How to run ITMS 7.5 on HTTPS

This document provides information about how to configure your IT Management Suite (ITMS) 7.5 environment to enable access using HTTPS (HTTP over SSL). The instructions in this document are valid for the ITMS 7.5 platform.

23 January 2014

Contents

Why use HTTPS communication in your ITMS environment?

Accessing ITMS (IT Management Suite) using HTTPS provides the following advantages:

- **Increased secure and reliable communication**
  HTTP is unsecured and is vulnerable to man-in-the-middle and eavesdropping attacks. HTTPS is designed to withstand such attacks, and creates a secured channel for a communication.
- **Ability to set up Cloud-enabled Management**
  After you configure your environment to use HTTPS mode, you can start setting up Cloud-enabled Management. Cloud-enabled Management lets you manage endpoints over the Internet even if the client computers are outside of the corporate environment and cannot access the management servers directly.

Where and when do you set up HTTPS in an ITMS environment?

You have to configure the following components in your ITMS environment to enable access using HTTPS:

- Notification Server
- Site servers (package server, task server, and so on)
- Symantec Management Agent
- Client computers

You can set up your ITMS environment on HTTPS either during ITMS installation, or after the ITMS installation is completed.
For more information, see How to configure HTTPS during ITMS installation and How to configure HTTPS after ITMS installation is completed topics that are included in this document.

What are the SMP requirements for an SSL certificate?

For a Symantec Management Platform (SMP) to use an SSL certificate, the certificate has to fulfill the following requirements:

Table 1: Symantec Management Platform requirements for SSL certificates

Element	Description
Digital signature	The certificate has a valid digital signature.
Trust	The certificate is issued by Certification Authority that is trusted by the Notification Server computer.
Validity	The certificate is valid at least for 30 days from the import date.
Enhanced Key Usage	The Enhanced Key Usage value of the certificate is Server Authentication OID (1.3.6.1.5.5.7.3.1).
Subject name or subject alternate name	Subject or subject alternate name matches the Notification Server computer Fully Qualified Domain Name.
Hashing algorithm	The certificate uses one of the following hashing algorithms: • SHA1 • SHA256 • SHA384 • SHA512
Asymmetric algorithm	The certificate uses the RSA asymmetric algorithm.
File format	.pfx

You can view the SSL certificates that are associated with a server in IIS. You can view the names of certificates and the fully qualified domain names (FQDNs) of hosts to which certificates have been issued. You can also view the FQDNs of the servers that issued the certificates.

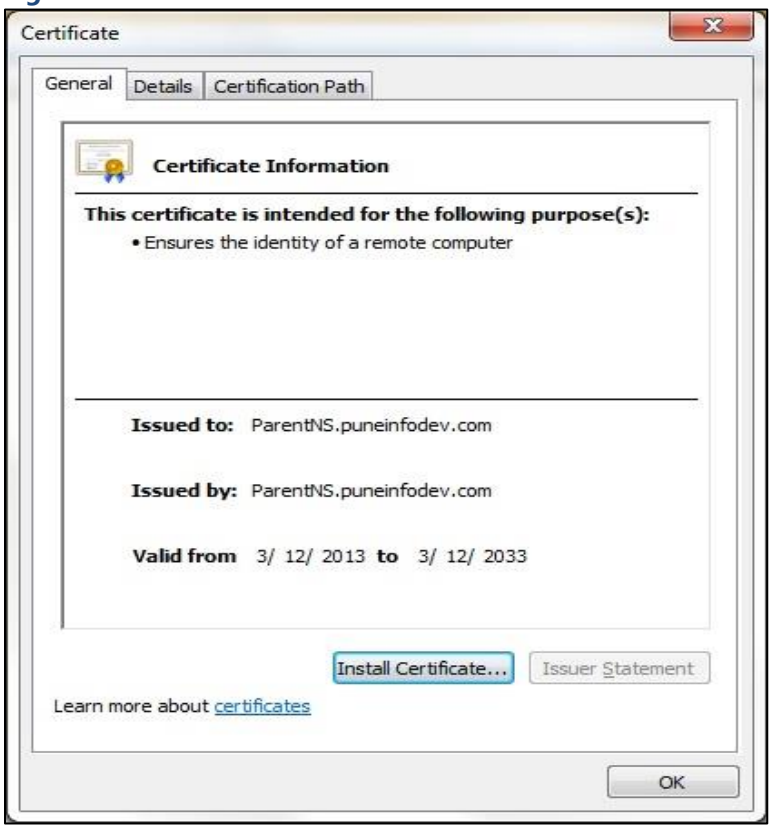
For more information, see the Creating or importing an SSL certificate topic in the ITMS 7.5 Cloud SymHelp.

How to view the SSL certificate details?

You can view the SSL certificates that are associated with a server in IIS. You can view the names of certificates and the fully qualified domain names (FQDNs) of hosts to which certificates have been issued. You can also view the FQDNs of the servers that issued the certificates.

For more information on how to view the SSL certificate on a computer, see the Viewing an SSL certificate topic in the ITMS 7.5 Cloud SymHelp.

Figure 1: Details of an SSL certificate



What are the differences between a self-signed SSL certificate, and a commercial SSL certificate?

The ITMS environment supports both self-signed and commercial SSL certificates, either of which can be used for configuring HTTPS.

A SSL certificate is issued by a certification authority, or certificate authority (CA). Following are a few types of certification authorities:

- Commercial certificate authorities, who charge for their services.
- Certificate authorities owned by institutions and governments for their own use.
- Self-signed and community-driven certificate authorities, which are free of charge.

Table 2: Differences between commercial certificate and self-signed certificate

Commercial certificate	Self-signed certificate
Provided by third-party certification authorities who charge a fee for their services.	Provided by creating locally self-signed certificates, and is community driven and obtained for free of charge.
Certificate is obtained by creating a private key on a secure computer, generating a certificate signing request, and then sending the certificate to the certification authority (CA). After receiving your certificate signing request, the CA verifies the identity, and then generates the public key and makes the key available to you.	Certificate is signed with its own private key.
Require both parties to trust the certification authorities.	If the parties know each other, trust each other to protect their private keys, and can confirm transfer public keys then self-signed certificates may decrease overall risk.
A compromised certificate can be revoked, which prevents its further use.	A compromised certificate cannot be revoked which may allow an attacker who has already gained access to monitor and inject data into a connection to hack an identity if a private key has been compromised.

How to configure HTTPS during ITMS installation?

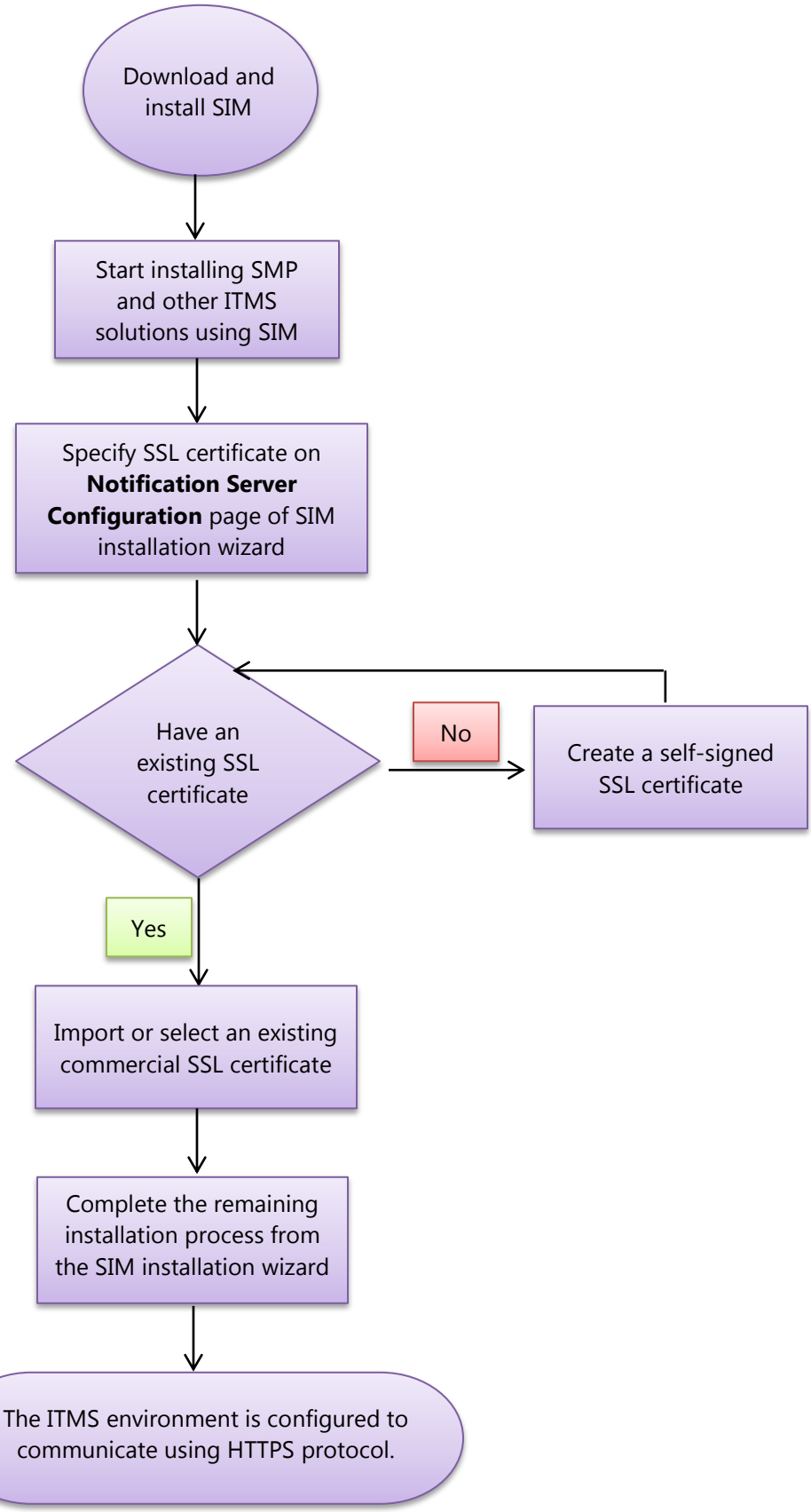
Notification Server is automatically configured to use HTTPS if you select the **Require HTTPS to access the Management Platform** check box on the **Notification Server Configuration** page, in Symantec Installation Manager, during the installation of IT Management Suite.

When you roll out Symantec Management Agents from a Notification Server that uses HTTPS, the Symantec Management Agents are also automatically configured to use HTTPS.

Therefore, when you configure HTTPS during ITMS installation, you do not need to manually configure the ITMS components (such as Notification Server, Symantec Management Agent, site servers, and client computers) to use HTTPS.

Figure 2: Configuring HTTPS during ITMS installation

Note:
For more information, see the following topic:
Installing Symantec Management Platform and IT Management Suite



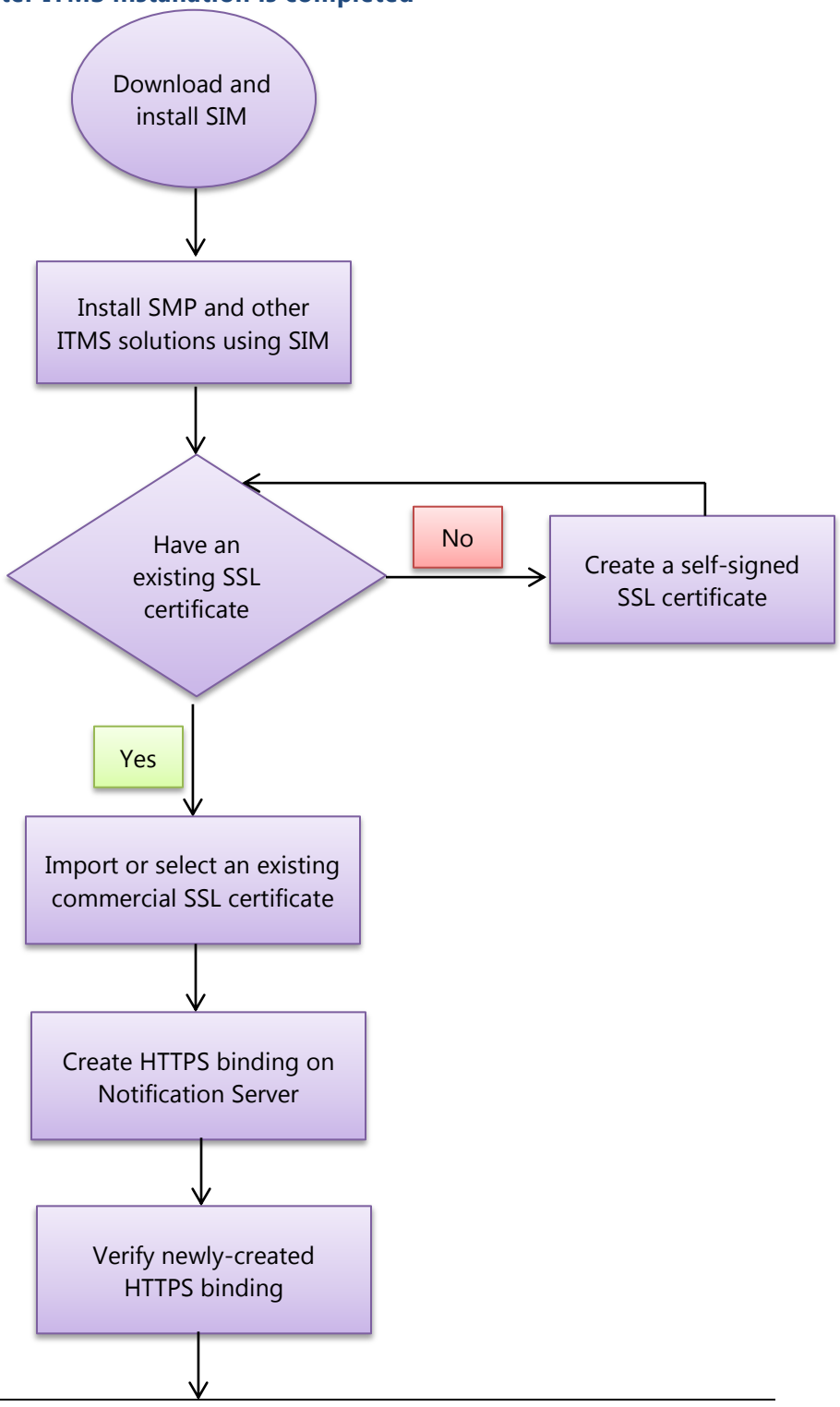
How to configure HTTPS after ITMS installation is completed?

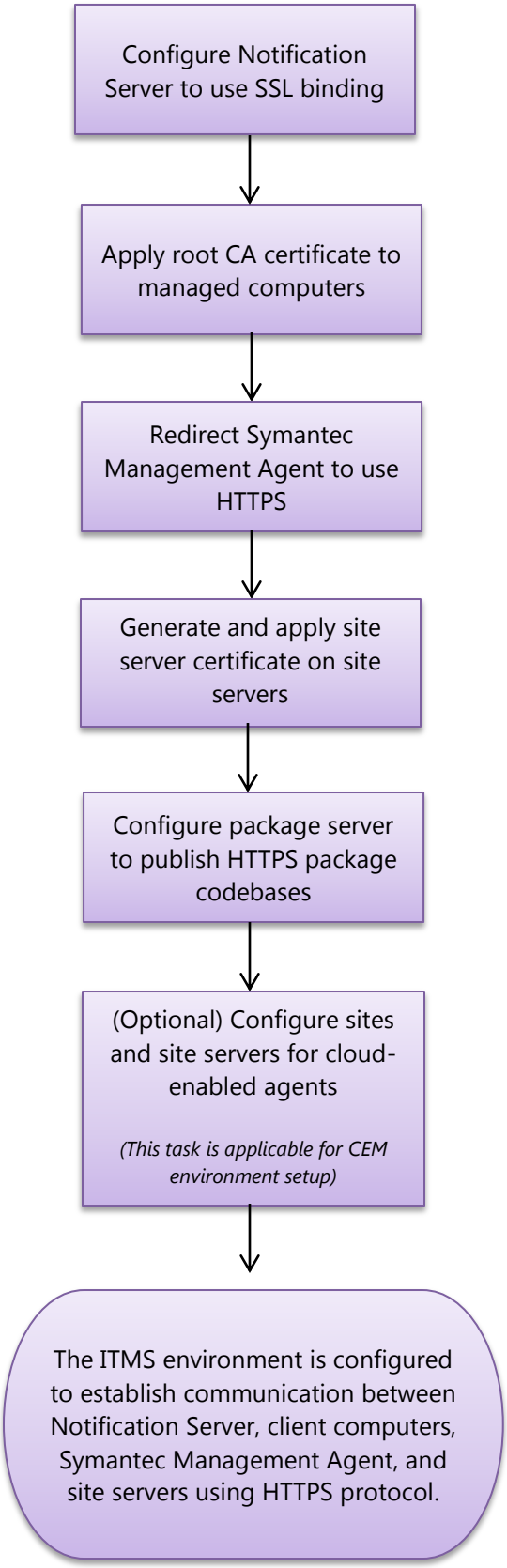
When you have not configured HTTPS during ITMS installation, you can configure the ITMS components to use HTTPS communication protocol after the installation is completed.

In such case, you must manually configure the ITMS components (such as Notification Server, site servers, Symantec Management Agent, and the client computers) to use HTTPS.

Figure 3: Configuring HTTPS after ITMS installation is completed

Note:
Click the individual item to view the associated help content.




Configure Notification Server to use SSL binding
Apply root CA certificate to managed computers
Redirect Symantec Management Agent to use HTTPS
Generate and apply site server certificate on site servers
Configure package server to publish HTTPS package codebases
(Optional) Configure sites and site servers for cloud-enabled agents
(This task is applicable for CEM environment setup)
The ITMS environment is configured to establish communication between Notification Server, client computers, Symantec Management Agent, and site servers using HTTPS protocol.

Where to get more information

Use the following documentation resources to learn about IT Management Suite 7.5:

Table 3: ITMS 7.5 documentation references

Document	Description	Location
ITMS 7.5 Cloud SymHelp	All available ITMS 7.5 and solution guides are accessible from this Symantec Help Center that is launched on cloud.	http://symhelp04.elasticbeanstalk.com/CS?locale=EN_US&vid=v90719369_v93032876&ProdId=SYMHELPHOME
Cloud enabled Management Whitepaper	Contains information about implementing cloud enabled management in the ITMS environment.	http://www.symantec.com/docs/DOC7049
ITMS 7.5 deliverables KB article	Contains URLs to all ITMS 7.5 suites and solutions documentation.	http://www.symantec.com/docs/DOC5131
ITMS 7.5 Planning for Implementation Guide	Contains information about the planning requirements for setting up the IT Management Suite environment	http://www.symantec.com/docs/DOC5670
ITMS 7.5 Installation and Upgrade Guide	Contains the installation, upgrade, and configuration information for ITMS 7.5 suites and solutions.	http://www.symantec.com/docs/DOC5697