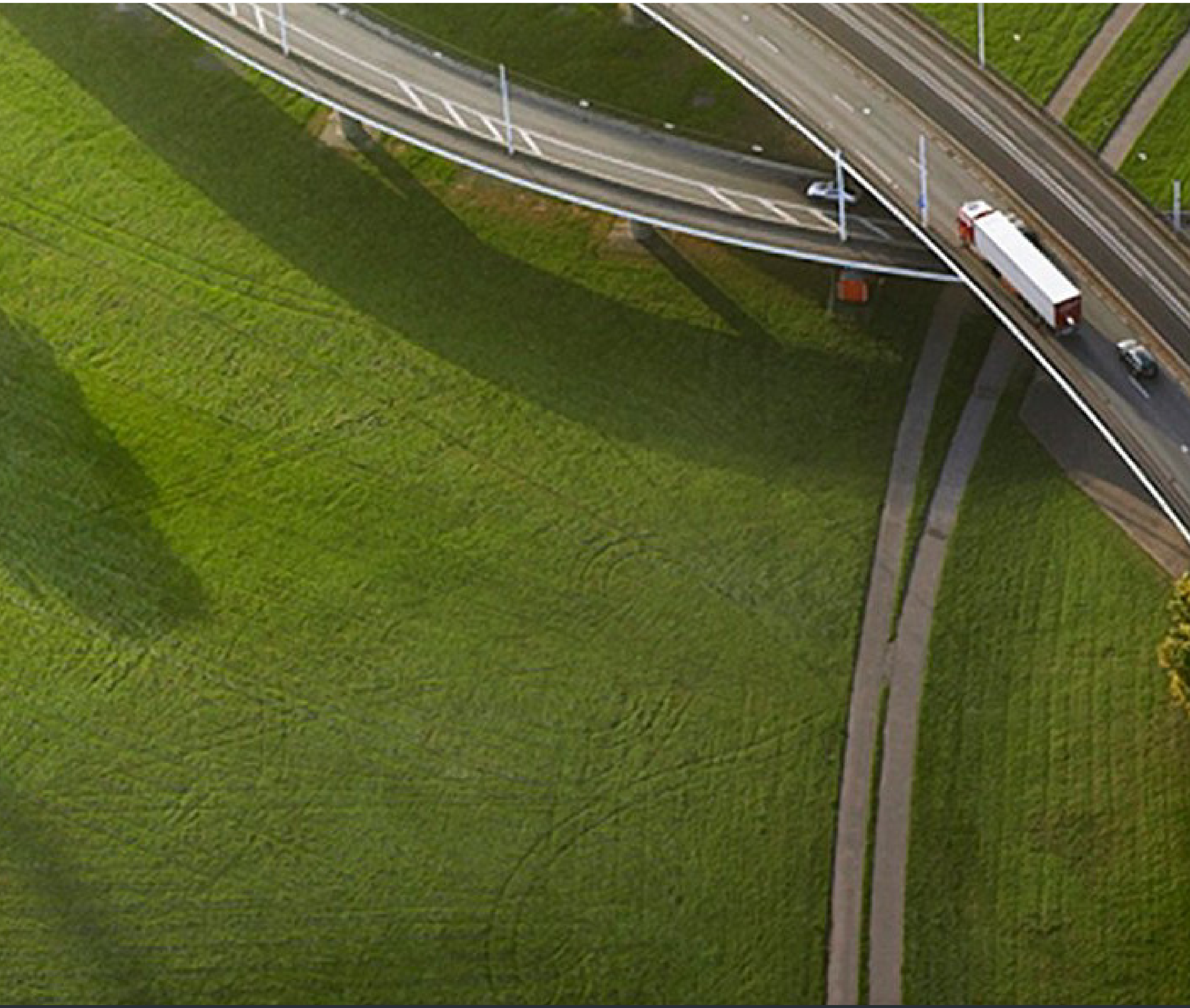


OpenScape WLAN Phone WL4 / WL4 Plus
Security Checklist

Planning Guide

A31003-M2000-P104-02-76A9

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.

Reference No.: A31003-M2000-P104-02-76A9

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.

unify atos collaboration solutions

unify.com

Contents

1 Introduction 4
1.1 General Remarks 4
1.2 History of Change 5
1.3 Customer Deployment - Overview 5

2 WL4 Hardening Procedures in General 7

3 WL4 Mobile Phone 9
3.1 Secure Voice over IP Communication 9
3.1.1 Activate Signalling and Payload encryption 9
3.1.2 Connection to Wireless LAN infrastructure 9
3.2 Configuration of WL4 10
3.2.1 WinPDM (Windows Portable Device Manager) 10

4 Addendum 11
4.1 DefaultAccounts 11
4.2 WiFi Connection 11
4.3 Certificate Handling 11
4.4 Port Table 12

5 References 13

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

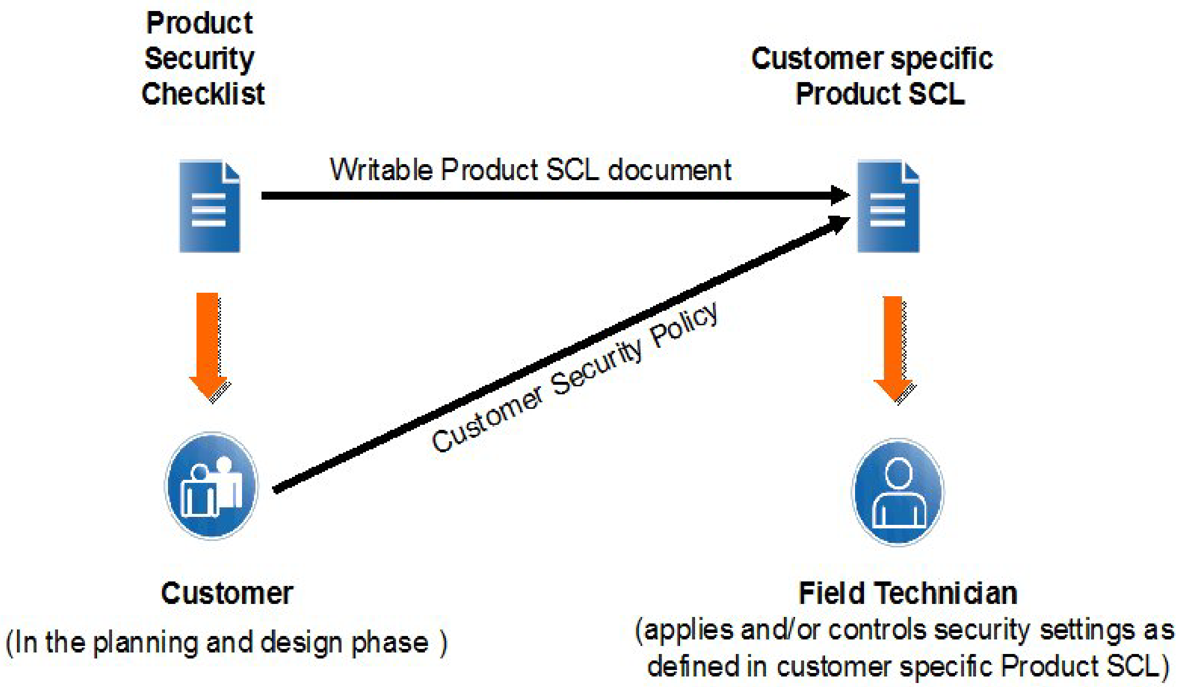
- to adapt these default settings to the needs of the individual customer and the specific characteristic of the solution to be deployed
- to weigh the costs of implementing security measures against the risks of omitting a security measureand to “harden” the systems appropriately.

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 .
- 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).

1.2 History of Change

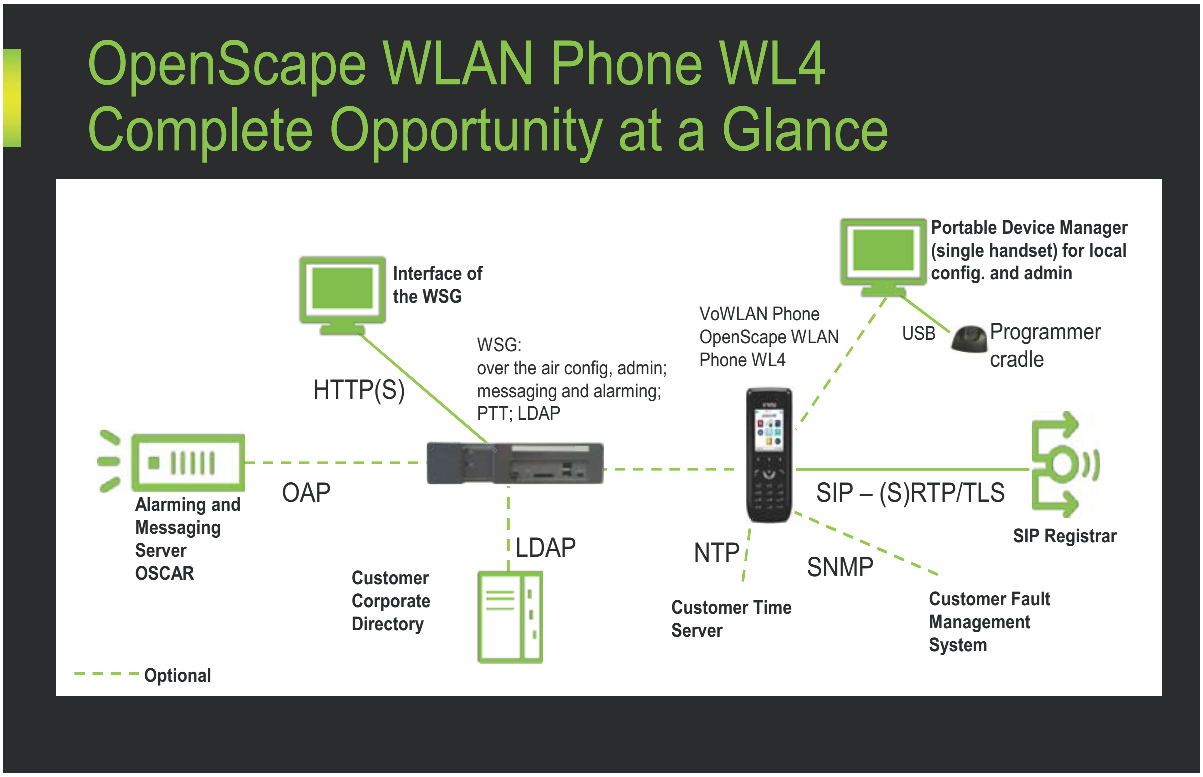
Date	Version	What
2020-06-24	1.0	Released for Version1

1.3 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 WL4 Hardening Procedures in General



OpenScape WLAN Phone WL4
Complete Opportunity at a Glance

Interface of the WSG
HTTP(S)
WSG: over the air config, admin; messaging and alarming; PTT; LDAP
VoWLAN Phone OpenScape WLAN Phone WL4
Portable Device Manager (single handset) for local config. and admin
USB
Programmer cradle
Alarming and Messaging Server OSCAR
OAP
LDAP
Customer Corporate Directory
SIP – (S)RTP/TLS
SIP Registrar
NTP
Customer Time Server
SNMP
Customer Fault Management System
Optional

The administration of the handset(s) is done centralized via the WSG (“Wireless Service Gateway”) server or via the so called WinPDM (“Windows Portable Device Manager”). For configuration via WinPDM, the phone is connected via a USB cradle to the PC which runs the WinPDM software.

CL-SWStatus	Up-to-date SW
Measures	Ensure that the WL4 and WinPDM software is up-to-date
References	
Needed Access Rights	**“admin”** or **“sysadmin”** account
Executed **WL4 (Basic or Plus)**	Yes: □ No: □
WinPDM	Yes: □ No: □
Customer Comments and Reasons	

3 WL4 Mobile Phone

The **WL4 Basic** and the **WL4 Plus** are two different products. Both phones have the same hardware but different firmware. While most of the functionality is the same for both, the “Plus” variant offers an alarming and messaging service. This feature is coupled with the proprietary OAP protocol which communicates with the OSCAR Alarming & Messaging server. The messaging service can be added to the WL3 Basic as well, by buying a corresponding license. This is not possible for the alarming service.

All statements related to security settings, apply for both products, if not stated else.

3.1 Secure Voice over IP Communication

3.1.1 Activate Signalling and Payload encryption

For confidentiality and integrity of VoIP communication, the activation of signalling and payload encryption shall be considered. The optional certificates that can be deployed on the phone.

CL-SPE	Signalling and Payload Encryption
Measures	Ensure that the WL4 and WinPDM software is up-to-date
References	
Needed Access Rights	**“admin”** or **“sysadmin”** account
Executed	Yes: □ No: □
Customer Comments and Reasons	

3.1.2 Connection to Wireless LAN infrastructure

Ensure that at least “WPA2 – PSK” (Pre-Shared Key) encryption is chosen. An even more secure approach is, to use “WPA2” (sometimes also called “WPA2 – Enterprise”). This is a RADIUS – server based authentication / encryption method and currently represents the most secure way to connect to a WiFi infrastructure. In this case certificates must be deployed on the handset either via WinPDM or via WSG.

CL-WiFi	WiFi Encryption
Measures	Ensure that WPA2-PSK or WPA-Enterprise is used
References	WL4 Manual
Needed Access Rights	**“admin”** or **“sysadmin”** account
Executed	Yes: □ No: □
Customer Comments and Reasons	

3.2 Configuration of WL4

The handset configuration can be done either via the WSG (this is thought for sites with a huge number of deployed phones) or via WinPDM (for a few Phone only).

3.2.1 WinPDM (Windows Portable Device Manager)

"WinPDM" is a PC software that is used to configure a handset via a USB cradle. Since this method requires physical access to the device, unauthorized access can easily be prevented.

CL Pwd	Overall Password concept
Measures	Admin password has been changed
References	WL4 admin documentation for customizing of PW Policies Addendum: chapter Default accounts
Needed Access Rights	Depending which passwords should be changed **“admin”** or **”sysadmin”** account.
Executed	Yes: □ No: □
Customer Comments and Reasons	

4 Addendum

4.1 DefaultAccounts

#	User Name	PW Policy configured	Unify Default PW (to be changed immediately)	Description
1	admin	Yes	changeme	Required for accessing some parts of the Webpage. Required for WSG access

INFO: Since the default passwords 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.

4.2 WiFi Connection

These factory defaults are configured on the handset for connecting to a WiFi network.

#	Parameters	Customer requirement for WL4 credentials	Unify Default credentials	Usage
1	SSID		AWS-INIT	Name of the WiFi network
2	Passphrase		AWS-INIT	Used for WPA-PSK and for WPA-PSK encryption

4.3 Certificate Handling

TLS can be used for WiFi authentication and encryption.

#	Interface	Customer requirement for WL4 credentials	Unify Default credentials	Usage
1	WiFi Connection		None	WiFi Infrastructure authentication and encryption.

4.4 Port Table

For latest updates of the port tables see IFMDB directly:

https://enterprise-businessarea.unify.com/portal/authsec/portal/cp/Home/CFEDBB57-913D-4C6D-9C1C-E21F663D3074/4F73C339-1ACF-4A59-B49C-94C18478C54A/3F396FA0-B9D2-4AD7-BAA0-F293D84ADA68/29F636BE-67EF-47B3-89B7-E7D5129614C6

or via SEBA portal.

5 References

WL4 Manual

available via e-Doku or SEBA Portal / product information

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

WSG Manual

available via e-Doku or SEBA Portal / product information

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

Interface Management Database (IFMDB)

available via SEBA Portal

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

Centre of Internet Security – Security Benchmarks

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