OpenScape Accounting V5

Security Checklist

Planning Guide

A31003-S4150-P100-02-76A9

Atos

Provide feedback to further optimize this document to edoku@atos.net.

As reseller please address further presales related questions to the responsible presales organization at Unify or at your distributor. For specific technical inquiries you may use the support knowledgebase, raise - if a software support contract is in place - a ticket via our partner portal or contact your distributor.

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Reference No.: A31003-S4150-P100-02-76A9

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.

atos.net

Contents

1 Introduction

1.1 History of Change

Date	Version	What
2017-10-17	1	Initial release v3
07-07-2022	1	Create V5 document

1.2 General Remarks

Information and communication and their seamless integration in “Unified Communications and Collaboration“ (UCC) are important, valuable assets forming the core parts of an enterprise business. These assets require every enterprise provide specific levels of protection, depending on individual requirements to availability, confidentiality, integrity and compliance for the communication system and IT infrastructure it utilizes.

Unify attempts to provide a common standard of features and settings of security parameters within 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 weigh the costs of implementing security measures against the risks of omitting a security measure and to “harden” the systems appropriately.

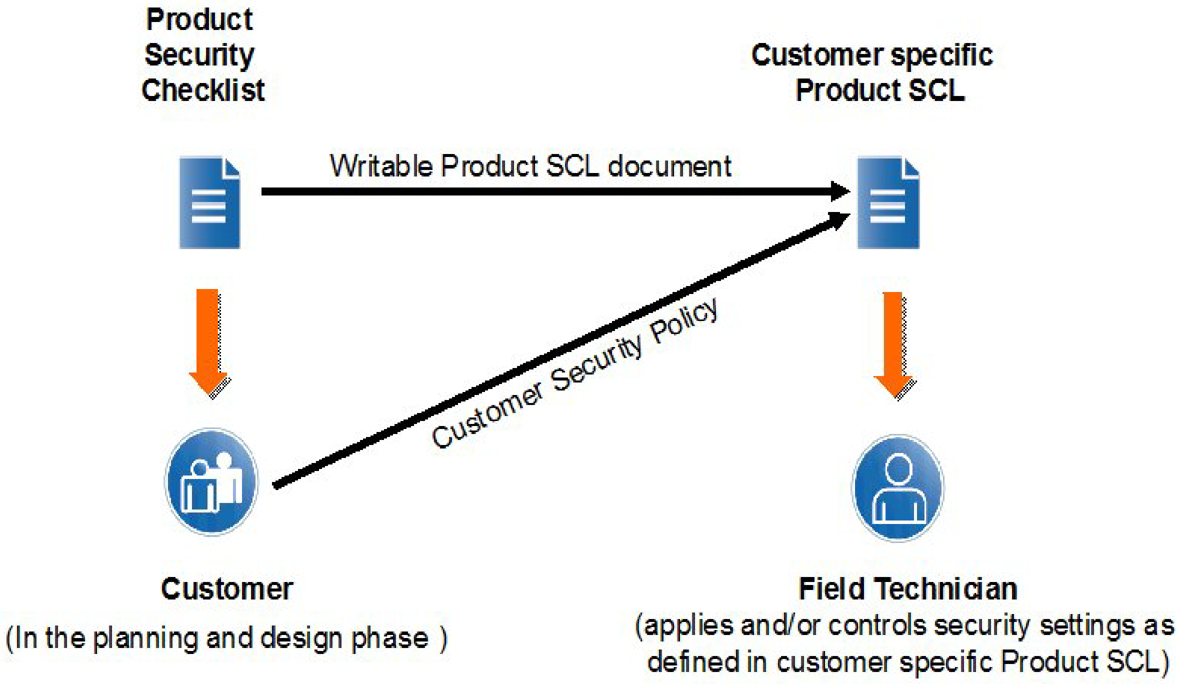
Product Security Checklists are published as a basis to support the customer and service department in both direct and indirect channels, as well as self-maintainers, to document security setting agreements and discussions.

The Security Checklists can be used for two purposes:

- **In the planning and design phase** of a particular customer project:
  Use the Product Security Checklists of every relevant product to evaluate, if all products that make part of the solution can be aligned with the customer’s security requirements – and document in the Checklist, how they can be aligned. The Product Security Checklist containing customer alignments can be identified as Customer specific Product Security Checklist.
  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

- **During installation and during major enhancements or software upgrade activities:**
  The Customer specific Product Security Checklists are used by a technician to apply and/or control the security settings of every individual product.

Figure: Usage of Security Checklists (SCL)


Product Security Checklist
Customer specific Product SCL
Writable Product SCL document
Customer Security Policy
Customer
(In the planning and design phase)
Field Technician
(applies and/or controls security settings as defined in customer specific Product SCL)

Update and Feedback

- By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included 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 partner portal http://www.unify.com/us/partners/partner-portal.aspx for the entire product .
  They can be retrieved from the Unify partner portal http://www.unify.com/us/partners/partner-portal.aspxfor the entire product .
- 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 (obso@atos.net).

1.3 Security Strategy for Unify Products

Reliability and security is a key requirement for all products, services and solutions delivered by Unify. This requirement is supported by a comprehensive security software development lifecycle that applies to all new products or product versions being developed from design phase until end of life of the product.

Products of Unify are developed according to the Baseline Security Policy, which contains the technical guidelines for the secure development, release and sustaining of the company's products. It defines the fundamental measures for software security that are taken throughout the whole lifecycle of a product, from design phase until end of life:

Product planning and design:

Threat and Risk analysis (Theoretical Security Assessment) to determine the essential security requirements for the product.

Product development and test:

Penetration Tests (Practical Security Assessment) to discover implementation vulnerabilities and to verify the hardening of the default system configuration.

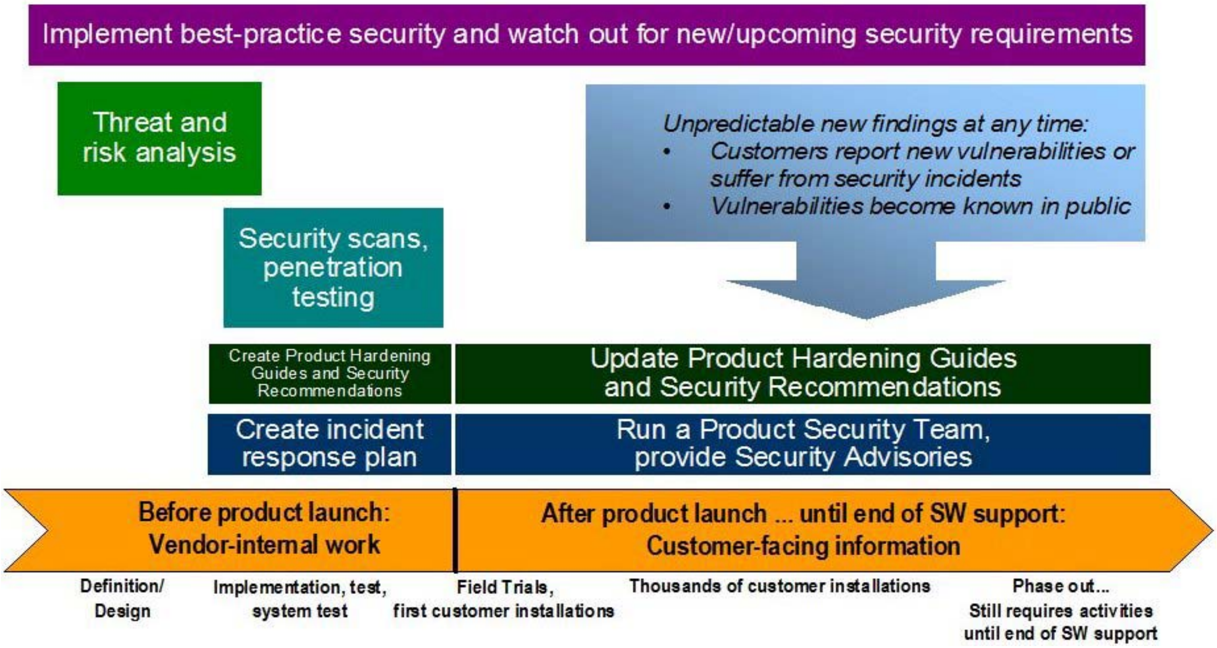
Installation and start of operation:

Hardening Guides (Security Checklist) to support the secure configuration of the product according to the individual customer's security policy.

Operation and maintenance:

Proactive Vulnerability Management to identify, analyse and resolve security vulnerabilities that emerge after products have been released, and to deliver guidance to customers how to mitigate or close these vulnerabilities.

Figure: Unify Baseline Security Policy- from Design to EOL


Implement best-practice security and watch out for new/upcoming security requirements
Threat and risk analysis
Unpredictable new findings at any time:
• Customers report new vulnerabilities or suffer from security incidents
• Vulnerabilities become known in public
Security scans, penetration testing
Create Product Hardening Guides and Security Recommendations
Update Product Hardening Guides and Security Recommendations
Create incident response plan
Run a Product Security Team, provide Security Advisories
Before product launch: Vendor-internal work
After product launch ... until end of SW support: Customer-facing information
Definition/ Design
Implementation, test, system test
Field Trials, first customer installations
Thousands of customer installations
Phase out... Still requires activities until end of SW support

For more information about the Unify product security strategy we refer to the relevant Security Policies [1] and [2] in chapter .

As we at Unify define a secure product, our products are not secure, but - they can be installed, operated and maintained in a secure way. The level of the products security should be scheduled by the customer.

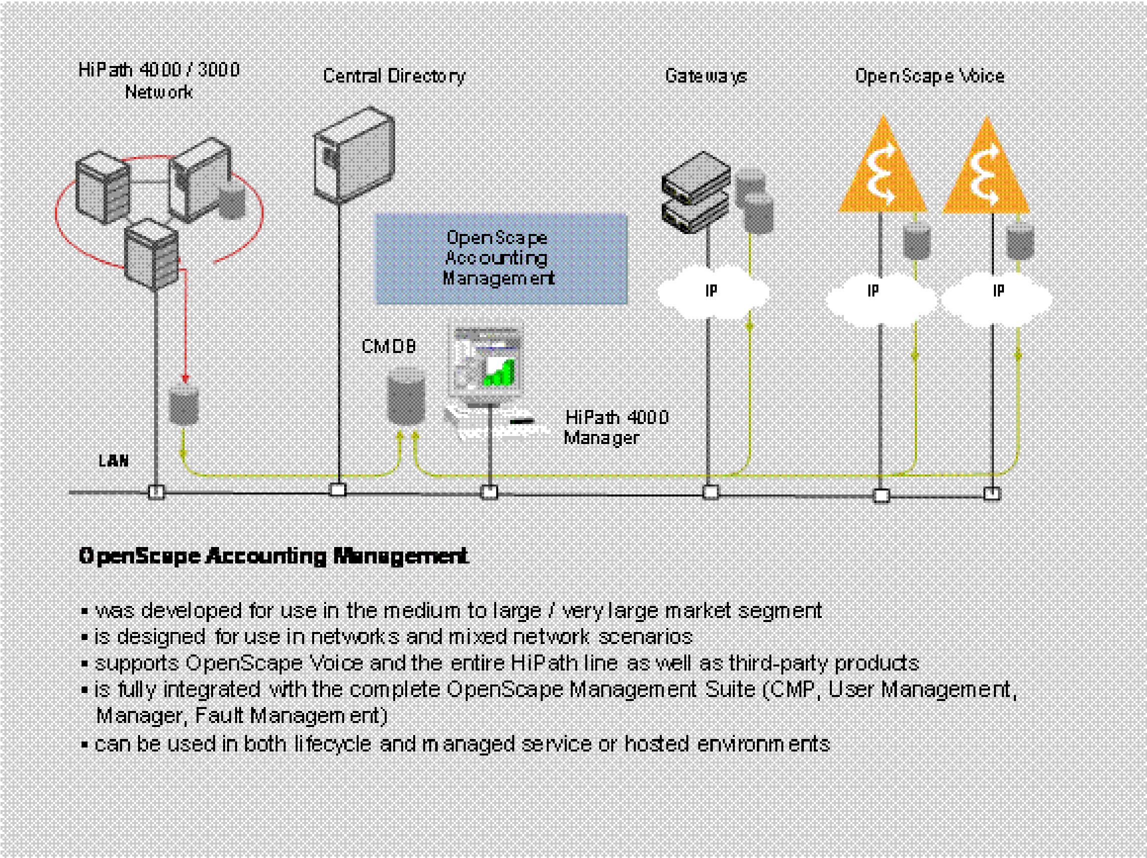
The necessary information for that is drawn up in the Product Security Checklist.

1.4 Customer Deployment- Overview

This Security Checklist covers the product and lists their security relevant topics and settings in a comprehensive form.

	Customer	Supplier
Company		
Name		
Address		
Telephone		
E-mail		
Covered Systems (e.g. System, SW version, devices, MAC/IP-addresses)		
Referenced Master Security Checklist	Version:	
	Date:	
General Remark		
Open issues to be resolved until		
Date		

2 OpenScape Accounting in General



OpenScape Accounting Management

- was developed for use in the medium to large / very large market segment
- is designed for use in networks and mixed network scenarios
- supports OpenScape Voice and the entire HiPath line as well as third-party products
- is fully integrated with the complete OpenScape Management Suite (CMP, User Management, Manager, Fault Management)
- can be used in both lifecycle and managed service or hosted environments

For safeguarding an OpenScape Accounting managed solution all components have to be considered:

- Infrastructure (LAN, WAN)
  Physical and logical protection of the infrastructure against manipulation of features as well as sabotage.
- OpenScape Accounting
  Protection from unauthorized access and breach of confidentiality through individual passwords and protection of interfaces
- Workplace and server PCs
  Admission control by suitable password, provisioning with actual security updates, virus protection where required

The recommended measures are listed in the following chapters.

All components	Up-to-date SW
Measures	Up-to-date-SW installed for
OpenScape Accounting	Yes: □ No: □

All components	**Up-to-date SW**
PCs / Servers OSc Acc Server	Yes: □ No: □
OSc Acc Client PC(s)	Yes: □ No: □
OSc Acc Database Server (optional)	Yes: □ No: □
Customer Comments / Reasons	

3 OS Hardening

Always refer to the release notes for an updated list of supported operating systems.

Operating System Name	Operating System Version	
Server		
Windows Server 2012, 2016, 2019, 2022	2012, 2016, 2019, 2022	
Clients		
Windows 10 (32 and 64 bit version)	Service Pack:	all SP
	Hot fixes:	all available Security- & Update Patches
Windows 11 (32 and 64 bit version)	Service Pack:	all SP
	Hot fixes:	all available Security- & Update Patches

3.1 OS Hardening according to CIS

Please follow the OS Benchmarks for windows of the Center of Internet Security CIS

https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform

The operating system is not part of the software delivery of OpenScape Accounting and therefore the hardening of the OS is up to the customer, but Unify proposes hardening procedures that should be executed by the customer.

Application specific Differences to CIS OS Hardening

t.b.d

3.2 Virus Protection

The OpenScape Accounting server has to be protected by virus protection software. There are no known limitations. But not all available virus protection softwares were tested

CL-VirusProtect Server PCs	Virus protection software is installed and active.
Measures	Virus scanner to be used (e.g. Trend Micro)
References	
Needed Access Rights	

CL-VirusProtect Server PCs	**Virus protection software is installed and active.**
Executed **Server1**	Yes □ No: □
Customer Comments and Reasons	Which Virus Software? □

4 Virtualization

OpenScape Accounting supports virtualization based on VMWare.

4.1 Virtualization Hardening according to CIS

Please follow the VMWare Benchmark issued by the Center of Internet Security (CIS).

https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform

4.2 Application specific Differences to CIS VM Hardening

There is no OpenScape Accounting specific difference to CIS VMWare hardening.

5 3rd Party Components

5.1 Apache Web Server

5.1.1 Apache 2.4 Hardening according to CIS

A self-signed server certificate for HTTPS encryption is delivered by default. (This has to be accepted as trusted by the user in the browser.)

For server authentication and against man-in-the-middle attacks at the administrator interface, an individual certificate is necessary. A customer specific certificate, which relies on a root certificate authority, has to be used. This enables the browser, used for administration, to set up a secure end-to-end connection with OpenScape Accounting.

CL- Browser Certificate	**Customer specific certificate for a secure end-to-end connection**
Measures	Import a customer certificate, which is issued for the OpenScape Accounting (server name or IP address) and activate it for the administration access.
References	
Needed Access Rights	
Executed	Yes □ No: □
Customer Comments and Reasons	

If no FM integration on a standalone system is used, all ports beside 443 must be closed on the OSc ACC server firewall.

CL-Disable Web Server Ports	**Disable access to unnecessary web server ports in firewall**
Measures	When OSc ACC is installed as standalone system, then the OS ACC server firewall must be configured to block all web server ports beside 443.
Needed Access Rights	

CL-Disable Web Server Ports	Disable access to unnecessary web server ports in firewall
Executed	Yes □ No: □
Customer Comments and Reasons	

5.2 Web Browser

Web browsers are available on many systems. They contain a complex and error-prone software. Because in many cases a browser is the entry point to the system the hardening of the browser is essential. Many browsers e.g. can detect malware in download files, disable access to known malicious websites, force secure communication.

5.2.1 Browser Hardening according to CIS

Browsers that are used for the system: IE V10, V11,Edge; Firefox V40 and greater

For Mozilla Firefox, IE see:

https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform

5.2.2 Application specific Differences to CIS Browser Hardening

There is no OpenScape Accounting specific difference to CIS Browser hardening.

5.3 Oracle database

With OpenScape Accounting the Oracle 11g Express Edition is delivered. Please note, that for this edition of the Oracle database no support or security patches are available.

It is recommended to use a commercial Oracle license in order to be able to apply security patches for the database. If Oracle Express Edition is used, then it has to be installed on the same server with OpenScape Accounting and access to Oracle must be blocked by the firewall. Alternatively, if customers decide to buy and use Oracle database, then it can be deployed to another server. However, in that case, the server which has Oracle database must be hardened as specified in CIS benchmark: http://benchmarks.cisecurity.org/downloads/benchmarks/?

CL-Disable Oracle Ports	**Disable access to all Oracle ports in firewall**
Measures	When OSc ACC is installed as standalone system with Oracle Express Edition, then the OS ACC server firewall must be configured to block all Oracle ports.
Needed Access Rights	
Executed	Yes □ No: □
Customer Comments and Reasons	

CL- Harden Oracle	**Disable access to unnecessary web server ports in firewall**
Measures	When Oracle Database is installed to another server, then the that server must be harened as specified in CIS benchmark for Oracle.
Needed Access Rights	
Executed	Yes □ No: □
Customer Comments and Reasons	

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)
- Audit (activity log)

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 necessary for him.

CL Pwd1 **Organizational**	**Overall Password concept**
Measures	Rules for password handling are defined see chapter.Password Policies and applied for administration
References	OpenScape Accounting; Administration and Usage; Administrator Documentation [1], Chapter 8.2 "Group Administration"
Needed Access Rights	
Executed	Yes □ No: □
Customer Comments and Reasons	

CL-RoleConcept **Organizational**	**Overall Role concept**
Measures	Role concept is defined.
References	OpenScape Accounting; Administration and Usage; Administrator Documentation [1], Chapter 8.2 "Group Administration"
Needed Access Rights	
Customer Name(s)/Role	Yes □ No: □
Service	

CL-RoleConcept Organizational	Overall Role concept
Name(s)/Role	
	Yes □ No: □
Name(s)/Role	
	Yes □ No: □
Customer Comments and Reasons	

Secure communication for local and remote administration plays an essential role as well. Details are given in chapter 8.

6.1.1 Initial Password Setup

During the installation of OpenScape Accounting a password for the Oracle database is asked. It is recommended to alter the default password. The password of the main system administrator OSc Acc must be altered with the first login. Please observe the password policies (addendum).

6.2 OpenScape Accounting Management Client

The access to the OpenScape Accounting occurs always encrypted via HTTPS. Administration access is documented in the system protocol. This protocol shall stay activated.

A self-signed server certificate for HTTPS encryption is delivered by default. (This has to be accepted as trusted by the user in the browser.)

For server authentication and against man-in-the-middle attacks at the administrator interface, an individual certificate is necessary. A customer specific certificate, which relies on a root certificate authority, has to be used. This enables the browser, used for administration, to set up a secure end-to-end connection with OpenScape Accounting.

A new password has to be entered after the first start according to Password recommendations (see chapter 10.1)

Note for Network Design:

The native OpenScape Accounting Client shall only be used within a secured, firewall protected LAN or on the OpenScape Accounting Server.

The user password is checked against the password policy. These can be adopted for every user group.

CL- Client Accounts	Create Client accounts and set Individual passwords
Measures	Implement user accounts, roles and individual passwords for • Basic user • Administrators • Revision/Audit
References	
Needed Access Rights	
Executed	Yes □ No: □
Customer Comments and Reasons	

7 Infrastructure

The Security Checklist is a help for the secure configuration of the OpenScape Accounting during the installation phase. The design phase of the customer network is before the installation phase. Thus in fact rules for the network design are not the focus of this document.

Practical experience has shown that it might be necessary to have information about a secure network design, because dependent on this network design communication connections have to be secured or not.

7.1 Planning of Internal IP Networks (LAN)

For the internal IP network, the requirements according to the administrator documentation [1] have to be met. Access to central components like switches and routers shall be restricted to technicians and administrators.

A logical or physical decoupling of voice and data network should be considered depending on the existing infrastructure. The IT service provider of the customer may have to be involved.

CL-LANDesign **LAN infrastructure**	**Design a protected infrastructure**
Measures	Access to routers and switches only for authorized persons and trusted devices. Keep OSc Acc server, optional OSc Acc Clients in the same internal network, which is protected by a firewall.
References	
Needed Access Rights	
Executed	Yes □ No: □
Customer Comments and Reasons	

8 Addendum

8.1 Password Policies

These are the recommended criteria for selection of passwords or PINs (numerical passwords). Please implement them unless other company specific rules are defined at customer site. Use the group administration to redefine the default password policies.

8.1.1 PW Policy supported by OpenScape Accounting

No	Password Policy Topic	PW default	PW range
Rules for Selection of Password			
1	Minimal Length standard	10	32
	- admin	12	
	- user	8	
	Maximal PW length that is supported by product (not security relevant, but implementation relevant)	32	1
2	Minimal number of upper case letters	1	0-32
3	Minimal number of lower case letters	1	0-32
4	Minimal number of numerals	1	0-32
5	Minimal number of special characters	1	0-32
6	Maximal number of identical characters in a row, (e.g. ‘5’ = 1, ‘555’ = 3)	32	32
7	Maximal number of sequential characters in a row (e.g. ‘12345’ = 5 or ‘asdfghjkl =9 , ‘a’ = 1)	32	32
8	Account name (reversed too) may not be part of password	False	False
9	Use blacklist of strings which may not be contained in password	False	False
10	Minimum character count for changed characters	0	0
11	Password history	5	0-10
12	- superuser	5	0-10
	- admin	5	0-10
	- user	5	0-10
Administrative Rules for Passwords			
	Maximum password age standard	60 days	0-90 days

No	Password Policy Topic	PW default	PW range
13	- superuser	60 days	0-90 days
	- admin	60 days	0-90 days
	- user	60 days	0-90 days
	Minimum password age	0	0-5
14	Notification before password expiration in days	4	0-min(14, max_password_age-1)
15	Password change requires knowledge of old password	True	True
16	Force change default passwords/PINs after the first use	False	True/False
	- admin	False	True/False
	- user	False	True/False

8.1.2 PW Policy Integration Aid for Technicians

Use the group administration to redefine the default password policies. The adoption of password policies is described in the service manual.

8.2 DefaultAccounts

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 have to be informed, that the security of server access on OS level is not independent of the security of OSc ACC.

• Access right settings for user accounts (read/write access to file system)

• OS Password policies

• Default PW replacement

For the protection of the data stored locally (e.g. in file systems) the user accounts shall only have limited access rights.

The following default accounts are configured during installation:

- system
  - Default database administrator user. User: system Password: oraclexe. The setup asks to change the password. Changing the password is recommended.
  - Privileges of this user: Full database access (read/write/execute/connect etc.)
- syscable
  - OpenScape Accounting administrator: User: syscable Password: syscable. This password must be changed at the first login.

- Privileges of this user: Full application access (read/write).
- Default language: German

After the installation for each account, a default password is available.

Since the default PW are publicly available, it is absolutely necessary to change them into customer specific passwords immediately after installation process.

Be aware that most successful attacks to Unify systems base on unchanged default passwords.

8.2.1 OpenScape Accounting accounts

#	User Name	PW Policy configured	Unify Default PW (to be changed immediately)	Description
1	system	As agreed in chapter	oraclexe	Database administrator (DBA) with full database access
2	syscable	As agreed in chapter	syscable	Application administrator with full access.

8.2.2 Client accounts

#	User Name	PW Policy configured	Unify Default PW (to be changed immediately)	Description
1				
2				
3				
4				

Client accounts are not created during installation.

8.3 Certificate Handling

A certificate guarantees the ownership of e.g. a public key to a person or organization.

A self-signed server certificate for HTTPS encryption is delivered by default. (This has to be accepted as trusted by the user in the browser.)

For server authentication and against man-in-the-middle attacks at the administrator interface, an individual certificate is necessary. A customer specific certificate, which relies on a root certificate authority, has to be used. This enables the browser, used for administration, to set up a secure end-to-end connection with OpenScape Accounting.

During the configuration via the Configuration Wizard, a self signed certificate matching the host's FQDN can be generated. Such a certificate must be used when not using a company-provided one.

8.3.1 Credentials used for OpenScape Accounting

TLS certificates are used in OpenScape Accounting for connections:

#	Interface	Customer requirement for OpenScape Accounting credentials	Unify Default credentials	Usage
1	HTTPS		OSc ACC default certificate	Web UI access
2				
3				

8.4 Port Table

Interfaces, which are not used, are deactivated by default and shall not be activated without explicit need. The ports used with OpenScape Accounting can be found in the administrator documentation.

For a standalone installation of OpenScape Accounting the port 1521 (Oracle Listener) can be closed on the firewall of the OpenScape Accounting Server.

#	Destination/ Source Port	Network/ Application Protocol	Default State	configu-rable	From	To	Description/ Function
1	D:22	TCP / SSH		Yes	OSc ACC	OpenScape 4000 Manager	SCP for master data alignment with OpenScape 4000 Manager
2	D:21	TCP / FTP		Yes	OSc ACC	OpenScape 4000 Manager	FTP for master data alignment with OpenScape 4000 Manager
3	S:161	UDP / SNMP GET	closed	Yes	HiPath FM	OSc ACC	SNMP for Open-Scape Fault Management Integration
4	D:162	UDP / SNMP Trap		Yes	OSc ACC	OpenScape FM	SNMP for Open-Scape Fault Management Integration
5	S:1521	TCP / Oracle *Net	open	Yes	Remote Clients and servers, locale web images	OSc ACC	Oracle OCI for remote clients
6	D/S:80xx	TCP / HTTP	open	Yes	OSc ACC	OSc ACC	HTTP for back-end web server
7	D/S:61740	TCP	open	Yes	OSc ACC	OSc ACC	HiPath License Agent
8	S:443	TCP / HTTP	closed	No	SSDP SP	SSDP Enterprise	HTTPS outgoing access for remote support
9	S:443	TCP / HTTPS		No	CMP	OSc ACC	CMP registration
10	D:443	TCP / HTTPS		Yes	OSc ACC	CMP	CMP UM
11	D:4709			No	OSc ACC	CMP	CMP SSO
12	D:25	TCP / SMTP		Yes	OSc ACC	Mailserver	SMTP for e-mail delivery
13	S:443	TCP / HTTPS	Closed	No	User PC (Browser)	OSc ACC	HTTPS for web access
14	S:443	TCP / HTTPS	Closed	No	CMP	OSc ACC	HTTPS for access to the CMP
15	D:389	TCP / LDAP		Yes	OSc ACC	LDAP Server	LDAP for fetching data from LDAP Servers
16	D:636	TCP / LDAPS		Yes	OSc ACC	LDAP Server	LDAPS for fetching data from LDAP Servers

#	Destination/ Source Port	Network/ Application Protocol	Default State	configu-rable	From	To	Description/ Function
17	D:22	TCP / SSH		No	OScACC	CMP SSH	SSH/SFTP access for sip endpoint retrieval
18	D:22	TCP / SSH		No	OScACC	OSV SSH	SFTP access for cdr data retrieval
19	D:8770	TCP / HTTP		No	OScACC	OSV HTTP	for SOAP client access for master data retrieval from OSV
20	D:443	TCP / HTTPS		No	OScACC	OSBiz	CDR data retrieval
21	D:8802	TCP / HTTPS		No	OScACC	OSBiz	WSI access for Welcome module

Please always refer to the entries within the IFMDB to get a current port list.

8.5 References

[1] OpenScape Accounting V3; Administration and Usage; Administrator Documentation

available via Partner Portal http://www.unify.com/us/partners/partner-portal.aspx

http://apps.g-dms.com:8081/techdoc

[2] OpenScape Accounting V3; Installation and Configuration, Installation Guide

available via Partner Portal http://www.unify.com/us/partners/partner-portal.aspx

http://apps.g-dms.com:8081/techdoc

[3] 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

[4] Secuity Policy - Vulnerability Intelligence Process,

http://networks.unify.com/security/advisories/Security_Policy_Vulnerability_Intelligence_Process.pdf

[5] Referenced Security Checklist e.g. because of shared interface

see E-Doku or TopNet

[6] Interface Management Database (IFMDB)

available via Partner Portal

http://www.unify.com/us/partners/partner-portal.aspx

[7] Center of Internet Security – Security Benchmarks

https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform

https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform

[8] OpenScape Common Management Platform, Security Checklist

available via Partner Portal http://www.unify.com/us/partners/partner-portal.aspx

http://apps.g-dms.com:8081/techdoc

Index