A MITEL
PRODUCT
GUIDE

OpenScape Solution Set V11

Customer Data Collection with WebCDC V1

Security Checklist
07/2025

A31003-S11A0-P101-01-76A9

Mitel

Notices

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

Trademarks

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

Contents

1 Introduction

1.1 General Remarks

Seamless integration of information and communication within Unified Communications and Collaboration (UCC) provides an important asset to an enterprise and forms a valuable core for their business processes. Accordingly, they must be adequately protected. Every enterprise may require a specific level of protection, which depends on individual requirements for availability, confidentiality, integrity and compliance of the IT and communication systems being used.

Unify attempts to provide a common standard of features and settings of security parameters within the delivered products. Beyond this, Unify generally recommends:

- 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 accordingly.

As a basis for that, the Security Checklists are published. They support the customer and the service both directly and indirectly, as well as those wanting to maintain it themselves, to agree on the settings and to document the decisions that are made.

The Security Checklists can be used for two purposes:

1. **In the planning and design phase** of a particular customer project.
   Use the Security Checklists of every relevant product to evaluate, 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 OpenScape Mobile Security Checklist containing customer alignments can be identified as Customer specific 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 and setup of the solution
   - During operation.
2. **During installation and during major enhancements or software upgrade activities:**
   The Security Checklists (ideally documented as described in step 1.) are used to apply and/or control the security settings of every individual product.

Update and Feedback

- By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included as soon as possible.
  Therefore, we recommend always using the latest version of the Security Checklists of the products that are part of your solution. They can be retrieved from our Partner Portal (formerly SEBA).

- We encourage you to provide feedback in any cases of unclarity, or problems with the application of this checklist.

Please contact the OpenScale Baseline Security Office (obso@unify.com).

1.2 Customer Deployment Overview

This Security Checklist covers the product WebCDC V1 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:	

	Customer	Supplier
General Remarks		
Open issues to be resolved until		
Date		

1.3 Security Model for WebCDC Environment

The security model adopted for WebCDC is based on the environment. The WebCDC server follows the Safe Environment Security Model, (i.e., the WebCDC server, the OpenScape devices, and the WebCDC users all reside on a network that is secured by company standards and WebCDC users access the WebCDC Portal from the same secured network.

Users connect to WebCDC server via the product portal and can use either:

- single sign-on using the corporate windows login credentials of the user or
- login using the credentials stored in the WebCDC application.

2 WebCDC Interfaces

2.1 WebCDC Overview

The WebCDC is a Windows application that is used to collect the customer data for an OSV solution and generate the configuration files for products such as OSV, OSB, OSSBC, UC, DLS, RG8700, Mediatrix, Xpr, OSCC and Concierge.

WebCDC is positioned behind a fire wall in the corporate network. Only one port 28081 is opened up for https access for WebCDC clients. A comprehensive list of opened ports for remote desktop connection for server maintenance (such as updates to the CDC versions) can be found in the Interface Management Data Base. WebCDC clients access the WebCDC application via web interface using https.

The following subsections give a brief description of external interfaces to WebCDC and the security aspects of each interface.

2.2 User - WebCDC Client

This is a web browser interface to the WebCDC server requiring user id and password.

Userid and password are administered by the WebCDC administrator. They are stored in a file (userid and hashed password) on the WebCDC server accessible by only an Administrative user logged in at the WebCDC server.

- Password complexity is enforced for WebCDC Web client as per the TSA guidelines
- WebCDC client login attempts are logged (user name, IP address, time).

The client can open up either a new project or an existing project and fill up the customer data, and generate the desired configuration files. These files can be uploaded to the local drive of the client.

2.3 WebCDC Client to WebCDC Server

This interface is a standard https using a "generic" self-signed certificate created for the WebCDC server using Open SSL. (The customer may install his own certificates later). The https interface is also used for transferring configuration files from the WebCDC server to the client PC local drive.

2.4 Local User to WebCDC Server

All users are defined with different privileges. The Administrator is the only user with privileges to access the SQlite database and to restrict access to other files/ functions as needed.

2.4.1 WebCDC Administrator

WebCDC Administrator is also a Windows Administrator whose user id and password are created at WebCDC server installation. WebCDC Administrator has access to all the files and data bases on the WebCDC server.

2.4.2 WebCDC Application User

WebCDC application also has an administrative access to the Windows server to install and upgrade the WebCDC application. No other windows user accounts are created on the WebCDC server.

3 WebCDC Hardening Measures at a Glance

To tighten security on the WebCDC server, the following measures are recommended:

- Windows 2008 Hardening
- Windows Administrator Accounts
  - Create one access group for Windows Administrator
  - Create a second access group, i.e., a Local User Account
- WebCDC default password
- Define packet filter rules that only allow incoming FTP traffic from specified-sources
- Block all ports not used by the WebCDC
- Define packet filter rules that only allow incoming FTP traffic from specified-sources

3.1 Windows OS Updates

Windows Server OS specific security updates are the responsibility of the administration team in charge of the WebCDC server. The Microsoft security updates must be applied as recommended by the vendor.

3.2 Windows Configuration Requirements

3.2.1 Windows Administrator Account

When Windows 2008 R2 is installed on the server, the "Administrator" local account is created by default. This account provides the rights required to administer the server's OS and all its applications.

During the installation process a password must be entered for this account. The password settings should follow the strictest procedures to protect its confidentiality.

4 Hardening

The security parameters indentified in the following sections should be configured for all WebCDC server installations.

4.1 3rd Party Applications and Window OS Updates

Security updates for WebCDC software components are made available only with new WebCDC releases via re-installation or via hot fixes if required and 3rd party applications that are part of the WebCDC are automatically updated.

Windows Server OS specific security updates are the responsibility of the administration team in charge of the WebCDC server. The Microsoft security updates must be applied as recommended by the vendor.

CL-WCDC-3rd_Party	**Verify 3rd Party Updates**
Measures	Verify that all security updates and latest versions of all3rd Party Applications have been installed.
References	Refer to the following documents:Refer to the 3rd party Application’s vendor website.
Needed Access Rights	administrator
Executed WebCDC:	Yes:  No: 
Customer Comments and Reasons	

4.2 Windows Administrator Account

When Windows 2008 R2 is installed on the server, the "Administrator" local account is created by default. This account provides the rights required to administer the server's OS and all its applications.

During the installation process a password must be entered for this account. The password settings should follow the strictest procedures to protect its confidentiality.

The "Administrator" password should be reset if the default one was used during installation.

CL-WCDC-Windows_Admin	Change Default Password for Windows Admin
Measures	Change the Windows Administrator password from the default password.
References	
Needed Access Rights	administrator
Executed WebCDC:	Yes:  No: 
Customer Comments and Reasons	

4.3 Secured HTTP Configuration for WebCDC Server

WebCDC clients/users connect to the WebCDC portal via customer service portal with HTTPS connectivity. Users use Single Sign On to log into the WebCDC application. Port 28081 is the secured port configured for HTTPS in the WebCDC server. The unsecured HTTP port 28080 is also automatically configured to redirect the traffic through to the port 28081.

A default digital certificate is included in the WebCDC server installation with a 10 year expiration; however, it is recommended to replace this default certificate with your SSL certificate, if your server already has one, or that the WebCDC administrator manually generates a self-signed certificate.

CL-WCDC-Personalized_Digital_Cert	Personalize the Digital Certificate
Measures	Generate a personalized Digital Certificate.
References	See below.
Needed Access Rights	administrator
Executed WebCDC:	Yes:  No: 
Customer Comments and Reasons	

4.3.1 How to Replace the Default WebCDC SSL Certificate with Your SSL Certificate

If you have already obtained a SSL certificate for your server, replace the default WebCDC certificate with your own.

Step by Step

1) Rename your certificate and key files to "server.crt" and "server.key". Do not use a passphrase on the key.

2) Copy these files to the Apache web server "conf" folder:

%programfiles (x86)%\Apache Software Foundation\Apache2.2\conf

3) Restart "Apache":

- From the "Start" menu, All Programs -> Apache HTTP Server -> Control Apache Server -> Restart

4.3.2 How to Generate a Self-Signed Certificate for the WebCDC Server

The default OpenSSL configuration enforces the generation of 1024 bit keys. For greater security, increase this default value in the openssl.cnf file to 2048 bit.

Step by Step

1) Open the openssl.cnf file with Notepad:

<system-drive>:\programfiles (x86)\Apache Software Foundation\Apache2.2\conf\openssl.cnf

2) Change the value of the "default_bits" entry to 2048:

default_bits = 2048

3) From the "Start" menu, click on "Run"

4) On the Open field type: cmd <Enter>

The command line opens.

The following procedures are run from the command line interface using the Windows Command Prompt (CMD) shell.

5) Type: cd %programfiles (x86)%\Apache Software Foundation\Apache2.2\bin <Enter>

6) Type: openssl req -config ../conf/openssl.cnf -new -out server.csr -keyout server.pem <Enter>

7) At the "Enter PEM pass phrase:" prompt, type a password to secure the access to the digital key.

Note down the password phrase since it will be required for administering the SSL certificates.

8) Enter the information that will describe your certificate. (Example follows.)

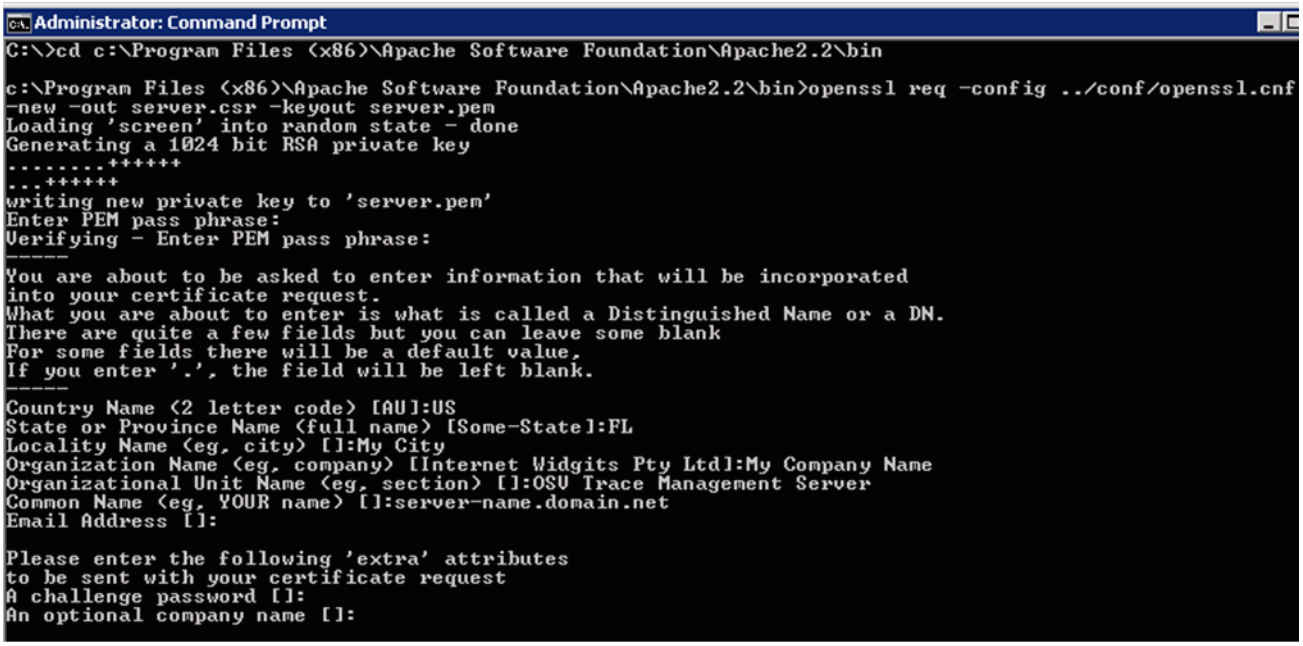
Some of these fields can be left blank, but you should provide the following parameters:

Country Name (2 letter code) [AU]: <country where the server is located>

State or Province Name (full name) [Some-State]: <state or province where server is located>

Organization Name (eg, company) []:<My Company Name>

Organizational Unit Name (eg, section) []: WebCDC Server



INFO: This step generates a digital key for this server. You can use this same key to submit a certificate signing request (CSR) to apply for a signed certificate by a Certificate Authority (CA). Once you get the certificate (server.crt) from the CA, you can use this certificate and proceed to the last step in this section.

9) Type: openssl rsa -in server.pem -out server.key <Enter>

10) At the "Enter pass phrase for server.pem:" prompt, type the password you set in the step above.

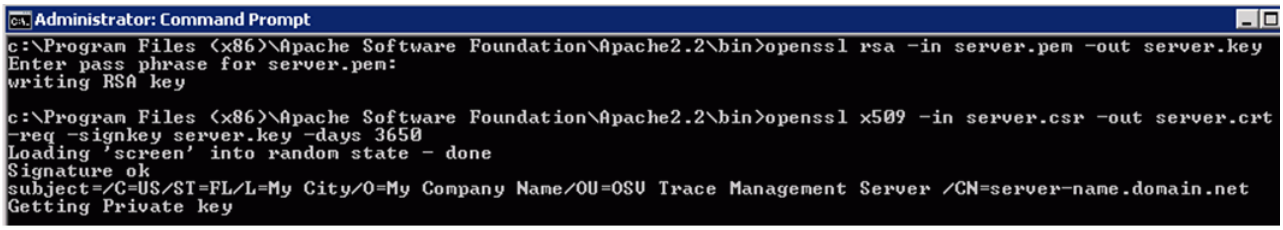
This step removes the password that was created for the key in the previous step. This is necessary for Apache to be able to automatically start in SSL mode. You should store the private key in a secure folder that is accessible only by the Administrator, SYSTEM, and user accounts that run the Apache service.

If your security policy enforces the use of a password, you will need to start Apache manually from the command line and enter the password when prompted.

11) Type: openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 3650 <Enter>

This command to creates your self-signed certificate.

INFO: The "-days 3650" parameter sets the certificate aging to 10 years. If you prefer a shorter certificate period, change the days to a shorter period. You will have to create a new certificate after this period expires.



The steps above generated a valid certificate.

12) Copy the files "server.crt" and "server.key" into the Apache web server "conf" folder:

%programfiles (x86)%\Apache Software Foundation\Apache2.2\conf

13) Restart "Apache":

From the "Start" menu, All Programs -> Apache HTTP Server -> Control Apache Server -> Restart

5 WebCDC Application Configuration Requirements

The WebCDC application installation is performed by the WebCDC administrator from a defined IP address with RDP (Remote Desktop Protocol) connection. WebCDC administrator userID and the WebCDC application password administrator are responsible for maintaining the user/WebCDC-client accounts in the WebCDC application.

6 Close Communication Ports

WebCDC uses the following TCP ports and automatically opens them during its installation: 28081 for HTTPS and 3389 for Remote Desktop Connection. The remaining open ports must be closed..

CL-WCDC-Close_Ports	Close Communication Ports
Measures	Close the Communications Ports when remote access is not allowed.
References	See below.
Needed Access Rights	administrator
Executed WebCDC:	Yes:  No: 
Customer Comments and Reasons	

6.1 How to Close Communication Ports

If you have already obtained a SSL certificate for your server, replace the default WebCDC certificate with your own.

Prerequisites

- Logged in as Administrator

Step by Step

1) Go to “Control Panel” > System and Security > Windows Firewall

2) Click on “Advanced Settings”

3) Locate the corresponding “Inbound Rules” and “Outbound Rules”

4) Close/disable the ports

On highly secure environments where only secure FTP is allowed, the nonse-cured FTP port 21 should be disabled.

a) From the “Inbound Rules”, select the “WebCDC FTP Port” rule.

b) Click on “Disable Rule” on the right pane.

c) Select the “FTP CMD IN” rule.

d) Click on “Disable Rule” on the right pane.

e) From the “Outbound Rules”, select the “FTP CMD OUT” rule.

f) Click on “Disable Rule” on the right pane.

7 References

- Support of Virus Protection Software for Server Applications
  http://wiki.unify.com/wiki/images/2/21/Security_Policy_-_Support_of_Virus_Protection_Software_for_Server_Applications.pdf
- Interface Management Database (IFMDB)
  available via the partners portal: http://www.unify.com/us/partners/partner-portal.aspx
- Center of Internet Security – Security Benchmarks
  https://benchmarks.cisecurity.org/en-us/?route=downloads.multiform