Symantec™
A Division of Broadcom

Notification Server Domain or Host Name Change for ITMS 8.5 RU4+ Whitepaper

Table of Contents

Copyright statement

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Intent

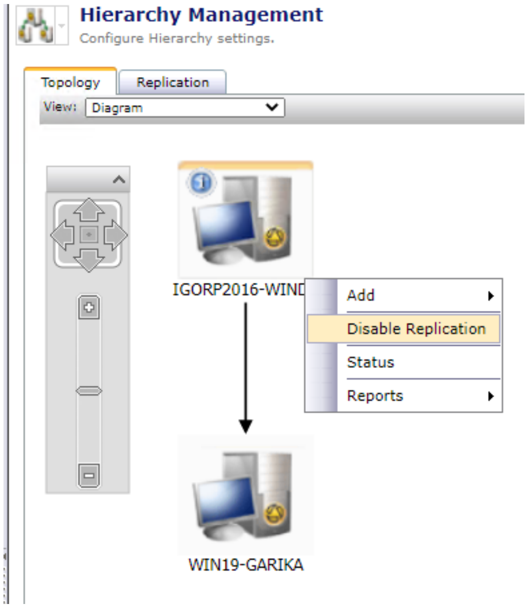
This whitepaper details the procedure required to modify the domain or the host name of an existing IT Management Suite (ITMS) Notification Server (NS), including instances where either Cloud-Enabled Management (CEM) and/or hierarchy are configured.

CAUTION

In this release, you may only change either the hostname or the domain name at one time. If you need to modify both, modify one and repeat this procedure for the other.

Before you begin

If your Notification Server environment is configured to use hierarchy mode, you must disable replication on all parent and child ITMS Notification Servers before modifying your configuration.



Define the New Domain or Host Name

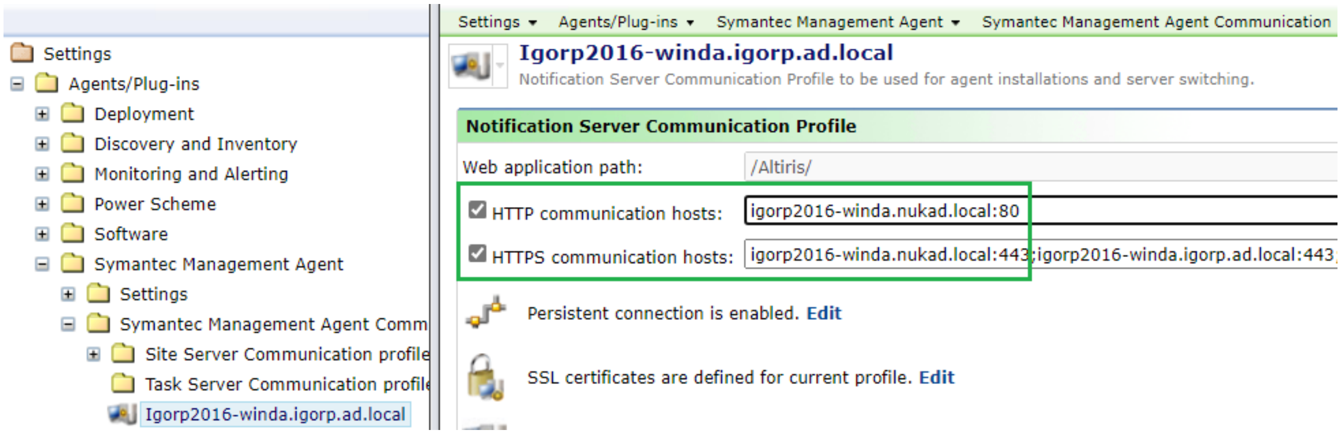
IMPORTANT
Ensure that the new NS domain name or host name can be resolved by the existing CEM gateway, managed intranet clients, site servers, and other hierarchy-managed notification servers.

1. Update the Default NS communication profile.

   Add the new NS domain or the new NS hostname for HTTP and HTTPS, and import a newly issued certificate(s) for the new domain or hostname. If you aren't familiar with the process to create a signed certificate, see https://aboutssl.org/how-to-create-a-self-signed-certificate-in-iis. ITMS certificate requirements can be found here.

   a) From the **SMP Console**, select **Settings** > **All Settings** and open the default NS Communication profile.

   b) Specify the new NS domain name or hostname for HTTPS (and HTTP if required).


Settings
Agents/Plug-ins
Deployment
Discovery and Inventory
Monitoring and Alerting
Power Scheme
Software
Symantec Management Agent
Settings
Symantec Management Agent Comm
Site Server Communication profile
Task Server Communication profil
Igorp2016-winda.igorp.ad.local
Settings ▾
Agents/Plug-ins ▾
Symantec Management Agent ▾
Symantec Management Agent Communication

Igorp2016-winda.igorp.ad.local

Notification Server Communication Profile to be used for agent installations and server switching.

Notification Server Communication Profile

Web application path: /Altiris/

☑ HTTP communication hosts: igorp2016-winda.nukad.local:80

☑ HTTPS communication hosts: igorp2016-winda.nukad.local:443;igorp2016-winda.igorp.ad.local:443

Persistent connection is enabled. Edit

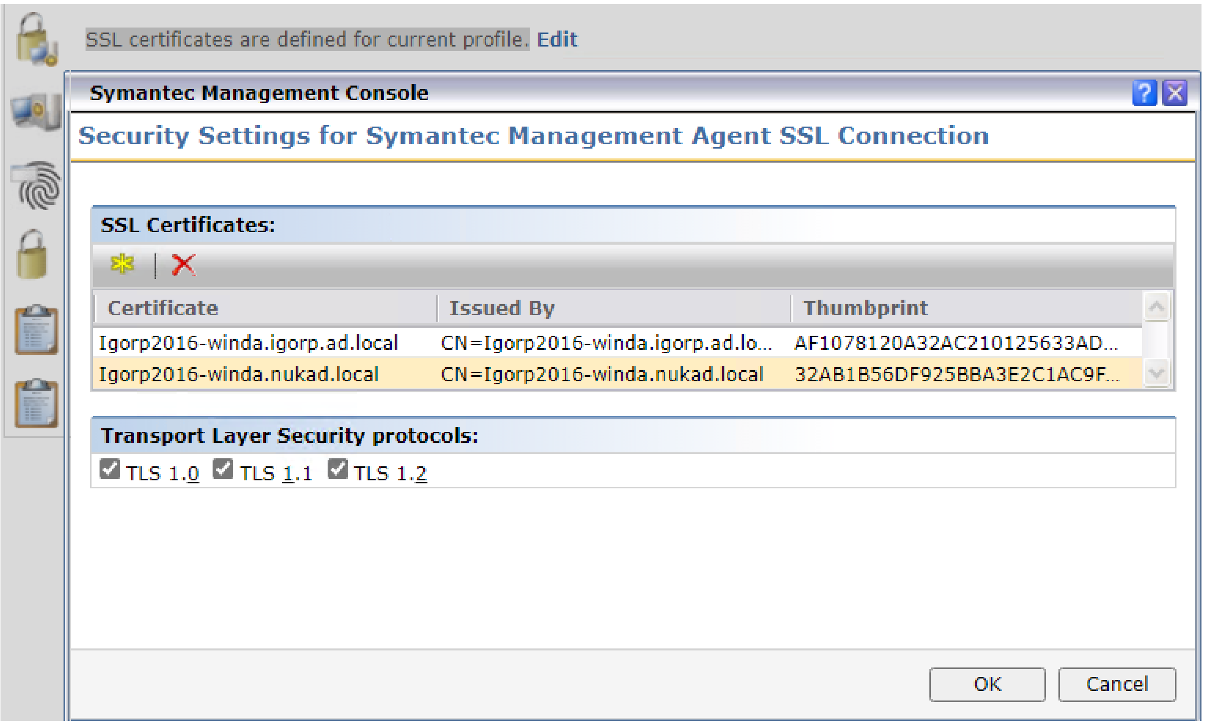
SSL certificates are defined for current profile. Edit

c) Next to **SSL certiciates are defined for current profile**, click **Edit**.

d) Click ✳ > **Import** and select the .pfx file that contains the certificate with your new domain name or hostname.

e) Click **Import New Certificate**. Verify that the new certificate appears in the **SSL Certificates** list, click **OK**, then **Save**.

f) Save the provided thumbprint for this new certificate to your local system, as it will be required in step 3.



SSL certificates are defined for current profile. Edit

Symantec Management Console

Security Settings for Symantec Management Agent SSL Connection

SSL Certificates:

Certificate	Issued By	Thumbprint
Igorp2016-winda.igorp.ad.local	CN=Igorp2016-winda.igorp.ad.lo...	AF1078120A32AC210125633AD...
Igorp2016-winda.nukad.local	CN=Igorp2016-winda.nukad.local	32AB1B56DF925BBA3E2C1AC9F...

Transport Layer Security protocols:

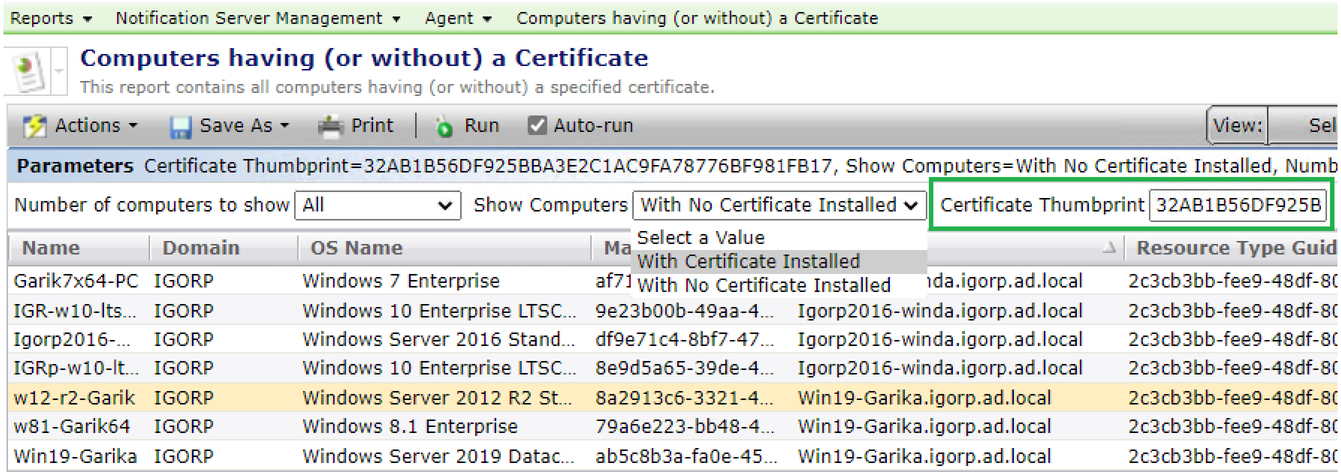
☑ TLS 1.0 ☑ TLS 1.1 ☑ TLS 1.2

2. Update the client configuration on all managed client computers.
   a) Schedule an **Update Client Configuration** task to all managed client computers and wait for the task to complete.
   b) Schedule a **Send basic inventory** task to all managed client computers.

3. Verify that client computers have the new certificate installed.
   a) In the SMP console, go to **Reports** > **All Reports**.
   b) Select **Notification Server Management** > **Agent** and open the **Computers having (or without) a Certificate**' report.
   c) Provide the thumbprint you saved in step 1-f in the **Certificate thumbprint** field and choose **Computers having (or without) a Certificate**.

⚠ **CAUTION**

Ensure that all required managed clients have received new certificate before you proceed. Those clients without the new certificate will lose connection with the NS once the NS will has a new domain name or host name.


Reports ▾
Notification Server Management ▾
Agent ▾
Computers having (or without) a Certificate
Actions ▾
Save As ▾
Print
Run
☑ Auto-run
View:
Sel

Computers having (or without) a Certificate

This report contains all computers having (or without) a specified certificate.

Parameters Certificate Thumbprint=32AB1B56DF925BBA3E2C1AC9FA78776BF981FB17, Show Computers=With No Certificate Installed, Numb

Number of computers to show: All

Show Computers: With No Certificate Installed

- Select a Value
- With Certificate Installed
- With No Certificate Installed

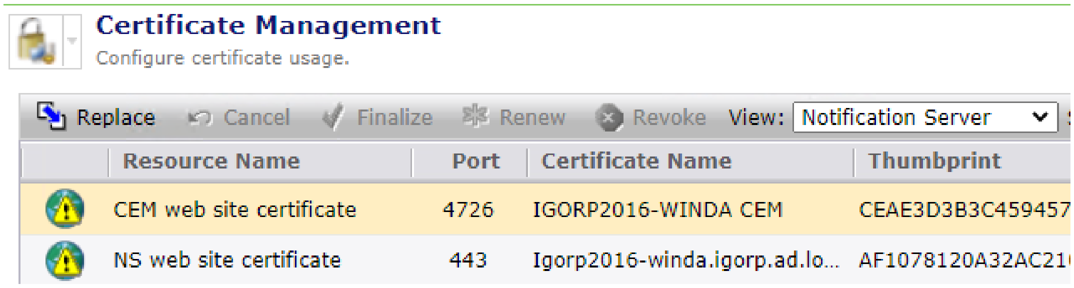
Certificate Thumbprint: 32AB1B56DF925B

Name	Domain	OS Name	Ma		Resource Type Guid
Garik7x64-PC	IGORP	Windows 7 Enterprise	af71	nda.igorp.ad.local	2c3cb3bb-fee9-48df-80
IGR-w10-lts...	IGORP	Windows 10 Enterprise LTSC...	9e23b00b-49aa-4...	Igorp2016-winda.igorp.ad.local	2c3cb3bb-fee9-48df-80
Igorp2016-...	IGORP	Windows Server 2016 Stand...	df9e71c4-8bf7-47...	Igorp2016-winda.igorp.ad.local	2c3cb3bb-fee9-48df-80
IGRp-w10-lt...	IGORP	Windows 10 Enterprise LTSC...	8e9d5a65-39de-4...	Igorp2016-winda.igorp.ad.local	2c3cb3bb-fee9-48df-80
w12-r2-Garik	IGORP	Windows Server 2012 R2 St...	8a2913c6-3321-4...	Win19-Garika.igorp.ad.local	2c3cb3bb-fee9-48df-80
w81-Garik64	IGORP	Windows 8.1 Enterprise	79a6e223-bb48-4...	Win19-Garika.igorp.ad.local	2c3cb3bb-fee9-48df-80
Win19-Garika	IGORP	Windows Server 2019 Datac...	ab5c8b3a-fa0e-45...	Win19-Garika.igorp.ad.local	2c3cb3bb-fee9-48df-80

Set a Placeholder CEM Certificate

In order to maintain a trust relationship between the components involved, you'll need to temporarily install a certificate that uses the new NS domain name or new hostname for the CEM Agent web site. Then you can apply the new NS certificate to the CEM Gateway server.

1. Browse to the SMP console > **Settings** > **All Settings** > **Notification Server** > **Certificate Management**.
   a) Select the **CEM web site certificate** resource name and click **Replace**.

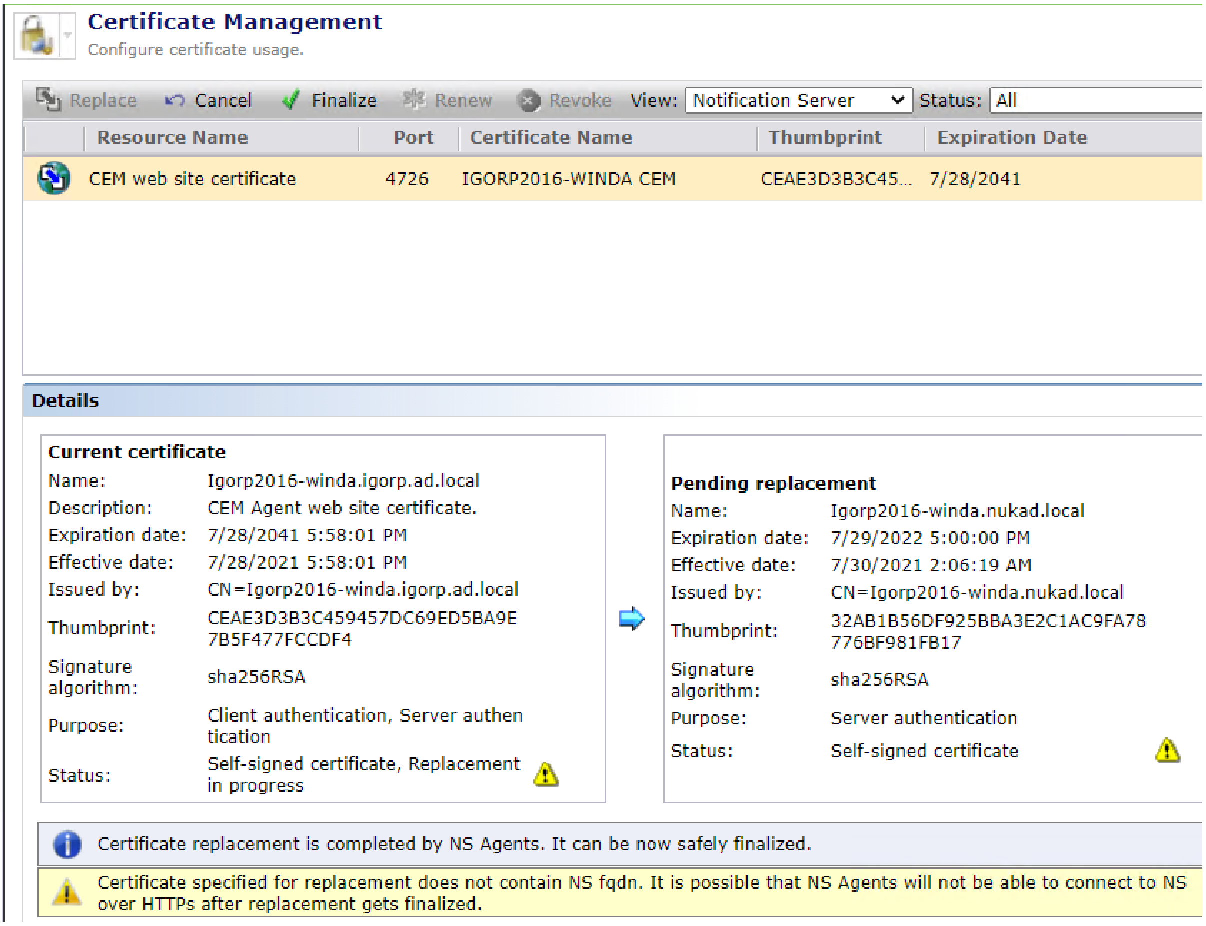


Certificate Management

Configure certificate usage.

	Resource Name	Port	Certificate Name	Thumbprint
⚠	CEM web site certificate	4726	IGORP2016-WINDA CEM	CEAE3D3B3C459457
⚠	NS web site certificate	443	Igorp2016-winda.igorp.ad.lo...	AF1078120A32AC21

   b) Select the updated certificate with your new domain name or new hostname and click **OK**.
   c) Verify that the certificate shows the correct details, and click **Finalize**.



Certificate Management

Configure certificate usage.

	Resource Name	Port	Certificate Name	Thumbprint	Expiration Date
	CEM web site certificate	4726	IGORP2016-WINDA CEM	CEAE3D3B3C45...	7/28/2041

Details

Current certificate

Name:	Igorp2016-winda.igorp.ad.local
Description:	CEM Agent web site certificate.
Expiration date:	7/28/2041 5:58:01 PM
Effective date:	7/28/2021 5:58:01 PM
Issued by:	CN=Igorp2016-winda.igorp.ad.local
Thumbprint:	CEAE3D3B3C459457DC69ED5BA9E7B5F477FCCDF4
Signature algorithm:	sha256RSA
Purpose:	Client authentication, Server authentication
Status:	Self-signed certificate, Replacement in progress ⚠

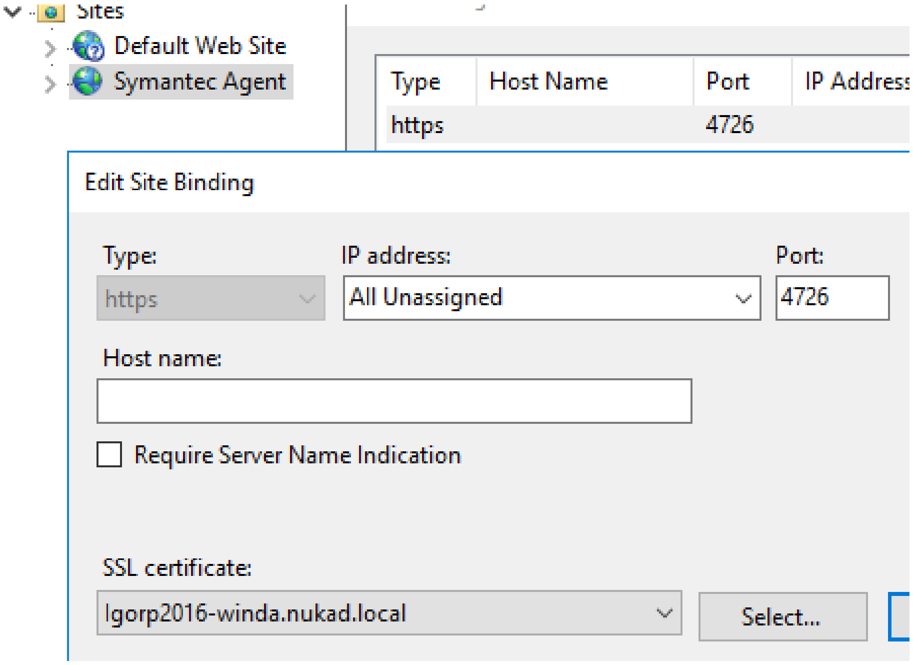
Pending replacement

Name:	Igorp2016-winda.nukad.local
Expiration date:	7/29/2022 5:00:00 PM
Effective date:	7/30/2021 2:06:19 AM
Issued by:	CN=Igorp2016-winda.nukad.local
Thumbprint:	32AB1B56DF925BBA3E2C1AC9FA78776BF981FB17
Signature algorithm:	sha256RSA
Purpose:	Server authentication
Status:	Self-signed certificate ⚠

Certificate replacement is completed by NS Agents. It can be now safely finalized.

⚠ Certificate specified for replacement does not contain NS fqdn. It is possible that NS Agents will not be able to connect to NS over HTTPs after replacement gets finalized.

d) Verify that the Symantec Agent website configuration includes port **4726** in your NS server configuration.



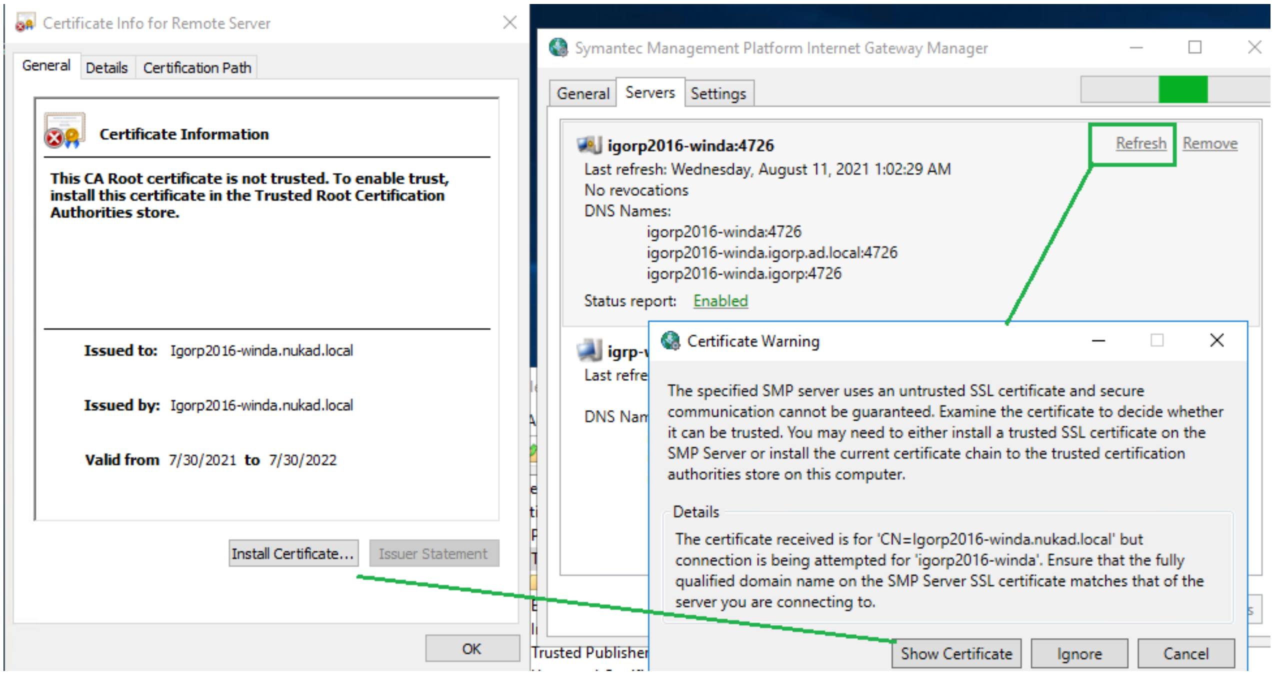
Sites
Default Web Site
Symantec Agent

Type	Host Name	Port	IP Address
https		4726	

Edit Site Binding

Type: https
IP address: All Unassigned
Port: 4726
Host name:
☐ Require Server Name Indication
SSL certificate: Igorp2016-winda.nukad.local

2. Re-establish the CEM connection using the new certificate
   a) Browse to the CEM Gateway server and open the **Symantec Management Platform Internet Gateway** Manager.
   b) Click Refresh to re-establish the connection with the NS.
   You are presented with the new certificate dialog.



Certificate Info for Remote Server

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Igorp2016-winda.nukad.local

Issued by: Igorp2016-winda.nukad.local

Valid from 7/30/2021 **to** 7/30/2022

Symantec Management Platform Internet Gateway Manager

igorp2016-winda:4726
Last refresh: Wednesday, August 11, 2021 1:02:29 AM
No revocations
DNS Names:
igorp2016-winda:4726
igorp2016-winda.igorp.ad.local:4726
igorp2016-winda.igorp:4726
Status report: Enabled

igrp-
Last refre
DNS Nan
Trusted Publisher

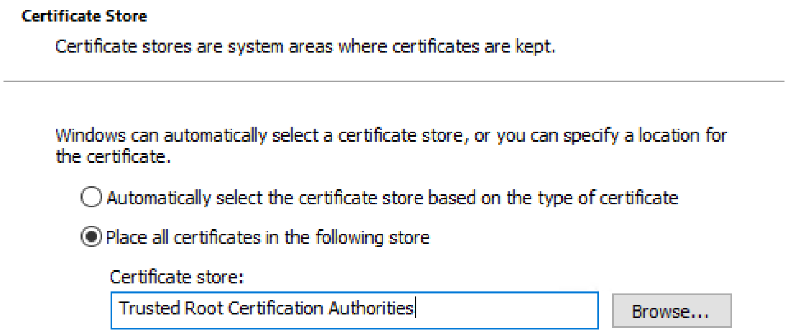
Certificate Warning

The specified SMP server uses an untrusted SSL certificate and secure communication cannot be guaranteed. Examine the certificate to decide whether it can be trusted. You may need to either install a trusted SSL certificate on the SMP Server or install the current certificate chain to the trusted certification authorities store on this computer.

Details

The certificate received is for 'CN=Igorp2016-winda.nukad.local' but connection is being attempted for 'igorp2016-winda'. Ensure that the fully qualified domain name on the SMP Server SSL certificate matches that of the server you are connecting to.

c) Install this new certificate in the **Trusted Root Certification Authorities** certificate store on the CEM Gateway server.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

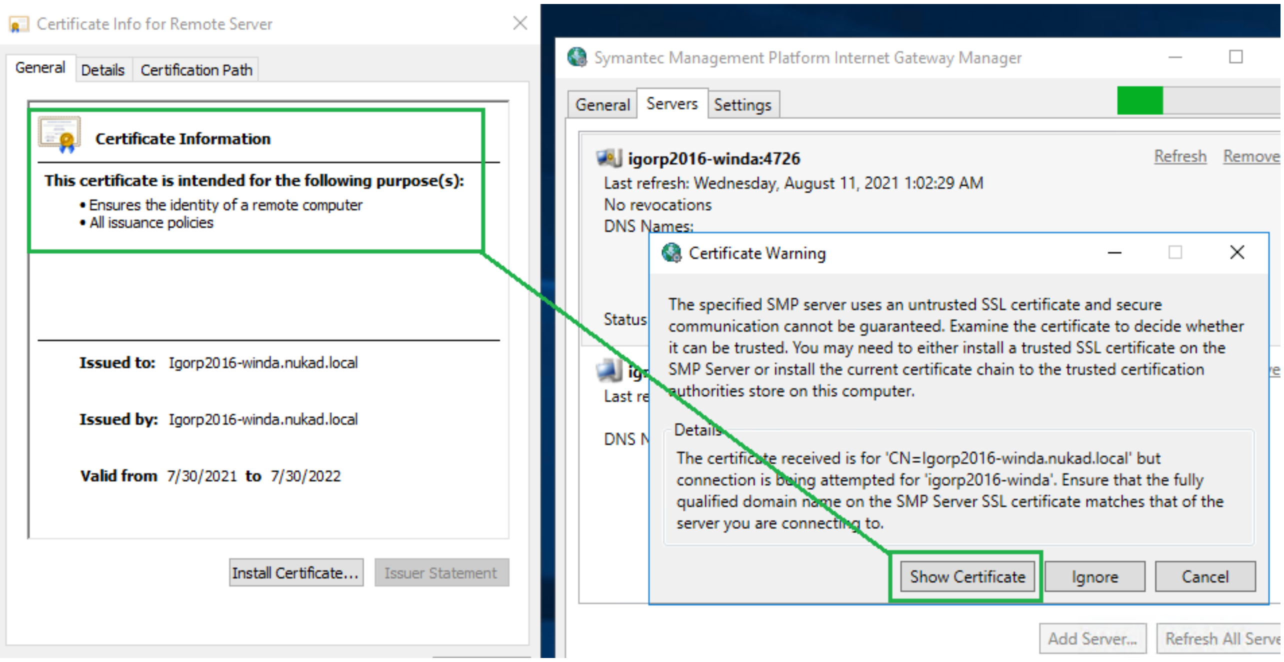
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

d) Once the certificate is installed, click **Show Certificate** in the Certificate Warning dialog to make sure that is now trusted on the CEM Gateway server.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- All issuance policies

Issued to: Igorp2016-winda.nukad.local

Issued by: Igorp2016-winda.nukad.local

Valid from 7/30/2021 **to** 7/30/2022

igorp2016-winda:4726

Last refresh: Wednesday, August 11, 2021 1:02:29 AM

No revocations

DNS Names:

Status

Certificate Warning

The specified SMP server uses an untrusted SSL certificate and secure communication cannot be guaranteed. Examine the certificate to decide whether it can be trusted. You may need to either install a trusted SSL certificate on the SMP Server or install the current certificate chain to the trusted certification authorities store on this computer.

Details

The certificate received is for 'CN=Igorp2016-winda.nukad.local' but connection is being attempted for 'igorp2016-winda'. Ensure that the fully qualified domain name on the SMP Server SSL certificate matches that of the server you are connecting to.

e) If the certificate appears as it should, click **Ignore**.

Install the Updated CEM Gateway Certificate

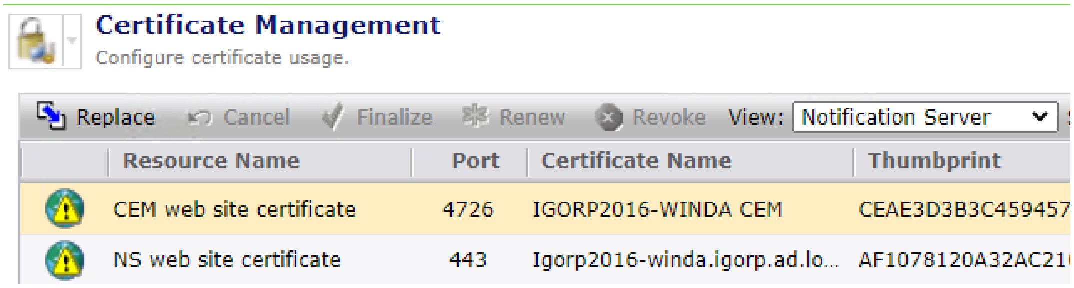
Now we need to configure the CEM clients to use the previous CEM certificate so that CEM-enabled clients will continue to be able to communicate with the NS.

Replace the certificate that is currently securing the connection between the CEM and the NS.

a) Browse to the **SMP Console** > **Settings** > **All Settings**.

b) Expand the Notification Server folder and select **Certificate Management**.

c) Click on the CEM web site certificate resource name and click Replace.
Ensure both the previous and the new certificate are listed.



Certificate Management

Configure certificate usage.

	Resource Name	Port	Certificate Name	Thumbprint
⚠	CEM web site certificate	4726	IGORP2016-WINDA CEM	CEAE3D3B3C459457
⚠	NS web site certificate	443	Igorp2016-winda.igorp.ad.lo...	AF1078120A32AC21

Modify the NSAppIdentity Definition

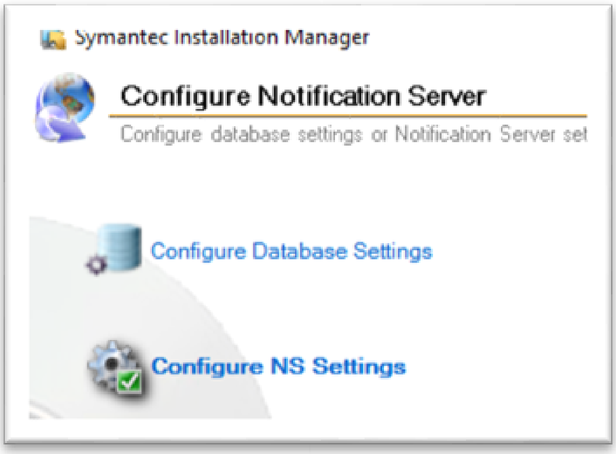
This whitepaper covers both scenarios - domain name and hostname changes for your ITMS notification server.

If you are going to change the NS domain name, you must change the NSAppIdentity account to use a local administrator account. This chapter can be ignored if you are modifying the hostname.

Change NSAppIdentity.

a) Open the **Symantec Installation Manager** on the NS server and **Configure Settings.**

b) Click Configure **NS Settings**.

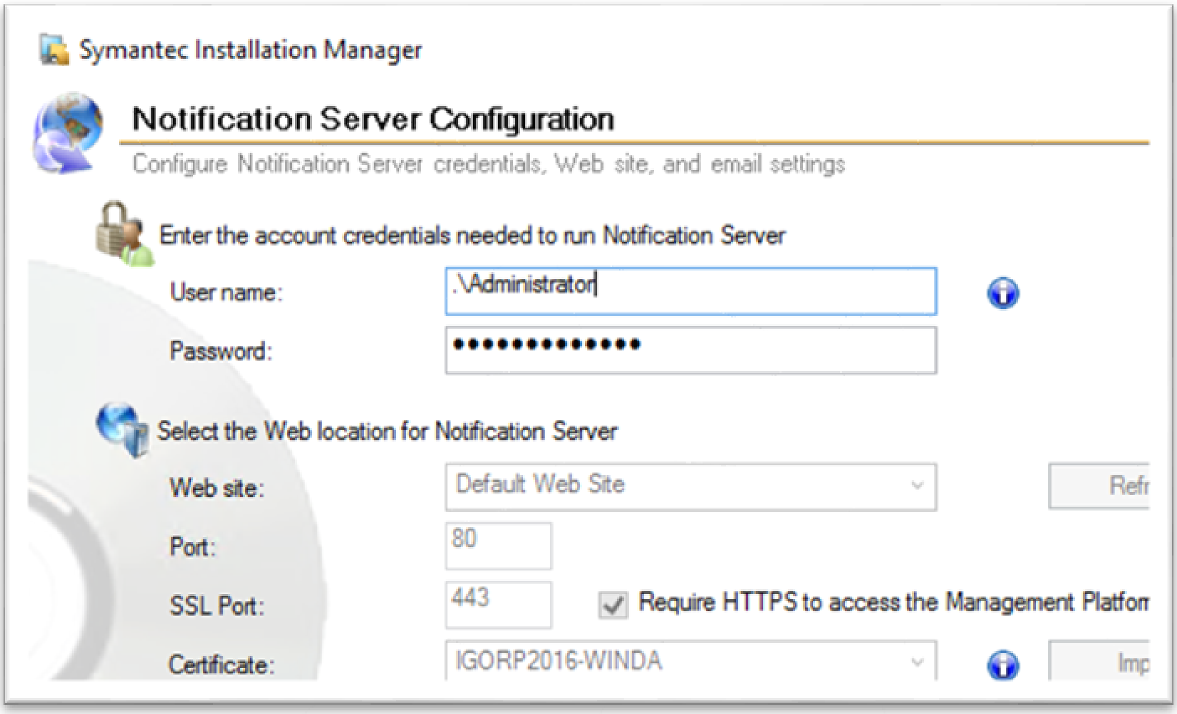


Symantec Installation Manager

Configure Notification Server

Configure database settings or Notification Server set

c) Specify an administrative account, click **Next**, and **Configure**.



Symantec Installation Manager

Notification Server Configuration

Configure Notification Server credentials, Web site, and email settings

Enter the account credentials needed to run Notification Server

User name: .\Administrator

Password: ••••••••••••••

Select the Web location for Notification Server

Web site: Default Web Site

Port: 80

SSL Port: 443

☑ Require HTTPS to access the Management Platfor

Certificate: IGORP2016-WINDA

Modify the NS Registry for the New Name

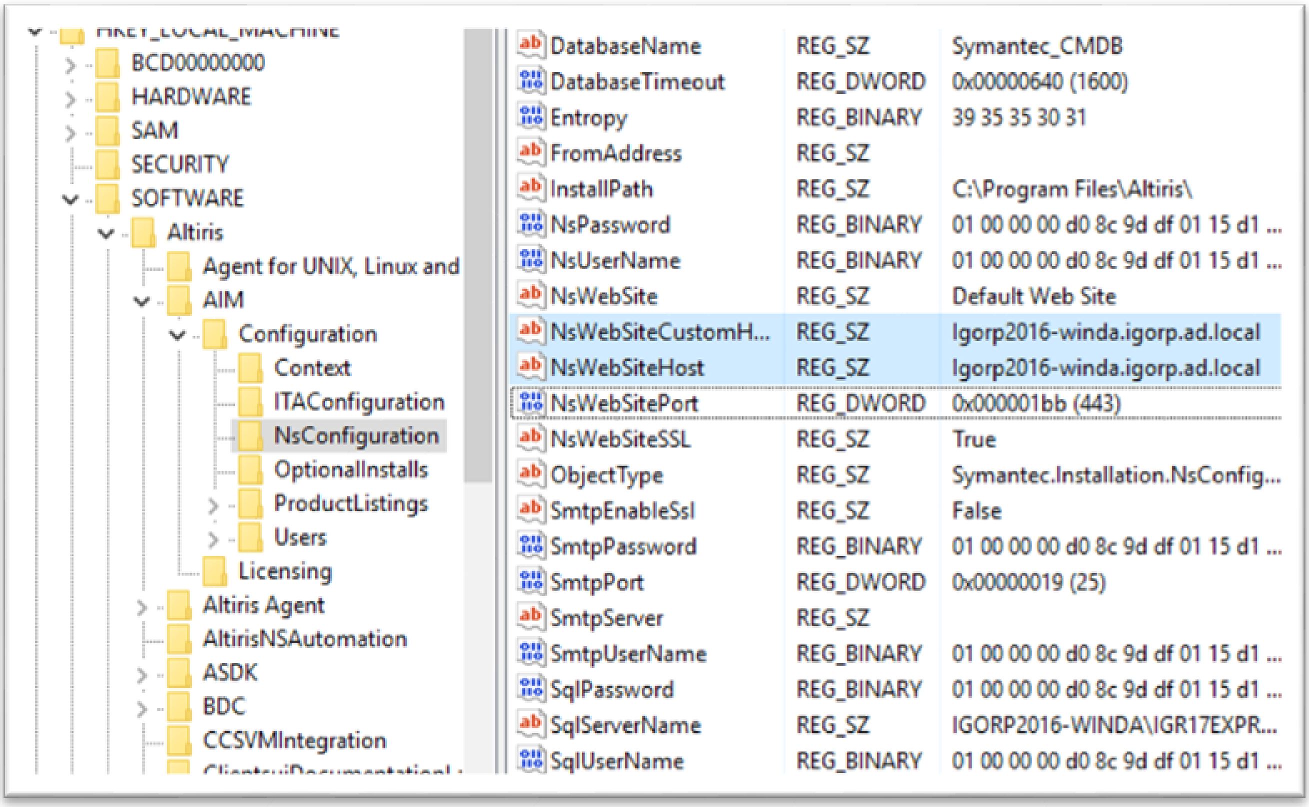
Because there is no configurable UI element to control this, you'll need to modify the Windows Server registry to set the new doamin or hostname.

1. Open the Windows Registry Editor on the Notification Server and browse to the following path: **[HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\AIM\Configuration\NsConfiguration]**
2. Make the following changes:

   • – • **NsWebSiteHost**: Specify the new NS domain or hostname

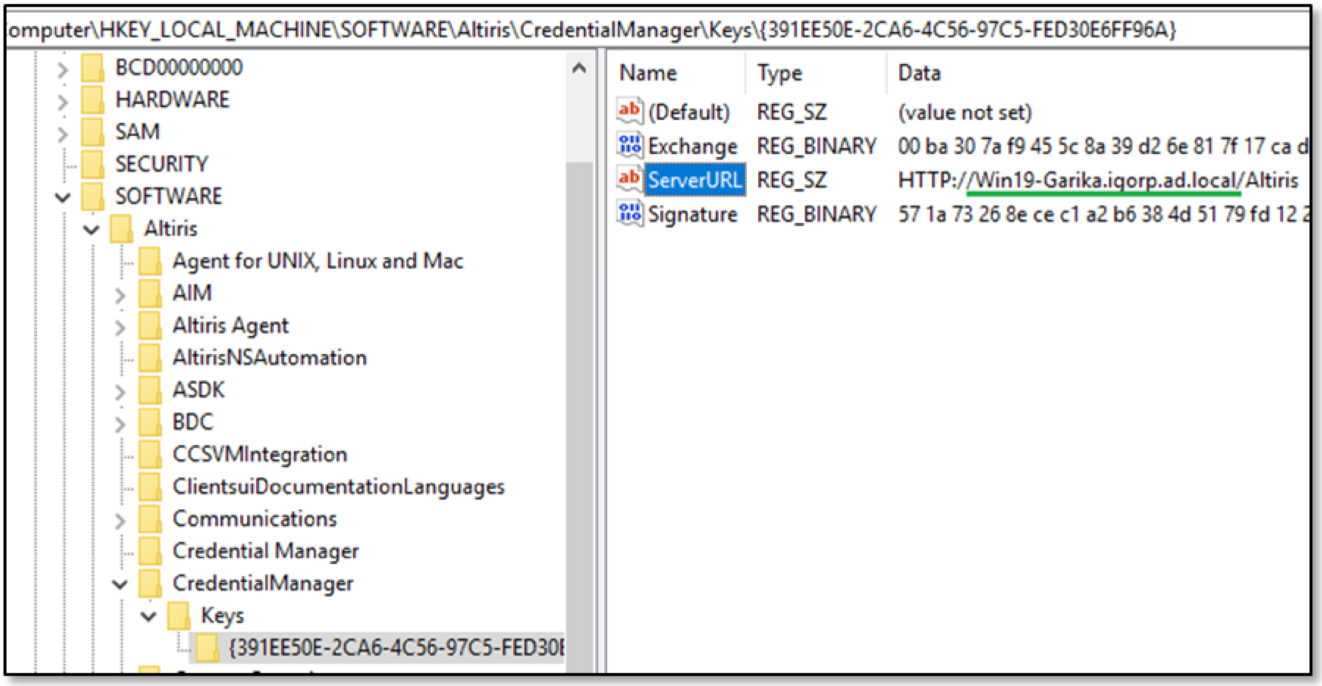
   • **NsWebSiteCustomHost**: Specify the new NS domain name or hostname

   • **SqlServerName**: Specify the SQL Server FQDN and ensure it is reachable from the new NS domain or the new NS hostname.



DatabaseName	REG_SZ	Symantec_CMDB
DatabaseTimeout	REG_DWORD	0x00000640 (1600)
Entropy	REG_BINARY	39 35 35 30 31
FromAddress	REG_SZ	
InstallPath	REG_SZ	C:\Program Files\Altiris\
NsPassword	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 ...
NsUserName	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 ...
NsWebSite	REG_SZ	Default Web Site
NsWebSiteCustomH...	REG_SZ	Igorp2016-winda.igorp.ad.local
NsWebSiteHost	REG_SZ	Igorp2016-winda.igorp.ad.local
NsWebSitePort	REG_DWORD	0x000001bb (443)
NsWebSiteSSL	REG_SZ	True
ObjectType	REG_SZ	Symantec.Installation.NsConfig...
SmtpEnableSsl	REG_SZ	False
SmtpPassword	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 ...
SmtpPort	REG_DWORD	0x00000019 (25)
SmtpServer	REG_SZ	
SmtpUserName	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 ...
SqlPassword	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 ...
SqlServerName	REG_SZ	IGORP2016-WINDA\IGR17EXPR...
SqlUserName	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 ...

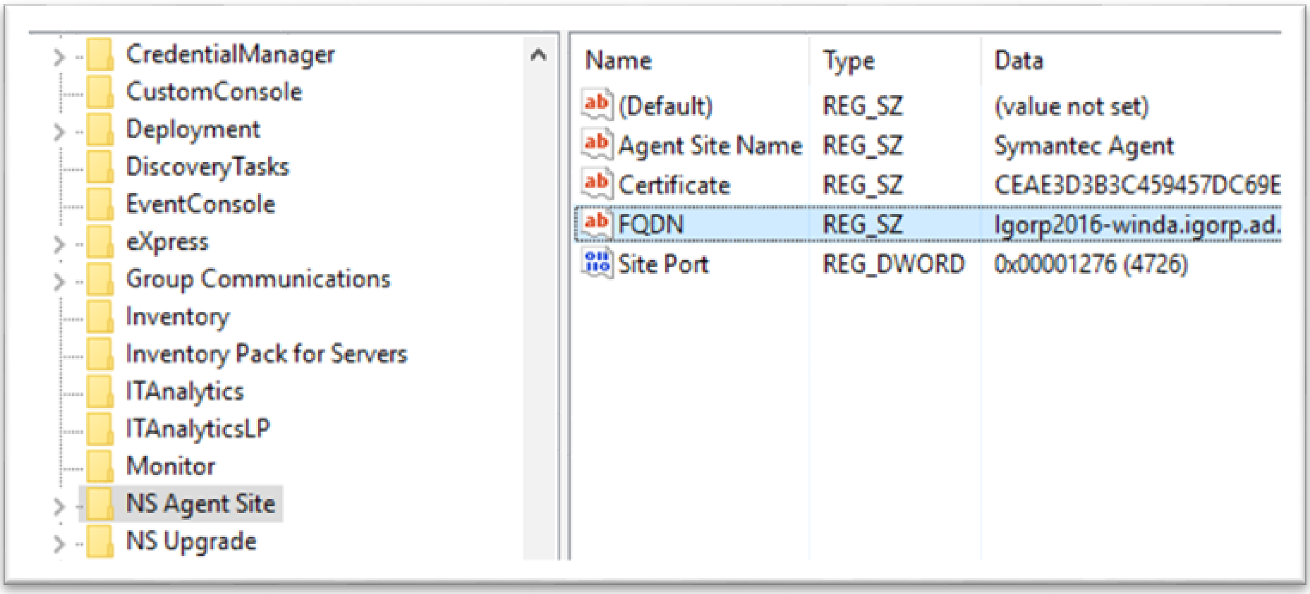
3. Change the old NS host name or domain name to the new one by modifying this StringValue key:
   1. **HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\CredentialManager\Keys\.**



omputer\HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\CredentialManager\Keys\{391EE50E-2CA6-4C56-97C5-FED30E6FF96A}

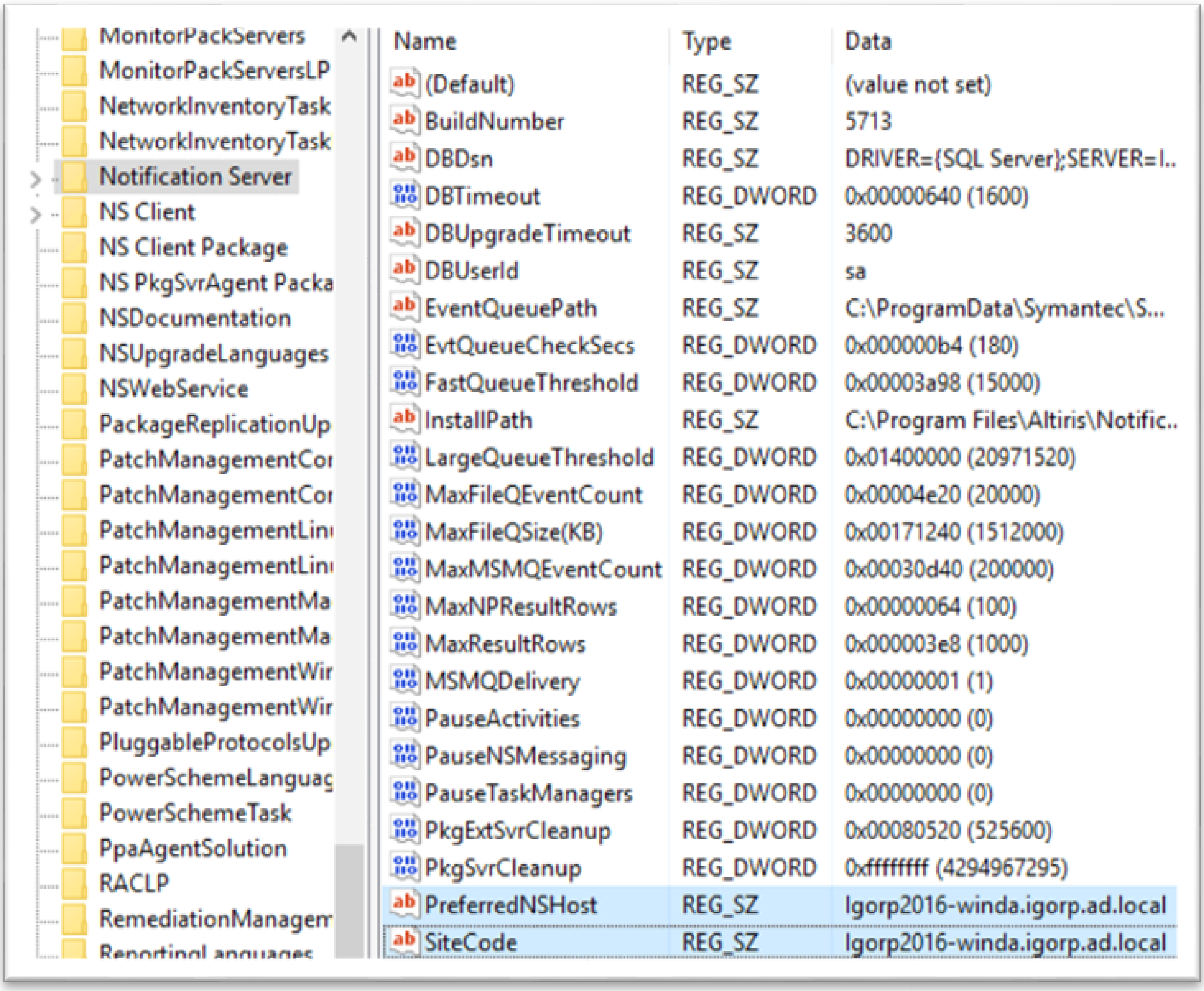
Name	Type	Data
(Default)	REG_SZ	(value not set)
Exchange	REG_BINARY	00 ba 30 7a f9 45 5c 8a 39 d2 6e 81 7f 17 ca d
ServerURL	REG_SZ	HTTP://Win19-Garika.igorp.ad.local/Altiris
Signature	REG_BINARY	57 1a 73 26 8e ce c1 a2 b6 38 4d 51 79 fd 12 2

4. Browse to the following path in the registry editor:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\NS Agent Site]
5. Modify the FQDN entry, and specify your new NS domain name or NS hostname.



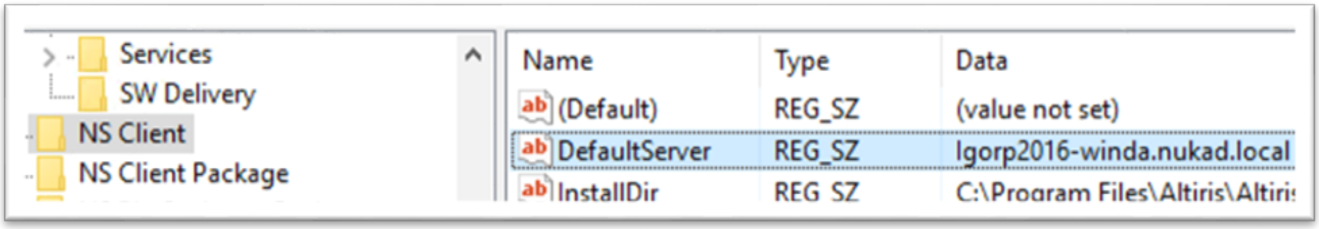
Name	Type	Data
(Default)	REG_SZ	(value not set)
Agent Site Name	REG_SZ	Symantec Agent
Certificate	REG_SZ	CEAE3D3B3C459457DC69E
FQDN	REG_SZ	Igorp2016-winda.igorp.ad.
Site Port	REG_DWORD	0x00001276 (4726)

6. Browse to the following path in the registry editor:
   1. Set the following values:
      – **PreferredNSHost:** Specify the new NS domain name or hostname.
      – **SiteCode**: Specify the new NS domain name or hostname.
      – **DBDsn**: Set the SQL Server FQDN here. Ensure that it can be reached by the NS from the new domain.
      – **PreferredNSHost**: Specify the new NS domain name or hostname.



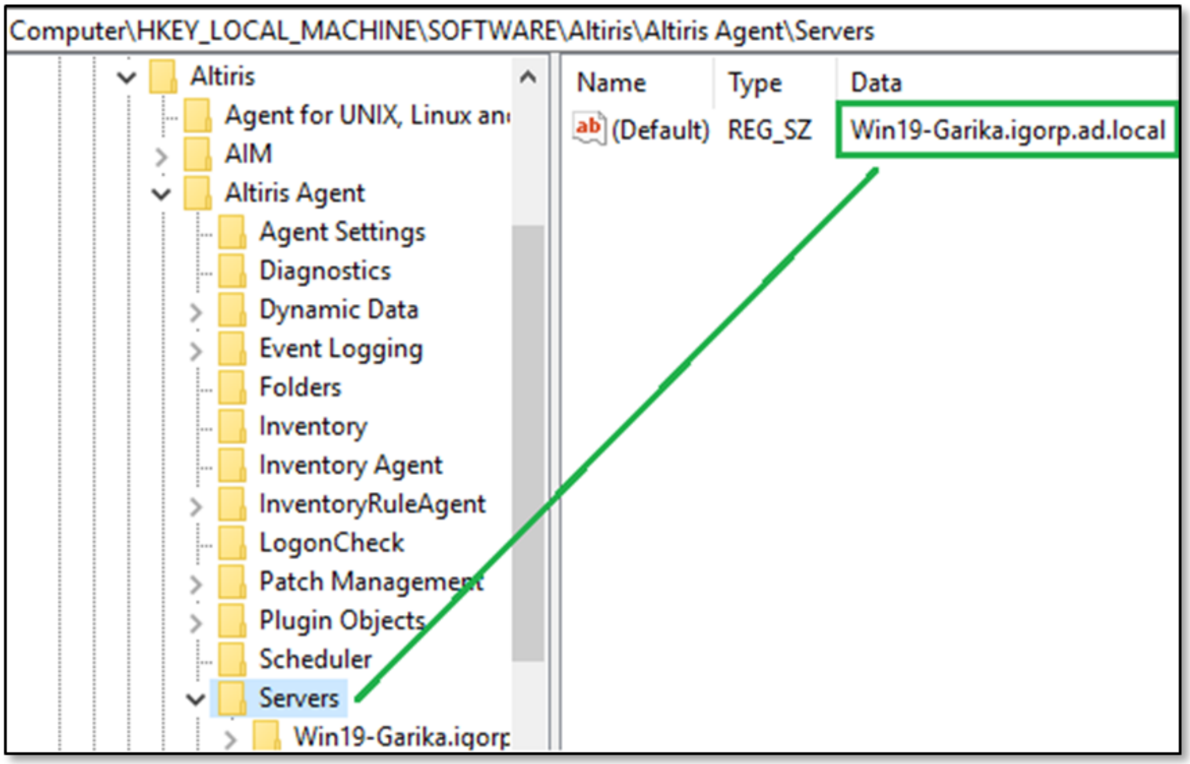
Name	Type	Data
(Default)	REG_SZ	(value not set)
BuildNumber	REG_SZ	5713
DBDsn	REG_SZ	DRIVER={SQL Server};SERVER=l..
DBTimeout	REG_DWORD	0x00000640 (1600)
DBUpgradeTimeout	REG_SZ	3600
DBUserId	REG_SZ	sa
EventQueuePath	REG_SZ	C:\ProgramData\Symantec\S...
EvtQueueCheckSecs	REG_DWORD	0x000000b4 (180)
FastQueueThreshold	REG_DWORD	0x00003a98 (15000)
InstallPath	REG_SZ	C:\Program Files\Altiris\Notific..
LargeQueueThreshold	REG_DWORD	0x01400000 (20971520)
MaxFileQEventCount	REG_DWORD	0x00004e20 (20000)
MaxFileQSize(KB)	REG_DWORD	0x00171240 (1512000)
MaxMSMQEventCount	REG_DWORD	0x00030d40 (200000)
MaxNPResultRows	REG_DWORD	0x00000064 (100)
MaxResultRows	REG_DWORD	0x000003e8 (1000)
MSMQDelivery	REG_DWORD	0x00000001 (1)
PauseActivities	REG_DWORD	0x00000000 (0)
PauseNSMessaging	REG_DWORD	0x00000000 (0)
PauseTaskManagers	REG_DWORD	0x00000000 (0)
PkgExtSvrCleanup	REG_DWORD	0x00080520 (525600)
PkgSvrCleanup	REG_DWORD	0xffffffff (4294967295)
PreferredNSHost	REG_SZ	Igorp2016-winda.igorp.ad.local
SiteCode	REG_SZ	Igorp2016-winda.igorp.ad.local

7. Browse to the following path in the registry editor:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\NS Client]
8. Modify the **DefaultServer** value and specify New NS domain name or hostname.



Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultServer	REG_SZ	Igorp2016-winda.nukad.local
InstallDir	REG_SZ	C:\Program Files\Altiris\Altiri

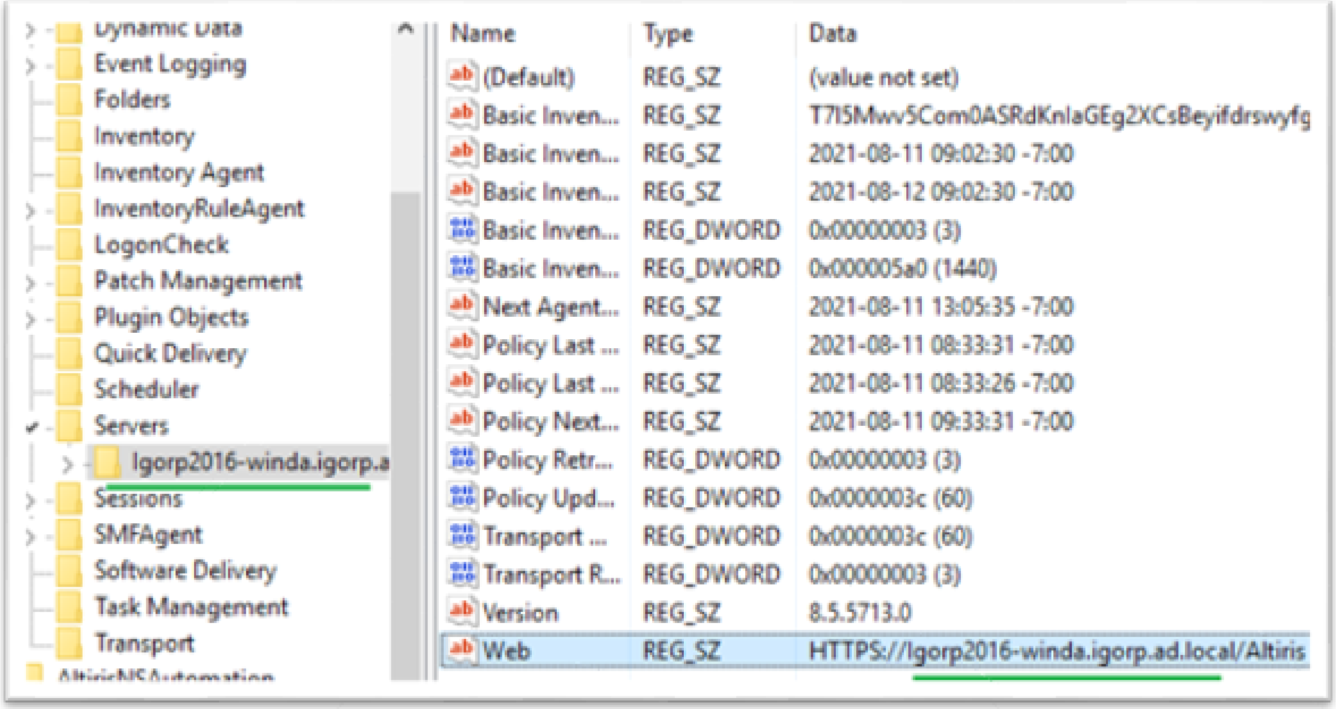
9. Browse to the following path in the registry editor:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\Servers]
   Modify the entry from the old NS hostname or domain name and replace it with the new one



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\Servers

Name	Type	Data
(Default)	REG_SZ	Win19-Garika.igorp.ad.local

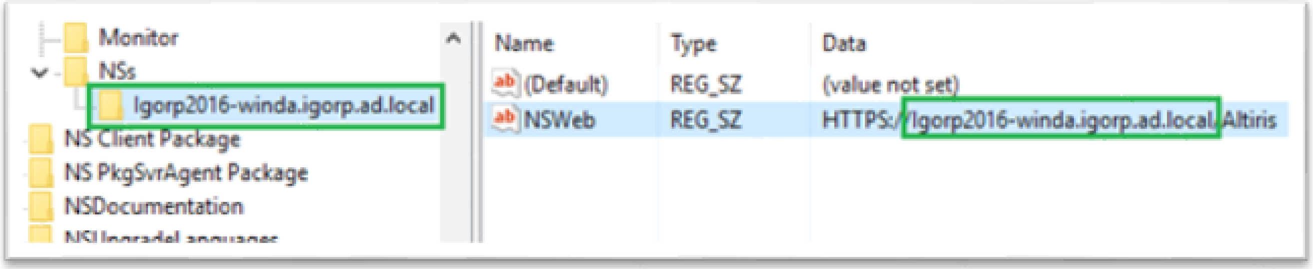
10. Browse to the following path in the registry editor:
[HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\Servers\Igorp2016-winda.igorp.ad.local]
Modify the **Web** entry, and set it as HTTPS://**<new NS hostname or domain name>**/Altiris



Name	Type	Data
(Default)	REG_SZ	(value not set)
Basic Inven...	REG_SZ	T7I5Mwv5Com0ASRdKnlaGEg2XCsBeyifdrswyfg
Basic Inven...	REG_SZ	2021-08-11 09:02:30 -7:00
Basic Inven...	REG_SZ	2021-08-12 09:02:30 -7:00
Basic Inven...	REG_DWORD	0x00000003 (3)
Basic Inven...	REG_DWORD	0x000005a0 (1440)
Next Agent...	REG_SZ	2021-08-11 13:05:35 -7:00
Policy Last ...	REG_SZ	2021-08-11 08:33:31 -7:00
Policy Last ...	REG_SZ	2021-08-11 08:33:26 -7:00
Policy Next...	REG_SZ	2021-08-11 09:33:31 -7:00
Policy Retr...	REG_DWORD	0x00000003 (3)
Policy Upd...	REG_DWORD	0x0000003c (60)
Transport ...	REG_DWORD	0x0000003c (60)
Transport R...	REG_DWORD	0x00000003 (3)
Version	REG_SZ	8.5.5713.0
Web	REG_SZ	HTTPS://Igorp2016-winda.igorp.ad.local/Altiris

11. Browse to the following path in the registry editor:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\NS Client\NSs\<domain or hostname>

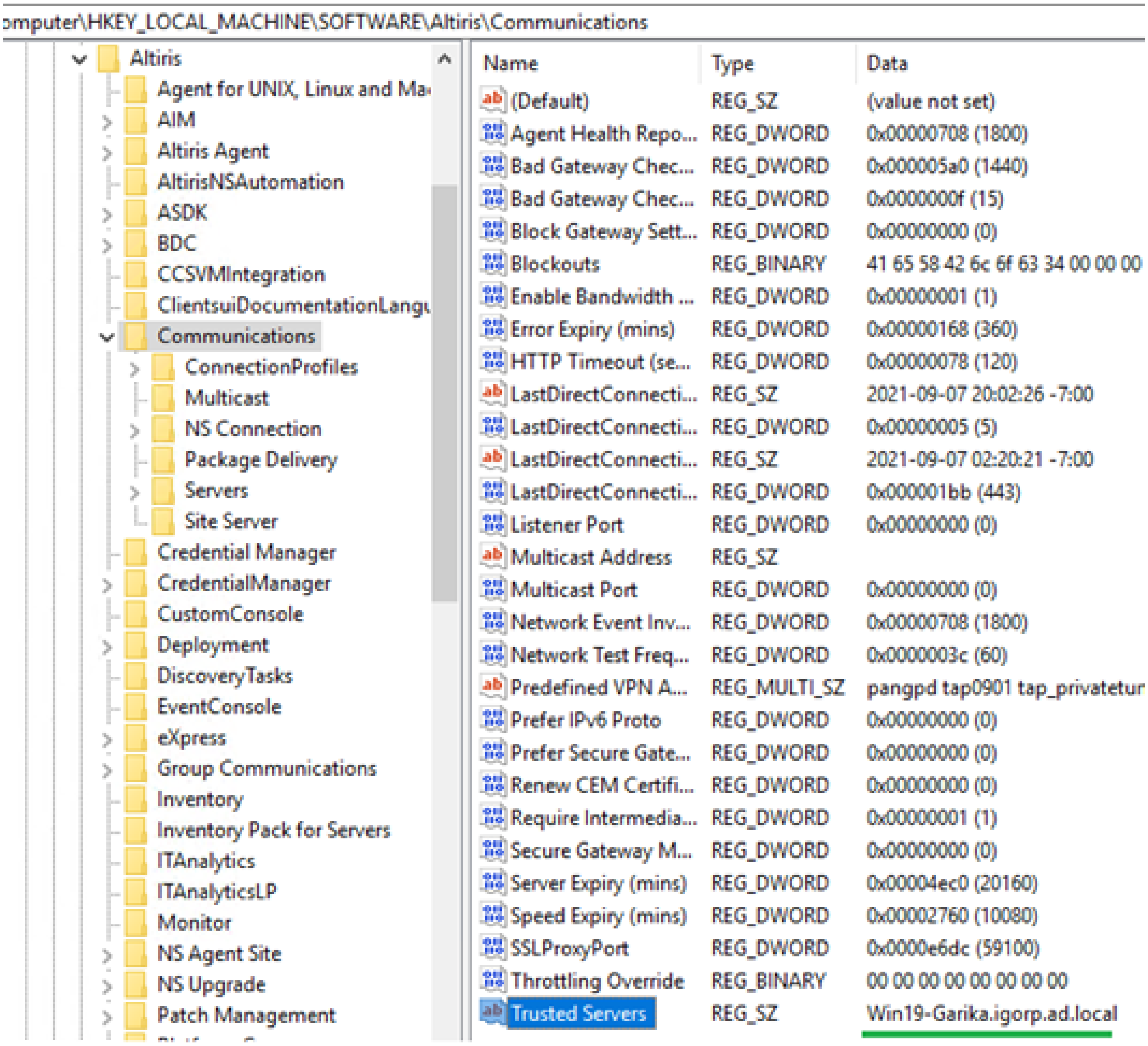
    Specify the new NS domain name or hostname in the **NSWeb** entry as **HTTPS://<new NS domain or hostname>/ Altiris**



- Monitor
- NSs
  - Igorp2016-winda.igorp.ad.local
- NS Client Package
- NS PkgSvrAgent Package
- NSDocumentation
- NSUpgradeLanguages

Name	Type	Data
(Default)	REG_SZ	(value not set)
NSWeb	REG_SZ	HTTPS://Igorp2016-winda.igorp.ad.local/Altiris

12. Change the old NS host name or domain name to the new one in the following **StringValue** key "Trusted Servers" under **[HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications]**

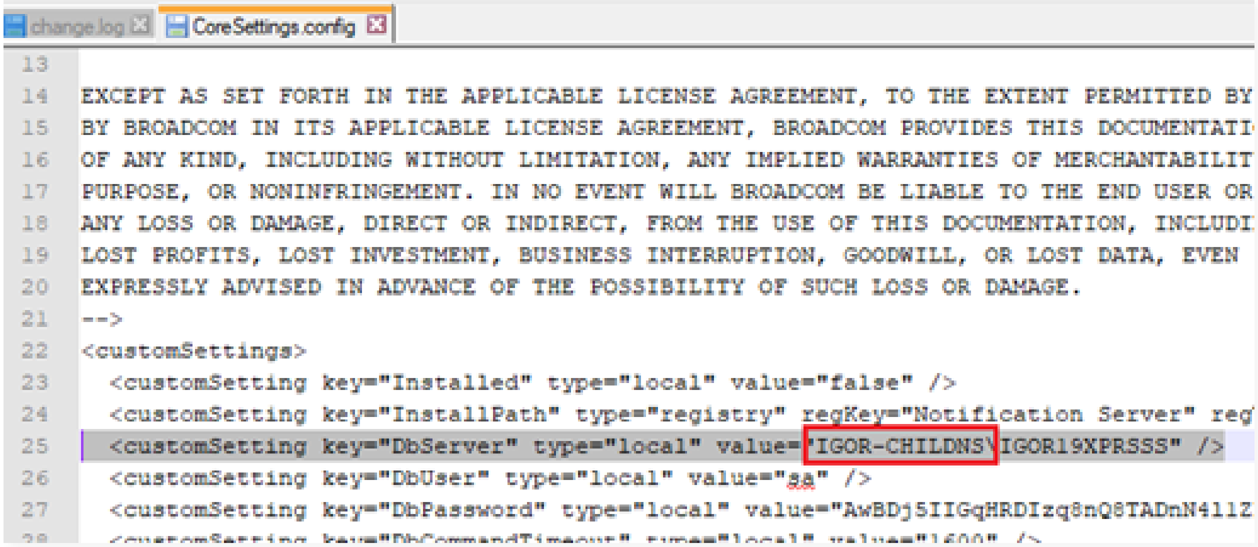


omputer\HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications

Name	Type	Data
(Default)	REG_SZ	(value not set)
Agent Health Repo...	REG_DWORD	0x00000708 (1800)
Bad Gateway Chec...	REG_DWORD	0x000005a0 (1440)
Bad Gateway Chec...	REG_DWORD	0x0000000f (15)
Block Gateway Sett...	REG_DWORD	0x00000000 (0)
Blockouts	REG_BINARY	41 65 58 42 6c 6f 63 34 00 00 00
Enable Bandwidth ...	REG_DWORD	0x00000001 (1)
Error Expiry (mins)	REG_DWORD	0x00000168 (360)
HTTP Timeout (se...	REG_DWORD	0x00000078 (120)
LastDirectConnecti...	REG_SZ	2021-09-07 20:02:26 -7:00
LastDirectConnecti...	REG_DWORD	0x00000005 (5)
LastDirectConnecti...	REG_SZ	2021-09-07 02:20:21 -7:00
LastDirectConnecti...	REG_DWORD	0x000001bb (443)
Listener Port	REG_DWORD	0x00000000 (0)
Multicast Address	REG_SZ	
Multicast Port	REG_DWORD	0x00000000 (0)
Network Event Inv...	REG_DWORD	0x00000708 (1800)
Network Test Freq...	REG_DWORD	0x0000003c (60)
Predefined VPN A...	REG_MULTI_SZ	pangpd tap0901 tap_privatetur
Prefer IPv6 Proto	REG_DWORD	0x00000000 (0)
Prefer Secure Gate...	REG_DWORD	0x00000000 (0)
Renew CEM Certifi...	REG_DWORD	0x00000000 (0)
Require Intermedia...	REG_DWORD	0x00000001 (1)
Secure Gateway M...	REG_DWORD	0x00000000 (0)
Server Expiry (mins)	REG_DWORD	0x00004ec0 (20160)
Speed Expiry (mins)	REG_DWORD	0x00002760 (10080)
SSLProxyPort	REG_DWORD	0x0000e6dc (59100)
Throttling Override	REG_BINARY	00 00 00 00 00 00 00 00
Trusted Servers	REG_SZ	Win19-Garika.igorp.ad.local

13. After the NS hostname or domain name change, but before you reboot the server, you will need to specify the correct SQL server instance name where the Symantec_CMDB database is running.

    a) On the notification server, open **C:\ProgramData\Symantec\SMP\Settings\CoreSettings.config** and change the **DBServer** value as in the image below:



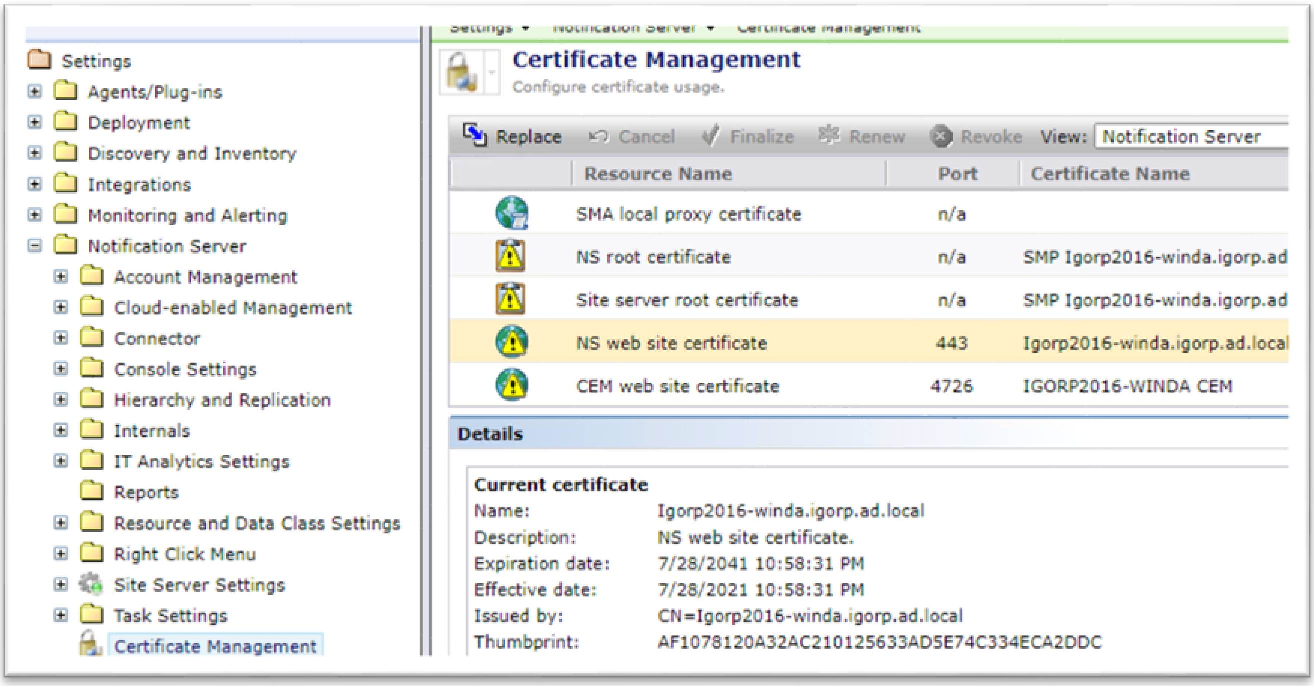
```

EXCEPT AS SET FORTH IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY
BY BROADCOM IN ITS APPLICABLE LICENSE AGREEMENT, BROADCOM PROVIDES THIS DOCUMENTATI
OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILIT
PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO THE END USER OR
ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDI
LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN
EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.
-->
<customSettings>
  <customSetting key="Installed" type="local" value="false" />
  <customSetting key="InstallPath" type="registry" regKey="Notification Server" reg
  <customSetting key="DbServer" type="local" value="IGOR-CHILDNS\IGOR19XPRSSS" />
  <customSetting key="DbUser" type="local" value="sa" />
  <customSetting key="DbPassword" type="local" value="AwBDj5IIGqHRDIzq8nQ8TADnN411Z
  <customSetting key="DbCommandTimeout" type="local" value="1600" />
```

    b) Verify your changes and save the updated file.

14. Open the **SMP Console** and go to **Settings** > **All Settings** > expand the **Notification Server** folder and go to **Certificate Management.**

15. Replace the old certificate with the new NS domain name or host name certificate for **NS web site certificate**.

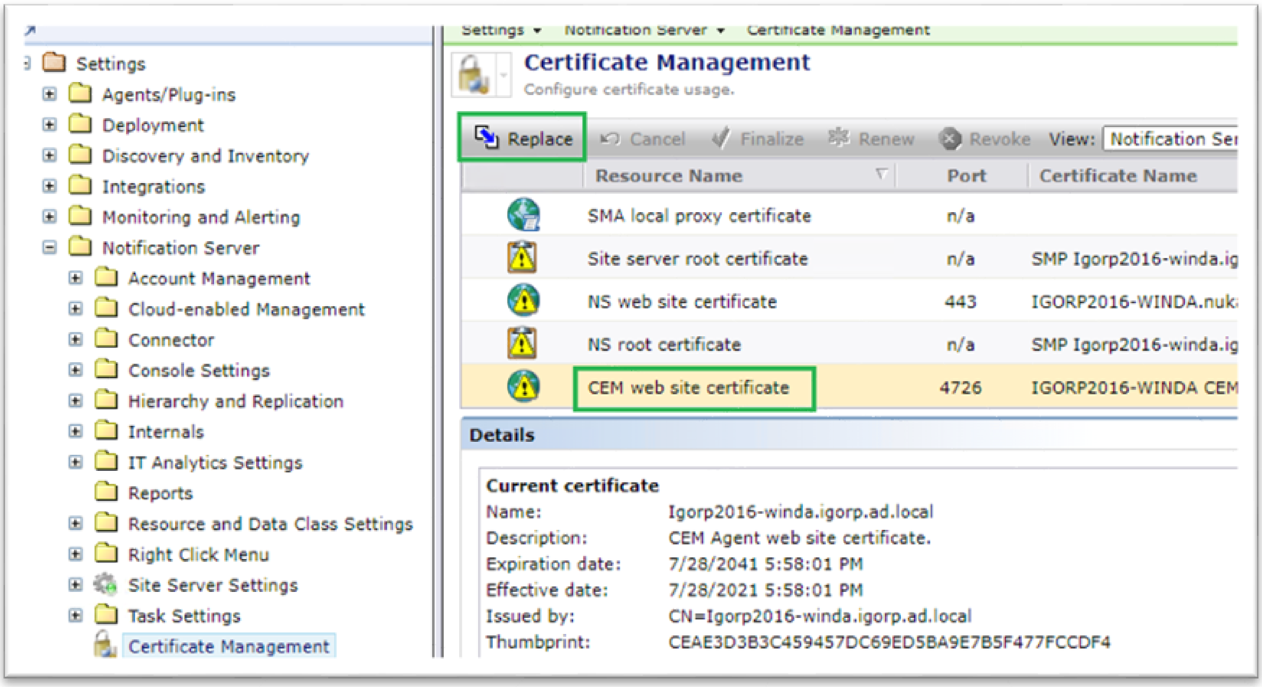


Resource Name	Port	Certificate Name
SMA local proxy certificate	n/a	
NS root certificate	n/a	SMP Igorp2016-winda.igorp.ad
Site server root certificate	n/a	SMP Igorp2016-winda.igorp.ad
NS web site certificate	443	Igorp2016-winda.igorp.ad.local
CEM web site certificate	4726	IGORP2016-WINDA CEM

Current certificate

Name:	Igorp2016-winda.igorp.ad.local
Description:	NS web site certificate.
Expiration date:	7/28/2041 10:58:31 PM
Effective date:	7/28/2021 10:58:31 PM
Issued by:	CN=Igorp2016-winda.igorp.ad.local
Thumbprint:	AF1078120A32AC210125633AD5E74C334ECA2DDC

16. Replace the old certificate with new NS domain name or host name certificate for the **CEM web site certificate**.



Certificate Management

Configure certificate usage.

Resource Name	Port	Certificate Name
SMA local proxy certificate	n/a	
Site server root certificate	n/a	SMP Igorp2016-winda.ig
NS web site certificate	443	IGORP2016-WINDA.nuk
NS root certificate	n/a	SMP Igorp2016-winda.ig
CEM web site certificate	4726	IGORP2016-WINDA CEM

Details

Current certificate

Name: Igorp2016-winda.igorp.ad.local
Description: CEM Agent web site certificate.
Expiration date: 7/28/2041 5:58:01 PM
Effective date: 7/28/2021 5:58:01 PM
Issued by: CN=Igorp2016-winda.igorp.ad.local
Thumbprint: CEAE3D3B3C459457DC69ED5BA9E7B5F477FCCDF4

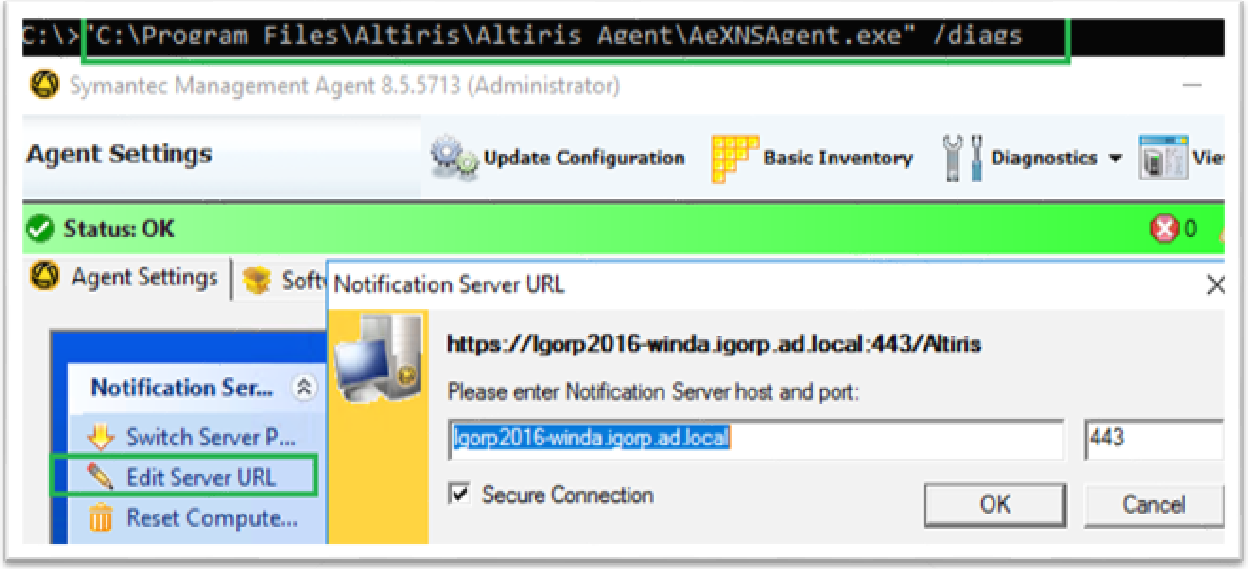
Once all of the above changes have been made, you can change the hostname or the domain name in your Windows Server and reboot. Refer to Windows help for steps to modify your system's domain or host name.

Troubleshooting

If, after the reboot, the Symantec Management Agent on the local Notification Server reports that it is still trying to communicate with the old NS domain name or hostname, you will need to enable diagnostics mode and manually specify the new NS domain name or hostname and refresh your policy.

To enable diagnostics mode:

1. Open the command prompt as Administrator and run the following command: AeXNSAgent.exe /diags



```
C:\>"C:\Program Files\Altiris\Altiris Agent\AeXNSAgent.exe" /diags
```

Notification Server URL

https://Igorp2016-winda.igorp.ad.local:443/Altiris

Please enter Notification Server host and port:

Igorp2016-winda.igorp.ad.local 443

☑ Secure Connection

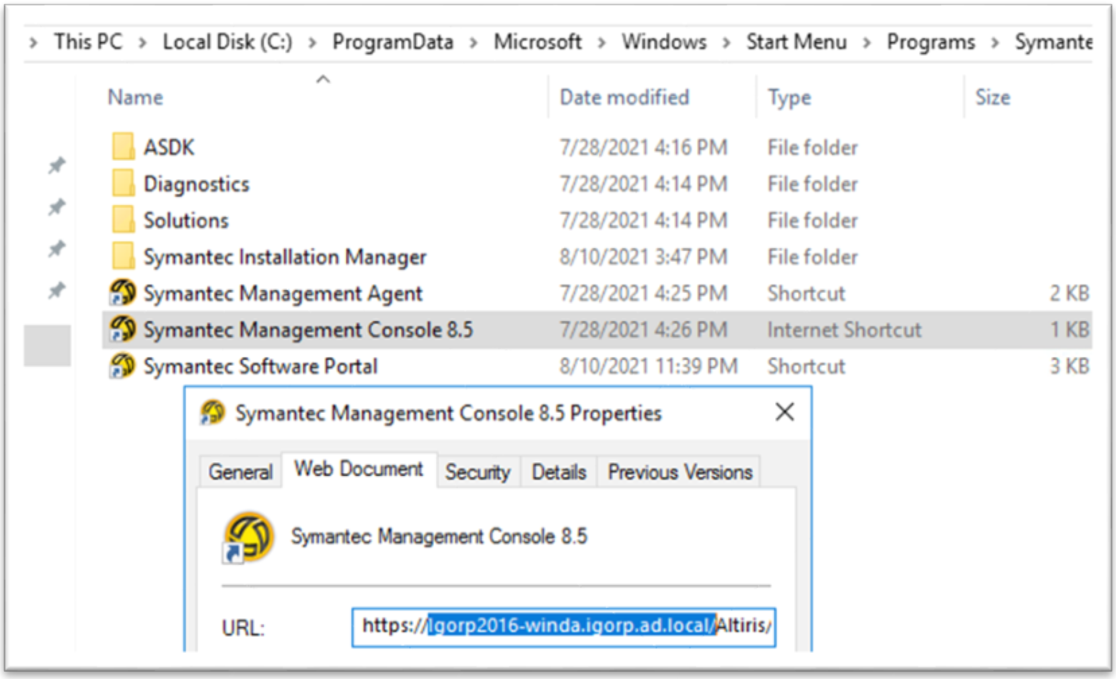
OK Cancel

2. Once the diagnostics mode is available, browse to the **Agent Settings** tab and select **Edit Server URL**. Modify the domain name or hostname as required.

Update the Symantec Management Portal Console

Now that the notification server has all of the necessary changes, it's time to update the Symantec Management Portal Console with the new domain (or hostname), and associated URLs, and certificates.

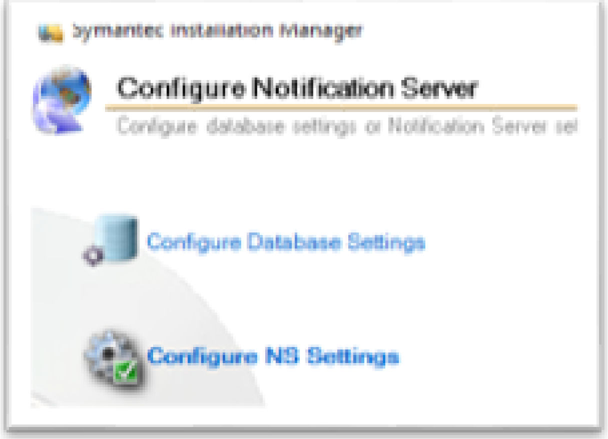
1. Modify the Windows shortcut URL for the Symantec Management Console to use the new NS hostname or domain name:


› This PC › Local Disk (C:) › ProgramData › Microsoft › Windows › Start Menu › Programs › Symante
Symantec Management Console 8.5 Properties
General
Web Document
Security
Details
Previous Versions
Symantec Management Console 8.5

Name	Date modified	Type	Size
ASDK	7/28/2021 4:16 PM	File folder	
Diagnostics	7/28/2021 4:14 PM	File folder	
Solutions	7/28/2021 4:14 PM	File folder	
Symantec Installation Manager	8/10/2021 3:47 PM	File folder	
Symantec Management Agent	7/28/2021 4:25 PM	Shortcut	2 KB
Symantec Management Console 8.5	7/28/2021 4:26 PM	Internet Shortcut	1 KB
Symantec Software Portal	8/10/2021 11:39 PM	Shortcut	3 KB

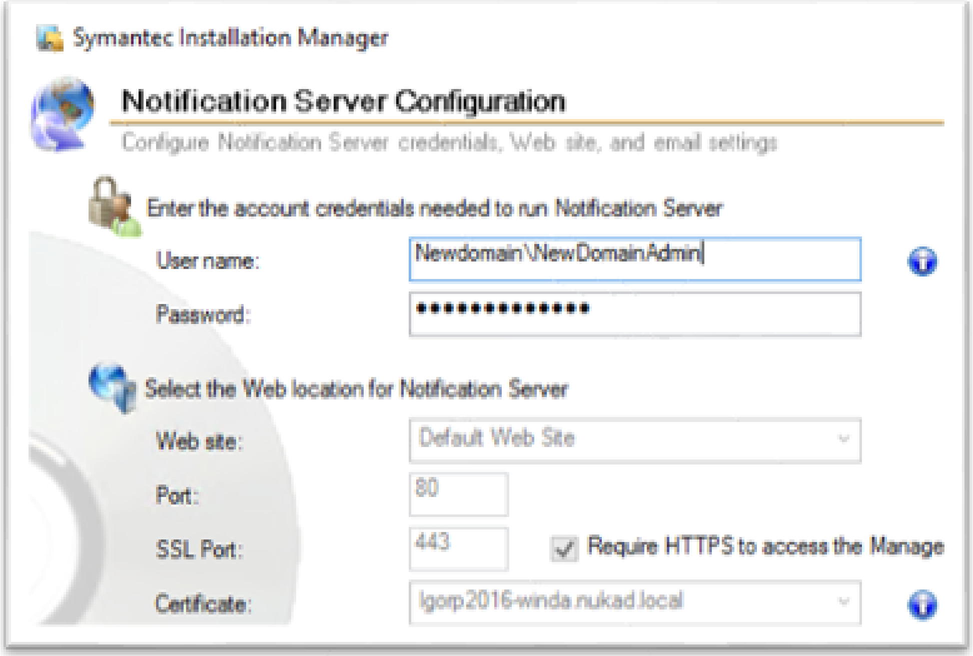
URL: https://igorp2016-winda.igorp.ad.local/Altiris/

2. Update **NSAppIdentity** to use the new account instead of the previously changed **NSAppIdentity** using the administrative account, then:
   a) Open the Symantec Installation Manager on the NS
   b) Click **Configure Settings**
   c) Click Configure NS Settings


Symantec Installation Manager
Configure Notification Server
Configure database settings or Notification Server set
Configure Database Settings
Configure NS Settings

d) Specify the new domain account.

e) Click **Next**, **Configure**.



Symantec Installation Manager

Notification Server Configuration

Configure Notification Server credentials, Web site, and email settings

Enter the account credentials needed to run Notification Server

User name: Newdomain\NewDomainAdmin

Password: ••••••••••••••

Select the Web location for Notification Server

Web site: Default Web Site

Port: 80

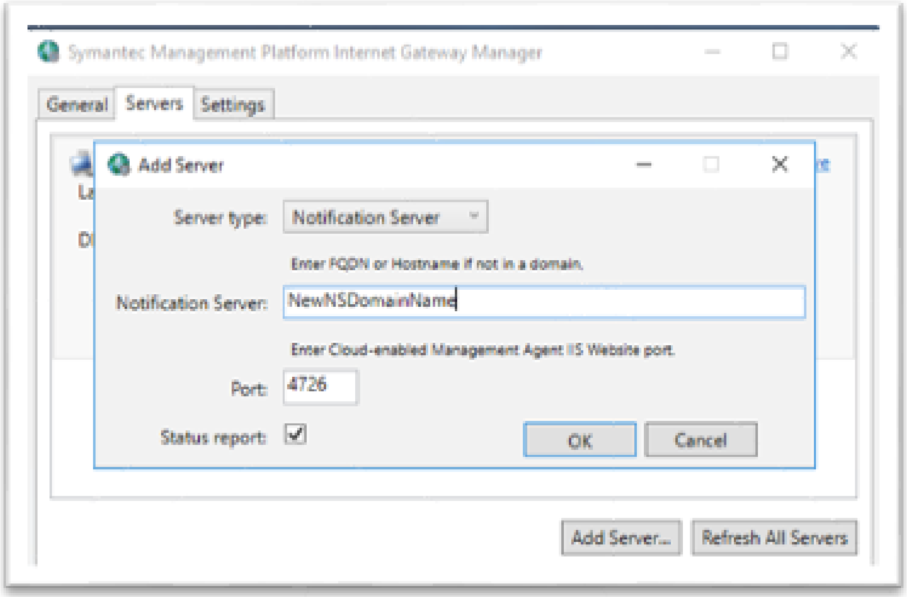
SSL Port: 443 ☑ Require HTTPS to access the Manage

Certificate: lgorp2016-winda.nukad.local

Update the Cloud-Enabled Management Gateway

Update the Cloud-Enabled Management gateway to use the new NS domain name or hostname.

1. Browse to the Symantec Management Platform Internet Gateway Manager (CEM) and add a new Notification Server using the new domain name or hostname.



Server type: Notification Server

Enter FQDN or Hostname if not in a domain.

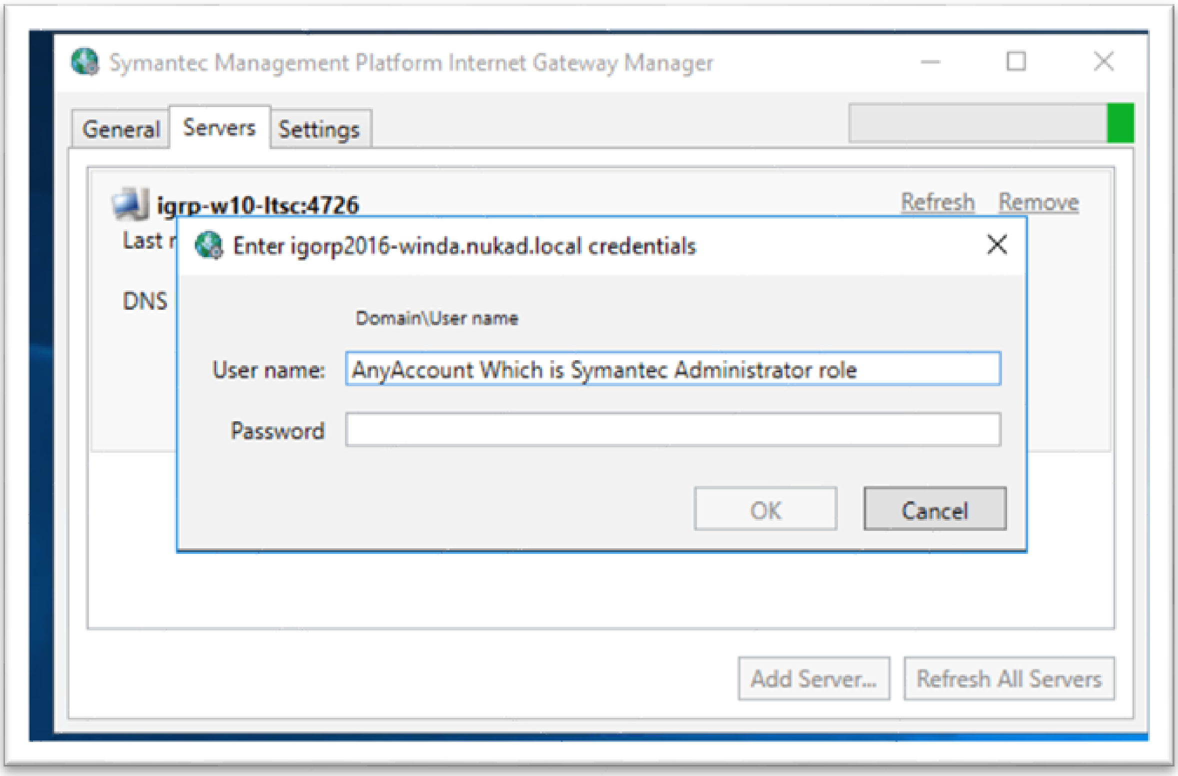
Notification Server: NewNSDomainName

Enter Cloud-enabled Management Agent IIS Website port.

Port: 4726

Status report: ☑

2. Add a new **NSAppIdentity** account or modify another account that is a member of the **Symantec Administrators** role to the new NS entry.



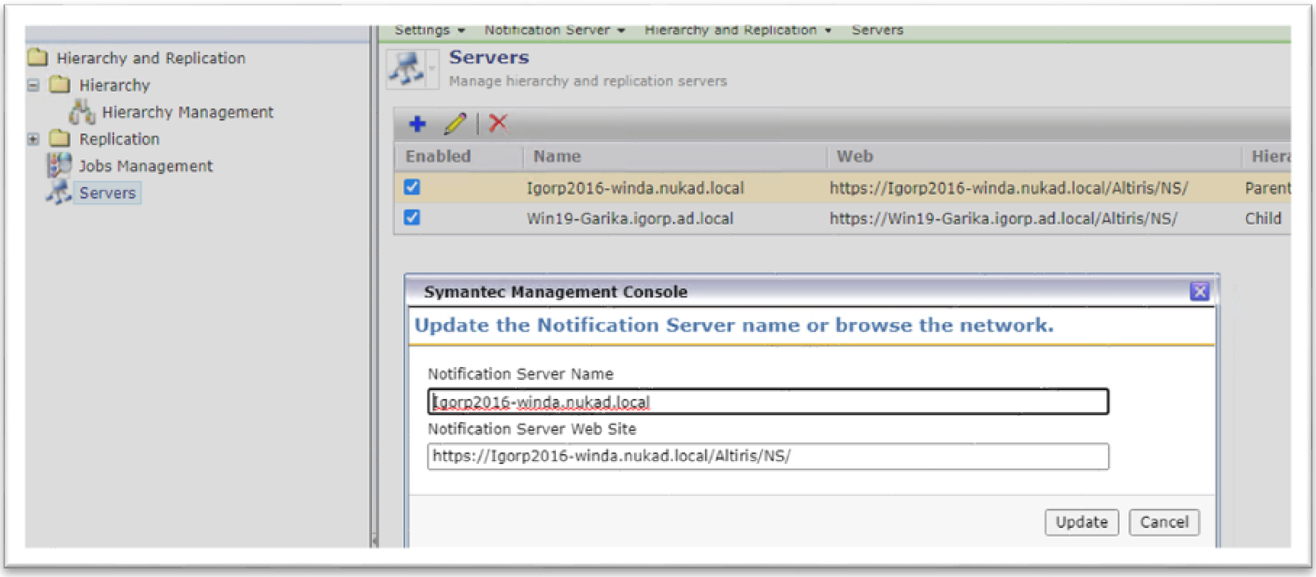
User name: AnyAccount Which is Symantec Administrator role

Password

Re-Enable Hierarchy Replication

Now that the Notfication Server's domain or hostname has been changed, it's time to replicate that change to the systems under its control.

1. Go to the child or parent NS, depending on which server has changed its domain name.
2. Browse to the SMP Console and select **Settings** > **Notification Server** > **Hierarchy** and click **Servers**.
3. Select the NS that has a new domain name or host name and click **Edit**.
4. Update the NS domain name or host name and click **Update**, then click **Save Changes** on the **Servers** page.


Settings ▾
Notification Server ▾
Hierarchy and Replication ▾
Servers
Hierarchy and Replication
Hierarchy
Hierarchy Management
Replication
Jobs Management
Servers
Servers
Manage hierarchy and replication servers
Symantec Management Console
Update
Cancel

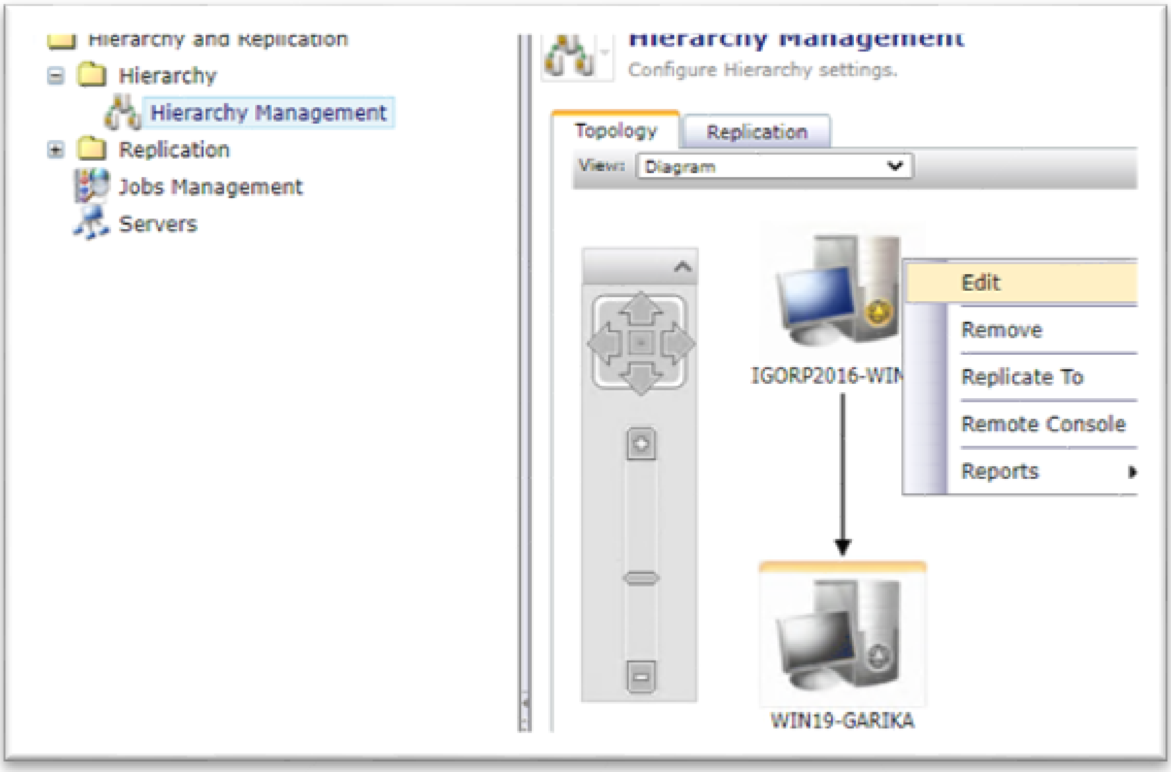
Enabled	Name	Web	Hiera
☑	Igorp2016-winda.nukad.local	https://Igorp2016-winda.nukad.local/Altiris/NS/	Parent
☑	Win19-Garika.igorp.ad.local	https://Win19-Garika.igorp.ad.local/Altiris/NS/	Child

Update the Notification Server name or browse the network.

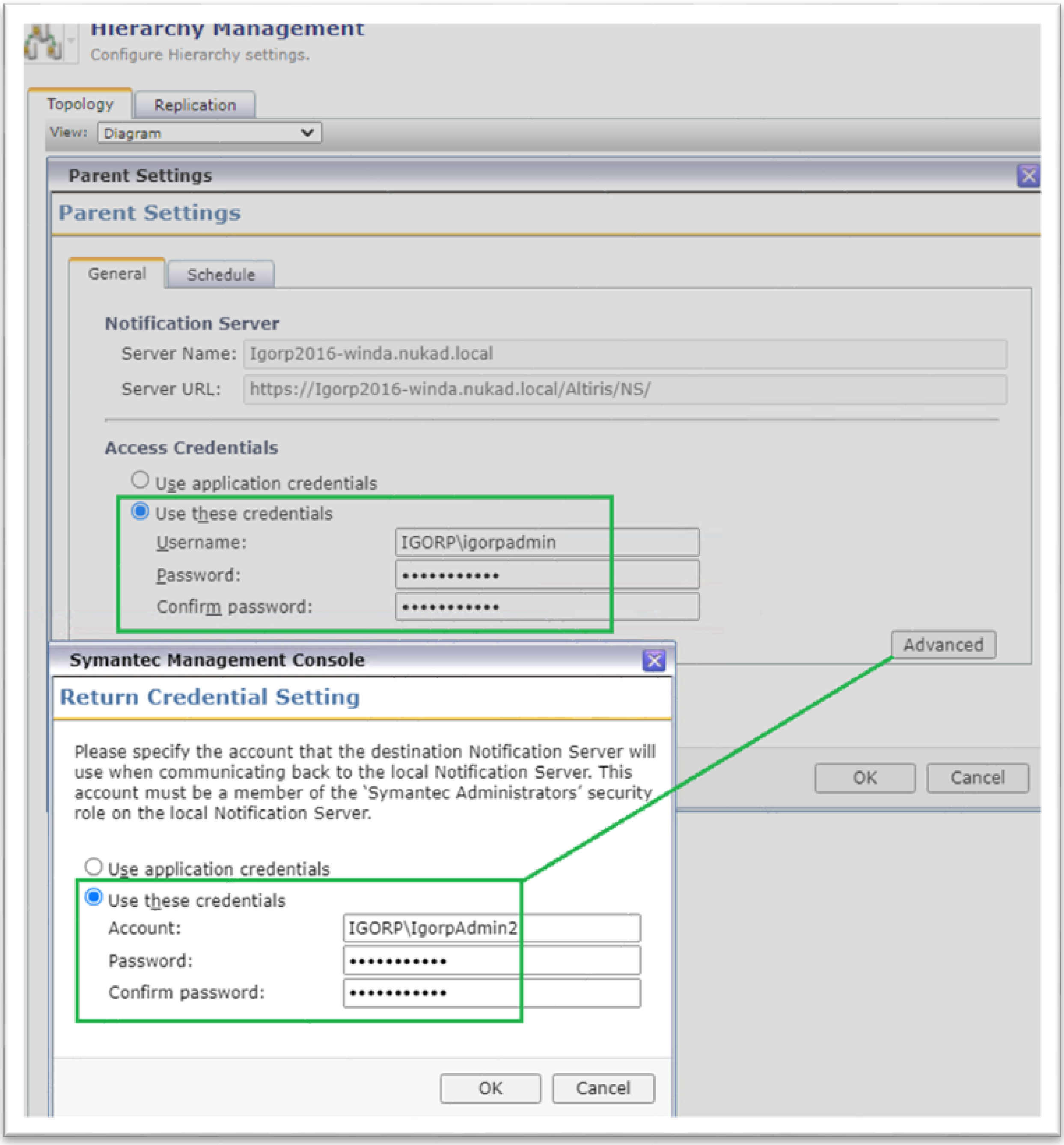
Notification Server Name: Igorp2016-winda.nukad.local

Notification Server Web Site: https://Igorp2016-winda.nukad.local/Altiris/NS/

5. Go to the child or parent NS, depending on which server has changed its domain name.
6. Browse to the SMP Console and click **Settings** > **Notification Server** > **Hierarchy** > **Hierarchy Management.**
7. Right-click click on the NS and select **Edit**.



8. Update the credentials to access the source and destination NS servers:



Hierarchy Management

Configure Hierarchy settings.

View: Diagram

Parent Settings

Parent Settings

Notification Server

Server Name: Igorp2016-winda.nukad.local

Server URL: https://Igorp2016-winda.nukad.local/Altiris/NS/

Access Credentials

○ Use application credentials

● Use these credentials

Username: IGORP\igorpadmin

Password: •••••••••••

Confirm password: •••••••••••

Symantec Management Console

Return Credential Setting

Please specify the account that the destination Notification Server will use when communicating back to the local Notification Server. This account must be a member of the 'Symantec Administrators' security role on the local Notification Server.

○ Use application credentials

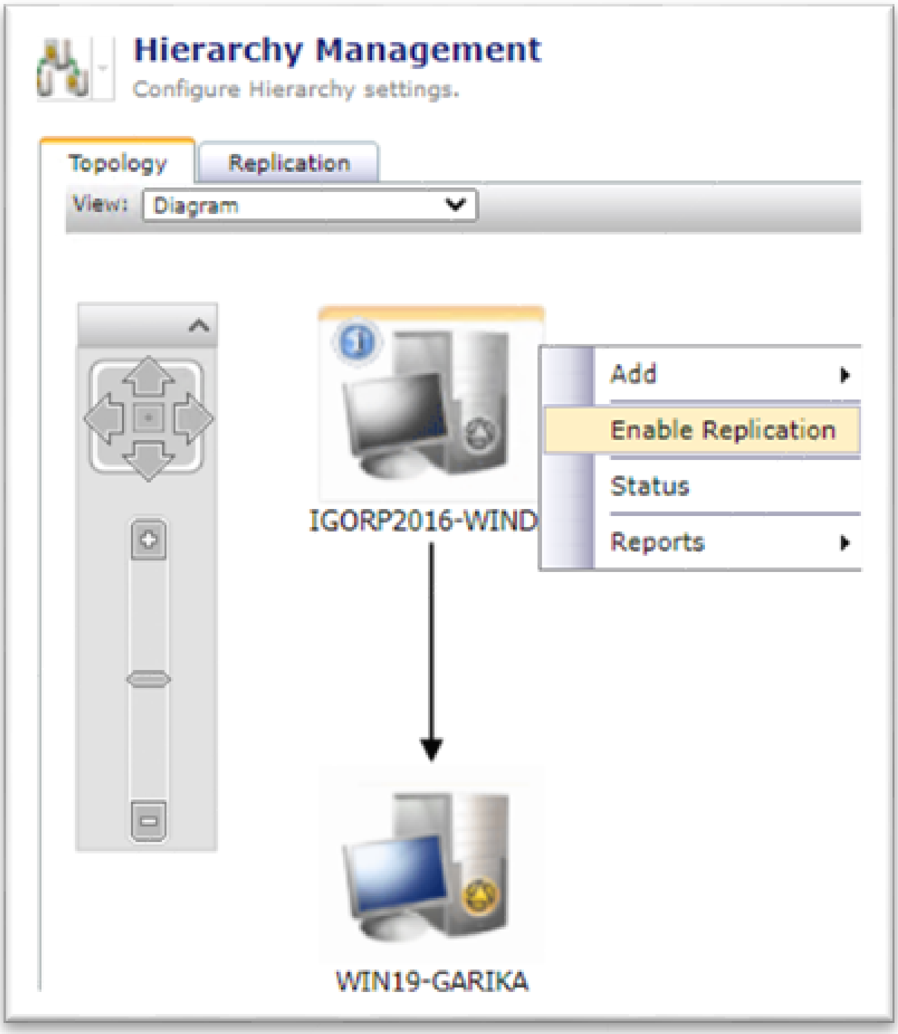
● Use these credentials

Account: IGORP\IgorpAdmin2

Password: •••••••••••

Confirm password: •••••••••••

9. When you have updated the credentials for replication, you can enable replication on all parent and child NS servers. Right-click on each Notification Server and select **Enable Replication**.



Hierarchy Management

Configure Hierarchy settings.

Topology | Replication

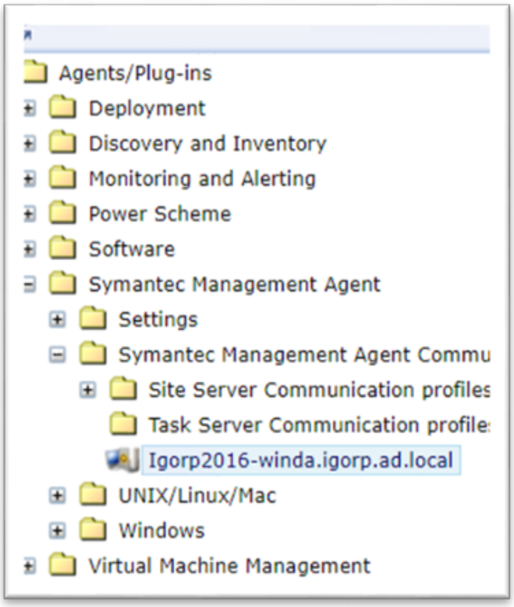
View: Diagram

Update the Notification Server Communication Profile

After the Notification Server's domain name or hostname changes, the default NS communication profile retains the previous NS domain name or hostname. By default, the SMP console does not permit modifying the domain name or hostname. To accomplish this task, you'll need to run a custom SQL query that activates the option.

NOTE

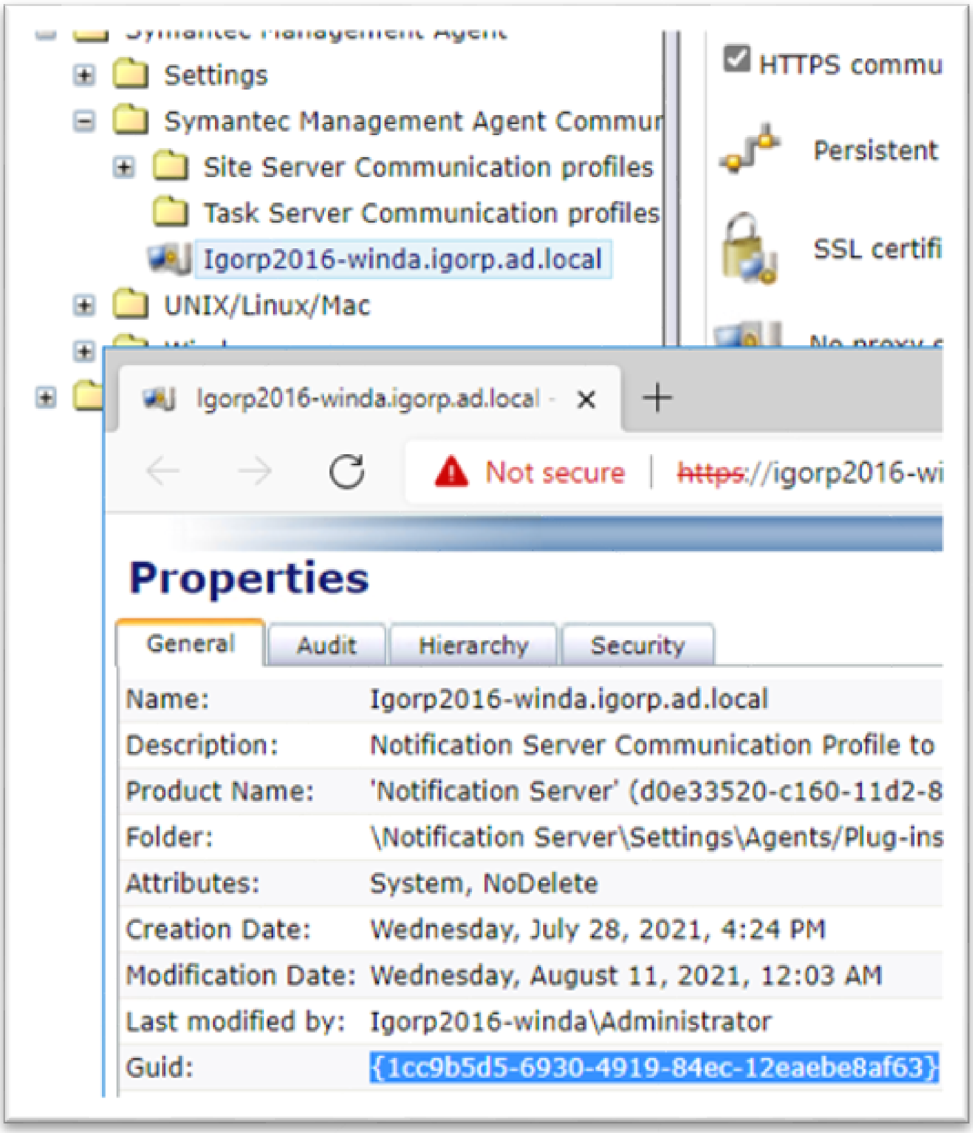
Take note of the profile tree below. The NS hostname is not editable.



- Agents/Plug-ins
  - Deployment
  - Discovery and Inventory
  - Monitoring and Alerting
  - Power Scheme
  - Software
  - Symantec Management Agent
    - Settings
    - Symantec Management Agent Commu
      - Site Server Communication profiles
      - Task Server Communication profile:
      - Igorp2016-winda.igorp.ad.local
    - UNIX/Linux/Mac
    - Windows
  - Virtual Machine Management

Section One: Rename the SMP Communication Profile

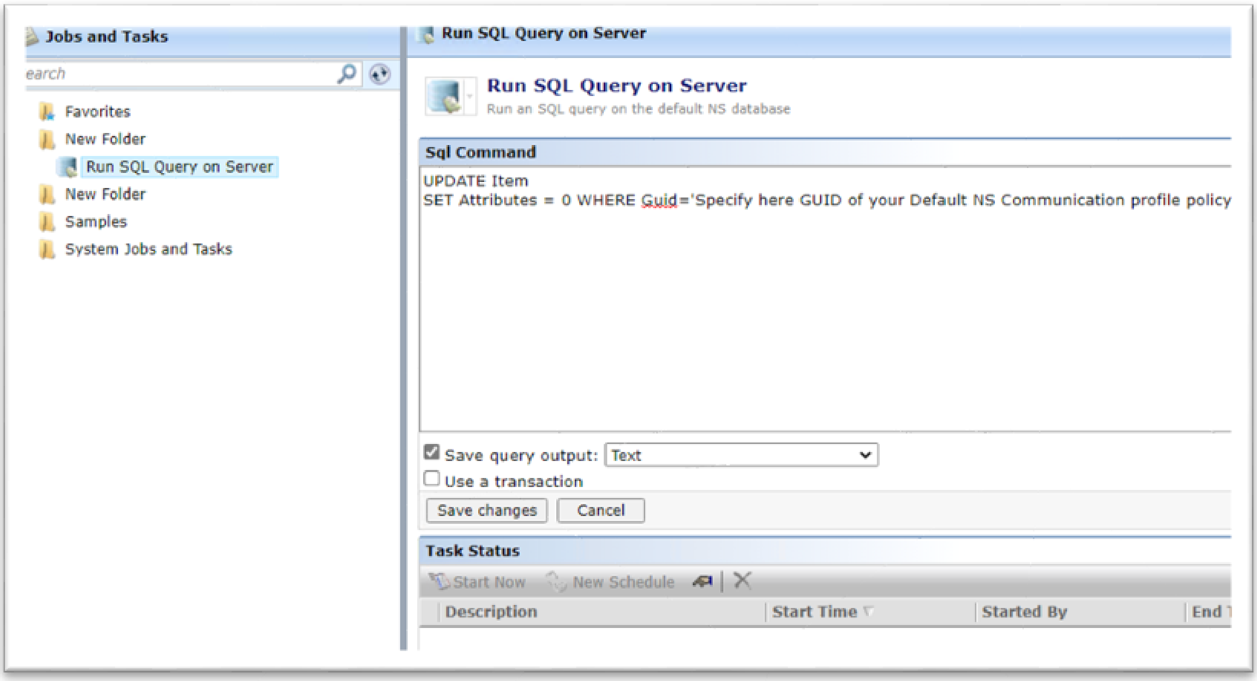
1. Right-click **Default NS Communication profile** in the SMP Console and select **Properties.**
2. At the bottom of the **Properties** window, note the Guid field.


Symantec Management Agent
Settings
Symantec Management Agent Commur
Site Server Communication profiles
Task Server Communication profiles
Igorp2016-winda.igorp.ad.local
UNIX/Linux/Mac
HTTPS commu
Persistent
SSL certifi
No proxy s
Igorp2016-winda.igorp.ad.local
Not secure
https://igorp2016-wi
General
Audit
Hierarchy
Security

Properties

Name:	Igorp2016-winda.igorp.ad.local
Description:	Notification Server Communication Profile to
Product Name:	'Notification Server' (d0e33520-c160-11d2-8
Folder:	\Notification Server\Settings\Agents/Plug-ins
Attributes:	System, NoDelete
Creation Date:	Wednesday, July 28, 2021, 4:24 PM
Modification Date:	Wednesday, August 11, 2021, 12:03 AM
Last modified by:	Igorp2016-winda\Administrator
Guid:	{1cc9b5d5-6930-4919-84ec-12eaebe8af63}

3. Highlight the text there, right-click, select **copy**, and close the properties window.
4. In the SMP console, click **Manage** > **Jobs and Tasks**.
5. Right-click any existing folder and click **Create new task** > **Run SQL Query on Server**. The SQL Command window displays.



```
UPDATE Item
SET Attributes = 0 WHERE Guid='Specify here GUID of your Default NS Communication profile policy
```

☑ Save query output: Text

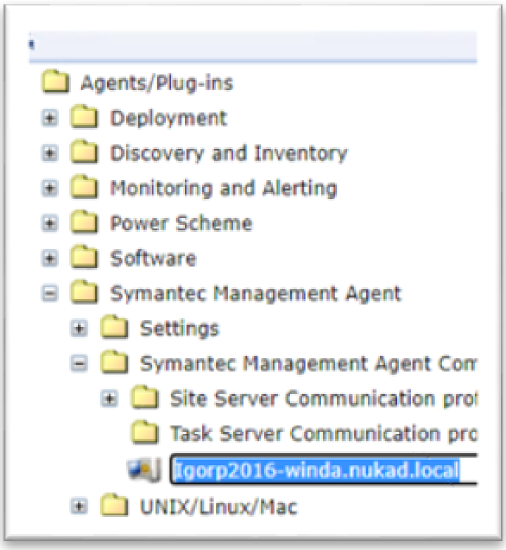
□ Use a transaction

6. Enter the following command string, as it appears below. Replace “<guid number>” with the guid value you saved in step 3 above:

```
UPDATE Item

SET Attributes = 0 WHERE Guid=<guid number>
```

7. Click **Run SQL Query** to execute the command. Now the console will permit you to rename the default NS Communication profile.
8. Browse to the profile tree, right-click the NS communication profile, and select **rename**.
9. Rename the profile.


Agents/Plug-ins
Deployment
Discovery and Inventory
Monitoring and Alerting
Power Scheme
Software
Symantec Management Agent
Settings
Symantec Management Agent Com
Site Server Communication prof
Task Server Communication pro
Igorp2016-winda.nukad.local
UNIX/Linux/Mac

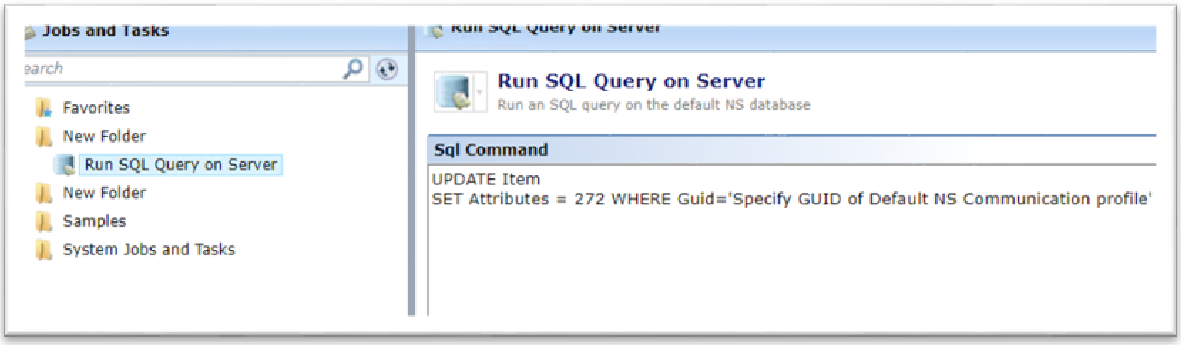
Section Two: Reset the Communications Profile Attributes

Now that you’ve renamed the NS communication profile, you’ll need to re-secure the communication profile, to ensure it’s no longer editable.

1. Modify the **Run SQL Query** task you created earlier, and replace the previous query with this one:

```
UPDATE Item

SET Attributes = 272 WHERE Guid='Specify GUID of Default NS Communication profile'
```



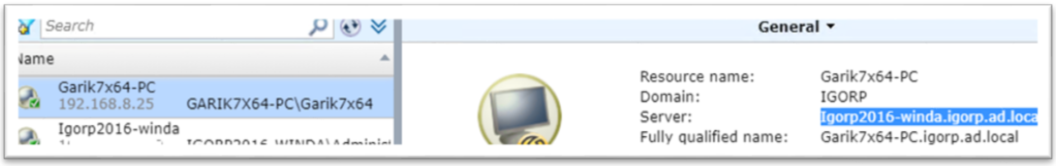
Sql Command

```
UPDATE Item
SET Attributes = 272 WHERE Guid='Specify GUID of Default NS Communication profile'
```

2. Click **Run SQL Query**.
3. When the **SQL Query** task is complete, you’ll need to restart the **IISADMIN** service on the NS. This ensures the profile can’t be edited or deleted in error.
   a. In Windows, click **Start** > **Run** > **services**.
   b. Locate **IISAdmin** in the list of services, right-click it, and select **restart**.

Update SMP Console UI With the New Name

Even though the clients can see and communicate with the new NS domain name or hostname, ITMS administrators will still see old NS Server name when you view the general properties for each PC as shown below.



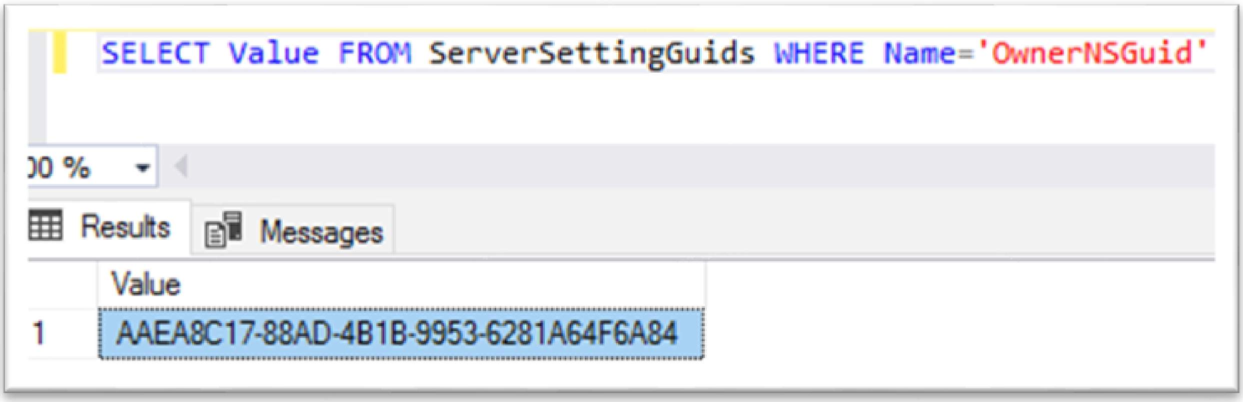
Garik7x64-PC 192.168.8.25 GARIK7X64-PC\Garik7x64
Igorp2016-winda

Resource name: Garik7x64-PC
Domain: IGORP
Server: Igorp2016-winda.igorp.ad.loca
Fully qualified name: Garik7x64-PC.igorp.ad.local

To resolve this, perform another SQL Query task.

1. Modify the **SQL Query** task you created earlier, and replace the previous query with this one:

```
SELECT Value FROM ServerSettingGuids WHERE Name='OwnerNSGuid'
```

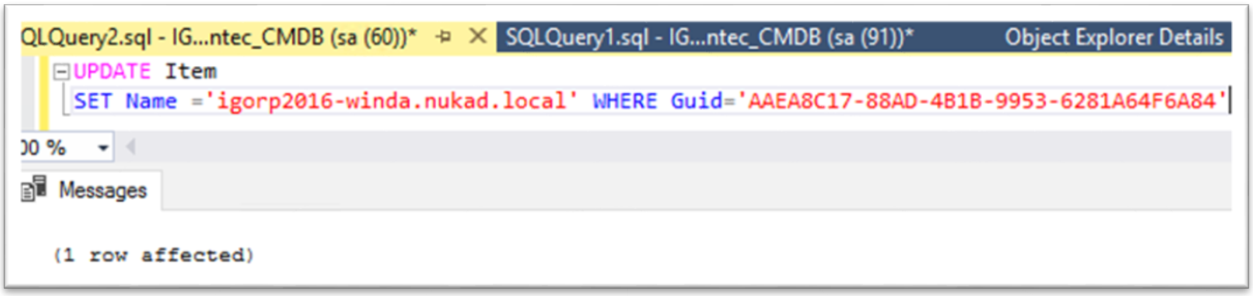


```
SELECT Value FROM ServerSettingGuids WHERE Name='OwnerNSGuid'
```

	Value
1	AAEA8C17-88AD-4B1B-9953-6281A64F6A84

2. Run the SQL Query. The Results field displays the guid. Right-click and copy the value displayed.
3. Modify the SQL Query again, this time to update the NS domain or hostname:

```
UPDATE Item
SET Name ='Specify here new FQDN of your NS' WHERE Guid='Specify here OwnerNSGuid'
```

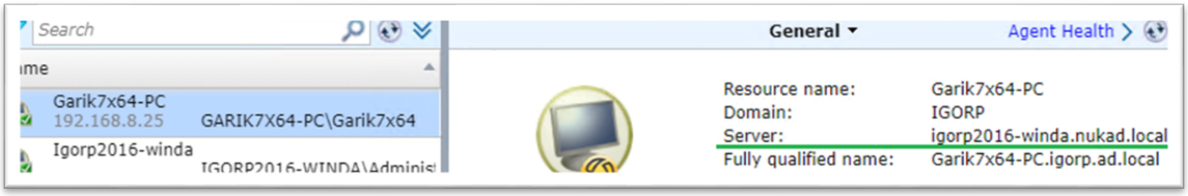

QLQuery2.sql - IG...ntec_CMDB (sa (60))*
SQLQuery1.sql - IG...ntec_CMDB (sa (91))*
Object Explorer Details
00 %
Messages

```
UPDATE Item
SET Name ='igorp2016-winda.nukad.local' WHERE Guid='AAEA8C17-88AD-4B1B-9953-6281A64F6A84'
```

```
(1 row affected)
```

4. Run the query and close the query page.

5. Browse to the ITMS Views page in the console and select a computer from the list. Note that the general information page now shows the correct NS domain name or hostname.



Garik7x64-PC 192.168.8.25 GARIK7X64-PC\Garik7x64

Igorp2016-winda IGORP2016-WINDA\Adminis

Resource name: Garik7x64-PC

Domain: IGORP

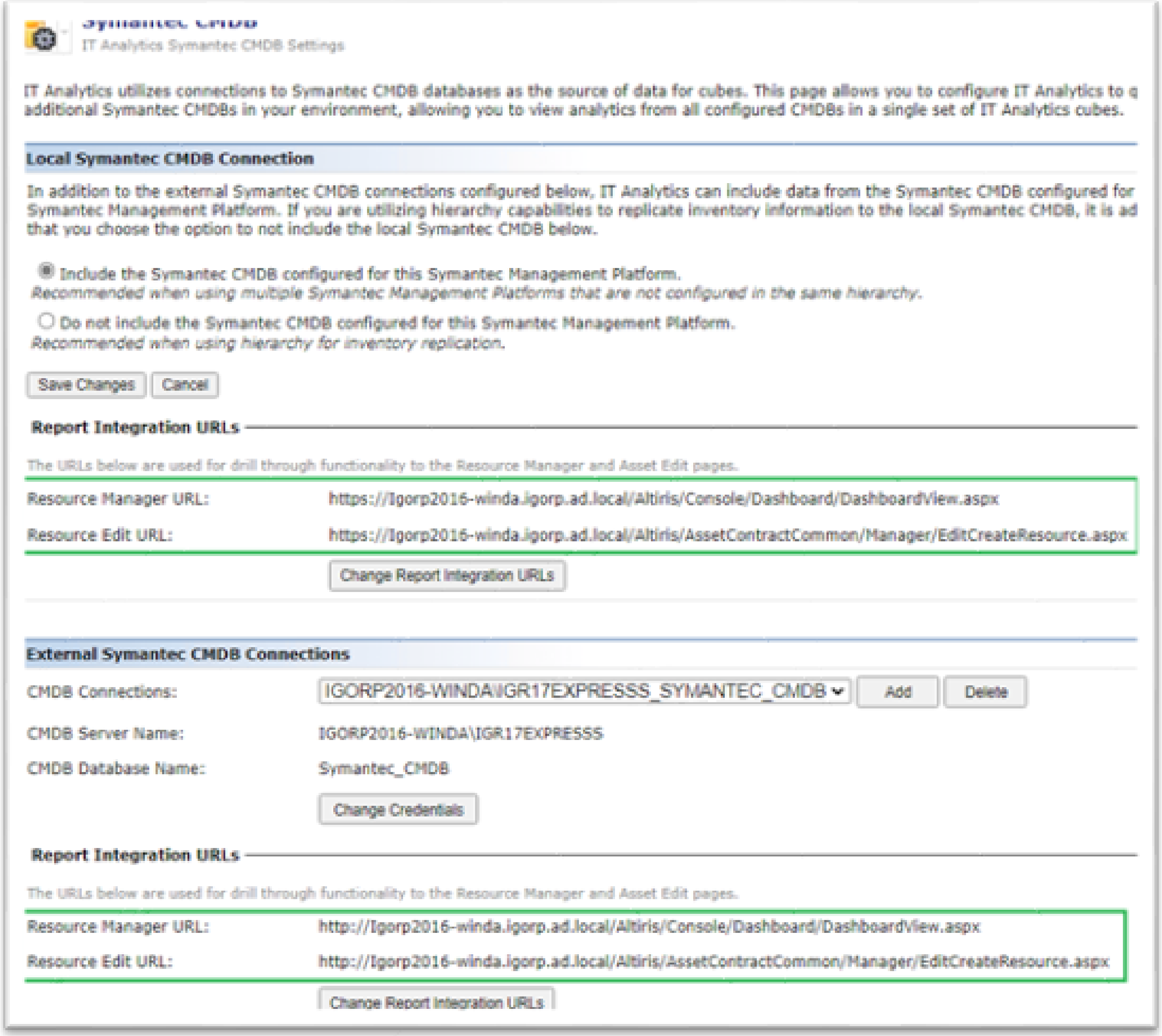
Server: igorp2016-winda.nukad.local

Fully qualified name: Garik7x64-PC.igorp.ad.local

Update IT Analytics Report Integration

Ensure that IT Analytics can communicate with the Notification Server for reporting.

1. Open the SMP Console, click **Settings** > **Notification Server** > **IT Analytics.**
2. Select **Symantec CMDB**. The IT Analytics Symantec CMDB Settings page opens.
3. Under **Local Symantec CMDB Connection**, locate the Report Integration URLs section and click **Change Report Integration URLs**.
4. Modify the URLs as appropriate to update them with the new domain or hostname.



Symantec CMDB

IT Analytics Symantec CMDB Settings

IT Analytics utilizes connections to Symantec CMDB databases as the source of data for cubes. This page allows you to configure IT Analytics to q additional Symantec CMDBs in your environment, allowing you to view analytics from all configured CMDBs in a single set of IT Analytics cubes.

Local Symantec CMDB Connection

In addition to the external Symantec CMDB connections configured below, IT Analytics can include data from the Symantec CMDB configured for Symantec Management Platform. If you are utilizing hierarchy capabilities to replicate inventory information to the local Symantec CMDB, it is ad that you choose the option to not include the local Symantec CMDB below.

● Include the Symantec CMDB configured for this Symantec Management Platform.
Recommended when using multiple Symantec Management Platforms that are not configured in the same hierarchy.

○ Do not include the Symantec CMDB configured for this Symantec Management Platform.
Recommended when using hierarchy for inventory replication.

Report Integration URLs

The URLs below are used for drill through functionality to the Resource Manager and Asset Edit pages.

Resource Manager URL: https://Igorp2016-winda.igorp.ad.local/Altiris/Console/Dashboard/DashboardView.aspx

Resource Edit URL: https://Igorp2016-winda.igorp.ad.local/Altiris/AssetContractCommon/Manager/EditCreateResource.aspx

External Symantec CMDB Connections

CMDB Connections: IGORP2016-WINDA\IGR17EXPRESSS_SYMANTEC_CMDB

CMDB Server Name: IGORP2016-WINDA\IGR17EXPRESSS

CMDB Database Name: Symantec_CMDB

Report Integration URLs

The URLs below are used for drill through functionality to the Resource Manager and Asset Edit pages.

Resource Manager URL: http://Igorp2016-winda.igorp.ad.local/Altiris/Console/Dashboard/DashboardView.aspx

Resource Edit URL: http://Igorp2016-winda.igorp.ad.local/Altiris/AssetContractCommon/Manager/EditCreateResource.aspx

Save Changes
Cancel
Change Report Integration URLs
Add
Delete
Change Credentials
Change Report Integration URLs

5. Repeat the process for the URLs under **External Symantec CMDB Connections**.

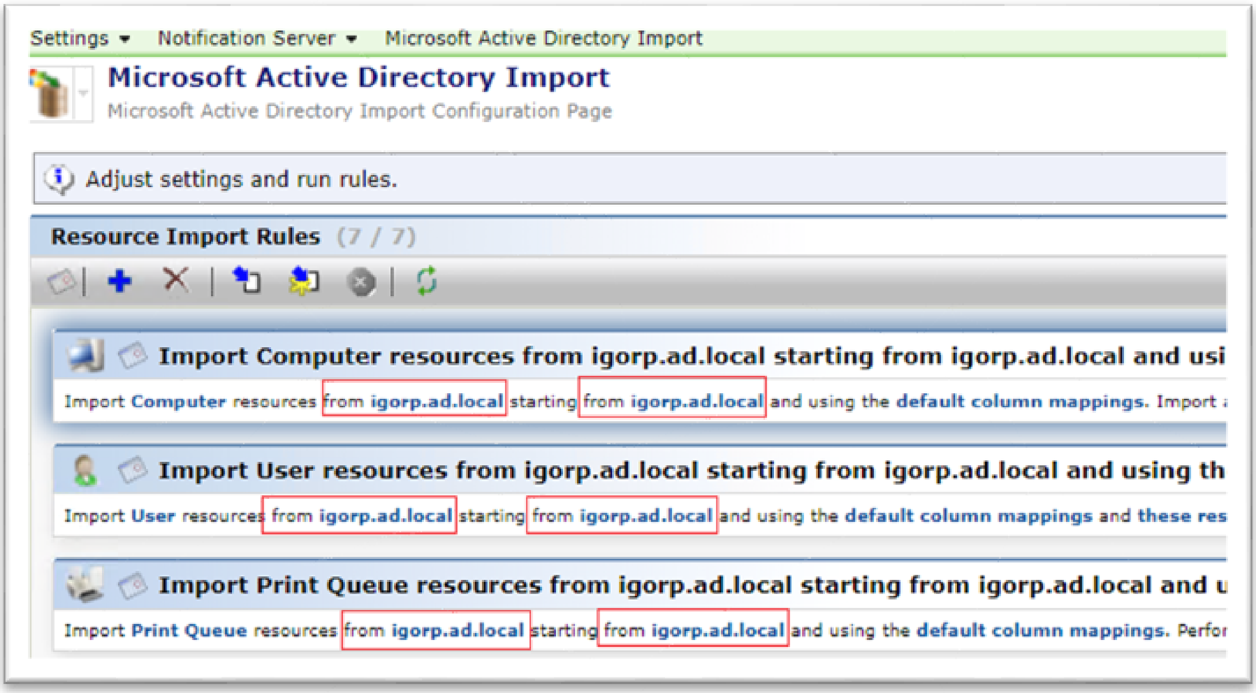
Other Settings

There are several other places where the domain name or hostname are referenced in a typical ITMS environment.

AD Import

After the NS Domain name change, AD Import rules will still have the old domain name specified. If the domain is no longer reachable, AD import rules will fail to execute.

1. Browse to the SMP Console > **Actions** > **Discover** > **Import Active Directory Import**.



Microsoft Active Directory Import

Microsoft Active Directory Import Configuration Page

Adjust settings and run rules.

Resource Import Rules (7 / 7)

Import Computer resources from igorp.ad.local starting from igorp.ad.local and usi

Import Computer resources from igorp.ad.local starting from igorp.ad.local and using the default column mappings. Import

Import User resources from igorp.ad.local starting from igorp.ad.local and using th

Import User resources from igorp.ad.local starting from igorp.ad.local and using the default column mappings and these res

Import Print Queue resources from igorp.ad.local starting from igorp.ad.local and u

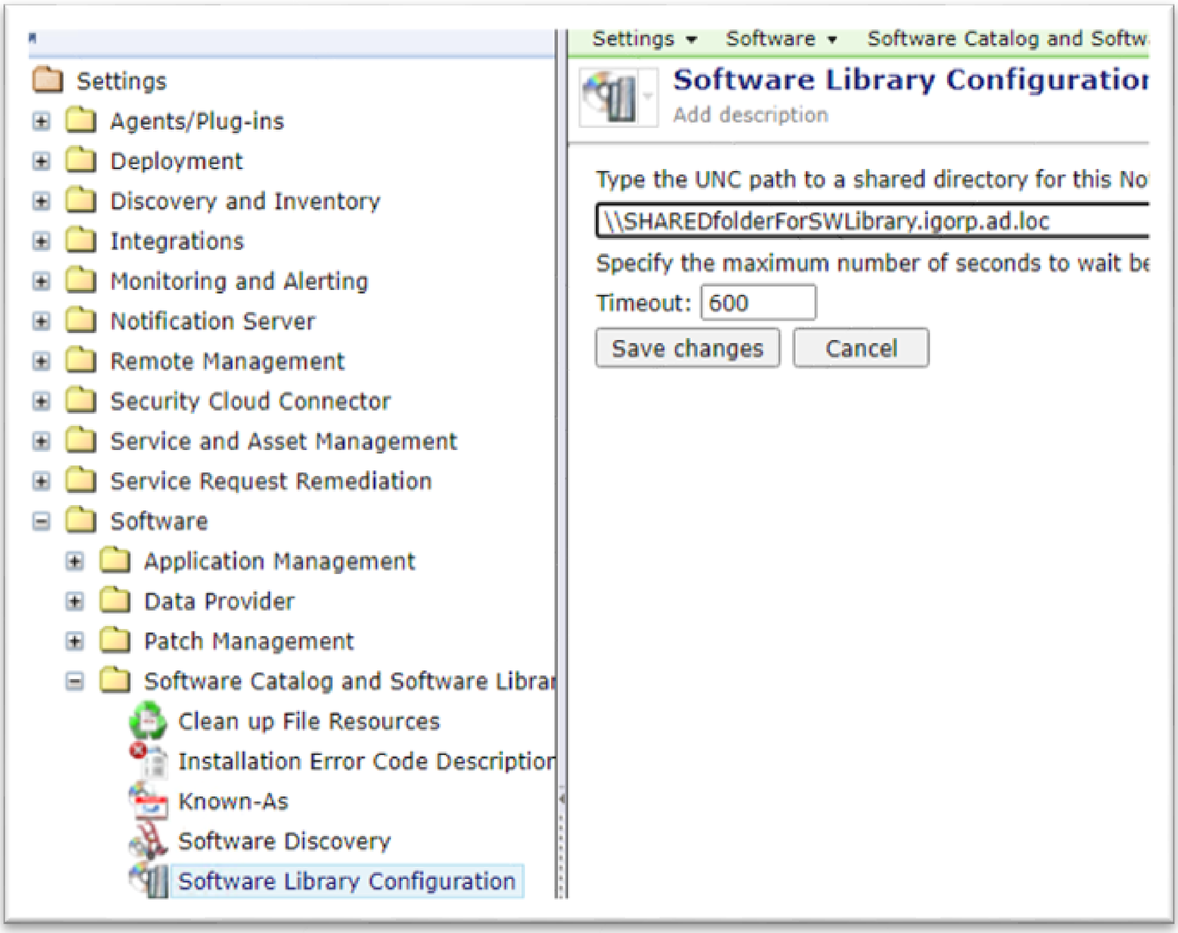
Import Print Queue resources from igorp.ad.local starting from igorp.ad.local and using the default column mappings. Perfor

2. Edit each entry as appropriate to set the new domain or hostname.

Software Library Location

Make sure that the previously set location for your Software Library is still accessible from the new NS domain or hostname.

1. Browse to the SMP Console, click **Settings > All Settings** > and expand the **Software** folder.
2. Expand **Software Catalog and Software Library Settings** and select **Software Library Configuration**.



Type the UNC path to a shared directory for this No

\\SHAREDfolderForSWLibrary.igorp.ad.loc

Specify the maximum number of seconds to wait be

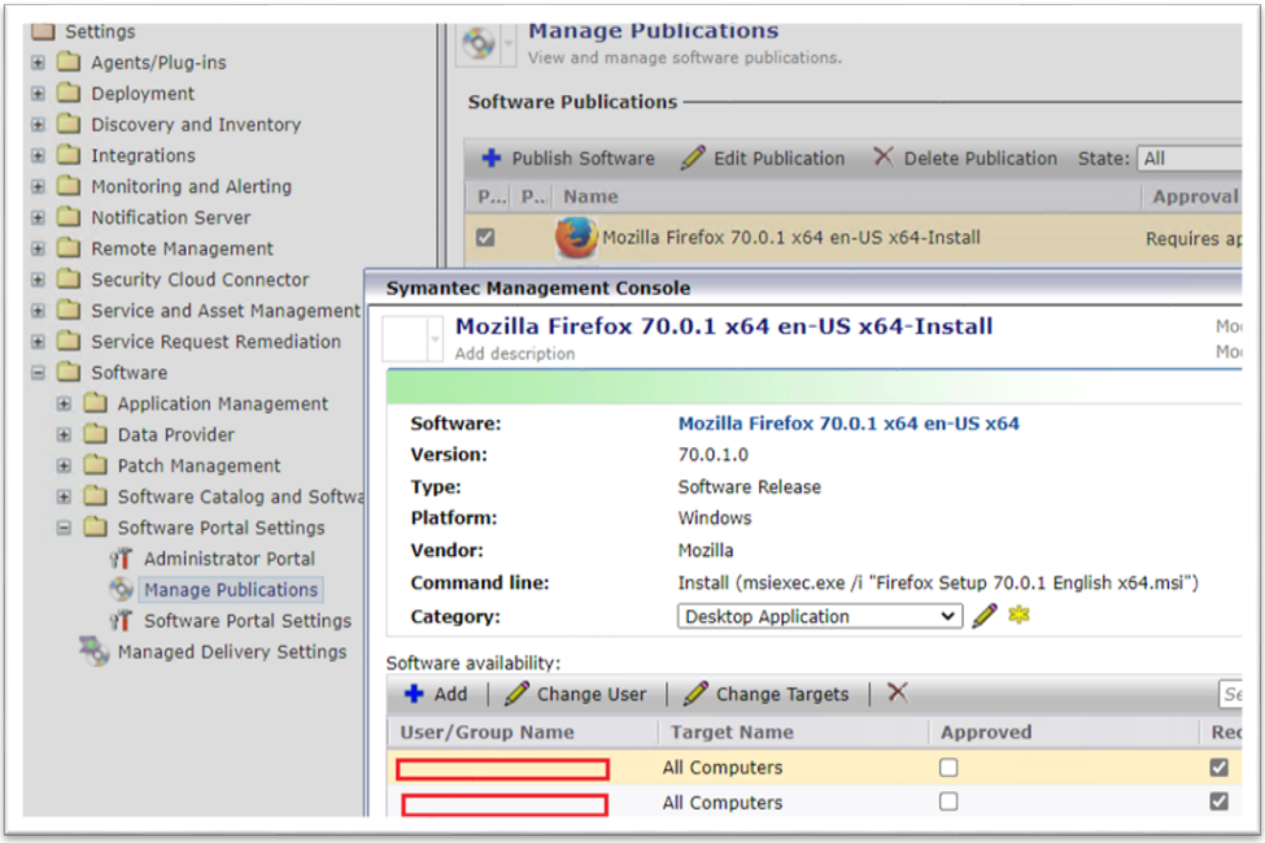
Timeout: 600

3. Update the URL as appropriate for the new domain or hostname.

Managed Delivery Policies

Review your previously published Software and Managed Delivery policies, as all managed clients will now be logged to the software portal using the new NS domain name or hostname. If this process was used to change the domain name, users should authenticate to the portal using their new domain name accounts. If there's a disconnect in the client's login domain and the portal domain, not all published software or managed delivery policies will be available.

1. Browse to the SMP Console and click **Settings** > **All Settings** and expand the **Software** folder.
2. Expand **Software Portal Settings** and open **Manage Publications**.
3. Select any previously published Item and click **Edit**.
4. You'll see that no domain group is available, so you will need to manually define the appropriate Domain/User group. This will ensure that your software and managed distribution policy is available again for your managed client computers.



- Settings
  - Agents/Plug-ins
  - Deployment
  - Discovery and Inventory
  - Integrations
  - Monitoring and Alerting
  - Notification Server
  - Remote Management
  - Security Cloud Connector
  - Service and Asset Management
  - Service Request Remediation
  - Software
    - Application Management
    - Data Provider
    - Patch Management
    - Software Catalog and Softwa
    - Software Portal Settings
      - Administrator Portal
      - Manage Publications
      - Software Portal Settings
    - Managed Delivery Settings

Manage Publications
View and manage software publications.

Software Publications

P...	P...	Name	Approval
☑		Mozilla Firefox 70.0.1 x64 en-US x64-Install	Requires ap

Symantec Management Console

Mozilla Firefox 70.0.1 x64 en-US x64-Install
Add description

Software:	Mozilla Firefox 70.0.1 x64 en-US x64
Version:	70.0.1.0
Type:	Software Release
Platform:	Windows
Vendor:	Mozilla
Command line:	Install (msiexec.exe /i "Firefox Setup 70.0.1 English x64.msi")
Category:	Desktop Application

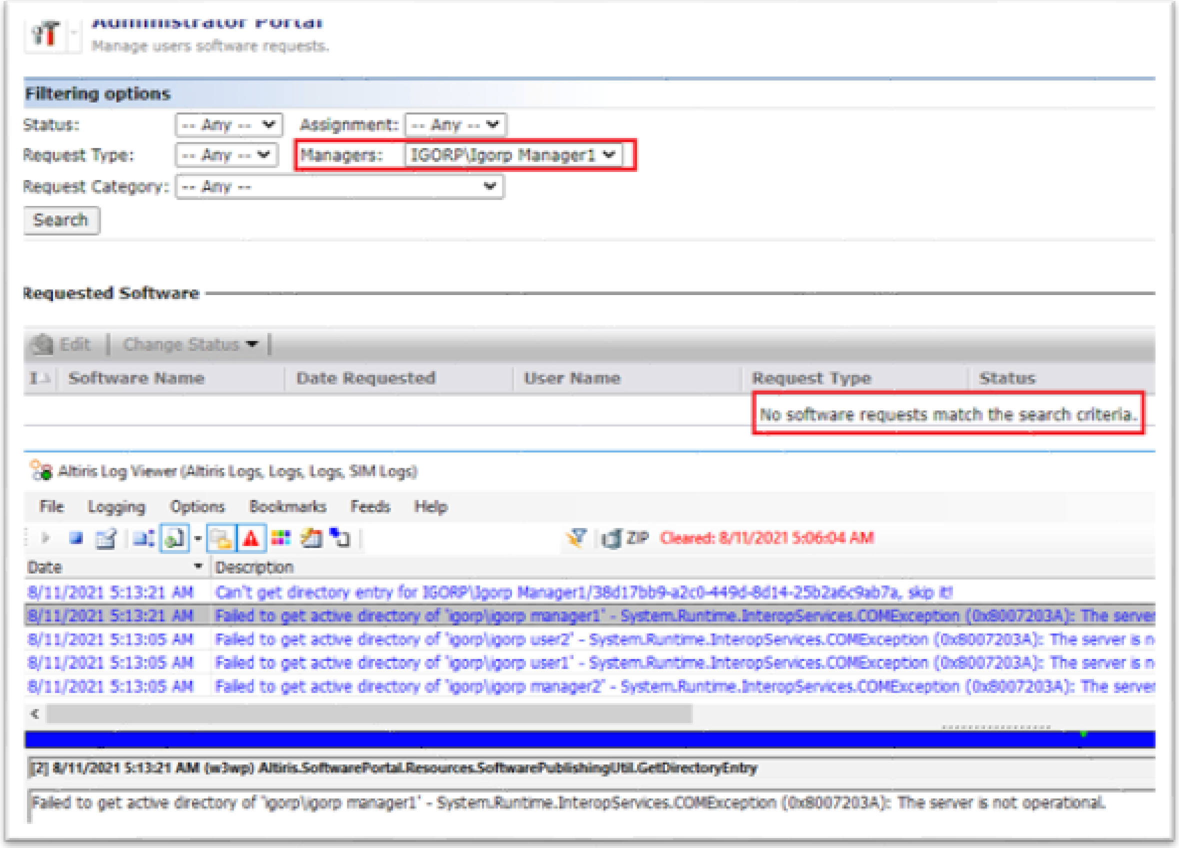
Software availability:

User/Group Name	Target Name	Approved	Rec
[redacted]	All Computers	□	☑
[redacted]	All Computers	□	☑

Administrative user account roles

If an administrator account (and their direct reports) defined in the Administrator Portal has a manager account from the previous domain, search will show no records because as the old domain is no longer accessible.

For example, this is how it appears when **IGORP** is the defined old domain and offline.



Administrator Portal

Manage users software requests.

Filtering options

Status: -- Any -- Assignment: -- Any --

Request Type: -- Any -- Managers: IGORP\Igorp Manager1

Request Category: -- Any --

Requested Software

I	Software Name	Date Requested	User Name	Request Type	Status

No software requests match the search criteria.

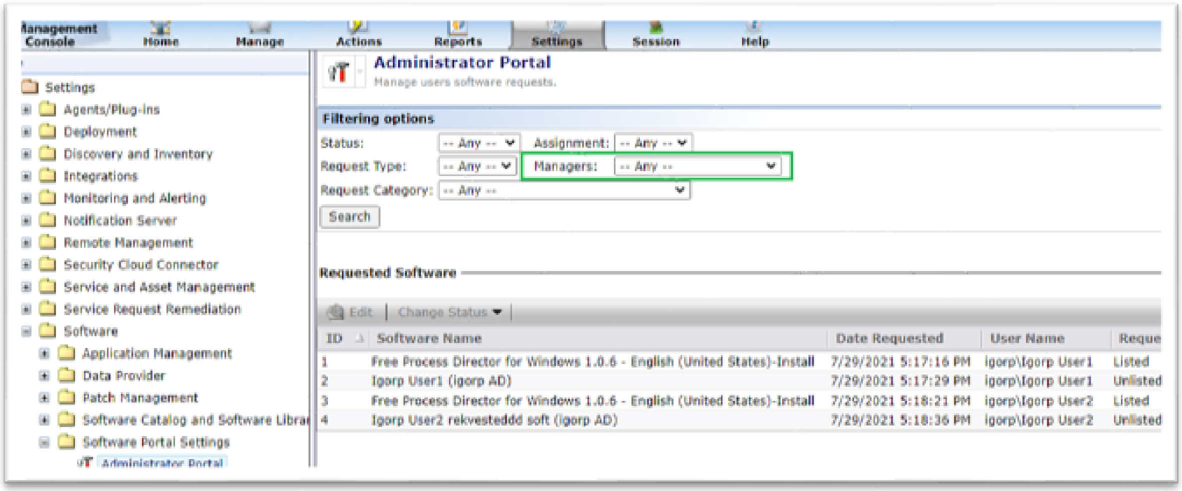
Altiris Log Viewer (Altiris Logs, Logs, Logs, SIM Logs)

Cleared: 8/11/2021 5:06:04 AM

```
Date                  Description
8/11/2021 5:13:21 AM  Can't get directory entry for IGORP\Igorp Manager1/38d17bb9-a2c0-449d-8d14-25b2a6c9ab7a, skip it!
8/11/2021 5:13:21 AM  Failed to get active directory of 'igorp\igorp manager1' - System.Runtime.InteropServices.COMException (0x8007203A): The server
8/11/2021 5:13:05 AM  Failed to get active directory of 'igorp\igorp user2' - System.Runtime.InteropServices.COMException (0x8007203A): The server is n
8/11/2021 5:13:05 AM  Failed to get active directory of 'igorp\igorp user1' - System.Runtime.InteropServices.COMException (0x8007203A): The server is n
8/11/2021 5:13:05 AM  Failed to get active directory of 'igorp\igorp manager2' - System.Runtime.InteropServices.COMException (0x8007203A): The server

[2] 8/11/2021 5:13:21 AM (w3wp) Altiris.SoftwarePortal.Resources.SoftwarePublishingUtil.GetDirectoryEntry
Failed to get active directory of 'igorp\igorp manager1' - System.Runtime.InteropServices.COMException (0x8007203A): The server is not operational.
```

As a workaround, you can view old client requests from these clients if you set the **Managers** drop-down to Any. From there, you can approve or deny any requests that are still in queue.



Administrator Portal

Manage users software requests.

Filtering options

Status: -- Any -- Assignment: -- Any --

Request Type: -- Any -- Managers: -- Any --

Request Category: -- Any --

Requested Software

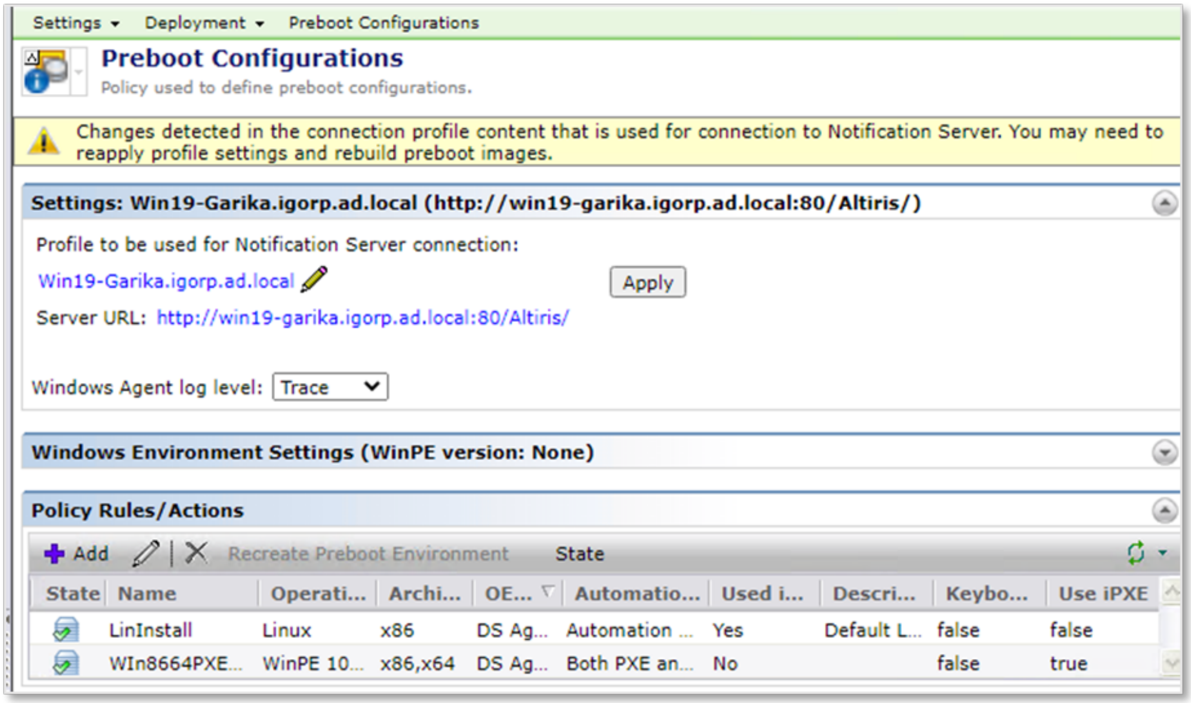
ID	Software Name	Date Requested	User Name	Reque
1	Free Process Director for Windows 1.0.6 - English (United States)-Install	7/29/2021 5:17:16 PM	igorp\Igorp User1	Listed
2	Igorp User1 (igorp AD)	7/29/2021 5:17:29 PM	igorp\Igorp User1	Unlisted
3	Free Process Director for Windows 1.0.6 - English (United States)-Install	7/29/2021 5:18:21 PM	igorp\Igorp User2	Listed
4	Igorp User2 rekvesteddd soft (igorp AD)	7/29/2021 5:18:36 PM	igorp\Igorp User2	Unlisted

Deployment Solution

Update the deployment solution configuration for new Windows Preboot environments.

1. In the Symantec Management Console, open **Settings** > **All Settings** > and expand the **Deployment** folder.
2. Select the **Preboot Configurations** page.

3. Make sure that the correct NS communication profile is set and click **Apply** to use a new NS domain name or hostname in the communication profile for WinPE & LinPE.
4. Rebuild the preboot environments and reinstall them on managed client computers.
5. Download the updated preboot environment to your PXE servers.



Preboot Configurations
Policy used to define preboot configurations.

⚠ Changes detected in the connection profile content that is used for connection to Notification Server. You may need to reapply profile settings and rebuild preboot images.

Settings: Win19-Garika.igorp.ad.local (http://win19-garika.igorp.ad.local:80/Altiris/)

Profile to be used for Notification Server connection:
Win19-Garika.igorp.ad.local
Server URL: http://win19-garika.igorp.ad.local:80/Altiris/

Windows Agent log level: Trace

Windows Environment Settings (WinPE version: None)

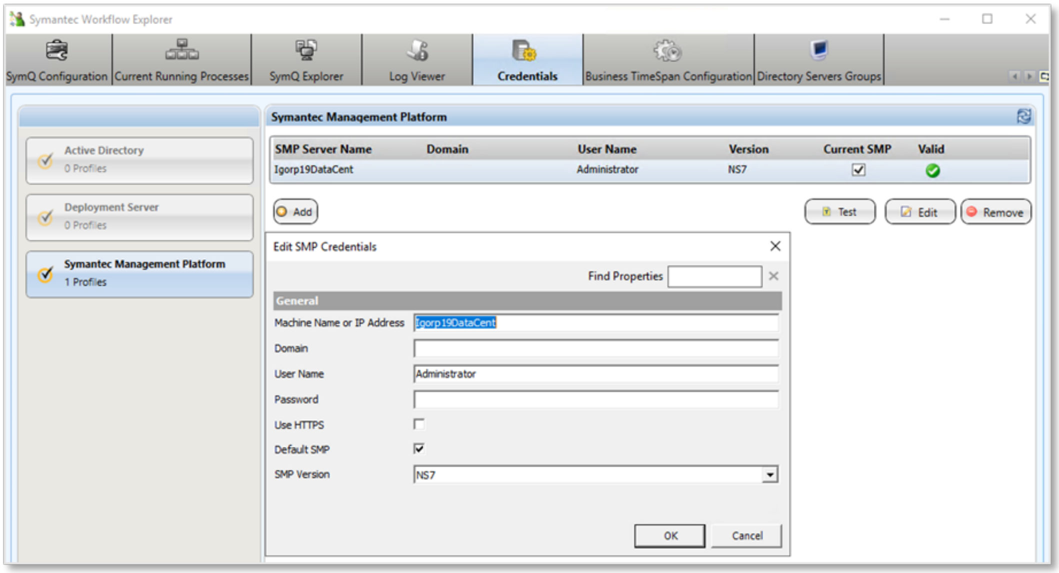
Policy Rules/Actions

State	Name	Operati...	Archi...	OE...	Automatio...	Used i...	Descri...	Keybo...	Use iPXE
✓	LinInstall	Linux	x86	DS Ag...	Automation ...	Yes	Default L...	false	false
✓	WIn8664PXE...	WinPE 10...	x86,x64	DS Ag...	Both PXE an...	No		false	true

Workflow Solution

Update the new NS domain name or hostname on existing Workflow installed servers.

1. Click the **Start menu** > **Symantec** > **Credentials Manager** > locate the old NS domain name or hostname and edit it to a new NS domain name or hostname.



Symantec Management Platform

SMP Server Name	Domain	User Name	Version	Current SMP	Valid
Igorp19DataCent		Administrator	NS7	☑	✓

Edit SMP Credentials

Machine Name or IP Address	Igorp19DataCent
Domain	
User Name	Administrator
Password	
Use HTTPS	□
Default SMP	☑
SMP Version	NS7

1. In the Symantec Workflow tray icon, open settings and update the NS domain name or hostname.
2. Click **Save Changes** and restart the Symantec Workflow service.

Symantec™

A Division of Broadcom