54AM						
									Pre	evious Scan	New Sc		
					C. Results	500			Canada Canad				
	High	Medium	Low	Info	Total	400				370			
New Issues	13	169	370	0	552	300							
Resolved Issues	5	24	80	0	109	200		16	9				
Recurrent Issues	0	0	0	0	0	100	4 12	24	80				
Trecurrent Issues	0	0	0	0	~	0			1. 1.1.1		0 0		
							High	Medium	Low		into		

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



Scan Result Actions

Navigating the All Scans table

In the <u>All Scans</u> screen you can implement the following scan result actions.

8.6.	H@CH .0 [SDLC	KMARX া	(Dasht	∽ ≫oard →	Projec	ts & Scans	یچ Management	t -	දි Users & T	3 'eams +	(Data /) Analysis	خ My	2 Profile	AppSec 0) Coach	idmin () La	adri ogoi
ojec	ts & Scar	ns / All Scans	A		-								1					
创	Delete	Company	e Scans											O	🖓 Filt	ters 🖽 Group	Зу	0
0		SCAN	SCAN	PROJE_	INITIAT	ORIGIN	RISK LEVEL SCORE		LOC	TEAM	SERVE	CX VER_	COMM.	ACCESS	LOCKED	ACTION		1
	0	11/27/	11/27/	Project 5	admin	Web Po_	·*	(79)	21403	CxServer	Localh	8.6.0	Attemp_	Public		QGGG	6J	ŀ
0		11/26/	11/26/_	Project 5	admin	Web Po	' <u></u> "	(79)	21403	CxServer	Localh	8.6.0		Public		0.6260	6	
0		11/20/	11/20/_	Project 5	admin	Web Po	·	(55)	6864	CxServer	Localh	8.6.0		Public		0.866	G.	
		11/20/	11/20/_	Project 6	admin_	Web Po_	·"	(64)	6836	CxServer	Localh	8.6.0		Public		QBEd	61	
0		11/20/	11/20/_	Project	admin	Web Po_	'I"	(100)	33594	CxServer	Localh	8.6.0		Public		QBGd	6	
		11/20/	11/20/_	Project 5	admin	Web Po	·	• (73)	18033	CxServer	Localh	8.6.0	Scan tri	Public		QBGd	E)	ſ
63		11/20/	11/20/	Project 4	admin	Web Po	'	(79)	21403	CxServer	Localh	8.6.0		Public		QBGd	6	
6		11/20/	11/20/_	Project	admin	Web Po	'ı"	(100)	33594	CxServer	Localh	8.6.0	Scan tri_	Public		QBEd	6J	Į.
		11/20/	11/20/	Project	admin	Web Po_	·!"	(100)	87967	CxServer	Localh.	8.6.0		Public		QGEd	G.	1
14	4	1 2 1	Pag	e size: 10	Ψ.											18 items	in 2 pa	ges

Column	Action	Description
	Q	Navigating Scan Results
Action		<u>Generating Scan Result</u> <u>Report</u>
	\uparrow	Open Scan Summary
	d	Download Scan Logs

Viewing the Scan Summaries

To view the Scan Summary:

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



Scan Start	11	/20/2017 2:5	53:55 PM			
Scan Complete	11	/20/2017 2:5	55:57 PM			
Scan Risk	73	•				
Preset	C	ieckmarx De	efault			
Scan Type	Fu	II Scan				
LOC	18	033				Top 5 Vulnerabilities (High and Medium)
Files Count	24					60
Project Name	Pr	oject 5				50 Medium
Team	C	Server				40 - Medium
Source Origin	N/	A (Zip File)				30 - Medium Medium
Scan Comment	Sc	an triggered	l by admin. M	lo code cl	hanges were detected.	20-
Engine Start Time	11	/20/2017 2:5	53:55 PM			10 - Medium
Engine End Time	11	/20/2017 2:5	55:55 PM			HITP Res. Cross Si. Hardcode. Download. Heap Ins
Scan Queued Time 11/20/2017 2:27:56 PM						
Total Scan Time	0.0	00:28:22				
Scanned Languages	La C J	inguage ommon ava	Has 010 018	h Numbe 75298194 14257646	r Creation date 10380 11/20/2017 807500 11/20/2017	
Last Update	20	/11/2017 02	:55PM			
Total	Issues	High	Medium	Low	Informational	Diek Indiator
Results	469	11	142	316	0	Non multiple
High Medium Low Info	31		91 2			Approx

The Scan Summary window includes the following scan information:

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

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

(i) This action is available to CxSAST Administrators, SP Managers, Company Managers, and Scanners.



Navigating Scan Results

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

\bookstore\CategoriesGrid.cs										ViewSta	te SortC
152									^	THE IT GAL	Y
154 // Categories Show begin 155 Categories SSOL = "":										Тс	String
156 Categories_sCountSQL = ""; 157											Y
<pre>158 string sWhere = "", sOrder = ""; 159</pre>										s	Order
160 161 hool HasParam = false:											¥
162 163									4	s	Order
164 //											¥
166 // build once of statement										Catego	ories_sSQL
168 if (Utility.GetParam("FormCategorie	s_Sort	ing").Le	ngth>08	&!IsPostBack	;)						¥
<pre>170 ViewState["SortDir"]="ASC";} 171 if(ViewState["SortDir"]="ASC";}</pre>	cOrder		FD BV	Les_sol Ling)	"SoctColumn"	1 ToString	()+" "+\/ieu	State Sorth	is"l ToStri	Catego	ories_sSQL
172 In (Viewscate Son Column JHull) 172 173 System Collections Specialized Str	ingDic	tionary	Darame	-new System	Collections S	perialized	StringDict	tionary():	1.105011		¥
174 175	INSDIC	cronary	r ur un s	-new System.	01100010013.5	peciaiizea		Lionary();		co	mmand
176										_	¥
177									>	col	mmand 🗸 🗸
Scan Results Severity	Method code wir may ena	Categories_(thout being p able an SQL Ir	CreateData roperly san ijection att	Source at line 151 o itized or validated, a ack.	f bookstore\Categorie and is eventually used	esGrid.cs gets u in a database q	iser input from the uery in method Ca	ViewState_SortColu tegories_CreateData	mn element. This element Source at line 151 of bool	's value then store\Categ	flows through the oriesGrid.cs. This
Contarp	Resul	ts Gra	iph (Codebashing							
	√ Resu	ilt State 🔻	V Resu	ult Severity 🐨 🗸	/ Assign to User 🔻	Comme	nts 🔔 Save Sca	an Subset 🖉 Ope	n Ticket	Filter	s 🗐 Group By 🔘
SQL_injection (25. Found) (1)	Id	Direct Link	Status	Source Folder	Source Filename	Source Line	Source Object	Destination Folder	Destination Filename	Destination	Destination Object
		2	Manu	Theekstere	CatagoriasCaid	171	ViewState	Vhashatara	CatanariasCaid as	215	
	-	_0	new	luoukstore	o alegoriesoriu	171	Viewoldie	luuukstore	Categoriesona.cs	210	command
	2	9	New	\bookstore	CategoriesGrid	171	viewstate	\bookstore	CategoriesGrid.cs	217	ccommand
JavaScript	3	ar 0	New	\bookstore	CategoriesGrid	171	ViewState	\bookstore	CategoriesGrid.cs	215	command
r Low	4	d ^{ar}	New	\bookstore	CategoriesGrid	171	ViewState	\bookstore	CategoriesGrid.cs	217	ccommand
Client_Insufficient_ClickJacking_Prot	5	e e e e e e e e e e e e e e e e e e e	New	\bookstore	EditorialCatGrid	171	ViewState	\bookstore	EditorialCatGrid.cs	215	command
	ć	ø			FIN 10 10 11	171	11: 0: 1	N 1 1	5 Pr - 10 - 0 - 1	017	' , [×]
< >	4	1 2	3 🕨	► Page s	ize: 10 🔻						25 items in 3 pages

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

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



Java	
🕨 🛞 Ні	gh
- 0	Command_Injection (5:Found) (?)
	Reflected_XSS_All_Clients (225 : Found) (?)
🗵	Second_Order_SQL_Injection (4:Found) (?)
(2)	SQL_Injection (72:Found) (?)
- 💌	Stored_XSS (70:Found) (?)
	XPath_Injection (4:Found) (?)
► <u>∧</u> M	edium
* P Lo	W.

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

(i) Codebashing™

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

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

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

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

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



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

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

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

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







Scan Results	PCI DSS v3.2	*
🔹 Java		
🔻 PCI DS	S (3.2) - 6.5.1 - Injec	tion flaws - particularly SQL injection
- 🖲 C	ommand_Injection	(3:Found) (?)
- 🖲 S	QL_Injection (71 : I	Found) (?)
- 🖲 X	Path_Injection (4 :	Found) (?)
- 🛆 P	arameter_Tamperin	g (4:Found) (?)
- 🛆 P	rivacy_Violation (2	6 : Found) (?)
<u>∧</u> R	eDoS_From_Regex	_Injection (1 ; Found) (?)
P B	lind_SQL_Injections	6 (48:Found) (?)
- Р н	euristic_SQL_Injecti	ion (7 : Found) (?)
P. S	tored_Code_Injectio	on (1:Found) (?)
🕨 PCI DS	S (3.2) - 6.5.3 - Insec	cure cryptographic storage
PCI DS	S (3.2) - 6.5.4 - Insed	cure communications

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





Scan	Results NIST SP 800-53 💌	
Ja	ava	
-	AC-3 Access Enforcement (P1)	
•	SC-13 Cryptographic Protection (P1)	
-	SC-23 Session Authenticity (P1)	
-	SC-28 Protection of Information at Rest (P1)	
-	SC-4 Information in Shared Resources (P1)	
-	SC-5 Denial of Service Protection (P1)	
-	SC-8 Transmission Confidentiality and Integrity (P1)	
-	SI-10 Information Input Validation (P1)	
	Command_Injection (3 : Found) (?)	
	SQL_Injection (71 : Found) (?)	
	XPath_Injection (4 : Found) (?)	
	Download of Code Without Integrity Check (6 : Found)	(?)

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

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

• **Graph** (right tab in **Results** pane) - Graphical display of first and last code elements of each found instance, with the relationships between them.

Results Graph 🧐 Codebashing				
🗸 Result State 🔻 🗸 Result Severity 🔻 🗸 Assign to User 🔻	Comments Graph Type: • Full	Graph 👔 😳 Key Nodes 👔 🤇	Ends r Q Q Q	Show related data flows 📕 Show not exploitable flows
VierState_Sort. VierState_Sort. VierState_Sort.	YeeState.Sort. Vandbute.Sort.	VexSee.Set. VexSee.Set.	Vendura.Son. Vendura.Son.	Ted Ted Ted
Tellving TaSking TaSking TaSking	Tageing Tageing	Telling Telling	ToDring Tubing	athen
			1	
		\sim	\sim /	
abile	atodar	stinier	ativitar	whee
		-		•
allider allider	aDrier	sEnder	alidar	1333.1
<				>

(i) In the CxSAST IDE plugins, the Graph pane displays full paths of the code elements that constitute the found instances, with the relationships between them.


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

Resu	ts Gra	ah (Codebashing										
V Resi	ilt State 🔻	√ Resu	lt Severity 🔻 🗸	Assign to User 🔻 👔	Comments	L Save Scan Subset 🖉 Op	en Ticket				🔞 🍸 Filte	rs 🗐 Group B	1
id	Direct Link	Status	Source Folder	Source Filename	Source Line	Source Object	Destination Folder	Destination Filename	Destination	Destination Object	Result State	Result Severity	A
1	P	New	\bookstore	CategoriesGrid.cs	171	ViewState_SortColumn	\bookstore	CategoriesGrid.cs	215	command	To Verify	High	
2	d ⁰	New	\bookstore	CategoriesGrid.cs	171	ViewState_SortColumn	\bookstore	CategoriesGrid.cs	217	ccommand	To Verify	High	
3	ø	New	\bookstore	CategoriesGrid.cs	171	ViewState_SortDir	\bookstore	CategoriesGrid.cs	215	command	To Verify	High	
4	a ^{go}	New	\bookstore	CategoriesGrid.cs	171	ViewState_SortDir	\bookstore	CategoriesGrid.cs	217	ccommand	To Verify	High	
5	d ⁰	New	\bookstore	EditorialCatGrid.cs	171	ViewState_SortColumn	\bookstore	EditorialCatGrid.cs	215	command	To Verify	High	
6	d ^{go}	New	\bookstore	EditorialCatGrid.cs	171	ViewState_SortColumn	\bookstore	EditorialCatGrid.cs	217	ccommand	To Verify	High	
ς	10.10				1.00				0000				

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

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

- **To Verify** (default) instance requires verification (i.e. authorized user)
- Not Exploitable instance has been confirmed as not exploitable (i.e. false positive). Instances defined with this state are not represented in the scan summary, graph, reports or dashboard, etc.
 - (i) Depending on your user permissions you may not be able to select the "Not Exploitable" state. If this is the case select the "Proposed Not Exploitable" state and then escalate the instance to an authorized user for confirmation.
- **Proposed Not Exploitable** instance has been proposed as not exploitable (i.e. potential false positive). Instances defined with this state are represented in the scan summary, graph, reports or dashboard, etc. until such a time that the state is changed to "Not Exploitable"
- **Confirmed** instance has been confirmed as exploitable and requires handling
- **Urgent** instance has been confirmed as exploitable and requires urgent handling

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



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

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

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

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

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

Click the link to obtain a URL to this results interface with the instance immediately selected.

Path (upper-right pane) - Displays the full path of code elements that constitute the vulnerability instance that is selected in the **Results** pane. This path represents the full attack vector for the vulnerability instance.

Select an instance in the **Results** pane (**Results** or **Graph** tab) and view its attack vector in the **Path** pane.





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

Select a code element in the **Path** pane to view it in its code context, in the **Source Code** pane (see below).

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



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

(i) When using the CxSAST IDE plugins you can immediately fix the code in place!



Scan Results Example

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

\bookstore\EditorialCatGrid.cs								ViewState_SortC	
150 151 ICollection editorial_categories_CreateDat	taSource() {					1		٧	
152 153								ToString	
<pre>154 // editorial_categories Show begin 155 editorial categories sSQL = "";</pre>								٧	
<pre>156 editorial_categories_sCountSQL = ""; 157</pre>								sOrder	
<pre>158 string sWhere = "", sOrder = ""; 159</pre>								٧	
160 161 bool HasParam = false:								sOrder	
162 163								۲	
164 //								editorial_categori.	
166 //	ame Asc".							٧	
168 if(Utility.GetParam("FormeditorIal_cat 169 {ViewState["SortColumn"]=Utility_GetParameter	tegories_Sorting).Length>0&&!Is	PostBack)					editorial_categori.	
170 ViewState["SortDir"]="ASC";} 171 if(ViewState["SortColumn"]!=null) sort	der = " ORDER BY	" + ViewState["	SortColumn"l.ToSt	ring()+" "+ViewSta	ate["SortDir	"l.ToString()		۲	
172 172 173 System Collections Specialized String	Dictionary Param	- new System Co	llections Special	ized StringDiction].105ci 116()		command	
174 175	Diccional y Param.	s -new system.co	iiiceions.speciai	izea.sei ingoiceio	iai y();			٧	
176								command	
178									
180 // Build base SQL statement							e		
			A 7			>			
Scan Results OWASP Top 10 2017	code without being pr may enable an SQL In	roperly sanitized or valida njection attack.	ated, and is eventually used i	n a database query in methor	d editorial_categor	ies_CreateDataSource	at line 151 of b	ookstore\EditorialCat	Grid.cs. This
	Results Gra	aph 🧖 🤭 Codebas	hing						
SQL_Injection (27 : Found) ()	🗸 Result State 🐨	✓ Result Severity ▼	🗸 Assign to User 🔻	🖉 Comments 🔟 Save	e Scan Subset 🖉	👂 Open Ticket	C) 🖓 Filters 🗐	Group By
Blind_SQL_Injections (2 : Found) (?)] Id Direct Link	Status Source Folder	Source Filename Source	Source Object	Destination Folde	Destination Filename	Destination O	Destinatio Result State	Result Ser
A2-Broken Authentication	🗌 1 🗬	New \bookstore	CardTypesGri_ 169	ViewState_SortColumn	\bookstore	CardTypesGrid.cs	command	204 To Verify	High ^
L Session_Fixation (5 : Found) (?)	4 🗌 2 🗬	New \bookstore	CardTypesGri_ 169	ViewState_SortDir	\bookstore	CardTypesGrid.cs	command	204 To Verify	High
A3-Sensitive Data Exposure	▶ 🗌 3 💣	New \bookstore	CategoriesGri 171	ViewState_SortColumn	\bookstore	CategoriesGrid.cs	command	215 To Verify	High
A5-Broken Access Control	🗆 4 🗬	New \bookstore	CategoriesGri 171	ViewState_SortColumn	\bookstore	CategoriesGrid.cs	ccomma	217 To Verify	High
A6-Security Misconfiguration	🗆 5 🗬	New \bookstore	CategoriesGri 171	ViewState_SortDir	\bookstore	CategoriesGrid.cs	command	215 To Verify	High
A7-Cross-Site Scripting (XSS)	6 ø [®]	New \bookstore	CategoriesGri 171	ViewState SortDir	\bookstore	CategoriesGrid.cs	ccomma	217 To Verify	High
Uncategorized		New \bookstore	EditorialCatGr 171	ViewState SortColumn	\hookstore	EditorialCatGrid	command	215 To Verify	High
	п. "	New \beekstore	EditorialCatCa 171	ViewPtate CortColumn	hoskstars	EditorialCatOrid		017 To Varify	Llink V
	< 	3 b b P	age size: 10 🔻					27 item	> is in 3 pages
50-2							_	E7 Mer	and pages

Briefly, an SQL_Injection vulnerability exists when user input is used in the syntax of an SQL query. Since those inputs could be interpreted as SQL syntax rather than user input, a user could manipulate the input in such a way as to alter query logic, potentially bypassing security checks and modifying the database, including execution of system commands.

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



CS	harp
+	A1-Injection
	SQL_Injection (27 : Found) (*)
	Blind_SQL_Injections (2 : Found) (?)
-	A2-Broken Authentication
	Session_Fixation (5 : Found) (?)
-	A3-Sensitive Data Exposure
-	A5-Broken Access Control
+	A6-Security Misconfiguration
	A7-Cross-Site Scripting (XSS)
-	Uncategorized

Clicking (¹¹) takes you to the **Codebashing**, where you can learn more about the selected vulnerability, why it happens, and how to eliminate it.

(i) Codebashing™

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

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

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

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

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



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

Cx Description												
								00	CONFUSE Click to le	D ABOUT SQL I arn all about	NJECTION it >	
SQL_Inject	tion											
Risk												
What might happen	n											
An attacker could dia details or credit card	irectly access a ds), and possib	ll of the system's o ly change or erase	ata. Using simple to existing data.	ools and text edition	ng, the attack	er would be abl	e to steal any sensiti	ive <mark>informatic</mark>	on stored by	v the system (:	such as personal u	iser
Cause												
How does it happen	n											
The application com neither checked for o	imunicates wi data type vali	h its database by s lity nor subsequen	ending a textual SC tly sanitized, the inp	QL query. The appli put could contain '	ication creates SQL command	s the query by s ds that would b	mply concatenatin <u>c</u> interpreted as sucl	g strings inclu h by the data	ding the us base.	er's input. Sin	ce the user input i	s
General Recon	mmendati	ons										
How to avoid it												

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



Generating Scan Result Reports

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

To generate a scan results report:

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



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

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

To customize categories:

Go to the relevant group under the Categories section, click the group to expand it and clear the vulnerabilities that you do not want to display in the report, as shown below.



Masp Top 10 2017	
- 🔳 A1-Injection	10
🗆 🔳 A2-Broken Authentication	
- A3-Sensitive Data Exposure	_

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

To change the report template:

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

Keport Cover Page			
		Add	
^P roject Name	New	Link to scan results	
ican Start	5/21/2017 3:10:19 PM	🗷 Team	
reset	Checkmarx Default	Checkmarx version	
can Time	00:03:35	Scan Comments	
.oc	33,594	Scan Type	
canned Files	189	Source Origin	
leport Date	6/19/2017 4:55:03 PM	Density	
Display Categories			
Language Hash Number Executive Summary Scanned Queries Scanned Files Vulnerability Description	port "As default, Organization description (if exists) will disp xternal link	layed as external link	
Language Hash Number Executive Summary Scanned Queries Scanned Files Vulnerability Description As ex Result Details	Port "As defoult. Organization description (if exists) will disp xternal link 	løyed as external link	
Language Hash Number Executive Summary Scanned Queries Scanned Files Vulnerability Description As ex Result Details Result Description Assign to User Comments Link to the result	Port "As defoult, Organization description (if exists) will disp xternal link	layed as external link	
Language Hash Number Executive Summary Scanned Queries Scanned Files Vulnerability Description Result Details Result Details Result Description Assign to User Comments Link to the result Show Code Snippets Source A Full Data	port "As default. Organization description (if exists) will disp xternal link 	layed as external link	
Language Hash Number Executive Summary Scanned Queries Scanned Files Vulnerability Description As en Result Details Result Description Assign to User Comments Link to the result Show Code Snippets Full Data Limit results to 50	port "As default, Organization description (if exists) will disp xternal link und Destinations Snippets I Flow Snippets	layed as external link	

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



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

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

Click Generate Report. The report starts generating.

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

	Filter Settings	
Severity		
Included: High, Medium, Low,	Information	
Excluded: None		
Result State		
Included: Confirmed, Not Exp	loitable, To Verify, Urgent, Proposed Not Exploitable	
Excluded: None		
Assigned to		
Categories		
Included:		
Uncategorized	All	
Custom	All	
PCI DSS v3.2	All	
OWASP Top 10 2013	All	
FISMA 2014	All	
NIST SP 800-53	All	
OWASP Top 10 2017	All	
Excluded:		
Uncategorized	None	
Custom	None	
PCI DSS v3.2	None	
OWASP Top 10 2013	None	
FISMA 2014	None	
NIST SP 800-53	None	
OWASP Top 10 2017	None	

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

The OWASP (2017 & 2013), PCI, FISMA and NIST summary sections in the scan report include a column named Best Fix Locations, which indicates the number of locations in the flow map that have been found as the best locations to fix the issues that belong to the selected category (for example, A1-Injection).



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



Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection*	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	83	51
A2-Broken Authentication and Session Management*	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	48	48
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	10	4
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	o	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	PASY	MODERATE	ALL DATA AND SYSTEM	73	73
A6-Sensitive Data Exposure*	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	3	3
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	11	2
AB-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	36	35
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	26	24



Scan Summary - PCI DSS v3.2

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

Scan Summary - FISMA 2014

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



Scan Summary - NIST SP 800-53

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

The Best fixed location is an absolute number that cannot be filtered and always displays all of the values. As a result, it is quite probable that while in effect the number of vulnerabilities far exceeds the number of best fix locations for a specified category (for example, 8000 and 600 respectively), the filtered report may display 350 issues and 300 best fix locations.



Comparing Scan Result Sets

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

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

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

?	You are about to co projects, results mig	mpare scans from di ght reveal significant	fferent differences
	2 12 NO 31	80	

A comparison summary is displayed:

Scans Compare									
	PREVIO	US SCAN				ł	NEW SCAN		
SCAN START	10/31/201	14 6:36:15 Al	M				11/5/2014 4:35:22	PM	
SCAN COMPLETE	10/31/201	14 9:22:06 AI	M				11/5/2014 4:36:54	PM	
SCAN RISK	100						100		
LOC	476732						8824		
FILES COUNT	7290						31		
PRESET	All						All		
SCAN TYPE	Full Scar	1					Full Scan		
SOURCE ORIGIN	N/A (Zip	File)					N/A (Zip File)		
SCAN COMMENT									
SCANNED LANGUAGES	La JavaScr Perl VbScrip	nguage ipt t	Hash Nu 14175761650 13757944990 03498203561	mber 015675 014496 141062	Creation date 10/30/2014 10/30/2014 10/30/2014	8	Language JavaScript VbScript ASP	Hash Number 1417576165015675 0349820356141062 1912797022324825	Creation date 10/30/2014 10/30/2014 10/30/2014 *
TOTAL RESULTS	11704						173		
	High	Medium	Low	Info	Total	.4000]	10500	Previous scan
New Issues	137	32	4	0	173	.0000) -	10280	📕 New Scan
Resolved Issues	245	578	10580	301	11704	800	0 -		
Recurrent Issues	0	0	0	0	0	600) -) _		
		Results 🔍				2001) - <u>245 137</u> 578	32 4 301	0
							nığıı Mer	Juni LUW I	OK 🗸



The comparison summary includes:

- The scan details table, showing the scan start and finish dates, risk levels, LOC (Lines of Code scanned), number of files, query set, source code origin, comments, code language details (including unique identifier and date of last change to the language queries), and total vulnerabilities found.
- The bottom-left table displays changes from the earlier scan to the newer one, in number of issues of each severity level:
 - **New Issues**: Issues that were found only in the newer scan
 - **Resolved Issues**: Issues that were found only in the older scan
 - **Recurring Issues**: Issues that were found in both scans
- The bottom-right chart graphically compares the number of found vulnerabilities in both scans, for each severity level.

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

\BS	Smal	I\BS\Login_jsp.ja	iva \BS	Small\BS\Sho	ppingCart_jsp	o.java 🔪								executeQu	егу	110
	So	can 2/13/201	14 11:13:4	17 AM Rest	lts		S	can 2/13/	2014 10:1	.6:35 AM R	esults			٧		
46	-10	(104/411/1	J. HEAD (/)			120	46		10,11040	11		17		ſS		10
48	ult:	Set openrs(java.sql.	Statement	stat, St	ring	48 sult	Set openr	s(java.so	1.Stateme	ent stat,	String	4	Y		
50);	10960 19 - 1	5000.000	nceAner V (oyı),		50 s);	10060 10	- 5141.02	recureXuer	Y (541),		*	rs		
52	·IIn (·	iawa sol Stu	atement s	tat Striv	ng table	Stri	52 53 cUp (ine ever	Statement	stat St	ring tabl	e Stri		٧		
54 55	Conn	ection conn' I	1 = null:		iy capie,	⇒(54 Conn	ection co	nn1 = nul	11:		c, 5013		openrs		
V F	esult	State 🔹 ✔ F	Result Severity	▼ 🗸 As	sign to User	🔹 🥖 Com	ments							🖓 Filters	🛃 Group By	0
0	ld	Query Name	Result Status	Source Folde	Source Filena	Source Line	Source Object	Destination Fi	Destination F	Destination Li	Destination O	Result State	Result Severi	Assigned Us	Comments	
		7	All			T				Y		All	All			٩
0	20	Second	Fixed	BS Small	Login_js	49	execute	BS Small	Shoppin	49	sql	To Verify	High	10 11495	n n	1
8	21	Stored_XSS	Recurrent	BS Small	Login_js	49	execute	BS Small	MyInfo_j	736	print	To Verify	High			1
٥	22	Stored_XSS	Recurrent	BS Small	Login_js	49	execute	BS Small	Login_js	518	print	To Verify	High			1
8	23	Stored_XSS	New	BS Small	Login_js	49	execute	BS Small	Shoppin	843	print	To Verify	High			1



Dashboard Analysis

In this section:

• Data Analysis



Data Analysis

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

To view the data analysis window:

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

CHCCKMARX V 8.8.0 [SDLC]	C / Dashboard -	E∂ Projects & Scans →	رچ Management 🗸	요 Users & Teams 👻	⊘ Data Analysis	Co My Profile	2	Codebashing	😥 Services & Support	admin admin U Logout
Data Analysis										
⊥ Template Basic		Time rang	ge Past month	▼ Chart Ty	pe Bar	▼ View	Mode 健 🕼	0		
Template Basic Filter Area Team Name Uuery Name Scan Date Scan Time Row Area Project Name Project Name Defer Layout Update Include Not Exploitable	Column Area Result Severity C Data Area Result Quantity Update	Time range Project 1 (CxTechDocs) Project 3 softs <								
		0	High	Medium	Low					
				© 2018 Che	ckmarx Top					

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

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



Team Name 🔄	Result Severity 🗢 💌
Query Name	
Scan Date 🔄	
Scan Time 🔄	
Row Area	∑ Data Area
Project Name 🛛 🔄	Result Quantity
Defer Lavout Update	Update

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

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

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

🛓 Template Basic 🔹	Time range	Past month 🔻	Chart Type	Bar 🔻	View Mode	Þ	ß	0
--------------------	------------	--------------	------------	-------	-----------	---	---	---

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



User Administration

In this section:

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

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

CHECKMARX	Deshboard -	Ed. Projects & Scans -	denagement -		Oata A	있 Inalysis N	کی) Iv Profile				Welcome admin admin	() Log
shboard / Projects State				Organization Confirm Users		Tree Branch View Service Provider Company Manag	ement	9	Ø	√ Filters	🗐 Group By	0
PROJECT NAME	LAST SCAN DATE	TEAM	LOC		R	Team Manageme	int	GH VULNERABILITIES	MEDIUM VU	ILNERABILITIES	ACTIONS	
Project 1 (Java)	3/31/2016	CxServer	214	03	1-	User Managemer	(2)		0		QGA	*
DocsProject4	3/31/2016	CxServer	335	11	1-	210	(0)	0	0		0.000	
Project 10_Users(4/5/201	3/31/2016	CxServer	335	11	1-	14	(0)	0	0		QBR	
DocsProject5	3/8/2016	CxServer	102	42	-	[***	(100)	197	275		Q. R. R.	
DocsProject3	3/8/2016	CxServer	214	03	· · -		(79)	13	141		QGA	
Perforce 5	2/15/2016	CxServer	147	93		[**	(100)	79	153		QBB	
Perforce 4	2/15/2016	CxServer	147	93	-	[³⁰⁰	(100)	79	153		Q. P. B.	
Perforce 3	2/15/2016	CxServer	697	31	-		(100)	380	536		0.66	
Perforce 2	2/15/2016	CxServer	697	31	-	[***	(100)	244	63		风窗园	-
4 4 1 2 3 +	▶ Page size	: 10									24 items in 3	pages

The Users & Teams menu includes the following options:

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



Role and Permission Overview

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

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

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

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



Creating and Managing User Accounts

CxSAST recognizes users with two types of authentication:

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

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

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

In this section:

- Creating User Accounts in the Web Interface
- Creating User Accounts via User Registration
- Managing Existing Users



Creating User Accounts in the Web Interface

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

To create a User account:

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

ers & Teams / Organiza	tion / User Management	1									
+ Create New User								Di 🖓 Riters	🗐 Group	÷Вү	Ó
ER NAME	E-MAIL	FULL NAME	COMPANY	LAST LOGIN DATE	TEAM	ROLE	ALENTOR	DATE CREATED	ACTIVE	-	r.
nināco	adminijiex	admin admin	305 million (1) m	4/5/2016 12:12:41 PM	DoServer	Server Manager	×	9/17/2015 5:48:42 PM	Δ,	Da .	1
er) Şicheckmark.com	user1@openidap.com	Uter 1 C1	Company 1		Team 1, Team 4	Scanner		4/5/2016 9:52:45 AM	04	Dn .	Ĭ.
r2@checkmanx.com	user2@openidap.com	User 2 C1	Company 1		Team 1	Scannor		4/5/2016 9:54:01 AM	<i>E</i> ,	(h)	1
tiveDirectoryLdap/,auto	auto@checkmeni.com	AutoFirstneme AutoLest	Company 1	4/5/2016 12:10:47 PM	Team 1	Raviewar		4/5/2016 12:10:05 PM	D _k	(h)	1
count information	Page size: 10			Team: 💌 co.2	 Diferent 				4 iten	u in 1 ;	page
ccount information	Page state 10								4 item	us in T ;	page
ccount information * First Name	Page size: 10		ų	Team:	3 DiServet	*			4 iten	u in 1 ;	page
ecount information *First Name *Last Name	• Page size: 10 User 1 C1	¥		Team:) CoServer (2) Service Provider (3) Commonw 1	*			4 item	uin1;	page
	Page stat: 10 User 1 Company 1	*		Tean: 🖉) Differver C Service Provider C Dimpory 1 * K (D Team 1				4 iten	us in 1 ;	page
	Pege stat: 10 User 1 [21 Company 1	* 		Team: 🖉 🖉	S Criserver				4 mm	sin1;	page
	Pigo data 20 Utar 1 C1 Dompory 1 user 1 @coenidatio.co			Team: 🖉 🖉	3 DiServer (2) Service Provider (2) Company 1 (2) Team (2) Team (2) Team (2) Team				4 item	un1)	page
	Pige start 20 Uter 1 C1 Dompany 1 user1@openidap.co			Tean: 🖉	3 Diferver 2 Service Provider 2 Service Provider 2 Dispany 1 4 (2) Team 4 (2) Team 4 (2) Team 4 (2) Team 4 (2) Team				4 item	sn1;	page
	Pige stars 20 Uter 1 C1 Dompany 1 user 1 @opendap.co			Tean: C	Diferver Service Provider Service Provider Diferver Service Provider Diferver Service Provider Service				4 item	un1)	page
	Page state: 10 Uter 1 E1 Dompory 1 user1 @openidap.co Weather Weather Weather			Team: 🖉 📿	Colorver				4 item	un1;	page
	 Page state: 10 Uter 1 C1 Dompany 1 user1 @openidap.co Vectorer 4. March 20 doity 10 	e opicitable state		Team: C	Colorver				4 item	un1;	pege
	Page state: 20 Uter 1 C1 Dompany 1 uari Gooenidap.co Kasener e: Alder to apply 1 e: Alder to apply 1 e: Alder to apply 1	en oppicitable state Projectable state		Team:	 Diferver Service Provider S				4 item	uin1)	pege
	Pige stars 20 Uter 1 C1 Company 1 User 1 Company 1 User 1 Company 1 C	et oppicitable state regionalities and regionalities and regionali		Team:	 Diferver Service Provider S				4 item	sn1;	page

Click Create New User.

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

(i) The information fields in the Create User window are displayed according to the selected User type.



C+ ODirec	ication User ctory User				
First Name: Last Name: E-mail: User Name: Password: Confirm Password: Job Title: Phone:			0		
Team:		P			
Role:	Select One	Ŧ			
Auditor:	0		11		
Skype:					
Country:	- Select One -	v	1		
Expires:	11/13/2019	ø			
Language:	English (United State	Ŧ			

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

Select a **Directory** from the drop-down (e.g. ActiveDirectoryLdap) and click **Find**. All the available Directory Users associated with the selected directory are displayed.



If there are no LDAP Directory Users displayed in the Directory User dialog window, check your LDAP connection settings (see <u>Connection Settings in LDAP Server</u> <u>Management</u>).

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

C+ ⊕ _{Ph}	rectory User			
* First Name:	David			
Last Name:	Press			
Directory User:	ActiveDirectoryLda	p\d 🔎		
E-mail;	David.Press@org.o	com		
Job Title:				
Phone:				
Cell Phone:				
'Team:		P		
Role:	- Select One	Ŧ		
Auditor	8			
Skype:				
Country:	- Select One -			
Expires:	11/13/2019			
Language:	English (United St	ate 🔻		

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

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



- For **Team**, click and then drill down the displayed organizational navigation tree to select one or more Teams to which this user will belong. If the user is to be a Company or SP Manager, just select a Team under the Company or SP; User may be turned into a Manager at a later stage.
- **Role** is either **Scanner** or **Reviewer**, at this point. User may be turned into a Manager at a later stage (by managing the Organizational Hierarchy; or, by using Organizational Tree mode).
 - A Scanner can delete projects\scans if the checkbox is selected. Select the Not Exploitable state checkbox to provide authorization to apply not exploitable state to instances.
 - A **Reviewer** can make changes to the status or severity of found instances if the checkbox is selected.
- Auditor: Reviewers can be turned into Auditors. Permissions to use CxAudit.
- Language defines the UI language for each user according to list of supported languages.

Click Create.



Creating User Accounts via User Registration

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

To sign up for a user account:

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

<u>.</u>	User Name	
a _t	Password	
	Login Options >>	

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

CHECKMARX V728				ڻ، ب
	Registration	kmara	Security Source Code Analysis tool	Ĩ
	 A adminiţicit 		Last lane	
	• • •		🔎 Job Title	
	* III Ind		Chart frame	
	C Prove Select Country- V		Cell Phone - Select Company - · ·	
	XASOT		Ø Bype	
	Generate New Image Enter The Code		Submit	
	© 2015 C	heckma	arx (Top	



(i) The required password complexity is as follows:

- 9 to 400 characters
- At least 1 uppercase letter
- At least 1 lower case letter
- At least 1 special character
- At least 1 digit
- 3. Type the captcha text, and click **Submit**.

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

To confirm a user account:

1. In Users & Teams displayed.

دک Users & Teams 🗕

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

CHECKMARX V72.0	(^/) Dashboard +	Projects & Scans 👻	Ç} Management ↓	2). Users & Teams +	🔘 Data Analysis	2 My Profile					Welcome admin admin	() Logout
Users & Teams / Confirm Users												
										file 7 Filters	但 Group By	0
CREATED DATE =	USER NAME		E-MAIL			FULL NAME	COMPANY NAME	COUNTRY	EXPIRATION DATE	TEAM		
						There are no records						
4 4 1 5 5	Page size: 10	Ŧ									0 items in	1 pages

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

You can view additional information about the user by hovering over the 1 . You can delete the request.

- 3. Optionally, change the Expiration date and/or Group (Team).
- 4. Click \checkmark to confirm the request.



Managing Existing Users

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

ers & Teams / Orga	nization / User Ma	nagement									
+ Create New User								🗇 🖓 Filte	rs 🕀	Group I	By O
SER NAME	E-MAIL	FULL NAME	COMPANY	LAST LOGIN DATE	TEAM	ROLE	AUDITOR	DATE CREATED	ACTIVE	Ŧ	1
avidp	david.pressdee	admin admin	A restriction of the second se	4/12/2017 11:56:37	CxServer	Server Manager	æ	11/22/2016 9:34:20	0x	Ca.	-
puser1@checkma.	spuser1@check.	SP User 1	Company		Users,Team 1	Scanner	×.	1/10/2017 4:26:07	∂ _k	20	٥
M\davidp	David Pißcheck	David P	Company		Users	Scanner		2/20/2017 9:25:43	0×	යිං	Ū
AVIDP-LAPTOPVA_	davidp@checkm	David P	Company		Users	Scanner		3/29/2017 11:57:53_	∂_{k}	25	0
Account informat	Page si	ze. 10 • •)								4 items	in 1 page
Account informat	tion Securit	ze 10 *			Team : ,	් එ වූ CuServer				4 items	in 1 page
Account informat * First Name: * Last Name:	tion Securit admin	ze: 10 ¥			Team :	× 2 CuServer ■ 2 Sp				4 items	in 1 page
Account informet First Name: Last Name: Company:	Page si tion Securit admin admin	ze: 10 *			Team:	Øඩු CoServer මඩු SP මඩු Co	mpany. Users			4 items	in 1 page
Account informat * First Name: * Last Name: Company: Job Title:	Page sit	ze: 10			Team :	්ඩු CoServer මෙහි SP මෙහි Co මෙහි Co මෙහි Co	mpany Users Team 1			4 items	in 1 page
Account informat * First Name: * Last Name: Company: Job Trile: * Email:	Page si tion Securit admin admin david	y y	rx.com		Team :	 ✓ (2) CuServer □ (2) SP □ (2) CuServer □ (2) CuServer	mpany Users Team 1 Provider 1			4 items	in 1 page
Account informat * First Name: * Last Name: Company: Job Title: * Email: Phone:	Page si tion Securit admin admin david, 052.	y y	ux.com		.Team :	 ※役、Colserver 回及、SP 回及、Coll 回及 回及 回及、Service ●役、Service 	mpany Users Team 1 Provider 1 Team 1			4 items	in 1 page
Account informa * First Name: * Last Name: Company: Job Title: * E-mail: Phone: Cell Phone:	Page si tion Securit admin admin david 052	ze: 10	xx.com		Team :	 ✓ A CiServer □ A SP □ A Co □ A Co □ A Co □ A SP 	mpany Users Team 1 Provider 1 Team 1			4 items	in 1 page
Account informat * First Name: * Last Name: Company: Job Title: * E-mail: Phone: Cell Phone: * Role:	Page si tion Securit admin admin david.j 052.	ze 10	rx.com		Team i	Coserver Cos	mpany Users Team 1 Provider 1 Team 1			4 items	in 1 page
Account informa * First Name: * Last Name: Company: Job Thie: * E-mail: Phone: Cell Phone: * Role: Auditor	Page si tion Securit admin admin danid 052 2ema 97	ze 10 ▼ y pressdee⊜checkma Manager	rx.com		Team :	Conserver Conser	mpany Users Team 1 Provider 1 Team 1			4 items	in 1 page
Image: Second	Page si tion Securit admin admin david 052	ze 10 V	ex.com		Team:	× Q CuServer	mpany Uses Team 1 Provider 1 Team 1			4 items	in 1 page
Image: Second	Page si tion Securit admin admin david, 052. Cerres Ø Englis	y y pressdee@oheckma	rx.com		Team:	 A (2) CoServer A (2) SP 	mpany Users Team 1 Provider 1 Team 1			4 items	in 1 page

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

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

- 1. Select the user in the table to display below the table their personal User Details.
- 2. Below the User Details, click **Edit**.
- 3. Select the desired group: SP, Company, or Team.
- 4. Select the appropriate Role for the desired level of authorization. Click **Update**.



In the table, Server, SP, and Company Managers can deactivate users (

Users can edit some of their own details from the Getting to Know the System Dashboard.

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



Managing Teams

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

To manage these Teams:

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

V 8.1.0	(/) Dashboard +	C) Projects & Scans -	्री Management -	2 <u>3</u> Users & Teams -	⊘ Data Analysis	යියා My Profile			Welcome admin admin	() Logou
sers & Teams / Organization /	Team Management			1	9					
+ Create New Team							10 S	7 Filters	Group By	0
TEAM NAME		COMP	ANY		SER	VICE PROVIDER				1
Team 1		Compr	any 1		Serv	vice Provider 1				1
Team 1		Compa	any 2		Serv	vice Provider 1				đ
Team 2		Compa	any 1		Serv	vice Provider 1				Û
Team 2		Compa	any 2		Serv	vice Provider 1				前
		Compa	iny 1		Serv	vice Provider 1				Û
Team 3										Û
Team 3 Team 3		Compa	iny 2		Serv	rice Provider 1				
Team 3 Team 3 Team 4		Compa	ny 2 ny 2		Serv	vice Provider 1 vice Provider 1				Ē
Team 3 Team 3 Team 4 Team 4	Page size: 10	Compa Compa Compa	any 2 any 2 iny 1		Serv Serv	rice Provider 1 rice Provider 1 rice Provider 1			8 items in	1 pages
Team Users	Page size: 10 ••	Compa Compa Compa Compa	ny 2 ny 2 ny 1		Sen	vice Provider 1 vice Provider 1 vice Provider 1			8 items in	II II 1 pages
Team 3 Team 4 Team 4 Team 4 Team Users Team 0 + Add a user to the Team	Page size: 10 •• letails Mapped + Create New User	Comps Comps	ny 2 ny 2 ny 1		Serv	rice Provider 1		Ø	8 items in T Filters	1 pages
Team 3 Team 4 Team 4 Team 4 Team Users Team 1 + Add a user to the Team FULL NAME	Page size: 10 Netails Mapped + Create New User	Comps Comps Groups E-MAIL	ny 2 ny 2 ny 1		Serv Serv RDLE	ice Provider 1 vice Provider 1 vice Provider 1		C	8 items in	1 pages
Team 3 Team 4 Team 4 Team 4 Team 4 Team Users Team Users Team Users FUL NAME AutoFirstname AutoLastname	Page size: 10 • Netails Mapped + Create New User	Compa Compa Compa Groups E-MAIL auto@che	ny 2 ny 2 ny 1		Serv Serv Serv ROLE Reviewer	vice Provider 1		Ø	8 items in	1 pages
Team 3 Team 4 Team 4 Team 4 Team Users Team 0 + Add a user to the Team FULL NAME AutoFirstname AutoLastname User 1 C1	Page size: 10 • Netails Mapped + Create New User	Compa Compa Compa Groups E-MAIL auto@che user1@op	ny 2 ny 2 ny 1 ckmarx.com enidap.com		Serv Serv ROLE Reviewer Scanner	vice Provider 1		()	8 items in	1 pages



Creating a Team

To create a new Team:

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

Select a **Parent Company** on the Organizational Tree and enter a new **Team Name** into the field.

Click Create. The new Team is displayed in the Team list.

You can now add User to the Team.

Adding a User to a Team

To add a User to a Team:

Select the Team from the Team list.



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

FULL NAME A	E-MAL
AutoFirstname AutoLastname	auto@checkmarx.com
User 1 C1	user1@openIdap.com
User 2 C1	user2@openIdap.com
Page size:	2 items in 1 manual

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

In certain cases, you may need to create a new user (see <u>Creating and Managing User</u> <u>Accounts</u>).

Click on the **Team Details** tab to view Team information.



Mapping LDAP Directory User Groups to CxSAST Teams

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

To map an LDAP User Group to a CxSAST Team:

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

Team Users	Team Details	Mapped Groups		
+ Add Group Ma	pping Save	Cancel		
- ActiveDirect	oryLdap			

Click Add Group Mapping. The Directory Group window is displayed.

Directory :	- Select One - 🛛 🖤	
Search Groups 1	Contains 👻	Find
CHOLPHANE	GHOLP DR	
	There are no re	cords
		OK V Cancel X

Select an LDAP Directory from the drop-down (e.g. ActiveDirectoryLdap) and click Find.



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

Team Users	Team Details	Mapped Groups
+ Add Group May	opping Save	Cancel
 ActiveDirecto 	oryLdap	
L QA 🗊		

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

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



Changing SAML User Teams and Roles in the CxSAST

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

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

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

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

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



CHOCKMARX V 8.5.0 [SDLC]	C ∧ Dashboard →	Projects & Scans →	رچ Management –	دی Users & Teams 👻	⊘ Data Analysis	යිලා My Profile
Users & Teams / Organization	n / User Management					
+ Create New User						
USER NAME	E-MAIL		FULL NAME	COMPANY		LAST LOGIN DATE
thierry	admin@cx	ι.	admin admin			9/3/2017 3:49:50 PM
test@user1.com	test@user	1.com	Test 1 User 1	Company		
ff@yopmail.com	ff@yopma	il.com	rwe fgfr			
a@b.com	a@b.com		ttt aaa	Company		
test2@user.com	test2@use	er.com	u u	Company		
test3@user.com	test3@use	er.com	mm	Company		
qq@qq.com	qq@qq.co	m	99 99	Company		8/16/2017 3:16:11 PM
Account information	Page size: 10	*				
* First Name:	Thierry			Team :	▼ □ 2 CxServer	
* Last Name:	Carsenty				T □ ℓA SP	
Company:	Company				• 🛛 🕁 ເຜ	Ilsere
Job Title:					▼ □ ℓ ₂ Test_i	Provider
* E-mail:	thierry.carsenty@cl	eckmarx.com				
Phone:	123456789					
Cell Phone:	123456789					
* Role:	Reviewer	tatus changes	Ψ.			
Auditor		10741				
Skype:						

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

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

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


Managing the Organizational Hierarchy

To manage the organizational hierarchy, go to **Users & Teams** > **Organization**. Available actions depend on the permissions of the logged-in user.

Tree Branch View

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

V7.2.0 Dashboard - Projects &	} Scans ★ Management ★	23. Users & Teams 👻	📿 Data Analysis	Co My Profile	Welcon admin ad	ne Min 🕛 Logout
Users & Teams / Organization / Tree Branch View						
Organizational Tree			Users			
+ Create New Team 🔟 Delete	+ Add User			¢	🖓 Filters 🗐 Group By	0
▼ 2B CxServer	E-MAIL	FULL NAME		ROLE		
😾 کے sp	howie@checkmarx.com	Howie Howe	rton	Scanner	88	
Company	john.doe@email.mail	John Doe		Scanner	000 000	
		Page size: 10			2 items in	1 pages
	© 2015	6 Checkmarx Top				

+ Create New Team

+ Add User

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



Team Management

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

CHECKMARX V72.0	(*/ Dashboard •	Projects & Scans -	🖉 Management -	25. Users & Teams -	⊙ Data Analysis	Co My Profile				Welcome admin admin	() Logod
Users & Teams / Organization /	Team Management										
+ Create New Team								0	Filters	E Group By	0
TEAM NAME A			0	OMPANY			SERVICE PROVIDER				
Users			C	Company			SP.				Û
4 4 1 5 1	Page size: 10	v								1 items in 1	pages
Team Users Tea	m Details										
+ Add a user to the Team	+ Create New	User							0	Filters	0
FULL NAME A			E-M	AL			ROLE				
						There are no reco	rds				

Each team-management window includes a table listing all the existing team of that level. To create a new team at the managed level (for example, in SP Management, to create a new SP),

click + Create New Team. The Create New Team window is displayed.



ιν	

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

2		
▼ 2 CxServer	-	
◆ 28 SP		
Select a Parent Company from the Tree		
		8
Enter Team Name: PPS		
iter Team Name: PPS		

In the Team Management window, click to add a new user to the Team. The Add a user to the Team window is displayed.



FULL NAME 🛦	E-MAIL	
Bill Doe	b@doe	
Joe Doe	j@doe	
Keiichiroh Akiyama	kelichiro_a	kiyama@iwi.co.jp
test-iwi user1	sichi.br761	9@gmail.com
	() A (0)	

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

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

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

Add User					
	● Create N ○ Add Exi	╋ Vew User sting User			
			Next 🕨	Cancel	×

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



	plication User main User				
First Name:					
Last Name:					
E-mail:					
User Name:					
Password:					
Confirm Password:					
Job Title					
Phone					
Cell Phone					
T	20	10			
Team:	PS	10			
Role:	- Select One -	Ŧ			
Auditor:					
Skype:					
Country:	Select One	Ŧ			
Expires:	6/7/2018				
Language	English (United State	-			

When selecting Add Existing User, the following window is displayed.

			D Filters	Group By
E-MAIL	FULL NAME	COMPANY	TEAM	ROLE
j@doe	Joe Doe	Company	Company	Company Manager
keiichiro_akiya	Keiichiroh Akiyama	Company	Users	Scanner
tole Select One		v		

Select the user and click **Add**.



Management Settings

In this section:

- Scan Settings
 - o Query Viewer
 - o Preset Manager
 - Predefined Presets
 - Limiting Engine Scans
- Connection Settings.
- Application Settings
- Maintenance Settings
- Managing Custom Fields
- My Profile Settings

Scan Settings



Query Viewer

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

To open the **Query Viewer**:

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



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



Preset Manager

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

To open the **Presets Manager**:

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

CHOCKMARX (8.8.0 [SDLC] (xpires: 6/13/2018	CA Dashboard ~	Projects & Scans 🗣	J? Management ~	දය Users & Teams	⊘ → Data Analysis	کے My Profile	Codebashing	G Services & Support	admin admi U Logout
anagement / Scan Settings	/ Preset Manager	4					2		
Drag a column header and dro	p it here to group by the	it column		P	reset name Checkmarx Defa	ult			
+ Create New Preset	Export Preset 🕘	Import Preset	🖓 Filtera 🗐 Group	By O	Express	on_Language_Injection_0	INL		^
PRESET			OWNER	ACTION	- 💽 💌 LDAP_In	jection.			
All				10	Reflecte	d_XSS_All_Clients			
Android				00	Resourc	e_Injection			
Apple Secure Coding Guide				10	IN Second	Order_SQL_Injection			
Checkmarx Default				00	I C Stored	(SS			
Default				00	- R (8) XPath_le	ijection			
Default 2014				ÛD	Java_Low_Vi	sibility			
Empty preset				00	► 🖃 🗄 Java_Mediun	_Threat			
Error handling				00	► 🖬 j∃ Java_Potenti	al			
FISMA				to.	Edit 🗸				
Query Description				*					
SQL_Injectio Risk What might happen An attacker could direct credit cards), and possib	n ly access all of the sy ily change or erase er	stem's data. Using sim; xisting data.	ple tools and text editin	ig, the attacker wo	build be able to steal any se	ensitive information sto	red by the system (su	th as personal user deta	ls or
1									, ,
				© 2018 Che	ckmarx Top				

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

Click Create New Preset to create a new preset.



Pre & Post Scan Actions

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

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

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

8.8.0 [SDLC] pires: 6/13/2018	CA Dashboard -	Cd Projects & Scans 🐱	J Management -	ے۔ Users & Teams 🗣	⊘ Data Analysis	යිලා My Profile	Codebashing	G Services & Support	admin adm Logou
nagement / Scan Setting	s / Pre & Post Scan Acti	ions	ans.						
+ Create New Action								🔞 🖓 Filtera	徂 Group By 〇
AME			COMMAND			TYPE			
itHub			git.bat			Post Scan Action			0
Details									
Details * Name:	GirHub								
Details * Name: * Command:	GifHub git.bat	None	×						
Details * Name: * Command: Arguments:	GirtHub git.bat	None. None	×						
Details * Name: * Command: Arguments: Edit 🗸	GirHub git.bat	None None	V.						

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

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



Source Control Users

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

To open **Source Control Users**:

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

Management / Scan Bettings / Source Control Users UESE RAME EMitsoulies	CHOCKMARX V 8.8.0 [SDLC] Expires: 6/13/2018	CA Dashboard -	C. Projects & Scans 🗣	J Management -	ے۔ Users & Teams 🗣	⊘ Data Analysis	යින My Profile	eee Codebashing	G Services & Support	admin admin 🖒 Logout
USER KAARE EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTendere EMTEndere EMTENDERE	Management / Scan Settings	/ Source Control Users								
USER HAME OMIsoulies Verden Cardeonials Verden Cardeonials Verden Cardeonials PROJECT HAME PROJECT HAME VESCOAT, OBA, SIGAN UNC sedminifice Codenver Verden Cardeonials Vestor									(B)	√ Filters
BMranker I M M Page size: 10 ▼ I Dems in 1 pages Update Credentials PROJECT NAME TPRE VMER TEAM WEBGOAT, OBA_SCAN UNC admin@cx Coderrer I Dems in 1 pages	USER NAME									
Image:	DM\svalero									
Items in 1 pages Update Credentials IP PROJECT NAME TYPE OWNER TEAM WEBBOAT_DSA_SCAN UNC admin@cs Cristerie Items in 1 pages										
Items in 1 page V Updare Credentials PROJECT NAME TYPE OWNER TEAM WEBGOAT_OSA_SCAN UNC admin@cx Cr.Server										
Image: 10 mm 1 interns in 1 pages										
Image:										
Image size: 10 v										
Image: size										
Image: Section Image: Sectio										
Update Credentials Filters Croup By PROJECT NAME TYPE OWNER TEAM WEEBGOAT_OSA_SOAN UNC admin@cx CrServer		Page size: 10	T							1 items in 1 pages
PROJECT NAME TYPE OWNER TEAM WEBGOAT_OSA_SCAN UNC admin@cx CxServer	Update Credentials								© ∏ Filters i	E Group Sy
WEBGOAT_DSA_SCAN UNC admin@cx CxServer	PROJECT NAME		TYPE		0	VNER		TEAM		
1 items in 1 pages	WEBGOAT_OSA_SCAN		UNC		ad	min@cx		CxServer		
1 Items in 1 pages										
Image: The size: 10 The size: 10										
Items in 1 pages										
1 items in 1 pages										
1 items in 1 pages										
Image: size 10 The size 10 10 10 10 10 10 10 10 10 <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>										
Image: State of the state o										
		Page size: 10	*							1 items in 1 pages
© 2018 Checkmarx Top					© 2018 Checkman	Top				

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

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



Query Viewer

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

To open the Query Viewer:

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



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



Creating a Custom Description

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

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

To create a custom description:

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

Click **Create Custom Description**. The **Upload File to Create Custom Description** window is displayed.

Custom Des	scription
Only HTML files are allowed	Choose file
Uploa	d

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



- For security reasons CxSAST only supports the following HTML tags, attributes and inline styles:
 - **Tags** b, br, caption, center, col, colgroup, dir, div, dl, dt, em, fieldset, font, footer, h1, h2, h3, h4, h5, h6, header, hr, i, li, ol, p, pre, span, strike, strong, table, tbody, td, tfoot, th, thead, tr, u, ul,
 - Attributes align, alt, bgcolor, border, cellpadding, cellspacing, charset, color, cols, colspan, dir, height, lang, list, nowrap, radiogroup, rows, rowspan, selected, size, span, style, title, valign, value, vspace, width, wrap
 - Styles (CSS values) background, background-color, background-position, background-repeat, border, border-bottom, border-bottom-color, border-bottomstyle, border-bottom-width, border-collapse, border-color, border-left, border-leftcolor, border-left-style, border-left-width, border-right, border-right-color, borderright-style, border-right-width, border-spacing, border-style, border-top, border-topcolor, border-top-style, border-top-width, border-width, bottom, caption-side, clear, clip, color, content, counter-increment, counter-reset, cursor, direction, display, empty-cells, float, font, font-family, font-size, font-style, font-variant, font-weight, height, left, letter-spacing, line-height, list-style, list-style-image, list-style-position, list-style-type, margin, margin-bottom, margin-left, margin-right, margin-top, maxheight, max-width, min-height, min-width, orphans, outline, outline-color, outlinestyle, outline-width, overflow, padding, padding-bottom, padding-left, padding-right, padding-top, page-break-after, page-break-before, page-break-inside, quotes, right, table-layout, text-align, text-decoration, text-indent, text-transform, top, unicodebidi, vertical-align, white-space, widows, width, word-spacing, z-index.

If you try to upload a file with anything else other than what is listed above, the description will not be saved.



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



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

Importing Queries

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

To import queries:

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

File name:	Select

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



Exporting Queries

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

To export queries:

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

_			
(i)	You can export corporate of Please select corp queries	You can export corporate queries. Please select corp queries to export.	

Click OK.



Preset Manager

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

To open the Preset Manager:

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

8.8.0 [SDLC] xpires: 6/13/2018	Dashboard 👻	Projects & Scans 👻	Management ~	Users & Team	ns 🛥 🛛 Data Analysis	My Profile	Codebashing	Services & Support	() Logour
anagement / Scan Settings	/ Preset Manager	л.	999.00 (C	A.					
orag a column header and dro	p it here to group by tha	t column			Preset name Checkmarx Defau	da			
+ Create New Preset Export Preset Import Preset PRESET All Android Apple Secure Coding Guide Checkmarx Default Default Default Empty preset Error handling		V Filters 3 Croup	ру С Астон ФО ФО ФО ФО ФО ФО	Image: Constraint of the second se					
FISMA				00	Edit				
Query Description									
SQL_Injectio Risk What might happen An attacker could direct credit cards) and possi	n ly access all of the sy	stem's data. Using simp xisting data.	e tools and text editir	ng, the attacker v	would be able to steal any se	nsitive information sto	red by the system (su	ch as personal user detai	ls or
creat caras), and possio	ny change of erase e	kisting data.							>

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



Creating a New Preset

To create a new preset:

From the **Preset Manager**, click **Create New Preset**. The Create New Presets window is displayed.

Create New	Preset		
"Name:	5 		
		Create 🗸	Cancel X

Enter a preset **Name** and click **Create**.

Select a Coding Language.

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

Click Save.

Modifying an Existing Preset

To modify an existing preset:

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

Select a Coding Language.

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

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

Click Save.



Importing a Preset

To import a preset:

From the **Preset Manager**, click **Import Preset**. The Import Preset window is displayed.

Select

Click **Select**, navigate to the preset (.XML file) and click **Open**.

① If the imported preset has the same name as an existing one, the existing preset will be overridden.

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

Exporting a Preset

To export a preset:

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

Deleting a Preset

To delete a preset:

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



Predefined Presets

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

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



Preset	Usage	Includes vulnerability queries for
Error Handling	For error handling related application security risks	Apex, ASP, CPP, CSharp, Java, Perl, PHP, Ruby and VbNet coding languages
FISMA	For homeland security application risks according to the 'Federal Information Security Modernization Act' compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
High and Medium	For high and medium related application security risks	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
High, Medium and Low	For high, medium and low related application security risks	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
HIPAA	For sensitive patient data related security risks according to the HIPAA (Health Insurance Portability and Accountability Act) compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Typescript, VB6, VbNet and VbScript coding languages
JSSEC	For Android related application security risks according to the JSSEC (Japan's Smartphone Security Association) compliance guidelines	Groovy and Java coding languages
MISRA_C	For C related application security risks according to the MISRA (Motor Industry Software Reliability Association) compliance guidelines	C++ coding language
MISRA_CPP	For C++ related application security risks according to the MISRA (Motor Industry Software Reliability Association) compliance guidelines	C++ coding language



Preset	Usage	Includes vulnerability queries for
Mobile	For mobile related application security risks	CSharp, Groovy, Java, JavaScript and ObjectiveC coding languages
NIST	For the application security risks according to the 'National Institute of Standards and Technology' compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
OWASP Mobile TOP 10-2016	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2016	CSharp, Groovy, Java, JavaScript and ObjectiveC coding languages
OWASP TOP 10-2010	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2010	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Typescript, VB6, VbNet and VbScript coding languages
OWASP TOP 10-2013	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2013	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
OWASP TOP 10-2017	For the top 10 web application security risks according to the OWASP (Open Web Application Security Project) compliance guidelines for 2017	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet and VbScript coding languages
PCI	For credit card payment application security risks according to the PCI (Payment Card Industry) compliance guidelines	Apex, ASP, CPP, CSharp, Go, Groovy, Java, JavaScript, ObjectiveC, Perl, PHP, PLSQL, Python, Ruby, Scala, Typescript, VB6, VbNet, and VbScript coding languages



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



Limiting Engine Scans

To Limit Engine Scans:

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

Server Name:			
* Server URI:			
* Scan LOC limits:	From:	To:	

The Adding Engine Server window includes the following properties:

- Server Name: The name of the server you are appointing as Engine Server
- Server URI: The address of the server
- Scan LOC limits: The Scan limits is <u>not</u> a mandatory field, in the event the fields are left empty assume the value From to include: All to: All. Define the lower and higher limits for size of projects that this engine can accept for scanning.
 - When the range is defined and the user clicks OK, the system performs a check of range continuity. In the event there is no continuity between ranges of all engines defined at that moment, a pop-up message is displayed: "Line 1: "Notice: Projects including the following ranges: line 2 : XXX YYY line 3: more then 1000 Line 4: Will not be scanned."
 - In the event the scan size falls out of defined engine ranges, the scan fails and the following message is displayed: "Scan has failed due to falling outside of the defined engines scan ranges".
 - After defining the scan engine range, in order to activate the user has to Restart the scan manager service.



Connection Setting

In this section:

- LDAP Management
- SAML Management



LDAP Management

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

Adding an LDAP Server

To add a new LDAP Server:

Select **Management** > **Connection Settings** > **LDAP Servers**. The LDAP Server window is displayed.

		1 Delete
+ Add New Server		
Global LDAP Configuration		
Synchronization default parameters (User Authorization Management) Applied only when synchronization is enabled		
Manual Role Authorization (Manage user role creation in LDAP and perform authorization locally on the CxServer)		
LDAP Role Authorization (Automatically update user role upon login)		
	× Cancel	Save Save

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

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



Configuring LDAP Authentication Settings

To configure LDAP Authentication settings:

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

Base DN cn=users,dc=example,dc=com Additional User DN ou=People ①	User Object Schema User Object Schema User Object Filter (object Category+Person)]0
Base DN Cn=users,dc=example,dc=com Additional User DN Cou=People ①	User Object Schema user,inetOrgPerson User Object Filter (objectCategory#Person)]0
cn=users,dc=example,dc=com Additional User DN ou=People	User Object Filter (objectCategory=Person)]@
Additional User DN cu=People	User Object Filter (objectCategory=Person)	1
ou+People ①	(objectCategory=Person)	and a second
	Dest Nama Attributa	0
	Call transic vitrabile	
	sAMAccountName	0
	User RDN Attribute	
	cn, sAMAccountName	0
	User First Name Attribute	
	givenName	۲
	User Last Name Attribute	
	sn	0
	User Email Attribute	
	mail	0
n Management)		
oon login. Otherwise, LDAP is used for authentication only. ta (mie and team) will not be updated		
	n Management) oon login. Otherwise, LDAP is used for authentication only. ta (role and team) will not be updated	User First Name Attribute givenName User Last Name Attribute Sn User Email Attribute mail Management) pon login. Otherwise, LDAP is used for authentication only. ta (role and team) will not be updated



Define the following Authentication parameters:

Parameter	Description
Name	Server name
Directory Type	 Provides auto selection for server parameters according to default settings (ActiveDirectory, OpenLDAP, or LDAP Server) Enable SSO (Map LDAP to Directory Domain) - Selecting this option ensures that SSO users are automatically created upon login and synchronized as LDAP users Domain - Select the relevant domain for this LDAP configuration.
Host Name	DAP server hostname (e.g. Idan company com)
Port	 Port of the LDAP server (e.g. 389, 636 (for SSL)) Use SSL - Selecting this option ensures that all information passed between the server and the client remains private Verify SSL Certificate - Selecting this option ensures SSL certificate verification
User Name	Name of the user that the application uses when connecting to the LDAP server (e.g. user@domain.name or cn=user,dc=domain,dc=name) NOTE: You can enable or disable the use of the LDAP control extension for paging of search results. If paging is enabled (default), the search will retrieve sets of data rather than all of the search results at once. Therefore, if you are searching for a specific user then the definition in the User Name field should also be specific (using full user DN, e.g. dn=myuser,ou=people,dc=company,dc=com)
Password	Password of the user specified above
Base DN	Used to search for users (e.g. cn=users, dc=example, dc=com)
Additional User DN	Used to limit users search to specific DN (e.g. ou=People)



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

Click **Save** to save the changes.

Click Test Connection.

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



Configuring LDAP Synchronization Settings

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

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

To configure LDAP Synchronization settings:

Check Enable Synchronization. The LDAP Synchronization window is displayed.

Synchronization (User Auth Use synchronization to automatically create and Admin users' (company managers and above) at	orization Managemei update user upon login. Otherwise, LE ithorization data (role and team) will n	ND is used for authentication only. ot be updated	
Enabled synchronization			
Group Schema Settings		Membership Schema Settings	
Additional Group DN		Group Members Attribute (member)	
ou-Groups	0	member	0
Group Object Schema		User Membership Attribute (memeberOf)	
group	•	memberOf	0
Group Object Filter			
(objectCategory=Group)	0		
Group ID Attribute (CN)			
cn	0		
Group Name Attribute			
name	(?)		

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



Define the following Synchronization parameters:

Parameter	Description
Additional Group DN	Used to limit groups search to specific DN (e.g. ou=Groups)
Group Object Schema	LDAP group object type (e.g. group)
Group Object Filter	LDAP filter expression to use when searching the groups (e.g. (objectCategory=Group))
Group ID Attribute (CN)	Attribute in LDAP defining the group's id (e.g. cn)
Group Name Attribute	Attribute in LDAP defining the group's name (e.g. name)
Group Members Attribute (member)	LDAP member attribute is a multi-value attribute that contains the list of distinguished names for the user, group, and contact objects that are members of the group (e.g. member)
User Membership Attribute (memberof)	LDAP membership attribute is a multi-valued attribute that contains groups of which the user is a direct member (e.g. memberOf)



Defining User Management (Synchronization)

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

lobal LDAP Configuration		
Synchronization default parameters (User Authorization Management) Applied only when synchronization is enabled		
Manual Role Authorization (Manage user role creation in LDAP and perform authorization locally on the CxServer)		
LDAP Role Authorization (Automatically update user role upon login)		
	× Cancel	B Save

Select the preferred Synchronization Default Parameters:

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

Click **Save** to save the changes.



Defining Role Mapping Settings

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

Default Role ID	
Scanner 🔻 🧿	
Allow to apply not exploitable state Allow to delete Projects\Scans	
Advanced Role Mapping	
Scanner	Reviewer
Scanner without authorities Group DN	Reviewer without authorities Group DN
cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org	cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org
Scanner with only Allow to apply not exploitable state option Group DN	Reviewer with all authorities Group DN
cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org	cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org
Scanner with only Allow to delete Projects\Scans option Group DN	
cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org	
Scanner with all authorities Group DN	

Define the following Role Mapping parameters:

Parameter	Description			
	Used to determine the CxSAST role of users who have otherwise not been assigned roles (e.g. Scanner, Reviewer)			
Default Role ID	 Scanner - can delete projects\scans if the checkbox is selected. Select the Not Exploitable state checkbox to provide authorization to apply not exploitable state to instances Reviewer - can make changes to the status or severity of found instances if the checkbox is selected 			



Parameter	Description
Advanced Role Mapping	Role mapping in CxSAST can be managed by checking the Advanced Role Mapping checkbox and the defining the parameters below.
	NOTE: Roles managed by LDAP are automatically updated upon login to CxSAST.
Scanner without authorities Group DN	Used to define a list of LDAP Group DNs. Members of these groups will be assigned the scanner role without Apply Not Exploitable State and Delete Projects\Scan options (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Scanner with only Allow to apply not exploitable state option Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the scanner role with only Apply Not Exploitable State option (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Scanner with only Allow to delete Project\Scans option Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the scanner role with only Delete Project\Scans option (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Scanner with all authorities Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the scanner role with Apply Not Exploitable State and Delete Projects\Scan options (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Reviewer without authorities Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the reviewer role without Allow Severity/Status Change options (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).
Reviewer with all authorities Group DN	Used to define a list of LDAP Group DNs. Members of this group will be assigned the reviewer role with Allow Severity/Status Change options (e.g. cn=dev, ou=grp, dc=my, dc=org, cn=qa, ou=grp, dc=my, dc=org).

Click **Save** to save the changes.

In order for users to automatically log in using Synchronization, complete <u>Mapping LDAP</u> <u>Directory User Groups to CxSAST Teams</u>



SAML Management

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

(i) SAML login for CxAudit is currently not supported.

Configuring SAML in CxSAST

Before you start with Configuring SAML in CxSAST, **Enabling HTTPS on the CxSAST Server** and **Configuring the Identity Provider**_are required in order to proceed.

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

HECKMARX ⁰ [SDLC] Dashboa	ard - Projects & Scans -	्री Management -	산 <u>라</u> Users & Teams 🝷	🔍 Data Analysis	ද්ලා My Profile	AppSec Coach	admi じ
ement / Connection Settings / SAM	L	1					
SAMI 1/2 01 CYSAMI							
CAME [V2.0]. OXOANE							
Enable SAML O Dis	able SAML Enable will open abi	lity to use SAML and effect I	ogin screen				
Authentication			JUser Au	uthorization M	anagement		
Identity Provider Name *③			Use Manual	Authorization to r	manage roles and team	ams locally on CxServer	
CxSAML			• Manu	al Authorization ()	O IdF	Authorization	
Issuer (Identity Provider) *			l free	4	0.81		
https://checkmarx.corp	o.net		Default Te	eam 🛛	Detaul	t Role 🔿	
Login URL * 💿			• • 4	ሲ CxServer		wei ,	
https://corp.okta.com/home/corp_cxsaml_1/0123456789/abcdefgh				ੇ ਸ਼ੁਰੂ ਂ ਹੈ. ੇ Compar	1y	w sevency/status changes	
Logout URL® Error URL®			🕈 🗷 🖓 User	rs 🗸			
https://checkmarx.corp	o.net/Cx1 https://checkr	marx.corp.net/Cx\	4		•		
Sign SAML IDP Requests	0		🕁 Down	load Metadata			
SP Certificate File 💿							
	heckmarx\Configuration\SA	🗋 Choose file	IDP Ce	ertificate			
Certificate Password		IdD Contine	to Filo * 🔿				
		Cert.cert	ne File 🧐		C Choose file		



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

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

Fill the following Authentication parameter fields:

Parameter	Description
Identity Provider Name	Name given to the SAML Identity Provider (e.g. CxSAML)
Issuer (Identity Provider)	Element which contains the unique identifier of the IdP, and will usually contain the URL of the IdP and a hash (e.g.: http://www.okta.com/exkac5ylseLJUQLeZ0h7). This parameter is provided by the Identity Provider setup information (see the CxSAST Plugin and Integration Guide > Configuring the Identity Provider for SAML).
Login URL	Identity Provider login location where SAML requests will be sent (e.g. https://corp.okta.com/home/corp_cxsaml_1/0123456789/abcdefghij). This parameter is provided by the Identity Provider setup information (see the CxSAST Plugin and Integration Guide > Configuring the Identity Provider for SAML).
Logout URL	Location where logout instances will be redirected (e.g. https://checkmarx.corp.net/CxWebClient).
Error URL	Location where error instances will be redirected (e.g. https://checkmarx.corp.net/CxWebClient/ErrorPages/Default_Error.aspx).
lssuer (Audience)	The local server name is the issuer by default. Changing the default is done in the database: [CxDB].[dbo].[CxComponentConfiguration], [Key] = 'SamlServiceProviderIssuer', [Value]= ' <sp issuer="">'</sp>
CxSAST Login URL	The local server name is the host name by default. Changing the default is done in the database: [CxDB].[dbo].[CxComponentConfiguration], [Key] = 'WebServer', [Value]= ' <host name="">'</host>
Sign SAML IdP Requests	Select to enable the Sign SAML IdP Requests option. This assures that every request sent to the IdP server is signed with a Service Provider certificate.



Parameter	Description
SP Certificate	Click Choose File and navigate to the relevant certificate file (.p12 or .pfx formats only).
File	NOTE: The uploaded certificate file should contain a private key.
Certificate	Enter the unique password for the certificate file.
Password	NOTE: Password is only required when a certificate is added or updated.

Select the preferred User Authorization method:

Method	Description
Manual Authorization	User creation managed by the SAML Identity Provider and authorization performed manually by CxSAST user management.
	 Default Team - All new users will be added to selected default team Default Role - All new users will be added to selected default role (scanner or reviewer) Scanner - can delete projects\scans if the checkbox is selected. Select the Not Exploitable state checkbox to provide authorization to apply not exploitable state to instances Reviewer - can make changes to the status or severity of found instances if the checkbox is selected
	By default, SAML users belong to one team and are either defined as scanners or reviewers upon login. You can manually change a logged in user's Team and Role from the CxSAST (see <u>Changing the SAML</u> <u>User's Team and Role in the CxSAST</u>).
IdP Authorization	Teams and roles managed by the SAML Identity Provider are automatically updated upon login to CxSAST. The definitions for the update are defined during the creation and mapping of user attributes in the SAML IdP (see <u>Creating and Mapping User Attributes in OKTA</u>).


Method	Description
Download Metadata	The Metadata file may be required for troubleshooting by the IdP admin, or for defining missing attributes (see Configuring the Identity Provider). Click Export Metadata . The metadata file is downloaded to the default download directory (see <u>Exporting the Metadata File from CxSAST</u>).
1910taulata	The information provided in the downloaded metadata file will depend on the Manual or IdP Authentication method currently selected.

Importing the SAML Certificate into CxSAST

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

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

(i) For instances where there is no other choice but to manually install the IdP certificate file on the CxSAST server trusted root certification authority (see <u>SAML Management</u>).

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

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

Exporting the Metadata File from CxSAST

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

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

(i) The information provided in the downloaded metadata file will depend on the Manual or IdP Authentication method currently selected (see <u>SAML Management</u>).



Application Management

General

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

Server Settings

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

CHECKMARX V8.6.0 [SDLC]	(7/) Dashboard +	C. Projects & Scans 🗣	<i>S</i> Management →	کے Users & Teams →	⊘ Data Analysis	Co3 My Profile	Coach AppSec Coach	admin admin U Logout
Management / Application Set	tings / General							
Server Settings								
Reports Folder		C:\CxReports						
Results Folder		C:\Program F	iles\Checkmarx\Check	marx Jobs Manager\Res	ults			
Executables Folder		C:\Program F	iles\Checkmarx\Execu	tables				
Path to GIT client executable		C:\Program F	iles\G <mark>it\bi</mark> n\git.exe					
Path to Perforce command-line	lient executable	C:\Program F	iles\Perforce\p4.exe					
Maximum number of concurrent	scans	2 🗘						
Web Server Address				Use Current				
Long Path Support								
Default Server Language		English (Unit	ed States)			¥		

Click Edit. The setting fields are enabled.

The panel includes the following settings:

- Reports Folder Set the reports folder to save reports in (e.g. C:\CxReports)
- **Results Folder** Set the results folder to save results in (e.g. C:\Program Files\Checkmarx\Checkmarx Jobs Manager\Results)
- **Executables Folder** Set the executables folder to save executables in (e.g. C:\Program Files\Checkmarx\Executables)
- Path to GIT client executable Set the GIT client executable path (e.g. C:\Program Files\git\bin\git.exe).
 - (i) The validation of 'git.exe' and 'p4.exe' is no longer mandatory in CxSAST when defining the 'Path to GIT client executable' and the 'Path to Perforce command-line client executable' parameters.



- Path to P4 command line client executable Set the Perforce client executable path (e.g. C:\Program Files\Perforce\p4.exe)
 - If you haven't already done so, download the P4 command line executable (HELIX P4: COMMAND-LINE) from: <u>https://www.perforce.com/downloads/helix</u>, run the .exe file making sure the installed files are placed into a directory that CxSAST can access (i.e. C:\Program Files\Perforce)". Use this same directory to fill the Path to P4 command line client executable parameter field.
- Maximum number of concurrent scans Set the maximum number of concurrent scans a CxManager can run. This cannot exceed the licensed number of concurrent scans. Reducing the number of concurrent scans below the licensed amount can help to prevent the CxManager out of resources. The default is 2. CxScansManager service must be restarted before any changes to this setting will go into effect.
- **Time remaining until task completion (min)** Set the time remaining until task completion (timer).
- Web Server Address Set the web server address in order to access links in generated report from outside the organization.
- **Long Path Support** Enables long path support for the CxSAST application. Enabling long path support is required on all CxEngines and all CxManagers. Without long path support the path of source file to be scanned is limited to 260 characters.
- **Default Server Language** Set the default server language.
- Allow Auto Sign In Enable/Disable auto sign in.

SMTP Settings

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

SMTP Settings		
Host	Outgoing mail server (SMTP)	
Port	25 🗢	
Encryption Type	Noné	٣
Email From Address		
Use Default Credentials	8	
User Name		0.
Password		

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



This panel includes the following settings:

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

OSA Settings

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

er OS filename)	
0	
	er OS filename)

Click Edit. The setting fields are enabled.

This panel includes the following settings:

- Organization Token Displays the organization token provided by WS (read-only)
- OSA Scan Options:
 - **Match by File Name** Check to enable. If the SHA-1 Hash does not identify an open source library, a match is attempted using the provided filename. Results can been viewed in the 'Match Type' column in the CxOSA report.
 - Unrecognized Libraries Check to enable. Libraries not identified are viewed in a separate section the CxOSA report (Unresolved libraries). The unresolved libraries lists library format files such as '.jar' and '.dll'

(i) Enabling either of these options will handover Open Source Filename to WS.



License Details

The License Details screen is divided into the following windows:

General

The General panel provides general license information.



This includes the following information:

- Edition CxSAST license edition (SDLC or Security Gate)
- Expiration Date CxSAST license expiry date
- LOC The number of lines of code the license was bought for
- HID Hardware identification number
- **CxOSA License** Open Source Analysis license status (Enabled, Disabled or Conditional with expiration date for Conditional version).
- (i) To request a new license, if you have not yet obtained a permanent license, copy your **Hardware ID**, which you will need in order to obtain a license from Checkmarx. Or, you can later obtain your hardware ID by using the shortcut in the Windows / Start menu Checkmarx folder.



Supported Languages

Apex 🖉	M ASP	CPP	CSharp	🔲 Go
Groovy	M HTML5	🧭 Java	JavaScript	Javascript_v2
🖉 Objc	Perl	PHP	PLSQL	🐼 Python
Ruby	🗷 Scala	Swift	✓ VB6	🕑 VbNet

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

Capacity

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

CapacityCapacity				
	In Use	Available		
Users	1	10	10 %	
Auditors	1	2		50 %
Projects	12	10000000	0 %	
Number of Concurrent Scans	2	2		
			1.07	

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

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



License Expiration Notification

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

-License Expiration Not	ification-
Notification by E-mail	

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

(i) The Notification by E-mail address is defined under the E-mail Notifications parameter in Server **SMTP Settings**.

Installation Information

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

	ashboard -	LQ Projects & Scans 🛛	G Management -	다음 Users & Teams 👻	Data Analysis	C(@) My Prof	ile	ee Coach	admin () L
ement / Application Setting	/ Installation Inf	ormation							
System Components	ij.								
							0 7	Filters 🗐 Group	By O
NAME	INSTALLA	TION PATH		DNS	IP	VERSION	HOTFIX	STATE	
CheckmarxWebPortal	C:\Progra	C:\Program Files\Checkmarx\CheckmarxWebPortal\		Davidp-LapTop	10.31.0.121	8.6.0	0		
Checkmarx Audit	C:\Progra	C:\Program Files\Checkmarx\Checkmarx Audit\		Davidp-LapTop	10.31.0.121	8.6.0	0		
Checkmarx Web Services	C:\Progra	m Files\Checkmarx\Check	marx Web Services\	Davidp-LapTop	10.31.0.121	8.6.0	0		
Checkmarx System Manaç	er C:\Progra	m Files\Checkmarx\Check	marx System Manager\	Davidp-LapTop	10.31.0.121	8.6.0	0		
Checkmarx Scans Manage	r C:\Progra	m Files\Checkmarx\Check	marx Scans Manager\	Davidp-LapTop	10.31.0.121	8.6.0	0	On	
Checkmarx Jobs Manager	C:\Progra	m Files\Checkmarx\Check	marx Jobs Manager\	Davidp-LapTop	10.31.0.121	8.6.0	0	On	
Checkmarx Engine Server	C:\Progra	m Files\Checkmarx\Check	marx Engine Server\	Davidp-LapTop	10.31.0.121	8.6.0	0		



External Services Settings

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

CHECKMARX V 8.6.0 [SDLC]	CA Dashboard +	ि Projects & Scans →	√ Management →	28 Users & Teams 👻	⊘ Data Analysis	Co My Profile	600 AppSec Coach	admin admin () Logout
Management / Application Se	ttings / External Servi	ices Settings		1	1. 1	1		
External Services Sett	ings							
Status: Not active								
Checkmarx offers additiona environments in order to im providers. By activating this organization, Checkmarx ex	I tools for application prove secure coding a feature, a secure han ternal servers and the	security and development and practices using externa idshake is performed betw e external service providers	l service sen your					
Activate external services								
Codebashing Settings								
Enable Codebashing This enables login to Cod	ebashing from CxSAS	T.						
Edit ✔								
				© 2017 Checkmerx				

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

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

Click Edit. The Codebashing Settings fields are enabled.

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

Engine Server Management

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



CHECKMARX 8.6.0 [SDLC]	(7/) Dashboard +	Projects & Scans 👻	چې Management -	습 Users & Teams 👻	⊘ Data Analysis	යිකු My Profile	Coach	admin admin U Logout
anagement / Application Set	ttings / Engine Manag	ement						
Engine Manag	ement						REGISTER ENG	
Engine Server Name	Status 🛩	Eng	ine URL			Scan Si	ze	Actions
EngineServer3	A Blocked	-		e an destruction point of	i di gorinatio co	0 - 1000	0000	***
EngineServer1	⇒ Scanning	I (1 of 1) http	://localhost/CxSourc	eAnalyzerEngineWCF/C	xEngineWebServices.	svc 0-9999	999999	***
EngineServer2	I tdle	10			-	0 - 9999	999999	***

```
① The Engine Server Management screen automatically refreshes itself every 20 seconds.
```

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

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



Performing Engine Sever Management Actions

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

Register a New Engine Server

You can register a new engine server to the system.

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

Register Engine Server		Х
Server Name		
Server URI		
Scan LOC limits From:	To:	
	CANCEL	

Define the following attributes:

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

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



Edit an Existing Engine Servers Attributes

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

To edit an existing engine server's attributes:

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

Edit Engine Serve	۲.
Server Name	
Localhost	
Server URI	
http://Localhost/(CxSourceAnalyzerEngineWCF/CxEngineV
Scan LOC limits	
From:	
0	
To:	
999999999	

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

Click Update to save the changes.

Unregister an Engine Server

You can unregister an existing engine server in the system.

To unregister an existing engine server:

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



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

ن (j)	You cannot ı	unregister a	in engine se	erver that is	currently	running a	scan.
--------------	--------------	--------------	--------------	---------------	-----------	-----------	-------

Block/unblock an Engine Server

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

To block an engine server in the system:

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

Are you sure you wa	int to block this engine?	
Blocking an engine	will prohibit it from acce	epting scan
requests		
		(Company of the local days)
	CANCEL	BLOCK ENGINE

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

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



Maintenance Settings

In this section:

• Data Retention Management



Data Retention Management

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

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

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

(i) Data retention settings apply globally to all projects within the system. This global configuration can be overridden for a specific project, either during the project creation or by editing the project's setting through the Data Retention tab (see <u>Creating and</u> <u>Configuring Projects</u> and <u>Viewing Project Details</u>).

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

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



Defining Data Retention Settings

To define the data retention settings:

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

CHOCKMARX V 8.8.0 [SDLC] Expires: 6/13/2018	CA Dashboard +	Projects & Scans 🗕	} Management →	උදු Users & Teams →	📿 Data Analysis	And the My Profile	Codebashing	G Services & Support	admin admin 🖒 Logout
Management / Maintenance /	Data Retention								
	Da Sc Sc Ref	la Retention: Ins to keep: Keep last successful scans ins to delete: Select date range to delete ention duration limit (Hours)	scans	• • • • • • • • • • • • • • • • • • •	This value is required.				
				© 2018 Checkmarx	Тор		Start		

The Data Retention window includes the following settings:

Scans to keep:

• **Keep last successful scans** - Set the requested number of scans to be kept. This setting leaves only the specified number of recent successful last scans and deletes all other scans. For example, if the value is set to 10, it will keep the last 10 successful scans for each project.

Scans to delete:

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



Click Start. The following message appears:



If you are unsure whether you have backed up your database, or if the range you defined for deletion includes locked scans, click **Cancel** to postpone the deletion.

If you want to continue, click **Yes, delete it.** The following message is displayed "**Data retention is now in progress**" and the progress of the data retention process is represented in the Stages panel.

Stag	tages:		
~	Configuration		
1	Heuristic File Cleanup		
	Deleting Scans		

Once the data retention process is complete, status information about last deletion is displayed in the **Last Executed Data Retention** panel.



Execution Information:	Selected Settings:
Initiator: admin@cx	Data Retention Mode: Keep last X scans for every project
Request Date: 11/23/2015 2:19:27 PM	Number of Scans to Keep: 10
Duration: 3 Second(s)	
Stage: Finished	
Progress: 6 / 6	

Data Retention Purged Data

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

Database Tables

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

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

File System

CxSRC folder – This folder holds the extracted source files which are being scanned.
 Files and folders inside the CxSrc folder are deleted as part of data retention except for the following scenario:

In case the exact same sources (ZIP, remote location..) are uploaded to the same existing scan, the extracted folder will be excluded from further data retention cleaning tasks.

- CxReports folder This folder holds the following:
 - Reports requested by the customer and created in the CxSAST reports page.
 These reports are deleted as part of the data retention
 - Eclipse IDE reports created after each developer scan request. These reports <u>are</u> <u>not</u> deleted as part of the data retention.



Unlocking Scans

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

To unlock the scans:

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



Managing Custom Fields

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

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

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

To define custom fields:

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

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

C I I INSTUIN	el surren nen	o casto integos tos	asyctocinaspa.	and the			du.
CHECKMARX	(7) Deshboard -	f3. Projecto & Scano •	Alexander -	23 Users & Teams -	Q Ovta Analysis	Cigo Ny Profile	Welcome admin admin
agement / Manage Costom f	ields.					la la	
+ Project Ma	inager						8
+ Product Ty	ipt:						

To edit the custom field's name:

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



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

CHECKMAR)	C/A DesNoord	· Projects & 1	kans - M	S ^g magement -	23. Users & Teams -	🕑 Data Analysis	Ca My Profile				Welcome admin admin	¢.
jects & Scans / Projects	ę.		- ala	-		l						
+ Create New Project	Delete									B V files	() Group By	0
PROJECT NAME		OWNER			TEAM		PRESET	TOTAL SC	LAST SCANNED -	SCANS LIST	ACTIONS	
Prol		adminibes			CuServer		Default 2014	4	8/4/2015 10:10 AM		DDTG	1
071		adminitics			CiSever		Default 2014	1	6/30/2015 9:22 AM	0	DD70	2
shitepa		admin@cs			Cidever		Default 2014	1	6/9/2015 7:24 AM	(1)	PPTO	ŝ.
double_byte_test		adminipex			Cidener		Default 2014	2	6/3/2015-4.39 PM	0	DDTO	į.
hovie		admin@cx			CoServer		Default 2014	1	5/12/2015 8:19 PM	EB	DRTS	a.
en		adminipex			CuServer		Default 2014	Ť	5/12/2015 6-48 PM	0	0070	þ.
test_man		adminipex			CuServer/SPI/Compa	nyislaeva	Default 2014	2	5/12/2015 6:08 PM	曲	PPTO	2
Test by Or		adminiplex			CoServer		Default 2014	2	5/12/2015 5:19 PM	曲	DDTD	β.
Test 2 by Or Sc		adminifick			Cidever		Default 2014	1	5/12/2015 5:11 PM	0	DDTO	2
testproject		admin@cx			Cidener		OWASP TOP 10 - 2013	1	5/11/2015 12:14 PM	0	DRTO	<u>)</u>
4 4 1 2 5	(A) Page size:	10 (*)									13 items in 2	2 page
Monitoring Gen	ral Locatio	Scheduling	Advanced	Custom F	ields							
Project Manager Bob	Jones	-1										
Product Type Pro	unt Type											
	×											-

CHECKMARX	(7) Deckboard -	C. Projects & Scient -	l) Naragement -	Dana & Teams -	Q. Data Analysia	Can Ny Profile		Welcome edmin admin (*) 1.69
Projecte & Scans / New Projec		11		N			ų.	
	General	Locatio	20	Scheduling	Advanci	ed Actions	Custom Fields	
		Step 5: Set custs	om fields					
		Project Manager	Project Manager					
		Project Type	Project Type					
			4	Back Next 🕨	Cancel X	Pinish 🗸		
				© 2015 Checkmar	x Top			



My Profile Settings

Accessing My Profile Settings

To access My Profile settings:

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

	-	admin		
	-	admin		
	-	Job Title		
		admin@cx		
	C	Phone		
	۵	Cell Phone		
	0	Skype		
	9	English (United States)	*	
	쓥	CxServer		
			Update 🗸	
	hai	nge Passwo	ord	
С	IIai			
С		Old Password		
С		Old Password New Password	0	

* Indicates a mandatory field



Defining Profile Account Information

The Account information window includes the following parameters:

Account Information:

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

Click Update.

Changing Profile Password

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

Change Password:

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

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

Click Update.