

Pathlock Quick Installation Guide

Vulnerability Management and Code Scanning



Contents

Introduction.....	2
Prerequisites	2
Installation	3
Assess Your System	5

Introduction

Welcome to the Quick Installation Guide for Pathlock's SAP Cyber Defense Application. This guide provides a structured, step-by-step setup process designed to get you up and running in less than four hours.

To ensure a smooth installation, please ensure that you (or your colleagues) have the necessary SAP Basis authorizations and a basic understanding of SAP Basis administration. Once setup is complete, you will be able to perform vulnerability management and code scanning assessments on your system. Please note that the application has certain limitations in depth and does not support cross-system analysis.

If you wish to activate the full version, an additional hour of configuration is required.

For assistance at any stage, please contact your local Pathlock representative or visit our website at <https://pathlock.com>. We look forward to your feedback and are committed to supporting your security needs.

Thank you for choosing Pathlock and enjoy your installation!

Prerequisites CAC

Pathlock always tries to keep the requirements as low as possible.

For a quick assessment, the minimum requirements are as follows

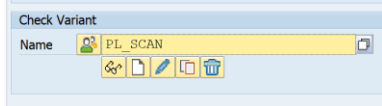
- SAP_BASIS 7.40 SP09
- SAP_GWFND 7.40 SP9
- SAP_UI 7.54 SP8

The application itself runs completely on the web. The UI5 libraries are fetched from SAP via the Internet. Therefore, an internet connection is required for the client.

However, at no point will any of your personal, company or system related data be shared with SAP or Pathlock through our application.



Installation

Step 1 Download, extract, and import transport and role upload as described in the package. You are done as soon as everything is completely implemented into your system.	Step 2 Open Transaction SUPC and generate the profile for all /SAST/* roles. After this step, all roles are generated and can be used.	Step 3 Pathlock SAP Cyber Defense needs two technical users to run. Please create: <ul style="list-style-type: none">- PL_BTC- PL_<SID>_RFC The name can be adapted; however, the guide is referencing to these users.						
Step 4 Assign the following roles to the users: PL_BTC /SAST/CQA_BTC PL_<SID>_RFC /SAST/CQA_RFC	Step 5 Pathlock is using RFC communication to minimize authorizations required for the end users. The following RFCs need to be configured: SAST_BE_RFC <ul style="list-style-type: none">- No user (option current user)- Points to the system itself SAST_<SID>_CORE <ul style="list-style-type: none">- PL_<SID>_RFC user- Points to the system itself	Step 6 Go to transaction SICF and activate the following services. If there is a *, please activate the whole node. Pathlock Unique: /default_host/sap/opu/odata/sast/* /default_host/sap/bc/ui5_ui5/sast/* General Services: /default_host/sap/bc/ui2/app_index /default_host/sap/bc/lrep /default_host/sap/bc/vbi /default_host/sap/public/bc/ur /default_host/sap/public/bc/ui2 /default_host/sap/public/bc/ui5_ui5* /default_host/sap/public/bc/icf/logoff /default_host/sap/bc/ui2/start_up /default_host/sap/public/bc/bsp						
Step 7 Activate the gateway via transaction SPRO. This is only required if you are not working with any gateway applications. SPRO / SAP Customizing Implementation Guide / SAP NetWeaver / SAP Gateway / OData Channel / Configuration / Activate or Deactivate SAP NetWeaver / Gateway Activate the OData Service Gateways	Step 8 Go to transaction /IWFND/MAINT_SERVICE and check if all /SAST/ASC* services are active. They are active as soon as the ICF note entry is green and the system alias is maintained. There should be nothing to do. If there is something missing, please activate the ICF note and add the system alias SAST_BE to the service.	Step 9 Create a Pathlock Code Scanning ATC variant. Open transaction SCI. In area "Check Variant" switch the button before the input to global variant and create than the variant PL_SCAN  Click on create and check the below entries <table><tr><td><input checked="" type="checkbox"/></td><td></td><td>Pathlock - Code Scanning</td></tr><tr><td><input checked="" type="checkbox"/></td><td></td><td>Pathlock - CS - Checks</td></tr></table> Save it.	<input checked="" type="checkbox"/>		Pathlock - Code Scanning	<input checked="" type="checkbox"/>		Pathlock - CS - Checks
<input checked="" type="checkbox"/>		Pathlock - Code Scanning						
<input checked="" type="checkbox"/>		Pathlock - CS - Checks						

**Step 10**

Assign yourself role
/SAST/BE_CQA

Step 11

The report
/SAST/CC_SYNCHRONISE_SY
STEMS should be scheduled
as background job.

Recommendations are
Every 15-30 min*
Step User: PL_BTC

This report collects
metadata (such as
responsible user) required
for code scanning findings.

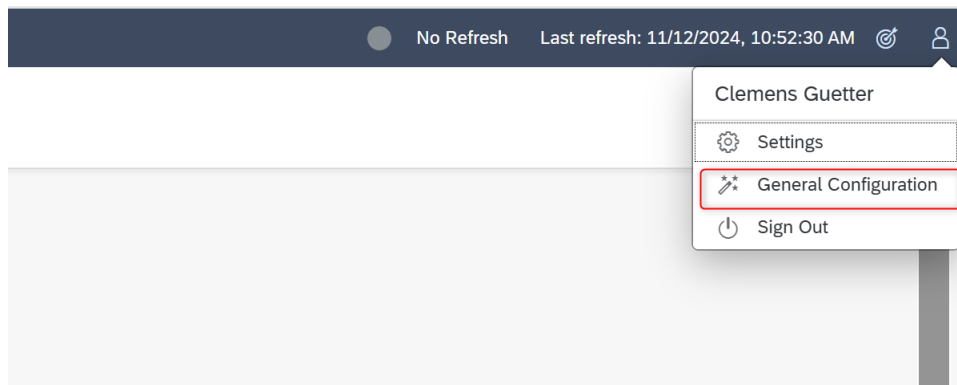
*For this quick assessment
you only need to execute it
once the assessment has
been completed.

You have now successfully installed Pathlock
Quick Assessment!

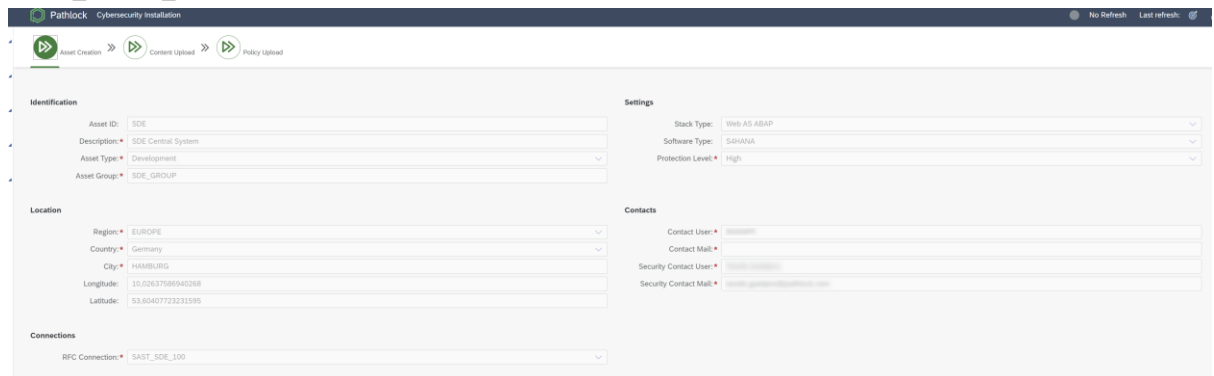


Assess Your System

1. Open Transaction /SAST/CAC
2. Open the General Configuration



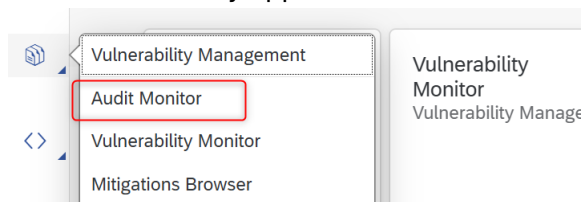
3. Create your system, example like this. After creating, it cannot be changed anymore in this free version. Please use as RFC connection the created connection SAST_<SID>_CORE.



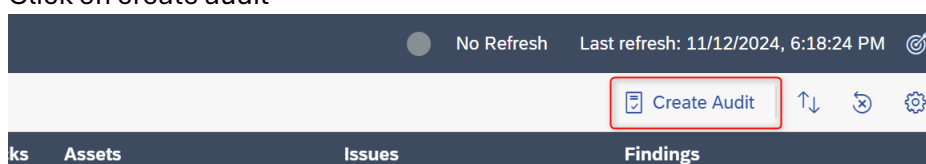
4. Upload via drag and drop the content and the policy. After uploading it should be green



- In content tab, the text file PATHLOCK_CONTENT* needs to be drag and dropped + submitted.
 - In policy tab, the XML file PATHLOCK_POLICY* needs to be drag and dropped + submitted.
5. Create first assessment
 - Go to Vulnerability Application



- Click on create audit





Now we can create the audit assessment. Below you can find the step by step guide through the wizard. With example inputs.

Create Audit

1 Administration 2 Scope Selection 3 Frequency Configuration 4 Asset Selection 5 Review

1. Administration

Start by setting up the basic details of your vulnerability audit assessment. Assign a unique identifier (Audit ID) to easily track this audit. Specify the individual or team responsible for conducting the audit, ensuring accountability. Additionally, categorize the audit by assigning relevant tags to help organize and filter assessments based on various criteria.

Identification

Audit ID: MY_ASSESSMENT

Description: My first Assessment

Tags:

Responsible

User: MYUSER

Mail: my_mail@my_company.com

Notification

External Mail: ☒

Audit Cycle Start Mail: ☒

Audit Cycle End Mail: ☒

[Next Step](#) [Cancel](#)

Create Audit

1 Administration 2 Scope Selection 3 Frequency Configuration 4 Asset Selection 5 Review

2. Scope Selection

Define the scope of your vulnerability audit assessment by selecting an appropriate policy. This policy will include all the checks that are part of the audit. Once a policy is chosen, you will see the specific check areas it covers. Additionally, you have the option to exclude all manual checks by toggling the switch.

Source

Policy ID: PATHLOCK

Orglevel ID: NONE

Checks

Technical System Parameters: ☒

Single Critical Authorization: ☒

Segregation Of Duty Conflicts: ☒

Organization And Documentation: ☒

Role Quality: ☐

Limitation

Exclude Manual Checks: ☐

[Previous Step](#) [Next Step](#) [Cancel](#)



Create Audit

1 Administration 2 Scope Selection 3 Frequency Configuration 4 Asset Selection 5 Review

3. Frequency Configuration

In this step, you will configure the frequency and execution settings for the audit.
For frequency, you can define a schedule (None, Daily, Weekly, etc.). If a schedule is set, you must also specify the start date and time in UTC.
For execution, you need to select the background user that will be used for processing. You can also choose whether to execute the assessment immediately after creation for the first time.

Frequency

Interval:

Start Date:

Start Time:

Execution

User:

Execute After Creation: ☒

Previous Step Review Cancel

Create Audit

1 Administration 2 Scope Selection 3 Frequency Configuration 4 Asset Selection 5 Review

4. Asset Selection

Specify the technical scope of your vulnerability audit assessment by assigning any number of assets where the audit should be executed. Additionally, you have the option to choose variants to further restrict the scope of the assessment if needed. Therefore, use variants with caution. For more details on variants, please refer to the manual.

[Add Asset](#)

Asset ID	Contact	Security Contact	Asset Tags
SDE Development	<input type="text" value=""/>	<input type="text" value=""/>	<div>Assets Prod COA All Security Threat TEST RK Dec</div>

Previous Step Review Cancel

Now review, finish, and complete the wizard.

After a few minutes, it really depends on the size of your system and the amount of custom code available, you should have the results of the assessment. You can expect a duration of 15-30 minutes, but sometimes it takes more than 1 hour to complete.

Now you have the first assessment done. You can now start to explore our application. If you want to know more about it, please get in touch with your Pathlock representative.