Ignition Proce	ess (contin	nued)
There are two o	options availab	le here, you can generate a CA automatically.
IP C Acce Servi New Confi Time Chan Secu Revia	Office Server ept License ✓ rer Type ✓ r Hardware ✓ figure Network ✓ e & Companding ✓ urity → iew Settings	Certified Authority Settings Generate CA automatically Import CA

There are two options available here, you can generate a Certificate Authority automatically from within the Avaya system

• Or if you have purchased a third party CA you can import it into the system. Click on Next.

Accept License	~	Certified Authority Settings	
Server Type	~	Generate CA automatically	
New Hardware	~	File: Browse Uploa	d
Configure Network	~	Password:	
Time & Companding	~		
Change Password	~		
Security	→		
Review Settings			
		Cancel Previous No	ext

Or if you have purchased a third party CA you can import it into the system. Some of the 3rd parties offering trustworthy certificates include RSA, Verisign, Entrust, Microsoft, Symantec and many more.

Click on Next.

• You need to download and install the root certificate into your browser before you complete Ignition. Click on OK.

Accept License Server Type Please import the CA into the bro	✓ ✓	Certified Authority Settings Generate CA automatically you apply the ignition settings. You can find the download link in the "Review Settings" step.
		ОК
Change Password Security Review Settings	 ✓ → 	Cancel Previous Next

You need to download and install the root certificate into your browser before you complete Ignition. Click on OK.

• A summary of the setting is displayed. Click Apply and alternatively use Previous and Next options to re adjust settings.

Accept License	~	Server Type:	Primary	1
		IP:	10.129.116.124	
Server Type	~	Netmask:	255.255.255.0	_
		Gateway:	10.129.116.254	
New Hardware	~	Primary DNS:	135.124.138.152	
Configure Notwork		Secondary DNS:	135.11.66.59	
Configure Network	v	Hostname:	Primary	
Time & Companding	~	Timezone:	Europe/London	_
		Use NTP:	Yes	_
Change Password	~	NTP Server:	0.pool.ntp.org	-
		Companding:	A-law	
Security	~	Password:	Change	
Review Settings	→	Additional Hardware:	/dev/sdb detected, to be mounted on /additional-hdd#1	
		Certified Authority:	Download CA (PEM-encoded) Download CA (DER-encoded)	
		ATTENTION: Prior to ordering have been finalized: LAN1 a these sattings will investigate Cancel	glicenses for IP Office please confirm the following setting nd LAN2 IP addresses, Timezone and Hostname. Changing any avieting licenses. Disease as documentation for more III Previous App	s rtatol y

A summary of the setting is displayed, click Apply. Alternatively use Previous and Next options to readjust settings.

There are links to download the certificate in the Review Settings screen.

Ignition Process (co	ntin	ued)		
ID Office Se	nuor	Edition	nition	
Accept License	√ ver	Server Type	Primary	
Server Type	~	IP.	10.129.116.124	
New Hardware	~	The settings have been as	pplied. 54	
Configure Network	~	Tod will be redirected to an	e royin page.	
Time & Companding	~	[OK pn	
Change Password	~	ッパー Saving network setting:	, please wait to be redirected. This might take up to 8 minutes.	
Security	~		A-law Change	
Review Settings	→		/dev/sdb detected, to be mounted on //additional-hdd#1	
			Download CA (PEM-encoded) Download CA (DER-encoded)	
		ATTENTION: Prior to ordering have been finalized: LAN1 an there eathere will investigate	licenses for IP Office please confirm the following settings id LAN2 IP addresses, Timezone and Hostname. Changing any adjeton teachers. Disease are documentation for more data	
			Previous Apply	

Click ok to finish the ignition process.

Installation and the ignition process has not changed so much between versions, but it is highly recommend to read all relevant documentation for the version you are working with.

If you didn't import the root certificate into your browser before completing Ignition then you will get another warning. The previous default IP Office certificate that you added an exception for at the start has been replaced b a different identity certificate that has been signed by the root CA.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified. What Should I Do? If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue. Get me out of here! Technical Details I Understand the Risks	You have asked Firefox to connect securely to 10.129.116.124:7070, but we can't cont connection is secure.	firm that you
 What Should I Do? If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue. Get me out of here! Technical Details I Understand the Risks 	Normally, when you try to connect securely, sites will present trusted identification to p are going to the right place. However, this site's identity can't be verified.	prove that you
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue. Get me out of here! • Technical Details • I Understand the Risks	What Should I Do?	
Get me out of here!	If you usually connect to this site without problems, this error could mean that someor impersonate the site, and you shouldn't continue.	ne is trying to
 Technical Details I Understand the Risks 	Get me out of here!	
I Understand the Risks	Technical Details	
	I Understand the Risks	

If you didn't import the root certificate into your browser before completing Ignition, then you will get another warning. The previous default IP Office certificate that you added an exception for at the start has been replaced by a different identity certificate that has been signed by the root CA.

- The server is now using a new identity certificate, not the default IP Office certificate.
- Issued to Common Name is 'Primary'. This is the hostname that was set in the network configuration settings during Ignition.
- Issued by Common Name contains the MAC address of the system.

This certificate has been	en verified for the following uses:	
SSL Client Certificate	,	
SSL Server Certificate		
Issued To Common Name (CN)	Primary	
Organization (O)	Avaya Inc	
Organizational Unit (OU Serial Number	00.8E-27-DE-27-R1-8E-C4-C0	
Issued By	VIDED BUSINESS CONTRACTOR	
Common Name (CN)	ipoffice-root-0050569F21F9.avaya.com	
Organization (O)	Avaya Inc	
Organizational Unit (OU) GCS	
Period of Validity		
Begins On	24/09/2014	
Expires On	22/09/2021	
Fingerprints		
SHA-256 Fingerprint	04:B0:B0:68:8A:7E:F6:0B:E1:64:18:F2:9F:11:3A:87: 1C:39:B5:24:B6:85:F6:01:D5:84:1C:58:03:A9:EF:92	
SHA1 Fingerprint	E1:2B:11:40:43:E9:70:E9:67:16:9D:92:A6:58:8A:36:78:C0:F9:68	
	5	lose

The server is now using a new identity certificate, not the default IP Office certificate.

the "Issued to Common Name" is 'Primary'. This is the hostname that was set in the network configuration settings during Ignition.

"Issued by Common Name" contains the MAC address of the system.

AVAYA | LEARNING

Ignition Process (continued)

- Import the certificate into your browser before you continue.
- If you do not import the certificate you will get security warnings for each different port you try to connect to for his system.
 - 7070 Web Management
 - 7071 Web Control
 - 9443 Secure one-X Portal
 - 9443 Web Conferencing
- Example provided here for importing certificate into Firefox.



Import the certificate into your browser before you continue.

If you do not import the certificate you will continuously get security warnings for each different port you try to connect to for this system.



To verify that the certificate was imported, Click on View Certificates.

nition I	Process (continued)
Go to the saved th	e Authorities tab and click on Import. Browse to the location where you ne root certificate you downloaded during Ignition and click on Open.
ľ	Certificate Manager
	Your Certificates People Servers Authorities Others
	You have certificates on file that identify these certificate authorities:
	Certificate Name Security Device 🛱
	▲ (c) 2005 TURKTRUST Bilgi Iletişim ve Bilişim Güvenliği Hizmetleri A.Ş. TÜRKTRUST Elektronik Setlifika Hizmet Soğlayırarı Builtin Ohizet Takan
	4A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
	A-Trust-nQual-03 Builtin Object Token
	#AC Camerfirma S.A.
	Chambers of Commerce Root - 2008 Builtin Object Token
	AC Camefirma SA CIF A82743287
	View Edit Trust Export Delete or Distrust
	ОК
l	

Go to the Authorities tab and click on Import. Browse to the location where you saved the root certificate you downloaded during Ignition and click on Open.

Ignition Proc	cess (continued)	
Select all of the	ne Trust checkboxes and click on OK.	
	Downloading Certificate You have been asked to truct a new Certificate Authority (CA)	
	Do you want to trust "ipoffice-root-0050569F21F9.avaya.com" for the following purposes? Image: Trust this CA to identify websites. Image: Trust this CA to identify email users. Image: Trust this CA to identify software developers. Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available). Image: View Examine CA certificate Image: OK Cancel	

Select all of the Trust checkboxes and click on OK



The certificate is now installed. Click on OK