Deployment Guide—Windows and Linux

Nymi Connected Worker Platform 1.21.0

v2.2

2026-10-20

Contents

1 Preface 6
1.1 Purpose 6
1.2 Audience 6
1.3 Revision history 6
1.4 Related documentation 8
1.5 How to get product help 10
1.6 How to provide documentation feedback 10
2 Deployment Overview 11
2.1 Components in a Decentralized Nymi Agent Configuration 11
2.2 Components in a Centralized Nymi Agent Configuration 15
2.3 Deployment of the Nymi WebAPI 17
2.4 Nymi WebAPI Configuration Requirements 18
3 Prepare for Connected Worker Platform Deployment 19
3.1 Hardware and Software Requirements 19
3.1.1 NES Requirements 19
3.1.2 Time Synchronization Requirements 20
3.1.3 User Terminal Requirements 20
3.1.4 Nymi WebAPI Interface Requirements 23
3.2 Networking Requirements 23
3.2.1 (Non-HA Deployments only) Domain Name Service Requirements 24
3.2.2 (HA Deployments only) Domain Name Service Requirements 24
3.2.3 (HA Deployments only) Load Balancer Requirements 25
3.2.4 Firewall Port Requirements 26
3.2.5 RDP/Citrix Client Considerations 27
3.3 Certificate Requirements 28
3.3.1 TLS Certificates 28
3.3.2 Nymi-specific Certificates 30
3.3.3 Using TLS Certificates Issued by Untrusted Certificate Authorities 31
3.4 Component Authentication Modes 31
3.5 Active Directory Requirements 32
3.5.1 Requirements for the Installer Account 32

3.5.2 Domain and Trust Requirements 32
3.5.3 Creating the Active Directory Group for NES Administrator 33
3.5.4 (Optional) Creating an Organizational Unit for User Terminals. 34
3.5.5 Creating the Nymi Infrastructure Service Account 34
3.5.6 Setting Service Principal Names 36
3.6 Database Requirements 38
3.6.1 Supported SQL Versions 38
3.6.2 Creating the NES database 39
3.6.3 Configuring SQL Database for Remote Access 40
3.7 CWP Package Requirements 44
3.7.1 Obtaining the NES Software Package 44
4 Deploy Nymi Enterprise Server 45
4.1 Install and Configure IIS 45
4.1.1 Installing IIS and ASP.NET 45
4.1.2 Importing the TLS server certificate 48
4.1.3 Adding HTTPS site bindings 55
4.1.4 Creating an Application Pool for Authentication Service 58
4.1.5 Verifying the Authentication Configuration 62
4.1.6 Securing IIS 63
4.1.7 Enabling Directory Browsing IIS 66
4.1.8 (HA Deployments Only) Generating Machine Keys 67
4.2 Importing a Fullchain Certificate 69
4.2.1 Importing Certificates 70
4.2.2 Moving the L2 certificate 73
4.3 Installing NES 75
4.3.1 Installing the NES Services Suite using the wizard 75
4.3.2 Configuring NES Services Manually 79
4.3.3 Saving the NES Configuration 100
4.3.4 (HA Deployments) Configuring Additional NES Servers from a Configuration File 102
4.4 Configuring IIS to Prevent NES Offloading 106
4.5 Validating the NES Deployment 112
4.5.1 Access the NES Administrator Console 112
4.6 Configuring NES to support Nymi Lock Control 115
4.7 Hardening the NES Keystore 117
4.7.1 (Optional)Encrypting usernames in the NES Database 128

5 Set Up a Centralized Nymi Agent 132
5.1 Importing the Root CA certificate 132
5.2 Installing/Updating Centralized Nymi Agent 133
5.3 Configuring the Nymi Agent 137
6 Install and Configure Endpoints 145
6.1 Setting the Nymi Bluetooth Endpoint ID Format 146
6.2 Install and Configure Endpoints with a Decentralized Nymi Agent 147
6.2.1 Bluetooth Adapter 147
6.2.2 Set Up a Decentralized Enrollment Terminal 148
6.2.3 Set Up Windows User Terminals for Authentication Tasks 154
6.2.4 Set Up Windows User Terminals for Lock and Unlock 159
6.3 Install and Configure Endpoints with a Centralized Nymi Agent 173
6.3.1 Set Up the Enrollment Terminal 174
6.3.2 Set Up Thick Client User Terminals 188
6.3.3 Set Up User Terminals for Lock and Unlock 226
7 Updating Connected Worker Platform 248
7.1 Creating the Nymi Infrastructure Service Account 248
7.2 Updating NES 249
7.2.1 Defining the NES for Policy Management 253
7.3 Updating the Enrollment Terminal 254
7.3.1 Updating the Centralized Nymi Band Application 254
7.3.2 Updating the Decentralized Nymi Band Application 257
7.4 Updating the Centralized Nymi Agent and the Clients 259
7.4.1 Update Centralized Nymi Agent 259
7.4.2 Update Clients that Connect to a Centralized Nymi Agent 267
7.5 Updating Clients that Connect to A Decentralized Nymi Agent 282
7.5.1 Updating the Nymi Runtime 282
7.5.2 Updating Nymi Lock Control 285
7.6 Updating the Nymi Band Firmware 287
7.6.1 Updating the Firmware on Multiple Nymi Bands 288
7.6.2 Updating the Firmware on a Nymi Band 291
7.6.3 Firmware updater log files 293
7.7 Changing the Connected Worker Platform Communication Protocol 294
8 Appendix—Recording the CWP Variables 296
9 Appendix—Recording the CWP Component FQDNs 297
10 Appendix—TLS Certificates Expiration Dates 298

11 Appendix—Silent Installations 299
11.1 Installing Nymi Bluetooth Endpoint Silently 299
11.2 Installing the Nymi Runtime Silently 300
11.3 Installing or Updating Nymi Lock Control Silently 301
11.4 Installing the Nymi Band Application Silently 302
11.5 Performing a Silent Nymi Agent Installation or Update 303

1 Preface

Nymi provides the Connected Worker Platform(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 Nymi SDK, Nymi Runtime, Nymi Enterprise Server, 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

The following table outlines the revision history for this document.

Revision history

1.0	**Date:** November 28, 2025 **Revision history** New section Configuring JWT Secret Key to include NES installation and update steps that required for Nymi Connect for Android deployments in an NES HA configuration.
2.0	**Date:** January 05, 2026 **Revision history** Second release of this document. Updates include new content for the CWP 1.20.1 release: • Revision of the NES installation and update instructions to introduce new key management section in NES configuration. • Addition of content about how deploy a highly available NES.
2.1	**Date:** 2026-06-23 **Revision history** Updates for the Connected Worker Platform 1.21.0 release: • Added support for the BleuIO Bluetooth Adapter. • Added BleuIO RSSI default values and the `[dongle.nymi]` configuration section.
2.2	**Date:** 2026-10-20 **Revision history** Added the Component Authentication Modes section (AD Mode and CWP Mode) for NCW 1.3.0 CWP Mode support.

1.4 Related documentation

Nymi Connected Worker Platform—Overview Guide

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

Nymi Connected Worker Platform—Administration Guide

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

Nymi Connect for Windows Installation and Configuration Guide

This guides contains information about how to install, configure and use the Nymi Connect application on Windows.

Nymi Connect for Android Installation and Configuration Guide

This guides 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(NAPI).

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

The Nymi with Evidian Solution—Deployment Guide provides information about how to deploy the Nymi with Evidian solution components.

Nymi Connected Worker Platform—Troubleshooting Guide

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

Nymi Connected Worker Platform with Evidian Troubleshooting Guide

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

Nymi Connected Worker Platform—FIDO2 Deployment Guide

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

Connected Worker Platform with POMSnet Installation and Configuration Guide

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

Nymi Band Regulatory Guide

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

Third-party Licenses

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

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@nymi.com

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@nymi.com

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.

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

Note: You can deploy a configuration that uses a mixture of user terminals with centralized or decentralized Nymi Agent but for simplicity Nymi recommends that 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.

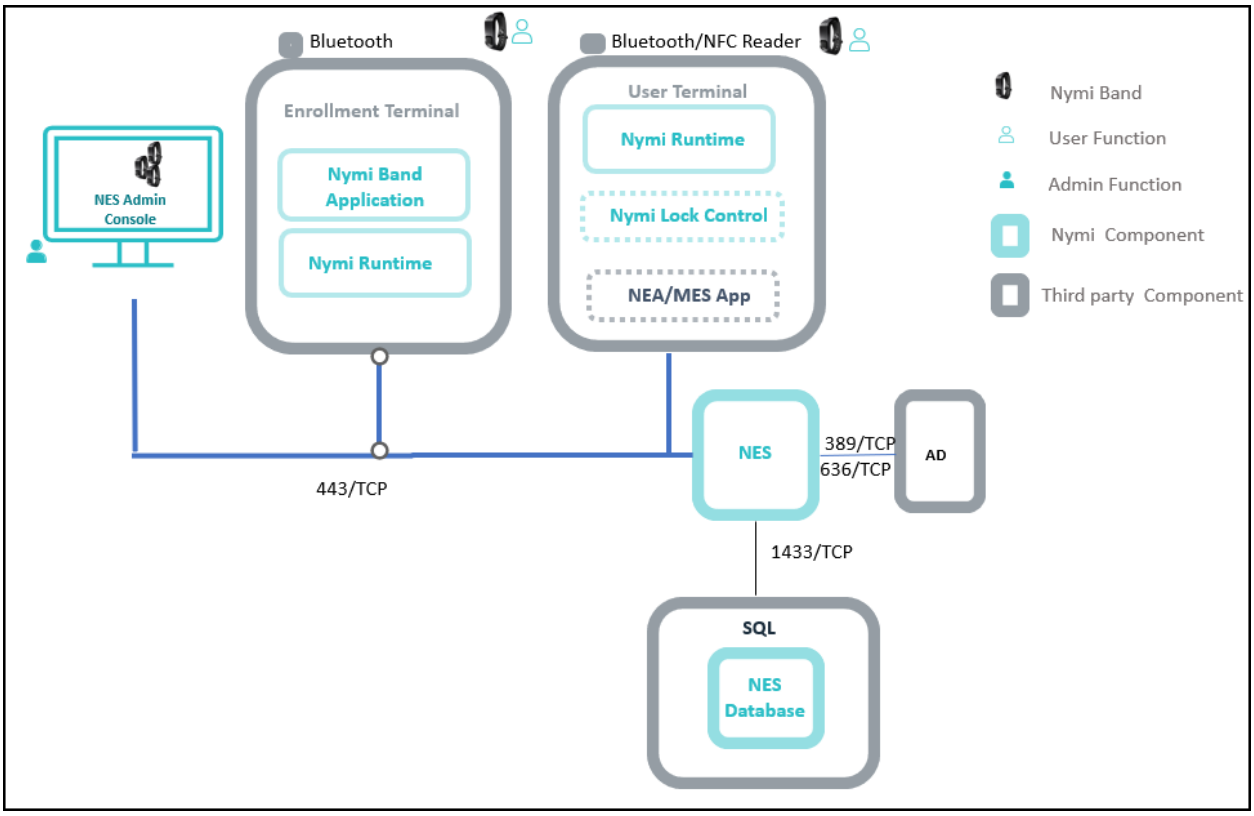


Figure 1. Connected Worker Platform components and connection ports

The Connected Worker Platform consists of the following components.

Connected Worker Platform Components

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 Nymi Band Application Terminal, which you use to enroll a new user and link them to their Nymi Band. The Nymi Band Application requires the Nymi Runtime application, which the Nymi Band Application automatically installs. The Nymi Band Application communicates with the Nymi Band through the Nymi-supplied Bluetooth adapter, which you plug into a USB port on the enrollment terminal.

Nymi Runtime	A Windows application that you install on the enrollment terminal and user terminals. Nymi Runtime includes the Nymi Agent and Nymi Bluetooth Endpoint components.Nymi Runtime supports communication between NES, the Nymi Band, NEAs, the Nymi Band Application and Nymi Lock Control. Nymi Runtime supports communication between NES, the Nymi Band and Rockwell Pharmasuite. Nymi Runtime supports communication between NES, the Nymi Band and eInfotree Excel Module.
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	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	Developers can create corporate applications that integrate with Connected Worker Platform by using the Nymi API. These applications are called Nymi-Enabled Applications (NEAs) and include Manufacturing Execution Systems (MES), Single Sign-On (SSO), and Human Machine Interface (HMI) applications. An NEA requires the Nymi Runtime software. An NEA
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: • Enrollment Service (ES)—Authenticates, validates, and authorizes certificate requests from requesters, such as the Nymi Band Application and NEAs. • Directory and Policy Services (DPS)—Maintains the NES database, which contains a list of Active Directory (AD) users and the Nymi Bands that are associated with each user. Provides IIS web services, which allows the NES Administrator Console access to the NES database. • Authentication Service (AS)—Provides authentication and authorization support for domain users and computers. AS uses adapters to interface with external directory and database systems, such as an AD adapter to interface with Active Directory.
SQL Server	Database server that contains tables that store information about the NES configuration and the Nymi Bands. Database server that contains tables that store information about the NES configuration and the Nymi Bands. The same SQL server can contain tables that store Evidian audit logs, which include information about when a user completes and authentication event in the Evidian SSO window by tapping their Nymi Band. 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. The same server or another server contains the eInfortree database.

Domain Controller (DC)	Windows server with Active Directory.

2.2 Components in a Centralized Nymi Agent Configuration

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

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

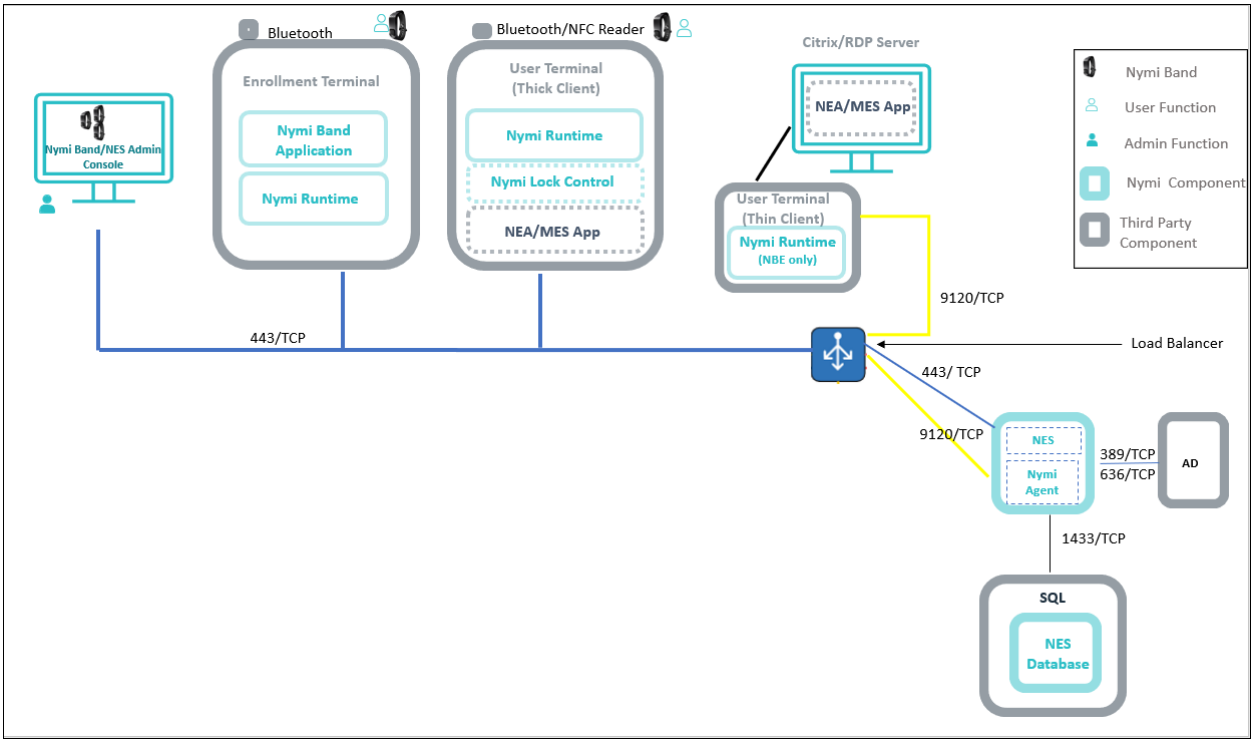


Figure 2. Connected Worker Platform components in a Citrix/RDP environment

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

> **Note:** While not displayed, it is assumed that NES, Nymi Agent, and the CWP Backend components are clustered.

Connected Worker Platform Components

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: • Access a remote session host and launch an NEA that is installed on a remote session host. • Use Nymi Lock Control to lock and unlock the desktop. When you install Nymi Runtime on the user terminal, only install the Nymi Bluetooth Endpoint component. The `nbe.toml` file defines the location of the centralized Nymi Agent. The Nymi Bluetooth Endpoint service communicates with the Nymi Agent service over websocket port 9120.
User Terminal (thin client)	An endpoint that users use to: • Access a remote session host and launch an NEA that is installed on a remote session host. • Use Nymi Lock Control to lock and unlock the remote or virtual desktop. When you install Nymi Runtime on the user terminal, only install the Nymi Bluetooth Endpoint component. The `nbe.toml` file defines the location of the centralized Nymi Agent. The Nymi Bluetooth Endpoint service communicates with the Nymi Agent service over websocket port 9120.
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 Nymi Connected Worker Platform—Deployment Guide.

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

For deployments in an RDP/Citrix environment or when the MES application (NEA) resides on a different host (such as a web or application server), theIP 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 mus preform 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 Connected Worker Platform 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 Nymi Enterprise Server (NES) hardware requirements differ based on the nature of user operations, load and other software that is deployed on the same server. The following section lists the recommendations for minimum hardware requirements.

- 1-5000 users:
    - 4 Core CPU
    - 8GB RAM
    - 20GB free disk space
- 5000-10000 users:
    - 4 Core CPU
    - 16GB RAM
    - 40GB free disk space

3.1.1.2 Software Requirements

NES has the following software requirements.

- Microsoft Windows Server 2016, 2019, or 2022

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

- Microsoft IIS
- Microsoft .NET Framework 4.8

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

3.1.2 Time Synchronization Requirements

Nymi Band enrollments require time synchronization between the Nymi Band Application Terminal and Nymi Enterprise Server(NES).

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

Enrollment	**Supported Operating System/Browser** • Windows 10, 64-bit, minimum build version 1607 • Windows 11, 64-bit > **Note:** Nymi recommends that you use 125% scaling and 1920 x 1080 screen resolution for the terminal hosting the Nymi Band Application **Hardware** • 4GB RAM • 5GB free disk space • 2 core CPU (recommended) • 1 USB 2.0 port • Nymi-supplied bluetooth adapter
Authentication tasks with a Nymi Band in a MES application(Nymi-Enabled Applications(NEAs) on Windows, HP ThinPro, and IGEL	**Supported Operating System/Browser** • 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 web browsers for web-based NEAs: • Firefox 70 and later • Chrome 78 and later • Internet Explorer 11 and later • Microsoft Edge 44.18362.387.0 **Hardware** • Nymi-supplied Bluetooth adapter • NFC reader (optional)

Locking and Unlocking the Desktop	**Supported Operating System/Browser** • 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 **Hardware** • 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 Nymi Band Application 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, navigate to **Start > Settings > Apps & features > Optional features**. Click **Add a feature**. From the list of available optional features, select **Media Feature Pack**.
- For Windows 10 versions that are earlier than 1909, download and install the media feature pack from Microsoft.
- For Windows 11, navigate to **Start > Settings > Apps > Optional features**. Next to **Add an optional feature**, select **View features**, and then form the list of optional features, select the Media Feature Pack.

3.1.3.3 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..

3.1.4 Nymi WebAPI Interface Requirements

Nymi provides an API interface that supports web-based Nymi-Enabled Applications called Nymi WebAPI.

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.

3.1.4.1 Configuring and deploying in a 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 Nymi WebAPI 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 NEA use the subscribe operation. See the Nymi SDK Developer Guide—Webapi(Windows) provides more information.
- Each component can co-locate with the 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 Nymi Band Application 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.

Table 1. FQDN Requirements

Component	FQDN Example
Nymi Enterprise Server (NES)	nes.cwp.company.com
Centralized Nymi Agent	nymiagent.cwp.company.com
Evidian EAM Controller	evidian.cwp.company.com
Centralized Nymi Agent with WebAPI enabled	nymiagentwebapi.cwp.company.com

3.2.2 (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 Nymi applications, such as the Nymi Band Application.

3.2.2.1 HA CWP Deployment

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 member 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 Appendix—Recording the CWP Component FQDNs.

Table 2. FQDN Requirements

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 WebAPI enabled) cluster member 0	nymiagentwebapi-0.cwp.company.com
Centralized Nymi Agent (with WebAPI enabled) cluster member 1	nymiagentwebapi-1.cwp.company.com
Centralized Nymi Agent (with WebAPI 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 balances 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 Nymi Enterprise Server(NES)
- 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:
    - Nymi Enterprise Server(NES)—Cluster members that are accessible on port 443.
    - Nymi Agent—Cluster members that are accessible on port 9120.
    - Nymi Agent (when WebAPI 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 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.

Table 3. Connection Port Requirements

Purpose	Protocol	Source	Virtual Server FQDN & Port	Destination and Port
SQL Access	MS SQL Proprietary	NES	n/a	SQL Server: 1433/ TCP
LDAP Access-Active Directory(AD)	LDAP/ LDAPS	NES	n/a	AD Server: 389/TCP (For LDAP configurations) 636/ TCP (For LDAPS configurations)
NES Communications	HTTPS	Machine that accesses NES Administrator Console All User Terminals (thick). RDP/ Citrix servers that run NEAs	nes.cwp. company.com: 443/TCP	NES: 443/TCP

Purpose	Protocol	Source	Virtual Server FQDN & Port	Destination and Port
		Centralized Nymi Agent		
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 Nymi-Enabled Applications(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
Supports centralized Nymi Agent (in Webapi mode) from Nymi Bluetooth Endpoints and web-based NEAs.	Websocket (WS) / Secure Websocket (WSS)	All User Terminals (thick)	nymiagentwebapi.cwp.company.com 80/TCP (WS protocol) 443/TCP (WSS protocol)	nymiagentwebapi-0.cwp.company.com nymiagentwebapi-1.cwp.company.com 80/TCP (WS protocol) 443/TCP (WSS protocol)

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 (ie 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.

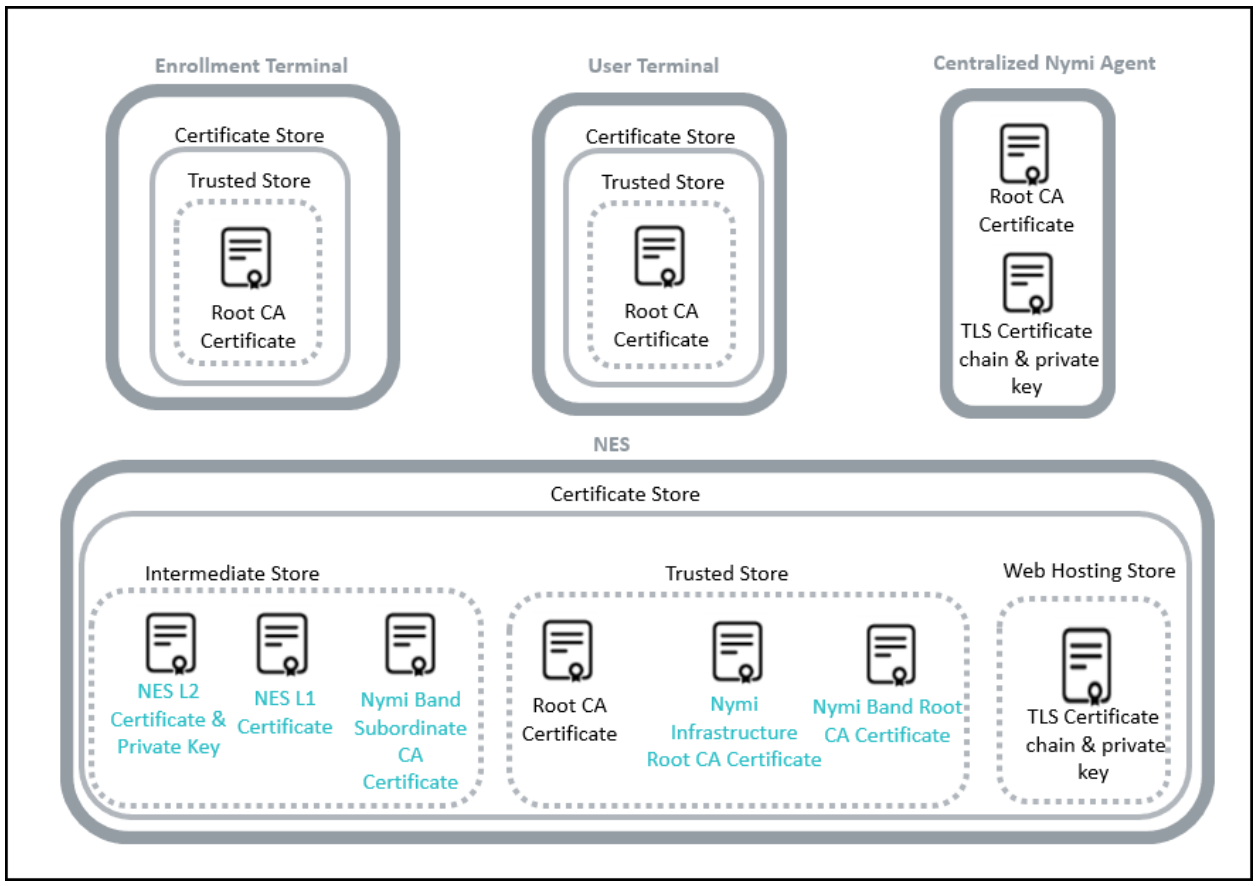


Figure 3. Certificates

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 certificate 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 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 web sockets for communications with native and web-based Nymi-Enabled Applications(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. See Microsoft documentation for information about installing Trust Root Certificates: https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate.html

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 instance and the public NES FQDN in the SAN field. If you use the same TLS certificate.

> **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 Solution Consultant. 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 Whitepaper.

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 Connected Worker Platform services. The methods that you use to import the untrusted root CA certificate into each component is described later in this guide.

3.4 Component Authentication Modes

Nymi components, like Nymi Connect, must authenticate to Nymi Enterprise Server (NES). The Connected Worker Platform (CWP) supports two component authentication modes:

- **AD Mode** — the component authenticates to NES using the Active Directory (AD) computer account of the machine on which it runs. This is the default mode and requires no per-device provisioning, but it requires that the machine is joined to the NES domain, or to a domain that has a trust relationship with it.
- **CWP Mode** — the component authenticates to NES using OAuth 2.0, which removes the dependency on Active Directory for component authentication. A component in CWP Mode is provisioned with a Client Registration Token (CRT) and does not need to be joined to an AD domain to authenticate to NES.

> **Note:** Active Directory is always used for user identity and authentication, regardless of the component authentication mode, so the Active Directory requirements in this chapter apply to every deployment. CWP Mode removes only the requirement to AD-join the machine for the component to authenticate to NES; a component may still require the machine to be AD-joined for other reasons, such as Nymi Lock Control, so check the requirements of each Nymi-Enabled Application.

A deployment can use both modes at the same time, and you can transition a device from AD Mode to CWP Mode. Nymi recommends CWP Mode for new deployments, because it removes the dependency on Active Directory for component authentication. CWP Mode requires CWP 1.20.1 or later.

For instructions on using CWP Mode:

- To create and manage the CRTs that CWP Mode uses, see Managing Client Registration Tokens in the Connected Worker Platform Administration Guide.
- To configure a Nymi Connect platform for CWP Mode and provision a device, see the Installation and Configuration Guide for that platform.

3.5 Active Directory Requirements

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

3.5.1 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 Nymi Enterprise Server(NES) software with one AD account and install the client software with a different account.

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

- Username less than 20 characters.
- Local administration privileges on the NES computer.
- Logon permissions to the SQL server and DB_OWNER rights to the NES 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 Nymi Band Application and Nymi Runtime software install the component software on the `C:` drive.

3.5.2 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

Nymi Enterprise Server (NES) server resides, within the same forests or different forests.

3.5.2.1 Domain Requirements

You require this information during the NES deployment process.

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

3.5.2.2 Trust Requirements

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

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

3.5.3 Creating the Active Directory Group for NES Administrator

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

About this task

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

Procedure

1. 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`.

    a. 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.

3.5.4 (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.

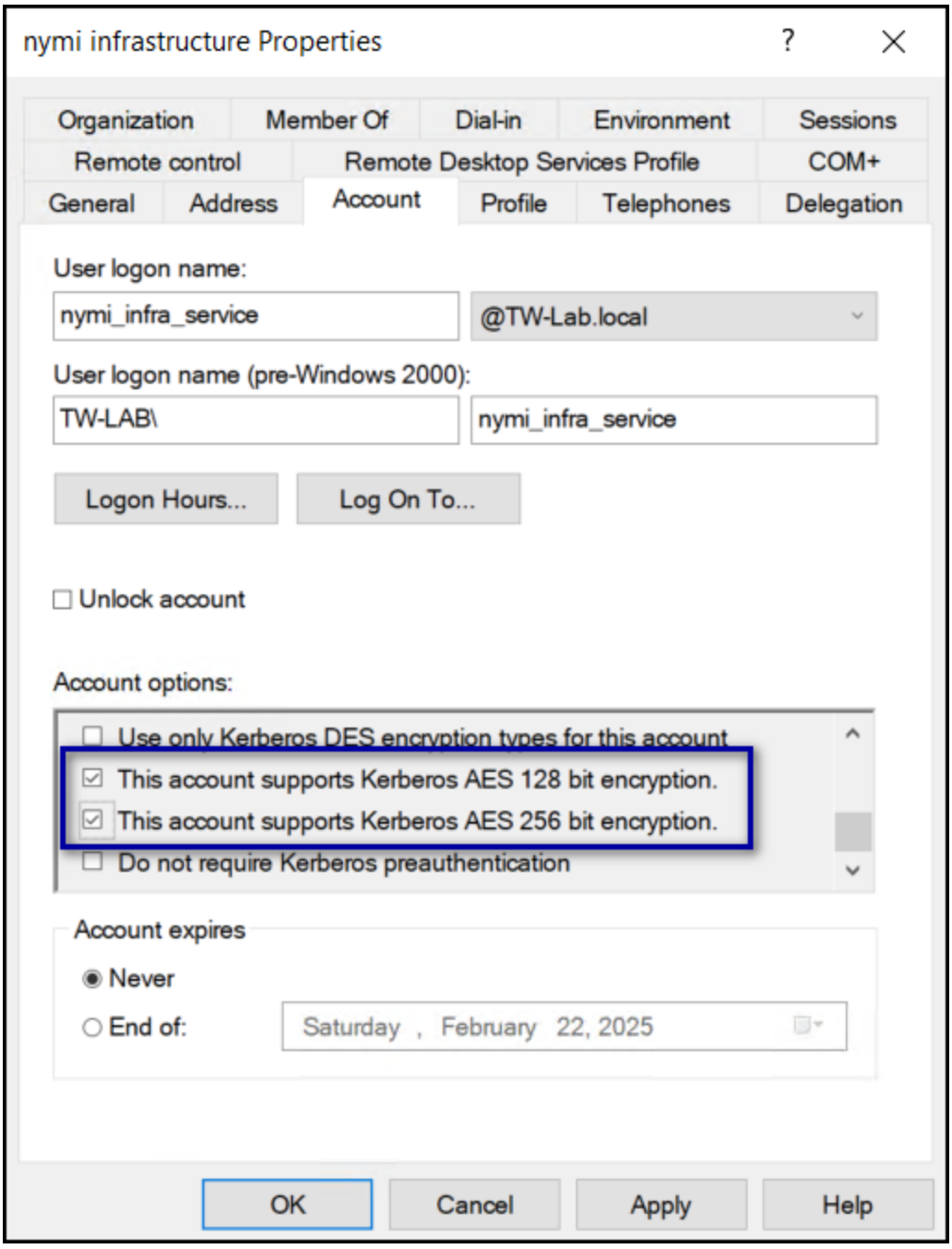
3.5.5 Creating the Nymi Infrastructure Service Account

Connected Worker Platform(CWP) 1.12.x and later uses a service account to support interprocess and to manage the Nymi Enterprise Server(NES) 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.



3.5.6 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, you must specify HTTP Service Principal Names (SPNs) in Active Directory.

About this task

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

Procedure

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

   ```
   setspn -T * -F -Q HTTP/nes_server1_fqdn

   setspn -T * -F -Q HTTP/nes_server2_fqdn

   setspn -T * -F -Q HTTP/nes_public_fqdn
   ```

   Output similar to the following appears when the HTTP SPN is set correctly for a NES 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:

   a. Open a command prompt as a Domain Administrator.

   b. Type the following command to set the SPN:

      ```
      setspn -S HTTP/nes_server_fdqn nymi_infrastructure_service_account
      ```

      Where:

      - `nes_server_fqdn` is the FQDN of the NES 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.

The example displays the command to set the HTTP SPN for a NES server with the FQDN `tw-srv2.tw-lab.local`, and the an application pool identity user account named `nymi_infra_service`

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

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

3.6 Database Requirements

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

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.

3.6.1 Supported SQL Versions

CWP solution supports the following Microsoft SQL versions:

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

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

3.6.2 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.

About this task

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

Procedure

1. Open **SQL Server Management Studio (SSMS)**, and then login to the SQL Server.
2. Right-click the SQL instance, and the select **Properties**.
3. In the **Object Explorer**, select **Security**.
4. Select **SQL Server and Windows Authentication Mode**, and then click **OK**.
5. In the **Object Explorer** right-click `Databases`, and the select `New Database`.
6. In the **New Database** window, perform the following actions:
    a. In the **Name** field, type nes.
    b. Click the elipses (...) beside **Owner**, and then in the **Enter the object names to select** field, type the name of the Nymi Infrastructure Service Account account.
    c. Click **Check names**.
    d. In the **Multiple Objects Found** field, select the service account name, and then click **OK**.
    e. On the **Select Database Owner** window, click **OK**.
    f. On the **New Database** window, click **OK**.

3.6.3 Configuring SQL Database for Remote Access

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

About this task

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

Procedure

1. In the left navigation pane, expand **SQL Server Network Configuration**, and then select the appropriate Protocols for the SQL Server option.
2. In the right pane, select TCP/IP, and then right-click and select **Enabled**.
3. Double-click **TCP/IP**.
4. In the **TCP/IP Properties** window, select the **IP addresses** tab.
5. Navigate to the **IPALL** section, and then for the **TCP port** value, type 1433.

   The following figure provides an example of the port setting.

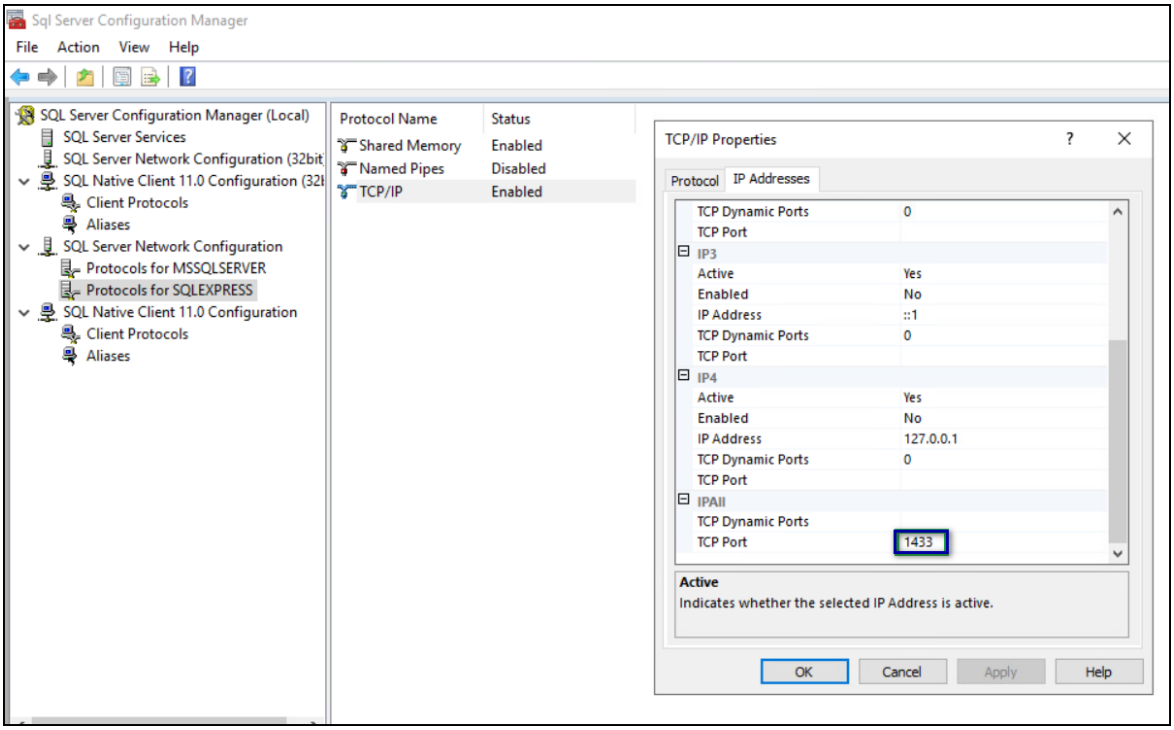


Figure 4. Configuring SQL Port

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

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

8. Restart SQL Server services.

9. For SQL Express only, perform the following steps in **SQL Configuration Manager**.

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

    b. Right-click **SQL Server Browser**, and then select **Properties**, as shown in the following figure

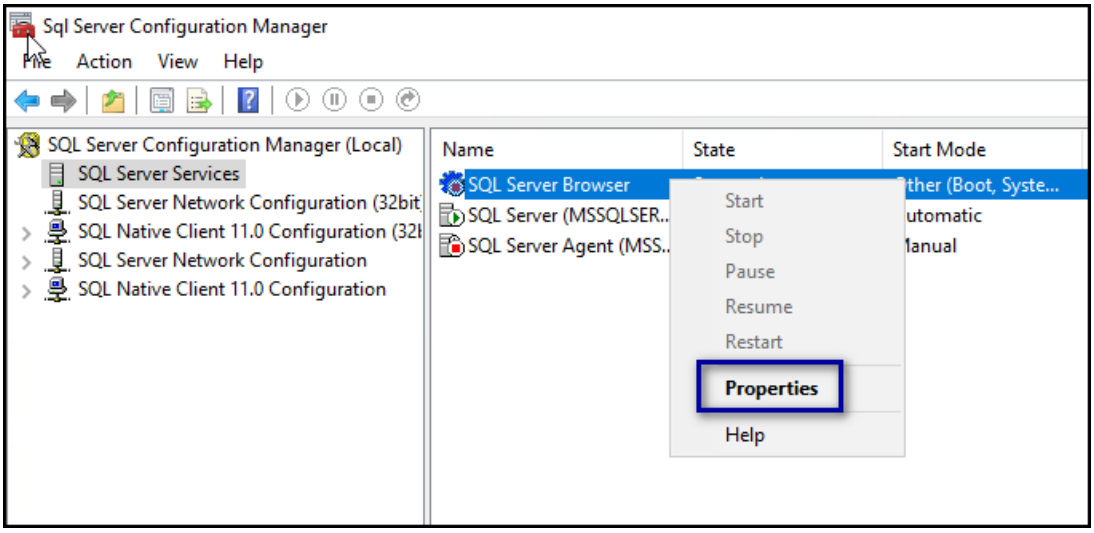


Figure 5. SQL Browser Properties option

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

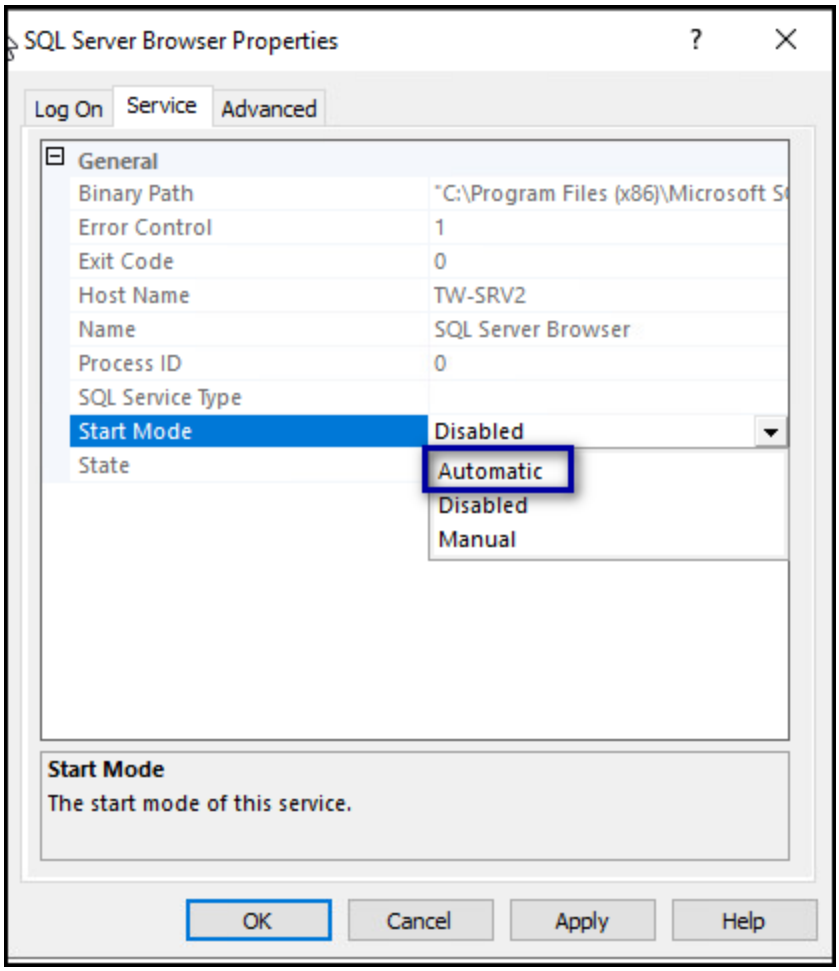


Figure 6. Start Mode

d. Right-click **SQL Server Browser** and select **Start**.

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

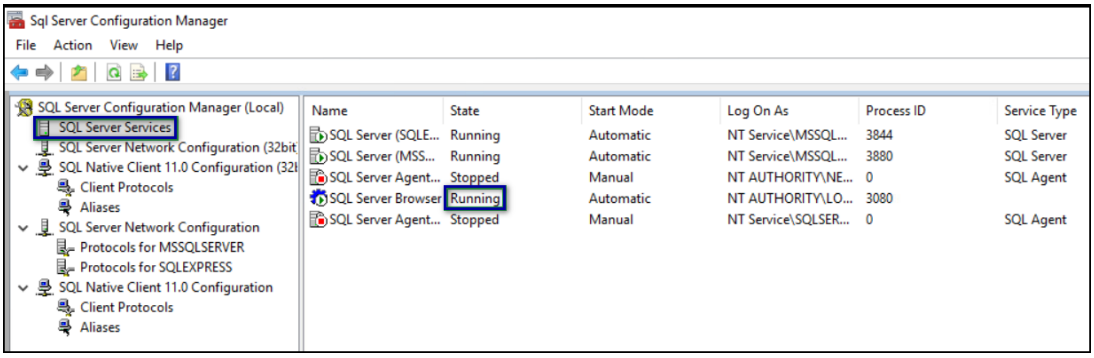


Figure 7. SQL Server Browser service

3.7 CWP Package Requirements

3.7.1 Obtaining the NES Software Package

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

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

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

4 Deploy Nymi Enterprise Server

The following sections provide information about how to deploy Nymi Enterprise Server (NES).

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.

Procedure

1. Open the **Server Manager** application, and then click **Add roles and features**.
2. On the **Before You Begin** page, click **Next**, as shown in the following figure.
3. On the **Select installation type** page, leave the default value **Role-based or feature-based installation**, and then click **Next**.
4. On the **Select destination server** page, leave the default selection **Select a server from the server pool**, select the host in the **Server Pool** list box, and then click **Next**.
5. On the **Select server roles** page, click **Web Server (IIS)**.

   The **Add features that are required for Web Server (IIS)** dialog box appears and provides a summary of tools that are required to install IIS.

6. On the **Add features that are required for Web Server (IIS)** dialog box, click **Add Features**.
7. On the **Select server roles** page, click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Web Server Role (IIS)** page, click **Next**.
10. On the **Select role services** page, expand **Application Development**, and then perform the following actions:
    a. Select **Application Initialization**.
    b. Select the latest available version of ASP.NET 4.x.

    > **Note:** NES supports ASP.NET 4.4 and later.

    c. On the **Add features that are required for ASP.NET** dialog box, click **Add Features**, as shown in the following figure, and then click **Next**.

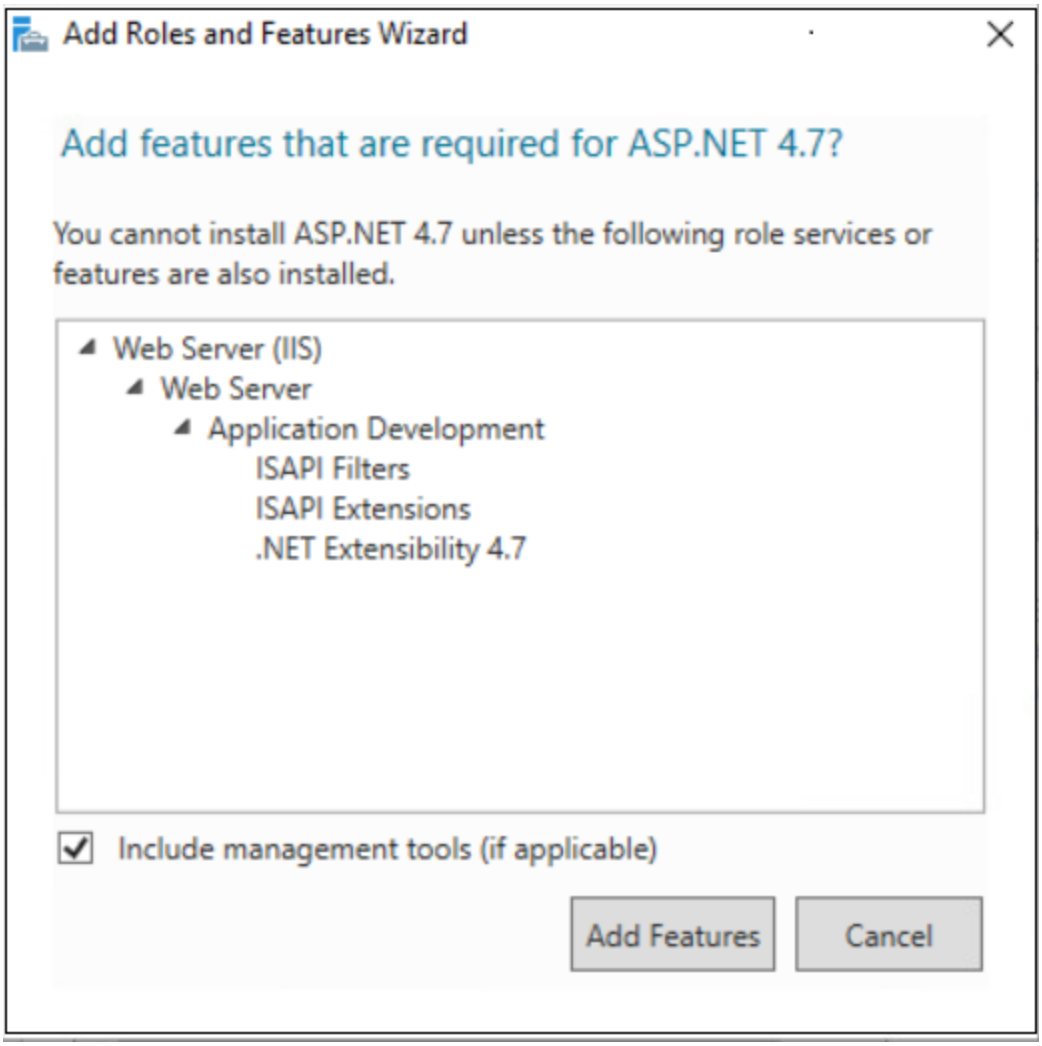


Figure 8. Add features that are required for ASP.NET

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

   The following figure shows the **Select server roles** page.

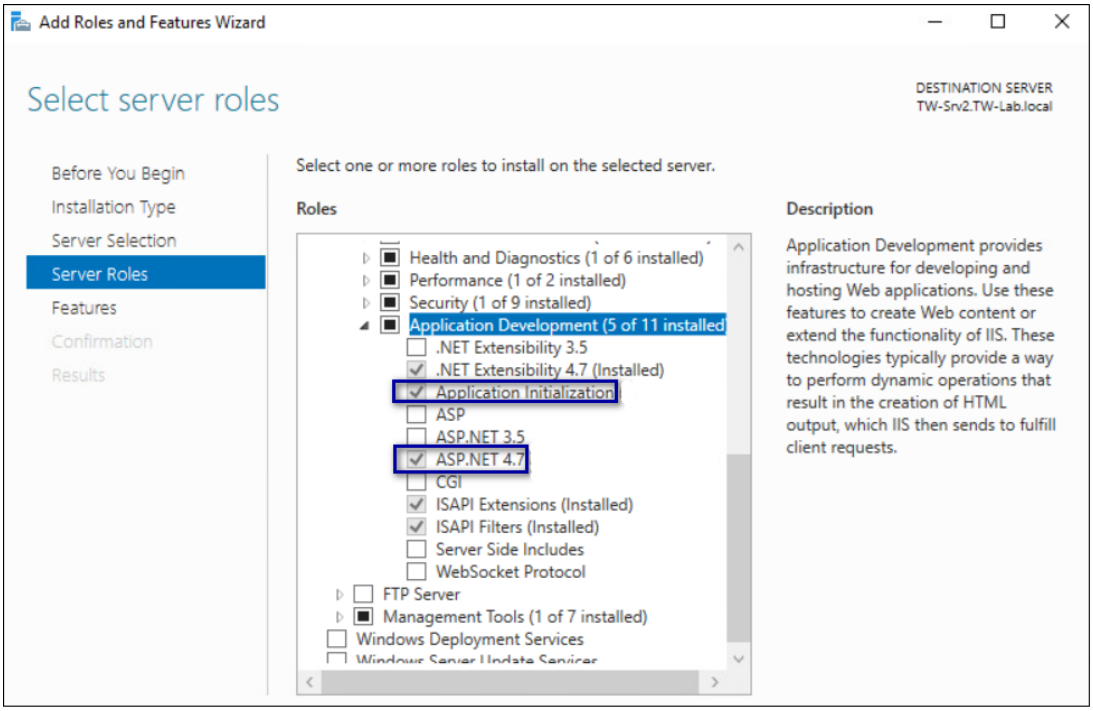


Figure 9. Select server roles page

11. On the **Select Features** page, click **Next**.
12. On the **Confirm installation selections** page, click **Install**.

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

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.

About this task

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

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

Procedure

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

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

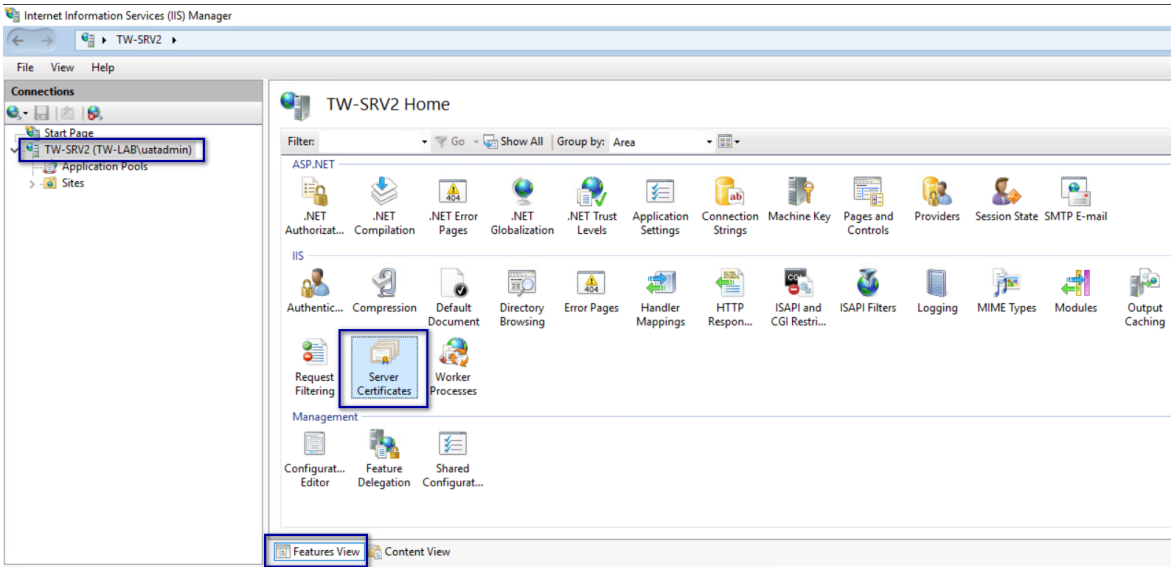


Figure 10. Server Certificates option

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

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

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

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

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

      The following figure provides an example of the **Import Certificates** window.

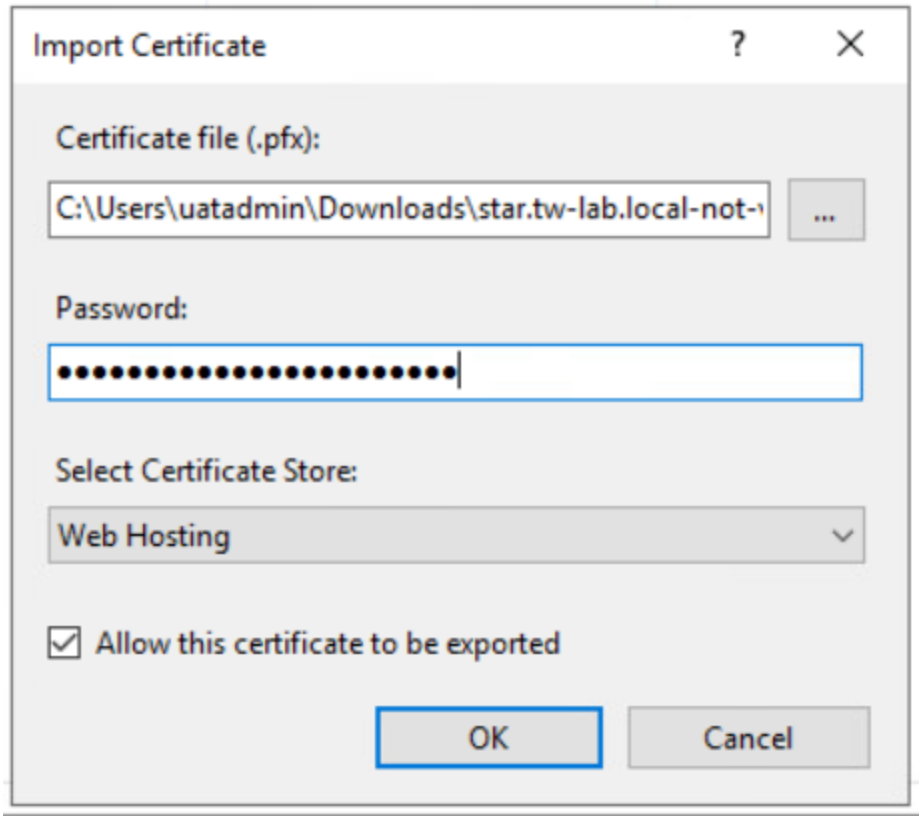


Figure 11. Server Certificates option

d. Click **OK**.

e. Right-click the TLS certificate that appears in the certificate list and select **Properties**.

f. On the **Details** tab, scroll down, and then select **Subject Alternative Name**. Confirm that the entry contains the FQDN of NES.

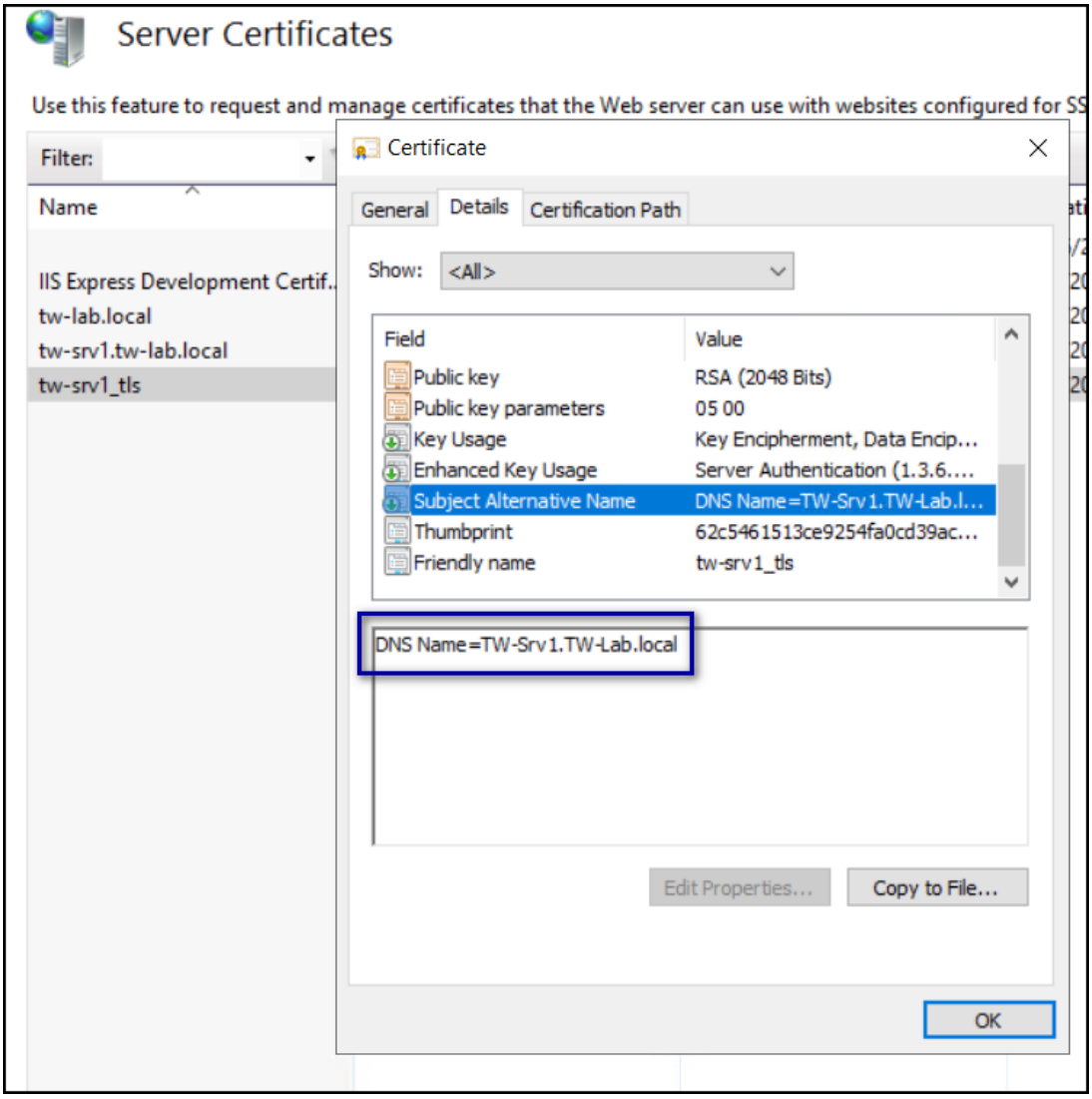


Figure 12. Server Certificates option

4. Minimize IIS.

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

    a. From the Window toolbar, in the **Search** field, type `Manage Computer`, and then select **Manage computer certificates**.

    b. On the **User Account Control** dialog, click Yes.

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

    d. Right-click **Certificates**, and then select **All Tasks > Import**, as shown in the following figure.

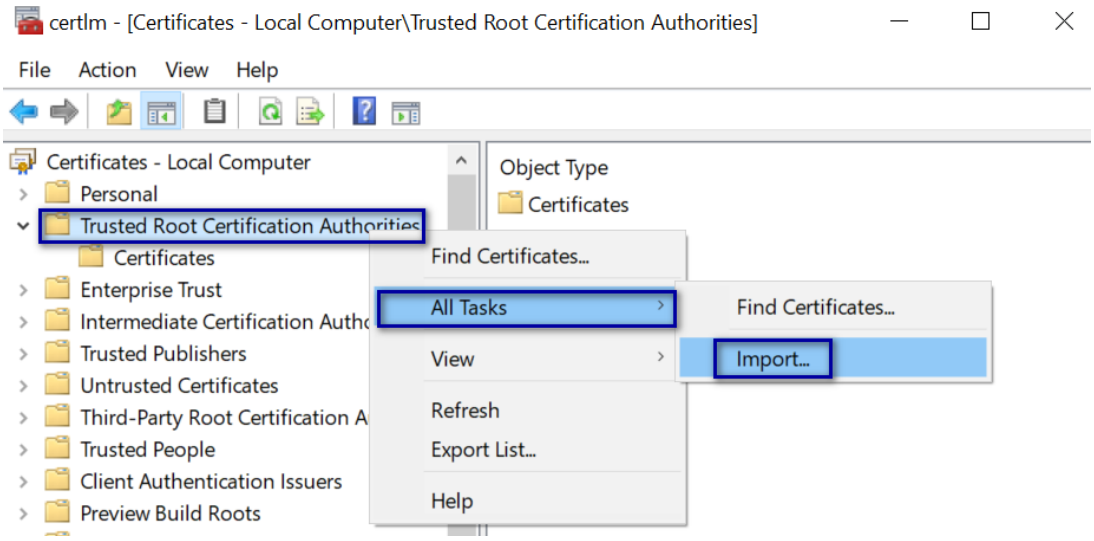


Figure 13. Import Certificate option

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

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

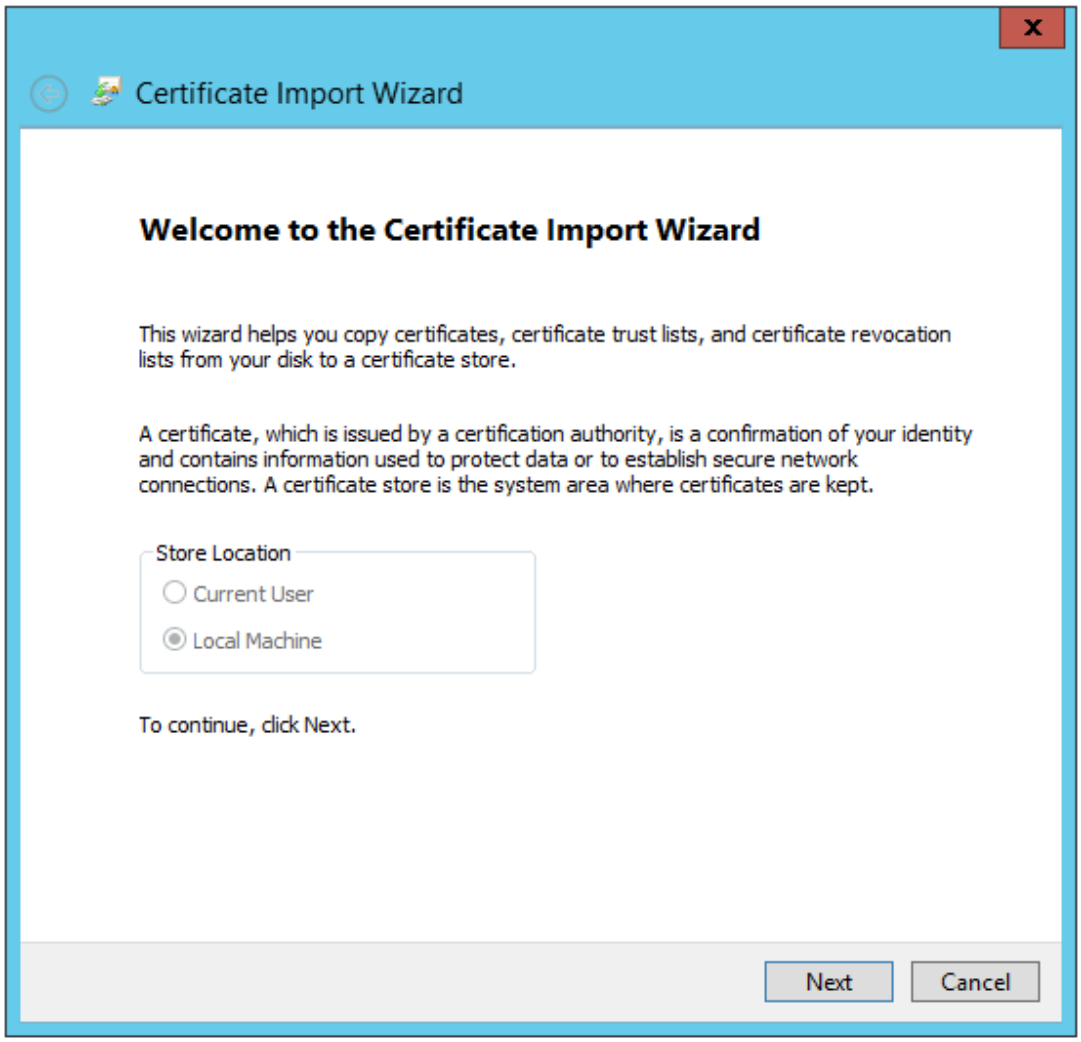


Figure 14. Welcome to the Certificate Import Wizard screen

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

   The following figure shows the **File to Import** screen.

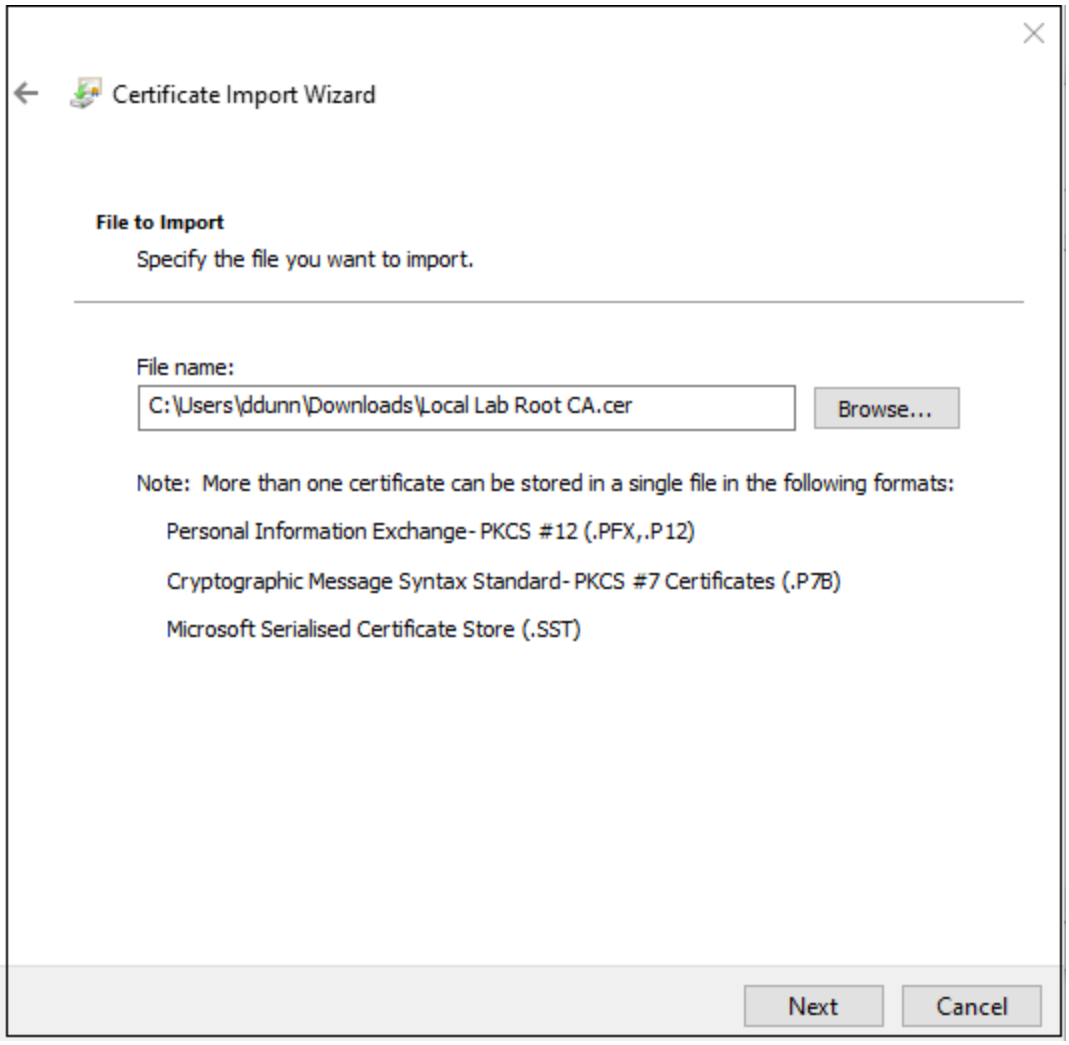


Figure 15. File to Import screen

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

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

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

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

k. Close the **certlm** window.

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.

About this task

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

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

Procedure

1. In the **Connections** navigation pane, click **Computer_Name > Sites**, as shown in the following figure.

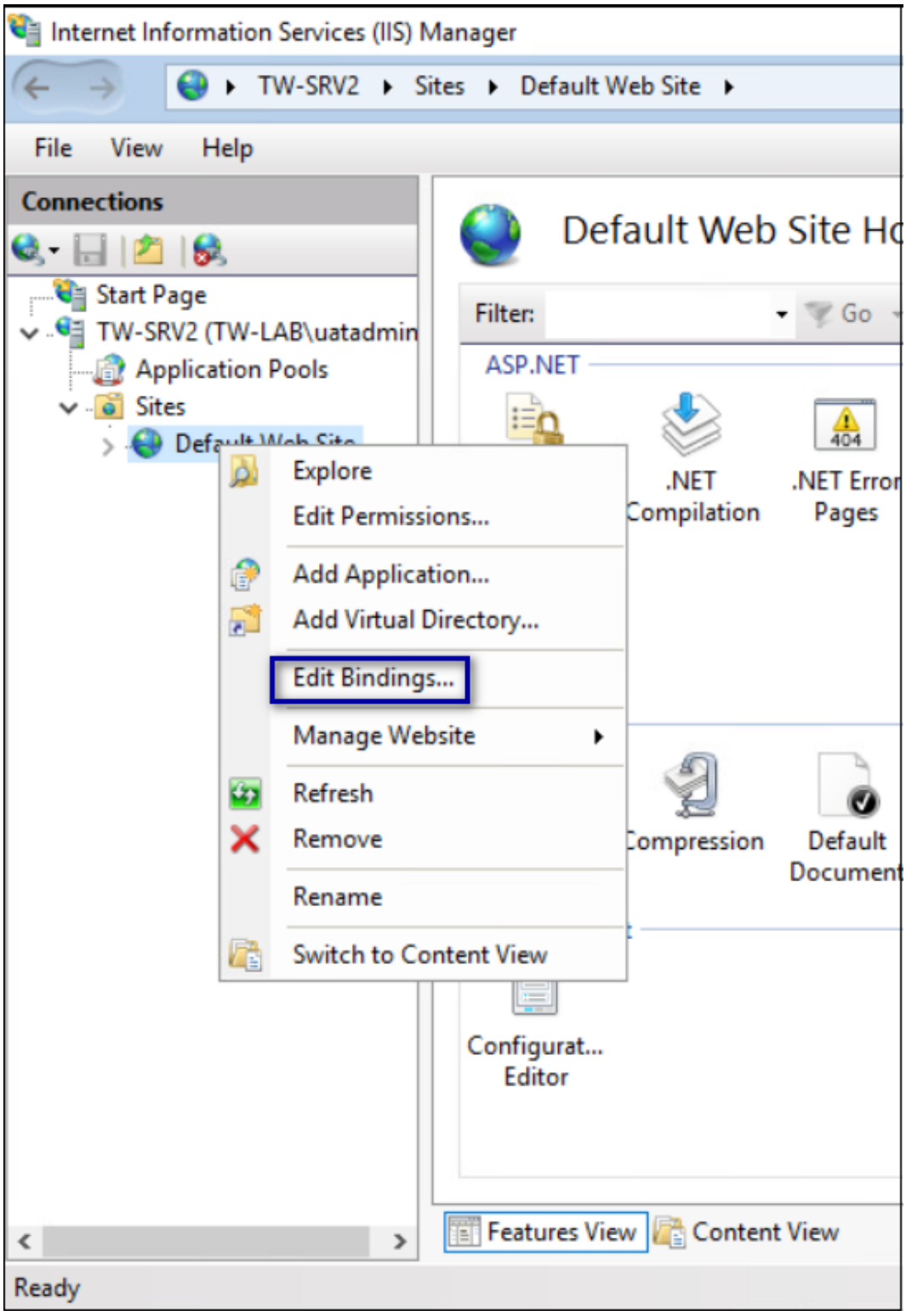


Figure 16. Edit Bindings Option

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

3. Click **Add**.

The **Add Site Binding** dialog box opens.

4. In the **Add Site Binding** dialog perform the following actions:

   a. From the **Type** list, select **https**.

   b. In the **IP Address** field, leave the default setting **All Unassigned**.

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

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

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

      The following figure provides an example of the **Add Site Binding** dialog.

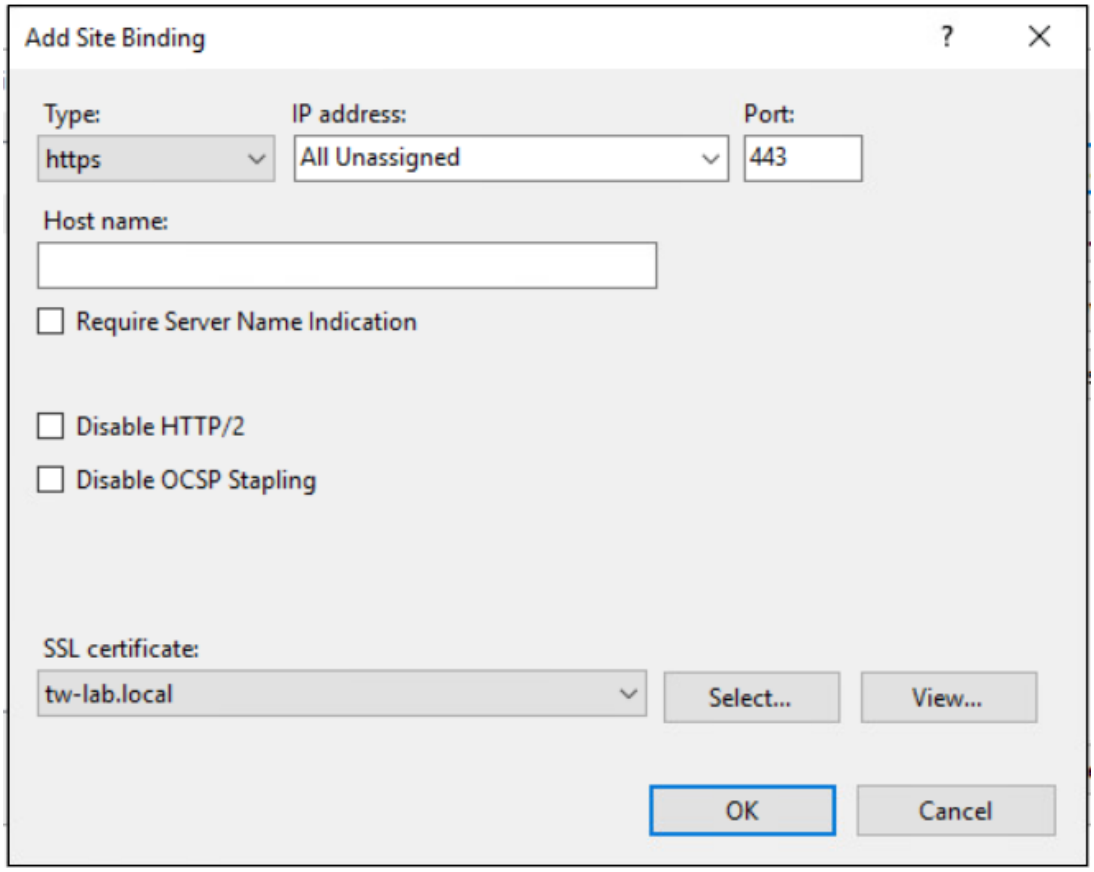


Figure 17. Add Site Binding Dialog

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

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

h. Click **OK**.

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

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.

About this task

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

Procedure

1. Expand **server_name**, right-click **Application Pools**, and then select **Add Application Pool**, as shown in the following figure.

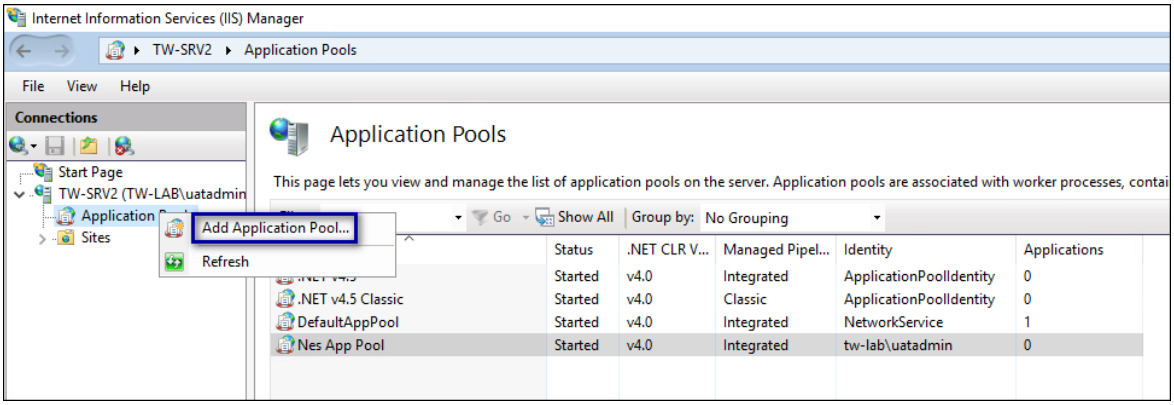


Figure 18. Create New Application Pool

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

   The following figure provides an example of the **Add Application Pool** window.

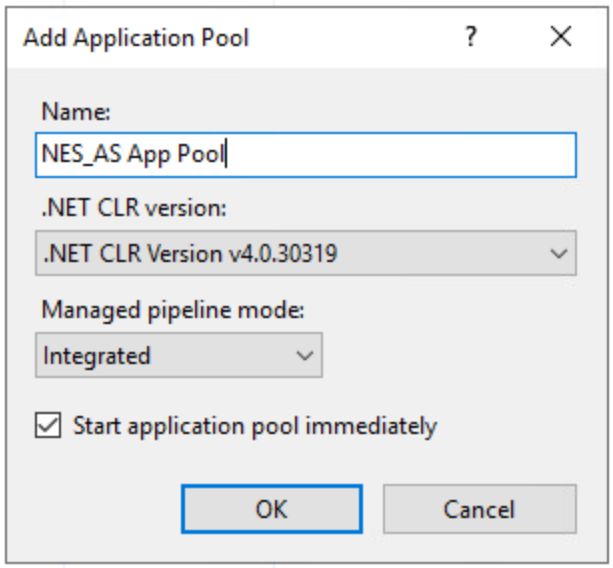


Figure 19. Add New Application Pool

3. Right-click **NES_AS App Pool**, and then select **Advanced Settings**, as shown in the following figure.

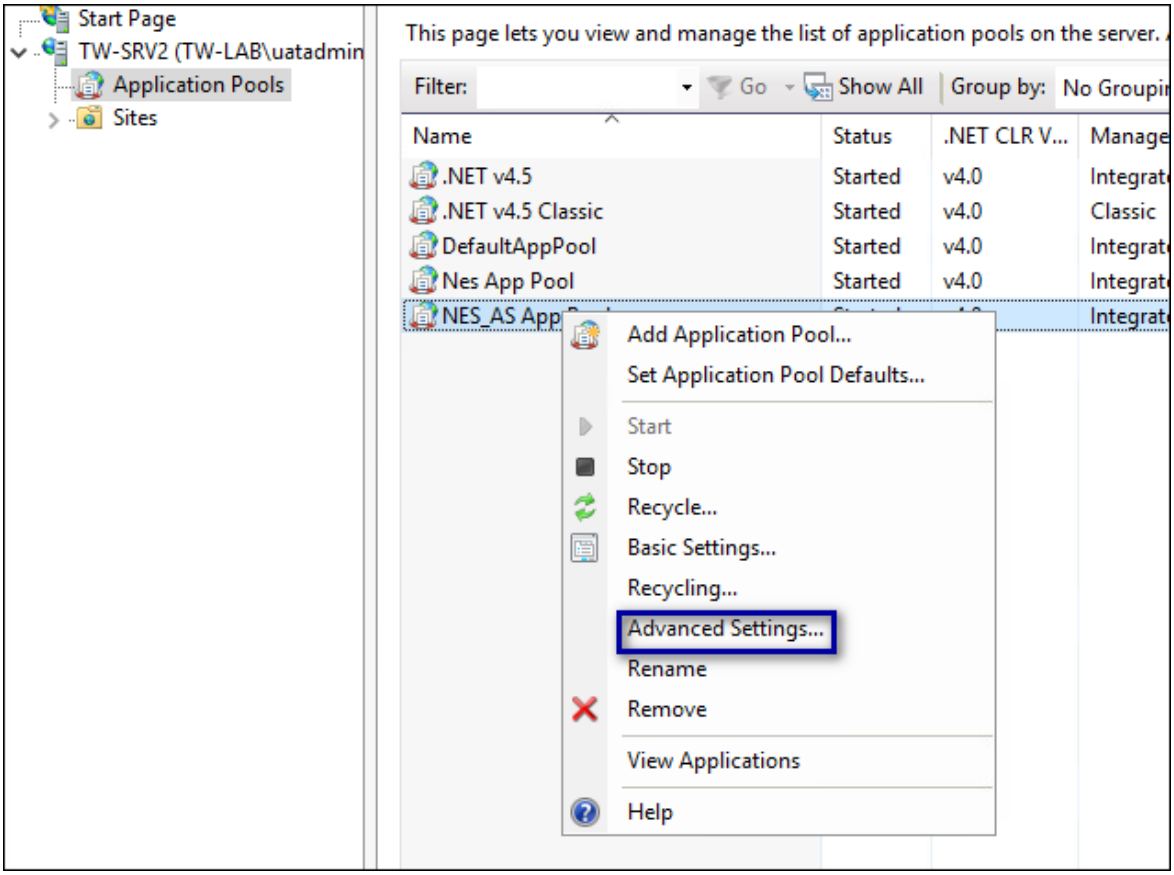


Figure 20. Advanced Settings for Application Pool

4. Click the **Ellipses** for the **Identity** parameter, as shown in the following figure.

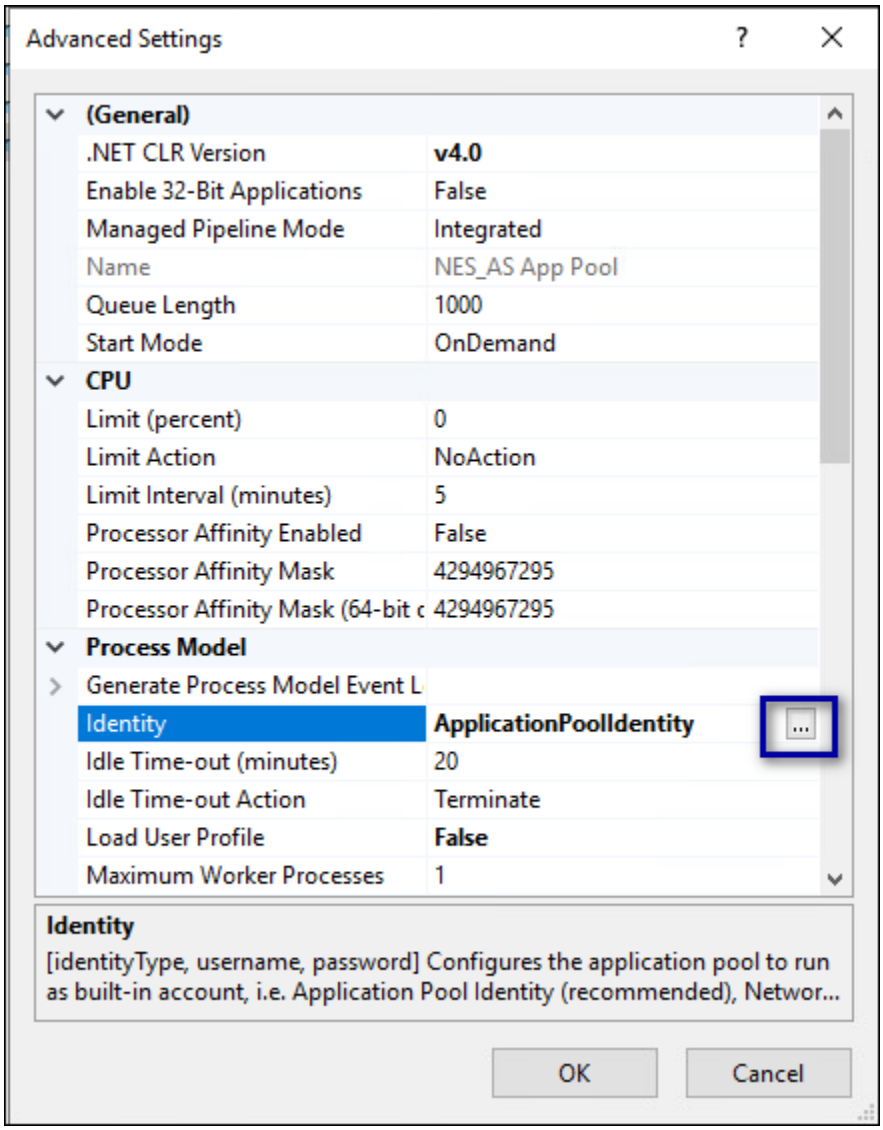
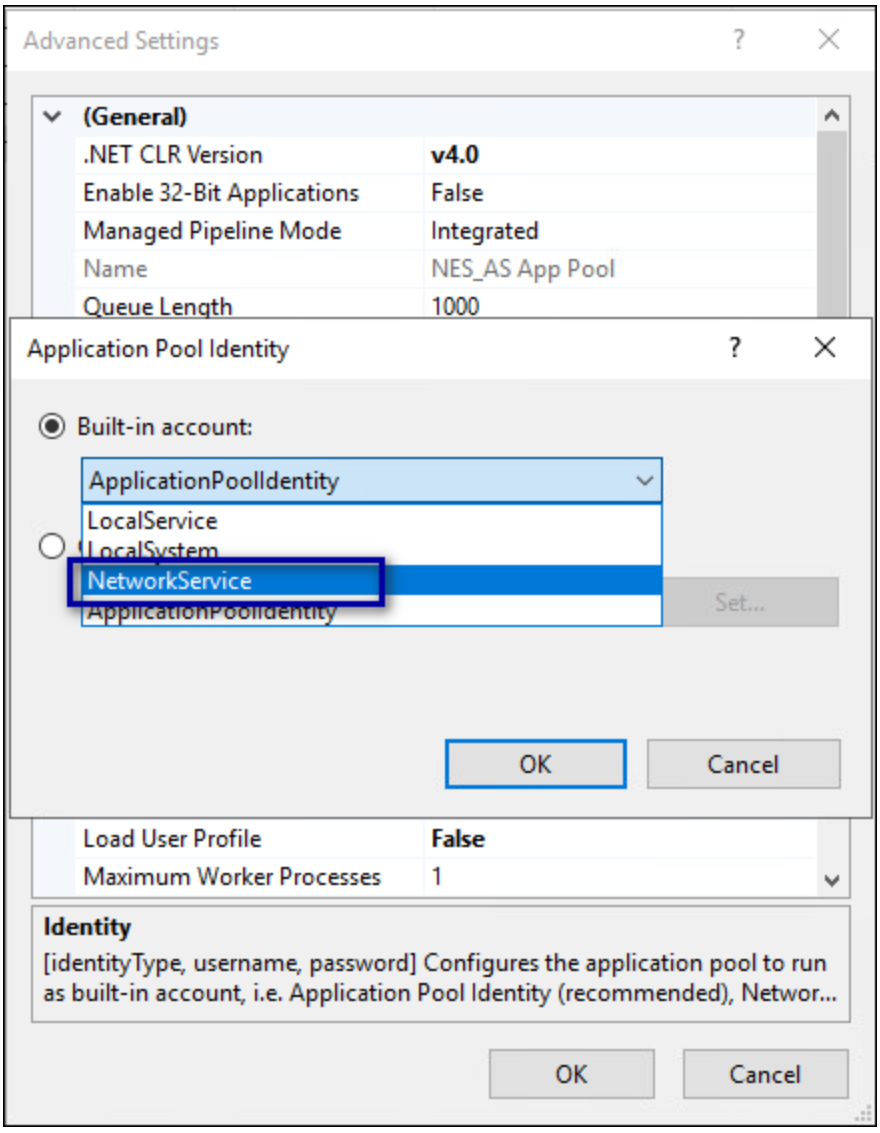


Figure 21. Edit Identity

5. Perform one of the following actions:

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



- For HA NES 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

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

What to do next

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 the **Internet Information Services (IIS) Manager** application to verify that the authentication configuration is correct.

Procedure

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

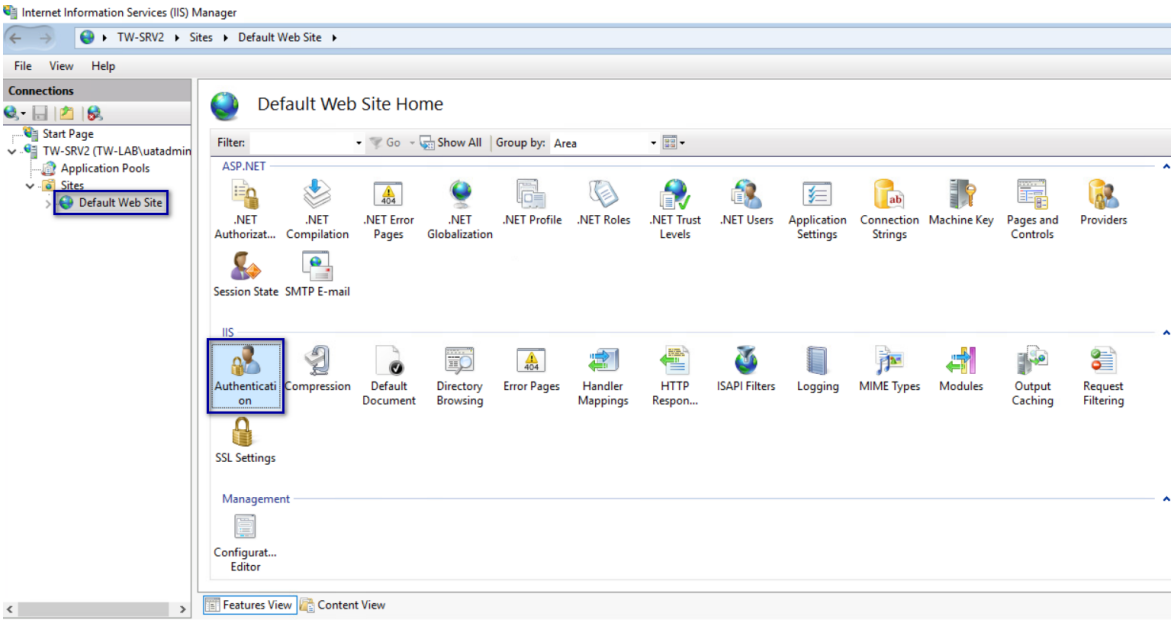


Figure 22. Authentication Option

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

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

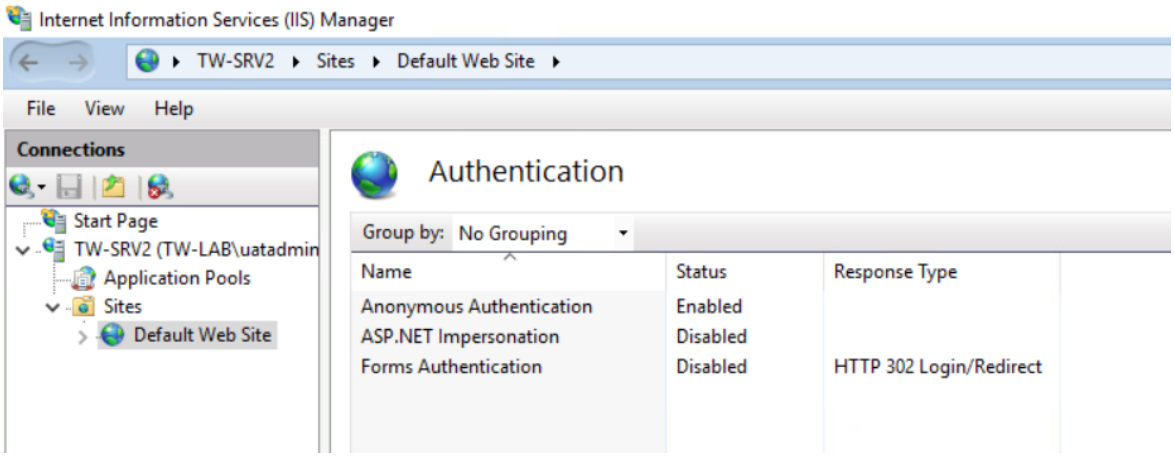


Figure 23. Authentication pane with Anonymous Authentication enabled

4.1.6 Securing IIS

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

About this task

Perform the following steps in the **Internet Information Services (IIS) Manager** application.

Procedure

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

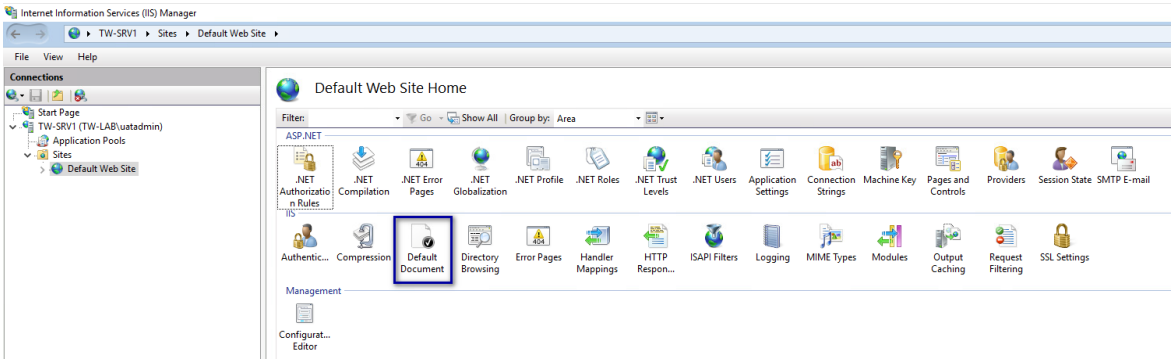


Figure 24. Default Document Option

2. On the **Default Document** page, select **Default.htm**, and then click **Disable** from the right menu, as shown in the following figure.

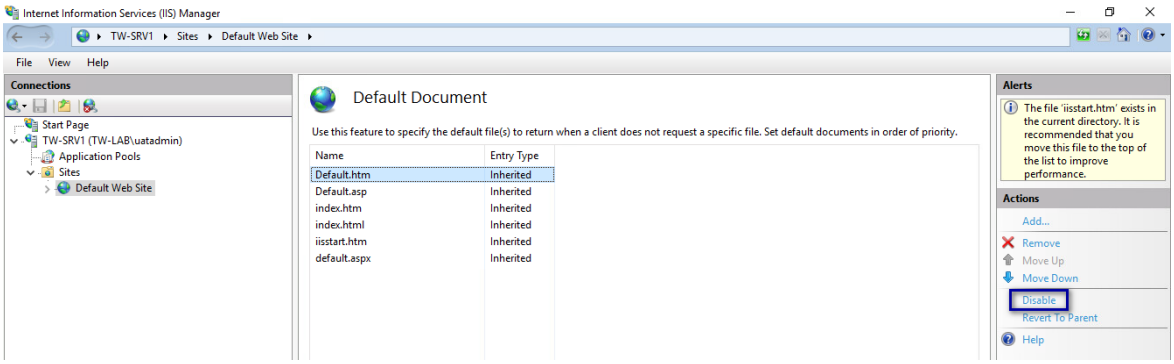
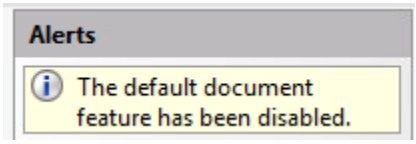


Figure 25. Disable Default.htm

After you click **Disable**, the **Alerts** section states that the page is disabled, as shown in the following figure



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

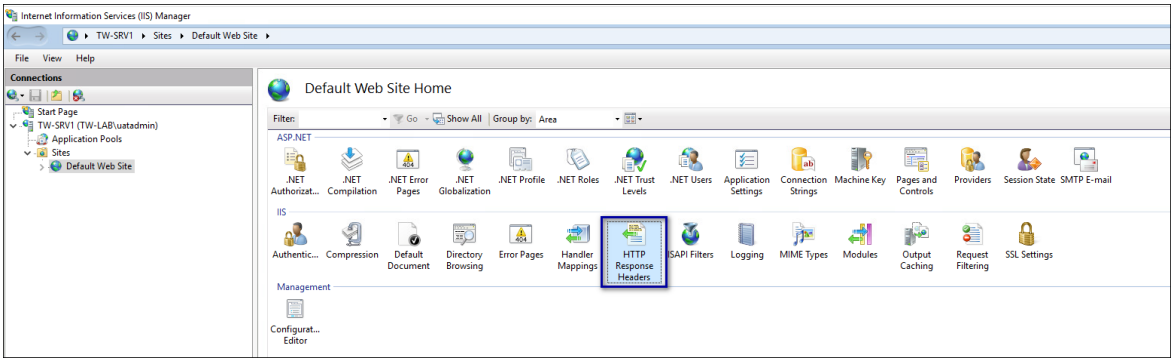


Figure 26. HTTP Response Headers Option

4. From the **Actions** section, click **Add**, as shown in the following figure.

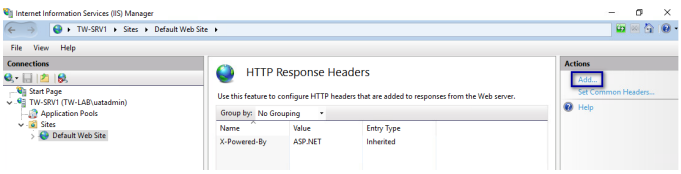


Figure 27. Add HTTP Response Headers Option

5. In the **Add Custom HTTP Response Headers** dialog box, perform the following actions:

   a. In the **Name** field, type `Strict-Transport-Security`.

   b. In the **Value** field, type `max-age=31536000`.

      The following figure provides an example of the **Add Custom HTTP Response Headers** dialog box.

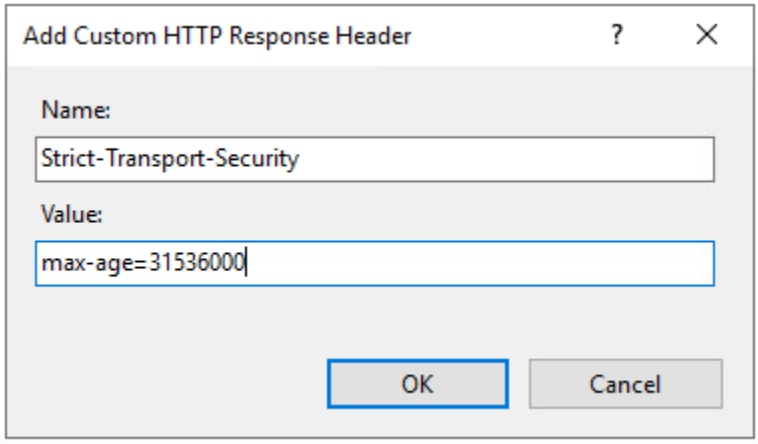
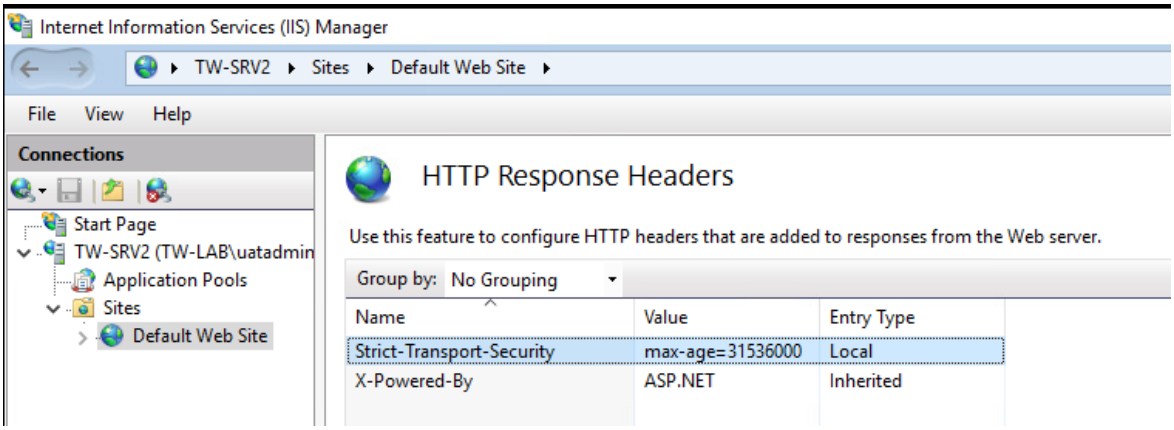


Figure 28. Add Custom HTTP Response Headers dialog box

   c. Click **OK**.

The Strict-Transport-Security header appears in the HTTP Headers table, as shown in the following figure.



6. Close **IIS Manager**

4.1.7 Enabling Directory Browsing IIS

Confirm that Directory Browsing is enabled.

About this task

Perform the following steps in the **Internet Information Services (IIS) Manager** application.

Procedure

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

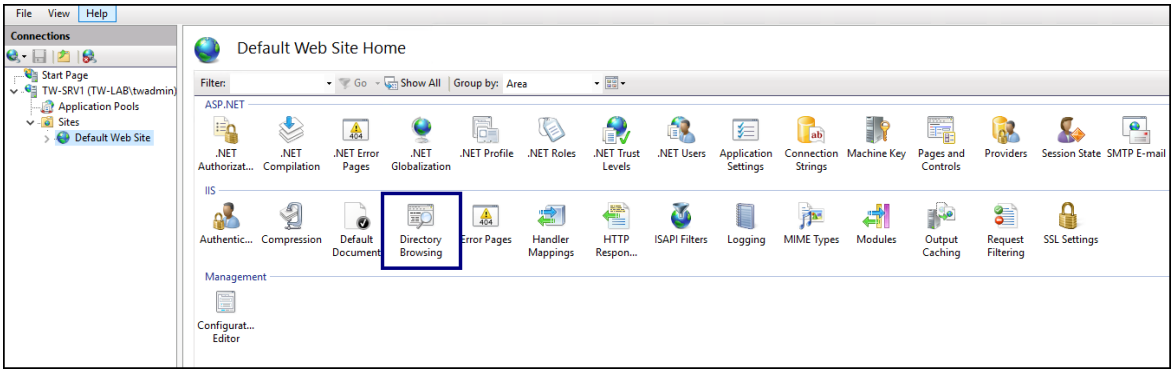


Figure 29. Directory Browsing Option

2. On the **Directory Browsing** page, review the **Actions** pane. If the message `Directory browsing has been disabled` appears, click **Enable**, as shown in the following figure.

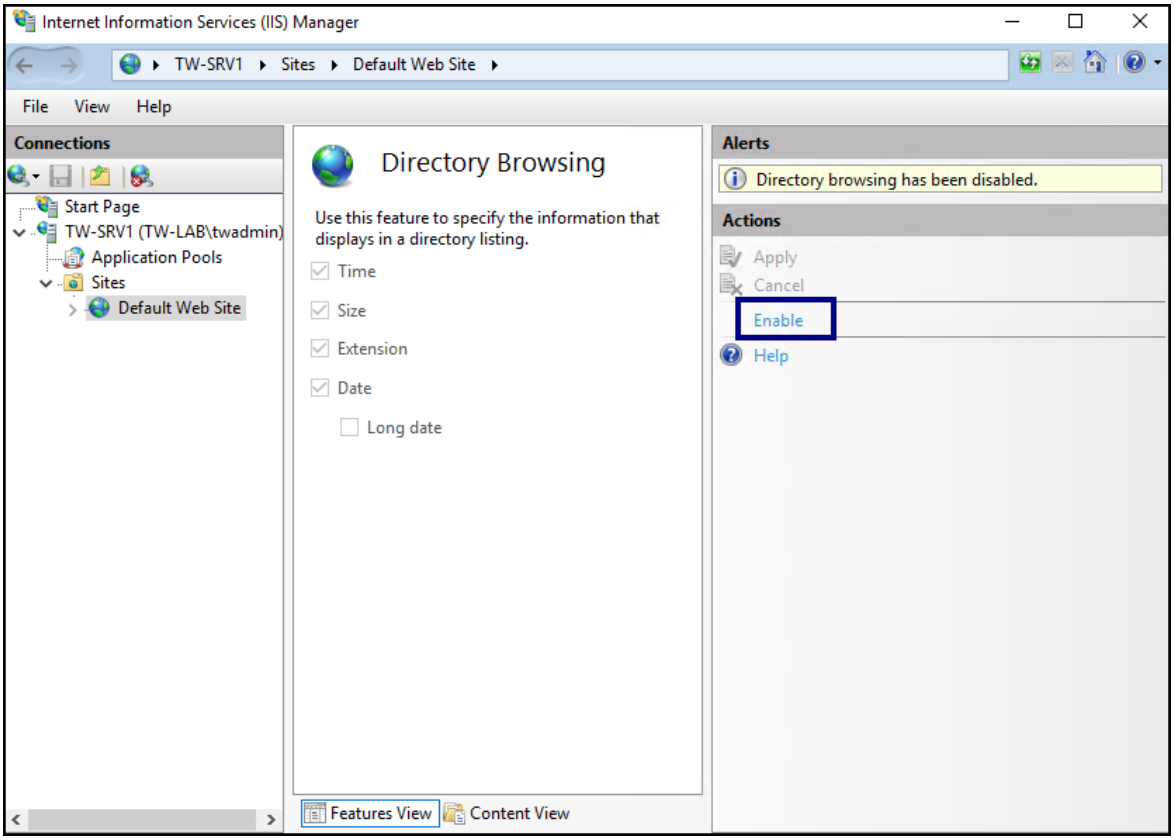


Figure 30. Enable Directory Browsing option

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 Nymi Enterprise Server (NES) servers.

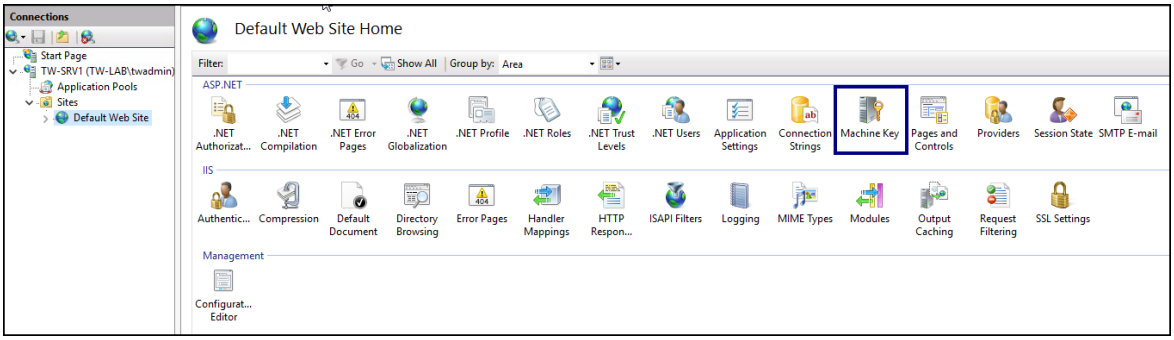
About this task

Perform the following steps in the **Internet Information Services (IIS) Manager** application on the first NES that you deploy.

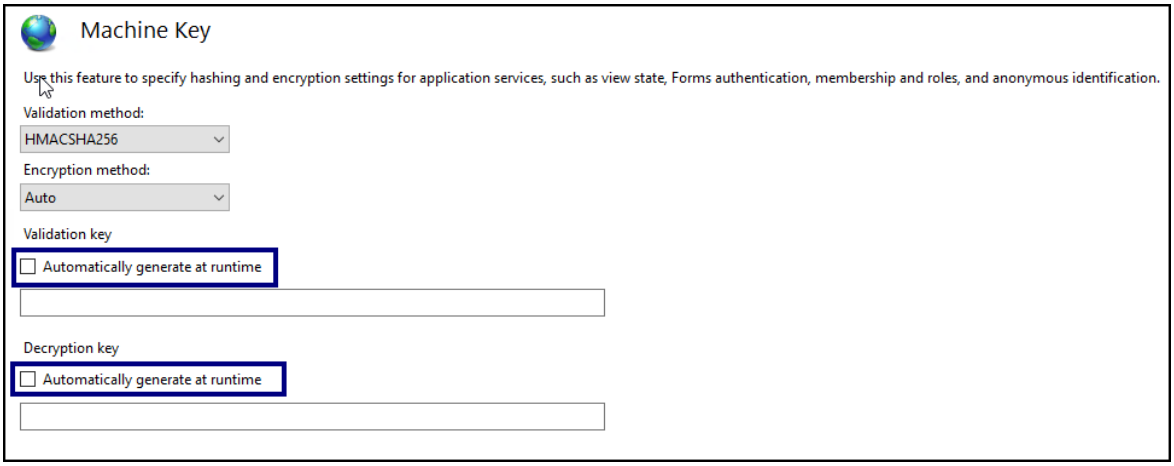
Procedure

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

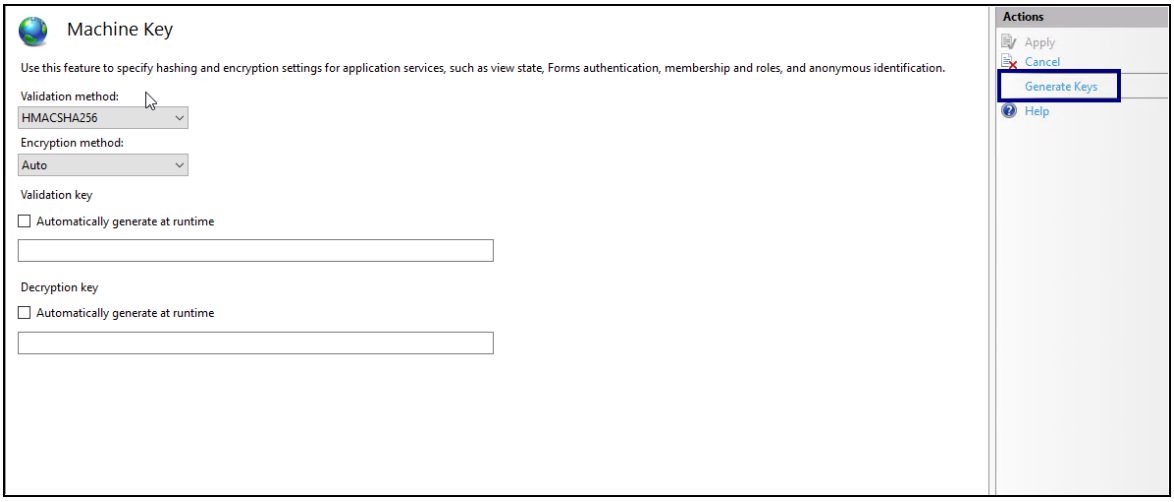
   The following figure shows the **Machine Key** option.



2. On the **Machine Keys** window, clear both **Automatically generate at runtime** options, as shown in the following figure.



3. In the **Actions** pane on the right side of the window, click **Generate Keys**, as shown in the following figure.



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 server:

    a. Expand `Computer_Name` > **Sites**, select **Default Web Site**, and then double-click **Machine Key**.
    b. On the **Machine Keys** window, clear both **Automatically generate at runtime** options, as shown in the following figure.
    c. In the **Validation Key** field, paste the Validation Key value from the first server.
    d. In the **Decryption Key** field, paste the Decryption Key value from the first server.
    e. Click **Apply** to save the generated keys.
    f. Restart the IIS service.

    The machine keys are now synchronized across all servers, which ensures consistent encryption and validation for applications running in a web farm configuration.

4.2 Importing a Fullchain Certificate

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

About this task

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

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

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

> **Note:** When you use

4.2.1 Importing Certificates

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

Procedure

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

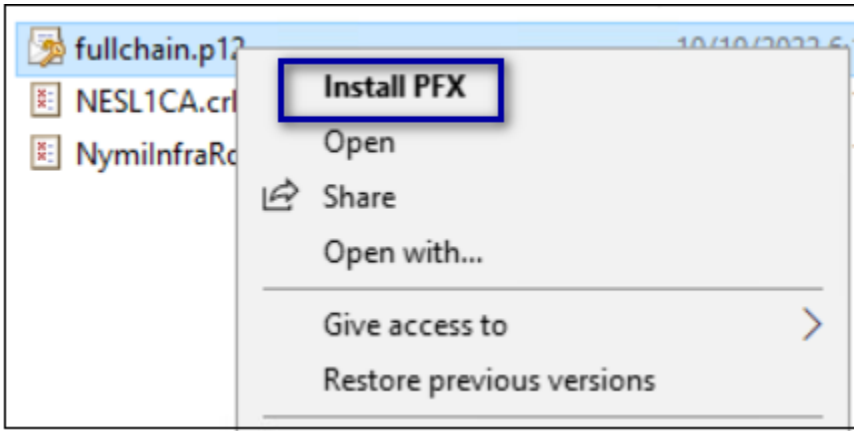


Figure 31. Install PFX Option

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

   The Certificate Import Wizard dialog box opens.

4. On the **Welcome to the Certificate Import Wizard** page, in the **Store Location** page, select **Local Machine**, as shown in the following figure.

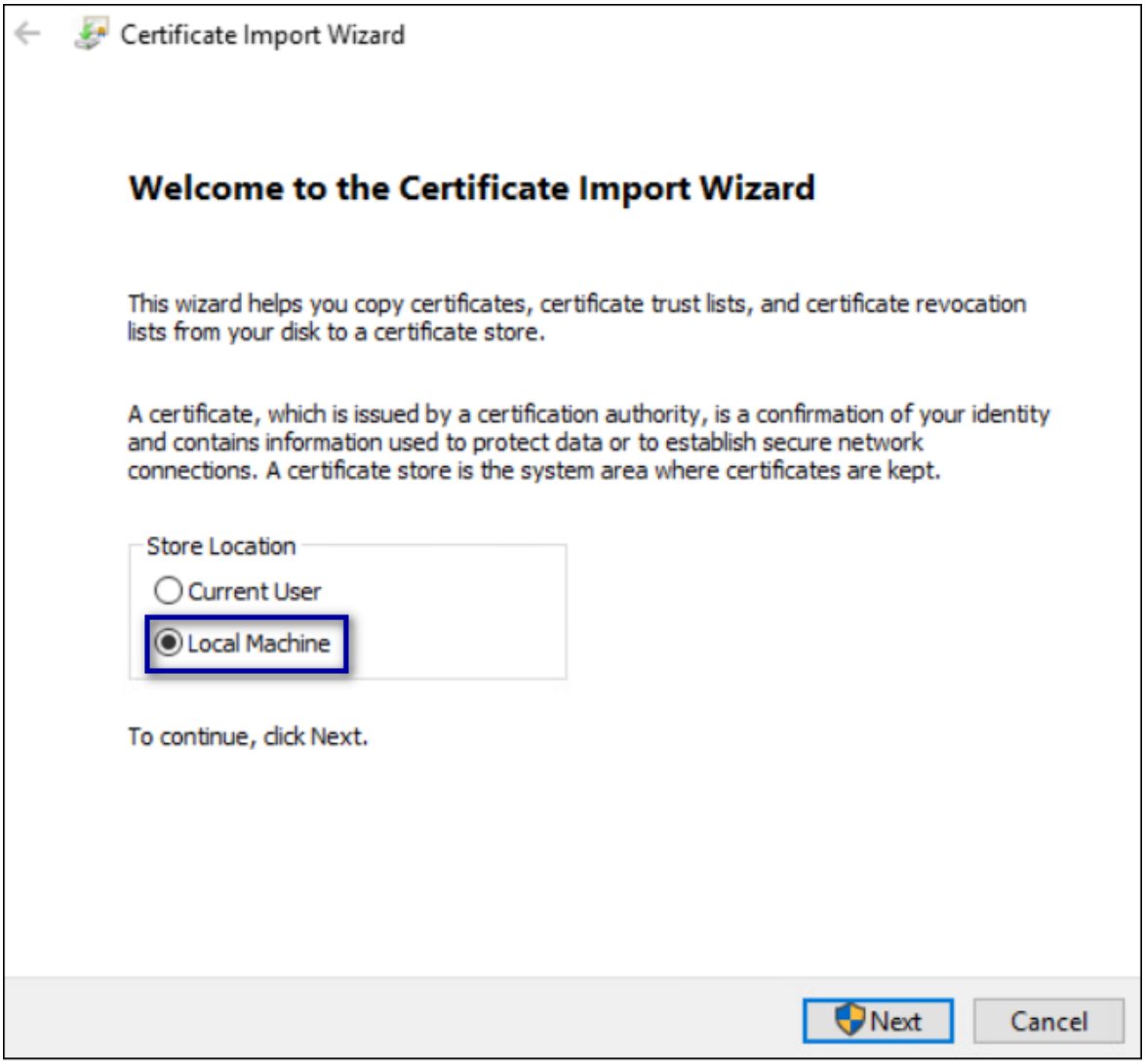


Figure 32. Local Machine Store Location

5. Click **Next**.

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

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

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

The following figure provides an example of the **Private Key Protection** page.

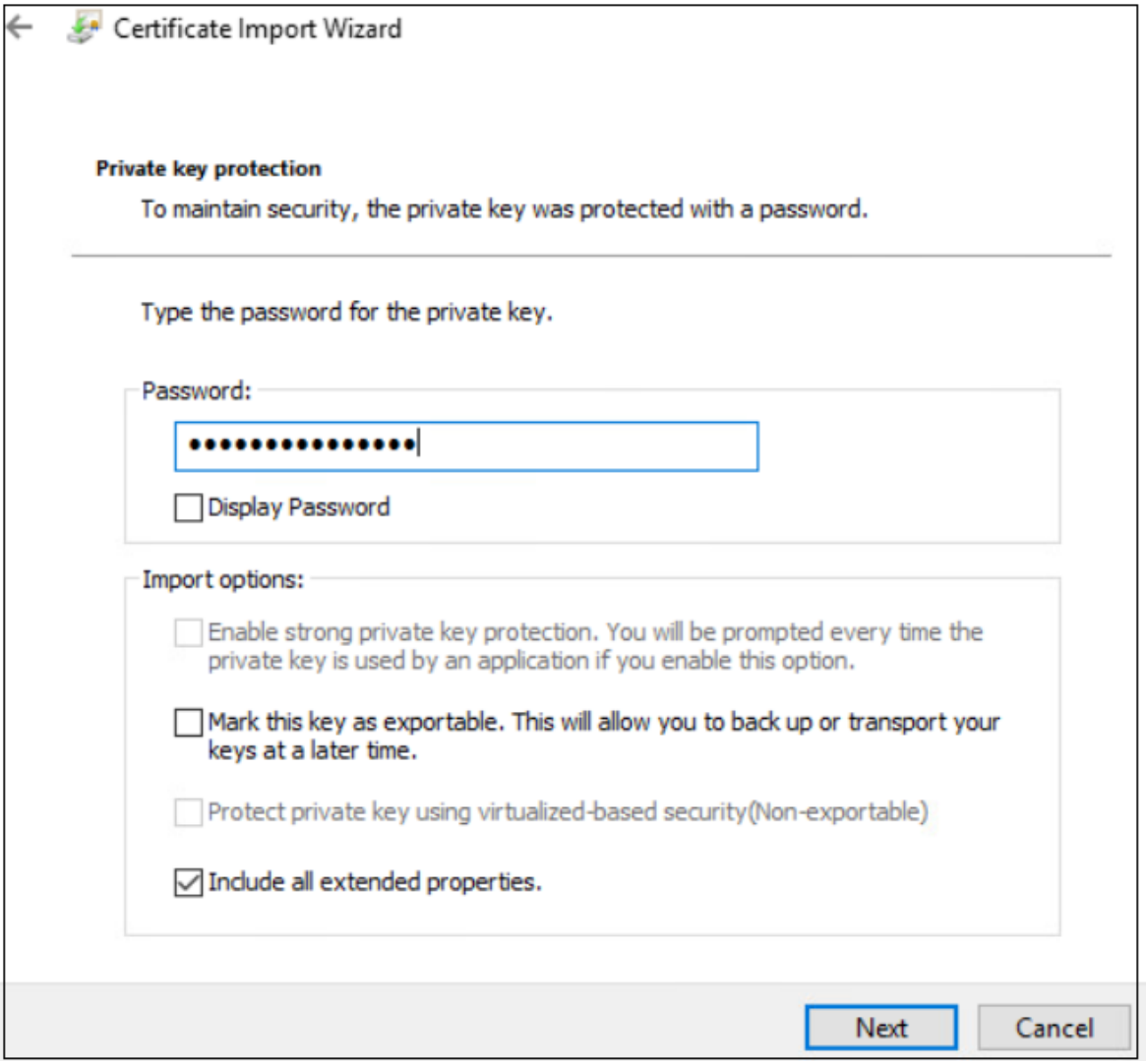


Figure 33. Private Key Protection Page

9. On the **Files to import** page, ensure that the `fullchain.p12` file appears in the **File name** field, and then click **Next**.
10. On the **Certificate Store** page, leave the default option Automatically select the certificate store based on the type of certificate, and then click **Next**.

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

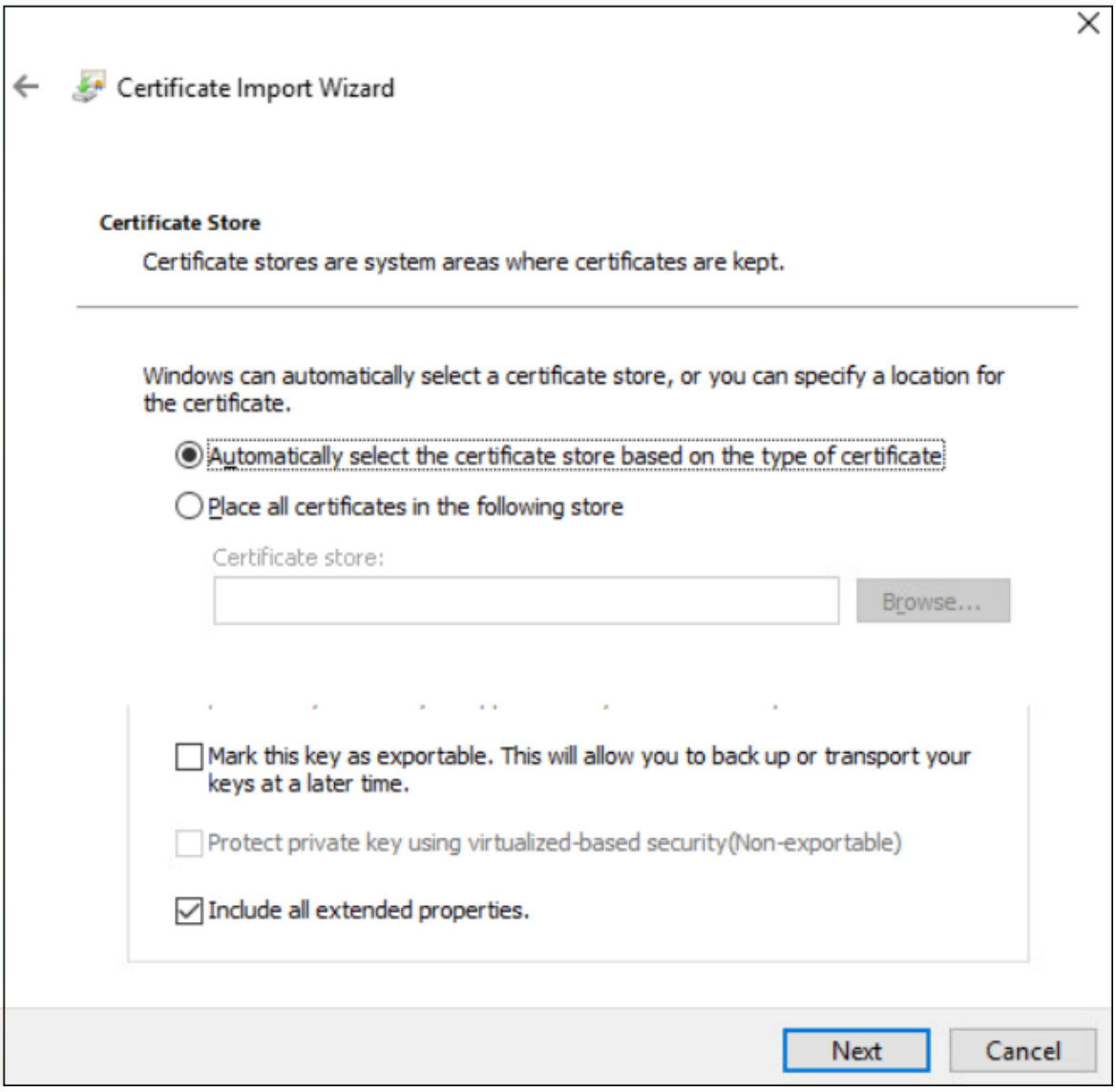


Figure 34. Certificate Store Page

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

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

4.2.2 Moving the L2 certificate

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

About this task

Procedure

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

   The **certlm** window appears.

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

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

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

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

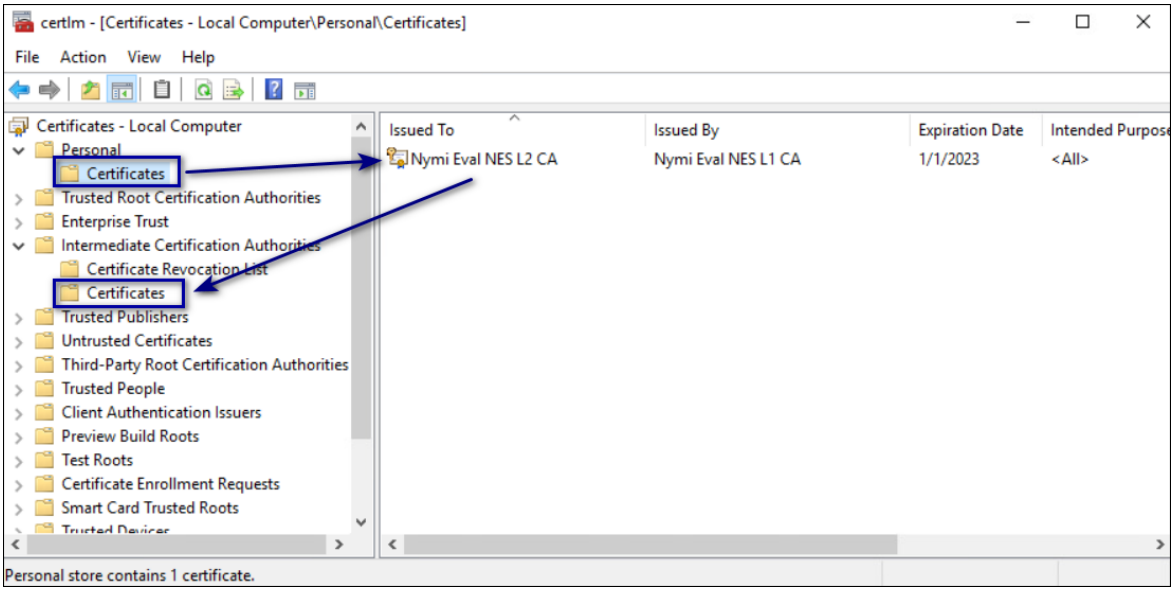


Figure 35. Certificates window

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

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

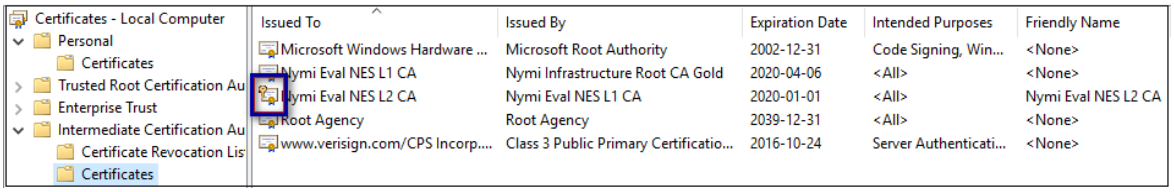


Figure 36. L2 Certificate with key

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

7. Close the **certlm** window.

4.3 Installing NES

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

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

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.

Before you begin

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

About this task

> **Note:** The installation process prompts you to install Microsoft .NET Framework 4.8 and SQL Server Express, if the applications are not previously installed on the NES host. If your environment already has a

SQL Server that is not locally installed on the NES server and you will create the database on that SQL server, you can skip the SQL Server Express installation.

Procedure

1. Log in to the host with a domain user account that has local administrator rights.
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 account and the deployment uses a remote SQL server, run the `install.exe` with the Nymi Infrastructure Service Account 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**.

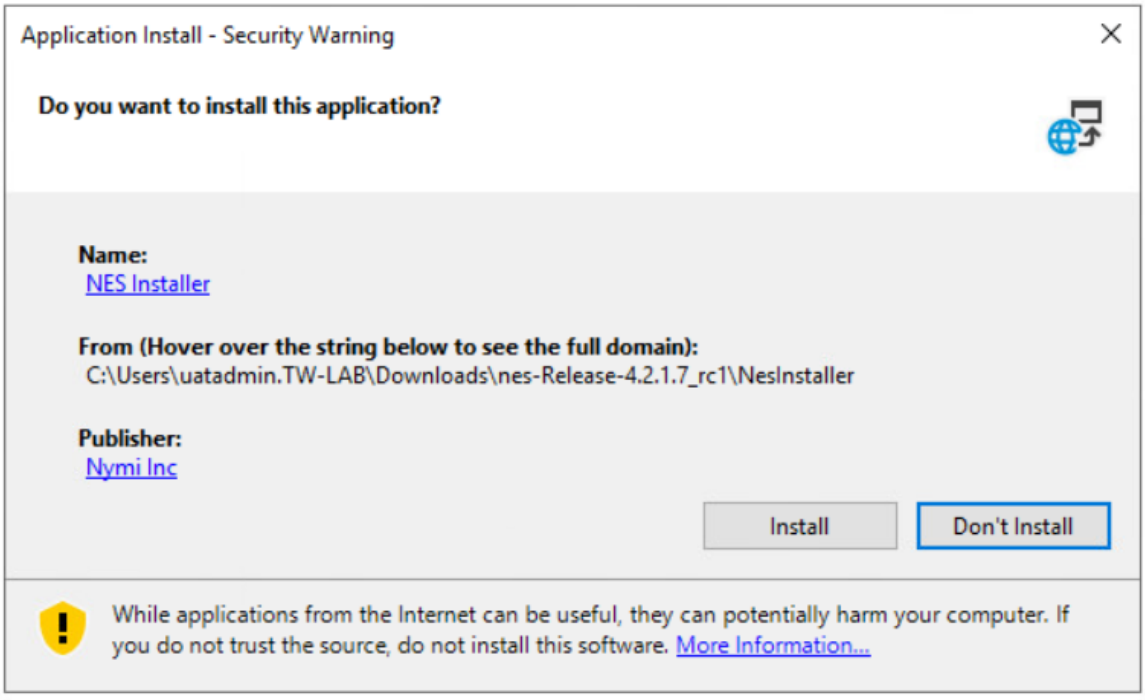


Figure 37. Security Warning

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

11. If you see the **Open File – Security Warning** page, click **Run**.
12. If you see the **User Account Control** dialog, page, click **Yes**.
13. If the installer does not detect a version of SQL Express on the host, the **Install Prerequisites** dialog appears. Perform of the following actions:

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

Results

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

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

The following figure shows the **Prerequisites Check** dialog.

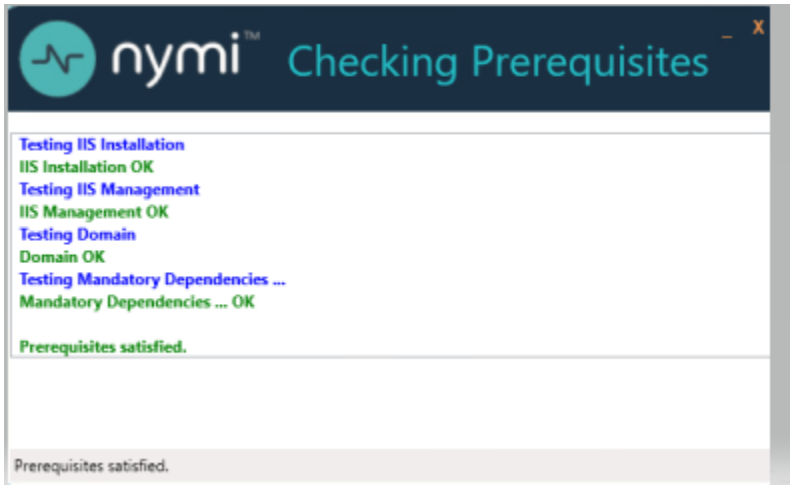


Figure 38. Prerequisites Check Dialog

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

Additional Information

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

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.

About this task

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

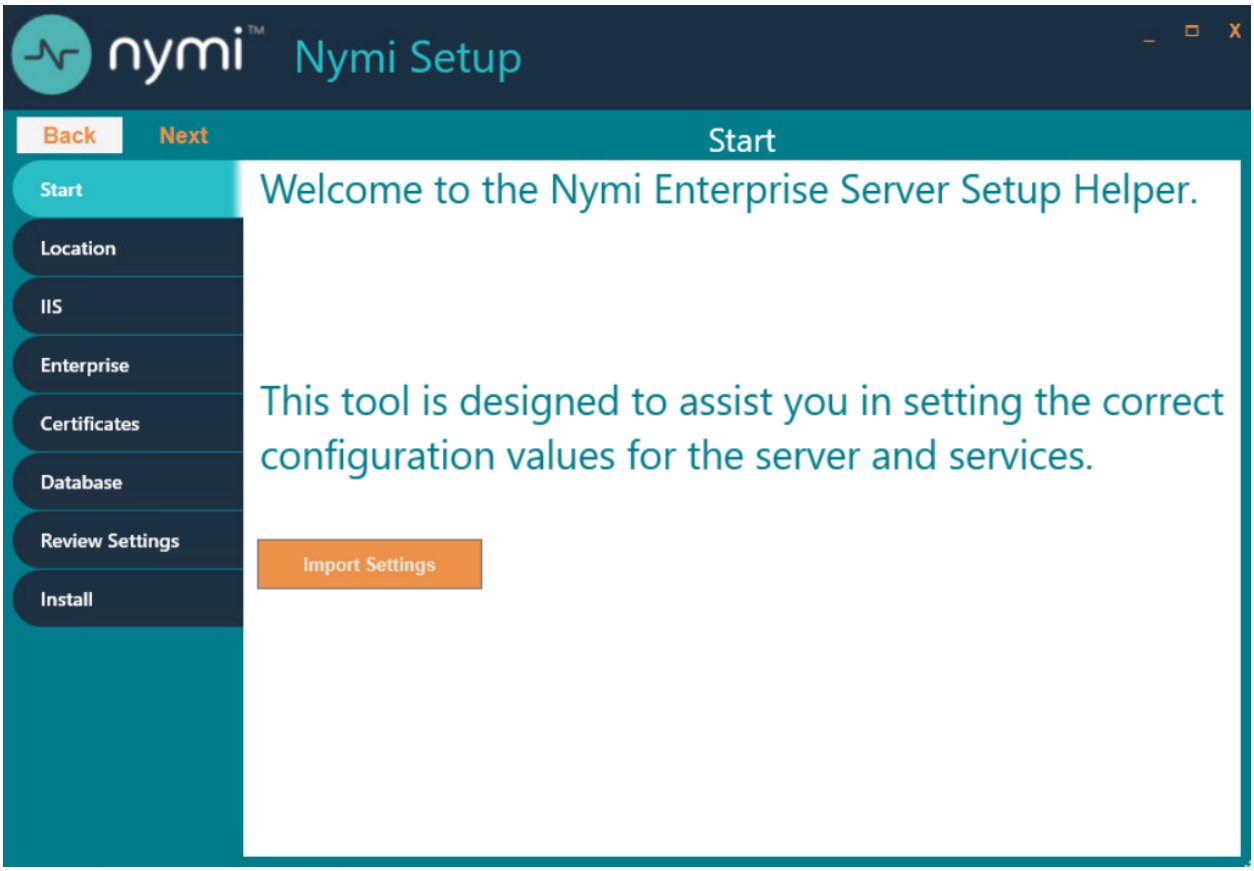


Figure 39. NES Setup Help wizard

Perform the following actions to configure the NES Services Suite.

> **Note:** For HA deployments, you will manually configure NES on the first server only. For the remaining NES servers, you will use the **Import Settings** button to load a configuration file, which includes all the NES configuration settings from the first NES server. Creating the configuration file to deploy a subsequent NES is explained later in this document.

Procedure

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

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

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

    This step optional, but recommended. The name cannot contain spaces.

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

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

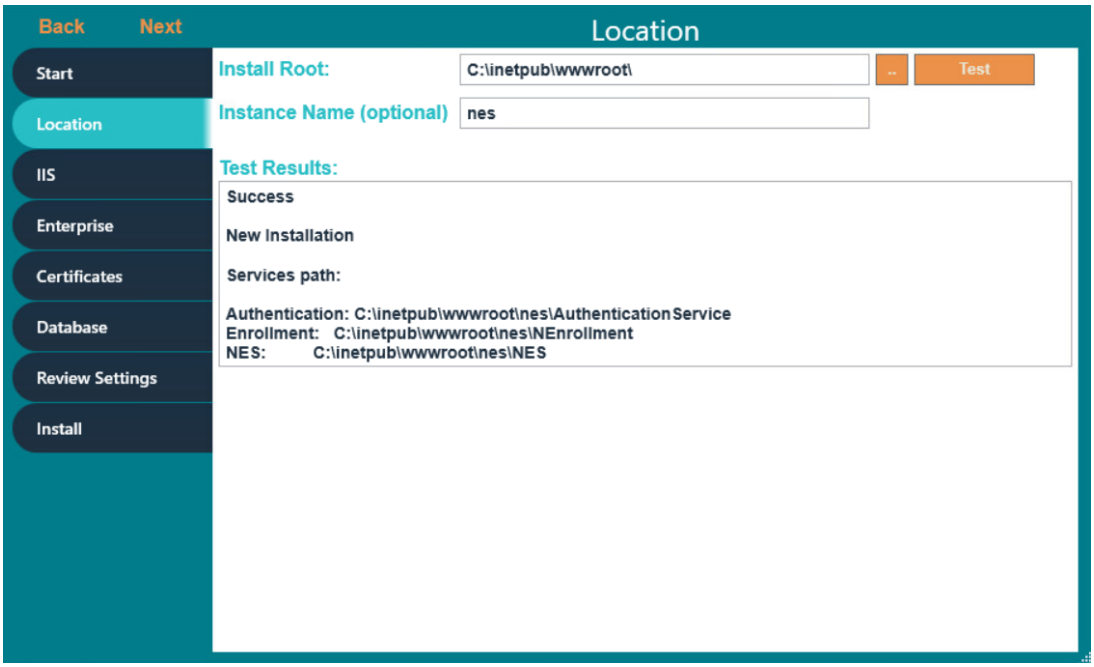


Figure 40. Location page in the NES Setup wizard

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

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

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

    b. 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 servers later.

    c. In the **Communication Protocol** section, available IIS site bindings appear. Select a communication protocol for the deployment.

    Nymi recommends that you select HTTPS to ensure secure communication and HTTPS is required for CWP with Evidian deployments. If an HTTPS address is not available, review Adding HTTPS site bindings to add a HTTPS site binding.

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

    d. In the **NES Admin and Enrollment Application Service** and **Authentication Service** sections, perform the following actions, based on your configuration scenario:

Single NES instance and remote SQL server that uses Windows Authentication	**NES Admin and Enrollment Application Service Configuration** i. In **Application Pool**, leave the default application pool. ii. 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 `domain\username`. C. In the **Password** field, type the password for the Nymi Infrastructure Service Account. iii. Click the **Test** button to validate the user credentials. **Authentication Service Configuration** i. From the **Application Pool** list, select **NES_AS App Pool**. ii. From the **Application Pool Identity** list, select **Network Service**.

Multiple NES instances in a high-availability configuration, remote SQL Server	**NES Admin and Enrollment Application Service Configuration** i. In **Application Pool**, leave the default application pool. ii. 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 `domain\username`. C. In the **Password** field, type the password for the Nymi Infrastructure Service Account. D. Click the **Test** button to validate the user credentials. **Authentication Service Configuration** i. From the **Application Pool** list, leave the default application pool. ii. 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 `domain\username`. > **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).

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

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

> **Note:** Service mapping defines the relative address of each of the web services (web apps) that run on the server.

The following figure provides an example of the **IIS Setup** page for a single NES instance deployment that uses a remote SQL database.

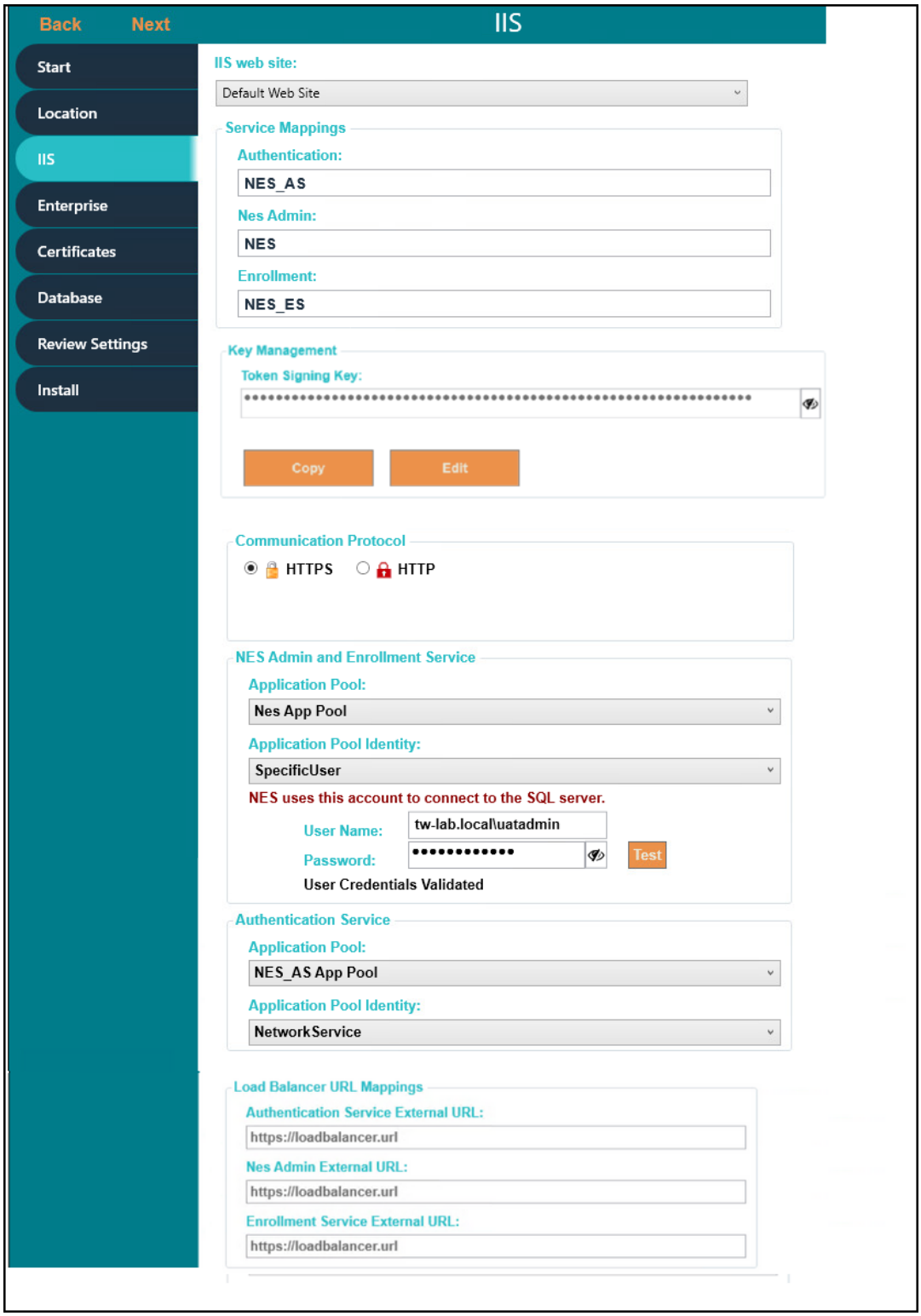


Figure 41. IIS Setup page in the NES Setup wizard

f. For environments where user terminals connect to NES with an FQDN that differs from the FDQN of the NES server, in the **Load Balancer URL Mappings** section, perform the following actions:

   i. In the **Authentication Service External URL** field, specify the load balancer URL for the Authentication Service, in the format `https://NES_loadbalancer_url/instance_name_AS`

      where:

      - `NES_loadbalancer_url` is the FQDN of NES that you user terminals use to connect to NES.
      - `instance_name` is the IIS instance name that you specified on the **Location** tab.

      For example `https://loadbalancer.org_name.com/NES_AS`.

   ii. In the **NES Admin External URL** field, specify the load balancer URL for the NES Administrator Service, in the format `https://NES_loadbalancer_url/instance_name.`

      For example `https://loadbalancer.org_name.com/NES`.

   iii. In the **Enrollment Service External URL** field, specify the load balancer URL for the NES Enrollment Service, in the format `https://NES_loadbalancer_url/instance_name_ES`.

      For example `https://loadbalancer.org_name.com/NES_ES`.

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

   a. In the **LDAP protocol** section, select LDAP or LDAPS.

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

   b. 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:

      i. In the **Domain** table, on an empty line, type the NetBIOS (Pre-Windows 2000) name of the domain that contains the user accounts. Refer to Appendix—Record the CWP Variables for your NetBIOS domain name.

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

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

> **Note:** Select a domain user whose password never expires.

iii. Press **Enter**.

iv. Press **Test** to confirm that NES can reach all domains.

c. 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 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 contacts AD to confirm that the validity of the account, and AD returns an `Invalid Max Password Age` message, NES uses the **Max Password Age** value to determine when the password expires. If the password expiration period has not been reached or exceed, NES allows the Nymi Band tap operation to complete.

d. 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. Refer to Appendix—Record the CWP Variables for the name of the NES Administrator group(s).

e. Press **Test** to confirm that NES can find each defined group.

f. If the solution in 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.

g. Press **Test** to confirm that NES can find each defined OU.

h. In the **Nymi Infrastructure Service Account** section, in the **User Name** field, enter the Nymi Infrastructure Service Account in the format `domain\name`.

The following figure provides an example of the **Enterprise** page.

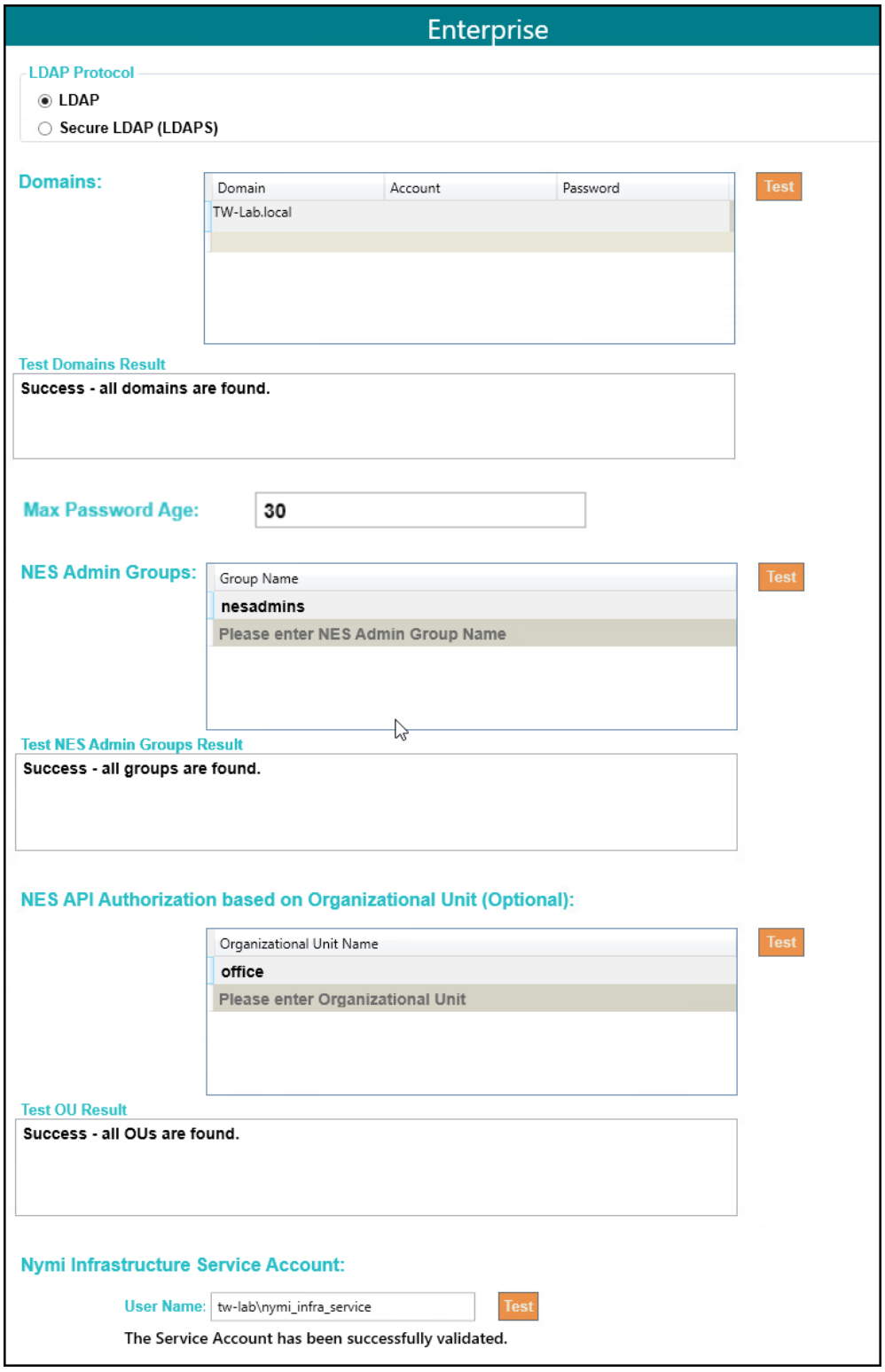


Figure 42. Enterprise page in the NES Setup wizard

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

    a. From the **Level One Certificate** list, select the L1 certificate from the list.

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

    b. From the **Level Two Certificate** list, select the L2 certificate.

    c. 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.

    d. In the **Password Required** pop-up, type the Full Chain certificate password, and then click **OK**.

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

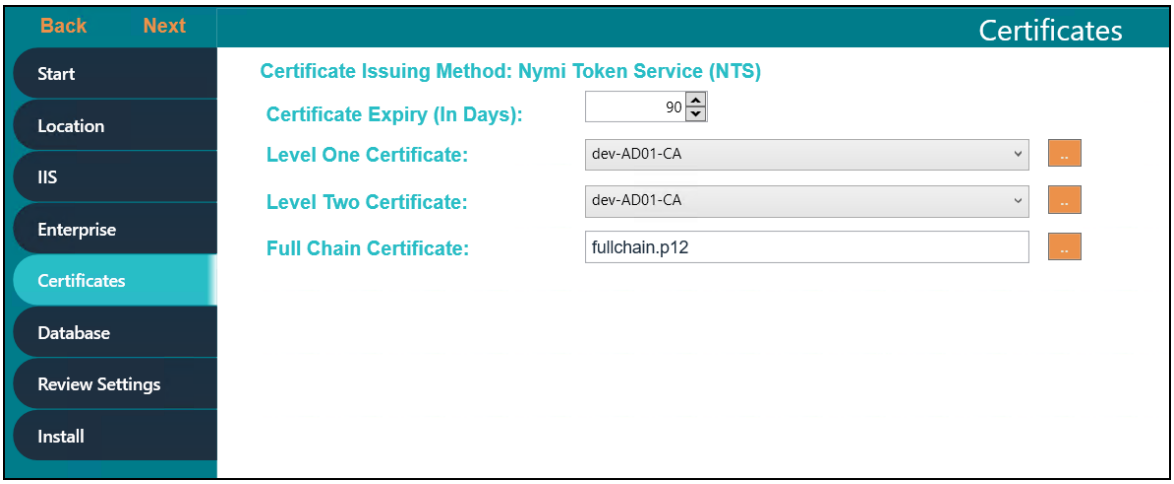


Figure 43. Certificates page in the NES Setup wizard

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

    ◦ Windows Authentication

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

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

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

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

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

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

The table displays the default account settings for the **Application Pool** and **Application Policy** identity settings that were defined on the **IIS** page appear. By default, the **Service type** login is an account that provides NES with access to the SQL database (Nymi Infrastructure Service Account).

◦ SQL Authentication

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

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

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

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

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

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

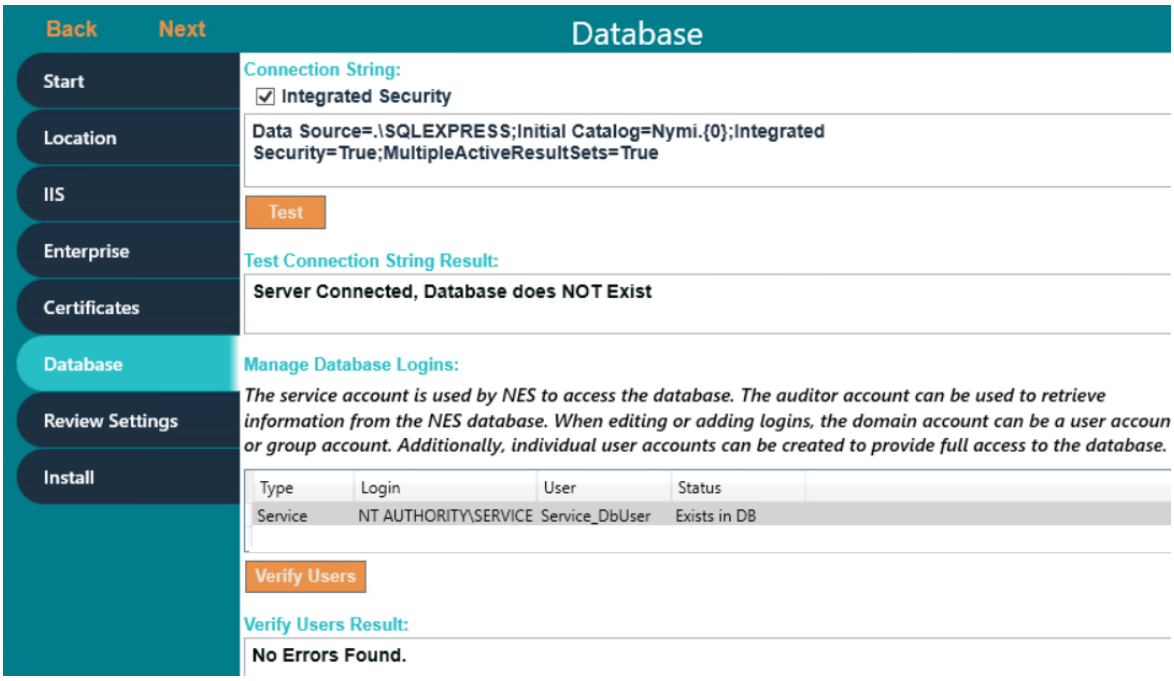


Figure 44. Database Setup page in NES Setup wizard for Windows Authentication

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

    a. Click **Test** to verify the configuration. Review the test results and address any errors if applicable.



Figure 45. Review Settings window

Consider the following information for some common warnings that might appear and how to resolve the issue.

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 Importing the TLS server certificates section, and the retry.

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

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

Table 4. Install page Options

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

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

   The following figure provides an example where the installation succeeds with a warning that the L2 certificate expires within 90 days.

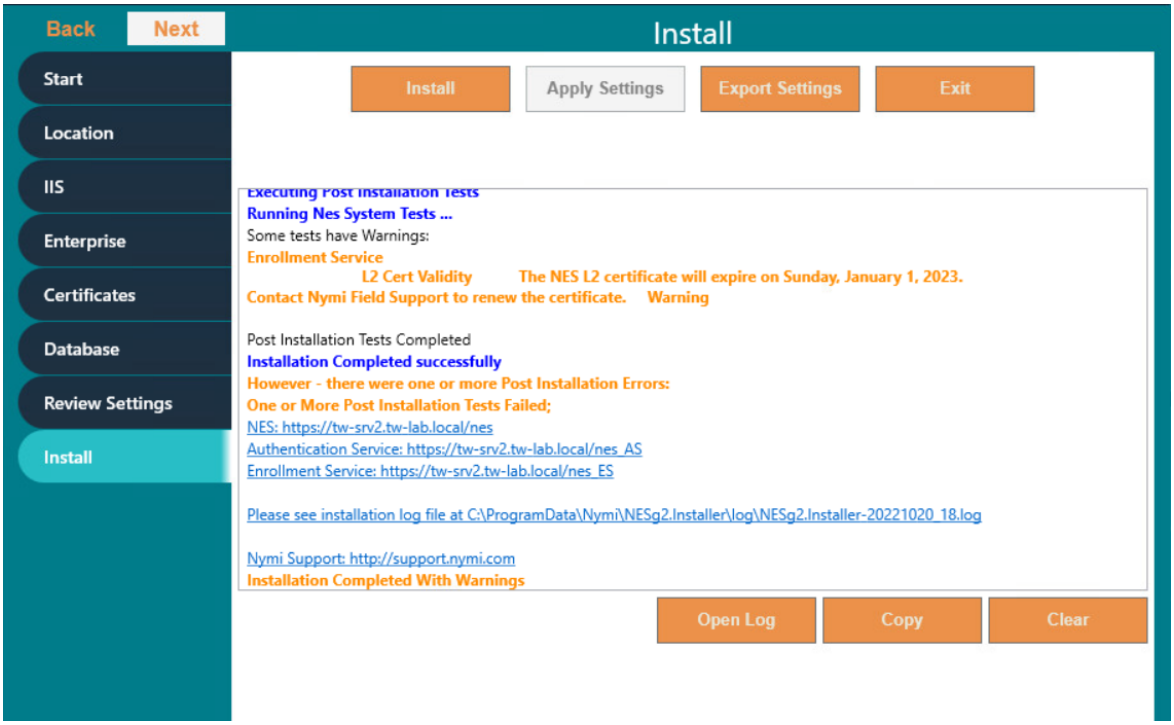


Figure 46. Install NES page in **NES Setup** wizard

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

9. In the left navigation pane, click **Review Settings**. The parameters for the NES installation are displayed for final review. Click **Test** to verify the configuration. Review the test results and address any errors if applicable.

4.3.2.1 Deploying the NES URL to User Terminals by using group policies

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

Before you begin

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

About this task

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

Procedure

1. On a Domain Controller, open the **Group Policy Management** panel.

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

       The group appears in the Security Filter section.
8. On the **Setting** tab, right-click **Computer Configuration**, and then select **Edit**.
9. Expand **Computer Configuration > Preferences > Windows Settings**.
10. Right-click **Registry**, and then select **New > Registry Item**.

    The **New Registry Properties** window appears.
11. From the **Action** list, select **Create**.
12. From the **Hive** list, leave the default value **HKEY_LOCAL_MACHINE**.
13. In the **Key Path** field, type `SOFTWARE\Nymi\NES`.
14. In the **Value name** 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. The FQDN consists of the `<hostname>.<domain>`. You can also find the FQDN by going to the terminal where NES was deployed and viewing the properties of the system. The `nes_server` is the **Full computer name**.
    - `NES_service_name` is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory.

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

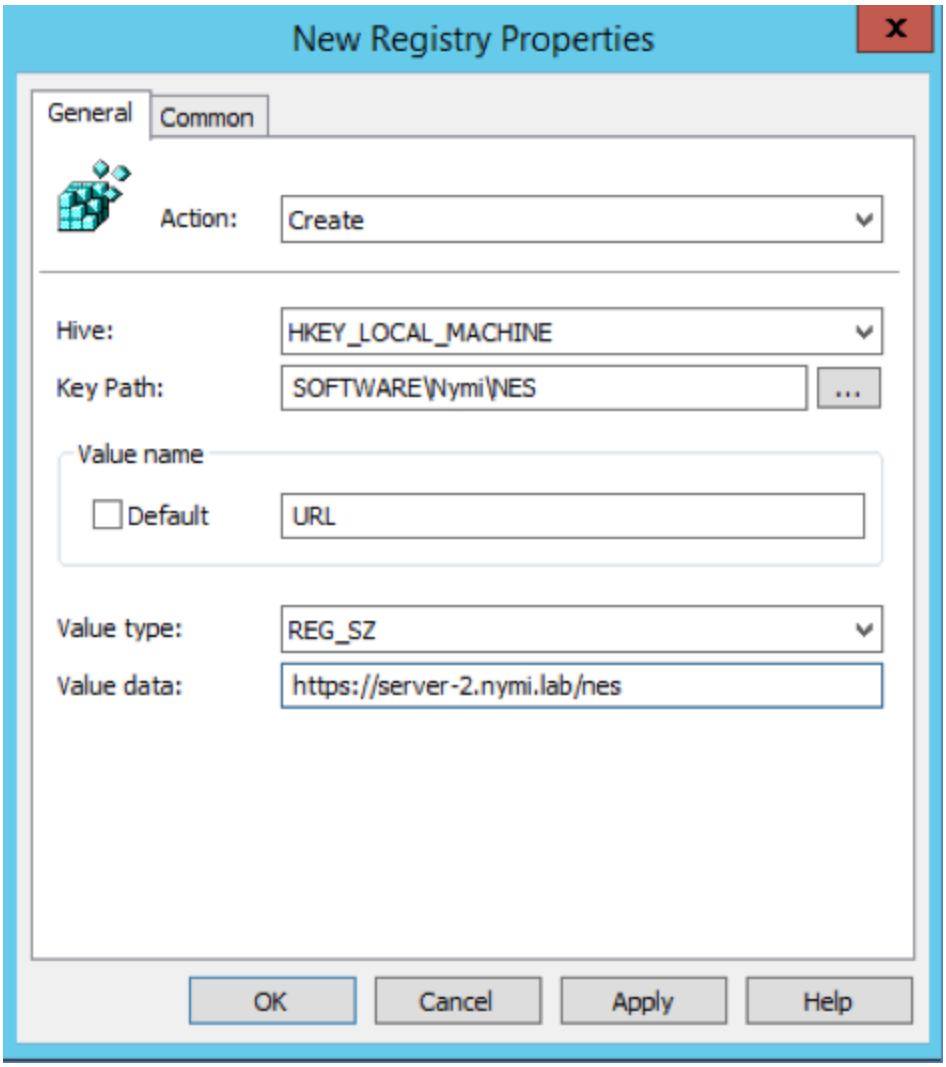


Figure 47. URL properties page

17. Click **OK**.

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

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

Before you begin

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

About this task

Create a group policy object to update the registry.

Procedure

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

The group appears in the Security Filter section.

8. On the **Setting** tab, right-click **Computer Configuration**, and then select **Edit**.
9. Expand **Computer Configuration > Preferences > Windows Settings**.
10. Right-click **Registry**, and then select **New > Registry Item**.

    The **New Registry Properties** window appears.
11. From the **Action** list, select **Create**.
12. From the **Hive** list, leave the default value **HKEY_LOCAL_MACHINE**.
13. In the **Key Path** field, type `SOFTWARE\Nymi\NES`.
14. In the **Value name** 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 that connects the Nymi Band Application to the Nymi Agent. You can choose any name for this mapping, but it is recommended that you specify a name that is descriptive.

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

4.3.3 Saving the NES Configuration

The NES Setup wizard provides you with the ability to save the NES configuration to a file.

About this task

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

> **Note:** For HA deployments, you must save the configuration of the first NES server to a file.

Procedure

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

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

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

    b. In the **Encryption** section, select one of the following options:

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

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

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

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

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

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

- Click **OK**.

c. Click **OK**.

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

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

You can configure additional NES server with the `.ninst` file from the command line or with the NES Setup wizard.

4.3.4.1 Configuring NES Silently from the Command Line

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

Before you begin

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

- Log into your machine with a domain user account that has local administrative privileges
- Copy and extract the installation package to the machine.
- Install .NET. The installation package contains the .NET 4.8 software and Microsoft SQL Server Express in the following directories: .NET 4.8 software: `..\NesInstaller\DotNetFX48\`. The .NET installation may require you to restart your computer.
- Install SQL Express if you do not have an existing MS SQL Server to store the NES database. The installation package contains Microsoft SQL Server Express 2019 in the following location: `..\PreRequisites\SqlExpress` During the SQL installation, accept all defaults. The installation process creates all Microsoft SQL Server users automatically. On the Database Engine Configuration screen, add additional users that require access to the audit reports in the SQL database.
- 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 provide you with information about the new entries.

About this task

To install NES using the silent installer:

Procedure

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

   where:

   - `path_to_fullchain_cert` is the absolute or relative path to the Nymi-provided fullchain PFX certificate file.
   - `cert_file` 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:\Program Data\Nymi\NesCmdinstall\log` directory. The installation process provides output to the screen as well as installation log files.

4.3.4.2 Configuring NES With a Configure File in the NES Setup Wizard

Perform the following steps to install Nymi Enterprise Server (NES) with the NES Setup Wizard and load the configuration values defined in an `.ninst` file.

About this task

Procedure

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

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

   If the value does not match:

   a. Click **Edit**, and then copy and paste the value from the first NES 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 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 the requests, and not off-loaded.

About this task

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

Procedure

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

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

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

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

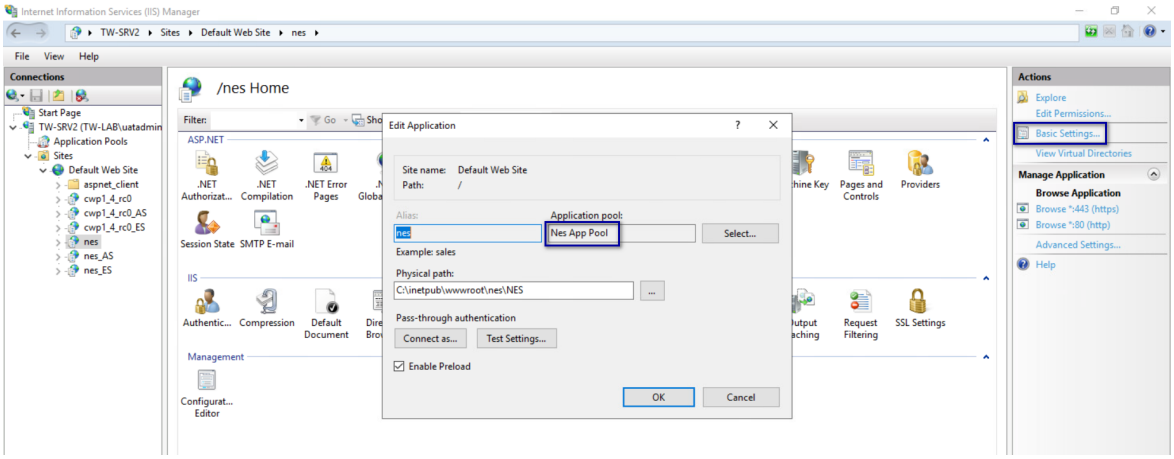


Figure 48. Edit Application window

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

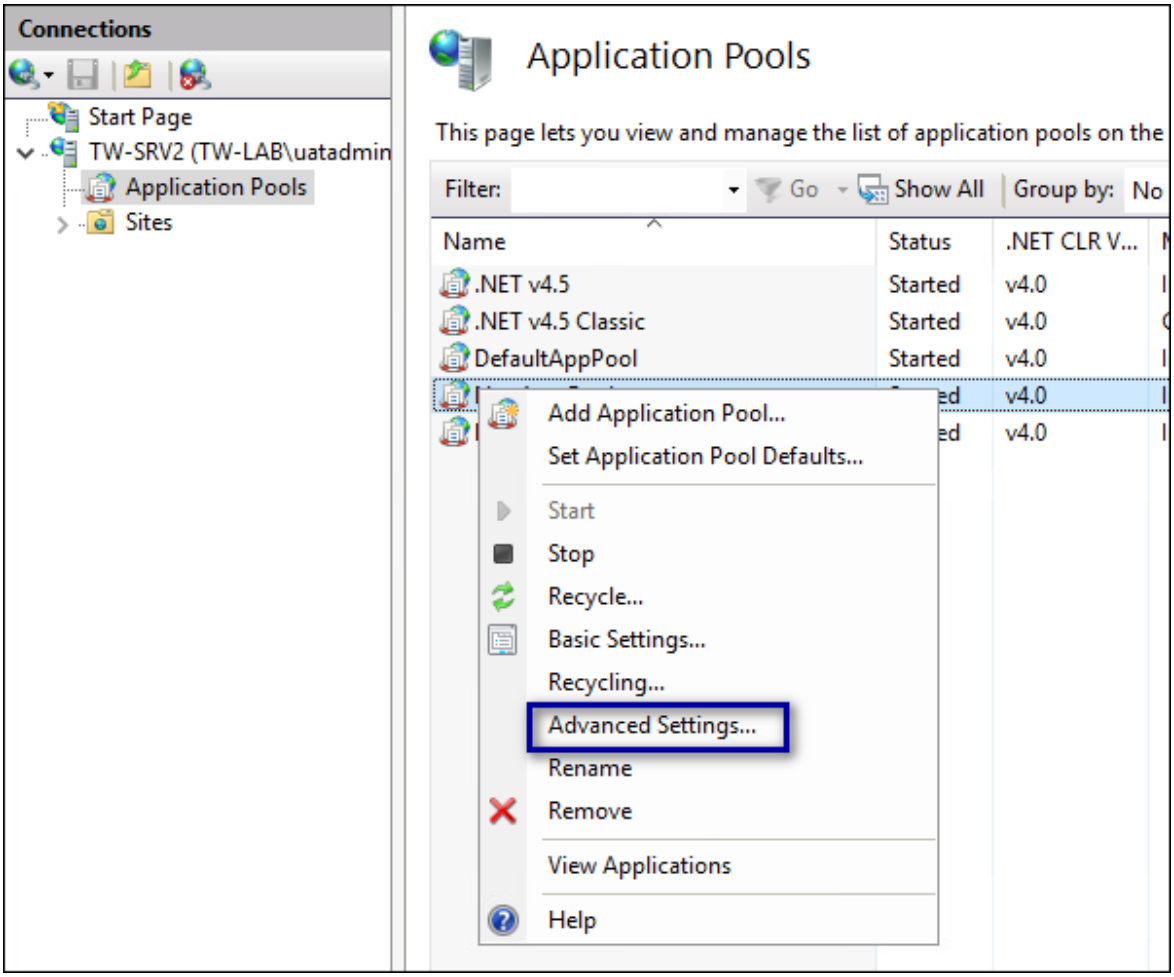


Figure 49. Advanced Settings menu option

3. In the **Advanced Settings** window, perform the following actions.

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

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

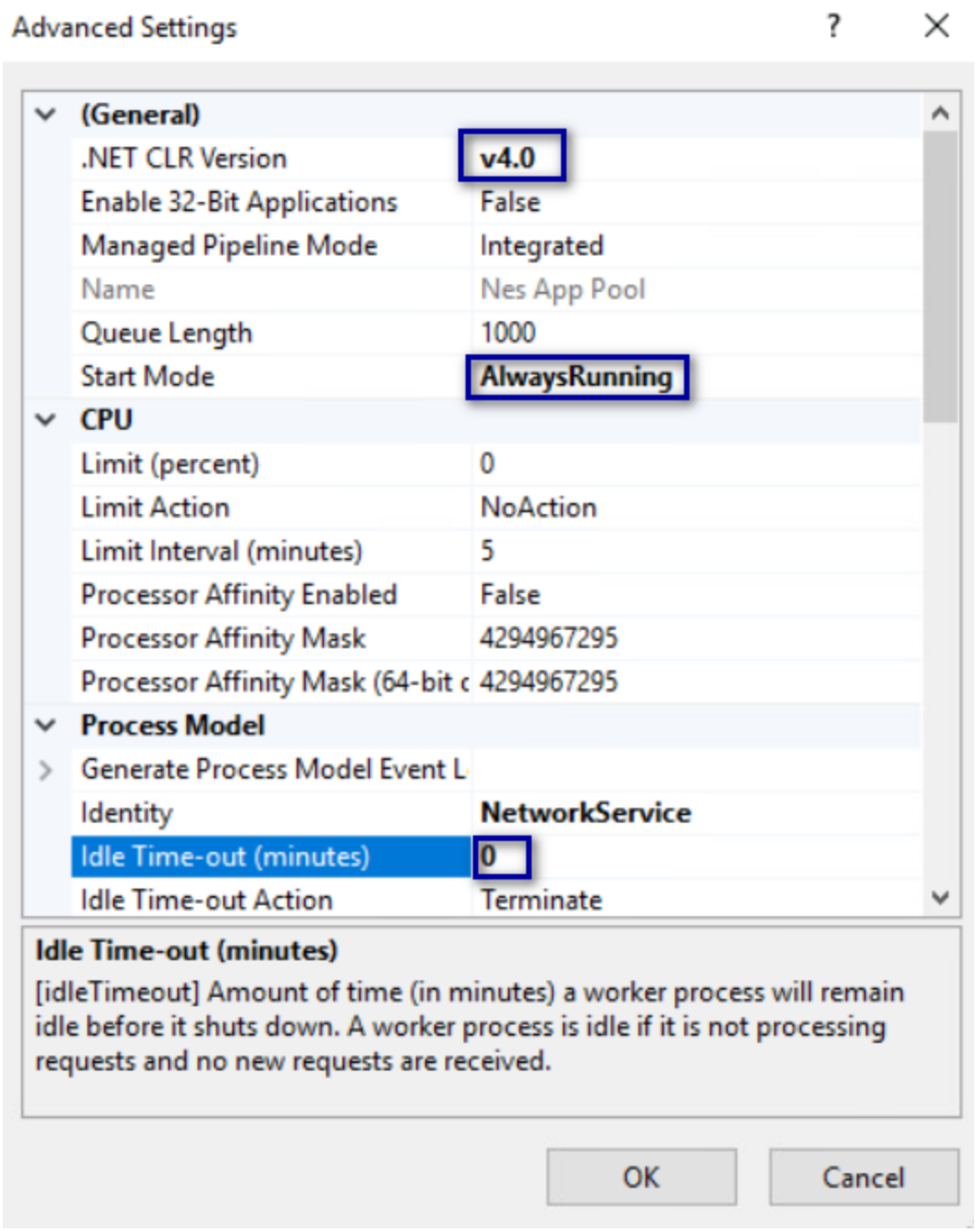


Figure 50. Advanced Settings window

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

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

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

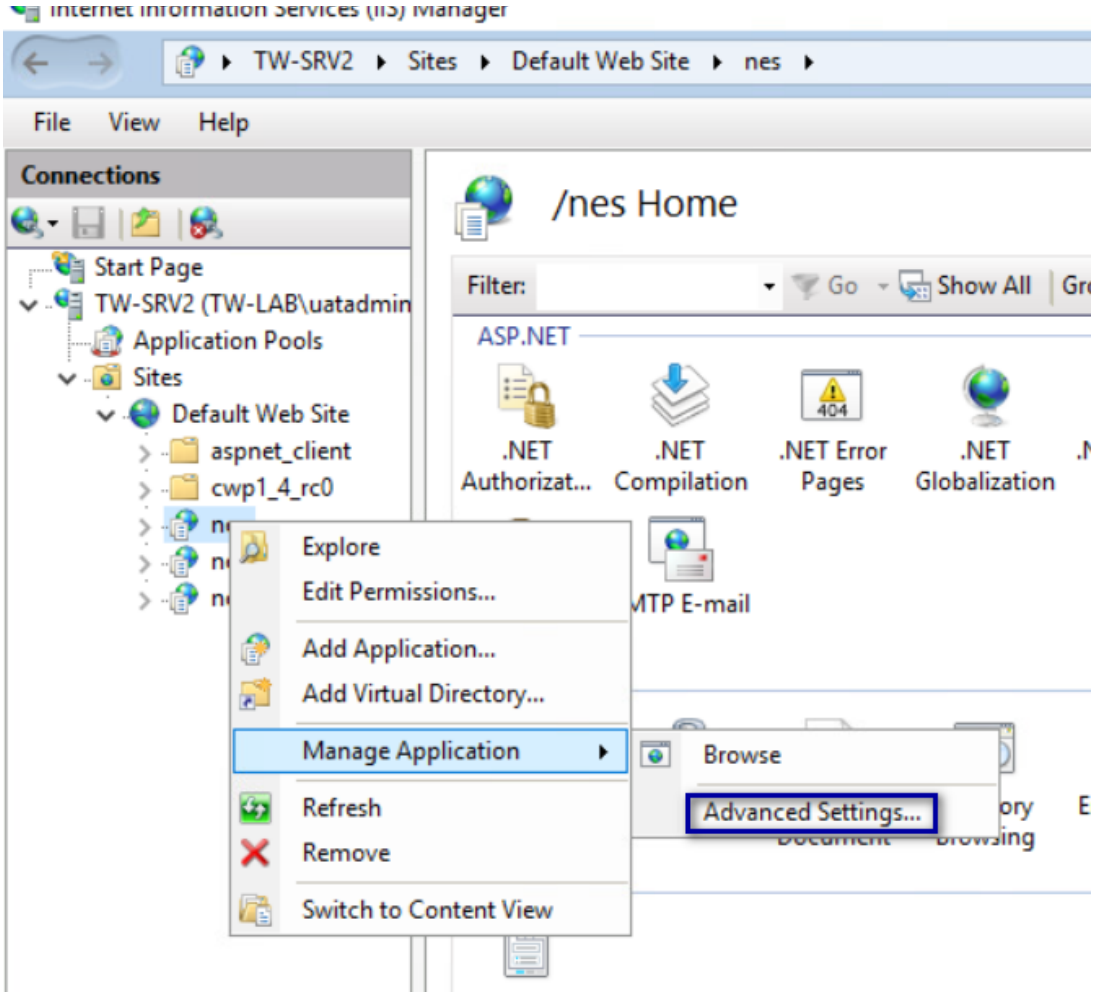


Figure 51. Advanced Settings option

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

    c. Click **OK**.

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

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

    f. Click **OK**.

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

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

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

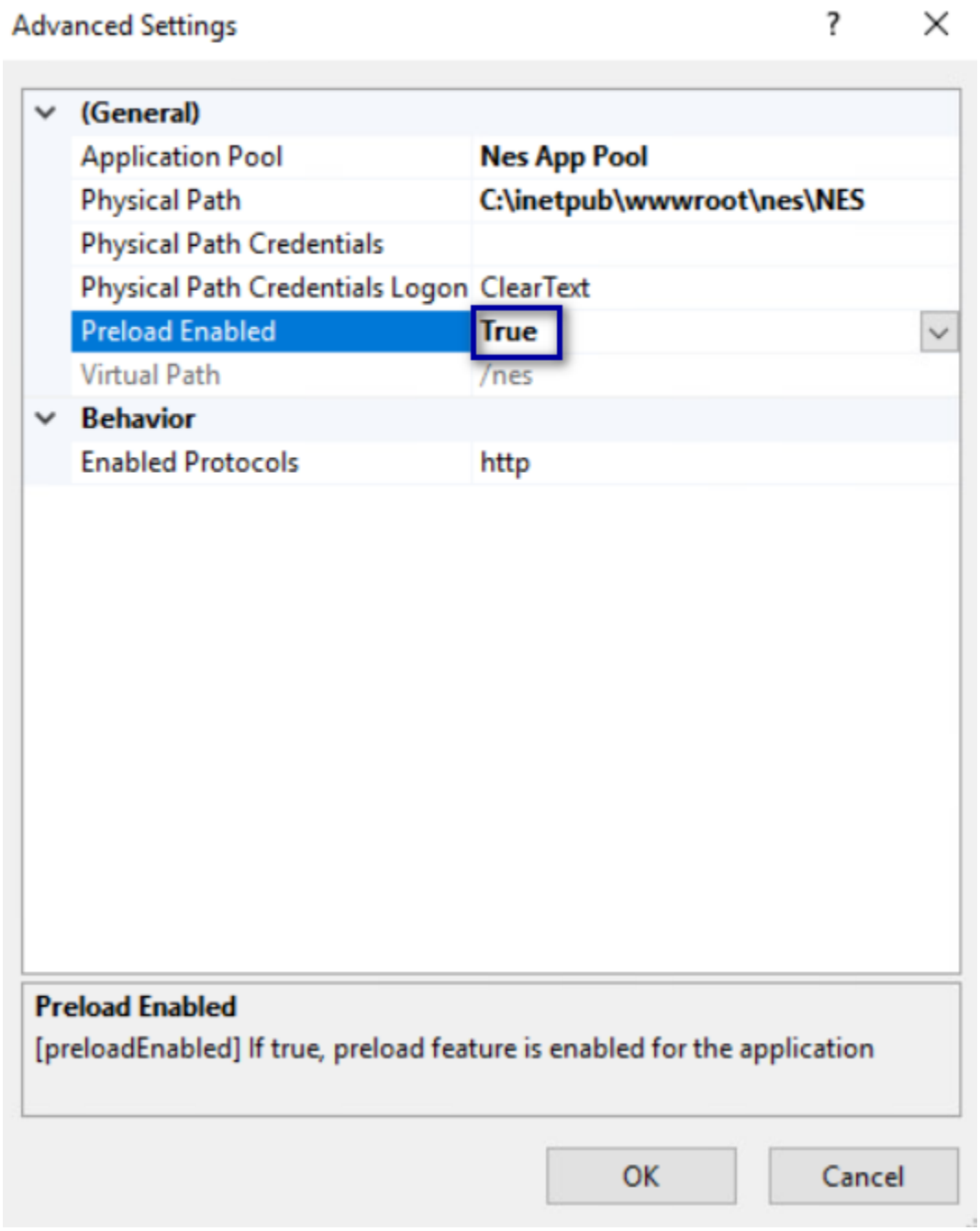


Figure 52. Advanced Settings window

i. Click **OK**.

5. In the **Connection** 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.

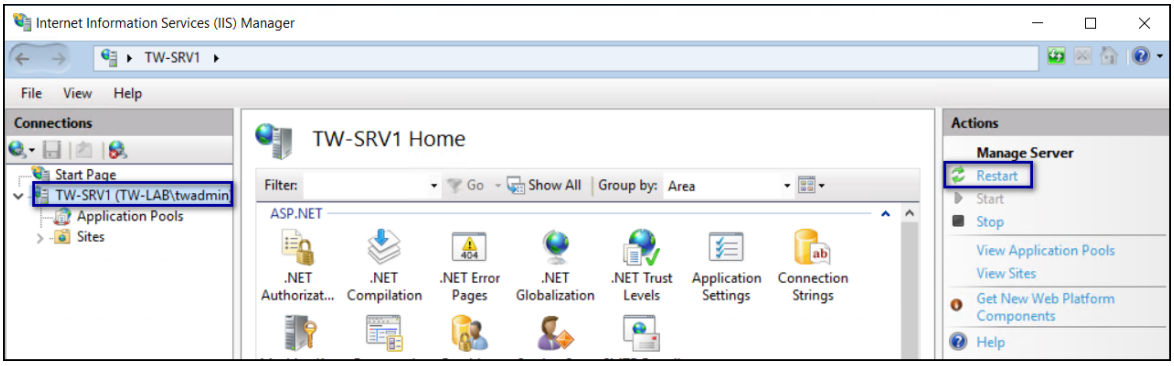


Figure 53. Restart IIS

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.

About this task

Procedure

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

depending on the NES configuration, where:

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

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

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

2. On the **Sign in** window, type the credentials of a user that is a member of the NES Administrators group, and then click **Sign In**.
3. On the main menu, click **About**.

   The **System Diagnostics** page appears.
4. Click **View Full System Diagnostics**.

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

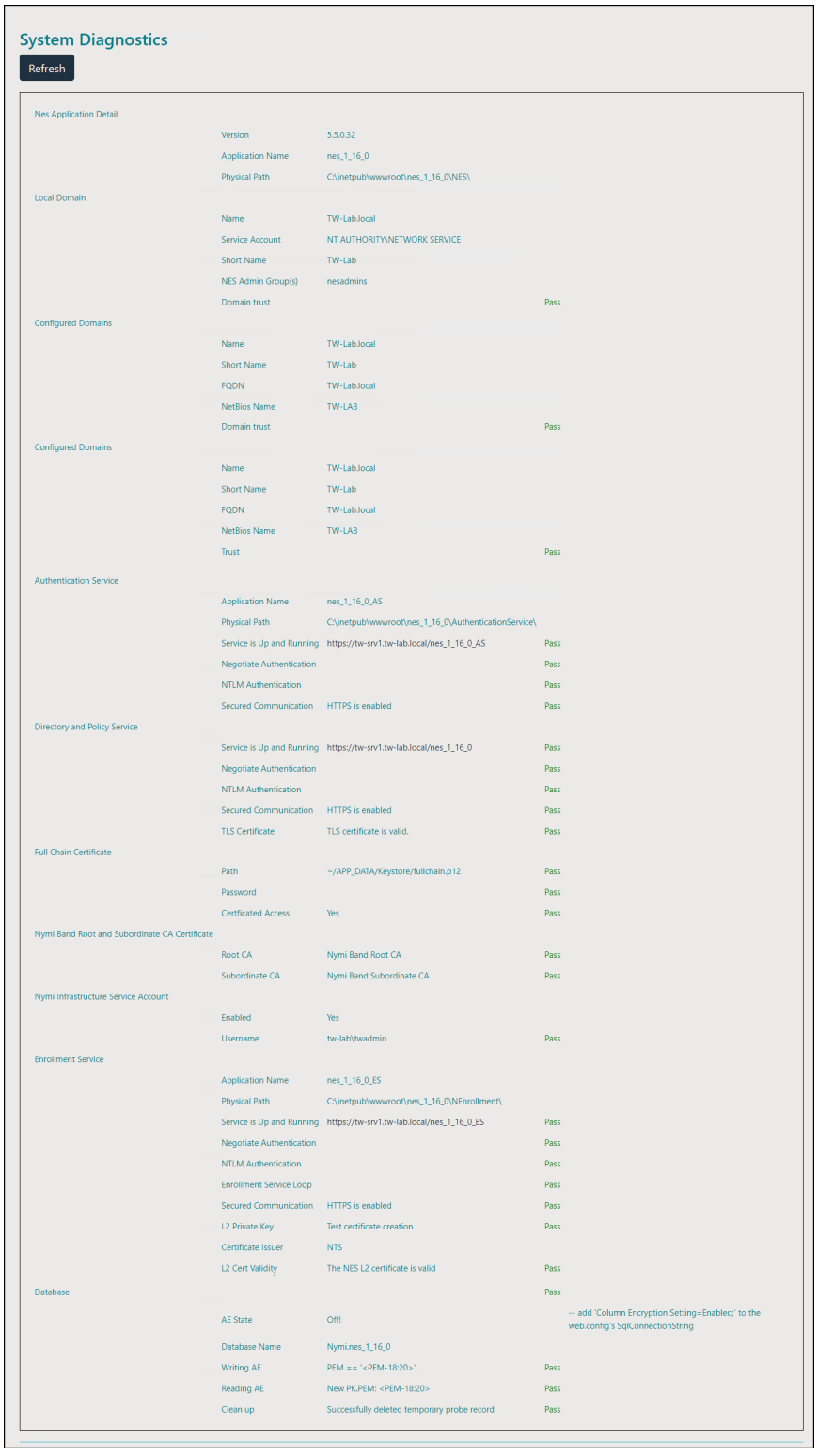


Figure 54. System Diagnostic Tests

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

What to do next

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

4.6 Configuring NES to support Nymi Lock Control

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

About this task

Procedure

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. From the **Lock Control** section, perform the one of the following actions to enable or disable Nymi Lock Control:
   - Select the **Enable Nymi Lock Control** option to display the following features. These features cannot be enabled unless **Enable Nymi Lock Control** is selected. The Nymi Band Application creates security settings during enrollment.
     - **Lock When Away**
     - **Unlock When Present**
     - **Keep Unlocked when Present**
   - Leave the option cleared to prevent users from unlocking their terminals with Nymi Lock Control.

> **Note:** Edit the `nbe.toml` file to define close proximity for Nymi Lock Control. Refer to Editing the nbe.toml File.

The following settings are available when Nymi Lock Control is enabled:

a. The **Lock When Away** option provides you with the ability to lock the terminal when the user moves away.

   - Select the option to configure Nymi Lock Control to lock 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 for at least 30 seconds. When the Nymi Band is out of range, a 10 second timer appears on the desktop. If the Nymi Band does not return within close range of the user terminal, the terminal will lock.

   - Clear the option to prevent Nymi Lock Control from locking the user terminal when the Nymi Band is not in close proximity of the user terminal.

     > **Note:** If the Nymi Band deauthenticates, the user terminal locks regardless of how you configure the **Lock When Away** option.

b. The **Unlock When Present** option provides you with the ability to define how close the Nymi Band must be to the terminal to allow the user to unlock the terminal with the Nymi Band:

   - Select the option to prevent 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.
   - Clear the option to allow a user to unlock the terminal by pressing the **Enter** key or space bar on the keyboard when the Nymi Band is within Bluetooth range, but not in close proximity of the user terminal.

c. The **Keep Unlocked when Present** option provides you with the ability to define how the Nymi Band interacts with operating system screen timeouts or sleep settings that lock the terminal:

   - Select the option to override any system screen timeouts or sleep settings, and keep the user terminal unlocked as long as the Nymi Band is present and authenticated.
   - Clear the option to prevent Nymi Lock Control from overriding any system screen timeouts or sleep settings.

5. Click **Save**.

Results

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

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

4.7 Hardening the NES Keystore

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

About this task

Hardening Nymi Enterprise Server(NES) can be based on enterprise IT policy or any industry standard hardening guideline. Nymi has taken steps to harden IIS according to the CIS Microsoft IIS 10 Benchmarks from the Centre for Internet Security (CIS).

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

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

Procedure

1. Edit the `C:\inetpub\wwwroot\NES\NEnrollment\web.config` file, and perform the following steps:

    a. Search for the string **SqlConnectionString**.

b. Add `Column Encryption Setting=Enabled` within the value attribute tags, as shown in the following example:

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

c. Save the file.

2. Edit the `C:\inetpub\wwwroot\NES\NES\web.config` file, and perform the following steps:

a. Search for the string **SqlConnectionString**.

b. Add `Column Encryption Setting=Enabled;` within the attribute tags, as shown in the following example:

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

c. Save the file.

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

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

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

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

7. Expand **Databases > Nymi.NES > Security > Always Encrypted Keys**. Right click **Column Master Key**, and then select **New Column Master Key**, as shown in the following figure.

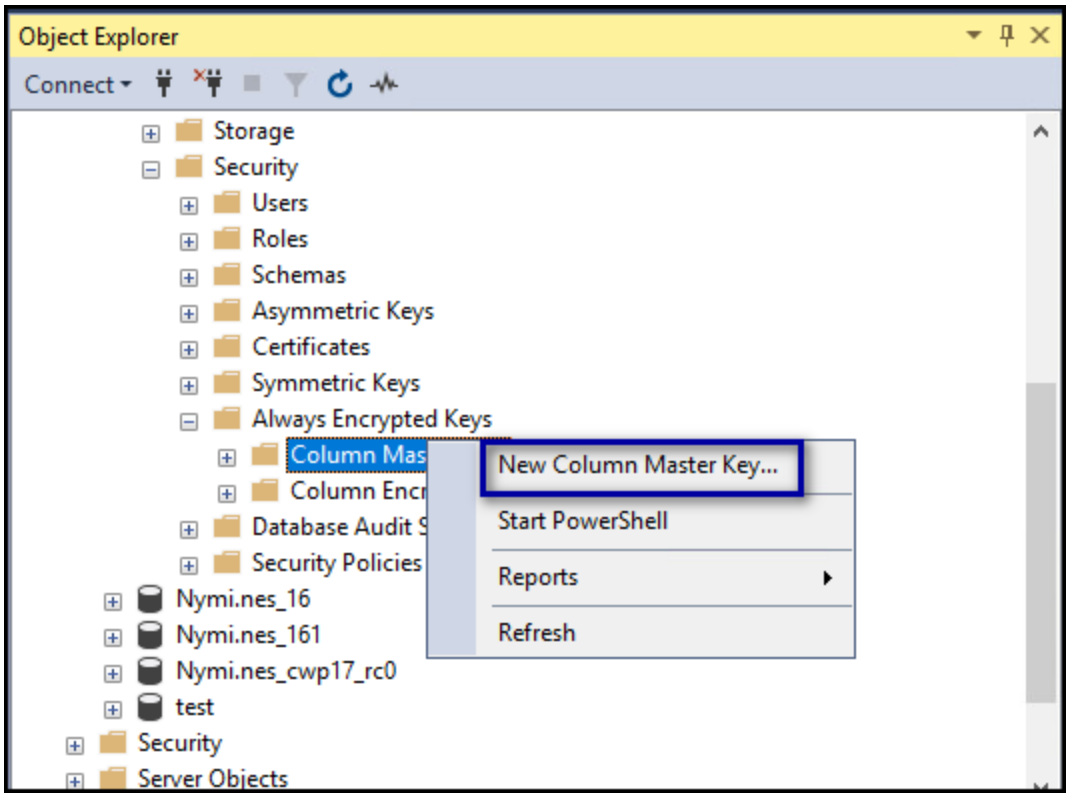


Figure 55. New Column Master Key option

8. On the **New Column Master Key** window, perform the following actions:

    a. In the **Name** field, type a name for the key.

    For example, `CMK_LocalMachine`.

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

    The following figure shows the **New Column Master Key** page.

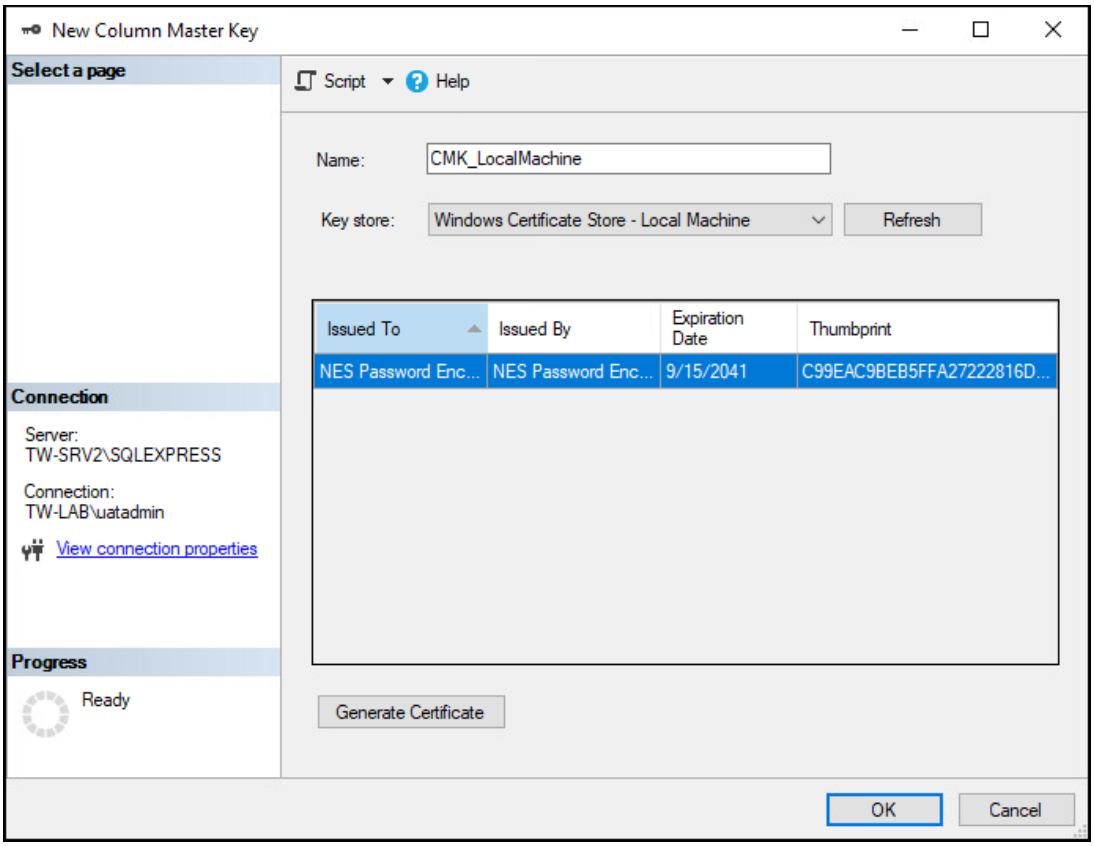


Figure 56. New Column Master Key page

c. Click **Generate Certificate**.

The table refreshes with the Always Encrypted Certificate, as shown in the following figure.

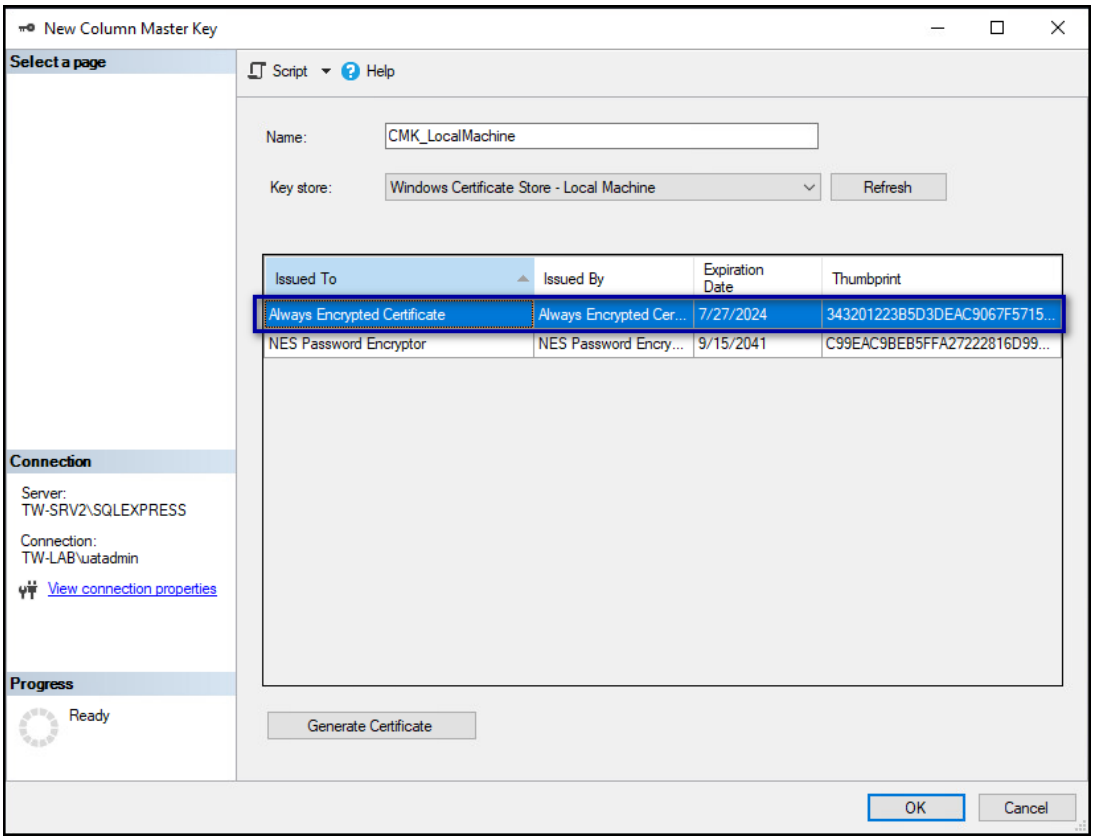


Figure 57. Always Encrypted Certificate

d. Click **OK**.

9. While in **Nymi.NES > Security > Always Encrypted Keys**, right-click **Column Encryption Keys**, and then select **New Column Encryption Key**, as shown in the following figure.

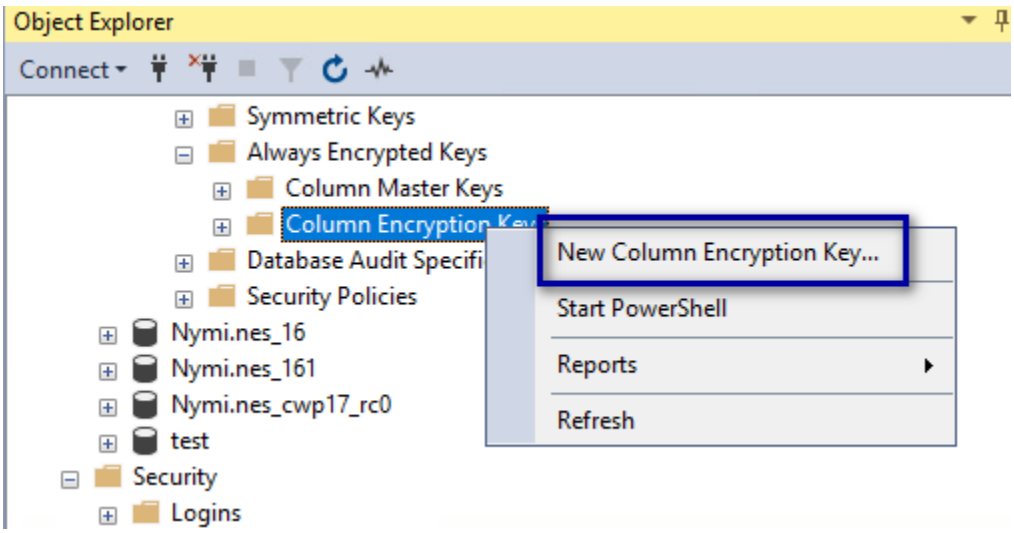


Figure 58. New Column Encryption Key option

10. On the **New Column Encryption Key** page, perform the following actions:

    a. In the **Name** field, type a name for the key.

       For example, `CEK_LocalMachine`.

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

       For example, `CMK_LocalMachine`.

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

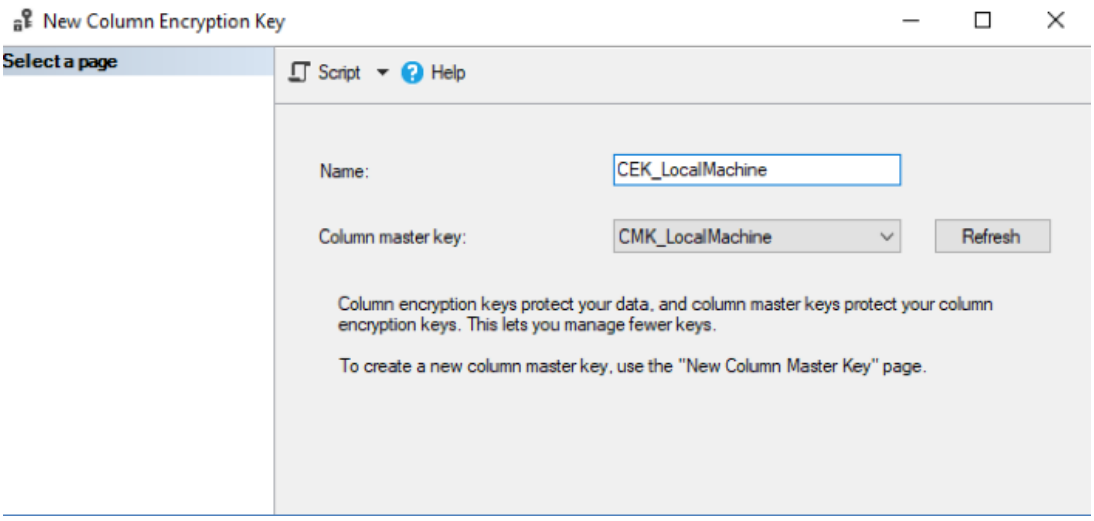


Figure 59. New Column Encryption Key page

    c. Click **OK**.

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

12. Under tables, right-click **nub.PrivateKeyStore**, and then select **Encrypt Columns**, as shown in the following figure.

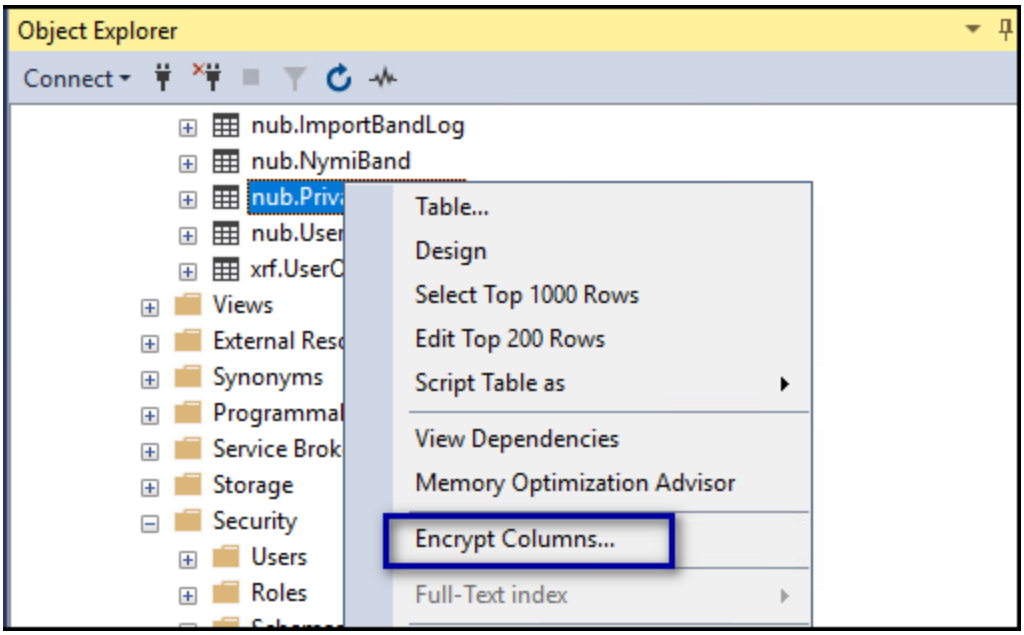


Figure 60. Encrypt Columns option

The **Always encrypted** wizard opens.

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

14. On the **Column Selection** page, perform the following actions:

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

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

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

    The following figure shows the **Column Selection** page.

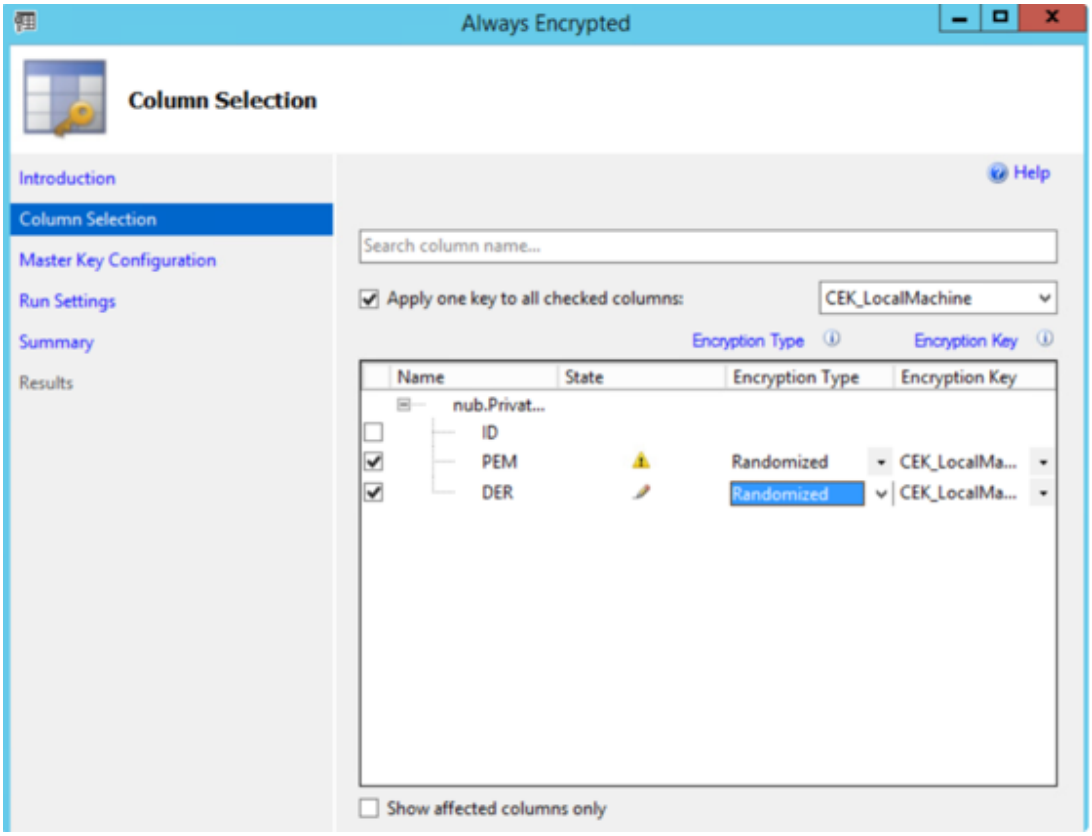


Figure 61. Column Selection page

d. Click **Next**.

15. On the **Master Key Configuration** page, click **Next**.

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

17. On the **Summary** page, review the results, and then click **Finish**. Click **Close**.

18. Under tables, right-click **nub.NymiBand**, and then select **Encrypt Columns**.

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

20. On the **Column Selection** page, perform the following actions:

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

    b. In the table, expand **nub.NymiBand**, scroll down and select **Adv_key_1** and then from the **Encryption Type** list, select **Randomized**.

The following figure provides an example of the **Encrypted Columns** window.

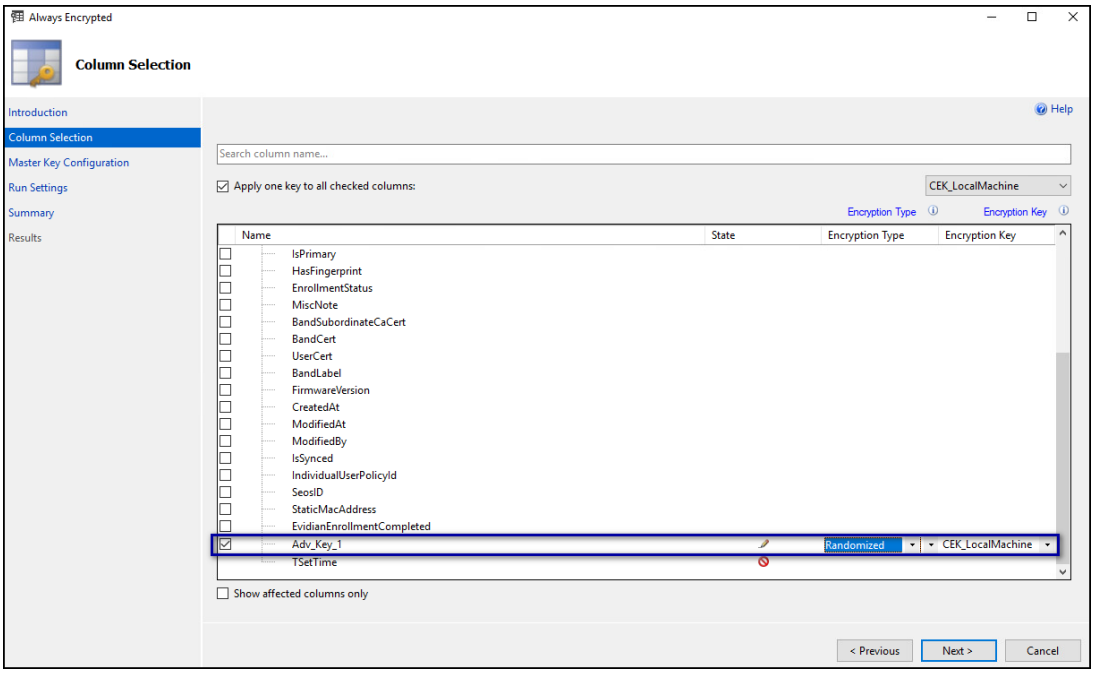


Figure 62. Encrypted Columns window

c. Click **Next**.

21. On the **Master Key Configuration** page, click **Next**.
22. On the **Run settings** page, leave the default value **Proceed to finish now**, and then click **Next**.
23. On the **Summary** page, review the results, and then click **Finish**. Click **Close**.
24. Close **SSMS**.

What to do next

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

1. Open **Manage Computer Certificates**.
2. Expand **Personal** and then select **Certificates** folder.

3. In the right pane, right-click **Always Encrypted Certificate** and then select **All Tasks > Manage Private Keys**, as shown in the following figure.

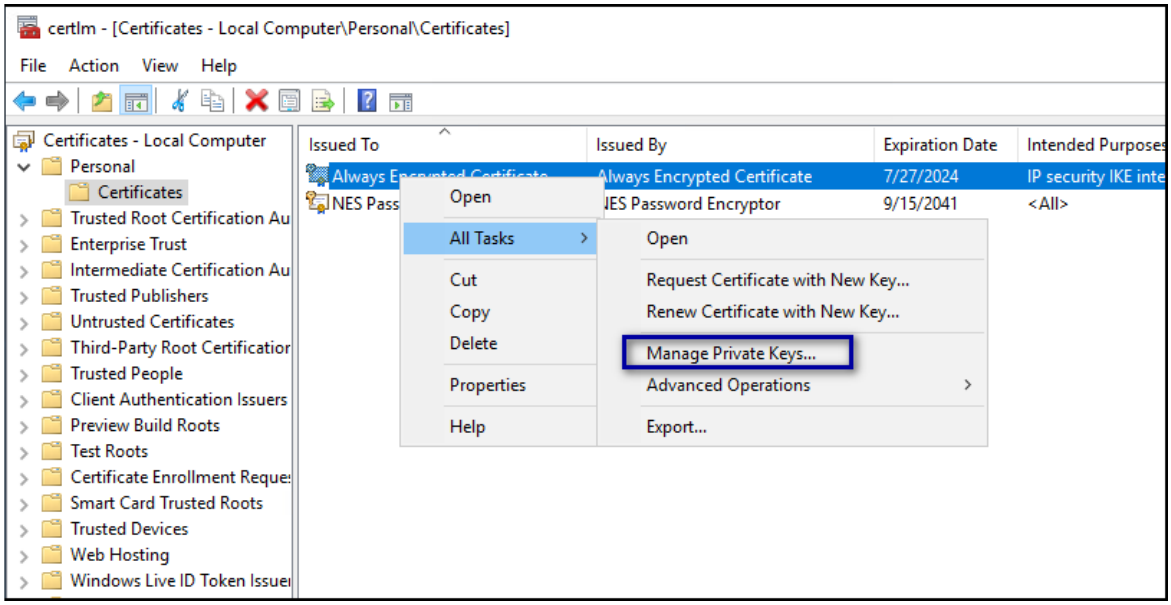


Figure 63. Manage Private Keys option

The **Permissions for Always Encrypted Certificate** window appears.

4. Click **Add**, as shown in the following figure.

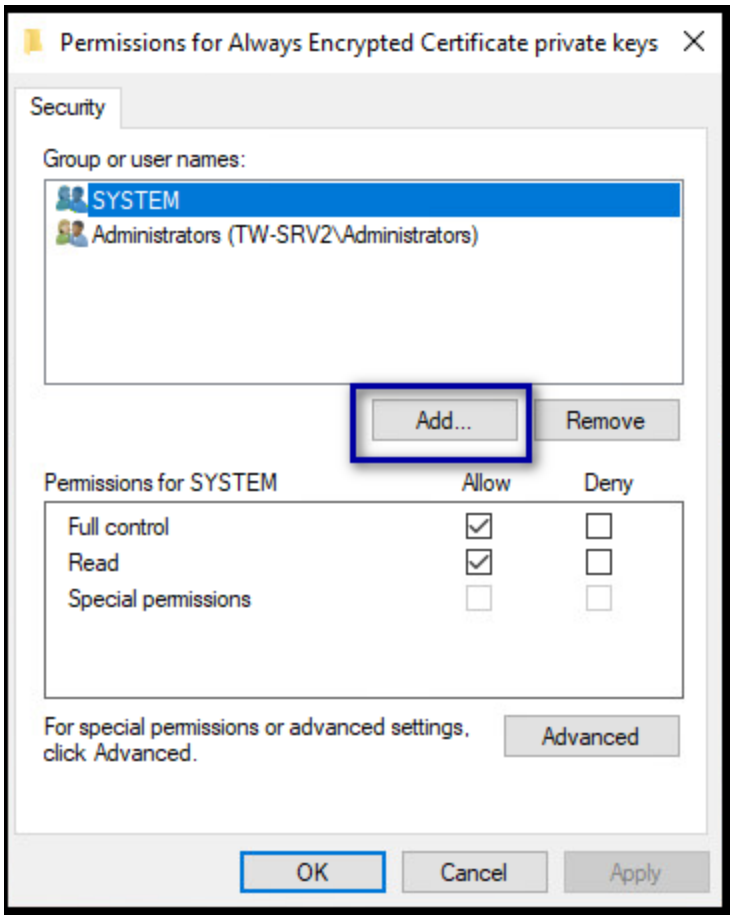
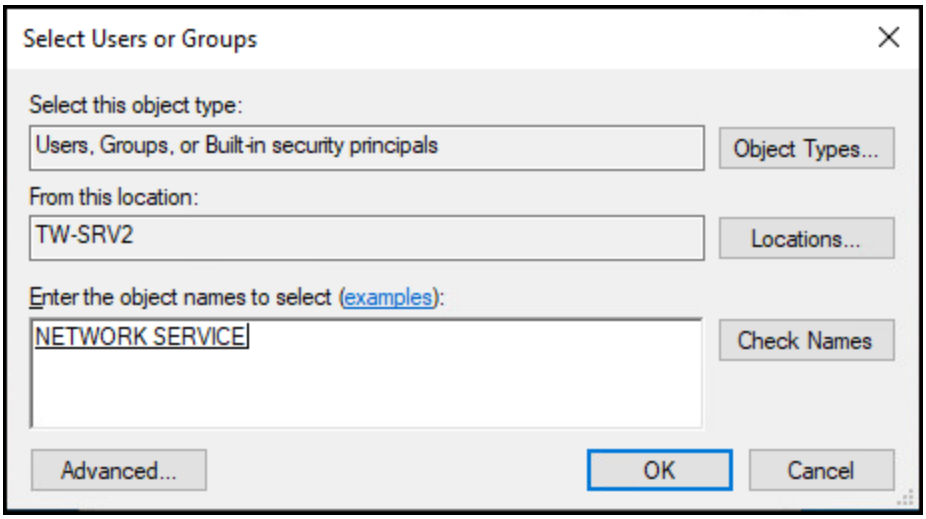


Figure 64. Add Permissions window

5. In the **Select Users, Computers, Service Accounts, or Groups** window, type the Application Pool Identity, and the select **Check Names**. The following figure provides an example of the **Select Users, Computers, Service Accounts, or Groups** window when the application identity is the network service account.



6. Click **OK**.
7. Click **OK**.
8. 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.

Procedure

1. Open SSMS by using the **Run as Administrator** option.
2. Encrypt the audit.UserCore table by performing the following steps:
    a. In **Tables**, right-click **audit.UserCore**, and then select **Encrypt Columns**, as shown in the following.

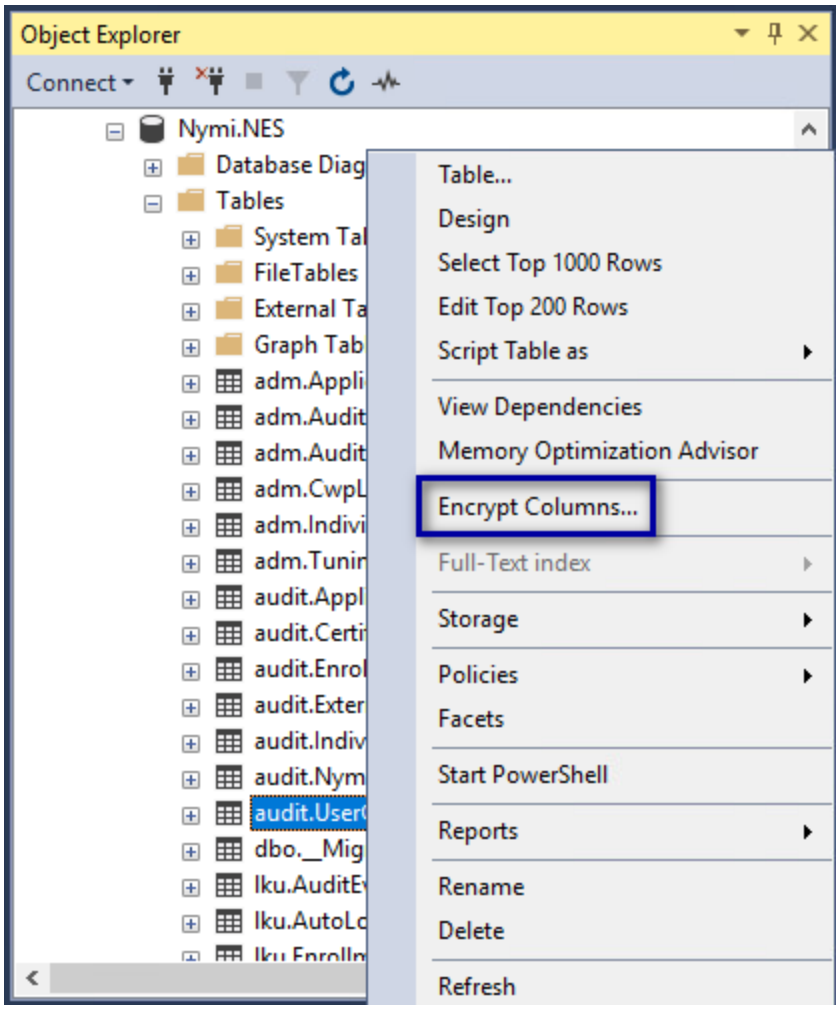


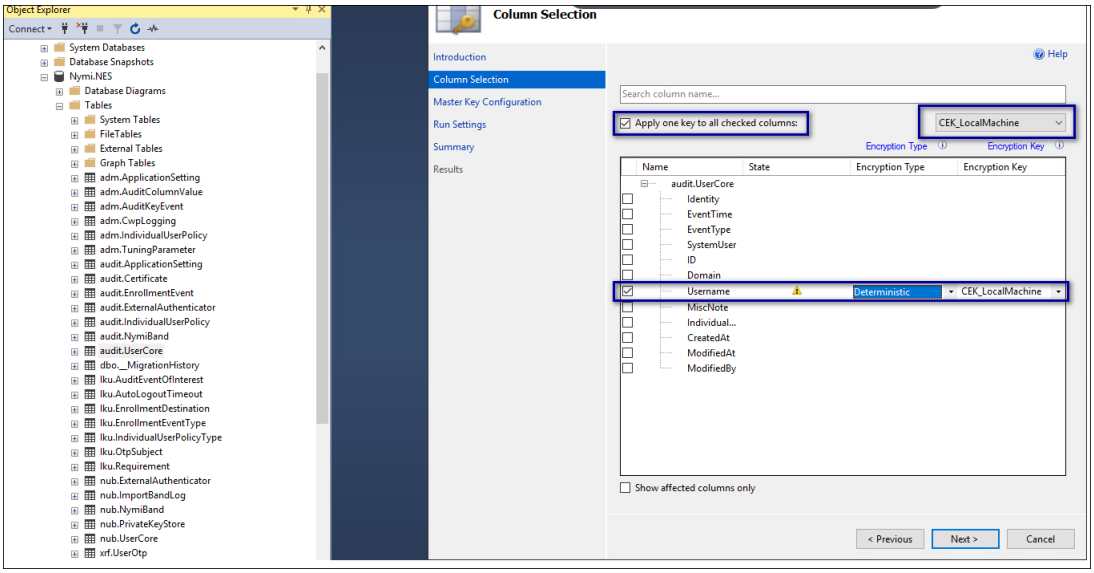
Figure 65. Encrypt Columns option

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

c. On the **Column Selection** window, enable **Apply one key to all checked columns** and ensure that **CEK_LocalMachine** appears in the list to the right.

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

   The following figure provides an example of the **Column Selection** window.



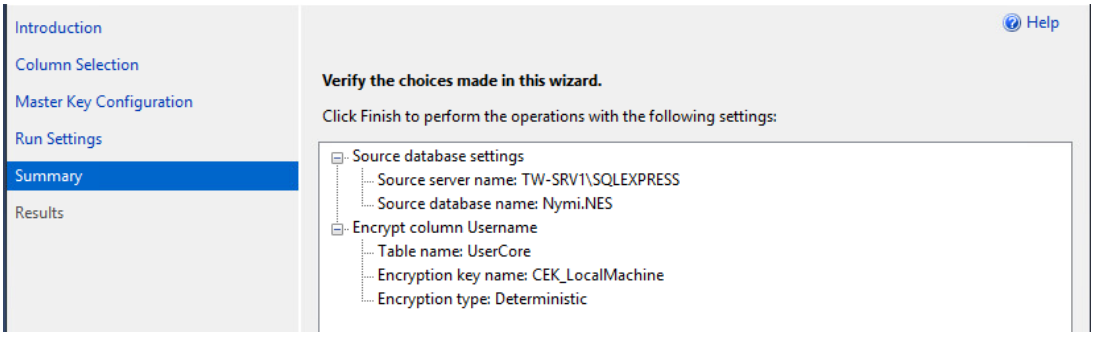
e. Click **Next**.

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

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

h. On the **Summary** page, review the results, and then click **Finish**. Click **Close**.

The following figure provides an example of the **Summary** page.



3. Encrypt the `usernames` in the `nub.UserCore` table by performing the following steps:

a. In **Tables**, right-click **nub.UserCore**, and then select **Encrypt Columns**.
b. On the **Introduction** page, click **Next**.
c. Enable **Apply one key to all checked columns** and ensure that **CEK_LocalMachine** appears in the list to the right.

d. In the **Tables**, select **username**, and then from the **Encryption Type** list, select **Deterministic**.
e. Click **Next**.
f. On the **Master Key Configuration** page, click **Next**.
g. On the **Run settings** page, leave the default setting **Proceed to finish now**, and then click **Next**.
h. On the **Summary** page, review the results, and then click **Finish**. Click **Close**.

5 Set Up a Centralized Nymi Agent

When your environment uses iOS devices, applications on RDP/Citrix session hosts, and web-based Nymi-Enabled Application(NEA)s, 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, standard Nymi Agent interface connect over plain text websocket.
- Nymi WebAPI interface. By default Nymi WebAPI interface is disabled.

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

5.1 Importing 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.

Before you begin

Install the Root CA on the following machines:

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

About this task

While logged into the user terminal as a local administrator, use the **certlm** application to import the root CA certificate into the Trusted Root Certification Authorities store.

Procedure

1. In the **certlm** window, right-click **Trusted Root Certification Authorities**, and then select **All Tasks > Import**.
2. On the **Welcome to the Certificate Import Wizard** screen, click **Next**.
3. On the **File to Import** screen, click **Browse**, navigate to the folder that contains the certificate file, select the file, and then click **Open**.
4. On the **File to Import** screen, click **Next**.
5. 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**.
6. On the **Completing the Certificate Import Wizard** screen, click **Finish**.

5.2 Installing/Updating Centralized Nymi Agent

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

About this task

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

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the `Nymi SDK` distribution package.
3. From the `..\nymi-sdk\windows\setup`folder, 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 option to make **Nymi Bluetooth Endpoint** unavailable.

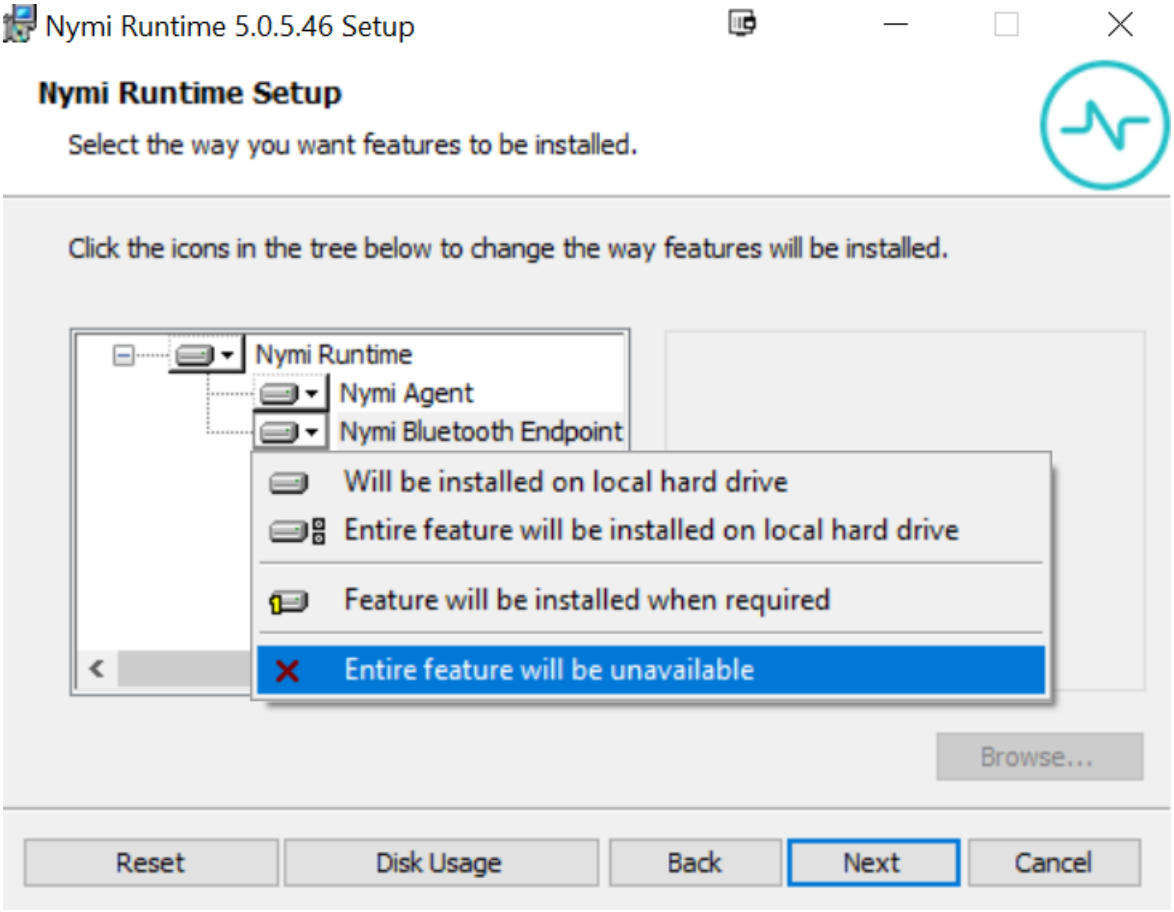


Figure 66. Nymi Bluetooth Endpoint feature will be unavailable

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

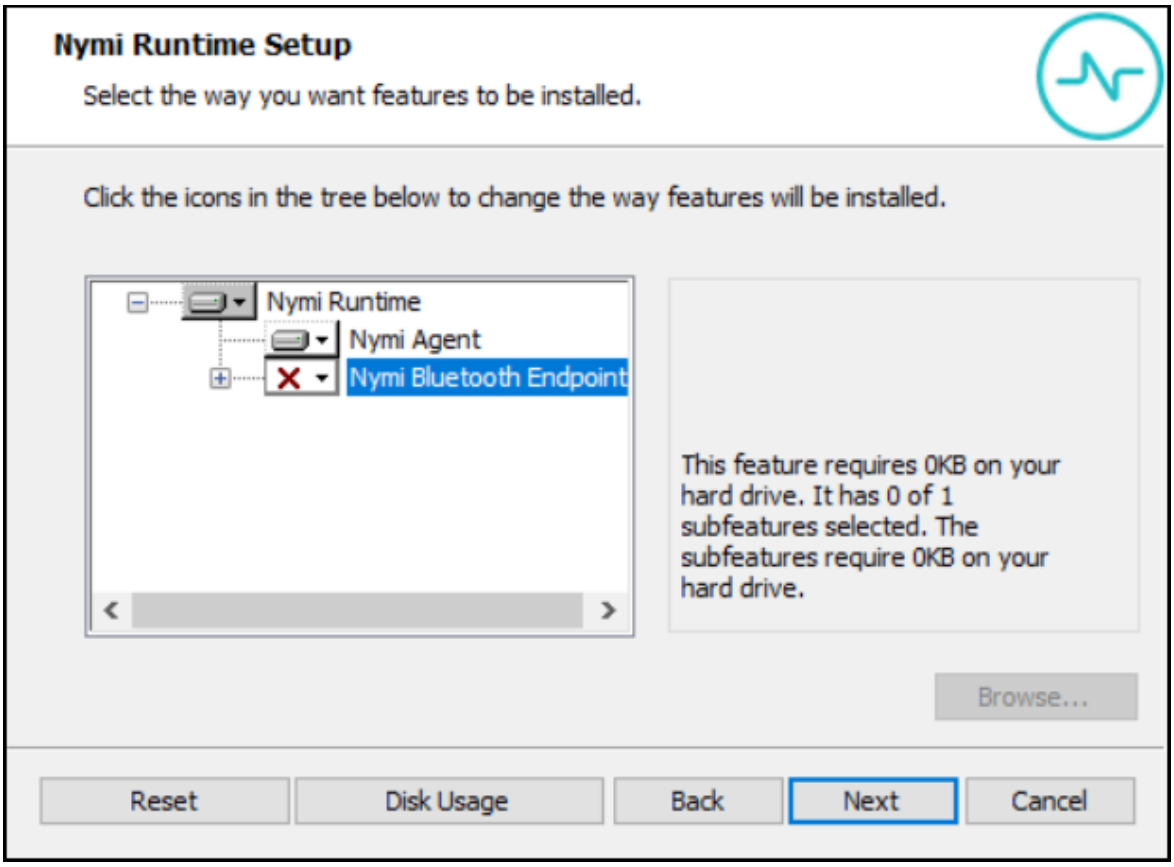


Figure 67. Nymi Bluetooth Endpoint feature is not available

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.

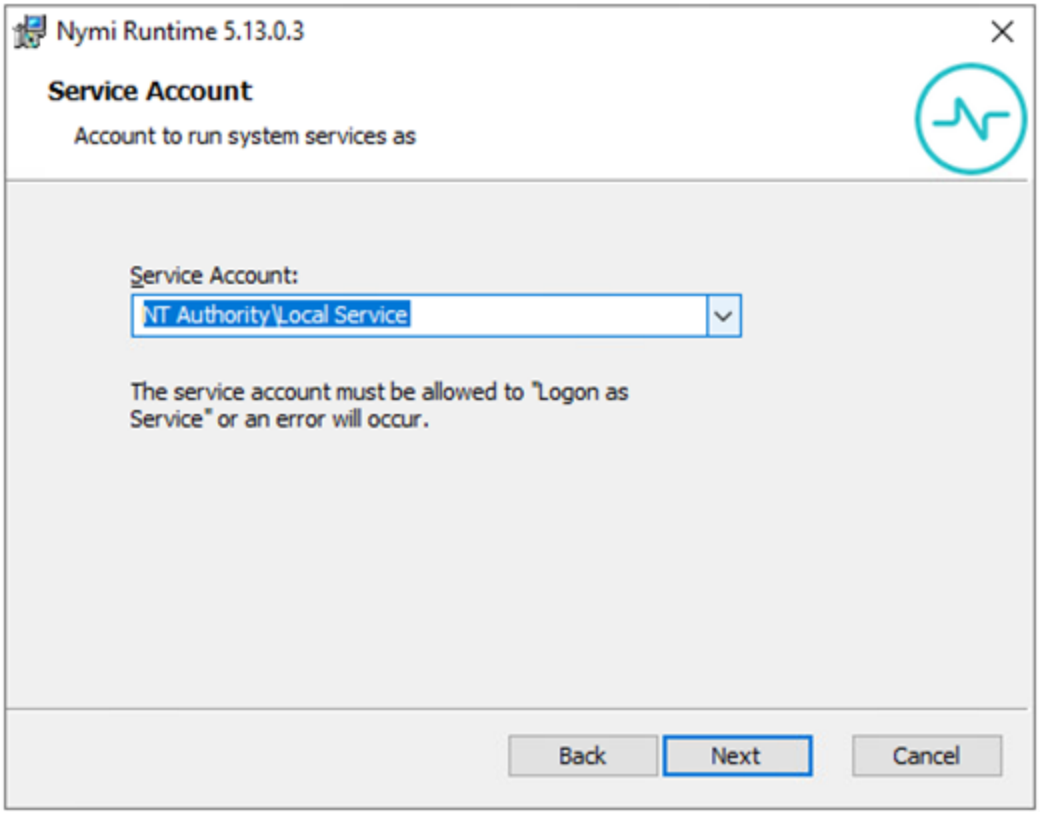


Figure 68. Nymi Runtime Service Account window

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.

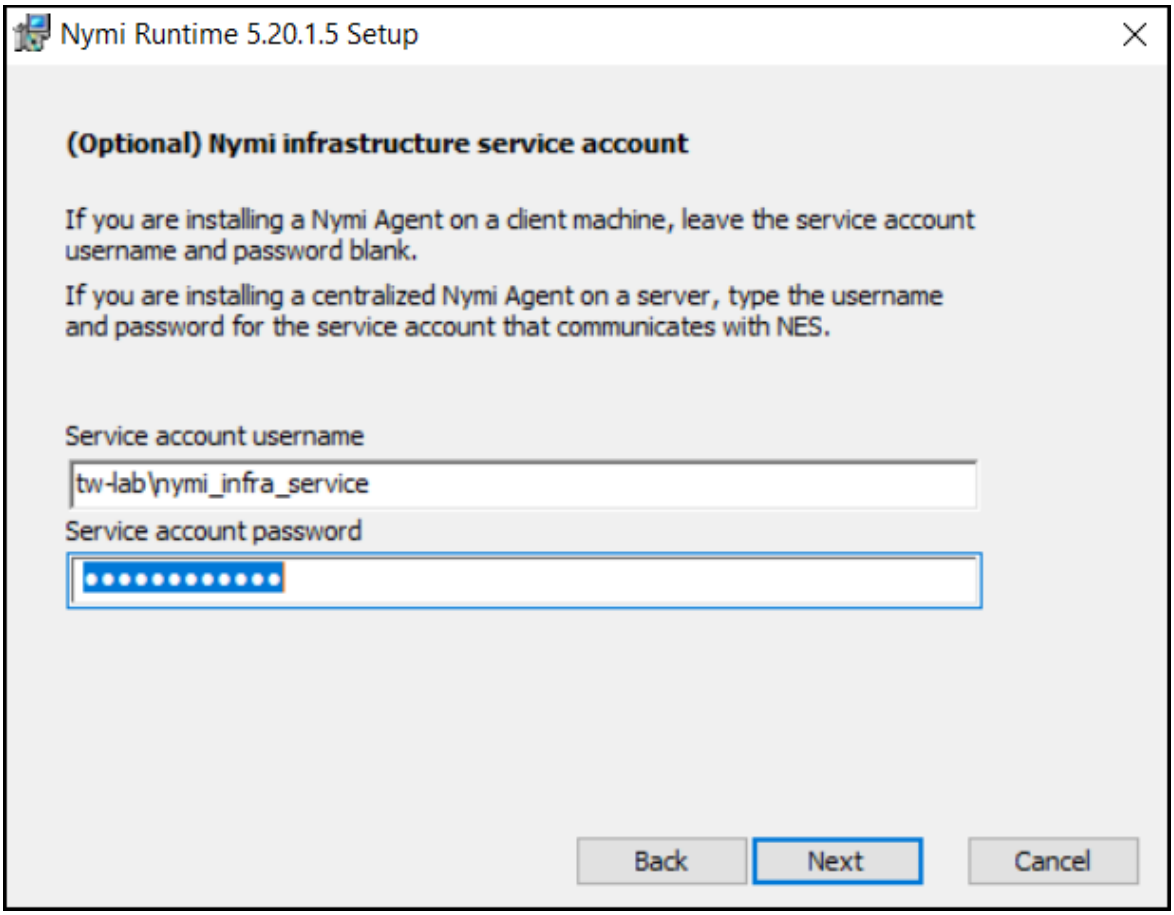


Figure 69. Nymi Infrastructure Service Account window

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**.

5.3 Configuring 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.

About this task

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.

Procedure

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`. The following table summarizes the available parameter setting 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.

`log_level = "warn"`	**Section Name:** [agent] **Description** Required. Defines the debug logging level. Change the value when instructed by Nymi. Support values include: ◦ error—to log only errors ◦ warn—to log both errors and warnings ◦ info—to log errors, warnings, and activity ◦ debug—to log everything including debugging information The default value is `warn`.

`protocol`	**Section Name:** [agent] **Description:** Optional. To enable the standard Nymi Agent to use secure websocket communications, uncomment protocol and change the value to wss. Note: Requires the configuration of the `cacertfile`, `cacert`, and `keyfile` parameters in the [agent] section. For example, protocol = “wss”
`port`	**Section Name:** [agent] **Description:** 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 you use the default port number.
`cacertfile`	**Section Name:** [agent] **Description:** 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. Note: Requires the configuration of `protocol= "wss"`, `certfile` and `keyfile` parameters in the [agent] section. For example: cacertfile = “certs/LocalLabRootCA3.pem”

`certfile`	**Section Name:** [agent] **Description:** 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. Note: Requires the configuration of `protocol= "wss"`, `cacertfile`, and `keyfile` parameters in the [agent] section. For example: “certfile =”certs/tw-srv1.tw-lab.local-cert.pem”
`keyfile`	**Section Name:** [agent] **Description:** 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. Note: Requires the configuration of `protocol= "wss"`, `cacertfile`, and `certfile` parameters in the [agent] section. For example: “keyfile =”certs/tw-srv1.tw-lab.local-key.pem”
`nea_name = "NymiWebAPI"`	**Section Name:** [nes] **Description:** Required for Nymi WebAPI. Uncomment this parameter to set the NEA name for the embedded NEAWebAPI server application.
`nes_url = "https://server.name.local.com"` For example, https://myserver.name.local.com	**Section Name:** [nes] **Description:** Required for Nymi WebAPI. Uncomment and specify the host URL for the NES server. Include only the protocol and hostname portion of the URI.

`directory_service_id = "NES_DPS"`	**Section Name:** [nes] **Description:** Required for Nymi WebAPI. Uncomment and specify the instance name for NES. For example, if your NES URL is https://server.name.local.com/NES, the directory/instance name is NES. For example, `directory_service_id = "NES"`
`credentials_location = certs/`	**Section Name:** [nes] **Description** Required when you specified a Nymi Infrastructure Service Account during the Nymi Agent installation. Uncomment this line and leave the default value. 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. **Note:** The `certs` folder contains a file with the encrypted username and password for the Nymi Infrastructure Service Account.

`protocol = "wss"` or `protocol = "ws"`	**Section Name:** [webapi] **Description** Required for Nymi WebAPI. Defines the connection protocol. If your deployment does not use Nymi WebAPI, leave both lines commented out. If your deployment uses Nymi WebAPI, uncomment one of the following lines: ◦ `protocol = "wss"` To enable secure websocket connections. ◦ `protocol = "ws"` To use plain text websocket connections. **Note:** Requires the configuration of the `cacertfile`, `certfile`, and `keyfile` parameters in the [webapi] section.
`port = 443` or `port = 80`	**Section Name:** [webapi] **Description** Optional for Nymi WebAPI. Defines an alternate server port on which Nymi Agent listens for Nymi WebAPI client WebSocket connections. By default the `ws` protocol listens on 80 and the `wss` 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 `ws` protocol, uncomment `port = 80`. ◦ For the `wss` protocol, uncomment `port = 443`.

`cacertfile = "path/certfile.pem"`	**Section Name:** [webapi] **Description:** 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 Note: Requires the configuration of the `protocol = "wss"`, `certfile`, and `keyfile` parameters in the [webapi] section. For example: “certs/LocalLabRootCA3.pem”
`certfile = "path/certfile.pem"`	**Section Name:** [webapi] **Description:** Required when the Nymi Agent uses the Nymi WebAPI with wss. Uncomment and specify the path to the TLS certificate in PEM format. Note: Requires the configuration of the `protocol = "wss"`, `cacertfile`, and `keyfile` parameters in the [webapi] section. For example: “certs/tw-srv1.tw-lab.local-cert.pem”
`keyfile = "path/keyfile.pem"`	**Section Name:** [webapi] **Description:** 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. Note: Requires the configuration of the `protocol = "wss"`, `cacertfile`, and `certfile` parameters in the [webapi] section. For example: “certs/tw-srv1.tw-lab.local-key.pem”

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.

6 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 theuser 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 NEAs
    - Windows thick client user terminals that access locally installed NEAs
    - Windows thick clients that use lock control to lock/unlock the desktop
    - Windows thick clients that perform centralized firmware updates
    - Windows thick clients that gather data for Smart Distancing and Contact Tracing activities
- Perform the steps outlined in the section Install and Configure Endpoints with a centralized Nymi Agent for:
    - iOS devices that access web-based NEAs
    - User terminals that access web-based NEAs
    - Thin client user terminals that access NEAs that are installed on a remote session host
    - Thin client user terminals that unlock the desktop on a remote session host
    - Thin clients that gather data for Smart Distancing and Contact Tracing activities

> **Note:** Starting with CWP 1.19.0, you can silently install and configure the Nymi and Evidian client software. The application is in a folder named `ClientInstaller`. This feature requires advanced Connected Worker Platform knowledge. Contact your Nymi Solution Consultant to use the silent installer.

6.1 Setting the Nymi Bluetooth Endpoint ID Format

The Nymi Bluetooth Endpoint identifies each user terminal to the applications that connect to it by an endpoint ID. 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` system environment variable.

`ENDPOINT_ID_MODE` value	Description
`IP` (default)	The endpoint ID is the IPv4 address of the user terminal. Suitable for most environments.
`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.

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

To set the endpoint ID format:

1. Set the system 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, RDP or Citrix servers with the PAS-X Client or Evidian Client installed.
2. Restart the computer so that the new setting takes effect. If the Nymi Bluetooth Endpoint is the only Nymi component installed, restarting the Nymi Bluetooth Endpoint is sufficient.

Note: 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.

6.2 Install and Configure Endpoints with a Decentralized Nymi Agent

This section for 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 the each use case and endpoint configuration.

Endpoint/ Use Case	Description	Nymi Component Requirements
Enrollment terminal	Where users enroll their Nymi Bands by using the Nymi Band Application, and can use the Nymi Band Application to authenticate to their Nymi Bands by using corporate credentials authentication. The Nymi Connected Worker Platform—Administration Guide provides more information about how to configure corporate credentials authentication.	Nymi Band Application
User Terminal for Authentication Tasks	Windows thick client where users access a locally-installed NEA.	Nymi Runtime(Nymi Bluetooth Endpoint and Nymi Agent).
User Terminal for lock and unlock tasks on the user terminal	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.

6.2.1 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.

Previously, Nymi supplied the Bluegiga Bluetooth Adapter (BLED112). Nymi can now provide customers with the BleuIO Bluetooth Adapter. On Windows, the Bluegiga Bluetooth adapter required a Bluegiga driver, which the Nymi software installed by default. The BleuIO Bluetooth adapter is a USB serial port device and does not require any specialized drivers.

> **Note:** You can continue to use your Bluegiga Bluetooth Adapter on existing machines. It is not necessary to replace Bluegiga Bluetooth Adapter with a BleuIO Bluetooth Adapter.

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.

6.2.2 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.

- Insert the Nymi-supplied Bluetooth adapter into an available USB port.
- Install the Nymi Band Application. The Nymi Band user requires physical access to the enrollment terminal.
- Set the NES_URL registry key.

6.2.2.1 Importing 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.

Before you begin

Install the Root CA on the following machines:

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

About this task

While logged into the user terminal as a local administrator, use the **certlm** application to import the root CA certificate into the Trusted Root Certification Authorities store.

Procedure

1. In the **certlm** window, right-click **Trusted Root Certification Authorities**, and then select **All Tasks > Import**.
2. On the **Welcome to the Certificate Import Wizard** screen, click **Next**.
3. On the **File to Import** screen, click **Browse**, navigate to the folder that contains the certificate file, select the file, and then click **Open**.
4. On the **File to Import** screen, click **Next**.
5. 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**.
6. On the **Completing the Certificate Import Wizard** screen, click **Finish**.

6.2.2.2 Installing/Updating the Nymi Band Application

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Before you begin

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

Procedure

1. Download the Nymi Band Application 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.

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

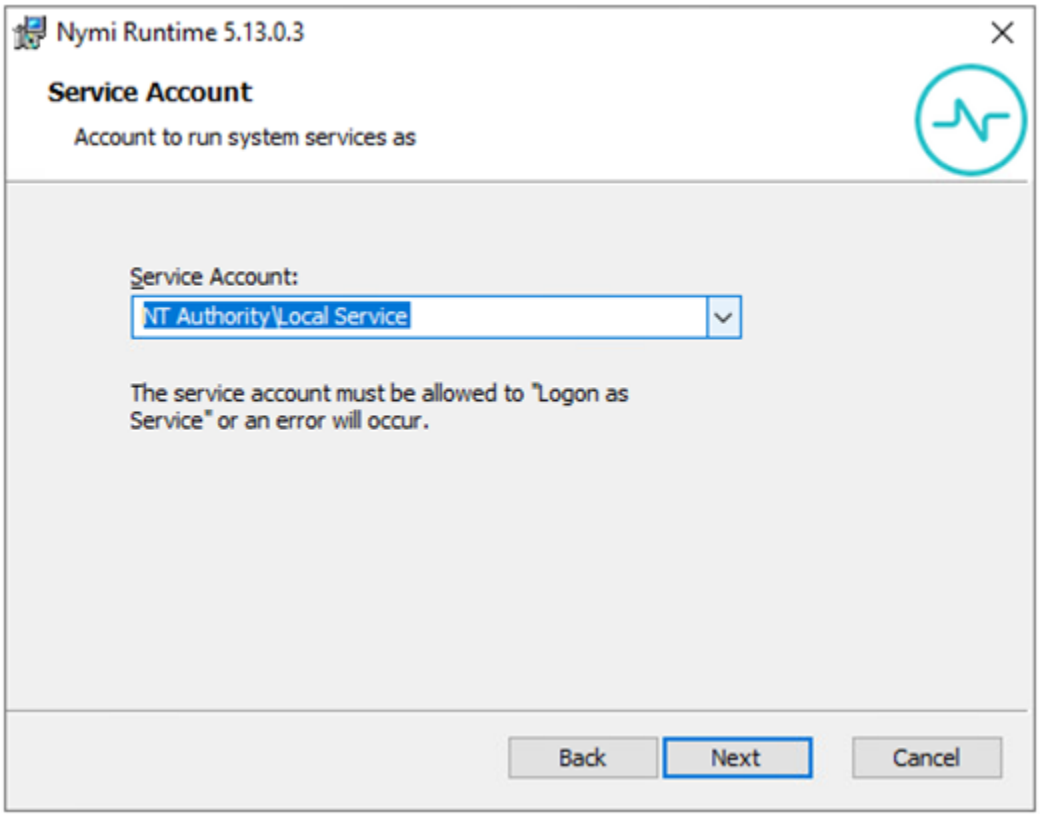


Figure 70. Nymi Runtime Service Account window

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

    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**.

What to do next

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

6.2.2.3 Configuring the Nymi Enterprise Server URL

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

Procedure

1. Run `regedit.exe`
2. On the **User Account Control** window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.
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 viewing the properties of the computer. The `nes_server` is the value that appears in the **Full computer name** field.
   - `NES_service_name` is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you

specify a name that is descriptive to the Connected Worker Platform, for example, NES.

8. Click **OK**.

6.2.2.4 Disabling Evidian Enrollment

Nymi supports using the same NES server to enroll users in Evidian and non-Evidian environments simultaneously.

About this task

On the enrollment terminal which does not enroll users to an Evidian Evidian EAM Controller, perform the following steps.

Procedure

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`.

6.2.2.5 Configuring the Communication Protocol

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

About this task

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

Procedure

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 the perform the following actions:
    a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`
    b. In the **Variable Value** field, type `0`.

    The following figure provides an example of the new variable.

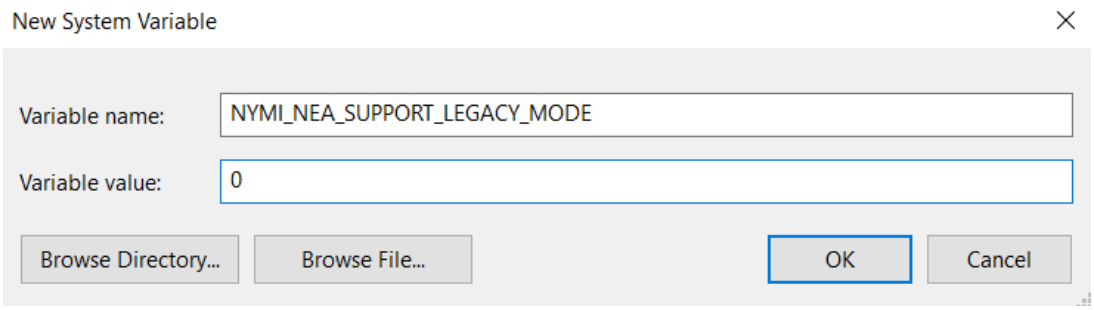


Figure 71. New System Variable window

    c. Click **OK**.

6.2.3 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 for NES (when the Root CA that issued the certificate is not a trusted CA).
- Insert the Nymi-supplied Bluetooth adapter into an available USB port.
- Optionally, insert a Nymi-verified NFC reader into an available USB port.

6.2.3.1 Importing 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.

Before you begin

Install the Root CA on the following machines:

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

About this task

While logged into the user terminal as a local administrator, use the **certlm** application to import the root CA certificate into the Trusted Root Certification Authorities store.

Procedure

1. In the **certlm** window, right-click **Trusted Root Certification Authorities**, and then select **All Tasks > Import**.
2. On the **Welcome to the Certificate Import Wizard** screen, click **Next**.
3. On the **File to Import** screen, click **Browse**, navigate to the folder that contains the certificate file, select the file, and then click **Open**.
4. On the **File to Import** screen, click **Next**.
5. 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**.
6. On the **Completing the Certificate Import Wizard** screen, click **Finish**.

6.2.3.2 Installing/Updating 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.

About this task

Procedure

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

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

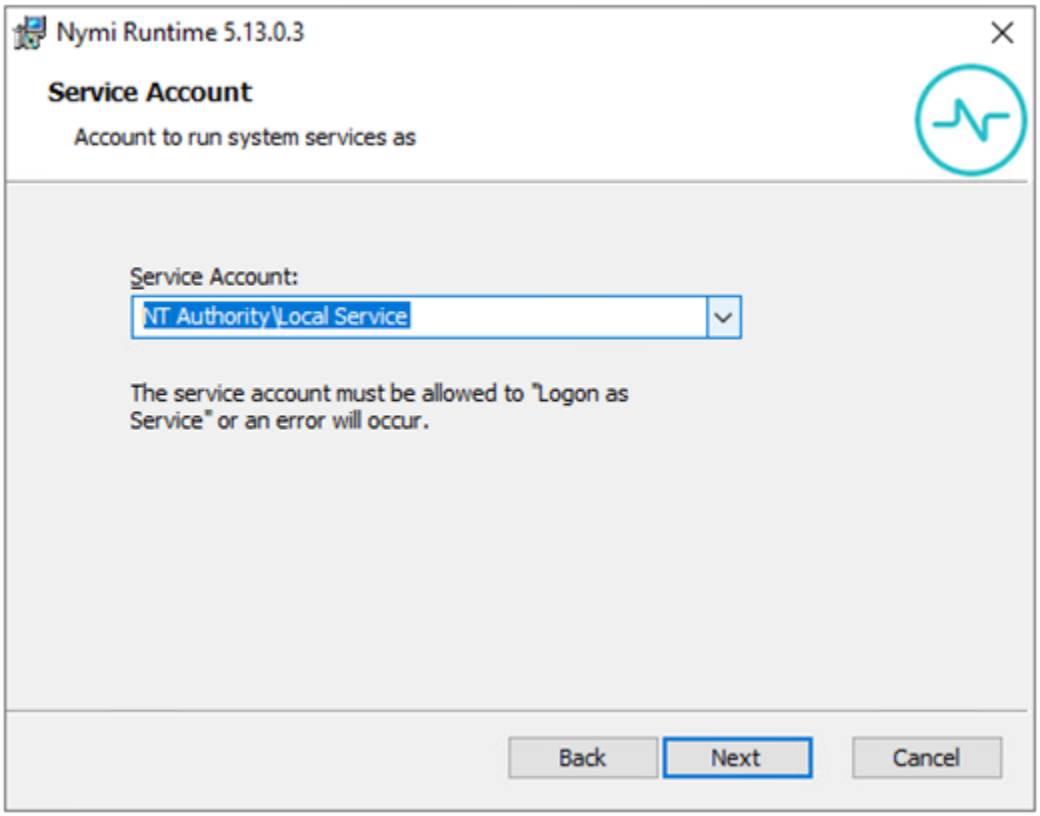


Figure 72. Nymi Runtime Service Account window

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

    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**.

What to do next

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

6.2.3.3 Configuring the Connected Worker Platform Communication Protocol

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

About this task

Perform the following steps on all user terminals (for Evidian environments on Wearable user terminals only) where users access Nymi-Enabled Applications(NEAs) 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.

Procedure

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 the perform the following actions:
    a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`
    b. In the **Variable Value** field, type `0`.

        The following figure provides an example of the new variable.

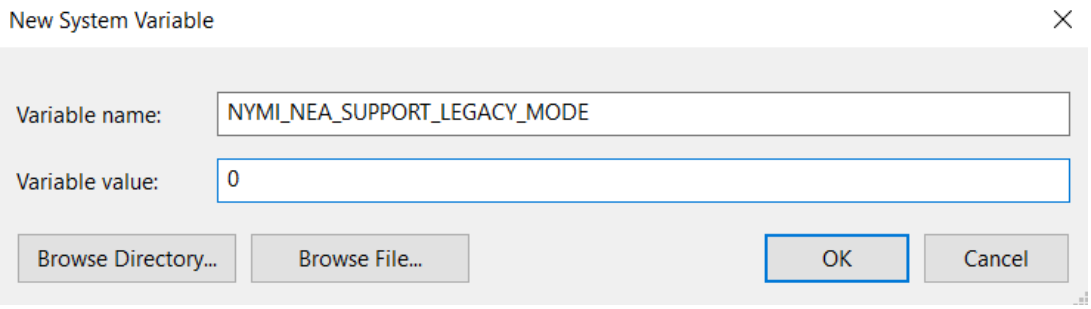


Figure 73. New System Variable window

c. Click **OK**.

6.2.4 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 theNymi Band to lock and unlock a desktop require that you:

- Import the Root CA certificate for NES (when the Root CA that issued the certificate is not a trusted CA).
- Insert the Nymi-supplied Bluetooth adapter into an available USB port.
- Install the Nymi Lock Control software
- Configure the Nymi Bluetooth Endpoint configuration file.

6.2.4.1 Configuring Nymi Lock Control

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

About this task

By default Nymi Lock Control is not enabled.

Procedure

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.

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. When the Nymi Band is out of range, a 10 second timer appears on the desktop. If the Nymi Band does not return within close range of the user terminal, the terminal will lock. Ensure that your Group Policy Object(GPO) settings do not push the Do not display the lock screen configuration option to the Nymi Lock Control user terminals. **Note:** Edit the `nbe.toml` file to define close proximity for Nymi Lock Control. Refer to Editing the nbe.toml File in the Nymi Connected Worker Platform—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. 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 `nbe.toml` file. The Editing the nbe.toml File section in the Nymi Connected Worker Platform—Deployment Guide provides more information. ◦ 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 user terminal by pressing the **Enter** key or space bar on the keyboard when the authenticated Nymi Band is within Bluetooth range, but not in close proximity of the user terminal.
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**.

Results

During enrollment the Nymi Band Application updates the Nymi Band to enable Nymi Lock Control support.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Band until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

When the Nymi Band Application updates on the Nymi Band completes, restart Nymi Lock Control.

6.2.4.2 Importing 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.

Before you begin

Install the Root CA on the following machines:

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

About this task

While logged into the user terminal as a local administrator, use the **certlm** application to import the root CA certificate into the Trusted Root Certification Authorities store.

Procedure

1. In the **certlm** window, right-click **Trusted Root Certification Authorities**, and then select **All Tasks > Import**.

2. On the **Welcome to the Certificate Import Wizard** screen, click **Next**.
3. On the **File to Import** screen, click **Browse**, navigate to the folder that contains the certificate file, select the file, and then click **Open**.
4. On the **File to Import** screen, click **Next**.
5. 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**.
6. On the **Completing the Certificate Import Wizard** screen, click **Finish**.

6.2.4.3 Updating Nymi Lock Control

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

Procedure

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 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.

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

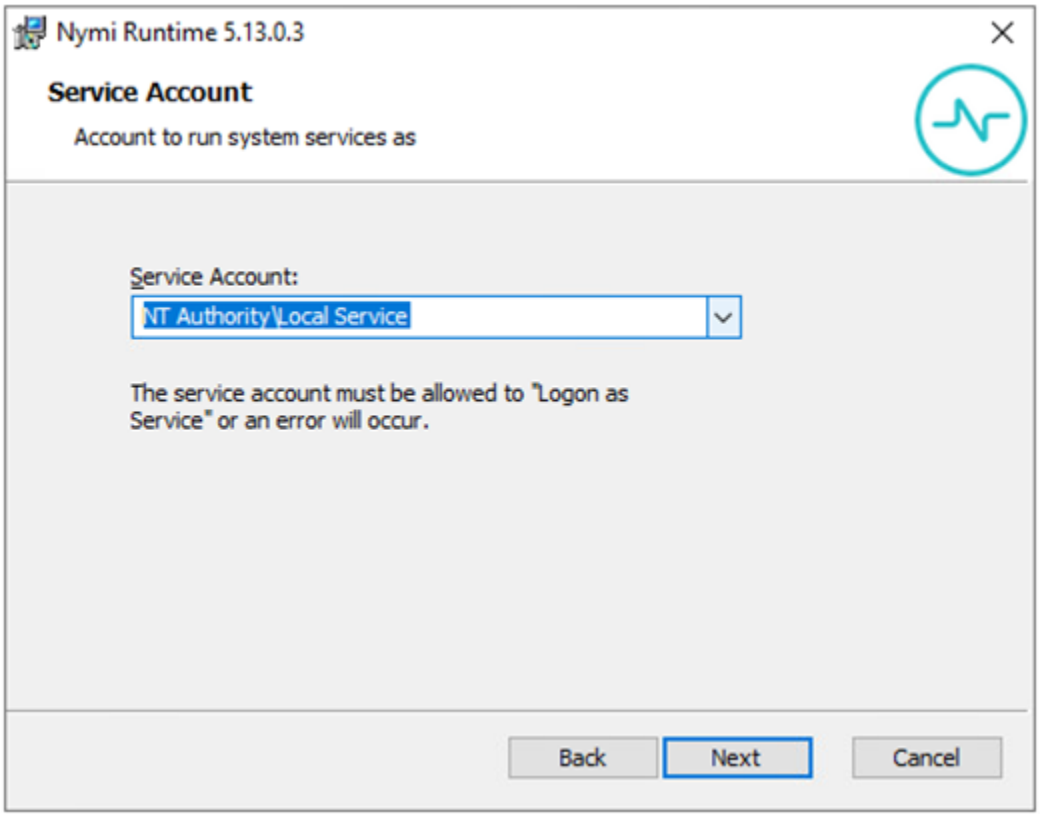


Figure 74. Nymi Runtime Service Account window

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, perform the following actions:

    a. To change the installation location, click **Browse**, navigate to a new installation folder, and then click **Select Folder**
    b. 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 Connected Worker Platform 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.

6.2.4.4 Configuring the Nymi Enterprise Server URL

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

About this task

Run `regedit` as an administrator.

Procedure

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

   > **Note:** If this path does not exist, create the keys.

2. In the NES key, create a new string value, as shown in the following figure.

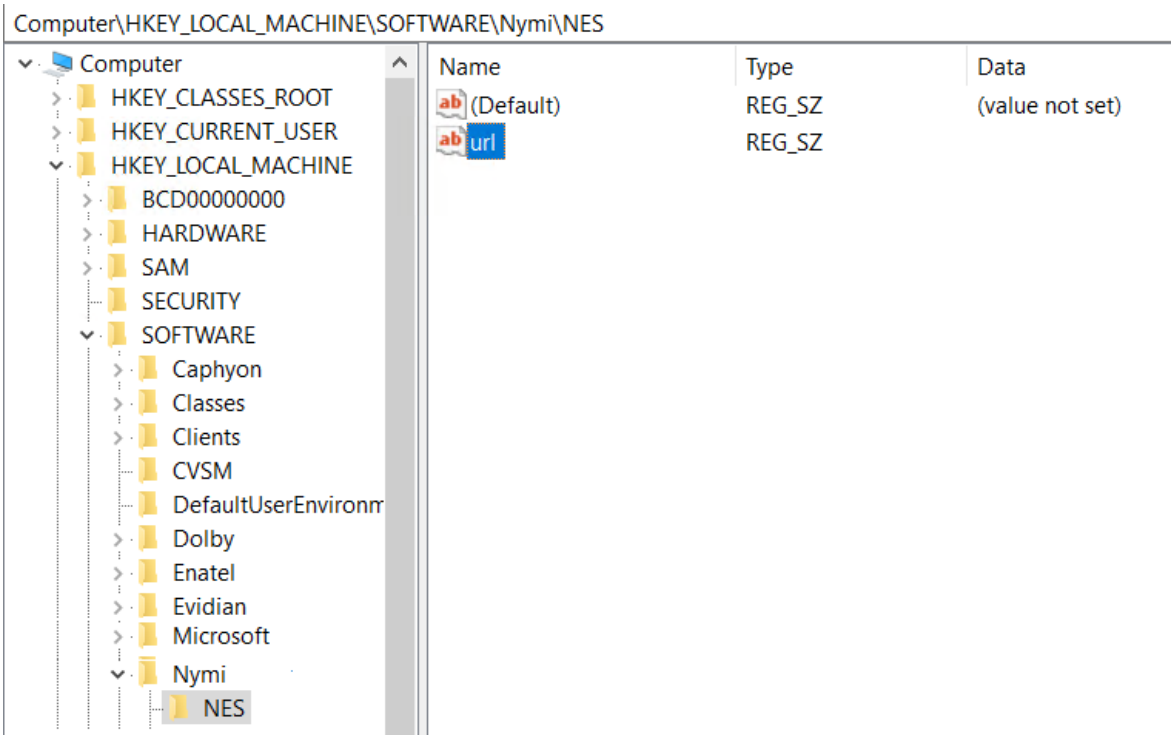


Figure 75. NES registry key

3. In the **Name** field, type URL.

4. Edit the string and in the value field, type `https://nes_server/instance`

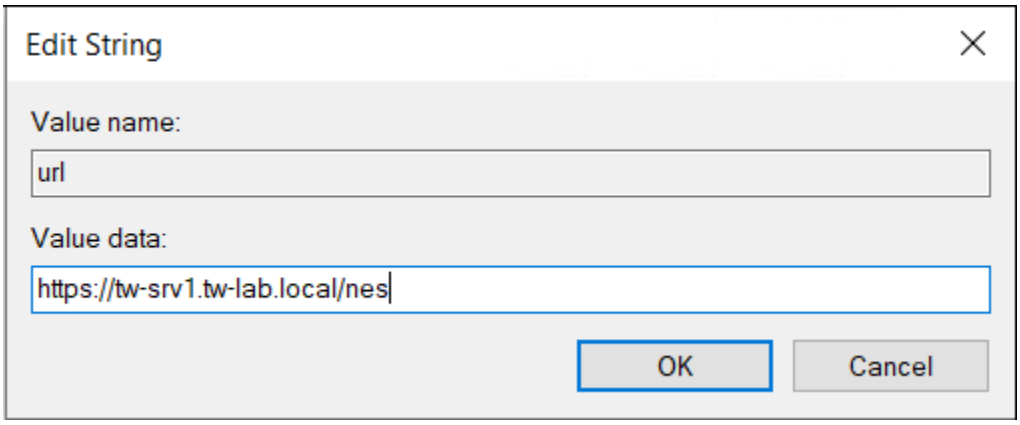
   Where:

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

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

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

The following figure provides an example of the URL key value.



6.2.4.5 Configuring the Connected Worker Platform Communication Protocol

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

About this task

Perform the following steps on all user terminals (for Evidian environments on Wearable user terminals only) where users access Nymi-Enabled Applications(NEAs) 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.

Procedure

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 the perform the following actions:
    a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`
    b. In the **Variable Value** field, type `0`.

    The following figure provides an example of the new variable.

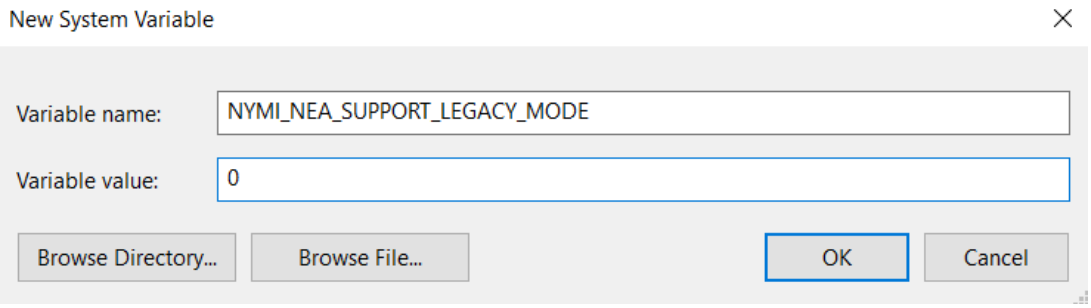


Figure 76. New System Variable window

    c. Click **OK**.

6.2.4.6 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 (ex. USB adapter). 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.

Starting in Connected Worker Platform 1.21.0, the Nymi software supports two types of Bluetooth Adapters, the Bluegiga BLED112 Adapter and the BleuIO Adapter.

The `C:\Nymi\Bluetooth_Endpoint\nbe.toml` and `/usr/bin/nbe.toml` include two different sections where you can define RSSI parameters:

Section Name	Bluetooth Adapter Type	Bluetooth Adapter Image
`[dongle.bluegiga]`	Bluegiga BLED112 Adapter	
`[dongle.nymi]`	BleuIO Adapter	

Note: Consider the following for IGEL:

- Specify all RSSI parameter names in capital letters.
- Use the Bluegiga BLED112 Bluetooth Adapter only.

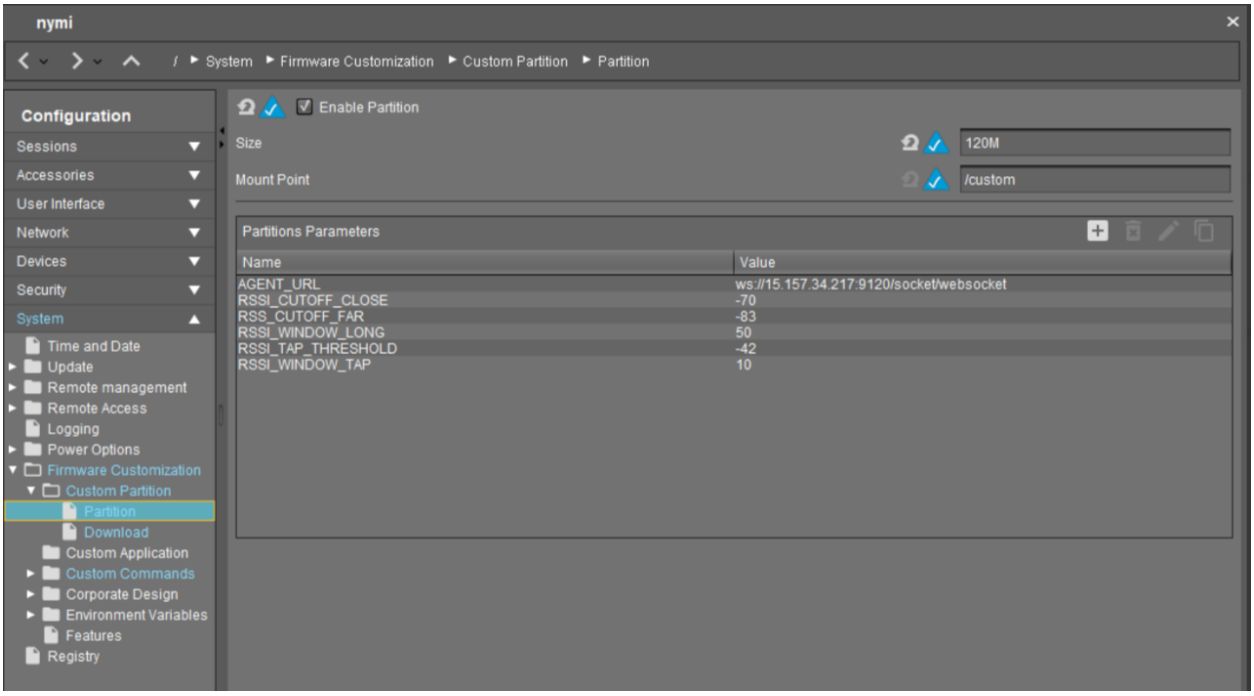
The following table provides a list of supported RSSI parameters, their default values and the purpose of each parameter.

Table 5. RSSI Values

RSSI Parameter	Default Value	Description
`rssi_window_tap`	Bluegiga: 10; BleuIO: 12	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 of the Bluetooth Adapter and decreases the sensitivity.
`rssi_window_long`	Bluegiga: 50; BleuIO: 55	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 **keep unlocked when present**, **lock when away**, or **unlock when present**.
`rssi_tap_threshold`	Bluegiga: -42; BleuIO: -35 (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. Suggested threshold between -20 (strict) and -35 (relaxed). 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 `rssi_tap_threshold`, for the duration of time that is defined by `rssi_window_tap`, a BLE tap is performed.
`rssi_cutoff_close`	Bluegiga: -70; BleuIO: -68 (must be 0 or negative)	This determines the outer range of the close distance-threshold (excluding tap

RSSI Parameter	Default Value	Description
		distance) for Nymi Lock Control. Enter 0 to bypass the proximity functionality of Nymi Lock Control. If the Nymi Band maintains a close distance to the BLE radio antenna and the RSSI values measured are within the `rssi_cutoff_close` value, Nymi Lock Control keeps the user terminal unlocked. If the Nymi Band moves away from the BLE radio antenna, and the RSSI values measured are on a decreasing trend and goes from the `rssi_cutoff_close` value to the `rssi_cutoff_far` value, Nymi Lock Control locks the user terminal.
`rssi_cutoff_far`	Bluegiga: -83; BleuIO: -80 (must be negative)	This determines the outer range of the far distance-threshold (excluding tap distance) for Nymi Lock Control. If the Nymi Band moves towards the BLE radio antenna, and the RSSI values measured are on an increasing trend and goes from the `rssi_cutoff_far` value to the `rssi_cutoff_close` value, Nymi Lock Control unlocks the user terminal.

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



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

6.3 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 accesses a web-based NEA.	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 tasks that require authentication in a Nymi-Enabled Application(NEA) on the remote sessions host.	Nymi Runtime (Nymi Bluetooth Endpoint only)

Endpoint/Use Case	Description	Nymi Component Requirements
User Terminal for lock and unlock tasks	Nymi Lock Control Nymi Runtime(Nymi Bluetooth Endpoint only) .	Where a user uses their Nymi Band to lock or unlock the desktop of the remote session host.

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.

Note: Starting with CWP 1.19.0, you can silently install and configure the Nymi and Evidian client software. The application is in a folder named `ClientInstaller`. This feature requires advanced Connected Worker Platform knowledge. Contact your Nymi Solution Consultant to use the silent installer.

6.3.1 Set Up the Enrollment Terminal

You can setup the enrollment terminal in two configurations.

- Centralized Enrollment Terminal—install the Nymi Band Application 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.
- De-Centralized Enrollment Terminal—Install the Nymi Band Application on a thick client user terminal, to limit the access a user has to perform enrollments.

6.3.1.1 Centralized Enrollment Terminal

In this configuration, you perform the following steps:

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

6.3.1.2 Decentralized Enrollment Terminal

In this configuration you install the Nymi Band Application and the Nymi Runtime software on a thick client enrollment terminal.

6.3.1.3 Deploy a Centralized Enrollment Terminal

When you deploy a centralized enrollment terminal, you install the Nymi Band Application on the Citrix/RDP server.

After you install the Nymi Bluetooth Endpoint on the thick client, users can launch the Nymi Band Application 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 Installing User Terminal Components chapter.

Installing the Nymi Band Application on RDP/Citrix Session Host

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Procedure

1. Download the Nymi Band Application 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**.

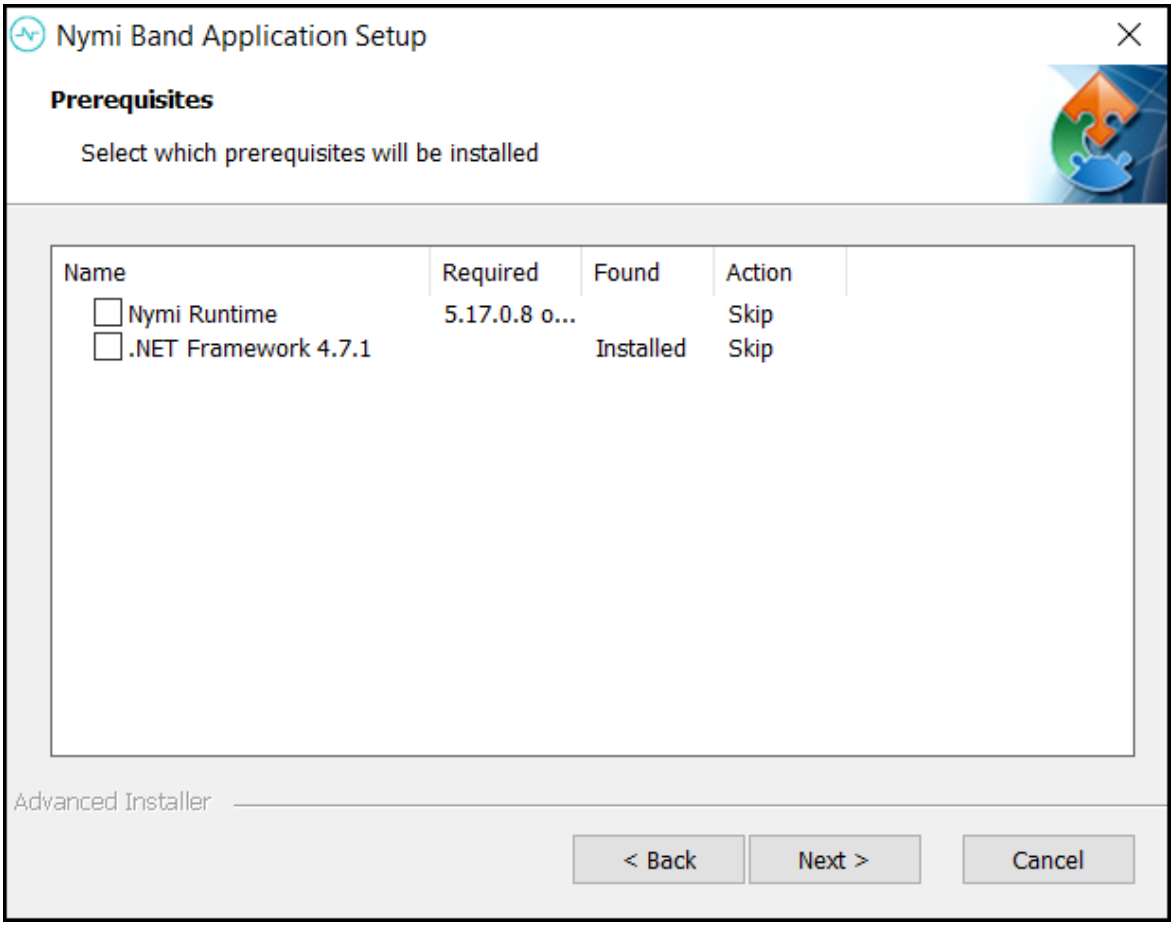


Figure 77. No Nymi Runtime Installation

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**.

Configuring Nymi Band Application to use a Centralized Nymi Agent

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

Procedure

1. Run `regedit.exe`
2. On the **User Account Control** window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.
4. Right-click **NES**, and then select **New > String value**.
5. In the **Value** field, type `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` 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”

Configuring the Nymi Enterprise Server URL

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

Procedure

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

3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.
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 viewing the properties of the computer. The `nes_server` is the value that appears in the **Full computer name** field.
   - `NES_service_name` is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.
8. Click **OK**.

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. You can install the Nymi Bluetooth Endpoint silently or with the installation wizard.

After you install the Nymi Bluetooth Endpoint, you must update the `nbe.toml` file.

Installing 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.

About this task

Perform the following steps to install Nymi Bluetooth Endpoint manually.

Procedure

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. Extract the `Nymi SDK` distribution package.
4. From the `..\nymi-sdk\windows\setup`folder, right-click the `Nymi Runtime Installer version.exe` file, and select **Run as administrator**.
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, expand **Nymi Runtime**.
9. Select **Nymi Agent**, and then select **Entire feature will be unavailable**, as shown in the following figure, and then click **Next**.

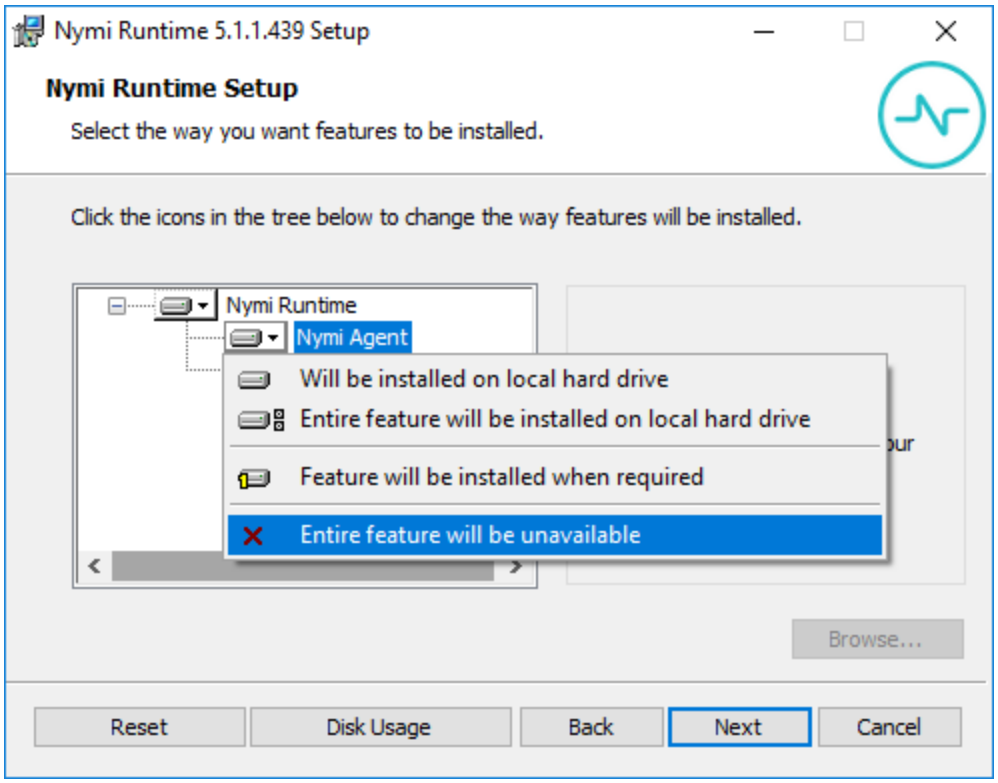


Figure 78. Nymi Agent feature will be unavailable

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

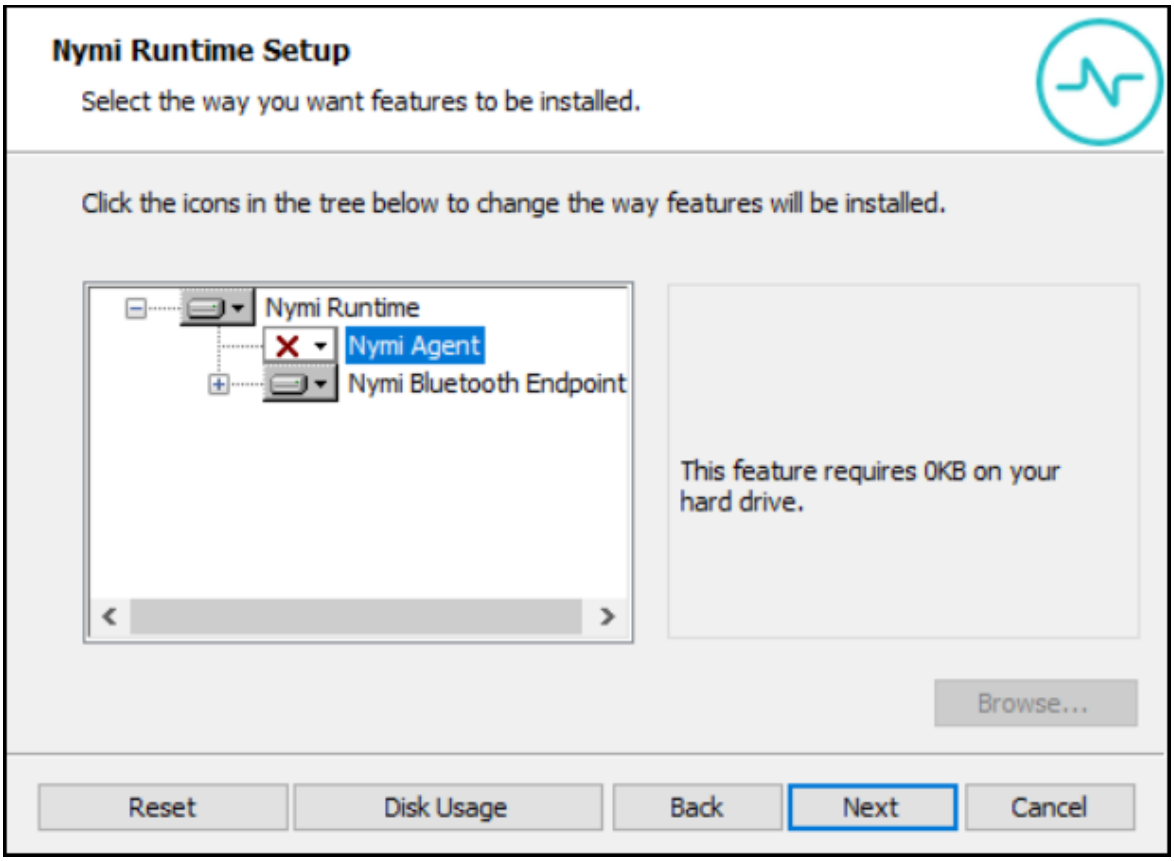


Figure 79. Nymi Agent feature is not available

11. 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.

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

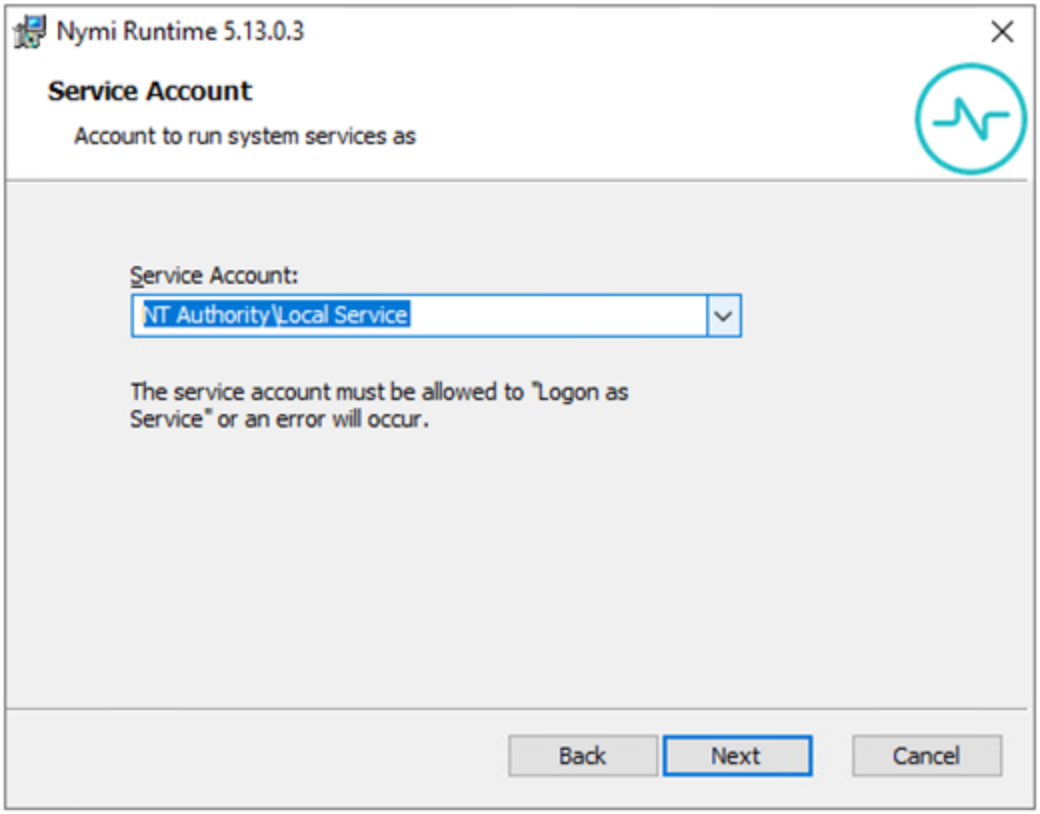


Figure 80. Nymi Runtime Service Account window

12. On the **Ready to install** page, click **Install**.
13. Click **Finish**.
14. On the **Installation Completed Successfully** page, click **Close**.

What to do next

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

Editing the Nymi Bluetooth Endpoint Configuration File

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

About this task

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

Procedure

1. Make a copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.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 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.

What to do next

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

6.3.1.4 Deploy a Decentralized Enrollment Terminal

Install the and the Nymi Band Application, which also installs the Nymi Runtime software on a thick client.

Installing/Updating the Nymi Band Application

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Before you begin

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

Procedure

1. Download the Nymi Band Application 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.

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

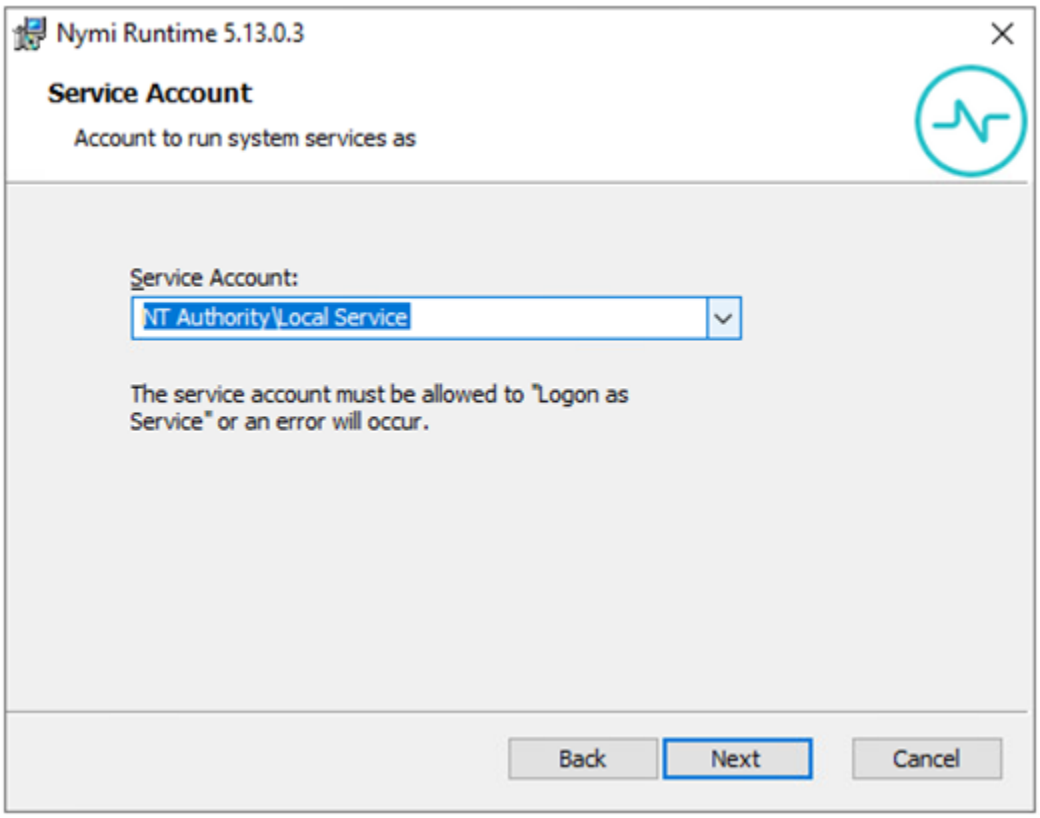


Figure 81. Nymi Runtime Service Account window

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

    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**.

What to do next

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

Configuring the Nymi Enterprise Server URL

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

Procedure

1. Run `regedit.exe`
2. On the **User Account Control** window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software > Nymi**.
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 viewing the properties of the computer. The `nes_server` is the value that appears in the **Full computer name** field.
- `NES_service_name` is the name of the service mapping for NES in IIS, which maps a virtual directory to a physical directory. You can choose any name for this mapping, but Nymi recommends that you specify a name that is descriptive to the Connected Worker Platform, for example, NES.

8. Click **OK**.

6.3.1.5 Configuring the Communication Protocol

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

About this task

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

Procedure

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 the perform the following actions:
   a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`
   b. In the **Variable Value** field, type `0`.

      The following figure provides an example of the new variable.

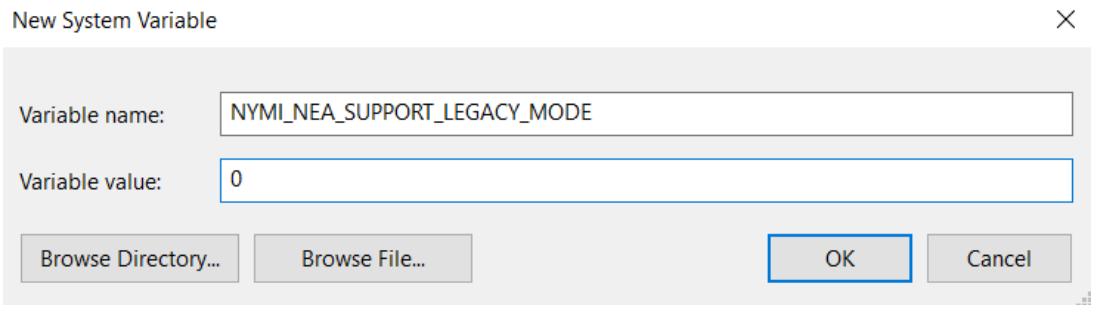


Figure 82. New System Variable window

c. Click **OK**.

6.3.2 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 reside on VMware Horizon thin clients a remote session host .

- Import the Root CA certificate for NES (when the Root CA that issued the certificate is not a trusted CA).
- Install the Nymi Bluetooth Endpoint service.
- Insert the Nymi-supplied Bluetooth adapter into an available USB port.
- Optionally, insert a Nymi-verified NFC reader into an available USB port.

6.3.2.1 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.

Previously, Nymi supplied the Bluegiga Bluetooth Adapter (BLED112). Nymi can now provide customers with the BleuIO Bluetooth Adapter. On Windows, the Bluegiga Bluetooth adapter required a Bluegiga driver, which the Nymi software installed by default. The BleuIO Bluetooth adapter is a USB serial port device and does not require any specialized drivers.

> **Note:** You can continue to use your Bluegiga Bluetooth Adapter on existing machines. It is not necessary to replace Bluegiga Bluetooth Adapter with a BleuIO Bluetooth Adapter.

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.

6.3.2.2 Importing 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 NEA, you need to import the TLS certificate.

About this task

See `https://wiki.mozilla.org/CA/AddRootToFirefox` in the Mozilla documentation for more information.

Procedure

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.

6.3.2.3 Importing the Root CA Certificate in Citrix/RDP Environments

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

About this task

While logged into the user terminal as a local administrator, use the **certlm** application to import the root CA certificate into the Trusted Root Certification Authorities store.

Procedure

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

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

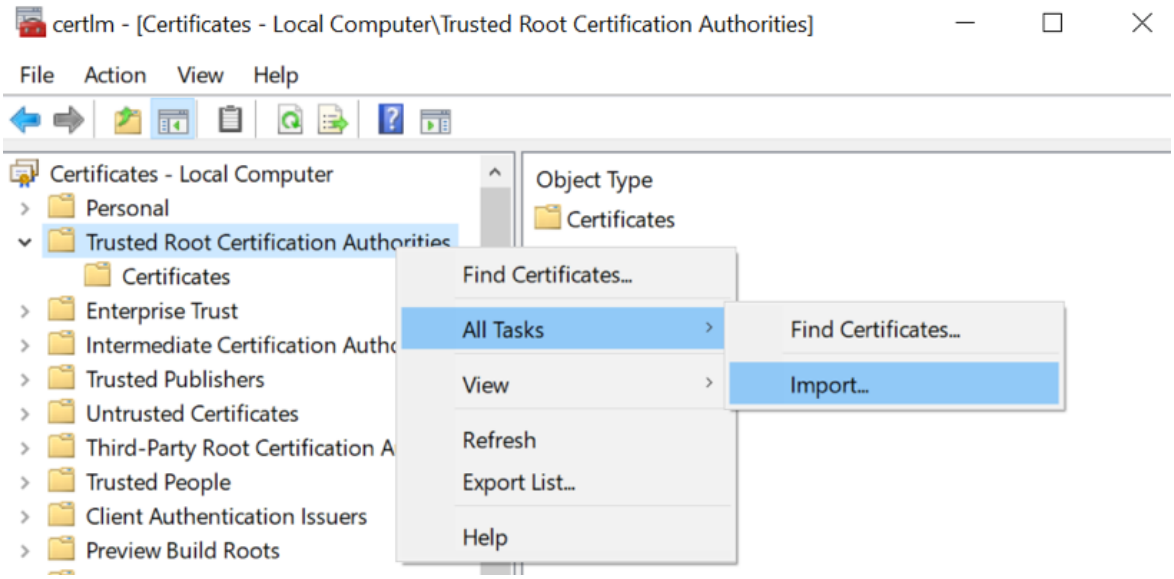


Figure 83. certlm application

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

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

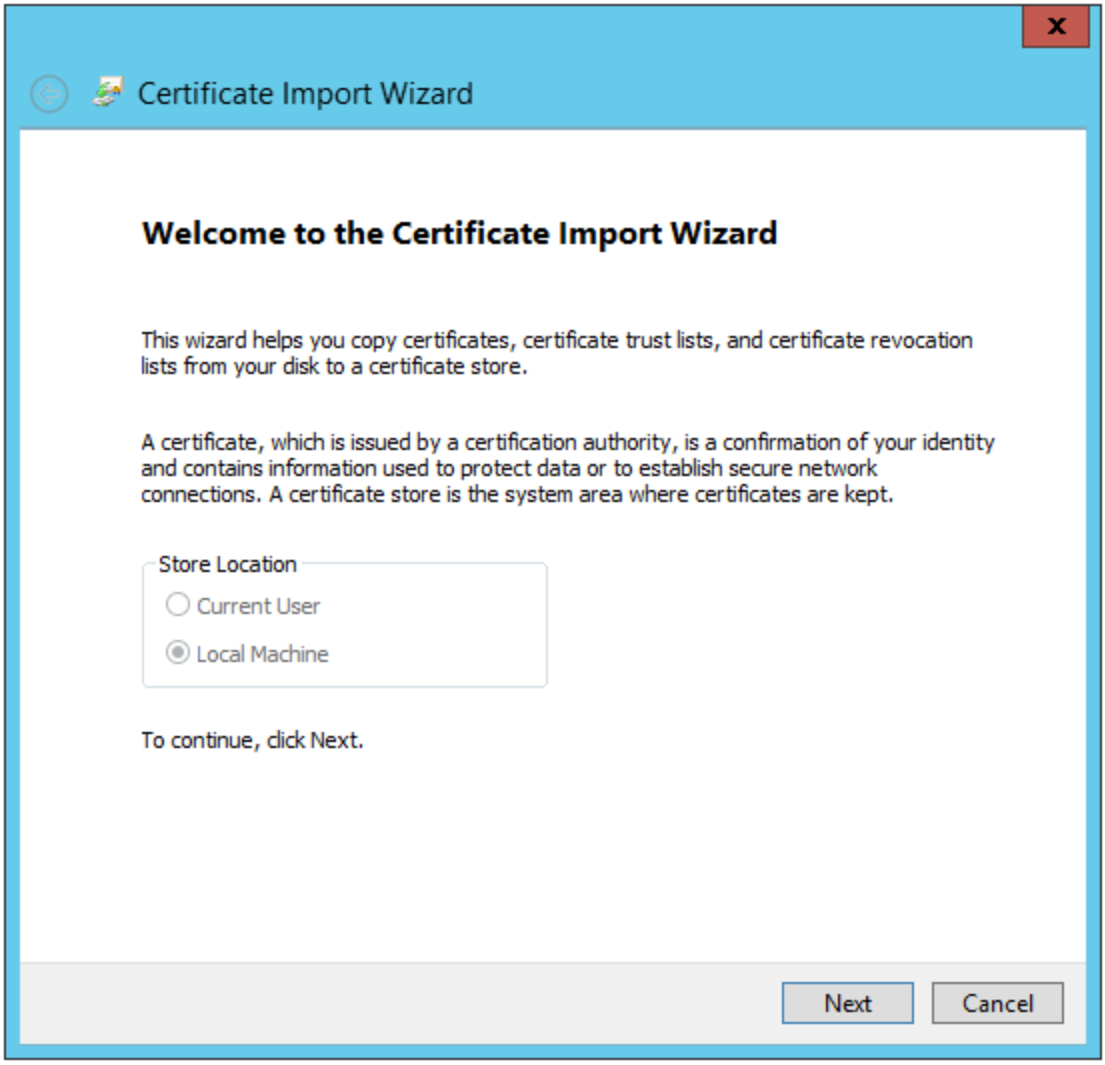


Figure 84. Welcome to the Certificate Import Wizard screen

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.

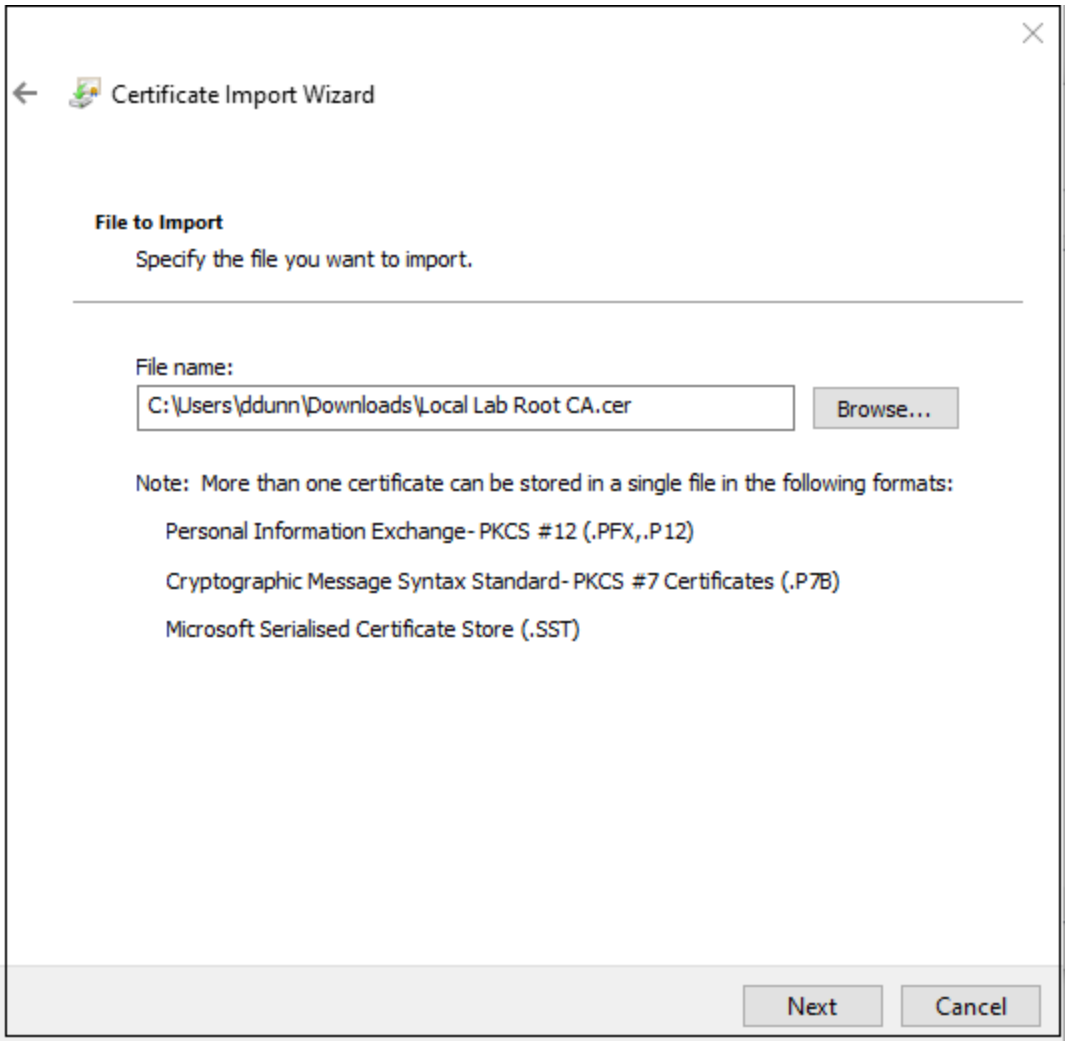


Figure 85. File to Import screen

6. On the **Certificate Store** screen, accept the default value **Place all certificates in the following store** with the value **Trusted Root Certification Authorities**, and then click **Next**.
7. On the **Completing the Certificate Import Wizard** screen, click **Finish**.
8. From the **Windows Start Menu**, type `Manage Computer`, and then select **Manage Computer Certificates**.

   The **certlm** window appears.
9. Navigate to **Personal > Certificates** folder.

   A list of certificates displays.
10. On the **User Account Control** dialog, click Yes.

11. Select the **Security** tab and then click the **Add** button.
12. In the new window, click **Add**, which opens the **Select Users, Computers, Service Accounts, or Groups** window.
13. In the **Permissions** area, under **Allow** column, select the **Read** permission.

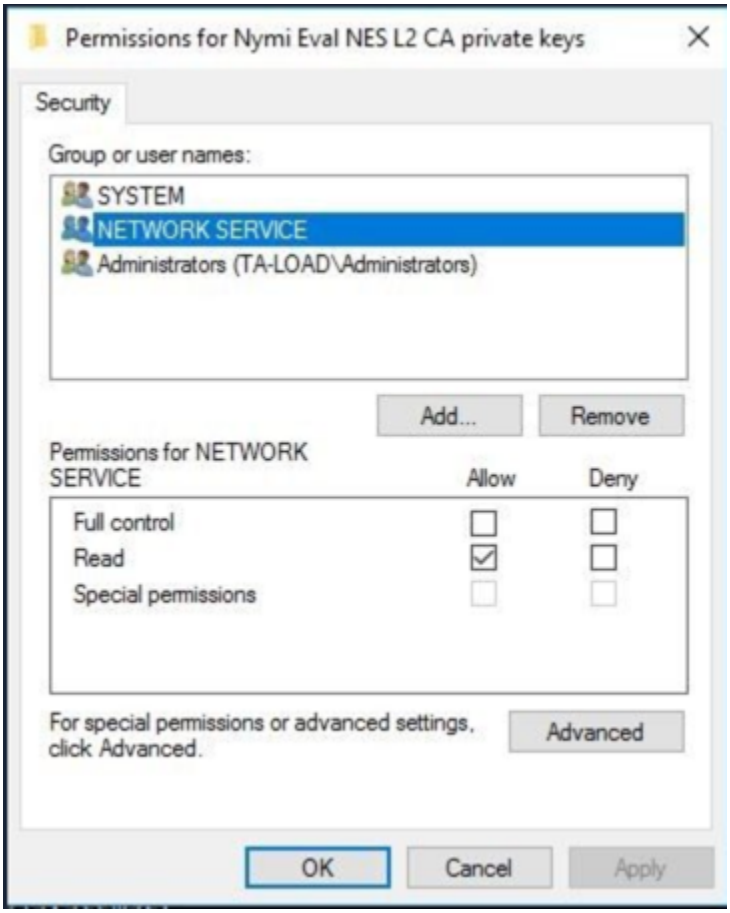


Figure 86. Setting Private Key Permissions

14. Click **OK**.

6.3.2.4 Installing 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.

About this task

Perform the following steps to install Nymi Bluetooth Endpoint manually.

Procedure

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. Extract the `Nymi SDK` distribution package.
4. From the `..\nymi-sdk\windows\setup`folder, right-click the `Nymi Runtime Installer version.exe` file, and select **Run as administrator**.
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, expand **Nymi Runtime**.
9. Select **Nymi Agent**, and then select **Entire feature will be unavailable**, as shown in the following figure, and then click **Next**.

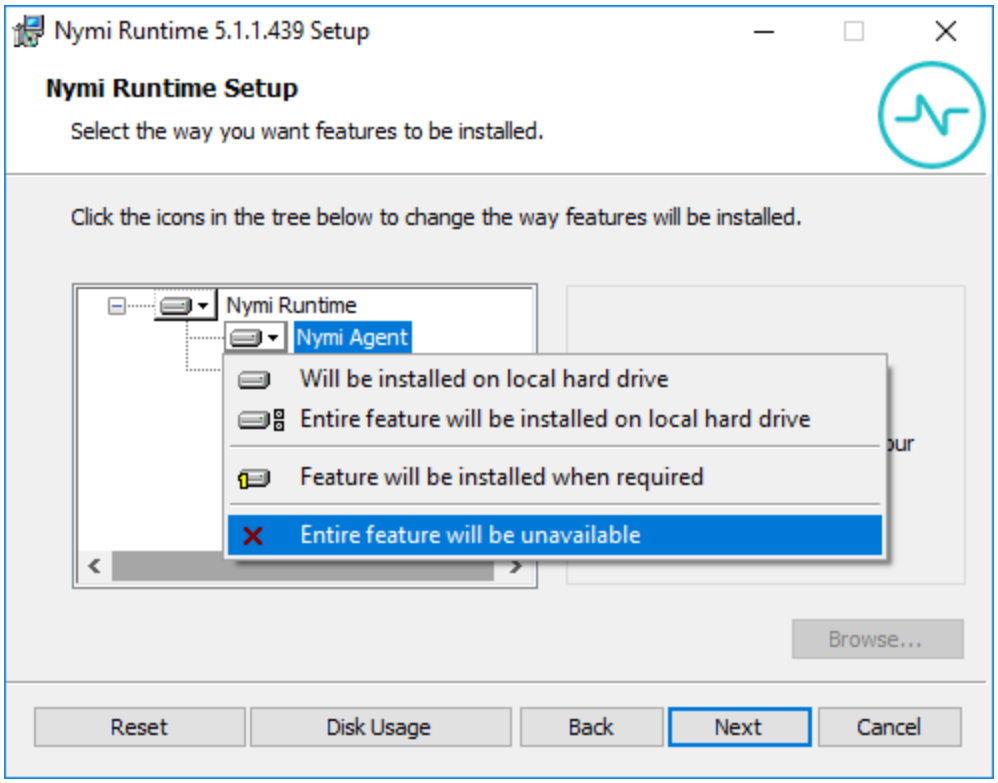


Figure 87. Nymi Agent feature will be unavailable

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

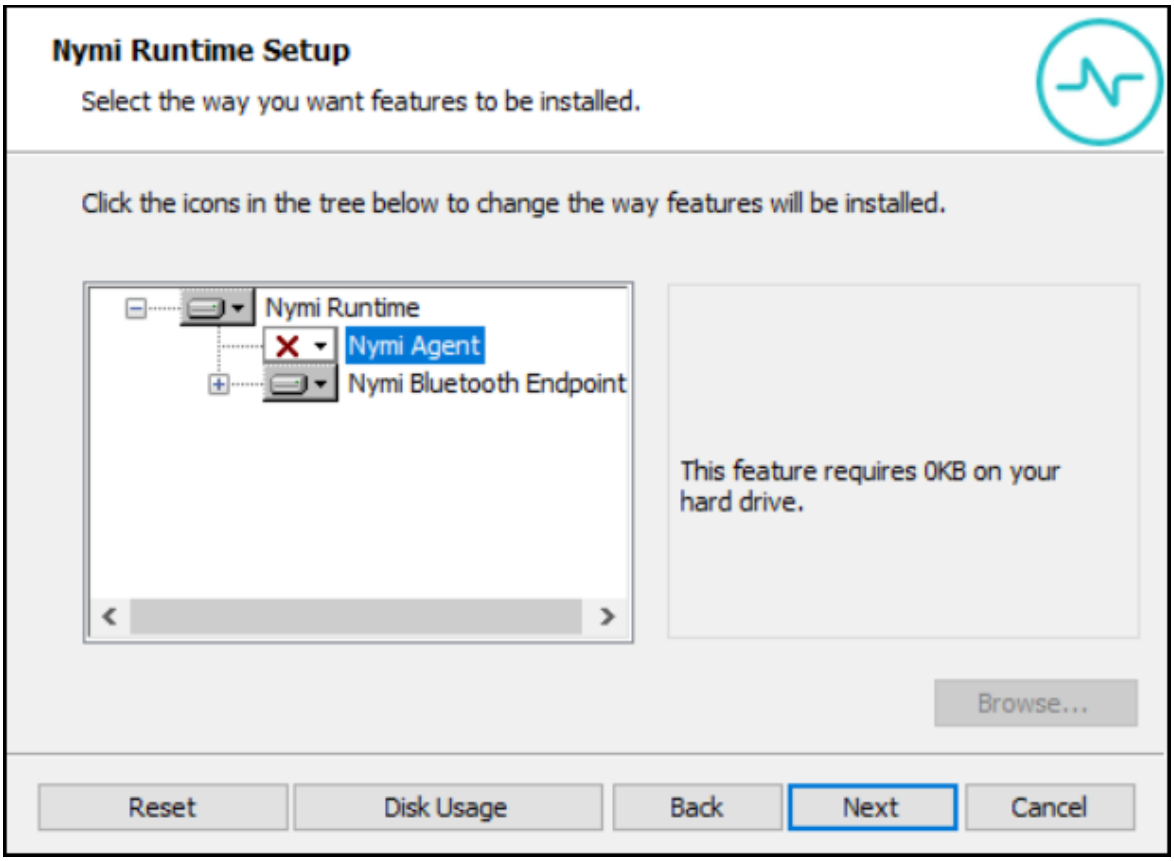


Figure 88. Nymi Agent feature is not available

11. 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.

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

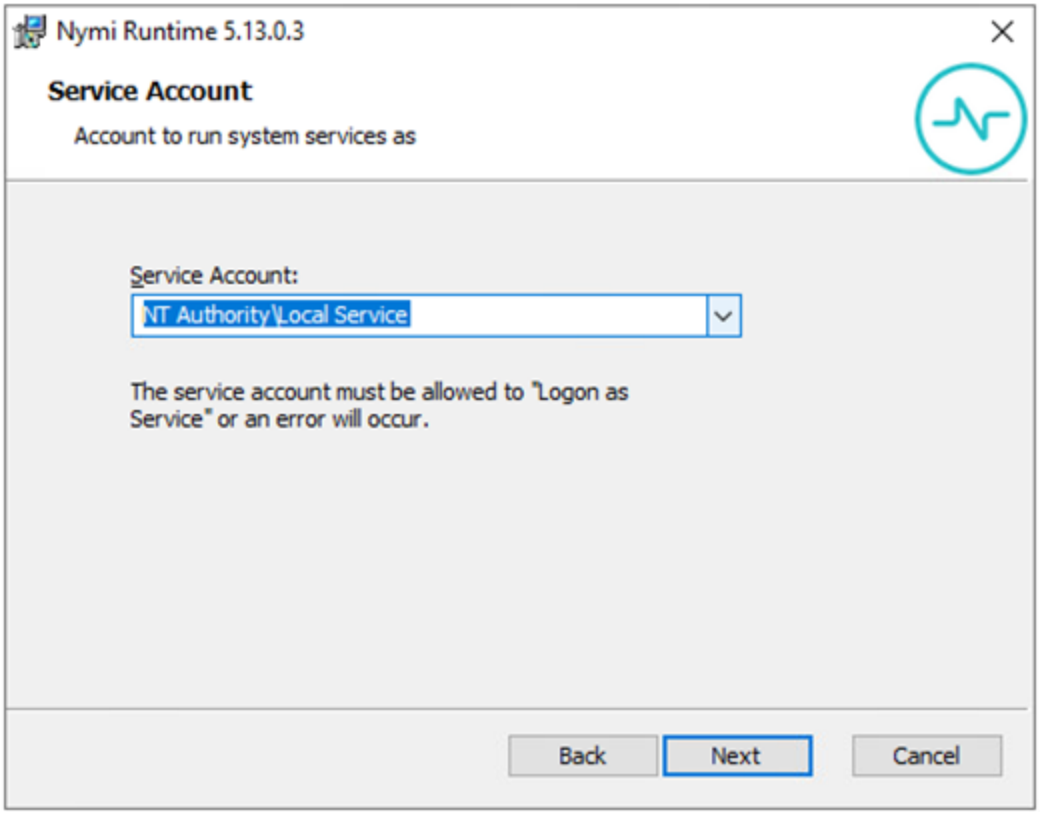


Figure 89. Nymi Runtime Service Account window

12. On the **Ready to install** page, click **Install**.
13. Click **Finish**.
14. On the **Installation Completed Successfully** page, click **Close**.

What to do next

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

6.3.2.5 (HP Thin Pro only) Installing Nymi Bluetooth Endpoint

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

About this task

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

Procedure

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

    a. Right-click the desktop or click **Start**.
    b. Click **Switch to Administrator** from the menu. You will be prompted to enter the administrator password.

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

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

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

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

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

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

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

5. Reboot the client.

6.3.2.6 (Windows and HP Thin Pro) Editing the Nymi Bluetooth Endpoint Configuration File

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

About this task

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

Procedure

1. Make a copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.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 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, or click the start button on the toolbar. Enter “Services” in the search bar. The Services application window appears.
    b. Search for **Nymi Bluetooth Endpoint** in the Services application.

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

On HP Thin Pro:

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

6. On HP Thin Pro only, revert the file system to read-only access.

   a. Open **X Terminal**.

   b. Type:

   ```
   fslock
   ```

   c. Close the terminal.

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

What to do next

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

6.3.2.7 (iGEL11) Installing Nymi Bluetooth Endpoint

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

Uploading Nymi Packages to Universal Management Suite

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

About this task

Obtain the installation package from Nymi.

Procedure

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

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

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

Results

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

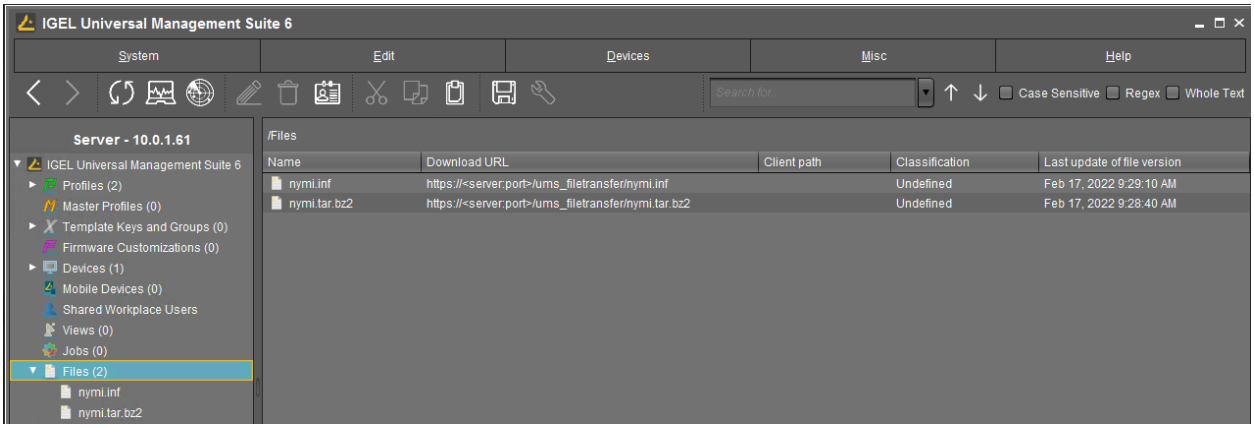


Figure 90. Files window

Creating a Profile and Custom Partition

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

Procedure

1. Connect to the **UMS Console**, right-click the `Profiles` folder, and then from the context menu, select `New Profile`.

   The **New Profile** window appears.

2. In the **Profile Name** field, type `Nymi`.

3. In the **Description** field, type `Install the Nymi Custom Partition`.

   The following figure provides an example of the **New Profile** window.

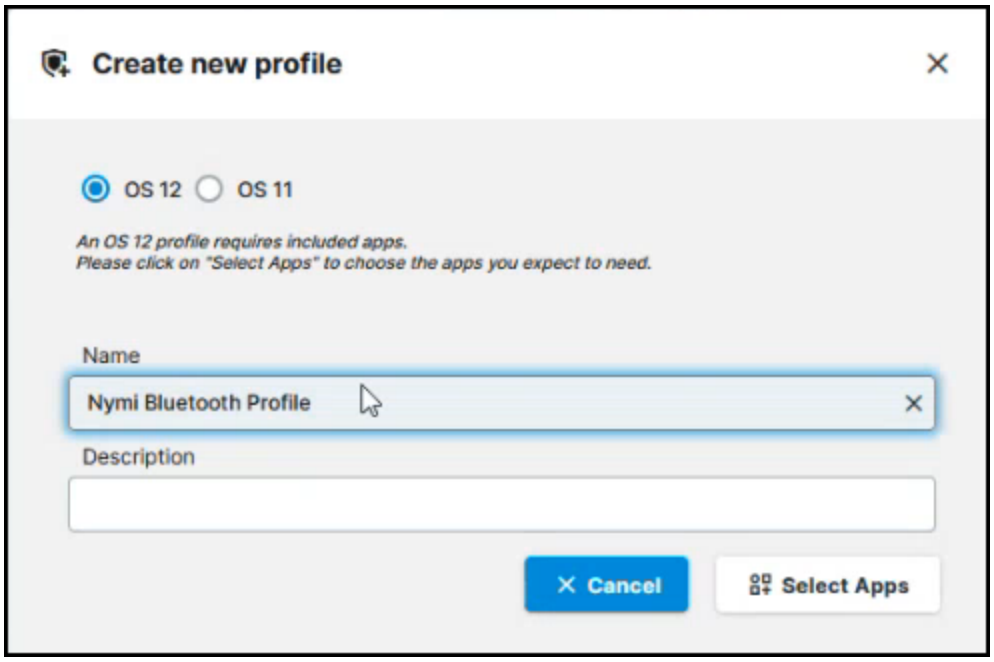


Figure 91. New Profile window

4. Click **OK**.

   The **Setup** window opens.

5. Navigate to **System > Firmware Customization > Custom Partition > Partition**.

6. Unlock the **Enable Partition** setting by clicking the orange triangle so that it turns blue, and then select **Enable Partition**.

7. Unlock the **Size** setting by clicking the orange triangle so that it turns blue. For the size value, type `120M`, as shown in the following figure.

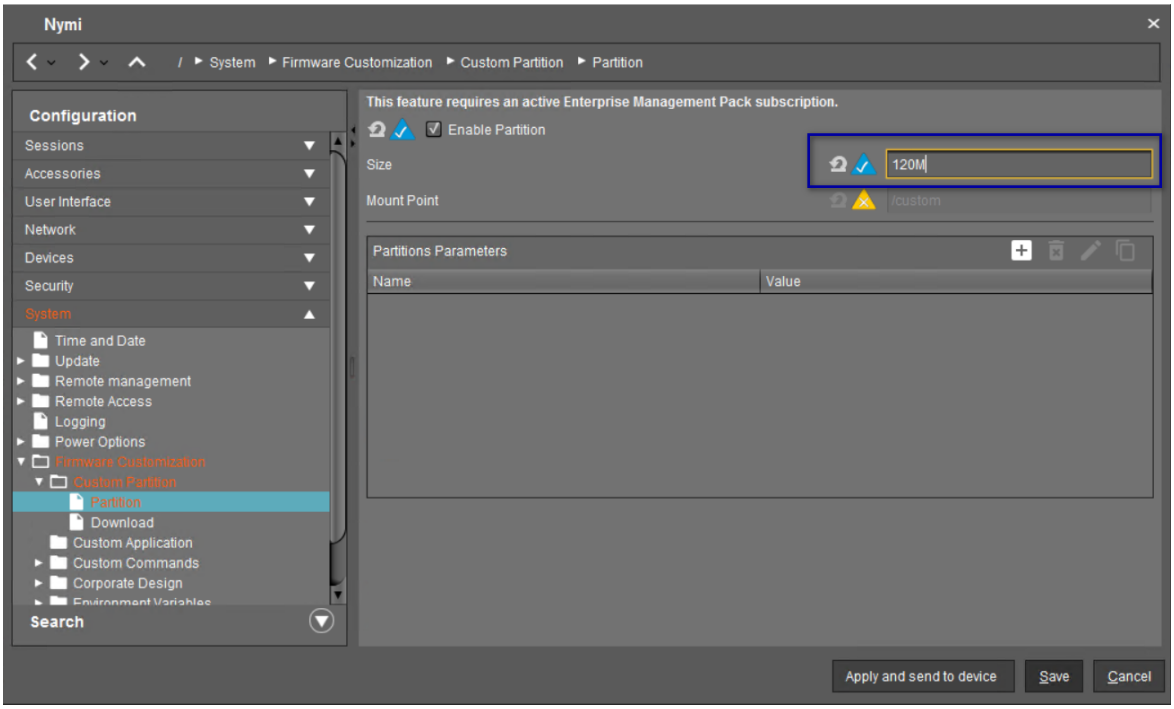


Figure 92. Set UMS partition size

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.

    a. In the **Name** field, type `AGENT_URL`.

    b. In the **Value** field, type `ws://agent_host:9120/socket/websocket`

       where `agent_host` is the IP address of the server on which you installed the Nymi Agent.

    c. Click **Confirm**.

       The following figure provides an example of **Nymi** partition window.

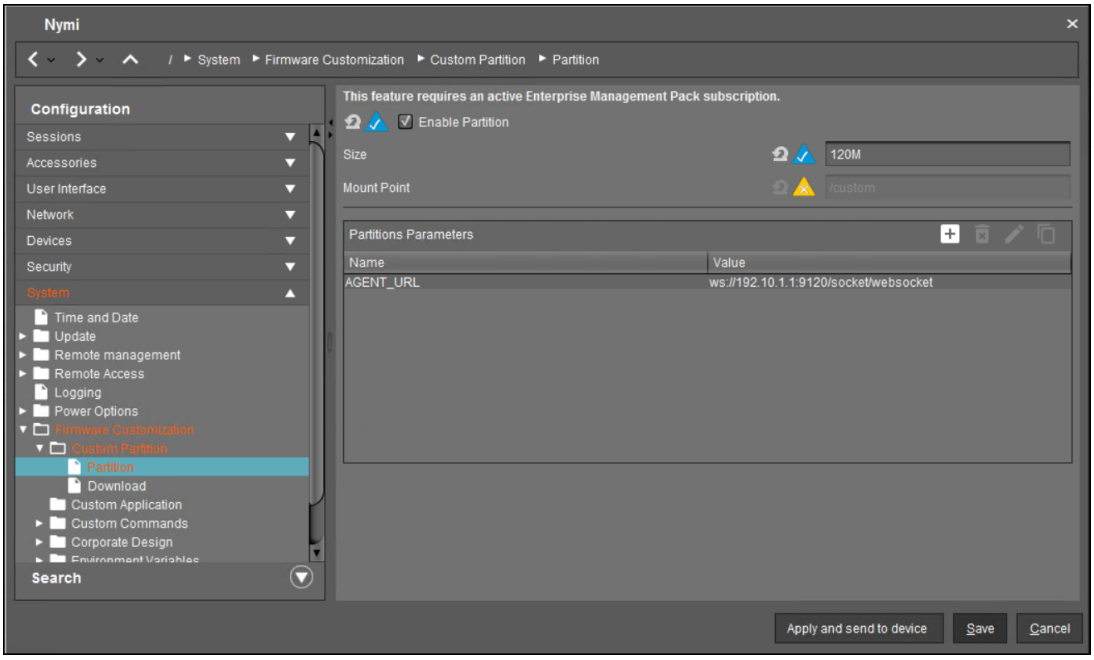


Figure 93. Partition window

d. Click **Save**.

e. On the **Update time** window click **On Reboot** and then click **Confirm**.

Customizing the Custom Partition

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

About this task

Procedure

1. Double-click the **Nymi** profile.
2. From the **Configuration** navigation pane for the partition, expand **System > Firmware Customization > Custom Commands > Base**, as shown in the following figure.

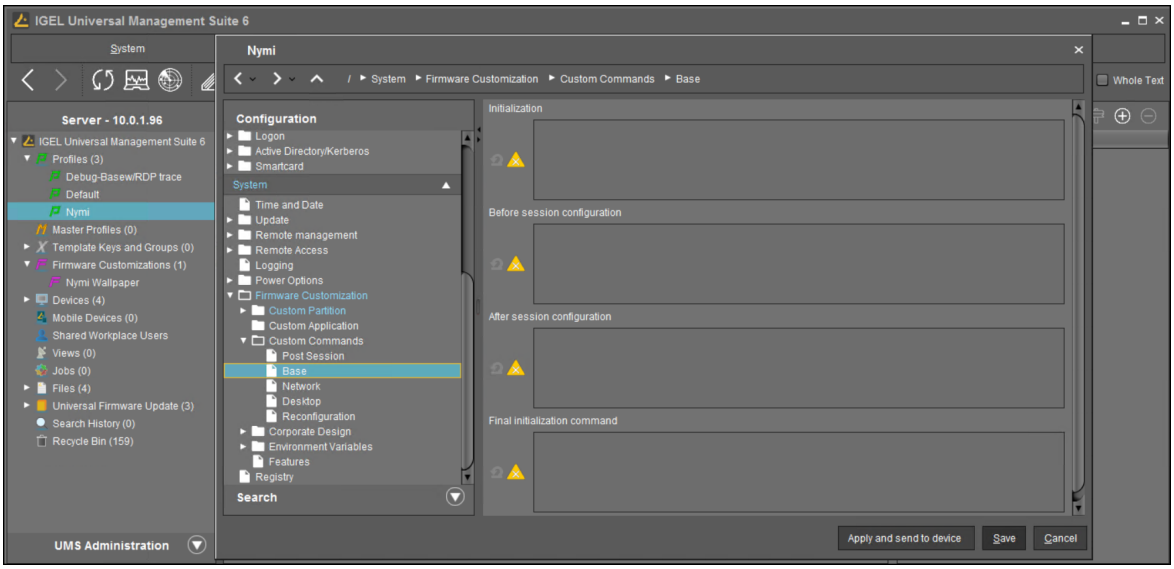


Figure 94. Base menu option

A dialog box appears.

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 "nymi: Initializing USB driver" | logger -it "nymi"
    ```

    ```
    modprobe cdc-acm
    ```

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

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

    ```
    /custom/nymi/usr/lib/nymi/nbedstart&
    ```

    ```
    systemctl enable /custom/nymi/etc/systemd/system/
    Nymi.service
    ```

    ```
    systemctl start Nymi.service
    ```

    e. Click **Save**.

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

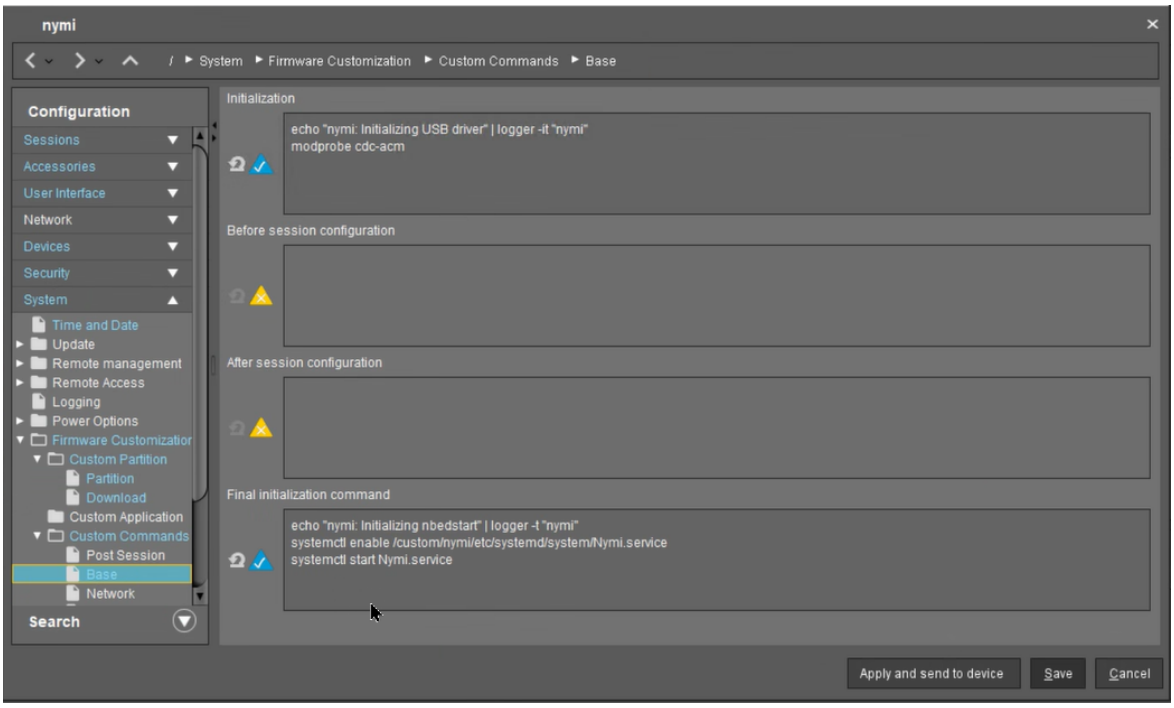


Figure 95. Nymi Base Commands

4. Double-click the **Nymi** profile.
5. From the **Configuration** navigation pane for the partition, expand **System > Firmware Customization > Custom Partition > Download**, as shown in the following figure.

   The following figure provides an example of the **Download option**.

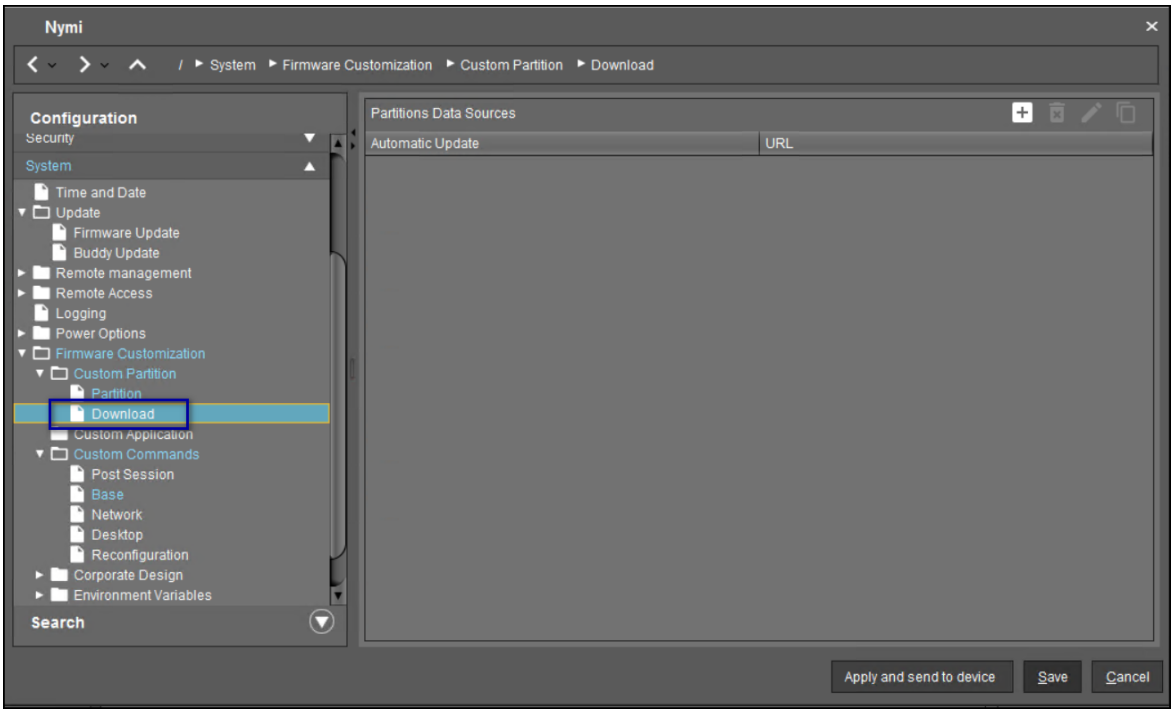


Figure 96. Downloads

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

   A dialog box appears.

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

   a. In the **URL** field, type the Download URL path for the `nymi.inf` file.

      For example, `https://10.0.1.61:8443/ums_filetransfer/nymi.inf`

   b. In the **Username** field, type the username of a user that has access to the UMS file transfer location.

   c. In the **Password** field, type the password for the user account that has access to the UMS file transfer location.

   d. In the **Final Action** field, type `/custom/nymi/custompart-nymi init`.

   e. Click **OK**.

   The following figure provides an example of the **Add** window.

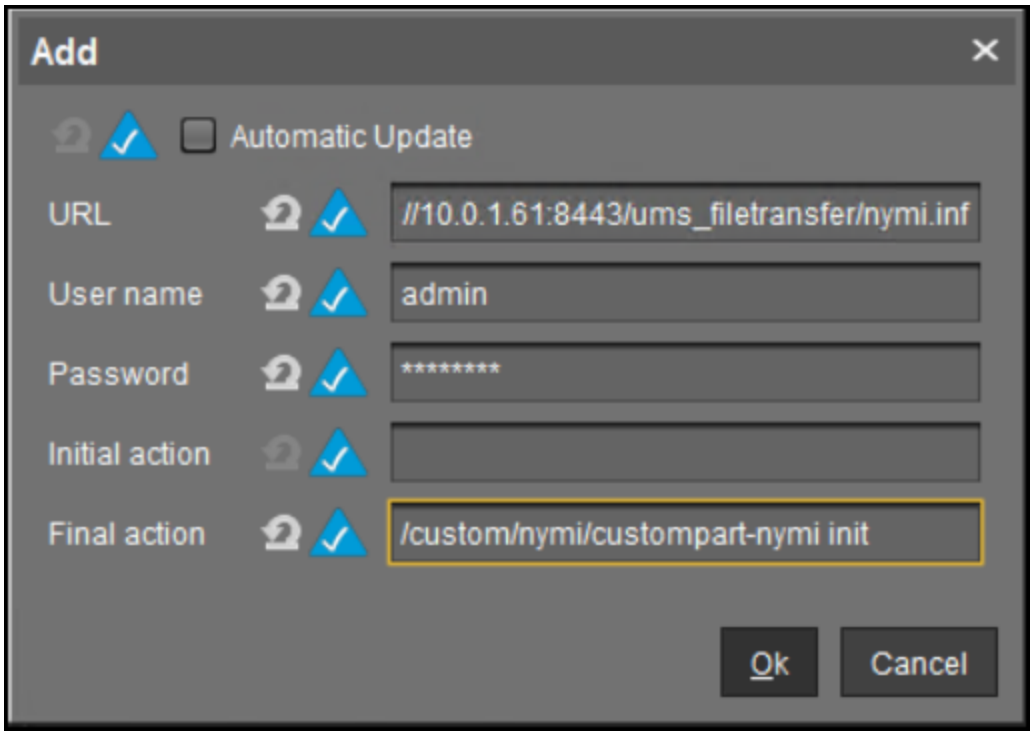


Figure 97. Add window

8. Click **Save**.

Assigning the Profile to iGel Devices

Assign the Nymi profile to the IGEL devices.

About this task

Perform the following steps in the UMS Console.

Procedure

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

The **Select Assignable Objects** window appears, as shown in the following figure.

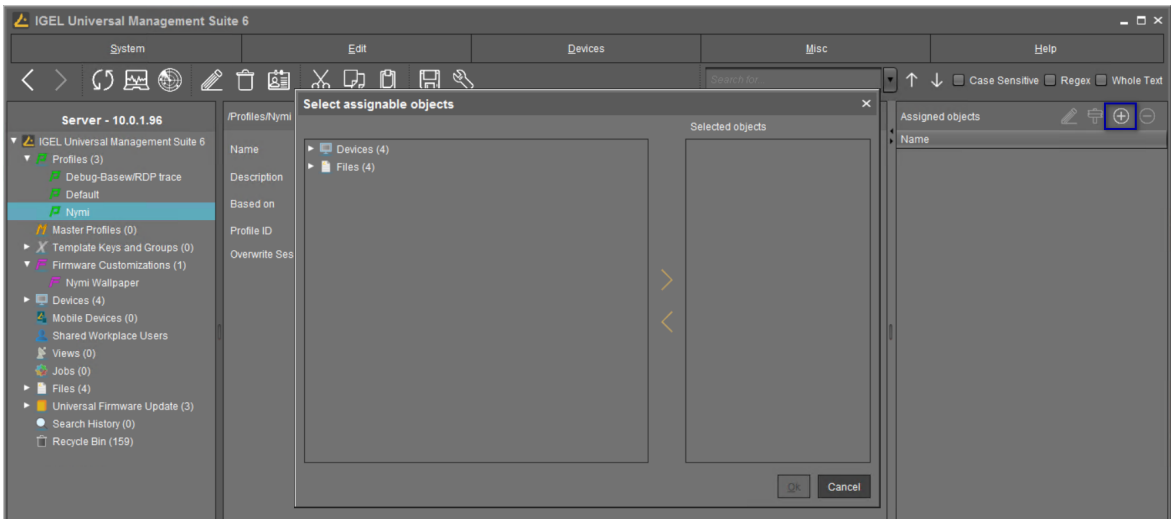


Figure 98. Select Assignable Objects window

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, as shown in the following figure.

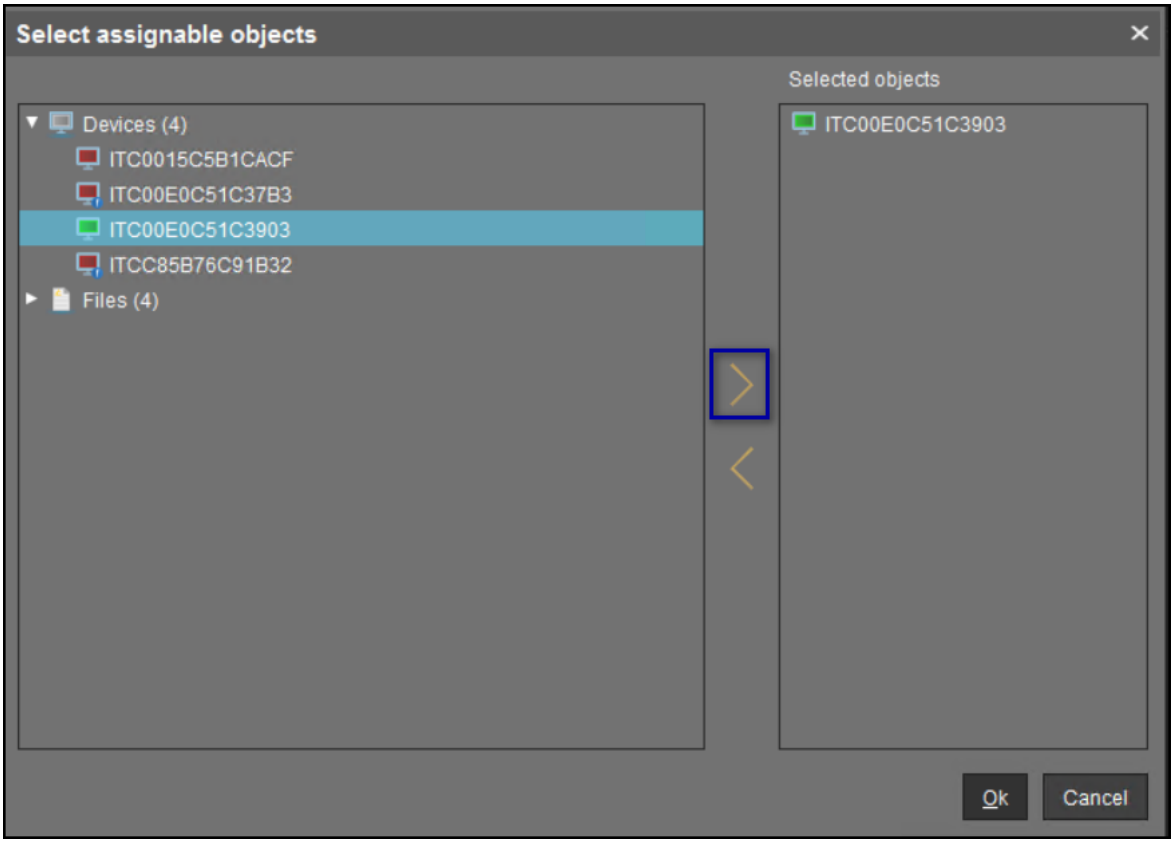


Figure 99. Selected Objects

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

   The following figure provides an example of the **Update time** window.

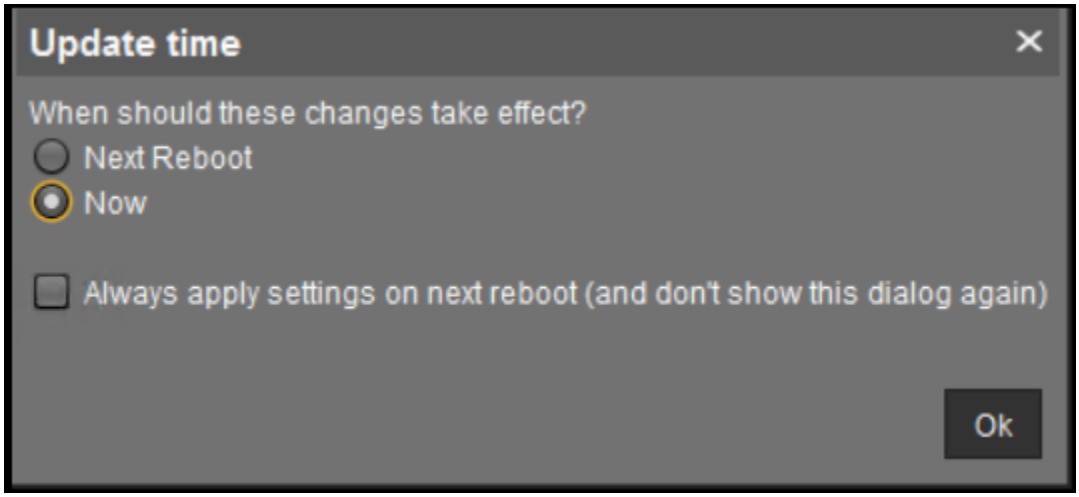


Figure 100. Update time window

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

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

6.3.2.8 (iGEL 12) Installing Nymi Bluetooth Endpoint

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

Uploading Nymi Packages to Universal Management Suite

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

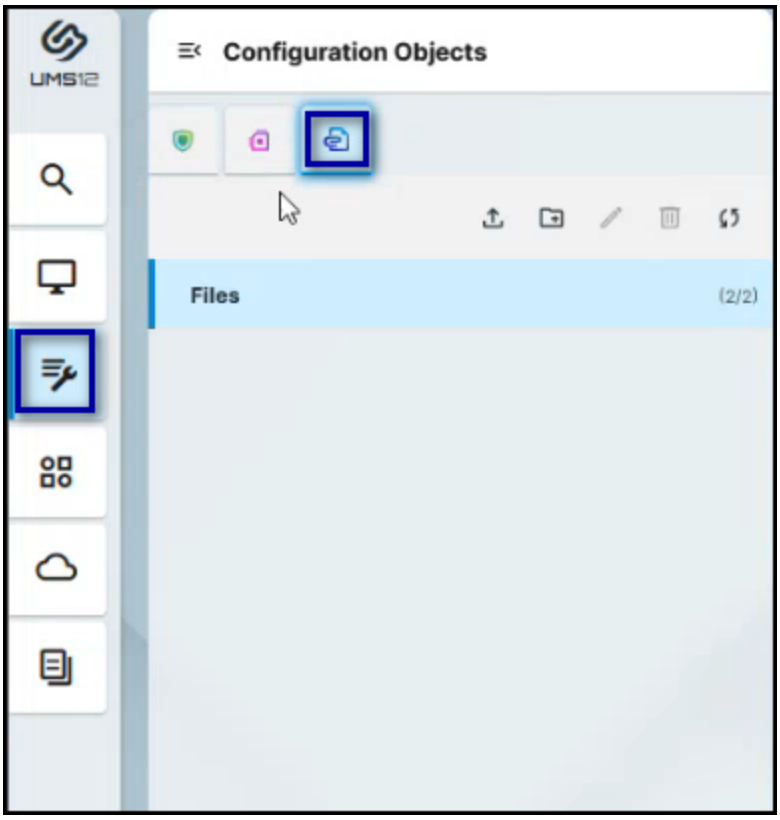
About this task

Obtain the installation package from Nymi.

Procedure

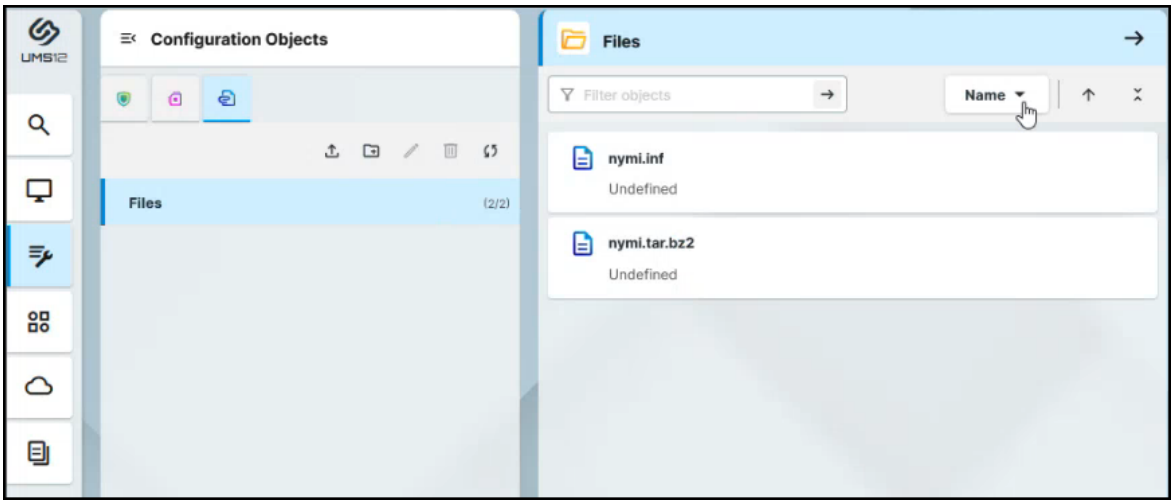
1. Extract the installation package to a machine that has access to the **UMS Web App**.
2. Connect to the **UMS Web App**, in the left navigation pane click **Configuration**, and then **Configuration** pane, click the **Files** button.

   The following figure highlights the **Configuration** option and the **File** 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, as shown in the following figure.



Creating a Profile and Custom Partition

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

Procedure

1. In the **Configuration options** pane, click `New Profile`, as highlighted in the following figure.

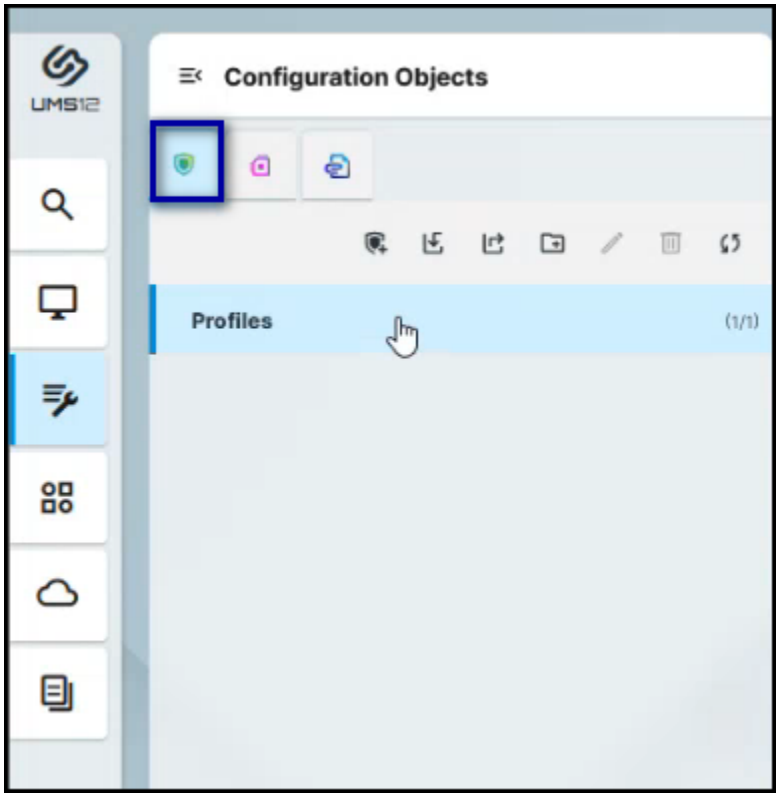


Figure 101. Create new profile option

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.

The following figure provides an example of the **New Profile** window.

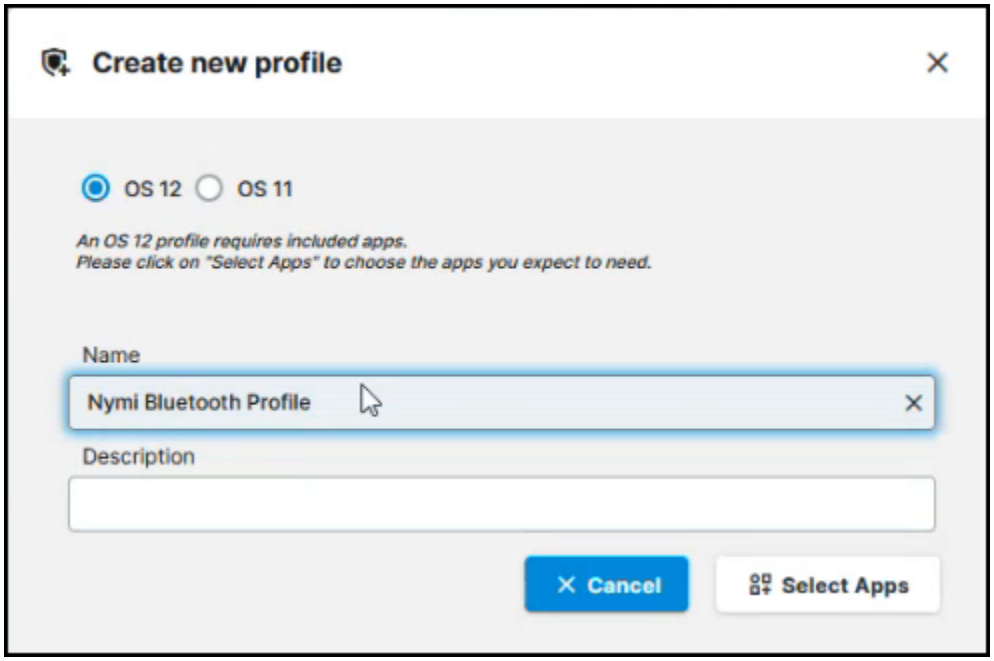


Figure 102. New Profile window

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

   The following figure provides an example of the window.

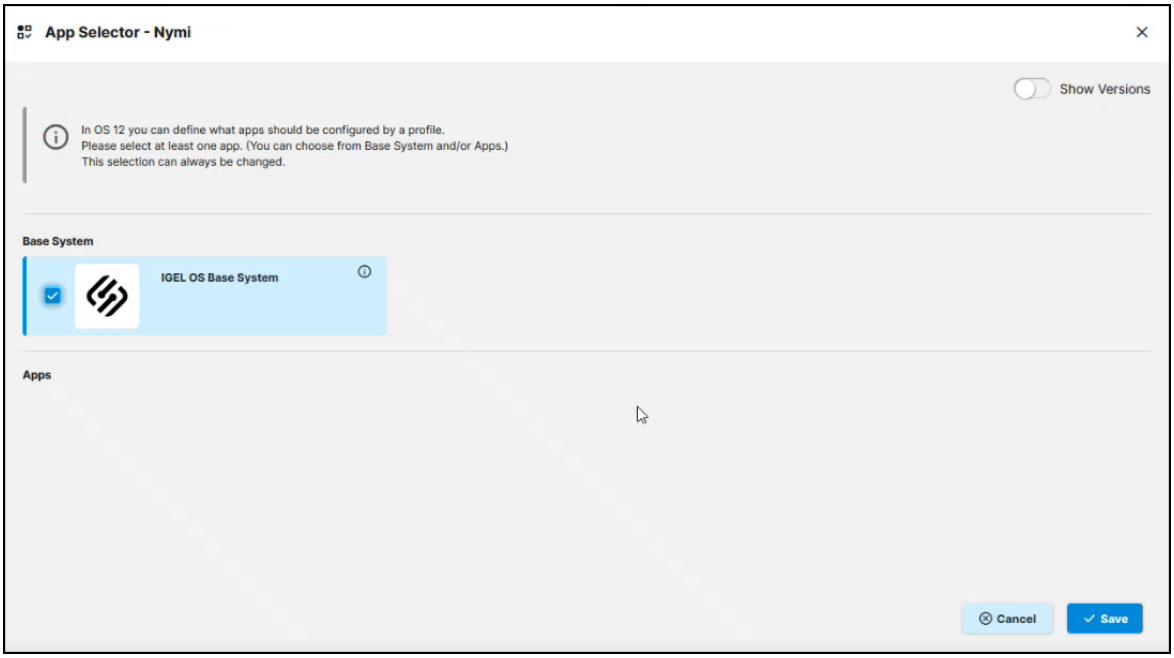


Figure 103. Select Apps window

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`, as shown in the following figure.

    c. Click the slider beside the **Mount Point** option, and then leave the mount point value as **/custom**.

    The following figure provides an example of the **Partition** window

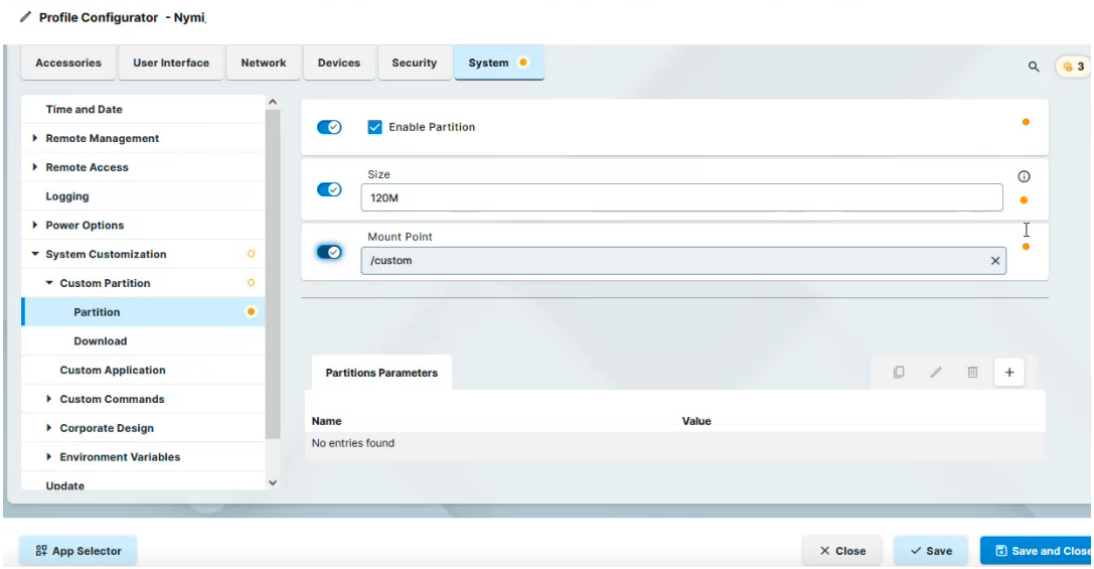


Figure 104. Set UMS partition size

d. In the **Partitions Parameters** section, click **[+]** (Add Item).

e. In the **Partition Parameters** window, perform the following actions.

   i. In the **Name** field, type `AGENT_URL`.

   ii. 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.

   iii. Click **Confirm**.

   The following figure provides an example of **Nymi** partition window.

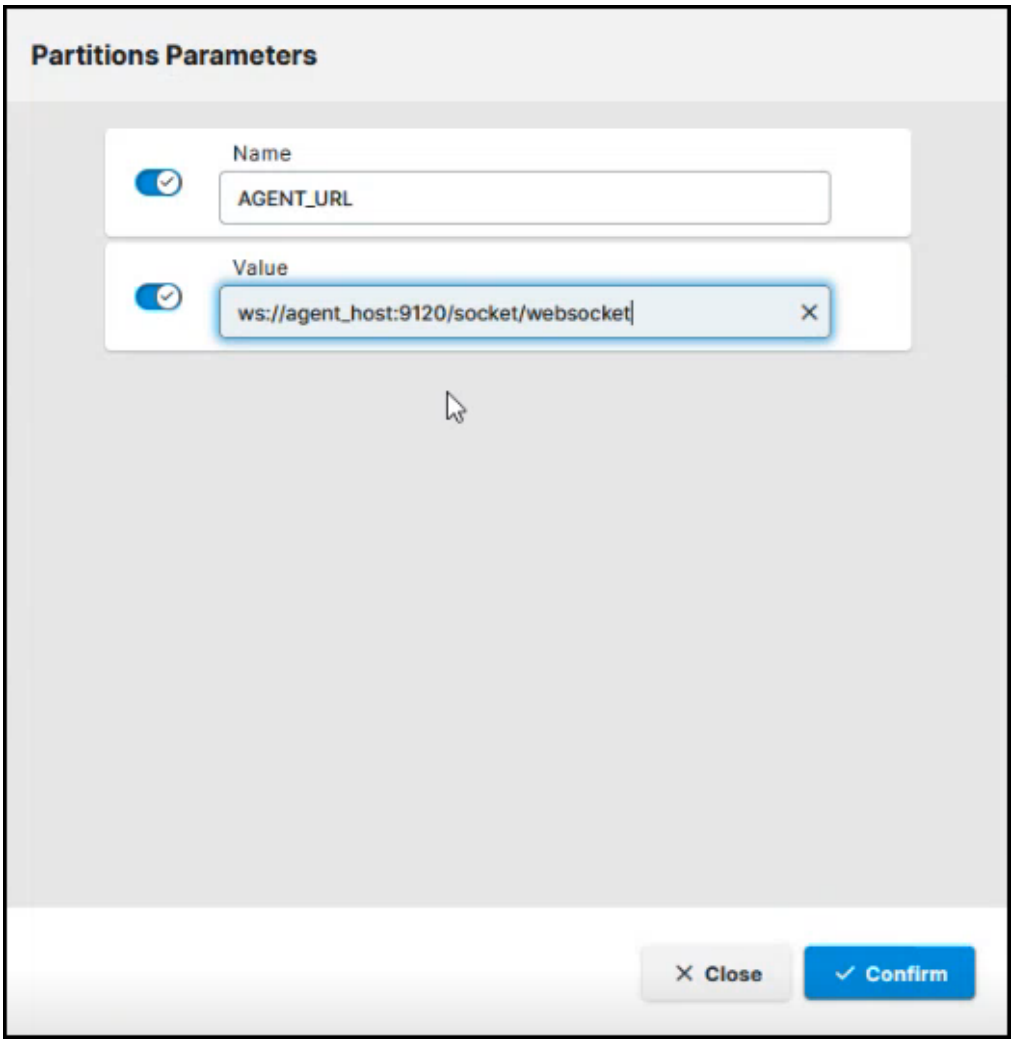


Figure 105. Partition Parameters window

iv. Click **Save and close**.

f. On the **Update time** window click **On Reboot**, and then click **Confirm**.

The following figure shows the **Update time** window.

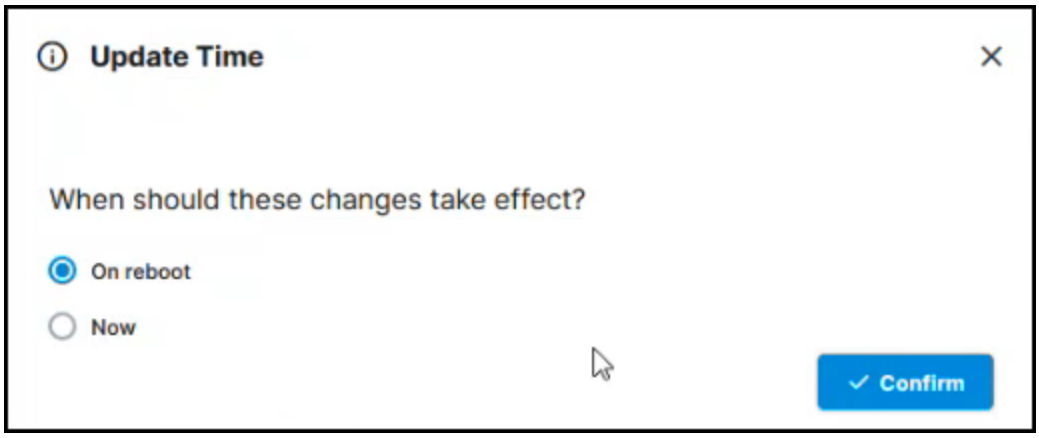


Figure 106. Update time window

Customizing 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.

About this task

Procedure

1. From the **System** menu option for the partition, expand **System Customization > Custom Parition > Custom Commands > Base**, as shown in the following figure.

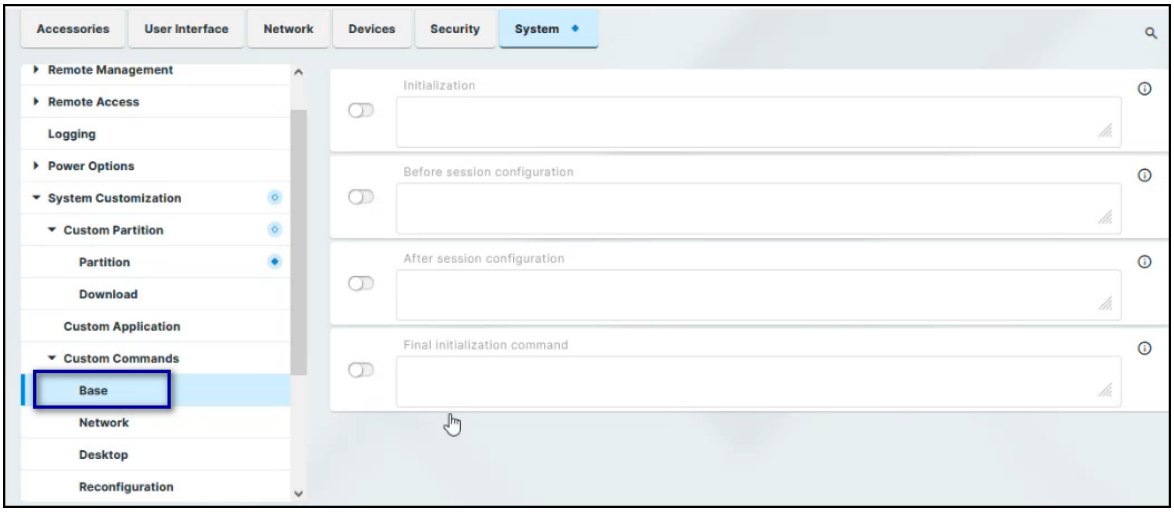


Figure 107. Base menu option

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 "nymi: Initializing USB driver" | logger -it "nymi"
    ```

    ```
    modprobe cdc-acm
    ```

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

    ```
    /custom/nymi/usr/lib/nymi/nbedstart&
    ```

    ```
    systemctl enable /custom/nymi/etc/systemd/system/
    Nymi.service
    ```

    ```
    systemctl start Nymi.service
    ```

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

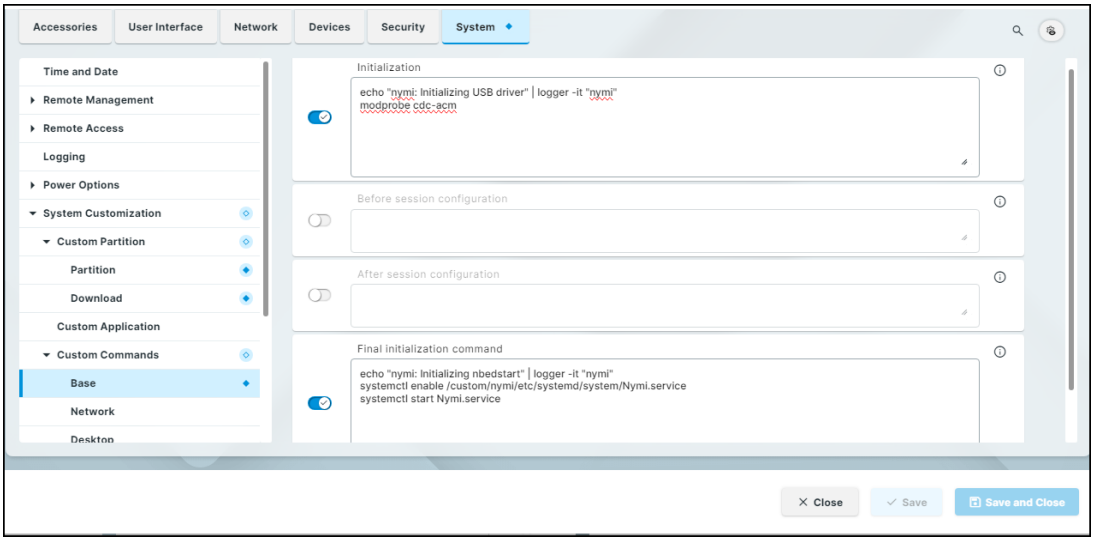


Figure 108. Nymi Base Commands

c. Click **Save**.

3. From the left navigation pane for the partition, expand **System Customization > Custom Commands > Download**, as shown in the following figure.

   The following figure provides an example of the **Download option**.

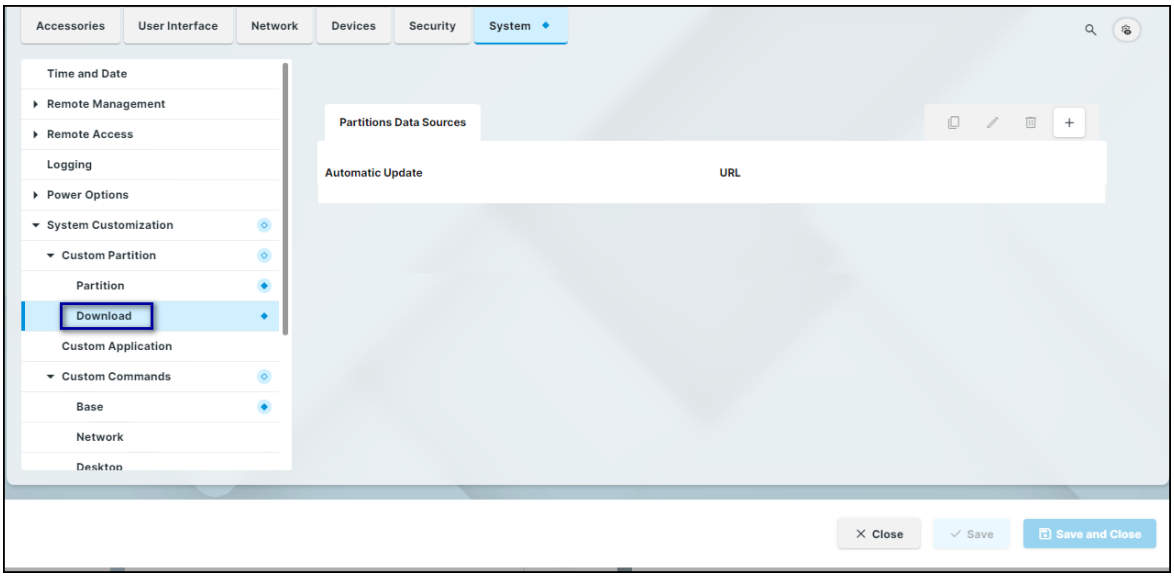


Figure 109. Download

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

   A dialog box appears.

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

    a. In the **URL** field, type the Download URL path for the `nymi.inf` file.

    For example, `https://10.0.1.61:8443/ums_filetransfer/nymi.inf`

    b. In the **Username** field, type the username of a user that has access to the UMS file transfer location.

    c. In the **Password** field, type the password for the user account that has access to the UMS file transfer location.

    d. In the **Initial Action** field, type `/custom/nymi/custompart-nymi init`.

    e. In the **Final Action** Field, type `/custom/nymi/custompart-nymi stop`

    f. Click **Confirm**.

    The following figure provides an example of the **Partition Data Sources** window.

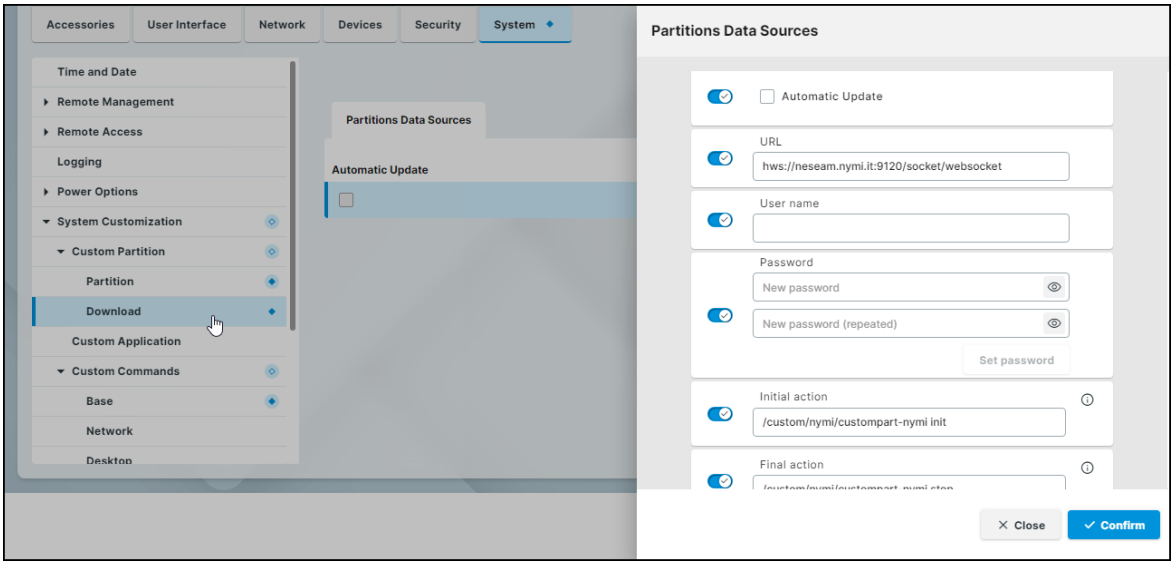


Figure 110. Partition Data Sources window

6. Click **Confirm**.

7. Click **Save and close**.

8. On the **Update time** window click **On Reboot**, and then click **Confirm**.

The following figure shows the **Update time** window.

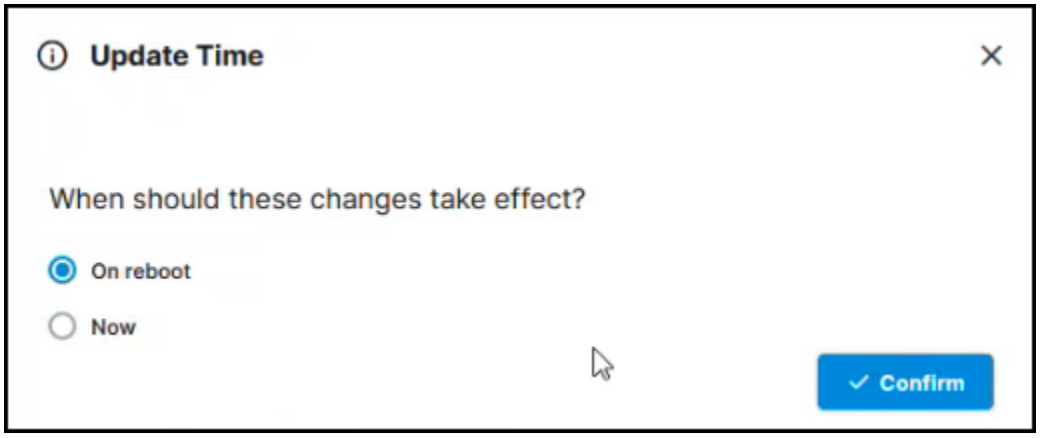


Figure 111. Update time window

Assigning the Profile to iGel Devices

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

Procedure

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, as highlighted in the following figure.

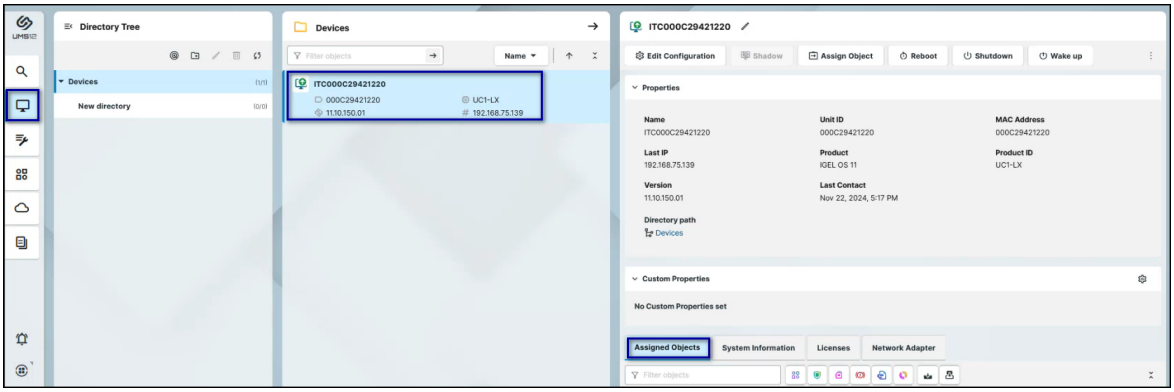


Figure 112. Assigned Devices option

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, as shown in the following figure.

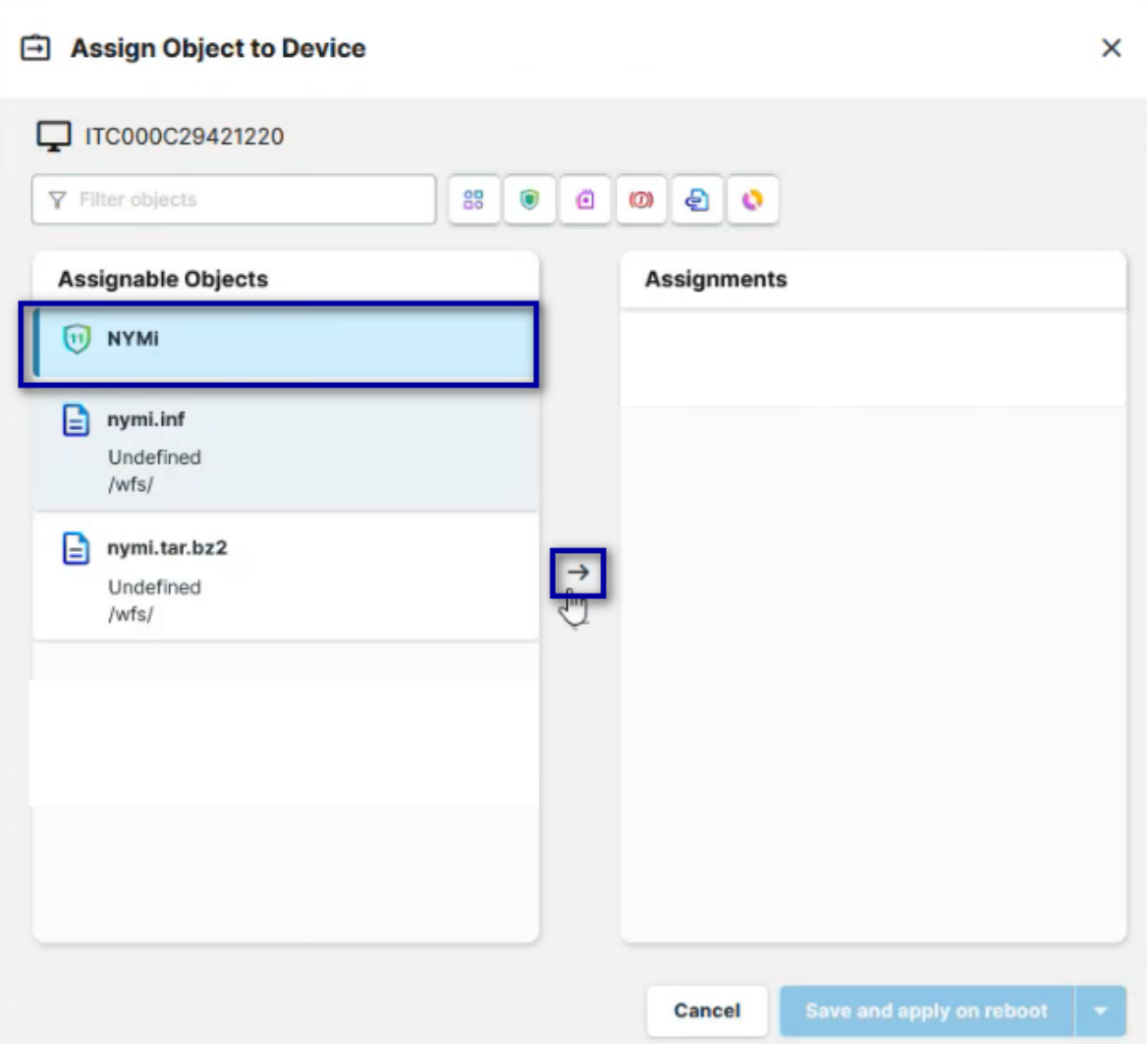


Figure 113. Selected Objects

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

   The **Assigned Objects** section displays the Nymi profile, as shown in the following figure.

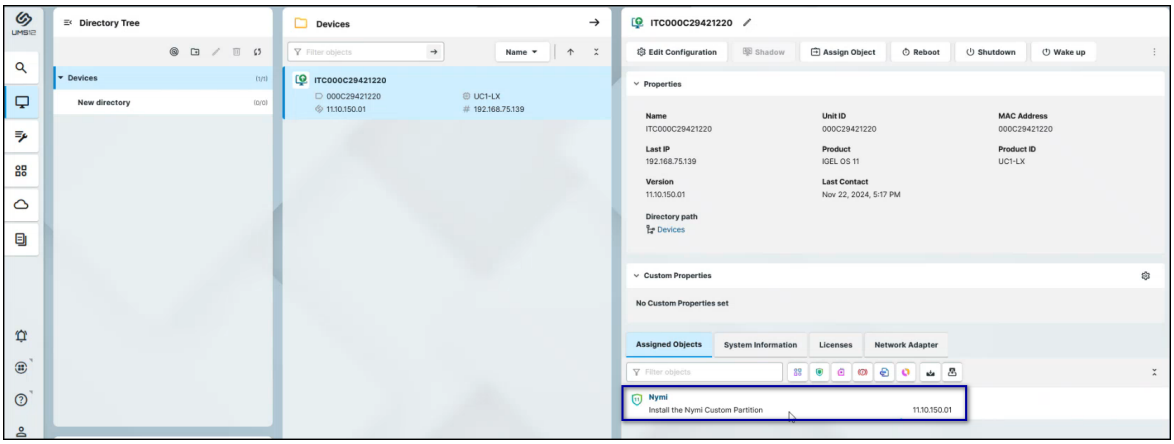


Figure 114. Assigned device

4. Reboot the IGEL client.

6.3.2.9 Configuring the Connected Worker Platform Communication Protocol

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

About this task

Perform the following steps on all user terminals (for Evidian environments on Wearable user terminals only) where users access Nymi-Enabled Applications(NEAs) 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.

Procedure

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 the perform the following actions:

    a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`

    b. In the **Variable Value** field, type `0`.

    The following figure provides an example of the new variable.

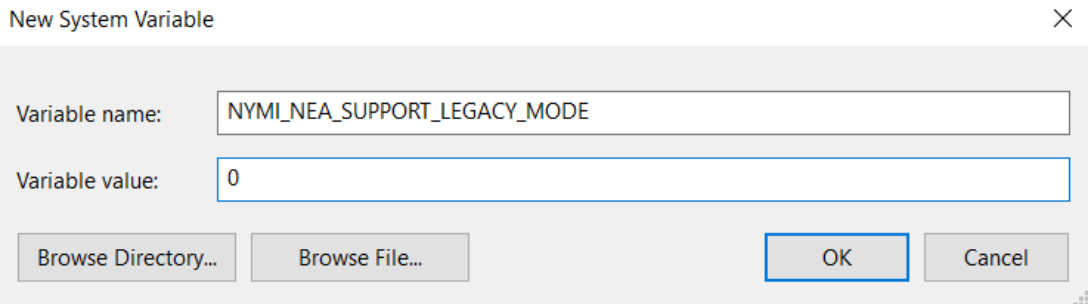


Figure 115. New System Variable window

    c. Click **OK**.

6.3.3 Set Up User Terminals for Lock and Unlock

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 for NES (when the Root CA that issued the certificate is not a trusted CA).
- Insert the Nymi-supplied Bluetooth adapter into an available USB port.
- Install the Nymi Bluetooth Endpoint service.
- Install the Nymi Lock Control software
- Configure the Nymi Bluetooth Endpoint configuration file.

6.3.3.1 Configuring Nymi Lock Control

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

About this task

By default Nymi Lock Control is not enabled.

Procedure

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.

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. When the Nymi Band is out of range, a 10 second timer appears on the desktop. If the Nymi Band does not return within close range of the user terminal, the terminal will lock. Ensure that your Group Policy Object(GPO) settings do not push the Do not display the lock screen configuration option to the Nymi Lock Control user terminals. **Note:** Edit the `nbe.toml` file to define close proximity for Nymi Lock Control. Refer to Editing the nbe.toml File in the Nymi Connected Worker Platform—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. 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 `nbe.toml` file. The Editing the nbe.toml File section in the Nymi Connected Worker Platform—Deployment Guide provides more information. ◦ 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 user terminal by pressing the **Enter** key or space bar on the keyboard when the authenticated Nymi Band is within Bluetooth range, but not in close proximity of the user terminal.
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**.

Results

During enrollment the Nymi Band Application updates the Nymi Band to enable Nymi Lock Control support.

Changing this option does not change the Nymi Band behaviour for existing enrolled Nymi Band until the user logs into the Nymi Band Application while wearing their authenticated Nymi Band.

When the Nymi Band Application updates on the Nymi Band completes, restart Nymi Lock Control.

6.3.3.2 Importing the Root CA Certificate in Citrix/RDP Environments

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

About this task

While logged into the user terminal as a local administrator, use the **certlm** application to import the root CA certificate into the Trusted Root Certification Authorities store.

Procedure

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

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

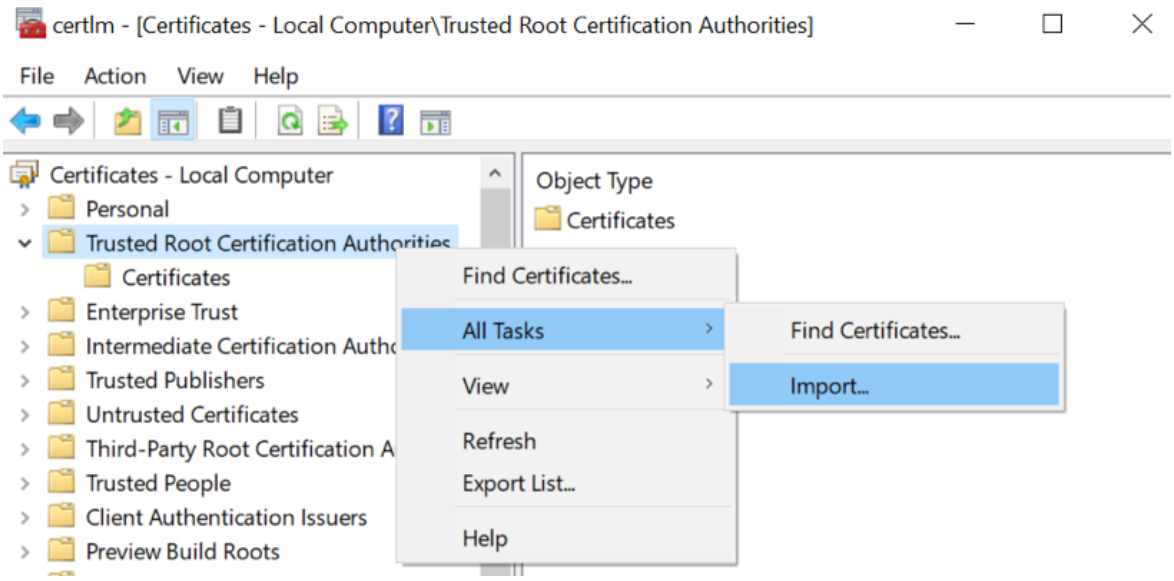


Figure 116. certlm application

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

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

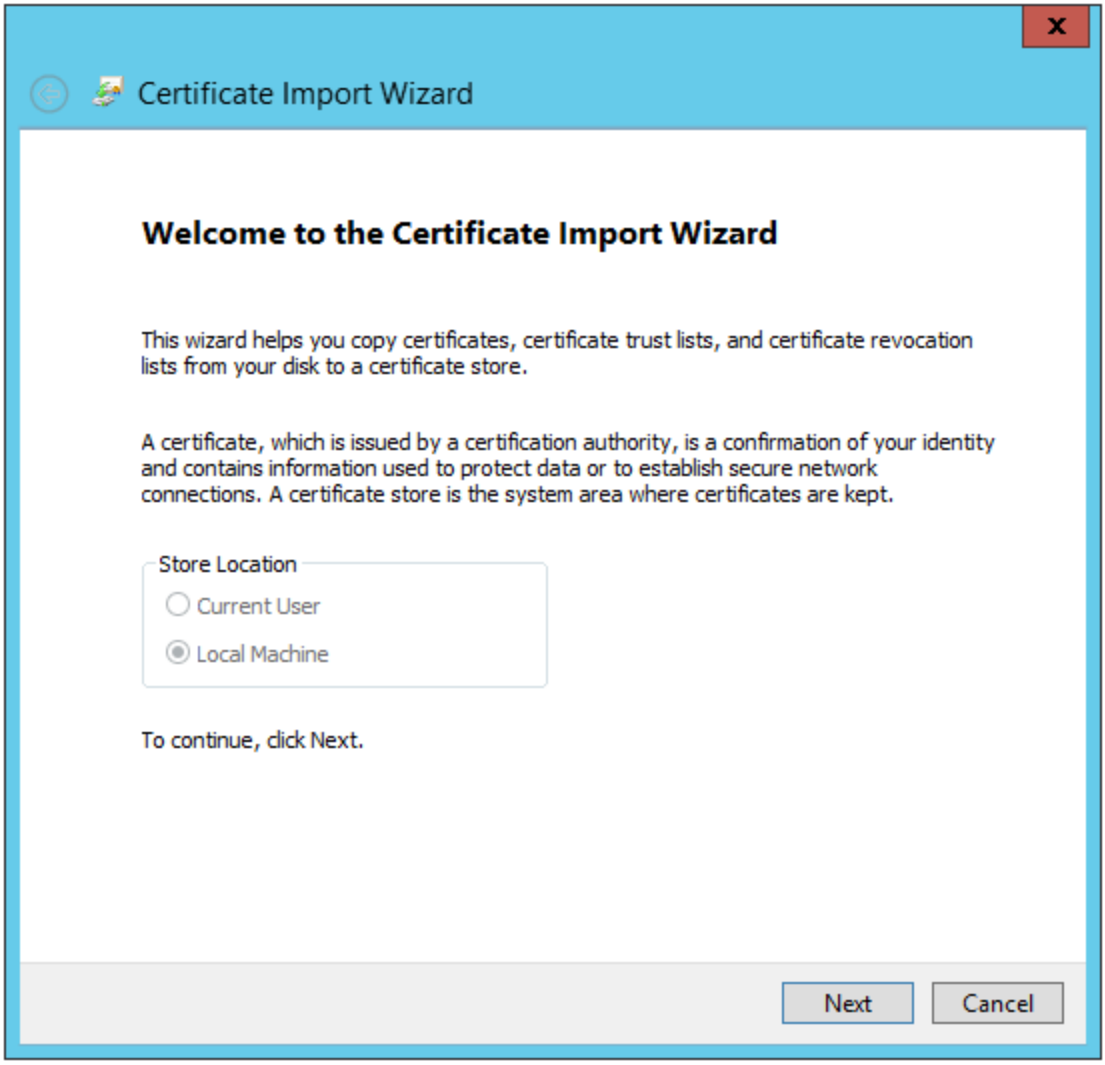


Figure 117. Welcome to the Certificate Import Wizard screen

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.

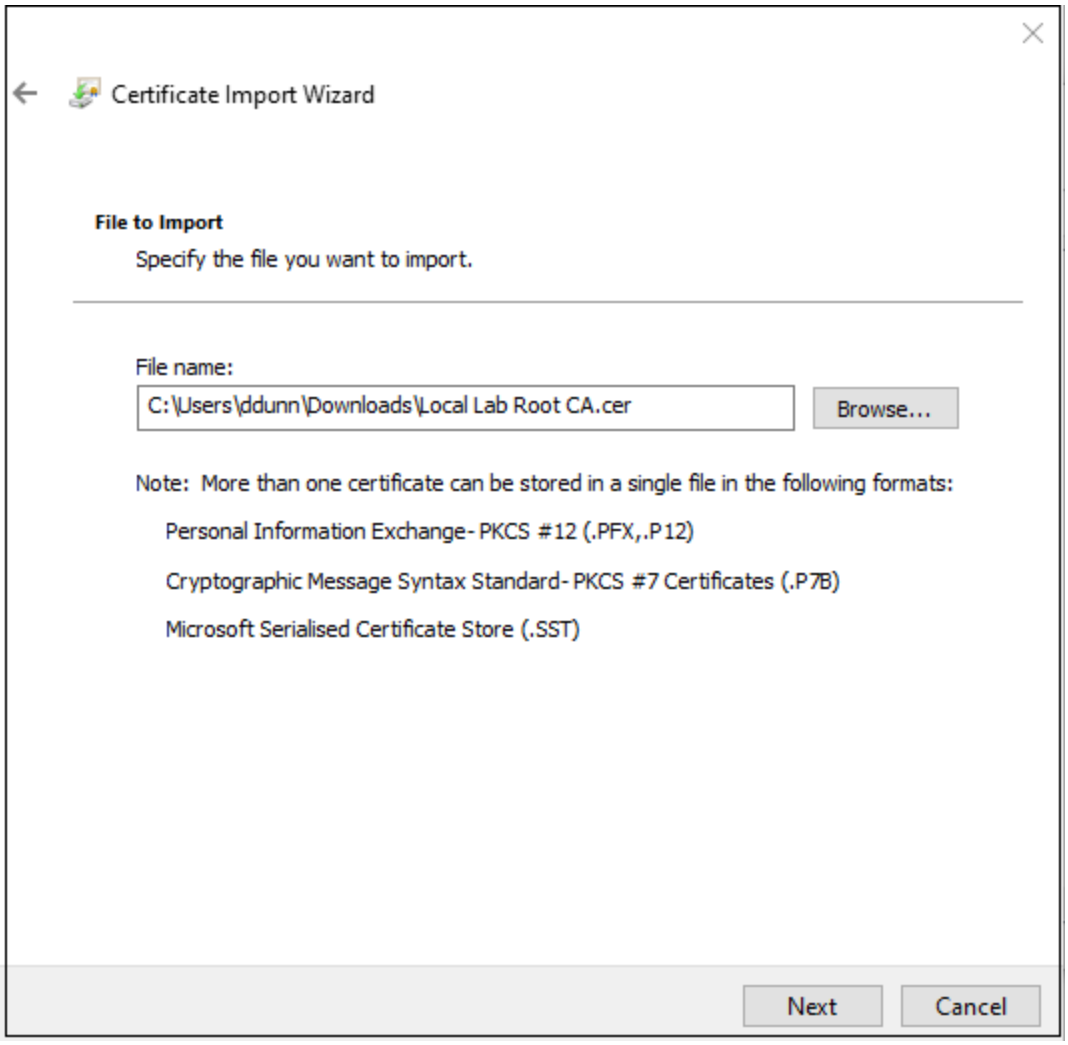


Figure 118. File to Import screen

6. On the **Certificate Store** screen, accept the default value **Place all certificates in the following store** with the value **Trusted Root Certification Authorities**, and then click **Next**.
7. On the **Completing the Certificate Import Wizard** screen, click **Finish**.
8. From the **Windows Start Menu**, type `Manage Computer`, and then select **Manage Computer Certificates**.

   The **certlm** window appears.
9. Navigate to **Personal > Certificates** folder.

   A list of certificates displays.
10. On the **User Account Control** dialog, click Yes.

11. Select the **Security** tab and then click the **Add** button.
12. In the new window, click **Add**, which opens the **Select Users, Computers, Service Accounts, or Groups** window.
13. In the **Permissions** area, under **Allow** column, select the **Read** permission.

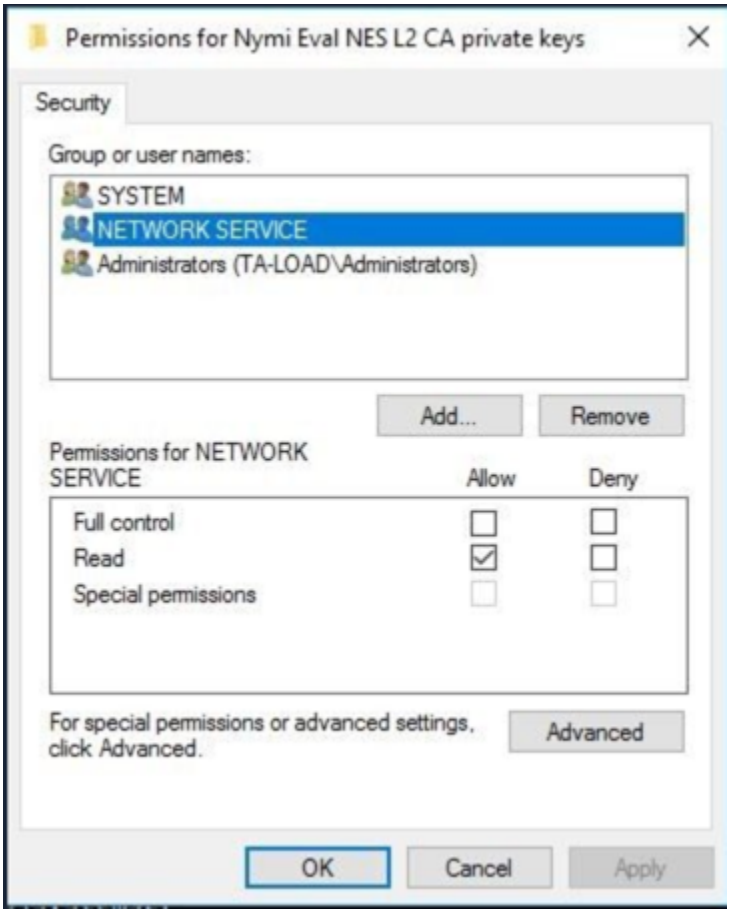


Figure 119. Setting Private Key Permissions

14. Click **OK**.

6.3.3.3 Installing Nymi Lock Control

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

About this task

Procedure

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**, as shown in the following figure, and then click **Next**.

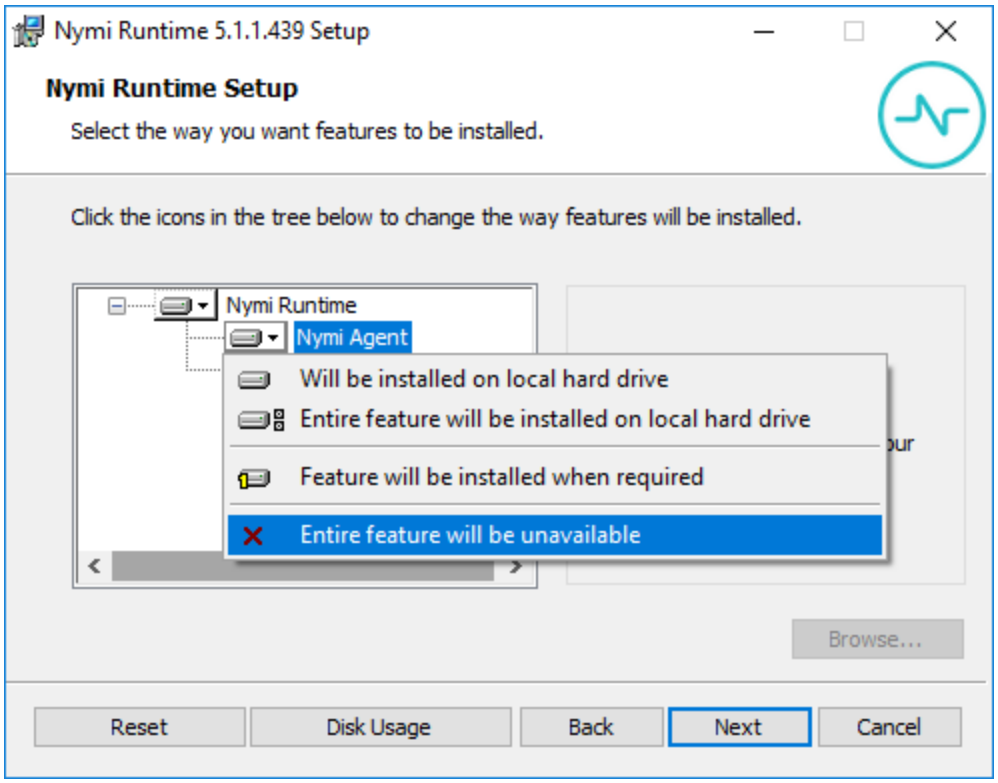


Figure 120. Nymi Agent feature will be unavailable

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.

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

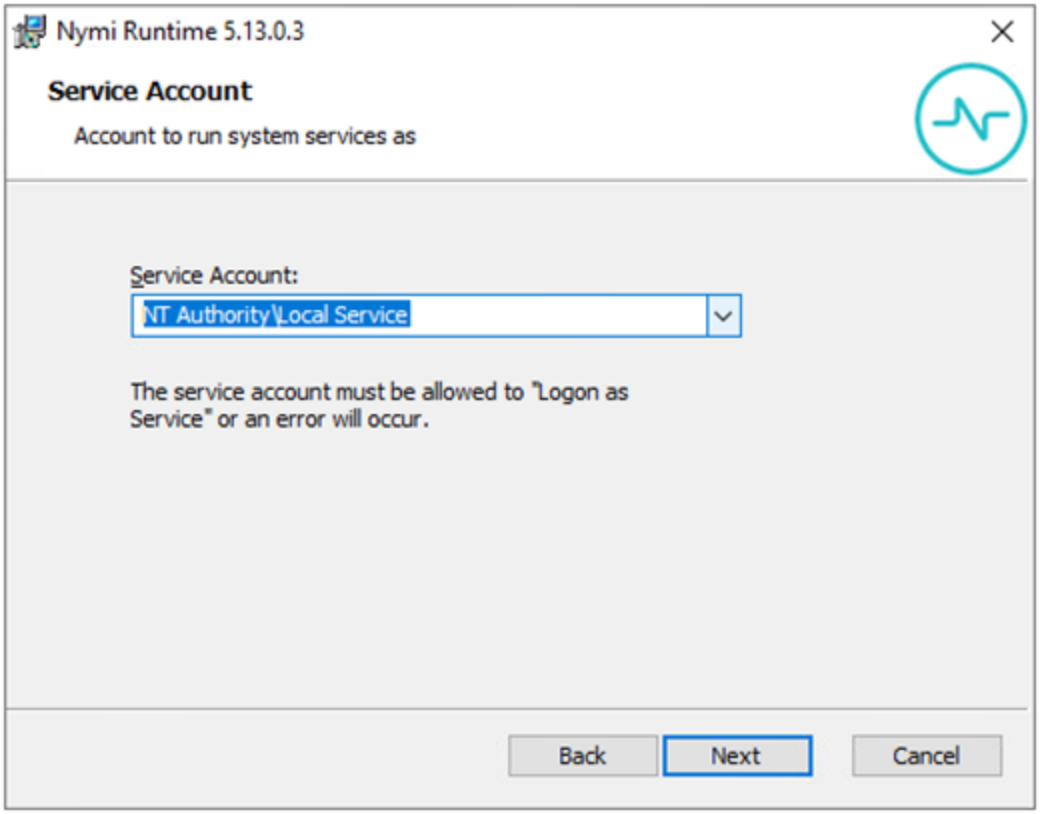


Figure 121. Nymi Runtime Service Account window

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, perform the following actions:
    a. To change the installation location, click **Browse**, navigate to a new installation folder, and then click **Select Folder**
    b. To keep the default installation location, click **Next**.
15. On the **Ready to Install** window, click **Install**.
16. On the **Completing the Nymi Lock Control Setup Wizard** window, click **Finish**.

6.3.3.4 (Windows and HP Thin Pro) Editing the Nymi Bluetooth Endpoint Configuration File

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

About this task

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

Procedure

1. Make a copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.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 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, or click the start button on the toolbar. Enter “Services” in the search bar. The Services application window appears.
   b. Search for **Nymi Bluetooth Endpoint** in the Services application.
   c. Right-click **Nymi Bluetooth Endpoint** and restart it.

   On HP Thin Pro:

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

6. On HP Thin Pro only, revert the file system to read-only access.

   a. Open **X Terminal**.

   b. Type:

   ```
   fslock
   ```

   c. Close the terminal.

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

What to do next

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

6.3.3.5 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.

Starting in Connected Worker Platform 1.21.0, the Nymi software supports two types of Bluetooth Adapters, the Bluegiga BLED112 Adapter and the BleuIO Adapter.

The `C:\Nymi\Bluetooth_Endpoint\nbe.toml` and `/usr/bin/nbe.toml` include two different sections where you can define RSSI parameters:

Section Name	Bluetooth Adapter Type	Bluetooth Adapter Image
`[dongle.bluegiga]`	Bluegiga BLED112 Adapter	
`[dongle.nymi]`	BleuIO Adapter	

Section Name	Bluetooth Adapter Type	Bluetooth Adapter Image
		

Note: Consider the following for IGEL:

- Specify all RSSI parameter names in capital letters.
- Use the Bluegiga BLED112 Bluetooth Adapter only.

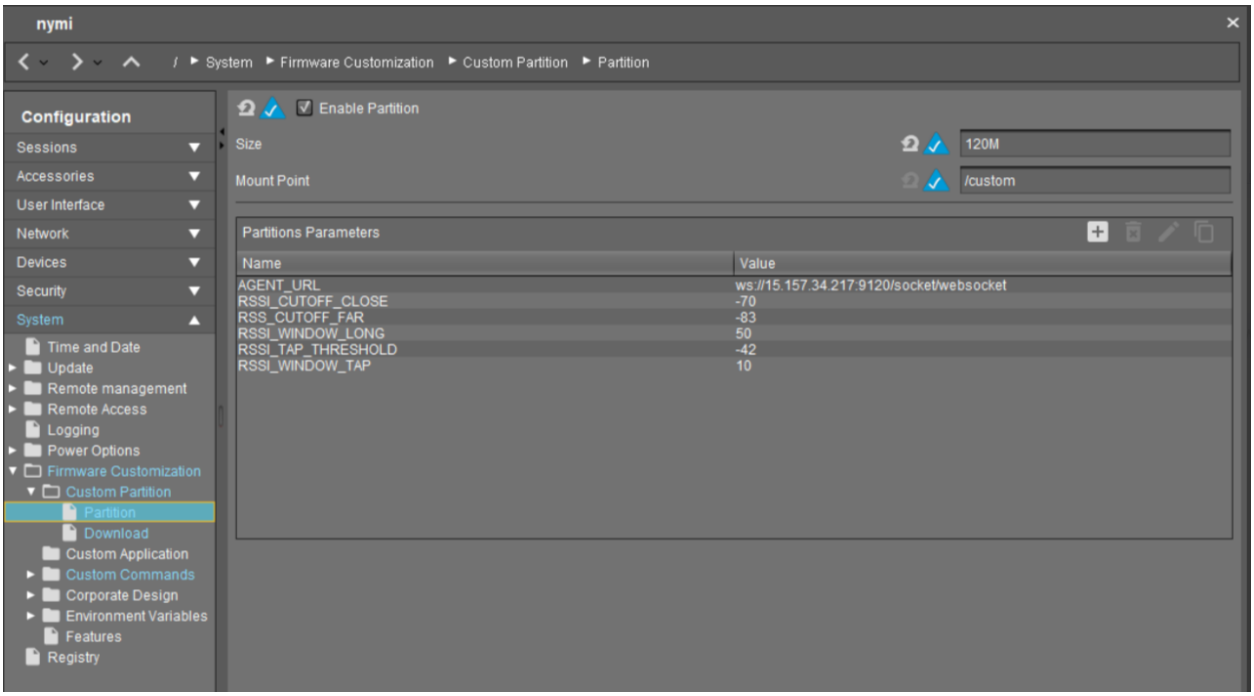
The following table provides a list of supported RSSI parameters, their default values and the purpose of each parameter.

Table 6. RSSI Values

RSSI Parameter	Default Value	Description
`rssi_window_tap`	Bluegiga: 10; BleuIO: 12	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 of the Bluetooth Adapter and decreases the sensitivity.
`rssi_window_long`	Bluegiga: 50; BleuIO: 55	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 **keep unlocked when present**,

RSSI Parameter	Default Value	Description
		lock when away, or **unlock when present**.
`rssi_tap_threshold`	Bluegiga: -42; BleuIO: -35 (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. Suggested threshold between -20 (strict) and -35 (relaxed). 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 `rssi_tap_threshold`, for the duration of time that is defined by `rssi_window_tap`, a BLE tap is performed.
`rssi_cutoff_close`	Bluegiga: -70; BleuIO: -68 (must be 0 or negative)	This determines the outer range of the close distance-threshold (excluding tap distance) for Nymi Lock Control. Enter 0 to bypass the proximity functionality of Nymi Lock Control. If the Nymi Band maintains a close distance to the BLE radio antenna and the RSSI values measured are within the `rssi_cutoff_close` value, Nymi Lock Control keeps the user terminal unlocked. If the Nymi Band moves away from the BLE radio antenna, and the RSSI values measured are on a decreasing trend and goes from the `rssi_cutoff_close` value to the `rssi_cutoff_far` value, Nymi Lock Control locks the user terminal.
`rssi_cutoff_far`	Bluegiga: -83; BleuIO: -80 (must be negative)	This determines the outer range of the far distance-threshold (excluding tap distance) for Nymi Lock Control. If the Nymi Band moves towards the BLE radio antenna, and the RSSI values measured are on an increasing trend and goes from the `rssi_cutoff_far` value to the `rssi_cutoff_close` value, Nymi Lock Control unlocks the user terminal.

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



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

6.3.3.6 Setting the NES URL

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

About this task

Procedure

1. Run `regedit.exe`
2. On the **User Account Control** window, click **Yes**.
3. Navigate to **HKEY_LOCAL_MACHINE > Software**.
4. Right-click **NES**, and then select **New > String value**.

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

   where:

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

6.3.3.7 Configuring the Connected Worker Platform Communication Protocol

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

About this task

Perform the following steps on all user terminals (for Evidian environments on Wearable user terminals only) where users access Nymi-Enabled Applications(NEAs) 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.

Procedure

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 the perform the following actions:
    a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`
    b. In the **Variable Value** field, type `0`.

    The following figure provides an example of the new variable.

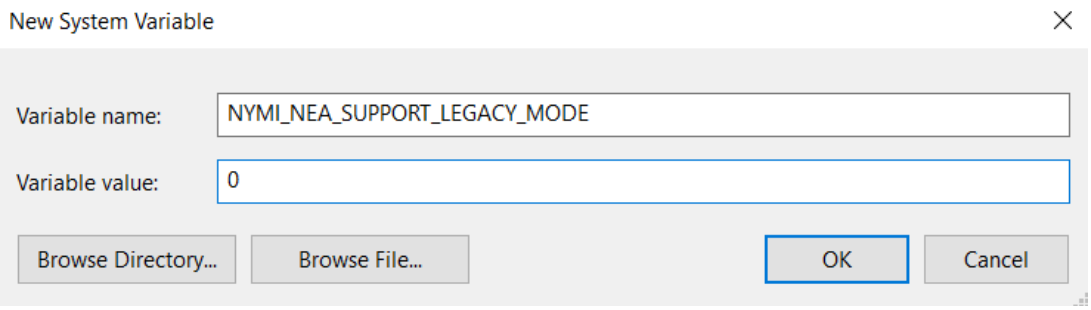


Figure 122. New System Variable window

    c. Click **OK**.

6.3.3.8 Configuring 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).

About this task

Perform the following steps on each user terminal.

Procedure

1. Run `regedit.exe`

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

6.3.3.9 Configuring Support for Virtual Desktop Lock and Unlock

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

About this task

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

Procedure

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

What to do next

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

7 Updating Connected Worker Platform

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

> **Note:** You cannot update Nymi Band 2.0 with Connected Worker Platform(CWP) firmware or use Nymi Band 2.0 with CWP infrastructure.

CWP 1.12.x and later provides NEA developers with enhancements that optimize Bluetooth tap performance for web-based NEAs. After you update the NEA 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 Nymi Band Application while wearing their authenticated Nymi Band. The Nymi Band Application applies changes to the Nymi Band that support the optimization.

Consider the following information:

- You must update the Nymi Band Application on the enrollment terminal before you attempt any new enrollments with a CWP 1.19.1 NES.
- You can update NES, Nymi Band Application, 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 the pre-CWP 1.19.1 firmware with CWP 1.19.1 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-CWP1.12.x infrastructure.
- The CWP 1.19.1 Nymi Band Application 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 Creating the Nymi Infrastructure Service Account

Connected Worker Platform(CWP) 1.12.x and later solution uses a service account to support interprocess and SQL server communications. When you update from 1.9.x and earlier, you can use an existing service account, for

example the one that you created for connectivity to to a remote SQL server or create a new account.

If you create a new account in Active Directory, ensure that the account meets the following requirements:

- User account is a domain user.
- Password never expires.

Nymi recommends that you name the service account `nymi_infra_service`, to align with product documentation.

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

7.2 Updating NES

When you update earlier versions of Nymi Enterprise Server(NES) to the current version of NES, there are new configuration parameters that you must provide.

Before you begin

Review the following information:

- Review the Connected Worker Platform Release Notes for important information about the release, including the order in which to update to components.
- Backup the Nymi Enterprise Server SQL database
- Ensure that you have access to the Fullchain certificate that Nymi provided to you during your initial production deployment and the password.
- Starting with Connected Worker Platform(CWP) 1.15.0, the size of the SymmetricKeyId column length increased from 36 to 512 characters. When updating from a release prior to CWP 1.15.0, if you use another database instance as a backup for the NES SQL database, ensure that you update the size of the SymmetricKeyId column length in the nub.NymiBand and audit.NymiBand tables.

About this task

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

Procedure

1. Extract the NES installation package to a local directory on the NES host.
2. From the directory that contains the extracted NES installation package, run `..\NesInstaller\install.exe`.
3. On the **User Access Control** window, click **Yes**.
4. On the **Open File - Security warning** window, click **Run**.
5. If applicable, on the **User Access Control** page, review the Microsoft .NET EULA, and then click **Accept**. Complete the .NET installation and continue with the NES installation.
6. On the **Application Install Security Warning** window, click **Install**.
7. On the **Open File - Security warning** window, click **Run**.
8. If the **Install Prerequisites** dialog appears and prompts to you install SQL Express, click **No**.
9. On the left navigation pane, click **Location**, and then perform the following steps.
    a. In the **Install Root** field, confirm that the path to the NES services is correct, as it was specified during the initial deployment.

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

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

       > **Note:** Ensure that the values that you specify in the **Install Root** and **Instance Name** match the values that you specified when you deployed the previous version of NES. When the

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

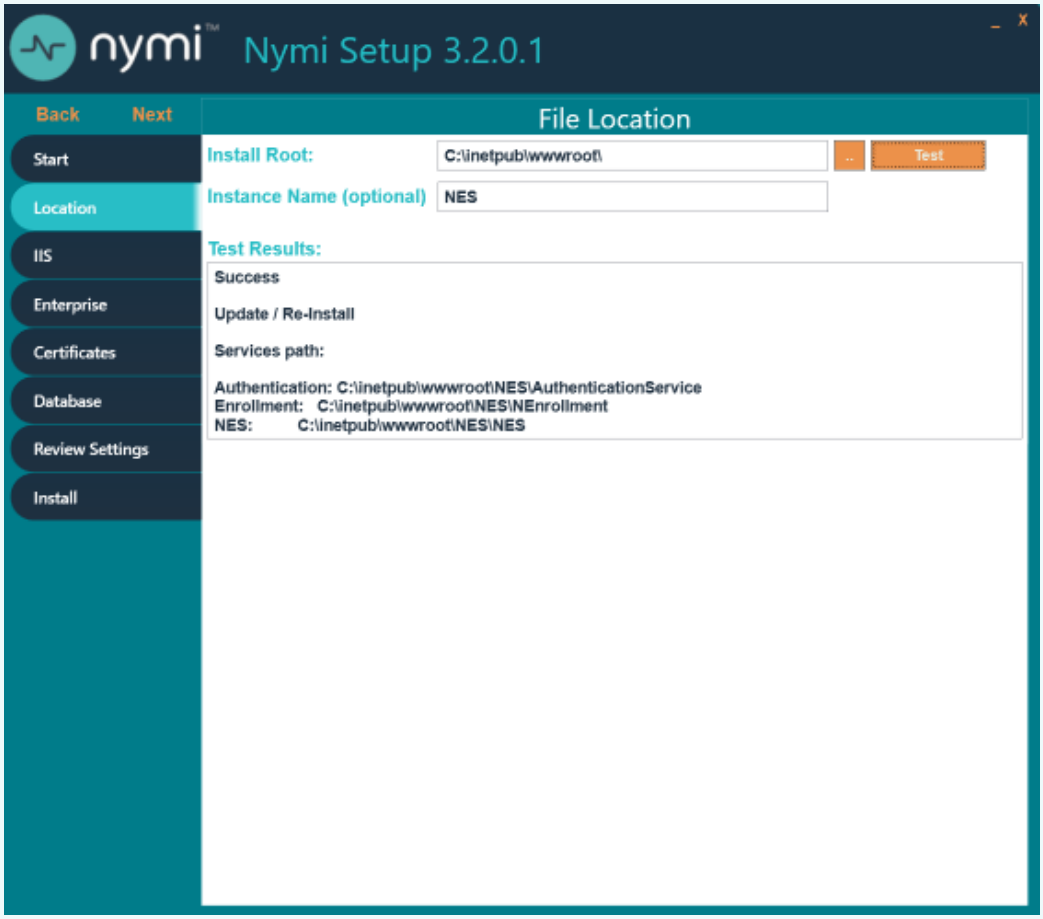


Figure 123. Update / Reinstall installation type

10. For HA deployments only, click IIS and perform one of the following actions:

    - On the first NES server that you update, in the **Key Management** section, click **Copy**, and then paste and save the value securely.
    - On subsequent servers that you update, in the **Key Management** section, click **Edit**, and then copy and paste the value from the first NES install. 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.

11. When updating from CWP 1.14.x and earlier, 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`.

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

    a. 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.
    b. In the **Password Required** pop-up, type the Full Chain certificate password, and then click **OK**.

13. In the left navigation pane, click **Database**, and then perform the following actions.

    a. Click **Test** to verify that the database connection string is valid and installer can connect to the existing NES database.
    b. Click **Verify users** to ensure that installer can detect users with access to the SQL database.

14. In the left navigation pane, click **Review Settings**, and then click **Test** to verify the configuration. Review the test results and address any errors if applicable.

15. In the left navigation pane, click **Install**.

16. Click **Update**.

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

17. On the **Update NES** window, click **Yes** to reapply the configuration.

    The **Install** window display the status of the update process.

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

What to do next

After you complete the update, export the NES configuration settings and archive your pre-CWP1.20.x .ninst configuration file. Saving the NES

Configuration provides more information about to how to export the configuration settings.

7.2.1 Defining the NES for Policy Management

After you update Nymi Enterprise Server(NES) from a pre-Connected Worker Platform(CWP) 1.18.0 version, perform the following steps to define which NES manages the policy settings on existing Nymi Bands.

About this task

While this step applies to updates of an IT/OT environment, you must also perform these steps for non-IT/OT configurations.

Procedure

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. From the **Select whether NES manages policies on these previously assigned Nymi Bands** option, select one of the following values:

   - **Enable policy management**—Choose this option when users are in an non-IT/OT configuration, or in an IT/OT configuration where existing users enrolled their Nymi Bands to this NES.
   - **Disable policy management**—Choose this option in an IT/OT configuration, when existing users registered their Nymi Bands to this NES.

   The following figure shows the **Select whether NES manages policies on these previously assigned Nymi Bands** option.

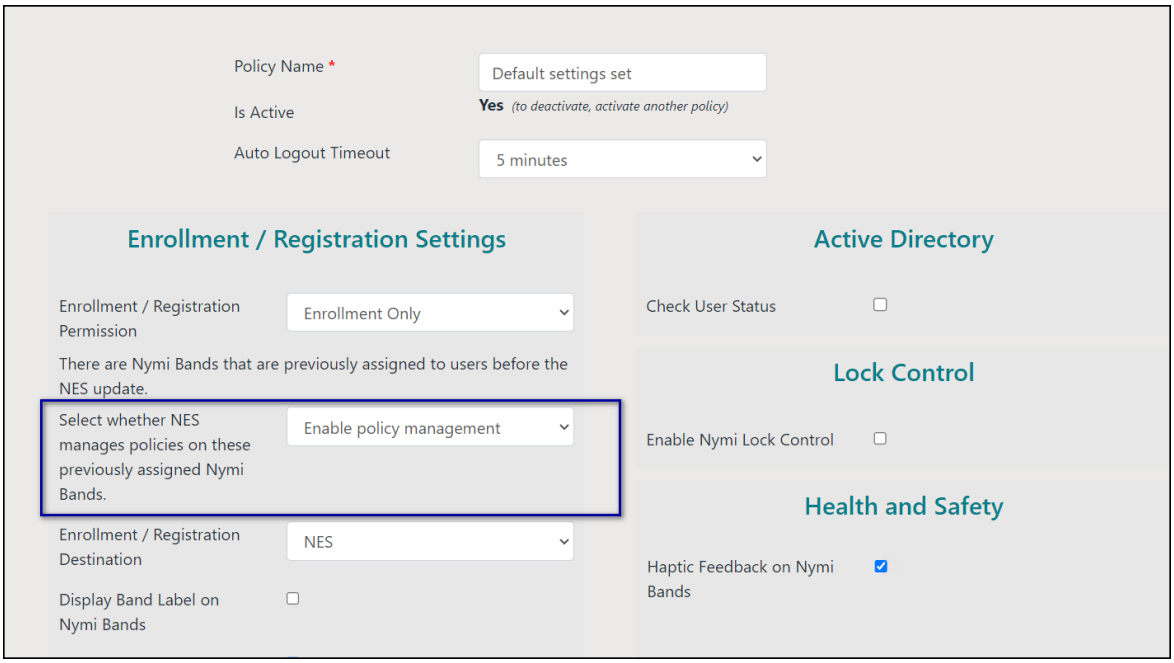


Figure 124. Select whether NES manages policies on these previously assigned Nymi Bands option

5. Click **Save**.

   NES updates the SQL database entries for existing users and when you set **Enable policy management**, existing enrolled Nymi Bands receive their policy configuration of this NES.

   > **Note:** After you assign a value to the option, the option disappears from the active policy. If you want to change the NES from which an existing Nymi Band receives policy updates, the user must re-enroll the Nymi Band on the other NES.

7.3 Updating the Enrollment Terminal

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

7.3.1 Updating the Centralized Nymi Band Application

Perform the following steps to update the Nymi Band Application.

Procedure

1. Create a backup copy of the `C:\Nymi\Bluetooth_Endpoint\nbe.toml` file.
2. Download the Nymi Band Application 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**.

   The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
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, as shown in the following figure, and then click **Next**.

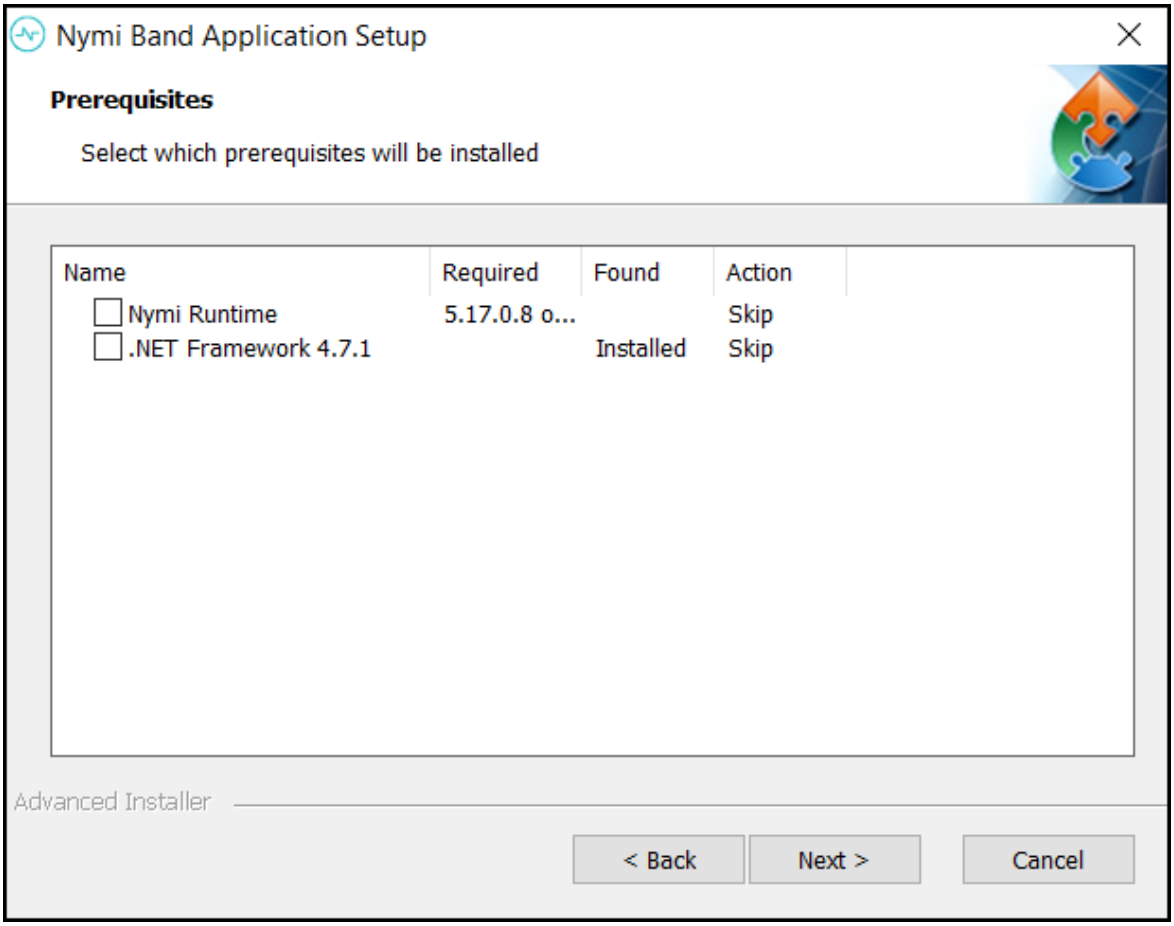


Figure 125. No Nymi Runtime Installation

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 Connected Worker Platform 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.

7.3.2 Updating the Decentralized Nymi Band Application

Perform the following steps to install the Nymi Band Application with the Installation Wizard.

Before you begin

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

Procedure

1. Download the Nymi Band Application 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.

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

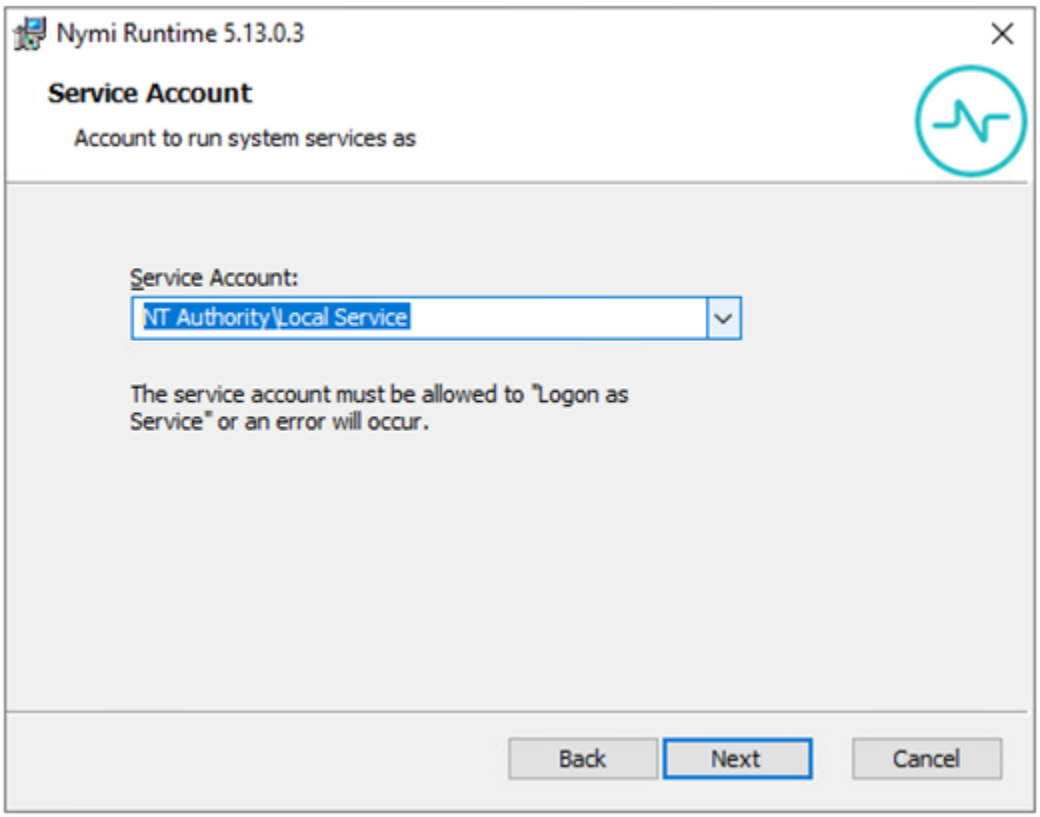


Figure 126. Nymi Runtime Service Account window

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

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**.

What to do next

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

7.4 Updating the Centralized Nymi Agent and the 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.

7.4.1 Update Centralized Nymi Agent

Update the Centralized Nymi Agent with the installation wizard.

7.4.1.1 Installing/Updating Centralized Nymi Agent

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

About this task

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

Procedure

1. Log in to the terminal, with an account that has administrator privileges.
2. Extract the `Nymi SDK` distribution package.
3. From the `..\nymi-sdk\windows\setup`folder, 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 option to make **Nymi Bluetooth Endpoint** unavailable.

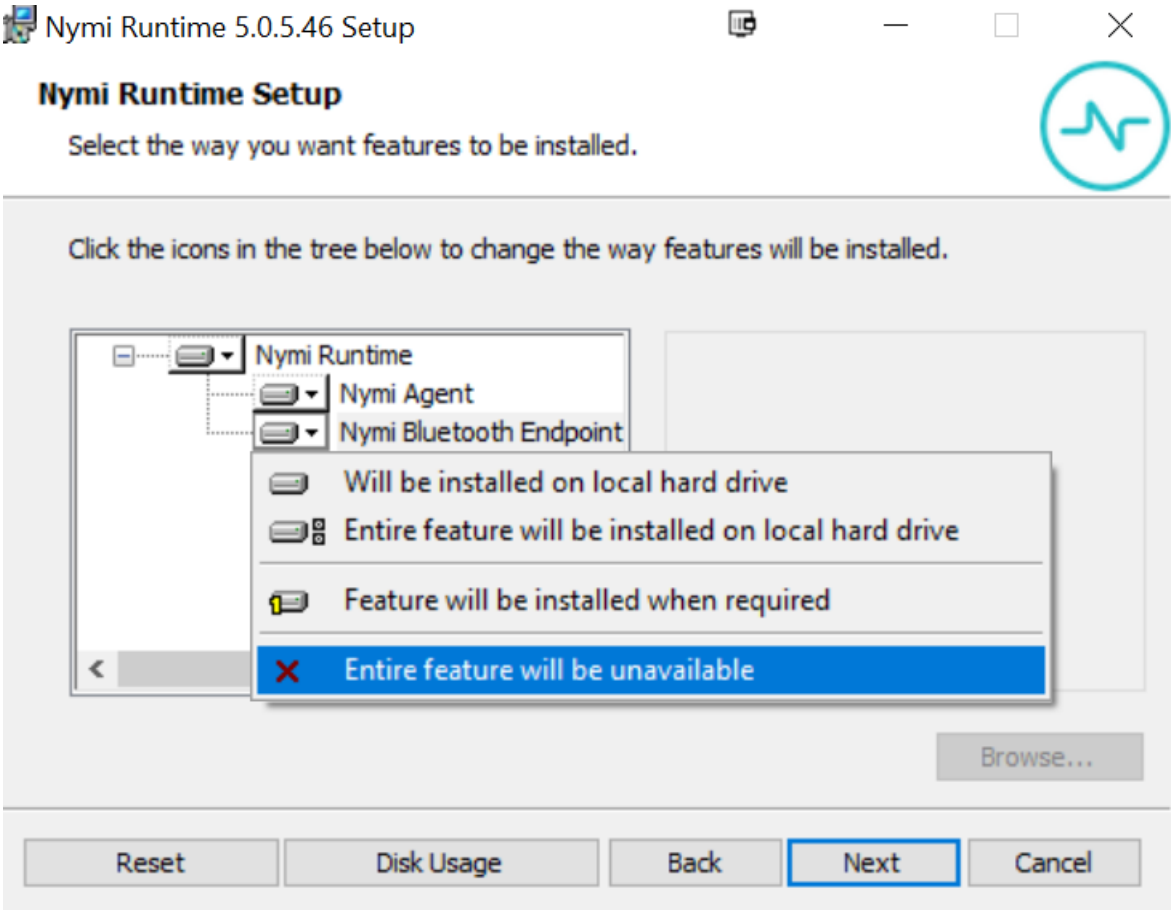


Figure 127. Nymi Bluetooth Endpoint feature will be unavailable

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

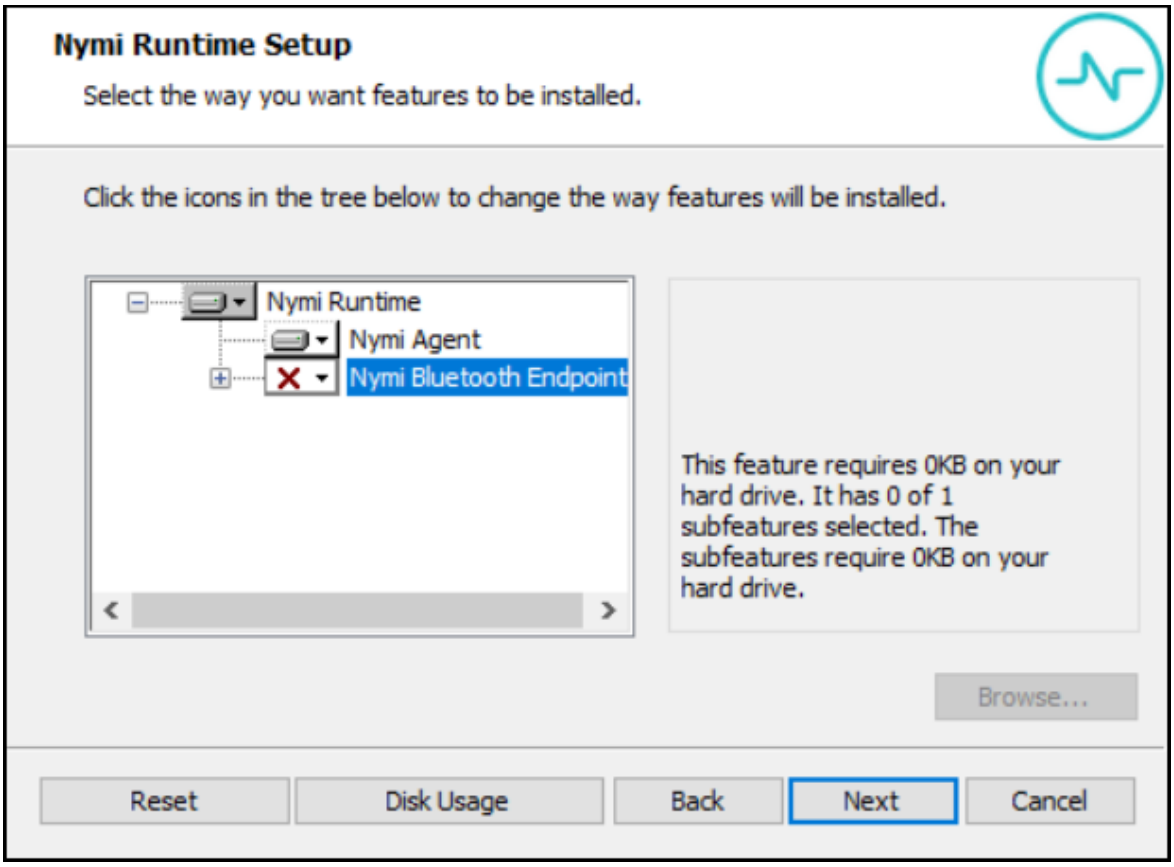


Figure 128. Nymi Bluetooth Endpoint feature is not available

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.

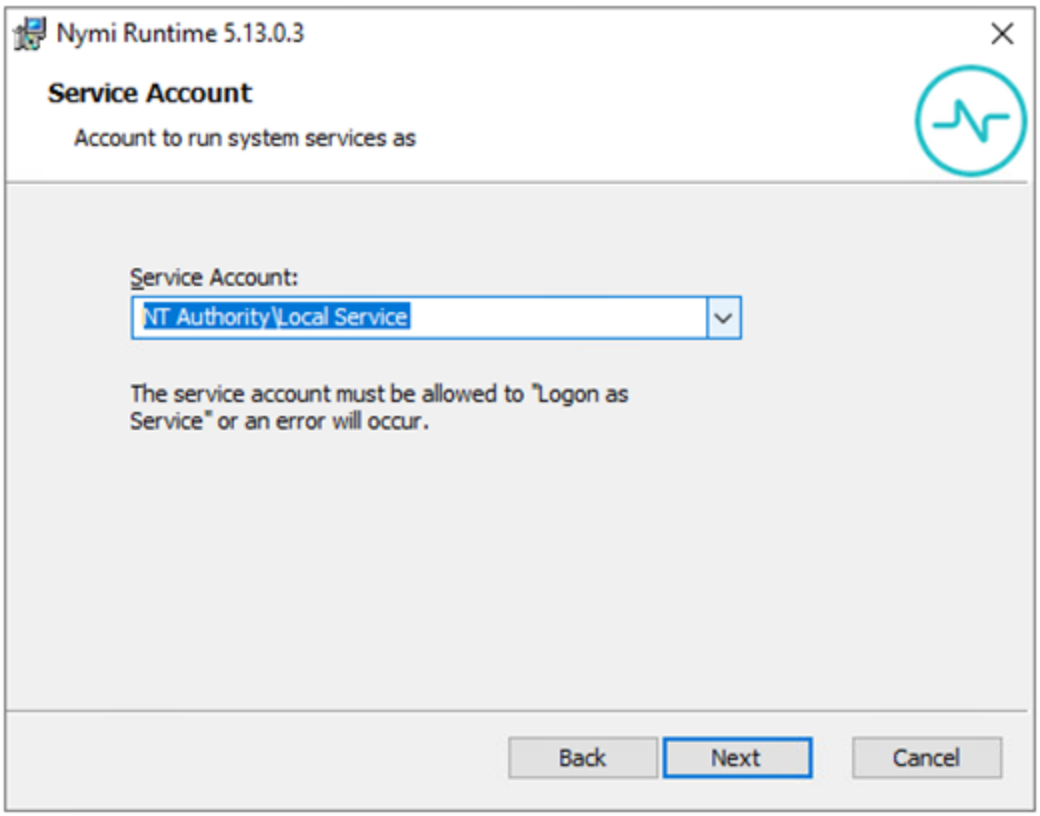


Figure 129. Nymi Runtime Service Account window

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.

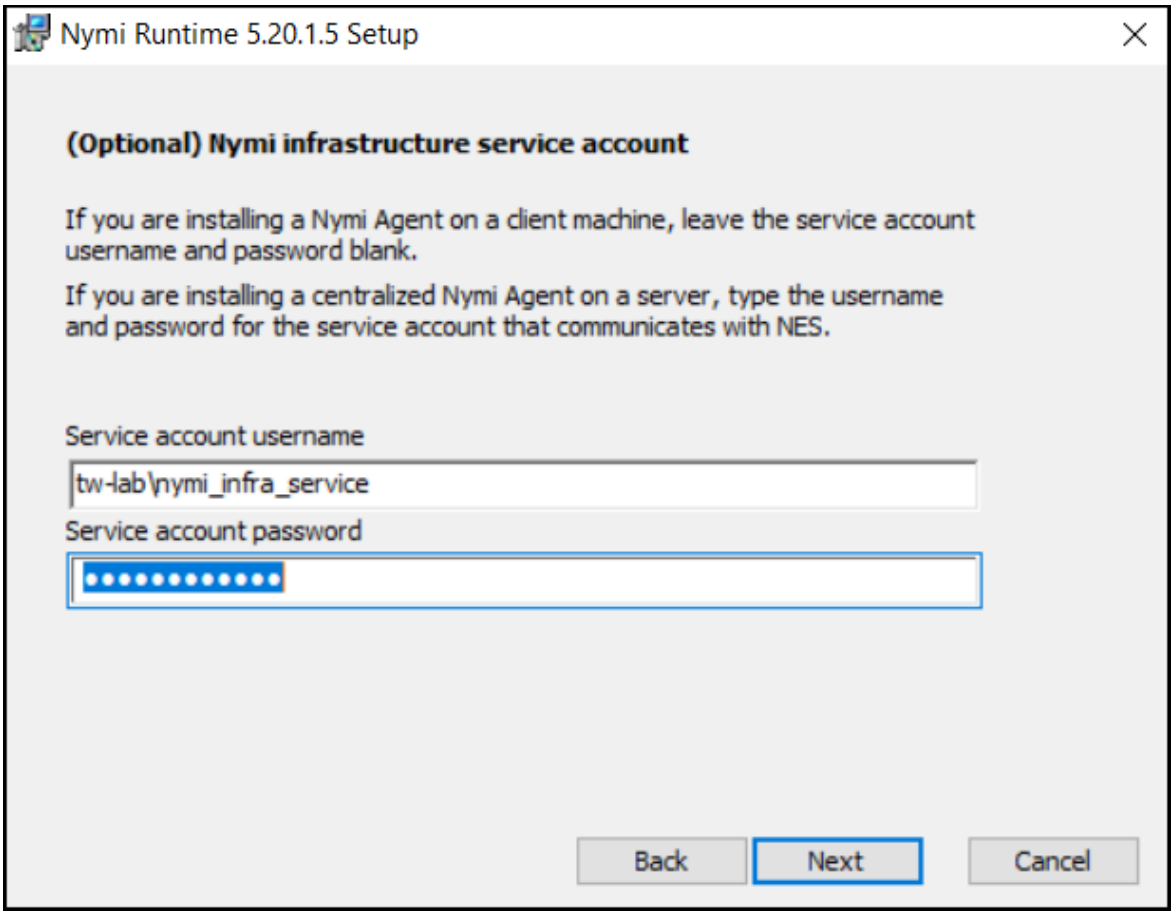


Figure 130. Nymi Infrastructure Service Account window

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**.

7.4.1.2 Configuring Nymi Agent

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

Procedure

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
`protocol`	[agent]	Optional. To enable the standard Nymi Agent to use secure websocket communications, uncomment protocol and change the value to wss. Note: Requires the configuration of the `cacertfile`, `cacert`, and `keyfile` parameters in the [agent] section. For example, protocol = “wss”

Parameter and Default Values	Section Name	Description
`port`	[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 you use the default port number.
`cacertfile`	[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. Note: Requires the configuration of `protocol= "wss"`, `certfile` and `keyfile` parameters in the [agent] section. For example: cacertfile = “certs/LocalLabRootCA3.pem”
`certfile`	[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. Note: Requires the configuration of `protocol= "wss"`, `cacertfile`, and `keyfile` parameters in the [agent] section. For example: “certfile =”certs/tw-srv1.tw-lab.local-cert.pem”
`keyfile`	[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. Note: Requires the configuration of `protocol= "wss"`, `cacertfile`, and `certfile` parameters in the [agent] section. For example: “keyfile =”certs/tw-srv1.tw-lab.local-key.pem”

6. Save the file.
7. Restart the **Nymi Agent** service.

Results

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"`

7.4.2 Update Clients that Connect to a Centralized Nymi Agent

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

7.4.2.1 (Windows Only) Updating 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.

Before you begin

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

About this task

Perform the following steps to install Nymi Bluetooth Endpoint manually.

Procedure

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

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

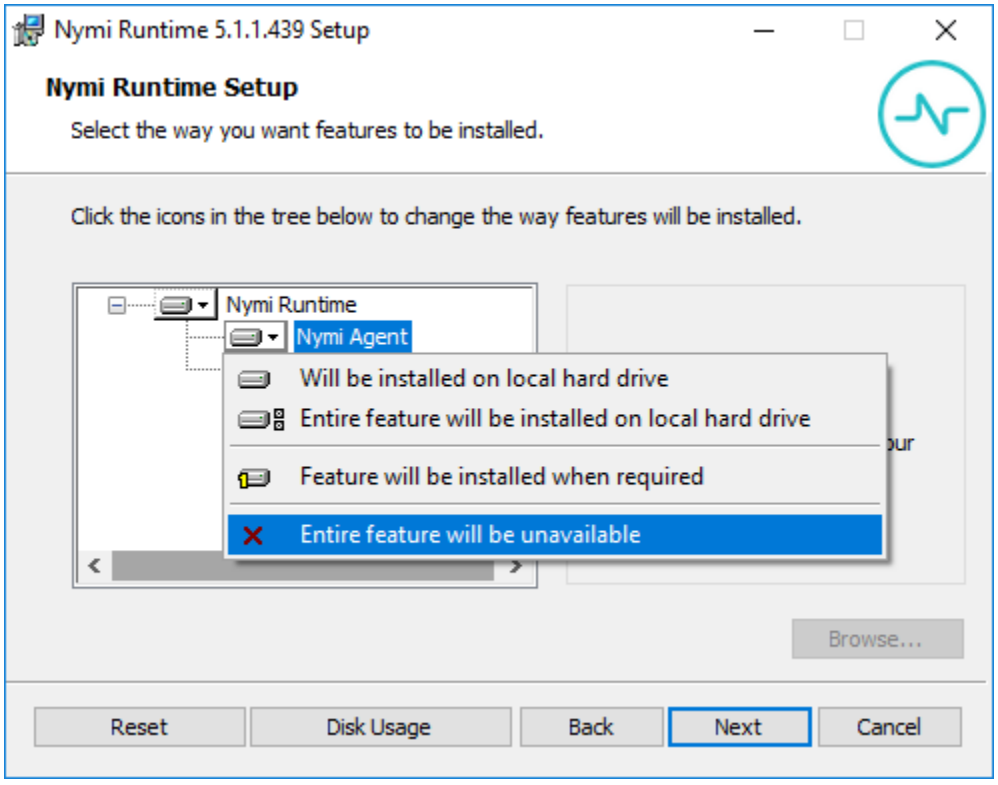


Figure 131. Nymi Agent feature will be unavailable

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

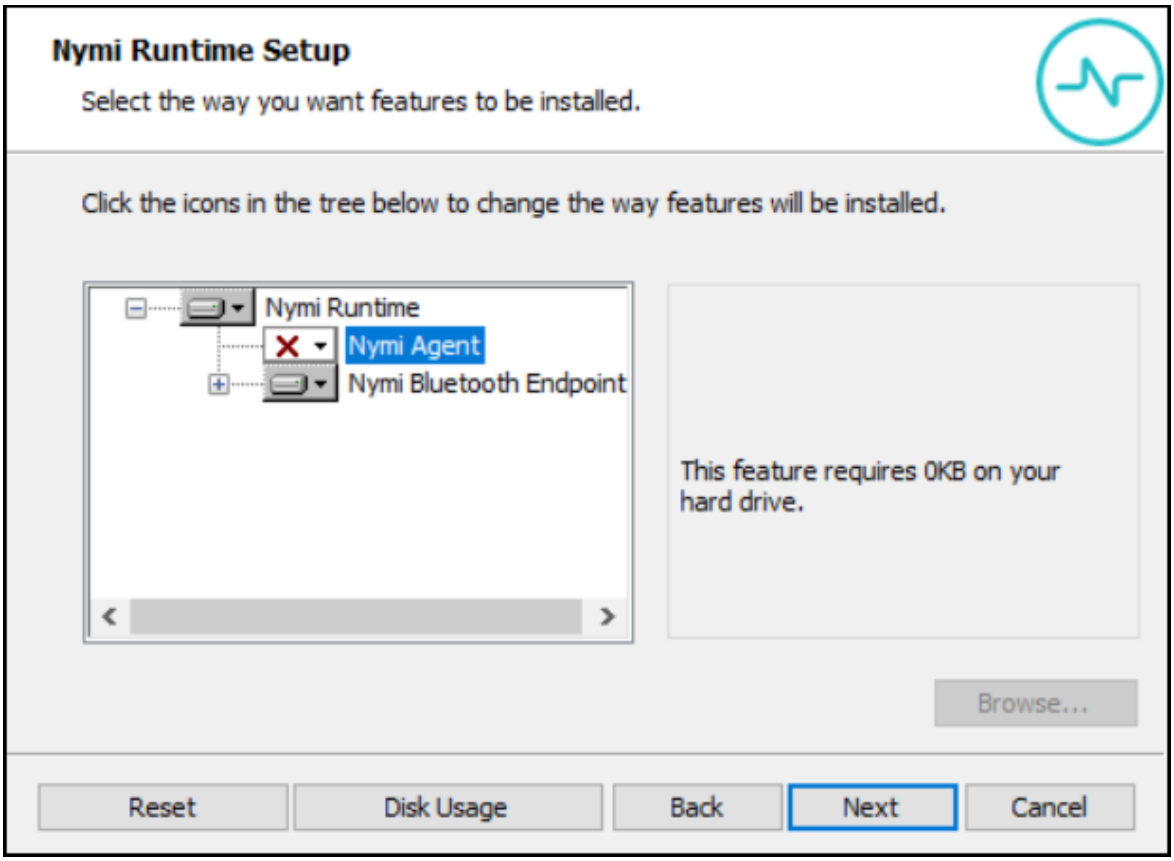


Figure 132. Nymi Agent feature is not available

11. 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.

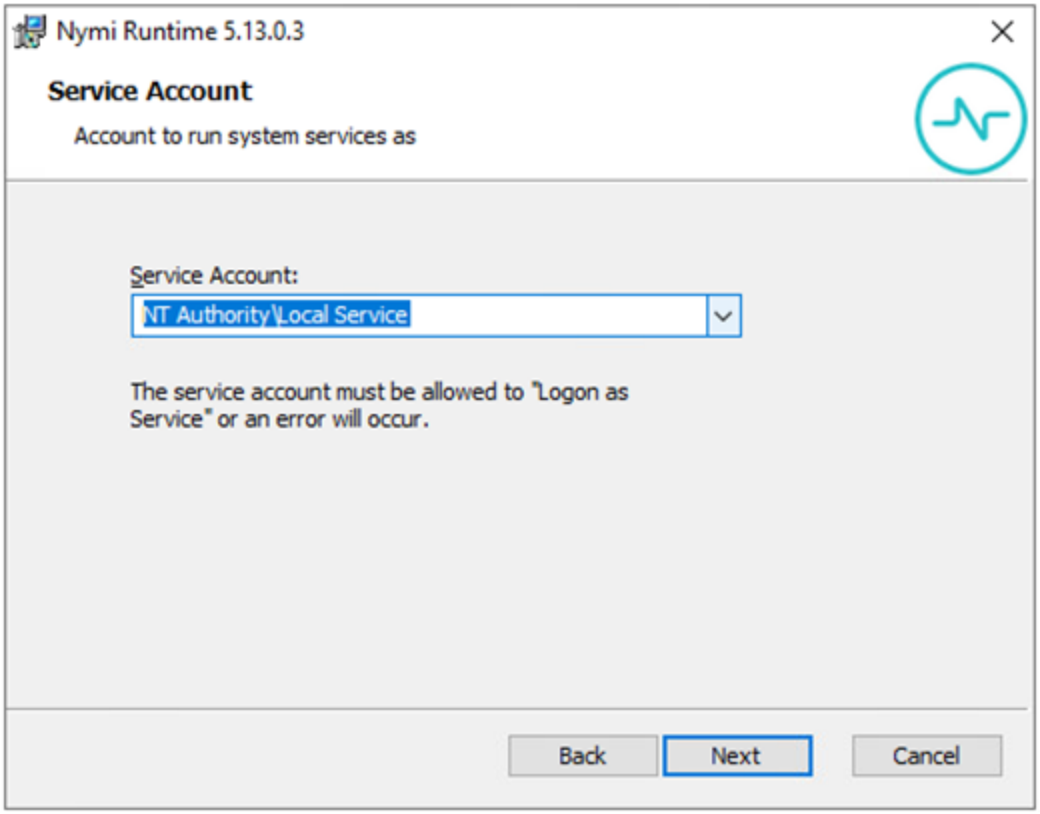


Figure 133. Nymi Runtime Service Account window

12. On the **Ready to install** page, click **Install**.
13. Click **Finish**.
14. On the **Installation Completed Successfully** page, click **Close**.
15. Stop the **Nymi Bluetooth Endpoint** service.
16. 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 Connected Worker Platform 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.

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

What to do next

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

7.4.2.2 Updating Nymi Lock Control

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

Procedure

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 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.

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

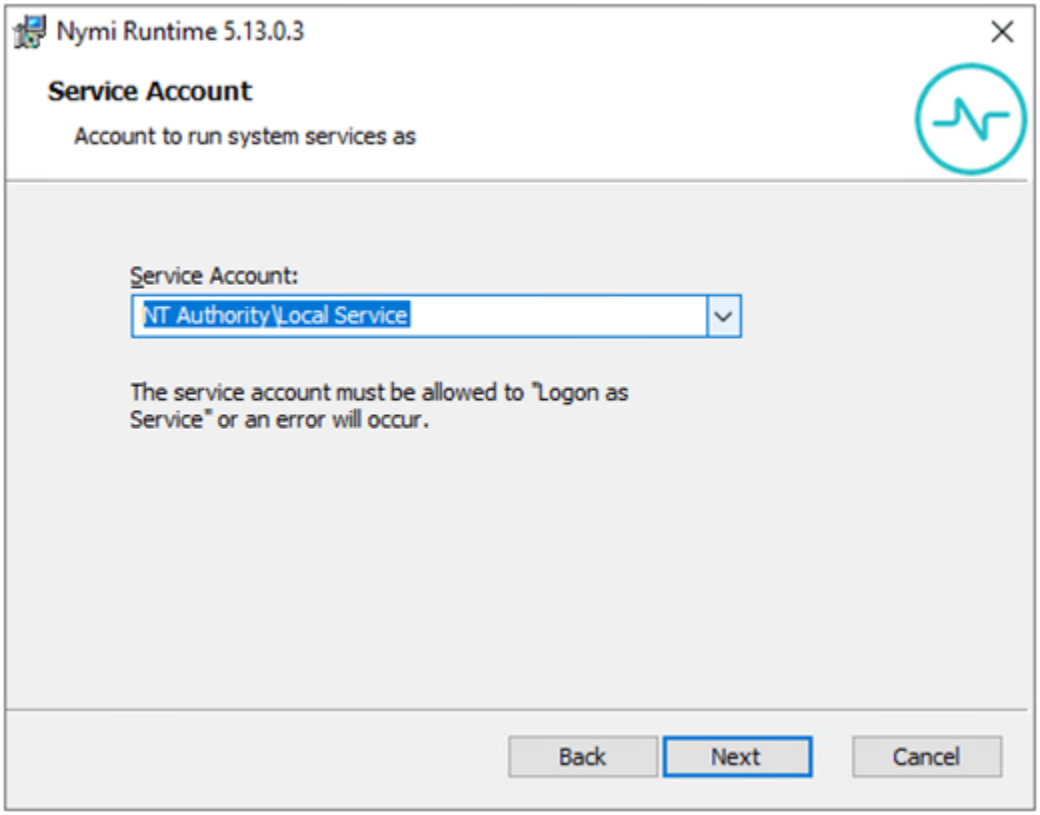


Figure 134. Nymi Runtime Service Account window

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, perform the following actions:
    a. To change the installation location, click **Browse**, navigate to a new installation folder, and then click **Select Folder**
    b. 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 Connected Worker Platform 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.

7.4.2.3 (HP Thin Pro only) Updating Nymi Bluetooth Endpoint

The following instructions describe how to update Nymi Bluetooth Endpoint manually.

About this task

Perform the following steps on the HP Thin Pro client.

Procedure

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 an the credentials of a person in the domain admin group.

    a. Right-click the desktop or click **Start**.
    b. Click **Switch to Administrator** from the menu. You will be prompted to enter the administrator password.

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

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

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

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

6. 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.

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

    a.

8. Reboot the client.

7.4.2.4 (IGEL only) Updating Nymi Bluetooth Endpoint

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

Uploading Nymi Packages to Universal Management Suite

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

About this task

Obtain the installation package from Nymi.

Procedure

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

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

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

Results

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

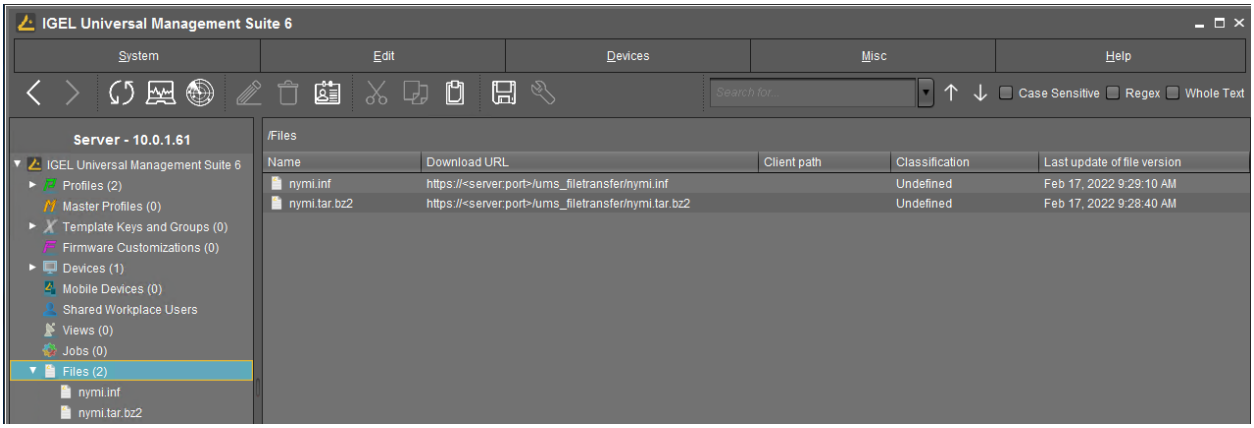


Figure 135. Files window

Updating Nymi Bluetooth Endpoint on IGEL

Perform the following steps to update the Nymi software on an IGEL user terminal.

About this task

The procedure requires you to reboot the client.

Procedure

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, as shown in the following figure.

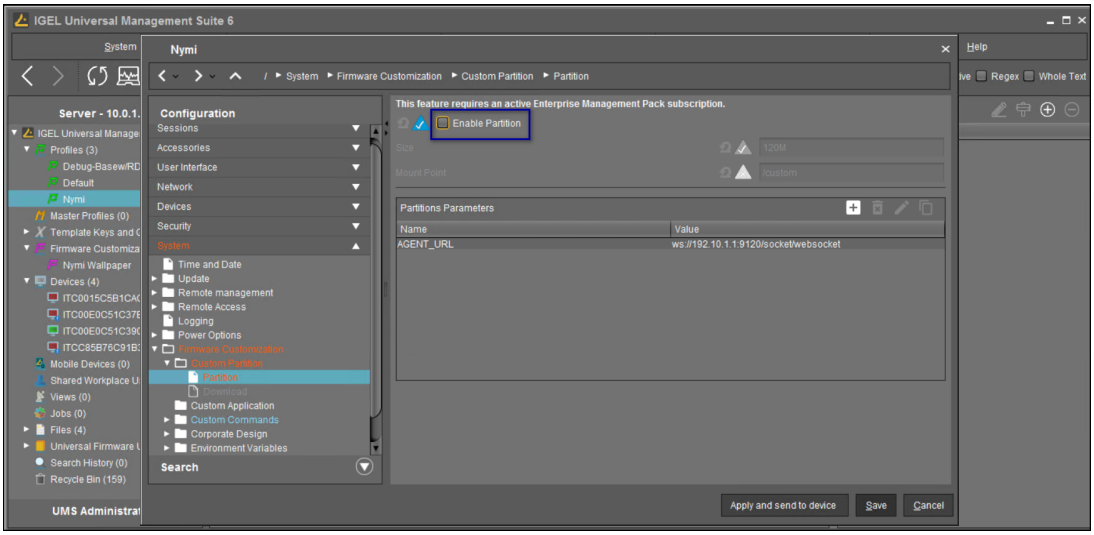


Figure 136. Disable the Partition option

d. Click **Apply and send to device**.

e. On the **Update time** dialog box, select **Now**, and then click **Ok**.

The following figure shows the **Update time** dialog.

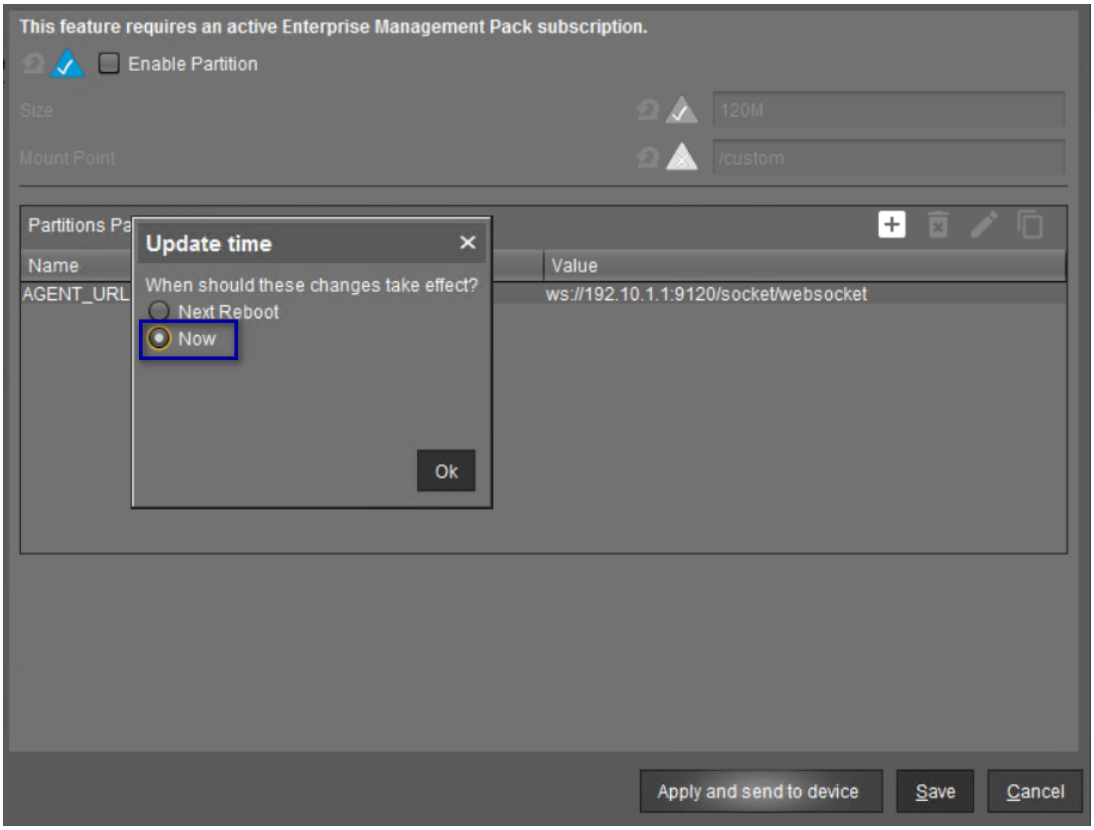


Figure 137. Update time window

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**.

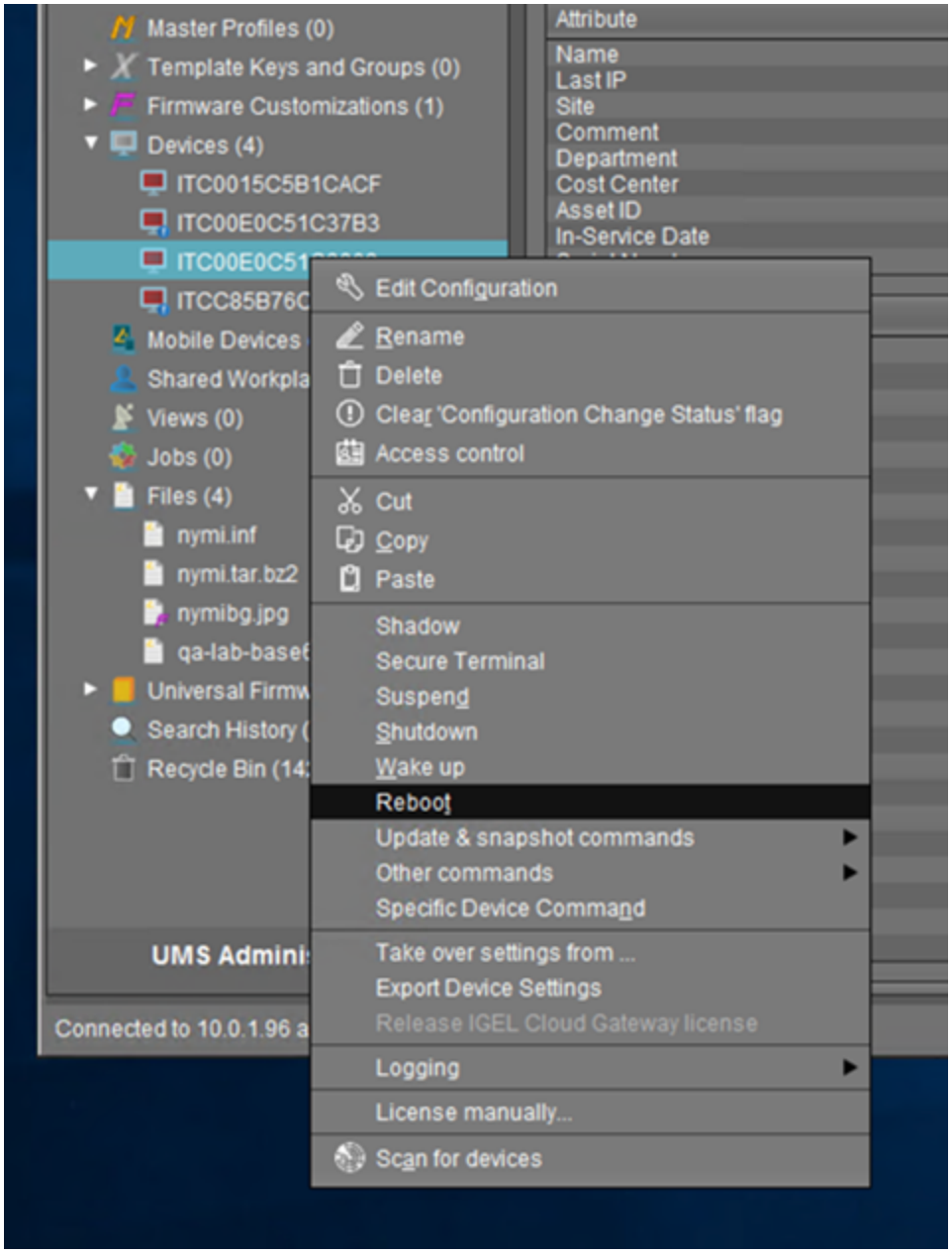


Figure 138. Reboot option

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**, as shown in the following figure.

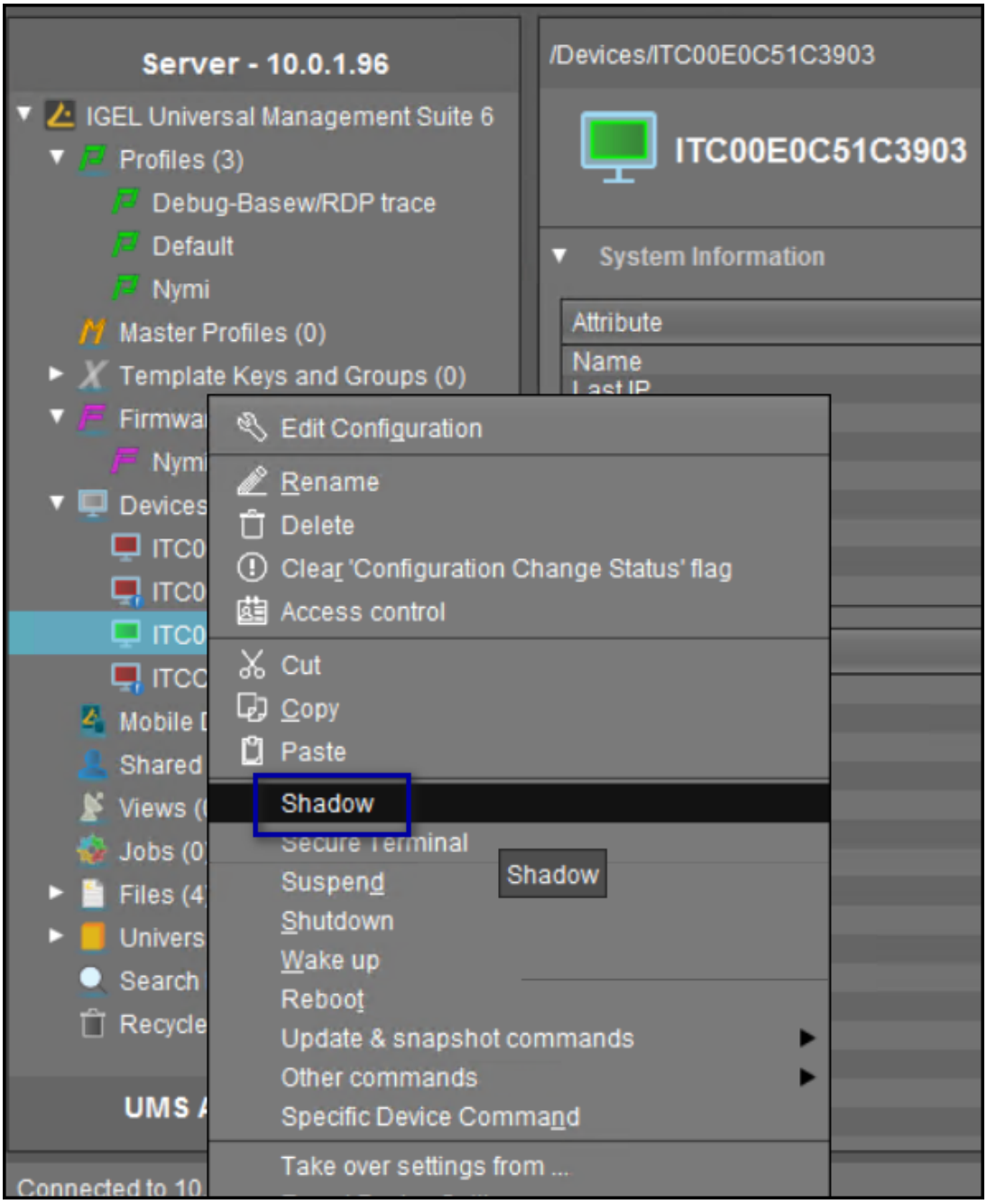


Figure 139. Shadow option

    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 `nymi.inf`, and then select **Delete**, as shown in the following figure.

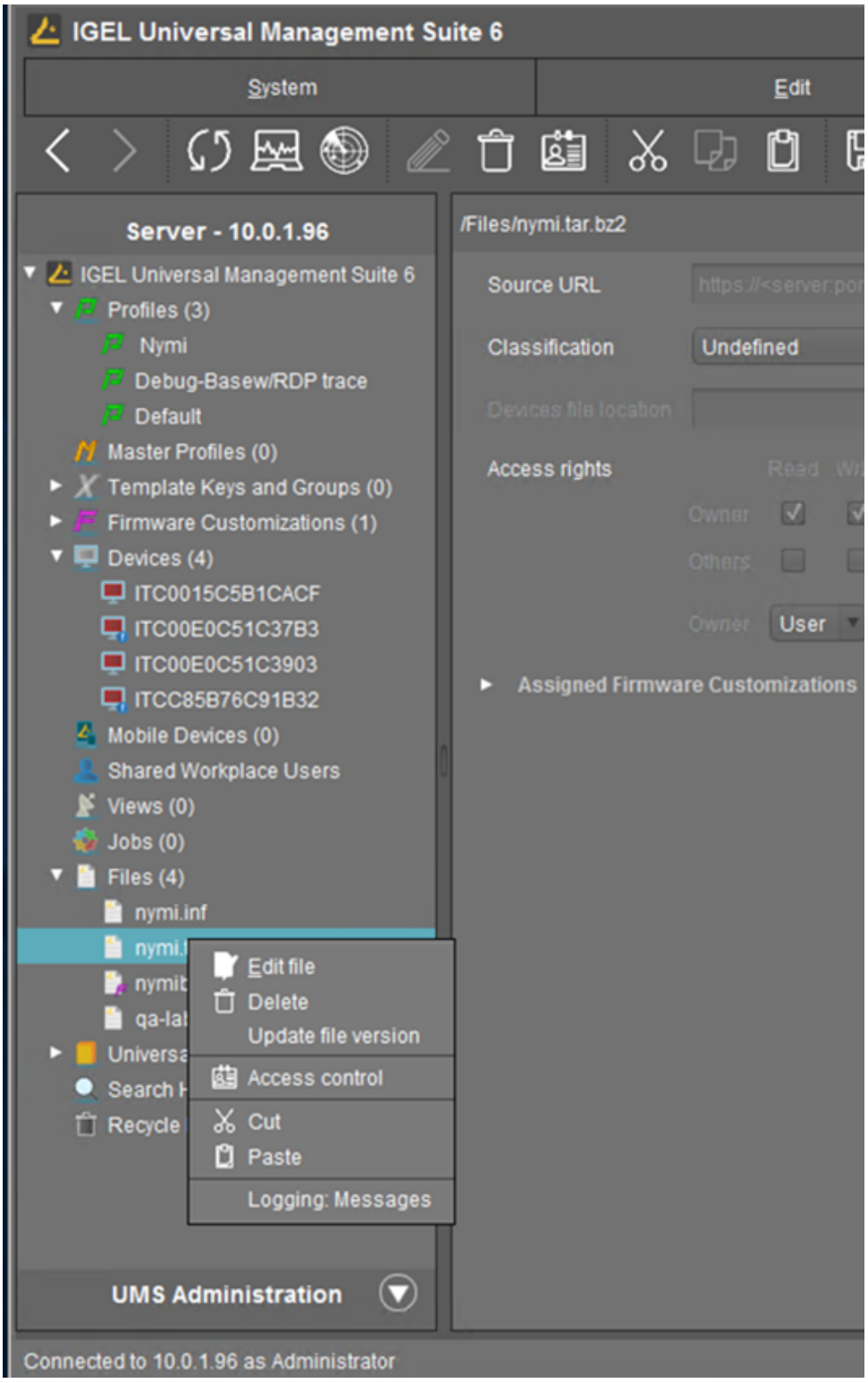


Figure 140. Delete menu option

6. In the left navigation pane of the UMS Console, in the **Files** section, right-click `nymi.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 `nymi.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 `nymi.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**.

7.5 Updating Clients that Connect to A Decentralized Nymi Agent

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

7.5.1 Updating the Nymi Runtime

Perform the following steps on each user terminal to update the Nymi Runtime.

Procedure

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

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

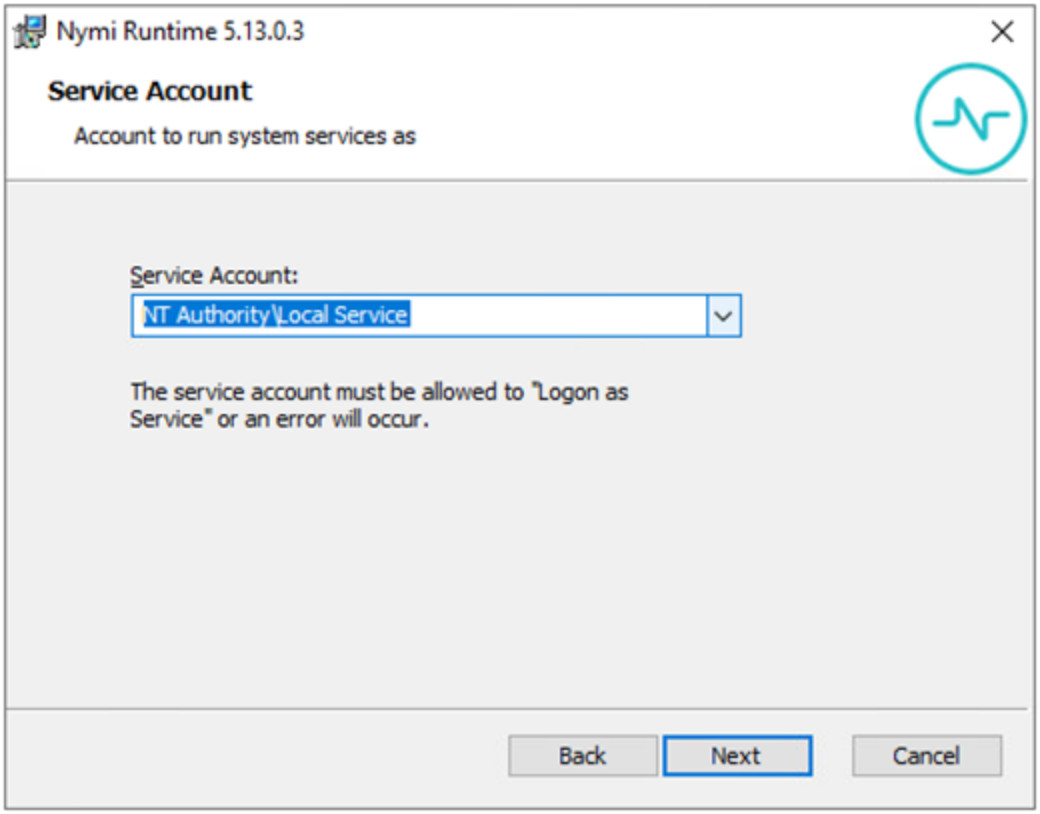


Figure 141. Nymi Runtime Service Account window

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

    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. 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. Entries that appear in a Connected Worker Platform 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.

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

What to do next

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

7.5.2 Updating Nymi Lock Control

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

Procedure

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 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.

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

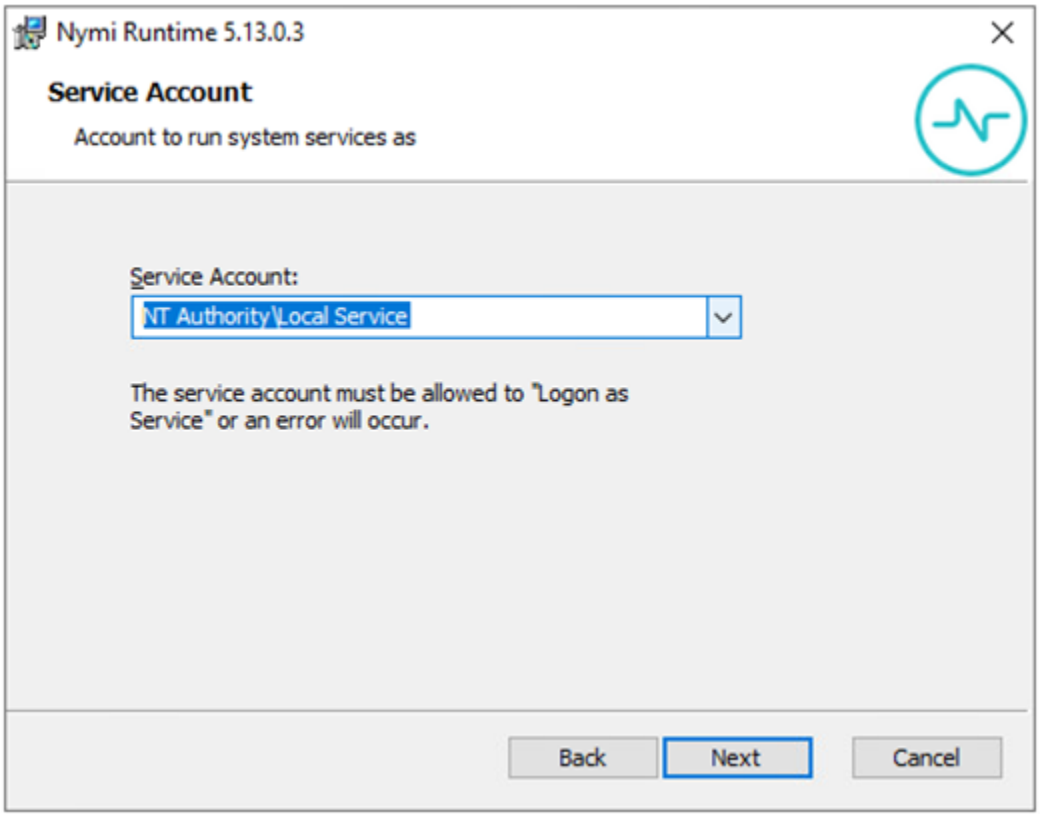


Figure 142. Nymi Runtime Service Account window

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, perform the following actions:

    a. To change the installation location, click **Browse**, navigate to a new installation folder, and then click **Select Folder**
    b. 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 Connected Worker Platform 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.

7.6 Updating the Nymi Band Firmware

Nymi provides a firmware updater utility to update Nymi Bands.

You can update one Nymi Band at a time or up to 5 consecutive Nymi Bands that are on charge and within bluetooth range of the computer that runs the utility.

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

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

7.6.1 Updating the Firmware on Multiple Nymi Bands

You can update the firmware on a maximum of five Nymi Bands at one time. Attempting to update more than five concurrently may require the user to stop and manually restart the firmware update utility.

Before you begin

Updating the firmware on multiple Nymi Band concurrently requires the following:

- Windows 10 computer.
- USB hub.
- Up to 5 Bluegiga Bluetooth adapters.



- Enough charging cradles to fill the ports in the USB hub (less the ports for the Bluetooth Adapters).

> **Note:** Currently, firmware updates and firmware log retrieval require a Bluegiga BLED112 Bluetooth Adapter. You cannot use a BleuIO Bluetooth Adapter to perform these operations.

Procedure

1. Download and extract the firmware package into a directory of your choice on a Windows computer. For example, `C:\Nymi_firmware`.
2. If the Windows machine has the Nymi Band Application or Nymi Runtime installed on it, stop the Nymi Bluetooth Endpoint service.
3. Disable or extend sleep mode on computer to prevent the utility from terminating when the computer goes to sleep.
4. Plug the USB hub into an electrical outlet, and then into a USB port on the Windows machine.
5. Plug up to 5 Bluetooth Adapters into the USB hub.
6. Plug Nymi Band charging cradles into the remaining ports on the USB hub, and put a Nymi Band on each cradle.

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

7. From a command prompt on the Windows computer, change to the directory that contains the `fw_updater_GOLD_<version>.exe` file.

   The firmware update utility interface appears and provides the following information:

   - Firmware version—The version of firmware version that the utility applies to eligible Nymi Bands.
   - Number of available BLE adapters—Number of Bluetooth Adapters that the utility detects in bluetooth range.
   - Number of in progress updates—Number of Nymi Band that are in **STAND BY** or **DOWNLOAD** state
   - Total number of Nymi Bands that are updated during the session.

   The following figure provides an example of the interface.

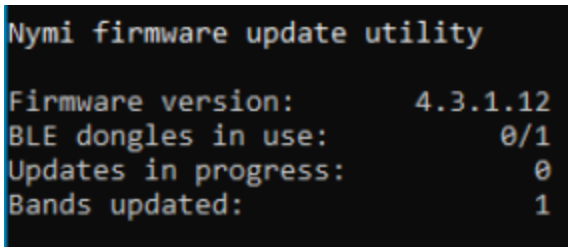


Figure 143. Firmware update utility interface

The utility scans the Bluetooth adapters on the USB hub for a Nymi Band that has a firmware version that is older than the version in the firmware package, or a Nymi Band with recovery firmware. When the utility detects a Nymi Band that requires the update, the Nymi Band screen displays **STAND BY**, and when the utility starts the transfer of the firmware to the Nymi Band, the Nymi Band screen displays **DOWNLOAD**.

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

8. When the Nymi Band firmware download completes, the Nymi Band automatically restarts and applies the update. A brief SUCCESS message appears when the update completes. Take the completed Nymi Band off charge and plug in another Nymi Band that requires updating.

   The firmware update process takes about 5 minutes.

9. To stop the application, press `Ctrl+C`.

   When the utility terminates, Nymi Bands that were in the process of downloading software will revert back to the previous firmware version.

10. If required, restart the Nymi Bluetooth Endpoint service.

Results

Some firmware updates, require you to re-enroll the Nymi Band, review Updating Nymi Connected Worker Platform for more information.

7.6.2 Updating the Firmware on a Nymi Band

You can update the firmware on a Nymi Band that you plug into a machine that has access to the firmware update utility.

Before you begin

Updating the firmware on a Nymi Band requires the following:

- Windows 10 computer with 2 USB ports.
- One Bluegiga Bluetooth Adapter.



- One charging cradle.

> **Note:** Currently, firmware updates and firmware log retrieval require a Bluegiga BLED112 Bluetooth Adapter. You cannot use a BleuIO Bluetooth Adapter to perform these operations.

Procedure

1. Download and extract the firmware package into a directory of your choice on a Windows computer. For example, `C:\Nymi_firmware`.
2. Disable or extend sleep mode on computer to prevent the utility from terminating when the computer goes to sleep.
3. If the Windows machine has the Nymi Band Application or Nymi Runtime installed on it, stop the Nymi Bluetooth Endpoint service.
4. Plug the Bluetooth Adapter into a USB port on the Windows machine.
5. Plug Nymi Band charging cradles into other USB port, and put the Nymi Band on the cradle.

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

6. Change to the directory that contains the `fw_updater_GOLD_version`.exe file, right-click on the file, and then select **Run as administrator**.

   The firmware update utility interface appears and provides the following information:

   - Firmware version—The version of firmware version that the utility applies to eligible Nymi Bands.
   - Number of available BLE adapters—Number of Bluetooth Adapters that the utility detects in bluetooth range.
   - Number of in progress updates—Number of Nymi Band that are in **STAND BY** or **DOWNLOAD** state
   - Total number of Nymi Bands that are updated during the session. The following figure provides an example of the interface.

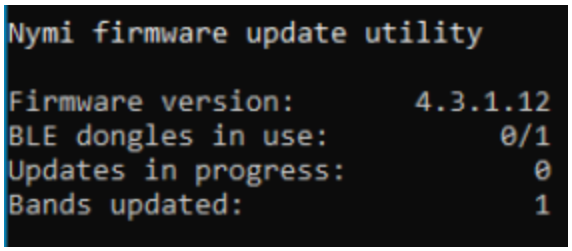


Figure 144. Firmware update utility interface

The utility scans the Bluetooth adapter for a Nymi Band that has a firmware version that is older than the version in the firmware package, or a Nymi Band with recovery firmware. When the utility detects a Nymi Band that requires the update, the Nymi Band screen displays **STAND BY**, and when the utility starts the transfer of the firmware to the Nymi Band, the Nymi Band screen displays **DOWNLOAD**.

7. When the Nymi Band firmware download completes, the Nymi Band automatically restarts and applies the update. A brief SUCCESS message appears when the update completes. Take the completed Nymi Band off charge and plug in another Nymi Band that requires updating.

   The firmware update process takes about 5 minutes.

8. The firmware update utility continues to scan the Bluetooth Adapter for a Nymi Band that requires an update. To stop the utility, press `Ctrl+C`.

   If you stop the utility while a firmware update was in progress of downloading the software, the Nymi Band reverts back to the previous firmware version.

9. If required, restart the Nymi Bluetooth Endpoint service.

Results

Some firmware updates, require you to re-enroll the Nymi Band, review Updating Nymi Connected Worker Platform for more information.

7.6.3 Firmware updater log files

By default, the firmware update utility creates two files in the same location as that contains the fw_updater_gold_v.exe file, which you can view at any time during the firmware update process.

> **Note:** You can use the `--log` argument to define an alternate location for the files.

- `result_log.csv`—Contains summary information about the Nymi Bands that the firmware update utility updates.
- `fw_updater.log`—Contains system diagnostic information about actions that utility runs during Nymi Band firmware updates. The utility creates a maximum of 5 rotating log files. Each of these log files cannot exceed 10MB.

7.7 Changing the Connected Worker Platform Communication Protocol

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

About this task

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 (for Evidian environments on Wearable user terminals only) where users access Nymi-Enabled Applications(NEAs) 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.

Procedure

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 the perform the following actions:

    a. In the **Variable Name** field, type `NYMI_NEA_SUPPORT_LEGACY_MODE`

    b. In the **Variable Value** field, type `0`.

    The following figure provides an example of the new variable.

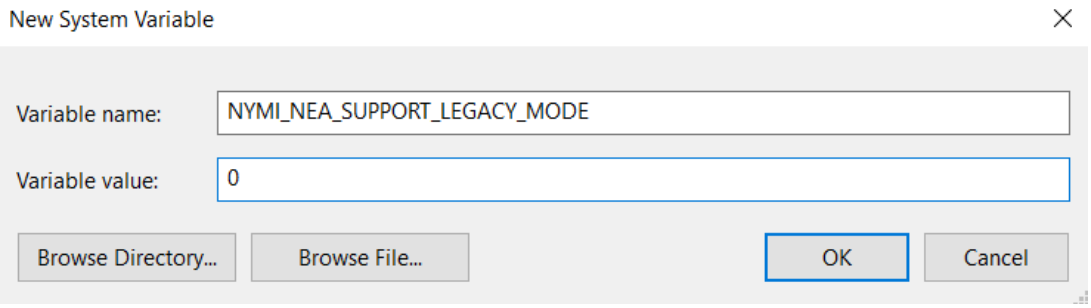


Figure 145. New System Variable window

    c. Click **OK**.

8 Appendix—Recording the CWP Variables

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

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

Table 7. CWP Values

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

9 Appendix—Recording the CWP Component FQDNs

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

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

Table 8. CWP Values

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

10 Appendix—TLS Certificates Expiration Dates

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

Table 9. Certificate Expiration Dates

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

11 Appendix—Silent Installations

You can deploy various client side components in the Connected Worker Platform(CWP) solution from a command prompt.

11.1 Installing Nymi Bluetooth Endpoint Silently

Procedure

1. Run a Command Prompt as administrator.

   You can install the Nymi Bluetooth Endpoint silently by typing one of the following commands:

   - ```
     "Nymi Runtime Installer version.exe" /exenoui InstallAgent=0 /q /
     log NymiRuntimeInstallation.log
     ```
   - For installations on non-English operating systems,

     ```
     "Nymi Runtime Installer version.exe" ServiceAccount="LocalSystem" /
     exenoui InstallAgent=0 /q /log NymiRuntimeInstallation.log
     ```

   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.
     ```

What to do next

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

11.2 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.

Procedure

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
     NymiRuntimeInstallation.log
     ```
   - For installations on non-English operating systems,

     ```
     "Nymi Runtime Installer version.exe" ServiceAccount="LocalSystem" /
     exenoui /q /log NymiRuntimeInstallation.log
     ```

   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.

What to do next

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

11.3 Installing or Updating Nymi Lock Control Silently

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

Procedure

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 Solution Consultant.
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 Connected Worker Platform 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.

11.4 Installing the Nymi Band Application Silently

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

Before you begin

Before you install the Nymi Band Application, install the Nymi Runtime

Procedure

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

2. Launch the command prompt as administrator.

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

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

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

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

11.5 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.

About this task

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

Procedure

1. You can install the Nymi Agent silently by typing one of the following commands:
   - ```
     "Nymi Runtime Installer version.exe" /exenoui InstallEndpoint=0 /q /log NymiRuntimeInstallation.log
     ```
   - For installations on non-English operating systems,

     ```
     "Nymi Runtime Installer version.exe" ServiceAccount="LocalSystem" /exenoui InstallEndpoint=0 /q /log NymiRuntimeInstallation.log
     ```

   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.text -o C:\Nymi\NymiAgent\
    ```

    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.

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