How to Reset SSL Certificates in an Upgraded 7.5.0 Domain Back to Using the SSL Certificates From an Old Version

<u>Domain</u>

Overview Example 7.3.1 -> 7.5.0 Single Node Upgrade Create 7.3.1 Single Node System View the 7.3.1 Admin Node Manager Certificate Run Sysupgrade View the 7.5.0 Admin Node Manager Certificate Extract the 7.3.1 Certificate Details for the Domain CA and the Admin Node Manager Revert the SSL Certificate for the 7.5.0 Admin Node Manager Revert the SSL Certificate for the 7.5.0 API Gateway Verify the 7.5.0 Domain is Operational Copy Domain CA Key and Certificate from Old Version to 7.5.0 Create a New API Gateway Instance in the 7.5.0 Domain Example 7.3.1 -> 7.5.0 Multi-Node Upgrade Create 7.3.1 Multi-Node System View the 7.3.1 Admin Node Manager Certificate Run Sysupgrade on NodeA and NodeB View the 7.5.0 Admin Node Manager Certificate Extract the 7.3.1 Certificate Details for the Domain CA and the Admin Node Manager on Node A Extract the 7.3.1 Certificate Details for the Node Manager on NodeB Revert the SSL Certificate for the 7.5.0 Admin Node Manager on NodeA Revert the SSL Certificate for the 7.5.0 API Gateway on NodeA Revert the SSL Certificate for the 7.5.0 Admin Node Manager on NodeB Revert the SSL Certificate for the 7.5.0 API Gateway on NodeB Verify the 7.5.0 Domain is Operational Copy Domain CA Key and Certificate from Old Version to 7.5.0 Create a New API Gateway Instance in the 7.5.0 Domain

How to Reset SSL Certificates in an Upgraded 7.5.0 Domain Back to Using the SSL Certificates From an Old Version Domain

Overview

In 7.5.0, we always regenerate the SSL certificates used for management traffic between Node Managers and API Gateways. This is safer during upgrade, as it means that the old and new version Node Managers cannot mistakenly communicate with each other. This section describes the manual steps that may be carried out after a successful upgrade to get the newly upgraded 7.5.0 domain to use the certificates from an old installation. In most cases this will not be a required as the new certificates generated during sysupgrade may be used. Some customers may wish to revert to using the old version certificates if they are custom certificates. Note that it is not possible to revert back to using certificates from an old version if the old version is older than 7.3.0.

Previously, SSL certificates were only regenerated at upgrade time when upgrading from versions older than 7.3.0, and upgrades of newer versions reused the old version system SSL certificates in the new version system.

The following steps give an overview of the procedure to reset the SSL certificates to use the certificates from an old version system in a newly upgraded 7.5.0 system. Follow the more detailed examples below when performing the steps.

- On the main Admin Node Manager node:
 - Using the old version Policy Studio edit the old version Node Manager entity store configuration.
 - Export the Domain CA certificate to a PEM file.
 - Export the Node Manager "topology-cert" certificate and key to a P12 file.
 - Using the 7.5.0 Policy Studio create a project using the "From existing configuration" option. Point the project at the 7.5.0 Admin Node Manager configuration.
 - Edit the "Management HTTPS Interface". Remove references to the "topology-cert" certificate and the "CN=Domain" CA certificate from the listener. These certificates are the new certificates generated via sysupgrade that we no longer wish to use if we are reverting to the certificates from the old version.
 - Remove the "topology-cert".
 - Remove the "CN=Domain" CA certificate.
 - Import the exported Domain CA certificate from the PEM file created using the old version Policy Studio.

- Import the exported "topology-cert" from the P12 file created using the old version Policy Studio.
- Set the Issuer on the imported "topology-cert" to the Domain CA.
- If there is a duplicate Node Manager certificate, Remove it.
- Edit the "Management HTTPS Interface", point it at the imported "topology-cert" and the imported Domain CA certificate.
- Copy the project contents to the ~/7.5.0/apigateway/conf/fed directory.
- Restart the Admin Node Manager
- For <u>each</u> API Gateway instance on the current node, edit the mgmt.xml to contain the correct Domain CA dname.
- For <u>each</u> API Gateway instance on the main Admin Node Manager host, copy the certs.xml from the old version to the 7.5.0 install, e.g. cp
 ~/7.3.1/apigateway/group-2/instance-1/conf/certs.xml
 - ~/7.5.0/apigateway/group-2/instance-1/conf/certs.xml.
- Restart each API Gateway instance.
- Check out <u>https://anm-host:8090</u>. The API Gateway instances on the main Admin Node Manager host should have a live status. The Admin Node Manager will not be able to communicate with other nodes in the domain yet. There will be SSL errors in the Admin Node Manager trace file at this point.
- If the old version used system generated SSL certificates then copy the apigateway/groups/certs directory from the old version installation into the new version installation. This will ensure that new API Gateways added to the 7.5.0 topology in future are signed using the same Domain CA key.
- On each subsequent node in the domain, do the following:-
 - Using the old version Policy Studio, edit the old version Node Manager entity store configuration for that node.
 - Export the Node Manager "topology-cert" certificate and key to a P12 file.
 - (No need to export the Domain CA certificate again).
 - Use the 7.5.0 Policy Studio as above, but point it at the current node's Node Manager configuration.
 - Edit the "Management HTTPS Interface" as above.
 - Import the exported Domain CA certificate as above.
 - Import the exported "topology-cert" for this node as above.
 - Set the Issuer on the imported "topology-cert" as above.
 - If there is a duplicate Node Manager certificate, Remove it.
 - Edit the "Management HTTPS Interface", to use imported certificates as above.
 - Copy the project contents to the ~/7.5.0/apigateway/conf/fed directory.
 - Restart the Node Manager on the current node.
 - For <u>each</u> API Gateway instance on the current node, edit the mgmt.xml to contain the correct Domain CA dname.
 - For <u>each</u> API Gateway instance on the current node, copy the certs.xml from the old version to the 7.5.0 install, e.g. cp ~/7.3.1/apigateway/group-

2/instance-1/conf/certs.xml ~/7.5.0/apigateway/group-2/instance-1/conf/certs.xml.

- Restart each API Gateway instance.
- There is no need to copy the apigateway/groups/certs directory on subsequent nodes.
- Check out <u>https://anm-host:8090</u>, all API Gateways running on this node should have a live status.

The following sections give more concrete examples of the procedure to revert the SSL certificates, for a single node 7.3.1 system, and a multi-node 7.3.1 system.

Example 7.3.1 -> 7.5.0 Single Node Upgrade

Create 7.3.1 Single Node System

If an API Gateway domain is using the default SSL management certificate option, (i.e. system generated keys and certificates), the default dname for the Domain CA certificate is CN=Domain. Create a 7.3.1 single node system with a single API Gateway instance with a non-default dname for the Domain CA certificate so that we can see more clearly when we are using the old version certificates, Vs the new default certificates in the 7.5.0 upgraded installation. This is not a requirement, i.e. the Domain CA certificate dname may be the same in the old and new version installations if required. For the purposes of this guide, the dname of the Domain CA in the 7.3.1 domain is CN=7.3.1-Domain. After upgrade, the dname of the Domain CA in the 7.5.0 domain will always be CN=Domain, there is no way to change during sysupgrade. It may be changed post upgrade via a complete regeneration of all SSL certificates, certificate regeneation is not covered here.

Create a 7.3.1 Node Manager using a non-default Domain CA dname as follows:-

cd 7.3.1-install-dir/posix/bin ./managedomain -i --domain_name 7.3.1-Domain

Start the Node Manager.

Create an API Gateway instance.

./managedomain -c -n APIGateway1 -g Group1

Start API Gateway instance.

If upgrading a pre-existing old version with a default Domain CA dname, use the validity times to determine whether you are viewing the old version certificate, or the new version certificate generated during sysupgrade.

View the 7.3.1 Admin Node Manager Certificate

This is an optional step. Start **7.3.1 Policy Studio** and view the certificate details when connecting to the Admin Node Manager.

Do you trust the following Server Certificate?			
Do you trust the following Server Certificate?			
General Details			
Certificate Hierarchy			
▼ 7.3.1-Domain			
nodemanager-1			
Cortificato Fields			
Senarromber			
Signature			
Issuer			
▼ Validity			
Not Before			
Not After			
Subject			
Subject Public Key Info			
Subject Public Key Algorithm			
Subject Public Key			
▼ Extensions			
X509v3 Key Usage			
Field Value			
Wed Jan 08 14:20:59 GMT 2116			A
			=: -
(•($\mathbf{\mathbf{\hat{\mathbf{A}}}}$
]
	ОК	No	Help

Note the CN of the certificate that signs the Node Manager certificate is set to "7.3.1-Domain".

Run Sysupgrade

Run sysupgrade in 7.5.0 installation, pointing it at the 7.3.1 installation and follow normal procedure, bringing down the old version processes when prompted.

cd 7.5.0-install-dir/apigateway/upgrade/bin
./sysupgrade /home/mcollins/AxwayInstalls/GOLD/7.3.1/apigateway

When sysupgrade completes, we should now have a 7.5.0 Admin Node Manager and API Gateway running.

Verify that the domain looks OK in the API Gateway Manager UI, i.e. https://localhost:8090.

View the 7.5.0 Admin Node Manager Certificate

This is an optional step. Start the 7.5.0 Policy Studio. Click "New Project from an API Gateway instance".

Do you trust the following server certificate from host 'localhost'?
Do you trust the following server certificate from host 'localhost'? General Details
Certificate Hierarchy
▼ Domain
nodemanager-1
Certificate Fields
▼ nodemanager-1
▼ Certificate
Version
Serial Number
Signature
Issuer
▼ Validity
Not Before
Not Arter
Subject
Subject Public Key Algorithm
Field Value
Wed Jan 08 14:34:17 GMT 2116
No Help OK

We see that a different Validity period and the CN of the Domain CA certificate is "Domain" as opposed to "7.3.1-Domain". We will now start to revert the SSL certificates for the 7.5.0 installation back to those used in the 7.3.1 domain.

Extract the 7.3.1 Certificate Details for the Domain CA and the Admin Node Manager

Use the 7.3.1 Policy Studio.

Choose the "Open File" option and point at the 7.3.1-installdir/apigateway/conf/fed/configs.xml file. Browse to "Certificates and Keys".

😣 🗆 🗉 File Edit Navigate	a Tasks	s Tools Window Help		
🛿 🛟 File: configs.xml 🏻 »1		≣ 🗢 ▼ 🗇 ▼ 🗄 😫 🗉 🖾 Exp	ort All 🚵 Import] 🛛 🏅
type filter text	åå⊽	🗣 Certificates and Keys 🛛 🤗 Certificates 😂	3	- 5
▼		Certificates with Keys Certificates CA		
 Business Services Policies External Connections 		Alias	Certificate Name	Ехрігу
 Resources E Libraries Certificates and Keys 		 topology-cert CN=Change this for production 	CN=nodemanager-1,OU=group-1,DC=host-1	Wed Jan 08 14:
 Certificates Key Pairs 		CN=Samples Test CA		
 PGP Key Pairs Sers and Groups Package Properties Server Settings 				
			Create/Import Edit View Rem	Keystore

Under the "Certificates with Key" tab, find the "topology-cert", click "Edit" Then click "Export Certificate and Key" and save the key and cert to a file on disk, e.g. 7.3.1.p12.

😣 🗆 🗉 File Edit Navigate	Tasks	Tools Window Help	
🛿 🔁 File: configs.xml		ः 🗢 र ः 😫 ा 🗗 Export All 🔤 Imp	ort 🔤 🖉 🦉
type filter text	ä∗	🗣 Certificates and Keys 🕱 🦃 Certificates 😫	- 8
 ▼ Conversion > Node Manager > Mathematical Structure > Mathematical Structure 		Certificates with Keys Certificates CA	
 Several Services Delicies External Connections Resources Extraites Certificates and Keys Certificates Certificates PGP Key Pairs PGP Key Pairs Berger Server Settings 		Alias Alias Alias AC Camerfirma S.A. AC Camerfirma SA CIF A82743287 AddTrust AB America Online Inc. Baltimore Certplus CN=7.3.1-Domain CN=7.3.1-Domain CN=AxwavRootCA.DC=axwav.DC=int C	Certificate Name
		Crea	ate/Import Edit View Remove Keystore

Under the "CA" tab, find the Domain CA certificate with alias "CN=7.3.1-Domain", click "Edit".

Then click "Export Certificate" and save the certificate to a file on disk, e.g. 7.3.1-domain-cert.pem.

Close 7.3.1 Policy Studio.

Revert the SSL Certificate for the 7.5.0 Admin Node Manager

Run 7.5.0 Policy Studio.

Create a new project based on the 7.5.0 Node Manager configuration, use the "From existing configuration" option and point at the 7.5.0-install-dir/apigateway/conf/fed directory.

Browse to "Listeners/Node Manager/Management Services/Ports" and edit the "Management HTTPS Interface".

Update it temporarily so that it does not use the "topology-cert" certificate on the "Network" tab, select any other certificate.

Click on the "Mutual Authentication" tab and ensure that the "CN=Domain" certificate is not selected as a trusted certificate.

Click OK.

Browse to "Certificates and Keys".

On the "Certificates with Keys" tab, find the "topology-cert". Select it and click "Remove".

⊗⊡ □ File Edit Navigate Tasks Tools Window	Help										
¤ 🔁 zz "1]= 💠	• • 🗢 • = 😫 = 🔤 Imp	ort Configuration F	ragment					- <u>6</u> 9		0 [
type filter text 👪	•	Certificates and Keys	🍘 Management S	Services - Ports	🤗 Certificates 😫						- 0
View Listeners View Anager View APIs View APIs View APIs View APIs View APIs View Anager View Node Manager View Node		Certificates and Keys Certificates with Keys (type filter text Alias CN=Change this for p CN=Domain CN=Domain CN=Samples Test CA	oroduction	Certificate Nam	e er-1,0U=group=1,DC	Expi	ry Jan 08 14:34:17 GMT 21	16			
🖉 Server Settings								Create/Import Edi	tView	Remove	Keystore
]]	119M o	213M 📋

Under the "CA" tab, find the Domain CA key, ie. "CN=Domain", that signed the "topology-cert", select it and click "Remove".

🐵 🗆 😐 File Edit Navigate Tasks Tools Window Hel	þ			
⊠ 😌 ZZ "1	🖕 💌 🐟 💌 🖩 🔛 Import Configuration Fragment		5 <u>6</u> 3	0 [🌜
type filter text 🔗 💌	😤 Certificates and Keys 🦉 Management Services - F	Ports 🔮 Certificates 😣		- 0
▼ 🔁 zz [Node Manager]	Certificates with Keys Certificates CA			
APIs				
Policies	type filter text			(8)
Resources	Alias	Certificate Name	Expiry	
Environment Configuration	CN=AxwayRootCA,DC=axway,DC=int			
🔻 🏟 Listeners	🔻 🛅 CN=Domain			
🔻 🏟 Node Manager	🛃 CN=Domain	CN=Domain	Wed Jan 08 14:34:17 GMT 2116	
Management Services	Comodo CA Limited			
Ports	Deutsche Telekom AG			
Paths	DigiCert Inc			
🕮 Virtual Hosts	Entrust, Inc.			
External Connections	Entrust.net			
🕨 🚘 Libraries	Equifax			
🔻 🗣 Certificates and Keys	Equifax Secure Inc.			
😤 Certificates	GeoTrust Inc.			
🔎 Key Pairs	▶ 🛅 GlobalSign			
b PGP Key Pairs	GlobalSign nv-sa			
Users and Groups	GTE Corporation			
Package Properties	KEYNECTIS			
🖉 Server Settings	L.m		I	
			Create/Import Edit View Remov	e Keystore

Under the "CA" tab, you will also find the "CN=7.3.1-Domain" certificate. This remains in the Node Manager configuration after upgrade. Remove this also.

Click "Create/Import".

Click "Import Certificate". Select the domain CA certificate file, e.g. 7.3.1-domain-cert.pem. Select "Use Subject" for alias. Click OK.

Click "Create/Import" again. Click "Import Certificate + Key". Select the p12 file exported from 7.3.1, e.g. 7.3.1.p12. Enter "topology-cert" as the "Alias Name". Click OK.

Select the "Certificates" tab, select the CN=nodemanager-1, OU=group-1..." certificate. Click "Remove".

Select the "topology-cert" again. Edit and select "Choose Issuer Certificate" and set it to "CN=7.3.1-Domain". Click OK.

× 🗆 Configu	ire Certificat	e and Private Key			
X.509 Certifica	icate <i>P</i> riv	ate Key			
Subject:	CN=nodemar	nager-1,OU=group-1,DC=host-1		Edit	
Alias Name: topology-cert Use Subject					
Public Key:		8-bit rsaEncryption key		Import	
Version:	3	8 💷 Select Certificate			
Issuer:	CN=7.3.1-D	Choose a specific Certificate			
Choose Is	suer Certific	Certificates			
Not valid be	fore:	Alias	Certificate Name	Expiry	
		CN=7.3.1-Domain			
Import Cert	ificate E	✓ E CN=7.3.1-Domain	CN=7.3.1-Domain	Wed Jan 08 16:2:	
			Create/Import Edit View	Remove Keystore	
		O Bind the Certificate at runtime			
		Binding variable \${env.}			
			Cancel Hel	рОК	

The following should now be seen on the "Certificates" screen tabs:-Tab "Certificates with Keys":



Tab "Certificates":

3 🔁 qaqa 👌 "ı	≡ 存 ▼ 🖨	🔻 📱 🖹 🖿 Import Configuration Fragm	nent 📲 🚰	0 🛛
ype filter text 🛛 👪 🔻	🏟 Node Manager 🛛 🦉 Man	agement Services - Ports 🦃 Certificate	s 🛛	- 5
😌 qaqa [Node Manager]	Certificates with Keys Certi	ficates CA		
 Policies 	type filter text			X
 Resources Environment Configuration Listeners Node Manager Management Services Ports Ports Paths Virtual Hosts External Connections 	Alias	Certificate Name	Expiry	
Libraries				

Ensure <u>no</u> nodemanager certificate is listed on the tab above.

Tab "CA":

😸 🗆 🗉 File Edit Navigate Tasks Tools Window Hel	p			
₩ 🔁 ZZ "1	🗢 💌 💠 👻 🗄 🖆 Import Configuration Fragmer	nt	: 5 1	0 🛛
type filter text 🛛 🕅 🔻	😤 Certificates and Keys 🧉 Management Services	- Ports 🔮 Certificates 😫		- 0
▼ 🕀 zz [Node Manager]	Certificates with Keys Certificates CA			
▶ 🤤 APIs ▶ 👩 Policies	type filter text			×
Resources	Alias	Certificate Name	Expiry	2
🔻 🎤 Environment Configuration	AddTrust AB			\sim
🔻 🟟 Listeners	America Online Inc.			
🔻 🏟 Node Manager	Baltimore			
🔻 🕟 Management Services	Certplus			
Ports	▼ 🛅 CN=7.3.1-Domain			
Paths	CN=7.3.1-Domain	CN=7.3.1-Domain	Wed Jan 08 14:20:59 GMT 2116	
🕮 Virtual Hosts	CN=AxwayRootCA,DC=axway,DC=int			\cup
External Connections	Comodo CA Limited			
🕨 🛲 Libraries	Deutsche Telekom AG			
🔻 🚔 Certificates and Keys	DigiCert Inc			
😤 Certificates	Entrust, Inc.			
🔎 Key Pairs	Entrust.net			
b PGP Key Pairs	Equifax			
Users and Groups	Equifax Secure Inc.			
Be Package Properties	🕨 🛅 GeoTrust Inc.			

Browse to "Listeners/Node Manager/Management Services/Ports" and edit the "Management HTTPS Interface".

Update it to use the "topology-cert" certificate on the "Network" tab.

Click on the "Mutual Authentication" tab and ensure that the Domain CA certificate from the old version, i.e. "CN=7.3.1-Domain", is selected as a trusted certificate.

Click OK.

Close the project.

Take a backup of 7.5.0-install-dir/apigateway/conf/fed. Go to the project directory on disk that you used above in the 7.5.0 Policy Studio. Copy all files in the project directory to 7.5.0-install-dir/apigateway/conf/fed. Restart the Admin Node Manager.

At this point only the Admin Node Manager has been reset to use the SSL certificates from 7.3.1. It cannot talk to the local API Gateway instance yet. Verify the trace for the Admin Node Manager is using the old 7.3.1 certificate, search for this trace statement:-

INFO 01/Feb/2016:14:56:41.738 [5537:00000000000000000000000] Topology certificate: dname=CN=nodemanager-1,0U=group-1,DC=host-1, issuer=CN=7.3.1-Domain, expiry=Wed Jan 08 14:20:59 GMT 2116

There will be lots of SSL errors in the Admin Node Manager trace file as it it trying to communicate with the local API Gateway, which is still using the default 7.5.0 SSL certificate signed by Domain CA with dname CN=Domain.

Revert the SSL Certificate for the 7.5.0 API Gateway

Edit the 7.5.0-install-dir/apigateway/groups/group-2/instance-1/conf/mgmt.xml, change the TrustedCA to be the dname of the 7.3.1 domain CA certificate. If the dname of the Domian CA in the old version was "CN=Domain", this step may be skipped.

```
<HTTP monitoringEnabled="false" name="Management Services" provider="HTTP">
    <$$LInterface activetimeout="60000" address="localhost" auditConn="1" backlog="64"
ciphers="FIPS:!SSLv3:!aNULL" clientAuth="required" depth="1"
dhParams="MEYCQQDaWDwW2YUiidDkr3VvTMqS3Uv1M7gE+w/t10+cikQD7VdGUNNpmdsp13Yna6LT1BLiGPTdHghM9tgAPnx
HdOgzAgEC" enabled="1" idletimeout="60000" inputEncodings=".inherit" maxRequestMemory="16777216"
name="Internal Management HTTPS Interface" opsSettingsUsage="PORT" outputEncodings=".inherit"
port="${env.PORT.MANAGEMENT}" protocol="any" recordCircuitPath="0" recordInboundTxns="0"
recordOutboundTxns="0" recordTrace="0" resolveSubjectCNtoNetAddr="0" reuseAddress="false"
ssloptions="nosslv2 nosslv3" tracelevel="INHERIT" transparentProxy="false">
        <include file="certs.xml" />
        <Identity cert="topology-cert" />
        <VerifyHasTrustedSigner />
        <VerifyIsLocalNodeManager />
   <TrustedCA cert="CN=7.3.1-Domain" /></SSLInterface>
   <MetricsFeedServer httpMethod="*" uriprefix="/metrics" />
   <OPDbViewer httpMethod="*" provider="HTTPops" uriprefix="/ops/" />
    <Application httpMethod="*" sessiontimeoutSeconds="300" uriprefix="/">
        <Servlet class="org.glassfish.jersey.servlet.ServletContainer" name="api" uri="api">
            <Property name="jersey.config.server.provider.classnames"
value="org.glassfish.jersey.media.multipart.MultiPartFeature" />
            <Property name="jersey.config.server.provider.packages"
value="com.vordel.api.monitoring;com.vordel.api.management;com.vordel.api.configuration;com.vorde
1.dwe.file;com.vordel.kps.rest;com.vordel.api.domainaudit;com.vordel.ama.rest;com.vordel.api.disc
overy" />
        </Servlet>
    </Application>
</HTTP>
```

Take a backup of the certs.xml file for the API Gateway instance in the 7.5.0 installation, i.e. 7.5.0-install-dir/apigateway/groups/group-2/instance-1/conf/certs.

Copy the 7.3.1-install-dir/apigateway/groups/group-2/instance-1/conf/certs.xml to the equivalent 7.5.0 directory.

Restart the local API Gateway.

Verify the 7.5.0 Domain is Operational

Open the API Gateway Manager UI and ensure that the API Gateway status is OK.

Copy Domain CA Key and Certificate from Old Version to 7.5.0

Make a backup of directory 7.5.0-install-dir/groups/certs.

Copy the content of directory 7.3.1-install-dir/groups/certs into the 7.5.0 equivalent.

This step is required if the old version was using system generated certificates. No processes need to be restarted after carrying out this step.

Create a New API Gateway Instance in the 7.5.0 Domain

./managedomain -c -n APIGateway2 -g Group2 --instance_management_port 6085 --instance_services_port 6086

Note: Choose two unused port numbers for the management port and services ports. Start the API Gateway and ensure the status of it is OK on the API Gateway Manager UI.

Example 7.3.1 -> 7.5.0 Multi-Node Upgrade

Create 7.3.1 Multi-Node System

We use a non-default Domain CA dname in this example, this is not a requirement, see the single node example for more information on this topic.

We will revert the SSL certificates of a 2 node 7.3.1 system with the following topology:-

- NodeA: ANM, APIGateway1 in Group1
- NodeB: NM, APIGateway2 in Group1

On NodeA:-

• Create a 7.3.1 Admin Node Manager on NodeA using a non-default Domain CA dname as follows:-

cd 7.3.1-install-dir/posix/bin

./managedomain -i --domain_name 7.3.1-Domain --anm_host NodeA

- Start the Admin Node Manager on NodeA.
- Create an API Gateway instance on NodeA.
 ./managedomain -c -n APIGateway1 -g Group1
- Start API Gateway instance.

On NodeB:-

- Create the Node Manager:cd 7.3.1-install-dir/posix/bin ./managedomain -a --anm_host NodeA --anm_host NodeB
- Start the Node Manager on NodeB.
- Create an API Gateway instance on NodeB.
 ./managedomain -c -n APIGateway2 -g Group1
- Start API Gateway instance.

View the 7.3.1 Admin Node Manager Certificate

This is an optional step. Start **7.3.1 Policy Studio** and view the certificate details when connecting to the Admin Node Manager.

Do you trust the following Server Certificate?			
Do you trust the following Server Certificate? General Details			
Certificate Hierarchy			
▼ 7.3.1-Domain			
nodemanager-1			
Certificate Fields			
Schartaunder			
Signature			
Issuer			0
Validity			
Not After			
Subject			
Subject			
Subject Public Key Algorithm			
Subject Public Key			
▼ Extensions			
X509v3 Key Usage			
Field Value			
Wed Jan 08 14:20:59 GMT 2116			Â
			8
(4)			
	ОК	No	Help

Note the CN of the certificate that signs the Admin Node Manager certificate is set to "7.3.1-Domain".

Run Sysupgrade on NodeA and NodeB

Run sysupgrade in 7.5.0 installation, pointing it at the 7.3.1 installation and follow normal procedure, bringing down the old version processes when prompted.

On NodeA:

```
cd 7.5.0-install-dir/apigateway/upgrade/bin
./sysupgrade /home/mcollins/AxwayInstalls/GOLD/7.3.1/apigateway
```

Run the export, preupgrade, upgrade, applydb steps on NodeA, then goto NodeB

On NodeB:

cd 7.5.0-install-dir/apigateway/upgrade/bin

./sysupgrade /home/mcollins/AxwayInstalls/GOLD/7.3.1/apigateway
--anm_host NodeA

Run the export, preupgrade, upgrade, applydb steps on NodeB, then stop all old version processes on NodeA and NodeB.

Return to **NodeA** and run the apply step.

Return to **NodeB** and run the apply step.

When sysupgrade completes, we should now have an equivalent 7.5.0 domain running on NodeA and NodeB.

Verify that the domain looks OK in the API Gateway Manager UI.

View the 7.5.0 Admin Node Manager Certificate

This is an optional step. Start the 7.5.0 Policy Studio Click "New Project from an API Gateway instance".

Do you trust the following server certificate from host 'localhost'?
Do you trust the following server certificate from host 'localhost'? General Details
Certificate Hierarchy
▼ Domain
nodemanager-1
Certificate Fields
▼ nodemanager-1
▼ Certificate
Version
Serial Number
Signature
Issuer
▼ Validity
Not Before
Not Arter
Subject
Subject Public Key Algorithm
Field Value
Wed Jan 08 14:34:17 GMT 2116
No Help OK

We see that a different Validity period and the CN of the Domain CA certificate is "Domain" as opposed to "7.3.1-Domain". We will now start to revert the SSL certificates for the 7.5.0 domain back to those used in the 7.3.1 domain.

Extract the 7.3.1 Certificate Details for the Domain CA and the Admin Node Manager on Node A

Use the 7.3.1 Policy Studio.

Choose the "Open File" option and point at the 7.3.1-installdir/apigateway/conf/fed/configs.xml file on **NodeA**. Browse to "Certificates and Keys".

😣 🗆 😐 File Edit Navigate	Tasks	Tools Window Help		
없 😌 File: configs.xml 🛛 »1		≣ 🗘 ▼ 🖘 🗟 ≣ 🗳 Exp	ort All 🚵 Import	0 🌜
type filter text	åå⊽	🥞 Certificates and Keys 🛛 🥞 Certificates 🕿	3	- 8
 ▼	Certificates with Keys Certificates CA			
 Policies External Connections 		Alias ▼	Certificate Name	Expiry
 Resources E Libraries Certificates and Keys 		 topology-cert CN=Change this for production 	CN=nodemanager-1,OU=group-1,DC=host-	1 Wed Jan 08 14:
 Certificates Key Pairs 		CN=Samples Test CA		
 PGP Key Pairs Users and Groups Or Package Properties Server Settings 				
			Create/Import Edit View Ren	Keystore

Under the "Certificates with Key" tab, find the "topology-cert., click "Edit" Then click "Export Certificate and Key" and save the key and cert to a file on disk, e.g. 7.3.1-NodeA.p12.

😣 🗆 🗉 File Edit Navigate T	asks Tools Window Help		
🛿 🔁 File: configs.xml 🔭	🗉 🔶 🔻 ই 📰 🗄 Export All	🖄 Import] 🤉 🍆
type filter text	👻 🗣 Certificates and Keys 🛿 🤗 Certificates 🛛		- 0
 ▼ ⊖ Node Manager ▶ Isteners ▶ Business Services 	Certificates with Keys Certificates CA		
 Delicies Delicies External Connections Resources Libraries Certificates and Keys Certificates Key Pairs PGP Key Pairs BPGP Key Pairs Mesers and Groups Deckage Properties Server Settings 	Alias Alias AC Camerfirma S.A. AC Camerfirma SA CIF A82743287 AddTrust AB AddTrust AB AddTrust AB Baltimore Baltimore CR=7.3.1-Domain CN=7.3.1-Domain CN=AxwavRootCA.DC=axwav.DC=int CN=AxwavRootCA.DC=axwav.DC=int CN=AxwavRootCA.DC=int CN=AxwavRootCA.DC=int CN=AxwavRootCA.DC=	Certificate Name CN=7.3.1-Domain Create/Import Edit View Remove	Keystore
			Reystore

Under the "CA" tab, find the Domain CA certificate with alias "CN=7.3.1-Domain", click "Edit".

Then click "Export Certificate" and save the key and cert to a file on disk, e.g. 7.3.1-domain-cert.pem.

Extract the 7.3.1 Certificate Details for the Node Manager on NodeB

Use the 7.3.1 Policy Studio.

Choose the "Open File" option and point at the 7.3.1-installdir/apigateway/conf/fed/configs.xml file on **NodeB**. Browse to "Certificates and Keys".

Studio - Certificates	pate # Loop Don (1) # Among # 1012	· 111 · pringetallo ·				
File Edit Navigate Tasks Tools	Window Help					
🛙 🔁 File: configs.xml 🔭	⇔ → → 😫 ⊿	Export All 🚵 Import	0 💊			
type filter text 🛛 🕅 ▼	😌 Node Manager 🛛 🤗 Certificates 🖾		- 0			
🔁 Node Manager	Certificates with Keys Certificates CA					
Listeners	ture filter tout					
😂 Business Services	type litter text					
Policies	Alias	Certificate Name	Expiry			
External Connections	CN=7.3.1-Domain					
a Resources	🖺 topology-cert	CN=nodemanager-2,OU=group-1,DC=hos	Wed Jan 08			
🚔 Libraries	CN=Change this for production					
Certificates and Keys	CN=Samples Test CA					
Certificates						
Key Pairs						
PGP Key Pairs						
Series and Groups						
Sonror Sottings						
Server settings						
		Create/Import Ed	dit View Remove Keystore			
44M of 60M						

Under the "Certificates with Key" tab, find the "topology-cert., click "Edit" Then click "Export Certificate and Key" and save the key and cert to a file on disk, e.g. 7.3.1-NodeB.p12.

Close 7.3.1 Policy Studio.

Revert the SSL Certificate for the 7.5.0 Admin Node Manager on NodeA

Run 7.5.0 Policy Studio.

Create a new project based on the 7.5.0 Node Manager configuration, use the "From existing configuration" option and point at the 7.5.0-install-dir/apigateway/conf/fed directory on **NodeA**.

Browse to "Listeners/Node Manager/Management Services/Ports" and edit the "Management HTTPS Interface".

Update it temporarily so that it does not use the "topology-cert" certificate on the "Network" tab. Click on the "Mutual Authentication" tab and ensure that the "CN=Domain" certificate is not selected as a trusted certificate.

Click OK.

Browse to "Certificates and Keys". On the "Certificates with Keys" tab, find the "topology-cert". Select it and click "Remove".

😕 💷 File Edit Navigate Tasks Tools Window	Help											
¤ 🔁 zz "1	🔶	🔹 🗢 🔹 🔡 🗉 Import	t Configuration Frag	jment					- 5		0 [ļ
type filter text	•	Certificates and Keys	🖲 Management Serv	vices - Ports	🤗 Certificates 😫						- 0	
▼ 🔁 zz [Node Manager] ▶ 🕼 APIs ▶ 🗊 Policies		Certificates with Keys Certificates with Keys	ificates CA								X	
		Alias CN=Change this for pro CN=Domain	Cuduction	ertificate Name	2	Expiry						
 ▼ № Node Manager ▼ Management Services ♥ Ports ▶ ♥ Ports ♥ ♥ Orts ♥ ♥ Orts ♥ ♥ Certificates and Keys ♥ ♥ Certificates and Keys ♥ Certificates ▶ Key Pairs ▶ PCP Key Pairs ▶ @ Users and Groups ▶ ♥ ♥ Gene Porte 	_	 ♀ topology-cert ▶ ■ CN-Samples Test CA 	c	N=nodemanagi	er-1,OU=group-1,DC=ho:	st-1 Wed Jan	06 14:34:17 GMT 2	116				
]	Create/Import	Edit View	Remove	Keystore	

Under the "CA" tab, find the Domain CA key ("CN=Domain") that signed the "topology-cert". Select it and click "Remove".

🐵 🗆 🗉 File Edit Navigate Tasks Tools Window Help	0								
⊠ 🔁 zz "1	Þ 🔹 🔿 🔻 🗄 🔡 Import Configu	ration Fragment			87 E	0 [🌜			
type filter text 🛛 👪 🔻	😤 Certificates and Keys 🛛 🦉 Manag	ement Services - Ports	😤 Certificates 🔀			- 0			
▼ 🔁 zz [Node Manager]	Certificates with Keys Certificates	CA							
APIs									
Policies	type filter text					(1)			
Resources	Alias	c	ertificate Name		Expiry				
🔻 🎤 Environment Configuration	CN=AxwayRootCA,DC=axway,D	C=int							
🔻 🟟 Listeners	🔻 🛅 CN=Domain								
🔻 🏟 Node Manager	CN=Domain	c	N=Domain		Wed Jan 08 14:34:17 GMT 2116	\cap			
Management Services	Comodo CA Limited								
Ports	Deutsche Telekom AG								
Baths	DigiCert Inc								
🕮 Virtual Hosts	Entrust, Inc.								
External Connections	Entrust.net								
🕨 🚘 Libraries	▶ 🛅 Equifax								
🔻 🖤 Certificates and Keys	Equifax Secure Inc.								
😤 Certificates	GeoTrust Inc.								
🔎 Key Pairs	GlobalSign								
🤣 PGP Key Pairs	GlobalSign nv-sa								
Users and Groups	GTE Corporation								
• @ Package Properties	KEYNECTIS								
Server Settings	L	1			1				
					Create/Import Edit View R	emove Keystore			

Under the "CA" tab, you will also find the "CN=7.3.1-Domain" certificate. This remains in the Node Manager configuration after upgrade. Remove this also.

Click "Create/Import".

Click "Import Certificate". Select the domain CA certificate file, e.g. 7.3.1-domain-cert.pem. Select "Use Subject" for alias. Click OK.

Click "Create/Import" again. Click "Import Certificate + Key". Select the p12 file exported from 7.3.1, e.g. 7.3.1-NodeA.p12. Enter "topology-cert" as the "Alias Name". Click OK.

Select the "Certificates" tab, select the CN=nodemanager-1, OU=group-1..." certificate. Click "Remove".

Select the "topology-cert" again. Select "Choose Issuer Certificate" and set it to "CN=7.3.1-Domain". Click OK.

× 🗉 Config	ure Certificat	e and Private Key		
X.509 Certif	ficate 🔑 Priva	ate Key		
X.509 Certifica	ate			
Subject:	CN=nodemar	nager-1,OU=group-1,DC=host-1		Edit
Alias Name:	topology-cer	t		Use Subject
Public Key:		8-bit rsaEncryption key		Import
Version:	3	8 💷 Select Certificate		
Issuer:	CN=7.3.1-D	Choose a specific Certificate		
Choose Is	ssuer Certific	Certificates		
Not valid be	fore:	type filter text		×
25 / Jan		Alias	Certificate Name	Expiry
		CN=7.3.1-Domain		
Import Cert	ificate E	🗹 🛃 CN=7.3.1-Domain	CN=7.3.1-Domain	Wed Jan 08 16:2!
			Create/Import Edit View	Remove Keystore
	-			
		O Bind the Certificate at runtime		
		Binding variable \${env.}		
			Cancel Help	ОК

The following should now be seen on the "Certificates" screen for each tab:-Tab "Certificates with Keys":



Tab "Certificates":

X 🔁 qaqa 👌	= 🗢 💌 🖨	🔻 🗄 🔡 Import Con	nfiguration Fragment	83 E	0
type filter text 🛛 👪 🔻	🕸 Node Manager 🛛 🦉 Mana	gement Services - Ports	🥞 Certificates 🛿		- 0
😌 qaqa [Node Manager]	Certificates with Keys Certifi	cates CA			
APIs Policies	type filter text				×
Resources	Alias	Certificat	e Name	Expiry	
🔻 🌽 Environment Configuration					
▼ 📣 Listeners					
🔻 🏟 Node Manager					
▼ Management Services					
▶ 🥮 Ports					
Paths					
I Virtual Hosts					
▶ Image: Participation Participation Participation					
🕨 🚘 Libraries					
Certificates and Keys			Create/Import	Edit View Remove	Keystore
······································		1		72M	of 191M

Ensure <u>no</u> nodemanager certificate is listed on the tab above.

🛞 🗆 🗉 File Edit Navigate Tasks Tools Window	Help			
¤⇔zz "1	🗉 🗢 💌 💠 👻 🗄 🔛 Import Configuration Fragment			0 🛛
type filter text	👻 🎈 Certificates and Keys 🛛 🎯 Management Services - Por	ts 🥊 Certificates 🛿		- 0
▼ 🔁 zz [Node Manager] ▶ 🗐 APIs	Certificates with Keys Certificates CA			
Policies	type filter text			×
Resources	Alias	Certificate Name	Expiry	
Environment Configuration	AddTrust AB			
🔻 🏟 Listeners	America Online Inc.			
🔻 🏟 Node Manager	Baltimore			
Management Services	Certplus			
Ports	CN=7.3.1-Domain			
Paths	CN=7.3.1-Domain	CN=7.3.1-Domain	Wed Jan 08 14:20:59 GMT 2116	
3 Virtual Hosts	CN=AxwayRootCA,DC=axway,DC=int			
External Connections	Comodo CA Limited			
🕨 🛲 Libraries	Deutsche Telekom AG			
🔻 👮 Certificates and Keys	DigiCert Inc			
😤 Certificates	Entrust, Inc.			
🔎 Key Pairs	Entrust.net			
PGP Key Pairs	Equifax			
Users and Groups	Equifax Secure Inc.			
Package Properties	GeoTrust Inc.			

Browse to "Listeners/Node Manager/Management Services/Ports" and edit the "Management HTTPS Interface".

Update it to use the "topology-cert" certificate on the "Network" tab.

Click on the "Mutual Authentication" tab and ensure that the Domain CA certificate from the old version, i.e. "CN=7.3.1-Domain", is selected as a trusted certificate. Click OK.

Close the project.

Take a backup of 7.5.0-install-dir/apigateway/conf/fed.

Go to the project directory on disk that you used above in the 7.5.0 Policy Studio. Copy all files in the project directory to 7.5.0-install-dir/apigateway/conf/fed. Restart the Admin Node Manager on NodeA.

At this point only the Admin Node Manager on NodeA has been reset to use the SSL certificates from 7.3.1. It cannot talk to the local API Gateway instance yet, or the remote Node Manager on NodeB. SSL errors will be visible in the trace. Verify the trace for the Admin Node Manager on NodeA is using the old 7.3.1 certificate, search for this trace statement:-

INFO 01/Feb/2016:14:56:41.738 [5537:00000000000000000000000] Topology certificate: dname=CN=nodemanager-1,0U=group-1,DC=host-1, issuer=CN=7.3.1-Domain, expiry=Wed Jan 08 14:20:59 GMT 2116

Revert the SSL Certificate for the 7.5.0 API Gateway on NodeA

Edit the 7.5.0-install-dir/apigateway/groups/group-2/instance-1/conf/mgmt.xml, change the TrustedCA to be the dname of the 7.3.1 domain CA certificate.

```
<HTTP monitoringEnabled="false" name="Management Services" provider="HTTP">
    <SSLInterface activetimeout="60000" address="localhost" auditConn="1" backlog="64"
ciphers="FIPS:!SSLv3:!aNULL" clientAuth="required" depth="1"
dhParams="MEYCQQDaWDwW2YUiidDkr3VvTMqS3Uv1M7gE+w/t10+cikQD7VdGUNNpmdsp13Yna6LT1BLiGPTdHghM9tgAPnx
HdOgzAgEC" enabled="1" idletimeout="60000" inputEncodings=".inherit" maxRequestMemory="16777216"
name="Internal Management HTTPS Interface" opsSettingsUsage="PORT" outputEncodings=".inherit"
port="${env.PORT.MANAGEMENT}" protocol="any" recordCircuitPath="0" recordInboundTxns="0"
recordOutboundTxns="0" recordTrace="0" resolveSubjectCNtoNetAddr="0" reuseAddress="false"
ssloptions="nosslv2 nosslv3" tracelevel="INHERIT" transparentProxy="false">
        <include file="certs.xml" />
        <Identity cert="topology-cert" />
        <VerifyHasTrustedSigner />
        <VerifyIsLocalNodeManager />
    <TrustedCA cert="CN=7.3.1-Domain" /></SSLInterface>
   <MetricsFeedServer httpMethod="*" uriprefix="/metrics" />
   <OPDbViewer httpMethod="*" provider="HTTPops" uriprefix="/ops/" />
    <Application httpMethod="*" sessiontimeoutSeconds="300" uriprefix="/">
        <Servlet class="org.glassfish.jersey.servlet.ServletContainer" name="api" uri="api">
            <Property name="jersey.config.server.provider.classnames"
value="org.glassfish.jersey.media.multipart.MultiPartFeature" />
            <Property name="jersey.config.server.provider.packages"
value="com.vordel.api.monitoring;com.vordel.api.management;com.vordel.api.configuration;com.vorde
1.dwe.file;com.vordel.kps.rest;com.vordel.api.domainaudit;com.vordel.ama.rest;com.vordel.api.disc
overy" />
        </Servlet>
    </Application>
</HTTP>
```

Take a backup of the certs.xml file for the API Gateway instance, i.e. 7.5.0-install-dir/apigateway/groups/group-2/instance-1/conf/certs.xml

Copy the 7.3.1-install-dir/apigateway/groups/group-x/instancex/conf/certs.xml to the equivalent 7.5.0 directory.

Restart the local API Gateway on NodeA.

Revert the SSL Certificate for the 7.5.0 Admin Node Manager on NodeB Repeat the same steps as described for NodeA. Ensure that 7.3.1-NodeB.p12 file is imported, i.e. the file specific to NodeB.

Revert the SSL Certificate for the 7.5.0 API Gateway on NodeB Repeat the same steps as described for NodeA.

Verify the 7.5.0 Domain is Operational

Open the API Gateway Manager and ensure that the API Gateway status is OK. All API Gateway instances should have a live status.

Copy Domain CA Key and Certificate from Old Version to 7.5.0

On NodeA only, make a backup of directory 7.5.0-install-dir/groups/certs.

Copy the content of directory 7.3.1-install-dir/groups/certs into the 7.5.0 equivalent.

This step is required if the old version was using system generated certificates. No processes need to be restarted after carrying out this step.

Create a New API Gateway Instance in the 7.5.0 Domain

On NodeA or NodeB:-

./managedomain -c -n APIGateway2 -g Group2 --instance_management_port 6085 --instance_services_port 6086

Note: Choose two unused port numbers for the management port and services port. Start the API Gateway and ensure the status of it is OK on the API Gateway Manager UI.