A MITEL
PRODUCT
GUIDE

# Unify OpenScape 4000 Manager V10

## Security Checklist

Security Checklist

Planning Guide
03/2025

A31003-H34A0-P101-4-76A9

Mitel®

## Notices

## Trademarks

# Contents

**1 Introduction . . . . 5**
1.1 Validity . . . . 5
1.2 General Remarks . . . . 5
1.3 History of Change . . . . 7
1.4 Customer Deployment - Overview . . . . 8

**2 OpenScape 4000 Manager V10 Hardening Procedures in General . . . . 9**

**3 Server Hardening . . . . 11**
3.1 BIOS Settings . . . . 11
3.2 OS Hardening . . . . 12
3.2.1 Disable IPv6 . . . . 12
3.2.2 App Armor. . . . . 12
3.3 Operating system user accounts . . . . 14
3.4 Boot loader . . . . 15
3.5 Virus Protection . . . . 16
3.6 SLES11 internal firewall / SuSEfirewall2 . . . . 17

**4 Virtualization . . . . 18**

**5 OpenScape 4000 Manager . . . . 19**
5.1 PKI based authentication . . . . 19
5.2 Configure Password Policy . . . . 20
5.3 Change predefined passwords for user accounts . . . . 21
5.4 Change predefined passwords for NSL accounts . . . . 22
5.5 Create administrator accounts and assign privileges . . . . 23
5.6 Security Mode Configuration . . . . 24
5.7 Legal Banner on Login Page . . . . 25
5.8 Backup and Restore - HBR . . . . 26
5.9 Apache Web Server . . . . 27

**6 Extending and 3rd Party Components . . . . 28**
6.1 OpenScape Fault Management . . . . 28
6.2 Accounting Management, DS Win, DTB . . . . 29
6.3 Informix DB / 3rd party products connecting to Informix DB . . . . 30

**7 Administration. . . . . 31**
7.1 System Access Protection- Authentication . . . . 31
7.2 Data Protection . . . . 32
7.3 Monitoring via SNMP . . . . 33
7.3.1 SNMP v1, v2 . . . . 33
7.3.2 SNMP v3 . . . . 34

**8 Infrastructure . . . . 35**
8.1 Protection of network infrastructure . . . . 35

**9 Addendum . . . . 36**
9.1 Password Policies . . . . 36
9.1.1 Supported Password Policy . . . . 36
9.1.2 Switch to the Extended Password Policy:. . . . . 37
9.1.3 Password Policy agreed for customer’s deployment . . . . 37
9.2 Default Accounts’ passwords . . . . 38

9.2.1 System Accounts . . . . . . . . . . 38
9.2.2 User Accounts . . . . . . . . . . 39
9.2.3 Default OS (SLES 11) Accounts . . . . . . . . . . 39
9.3 Certificate Handling . . . . . . . . . . 40
**10 TCP and UDP communication ports list . . . . . . . . . . 41**
**11 References . . . . . . . . . . 42**

# 1 Introduction

## 1.1 Validity

This Security Checklist is valid for the following product versions:

- OpenScape 4000 Manager V10R0

Starting with OpenScape 4000 Manager V10R1 there is a new combined document “OpenScape 4000 V10R1 and Affiliated Products Security Checklist” which is valid also for OpenScape 4000 Manager.

## 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:

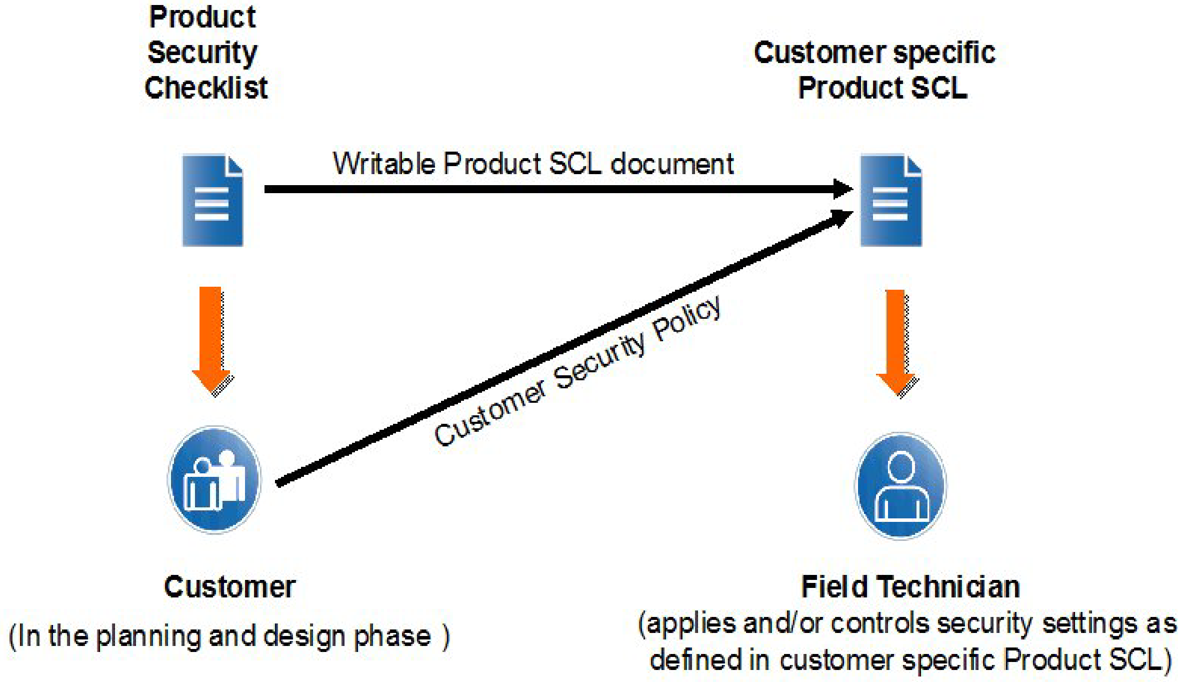
  – During installation/setup of the solution

  – 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 1 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 .

- 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 History of Change

| Date | Version | What |
|---|---|---|
| 2013-11-12 | 1 | Updated from Manager V6 R2 checklist |
| 2013-11-22 | 2 | Product name to OpenScape |
| 2014-06-30 | 3 | Update for Manager V7 R1 |
| 2016-05-01 | 4 | Update for Manager V7 R2 |
| 2017-05-31 | 5 | Update for Manager V8R0 |
| 2018-05-20 | 6 | Update for Manager V8R2 |
| 2020-03-26 | 7 | Update for Manager V10R0 |

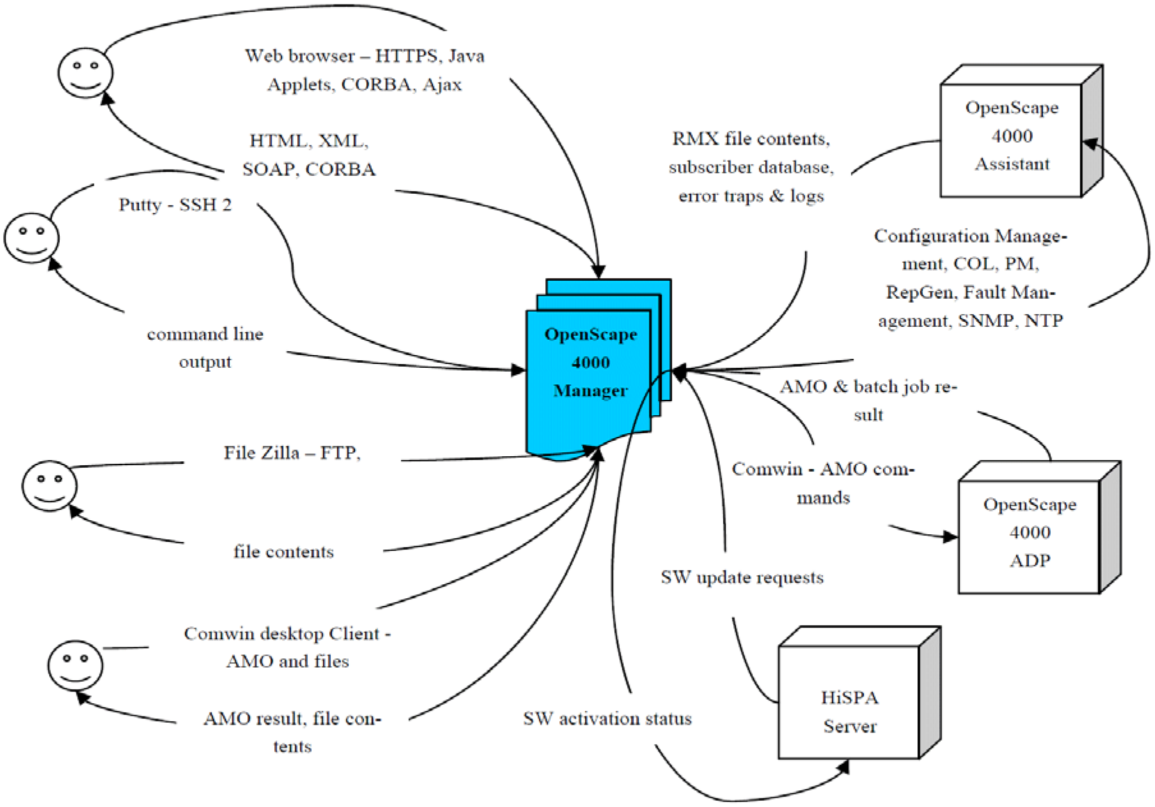
## 1.4 Customer Deployment - Overview

This Security Checklist covers the product OpenScape 4000 Manager V10 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: | |
| Open Issues to be resolved until | | |
| General Remark | | |
| Date | | |

# 2 OpenScape 4000 Manager V10 Hardening Procedures in General

*Figure 2 Use Case diagram for OpenScape 4000 Manager V10*



Security Checklist is provided in order to create the prerequisites in the service to install all Unify and certified 3rd party components of OpenScape 4000 Manager V10 corresponding to the current security requirements.

This Security Checklist supports the service technicians and re-sellers and consulting in the examination and setting of the required security measures in the software and at the hardware for OpenScape 4000 Manager V10.

The current security settings are to be confirmed by the customer by means of signature in the delivery of OpenScape 4000 Manager V10.

The Security Checklist includes information on settings of:

- Hardware
- BIOS
- operating system
- OpenScape 4000 Manager
- extending software
- 3rd party software

Deviations of the security settings on customer wish are to be documented.

The recommended measures are listed in the following chapters.

| **CL-SW status<br>All components** | **Up-to-date SW** |
|---|---|
| Measures | The following security patches and updates have to be installed:<br>1) BIOS update should be done according to HW vendor description.<br>2) Latest SLES11 updates must be made according to the Updates Manual [1] and Install & Service Manual [6].<br>3) OpenScape 4000 Manager Server has to be installed / updated according to Installation and Service Manual [6]. The latest Hotfix for OpenScape 4000 Manager V10 must be installed.<br>Up-to-date SW has been installed for |
| **OpenScape 4000 systems**<br>Manager V10 | Yes: No: Version: |
| SWU | Yes: No: Version: |
| Assistant | Yes: No: Version: |
| Gateways (HG35xx, SoftGate) | Yes: No: Version: |
| ComWin<br>(OpenScape 4000 Expert Access) | Yes: No: Version: |
| **Central Components**<br>Hardware | Yes: No: Version: |
| BIOS | Yes: No: Version: |
| Operating System | Yes: No: Version: |
| **Clients**<br>Web Browser | Yes: No: Version: |
| **Extending and 3rd party components**<br>OpenScape FM | Yes: No: Version: |
| Accounting Management | Yes: No: Version: |
| DS-Win | Yes: No: Version: |
| DTB | Yes: No: Version: |
| References | Updates Manual [1] Installation and Service Manual [6] |
| Customer Comments and Reasons | |

# 3 Server Hardening

## 3.1 BIOS Settings

BIOS is not delivered by Unify, thus the BIOS hardening is up to the customer, but Unify proposes hardening procedures that should be executed by the customer.

| CL-BIOS | BIOS |
|---|---|
| Measures | Set BIOS Password on OpenScape 4000 Server according to your password policy, in order to avoid unauthorized change of BIOS configuration. BIOS Password can be changed within the BIOS settings. The computer displays how to enter the BIOS during startup. Setting Boot password is not recommended, because it would not allow rebooting the server without physical access to the system keyboard to enter the boot password.<br>Disable booting from USB flashdisk or DVD. This option can be changed within the BIOS settings. The computer displays how to enter the BIOS during startup. Booting from DVD may be necessary for SLES operating system installation and upgrade. If you install software from a DVD please take in account that booting from DVD must be enabled.<br>Disable booting from Network. This option can be changed within the BIOS settings. The computer displays how to enter the BIOS during startup. |
| References | |
| **Needed Access Rights** | Administrator |
| **Executed**<br>BIOS Password<br>Boot from USB flashdisk or DVD<br>Boot from Network | Yes: No:<br>Yes: No:<br>Yes: No: |
| Customer Comments and Reasons | |

## 3.2 OS Hardening

The operating system used for OpenScape 4000 Manager V10 is SuSE Linux Enterprise Server 11 (SLES11) Service Pack 4 (SP4).

The OS is not delivered by Unify, thus the hardening of the OS is up to the customer, but Unify proposes hardening procedures that should be executed by the customer.

To prevent buffer overflow attacks it is strongly recommended to keep the Address Space Layout Randomization (ASLR) and the Executable Space Protection (NX) enabled in the SLES kernel.

SuSE SLES has ASLR and NX enabled per default.

### 3.2.1 Disable IPv6

If IPv6 connectivity is not needed, it can be disabled.

| IPv6 | IPv6 |
|---|---|
| Measures | 1. Run YaST typing "yast" in your shell.<br>2. Navigate to *Network Devices -> Network Settings -> Global Options -> IPv6 Protocol Settings.*<br>3. Uncheck the **[ ] Enable IPv6** box.<br>4. Confirm the change with OK.<br>5. Quit YaST |
| References | NA |
| **Needed Access Rights** | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

### 3.2.2 App Armor

The SuSE security tool AppArmor is supported from OpenScape 4000 Manager V10. Several pre-defined profiles are configured automatically by the Manager SW to comply with its requirements.

| CL-AppArmor | AppArmor |
|---|---|
| Measures | Please check that the AppArmor tool is installed on the SLES11 and the following profiles are disabled (not seen in apparmor_status output):<br>`/sbin/syslog-ng, /usr/sbin/ntpd, /sbin/klogd, /usr/lib/PolicyKit/polkit-grant-helper, /usr/lib/PolicyKit/polkit-read-auth-helper` |

| CL-AppArmor | AppArmor |
|---|---|
| References | Installation and Service Manual [6] chapter 3.11.2.4 Selecting software packages |
| **Needed Access Rights** | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 3.3 Operating system user accounts

For all customer defined accounts, please mind to follow these steps:

- set access right settings for user accounts (read/write access to file system).
- Define OS password policies. The Manager V10 password policy can serve as an example for that. Please refer to this document's chapter Password Policies.
- replace default passwords

***NOTE:*** Manager V10 specific accounts are listed in the appendix in this document's chapter Default Accounts' passwords.

| **CL-SrvPwd<br>Desktop and other<br>Server PCs** | **Access to the server / PCs are protected by passwords.** |
|---|---|
| Measures | • Customer specific password policy is defined<br>• The default passwords are replaced by individual passwords<br>• Access right settings for user accounts are done (read/write access to file system). For the protection of the data stored locally (e.g. in file systems) the user accounts shall only have limited access rights. |
| References | Manager V10 password policies, see chapter Supported Password Policy<br>Manager V10 default accounts see chapter Password Policy agreed for customer's deployment |
| **Needed Access Rights** | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 3.4 Boot loader

Even before the operating system is booted, boot loader GRUB enables access to file systems. Users without root permissions can access files in your Linux system to which they have no access once the system is booted. To block this kind of access or prevent users from booting certain operating systems, set a boot password. Without a boot password, even root console access is possible for an attacker with physical access to the system.

| **CL-Bootloader**<br>**Desktop and other**<br>**Server PCs** | **Boot loader password is configured** |
|---|---|
| Measures | IMPORTANT: If you use a boot password for GRUB, the usual splash screen is not displayed.<br>As the user root, proceed as follows to set a boot password:<br>At the root prompt, encrypt the password using grub-md5-crypt<br>`# grub-md5-crypt`<br>`Password: ****`<br>`Retype password: ****`<br>`Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/`<br><br>Paste the encrypted string into the global section of the file /boot/grub/menu.lst<br>`gfxmenu (hd0,4)/message`<br>`color white/blue black/light-gray`<br>`default 0`<br>`timeout 8`<br>`password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/`<br><br>Now GRUB commands can only be executed at the boot prompt after pressing P and entering the password. However, users can still boot all operating systems from the boot menu. |
| References | |
| **Needed Access Rights** | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 3.5 Virus Protection

Unify Baseline Security Policy recommendation can be found in “Support of Virus Protection Software for Server Applications” [2]. Trend Micro ServerProtect for Linux is recommended for OpenScape Manager 4000 V10.

| **CL-VirusProtect<br>Desktop and other Server PCs** | **Virus protection software is installed and active.** |
|---|---|
| Measures | Trend Micro ServerProtect is installed and active on the SLES 11 system. Complete scan has been executed. |
| References | [2] |
| Needed Access Rights | Administrator |
| Executed<br>**Server1** | Yes: No: |
| ... | Yes: No: |
| Customer Comments and Reasons | |

## 3.6 SLES11 internal firewall / SuSEfirewall2

SLES11 is supplied with an internal SuSE firewall which can close unused ports and limit access only to used listed ports and IP addresses. During the installation, the Manager preconfigures the SuSE firewall to open all Manager specific UDP and TCP ports on all network interfaces. However this is not considered to be final firewall configuration, thus firewall itself is not enabled by default and the configuration must be finished manually.

| **CL-SuSEfirewall2** | **SuSE firewall** |
|---|---|
| Measures | 1 Identify the deployment of Unify or 3rd party products accessing the Manager. Use IFMDB firewall report as input (see chapter TCP and UDP communication ports list) to identify the UDP and TCP ports really needed.<br>2 By default all Manager specific ports are preconfigured to be open on the firewall during the Manager installation. Please identify the ports (and CLAN interfaces if more than one) which are not needed and close them on the firewall using YaST.<br>3 Enable and configure internal firewall according to the actual deployment:<br>a Identify network interfaces (eventually peers' IP addresses) needed for communication between Manager and other products.<br>b Run YaST typing "yast" in your shell.<br>c Select Security and Users in left panel.<br>d Select Firewall in the right panel.<br>e Follow the firewall configuration wizard.<br>For a more precise SuSEfirewall2 configuration see SuSEfirewall2 Linux manual pages. |
| References | |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

# 4 Virtualization

OpenScape Manager V10 can be deployed inside VMware virtual machine. All VMware products, which support SLES11 SP4, are supported.

# 5 OpenScape 4000 Manager

## 5.1 PKI based authentication

Both password authentication and certificate based authentication are supported to login into the Manager WBM and SSH console. No PKI certificates are delivered with the Manager product. The customer must deliver his own PKI certificates and import them into the product.

PKI usage principles are described in service manual [7] appendix, PKI Manual The configuration of PKI authentication. Please get to know them before using PKI authentication mode. The PKI authentication mode can be selected in **Access Management > Security Mode Configuration.** Customer's certification authorities and revocation lists can be configured in **Access Management > Configuration of PKI Authentication.** Personal certificates can be assigned to user accounts in the **Access Management > Account Management > User Account Administration**.

| CL-PKI | PKI based authentication | |
|---|---|---|
| Measures | 1 | Prior to configuring PKI, please make sure the mode "Password and PKI authentication" is enabled. **Important:** Enable both authentication modes during system setup. Access to system can be blocked when configuration is not done properly and only PKI authentication is enabled. |
| | 2 | If your company already uses PKI based employees authentication, e.g. via smartcards, these can be reused for the Manager authentication. If not, please choose the appropriate certification authority and order the personal certificates to be used with Mgr. V10. |
| | 3 | Import your Root CA (that is the origin of the chain of trust) into the "Configuration of PKI Authentication". |
| | 4 | Import your Intermediate Certificate Authorities in the same place. |
| | 5 | Choose your preferred type of certificate validation control. Either Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) is supported. |
| | 6 | Assign the personal certificate to the user account in **Access Management > Account Management > User Account Administration** The certificates' common name list is maintained by your certification authority. |
| | 7 | When finished with user certificate assignment, please first test the PKI authentication functionality. Logout and try to re-login with your smartcard's certificate. |
| | 8 | If the test succeeded, it is safe now to disable the password authentication completely and enable the "Only PKI" mode. |
| References | [5] Access Management<br>http://en.wikipedia.org/wiki/Public-key_infrastructure | |
| Needed Access Rights | Administrator | |
| **Executed** | Yes: | No: |
| Customer Comments and Reasons | | |

## 5.2 Configure Password Policy

Passwords must have certain quality in order to avoid unauthorized access.
Password quality can be enforced using the configurable password policy.
The password policy rules are described in this document’s chapter Password Policies.

| CL-Password policy | Configure the Password Policy in accordance to customer’s defined Password Policy. |
|---|---|
| Measures | Configure the password policy according to the recommendation described in the chapter Password Policies |
| References | Access Management OpenScape 4000 Manager V10 Access Management (Assistant/Manager) online help is available from WBM, Chapter 2.7 |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

**Related Topics**

- Password Policies

## 5.3 Change predefined passwords for user accounts

During the installation all accounts are created with default passwords which are generally known. Thus, all passwords need to be changed upon first usage of the corresponding account.

| CL-Predef pass | Change default passwords for engr, rsta, rsca and cusa accounts |
|---|---|
| Measures | First please evaluate if all the accounts are necessary for administration. If not, lock unused accounts. For information on these accounts see Access Management [5], chapter 1.2.1.<br>The user is asked to change the password during the first log in with the engr account.<br>For each of the three other accounts please change the default password. |
| References | Access Management [5] chapter 2.7.1; chapter 3.3 |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 5.4 Change predefined passwords for NSL accounts

Network Single Logon (NSL) accounts are used for secure non-interactive communication between Manager and Assistant. During the installation all NSL accounts are created with default empty password. Thus, all passwords need to be changed to prevent unauthorized access to system. NSL accounts are not used for interactive login into the system.

NSL accounts are used for connection from the Manager to the assigned Assistant. When you change NSL password on the Manager, don't forget to change corresponding password on the Assistant. For Assistant see OpenScape 4000 Assistant V10 [10].

| CL-NSL pass | Change default passwords for NSL accounts – nsl-syst, nsl-engr, nsl-rsta, nsl-rsca, nsl-cusa and nsl-cust accounts. |
|---|---|
| Measures | A) For each of these accounts do separately:<br>1. Navigate to **Access Management > Account Management > System Account Administration.**<br>2. Select an account.<br>3. Enter a new password in **New password** and **Retype Password** fields.<br>4. Save using the button **Apply**<br>B) Set up the same password for all connected OS4k Assistants<br>1. Open **System Management -> OpenScape 4000 Administration,** click the button **Search** and select the first Object<br>2. Enable **Access Management** checkbox in Active Application table<br>3. New tabsheet **Access Management** will appear, go into it<br>4. Fill in the new password in the relevant field, you can use the option "Same value for all ... passwords" to simplify the task<br>5. Save the changes using the button **Save only**<br>6. Change the password for this account also in the Assistant's WBM - **System Account Administration**. The procedure is the same as for Manager - step A.<br>7. Repeat for all connected Assistants**.** |
| References | Access Management [5], chapter 2.9.1; chapter 3.5 |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 5.5 Create administrator accounts and assign privileges

You can create individual administrator accounts and assign them appropriate access rights. This enables you to manage user access to OpenScape 4000 Manager and accommodate users with sufficient rights.

| CL-Accom admins | Administrator Accounts |
|---|---|
| Measures | Create administrator accounts for customer administrators if needed and assign appropriate access rights:<br>1 In the **Access Management** navigate to **Account Management > User Account Administration.**<br>2 For each new user account do:<br>a Select **User > Add …** in menu.<br>b Enter user name, description and desired security profile<br>c Set password and/or password properties.<br>3 In the **Access Management** navigate to **Account Management > Access Right Configuration**.<br>4 For each new user account do:<br>a Select user in **Users** list.<br>b Select access rights in **Access Rights Groups** list to be assigned to the selected user.<br>c Select **Assign** in context menu.<br>d Check in the **Users** list that the access rights were assigned. |
| References | Access Management[5]., chapter 2.8; Chapter 3.5 |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 5.6 Security Mode Configuration

There are multiple security related enhancements configurable in the **Access Management > Security Mode Configuration**. Most of the Manager <--> Assistant connections like System Management, Configuration Management, Comwin, etc. are encrypted using SSL. However there still might be Manager - Assistant network communication which is not encrypted. Please refer to [5], to see how Security Mode features affect the communication between the Manager and the Assistant. Please mind that when switching to higher version of TLS (e.g. TLS 1.3) you might need to enable this protocol in the web browser configuration.

| CL-Security Mode | Security Mode configuration |
|---|---|
| Measures | For enhanced security, please consider to enable/disable the following option on the Access Management -> Security Mode Configuration page: |
| References | Access Management [5], chapter 2.8; Chapter 3.5 |
| Needed Access Rights | Administrator |
| **Executed**<br>Restricted access to system shell from "SSH connection to Manager" application | Yes: No: |
| Restricted access to Security Management API from customer network | Yes: No: |
| Support legacy HiPath 4000 systems (enable port 102) | Yes: No: |
| Disable unencrypted remote ODBC access (see ch. 6.3) | Yes: No: |
| Disable unencrypted remote JDBC access (see ch. 6.3) | Yes: No: |
| Customer Comments and Reasons | |

## 5.7 Legal Banner on Login Page

It is recommended to display a legal banner on the login page of OpenScape 4000 system. This information might be a warning banner, restriction information, system news or customer specific info. This can be done in the Access Management -> Customize Banner on Login Page. The banner is configurable both for WBM and SSH console.

| CL-Legal Banner | Legal Banner on Login Page |
|---|---|
| Measures | 1. Go to the Access Management -> Customize Banner on Login Page.<br>2. Define the text which will be displayed during each login.<br>3. Optionally enable the flag "User has to agree with message to continue login process". |
| References | Access Management [5] chapter 2.16 |
| Needed Access Rights | Administrator |
| **Executed** | |
| Display banner on Login Page | Yes: No: |
| User has to agree with message | Yes: No: |
| Customer Comments and Reasons | |

## 5.8 Backup and Restore - HBR

In Backup and Restore (HBR) component the backup can be made to the remote NFS or SFTP server. SFTP stands for Secure FTP based on SSH. The following Windows based SFTP servers are successfully tested with HBR:

Free edition of SilverSHielD SSH/SFTP server – Free SSH (SSH2) and SFTP server for Windows

- CopSSH
- KpyM
- SSHWindows
- CYGWIN OpenSSH

On Linux, the most common OpenSSH is supported. Nevertheless, others generally should work.

We recommend enforcing the use of SFTP per default instead of NFS

.

| CL-HBR | Backup Restore |
|---|---|
| Measures | In HBR – Administration - Backup Server configure the backup server via SFTP. |
| References | HBR user online help |
| Needed Access Rights | Customer |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 5.9 Apache Web Server

Since the web-server certificate and its private key are part of the general installation CD, each customer gets the same key material. It is recommended to the customer to use his own key material.

| CL-Apache own key | Provide own key material for SSL if possible. |
|---|---|
| Measures | Generate and activate web server SSL certificate as described in the documents below. |
| References | Service Manual [6], chapter 3.14.4 Generating and Activating an Individual Certificate<br>Access Management [5], chapter 2.11.1; Chapter 3.8 |
| **Needed Access Rights** | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

# 6 Extending and 3rd Party Components

Please refer to OpenScape 4000 Manager V10 Hardening Procedures in General for an overview over Unify OpenScape 4000 Manager extending software and 3rd party components in which security settings must be adapted at Manager installation time. It has to be outlined if the component is installed or not.

## 6.1 OpenScape Fault Management

The hipath_dbr account is created on the Informix RDBMS to establish JDBC access from the OpenScape Fault Management. By default hipath_dbr account is locked. Open and use this account only if OpenScape Fault Management is used. The password of the hipath_dbr account must be manually distributed to the Opencape Fault Management.

The OpenScape Fault Management should be preferably installed on the OpenScape 4000 Manager Server itself. In this case all Informix data including user authentication are transferred just locally and cannot be exploited. Otherwise it must be taken into account that JDBC is unsecured plain text protocol and the communication between OpenScape FM and Manager cannot be secured.

| CL-Opencape | Opencape FM JDBC account |
|---|---|
| Measures | Evaluate if OpenScape Fault Management is used:<br>1 If YES, then change the default password for account hipath_dbr:<br>a Navigate to **Access Management > Account Management > System Account Administration.**<br>b **Select hipath_dbr account.** Uncheck the checkbox **"Lock user account"**.<br>c Enter a new password in **New password** and **Retype Password** fields.<br>d Distribute the password of the hipath_dbr account to the OpenScape Fault Management according to valid OpenScape Fault Management documentation.<br>2 If NOT, you can optionally disable the unencrypted remote JDBC access completely, see chapter 6.3<br>3 Port 1527 must be opened for JDBC communication between OpenScape Fault Management and Informix DB. Evaluate on which position in the LAN the OpenScape FM and OpenScape 4000 Manager systems are deployed and configure SLES11 internal firewall and/or external firewall appropriately.<br>Note: The same deployment can exist with a 3rd party product using JDBC access to Informix DB. |
| References | Access Management [5], chapter 2.9.1; Chapter 3.5 |
| **Needed Access Rights** | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 6.2 Accounting Management, DS Win, DTB

Older version of HiPath Accounting Management, DS-Win and DTB communicate with OpenScape 4000 Manager using insecure FTP protocol. SFTP support on HP AM exists since HP AM V2 R6 Patch 27 therefore FTP is not activated by default and has to be activated manually. FTP server is not the secure way to connect to Manager Server. All data including authentication passwords are transferred in plaintext via FTP and thus can be intercepted. FTP should be used only if the customer agrees with the security risks involved.

If HiPath Accounting Management and/or DS-Win and/or DTB are used, install the applications preferably on the same LAN segment as OpenScape 4000 Manager Server or use newer version of the application, which supports SSH or SFTP protocol.

- HiPath AM V2.0 R6 Patch 27 or newer supports SSH/SFTP
- DS-Win V6 R6.10 or newer supports SSH/SFTP

| **CL-Accounting_Management** | **Accounting Management, DS Win, DTB** |
|---|---|
| Measures | If FTP is really needed, please activate it:<br>1 Make sure that vsftpd package is installed on SLES11. You can verify that by: „rpm -q vsftpd”. If vsftpd is not installed, use YaST -> Software -> Software Management to install it.<br>2 If the ftp connection is needed for a user with cust profile, there is workaround how to enable SSH/FTP access for him:<br>a add XIE access rights to user to create linux account but with /bin/false as default shell<br>b change default shell for account with command: usermod -s /bin/sh <account name><br>c Edit the following security configuration file if needed, make sure that users who will use FTP are **not** listed: /etc/ftpusers<br>3 For engr, rsta, rcsa users, the above documented steps are not needed.<br>4 Edit the following configuration files to allow ftp connection:<br>a /etc/xinetd.d/vsftpd:<br>disable=no<br>b /etc/vsftpd.conf:<br>write_enable=YES<br>local_enable=YES<br>anonymous_enable=NO<br>listen=NO<br>5 start the xinetd:<br>chkconfig -a xinetd<br>/etc/init.d/xinetd start<br>6 If xinetd is already active, restart is needed:<br>/etc/init.d/xinetd restart<br>7 Make sure the ports 20 and 21 are allowed in firewall. |
| References | |
| **Needed Access Rights** | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 6.3 Informix DB / 3rd party products connecting to Informix DB

The uas_read and uas_rdwr accounts are created on the Informix RDBMS to establish ODBC/JDBC access from 3rd party products.

3rd party products connect to Informix DB via ODBC/JDBC. This solution brings a risk because both authentication and data are transferred in plaintext.

By default uas_read and uas_rdwr accounts are locked. Open and use these accounts only if 3rd party products are used. Evaluate if 3rd party product needs read-only or read-write access to data stored on Informix DB and distribute the new passwords to them.

If 3rd party products are not used lock uas_read and/or uas_rdwr accounts with **Lock user account** checkbox.

Distribute uas_read and uas_rdwr accounts' passwords to 3rd party products according to the documentation obtained from the suppliers.

| CL-Informix clients | Informix DB / 3rd party products connecting to Informix DB |
|---|---|
| Measures | 1 Change default passwords for accounts uas_read, uas_rdwr.<br>1) On the **Start Page** of **OpenScape 4000 Manager** navigate to **Access Management > Account Management >System Account Administration**.<br>2) Select **uas_read** and/or **uas_rdwr** accounts. Uncheck the checkbox "Lock user account".<br>3) Enter a new password in **"New password"** and **"Retype Password"** fields.<br>4) save using the button **Apply**<br>2 Check proper function of 3rd party product using remote ODBC access to the port 1526 of Informix DB.<br>3 Configure server's and infrastructure firewalls according to the deployment. |
| References | Access Management [5] chapter 2.9.1; chapter 3.5 |
| Needed Access Rights | Administrator |
| **Executed**<br>1<br>2<br>3 | Yes: No:<br>Yes: No:<br>Yes: No: |
| Customer Comments and Reasons | |

# 7 Administration

## 7.1 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, digital certificates)
- 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**<br>**Organizational** | **Overall Password concept** |
|---|---|
| Measures | Rules for password handling are defined - see this document’s chapter Password Policies and apply the relevant security policies for administration |
| References | |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

| **CL-RoleConcept**<br>**Organizational** | **Overall Role concept** |
|---|---|
| Measures | Role concept is defined |
| References | |
| Needed Access Rights | Administrator |
| **Customer**<br>Name(s)/Role | Yes: No: |
| **Service**<br>Name(s)/Role | Yes: No: |
| Name(s)/Role | Yes: No: |
| Customer Comments and Reasons | |

## 7.2 Data Protection

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

In the OpenScape 4000 Manager also personal data and communication data are stored. Confidentiality has to be assured through protection of the administration. The backup data at USB drives or external servers has to be safeguarded as well.

| **CL-DataProtect Organizational** | **Access control to infrastructure and data storage** |
|---|---|
| Measures | Physical access to systems and storage devices is protected and access rules are defined. |
| References | See the Chapter 3.3 |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

## 7.3 Monitoring via SNMP

The Manager offers SNMP V3 interface. For its configuration see the OpenScape 4000 Manager V10, Installation and Service Manual [6] chapter 6.

This step is an administrative task, which is not performed once after installation but continuously during the operation of Manager V10 whenever new network elements are added for monitoring. It also involves the network elements themselves (see the relevant documentation of the monitored devices).

The Simple Network Management Protocol (SNMP) can be used for sending error messages from the monitored device to the SNMP server /host by trap.From the standard security point of view this is unproblematic.

If the SNMP server/host sends “get” or “set” advises to the monitored devices there is a risk for them. Thus in this case the SNMP interface should be configured more secure. See the details below.

### 7.3.1 SNMP v1, v2

In practical experience the SNMP v2c version from 1996 is used equivalent to SNMP v2.From the security point of view this version provides the same as SNMP v1. The SNMP v3 is supported by OpenScape 4000 Manager V10 and its usage is recommended. See this document’s chapter SNMP v3 for details.

A community string is available in SNMP v1 and SNMP v2. It is comparable to a user ID or a password and it allows access to statistical data of a device. The standard community string names „public" (read only; get) and "private" (read and write access; get, set) should be changed into individual names.By default trap managers make use of the community string “public”.

As the community string is transmitted in clear text, it can be eavesdropped easily. Thus also IP addresses of systems that may contact the monitored system via SNMP shall be restricted.

| CL-SNMPv1/v2 Manager | SNMP (v1, v2) security settings |
|---|---|
| Measures | A) Check if the SNMP v3 can be used. If yes, then please deactivate the SNMP v1,v2.<br>1. Navigate to Fault Management -> SNMP Configurator<br>2. Make sure that no community string is defined under the heading "SNMP V1 Configuration”<br>B) If SNMP v1 is required, set individual Community String name; delete default community string names **public** and **private**. |
| References | see Installation and Service Manual [6] chapter 6 |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: Deactivated |
| Customer Comments and Reasons | |

## 7.3.2 SNMP v3

OpenScape 4000 Manager V10, HiPath Accounting Management and OpenScape Fault Management can use SNMP v3.

It also involves the network elements themselves. They have to be configured to use SNMPv3. Other SNMP versions should be deactivated.

| CL- SNMPv3 | SNMP v3 security settings |
|---|---|
| Measures | 1. Please make sure that SNMPv3 is used for all devices which support it. To check/configure this, select “IP->Configuration” from context menu of the corresponding IP node object in OpenScape FM.<br>2. Also check if SNMPv3 is the only protocol activated on the device.<br>3. Activate secure Authentication<br>4. Activate Encrypted Communication<br>5. Define access classes for MIB sub trees<br>6. Activate SNMP over TLS<br>7. Activate SNMP over SSH |
| References | see Installation and Service Manual [6] chapter 6 |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

# 8 Infrastructure

## 8.1 Protection of network infrastructure

For the internal IP network, the requirements according to the administrator documentation 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-VLAN**<br>**LAN infrastructure** | **Protect infrastructure** |
|---|---|
| Measures | 1. Access to routers and switches only for authorized persons and trusted devices<br>2. Use separate VLAN for voice communication (optional) |
| References | |
| Needed Access Rights | Administrator |
| **Executed** | Yes: No: |
| Customer Comments and Reasons | |

# 9 Addendum

## 9.1 Password Policies

**Related Topics**

- Configure Password Policy

### 9.1.1 Supported Password Policy

OpenScape 4000 Manager V10 with extended password handling rules activated supports the Unify Password and Login Policies, described in relevant Unify OBSO documentation.
The following table lists Manager's available password policy configuration options.

| Password Policy Topic | Range |
|---|---|
| **Rules for Selection of Password** | |
| Minimal Length | 6 - 20 |
| Maximal password length that is supported by product (not security relevant, but implementation relevant) | min length – 20 |
| Minimal number of upper case letters | 0 – 20 |
| Minimal number of numerals | 0 - 20 |
| Minimal number of special characters | 1 - 20 |
| Minimal number of lower case letters | 0 – 20 |
| Use blacklist of strings which may not be contained in password (not configurable, blacklist provided by cracklib, list contains English words only) | always active when extended password handling rules active |
| Minimum character count for changed characters | 3 - 20 |
| Password history | 1 -10 |
| **Administrative Rules for Passwords** | |
| Maximum password age | 0 - 180 |
| Minimum password age | 0 - 30 |
| Password change requires knowledge of old password | always active, cannot be deactivated (except **engr** account) |
| Force change default passwords / PINs after the first use | true/false |

## 9.1.2 Switch to the Extended Password Policy:

1.Navigate to **Account Management > Account and Password Policy**

2.Check the checkbox **Use extended password handling rules**.

3.If necessary tune up the parameters of Password Policy.

4.Click **Save Changes**

These are the recommended criteria. Please implement them unless other company specific rules are defined at customer site.

| | | |
|---|---|---|
| Minimum length of the password | 15 | characters |
| Password must contain at least | 1 | upper case letters |
| Password must contain at least | 1 | lower case letters |
| Password must contain at least | 1 | numbers |
| Password must contain at least | 1 | special characters |
| Password history length | 10 | passwords |
| Minimum time between password changes | 1 | days |
| New password must differ from previous password by at least | 4 | characters |

***NOTE:*** Do not use trivial or easy to guess passwords. Take care that password entry cannot be observed.

## 9.1.3 Password Policy agreed for customer’s deployment

| | | |
|---|---|---|
| Minimum length of the password | | characters |
| Password must contain at least | | upper case letters |
| Password must contain at least | | lower case letters |
| Password must contain at least | | numbers |
| Password must contain at least | | special characters |
| Password history length | | passwords |
| Minimum time between password changes | | days |
| New password must differ from previous password by at least | | characters |

## 9.2 Default Accounts’ passwords

Here are the Manager default accounts including accounts for other systems that can access the OpenScape 4000 Manager. Each product listed in the Security Checklist should be represented here as well.

***NOTE:*** Each account is either locked after the installation or a default password is available.

***NOTE:* Be aware that most successful attacks to Unify systems base on unchanged default passwords. Since the default passwords are publicly available, it is absolutely necessary to change them into customer specific passwords immediately after installation process.**

The following shall be described for every account:

- Component, that provides this account (e.g. database…)
- Purpose (e.g. administration, diagnostics, …)
- Privileges (read/write access to the following components…)
- Change instruction for password (refer to manual where it is described how the password can be changed).

### 9.2.1 System Accounts

| # | User Name | Password Policy configured | Unify Default Password (to be changed immediately) | Description |
|---|---|---|---|---|
| 1 | hipath_dbr | Yes, as agreed in this document’s chapter Password Policy agreed for customer’s deployment | account is locked by default | Informix DB account for OpenScape FM JDBC access. |
| 2 | uas_read, uas_rdwr | Yes | locked by default | The uas_read and uas_rdwr accounts are created on the Informix RDBMS to establish ODBC/JDBC access from 3rd party components. |
| 3 | nsl-syst<br>nsl-engr<br>nsl-rsta<br>nsl-rsca<br>nsl-cusa<br>nsl-cust | Yes | <empty> | NSL accounts are used for secure non interactive access, e.g. communication between Manager and Assistant. |

| # | User Name | Password Policy configured | Unify Default Password (to be changed immediately) | Description |
|---|---|---|---|---|
| 4 | ncc | No, password policy does not apply for this account and the maximum password length is limited to 8 characters. | <empty> | ncc account is used for OpenFT file transfer of batchjob result from RMX to Manager |
| 5 | apeftp | No | locked by default | not used on Manager (Assistant only) |

## 9.2.2 User Accounts

| # | User Name | Password Policy configured | Unify Default Password (to be changed immediately) | Description |
|---|---|---|---|---|
| 1 | engr<br>rsta<br>rsca<br>cusa | Yes, as agreed in this document's chapter Password Policy agreed for customer's deployment | 4K-admin | These are predefined accounts for OpenScape 4000 Management V10 service access. |
| 2 | sso | No, not needed, account is locked | locked by default | Account sso is used for access to configuration of the feature Smart Switch Over. Configuration menu is invoked immediately after login with this user via ssh. |

## 9.2.3 Default OS (SLES 11) Accounts

| # | User Name | Password Policy configured | Unify Default Password (to be changed immediately) | Description |
|---|---|---|---|---|
| 1 | root | Customer password policy should be applied | - | root account shouldn't be allowed from remote access. It should not be used directly for system maintenance if not necessary. Account 'engr' should be used instead. |

## 9.3 Certificate Handling

**WARNING: Since the default certificates don't even fulfill minimum security requirements, it is absolutely necessary to change them into customer specific certificates immediately after installation process.**

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

The product handles the following types of certificates:

| # | Type/<br>Interface | Customer requirement for OpenScape 4000 Assistant V10 credentials | Expiration Date for Customer specific key material | Unify Default<br>Credentials | Usage/Comment |
|---|---|---|---|---|---|
| 1 | PKI | | | none | Application: client authentication – for login into WBM.<br>PKI is used when authentication mode is "Only PKI" or "Password and PKI". Customer delivered PKI is supported. See chapter PKI based authentication |
| 2 | SSL on server | | | delivered, issued by<br>**Unify I&C Security CA** | Application: used over HTTPS for encryption and server authentication, e.g. apache web server authentication and traffic encryption, i.e. web based management, Tomcat Servlets, etc., authentication and encryption of various application daemons to Java Applet clients.<br>Since the web-server certificate and its private key are part of the general installation CD, each customer gets the same key material. This key material is not used for client authentication, but for web server authentication only. It must be replaced after installation. |

***NOTE:*** Please make sure that pre-shared keys and certificates are stored and transmitted confidentially.

# 10 TCP and UDP communication ports list

***NOTE:*** IMPORTANT: It is not the purpose of this section to list all available ports in the OpenScape 4000 V10 but rather to provide a hint on how to automatically produce them in a structured manner by using the IFMDB tool. Please follow the steps below once logged on to the Unify Partner Portal.

OpenScape 4000 V10 port list is published in the Interface Management Data Base (IFMDB).

To get all information that is necessary for the Security Checklist Port list you should proceed the following way in IFMDB:

**Step by Step**

1. Go to "Reports -> Firewall Scenario" screen
2. Select Entity for the Left side of firewall, for example, select “OpenScape 4000 Assistant”
3. Select SW- Version: for example, select latest release of “OpenScape 4000 Manager V10 <XX>”
4. Select Interfaces: select both NormalMode and SecureMode interfaces via the checkboxes
5. Select Entity and its interfaces for the Right side of the firewall: for example, “OpenScape 4000 Manager V10 <XX>”
6. choose the Detail level and Style template to be used. Choose Excel format optionally.
7. click Continue to generate your report.

# 11 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

**[2] Interface Management Database (IFMDB)**

available via SEBA Portal

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

**[4] Access Management**

OpenScape 4000 Manager V10 Access Management (Assistant/Manager) online help is available from WBM

**[5] Installation and Service Manual**

OpenScape 4000 Manager V10 Installation and Service Manual, available via SEBA Portal

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

**[6] The configuration of PKI authentication**

service manual appendix

https://www.g-dms.com/livelink/livelink.exe?func=ll&objId=58564427&objAction=download

**[7] HiPath Secured Infrastructure for Remote Access (SIRA) V1.0, Equipment Explorer, Administrator Documentation, Issue 7**

http://apps.g-dms.com:8081/techdoc/en/P31003S8210A1040176A9/wwhelp/wwhimpl/js/html/wwhelp.htm?href=wwh3master.html

**[8] OpenScape 4000 Assistant V10 Security Checklist**

available via SEBA Portal

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