

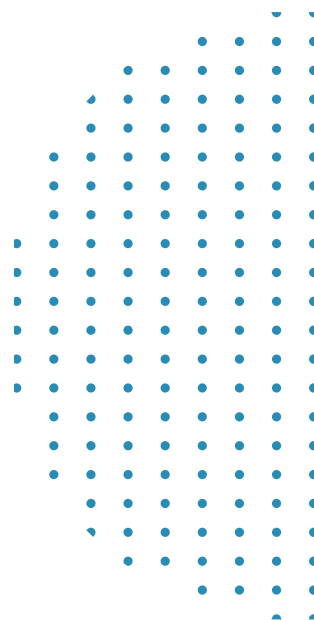


The Onapsis Platform

# Technical Specifications

## For Onapsis Products

September 2023



Copyright 2023 Onapsis and/or its affiliates. All rights reserved.

The Products (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Products, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Products, no part of these Products may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this documentation may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Onapsis, Inc.

Onapsis may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this documentation. Except as expressly provided in any written license agreement from Onapsis, the furnishing of this documentation does not give you any license to these patents, trademarks, copyrights, or other intellectual property. Onapsis is a registered trademark of Onapsis Inc. and/or its affiliates.

All other trademarks are property of their respective owners.

**NOTE:** This document is an excerpt from the product installation guides. Therefore, there may be references to content that is not included in this document. Complete installation details are provided in the installation guides for each product.

# Contents

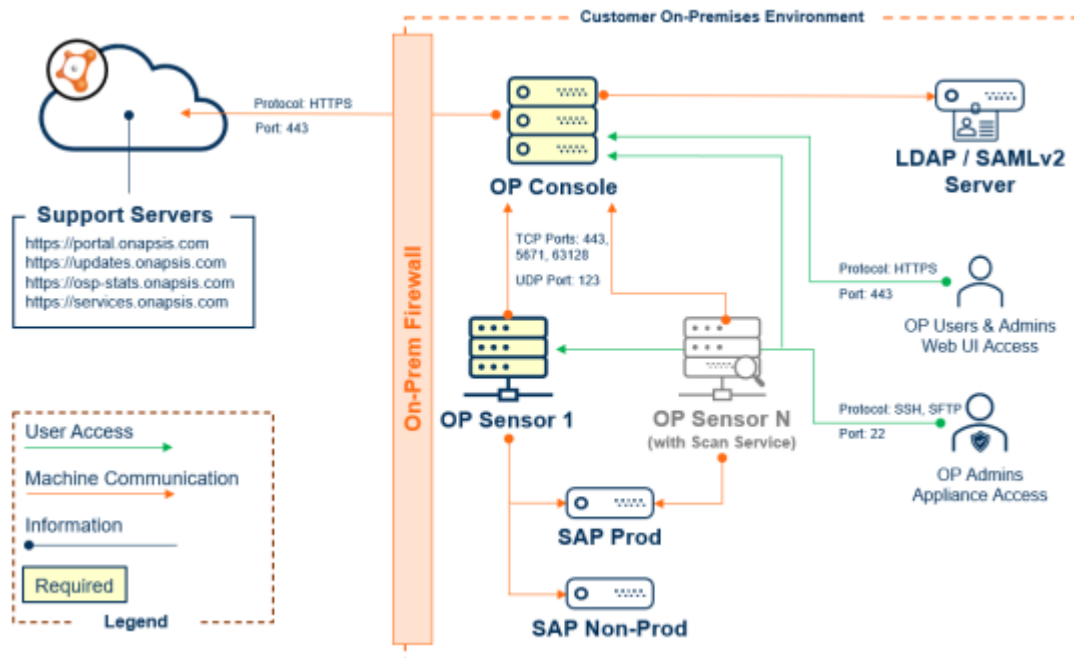
<b>Assess, Comply, and Defend .....</b>	<b>5</b>
Recommended installation architecture .....	5
Product components .....	6
Installation planning .....	9
Console and sensor requirements .....	9
Prerequisites.....	12
Install add-ons and create users.....	12
Install Scan Service.....	13
Supported SAP versions for code scans .....	14
Configure SAP for Defend .....	14
Configure SuccessFactors for Assess .....	14
<b>Control for Code ABAP .....</b>	<b>15</b>
Installation overview .....	15
Recommended installation architecture.....	15
Product components .....	16
Available languages .....	17
What additional components are available? .....	17
Installation planning .....	21
Network segment recommendations .....	21
Central database recommendations .....	21
Central System and Satellite System requirements.....	22
Scanning System requirements .....	24
Source System requirements .....	27
JCo requirements.....	28
<b>Control for Code HANA .....</b>	<b>30</b>
Overview .....	30
Code scans at different development stages .....	30
Supported code languages.....	31
Test cases .....	32
Requirements .....	32
Supported operating systems .....	32
Other software requirements .....	32
Configure Scan Server availability.....	33
Web browser requirements .....	34
Configure required database access .....	34

<b>Control for Transport .....</b>	<b>36</b>
Installation options .....	36
Setup 1 - Zero footprint .....	36
Setup 2 - Developer optimum .....	39
Understand the prerequisites .....	42
Central System and Satellite System prerequisites .....	42
Source System prerequisites .....	43
Frontend prerequisites .....	43
Special Test Case prerequisites .....	43
<b>CleanupSolutions .....</b>	<b>45</b>
System requirements .....	45
SAP landscape .....	45
Supported SAP NetWeaver (ABAP) systems .....	45
<b>On-Change Control .....</b>	<b>47</b>
Installation planning .....	47
Installation overview .....	47
Software prerequisites .....	47
Scan planning .....	48
Approval planning .....	49
<b>Control Central .....</b>	<b>52</b>
Scan Service .....	52
Overview .....	52
Control for Code ABAP .....	55
Installation overview .....	55
Installation planning .....	59

# Assess, Comply, and Defend

## Recommended installation architecture

For SAP systems, the Onapsis Platform supports a wide variety of installation options based on your organization's needs and work processes. Because of this, there is not one standard installation process that applies to each organization. The following graphic represents our recommended on-premise installation architecture.



As you can see, at a minimum, you need to install the Onapsis Platform console and at least one sensor. If you licensed Assess for Code, you must also install the Scan Service on a sensor to be able to scan custom code from Assess. For more information, see *Install the Scan Service* in the *Onapsis Platform User and Administrator Guide*.

## Product components

The various components are:

Component	Required?	Description
<b>System scanning and monitoring components</b>		
Console	Yes	<ul style="list-style-type: none"><li>▪ Each installation requires one console, and the console requires internet access to communicate and receive updates.</li><li>▪ Provides the management and reporting web application user interface. Users log into the web application to:<ul style="list-style-type: none"><li>▪ Configure and schedule scans.</li><li>▪ Configure incident notifications.</li><li>▪ View, understand, and act on the results.</li></ul></li><li>▪ Manages the sensors (maximum of twenty).</li><li>▪ Continuously communicates with the Onapsis Update Server to get the latest software updates (updates occur two times each month).</li></ul>
Sensors	Yes	<ul style="list-style-type: none"><li>▪ Each installation requires at least one sensor. The number of sensors you need is based on your landscape size, complexity, and network segmentation.</li><li>▪ Virtual "headless" devices that perform most of the work to find and analyze system vulnerabilities, such as:<ul style="list-style-type: none"><li>▪ Request tasks from the console.</li><li>▪ Gather the technical data provided.</li><li>▪ Pass data back to the console to display in the user interface.</li></ul></li><li>▪ Sensors are updated from the console and can be deployed on premises or in the cloud.</li></ul>

Component	Required?	Description
Add-ons for SAP systems	Based on system and product licensed	<ul style="list-style-type: none"> <li>Used to extract technical information such as configurations, log data, component versions, patch information, and user authorizations from SAP for analysis.</li> <li>Certified by SAP.</li> <li>Run as a component on top of your SAP systems and, therefore, do not interact with any functional (business-related) SAP module.</li> <li>For ABAP systems, the add-on and role is required for Defend. For Assess and Comply, the add-on is optional. Without the add-on and just the user role, you are able to most, but not all, checks. For more information, see the <i>Use the Onapsis Platform without add-ons</i> help topic. The ABAP add-on is typically updated twice a year.</li> <li>For Java systems, the add-on and user role is required. The Java add-on is typically updated once a year.</li> <li>For HANA systems, no add-on is needed, but the user role is required.</li> <li>If you license Defend, typically you test Defend in your SAP non-production systems before configuring it for your SAP production systems.</li> </ul>
System logs (not shown)	For Defend	If you license Defend, the platform analyzes system logs to report notable events and incidents. In some cases, you must enable or configure the log to be read by the platform. For more information, see the Enable required SAP logs topic in the product help.

Component	Required?	Description
-----------	-----------	-------------

**Optional code scan components**

Scan Service	No	<ul style="list-style-type: none"><li>▪ Installed on one of the Onapsis Platform sensors.</li><li>▪ Routes code scan requests to the assets and passes the resulting scan data back to the Onapsis Platform.</li></ul>
--------------	----	--

**IMPORTANT:** For further information and advice on the best way to set up your landscape and all of the various components, contact your Onapsis representative to complete a solution architecture review. The solution architecture review determines whether the recommended approach is the optimal installation architecture for your organization.



## Installation planning

Recommendations for preparing for the installation and installation requirements are described here.

### Console and sensor requirements

The technical requirements for the Onapsis Platform console and sensors are provided here.

### Appliance sizing requirements

The requirements and recommendations are based on the products licensed as follows:

Products	Appliance	Minimum requirements	Recommendations
Assess and Comply	Console	<ul style="list-style-type: none"> <li>vCPU: 8</li> <li>RAM: 16 GB</li> <li>Swap: 16 GB</li> <li>HDD: 200 GB</li> </ul>	<ul style="list-style-type: none"> <li>CPU Compatible with Intel Xeon Scalable Family processor (2nd or 3rd generation)</li> </ul>
	Each sensor	<ul style="list-style-type: none"> <li>vCPU: 8</li> <li>RAM: 16 GB (plus an additional 16 GB for Assess for Code)</li> <li>Swap: 16 GB</li> <li>HDD: 200 GB</li> </ul>	
Assess, Comply, and Defend	Console	<ul style="list-style-type: none"> <li>vCPU: 8</li> <li>RAM: 32 GB</li> <li>Swap: 32 GB</li> <li>HDD: 200 GB</li> </ul>	
	Each sensor	<ul style="list-style-type: none"> <li>vCPU: 16</li> <li>RAM: 32 GB</li> <li>Swap: 32 GB</li> <li>HDD: 200 GB</li> </ul>	

NOTE: You may need to increase the disk space (HDD) depending on the size of your SAP landscape. Sizing requirements for cloud deployments are provided in the respective cloud deployment guidelines.

## Additional requirements

The additional requirements are:

Requirement	Details
Virtualization technology	<p>The required Onapsis appliances (console and/or sensor) are delivered in a prebuilt virtual appliance in Open Virtualization Appliance (OVA) format. The OVA is self-contained and includes a Linux-based OS and the Onapsis solution. No additional OS is required to install the OVA.</p> <div><p><b>IMPORTANT:</b> You should deploy the virtual appliances using the OVA file provided by Onapsis. You cannot install the OVA on a pre-existing virtual machine. To download the necessary file, see <a href="#">Download the Onapsis Platform OVA file</a>.</p></div> <p>You must obtain the IP address, netmask, gateway, DNS search suffix, and IP address for each virtual machine (VM) so you can access each appliance.</p> <p>The platform runs on top of the following supported platforms:</p> <ul style="list-style-type: none"><li>▪ VMware latest version</li><li>▪ KVM latest version</li><li>▪ Microsoft Hyper-V latest version</li></ul> <div><p><b>NOTE:</b> There are known issues with vSphere 6.5. These issues may interfere with your ability to successfully deploy the prebuilt virtual machine in OVA format. If you are experiencing problems, contact Onapsis.</p></div>

Requirement	Details
	<p>Deployment in Cloud environments such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and so on is also supported. Each cloud provider has a unique set of technologies, tools, and processes. For example, AWS deployment is facilitated by an AMI. Deployment of the AMI is an AWS process likely defined within your organization rather than an Onapsis Platform process. Once the AMI is deployed, you would follow the standard Onapsis Platform installation process. For more information on Cloud deployments, contact Onapsis.</p>
Internet connectivity	<p>Required by the console for communication with <a href="https://updates.onapsis.com">updates.onapsis.com</a>, <a href="https://portal.onapsis.com">portal.onapsis.com</a>, <a href="https://osp-stats.onapsis.com">osp-stats.onapsis.com</a>, <a href="https://services.onapsis.com">services.onapsis.com</a>, and <a href="https://*.newrelic.com">*.newrelic.com</a>.</p>
Browsers	<p>One of the following:</p> <ul style="list-style-type: none"> <li>▪ Google Chrome (recommended)</li> <li>▪ Microsoft Edge</li> <li>▪ Mozilla Firefox</li> <li>▪ Apple Safari</li> </ul> <div data-bbox="576 1224 1425 1407"> <p><b>NOTE:</b> The current and previously released browser versions are supported. If you use an unsupported browser, the web application may not render properly, and you may be unable to use some features.</p> </div>

## Supported SAP versions for system scans

For the list of supported SAP systems and versions, see [Supported SAP versions for system scanning](#).

## Prerequisites

Before you begin your installation, ensure you complete the following. To complete this list, you may need to coordinate with the appropriate teams in your organization, such as networking, security, and so on.

- Obtain default passwords
- Download the Onapsis Platform OVA file
- Download licenses
- Download and extract the NWRFC Library files
- Obtain network information
- Open required ports
- Adjust firewall settings

You can install the Onapsis add-ons and users before or after installation the Onapsis Platform on SAP systems. For complete details, see [Install add-ons and create users](#) (on page [12](#)).

## Install add-ons and create users

To enable the Onapsis Platform to communicate with your SAP systems, you need to install the SAP-certified add-ons and/or create the related users and roles the platform uses to authenticate to each target system. This ensures the Onapsis Platform can discover your SAP systems and extract and analyze technical information such as configurations, log data, component versions, patch information, and user authorization. You can install the add-on and role before or after you complete the Onapsis Platform installation. The add-on runs as a component on top of your SAP systems and does not interact with any functional (business-related) SAP modules.

The available add-ons and roles are system-based and include:

- **ABAP add-on and role:** For ABAP, S/4 HANA, and BW/4 HANA systems.

**NOTE:** Starting with the 2.2020.22 release, you can run Assess scans and Comply audits on ABAP, S/4 HANA, and BW/4 HANA systems without installing the ABAP add-on. For more information, see the *Use the Onapsis Platform without add-ons* help topic.

- **Java add-on and role:** For Java systems.
- **HANA role:** For HANA database/db.
- **BOBJ role:** For Business Objects Support for Assess and Comply.

The user and role are required regardless of whether you need to install the add-on (which is required for Defend). The user requires minimal rights, which are assigned by the role provided by Onapsis. This user and role should be created in the active working client. For more role authorization details, see the role or installation guide related to your SAP system type.

**NOTE:** For dual stack systems, you must follow the add-on, user, and role requirements for each individual ABAP and Java stack. For HANA database, an add-on is not required, but you still must create a user and role for the system database and each tenant database.

For more information on installing or updating add-ons and/or the required users and roles, see the guide related to your system. For the most complete detection capabilities, Onapsis recommends that you use the latest versions of the ABAP and Java add-on when using Defend.

If you are not sure whether the Onapsis add-ons and/roles have already been installed, see Verify Onapsis add-ons or roles are installed.

## Install Scan Service

As mentioned in the Installation overview, if you are using the Assess for Code to scan code on SAP assets for vulnerabilities, you must configure the Onapsis Platform to use the Scan Service.

You install the Scan Service on one of the Onapsis Platform sensors to route code scan requests to the assets and pass the resulting scan data back to the Onapsis Platform. The Scan Service can scan any asset, regardless of the sensor to which the asset is connected.

**IMPORTANT:** For information on obtaining the Assess for Code license and enabling the Scan Service in the Onapsis Platform after you install it, contact your Onapsis representative.

Before you install the Scan Service, you must meet the following requirements:

- Choose a sensor to install the Scan Service on. The operating system must have at least 32 GB of RAM as the Onapsis Platform requires 16 GB and the Scan Service requires 16 GB. For performance reasons, Onapsis recommends that you run the Scan Service on a dedicated sensor.

- Download the latest SAP JCO library files. You will need to upload them to the Onapsis Platform. This library is required for the Scan Service to communicate with the assets using the RFC protocol.
- Ensure the Onapsis console has access to `services.onapsis.com`, as explained in [Adjust firewall settings](#).
- Ensure Onapsis ABAP role version 24 (or higher) is used on each system you want to scan. For more information, see [Upload the ABAP role file](#). For the specific authorizations required for Assess for Code and code scanning, see [Onapsis ABAP role authorizations](#). Both of these topics are in the product help and the [Onapsis Platform ABAP Installation Guide \(for ABAP, S/4 HANA, and BW/4 HANA\)](#).

To configure the Scan Service, take the following steps:

1. Click **SETTINGS > INTEGRATIONS > Scan Service**.
2. In the **HOST SENSOR** section, select the sensor to install the Scan Service on.
3. In the **UPLOAD SAP JCO LIBRARY** section, upload the JCO library files.

Installation starts when you save the page and could take up to 20 minutes.

## Supported SAP versions for code scans

For the list of supported SAP systems and versions, see [Supported SAP versions for code scanning](#).

## Configure SAP for Defend

When you license Defend, you must set your SAP time zones and enable specific logs per system type. For complete details, see the [SAP Configuration Guide for Defend](#).

## Configure SuccessFactors for Assess

When you license Assess and want to scan your SuccessFactors instance for vulnerabilities, you must configure your SuccessFactors instance and configure the Onapsis Platform sensor for SaaS targets. For complete details, see the [SuccessFactors Configuration and User Guide](#).

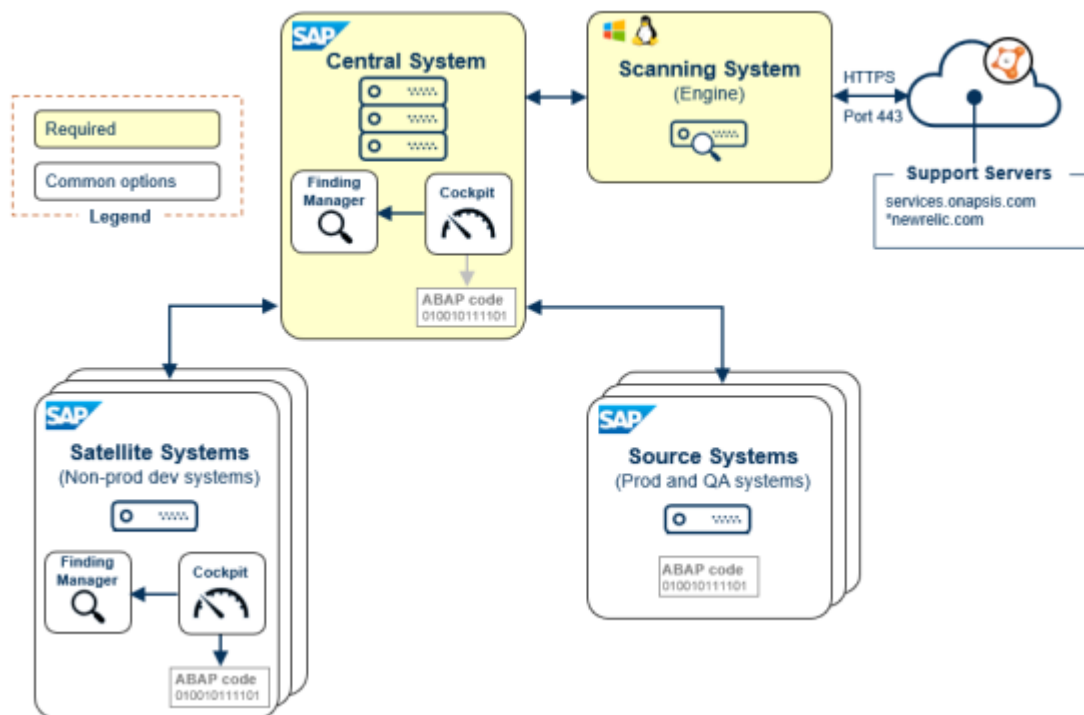
# Control for Code ABAP

## Installation overview

Control for Code enables a holistic approach to securing all of the ABAP code on all of your systems, throughout your system landscape, no matter how many systems are involved. To support this approach, Control for Code has various components to support a wide variety of installation and integration options based on the technologies used in your organization and your organization's needs and work processes. Because of this, the installation can be quite complex. This document is intended to get you setup and scanning custom ABAP code as soon as possible. Over time, you may revisit this document to expand your installation and integration configuration to meet your evolving needs.

## Recommended installation architecture

The following graphic represents our recommended installation architecture.



As you can see, at a minimum, you need to install a Central System and a Scanning System. The Central System is the first system you set up as it is where you install the Control for Code add-on. We recommend that you use a new SAP system and dedicate

it to serving as the Central System. Note that this is simply a logical designation, that is, you can use one of your existing systems as a Central System. The actual scanning of code is performed on the Scanning System, by the scanning engine, which runs on a Windows or Linux computer.

**NOTE:** It is possible for the Central System and the Scanning System to run on the same hardware, but typically our customers purchase new hardware so that the Scanning System can run on a dedicated computer.

You can include Source Systems that enable you to scan code on those systems from the Central System, without needing to install the Control for Code add-on on the Source Systems. You can install the Control for Code add-on on Satellite Systems to enable developers to scan code locally on those systems.

In the scenario shown, you have the best of both worlds for both your developers and the rest of your development team. That is, developers can work on Satellite Systems and enjoy the full power of the Cockpit and the Finding Manager, while QA personnel, Release Managers, Code Auditors and so forth can work on the Central System and double-check the code, perform standardized quality checks, audit code and so forth.

In a nutshell, you can build Control for Code right into your development environment and processes so that you can first get your code clean, and then ensure that it stays that way.

## Product components

The various components are:

- **Central System:** A logical system designation for a single, centralized system that collects communication event data from connected systems throughout your system landscape. The Central System has two GUI components for your development team:
  - **Cockpit** enables you to start scans
  - **Finding Manager** displays the results of your scans.

**NOTE:** If you want to scan locally without having to log on to a Central System or be connected to the Scanning System through the Central System, you can install the product on the local system where the ABAP code is, in which case the Central System shown here is essentially a local development system connected directly to the Scanning System.



- **Scanning System:** Where the actual scanning of code is performed by the scanning engine, which runs on a Windows or Linux computer.
- **Satellite System:** A system for developers that has the Cockpit and Finding Manager installed so developers can scan ABAP code locally.
- **Source System:** A system that is connected to the Central System, but which has no actual components installed on it. Source Systems are, therefore, referred to as having zero footprint as you don't need to maintain product installations on those systems. The Integrated Scanner ATC/SCI (ISA) can be installed on a Source System to augment it with developer code scanning tools.

## Available languages

The Control for Code GUI components and test cases are available in English and German.

## What additional components are available?

In addition to the recommended components there are various integrated scanner options for developers and a few integration options to further lock down and streamline your code development processes.

The following table provides information to help understand the advantages and disadvantages of each available component, and the related section in this document.

**IMPORTANT:** For further information and advice on the best way to set up your landscape to include Control for Code and all of the various components, contact your Onapsis representative to complete a solution architecture review. The solution architecture review determines whether the recommended approach is the optimal installation architecture for your organization as there are a few scenarios where this preferred approach may not be appropriate for your landscape or needs. (For example, you may have one system line, you may not want central scanning, or you may want to use Source Systems to scan non-production systems, and so on).

Component	Required?	Advantages / Disadvantages
<b>System designation</b>		
Central System	Yes	<ul style="list-style-type: none"> <li>Scan other systems from a central location.</li> <li>Install and maintain Control for Code add-on (Cockpit and Finding Manager) in a single system.</li> <li>Configure Control for Code once.</li> </ul> <p>See: Step 1: Install Central System</p>
Scanning System	Yes	<ul style="list-style-type: none"> <li>Depending on your landscape, you may need multiple scanning systems.</li> </ul> <p>See: Step 2: Install Scanning System</p>
Source System	No	<ul style="list-style-type: none"> <li>Scan QA, Production, or other systems from a central location.</li> <li>Zero footprint: No need to install or maintain Control for Code add-on on these systems which saves time and maintenance if you have multiple SAP systems.</li> <li>Doesn't provide local scanning.</li> </ul> <p>See: Step 6: (Optional) Configure Source Systems</p>
Satellite System	No	<ul style="list-style-type: none"> <li>Provides local scanning.</li> <li>Developers can scan Dev systems locally.</li> <li>Need to install and maintain Control for Code add-on on these systems.</li> </ul> <p>See: Step 7: (Optional) Install Satellite Systems</p>
Developer System	No	<ul style="list-style-type: none"> <li>See Integrated Scanner Eclipse (ISE) plugin.</li> </ul>

Component	Required?	Advantages / Disadvantages
<b>Plugins for specific developer environments</b>		
Integrated Scanner Eclipse (ISE)	No	<ul style="list-style-type: none"> <li>▪ For developers working with the Eclipse Interactive Development Environment (IDE).</li> <li>▪ Install and use the ISE plugin to scan ABAP code either locally on the Satellite System or via the Central System connected to the Source System.</li> <li>▪ Scan code without leaving the IDE.</li> <li>▪ Scan results are displayed in in the IDE.</li> <li>▪ Common GUI for analyzing and correcting code issues.</li> <li>▪ Need to maintain ISE plugin on the system.</li> </ul> <p>See: Integrated Scanner Eclipse (ISE)</p>
Integrated Scanner Workbench (ISW)	No	<ul style="list-style-type: none"> <li>▪ For developers working in ABAP Workbench.</li> <li>▪ Install and use the ISW plugin to scan ABAP code locally on the Satellite System.</li> <li>▪ Extends ABAP Workbench menu options to enable developers to invoke code scanner anytime without leaving the IDE.</li> <li>▪ Scan results are displayed in the Finding Manager.</li> <li>▪ Common GUI for analyzing and correcting code issues.</li> <li>▪ Need to maintain ISW plugin on the system.</li> </ul> <p>See: Integrated Scanner Workbench (ISW) on Satellite Systems</p>

Component	Required?	Advantages / Disadvantages
Integrated Scanner for ATC/SCI (ISA)	No	<ul style="list-style-type: none"> <li>For developers working in ABAP Test Cockpit (ATC) and the SAP Code Inspector (SCI).</li> <li>Install and use the ISA plugin to scan ABAP code locally on the Satellite System or via the Central System connected to the Source System.</li> <li>Control for Code tests cases are integrated into ATC/SCI checks.</li> <li>View Control for Code findings within SAP ATC or SCI.</li> <li>On the Source Systems, you don't have full functionality, but you can scan those Source Systems without having to install and maintain the Control for Code add-on.</li> <li>Need to maintain ISA plugin on the system.</li> </ul> <p>See: Integrated Scanner for ATC/SCI (ISA)</p>
<b>Integration options</b>		
Transport Management System (TMS) integration	No	<ul style="list-style-type: none"> <li>SAP's TMS findings are displayed in the Control for Code Finding Manager on the Satellite System.</li> <li>Review findings in one location.</li> <li>Provides additional control benefits if the ISW or ISA plugins are used.</li> <li>Build processes around transporting code, based on whether it is clean or whether there are findings.</li> </ul> <p>See: Set up TMS integration on Satellite Systems</p>
Finding Status Workflow (FSW) integration	No	<ul style="list-style-type: none"> <li>Built into the Control for Code Finding Manager on the Satellite System.</li> <li>FSW ensures a finding can only be set to "No Issue" when there is an approver involved.</li> <li>Build approval process around Control for Code.</li> </ul> <p>See: Set up FSW on Satellite Systems</p>

Component	Required?	Advantages / Disadvantages
API	No	<ul style="list-style-type: none"> <li>▪ Build custom integrations and functionality.</li> <li>▪ Create custom processes that perfectly suit your ABAP developers and your ABAP development environment.</li> <li>▪ Need to develop and maintain the custom solution.</li> </ul> <p>See: Use the API on Satellite Systems</p>

## Installation planning

Recommendations for preparing for the installation and the installation requirements are described here.

### Network segment recommendations

Typically, developers use Control for Code to scan their own code during normal work hours using the SE80 development environment, and they release transports on a regular basis, so it is important that Control for Code results are produced quickly. So, we recommend that you install your Scanning System in the same network segment as the SAP system, preferably in the same data center.

Installing Control for Code on a different network segment is not recommended due to latency issues and will result in significant performance reduction as Control for Code makes use of multiple RFC calls during a scan.

**CAUTION:** Even a scan of a very small package can increase to several minutes if the Scanning Engine is not in the same network segment.

### Central database recommendations

If you are running your SAP systems with a central database instance and multiple Application Servers (ASs), we recommend that you configure the RFC Connections for Control for Code in SM59 on the central database instance to be the gateway for all application servers. While it is possible to configure Control for Code on each AS, this approach creates significant overhead because each application server needs to have its own configuration of RFC destinations and Scanning Systems.

## Central System and Satellite System requirements

Before you start to install the base components on your ABAP Central System and Satellite System, ensure that you meet all of the system and software requirements described here.

### Supported SAP systems

At the time this documentation was published, Control for Code supports SAP systems for the following SAP products. Do not use other SAP systems without first checking with Onapsis.

**NOTE:** If you want to use a system as a Source System, ensure you also review the requirements listed in Source System requirements (on page [27](#)).

**CAUTION:** Do not install Control for Code on non-Unicode SAP systems because they are not currently supported.

- SAP NetWeaver 7.00 SP27 or higher
- SAP NetWeaver 7.01 SP27 or higher
- SAP NetWeaver 7.02 SP27 or higher
- SAP NetWeaver 7.03 SP27 or higher
- SAP NetWeaver 7.31 SP05 or higher
- SAP NetWeaver 7.40
- SAP NetWeaver 7.50
- SAP NetWeaver 7.51
- SAP NetWeaver 7.52
- SAP S/4HANA 1709
- SAP S/4HANA 1809
- SAP S/4HANA 1909
- SAP S/4HANA 2020
- SAP S/4HANA 2021
- SAP S/4HANA 2022
- SAP BW/4HANA (any version)

- SAP S/4HANA Foundation (any version)
- ABAP Foundation on HANA (any version)
- SAP S/4HANA Cloud extended edition (EX)

## **SAP kernel recommendations**

Onapsis recommends that you operate your SAP systems using an SAP kernel that is within the official maintenance period of SAP. Nonetheless, Control for Code may run properly with older versions of SAP kernel. Note that Control for Code cannot be installed on systems with SAP kernel 7.01, which is out of the maintenance period by SAP. For more information, see the SAP Service Marketplace or get in touch with Onapsis Support.

## **Central System SAP release recommendation**

Control for Code versions after 5.3.x require the Central System to have SAP NetWeaver 7.4 with Support Package 8 or higher. Older versions of SAP NetWeaver are not supported in releases after version 5.3.x.

## **SPAM/SAINT requirements**

The installation of Onapsis Reporting requires a SPAM/SAINT version 0063 or higher. If you use SPAM/SAINT version 0063, you have to implement [SAP Note 2378346](#). To uninstall the relevant software components, you need SPAM/SAINT version 0064 or higher.

## **Frontend GUI requirements**

Normally, Control for Code requires SAP GUI. Onapsis always recommends using the latest SAP GUI version, including patches, regardless of the SAP system version. Follow the instructions provided in the Service Market Place to install SAP GUI.

As an alternative, you can use the Integrated Scanner Eclipse (ISE) plugin as your frontend GUI, but this plugin does not provide full functionality. For more information, see ISE requirements.

## Scanning System requirements

The hardware requirements for your Scanning System are detailed here.

**NOTE:** It is possible for the Scanning System and the Central System to run on the same hardware, but typically, our customers purchase new hardware so that the Scanning System can run on a dedicated computer.

### Minimum hardware requirements

The minimum hardware requirements for a Scanning System depend on your usage scenario.

The minimum processing power you will need for each instance depends not only on the types of scans you perform, but how many scans you need to run in parallel.

Typically, you use Control for Code to perform two types of scans:

- **Large scans:** Scans that comprise your whole namespace or a large part of it. These are usually planned as background jobs and scheduled to run periodically.
- **Small scans:** Scans for only small parts of your namespace that are typically triggered by developers for small code parts or when using the TMS Integration for small to medium-sized transports.

The minimum requirements for the Scanning System are:

- **CPU:** AMD64/EM64T 64-bit mode compatible multi-core CPU (Quad-Core or 2x Dual-Core)
- **HDD:** 7 GB hard disk space—in addition to the operating system
- **RAM:** How much RAM you require for your Scanning System depends on how many large scans and small scans you need to run in parallel. For the majority of customers, we recommend starting with 4GB of RAM for a single large scan and 1 GB for a single small scan. Multiply the number of expected parallel scans with these numbers to get the total required RAM for the Scan Engine.

**Example:** Assume you need to run three (3) large scans in parallel and do not expect to have more than ten (10) small scans running in parallel. In addition to RAM needed by the operating system, you will require 22 GB of additional RAM:

- 12 GB for the three large scans
- 10 GB for the ten small scans



Additional considerations:

- **Allow a buffer:** When calculating the number of instances, use a high enough number of instances to allow for a buffer. This is because free scan instances are critical for some business processes, such as the TMS Integration. For the TMS Integration, also consider configuring dedicated instances as described in [Configure multiple engine instances](#).
- **Plan ahead:** Consider whether you plan to add systems in the future. For example, if you know you will be adding systems later, you might choose a scanning system with more resources or a system that can easily scale.

Before you set up all necessary instances, you might start by testing a Scanning System that runs a single Control for Code instance for large scans and another instance for small scans. If you need help with your specific setup or have questions regarding your specific requirements and setup, please contact your Onapsis account manager.

## Custom sizing considerations

If you have at least one of the following requirements, contact Onapsis to obtain a customized sizing for your specific environment:

- High-availability setup
- High-frequency usage
- Parallel usage of connections by more than 10 developers
- Use of a central Control for Code instance connected with many SAP systems
- Scanning complete SAP Standard ABAP Code including Customer ABAP Code

## Supported operating systems

You need to have one of the following operating systems to install and run the Scanning System:

OS	Supported versions	Additional requirements
Linux	<p>Onapsis strongly recommends that you use a Linux installation with X windows. Otherwise, some configuration functionality will be limited.</p> <ul style="list-style-type: none"> <li>64-bit Suse Linux Enterprise Server 15</li> <li>64-bit Suse Linux Enterprise Server 12</li> <li>64-bit RedHat Enterprise Server 8</li> <li>64-bit RedHat Enterprise Server 7</li> <li>64-bit Ubuntu 20</li> </ul> <p>Earlier versions that are out of maintenance are not recommended, although the product may continue to work.</p>	
Windows	<p>The following Windows operating systems are supported:</p> <ul style="list-style-type: none"> <li>Windows Server 2022 x64</li> <li>Windows Server 2019 x64</li> <li>Windows Server 2016 x64</li> <li>Windows Server 2012 R2 x64</li> </ul> <p>Earlier versions that are out of maintenance are not recommended, although the product may continue to work.</p>	.NET Framework 4.0 and higher

## Required Java Runtime Environment

If you do not yet have a Java Runtime Environment installed, then you need to install one. Control for Code works best when the following Java version is installed on the host machine:

Java 64-bit Version JDK/JRE 11

Control for Code supports operation on 64-bit operating systems only. For downloads, use the JRE file. If you have both 32-bit and 64-bit Java installed on your system, verify that both `JAVA_HOME` and the corresponding `PATH` to Java use the 64-bit version.

The preferred version is still Java JRE 11, although Control for Code is able to run on JRE 17. Newer Java versions are tested when they are available and may also be supported. Contact your Onapsis representative if you are not certain whether you can use a newer version of Java.

We test our software on both Oracle and OpenJDK versions so you can choose the one that is most convenient for you in terms of the license and legal requirements. If you choose the Oracle release of Java, see the following website for a list of systems supported by Oracle Java 64-bit Version JDK/JRE, or to download the JRE:

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

If you prefer to use the OpenJDK version, you must install the JDK version. We recommend that you download it from:

<https://adoptopenjdk.net/>

We also test with Amazon Corretto and SAP Machine:

<https://aws.amazon.com/en/corretto/>

<https://sap.github.io/SapMachine/>

These hyperlinks lead to third-party download pages. The download provided there might be newer than the version mentioned here.

## Additional recommended software

Adobe PDF Reader 8.x or higher is recommended. PDF Reader is only necessary to view PDF reports. In TMS or Online Scan scenarios, this is only needed on the clients.

## Source System requirements

Source Systems are not required, but they enable you to use the Central System to scan ABAP code on target Source Systems without any additional installation. The Central System can read all required contents via Remote Function Calls (RFCs). To have all required remote functions available, the remote systems need to provide a certain Support Package (SP) level, as itemized in the table below:

SAP_BASIS	SP-Name	SP Required on Source System
700	SAPKB700	34

SAP_BASIS	SP-Name	SP Required on Source System
701	SAPKB701	19
702	SAPKB702	19
731	SAPKB731	21
740	SAPKB740	16
750 or higher	SAPK-75???INSAPBASIS	none

It is possible you could manually apply corrections to have Control for Code support a lower Support Package. Check each of the following SAP Notes to see if it supports your current support package stack. You can then manually apply the corrections mentioned in SAP notes: [2190065](#), [2196792](#), and [2270689](#).

## JCo requirements

The SAP Java Connector is required to process scenarios via RFC. Use the 64-bit version of SAP JCo corresponding to your operating system. The supported versions at the time this document was published are JCo 3.1.7 and 3.1.6.

OS	Required JCo files
Linux (64-bit)	<ul style="list-style-type: none"> <li>sapjco3.jar</li> <li>libsapjco3.so</li> </ul>
Windows (64-bit)	<ul style="list-style-type: none"> <li>sapjco3.jar</li> <li>sapjco3.dll</li> <li>.NET Framework 2.0 SP1</li> <li>Microsoft Visual Studio 2013 C/C++ Redistributable.</li> </ul>

To obtain the latest JCo version:

1. Visit <https://support.sap.com/>.
2. Log in.
3. Select **Products** in the top toolbar.

4. Select **SAP Java Connector** under **Connectors**.

Select the software version that matches your operating system.

### Requirements for using RFC via SNC

If you want to use Secure Network Communications (SNC) with RFC, you also need:

- The 64-bit SAP crypto libraries need to be installed. In order to obtain the latest SAP Crypto Library version, visit <https://support.sap.com/software/patches.html> and select the software version matching your operating system.
- A CA certificate and your own certificate have to be imported into your keystore. The utility **sapgenpse.exe** must be installed to import the certificates.
- SNC must be installed and running on the SAP system. To check if it is, run the report SSF02 via SA38

An RFC Connection with SNC enabled must be configured.

# Control for Code HANA

## Overview

You can use Onapsis Control for Code (HANA) to scan native SAP HANA and Fiori application code to find security vulnerabilities and view suggested solutions.

## Code scans at different development stages

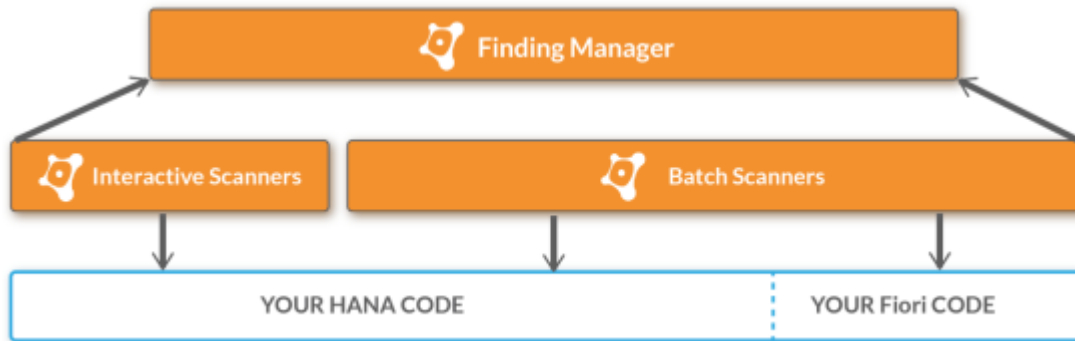
You can scan code at three points in the development cycle: during development, integrated into the CI/CD process, and in deployed production applications.

- **Development:** By finding vulnerabilities during development you can secure your code as you write it. The integration with various supported Integrated Development Environments is intuitive and similar to grammar checks in text applications. Control for Code highlights vulnerabilities in the code itself and explanations and solutions are seamlessly integrated into the IDE.
- **CI/CD:** Control for Code integrates with Transport Manager to create a checkpoint before the code is deployed. You can reject transport requests with critical and high impact vulnerabilities from deploying and assign approvers to review findings. You can scan HANA code created on SAP HANA systems, or SAPUI5 code in SAPUI5 ABAP Repositories before it is transported to other SAP systems. You can use the Jenkins plugin to automatically scan a project's source code each time the Jenkins server builds the project.
- **Production:** Finally, you can scan deployed application code in various production repositories, including:
  - SAP HANA packages in large SAP HANA deployments
  - UI5 source code in SAPUI5 ABAP repositories on SAP NetWeaver
  - Source code in Git repositories
  - SAP systems source code stored in ZIP, TGZ, or MTAR files

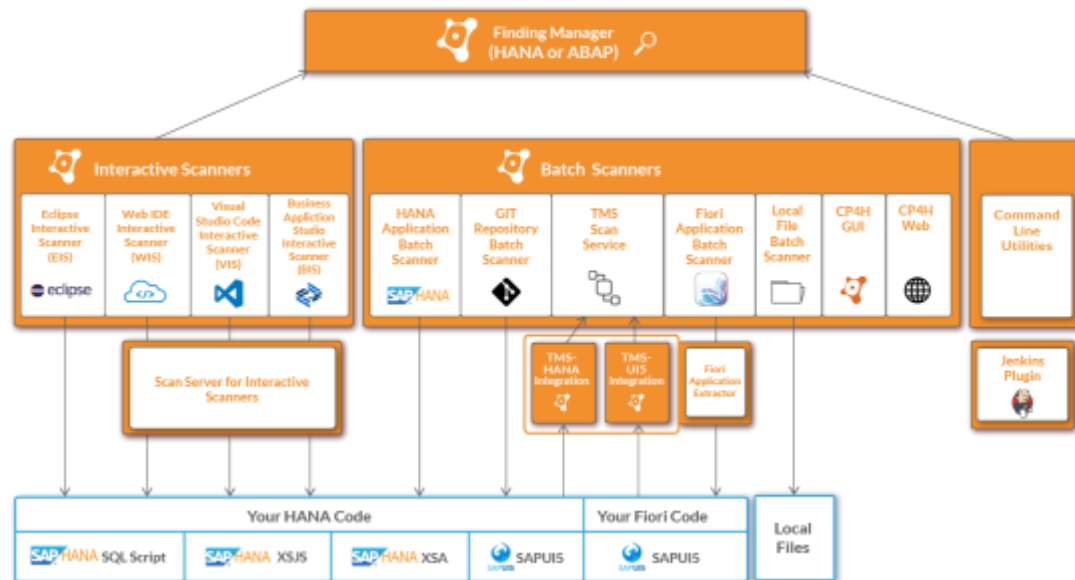
You can configure and run scans from the Control for Code GUI or Control for Code Web. Scanners are provided for Windows and Linux/UNIX environments.

Scan results are uploaded to the Finding Manager, which can have either a HANA or an ABAP database in the backend.

Simple architecture:



Detailed architecture:



## Supported code languages

Control for Code can scan the following code languages:

- SQLScript
- XSJS
- SAPUI5
- Core Data Services for XSA
- XSA/Node.js

Supported application types	HANA Native		Fiori
	XS Classic	XS Advanced	
Supported languages	SAPUI5	SAPUI5	SAPUI5
	SQLScript	SQLScript	
		CDS	
	XSJS	Node.js	



## Test cases

All of the scanners use Onapsis-provided Test Cases to identify vulnerabilities that can expose your applications to attack. For information on Test Cases, see the *Control for Code Test Cases Guide for SAP HANA®*.

## Requirements

The following are general requirements for the batch scanners and browser-based components such as Control for Code GUI and Control for Code Web. For IDE integrations, TMS integration, Jenkins integration, and Finding Manager requirements, see each of those installation sections.

## Supported operating systems

The Control for Code batch scanners and browser components support the following operating systems.

OS	Supported versions
Linux ( <b>Recommended</b> )	All recent systemd based GNU/Linux distributions.
Windows	Windows 10

## Other software requirements

The following are general requirements for batch-scanners and apply to all Control for Code HANA components that include batch-scanners:

- CP4H Web



- CP4H GUI
- Scan Server for Interactive Scanners (requirements apply if installed on a remote computer)
- Eclipse Interactive Scanner
- Jenkins Plugin

Requirement	Supported versions / Notes
Java Runtime Environment	<p>For both Windows and Linux, the scanners have been tested on:</p> <ul style="list-style-type: none"> <li>▪ Java SE 8</li> <li>▪ Java SE 10</li> <li>▪ OpenJDK 11</li> </ul> <p><b>NOTE:</b> You should configure the Java Virtual Machine (JVM) to use a heap size of 4096 MB or more.</p>
SAP Java Connector (JCo)	<p>SAP Java Connector 3.0.18 or above is required.</p> <p>You will be asked for the location of your JCo files when you install Control for Code. Use the 64-bit version of SAP JCo corresponding to your operating system, as described below:</p> <p>JCo for Linux (64-bit)</p> <ul style="list-style-type: none"> <li>▪ sapJCo3.jar</li> <li>▪ libsapJCo3.so</li> </ul> <p>JCo for Windows (64-bit)</p> <ul style="list-style-type: none"> <li>▪ sapJCo3.jar</li> <li>▪ sapJCo3.dll</li> </ul>
Node.js	<p>Tested on 14.15.0 and required to scan Core Data Services (CDS) and Node.js in XS Advanced applications.</p>

## Configure Scan Server availability

If you use Visual Studio, Business Application Studio, WebIDE, or cloud extensions, those extensions must be able to communicate with the Scan Server. Cloud extension communication might require that you configure the Scan Server host system to be open to web communication.

## Web browser requirements

The following browsers are supported to use Control for Code GUI, Control for Code Web, and Finding Manager:

- Google Chrome
- Firefox

**CAUTION:** Internet Explorer 11 or Edge browsers are not recommended. Control for Code GUI and Control for Code Web are built using SAPUI5 and therefore depend on full SAPUI5 browser support.

## Configure required database access

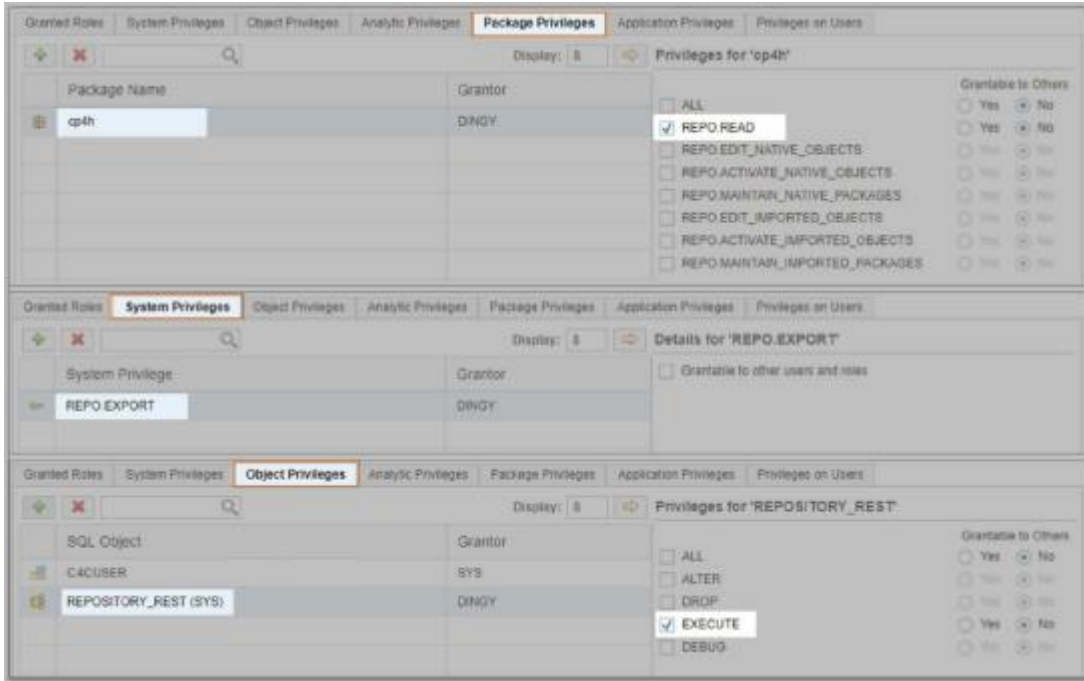
To scan SAP HANA application code, Control for Code must access the SAP HANA database repository and export the code. The repository is secured with authorization checking, so to run a Control for Code scan a user must have the following repository privileges:

Privilege Type	Privilege
Package privileges	The user running Control for Code should be granted the following privileges for all packages to be scanned: REPO.READ
System privileges	REPO.EXPORT
Object privileges	To be able to access the repository in SAP HANA Studio or another client, the user needs the EXECUTE privilege on the database procedure REPOSITORY_REST.

To check a user's privileges, take the following steps:

1. Log into the SAP GUI.
2. Navigate to **Security**.
3. Select the user under **Users**.

4. Click the **Package Privileges** tab and check the privileges, for example in the following screenshot the user C4CUSER has been granted the REPO.READ package privilege on the cp4h package, the REPO.EXPORT system privilege and the EXECUTE object privilege on REPOSITORY\_REST (SYS):



The image displays three screenshots of the Onapsis Privilege Management interface, illustrating the configuration of privileges for different users and objects.

**Top Screenshot: Package Privileges for 'cp4h'**

Package Name	Grantor	Privileges for 'cp4h'	Grantable to Others
cp4h	DINGY	<input checked="" type="checkbox"/> REPO.READ	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> REPO.EDIT_NATIVE_OBJECTS	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> REPO.ACTIVATE_NATIVE_OBJECTS	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> REPO.MAINTAIN_NATIVE_PACKAGES	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> REPO.EDIT_IMPORTED_OBJECTS	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> REPO.ACTIVATE_IMPORTED_OBJECTS	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> REPO.MAINTAIN_IMPORTED_PACKAGES	<input type="radio"/> Yes <input checked="" type="radio"/> No

**Middle Screenshot: System Privileges**

System Privilege	Grantor	Details for 'REPO.EXPORT'
REPO.EXPORT	DINGY	<input type="checkbox"/> Grantable to other users and roles

**Bottom Screenshot: Object Privileges for 'REPOSITORY\_REST'**

SQL Object	Grantor	Privileges for 'REPOSITORY_REST'	Grantable to Others
C4CUSER	SYS	<input type="checkbox"/> ALL	<input type="radio"/> Yes <input checked="" type="radio"/> No
REPOSITORY_REST (SYS)	DINGY	<input checked="" type="checkbox"/> EXECUTE	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> ALTER	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> DROP	<input type="radio"/> Yes <input checked="" type="radio"/> No
		<input type="checkbox"/> DEBUG	<input type="radio"/> Yes <input checked="" type="radio"/> No

# Control for Transport

## Installation options

The two installation options are summarized below to help you determine which is best. The options are described in detail in the sections that follow.

	Summary	Advantages	Disadvantages
Setup 1 - Zero footprint (on page <a href="#">36</a> )	You inspect Transport Requests (TRs) throughout your system landscape from a single system, called the Central System.	<ul style="list-style-type: none"> <li>You only need to install Control for Transport on the Central System</li> <li>All inspection results are stored and accessed centrally</li> </ul>	<ul style="list-style-type: none"> <li>Adhoc inspections are not possible because, although the Control for Transport Cockpit is available, it can only be used to validate the setup of the Central System</li> <li>TMS integration with Approval Workflow is not possible</li> </ul>
Setup 2 - Developer optimum (on page <a href="#">39</a> )	You install Control for Transport on individual SAP systems.	<ul style="list-style-type: none"> <li>Adhoc inspections at any point in time via the Control for Transport Cockpit</li> <li>TMS integration with Approval Workflow is possible</li> </ul>	<ul style="list-style-type: none"> <li>You need to install Control for Transport on all involved systems (Satellite Systems)</li> <li>Inspection results are stored and accessed on several systems</li> </ul>

### Setup 1 - Zero footprint

With Zero Footprint, you set up a Central System from which you manage the Transport Paths between systems that you want to inspect. These systems that you want to inspect are referred to as Source Systems. On dedicated Source Systems, you add a

tiny code snippet so that Control for Transport is automatically invoked whenever a TR is imported or exported. In this way, you ensure that TRs are always inspected. More specifically, there are two types of Source Systems that you need to set up:

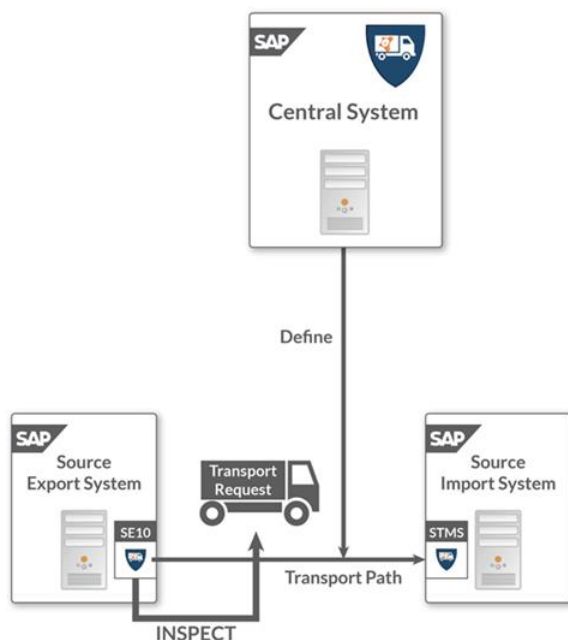
- **Source Export Systems** - A Control for Transport **Inspection Before Export** is invoked automatically whenever a user exports (i.e., releases) using the SE10 transaction.
- **Source Import Systems** - A Control for Transport **Inspection Before Import** is invoked automatically whenever a user imports a TR through the STMS transaction.

Code snippets added to SE10 and STMS enable this functionality on systems that you designate as Source Systems. In a 3-system-landscape you would typically add the code snippet for transaction STMS on the development and on the production system, while you add the code snippet for transaction SE10 only on the development system. Further information can be found in the *Control for Transport Installation Guide*. After each system is set up, you define the *Transport Paths* between each system.

The diagrams that follow illustrate an Inspection Before Export and an Inspection Before Import on a Source System.

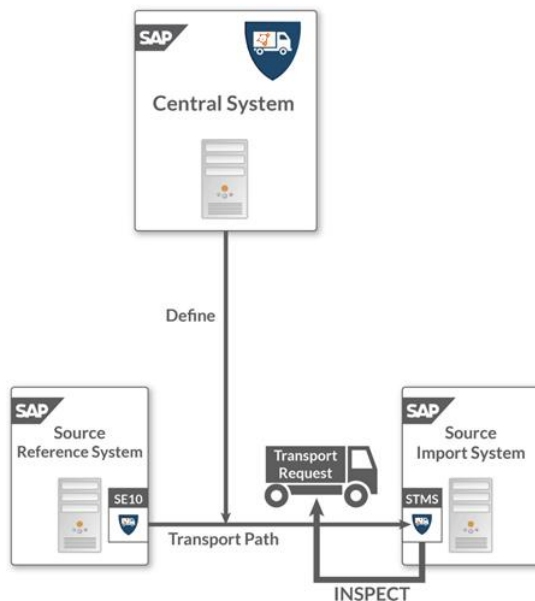
### Inspection before export

With an Inspection Before Export, any export invoked on a Source System using SE10 automatically triggers an inspection of the TR, based on the Transport Path that you have defined on the Central System:



## Inspection before import

With an Inspection Before Import, any import invoked on a Source System using STMS automatically triggers an inspection of the TR, based on the Transport Path that you have defined on the Central System:



Also, you have to prepare the modification in the Source Import System to implement the STMS trigger.

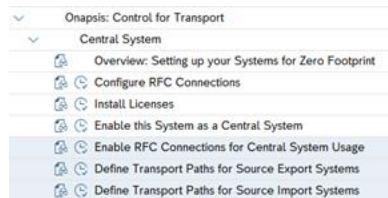
## Prepare for Setup 1

To prepare for Setup 1, you should identify which systems in your landscape will be Source Systems. As mentioned earlier, Zero Footprint does not provide the possibility for adhoc inspections with the Control for Transport Cockpit. Thus, Control for Transport is invoked automatically behind the scenes during the export or import of a transport request.

Regardless of this, each Source System needs:

- An enabled RFC Connection from the Central System to the Source System.
- An RFC connection from the Source System to the Central System.
- A Transport Path for exports and/or imports.

After installing Control for Transport on the Central System, you have access to the IMG, and in the **Central System** node, the last three options allow you to enable the RFC Connections and then to set up the Transport Paths for both types of Source Systems. The second node, **Configure RFC Connections**, enables you to set up your RFC Connections before:



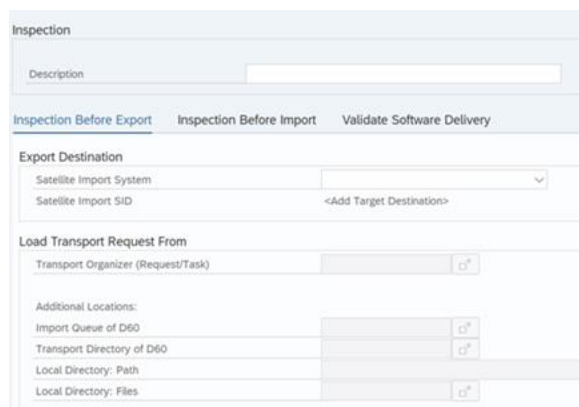
The *Control for Transport Installation Guide* has complete information about setting up your Central and Source Systems.

## Setup 2 - Developer optimum

With Developer Optimum, you need to install Control for Transport on each SAP system on which you want to inspect an import or an export. While this involves a bit more work, it has the advantage of providing you with the Cockpit and other GUI elements, which are very convenient for initiating inspections. So, with Setup 1, Control for Transport is invoked automatically in the background, with Setup 2, Control for Transport can be additionally invoked manually through the Cockpit.

### Inspection before export

On each Satellite System, you can start an **Inspection Before Export** using the first tab of the Cockpit, which is shown below:

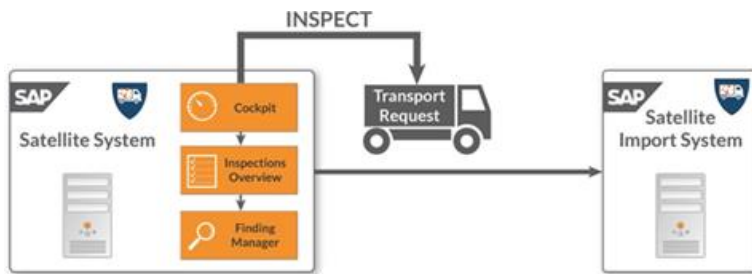


The process is quite simple:

1. Specify an **Export Destination**. That is, a system to which you intend to export the TR. The available options are listed in the **Satellite Import System** drop-down. You define the systems that display in this drop-down as described in the Prepare for Setup 2 (on page [41](#)).
2. Specify a TR that you want to inspect. Typically, you do this using the first option under **Load Transport Request From**, which is the **Transport Organizer**. However, you can also choose from a few different **Additional Locations**, including the **Import Queue**, a **Transport Directory** or even **Files** stored in a **Local Directory**.
3. Execute to start the inspection.

All your inspections are stored persistently, and the results of every inspection can be accessed later via the **Finding Manager**, as described in the *Control for Transport User Guide*.

Conceptually, the process looks like this:



## Inspection before import

On each Satellite System, you can initiate an **Inspection Before Import** using the second tab in the Cockpit:

Inspection

Description

Inspection Before Export   **Inspection Before Import**   Validate Software Delivery

Load Transport Request From

Import Queue

Additional Locations:

Transport Directory

Local Directory: Path

Local Directory: Files

◀ ▶



The process is quite similar to an Inspection Before Export, except of course there is no destination. Rather, you simply specify the TR that you intend to import. So, the process is:

1. Specify a TR that you want to inspect. Typically, you do this using the first option under **Load Transport Request From** , which is the **Import Queue** . However, you can also choose from a few different **Additional Locations**, including the **Import Queue**, a **Transport Directory** or even **Files** stored in a **Local Directory**.
2. Execute to start the inspection.

All of your inspections are tracked with the **Inspections Overview** GUI so that you can track the status of each, and the results of inspections display in the Finding Manager, as described in the *Control for Transport User Guide*.

Conceptually, the process looks like this:



## Prepare for Setup 2

First, you should identify which of your systems will serve as Satellite Systems. Once you do this setting them up is fairly similar to Source Systems:

1. Enable RFC Connections to Satellite Import Systems. These then display in the Satellite Import Systems drop-down in the Cockpit.
2. Identify the RFC Connection to the Satellite Reference System.

You do this with the third and fourth options in the Satellite System node of the IMG, both of which are highlighted below. The second node, Configure RFC Connections, enables you to set up the required RFC Connections before.



## Understand the prerequisites

This chapter lists the supported SAP NetWeaver (ABAP) versions for Central Systems, Satellite Systems, and Source Systems.

**CAUTION:** Control for Transport does not support the inspection of non-unicode transport files. Control for Transport inspects unicode transport files only.

### Central System and Satellite System prerequisites

One of the following SAP Basis levels and Support Packages are required for a successful installation of the product:

- 7.00 SP27 or higher
- 7.01 SP12 or higher
- 7.02 SP12 or higher
- 7.31 SP05 or higher
- 7.40
- 7.50
- SAP\_BASIS 7.51 (including SAP S/4HANA 1610)
- SAP\_BASIS 7.52 (including SAP S/4HANA 1709)
- SAP\_BASIS 7.53 (including SAP S/4HANA 1809)
- SAP S/4HANA 1909
- SAP S/4HANA 2020

**NOTE:** Control for Transport versions after 4.1 will require the Central System to have SAP NetWeaver 7.4 with Support Package 8 or higher. Older versions of SAP NetWeaver will not be supported in Control for Transport releases after version 4.1.

## Source System prerequisites

The following Support Package (SP) levels are supported:

SAP_BASIS	SP-Name	SP Required on Source System
700	SAPKB700	34
701	SAPKB701	19
702	SAPKB702	19
731	SAPKB731	21
740	SAPKB740	17
750 or higher	SAPK-75???INSAPBASIS	none

It is possible you could manually apply corrections to have Control for Code (ABAP) support a lower Support Package. Check each of the following SAP Notes to see if it supports your current support package stack. You can then manually apply the corrections mentioned in the note.

- 2190065
- 2196792
- 2270689

## Frontend prerequisites

- Control for Transport requires the SAP GUI. Onapsis always recommends using the latest SAP GUI version including patches, regardless of the SAP system version. Please follow the instruction guides provided in the SAP Support Portal.
- Adobe Reader version 10.x or newer is recommended to view the Control for Transport reports.

## Special Test Case prerequisites

There are special prerequisites for particular Test Cases (TCs) on top of the minimum prerequisites mentioned above.

## ST-PI Prerequisites for TCs 16, 20, 24, 158 and 159

The required statistics for TC158 and TC159 are read from tables **/SDF/OI\_TABSTAT** and **/SDF/OI\_REPSTAT**, which belongs to the **ST-PI** software component. In order to populate these tables, it needs to activate the collector for the online import check for one week. Among others, the collector reads the UPL data and calculates and stores hourly values for the calling rate of each include, summarized at the master include level.

Therefore, the online import data collector requires minimum support package levels of the installed **ST-PI** version:

- For ST-PI release 7.40 - Support Package 6 or higher is required
- For ST-PI releases 2008\_1\_xxx - Support Package 16 or higher is required

These SP levels of the ST-PI component are also required for TCs 16, 20, and 24 in a Zero Footprint Scenario (Setup 1).

# CleanupSolutions

## System requirements

### SAP landscape

You install the Control CleanupSolutions main component on each SAP NetWeaver ABAP system in your system landscape. Control CleanupSolutions is only available for Unicode systems.

If you want to install the Control CleanupSolutions CodeProfiler Bridge, CodeProfiler for ABAP version 4.2 or higher must also be installed on your system. Note that as of October 2021, CodeProfiler for ABAP was renamed Control for Code.

### Supported SAP NetWeaver (ABAP) systems

Control CleanupSolutions supports SAP NetWeaver Releases 7.00 or higher and the same SAP NetWeaver versions as Control for Code for ABAP, which are (at the time of the publication of this document):

- SAP NetWeaver 7.00
- SAP NetWeaver 7.01
- SAP NetWeaver 7.02
- SAP NetWeaver 7.03
- SAP NetWeaver 7.31
- SAP NetWeaver 7.40
- SAP NetWeaver 7.50
- SAP NetWeaver 7.51
- SAP NetWeaver 7.52
- SAP S/4HANA 1709
- SAP S/4HANA 1809
- SAP S/4HANA 1909
- SAP S/4HANA 2020

- SAP S/4HANA 2021
- SAP S/4HANA 2022
- SAP BW/4HANA (any version)
- SAP S/4HANA Foundation (any version)
- ABAP Foundation on HANA (any version)
- SAP S/4HANA Cloud extended edition (EX)

If you use other releases, contact Onapsis.

# On-Change Control

## Installation planning

### Installation overview

The following diagram summarizes the installation steps:

- Installation of SAR file (add-on) in Solution Manager client 000
- Assign On-Change Control roles and business roles to target users
- Copy the Transport Generic Check BAdI implementation in your namespace
- Define and assign RFC permission to execute inspections and allow SAP GUI access
- Customize the scan and approval process



### Software prerequisites

NOTE: This document assumes at least one scanner tool (Control for Code or Control for Transport) is installed. To install either of these tools, please review the corresponding installation guides.

On-Change Control is an SAP Add-on installed in a Solution Manager system.

Product	Minimum Version Required	Notes
SAP Solution Manager	7.2 SP10 or higher	ChaRM must also be configured and running for every managed system.
Onapsis Control for Transport (if used)	Latest two versions	On-Change Control is compatible with both full deployments and zero footprint installations.
Onapsis Control for Code (if used)	Latest two versions	This document assumes all scanner tools are up and running in the managed system.
Onapsis Control Central (if used)	Latest version	On-Change Control is compatible with the initial version of Control Central delivered with Onapsis Control v2022r1.

The following component and support package (SP) levels are supported:

Component	SP Name	Release	SP Level
ST	SAPK-72010INSTMAIN	720	0010
SAP_BASIS	SAPKB74021	740	0021
SAP_ABA	SAPKA74021	740	0021
WEBCUIF	SAPK-74718INWEBCUIF	747	0018
BBPCRM	SAPKU71318	713	0018

## Scan planning

On-Change Control enables you to deploy a client sensitive online scan and an automatic scan at the release stage. That is, from a single customization point, you can select exactly which scanner and test cases are going to be executed per client.



Before you install On-Change Control, you should consider and reach agreement on the following scan setting questions:

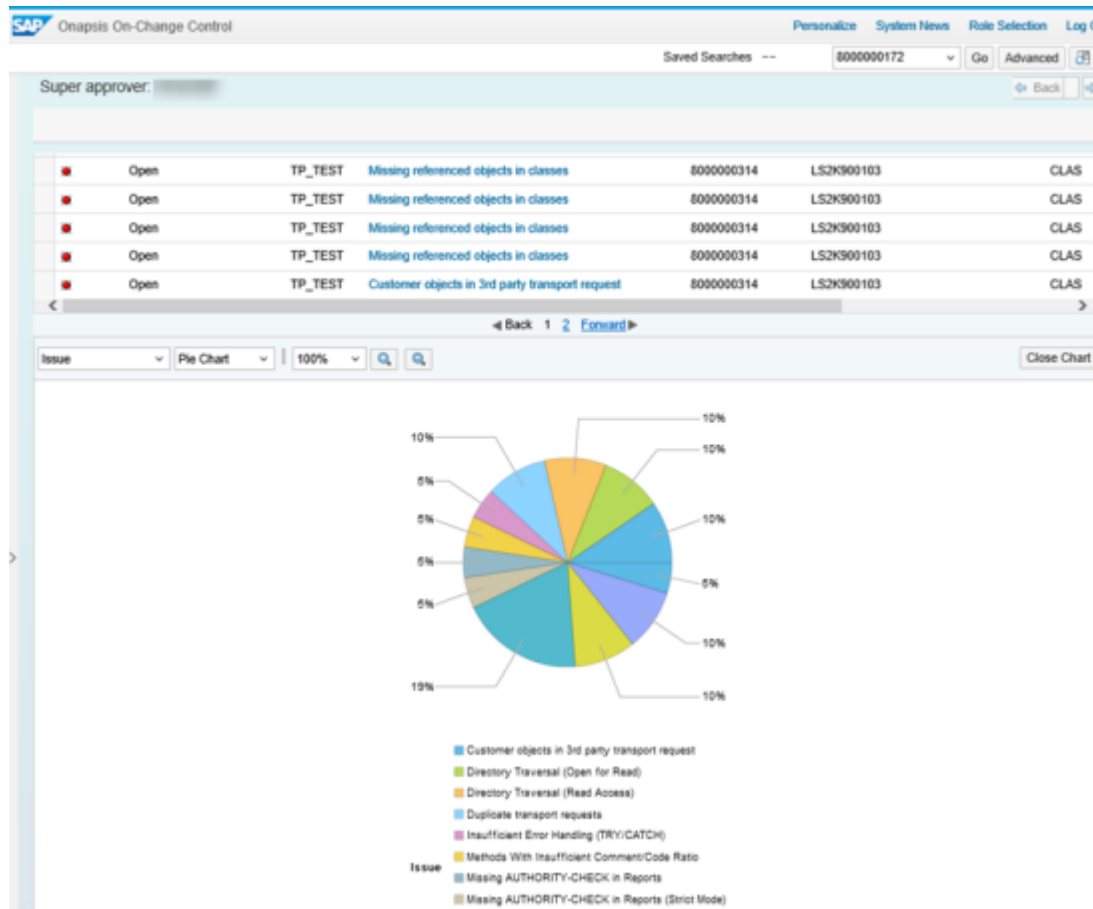
	Question	Purpose
1	Which Transaction Types are relevant for my On-Change Control installation?	Identify the ChaRM transaction types in scope
2	Which systems are going to be scanned?	Determine the systems that are in scope for the On-Change Control integration
3	Which scanner will be used on each system?	Identify the scanners to be used to scan each of the systems in scope
4	What type of installation is used on every managed system?	Prepare the On-Change Control configuration according to managed systems landscape: full Installation versus zero footprint Installation
5	What test cases will be run on each system?	Prepare the On-Change Control configuration in terms of test cases groups to be used
6	Am I authorized to add permissions in standard "ChaRM RFCs"?	Determine if the standard ChaRM RFCs are intended to be used
7	Is the Navigation from ChaRM to managed allowed (trusted navigation)?	In case the navigation to Control for Transport or Control for Code Finding Manager (FidMan) is needed to check finding details
8	Is there a system where you want to define an automatic approval?	Start the scanning process, with automatic approval process, immediately after installation with the purpose of collecting finding information to plan the future approver groups.

## Approval planning

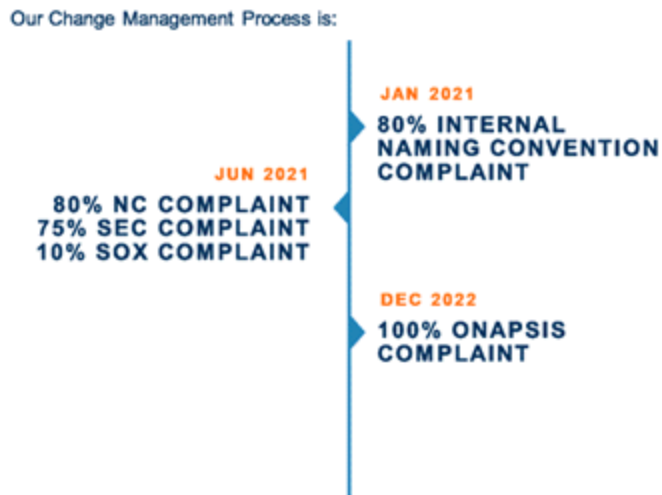
Onapsis Control Central, Control for Transport, and Control for Code cover an extensive range of test cases from different domains. Consequently, these products can produce an overwhelming number of findings, especially if your organization has not previously worked with any automatic control system.

In order to prevent this negative impact, we recommend setting a "trial period" by configuring clients with an automatic approval process. After a certain period of time, and depending on the volume of releases produced per client, you would then be able to define the number of approvers, the grouping of findings (approval domain), and the skills required to set up a new control team.

You would be able to use your issue profile to determine the group of specialists required and the expected workload and plan for new approval teams.



As resources are always limited, On-Change Control offers a flexible framework to configure different deployment options. You can define the number of test cases to be applied per client and gradually increase the number of controls and improve the quality of your change management process. The following graphic is an example of a staggered approach for security compliance, where you begin with limited coverage and continue to expand test cases, controls, and targets over time.



Before you set up your approval process plan, you should answer the following questions:

	Question	Purpose
1	Is there an active approval group?	Identify if the review and approval process within the Change Management is already defined in your organization
2	What kind of findings does this group validate?	Determine the skills and team structure to be put in place for handling the review and approval activities
3	What kind of findings are expected to occur?	Determine the skills of the resources needed to process the findings
4	What volume of findings will be produced per system and month?	Determine the size of team working on processing the findings generated during the Change Management Process

# Control Central

## Scan Service

### Overview

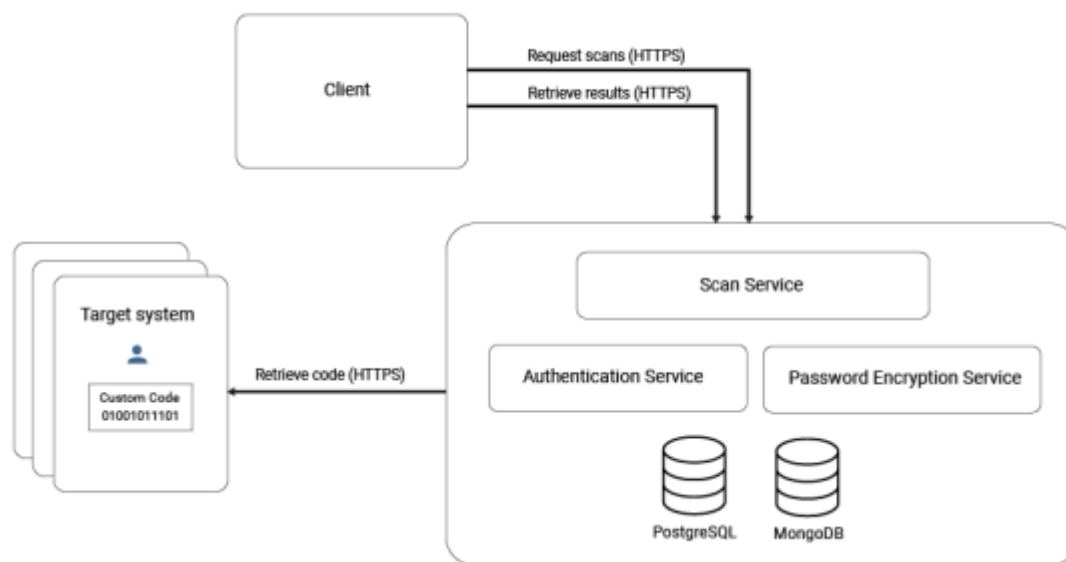
You can use the Onapsis Scan Service to scan custom source code for security vulnerabilities. Clients communicate with the Scan Service through a REST API. The Scan Service is packaged with Onapsis Control Central, however it is client agnostic, meaning it can process scan requests from any client.

The service can retrieve the source code from target systems or you can provide the code in archive files. In this release, the Scan Service can retrieve source code from SAP ABAP systems (SAPUI5 ABAP repositories), SAP HANA systems, and Git repositories.

Before you install the Scan Service you must configure its security, including client authentication and HTTPS communication. The Scan Service includes the core Scan Service API and several other APIs for administration and security configuration.

### Architecture

The following graphic is a high-level representation of the Scan Service architecture:



This guide only describes the Scan Service. For information on configuring specific clients for the Scan Service, refer to the client documentation.

## Requirements

You must meet the following Scan Service minimum requirements.

### License requirements

To scan ABAP and HANA target systems, the Scan Service uses Scan Engine ABAP 5.5 and Scan Engine HANA 2.8. To use those, you must have the appropriate licenses. For information, ask your Onapsis representative.

### Hardware requirements

Scan Service minimum hardware requirements depend to some extent on the clients, and how you use the Scan Service. For example, you can use Control Central to perform large scans on your whole namespace or small scans on parts of your namespace. Large scans might require more disk space and RAM. For information on additional requirements for specific clients, see the client documentation.

Minimum hardware requirements:

- CPU: AMD64/EM64T 64-bit mode compatible multi-core CPU (Quad-Core)
- Hard disk: 128 GB hard disk space (above what is required for the operating system)
- RAM: 16 GB

### Software requirements

Meet the following Scan Service minimum software requirements.

#### Install an Ubuntu or RedHat host system

You must install an Ubuntu 20 or Red Hat (RHEL) 8.4 operating system. It is highly recommended that you make sure the system is up to date with the latest security patches.

#### Install Kubernetes

To install Kubernetes on the host system, take the following steps:

1. Log into the host computer as a user in the sudo group.
2. Install latest kubectl install file, for example run the following curl command:

```
$ curl -LO "<https://dl.k8s.io/release/$>(curl -L -s  
'https://dl.k8s.io/release/stable.txt')/bin/linux/amd64/kubectl"
```

3. Check the file hash, for example run the following curl command:

```
$ curl -LO "<https://dl.k8s.io/$>(curl -L -s  
https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl.sha256"
```

4. Install kubectl and installation check the version, for example run the following curl command:

```
$ sudo install -o root -g root -m 0755 kubectl  
/usr/local/bin/kubectl kubectl version --client --output=yaml
```

**NOTE:** For more information, see the [Kubernetes documentation](#).

#### Install Java and OpenSSL

You need Java and OpenSSL to prepare the keystores, truststores, and X.509 certificates used by the Scan Service. You can generate them on any machine and copy them to the Ubuntu machine where you install Scan Service. The following are minimum supported versions. If you use other versions, see the vendor documentation for those versions:

- Java 8, OpenJDK 11
- OpenSSL 1.1.1n

To install Java on the host system you can usually run the `yum install -y java-11-openjdk.x86_64` command. If installation fails with the error "No available modular metadata for modular package," then take the following steps to install Java manually:

1. Download the `javapackages-filesystem-5.3.0-1.el8 rpm` file from a trusted website.
2. To install the Java packages filesystem layout, run the following command:

```
$ yum install -y javapackages-filesystem-5.3.0-  
1.el8.noarch.rpm
```

3. To install Java and check the version, run the following commands:

```
$ yum install -y java-11-openjdk.x86_64
```

```
$ java -version
```

4. To install Open SSL and check the version, run the following commands:

```
$ sudo yum -y install openssl openssl-devel
```

```
$ openssl version
```

#### SAP JCO library files

Download the following SAP JCO library files for Linux (64-bit), version 3.1.2 or higher:

- sapjco3.jar
- libsapjco3.so

## Control for Code ABAP

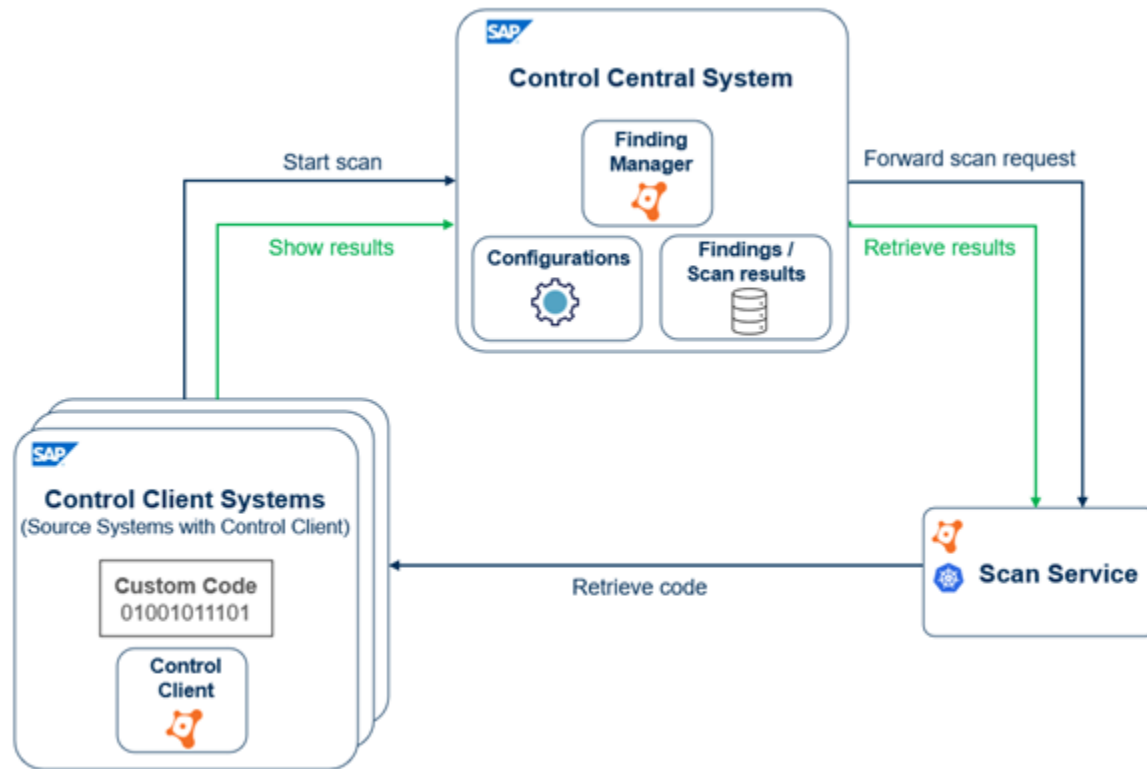
### Installation overview

The goal of Onapsis Control is to automate custom code analysis to help identify, resolve, and eliminate errors during development—before negative consequences arise in your business-critical applications. The streamlined logic and architecture means you can deploy Onapsis Control Central across your landscape with minimal deployment and maintenance efforts on each ABAP system.

You can build Onapsis Control solutions into your development environment and processes so that you can first get your code clean, and then ensure that it stays that way.

### Recommended architecture

The following graphic represents our recommended installation architecture for Onapsis Control Central.



As you can see, you need one Control Central System, one Scan Service, and at least one Control Client System on which to scan code. The Control Client System is any supported Source System on which you have installed the Onapsis Control Client.

**NOTE:** You can also scan code on the Control Central System if you install the Onapsis Control Client on the Control Central System.



## Product components

The various components are:

Component	Required?	Description
<b>System scanning components</b>		
Control Central System	Yes	<p>A logical system designation for a single, centralized system that:</p> <ul style="list-style-type: none"> <li>Processes scans of Control Client Systems.</li> <li>Maintains configuration details related to Control Client systems.</li> <li>Contains functionality used by all Control Clients. (For example, the Finding Manager and the ability to monitor and troubleshoot scans.)</li> <li>Creates and secures the connection to the Scan Service.</li> </ul> <p>We recommend that you use a new SAP system and dedicate it to serving as the Control Central System so that you have full control to apply updates for future releases.</p>
Control Client System	Yes	<ul style="list-style-type: none"> <li>Source System on which you have installed the Onapsis Control Client to enable code scanning.</li> <li>Developers can initiate code scans on these Control Client Systems and review scan results.</li> <li>Typically, these are your development systems.</li> </ul>
Scan Service	Yes	<ul style="list-style-type: none"> <li>Performs the actual scanning of custom code.</li> <li>Client agnostic, meaning it can process scan requests from any client, for example Onapsis Control Central or the Onapsis Azure Integration.</li> <li>Clients communicate with the Scan Service through a REST API.</li> </ul> <p>For details, see the <i>Onapsis Scan Service Installation Guide</i>.</p>

Component	Required?	Description
Source System	Yes	<ul style="list-style-type: none"> <li>Any target system that meets the minimum requirements to be scannable (see Source System requirements (on page <a href="#">62</a>)).</li> <li>Once the Onapsis Control Client is installed on Source Systems, they are referred to as Control Client Systems.</li> </ul>
<b>Available integrations</b>		
ABAP Workbench	Yes	<ul style="list-style-type: none"> <li>Provides additional menu options in the ABAP Workbench that enable developers to execute scans without leaving the development environment.</li> <li>Integration with SE80 is the minimum required integration, SE38, SE37, SE24, and SE10-SE09 are also available.</li> </ul>
SAP Transport Management System (TMS)	No	<ul style="list-style-type: none"> <li>Integration is dependent on your license agreement.</li> <li>Recommended for development systems.</li> <li>Ensures only clean code can be transported into your QA or production systems.</li> </ul>
Integrated Scanner for ATC/SCI (ISA)	No	<ul style="list-style-type: none"> <li>For developers working in ABAP Test Cockpit (ATC) and the SAP Code Inspector (SCI).</li> <li>Install Control Client on a central ATC System connected to the Control Central System to scan each development system locally or remotely, or install Control Client directly on a satellite ATC system to scan that system.</li> <li>Control test cases are integrated into ATC/SCI checks. View Control findings within SAP tools.</li> </ul>

Component	Required?	Description
SAP Change Request Management (ChaRM)	No	<ul style="list-style-type: none"> <li>Integration is dependent on licensing Onapsis On-Change Control.</li> <li>Detects finding in change documents to ensure your change management process is executed safely and securely.</li> <li>Provides an approval framework to manage findings by accepting or rejecting associated risk.</li> </ul>
Azure Pipeline	No	<ul style="list-style-type: none"> <li>Adds a Control code scan task to your Azure DevOps pipeline.</li> <li>Provides REST APIs to scan source code.</li> </ul>

**IMPORTANT:** For further information and advice on the best way to set up your landscape and the various components, contact your Onapsis representative to complete a solution architecture review. The solution architecture review determines whether the recommended approach is the optimal installation architecture for your organization. For example, if you have several geographical system landscapes, you will need a Control Central System and Scan Service for each one.

## Installation planning

Here we provide recommendations for preparing for the installation and the installation requirements. Carefully planning the installation and integration into your SAP system landscape ensures that you have a successful installation and that you can take full advantage of all the product features.

### Network segment recommendations

To reduce latency and performance reduction, we recommend that you plan to install the Control Central System and the Scan Service in the same network segment as the SAP system, preferably in the same data center. For more information on the Scan Service, see the *Onapsis Scan Service Installation Guide*.

## SAP kernel recommendations

Onapsis recommends that you operate your SAP systems using an SAP kernel that is within the official maintenance period of SAP. Nonetheless, Onapsis Control products may run properly with older versions of SAP kernel. For additional details, see [Supported SAP versions](#) (on page [60](#)).

## SAP System requirements

Before you start to install the base components on your SAP systems, ensure that they meet all of the system and software requirements described in [Supported SAP versions](#) (on page [60](#)).

### SPAM and SAINT requirements

The installation requires a SPAM and SAINT version 0063 or higher. If you use SPAM and SAINT version 0063, you have to implement [SAP Note 2378346](#). To uninstall the relevant software components, you need SPAM and SAINT version 0064 or higher.

### Frontend GUI requirements

Onapsis Control Central requires SAP GUI. Onapsis always recommends using the latest SAP GUI version, including patches, regardless of the SAP system version. Follow the instructions provided in the Service Marketplace to install SAP GUI.

## Appendix 6: Supported SAP versions

The minimum requirements for each system are listed here. This list reflects the SAP products supported at the time Onapsis Control Central was released. Over time, the SAP products listed here may go out of SAP maintenance. Onapsis only supports products installed on systems within the official maintenance period. Although Onapsis Control Central may continue to function against SAP systems that are out of maintenance, new Onapsis Control Central functionality is only tested against systems within the official maintenance period. Do not use other SAP systems without first checking with Onapsis.

**CAUTION:** Do not install Onapsis Control Central on non-Unicode SAP systems because they are not currently supported.

## Control Central System requirements

The minimum requirements are:

- SAP NetWeaver 7.40 with SP 17 or higher

NOTE: It is possible to use a Support Package (SP) level 10 or higher. However, if you plan to scan code on the Control Central System, meaning it also acts as your Source System, SP 17 or higher will work out of the box, while lower SP levels (less than 17 but higher than 10) require additional, manual steps. For more information, see [Source System requirements](#).

- SAP NetWeaver 7.50
- SAP NetWeaver 7.51
- SAP NetWeaver 7.52
- SAP S/4HANA 1709
- SAP S/4HANA 1809
- SAP S/4HANA 1909
- SAP S/4HANA 2020
- SAP S/4HANA 2021
- SAP S/4HANA 2022
- SAP BW/4HANA (any version)
- SAP S/4HANA Foundation (any version)
- ABAP Foundation on HANA (any version)
- SAP S/4HANA Cloud extended edition (EX)

If you want to scan custom code on your Central System, ensure you also review the requirements for the Control Client System.

## Control Client System requirements

The minimum requirements are:

- SAP NetWeaver 7.00 with BASIS\_RELEASE 700 SP 34 or higher

NOTE: It is possible to use a lower Support Package (SP) level. However, using a lower SP level requires additional, manual steps. For more information, see [Source System requirements](#). However, for BASIS\_RELEASE 700, the SP level must be 27 or higher in order to import the Onapsis Control Client software components.

- SAP NetWeaver 7.01 with BASIS\_RELEASE 701 SP 19 or higher\*
- SAP NetWeaver 7.02 with BASIS\_RELEASE 702 SP 19 or higher\*
- SAP NetWeaver 7.31 with BASIS\_RELEASE 731 SP 21 or higher\*
- SAP NetWeaver 7.40 with BASIS\_RELEASE 740 SP 17 or higher\*

\* NOTE: It is possible to use a lower Support Package (SP) level. However, using a lower SP level requires additional, manual steps. For more information, see [Source System requirements \(on page 62\)](#).

- SAP NetWeaver 7.50
- SAP NetWeaver 7.51
- SAP NetWeaver 7.52
- SAP S/4HANA 1709
- SAP S/4HANA 1809
- SAP S/4HANA 1909
- SAP S/4HANA 2020
- SAP S/4HANA 2021
- SAP S/4HANA 2022
- SAP BW/4HANA (any version)
- SAP S/4HANA Foundation (any version)
- ABAP Foundation on HANA (any version)
- SAP S/4HANA Cloud extended edition (EX)

## Source System requirements

Source Systems are the target systems that should be scanned. All of the content required for a scan is retrieved via Remote Function Calls (RFCs) using the standard SAP Function Modules. To install the Onapsis Control Client on the source system, see [Control Client System requirements \(on page 62\)](#).

The following SAP products are supported:

- SAP NetWeaver 7.00 with BASIS\_RELEASE 700 SP 34 or higher\*
- SAP NetWeaver 7.01 with BASIS\_RELEASE 701 SP 19 or higher\*

- SAP NetWeaver 7.02 with BASIS\_RELEASE 702 SP 19 or higher\*
- SAP NetWeaver 7.31 with BASIS\_RELEASE 731 SP 21 or higher\*
- SAP NetWeaver 7.40 with BASIS\_RELEASE 740 SP 17 or higher\*
- SAP NetWeaver 7.50
- SAP NetWeaver 7.51
- SAP NetWeaver 7.52
- SAP S/4HANA 1709
- SAP S/4HANA 1809
- SAP S/4HANA 1909
- SAP S/4HANA 2020
- SAP S/4HANA 2021
- SAP S/4HANA 2022
- SAP BW/4HANA (any version)
- SAP S/4HANA Foundation (any version)
- ABAP Foundation on HANA (any version)
- SAP S/4HANA Cloud extended edition (EX)

\* NOTE: It is possible you could manually apply SAP Note [2190065](#), [2196792](#), or [2270689](#) to use a lower SP. Check each of the SAP Notes to see if it supports your current SP stack, and then manually apply the corrections mentioned in the note. As these SAP Notes are part of the SAP standard, implementing these notes is outside the scope of the services and support provided by Onapsis. Additionally, the SAP notes are updated frequently and, as the requirements have changed over time and are likely to continue to change in the future, we cannot provide a reliable statement about the minimum supported SP levels.