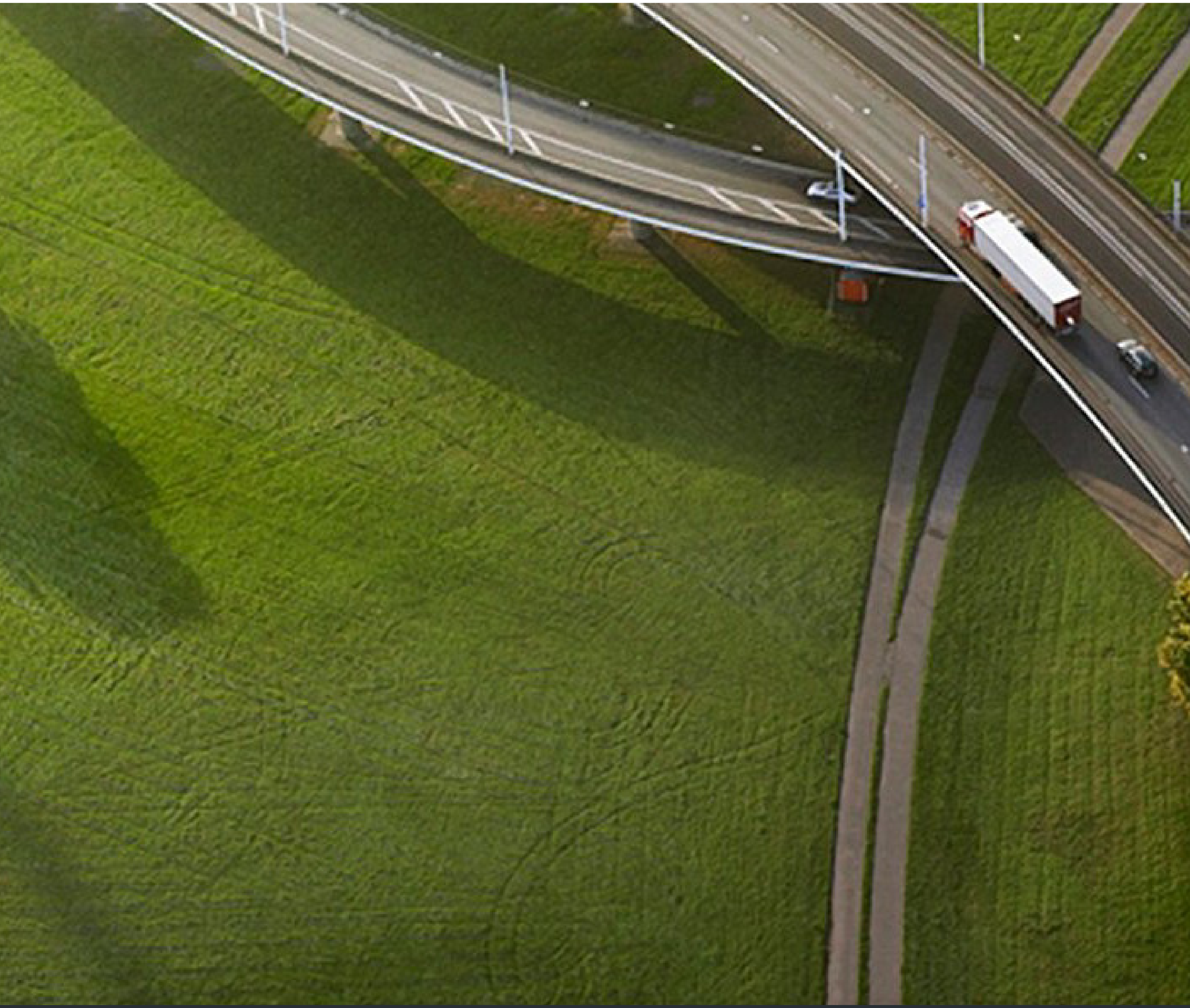

Circuit Meeting Room Security Checklist

Planning Guide

P31003-A4012-P100-01-76A9

Provide feedback to further optimize this document to edoku@unify.com.

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.

Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany

Reference No.: P31003-A4012-P100-01-76A9

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.

unify
atos collaboration solutions

unify.com

Table of Contents

1. Introduction

1.1. 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.

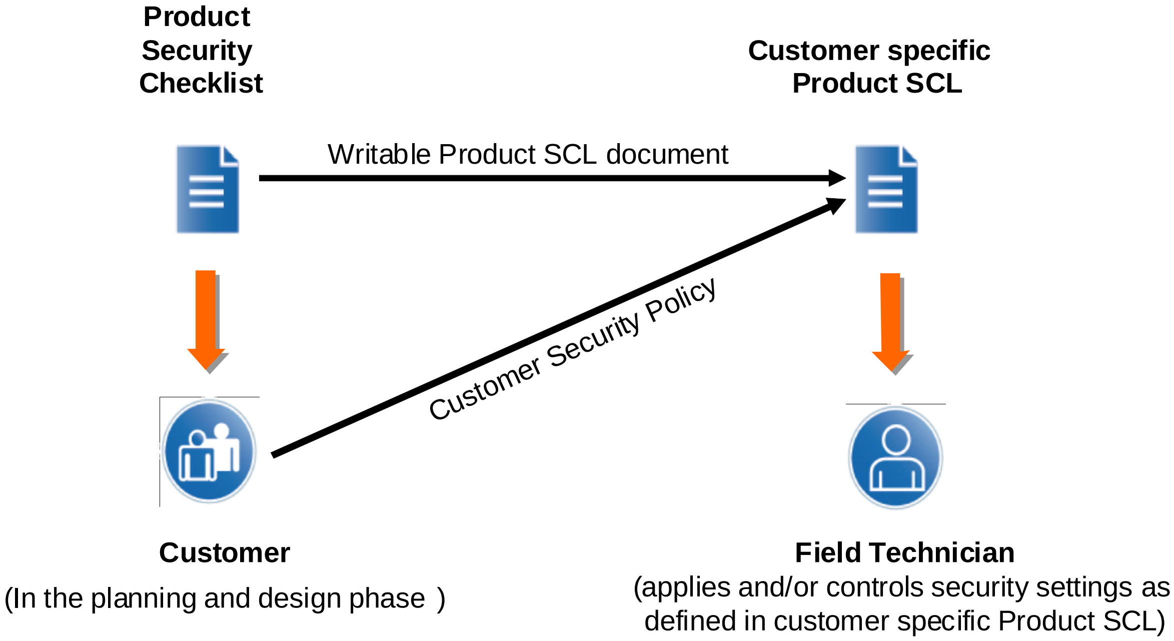
Product Security Checklist
Customer specific Product SCL
Writable Product SCL document
Customer Security Policy
Customer
(In the planning and design phase)
Field Technician
(applies and/or controls security settings as defined in customer specific Product SCL)

Figure 1: Usage of Security Checklists (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
- 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@unify.com).

1.2. 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.

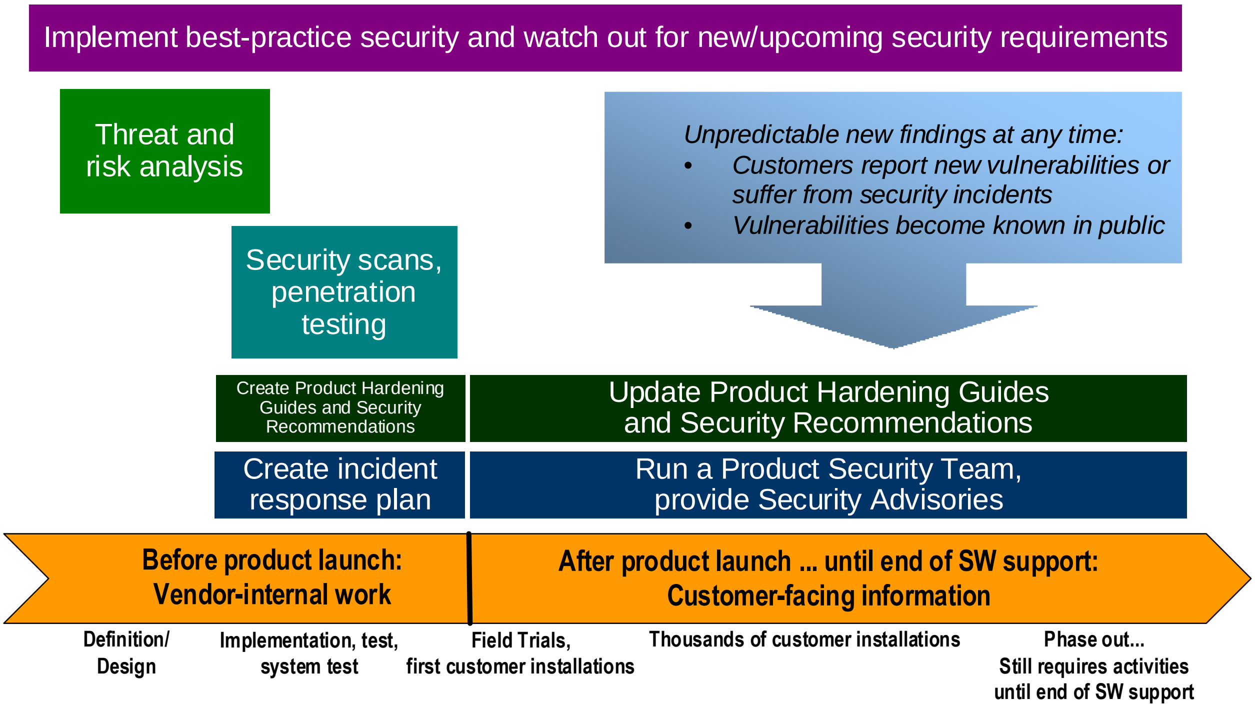
Implement best-practice security and watch out for new/upcoming security requirements
Threat and risk analysis
Security scans, penetration testing
Unpredictable new findings at any time:
• Customers report new vulnerabilities or suffer from security incidents
• Vulnerabilities become known in public
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

Figure 2: Unify Baseline Security Policy - from Design to EOL

For more information about the Unify product security strategy we refer to the relevant Security Policies [3], [4], [5].

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.

1.3. Customer Deployment - Overview

This Security Checklist covers the product Circuit Meeting Room and lists its 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 Remarks		
Open Issues to be solved until		
Date		

2. Circuit Meeting Room Interfaces and Ports

Considering hardening for Circuit Meeting Room all interfaces and ports have to be analysed.

The interfaces for the Circuit Meeting Room device are shown in a landscape diagram below. Complete information about used interfaces/IP ports is part of the release notes as well as from the Unify Partner Portal (http://www.unify.com/us/partners/partner-portal.aspx).

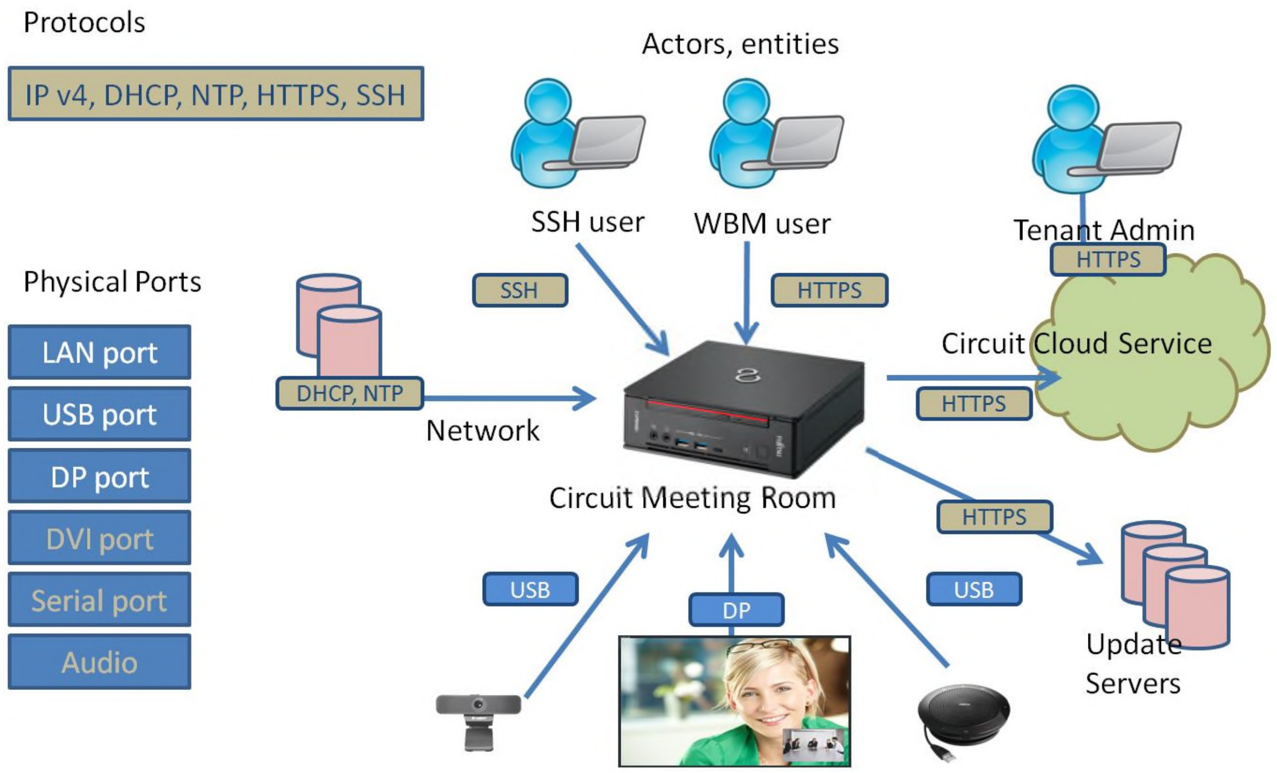

Figure 3 Circuit Meeting Room Interfaces

3. Device Hardening Measures at a Glance

To improve the security on Circuit Meeting Room the following measures are recommended:

- Device Administration
  - Secure local device administration
    - Physical access (Kensington Lock)
    - Set BIOS password
  - Hardening of web-based management
    - Set password (this is enforced when you first log in with the factory password)
    - Install customer individual WBM certificate and private key

- Install latest ("Up-to-date") Circuit Meeting Room software during initial setup phase.

  The Circuit Meeting Room comprises of two major SW components:
  - The Operating System and related SW ("Dashboard")
  - The Circuit App.

  The two components have different options and sources for updates:
  - The Operating System and related SW (including a version of the Circuit App) can be downloaded from the Unify Software Supply Server in the Internet (recommended) or the Unify Partner Portal (http://www.unify.com/us/partners/partner-portal.aspx).
  - The Circuit App can be downloaded from the Circuit Cloud.

  How to upgrade those components:
  - You can log into the web administration pages of the Circuit Meeting Room (Dashboard) and trigger an online update of the Operating System and related SW (including a version of the Circuit App) from the Unify Software Supply Server. Or you can first download the Operating System and related SW (including a version of the Circuit App) from the Unify Partner Portal to a local computer in your network, and then log into the Dashboard, select the files and submit for installation. This is an offline process.
    The Circuit App is automatically updated.

The recommended measures are listed in the following chapters.

4. Device Hardening Measures

4.1. Set BIOS password

The BIOS comes with some default options which shall not be changed during normal operation, e.g. no boot is allowed from removable media. In order to protect these settings a BIOS password shall be set during initial installation.

CL – BIOS PW	Set BIOS (CMOS) password
Measure	• Plug in a standard USB keyboard • Press F2 and hold down while you power up the device • Navigate to "Security", then "Administrator Password" and press "return" key to open Edit field. Type in password, and complete this via "Save and Exit" option. This will exit the BIOS and re-start the device automatically.
References	None
Needed Access Rights	None
Executed:	Yes: ☐ No: ☐
Customer Comments and Reasons. If some measures are not executed then please explain here:	

4.2. Set Initial password for the Web Administration Pages (Dashboard)

CL – Dashboard PW	**Set password for Dashboard access**
Measure	When the initial configuration is done and the user logs in to the Dashboard for the first time, a setup wizard is started. The wizard enforces a new password matching the password policy.
References	Configuration Guide
Needed Access Rights	Administrator
Executed:	Yes: □ No: □
Customer Comments and Reasons. If some measures are not executed then please explain here:	

4.3. Install customer certificate for the Web Administration Pages (Dashboard)

For improved security it is recommended to perform the initial configuration of the Circuit Meeting Room in a separate staging lab.

Administration of the Circuit Meeting Room is done via Web configuration pages (“Dashboard”) provided by a built-in web server. Access to this web server is done via HTTPS. Attempts to access using the standard HTTP port are automatically redirected to HTTPS.

On delivery, a default Web Server certificate is provided on Circuit Meeting Room for accessing the Dashboard. This must be replaced with a customer generated certificate.

CL – Dashboard Certificate	**Install customer certificate for Dashboard**
Measure	Replace the factory certificate by a customer certificate for the device. This step requires working with the Dashboard, so for security reasons: • Either use a local keyboard/mouse and USB stick or • setup device in a staging are when using remote access to Dashboard
References	Configuration Guide
Needed Access Rights	Administrator
Executed:	Yes: ☐ No: ☐
Customer Comments and Reasons. If some measures are not executed then please explain here:	

4.4. Install latest ("Up-to-date") Circuit Meeting Room Software (Operating System)

The latest ("up-to-date") released Circuit Meeting Room software version should be installed during initial setup. The software is ready to download directly from the Unify Software Supply Server or from the Unify Partner Portal (http://www.unify.com/us/partners/partner-portal.aspx).

CL – Update OS	**Operating System Update**
Measure	When the user logs in to the Dashboard for the first time, a setup wizard is started. The wizard checks for updates and prompts for installation of the latest version. The user can also download and install offline the latest Operating System software (which includes the Dashboard and a version of the Circuit App).
References	Configuration Guide
Needed Access Rights	Administration password
Executed:	Yes: □ No: □
Customer Comments and Reasons. If some measures are not executed then please explain here:	

4.5. Protect Circuit Meeting Room Hardware (Theft Protection)

CL – Kensington Lock	**Kensington Lock – Theft Protection**
Measure	Lock the Circuit Meeting Room at its installation location (prevent HW manipulation as well as theft protection).
References	Configuration Guide
Needed Access Rights	None – only physical access to the device
Executed:	Yes: □ No: □
Customer Comments and Reasons. If some measures are not executed then please explain here:	

4.6. Minimize Secure Shell access to the Device

The Secure Shell interface is reserved for technical specialists. **It is deactivated by default and can be enabled by the Administration user via Dashboard for each access.** It is enabled for a limited period of time only, and a password is set for the access. A different password should be used for each access and the time interval should be set reasonable short (e.g. as needed by the technical specialist). To prevent all access via secure shell, the secure shell access is disabled per default and its control is protected by the Dashboard password which is set during the initial setup.

CL – SSH Minimized Access	**4.9. Minimize Secure Shell access to the Device**
Measure	• Activate SSH only when required (e.g. trouble shooting with technician) • Do not provide administration password for Dashboard to unauthorized people / use temporary password if remote access is required for authorized technician.
References	Configuration Guide
Needed Access Rights	Administration password
Executed:	Yes: □ No: □
Customer Comments and Reasons. If some measures are not executed then please explain here:	

5. Addendum

5.1. Default Accounts

There is one default account for the Web Administration pages – the factory password is: Admin%123

A change is enforced upon first usage.

5.2. Password and PIN Policies

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. Circuit Meeting Room technically supports the password policy depicted in Table 1.

This policy is applied to both Web Administration pages and SSH access.

Table 1 Password Policy supported by Circuit Meeting Room Device

#	Password policy of Circuit Meeting Room	Value
1	Minimal length	8
2	Maximal length	20
3	Minimal number of upper case letters	1
4	Minimal number of lower case letters	1
5	Minimal number of numerals	1
6	Minimal number of special characters	1
7	Password change requires knowledge of old password	Yes
8	Force change default passwords after the first use	Yes

5.3. Port Table

For latest updates of the Circuit Meeting Room port tables refer to the Interface Management Database (IFMDB) via Unify Partner Portal.

Use the link http://www.unify.com/us/partners/partner-portal.aspx, go to Menu item “support” and then click IFMDB in the pull down menu.

6. References

- Circuit Meeting Room administrator documentations
  https://www.unify.com/us/partners/partner-portal.aspx
  https://www.circuit.com/support
- Interface Management Database (IFMDB**)** available via Unify Partner Portal
  https://www.unify.com/us/partners/partner-portal.aspx
- Circuit Meeting Room on Unify expert wiki
  http://wiki.unify.com/wiki/Devices