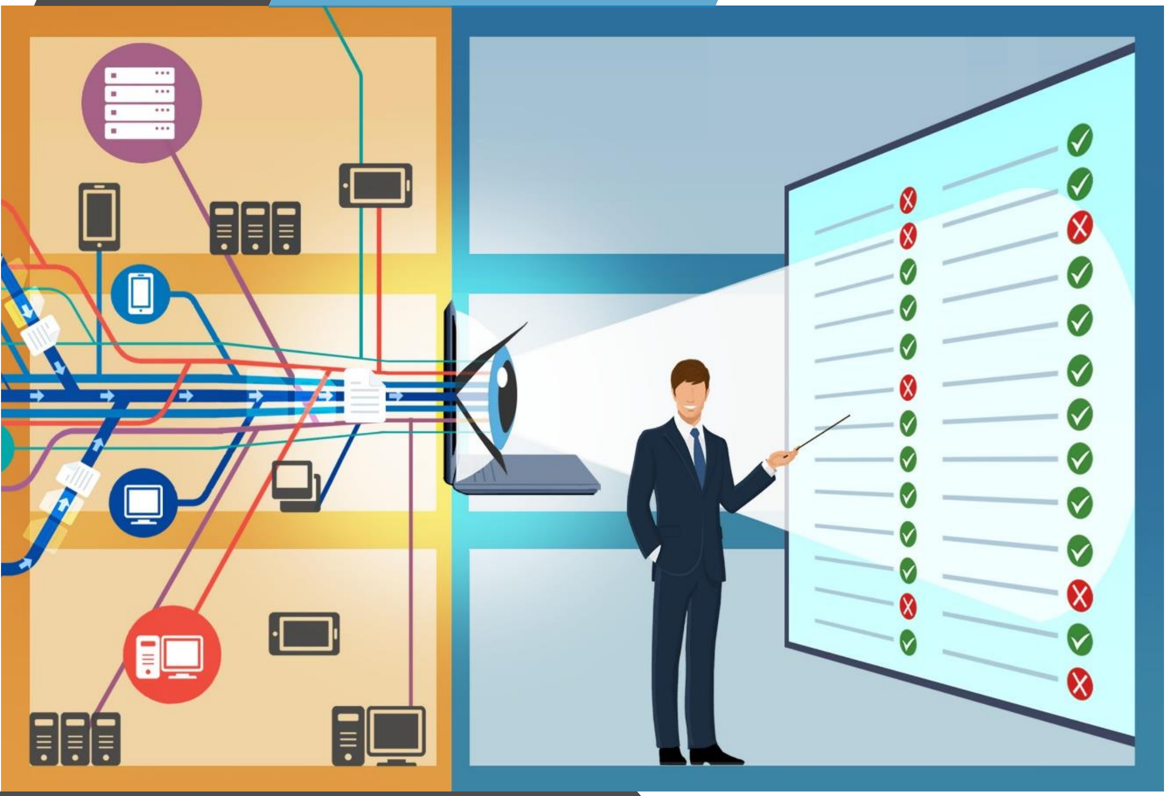
CSAT



Scan and installation requirements

QS solutions

Cyber Security Assessment Tool

Scan and installation requirements

CSAT

Copyright notice

Disclaimer

The use of this document is for informational purposes only and reflects the publisher's opinion as per date of publishing. Liability is limited to the publisher's terms and conditions as depicted in the underlaying master-agreement and/or purchase order.

1. CSAT general information

CSAT Installation and Data Storage

The CSAT is an application installed within your IT infrastructure. Collected data is stored in a database on a freshly installed and clean machine. The CSAT software is not distributing the data off-site. All data will stay on the machine in your infrastructure. There is no way QS solutions or any third party can access the data on the customer's machine, other than parties provided with access by your organization.

The CSAT is designed to help organizations improve their Cybersecurity based on facts from their Hybrid IT environment. To do so, QS solutions decided that CSAT End Users should be able to decide where their data is stored by allowing them to prepare a machine where CSAT and its database and services will be installed. The collected data can be analyzed on the customer's machine and will be great input to make informed decisions on new security initiatives.

Indicated CSAT Server Database size

The collected data is stored in a Microsoft SQL database. With the default installation, this database is stored on the CSAT server. To indicate the database size: in an environment where there are 100 endpoints scanned without a browser scan, the database is usually around 180MB. This number is intended as an indication of database size.

2. CSAT Server Requirements

CSAT server installations are **only supported on a clean installation of the Operating System**. Existing components or hardening might interfere with the CSAT components. A clean installation is defined as a default Windows installation based on the Microsoft provided installation media, non-domain joined.

Note: Implementing hardening and AD Domain Policies on the Operating System should be applied after the CSAT installation. When CSAT is not installed on a clean installation of the operating system, installation of the CSAT server software could fail and possibly make the device unstable or unusable for its purpose. In such cases, assessments are highly likely to fail.

The following Operating Systems are supported to install CSAT server:

- Windows 10 Professional or Enterprise, build 1803 or higher
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2, though not recommended

The CSAT server software installation will install Microsoft SQL Server Express 2017 with a SQL instance and Microsoft .NET Core on the device. During the installation there is the possibility to apply the “SQL September 2020 update”. It is required that you have (local) administrator-privileges on the device on which you are installing CSAT.

The minimal requirements for the CSAT server are:

Windows updates	Up to date with the latest Windows updates
CPU cores	Four CPU cores from one CPU socket
CPU speed	1.4 GHz (2.0 GHz recommended)
Memory	4 GB
Hard disk	At least 50 GB of free space (SSD recommended)
.NET Framework	Version 4.6 or higher

Should you choose to use an Azure Virtual Machine, we recommend using the Azure template D4s_v3 or one with better specifications. CSAT is also listed in the Azure Marketplace.

For better performance, we recommend using the CPU cores from one CPU. SQL Express can use a maximum of four CPU cores on one CPU. This also applies when using virtualization. If more than four CPU cores are needed, we recommend installing SQL Server Standard.

3. Scan requirements

Below you will find the scan requirements per scan sources. In this chapter is explained what the requirements for a successful scan are and how the scan is performed.

Active Directory

CSAT uses the Lightweight Directory Access Protocol (LDAP) or LDAPS (over SSL) for collecting data from Active Directory (AD), by executing LDAP(S) queries to an AD domain controller. The AD scan of a single domain can be done with a normal user account. To scan a forest, a domain admin account needs to be used. Ensure that the LDAP traffic is not blocked from the CSAT server to the AD servers.

Email DNS

During the Email DNS scan, information about the SPF, DKIM and DMARC records is collected from the external and/or internal DNS records. The CSAT server must be able to query the setup DNS server on the CSAT server for this data, because CSAT uses the DNS protocol to collect the DNS data.

Microsoft Cloud

To scan Microsoft Cloud (Azure, Azure Active Directory, Office 365, SharePoint Online and Intune), CSAT uses the Microsoft Graph API (REST/GRAPH calls) to collect the information. These Microsoft Graph API calls are made to an Azure AD application. The Azure AD application needs to be created on the Azure tenant that is to be scanned. This app needs to be created and approved by an Azure Administrator with either one of the following roles: Application Administrator, Cloud Application Administrator or Global Administrator. The creation and installation of said Azure AD application can be found in the ’CSAT Installation Manual’.

When you are using the Microsoft Cloud scan, the CSAT server must be able to send and retrieve data from “https://graph.microsoft.com” and “https://login.microsoftonline.com”. For both stated links, all subpages must be reachable. For the Azure Application creation tool, the CSAT server must be able to retrieve data from “https://csatreleases.blob.core.windows.net/public/” and all subpages.

Note

- If there are policy-based security devices in place at your perimeter, ensure that the above-mentioned URLs are allowed for the CSAT server.
- CSAT will not work in case there is a proxy server or SSL inspection in place. For the scan to work, traffic from the CSAT server to the internet needs to be temporarily exempted from the proxy/SSL inspection.

G Suite

To scan the G Suite (Google Suite) environment, CSAT uses Google API to collect the data. A Google Developer application is needed granted with certain permissions. Said developer application needs to be granted access to the environment. The creation and installation of this application can be found in the ’CSAT Installation Manual’.

When using the G Suite scan, the CSAT server must be able to send to and retrieve data from the internet page “https://www.googleapis.com” and all subpages.

Note

- If there are policy-based security devices in place at your perimeter, ensure that the above-mentioned URLs are allowed for the CSAT server.

- CSAT will not work in case there is a proxy server or SSL inspection in place. For the scan to work, traffic from the CSAT server to the internet needs to be temporarily exempted from the proxy/SSL inspection.

SharePoint On-Premises

To scan the SharePoint on-premises environment, CSAT uses the SharePoint on-premises API service. The following requirements need to be met.

- The SharePoint edition needs to be 2010 or newer and must be a Standard or Enterprise edition. SharePoint Foundation is not supported.
- The ports 443 and 80 need to be allowed to and from the CSAT server to the SharePoint server(s)
- The Search service application needs to be enabled/started.
- A SharePoint administrator account with the following roles/permissions: "Site Collection Administrator" of all individual site collections that are ought to be scanned. The account must be running under the Search service application.

SNMP

Information about devices that have the SNMP V1 and SNMP V2 service enabled can be collected, CSAT does not support SNMP V3. SNMP V3 support is road mapped for a future version of CSAT. To be able to scan the SNMP devices, ensure that the SNMP UDP port 161 is open for the SNMP devices to and from the CSAT server.

SSH

With the SSH scan, a device with SSH enabled can be scanned. SSH is generally used to access Unix-like operating systems. To be able to scan the SSH devices, ensure that the port configured in the SSH scan is open from and to the endpoint(s) and the CSAT server. The default TCP port for SSH is 22, however a custom configured port is supported.

Endpoint Scan

The information gathering for the endpoint(s) assessment is done through WMI (Windows Management Instrumentation).

When initiating a CSAT scan from within the CSAT server, a dissolvable agent will be sent to the endpoint through a WMI connection. The program (csat_dwnldr.exe executable) is a bootstrapper that downloads the csat.exe program from the CSAT server. This csat.exe is then used to collect data from the endpoint that cannot be collected remotely through WMI. When the csat.exe has finished scanning and uploaded the data to the CSAT server, the downloaded files and directories are automatically removed from the endpoint. This principle is known as a "dissolvable agent", which results that no CSAT related footprint is left behind on the endpoints.

If the WMI services are not configured correctly at the endpoint, limited information is collected. Indications of misconfigured WMI are corrupted WMI repositories, and incorrect client network setup – to name a few common errors we have seen.

Network traffic and CPU usage

The dissolvable agent that is sent to the endpoints is less than 5 MB in size. The dissolvable agent is sent to a maximum of 30 endpoints simultaneously. This ensures that at peak usage only 150 MB Is being sent from CSAT server to the endpoints.

When an endpoint is being scanned, the CPU usage is between 1 and 5 percent and memory usage is between 40 and 70 MB. When the data has been collected, a zip file is created and sent back to the CSAT server. This zip file is usually around 100 KB in size. Because not all endpoints are scanned at the same time, the data sent over the network from the scanned endpoints to the CSAT server is generally around 100 MB at peak usage.

Indicated Endpoint scan running time

The following chart indicates the agent's running time, as well as an indication of the size of the zip-file that is being created, depending on the scan options that are being used.

Client type	Scan level	Browser scan	Average scan time	Zip file size
Windows Client OS	5	Off	2 min	0,2 MB
Windows Client OS	5	On	2 min 02 sec	1,2 MB
Windows Client OS	9	Off	2 min	0,4 MB
Windows Client OS	9	On	2 min 30 sec	1,5 MB
Windows Server OS	5	Off	1 min 10 sec	0,1 MB
Windows Server OS	9	Off	1 min 15 sec	0,2 MB

Endpoint Requirements

The endpoints that are scanned by CSAT must meet the following requirements:

- .NET version 3.0 or higher (minimal required version)
- If you are using internal firewalls, VPN, IPS, IDS and/or network ACL solutions, ensure that traffic from CSAT server to the targeted endpoints is not blocked.
- Anti-virus/Anti-malware software should allow the execution of the CSAT.exe in the C:\windows\temp folder
- A local administrator or domain administrator account must be used for the endpoints that CSAT will scan. We recommend creating a temporary CSAT scanning account, after the scan the account can be removed/inactivated.

To ensure that the CSAT server can scan the endpoints, inbound firewall rules need to be enabled for the active firewall-profile on the endpoints. All required rules are predefined in Windows Firewall and need only to be enabled for the active firewall-profile. The required ports are listed in the next section.

Antivirus software exclusion

For the endpoint scan, the dissolvable agent is deployed to "C:\Windows\Temp\csat". CSAT invokes the following executables to perform its scan:

- C:\Windows\System32\cmd.exe
- C:\Windows\System32\certutil.exe
- C:\Windows\Temp\csat\cmd.exe
- C:\Windows\Temp\csat\csat.exe
- C:\Windows\Temp\csat\csat_dwnldr.exe

Some antivirus software products could block the execution (this is not the case with Windows Defender) of the above executables. Should this happen in your environment, temporarily exclude the above listed executables within the antivirus solution settings. Refer to your antivirus documentation to see how to add the exclusions in the management portal.

Firewall / Network Requirements

CSAT uses the below ports for the CSAT services

On the CSAT server:

Port number	TCP, UDP	Explanation
443	TCP, outbound	To connect with Office 365, SharePoint Online and AAD scan (from CSAT server to the internet)
8080	TCP, inbound TCP, outbound	Deployment service, to deploy the dissolvable agent (from CSAT server to targeted internal endpoints/subnets)
53	TCP, outbound	DNS, outbound to both internal and internet DNS servers
389, or	TCP, outbound	LDAP, outbound to the Active Directory Domain Controllers
686	TCP, outbound	LDAPS (secure LDAP)
161	UDP, both	SNMP, outbound from server to endpoints SNMP, inbound from endpoints to server
22	TCP, outbound	SSH-traffic

CSAT Server internal only ports, not permitted to be accessed from the network/internet

Port number	TCP, UDP	Explanation
4432	TCP, inbound	CSAT Portal, no outbound traffic
8018	TCP, inbound	Enumeration service, no outbound traffic
8090	TCP, inbound	Analysis service, no outbound traffic
8288	TCP, inbound	Used by the Network service, no outbound traffic

On endpoint devices:

All the below named ports are inbound for the active firewall profile. **It is strongly recommended NOT enabling these ports within the Public Network profile.** In some network environments, it might be necessary to add the IP address of the CSAT server as the originating IP address to the below firewall rules, depending on your network security policy/configuration.

Firewall rule name	Group	Port
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	139
File and Printer Sharing (SMB-In)	File and Printer Sharing	445
Remote Scheduled Tasks Management (RPC)	Remote Scheduled Tasks Management	RPC Dynamic Ports
Windows Management Instrumentation (DCOM-In)	Windows Management Instrumentation	135
Windows Management Instrumentation (WMI-In)	Windows Management Instrumentation	All (only allow svchost.exe)

In environments where outbound traffic from endpoints is restricted, the following rule should be added to the endpoint's firewall profile:

Port number	TCP, UDP	Explanation
8080	TCP, outbound	Transport of scan results from endpoint to CSAT server

CSAT uses the following firewall rules:

- “File and Printer Sharing (NB-Session-In)” with port 139 is used for the NetBIOS Session to the endpoint.
- “File and Printer Sharing (SMB-In)” with port 445 is used to send SMB data for the dissolvable agent to the endpoint(s).
- “Remote Scheduled Tasks Management (RPC)” with the RCP dynamic ports is used to send SMB data for the dissolvable agent to the endpoint(s). The RPC dynamic ports are 49152-65535.
- “Windows Management Instrumentation (DCOM-In)” is used for the initial WMI connection to the endpoint.
- “Windows Management Instrumentation (WMI-In)” is a random port. The port is used to send the CSAT dissolvable agent files to the endpoint. If you want you can change the WMI random port to a fixed port, use the following instruction to set a fixed WMI port on the endpoint “https://docs.microsoft.com/en-us/windows/win32/wmisdk/setting-up-a-fixed-port-for-wmi”.
- TCP port 8080: The CSAT agent is undertaking several actions to collect data. After the agent has finished collecting, it sends the data back to the CSAT server. To send said data the endpoint(s) must be allowed to communicate with the CSAT server over TCP 8080