Deployment Guide

Nymi Connected Worker Platform
v1.0
2022-05-16

Contents

Preface..... 4

Deploy Connected Worker Platform..... 6

Hardware and Software Requirements..... 6

NES Requirements..... 6

Minimum requirements for the Nymi Band Application..... 7

Minimum Requirements for Nymi Lock Control..... 7

Minimum Requirements for User Terminals..... 7

Connected Worker Platform Components in a Local Configuration..... 8

Connected Worker Platform Deployment in Citrix Environment..... 11

Connected Worker Platform Deployment in RDP Environment..... 12

Connected Worker Platform Certificate Overview..... 13

Configuration Settings Attribute Values..... 15

Obtaining Certificates..... 15

Certificates Expiration Dates..... 16

Deploy NES..... 16

Deployment Checklist..... 16

Prerequisite Configuration..... 17

Install and Configure IIS..... 18

Importing a Fullchain Certificate..... 23

Installing NES..... 25

Configuring IIS to Prevent NES Offloading..... 43

Setting Service Principal Names (SPN)..... 46

Managing Database Logins..... 48

Connect to NES for the First Time..... 49

Hardening NES..... 50

Installing and Configuring CWP Components in Local Configuration..... 54

User terminal for Nymi Band Enrollment..... 54

User terminal for NEAs..... 56

User terminal for NES administration..... 69

Installing and Configuring CWP in Citrix and RDP Environments..... 69

User terminal for Nymi Band Enrollment..... 70

Importing the Root CA Certificate in Citrix/RDP Environments..... 72

Centralized Nymi Agent..... 74

Citrix/RDP and Thin Clients..... 76

Nymi API WebSocket Interface Configuration..... 93

Connected Worker Platform High Availability..... 94

Overall Deployment Process..... 94

Deploy the NES Cluster..... 94

Deploy the Nymi Agent Cluster....97

Deploy Smart Distancing and Contact Tracing....100

Prepare for Kubernetes and SDCT Deployment....102
Hardware and Software Requirements....103
DNS Requirements....104
Firewall Port Requirements....105
Certificate Requirements....107
Deployment, Installation, and Configuration Overview....107
Installing Bash on the Kubernetes Administration Terminal....108
Obtaining the SDCT packages....110
Recording the SDCT Variables....110
Creating AD Group for Health Check Application Access....111
Prepare the Database....111
Kubernetes Deployment....114
Deploy A Kubernetes Cluster in AWS Using EKS....115
Customize the Kubernetes environment for SDCT....119
Encrypting the Passwords for Kubernetes Components....132
Launching the Kubernetes Environment....133

Upgrading Connected Worker Platform....135

Upgrading NES....135
Upgrading the Enrollment Terminal....137
Upgrading the Nymi Band application....137
Upgrading User Terminals and Centralized Nymi Agent....138
Upgrading the Nymi Runtime....139
Installing NBE on an HP Thin Pro....140
Update Smart Distancing and Contact Tracing....141
Update the User Terminal....141
Update the CWP environment....146
Update Nymi Band Firmware....149
Before you perform a firmware update....149
Updating Nymi Band Firmware....150
Firmware updater log files....151

Appendix 1 - Scripts....152

Environment Variables for Bare Metal Deployments....152
Details of the create-cluster Script....152
Environment Variables For AWS....153

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 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
1.0	May 16, 2022	First version of this guide the CWP 1.3 release. This includes the following changes: • Moving upgrade instructions from the Nymi Connected Worker Platform Administration Guide. • Added information about how to prevent NES offloading in IIS.

Related documentation

- **Nymi Connected Worker Platform Overview Guide**

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

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

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

  This document provides information about how to develop Nymi-enabled Applications by using the `Nymi API`(`NAPI`).
- **Nymi SDK for C Developer's Guide**

  This document provides information about how to develop Nymi-enabled Applications by using the `Nymi API`(`NAPI`).
- **Nymi SDK for WebSocket Developer's Guide**

  This document provides Nymi developers with an alternative way to utilize the functionality of the `Nymi SDK`, over a WebSocket connection managed by a web-based or other applications.
- **Nymi Connected Worker Platform Troubleshooting Guide**

  This document provides information about how to troubleshoot issues and the error messages that you might experience with the `NES Administrator Console`, the Nymi Enterprise Server deployment, the Nymi Band, and the `Nymi Band Application`.
- **Connected Worker Platform Release Notes**

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

How to get product help

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

How to provide documentation feedback

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

Deploy Connected Worker Platform

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.

Hardware and Software Requirements

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

NES Requirements

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

Software requirements

NES has the following software requirements.

- Microsoft Windows Server 2016 or 2019
- Microsoft IIS
- Microsoft SQL Server 2016 and later
- Microsoft .NET Framework 4.8

Note: Microsoft SQL Server Express 2017 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

Minimum requirements for the Nymi Band Application

The section summarizes the minimum software and hardware requirements for the Nymi Band Application.

Software requirements

- Windows 10, 64-bit
- Windows 7, 64-bit

Note: It is recommended to use 125% scaling and 1920 x 1080 screen resolution for the terminal hosting the Nymi Band Application.

Hardware requirements

- 4GB RAM
- 5GB free disk space
- 2 core CPU (recommended)
- 1 USB 2.0 port
- Bluetooth Low Energy (BLE) radio antenna, present in Bluegiga BLED112 BLE adapter.

Minimum Requirements for Nymi Lock Control

`Nymi Lock Control` supports the following operating system versions:

- Windows 10, 64-bit

Other considerations:

- `Nymi Lock Control` is a single domain solution. All terminals must be on the same domain as the Nymi Enterprise Server host, not across separate domains.
- `Nymi Lock Control` users can lock the desktop of a user terminal and the desktop of a Microsoft Remote Desktop Connection and Citrix when Network Level Authentication (NLA) is disabled.
- Each user terminal requires a connected Bluetooth Low Energy (BLE) radio antenna, such as a Bluegiga BLE adapter..

Minimum Requirements for User Terminals

CWP 1.3 supports the following operating systems on which you can install `Nymi Runtime` and use the Nymi Band to perform authentication tasks in an MES application.

- Windows 10 x86-64, including on Citrix, RDP, and VMWare Horizon
- HP ThinPro x86-64, including on VMWare Horizon
- IGEL OS v10, including IGEL Thin Client on Citrix

Connected Worker Platform Components in a Local Configuration

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.

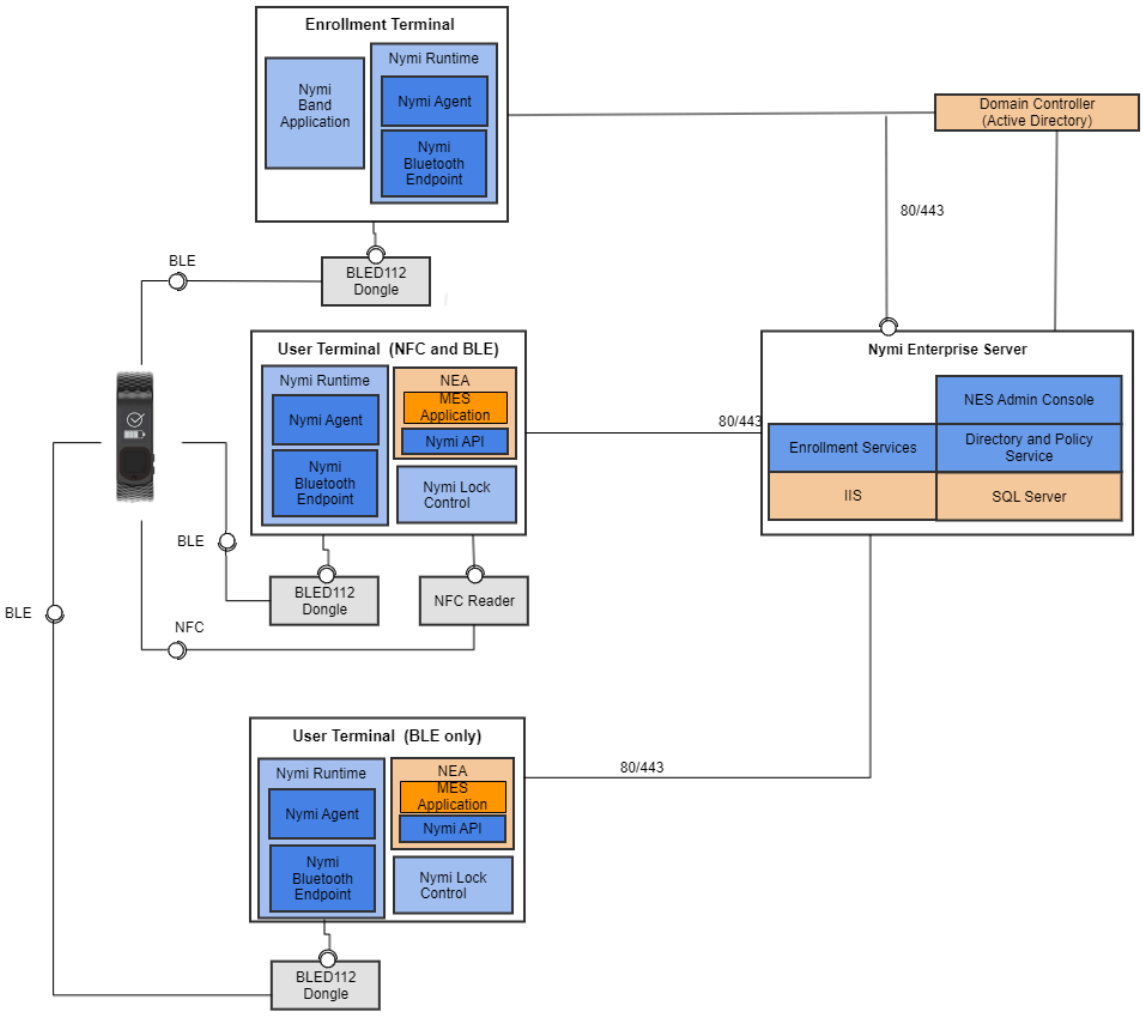


Figure 1: Connected Worker Platform components and connection ports

This guide Connected Worker Platform consists of the following components. Smart Distancing and Contact Tracing components are described in the Nymi Smart Distancing and Contact Tracing Installation and Configuration Guide.

Table 2: Connected Worker Platform Components Covered in this Guide

Component	Description
Enrollment Terminal	Windows 10 machine that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal and is used to enroll a new user and link them to their Nymi Band. The `Nymi Band Application` requires the `Nymi Runtime` application, which the `Nymi Band Application` automatically installs.
Nymi Runtime	A Windows application that you install on the enrollment terminal and user terminals. `Nymi Runtime` includes the `Nymi Agent` and `Nymi Bluetooth Endpoint` components. `Nymi Runtime` supports communication between NES, the Nymi Band, NEAs, the `Nymi Band Application` and `Nymi Lock Control`.
User Terminal	Windows 10 machine on which you install Nymi components that allow users to perform authentication tasks with the Nymi Band.
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.
Nymi-enabled Application	Developers can create corporate applications that integrate with Connected Worker Platform by using the `Nymi API`. These applications are called Nymi-enabled Applications (NEAs) and include Manufacturing Execution Systems (MES), Single Sign-On (SSO), and Human Machine Interface (HMI) applications. An NEA requires the Nymi Runtime software.
Nymi Lock Control	A Windows application that allows the user to unlock their terminal without entering their username and password.

Component	Description
Nymi Enterprise Server (NES)	• A Management server and collection of services that provides the `NES Administrator Console` and coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates. Includes the following services: • Enrollment Service (ES) - authenticates, validates, and authorizes certificate requests from requesters, such as the Nymi Band Application and NEAs. • Directory and Policy Services (DPS) - maintains the NES database, which contains a list of Active Directory (AD) users and the Nymi Bands that are associated with each user. Provides IIS web services, which allows the NES Administrator Console access to the NES database. • Authentication Service (AS) - provides authentication and authorization support for domain users and computers. AS uses adapters to interface with external directory and database systems, such as an AD adapter to interface with Active Directory.
Domain Controller (DC)	Windows server with external directory and database systems, such as Active Directory.

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.

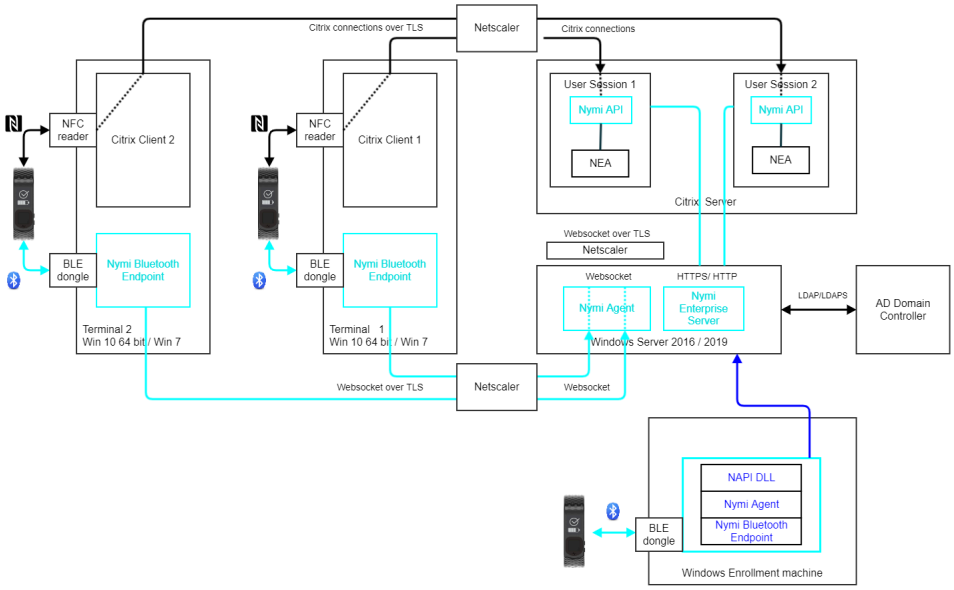


Figure 2: Connected Worker Platform components in a Citrix environment

In Citrix and RDP environments, the user launches an NEA that is installed on a remote session host. Different user sessions run their own NEA instance. In this configuration the NEA communicates with a centralized Nymi Agent, which is installed on a single machine or a cluster of two or more machines in the 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.

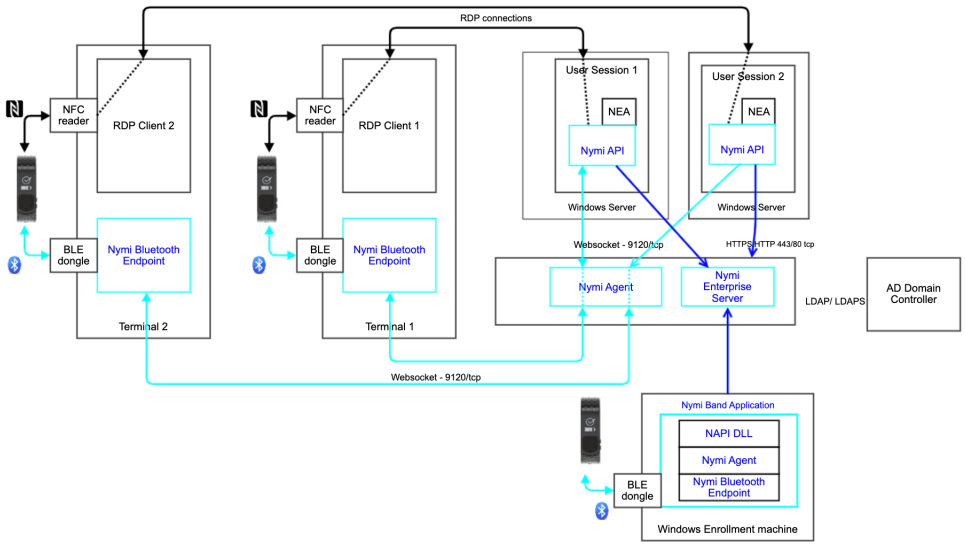


Figure 3: Connected Worker Platform components in a RDP environment

In RDP environments, the user launches an NEA that is installed on a remote session host. Different user sessions run their own NEA instance. In this configuration the NEA communicates with a centralized Nymi Agent, which is installed on a single machine or a cluster of two or more machines in the 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.

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.

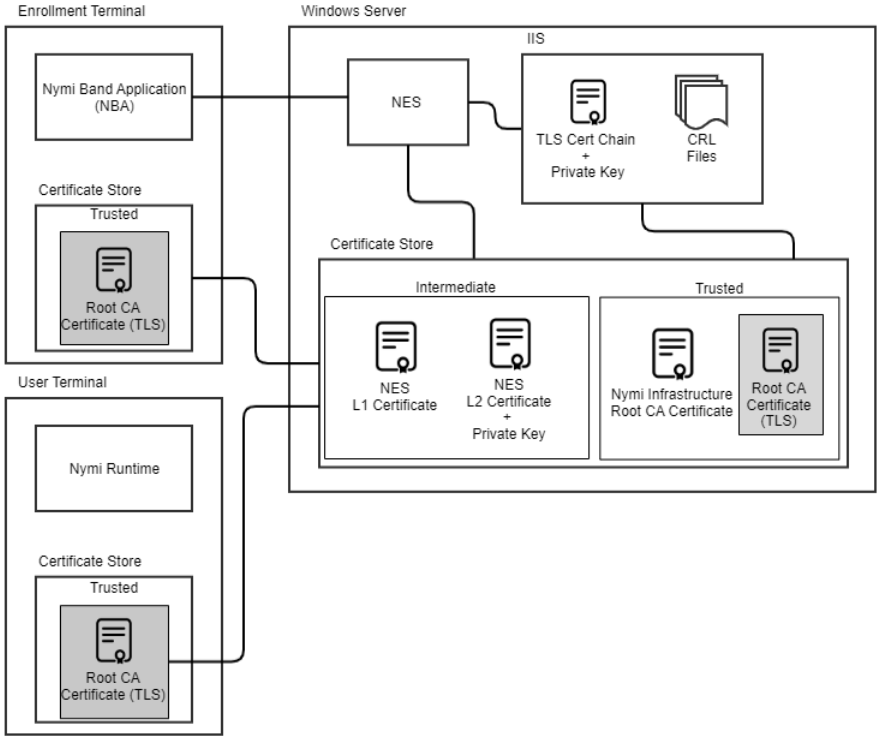


Figure 4: Certificates required in a Connected Worker Platform environment

- 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.

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)	

Obtaining Certificates

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

About this task

Contact your Nymi Solution Consultant to plan the certificate configuration.

Procedure

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.

Procedure

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.

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.	

Deploy NES

The following sections provide information about how to deploy NES.

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	

Task	Status
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	
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.

About this task

Procedure

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.

About this task

Procedure

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.

Procedure

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

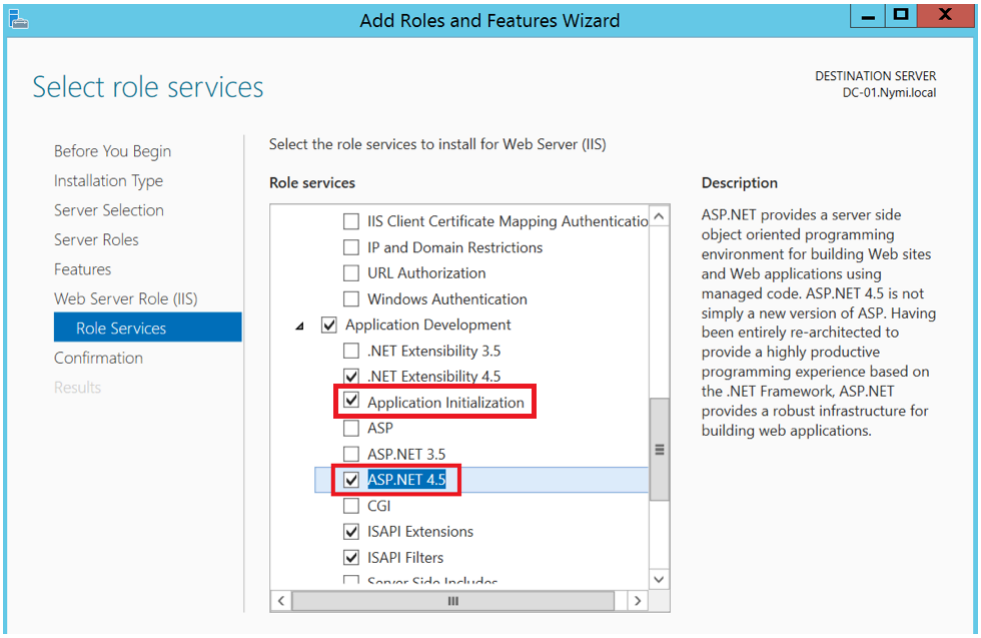


Figure 5: Select role services page with ASP.NET and Application Initialization selected

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.

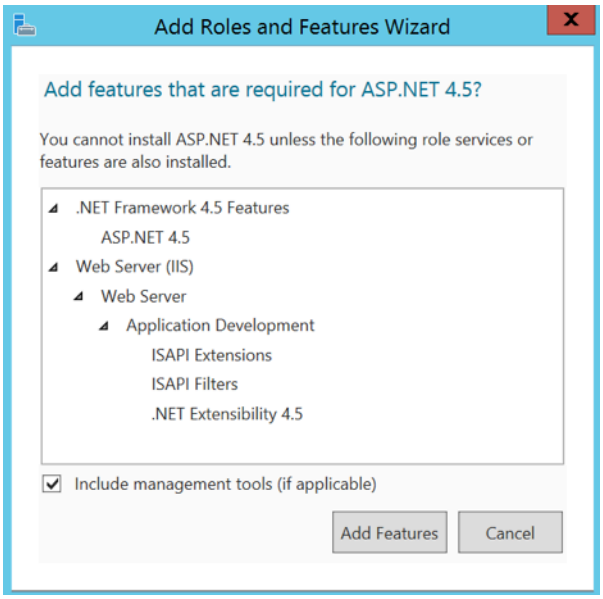


Figure 6: Add features that are required for ASP.NET

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

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

Importing the TLS server certificate

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

About this task

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

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

Procedure

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

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

About this task

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

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

Procedure

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

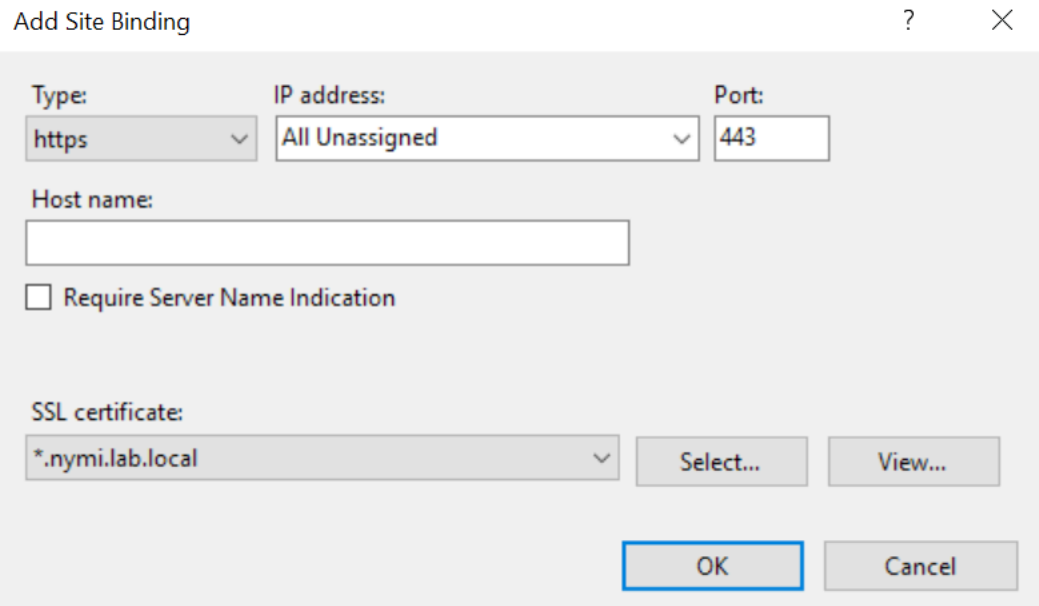


Figure 7: Add Site Binding Dialog

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**.

Importing a Fullchain Certificate

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

About this task

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

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

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

Importing certificates

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

About this task

Procedure

1. Extract the certificate zip file to a directory.
2. Right-click the *fullchain.p12* certificate file and then select **`Install PFX`**.
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`**.

Moving the L2 certificate

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

About this task

Procedure

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

   The `certlm` window appears.
2. On the `User Account Control` dialog, click `Yes`.
3. Navigate to **`Personal > Certificates`** folder.
4. Expand **`Intermediate Certification > Certificates`**, and then move the NES L2 CA certificate from **`Personal > Certificates`** to the **`Intermediate Certification > Certificates`** folder.

   You can move the file by dragging and dropping it from one folder to the other folder.
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, install and configure NES. You can configure NES in one of the following ways:

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

Installing the NES Services Suite using the wizard

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

About this task

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

Procedure

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

   Note: For the best user experience with the NES installation wizard, resolution of 1920 x 1080 and 100% scaling is recommended.
2. In the *C:\nestemp\NesInstaller* folder, run *install.exe*.
3. On the `User Account Control` dialog, click **`Yes`**.
4. On the `Open File – Security Warning` page, click **`Run`**.
5. On the `NESg2. Installer Setup` page, review the Microsoft .NET EULA, and then click **`Accept`**.
6. On the `Open File - Security Warning` dialog, click **`Run`**.
   The installer installs .NET.
7. Restart the host when the installation process prompts you.
8. If the installation process does not continue after the restart, rerun *C:\nestemp\NesInstaller \install.exe*.
9. On the `Open File - Security Warning` dialog, click **`Run`**.
10. On the `Application Install Security Warning` pop-up, click **`Install`**.

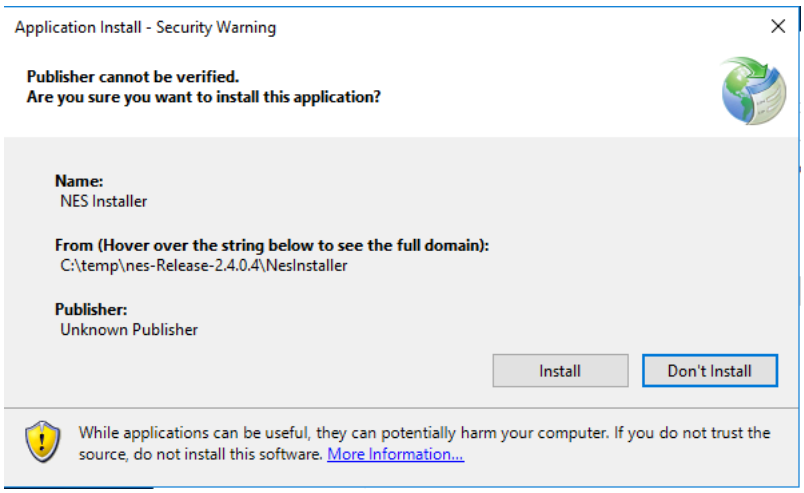


Figure 8: Security Warning

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 SQL Server application is on a different server, the Install Prerequisites dialog appears. Click **No** to continue with the software installation.

    When you configure NES in the following section, you provide connection information for the remote SQL Server.
14. If the installer does not detect a version of SQL Server on the host, the Install Prerequisites dialog appears. Perform of the following actions:

    a) To install SQL Express, click **Yes**.

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

Results

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

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

The following figure shows the Prerequisites Check dialog.

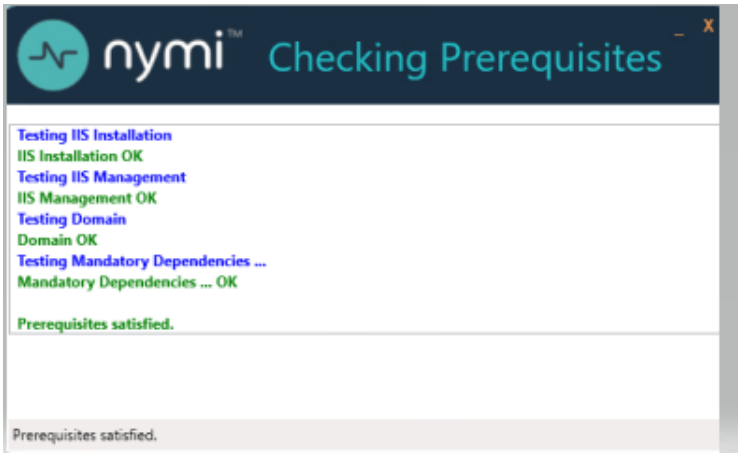


Figure 9: Prerequisites Check Dialog

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 Manually

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

Before you begin

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

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

About this task

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

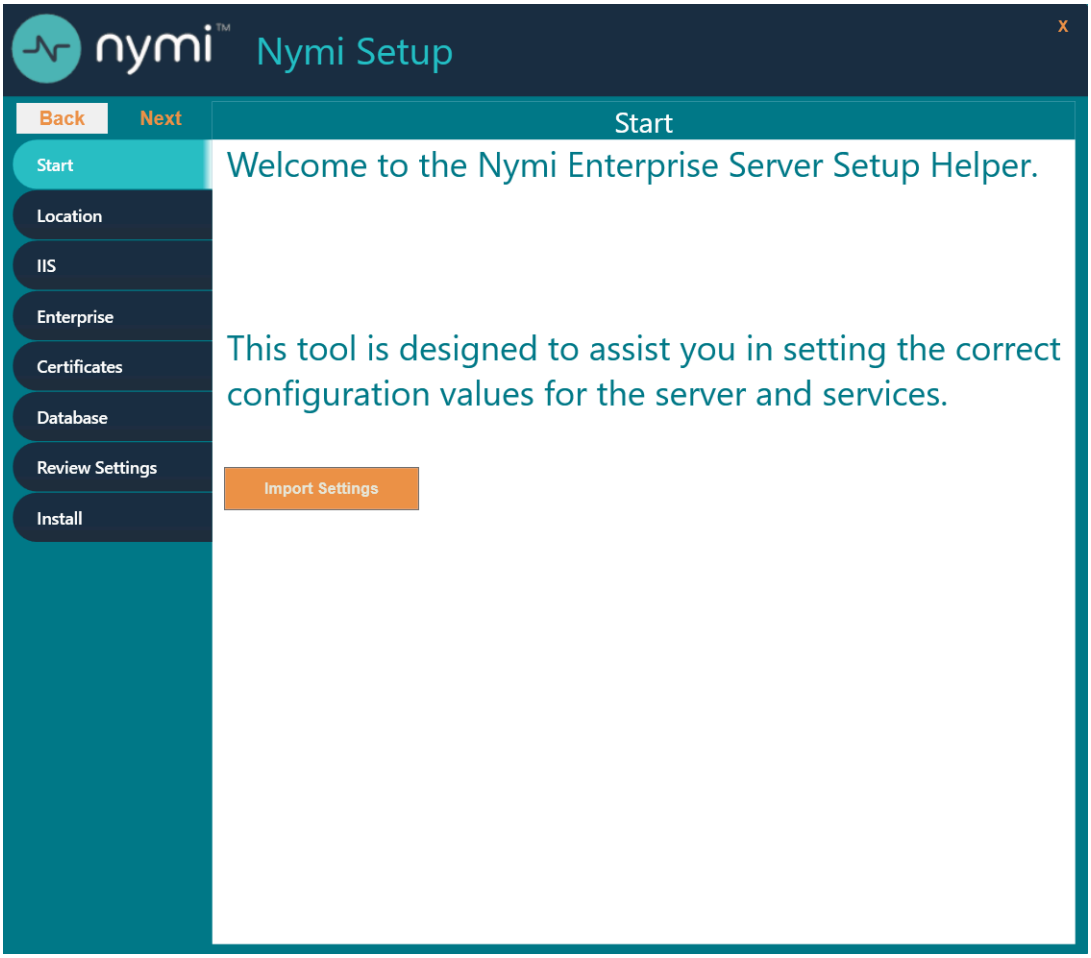


Figure 10: NES Setup Help wizard

Perform the following actions to configure the NES Services Suite.

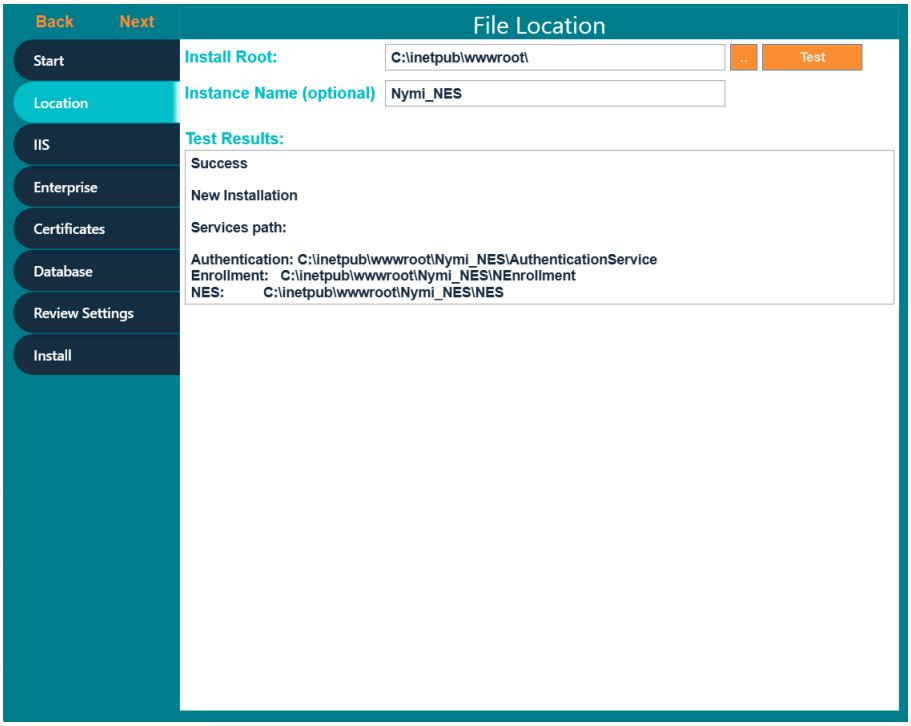
Note: The **Import Settings** button allows you to load a configuration file to install NES. Creating the configuration file to deploy a subsequent NES is explained later in this document.

Procedure

1. In the left navigation pane, select Location, and then perform the following actions:
   a) In the **Install Root** field, leave the default location *C:\inetpub\wwwroot* or, to select an alternate installation path for the NES services, click the ellipses and navigate to the folder.
   b) In the **Instance Name** field, type a descriptive name for the NES web application instance name, for example NES.

      This step optional, but recommended. The name cannot contain spaces. Record the Instance Name in the Configuration Attribute Values table.
   c) Click the **Test** button to determine the status of the installation. The test result specifies the type of installation, and the paths for the Authentication Service, NES, and Enrollment Service. The service locations are based on the value specified in the **Instance Name** field.

The following figure provides an example of the `Location` page.



`Figure 11: 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 and is required for CWP with Evidian deployments. If an HTTPS address is not available, review *Adding HTTPS site bindings* to add a HTTPS site binding.

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

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

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

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

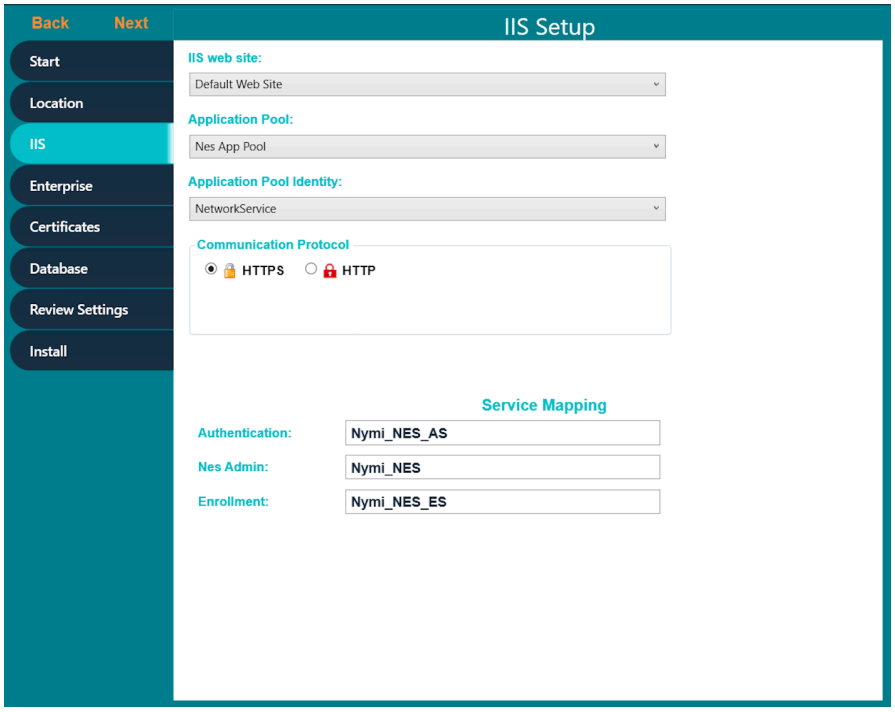


Figure 12: IIS Setup page in the NES Setup wizard

The following figure displays the warning that appears when you select HTTP as the communication protocol.

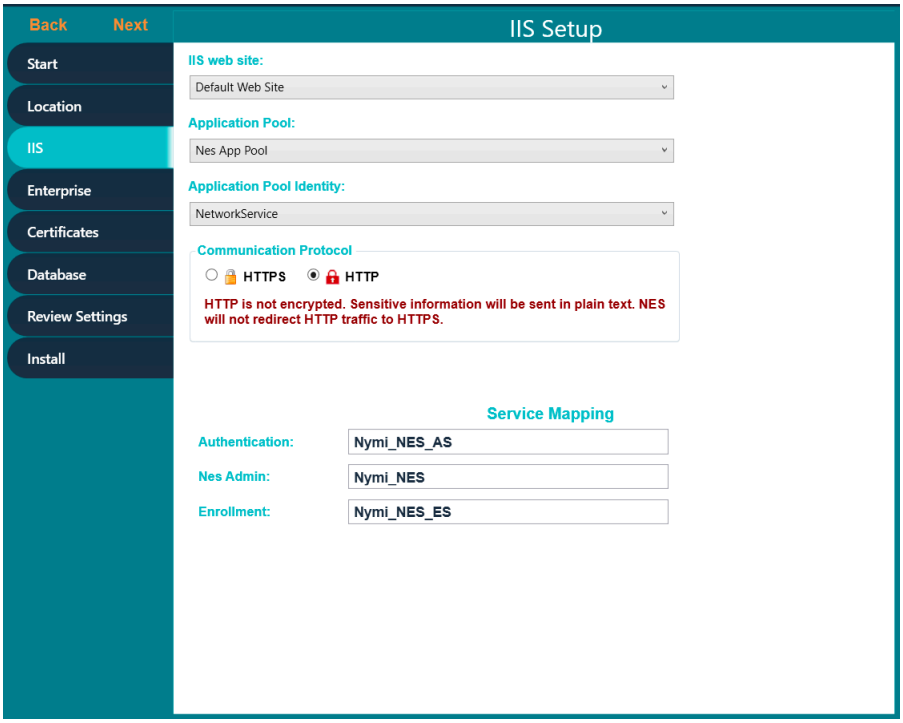


Figure 13: IIS Setup Page HTTP Warning

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:

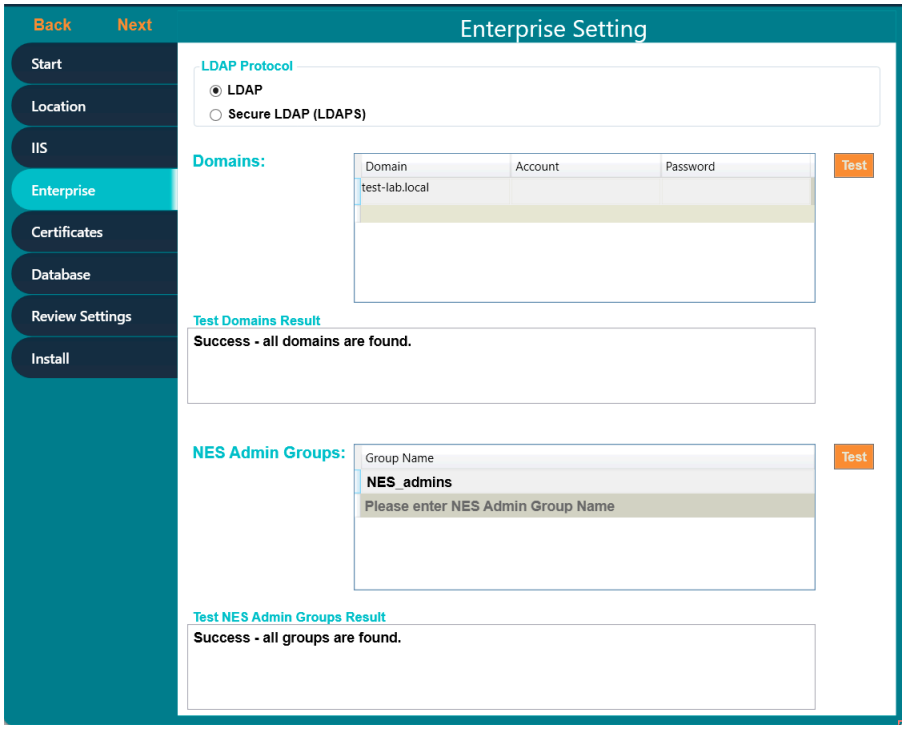
   a) In the **Domain** table, on an empty line, type the NetBIOS (Pre-Windows 2000) name of the domain that contains the user accounts.

   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 14: 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 **Certificate Expiry** field, leave the default value for the length of time that the NEA tokens remains valid. The default is 14 days.
   b) From the **Level One Certificate** list, select the CN value of the L1 certificate from the list.

      The L1 certificate name is in the form *enterprise_name* `NES L1` CA.
   c) From the **Level Two Certificate** list, select the CN of the L2 certificate.

      The following figure provides an example of the `Certificates` page.

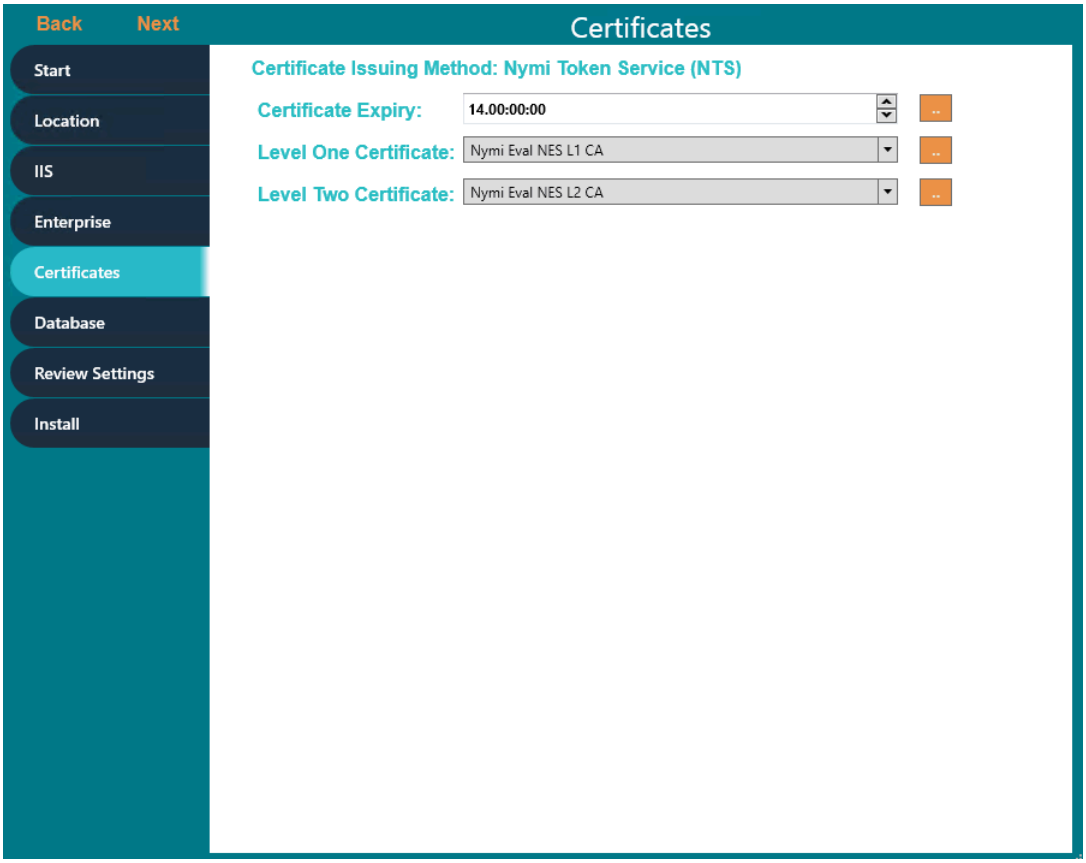


Figure 15: Certificates page in the NES Setup wizard

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

   - Windows Authentication

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

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

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

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

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

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

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

- SQL Authentication

a. Clear the **Integrated Security** option. This sets the security property in the **Connection String** to **False**.
b. If required, update the connection string with the database instance that you want to use instead of the default SQL Express 2012. Refer to https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax for more information about defining the connection string.
c. In the **SQL Login** section, enter the username and password, and then click **Verify** to ensure the provided credentials are valid.
d. Click **Test** to verify that the database connection string is valid and NES can connect to the database server.

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

The following figure provides an example of the **Database Setup** page for Windows Authentication.

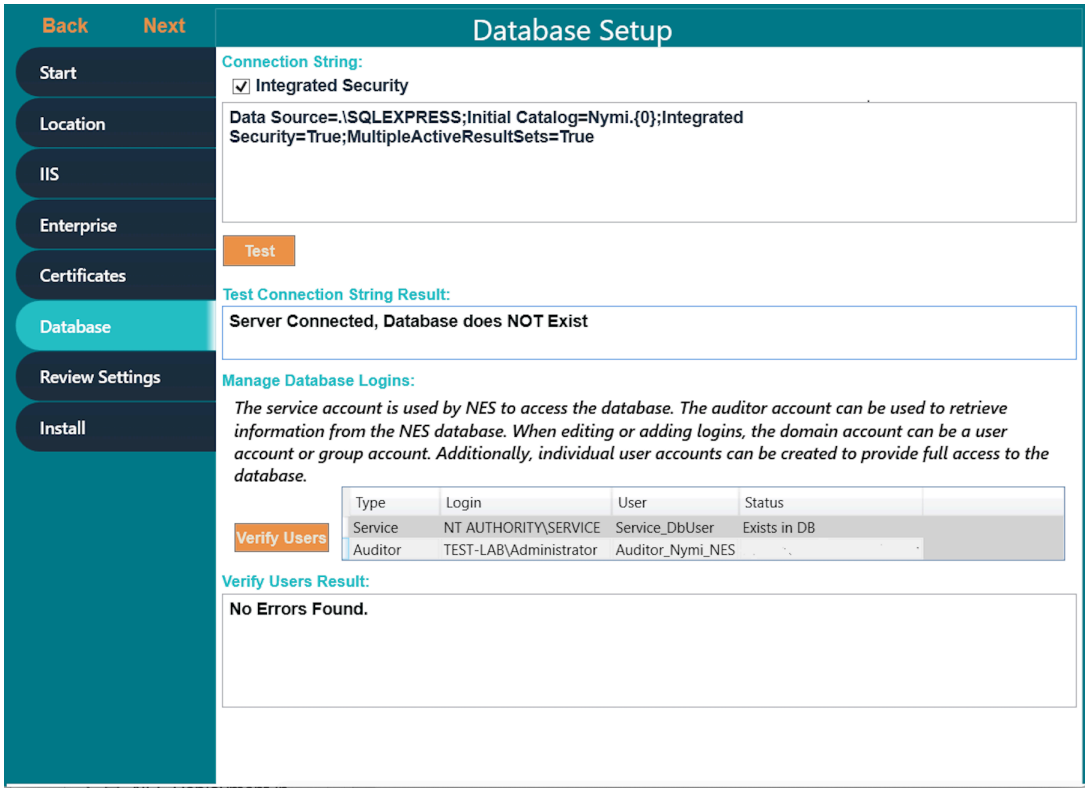


Figure 16: Database Setup page in NES Setup wizard for Windows Authentication

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.

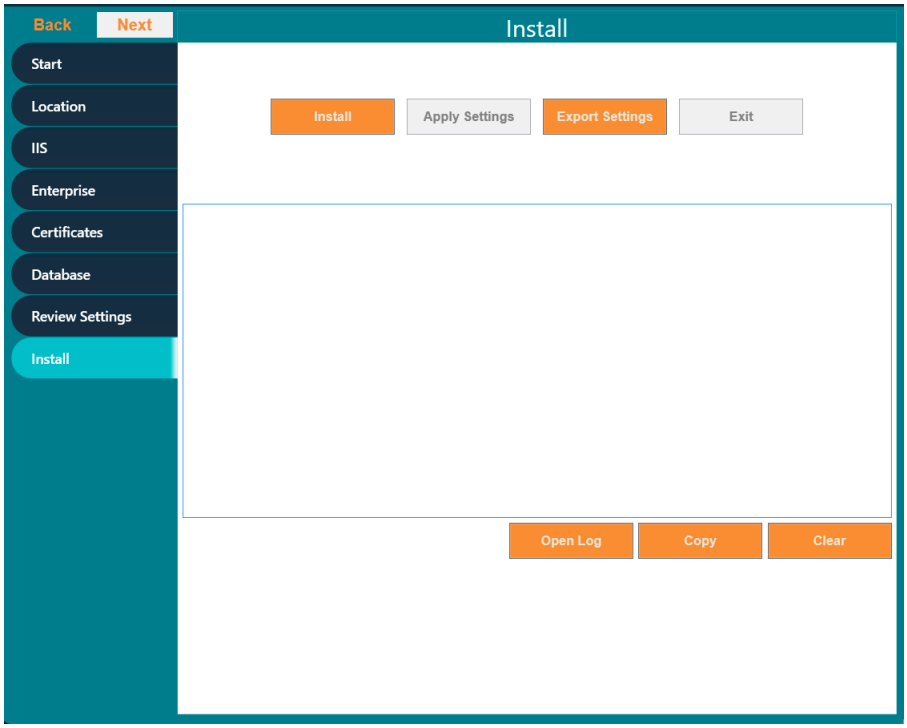


Figure 17: Install NES page in NES Setup wizard

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.

About this task

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

Procedure

1. In the *C:\nestemp\NesInstaller* folder, run *install.exe*.
2. On the `Location` tab, in the **`Instance Name`** field, type the instance name that was specified during the deployment.
3. On the `Database` tab, click **`Test`** and **`Verify Users`** to load the database information.
4. On the `Install` tab, click **`Export Settings`**.
5. On the `Export Settings` dialog, perform the following actions:
   a) In the **`File Name`** section, click the ellipses, and then navigate to the location where you want to save the configuration file.

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

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

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

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

        Note: This saves the file with machine-specific encryption; therefore, you can only load the configuration file on the same machine on which you save the configuration.
      - **`Private key`**, to save the configuration and encrypt the configuration file with a private key.

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

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

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

   c) Click **`OK`**.

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.

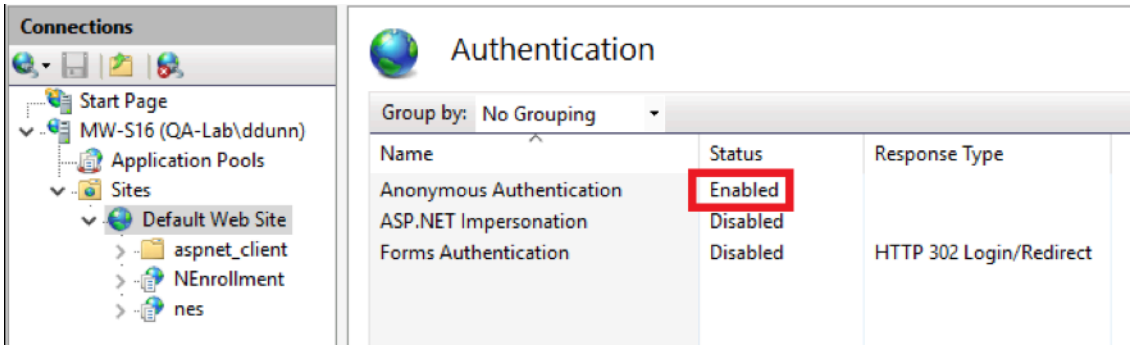
About this task

Procedure

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 18: 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.

Before you begin

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

About this task

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

Procedure

1. On a Domain Controller, open the `Group Policy Management` panel.
2. Expand **`Forest > Domains`**, right-click the domain that contains the hosts, and then select **`Create a GPO in this domain, and Link it here`**.
3. In the **`Name`** field, type `Nymi`.
4. In the **`Source Starter GPO`** field, leave the default value (none).
5. Click **`OK`**.
6. Expand the domain and select **`Nymi`**. Click **`OK`**.
7. On the **`Scope`** tab, under **`Security Filtering`**, perform the following actions:
   a) Select **`Authenticated Users`**.
   b) Click **`Remove`**.
   c) On the `Group Policy Management` confirmation window, click **`OK`**.
   d) On the warning window, click **`OK`**.
   e) Click **`Add`**.

f) On the `Select Users, Groups and Computers` window, type the name of the group that contains the user terminals, click **`Check Names`**, and then click **`OK`**.
The group appears in the Security Filter section.

8. On the **`Setting`** tab, right-click **`Computer Configuration`**, and then select **`Edit`**.
9. Expand **`Computer Configuration > Preferences > Windows Settings`**.
10. Right-click **`Registry`**, and then select **`New > Registry Item`**.
    The `New Registry Properties` window appears.
11. From the **`Action`** list, select **`Create`**.
12. From the **`Hive`** list, leave the default value **`HKEY_LOCAL_MACHINE`**.
13. In the **`Key Path`** field, type `SOFTWARE\Nymi\NES`.
14. In the **`Value name`** section, type `URL`.
15. In the **`Value Data`** field, type `https://nes_server/NES_service_name/`
    where:

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

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

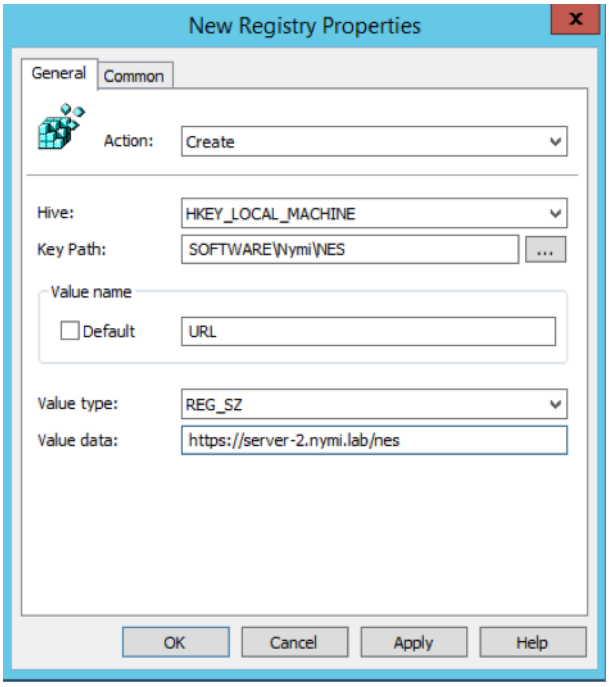


Figure 19: URL properties page

16. Click **OK**.

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

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

Before you begin

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

About this task

Create a group policy object to update the registry.

Procedure

1. On a Domain Controller, open the `Group Policy Management` panel.
2. Expand **`Forest > Domains`**, right-click the domain that contains the hosts, and then select **`Create a GPO in this domain, and Link it here`**.
3. In the **`Name`** field, type `Nymi Agent`.
4. In the **`Source Starter GPO`** field, leave the default value (none).
5. Click **`OK`**.
6. Expand the domain and select **`Nymi Agent`**. Click **`OK`**.
7. On the **`Scope`** tab, under **`Security Filtering`**, perform the following actions:
   a) Select **`Authenticated Users`**.
   b) Click **`Remove`**.
   c) On the `Group Policy Management` confirmation window, click **`OK`**.
   d) On the warning window, click **`OK`**.
   e) Click **`Add`**.
   f) On the `Select Users, Groups and Computers` window, type the name of the group that contains the user terminals, click **`Check Names`**, and then click **`OK`**.
   The group appears in the Security Filter section.
8. On the **`Setting`** tab, right-click **`Computer Configuration`**, and then select **`Edit`**.
9. Expand **`Computer Configuration > Preferences > Windows Settings`**.
10. Right-click **`Registry`**, and then select **`New > Registry Item`**.
    The `New Registry Properties` window appears.
11. From the **`Action`** list, select **`Create`**.
12. From the **`Hive`** list, leave the default value **`HKEY_LOCAL_MACHINE`**.
13. In the **`Key Path`** field, type `SOFTWARE\Nymi\NES`.
14. In the **`Value name`** section, type `AgentUrl`.
15. In the **`Value Data`** field, type `ws://NymiAgent:port/socket/websocket`
    where:

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

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

16. Click **OK**.

Configuring NES from a Configuration File

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

Before Installing NES using the Silent Installer

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

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

Installing .NET and SQL Server Express

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

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

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

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

Configuring NES Silently from the Command Line

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

Before you begin

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

- Log into your machine with a domain user account that has local administrative privileges
- Copy and extract the installation package to the machine
- Install .NET. The installation package contains the .NET 4.8 software and Microsoft SQL Server Express in the following directories: .NET 4.8 software: ..*NesInstaller**DotNetFX48*\ . The .NET installation may require you to restart your computer.

- Install SQL Express if you do not have an existing MS SQL Server to store the NES database. The installation package contains Microsoft SQL Server Express 2019 in the following location: .. *PreRequisites**SqlExpress* During the SQL installation, accept all defaults. The installation process creates all Microsoft SQL Server users automatically. On the Database Engine Configuration screen, add additional users that require access to the audit reports in the SQL database.

About this task

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

To install NES using the silent installer:

Procedure

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

   where:

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

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

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

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

Configuring NES With a Configure File in the NES Setup Wizard

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

About this task

Procedure

1. In the NES Setup Wizard, on the `Start` screen, click **`Import Settings`**.

2. In the Open window, navigate to the directory that contains the *ninst* configuration file, and then double-click the *.ninst* file.
   A **Loaded Successfully** message appears on the screen.
3. On the **Review Settings** tab, click **Test**
   The window displays a Success message when the configuration file values are valid or displays error messages when the configuration file requires correction.
4. If the **Review Settings** test did not report errors, on the **Install** tab, click **Install**.
5. When the installation completes, close the NES Setup wizard.

Configuring IIS to Prevent NES Offloading

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

About this task

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

Procedure

1. In the Connections navigation pane, expand **Computer_Name > Application Pools > Default Web Site**, and then perform the following steps to determine the application pool name for each NES application.
   a) Select the **nes** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.
   b) In the Edit Application window, make note of the value that appears in the **Application Pool** field, and then click **OK**.
   c) Select the **nes_AS** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.
   d) In the Edit Application window, make note of the value that appears in the **Application Pool** field, and then click **OK**.
   e) Select the **nes_ES** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.
   f) In the Edit Application window, make note of the value that appears in the **Application Pool** field, and then click **OK**.

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

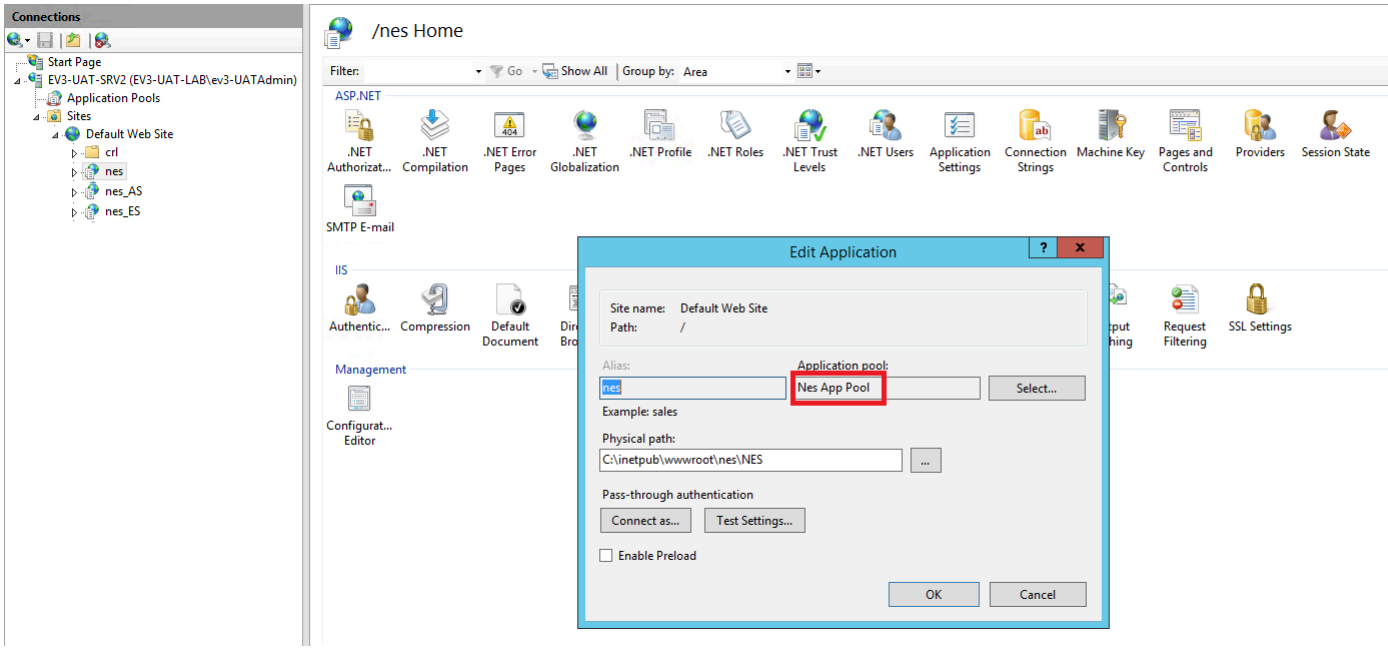


Figure 20: Edit Application window

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

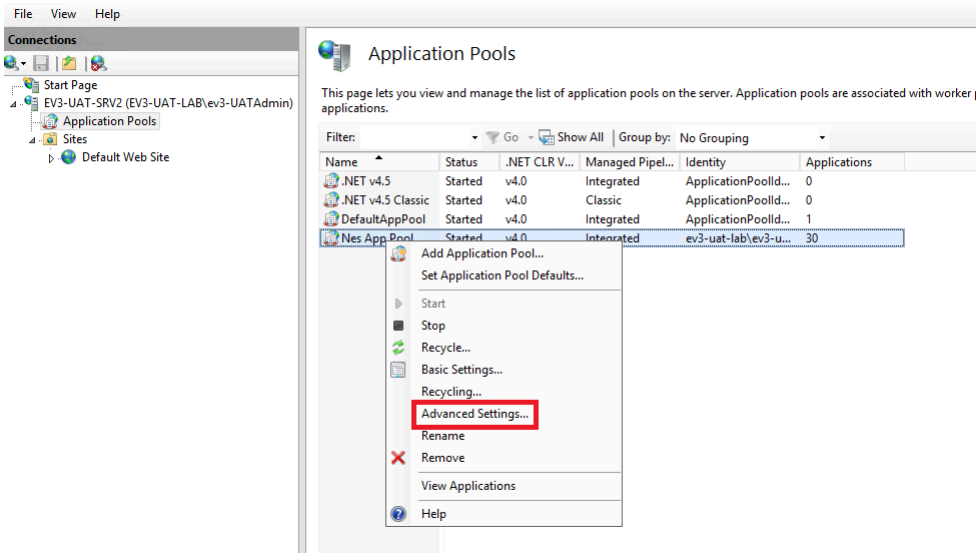
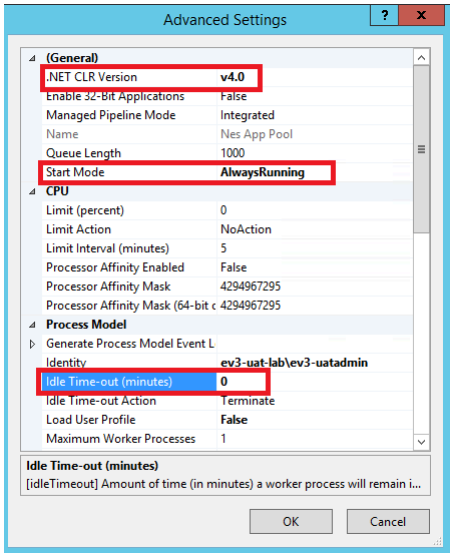


Figure 21: Advanced Settings menu option

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

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



`Figure 22: Advanced Settings window`

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

4. In the `Connections` navigation pane, expand **`Computer_Name > Application Pools > Default Web Site`**, and then perform the following steps.
   a) Right-click **`nes`** and then select **`Manage Application > Advanced Settings`**.
   b) On the `Advanced Settings` window, from the **`Preload Enabled`** list, select **`True`**.
   c) Click **`OK`**.
   d) Right-click **`nes_AS`** and then select **`Manage Application > Advanced Settings`**.
   e) On the `Advanced Settings` window, from the **`Preload Enabled`** list, select **`True`**.
   f) Click **`OK`**.
   g) Right-click **`nes_ES`** and then select **`Manage Application > Advanced Settings`**.
   h) On the `Advanced Settings` window, from the **`Preload Enabled`** list, select **`True`**.
   The following figure provides an example of the **`Advanced Settings`** window.

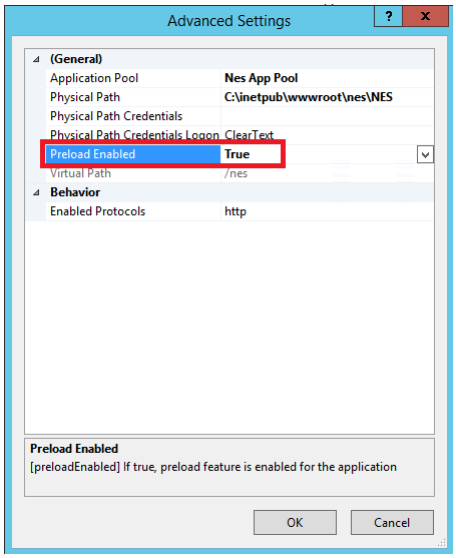


Figure 23: Advanced Settings window

i) Click **OK**.

5. Close IIS Manager.

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

About this task

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

Note: To check the existing SPN entries associated with the App Pool Account, run the command `setspn -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.

Procedure

Open a command prompt as an Administrator and type:

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

where:

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

Single Node SPN Creation

About this task

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

Procedure

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 application 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

About this task

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

Procedure

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

   where you replace:

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

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

   where you replace:

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

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

   where you replace:

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

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.

About this task

To add a new user perform the following steps:

Procedure

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

About this task

To edit a database login, perform the following steps:

Procedure

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

About this task

You can delete any Auditor login that you have added.

Procedure

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.

About this task

Procedure

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

   depending on the NES configuration, where:

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

     For example, `https://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.

What to do next

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.

Before you begin

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

About this task

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

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

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

Procedure

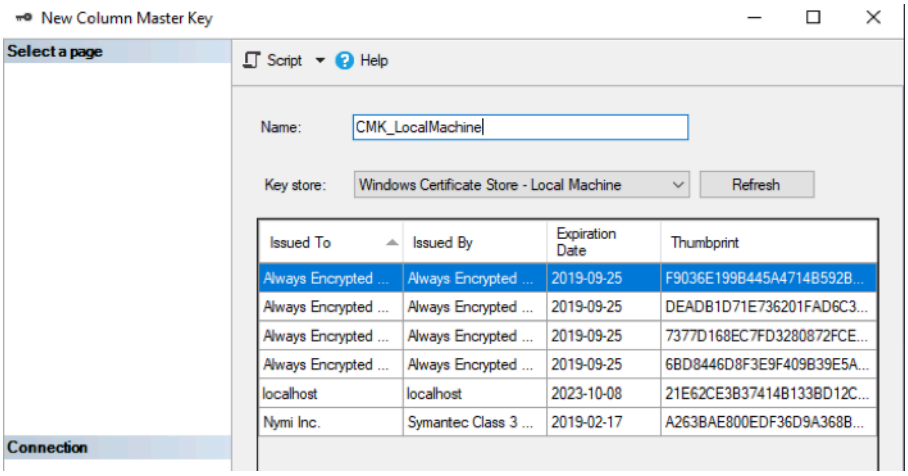
1. Edit the *C:\inetpub\wwwroot\NES\NEnrollment\web.config* file, and perform the following steps:
   a) Search for the string **`SqlConnectionString`**.

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

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

c) Save the file.

2. Download and install the SQL Server Management Studio (SSMS) software.
3. Open SSMS by using the **`Run as Administrator`** option.
4. Click **`Connect > Database Engine`**.
5. On the `Connect to Server` page, if you are using SQL authentication, type the server name and your credentials, and then click **`Connect`**, otherwise, click **`Connect`**.
6. Expand **`Databases > Nymi.NES > Security > Always Encrypted Keys`**. Right click **`Column Master Key`**, and then select **`New Column Master Key`**.
7. On the `New Column Master Key` window, perform the following actions:
   a) In the **`Name`** field, type a name for the key.
   For example, `CMK_LocalMachine`.
   b) In the **`Key store`** field, select **`Windows Certificate Store – Local Machine`**.
   The following figure shows the `New Column Master Key` page.

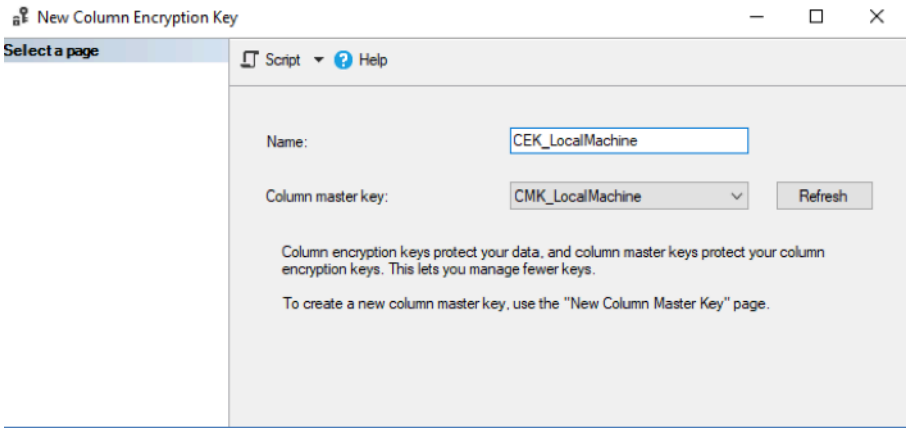


`Figure 24: New Column Master Key page`

   c) Click **`Generate Certificate`**.
   d) Click **`OK`**.
8. While in **`Nymi.NES > Security > Always Encrypted Keys`**, right-click **`Column Encryption Keys`**, and then select **`New Column Encryption Key`**.
9. On the `New Column Encryption Key` page, perform the following actions:
   a) In the **`Name`** field, type a name for the key.
   For example, `CEK_LocalMachine`.
   b) In the **`Column master key`** field, select the name of the column master key that you created.

For example, `CMK_LocalMachine`.

The following figure shows the `New Column Encryption Key` page.



`Figure 25: New Column Encryption Key page`

c) Click **OK**.

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

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

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

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

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

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

c) In the table, select **DER**, and then from the **Encryption Type** list, select **Randomized**.
The following figure shows the `Column Selection` page.

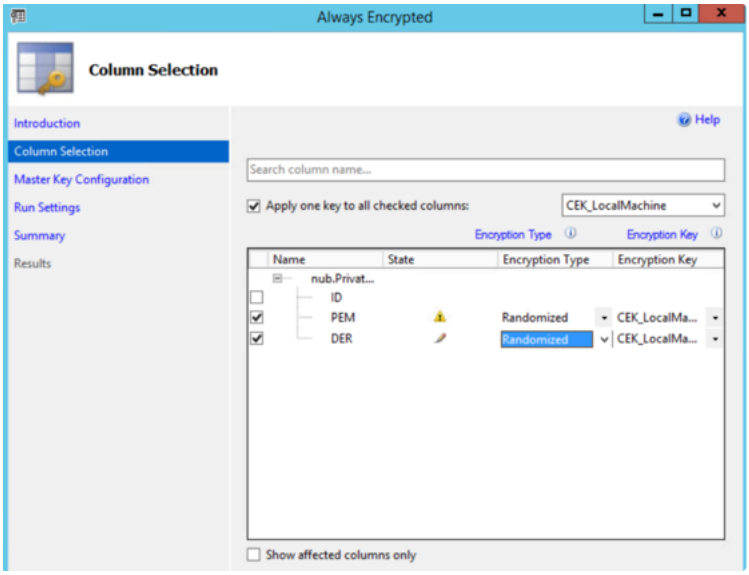


Figure 26: Column Selection page

d) Click **Next**.

14. On the Master Key Configuration page, click **Next**.
15. On the Run settings page, leave the default value **Proceed to finish now**, and then click **Next**.
16. On the Summary page, review the results, and then click **Finish**.
17. Close SSMS.

What to do next

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

1. Open Manage Computer Certificates.
2. Expand **Personal**, and then right-click **Always Encrypted Certificate** and then select **All Tasks > Manage Private Keys**. The Permissions for Always Encrypted Certificate window appears.
3. Click **Add**.
4. In the Select Users, Computers, Service Accounts, or Groups windows, type the Application Pool Identity account, and the select **Check Names**.
5. Click **OK**.
6. Click **OK**.

Encrypt usernames in the NES Database

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

Procedure

1. Encrypt the audit.UserCore table by performing the following steps:
   a) In Tables, right-click **audit.UserCore**, and then select **Encrypt Columns**.

b) On the Introduction page, click **Next**.
c) Enable **Apply one key to all checked columns** and ensure that **CEK_LocalMachine** appears in the list to the right.
d) In the **Tables**, select **username**, and then from the **Encryption Type** list, select **Deterministic**.
e) Click **Next**.
f) On the Master Key Configuration page, click **Next**.
g) On the Run settings page, leave the default setting **Proceed to finish now**, and then click **Next**.
h) On the Summary page, review the results, and then click **Finish**.

2. Encrypt the nub.UserCore table by performing the following steps:
a) In Tables, right-click **nub.UserCore**, and then select **Encrypt Columns**.
b) On the Introduction page, click **Next**.
c) Enable **Apply one key to all checked columns** and ensure that **CEK_LocalMachine** appears in the list to the right.
d) In the **Tables**, select **username**, and then from the **Encryption Type** list, select **Deterministic**.
e) Click **Next**.
f) On the Master Key Configuration page, click **Next**.
g) On the Run settings page, leave the default setting **Proceed to finish now**, and then click **Next**.
h) On the Summary page, review the results, and then click **Finish**.

Installing and Configuring CWP Components in Local Configuration

There are three types of user terminals in a CWP environment:

- User terminal for NEAs - where a user performs repetitive tasks that require authentication, possibly by using an NEAs, such as an MES applications. The user terminal can also be locked or unlocked using Nymi Lock Control.
- Enrollment terminal - where users enroll their Nymi Bands using the Nymi Band Application.
- User terminal for NESadministration - where NES Administrators can connect to the NES Administrator Console to manage NES.

The following sections describes the tasks that you need to perform to prepare each user terminal.

User terminal for Nymi Band Enrollment

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

1. Insert the Nymi-supplied Bluetooth adapter into an available USB port.
2. Import the Root CA certificate.

3. Install the Nymi Band Application. The Nymi Band user requires physical access to the network terminal.
4. Set the NES_URL registry key.

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

Nymi Band Application Installation

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

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

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

Performing a customizable Nymi Band Application installation

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

About this task

Procedure

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

Performing a silent Nymi Band Application Installation or Upgrade

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

About this task

Procedure

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

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

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

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

Setting the NES URL

After you install the `Nymi Band Application`, ensure that the enrollment process uses the correct NES URL.

About this task

Procedure

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

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

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

   where:

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

User terminal for NEAs

User terminals are machines that users use to perform daily tasks with the Nymi Band.

Importing the Root CA certificate

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

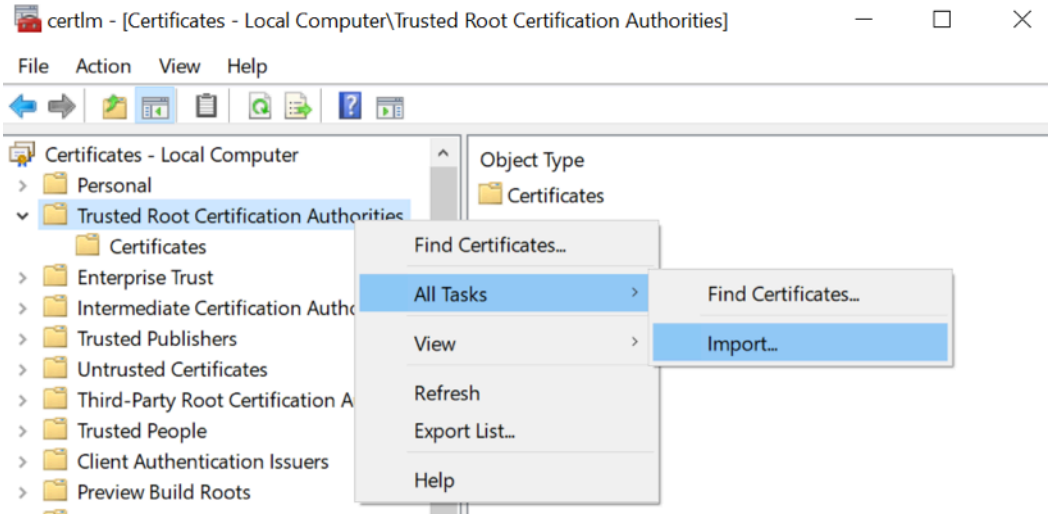
About this task

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

Procedure

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

   The following figure shows the `certlm` window.



   `Figure 27: certlm application on Windows 10`

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

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

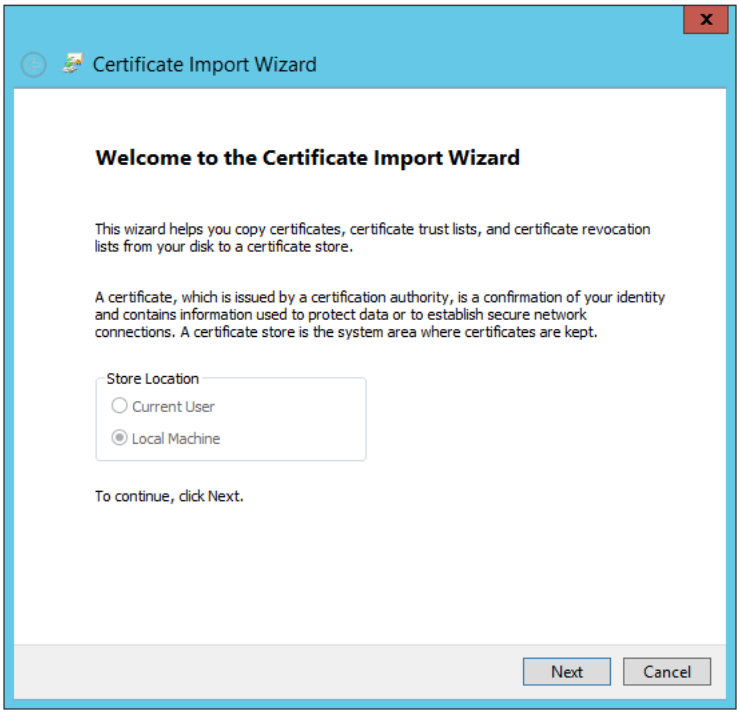


Figure 28: Welcome to the Certificate Import Wizard screen

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

   The following figure shows the File to Import screen.

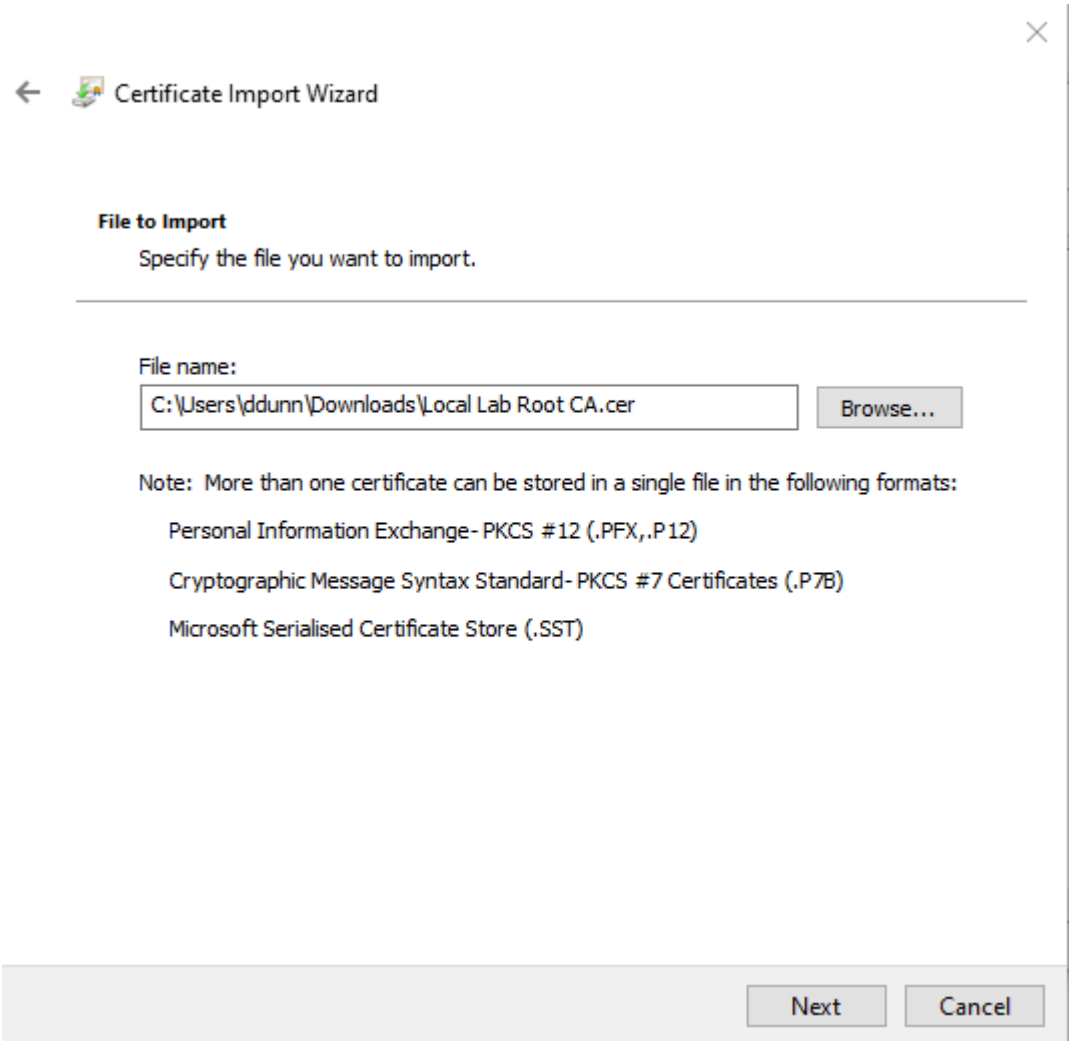


Figure 29: File to Import screen

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

Prepare User terminals for Nymi-enabled Applications

Before a user can use a Nymi-enabled Application, the NES Administrator must perform the following actions on the user terminal:

1. Insert the Nymi-supplied Bluetooth Adapter into an available USB port. The Bluetooth Adapter is used to detect Nymi Bands as they move in and out of Bluetooth signal range, and is primarily used for communication with the band during enrollment, Windows unlock, MES signing, as well as monitoring signal strength for presence.
2. Attach a Nymi-verified NFC reader into an available USB port.
3. Install the NEA.

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*).

Install and Configure Nymi Lock Control

Perform the steps in the following section to install `Nymi Lock Control` on user terminals in the environment and configure NES to enable `Nymi Lock Control` support.

Configuring and Installing Nymi Lock Control on User Terminals

On each user terminal that will use `Nymi Lock Control` to lock and unlock the terminals, you must create a registry key that defines the path to NES and install the `Nymi Lock Control` application.

Configuring User Terminals for Nymi Lock Control

Create a GPO to push the NES URL registry key to each user terminal, or perform the following steps to manually create the registry key on the user terminal.

About this task

Run *regedit* as an administrator.

Procedure

1. Navigate to *HKEY_LOCAL_MACHINE\Software\Nymi\NES*.

   Note: If this path does not exist, create the keys.
2. In the *NES* key, create a new string value.
3. In the **`Name`** field, type `URL`.
4. Edit the string and in the value field, type `https://nes_server/nes_service_name`

   Where:

   - *`nes_server`* is the Fully Qualified Domain name of the NES host.
   - *`nes_service_name`* is the services mapping name of the NES web application. The default value is nes.

     For example, https://ev3-uat-srv1/ev3-uat-lab.local/nes

     Note: The service mapping name for NES was defined during deployment.

- Close *regedit.exe*.

Installing Nymi Lock Control

Perform the following steps on each user terminal in the environment.

About this task

Procedure

1. Copy the *NymiLockControl-installer-vw.x.y.z* to a directory on the user terminal.
2. Right-click *NymiLockControl-installer-vw.x.y.z* and select **`Run as administrator`**.
3. On the `User Account Control` window, click **`Yes`**.
4. On the `Welcome to Nymi Lock Control Setup Wizard` window, click **`Next`**.
5. On the `Select Installation Folder` window, perform the following actions: optionally, click **`Browse`** and select a different installation folder, and then click **`Next`**
   a) Optionally, click **`Browse`**, navigate to a new installation folder, and then click **`Select Folder`**
   b) Click **`Next`**.
6. On the `Ready to Install` window, click **`Install`**.
7. On the `Completing the Nymi Lock Control Setup Wizard` window, click **`Finish`**.

Edit the Nymi Bluetooth Endpoint Configuration File

The `Nymi Bluetooth Endpoint` application enables BLE functionality for Nymi Lock Control and BLE tap. Editing the `Nymi Bluetooth Endpoint` configuration file adjusts the behavior of these features.

Note: Nymi Lock Control functions with a BLE radio antenna or NFC reader. The settings described in this section refer to Nymi Lock Control with a BLE adapter only, and not an NFC reader.

Nymi Lock Control and BLE tap behavior is dependent on the distance between the Nymi Band and the BLE radio antenna. The distance between the radio antenna and the Nymi Band is represented by changes in the Received Signal Strength Indication (RSSI) value, and is determined by measuring the radio signals received by the BLE radio antenna. Close distances between the Nymi Band and BLE radio antenna result in stronger signals, and far distances result in weak signals. BLE tap and Nymi Lock Control actions occur when the trends in changing RSSI values reach a certain threshold defined in the `Nymi Bluetooth Endpoint` configuration settings.

The default RSSI values used by `Nymi Bluetooth Endpoint` may not be optimal for certain users. For example, under default settings the user terminal may unlock when the user is too far away, or the user terminal may accidentally lock while the user is present. In these cases, the BLE radio antenna is too sensitive, not sensitive enough, or the placement of the BLE adapter prevents the Nymi Band from being read consistently. Edit the `Nymi Bluetooth Endpoint` configuration settings on a user terminal to adjust for these discrepancies.

To adjust the sensitivity of BLE taps and `Nymi Lock Control`, edit the Received Signal Strength Indication (RSSI) values in the `Nymi Bluetooth Endpoint` configuration file, *nbe.toml*.

Note: The *nbe.toml* file described in this section is only used to apply adjustments to Nymi Lock Control and BLE tap behavior with a BLE radio antenna (ex. USB adapter). If the *nbe.toml* file is renamed or deleted, Nymi Lock Control and BLE taps behave under the default settings described in Editing the nbe.toml File on page 62.

Editing the nbe.toml File

About this task

A backup configuration file is installed on the user terminal when the `Nymi Bluetooth Endpoint` is installed or updated. This file, *nbe.default.toml*, contains the default values that control BLE tap behavior with the Nymi Band and BLE adapter. Use the values in the *nbe.default.toml* file as a template for the *nbe.toml* file. These files are located in *C:\Nymi\Bluetooth_Endpoint* on Windows, and */usr/bin/nbe.toml* on HP Thin Pro.

Note: `Nymi Bluetooth Endpoint` will only recognize RSSI values in the *nbe.toml* file. Retain a backup of a useful configuration by copying the *nbe.toml* file and renaming it.

Table 7: Default configuration settings for `Nymi Lock Control` and BLE tap intent

***nbe.toml* Entry**	**Default Value**	**Description**
agent_url	"ws://127.0.0.1:9120/socket/websocket" (do not change)	Identifies the location of the agent URL. The default value shown in this table is generated if the agent is installed locally. If the agent URL is installed centrally (via remote installation), the hostname of the URL will be different. **The agent_url must be present when using an *nbe.toml* file.**
rssi_window_tap	10	This determines the duration the Nymi Band must be within tap-distance of the BLE radio antenna to complete a tap. A larger value increases the duration required to perform and decrease the sensitivity.
rssi_window_long	50	This determines the frequency that `Nymi Bluetooth Endpoint` checks the distance between the BLE radio antenna and the Nymi Band. `Nymi Bluetooth Endpoint` tracks trends in these changes to trigger a Nymi Lock Control action, such as **`keep unlocked when present`**, **`lock when away`**, or **`unlock when present`**.

nbe.toml Entry	Default Value	Description
rssi_tap_threshold	0 (must be 0 or negative)	This determines the range at which a tap event will occur. A smaller negative value means a closer distance to the BLE antenna. BLE tap is disabled by default (value = 0). **Enter a non-zero, negative number to enable BLE tap**. Nymi recommends an RSSI value of -42. If the Nymi Band maintains a minimum distance specified by *rssi_tap_threshold*, for a duration *rssi_window_tap*, a BLE tap is performed.
rssi_cutoff_close	-70 (must be 0 or negative)	This determines the outer range of the close distance-threshold (excluding tap distance) for Nymi Lock Control. Enter 0 to bypass the proximity functionality of Nymi Lock Control. If the Nymi Band maintains a close distance to the BLE radio antenna and the RSSI values measured are within the *rssi_cutoff_close* value, Nymi Lock Control keeps the user terminal unlocked. If the Nymi Band moves away from the BLE radio antenna, and the RSSI values measured are on a decreasing trend and goes from the *rssi_cutoff_close* value to the *rssi_cutoff_far* value, Nymi Lock Control locks the user terminal.
rssi_cutoff_far	-75 (must be negative)	This determines the outer range of the far distance-threshold (excluding tap distance) for Nymi Lock Control. If the Nymi Band moves towards the BLE radio antenna, and the RSSI values measured are on an increasing trend and goes from the *rssi_cutoff_far* value to the *rssi_cutoff_close* value, Nymi Lock Control unlocks the user terminal.

Procedure

1. Make a copy of the *C:\Nymi\Bluetooth_Endpoint\nbe.default.toml* file (On HP Thin Pro, */usr/bin/nbe.default.toml*), and name the file *nbe.toml*.
2. Edit the *nbe.toml* file with a text editor.
3. Edit the RSSI values in the file. Refer to the descriptions in the table above.
4. Save the *nbe.toml* file.
5. Restart the `Nymi Bluetooth Endpoint`.

   On Windows:

   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.

On HP Thin Pro:

a. Stop the Nymi Bluetooth Endpoint service by typing killall -9 nbed.
b. Start the Nymi Bluetooth Endpoint by typing /usr/bin/nbedstart.

Results

Once restarted, the Nymi Bluetooth Endpoint application will be updated with the edits made in the *nbe.toml* file. Updated BLE tap intent and Nymi Lock Control settings will be implemented on the user terminal. If the *nbe.toml* file is not present, Nymi Bluetooth Endpoint behaves under default settings.

Configuring NES to support Nymi Lock Control

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

About this task

Results

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

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

Setting the NES URL

After you install the Nymi Band Application, ensure that the enrollment process uses the correct NES URL.

About this task

Procedure

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

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

   .
5. Right-click **NES**, and then select **New > String value**.
6. In the **Value** field, type URL.

7. Double-click **URL** and in the **Value Data** field, type `https://nes_server/NES_service_name/` or `http://nes_server/NES_service_name` depending on the NES configuration

   where:

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

8. Click **OK**.

Configuring Nymi Lock Control for Virtual Desktops

To unlock virtual desktops with Nymi Lock Control, configure Client IP Caching on the user terminal.

About this task

Perform the following steps to support desktop unlock with the Nymi Band in a virtual desktop environment.

Procedure

1. Run **regedit.exe**
2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Nymi*.
3. Right-click Nymi Lock Control, and then select **New > DWORD (32-bit)**.
4. In the **Value** field, type `CacheClientIp`.
5. Double-click **ClientCacheIp** and in the **Value Data** field, type `00000001`.
6. Click **OK**.

What to do next

Note: This functionality is not supported in a shared remote desktop environment such as Citrix Virtual Applications. In such an environment, this setting causes unpredictable behavior when more than one user is connected to an NEA at the same time.

Install Nymi Runtime

`Nymi Runtime` facilitates communication between NES and the Nymi Bands.

Install the `Nymi Runtime` on each user terminal on which you will also install a Nymi-enabled Application. You can perform a customizable installation or a silent installation.

Note: Nymi Lock Control and the Nymi Band Application automatically install Nymi Runtime, machines with Nymi Lock Control or Nymi Band Application, it is not necessary for you to install the Nymi Runtime application.

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.

About this task

Procedure

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

Performing a silent installation or upgrade of Nymi Runtime

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

About this task

Procedure

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

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

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

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

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

What to do next

The silent installation process creates an installation log file in the *%temp%* directory named Nymi Runtime_*version_time*.*log*

Edge Agent Certificate Requirements

Kafka requires a TLS certificate that is issued by a trusted public CA or trusted enterprise CA. If this is not possible, for example in a POC or Pilot environment), then you can use a TLS certificate that is issued by an untrusted root CA. Additional steps are required and described in the following sections.

Note: Self-signed certificates with Kafka are not supported.

Installing the Nymi Edge Agent Application in a Local Configuration

Install Nymi Edge Agent on the user terminals in your environment that are on the same domain as NES.

Before you begin

- Install the latest version of OpenSSL for Windows and add the *bin* directory is included in the system path.
- The Nymi Edge Agent package has been extracted to a central location.

About this task

Perform the following steps on each user terminal:

Procedure

1. Copy the extracted *edgeagents* folder to the user terminal.

   The folder contains the following files:

   - *decrypt.key* file, which is used to decrypt the SASL and NES usernames and passwords.
   - *edgeagents-service-x64-*`version`*.msi* file, which installs the `Nymi Edge Agent` software on a thick client user terminal and uses the parameters detailed in the *edge_agents.conf* file.
   - *edgeagents-terminal-service-x64-*`version`*.msi* file, which installs the `Nymi Edge Agent` software on a RDP sessions host/Citrix server and uses the parameters detailed in the *edge_agents.conf* file.
   - *secretutil.cmd* file, which is Windows command utility that encrypts secrets.
   - *edge_agents.conf* file, which used to configure the parameters of the `Nymi Edge Agent` installation, and includes keys generated from the PowerShell utility.
   - *KafkaCA.pem* file, which is a default client truststore certificate.

2. Perform the following steps to generate the secret keys by using the *secretutil.cmd* file.

   a) Click the **`Start`** menu and type `cmd`. Right-click **`Command Prompt`** and click **`Run as administrator`**.

b) Change the directory that contains the extracted `Nymi Edge Agent` installation package. For example, the *C:\edgeagents* folder.

c) Initialize *secretutil.cmd* with the following command:

```
secretutil.cmd -init
```

d) Use the *secretutil.cmd* command to encrypt the sasl username and password.

1. By default, the username is ctca. Type the following command to encrypt the username in an output file.

   ```
   secretutil.cmd -enc ctca>OUTPUT FILE NAME.txt
   ```

   where *`OUTPUT FILE NAME.txt`* is the name of the file that contains the encrypted username.

2. Type the following command to encrypt the SASL password.

   ```
   secretutil.cmd -enc PASSWORD>OUTPUT FILE NAME 2.txt
   ```

   where *`PASSWORD`* is the password specified by the person who implemented the server side components when they ran the *init-crypto* command and *`OUTPUT FILE NAME 2.txt`* is the name of the file that contains the encrypted password.

The output files contain the secret keys used in the *edge_agents.conf* file.

3. Perform the following steps to update the *edge_agents.conf* file with the secret keys that you created in the previous step.

   a) Open the *edge_agents.conf* file with a text editor.

   b) Update the value for the key `sasl.username`. It is the encrypted value in the username output text file.

   ```
   sasl.username=[encrypted username]
   ```

   c) Update the value for the key `sasl.password`. It is encrypted value in the password output text file.

   ```
   sasl.password=[encrypted password]
   ```

4. Save the *edge_agents.conf* file.

5. For Kafka TLS certificates that are issued from an untrusted CA only, perform the following steps to install the Kafka Truststore.

   a) Obtain the Kafka Broker root CA certificate from the person who implemented the CWP cluster. The file is stored in the CWP deployment package, in the *cwp/certs* folder.

   b) If required, rename the Kafka Broker root CA cert to *KafkaCA.pem*.

   c) Backup the *KafkaCA.pem* certificate in the `Nymi Edge Agent` installation directory.

   d) Replace the default *KafkaCA.pem* file in the `Nymi Edge Agent` installation package directory with the new *KafkaCA.pem* certificate file that you obtained from the implementation engineer.

6. Open the *edge_agents.conf*, and ensure that the value defined in the *`sasl.ca.path`* key is *C:\Nymi\Edge_Agents\certs\KafkaCA.pem*.

7. Edit the following configuration parameters in the *edge_agents.conf* file.

   Producer Specific Properties:

- *bootstrap.servers*, which defines a list of host and port pairs of Kafka brokers.

NES Specific Properties:

- *nes.url*, which specifies the NES URL.
- *agent.url*, which specifies the `Nymi Agent` URL. When you do not specify a value, `Nymi Edge Agent` will pick up the local `Nymi Agent` URL.

8. Save the *edge_agents.conf* file.

   Note: Ensure the *edge_agents.conf* file is configured prior to installing *edge_agents.msi*. This configuration file can then be copied to different machines being installed with `Nymi Edge Agent`.

9. Run the installer file *edgeagents-service-x64-version.msi*.
   The Nymi Edge Agent application is installed without any user interactions in the *C:\Nymi \Edge_Agents* folder and the .Nymi Nymi Edge Agent service appears with a Running status in Windows Services.

   Note: The section *Edge Agent Log Files* provides information about `Nymi Edge Agent` log files.

User terminal for NES administration

NES Administrators can use any user terminal with a web browser to access the NES Administrator Console.

An NES Administrator is not required to perform any configuration tasks on the user terminal before accessing the NES Administrator Console.

Installing and Configuring CWP in Citrix and RDP Environments

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

There are three types of user terminals in a CWP environment:

- Centralized Nymi Agent host - Machine that hosts the `Nymi Agent` service and provides an inter
- Citrix/RDP client - Machine that a user logs into and then perform repetitive authentication tasks in applications, such as MES applications that are hosted on a remote session.
- Thin client - Machine that a user uses to connect to server-based environments, such as virtual desktops. These servers host desktops and MES applications that are displayed over the network to the thin client machine.
- Remote session host - Citrix or RDP session host on which you install MES applications. Local clients connect to the remote session host to perform authentication tasks.
- Enrollment terminal - Machine on which the user enrolls their Nymi Band by using the Nymi Band Application.
- User terminal for NES administration - Machine on which NES Administrators can connect to the NES Administrator Console to manage NES.

The following sections describes the tasks that you need to perform to prepare each machine.

User terminal for Nymi Band Enrollment

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

1. Insert the Nymi-supplied Bluetooth adapter into an available USB port.
2. Import the Root CA certificate.
3. Install the Nymi Band Application. The Nymi Band user requires physical access to the network terminal.
4. Set the NES_URL registry key.

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

Nymi Band Application Installation

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

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

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

Performing a customizable Nymi Band Application installation

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

About this task

Procedure

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

Performing a silent Nymi Band Application Installation or Upgrade

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

About this task

Procedure

1. Save the Nymi Band Application package, provided to you by your Nymi Solution Consultant.
2. Launch the command prompt as administrator.

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

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

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

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

Setting the NES URL

After you install the `Nymi Band Application`, ensure that the enrollment process uses the correct NES URL.

About this task

Procedure

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

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

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

   where:

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

Importing the Root CA Certificate in Citrix/RDP Environments

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

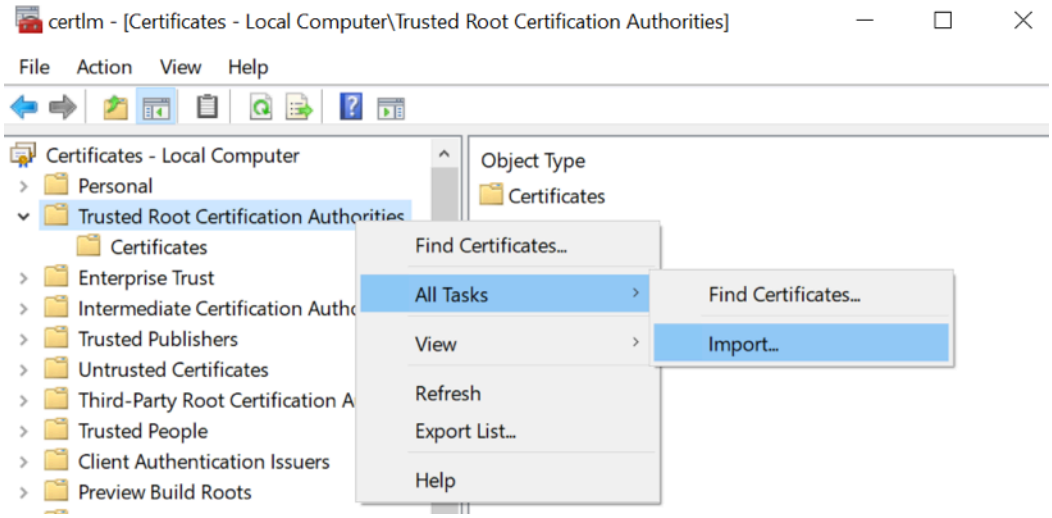
About this task

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

Procedure

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

   The following figure shows the `certlm` window.



`Figure 30: certlm application on Windows 10`

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

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

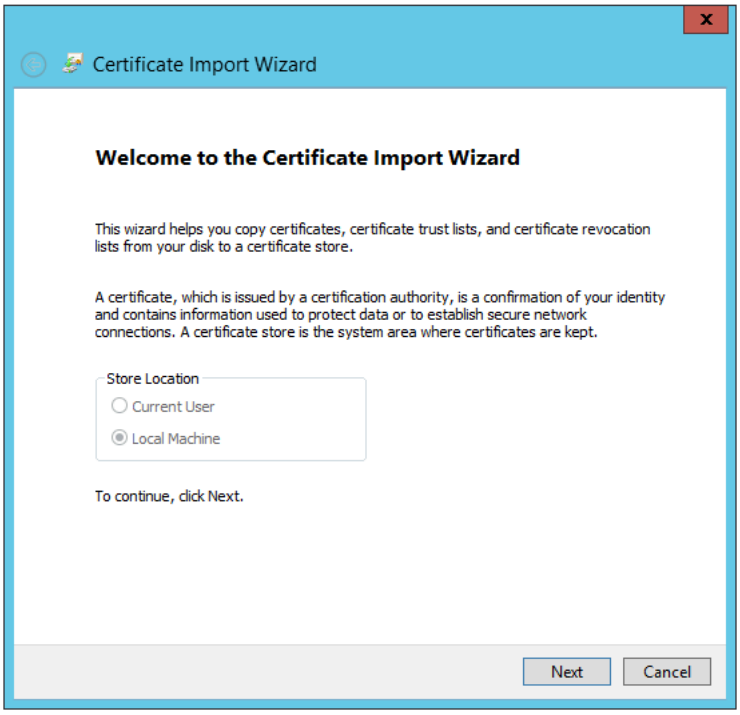


Figure 31: Welcome to the Certificate Import Wizard screen

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

   The following figure shows the File to Import screen.

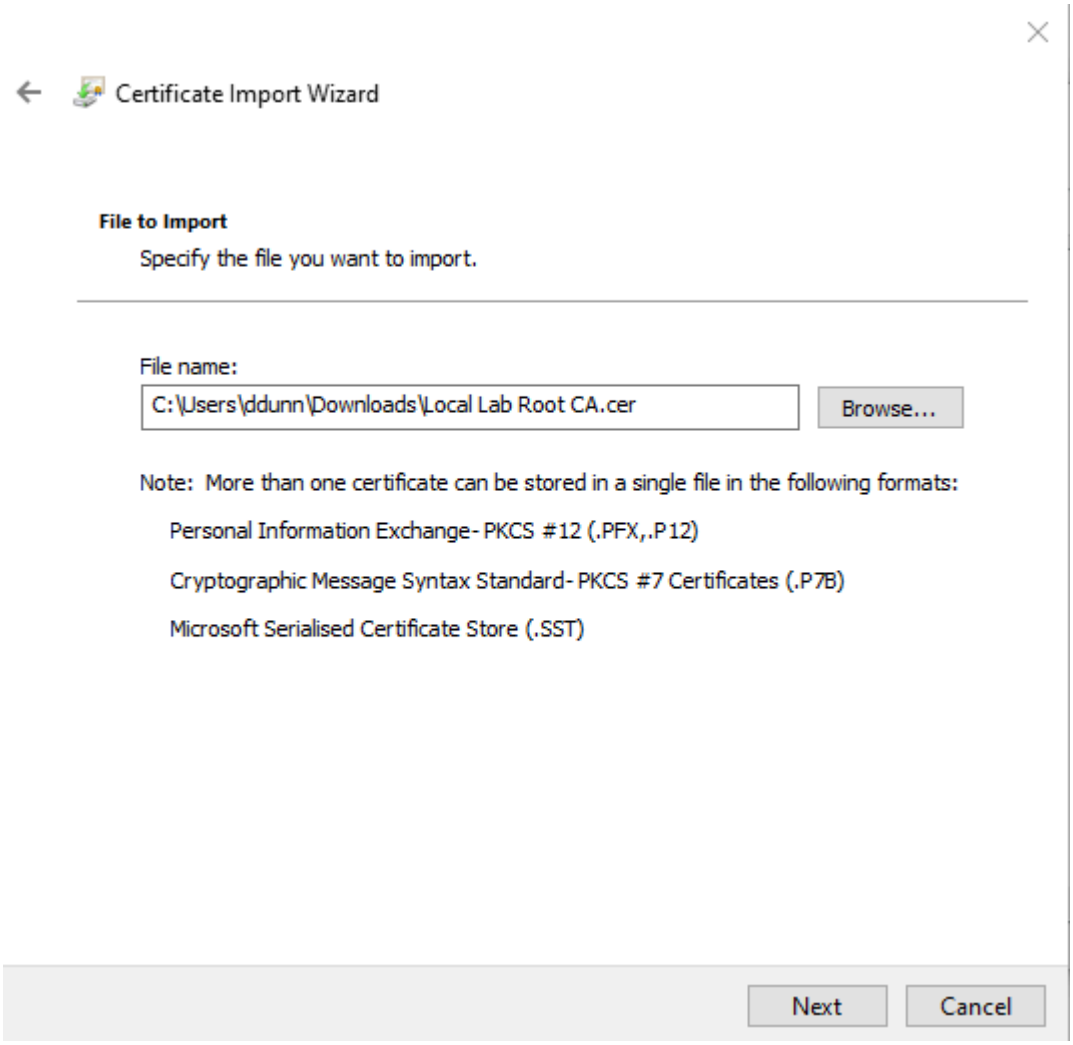


Figure 32: File to Import screen

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

Centralized Nymi Agent

For example, install the Nymi Agent application on the same machine as NES.

Installing the Nymi Agent

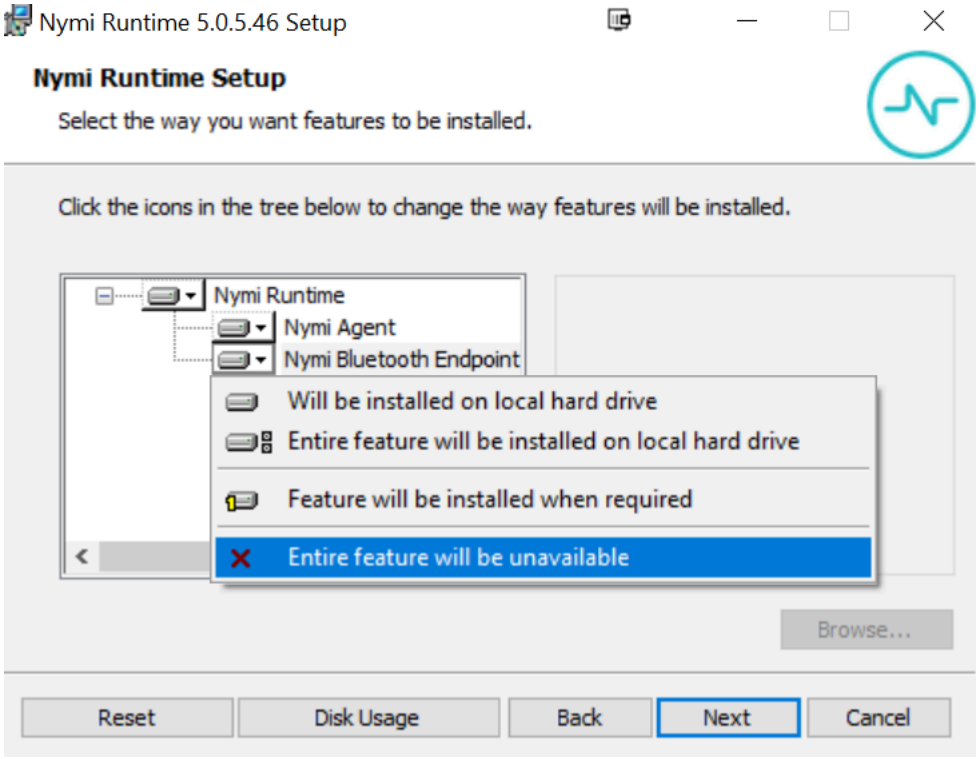
Install the Nymi Agent application, which is included in the Nymi Runtime installation package, on a machine in the environment.

About this task

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

Procedure

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



`Figure 33: Nymi Bluetooth Endpoint feature will be unavailable`

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

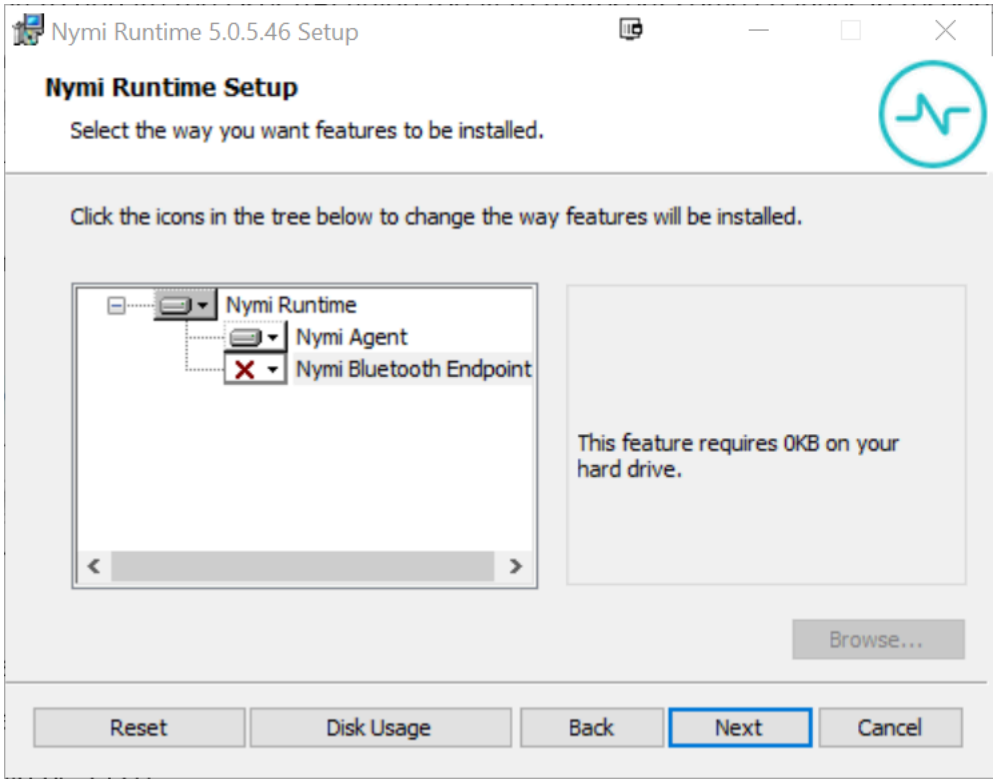


Figure 34: Nymi Bluetooth Endpoint feature is not available

10. On the Service Account window, click **Next**.
11. On the Ready to install page, click **Install**.
12. Click **Finish**.
13. On the Installation Completed Successfully page, click **Close**.

Results

Note: The Nymi Agent must be able to receive incoming WebSocket connections on TCP port 9120 (used for communication with NBE). If the Nymi WebAPI is in use, it must also be able to receive incoming WebSocket connections on the TCP port configured for Nymi WebAPI 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.

Citrix/RDP and Thin Clients

This section describes how to prepare Citrix/RDP and thin clients.

Prepare User terminals for Nymi-enabled Applications

Before a user can use a Nymi-enabled Application, the NES Administrator must perform the following actions on the user terminal:

1. Insert the Nymi-supplied Bluetooth Adapter into an available USB port. The Bluetooth Adapter is used to detect Nymi Bands as they move in and out of Bluetooth signal range, and is primarily used for communication with the band during enrollment, Windows unlock, MES signing, as well as monitoring signal strength for presence.
2. Attach a Nymi-verified NFC reader into an available USB port.
3. Install the NEA.

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*).

Installing the Nymi Bluetooth Endpoint on Citrix/RDP Clients

About this task

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.

Procedure

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

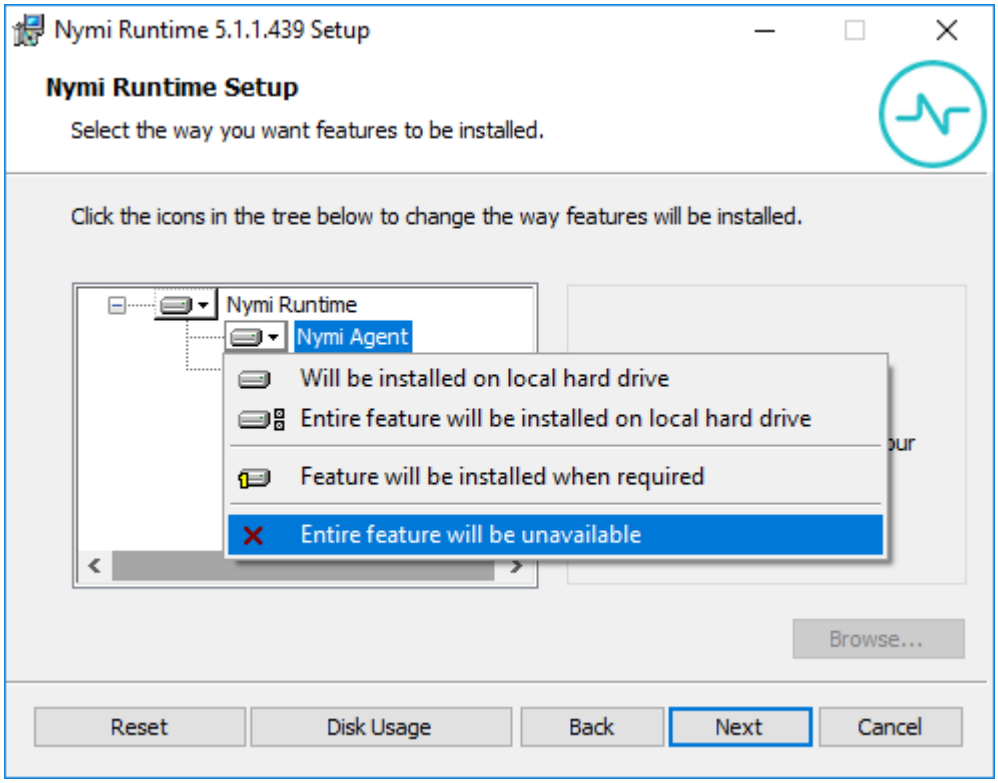


Figure 35: Nymi Agent feature will be unavailable

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

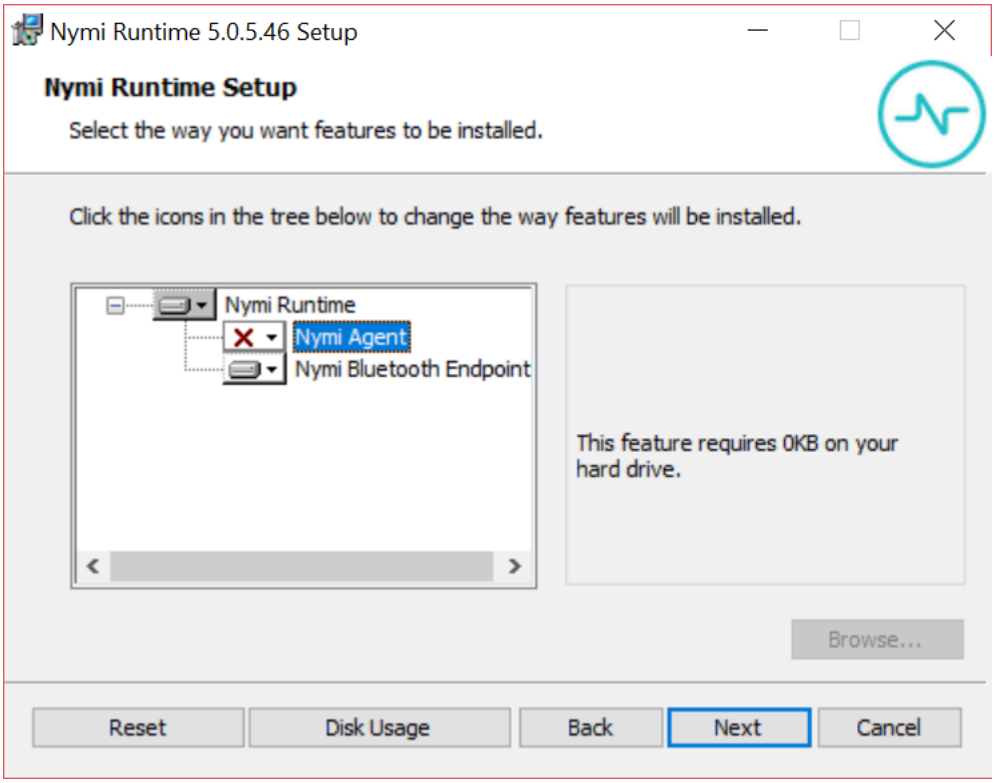


Figure 36: Nymi Agent feature is not available

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_x.y.z_amd64.deb* from Nymi.

About this task

Retrieve the installation file *nbed_x.y.z_amd64.deb* from Nymi.

Procedure

1. Switch your user mode to **Administrator** from the system menu, or log in by entering an the credentials of a person in the domain admin group.
   a) Right-click the desktop or click **Start**.
   b) Click **Switch to Administrator** from the menu. You will be prompted to enter the administrator password.

   The screen is surrounded by a red border when in administrator mode.
2. Extract the file, *nbed_x.x.z_amd64.deb*, from the Nymi distribution package and save it to the machine. Where *x.y.z* is the version of the file. Note the file path.
3. Unlock read/write access with **X Terminal**.
   a) Click **Start** and go to **Tools**.
   b) Click **X Terminal**.
   c) Type `fsunlock`
4. In **X Terminal** change the directory to the file location of *nbed-cron_x.y.z_amd64.deb* and install the extracted file.

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

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

Installing Nymi Bluetooth Endpoint on IGEL

Use the UMS server to host the `Nymi Bluetooth Endpoint` package and perform the installation of the application on IGEL thin clients.

Uploading Nymi Packages to Universal Management Suite

Follow the instructions below to upload the `Nymi Bluetooth Endpoint` package to the Universal Management Suite (UMS) server.

About this task

Obtain the installation package from Nymi.

Procedure

1. Extract the installation package to a machine that has access to the UMS Console.
2. Connect to the UMS Console.
3. In UMS Console, right-click the **Files** folder in the left navigation pane, and then select **New File**.

   The `New file` window appears.
4. In the **File Source** section, select the appropriate source option, for example, **Upload Local File to UMS Server**, and then navigate to the folder location that contains the *nymi.tar.bz2* file, select the file, and then click **Open**.
5. Click **OK**.

6. Right-click the **Files** folder in the left navigation pane, and then select **New File**.
   The New file window appears.
7. In the **File Source** section, select the appropriate source option, for example, **Upload Local File to UMS Server** , and then navigate to the folder location that contains the *nymi.inf* file, select the file, and then click **Open**.
8. Click **OK**.

Results

The following figure provides a example of the Files folder with the files. Make note of the value in **Download URL** field for each file, as you will require is information in the *Customizing the Custom Partition* section.

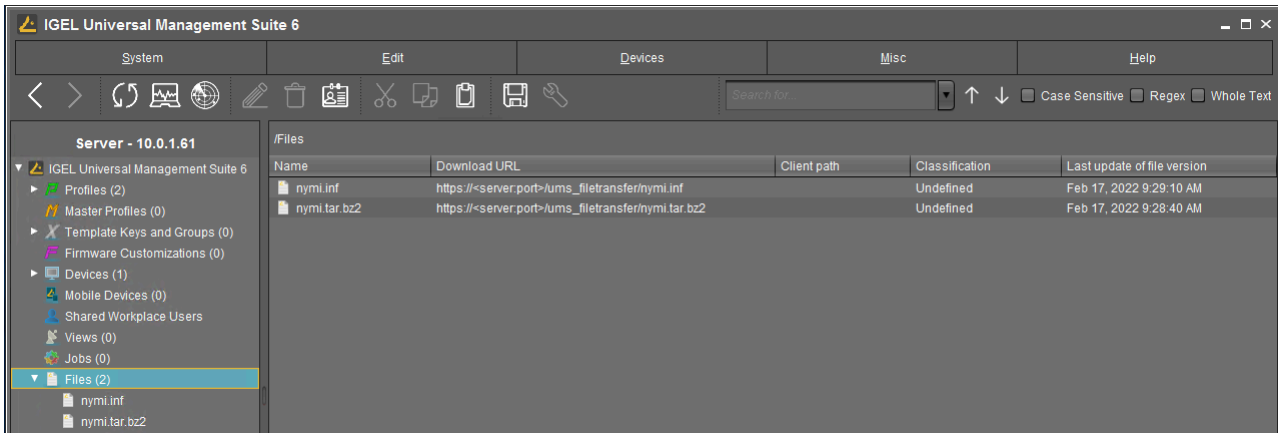


Figure 37: Files window

Creating a Profile and Custom Partition

Perform the following instructions to create a profile and partition on the UMS server for the Nymi Bluetooth Endpoint software installation.

Procedure

1. Connect to the UMS Console, right-click the *Profiles* folder, and then from the context menu, select *New Profile*.
   The New Profile window appears.
2. In the **Profile Name** field, type Nymi.
3. In the **Description** field, type Install the Nymi Custom Partition.
   The following figure provides an example of the New Profile window.

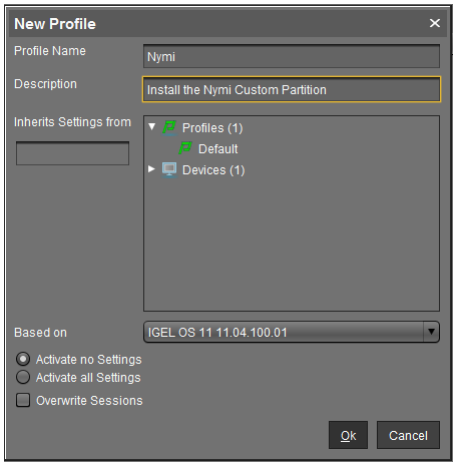


Figure 38: New Profile window

4. Click **OK**.
   The Setup window opens.
5. Navigate to **System > Firmware Customization > Custom Partition > Partition**.
6. Unlock the **Enable Partition** setting by clicking the orange triangle so that it turns blue, and then select **Enable Partition**.
7. Unlock the **Size** setting by clicking the orange triangle so that it turns blue. For the size value, type 12M.
8. Leave the mount point value as **/custom**.
9. In the **Partitions Parameters** list, click **[+]** (Add).
   A dialog box appears.
10. In the Add box, perform the following actions.
    a) In the **Name** field, type AGENT_URL.
    b) In the **Value** field, type ws://*agent_host*:9120/socket/websocket
       where *agent_host* is the IP address of the server on which you installed the Nymi Agent.
    c) Click **OK**.
       The following figure provides an example of Nymi partition window.

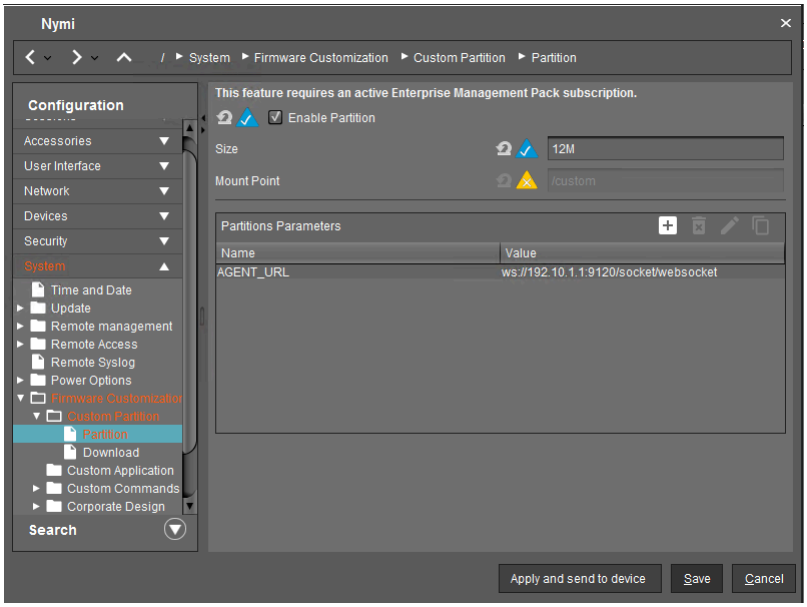


Figure 39: Partition window

d) Click **Save**.

Customizing the Custom Partition

After you create the Nymi partition, perform the following actions in the UMS Console to customize the `Nymi Bluetooth Endpoint` installation.

About this task

Procedure

1. From the `Configuration` navigation pane for the partition, navigate to **`Firmware Customization > Custom Commands > Base`**.

   A dialog box appears.

2. Perform the following actions in `Nymi Base Commands` dialog box.

   a) Unlock the **`Initialization`** setting by clicking the orange triangle so that it turns blue.

   b) In the **`Initialization`** field, type `modprobe cdc-acm`

   c) Unlock the **`Final Initialization Command`** setting by clicking the orange triangle so that it turns blue.

   d) In the **`Final Initialization Command`** field, type `/custom/nymi/custompart-nymi init`

   e) Click **Save**.

   The following figure provides an example of the `Nymi Base Commands` window.

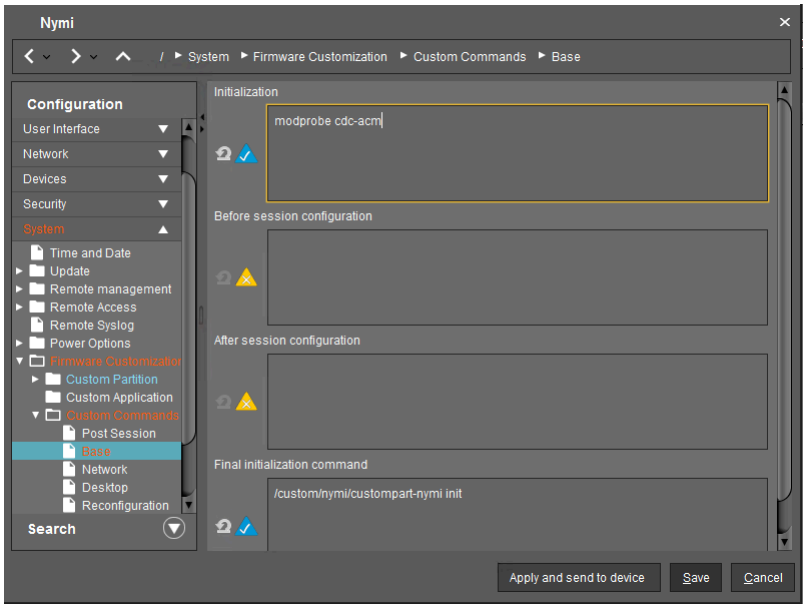


Figure 40: Nymi Base Commands

3. From the Configuration navigation pane, under the `Firmware Customization` folder, select **`Download`**.
4. In the **`Partitions Data Sources`** section, click **`[+]`** (Add).
   A dialog box appears.
5. Perform the following actions in the `Add` window.
   a) In the **`URL`** field, type the Download URL path for the *nymi.inf* file.
   For example, `https://10.0.1.61:8443/ums_filetransfer/nymi.inf`
   b) In the **`Username`** field, type the username of a user that has access to the UMS file transfer location.
   c) In the **`Password`** field, type the password for the user account that has access to the UMS file transfer location.
   d) In the **`Final Action`** field, type `/custom/nymi/custompart-nymi init`.
   e) Click **`OK`**.
6. Click **`Save`**.

Assigning the Profile to iGel Devices

Assign the Nymi profile to the IGEL devices.

About this task

Perform the following steps in the UMS Console.

Procedure

1. In the left navigation pane, select **`Profiles > Nymi`**.
2. In the **`Assigned Objects`** pane, click **`[+]`** Add.
   The `Select Assignable Objects` window appears.

3. In the left pane, expand **Devices**, select the IGEL clients, and then click the **>** button.
4. Click **OK**.
5. On the Update time? window, select **Now**, and then click **OK**.
   The Nymi Bluetooth Endpoint package installs on the selected IGEL client.
6. After the installation completes on the IGEL client, reboot the IGEL client.

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

About this task

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

Procedure

1. Make a copy of the *C:\Nymi\Bluetooth_Endpoint\nbe.default.toml* file (On HP Thin Pro, */usr/bin/nbe.default.toml*), 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.

   On Windows:

   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.

   On HP Thin Pro:

   a. Stop the Nymi Bluetooth Endpoint service by typing killall -9 nbed.
   b. Start the Nymi Bluetooth Endpoint by typing /usr/bin/nbedstart.
6. On HP Thin Pro only, revert the file system to read-only access.
   a) Open **X Terminal**.
   b) Type:

   ```
   fslock
   ```

   c) Close the terminal.
7. On HP Thin Pro only, Revert to **User** mode from the system menu, or log in using the credentials of a person in the user domain group.

Installing and Configuring Nymi Bluetooth Endpoint 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.

About this task

Perform the following steps on the domain controller.

Procedure

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 Nymi Lock Control

Perform the following steps on the RDP sessions host/ Citrix server.

About this task

Procedure

1. Copy the *NymiLockControl-installer-vw.x.y.z* to a directory on the user terminal.
2. Right-click *NymiLockControl-installer-vw.x.y.z* and select **`Run as administrator`**.
3. On the `User Account Control` window, click **`Yes`**.
4. On the `Welcome to Nymi Lock Control Setup Wizard` window, click **`Next`**.
5. On the `Select Installation Folder` window, perform the following actions: optionally, click **`Browse`** and select a different installation folder, and then click **`Next`**
   a) Optionally, click **`Browse`**, navigate to a new installation folder, and then click **`Select Folder`**
   b) Click **`Next`**.
6. On the `Ready to Install` window, click **`Install`**.
7. On the `Completing the Nymi Lock Control Setup Wizard` window, click **`Finish`**.

Configuring NES to support Nymi Lock Control

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

About this task

Results

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

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

Setting the NES URL

After you install the Nymi applications, create a registry key to define the NES URL on the RDP session host/ Citrix server.

About this task

Procedure

1. Run *regedit.exe*
2. On the `User Account Control` window, click **`Yes`**.
3. Navigate to **`HKEY_LOCAL_MACHINE > Software > Nymi`**.
4. Right-click **`NES`**, and then select **`New > String value`**.
5. In the **`Value`** field, type `URL`.
6. Double-click **`URL`** and in the **`Value Data`** field, type `https://nes_server/NES_service_name/` or `http://nes_server/NES_service_name` depending on the NES configuration

   where:

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

Disabling Network Level Authentication

To use `Nymi Lock Control` to lock and unlock a RDP session host or Citrix server, disable Network Level Authentication (NLA)

About this task

Perform the following steps on each RDP/Citrix client.

Procedure

1. Run *regedit.exe*

2. From the **`File`** menu, select **`Connect Network Registry`**
3. Type the name of the RDP session host or Citrix server, and then click **`OK`**.
4. Navigaate to *HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp*
5. Edit the **`SecurityLayer`** key and change the value to `0`.
6. Click **`OK`**.
7. Close *regedit.exe*.

Edge Agent Certificate Requirements

Kafka requires a TLS certificate that is issued by a trusted public CA or trusted enterprise CA. If this is not possible, for example in a POC or Pilot environment), then you can use a TLS certificate that is issued by an untrusted root CA. Additional steps are required and described in the following sections.

Note: Self-signed certificates with Kafka are not supported.

Installing the Nymi Edge Agent Application on the RDP session host / Citrix server

Install `Nymi Edge Agent` on the RDP session host / Citrix server in your environment that is on the same domain as NES.

Before you begin

- Install the latest version of OpenSSL for Windows and add the *bin* directory is included in the system path.
- The `Nymi Edge Agent` package has been extracted to a central location.
- If an untrusted root CA issues the NES certificate, you must import the root CA certificate for the untrusted root. *Importing the Root CA certificate* provides more information.

About this task

Perform the following steps on the RDP session host / Citrix server:

Procedure

1. Copy the extracted *edgeagents* folder to the RDP session host / Citrix server.

   The folder contains the following files:

   - *decrypt.key* file, which is used to decrypt the SASL and NES usernames and passwords.
   - *edgeagents-service-x64-`version`.msi* file, which installs the `Nymi Edge Agent` software on a thick client user terminal and uses the parameters detailed in the *edge_agents.conf* file.
   - *edgeagents-terminal-service-x64-`version`.msi* file, which installs the `Nymi Edge Agent` software on a RDP sessions host/Citrix server and uses the parameters detailed in the *edge_agents.conf* file.
   - *secretutil.cmd* file, which is Windows command utility that encrypts secrets.
   - *edge_agents.conf* file, which used to configure the parameters of the `Nymi Edge Agent` installation, and includes keys generated from the PowerShell utility.
   - *KafkaCA.pem* file, which is a default client truststore certificate.
2. Perform the following steps to generate the secret keys by using the *secretutil.cmd* file.

a) Click the **`Start`** menu and type `cmd`. Right-click **`Command Prompt`** and click **`Run as administrator`**.
b) Change the directory that contains the extracted `Nymi Edge Agent` installation package. For example, the *C:\edgeagents* folder.
c) Initialize *secretutil.cmd* with the following command:

```
secretutil.cmd -init
```

d) Use the *secretutil.cmd* command to encrypt the sasl username and password.

1. By default, the username is ctca. Type the following command to encrypt the username in an output file.

   ```
   secretutil.cmd -enc ctca>OUTPUT FILE NAME.txt
   ```

   where *`OUTPUT FILE NAME.txt`* is the name of the file that contains the encrypted username.
2. Type the following command to encrypt the SASL password.

   ```
   secretutil.cmd -enc PASSWORD>OUTPUT FILE NAME 2.txt
   ```

   where *`PASSWORD`* is the password specified by the person who implemented the server side components when they ran the *init-crypto* command and *`OUTPUT FILE NAME 2.txt`* is the name of the file that contains the encrypted password.

The output files contain the secret keys used in the *edge_agents.conf* file.

3. Perform the following steps to update the *edge_agents.conf* file with the secret keys that you created in the previous step.
   a) Open the *edge_agents.conf* file with a text editor.
   b) Update the value for the key `sasl.username`. It is the encrypted value in the username output text file.

   ```
   sasl.username=[encrypted username]
   ```

   c) Update the value for the key `sasl.password`. It is encrypted value in the password output text file.

   ```
   sasl.password=[encrypted password]
   ```

4. Save the *edge_agents.conf* file.
5. For Kafka TLS certificates that are issued from an untrusted CA only, perform the following steps to install the Kafka Truststore.
   a) Obtain the Kafka Broker root CA certificate from the person who implemented the CWP cluster. The file is stored in the CWP deployment package, in the *cwp/certs* folder.
   b) If required, rename the Kafka Broker root CA cert to *KafkaCA.pem*.
   c) Backup the *KafkaCA.pem* certificate in the `Nymi Edge Agent` installation directory.
   d) Replace the default *KafkaCA.pem* file in the `Nymi Edge Agent` installation package directory with the new *KafkaCA.pem* certificate file that you obtained from the implementation engineer.
6. Open the *edge_agents.conf*, and ensure that the value defined in the *`sasl.ca.path`* key is *C:\Nymi\Edge_Agents\certs\KafkaCA.pem*.

7. Uncomment the line `launcher.mode = 1`.
8. Edit the following configuration parameters in the *edge_agents.conf* file.

   Producer Specific Properties:

   - `bootstrap.servers`, which defines a list of host and port pairs of Kafka brokers.

   NES Specific Properties:

   - `nes.url`, which specifies the NES URL.
   - `agent.url`, which specifies the `Nymi Agent` URL. When you do not specify a value, `Nymi Edge Agent` will pick up the local `Nymi Agent` URL.
9. Save the *edge_agents.conf* file.

   Note: Ensure the *edge_agents.conf* file is configured prior to installing *edge_agents.msi*. This configuration file can then be copied to different machines being installed with `Nymi Edge Agent`.
10. Run the installer file *edgeagents-terminal-services-x64-`version`.msi*.
    The `Nymi Edge Agent` application is installed in the *C:\Nymi\Edge_Agents* folder and an `Nymi Edge Agent` service starts. Each time a user logs in to a Citrix or RDP session, an `Nymi Edge Agent Launcher` process starts and the `Nymi Edge Agent` service starts an `Nymi Edge Agent` process.

    Note: In `Task Manager`, the `Nymi Edge Agent Launcher` process appears as `Nymi Edge Agent` in the list of processes.

    When the user session ends, the additional `Nymi Edge Agent` and `Nymi Edge Agent Launcher` processes terminate.

    Note: The section *Nymi Edge Agent Log Files* provides information about `Nymi Edge Agent` log files.

Installing the Nymi Edge Agent Application on VMWare Horizon

Install `Nymi Edge Agent`as NES.

Before you begin

- Install the latest version of OpenSSL for Windows and add the *bin* directory is included in the system path.
- The `Nymi Edge Agent` package has been extracted to a central location.
- If an untrusted root CA issues the NES certificate, you must import the root CA certificate for the untrusted root. *Importing the Root CA certificate* provides more information.

About this task

Perform the following steps on the RDP session host / Citrix server:

Procedure

1. Copy the extracted *edgeagents* folder to the RDP session host / Citrix server.

   The folder contains the following files:

   - *decrypt.key* file, which is used to decrypt the SASL and NES usernames and passwords.

- *edgeagents-service-x64-`version`.msi* file, which installs the `Nymi Edge Agent` software on a thick client user terminal and uses the parameters detailed in the *edge_agents.conf* file.
- *edgeagents-terminal-service-x64-`version`.msi* file, which installs the `Nymi Edge Agent` software on a RDP sessions host/Citrix server and uses the parameters detailed in the *edge_agents.conf* file.
- *secretutil.cmd* file, which is Windows command utility that encrypts secrets.
- *edge_agents.conf* file, which used to configure the parameters of the `Nymi Edge Agent` installation, and includes keys generated from the PowerShell utility.
- *KafkaCA.pem* file, which is a default client truststore certificate.

2. Perform the following steps to generate the secret keys by using the *secretutil.cmd* file.
   a) Click the **`Start`** menu and type `cmd`. Right-click **`Command Prompt`** and click **`Run as administrator`**.
   b) Change the directory that contains the extracted `Nymi Edge Agent` installation package. For example, the *C:\edgeagents* folder.
   c) Initialize *secretutil.cmd* with the following command:

```
secretutil.cmd -init
```

   d) Use the *secretutil.cmd* command to encrypt the sasl username and password.
      1. By default, the username is ctca. Type the following command to encrypt the username in an output file.

```
secretutil.cmd -enc ctca>OUTPUT FILE NAME.txt
```

         where *`OUTPUT FILE NAME.txt`* is the name of the file that contains the encrypted username.
      2. Type the following command to encrypt the SASL password.

```
secretutil.cmd -enc PASSWORD>OUTPUT FILE NAME 2.txt
```

         where *`PASSWORD`* is the password specified by the person who implemented the server side components when they ran the *init-crypto* command and *`OUTPUT FILE NAME 2.txt`* is the name of the file that contains the encrypted password.

   The output files contain the secret keys used in the *edge_agents.conf* file.

3. Perform the following steps to update the *edge_agents.conf* file with the secret keys that you created in the previous step.
   a) Open the *edge_agents.conf* file with a text editor.
   b) Update the value for the key `sasl.username`. It is the encrypted value in the username output text file.

```
sasl.username=[encrypted username]
```

   c) Update the value for the key `sasl.password`. It is encrypted value in the password output text file.

```
sasl.password=[encrypted password]
```

4. Save the *edge_agents.conf* file.

5. For Kafka TLS certificates that are issued from an untrusted CA only, perform the following steps to install the Kafka Truststore.
   a) Obtain the Kafka Broker root CA certificate from the person who implemented the CWP cluster. The file is stored in the CWP deployment package, in the *cwp/certs* folder.
   b) If required, rename the Kafka Broker root CA cert to *KafkaCA.pem*.
   c) Backup the *KafkaCA.pem* certificate in the `Nymi Edge Agent` installation directory.
   d) Replace the default *KafkaCA.pem* file in the `Nymi Edge Agent` installation package directory with the new *KafkaCA.pem* certificate file that you obtained from the implementation engineer.
6. Open the *edge_agents.conf*, and ensure that the value defined in the *`sasl.ca.path`* key is *C:\Nymi\Edge_Agents\certs\KafkaCA.pem*.
7. Uncomment the line *`launcher.mode = 1`*.
8. Uncomment the line *`launcher.vmwarehorizon`* and change the value to 1.
9. Uncomment the line *`launcher.vmwarehorizon.remoteipmode`*, and set the value to one of the following numbers, depending on your configuration .
   - If the *`HKEY_CURRENT_USER\Volatile Environment\ViewClient_IP_Address`* key defines the remote IP address, set the value to `1`.
   - If the *`HKEY_CURRENT_USER\Volatile Environment\ViewClient_Broker_Remote_IP_Address`* key defines the remote IP address, set the value to `0`.
10. Edit the following configuration parameters in the *edge_agents.conf* file.

    Producer Specific Properties:

    - *`bootstrap.servers`*, which defines a list of host and port pairs of Kafka brokers.

    NES Specific Properties:

    - *`nes.url`*, which specifies the NES URL.
    - *`agent.url`*, which specifies the `Nymi Agent` URL. When you do not specify a value, `Nymi Edge Agent` will pick up the local `Nymi Agent` URL.
11. Save the *edge_agents.conf* file.

    Note: Ensure the *edge_agents.conf* file is configured prior to installing *edge_agents.msi*. This configuration file can then be copied to different machines being installed with `Nymi Edge Agent`.
12. Run the installer file *edgeagents-terminal-services-x64-`version`.msi*.
    The `Nymi Edge Agent` application is installed in the *C:\Nymi\Edge_Agents* folder and an `Nymi Edge Agent` service starts. Each time a user logs in to a VMWare Horizon session, an `Nymi Edge Agent Launcher` process starts and the `Nymi Edge Agent` service starts an `Nymi Edge Agent` process. When the user session ends, the additional `Nymi Edge Agent` and `Nymi Edge Agent Launcher` processes terminate.

    Note: The section *Edge Agent Log Files* provides information about `Nymi Edge Agent` log files.

Encrypting the Key File with EFS

The `Nymi Edge Agent` service runs under the Network Service account. Nymi recommends that you encrypt the *decrypt.key* file with EFS on each host after you install the `Nymi Edge Agent` application.

About this task

Nymi provides you with a script to perform the encryption.

Procedure

1. Run Power Shell as an administrator.
2. Enable the ability to run a script file in one of the following ways:
   - By setting the execution policy to `RemoteSigned`.
     a. From Power Shell, type `get-executionpolicy`.

        The output displays the current execution policy setting.
     b. Type `set-executionpolicy RemoteSigned`, and when prompted, type `Y`

        The execution policy is set to RemoteSigned.

     MSDN provides more information about how to modify execution policy settings.
   - By unblocking the script file.
     a. From Power Shell, type `unblock-file c:\Nymi\Edge_Agents\tools\encrypt-withEFS.ps1`

     MSDN provides more information about how to unblock script files.
3. Change to the *c:\Nymi\Edge_Agents\tools* directory.
4. Type *.\encrypt-withEFS.ps1 -file ..\conf\certs\decrypt.key*
5. Optional, use the **`set-executionpolicy`** command to set the execution policy to the original value.

Nymi API WebSocket Interface Configuration

Configuring and deploying in a physical environment

Take the following into consideration when configuring the `Nymi WebAPI` 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 WebAPI` 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 WebAPI` 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.

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 WebAPI` (if enabled). This section of the guide provides deployment information for setting up a centralized NES cluster and a Nymi Agent cluster for high availability and scalability. The centralized NES and Nymi Agent clustering architecture is defined in *Centralized Deployment Reference Architecture For NEE versions 2.5, 2.6 and 3.2*.

Introduction

This 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

About this task

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

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

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

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

About this task

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

Procedure

1. Designate a SQL Server instance as the primary replica during deployment.
2. Use the provided database DDL script to create the NES database on the primary replica.
3. Enable TCP on port 1433 for client connections on each SQL Server instance.
4. Windows authentication is enabled on each SQL Server Instance.
5. SQL Server Browser service's start mode is set to automatic on all SQL Server nodes.
6. SQL Server agent service's start mode is set to automatic on all SQL Server nodes.
7. Designate the name and IP address for the Availability Group Listener, this will be used for NES to connect to the NES database.
8. There is a valid AD account for NES to connect to the NES database. The account needs to have read/write permission on the NES database. To use Kerberos authentication, the SQL Server Service Principal Name (SPN) needs to be set for all SQL Server nodes and the AG Listener under the account.
9. To enable SQL Server transparent data encryption (TDE) in the Availability Group, create a master key and import the master key into every SQL Server instance.

Results

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

Deploy NES Instances

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

About this task

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

Procedure

1. Follow the steps in the *Installing NES* section to install NES on the individual servers. For the deployment, the following information is applicable:
   a) For the NES_URL value, use the fully qualified domain name (FQDN) of the NES virtual server instead of the FQDN of the individual server.

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

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

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

2. Follow the steps in *Setting Service Principal Names* and ensure that you set the Service Principal Name(SPN) to the service account.

Configure the NES Cluster on the Load Balancer

About this task

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

Procedure

1. Include all the NES instances as the backend servers for the virtual server.
2. Configure the cluster in active-active mode
3. Make source IP based session affinity (persistence) is configured.
4. For Layer 7 load balancer, SSL/TLS offloading can be configured for NES 3.2, and SSL/TLS bridging can be configured for NES 2.5, 2.6 and 3.2.
5. The URL for the liveness test of the NES instances is: *<nes_admin_service>/nes/ping* where *<nes_admin_service>* is the name of the NES Admin service.

Configure SSL/TLS Bridging

Follow this section for configuring SSL/TLS bridging.

About this task

Procedure

1. Each NES instance has HTTPs enabled with a valid TLS certificate for the instance during the installation
2. There is a valid TLS certificate for the cluster's FQDN
3. The cluster's IP address is allocated to the load balancer and is bound to the cluster's FQDN in the respective DNS.
4. Import the TLS certificate into the load balancer, and bind it to the NES cluster.
5. When applicable, ensure the signing CA certificate(s) for each NES instance's TLS certificate is trusted by the load balancer
6. Configure the load balancer to use the HTTPs URLs of the individual NES instance.

Configure SSL/TLS Offloading

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

About this task

Procedure

1. Each NES instance has HTTPs enabled during the installation.
2. There is a valid TLS certificate for the cluster's FQDN.
3. The cluster's IP address is allocated to the load balancer and is bound to the cluster's FQDN in the respective DNS.
4. Import the TLS certificate into the load balancer, and bind it to the NES cluster.
5. Configure the load balancer to use the HTTP URLs of the individual NES instance.

Deploy the Nymi Agent Cluster

About this task

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

Procedure

1. When the Nymi cluster needs to support thin-client or RDP, the cluster must be configured in active-passive mode.
2. When the Nymi Agent cluster does not need to support thin-client, RDP, and WebApi, the cluster can be configured in active-active mode.
3. When the Nymi Agent cluster needs to support WebApi, two clusters must be configured on the same load balancer (or load balancer cluster). One cluster for the websocket service on port 9120, and one for the WebApi. Whether both the clusters can be configured in active-active mode or not will depend on the capability of the load balancer. The same session affinity/persistence needs to be applied across the two clusters.
4. It is not possible to use WebApi in thin-client or RDP environments.

Deploy Nymi Agent Instances

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

About this task

Configure the Load Balancer Without WebApi Support

About this task

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

Procedure

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

2. The virtual server's service port should be TCP/9120.
3. The backend server port should be TCP/9120.
4. Configure the virtual server in active-active mode if it does not need to support thin-client, RDP.
5. Ensure the source IP based session affinity (persistence) is configured when the virtual server is configured in active-active mode.
6. For liveness tests on the backend servers, use TCP connection test on port 9120 of the backend servers.
7. Configure the liveness test for the Nymi Agent instances to use TCP connection on the designated websocket port.

Configure the Load Balancer With WebApi Support

About this task

For WebApi, two clusters are required, one for the websocket service on port 9120, and one for the WebApi. Whether the cluster can be configured in active-active mode or not will depend on the capability of the load balancer. If the load balancer supports session affinity across multiple virtual servers (for example, with Citrix Netscaler's *Persistence Groups*, and F5's *Match Across options)*, it is possible to configure both Nymi Agent clusters in active-active mode. Active-active mode will also require source IP based session affinity so that all the traffic from a specific source IP will be directed to the same Nymi Agent instance in both clusters.

Procedure

Configure the Load Balancer for the Websocket Service on Port 9120

About this task

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

Procedure

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

Configure the Load Balancer for the WebApi Service

About this task

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

Procedure

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

Configure SSL/TLS Offloading

About this task

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

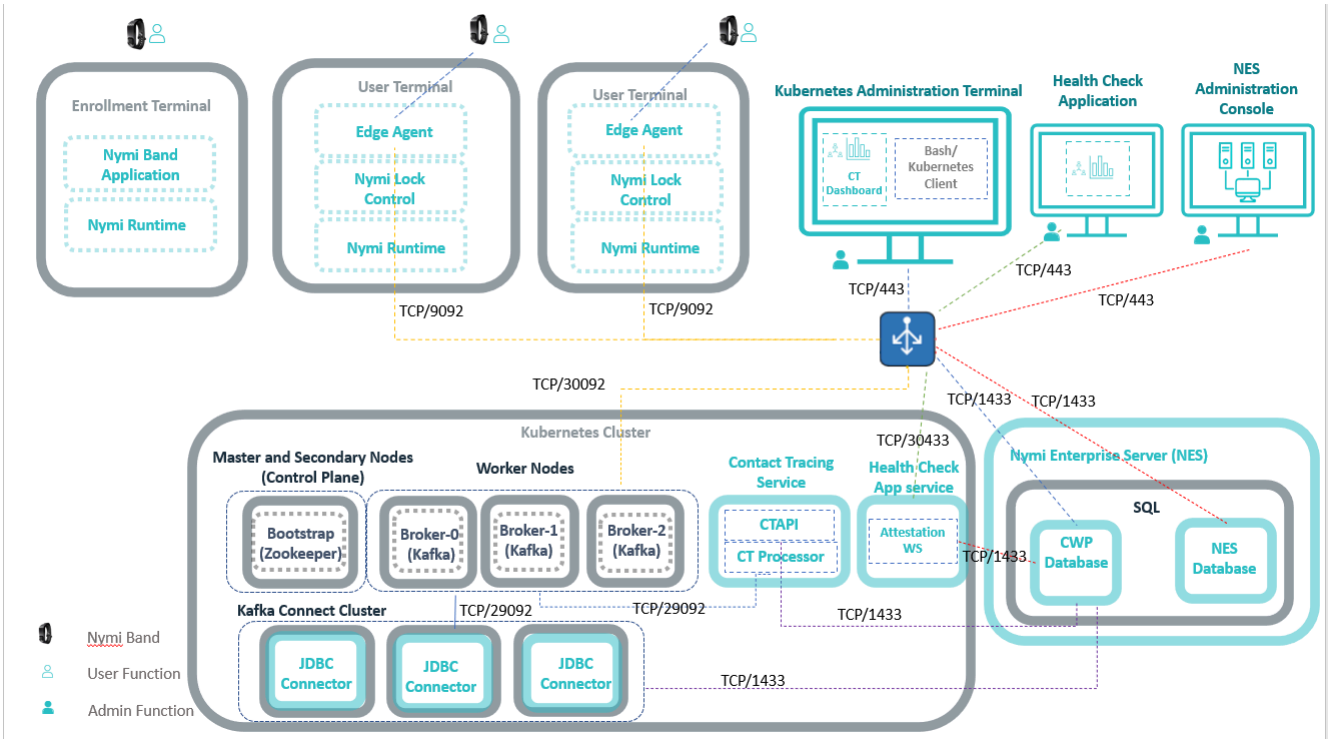
Procedure

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

Deploy Smart Distancing and Contact Tracing

`Connected Worker Platform` includes many components, which together provide a Smart Distancing and Contact Tracing(SDCT) container clustered service that addresses contact tracing, smart reminders, and attestations requirements to support a safe workplace environment.

The following section provides an overview of the `Connected Worker Platform` with the SDCT service.



`Figure 41: Connected Worker Platform with SDCT Environment`

Enrollment Terminal

Terminal on which you install the `Nymi Band Application`. User access the `Nymi Band Application` to enroll to a Nymi Band. The `Nymi Band Application` also installs the `Nymi Runtime` application.

Contact Tracing Events

When a user wearing an authenticated Nymi Band stays in close proximity to another user wearing an authenticated Nymi Band for approximately 15 cumulative minutes over a 24-hour period.

User Terminal

A thick or thin client that is used by a Nymi Band user to perform daily tasks. When you install `Nymi Lock Control` and `Nymi Runtime` on the user

terminal, users can lock and unlock the user terminal with an authenticated Nymi Band.

Nymi Edge Agent

The `Nymi Edge Agent` is installed on each user terminal in the environment and establishes BLE communication with Nymi Bands via `Nymi Bluetooth Endpoint` and the `Nymi Agent` services that are installed by `Nymi Runtime`.

`Nymi Edge Agent` retrieves contact tracing data from Nymi Bands within 3-4 meters of the user terminal. `Nymi Edge Agent` sends the data to the Kafka processing system in the Kubernetes cluster.

Kubernetes Cluster

Provides container cluster deployment, orchestration, scaling, failover and management for the SDCT container clusters. The Kubernetes cluster includes:

- At least one master node and one or more secondary nodes on which Zookeeper resides. Also referred to as the control plane. The control plane consists of control plane master nodes that manage Kubernetes controllers, such as replication controller, endpoint controller, namespace controller, and service accounts controller. A control plane may consist of one or more master nodes (control plane master nodes) to run across multiple computers for high availability, however only one master node may be active at a time.
- Three or more worker nodes on which the brokers and Kafka reside. The worker nodes run containerized applications and host pods (components of an application's workload).

  Each node consists of:

  - kubelet, which ensures that containers are running in a pod
  - kube-proxy, which directs network traffic to and from pods
  - container runtime, which runs the containers.

  Each node is managed by the control plane. Typically, there are several nodes in a cluster, and a pod typically has one container.

  Zookeeper sends jobs to the brokers. SDCT interacts with 5 services in the cluster: bootstrap, broker-0, broker-1, broker-2, and `Contract Tracing API` (`CTAPI`).
- Contact Tracing Service, which includes:

- `CTAPI` is the part of Contact Tracing Service that provides the contact tracing dashboard and an API to access contact tracing graph data.
- `Contact Tracing Processor` is the part of Contact Tracing Service that generates contact tracing graph data from contact tracing events.

- Kafka, receives and processes contact tracing data from `Nymi Edge Agent`. The Kafka processing system and the `Contact Tracing Processor` transform contact tracing data and then send the data to the CWP Database.
- Kafka Connect Cluster contains Kafka Connect Nodes. Each Kafka Connect Node contains a JDBCConnector.
- JDBCConnector uses Kafka Connect to store authentication and temperature information events in the CWP Database. The configuration of the JDBCConnector determines how the information that is retrieved from the Nymi Band (and published on Kafka) is stored in the CWP Database.

CWP Database

Stores information about contact tracing, Nymi Band authentication, temperature sensing, and Health Attestation results that are received from `CTCS`. Contact tracing data contains information from the Nymi Enterprise Server for contact tracing purposes.

SDCT Management Terminal

Provides the CWP Administrator with the following tools to manage the SDCT environment.

- bash to create and manage the Kubernetes cluster.
- kubectl (AWS only) to manage the Kubernetes cluster and services.
- Contact Tracing Dashboard, a web-based application that allows you to visualize and analyze contact tracing data from the CWP Database for employees that are enrolled in the Contact Tracing program. Use the Contact Tracing Dashboard to view the relationships between contact tracing events from different users. Contact Tracing Dashboard retrieves events in the `CWP Database` via `CTAPI`.

Prepare for Kubernetes and SDCT Deployment

Review the following sections for infomration about hardware, software, and firewall port requirements, as well as how to prepare the Kubernetes Administration Terminal and create the CWP Database.

Hardware and Software Requirements

This section describes the hardware and software requirements for Smart Distancing and Contact Tracing.

NES

- Microsoft SQL Server Management Studio
- Windows 2016
- Windows 2019

Note: Refer to the Nymi Connected Worker Platform NES Deployment Guide for more information about NES requirements and deployment information.

User Terminal

Review the following requirements for the user terminals on which you install Nymi Edge Agent.

- Supported Operating Systems:
  - Windows 10 64-bit
- TLS 1.2 enabled
- Oracle Java SE Runtime 8 32-bit or 64-bit (included in Oracle JDK 1.8.x)
- OpenSSL (latest version)
- Resides on the same domain as NES
- Root CA certificate for NES and Kafka

Kubernetes Administration Terminal

Review the following requirements for the user terminal that you use to access the Kubernetes cluster:

- OS that supports *kubectl* and *bash* terminal, including Windows 10 64-bit with Linux Bash Shell
- Oracle Java JDK 8 or later (32-bit or 64-bit)
- Javascript-enabled browser, such as Microsoft Edge, Google Chrome, Safari, or Mozilla Firefox

Kubernetes Cluster Deployment

The requirements for the Amazon Linux 2 Kubernetes Cluster deployment include:

- Control plane node: AWS Elastic Kubernetes Services (EKS)
- Worker node: EC2 instance with Amazon Linux II OS (ex. t3.xlarge, t4g.large), 4-core CPU, 16 GB RAM, 512 GB SSD
- Self signed or CA-issued TLS certificates for Kafka and `CTAPI`.

  Note: TLS certificate for `CTAPI` and Kafka can be the same, but the SubjectAlternativeNames must include all of the FQDNs.

CWP Database

The Contact Tracing, Health Attestation and Temperature Alert features store data in a Microsoft SQL database that supports TLS 1.2 and later.

The following Microsoft SQL versions are supported:

- SQL Server or SQL Server Express 2016
- SQL Server or SQL Server Express 2017
- SQL Server or SQL Server Express 2019

If your NES database is one of these supported versions, you can deploy the CWP Database on the SQL server with the NES instance.

Note: SQL Server / SQL Express 2016 and SQL Server / SQL Express 2017 require a patch to provide TLS 1.2 support. Microsoft provides more information.

DNS Requirements

CWP requires DNS or */etc/hosts* file entries for the following components.

Note: *`namespace`* is the namespace of CWP and *`domain`* is the public domain name that you will define for the *`KAFKA_BROKER_PUBLIC_DOMAIN`* environment variable.

Host	Purpose
Kubernetes API Server Endpoint	Required when joining a node to the cluster and by kubtctl, should be the same as the server specified in *~/.kube/admin.conf*.
Kafka bootstrap server	Can be any valid DNS name of your choice.
broker.*`namespace`*.svc.cluster.local	For internal Kafka Client access to Kafka Bootstrap Server.
broker-0.broker.*`namespace`*.svc.cluster.local	For internal kafka client access to kafka broker 0.
broker-1.broker.*`namespace`*.svc.cluster.local	For internal kafka client access to kafka broker 1.
broker-2.broker.*`namespace`*.svc.cluster.local	For internal kafka client access to kafka broker 2.
`FQDN_CWP_web_server`	For web access to the `Health Check Application`. The FQDN of the virtual server on which the `Health Check Application` Service resides. **Note:** The FQDN that you choose must match the Subject Alternative Name for the CWPWEB TLS certificate.
`FQDN_CTAPI`	For web access to the Contact Tracing Dashboard. The FQDN of the virtual server on which `CTAPI` resides. **Note:** The FQDN that you choose must match the Subject Alternative Name for the `CTAPI` TLS certificate.

Host	Purpose
Load Balancers	For a managed Kubernetes cluster in AWS or Azure, the deployment process creates load balancers for the Kafka bootstrap server, Kafka brokers, `CTAPI` and the `Health Check Application` service. The DNS entries that are required for the public IP addresses of the load balancers differ based the configuration: • When you use static IP addresses, define a type A record for the IP address of the load balancer. • When you use dynammic IP addresses, define a CNAME record for the FQN of the load balancer.

Firewall Port Requirements

The following tables outline the port requirements for the `Connected Worker Platform` components.

Table 8: Control Plane Nodes Firewall Port Requirements

Protocol	Direction	Port Range	Purpose	Used By
TCP	Inbound	443	Kubernetes Dashboard service	Cluster
TCP	Inbound	6443 (overridable)	Kubernetes API server	Cluster
TCP	Inbound	2379-2380	etcd server client Cluster	kube-apiserver, etcd
TCP, UDP	Inbound	53	Core DNS	Cluster
TCP	Inbound	179	BGP routing	Calico CNI
TCP	Inbound	9500	Longhorn CSI (for self-managed Kubernetes Clusters	Cluster
TCP	Inbound	9090	Prometheus API access	Frontend
TCP	Inbound	9100	Prometheus Node Exporter	Cluster
TCP	Inbound	22	ssh	remote access

Table 9: Worker Nodes Firewall Port Requirements

Protocol	Direction	Port Range	Purpose	Used By
TCP	Inbound	10250	kubelet API	Self, Control plane

Protocol	Direction	Port Range	Purpose	Used By
TCP	Inbound	10255	kubelet API read-only	Control plane
TCP	Inbound	10256	Health check	Control plane
TCP	Inbound	179	BGP routing, for pod to pod networking	Pods
TCP	Inbound	22	ssh for deployment and maintenance	administrators
TCP	Inbound	30090-30094	Kafka Broker (internal access)	`Nymi Edge Agent`
TCP	Inbound	31443	CTAPI Web service (external access)	Client, Load Balancer

Table 10: Load Balancer Firewall Port Requirements

Protocol	Direction	Port Range	Purpose	Used By
TCP	Inbound	9092	Load balancer for Kafka Broker	`Nymi Edge Agent`
TCP	Inbound	443	CTAPI Web service	`Contact Tracing Dashboard`, `Health Check Application`, NES Administrator Console

Table 11: Kafka Connect Requirements

Protocol	Direction	Port Range	Purpose	Used By
TCP	Inbound	29092	JDBC Connector	Worker Nodes, Contact Tracing Service

Table 12: CWP Database Requirements

Protocol	Direction	Port Range	Purpose	Used By
TCP	Inbound	1443	SQL database	JDBC Connector, Contact Tracing Service

Certificate Requirements

The environment requires TLS certificates to gain secure access to the Kubernetes cluster, the `Contact Tracing Dashboard` and the `Health Check Application`.

Kafka TLS Certificate

Create a TLS certificate for Kafka.

Before you generate and install the TLS certicate, create a certificate that:

- Is in PKCS#12 format.
- Contains the TLS certificate, the private key of the certificate, and the certificate of the signing authority.
- Has extended key usage Server Authentication. (1.3.6.1.5.5.7.3.1) and Client Authentication (1.3.6.1.5.5.7.3.2).
- Has subject alternative names that match the FDQNs of the following internal and external Kafka broker listeners:
  - broker-0.broker.*`namespace`*.svc.cluster.local
  - broker-1.broker.*`namespace`*.svc.cluster.local
  - broker-2.broker.*`namespace`*.svc.cluster.local
  - *`namespace`*-broker-0.*`domain`*
  - *`namespace`*-broker-1.*`domain`*
  - *`namespace`*-broker-2.*`domain`*

  where:

  - *`namespace`* is the namespace of CWP.
  - *`domain`* is the public domain name that you will later define for the *`KAFKA_BROKER_PUBLIC_DOMAIN`* environment variable.

CTAPI and Health Check Application Service TLS Certificate

Create a TLS certificates for the `CTAPI` and the `Health Check Application` Service.

Before you generate and install the TLS certificate, create a certificate that:

- Is in PKCS#12 format.
- Contains the TLS certificate, the private key of certificate, and the certificate of the signing authority.

Deployment, Installation, and Configuration Overview

The following section provides a high level overview of the deployment, installation and configuration process.

About this task

Procedure

1. Review the required firewall ports, and update as required.

2. Install `Nymi Runtime`, `Nymi Bluetooth Endpoint`, and `Nymi Agent`.
   a) Install `Nymi Bluetooth Endpoint` on the user terminal used to collect contact tracing data from Nymi Bands.
   b) Install `Nymi Agent` on the terminal used to access the Contact Tracing Dashboard (for example, the server).

      For users running Citrix or RDP, install the `Nymi Agent` on the Contact Tracing server.
3. Install bash.exe (Ubuntu). Refer to Installing Bash on the Kubernetes Administration Terminal on page 108.
4. Deploy an AWS with EKS Kubernetes Cluster. Refer to Deploy A Kubernetes Cluster in AWS Using EKS on page 115.
5. Create the SQL database for Contact Tracing. Refer to Creating the CWP Database and tables on page 111.
6. Prepare the Kubernetes environment for Contact Tracing services. This process involves obtaining certificates and editing environment variables. Refer to Customize the Kubernetes environment for SDCT on page 119.
   a) Set up the service account password.
   b) Install TLS certificates for Kafka and CTAPI. Refer to Preparing Certificates to install SDCT on page 119.
   c) Set up environment variables. Refer to ENV variables.
7. Encrypt passwords to Kubernetes components. Refer toEncrypting the Passwords for Kubernetes Components on page 132. Verify that the passwords in the env file are updated.
8. Launch Kubernetes (refer to Launching the Kubernetes Environment on page 133), then ensure the Kubernetes cluster is running.

   ```
   kubectl get pods -A
   ```
9. Install `Nymi Edge Agent` on a domain-joined (NES) terminal. Refer to .Installing and Running the Contact Tracing Collection Agent. You will need to:
   a) Encrypt the SASL username and password.
   b) Encrypt the truststore password.
   c) Update TLS certificates.
   d) Update the *edge_agents.conf* file to include the newly encrypted username and password.
   e) Install `Nymi Edge Agent` and configure the environment variables.
10. Enable SDCT components in Nymi Enterprise Server.

    On Nymi Enterprise Server, go to the NES Administrator Console and enable Smart Distancing and Contact Tracing.
11. Update the configuration settings on the Nymi Bands by having Nymi Band users log into Nymi Band Application.

Installing Bash on the Kubernetes Administration Terminal

If you do not have a Linux system, install Linux Bash shell on a user terminal in your environment that will act as the Kubernetes Administration Terminal.

Before you begin

Before you perform these steps, ensure that Oracle JDK 8 or later is installed on the terminal.

About this task

The following procedure describes how to install Linux Bash Shell on a Windows 10 machine.

Note: You will need to restart the computer to apply changes to the terminal.

Procedure

1. Log into Windows as an administrator.
2. Go to **Programs and Features**.
   Start > Control Panel > Programs > Programs and Features
3. Select **Turn Windows Features On or Off**.
   A window appears with a list of Windows features.
4. Select **Virtual Machine Platform** and **Windows Subsystem for Linux**, and then click **OK**.
   Windows will search for and install the required files. Restart the terminal to apply the changes.
5. Perform the following steps to obtain **Ubuntu** from the **Microsoft Store**.
   a) From the **Start** menu, type `Microsoft Store`, and then select **Microsoft Store**.
   b) In the **Search** field, type `Ubuntu`.
   c) From the list of apps that appear. select the **Ubuntu** application without the version number.

      Note: The **Ubuntu** application without the version number contains the most recent version. You may choose an earlier version if it is more applicable for your system.
   d) Click **Get**.

      A window appears that prompts you to sign in. You may skip this by closing the pop-up window.

      The **Ubuntu** application downloads in the background.
   e) When complete, click **Launch**.
      An **Ubuntu** windows appears and installs Ubuntu.
   f) At the **Enter a new UNIX username** prompt, type a new username.
   g) As the **New password** and **Retype new password** prompt, type a password for the user.
6. From the **Microsoft Store**, search for the **Windows Terminal** application.
7. Click **Get**
   The **Windows Terminal** application installs.

Results

To open **bash**, go to the **Start** menu and type `bash`.

Alternatively, you can open **Windows Terminal**, click on the dropdown arrow from the top tool bar, and then select **Windows Powershell** or **Ubuntu**.

Obtaining the SDCT packages

Your Nymi Solution Consultant provides you with packages that contains several files and scripts to assist you in the SDCT and Kubernetes configuration and deployment.

About this task

- *edgeagents-x64.u.v+wx-yz.zip* - Contains the files to deploy and configure `Nymi Edge Agent` on the User Terminal/Collection Agent.
- *cwp-deployment-1.3.u.bc* - Contains the files to deploy and configure CWP in the Kubernetes cluster.
- *cwp-deployment-update-1.3.u.bc* - Contains the files to update CWP in the Kubernetes cluster.

Procedure

1. Download and extract the *edgeagents-x64.v+wx-yz.zip* package to a central location that is accessible to the user terminals.
   The *edgeagents* folder is created.
2. For a new install, download and extract the file *cwp-deployment-1.3.v.bc* to a central location that is accessible to the Kubernetes Administration Terminal, and then copy to the folder to the Kubernetes Administration Terminal.
   For example, the *cwp-deployment-1.3.x.y* folder is created that contains the *cwp* and *deploy*folders.

   Note: The folder in which you extracted the CWP 1.3 installation package is referred to as the CWP 1.3 deployment folder (*CWP_12_deployment_folder*) in this guide.
3. For an upgrade, download and extract the file *cwp-deployment-update-1.3.v.de* to a central location that is accessible to the Kubernetes Administration Terminal, and then copy the folder to the Kubernetes Administration Terminal.
   For example, the *cwp-deployment-update-1.2.x.y* folder is created that contains the the *cwp* and *kube* folders.

   Note: The folder in which you extracted the CWP 1.3 upgrade package is referred to as the CWP 1.3 deployment folder (*CWP_12_deployment_folder*) in this guide.

Recording the SDCT Variables

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

Use the following table to keep track of values for variables that you define during the deployment.

Table 13: Environment Variable Values

Variable Name	When Used	Value
CT_DB_CATALOG	The SQL database name for contact tracing. Required when you configure the *.env* file.	
CT_DB_USERNAME	Required when you configure the *.env* file.	

Variable Name	When Used	Value
CT_DB_PWD	Define this value when you run the *init-crypto* script.	
CT_DB_INSTANCE	Required when you configure the *.env* file.	
KAFKA_BROKER _PUBLIC_DOMAIN	The public domain. Required when you configure the *.env* file.	

Creating AD Group for Health Check Application Access

Create a new Active Directory group with a list of Health and Safety users and groups that require administrative access to the Health Check Application

About this task

When creating the Active Directory group:

Procedure

1. For the **`Group Type`**, select **`Security`**
2. For the **`Group Scope`**, select the option according to your IT policy.

Prepare the Database

Before you deploy CWP, prepare the SQL database.

Creating the CWP Database and tables

Perform the following steps in SSMS to create the `CWP Database` and tables, and then ensure that `CTAPI` can to connect to the NES and SQL database.

Before you begin

- Ensure that the extracted CWP deployment package is in a central location.

About this task

Perform the following steps on a machine that has SSMS installed and has access to the NES database server.

Procedure

1. Navigate to the *`CWP_12_deployment_folder`*`\cwp\ctprocessor` folder in the shared location, and then copy the the *ct-mssql.sql* file to a local directory.
2. Navigate to the *`CWP_12_deployment_folder`*`\kafka-connect\config` folder in the shared location, and then copy the *auth-mssql.sql* file to a local directory.
3. Open SSMS, and then login to the SQL Server.
4. Right-click the SQL instance, and the select **`Properties`**.

5. In the **Object Explorer**, select **Security**
6. Select **SQL Server and Windows Authentication Mode**, and then click **OK**.
7. In the **Object Explorer** right-click Databases, and the select New Database.
8. Name the database ContactTracing, and then click **OK**.
   Record the value that you specify in the SDCT Variables table for the variable *CT_DB_CATALOG*.
9. In the **Object Explorer**, go to **Security > Logins**.
10. Right-click **Logins** and click **New Login**.
    A **Login - New** window appears.
11. On the **General** page, perform the following actions.
    a) Specify a login name.
       Record the value that you specify in the SDCT Variables table for the variable *CT_DB_USERNAME*.
    b) Click **SQL Server authentication** and enter a password.
       Record the value that you specify in the SDCT Variables table for the variable *CT_DB_PWD*
12. On the **Server Roles** page, select **DBCreator**, and leave the default option **Public**.
13. On the **User Mapping** page, perform the following actions.
    a) In the **Map** column, select the checkbox beside the **CWP** database, that you created previously.
    b) In the **Database role membership for CWP** section at the bottom of the window, select **db_owner** and leave the default selection **public** enabled.
    c) Click **OK**.
14. From the **File** menu, select **Open > File...**, navigate to folder that contains the *ct-mssql.sql* script file that you downloaded, and then click **Open**.
    The script opens in the query window.
15. On the menu bar, click **Execute**.
    The script creates a table for Contact Tracing proximity events with the username and password that you specified previously.
    The script creates the dbo.CovidContacts table.
16. From the **File** menu, select **Open > File...**, navigate to folder that contains the *auth-mssql.sql* script file that you downloaded, and then click **Open**.
    The script opens in the query window.
17. On the menu bar, click **Execute**.
    The script creates the SQL table for authentication events with the username and password that you specified previously.
    The script creates the and dbo.AuthInfo table.
18. Close SSMS.

Results

The following figure shows SSMS with the new CWP Database and the **Message** window after successfully executing the *ct-mssql.sql* script.

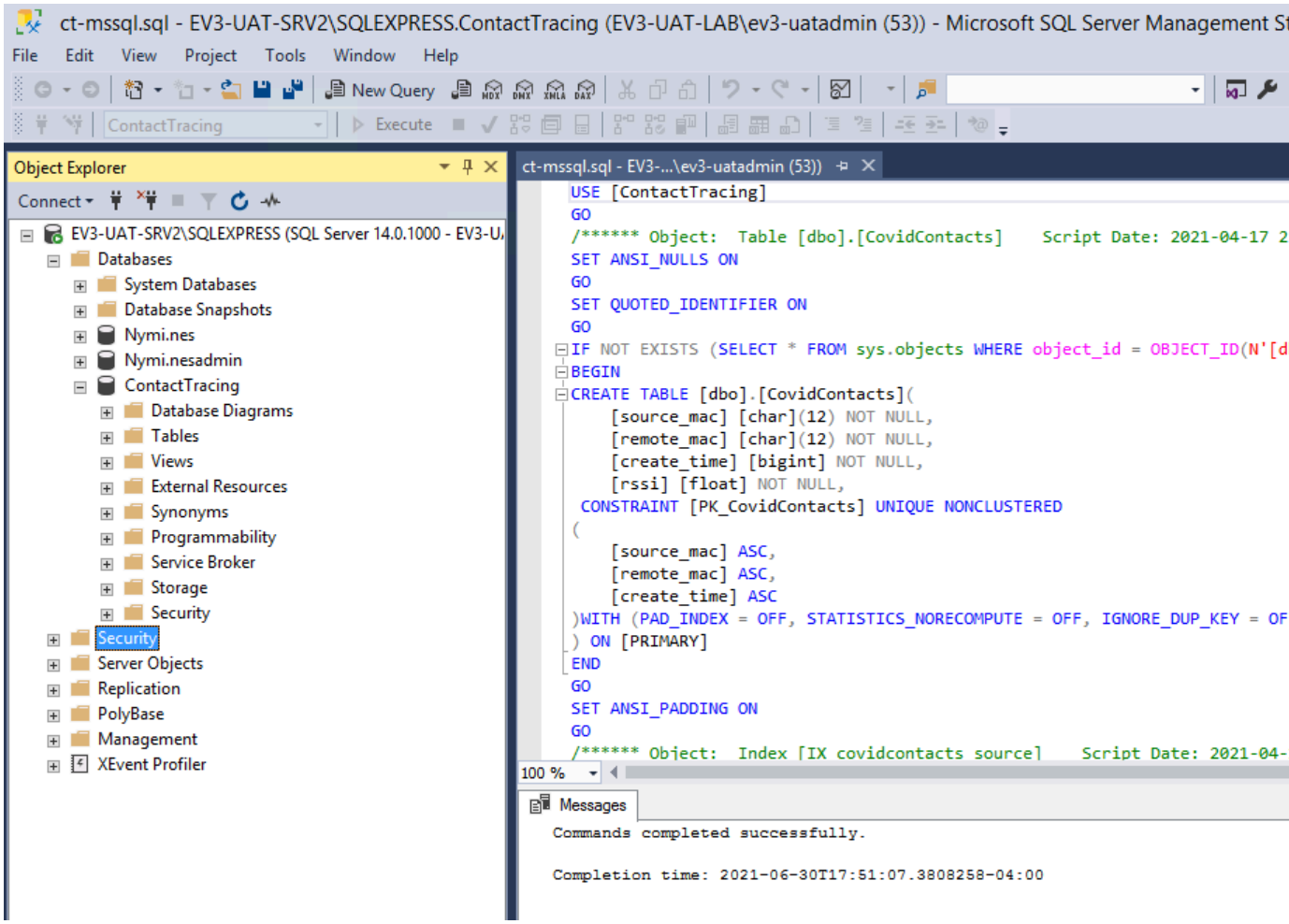


Figure 42: SSMS with ContactTracing Database

Creating Tables for Health Attestation and Temperature Alerts

If your environment uses the Health Attestation and Temperature Alerts features, run the Nymi-provided SQL scripts to create the appropriate tables.

Before you begin

- The user that creates the database must have db_owner or db_ddladmin privilege to the `CWP Database`.
- Ensure that the extracted CWP deployment package is in a central location.

About this task

Perform the following steps from a computer that has SSMS installed and access to the SQL Server with the `CWP Database`.

Procedure

1. Open SSMS and connect to the SQL server.
2. Navigate to the *CWP_12_deployment_folder**cwp**cwpweb**config* folder in the shared location.
3. Copy the *mssql.sql* file to local directory.
4. Navigate to the *CWP_12_deployment_folder**cwp**kafka-connect**config* folder in the shared location.
5. Copy the *temp-mssql.sql* file to a local directory.
6. In the local directory, double-click on the *mssql.sql* file.
   A new query window appears.
7. Click the **Execute** button.
   The script creates the dbo.NymiAttestationInfo and dbo.JwtStore tables.
8. In the local directory, double-click on the *temp-mssql.sql* file.
   A new query window appears.
9. Click the **Execute** button.
   The script creates the dbo.NymiTempInfo table.

Configuring the SQL Server

Ensure that the TCP/IP is enabled fo the SQL instance.

About this task

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

Procedure

1. In the left navigation pane, expand SQL Server Network Configuration, and then select the appropriate Protocols for the SQL Server option.
2. In the right pane, select TCP/IP, and then right-click and select **Enabled**.
3. Double-click **TCP/IP**.
4. In the TCP/IP Properties window, select the **IP addresses** tab.
5. Navigate to the IPALL section, and then for the **TCP port** value, type 1433.
6. Click **OK**, and then click **Apply**.
7. On the prompt to restart the SQL services, click **OK**.
8. Restart SQL server services.

Kubernetes Deployment

To implement Smart Distancing and Contact Tracing, you must deploy a Kubernetes cluster with at least physical computer or virtual machine that acts as the worker node.

For high availability, the number of control plane master nodes that you require depends on how the ETCD cluster is deployed. There are two choices:

- In a stacked Kubernetes production environment with bundled ETCD cluster. There must be at least 3 control plane master nodes.
- In a Kubernetes environment that uses an external ETCD cluster. There must be at least 2 control plane master nodes.

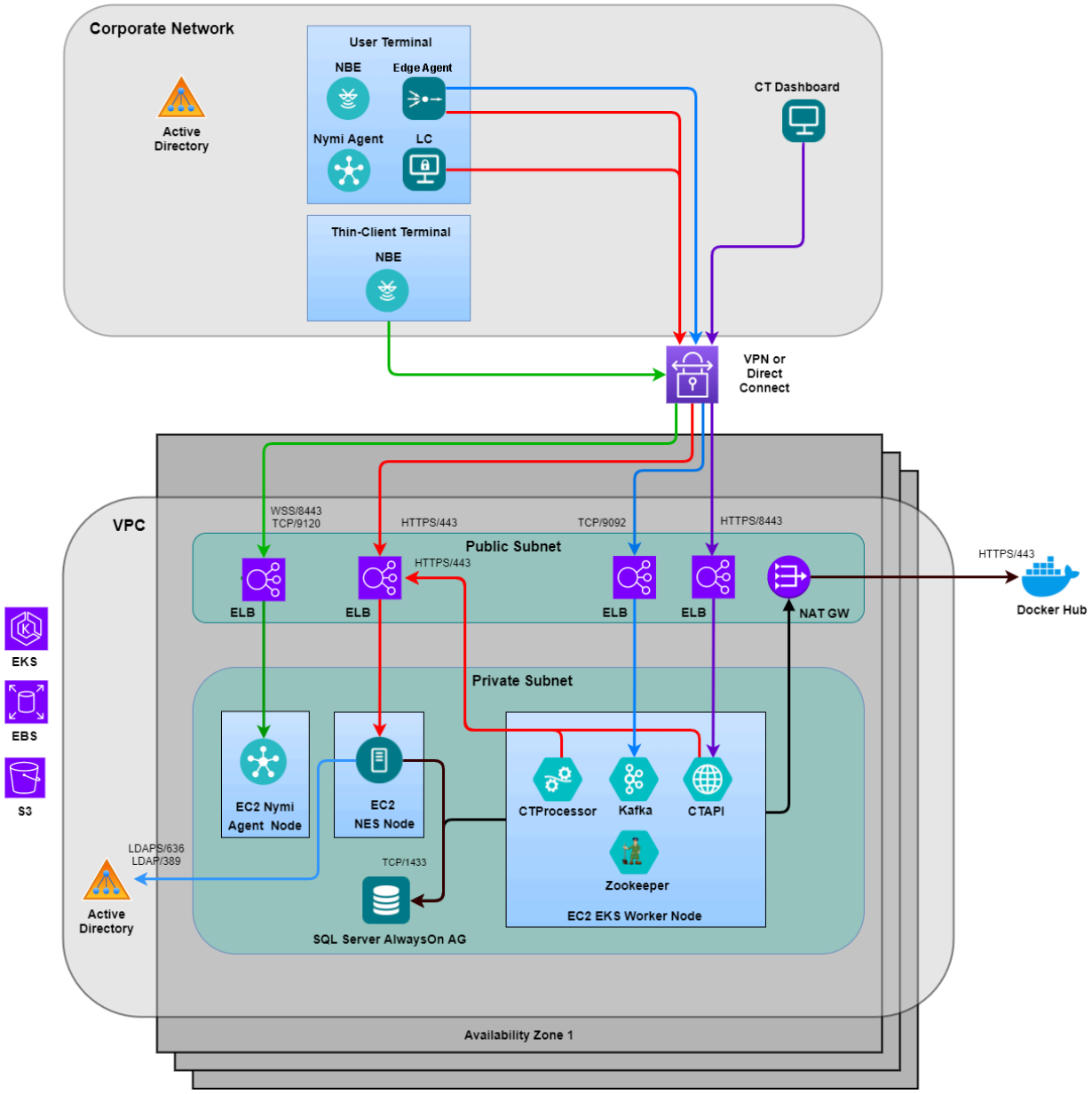
Note: ETCD is an open source distributed key-value store that manages data for Kubernetes. ETCD is a quorum based system. The number of nodes required in an N-node cluster is N/2 + 1.

Table 14: Number of Nodes Required for High Availability

No. of Nodes	Quorum Required	No. of Nodes Allowed to Fail
2	2	0
3	2	1
4	3	1
5	3	2
6	4	2

Deploy A Kubernetes Cluster in AWS Using EKS

The following diagram provides an overview of the CWP Kubernetes cluster deployment architecture for AWS EKS.


Corporate Network
Active Directory
User Terminal
NBE
Edge Agent
Nymi Agent
LC
Thin-Client Terminal
NBE
CT Dashboard
VPN or Direct Connect
VPC
WSS/8443
TCP/9120
HTTPS/443
TCP/9092
HTTPS/8443
Public Subnet
HTTPS/443
ELB
ELB
ELB
ELB
NAT GW
HTTPS/443
Docker Hub
EKS
EBS
S3
Private Subnet
EC2 Nymi Agent Node
EC2 NES Node
CTProcessor
Kafka
CTAPI
Zookeeper
EC2 EKS Worker Node
LDAPS/636
LDAP/389
TCP/1433
Active Directory
SQL Server AlwaysOn AG
Availability Zone 1

Kubernetes deployment in AWS with EKS includes the following steps:

1. Create a AWS VPC for EKS Cluster
2. Create a ESK Cluster

Note: It is very important to keep the *env* file after the deployment. It contains crucial parameters required for removing the cluster and VPC.

VPC Considerations

To create an EKS cluster, you require an available VPC.

The VPC should include subnets across multiple available zone in the respective AWS region. In a production environment, consider using 3 or more availability zones when possible.

The VPC may include both public and private subnets. The following table summarize the subnet configurations:

Table 15: VPC Subnet Configurations

Subnet Configuration	Detail	Application
Both public and private subnets	Public subnet for ELB and Private subnets for EKS worker nodes	Internet facing
Public subnets only	Public subnet for ELB and EKS worker nodes	Internet facing
Private subnets only	Private subnets for the EKS worker nodes. This configuration requires a NAT Gateway to allow nodes to access internet	Not for internet facing

Installing Kubernetes Client (AWS)

Perform the following steps to create the Kubernetes client when using AWS.

About this task

Procedure

1. On the Kubernetes Administration Terminal, open a **bash** terminal and change to the *CWP_12_deployment_folder*/*deploy/kube/client* folder.
2. Type `./init-client -a aws-region -c cluster name`

   Where:

   - *aws-region* defines the AWS region where the cluster resides.
   - *cluster name* defines the name of the EKS cluster.

Running the VPC Creation Script

Perform a new VPC deployment by using the **create-vpc** script.

About this task

Perform the following steps on the designated initial master node.

Procedure

1. On the Kubernetes Administration Terminal, open a PowerShell or **bash** terminal and change to the *CWP_12_deployment_folder*/deploy/kube/init/aws folder in the shared location.
2. Type `./create-vpc -region aws-region [-public] [-private] [-cidr network_CIDR]`

   where:

   - *aws-region* - Defines the AWS region on which to create the VPC.
   - -public - Creates a public subnet in each availability zone, up to a maximum of 3 availability zones may be used
   - -private - Creates a private subnet in each availability zone, up to a maximum of 3 availability zones may be used
   - -cidr *network_CIDR* - Defines the network CIDR of the VPC. It is recommended to use a class A private network CIDR with 16 bit blocks.

   For example, the following command creates a VPC with private subnets in the designated region *us-east-2*: `./create-vpc -region us-east-2 -private -cidr 10.120.0.0/16`

   This command distributes the network CIDRs of the subnet according to the size of the CIDR blocks on the VPC. The size of the network CIDRs will be 1/16 of the size of the VPCs.

Creating a EKS Cluster

Create a new EKS cluster by using the **create-cluster** script:

About this task

Perform the following steps on the designated initial master node.

Procedure

1. Open a **bash** terminal and change to the *CWP_12_deployment_folder*/deploy/kube/init/aws folder.
2. Type `./create-cluster [-public] [-private] -admin|-a kubernetes_admin`

   where:

   - *-public* - Is specified if the respective VPC has public subnet.
   - *-private* - Is specified if the respective VPC has private subnet. This also enables *-public*.
   - *kubernetes_admin* - Defines the Kubernetes administrator account that manages the Kubernetes cluster. You can define any valid account name. The default value is *kube-admin*.

   For example,

   - To create an EKS cluster with a VPC that has both public and private subnets, type `./create-cluster -private`

- To create a VPC with only public subnets, type `./create-cluster -public`

Results

AWS EKS automatically creates an Elastic Load Balancing (ELB) for a *LoadBalancer* type service.

An AWS Network Load Balancer at layer 4 of the OSI model load balances the network traffic.

you can use an Ingress controller instead of an external load balancer. This guide does not document the use of an ingress controller.

Customize the Kubernetes environment for SDCT

Perform the follow steps to customize the Kubernetes environment.

Preparing Certificates to install SDCT

SDCT requires TLS certificates to secure communications.

About this task

Perform the following steps on the Kubernetes Administration Terminal.

Procedure

1. Copy the CTAPI TLS certificates (PKCS12) into the *`CWP_12_deployment_folder`*`/cwp/certs` folder, and then rename the certificate file to `tls.pfx`.

   Note: The deployment script will extract values for *`tls.crt`* and *`tls.key`* from the certificate.
2. Copy the Kafka TLS certificate (PKCS12) into the *`CWP_12_deployment_folder`*`/cwp/certs` folder, and then rename the Kafka certificate file to `kafka-tls.pfx`.

Results

When you run the *./init-crypto* script, you are prompted to specify the TLS certificate password.

Setting the Environment Variables in the .env File

Nymi-supplied scripts create the environment based on variables that you define in the *.env* file.

About this task

The *.env* contains environment variables that are common to all environments. The file *.env* includes the credentials and IP addresses of the domain, NES, and the Contact Tracing Dashboard. Refer to the SDCT Variables table for the values that you recorded during the SQL database and domain setup.

Procedure

1. On the Kubernetes Administration Terminal, in Windows Explorer, navigate to *`CWP_12_deployment_folder`*`\deploy\kube` folder.
2. Edit the *.env* file and configure the values to match your environment.

   The following table summarizes the general configuration variables.

Variable	Description
CWP_COMPONENTS	Specifies the list of CWP components to deploy. The default value is =(zookeeper broker ctapi ctprocessor cwpweb kafka-connect)
NES_USER_API_BASE_URL	Specifies the URL that an NES Administrator uses to access the `NES Administrator Console` in a web browser. Specify the value in the format `https://nes_ip_address/service_name`. You can also find these values by running the NES installer on the NES server, and then selecting the **`Review Settings`** tab. For example: =https://10.0.4.167/nes
CORP_LDAP_PROTOCOL	Specifies the LDAP protocol that used in the domain, `ldap` or `ldaps`.
CORP_LDAP_PORT	Specifies the port on which Kubernetes uses to connect to the domain. Type `389` for LDAP or `636` for LDAPS.
CORP_LDAP_DC	Specifies the IP address of the Active Directory domain controller.
CORP_LDAP_BASEDN	Specifies the base Distinguished Name (DN) to use to search LDAP. The first DC should be the Active Directory domain (ie. ***`CORP_LDAP_DOMAIN`***. For example: ="DC=qa-lab,DC=local"
CORP_LDAP_API_GROUP	Specifies the LDAP group that has access to AWS. The default value is Domain Users, which you can change if necessary.
CORP_LDAP_DASHBOARD_GROUP	Specifies the LDAP group that contains users that require administrator access to the `Contact Tracing Dashboard`.

Variable	Description
CORP_LDAP_ATTESTATION_ADMIN_GROUPS	Specifies the name of the Health and Safety AD group. Use commas to separate multiple group names. **Note:** Users in this group have administrator access to the Health Check Application.
CORP_LDAP_DOMAIN	Specifies FDQN of the Active Directory domain in which NES resides. For example: `=qa-lab.local`
CORP_LDAP_USER	Specifies the service account, which is an Active Directory domain account that is a member of the NES administrator group. For example: `=adeed`
CORP_LDAP_USERDN	Specifies the DN of the ***CORP_LDAP_USER*** that is used by LDAP. The format should consist of the name of an object and the LDAP designator. For example: `="CN=adeed,CN=Users,DC=qa-lab,DC=local"`
CORP_LDAP_PASSWORD	Specifies password of the service account. Do not type a value for this variable. The *init-crypto* command will encrypt the password and update the file with the appropriate value.
NODE_TLS_REJECT_UNAUTHORIZED	This value is dependent on the NES certificate trust. If this value is `0` certificate validation is disabled for TLS connections. Nymi recommends that you specify a value of 1.

The following table provides information on the configuration parameters that are specific to Kafka. Modify values if your configuration uses values that differ from the default.

Variable	Description
KAFKA_BROKER_PUBLIC_DOMAIN	Required. Specfies the public domain for the Kubernetes cluster, to allow machines that are on a

Variable	Description
	different domain from the Kubernetes cluster, access to the Kubernetes cluster. You can obtain this value from the SDCT Environment Variables
KAFKA_BROKER_EXTERNAL_PORT	Specifies the Kafka broker listener port for external client. The default value is `=9092`
KAFKA_BROKER_INTERNAL_PORT	Specifies the Kafka broker listener port for internal client. The default value is `=29092`
KAFKA_BROKER_INTER_BROKER_PORT	Specifies the Kafka broker listener port between broker instances. The default value is `=9095`
KAFKA_BROKER_BOOTSTRAP_NODE_PORT	Specifies the node port on which the kafka broker bootstrap service connects to the external load balancer. The default value is `30090` .
KAFKA_LISTENER_SECURITY_PROTOCOL_INTERNAL	Specifies the Kafka broker listener protocol in the Kubernetes cluster. The default value is `=SSL`
KAFKA_LISTENER_SECURITY_PROTOCOL_EXTERNAL	Specifies the Kafka broker listener protocol outside the kubernetes cluster. The default value is `=SASL_SSL` .
KAFKA_LISTENER_SECURITY_PROTOCOL_INTER_BROKER	Specifies the Kafka broker listener protocol between the broker instances. The default value is `=SSL` .
KAFKA_SSL_KEYSTORE_PASSWORD	Specifies the Kafka broker TLS certificate keystore password. Do not type a value for this variable. The

Variable	Description
	init-crypto command will encrypt the password and update the file with the appropriate value.
KAFKA_SASL_ADMIN_PASSWORD	Specifies the Kafka SASL admin password. Do not type a value for this variable. The *init-crypto* command will encrypt the password and update the file with the appropriate value.
KAFKA_SASL_CTPROCESSOR_PASSWORD	Specifies the CT Processor password. Do not type a value for this variable. The *init-crypto* command will encrypt the password and update the file with the appropriate value.
KAFKA_SASL_CTCA_PASSWORD	Specifies the `Nymi Edge Agent` password. Do not type a value for this variable. The *init-crypto* command will encrypt the password and update the file with the appropriate value.
KAFKA_BROKER_BOOTSTRAP_NODE_PORT	Bootstrap node port. The default value is `30090` .
KAFKA_SSL_ENABLED_PROTOCOLS	Comma separated list of secure protocols. The default value is `TLSv1.3,TLSv1.2` .
KAFKA_SSL_CIPHER_SUITES	Lists the cipher suites. Leave the default value `"TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,` `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,` `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,` `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,` `TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,` `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_DH` `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256"`
KAFKA_CONNECT_CPU_REQUESTS	CPU request for Kafka-connect.
KAFKA_CONNECT_MEMORY_REQUESTS	Defines the memory request for Kafka-connect.

Variable	Description
KAFKA_CONNECT_CPU_LIMITS	Defines the CPU limits for Kafka-connect.
KAFKA_CONNECT_MEMORY_LIMITS	Defines the memory request for Kafka-connect.

The following table provides information about the variables that you defined when you configured the `CWP Database`. Use the *SDCT Variables* table to obtain the values that are specific to your environment.

Variable	Description
CT_DB_HOST	Specifies the IP address of the machine that is hosting the CWP Database. For example: `=10.0.4.102`
CT_DB_PORT	Specifies the port for the SQL database. The default value is `=1433`
CT_DB_INSTANCE	Specifies name of the SQL instance, on which you created the `CWP Database`. For example: `=SQLEXPRESS`
CT_DB_CATALOG	Specifies the location of the `ContactTracing` catalogue, where various schema and mappings are kept in an SQL environment. This value is the name that you specified for the `CWP Database`. For example: `=ContactTracing`
CT_DB_SCHEMA	The SQL server schema for the `CWP Database`. If this is not particularly defined, use the default, `dbo`. `=dbo`
CT_DB_USERNAME	Specifies the SQL username to use to log into the `CWP Database`.

Variable	Description
	For example: `=ct_sa`
CT_DB_PASSWORD	Specifies password of the SQL database user. The init-crypto script prompts you for this password and then encrypts the password. It is not necessary to type the password.
TLS_CA_CERT	Specifies the location of the TLS signing CA certificate.
TLS_SKIP_CERTIFICATE_VALIDATION	Determines if the script should skip Certificate verification. Acceptable values are True or False.
CWPWEB_PORT	Specifes the port on which the Health Check Application connects to the CWP Database. The default value is 443.

Results

The environment variables defined in these file provides values to the ConfigMaps that are used by the CWP components. ConfigMaps are defined in *kube/cwp/base.in/config.yml* folder.

Setting the Envrionment Variables in the .prod-env

Nymi-supplied scripts create the environment based on variables that you define in the *.prod-env* file.

About this task

The *.prod-env* contains environment variables that are customer environment-specific.

Procedure

1. On the Kubernetes Administration Terminal, in Windows Explorer, navigate to *`CWP_12_deployment_folder`\deploy\kube* folder.
2. Edit the *.prod-env* file and configure the values to match your environment.

   The following table summarizes the general configuration variables.

Variable	Description
CWP_NAMESPACE	Defines the global namespace. Leave the default value cwp.
CWP_ENV	Defines the global namespace. Leave the default value production.
DOCKER_HUB_ENV_SUFFIX	Specifies the docker hub repositories where images for the respective environment are stored. Leave this variable undefined.

Variable	Description
KAFKA_BROKER_SERVER	Defines the internal port on which Kafka connects to the boostrap server. Leave the default value `broker.${CWP_NAMESPACE}.svc.cluster.local: ${KAFKA_BROKER_INTERNAL_PORT}` **Note:** The *KAFKA_BROKER_INTERNAL_PORT* is defined in the *.env* file.

ZOOKEEPER_SERVERS	Defines the Zookeeper servers in the Kubernetes cluster. Leave the default value
	`"zookeeper-0.zookeeper. ${CWP_NAMESPACE}.svc.cluster.local:2888:3888;`
	`zookeeper-1.zookeeper.${CWP_NAMESPACE}`
	`.svc.cluster.local:2888:3888;zookeeper-2.zookeeper. ${CWP_NAMESPACE}.svc.cluster.local:2888:3888"`

ZOOKEEPER_REPLICAS	Specifies the number of initial Zookeeper replicas. The default value is 3.
KAFKA_REPLICAS	Specifies the number of initial Kafka replicas. The default value is 3.
VERNE_REPLICAS	Specifies the number of initial Verne replicas. The default value is 3.
WEB_REPLICAS	Specifies the number of initial Web replicas. The default value is 1.
CT_REPLICAS	Specifies the number of initial CT replicas. The default value is 3.
ZOOKEEPER_MAX_REPLICAS	Specifies the maximum number of initial Zookeeper replicas. The default value is 6.
KAFKA_MAX_REPLICAS	Specifies the maximum number of initial Kafka replicas. The default value is 9.
VERNE_MAX_REPLICAS	Specifies the maximum number of initial Verne replicas. The default value is 9.
WEB_MAX_REPLICAS	Specifies the maximum number of initial Web replicas. The default value is 9.
CT_MAX_REPLICAS	Specifies the maximum number of initial CT replicas. The default value is 9.

Variable	Description
ZOOKEEPER_MIN_AVAILABLE	Defines the minimum number of Zoopkeeper replicas to always have available. The default value is `$(($ZOOKEEPER_REPLICAS/2 + 1))` .
KAFKA_MIN_AVAILABLE	Defines the minimum number of Zoopkeeper replicas to always have available. The default value is `$(($KAFKA_REPLICAS/2 + 1))` .
VERNE_MIN_AVAILABLE	Defines the minimum number of Verne replicas to always have available. The default value is `$(($VERNE_REPLICAS/2 + 1))` .
WEB_MIN_AVAILABLE	Specfies the minimum number of Web replicas to always have available. The default value is 1.
CT_MIN_AVAILABLE	Specifies the minimum number of CT replicas to always have available. The default value is 1.
ZOOKEEPER_DATA_SIZE	Specifies the persistent volume size for Zookeeper data. The default values is `8Gi` .
KAFKA_DATA_SIZE	Specifies the persistent volume size for Kafka data. The default values is `32Gi` .
VERNE_DATA_SIZE	Specifies the persistent volume size for Verne data. The default values is `8Gi` .
PV_RECLAIM_POLICY	Specifies the persistent volume policy to reclaim disk space. Supported values are Delete, Retain or Recycle. The default value is `Delete`

Variable	Description
	Note: Most systems do not support Recycle.
KAFKA_LOG_RETENTION_HOURS	Specifies the number of hours to retain the Kafka log file entries. The default value is `1` .
KAFKA_TOPIC_MULTIPLIER	The default value is `3` .
KAFKA_REPLICATION_FACTOR	The default value is `3` .
KAFKA_MIN_REPLICATION_FACTOR	The default value is `1` .
KAFKA_DEFAULT_PARTITIONS	The default value is `$((KAFKA_TOPIC_MULTIPLIER*KAFKA_REPLICAS))` .

The following table summarizes variables that control the resource requests and limits.

Variable	Description
ZOOKEEPER_CPU_REQUESTS	Specifies the amount of CPU initially requested by Zookeeper in milliCPUs. The default value is `100m` .
ZOOKEEPER_MEMORY_REQUESTS	Specifies the amount of memory initially requested by Zookeeper in mebibytes. The default value is `512Mi` .

Variable	Description
ZOOKEEPER_CPU_LIMITS	Specifies the maximum amount of CPU that Zookeeper can request in milliCPUs. The default value is `200m` .
ZOOKEEPER_MEMORY_LIMITS	Specifies the maximum amount of memory that Zookeeper can request in mebibytes. The default value is `1024Mi` .
ZOOKEEPER_BROKER_CPU_REQUESTS	Specifies the amount of CPU initially requested by the Zookeeper Broker in milliCPUs. The default value is `1000m` .
ZOOKEEPER_BROKER_MEMORY_REQUESTS	Specifies the amount of memory initially requested by the Zookeeper Broker in mebibytes. The default value is `1024Mi` .
ZOOKEEPER_BROKER_CPU_LIMITS	Specifies the maximum amount of CPU that the Zookeeper Broker can request in milliCPUs. The default value is `2000m` .
ZOOKEEPER_BROKER_MEMORY_LIMITS	Specifies the maximum amount of memory that the Zookeeper Broker can request in mebibytes. The default value is `4096Mi` .
VERNE_CPU_REQUESTS	Specifies the amount of CPU initially requested by Verne in milliCPUs. The default value is `1000m`

Variable	Description
	.
VERNE_MEMORY_REQUESTS	Specifies the amount of memory initially requested by Verne in mebibytes. The default value is `1024Mi` .
VERNE_CPU_LIMITS	Specifies the maximum amount of CPU that Verne can request in milliCPUs. The default value is `2000m` .
VERNE_MEMORY_LIMITS	Specifies the maximum amount of memory that the Verne can request in mebibytes. The default value is `4096Mi` .
CTPROCESSOR_CPU_REQUESTS	Specifies the amount of CPU initially requested by the CTProcessor in milliCPUs. The default value is `200m` .
CTPROCESSOR_MEMORY_REQUESTS	Specifies the amount of memory initially requested by CTProcessor in mebibytes. The default value is `2564Mi` .
CTPROCESSOR_CPU_LIMITS	Specifies the maximum amount of CPU that CTProcessor can request in milliCPUs. The default value is `1500m` .
CTPROCESSOR_MEMORY_LIMITS	Specifies the maximum amount of memory that the CTProcessor can request in mebibytes. The default value is `1024Mi` .

Variable	Description
KAFKA_CONNECT_CPU_REQUESTS	Specifies the amount of CPU initially requested by Kafka Connect in milliCPUs. The default value is `100m` .
KAFKA_CONNECT_MEMORY_REQUESTS	Specifies the amount of memory initially requested by Kafka Connect in mebibytes. The default value is `2564Mi` .
KAFKA_CONNECT_CPU_LIMITS	Specifies the maximum amount of CPU that Kafka Connect can request in milliCPUs. The default value is `1000m` .
KAFKA_CONNECT_MEMORY_LIMITS	Specifies the maximum amount of memory that the Kafka Connect can request in mebibytes. The default value is `512Mi` .
CTAPI_CPU_REQUESTS	Specifies the amount of CPU initially requested by `CTAPI` in milliCPUs. The default value is `100m` .
CTAPI_MEMORY_REQUESTS	Specifies the amount of memory initially requested by `CTAPI` in mebibytes. The default value is `245Mi` .
CTAPI_CPU_LIMITS	Specifies the maximum amount of CPU that `CTAPI` can request in milliCPUs. The default value is `1000m` .

Variable	Description
CTAPI_MEMORY_LIMITS	Specifies the maximum amount of memory that the `CTAPI` can request in mebibytes. The default value is `2048Mi` .
CWPWEB_CPU_REQUESTS	Specifies the amount of CPU initially requested by CWWeb in milliCPUs. The default value is `200m` .
CWPWEB_MEMORY_REQUESTS	Specifies the amount of memory initially requested by CWWweb in mebibytes. The default value is `512Mi` .
CWPWEB_CPU_LIMITS	Specifies the maximum amount of CPU that CWWeb can request in milliCPUs. The default value is `1000m` .
CWPWEB_MEMORY_LIMITS	Specifies the maximum amount of memory that the CWWeb can request in mebibytes. The default value is `2048Mi` .

3. Save the file.

What to do next

The logging environment variables are described in the *Troubleshooting* chapter.

Encrypting the Passwords for Kubernetes Components

An RSA key pair protects the password of the Active Directory account that is used as a `Connected Worker Platform` service account. The password is encrypted using the public key and is stored in the *env* file. The private key is passed to the CWP containers for decrypting the password.

About this task

This section describes the instructions to harden the passwords that are contained in the *env* file and accessed during installation of the Kubernetes components.

Note: Run the *./init-crypto* script, before you run the `./cwp env_name up` command.

Ensure that you only run the init-crypto script once, unless the .env and certs directory is overridden.

Procedure

1. On the Kubernetes Administration Terminal, open a **bash** terminal, and then change to the *../deploy/kube* directory.
2. Type `./init-crypto env_name`.
3. When prompted, specify the password for each Kubernetes component.

   The script encrypts the following passwords and stores them in the `conkeyref="prod_names/cwp_deploy"`*/deploy/kube/.env* environment variable file:

   - `CORP_LDAP_PASSWORD` - Password used to log into the NES Administrator Console.
   - `KAFKA_SSL_KEYSTORE_PASSWORD` - Kafka broker TLS certificate keystore password.
   - `KAFKA_SASL_ADMIN_PASSWORD` - Kafka SASL admin password.
   - `KAFKA_SASL_CTPROCESSOR_PASSWORD` - Kafka password for the CT Processor.
   - `KAFKA_SASL_CTCA_PASSWORD` - Kafka password for the `Nymi Edge Agent`.

Launching the Kubernetes Environment

Before you begin

Ensure that the extracted CWP installation package has been copied to the Kubernetes Administration Terminal.

About this task

The instructions in this section enables you to launch the Kubernetes environment with 3 nodes.

Procedure

1. On the Kubernetes Administration Terminal, open a **bash** terminal, and then change to `CWP_12_deployment_folder`*/deploy/kube* folder.
2. Initialize the client by typing one of the following commands:
   - For bare-metal deployments, type `./init-client -m user@master-node`

     Where:

     - `master-node` is the address of the initial master node
     - `user` is a user on the node.
   - For AWS deployments, type `./init-client -a aws-region -c cluster name`

     Where:

     - `aws-region` is the AWS region where the cluster resides, and
     - `cluster name` is the name of the EKS cluster
3. Update the environment by typing `./cwp update prod update`
4. Launch the environment by typing `./cwp prod up`.

Creating a Backup of the Data Folders

After you launch the `Connected Worker Platform` platform and terminate the respective containers, ensure that you save the contents of the following data folders under the host(s):

- *runtime/kafka/data/kafka*.
- *runtime/zookeeper/data/Zookeeper*.

Upgrading Connected Worker Platform

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

- You can upgrade the Nymi Components (NES, `Nymi Band Application`, `Nymi Runtime`, and Nymi Band firmware) in any order.
- You can upgrade NES, `Nymi Band Application`, and `Nymi Runtime` directly from NEE 3.2.1, 3.3.x and CWP 1.2.1.
- CWP 1.3 NES supports the CWP 1.2.1 and Nymi Enterprise Edition 3.3.x `Nymi Band Application`.
- When you upgrade the Nymi Band Application, you must also upgrade NES before performing any enrollments.
- You can use a Nymi Band 3.0 with CWP 1.3 firmware only on user terminals that use the `Nymi Runtime` that is included with CWP 1.3.
- You cannot use a Nymi Band 2.0 in a CWP 1. 3 infrastructure.
- You can use a Nymi Band 3.0 with NEE 3.2.1, NEE 3.3.0 or CWP 1.2.1 firmware in CWP 1.3 environment; however, new functionality introduced in an NEE or CWP version that is newer than the firmware is not available.
- You cannot use a Nymi Band 3.0 with CWP 1.3 firmware in a NEE 2.6.1, NEE .3.2.1 or NEE 3.3.x environment.
- When you upgrade from NEE 3.3.x and earlier, you must re-enroll the Nymi Band.

Upgrading NES

You can upgrade earlier versions of NES to the current version of NES. To upgrade a NES implementation that uses ADCS/NDES to manage certificates, you must refer to the Nymi Connected Worker Platform Migration Guide for detailed information on migrating to the Nymi Token Service (NTS) for NES certificate issuance method.

About this task

`Nymi Token Service` (NTS) issues authentication tokens to NEAs that allow the NEAs, including the `Nymi Band Application`, to authenticate to Nymi Bands that are enrolled in the enterprise. NTS provides you with a simplified, secure deployment that does not require ADCS/NDES user accounts and reliance on specific user account permission requirements in AD security policies.

To upgrade a previous version of NES that uses NTS, perform the following steps:

Note: For upgrades from NES 2.X, Microsoft .NET framework will be upgraded to Microsoft .NET Framework 4.8.

Procedure

1. Extract the NES installation package to a local directory on the NES host.

2. From the directory that contains the extracted NES installation package, run ..*NesInstaller* *install.exe*.
3. On the `User Access Control` window, click **`Yes`**.
4. On the `Open File - Security warning` window, click **`Run`**.
5. If applicable, on the `User Access Control` page, review the Microsoft .NET EULA, and then click **`Accept`**. Complete the .NET installation and continue with the NES installation.
6. On the `Application Install Security Warning` window, click **`Install`**.
7. On the `Open File - Security warning` window, click **`Run`**.
8. On the left navigation pane, click **`Location`**, and then perform the following steps.
   a) In the **`Install Root`** field, confirm that the path to the NES services is correct, as it was specified during the initial deployment.

      The default location is *C:\inetpub\wwwroot*.
   b) In the **`Instance Name`** field, type the descriptive name that was specified during the initial deployment for the NES web application instance name. For example, NES. See Configuration Attribute Values in the Nymi Connected Worker Platform NES Deployment Guide.

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

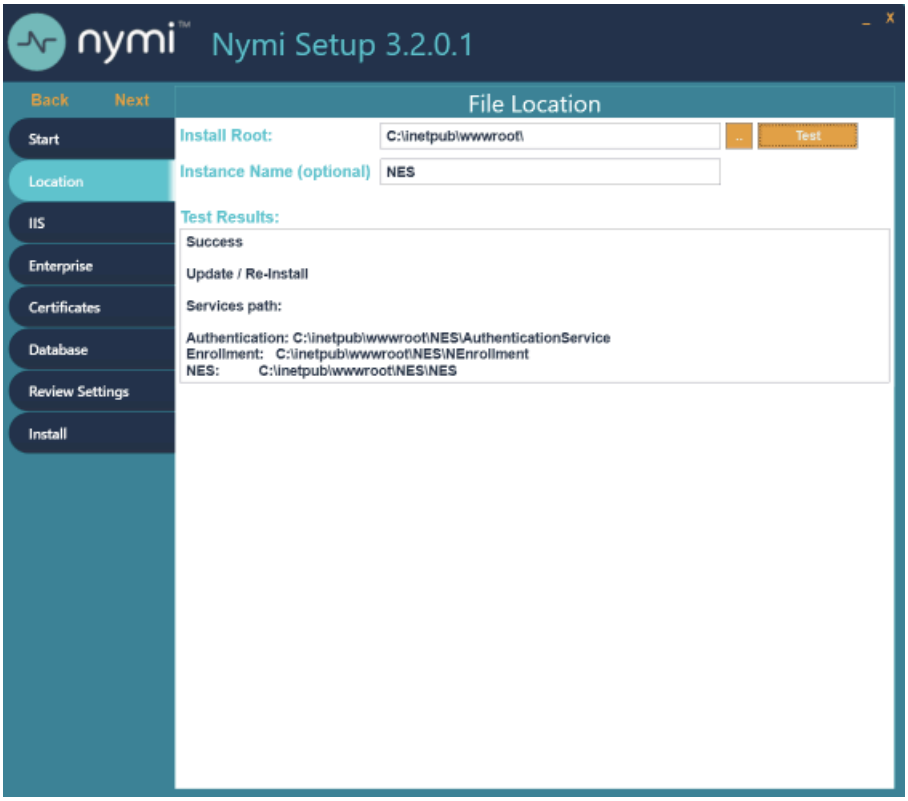


Figure 44: Update / Reinstall installation type

9. On the left navigation pane, click **Install**.
10. Click **Update**.

    Note: If the update option is not available, the **Install Root** or **Instance Name** fields on the **Location** tab are not the same values that were specified when you deployed the previous NES version.
11. On the Level Two certificate warning window, click **OK**.
12. On the Update NES window, click **Yes** to reapply the configuration.
    The Install window display the status of the upgrade process.
13. When the Install window displays the Installation Complete message, close the Nymi Setup window.

Upgrading the Enrollment Terminal

Upgrade the Nymi Band Application on each enrollment terminal in the environment.

Upgrading the Nymi Band application

Upgrades from a previous version are supported.

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

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

Performing a silent Nymi Band Application Installation or Upgrade

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

About this task

Procedure

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

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

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

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

Performing a Nymi Band application upgrade by using the installation wizard

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

About this task

Procedure

1. Download the Nymi Band Application software to a directory on the network terminal. For example, *C:\Downloads*
2. Double-click the installation file *Nymi-Band-App-installer-v_`version`*, and then follow the prompts to update the software.

Upgrading User Terminals and Centralized Nymi Agent

Upgrade the `Nymi Runtime`software on user terminals that use the Nymi Band to perform authentication tasks. In Citrix/RDP environments, update the `Nymi Runtime`software on server that acts as the centralized `Nymi Agent`. In environments that use the Smart Distancing and Contact

Tracing or the Temperature Alert feature, install `Nymi Edge Agent` on the user terminals in your environment that are on the same domain as NES.

Upgrading the Nymi Runtime

Upgrades from a previous version are supported.

You are not required to remove the previous version before installing the newer version. You can upgrade the `Nymi Runtime` by using the installation wizard or silently from a command prompt. In Citrix/RDP

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.

About this task

Procedure

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

Performing a silent installation or upgrade of Nymi Runtime

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

About this task

Procedure

1. Log in to the network terminal with an account that has administrator privileges.
2. Extract the Nymi API distribution package.

3. Launch the command prompt as administrator.
4. Change to the ..*nymi-sdk**windows**runtime* folder, and then type: "Nymi Runtime *Installer version.exe" /exenoui /q*

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

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

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

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

What to do next

The silent installation process creates an installation log file in the *%temp%* directory named Nymi Runtime_*version_time.log*

Installing NBE on an HP Thin Pro

Follow the instructions below to manually install `Nymi Bluetooth Endpoint` manually. Retrieve the installation file *nbed_x.y.z_amd64.deb* from Nymi.

About this task

Retrieve the installation file *nbed_x.y.z_amd64.deb* from Nymi.

Procedure

1. Switch your user mode to **`Administrator`** from the system menu, or log in by entering an the credentials of a person in the domain admin group.
   a) Right-click the desktop or click **`Start`**.
   b) Click **`Switch to Administrator`** from the menu. You will be prompted to enter the administrator password.

   The screen is surrounded by a red border when in administrator mode.
2. Extract the file, *nbed_x.x.z_amd64.deb*, from the Nymi distribution package and save it to the machine. Where *x.y.z* is the version of the file. Note the file path.
3. Unlock read/write access with **`X Terminal`**.
   a) Click **`Start`** and go to **`Tools`**.
   b) Click **`X Terminal`**.
   c) Type `fsunlock`
4. In **`X Terminal`** change the directory to the file location of *nbed-cron_x.y.z_amd64.deb* and install the extracted file.

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

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

5. Reboot the client.

Update Smart Distancing and Contact Tracing

Review this section to determine how to update the user terminals and Kubernetes environment when there is a new CWP release.

Update the User Terminal

On each user terminal, you must upgrade the Nymi Runtime, remove the current version of `Nymi Edge Agent`, and then install the new `Nymi Edge Agent` version.

Note: The Nymi Connected Worker Platform NES Deployment Guide describes how to update the Nymi Runtime.

Install Nymi Edge Agent and Nymi-Based Applications

Install the `Nymi Edge Agent` and the `Nymi Runtime` software on User Terminals or the RDP session host / Citrix server in the environment to collect information from Nymi Bands.

The installation process differs for local and RDP/Citrix configurations:

- In a local configuration, install `Nymi Edge Agent` and the `Nymi Runtime` application on each thick client user terminal. The Nymi Connected Worker Platform Administration Guide provides detailed information about how to install `Nymi Runtime`.
- In a remote configuration install:
  - `Nymi Edge Agent` on a RDP session host or Citrix server, which installs the Edge Agent service. When a user logs into a remote session, one EdgeAgentsLauncher process and one EdgeAgents process start for each user session.
  - `Nymi Bluetooth Endpoint` application on each thin client user terminal.
  - `Nymi Agent` application on any server in the environment.

  The Nymi Connected Worker Platform NES Deployment Guide provides detailed information about how to install and configure the `Nymi Bluetooth Endpoint` and the `Nymi Agent` application for configurations that use RDP or Citrix.

Installing the Nymi Edge Agent Application on the RDP session host / Citrix server

Install `Nymi Edge Agent` on the RDP session host / Citrix server in your environment that is on the same domain as NES.

Before you begin

- Install the latest version of OpenSSL for Windows and add the *bin* directory is included in the system path.
- The `Nymi Edge Agent` package has been extracted to a central location.
- If an untrusted root CA issues the NES certificate, you must import the root CA certificate for the untrusted root. *Importing the Root CA certificate* provides more information.

About this task

Perform the following steps on the RDP session host / Citrix server:

Procedure

1. Copy the extracted *edgeagents* folder to the RDP session host / Citrix server.

   The folder contains the following files:

   - *decrypt.key* file, which is used to decrypt the SASL and NES usernames and passwords.
   - *edgeagents-service-x64-`version`.msi* file, which installs the `Nymi Edge Agent` software on a thick client user terminal and uses the parameters detailed in the *edge_agents.conf* file.
   - *edgeagents-terminal-service-x64-`version`.msi* file, which installs the `Nymi Edge Agent` software on a RDP sessions host/Citrix server and uses the parameters detailed in the *edge_agents.conf* file.
   - *secretutil.cmd* file, which is Windows command utility that encrypts secrets.
   - *edge_agents.conf* file, which used to configure the parameters of the `Nymi Edge Agent` installation, and includes keys generated from the PowerShell utility.
   - *KafkaCA.pem* file, which is a default client truststore certificate.
2. Perform the following steps to generate the secret keys by using the *secretutil.cmd* file.
   a) Click the **`Start`** menu and type `cmd`. Right-click **`Command Prompt`** and click **`Run as administrator`**.
   b) Change the directory that contains the extracted `Nymi Edge Agent` installation package. For example, the *C:\edgeagents* folder.
   c) Initialize *secretutil.cmd* with the following command:

   ```
   secretutil.cmd -init
   ```

   d) Use the *secretutil.cmd* command to encrypt the sasl username and password.

      1. By default, the username is ctca. Type the following command to encrypt the username in an output file.

      ```
      secretutil.cmd -enc ctca>OUTPUT FILE NAME.txt
      ```

      where *`OUTPUT FILE NAME.txt`* is the name of the file that contains the encrypted username.
      2. Type the following command to encrypt the SASL password.

      ```
      secretutil.cmd -enc PASSWORD>OUTPUT FILE NAME 2.txt
      ```

      where *`PASSWORD`* is the password specified by the person who implemented the server side components when they ran the *init-crypto* command and *`OUTPUT FILE NAME 2.txt`* is the name of the file that contains the encrypted password.

   The output files contain the secret keys used in the *edge_agents.conf* file.
3. Perform the following steps to update the *edge_agents.conf* file with the secret keys that you created in the previous step.
   a) Open the *edge_agents.conf* file with a text editor.

b) Update the value for the key sasl.username. It is the encrypted value in the username output text file.

```
sasl.username=[encrypted username]
```

c) Update the value for the key sasl.password. It is encrypted value in the password output text file.

```
sasl.password=[encrypted password]
```

4. Save the *edge_agents.conf* file.
5. For Kafka TLS certificates that are issued from an untrusted CA only, perform the following steps to install the Kafka Truststore.
   a) Obtain the Kafka Broker root CA certificate from the person who implemented the CWP cluster. The file is stored in the CWP deployment package, in the *cwp/certs* folder.
   b) If required, rename the Kafka Broker root CA cert to *KafkaCA.pem*.
   c) Backup the *KafkaCA.pem* certificate in the `Nymi Edge Agent` installation directory.
   d) Replace the default *KafkaCA.pem* file in the `Nymi Edge Agent` installation package directory with the new *KafkaCA.pem* certificate file that you obtained from the implementation engineer.
6. Open the *edge_agents.conf*, and ensure that the value defined in the *`sasl.ca.path`* key is *C:\Nymi\Edge_Agents\certs\KafkaCA.pem*.
7. Uncomment the line *`launcher.mode = 1`*.
8. Edit the following configuration parameters in the *edge_agents.conf* file.

   Producer Specific Properties:

   - *`bootstrap.servers`*, which defines a list of host and port pairs of Kafka brokers.

   NES Specific Properties:

   - *`nes.url`*, which specifies the NES URL.
   - *`agent.url`*, which specifies the `Nymi Agent` URL. When you do not specify a value, `Nymi Edge Agent` will pick up the local `Nymi Agent` URL.
9. Save the *edge_agents.conf* file.

   Note: Ensure the *edge_agents.conf* file is configured prior to installing *edge_agents.msi*. This configuration file can then be copied to different machines being installed with `Nymi Edge Agent`.
10. Run the installer file *edgeagents-terminal-services-x64-`version`.msi*.
    The `Nymi Edge Agent` application is installed in the *C:\Nymi\Edge_Agents* folder and an `Nymi Edge Agent` service starts. Each time a user logs in to a Citrix or RDP session, an `Nymi Edge Agent Launcher` process starts and the `Nymi Edge Agent` service starts an `Nymi Edge Agent` process.

    Note: In `Task Manager`, the `Nymi Edge Agent Launcher` process appears as `Nymi Edge Agent` in the list of processes.

    When the user session ends, the additional `Nymi Edge Agent` and `Nymi Edge Agent Launcher` processes terminate.

    Note: The section *Nymi Edge Agent Log Files* provides information about `Nymi Edge Agent` log files.

Installing the Nymi Edge Agent Application in a Local Configuration

Install Nymi Edge Agent on the user terminals in your environment that are on the same domain as NES.

Before you begin

- Install the latest version of OpenSSL for Windows and add the *bin* directory is included in the system path.
- The Nymi Edge Agent package has been extracted to a central location.

About this task

Perform the following steps on each user terminal:

Procedure

1. Copy the extracted *edgeagents* folder to the user terminal.

   The folder contains the following files:

   - *decrypt.key* file, which is used to decrypt the SASL and NES usernames and passwords.
   - *edgeagents-service-x64-*`version`*.msi* file, which installs the `Nymi Edge Agent` software on a thick client user terminal and uses the parameters detailed in the *edge_agents.conf* file.
   - *edgeagents-terminal-service-x64-*`version`*.msi* file, which installs the `Nymi Edge Agent` software on a RDP sessions host/Citrix server and uses the parameters detailed in the *edge_agents.conf* file.
   - *secretutil.cmd* file, which is Windows command utility that encrypts secrets.
   - *edge_agents.conf* file, which used to configure the parameters of the `Nymi Edge Agent` installation, and includes keys generated from the PowerShell utility.
   - *KafkaCA.pem* file, which is a default client truststore certificate.
2. Perform the following steps to generate the secret keys by using the *secretutil.cmd* file.
   a) Click the **`Start`** menu and type `cmd`. Right-click **`Command Prompt`** and click **`Run as administrator`**.
   b) Change the directory that contains the extracted `Nymi Edge Agent` installation package. For example, the *C:\edgeagents* folder.
   c) Initialize *secretutil.cmd* with the following command:

   ```
   secretutil.cmd -init
   ```

   d) Use the *secretutil.cmd* command to encrypt the sasl username and password.

      1. By default, the username is ctca. Type the following command to encrypt the username in an output file.

      ```
      secretutil.cmd -enc ctca>OUTPUT FILE NAME.txt
      ```

      where *`OUTPUT FILE NAME.txt`* is the name of the file that contains the encrypted username.

2. Type the following command to encrypt the SASL password.

```
secretutil.cmd -enc PASSWORD>OUTPUT FILE NAME 2.txt
```

where *PASSWORD* is the password specified by the person who implemented the server side components when they ran the *init-crypto* command and *OUTPUT FILE NAME 2.txt* is the name of the file that contains the encrypted password.

The output files contain the secret keys used in the *edge_agents.conf* file.

3. Perform the following steps to update the *edge_agents.conf* file with the secret keys that you created in the previous step.
   a) Open the *edge_agents.conf* file with a text editor.
   b) Update the value for the key sasl.username. It is the encrypted value in the username output text file.

```
sasl.username=[encrypted username]
```

   c) Update the value for the key sasl.password. It is encrypted value in the password output text file.

```
sasl.password=[encrypted password]
```

4. Save the *edge_agents.conf* file.
5. For Kafka TLS certificates that are issued from an untrusted CA only, perform the following steps to install the Kafka Truststore.
   a) Obtain the Kafka Broker root CA certificate from the person who implemented the CWP cluster. The file is stored in the CWP deployment package, in the *cwp/certs* folder.
   b) If required, rename the Kafka Broker root CA cert to *KafkaCA.pem*.
   c) Backup the *KafkaCA.pem* certificate in the `Nymi Edge Agent` installation directory.
   d) Replace the default *KafkaCA.pem* file in the `Nymi Edge Agent` installation package directory with the new *KafkaCA.pem* certificate file that you obtained from the implementation engineer.
6. Open the *edge_agents.conf*, and ensure that the value defined in the *sasl.ca.path* key is *C:\Nymi\Edge_Agents\certs\KafkaCA.pem*.
7. Edit the following configuration parameters in the *edge_agents.conf* file.

   Producer Specific Properties:

   - *bootstrap.servers*, which defines a list of host and port pairs of Kafka brokers.

   NES Specific Properties:

   - *nes.url*, which specifies the NES URL.
   - *agent.url*, which specifies the `Nymi Agent` URL. When you do not specify a value, `Nymi Edge Agent` will pick up the local `Nymi Agent` URL.
8. Save the *edge_agents.conf* file.

   Note: Ensure the *edge_agents.conf* file is configured prior to installing *edge_agents.msi*. This configuration file can then be copied to different machines being installed with `Nymi Edge Agent`.
9. Run the installer file *edgeagents-service-x64-version.msi*.

The Nymi Edge Agent application is installed without any user interactions in the *C:\Nymi \Edge_Agents* folder and the .Nymi Nymi Edge Agent service appears with a Running status in Windows Services.

Note: The section *Edge Agent Log Files* provides information about `Nymi Edge Agent` log files.

Update the CWP environment

Nymi provides you with scripts to update the CWP environment, including environment variables and services.

In CWP 1.2, some environment variable names have changed. The script renames the CWP 1.1 environment variable names to the new environment variable names. The following table provides a list of the CWP 1.1 environment variables names and the corresponding new variable name.

\

Note: When you update to CWP 1.2, existing contact events remain unchanged in the Contact Tracing Dashboard.

CWP 1.1	CWP 1.2	Purpose
NES_SAM_ACCOUNT_USER_DOMAIN	*CORP_LDAP_DOMAIN*	Specifies FDQN of the Active Directory domain in which NES resides. For example: =qa-lab.local
NES_SAM_ACCOUNT_USERNAME	*CORP_LDAP_USER*	Specifies the service account, which is an Active Directory domain account that is a member of the NES administrator group. For example: =adeed

CWP 1.1	CWP 1.2	Purpose
NES_SAM_ACCOUNT_PASSWORD	*CORP_LDAP_PASSWORD*	Specifies password of the service account. Do not type a value for this variable. The *init-crypto* command will encrypt the password and update the file with the appropriate value.

Updating the CWP in Kubernetes Environment

Nymi provides customers with an update package that updates the configuration and installs new services.

Before you begin

- Ensure that you copied the extracted CWP update package to the Kubernetes Administration Terminal.

  Note: The folder in which you extracted the CWP 1.2 update package is referred to as the CWP 1.2 deployment folder (*CWP_12_deployment_folder*).
- Ensure that you know the path to the CWP 1.1.x deployment folder, referred to as the *master deployment folder*. For example */cwpall*.

About this task

Perform the following steps from the Kubernetes Administration Terminal, in a **bash** terminal.

Procedure

1. Change to the *CWP_12_deployment_folder*/*deploy/kube/updates* folder, and then type `./update prod` *CWP_master_folder*.
   The update script revises the environment variables in the *master deployment folder* and creates a backup of the original deployment configuration files in *.cwp*.cwp folder in the home folder (~/) of the current user. The backup file/folder format is: *datetime-cwp-1.2-update*. Where *datetime* is in the format `time yyyymmdd.HHMM`. For example 10:35AM October 11 2021 will be: 20211011.1030.
2. Edit the *master deployment folder*/*deploy/kube/.env* file, and then specify values for the following environment variables:

Option	Description
CORP_LDAP_USERDN	Specifies the DN of the *CORP_LDAP_USER* that is used by LDAP.

Option	Description
	The format should consist of the name of an object and the LDAP designator. For example: `="CN=adeed,CN=Users,DC=qa-lab,DC=local"`
CORP_LDAP_ATTESTATION_ADMIN_GROUPS	Specifies the name of the Health and Safety AD group. Use commas to separate multiple group names. **Note:** Users in this group have administrator access to the Health Check Application.

3. Edit the *`master deployment folder`/deploy/kube/.prod-env* file, and then modify values for the following environment variables to match your environment, as appropriate:

Option	Description
KAFKA_CONNECT_CPU_REQUESTS	Specifies the amount of CPU initially requested by Kafka Connect in milliCPUs. The default value is `100m` .
KAFKA_CONNECT_MEMORY_REQUESTS	Specifies the amount of memory initially requested by Kafka Connect in mebibytes. The default value is `2564Mi` .
KAFKA_CONNECT_CPU_LIMITS	Specifies the maximum amount of CPU that Kafka Connect can request in milliCPUs. The default value is `1000m` .
KAFKA_CONNECT_MEMORY_LIMITS	Specifies the maximum amount of memory that the Kafka Connect can request in mebibytes. The default value is `512Mi` .

4. Change to the*`master deployment folder`*/*deploy/kube* folder, and then type `./cwp prod update`
   The new CWP services are deployed.

Update Nymi Band Firmware

Nymi provides you with a utility that enables you to update the firmware on one or multiple Nymi Bands. This utility is intended to be used in an unattended or batch mode, which simplifies the process of updating a large number of Nymi Bands. During the update process, the utility provides the operator with high-level status information about the process. The upgrade process generates a log file that details the Nymi Bands that were updated, including serial numbers and firmware versions.

Firmware Update Workflow

When you run the update utility, it determines if there are any Nymi Bands in the vicinity that are on charge and require an update. The firmware update utility only updates Nymi Bands with an older firmware.

If the utility detects a Nymi Band that requires a firmware update, the utility performs the following actions:

- Prepares to install the update. The Nymi Band screen displays **STAND BY**.
- Transfers the firmware to the Nymi Band. The Nymi Band screen displays **DOWNLOAD** with a progress bar.
- Restarts the Nymi Band and applies the firmware update to the Nymi Band. The Nymi Band screen displays messages about the update progress.
- The Nymi Band displays `SUCCESS` , for a brief period of time, after it is updated.
- When the utility completes a Nymi Band update, the utility scans for other Nymi Bands in the vicinity (within Bluetooth range) that require an update. If a Nymi Band is found, the update is started on another Nymi Band.
- The utility keeps running until terminated by the user.

  Note: If the Nymi Band uses recovery firmware, the messages that are displayed during a firmware update may be different than what is indicated above.

Before you perform a firmware update

Firmware update recommendations

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

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

Requirements for multiple Nymi Band update

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

Updating Nymi Band Firmware

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

About this task

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

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

Procedure

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

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

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

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

   As each Nymi Band firmware update completes, take the completed Nymi Band off charge and plug in another Nymi Band that requires updating. The firmware update utility continues to scan for Nymi Bands that require an update.
6. To stop the application, press `Ctrl+C`.
7. If required, restart the Nymi Bluetooth Endpoint service before using the Nymi Band Application or an application that uses `Nymi Runtime`.

Results

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

Firmware updater log files

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

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

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

Appendix 1 - Scripts

The following section provides information about the Nymi-provided CWP deployment scripts.

Environment Variables for Bare Metal Deployments

The `deploy/kube/init/bare/env` file contains the environment variables that are used during the Kubernetes deployment.

Important variables for bare-metal installation include:

- `K8S_VERSION`, which defines the Kubernetes version to install
- `CLUSTER_NAME`, which defines the name of the Kubernetes cluster

Details of the create-cluster Script

The **`create-cluster`** starts additional scripts during different stage of the deployment:

init-kube

The script that installs kubernetes and is invoked with **`sudo`**. The script supports the following options:

- `-c` - Installs a Kubernetes master node. When this option is excluded, the script installs a Kubernetes worker.
- `-d` - Installs and uses Docker for the container runtime instead of the default container runtime `containerd`.
- `-x` - Disables the Control Plane Node isolation mode. When you use this option, you cannot run pods on the control plane nodes

create-node

This script creates the initial Control Plane Master node in a new kubernetes cluster or join nodes to an existing Kubernetes cluster. It needs to be invoked with **`sudo`** and can take the following command line options:

- `-c` - Initialize kubernetes cluster on the initial master node
- `-s` - Joins a secondary master to a kubernetes cluster
- `-w` - Joins a worker node to a kubernetes cluster
- `-evAPI_server_fqdn` - Specifies the FQDN of the control-plane API Server endpoint. The default value is ***`kube-api-server`*** with IP address that is mapped to the first Control Plane Master node.

- `-t kubeadm_token` is cluster token for a node to join the cluster> This is required for secondary master nodes and worker nodes
- `-h hash` is cluster key hash for a node to join the cluster. This is required for secondary master nodes and worker nodes

Environment Variables For AWS

The *`deploy/kube/init/aws/env`* file contains the environment variables that are used for the installation.

The important variables for AWS include:

- *`CLUSTER_NAME`* - Name of the Kubernetes cluster.
- *`AWS_REGION`* - AWS region on which to install the EKS cluster.
- *`INSTANCE_TYPE`* - AWS EC2 instance type to use for EKS worker nodes.
- *`MIN_WORKER_NODES`*: - Auto-scaling parameter that defines minimal number of worker nodes in the cluster.
- *`DESIRED_WORKER_NODES`* - Auto-scaling parameter that defines the number of worker nodes in the cluster.
- *`MAX_WORKER_NODES`* - Auto-scaling parameter that defines the maximal number of worker nodes in the cluster
- *`ROOT_VOLUME_SIZE`* - Disk size of each node in Gigabyte

Nymi Inc. (Nymi) believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

The information in this document is provided as-is and Nymi makes no representations or warranties of any kind. This document does not provide you with any legal rights to any intellectual property in any Nymi product. You may copy and use this document for your referential purposes.

This software or hardware is developed for general use in a variety of industries and Nymi assumes no liability as a result of their use or application.Nymi, Nymi Band, and other trademarks are the property of Nymi Inc. Other trademarks may be the property of their respective owners.

Published in Canada.
Nymi Inc.
Toronto, Ontario
www.nymi.com