



Deployment Guide— Windows and Linux

Connected Worker Platform —Windows
and Linux

Version v2.0
January 05, 2026

Contents

1	Preface	6
1.1	Purpose	6
1.2	Audience	6
1.3	Revision history	6
1.4	Related documentation	7
1.5	How to get product help	8
1.6	How to provide documentation feedback	8
2	Deployment Overview	9
2.1	Components in a Decentralized Nymi Agent Configuration	9
2.2	Components in a Centralized Nymi Agent Configuration	11
2.3	Deployment of the Nymi WebAPI	13
2.4	Nymi WebAPI Configuration Requirements	14
3	Prepare for Connected Worker Platform Deployment	15
3.1	Hardware and Software Requirements	15
3.1.1	NES Requirements	15
3.1.2	Time Synchronization Requirements	16
3.1.3	User Terminal Requirements	16
3.1.4	Nymi Lock Control Considerations	18
3.1.5	Nymi WebSocket API Interface Requirements	18
3.2	Networking Requirements	19
3.2.1	(Non-HA Deployments only) Domain Name Service Requirements	19
3.2.2	(HA Deployments only) Domain Name Service Requirements	19
3.2.3	(HA Deployments only) Load Balancer Requirements	20
3.2.4	Firewall Port Requirements	21
3.2.5	RDP/Citrix Client Considerations	22
3.3	Certificate Requirements	22
3.3.1	TLS Certificates	23
3.3.2	Nymi-specific Certificates	25

3.3.3	Using TLS Certificates Issued by Untrusted Certificate Authorities	25
3.4	Active Directory Requirements	26
3.4.1	Requirements for the Installer Account	26
3.4.2	Domain and Trust Requirements	26
3.4.3	Creating the Active Directory Group for NES Administrator	27
3.4.4	(Optional) Creating an Organizational Unit for User Terminals	28
3.4.5	Creating the Nymi Infrastructure Service Account	28
3.4.6	Setting Service Principal Names	29
3.5	Database Requirements	31
3.5.1	Supported SQL Versions	31
3.5.2	Creating the NES Database	31
3.5.3	Configuring SQL Database for Remote Access	32
3.6	CWP Package Requirements	35
3.6.1	Obtaining the NES Software Package	35
4	Deploy Nymi Enterprise Server	36
4.1	Install and Configure IIS	36
4.1.1	Installing IIS and ASP.NET	36
4.1.2	Importing the TLS Server Certificate	38
4.1.3	Adding HTTPS Site Bindings	41
4.1.4	Creating an Application Pool for Authentication Service	42
4.1.5	Verifying the Authentication Configuration	46
4.1.6	Securing IIS	47
4.1.7	Enabling Directory Browsing in IIS	48
4.1.8	(HA Deployments Only) Generating Machine Keys	49
4.2	Importing a Fullchain Certificate	51
4.2.1	Importing Certificates	51
4.2.2	Moving the L2 Certificate	54
4.3	Install NES	55
4.3.1	Installing the NES Services Suite Using the Wizard	55
4.3.2	Configuring NES Services Manually	58
4.3.3	Deploying the NES URL to User Terminals by Using Group Policies	70

4.3.4	Deploying the Nymi Agent URL to User Terminals by Using Group Policies	72
4.3.5	Saving the NES Configuration	74
4.3.6	(HA Deployments) Configuring Additional NES Servers from a Configuration File	74
4.4	Configuring IIS to Prevent NES Offloading	77
4.5	Validating the NES Deployment	82
4.5.1	Access the NES Administrator Console	82
4.6	Configure NES for Nymi Lock Control	83
4.7	Hardening the NES Keystore	83
4.7.1	(Optional) Encrypting Usernames in the NES Database	86
5	Install and Configure Endpoints	87
5.1	Install and Configure Endpoints with a Decentralized Nymi Agent	87
5.1.1	Bluetooth Adapter	88
5.1.2	Set Up a Decentralized Enrollment Terminal	89
5.1.3	Set Up Windows User Terminals for Authentication Tasks	92
5.1.4	Set Up Windows User Terminals for Lock and Unlock	94
5.2	Install and Configure Endpoints with a Centralized Nymi Agent	102
5.2.1	Configuring Endpoint ID	102
5.2.2	Set Up the Enrollment Terminal	104
5.2.3	Set Up Thick Client User Terminals	110
5.2.4	Set Up User Terminals for Lock and Unlock (Remote)	134
6	Set Up a Centralized Nymi Agent	140
6.1	Import the Root CA Certificate	140
6.2	Install the Nymi Agent on the Centralized Server	143
6.3	Configure the Nymi Agent	147
7	Upgrade the Connected Worker Platform	153
7.1	Update the Enrollment Terminal	154
7.1.1	Update the Centralized NBA	154
7.1.2	Update the Decentralized NBA	156
7.2	Update the Centralized Nymi Agent and Clients	157
7.2.1	Update the Centralized Nymi Agent	157

7.2.2	Configuring Nymi Agent	158
7.2.3	Update Clients that Connect to a Centralized Nymi Agent	160
7.3	Update Clients with a Decentralized Nymi Agent	164
7.4	Update Nymi Lock Control	164
7.5	Change the CWP Communication Protocol	165
8	Reference	166
8.1	Environment Summary	166
8.2	FQDN Summary	166
8.3	Certificate Expiration	167
8.4	Silent Installations	167
8.4.1	Installing the Nymi Runtime Silently	167
8.4.2	Installing the Nymi Bluetooth Endpoint Silently	168
8.4.3	Performing a Silent Nymi Agent Installation or Update	169
8.4.4	Installing the Nymi Band Application Silently	170
8.4.5	Installing or Updating Nymi Lock Control Silently	171

1 Preface

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

CWP contains the following elements:

- Device Hardware — Refers to the Nymi Band™ and firmware.
- Infrastructure — Consists of software, such as the NES, Nymi Runtime, and the Nymi Band Application.

1.1 Purpose

This guide provides detailed information about the steps that an IT administrator performs to deploy or update the components of the CWP solution in an environment that consists of Windows or Linux machines.

1.2 Audience

This guide provides information to IT administrators who manage the CWP infrastructure and are familiar with Windows server, Active Directory, and command line tools.

1.3 Revision history

Version	Date	Revision history
1.0	November 28, 2025	New section <i>Configuring JWT Secret Key</i> to include NES API installation and update steps for NCA deployments in an NES API HA configuration.
2.0	January 05, 2026	Second release. Updates include new content for the CWP 1.20.1 release: revision of NES installation and update instructions to introduce new key management section; addition of content about deploying a highly available NES.

1.4 Related documentation

The Nymi documentation suite includes the following guides:

- *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.
- *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 Connect for Windows Installation and Configuration Guide* — This guide contains information about how to install, configure and use the Nymi Connect application on Windows.
- *Nymi Connect for Android - Deployment and Administration Guide* — This guide contains information about how to install, configure and use the Nymi Connect application on Android devices.
- *Nymi SDK Developer Guide—NymiAPI(Windows)* — This document provides information about how to develop Nymi-enabled Applications by using the Nymi API.
- *Nymi SDK Developer Guide—Webapi(Windows)* — This document provides information about how to understand and develop Nymi-enabled Applications (NEA) on Windows by utilizing the functionality of the Nymi SDK, over a WebSocket connection that is managed by a web-based or other application.
- *Connected Worker Platform with Evidian Installation and Configuration Guide* — This guide provides information about how to deploy the Nymi with Evidian solution components.
- *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 with Evidian Troubleshooting Guide* — This document provides overview information about how to troubleshoot issues that you might experience when using the Nymi solution with Evidian.
- *Connected Worker Platform—FIDO2 Deployment Guide* — This guide provides information about how to configure Connected Worker Platform and FIDO2

components to allow authenticated users to use the Nymi Band to perform authentication operations.

- *Connected Worker Platform—POMSnet Installation and Configuration Guide* — This guide provides information about how to configure the Connected Worker Platform and POMSnet components to allow authenticated users to use the Nymi Band to perform authentication operations in POMSnet.
- *Nymi Band Regulatory Guide* — This guide provides regulatory information for the Generation 3 (GEN3) Nymi Band.
- *Third-Party Licenses* — This document contains information about open source applications that are used in Nymi product offerings.

1.5 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@nymicom.

1.6 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@nymicom.

2 Deployment Overview

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

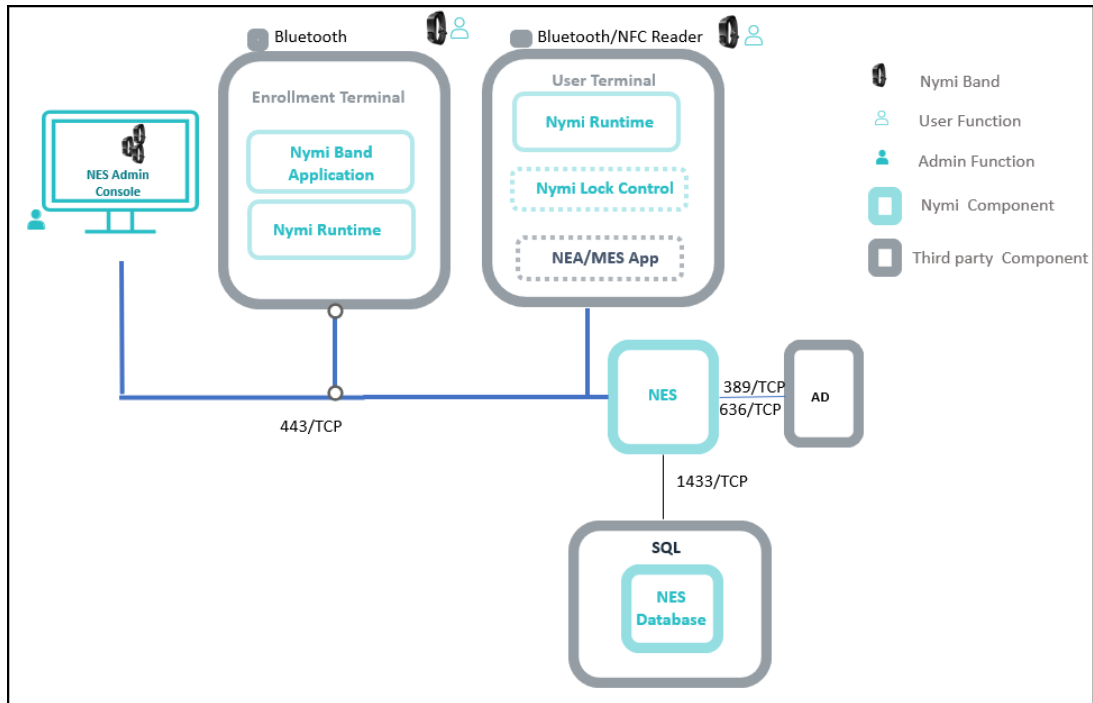
Review the following information to decide which configuration to deploy.

Configuration	When to use
Decentralized Nymi Agent	If your environment meets all of the following configuration scenarios, you can deploy a decentralized Nymi Agent solution.
Centralized Nymi Agent	If your environment meets any of the following configuration scenarios, you must deploy a centralized Nymi Agent solution.

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

2.1 Components in a Decentralized Nymi Agent Configuration

The Connected Worker Platform (CWP) enables users to use Nymi Bands and administrators to manage Nymi Bands and CWP components in an enterprise setting. CWP is comprised of Nymi-specific components and enterprise components, as shown in the following figure.



CWP components and connection ports

The CWP consists of the following components.

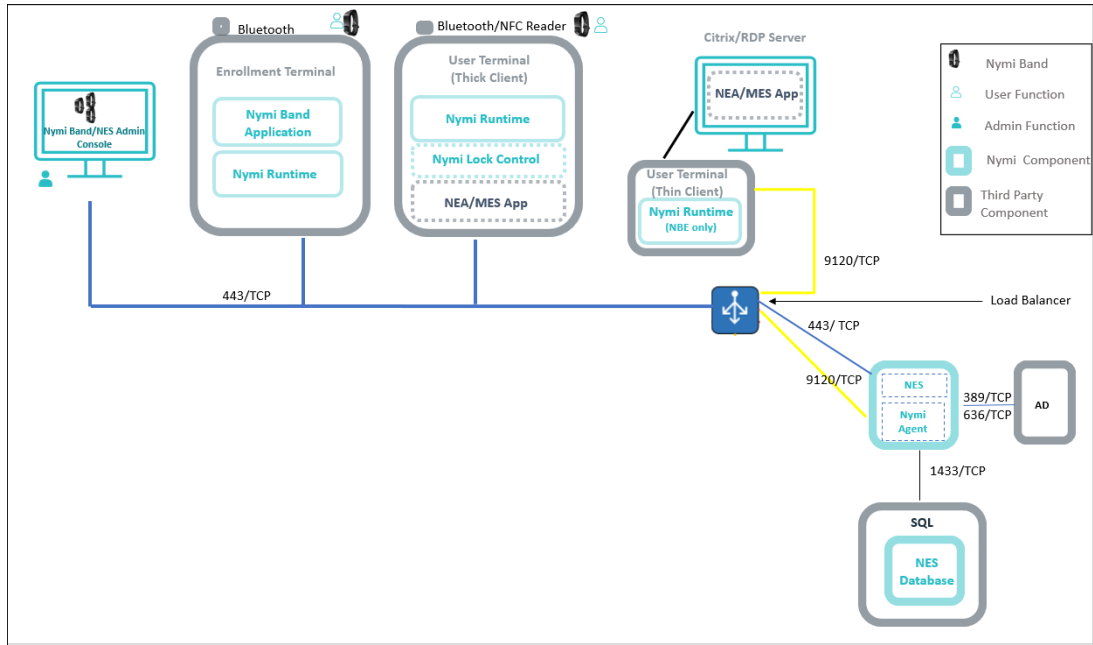
Component	Description
Enrollment Terminal	Windows 10 or Windows 11 endpoint that users access to enroll their Nymi Band.
Nymi Band Application (NBA)	A Windows application that you install on the enrollment terminal, which you use to enroll a new user and link them to their Nymi Band. The NBA requires the Nymi Runtime application, which the NBA automatically installs. The NBA communicates with the Nymi Band through the Nymi-supplied Bluetooth adapter, which you plug into a USB port on the enrollment terminal.
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 NBA and Nymi Lock Control.
User Terminal	Windows 10 or Windows 11 endpoint on which you install Nymi components that allow users to perform authentication tasks with a Nymi Band tap on the NFC reader or Bluetooth Adapter.
Nymi Band	

Component	Description
	A wearable device that is associated with the biometrics of a single user. An authenticated Nymi Band is Bluetooth Low Energy (BLE) and Near Field Communication (NFC)-enabled. Note: Nymi Connect for Android supports the BLE component of the Nymi Band only.
Nymi-enabled Application (NEA)	Developers can create corporate applications that integrate with CWP 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, and automatically lock the user terminal when they walk away.
Nymi Enterprise Server (NES)	Windows-based management server and collection of services that administrators access through a web-based application. NES coordinates communication between the Nymi Band and the customer identity ecosystem (Active Directory) to manage policies and certificates. Includes the following services:
NES Administrator Console	A web interface that provides NES Administrator the ability to manage the NES configuration and users.
SQL Server	Database server that contains tables that store information about the NES configuration and the Nymi Bands. For Proof of Concept (POC) and pre-production environments, you can use the Nymi-provided SQL Server Express software. For production environments Nymi recommends that you use SQL server.
Domain Controller (DC)	Windows server with Active Directory.

2.2 Components in a Centralized Nymi Agent Configuration

A CWP deployment in an environment that uses MES applications that are hosted on an RDP /Citrix server contain the same components as a CWP deployment in a local environment, but some components are configured differently.

The following figure provides an overview of the CWP components in a centralized Nymi Agent environment.



CWP components in a Citrix/RDP environment

The following table summarizes how the component configurations differ in a remote environment. For general information about the CWP components, see the section *CWP Components in a Local Environment*.

Component	Description
Enrollment Terminal	Windows 10 or Windows 11 endpoint that users access to enroll their Nymi Band. Nymi recommends that you use a thick client for the enrollment terminal.
User Terminal (thick client)	A Windows 10 endpoint that users use to:
User Terminal (thin client)	An endpoint that users use to:
Citrix/RDP server	Remote session host. In Citrix and RDP environments, the user uses a thin client to connect to a remote session host and then launches an NEA that is installed on a remote session host. Different user sessions run their own NEA instance.
Centralized Nymi Agent	Nymi Runtime component that you install on a server that is accessible to all user terminals, for example the NES server.

2.3 Deployment of the Nymi WebAPI

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

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

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

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

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

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

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

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

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

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

2.4 Nymi WebAPI Configuration Requirements

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

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

3 Prepare for Connected Worker Platform Deployment

Review this section for information about the requirements and steps that you must perform to prepare for the Connected Worker Platform (CWP) components.

3.1 Hardware and Software Requirements

The following sections provide more information about the hardware and software requirements for CWP components.

3.1.1 NES Requirements

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

3.1.1.1 Hardware Requirements

The NES API 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
 - 8 GB RAM
 - 20 GB free disk space
- 5000–10000 users:
 - 4 Core CPU
 - 16 GB RAM
 - 40 GB free disk space

3.1.1.2 Software Requirements

The NES API has the following software requirements.

- Microsoft Windows Server 2016, 2019, or 2022

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

- Microsoft IIS
- Microsoft .NET Framework 4.8

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

3.1.2 Time Synchronization Requirements

Nymi Band enrollments require time synchronization between the Enrollment Terminal and the NES API.

When the Enrollment Terminal is on a domain, the time source for both the Enrollment Terminal and the NES API is Active Directory Domain Services (AD DS). If your Enrollment Terminal is not domain-joined, ensure that you find an alternate method to synchronize both the Enrollment Terminal and the NES API with a reliable time source.

3.1.3 User Terminal Requirements

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

3.1.3.1 Hardware and Software Requirements

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

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

Use Case	Supported Operating System/ Browser	Hardware
Enrollment	Windows 10, 64-bit, minimum build version 1607; Windows 11, 64-bit. Note: Nymi recommends 125% scaling and 1920 x 1080 screen resolution for the terminal hosting the NBA.	4 GB RAM; 5 GB free disk space; 2 core CPU (recommended); 1 USB 2.0 port; Nymi-supplied Bluetooth adapter
Authentication tasks with a Nymi Band in an NEA on Windows, HP ThinPro, and IGEL	Windows 10 x86-64 (minimum build version 1607) and Windows 11, including on Citrix, RDP, and VMWare Horizon; HP ThinPro x86-64, including on VMWare Horizon; IGEL OS v10, including IGEL Thin Client on Citrix. Tested browsers: Firefox 70+, Chrome 78+, Internet Explorer 11+, Microsoft Edge 44.18362.387.0	Nymi-supplied Bluetooth adapter; NFC reader (optional)
Locking and Unlocking the Desktop	Windows 10 x86-64 (minimum build version 1607) and Windows 11, including on Citrix, RDP, and VMWare Horizon; HP ThinPro x86-64, including on VMWare Horizon	Nymi-supplied Bluetooth adapter; NFC reader (optional)

3.1.3.2 Windows N Edition Requirements

Windows N Edition does not include media features by default. The NBA includes embedded video that cannot display without the media feature pack.

To obtain the media feature pack, perform one of the following actions:

- For Windows 10 version 1909 and later, and Windows 11, go to **Settings > Apps > Apps & features > Optional features > Add a feature**, install **Media Feature Pack**, and then restart the machine.
- For Windows 10 versions earlier than 1909, download and install the media feature pack from the [Microsoft Media Feature Pack](#) page, and then restart the machine.

3.1.4 Nymi Lock Control Considerations

Review the following information about Nymi Lock Control:

- 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.

3.1.5 Nymi WebSocket API Interface Requirements

Nymi provides an API interface that supports web-based NEAs called the WebSocket API.

Consider the following:

- In an environment where thick clients access web-based NEAs, you can install both the Nymi Bluetooth Endpoint and Nymi Agent components of the Nymi Runtime package.
- In an environment where thin clients access web-based NEAs on an RDP/Citrix server, you must install the Nymi Bluetooth Endpoint component of the Nymi Runtime on the thin client user terminal, and install the Nymi Agent on a server that is accessible to all thin clients.

3.1.5.1 Configuring and deploying in an environment with thin client user terminals

Take the following into consideration when configuring the solution in a physical environment.

- Ensure that Nymi Agent and user terminals have connectivity to NES.
- Ensure that the Nymi Agent and WebSocket components use 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 Agent and the thick clients, ensure that your NEAs use the subscribe operation. The *Connected Worker Platform WebSocket API Developer's Guide* provides more information.
- Each component can co-locate with NES (ensure that distinct TCP ports are being used).

3.2 Networking Requirements

The solution requires Domain Name Service (DNS) and firewall port changes to support inter-component communications.

3.2.1 (Non-HA Deployments only) Domain Name Service Requirements

The Connected Worker Platform (CWP) solution uses fully-qualified domain names (FQDNs) that point to CWP infrastructure services that are accessed by CWP applications, such as NBA and the NES Administrator Console.

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

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

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

3.2.2 (HA Deployments only) Domain Name Service Requirements

Every CWP service is a cluster that consists of multiple cluster members. For each CWP service, you must define a virtual server on the load balancer to distribute traffic to the cluster members.

In a clustered CWP deployment, you must assign FQDNs to the following components and add them to DNS:

- All cluster members for all CWP services
- All virtual servers

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

Record each FQDN value in the *FQDN Summary*.

Component	FQDN Example
NES cluster member 0	nes-0.cwp.company.com
NES cluster member 1	nes-1.cwp.company.com
NES virtual server	nes.cwp.company.com
Centralized Nymi Agent cluster member 0	nymiagent-0.cwp.company.com
Centralized Nymi Agent cluster member 1	nymiagent-1.cwp.company.com
Centralized Nymi Agent virtual server	nymiagent.cwp.company.com
Centralized Nymi Agent (with WebSocket API enabled) cluster member 0	nymiagentwebapi-0.cwp.company.com
Centralized Nymi Agent (with WebSocket API enabled) cluster member 1	nymiagentwebapi-1.cwp.company.com
Centralized Nymi Agent (with WebSocket API enabled) virtual server	nymiagentwebapi.cwp.company.com

3.2.3 (HA Deployments only) Load Balancer Requirements

The Connected Worker Platform (CWP) solution supports the use of load balancers for load distribution to clustered CWP services. One or more load balancers can perform load balancing.

You can deploy a load balancer between the external clients and the cluster, preferably in a highly-available configuration.

Consider the following load balancer requirements:

- Use a Layer 4 or Layer 7 load balancer that supports session persistence (affinity) by using the source IP address.
- Configure an active-active load balancing policy for NES API.
- Configure an active-passive load balancing policy for Nymi Agent.
- Configure session persistence (affinity) by using source IP.
- Define the following virtual servers on the load balancer:
 - NES API — Cluster members that are accessible on port 443.
 - Nymi Agent — Cluster members that are accessible on port 9120.

- Nymi Agent (when WebSocket API is enabled) — Cluster members that are accessible on port 80 (default port for ws protocol) or 443 (default port for wss protocol).

3.2.4 Firewall Port Requirements

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

3.2.4.1 Connection Port Requirements

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

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

Purpose	Protocol	Source	Virtual Server FQDN & Port	Destination and Port
SQL Access	MS SQL (Proprietary)	NES	n/a	SQL Server: 1433/TCP
LDAP Access – Active Directory (AD)	LDAP/ LDAPS	NES	n/a	AD Server: 389/TCP (LDAP) or 636/TCP (LDAPS)
NES Communications	HTTPS	Machine that accesses NES Administrator Console; all user terminals (thick); centralized Nymi Agent; RDP/Citrix servers that run NEAs	nes.cwp.company.com: 443/TCP	NES: 443/TCP

Purpose	Protocol	Source	Virtual Server FQDN & Port	Destination and Port
Supports Centralized Nymi Agent communications. Nymi Agent receives incoming WebSocket connections on TCP port 9120, which is used for communication with Nymi Bluetooth Endpoint and native NEAs.	TCP	All user terminals (thick and thin); RDP/Citrix servers that run NEAs	nymiagent.cwp.company.com: 9120/TCP	nymiagent-0.cwp.company.com, nymiagent-1.cwp.company.com: 9120/TCP

3.2.5 RDP/Citrix Client Considerations

In an RDP/Citrix environment with a Centralized Nymi Agent configuration, ensure that user terminals with multiple network interfaces do not switch networks.

For example, network switching can occur when you configure:

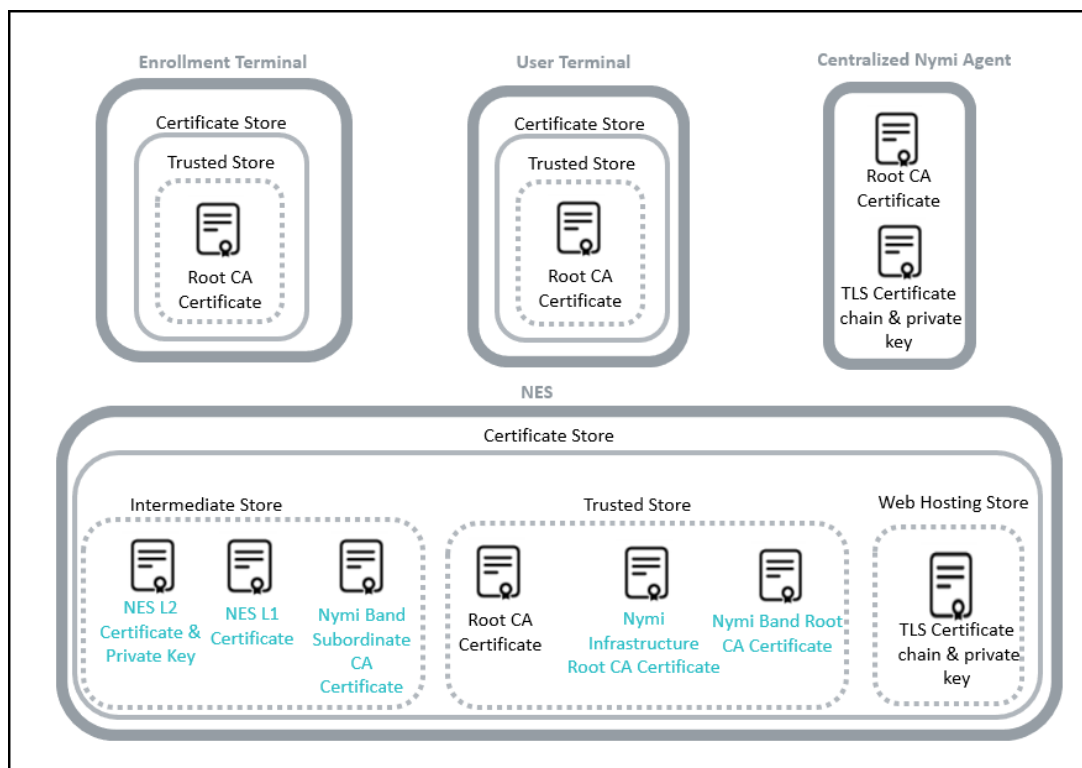
- A tablet or laptop to connect to multiple WIFI networks (i.e., an internal and guest network) and the user terminal encounters an intermittent issue with one network, the user terminal connection might switch to the other network.
- A desktop computer with WIFI and Ethernet connections and a user plugs/unplugs the Ethernet cable, the user terminal switches to the available connection.

When a network switch occurs, the user terminal usually acquires a new IP address. The RDP/Citrix session and the websocket connection to the Nymi Agent can recover and reconnect, but client applications such as Evidian, and the Nymi API DLL continue to run and subscribe to the previous IP address. As a result, the Nymi API cannot communicate with the Nymi Bluetooth Endpoint and the application does not detect a Nymi Band tap.

3.3 Certificate Requirements

The solution relies on TLS certificates and Nymi-specific certificates to ensure secure communications.

The following figure provides a high-level overview of the certificates used by the solution.



Certificates

3.3.1 TLS Certificates

Connected Worker Platform (CWP) uses TLS certificates to secure client communications with Nymi Enterprise Server (NES) and a centralized Nymi Agent. These certificates serve the same purpose as typical TLS certificates that support secure communications within your enterprise network, for example, for web and email traffic. Nymi recommends that you use a trusted Certificate Authority (CA) to issue the TLS certificate.

Note: If you use a self-signed TLS certificate or a certificate that was issued by an untrusted private root CA, you require a Root CA Certificate. You must import the Root CA Certificate on each user terminal, the enrollment terminal, Citrix/RDP clients, centralized Nymi Agent, and the NES API server. This guide describes how to import the Root CA Certificate.

Nymi Enterprise Server Certificate Format

NES uses the Windows certificate store for TLS certificates. The Windows certificate store supports several certificate formats, such as PKCS#12, which includes the TLS certificate chain and the password-protected private key all in one file. Copy the certificate file to the server that you designate for NES and record the password of the TLS certificate in a secure manner. The NES deployment process prompts you for the password.

Note: The procedures detailed in this guide assume that you have the NES certificate and private key in PKCS#12 format.

Centralized Nymi Agent Certificate Format

Nymi Agent relies on WebSocket for communications with native and web-based NEAs and Nymi Bluetooth Endpoint. Nymi recommends that you secure WebSocket communications between the Nymi components.

Obtain the following certificate and private key files in base64 PEM format from your security team, and copy the files to the server that you designate as the Nymi Agent server:

- Certificate file, which contains the TLS Server Certificate only.

Note: You cannot use a wildcard certificate.

- Private key file that has the unencrypted private key for the TLS server certificate.
- Certificate Authority (CA) certificate file bundle, which contains the CA certificate chain that starts from the root CA and ends in the subordinate CA that issues the server certificate.

Nymi recommends that you issue the NES and centralized Nymi Agent TLS server certificate from a Root CA that is trusted by the client machines. If the Root CA is not trusted by the client machines, install the root CA certificate in the Trusted Root Certification Authorities container for the client machine.

Subject Alternative Name Requirements

The TLS certificate must contain the appropriate fully qualified domain name (FQDN) for the Subject Alternative Name (SAN).

In a clustered deployment, ensure that you include the FQDN of each NES API instance and the public NES API FQDN in the SAN field.

Note: You can use the same TLS certificate for NES and Nymi Agent if the SAN includes all the FQDNs and the TLS certificate matches the requirements outlined for the centralized Nymi Agent. Ensure that the format of the TLS certificate matches the previously stated format requirements.

3.3.2 Nymi-specific Certificates

Required to support secure communications between the Nymi Bands and the CWP services. Nymi provides two certificate files:

- Fullchain PFX file, which you obtain from your Nymi Field Representative. This certificate is unique for each organization and includes the following content:
 - Nymi Infrastructure Root CA certificate
 - NES L1 certificate
 - NES L2 certificate and associated private key

This guide describes how to implement the full chain certificate when you deploy NES.

- Nymi Band PKI certificate files:
 - Nymi Band Root CA Gold
 - Nymi Band Subordinate CA Gold

The NES installation package includes the Nymi Band PKI certificate files and the NES installation automatically installs the certificate.

For more information about the Nymi-specific certificates, refer to the *Connected Worker Platform Security Guide*.

3.3.3 Using TLS Certificates Issued by Untrusted Certificate Authorities

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

To use an untrusted CA, ensure that you:

- Use a single untrusted root CA to issue all TLS certificates.

- Import the untrusted root CA certificate into each machine that communicates with the CWP services. The methods that you use to import the untrusted root CA certificate into each component is described later in this guide.

3.4 Active Directory Requirements

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

3.4.1 Requirements for the Installer Account

When you install the Nymi component software on each computer in the environment, you can use the same account or different accounts. For example, you can install the NES API software with one AD account and install the client software with a different account.

The account that you use to install the NES API software must meet the following requirements:

- Username less than 20 characters.
- Local administration privileges on the NES API computer.
- Logon permissions to the SQL server and DB_OWNER rights to the NES API database. After you complete the software installation, you can remove these rights for the user account.

When you install the Nymi client software, the account that you use must meet the following requirements:

- Username less than 20 characters.
- Local administrative privileges.
- Write permission to the drive on which you install the software. The NBA and Nymi Runtime software install the component software on the C: drive.

3.4.2 Domain and Trust Requirements

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

3.4.2.1 Domain Requirements

You require this information during the NES API deployment process.

- Communication protocol that the solution uses to connect to Active Directory. For example, LDAP or LDAPS.
- Port number on which to contact Active Directory. The default port number for LDAP is 389.
- The NetBIOS domain name, which you can see in the properties of an AD user account.

3.4.2.2 Trust Requirements

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

Note: For Nymi with Evidian deployments, you require at a minimum a selective two-way trust.

3.4.3 Creating the Active Directory Group for NES Administrator

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

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

1. Log into the Active Directory server with a domain administrator account.
2. Create a group to contain the users who will act as an NES Administrator. For example, a group named `NES_admins`.
 - In the **Group Scope** section, select one of the following options:
 - 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 from any domain to the NES Administrator group.
 - When you select **Global**, you can only add users that are local to the domain. If users in multiple domains require administrator access to NES, you must create a global group in each domain

with NES Administrator users, and then add the NES Administrator users to this group.

- The solution does not support the **Domain local** group scope.

3. In the **Group Type** section, select **Security**.

4. Click **OK**.

5. Add each user account that requires NES Administrator access to the group.

Note: Do not include AD groups in the group.

3.4.4 (Optional) Creating an Organizational Unit for User Terminals

Create an Organizational Unit (OU) in Active Directory (AD) to limit the user terminals in your environment on which users can use the Nymi Lock Control software.

The NES installation wizard prompts you for this OU.

3.4.5 Creating the Nymi Infrastructure Service Account

Connected Worker Platform (CWP) 1.12.x and later uses a service account to support interprocess communication and to manage the NES API database in SQL.

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

- Domain user.
- Password never expires.
- Logon as a service privileges.
- Username is less than 20 characters.
- Supports 128 and 256 bit AES encryption. To confirm this setting:
 1. Edit the properties of the user account in **Active Directory Users and Computers**.
 2. On the **Account** tab, in the **Account Options** section, scroll down, and then select **The Account Support Kerberos 128 bit AES encryption** and **The Account Support Kerberos 256 bit AES encryption**, as shown in the following figure.

nymi infrastructure Properties

Organization	Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones
		Delegation		

User logon name:
 nymi_infra_service @TW-Lab.local

User logon name (pre-Windows 2000):
 TW-LAB\ nymi_infra_service

Logon Hours... Log On To...

☐ Unlock account

Account options:

- ☐ Use only Kerberos DES encryption types for this account
- ☒ This account supports Kerberos AES 128 bit encryption.
- ☒ This account supports Kerberos AES 256 bit encryption.
- ☐ Do not require Kerberos preauthentication

Account expires

☒ Never

☐ End of: Saturday , February 22, 2025

OK Cancel Apply Help

AES encryption settings

3.4.6 Setting Service Principal Names

If the NES Authentication Service Application Pool uses the Nymi Infrastructure Service Account as the application pool identity, for example, when you deploy a highly-available NES API, you must specify HTTP Service Principal Names (SPNs) in Active Directory.

Perform the following steps on any computer that is on the same domain as the NES API servers.

1. Open a command prompt.
2. Type the following commands to view the existing SPN entries that are associated with the Application Pool Identity account:

```
setspn -T * -F -Q HTTP/nas_server1_fqdn
setspn -T * -F -Q HTTP/nas_server2_fqdn
setspn -T * -F -Q HTTP/nas_public_fqdn
```

Output similar to the following appears when the HTTP SPN is set correctly for an NES API server:

```
Checking forest DC=TW-Lab,DC=local
CN=Nymi Infra,CN=Users,DC=TW-Lab,DC=local
HTTP/tw-srv2.tw-lab.local
```

3. If an HTTP SPN is missing for any one of the NES instances or for the NES public FQDN, perform the following actions:

1. Open a command prompt as a Domain Administrator.
2. Type the following command to set the SPN:

```
setspn -S HTTP/<nas_server_fqdn> <nymi_infrastructure_service_account>
```

Where:

- `nas_server_fqdn` is the FQDN of the NES API server or the NES public FQDN that does not have an HTTP SPN.
- `nymi_infrastructure_service_account` is the NES AS application pool identity account name.

Example:

```
C:\Windows\system32>setspn -S HTTP/tw-srv2.tw-lab.local nymi_infra_
Checking domain DC=TW-Lab,DC=local

Registering ServicePrincipalNames for CN=Nymi Infra,CN=Users,DC=TW-
HTTP/tw-srv2.tw-lab.local
Updated object
```

3.5 Database Requirements

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

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

Ensure that the account that starts the SQL Server has permissions to register an SPN in Active Directory Domain Services. [Microsoft provides more information.](#)

3.5.1 Supported SQL Versions

The CWP solution supports the following Microsoft SQL versions:

- SQL Server / SQL Server Express 2016
- SQL Server / SQL Server Express 2017
- SQL Server / SQL Server Express 2019
- SQL Server / SQL Server Express 2022

Starting with CWP 1.18.0, the Nymi IT/OT Solution supports SQL Server Express. The NES installation package includes Microsoft SQL Server Express 2017; however, Nymi recommends that you use MS SQL Server in production environments.

Note: The CWP solution uses TLS 1.2. If you use SQL Server / SQL Express 2016 or SQL Server / SQL Express 2017, you must apply a patch to provide TLS 1.2 support. [Microsoft](#) provides more information.

3.5.2 Creating the NES Database

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

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

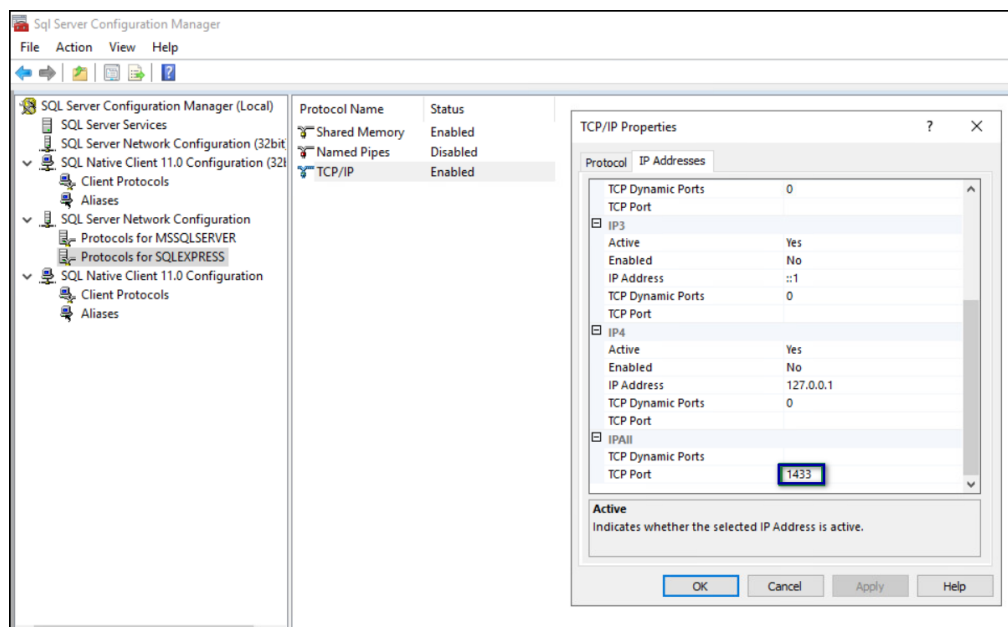
1. Open SQL Server Management Studio (SSMS).
2. Connect to the SQL Server instance.
3. Right-click **Databases**, and then select **New Database**.

4. In the New Database window, perform the following actions:
 - In the **Name** field, type `nes`.
 - Click the ellipsis (...) beside **Owner**, and then in the **Enter the object names to select** field, type the name of the Nymi Infrastructure account.
 - Click **Check Names**.
 - In the **Multiple Objects Found** field, select the service account name, and then click **OK**.
 - On the **Select Database Owner** window, click **OK**.
 - On the **New Database** window, click **OK**.

3.5.3 Configuring SQL Database for Remote Access

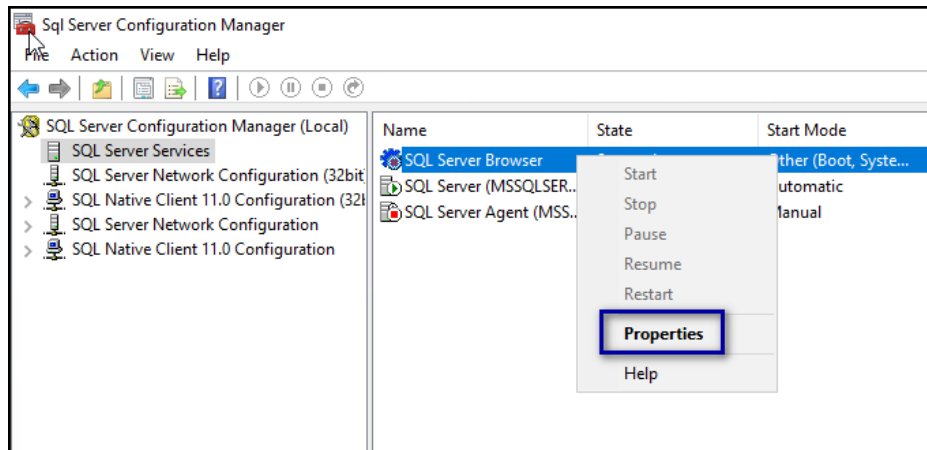
Perform the following actions in the SQL Server Configuration Manager application.

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



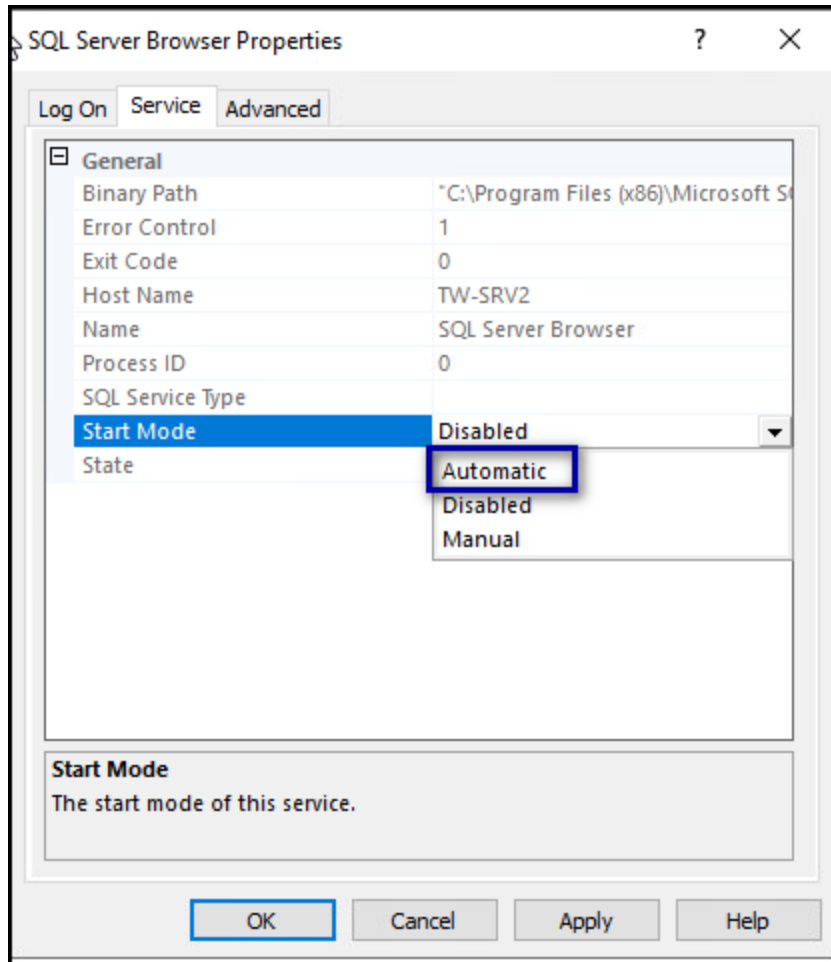
SQL port setting

6. Click **OK**, and then click **Apply**.
7. On the prompt to restart the SQL services, click **OK**.
8. Restart SQL Server services.
9. For SQL Express only, perform the following steps in SQL Server Configuration Manager:
 - In the left navigation pane, select **SQL Services**.
 - Right-click **SQL Server Browser**, and then select **Properties**, as shown in the following figure.



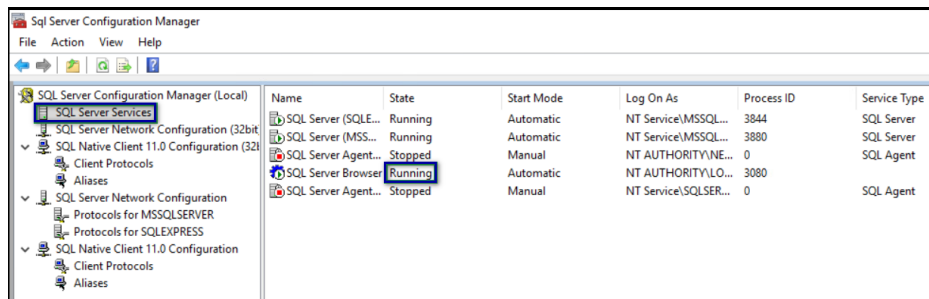
SQL Browser Properties option

- On the **Service** tab, from the **Start Mode** list, select **Automatic**, as shown in the following figure.



Start Mode

- Right-click **SQL Server Browser** and select **Start**. The SQL Server Browser service state changes to Start, as shown in the following figure.



SQL Server Browser service

3.6 CWP Package Requirements

3.6.1 Obtaining the NES Software Package

Your Nymi Field Representative provides you with a package that installs NES.

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

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

4 Deploy Nymi Enterprise Server

The following sections provide information about how to deploy the NES API.

4.1 Install and Configure IIS

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

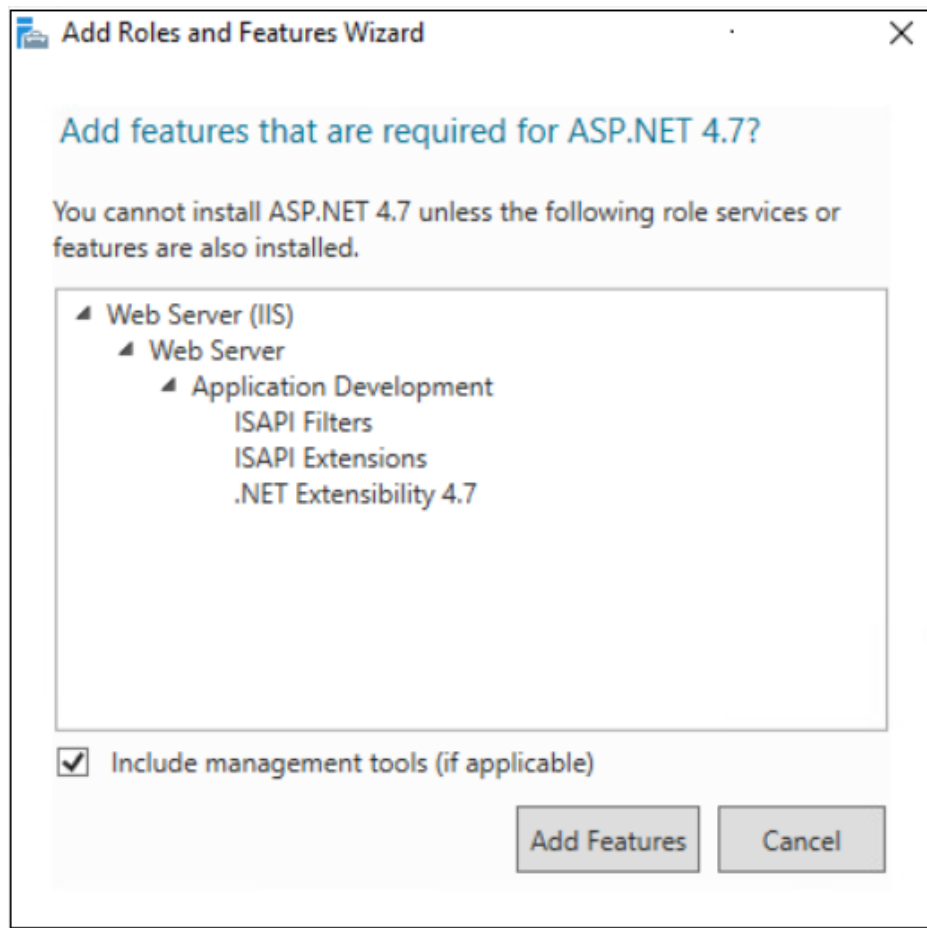
4.1.1 Installing IIS and ASP.NET

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

1. Open the **Server Manager** application, and then click **Add roles and features**.
2. On the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, leave the default value **Role-based or feature-based installation**, and then click **Next**.
4. On the **Select destination server** page, leave the default selection **Select a server from the server pool**, select the host in the **Server Pool** list box, and then click **Next**.
5. On the **Select server roles** page, click **Web Server (IIS)**. The **Add features that are required for Web Server (IIS)** dialog box appears.
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 **Application Development**, and then perform the following actions:
 1. Select **Application Initialization**.
 2. Select the latest available version of ASP.NET 4.x.

Note: NES supports ASP.NET 4.4 and later.

3. On the **Add features that are required for ASP.NET** dialog box, click **Add Features**, and then click **Next**.



Add features that are required for ASP.NET

4. On the **Select role services** page, leave the other default options selected, and then click **Next**.
11. On the **Select Features** page, click **Next**.
12. On the **Confirm installation selections** page, click **Install**. The **Installation Progress** page appears and provides the status of the IIS installation, which takes several minutes. When the installation completes, click **Close**. Restart the host, if prompted.

4.1.2 Importing the TLS Server Certificate

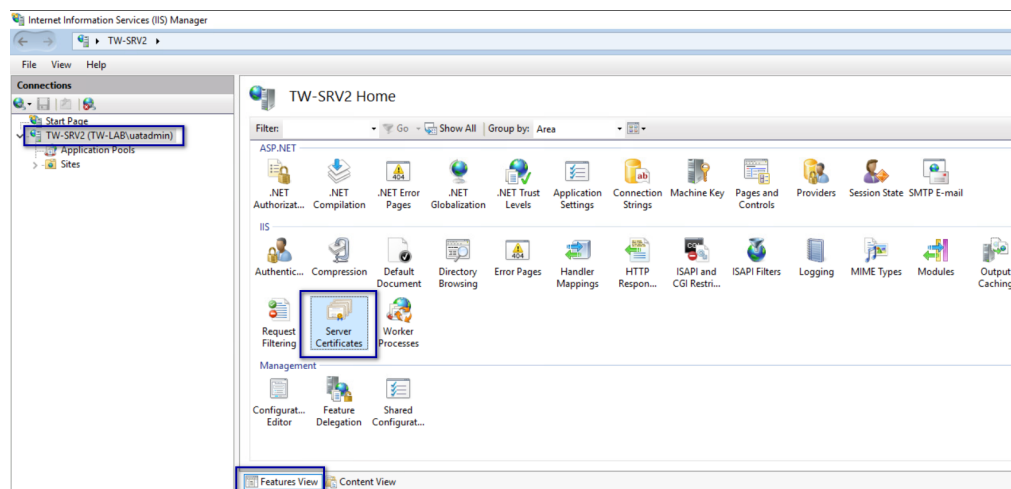
For HTTPS deployments, import the TLS server certificate obtained for the NES host. If the TLS server certificate is not signed by a Trusted Root CA, then you also need to import the Root CA certificate.

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 **IIS Manager** to import the TLS server certificate and the associated private key.

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

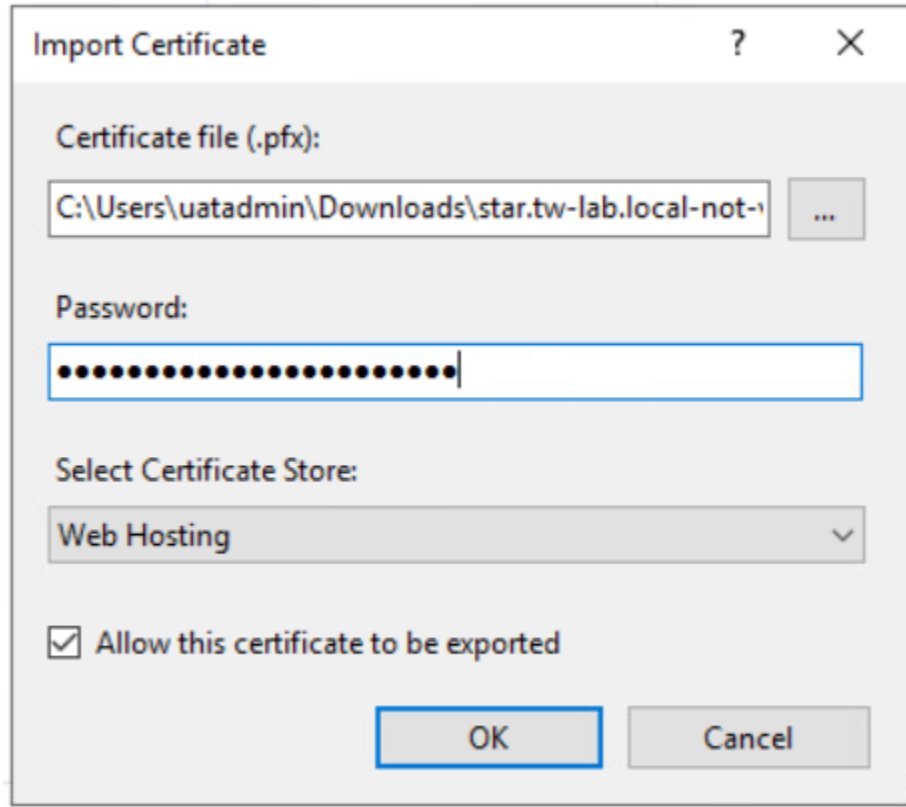
Note: If you cannot find **Server Certificates**, click the **Features View** tab, which appears at the bottom of the window.



Server Certificates option

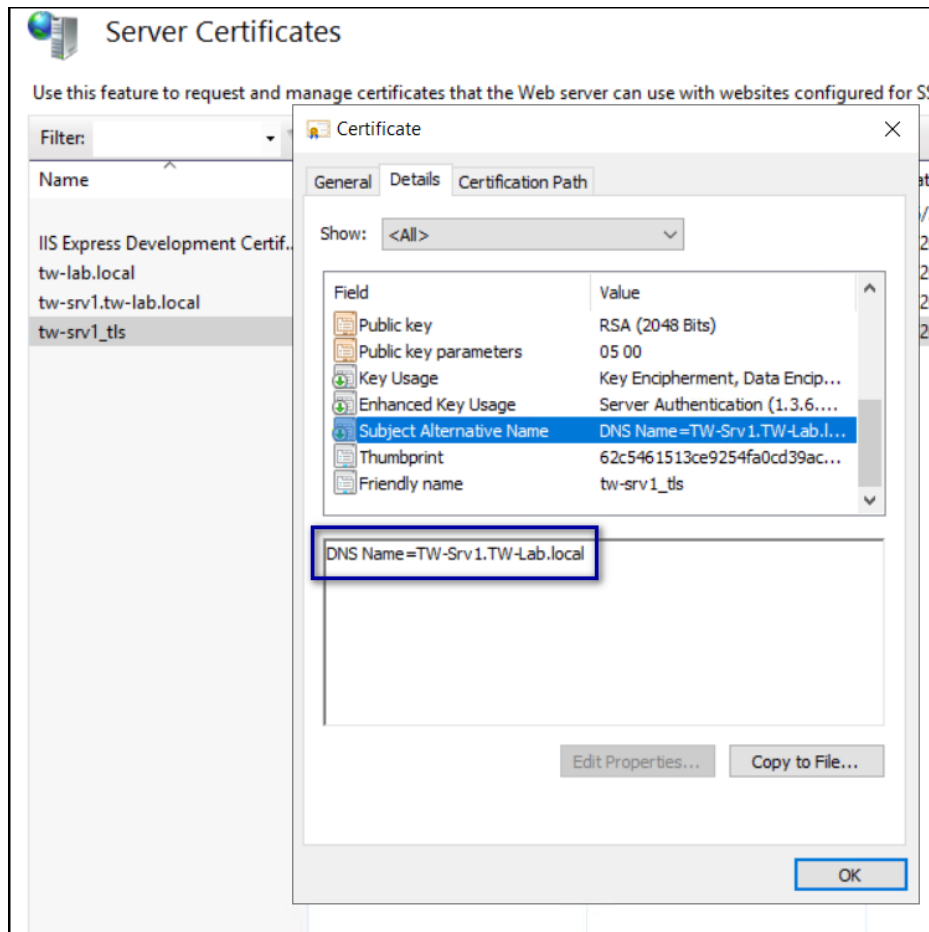
2. In the **Actions** navigation pane, on the right side of the window, click **Import**.
3. In the **Import Certificate** window, perform the following actions:
 1. In the **Certificate file (.pfx)** field, click the ellipsis (...) button, change the extension list to ***.***, browse to the location of the TLS certificate, select the certificate file, and then click **Open**.

2. In the **Password** field, type the password that was used to encrypt the private key, and then click **OK**.
3. In the **Select Certificate Store** list, select **Web Hosting**.



Import Certificates window

4. Click **OK**.
5. Right-click the TLS certificate that appears in the certificate list and select **Properties**.
6. On the **Details** tab, scroll down, and then select **Subject Alternative Name**. Confirm that the entry contains the FQDN of the NES API.



Subject Alternative Name

4. Minimize IIS.
5. Perform the following steps using the **Certificate MMC** to import the Root CA certificate (if needed).
 1. From the Windows toolbar, in the **Search** field, type **Manage Computer**, and then select **Manage computer certificates**.
 2. On the **User Account Control** dialog, click **Yes**.
 3. Expand **Certificates - Local Computer > Trusted Root Certificate Authority**.
 4. Right-click **Certificates**, and then select **All Tasks > Import**.

Import Certificate option
Import Certificate option

5. On the **Welcome to the Certificate Import Wizard** page, click **Next**.
6. On the **File to Import** page, click **Browse**, navigate to the root CA certificate file, and then click **Next**.
7. On the **Certificate Store** page, confirm the certificate store, and then click **Next**.
8. On the **Completing the Certificate Import Wizard** page, click **Finish**.
9. On the **Certificate Import Wizard** dialog, click **OK**.
10. Close the **certlm** window.

4.1.3 Adding HTTPS Site Bindings

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

Perform the following steps in **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*.

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

Edit Bindings option
Edit Bindings option

2. Right-click **Default Web Site**, and then select **Edit Bindings**.
3. Click **Add**. The **Add Site Binding** dialog box opens.
4. In the **Add Site Binding** dialog, perform the following actions:
 1. From the **Type** list, select **https**.
 2. In the **IP Address** field, leave the default setting **All Unassigned**.
 3. In the **Port** field, leave the default setting **443**.
 4. Leave the **Host name** field blank.
 5. From the **SSL certificate** list, select the TLS certificate that you imported.

Add Site Binding dialog
Add Site Binding dialog

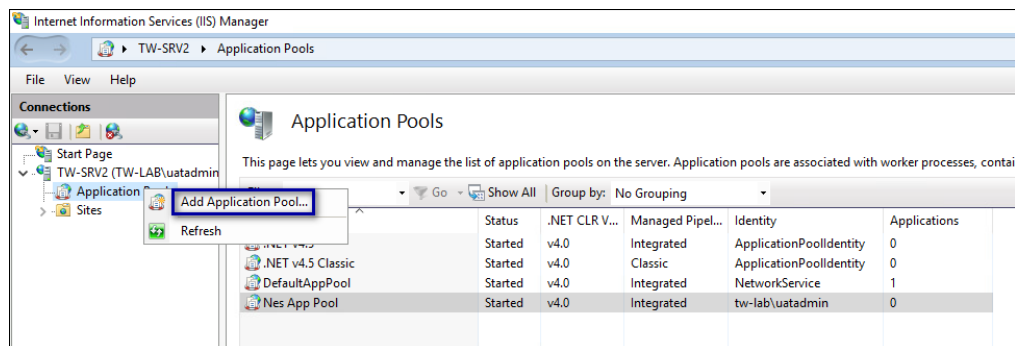
6. Click the **View** button, and identify the expiration date of the TLS certificate (see the line *Valid from (start date to expiration date)*).
 7. Record the expiration date in the *Certificate Expiration Date* table.
 8. Click **OK**.
5. On the **Site Bindings** dialog, click **Close**.

4.1.4 Creating an Application Pool for Authentication Service

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

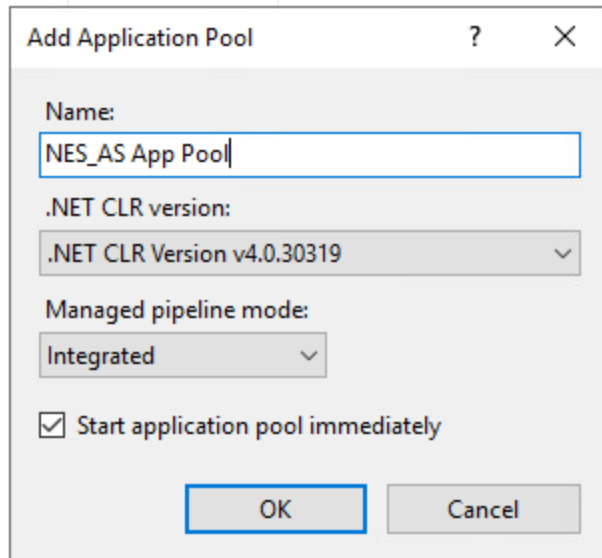
Perform the following steps in **IIS Manager**:

1. Expand *server_name*, right-click **Application Pools**, and then select **Add Application Pool**.



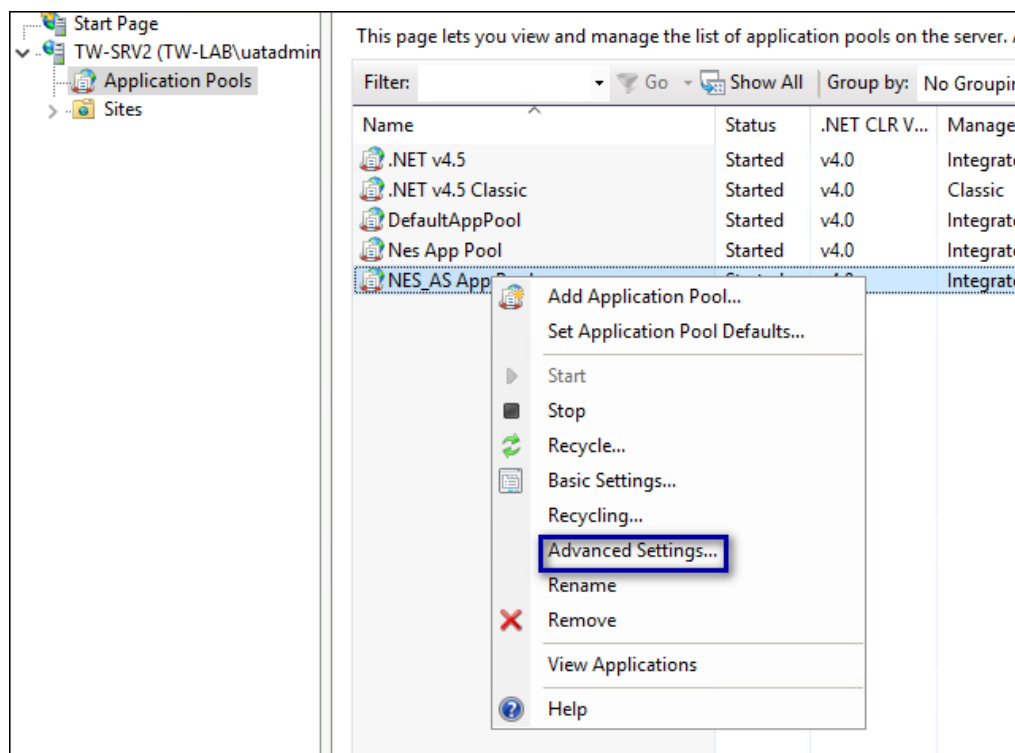
Create New Application Pool

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



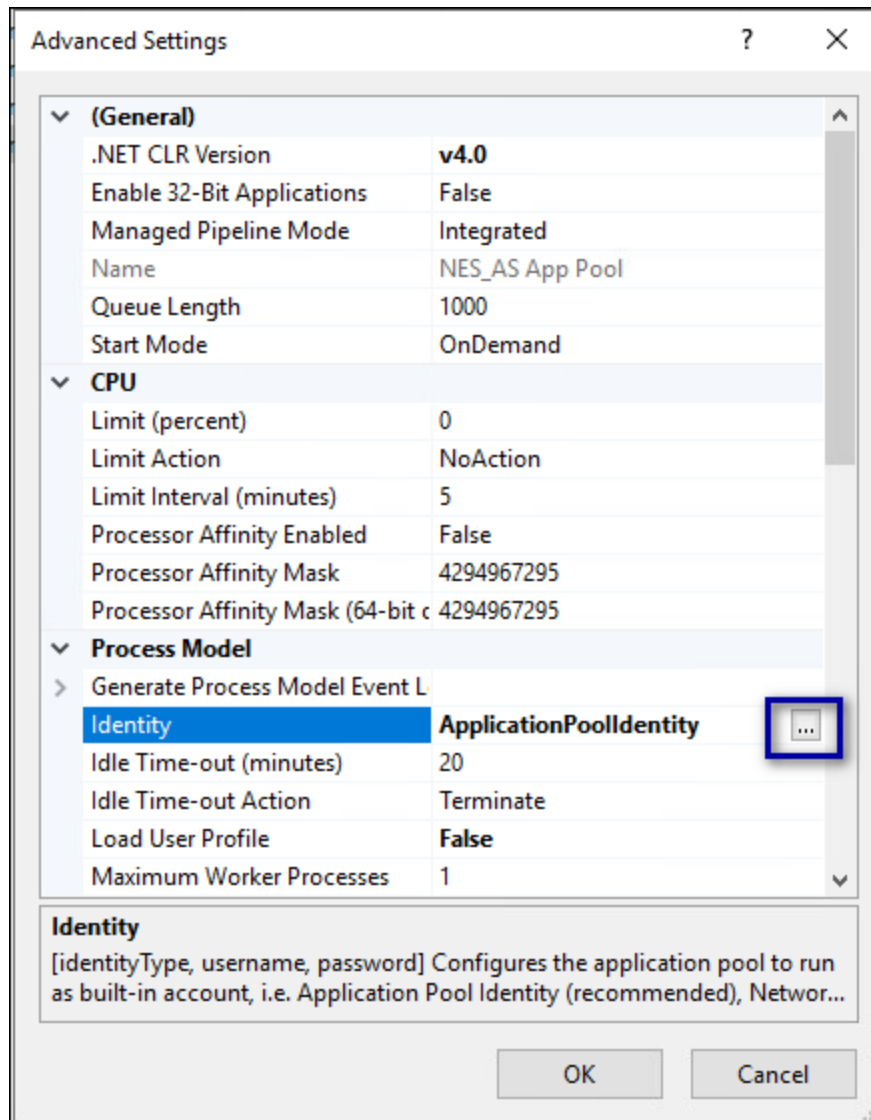
Add New Application Pool

3. Right-click **NES_AS App Pool**, and then select **Advanced Settings**.



Advanced Settings for Application Pool

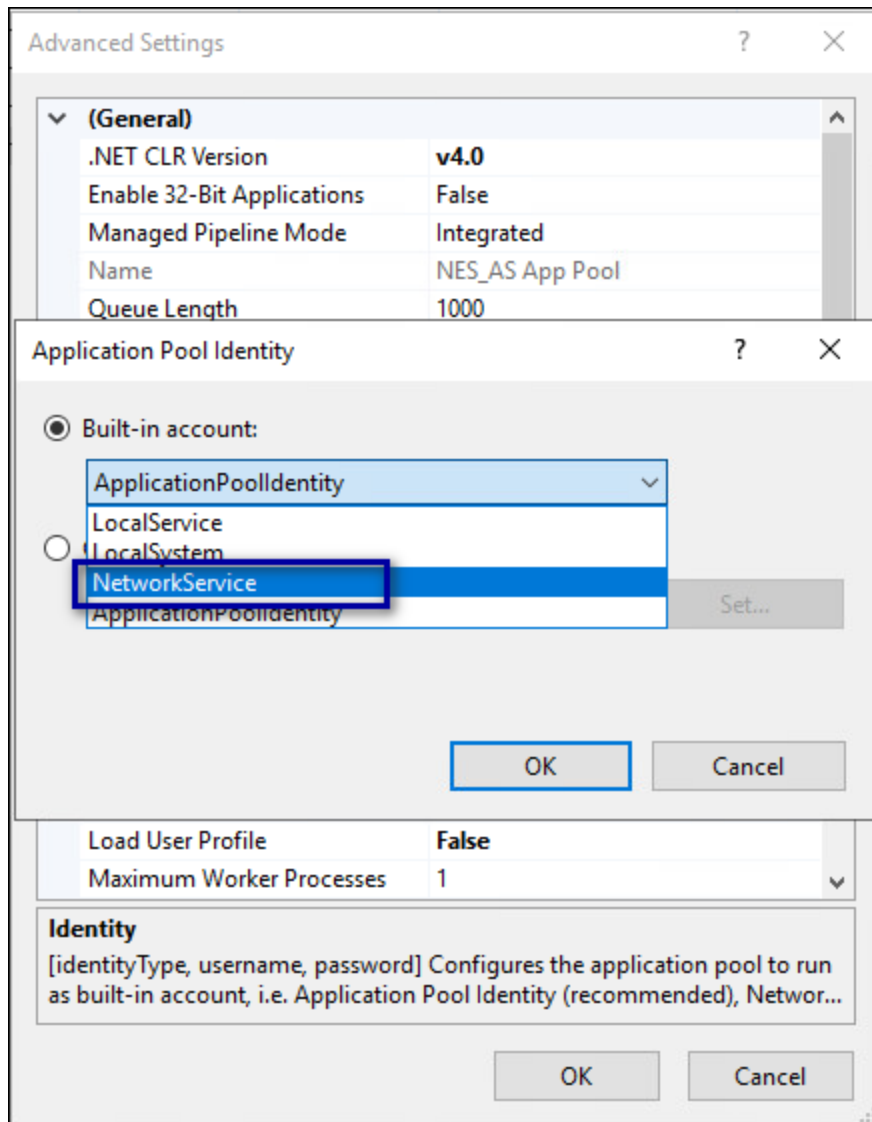
4. Click the **Ellipses** for the **Identity** parameter.



Edit Identity

5. Perform one of the following actions:

- For non-HA NES API deployments, from the **Built-in account** list, select **network service**, and then click **OK**.



Network Service selection

- For HA NES API deployments, select **Custom Account**, and then click **Set**. In the **Application Pool Identity** window, type the username and password of the Nymi Infrastructure Service Account, and then click **OK**.

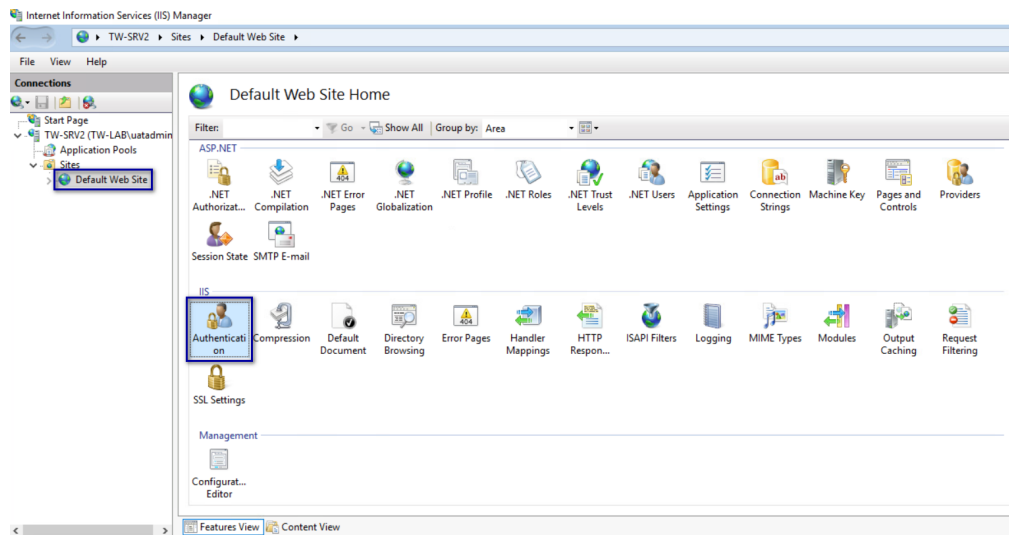
6. On the **Advanced Settings** window, click **OK**.

In an HA deployment, ensure that you set the Application Pool Identity to the same account on each IIS instance.

4.1.5 Verifying the Authentication Configuration

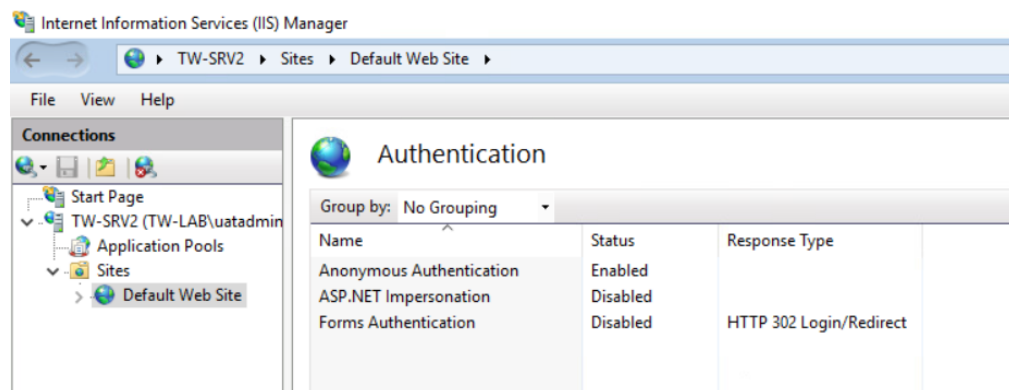
Perform the following steps in **IIS Manager** to verify that the authentication configuration is correct.

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



Authentication option

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



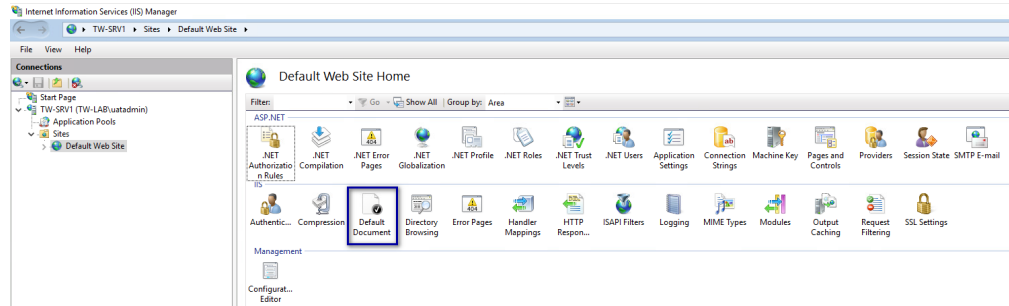
Authentication pane with Anonymous Authentication enabled

4.1.6 Securing IIS

Secure IIS by disabling the default page and creating a response header.

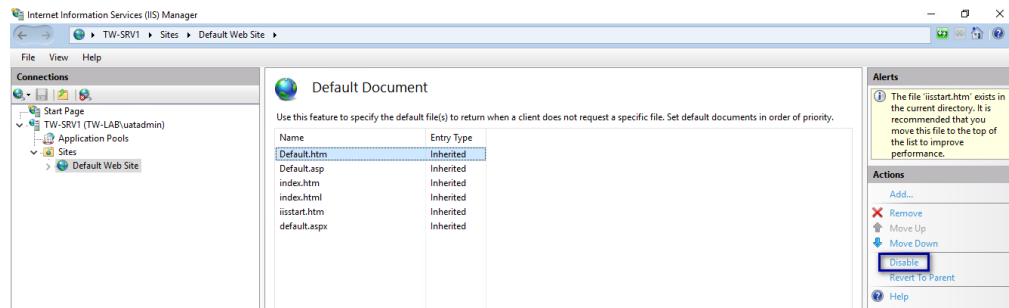
Perform the following steps in **IIS Manager**.

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



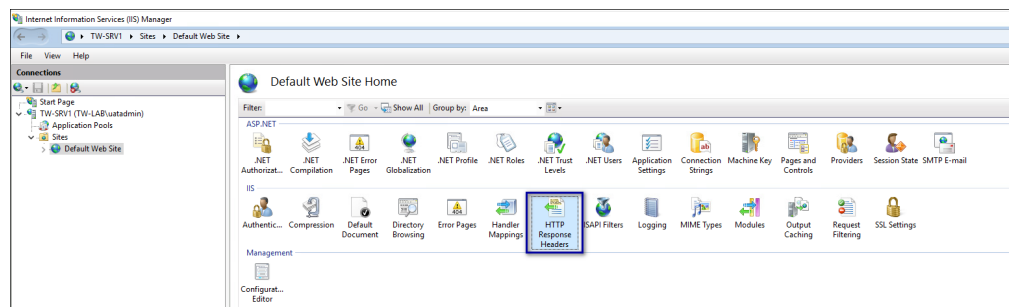
Default Document option

2. On the **Default Document** page, select **Default.htm**, and then click **Disable** from the right menu.



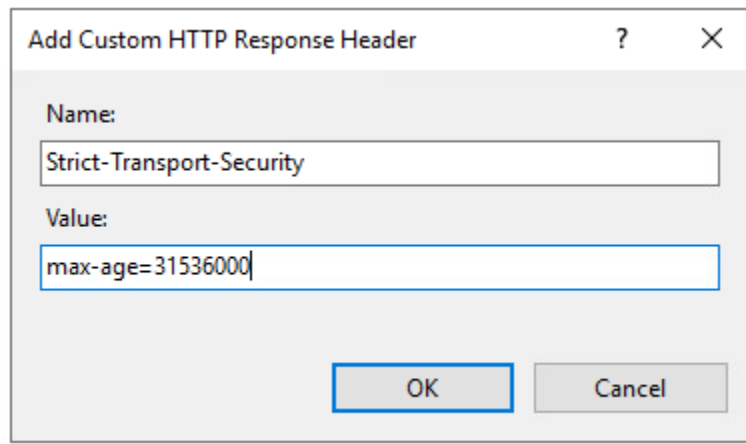
Disable Default.htm

3. From the **Connections** navigation pane, select **Default Website**, and then double-click **HTTP Response Headers**.



HTTP Response Headers option

4. From the **Actions** section, click **Add**.
5. In the **Add Custom HTTP Response Headers** dialog box, perform the following actions:
 1. In the **Name** field, type `Strict-Transport-Security`.
 2. In the **Value** field, type `max-age=31536000`.



The screenshot shows a dialog box titled "Add Custom HTTP Response Header". It has two text input fields: "Name:" and "Value:". The "Name:" field contains the text "Strict-Transport-Security". The "Value:" field contains the text "max-age=31536000". At the bottom right, there are two buttons: "OK" and "Cancel". The "OK" button is highlighted with a blue border.

Add Custom HTTP Response Headers dialog box

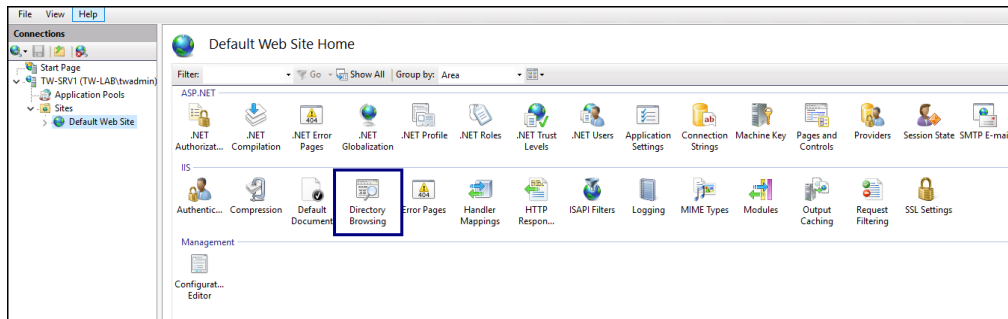
3. Click **OK**.
6. Close **IIS Manager**.

4.1.7 Enabling Directory Browsing in IIS

Confirm that Directory Browsing is enabled.

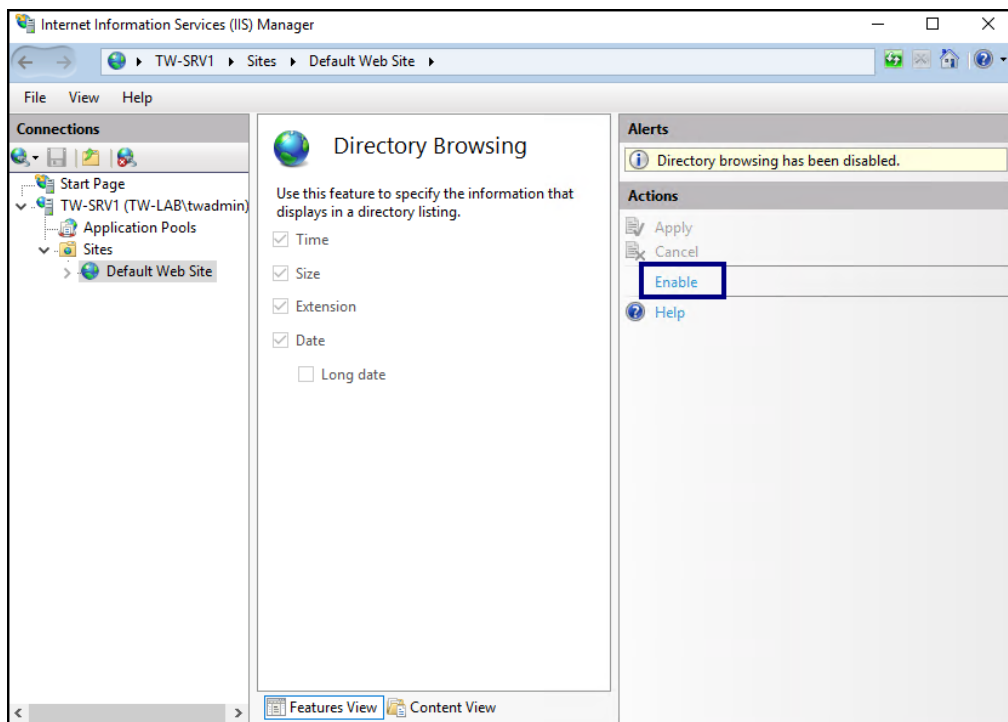
Perform the following steps in **IIS Manager**.

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



Directory Browsing option

2. On the **Directory Browsing** page, review the **Actions** pane. If the message *Directory browsing has been disabled* appears, click **Enable**.



Enable Directory Browsing

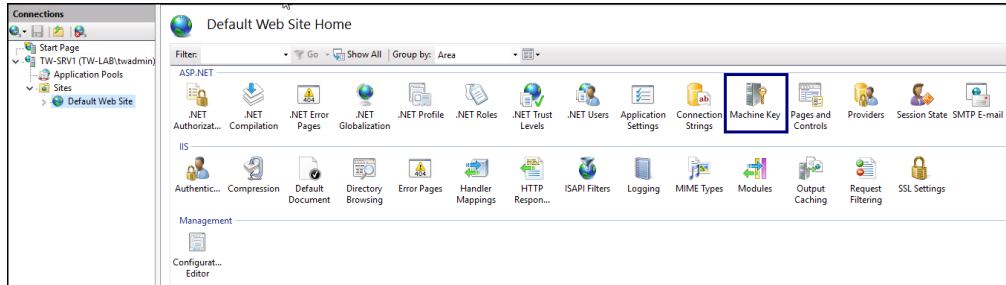
3. Leave the remaining options with their default selections and close **IIS Manager**.

4.1.8 (HA Deployments Only) Generating Machine Keys

Generate and synchronize machine keys in IIS Manager to ensure consistent encryption and validation across all NES API servers.

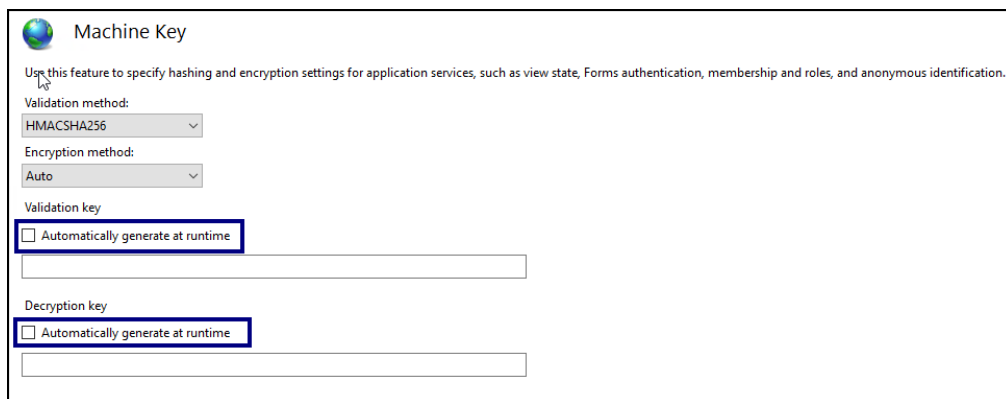
Perform the following steps in **IIS Manager** on the first NES API that you deploy.

1. Expand *Computer_Name* > **Sites**, select **Default Web Site**, and then double-click **Machine Key**.



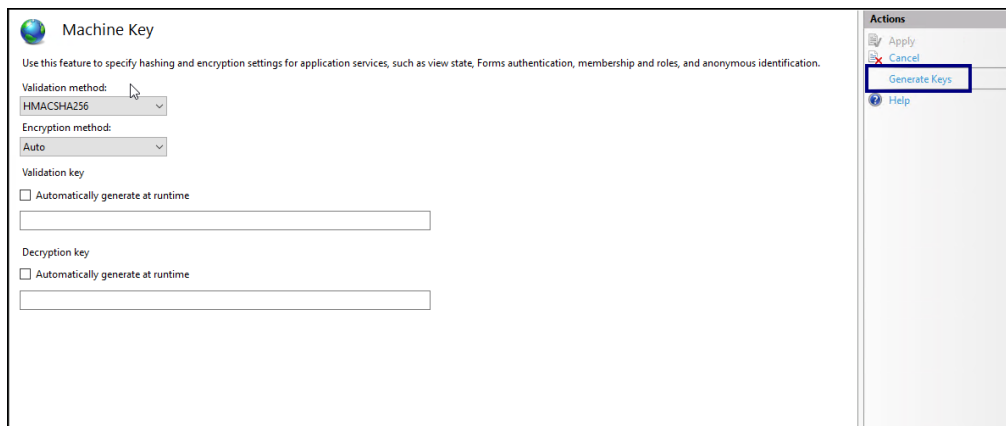
Machine Key option

2. On the **Machine Keys** window, clear both **Automatically generate at runtime** options.



Clear auto-generate options

3. In the **Actions** pane on the right side of the window, click **Generate Keys**.



Generate Keys

4. Copy the Validation Key and Decryption Key to a text file.
5. Click **Apply** to save the generated keys.
6. Restart the IIS service.
7. Perform the following steps in **IIS Manager** on each remaining NES API server:
 1. Expand *Computer_Name* > **Sites**, select **Default Web Site**, and then double-click **Machine Key**.
 2. On the **Machine Keys** window, clear both **Automatically generate at runtime** options.
 3. In the **Validation Key** field, paste the Validation Key value from the first server.
 4. In the **Decryption Key** field, paste the Decryption Key value from the first server.
 5. Click **Apply** to save the generated keys.
 6. Restart the IIS service.

4.2 Importing a Fullchain Certificate

To support certificate management in CWP, 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.

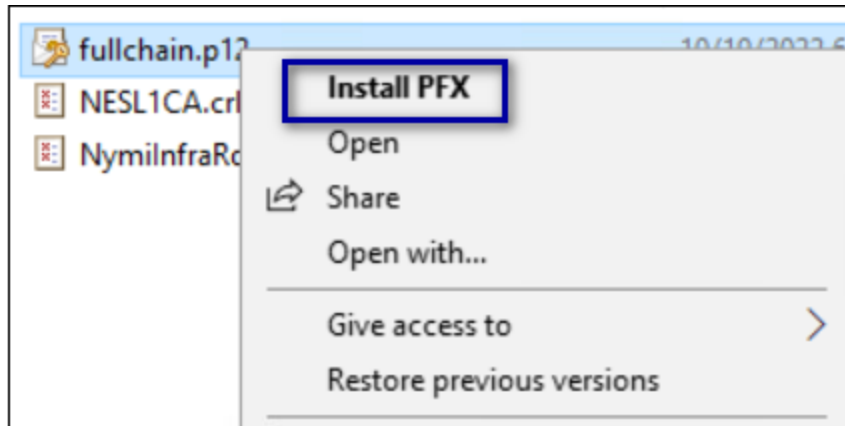
The PKCS12 file (`fullchain.p12`) contains the following certificates:

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

4.2.1 Importing Certificates

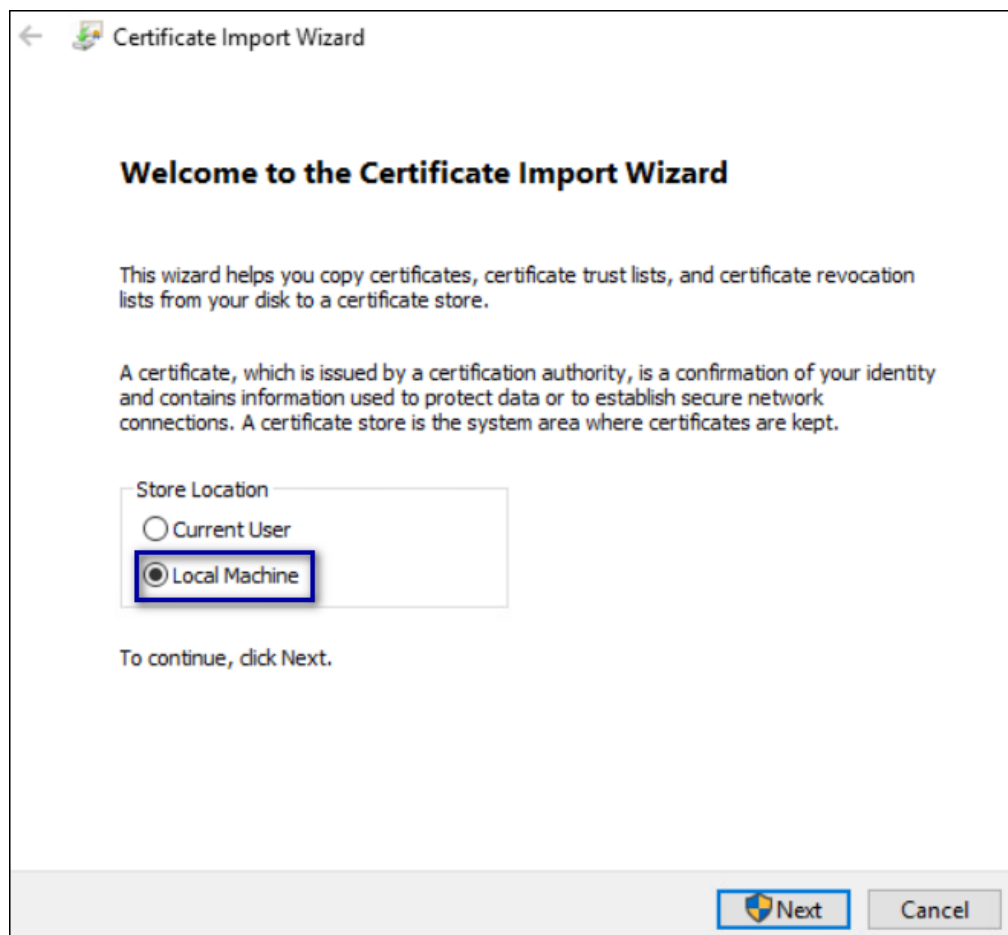
Perform the following steps to import the certificates on the NES host.

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



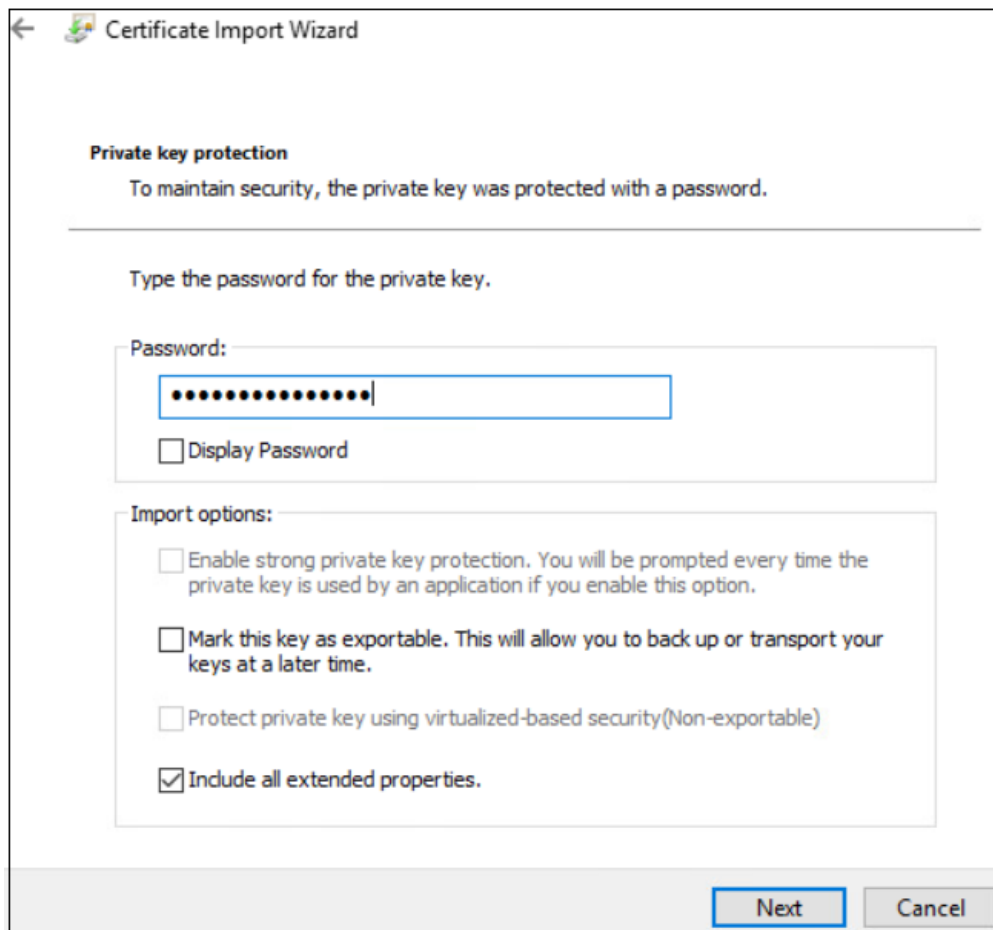
Install PFX option

3. In the **Open File - Security Warning** dialog, click **Open**.
4. On the **Welcome to the Certificate Import Wizard** page, in the **Store Location** section, select **Local Machine**.



Local Machine Store Location

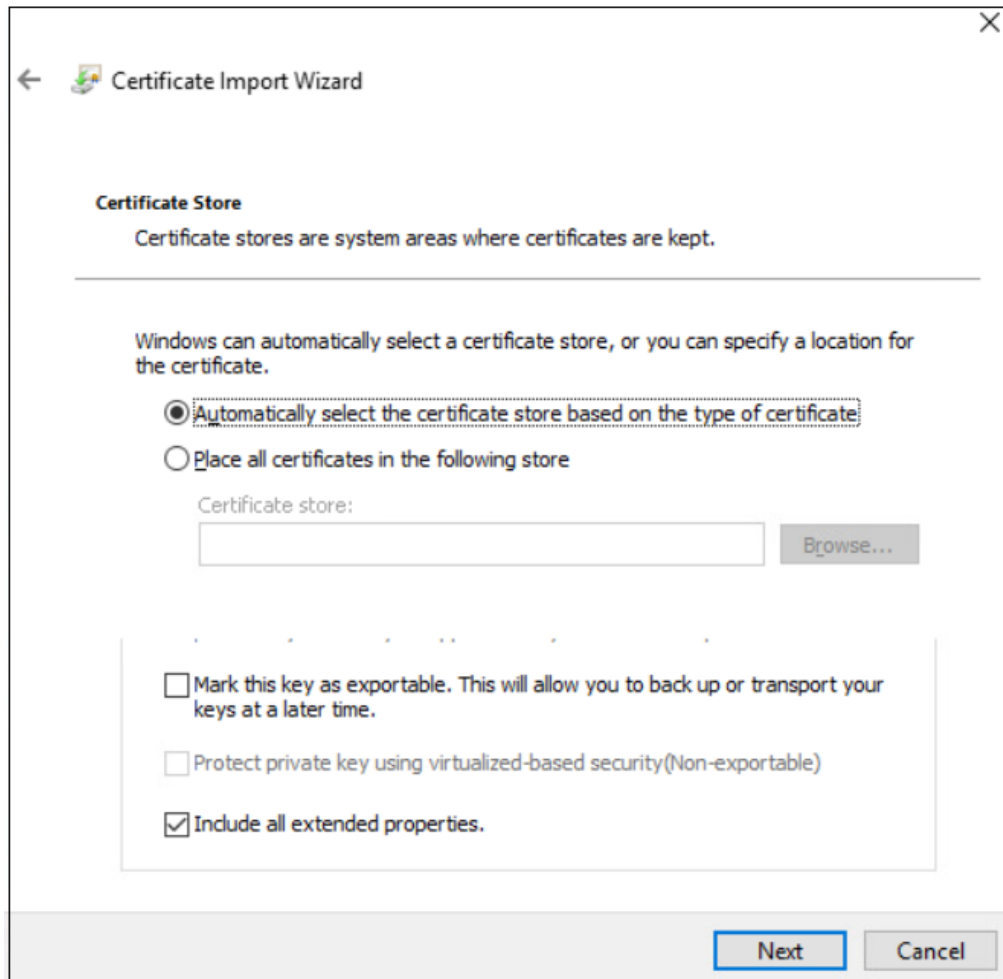
5. Click **Next**.
6. On the **User Account Control** window, click **Yes**.
7. On the **Files to import** page, ensure that the `fullchain.p12` file appears in the **File name** field, and then click **Next**.
8. On the **Private Key Protection** page, in the **Password** field, type the Nymi-provided private key password, and then click **Next**.



The image shows the 'Certificate Import Wizard' window, specifically the 'Private key protection' page. The window has a title bar with a back arrow and the text 'Certificate Import Wizard'. The main content area is titled 'Private key protection' and contains the text 'To maintain security, the private key was protected with a password.' Below this, it says 'Type the password for the private key.' There is a 'Password:' label followed by a text box containing 12 dots. Below the text box is a checkbox labeled 'Display Password'. Underneath is the 'Import options:' section, which contains four checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (unchecked), 'Protect private key using virtualized-based security(Non-exportable)' (unchecked), and 'Include all extended properties.' (checked). At the bottom right of the window are 'Next' and 'Cancel' buttons.

Private Key Protection page

9. 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 option ensures all the certificates in the certification path (Root, Intermediate) are placed in the correct store.



Certificate Store page

10. On the **Completing the Certificate Import Wizard** page, click **Finish**.
11. On the **Certificate Import Wizard** dialog, click **OK**.

4.2.2 Moving the L2 Certificate

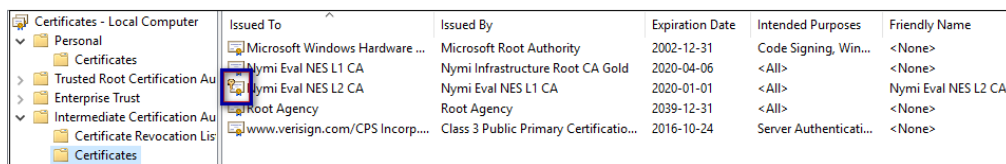
Perform the following steps to move the L2 certificate from the Personal Certificates folder to the Intermediate Certification folder.

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.

- 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.

Certificates window
Certificates window

- In **Intermediate Certification > Certificates**, verify that the 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.



L2 Certificate with key

- Record the expiration date of the NES L2 CA certificate (shown in the Expiration Date column) in the *Certificate Expiration Dates* table.
- Close the **certlm** window.

4.3 Install 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.

4.3.1 Installing the NES Services Suite Using the Wizard

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

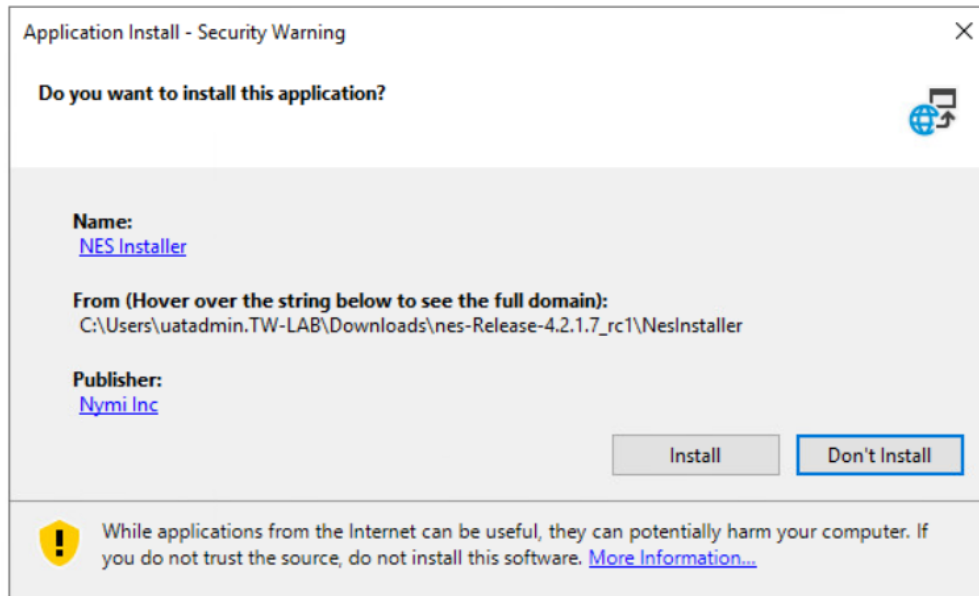
For the best user experience with the NES installation wizard, use display settings that include a resolution of 1920 x 1080 and 100% scaling.

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.

1. Log in to the host with a domain user account that has local administrator rights.
2. In the `C:\nestemp\NesInstaller` folder, run `install.exe`.

Note: If the account that you used to log into the host is not the Nymi Infrastructure Service Account and the deployment uses a remote SQL server, run the `install.exe` with the Nymi Infrastructure Service Account or an account that is owner of the NES SQL database.

3. If you see the **User Account Control** dialog, click **Yes**.
4. If you see 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. If you see 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. If you see the **Open File - Security Warning** dialog, click **Run**.
10. On the **Application Install Security Warning** pop-up, click **Install**.



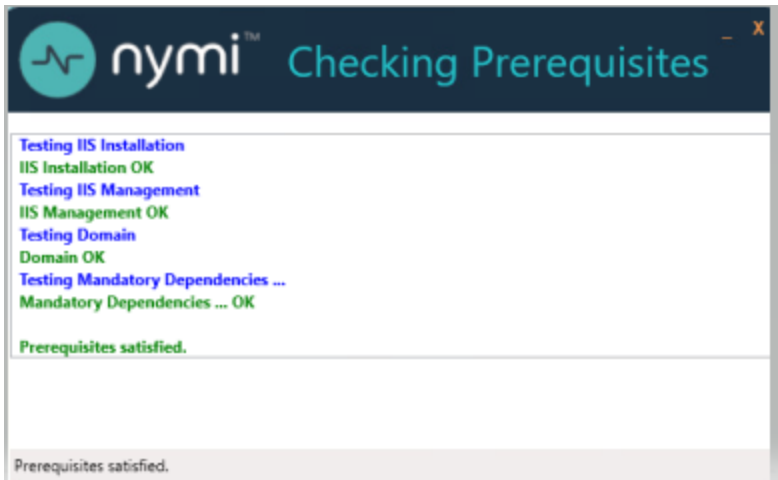
Security Warning

11. If you see the **Open File – Security Warning** page, click **Run**.
12. If you see the **User Account Control** dialog, click **Yes**.
13. If the installer does not detect a version of SQL Express on the host, the **Install Prerequisites** dialog appears. Perform one of the following actions:
 - To install SQL Express on the NES server, click **Yes**.
 - To use an existing instance of SQL server on this machine or on another machine, click **No**. When you configure NES in the following section, you provide connection information for the remote SQL Server.

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

- If the prerequisite 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.



Prerequisites Check Dialog

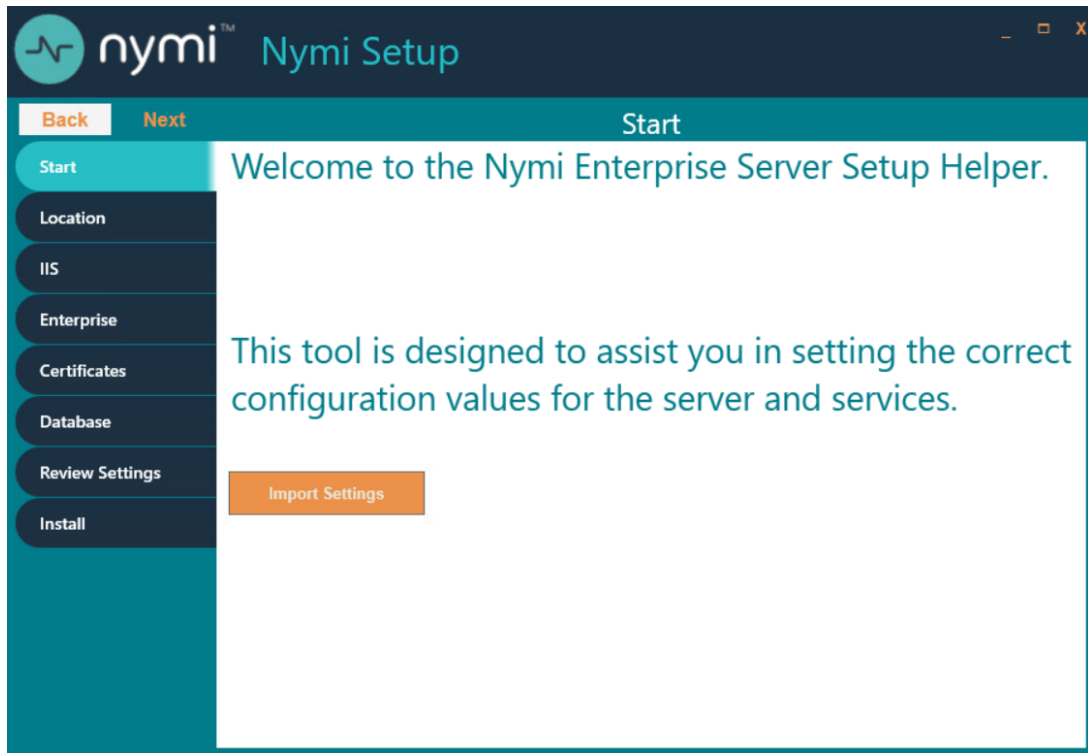
Note: If you see an error message indicating that the installer was not run with a domain user, you did not run the installer under a domain user account. To resolve this, you must go to **Add or Remove Programs** and uninstall **Microsoft SQL Server**. When prompted to select the features to remove,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

4.3.2 Configuring NES Services Manually

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

Note: For HA deployments, you will manually configure the NES API on the first server only. For the remaining NES API servers, you will use the **Import Settings** button to load a configuration file, which includes all the NES API configuration settings from the first NES API server.

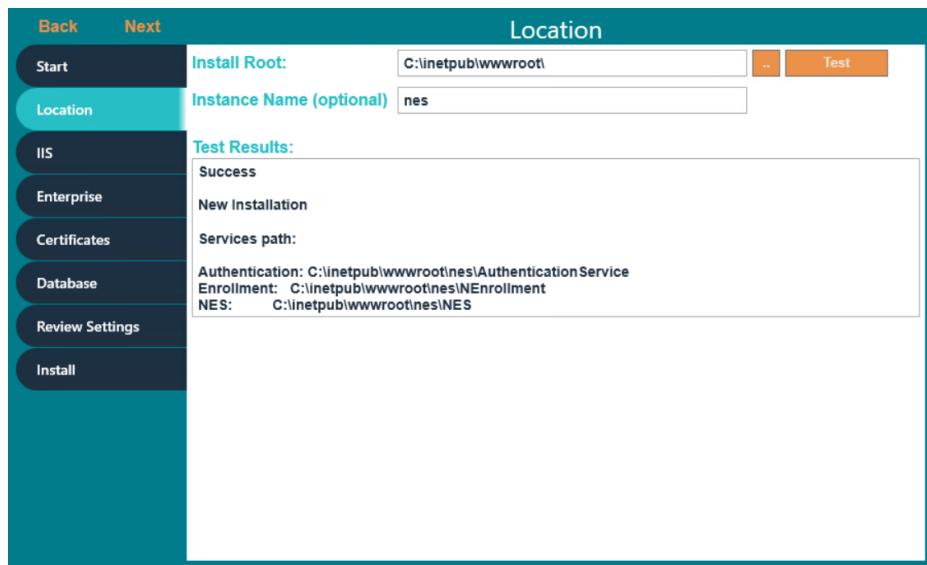
The following figure provides an example of the NES Setup wizard.



NES Setup Help wizard

Perform the following actions to configure the NES Services Suite.

1. In the left navigation pane, select **Location**, and then perform the following actions:
 1. In the **Install Root** field, leave the default location `C:\inetpub\wwwroot` or, to select an alternate installation path, click the ellipses and navigate to the folder.
 2. In the **Instance Name** field, type a descriptive name for the NES web application instance name, for example `NES`. This step is optional but recommended. The name cannot contain spaces.
 3. 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.



Location page in the NES Setup wizard

2. In the left navigation pane, click **IIS**, and then perform the following actions:
 1. 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.
 2. For HA deployments only, in the **Key Management** section, click **Copy**, and then paste and save the value securely. You will confirm that this value matches on the other NES API servers later.
 3. In the **Communication Protocol** section, available IIS site bindings appear. Select a communication protocol for the deployment. Nymi recommends that you select HTTPS to ensure secure communication. HTTPS is required for CWP with Evidian deployments. If an HTTPS address is not available, review *Adding HTTPS site bindings* to add a HTTPS site binding.

Note: HTTP is not encrypted. Sensitive information is sent in plain text.
 4. In the **NES Admin and Enrollment Application Service** and **Authentication Service** sections, perform the following actions, based on your configuration scenario:

Scenario	NES Admin and Enrollment Application Service Configuration	Authentication Service Configuration
Single NES instance and remote SQL server that uses Windows Authentication	1. In Application Pool, leave the default application pool. 2. From the Application Pool Identity list: a. Select SpecificUser from the drop-down list. b. In the User Name field, type the username of the Nymi Infrastructure Service Account in the format <code>domain\username</code>. c. In the Password field, type the password for the Nymi Infrastructure Service Account. 3. Click the Test button to validate the user credentials.	1. From the Application Pool list, select NES_AS App Pool. 2. From the Application Pool Identity list, select Network Service.
Multiple NES instances in a high-availability configuration, remote SQL Server	1. In Application Pool, leave the default application pool. 2. From the Application Pool Identity list: a. Select SpecificUser from the drop-down list. b. In the User Name field, type the username of the Nymi Infrastructure Service Account in the format <code>domain\username</code>. c. In the Password field, type the password for the Nymi Infrastructure Service Account. d. Click the Test button to validate the user credentials.	1. From the Application Pool list, leave the default application pool. 2. From the Application Pool Identity list: a. Select SpecificUser from the drop-down list. b. In the User Name field, type the username of the Nymi Infrastructure Service Account in the format <code>domain\username</code>. Note: Ensure that you specify the same user account that you provided for the NES Admin and Enrollment service configuration. If you specify a different user, both application pools use the username that you specify for the Authentication service configuration. c. In the Password field, type the password for the Nymi Infrastructure Service Account. d. Click the Test button to validate the user credentials. Note: A message appears warning you that the implementation requires Service Principle Names (SPNs).

Scenario	NES Admin and Enrollment Application Service Configuration	Authentication Service Configuration
Local SQL configuration (SQL Express) or SQL server that uses SQL Authentication	In the Application Pool and Application Pool Identity , leave the default selections.	In the Application Pool and Application Pool Identity , leave the default selections.

5. 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 that run on the server.

6. For environments where user terminals connect to the NES API with an FQDN that differs from the FQDN of the NES API server, in the **Load Balancer URL Mappings** section:
 1. In the **Authentication Service External URL** field, specify the load balancer URL in the format `https://NES_loadbalancer_url/instance_name_AS`.
 2. In the **NES Admin External URL** field, specify the load balancer URL in the format `https://NES_loadbalancer_url/instance_name`.
 3. In the **Enrollment Service External URL** field, specify the load balancer URL in the format `https://NES_loadbalancer_url/instance_name_ES`.

Back

Next

IIS

Start

Location

IIS

Enterprise

Certificates

Database

Review Settings

Install

IIS web site:

Default Web Site

Service Mappings

Authentication:

NES_AS

Nes Admin:

NES

Enrollment:

NES_ES

Key Management

Token Signing Key:

.....

Copy

Edit

Communication Protocol

☒ HTTPS
 ☐ HTTP

NES Admin and Enrollment Service

Application Pool:

Nes App Pool

Application Pool Identity:

SpecificUser

NES uses this account to connect to the SQL server.

User Name:

tw-lab.local\uatadmin

Password:

.....

Test

User Credentials Validated

Authentication Service

Application Pool:

NES_AS App Pool

Application Pool Identity:

NetworkService

Load Balancer URL Mappings

Authentication Service External URL:

https://loadbalancer.url

Nes Admin External URL:

https://loadbalancer.url

Enrollment Service External URL:

https://loadbalancer.url

IIS Setup page in the NES Setup wizard

3. In the left navigation pane, click **Enterprise**, and perform the following actions:
 1. In the **LDAP protocol** section, select LDAP or LDAPS.

2. In the **Domains** table, the domain in which the NES host resides appears. If Nymi Band users, NES Administrators, or the NES service account reside in other domains, perform the following steps to add the additional domains:
 1. In the **Domain** table, on an empty line, type the NetBIOS (Pre-Windows 2000) name of the domain that contains the user accounts.
 2. Type a domain username and password for the domain if one of the following conditions are met: the domain is not in the same forest as the NES API domain; a two-way trust does not exist between the domain and the domain in which NES resides; or the domain is not in the same forest as the NES API domain and does not have a two-way trust with the domain in which the NES API service account resides.
Note: Select a domain user whose password never expires.
 3. Press **Enter**.
 4. Press **Test** to confirm that NES API can reach all domains.
3. Optionally, in the **Max Password Age** field, specify the password expiration interval in days that your password policy enforces for your user accounts.

Note: Consider defining a **Max Password Age** value if you will configure the NES API policy to require the NEA to check the status of the user account when a user performs a Nymi Band tap. In the event that NES API contacts AD to confirm that the validity of the account, and AD returns an *Invalid Max Password Age* message, NES API uses the **Max Password Age** value to determine when the password expires. If the password expiration period has not been reached or exceeded, NES API allows the Nymi Band tap operation to complete.
4. In the **Nes Admin Groups** table, specify the NES Administrator group name by right-clicking in the field, selecting **Add**, and then typing the name of the group. In a multi-domain configuration where you have configured multiple global NES Administrator groups in different domains, add each group.
5. Press **Test** to confirm that NES API can find each defined group.
6. If the solution includes user terminals with Nymi Lock Control, in the **NES API Authorization Based on Organizational Unit (Optional)** table, perform one of the following actions: to restrict the user terminals on which users can use Nymi Lock Control, specify the OU name (if your organization has multiple OUs of the same name, specify the entire DN of the OU); to

allow users to use Nymi Lock Control on any user terminal, leave the table empty.

7. Press **Test** to confirm that NES can find each defined OU.
8. In the **Nymi Infrastructure Service Account** section, in the **User Name** field, enter the account in the format `domain\name`.

Enterprise

LDAP Protocol

☒ LDAP

☐ Secure LDAP (LDAPS)

Domains:

Domain	Account	Password
TW-Lab.local		

Test

Test Domains Result

Success - all domains are found.

Max Password Age:

30

NES Admin Groups:

Group Name
nesadmins
Please enter NES Admin Group Name

Test

Test NES Admin Groups Result

Success - all groups are found.

NES API Authorization based on Organizational Unit (Optional):

Organizational Unit Name
office
Please enter Organizational Unit

Test

Test OU Result

Success - all OUs are found.

Nymi Infrastructure Service Account:

User Name:

tw-lab\nymmi_infra_service

Test

The Service Account has been successfully validated.

Enterprise Settings page in the NES Setup wizard

4. In the left navigation pane, click **Certificates**, and then perform the following actions:
 1. From the **Level One Certificate** list, select the L1 certificate.
 2. From the **Level Two Certificate** list, select the L2 certificate.
 3. From the **Full Chain** list, click the ellipses (...) and navigate to the folder that contains the Full Chain PFX certificate file, and then select the file.
 4. In the **Password Required** pop-up, type the Full Chain certificate password, and then click **OK**.

Back	Next	Certificates
Start		Certificate Issuing Method: Nymi Token Service (NTS)
Location		Certificate Expiry (In Days): 90
IIS		Level One Certificate: dev-AD01-CA
Enterprise		Level Two Certificate: dev-AD01-CA
Certificates		Full Chain Certificate: fullchain.p12
Database		
Review Settings		
Install		

Certificates page in the NES Setup wizard

5. In the left navigation pane, click **Database**. Configure the database settings based on your authentication method:

- **Windows Authentication:**

1. Leave the **Integrated Security** option selected.
2. If required, update the connection string with the database instance that you want to use.
3. Click **Test** to verify the connection.

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

4. In the **Manage Database Logins** section, click **Verify Users** to ensure that NES can create users with access to the SQL database. The table displays the default account settings, application pool identity, and service type login.

◦ **SQL Authentication:**

1. Clear the **Integrated Security** option. This sets the security property in the Connection String to False.
2. If required, update the connection string.
3. In the **SQL Login** section, enter the username and password, and then click **Verify**.
4. Click **Test** to verify the connection.

Database

Connection String:

☒ Integrated Security

Data Source=.;Initial Catalog=Nymi.{0};Integrated Security=True;MultipleActiveResultSets=True

Test

Test Connection String Result:

Server Connected, Database does NOT Exist

Manage Database Logins:

The service account is used by NES to access the database. The auditor account can be used to retrieve information from the NES database. When editing or adding logins, the domain account can be a user account or group account. Additionally, individual user accounts can be created to provide full access to the database.

Type	Login	User	Status
Service	NT AUTHORITY\SERVICE	Service_DbUser	Exists in DB

Verify Users

Verify Users Result:

No Errors Found.

Database page in the NES Setup wizard

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

1. Click **Test** to verify the configuration. Review the test results and address any errors.

Common warnings:

Error	Resolution
SelectedSiteBindings: The underlying connection was closed: Could not establish a trust relationship for the SSL/TLS secure channel.	Import the TLS certificate as described in the <i>Importing the TLS server certificates</i> section, and retry.
Error in 'Fullchain Certificate Path': PKCS12 Keystore MAC invalid - wrong password or corrupted file.	The password for the Fullchain certificate is incorrect, or the wrong file was selected. From the Full Chain list, click the ellipses (...) and navigate to the folder that contains Full Chain PFX certificate file, and then select the file. In the Password

Error	Resolution
	Required pop-up, type the Full Chain certificate password, and then click OK .

Review Settings

Nes Admin:

Description	Value
Application Pool	Nes App Pool
Application Pool Identity	NetworkService
Application Pool Identity User Nam	
Authentication Service Web Page	https://tw-srv1.tw-lab.local/nas_AS
Computer OU Names	office
Enable HTTP	False
Enable Secure LDAP (LDAPS)	False
Enrollment Service Web Page	https://tw-srv1.tw-lab.local/nas_ES
Full Chain Certificate Path	~/APP_DATA/Keystore/fullchain.p12
Nymi Infrastructure Service Account	tw-lab\nymmi_infra_service
Service Binding	https://tw-srv1.tw-lab.local/nas
Sql Connection String	Data Source=.\SQLEXPRESS;Initial Catalog=Nymi.nes;Integrated Security=True;MultipleActiveResultSets=True

Authentication:

Description	Value
Application Pool	Nes App Pool
Application Pool Identity	NetworkService
Application Pool Identity User Nam	
Authentication Provider	AuthenticationProviders.dll\ADAuthenticationProvider,TW-Lab.local
Enable HTTP	False
Enable Secure LDAP (LDAPS)	False
Firmware Console Admin Group	
Firmware Console User Group	
Nes Admin Group	nesadmins
Service Binding	https://tw-srv1.tw-lab.local/nas_AS
Token Life Span	00:30:00

Enrollment:

Description	Value
Certificate Expiry	90.00:00:00
Enable HTTP	False
Enable Secure LDAP (LDAPS)	False
Issue Certificates using NTS	True
L1 Certificate CN	Nymi Eval NES L1 CA
L2 Certificate CN	Nymi Eval NES L2 CA
NES Service Web Page	https://tw-srv1.tw-lab.local/nas
Service Binding	https://tw-srv1.tw-lab.local/nas_ES

Test

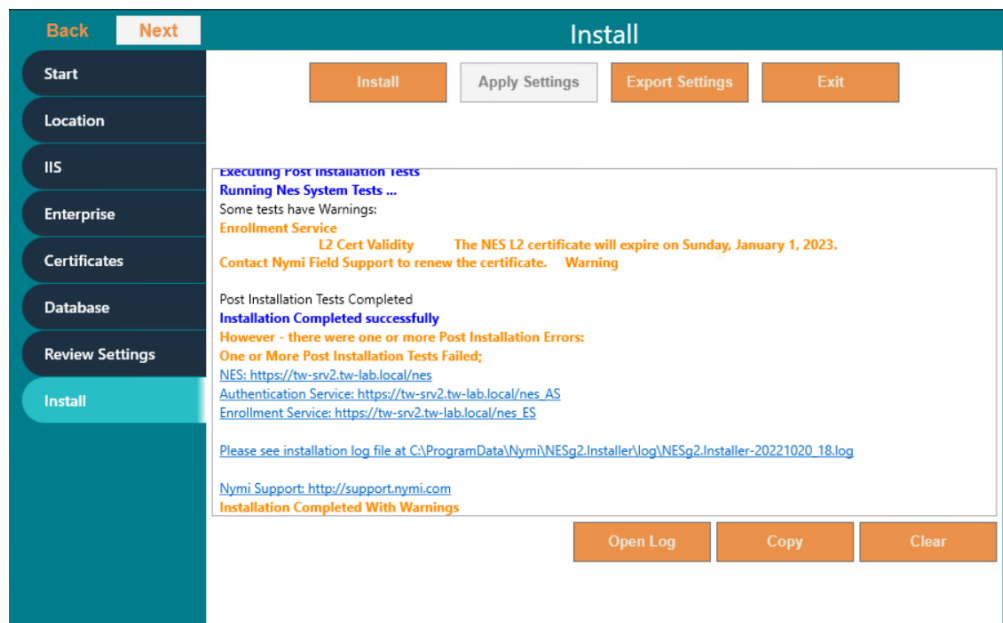
Success

Review Settings page in the NES Setup wizard

7. In the left navigation pane, click **Install**. The Install page provides the following 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.

Button	Description
Exit	Exit installation wizard without installing NES.



Install page in the NES Setup wizard

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

Note: If the NES installation fails with the error message “Cannot Allow Access to certificate”, additional troubleshooting actions are required for the fullchain certificate. Save the NES configuration using **Export Settings** and close the installer. Delete the L1 and L2 certificates from the intermediate certificate authority, re-import the fullchain certificate, move the L2 certificate to the intermediate certificate store, and re-run the installer using the saved configuration file.

4.3.3 Deploying the NES URL to User Terminals by Using Group Policies

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

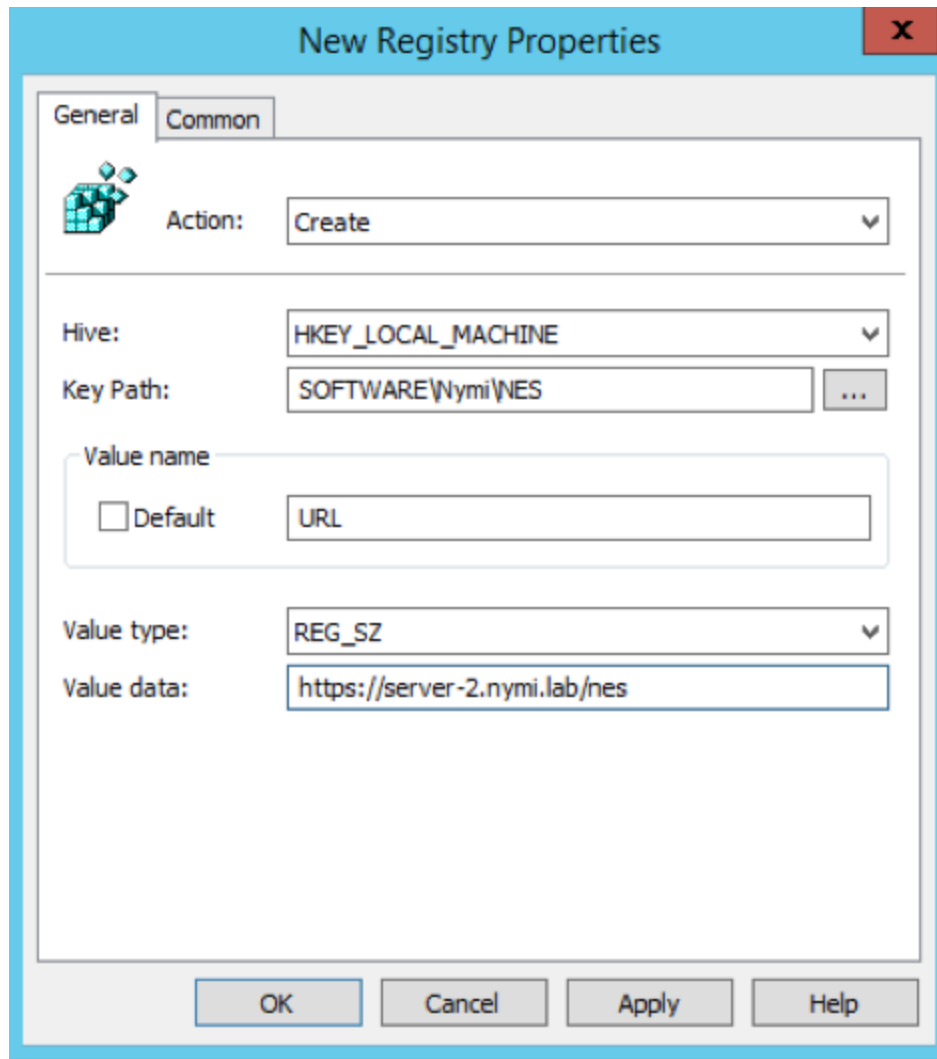
The user that creates the group policy requires domain administrator rights. Create a group that contains all the user terminals that require this change.

- 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:
 1. Select **Authenticated Users**.
 2. Click **Remove**.
 3. On the confirmation and warning windows, click **OK**.
 4. Click **Add**.
 5. 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**.
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**.
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** field, type `URL`.
15. In the **Value type** list, leave the default selection **REG_SZ**.
16. In the **Value Data** field, type `https://nes_server/NES_service_name/`

Where:

- `nes_server` is the FQDN of the NES host.
- `NES_service_name` is the name of the service mapping for NES in IIS.



URL properties page

17. Click **OK**.

4.3.4 Deploying the Nymi Agent URL to User Terminals by Using Group Policies

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

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

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**, remove **Authenticated Users** and add the group that contains the user terminals (same process as above).
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**.
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** field, type `AgentUrl`.
15. In the **Value type** list, leave the default selection **REG_SZ**.
16. 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.

17. Click **OK**.

4.3.5 Saving the NES Configuration

The NES Setup wizard provides you with the ability to save the NES API configuration to a file. The configuration file allows you to perform a silent installation of the NES API host. For HA deployments, you must save the configuration of the first NES API server to a file.

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:
 - In the **File Name** section, click the ellipses and navigate to the location where you want to save the configuration file. Type the file name and click **Save**. The configuration file is saved as a `.ninst` file.
 - In the **Encryption** section, select one of the following options:
 - **None** — save without encrypting sensitive information.
 - **Machine** — save with machine-specific encryption (configuration file can only be loaded on the same machine).
 - **Private key** — encrypt with a private key (allows loading on a different machine). To create a new private key file, click **New**, navigate to the save location, type the file name, and click **Save**. The key file is saved as a `.key` file.
 - Click **OK**.

4.3.6 (HA Deployments) Configuring Additional NES Servers from a Configuration File

For an HA configuration, after you complete the first NES API server deployment with the NES Setup wizard, configure the additional NES servers with the `.ninst` file that you created.

You can configure additional NES API servers from the command line or with the NES Setup wizard.

4.3.6.1 Configuring NES Silently from the Command Line

Before you perform a silent installation of 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 in the following directory: `..\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.
- To use an `ninst` file that you created before CWP 1.12.2, you need to perform several modifications to the file:

- Create a new entry for the Nymi Infrastructure Service Account.
- Create a new entry for the Fullchain certificate password.
- Add the following entry that appears in the sample `.ninst`:

```
"PFXFullChainPath": "~/APP_DATA/Keystore/fullchain.p12"
```

Note: Do not modify the path value for this entry, but if required, change the fullchain filename to match the name of the certificate file that Nymi provided you.

The sample `.ninst` file located in the NES installation package in the `NesCmdInstall` folder provides you with information about the new entries.

To install NES using the silent installer:

1. Copy the `.ninst` file 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 the `C:\nestemp\nes-Release-x.x.x.x\NesCmdInstall` directory.

3. Type the following command:

```
NesCmdInstall.exe --fullchain <path_to_fullchain_cert\cert_filename> --
```

Where:

- *path_to_fullchain_cert* is the absolute or relative path to the Nymi-provided fullchain PFX certificate file.
- *cert_filename* is the name of the Nymi-provided fullchain PFX certificate file.
- *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.
- *key_filename* is the name of the private 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:\ProgramData\Nymi\NesCmdinstall\log`. The installation process provides output to the screen as well as installation log files.

4.3.6.2 Configuring NES with a Configuration File in the NES Setup Wizard

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 file. A **Loaded Successfully** message appears on the screen.
3. In the left navigation pane, click **IIS**, in the **Key Management** section, click the **Eye** icon to display the Token Signing key. Confirm that the value matches the value that you copied from the first NES API install.

If the value does not match:

- a. Click **Edit**, and then copy and paste the value from the first NES API install.

- b. Click **Test** to confirm that the value is valid. If the test fails, use the **Eye** icon to display the Token Signing key and confirm that the value is correct and does not contain a space before and after the value.
4. If you used a `ninst` file that was created prior to CWP 1.12.x, perform the following actions:
 - a. In the left navigation pane, click **Enterprise**, scroll down to the **Nymi Infrastructure Service Account** section. In the **User Name** field, enter the Nymi Infrastructure Service Account in the format `domain\name`.
 - b. In the left navigation pane, click **Certificates**, and perform the following actions.
 - c. From the **Full Chain** list, click the ellipses (...) and navigate to the folder that contains the Full Chain PFX certificate file, and then select the file.
 - d. In the **Password Required** pop-up, type the Full Chain certificate password, and then click **OK**.
5. 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.
6. If the Review Settings test did not report errors, on the **Install** tab, click **Install**.
7. When the installation completes, close the NES Setup wizard.

4.4 Configuring IIS to Prevent NES Offloading

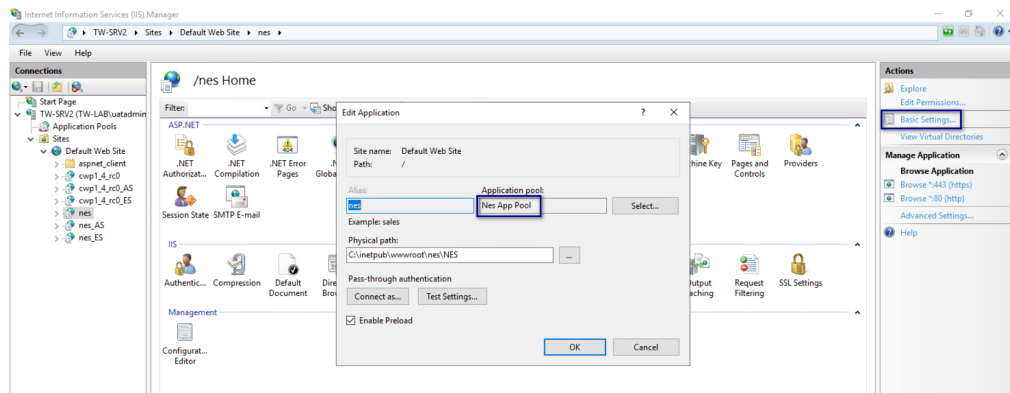
Configure IIS to ensure that NES applications are always available to service requests, and not offloaded.

Perform the following steps in **IIS Manager**.

1. In the **Connections** navigation pane, expand *Computer_Name* > **Sites** > **Default Web Site**, and then perform the following steps to determine the application pool name for each NES application.
 - a. Select the **nes** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.

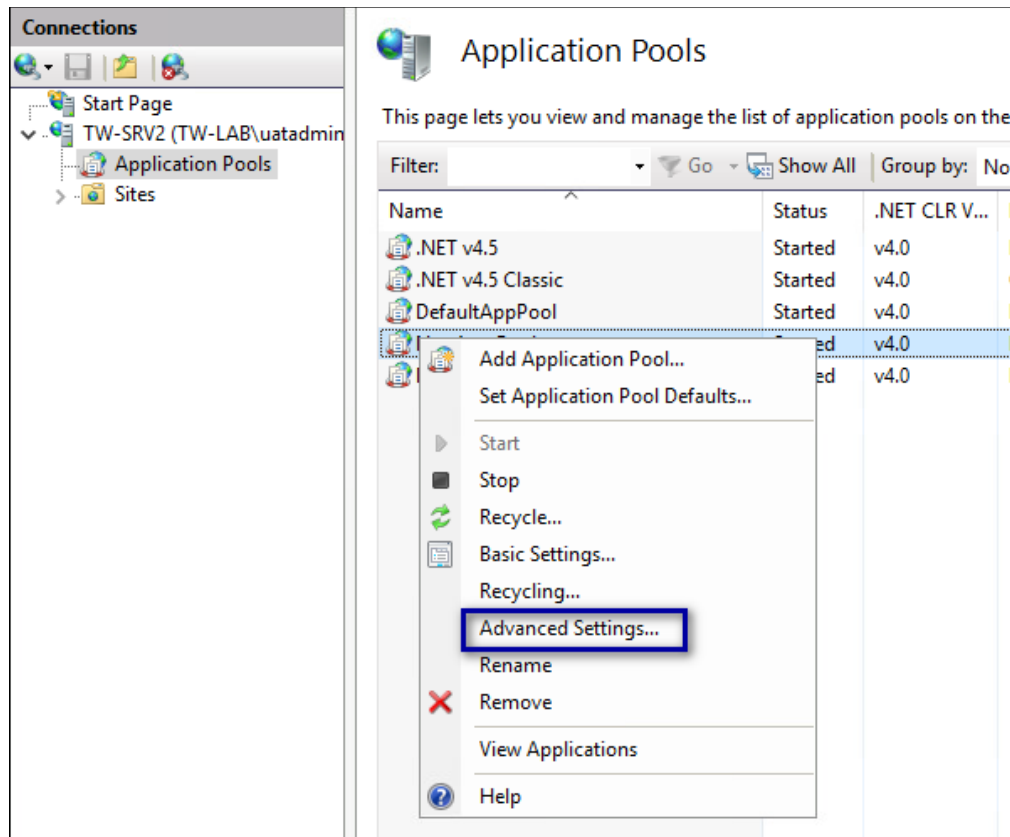
- b. In the **Edit Application** window, make note of the value that appears in the **Application Pool** field, and then click **OK**.
- c. Select the **nes_AS** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.
- d. In the **Edit Application** window, make note of the value that appears in the **Application Pool** field, and then click **OK**.
- e. Select the **nes_ES** application, and then in the **Actions** menu on the right side of the window, select **Basic Settings**.
- f. In the **Edit Application** window, make note of the value that appears in the **Application Pool** field, and then click **OK**.

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



Edit Application window

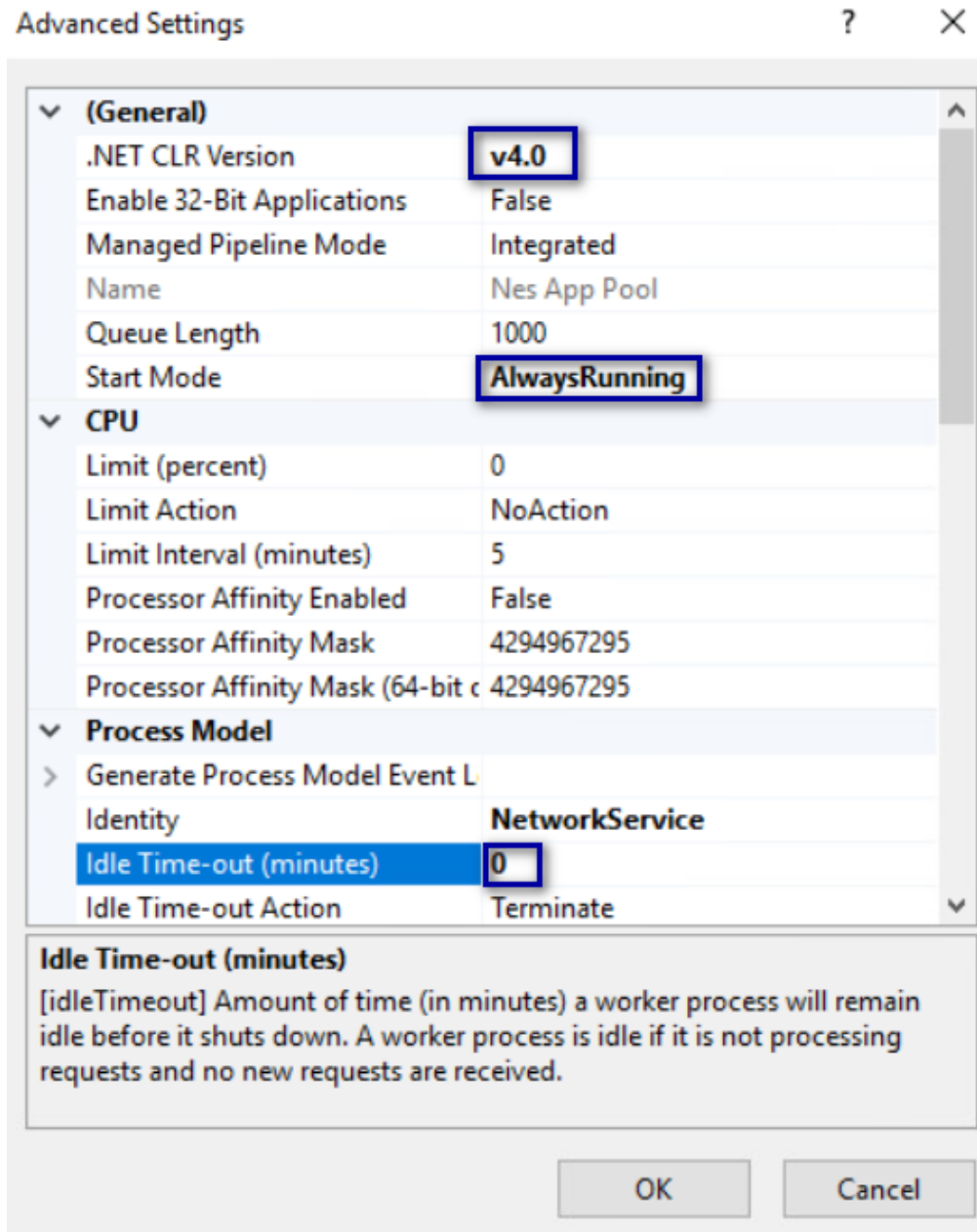
2. In the **Connections** navigation pane, expand *Computer_Name* > **Application Pools**, right-click the application pool for the NES applications, and then select **Advanced Settings**, as shown in the following figure.



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**.

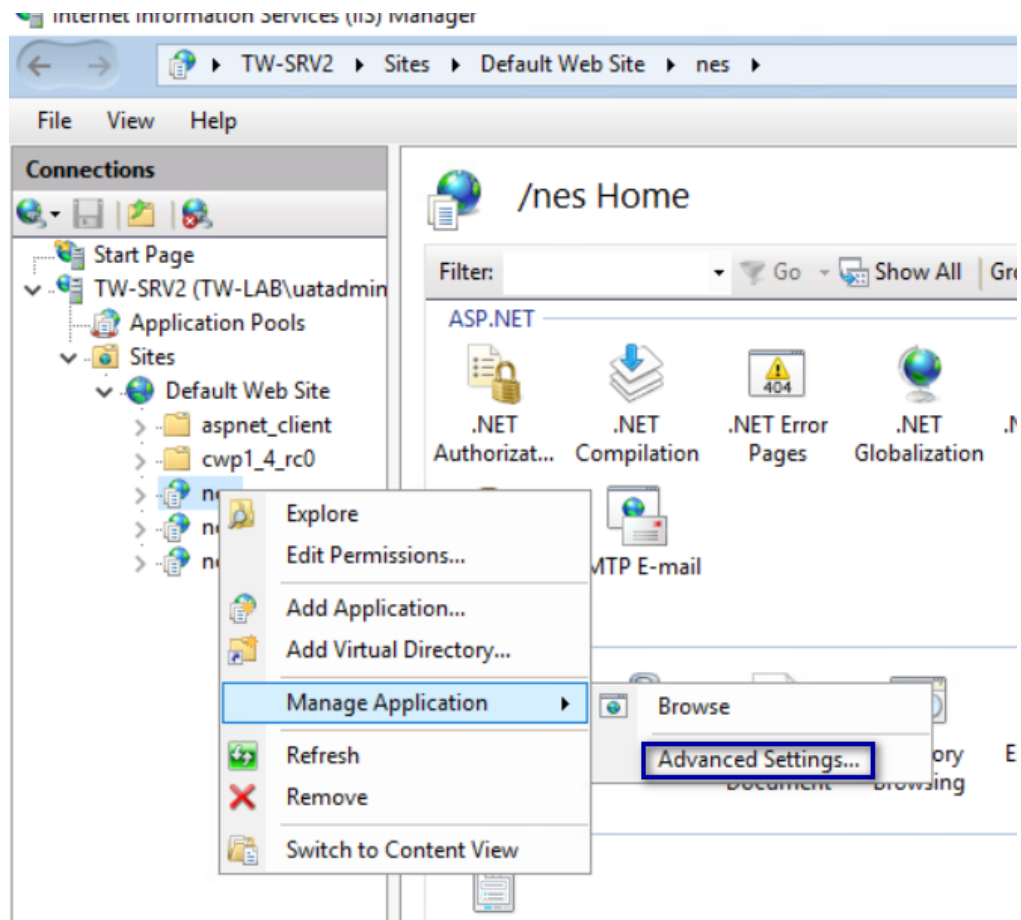
The following figure provides an example of the **Advanced Settings** window.



Advanced Settings window

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

4. In the **Connections** navigation pane, expand *Computer_Name* > **Sites** > **Default Web Site**, and then perform the following steps.
 - a. Right-click **nes** and then select **Manage Application** > **Advanced Settings**, as shown in the following figure.



Advanced Settings option

- a. On the **Advanced Settings** window, from the **Preload Enabled** list, select **True**.
- b. Click **OK**.
- c. Right-click **nes_AS** and then select **Manage Application > Advanced Settings**.
- d. On the **Advanced Settings** window, from the **Preload Enabled** list, select **True**.
- e. Click **OK**.
- f. Right-click **nes_ES** and then select **Manage Application > Advanced Settings**.
- g. On the **Advanced Settings** window, from the **Preload Enabled** list, select **True**.

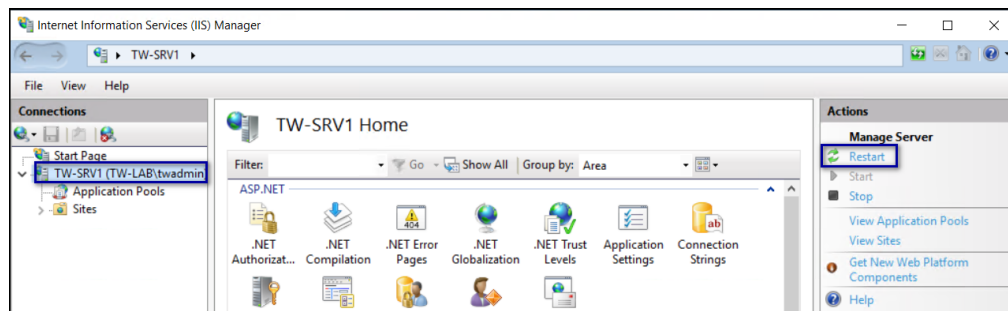
The following figure provides an example of the **Advanced Settings** window.

Advanced Settings window

Advanced Settings window

i. Click **OK**.

5. In the **Connections** pane, select the server name, and then in the **Actions** menu on the right side of the window, click **Restart**, as shown in the following figure.



Restart IIS

6. Close **IIS Manager**.

4.5 Validating the NES Deployment

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

Use the NES Administrator Console to validate the NES deployment.

4.5.1 Access the NES Administrator Console

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

1. Open a web browser and navigate to the NES Administrator Console URL.
2. Sign in with an NES Administrator account.
3. In the main menu, click **About**.
4. Click **View Full System Diagnostics**. The NES server analyzes the status of dependencies and displays the results on the page.
5. Verify the username has administrative access by observing **Policies** and **Search** in the main menu.

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

4.6 Configure NES for Nymi Lock Control

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

1. Log in to the NES Administrator Console.
2. In the main menu, click **Policies**.
3. Click **Edit** on the active policy.
4. Enable the Nymi Lock Control option.
5. Click **Save**.

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 NBA to receive the update in the group policy. The NBA will prompt the user to create an internal security key, which allows the Nymi Band to operate with Nymi Lock Control.

4.7 Hardening the NES Keystore

Hardening is the process of reducing vulnerabilities by eliminating attack vectors and condensing the system's attack surface.

Hardening the NES API can be based on enterprise IT policy or any industry standard hardening guideline. Nymi has taken steps to harden IIS according to the CIS Microsoft IIS 10 Benchmarks from the Centre for Internet Security (CIS). To harden the SQL server based on an industry standard hardening guideline, you must secure the external authenticator private keys by encrypting columns.

Perform the following steps on the NES host to enable column encryption and encrypt sensitive information.

1. Edit the `C:\inetpub\wwwroot\NES\NEnrollment\web.config` file:

- Search for the string `SqlConnectionStrings`.
- Add `Column Encryption Setting=Enabled` within the value attribute tags:

```
<add key="SqlConnectionStrings"
      value="Data Source=.\SQLEXPRESS;Initial Catalog=Nymi.{0};Integrated Security=True;MultipleActiveResultSets=True;Column Encryption Setting=Enabled" />
```

- Save the file.

2. Edit the `C:\inetpub\wwwroot\NES\NES\web.config` file:

- Search for the string `SqlConnectionStrings`.
- Add `Column Encryption Setting=Enabled`; within the value tags:

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

- Save the file.

3. Download and install SQL Server Management Studio (SSMS).

4. Open SSMS by using **Run as Administrator**.

5. Click **Connect > Database Engine**.

6. On the **Connect to Server** page, type the server name and credentials (if using SQL authentication), and then click **Connect**.

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

8. On the **New Column Master Key** window:

- In the **Name** field, type a name for the key (e.g., `CMK_LocalMachine`).
- In the **Key store** field, select **Windows Certificate Store – Local Machine**.
- Click **Generate Certificate**.
- Click **OK**.

9. Right-click **Column Encryption Keys**, and then select **New Column Encryption Key**.

10. On the **New Column Encryption Key** page:
 - In the **Name** field, type a name for the key (e.g., `CEK_LocalMachine`).
 - In the **Column master key** field, select the column master key you created.
 - Click **OK**.
11. Expand **Database > Nymi.NES > Tables**.
12. Right-click **nub.PrivateKeyStore**, and then select **Encrypt Columns**. The Always Encrypted wizard opens.
13. On the **Introduction** page, click **Next**.
14. On the **Column Selection** page:
 - Enable **Apply one key to all checked columns** and ensure `CEK_LocalMachine` appears.
 - Select **PEM**, set Encryption Type to **Randomized**.
 - Select **DER**, set Encryption Type to **Randomized**.
 - Click **Next**.
15. On the **Master Key Configuration** page, click **Next**.
16. On the **Run settings** page, leave the default, and then click **Next**.
17. On the **Summary** page, review the results, click **Finish**, and then click **Close**.
18. Right-click **nub.NymiBand**, and then select **Encrypt Columns**.
19. On the **Introduction** page, click **Next**.
20. On the **Column Selection** page:
 - Enable **Apply one key to all checked columns**.
 - Select **Adv_key_1**, set Encryption Type to **Randomized**.
 - Click **Next**.
21. On the **Master Key Configuration** page, click **Next**.
22. On the **Run settings** page, click **Next**.
23. On the **Summary** page, click **Finish**, and then click **Close**.
24. Close SSMS.

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

1. Open **Manage Computer Certificates**.
2. Expand **Personal** and then select **Certificates**.
3. Right-click **Always Encrypted Certificate** and then select **All Tasks > Manage Private Keys**.
4. Click **Add**.
5. Type the Application Pool Identity, click **Check Names**, and then click **OK**.
6. Click **OK**.
7. Close **Manage Computer Certificates**.

4.7.1 (Optional) Encrypting Usernames in the NES Database

Perform the following steps to encrypt the usernames in the `audit.UserCore` table.

1. Open SSMS by using **Run as Administrator**.
2. Encrypt the `audit.UserCore` table:
 1. In **Tables**, right-click **audit.UserCore**, and then select **Encrypt Columns**.
 2. On the **Introduction** page, click **Next**.
 3. On the **Column Selection** window, enable **Apply one key to all checked columns** and ensure `CEK_LocalMachine` appears.
 4. Select **username**, and then from the **Encryption Type** list, select **Deterministic**.
 5. Click **Next**.
 6. On the **Master Key Configuration** page, click **Next**.
 7. On the **Run settings** page, click **Next**.
 8. On the **Summary** page, click **Finish**, and then click **Close**.
3. Encrypt the usernames in the `nub.UserCore` table:
 1. In **Tables**, right-click **nub.UserCore**, and then select **Encrypt Columns**.
 2. On the **Introduction** page, click **Next**.
 3. Enable **Apply one key to all checked columns**.
 4. Select **username**, and then from the **Encryption Type** list, select **Deterministic**.
 5. Click **Next**.
 6. On the **Master Key Configuration** page, click **Next**.
 7. On the **Run settings** page, click **Next**.
 8. On the **Summary** page, click **Finish**, and then click **Close**.

5 Install and Configure Endpoints

After you deploy and configure NES, install the appropriate software on each endpoint in your environment.

Endpoints include the enrollment terminal and the user terminals.

Installation and configuration instructions differ for endpoints that use a centralized Nymi Agent or a decentralized Nymi Agent:

- Perform the steps outlined in the section *Install and Configure Endpoints with a decentralized Nymi Agent* for:
 - Enrollment terminal
 - iOS devices that access native iOS Nymi-enabled Applications
 - Windows thick client user terminals that access locally installed Nymi-enabled Applications
 - Windows thick clients that use lock control to lock/unlock the desktop
- Perform the steps outlined in the section *Install and Configure Endpoints with a centralized Nymi Agent* for:
 - iOS devices that access web-based Nymi-enabled Applications
 - User terminals that access web-based Nymi-enabled Applications
 - Thin client user terminals that access Nymi-enabled Applications that are installed on a remote session host
 - Thin client user terminals that unlock the desktop on a remote session host

5.1 Install and Configure Endpoints with a Decentralized Nymi Agent

This section provides information about how to deploy Nymi components on user terminals for each use case that uses a decentralized Nymi Agent. You can use a user terminal to perform activities for more than one use case.

The following table provides more information about each use case and endpoint configuration.

Endpoint/Use Case	Description	Nymi Component Requirements
Enrollment terminal	Where users enroll their Nymi Bands by using the NBA, and can use the NBA to authenticate to their Nymi Bands by using corporate credentials authentication.	NBA
User Terminal for Authentication Tasks	Windows thick client where users access a locally-installed Nymi-enabled Application.	Nymi Runtime (Nymi Bluetooth Endpoint and Nymi Agent)
User Terminal for lock and unlock tasks	Windows client where a user uses their Nymi Band to lock or unlock the physical desktop.	Nymi Lock Control, Nymi Runtime (Nymi Bluetooth Endpoint and Nymi Agent)

Note: If the Root CA that issued the NES TLS server certificate is not a Trusted Root CA, you must also install the Root CA certificate for NES on every endpoint.

5.1.1 Bluetooth Adapter

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

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

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

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

5.1.2 Set Up a Decentralized Enrollment Terminal

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

- Place the Bluetooth adapter.
- Install the NBA. The Nymi Band user requires physical access to the enrollment terminal.
- Set the NES_URL registry key.

5.1.2.1 Import the Root CA Certificate

Perform the following steps only if the Root CA issuing the TLS server certificate is not a Trusted Root CA. For example, when you use a self-signed TLS server certificate. Refer to [Import the Root CA Certificate](#) for instructions.

5.1.2.2 Install the NBA

Perform the following steps to install the NBA with the Installation Wizard.

Prerequisite: For an update, uninstall the previous version of Nymi Runtime.

1. Download the NBA package.
2. Double-click the `Nymi-Band-App-installer-v_version.exe` file.
3. On the **User Account Control** window, click **Yes**.
4. On the **Prerequisites** window, click **Next**.
5. On the **Welcome** page, click **Install**.
6. 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.

7. On the **Welcome to the Nymi Runtime Setup Wizard** page, click **Next**.
8. On the **Nymi Runtime Setup** window, click **Next**.

9. On the **Service Account** window, perform one of the following actions to choose the account that starts the service:

- Accept the default service account NTAuthority, click **Next**.
- For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **Next**.

Note: The service account must have permission to run as a service. [Enable Service Log On](#) provides more information about how to modify the local policy to enable this permission for the service account.

10. On the **(Optional) Nymi Infrastructure Service Account**, click **Next**.

Note: Only deployments that use web-based Nymi-enabled Applications (NEAs) with a centralized Nymi Agent require you to configure the Nymi Infrastructure Service Account.

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

12. Click **Finish**.

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

14. On the **Welcome to Nymi Band Application Setup Wizard** window, click **Next**.

15. On the **Select Installation Folder** window, click **Next** to accept the default installation location.

16. In the **Ready to Install** window, click **Install**.

17. On the **Completing the Nymi Band Application Setup Wizard** window, click **Finish**.

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

5.1.2.3 Configure the NES URL

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

1. Run `regedit.exe`.
2. On the **User Account Control** window, click **Yes**.

3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.
4. Right-click **Nymi**, and then select **New > Key**. Name the key **NES**.
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 and 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. Nymi recommends that you specify a name that is descriptive, for example, NES.
8. Click **OK**.

5.1.2.4 Disable Evidian Enrollment

Nymi supports using the same NES server to enroll users in Evidian and non-Evidian environments simultaneously. On the enrollment terminal which does not enroll users to an Evidian EAM Controller, perform the following steps.

1. Launch `regedit.exe`.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Nymi`.
3. Right-click **NES**, and then select **New > String value**.
4. In the **Name** field, type `HideEvidianEnrollmentError`.
5. Edit the key and then in the **Value data** field, type `True`.
6. Click **OK**.
7. Close **Registry Editor**.

5.1.2.5 Configure the Communication Protocol

If you use the enrollment terminal to also access applications, perform the following steps to disable the legacy protocol.

Note: After you set this environment variable, user terminals cannot communicate with Nymi Bands that use pre-CWP 1.15.x firmware.

1. In the Windows search field, type `env`, and then from the pop-up menu, select **Edit the System Environment Variables**.
2. Click **Environment Variables**.
3. In the **System Variables** section, click **New**, and then perform the following actions:
 - a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`.
 - b. In the **Variable Value** field, type `0`.
 - c. Click **OK**.

5.1.3 Set Up Windows User Terminals for Authentication Tasks

You can use the Nymi Band to perform daily authentication tasks that would normally require the user to supply a user name and password, such as e-signatures in an MES application.

User terminals that you will use for authentication tasks require that you:

- Import the Root CA certificate, if the Root CA is not a Trusted Root CA.
- Install Nymi Runtime.
- Place the Bluetooth adapter.
- Optionally, insert a Nymi-verified NFC reader into an available USB port.

5.1.3.1 Import the Root CA Certificate

Refer to [Import the Root CA Certificate](#) for instructions.

5.1.3.2 Install Nymi Runtime

Perform the following steps to install or update Nymi Runtime on a user terminal, on which you want to install a Nymi-enabled Application.

1. Log in to the terminal with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the `..\nymi-sdk\windows\setup` folder, right-click the `Nymi Runtime Installer version.exe` file, and select **Run as administrator**.
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, perform one of the following actions to choose the account that starts the service:
 - Accept the default service account `NTAuthority`, click **Next**.
 - For non-English Windows Operating Systems, choose the `LocalSystem` account from the drop list, and then click **Next**.

Note: The service account must have permission to run as a service. [Enable Service Log On](#) provides more information.

9. On the **(Optional) Nymi Infrastructure Service Account**, click **Next**.
10. On the **Ready to install** page, click **Install**.
11. Click **Finish**.
12. On the **Installation Completed Successfully** page, click **Close**.

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

5.1.3.3 Configure the CWP Communication Protocol

Starting with CWP 1.15, the Nymi solution supports a new, high performance protocol over Bluetooth between the Nymi Runtime and Nymi Bands.

Perform the following steps on all user terminals where users access Nymi-enabled Applications to disable the legacy protocol. The enrollment terminal only requires the environment variable if users access Nymi-enabled Applications on the enrollment terminal.

Note: After you set this environment variable, user terminals cannot communicate with Nymi Bands that use pre-CWP 1.15.x firmware.

1. In the Windows search field, type `env`, and then from the pop-up menu, select **Edit the System Environment Variables**.
2. Click **Environment Variables**.
3. In the **System Variables** section, click **New**, and then perform the following actions:
 - a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`.
 - b. In the **Variable Value** field, type `0`.
 - c. Click **OK**.

5.1.4 Set Up Windows User Terminals for Lock and Unlock

You can use the Nymi Band to lock and unlock the desktop of thick client computers.

User terminals on which you will use the Nymi Band to lock and unlock a desktop require that you:

- Import the Root CA certificate, if the Root CA is not a Trusted Root CA.
- Place the Bluetooth adapter.
- Install Nymi Lock Control.
- Configure the Nymi Bluetooth Endpoint configuration file.

5.1.4.1 Configure Nymi Lock Control

Perform the following steps to enable and configure Nymi Lock Control.

By default Nymi Lock Control is not enabled.

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. From the navigation bar, select **Policies**.

The **Policies** page appears with a table that displays a list of existing group and individual policies.

3. In the **Policies** window, select the active policy.
4. In the **Lock Control** section, select the **Enable Nymi Lock Control** option.

The following options appear to customize Nymi Lock Control:

Option	Description
Lock When Away	Configure Nymi Lock Control with the ability to lock the user terminal when Nymi Lock Control does not detect the authenticated Nymi Band. Default: Enabled. When enabled, Nymi Lock Control locks the user terminal when a user removes an authenticated Nymi Band or when the Nymi Band is not in close proximity of the user terminal. If the Nymi Band does not return within close range of the user terminal, the terminal will lock. When the Nymi Band is out of range, a 10 second timer appears on the desktop. Ensure that your Group Policy Object (GPO) settings do not push the <i>Do not display the lock screen</i> configuration option to Nymi Lock Control user terminals. Edit the <code>nbe.toml</code> file to define close proximity for Nymi Lock Control. Refer to <i>Editing the nbe.toml File</i> in the Deployment Guide.
Unlock When Present	Configures Nymi Lock Control to check if the Nymi Band is in close proximity before unlocking the user terminal. If not, then unlock fails. Default: Enabled. When enabled, prevents an unauthorized user from unlocking the user terminal while the Nymi Band user is in Bluetooth range, but not in close proximity to the terminal. When disabled, allows a user to unlock the terminal by pressing the Enter key or space bar when the authenticated

Option	Description
	Nymi Band is within Bluetooth range. You can define how close the Nymi Band must be to the user terminal to allow the user to unlock the terminal with the Nymi Band in the <code>nbe.toml</code> file. The <i>Editing the nbe.toml File</i> section in the Deployment Guide provides more information.
Keep Unlocked when Present	Provides you with the ability to define how the Nymi Band interacts with operating system screen timeouts or sleep settings that lock the user terminal. Default: Enabled. When enabled, overrides any system screen timeouts or sleep settings, and keeps the user terminal unlocked as long as the Nymi Band is present and authenticated. When disabled, prevents Nymi Lock Control from overriding any system screen timeouts or sleep settings.

5. Click **Save**.

During enrollment the NBA updates the Nymi Band to enable Nymi Lock Control support. Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Bands until the user logs into the NBA while wearing their authenticated Nymi Band. When the NBA update on the Nymi Band completes, restart Nymi Lock Control.

5.1.4.2 Import the Root CA Certificate

Refer to [Import the Root CA Certificate](#) for instructions.

5.1.4.3 Install Nymi Lock Control

Perform the following steps on each Windows user terminal in the environment on which you want to install Nymi Lock Control.

1. Log in to the terminal with an account that has administrator privileges.
2. Create a backup copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file.
3. Right-click `NymiLockControl-installer-vw.x.y.z` and select **Run as administrator**.

4. On the **User Account Control** window, click **Yes**.
5. On the **Welcome to the Prerequisites Setup Wizard**, click **Next**.
6. On the **Prerequisites** window, leave the default selections, and then click **Next**.
7. On the **Welcome** window, click **Install**.
8. On the **Welcome to the Nymi Runtime Setup Wizard** page, click **Next**.
9. On the **Nymi Runtime Setup** window, leave the default options, and then click **Next**.
10. On the **Service Account** window, perform one of the following actions:
 - Accept the default service account NTAuthority, click **Next**.
 - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **Next**.
- Note:** The service account must have permission to run as a service.
11. On the **Ready to install** page, click **Install**.
12. Click **Finish**.
13. On the **Installation Completed Successfully** page, click **Close**.
14. On the **Welcome to Nymi Lock Control Setup Wizard** window, click **Next**.
15. On the **Select Installation Folder** window, to keep the default installation location, click **Next**.
16. On the **Ready to Install** window, click **Install**.
17. On the **Completing the Nymi Lock Control Setup Wizard** window, click **Finish**.
18. Stop the **Nymi Bluetooth Endpoint** service.
19. Edit the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file. Compare and modify the following parameter values as required, with the value that appears in your backed up `nbe.toml` file:

- a. `agent_url` parameter.

b. RSSI parameters. Entries that appear in a CWP 1.19.2 and earlier TOML file apply to the Bluegiga Bluetooth Adapter; therefore, update the values that appear in the `[dongle.bluegiga]` section.

c. `endpoint_id` parameter. If the parameter appears in your backup copy of the `nbe.toml` file, copy and paste the parameter definition on a blank line before the `[dongle.bluegiga]` section of the current `nbe.toml` file.

20. Start the **Nymi Bluetooth Endpoint** service.

21. Log out and log back into the user terminal.

5.1.4.4 Configure the NES URL

Create a GPO to push the NES URL registry key to each user terminal, or perform the steps in [Configure the NES URL](#) to manually create the registry key on the user terminal.

5.1.4.5 Configure the Communication Protocol

Refer to [Configure the CWP Communication Protocol](#) for instructions.

5.1.4.6 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. If the `nbe.toml` file is renamed or deleted, Nymi Lock Control and BLE taps behave under the default settings.

Tuning Nymi Band Tap Behaviour for Nymi Lock Control

Nymi Bluetooth Endpoint uses the Bluetooth adapter to detect nearby Nymi Bands. NBE evaluates the signal strength of a Nymi Band against predefined RSSI settings to decide if a Nymi Band tap has occurred.

To change how close a user needs to place the Nymi Band near the Bluetooth adapter for Nymi Bluetooth Endpoint to detect a tap, you can adjust the RSSI settings.

How you modify the RSSI parameters depends on the operating system:

- On Windows thick clients, edit the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file in administrator mode.
- On HP Thin Pro, edit the `/usr/bin/nbe.toml` file.
- On IGEL, in UMS, navigate to **System > Firmware Customization > Custom Partition > Partition** and define the partition parameters.

Note: On Windows and HP Thin Client, when the `nbe.toml` file is not present, Nymi Bluetooth Endpoint uses the default values. On IGEL, when you do not define the parameters in UMS, Nymi Bluetooth Endpoint uses the default values.

There are two types of RSSI parameters that define tap behaviour:

- Tap Windows parameters — Evaluates a defined number of RSSI measurements captured by the Bluetooth Adapter to determine a rolling average. The average allows the Nymi Bluetooth Endpoint to smooth out signal fluctuations and ignore outliers.
- Tap Threshold parameters — Define the specific RSSI levels that trigger an event. For example, when the average RSSI from the tap window parameters exceeds the tap threshold, Nymi Bluetooth Endpoint detects a tap.

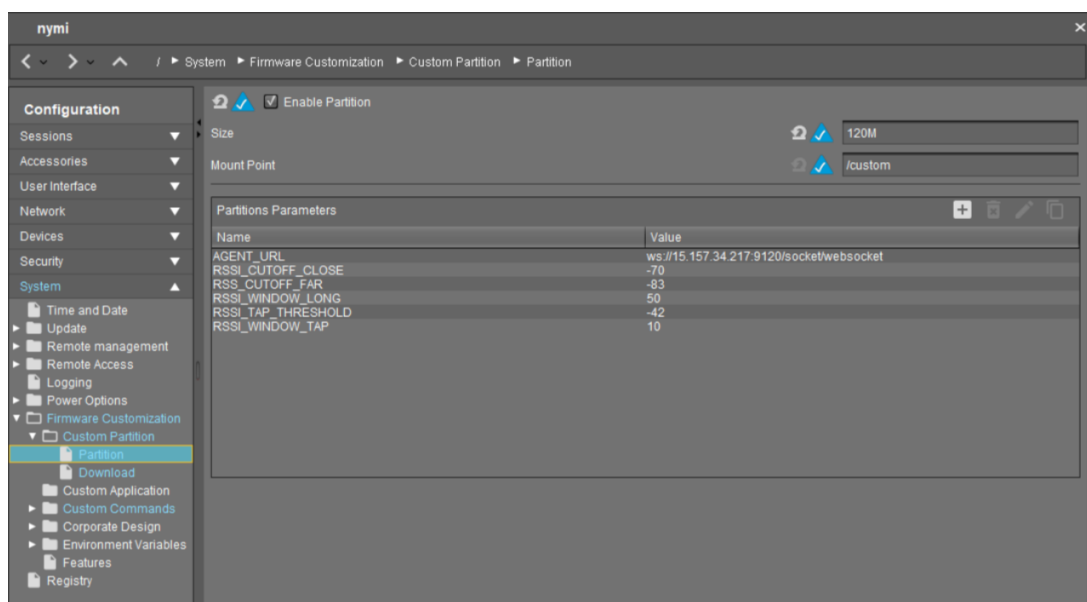
The following table provides a list of supported RSSI parameters, their default values and the purpose of each parameter.

Note: For IGEL, specify all RSSI parameter names in capital letters.

RSSI Parameter	Default Value	Description
<code>rss_i_window_tap</code>	10	Defines how long the user must keep their Nymi Band within the tap threshold distance of the Bluetooth Adapter to complete a Nymi Band tap. A larger value increases the amount of time that a user must keep their Nymi Band within Bluetooth range and decreases the sensitivity.
<code>rss_i_window_long</code>	Bluegiga: 50	Defines how often the Nymi Bluetooth Endpoint service checks the distance between the Bluetooth Adapter and the Nymi Band. This helps determine proximity. Nymi Bluetooth Endpoint tracks trends in these changes to trigger a Nymi Lock Control action, such as <i>keep unlocked when present, lock when away, or unlock when present</i> .
<code>rss_i_tap_threshold</code>	Bluegiga: -42 (must be 0 or negative)	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. If the Nymi Band maintains a minimum distance specified by <code>rss_i_tap_threshold</code> , for the duration of time defined by

RSSI Parameter	Default Value	Description
		<code>rss_i_window_tap</code> , a BLE tap is performed.
<code>rss_i_cutoff_close</code>	Bluegiga: -70 (must be 0 or negative)	Determines the outer range of the close distance-threshold (excluding tap distance) for Nymi Lock Control. Enter 0 to bypass the proximity functionality. If the Nymi Band maintains a close distance and RSSI values are within the <code>rss_i_cutoff_close</code> value, Nymi Lock Control keeps the user terminal unlocked. If the Nymi Band moves away and RSSI values decrease from <code>rss_i_cutoff_close</code> to <code>rss_i_cutoff_far</code> , Nymi Lock Control locks the user terminal.
<code>rss_i_cutoff_far</code>	Bluegiga: -83 (must be negative)	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 RSSI values increase from <code>rss_i_cutoff_far</code> to <code>rss_i_cutoff_close</code> , Nymi Lock Control unlocks the user terminal.

The following figure provides an example of the Partition Parameters window in UMS with each RSSI value.



IGEL RSSI values

After you save the changes, restart the Nymi Bluetooth Endpoint, which reloads the parameter settings.

5.2 Install and Configure Endpoints with a Centralized Nymi Agent

Review this section for information about how to deploy Nymi components on user terminals for each use case that uses a centralized Nymi Agent.

The following table summarizes each endpoint configuration.

Endpoint/Use Case	Description	Nymi Component Requirements
User Terminal for Authentication Tasks (Windows thick client)	Users access a web-based Nymi-enabled Application.	Nymi Runtime (Nymi Bluetooth Endpoint only)
User Terminal for Authentication Tasks (Windows/Linux Thin Client)	Where a user logs into a remote session host and uses their Nymi Band to perform repetitive authentication tasks in a Nymi-enabled Application on the remote session host.	Nymi Runtime (Nymi Bluetooth Endpoint only)
User Terminal for lock and unlock tasks	Where a user uses their Nymi Band to lock or unlock the desktop of the remote session host.	Nymi Lock Control, Nymi Runtime (Nymi Bluetooth Endpoint only)

Note: If the Root CA that issued the NES TLS server certificate is not a Trusted Root CA, you must also install the Root CA certificate for NES on every endpoint.

5.2.1 Configuring Endpoint ID

You can configure the format of the endpoint ID that Nymi Bluetooth Endpoint uses to identify a user terminal. The endpoint ID uniquely identifies the Nymi Bluetooth Endpoint to the applications that connect to it. By default, the endpoint ID is the IPv4 address of the user terminal, which is suitable for most environments.

In some environments, more than one user terminal can be assigned the same IP address — for example, when terminals connect over VPNs, or when multiple sites use overlapping IP subnets that reach the corporate network through NAT. In these environments the IP address alone may not be unique, which can cause an application

to connect to the wrong Nymi Bluetooth Endpoint and lead to data integrity issues. To prevent this ambiguity, you can configure the endpoint ID to be derived from the hostname, or from the hostname combined with the IP address. You set the endpoint ID format with the `ENDPOINT_ID_MODE` environment variable. The following table lists the supported formats, their values, and the purpose of each format.

Endpoint_ID_MODE value	Description
IP (default)	The endpoint ID is the IPv4 address of the user terminal. Suitable for most environments. If WebAPI is used, then this is the only supported <code>ENDPOINT_ID_MODE</code> .
HOSTNAME	The endpoint ID is the hostname of the user terminal, as reported by the operating system. Allows the IP address of the terminal to change (for example, when switching to a different Wi-Fi network) while maintaining connectivity.
HOSTNAME_IP	The endpoint ID is the hostname and the IPv4 address of the user terminal. Provides the maximum protection against endpoint ID conflicts.

Note: When a decentralized Nymi Agent is used, it is not necessary to configure `ENDPOINT_ID_MODE`, since the Nymi Bluetooth Endpoint and Nymi API only connect to the local Nymi Agent and are therefore unaffected by IP address collisions between different computers.

The `ENDPOINT_ID_MODE` environment variable is supported in CWP 1.20.2 and later. When the variable is not set, Nymi Bluetooth Endpoint uses the default IP format. To set the endpoint ID format:

1. Set the environment variable `ENDPOINT_ID_MODE` to the required format (for example, `ENDPOINT_ID_MODE=HOSTNAME_IP`) on each user terminal and on each computer that runs a connecting application. You can use Active Directory group policy to apply this setting to all computers at once. Computers that run a connecting application include, for example, Windows 10 / 11 computers, RDP servers, or Citrix servers with the Nymi Connect for Windows Client, Evidian Client, Nymi Lock Control, or Nymi Band Application installed.

2. Restart the computer so that the new setting takes effect. If Nymi Bluetooth Endpoint is the only Nymi component installed, restarting Nymi Bluetooth Endpoint is sufficient.

Apply the same endpoint ID format consistently across all user terminals and connecting applications. A mismatch between components can cause BLE tap to work unreliably. When you change the format on an existing deployment, apply the change during a maintenance window.

5.2.2 Set Up the Enrollment Terminal

You can set up the enrollment terminal in two configurations.

- **Centralized Enrollment Terminal** — Install the NBA on a Citrix/RDP session host, to allow users to perform enrollments from any thick client user terminal with access to the RDP/Citrix session host.
- **Decentralized Enrollment Terminal** — Install the NBA on a thick client user terminal, to limit the access a user has to perform enrollments.

5.2.2.1 Deploy a Centralized Enrollment Terminal

When you deploy a centralized enrollment terminal, you install the NBA on the Citrix/RDP server. After you install the Nymi Bluetooth Endpoint on the thick client, users can launch the NBA from the Citrix Storefront or RDP session host to complete enrollments.

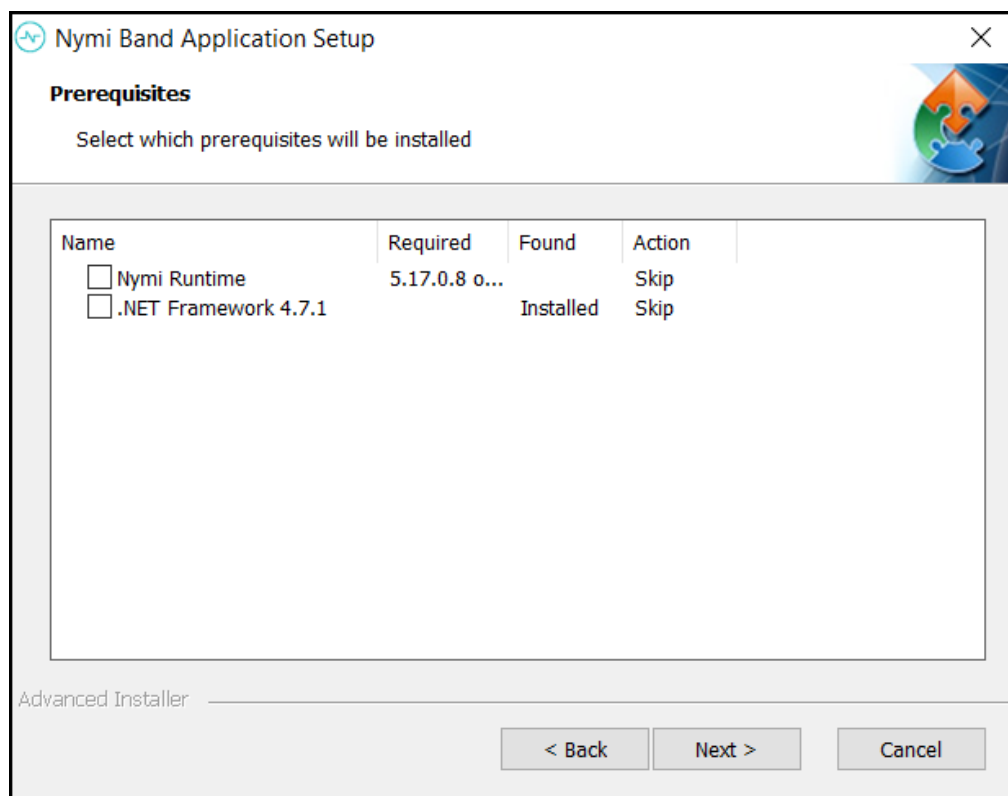
Note: Instructions about how to install and configure the thick client user terminals are covered later in this guide in the *Set Up Thick Client User Terminals* section.

In this configuration, you perform the following steps:

- Install the NBA on the Citrix/RDP session host, without installing Nymi Runtime.
- Configure the NBA to use the centralized Nymi Agent.
- Install the Nymi Bluetooth Endpoint on the thick client that users will use to access the NBA.
- Configure the Nymi Bluetooth Endpoint on the thick client enrollment terminal to use the centralized Nymi Agent.

Install the NBA on the RDP/Citrix Session Host

1. Download the NBA package.
2. Double-click the `Nymi-Band-App-installer-v_version.exe` file.
3. On the **User Account Control** window, click **Yes**.
4. On the **Welcome to Prerequisites** window, click **Next**.
5. On the **Prerequisites** window, clear the option to install Nymi Runtime, as shown in the following figure, and then click **Next**.



No Nymi Runtime Installation

6. On the **Welcome to Nymi Band Application Setup Wizard** window, click **Next**.
7. On the **Select Installation Folder** window, click **Next** to accept the default installation location.
8. In the **Ready to Install** window, click **Install**.
9. On the **Completing the Nymi Band Application Setup Wizard** window, click **Finish**.

Configure NBA to use a Centralized Nymi Agent

Perform the following steps on the enrollment terminal to configure the NBA to use a centralized Nymi Agent.

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 `AgentURL`.
6. Edit the **AgentURL** key, and in the **Value data** field, type the URL to the Nymi Agent service, in the following format:

```
protocol://agent_server:agent_port/socket/websocket
```

where:

- *protocol* is the websocket protocol to use to connect to the Nymi Agent:
 - `ws` for websocket
 - `wss` for secure websocket
- *agent_server* is one of the following:
 - For WSS, the FQDN of the centralized Nymi Agent machine
 - For WS, the IP address of the centralized Nymi Agent machine
- *agent_port* is the port on which to connect to the centralized Nymi Agent machine, for example 9120

For example, for WSS: `wss://agent.nymi.com:9120/socket/websocket`

Configure the NES URL

Perform the steps in [Configure the NES URL](#) to create the NES URL registry key on the session host.

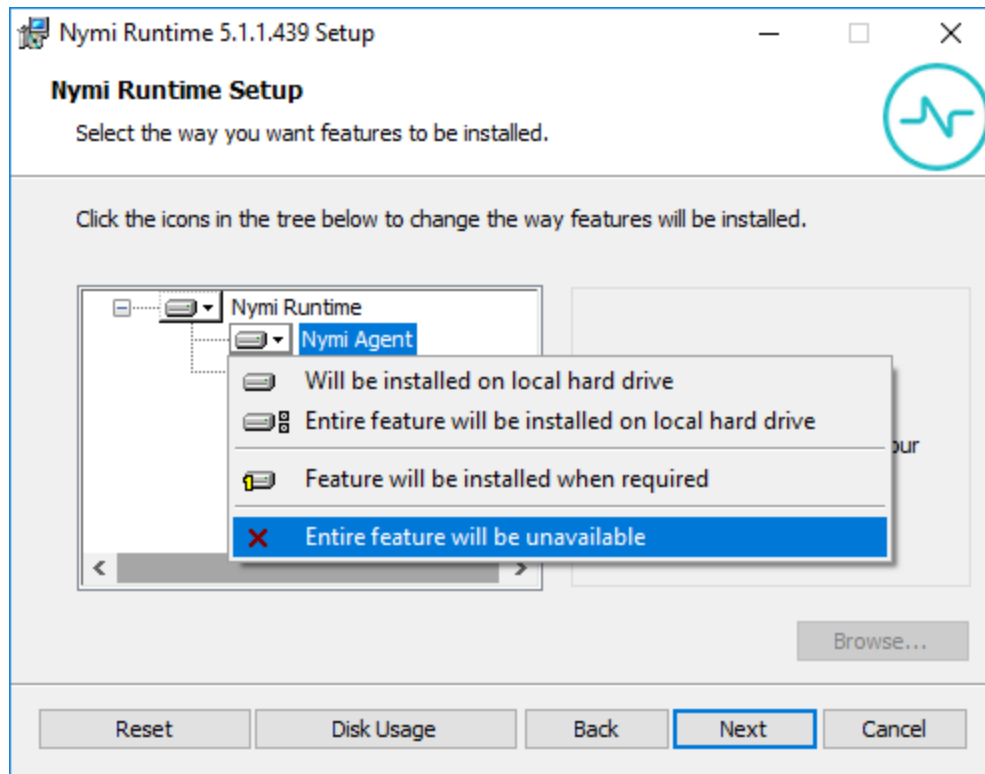
Install and Configure the Nymi Bluetooth Endpoint

Install the Nymi Bluetooth Endpoint on the thin client that users will access to connect to the Citrix/RDP centralized enrollment terminal. After you install the Nymi Bluetooth Endpoint, you must update the `nbe.toml` file.

1. Log in to the terminal with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the `..\nysi-sdk\windows\setup` folder, right-click the `Nymi Runtime Installer version.exe` file, and select **Run as administrator**.
4. On the **Welcome** page, click **Install**.
5. On the **User Account Control** page, click **Yes**.

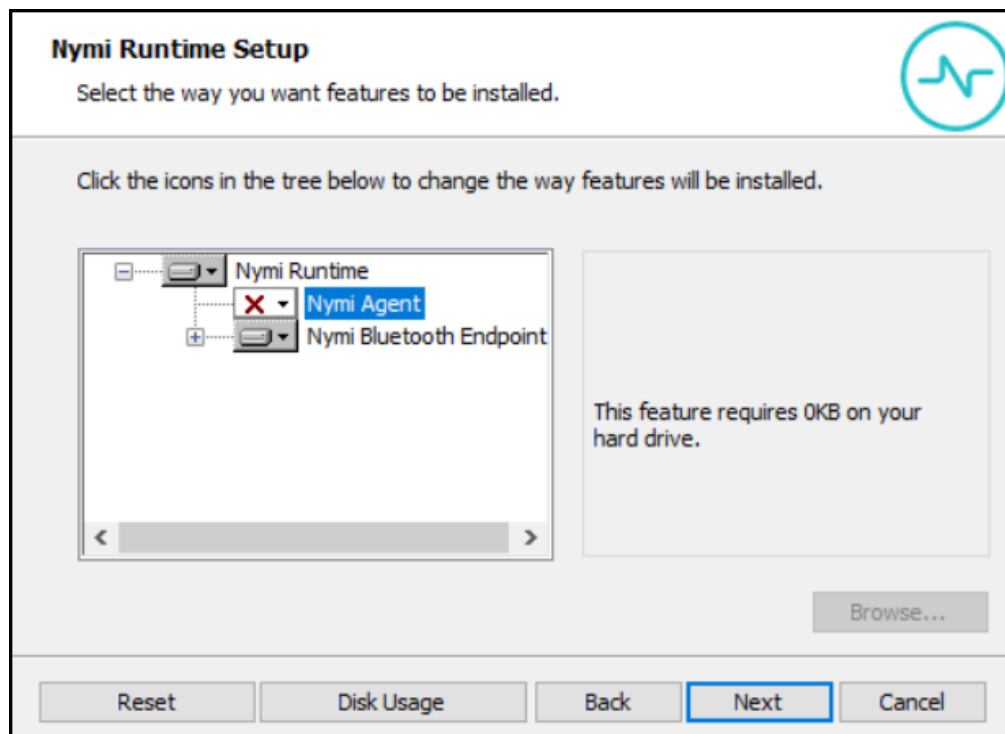
The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.

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, and then click **Next**.



Nymi Agent feature will be unavailable

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



Nymi Agent feature is not available

10. On the **Service Account** window, perform one of the following actions:
 - Accept the default service account NTAuthority, click **Next**.
 - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **Next**.
11. On the **Ready to install** page, click **Install**.
12. Click **Finish**.
13. On the **Installation Completed Successfully** page, click **Close**.

Confirm that the status of the Nymi Bluetooth Endpoint service is running.

Edit the Nymi Bluetooth Endpoint Configuration File

The Nymi Bluetooth Endpoint uses the `nbe.toml` file to define the location of a remote Nymi Agent. Perform the following steps to specify the URL to the remote Nymi Agent.

1. Make a copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file.
2. Edit the `nbe.toml` file with a text editor in administrator mode.
3. Edit the default `agent_url` parameter and perform the following changes:
 - For WSS:
 - Change the protocol from `ws` to `wss`
 - Replace `127.0.0.1` with the FQDN of the centralized Nymi Agent machine.
 - For WS, replace `127.0.0.1` with the IP address of the centralized Nymi Agent machine.

For example, for WSS: `agent_url = "wss://agent.nymi.com:9120/socket/websocket"`

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

Note: Optionally, you can also change the communication port from the default value 9120.

4. Save the `nbe.toml` file.

5. Restart the **Nymi Bluetooth Endpoint** service.

You can use Group Policies to push the modified `nbe.toml` file to the `C:\Nymi\Bluetooth_Endpoint` folder on each user terminal.

5.2.2.2 Deploy a Decentralized Enrollment Terminal

Install the NBA, which also installs the Nymi Runtime software on a thick client. Refer to [Install the NBA](#) and [Configure the NES URL](#) for instructions.

5.2.2.3 Configure the Communication Protocol

If you use the enrollment terminal to also access applications, refer to [Configure the Communication Protocol](#) for instructions on disabling the legacy protocol.

5.2.3 Set Up Thick Client User Terminals

You can use the Nymi Band to perform daily authentication tasks that would normally require a username and password in an MES application that resides on a remote session host.

User terminals require that you:

- Import the Root CA certificate, if the Root CA is not a Trusted Root CA.
- Install the Nymi Bluetooth Endpoint service.
- Place the Bluetooth adapter.
- Optionally, insert a Nymi-verified NFC reader into an available USB port.

5.2.3.1 Bluetooth Adapter

Refer to [Bluetooth Adapter](#) for placement guidelines.

5.2.3.2 Import the TLS Certificate into Firefox

If you have issued your own TLS root certificate using a private certificate authority (CA), before Firefox can open a WebSocket connection for the Nymi-enabled Application, you need to import the TLS certificate.

See the [Mozilla documentation](#) for more information.

1. Open Firefox web browser.
2. In the right pane, navigate to **Options**.
3. Select **Privacy and Security**.
4. Under **Certificates**, click **View Certificates** and then select **Authorities**.
5. Click **Import** and select the TLS root certificate from your machine.
6. Click **OK**.
7. Run the Nymi WebAPI and open the WebSocket connection by using Firefox.

5.2.3.3 Import 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.

Refer to [Import the Root CA Certificate](#) for instructions.

5.2.3.4 Install the Nymi Bluetooth Endpoint (Windows)

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.

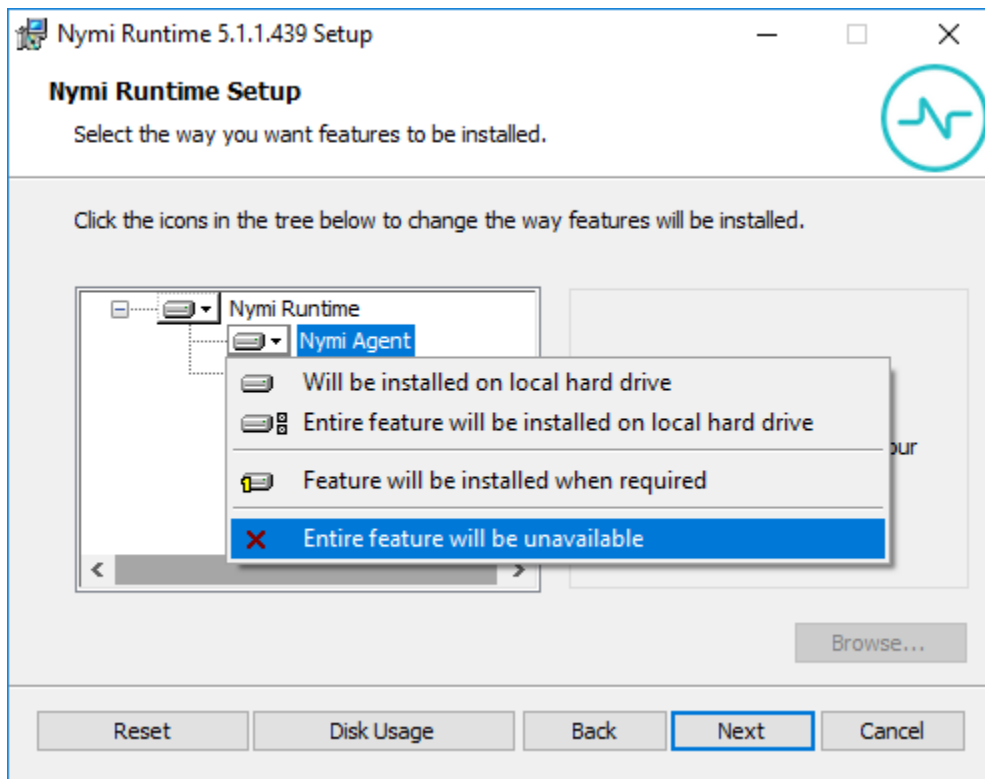
Perform the following steps to install Nymi Bluetooth Endpoint manually.

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, right-click the `Nymi Runtime Installer version.exe` file, and select **Run as administrator**.
4. On the **Welcome** page, click **Install**.

5. On the **User Account Control** page, click **Yes**.

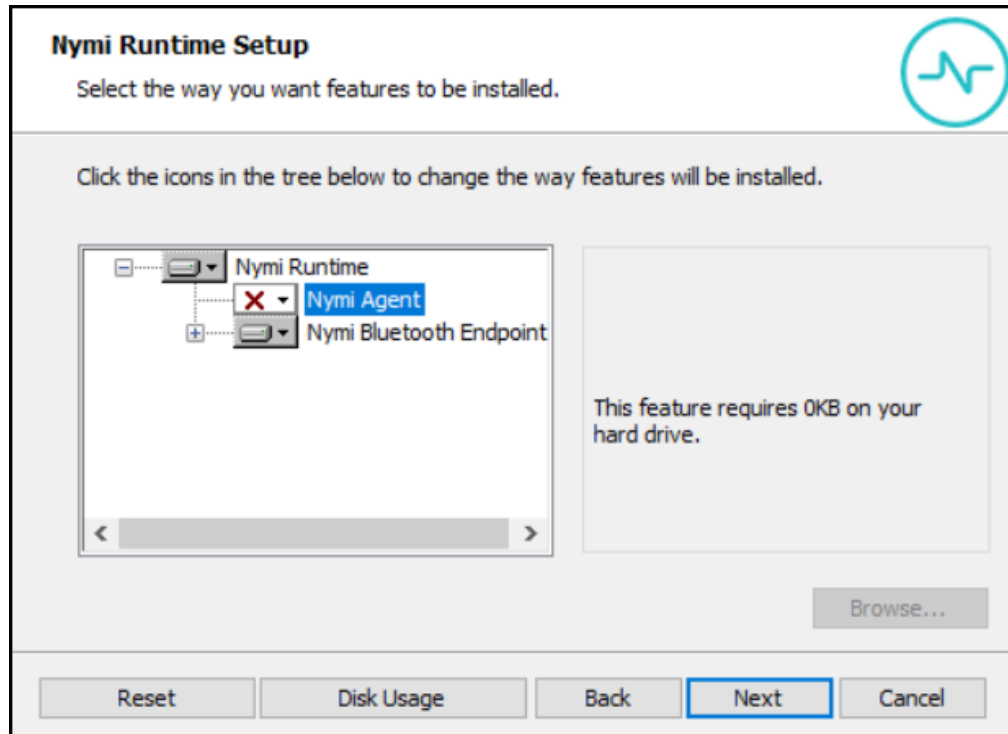
The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.

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**, and then click **Next**.



Nymi Agent feature will be unavailable

9. Observe that **Nymi Agent** is not available, and then click **Next**.



Nymi Agent feature is not available

10. On the **Service Account** window, perform one of the following actions:
 - Accept the default service account NTAAuthority, click **Next**.
 - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **Next**.

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

12. Click **Finish**.

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

Confirm that the status of the Nymi Bluetooth Endpoint service is running.

5.2.3.5 Install the Nymi Bluetooth Endpoint (HP Thin Pro)

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

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

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

2. Extract the file, `nbed-cron_x.y.z_amd64.deb`, from the Nymi distribution package and save it to the machine.
3. Unlock read/write access with **X Terminal**.
 - a. Click **Start** and go to **Tools**.
 - b. Click **X Terminal**.
 - c. Type `fsunlock`.
4. In **X Terminal** change the directory to the file location of `nbed-cron_x.y.z_amd64.deb` and install the extracted file.

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

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

5. Reboot the client.

5.2.3.6 (Windows and HP Thin Pro) Edit the Nymi Bluetooth Endpoint Configuration File

The Nymi Bluetooth Endpoint uses the `nbe.toml` file to define the location of a remote Nymi Agent. Perform the following steps to specify the URL to the remote Nymi Agent.

1. Make a copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file (On HP Thin Pro, `/usr/bin/nbe.toml`).
2. Edit the `nbe.toml` file with a text editor in administrator mode.
3. Edit the default `agent_url` parameter and perform the following changes:
 - For WSS:
 - Change the protocol from `ws` to `wss`
 - Replace `127.0.0.1` with the FQDN of the centralized Nymi Agent machine.
 - For WS, replace `127.0.0.1` with the IP address of the centralized Nymi Agent machine.

For example, for WSS: `agent_url = "wss://agent.nymi.com:9120/socket/websocket"`

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

Note: Optionally, you can also change the communication port from the default value 9120.

4. Save the `nbe.toml` file.
5. Restart the Nymi Bluetooth Endpoint.

On Windows:

- a. Press the Windows key on the keyboard. Enter "Services" in the search bar.
- 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.

You can use Group Policies to push the modified `nbe.toml` file to the `C:\Nymi\Bluetooth_Endpoint` folder on each user terminal.

5.2.3.7 (IGEL 11) Install the Nymi Bluetooth Endpoint

Perform the steps in this section to install Nymi Bluetooth Endpoint on IGEL 11 devices.

Upload Nymi Packages to Universal Management Suite

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

Obtain the installation package from Nymi.

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**.

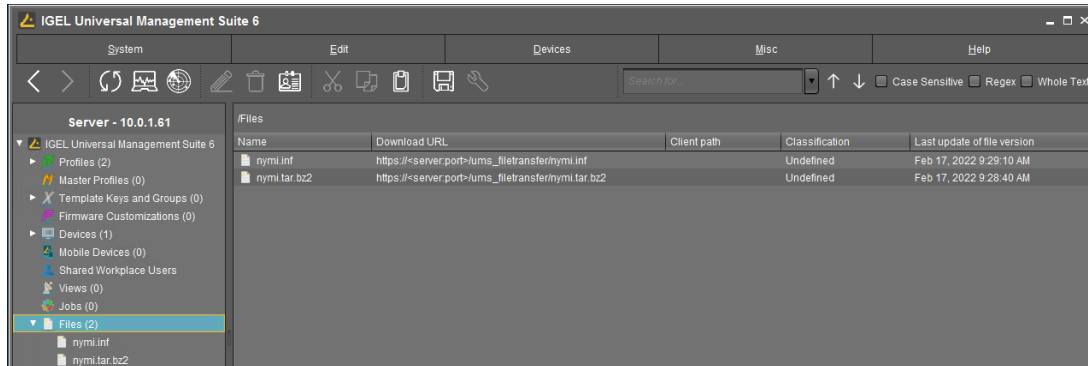
The **New file** window appears.

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 `nyimi.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**.

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 `nyml.inf` file, select the file, and then click **Open**.

8. Click **OK**.

Make note of the value in **Download URL** field for each file, as you will require this information in the *Customizing the Custom Partition* section.



Files window

Create 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.

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`.

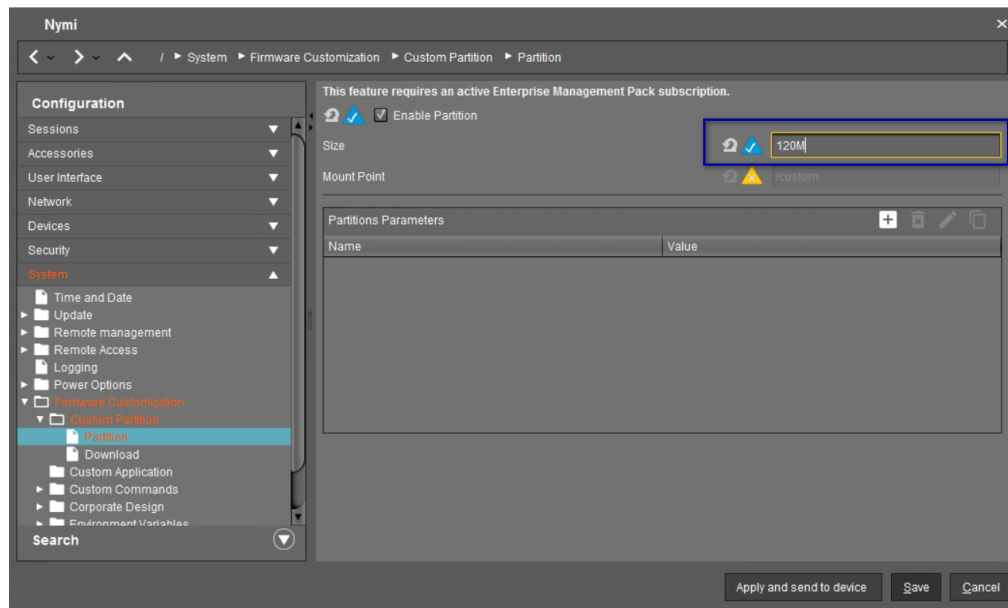
4. Click **OK**.

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 120M.



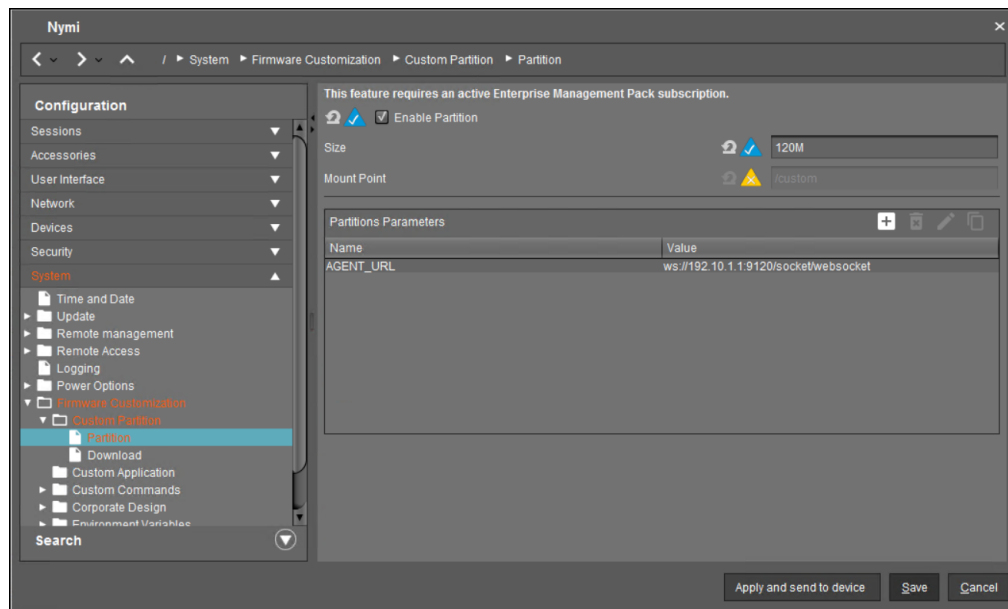
Set UMS partition size

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:

- In the **Name** field, type `AGENT_URL`.
- 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.
- Click **Confirm**.



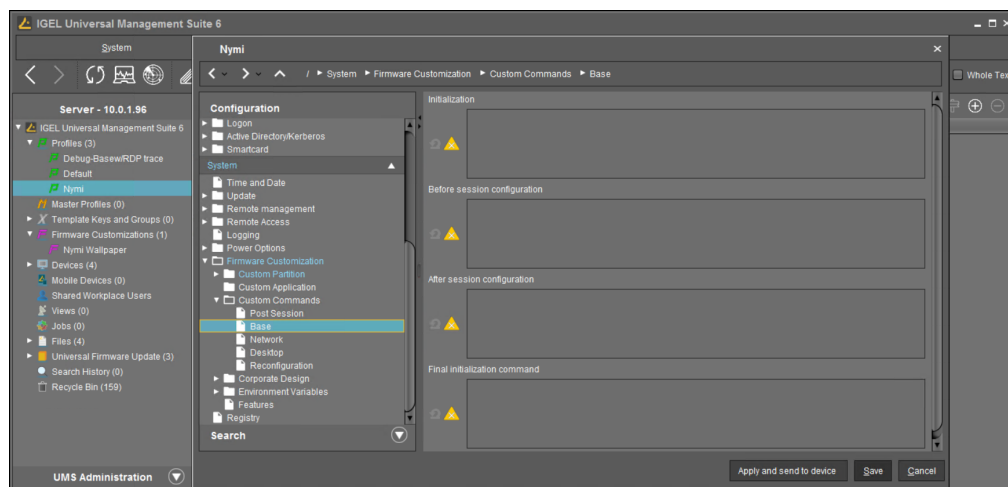
Partition window

- a. Click **Save**.
- b. On the **Update time** window, click **On Reboot** and then click **Confirm**.

Customize the Custom Partition

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

1. Double-click the **Nymi** profile.
2. From the **Configuration** navigation pane, expand **System > Firmware Customization > Custom Commands > Base**.



Base menu option

3. 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 the following commands on separate lines:

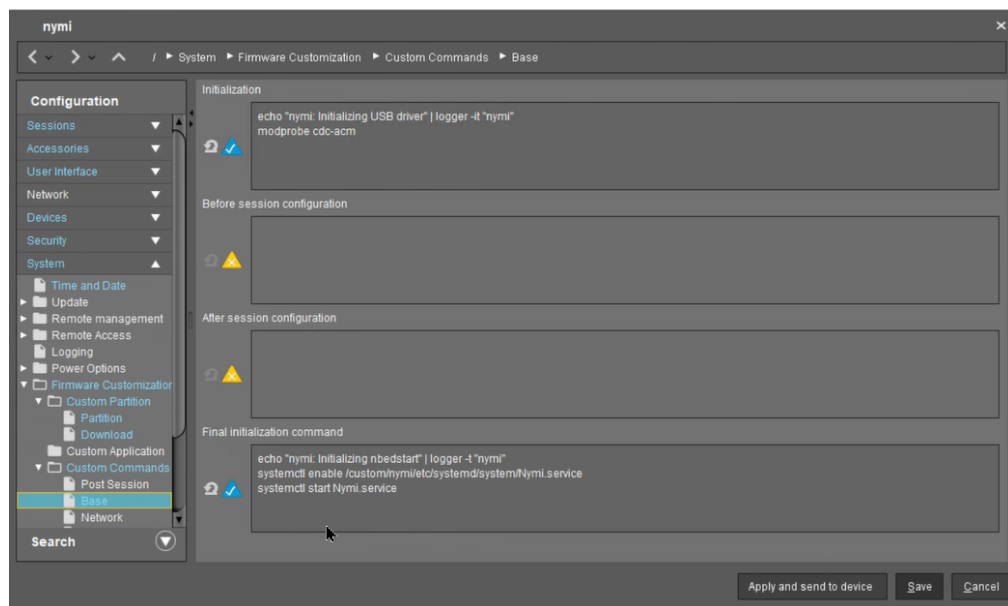
```
echo "nyimi: Initializing USB driver" | logger -it "nyimi"  
modprobe cdc-acm
```

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

b. In the **Final Initialization Command** field, type the following commands on separate lines:

```
/custom/nyimi/usr/lib/nyimi/nbedstart&  
systemctl enable /custom/nyimi/etc/systemd/system/Nyimi.service  
systemctl start Nyimi.service
```

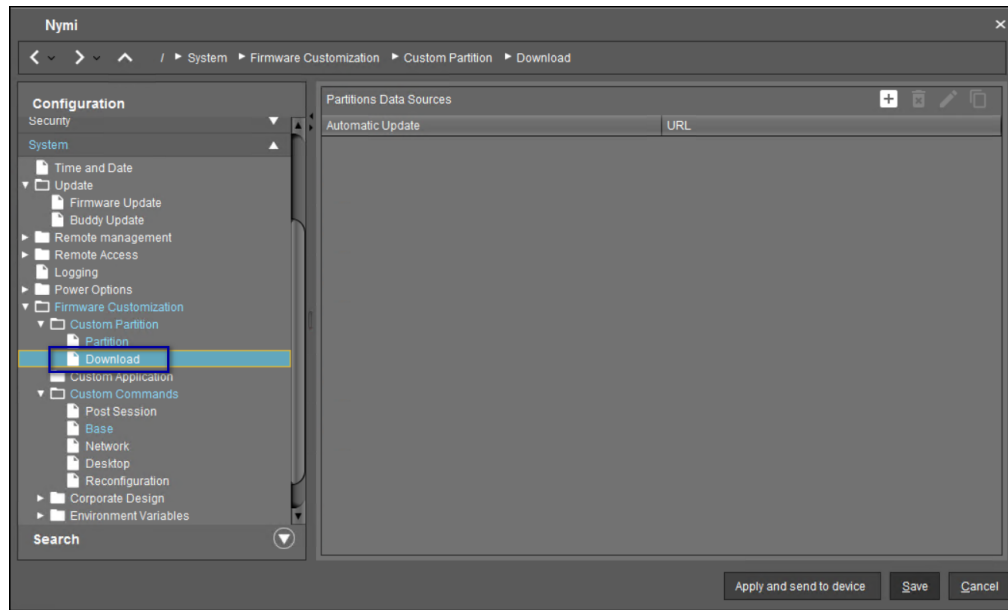
a. Click **Save**.



Nymi Base Commands

4. Double-click the **Nymi** profile.

5. From the **Configuration** navigation pane, expand **System > Firmware Customization > Custom Partition > Download**.



Downloads

6. In the **Partitions Data Sources** section, click **[+]** (Add).

A dialog box appears.

7. Perform the following actions in the **Add** window:

- In the **URL** field, type the Download URL path for the `nyimi.inf` file. For example, `https://10.0.1.61:8443/ums_filetransfer/nyimi.inf`.
- In the **Username** field, type the username of a user that has access to the UMS file transfer location.
- In the **Password** field, type the password for the user account.
- In the **Final Action** field, type `/custom/nyimi/custompart-nyimi init`.
- Click **OK**.

Add

☐ Automatic Update

URL

User name

Password

Initial action

Final action

Ok Cancel

Add window

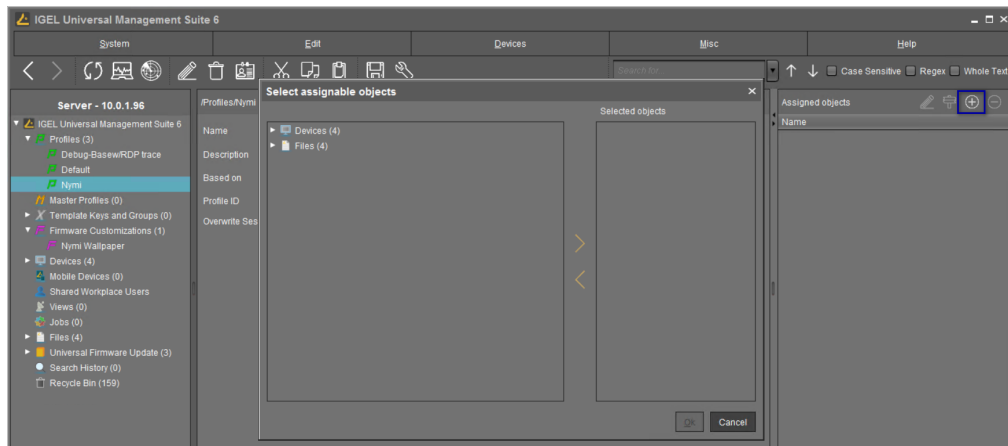
8. Click **Save**.

Assign the Profile to IGEL Devices

Assign the Nymi profile to the IGEL devices. Perform the following steps in the UMS Console.

1. In the left navigation pane, select **Profiles > Nymi**.
2. In the **Assigned Objects** pane that appears on the right side of the window, click **[+] Add**.

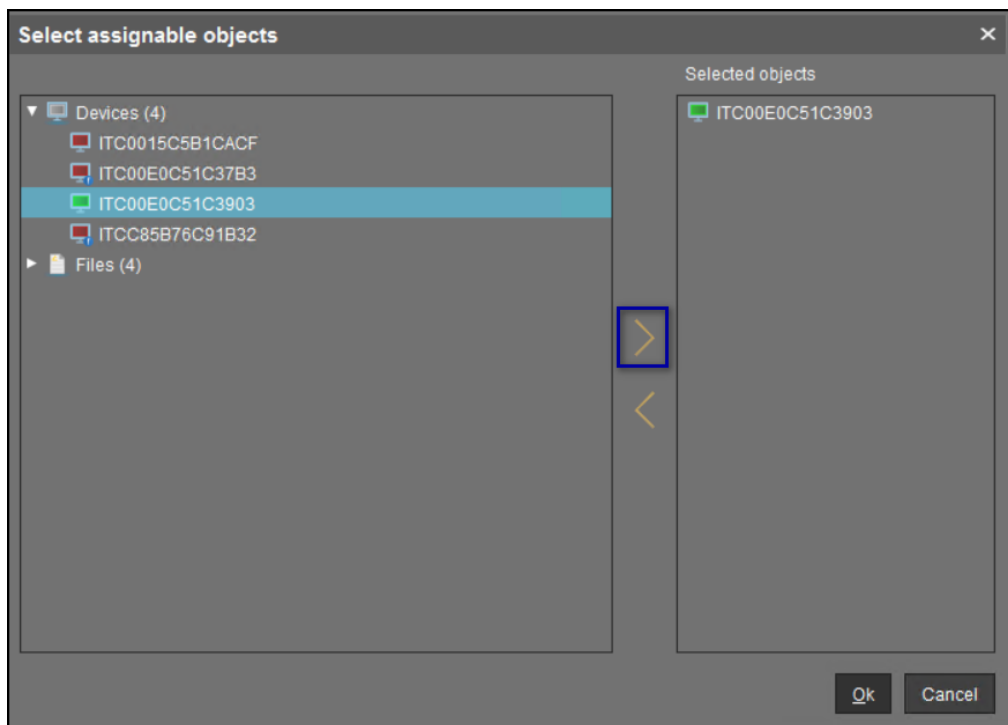
The **Select Assignable Objects** window appears.



Select Assignable Objects window

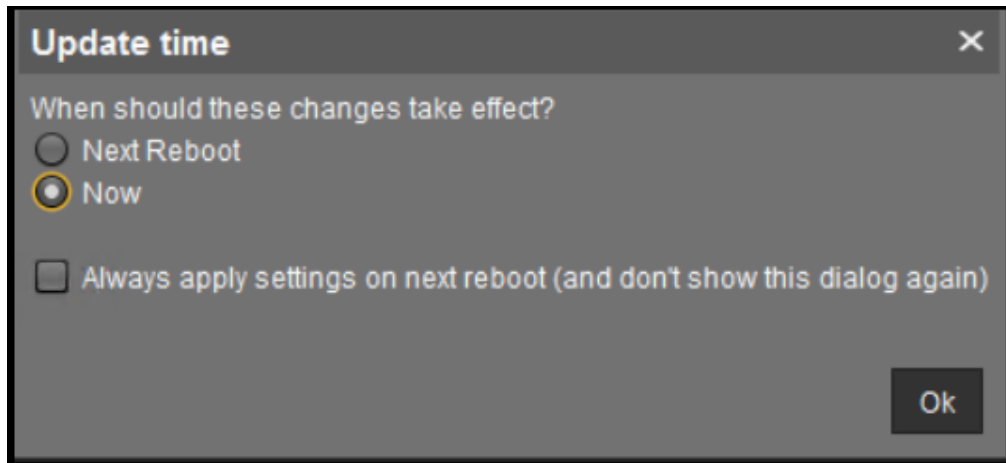
3. In the left pane, expand **Devices**, select the IGEL clients, and then click the > button.

The IGEL clients that you select appear in the **Selected objects** pane.



Selected Objects

4. Click **OK**.
5. On the **Update time?** window, select **Now**, and then click **OK**.



Update time window

The Nymi Bluetooth Endpoint package installs on the selected IGEL client.

6. After the installation completes on the IGEL client, reboot the IGEL client.

5.2.3.8 (IGEL 12) Install the Nymi Bluetooth Endpoint

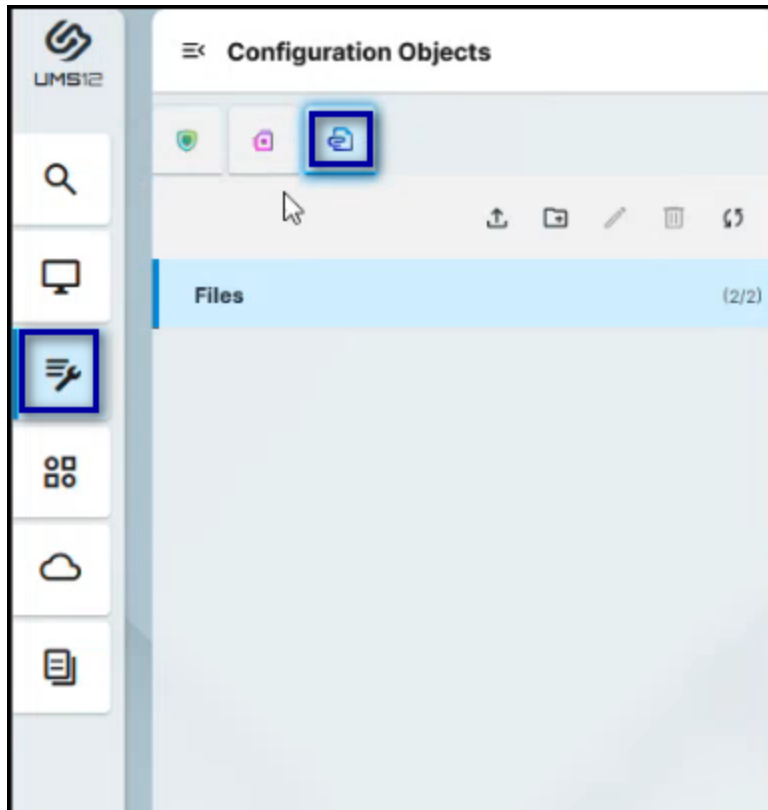
Perform the steps in this section to install Nymi Bluetooth Endpoint on IGEL 12 devices.

Upload Nymi Packages to Universal Management Suite

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

Obtain the installation package from Nymi.

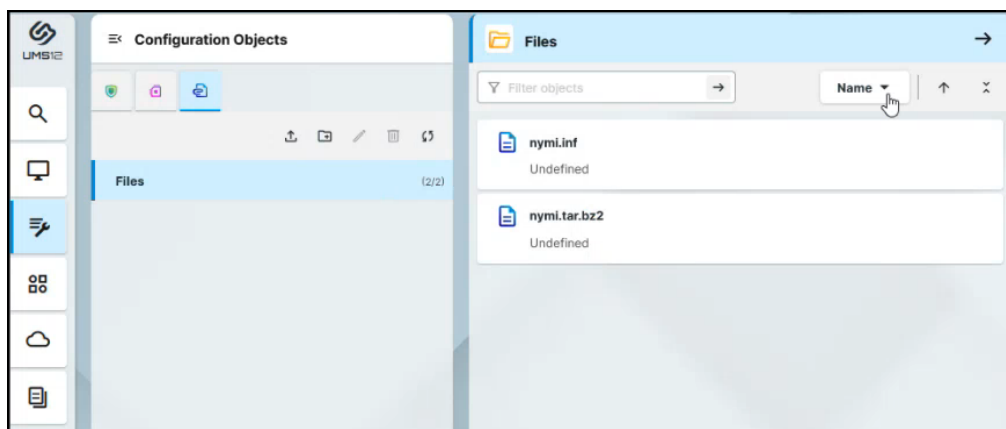
1. Extract the installation package to a machine that has access to the UMS Web App.
2. Connect to the UMS Web App, in the left navigation pane click **Configuration**, and then in the **Configuration** pane, click the **Files** button.



Files button

3. In the **File** window, click the **Upload** button, and then in the **Upload File** window, drag and drop the `nymi.inf` and `nymi.tar.gz` files.

The files appear in the Files window.

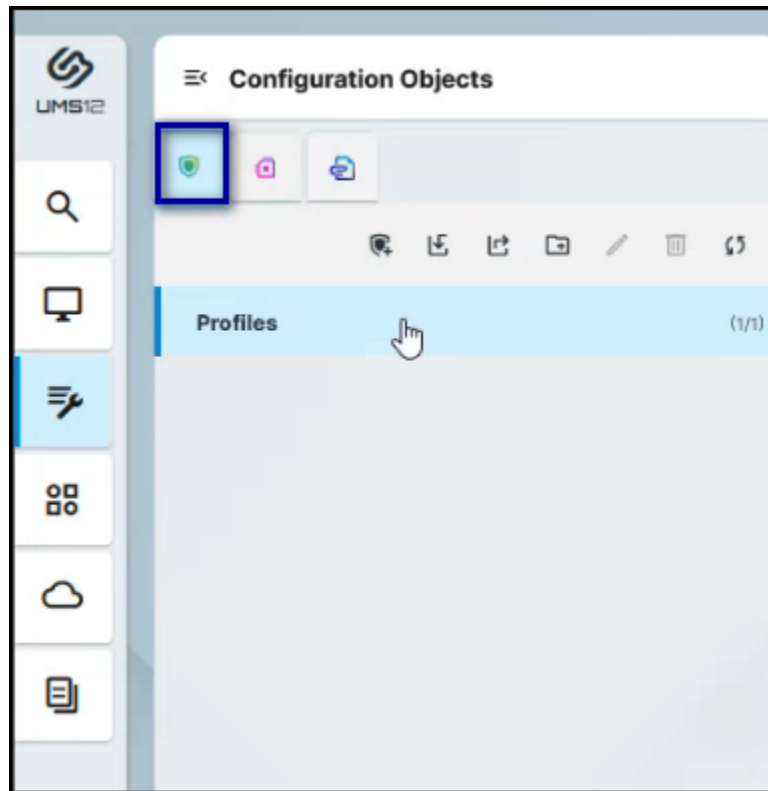


Files window

Create 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.

1. In the **Configuration options** pane, click **New Profile**.



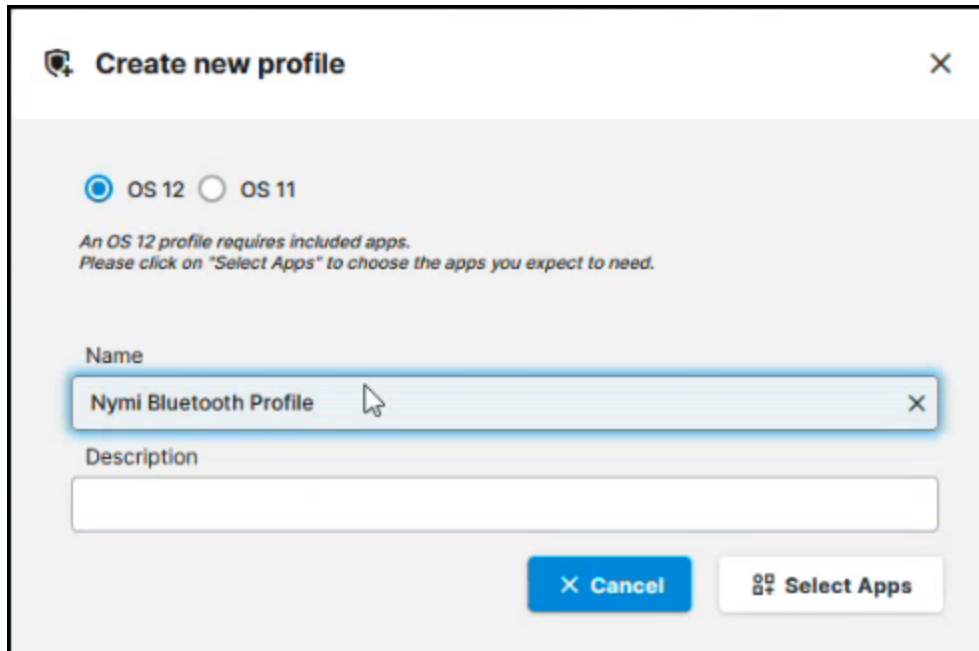
Create new profile option

2. In the **Create Profile** window, perform the following actions:

- a. Select the **OS 12** option.

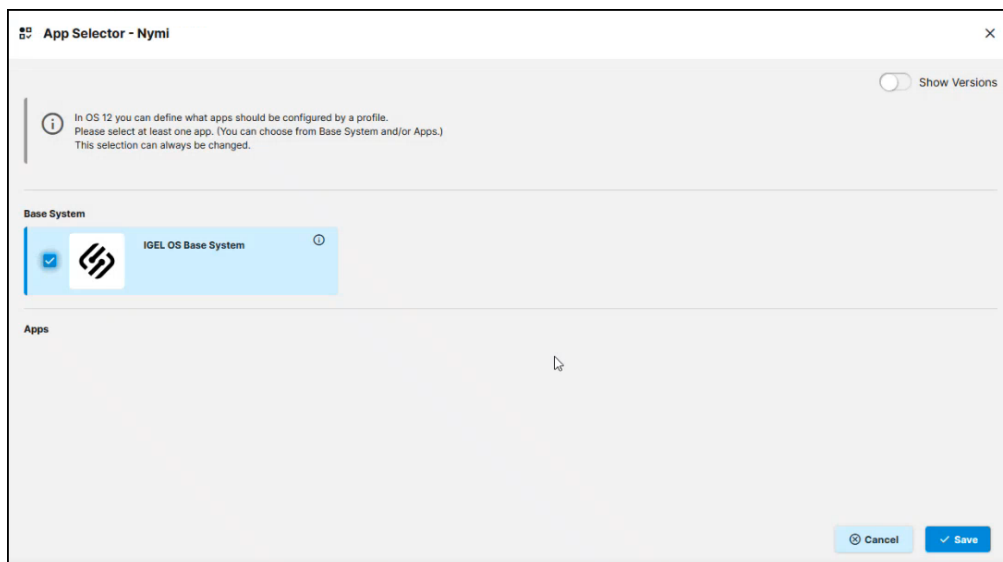
Note: You cannot use the same profile for OS 12 and OS 11.

- b. In the **Name** field, specify a name for the profile.
- c. Optionally, in the **Description** field, type descriptive information for the profile.



New Profile window

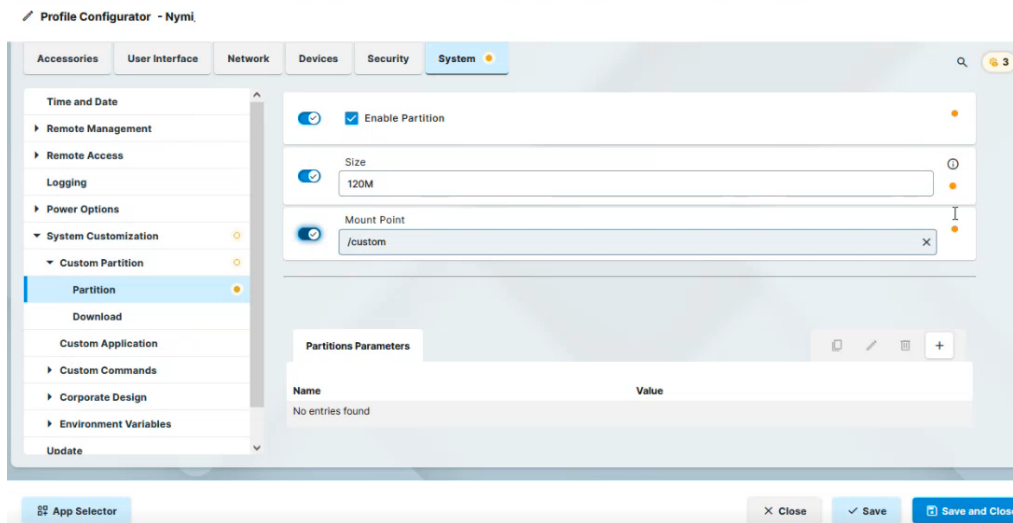
3. Click **Select Apps**, select the **IGEL OS Base system** option and then click **Save**.



Select Apps window

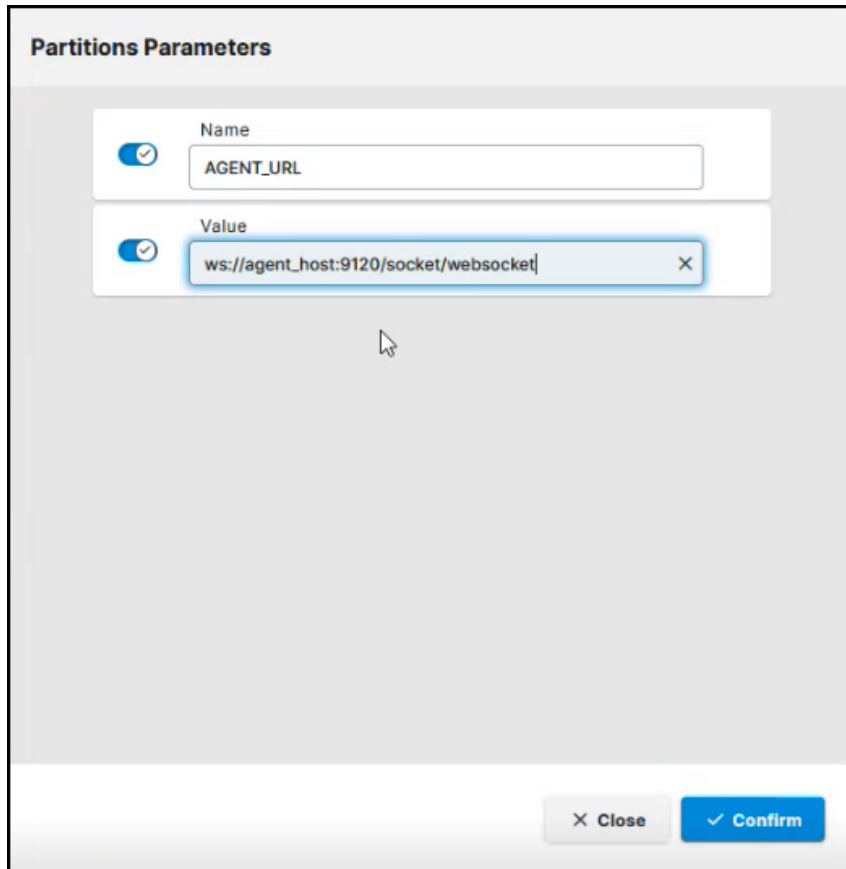
The **Setup** window opens.

4. Navigate to **System > System Configuration > Custom Partition > Partition**, and then perform the following actions.
 - a. Click the slider beside the **Enable Partition** option, and then select **Enable Partition**.
 - b. Click the slider beside the **Size** option, and then in the **Size** field, type 120M.
 - c. Click the slider beside the **Mount Point** option, and then leave the mount point value as /custom.



Set UMS partition size

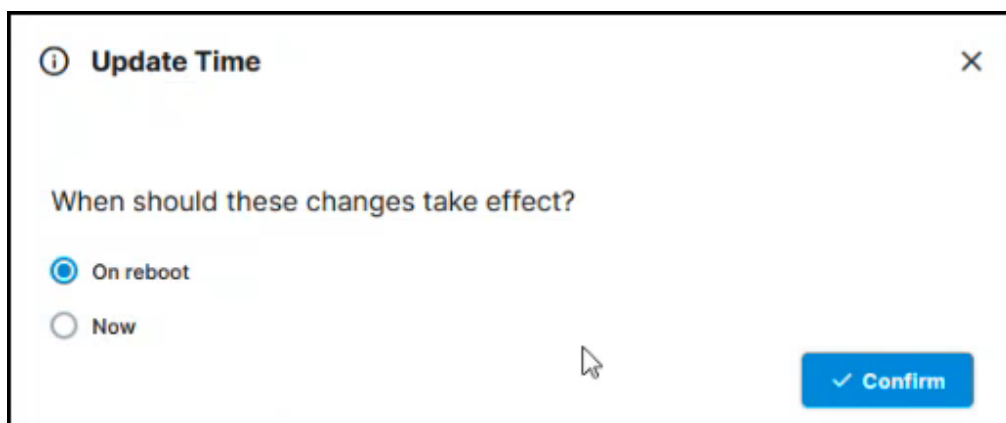
- a. In the **Partitions Parameters** section, click **[+]** (Add Item).
- b. In the **Partition Parameters** window, perform the following actions.
 1. In the **Name** field, type `AGENT_URL`.
 2. In the **Value** field, type `ws://agent_host:9120/socket/websocket`, where *agent_host* is the IP address of the server on which you installed the Nymi Agent.
 3. Click **Confirm**.



The 'Partitions Parameters' window is a light gray dialog box. It contains two sections, each with a blue toggle switch and a checkmark icon. The first section is labeled 'Name' and has a text input field containing 'AGENT_URL'. The second section is labeled 'Value' and has a text input field containing 'ws://agent_host:9120/socket/websocket|'. At the bottom right of the window are two buttons: a gray 'Close' button with an 'X' icon and a blue 'Confirm' button with a checkmark icon.

Partition Parameters window

4. Click **Save and close**.
- c. On the **Update time** window, click **On Reboot**, and then click **Confirm**.



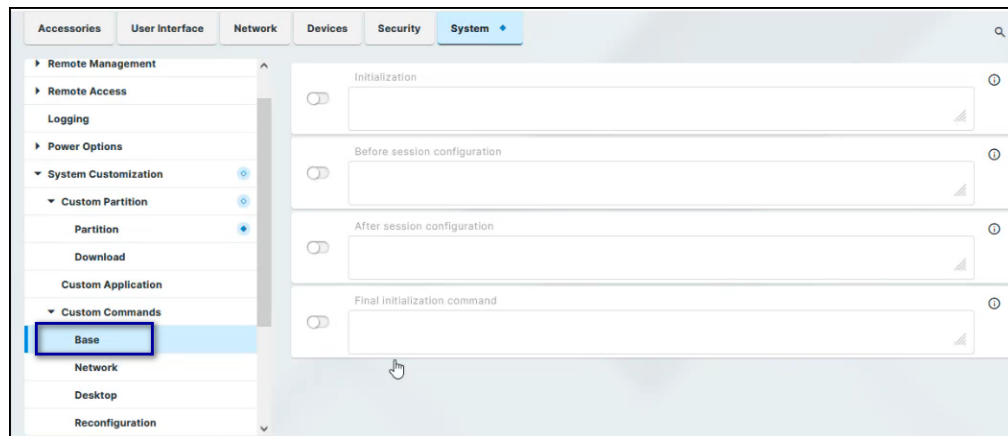
The 'Update Time' window is a light gray dialog box. It has a title bar with an information icon, the text 'Update Time', and a close 'X' icon. The main content area asks 'When should these changes take effect?'. There are two radio button options: 'On reboot' (which is selected with a blue dot) and 'Now'. At the bottom right is a blue 'Confirm' button with a checkmark icon.

Update time window

Customize the Custom Partition

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

1. From the **System** menu option for the partition, expand **System Customization > Custom Partition > Custom Commands > Base**.



Base menu option

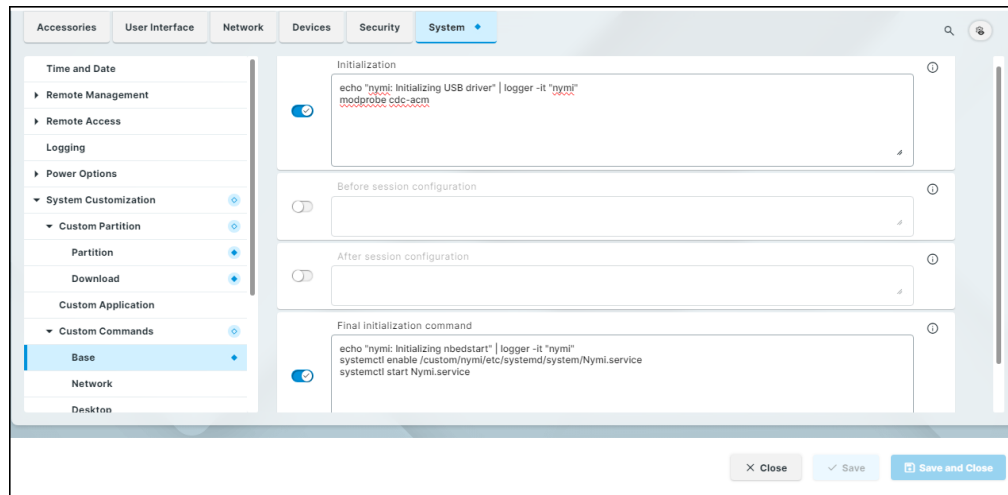
2. Perform the following actions in **Nymi Base Commands** dialog box:

- a. In the **Initialization** section, click the slider and in the field, type the following commands on separate lines:

```
echo "nyimi: Initializing USB driver" | logger -it "nyimi"  
modprobe cdc-acm
```

- a. In the **Final Initialization Command** field, click the slider and in the field, type the following commands on separate lines:

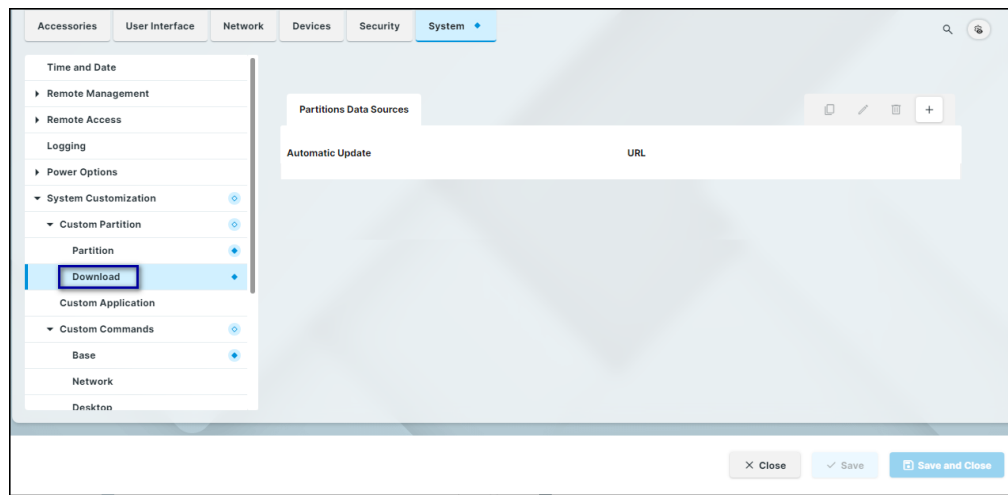
```
/custom/nyimi/usr/lib/nyimi/nbedstart&  
systemctl enable /custom/nyimi/etc/systemd/system/Nyimi.service  
systemctl start Nyimi.service
```



Nymi Base Commands

a. Click **Save**.

- From the left navigation pane for the partition, expand **System Customization > Custom Commands > Download**.



Download

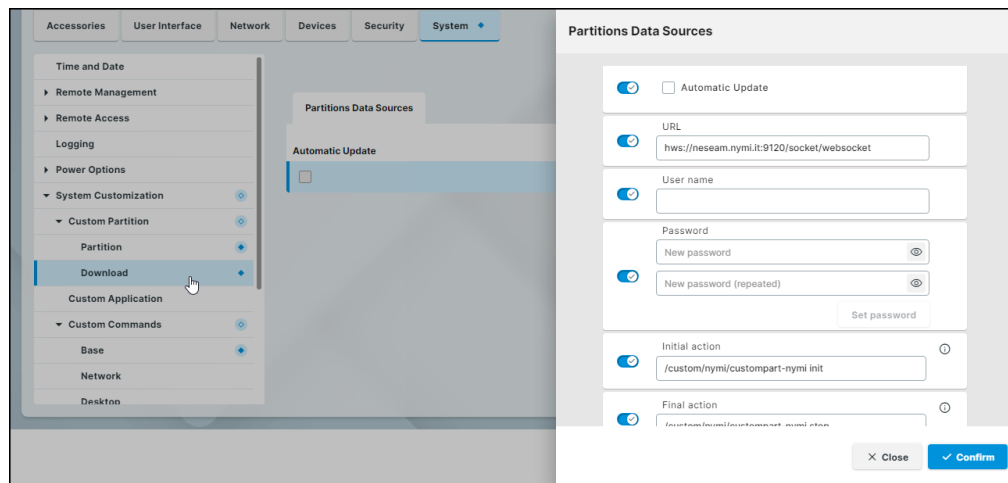
- In the **Partitions Data Sources** section, click **[+]** (Add).

A dialog box appears.

- Perform the following actions in the **Partition Data Sources** window.

a. In the **URL** field, type the Download URL path for the `nyml.inf` file. For example, `https://10.0.1.61:8443/ums_filetransfer/nyml.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 **Initial Action** field, type `/custom/nymi/custompart-nymi init.`
- e. In the **Final Action** field, type `/custom/nymi/custompart-nymi stop.`
- f. Click **Confirm**.



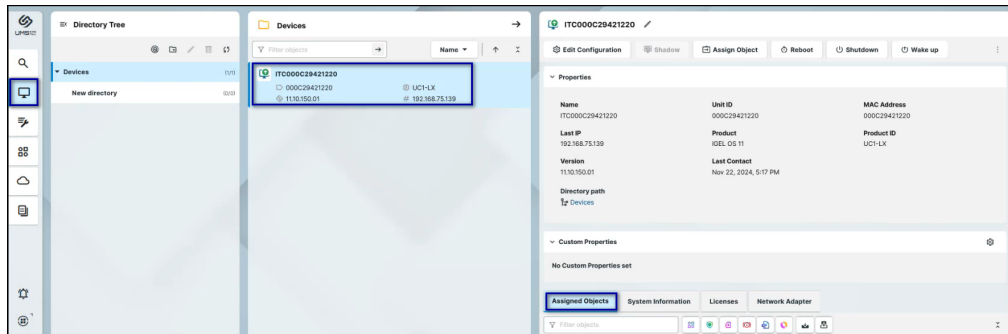
Partition Data Sources window

6. Click **Confirm**.
7. Click **Save and close**.
8. On the **Update time** window, click **On Reboot**, and then click **Confirm**.

Assign the Profile to IGEL Devices

Assign the Nymi profile to the IGEL devices from the UMS Web App.

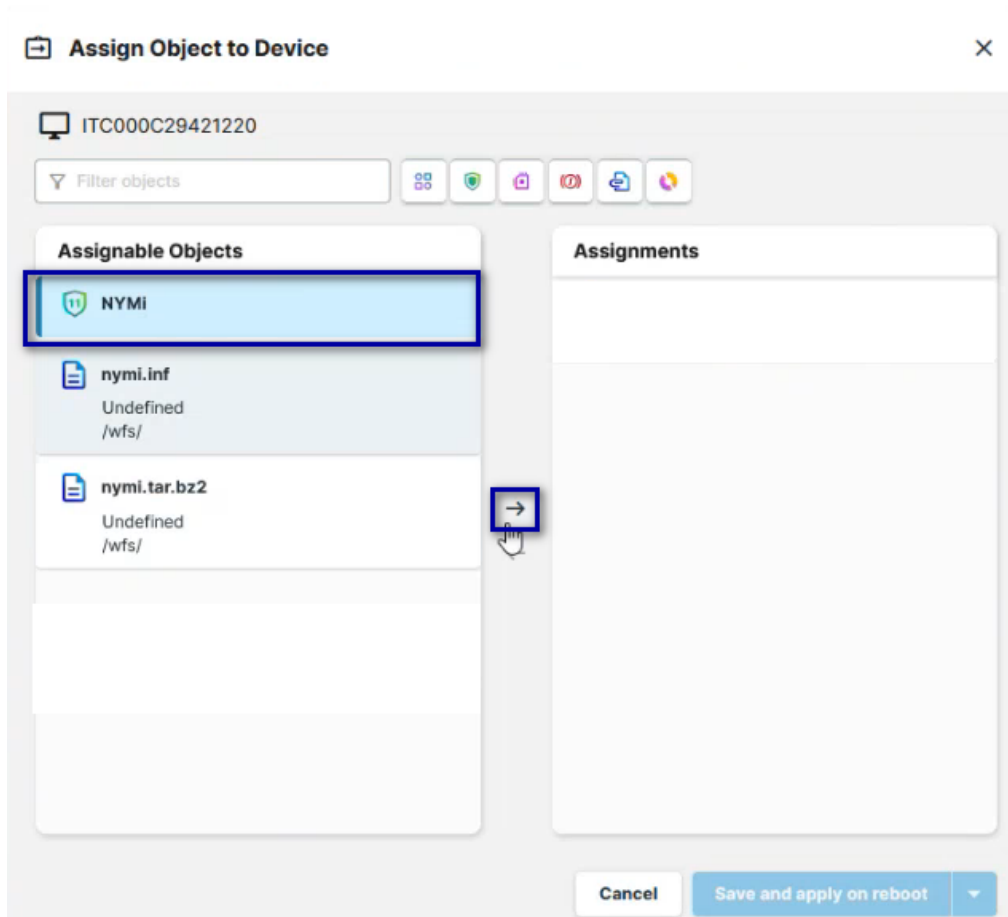
1. In the left navigation pane, select **Directory**. In the **Devices** pane that appears on the right side of the window, select the device, and then in the device properties window, click the **Assigned Devices** tab.



Assigned Devices option

2. In the left pane, expand **Devices**, select the IGEL clients, and then click the > button.

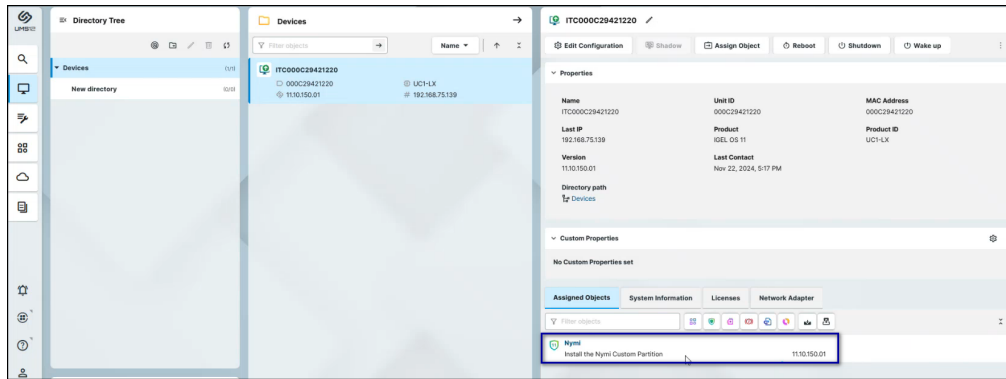
The IGEL clients that you select appear in the **Selected objects** pane.



Selected Objects

3. Click **Save and apply on reboot** or **Save and apply now**.

The **Assigned Objects** section displays the Nymi profile.



Assigned device

4. Reboot the IGEL client.

5.2.3.9 Configure the Communication Protocol

Refer to [Configure the CWP Communication Protocol](#) for instructions.

5.2.4 Set Up User Terminals for Lock and Unlock (Remote)

You can use the Nymi Band to lock and unlock the desktop of the user terminal that you use to connect to the remote session hosts. You can also use the Nymi Band to lock and unlock virtual desktops.

User terminals on which you will use the Nymi Band to lock and unlock require that you:

- Import the Root CA certificate, if the Root CA is not a Trusted Root CA.
- Place the Bluetooth adapter.
- Install the Nymi Bluetooth Endpoint service.
- Install Nymi Lock Control.
- Configure the Nymi Bluetooth Endpoint configuration file.

5.2.4.1 Configure Nymi Lock Control

Refer to [Configure Nymi Lock Control](#) for instructions on enabling Nymi Lock Control in the NES Administrator Console.

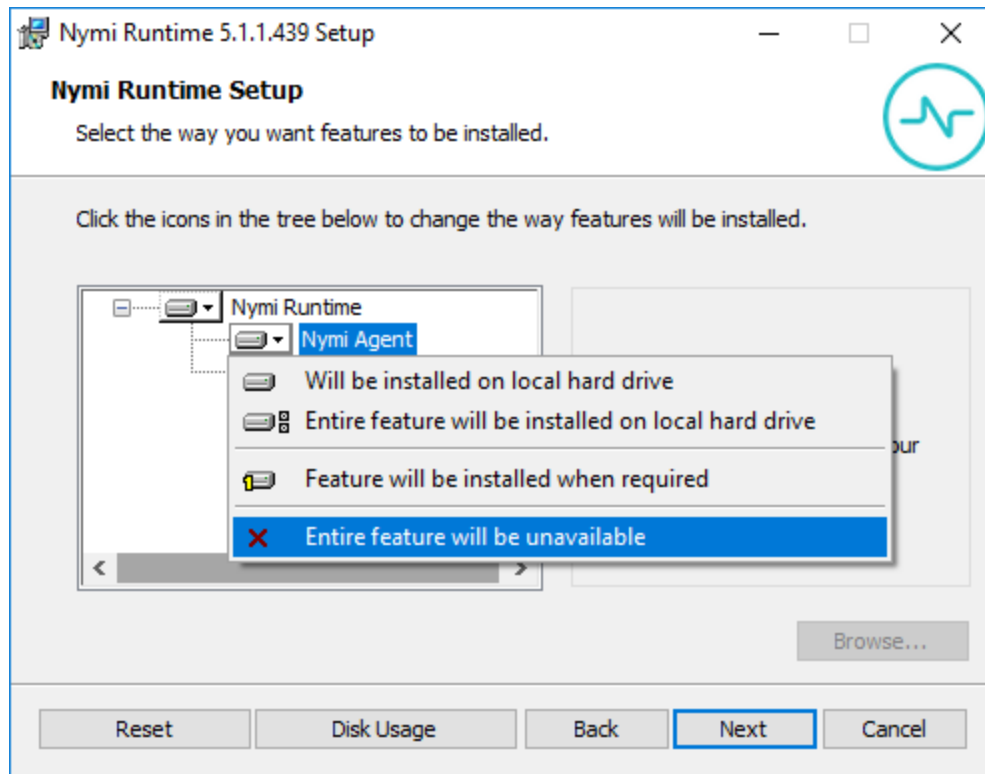
5.2.4.2 Import the Root CA Certificate

Refer to [Import the Root CA Certificate in Citrix/RDP Environments](#) for instructions.

5.2.4.3 Install Nymi Lock Control (Remote)

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

1. Right-click `NymiLockControl-installer-vw.x.y.z` and select **Run as administrator**.
2. On the **User Account Control** window, click **Yes**.
3. On the **Welcome to the Prerequisites Setup Wizard**, click **Next**.
4. On the **Prerequisites** window, leave the default selections, and then click **Next**.
5. On the Welcome window, click **Install**.
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**.



Nymi Agent feature will be unavailable

9. On the **Service Account** window, perform one of the following actions:
 - Accept the default service account NTAAuthority, click **Next**.
 - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **Next**.
10. On the **Ready to install** page, click **Install**.
11. Click **Finish**.
12. On the **Installation Completed Successfully** page, click **Close**.
13. On the **Welcome to Nymi Lock Control Setup Wizard** window, click **Next**.
14. On the **Select Installation Folder** window, click **Next**.
15. On the **Ready to Install** window, click **Install**.
16. On the **Completing the Nymi Lock Control Setup Wizard** window, click **Finish**.

5.2.4.4 Edit the Nymi Bluetooth Endpoint Configuration File

Refer to [\(Windows and HP Thin Pro\) Edit the Nymi Bluetooth Endpoint Configuration File](#) for instructions.

5.2.4.5 Set the NES URL (Remote)

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

1. Run `regedit.exe`.
2. On the **User Account Control** window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software**.
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/`, where *nes_server* is the FQDN of the NES host and *NES_service_name* is the service mapping name for NES in IIS.
7. Click **OK**.

5.2.4.6 Configure Support for Citrix/RDP Lock and Unlock

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

Perform the following steps on each user terminal.

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. Navigate 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`.

5.2.4.7 Configure Support for Virtual Desktop Lock and Unlock

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

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

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 **CacheClientIp** and in the **Value Data** field, type `00000001`.
6. Click **OK**.
7. Right-click **Nymi Lock Control**, and then select **New > String value**.
8. In the **Value** field, type `ViewClientVariable`.
9. Double-click **ViewClientVariable** and in the **Value Data** field, type `ViewClient_Broker_Remote_IP_Address`.
10. Click **OK**.

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 Nymi-enabled Application at the same time.

5.2.4.8 Configure the Communication Protocol

Refer to [Configure the CWP Communication Protocol](#) for instructions.

5.2.4.9 Edit the Nymi Bluetooth Endpoint Configuration File

Refer to [Edit the Nymi Bluetooth Endpoint Configuration File](#) for instructions on tuning RSSI values for Nymi Lock Control.

6 Set Up a Centralized Nymi Agent

When your environment uses iOS devices, applications on RDP/Citrix session hosts, and web-based Nymi-enabled Applications (NEAs), you must deploy a centralized Nymi Agent on a Windows server in the environment, such as the Nymi Enterprise Server (NES) server.

The Nymi Agent has two server interfaces:

- Standard Nymi Agent interface. By default, the standard Nymi Agent interface connects over plain text websocket.
- Nymi WebAPI interface. By default, the Nymi WebAPI interface is disabled.

Nymi recommends that you configure the Nymi Agent to use secure websocket connections for both the standard Nymi Agent interface, and if enabled, the Nymi WebAPI interface. This chapter provides more information.

6.1 Import the Root CA Certificate

Perform the following steps only if the Root CA issuing the TLS server certificate is not a Trusted Root CA. For example, when you use a self-signed TLS server certificate.

Prerequisites: Install the Root CA on the following machines:

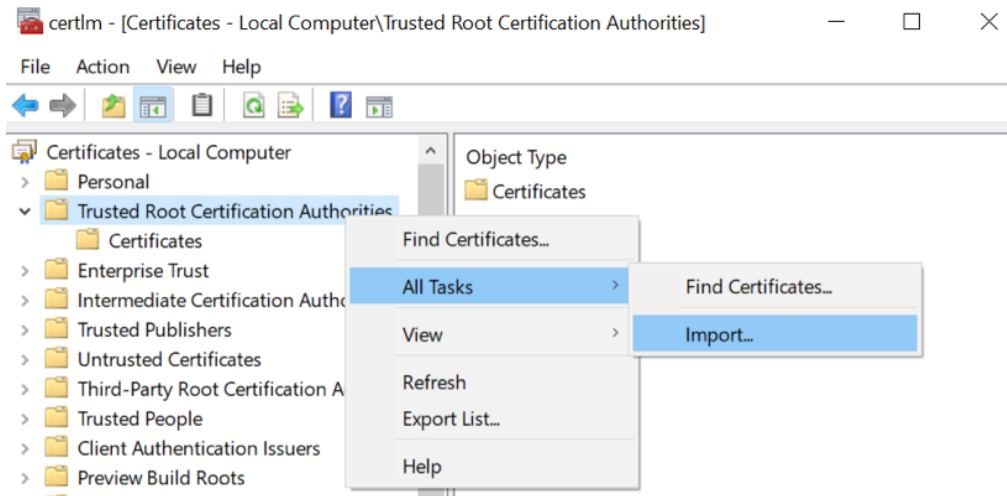
- All user terminals, including user terminals that run Nymi-enabled Applications
- Enrollment terminal
- Centralized Nymi Agent

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.

Note: This procedure was written for Windows 10.

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**.

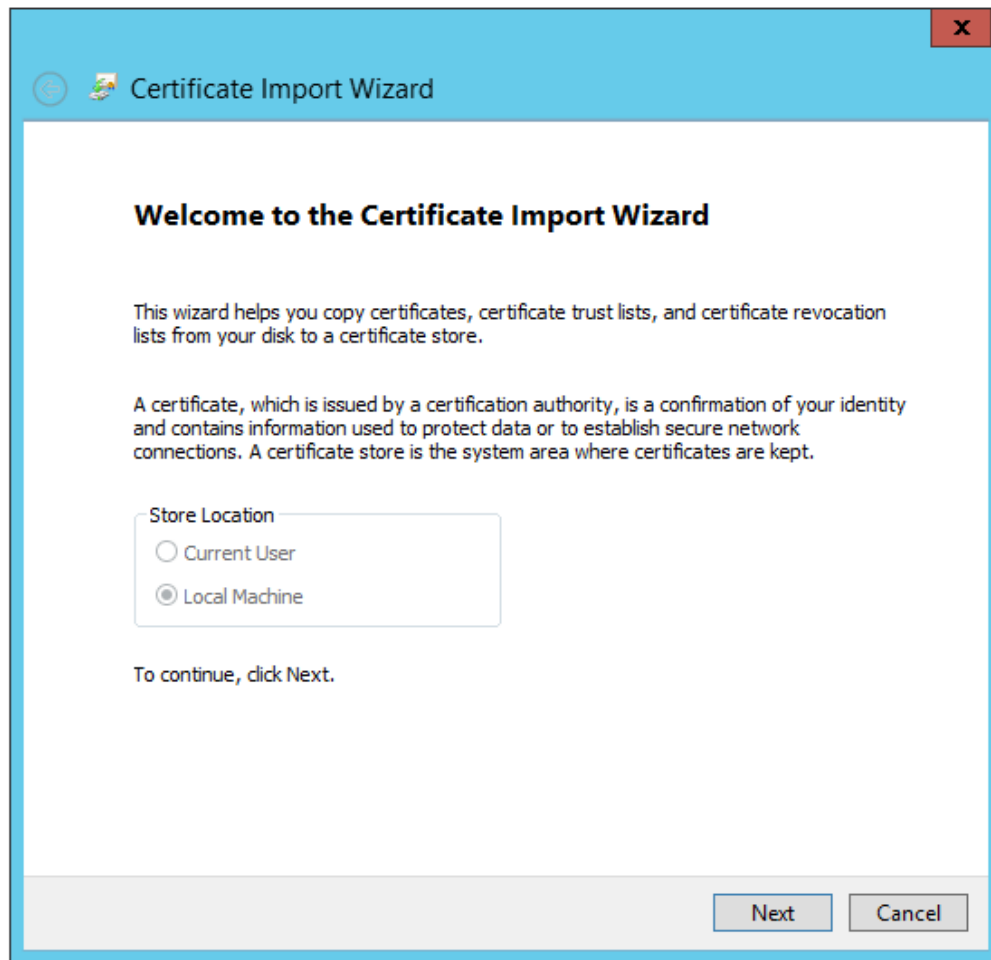
The following figure shows the **certlm** window.



certlm application

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

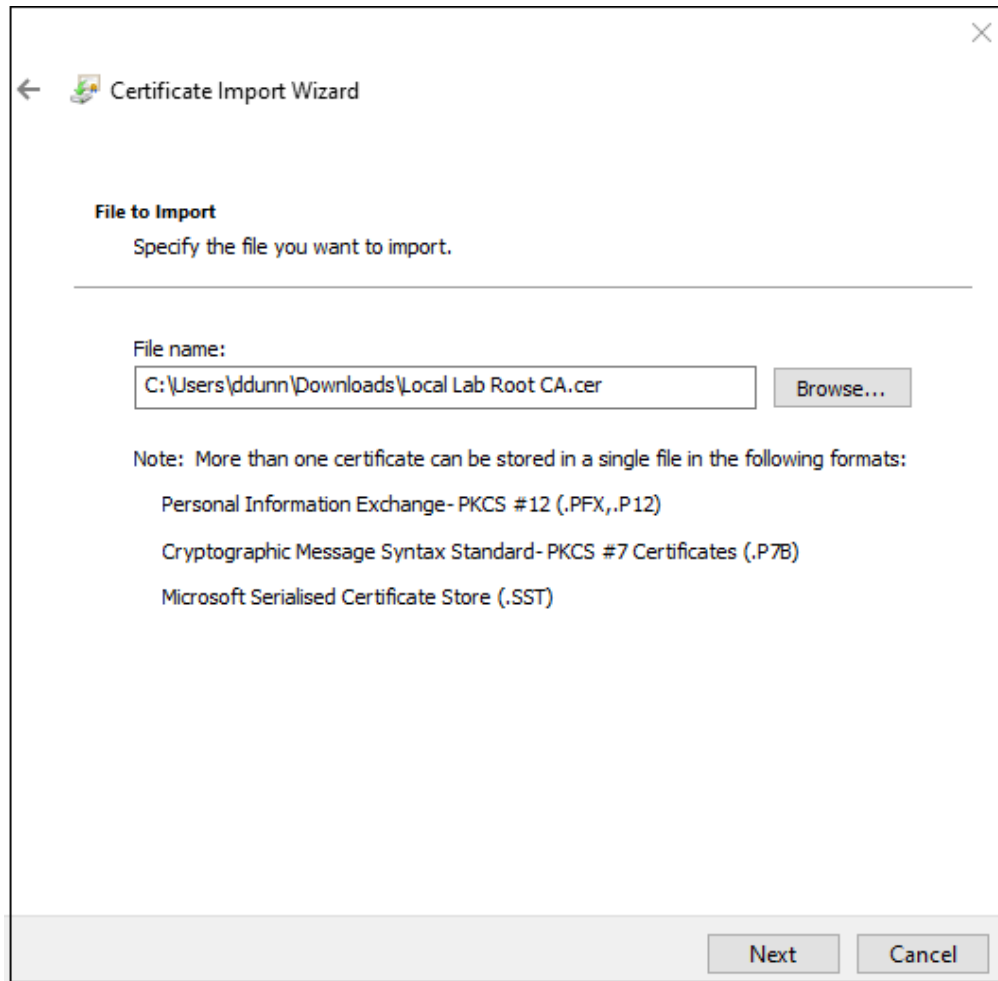
The following figure shows the **Welcome to the Certificate Import Wizard** screen.



Welcome to the Certificate Import Wizard screen

4. On the **File to Import** screen, click **Browse**, navigate to the folder that contains the 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.



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**.

6.2 Install the Nymi Agent on the Centralized Server

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

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

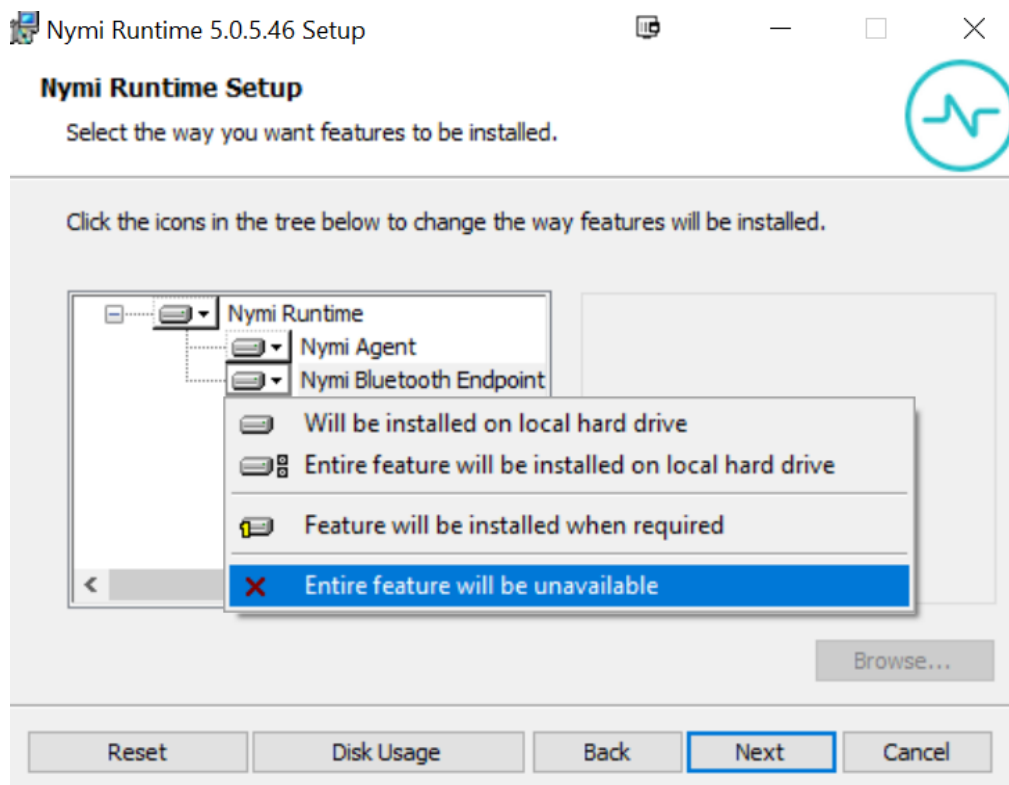
1. Log in to the terminal with an account that has administrator privileges.

2. Extract the Nymi SDK distribution package.
3. From the `..\nymi-sdk\windows\setup` folder, right-click the `Nymi Runtime Installer version.exe` file, and select **Run as administrator**.
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.

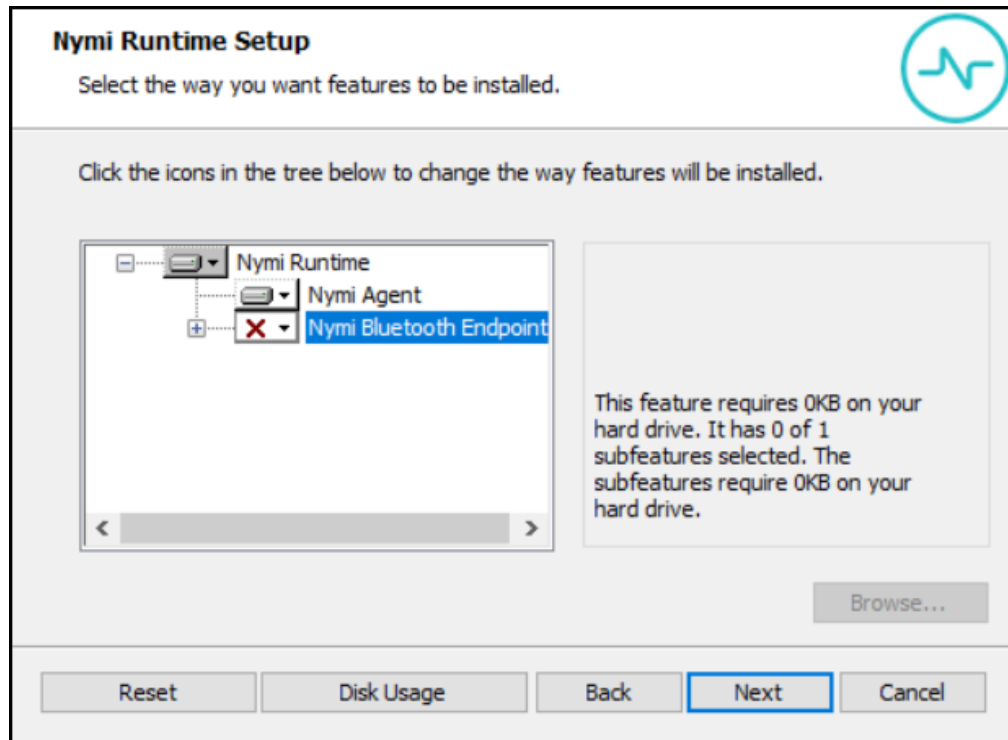
6. On the **Welcome to the Nymi Runtime Setup Wizard** page, click **Next**.
7. On the **Nymi Runtime Setup** page, expand **Nymi Runtime**.
8. Select **Nymi Bluetooth Endpoint**, and then select **Entire feature will be unavailable**.

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



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**.



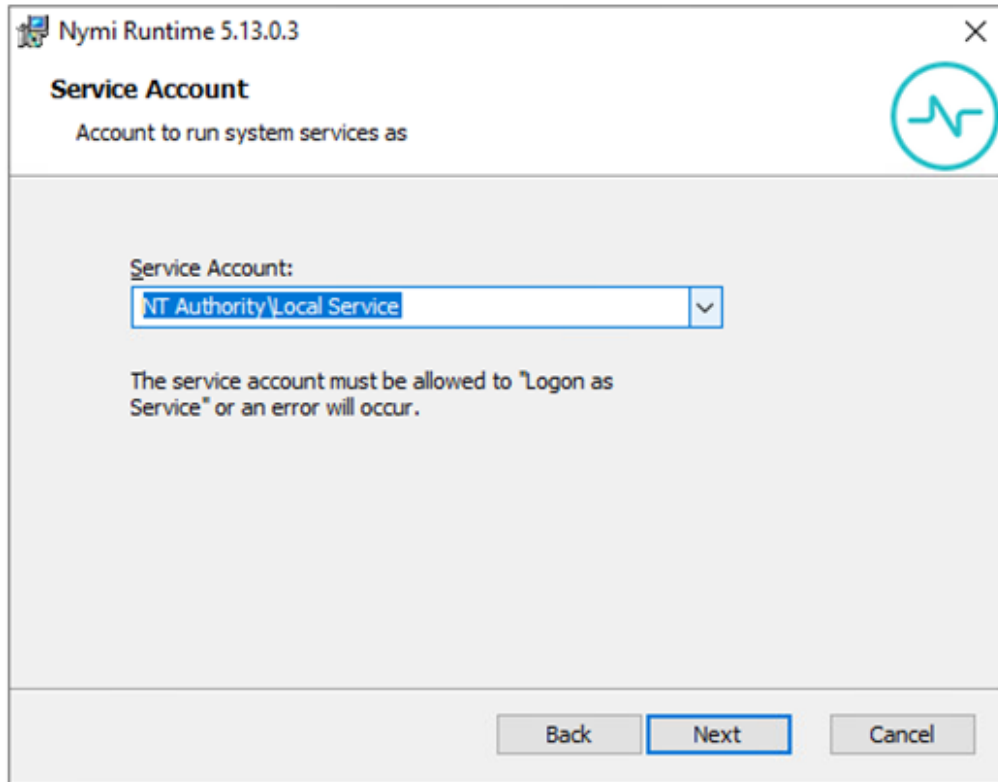
Nymi Bluetooth Endpoint feature is not available

10. On the **Service Account** window, perform one of the following actions to choose the account that starts the service:

- Accept the default service account NTAuthority, click **Next**.
- For non-English Windows Operating Systems and for Nymi WebAPI configurations where you install the centralized Nymi Agent on the NES server, choose the LocalSystem account from the drop list, and then click **Next**.

Note: The service account must have permission to run as a service. [Enable Service Log On](#) provides more information about how to modify the local policy to enable this permission for the service account.

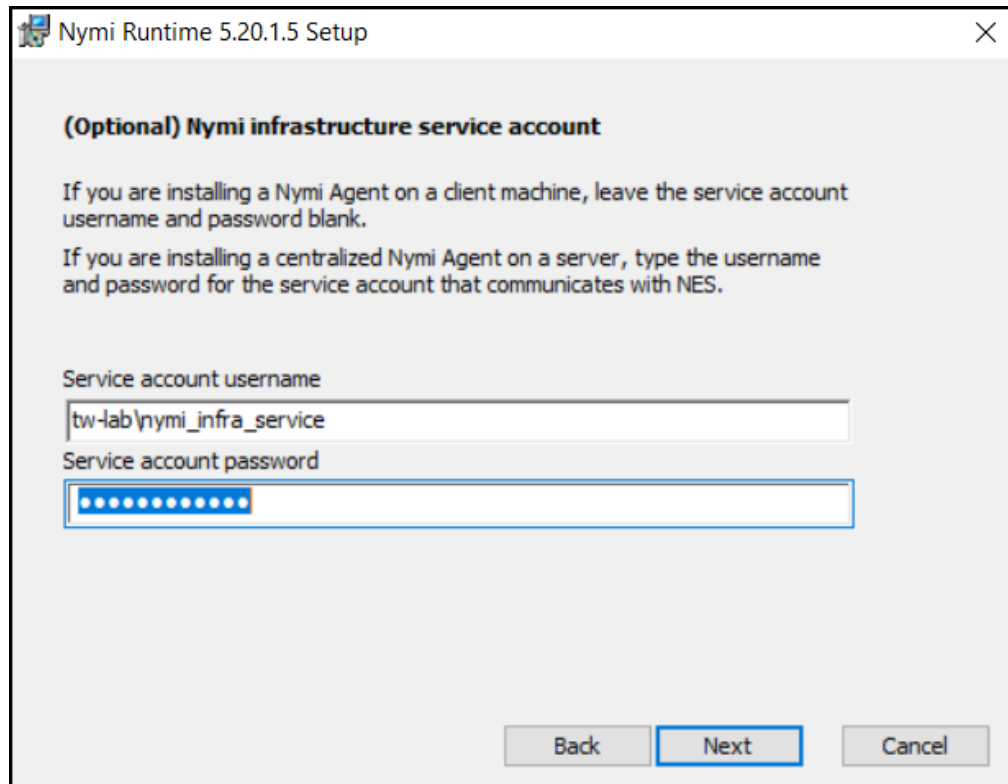
The following figure shows the **Service Account** window.



Nymi Runtime Service Account window

11. On the **(Optional) Nymi Infrastructure Service Account** window, specify the username and password of the Nymi Infrastructure Service Account. When you specify the username, include the domain name, for example `tw-lab\nymi_infra_service_acct`.

The following figure shows the **Nymi Infrastructure Service Account** window.



Nymi Infrastructure Service Account window

The installer creates the following files in the `C:\Nymi\NymiAgent\certs` folder:

- `credentials` — contains the encrypted credentials for the Nymi Infrastructure Service Account
- Private key, which is used to encrypt the credentials
- Public key, which is used to encrypt the credentials

12. On the **Ready to install** page, click **Install**.

13. Click **Finish**.

14. On the **Installation Completed Successfully** page, click **Close**.

Use the Services applet to confirm that the status of the Nymi Agent service is running.

6.3 Configure the Nymi Agent

A centralized Nymi Agent uses a TOML formatted configuration file to set configuration parameters, such as defining the log level, enabling Nymi WebAPI, and enabling the use

of secure websocket communications between the centralized Nymi Agent and other Nymi components.

Nymi provides a sample TOML file that you can rename and edit to define the configuration for your environment and use case. Perform the following steps on the Nymi Agent machine.

1. Change to the `C:\Nymi\NymiAgent` directory.
2. Rename the `C:\Nymi\NymiAgent\nymi_agent_default.toml` file to `C:\Nymi\NymiAgent\nymi_agent.toml`.
3. Edit the `C:\Nymi\NymiAgent\nymi_agent.toml` file. The following table summarizes the available parameter settings and when to use each setting.

Note: The TOML file has several sections and some sections contain parameter names that are the same. Ensure that you are in the correct section before you make updates.

Parameter and Sample Value	Section	Description
<code>log_level = "warn"</code>	[agent]	Required. Defines the debug logging level. Change the value when instructed by Nymi. Supported values: error (log only errors), warn (log errors and warnings), info (log errors, warnings, and activity), debug (log everything including debugging information). The default value is <code>warn</code> .
<code>protocol = "wss"</code>	[agent]	Optional. To enable the standard Nymi Agent to use secure websocket communications, uncomment <code>protocol</code> and change the value to <code>wss</code> . Requires configuration of the <code>cacertfile</code> , <code>certfile</code> , and <code>keyfile</code> parameters in the [agent] section.
<code>port = 9120</code>	[agent]	Optional. Defines an alternate server port on which Nymi Agent communicates with the Nymi Bluetooth Endpoint and NEAs. The default port number is 9120. Nymi recommends that

Parameter and Sample Value	Section	Description
		you use the default port number.
<code>cacertfile = "certs/LocalLabRootCA3.pem"</code>	[agent]	Required when you want to use the wss protocol to secure communication between the centralized Nymi Agent and Nymi Bluetooth Endpoint, and Nymi Agent and native NEAs. Uncomment and specify the path to the PEM-formatted CA certificate bundle. The CA certificate bundle must start from the root CA and end in the subordinate CA issuing the server certificate. Requires configuration of <code>protocol = "wss"</code> , <code>certfile</code> , and <code>keyfile</code> parameters in the [agent] section.
<code>certfile = "certs/tw-srv1.tw-lab.local-cert.pem"</code>	[agent]	Required when you want to use the wss protocol to secure communication between the centralized Nymi Agent and Nymi Bluetooth Endpoint, and Nymi Agent and native NEAs. Uncomment and specify the path to the TLS certificate file containing the Nymi Agent server certificate in PEM format. Requires configuration of <code>protocol = "wss"</code> , <code>cacertfile</code> , and <code>keyfile</code> parameters in the [agent] section.
<code>keyfile = "certs/tw-srv1.tw-lab.local-key.pem"</code>	[agent]	Required when you want to use the wss protocol to secure communication between the centralized Nymi Agent and Nymi Bluetooth Endpoint, and Nymi Agent and native NEAs. Uncomment and specify the path to the TLS certificate private key file, unencrypted and PEM formatted. Requires configuration of <code>protocol = "wss"</code> , <code>cacertfile</code> , and <code>certfile</code> parameters in the [agent] section.

Parameter and Sample Value	Section	Description
<code>nea_name = "NymiWebAPI"</code>	[nes]	Required for Nymi WebAPI. Uncomment this parameter to set the NEA name for the Nymi WebAPI server application.
<code>nes_url = "https:// server.name.local.com"</code>	[nes]	Required for Nymi WebAPI. Uncomment and specify the host URL for the NES server. Include only the protocol and hostname portion of the URL. For example, <code>https://myserver.name.local.com</code> .
<code>directory_service_id = "NES_DPS"</code>	[nes]	Required for Nymi WebAPI. Uncomment and specify the instance name for NES. For example, if your NES URL is <code>https://server.name.local.com/NES</code> , the directory/instance name is NES. For example, <code>directory_service_id = "NES"</code> .
<code>credentials_location = certs/</code>	[nes]	Required when you specified a Nymi Infrastructure Service Account during the Nymi Agent installation. Uncomment this line and leave the default value. The <code>credentials_location</code> parameter enables the use of the Nymi Infrastructure Service Account to complete authentication tasks with underlying functionality that improves the performance of Nymi Band taps in web-based NEAs and with BLE Taps. Note: The <code>certs</code> folder contains a file with the encrypted username and password for the Nymi Infrastructure Service Account.
<code>protocol = "wss" or protocol = "ws"</code>	[webapi]	Required for Nymi WebAPI. Defines the connection protocol. If your deployment does not use Nymi WebAPI, leave both lines commented out. Uncomment <code>protocol = "wss"</code> to enable secure websocket connections, or <code>protocol = "ws"</code> to use plain text websocket

Parameter and Sample Value	Section	Description
		connections. Note: The wss protocol requires configuration of the <code>cacertfile</code> , <code>certfile</code> , and <code>keyfile</code> parameters in the <code>[webapi]</code> section.
<code>port = 443 or port = 80</code>	<code>[webapi]</code>	Optional for Nymi WebAPI. Defines an alternate server port on which Nymi Agent listens for Nymi WebAPI client WebSocket connections. By default the <code>ws</code> protocol listens on 80 and the <code>wss</code> protocol listens on 443. To change the default port uncomment one of the following lines and specify the port number that applies to your configuration: for the <code>ws</code> protocol, uncomment <code>port = 80</code> ; for the <code>wss</code> protocol, uncomment <code>port = 443</code> .
<code>cacertfile = "certs/LocalLabRootCA3.pem"</code>	<code>[webapi]</code>	Required when the Nymi Agent uses the Nymi WebAPI with wss. Uncomment and specify the path to the PEM-formatted CA certificate bundle. The CA certificate bundle must start from the root CA and end in the subordinate CA issuing the server certificate. Requires configuration of the <code>protocol = "wss"</code> , <code>certfile</code> , and <code>keyfile</code> parameters in the <code>[webapi]</code> section.
<code>certfile = "certs/tw-srv1.tw-lab.local-cert.pem"</code>	<code>[webapi]</code>	Required when the Nymi Agent uses the Nymi WebAPI with wss. Uncomment and specify the path to the TLS certificate in PEM format. Requires configuration of the <code>protocol = "wss"</code> , <code>cacertfile</code> , and <code>keyfile</code> parameters in the <code>[webapi]</code> section.
<code>keyfile = "certs/tw-srv1.tw-lab.local-key.pem"</code>	<code>[webapi]</code>	Required when the Nymi Agent uses the Nymi WebAPI with wss. Uncomment and specify the path to the TLS certificate private key in unencrypted PEM format. Requires configuration

Parameter and Sample Value	Section	Description
		of the protocol = "wss", cacertfile, and certfile parameters in the [webapi] section.

4. For secure Nymi Agent and secure WebSocket, copy the following files to the C:\Nymi\NymiAgent\certs directory:

- CA root certificate bundle in PEM format (when you use a Trusted Root CA only)
- Server certificate in PEM format
- Server certificate private key in PEM format

Note: Secure Nymi Agent and secure WebSocket can share the CA root certificate bundle file, the server certificate file, and the server certificate private key file. Therefore, create only one copy of each file for both secure Nymi Agent and secure WebSocket.

5. Restart the **Nymi Agent** service.

7 Upgrade the Connected Worker Platform

This section describes how to upgrade CWP components from a previous version.

First, review the *Release Notes* for information regarding the order of component updates as well as backwards compatibility information, and then review the following information to plan your update. Infrastructure refers to NES, the NBA, and the Nymi Runtime software.

Note: You cannot update Nymi Band 2.0 with CWP firmware or use Nymi Band 2.0 with CWP infrastructure.

CWP 1.12.x and later provides Nymi-enabled Application developers with enhancements that optimize Bluetooth tap performance for web-based NEAs. After you update the Nymi-enabled Application to a version that uses the new functionality available starting with the CWP 1.12.x Nymi SDK (Authenticated Tap), ensure that each user with a Nymi Band that was enrolled prior to the update logs in to the NBA while wearing their authenticated Nymi Band. The NBA applies changes to the Nymi Band that support the optimization.

Consider the following information:

- You must update the NBA on the enrollment terminal before you attempt any new enrollments with a CWP NES.
- You can update NES, NBA, and Nymi Runtime directly from NEE 3.3.x or CWP 1.3.x and later.
- You can use a Nymi Band 3.0 that runs pre-CWP firmware with CWP infrastructure; however, new functionality is not available.
- You cannot use a Nymi Band 3.0 that runs CWP 1.12.x and later firmware with pre-CWP 1.12.x infrastructure.
- The CWP NBA can only enroll and externally authenticate Nymi Bands with the CWP 1.6 and later firmware.
- When you update the firmware from NEE 3.3.0 and earlier, you must re-enroll the Nymi Band.

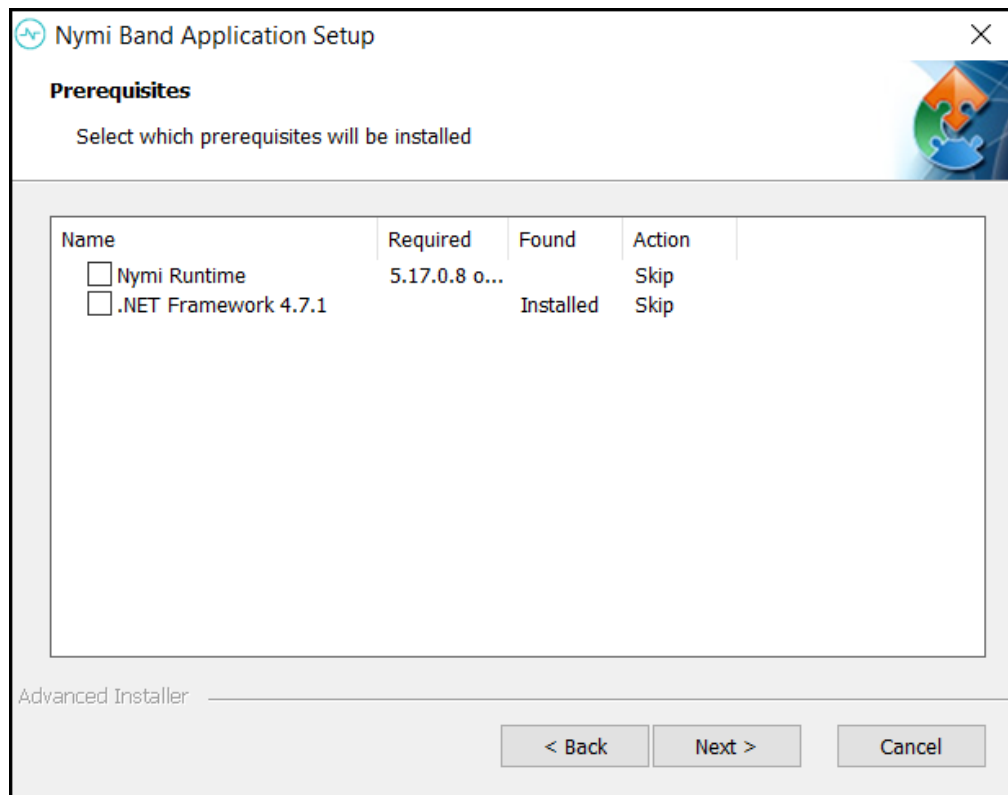
7.1 Update the Enrollment Terminal

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

7.1.1 Update the Centralized NBA

Perform the following steps to update the NBA.

1. Create a backup copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file.
2. Download the NBA package.
3. Double-click the `Nymi-Band-App-installer-v_version.exe` file.
4. On the **User Account Control** window, click **Yes**.
5. On the **Prerequisites** window, click **Next**.
6. On the **Welcome** page, click **Install**.
7. On the **User Account Control** page, click **Yes**.
8. On the **Welcome to the Nymi Runtime Setup Wizard** page, click **Next**.
9. On the **Prerequisites** window, clear the option to install Nymi Runtime, and then click **Next**.



No Nymi Runtime Installation

10. On the **Ready to install** page, click **Install**.
11. Click **Finish**.
12. On the **Installation Completed Successfully** page, click **Close**.
13. On the **Welcome to Nymi Band Application Setup Wizard** window, click **Next**.
14. On the **Select Installation Folder** window, click **Next** to accept the default installation location.
15. In the **Ready to Install** window, click **Install**.
16. On the **Completing the Nymi Band Application Setup Wizard** window, click **Finish**.
17. Stop the **Nymi Bluetooth Endpoint** service.

18. Edit the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file. Compare and modify the following parameter values as required, with the value that appears in your backed up `nbe.toml` file:

a. `agent_url` parameter.

b. RSSI parameters. Entries that appear in a CWP 1.19.2 and earlier TOML file apply to the Bluegiga Bluetooth Adapter; therefore, update the values that appear in the `[dongle.bluegiga]` section.

c. `endpoint_id` parameter. If the parameter appears in your backup copy of the `nbe.toml` file, copy and paste the parameter definition on a blank line before the `[dongle.bluegiga]` section of the current `nbe.toml` file.

19. Start the **Nymi Bluetooth Endpoint** service.

7.1.2 Update the Decentralized NBA

Perform the following steps to update the NBA with the Installation Wizard.

Prerequisite: Uninstall the previous version of Nymi Runtime.

1. Download the NBA package.

2. Double-click the `Nymi-Band-App-installer-v_version.exe` file.

3. On the **User Account Control** window, click **Yes**.

4. On the **Prerequisites** window, click **Next**.

5. On the **Welcome** page, click **Install**.

6. 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.

7. On the **Welcome to the Nymi Runtime Setup Wizard** page, click **Next**.

8. On the **Nymi Runtime Setup** window, click **Next**.

9. On the **Service Account** window, perform one of the following actions:
 - Accept the default service account NTAuthority, click **Next**.
 - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **Next**.

Note: The service account must have permission to run as a service.

10. On the **(Optional) Nymi Infrastructure Service Account**, click **Next**.
11. On the **Ready to install** page, click **Install**.
12. Click **Finish**.
13. On the **Installation Completed Successfully** page, click **Close**.
14. On the **Welcome to Nymi Band Application Setup Wizard** window, click **Next**.
15. On the **Select Installation Folder** window, click **Next** to accept the default installation location.
16. In the **Ready to Install** window, click **Install**.
17. On the **Completing the Nymi Band Application Setup Wizard** window, click **Finish**.

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

7.2 Update the Centralized Nymi Agent and Clients

To update the Centralized Nymi Agent server and the clients that rely on a centralized Nymi Agent, you must remove the Nymi Runtime software, and then install the new version of the Nymi Runtime software with the appropriate Nymi Runtime components.

7.2.1 Update the Centralized Nymi Agent

Update the Centralized Nymi Agent with the installation wizard. Refer to [Install the Nymi Agent on the Centralized Server](#) for the procedure.

7.2.2 Configuring Nymi Agent

Perform the following actions on the centralized Nymi Agent server to take advantage of improvements that support secure communications between the centralized Nymi Agent and other Nymi components.

1. Change to the `C:\Nymi\NymiAgent` directory.
2. For updates from Connected Worker Platform (CWP) versions prior to CWP 1.16.0, edit the `C:\Nymi\NymiAgent\nymi_agent.toml` file, after the parameter `directory_service_id` parameter, add the following line:

```
credentials_location = "certs/"
```

The `credentials_location` parameter enables the use of the Nymi Infrastructure Service Account to complete authentication tasks with underlying functionality that improves the performance of Nymi Band taps in web-based NEAs and with BLE Taps.

3. To use secure websocket communications between the centralized Nymi Agent and Nymi Bluetooth Endpoint and centralized Nymi Agent with NEAs, edit the `C:\Nymi\NymiAgent\nymi_agent_default.toml` file and copy the new content in the `[agent]` section.

The new content starts with the following line:

```
# Getting wss connection in agent can be done by enabling  
below flags
```

and ends with the following line:

```
#keyfile = "/path/to/keyfile.pem"
```

Note: Refer to the section *Certificates for Secure Websocket Connections* for more information about the TLS requirements.

4. Paste the new content into the `C:\Nymi\NymiAgent\nymi_agent.toml` file, in the `[agent]` section.
5. Edit the values for the new parameters.

The following table provides information about each new parameter.

Parameter and Default Values	Section Name	Description
<code>protocol = "wss"</code>	[agent]	To enable the standard Nymi Agent to use secure websocket communications, uncomment <code>protocol</code> and change the value to <code>wss</code> . Requires configuration of the <code>cacertfile</code> , <code>certfile</code> , and <code>keyfile</code> parameters in the [agent] section.
<code>port = 9120</code>	[agent]	Defines an alternate server port on which Nymi Agent communicates with the Nymi Bluetooth Endpoint and NEAs. The default port number is 9120. Nymi recommends that you use the default port number.
<code>cacertfile = "certs/LocalLabRootCA3.pem"</code>	[agent]	Uncomment and specify the path to the PEM-formatted CA certificate bundle. The CA certificate bundle must start from the root CA and end in the subordinate CA issuing the server certificate. Requires configuration of <code>protocol = "wss"</code> , <code>certfile</code> , and <code>keyfile</code> parameters in the [agent] section.
<code>certfile = "certs/tw-srv1.tw-lab.local-cert.pem"</code>	[agent]	Uncomment and specify the path to the TLS certificate file containing the Nymi Agent server certificate in PEM format. Requires configuration of <code>protocol = "wss"</code> , <code>cacertfile</code> , and <code>keyfile</code> parameters in the [agent] section.
<code>keyfile = "certs/tw-srv1.tw-lab.local-key.pem"</code>	[agent]	Uncomment and specify the path to the TLS certificate private key file, unencrypted and PEM formatted. Requires configuration of <code>protocol = "wss"</code> , <code>cacertfile</code> , and <code>certfile</code> parameters in the [agent] section.

6. Save the file.

7. Restart the **Nymi Agent** service.

Ensure that you edit the `nbe.toml` file on each user terminal and change the protocol that is used to connect to the Nymi Agent from `ws` to `wss`. For example, `agent_url = "wss://tw-srv2.tw-lab.local:9120/socket/websocket"`

7.2.3 Update Clients that Connect to a Centralized Nymi Agent

Update the Nymi Bluetooth Endpoint component of the Nymi Runtime on each client that connects to a centralized Nymi Agent.

7.2.3.1 (Windows Only) Update the Nymi Bluetooth Endpoint

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.

Prerequisite: Uninstall the previous version of Nymi Runtime.

1. Log in to the terminal with an account that has administrator privileges.
2. Extract the Nymi SDK distribution package.
3. From the `..\nysi-sdk\windows\setup` folder, right-click the `Nymi Runtime Installer version.exe` file, and select **Run as administrator**.
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**, and then click **Next**.
9. Observe that **Nymi Agent** is not available, and then click **Next**.

10. On the **Service Account** window, perform one of the following actions:
 - Accept the default service account NTAuthority, click **Next**.
 - For non-English Windows Operating Systems and for Nymi WebAPI configurations where you install the centralized Nymi Agent on the NES server, choose the LocalSystem account from the drop list, and then click **Next**.
11. On the **Ready to install** page, click **Install**.
12. Click **Finish**.
13. On the **Installation Completed Successfully** page, click **Close**.
14. Stop the **Nymi Bluetooth Endpoint** service.
15. Edit the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file. Compare and modify the following parameter values as required, with the value that appears in your backed up `nbe.toml` file:
 - a. `agent_url` parameter.
 - b. RSSI parameters.
 - c. `endpoint_id` parameter.
16. Start the **Nymi Bluetooth Endpoint** service.

Confirm that the status of the Nymi Bluetooth Endpoint service is running.

7.2.3.2 (HP Thin Pro) Update the Nymi Bluetooth Endpoint

The following instructions describe how to update Nymi Bluetooth Endpoint manually. Perform the following steps on the HP Thin Pro client.

1. Backup the `/usr/bin/nbe.toml` file.
2. Obtain the installation file `nbed-cron_x.y.z_amd64.deb` from Nymi.
3. Switch your user mode to **Administrator** from the system menu, or log in by entering 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.

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

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

5. In **X Terminal** change the directory to the file location of `nbed-cron_x.y.z_amd64.deb` and install the extracted file.

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

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

6. Edit the `/usr/bin/nbe.toml` file, and then perform the following actions:

- a. `agent_url` parameter.
 - b. RSSI parameters. Entries that appear in a CWP 1.19.2 and earlier TOML file apply to the Bluegiga Bluetooth Adapter; therefore, update the values that appear in the `[dongle.bluegiga]` section.
 - c. `endpoint_id` parameter. If the parameter appears in your backup copy of the `nbe.toml` file, copy and paste the parameter definition on a blank line before the `[dongle.bluegiga]` section of the current `nbe.toml` file.

7. Reboot the client.

7.2.3.3 (IGEL) Update the Nymi Bluetooth Endpoint

Update the Nymi packages in the Universal Management Suite (UMS), and then Nymi Bluetooth Endpoint software on the IGEL clients.

Perform the following steps to update the Nymi software on an IGEL user terminal. The procedure requires you to reboot the client.

1. Perform the following steps to take the partition offline.
 - a. From the UMS console, in the **Profiles** section, right-click the profile that contains the Nymi custom partition, and then select **Edit Configuration**.
 - b. Navigate to **System > Firmware Customization > Custom Partition > Partition**.
 - c. Clear the **Enable Partition** option.
 - d. Click **Apply and send to device**.
 - e. On the **Update time** dialog box, select **Now**, and then click **Ok**.
2. Click **Save**.
3. From the left navigation pane in the UMS console, right-click the device that contains the profile for the Nymi custom partition, and then select **Reboot**.
4. Perform the following steps after the device reboot completes to confirm that the custom partition does not appear:
 - a. In the left navigation pane of the UMS Console, right-click on the device, and then select **Shadow**.
 - b. When prompted, type the login credentials.
 - c. On the Desktop, open a terminal window.
 - d. Type the following command to change to the root directory: `cd /`.
 - e. Type `ls -l` and confirm that the `/custom` partition does not appear in the output.

Note: If the partition appears, repeat the steps to disable the partition on all devices that contain the Nymi custom partition.
5. In the left navigation pane of the UMS Console, in the **Files** section, right-click `nyimi.inf`, and then select **Delete**.

6. In the left navigation pane of the UMS Console, in the **Files** section, right-click `nyimi.tar.bz2`, and then select **Delete**.
7. In the left navigation pane of the UMS Console, right-click **Files**, and then select **New File**. Navigate to the folder that contains the new `nyimi.inf`, and then select the file.
8. In the left navigation pane of the UMS Console, right-click **Files**, and then select **New File**. Navigate to the folder that contains the new `nyimi.tar.bz2`, and then select the file.
9. From the left navigation pane in the UMS console, right-click the device that contains the profile for the Nymi custom partition, and then select **Reboot**.
10. From the UMS console, in the **Profiles** section, right-click the profile that contains the Nymi custom partition, and then select **Edit Configuration**.
11. Navigate to **System > Firmware Customization > Custom Partition > Partition**.
12. Select the **Enable Partition** option.
13. Click **Apply and send to device**.
14. On the **Update time** dialog box, select **Now**, and then click **Ok**.
15. From the left navigation pane in the UMS console, right-click the device that contains the profile for the Nymi custom partition, and then select **Reboot**.

7.3 Update Clients with a Decentralized Nymi Agent

Update the Nymi Runtime software on Windows user terminals that use the Nymi Band to perform authentication tasks.

Refer to [Install Nymi Runtime](#) for the installation procedure. For an update, uninstall the previous version of Nymi Runtime first.

7.4 Update Nymi Lock Control

Refer to [Install Nymi Lock Control](#) for the installation procedure.

7.5 Change the CWP Communication Protocol

Starting with CWP 1.15, the Nymi solution supports a new, high performance protocol over Bluetooth between the Nymi Runtime and Nymi Bands.

After you update all CWP components, including Nymi Band firmware on all Nymi Bands to CWP 1.15.x and later, perform the following steps on all Windows user terminals where users access Nymi-enabled Applications to disable the legacy protocol. The enrollment terminal only requires the environment variable if users access NEAs on the enrollment terminal.

Note: After you set this environment variable, user terminals cannot communicate with Nymi Bands that use pre-CWP 1.15.x firmware.

1. In the Windows search field, type `env`, and then from the pop-up menu, select **Edit the System Environment Variables**.
2. Click **Environment Variables**.
3. In the **System Variables** section, click **New**, and then perform the following actions:
 - a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`.
 - b. In the **Variable Value** field, type `0`.
 - c. Click **OK**.

8 Reference

8.1 Environment Summary

Throughout the deployment process, you will perform configuration tasks that you will be required to remember later on. Use the following table to keep track of values for variables that you define when you deploy the CWP solution.

Component	Variable Name	When Used	Value
Nymi Enterprise Server (NES) FQDN		NES deployment	
NES URL	NES_URL	Connect to the NES Administrator Console	
NES Communication port number (LDAP/LDAPS)	CORP_LDAP_PORT	CWP Backend deployment (cca script)	
NES Administrators group name and user accounts		NES deployment	
NES Administrator accounts		Access to NES Administrator Console	
Nymi Infrastructure Service Account		Nymi Agent communications with NES and NES communications with the SQL server.	

8.2 FQDN Summary

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

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

8.3 Certificate Expiration

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

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

8.4 Silent Installations

This section describes how to perform silent installations of CWP components. Silent installations are useful when you want to install software remotely by using a software distribution application.

8.4.1 Installing the Nymi Runtime Silently

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

1. Log in to the network terminal with an account that has administrator privileges.
2. Download and extract the Nymi SDK package.
3. Launch the command prompt as administrator.
4. Change to the `..\nymi-sdk\windows\runtime` folder, and then type one of the following commands:

- `"Nymi Runtime Installer version.exe" /exenoui /q /log NymiRuntimeIn`

- For installations on non-English operating systems:

- `"Nymi Runtime Installer version.exe" ServiceAccount="LocalSystem" /`

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

Note: Ensure that you enclose the filename 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 and `NymiRuntimeInstallation.log` file contains information about the installation.

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.

Confirm that the Nymi Agent and Nymi Bluetooth Endpoint services are running.

8.4.2 Installing the Nymi Bluetooth Endpoint Silently

1. Run a Command Prompt as administrator.
2. You can install the Nymi Bluetooth Endpoint silently by typing one of the following commands:

- `"Nymi Runtime Installer version.exe" /exenoui InstallAgent=0 /q /lc`

- For installations on non-English operating systems:

- `"Nymi Runtime Installer version.exe" ServiceAccount="LocalSystem" /`

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

Note: Ensure that you enclose the filename 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 and `NymiRuntimeInstallation.log` file contains information about the installation.

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.

Confirm that the status of the Nymi Bluetooth Endpoint service is running.

8.4.3 Performing a Silent Nymi Agent Installation or Update

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

1. You can install the Nymi Agent silently by typing one of the following commands:

- `"Nymi Runtime Installer version.exe" /exenoui InstallEndpoint=0 /q`

- For installations on non-English operating systems:

- `"Nymi Runtime Installer version.exe" ServiceAccount="LocalSystem" /`

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

Note: Ensure that you enclose the filename 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 and `NymiRuntimeInstallation.log` file contains information about the installation.

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.

2. Perform the following steps to ensure that the Nymi Agent uses the Nymi Infrastructure Service Account to communicate with Nymi Enterprise Server (NES).

a. Create a text file named `creds.txt` that contains two lines:

- Username of the Nymi Infrastructure Service Account
- Password of the Nymi Infrastructure Service Account

b. Open a Command prompt with the **Run as Administrator** option.

- c. From the command prompt, change to the `C:\Nymi\NymiAgent\Tools` directory, and type the following command:

```
cryptoutil.exe encrypt-service-account -i C:\Nymi\NymiAgent\creds.t
```

The Cryptoutil tool creates the following files in the `C:\Nymi\NymiAgent\certs` folder:

- `credentials` — contains the encrypted credentials for the Nymi Infrastructure Service Account
- Private key
- Public key

- d. Permanently delete the `C:\Nymi\NymiAgent\creds.txt` file.

8.4.4 Installing the Nymi Band Application Silently

Perform the following steps to install or update the NBA silently, for example, when you want to install the software remotely by using a software distribution application.

Prerequisite: Before you install the NBA, install the Nymi Runtime.

1. Save the NBA package, provided to you by your Nymi field representative.
2. Launch the command prompt as administrator.
3. From the folder that contains the NBA, 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 NBA and Nymi Runtime applications appear in the **Program and Features** applet.

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

8.4.5 Installing or Updating Nymi Lock Control Silently

Perform the following steps to install or update Nymi Lock Control silently, for example, when you want to install the software remotely by using a software distribution application.

1. Create a backup copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file.
2. Save the Nymi Lock Control package, provided to you by your Nymi field representative.
3. Launch the command prompt as administrator.
4. From the folder that contains the Nymi Lock Control, type `NymiLockControl-installer-vversion.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 Lock Control application 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.

5. Stop the **Nymi Bluetooth Endpoint** service.
6. Edit the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file. Compare and modify the following parameter values as required, with the value that appears in your backed up `nbe.toml` file:
 - a. `agent_url` parameter.
 - b. RSSI parameters. Entries that appear in a CWP 1.19.2 and earlier TOML file apply to the Bluegiga Bluetooth Adapter; therefore, update the values that appear in the `[dongle.bluegiga]` section.
 - c. `endpoint_id` parameter. If the parameter appears in your backup copy of the `nbe.toml` file, copy and paste the parameter definition on a blank line before the `[dongle.bluegiga]` section of the current `nbe.toml` file.

7. Start the **Nymi Bluetooth Endpoint** service.

8. Log out and log back into the user terminal.

Copyright ©2026 Nymi Inc. All rights reserved.

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