



## Security Advisory Report - OBSO-1401-02

### Informational - Expiry of Default Root CA Certificate in OpenScape Solutions

Creation Date: 2014-01-28  
Last Update: 2014-01-28

#### Summary

On Feb 24, 2014 the default root CA certificate that is part of every initial installation of OpenScape Solution (V4 R1, V5, V6, V7 R1) reaches its end of validity.

TLS (Transport Layer Security) connections in test and demo installations of OpenScape Solution using the default root CA certificate will fail after that date. Detailed instructions are available to verify if a particular production system is affected.

#### Vulnerability Details

Starting Feb 24, 2014 TLS connections between different systems in an OpenScape Solution (such as SIP-TLS or https) will fail if they still rely on the default root CA certificate.

The default root CA certificate as delivered by OpenScape products is identical for all systems world-wide and should only be used for easy setup of test and demo installations. In production systems customer-individual certificates must be used instead.

However, there is evidence that the default certificates were not replaced in various customer installations; affected customers - where known - are already informed and appropriate configuration changes being made.

A comprehensive guide is available to verify if a particular customer deployment is affected.

Customers without their own PKI / certificate management in place may consider the use of a new OpenScape Voice Method of Procedure (MOP) to establish a customer-specific solution.

The MOP will be released for:

- V7 R1: MOP Q3031
- V6: MOP Q3030
- V5, V4 R1: in work

#### Affected Products

- All products in OpenScape solutions where TLS for SIP and/or for other connections (e.g. https or other TLS-protected communication links such as from OpenScape Mobile) is enabled and no individual certificate management is in place.

#### Recommended Actions

We recommend customers to review their installed base as soon as possible to ensure that no TLS links (e.g. TLS-SIP, https) are still relying on the certificate hierarchy that is delivered by default with every version of the OpenScape solution.

Turning off TLS (i.e. configuring SIP-TCP instead of SIP-TLS, http instead of https etc.) is not recommended as this would further downgrade the security posture of your solution, and is even not possible for certain solution elements (for example for the OpenScape Mobile single sign-on to OpenScape Voice and UC).

The service information listed in the references section provides all details regarding

- how to determine if a particular Voice/UC installation is affected
- how to migrate to a customer-specific certificate hierarchy

*In OpenScape solutions, where the expiring default root CA certificate is not used or where TLS-based communication links are not used at all, nothing needs to be done.*

In case of any questions contact your Service representative at Unify.

#### References

- [Unify Service Information INF-14-000135](#) (access via [Customer Support Portal](#))

## Revision History

2014-01-28: Initial release

---

Advisory ID: OBSO-1401-02 (a=71), status: general release

Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see <https://www.unify.com/security/advisories>.

### Contact and Disclaimer

OpenScape Baseline Security Office

[obso@unify.com](mailto:obso@unify.com)

© Unify Software and Solutions GmbH & Co. KG 2014

Mies-van-der-Rohe Str. 6, D-80807 München

[www.unify.com](http://www.unify.com)

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.