Deployment Guide

Nymi Connected Worker Platform
v5.0
2021-05-03

Contents

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.

This document provides an overview of the components and the steps that are required to deploy the Nymi Enterprise Server (NES). This installation uses the `Nymi Token Service` to install certificates that enable communication between components. This document also provides information about deploying the Connected Worker Platform in a Citrix or RDP environment.

Audience

This guide provides information to NES Administrators. An NES Administrator is the person in the enterprise that manages the `Connected Worker Platform` for their workplace.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
5.0	May 3, 2021	Update to reflect Nymi Enterprise Edition rebrand to Connected Worker Platform. Changes include new content regarding how to install Nymi Bluetooth Endpoint on Thin Clients.
4.0	February 26, 2021	Update to include changes for Nymi Enterprise Edition 3.4.0. This includes authentication lockout.

Version	Date	Revision history
3.0	December 18, 2020	Third release of this document. Updated for Nymi Enterprise Edition 3.3.0. Includes the following changes: • Update to Setting Service Principal Names (SPN) • A new section in the Overview section that provides an overview of the certificates that are used in the Nymi Enterprise Edition solution.
2.0	September 18, 2020	Second release of this document. Updated for the Nymi Enterprise Edition 3.2.0 release.
1.0	April 15, 2020	First release of this document for Nymi Enterprise Edition 3.1.0.

How to get product help

If the Nymi software or hardware does not function as described in this document, contact your administrator for immediate support. Alternatively, 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

Connected Worker Platform Overview

The `Connected Worker Platform` is an authentication solution that minimizes the impact of compliance and security requirements on manufacturing workflows. It combines a wearable component, the Nymi Band, with enterprise software, creating a secure authentication solution.

The Connected Worker Platform 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 and Nymi Band Application, that runs on terminals and servers.

Connected Worker Platform Components

The `Connected Worker Platform` enables administrators and users to manage Nymi Bands in an enterprise setting. The `Connected Worker Platform` is comprised of Nymi-specific components and enterprise components, as shown in the following figure.
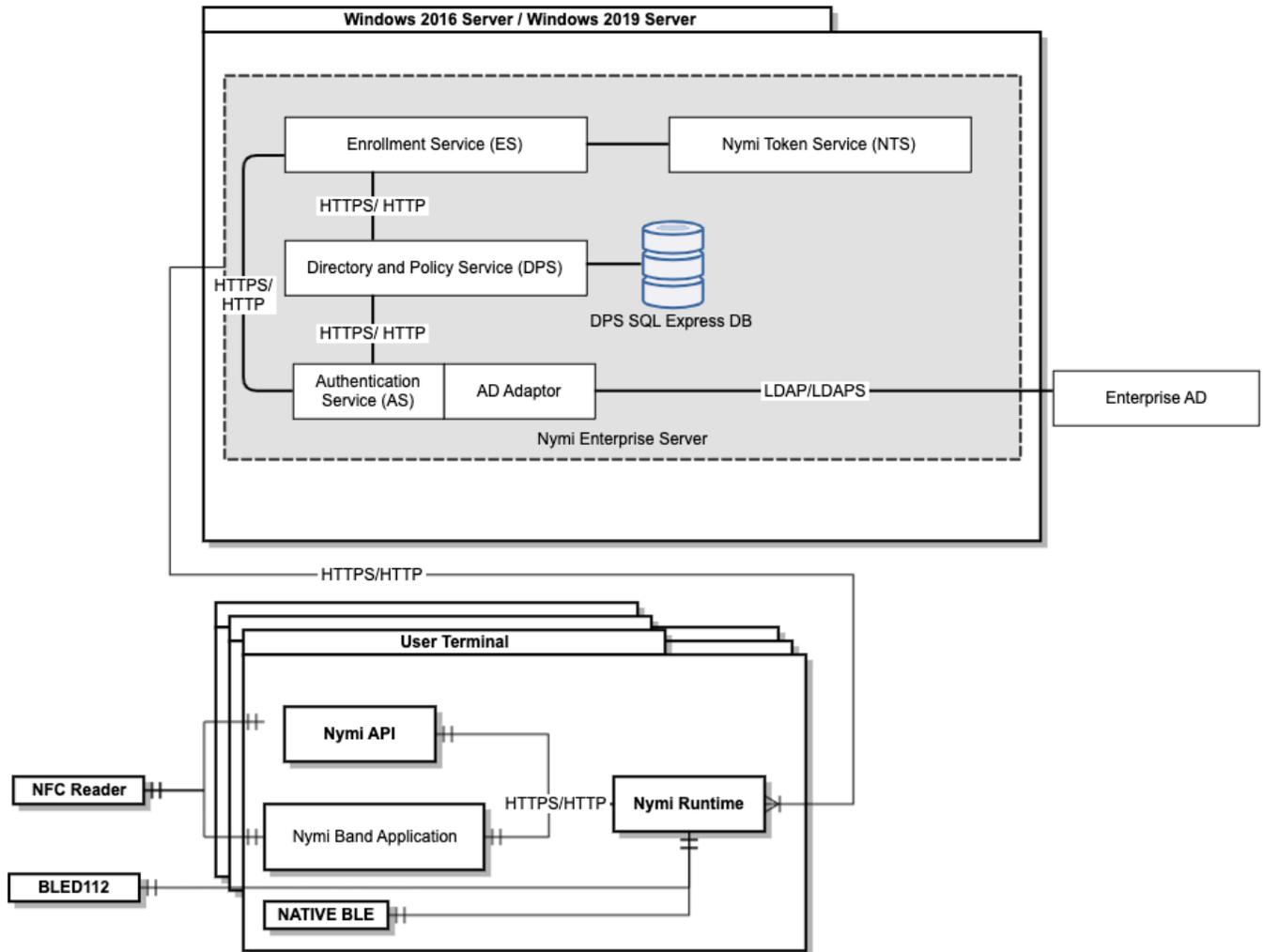
Figure 1: Nymi Connected Worker Platform Architecture

The Connected Worker Platform consists of the following components:

Table 2: CWP Components

Component	Description
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
Enterprise Applications	Using the Nymi Runtime Software, which is installed on an endpoint, developers can create Nymi-enabled Applications (NEAs) that integrate CWP with common corporate applications such as Manufacturing Execution Systems (MES), Single Sign-On (SSO), and HMI (Human Machine Interface).
Nymi Band Application (NBA)	A Windows application that is used to enroll new users and link them to their Nymi Band. The NES Administrator installs the NBA on a Windows 10 or Windows 7 host, which connects to NES and provides enrollment services to Nymi Band users. `Connected Worker Platform` is comprised of two services: Nymi Agent and Nymi Runtime.
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.
NES Administrator Console	A web interface into NES that an NES Administrator accesses from any network device to manage group policies, certificates, user and Nymi Band assignment.
Identity Ecosystem	External directory and database systems, such as Active Directory.

Connected Worker Platform Certificate Overview

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

The following figure provides a high-level overview of the certificates that the `Connected Worker Platform` requires.
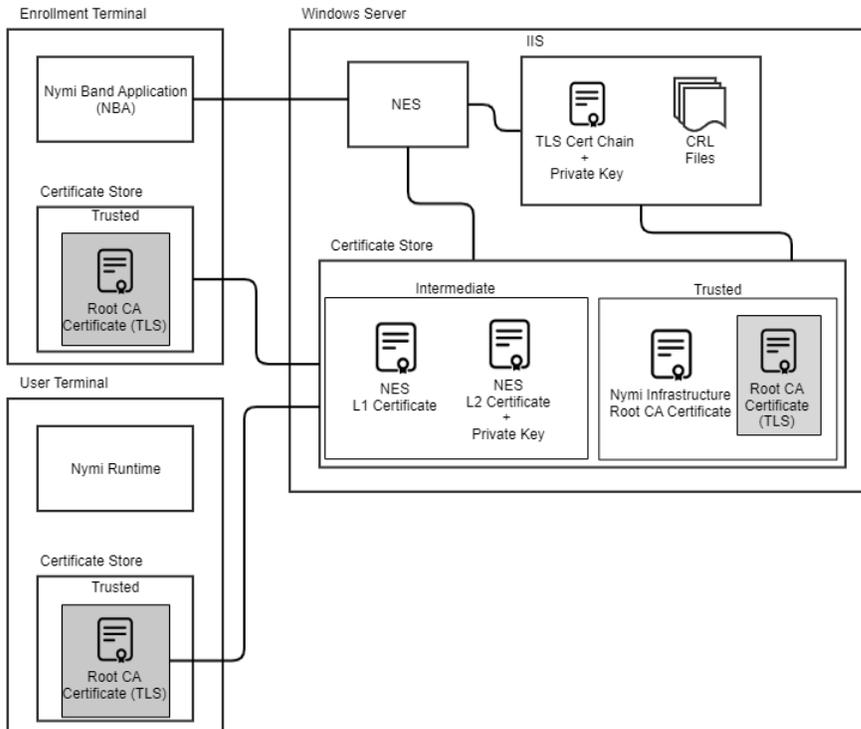
Figure 2: Certificates required in a Connected Worker Platform environment

- TLS certificate: Allows the use of HTTPS for secure connectivity to NES by following components:
  - `Nymi Band Application`
  - Nymi-enabled Application
  - Nymi Agent
  - NES Administrator Console when accessed through a web browser.
- NES L2 certificate: Allows NES to issue NEA certificates via `Nymi Token Service`(NTS).
- NEA certificate(not shown): Allows NEAs authentication to Nymi Bands and establishment of a secure communication channel over BLE.
- Nymi Band certificate: Allows Nymi Band authentication to NEAs and establishment of a secure communication channel over BLE.
- NES L1 certificate: Provided to Nymi Bands during enrollment time to bind the Nymi Bands to the NES and NEAs of an enterprise.

- Nymi Infrastructure Root CA certificate: The root of trust of the Nymi infrastructure PKI (which issues the NES L1, NES L2 and NEA certificates).
- 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.

Obtaining Certificates

NES supports HTTP and HTTPS communication. It is recommended to configure NES to use HTTPS to secure communication.

Contact your Nymi Solution Consultant to plan the certificate configuration.

1. Nymi provides the NES Level 2 (L2) certificate for use by the Nymi Token Service (NTS) to issue authentication tokens. This certificate is imported when you import the Fullchain Certificate, as described later in this document. Contact your Nymi Solution Consultant to obtain this certificate.

2. For HTTPS deployments, NES also requires a TLS certificate to allow secure communications between clients and NES over HTTPS. The NES Administrator is responsible for obtaining this certificate from a public root certificate authority, or an enterprise certificate authority, which is trusted by all the clients.

   If the TLS certificate is not issued by a trusted root CA (e.g. if a self-signed certificate is used in a lab deployment), then the signed CA certificate needs to be imported into every client machine that communicates with NES (i.e. every machine that runs the NBA, an NEA, and access the NES Administration web interface from a browser). The process of importing the TLS and signed CA certificates are described later in this document.

TLS Certificate Requirements
The following conditions should be considered when obtaining a TLS certificate for the deployment.

1. The TLS certificate should be a web site certificate.
2. For environments where a public URL is specified for NES services, a subjective alternative name (SAN) must be specified for the public URL. When setting the SAN, there are two options: a wildcard TLS certificate with SAN *.dns_domain, or a certificate that specifies the FQDN for the public URL and every individual server's FQDN.
3. The following Key Usage characteristics should be set: DigitalSignature, KeyEncipherment, DataEncipherment.
4. The following Enhanced Key Usage characteristic should be set: Server Authentication.

Hardware and Software Requirements

The host on which you deploy the NES software must meet the following minimum software and hardware requirements.

Software requirements

NES has the following software requirements.

- Microsoft Windows Server 2016 or 2019
- Microsoft IIS
- Microsoft SQL Server 2012, 2016, 2017, or 2019
- Microsoft .NET Framework 4.8

Note: Microsoft SQL Server Express 2012 and Microsoft .NET Framework 4.8 are bundled in the NES installer.

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

Configuration Settings Attribute Values

Print this table and record key information that you are required to provide during the NES deployment.

Table 3: Deployment Configuration Information

Configuration attribute	Configuration value
Country code (for certificates):	
NES Admin Group name:	
Users who are part of the NES Admin Group:	
NetBIOS (Pre-Windows 2000) Domain name	
NES hostname:	
NES Service Mapping name (NES service name):	
NES Admin service mapping name:	
Enrollment service mapping name:	
NES Administrator Console website (https://FQDN_nes_server/nes_service_name) (Provide to IT Admin)	

Certificates Expiration Dates

NES makes use of a number of certificates. Each certificate has an expiration date. Record the expiration date of each certificate as you go through the deployment procedure, and keep this for your records. Certificates must be renewed before expiration to avoid disruption of CWP services. For more details on certificate management, see the Connected Worker Platform Administration Guide.

Table 4: Certificate expiry dates

Certificate Type	Expiration Date
L2 Certificate • L2 certificate expiration date can be viewed using certlm.msc.	
(For HTTPS Deployments) TLS Server Certificate • Certificate expiration date is dependent on the certificate.	

Deployment Checklist

The following deployment checklist includes items to consider when planning the NES deployment.

Table 5: Production environment Deployment Checklist

Task	Status
Domain Controller Configuration	
On the Domain Controller (DC), create the following domain user and group accounts: • Security Group for NES Administrators. For example, NES_Admins • Create a Group Policy Object (GPO) to configure the URL to the NES host on all computers in the domain.	
(For secure LDAP Deployments) Configure Active Directory for LDAPS	
Firewall Configuration	
Depending on the NES configuration, ensure that the HTTP/HTTPs port is open for bidirectional communications between NES and machines in the environment with an installed Nymi Component, for example, the enrollment terminal, user terminals, Nymi agent server etc.	
NES Host Configuration	
(For HTTPS Deployments) Obtain TLS certificate.	
Add a dedicated Windows Server 2016 or Windows Server 2019 machine to the domain for use as the NES host.	
In `Server Manager`, install the following roles and features: • Web Server (IIS) with the latest version of ASP.NET 4.x role services.	
(For HTTPS Deployments) In `IIS Manager`: • Import the TLS certificate. • Add HTTPS site bindings by using the imported TLS certificate.	
Install certificates using the Fullchain file.	
Run the NES install file (*install.exe*) and configure NES to use above configurations.	
Client Configuration	

Task	Status
Certificate and Enrollment URL: • For deployments with HTTPS configured, if the TLS certificate is not issued by a trusted Root CA, then add the certificate o f the Root CA into the Trusted Root Cert store of every client machine. To do this, run **certlm.msc** as an Administrator, and then import the certificate into the Trusted Root Cert store of every client and server machine. • Perform the following configuration one time, on a client computer. From a web browser, go to `https://FQDN_nes_server/nes_service_name`, login, and then configure the URL in the default policy.	

Prerequisite Configuration

Connected Worker Platform integrates with a Windows domain structure. Before you install NES, review the following section to prepare the environment.

Configuring Active Directory

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

1. Create a group that contains the users who will act as NES Administrators. 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 admin users, and add the NES admin users to this group.

2. Record the administrator group name and a list of user accounts that you added this group, in the Configuration Attribute Values table.

Preparing the NES host

Perform the following actions to prepare the NES host for the NES deployment.

1. Designate a host in the environment for NES. Record the full name of the NES host in the Configuration Settings Attribute Values table.

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

2. Extract the contents of the NES Deployment package that was provided to you by your Nymi Solution Consultant, into the *C:\nestemp* folder. The package extracts the following files into the folders:

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

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).

Installing IIS and ASP.NET

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

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 select the latest available version of ASP.NET 4.x.

Note: NES supports ASP.NET 4.4 and later.

a) On the `Add features that are required for ASP.NET` dialog box, click **Add Features**.

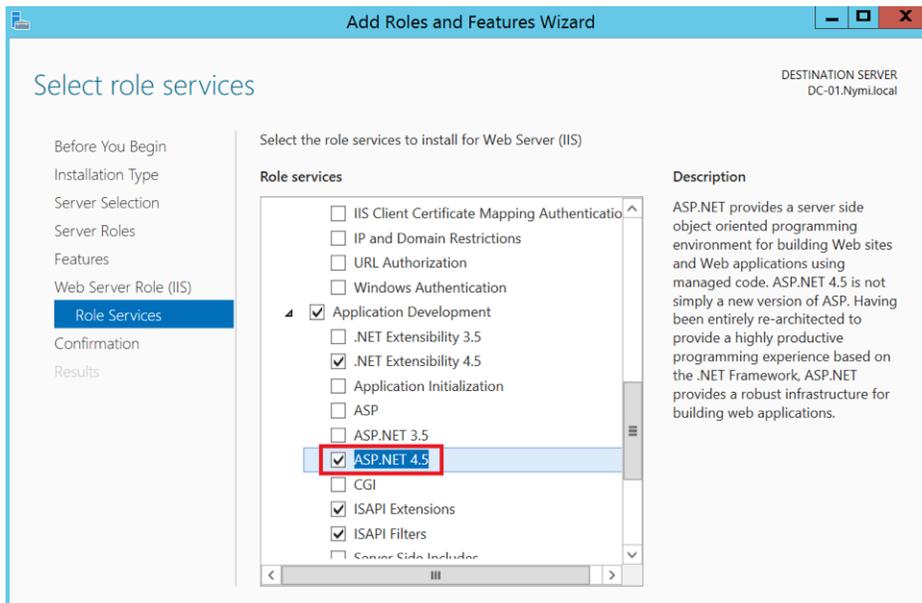The following figure shows the `Add features that are required for ASP.NET` page.

Figure 3: Select role services page with ASP.NET selected

b) On the `Select role services` page, click **Next**.

The following figure provides an example of the `Select Role services` page, with **ASP.NET** selected.
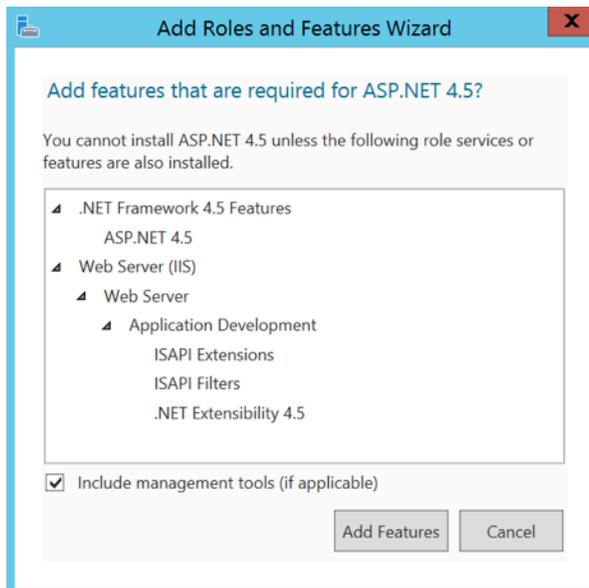
Figure 4: Add features that are required for ASP.NET

11. 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.

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.

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.

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.

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`**.

   d) Click **`OK`**.

4. Minimize IIS.

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

6. From the Window start menu, type `Manage Computer`, and then select **`Manage Computer certificates`**.

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

8. Expand **`Certificates - Local Computer > Trusted Root Certificate Authority`**.

9. Right-click **`Certificates`**, and then select **`All Tasks > Import`**.

10. On the `Welcome to the Certificate Import Wizard` page, click **`Next`**.

11. On the `File to Import` page, click **`Browse`**.

12. From the drop list, select **`All Files *.*`**.

13. Navigate to the folder that contains the *.pem* file for the root CA certificate.

14. Select the *.pem*, and then click **`Open`**.

15. On the `File to Import` page, click **`Next`**.

16. On the `Certificate Store` page, leave the default selection **`Trusted Root Certificate Authorities`** in the **`Place all certificates in the following store`**, and then click **`Next`**.

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

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

19. Close the `certlm` window.

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.

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 *Creating the CRL directory in IIS*.

1. In the `Connections` navigation pane, click Computer_Name > Sites.

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.
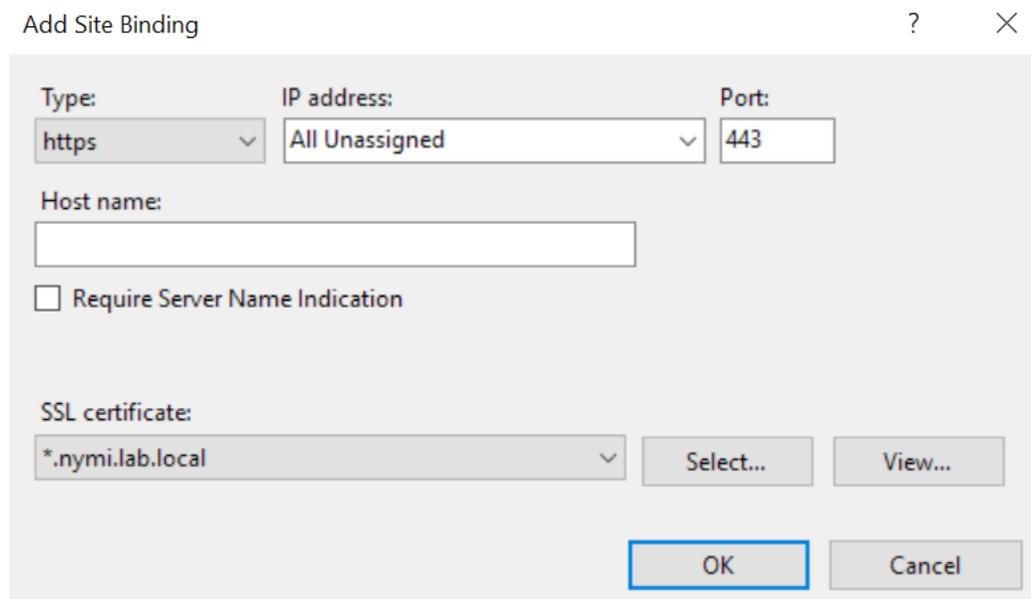
Figure 5: Add Site Binding Dialog

   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**.

Creating the CRL directory in IIS

NTS uses Certificate Revocation Lists (CRLs) to verify the validity of certificates that are used in Connected Worker Platform. The CRLs are distributed by IIS to clients as needed.

Perform the following steps in IIS Manager to create the virtual directory that IIS uses to distribute CRLs.

1. In the `Connections` navigation pane, expand *`Computer_Name`* **`> Sites > Default Web Site`**.

2. In the `Action` pane on the right, select `View Virtual Directories`, and then click **`Add Virtual Directory`**.

   The `Add Virtual Directory` dialog appears.

3. In the **`Alias`** field of the `Add Virtual Directory`, type **`crl`**.

4. In the `Physical Path` field, click the ellipses. In the `Browse for Folder` dialog, expand **`This PC > Local Disk (C:) > inetpub`**, and then select **`wwwroot`**.

5. Click **`Make New Folder`**, and then name the new folder *crl*. Click **OK**.

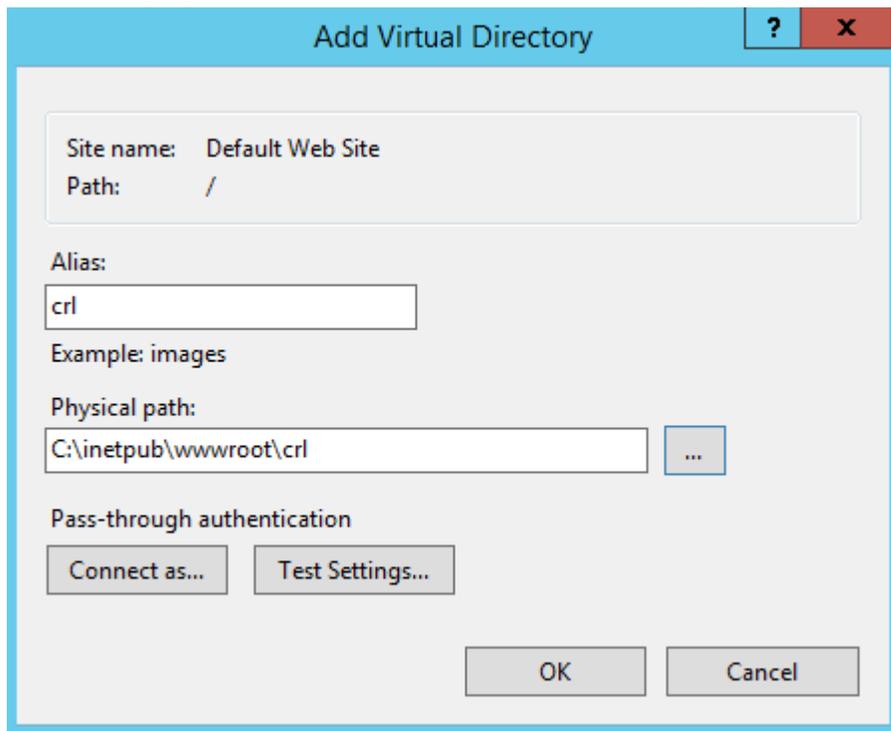   The following figure shows the `Add Virtual Directory` dialog.

Figure 6: Add Virtual Directory Dialog

6. Click **OK**.

7. Minimize the **`IIS Manager`** window.

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 and 2 Certificate Revocation List (CRL) files. The password for the PKCS12 file is provided to you separately.

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.

Importing certificates

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

1. Extract the certificate zip file to a directory.
2. Right-click the *fullchain.p12* certificate file and then select **Install PFX**.
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` screen, in the **Store Location** page, select **Local Machine**.
5. Click **Next**.
6. On the `User Account Control` window, click **Yes**.
7. On the `Files to import` page, perform the following actions 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**.
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.
11. On the `Completing the Certificate Import Wizard` page, click **Finish**.
12. On the `Certificate Import Wizard` dialog, click **OK**.

13. Copy the CRL files to the *C:\inetpub\wwwroot\crl*.

If you copied the CRL files to the path listed above and receive a message to replace the files, click **Yes**.

Moving the L2 certificate

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.

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.

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.

Installing NES

After you install and configure IIS, perform one of the following actions to install NES:

- Using the NES Service Suite Wizard
- Using the Silent Installer

Installing the NES Services Suite using the wizard

Perform the following steps to install the NES Services Suite.

Note: The installation process prompts you to install Microsoft .NET Framework 4.8 and SQL Server Express on the NES host. The SQL Server Express installation is optional. For production deployments of NES, it is not recommended to use SQL Server Express.

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**.

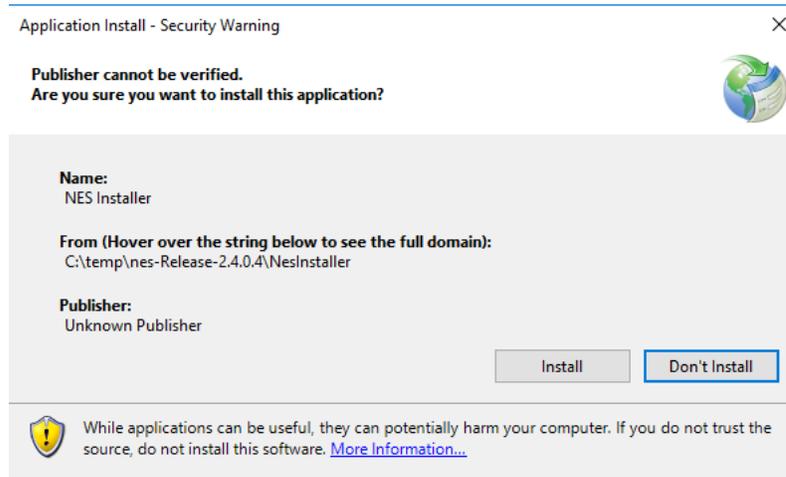**10.** On the `Application Install Security Warning` pop-up, click **Install**.

Figure 7: 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 2012, click **Yes**.

b) If a version of SQL server exists on the machine, click **No**.

After the SQL Server Express 2012 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.

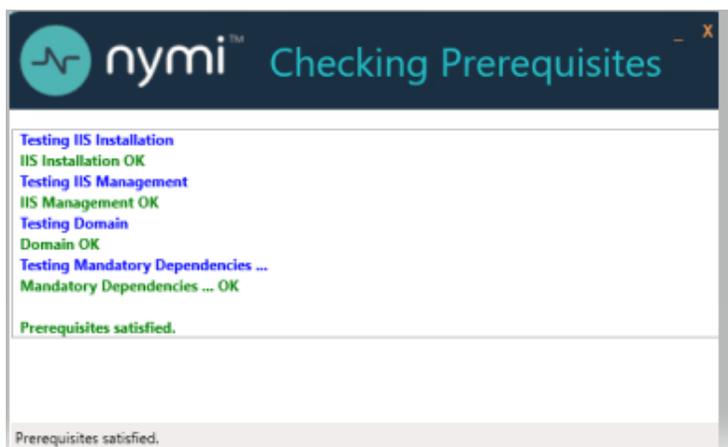The following figure shows the `Prerequisites Check` dialog.

Figure 8: 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.

Configuring NES Services

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

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

• NES admin group name

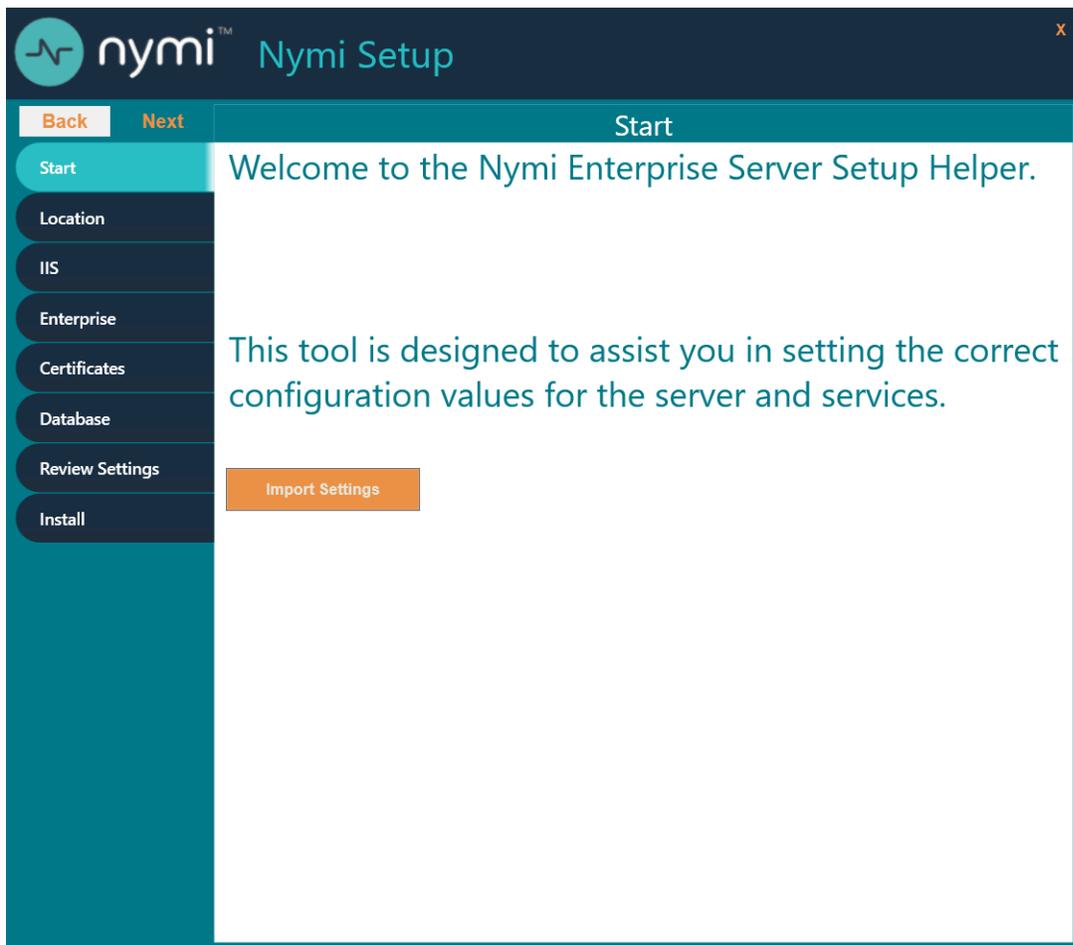The following figure provides an example of the `NES Setup` wizard.

Figure 9: 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.

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 10: 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 upgrading 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 want to run the application from a custom user account that is under an application pool, select **`SpecificUser`** from the drop-down list and perform the following actions:

      - In the **`User Name`** field, type the username using the domain\username format.
      - In the **`Password`** field, type the password for the user.
      - Click the **`Test`** button to ensure that the credentials of the user are valid.

   d) In the **`Communication Protocol`** section, select a communication protocol for the deployment. The installer uses available site bindings in IIS to determine the protocol which can be selected.

      HTTPS is recommended to ensure secure communication. 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 11: IIS Setup page in the NES Setup wizard

The following figure displays the warning that appears when you select HTTP as the communication protocol.
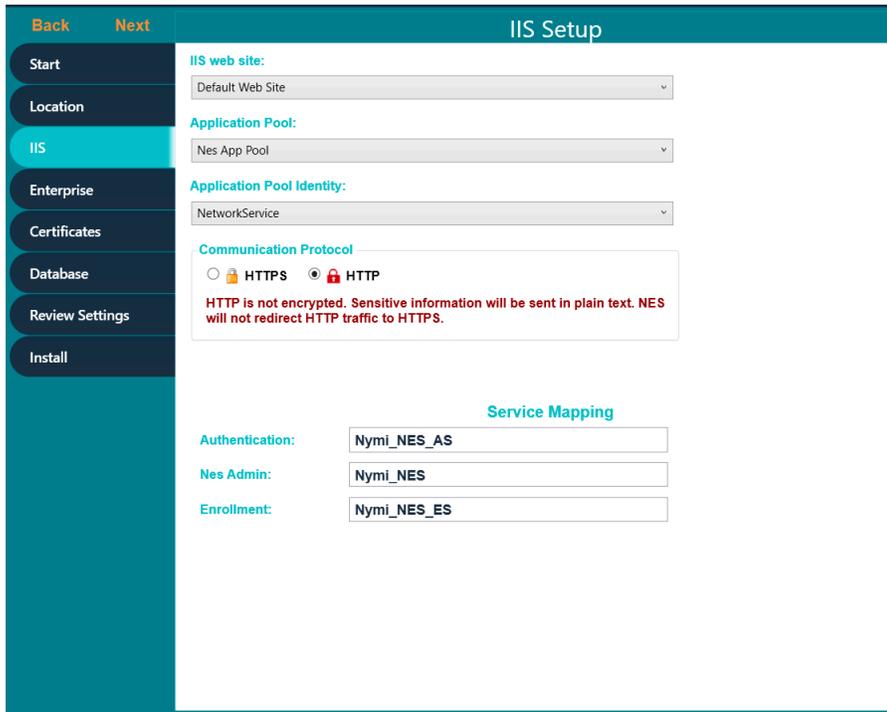
Figure 12: IIS Setup Page HTTP Warning

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

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

   By default, LDAP is selected for the communication protocol. For secure LDAP, ensure Active Directory on the Domain Controller is configured for LDAPS, and that appropriate certificates are imported on the NES server.

4. In the Domains table, by default the domain in which the NES host resides appears. Add additional domains when Nymi Band users reside in different domains and when users in other domains will manage NES. After configuring the domain(s), click **Test** to verify the domain(s) can be reached.

   Note: NES understands domain trust relationships, therefore when configuring multiple domains in the same forest, specify the domain name but it is not necessary to specify a separate username and password. The Application Pool Identity selected in the IIS window needs to be a member of one of the domains. Similarly, a domain in a different forest that has two-way trust with the domain in which the application pool identity resides does not need separate accounts specified. If used, separate accounts must be part of the domain that is

being configured, and have low privilege. For example, they should not be part of the *Domain Administrators* account group. Set the password to *never expire* so that the connection is always available.

To add additional domains and domain groups to the NES configuration, perform the following steps:

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 when the domain is not in the same forest as the NES domain and a two way trust does not exist.

c) Press **Enter**.

d) Press Test to confirm that the domain is reachable.

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

Figure 13: Enterprise page in the NES Setup wizard

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

6. In the left navigation pane, click **Certificates**, and then perform the following actions for issuing certificates using the NTS method:

   a) In the **OTP Expiry** field, leave the default value for the length of time that the one-time password remains valid. The default is 1 hour.

   b) In the **Certificate Expiry** field, leave the default value for the length of time that the NEA certificates remains valid. The default is 14 days.

   c) 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.

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

   The following figure provides an example of the Certificates page.

Figure 14: 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**.

   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 Authenication

  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 15: 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.

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

Table 6: 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.
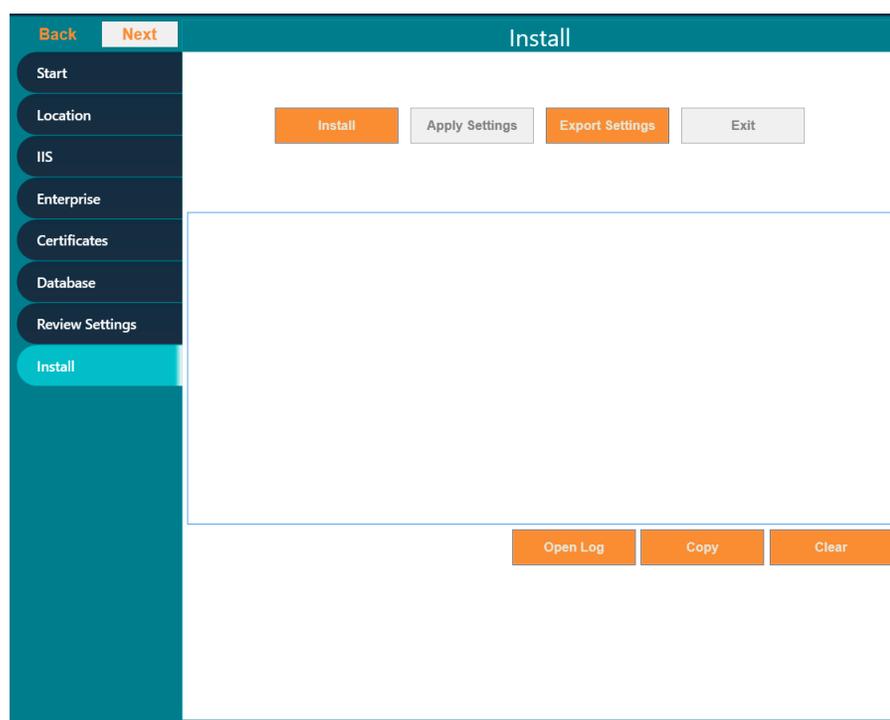
Figure 16: Install NES page in NES Setup wizard

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 NESconfiguration 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.

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

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**.

Verifying the authentication configuration on the NES host

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

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

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.
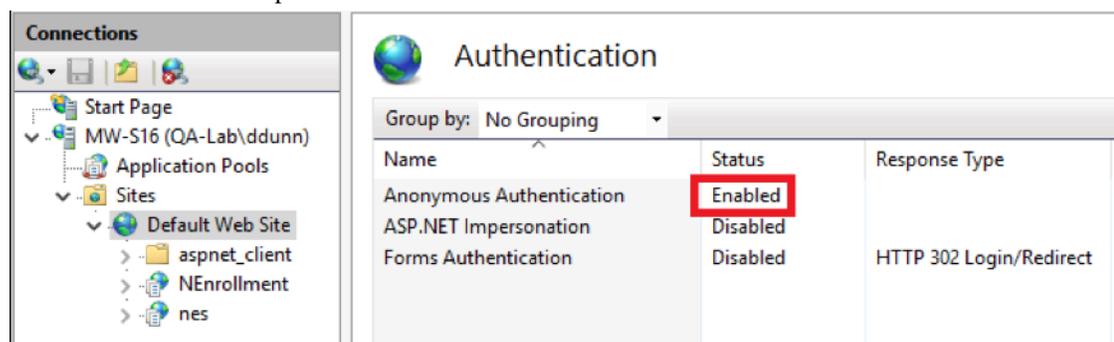
Figure 17: Authentication pane with Anonymous Authentication enabled

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.

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

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

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.
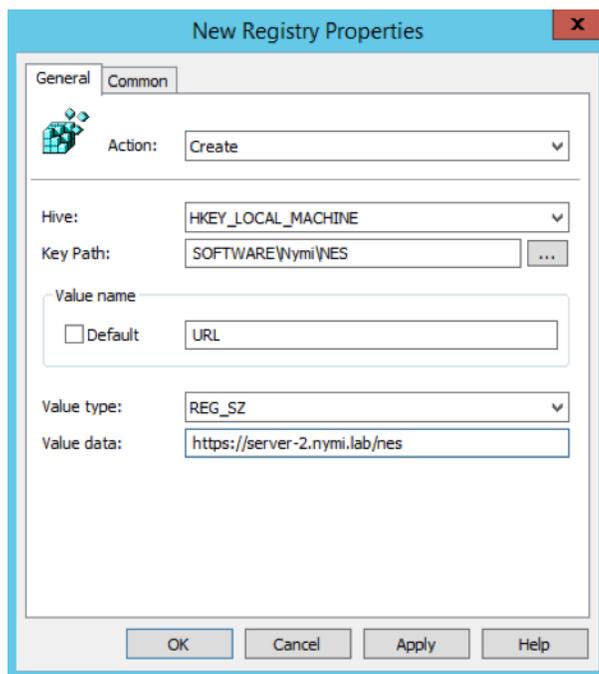
Figure 18: URL properties page

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`.

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

Create a group policy object to update the registry.

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**.

NES Silent Installer

Silent installations allow you to perform an NES installation without user intervention, based on values that are defined in a configuration file. The option to create a configuration file is available to you when you perform an NES configuration by using the NES Setup wizard.

> It is beneficial to perform a silent installation of NES when you are ready to move from a POC deployment to a production deployment. In this example, you would

perform an NES installation and configuration in the POC environment, and select the option to save the configuration file in the NES Setup wizard. You can then copy the configuration file to the production NES server, and use the file to silently install the NES with the POC configuration. The *Configuring NES Services* section describes how to save the configuration file.

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

Installing .NET and SQL Server Express

The installation package contains the .NET 4.8 software and Microsoft SQL Server Express 2012 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 2012: *..\PreRequisites\SqlExpress*

  Note: If required, you can download and install Microsoft SQL Server Express 2016, or Microsoft SQL Server Express 2017 instead.

  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.

Installing NES using the silent installer

Use the following information to install NES using the Silent Installer.

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:

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.

Setting Service Principal Names (SPN)

This section provides information on creating SPNs for NES. After installing NES, it is required to create 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.

Removing SPN

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 -l %computername% | <App_Pool_Identity>`. Only include `<App_Pool_Identity>` if the Application Pool identity is not a local account, such as NetworkService, or LocalSystem.

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.

Single Node SPN Creation

To create SPNs for a single node of NES, complete the following.

Open a command prompt as an Administrator and type:

- `setspn -S HTTP/%computername% <%computername% | App_Pool_Identity>` and
- `setspn -S HTTP/%computername%.%userdnsdomain% <%computername% | App_Pool_Identity>`

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.

Note: If NES is not configured for traffic on the standard ports (HTTP/80, HTTPs/443) , it is important to specify the port while completing the setspn command. e,g. `setspn -S HTTPs/winserver:8443 winserver`, if it is listening on port 8443 instead of 443. If the user account that performed the install is a member of a different domain, replace %userdnsdomain% with the domain of the NES server.

NES Cluster SPN Creation

For a NES cluster, use an AD account as the App Pool Identity. Repeat the SPN creation for every NES instance. In addition, the SPN for the public FQDN of the NES cluster need to be created as follows:

Open a command prompt as an Administrator and type `setspn -S HTTP/<nes_cluster_fqdn> <App_Pool_Identity>`

where:

- *nes_cluster_fqdn* is the Fully Qualified Domain Name (FQDN) of the NES cluster host.

Note: If the NES cluster is not configured for traffic on the standard ports (HTTP/80, HTTPs/443) , it is important to specify the port while completing the **setspn** command. e,g. `setspn -S HTTP/%computername%:8443 %computername%`, if it is listening on port 8443 instead of 443. If the user account that performed the install is a member of a different domain, replace %userdnsdomain% with the domain of the NES server.

Managing Database Logins

Manage the database logins using the Add, Edit and Delete buttons.

The **Database** page in the installation wizard enables you to configure settings that apply applied to the database. You can manage the Database Logins settings by adding, editing and deleting information.

Adding Database Logins

The Database window enables you to configure settings that apply to the database. In the Connection String area, if the connection uses Integrated Security and the Security property is set to **True**, you can add Database Logins.

To add a new user perform the following steps:

1. In an empty row of the `Manage Database Logins` table, right-click and select **Add**. The `Select User Credentials` window appears.
2. From the **Login Type** drop-down list, select Auditor or User.

    • Auditor – Provides the database user with read-only access to the database
    • User – Provide the database user with full control access to the database

3. In the **Domain Account** field, type the domain name followed by the user account or group account.

    Note: Ensure that a backslash separates the domain and account user or group.

4. In the **Database User** field, type the name of the database user.
5. Click **OK**.
6. On the Database page, click the **Verify Users** button to ensure that the new user is valid. The Database Login is added to the **Manage Database Logins** area. This Database Login is added to the SQL database when you are finished configuring the NES Setup Wizard. Proceed to the `Install` tab, and and press **Install** or **Upgrade**.

Editing Database Logins

To edit a database login, perform the following steps:

1. In the `Manage Database Logins` table, right-click and select **Edit**.
2. Modify the fields as required.

    Note: You cannot change the Login type for a service login account.

3. Click **OK**.

Deleting Database Login

You can delete any Auditor login that you have added.

1. In the **Manage Database Logins** area, click the row that you want to delete and right-click.

2. From the drop-down box, select **Delete**.

3. Enter **Delete**.

4. Click **OK** to confirm the deletion.
   The selected login is deleted.

Connect to NES for the First Time

An NES Administrator uses a web browser on a network device to connect to the NES Administrator Console.

Accessing NES Administrator Console

Perform the following steps to connect to the NES Administrator Console and the System Diagnostics page.

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://server-2.nymi.lab/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.

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

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

The *Nymi Connected Worker Platform Troubleshooting Guide* provides information about how to resolve issues that you might encounter when you try to access the NES Administrator Console.

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.

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.

1. Ensure the NES Application Pool Identity uses the `LocalSystem` identity option from the Application Pool Identity list, or from the domain user account that is not in the local Administrators group. Changes to the Application Pool Identity are made on the IIS page in the NES installer.

2. Uninstall the `SQL Server Express 2012` software. In the **Program and Features** applet of `Control Panel`, select **Microsoft SQL Server 2012 (64bit)**.
   When prompted, select all components for removal.

3. Download and install the SQL Server Express 2017 software.
   When prompted, select the **Basic** installation type.

4. In the *C:\nestemp\NesInstaller* folder, run *install.exe*.
   The Nymi wizard opens.

5. On the `Location` page, in the `Instance Name (optional)` field, enter the NES instance name.
   For example, **NES**

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

7. On the `Install` page of the `NES Setup` wizard, click **Upgrade**.

   The `NES Setup` wizard recreates the SQL database that was removed during the uninstall of SQL Server Express 2012.

   Note: If you get the error message `CREATE DATABASE permission denied to database 'master'`, perform the following steps:

   • Re-run the install.
   • On the `Install` page of the wizard, click **Upgrade**.

8. Close the `NES Setup` wizard.

9. Edit the *C:\inetpub\wwwroot\NES\nes\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 codeblock

   ```
   <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.

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

11. Open SSMS by using the **Run as Administrator** option.

12. Click **Connect > Database Engine**.

13. 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**.

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

15. 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.
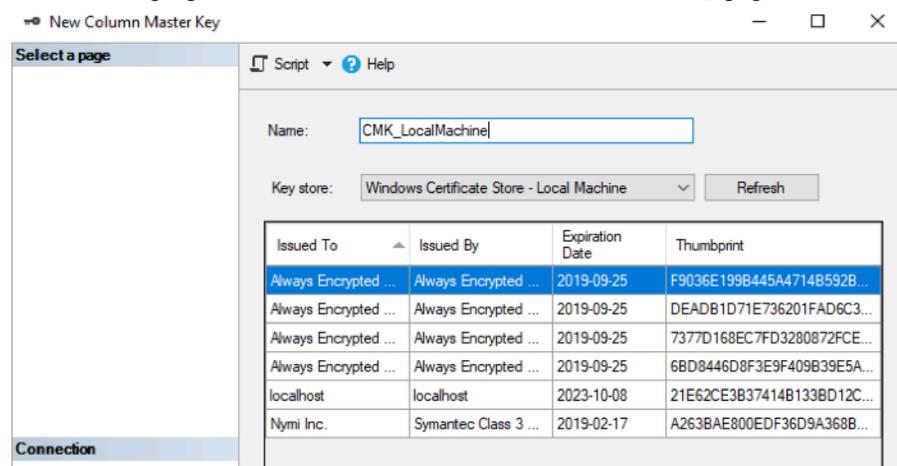
Figure 19: New Column Master Key page

c) Click **Generate Certificate**.

d) Click **OK**.

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

17. 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.
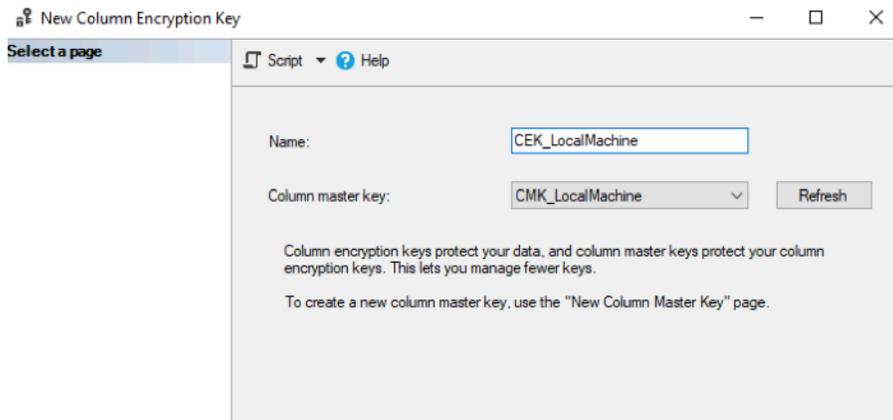
Figure 20: New Column Encryption Key page

    c) Click **OK**.

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

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

20. On the `Introduction` page, click **Next**.

21. 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.
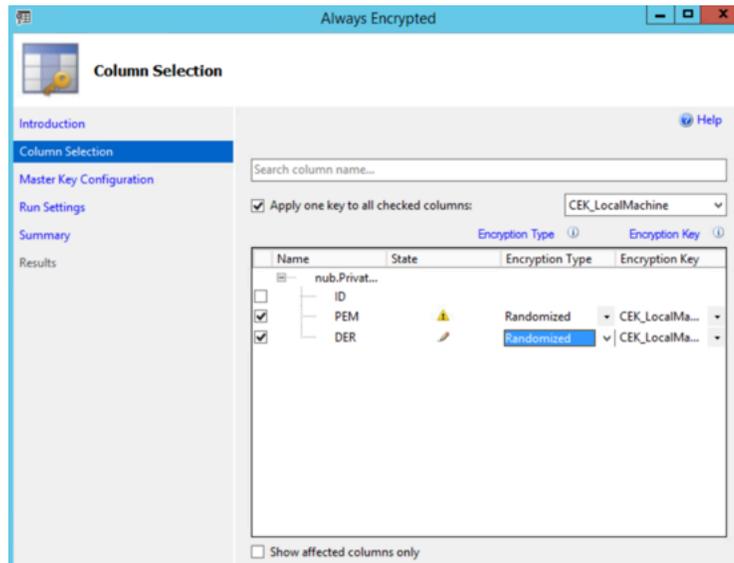
`Figure 21: Column Selection page`

    d) Click **`Next`**.

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

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

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

25. Close `SSMS`.

Encrypt usernames in the NES Database

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

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**.

Connected Worker Platform Deployment in Citrix and RDP Environments

The Connected Worker Platform supports deployments in Citrix and RDP environments.

Connected Worker Platform Deployment in Citrix Environment

The following figure provides an overview of the `Connected Worker Platform` components that are installed in a Citrix environment.

Figure 22: Connected Worker Platform components in a Citrix environment

This figure shows the following configuration:

- The `Nymi Bluetooth Endpoint` is installed on each Citrix client. The `Nymi Bluetooth Endpoint` service on each Citrix client communicates with the `Nymi Agent` service, which is installed on a separate host, on websocket port 9120.
- The `Nymi Agent` is installed in an central location that is accessible to all user terminals, for example on the NES server.
- An *nbe.toml* file is installed on the Citrix client, and is configured with the location of the `Nymi Agent`.
- An NEA runs on the Citrix server and includes the *nymi_api* for communicating with Nymi Bands.

Connected Worker Platform Deployment in RDP Environment

The `Connected Worker Platform` support deployments in RDP Environments.

The following figure provides an overview of the `Connected Worker Platform` components that are installed in an RDP environment.
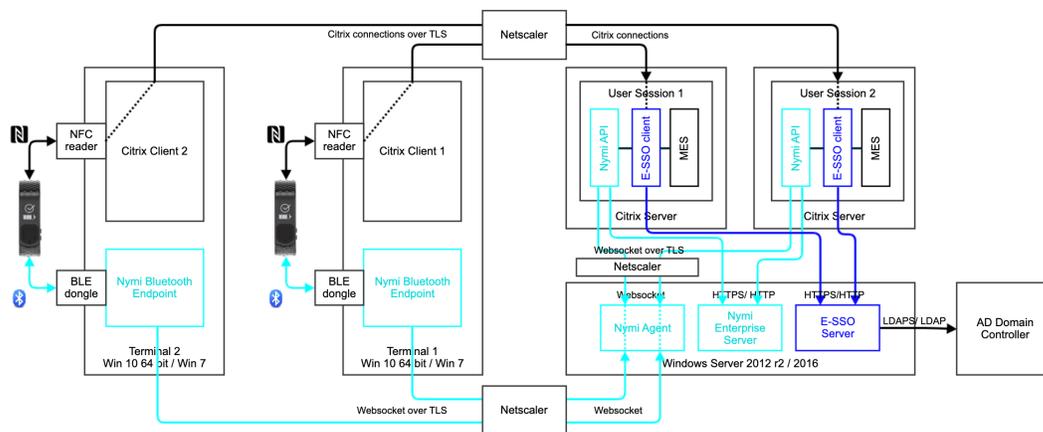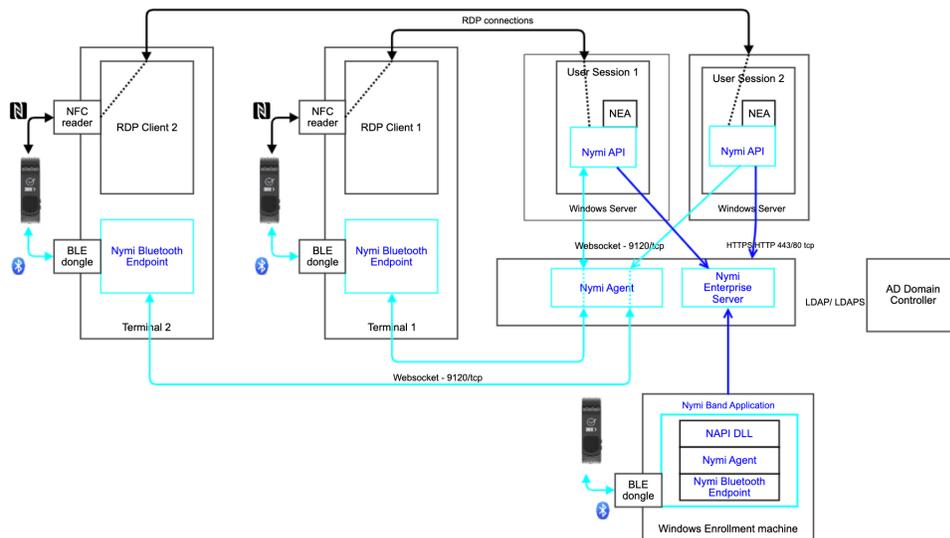
Figure 23: Connected Worker Platform components in a RDP environment

This figure shows the following configuration:

- The `Nymi Bluetooth Endpoint` is installed on each RDP client. The `Nymi Bluetooth Endpoint` service on each RDP client communicates with the `Nymi Agent` service, which is installed on a separate host, on websocket port 9120.
- The `Nymi Agent` is installed in an central location that is accessible to all user terminals, for example on the NES server.
- An *nbe.toml* file is installed on the RDP client, and is configured with the location of the `Nymi Agent`.
- An NEA runs on the RDP server and includes the *nymi_api* for communicating with Nymi Bands.

Installing and Configuring CWP in Citrix and RDP Environments

This section provides information about installing and configuring Nymi components in Citrix and RDP environments.

Nymi API WebSocket Interface Configuration

Configuring and deploying in a physical environment

Take the following into consideration when configuring the `Nymi API WebSocket Interface` and the `Nymi Agent` in a physical environment.

- Ensure that both components have connectivity to NES.
- Each component needs a distinct TCP port.
- Determine how to configure transport layer security, either by configuring it on the server or by offloading.

- If there is a Network Address Translation (NAT) between the `Nymi API WebSocket Interface` and the `Nymi Agent`, the `Nymi Agent` and the client machines use the subcribe operation. See the Nymi API guide that is appropriate for your system for more information.
- Each component can co-locate with the NES (ensure that distinct TCP ports are being used).

Configuring and deploying in a virtual environment

Take the following into consideration when configuring the `Nymi API WebSocket Interface` and the `Nymi Agent` in a Citrix or RDP environment.

In this type of environment, the remote client is used to connect to a Nymi-enabled Application.

Ensure that the following requirements are met:

- Nymi Bluetooth Endpoint is installed on the same machine that is running the remote client software
- The Nymi-enabled Application has knowledge of the remote session address, so it can connect to the correct Nymi Bluetooth Endpoint.

Installing the Nymi Agent

Install the `Nymi Agent` application, which is included in the `Nymi Runtime` installation package, on a machine in the environment. For example, install the `Nymi Agent` application on the same machine as NES. When you install the `Nymi Runtime` software, you can choose to install the `Nymi Agent` application only.

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.
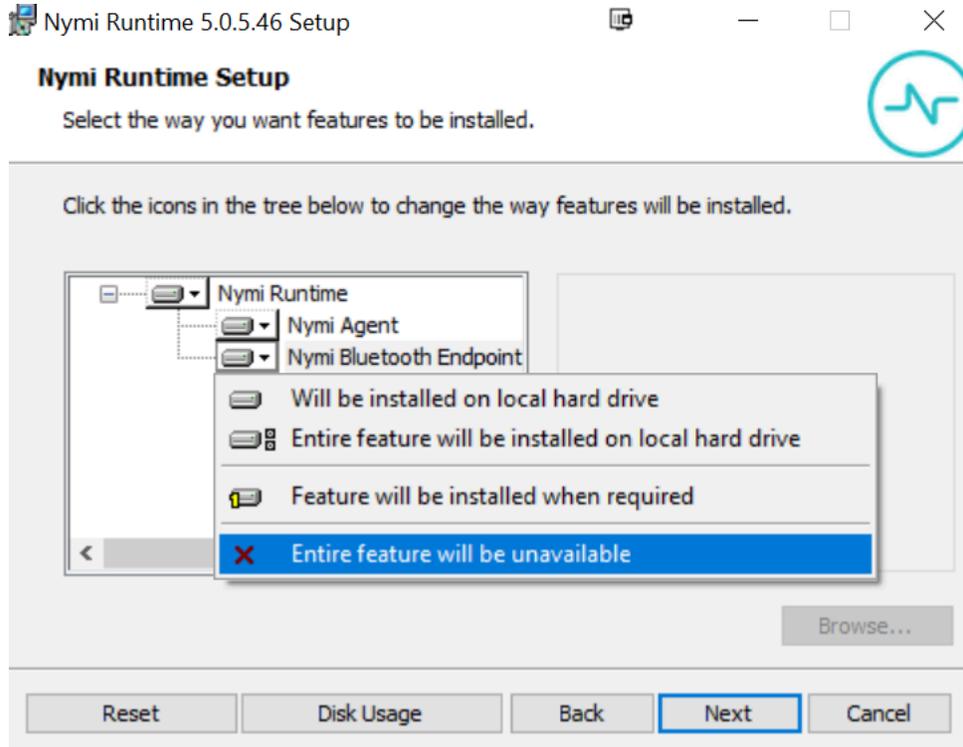

Figure 24: `Nymi Bluetooth Endpoint feature will be unavailable`

Connected Worker Platform Deployment in Citrix and RDP Environments

9. Observe that **Nymi Bluetooth Endpoint** is not available, as shown in the following figure, and then click **Next**.
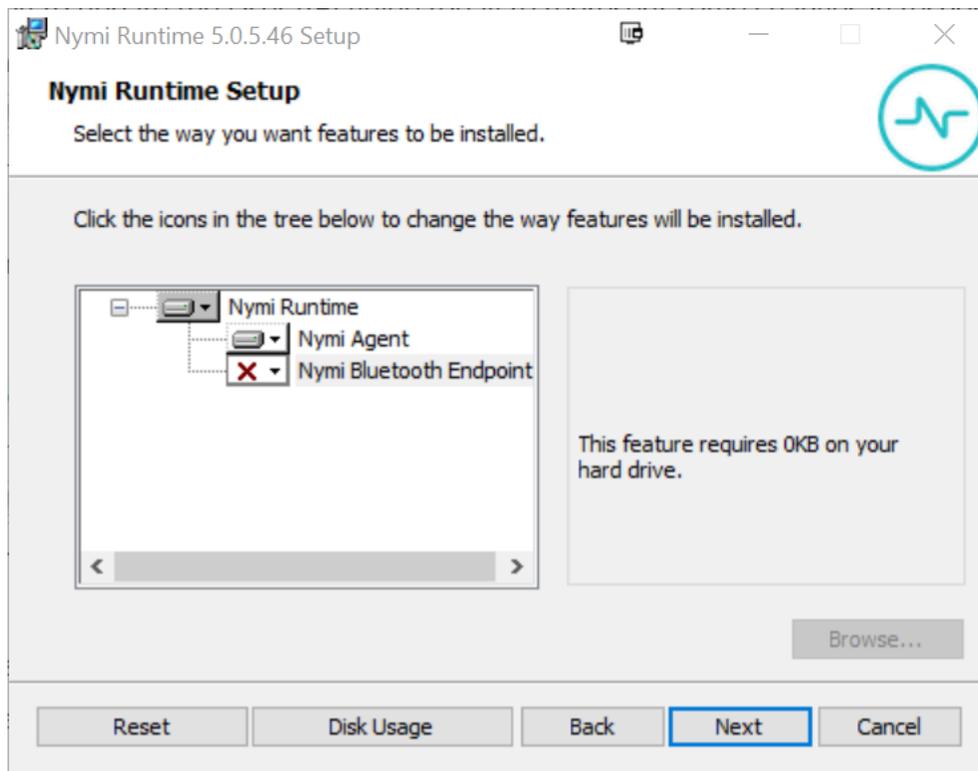

Figure 25: Nymi Bluetooth Endpoint feature is not available

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**.

Note: The `Nymi Agent` must be able to receive incoming WebSocket connections on TCP port 9120 (used for communication with NBE). If the `Nymi API WebSocket Interface` is in use, it must also be able to receive incoming WebSocket connections on the TCP port configured for `Nymi API WebSocket Interface` connections (default 80 when using the ws protocol, and default 443 when using the wss protocol). See the *Nymi API WebSocket Interface Guide* for information about configuring this port. Please ensure that these ports are open in the firewall on the server running the `Nymi Agent`.

Installing the Nymi Bluetooth Endpoint on Local Clients

Install the `Nymi Bluetooth Endpoint`, which is included in the `Nymi Runtime` installation package, on each Citrix or RDP client in the environment. When you install the `Nymi Runtime` software, you can choose to install the `Nymi Bluetooth Endpoint` only.

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

2. Extract the `Nymi SDK` distribution package.

Copyright ©2021   Nymi Connected Worker Platform Deployment Guide v5.0   61

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` window, expand **Nymi Runtime**.

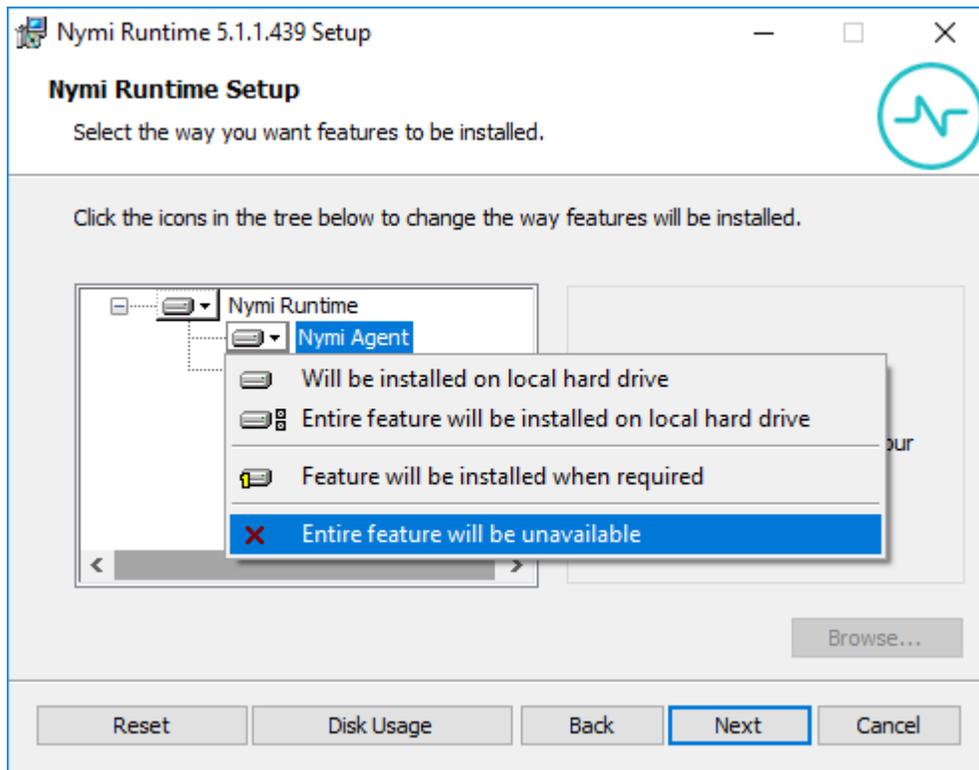8. Select **Nymi Agent**, and then select **Entire feature will be unavailable**, as shown in the following figure.

Figure 26: Nymi Agent feature will be unavailable

9. Observe that **Nymi Agent** is not available, as shown in the following figure, and then click **Next**.
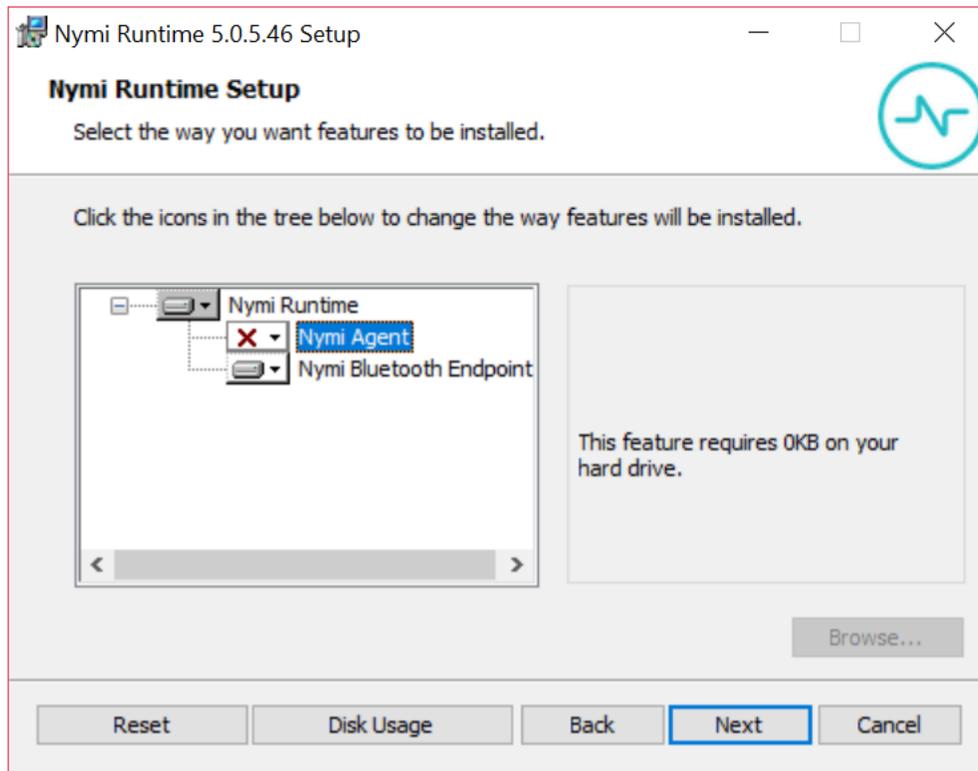
Figure 27: Nymi Agent feature is not available

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**.

Installing Nymi Bluetooth Endpoint on a Thin Client

Thin clients are used to connect to server-based environments, such as virtual desktops, where processes are powered. These servers host desktops and applications, and displays them over the network to the thin client machine. The client machine that communicates with a Nymi Band requires is the `Nymi Bluetooth Endpoint` installed locally, however installing software on thin clients differ between machines and operating systems. As a result, the installation instructions for `Nymi Bluetooth Endpoint` on a thin clients will differ as well. Please refer to the release notes for installation instructions for a particular machine.

Installing NBE on an HP Thin Pro

Follow the instructions below to manually install `Nymi Bluetooth Endpoint` manually. Retrieve the installation file *nbed_1.6.1_amd64.deb* from Nymi. For installation with APT/Repository, refer to

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_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) Unlock read/write access.

   ```
   fsunlock
   ```

4. In **X Terminal** change the directory to the file location of *nbed_x.y.z_amd64.deb* and install the extracted file.

   ```
   dpkg -i nbed_x.y.z_amd64.deb
   ```

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

5. Configure the `Nymi Bluetooth Endpoint` configuration file. The file is located in */usr/bin/ nbe.toml*. Refer to Editing the nbe.toml File.

   The template file, *nbe.default.toml* file contains default information for `Nymi Bluetooth Endpoint`. Edit and save the file as *nbe.toml* to configure `Nymi Bluetooth Endpoint`.

6. Revert the file system to read-only access.

   a) Open **X Terminal**.

   b) Enter:

   ```
   fslock
   ```

   c) Close the terminal.

7. Revert to **User** mode from the system menu, or log in using the credentials of a person in the user domain group. Refer to step 1.

Installing NBE via APT/Repository

Follow the instructions below to install `Nymi Bluetooth Endpoint` via APT/Repository.

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. Unlock read/write access with **X Terminal**.

    a) Click **Start** and go to **Tools**.

    b) Click **X Terminal**.

    c) Unlock read/write access.

```
fsunlock
```

3. Enable the installation of packages by editing the *sources.list* entry:

```
deb http://apt.nymi.com/ xenial main
```

   Refer to the following link for installing a package from Debian (for HP thin clients): https://support.hp.com/si-en/product/hp-t5325-thin-client/4063703/document/c02919995/

4. Download the public key for the Nymi repository server.

```
wget http://apt.nymi.com/nymi_apt.gpg
```

5. Install the key in the APT system.

```
sudo apt-key add ./nymi_apt.gpg
```

6. Update the repository data.

```
sudo apt update
```

7. Install `Nymi Bluetooth Endpoint` via APT.

```
sudo apt install nbed
```

8. Edit the *nbe.default.toml* file and save it as *nbe.toml* to configure `Nymi Bluetooth Endpoint`.

9. Revert the file system to read-only access.

    a) Open **X Terminal**.

    b) Enter:

```
fslock
```

    c) Close the terminal.

10. Revert to **User** mode from the system menu, or log in using the credentials of a person in the user domain group. Refer to step 1.

Editing the Nymi Bluetooth Endpoint Configuration File

The `Nymi Bluetooth Endpoint` file uses the *nbe.toml* file to define the location of a remote `Nymi Agent`

Perform the following steps to specify the URL to the remote `Nymi Agent`.

1. Make a copy of the *C:\Nymi\Bluetooth_Endpoint\nbe.default.toml* file, and name the file *nbe.toml*.

2. Edit the *nbe.toml* file with a text editor.

3. Edit the default `agent_url` parameter and replace the default IP address (127.0.0.1) with the FQDN of the machine that is running the remote `Nymi Agent`.

   For example:

   ```
   agent_url = "ws://agent.nymi.com:9120/socket/websocket"
   ```

   where `agent.nymi.com` is the FQDN of the remote `Nymi Agent` machine.

4. Save the *nbe.toml* file.

5. Restart the `Nymi Bluetooth Endpoint`.

   a) Press the Windows key on the keyboard, or click the start button on the toolbar. Enter "Services" in the search bar. The Services application window appears.

   b) Search for **Nymi Bluetooth Endpoint** in the Services application.

   c) Right-click **Nymi Bluetooth Endpoint** and restart it.

Configuring NBE on Citrix or RDP clients by using group policies

Perform the following steps to create a text file that contains the `Nymi Agent` URL, and then use `Group Policy Preferences` to push the file to each Citrix or RDP client.

Perform the following steps on the domain controller.

1. On the domain controller, create file named *nbe.toml*.

2. Edit the *nbe.toml* file with a text editor and add the following line:

   ```
   agent_url = "ws://agent_server:9120/socket/websocket"
   ```

   where *agent_server* is the FQDN of the host on which you install the `Nymi Agent` software, for example, the NES host that you recorded in the Configuration Attribute Values table.

3. Edit the RSSI (Received Signal Strength Indicator) values in the *nbe.toml* file to configure `Nymi Lock Control` behavior and enable BLE tap. Refer to *Edit the nbe.toml File* in the Nymi Connected Worker Platform Administration Guide for default and suggested values.

4. Use `Group Policy Preferences` to push the *nbe.toml* file to the *C:\nymi\Bluetooth_Endpoint * directory on each Citrix or RDP client that accesses the solution.

Installing the Nymi-enabled Application

The following section describes the tasks that you need to perform to prepare each type network terminal in the environment.

1. Insert the Nymi-supplied Bluetooth Adapter into an available USB port. The Bluetooth adapter is used to detect the presence or absence of Nymi Bands as they move in and out of Bluetooth signal range.

2. Attach a Nymi-supported NFC reader into an available USB port.

3. Install the `Nymi Runtime`. The preceding section describes the `Nymi Runtime` installation procedure.

4. Install the Nymi-enabled Application.

Bluetooth Adapter Placement

The Bluetooth Low Energy (BLE) radio antenna in a 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:

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

Note: The presence of liquids between the Nymi Band and BLE adapter negatively affects the Bluetooth signal quality. This includes beverages and the human body. If BLE taps behave unexpectedly, consider another placement for the BLE 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*).

Performing a customizable Nymi Runtime installation or upgrade

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

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*.

Performing a customizable Nymi Band Application installation

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

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.

Connected Worker Platform High Availability

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 API WebSocket Interface` (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 guide 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.

Overall Deployment Process

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
3. Configure the load balancer for the NES cluster
4. Deploy the Nymi Agent instances
5. Configure the load balancer for the Nymi Agent cluster

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.

Deploy SQL Server AlwaysOn Availability Group

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:

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

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.

Deploy NES Instances

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

1. Map the NES cluster's (virtual server) fully qualified domain name (FQDN) to 127.0.0.1 in C:\Windows\System32\drivers\etc\hosts

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

   a) The NES virtual server's fully qualified domain name (FQDN) instead of the individual server's FQDN should be used in the NES URL

   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 SSL offloading is to be used for NES cluster, make sure HTTP is enabled

Configure the NES Cluster on the Load Balancer

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

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.

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.

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.

Deploy the Nymi Agent Cluster

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

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.

Deploy Nymi Agent Instances

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

Configure the Load Balancer Without WebApi Support

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

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.

Configure the Load Balancer With WebApi Support

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.

Configure the Load Balancer for the Websocket Service on Port 9120

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:

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

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:

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.

Configure SSL/TLS Offloading

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

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.