Authentication on iOS Deployment Guide

Nymi Connected Worker Platform
v1.0
2023-05-23

Contents

3 - Preface

Nymi™ provides periodic revisions to the Nymi Connected Worker Platform. Therefore, some functionality that is described in this document might not apply to all currently supported Nymi products. The product release notes provide the most up to date information.

Purpose

This document is part of the Connected Worker Platform (CWP) documentation suite.

CWP connects people with technology through safe, simple, and secure solutions. CWP supports numerous use cases and digital systems, and combines point solutions into a single offering. CWP simplifies the connection of workers to the digital space that is found in modern organizations.

CWP contains three elements: device hardware, infrastructure and solution. The device hardware refers to the Nymi Band and firmware. Infrastructure consists of software, such as SDK, Nymi Enterprise Server, Nymi Agent and Nymi Band Application and the CWP Backend, which runs on terminals and servers.

Audience

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	May 23, 2023	First release of this document for the CWP 1.8.0 release.

Related documentation

- **Nymi Connected Worker Platform—Overview Guide**

  This document provides overview information about the Connected Worker Platform (CWP) solution, such as component overview, deployment options, and supporting documentation information.

- **Nymi Connected Worker Platform—Administration Guide**

  This document provides information about how to use the NES Administrator Console to manage the Connected Worker Platform (CWP) system. This document describes how to set up, use and manage the Nymi Band™, and how to use the Nymi Band Application. This

document also provides instructions on deploying the Nymi Band Application and Nymi Runtime components.

- **Nymi SDK for C Developer's Guide**

  This document provides information about how to develop Nymi-enabled Applications by using the Nymi API(NAPI).

- **Nymi SDK for WebSocket Developer's Guide**

  This document provides information about how to understand and develop Nymi-enabled Applications (NEA) by utilizing the functionality of the Nymi SDK, over a WebSocket connection that is managed by a web-based or other application. Separate guides are provided for Windows and iOS application development.

- **Connected Worker Platform with Evidian Installation and Configuration Guide**

  The Nymi Connected Worker Platform with Evidian Guides provides information about installing the Evidian components and configuration options based on your deployment. Separate guides are provided for Wearable, RFID-only, and mixed Wearable and RFID-only deployments.

- **Nymi Connected Worker Platform—Troubleshooting Guide**

  This document provides information about how to troubleshoot issues and the error messages that you might experience with the NES Administrator Console, the Nymi Enterprise Server deployment, the Nymi Band, and the Nymi Band Application.

- **Nymi Connected Worker Platform with Evidian Troubleshooting Guide**

  This document provides overview information about how to troubleshoot issues that you might experience when using the Nymi solution with Evidian.

- **Nymi Connected Worker Platform—FIDO2 Deployment Guide**

  The Nymi Connected Worker Platform—FIDO2 Deployment Guide provides information about how to configure Connected Worker Platform and FIDO2 components to allow authenticated users to use the Nymi Band to perform authentication operations.

- **Connected Worker Platform with POMSnet Installation and Configuration Guide**

  The Nymi Connected Worker Platform—POMSnet Installation and Configuration Guides provides information about how to configure the Connected Worker Platform and POMSnet components to allow authenticated users to use the Nymi Band to perform authentication operations in POMSnet.

- **Nymi Band Regulatory Guide**

  This guide provides regulatory information for the Generation 3 (GEN3) Nymi Band.

- **Third-party Licenses**

  The Nymi Connected Worker Platform—Third Party Licenses Document contains information about open source applications that are used in Nymi product offerings.

- **Connected Worker Platform Release Notes**

  This document provides supplemental information about the Connected Worker Platform, including new features, limitations, and known issues with the Connected Worker Platform components.

How to get product help

If the Nymi software or hardware does not function as described in this document, you can submit a support ticket to Nymi, or email support@nymi.com

How to provide documentation feedback

Feedback helps Nymi to improve the accuracy, organization, and overall quality of the documentation suite. You can submit feedback by using support@nymi.com

4 - Deployment Overview

You can deploy the Nymi solution in two different configurations, where you install the Nymi Agent software on each user terminal or you deploy a single instance of the Nymi Agent in a centralized location and configure endpoints to use the centralized Nymi Agent.

Review the following information to decide which configuration to deploy.

Decentralized Nymi Agent	If your environment meets all of the following configuration scenarios, you can deploy a decentralized Nymi Agent solution.
	• User terminals are thick Windows clients only. • User Terminals perform Nymi Band taps in native MES application.
Centralized Nymi Agent	If your environment meets any of the following configuration scenarios, you must deploy a centralized Nymi Agent solution.
	• User Terminals are iOS clients. • User Terminals include thin clients, such as HP ThinPro, RDP, and Citrix. • User Terminals perform Nymi Band taps in web-based MES applications, such as POMSnet.

Note: You can deploy a configuration that uses a mixture of user terminals with centralized or decentralized Nymi Agent but for simplicity Nymi recommends that it you choose one and configure your all your user terminals to use a centralized or decentralized Nymi Agent.

4.1 - Components in a iOS Only Environment

The Connected Worker Platform(CWP) enables users to use Nymi Bands and administrators to manage Nymi Bands and CWP components in an enterprise setting.

CWP is comprised of Nymi-specific components and enterprise components, as shown in the following figure.
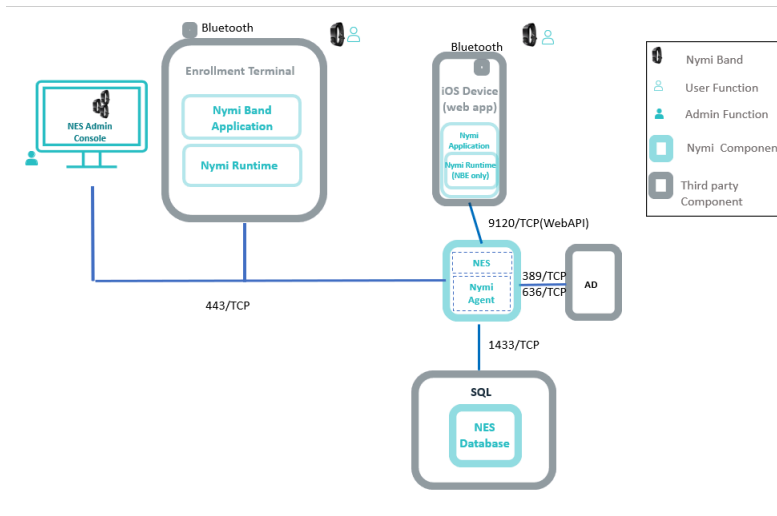
Figure 1: CWP components and firewall connection ports

The Connected Worker Platform consists of the following components.

Table 2: Connected Worker Platform Components

Component	Description
Enrollment Terminal	Windows 10 endpoint that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal and is used to enroll a new user and link them to their Nymi Band. The Nymi Band Application requires the Nymi Runtime application, which the Nymi Band Application automatically installs. The Nymi Band Application communicates with the Nymi Band through the Nymi-supplied Bluetooth adapter, which you plug into a USB port on the enrollment terminal.
Nymi Band	A wearable device that is activated by the assigned user's biometrics. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled. See the Nymi Band section in this guide for more information.

Component	Description
Nymi-enabled Application	Developers can create corporate applications that integrate with Connected Worker Platform by using the Nymi WebAPI component of the Nymi API. These applications are called Nymi-enabled Applications (NEAs) and include Manufacturing Execution Systems (MES), Single Sign-On (SSO), and Human Machine Interface (HMI) applications. An NEA communicates with the Nymi Runtime components.
iOS Device	An iPad endpoint that users use to: • Perform authentication tasks in a web-based Nymi-enabled Application(NEA). • Perform authentication tasks in a native iOS NEA.
Nymi Application	Required when the iOS device connects to a web-based NEA to perform authentication tasks. A Nymi-supplied native iOS application that: • Embeds the Nymi Bluetooth Endpoint application, which provides an interface between the native Bluetooth Adapter (BLE) and the Nymi Agent. • Detects an intent to perform an authentication task with a Nymi Band (a tap) and passes the request to the NEA.

Component	Description
Nymi Enterprise Server (NES)	• A management server and collection of services that provides the NES Administrator Console and coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates. Includes the following services: • Enrollment Service (ES)—Authenticates, validates, and authorizes certificate requests from requesters, such as the Nymi Band Application and NEAs. • Directory and Policy Services (DPS)—Maintains the NES database, which contains a list of Active Directory (AD) users and the Nymi Bands that are associated with each user. Provides IIS web services, which allows the NES Administrator Console access to the NES database. • Authentication Service (AS)—Provides authentication and authorization support for domain users and computers. AS uses adapters to interface with external directory and database systems, such as an AD adapter to interface with Active Directory.
SQL Server	Database that contains table that store information about NES configuration and Nymi Bands. For Proof of Concept (POC) and pre-production environments, you can use the Nymi-provided SQL Server Express software. For production environments Nymi recommends that you use SQL server.
Domain Controller (DC)	Windows server with Active Directory.

Component	Description
Centralized Nymi Agent	Required for iOS devices. Provides BLE management, manages operations and message routing. Facilitates communication between NEAs and the Nymi Band, and maintains knowledge of the Nymi Band presence and authenticated states. The Nymi Agent is installed in a central location on a single machine or a cluster of two or more machines that is accessible to all user terminals, for example on the NES server. To enable Nymi WebAPI communications between the Nymi Agent and the Nymi Bluetooth Endpoint, you must configure a *nymi_agent.toml* file.
	For web-based NEAs that are accessed by an iOS device, the webpage or NEA defines the Nymi Agent host and communication port number. The *Nymi SDK for WebSocket Developer's Guide* provides more information.

Use Case and Workflow

A user with an authenticated Nymi Band can perform an action that requires an authentication task, such as an e-signature in a web-based Nymi-enabled Application(NEA)

A typical worflow for a Nymi Band user is as follows:

- Nymi Band user authenticates to their Nymi Band.
- Nymi Band user connects to a web-based NEA on their iOS device and performs an activity that requires an e-signature.
- NEA launches the Nymi Application.
- Nymi Application appears on the iOS device screen and prompts the user to perform a Nymi Band tap to complete the authentication task.
- User taps their Nymi Band on the bluetooth adapter on the iOS device.
- Nymi Application communicates with the Nymi Band through the integrated bluetooth adapter on the iOS device.
- Nymi Application communicates with the web-based NEA to complete the authentication task after the user successfully completes the Nymi Band tap.

4.2 - Deployment of the Nymi WebAPI

You can deploy the Nymi WebAPI in a centralized or decentralized Nymi Agent configuration.Deploy the Nymi WebAPI in a centralized Nymi Agent configuration

In a decentralized Nymi Agent configuration, you deploy Nymi Agentand Nymi Bluetooth Endpoint components on each workstation to access a locally installedNymi-enabled Application(NEA).

In a centralized Nymi Agent configuration, for example, when you use the Nymi Band with Citrix and RDP published applications or desktops, you install:

- Nymi Agent component on a server that multiple workstations can access, such as the Nymi Enterprise Server(NES) server
- Nymi Bluetooth Endpoint component on each workstation.

Note: For more information about how to deploy a centralizedNymi Agent see the Nymi Connected Worker Platform—Deployment Guide.

The Nymi Bluetooth Endpoint and NEA must know the identity of the workstation to which the application wants to connect. By default, this identity is the IP address of the workstation. When you deploy Nymi Agent locally on the client workstation, both components use the loopback address, so they will connect automatically. When you deploy a centralized Nymi Agent, the Nymi Agent subscribes the Bluetooth Endpoint, the Nymi DLL, and WebSocket connections to the Nymi WebAPI by using the source IP of the connection. Therefore, if the Bluetooth Endpoint and application that is using the Nymi WebAPI are on the same host the application will work on connection.

For deployments in an RDP/Citrix environment or when the MES application (NEA) resides on a different host (such as a web or application server), the The IP address of the client that runs the NEA is different from the IP address of the workstation. Therefore, ensure that the NEA can determine the IP address of the client workstation that runs the Nymi Bluetooth Endpoint. You can determine the IP address by using the source IP address of the client requests.

- In remote desktop sessions, the IP address is usually available through Windows Terminal Services APIs.
- If you are not using RDP or Citrix, the IP address is usually available through vendor-specific environments or APIs.
- For remote applications, such as web-based application, you can determine the IP address by using the source IP address of the client requests.

When the application determines the IP address of the client workstation, the application must use the **subscribe** operation to connect to the correct Nymi Bluetooth Endpoint. Keep in mind that multiple IP addresses on the user workstation or NAT between components can interfere with determining client IP addresses and should be taken into consideration during deployment of an application.

If users might move between two or more client workstationsiOS devices, they must terminate their session before switching to another workstation, or the application must take this into account and start a new **subscribe** operation after reconnection.

4.3 - Nymi WebAPI Configuration Overview

Review the following requirements for the Nymi WebAPI and Nymi Agent components:

- Provide access to a distinct port for each component, port numbers are described later in this document.
- Configure transport layer security: on the server or by offloading.
- Ensure that both components have connectivity to NES.
- Ensure that there is no Network Address Translation (NAT) between the Nymi WebAPI of the Nymi Agent and the user terminals.
- When you use a centralized Nymi Agent on the same server as NES, ensure that each component can co-locate with the NES (ensure that you use distinct TCP ports).

5 - Connected Worker Platform Requirements

Review this section for information about the requirements for the Connected Worker Platform(CWP) components .

5.1 - Hardware and Software Requirements

The following sections provide more information about the hardware and software requirements for Connected Worker Platform components.

5.1.1 - NES Requirements

The following sections define the hardware and software requirements to consider before you deploy NES.

Hardware Requirements

The NES hardware requirements differ based on the nature of user operations, load and other software that is deployed on the same server. The following section lists the recommendations for minimum hardware requirements.

- 1-5000 users:

  - 4 Core CPU
  - 8GB RAM
  - 20GB free disk space
- 5000-10000 users:

  - 4 Core CPU
  - 16GB RAM
  - 40GB free disk space

Software Requirements

NES has the following software requirements.

- Microsoft Windows Server 2016 or 2019

  Note: Ensure that the host is not a Domain Controller (DC).

- Microsoft IIS
- Microsoft .NET Framework 4.8

    Note: The NES installation package includes Microsoft .NET Framework 4.8, and installs the software if required.

5.1.2 - User Terminal Requirements

User terminals are endpoints that can perform different functions in the environment, including enrollment, MES authentication tasks, and desktop locking and unlocking with Nymi Lock Control. User terminals include thick clients and thin clients.

Hardware and Software Requirements

All thick client user terminals require connectivity to the server on which you install Nymi Enterprise Server(NES). The following table summarizes the supported operating systems and the hardware device requirements for each user terminal use case.

Note: You can configure and use a user terminal for multiple use cases.

Use Cases	Supported Operating System/ Browser	Hardware
Enrollment	- Windows 10, 64-bit, minimum build version 1607 - Windows 7, 64-bit **Note:** Nymi recommends that you use 125% scaling and 1920 x 1080 screen resolution for the terminal hosting the Nymi Band Application	4GB RAM 5GB free disk space 2 core CPU (recommended) 1 USB 2.0 port - Nymi-supplied bluetooth adapter
Authentication tasks with a Nymi Band in a web-based Nymi-enabled Application (iOS device)	- iOS version 13 and later - Safari 15.7	Integrated Bluetooth adapter

5.2 - Networking Requirements

Nymi recommends that you deploy all Connected Worker Platform components for high availability but gives you the option to deploy the NES Nymi Agent components in a standalone configuration.

5.2.1 - Domain Name Service Requirements for Non-Clustered Deployment

The Connected Worker Platform(CWP) solution uses fully-qualified domain names (FQDNs) that point to CWP infrastructure services that are accessed by CWP applications, such as Nymi Band Application or by administrators through a browser (Nymi Band Management Console).

Non-Clustered CWP Deployment

In a non-clustered CWP deployment, you must assign FQDNs to the following components.

Note: This guide uses *company.com* as an example domain name and *cwp.company.com* as an example subdomain name.

Record each FQDN value in *Appendix—Recording the CWP Component FQDNs.*

Table 3: FQDN Requirements

Component	FQDN Example
Nymi Enterprise Server(NES)	nes.cwp.company.com
Centralized Nymi Agent	nymiagent.cwp.company.com

5.2.2 - Firewall Port Requirements

The Nymi Solution uses connection ports to facilitate bidirectional communications between components.

Connection Port Requirements

The following table provides a summary of the connection port requirements for the Nymi Solution and FQDNs. Ensure that you replace the sample FQDNs with the actual FQDNs for your virtual servers. For each row that contains load balancer port information, you must configure virtual server on a load balancer to distribute traffic to the destinations. The load balancer must accept incoming traffic on the load balancer port.

Note: Your firewall and load balancer might require configuration changes to allow the specific protocol that is specified in the Protocol column of the table. Refer to your firewall or load balancer documentation for more information.

Record the virtual server FQDN and port for each component in *Appendix—Record the CWP Variables*.

Table 4: Connection Port Requirements

Purpose	Protocol	Source	Virtual Server FQDN & Port	Destination and Port
SQL Access	MS SQL Proprietary	NES	n/a	SQL Server: 1433/TCP
LDAP Access-Active Directory(AD)	LDAP/LDAPS	NES	n/a	AD Server: 389/TCP (For LDAP configurations) 636/TCP (For LDAPS configurations)
NES Communications	HTTPS	Machine that accesses NES Administrator Console All User Terminals (thick). RDP/Citrix server that run NEAsCentralized Nymi Agent	nes.cwp. company.com: 443/TCP	NES: 443/TCP
Internal Websocket Communications to Remote Nymi Agent from Nymi Bluetooth Endpoints and Nymi-enabled Applications(NEAs)	Websocket	All User Terminals (thick and thin) RDP/Citrix Servers that run NEAs	nymiagent.cwp. company.com 9120/TCP	nymiagent-0.cwp. company.com nymiagent-1.cwp. company.com: 9120/TCP

5.3 - Connected Worker Platform Certificate Requirements

The Connected Worker Platform relies on several certificates to ensure secure communications.

The Connected Worker Platform(CWP) solution uses two types of certificates:

- TLS Certificates—Required to support secure communications over TLS between CWP components. These certificates serve the same purpose as typical TLS certificate that

support secure communications within your enterprise network, for example for web and email traffic. It is your responsibility to obtain the TLS certificates for your CWP deployment.

- Root CA Certificate(TLS): Certificate for the root-of-trust for the public key infrastructure (PKI) that issues the TLS certificate. The steps to import the Root CA Certificate (TLS) are required only if it is not already in the Trusted Root Certification Authority store of the machines, for example, if an untrusted private root CA is used to issue the TLS certificate. The steps are not required if a trusted public root CA or a trusted private root CA (for example, an enterprise root CA) is used to issue the TLS certificate.
- Nymi-specific Certificates—Required to support secure communications between Nymi Bands and CWP services. These certificates are provided by Nymi in a PFX file, which includes the following content:

  - Nymi Infrastructure Root CA certificate
  - NES L1 certificate
  - NES L2 certificate and associated private key

  Nymi-provided certificates are deployed on NES
- For more information about the Nymi-specific certificates, refer to the *Connected Worker Platform Security Whitepaper*.

The following figure provides a high-level overview of the certificates that the Connected Worker Platform requires.

Figure 2: Certificates required in a Connected Worker Platform environment

5.3.1 - TLS Certificate Requirements

Ensure that you use a trusted Certificate Authority(CA) to issue the TLS certificate for NES. The TLS certificate must contain the appropriate fully qualified domain name(FQDN) for the subject alternative name(SAN).

- For a standalone NES deployment, ensure that the SAN contains the FQDN of the NES server.
- For a high availability NES deployment that uses a load balancer, include the FQDNs for the virtual server and all the physical servers.

Package the TLS certificate and CA certificate chain that the CA provides to you with the private key of the certificate into a PKCS#12 file. Record the password of the TLS certificate in a secure manner. You will be required to provide the password during deployment.

Record the expiration date of the TLS certificate in *Appendix—Certificate Expiration Dates*.

5.3.2 - Issuing TLS Certificates Using Untrusted Certificate Authorities

In some situations, it is not possible to issue the required TLS certificates by using a trusted Certificate Authority(CA).

An untrusted CA can be used subject to the following conditions:

- Use a single untrusted root CA to issue all TLS certificates.
- You must import the untrusted root CA certificate into each machine that communicates with the Connected Worker Platform services. The methods that you use to import the untrusted root CA certificate into each component is described later in this guide.

5.3.3 - NEA Certificates for Nymi WebAPI

An NEA and the Nymi Band establish trusted communication by using certificates. The first time that a user runs the NEA, the NEA retrieves a certificate from NES. The NEA certificate is stored in a keystore. Access to the keystore, by default, is enabled for all users.

By default, the keystore is in the *%APPDATA%\Roaming\Nymi/etc/pki/ca-trust/source/anchors* directory.

Alternative locations include:

- *C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Nymi* for the Local Service account.
- *C:\Windows\system32\config\systemprofile\AppData\Roaming\Nymi* for the LOCAL SYSTEM (64-bit binary) account.
- *C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Nymi* for the LOCAL SYSTEM (32-bit binary) account.

5.4 - Active Directory Requirements

The Connected Worker Platform(CWP) relies Windows Active Directory(AD) for user identity and authentication. Review the following sections for information about AD domain, AD groups, and service account requirements.

5.4.1 - Domain and Trust Requirements

Domain Requirements

Connected Worker Platform(CWP) supports environments that have users and administrators in a domain that differs from the domain in which the NES server resides, within the same forests or different forests.

Record the following configuration information about the Active Directory in *Appendix—Record the CWP Variables*. You require this information during the NES deployment process.

- Communication protocol that NES uses to connect to the Active Directory. For example, LDAP or LDAPs.
- Port number on which to contact the Active Directory. The default port number for LDAP is 389. The default port number for LDAPS is 636.

Trust Requirements

The domain in which NES resides must trust the user domain.

Note: For Nymi with Evidian deployments, you require a selective two-way trust. The Nymi Connected Worker Platform with Evidian Guides provide more information.

5.4.2 - Creating the Active Directory Group for NES

Perform the following actions to prepare the Domain Controller for the NES deployment.

About this task

Create an Active Directory group for users that act as an. NES Administrator. An NES Administrator is the person in the enterprise that manages the Connected Worker Platform for their workplace.

Procedure

1. Create a group that contains the users who will act as NES Administrator. For example, a group named `NES_admins`.

   When you create the group, in the **Group Type** section, select **Security**. The selection for the **Group Scope** depends on the configuration of the environment.

   - In a single domain environment, choose a group scope according to your IT policy.
   - In a multi-domain environment:

     - When you select **Universal**, you can add users and groups from any domain to the NES admins group.
     - When you select **Global**, you can only add users and groups that are local to the domain. If users in multiple domains require admin access to NES, you must create a global group in each domain with NES Administrator users, and add the NES Administrator users to this group.

2. Record the administrator group name and a list of user accounts that you added this group, in *Appendix—Record the CWP Variables*.

5.4.3 - Creating a Service Account for MS SQL Server Access

The Connected Worker Platform solution store information in a MS SQL Server. You can use an existing or new SQL server and you can use a SQL server that is local to the NES server or on a different machine.

Nymi recommends that you configure the SQL database to use Windows authentication mode, which requires you to define an NES service account. During the NES deployment, you will configure IIS to run the NES application under this service account.

Create a service account in Active Directory, that meets the following requirements:

- The user account is a domain user in the same domain as the SQL server.

- The password of the user account does not expire.

Record the account name and domain in *Appendix—Record the CWP Variables*, which specify the credentials during the NES deployment.

5.5 - Database Requirements

The Connected Worker Platform(CWP) solution can use a new or existing SQL server instance, which you can reside on the NES server or on another server in the environment.

Supported SQL Versions

CWP solution supports the following Microsoft SQL versions:

- SQL Server/SQL Server Express 2016
- SQL Server/SQL Server Express 2017
- SQL Server/SQL Server Express 2019

The NES installation package includes Microsoft SQL Server Express 2017; however, Nymi recommends that you use SQL Server in production environments.

Note: The CWP solutions uses TLS 1.2. If you use SQL Server / SQL Express 2016 or SQL Server / SQL Express 2017 you must apply a patch to provide TLS 1.2 support. Microsoft provides more information.

Configuration Requirements

Nymi recommends that you configure the SQL database to use Windows authentication mode and:

- Ensure that the account that starts the SQL Server has permissions to register an SPN in Active Directory Domain Services. Microsoft provides more information.
- Assign dbowner rights to the NES service account. *Creating the Service Account for SQL Server Access* provides more information about creating the service account.

5.5.1 - Creating the NES database

If you use an SQL server that is not on the same machine as NES, install the SQL Server software if required, and then create the NES database.

About this task
Perform the following steps on a machine that has SSMS installed and has access to the SQL Server.

Procedure

1. Open SSMS, and then login to the SQL Server.

2. Right-click the SQL instance, and the select **Properties**.

3. In the **Object Explorer**, select **Security**.

4. Select **SQL Server and Windows Authentication Mode**, and then click **OK**.

5. In the **Object Explorer** right-click Databases, and the select New Database.

6. In the `New Database` window, perform the following actions:

   a) In the **Name** field, type nes.

   b) Click the elipses (...) beside **Owner**, and then in the **Enter the object names to select** field, type the name of the service account.

   c) Click **Check names**.

   d) In the **Multiple Objects Found** field, select the service account name, and then click **OK**.

   e) On the `Select Database Owner` window, click **OK**.

   f) On the **New Database** window, click **OK**.

5.5.2 - Configuring SQL Database for Remote Access

Enable TCP/IP on the SQL instance to allow access to the FirmwareUpdate database.

About this task

Perform the following actions in the `SQL Server Configuration Manager` application.

Procedure

1. In the left navigation pane, expand `SQL Server Network Configuration`, and then select the appropriate Protocols for the SQL Server option.

2. In the right pane, select TCP/IP, and then right-click and select **Enabled**.

3. Double-click **TCP/IP**.

4. In the `TCP/IP Properties` window, select the **IP addresses** tab.

5. Navigate to the `IPALL` section, and then for the **TCP port** value, type 1433.

   The following figure provides an example of the port setting.
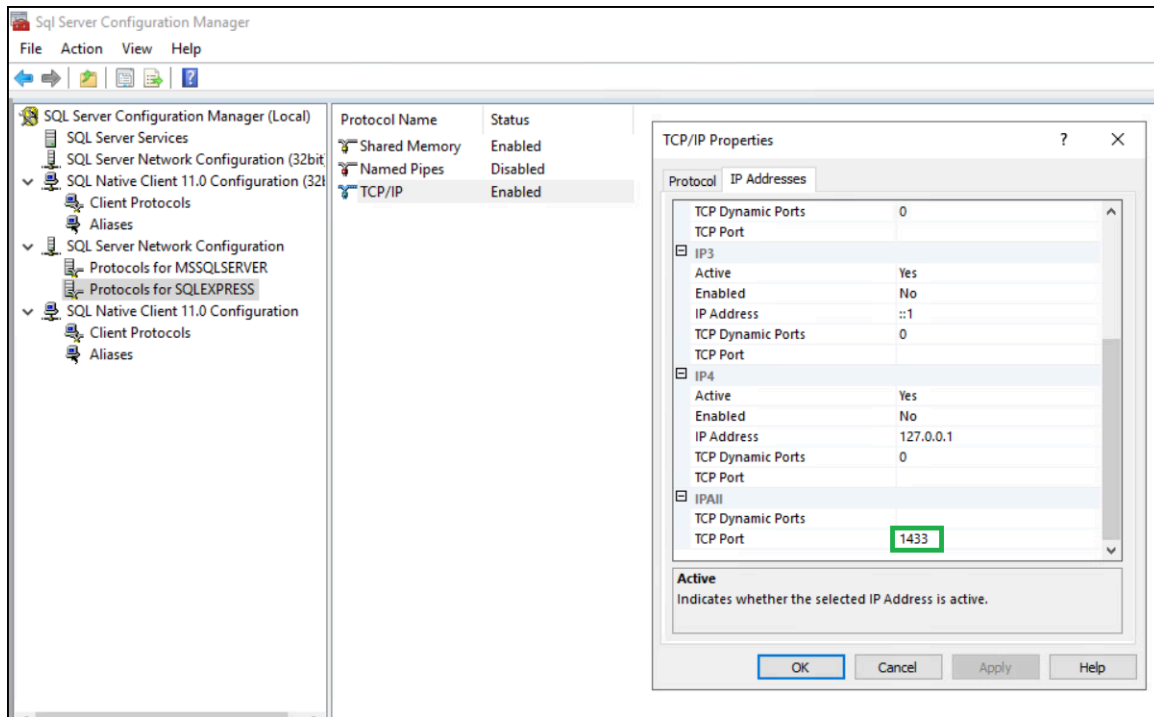
Figure 3: Configuring SQL Port

6. Click **OK**, and then click **Apply**.

7. On the prompt to restart the SQL services, click **OK**.

8. Restart SQL Server services.

9. For SQL Express only, perform the following steps.

   a) In the left navigation pane, select **SQL Services**.

   b) Right-click **SQL Server Browser** and select **Start**.

   The SQL Server Browser service state changes to **Start**, as shown in the following figure.
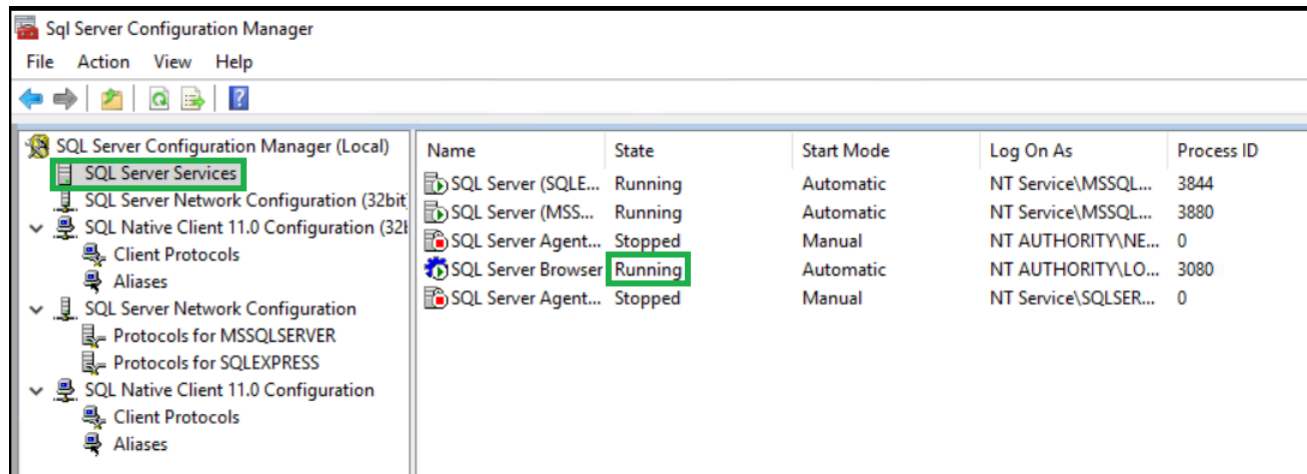
Figure 4: SQL Server Browser service

5.6 - CWP Package Requirements

5.6.1 - Obtaining the NES Software Package

Your Nymi Solution Consultant provides you with a package that installs NES.

Extract the contents of the NES software package into the *C:\nestemp* folder of the designated NES server. The package extracts the following files into the folders:

- *AccessControl*
- *AuthenticationService*
- *NEnrollment*
- *nes*
- *NesCmdInstall*
- *NesInstaller*
- *NesSystemInfo*
- *PreRequisites*

6 - Deploy NES

Deploy NES in a standalone or high availability configuration.

6.1 - Deploy NES in a Standalone Configuration

The following sections provide information about how to deploy a standalone NES.

6.1.1 - Install and Configure IIS

NES supports HTTP and HTTPS for communication between NES services. It is recommended to use HTTPS. To complete prerequisite activities for NES deployment, install Microsoft Internet Information Server (IIS) and Microsoft ASP.NET on the NES host, and then import the TLS server certificate into IIS for secure deployments (HTTPS).

6.1.1.1 - Installing IIS and ASP.NET

This section describes how to install IIS and ASP.NET on the NES host.

Procedure

1. Open the `Server Manager` application, and then click **Add roles and features**.
2. On the `Before You Begin` page, click **Next**.
3. On the `Select installation type` page, leave the default value **Role-based or feature-based installation**, and then click **Next**.
4. On the `Select destination server` page, leave the default selection **Select a server from the server pool**, select the host in the **Server Pool** list box, and then click **Next**.
5. On the `Select server roles` page, click **Web Server (IIS)**.
   The `Add features that are required for Web Server (IIS)` dialog box appears and provides a summary of tools that are required to install IIS.
6. On the `Add features that are required for Web Server (IIS)` dialog box, click **Add Features**.
7. On the `Select server roles` page, click **Next**.
8. On the `Select features` page, click **Next**.
9. On the `Web Server Role (IIS)` page, click **Next**.
10. On the `Select role services` page, expand **Web Server (IIS) > Web Server > Application Development**, and then perform the following actions: .

a) Select **Application Initialization**.

b) Select the latest available version of ASP.NET 4.x.

Note: NES supports ASP.NET 4.4 and later.

c) On the `Add features that are required for ASP.NET` dialog box, click **Add Features**, as shown in the following figure.
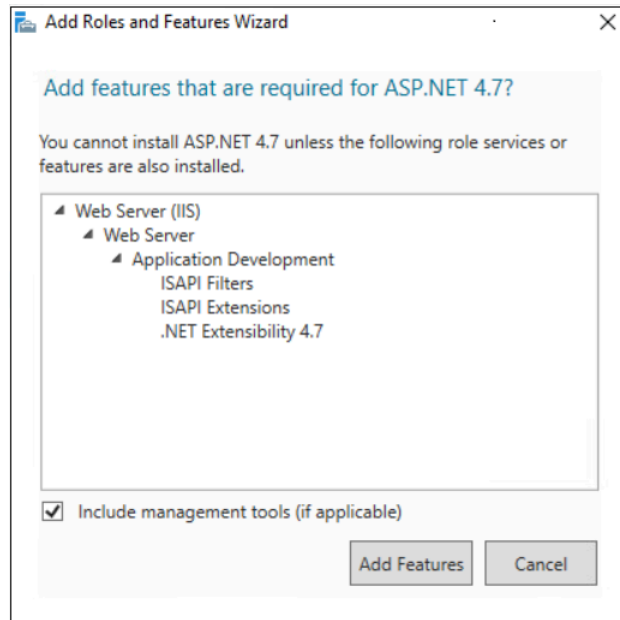
Figure 5: Add features that are required for ASP.NET

d) On the `Select role services` page, leave the other default options selected, and then click **Next**.

The following figure shows the `Select server roles` page.
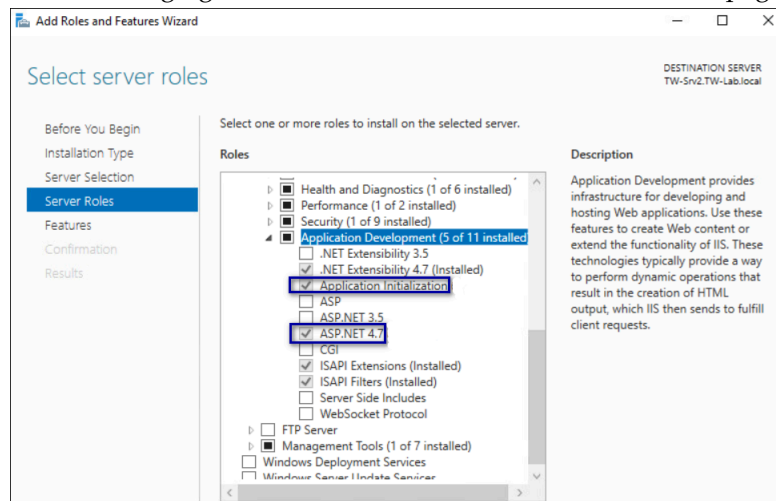
Figure 6: Select server roles page

11. On the `Select Features` page, click **Next**.

12. On the `Confirm installation selections` page, click **`Install`**.

The `Installation Progress` page appears and provides the status of the IIS installation, which takes several minutes. When the installation completes, click **`Close`**. Restart the host, if prompted.

6.1.1.2 - Importing the TLS server certificate

For HTTPS deployments, import the TLS server certificate obtained for the NES host. If the TLS server certificate is not signed by a Trusted Root CA, then you also need to import the Root CA certificate.

About this task

Note: The following procedure assumes that the TLS server certificate and the associated private key are packaged in the same file. Depending on how the private key for your certificate is generated, your procedure might differ. If you have already imported the certificate or you do not require step-by-step instruction, proceed to *Adding HTTPS site bindings*.

Perform the following steps in the `IIS Manager` to import the TLS server certificate and the associated private key.

Procedure

1. In the `Connections` navigation pane, click `Computer_Name`, and then in the `IIS` section, double-click **`Server Certificates`**.

Note: If you cannot find `Server Certificates`, click the **`Features View`** tab, which appears at the bottom of the window.
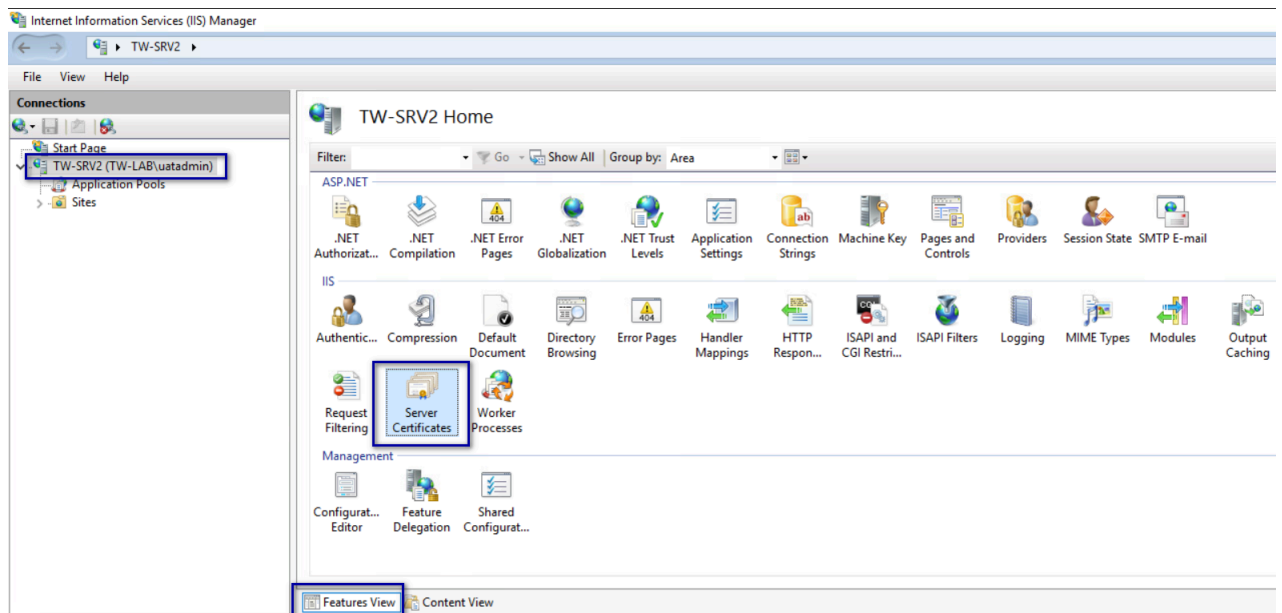
Figure 7: Server Certificates option

2. In the `Actions` navigation pane, on the right side of the window, click **`Import`**.

3. In the `Import Certificate` window perform the following actions:

    a) In the **`Certificate file (.pfx)`** field, click the ellipsis (…) button, change the extension list to *.*, browse to the location of the TLS certificate, select the certificate file, and then click **`Open`**.

    b) In the **`Password`** field, type the password that was used to encrypt the private key, and then click **`OK`**.

    c) In the **`Select Certificate Store`** list, select **`Web Hosting`**.

    The following figure provides an example of the `Import Certificates` window.
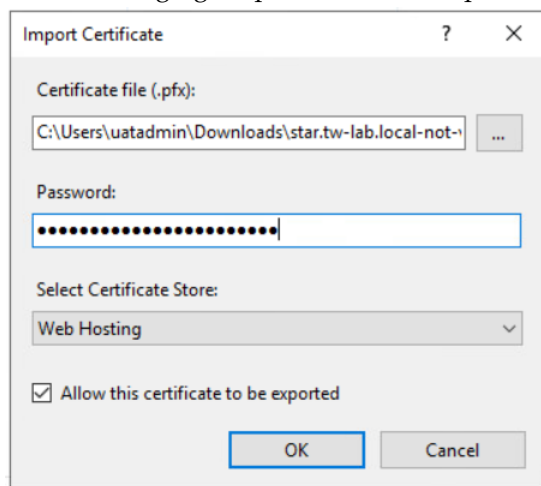
Figure 8: Server Certificates option

    d) Click **`OK`**.

4. Minimize IIS.

5. Perform the following steps using the `Certificate MMC` to import the Root CA certificate (if needed).

a) From the Window Start menu, type Manage Computer, and then select **Manage computer certificates**.

b) On the `User Account Control` dialog, click Yes.

c) Expand **Certificates - Local Computer > Trusted Root Certificate Authority**.

d) Right-click **Certificates**, and then select **All Tasks > Import**, as shown in the following figure.
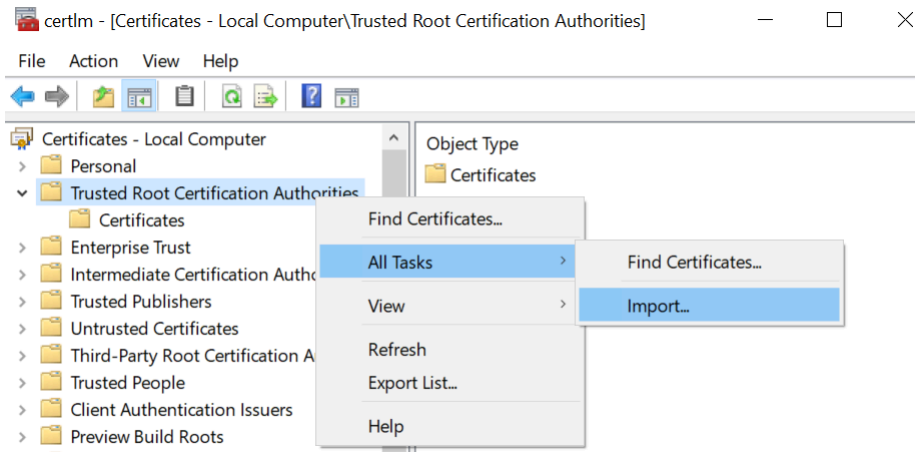
Figure 9: Import Certificate option

e) On the `Welcome to the Certificate Import Wizard` screen, click **Next**.

The following figure shows the `Welcome to the Certificate Import Wizard` screen.

Figure 10: Welcome to the Certificate Import Wizard screen

f) On the `File to Import` screen, click **Browse**, navigate to the folder that contains the root certificate file, select the file, and then click **Open**.

The following figure shows the `File to Import` screen.
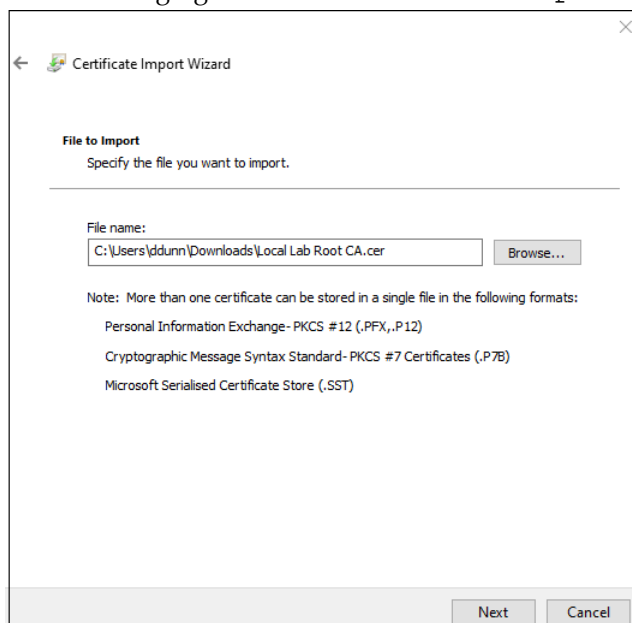
Figure 11: File to Import screen

g) On the `File to Import` screen, click **Next**.

h) On the `Certificate Store` screen, accept the default value **Place all certificates in the following store** with the value **Trusted Root Certification Authorities**, and then click **Next**.

i) On the `Completing the Certificate Import Wizard` screen, click **Finish**.

j) On the `Certificate Import Wizard` dialog, click **OK**.

k) Close the `certlm` window.

6.1.1.3 - Adding HTTPS site bindings

HTTPS provides TLS-encrypted communication between the NES host and the host that an administrator uses to connect to the NES Administrator Console web application.

About this task

Perform the following steps in `Internet Information Service Manager` (IIS Manager) to add HTTPS bindings to the NES website.

If you have already created the bindings or you will use HTTP only, proceed to *Importing a Fullchain Certificate*.

Procedure

1. In the `Connections` navigation pane, click **Computer_Name > Sites**, as shown in the following figure.
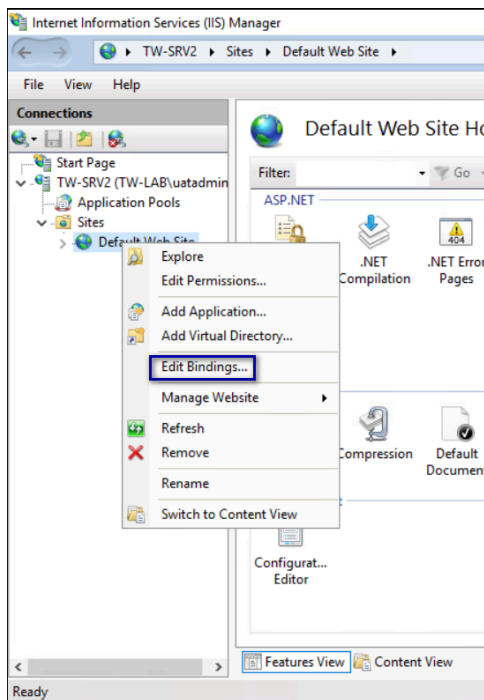
Figure 12: Edit Bindings Option

2. Right-click **Default Web Site**, and then select **Edit Bindings**.
3. Click **Add**.

   The `Add Site Binding` dialog box opens.
4. In the `Add Site Binding` dialog perform the following actions:
   a) From the **Type** list, select **https**.
   b) In the **IP Address** field, leave the default setting **All Unassigned**.

c) In the **Port** field, leave the default setting **443**.

d) Leave the **Host name** field blank.

e) From the **SSL certificate** list, select the TLS certificate that you imported.

The following figure provides an example of the Add Site Binding dialog.
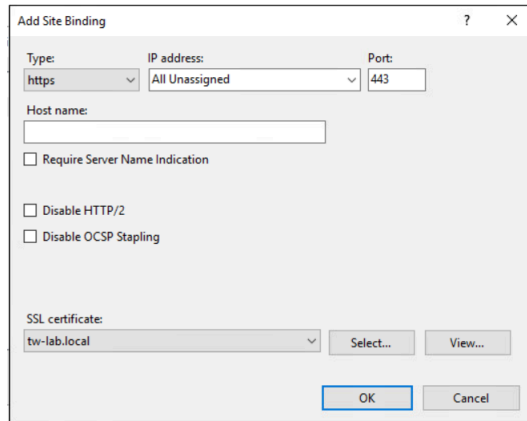
Figure 13: Add Site Binding Dialog

f) Click the **View** button, and identify the expiration date of the TLS certificate (see the line *Valid from (start date to expiration date)*.

g) Record the expiration date in the *Certificate Expiration Date* table.

h) Click **OK**.

5. On the Site Bindings dialog, click **Close**.

6.1.1.4 - Verifying the Authentication Configuration

Perform the following steps in the Internet Information Services (IIS) Manager application to verify that the authentication configuration is correct.

About this task

Procedure

1. On the Connections navigation pane, expand *Computer_Name* > **Sites**, select **Default Web Site**, and then double-click **Authentication**.
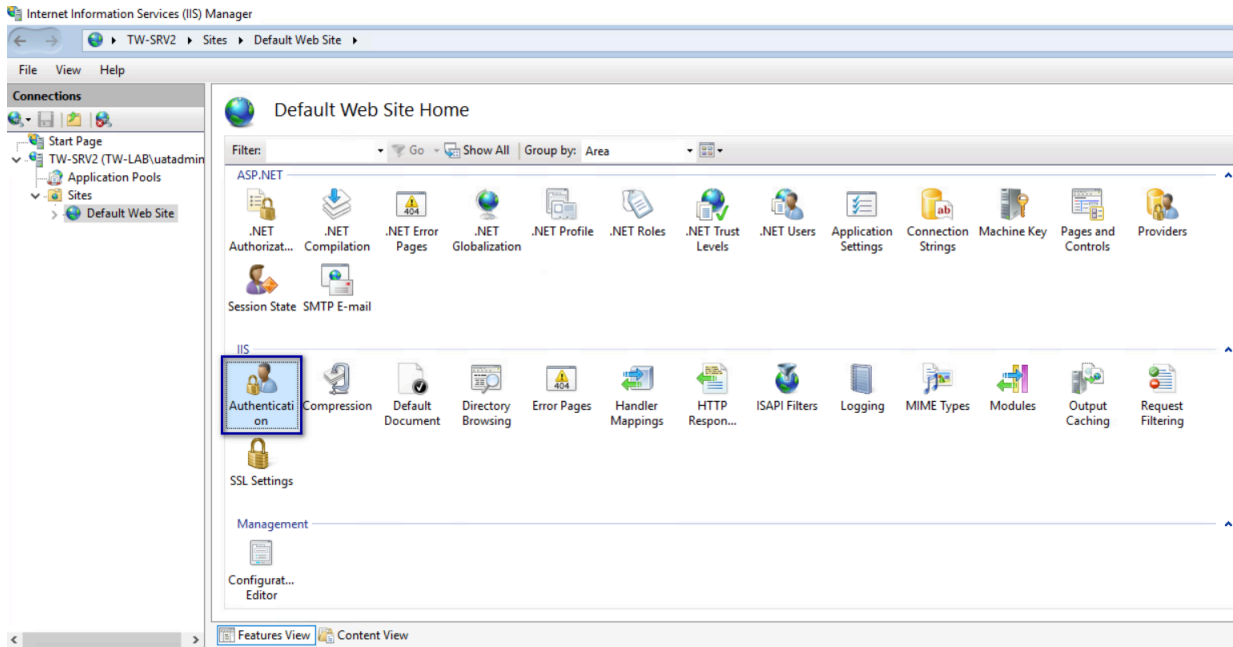
Figure 14: Authentication Option

2. In the `Authentication` pane, ensure that **`Anonymous Authentication`** is the only enabled option.

The following figure provides an example of the `Authentication` pane with only the **`Anonymous Authentication`** option enabled.
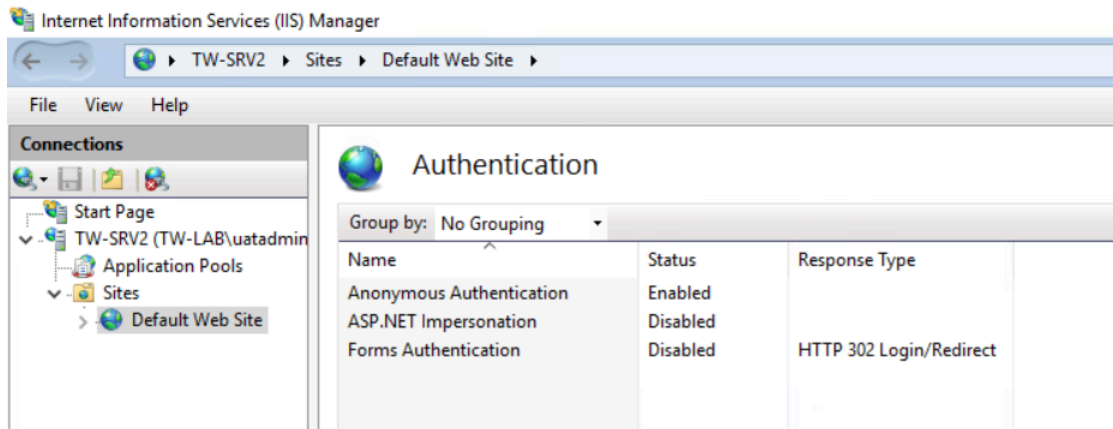
Figure 15: Authentication pane with Anonymous Authentication enabled

6.1.2 - Importing a Fullchain Certificate

To support certificate management in Connected Worker Platform, you must install and configure the certificates. Nymi provides you with a zipped certificate file package that contains a PKCS12 file. The password for the PKCS12 file is provided to you separately.

About this task

The PKCS12 file (fullchain.p12) excludes the password, but contains the following certificates:

- Root certificate
- L1 certificate
- L2 certificate
- L2 private key

Perform the following steps to import the certificates on the NES host.

6.1.2.1 - Importing Certificates

Perform the following steps to import the certificates on the NES host.

About this task

Procedure

1. Extract the certificate zip file to a directory.
2. Right-click the *fullchain.p12* certificate file, and then select `Install PFX`, as shown in the following figure.
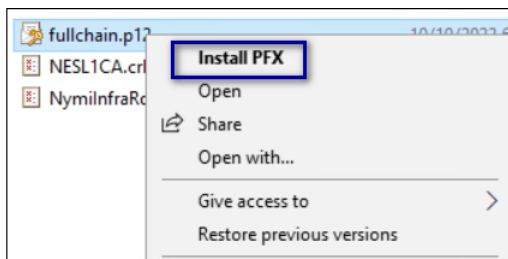
Figure 16: Install PFX Option

3. In the `Open File - Security Warning` dialog, click `Open`.

   The Certificate Import Wizard dialog box opens.
4. On the `Welcome to the Certificate Import Wizard` page, in the `Store Location` page, select `Local Machine`, as shown in the following figure.
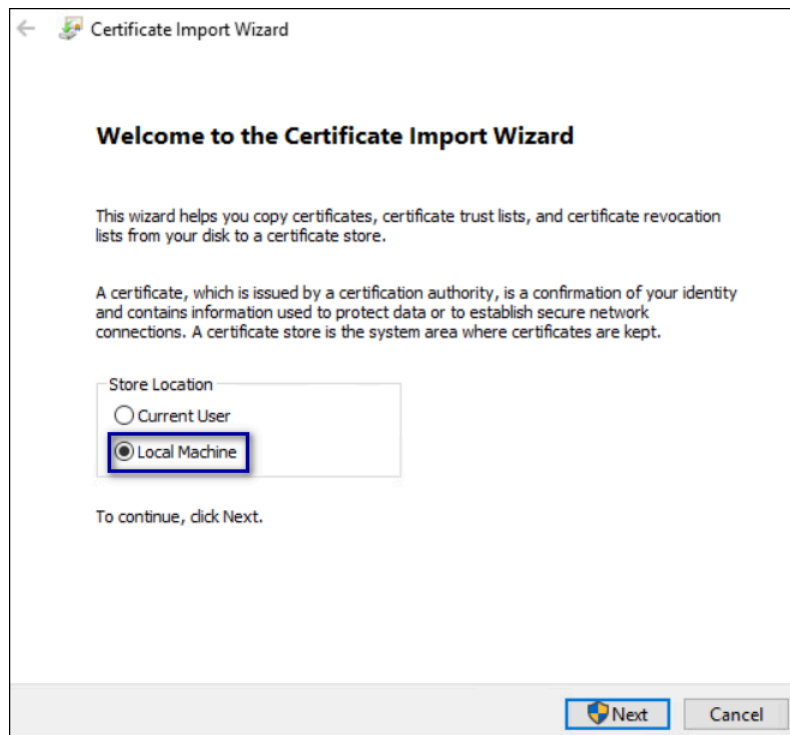
Figure 17: Local Machine Store Location

5. Click **Next**.

6. On the `User Account Control` window, click **Yes**.

7. On the `Files to import` page, ensure that the fullchain.p12 file appears in the *File name* field, and then click **Next**.

8. On the `Private Key Protection` page, in the `Password` field, type the Nymi-provided private key password, and then click **Next**.

   The following figure provides an example of the `Private Key Protection` page.
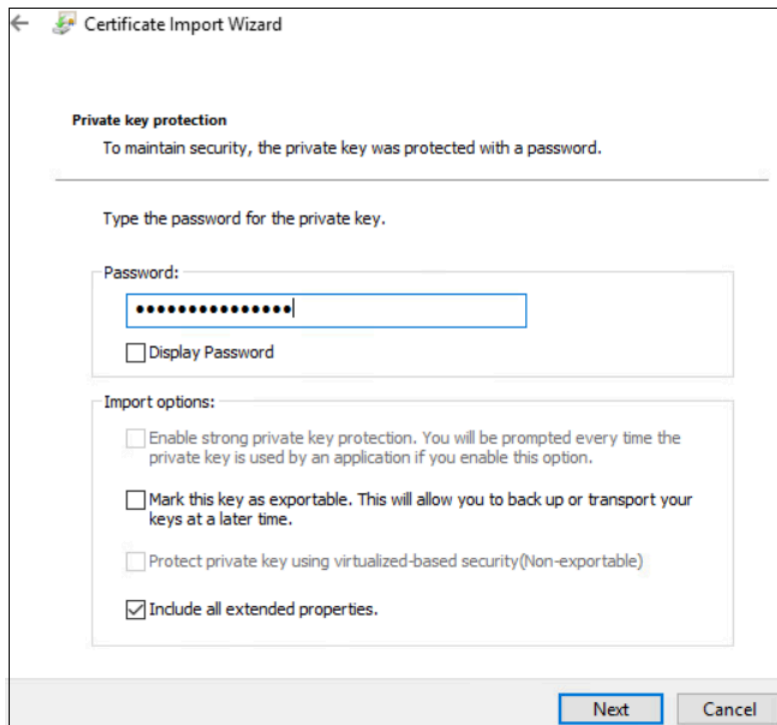
Figure 18: Private Key Protection Page

9. On the `Files to import` page, ensure that the *fullchain.p12* file appears in the **File name** field, and then click **Next**.

10. On the `Certificate Store` page, leave the default option Automatically select the certificate store based on the type of certificate, and then click **Next**.

This options ensures all the certificates in the certification path (Root, Intermediate) are placed in the correct store. The following figure provides an example of the Certificate Store page.
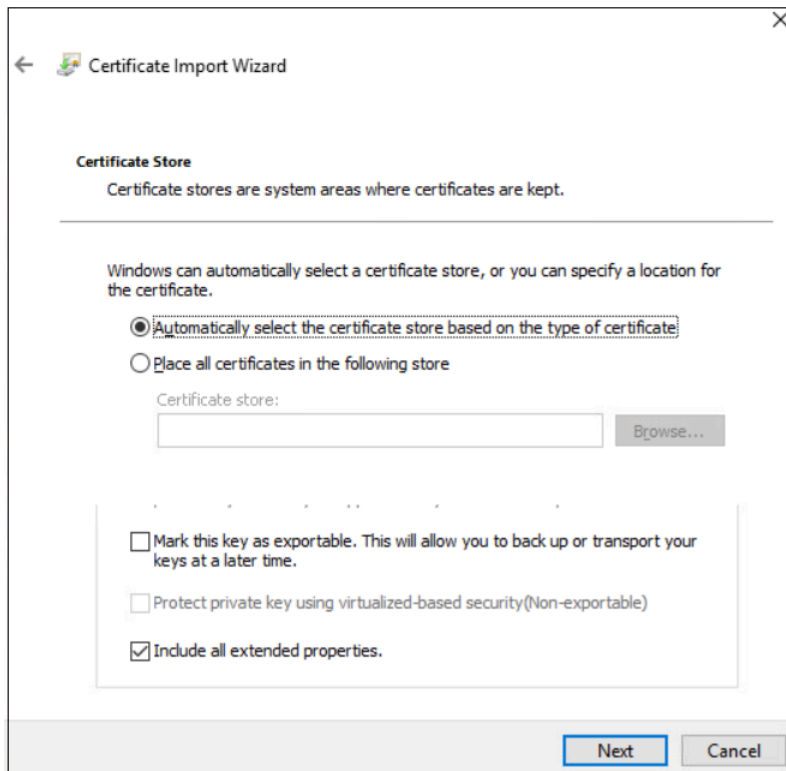
Figure 19: Certificate Store Page

11. On the `Completing the Certificate Import Wizard` page, click **Finish**.

12. On the `Certificate Import Wizard` dialog, click `OK`.

6.1.2.2 - Moving the L2 certificate

Perform the follow steps to move the L2 certificate from the Personal Certificates folder to the Intermediate Certification folder.

About this task

Procedure

1. From the `Windows Start Menu`, type Manage Computer, and then select `Manage Computer Certificates`.

   The `certlm` window appears.

2. On the `User Account Control` dialog, click Yes.

3. Navigate to **Personal > Certificates** folder.

4. Expand **Intermediate Certification > Certificates**, and then move the NES L2 CA certificate from **Personal > Certificates** to the **Intermediate Certification > Certificates** folder.

   You can move the file by dragging and dropping it from one folder to the other folder. The following figure provides an example of the certificates window.
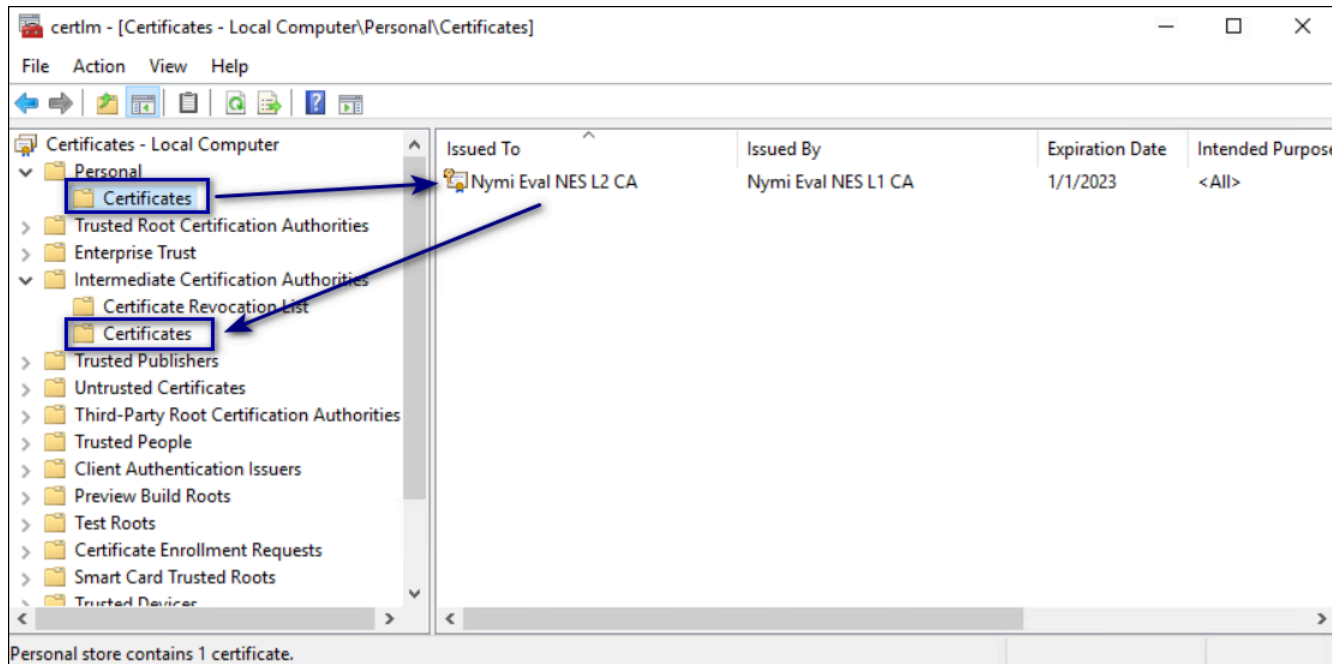
Figure 20: Certificates window

5. In **Intermediate Certification > Certificates** verify that NES L2 CA certificate has a key.

When the L2 certificate has a key, a key symbol displays in the upper-left corner of the L2 certificate icon as shown in the following figure.

Figure 21: L2 Certificate with key

6. Record the expiration date of the NES L2 CA certificate (shown in the Expiration Date column) in the Certificate Expiration Dates table.

7. Close the `certlm` window.

6.1.3 - Installing NES

After you install and configure IIS, install and configure NES. You can configure NES in one of the following ways:

- Using the NES Service Suite Wizard and specifying each configuration option.
- Using the NES Service Suite Wizard and loading configuration options from a *.ninst* file.
- Using the *NESCmdInstall.exe* file to load configuration options from a *.ninst* file, from a command prompt.

6.1.3.1 - Installing the NES Services Suite using the wizard

Perform the following steps to install required third party software and the NES Services Suite.

About this task

Note: The installation process prompts you to install Microsoft .NET Framework 4.8 and SQL Server Express, if the applications are not previously installed on the NES host. If your environment already has a SQL Server that is not locally installed on the NES server and you will create the database on that SQL server, you can skip the SQL Server Express installation.

Procedure

1. Log in to the host with a domain user account that has local administrator rights.

   Note: For the best user experience with the NES installation wizard, resolution of 1920 x 1080 and 100% scaling is recommended.

2. In the *C:\nestemp\NesInstaller* folder, run *install.exe*.

3. On the `User Account Control` dialog, click **Yes**.

4. On the `Open File - Security Warning` page, click **Run**.

5. On the `NESg2. Installer Setup` page, review the Microsoft .NET EULA, and then click **Accept**.

6. On the `Open File - Security Warning` dialog, click **Run**.
   The installer installs .NET.

7. Restart the host when the installation process prompts you.

8. If the installation process does not continue after the restart, rerun *C:\nestemp\NesInstaller \install.exe*.

9. On the `Open File - Security Warning` dialog, click **Run**.

10. On the `Application Install Security Warning` pop-up, click **Install**.
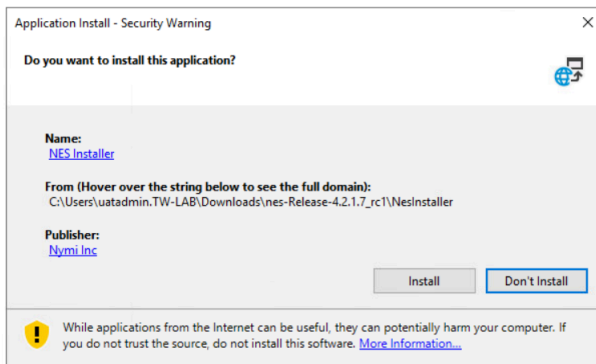
Figure 22: Security Warning

An `NESg2. Installer Setup` page appears, and a status bar displays the progress of the installation.

11. On the `Open File – Security Warning` page, click **Run**.

12. On the `User Account Control` dialog, page, click **Yes**.

13. If the installer does not detect a version of SQL Express on the host, the `Install Prerequisites` dialog appears. Perform of the following actions:

   a) To install SQL Express on the NES server, click **Yes**.

b) To use an existing instance of SQL server on this machine or on another machine, click `No`. When you configure NES in the following section, you provide connection information for the remote SQL Server.

Results

After the third party software installation completes, the installation process performs a prerequisite check and the `Prerequisite Check` dialog appears.

- If the prerequisites check fails, the installer provides you with more information. Review the information, and then click `Exit`. Correct any prerequisite requirements before running the installation again.
- If the prerequisite check is successful, the `Prerequisite check` dialog briefly appears, then closes and the `NES Setup` wizard opens. See the *Configuring NES Services* section for information on the installation wizard.

The following figure shows the `Prerequisites Check` dialog.
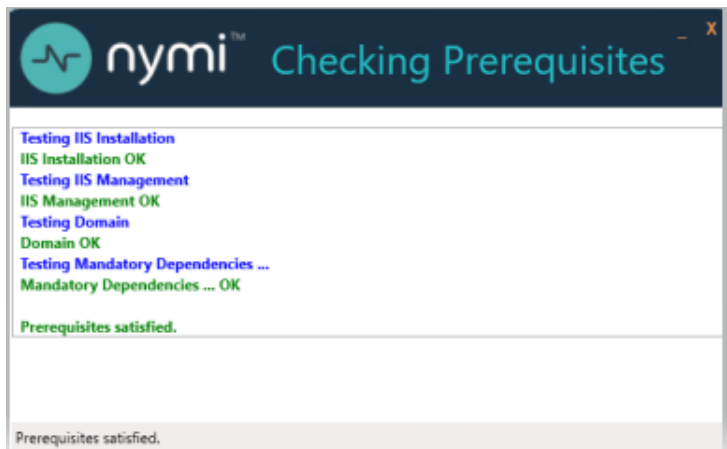
Figure 23: Prerequisites Check Dialog

Note: If you see an error message indicating that the installer was not run with a domain user, you did not run the installer under a domain user account. To resolve this, you must go to `Add or Remove Programs` and uninstall `Microsoft SQL Server`. When prompted to select the features to remove, select all features. When the uninstall completes, log in to the NES host as a domain user and then run *setup.exe* again.

Additional Information

- During NES installation, the process of creating the NES database on the NES server, provides users with administrative privileges to the database. It is recommended that you create a second database user with view access to the audit tables after NES deployment.
- During installation, the installer may disappear and then resume. This is normal behavior as processes are working in the background.

6.1.3.2 - Configuring NES Services Manually

After the `NES Setup` wizard completes the installation of .NET and SQL server, the wizard configures and installs the NES Service Suite.

Before you begin

The following configuration settings values in the Configuration Attribute values table are required:

- NetBIOS Domain name
- NES admin group name
- NES L2 certificate CN

About this task

The following figure provides an example of the `NES Setup` wizard.
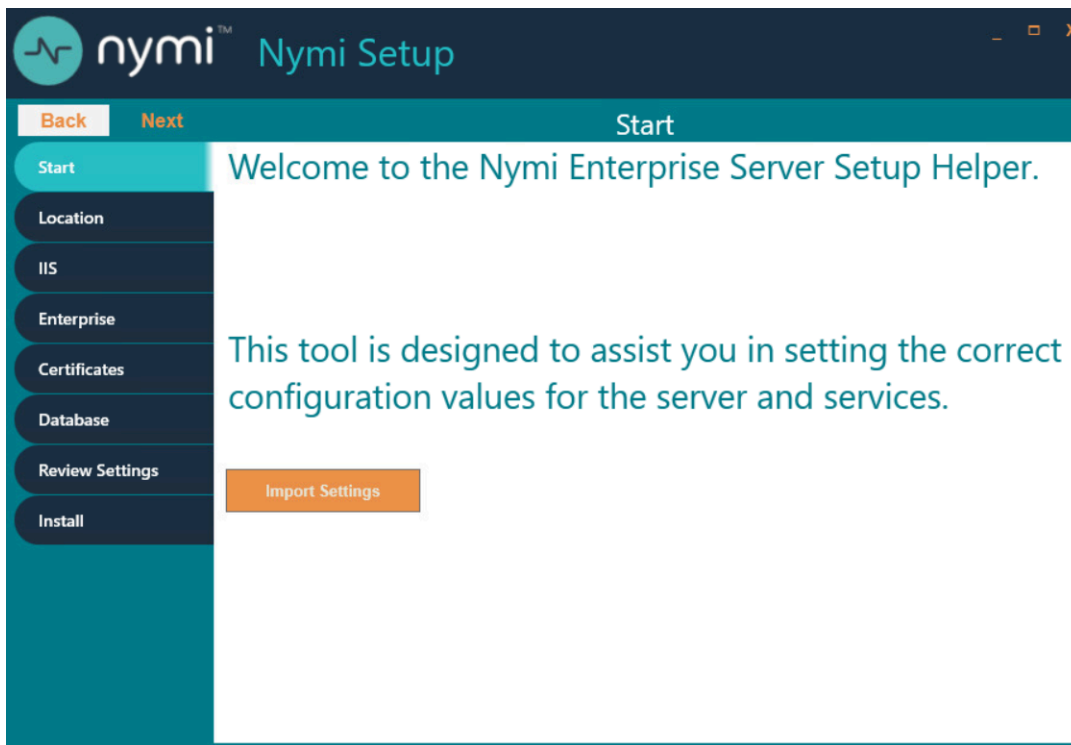
Figure 24: NES Setup Help wizard

Perform the following actions to configure the NES Services Suite.

Note: The **Import Settings** button allows you to load a configuration file to install NES. Creating the configuration file to deploy a subsequent NES is explained later in this document.

Procedure

1. In the left navigation pane, select `Location`, and then perform the following actions:

a) In the **Install Root** field, leave the default location *C:\inetpub\wwwroot* or, to select an alternate installation path for the NES services, click the ellipses and navigate to the folder.

b) In the **Instance Name** field, type a descriptive name for the NES web application instance name, for example NES.

This step optional, but recommended. The name cannot contain spaces. Record the Instance Name in the Configuration Attribute Values table.

c) Click the **Test** button to determine the status of the installation. The test result specifies the type of installation, and the paths for the Authentication Service, NES, and Enrollment Service. The service locations are based on the value specified in the **Instance Name** field.

The following figure provides an example of the Location page.
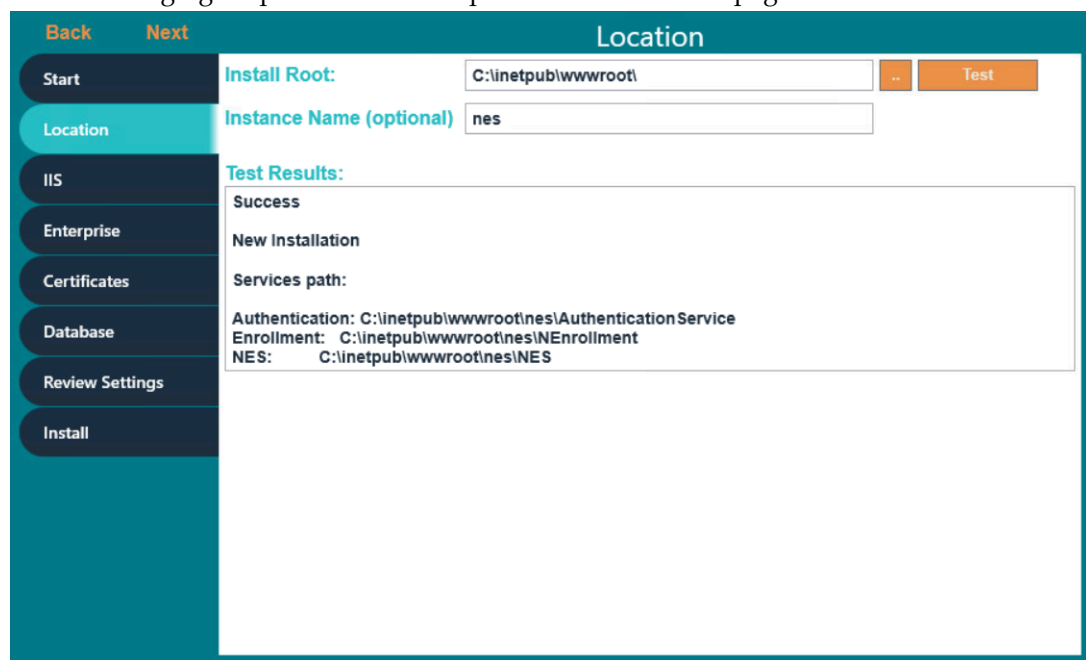
Figure 25: Location page in the NES Setup wizard

2. In the left navigation pane, click IIS, and then perform the following actions:

a) From the **IIS web site** drop-down list, leave the default selection **Default Web Site**.

Alternatively, to install the services on a different existing IIS website, select another website from the list.

b) In the **Application Pool** drop-down list, leave the default setting: **NES App Pool**.

Note: When updating NES from a previous NES release, the default Application Pool appears as **Default App Pool**. It is recommended that you select an application pool that is dedicated to NES.

The Application Pool is used to isolate groups of applications for security, stability and performance reasons. To simplify the deployment of NES, it is recommended to create a dedicated Application Pool for NES.

c) In the **`Application Pool Identity`** drop-down list, select an existing identity or leave the default setting: **`NetworkService`**.

If you use a SQL server that is not installed on the NES server, select **`SpecificUser`** from the drop-down list and perform the following actions:

- In the **`User Name`** field, type the username of the SQL service account in the format domain \username.
- In the **`Password`** field, type the password for the SQL service account.
- Click the **`Test`** button to validate the user credentials.

d) In the **`Communication Protocol`** section, available IIS site bindings appear. Select a communication protocol for the deployment.
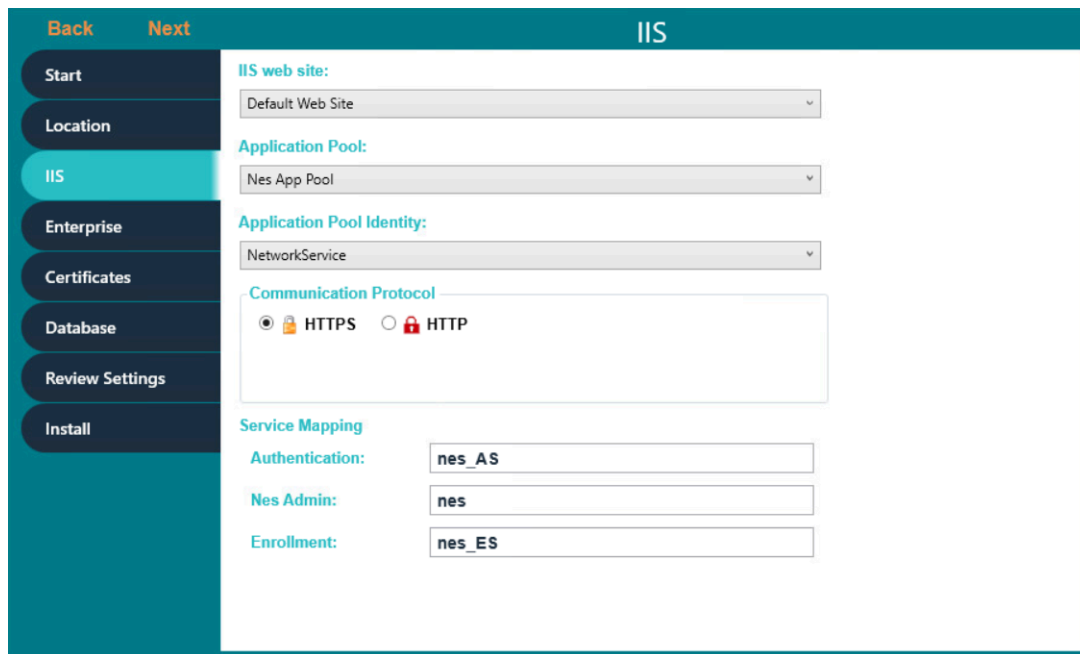
Nymi recommends that you select HTTPS to ensure secure communication and HTTPS is required for CWP with Evidian deployments. If an HTTPS address is not available, review *Adding HTTPS site bindings* to add a HTTPS site binding.

Note: HTTP is not encrypted. Sensitive information is sent in plain text.

e) In the `Service Mapping` area, review the recommended mapping names for each service. If required, edit the mapping and specify a name that does not contain spaces.

Note: Service mapping defines the relative address of each of the web services (web apps) that run on the server. Record the names of the NES and Enrollment service mappings in the Configuration Attribute Values table.

The following figure provides an example of the `IIS Setup` page.

Figure 26: IIS Setup page in the NES Setup wizard

The following figure displays the warning that appears when you select HTTP as the communication protocol.
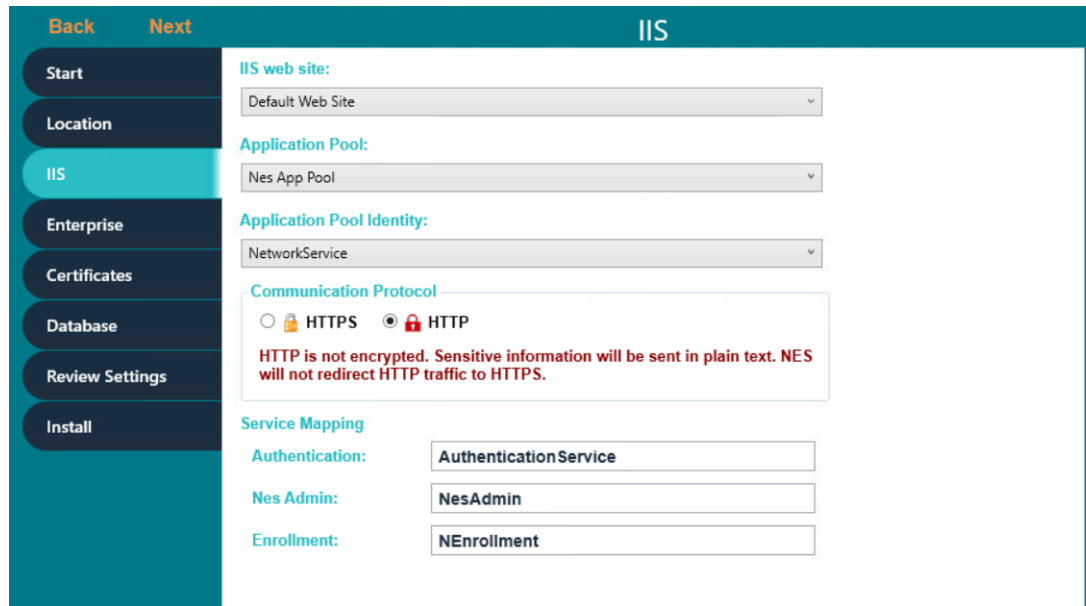
Figure 27: IIS Setup Page HTTP Warning

3. In the left navigation pane, click `Enterprise`, and perform the following actions:

   a) In the `LDAP protocol` section, select LDAP or LDAPS.

   Refer to *Appendix – Record the CWP Variables* for your site-specific configuration information.

4. In the **`Domains`** table the domain in which the NES host resides appears. If Nymi Band users, NES Administrators, or the SQL service account reside in other domains, perform the following steps to add the additional domains:

   a) In the **`Domain`** table, on an empty line, type the NetBIOS (Pre-Windows 2000) name of the domain that contains the user accounts.

   b) Type a domain username and password for the domain if the one of following conditions are met:

   - The domain is not in the same forest as the NES domain.
   - A two-way trust does not exist between the domain and the domain in which NES resides.
   - The domain is not in the same forest as the NES domain and does not have a two-way trust with the domain in which the SQL service account resides.

   Note: Select a domain user whose password never expires.

   c) Press **`Enter`**.

   d) Press **`Test`** to confirm that all domains are reachable.

   The following figure provides an example of the `Enterprise Setup` page.
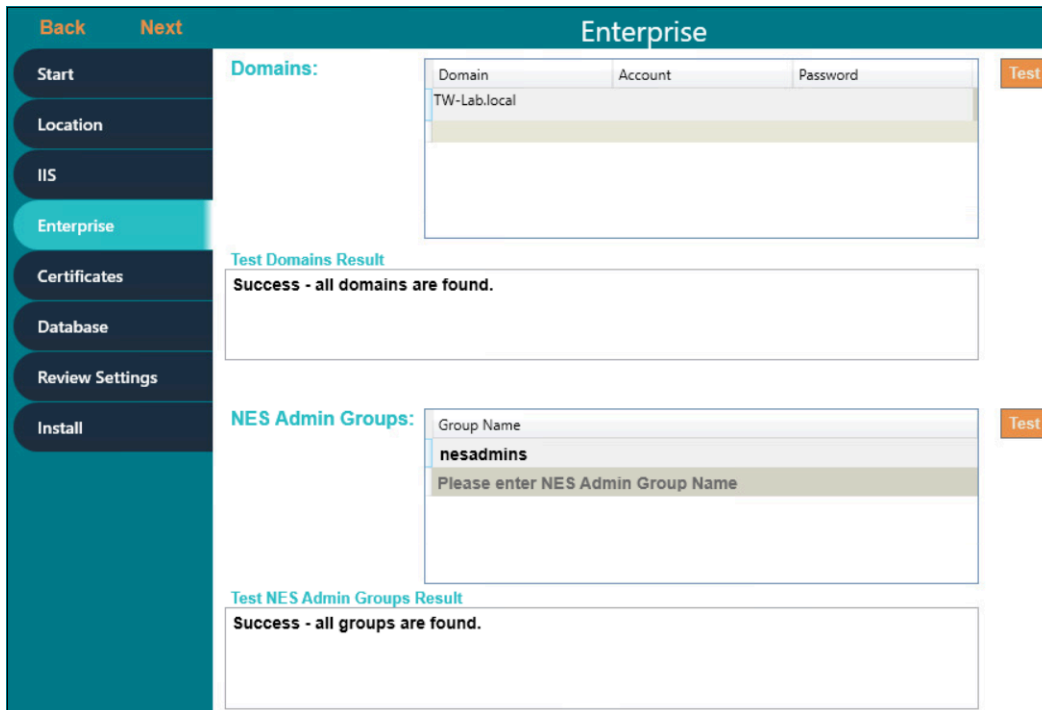
Figure 28: Enterprise page in the NES Setup wizard

5. In the **Nes Admin Groups** table, enter the NES Administrator group name by right clicking in the field, selecting **Add**, and then typing the name of the group. In a multi-domain configuration where you have configured multiple global NES Administrator groups in different domains, add each group.

   Refer to *Appendix – Record the CWP Variables* for the name of the NES Administrator groups.

6. In the left navigation pane, click **Certificates**, and then perform the following actions:

   a) In the **Certificate Expiry** field, change the default value for the length of time that the NEA tokens remains valid to 90.00:00:00.

   b) From the **Level One Certificate** list, select the CN value of the L1 certificate from the list.

      The L1 certificate name is in the form *enterprise_name* NES L1 CA.

   c) From the **Level Two Certificate** list, select the CN of the L2 certificate.

      The following figure provides an example of the Certificates page.
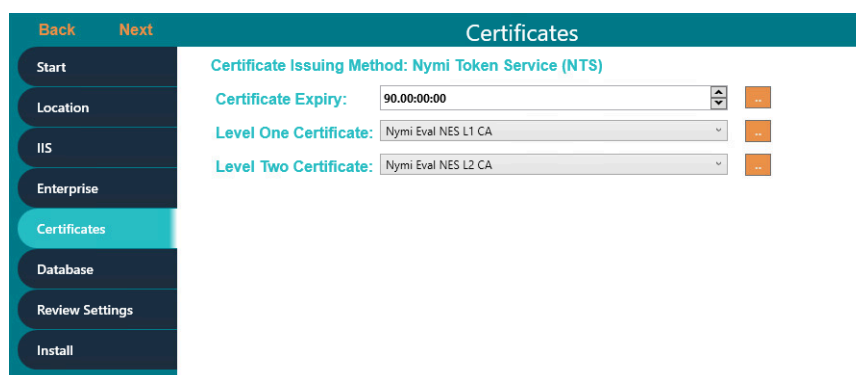
Figure 29: Certificates page in the NES Setup wizard

7. In the left navigation pane, click `Database` The Database page provides database configuration settings that enable NES to create a database. Perform the following actions to ensure that NES can create the database. The steps required differ depending on whether the SQL server uses SQL authentication or Windows authentication.

- Windows Authentication

  a. Leave the **Integrated Security** option selected. This sets the security property in the **Connection String** to **True**.

     The default connection string for SQL Express is Data Source=.\SQLEXPRESS;Initial Catalog=Nymi.{0};Integrated Security=True;MultipleActiveResultSets=True

  b. If required, update the connection string with the database instance that you want to use, instead of the default SQL Express 2012. Refer to https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax for more information about defining the connection string.

  c. Click **Test** to verify that the database connection string is valid and NES can connect to the database server.

     Note: If you do not use an existing database, the test reports that the database does not exist. NES creates the database during the installation process.

  d. In **Manage Database Logins** section, click the **Verify Users** button to ensure that NES can create users with access to the SQL database.

     The table displays the default account settings for the **Application Pool** and **Application Policy** identity settings that were defined on the `IIS` page appear. By default, the **Service type** login is an account that provides NES with access to the SQL database. The **Auditor type** login is an account that provides a user with access to view the NES audit tables. For additional information about adding, editing and deleting database users or accounts, see *Managing Database Logins*.

- SQL Authentication

  a. Clear the **Integrated Security** option. This sets the security property in the **Connection String** to **False**.

  b. If required, update the connection string with the database instance that you want to use instead of the default SQL Express 2012. Refer to https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax for more information about defining the connection string.

    c. In the **SQL Login** section, enter the username and password, and then click **Verify** to ensure the provided credentials are valid.

    d. Click **Test** to verify that the database connection string is valid and NES can connect to the database server.

> **Note:** If you do not use an existing database, the test reports that the database does not exist. NES creates the database during the installation process.

The following figure provides an example of the `Database Setup` page for Windows Authentication.
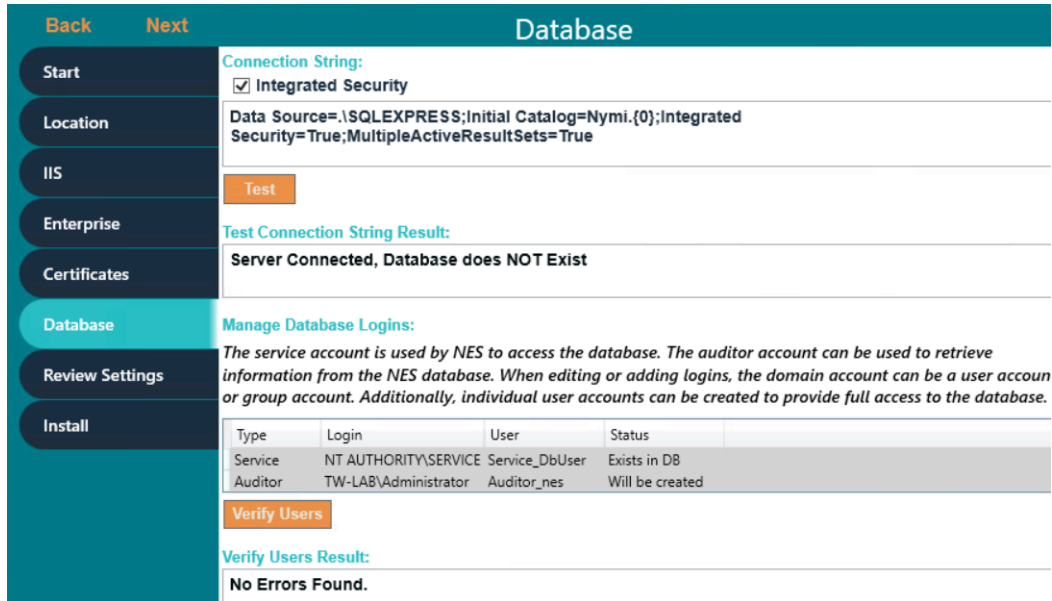
Figure 30: Database Setup page in NES Setup wizard for Windows Authentication

8. In the left navigation pane, click `Review Settings`. The parameters for the NES installation are displayed for final review.

    a) Click **Test** to verify the configuration. Review the test results and address any errors if applicable.
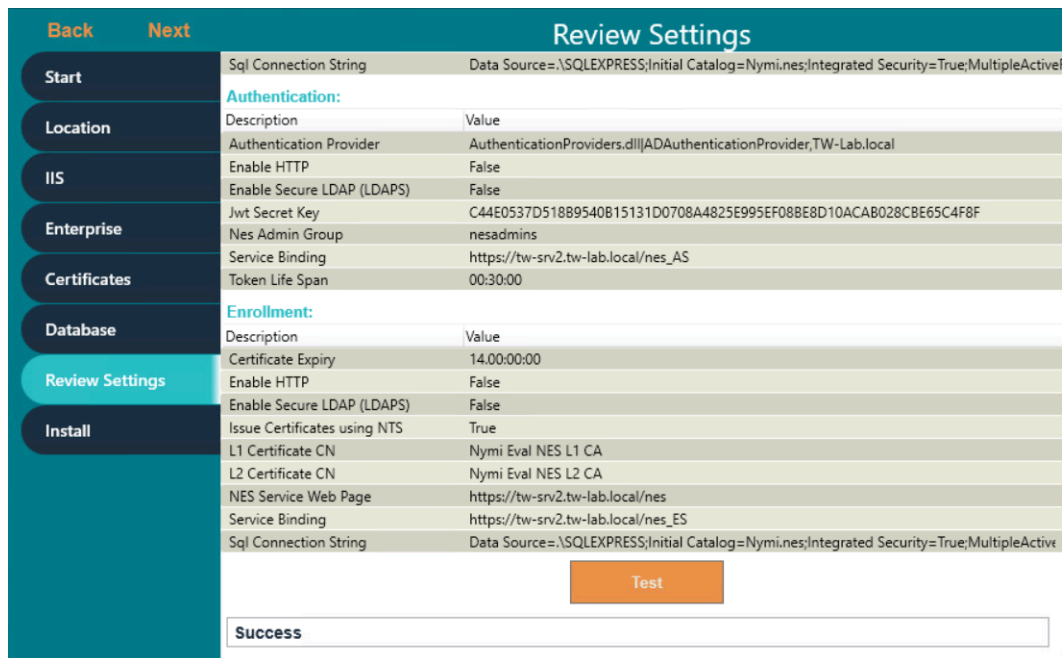
Figure 31: Review Settings window

If you receive a warning dialog that states `SelectedSiteBindings: The underlying connection was closed: Could not establish a trust relationship for the SSL/TLS secure channel.` To resolve this message, import the TLS certificate as described in the *Importing the TLS server certificates* section.

9. In the left navigation pane, click `Install`. The Install page provides different options depending on the status of the installation.

Table 5: Install page Options

Button	Description
Install	Installs a fresh installation of NES.
Upgrade	Upgrades an existing installation of NES.
Apply Settings	Apply settings to an existing NES installation.
Export Settings	Export the configuration file for NES settings.
Exit	Exit installation wizard without installing NES.

10. For a new installation, click the **Install** button.

The following figure provides an example where the installation succeeds with a warning that the L2 certificate expires within 90 days.
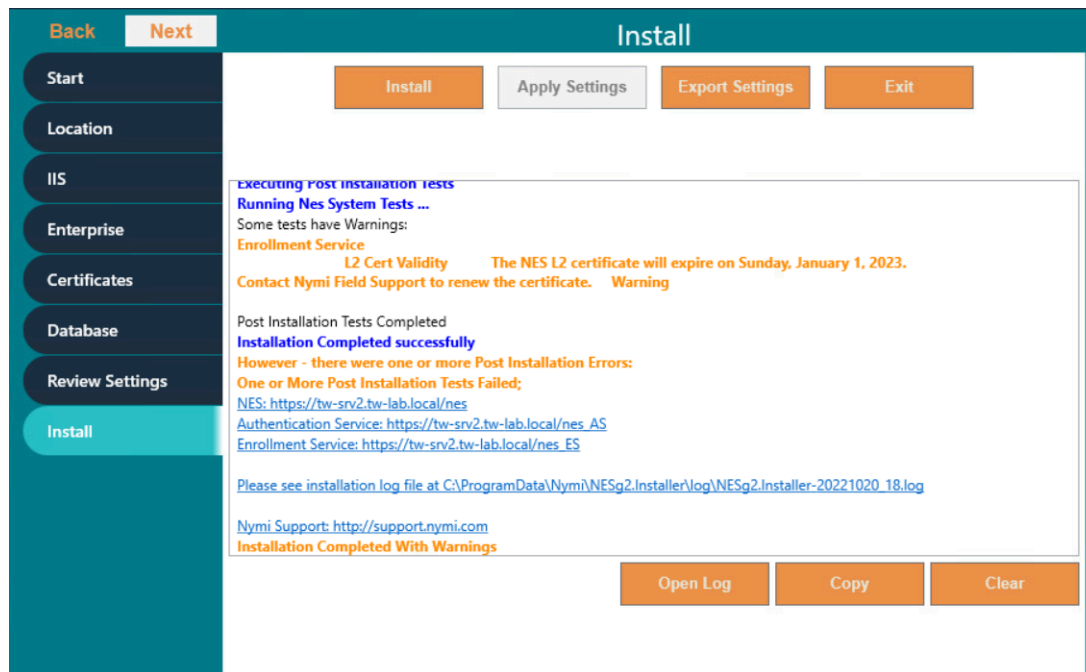
Figure 32: Install NES page in `NES Setup` **wizard**

Note: If the NES installation fails with the error message "Cannot Allow Access to certificate: 'Nymi Eval NES L2 CA' for account: 'NT AUTHORITY\SERVICE'.", additional troubleshooting actions are required for the fullchain certificate. Save the NES configuration using **Export Settings** and close the NES installer. Delete the L1 and L2 certificates from the intermediate certificate authority, and re-import the fullchain certificate following *Importing a Fullchain Certificate*. Move the L2 certificate from the personal certificate store to the intermediate certificate store and re-run the NES installer using the saved NES configuration file. On the Start page, the Import Settings button allows you to load a configuration file to install NES.

11. When the installation completes, perform one of the following actions:

a) Close the `NES Setup` wizard.

b) Click **Export Settings** to save the NES configuration settings for future deployments.

The section *Saving the NES configuration for silent installations* provides more information.

Saving the NES Configuration File for Silent Installations

The NES Setup wizard provides you with the ability to save the NES configuration to a file. The NES configuration file allows you to perform a silent installation of the NES host, with the configuration settings that you have defined during a previous NES deployment.

About this task

The NES configuration can be saved and used for a future NES deployment.

Procedure

1. In the *C:\nestemp\NesInstaller* folder, run *install.exe*.

2. On the `Location` tab, in the **`Instance Name`** field, type the instance name that was specified during the deployment.

3. On the `Database` tab, click **`Test`** and **`Verify Users`** to load the database information.

4. On the `Install` tab, click **`Export Settings`**.

5. On the `Export Settings` dialog, perform the following actions:

    a) In the **`File Name`** section, click the ellipses, and then navigate to the location where you want to save the configuration file.

       The default location is the *Documents* folder for the logged in user.

       1. In the **Name** field, type the file name. The default file name is the Instance Name of the NES configuration.
       2. Click **Save**. The configuration file is saved as a file with a *.ninst* extension.

    b) In the `Encryption` section, select one of the following options:

       • **`None`**, to save the configuration file without encrypting sensitive information.
       • **`Machine`**, to save the configuration with machine encryption.

         Note: This saves the file with machine-specific encryption; therefore, you can only load the configuration file on the same machine on which you save the configuration.

       • **`Private key`**, to save the configuration and encrypt the configuration file with a private key.

         Note: This option allows you to load the configuration file with the generated private key file, on a different machine.

         NES Setup can create a new private key for you or you can use an existing private key.

         • To use an existing private key, click the Ellipsis, and then navigate to the location of the file. Select the file, and then click **Open**.
         • To create a new private key file, click **New**. Navigate to the location where you want to save the file. In the **Name** field, type the file name. The default file name is the Instance Name for the configuration. Click **Save**. Click **OK**. The configuration file is saved as a file with a *.key* extension.

       • Click **OK**.

    c) Click **OK**.

Deploying the NES URL to User Terminals by using group policies

Use Windows group policies to modify the registry on each network terminal to specify the address of the NES web application.

Before you begin

The user that creates the group policy requires domain administrator rights. Create a group that contains all the user terminals that require this change.

About this task

Perform the following actions to create a group policy object to change the registry.

Procedure

1. On a Domain Controller, open the `Group Policy Management` panel.
2. Expand **`Forest > Domains`**, right-click the domain that contains the hosts, and then select **`Create a GPO in this domain, and Link it here`**.
3. In the **`Name`** field, type Nymi.
4. In the **`Source Starter GPO`** field, leave the default value (none).
5. Click **`OK`**.
6. Expand the domain and select **`Nymi`**. Click **`OK`**.
7. On the **`Scope`** tab, under **`Security Filtering`**, perform the following actions:
   a) Select **`Authenticated Users`**.
   b) Click **`Remove`**.
   c) On the `Group Policy Management` confirmation window, click **`OK`**.
   d) On the warning window, click **`OK`**.
   e) Click **`Add`**.
   f) On the `Select Users, Groups and Computers` window, type the name of the group that contains the user terminals, click **`Check Names`**, and then click **`OK`**.
      The group appears in the Security Filter section.
8. On the **`Setting`** tab, right-click **`Computer Configuration`**, and then select **`Edit`**.
9. Expand **`Computer Configuration > Preferences > Windows Settings`**.
10. Right-click **`Registry`**, and then select **`New > Registry Item`**.

    The `New Registry Properties` window appears.
11. From the **`Action`** list, select **`Create`**.
12. From the **`Hive`** list, leave the default value **`HKEY_LOCAL_MACHINE`**.
13. In the **`Key Path`** field, type SOFTWARE\Nymi\NES.
14. In the **`Value name`** section, type URL.
15. In the **`Value Data`** field, type https://nes_server/NES_service_name/

    where:

    - *nes_server* is the FQDN of the NES host. The FQDN consists of the <hostname>.<domain>. You can also find the FQDN by going to the terminal where NES was deployed and viewing the properties of the system. The *nes_server* is the **`Full computer name`**.
    - *NES_service_name* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory.

    The website that you specified in the **`Value Data`** field is the address of the NES Administrator Console website that NES Administrators access to manage NES. Record the value in the Configuration Attribute Values table.
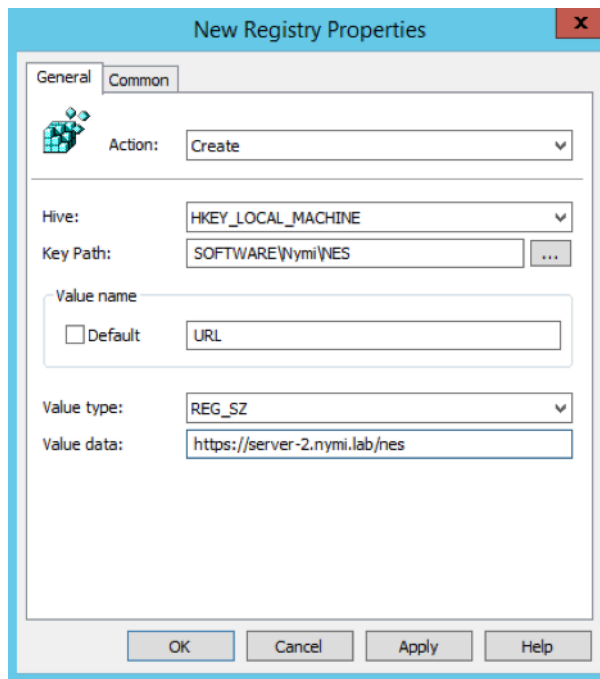
Figure 33: URL properties page

16. Click **OK**.

Deploying the Nymi Agent URL to User Terminals by using group policies

Perform the following steps when you use a centralized Nymi Agent. Use Windows group policies to modify the registry on user terminals to enable Nymi Bluetooth Endpoint to communicate with the remote Nymi Agent.

Before you begin

The user that creates the group policy requires domain administrator rights. Create a group that contains all the user terminals that require this change.

About this task

Create a group policy object to update the registry.

Procedure

1. On a Domain Controller, open the `Group Policy Management` panel.
2. Expand **Forest > Domains**, right-click the domain that contains the hosts, and then select **Create a GPO in this domain, and Link it here**.
3. In the **Name** field, type Nymi Agent.
4. In the **Source Starter GPO** field, leave the default value (none).
5. Click **OK**.

6. Expand the domain and select `Nymi Agent`. Click `OK`.
7. On the `Scope` tab, under `Security Filtering`, perform the following actions:
   a) Select `Authenticated Users`.
   b) Click `Remove`.
   c) On the `Group Policy Management` confirmation window, click `OK`.
   d) On the warning window, click `OK`.
   e) Click `Add`.
   f) On the `Select Users, Groups and Computers` window, type the name of the group that contains the user terminals, click `Check Names`, and then click `OK`.
      The group appears in the Security Filter section.
8. On the `Setting` tab, right-click `Computer Configuration`, and then select `Edit`.
9. Expand `Computer Configuration > Preferences > Windows Settings`.
10. Right-click `Registry`, and then select `New > Registry Item`.
   The `New Registry Properties` window appears.
11. From the `Action` list, select `Create`.
12. From the `Hive` list, leave the default value `HKEY_LOCAL_MACHINE`.
13. In the `Key Path` field, type SOFTWARE\Nymi\NES.
14. In the `Value name` section, type AgentUrl.
15. In the `Value Data` field, type ws://NymiAgent:port/socket/websocket

   where:

   • `NymiAgent` is the FQDN of the Nymi Agent host.
   • `port` is the port number
   • `socket` is the name of the socket
   • `websocket` is the communication protocol that connects the Nymi Band Application to the Nymi Agent. You can choose any name for this mapping, but it is recommended that you specify a name that is descriptive.

   The IP address that you specified in the `Value Data` field is the address of the Nymi Agent that the Nymi Band Application connects to. Record the value in the Configuration Attribute Values table.
16. Click `OK`.

6.1.3.3 - Configuring NES from a Configuration File

You can configure NES based on values that are defined in a configuration file. The option to create a configuration file (*.ninst* file) is available to you when you perform an NES configuration by using the NES Setup wizard. You can configure NES from the command line or with the NES Setup wizard.

Before Installing NES using the Silent Installer

Before installing NES using the Silent Installer, perform the following:

• Log into your machine with a domain user account that has local administrative privileges
• Copy and extract the installation files to the machine

- If you are using a *.ninst* file from a pre-CWP1.6 NES installation, edit the file and add the following entries before the last } that appears in the file:

```
        "JwtSecretKey":
"C44E0537D518B9540B15131D0708A4825E995EF08BE8D10ACAB028CBE65C4F8F",
            "NesBinding": "https://nes_server/NES_service_name}"
```

where:

- `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
- `NES_service_name` is the service mapping name for the NES web application. The default service mapping name is *nes*.

  For example, https://nes.cwp.company.com/nes.

  Note: The service mapping name for NES is defined during deployment. Contact the person who performed the deployment to obtain the NES service mapping name value. Record the URL of ph conkeyref="prod_names/nes"/> in *Appendix—Record the CWP Variables*. You will use this URL to connect to the NES Administrator Console .

Installing .NET and SQL Server Express

The installation package contains the .NET 4.8 software and Microsoft SQL Server Express 2017 in the following directories:

- .NET 4.8 software: *..\NesInstaller\DotNetFX48*

  Note: The .NET software may require you to restart your computer.
- Microsoft SQL Server Express 2017: *..\PreRequisites\SqlExpress*

  Note: During the installation, accept all defaults. The Silent Installer creates all Microsoft SQL Server users automatically. On the `Database Engine Configuration` screen, add additional users that require access to the audit reports in the SQL database.

Configuring NES Silently from the Command Line

Perform the following steps to install Nymi Enterprise Server (NES) from command line, by using the configuration values defined in an *ninst* file.

Before you begin

Before perform a silent installation NES by using a configuration file, perform the following actions:

- Log into your machine with a domain user account that has local administrative privileges
- Copy and extract the installation package to the machine
- Install .NET. The installation package contains the .NET 4.8 software and Microsoft SQL Server Express in the following directories: .NET 4.8 software: *..\NesInstaller\DotNetFX48* . The .NET installation may require you to restart your computer.
- Install SQL Express if you do not have an existing MS SQL Server to store the NES database. The installation package contains Microsoft SQL Server Express 2019 in the

following location: *..\PreRequisites\SqlExpress* During the SQL installation, accept all defaults. The installation process creates all Microsoft SQL Server users automatically. On the Database Engine Configuration screen, add additional users that require access to the audit reports in the SQL database.

About this task

Nymi provides a sample *.ninst* file located in the NES release folder in the following location: *bundle-folder\NesCmdInstall*. Also included in the sample file is an example of how to configure NES in a multiple domain environment.

To install NES using the silent installer:

Procedure

1. Copy the *.ninst* files and if created, the private key file to the *C:\nestemp\nes-Release-x.x.x.x\NesCmdInstall* directory.
2. Open a command prompt as an Administrator and change the path to *C:\nestemp\nes-Release-x.x.x.x\NesCmdInstall* directory.
3. Type NesCmdInstall.exe --config `path_to_config_file`\ninst_filename [--key path_to_private_key_file\filename] --allowwarnings

   where:

   - `ninst_filename` is the name of the NES configuration file.
   - `path_to_config_file` is the absolute or relative path to the configuration file.
   - `path_to_private_key_file` is the absolute or relative path to the key file.

   Note: Use the --key parameter with the `path_to_private_key_file` to install the private keys manually.

   For example, to configure NES when the configuration file and private key file are in the *C:\nestemp\nes-Release-x.x.x.x\NesCmdInstall* directory, type `NesCmdInstall.exe --config NTS.ninst --key nes.key --allowwarnings`

4. On the `User Account Control` dialog, click **Yes**.

   Installation log files are located in *C:\Program Data\Nymi\NesCmdinstall\log* directory. The installation process provides output to the screen as well as installation log files.

Configuring NES With a Configure File in the NES Setup Wizard

Perform the following steps to install Nymi Enterprise Server (NES) with the NES Setup Wizard, by using the configuration values defined in an *ninst* file

About this task

Procedure

1. In the NES Setup Wizard, on the `Start` screen, click **Import Settings**.
2. In the `Open` window, navigate to the directory that contains the *ninst* configuration file, and then double-click the *.ninst* file.

A **Loaded Successfully** message appears on the screen.

3. On the **Review Settings** tab, click **Test**
   The window displays a Success message when the configuration file values are valid or displays error messages when the configuration file requires correction.

4. If the **Review Settings** test did not report errors, on the **Install** tab, click **Install**.

5. When the installation completes, close the NES Setup wizard.

6.1.4 - Configuring IIS to Prevent NES Offloading

Configure IIS to ensure that NES applications are always available to service the requests, and not off-loaded.

About this task
Perform the following steps in Internet Information Service Manager (IIS Manager).

Procedure

1. In the Connections navigation pane, expand **Computer_Name > Sites > Default Web Site**, and then perform the following steps to determine the application pool name for each NES application.

   a) Select the **nes** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.

   b) In the Edit Application window, make note of the value that appears in the **Application Pool** field, and then click **OK**.

   c) Select the **nes_AS** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.

   d) In the Edit Application window, make note of the value that appears in the **Application Pool** field, and then click **OK**.

   e) Select the **nes_ES** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.

   f) In the Edit Application window, make note of the value that appears in the **Application Pool** field, and then click **OK**.

   The following figure provides an example of the **Basic Settings** menu option and the Edit Application window.
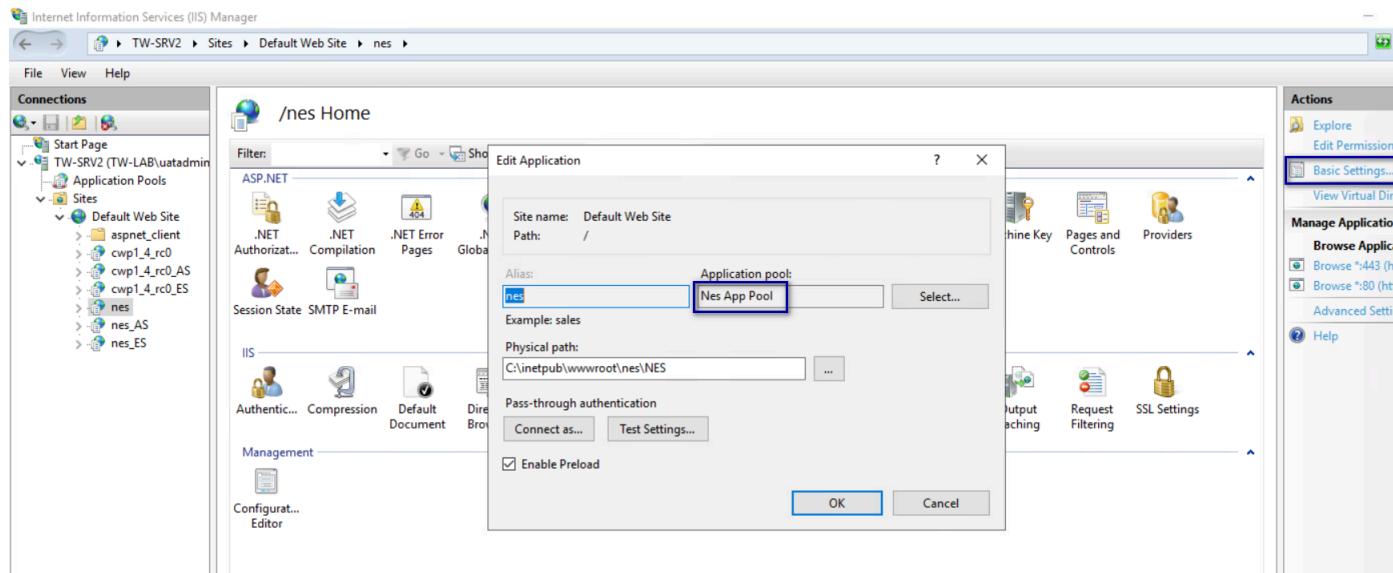
Figure 34: Edit Application window

2. In the `Connections` navigation pane, expand **Computer_Name > Application Pools**, right-click the application pool for the NES applications, and then select **Advanced Settings**, as shown in the following figure.
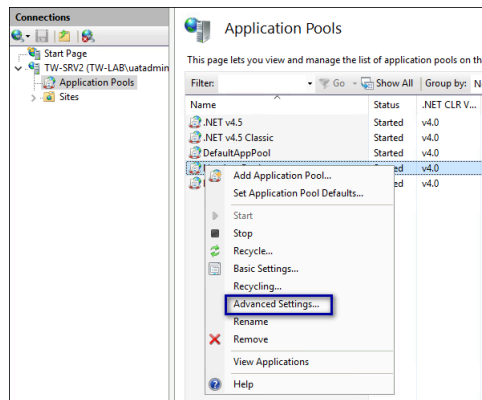
Figure 35: Advanced Settings menu option

3. In the `Advanced Settings` window, perform the following actions.
   a) In the **General** section, confirm that the **.NET CLR Version** value is v4.0.
   b) In the **General** section, from the **Start Mode** list, select **Always Running**.
   c) In the **Process Model** section, for the **Idle Timeout (minutes)** value, type 0.
   d) Click **OK**.

   The following figure provides an example of the `Advanced Settings window`.
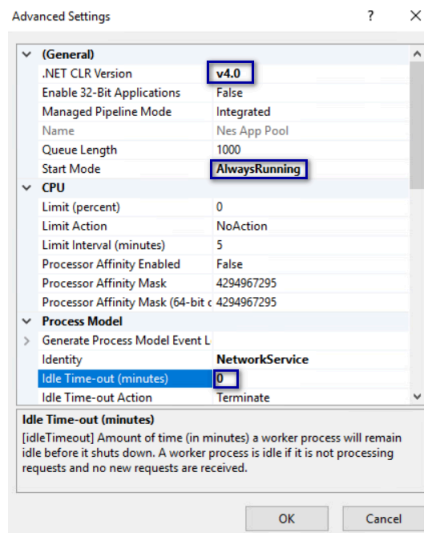
Figure 36: Advanced Settings window

Note: If the NES applications use different application pools, configure the **Advanced Settings** option for each application pool.

4. In the `Connections` navigation pane, expand **Computer_Name > Sites > Default Web Site**, and then perform the following steps.

a) Right-click **nes** and then select **Manage Application > Advanced Settings**, as shown in the following figure.
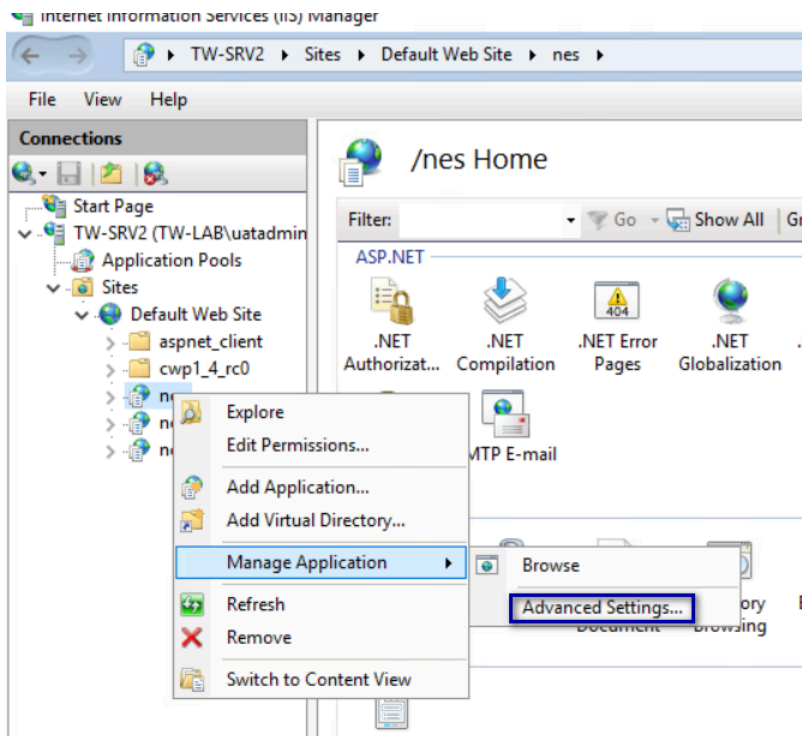
Figure 37: Advanced Settings option

b) On the `Advanced Settings` window, from the **Preload Enabled** list, select **True**.

c) Click **OK**.

d) Right-click **nes_AS** and then select **Manage Application > Advanced Settings**.

e) On the `Advanced Settings` window, from the **Preload Enabled** list, select **True**.

f) Click **OK**.

g) Right-click **nes_ES** and then select **Manage Application > Advanced Settings**.

h) On the `Advanced Settings` window, from the **Preload Enabled** list, select **True**.

The following figure provides an example of the **Advanced Settings** window.
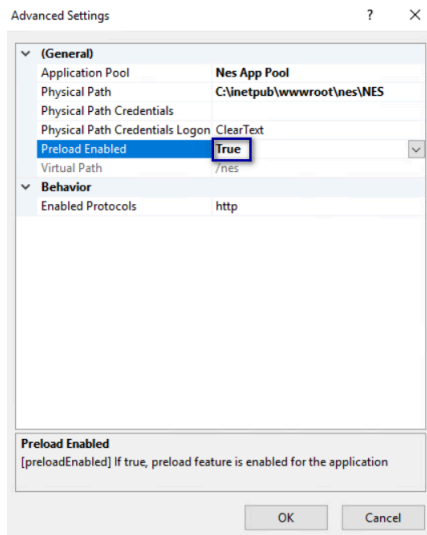
Figure 38: Advanced Settings window

i) Click **OK**.

5. Close `IIS Manager`.

6.1.5 - Creating an Application Pool for Authentication Service

To support Windows authentication to a remote SQL Server, the NES Enrollment Service and Directory service need to run under a specific domain service account. If the NES Authentication service runs under a specific user account, the configuration requires HTTP Service Principal Names (SPNs). To avoid the need to configure HTTP SPNs, create a separate Application Pool that uses the Network Service account as the application pool identity.

About this task

Perform the following steps in IIS Manager.

Procedure

1. Expand `server_name`, right-click `Application Pools`, and then select `Add Application Pool`, as shown in the following figure.
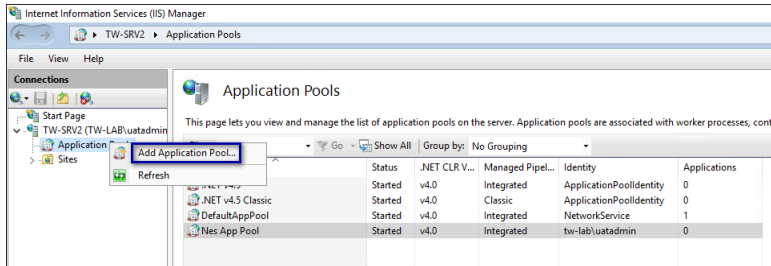
Figure 39: Create New Application Pool

2. In the `Name` field, type NES_AS App Pool, and then click `OK`.

   The following figure provides an example of the `Add Application Pool` window.
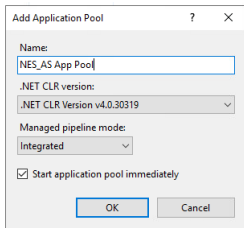
Figure 40: Add New Application Pool

3. Right-click `NES_AS App Pool`, and then select `Advanced Settings`, as shown in the following figure.
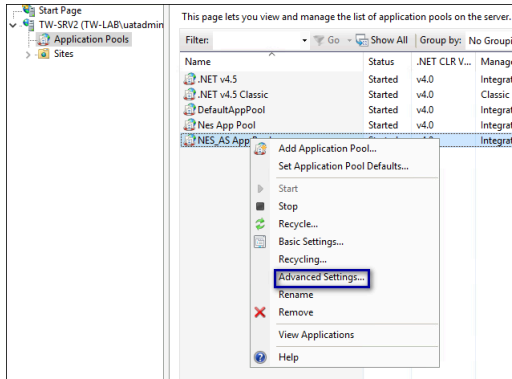
Figure 41: Advanced Settings for Application Pool

4. Click the `Elipses` for the `Identity` parameter, as shown in the following figure.
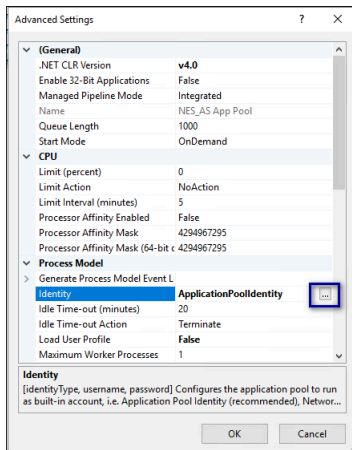
Figure 42: Edit Identity

5. From the **Built-in account** list, select **network service**, as shown in the following figure, and then click **OK**.
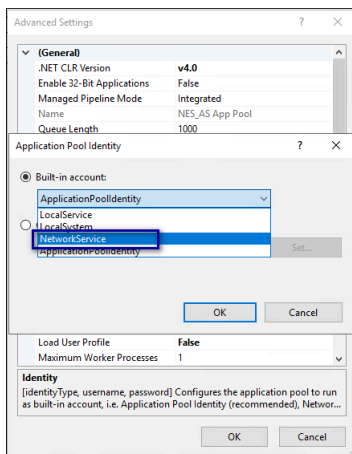
Figure 43: Built-in account list

6. On the **Advanced Settings** window, click **OK**.

7. Right-click **NES App Pool**, and then select **View Applications**, as shown in the following figure.
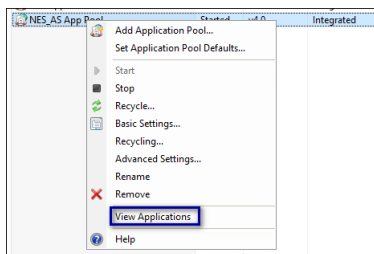
Figure 44: View Applications option

8. If you do not see the NES_AS App Pool application pool, click **Remove filter**, as shown in the following figure.
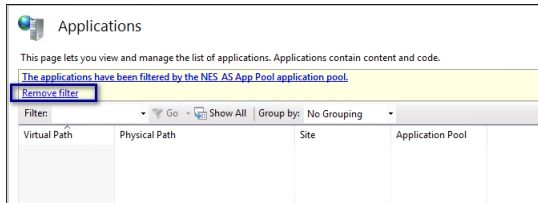
Figure 45: Remove App Pool Filter

9. Right-click **/NES_AS**, and then select **Change Application Pool**, as shown in the following figure.
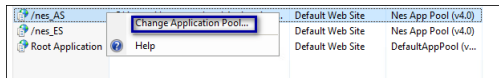
Figure 46: Change Application Pool

10. From the list, select **NES_AS App Pool**, as shown in the following figure, and then click **OK**.
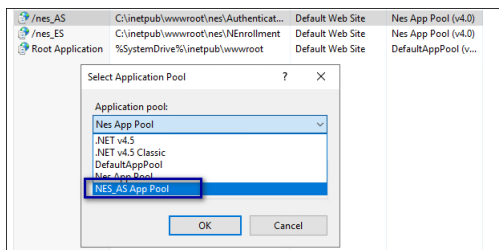
Figure 47: Select Application Pool

11. Select the server name, and then in the Actions pane, select **Restart**, as shown in the following figure.
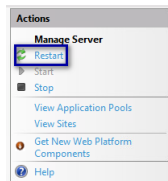
Figure 48: Restart IIS

6.1.6 - Validating the NES Deployment

NES provides users with a web-based interface called the NES Administrator Console to manage NES and monitor the status of the components of the system.

Use the NES Administrator Console to validate the NES deployment.

6.1.6.1 - Access the NES Administrator Console

Perform the following steps to connect to the NES Administrator Console and confirm the status of the system.

About this task

Procedure

1. Connect to the NES Administrator Console in a browser by typing
   https://`nes_server`/`NES_service_name` or http://`nes_server`/`NES_service_name`
   depending on the NES configuration, where:

   - `nes_server` is the Fully Qualified Domain Name (FQDN) of the NES host.
   - `NES_service_name` is the service mapping name for the NES web application. The default
     service mapping name is *nes*.

     For example, https://nes.cwp.company.com/nes.

     Note: The service mapping name for NES is defined during deployment. Contact the person who
     performed the deployment to obtain the NES service mapping name value. Record the URL of ph
     conkeyref="prod_names/nes"/> in *Appendix – Record the CWP Variables*. You will use this URL to
     connect to the NES Administrator Console .

2. Click the `Sign in` button.
   The Sign in dialog opens. Enter username and password.

3. On the main menu, click `About`.
   The `System Diagnostics` page appears.

4. Click `View Full System Diagnostics`.
   The NES server analyzes the status of dependencies and displays the results on the page. The
   following figure shows the various tests that are performed and the status. In this example, all tests
   passed and there was one warning the that L2 certificate will expire soon.

	NetBios Name	TW-LAB		
	Trust		Pass	
Authentication Service				
	Application Name	cwp1_4_rc0_AS		
	Physical Path	C:\inetpub\wwwroot\cwp1_4_rc0\AuthenticationService\		
	Service is Up and Running	https://tw-srv2.tw-lab.local/cwp1_4_rc0_AS	Pass	
	Negotiate Authentication		Pass	
	NTLM Authentication		Pass	
	Secured Communication	HTTPS is enabled	Pass	
Directory and Policy Service				
	Service is Up and Running	https://tw-srv2.tw-lab.local/cwp1_4_rc0	Pass	
	Negotiate Authentication		Pass	
	NTLM Authentication		Pass	
	Secured Communication	HTTPS is enabled	Pass	
	TLS Certificate	TLS certificate is valid.	Pass	
Enrollment Service				
	Application Name	cwp1_4_rc0_ES		
	Physical Path	C:\inetpub\wwwroot\cwp1_4_rc0\NEnrollment\		
	Service is Up and Running	https://tw-srv2.tw-lab.local/cwp1_4_rc0_ES	Pass	
	Negotiate Authentication		Pass	
	NTLM Authentication		Pass	
	Enrollment Service Loop		Pass	
	Secured Communication	HTTPS is enabled	Pass	
	TLS Certificate	TLS certificate is valid.	Pass	
Enrollment Service				
	Application Name	cwp1_4_rc0_ES		
	Physical Path	C:\inetpub\wwwroot\cwp1_4_rc0\NEnrollment\		
	Service is Up and Running	https://tw-srv2.tw-lab.local/cwp1_4_rc0_ES	Pass	
	Negotiate Authentication		Pass	
	NTLM Authentication		Pass	
	Enrollment Service Loop		Pass	
	Secured Communication	HTTPS is enabled	Pass	
	OTP	Get OTP From Enrollment Service	Pass	
	L2 Private Key	Test certificate creation	Pass	
	Certificate Issuer	NTS		
	L2 Cert Validity	The NES L2 certificate will expire on Sunday, January 1, 2023. Contact Nymi Field Support to renew the certificate.	Warning	L2 certificate expires soon
Database			Pass	
	AE State	Off!		-- add 'Column Encryption Setting=Enabled;' to the web.config's SqlConnectionString
	Database Name	Nymi.cwp1_4_rc0		
	Writing AE	PEM == '<PEM-12:06>'.	Pass	
	Reading AE	New PK.PEM: <PEM-12:06>	Pass	
	Clean up	Successfully deleted temporary probe record	Pass	

Figure 49: System Diagnostic Tests

5. Verify the username has administrative access by observing `Policies`, and `Search` in the main menu.

What to do next

The *Nymi Connected Worker Platform—Troubleshooting Guide* provides information about how to resolve issues that you might encounter when you run system diagnostics and attempt to access the NES Administrator Console.

6.1.7 - Configuring NES to support Nymi Lock Control

Edit the active policy in NES to enable the use of Nymi Lock Control.

About this task

Results

Users can use an authenticated Nymi Band to unlock user terminals, when Nymi Lock Control is installed on the user terminal.

Note: If you enabled Nymi Lock Control in NES *after* users already enrolled their Nymi Bands, the Nymi Band user must log into the Nymi Band Application to receive the update in the group policy. The Nymi Band Application will prompt the user to create an internal security key, which allow the Nymi Band to operate with Nymi Lock Control.

6.1.8 - Hardening NES

Hardening is the process of reducing vulnerabilities by eliminating attack vectors and condensing the system's attack surface. Hardening NES can be based on enterprise IT policy or any industry standard hardening guideline.

Before you begin

esnure that the Application Pool Identity account has access to the encryption key.

About this task

Nymi has taken steps to harden IIS according to the CIS Microsoft IIS 10 Benchmarks from the Centre for Internet Security (CIS).

To harden the SQL server based on an industry standard hardening guideline, for example, CIS Microsoft SQL Server Benchmarks, you must secure the external authenticator private keys by encrypting columns, and optionally by securing the usernames.

Perform the following steps on the NES host to encrypt the columns.

Procedure

1. Edit the *C:\inetpub\wwwroot\NES\NEnrollment\web.config* file, and perform the following steps:
   a) Search for the string `SqlConnectionString`.

    b) Add Column Encryption Setting=Enabled; within the <value> </value> attribute tags, as shown in the following example:

```
<setting name="SqlConnectionString" serializeAs="String">
    <value>Data Source=.\SQLEXPRESS;initial catalog=Nymi.{0};Integrated Security=True;
MultipleActiveResultsSets=True;
    Column Encryption Setting=Enabled;</value> </setting>
```

    c) Save the file.

2. Download and install the SQL Server Management Studio (SSMS) software.

3. Open SSMS by using the `Run as Administrator` option.

4. Click `Connect > Database Engine`.

5. On the `Connect to Server` page, if you are using SQL authentication, type the server name and your credentials, and then click `Connect`, otherwise, click `Connect`.

6. Expand `Databases > Nymi.NES > Security > Always Encrypted Keys`. Right click `Column Master Key`, and then select `New Column Master Key`.

7. On the `New Column Master Key` window, perform the following actions:

    a) In the `Name` field, type a name for the key.

       For example, CMK_LocalMachine.

    b) In the `Key store` field, select `Windows Certificate Store – Local Machine`.

       The following figure shows the New Column Master Key page.
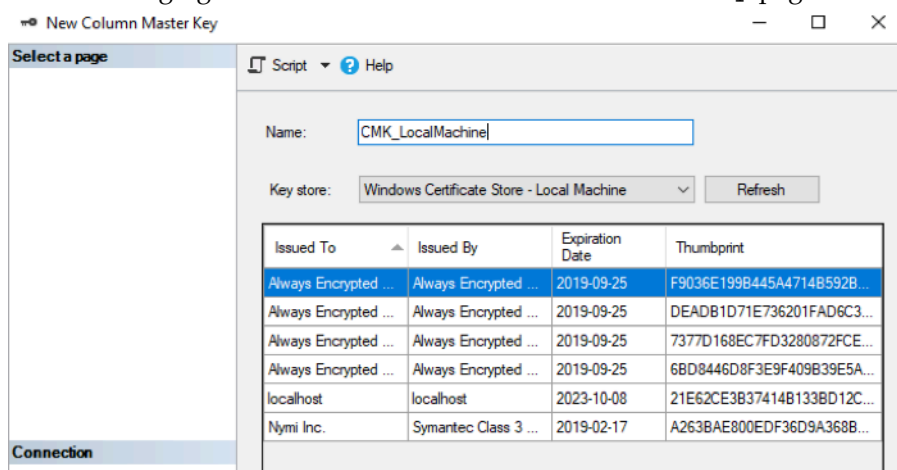
Figure 50: New Column Master Key page

    c) Click `Generate Certificate`.

    d) Click `OK`.

8. While in `Nymi.NES > Security > Always Encrypted Keys`, right-click `Column Encryption Keys`, and then select `New Column Encryption Key`.

9. On the `New Column Encryption Key` page, perform the following actions:

    a) In the `Name` field, type a name for the key.

       For example, CEK_LocalMachine.

    b) In the `Column master key` field, select the name of the column master key that you created.

For example, CMK_LocalMachine.

The following figure shows the New Column Encryption Key page.
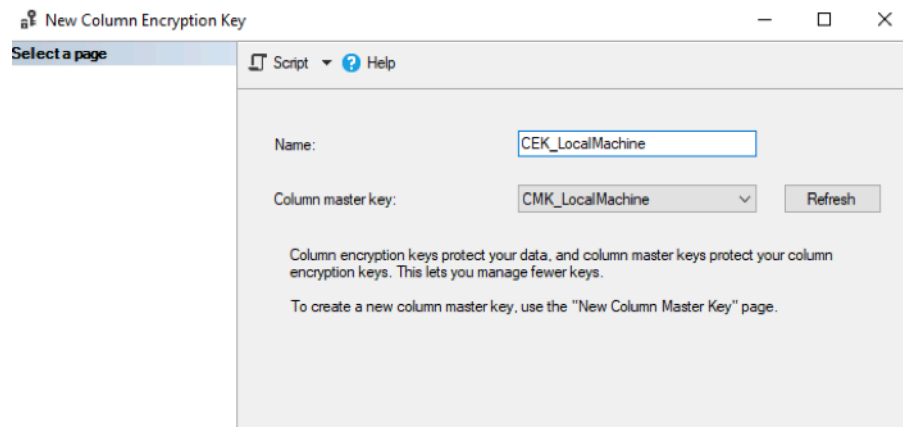
Figure 51: New Column Encryption Key page

   c) Click **OK**.

10. In the left navigation pane, expand **Database > Nymi.NES > Tables**.

11. Under tables, right-click **nub.PrivateKeyStore**, and then select **Encrypt Columns**.
The Always encrypted wizard opens.

12. On the Introduction page, click **Next**.

13. On the Column Selection page, perform the following actions:

   a) Enable **Apply one key to all checked columns** and ensure that **CEK_LocalMachine** appears in the list to the right.

   b) In the table, select **PEM**, and then from the **Encryption Type** list, select **Randomized**.

   c) In the table, select **DER**, and then from the **Encryption Type** list, select **Randomized**.

     The following figure shows the Column Selection page.
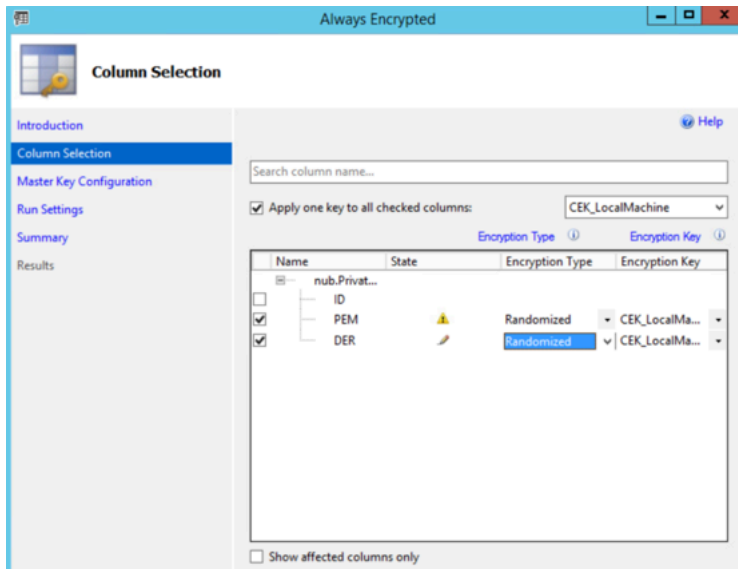
Figure 52: Column Selection page

    d) Click **Next**.

14. On the `Master Key Configuration` page, click **Next**.

15. On the `Run settings` page, leave the default value **Proceed to finish now**, and then click **Next**.

16. On the `Summary` page, review the results, and then click **Finish**.

17. Close `SSMS`.

What to do next

Ensure that NES Application Pool Identity has access to the encryption key:

1. Open `Manage Computer Certificates`.

2. Expand **Personal**, and then right-click **Always Encrypted Certificate** and then select **All Tasks > Manage Private Keys**. The `Permissions for Always Encrypted Certificate` window appears.

3. Click **Add**.

4. In the `Select Users, Computers, Service Accounts, or Groups` windows, type the Application Pool Identity account, and the select **Check Names**.

5. Click **OK**.

6. Click **OK**.

6.1.8.1 - Encrypt usernames in the NES Database

You have the option to encrypt the usernames in the audit.UserCore table and the nub.UserCore table.

Procedure

1. Encrypt the audit.UserCore table by performing the following steps:

a) In `Tables`, right-click **audit.UserCore**, and then select **Encrypt Columns**.

b) On the Introduction page, click **Next**.

c) Enable **Apply one key to all checked columns** and ensure that **CEK_LocalMachine** appears in the list to the right.

d) In the **Tables**, select **username**, and then from the **Encryption Type** list, select **Deterministic**.

e) Click **Next**.

f) On the `Master Key Configuration` page, click **Next**.

g) On the `Run settings` page, leave the default setting **Proceed to finish now**, and then click **Next**.

h) On the `Summary` page, review the results, and then click **Finish**.

2. Encrypt the nub.UserCore table by performing the following steps:

a) In `Tables`, right-click **nub.UserCore**, and then select **Encrypt Columns**.

b) On the Introduction page, click **Next**.

c) Enable **Apply one key to all checked columns** and ensure that **CEK_LocalMachine** appears in the list to the right.

d) In the **Tables**, select **username**, and then from the **Encryption Type** list, select **Deterministic**.

e) Click **Next**.

f) On the `Master Key Configuration` page, click **Next**.

g) On the `Run settings` page, leave the default setting **Proceed to finish now**, and then click **Next**.

h) On the `Summary` page, review the results, and then click **Finish**.

6.2 - Deploy NES in a High Availability Configuration

In order to ensure continuous service delivery in a production environment, Nymi Server components can be deployed in a highly-available configuration. These components includes the Nymi Enterprise Server, the Nymi Agent (if deployed on centralized servers), and the Nymi WebAPI (if enabled). This section of the guide provides deployment information for setting up a centralized NES cluster and a Nymi Agent cluster for high availability and scalability. The centralized NES and Nymi Agent clustering architecture is defined in *Centralized Deployment Reference Architecture For NEE versions 2.5, 2.6 and 3.2*.

Introduction

This section will focus on NES and Nymi Agent clusters deployment. However, the following will not be covered:

• SQL Server AlwaysOn Availability Group Deployment

- Hardening of SQL Server like TLS communication and SQL Server transparent data encryption (TDE)
- Load balancer deployments; contact your Nymi Solution Consultant for more information.

6.2.1 - Overall Deployment Process

About this task

For high availability deployments, the deployment process includes the following steps.

1. Deploy SQL AlwaysOn Availability Group: a minimum of two SQL Server instances (SQL Server 2012+ Enterprise Edition, SQL Server 2016+ Standard Edition) with synchronous commit. The deployment will also need an additional server as the quorum witness depending on the quorum modes.
2. Deploy NES instances.

   Note: When you configure NES, on the `IIS` tab, ensure that you specify the service account for the `Application Pool Identity`.
3. Configure a load balancer for the NES cluster nodes and make note of the IP address and URL.
4. Deploy the Nymi Agent instances.
5. Configure the load balancer for the Nymi Agent cluster.

6.2.2 - Deploy the NES Cluster

For NES cluster deployments, a SQL Server AlwaysOn Availability Group with at least two SQL Server instances, two or more NES servers, and a load balancer is required.

6.2.2.1 - Deploy SQL Server AlwaysOn Availability Group

About this task

The deployment steps for SQL Server AlwaysOn Availability Group is beyond the scope of this document. Refer to this Microsoft documentation for details. Before the SQL Server AlwaysOn Availability Group deployment, perform the following prerequisites:

Procedure

1. Designate a SQL Server instance as the primary replica during deployment.
2. Use the provided database DDL script to create the NES database on the primary replica.
3. Enable TCP on port 1433 for client connections on each SQL Server instance.
4. Windows authentication is enabled on each SQL Server Instance.
5. SQL Server Browser service's start mode is set to automatic on all SQL Server nodes.
6. SQL Server agent service's start mode is set to automatic on all SQL Server nodes.
7. Designate the name and IP address for the Availability Group Listener, this will be used for NES to connect to the NES database.

8. There is a valid AD account for NES to connect to the NES database. The account needs to have read/write permission on the NES database. To use Kerberos authentication, the SQL Server Service Principal Name (SPN) needs to be set for all SQL Server nodes and the AG Listener under the account.

9. To enable SQL Server transparent data encryption (TDE) in the Availability Group, create a master key and import the master key into every SQL Server instance.

Results

After prerequisite completion, follow Microsoft documentation to deploy the Availability Group. In order to allow automatic failover of the Availability Group, there must be at least one secondary replica configured for synchronous commit with the primary replica.

6.2.2.2 - Deploy NES Instances

This section includes information for deploying NES instances for the NES cluster deployment.

About this task

Ensure that the Subject Alternative Names(SANs) for the TLS certificate has the DNS entries for all the FQDNs.

Procedure

Follow the steps in the *Installing NES* section to install NES on the individual servers. For the deployment, the following information is applicable:

a) For the NES_URL value, use the fully qualified domain name (FQDN) of the NES virtual server instead of the FQDN of the individual server.

b) Use the name or address of the respective SQL Server AlwaysON Availability Group listener for the NES database connection. In addition, the database connection string should include IntegratedSecurity=SSPI; MultiSubnetFailover=True

c) If you use SSL offloading for NES cluster, ensure that you enable HTTP.

Note: When there is a dedicated link between the load balancer and NES that cannot be intercepted, use HTTP off-loading.

6.2.2.3 - Configure the NES Cluster on the Load Balancer

About this task

Follow documentation for the load balancer used in your environment for configuring the NES cluster (virtual server) and ensure the following is configured correctly.

Procedure

1. Include all the NES instances as the backend servers for the virtual server.

2. Configure the cluster in active-active mode

3. Make source IP based session affinity (persistence) is configured.

4. For Layer 7 load balancer, SSL/TLS offloading can be configured for NES 3.2, and SSL/TLS bridging can be configured for NES 2.5, 2.6 and 3.2.

5. The URL for the liveness test of the NES instances is: *<nes_admin_service>/nes/ping* where *<nes_admin_service>* is the name of the NES Admin service.

Configure SSL/TLS Bridging

Follow this section for configuring SSL/TLS bridging.

About this task

Procedure

1. Each NES instance has HTTPs enabled with a valid TLS certificate for the instance during the installation

2. There is a valid TLS certificate for the cluster's FQDN

3. The cluster's IP address is allocated to the load balancer and is bound to the cluster's FQDN in the respective DNS.

4. Import the TLS certificate into the load balancer, and bind it to the NES cluster.

5. When applicable, ensure the signing CA certificate(s) for each NES instance's TLS certificate is trusted by the load balancer

6. Configure the load balancer to use the HTTPs URLs of the individual NES instance.

Configure SSL/TLS Offloading

The following steps are applicable for configuring SSL/TLS offloading for NES.

About this task

Procedure

1. Each NES instance has HTTPs enabled during the installation.

2. There is a valid TLS certificate for the cluster's FQDN.

3. The cluster's IP address is allocated to the load balancer and is bound to the cluster's FQDN in the respective DNS.

4. Import the TLS certificate into the load balancer, and bind it to the NES cluster.

5. Configure the load balancer to use the HTTP URLs of the individual NES instance.

6.2.3 - Deploy the Nymi Agent Cluster

About this task

For a Nymi Agent cluster, two or more servers are required. The following section includes information for deploying the Nymi Agent cluster.

Procedure

1. When the Nymi cluster needs to support thin-client or RDP, the cluster must be configured in active-passive mode.

2. When the Nymi Agent cluster does not need to support thin-client, RDP, and WebApi, the cluster can be configured in active-active mode.

3. When the Nymi Agent cluster needs to support WebApi, two clusters must be configured on the same load balancer (or load balancer cluster). One cluster for the websocket service on port 9120, and one for the WebApi. Whether both the clusters can be configured in active-active mode or not will depend on the capability of the load balancer. The same session affinity/persistence needs to be applied across the two clusters.

4. It is not possible to use WebApi in thin-client or RDP environments.

6.2.3.1 - Deploy Nymi Agent Instances

Follow *Installing the Nymi Agent* to install the Nymi Agent on individual servers.

About this task

6.2.3.2 - Configure the Load Balancer Without WebApi Support

About this task

Follow documentation for the load balancer used in your environment for configuring the Nymi Agent cluster (virtual server) and ensure following is configured correctly:

Procedure

1. Include all the Nymi Agent instances as the backend servers for the virtual server.

2. The virtual server's service port should be TCP/9120.

3. The backend server port should be TCP/9120.

4. Configure the virtual server in active-active mode if it does not need to support thin-client, RDP.

5. Ensure the source IP based session affinity (persistence) is configured when the virtual server is configured in active-active mode.

6. For liveness tests on the backend servers, use TCP connection test on port 9120 of the backend servers.

7. Configure the liveness test for the Nymi Agent instances to use TCP connection on the designated websocket port.

6.2.3.3 - Configure the Load Balancer With WebApi Support

About this task

For WebApi, two clusters are required, one for the websocket service on port 9120, and one for the WebApi. Whether the cluster can be configured in active-active mode or not will

depend on the capability of the load balancer. If the load balancer supports session affinity across multiple virtual servers (for example, with Citrix Netscaler's *Persistence Groups*, and F5's *Match Across options)*, it is possible to configure both Nymi Agent clusters in active-active mode. Active-active mode will also require source IP based session affinity so that all the traffic from a specific source IP will be directed to the same Nymi Agent instance in both clusters.

Procedure

Configure the Load Balancer for the Websocket Service on Port 9120

About this task
Follow documentation for the load balancer used in your environment for configuring the virtual server for the websocket service on port 9120 and ensure the following is configured correctly:

Procedure

1. Include all the Nymi Agent instances as the backend servers for the virtual server.
2. The virtual server's service port should be TCP/9120.
3. The backend server port should be TCP/9120.
4. For liveness tests on the backend servers, use TCP connection test on port 9120 of the backend servers.
5. Configure the virtual server in active-active mode or active-passive mode according to the capability of the load balancer as specified above.

Configure the Load Balancer for the WebApi Service

About this task
In addition to the virtual server for the the websocket service on port 9120, an additional virtual server for the the WebApi service on the load balancer must be configured as follows:

Procedure

1. Include all the Nymi Agent instances as the backend servers for the virtual server.
2. The virtual server's service port should be TCP/443 for SSL/TLS offloading.
3. The backend server port should be TCP/*<WebApi_port>*, where *<WebApi_port>* is the WebApi service port on the Nymi Agent instances
4. For liveness tests on the backend servers, use TCP connection test on the backend server port *<WebApi_port>*.
5. Configure the virtual server in active-active mode or active-passive mode according to the capability of the load balancer as specified above.

6.2.3.4 - Configure SSL/TLS Offloading

About this task

When a layer 7 load balancer is used, it is recommended to configure SSL/TLS offloading for the WebApi virtual server as follows:

Procedure

1. Configure the backend server's WebApi to use plain websocket without TLS.
2. Configure the virtual server to connect to the backend servers without TLS
3. Ensure there is a valid TLS certificate for the virtual server's FQDN
4. Ensure the virtual server's IP address is allocated to the virtual server's FQDN.
5. Import the TLS certificate into the load balancer, and bind it to the WebApi virtual server.

6.2.4 - Setting Service Principal Names

This section provides information on creating for NES. When you use a remote SQL server, NES uses the service account to access the SQL server. During the NES deployment, you define the IIS Application Pool Identity for the NES instance as the NES service account. You must create HTTP Service Principal Names (SPNs) for the Application Pool Identity account. Creating SPNs requires sufficient privileges.

Note: If the Application Pool Identity account is changed, the SPNs need to be re-registered with the new identity account. Re-registering the SPNs involves two steps

1. Removing the old SPNs registered under the old Application Pool Identity account
2. Register the SPNs with the new Application Pool Identity account.

6.2.4.1 - Removing SPN

About this task

To remove an SPN registered under the old Application Pool Identity, complete the following.

Note: To check the existing SPN entries associated with the App Pool Account, run the command setspn -I %computername% | <App_Pool_Identity> . Only include <App_Pool_Identity> if the Application Pool identity is not a local account, such as NetworkService, or LocalSystem.

Procedure

Open a command prompt as an Administrator and type:

- setspn -d HTTP/%computername% %computername% and
- setspn -d HTTP/%computername%.%userdnsdomain% %computername%

where:

- *`%computername%`* is the computer name of the NES server.
- *`%userdnsdomain%`* is the DNS name or Fully Qualified Domain Name (FQDN) of the domain.
- *`App_Pool_Identity`* is the App Pool Identity used for the NES installation. Replace the last argument with the application pool identity if an AD account is used as the appliction pool identity.

6.2.4.2 - NES Cluster SPN Creation

About this task

For an NES cluster, create an SPN for each NES node, the FQDN of the each NES node, and the public FQDN of each NES node.

Procedure

1. Open a command prompt as an Administrator and type setspn -S HTTP/%computername%:*port#* %computername%|*App_Pool_Identity*

   where you replace:

   - *`App_Pool_Identity`* is the service account.
   - *`port#`* specifies the port when the default service port is not used. If NES is not configured for traffic on the standard ports (HTTP/80, HTTPs/443), it is important that you specify the port. e,g. setspn -S HTTPs/winserver:8443 winserver, if it is listening on port 8443 instead of 443.

2. Type setspn -S HTTP/%computername%.*userdomainport#* %computername%|*App_Pool_Identity*

   where you replace:

   - *`userdomain`* is the domain name of the NES instance.
   - *`App_Pool_Identity`* is the service account.
   - *`port#`* specifies the port when the default service port is not used. If NES is not configured for traffic on the standard ports (HTTP/80, HTTPs/443), it is important that you specify the port. e,g. setspn -S HTTPs/winserver:8443 winserver, if it is listening on port 8443 instead of 443.

3. If the NetBIOS domain name differs from the public FQDN of the NES cluster, type setspn -S HTTP/%computername%.*publicdomainport#* %computername%|*App_Pool_Identity*

   where you replace:

   - *`publicdomain`* is the FDQN domain name of NES cluster.
   - *`App_Pool_Identity`* is the service account.
   - *`port#`* specifies the port when the default service port is not used. If NES is not configured for traffic on the standard ports (HTTP/80, HTTPs/443), it is important that you specify the port. e,g. setspn -S HTTPs/winserver:8443 winserver, if it is listening on port 8443 instead of 443.

7 - Set Up a Centralized Nymi Agent

When your environment uses iOS devices, thin clients, and web-based Nymi-enabled Applications, deploy a centralized Nymi Agent on a Windows server in the environment, for example, the NES server.

7.1 - Installing the Nymi Agent

Install the Nymi Agent application, which is included in the Nymi Runtime installation package, on a machine in the environment.

About this task

When you install the Nymi Runtime software, you can choose to install the Nymi Agent application only.

Note: You can install the Nymi Agent silently by typing the following command: **"Nymi Runtime Installer.exe" /exenoui InstallEndpoint=0 /q**.

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the *..\nymi-sdk\windows\setup* folder, run the *Nymi Runtime Installer version.exe* file.
4. On the `Welcome` page, click **Install**.
5. On the `User Account Control` page, click **Yes**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **Next**.
7. On the `Nymi Runtime Setup` page, expand **Nymi Runtime**.
8. Select **Nymi Bluetooth Endpoint**, and then select **Entire feature will be unavailable**.

   The following figure provides an example of the `Nymi Runtime Setup` window with option to make **Nymi Bluetooth Endpoint** unavailable.

Figure 53: Nymi Bluetooth Endpoint feature will be unavailable

9. Observe that `Nymi Bluetooth Endpoint` is not available, as shown in the following figure, and then click `Next`.
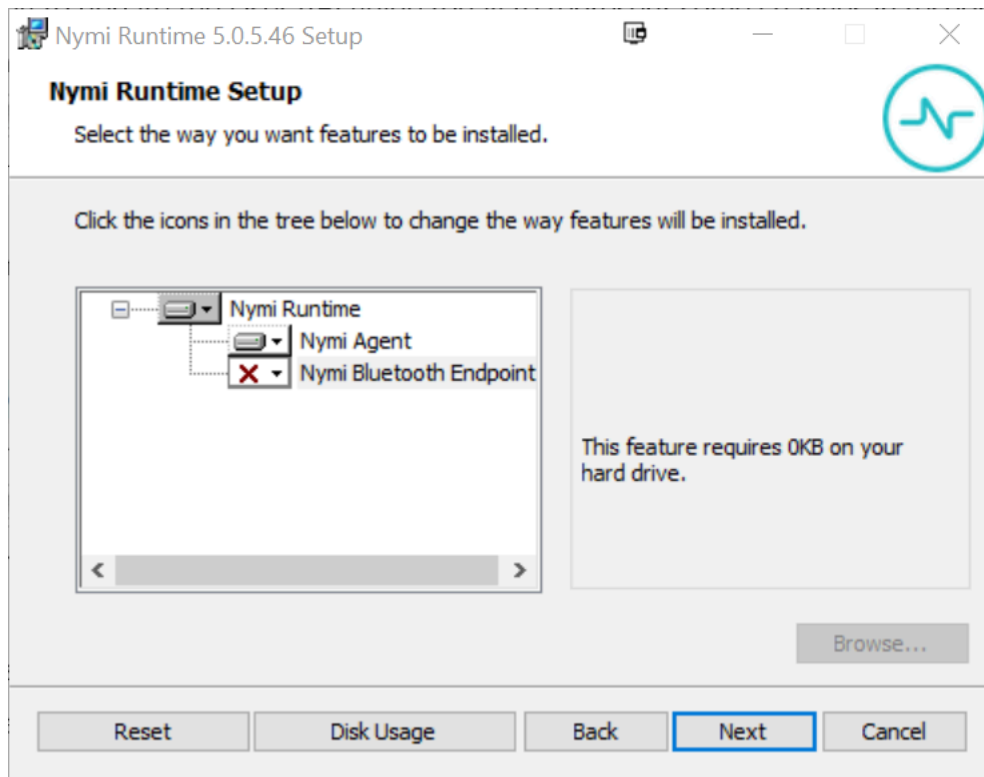
Figure 54: Nymi Bluetooth Endpoint feature is not available

10. On the `Service Account` window, click **Next**.

11. On the `Ready to install` page, click **Install**.

12. Click **Finish**.

13. On the `Installation Completed Successfully` page, click **Close**.

Results

Note: Take the following TCP port requirements into consideration:

- Nymi Agent receives incoming WebSocket connections on TCP port 9120, which is used for communication with Nymi Bluetooth Endpoint.
- Nymi WebAPI receives incoming WebSocket connections on the TCP port configured for Nymi WebAPI connections (default 8080 when using the ws protocol, and default 4443 when using the wss protocol).

Ensure that firewalls allow incoming communication on these ports on the server that runs the Nymi Agent.

7.1.1 - Configuring the Nymi Agent toml File for Nymi WebAPI

If user terminals access web-based NEAs, you must enable the centralized Nymi Agent to use the Nymi WebAPI. By default, the Nymi Agent does not use Nymi WebAPI.

Before you begin

On the centralized Nymi Agent server, ensure that:

- Each network interface uses a distinct TCP port that is not 9120/tcp.
- The machine has connectivity to NES
- Network Address Translation (NAT) does not exist between the Nymi Agent machine and the user terminals.
- Nymi Agent can co-locate with the NES (ensure that you use distinct TCP ports)

Note: The Nymi Agent must be able to receive incoming WebSocket connections on TCP port 9120 (used for communication with Nymi Bluetooth Endpoint) and on the TCP port configured for Nymi WebAPI connections (default 8080 when using the ws protocol, and default 4443 when using the wss protocol). Ensure that these ports are open bi-directionally in the firewall on the machine that runs the Nymi Agent.

About this task

To enable Nymi WebAPI, perform the following step to define configuration settings in a *nymi_agent.toml* file on the centralized Nymi Agent server.

Procedure

1. Rename the *C:\Nymi\NymiAgent\nymi_agent_default.toml* file to *C:\Nymi\NymiAgent \nymi_agent.toml*
2. Edit the *nymi_agent.toml*, configure and uncomment the following parameters:

Table 6: Nymi Agent TOML File

Setting and Default Value(s)	Description
log_level = "warn"	Defines the logging level. Specify one of the following values: - error—to log only errors - warn—to log both errors and warnings - info—to log errors, warnings, and activity - debug—to log everything including debugging information
`nea_name = "NymiWebAPI"`	Required for Nymi WebAPI. Sets the NEA name for the embedded NEA application.

Setting and Default Value(s)	Description
`nes_url = "https://server.name.local.com"` For example, https://myserver.name.local.com	Required for Nymi WebAPI. The host URL for the NES server. Include only the protocol and hostname portion of the URI. For example, replace https://server.name.local with your nes_url.
directory_service_id = "NES"	Required for Nymi WebAPI. Specifies the directory service name for NES. For example if your NES URL is https://server.name.local.com/NES, the directory name is NES.
Certificate bundle in PEM format for the signing CA certificate chains for the TLS certificates that are used by NES and WebAPI.	The TLS client root CA certificate bundle to use when communicating with NES. If it is not specified a built-in bundle containing well known root CAs is used. Specify the path to a CA certificate or bundle to customize the trusted CA bundle using the PEM format.
protocol = "wss" or *protocol = "ws"*	Required for WebAPI. Defines the protocol that is supported by the Nymi WebAPI server. Uncomment one of the parameters: • *protocol = "wss"* to support a secure WebSocket using TLS. Nymi recommends that you configure secure WebSocker using TLS in production environments. • *protocol = "ws"* to support a plain WebSocket.
port = 4443 or *port = 8080*	Required for WebAPI. Defines the server port on which to listen for Nymi WebAPI client WebSocket connections. The parameter you uncomment depends on the *protocol* configuration: • For the *ws* protocol, uncomment *port = 8080*. • For the *wss* protocol, uncomment *port = 8080*. **Note:** You can set an alternate port using this setting.
cacertfile = "/path/to/certfile.pem"	Specifies the path to the PEM-formatted certificate bundle for the signing CA certificate chains for the TLS certificates that are used by NES and WebAPI.
certfile = "/path/to/certfile.pem"	The path to the server certificate in PEM format.
keyfile = "/path/to/keyfile.pem"	The path to the server certificate private key in PEM format.

7.1.2 - Managing Security and Certificates

System Administrators need to obtain and import TLS key pairs that include certificates for your environment and for the Nymi WebAPI.

To ensure that trusted communication is configured and TLS is used by the WebSocket, obtain and install the following certificates:

- TLS Server Certificate chain including any intermediate CA certificates in base64 PEM format (note that the host certificate cannot be a wildcard certificate)
- Private key corresponding to the TLS server certificate, in base64 PEM format (the private key cannot be encrypted)
- Certificate of the root Certificate Authority (CA) issuing the TLS server certificate, in base64 PEM format

You must install these three PEM files at the location that is specified in the *nymi_agent.toml* file, to ensure that the Nymi Agent can communicate with the Nymi-enabled Application.

The Nymi WebAPI needs to connect to NES over HTTPS. The NES TLS server certificate must be issued by a Root CA trusted by the Nymi WebAPI. If the Root CA is not trusted by the workstation install the root CA certificate in the Trusted Root Certification Authorities container for the local machine. See Microsoft documentation for information about installing Trust Root Certificates: https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate.html

For example, you can install the certificates in the certificate keystore at the following location: *C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Nymi\NSL*

Note: For additional information about importing certificates, see the Nymi Connected Worker Platform—Deployment Guide.

Note: Ensure that you have configured the certificate settings in the *nymi_agent.toml* configuration file. For more information see the, *Configuration Overview* section.

8 - Install and Configure Endpoints

Install and configure the Nymi software and dependencies on the enrollment terminal and iOS devices that access web-based applications.

8.1 - Set Up the Enrollment Terminal

Before a user can enroll and authenticate the Nymi Band, the NES Administrator must perform the following actions on at least one machine in the environment (the enrollment terminal). You cannot use a thin client as an enrollment terminal.

* Insert the Nymi-supplied Bluetooth adapter into an available USB port.
* Optionally, insert a Nymi-verified NFC reader into an available USB port.
* Install the Nymi Band Application. The Nymi Band user requires physical access to the enrollment terminal.
* Set the NES_URL registry key.

Note: The Nymi Band Application includes the Nymi Runtime software.

8.1.1 - Bluetooth Adapter Placement

The enrollment terminal and each user terminal requires a Bluetooth adapter. The Bluetooth Low Energy (BLE) radio antenna in the Nymi-supplied BLED112 USB Adapter provides seamless Bluetooth capability between the Nymi Band and devices such as a laptop computer.

To ensure optimal system performance, place the Bluetooth adapter in a location that meets the following criteria:

* Is in clear line of sight to the Nymi Band.
* Is on the same side of the computer that you wear your Nymi Band.
* Is near the computer keyboard.

Note: The presence of liquids between the Nymi Band and Bluetooth adapter negatively affects the Bluetooth signal quality. This includes beverages and the human body. If Bluetooth (BLE) taps behave unexpectedly, consider another placement for the Bluetooth adapter, or edit the Nymi Bluetooth Endpoint configuration file to adjust the signal strength thresholds to perform a BLE tap (see *Edit the nbe.toml File*).

8.1.2 - Importing the Root CA certificate

Perform the following steps only if the Root CA issuing the NES TLS server certificate is not a Trusted Root CA (for example, if a self-signed TLS server certificate is used for NES). Install the Root CA on each user terminal to support the establishment of a connection with the NES host.

About this task

While logged into the user terminal as a local administrator, use the `certlm` application to import the root CA certificate into the Trusted Root Certification Authorities store. For example, on Windows 10, perform the following steps:

Procedure

1. In `Control Panel`, select **Manage Computer Certificates**.
2. In the `certlm` window, right-click **Trusted Root Certification Authorities**, and then select **All Tasks > Import**.

   The following figure shows the `certlm` window.
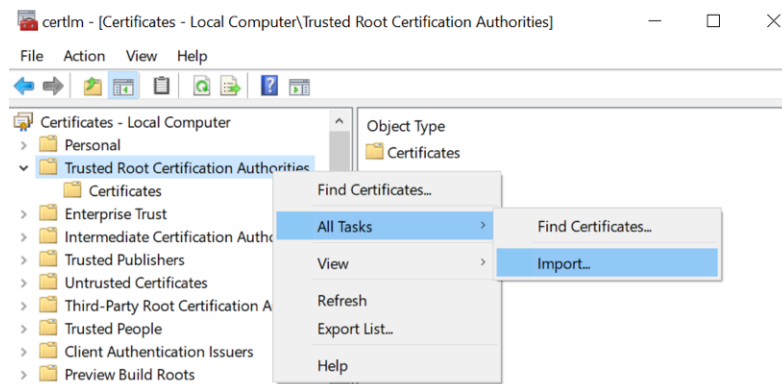
Figure 55: certlm application on Windows 10

3. On the `Welcome to the Certificate Import Wizard` screen, click **Next**.

   The following figure shows the `Welcome to the Certificate Import Wizard` screen.

Figure 56: Welcome to the Certificate Import Wizard screen

4. On the `File to Import` screen, click **Browse**, navigate to the folder that contains the root certificate file, select the file, and then click **Open**.

5. On the `File to Import` screen, click **Next**.

The following figure shows the `File to Import` screen.
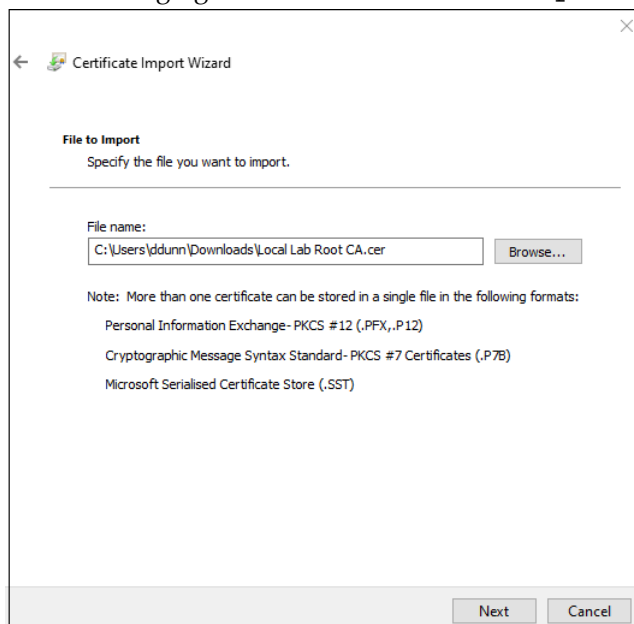
Figure 57: File to Import screen

6. On the `Certificate Store` screen, accept the default value **Place all certificates in the following store** with the value **Trusted Root Certification Authorities**, and then click **Next**.

7. On the `Completing the Certificate Import Wizard` screen, click **Finish**.

8.1.3 - Install the Nymi Band Application

Perform the following steps to install the Nymi Band Application on each enrollment terminal that you will use to enroll and authenticate users to their Nymi Bands.

You can perform a customizable installation, or a silent installation.

Note: The bluetooth (BLE) driver is installed with the installation of Nymi Runtime. The BLE driver may also be installed separately by going to the Nymi SDK package and installing the *BleDriver .msi* file.

8.1.3.1 - Performing a customizable Nymi Band Application installation

Perform the following steps to install the Nymi Band Application on a network device.

About this task

Procedure

1. Download the Nymi Band Application package.
2. Double-click to run the Nymi-Band-App-installer-v_`version`.exe installer.
3. Follow the prompts in the Nymi Band Application installation wizard and when prompted, install all the prerequisite packages and BLE device driver from Silicon Labs.
4. In the `Windows Services` applet, confirm that you can see the Nymi Agent and Nymi Bluetooth Endpoint services, and that the status of each service is `Running`.
5. Close the Nymi Band Application.

8.1.3.2 - Performing a silent Nymi Band Application Installation or Upgrade

Perform the following steps to install or upgrade the Nymi Band Application silently, for example, when you want to install the software remotely by using a software distribution application.

About this task

Procedure

1. Save the Nymi Band Application package, provided to you by your Nymi Solution Consultant.
2. Launch the command prompt as administrator.
3. From the folder that contains the Nymi Band Application, type *Nymi-Band-App-installer-v_`version`.exe /exenoui /q*

   Where you replace `version` with the version of the Nymi installation file.

The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, the Nymi Band Application and Nymi Runtime applications appear in the `Program and Features` applet.

Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

8.1.4 - Configuring the Nymi Enterprise Server URL

After you install the Nymi Band Application, perform the following steps to ensure that the enrollment process connect to the correct Nymi Enterprise Server(NES).

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.

   Note: If you installed the Nymi Band Application on a Citrix server, set navigate to HKEY_CURRENT_USER instead of HKEY_LOCAL_MACHINE

   .
4. Right-click **NES**, and then select **New > String value**.
5. In the **Value** field, type URL.
6. Double-click **URL** and in the **Value Data** field, type https://nes_server/ NES_service_name/ or http://*nes_server*/*NES_service_name* depending on the NES configuration

   where:

   - *nes_server* is the FQDN of the NES host. The FQDN consists of the hostname.domain_name. You can also find the FQDN by going to the server on which you deployed NES viewing the properties of the computer. The *nes_server* is the value that appears in the **Full computer name** field.
   - *NES_service_name* is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but it is recommended that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
7. Click **OK**.

8.2 - Set Up iOS User Terminals for Authentication Tasks

To use the Nymi Band to perform authentication tasks in web-based Nymi-enabled Applications(NEAs) on iOS devices, you must install the Nymi Application on each iOS device.

Nymi recommends that you use a mobile device management (MDM) system to perform the following actions on enrolled iOS devices.

Perform the following actions

- Import the Root CA certificate for NES (when the Root CA that issued the certificate is not a trusted CA).

  Apple recommends deploying certificates with a Mobile Device Management (MDM) system. Certificate payloads are automatically trusted for SSL when installed with Configurator, MDM, or as part of an MDM enrollment profile.

  Apple Support provides more information.

  Note: If you manually import a device profile, you must enable trust for SSL/TLS. Apple Support provides more information.
- Enable Bluetooth. The Nymi Application communicates with the Nymi Band by using the integrated Bluetooth adapter on the iOS device.
- Deploy the Nymi Application.
- Manage the Nymi Application.
- Configure the Nymi Application.

Note: iOS devices that access web-based NEAs do not make use of an *nbe.toml* file to define the location of the centralized Nymi Agent. The webpage or NEA defines the Nymi Agent location and communication port number.

8.2.1 - Preparing the Mobile Device Management System

Perform the following in your Mobile Device Management(MDM) System.

Before you begin
Enroll one iOS device into the MDM.

About this task
Nymi recommends that you deploy the Nymi Application to one iOS device and test the configuration before deploying the Nymi Application to all iOS devices in your environment.

Procedure

1. Extract the Nymi SDK package to the computer that you use to access MDM.
2. Upload the installation package *../ios/Apps/Nymi Application.ipa* to MDM.
3. Upload the updated *../ios/Apps/Preferences.plist* file.
4. Create a new device profile and perform the following actions:

   - Enable Bluetooth
   - Add the *Preferences.plist* file
   - Add the *Nymi Application.ipa* file

- Disable the NSURL Session WebSocket option in Safari.

5. Push the device profile to the iOS device.

What to do next

After your Mobile Management System pushes the device profile that contains the Nymi Application and associated configuration options, the Nymi Application appears as an application on the iOS device.

8.2.2 - Calibrating the Nymi Application

The location of the integrated Bluetooth adapter on an iOS device can differ between each model, and the tap behaviour of the Nymi Band differs when a user wears PPE. Nymi provides you with the Nymi Calibration tool to help you find the location of the Bluetooth adapter and to configure the tap behaviour of the Nymi Band. Nymi recommends that you use the tool on one device before you deploy Nymi Application to other iOS devices.

Before you begin

Ensure that you prepare in the following manner:

- Nymi provides the application through TestFlight. Provide Nymi with the Apple ID of each iOS user
- Wear an authenticated Nymi Band.
- Wear any PPE that an operator of the iOS device wears over top of the Nymi Band

About this task

Perform the following steps on the iOS device that has the Nymi Application.

Procedure

1. Read the instructions that you receive in the email from TestFlight. After you accept the invitation from TestFlight, you will get an email with a redeem code.

2. Download and install the TestFlight application from the App Store.

3. Launch the TestFlight application, and when prompted, type the redeem code.

4. Wear an authenticated Nymi Band and start the Nymi Calibration application.

5. When prompted to allow the Nymi Calibration application access to the Bluetooth adapter, as shown in the following figure.
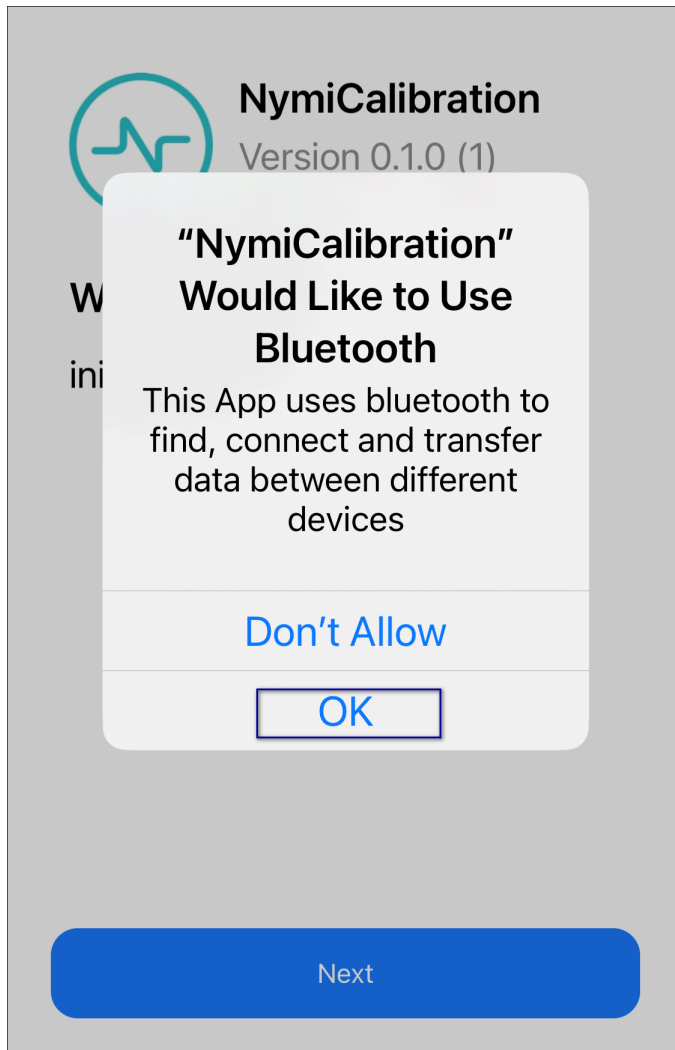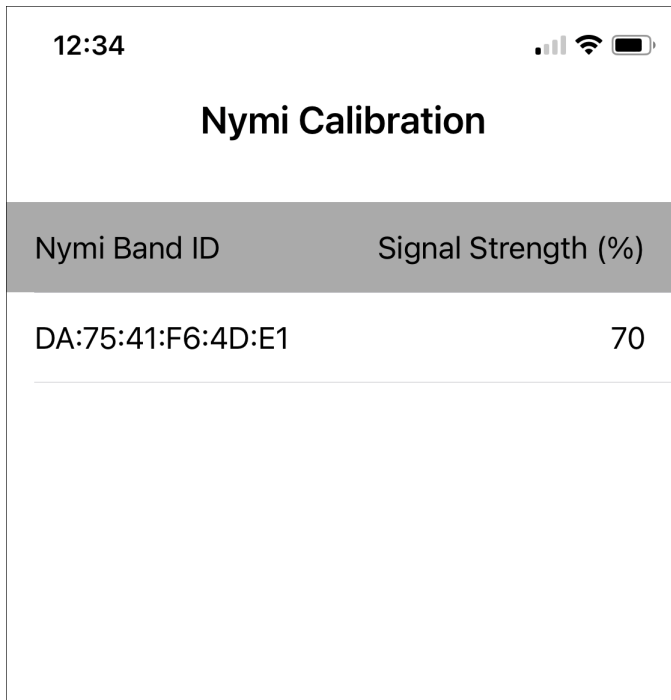
6. Click **Next**.

The Nymi Calibration appears on screen and displays the MAC address of all Nymi Bands that are within Bluetooth range of the iOS device and signal strength of the current location of each Nymi Band.

7. Determine the location of the integrated Bluetooth adapter by placing the Nymi Band in various positions on the back of iOS device. Make note of the location that displays the highest signal strength percentage.

The closer the Nymi Band is to the Bluetooth adapter, the higher the signal strength percentage.

The following figure provides a example of a single Nymi Band that is in Bluetooth range of the iOS device and the location of the Nymi Band has a high signal strength percentage.

12:34	📶 📶 🔋

Nymi Calibration

Nymi Band ID	Signal Strength (%)
DA:75:41:F6:4D:E1	70

8. Place a sticker over the location on the iOS device that has the highest signal strength value.

   The sticker location is where users should tap their Nymi Band when they are prompted to tap their Nymi Band when performing an operation that requires authentication in an Nymi-enabled Application.

9. On the switch, tap **Calibrator**.
   The Calibrator window appears with a slider that allows you to choose 5 different profile settings, as shown in the following figure.
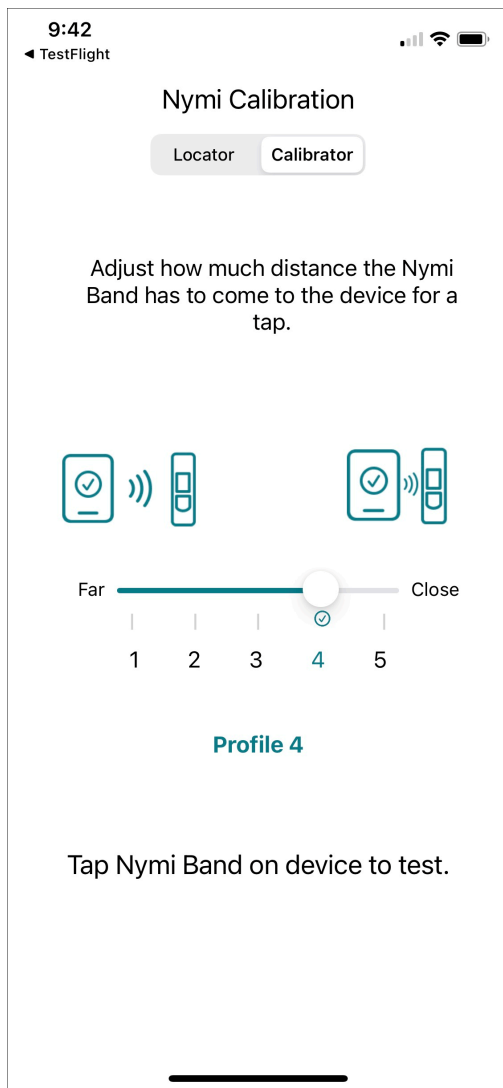
10. With the default profile selected value, move the Nymi Band towards the Bluetooth adapter, and observe the screen.

When the tool detects the Nymi Band, a check mark appears on screen.

The detected position is the same position a user must place the Nymi Band when they perform an e-signature.

11. To change position in which the Nymi Application detects the Nymi Band, use the slider to adjust the profile level.

- To reduce the detection distance between the Nymi Band and the Nymi Application, move the slider to the left.
- To increase the detection distance between the Nymi Band and the Nymi Application, move the slider to the left.

Results

Place a sticker in the same location on each iOS device in the environment and make note of the profile number that provides the best tap results for your environment.

8.2.3 - Customizing the Nymi Application

After you verify the Nymi Application and determine the optimal Nymi Band tap profile value, edit the Nymi Application configuration plist file and upload the new plist file to the Mobile Device Management (MDM) system.

About this task

Perform the following steps from a computer that has access to the *Preferences.plist* file and the MDM system.

Procedure

1. Edit the *Preferences.plist* file.
2. Search for *Profile* and update default value in the string property to match the value that you determined during testing.
   The following example displays the settings that appear for the *RSSI Windows Tap* item. The default item value appears in the \<string> property after the \<key> property named *DefaultValue*.

   ```
   <string>Profile</string>
   <key>Key</key>
   <string>Profile</string>
   <key>DefaultValue</key>
   <string>3<string>
   ```

3. Save the *Preferences.plist* file and then upload the file to MDM.
4. Add the *Preferences.plist* file to the device profile.

What to do next

After the device profile update occurs on the iOS device, retest Nymi Band taps with the Nymi Application.

8.2.4 - Testing Nymi Band Taps

The Nymi Application does not require you perform any configuration steps to interact with the Nymi Band; however, Nymi recommends that you test the performance of Nymi Band with your web-based Nymi-enabled Application(NEA) to ensure that you experience consistently fast and reliable e-signatures.

Ensure that you prepare in the following manner:

* Wear an authenticated Nymi Band
* Wear any PPE that an operator of the iOS device wears over top of the Nymi Band

Launch the web-based NEA and perform several operations that require a e-signature. Confirm the following behaviour:

- Nymi Application appears on screens and prompts you to tap the Nymi Band on the Bluetooth adapter
- Nymi Application disappears and the e-signature operation completes successfully in the NEA

If the response time to complete the e-signature is slower than expected or you do not observe an acceptable success rate with the Nymi Band taps, adjust the Profile setting in the MDM device profile, push the change, and then retest.

8.2.5 - Deploying the Nymi Application

After you verify and customize the Nymi Application configuration, add the remaining iOS devices to the device profile and push the update to the iOS devices.

9 - Updating Connected Worker Platform

Review the following information to plan your update. Infrastructure refers to NES, the Nymi Band Application and the Nymi Runtime software.

- You can update the Nymi Components (NES, Nymi Band Application, Nymi Runtime, and Nymi Band firmware) in any order.
- You can update NES, Nymi Band Application, and Nymi Runtime directly from NEE 3.2.1, 3.3.x and CWP 1.3.x.
- Update NES, Nymi Band Application, and Nymi Runtime components at the same time.
- You can use a Nymi Band 3.0 with CWP 1.6 firmware on user terminals that use a the CWP 1.6 or CWP 1.3.x Nymi Runtime.
- You cannot use a Nymi Band 2.0 in a CWP 1.6 infrastructure.
- You can use a Nymi Band 3.0 with NEE 3.2.1 and later firmware or CWP 1.3.x firmware in CWP 1.6 environment; however, new functionality introduced in an NEE or CWP version that is newer than the firmware is not available.
- The CWP 1.6 Nymi Band Application can only enroll and externally authenticate Nymi Bands with the CWP 1.6 firmware.
- You cannot use a Nymi Band 3.0 with CWP 1.6 firmware in an NEE environment.
- When you update the firmware from NEE 3.3 and earlier, you must re-enroll the Nymi Band.

9.1 - Updating NES

You can update earlier versions of NES to the current version of NES.

About this task

To update a previous version of NES, perform the following steps:

Procedure

1. Extract the NES installation package to a local directory on the NES host.
2. From the directory that contains the extracted NES installation package, run *..\NesInstaller \install.exe.*
3. On the `User Access Control` window, click **Yes**.
4. On the `Open File - Security warning` window, click **Run**.
5. If applicable, on the `User Access Control` page, review the Microsoft .NET EULA, and then click **Accept**. Complete the .NET installation and continue with the NES installation.

6. On the `Application Install Security Warning` window, click **Install**.

7. On the `Open File - Security warning` window, click **Run**.

8. On the left navigation pane, click **Location**, and then perform the following steps.

a) In the **Install Root** field, confirm that the path to the NES services is correct, as it was specified during the initial deployment.

The default location is *C:\inetpub\wwwroot.*

b) In the **Instance Name** field, type the descriptive name that was specified during the initial deployment for the NES web application instance name. For example, NES. See Configuration Attribute Values in the Nymi Connected Worker Platform—Deployment Guide.

Note: Ensure that the values that you specify in the **Install Root** and **Instance Name** match the values that you specified when you deployed the previous version of NES. When the values that you specified in the **Install Root** and **Instance Name** are correct, the **Location** test results will show Install Type: Update/ Re-Install. If there is no match for the values entered, the **Location** test results will show New Installation for the Install Type. The following figure provides an example of the **Location** window for an NES upgrade.
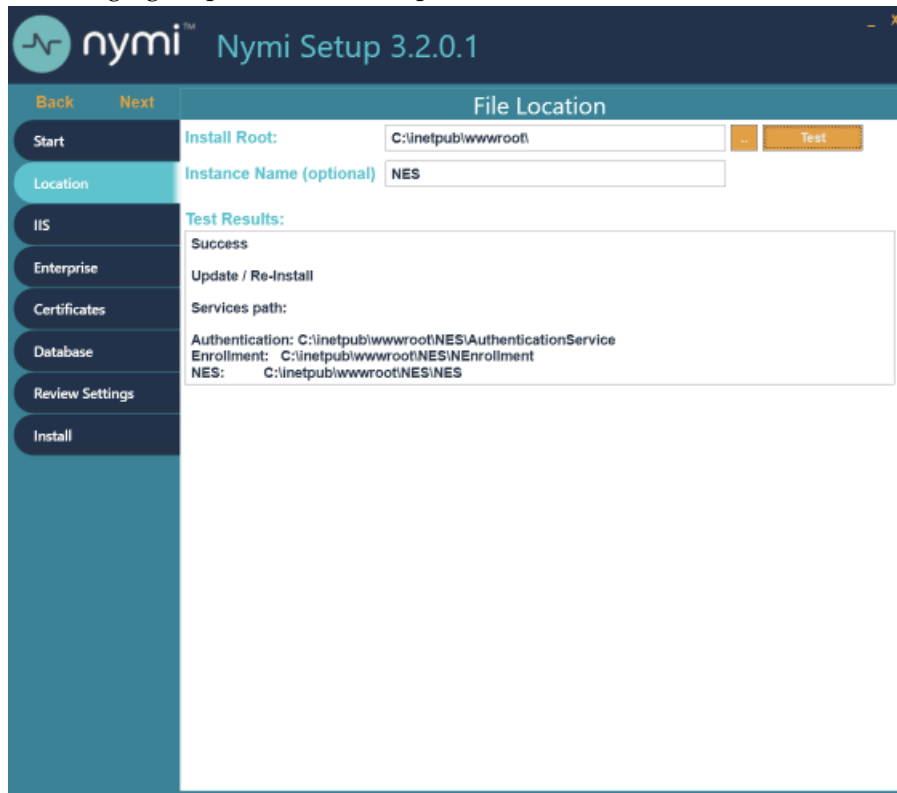

Figure 58: Update / Reinstall installation type

9. On the left navigation pane, click **Install**.

10. Click **Update**.

Note: If the update option is not available, the **Install Root** or **Instance Name** fields on the **Location** tab are not the same values that were specified when you deployed the previous NES version.

11. On the Level Two certificate warning window, click **OK**.

12. On the `Update NES` window, click **Yes** to reapply the configuration.
The `Install` window display the status of the update process.

13. When the Install window displays the Installation Complete message, close the `Nymi Setup` window.

9.2 - Updating the Enrollment Terminal

Update the Nymi Runtime and Nymi Band Application on each enrollment terminal in the environment.

9.2.1 - Updating the Nymi Runtime

Updates from a previous version are supported.

You are not required to remove the previous version before installing the newer version. You can update the Nymi Runtime by using the installation wizard or silently from a command prompt.

9.2.1.1 - Performing a Customizable Nymi Runtime Installation or Update

Perform the following steps to install or update Nymi Runtime on a network device, on which you want to install a Nymi-enabled application.

About this task

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the *..\nymi-sdk\windows\setup* folder, run the *Nymi Runtime Installer version.exe* file.
4. On the `Welcome` page, click **Install**.
5. On the `User Account Control` page, click **Yes**.
The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **Next**.
7. On the `Nymi Runtime Setup` page, click **Next**.
8. On the `Service Account` window, click **Next**.

9. On the `Ready to install` page, click **Install**.

10. Click **Finish**.

11. On the `Installation Completed Successfully` page, click **Close**.

12. In the `Windows Services` applet, confirm that you can see the *Nymi Agent* and *Nymi Bluetooth Endpoint* services, and that the status of each service is *Running*.

9.2.1.2 - Performing a Silent installation or Update of Nymi Runtime

Perform the following steps to install or update the Nymi Runtime and the BLE adapter drivers silently, without user intervention.

About this task

Procedure

1. Log in to the network terminal with an account that has administrator privileges.

2. Extract the Nymi API distribution package.

3. Launch the command prompt as administrator.

4. Change to the *..\nymi-sdk\windows\runtime* folder, and then type: *"Nymi Runtime Installer version.exe" /exenoui /q*

   Where you replace *version* with the version of the Nymi Installation file.

   Note: Ensure that you enclose the command in double quotes.

   The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, Nymi Runtime appears in the `Program and Features` applet.

   Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

What to do next

If required, you can review the installation log file in the *%temp%* directory named Nymi Runtime_*version_time*.log

9.2.2 - Updating the Nymi Band Application

Upgrades from a previous version are supported.

You are not required to remove the previous version before installing the newer version. You can upgrade the Nymi Band Application by using the installation wizard or silently from a command prompt.

Note: Before performing an upgrade of the Nymi Band Application, kill all user sessions for logged in users who are not performing the upgrade.

9.2.2.1 - Performing a silent Nymi Band Application Installation or Upgrade

Perform the following steps to install or upgrade the Nymi Band Application silently, for example, when you want to install the software remotely by using a software distribution application.

About this task

Procedure

1. Save the Nymi Band Application package, provided to you by your Nymi Solution Consultant.

2. Launch the command prompt as administrator.

3. From the folder that contains the Nymi Band Application, type *Nymi-Band-App-installer-v_`version`.exe /exenoui /q*

   Where you replace `version` with the version of the Nymi installation file.

   The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, the Nymi Band Application and Nymi Runtime applications appear in the `Program and Features` applet.

   Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

9.2.2.2 - Performing a Nymi Band application upgrade by using the installation wizard

Perform the following steps to upgrade the Nymi Band Application on each network terminal that you will use to enroll and authenticate users to their Nymi Bands.

About this task

Procedure

1. Download the Nymi Band Application software to a directory on the network terminal. For example, *C:\Downloads*

2. Double-click the installation file *Nymi-Band-App-installer-v_`version`*, and then follow the prompts to update the software.

9.3 - Updating User Terminals and Centralized Nymi Agent

update the Nymi Runtimesoftware on Windows user terminals that use the Nymi Band to perform authentication tasks. In Citrix/RDP environments, update the Nymi Runtimesoftware on server that acts as the centralized Nymi Agent.

9.3.1 - Updating the Nymi Runtime

Updates from a previous version are supported.

You are not required to remove the previous version before installing the newer version. You can update the Nymi Runtime by using the installation wizard or silently from a command prompt.

9.3.1.1 - Performing a Customizable Nymi Runtime Installation or Update

Perform the following steps to install or update Nymi Runtime on a network device, on which you want to install a Nymi-enabled application.

About this task

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the *..\nymi-sdk\windows\setup* folder, run the *Nymi Runtime Installer version.exe* file.
4. On the `Welcome` page, click **Install**.
5. On the `User Account Control` page, click **Yes**.
   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
6. On the `Welcome to the Nymi Runtime Setup Wizard` page, click **Next**.
7. On the `Nymi Runtime Setup` page, click **Next**.
8. On the `Service Account` window, click **Next**.
9. On the `Ready to install` page, click **Install**.
10. Click **Finish**.
11. On the `Installation Completed Successfully` page, click **Close**.
12. In the `Windows Services` applet, confirm that you can see the `Nymi Agent` and `Nymi Bluetooth Endpoint` services, and that the status of each service is `Running`.

9.3.1.2 - Performing a Silent installation or Update of Nymi Runtime

Perform the following steps to install or update the Nymi Runtime and the BLE adapter drivers silently, without user intervention.

About this task

Procedure

1. Log in to the network terminal with an account that has administrator privileges.
2. Extract the Nymi API distribution package.
3. Launch the command prompt as administrator.
4. Change to the *..\nymi-sdk\windows\runtime* folder, and then type: "Nymi Runtime *Installer version.exe*" /exenoui /q

   Where you replace `version` with the version of the Nymi Installation file.

   Note: Ensure that you enclose the command in double quotes.

   The installation command returns to a command prompt immediately, and the installation completes silently. When the installation completes, Nymi Runtime appears in the `Program and Features` applet.

   Note: Alternately, you can track the progress by performing an unattended installation, which displays the installation screens but does not require user intervention by replacing the */q* option with the */passive* option in the installation command.

What to do next

If required, you can review the installation log file in the *%temp%* directory named Nymi Runtime_`version_time`.log

9.3.2 - Installing Nymi Bluetooth Endpoint on an HP Thin Pro

Follow the instructions below to manually install Nymi Bluetooth Endpoint manually. Retrieve the installation file *nbed-cron_x.y.z_amd64.deb* from Nymi.

About this task

Retrieve the installation file *nbed-cron_x.y.z_amd64.deb* from Nymi.

Procedure

1. Switch your user mode to **Administrator** from the system menu, or log in by entering an the credentials of a person in the domain admin group.

   a) Right-click the desktop or click **Start**.

   b) Click **Switch to Administrator** from the menu. You will be prompted to enter the administrator password.

The screen is surrounded by a red border when in administrator mode.

2. Extract the file, *nbed-cron_x.x.z_amd64.deb*, from the Nymi distribution package and save it to the machine. Where *x.y.z* is the version of the file. Note the file path.

3. Unlock read/write access with `X Terminal`.

   a) Click `Start` and go to `Tools`.
   b) Click `X Terminal`.
   c) Type fsunlock

4. In `X Terminal` change the directory to the file location of *nbed-cron_`x.y.z`_amd64.deb* and install the extracted file.

   dpkg -i nbed-cron_x.y.z_amd64.deb

   Where you replace `x.y.z` with the actual version number of the file.

5. Reboot the client.

9.4 - Updating the Nymi Band Firmware

Nymi provides a firmware updater script for diagnostic purposes or to update Nymi Bands.

Run the *fw_updater.exe* file on a computer with a bluetooth adapter to manually update up to 5 consecutive Nymi Bands that are on charge and within bluetooth range of the computer.

During the update process, the utility provides the operator with high-level status information about the process. The upgrade process generates a log file that details the Nymi Bands that were updated, including serial numbers and firmware versions.

When the utility completes a Nymi Band update, the utility scans for other Nymi Bands in the vicinity (within Bluetooth range) that require an update. If a Nymi Band is found, the update is started on another Nymi Band. The utility keeps running until terminated by the user.

9.4.1 - Before you perform a firmware update

Firmware update recommendations

- Nymi recommends that you update the firmware on a maximum of five Nymi Bands at one time. Attempting to update more than five concurrently may require the user to stop and manually restart the utility.
- You may need to disable or extend sleep mode on the Windows computer to prevent the utility from terminating when the computer goes to sleep. When the utility terminates, Nymi Bands that were in the process of downloading software will revert back to the previous firmware version. If the firmware update terminates, restart the *fw_updater* utility, which will restart the upgrade process on Nymi Bands, that are on charge, require an update, and are within Bluetooth range.

- To display additional help information while using the firmware update utility, run the fw_updater_gold_v<version>.exe application with the --help argument.
- The fw_updater_gold_v<version>.exe utility requires the Nymi Band to be in close proximity of the Bluetooth adapter(s) before the firmware update transfers to the Nymi Band. The range varies with the environment, and the default range is approximately 6-18 inches. The default range is limited to avoid unintended updates of Nymi Bands. If an increased range is desired, run the fw_updater_gold_v<version>.exe utility with the --rssi <value> argument, with <value> having a range of -50 to -99. A lower RSSI value (closer to -99) provides longer range, while a larger value (eg. -50) will decrease it. By default a value of -60 is used.

Requirements for multiple Nymi Band update

- A Nymi Band with a charging cradle or multiple Nymi Bands to update
- A USB hub with one or more (up to a maximum of five) Bluetooth adapters plugged into it
- One charging cradle for each Nymi Band
- The executable file has the same version number as the fw_updater utility executable file (*fw_updater_gold_v<version>.exe*)
- Windows 10 computer

9.4.2 - Updating Nymi Band Firmware

During a firmware update, the utility provides you with update and status information, such as:

About this task

- Firmware version
- Number of available BLE adapters
- Number of in progress updates
- Total number of Nymi Bands that are updated during the session.

Perform the following steps to concurrently update the firmware on multiple Nymi Bands.

Procedure

1. Download and extract the firmware package into a directory of your choice on a Windows computer. For example, *C:\Nymi_firmware*.
2. If the Windows machine has the Nymi Band Application or Nymi Runtime installed on it, stop the Nymi Bluetooth Endpoint service.
3. Plug the USB hub into an electrical outlet, and then into a USB port on the Windows machine.
4. Put up to five Nymi Bands on charge. Plug each charging cable and up to five Bluetooth adapters into the USB hub. Double-click the fw_updater_gold_v<version>.exe executable in the file folder.

   Note: If you put a drained Nymi Band on charge, the charging icon appears, and the upgrade process starts when there is a sufficient battery charge on the Nymi Band.

On start up, the application scans the Bluetooth adapters on the USB hub for a Nymi Band that has a firmware version that is older than the version in the firmware package, or a Nymi Band with recovery firmware. A firmware transfer starts for each detected Nymi Band.

5. The Nymi Band automatically restarts when the download completes, and then completes the firmware update process. A brief SUCCESS message appears.

As each Nymi Band firmware update completes, take the completed Nymi Band off charge and plug in another Nymi Band that requires updating. The firmware update utility continues to scan for Nymi Bands that require an update.

6. To stop the application, press Ctrl+C.

7. If required, restart the Nymi Bluetooth Endpoint service before using the Nymi Band Application or an application that uses Nymi Runtime.

Results

After you update a Nymi Band with version NEE 3.3.x and earlier firmware, you must re-enroll the Nymi Band

9.4.3 - Firmware updater log files

At any time during the firmware update process, you can view firmware log file information. The *result_log.csv* is available in the same directory where the fw_updater_gold_v<version>.exe file is executed. You can provide this file to Nymi Support when troubleshooting is required. Alternatively, if a --log argument was provided using a command line, then the log is available in the directory determined by the user.

The *fw_updater.log* file contains system diagnostic information about actions that are run during Nymi Band firmware upgrades. This file is required by Nymi Support to help resolve Nymi firmware issues regarding upgrades.

Nymi creates a maximum of 5 rotating log files. Each of these log files cannot exceed 10MB.

10 - Appendix—Recording the CWP Variables

Throughout the deployment process, you will perform configuration tasks that you will be required to remember later on.

Use the following table to keep track of values for variables that you define when you deploy the CWP solution.

Table 7: CWP Values

Component	CWP Backend Variable Name	When Used	Value
Nymi Enterprise Server(NES) FDQN		NES deployment	
NES URL	NES_URL	Connect to the NES Administrator Console	
NES Communication port number (LDAP/LDAPS)	CORP_LDAP_PORT	CWP Backend deployment (cca script)	
NES Administrators group name and user accounts		NES deployment CWP Backend deployment (cca script)	
NES Administrator accounts		Access to NES Administrator Console	

11 - Appendix—Recording the CWP Component FQDNs

Throughout the deployment process, you will perform configuration tasks that you will be required to remember later on.

Use the following table to keep track of FQDNs for various components in the CWP solution.

Table 8: CWP Values

Component	FQDN
Nymi Enterprise Server(NES) FDQN	
Centralized Nymi Agent & virtual server port #	

12 - Appendix—TLS Certificates Expiration Dates

The Connected Worker Platform(CWP) makes use of a server TLS certificates. Each certificate has an expiration date. Record the expiration date of each certificate as you go through the deployment procedure and keep this sheet for your records. Renew certificates before the expiration date to avoid disruption of CWP services. For more details on certificate management, see the *Nymi Connected Worker Platform—Administration Guide*.

Table 9: Certificate Expiration Dates

Certificate Type	Expiration Date
Nymi Enterprise Server(NES) TLS Server Certificate	
Nymi Agent(WebAPI)	