

OpenScape Business V3

Whitepaper SSL certificate handling

Release Number 09/2024



Content

1		Introduction	3
	1.1 1.2 1.3	What are SSL certificates? 3 For which web services does OpenScape Business use the SSL certificate? 3 Where can I get a trusted SSL certificate from? 3	
	1.4	Why has the certificate issue become so important?	5
2	2.1	SSL format requirements Requirements for SSL certificates to be used in OpenScape Business	5
3	3.1	How to request and install trusted SSL certificates How to install a trusted SSL certificate	6
4	4.1 4.2	Renew of a temporary self-signed SSL certificate	12 2 z system?
5		Certificate Handling for Booster Server	17
6		Client side considerations	
7		Future plans	

History of change

V1.0	Initial Creation	21/11/2023
V1.1	Editorial changes	30/09/2024

Disclaimer

This document is intended for trained OpenScape Business technicians.

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 the contract.

Availability and technical specifications are subject to change without notice.

The following description refers to OpenScape Business V3R3 and above.

1 Introduction

1.1 What are SSL certificates?

TLS/SSL certificates are used to protect data during communication between servers such as OpenScape Business and web-based clients by means of encryption and to verify the identity of the company belonging to the website so that the user can be sure that he is really communicating with the real server.

OpenScape Business issues itself a temporary ("self-signed") SSL certificate during the initial system installation or upon change of the LAN IP address, but this certificate does not contain sufficient data for identity verification apart from the user's own LAN IP address.

Such a certificate does not comply with current security standards and must be replaced by a trustworthy, individual SSL certificate issued by an official Certificate Authority (CA) as soon as possible after the initial installation of OpenScape Business. This is the only way to meet the minimum standards of current client operating systems and web browsers for secure Internet communication.

CA's usually offer SSL certificates with different trust levels: Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV). For OpenScape Business, domain validated certificates are sufficient. This is usually the cheapest option, with some CA's even free of charge.

1.2 For which web services does OpenScape Business use the SSL certificate?

The active SSL certificate is used for administrator access via the Admin Portal as well as for various other web-based applications (e.g. key programming) and WSI-based UC clients such as myPortal @work, myPortal to go, Application Launcher, myContacts and myPortal for Teams.

1.3 Where can I get a trusted SSL certificate from?

To obtain an SSL certificate, you must contact a certification authority. You must verify the domain name used to reach OpenScape Business in order to create a Certificate Signing Request (CSR), which is then sent to the CA for validation.

It should be noted that CA issued, trusted SSL certificates only have a limited validity period of a few months to a few years to ensure that they comply with current security standards. It is important to keep an eye on the expiration date and to renew SSL certificates before the expiration date is reached.

Failure to renew SSL certificates can result in the client environment classifying the website as "insecure" and preventing communication with the server.

Please note that some client environments have special requirements for SSL certificates, which may not be met by every CA. Such special requirements are linked further down in the section "client side considerations". When selecting your CA, please follow the corresponding instructions.

1.4 Why has the certificate issue become so important?

The use of trustworthy, customer or server-specific SSL certificates is extremely important and is increasingly being enforced by the major operating system and browser manufacturers. Security, professionalism, integrity and confidentiality when handling personal data are the key arguments for this.

Due to the increasing use of web-based services and clients, including via the Internet, the permanent use of the temporary, self-signed (and therefore insecure) default SSL certificate of OpenScape Business is out of the question.

In addition, the temporary, self-signed certificate of OSBiz has a multi-year validity, while some client environments have started restricting the certificate validity – sometimes to not more than one year.

Moreover, in many customer installations that were originally set up with older software releases prior to V3R2.1, the validity of these temporary, self-signed certificates expires on January 1, 2024.

The Admin Portal of OpenScape Business provides a range of tools for generating and managing SSL certificates and also supports the system administrator in creating certificate signing requests. The most important functions in this regard are explained below.

2 SSL format requirements

2.1 Requirements for SSL certificates to be used in OpenScape Business

- OSBiz requires an TLS/SSL server certificate according to the International Telecommunication Union (ITU) standard X.509
- Supported signature algorithms: sha256RSA, sha384RSA, sha512RSA
- Supported certificate file format: PKCS #12 or PEM format
- Public key length: 2048

3 How to request and install trusted SSL certificates

Dependent on the certificate authority (CA) of your choice, there are different options, in particular:

1) Using the web portal of the certificate authority to request a certificate for your domain. You will have to provide some basic data like the domain name which you own and you intend to use to access the OSBiz system.

Also you may have to choose a certificate validation method. Once you have made your choice – for example DNS validation – the CA will give you a challenge which you have to fulfill according to the guidelines of your CA. Example (CA Provider ZeroSSL):

Define the certificate content (configurable scope depends on the chosen CA):

📥 ZeroSSL	Help Center Partner Program
Get Premium SSL	New Certificate Cancel
 Dashboard Certificates Developer 	SSL Certificate Setup You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below.
	 Domains I need a wildcard certificate Please enter at least one domain to secure. For single-domain certificates the WWW-version of your domain will always be included at no extra charge. Enter Domains
	合 osbiz.mycompany.de Image: Sobiz.mycompany.de ⊕ Add Domain Image: Next Step →
	Validity CSR & Contact
	> Finalize Your Order

2) Define further certificate properties:

ZeroSSL	Help Center Partner Program	control Marcola
Get Premium SSL	New Certificate	Cancel
Dashboard Certificates	SSL Certificate Setup You're on your way to issuing a brand-new SSL certificate for one or multiple domains.	
Developer	Domains	— —
	 Validity You can now choose between generating 90-day or one-year certificate validity. To keep manual work at a minimum, we recommend 1-year certificates. 90-Day Certificate 1-Year Certificate 	Next Step →
	SR & Contact	
	> Finalize Your Order	

3) Auto-Generate the CSR:

井 ZeroSSL	Help Center Partner Program
Get Premium SSL	You're Almost Done Cancel
Dashboard Certificates Developer	SSL Certificate Setup You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below. Omains
	 ✓ Validity ✓ CSR & Contact Before validation, we will auto-generate contact information and a CSR for your certificate. To enter your information manually or paste an existing CSR, please uncheck the box below. ✓ Auto-Generate CSR
	> Finalize Your Order

Next, the Certificate Authority needs to verify that you are the domain owner. This will be done via a specific challenge that only the domain administrator can fulfill. For example, a DNS server challenge will ask you to create a specific DNS entry for your domain.

After this is done and the CA confirms successful domain validation, you will be able to download the certificate and key file, which you then import and activate via OSBiz Admin Portal.



4) Using OSBiz Admin Portal to create a Certificate Signing Request (CSR).

Navigate to Expert Mode -> Security -> SSL -> Certificate Management -> Server Certificate

Expert mode - Telephony Server	•
Security	Server Certificates
Application Firewall	Generate Certificate Signing Request (CSR) Imput Server Certificate (PECS#12)
Deployment and Licensing Client (DLSC)	
 Signaling and Payload Encryption (SPE) SSI 	Certificate Request Name: []
Certificate Generation	Type of Signature Algorithm: sha256RSA V
Certificate Management	
Server Certificates	Public Key Length: 2048 V
Web Security	Eublect Name
Sql Security	Country (C):
	Organization (O):
	Organization Unit (OU):
	Company Name (Chi)
	Common name (UR)
	Distionabad Nama Format
	Distinguished Rame Formate
	Subject Alternative Name Extension: DNS Name v (optional)
	Add Bullard Muser / (anti-anti-
	Active Subject Asternative Herme. [optional]
	Apply Help

In Generate Certificate Signing Request (CSR) page, the following fields must be filled in order to generate the key and csr files

General:

- Certificate Request Name: A name for the CSR which will be used in the name of the file that will be downloaded.
- Type of Signature Algorithm: Select between sha256RSA and sha512RSA
- Public Key Length: The only option is 2048

Subject Name:

- Country (C): Use a two letter country code e.g. DE
- Organization (O): denotes the formal name of the overarching entity or company to which the certificate is assigned.
- Organization Unit (OU): designates a specific subunit or department within an organization, offering additional granularity to identify the organizational structure
- Common Name (CN): a vital identifier, usually representing the domain name for which the certificate is issued, providing a key element for verifying the certificate holder identity.

Subject Alternative Name (Optional):

The Subject Alternative Name (SAN) extension is a feature of X.509 certificates used in the field of cryptography. X.509 is a standard that defines the format of public-key certificates. The SAN extension allows additional identities, such as host names, IP addresses, or email addresses, to be associated with a single X.509 certificate. This is particularly useful in scenarios where a server may be accessed by different names or addresses.

Distinguished Name Format: Information similar to the Subject name such as Country (C), Organization (O), Organization Unit (OU), Common Name (CN) must be filled.

Other Format:

- Subject Alternative Name Extension: Option are DNS, IP Address, Email Address, Uniform Resource Indicator
- Subject Alternative Name: The SAN extension helps address limitations in cases where a single common name is insufficient or when there is a need to include multiple identities within a single certificate. This is important for modern web services, where a server might be accessible through multiple domain names or IP addresses.

Here's an example of how the SAN extension might look in a certificate: Subject Alternative Name: DNS:www.example.com DNS:mail.example.com IP Address:192.168.1.1 Email:admin@example.com

when Subject Alternative Name option has been filled the Add button must be used in order to be included in the CSR.

Expert mode - Telephony Sapres	
Expert mode - telephony server	
Application Einewall	Server Certificates
Papingment and Ligensing Client (DLSC)	Generate Certificate Signing Request (CSR) Import Server Certificate [WCS#12]
Signaling and Payload Encoration (SEE)	
TSSI	Certificate Request Name: Mycertificate
Certificate Generation	Type of Signature Algorithm: sha256RSA 💙
Certificate Management	Public Key Length: 2008 V
Server Certificates	
Web Security	Counter(P): DE
su security	country (c). Dr
	Organization (0): Example Co
	Organization Unit (OU): Example
	Common Name (CN): www.example.com
	Subject Alternative Name
	Distinguished Name Format Other Format 8
	Subject Alternative Name Extension: DNS Name 🕶 (optional)
	Add Subject Alternative Name www.example.com (ontional)
	Deleter DNS: www.example.com
	Apply Help

By applying the information two files will be generated and downloaded "Certificate_Name".csr and key_csr.pem

The generated CSR can be seen under the list of Server Certificates

Expert mode - Telephony Server					
Security	Server Certificates				
Application Firewall	View Certificate	Delete Certificate	Expert Certificate / CSR TX 50V1	brown Updated Certificate / Certificate for CULTX 3041	Activate Certificate
Deployment and Licensing Client (DLSC)			and a second second second		
 Signaling and Payload Encryption (SPE) 			Name of the Certifica	ite: Mycertificate	
551			Certificate Ty	pe: Certificate Signing Request (CSR)	
Certificate Generation			Type of Signature Algorith	WE.	
Terver Certificates			Start Time of Validity Period (Ob	The	
Default Server Certificate (active)			Start time of validity Period (Giv	1)	
Mycertificate			End Time of Validity Period (GN	T):	
Web Security	and the second se		CRL Distribution Po	int:	
Sidi Security	Issued by CA				
				1845	
	Subject Name				
			Country (C): DE	
			Organization (O): Example Co	
			Organization Unit (O	U): Example	
			Common Name (C	Ni youw example com	
	Subject Alternative Name		communication (c	1). The eventue con	
	Encod which the state of the Property of				
	Public Key Encryption Data				
	Contraction of the second second		Public Key Len	nh: 2048	
				45906F472F72B5F6F8D4458F9	
			Public K	ey E2062A267DB02F010AE6227FF6 *	
				DAF011B1441482BE4827570BDF	
				F254 33B6 BAA8 1839 4038 C273	
			Fingerpr	int 118B E609 43BA 679B	
	Help				
Alexandre and a second s					

5) Using 3rd party tools (usually based on OpenSSL) to create a Certificate Signing Request (CSR) and provide this to the Certificate Authority (CA) of your choice. Again you will have to fulfill a challenge given by the CA to verify that you are the owner of the domain which is covered by the trusted SSL certificate. After you have received the certificate from your CA, you can install and activate it via OSBiz Admin Portal.

3.1 How to install a trusted SSL certificate

Dependent on your certificate authority, you may receive SSL certificates in different formats. The Admin Portal of OpenScape Business supports two options for the import of SSL certificates:

- 1. Import in **PKCS #12** format (file extension*.p12). PKCS is an archive file format for storing multiple cryptography objects as a single file. It is commonly used to bundle a private key with its certificate.
- 2. Import in **PEM** format, where certificate and private key as separate files (file extension *.cer and *.key).

Both import options are offered in Admin Portal under

Expert Mode – Telephony Server – Security – SSL – Server Certificates – Import Server Certificates. Example using option 2:

- 1. Enter a name and a passphrase for the certificate you import. The passphrase requires at least 7, at maximum 32 characters.
- 2. Select the certificate file and key file as obtained by your certificate authority.
- 3. Press the button "Import Certificate and Key"

Expert mode - Telephony Server				8
Security	Server Certificates			
Application Firewall Deployment and Licensing Client (DLSC)	Generate Certific	ate Signing Request (CSR)	Import Ser	ver Certificate
Signaling and Payload Encryption (SPE)	Import PKCS#12			
▼SSL		Name of the Certificat	e:	
▼Certificate Generation				
▼Certificate Management		Passphrase for decryption	n:	
Server Certificates		File with Certificat	batei auswählen Keine ausgewäl	hlt
Default Server Certificate (active)	Import Certificate and Key files			
ayi arcuity		Name of the Certificat	e: MyZeroSSI Certificate	
		Passphrase for decryption	n: [•••••	
		Certificate File	e: Datei auswählen certificate.crt	
		Key File	e: Datei auswählen private.key	
	View Fingerprint of Certificate	Import Certificate from File	Import Certificate and Key	Help

After successful import, you will see the new certificate in the list of Server Certificates, showing the name that you have defined in the previous step.

Expert mode - Telephony Server					
Security	Server Certificates				
Application Firewall	Mone Cortificato	Delate Certificate	Execut Partificate / CER IN 5001	Tempet Hindured Cambrata / Partificate for CED IV COD	Automatic Constitution
Deployment and Licensing Client (DLSC)		Derete Certificate	refere connecte / case [senses]	subsic obmicer commence (commence in cost (support	PROVINCE CAS OF RANCE
 Signaling and Payload Encryption (SPE) 			Name of the Certifica	e: ZeroSSL	
▼SSL			Certificate Tyr	CA Signed Peer Certificate	
Certificate Generation			Certilicate Typ	e. CA-Signed Feel Certificate	
Certificate Management			Serial Number of Certifica	B. Segments to be experienced a new endown conversion of the second sec second second sec	
Default Server Certificate (active)			Serial Number of Certificate (he): In the second s	
E ZeroSSL			Type of Signature Algorith	n: sha384RSA	
Sql Security			Start Time of Validity Period (GM): Friday, 11/10/2023 00:00:00	
			End Time of Validity Period (GM): Thursday, 02/08/2024 23:59:59	
			CRL Distribution Poi	t:	
	Issued by CA				
			Country (): AT	
			Organization (0): ZeroSSL	
			Organization Unit (OU):	
			Common Name (Cf): ZeroSSL RSA Domain Secure Site CA	
	Subject Name				
			Country (0): DE	
			Organization (0): myOrganisation	
			Organization Unit (OU	I):	
			Common Name (Cf	0:	
	Subject Alternative Name				
				We want a west as	-
	Help				

4. New certificates are not automatically activated upon import. Please navigate to the *Activate Certificate* tab to activate the new certificate.

Please note that the integrated web server of OpenScape Business will restart upon certificate activation. This means that for approx. 2-3 minutes, the Admin Portal and any other web services will not be reachable.

4 Renew of a temporary self-signed SSL certificate

4.1 How can I renew the temporary, self-signed SSL certificate of OpenScape Business?

As explained above, such a certificate does not comply with current security standards and must be replaced by a trustworthy, individual SSL certificate as soon as possible. If you cannot obtain a trusted SSL certificate in time before the initial self-signed certificate expires, you can create a new temporary self-signed certificate. This happens automatically whenever you change the LAN IP address of an OSBiz X system.

It can also be triggered manually via Admin Portal. Please navigate to: Expert Mode – Telephony Server – Security – SSL –Certificate Generation – Tab "Generate Self-Signed Certificate"

Here you must specify the name and serial number of the certificate and enter the further certificate properties. Please note that some client environments generally do not trust certificates which have a validity of more than one year.

Sxpert mode - Telephony Server					
Security Application Firewall Deployment and Licensing Client (DLSC) Firewalls and Revised Forewards (FEF)	Display General Information Generate CA Certificate		Generate Self-Signed Certificate		
SSL		Name of the Certificate:	MyUnsecureCertificate		
Certificate Generation	Set	ial Number of Certificate:	4356465		
Certificate Management Server Certificates	Typ	e of Signature Algorithm:	sha256RSA 🗸		
Default Server Certificate (active)		Public Key Length:	2048 🗸		
Sql Security	Start Time of Validity Period (GMT)				
		Day	Month	Year	
		15	11	2023	
		Hour	Min.	Sec.	
		0	0	0	
	End Time of Validity Period (GMT)	Day	Month	Voar	
		Day		2024	
			03	2024	
		Hour	Min.	Sec.	
	Rublant Hama	0	0	0	
	Subject Name	Country (C):	DE		
		Organization (O):	myOrganisation		
	Common Manne (N): [102.188.1.2				
	Subject Alternative Name	Contraction (Crity)	YOR: FOOT FIRE		
	Distir	nguished Name Format⊖	Other Format		
	Subject Alte	ernative Name Extension:	DNS Name v (optional)		
	Add St	ubject Alternative Name:	(optional)		
	CR	L Distribution Point Type:	DNS Name v (optional)		
		CRL Distribution Point:	(optional)		
	Ante late				
	Арріу неір				

A self-signed SSL certificate also has to be activated manually after creation.

For obvious reason, any web browser will show the connection as untrusted / unsecure when utilizing e.g. Admin Portal with such a certificate.

4.2 Can I create an own certificate and import it on client side to let the web browser trust a specific OSBiz system?

Yes, this is possible. Please note again that such a certificate does not comply with current internet security standards. While it may be applicable when the specific OpenScape Business is accessed only for administration from the internal LAN, such an approach is definitely not recommended if any OpenScape Business Web Services are exposed to the internet.

Navigate to Expert Mode -> Security -> SSL -> Certificate Generation and select the Generate CA Certificate Tab

Expert mode - Telephony Server						
Security Application Firewall Deployment and Licensing Client (DLSC)	Display General Information Generate CA Certificate		Generate Self-Signed Certificate			
Signaling and Payload Encryption (SPE) Ssi	Name	e of the Certificate:				
Certificate Generation	Serial Nur	nber of Certificate:	1			
Certificate Management	Tune of Si	anature Algorithm	·			
Web Security	i i ju di di					
adi alcunty		Public Key Length: 2048 V				
	Start Time of Validity Period (GMT)	Mont	th ×	ear.		
	17	1		022		
				023		
	Hour	Min.	5	ec.		
	0	0	0			
	End Time of Validity Period (GMT)	1 miles				
	Day	Mont	л тө —	ear		
	17	11	2	033		
	Hour	Min.	S	ec.		
	0	0	0			
	Subject Name					
		Country (C):				
		Organization (O):]			
	Organ	nization Unit (OU):]			
	Cor	nmon Name (CN):	1			
	Subject Alternative Name					
	Distinguishe	d Name Format⊖ Other Format				
	Subject Alternative	Name Extension: DNS Name 🗸	(optional)			
	Add Subject A	liternative Name:	(optional)			
	CRL Distri	ibution Point Type: DNS Name 🗸	Type: DNS Name v (optional)			
	CRL	Distribution Point:] (optional)			
	Apply Help					

To proceed with generating the certificate, the following fields must be filled:

General:

- Name of the Certificate: A name for the certificate file
- Serial Number of Certificate: is part of the certificate's metadata and is typically a nonnegative integer
- Type of Signature Algorithm: Select between sha256RSA, sha512RSA
- Public Key Length: Only 2048 is supported

Start Time of validity period:

This is the start time of the validity period. The certificate should not be considered valid for use before this date and time. It represents the earliest point in time when the certificate is considered valid.

End Time of Validity Period:

This is the end time of the validity period. The certificate is considered valid up to and including this date and time. After this date, the certificate is no longer considered trustworthy, and clients may reject it.

Subject Name:

- Country (C): Use a two letter country code e.g. DE
- Organization (O): entity or company to which the certificate is assigned.
- Organization Unit (OU): a specific subunit or department within an organization
- Common Name (CN): a key element for verifying the certificate holder identity.

Subject Alternative Name (optional):

Option are DNS, IP Address, Email Address, Uniform Resource Indicator

Once all mandatory fields have been completed, the CA certificates will be listed under the Certificate Generation section.

Stocar/J Display General Information Page/sector Fermal Userator Fermal Deployment and Userator Christical Sector Fermal Userator (SSS) Veri Conflicute (SSSS) Pege/sector Fermal Userator (SSS) Veri Conflicute (SSSS) Pege/sector Fermal Userator (SSSS) Name of the Certificate (MCGr42) Update Christiane (SSSS)	1
P Application Freeail Delay Conflicate Department on Application Freeail Control (CAS) (
Deployment and Lorensing Client (DLSC) Signal and Payload Encryption (SPE) Name of the Certificate: MyCaCertificate	
Pageaing and Payload Encryption (SPE) Name of the Certificate MyCaCertificate	
Certificate Type: Self-Signed CA Certificate	
Controllar Orthogon Serial Number of Certificate: 12456789	
Certificate Management Social Mumbar of Contilicate (host) - 07507015	
Web Security Technology of Control of Contro	
Sql Security Type of Signature Algorithm: snazSoHSA	
Start Time of Validity Period (GMT): Friday, 11/17/2023 00:00.00	
End Time of Validity Period (GMT): Sunday, 11/17/2024 00:00.00	
CRL Distribution Point:	
Issued by CA	
Country (C): DE	
Organization (O): Unity	
Organization Unit (OU): Unity Software and Solutions GmbH & Co. KG	
Common Nama (CN): Unity	
Subject Name	
Country (C): DE	
Ornarization (0): Unity	
Organization (c), City City Organization (c), City City	
Organization on (UV) only volume and volume a	
Common Name (UN): Unity	
Subject Aller native Name	
Public Key Landty 2048	
r sum, rey benyar. Avec	
C/3444/2/3005/2/06392/04/2/A ~ Public Kar, 96562/2015/874/C18/200087 *	
BF335B624001099762903468412	
3E00 6033 8088 6152 1C38 6890	
Fingerprint 5307 0086 DE4A A165	
Help	

On the designated web page, you can conveniently download the CA (Certificate Authority) certificate. Simply navigate to the "Export Certificate" tab and initiate the download by clicking the "Load" button.

Expert mode - Telephony Server					•
Security	Display General Infor	mation			
Application Firewall	Man Cathlada	Dalata Castilizata	Execut Castilizate (Y 500)	Connector P.J. Finand Connec Contractor (IN/CE 613)	Hadda Ch. Stand Course Caddinate IV 5001
Deployment and Licensing Client (DLSC)	view Certificate	Delete Certificate		Generate CA-signed Server Certificate [PKCS#12]	Update CA-signed Server Certificate [X.509]
Signaling and Payload Encryption (SPE)					
▼SSL					
▼Certificate Generation					
MyCaCertificate					
Certificate Management					
Web Security					
Sql Security					
	Load	Help			

The resulting file will be named "Name of the Certificate.crt".

Utilize the "Generate CA-Signed Server Certificate [PKCS#12]" tab to seamlessly create a CA-Signed Server Certificate.

Expert mode - Telephony Server						•	
Security	Display General Inform	nation					
Application Firewall	the Continue	Dalas Catlante	Frank Cardinate IV (198)	Control of C	Consel Consel Contillicular (DV/CC+13)	Harden Ch. Frank Press, Conflicts IV (195)	
Deployment and Licensing Client (DLSC)	View Certificate	Delete Ceruncate	Export Certificate [JC309]			obnare oversitien zeuser ceutruren fintanal	
Signaling and Payload Encryption (SPE)				Passobrase for encryption			
▼SSL				r adoptitado for anotypoon.			
▼Certificate Generation			Re	enter Passphrase for encryption:	9		
MyCaCertificate				Serial Number of Certificate:			
Certificate Management	Serial Number of Certificate:						
Web Security				Type of Signature Algorithm:	sha256RSA		
sqi sicurity				Public Key Length:	2048 •		
	Start Time of Validity Pe	eriod (GMT)					
				Day	Month	Year	
				17	11	2023	
						2727	
				Hour	Min.	Sec.	
	0				0	0	
	End Time of Validity Per	riod (GMT)					
				Day	Month	Year	
				17	11	2033	
						<u></u>	
				Hour	Min.	Sec.	
	0				0	0	
	Subject Name						
	Country (C						
	Organization (O						
	Organization Unit (OU						
	Common Name (OK						
	Exhibit Alternative Mar			common Hanne (crti).			
	Subject Alternative Nam			Distinguished Name Format	Others Form of		
				Distinguished Name Format			
	Subject Alternative Name Extension Add Subject Alternative Name				DNS Name v (optional)		
					(antianal)		
					[optioner]		
	CRL Distribution Point Type				DNS Name (optional)		
	Generate Cettificate Help					*	

Passphrase for encryption: a passphrase for the certificate with length 7-32 characters

The remaining fields share similarities with those described earlier.

- Serial Number of Certificate:
- Type of Signature Algorithm:
- Start Time of Validity Period
- End Time of Validity Period
- Subject Name
- Subject Alternative Name

Upon clicking the "Generate Certificate" button, a file named "BasedOnName of the Certificate.p12" will be promptly downloaded.

The downloaded certificate can be Imported in the system from Expert Mode -> Security -> SSL - > Certificate Management -> Server Certificate Import Server Certificate Tab

5 Certificate Handling for Booster Server

When initially installing a Booster Server, a certificate is created with the IP address of the booster serving as the common name. The certificate has a 10-year validity period and is issued for the organization "Unify Software and Solutions GmbH & Co. KG," with the organizational unit specified as "Unify."

It is possible to replace the default certificate on the Booster Server by transferring a different certificate through the Web-Based Management (WBM) interface of the system. Once transferred, the new certificate can be activated, providing an alternative security configuration for the Booster Server.

- 1. Go to Expert Mode.
- 2. Navigate to Security -> SSL -> Certificate Management -> Server Certificates.
- 3. Choose one of the imported certificates.
- 4. Access the "Activate Certificate" tab.
- 5. From the system drop-down menu, select "OpenScape Business UC Booster Server."
- 6. Click the "Activate Now" button to apply the selected certificate to the Booster Server.

Expert mode - Telephony Server					•			
Security	Server Certificates							
Application Firewall	Server Gerundates							
Deployment and Licensing Client (DLSC)	view coluncate	Ublete Ceruncate	Expert Gereincate / Cak (X.509)	Import opoates Celoncate / Celoncate na Cok (2.509)				
Signaling and Payload Encryption (SPE)								
▼SSL	Warning: This action will distribute and activate the certificate to the system selected below.							
Certificate Generation	All current nttp connections of the selected system will be broken:							
Certificate Management	System							
Server Certificates			System Or	penScape Business UC Booster Server 🗸				
Default Server Certificate (active)								
ZeroSSI								
Web Security								
Sql Security								
	Activate Now P	felp						

6 Client side considerations

OpenScape Business clients and devices are in use with many different client environments, operating systems, web browsers etc.

The manufacturers of these environments have different detailed requirements for the format, content and validity period of the server-side SSL certificates. When creating the Certificate Signing Request for your trusted SSL certificate, please follow the relevant guidelines for your client environment.

For example, Apple frequently publishes server certificate requirement updates on their support portal which are relevant for iOS and macOS based client applications:

https://support.apple.com/en-ca/103769 https://support.apple.com/en-us/102028

7 Future plans

Unify is working on the implementation of "Let's Encrypt" in OpenScape Business. Let's Encrypt is a non-profit certificate authority that provides SSL certificates for Transport Layer Security (TLS) encryption at no charge.

With Let's Encrypt, the SSL certificates are handled by an automated process designed to overcome manual creation, validation, signing, installation, and renewal of certificates for secure websites.

mitel.com



© 2024 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.