

Configure FNMS Beacons and Agents to use Certificate Authentication

Author: Helgi Sigurdsson
Created: 26th May 2021

Contents

Document History	2
Introduction	2
Intended audience.....	3
High-level Design	3
Purpose and Design.....	3
Setup and configuration	3
Prerequisites.....	4
Certificate Deployment	4
Configure IIS	6

Document History

Date	Revision	Description	Author(s)
26. May 2021	1.0	Initial revision	Helgi Sigurdsson

Introduction

This document specifies the requirements, design and implementation of secure communication between the FlexNet Inventory Agent and an Inventory Beacon.

This document is intended be treated as a living document for the lifetime of the FlexNet Manager Suite (FNMS) implementation. It should be updated and maintained to be an accurate record of the current design and implementation of this configuration as changes are made.

Intended audience

This document is intended to be used by the following people:

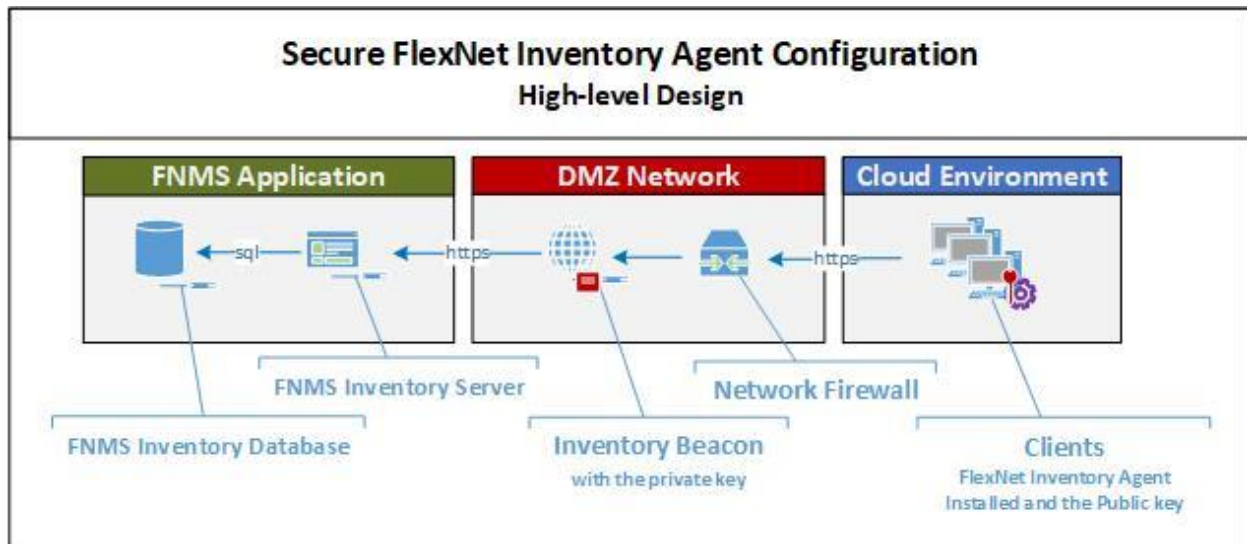
- Systems engineers responsible for implementing and maintaining the FlexNet Manager Suite (FNMS)
- Flexera Software consultants working on the system.

It is assumed that readers of this document have good knowledge in FlexNet Manager Suite (FNMS) administration to understand basic concepts and aspects of the FlexNet Manager Suite (FNMS) product solution.

High-level Design

Purpose and Design

The purpose of this solution is to ensure that only authorized inventory devices can access the inventory beacon. This setup is based on standard Server and Client authentication certificates. The picture below shows the high-level design of this configuration:



This solution can only be implemented on Inventory Beacon using IIS and with Client and Server Authentication certificates. The Private key of the certificate is stored on the Server and in the public key is stored in the Personal Certificate store of the Client computer.

Setup and configuration

The setup of this solution requires minimal changes for the web sites that are used by the inventory agent. It also involves deploying the client certificate with the public key as part of the Inventory Agent installation.

Prerequisites

This solution requires:

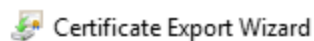
- FlexNet Inventory beacon with Internet Information Services
- Client and Server Authentication certificate with the private key
- The certificate issuer needs to be in the Trusted Root Certification Authorities store on both the beacon and all the clients that are communicating with the beacon.

It is recommended to use certificate from known Certificate issuer, but Self-signed certificates can also be used.

Certificate Deployment

The high-level configuration process is as follows:

1. Create and complete a Client and Server Authentication certificate request
2. Import the Certificate into the Personal store for the computer account on the Inventory Beacon
3. Export the Certificate from the Beacon and make sure the Private Key is included in the export:



Export Private Key

You can choose to export the private key with the certificate.


Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

Yes, export the private key

No, do not export the private key

4. Mark the **Delete the Private Key if the export is Successful** check box

•  Certificate Export Wizard


Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
 - Include all certificates in the certification path if possible
 - Delete the private key if the export is successful
 - Export all extended properties
 - Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

5. Secure the certificate with a password.

 Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

Group or user names (recommended)

Add

Remove

Password:

Confirm password:

Encryption: TripleDES-SHA1 ▾

Next

Cancel

- Specify the name of the export file.



File to Export

Specify the name of the file you want to export

File name:

C:\Cert\BeaconCert.pfx

Browse...

- Deploy the exported certificate to all the clients that are allowed to communicate with the beacon

Configure IIS

The Certificate created/imported on the Inventory Beacon must be specified in the Default Web Site Bindings as shown below:

Edit Site Binding ? X

Type: **https** IP address: **All Unassigned** Port: **443**

Host name:

Require Server Name Indication

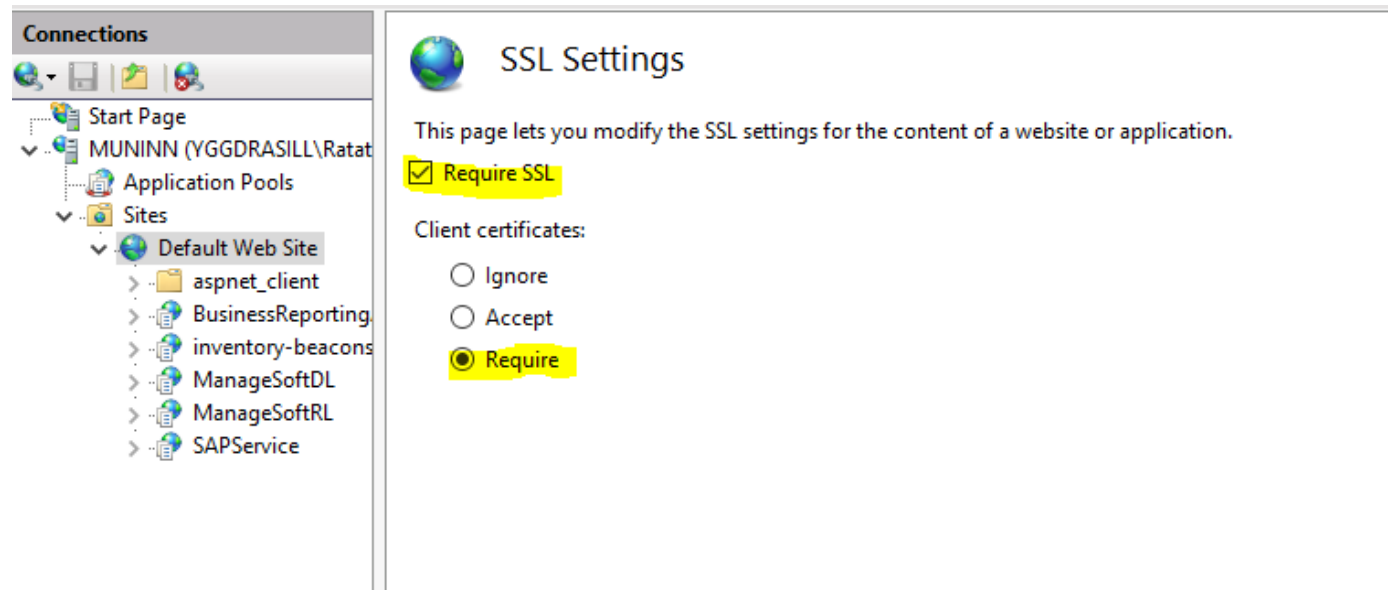
Disable HTTP/2

Disable OCSP Stapling

SSL certificate: **SSLBeacon.Corp.net** Select... View...

OK Cancel

The last step is to configure the SSL settings for the Default Web Site SSL to require Certificate as shown below:



Make sure that the SSL Settings have been applied to all Child Sites.

About Flexera

Flexera helps executives succeed at what once seemed impossible: getting clarity into, and full control of, their company's technology "black hole." From on-premises to the cloud, Flexera helps business leaders turn IT insight into action. With a portfolio of integrated solutions that deliver unparalleled technology insights, spend optimization and agility, Flexera helps enterprises optimize their technology footprint and realize IT's full potential to accelerate their business. For over 30 years, our 1300+ team members worldwide have been passionate about helping our more than 50,000 customers fuel business success. To learn more, visit flexera.com