Unify OpenScape Composer

OpenScape Composer V2

Security Checklist
July 2024

A31003-X3020-P100-09-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Table of Content

History of Change

Date	Issue	Summary
10/2019	1.0	Initial Creation based on the security checklist OpenScape Composer V1
11/2021	2.0	DOCLOC-5163
05/2023	5.0	Documentation updates and enhancements
06/2023	6.0	Added Chapter 7.3 Transport Layer Security (TLS) Configurations
06/2023	7.0	Added security policy option NonTLS under 7.5 Communication Server/Managed Network
03/2024	8.0	Removed CIS references
07/2024	9.0	Rebranded to the Mitel layout

1 Introduction

1.1 General Remarks

Information and communication - and their seamless integration in “Unified Communica- tions and Collaboration” (UCC) - are important and valuable assets for an enterprise and are the core parts of their business processes. Therefore, they must be adequately pro- tected. Every enterprise can require a specific level of protection, which depends on indi- vidual requirements to availability, confidentiality, integrity and compliance of the used
IT and communication systems.

Unify attempts to provide a common standard of features and settings of security pa- rameters within the delivered products. Beyond this, we generally recommend

- to adapt these default settings to the needs of the individual customer and the specific characteristic of the solution to be deployed
- to outweigh the costs (of implementing security measures) against the risks (of omitting a security measure) and to “harden” the systems appropriately.

As a basis for that, the Security Checklists are published. They support the customer and the service in both direct and indirect channels, as well as self-maintainers, to agree on the settings and to document the decisions that are taken.
The Security Checklists can be used for two purposes:

1. **In the planning and design phase** of a particular customer project:
   Use the Security Checklists of every relevant product to evaluate, whether all products that make part of the solution can be aligned with the customer’s securi- ty requirements – and document in the Checklist, how they can be aligned.
   This ensures that security measures are appropriately considered and included in the Statement of Work to build the basis for the agreement between Unify and the customer: who will be responsible for the individual security measures:
   - During installation/setup of the solution
   - During operation
2. **During installation and during major enhancements or software upgrade activities:**
   The Security Checklists (ideally documented as described in step 1.) are used to apply and/or control the security settings of every individual product.

Update and Feedback

- By their nature, security-relevant topics are prone to continuous changes and up- dates. New findings, corrections and enhancements of this checklist are being includ- ed as soon as possible. Therefore, we recommend using always the latest version of the Security Checklists of the products that are part of your solution.
  They can be retrieved from the Unify support portal at the relevant product infor- mation site.

- We encourage you to provide feedback in any cases of unclarity, or problems with the application of this checklist.
  Please contact the OpenScape Baseline Security Office (Mitel Security Advisories).

1.2 Customer Deployment - Overview

This Security Checklist covers the product **OpenScape Composer** and lists its security relevant topics and settings in a comprehensive form.

	Customer	**Supplier**
Company Name Address Telephone E-Mail		
Covered Systems (for example, System, SW version, devices, MAC/IP-addresses)		
Referenced Master Security Checklist	Version: Date:	
General Remarks		
Open Issues to be solved until		
Date		

2 OpenScape Composer hardening measures in General

The OpenScape Composer is a system and network management platform designed as client-server application. The clients (either standalone Java application or browser-web- based) communicate with the server via network using HTTPS and WebSockets. The server itself communicates with the managed network elements using standard protocols like SOAP or via SSH (see Figure 1 Architectural Overview).

This security checklist focuses on the network communication paths of OpenScape Com- poser between the clients and the server and between the server and the managed net- work elements. The general risk in not securing these connections is the interception of access parameters like user names and passwords.

In general, the OpenScape Composer database itself contains no sensitive or confidential user data. However, intercepted passwords could be misused to get unauthorized access to other systems.

The recommended measures to prevent this are listed in the following chapters.

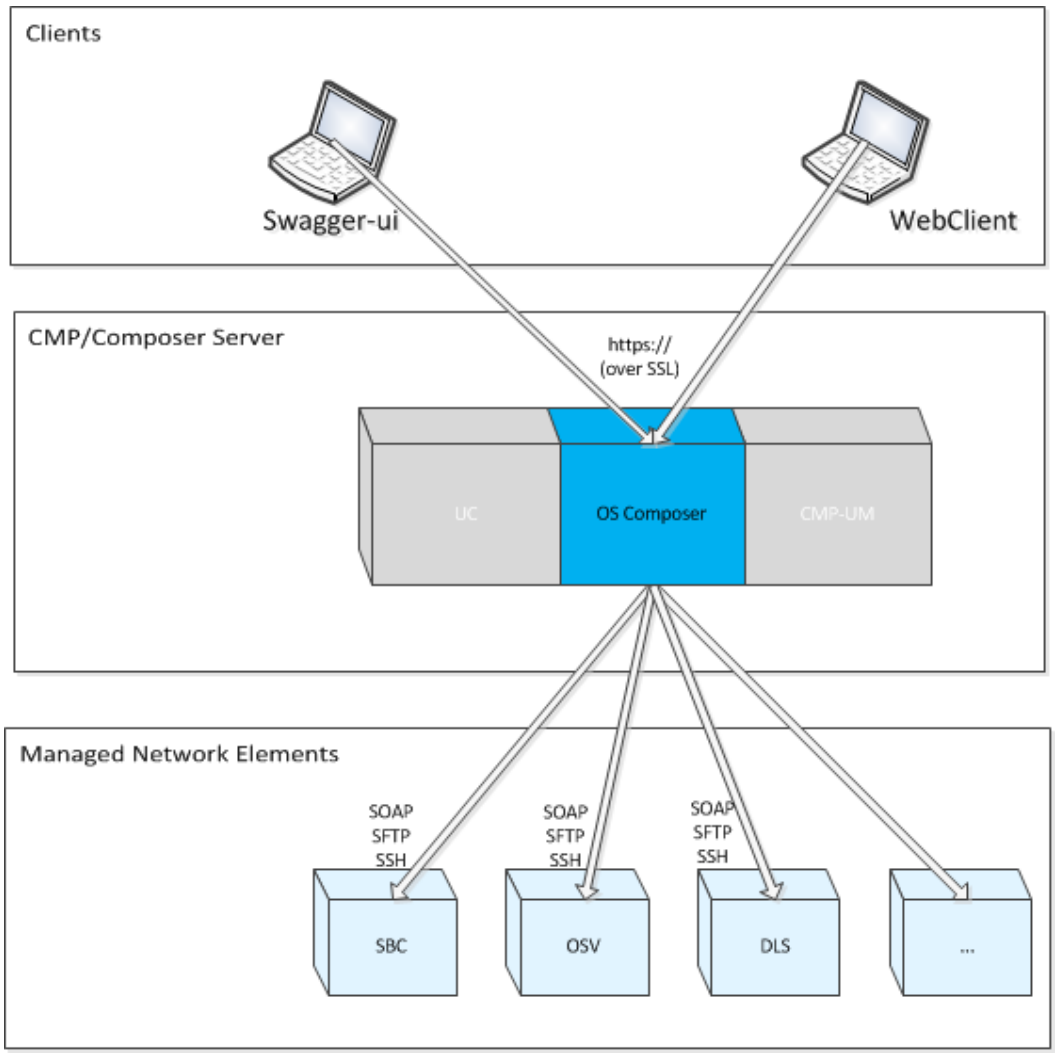
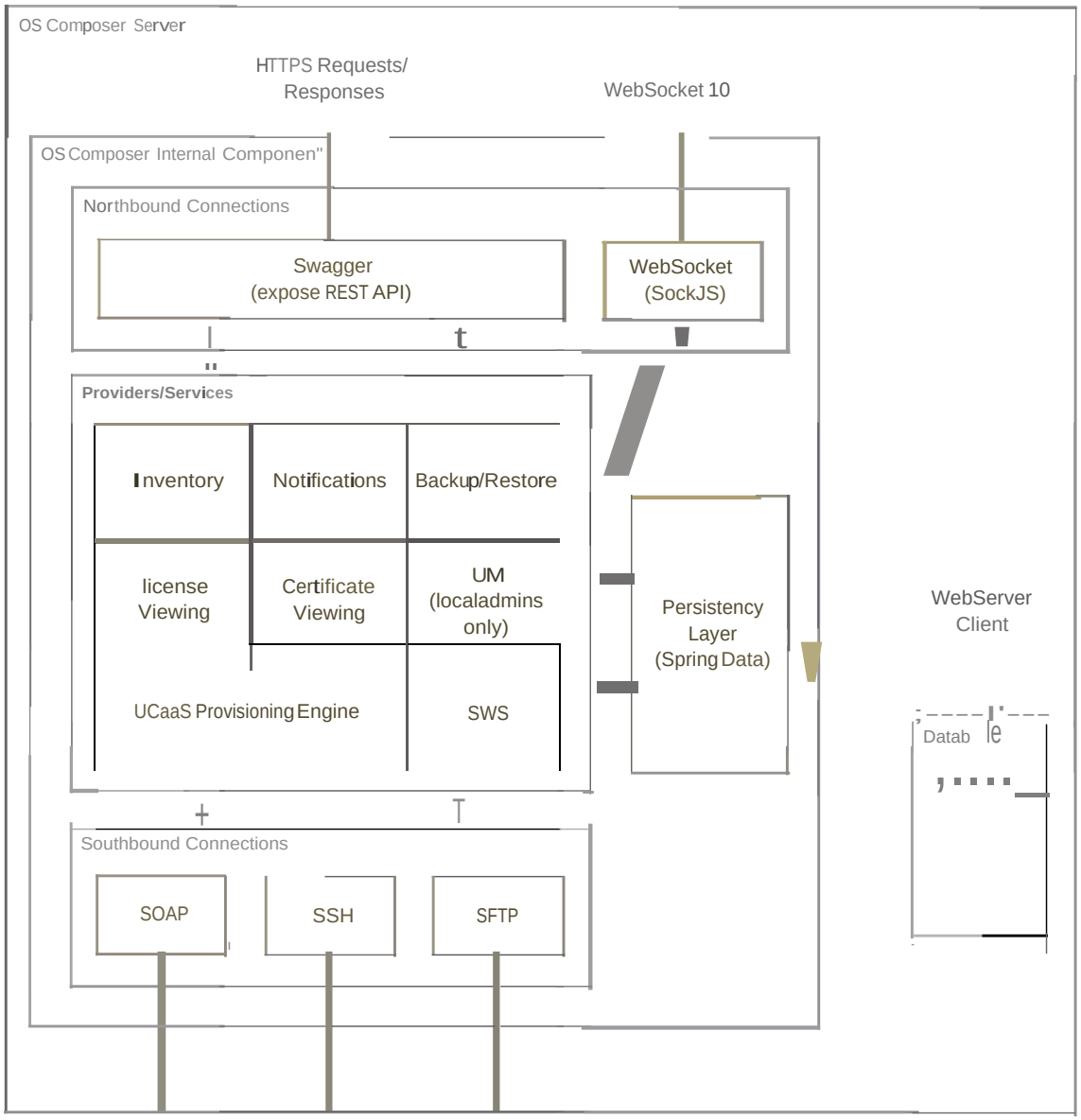


Figure 1 Architectural Overview

The internal architecture of OS Composer is illustrated in the component diagram below. On a high-level view, OS Composer is partitioned in three logical layers; Northbound connections, Providers/Services and Southbound connections.
Northbound connections deal with connections coming from other clients or servers act- ing as clients for OS offering a REST API (through https://) as well as WebSocket Con-
nections using SockJS. Providers and Services offer the core functionality of OS Compos-
er including all the business logic to be served through REST API or WebSockets. Providers and Services that either fetch or persist data from database make use of the Persistency Layer which in turn forwards requests to the database.
Southbound connections are the communication channels for OS Composer to react with all the managed network elements (OSV, SBC, DLS, etc.) using either SOAP, SFTP or direct SSH connections.


OS Composer Server
HTTPS Requests/
Responses
WebSocket 10
OS Composer Internal Componen"
Northbound Connections
Swagger
(expose REST API)
WebSocket
(SockJS)
Providers/Services
Inventory
Notifications
Backup/Restore
license
Viewing
Certificate
Viewing
UM
(localadmins
only)
UCaaS Provisioning Engine
SWS
Persistency
Layer
(Spring Data)
WebServer
Client
Datab
Southbound Connections
SOAP
SSH
SFTP

CL-1 All components	**Up-to-date SW**
Measures	Up-to-date SW installed for (Download for Unify products available at https://sws.unify.com/SWS/SWSIntra.aspx)
OpenScape Composer Server	Yes: ☐ No: ☐
Central Components 1) Latest patch level of Java Runtime Environment IBM: 1.8	Yes: ☐ No: ☐
Further 3rd party components Browser OS	Yes: ☐ No: ☐ Yes: ☐ No: ☐
PCs / Servers / Devices Servers Client PCs	Yes: ☐ No: ☐ Yes: ☐ No: ☐
Comments, Reasons, References	

3 Server Hardening

Each Server the OpenScape Composer runs on shall be hardened. That may be more than one Server for distributed or cold-standby deployment of OpenScape Composer.

The build-in Client offered by OpenScape Composer is browser based so the general re- quirements are to have a PC where:

- The operating system is Linux (for example SLES 12), please also see sales infor- mation)
- Current security updates are installed (see also section 2).
- A suitable virus protection SW shall be installed and active (see 3.2).
- Access to the system is protected by passwords according to the password rules fixed in 7.1.

3.1 OpenScape Composer Protection on Server Level

Whether the user accounts on Operating System Level shall be content of the security Checklist or not, depends on the customer deployment. Many customers do that on their own. Nevertheless, they must be informed, that the security of server access on OS level is not independent of the security of OpenScape Composer.

- Access right settings for user accounts (read/write access to file system)
- OS Password policies
- Default PW replacement

OpenScape Composer Data Protection on Server:

For the protection of the data stored locally (for example, in file systems) the user ac- counts shall only have limited access rights.

The installation is performed as “root”-user and the OpenScape Composer server is run- ning as “root”. This is necessary to open port numbers below 1024 and to use ICMP. The main installed component is the well-known SpringBoot “fat” jar which also embeds the application server, in this case Tomcat. It should be emphasised here that there is no management application loaded to control the embedded Tomcat so there are no other user accounts that could be used to login and misuse or attack Tomcat via network.

CL-2 **Desktop and other Server PCs**	**File system access rights – for Linux installations**
Measures:	Check that only “root” has read/write access to the installation directory (default: /opt/cmpnext).
Executed	Yes: □ No: □
Comments, Reasons, References	

CL-3 **Desktop and other Server PCs**	**Access to the server is protected by passwords.**

Measures	The default passwords are replaced by passwords according to the PW policy
References	PW Policy, for example, see chapter 7.1.1
Needed Access Rights	
Executed OpenScape Composer Server:	Yes: □ No: □
Customer Comments and Reasons	

3.2 Virus Protection

Unify Baseline Security Policy recommendation can be found in [4].

CL-4 **Desktop and other Server PCs**	**Virus protection software is installed and active.**
Measures	Virus scanner to be used (for example, Trend Micro)
Executed OpenScape Composer Server:	Yes: □ No: □
Executed	Yes: □ No: □
Comments, Reasons, References	

4 Virtualization

The OpenScape Composer can run on a virtualized system under VMWare vCenter Serv- er.

5 OpenScape Composer

5.1 Initial Password setup

OpenScape Composer comes with its own user and access rights management. After in- stallation, the only existing user “operator” has a default password. The password must be set at the first login.

CL-5 OpenScape Composer	**Change password for “operator”**
Measures	Login to OpenScape Composer, enter the default password for “operator” and type a new password when prompted (also see 7.1 for password policies)
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

5.2 OpenScape Composer Client

To enable encrypted and secure communication between the OpenScape Composer client (Administrator- and Web-Client) and OpenScape Composer server, HTTPS over SSL should be activated. This is already the default after installation. However, it should be checked because it may have been deactivated in the past for example, if this is an up- date installation.

CL-6 OpenScape Composer	**HTTPS Client Access**
Measures	☐ Check if HTTPS is switched on for the OpenScape Composer server (Server should be reachable only on the https URL for example, https://ComposerIP:ComposerPort and **NOT** on the http://ComposerIP:ComposerPort) (for example, https://10.1.1.1:8085/)
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

5.2.1 HTTPS access with customer specific certificate

The access to the OpenScape Composer should always be encrypted via HTTPS. This pro- tocol should stay activated.
A self-signed server certificate for HTTPS encryption is generated by default. (This must be accepted as “trusted” by the user in the browser.)
A customer specific certificate which relies on a root certificate authority (CA) can be used. This enables the browser, used for OpenScape Composer access, to set up a se-

cure end-to-end connection with the OpenScape Composer server without showing a cer- tificate warning message.

CL-7 OpenScape Composer	**Customer specific certificate for OpenScape Composer's build-in Web-Server (port 8085)**
Measures	Create a customer certificate, which is issued for the Open- Scape Composer (server name or IP address) and activate it for the OpenScape Composer client access.
References	
Executed	Yes: □ No: □
Comments, Reasons, References	

5.3 OrientDB Database

OrientDB offers a wide range of Drivers like JDBC, OrientJS for NodeJS, Java Native API and others. Composer is currently connecting to Database with the Java Native API but in any case, whatever the driver is, credentials are required to authenticate connections from client to Database server.

Securing Driver connections depends on the database manufacturer and is not in the scope of this document.

CL-8 **OpenScape Composer Database hardening advisories**	**Database Specific Hardening Advisories.** **Default Passwords must be changed for the four ac- counts: root, admin, reader, write**

Measures	**Configure orientdb server users (orientdb root user)** 1. export JAVA_HOME=/opt/cmpnext/packages/ibm-java-x86_64-80/jre/ export PATH=$JAVA_HOME/bin:$PATH 2. cd /opt/cmpnext/packages/orientdb-community/bin/ sh console.sh 3. SET server user root <new_password> * exit 4. (If the orientdb: path already exists, just add on the existing configuration. Note: make sure the same order as the one in application.yml is kept) orientdb: rootPassword: <new_password> 5. systemctl restart cmpn **Configure cmpn db users** 1. export JAVA_HOME=/opt/cmpnext/packages/ibm-java-x86_64-80/jre/ export PATH=$JAVA_HOME/bin:$PATH 2. cd /opt/cmpnext/packages/orientdb-community/bin/ sh console.sh 3. connect remote:127.0.0.1/cmpn admin <admin_pswd> (Default password is admin) 4. select from ouser 5. run the following command for all users except admin (if they exist) drop user <name> e.g. drop user reader 6. update ouser set password = '<new_account_password>' where name = 'admin' exit 7. (If the orientdb: path already exists, just add on the existing configuration. Note: make sure the same order as the one in application.yml is kept) orientdb: password: <new_account_password> 8. systemctl restart cmpn
References	
Needed Access Rights	

Executed	Yes: □ No: □
Customer Comments and Reasons	

5.4 Web Browser

Web browsers are available on many systems. Because in many cases a browser is the entry point to the system for attackers, the hardening of the browser is essential. Many browsers for example, can detect malware in download files, disable access to known malicious websites or force secure communication.

6 Administration

6.1 System Access Protection- Authentication

The administration of the system and the involved components has to be protected from unauthorized access. This includes the following aspects:

- Authentication of every user (user name, password)
- Authorization (roles and privileges)

Fixed passwords are a serious security risk. In any case, individual and safe password must be used for all users. Every user shall only get those rights or roles, which are nec- essary for him.

OpenScape Composer allows to assign individual roles to users. There are pre-defined roles which can be used.

CL-9 Organizational	**Overall Password concept**
Measures	Rules for password handling are defined and applied for administration
References	see 7.1
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	

CL-10 Organizational	**Overall Role concept**
Measures	Role concept is defined. OpenScape Composer comes with a default role: Operator. Currently this is sufficient, and no additional role concept has to be defined. More **Operator** accounts can be created by logging in with the default 'op- erator' account and navigating to User Management Tab -> User List -> Add.
References	
Customer Name(s) / Role	Yes: ☐ No: ☐
Service Name(s) / Role Name(s) / Role	Yes: ☐ No: ☐
Comments, Reasons, References	

6.2 Data Protection

Access to central components shall only be possible for technicians and administrators.

CL-11 Organizational	**Access control to infrastructure and data storage**
Measures	Physical access to systems and storage devices is locked and access rules are defined.
Executed	Yes: ☐ No: ☐
Comments, Reasons, References	Measures to be done:

6.3 Network Ports – Firewall Concept

Addendum 0 shows a list of network ports used for the communication between Open- Scape Composer server and client, and between OpenScape Composer server and the managed network elements, servers and applications. This information may be used for firewall configuration to increase security.

It has to be distinguished between ports needed for the communication between Open- Scape Composer client and server and between OpenScape Composer server and the managed network elements, applications and systems. The ports between client and server are required for the operation/administration of OpenScape Composer.

The number of ports used for the communication between the OpenScape Composer server and the monitored network environment is quite large because of the complexity of the heterogeneous environments OpenScape Composer can monitor. Blocking some of these ports may or may not restrict the operation of OpenScape Composer, depending if they are relevant in the customer environment or not.

Interfaces which are not used in the customers scenario shall be deactivated and not be activated without explicit need. The ports used with OpenScape Composer can be found in the addendum 0. This information may be used for external firewall configuration for example, for network separation to increase security.

Since connection problems caused by firewall rules can cause management problems which are not easy to identify, it is not recommended to block outgoing network ports at OpenScape Composer side.

7 Addendum

7.1 Password Policies

OpenScape Composer supports the Password Policy depicted in https://hisat.global-intra.net/wiki/index.php/General_Security_Requirements

This policy is summarized in the table in the next section.

7.1.1 PW Policy supported by OpenScape Composer

Minimal Length	8
Maximum Length	255
At least one character from at least 3 of the following groups: 1. lowercase letters 2. uppercase letters 3. numbers 4. special characters (e.g. @, !, $)	
Maximal number of repeated characters	-
Maximal number of sequential characters	-
Change interval	-
Maximum number of erroneous login attempts with different passwords	-
Password History	1

The Password policy is checked automatically!
Do not use trivial or easy to guess passwords. Do not reuse old passwords. Take care that password entry cannot be observed.

7.2 Certificate Handling

7.2.1 OpenScape Composer build-in Web-Server

OpenScape Composer uses a self-generated certificate for HTTPS access. This can be replaced by a customer specific certificate, if needed. See section 5.2.1 HTTPS access with customer specific certificate.

7.3 Transport Layer Security (TLS) Configurations

As of version V2 R3.2.0, OpenScape Composer uses TLSv1.2 and TLSv1.3 by default. To enable older TLS versions, the default configuration should be overridden.
To do this, add the following entry in the **/opt/cmpnext/app/application-production.yml** file:

server.ssl.enabled-protocols=TLSv1,TLSv1.2,TLSv1.3

OpenScape Composer uses the following Cipher Suites:

TLSv1.3:
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_CHACHA20_POLY1305_SHA256

TLSv1.2:
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA38,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLSv1.0/TLSv1.1:
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

The cipher lists mentioned above are also arranged in order of server preference.

Port Table

7.4 Client/Server Communication

#	Source	Destination	Port	Proto-col	Description/Function
1	Browser	Composer Server	8085	HTTPS	WebClient/Swagger Con-sumer

7.5 Communication Server/Managed Network

#	Source	Destination	Port	Protocol	Description/Function
1	OpenScape Composer	SFTP Repository	22	SFTP	Transfer files between Open-Scape Composer and an SFTP Repository
2	OpenScape Composer	FTP Repository	21	FTP	Transfer files between Open-Scape Composer and an FTP Repository
3	OpenScape Composer	All Applications	22	SSH	OpenScape Composer SSH communication with other Appli-cations
4	OpenScape Composer	All Applications	22	SFTP	Transfer files between Open-Scape Composer and other ap-plications via SFTP
5	OpenScape Composer	OSV SOAP Server with TLS	8757, 8758, 8759, 8760 (one can be chosen)	HTTPS	OpenScape Composer communication with OSV SOAP server
6	OpenScape Composer	OSV SOAP Server without TLS	8767, 8768, 8769, 8770 (one can be chosen)	HTTP	OpenScape Composer communication with OSV SOAP server
7	OpenScape Composer	SBC/OSB SOAP Server	443	HTTPS	OpenScape Composer communi-cation with SBC/OSB SOAP serv- er
8	OpenScape Composer	DLS SOAP Server	10444	HTTPS	OpenScape Composer communication with DLS SOAP server
9	OpenScape Composer	SWS SOAP Server	447	HTTPS	OpenScape Composer communication with SWS SOAP server
10	OpenScape Composer	UC, Media Server and MCSA	4711	HTTPS	OpenScape Composer communication with UC, Media Server and MCSA applica-tions using the Symphonia Framework

8 References

[1] **Support of Operating System Updates for Server Applications**
http://wiki.unify.com/images/c/c0/Security_Policy_-_Support_of_Operating_System_Updates_for_Server_Applications.pdf