

The Fortified Watchtower

How to Set up Checkmk Securely



Ralf Spenneberg
CEO, OpenSource Security GmbH

OpenSource Security



Who am I?

Ralf Spenneberg

- Checkmk Gold and Training Partner since 2013
- Strong Security Background

Customers



Security goals of this talk



Authentication

Security begins with authentication



Software Deployment

Our bakery is a software deployment system



Network Isolation

Network isolation is good practice



Updates

Only Updates fix found vulnerabilities!

Authentication



Authentication

Security begins with authentication



Software Deployment

Our bakery is a software deployment system



Network Isolation

Network isolation is good practice



Updates

Only Updates fix found vulnerabilities!

What do you need for good authentication?



Single-Sign On



SAML

What do you need for good authentication?



Single-Sign On



SAML



Open Source Identity and
Access Management



User Federation (LDAP/AD)



Clustering

The road to Single-Sign-On



**Connect Checkmk
to Keycloak**

**Configure
Keycloak**

**Enforce
Policies**

Single-Sign-On in Checkmk



Login with SAML Connection to Keycloak

or

Username:

Password:

Login

© Checkmk GmbH

Single-Sign-On in Checkmk



Login with SAML Connection to Keycloak

or

Username:

Password:

Login



TLS secured access



SAML endpoints must have been registered with Keycloak

© Checkmk GmbH

Connecting Checkmk to Keycloak



Checkmk service provider metadata (generated automatically)

| | |
|---|---|
| Entity ID | https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py |
| Metadata endpoint | https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py?RelayState=saml |
| Assertion Consumer Service endpoint | https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_acs.py?acs |

Connection

| | |
|---|---|
| Identity provider metadata (required) | URL |
| | https://keycloak.conf12.nohup.info/realms/checkmk_realm/protocol/saml/descriptor |
| Checkmk server URL (required) | https://checkmk.conf12.nohup.info |
| Identity provider connection timeout | Connection timeout <input type="text" value="12"/> seconds |
| | Read timeout <input type="text" value="12"/> seconds |

Keycloak client configuration



Clients > Client details

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py

Clients are applications and services that can request authentication of a user.

Settings

Keys

Credentials

Roles

Client scopes

Sessions

Advanced

Events

General settings

Client ID * ⓘ

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py

Name ⓘ

Checkmk Server

Signature and encryption



Signature and Encryption

Sign documents  On

Sign assertions  On

Signature algorithm 

SAML signature key name 

Canonicalization method 

Metadata descriptor URL 

Use metadata descriptor URL  On



Mapping access attributes

Client Scope

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py-dedicated

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope

Search for mapper



Add mapper

Refresh

| Name | Category | Type |
|------------|---------------------------|----------------|
| group | Group Mapper | Group list |
| username | AttributeStatement Mapper | User Attribute |
| X500 email | AttributeStatement Mapper | User Property |

Mapping access attributes

Client Scope

Username

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py-dedicated

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope

Search for mapper



Add mapper ▾

Refresh

| Name | Category | Type |
|------------|---------------------------|----------------|
| group | Group Mapper | Group list |
| username | AttributeStatement Mapper | User Attribute |
| X500 email | AttributeStatement Mapper | User Property |



Mapping access attributes

Client Scope

Username

Groups

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py-dedicated

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope

Search for mapper



Add mapper

Refresh

| Name | Category | Type |
|------------|---------------------------|----------------|
| group | Group Mapper | Group list |
| username | AttributeStatement Mapper | User Attribute |
| X500 email | AttributeStatement Mapper | User Property |



Mapping access attributes

Client Scope

Username

Groups

E-mail

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py-dedicated

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope

Search for mapper



Add mapper

Refresh

| Name | Category | Type |
|------------|---------------------------|----------------|
| group | Group Mapper | Group list |
| username | AttributeStatement Mapper | User Attribute |
| X500 email | AttributeStatement Mapper | User Property |



Mapping access attributes

Client Scope

Username

Groups

E-mail

Complex Mappers via Javascript

https://checkmk.conf12.nohup.info/keycloak/check_mk/saml_metadata.py-dedicated

This is a client scope which includes the dedicated mappers and scope

Mappers

Scope

Search for mapper



Add mapper

Refresh

| Name | Category | Type |
|------------|---------------------------|----------------|
| group | Group Mapper | Group list |
| username | AttributeStatement Mapper | User Attribute |
| X500 email | AttributeStatement Mapper | User Property |

Enforce global MFA with Keycloak

Per realm or user

Users > User details

ralf

Details | Attributes | Credentials | Role mapping | Groups | Consents

ID * 59f4c377-1f1e-40f4-be22-d6ef45585aa3

Created at * 4/19/2026, 1:40:21 PM

Required user actions ?

Configure OTP × | Select action

Configure OTP

Update Password

Update Profile


Email verified ?

CHECKMK REALM

Mobile Authenticator Setup

You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
 - Microsoft Authenticator
 - FreeOTP
 - Google Authenticator
2. Open the application and scan the barcode:



Unable to scan?

Troubleshooting with SAML Tracer browser plugin



The screenshot shows the SAML-tracer browser plugin interface. The top bar includes controls like 'Clear', 'Pause', 'Autoscroll', 'Hide resources', 'Show protocol requests only', 'Colorize', 'Export', and 'Import'. Below this is a list of HTTP requests. One request is highlighted in blue, and its details are shown in a modal window below. The modal window displays the request parameters and the SAML 2.0 Assertion content.

HTTP Parameters:

| | |
|------------------------------|-------------------|
| member | admin |
| username | ralf |
| urn:oid:1.2.840.113549.1.9.1 | ralf@os-s.de |
| Role | uma_authorization |

SAML 2.0 Assertion:

```

ID ID_22426056-f674-4d2e-89e2-a13da6f62891
Version 2.0
IssueInstant 2026-05-20T10:43:30.723Z
Subject ralf
  -SAML 2.0 AttributeStatement
    member admin
    username ralf
    urn:oid:1.2.840.113549.1.9.1 ralf@os-s.de
    Role uma_authorization
    Role manage-account

```

Software deployment



Authentication

Security begins with authentication



Software Deployment

Our bakery is a software deployment system



Network Isolation

Network isolation is good practice



Updates

Only Updates fix found vulnerabilities!

Bakery

Great for supply chain attacks!

Automated

Software deployment



Successful attacks
are catastrophic

Bakery

Great for supply chain attacks!

Automated

Software deployment



Successful attacks
are catastrophic



You are responsible for the integrity of the agent package!



Signing only protects these files during storage and for the transport over the network.



The files used to build the agent are not protected.

Hardening the Bakery



Harden the CMK Server

Console Access

- Root only for Updates
 - Use site user

Web Access

- SSO and MFA
 - Ensure trusted users

Checkmk

Bakery

- Non-root agent
- Separate signature keys
- HTTPS

Additional

- Monitor ~/local and MKPs
- File Integrity Monitor

Network isolation



Authentication

Security begins with authentication



Software Deployment

Our bakery is a software deployment system



Network Isolation

Network isolation is good practice



Updates

Only Updates fix found vulnerabilities!

Network isolation



VLANs

Put Servers on
separate VLANs

Network isolation



VLANs

Put Servers on
separate VLANs



Users

Restrict the
synced Users

Remove the automation
user if not needed

Network isolation



VLANs

Put Servers on
separate VLANs



Users

Restrict the
synced Users

Remove the automation
user if not needed



Connections

Central to Remote
(Livestatus, Distributed
Setup, MQTT etc.)

Remote to Central
(Agent Bakery)

Use TLS

Updates



Authentication

Security begins with authentication



Software Deployment

Our bakery is a software deployment system



Network Isolation

Network isolation is good practice



Updates

Only Updates fix found vulnerabilities!

Checkmk vulnerabilities



33 CVEs

2024

1 high (CVSS 4.0)

23 CVEs

2025

5 high (CVSS 4.0)

14 CVEs

2026

6 high (CVSS 4.0)

Install updates !

- https://thl-cmk.hopto.org/checkmk/checkmk/checkmk_update
- Risk based prioritization
 - Known Exploit Vulnerability (KEV)
 - Exploitability (EPSS)
 - Exploit Prediction Scoring System (EPSS) is a data-driven machine-learning model that estimates the probability that a published CVE will be exploited in the wild in the next 30 days
- Contextual analysis
 - Feature used?

CVE-2026-33276 - XSS in Unified Search via Unescaped Host/Service Names

Description

Stored cross-site scripting (XSS) in Checkmk 2.5.0 (beta) before 2.5.0b2 allows authenticated users with permission to create hosts or services to execute arbitrary JavaScript in the browsers of other users performing searches in the Unified Search feature.

PUBLISHED: 2026-03-31

SCORE: **8.6 High**

EPSS: **< 1% Very Low**

KEV: **No**

IMPACT: Stored Cross-Site ...

ACTION: Immediate Patch

Goals accomplished



Authentication

Security begins with authentication



Software Deployment

Our bakery is a software deployment system



Network Isolation

Network isolation is good practice



Updates

Only Updates fix found vulnerabilities!



Checkmk #12

Conference