

Pathlock Quick Installation Guide

Vulnerability Management and Code Scanning



Contents

Introduction.....	3
Prerequisites	3
Installation	4
Assess Your System	6
Frequently Asked Questions.....	12
Upload of Policy is not working.....	12
Upload of Roles in PFCG shows warnings.....	12



Introduction

Welcome to the Quick Installation Guide for Pathlock's SAP Cyber Defense Application (light version). 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 a colleague) have the required 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

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

For a quick assessment, the minimum requirements are as follows

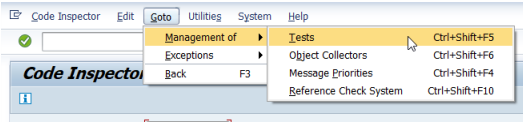
- SAP_BASIS 7.40 SP09
- SAP_GWFND 7.40 SP9
- SAP_UI 7.54 SP8

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 files according to the instructions provided in the package. You are done as soon as everything is completely implemented into your system.	Step 2 Open transaction SUPC and generate profiles for all roles starting with /SAST/*. 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/LIGHT_BTC PL_<SID>_RFC /SAST/LIGHT_RFC	Step 5 Pathlock is using RFC communication to minimize authorizations required for the end users. The following RFC needs to be configured: <ul style="list-style-type: none">- Name: SAST_<SID>_CORE- User: PL_<SID>_RFC user- Target: Points to the system itself	Step 6 Open transaction SICF and activate the following services. For any paths ending with *, activate the full node. Pathlock Specific: /default_host/sap/opu/odata/sast/* /default_host/sap/bc/ui5_ui5/sast/* General SAP Services: /default_host/sap/bc/ui2/app_index /default_host/sap/bc/ui2/start_up /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/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 Gateway Activate the OData Service Gateways	Step 8 Open 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 Activate Pathlock Code Scanning Tests in ATC. Open transaction SCI . Go to “Goto → Management of → Test” in SAP menu  Select the following check classes in the exact order and save after each selection: 1. /SAST/CODE_CHECK_SAST 2. /SAST/CODE_CHECK_GEN 3. /SAST/CC_GEN_CHECK <table><thead><tr><th>Check Class</th><th>Info</th><th>Description</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/> /SAST/CC_GEN_CHECK</td><td></td><td>Pathlock - CS - Generic Code Check</td></tr><tr><td><input checked="" type="checkbox"/> /SAST/CODE_CHECK_GEN</td><td></td><td>Pathlock - CS - Checks</td></tr><tr><td><input checked="" type="checkbox"/> /SAST/CODE_CHECK_SAST</td><td></td><td>Pathlock - Code Scanning</td></tr><tr><td><input checked="" type="checkbox"/> CL_ACI_CI_TEST_VS_SYNTAX_CHECK</td><td></td><td>ACI test: compare ACI with SYNTAX-CHECK results</td></tr><tr><td><input type="checkbox"/> CL_CHW_EHR_CONFLICTS</td><td></td><td>ENBAUENMENT-SECTION Tests</td></tr><tr><td><input checked="" type="checkbox"/> CL_CI_CATEGORY_ABAP_COMPILER</td><td></td><td>Syntax Check/Generation</td></tr></tbody></table>	Check Class	Info	Description	<input checked="" type="checkbox"/> /SAST/CC_GEN_CHECK		Pathlock - CS - Generic Code Check	<input checked="" type="checkbox"/> /SAST/CODE_CHECK_GEN		Pathlock - CS - Checks	<input checked="" type="checkbox"/> /SAST/CODE_CHECK_SAST		Pathlock - Code Scanning	<input checked="" type="checkbox"/> CL_ACI_CI_TEST_VS_SYNTAX_CHECK		ACI test: compare ACI with SYNTAX-CHECK results	<input type="checkbox"/> CL_CHW_EHR_CONFLICTS		ENBAUENMENT-SECTION Tests	<input checked="" type="checkbox"/> CL_CI_CATEGORY_ABAP_COMPILER		Syntax Check/Generation
Check Class	Info	Description																					
<input checked="" type="checkbox"/> /SAST/CC_GEN_CHECK		Pathlock - CS - Generic Code Check																					
<input checked="" type="checkbox"/> /SAST/CODE_CHECK_GEN		Pathlock - CS - Checks																					
<input checked="" type="checkbox"/> /SAST/CODE_CHECK_SAST		Pathlock - Code Scanning																					
<input checked="" type="checkbox"/> CL_ACI_CI_TEST_VS_SYNTAX_CHECK		ACI test: compare ACI with SYNTAX-CHECK results																					
<input type="checkbox"/> CL_CHW_EHR_CONFLICTS		ENBAUENMENT-SECTION Tests																					
<input checked="" type="checkbox"/> CL_CI_CATEGORY_ABAP_COMPILER		Syntax Check/Generation																					

**Step 10**

Assign yourself role /SAST/BE_CQA to your user.

Step 11

The report /SAST/CC_SYNCHRONISE_SYSTEMS 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.

Step 12

The report /SAST/VM_AUDIT_COLLECT should be scheduled as background job.

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

This report collects all audit results. Only after execution, an audit assessment can be finalized.

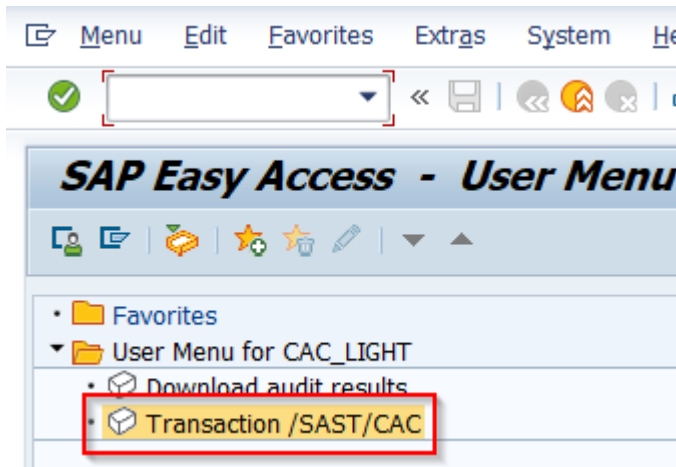
*For this quick assessment you only need to execute it once the assessment has been completed.

You have now successfully installed Pathlock Quick Assessment!

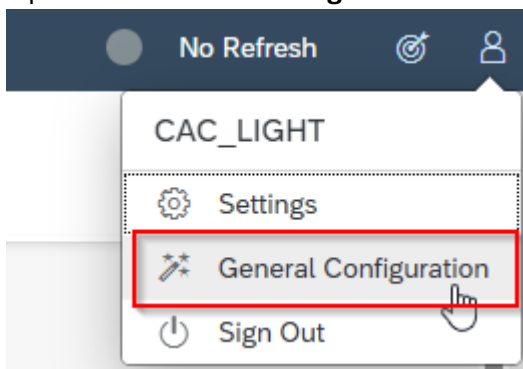


Assess Your System

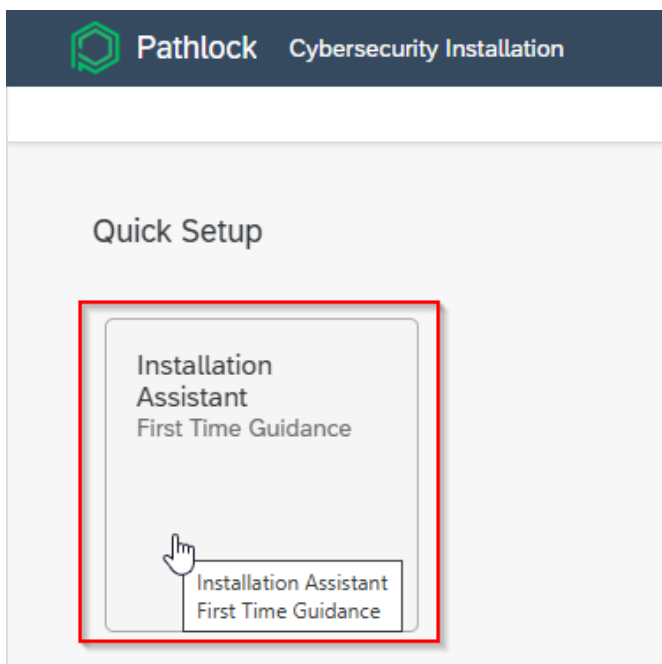
1. Open your SAP system with your user with assigned role /SAST/BE_CQA (s. step 10) and open Transaction **/SAST/CAC**



2. Open the **"General Configuration"**



3. Click on **"Installation Assistant"** tile





4. Create your system and use as RFC connection the created connection **SAST_<SID>_CORE** (s. step 5) like in this example and click on submit.

Note: After creating, it cannot be changed anymore in this free version. Please use as RFC connection the created connection SAST_<SID>_CORE.

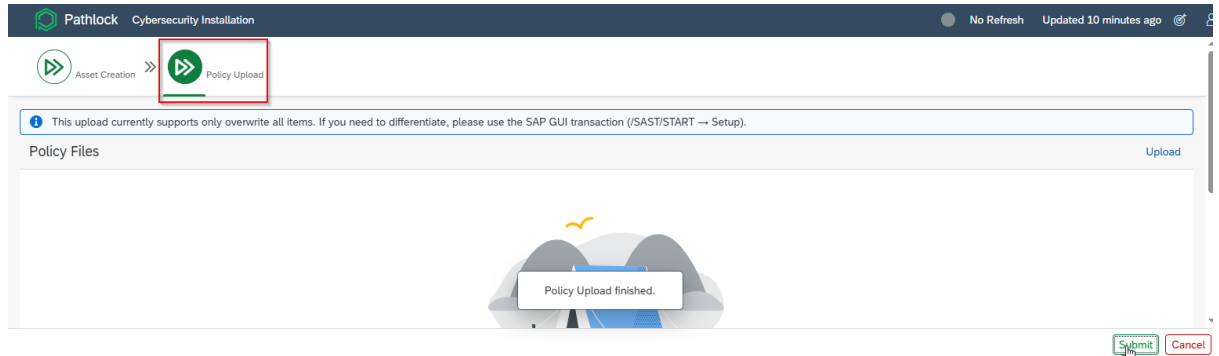
The screenshot shows the 'Asset Creation' form in the Pathlock Cybersecurity Installation interface. The form is divided into several sections: Identification, Location, Settings, Contacts, and Connections. The 'Identification' section includes fields for Asset ID (YS3), Description (YS3 Central System), Asset Type (Development), and Asset Group (YS3_GROUP). The 'Location' section includes fields for Region (EUROPE), Country (Germany), City (Hamburg), Longitude (9.763017211), and Latitude (53.5586627). The 'Settings' section includes fields for Stack Type (Web AS ABAP), Software Type (SAP Netweaver ABAP), and Protection Level (Very high). The 'Contacts' section includes fields for Contact User (T), Contact Mail (tr), Security Contact User (T), and Security Contact Mail (tr). The 'Connections' section includes a dropdown for RFC Connection (SAST_YS3_CORE). At the bottom right, there are 'Submit' and 'Cancel' buttons.

5. Click on next step “**Policy Upload**”, deposit the policy (XML file PATHLOCK_POLICY*) via drag and drop, check check box for policy file and click on “Submit”.

The screenshot shows the 'Policy Upload' form in the Pathlock Cybersecurity Installation interface. The form is divided into several sections: Policy Files, Upload, and Pending. The 'Policy Files' section includes a message: 'This upload currently supports only overwrite all items. If you need to differentiate, please use the SAP GUI transaction (/SAST/START → Setup)'. The 'Upload' section includes a large area with a 'Drop files here' message and a 'You can also upload several files all at once.' message. The 'Pending' section includes a table with one row: PATHLOCK_POLICY_2025Q2.XML, with a 'Pending' status and a progress bar showing 0%. At the bottom right, there are 'Submit' and 'Cancel' buttons.



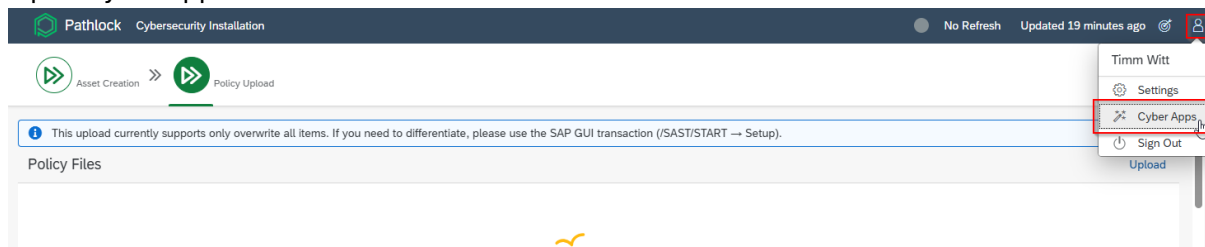
Please check if the symbol next to the policy upload turns green. If it does not, the upload was unsuccessful. In that case, refer to the instructions in the FAQ section “Upload of Policy is not working”.



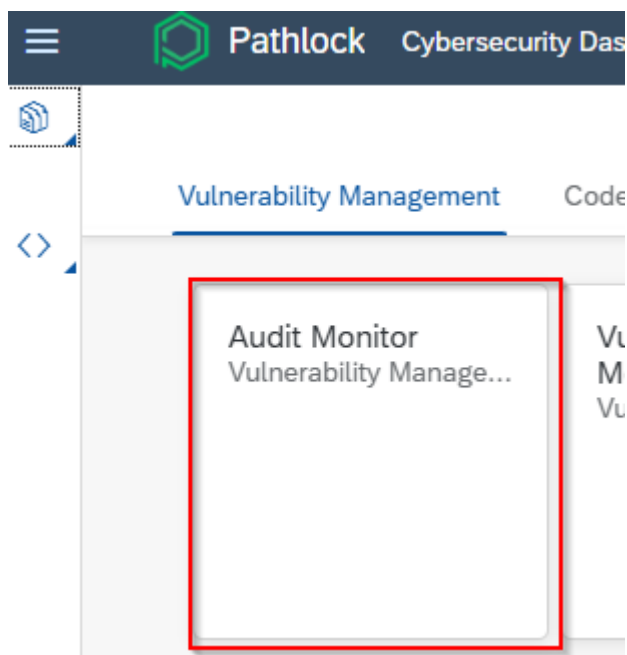
Note: So that the policy can be used in the following please reload the page (F5)

6. Create first assessment

- Open Cyber Apps

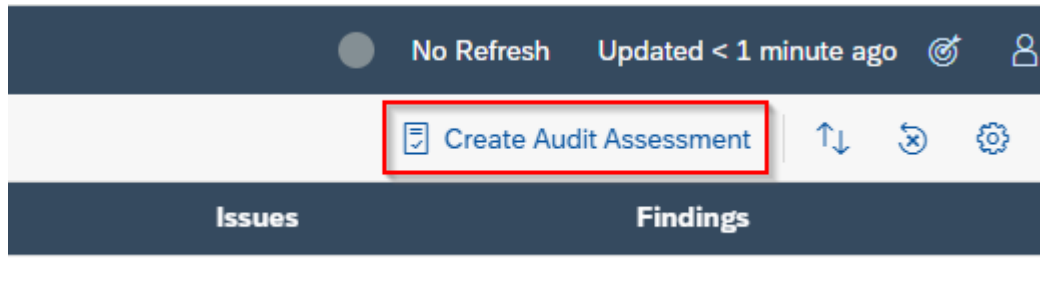


- Go to “Audit Monitor”





- Click on “Create Audit Assessment”



Now the audit assessment can be created. Below you can find the step-by-step guide through the wizard. With example inputs.

Create Audit Assessment

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: * FIRST_ASSESSMENT

Description: * Assessment for System YS3

Tags:

Responsible

User: * CAC_LIGHT

Mail: * CAC_LIGHT@company.com

Notification

External Mail:

Audit Cycle Start Mail:

Audit Cycle End Mail:

Next Step

Cancel



Create Audit Assessment

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_LIGHT

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: * None

Start Date: *

Start Time: *

Execution

User: * PL_BTC

Execute After Creation: ☒

Previous Step **Review** Cancel





Create Audit Assessment

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
YS3 (ABAP) Development	 TEST test@test.de	TEST test@test.de	

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

Now review, finish, and complete the wizard.

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

Please note: In order for the results to be displayed, the **Collector Job must have run**. As described in Step 12 of the documentation, this job needs to be either **scheduled via job** or **triggered manually**.

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



Frequently Asked Questions

Upload of Policy is not working

If the upload of the policy file is not working, please verify the virus scan configuration:

1. Open transaction **/IWFND/VIRUS_SCAN** in your SAP system.
2. Check the current configuration of the virus scan settings:
 - **If nothing is configured**, the virus scan should be **disabled**.
 - **If the virus scan is configured**, you need to either **disable it** or **adjust the configuration** to allow file uploads.

If the virus scan is not properly configured or disabled, the system will block all file uploads by default. Ensuring the correct setup here will allow the upload process to complete successfully.

Upload of Roles in PFCG shows warnings

If you upload the roles file in PFCG, you might get a warning “Invalid services (USOBHASH entry missing)” depending on your SAP version.

The warning is triggered because the roles were created on a higher SAP version where the corresponding services exist.

This warning can be ignored as the missing entries have no functional impact as they are not required for your SAP release.