Unify OpenScape 4000 Assistant V11

Release Notes

Software Version: V11 R0.22.2

2024-07-04

☐ Major Release ☐ Minor Release ☐ Fix Release ☒ Hotfix Release

Current release status can be verified via the Software Supply Server (SWS)

Deliverables

☐ Full Release ☒ Delta Release

Export Control Classification Data

AL: 5D002C1A ECCN: 5D002ENCR

Release Notes Version: V1.0

About this document

This document provides general information about the release, generics, and other relevant notes for the corresponding product and its correction versions.

NOTICE

Unify OpenScape 4000 Assistant
2024-07-04

Delivered Files

Product Item Number		File Name
1	P30152-P1698-U1-1	ADP-V11_R0.22.**2**.tar
2		
3		

Table of Contents

1. History of Change

1.1. Release Notes content

Version	Date	Description of changes
1.0	2024-07-04	Initial creation

1.2. Product versions history

Software Version	Production Version	Date	Remarks
V11 R0.22.0	V11 R0.22.0 - OS4K RLC Upgrade Package (ASS V11 R0.22.0, CSTA V11 R0.22.0, PLT R0.22.0, MGR V11 R0.22.0)	2024-03-01	

Note: List of all released software versions since [major] or [minor] software release in SWS

2. Changes

2.1. Implemented Change Requests / New features

Not applicable for this release

Tracking Reference	Internal Reference	Summary	Released in Version

2.2. Resolved Reported Problems / Symptoms

Tracking Reference	Internal Reference	Summary	Released in Version
		For details see attached "RN_OS4K_Ass-HF_V11-R0_22_2.xlsx" from Nuxeo.	

2.3. Resolved Vulnerabilities

Not applicable for this release

Tracking Reference	Internal Reference	Severity Level	Summary	Released in Version
PRB00007 6444	OSFOURK-27432	Critical, CVSS 9.8	An OS command injection vulnerability that may allow an unauthenticated attacker to upload arbitrary files and get administrative access to the system. [1)]	V11 R0.22.2
PRB00007 6507	OSFOURK-27450	Critical, CVSS 9.8	An OS command injection vulnerability that may allow an unauthenticated attacker to upload arbitrary files and get administrative access to the system. [1)]	V11 R0.22.2

1) We'd like to thank DB Systel for disclosing and supporting us to remediate the issue

Note: It is strongly recommended applying the fix version if it includes resolved vulnerabilities.

3. Important Issues, Workarounds, Hints and Restrictions

This section provides the latest information at time of software release and is only pertaining to the time of release notes generation.

3.1. Important Issues

Not applicable for this release

Tracking Reference	Internal Reference	Summary	Workaround / Actions

3.2. Workarounds, Hints

Not applicable for this release

Tracking Reference	Internal Reference	Summary	Workaround / Actions

3.3. Restrictions

Not applicable for this release

Tracking Reference	Internal Reference	Summary	Workaround / Actions

4. Installation and Upgrade / Update

4.1. Installation

4.1.1. Data and Information Security

It is mandatory to apply the Security Checklist so that system default settings are hardened according to best practices. This is most relevant after a first installation, but also strongly recommended after each Major or Minor version upgrade. It presents a checklist to ensure all necessary installation and configuration steps can be taken and adapted to the individual customer's environment and security policy. Deviations from the standard settings should be documented in the security checklist in consultation with the customer's contact person.

The best possible standard of data security and protection is only provided on our latest solutions or product versions. It is recommended to regularly install product updates in order to remove identified security vulnerabilities and software defects, improve stability and add latest functionality.

Country-specific regulations must be observed.

The latest version of the V11 checklist can be found under the following link:

https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/a4aeeade-3b77-4a59-80b1-1304a0acd5ee

4.2. Upgrade / Update / Migration

The precondition for the activation of Hotfix is the V11 R0.22.0.

The hotfix is transferred by means of SWM and activated using SWA.

4.2.1. Fallback

As fallback scenario always takes a full DATA backup on external storage (e.g. sftp server) with the earlier version.

4.3. Special settings and instructions

Not applicable for this release

5. Hardware and Software Compatibility

5.1. Hardware

Assistant is running as Virtual Appliance on OpenScape 4000 host machine, therefore no HW requirements for Assistant apply. HW requirements of the Linux host are described in the OpenScape 4000 V11 Switch Release Note.

5.2. Firmware

Not applicable for this release

5.3. Loadware

Not applicable for this release

5.4. Software / Applications

Not applicable for this release

5.5. Operating systems

5.5.1 Client requirements

Please refer to “Assistant Online Client Preparation” for getting the info about the latest supported client platforms.

These notes have the information about the latest supported Operating System, Browser and JRE Versions of a Client PC when this document was released.

The official Unify communication regarding “Java Licensing Requirements” can be found under the following Wiki link: https://wiki.unify.com/wiki/Product_Java_Dependencies_Overview

4K System Release	Assistant/Manager Version	Operating System	Browser Version	Released JRE Versions
V10 R1 V11 R0	V10 R1 V11 R0	Windows 10, 11 and Windows Server 2016, 2019	Edge, Chrome and Firefox are supported browsers. IE might still work with JNLP but no support is offered.	OpenWebStart application (delivered as part of Assistant) is used to run Assistant applications, like CM. The formerly required JRE8 isn't needed anymore
To ensure protection against the latest security vulnerabilities it is always recommended to use the most current System/Assistant version and corresponding HF				
Note 1: Windows 32-bit clients are not supported anymore.				

5.6. Compliant products

This section lists the versions associated with the communication platforms, other products and third-party products that have been tested for use with this version of the product and are known to work.

5.6.1. Communication platforms

Hardware and software products that have been tested together with this version of the product are listed in the common compatibility matrix, which also includes the respective versions required to use with the current version of this product.

The current Common Compatibility Matrix can be found on the Unify Partner Portal https://unify.com/en/partners/partner-portal under Sell - Portfolio Information.

Note: Use the "Search & Find" option under Portfolio Information and Search Documentation for "Common Compatibility Matrix" (search on title only!).

5.6.2. Other products

(if nothing please insert "Not applicable for this release")

5.6.3. Third-Party products

(if nothing please insert "Not applicable for this release")

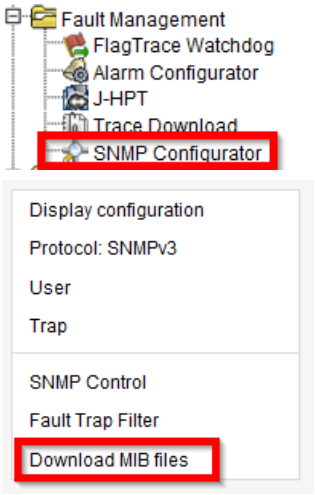
6. Service Information

6.1. Management information base

☒ Product sends SNMP V2 traps ☒ Product sends SNMP V3 traps ☐ Not supported

MIB Documents can be reach via Manager GUI. Steps for MIB files;

Fault Management SNMP Configurator Download MIB files



6.2. License management

This product is licensed using:

☒ CLS ☐ CSC ☐ Other or not relevant, as described below.

6.3. Remote serviceability

This product is certified for the following:

☒ RSP ☒ HiSPA/SIRA ☐ RTPatch ☐ Other remote access or not relevant, as described below.

6.4. Product tooling structure

Main Category	Communication Systems
Product Family	OpenScape 4000
Product	OpenScape 4000
Product Version	OpenScape 4000 V11
Product Item Number	**P30152-P1698-U1-1 (V11 R0.22.0)**

6.5. Case tracking system

Tickets can be generated and tracked via the WEB Support Portal (AWSP).

http://atosunify.service-now.com/unify

A short instruction can be found on the AWSP directly.

7. Documentation Reference

The product documentation can be found on the Unify Partner Portal https://unify.com/en/partners/partner-portal under Sell - Portfolio Information.

8. References

Not applicable for this release