Deployment Guide

Nymi with Evidian Solution
v12.0
2025-08-07

Contents

3 - Preface

Nymi™ provides periodic revisions to products like the Nymi Band and Nymi Connected Worker Platform. Therefore, some functionality that is described in this document might not apply to all currently supported Nymi products. The *Connected Worker Platform Release Notes* provide the most up to date information.

Purpose

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

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

Audience

This guide provides information about how to deployment the components in the Nymi with Evidian Solution to NES and Evidian Access Management Administrators. An NES Administrator and Evidian Access Management Administrator are people in the enterprise that manages the Nymi with Evidian Solution in their workplace.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
12.0	August 07, 2025	Twelfth release of this document. This document combines the information from 3 Nymi with Evidian Installation and Configuration Guides into a single deployment guide and removes administration content which now appears in the *Nymi With Evidian Solution—Administration Guide*. Additionally, added new registry keys for the RFID-only client configurations.

Version	Date	Revision history
11.0	November 15, 2024	Eleventh release of this document. Updated to include: • Steps for NES configuration when you use CWP 1.18.0 and later. • Addition of how to delegate admin role to users. • Inclusion of Windows 11 support for clients. • Updates to the NES URL registry key type. • Changed service account from SQL service account to Evidian service account in the *Install Audit Database* section.
10.0	March 25, 2024	Tenth release of this document for CWP 1.3 and later releases. Updated to include: • New self-enrollment functionality that applies to CWP 1.16.0 and later • New registry key setting DoNotManageProcList for Citrix.
9.0	February 29, 2024	Ninth release of this document for the CWP 1.3 and later releases. Updates include: • Updates to the *Post Deployment Considerations* chapter to include information about backup and recovery. • Reorganization of Evidian EAM Client installation content to group Evidian-specific registry key settings into a single table. • Updated content in the Creating the Access Point Profile sections to remove the reference to enable the option *Always authenticate on cache.*

Version	Date	Revision history
8.0	February 26, 2024	Eighth release of this document for the CWP 1.3 and later releases. Updates include: • Addition of the RFIDSelfEnrollAllowed registry key to prevent users from performing a self-enrollment in Evidian, which allows them to use the same in multiple environments. • Addition of the RFIDSelfEnrollAllowed registry key to prevent users from performing a self-enrollment in Evidian, which allows them to use the same in multiple environments. • Changes to the Installing the Audit Database section.

Version	Date	Revision history
7.0	November 15, 2023	Seventh release of this document for the CWP 1.3 and later releases. Updates include: • Adjustments to the sequence of steps for Enrollment Terminal. • Change of name for section "Optimizing NFC Taps" to "Enabling NFC Taps" • Addition of information about how to propagate technical definition updates. • Updated the Installing EAM Controller section to include steps to create customized access point profile and user profile. • Updated installing and Configuring Software on the user terminals to include information about registry changes to prevent Active Directory users that do not use the Nymi with Evidian Solution from seeing Evidian eSSO login windows. • Created *Post Deployment Considerations* chapter.
6.0	October 6, 2023	Sixth release of this document for the CWP 1.3 and later releases. Updates include: • Adjusted the sequence of steps for Enrollment Terminal. • Added new content related to Evidian components to the *Updating Nymi and Evidian Components* chapter. • Updated section *Optimizing NFC Taps* to include unsupported use case and where to set the registry keys.

Version	Date	Revision history
5.0	August 21, 2023	Fifth release of this document for the CWP 1.3 and later releases. Updates include: • New content that describes how to optimize NFC tap performance in a wearable configuration. • Revisions of the Updating chapter. • Details about support for Nymi Band taps on a Bluetooth adapter. • New appendix to document how change a user terminal from RFID-only mode to wearable mode.
4.0	June 19, 2023	Fourth release of this document for the CWP 1.3 and later releases. Updates include: • New content in the topic to create an SSO definition for a new target application. • New content that describes how to configure the username field for SSO. • New content that describes how to perform a delete user data operation for a found Nymi Band. • Corrected images sizes in some topics.
3.0	March 17, 2023	Third release of this document for the CWP 1.3 and later releases. Updates include: • Extensive updates to include more images.
2.0	January 13, 2023	Second release of this document for the CWP 1.3 and later releases. Updates include: • Changes to EAM client deployments.

Version	Date	Revision history
1.0	May 16, 2022	First release of this document for the CWP 1.3 and later releases.

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 With Evidian Solution—Administration Guide**

  The Nymi With Evidian Solution—Administration Guide provides information about how to administer and maintain the Nymi with Evidian solution.
- **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.

How to get product help

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

How to provide documentation feedback

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

4 - Nymi Connected Worker Platform with Evidian Access Management Solution Overview

The Nymi with Evidian Solution extends the use of the Nymi Band. With Evidian Authentication Manager, a user can use their Nymi Band to lock and unlock a Windows desktop. With Evidian Single Sign On (SSO), a user can use their Nymi Band to perform MES authentication events. There are several supported deployment configurations in the Nymi with Evidian Solution.

Supported Evidian Authentication Methods

The Nymi Band supports three authentication methods when a user performs a Nymi Band tap to complete authentication tasks in an Evidian environment:

- Wearable mode—The Nymi with Evidian Solution cryptographically authenticates the Nymi Band over Bluetooth. This is the default and recommended authentication method. In this mode, the solution configures the Nymi Band as a wearable device and users can perform an Nymi Band tap on the Nymi-supplied Bluetooth Adapter (BLE tap) or NFC reader (NFC tap) to complete authentication tasks.
- RFID-only mode—The Nymi with Evidian Solution identifies the Nymi Band by using only the NFC UID without cryptographic authentication. In this mode, the solution configures the Nymi Band as an RFID-only device and users can perform a Nymi Band tap on an NFC reader (NFC Taps) to complete authentication tasks.
- RFID-only mode with Secure NFC—Extends RFID-only mode. The Nymi with Evidian Solution identifies the Nymi Band by using SEOS credentials which can be encoded onto the secure NFC applet on any SEOS-capable Nymi Band. The credential is protected by cryptographic authentication and anti-spoofing mechanism that provide a security layer when the Nymi Band is tapped on a SEOS-capable reader.

The Nymi-POMSnet Solution extends the use of the Nymi Band. The Nymi Band gives users passwordless access to POMSnet and the ability to apply their digital signature to process sign-offs.

You can deploy the Nymi with Evidian Solution in two different configurations. Review the following information to decide which configuration to deploy.

Deployment Configuration	Use Case	Nymi Agent Installation
Decentralized Nymi Agent	User terminals are thick clients and your application is installed on the user terminal.	Install the Nymi Agent software on each user terminal.

Deployment Configuration	Use Case	Nymi Agent Installation
Centralized Nymi Agent	User terminals are thin clients that connect to an RDP session host or Citrix server to access the application.	Deploy a single instance of the Nymi Agent in a centralized location and configure the user terminals to use the centralized Nymi Agent.

Consider the following:

- Most deployments make use of a Centralized Nymi Agent configuration.
- 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 configuration, and then configure your all your user terminals to use a centralized or decentralized Nymi Agent.

If you choose to implement a decentralized Nymi Agent configuration, refer *Appendix A* for instructions about how to install and configure the Nymi components.

Supported Nymi with Evidian Solution Configurations

You can deploy the Nymi with Evidian Solution in two different configurations. Review the following information to decide which configuration to deploy.

Deployment Configuration	Use Case	Nymi Agent Installation
Decentralized Nymi Agent	User terminals are thick clients and your application is installed on the user terminal.	Install the Nymi Agent software on each user terminal.
Centralized Nymi Agent	User terminals are thin clients that connect to an RDP session host or Citrix server to access the application.	Deploy a single instance of the Nymi Agent in a centralized location and configure the user terminals to use the centralized Nymi Agent.

Consider the following:

- Most deployments make use of a Centralized Nymi Agent configuration.
- 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 configuration, and then configure your all your user terminals to use a centralized or decentralized Nymi Agent.

If you choose to implement a decentralized Nymi Agent configuration, refer *Appendix A* for instructions about how to install and configure the Nymi components.

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

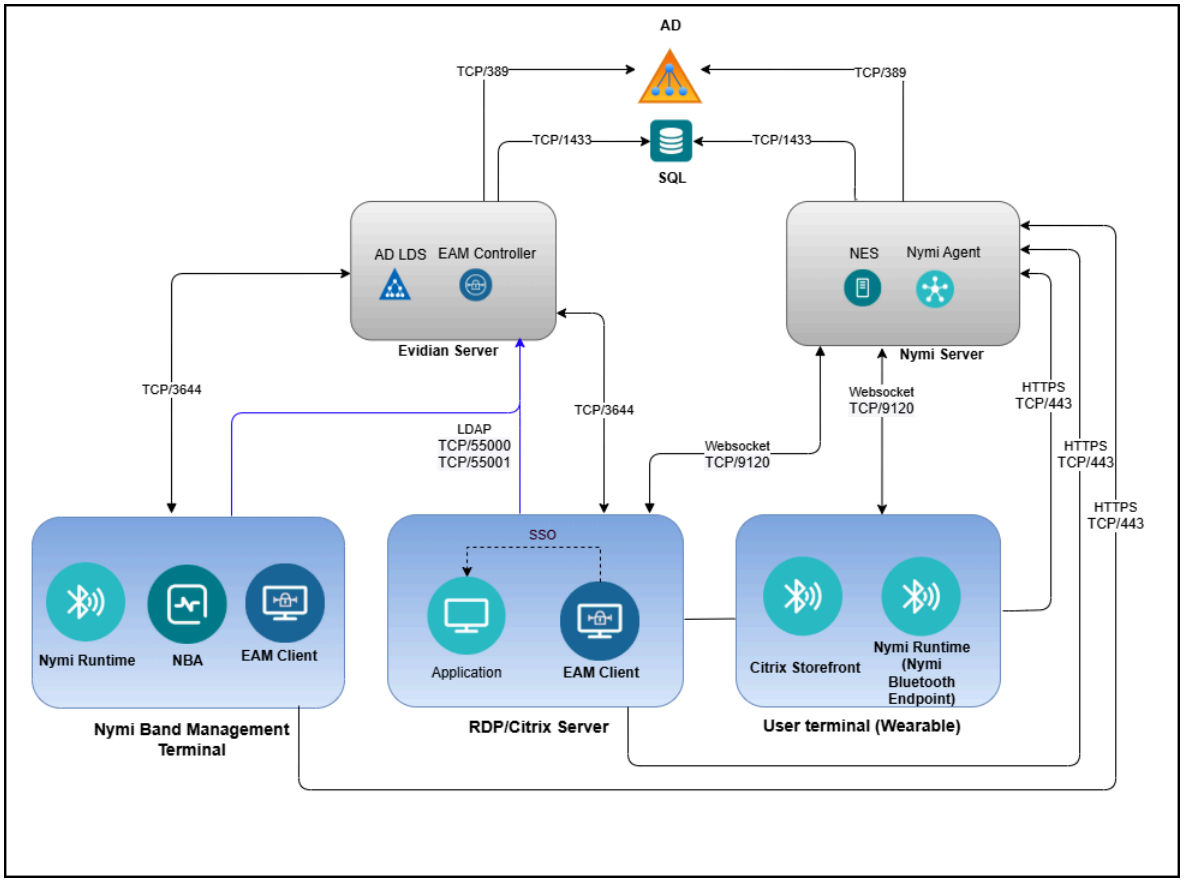


Figure 1: Connected Worker Platform with Evidian components in a Citrix/RDP environment

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*.

Table 2: Connected Worker Platform Components

Component	Description
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.
Nymi Band Application 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.

Component	Description
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 client-based Windows application. Nymi Runtime supports communication between NES, the Nymi Band, NEAs, the Nymi Band Application and Nymi Lock Control. Nymi Runtime contains two components, that you can install together or separately, the Nymi Agent and the Nymi Bluetooth Endpoint.
Thin Client User Terminal (wearable)	A Windows 10 or Windows 11 endpoint that users use to access a remote session host and launch an NEA that is installed on a remote session host. In a wearable configuration, you only install the Nymi Bluetooth Endpoint component of the Nymi Runtime on the user terminal. You must plug the Nymi-supplied Bluetooth adapter into a free USB port on the thin client user terminal and you can perform Nymi Band taps on the Bluetooth adapter or an NFC reader.
User Terminal (thick client) *not pictured	An endpoint that users use to access an NEA that is installed the user terminal. A thick client user terminal does not connect to a Centralized Nymi Agent. When you install Nymi Runtime on a thick client user terminal, you install the Nymi Bluetooth Endpoint and the Nymi Agent components.
Thin Client User Terminal (RFID-only)	A Windows 10 or Windows 11 endpoint that users use to access a remote session host and launch an NEA that is installed on a remote session host. In RFID-only mode, you do not install any Nymi or Evidian components on the thin client and you do not plug in the Nymi-supplied Bluetooth adapter.

Component	Description
RDP/Citrix 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 application that requires log in or e-signature request that require user credentials. Different user sessions run their own application instance. You must install the Evidian EAM Client software on the RDP/Citrix server
Centralized Nymi Agent	A Nymi Runtime component that you install on a server that is accessible to all user terminals, for example the NES server.
Enterprise Access Management Client	The client-side Evidian software that provides users with a single sign-on (SSO) experience at the user terminal.
Evidian Enterprise Access Management Controller	Evidian Enterprise Access Management (EAM) Controller allows centralization of User Access policy definition and audit events. Includes Evidian Enterprise SSO software that provides agile single sign-on (SSO). The Evidian EAM Management Console application provides the interface to perform management activities.
AD LDS	Microsoft component that the EAM controller installs locally by default. Provides storage of Active Directory data related to users and computers.
SQL Server	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.

4.1 - Nymi Connected Worker Platform with Evidian Access Management

Solution Overview (Decentralized Nymi Agent)

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

Note: The Nymi with Evidian Solution in a decentralized Nymi Agent configuration is also referred to as a local configuration.

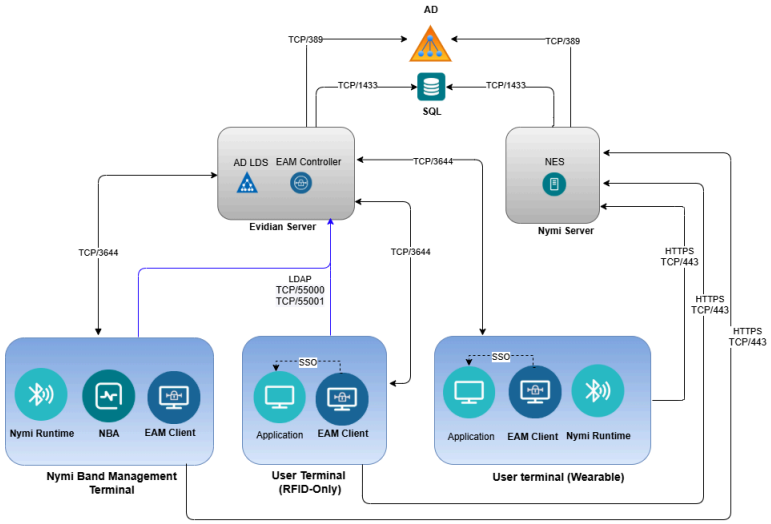


Figure 2: Connected Worker Platform with Evidian components in a Decentralized Nymi Agent environment

The following table summarizes the component configurations local configuration.

Table 3: Connected Worker Platform Components

Component	Description
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.
Nymi Band Application 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.

Component	Description
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 client-based Windows application. Nymi Runtime supports communication between NES, the Nymi Band, NEAs, the Nymi Band Application and Nymi Lock Control. Nymi Runtime contains two components, that you can install together or separately, the Nymi Agent and the Nymi Bluetooth Endpoint.
Wearable User Terminal (thick client)	An endpoint that users use to access an application that is installed the user terminal. A thick client user terminal does not connect to a Centralized Nymi Agent. When you install Nymi Runtime on a thick client user terminal, you install the Nymi Bluetooth Endpoint and the Nymi Agent components.
RFID-Only User Terminal (thick client)	A Windows 10 or Windows 11 endpoint that users use to access an application that is installed on the user terminal. In RFID-only mode, you do not install any Nymi components on the user terminal and you do not plug in the Nymi-supplied Bluetooth adapter.
Enterprise Access Management Client	The client-side Evidian software that provides users with a single sign-on (SSO) experience at the user terminal.
Evidian Enterprise Access Management Controller	Evidian Enterprise Access Management (EAM) Controller allows centralization of User Access policy definition and audit events. Includes Evidian Enterprise SSO software that provides agile single sign-on (SSO). The Evidian EAM Management Console application provides the interface to perform management activities.
AD LDS	Provides data storage and retrieval support for directory-enabled applications.

Component	Description
SQL Server	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.

5 - Use Cases

A user can tap their authenticated Nymi Band on a supported NFC reader or the Nymi-supplied Bluetooth adapter to perform the following tasks:

- Manufacturing Execution System (MES) application login
- Double signature
- Citrix Storefront login
- RDP login
- Single sign on with enterprise authentication

6 - Environment Configuration

The section outlines the configuration requirements for the Nymi with Evidian Solution.

6.1 - Networking Requirements

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

6.1.1 - Domain Name Service Requirements for Non-Clustered Deployment

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

Non-Clustered CWP Deployment

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

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

Table 4: 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

6.1.2 - 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.

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.

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.

6.1.3 - Firewall Port Requirements

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

Connection Port Requirements

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

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

Table 5: Connection Port Requirements

Purpose	Protocol	Source	Virtual Server FQDN & Port	Destination and Port
SQL Access	MS SQL Proprietary	NES Evidian EAM Controller	n/a	SQL Server: 1433/TCP
LDAP Access-Active Directory(AD)	LDAP/LDAPS	NES Evidian EAM Controller	n/a	AD Server: 389/TCP (For LDAP configurations) 636/TCP (For LDAPS configurations)

Purpose	Protocol	Source	Virtual Server FQDN & Port	Destination and Port
NES Communications	HTTPS	Machine that accesses NES Administrator Console All Wearable Mode User Terminals (thick). RDP/Citrix servers that run NEAs Centralized Nymi Agent	nes.cwp.company.com: 443/TCP	NES: 443/TCP
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 Wearable User Terminals (thick and thin) RDP/Citrix Servers that run NEAs. in a wearable mode configuration.	nymiagent.cwp.company.com 9120/TCP	nymiagent-0.cwp.company.com nymiagent-1.cwp.company.com: 9120/TCP

Purpose	Protocol	Source	Virtual Server FQDN & Port	Destination and Port
Support Evidian communications	TCP	All user terminals with the Evidian EAM Client software (including RDP/Citrix session hosts)	eam_server.cwp.company.com Port 3644 to the Evidian EAM Controller. **Note:** Ensure that port 3644 is open bidirectionally. For LDAP, port 55000 to the Evidian EAM Controller or For LDAPs, port 55001 to the Evidian EAM Controller	eam_server-01.cwp.company.co eam_server-02.cwp.company.co Port 3644 to the Evidian EAM Controller. For LDAP, port 55000 to the Evidian EAM Controller or For LDAPs, port 55001 to the Evidian EAM Controller

6.1.4 - 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.

6.2 - Active Directory Requirements

The Nymi with Evidian Solution has several Active Directory (AD) user account and AD group requirements.

6.2.1 - Evidian Active Directory Requirements

To prevent Active Directory (AD) accounts from using the Evidian Enterprise Access Management (EAM) solution and Evidian licenses, create one AD group that contains the AD user accounts that use the Nymi Band to complete authentication tasks.

This group is referred to as an inclusion group. You will associate the inclusion group with an Evidian access point profile that is assigned to user terminals on which you will deploy the Evidian ESSOAgent software, as described later in this guide.

Evidian allocates one Evidian license to a user in the inclusion group, the first time the user logs into an Evidian EAM Client or when the SSO engine starts.

Note: As you add new users to the Nymi with Evidian Solution, ensure that you add their user account to the inclusion group.

6.2.2 - 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.

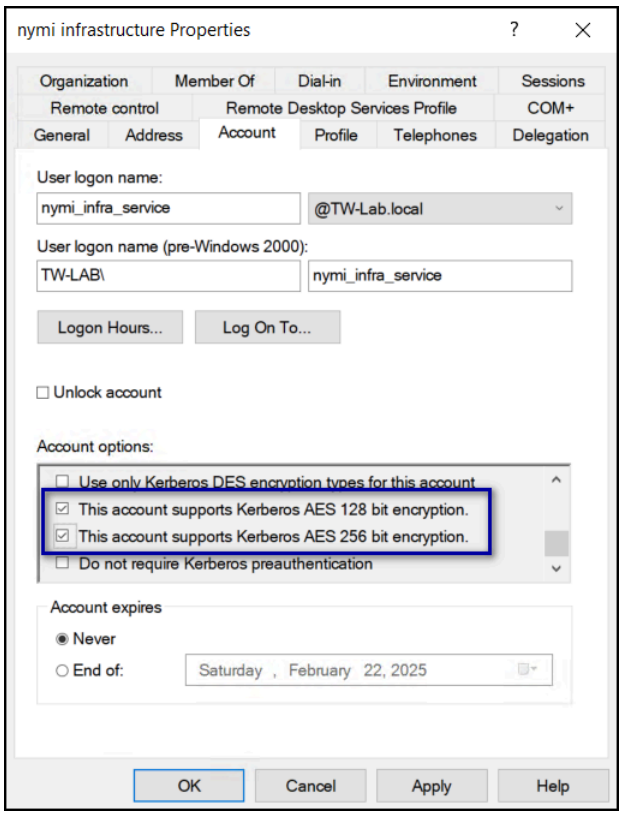
6.2.3 - Creating the Nymi Infrastructure Service Account

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.



6.2.4 - Creating the Evidian Service Account

Evidian uses a service account for SQL server and AD LDS authentication.

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

- Domain user.
- Password never expires.
- A member of the inclusion group.
- Username is less than 20 characters.
- Allow log on locally privileges, when you use Windows authentication to allow access to the Evidian audit database access.
- Ability to log in to the SQL server and db_owner rights to the Evidian Audit database.
- AD LDS instance administrator for both the configuration and application data partitions, which the Evidian EAM Controller installation process sets automatically.

Note: You can use the Nymi Infrastructure Service Account as the Evidian service account.

6.3 - Nymi Band Application Terminal and User Terminal Requirements

The user terminal is a Windows 10 (minimum build version 1607) or Windows 11 machine that operators use to perform MES authentication tasks. A Nymi Band Application Terminal is a Windows 10 (minimum build version 1607) or Windows 11 machine that users access to perform enrollments or authenticate to their NB by using their corporate credentials.

User terminals include:

- Thick client machines
- Thin client machines
- RDP/Citrix session hosts

The following table summarizes the Nymi Band Application Terminal and user terminal requirements.

Component Type	Hardware and Software Requirements
Nymi Band Application Terminal	• Nymi Band Application software, which also installs the Nymi Runtime software • Evidian EAM Client software • Evidian license file • Bluetooth Adapter • Local Administrator access or Directory Administrator Access.
Wearable Mode Thick Client	• Nymi Runtime software including the Nymi Bluetooth Endpoint and the Nymi Agent components. • Evidian EAM Client software • Evidian license file • Nymi-supported NFC Reader (optional) • Bluetooth Adapter
Wearable Mode Thin Client	• Nymi Runtime software including the Nymi Bluetooth Endpoint component. • Nymi-supported NFC Reader (optional) • Bluetooth Adapter
RFID-only Thick and Thin clients	• Evidian EAM Client software • Evidian license file • Nymi-supported NFC Reader

Component Type	Hardware and Software Requirements
RDP server / Citrix Session Host	• Evidian EAM Client • Evidian license file • Smart Card USB redirection enabled **Note:** Environments can also have GPO restrictions on USB redirection. Allow Smart Card USB redirection provides more information.

6.3.1 - 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.

6.4 - NES Requirements

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

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

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.

6.5 - Evidian EAM Controller Requirements

Install the following software on the Evidian EAM Controller to support communications with the audit database.

- Microsoft OLE DB Driver for SQL
- Visual C++ redistributable for Visual Studio 2022 version 1434 or later (x64 and x86 versions)
- **Note:** When the installation completes, a server reboot is required.

6.6 - 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.

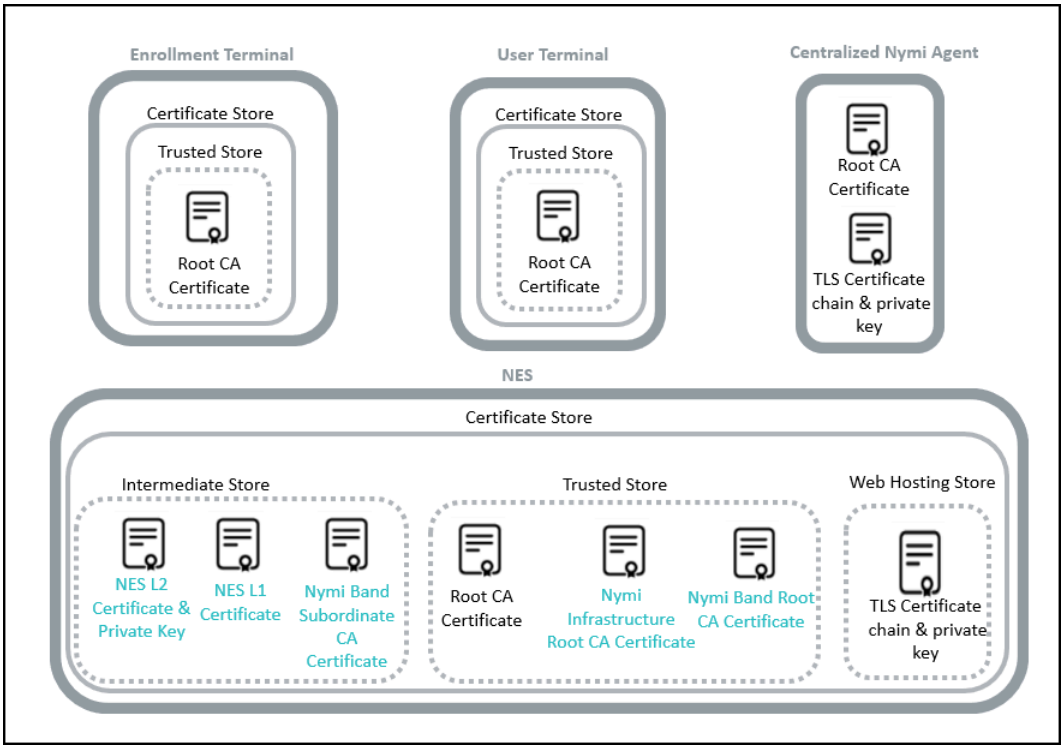


Figure 3: Certificates

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

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.

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

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.

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.

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

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*.

6.6.1 - Evidian Certificate Requirements

For LDAPS configurations, you require a TLS certificate for the Evidian EAM Controller.

The TLS certificate must meet the following requirements:

- Be issued by a trusted Certificate Authority (CA).
- Be in PKCS #12 format (.PFX or .P12)
- Implement the enhanced key usage (EKU) extension and contain the PKI Server Auth (1.3.6.1.5.5.7.3.1) OID. Enhanced Key Usage: Server Authentication (1.3.6.1.5.5.7.3.1).
- Specify the FQDN of the Evidian EAM Controller/ADLDS server in the certificate subject line.

Note: If the Nymi Enterprise Server(NES) and Evidian EAM Controller/AD LDS server are the same machine, you can use the same TLS certificate.

6.6.2 - 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.

6.7 - 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.

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.

6.7.1 - Creating the EAM Audit Database

The EAM installation package includes a SQL script that you can use in SQL Server Management Studio(SSMS) to create the audit database.

Before you begin

Consider the following:

- You can install the Audit Database on the same SQL Server that you use for Nymi Enterprise Server(NES).
- On the Evidian EAM Controller machine, ensure that the Evidian service account has the right to log in locally and is a member of the local Administrators group.
- On the SQL Server, ensure that the SQL browsing service is running.

About this task

Perform the following steps to create a EAM audit database on an existing SQL Server.

Procedure

1. From the EAM installation package, obtain the *MSSQLV2.sql* file from the *.. \EAM.x64\TOOLS\WGSrvConfig\Support* directory.
2. Use SSMS to connect to the SQL Server.
3. From the **`Tools`** menu, select **`New Query`**.
4. In the **`New Query`** window, copy and paste the contents of the *MSSQLV2.sql* file.

Results

The eamaudit database appears in the **`Databases`** folder.

What to do next

Assign the Evidian service account db_writer and db_reader rights to the Audit Database.

6.7.2 - 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**.

6.7.3 - 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.

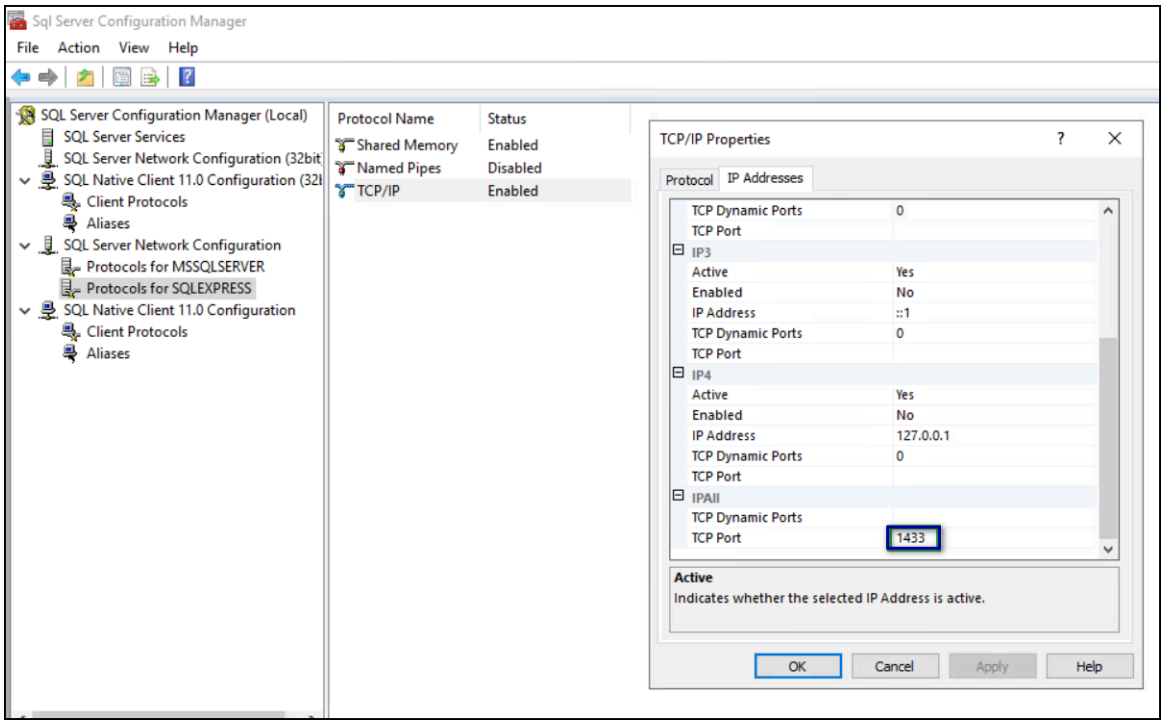


Figure 4: Configuring SQL Port

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

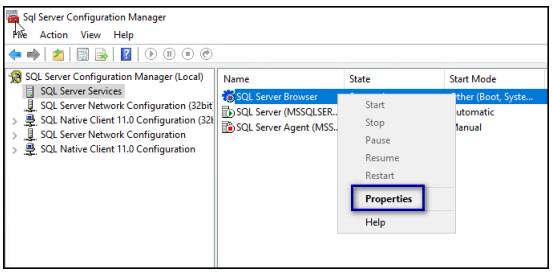


Figure 5: SQL Browser Properties option

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

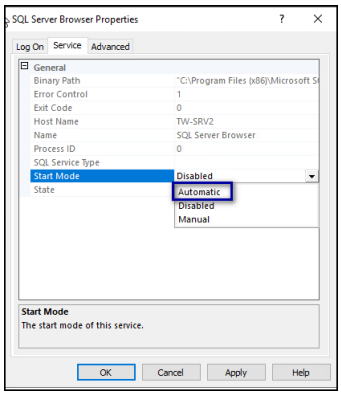


Figure 6: Start Mode

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

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

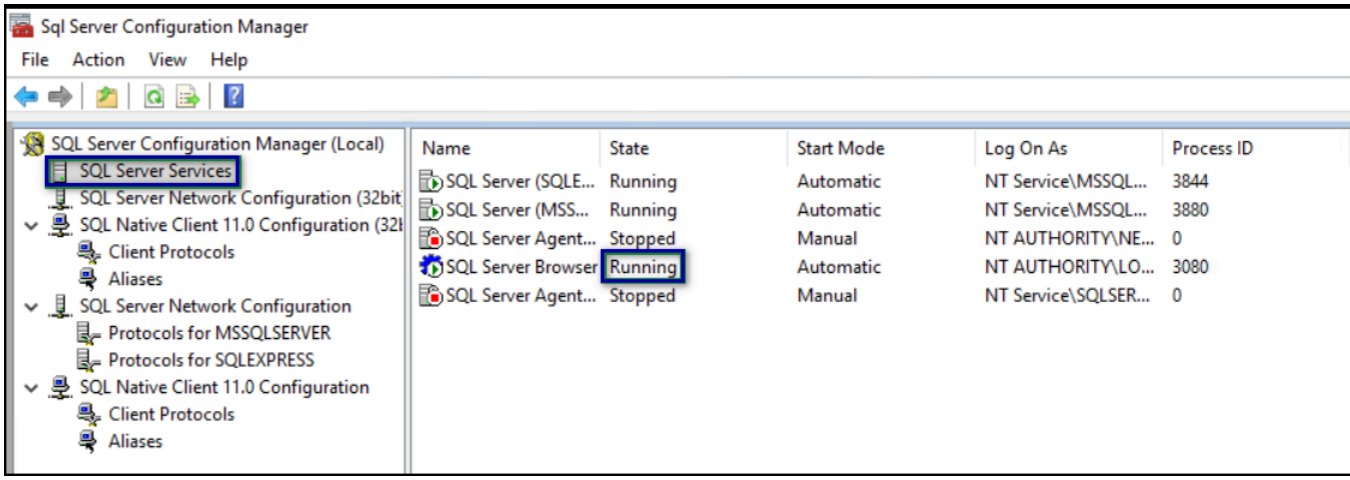


Figure 7: SQL Server Browser service

6.8 - Bluetooth Tap Support

In a wearable configuration, users can perform a Nymi Band tap on the Nymi-supplied Bluetooth adapter (BLE tap) to complete authentication tasks.

The Nymi with Evidian Solution supports BLE taps by default when you deploy the following versions of software in your environment:

- Connected Worker Platform 1.8.1 or later. Nymi recommends that you install or update to the latest CWP version.
- Evidian Access Management version 10.03b8573-hotfix-2 or later. Nymi recommends that you install or update to Evidian Access Management version 10.03b8820-hotfix-11.

7 - Install and Configure Nymi and Evidian Components

Install and configure the Nymi and Evidian Components in the environment.

Nymi recommends that you install the Nymi and Evidian software in the following order:

- Install and configure the Nymi Enterprise Server(NES) software on a server.
- Install and configure the Centralized Nymi Agent.
- Install and configure the Evidian EAM Controller software.
- Install and configure the Nymi Band Application Terminal.
- Install and Configure the user terminals.

7.1 - Obtain the Required Software

Obtain the required software files or the Fileshare link for the software package from your Nymi Solution Consultant.

When you receive the zip file, download and extract the contents to a machine and folder that is accessible to the Nymi Enterprise Server(NES), Evidian EAM Controller, centralized Nymi Agent server, Nymi Band Application Terminal, and user terminals.

7.2 - Install Server Components

In a Connected Worker Platform with Evidian deployment, there are two servers in the configuration, NES and the Evidian EAM Controller.

You can install the Nymi Enterprise Server(NES) software on the same server on which you plan to install the Evidian EAM Controller software. For deployments in a production environment, Nymi recommends that you install the NES and Evidian EAM Controller software on separate servers.

Note: Ensure that you configure NES with the HTTPS communication protocol.

7.2.1 - Deploy NES in a Standalone Configuration

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

7.2.1.1 - Install and Configure IIS

NES supports HTTP and HTTPS for communication between NES services. It is recommended to use HTTPS. To complete prerequisite activities for NES deployment, install

Microsoft Internet Information Server (IIS) and Microsoft ASP.NET on the NES host, and then import the TLS server certificate into IIS for secure deployments (HTTPS).

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`**.

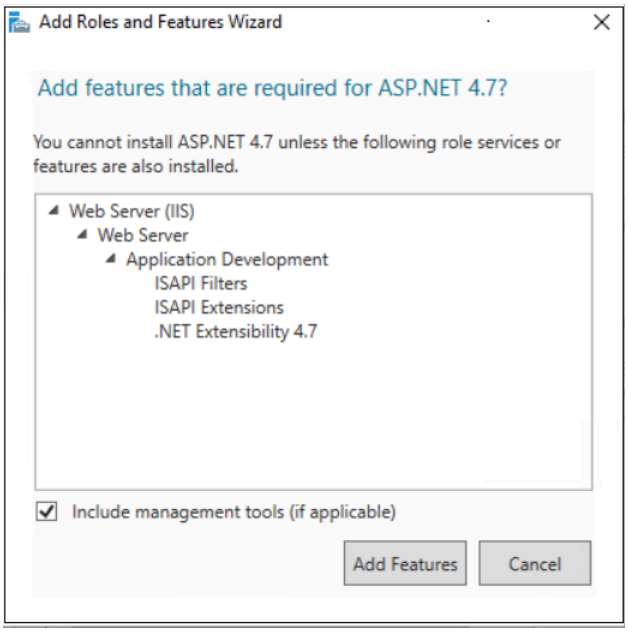


Figure 8: Add features that are required for ASP.NET

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.

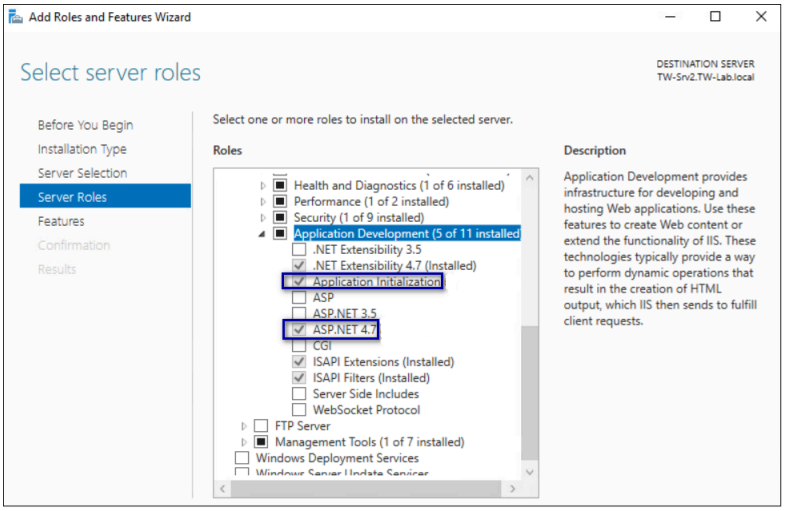


Figure 9: Select server roles page

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.

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.

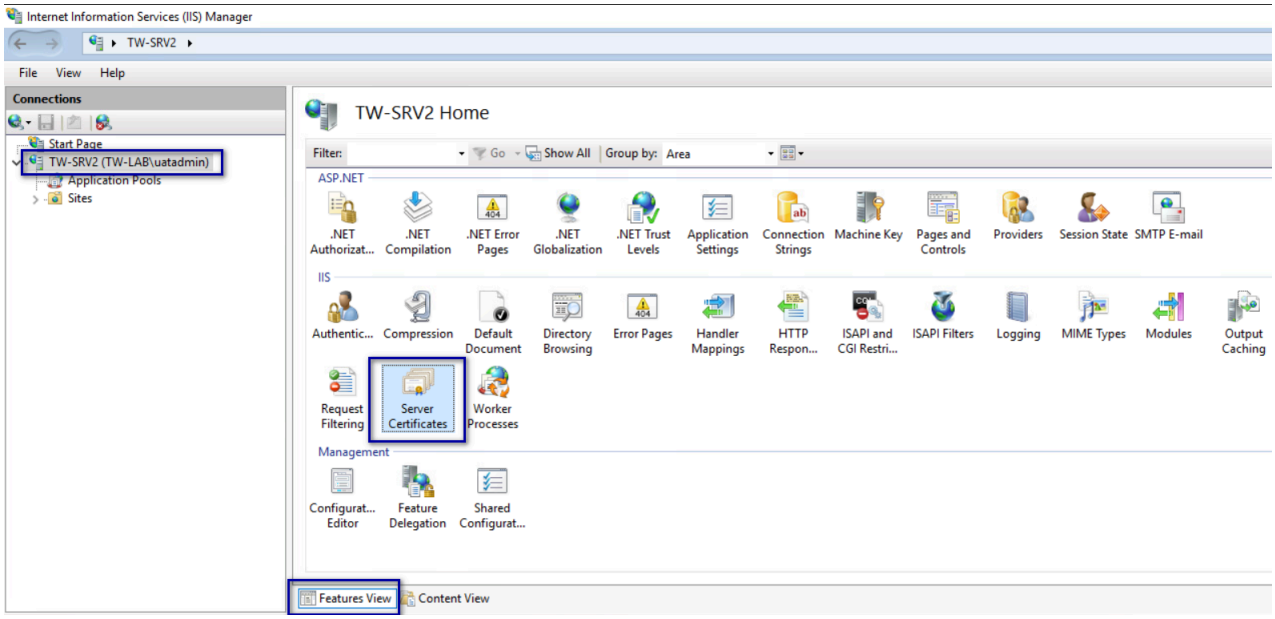


Figure 10: Server Certificates option

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.

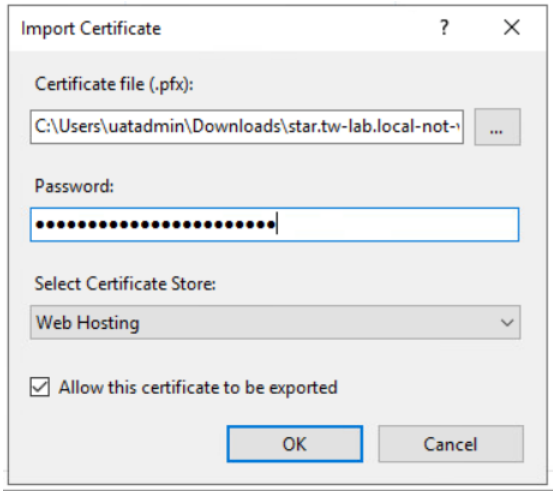


Figure 11: Server Certificates option

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.

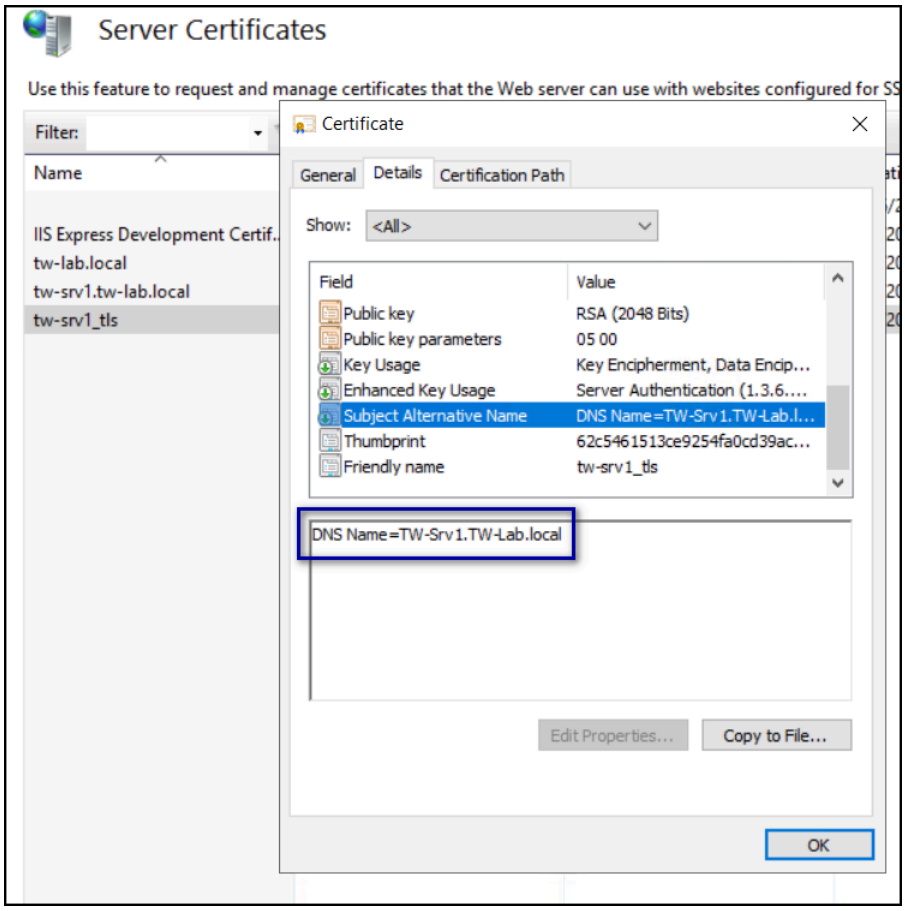


Figure 12: Server Certificates option

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.

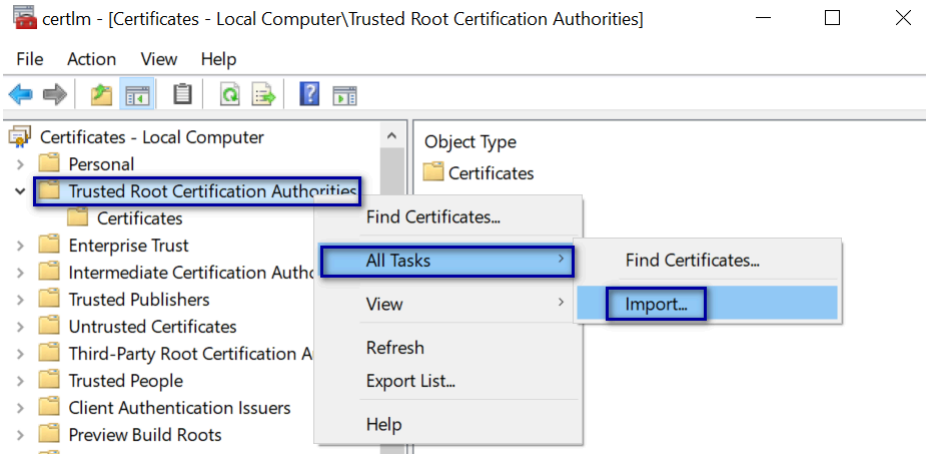


Figure 13: Import Certificate option

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

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

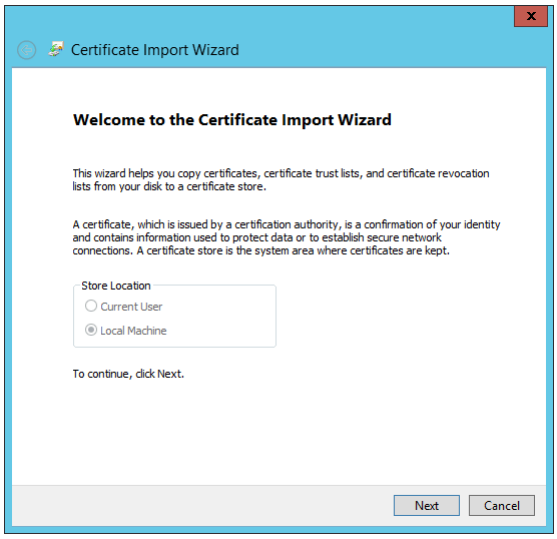


Figure 14: Welcome to the Certificate Import Wizard screen

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.

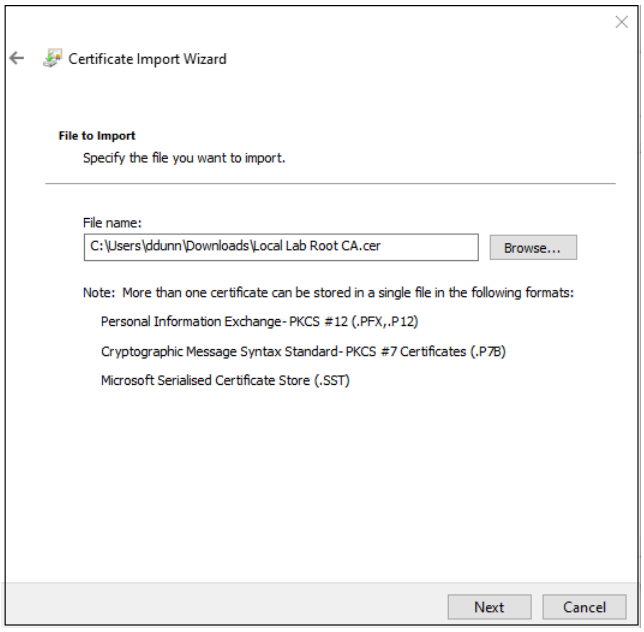


Figure 15: File to Import screen

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.

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.

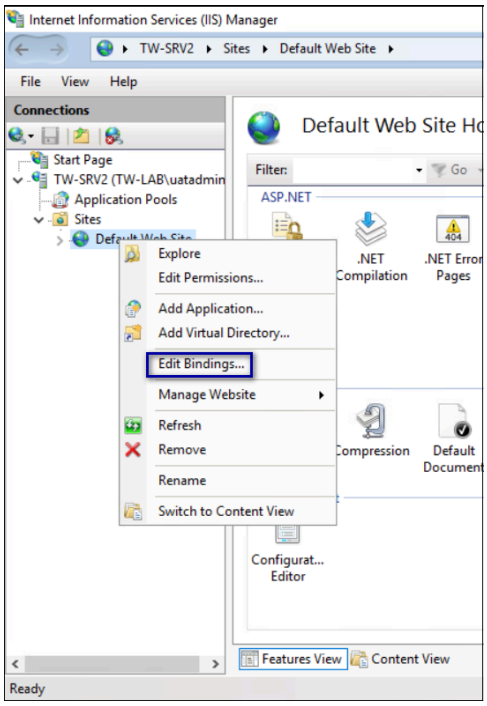


Figure 16: Edit Bindings Option

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.

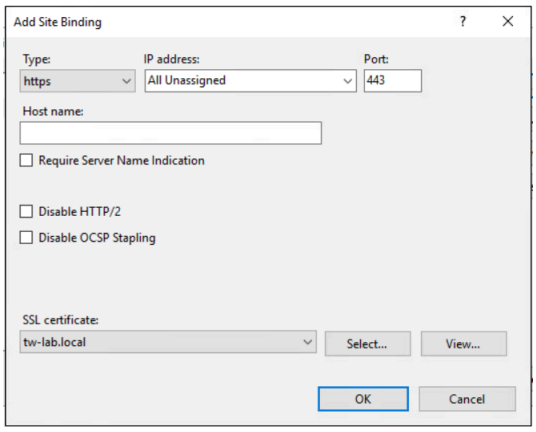


Figure 17: Add Site Binding Dialog

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`**.

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

Note: This procedure only applies to a configuration that uses a single NES instance on a remote SQL server (not local to the NES server) with SQL Authentication.

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.

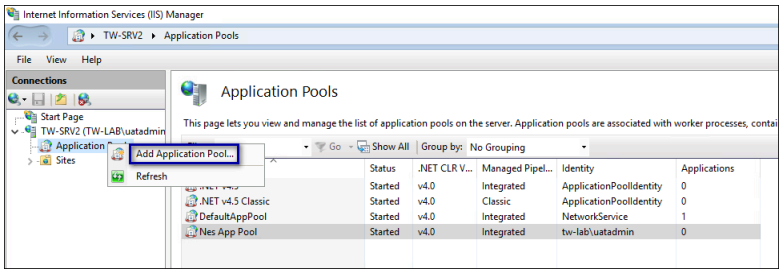


Figure 18: Create New Application Pool

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.

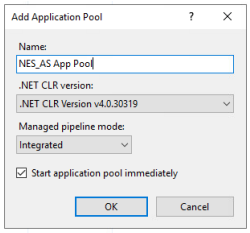


Figure 19: Add New Application Pool

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

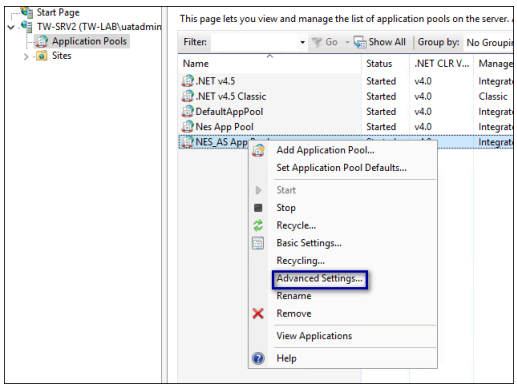


Figure 20: Advanced Settings for Application Pool

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

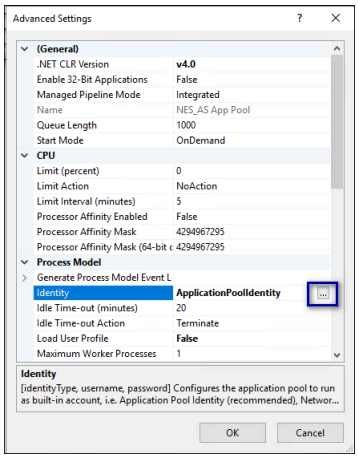


Figure 21: Edit Identity

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

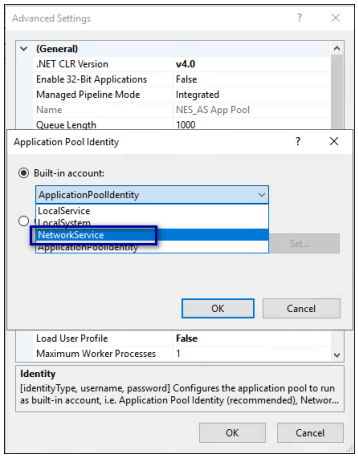


Figure 22: Built-in account list

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

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`**.

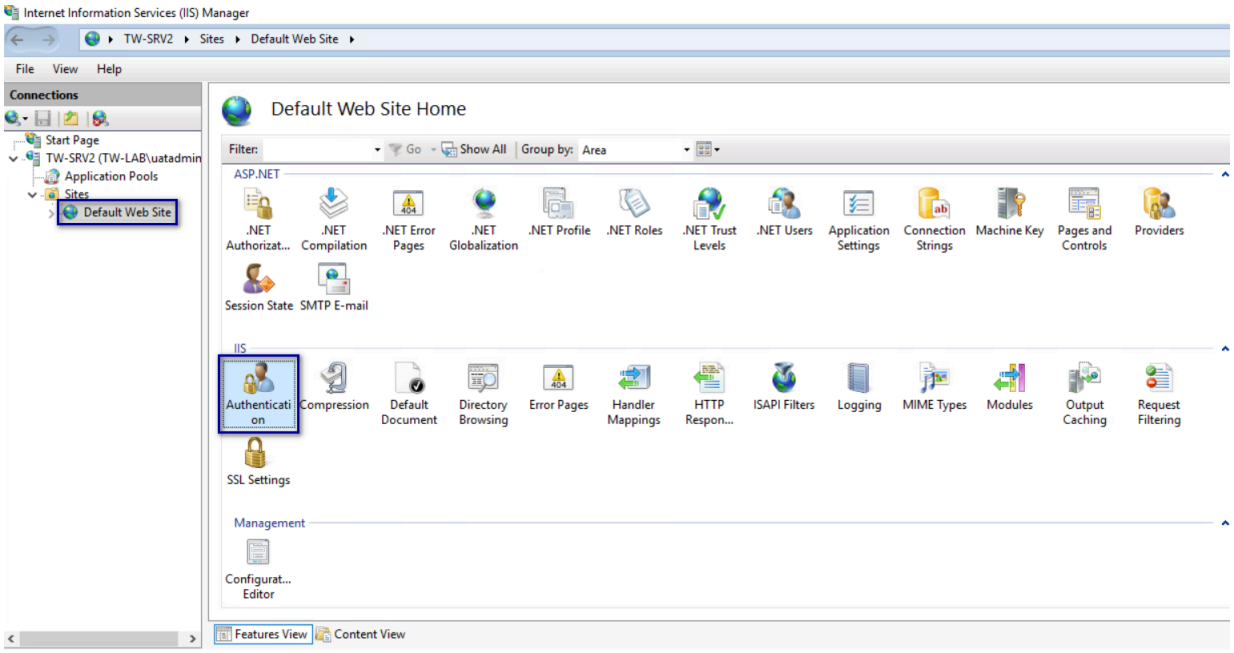


Figure 23: Authentication Option

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.

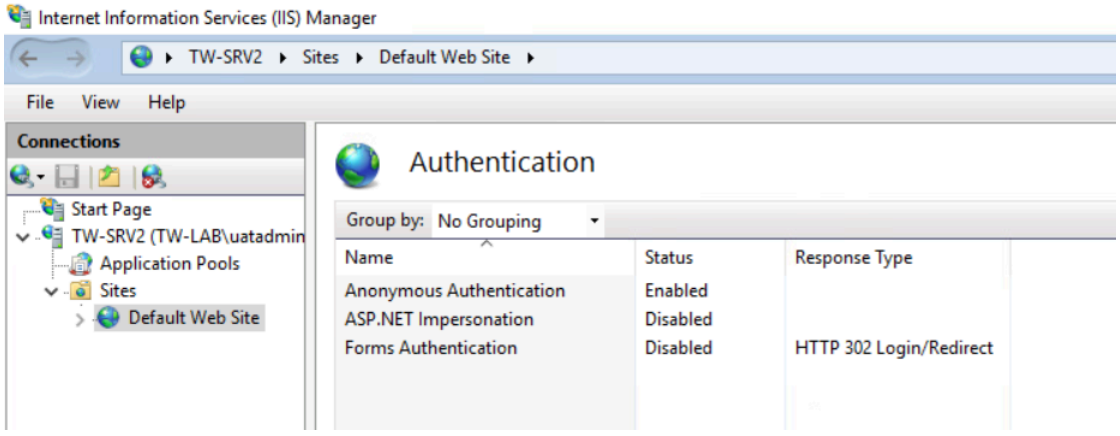


Figure 24: Authentication pane with Anonymous Authentication enabled

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`**.

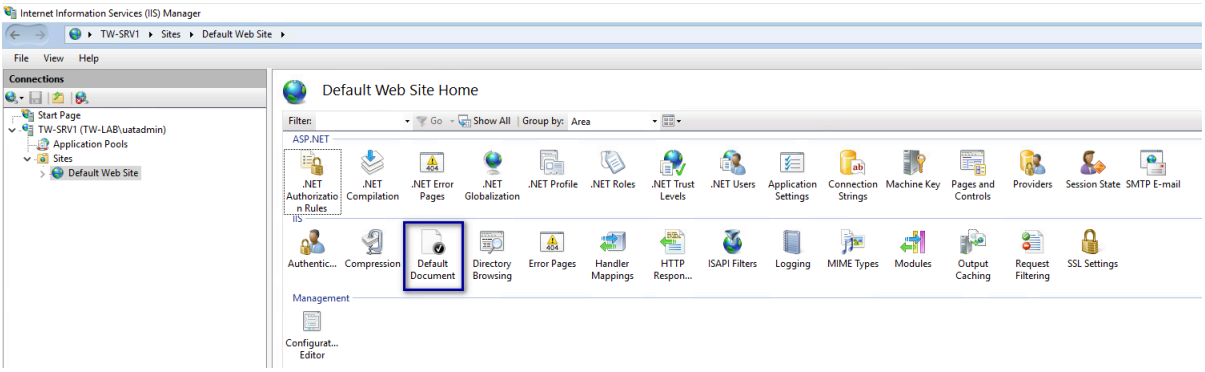


Figure 25: Default Document Option

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

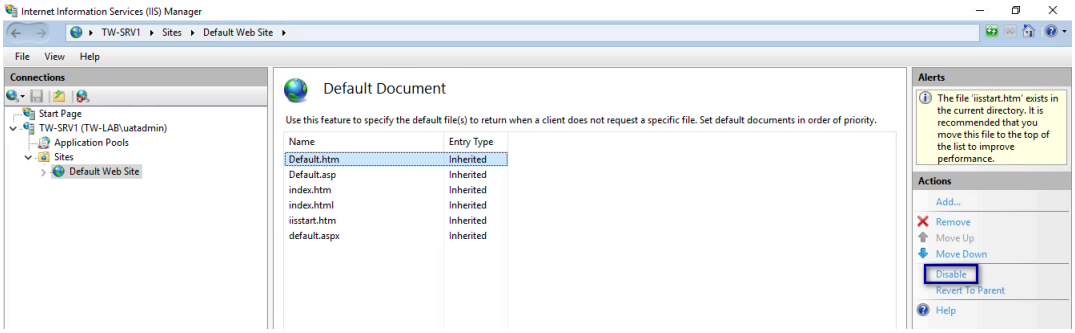
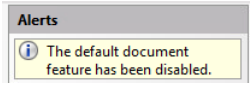


Figure 26: Disable Default.htm

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`**

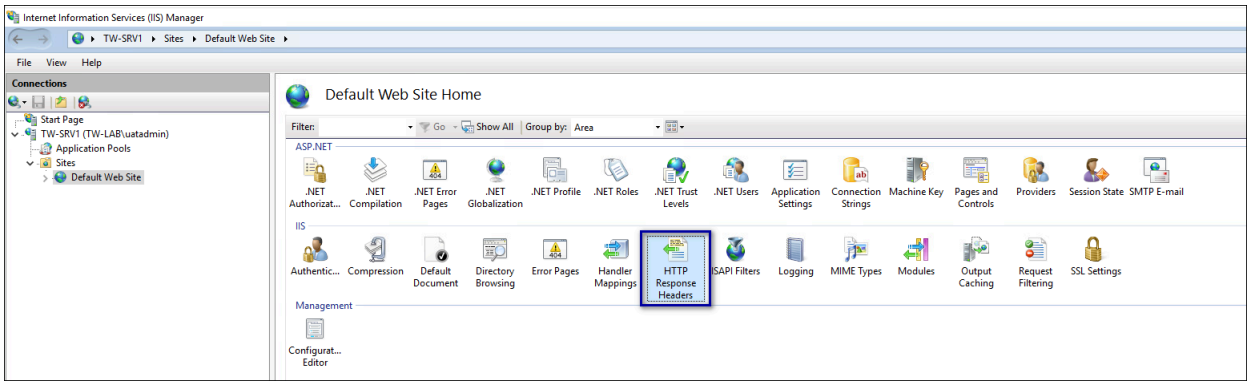


Figure 27: HTTP Response Headers Option

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

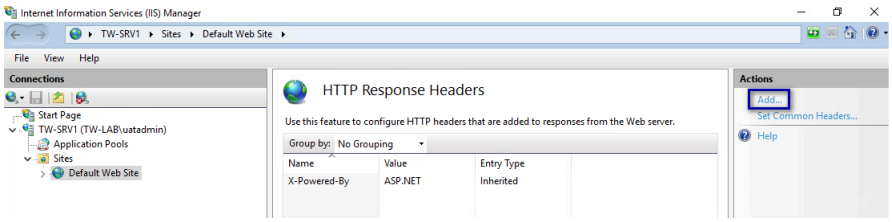


Figure 28: Add HTTP Response Headers Option

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.

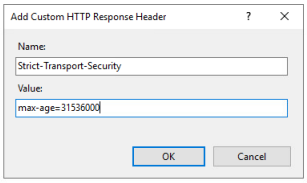


Figure 29: Add Custom HTTP Response Headers dialog box

   c) Click **OK**.

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

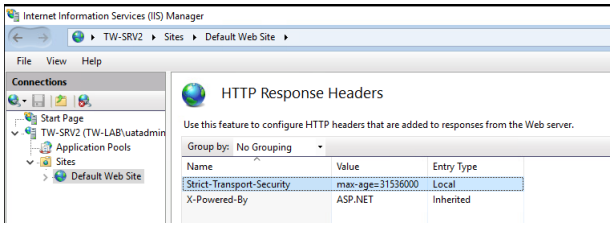


Figure 30:

6. Close `IIS Manager`

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`**.

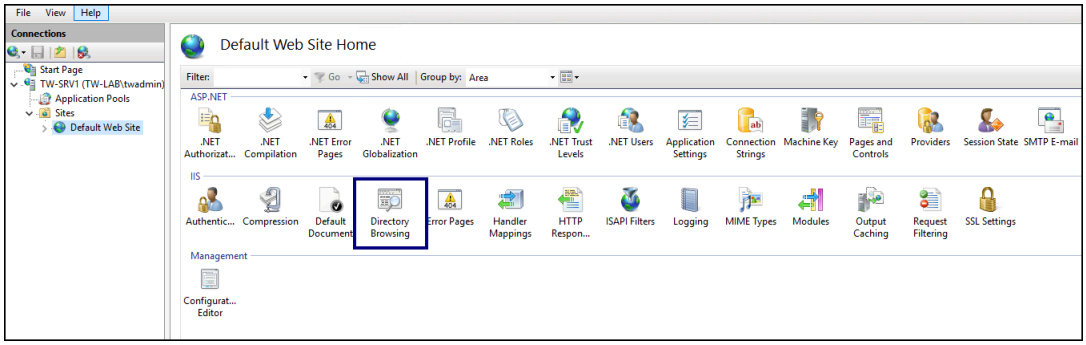


Figure 31: Directory Browsing Option

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.

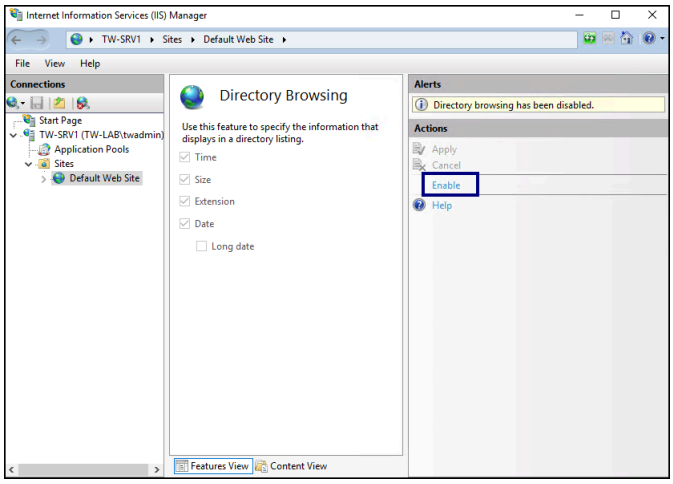


Figure 32: Enable Directory Browsing option

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

7.2.1.2 - Importing a Fullchain Certificate

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

About this task

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

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

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

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.

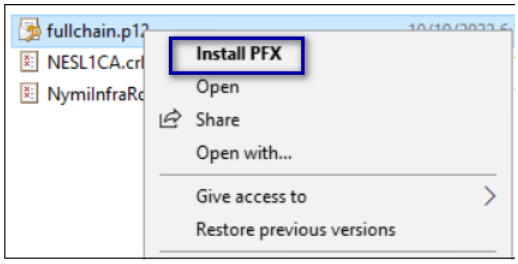


Figure 33: Install PFX Option

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.

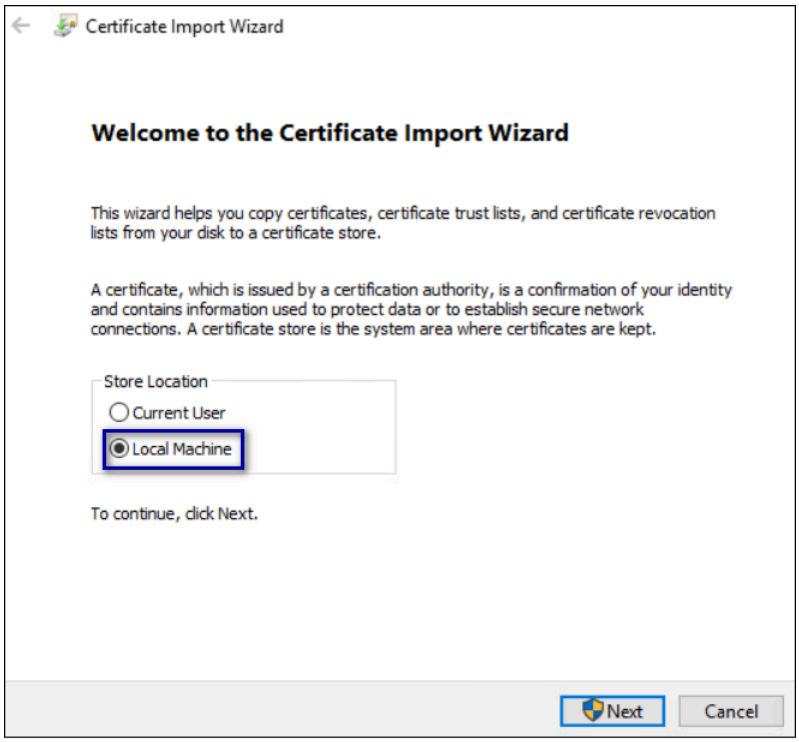


Figure 34: Local Machine Store Location

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.

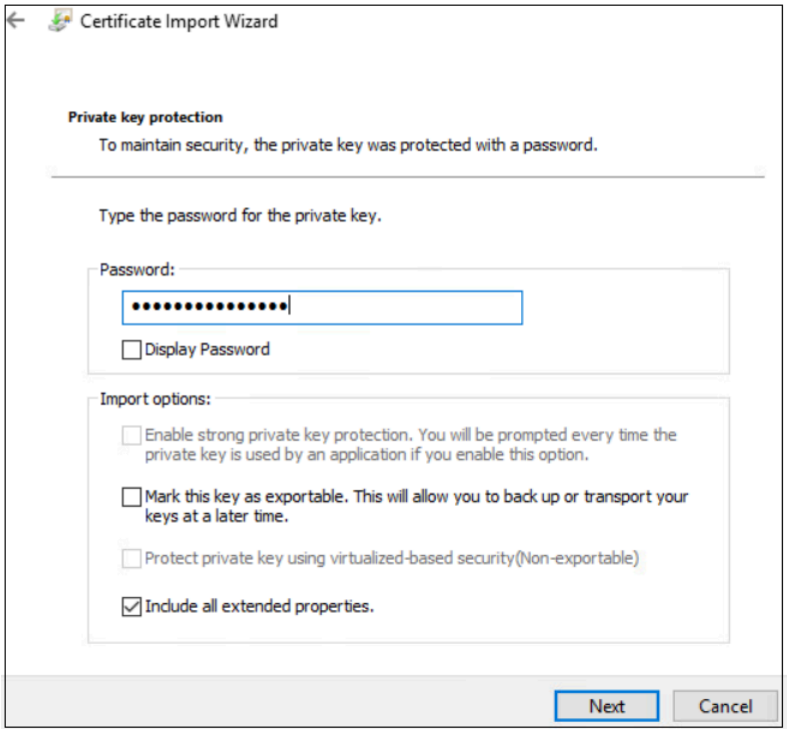


Figure 35: Private Key Protection Page

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.

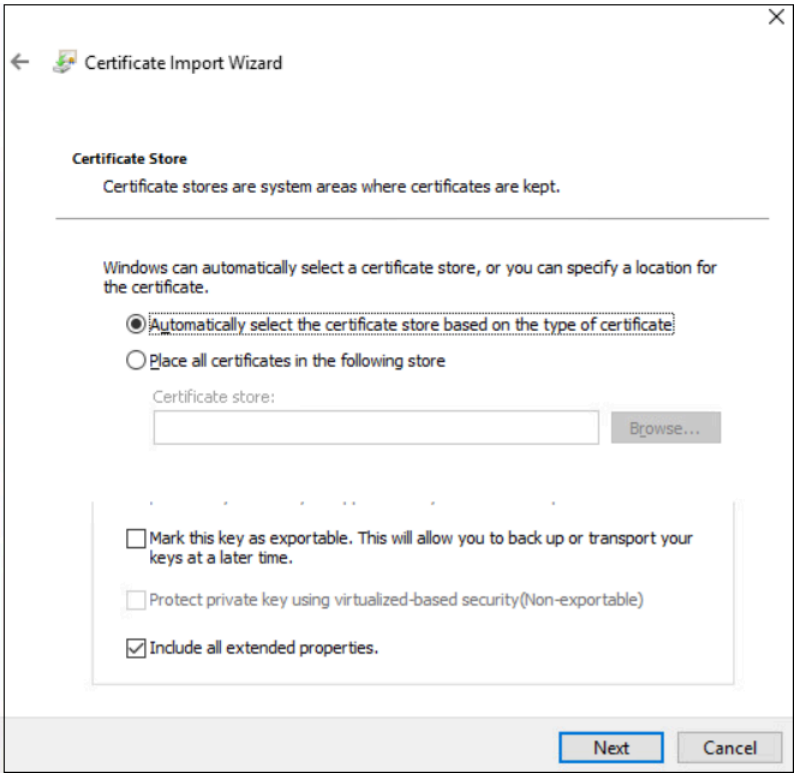


Figure 36: Certificate Store Page

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

Moving the L2 certificate

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

About this task

Procedure

1. From the `Windows Start Menu`, type ***Manage Computer***, and then select `Manage Computer Certificates`.
   The `certlm` window appears.
2. On the `User Account Control` dialog, click `Yes`.
3. Navigate to **`Personal > Certificates`** folder.
4. Expand **`Intermediate Certification > Certificates`**, and then move the NES L2 CA certificate from **`Personal > Certificates`** to the **`Intermediate Certification > Certificates`** folder.
   You can move the file by dragging and dropping it from one folder to the other folder. The following figure provides an example of the certificates window.

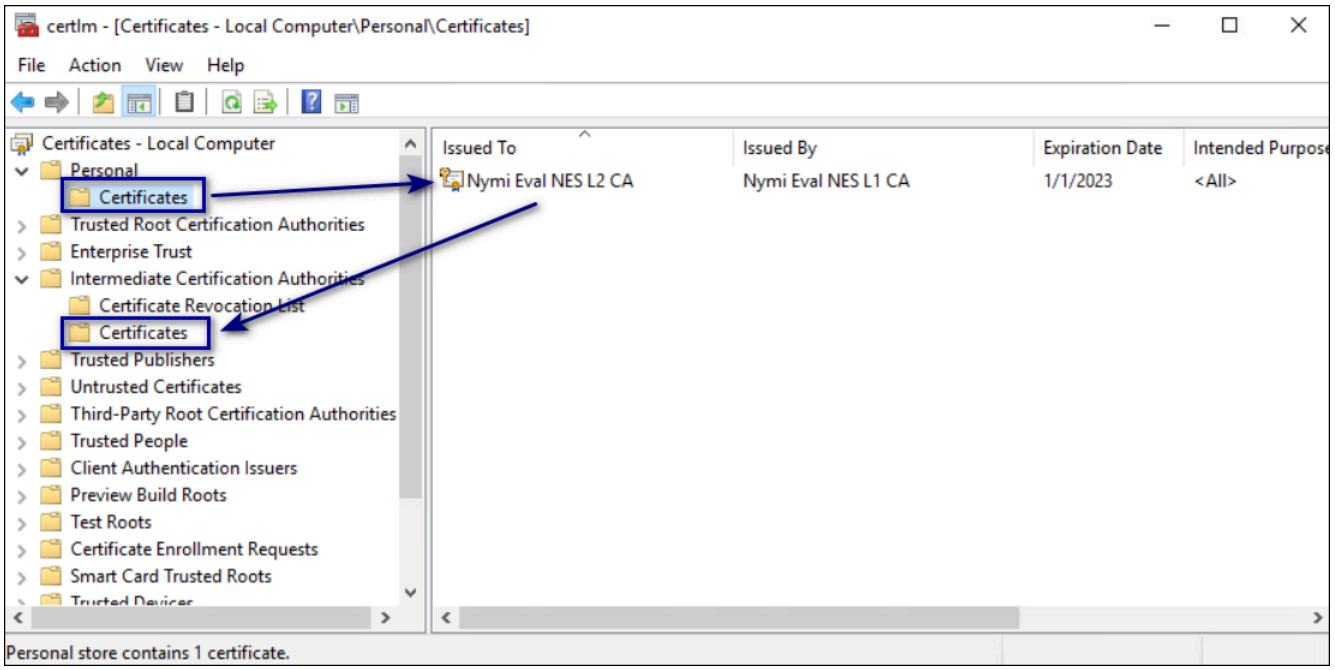


Figure 37: Certificates window

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.

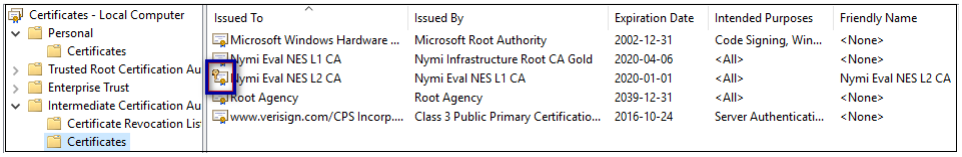


Figure 38: L2 Certificate with key

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.

7.2.1.3 - Installing NES

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

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

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`**.

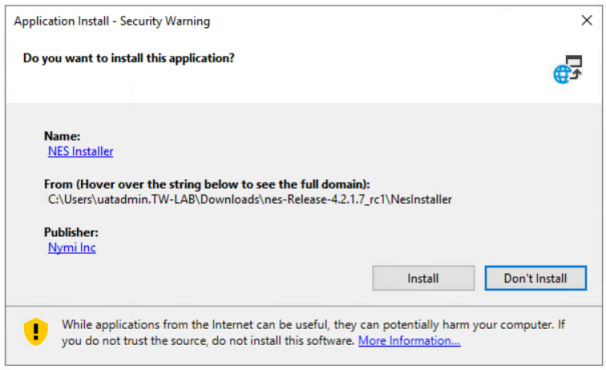


Figure 39: Security Warning

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.

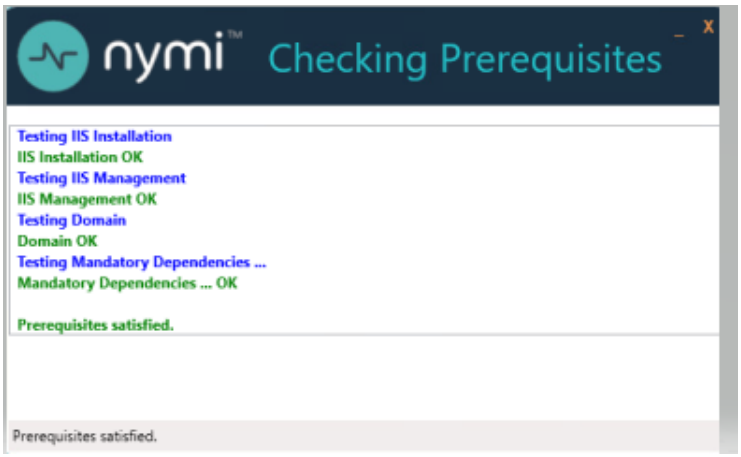


Figure 40: Prerequisites Check Dialog

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

Additional Information

- During NES installation, the process of creating the NES database on the NES server, provides users with administrative privileges to the database. It is recommended that you create a second database user with view access to the audit tables after NES deployment.

- During installation, the installer may disappear and then resume. This is normal behavior as processes are working in the background.

Configuring NES Services Manually

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

Before you begin

NES configuration requires several configuration settings values that you recorded in *Appendix—Record the CWP Variables*. If the Nymi Band users complete authentication tasks in a web-based Nymi-enabled Application(NEA) on a Windows user terminal by tapping their Nymi Band on a Bluetooth adapter, you must also provide the path to the Nymi-supplied Full Chain PFX file and the password.

About this task

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

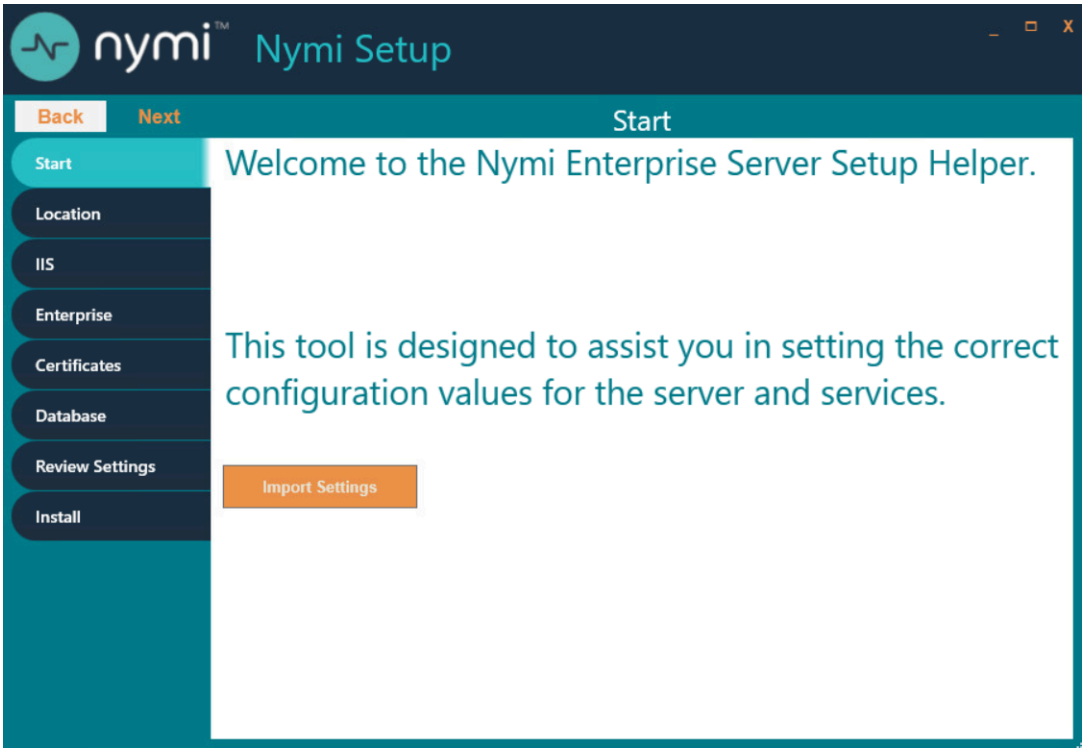


Figure 41: NES Setup Help wizard

Perform the following actions to configure the NES Services Suite.

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

Procedure

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

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

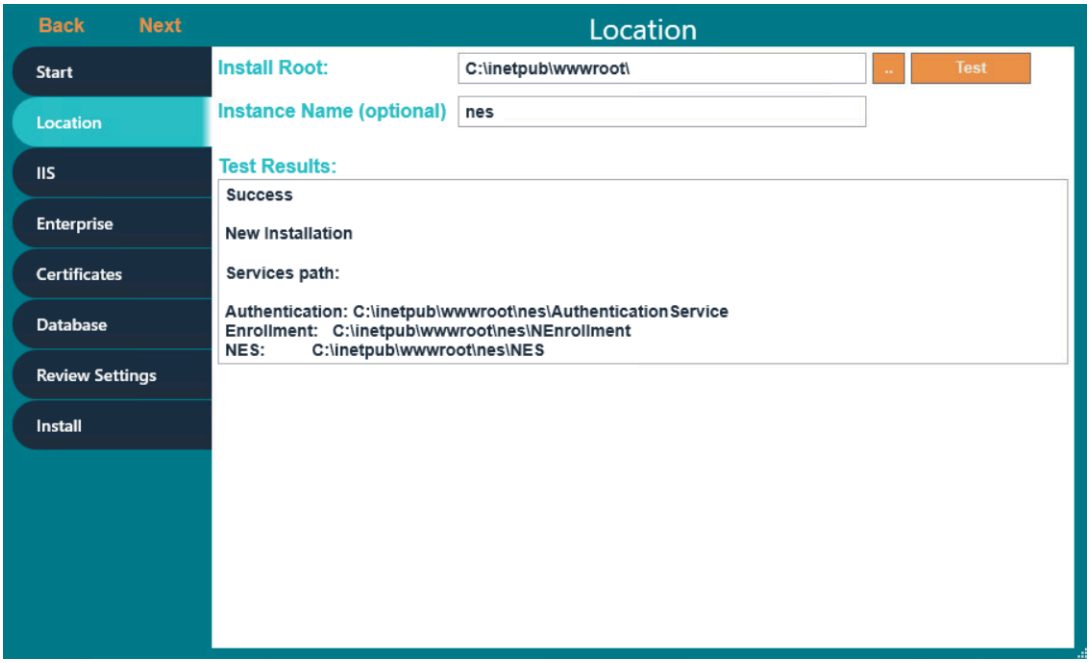


Figure 42: Location page in the NES Setup wizard

2. In the left navigation pane, click `IIS`, and then perform the following actions:
   a) From the **`IIS web site`** drop-down list, leave the default selection **`Default Web Site`**.

      Alternatively, to install the services on a different existing IIS website, select another website from the list.
   b) In the **`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.

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

Scenario	NES Admin and Enrollment Application Service Configuration	Authentication Service Configuration
Single NES instance and remote SQL server that uses Windows Authentication	1. In **Application Pool**, leave the default application pool. 2. From the **Application Pool Identity** list: a. Select **SpecificUser** from the drop-down list. b. In the **User Name** field, type the username of the Nymi Infrastructure Service Account in the format ***domain\username***. c. In the **Password** field, type the password for the Nymi Infrastructure Service Account. 3. Click the **Test** button to validate the user credentials.	1. From the **Application Pool** list, select **NES_AS App Pool**. 2. From the **Application Pool Identity** list, select **Network Service**.
Multiple NES instances in a high-availability configuration, remote SQL Server	1. In **Application Pool**, leave the default application pool. 2. From the **Application Pool Identity** list: a. Select **SpecificUser** from the drop-down list. b. In the **User Name** field, type the username of the Nymi Infrastructure Service Account in the format ***domain\username***. c. In the **Password** field, type the password for the Nymi Infrastructure Service Account.	1. From the **Application Pool** list, leave the default application pool. 2. From the **Application Pool Identity** list: a. Select **SpecificUser** from the drop-down list. b. In the **User Name** field, type the username of the Nymi Infrastructure Service Account in the format ***domain\username***. **Note:** Ensure that you specify the same user account that you provided for

Scenario	NES Admin and Enrollment Application Service Configuration	Authentication Service Configuration
	d. Click the **Test** button to validate the user credentials.	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	In the **Application Pool** and **Application Pool Identity**, leave the default selections.	In the **Application Pool** and **Application Pool Identity**, leave the default selections.

d) 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.

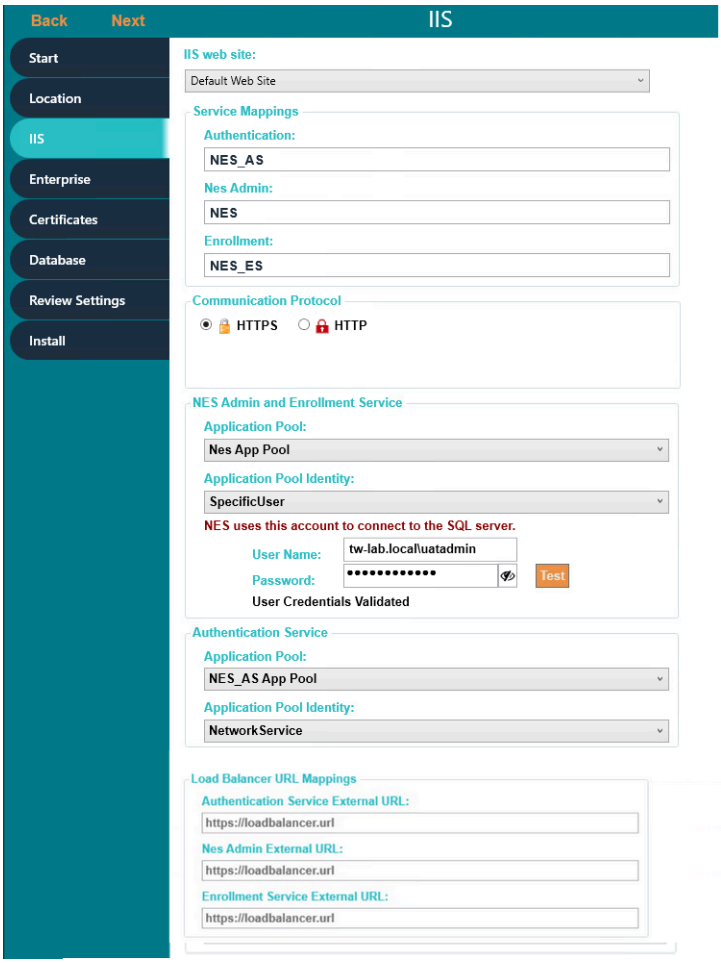


Figure 43: IIS Setup page in the NES Setup wizard

e) For a highly-available NES configuration only, in the **`Load Balancer URL Mappings`** section, perform the following actions:

1. In the **`Authentication Service External URL`** field, specify the load balancer URL for the Authentication Service, for example ***https://loadbalancer.org_name.com/NES_AS***.
2. In the **`NES Admin External URL`** field, specify the load balancer URL for the NES Administrator Service, for example ***https://loadbalancer.org_name.com/NES***.
3. In the **`Enrollment Service External URL`** field, specify the specify the load balancer URL for the NES Enrollment Service, 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:

1. 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.
2. 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.
3. Press **Enter**.
4. 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.

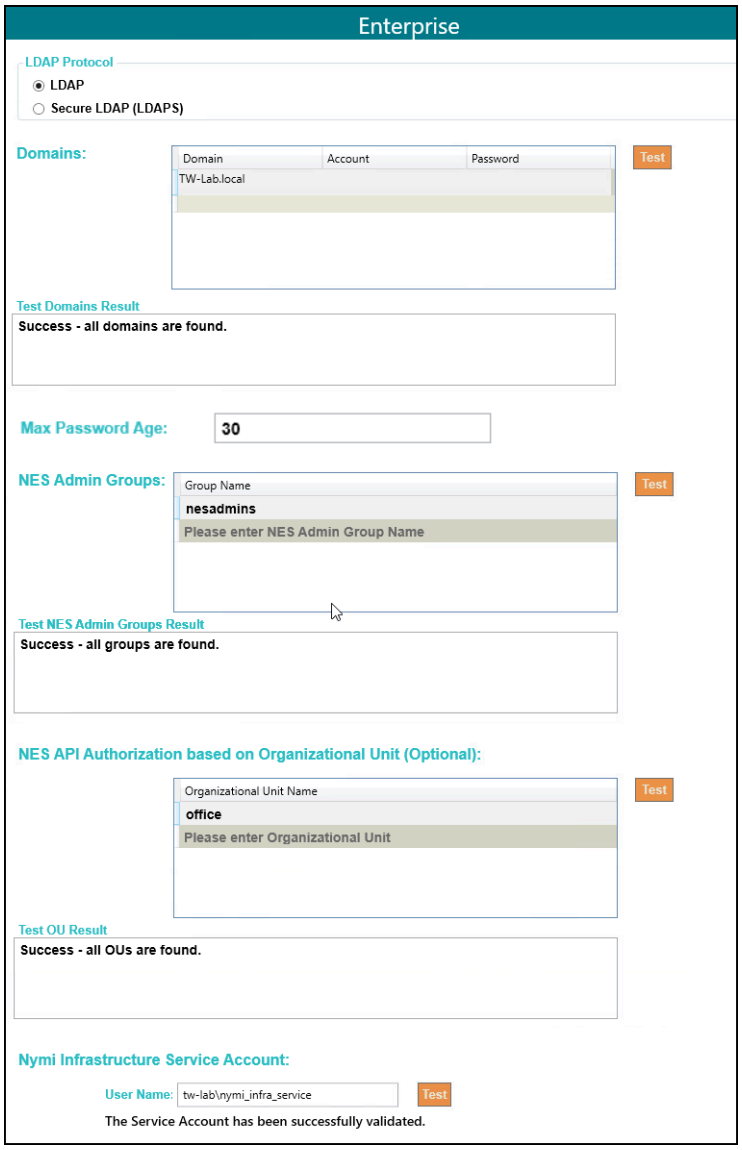


Figure 44: Enterprise page in the NES Setup wizard

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.

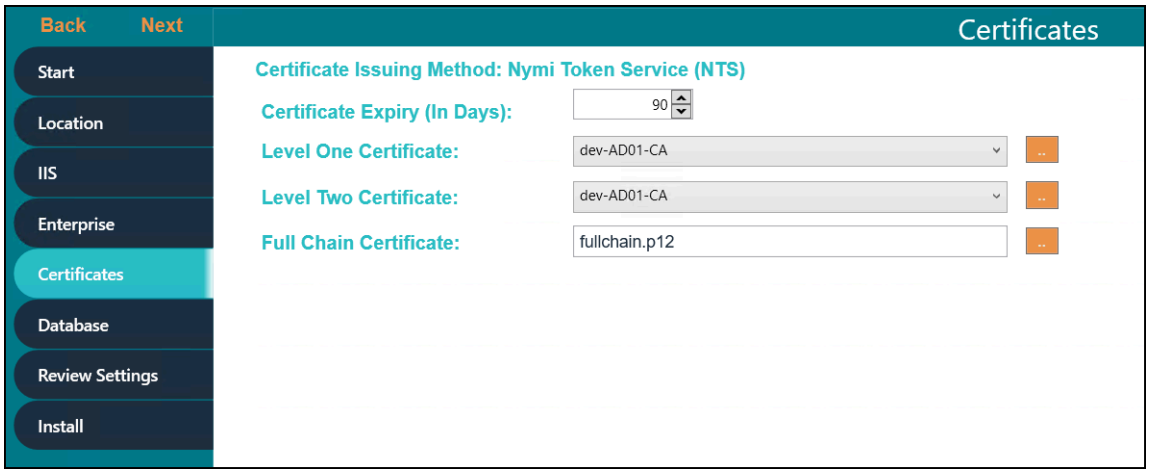


Figure 45: Certificates page in the NES Setup wizard

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.

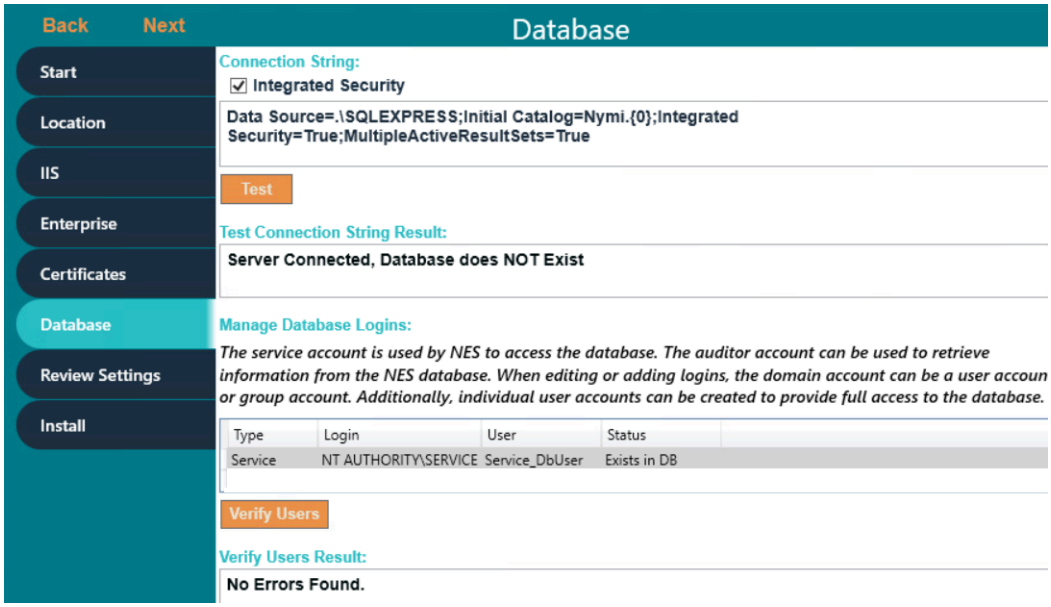


Figure 46: Database Setup page in NES Setup wizard for Windows Authentication

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.

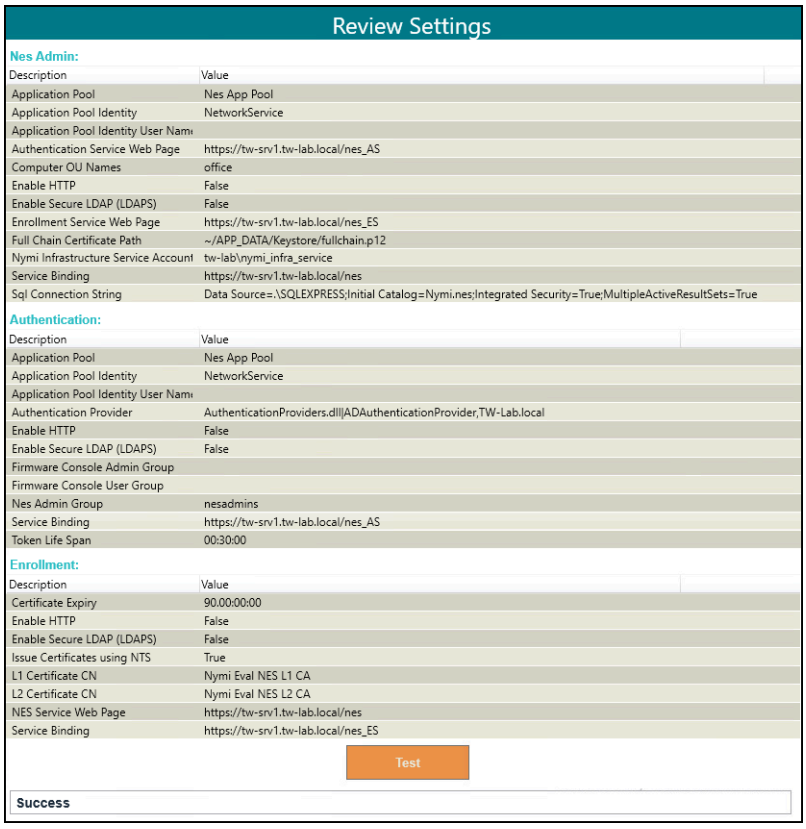


Figure 47: Review Settings window

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 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 6: Install page Options

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

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.

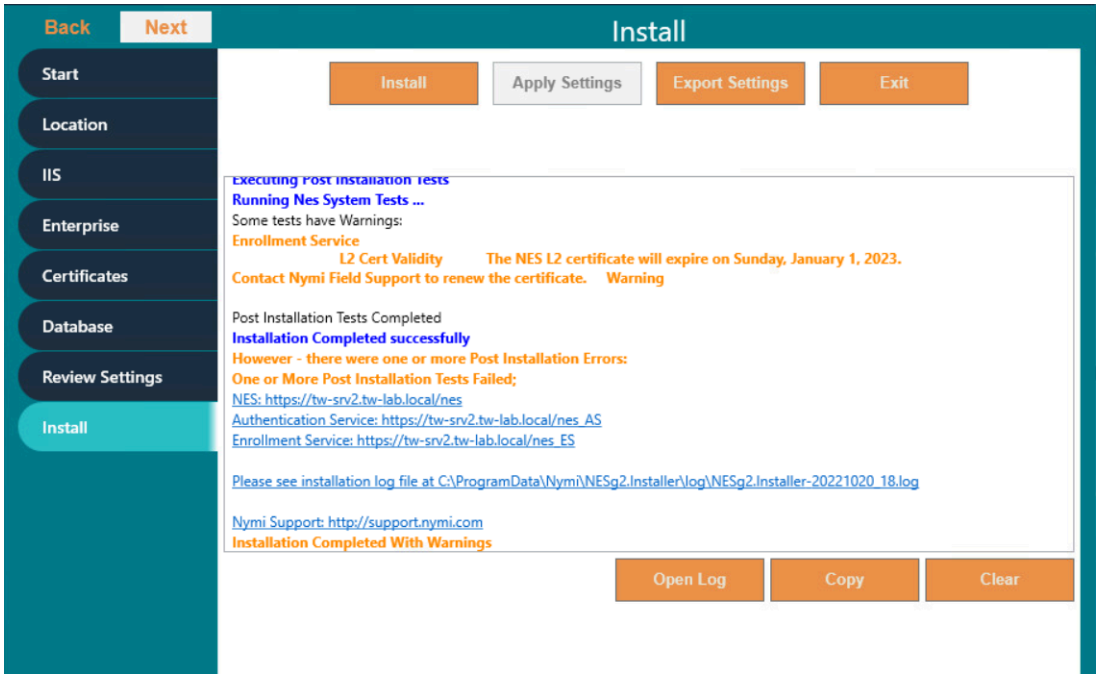


Figure 48: Install NES page in `NES Setup` wizard

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

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.

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.

Procedure

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

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

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

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

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

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

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

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

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

   c) Click **`OK`**.

Configuring NES from a Configuration File

You can configure NES based on values that are defined in a configuration file. The option to create a configuration file (*.ninst* file) is available to you when you perform an NES

configuration by using the NES Setup wizard. You can configure NES from the command line or with the NES Setup wizard.

Before Installing NES using the Silent Installer

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

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

Installing .NET and SQL Server Express

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

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

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

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

Configuring NES Silently from the Command Line

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

Before you begin

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

- Log into your machine with a domain user account that has local administrative privileges
- Copy and extract the installation package to the machine
- Install .NET. The installation package contains the .NET 4.8 software and Microsoft SQL Server Express in the following directories: .NET 4.8 software: *..\NesInstaller\DotNetFX48* . The .NET installation may require you to restart your computer.
- Install SQL Express if you do not have an existing MS SQL Server to store the NES database. The installation package contains Microsoft SQL Server Express 2019 in the following location: *..\PreRequisites\SqlExpress* During the SQL installation, accept all defaults. The installation process creates all Microsoft SQL Server users automatically. On the Database Engine Configuration screen, add additional users that require access to the audit reports in the SQL database.
- If you are using a *.ninst* file from a pre-CWP1.6 NES installation, edit the file and add the following entries before the last } that appears in the file:

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

```
```

where:

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

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

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

- 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\NesCmdInstall* directory.
2. Open a command prompt as an Administrator and change the path to *C:\nestemp\nes-Release-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.

Configuring NES With a Configure File in the NES Setup Wizard

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

About this task

Procedure

1. In the NES Setup Wizard, on the Start screen, click **Import Settings**.
2. In the Open window, navigate to the directory that contains the *ninst* configuration file, and then double-click the *.ninst* file.
   A **Loaded Successfully** message appears on the screen.
3. 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**.
4. 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.
5. If the **Review Settings** test did not report errors, on the **Install** tab, click **Install**.
6. When the installation completes, close the NES Setup wizard.

7.2.1.4 - Configuring IIS to Prevent NES Offloading

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

About this task

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

Procedure

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

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

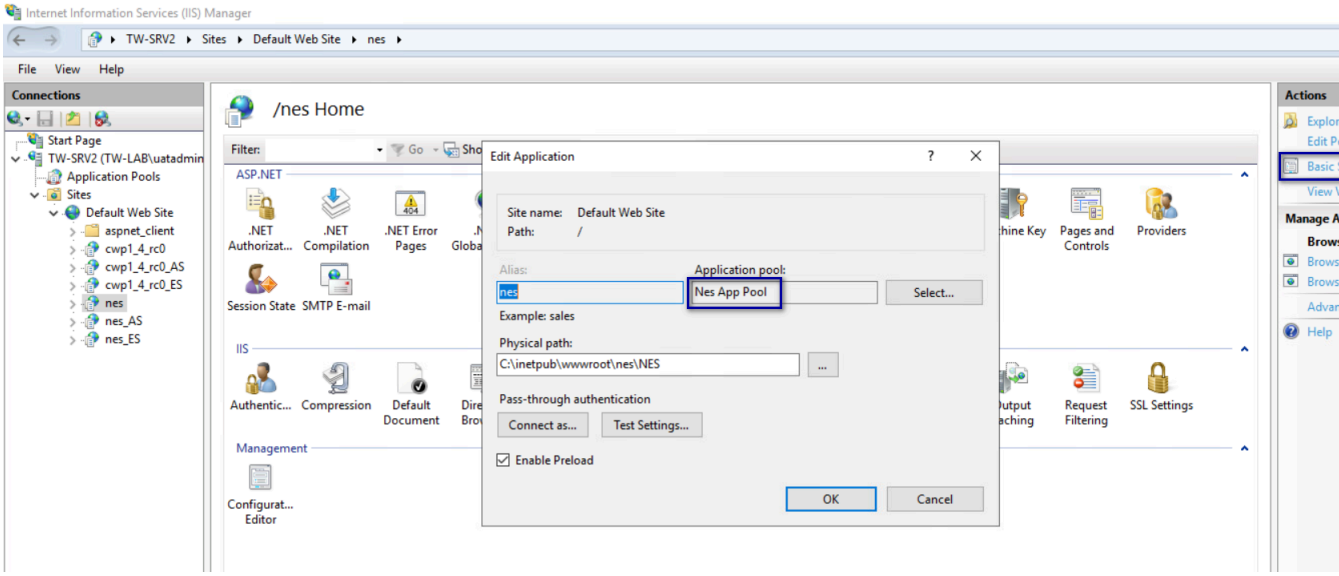


Figure 49: Edit Application window

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.

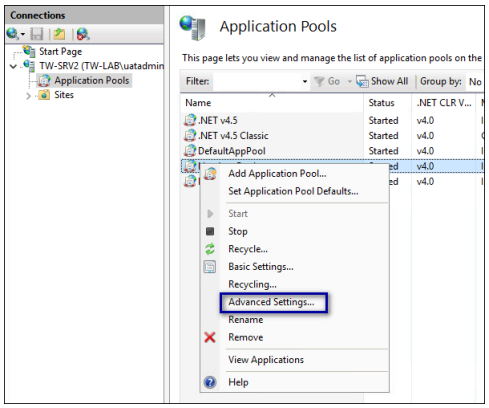


Figure 50: Advanced Settings menu option

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`.

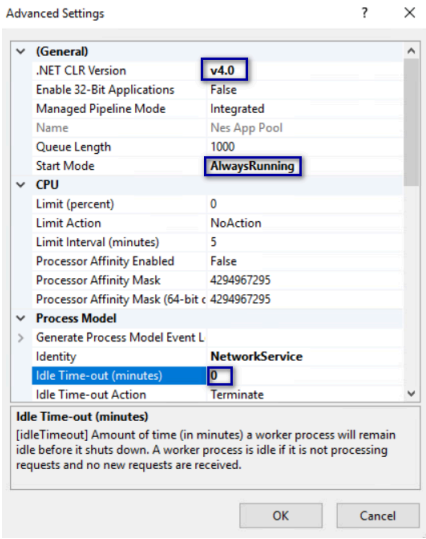


Figure 51: Advanced Settings window

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.

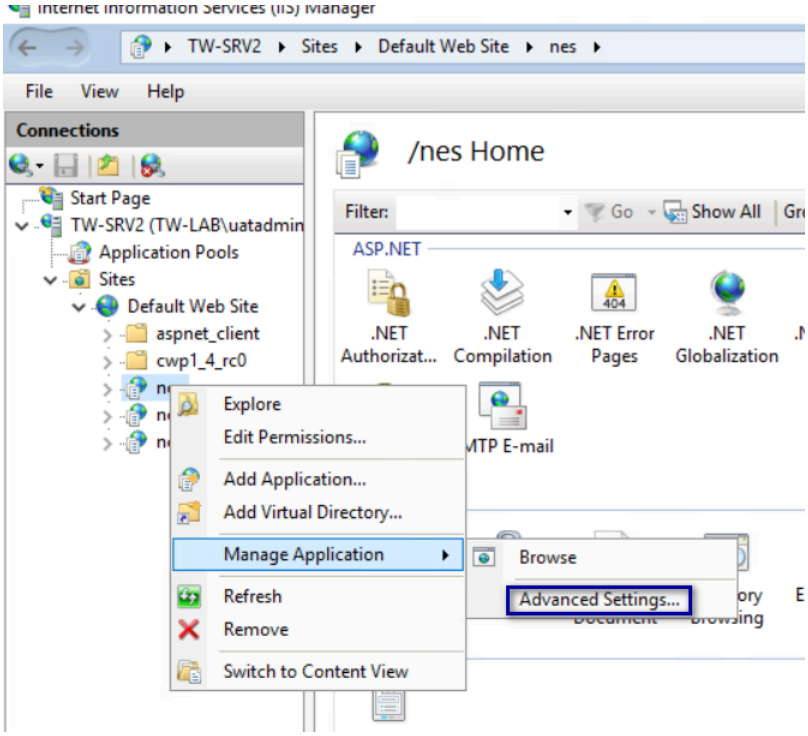


Figure 52: Advanced Settings option

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.

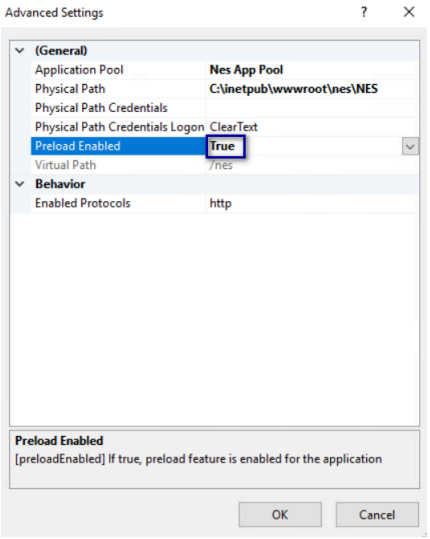


Figure 53: Advanced Settings window

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.

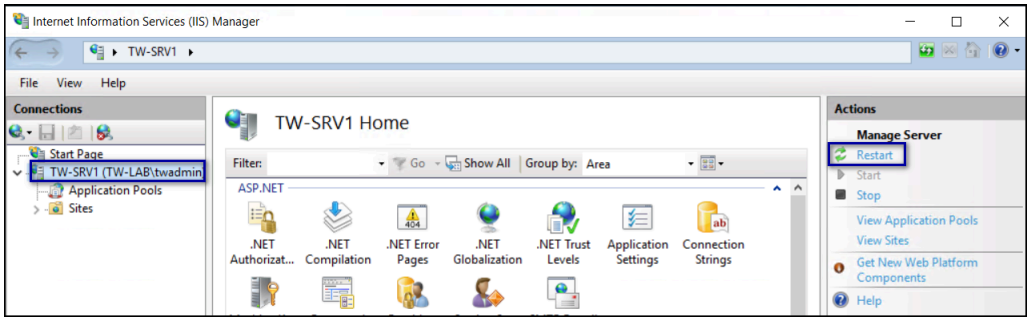


Figure 54: Restart IIS

6. Close `IIS Manager`.

7.2.1.5 - 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.

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.

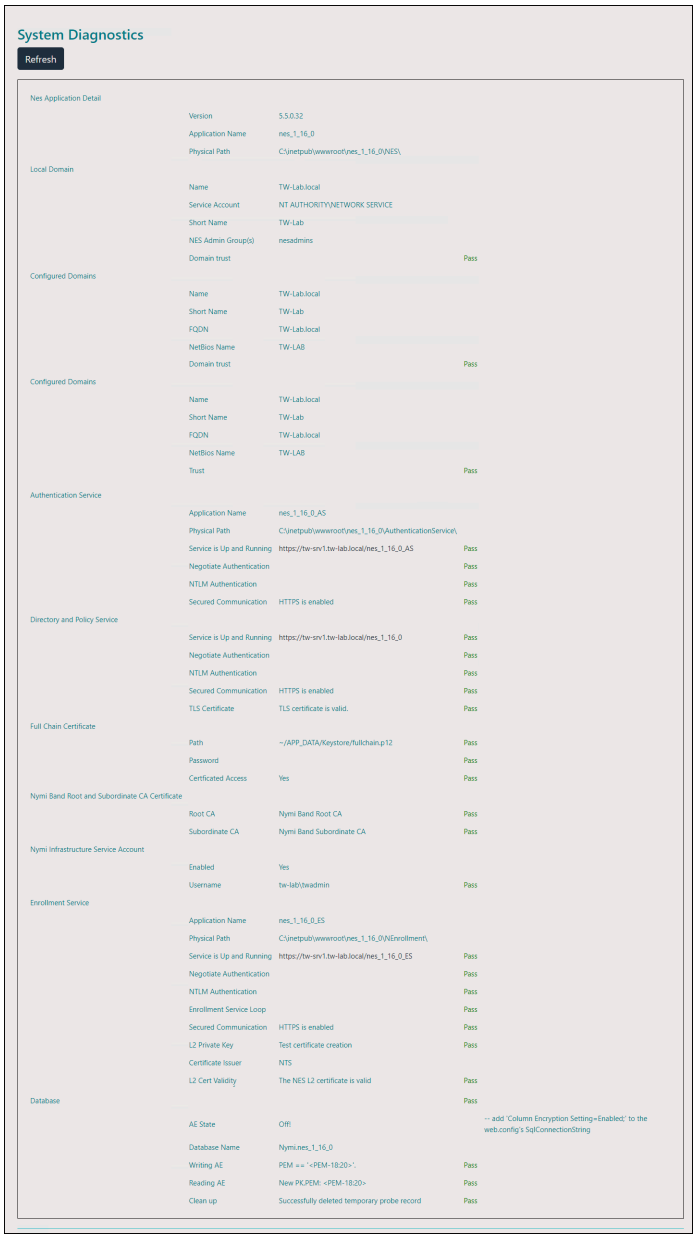


Figure 55: System Diagnostic Tests

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.

7.2.1.6 - 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 <value> </value> attribute tags, as shown in the following example:

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

   c) Save the file.
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.

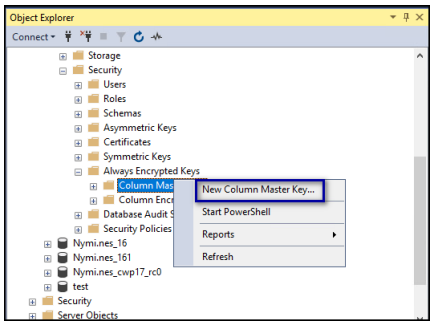


Figure 56: New Column Master Key option

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.

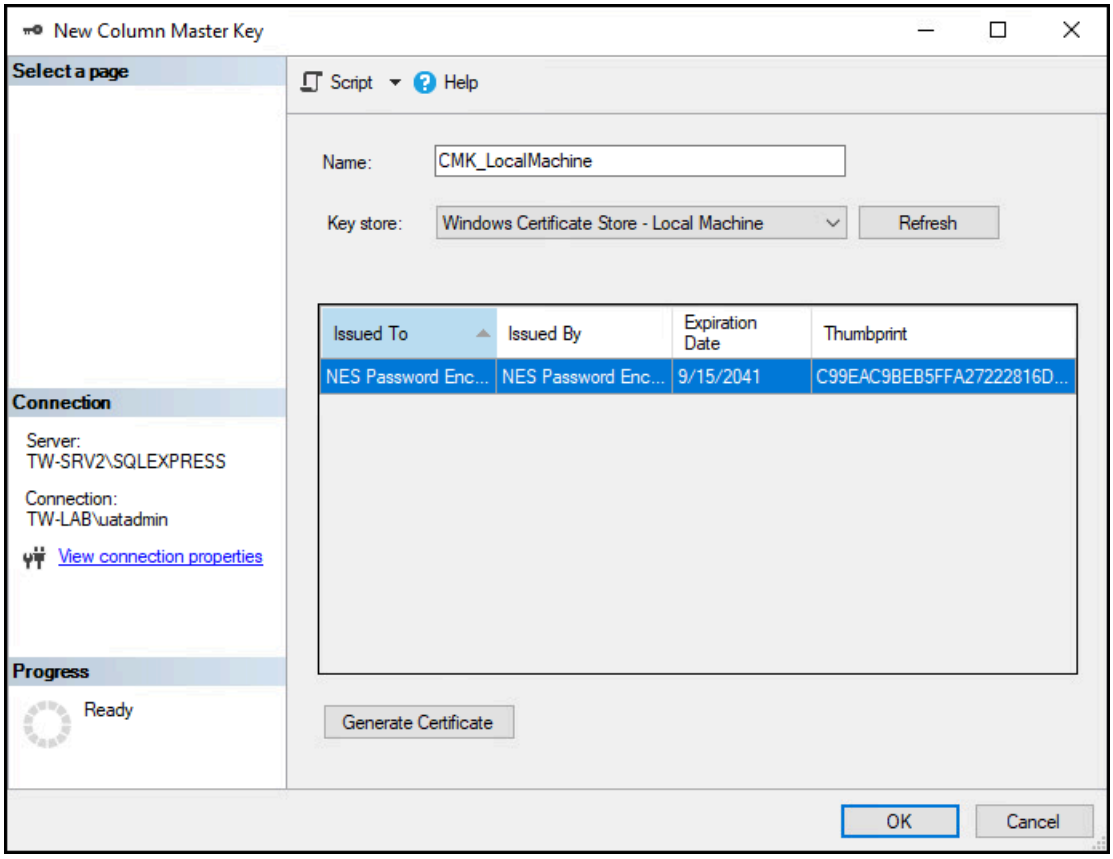


Figure 57: New Column Master Key page

   c) Click **Generate Certificate**.

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

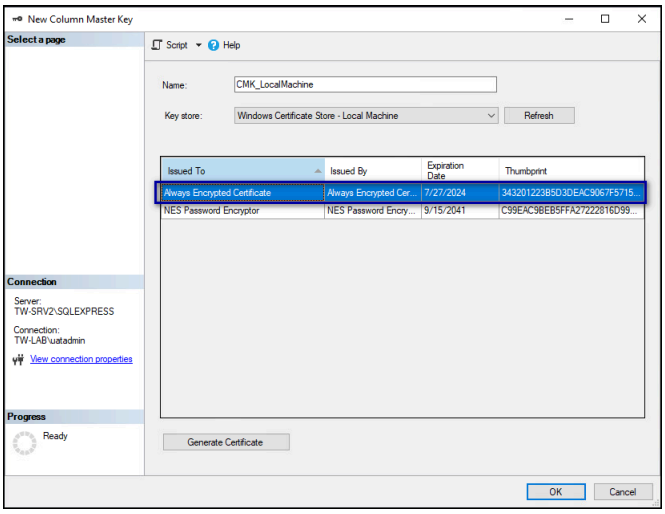


Figure 58: Always Encrypted Certificate

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.

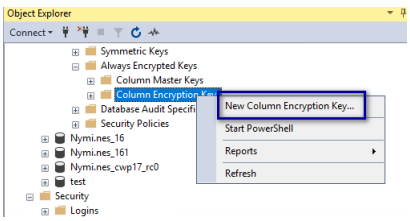


Figure 59: New Column Encryption Key option

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.

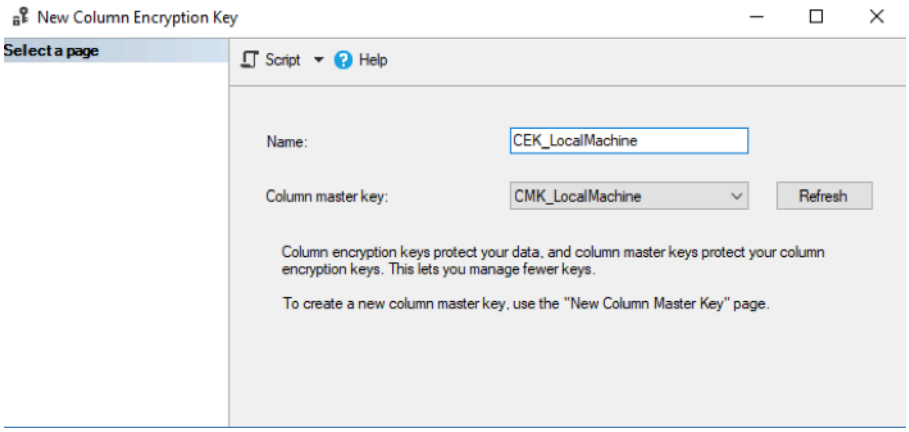


Figure 60: New Column Encryption Key page

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.

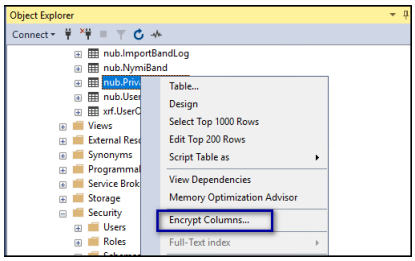


Figure 61: Encrypt Columns option

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.

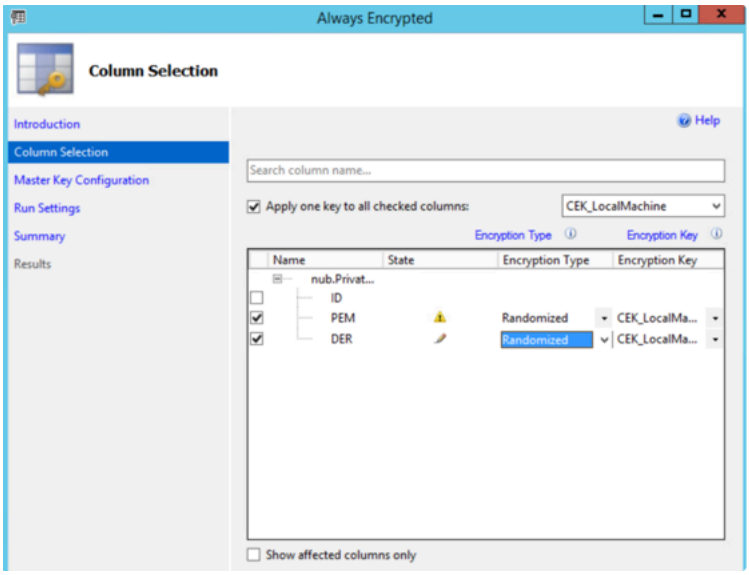


Figure 62: Column Selection page

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.

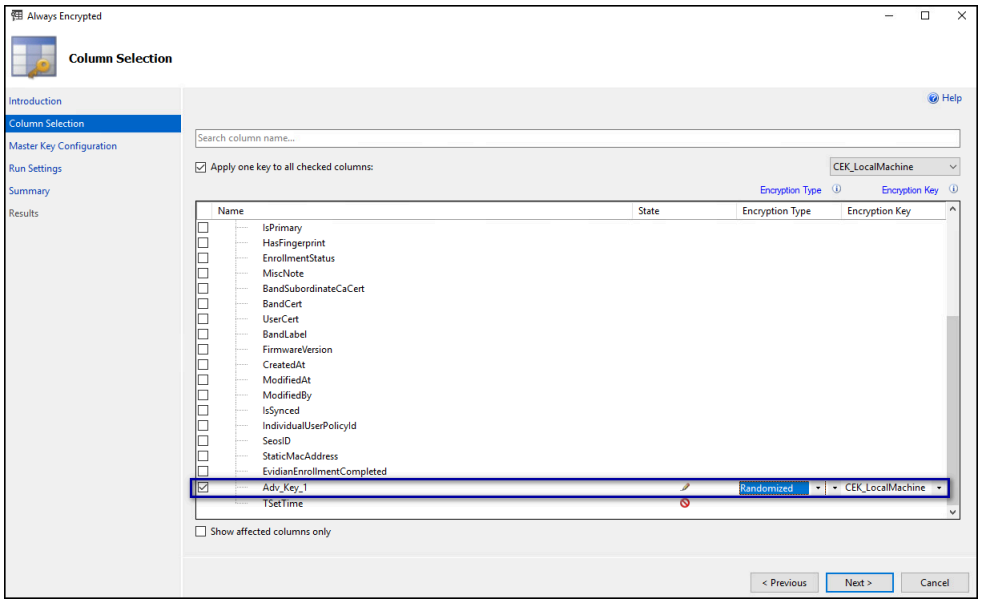


Figure 63: Encrypted Columns window

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.

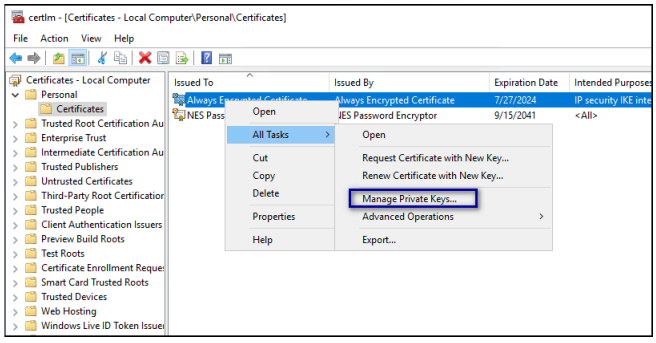


Figure 64: Manage Private Keys option

The `Permissions for Always Encrypted Certificate` window appears.

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

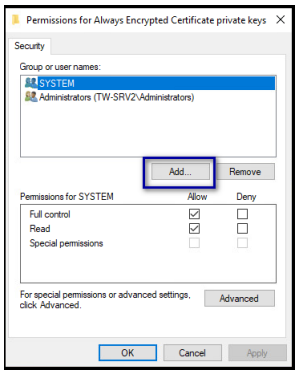
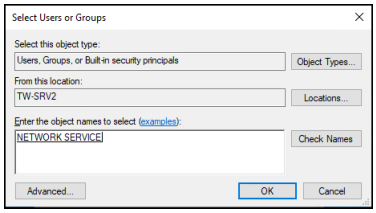


Figure 65: Add Permissions window

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`.

(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.

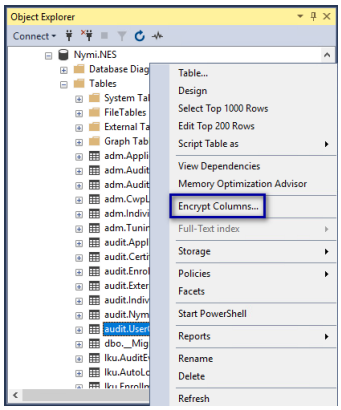


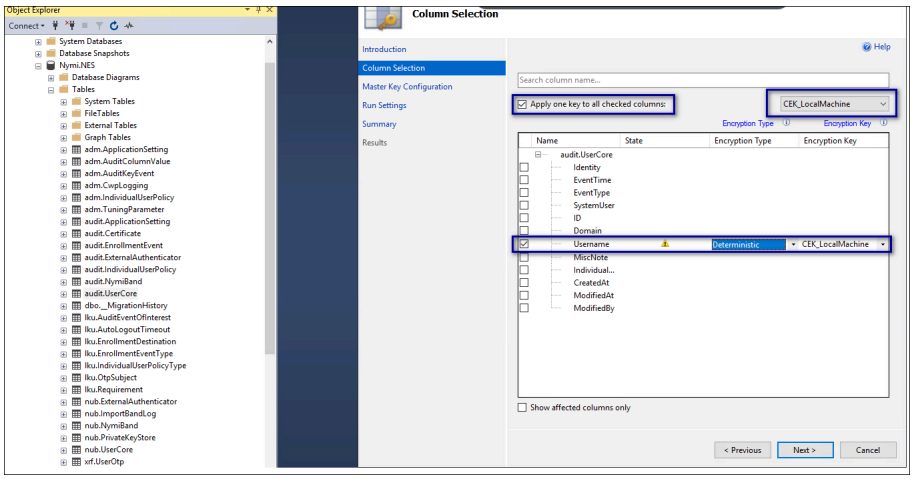
Figure 66: Encrypt Columns option

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.



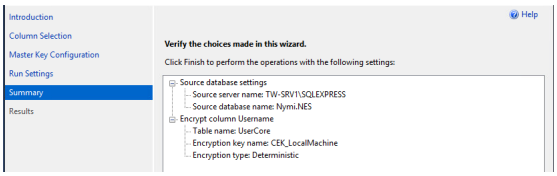
e) Click **`Next`**.

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`**.

7.2.1.7 - Configuring NES Policies

Nymi Enterprise ServerNES provides you with the ability to customize the Nymi with Evidian solution by using group and individual policies.

This section provides you with information about how to edit the NES policy to enable Evidian enrollments and optionally, allow users to create a Nymi Band label during enrollment and allow corporate credentials authentication in your configuration. The *Nymi Connected Worker Platform—Administration Guide* provides information further information about group policies, how to use individual policies, and how to enable or disable other policy options in NES.

Enabling Evidian Enrollments

Enrollment in an Evidian environment requires you to enable the option **`NES and Evidian`** in the active Nymi Enterprise Server(NES) policy.

For an IT/OT configuration, enable this option on the Enrollment NES or Registration NES to match your use case. For example, when you use Evidian in both IT and OT enable this option on the Enrollment NES and Registration NES.

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. Click **`Policies`**.
3. Edit the active policy.
4. From the **`Enrollment / Registration Destination`** list, select the option **`NES and Evidian`**, as shown in the following figure, and then click **`Save`**.

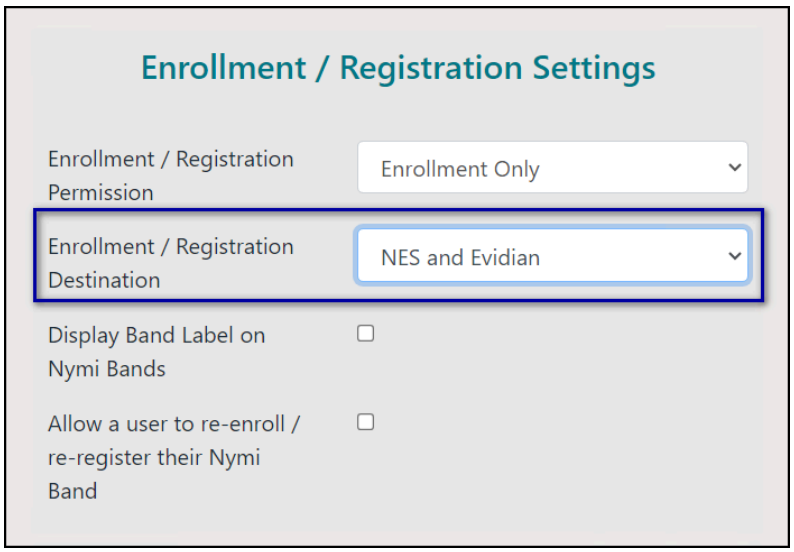


Figure 67: NES and Evidian enrollment option

Note: In CWP 1.17.0 and earlier the list name is **`Enrollment Destination`**.

Configuring a Band Label on the Nymi Band

Perform the following steps to set a label on the Nymi Band.

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 **`Enrollment Settings`** section, select **`Display Band Label on Nymi Bands`**
   The **`Allow Band Label Customization`** option appears.

   Perform one of the following actions:

   - Leave the **`Allow Band Label Customization`** cleared to display the first 12 characters of the Active Directory username for the user on the Nymi Band. The Nymi Band displays the Band Label as two rows of six characters.
   - Select **`Allow Band Label Customization`** to enable users to customize the Band Label that displays on their Nymi Band. Users must re-enroll to customize the Band Label on the **`Set Band Label`** screen during enrollment.
5. Click **`Save`**.

Results

During enrollment, the Nymi Band Application displays a band label screen to the user with the first 12 characters of their Active Directory username. When **`Allow Band Label Customization`** is enabled, the user can modify the label.

If you enable the **Display Band Label on Nymi Bands** option after enrollment has completed for users, users can apply this change to their Nymi Band by logging into the Nymi Band Application while wearing their authenticated Nymi Band. The Nymi Band Application applies changes to the Nymi Band to display the Active Directory username of the user.

If you enable the **Allow Band Label Customization** after enrollment has completed for users, the users must re-enroll their Nymi Band to set a customized band label.

Configuring Corporate Credentials Authentication

Perform the following steps to configure the Nymi Band Application to create a corporate credential authenticator for a user during enrollment, which allows a user to authenticate the Nymi Band by Active Directory username and password.

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 **Enrollment Settings** section, select the option **Corporate Credentials Authentication**.
5. Click **Save**.

Results

When a user enrolls their Nymi Band, the Nymi Band Application creates a corporate credential authenticator on the Nymi Band. For subsequent authentications of the Nymi Band, if the user cannot authenticate by fingerprint, the user can log into the Nymi Band Application while wearing their Nymi Band, and the Nymi Band Application can authenticate the user to their Nymi Band, based on the AD credentials that were used to log into the that enables users to the Nymi Band Application.

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.

The Nymi Band Application creates a corporate credential authenticator on the Nymi Band.

Disabling Corporate Credentials Authentication

Perform the following steps to disable corporate credentials authentication in an NES policy.

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 **`Enrollment Settings`** section, clear the option **`Corporate Credentials Authentication`**.
5. Click **`Save`**.

Results

When a user enrolls their Nymi Band, the Nymi Band Application does not create a corporate credentials authenticator on the Nymi Band and the user can only authenticate with their fingerprint.

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.

The Nymi Band Application removes the corporate credential authenticator from the Nymi Band.

7.2.2 - Installing and Configuring the Evidian EAM Controller software

Install the Evidian EAM Controller software on a server.

Before you begin

Obtain a valid EAM license file.

About this task

For production deployments, Nymi recommends that you install the software on a dedicated server. For simplicity, this document assumes that the NES and Evidian EAM Controller software are installed on the same machine.

Note: The installation of the Evidian EAM Controller software requires that you restart the server.

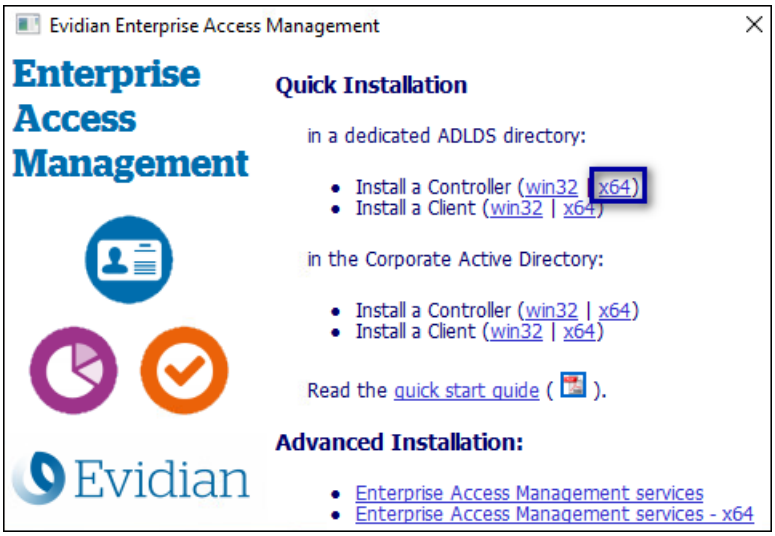
Procedure

1. Log in to the server as a local administrator.
2. Download and extract the Evidian software package, *EAM-v10.0x.xxxxxxx.zip* to a directory on the server, (for example, the *Downloads* directory).
3. Double-click the *C:\Downloads\EAM-v10.0x.xxxxxxx\Start.hta* file, and on the **`Open File – Security Warning window`**, click **`Run`**.

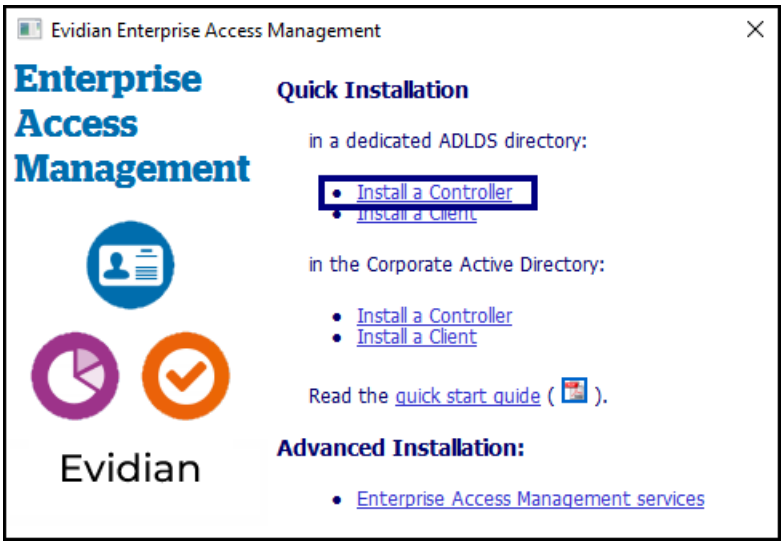
   Note: Note: If you run the *hta* file using Microsoft Explorer, which has enhanced security settings, you may experience issues. Create an exception, or alternatively, run the *.exe* file

(for example, *ESSOControllerSetup-Dedicated.exe*) directly from *EAM-v10.0x.XXXX \QuickInstall.x64\Controller* folder and then proceed to step 7.

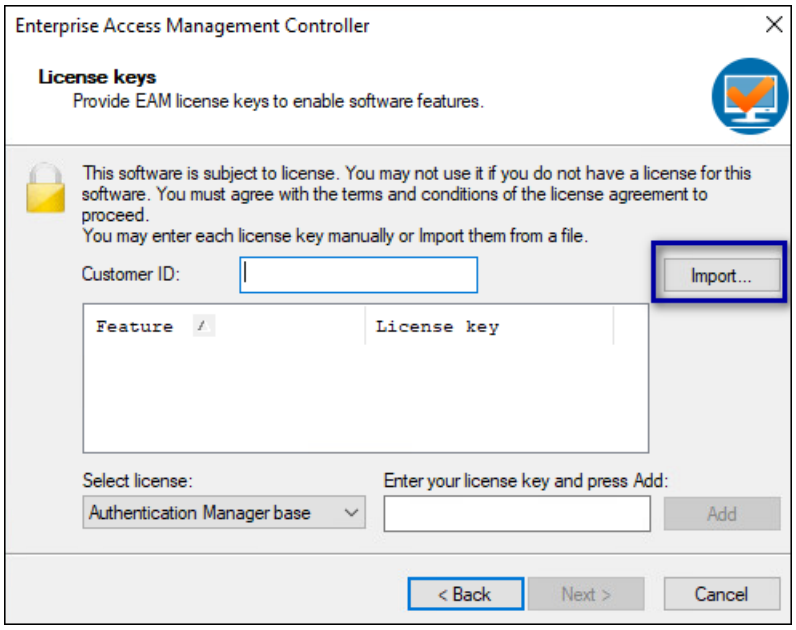
4. On the `Quick Installation` window, perform one of the following actions:
   - For Evidian EAM 10.03, in the **`in a dedicated ADLDS directory`** section, click **`x64`** beside **`Install a Controller`**, as shown in the following figure.



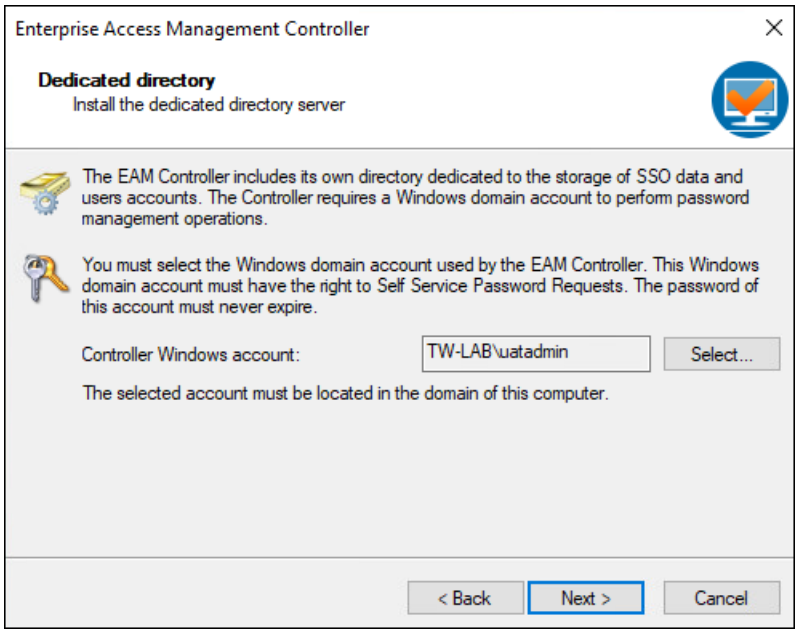
   - For Evidian EAM 10.04, in the **`in a dedicated ADLDS directory`** section, click **`Install a Controller`**, as shown in the following figure.



5. On the `User Account Control` window, click **`Yes`**.
6. On the `Welcome to the EAM Controller installation assistant` window, click **`Next`**.
7. On the `License keys` window, click **`Import`**, as shown in the following figure.



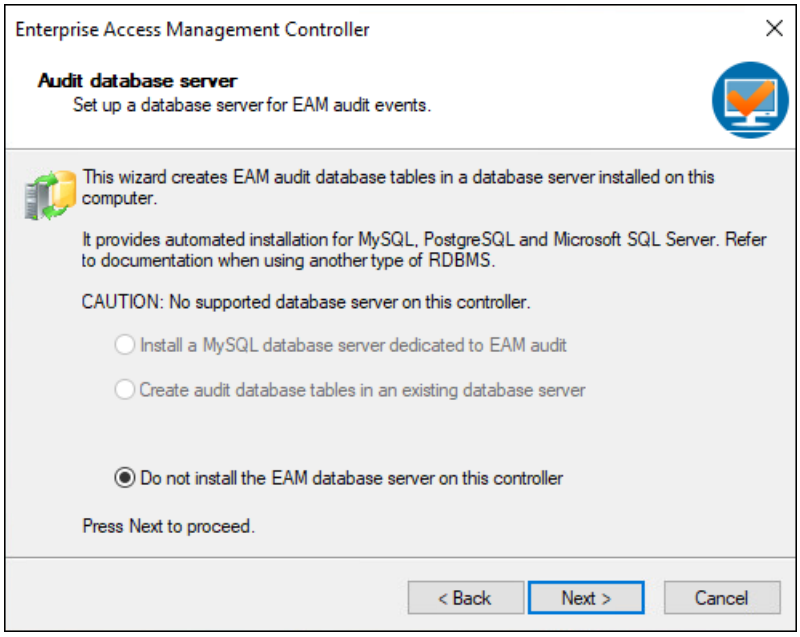
8. In the `Open` window, select the license file in the *Downloads* directory, and the click **`Open`**.
   If you do not see the file, select **`All Files *.*`** from the file type list.
9. On the `EAM Controller configuration` window, click **`OK`**.
10. On the `License keys` window, click **`Next`**.
11. On the `Storage for security objects` window, click **`Next`**.
12. On the `Dedicated Directory` window, click **`Select`**.
13. In the `Dedicated directory` window, type the username and password for a domain account that will act as the dedicated EAM administrator.
    Specify an account that matches the following requirements:
    - Local administrator access to the server
    - Password never expires
14. Click **`OK`**.
    The domain account displays in the **`Controller Windows account`** field, as shown in the following figure.



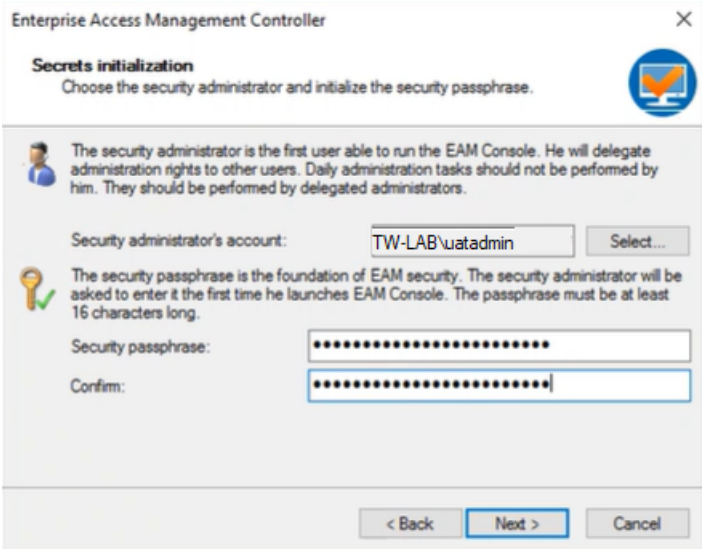
15. On the `Dedicated Directory` window, click **`Next`**.

A configuration progress window and a command prompt window appear. Do not close the command prompt window. When the configuration completes, the progress window closes.

16. On the `Audit database server` window, select **`Do not install the EAM database server on this EAM Controller`**, and then click **`Next`**.

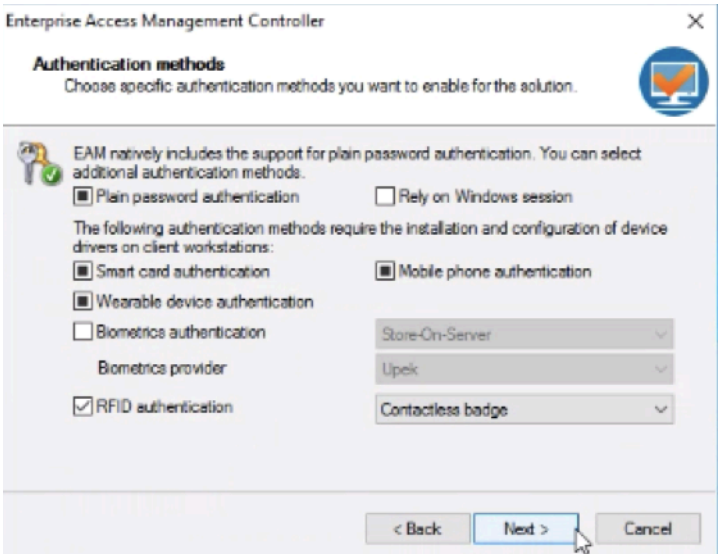


17. On the `Secrets Initialization` window, in the **`Security Passphrase`** and **`Confirm`** fields, type a security passphrase, as shown in the following figure.



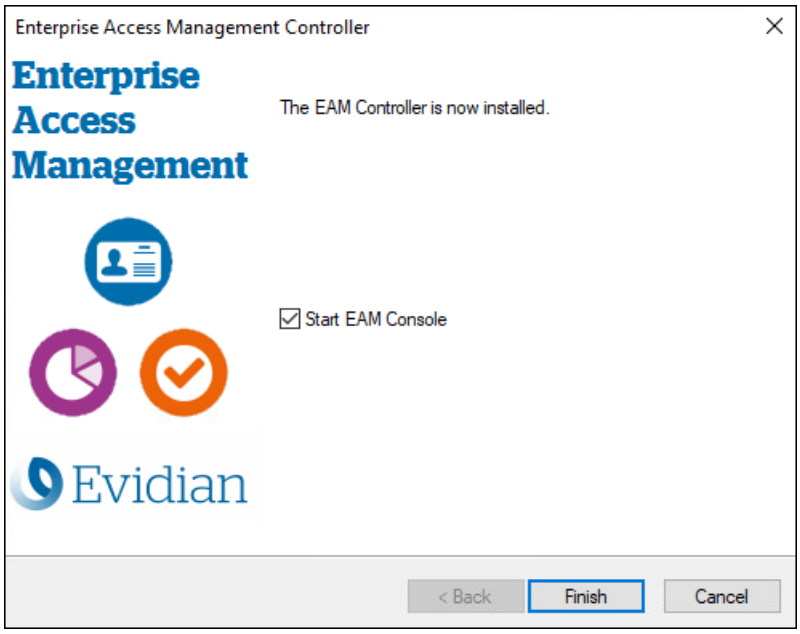
Note: IMPORTANT: Ensure that you make a note of the passphrase. The first time each EAM administrator connects to the Evidian EAM Management Console for the first time, the user is prompted to type the passphrase.

18. Click **`Next`**.
19. On the `Authentication methods` window, select **`RFID authentication`**, and leave the default selection **`Contactless badge`** from the drop-down list, as shown in the following figure. Click **`Next`**.

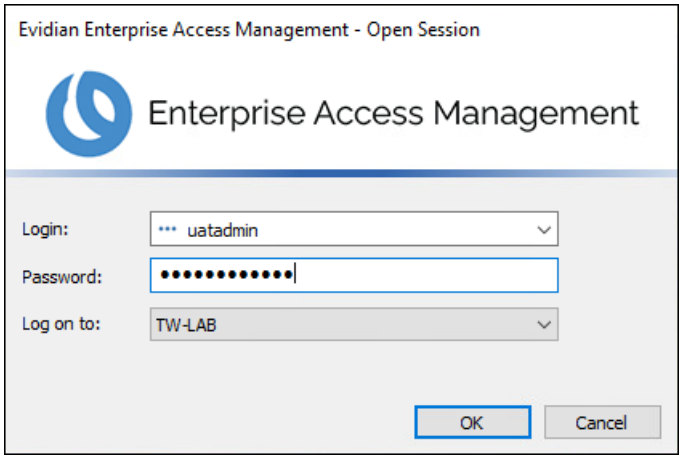


20. On the `Software installation` window, click **`Next`**.

    The Windows Installer window appears, and the installation process begins.
21. On the window that displays **`The EAM Controller is now installed`**, select **`Start EAM Console`**, as shown in the following figure, and then click **`Finish`**.

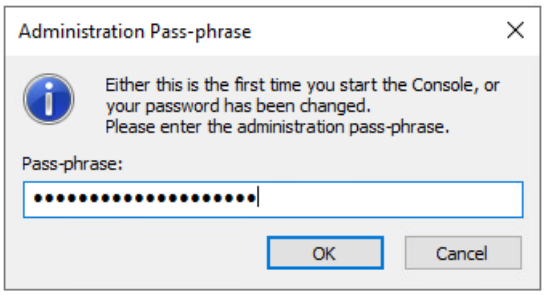


22. On the `Evidian Enterprise Access Management – Open Session` window, type your login and password and then select the domain to which you want to log on, as shown in the following figure. Click **OK**.



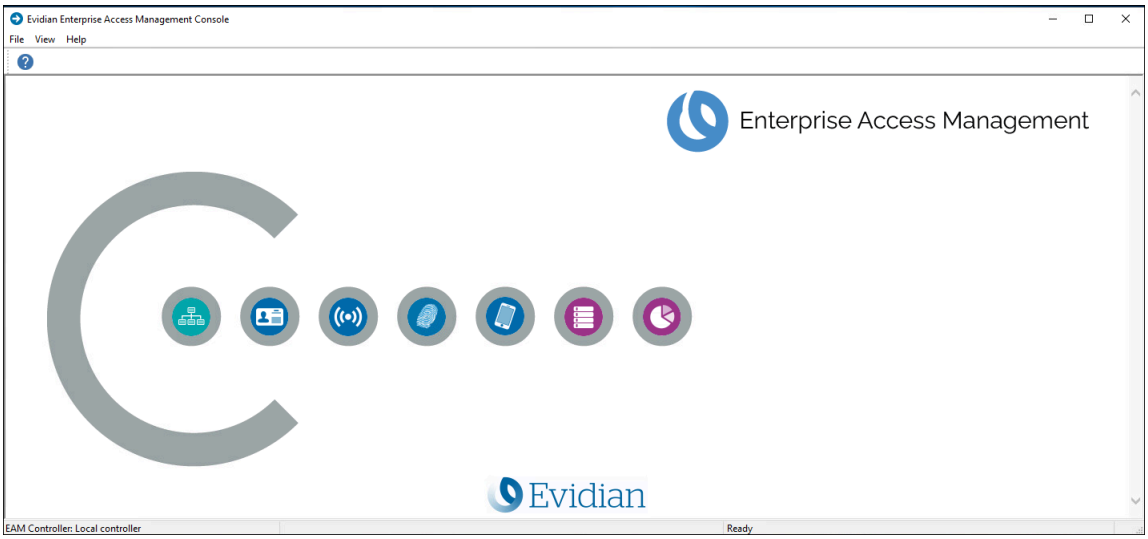
23. On the `Administration Pass-phrase` window, type the 16-character passphrase that you created in the `Secrets Initialization` window, and then click **OK**.

The following figure provides an example of the `Administration Pass-phrase` window.



Results

The Evidian EAM Management Console launches, as shown in the following figure.



7.2.2.1 - Defining the Authentication Method and Enabling Manage Access Points

The *Evidian-Supplementary-Files* directory of the Nymi installation package contains two *TokenManagerStructure*(TMS) files. TMS files define the supported authentication types and authentication modules. The Evidian EAM Controller loads the contents of the TokenManagerStructure file and pushes the configuration to the Evidian EAM Clients.

About this task

The *TokenManagerStructure* file for the Nymi Band as a Wearable device differs from the *TokenManagerStructure* for the Nymi Band as an RFID-only device.

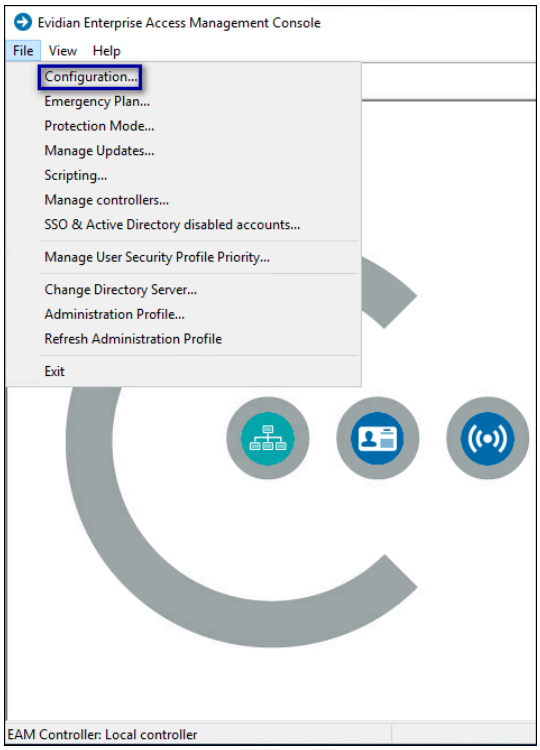
In a mixed mode environment, you must decide which mode is default, wearable or RFID-only.

For user terminals that use the non-default authentication method, you must place a different version of the TokenManagerStructure file locally on the user terminal as described later in this guide.

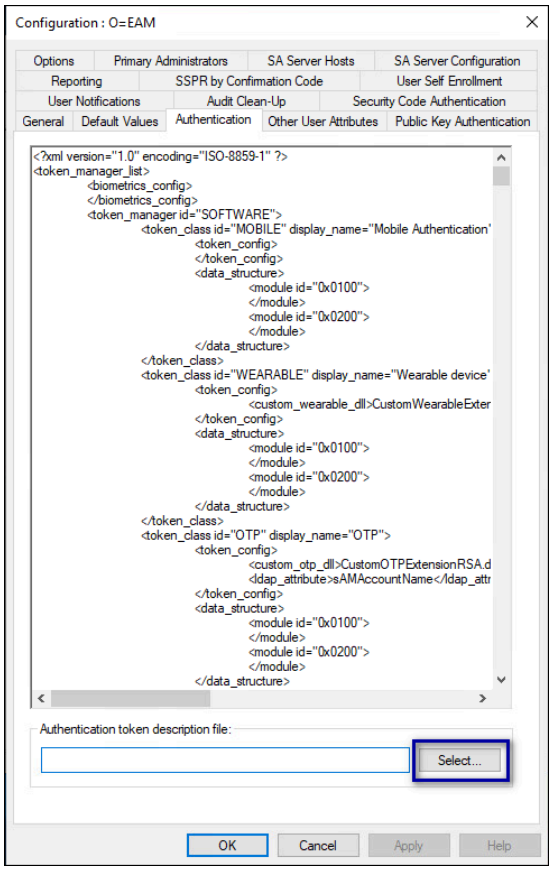
Perform the following steps to define the default authentication method in the Evidian EAM Management Console.

Procedure

1. From the **`File`** menu, select **`Configuration`**, as shown in the following figure.



2. On the **`Authentication`** Tab, click the **`Select`** button, as shown in the following figure.



3. In the `Open File` dialog, navigate to the directory that contains the TokenManagerStructure files, select the appropriate TokenManagerStructure file, and then click **`Open`**.
   - To use Wearable as the default mode, select the *TokenManagerStructure-Nymi-Wearable.xml* file.
   - To use RFID-only as the default mode, select the *TokenManagerStructure-Nymi-RFID.xml* file.
4. Click **`Apply`**, which validates the structure of the file.
5. Click **`OK`**.
6. Close the `EAM Console` window.
7. Run *regedit* and navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard \FrameWork\Config*.
8. Edit the **`ManageAccessPoints`** key and change the value to ***`1`***, as shown in the following figure.

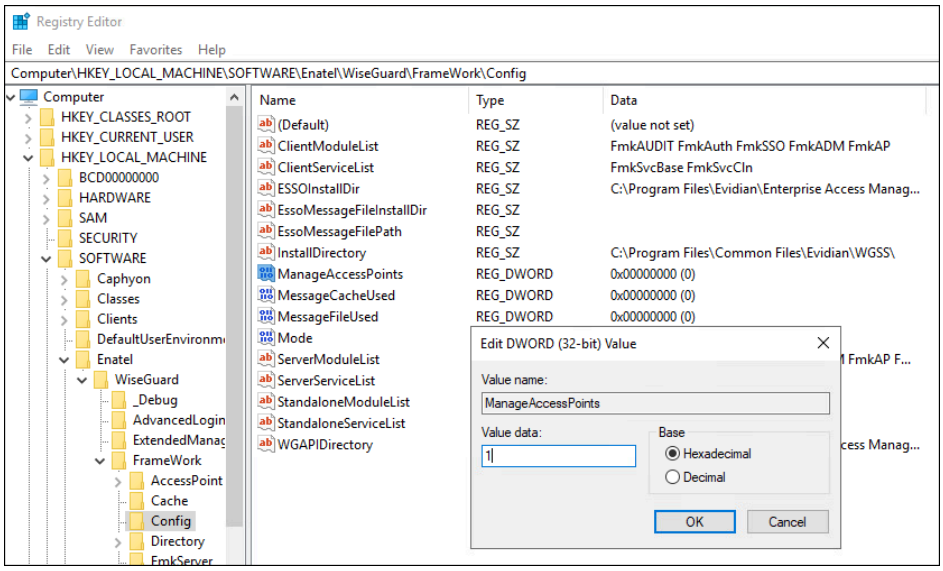


Figure 68: Manage Access Points Registry Setting

9. Click **OK**.
10. Restart the **Enterprise Access Management Security Services** service.

7.2.2.2 - Modifying EAM Settings to Support Coexistence with other Solutions

If Evidian Authentication Manager is enabled, when an Evidian-integrated application is not waiting for an SSO operation and a user performs an NFC tap, the desktop locks.

About this task

If user terminals need to simultaneously support Evidian-integrated applications and Nymi-integrated MES applications, perform the following steps in the Evidian EAM Management Console to modify the settings in the access point profile, to prevent unexpected desktop locks when performing a Nymi Band tap in the Nymi-integrated MES application.

Procedure

1. In the Directory view, expand **EAM > Evidian Enterprise Access Management > User Access > AccessPoint Profiles > Default Access Point Profile**.
2. On the **Authentication Manager** tab, from the **Default action when token removed** list, select **Do nothing**.
3. Click **Apply**.

Results

A user cannot perform an tap to lock the Windows session; however, the Windows session still locks when the Nymi Band deauthenticates or when the user is away from the user terminal.

7.2.2.3 - Configure Access Point Profile

In Evidian, access point security profiles are security objects that define a set of rights and properties that you can apply to one or more user terminals.

If your environment will use a mix of Wearable mode and RFID-only mode (Mixed mode), Nymi recommends that you create two access point profiles, one for user terminals and the enrollment terminal that support Wearable mode and another access point profile for user terminals that support RFID-only mode.

If your environment only uses one mode, you can modify the configuration of the Default Access Point Profile.

Nymi recommends that you modify the access point profile to change the following behaviour:

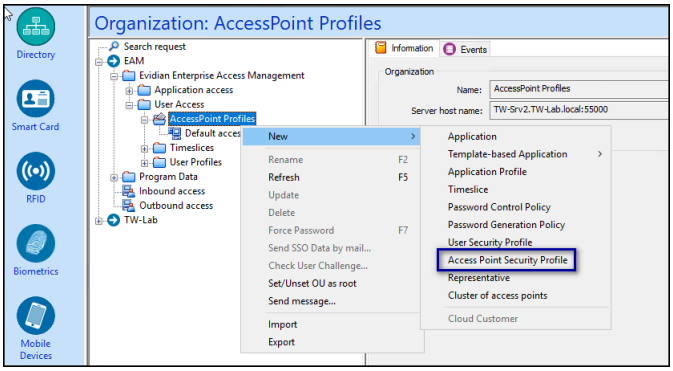
- To reduce the amount of time that it takes to complete an authentication task with the Nymi Band, you can configure the user terminals to cache login information.
- To prevent the Evidian software from loading unnecessary authentication methods, select only the authentication methods that the Nymi with Evidian Solution requires.
- To use the inclusion group.

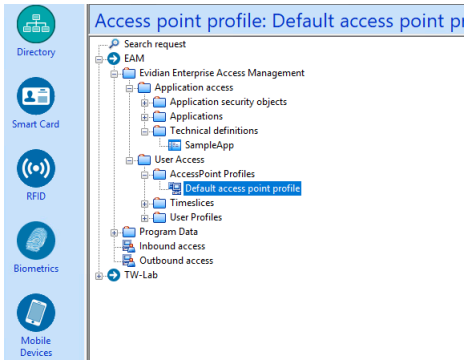
Configuring an Access Point Profile for Wearable Mode

Perform the following steps to configure an access point profile that supports wearable mode only.

Procedure

1. From the Evidian EAM Management Console, expand **`EAM > Evidian Enterprise Access Management > User Access`**.
2. Perform one of the following actions:

Option	Description
Mixed Mode environment	**a.** Right-click **`AccessPoint Profiles`**, and then select **`New > Access Point Security Profile`**, as shown in the following figure.  **b.** In the **`Name`** field, type ***Wearable-only***.

Option	Description
Wearable mode only environment	For environments where you will use wearable mode only, select **`Default access point profile`**, as shown in the following figure. 

3. In the **`Authorized authentication methods`** section, ensure that only the following methods are selected:

   - Password
   - RFID Pcsc
   - Wearable

   The following figure provides an example of the **`Configuration`** tab.

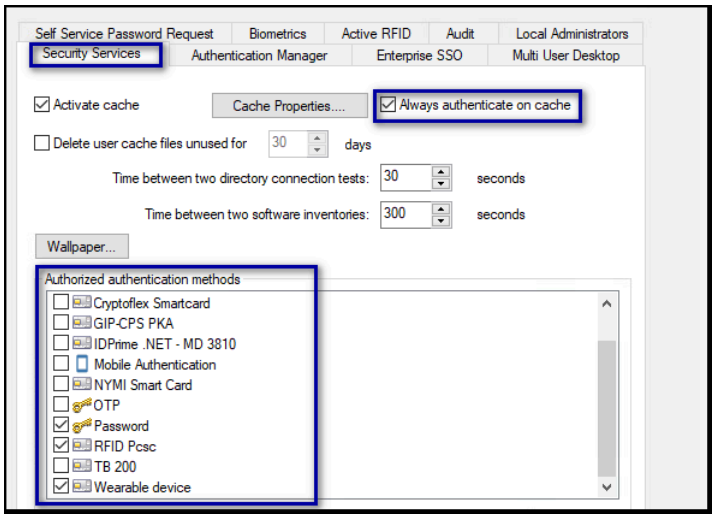


Figure 69: Access Point Profile Configuration tab

4. Click **`Apply`**.
5. On the **`Configuration`** tab, select the **`Authentication Manager`** tab, and then click **`Manage Accounts`**.
6. In the `Manage Accounts` window, click **Add**, as shown in the following figure.

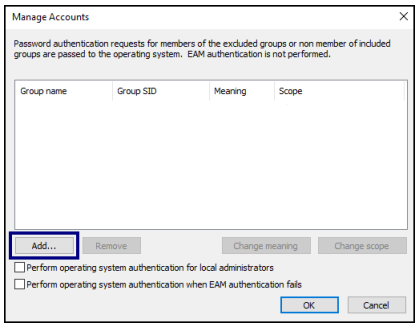


Figure 70: Add option

7. In the `Select Group` window, expand you domain, select **`Users`**, select the AD inclusion group, and then click **`OK`**.

   The following figure provides an example of the `Select Group` window with the inclusion group highlighted.

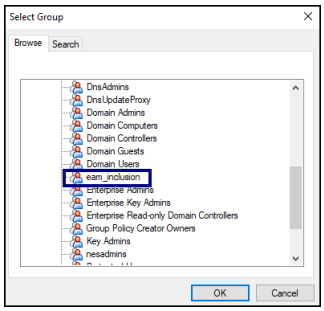


Figure 71: Inclusion Group

8. In the **`Group`** table, select the AD inclusion group that you created, which contains all your Nymi Band users, and then click **`Change meaning`**.
   The value in the **`Meaning`** column for the group in the group table changes to **`Included`**.

   The following figure provides an example of the **`Group`** table.

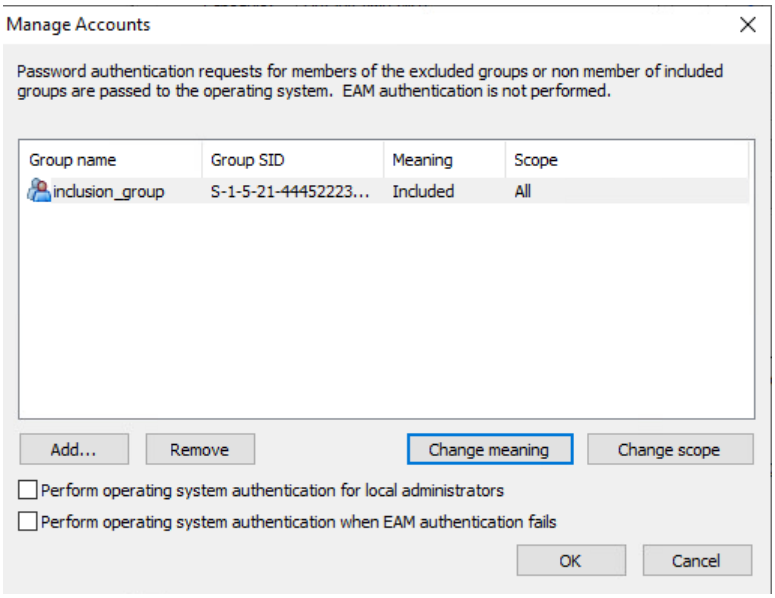


Figure 72: Inclusion Group table

9. For deployments that use Authentication Manager only, select the following options:

- Perform operating system authentication for local administrators.
- Perform operating system authentication when EAM fails.

The following figure provides an example of the options.

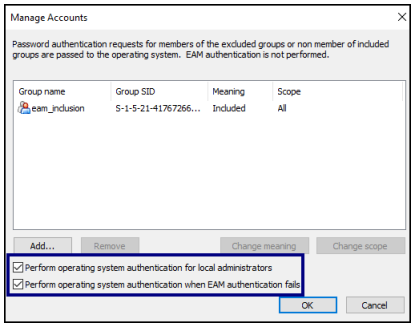


Figure 73: Authentication Manager options

Note: Authentication Manager is module that you install on client machines that allow user to tap their Nymi Band to log into the Windows desktop.

10. Click **OK**.

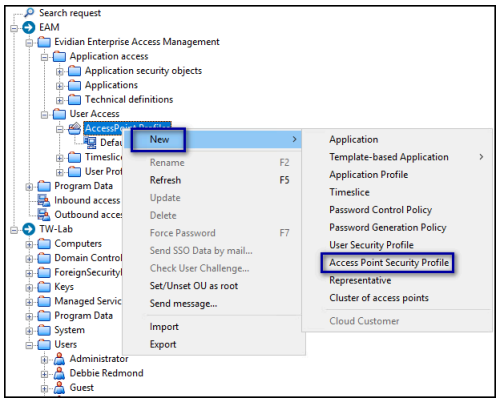
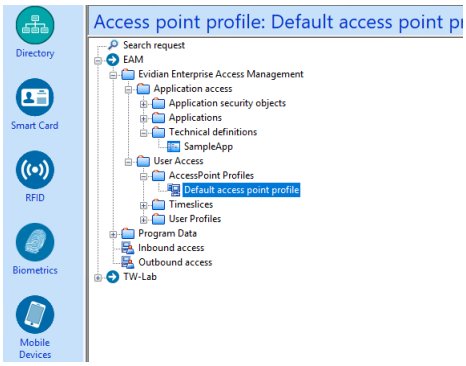
11. Click **Apply**.

Configuring an Access Point Profile for RFID-only Mode

Perform the following steps to create an access point profile that supports RFID-only mode.

Procedure

1. From the Evidian EAM Management Console, expand **`EAM > Evidian Enterprise Access Management > User Access`**.
2. Perform one of the following actions.

Option	Description
Mixed Mode environment	**a.** Right-click **`AccessPoint Profiles`**, and then select **`New > Access Point Security Profile`**, as shown in the following figure.  **b.** In the **`Name`** field, type ***RFID-only***.
RFID mode only environment	For environments where you will use RFID mode only, select **`Default access point profile`**, as shown in the following figure. 

3. In the **`Authorized authentication methods`** section, ensure that only the following methods are selected:
   - Password
   - RFID Pcsc
   - Wearable

   The following figure provides an example of the **`Configuration`** tab.

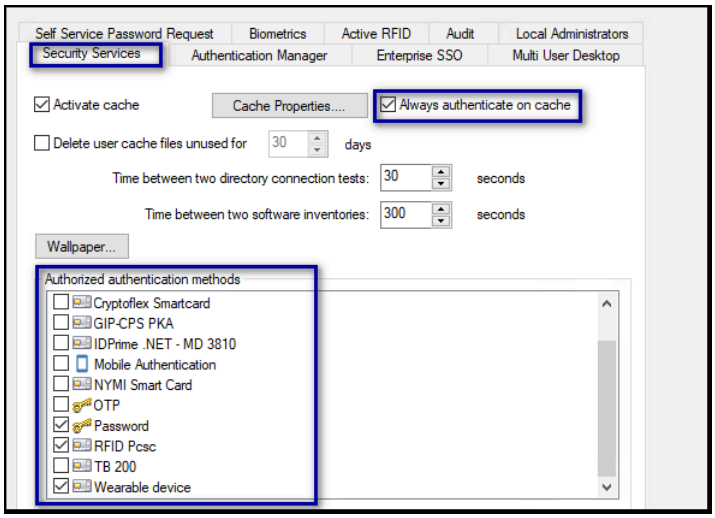


Figure 74: Access Point Profile Configuration tab

4. Click **Apply**.
5. On the **Authentication Manager** tab, perform the following actions:
   a) From the **Default action when token removed** list, select **Do nothing**.
   b) Select **Allow Roaming Session**, and then click **Apply**

   The following figure provides an example of the Authentication Manager window.

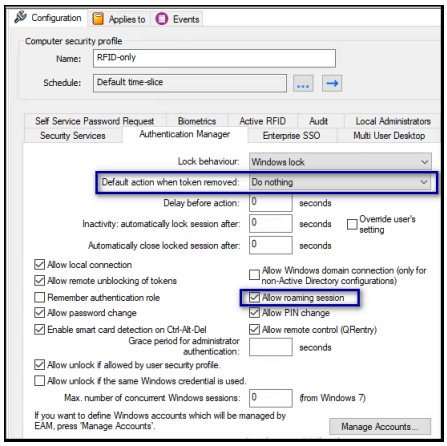


Figure 75: Authentication Manager window

6. On the **Configuration** tab, select the **Authentication Manager** tab, and then click **Manage Accounts**.
7. In the Manage Accounts window, click **Add**, as shown in the following figure.

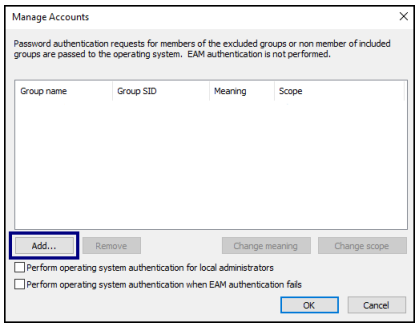


Figure 76: Add option

8. In the `Select Group` window, expand you domain, select **`Users`**, select the AD inclusion group, and then click **`OK`**.

   The following figure provides an example of the `Select Group` window with the inclusion group highlighted.

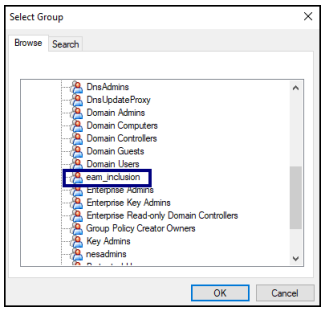


Figure 77: Inclusion Group

9. In the **`Group`** table, select the AD inclusion group that you created, which contains all your Nymi Band users, and then click **`Change meaning`**.
   The value in the **`Meaning`** column for the group in the group table changes to **`Included`**.

   The following figure provides an example of the **`Group`** table.

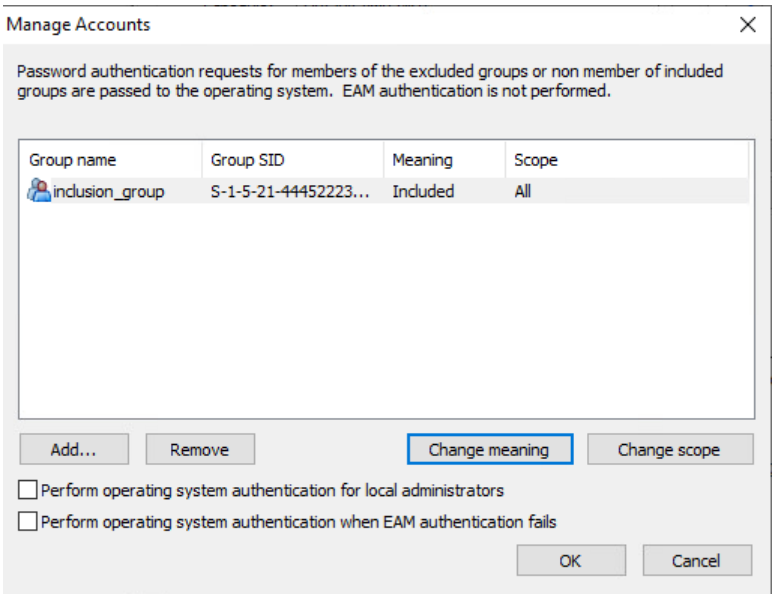


Figure 78: Inclusion Group table

10. For deployments that use Authentication Manager only, select the following options:

    - Perform operating system authentication for local administrators.
    - Perform operating system authentication when EAM fails.

    The following figure provides an example of the options.

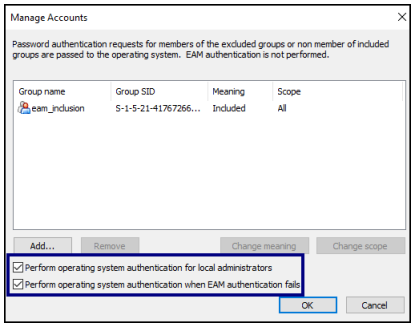


Figure 79: Authentication Manager options

Note: Authentication Manager is module that you install on client machines that allow user to tap their Nymi Band to log into the Windows desktop.

11. Click **OK**.
12. Click **Apply**.

(Mixed Mode only) Assigning Access Point Profiles to User Terminals

When your configuration uses a mix of wearable-only and RFID-only user terminals, you must assign each user terminal to the appropriate access point profile.

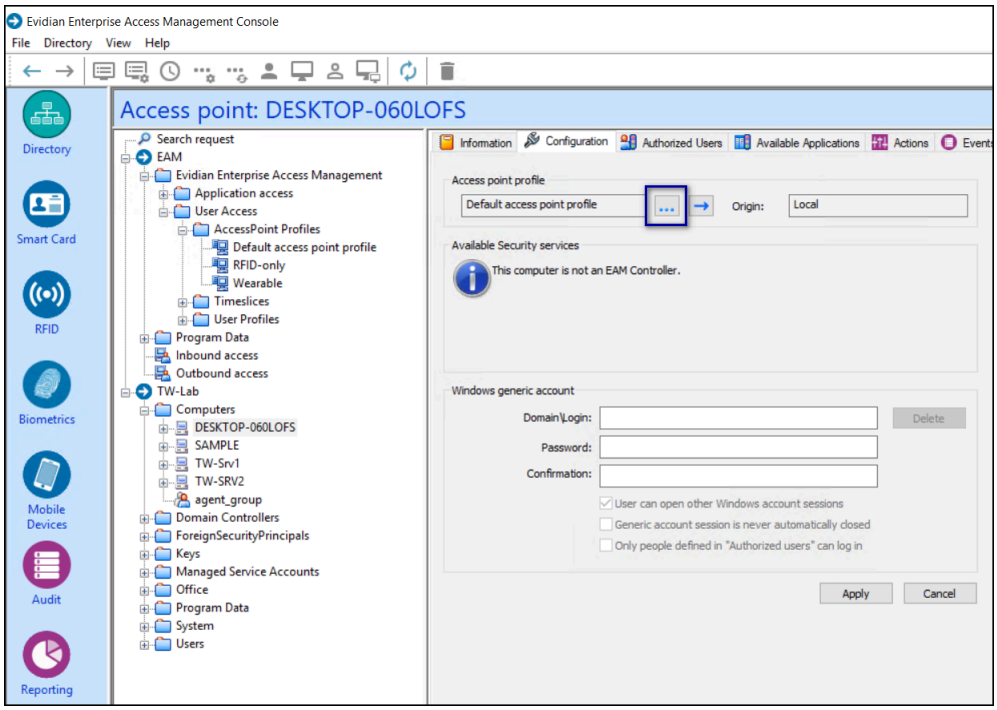
About this task

Assign the access point profile to each user terminal on which you will install the Evidian EAM Client software, including Citrix/RDP servers.

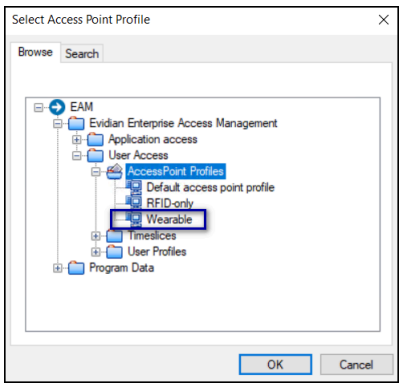
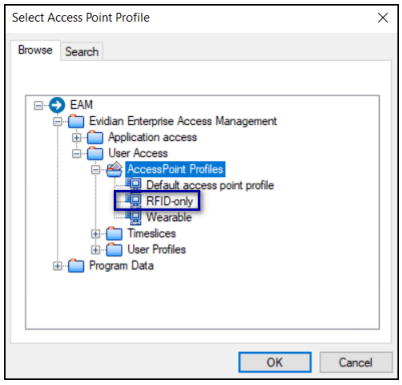
Note: Assign the wearable profile to the Nymi Band Application Terminal.

Procedure

1. In the Evidian EAM Management Console, from the left navigation panel, expand **`your_domain > Computers`**, and then select the groups of machines on which you will install the Evidian EAM Client.
2. On the **`Security Profiles`** tab, in **`Access Point Profiles`** section, the click the ellipses (...), as shown in the following figure.



3. In the **`Select Access Point`** pop-up, expand **`EAM > Evidian Enterprise Access Management > User Access > Access Point Profiles`**, and then select the appropriate profile for the authentication mode:

Option	Description
Wearable mode	
RFID-only mode	

4. Click **OK**.
5. On the `Configuration` tab, click **Apply**.

Creating Server Access Point Profile

To allow Evidian primary and auxiliary administrators to log into the Evidian EAM Management Console without the need to add the users to the Active Directory inclusion group, create a new access point profile and assign the Evidian EAM Controller to the profile.

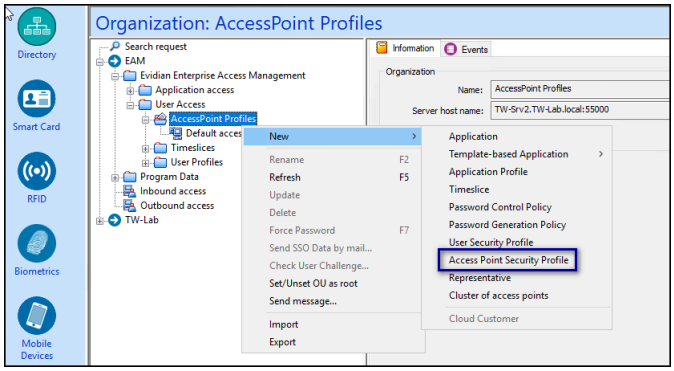
About this task

Perform the following steps in the Evidian EAM Management Console.

Procedure

1. From the Evidian EAM Management Console, expand **EAM > Evidian Enterprise Access Management > User Access**.

2. Right-click **AccessPoint Profiles**, and then select **New > Access Point Security Profile**, as shown in the following figure.



3. In the **Name** field, type ***EAM Server***.
4. Click **Apply**.
5. In the Evidian EAM Management Console, from the left navigation panel, expand **your_domain > Computers**, and then select Evidian EAM Controller.
6. On the **Security Profiles** tab, in **Access Point Profiles** section, the click the ellipses (...).
7. In the **Select Access Point** pop-up, expand **EAM > Evidian Enterprise Access Management > User Access > Access Point Profiles**, and then select the **EAM Server** profile, as shown in the following figure.

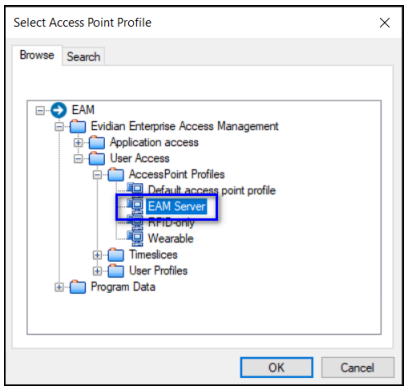


Figure 80: Access Point Profiles for EAM server

8. Click **OK**.
9. Click **Apply**.

7.2.2.4 - Configure User Profile

In Evidian, user security profiles are security objects that define a set of rights and properties that you can apply to one or more users.

If your environment will use a mixture of Wearable mode and RFID-only mode, Nymi recommends that you create two user security profiles, one for user that require Wearable mode and another user security profile for users that require RFID-only mode.

If your environment will only use one mode, you can modify the configuration of the Default User Profile.

Configuring the User Profile for Wearable

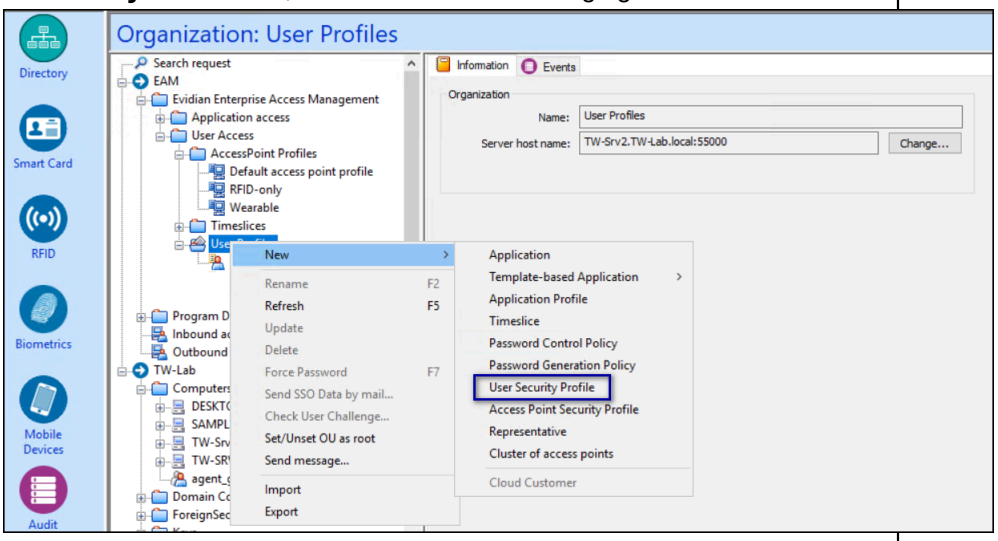
User Profiles provide you with the ability to configure Evidian behaviour for multiple user accounts.

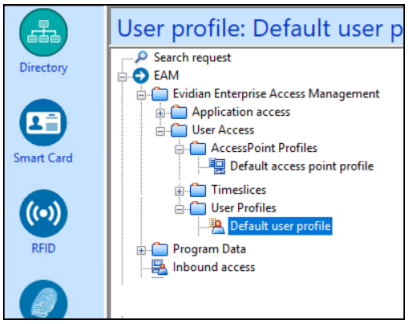
About this task

Perform the following steps in the Evidian EAM Management Console on all user profiles for users that use their Nymi Bands in the wearable configuration.

Procedure

1. From the **`Directory`** window, navigate to **`EAM > Enterprise Access Management`**.
2. Perform one of the following actions:

Option	Description
Mixed Mode environment	**a.** **`User Profiles`**, and then select **`New > User Security Profile`**, as shown in the following figure.  **b.** In the **`Name`** field, type ***Wearable***.

Option	Description
Wearable mode only environment	For environments where you will use Wearable mode only, select **`Default user profile`**, as shown in the following figure. 

3. On the **`Authentication`** tab, in the **`User authentication methods`** section, ensure that only the following methods are selected:

   - Password
   - RFID Pcsc
   - Wearable

   The following figure provides an example of the **`Authentication`** tab.

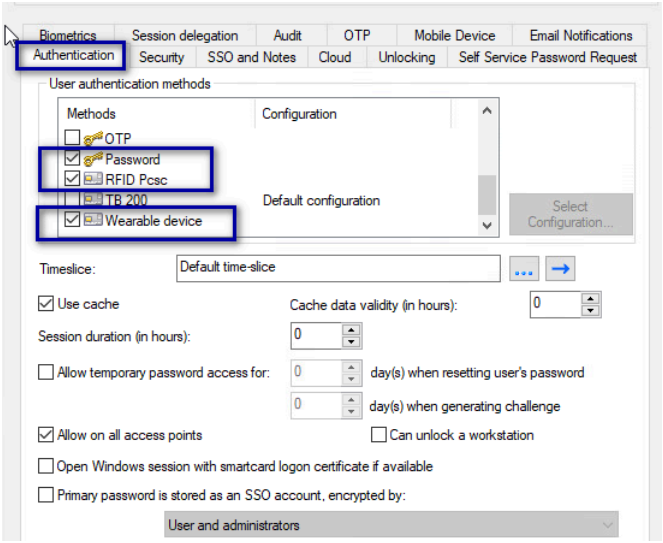


Figure 81: User Profile Authentication tab

4. Click **`Apply`**.

Configuring a User Profile for RFID-only

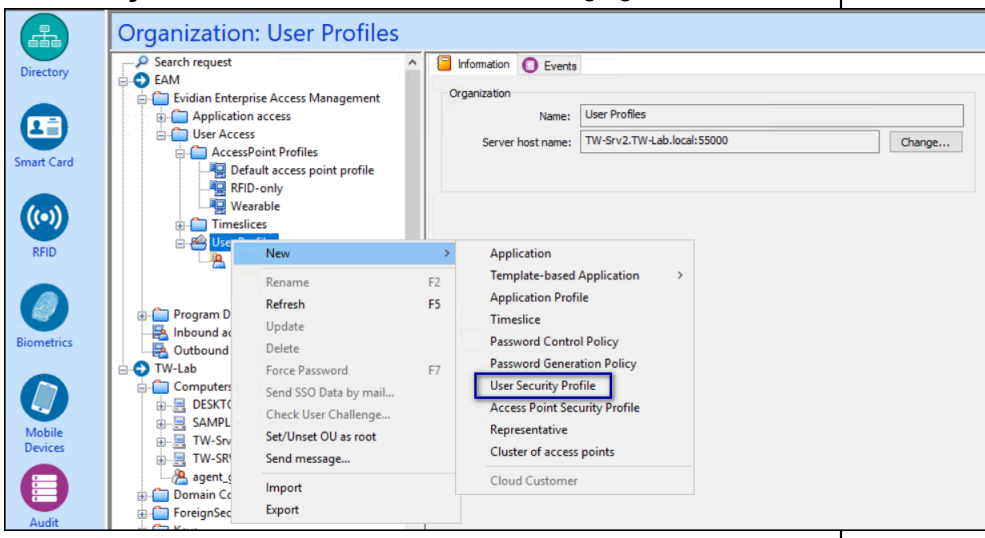
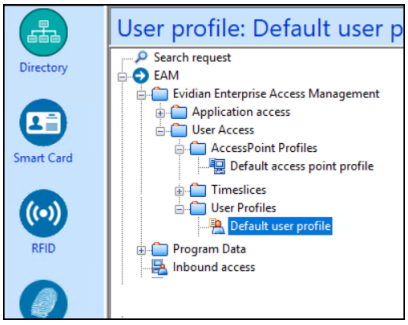
User Profiles provide you with the ability to configure Evidian behaviour for multiple user accounts. For users that to perform authentication events on user terminals without Bluetooth communication, enable and configure roaming sessions.

About this task

Perform the following steps in the to configure a user profile for users that use Nymi Bands in RFID-only mode.

Procedure

1. From the **`Directory`** window, navigate to **`EAM > Enterprise Access Management`**.
2. Perform one of the following actions:

Option	Description
Mixed Mode environment	**a.** **`User Profiles`**, and then select **`New > User Security Profile`**, as shown in the following figure.  **b.** In the **`Name`** field, type ***RFID-only***.
RFID-only mode environment	For environments where you will use RFID mode only, select **`Default user profile`**, as shown in the following figure. 

3. On the **`Authentication`** tab, in the **`User authentication methods`** section, ensure that only the following methods are selected:
   - Password
   - RFID Pcsc
   - Wearable

The following figure provides an example of the **Authentication** tab.

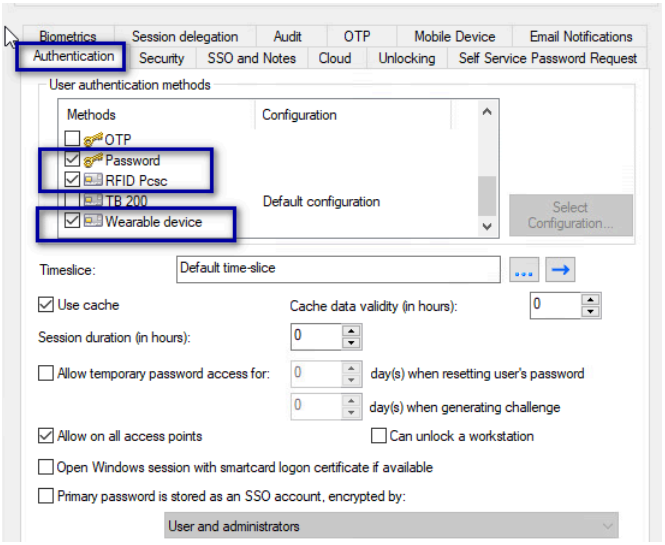


Figure 82: User Profile Authentication tab

4. Click **Apply**.
5. Navigate to **Evidian Enterprise Access Management > User access > User Profiles > Default user profile**, as shown in the following figure.

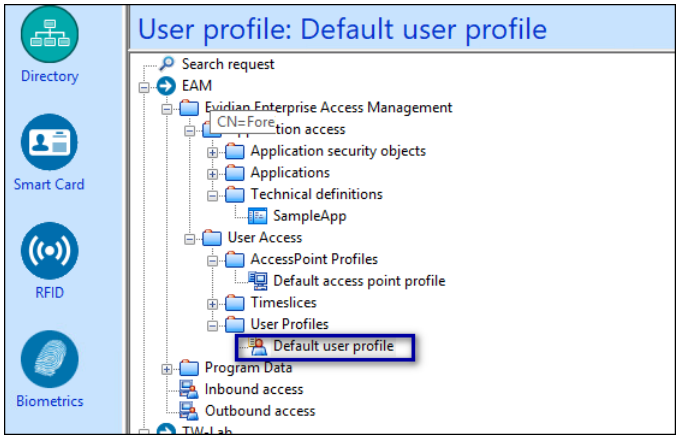


Figure 83: User Profiles

6. On the **Security** tab, select **Roaming Session Duration** and **No duration limit**, as shown in the following figure, and then click **Apply**.

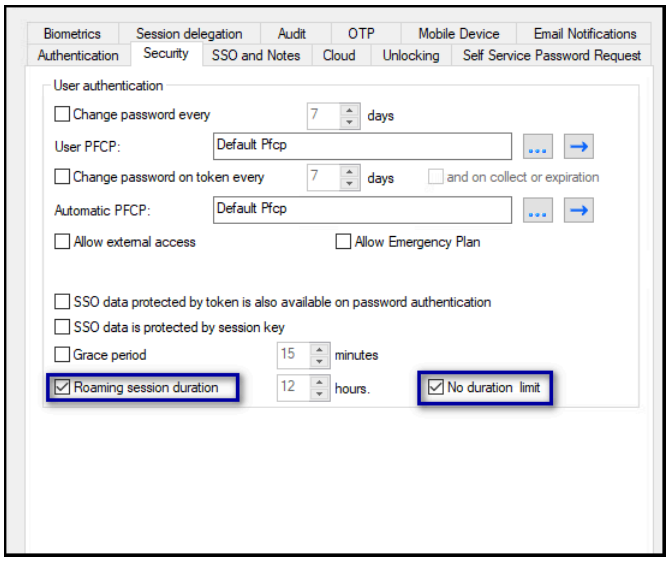


Figure 84: Roaming Session Duration Limit

(Mixed Mode only) Assigning User Profiles to Users

When your configuration requires some users to use the Nymi Band in wearable mode and other users to use the Nymi Band in RFID-only mode, you must assign each user to the appropriate user security profile.

About this task

Procedure

1. In the left navigation pane of the Evidian EAM Management Console, navigate to **`your_domain > Users`**, and then select the user.

   Alternatively, you can use the **`Search request`** option to search for the user.

   The `User Properties` page appears.
2. On the **`Security Profiles`** tab, click the ellipses(...), as shown in the following figure.

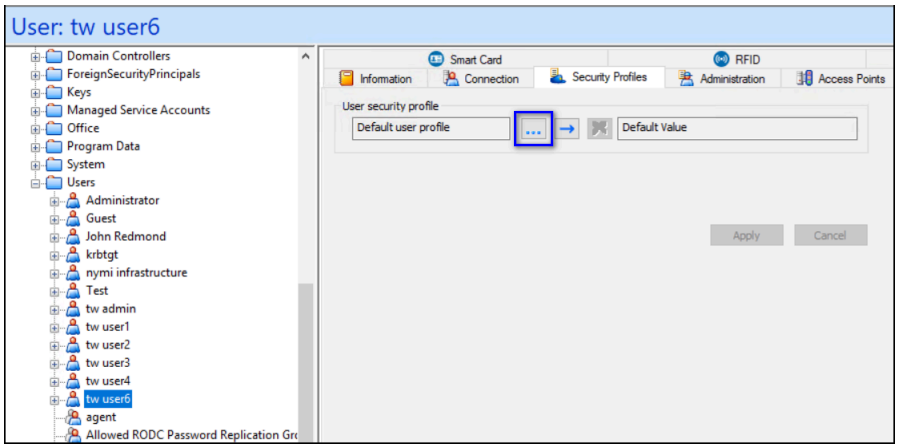
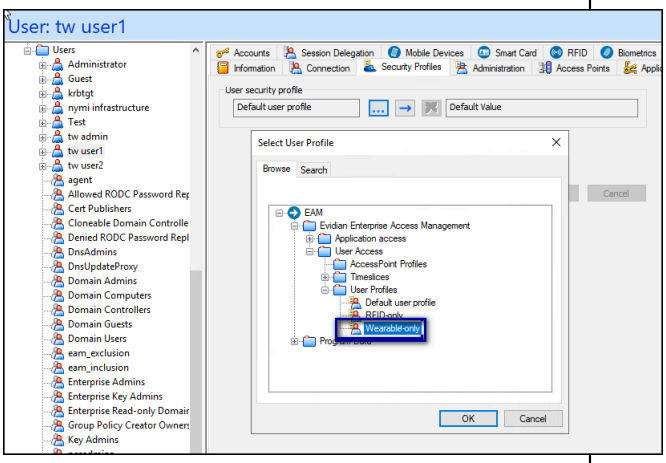
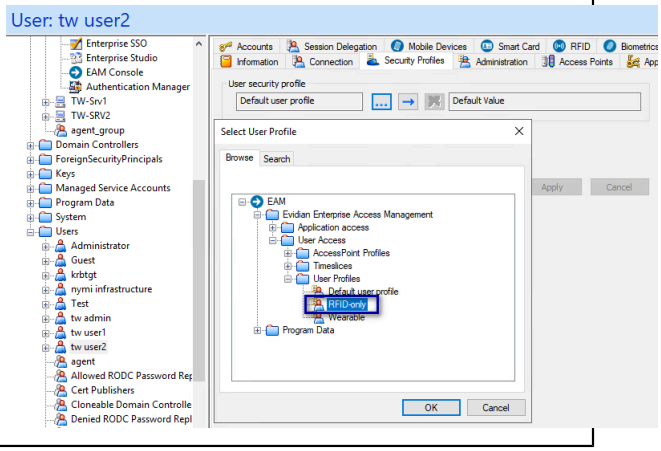


Figure 85: Change User Profile

3. On the `Select User Profile` pop up, expand **`EAM > Evidian Enterprise Access Management > User Access > User Profiles`**, and the select the appropriate user profile.

Option	Description
Wearable mode	
RFID-only mode	

4. Click **OK**.

7.2.2.5 - Configuring Additional EAM Administrators

Nymi strongly advises that you add additional administrators to the Evidian EAM Controller.

About this task

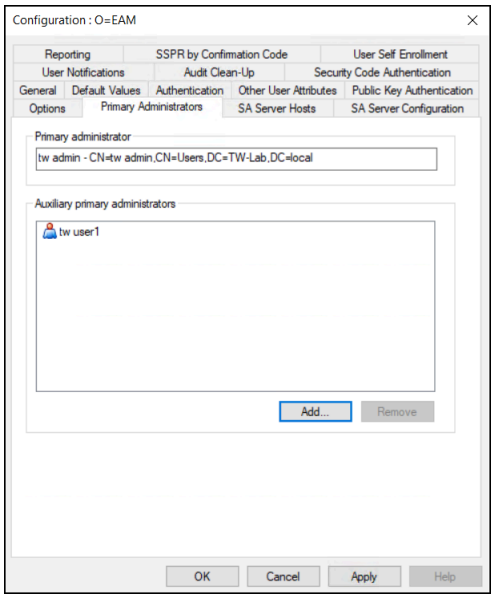
By adding at least one additional auxiliary primary administrator, you ensure that you have full access to the Evidian EAM Controller in the case where the primary administrator is locked out of the Evidian EAM Controller, for example, if the password of the primary administrator changes.

Procedure

1. Log into the Evidian EAM Management Console and click **`Accounts and access rights management`**  .
2. From the **`File`** menu, select **`Configuration`**, and then click the **`Primary Administrators`** tab.
3. Click **`Add`**.
4. In the `Select Users` window, select the **`Search`** tab.
5. In the **`Filter`** field, type the user name that you want to add, and then click **`Search`**.

   Note: You can not use Active Directory groups, you can only add individual users.
6. Select the user, and then click **`OK`**.

   The following figure provides an example of the screen with one auxiliary primary administrator.



7. Click **`Apply`**.
8. Click **`OK`**.
9. Close the Evidian EAM Management Console.

7.2.2.6 - Configuring the Evidian EAM Controller to Use the Audit Database

Before you begin

Download the following dependency software:

- Visual C++ Redistributable for Visual Studio 2015-2022 x64 version 14.34 or later
- Visual C++ Redistributable for Visual Studio 2015-2022 x86 version 14.34 or later
- Microsoft OLE DB Driver for SQL (x64)

Note: The x64 installer for Microsoft OLE DB Driver installs both the 64-bit and 32-bit driver, the x64 installer for the Microsoft Visual C++ Redistributable does not install the 32-bit binaries. You must install both the x86 and x64 versions of the Visual C++ redistributable package before you install the Microsoft OLE DB Driver for SQL (x64) package. The installation of the dependency software might require a reboot.

About this task

Perform the following steps on the Evidian EAM Controller.

Procedure

1. Run `Registry Editor` and perform the following steps:
   a) Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork \AuditSrv*
   b) Create a new DWORD (32-bit) value named *UseSQLServerSyntax*.
   c) Edit the key and in the **`Value Data`** field, type ***1***
   d) Click **OK**.
   e) Close `Registry Editor`.
2. Stop the **`Enterprise Access Management Security Server`** service.
3. Install the dependency software in the following order:
   - Visual C++ Redistributable for Visual Studio 2015-2022 x86 version 14.34 or later
   - Visual C++ Redistributable for Visual Studio 2015-2022 x64 version 14.34 or later
   - Microsoft OLE DB Driver for SQL (x64)
4. Start the **`Enterprise Access Management Security Server`** service.
5. From the EAM installation package, navigate to the *..\EAM.x64\TOOLS\WGSrvConfig* folder.
6. Hold the **`Shift`** key, right-click *WGSRVConfig.exe*, and select **`Run as a different user`**.
7. In the `Run as a different user` window, specify the username and password of a domain user has local administrator privileges.
8. Under **`Controller Configuration`**, click **`Configure local audit database`**, as shown in the following figure.

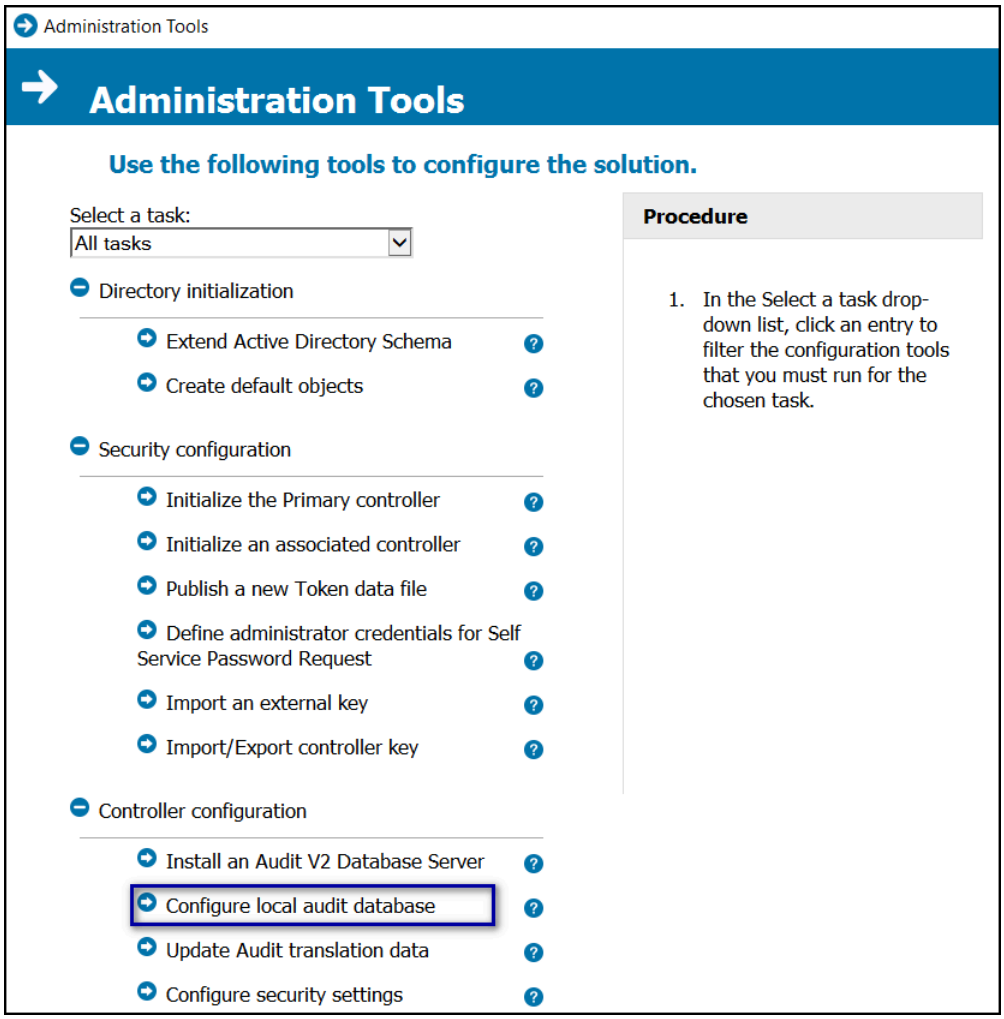


Figure 86: Configure local audit database option

9. In the **`Use existing corporate database`** section, next to **`Next to Data Source Name`**, click the ellipses (...).
10. Select **`Microsoft OLE DB Driver for SQL Server`** , as shown in the following figure.

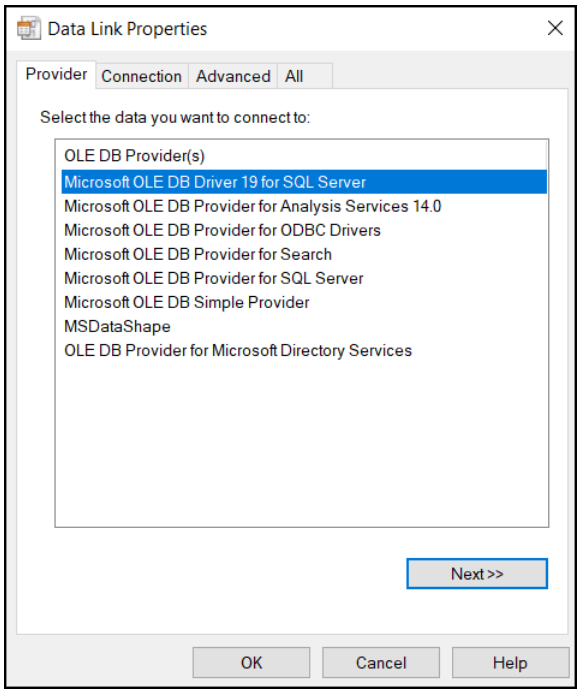


Figure 87: Microsoft OLE DB Driver for SQL Server driver option

11. Click **Next**.
12. In the **Data Link Properties**, perform the following actions:
    a) In the **Select or enter a server name** field, type FQDN of the SQL server.
    b) From the **Enter information to log on to the server** list, select the appropriate authentication method for your configuration.
       - If the SQL server uses Windows Authentication, select **Windows authentication**.
       - If the SQL server uses SQL Authentication, select **SQL authentication** and then type the username and password of the SQL account and select then **Allow saving password**.
    c) In the **Step 3** section, enable **Select the database**.
    d) From the list, select the EAM audit database.(**eamaudit**).

       The following figure provides an example of the `Select the database` window.

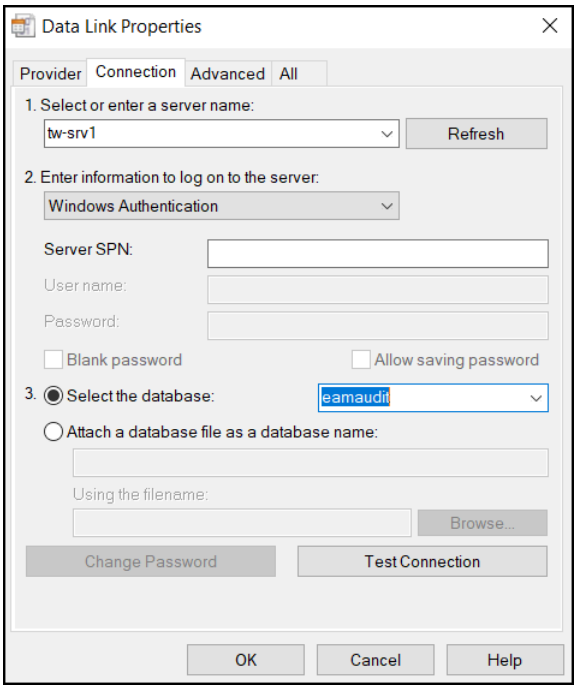


Figure 88: Select the database window

e) Click **`Test Connection`**.

f) On the `Test Connection Succeeded` window, click **OK**.

g) Click **OK**.

h) On the `Credential to access the database` window, specify the username and password of the SQL account, and then click **OK**, as shown in the following figure.

Note: Ensure that the user account has log on locally rights.

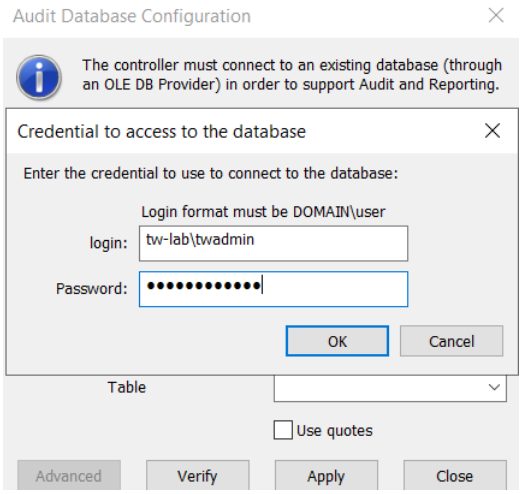


Figure 89: Credential to access the database window

The `Audit Database Configuration` window appears with information about the database.

i) On the `Audit Database Configuration` window, click **`Verify`**, as shown in the following figure.

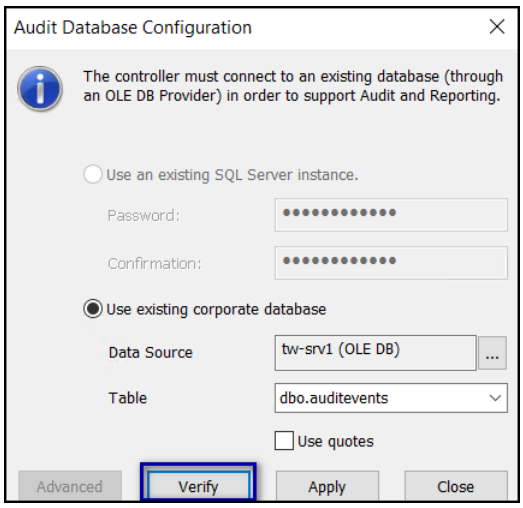


Figure 90: Audit Database Configuration window

j) On the `EAM Configuration` pop-up, click **`OK`**.

k) Click **`Close`**.

13. On the `Administration Tools` window, in the click **`Update Audit translation data`**, as shown in the following figure.

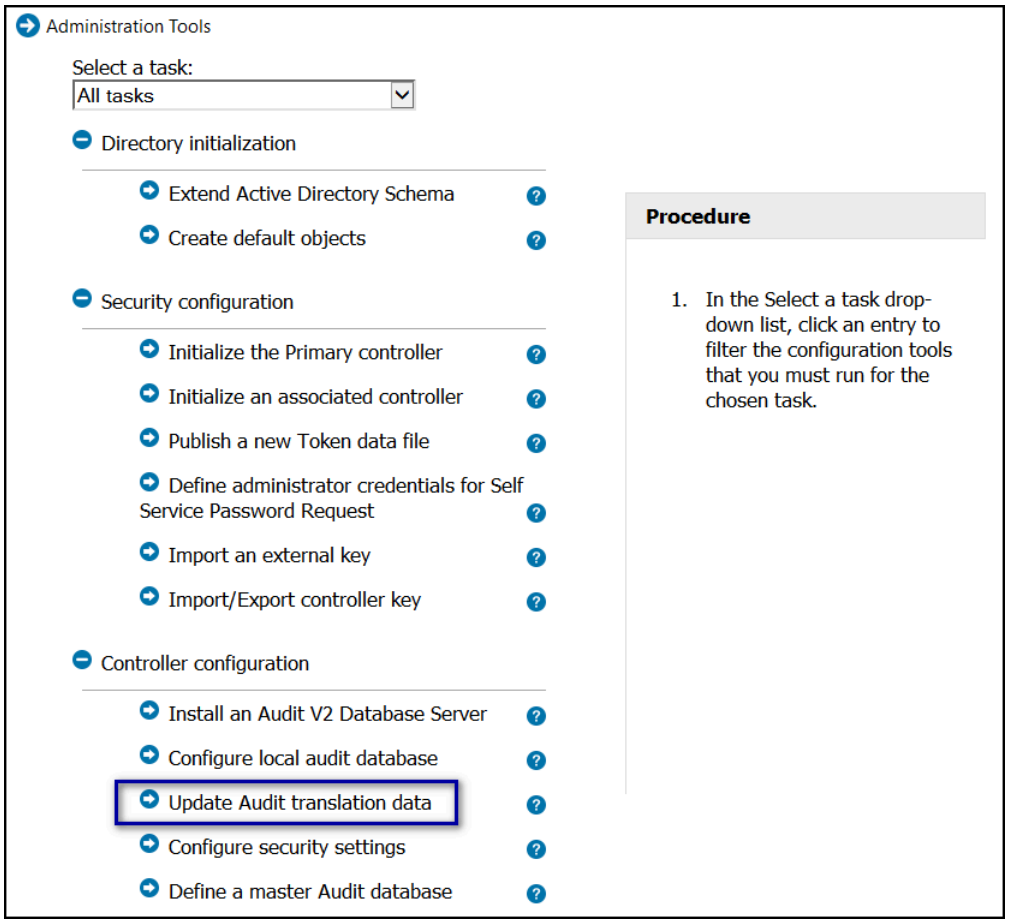


Figure 91: Update Audit translation data window

14. On the `Insert/Update Audit Metadata` window, perform one of the following actions:

- If you have a local and a central (master) database, select both the **`Import translations in local database`** and **`Import translations in master database`** options.
- If you only have a local database, select **`Import translations in local database`**.

The following figure provides an example of the `Insert/Update Audit Metadata` window.

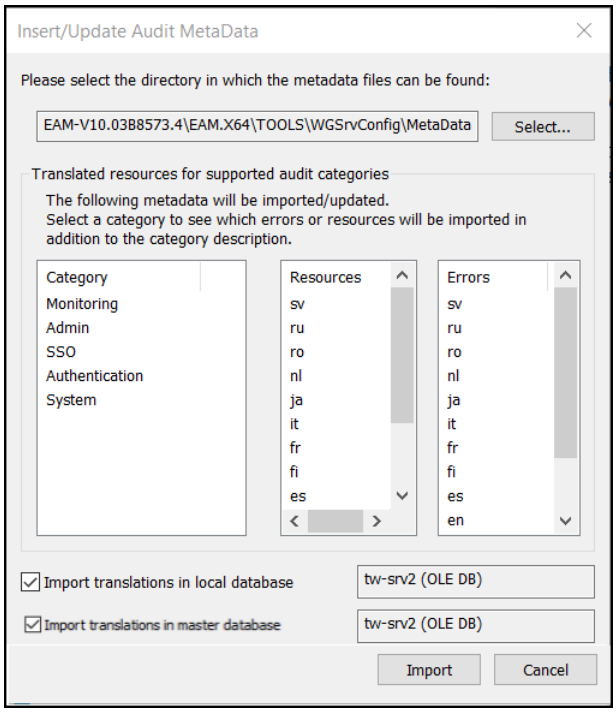


Figure 92: Update Audit translation data window

15. Click **`Import`**, and on the `EAM Configuration` pop-up, click **`OK.`**
16. Close the `Administration Tools` window.
17. Restart the **`Enterprise Access Management Security Services`** service.

What to do next

Launch Evidian EAM Management Console and click the **`Audit Reports`** button. Click **`Apply`**.

7.2.2.7 - Configuring Support for Users in Multi Domain Environments

If your configuration will include user accounts that reside in a domain that differs from the Evidian EAM Controller domain, you must edit the **`PossibleDomainsList`** in the Registry on the Evidian EAM Controller to allow you to manage the accounts in the Evidian EAM Management Console.

About this task

Procedure

1. Run **regedit**.
2. In *HKLM\Software\Enatel\WiseGuard\FrameWork\Directory*, right-click **`PossibleDomainsList`**, and then select **`Modify..`**, as shown in the following figure.

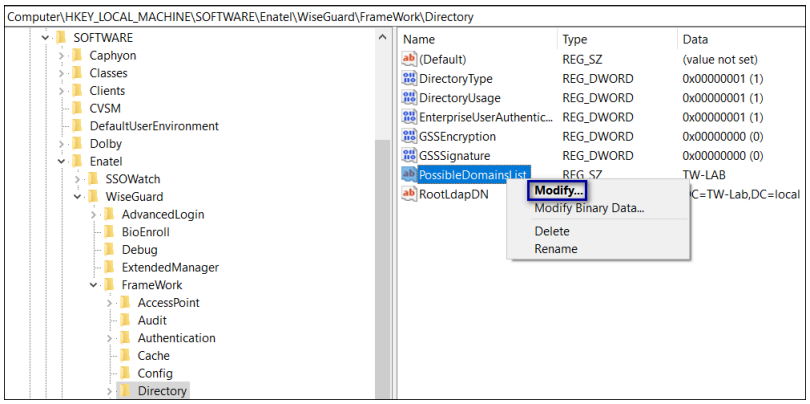


Figure 93: Modify PossibleDomainsList

3. In the **`Value Data`** field, type the NETBIOS name for each domain that contains users, that will log in to the user terminal.

   Note: Separate each domain with a space, as shown in the following example.

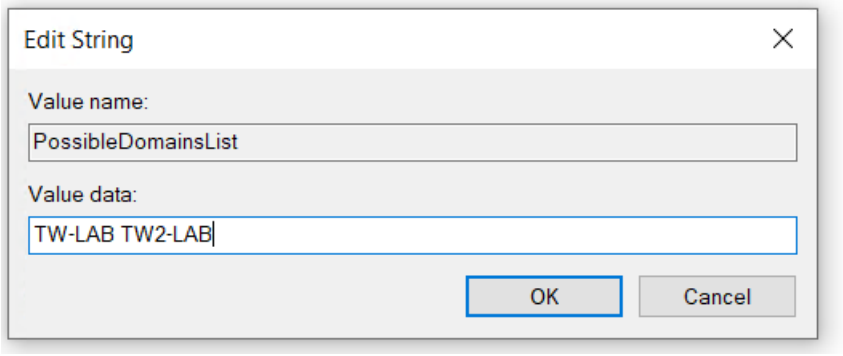


Figure 94: Configuring Multi-Domain Access

4. Click **OK**.

7.2.2.8 - Configure the Evidian EAM Controller for LDAPS

To allow the Evidian EAM Controller to use LDAPs, you must perform the following steps.

- Import the TLS certificate.
- Provide the EAM service account read-only access to the private key.
- Enable SSL in the registry.
- Install Ldp
- Test the LDAP connection.

Importing the TLS Certificate for LDAPs

Import the TLS certificate on the Evidian EAM Controller.

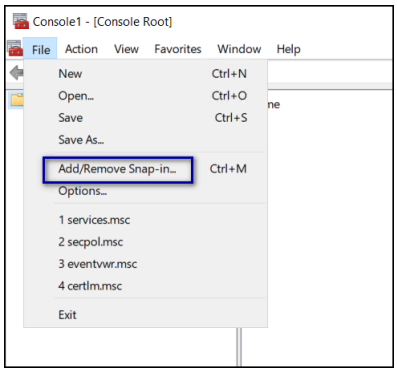
About this task

Perform the following steps in the Microsoft Management Console (mmc)

Procedure

1. From the **File** menu, select **Add/remove Snap-in** as shown in the following figure.

   Figure 95: Add/Remove Snap-in



2. On the Add or Remove Snap-ins window, select **Certificates**, and then click **Add**, as shown in the following figure.

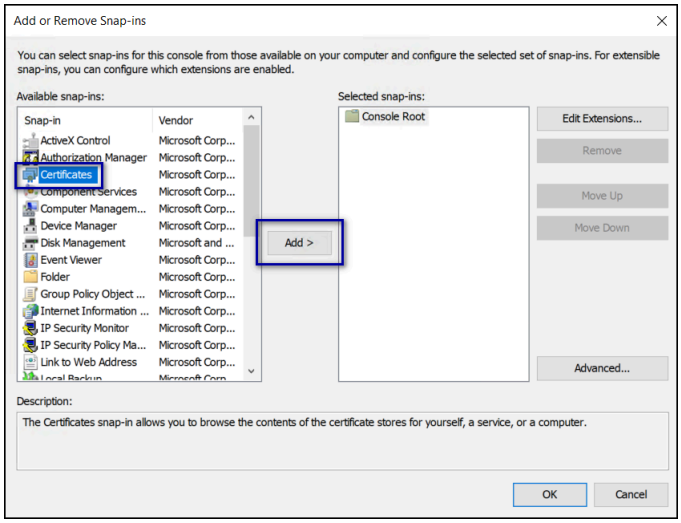


   Figure 96: Add or Remove Snap-ins window

3. On the Certificates snap-in window, select **Service account**, and then click **Next**, as shown in the following figure.

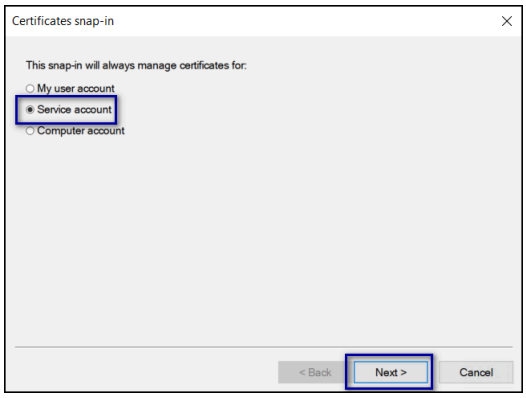


Figure 97: Certificates snap-in window

4. On the `Select Computer` window, leave the default value **`Local machine`**, and then click **`Next`**, as shown in the following figure.

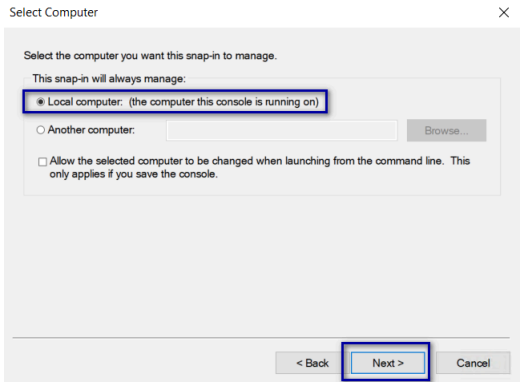


Figure 98: Select Computer window

5. On the `Certificate Snap-in` window, select **ESSOSERVER**, and then click **`Finish`**, as shown in the following figure.

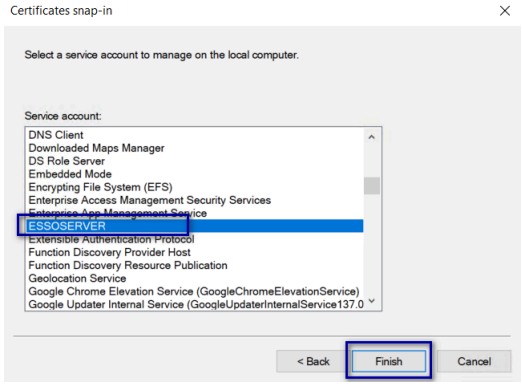


Figure 99: Certificate Snap-ins window

6. On the `Add or Remove Snap-ins` window, click **`OK`**, as shown in the following figure.

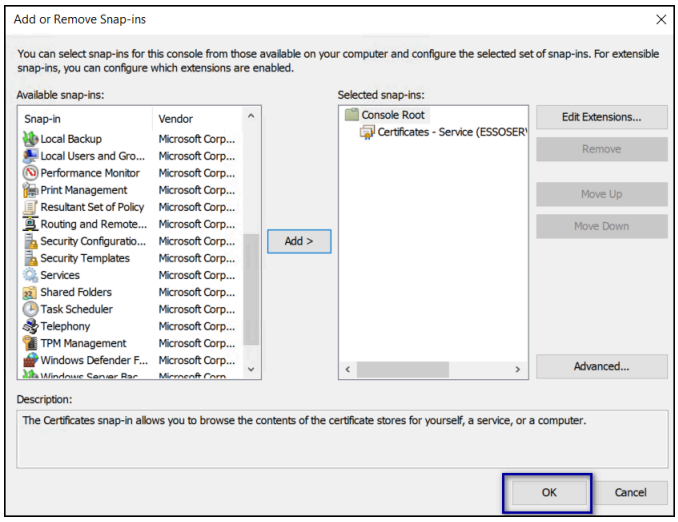


Figure 100: Add or Remove Snap-ins window

7. In the `Console` window, expand **`Certificates`**, right-click **`ADAM_ESSOSERVER \Personal`**, and then select **`All Tasks > Import`**, as shown in the following figure.

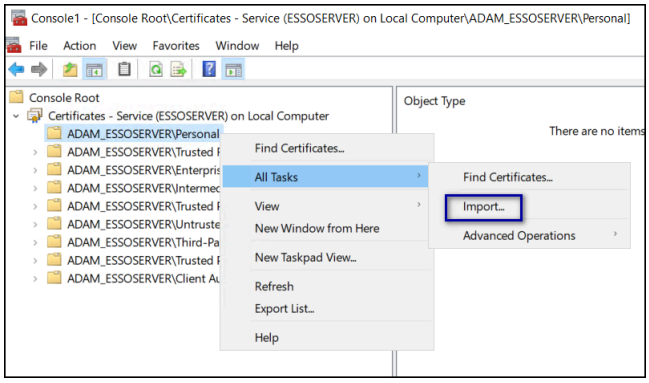


Figure 101: Import Certificate option

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

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

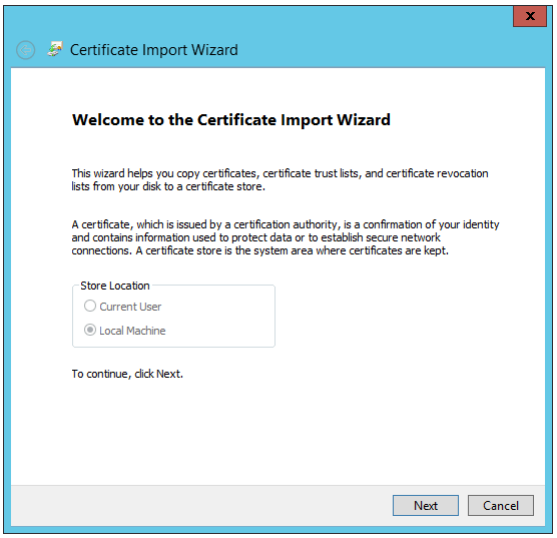


Figure 102: Welcome to the Certificate Import Wizard screen

9. On the `File to Import` screen, click **`Browse`**, navigate to the folder that contains the certificate file, select the file, and then click **`Open`**.
10. On the `Files to import` screen, click **`Next`**, as shown in the following figure.

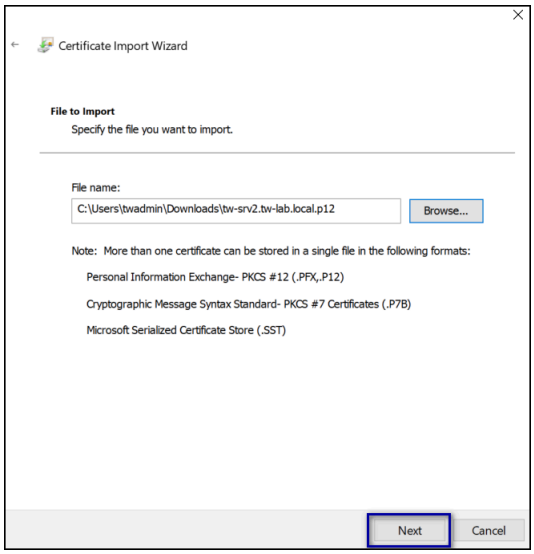


Figure 103: Files to import

11. On the `Private key protection` window, in the **`password`** field, type the password for the TLS certificate, and then click **`Next`**

    The following figure provides an example of the `Private key protection` window.

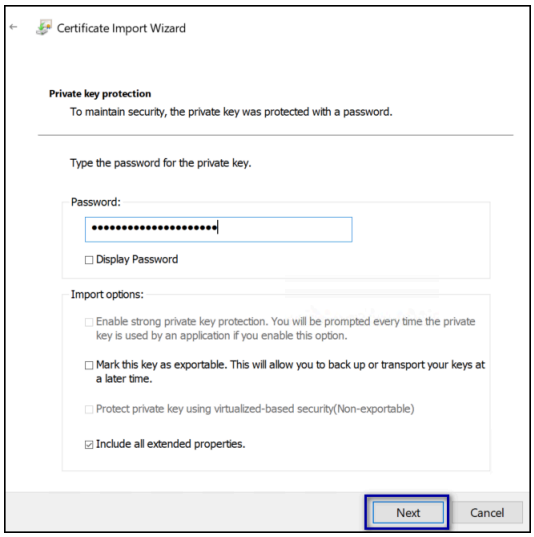


Figure 104: Private key protection

12. On the `Certificate Stores` window, leave the default certificate location, and then click **`Next`**.

The following figure provides an example of the `Private key protection` window.

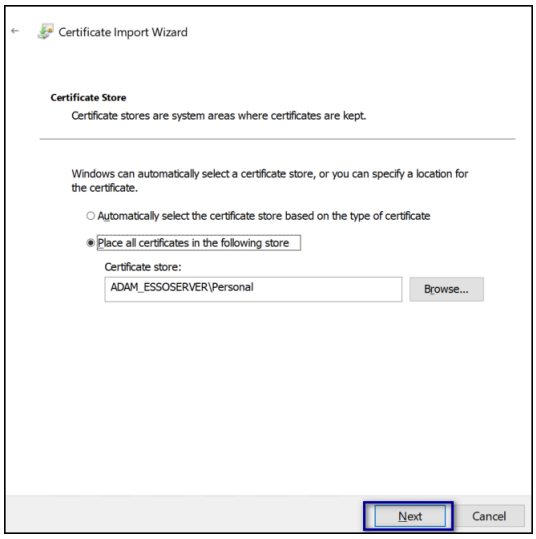


Figure 105: Private key protection

13. On the `Completing the Certificate Import Wizard` window, click **`Finish`**, as shown in the following figure.

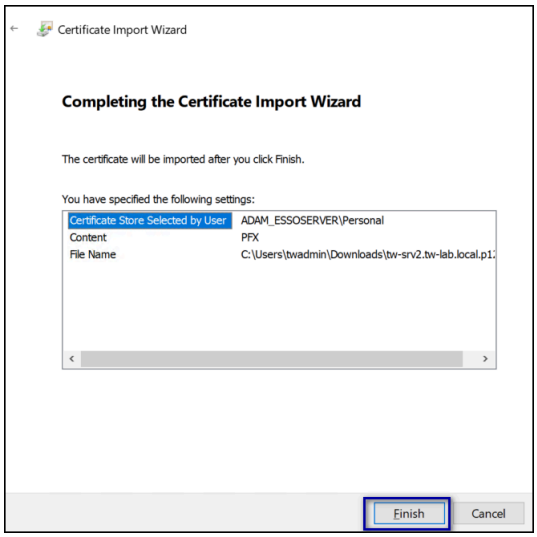


Figure 106: Completing the Certificate Import Wizard

The `Import was successful` pop-up appears.

14. On the `Console` window, click **`Certificates`**.

The imported certificate appears in the `Certificate` window, as shown in the following figure.

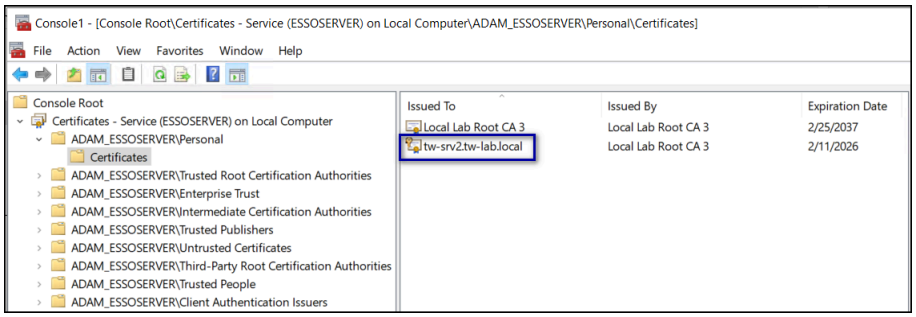


Figure 107: TLS Certificate

Providing the ESSOSERVER service account Read Access to Private Key

In an LDAPS configuration, the ESSOSERVER service account requires read access to the private key of the TLS certificate.

Before you begin

On the Evidian EAM Controller, from the Windows **`Services`** applet, determine which account starts the ESSOSERVER service. The default account is Network Service, as shown in the following figure.

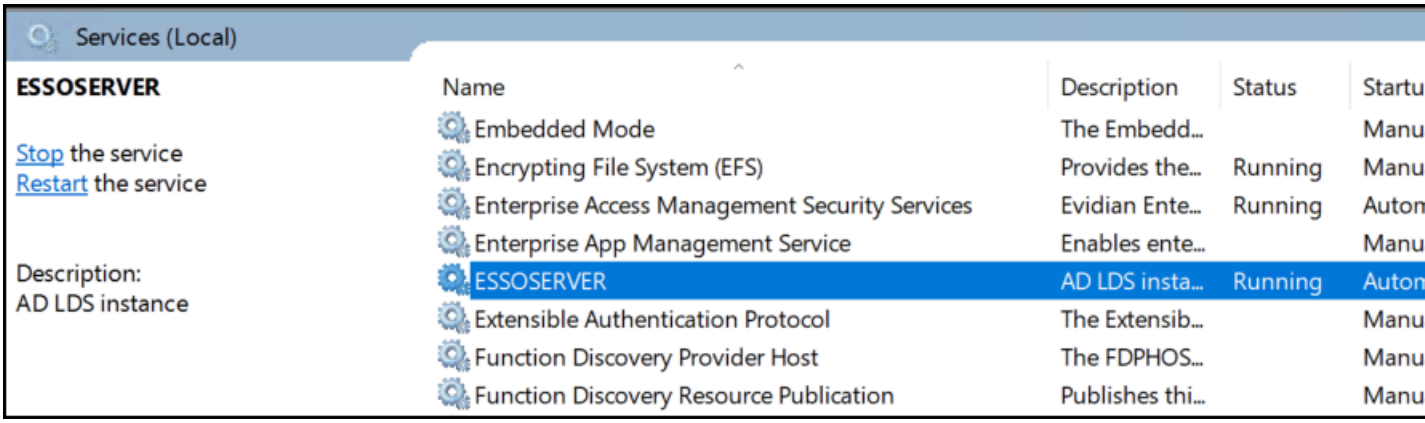


Figure 108: ESSOSERVER service

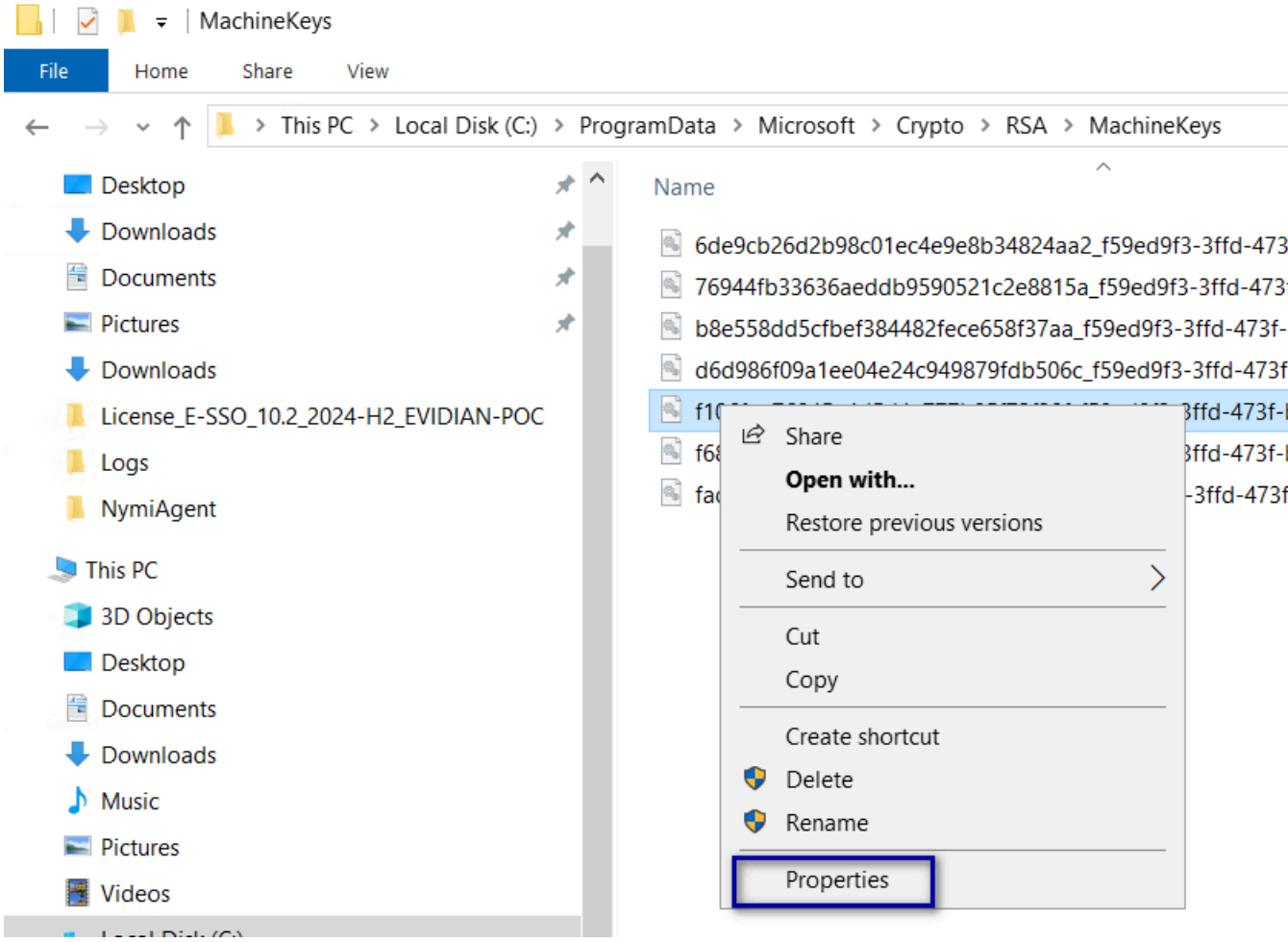
About this task

Perform the following steps on the Evidian EAM Controller.

Procedure

1. From `File Explorer`, navigate to *C:/ProgramData/Microsoft/Crypto/RSA/MachineKeys*.
2. right-click the file with a timestamp that matches the date that you imported the TLS certificate, and then select **`Properties`**.

   The following figure provides a example of a TLS certificate that was imported on 1 May 2025.



3. On the **`Security`** tab, click **`Advanced`**, as shown in the following figure.

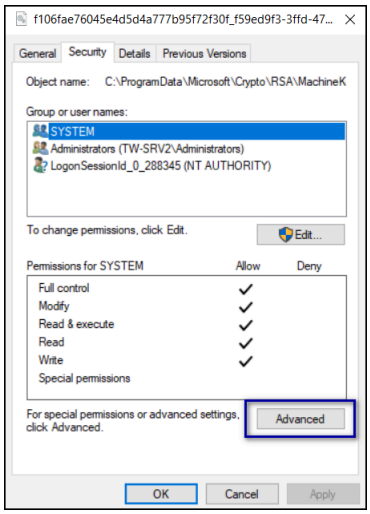


Figure 109: Advanced option

4. On the `Advanced Security Settings` window, click **`Change permissions`**, as shown in the following figure.

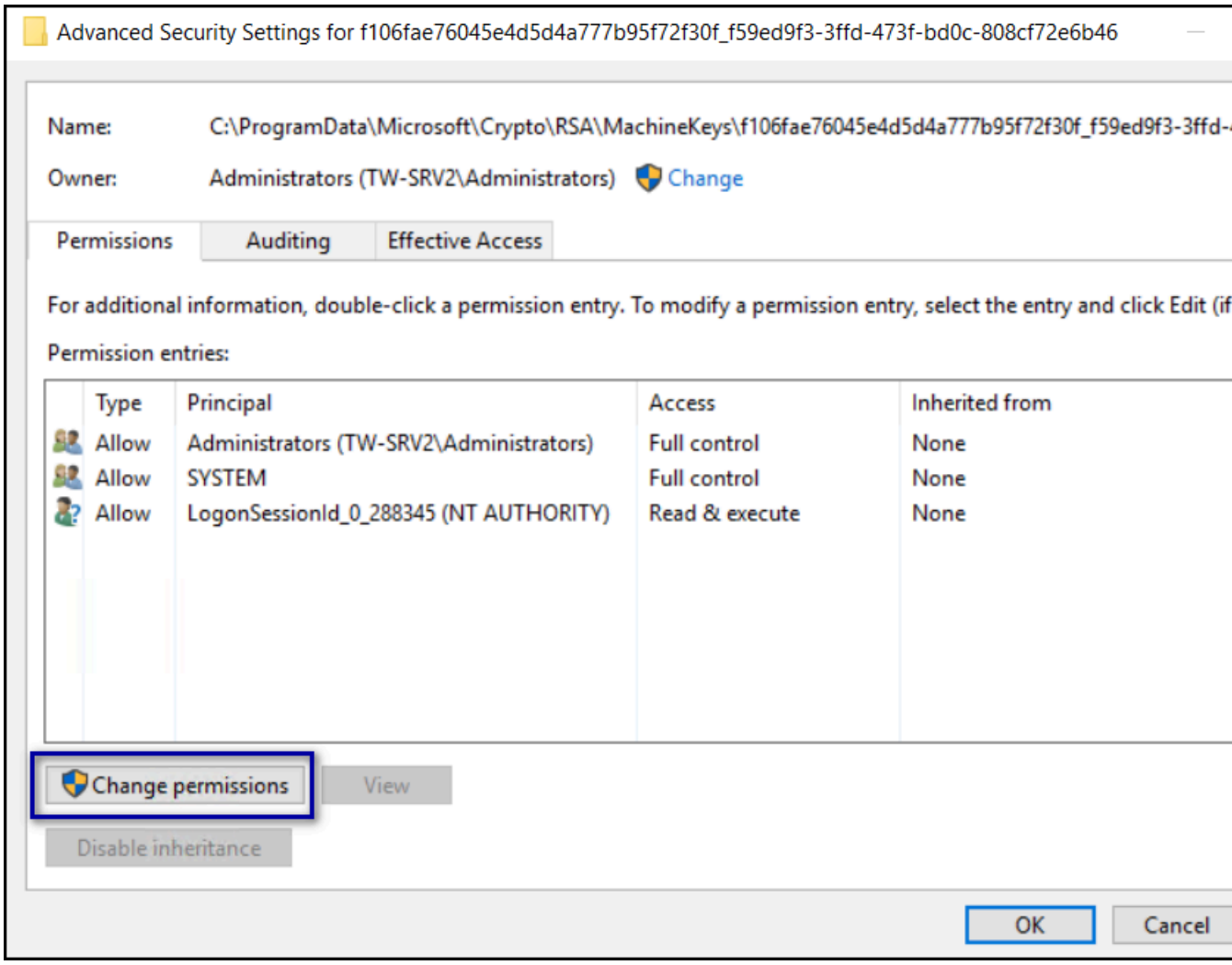


Figure 110: Change Permissions Option

5. On the `Advanced Security Settings` window, click **Add**, as shown in the following figure.

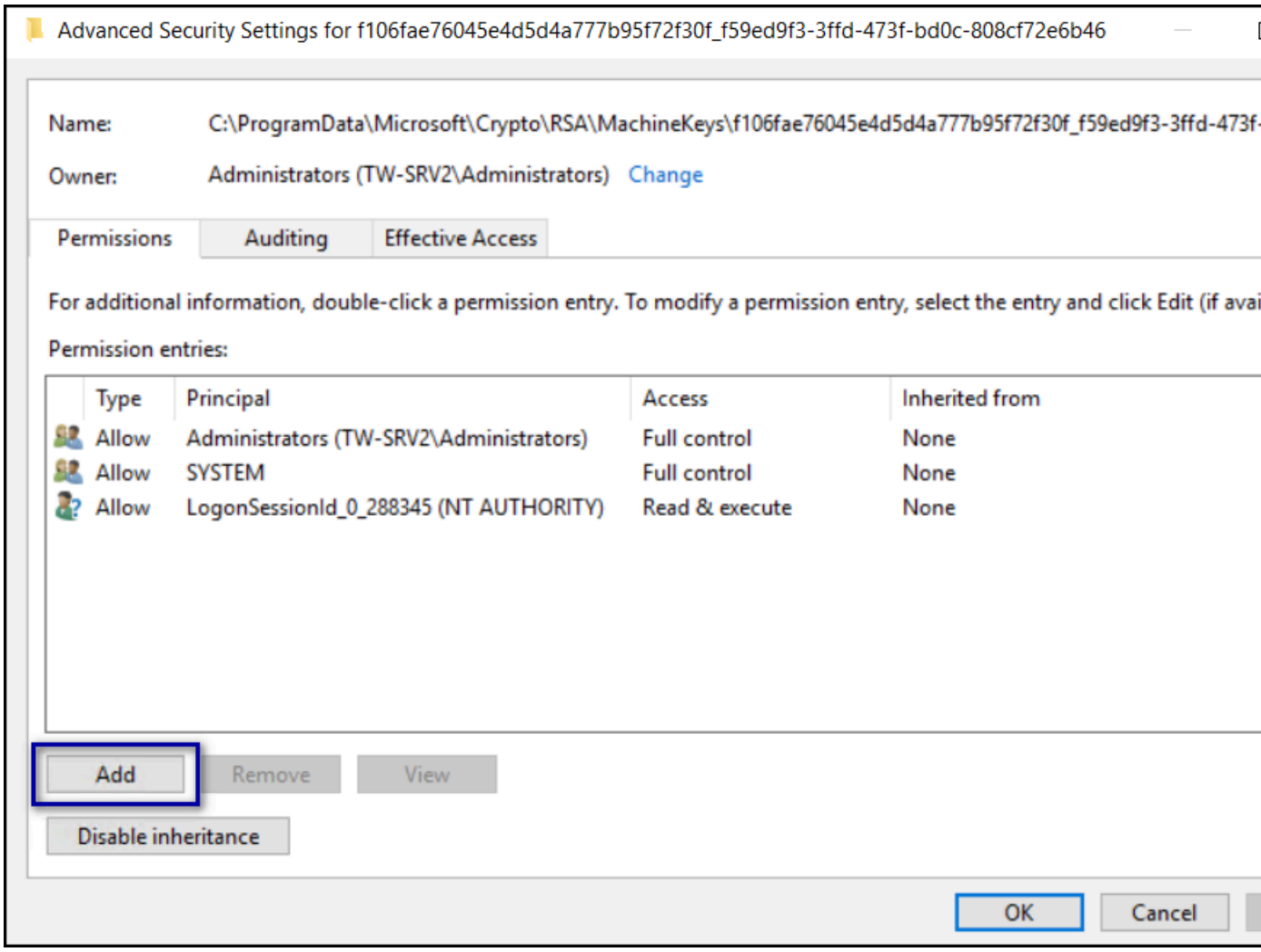


Figure 111: Add Option

6. Click **`Select a principal`**, as shown in the following figure, and the perform the following actions:

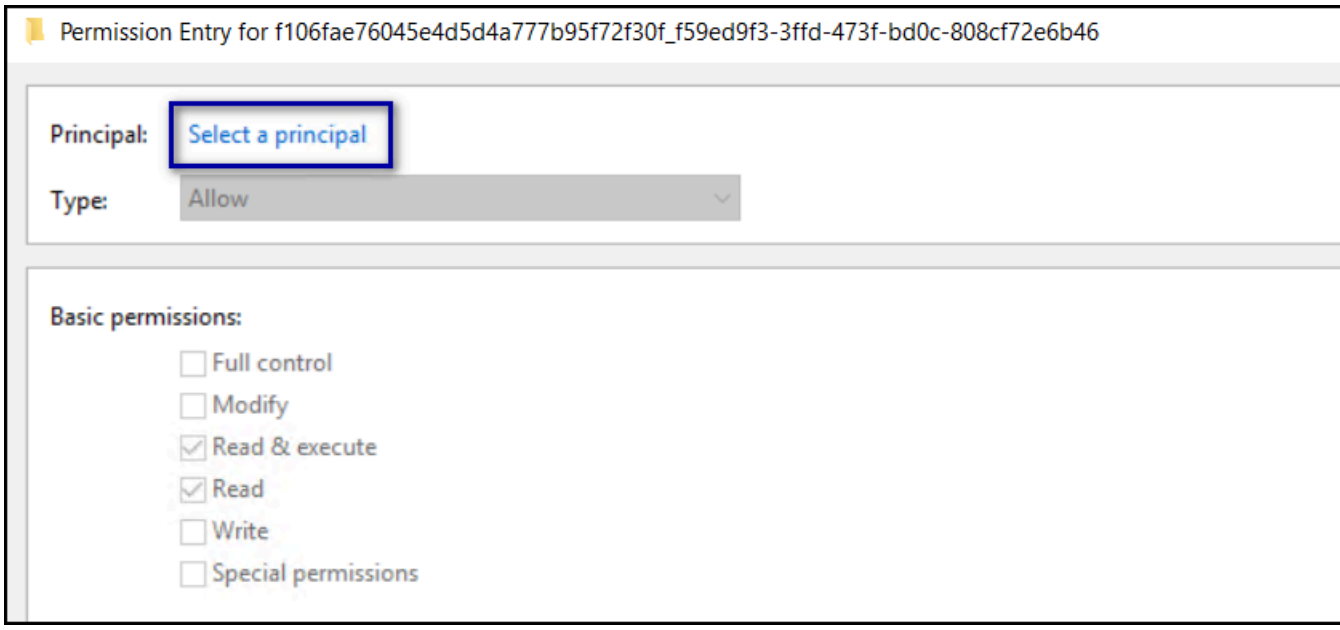


Figure 112: Select a principal option

a) On the `Select User, Computer or Group` window, in the **`Enter the object name to select`** field, enter the service account name, and then click **`Check Names`**.

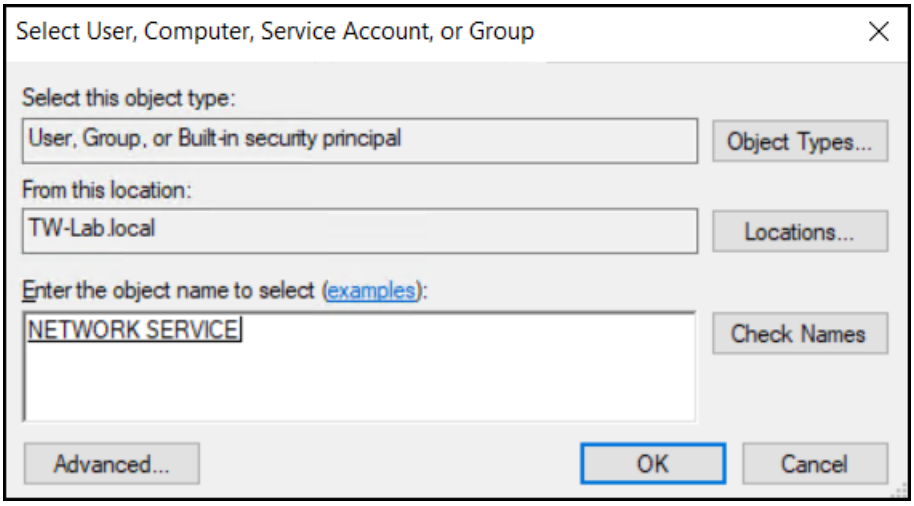


Figure 113: Enter the object name to select field

b) Click **`Ok`**.

c) Clear the **`Read & Execute`** so that only the **`Read`** option remains selected, and then click **`Ok`**.

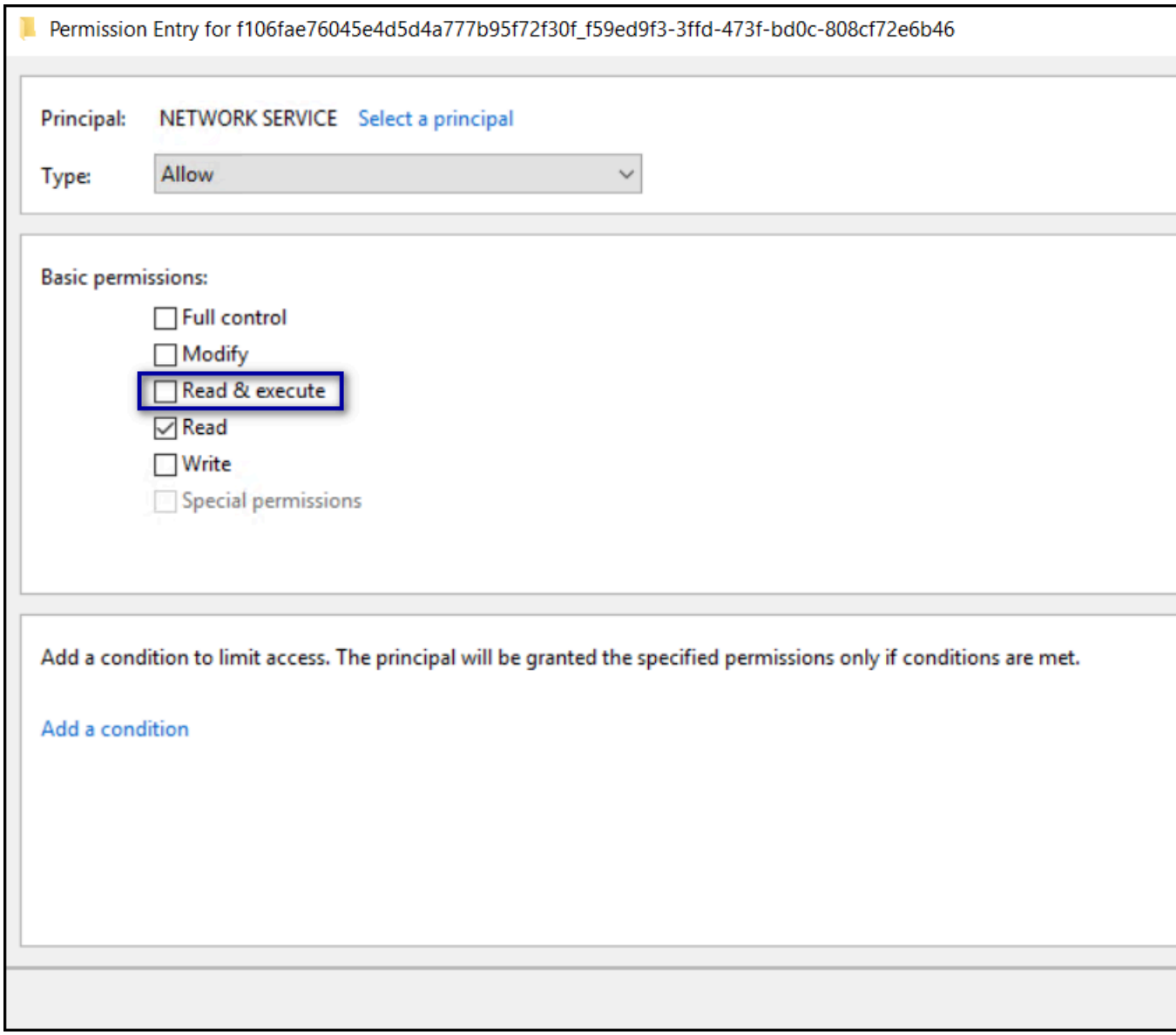


Figure 114: Modify Permissions

d) Click **Apply**, and then **OK**.

e) Click **OK**.

7. Restart the **ESSOSERVER** service.

Enabling LDAPS Support on the Evidian EAM Controller

The Nymi with Evidian Solution supports the use of LDAPS in an AD or AD LDS configuration.

Evidian Authentication Manager and Enterprise SSO 10.0 evolution 2 patch level 3 and later supports LDAPS on AD LDS. For more information on how to install LDAPS for AD LDS, see Microsoft.

The following table summarizes the registry key changes that you must make on the Evidian EAM Controller to use LDAPS for each configuration.

Configuration	Registry Setting
Support LDAPS for the communication with an AD LDS instance.	Create the following registry keys: Key #1 • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\WGDirectory* • **Type:** DWORD 32-bit • **Name:** ***SSL*** • **Value:** ***1*** Key #2 If some of your Active Directory(AD) Domain Controllers(DCs) do not use SSL or are not reachable, perform the following steps to define which AD DCs the Evidian software should use for LDAPS: • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\WGDirectory* • **Type:** DWORD 32-bit • **Name:** ***ServerList*** • **Value:** ***fqdn1:55001 fdqn2:55001*** where: • *fqdn1* and *fqdn2* are the fully qualified domain names of the LDAP Directory Servers. • *55001* is the LDAPS port number. For Example: srvad1.mycompany.lan:55001 srvad2.mycompany.lan:55001 **Note:** You can separate the server entries with a comma or space. Ensure that the *GSSEncryption* and *GSSSignature* registry keys are deleted in the following location: *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard\FrameWork \WGDirectory*

Configuration	Registry Setting
Support LDAPS for the communication with an Active Directory instance.	Create the following registry keys: Key #1 • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\Directory* • **Type:** DWORD 32-bit • **Name:** ***SSL*** • **Value:** ***1*** Key #2 If some of your AD DCs do not use SSL or are not reachable, perform the following steps to define which AD DCs the Evidian software should use for LDAPS: • **Location:***HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\Directory* • **Type:** DWORD 32-bit • **Name:** ***ServerList*** • **Value:** ***fqdn1:port fdqn2:port*** where: • *fqdn1* and *fqdn2* are the fully qualified domain names of the LDAP Directory Servers. • *port* is the LDAPS port number and is not required if LDAPS communications occur over the default port 636. For Example: srvad1.mycompany.lan srvad2.mycompany.lan **Note:** You can separate the server entries with a comma or space. Ensure that the *GSSEncyption* and *GSSSignature* registry key values are set to 0 in the following location: *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard\FrameWork \Directory*

Installing AD DS Tools

Install AD DS Tools on the EAM controller to provide you with applications that support the deployment.

About this task

Perform the following steps in the Windows `Server Manager` application.

Procedure

1. On the `Dashboard`, click **`Add roles and features`**.
2. On the `Before you begin` page, click **`Next`**, as shown in the following figure.

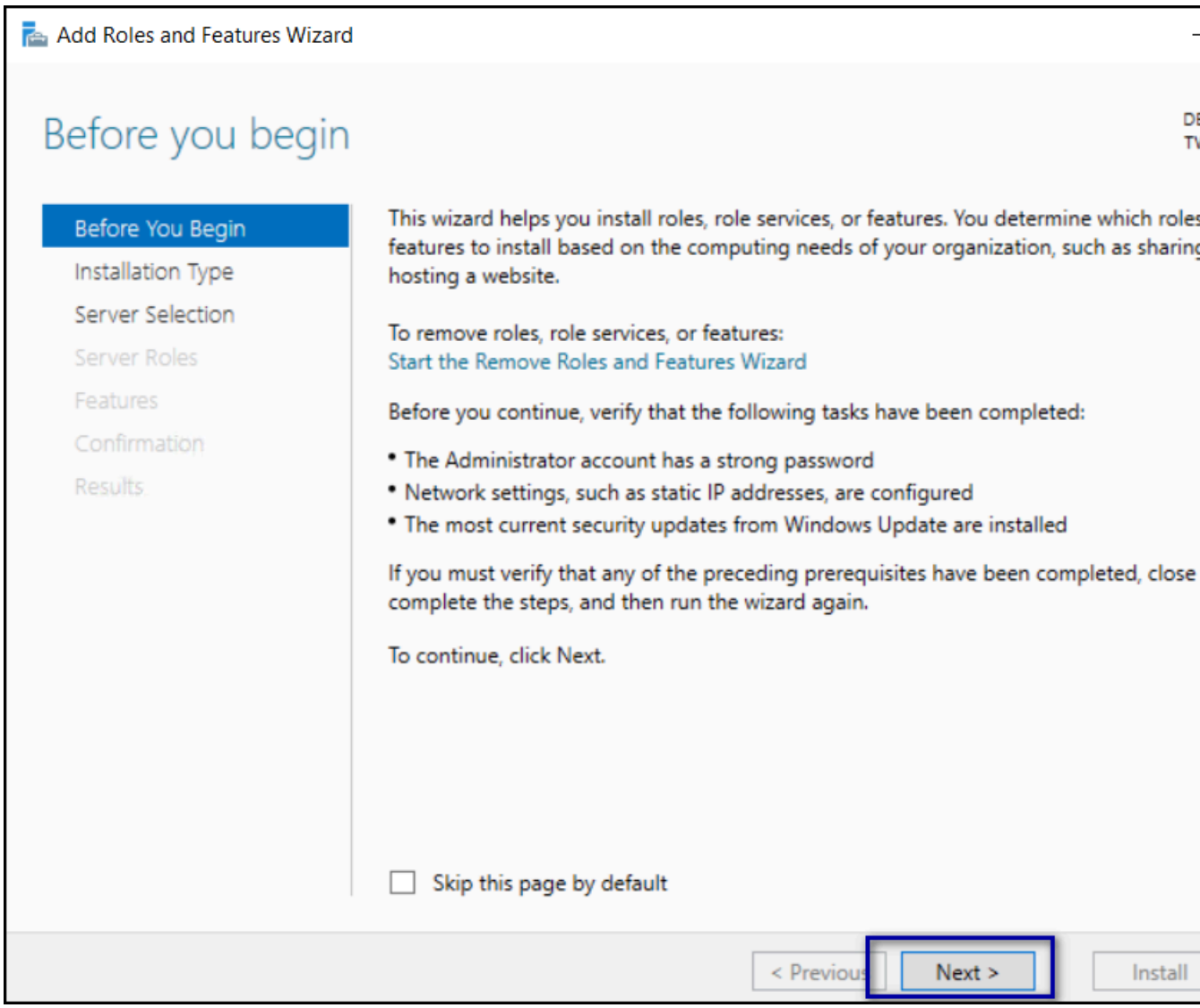


Figure 115: Before you begin

3. On the `Add Roles and Features Wizard` window, click **`Next`**, as shown in the following figure.
4. On the `Selection installation type` window,leave the default selection **`Role-based or feature-based installation`**, and the click **`Next`**.

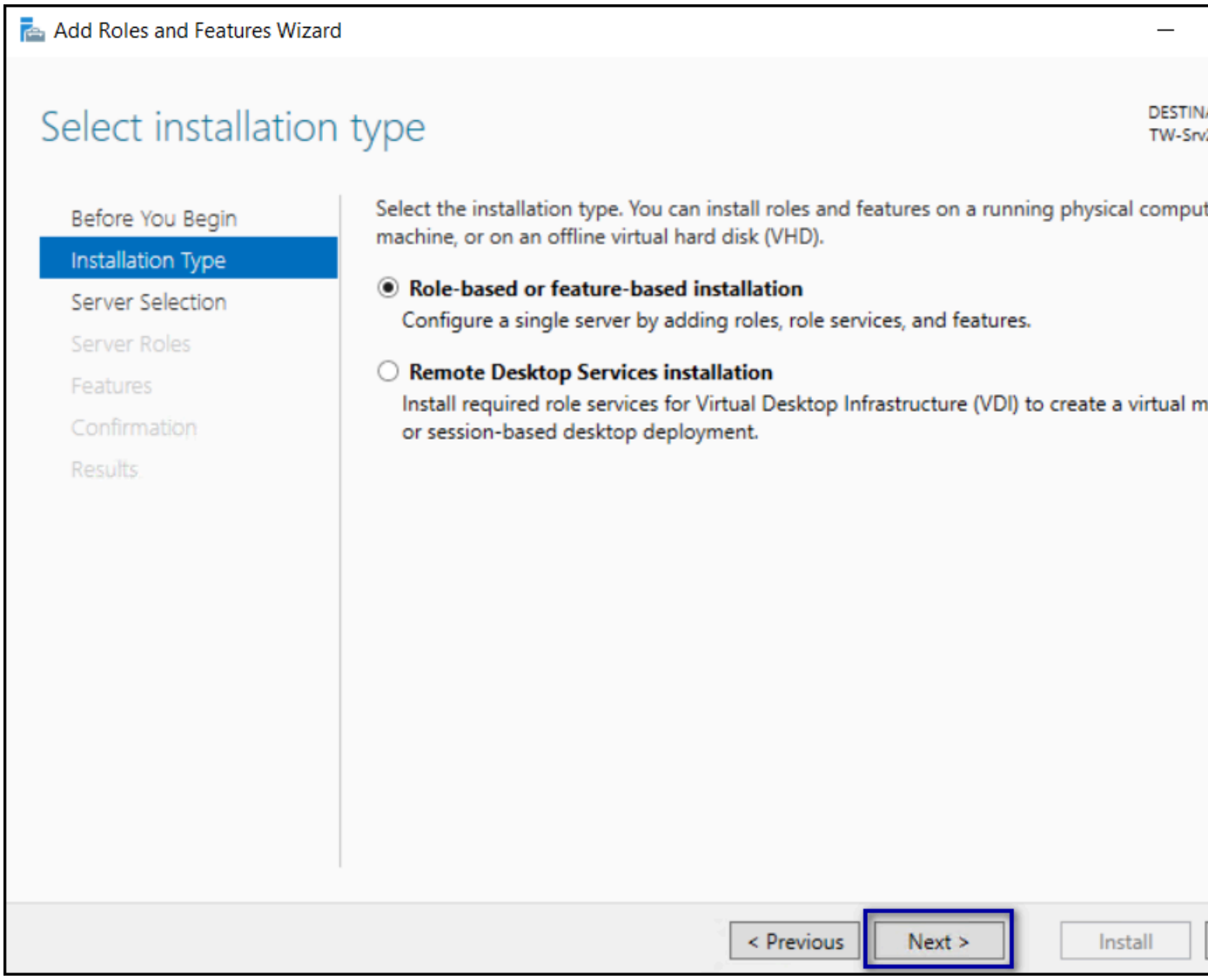


Figure 116: Select Installation Type window

5. On the `Select Server Destination` window, click **`Next`**, as shown in the following figure.

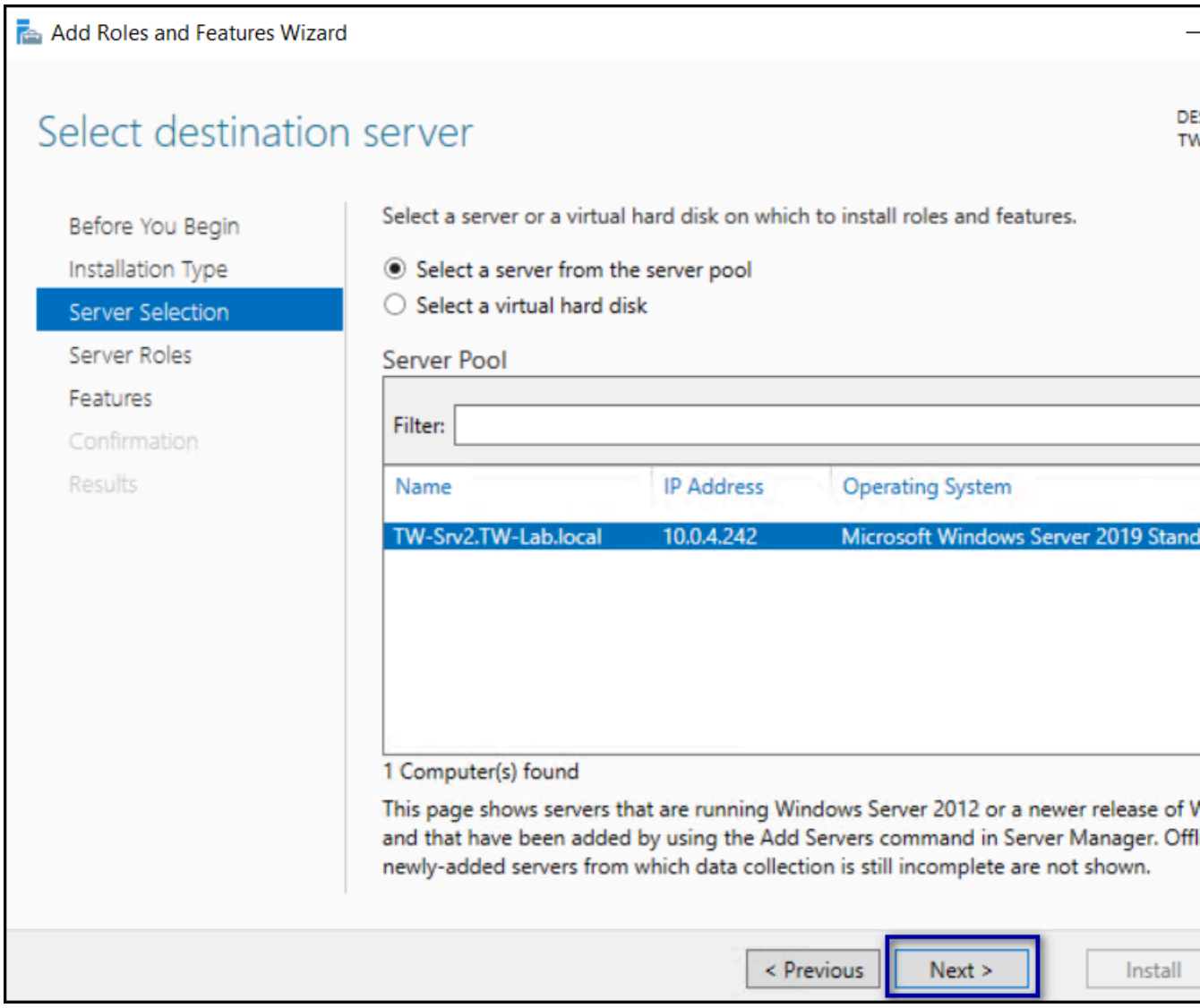


Figure 117: Select Destination Server window

6. On the `Select server roles` window, click **`Next`**, as shown in the following figure.

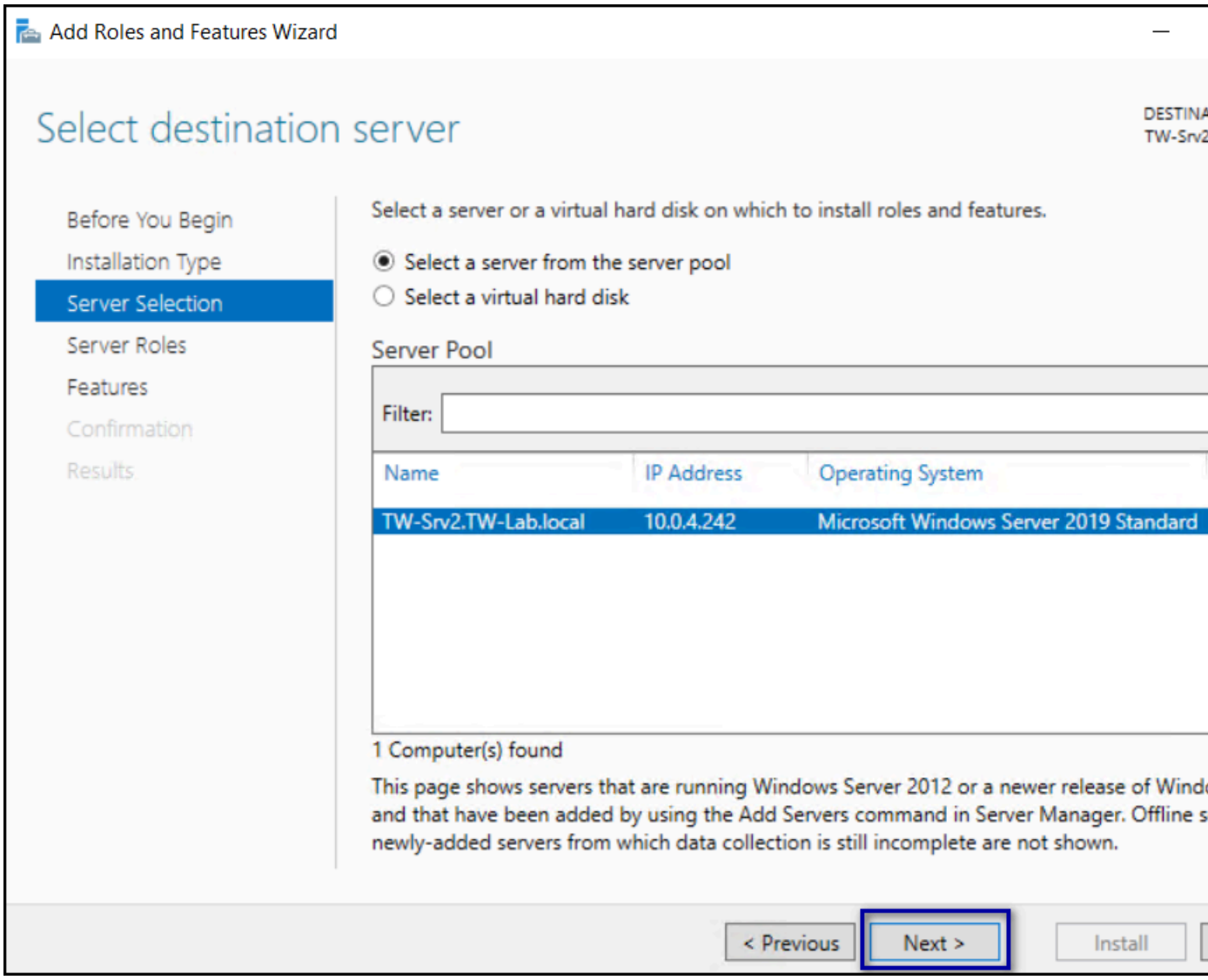


Figure 118: Select Server Roles window

7. On the `Select features` window, expand **`Remote Server Administration Tools > Role Administration Tools > AD DS and AD LDS Tools > AD DS Tools`**, and then select **`Active Directory Administrative Center`**, as shown in the following figure.

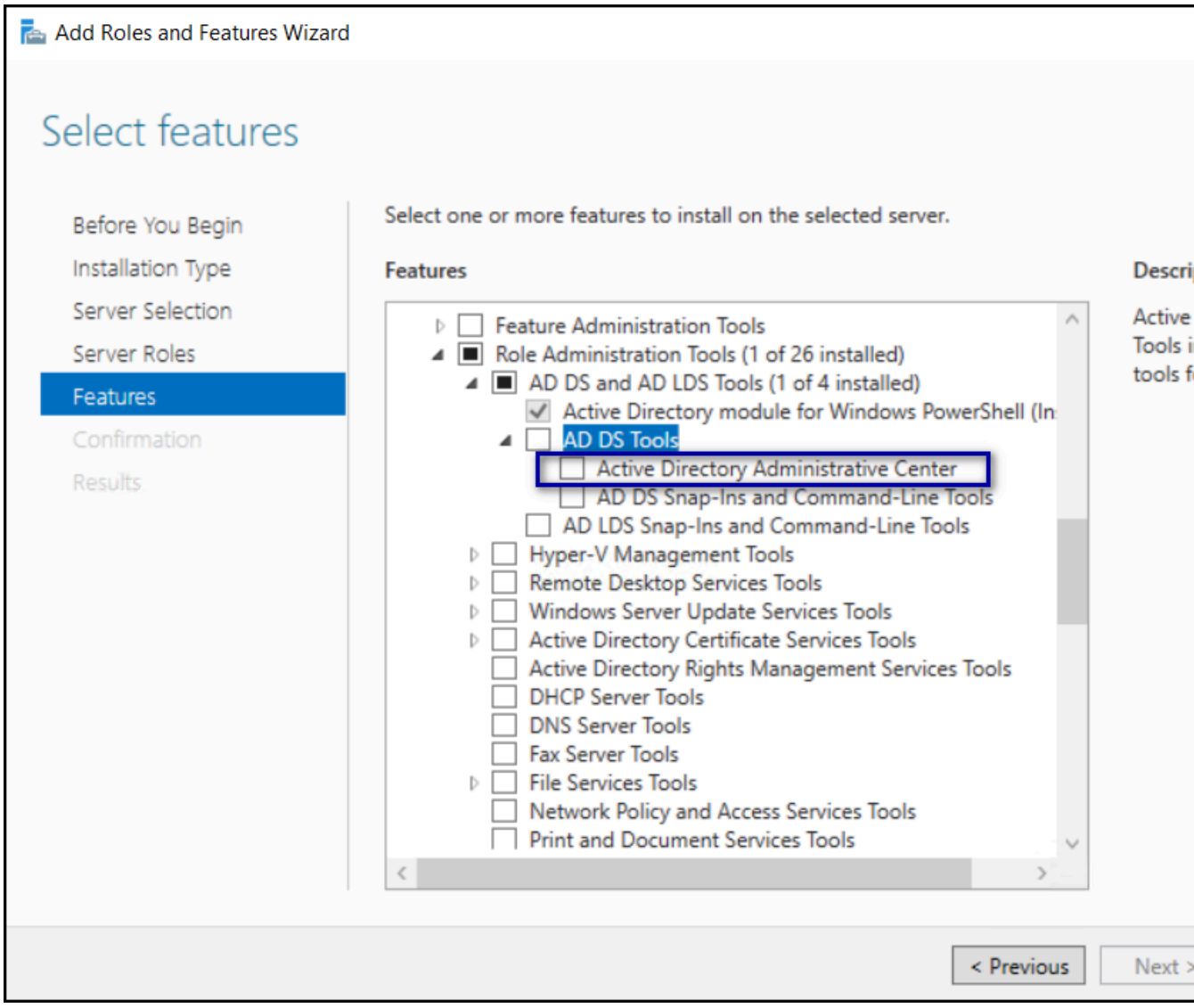


Figure 119: Active Directory Administrative Center option

8. On the `Add features that are required for Active Directory Administrative Center` pop-up, click **`Add features`**, as shown in the following figure.

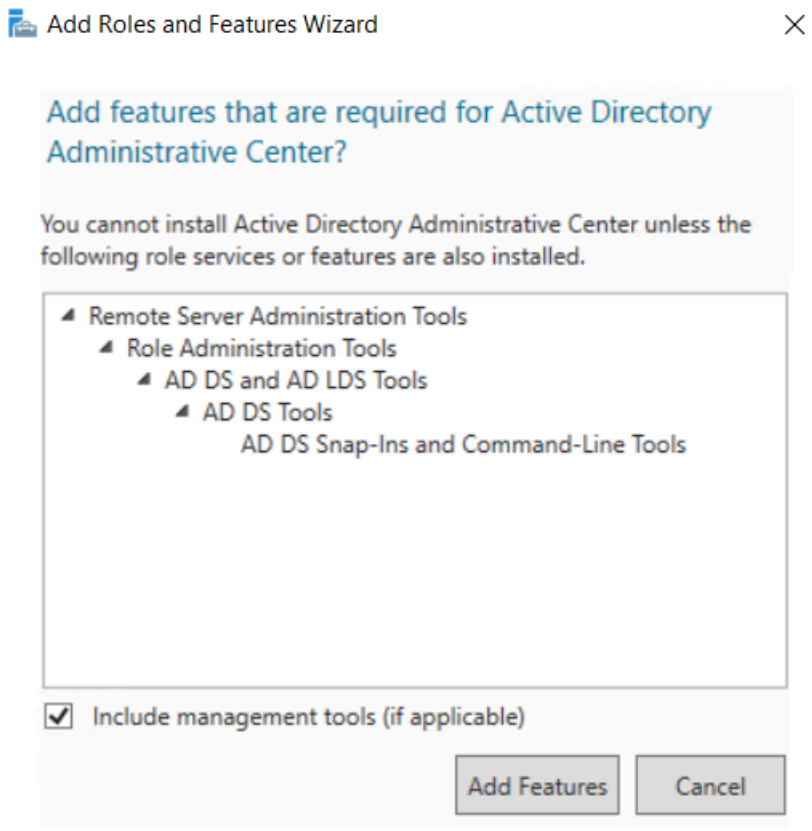


Figure 120: Add features that are required for Active Directory Administrative Center pop-up

9. On the `Select features` window, click **`Next`**, as shown in the following figure.

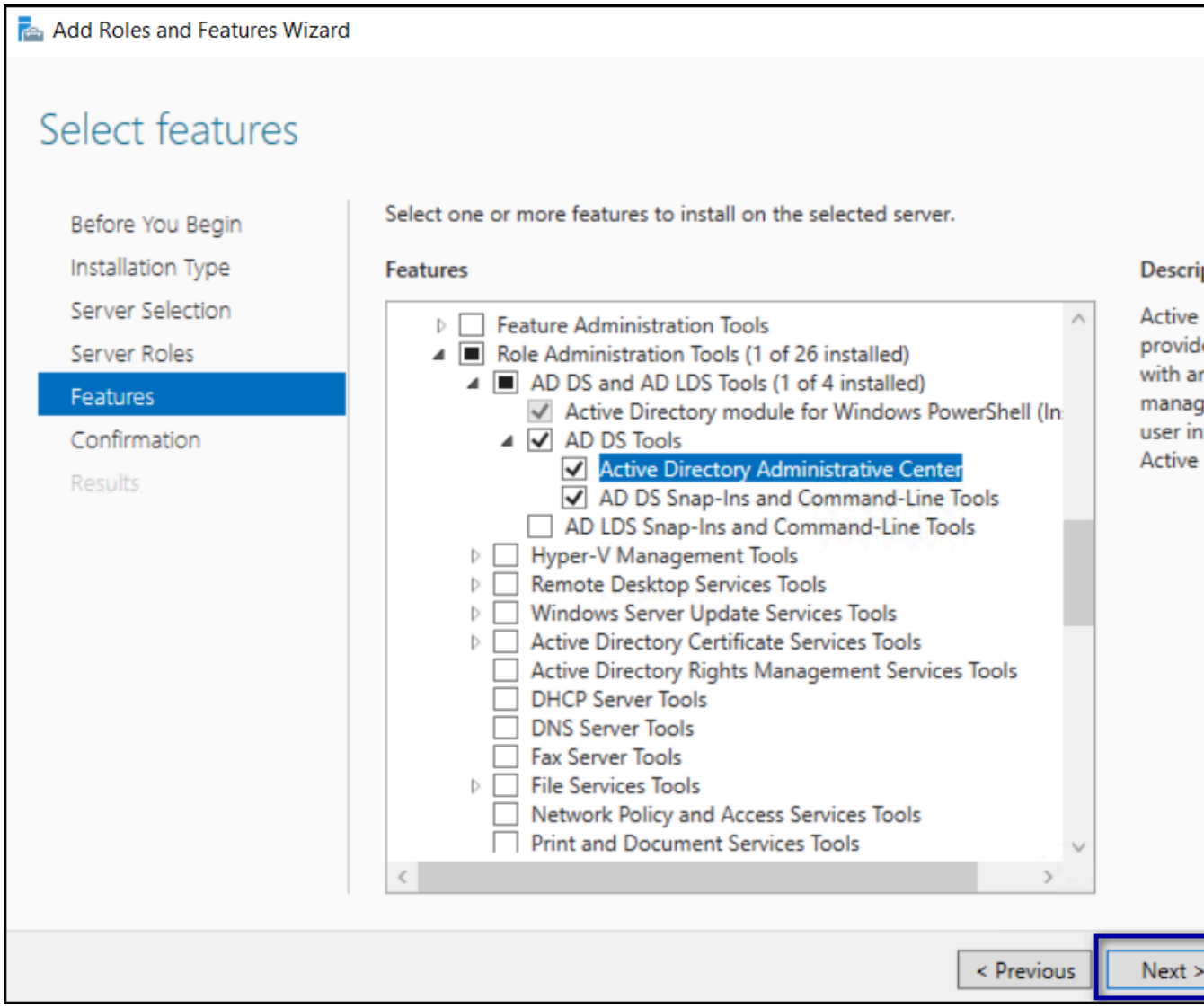


Figure 121: Select Features window

10. On the `Confirm Installation Features` window, click **`Install`**, as shown in the following figure.

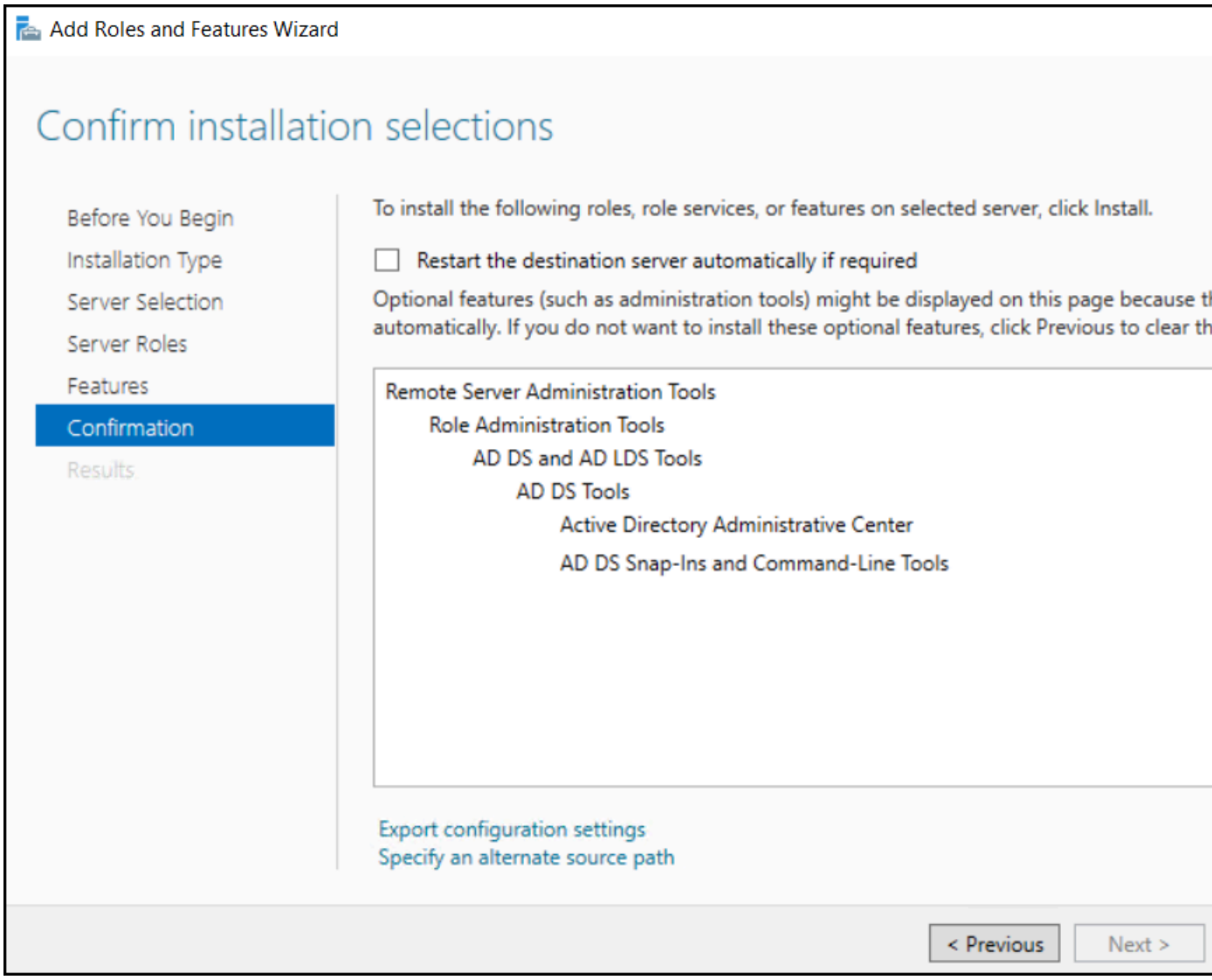


Figure 122: Select Features window

11. When the installation completes, click **`Close`**.

12. Close `Server Manager`.

Testing the LDAP Connection

Use the Microsoft LDP GUI Tool (ldp.exe), which is a component of the AD DS Tools set, to confirm that the environment can establish a connection to LDAPS.

About this task

Perform the following steps on the Evidian EAM Controller.

Procedure

1. Launch *ldp.exe*.
2. From the **`Connection`** menu, select **`Connect`**, as shown in the following figure.

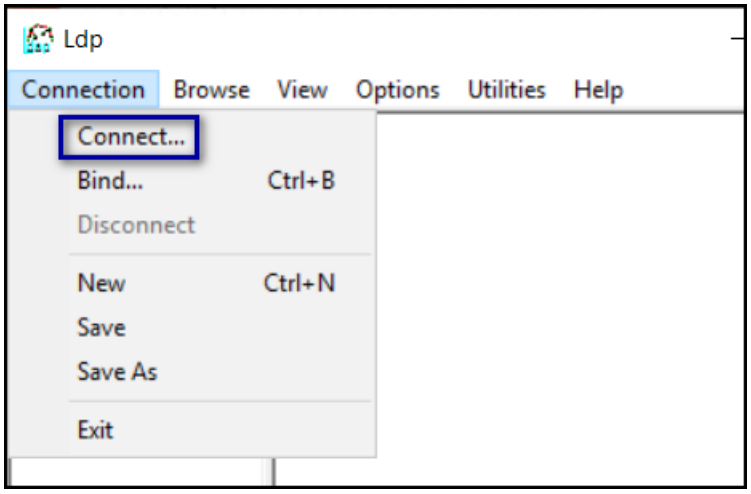


Figure 123: Connect option

3. On the `Connect` window, perform the following actions:
   a) In the **`Server`** field, type ***localhost***.
   b) In the **`Port`** field, change the value to **`55001`**, and then click **`OK`**.

   The following figure provides an example of the `Connect` window.

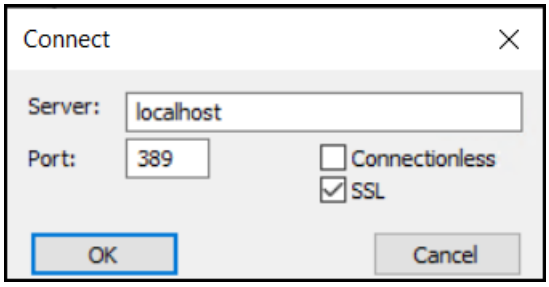


Figure 124: Connect window

4. Click **`OK`**.
   When the command completes successfully, output appears with connection information. When the connection fails, an error message pop-up appears.

   The following figure provides an example of a successful connection.

Figure 125: Successful LDAPS connection results

The following figure provides an example of a failed connection.

Figure 126: Failed LDAPS connection results

7.2.3 - (Wearable mode only) Deploying a Centralized Nymi Agent

Wearable mode environments with users that access applications on Citrix/RDP session hosts require a centralized Nymi Agent.

About this task

On one server in your environment, install the Nymi Agent component of the Nymi Runtime software.

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

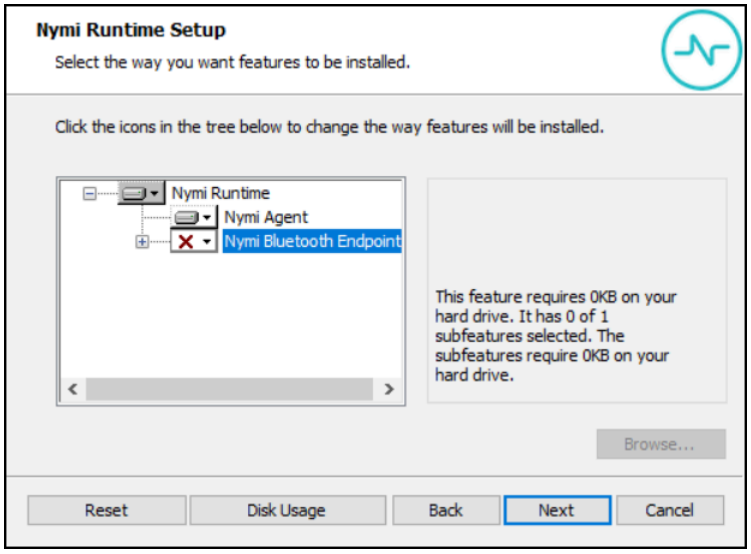


Figure 127: Nymi Bluetooth Endpoint feature is not available

9. On the `Service Account` window, choose **`LocalSystem`** 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.

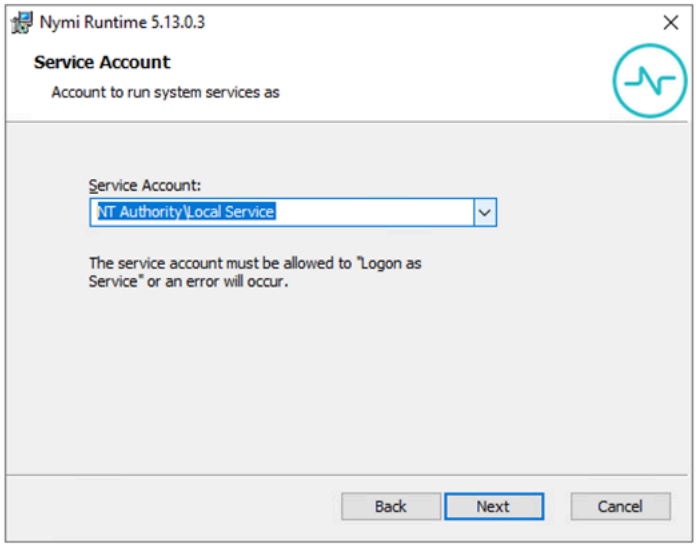


Figure 128: Nymi Runtime Service Account window

10. 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.

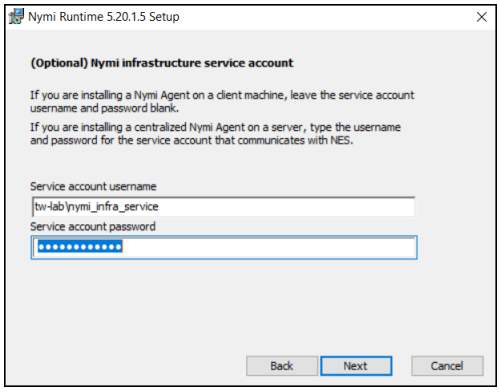


Figure 129: Nymi Infrastructure Service Account window

    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.

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

7.2.3.1 - 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`**.

7.2.3.2 - Configuring the Nymi Agent

A centralized Nymi Agent uses a TOML formatted configuration file to set configuration parameters.

About this task

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 applicable parameter settings and when to use each setting.

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

Parameter and Sample Value	Section Name	Description
log_level = "warn"	[agent]	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	[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"
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.

Parameter and Sample Value	Section Name	Description
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"

Parameter and Sample Value	Section Name	Description
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"
nes_url = "https://server.name.local.com" For example, https://myserver.name.local.com	[nes]	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"	[nes]	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"*

Parameter and Sample Value	Section Name	Description
credentials_location = certs/	[nes]	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.

4. For secure Nymi Agent, 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
5. Restart the **`Nymi Agent`** service.

7.3 - Installing and Configuring Software on the Nymi Band Application Terminal

The enrollment terminal is the machine that you use to enroll Nymi Bands. This machine requires a connected Nymi-supplied Bluetooth adapter.

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.

7.3.1 - 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.

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.

Decentralized Enrollment Terminal

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

7.3.1.1 - 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`**.

7.3.1.2 - Deploy a Centralized Enrollment Terminal

When you deploy a centralized enrollment terminal, you install the Nymi Band Application and Evidian software 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.

Configuring the Evidian EAM Client

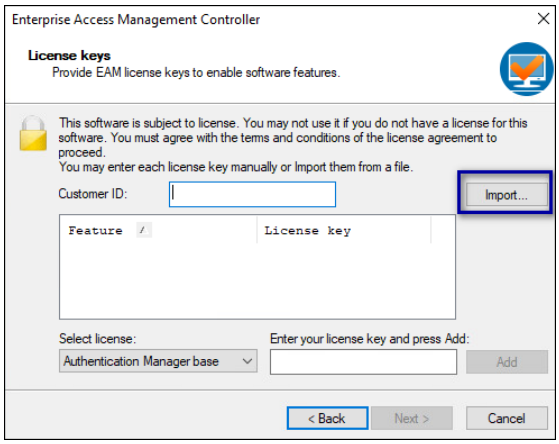
Configure the Evidian EAM Client settings the Citrix/RDP server assigned as the enrollment terminal.

Before you begin

- Complete the steps to configure the Evidian EAM Controller.
- Ensure that the machine is on the same domain as the Evidian EAM Controller.
- Obtain the Evidian license file from the Nymi Solution Consultant.

Procedure

1. Log in to the machine with an account that has Local Administrator access.
2. Download and extract the Evidian software package, *EAM-v10.0x.xxxxxxx.zip* to a directory on the host, for example, the *Downloads* directory.
3. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\Tools\WGConfig\WGConfig.exe* file.
4. On the `User Access Control` window, click **`Yes`**.
5. On the `Welcome to the Configuration Assistant` window, click **`Next`**.
6. If the required Microsoft Visual C++ Redistributable software is not installed on the server, the `Prerequisites` window appears. Click **`Next`** to install the software.
   The Windows Installer window appears.
7. On the `License keys` window, click **`Import`**, as shown in the following figure.



8. In the `Open` window, select the license file in the *Downloads* directory, and the click **`Open`**.

   If you do not see the file, select **`All Files *.*`** from the file type list.

9. On the `Installation mode` window, leave the default option **`with a controller`** selected, and then click **`Next`**.

   The following figure provides an example of the `Installation mode` window.

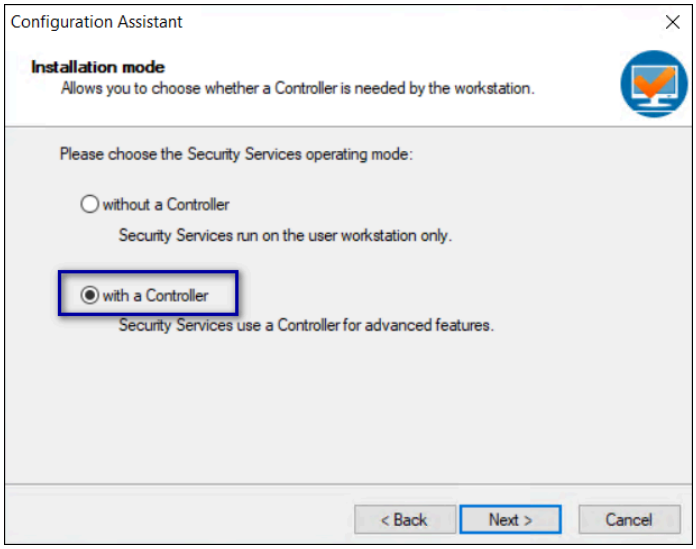


Figure 130: Installation mode window

10. On the `Users directory` window, leave the default option **`Microsoft Active Directory`** selected, and then click **`Next`**.

    The following figure provides an example of the `Users directory` window.

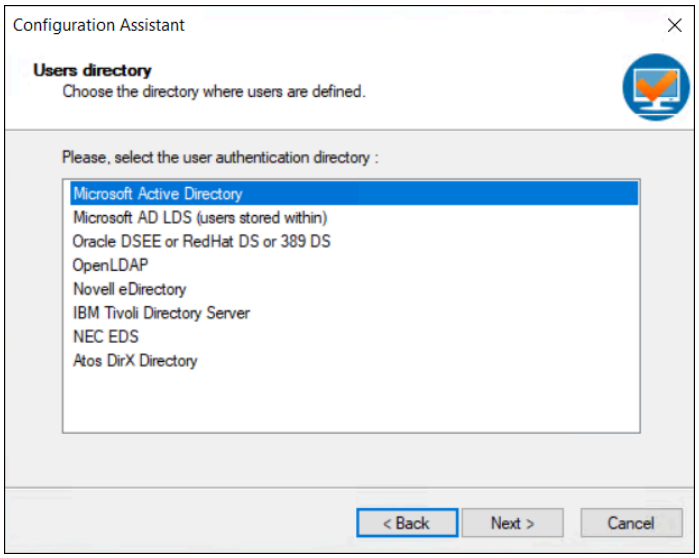


Figure 131: Users directory window

11. On the `Security repository` window, select the option **`Integrated with AD LDS: the security data is stored in an AD LDS server`**, and then click **`Next`**.

    The following figure provides an example of the `Security repository` window.

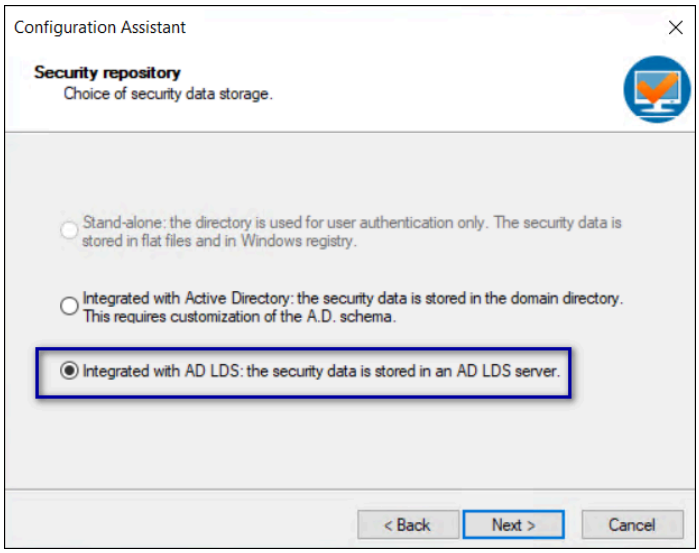


Figure 132: Security repository window

12. On the `LDAP Configuration` window, perform the following action:

    a) In the **`Name/address`** field, type the FQDN of the Evidian EAM Controller, and in the **`Port`** field, type ***55000***.

    b) Click **`Add`**.

    c) Leave the default option **`Use a dedicated naming context for the Evidian Enterprise Access Management data`** selected, and then in the **`Evidian Enterprise Access Management data context`** field, type ***O=EAM***.

    The following figure provides an example of the `LDAP Configuration` window.

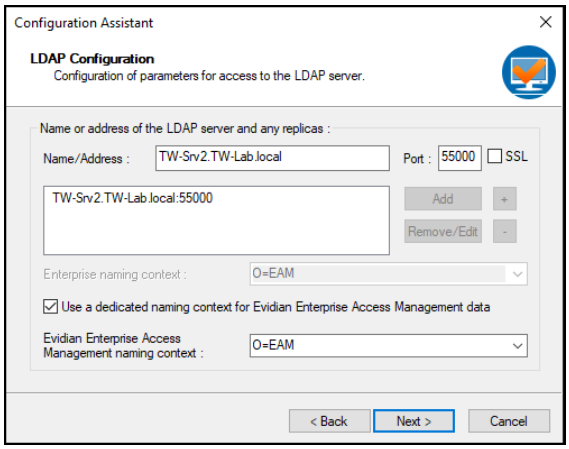


Figure 133: LDAP Configuration

d) Click **Next**.

13. On the Access-point management window, select **Manage access points**, as shown in the following figure, and then click **Next**.

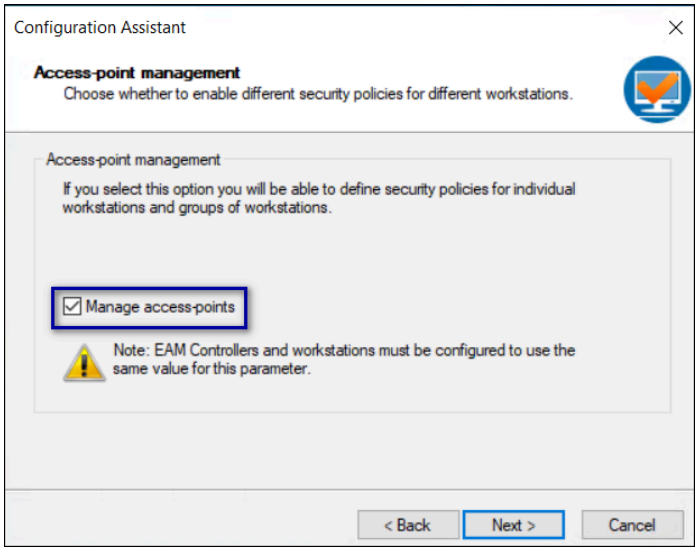


Figure 134: Access-point management window

14. On the Restart Computer window, leave the default selection **Do not restart the computer**, as shown in the following figure, and the click **Finish**.

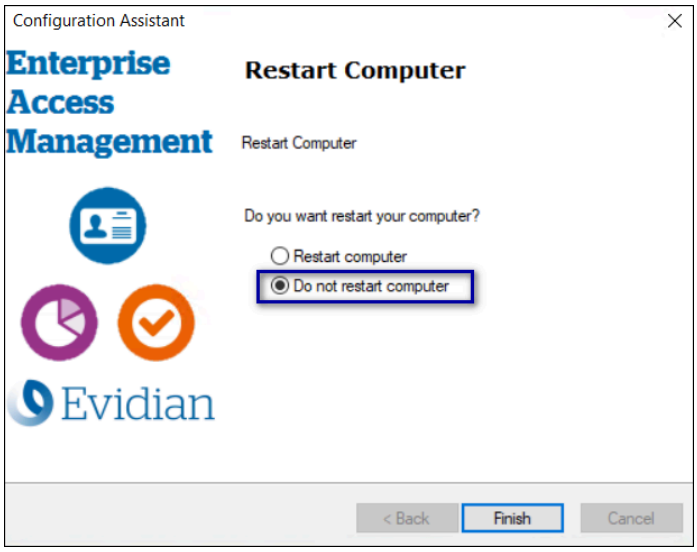


Figure 135: Restart Computer window

15.

Installing the Evidian EAM Client

The Evidian EAM Client installation software provides you with the ability to install required and optional features such as Authentication Manager, the Evidian SSO Engine, the Evidian EAM Management Console and language support. Install the Evidian SSO Agent on the Citrix/ RDP session host assigned as the enrollment terminal.

Before you begin

- Complete the steps to configure the Evidian EAM Controller.
- Determine the Nymi Band use cases. To use the Nymi Band to unlock user terminals, you will configure the Evidian EAM Client with Authentication Manager. To use the Nymi Band for SSO activities only, you will configure the Evidian EAM Client with Windows Login only.

About this task

You do not require Evidian SSO Agent on thin client user terminals.

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\VCRedist_x64.msi*.

   Note: If the required version of Microsoft Visual C++ redistributable is already installed on the server, a pop-up screen briefly appears, and then disappears.
2. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\ESSOAgent.msi* file.
3. On the `Enterprise Access Management Client Installation`, click **`Next`**.
4. On the `License Agreement` window, click **`I accept the license agreement`**, and then click **`Next`**.

The following figure shows the `License Agreement` window.

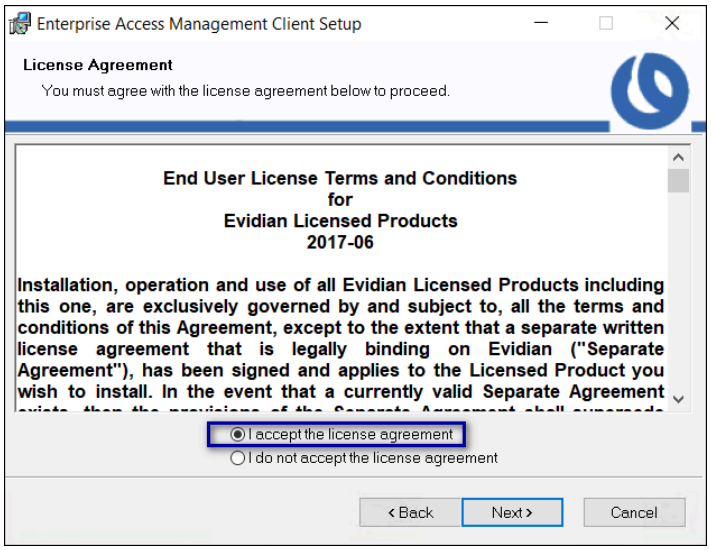


Figure 136: License Agreement window

5. On the `Destination Folder` window, accept the default, and then click **`Next`**.

   The following figure shows the `Destination Folder` window.

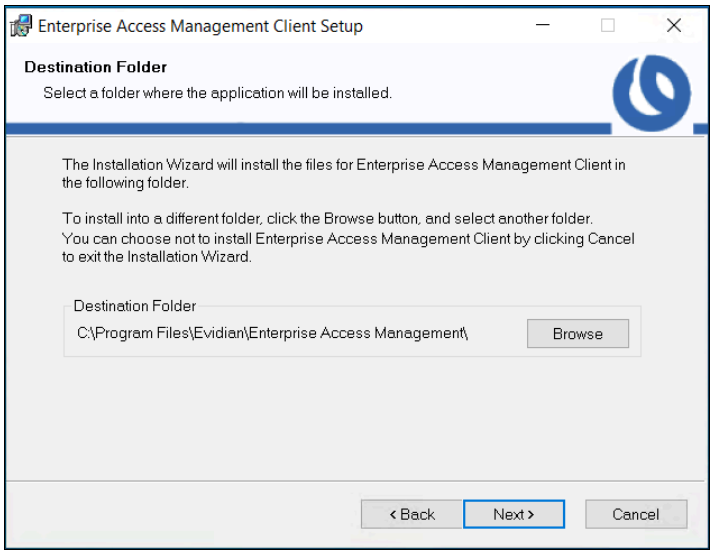


Figure 137: Destination Folder window

6. On the `Select Installation Type` window, select **`Custom`**, and then click **`Next`**.

   The following figure shows the `Select Installation Type` window.

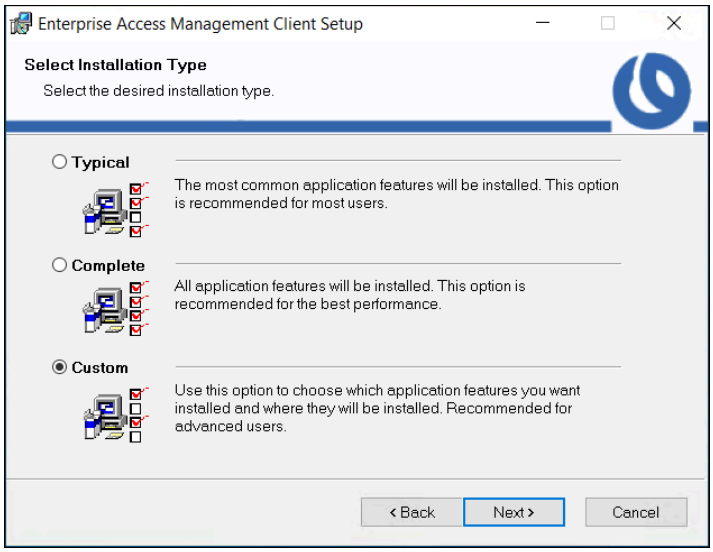
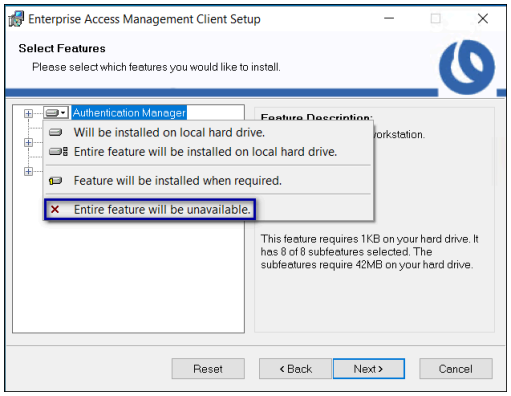
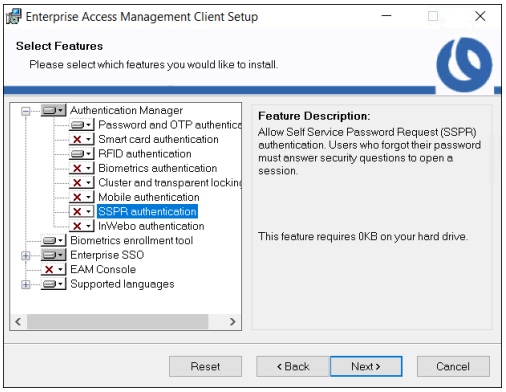


Figure 138: Select Installation Type window

7. On the `Select features` window, for **`Authentication Manager`** perform one of the following actions based on your Nymi Band use case:

   Note: Unless otherwise noted, leave the default option for a feature.

Option	Description
Do not use the Nymi Band to log into terminal.	Select **`Authentication Manager`**, and then select **`Entire feature will be unavailable`**. 
Use the Nymi Band to log into terminal	Expand **`Authentication Manager`**. For each of the following features: • Smart card authentication • Biometrics authentication • Cluster and transparency • Mobile authentication • SSPR authentication • InWebo authentication

Option	Description
	Select the feature, and then select **Entire feature will be unavailable**, as shown in the following figure.  The only features to install are **Password and OTP authentication** and **RFID authentication**.

8. Click **Biometric enrollment tool**, and then select **Entire feature will be unavailable**, as shown in the following figure.

   The following figure shows the `Select Features` window.

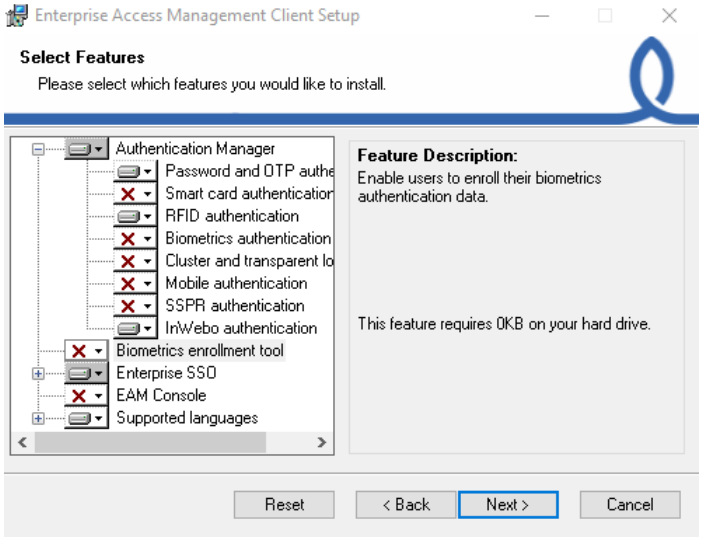


Figure 139: Select Features - Authentication Manager options and without Biometric enrollment tool

9. If you removed the **Authentication Manager** feature, and want the SSO Login window to open with the username of the user that logged into Windows, select **Integrate with Windows**, and then select **Entire feature will be installed on local hard drive**, as shown in the following figure.

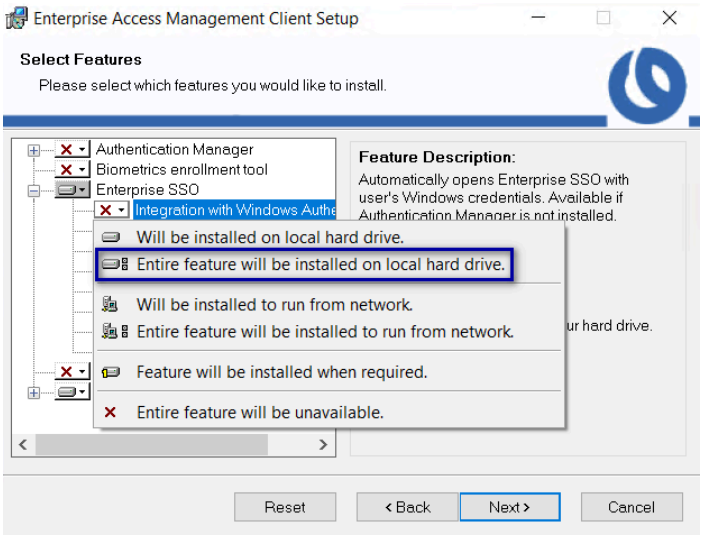
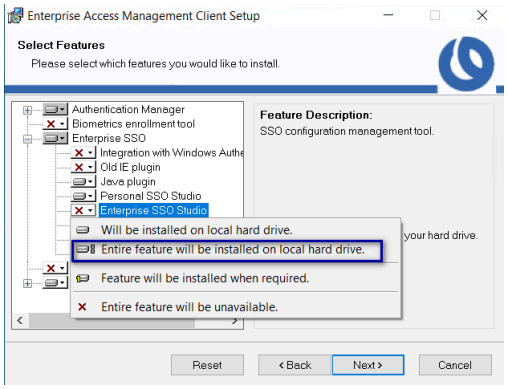
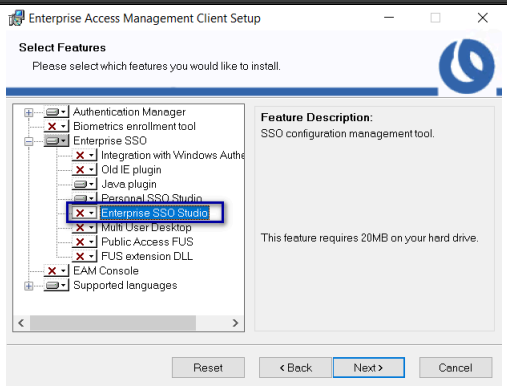
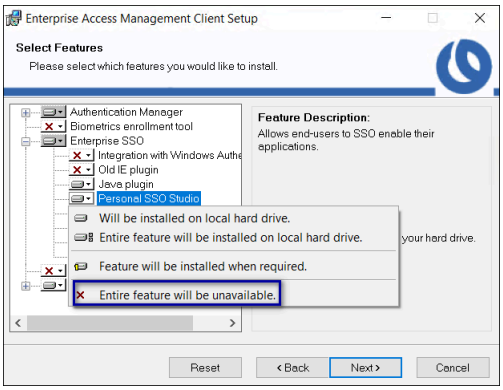


Figure 140: Integrate with Windows

10. For **`Enterprise SSO`**, perform one of the following actions based on your Nymi Band use case:

Note: Unless otherwise noted, leave the default option for a feature.

Option	Description
Use the Nymi Band for SSO	Click **`Enterprise SSO Studio`**, and then select **`Entire feature will be installed on local hard drive`**, as shown in the following figure. 
Use the Nymi Band for Windows login only	Leave the default **`Enterprise SSO`** configuration, as shown in the following figure.

Option	Description
	
All use cases	Click **`Personal SSO Studio`**, and then select **`Entire feature will be unavailable`**, as shown in the following figure. 

11. Select **`EAM Console`**, and then select **`Entire feature will be installed on local hard drive`**, as shown in the following figure.

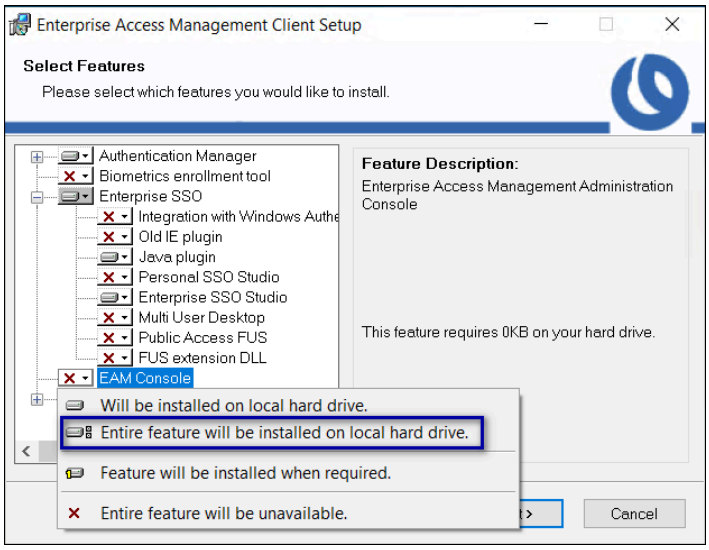


Figure 141: Install EAM Console Feature

12. Click **`Next`**.
13. On the `Ready to install the application` window, click **`Next`**, as shown in the following figure.

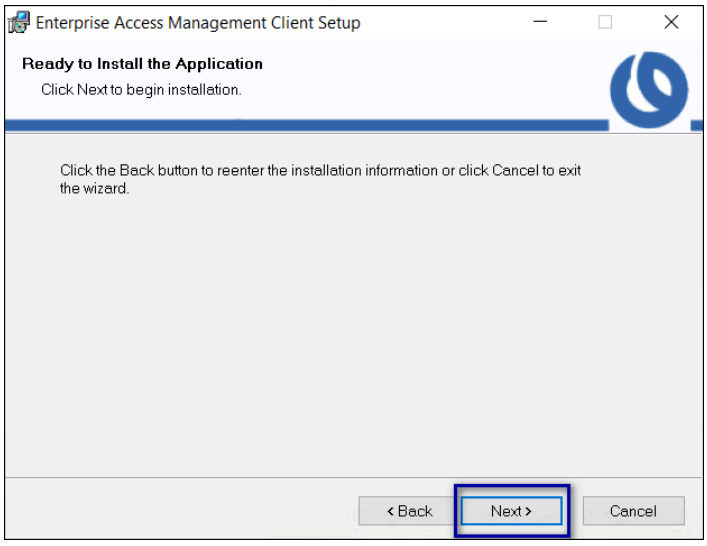


Figure 142: Ready to install the application

14. On the `User account control` pop-up, click **`Yes`**, as shown in the following figure.

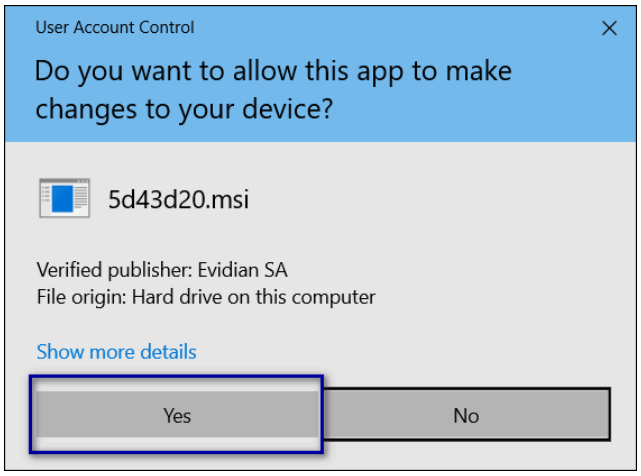


Figure 143: User account control

15. On the `Enterprise Access Management Client has been successfully installed` window, click **`Finish`**, as shown in the following figure.

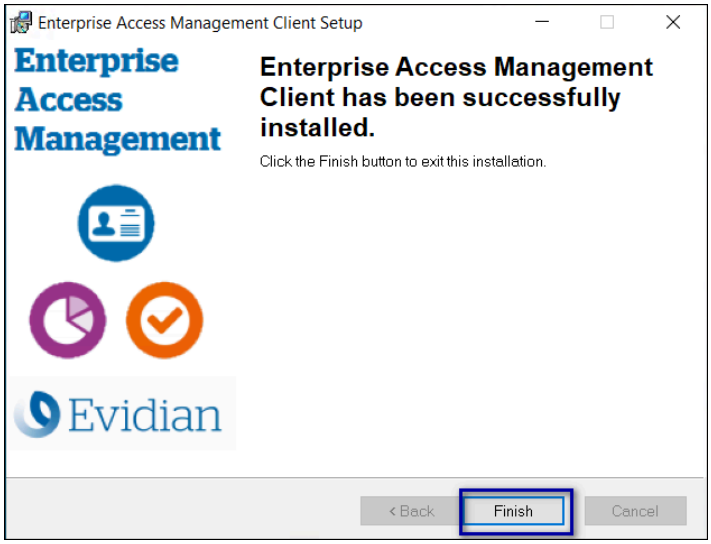


Figure 144: Evidian Client Installation Success window

16. In the Windows System Tray, click on the Enterprise SSO (eSSO) icon.
17. Click the **`Home`** icon, and then click **`Refresh`**, as shown in the following figure.

    The Evidian EAM Client contacts the Evidian EAM Controller to retrieve new technical definitions.

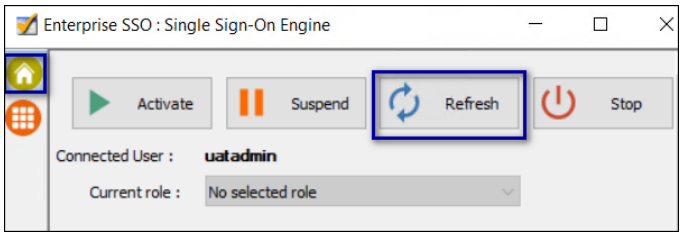


Figure 145: eSSO application Home Window

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`**.

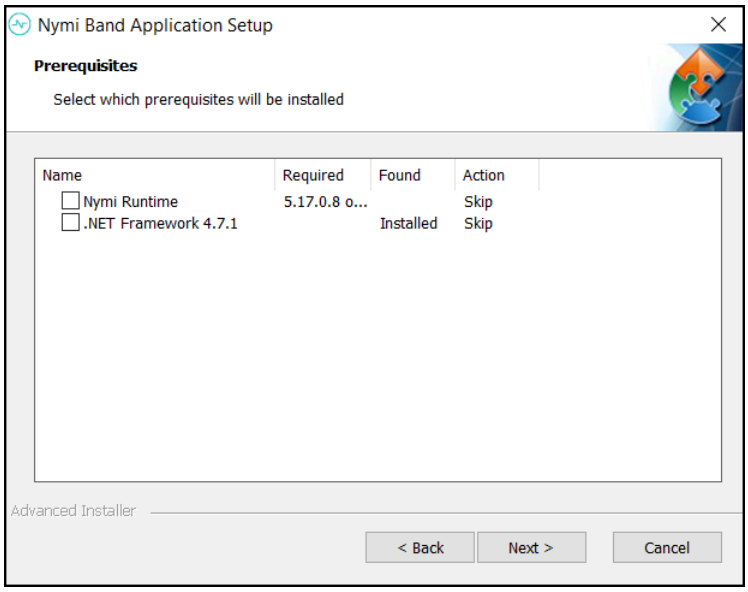


Figure 146: No Nymi Runtime Installation

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://agent_server:agent_port/socket/websocket`

   where:

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

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

7.3.1.3 - Deploy a Decentralized Enrollment Terminal

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

Configuring the Evidian EAM Client

Configure the Evidian EAM Client settings on each thick client user terminal, the NBA terminal, and Citrix/RDP session host.

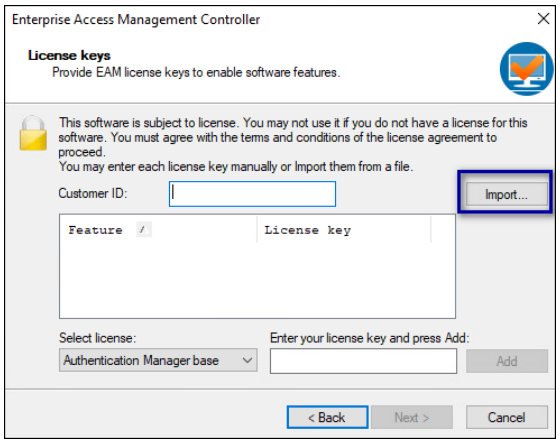
Before you begin

- Complete the steps to configure the Evidian EAM Controller.
- Ensure that the machine is on the same domain as the Evidian EAM Controller.
- Obtain the Evidian license file from the Nymi Solution Consultant.

Procedure

1. Log in to the machine with an account that has Local Administrator access.

2. Download and extract the Evidian software package, *EAM-v10.0x.xxxxxxx.zip* to a directory on the host, for example, the *Downloads* directory.
3. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\Tools\WGConfig \WGConfig.exe* file.
4. On the `User Access Control` window, click **`Yes`**.
5. On the `Welcome to the Configuration Assistant` window, click **`Next`**.
6. If the required Microsoft Visual C++ Redistributable software is not installed on the server, the `Prerequisites` window appears. Click **`Next`** to install the software.
   The Windows Installer window appears.
7. On the `License keys` window, click **`Import`**, as shown in the following figure.



8. In the `Open` window, select the license file in the *Downloads* directory, and the click **`Open`**.
   If you do not see the file, select **`All Files *.*`** from the file type list.
9. On the `Installation mode` window, leave the default option **`with a controller`** selected, and then click **`Next`**.
   The following figure provides an example of the `Installation mode` window.

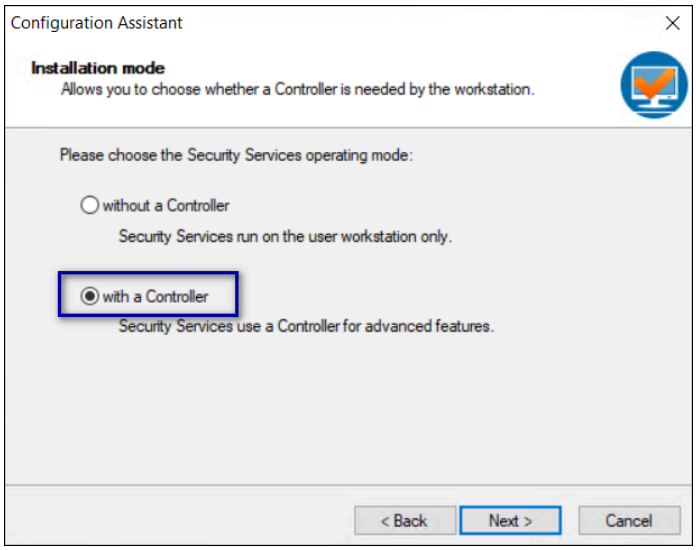


Figure 147: Installation mode window

10. On the `Users directory` window, leave the default option **`Microsoft Active Directory`** selected, and then click **`Next`**.

    The following figure provides an example of the `Users directory` window.

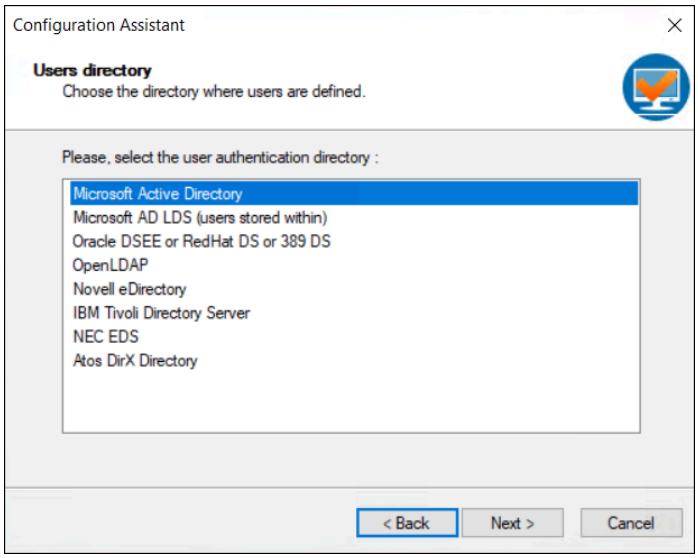


Figure 148: Users directory window

11. On the `Security repository` window, select the option **`Integrated with AD LDS: the security data is stored in an AD LDS server`**, and then click **`Next`**.

    The following figure provides an example of the `Security repository` window.

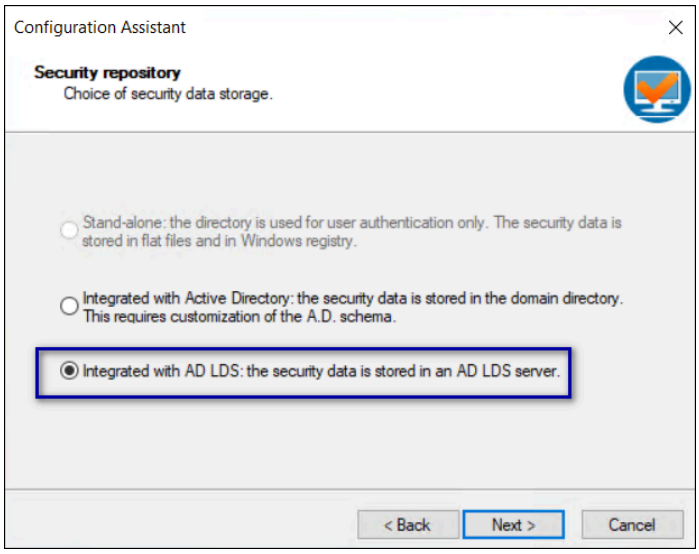


Figure 149: Security repository window

12. On the LDAP `Configuration` window, perform the following action:

a) In the **`Name/address`** field, type the FQDN of the Evidian EAM Controller, and in the **`Port`** field, type ***55000***.

b) Click **`Add`**.

c) Leave the default option **`Use a dedicated naming context for the Evidian Enterprise Access Management data`** selected, and then in the **`Evidian Enterprise Access Management data context`** field, type ***O=EAM***.

The following figure provides an example of the LDAP `Configuration` window.

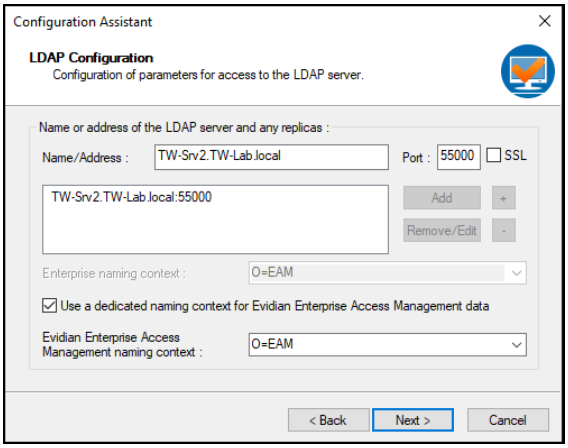


Figure 150: LDAP Configuration

d) Click **`Next`**.

13. On the `Access-point management` window, select **`Manage access points`**, as shown in the following figure, and then click **`Next`**.

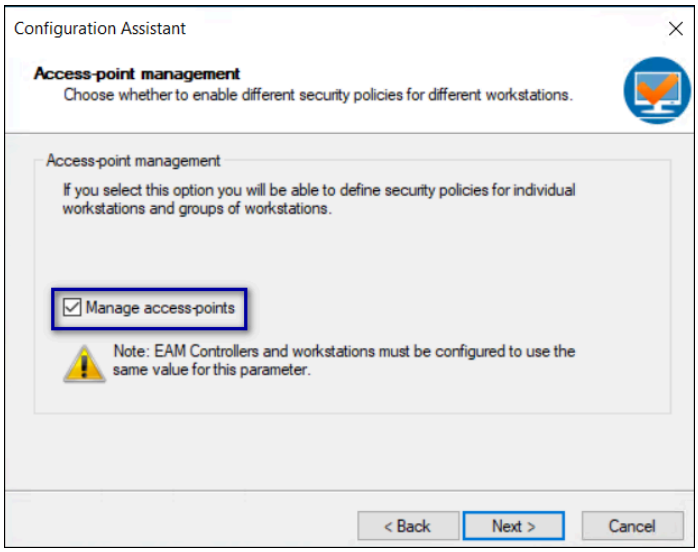


Figure 151: Access-point management window

14. On the `Restart Computer` window, leave the default selection **`Do not restart the computer`**, as shown in the following figure, and the click **`Finish`**.

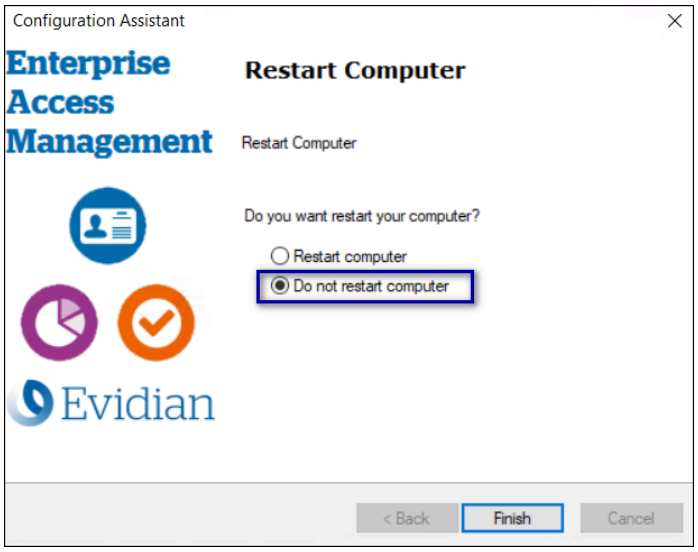


Figure 152: Restart Computer window

15.

Installing the Evidian EAM Client

The Evidian EAM Client installation software provides you with the ability to install required and optional features such as Authentication Manager, the Evidian SSO Engine, the Evidian EAM Management Console and language support. Install the Evidian SSO Agent on the thick client assigned as the enrollment terminal.

Before you begin

- Complete the steps to configure the Evidian EAM Controller.
- Determine the Nymi Band use cases. To use the Nymi Band to unlock user terminals, you will configure the Evidian EAM Client with Authentication Manager. To use the Nymi Band for SSO activities only, you will configure the Evidian EAM Client with Windows Login only.

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\VCRedist_x64.msi*.

   Note: If the required version of Microsoft Visual C++ redistributable is already installed on the server, a pop-up screen briefly appears, and then disappears.
2. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\ESSOAgent.msi* file.
3. On the `Enterprise Access Management Client Installation`, click **`Next`**.
4. On the `License Agreement` window, click **`I accept the license agreement`**, and then click **`Next`**.

   The following figure shows the `License Agreement` window.

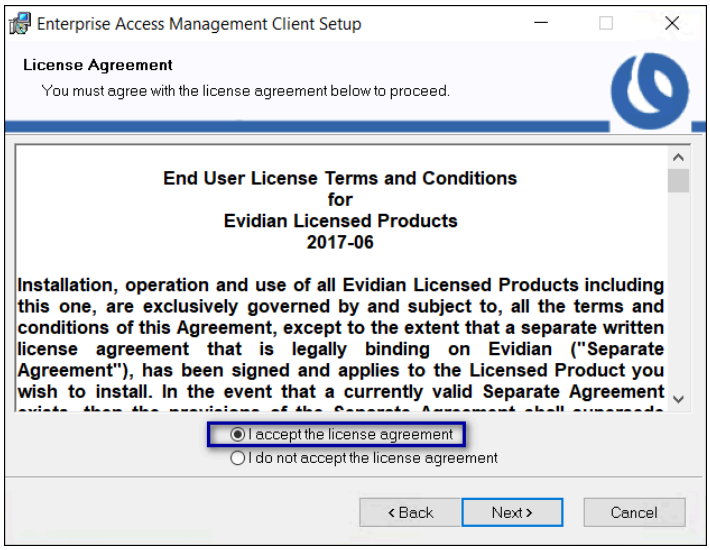


Figure 153: License Agreement window

5. On the `Destination Folder` window, accept the default, and then click **`Next`**.

   The following figure shows the `Destination Folder` window.

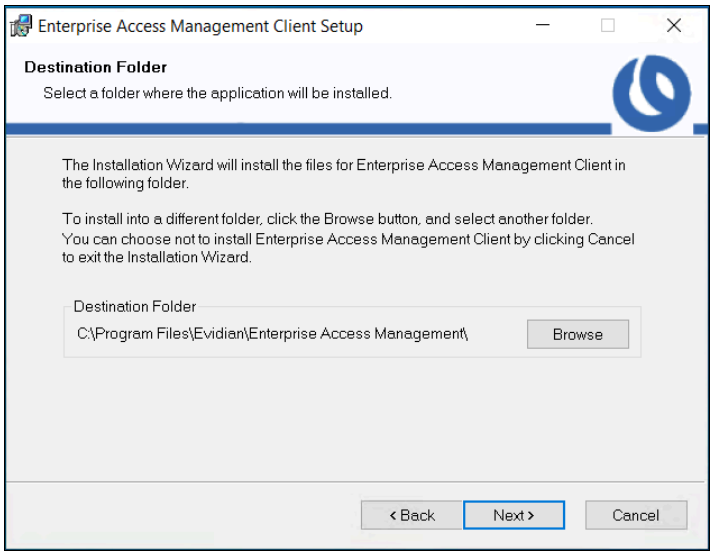


Figure 154: Destination Folder window

6. On the `Select Installation Type` window, select **`Custom`**, and then click **`Next`**.

   The following figure shows the `Select Installation Type` window.

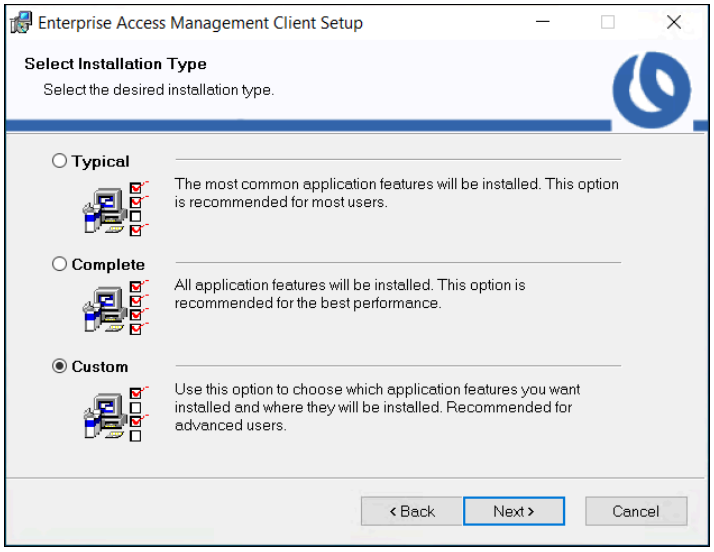
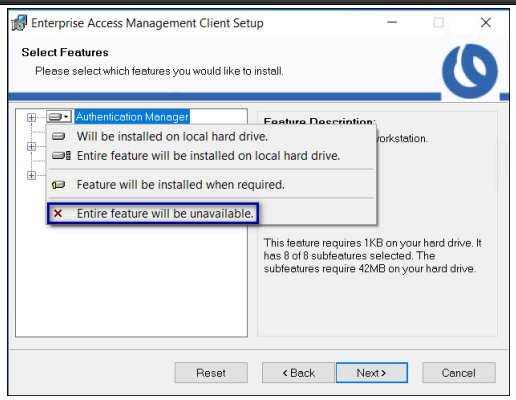
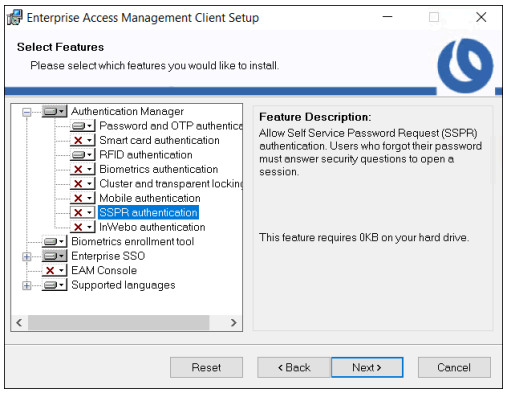


Figure 155: Select Installation Type window

7. On the `Select features` window, for **`Authentication Manager`** perform one of the following actions based on your Nymi Band use case:

   Note: Unless otherwise noted, leave the default option for a feature.

Option	Description
Do not use the Nymi Band to log into terminal.	Select **`Authentication Manager`**, and then select **`Entire feature will be unavailable`**.

Option	Description
	
Use the Nymi Band to log into terminal	Expand **`Authentication Manager`**. For each of the following features: • Smart card authentication • Biometrics authentication • Cluster and transparency • Mobile authentication • SSPR authentication • InWebo authentication Select the feature, and then select **`Entire feature will be unavailable`**, as shown in the following figure.  The only features to install are **`Password and OTP authentication`** and **`RFID authentication`**.

8. Click **`Biometric enrollment tool`**, and then select **`Entire feature will be unavailable`**, as shown in the following figure.

   The following figure shows the `Select Features` window.

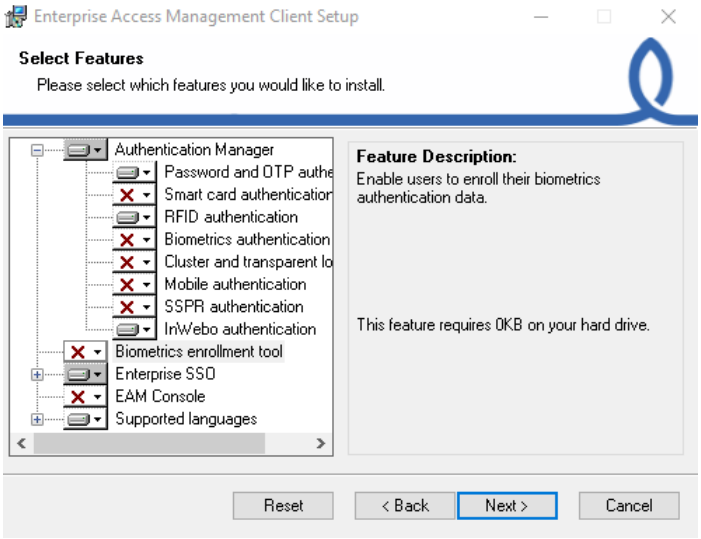


Figure 156: Select Features - Authentication Manager options and without Biometric enrollment tool

9. If you removed the **`Authentication Manager`** feature, and want the SSO Login window to open with the username of the user that logged into Windows, select **`Integrate with Windows`**, and then select **`Entire feature will be installed on local hard drive`**, as shown in the following figure.

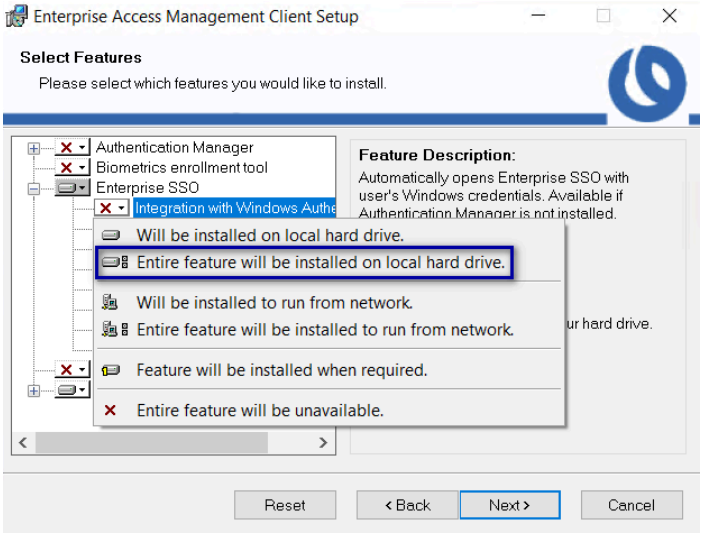
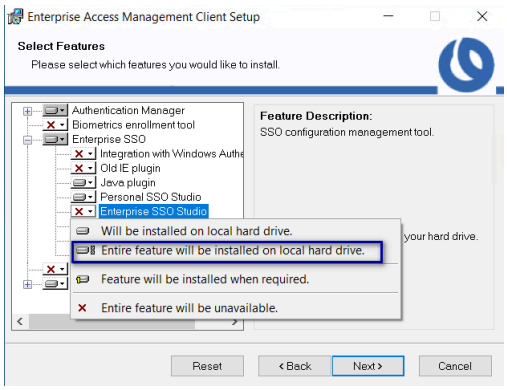
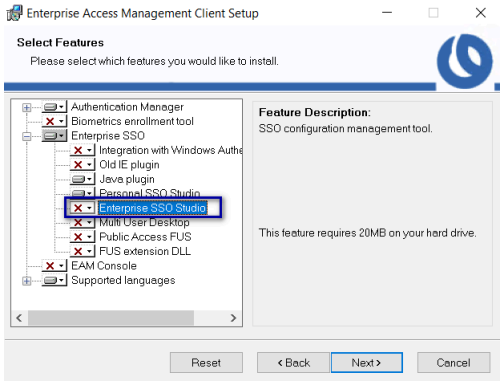
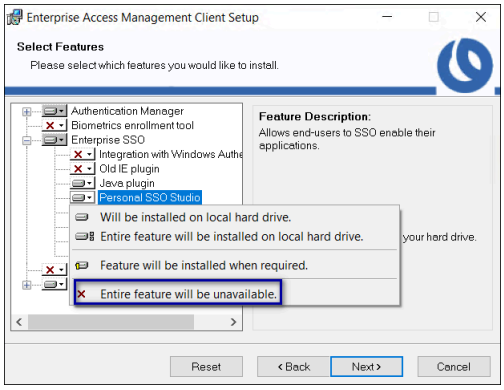


Figure 157: Integrate with Windows

10. For **`Enterprise SSO`**, perform one of the following actions based on your Nymi Band use case:

Note: Unless otherwise noted, leave the default option for a feature.

Option	Description
Use the Nymi Band for SSO	Click **`Enterprise SSO Studio`**, and then select **`Entire feature will be`**

Option	Description
	`installed on local hard drive`, as shown in the following figure. 
Use the Nymi Band for Windows login only	Leave the default **`Enterprise SSO`** configuration, as shown in the following figure. 
All use cases	Click **`Personal SSO Studio`**, and then select **`Entire feature will be unavailable`**, as shown in the following figure. 

11. Select **`EAM Console`**, and then select **`Entire feature will be installed on local hard drive`**, as shown in the following figure.

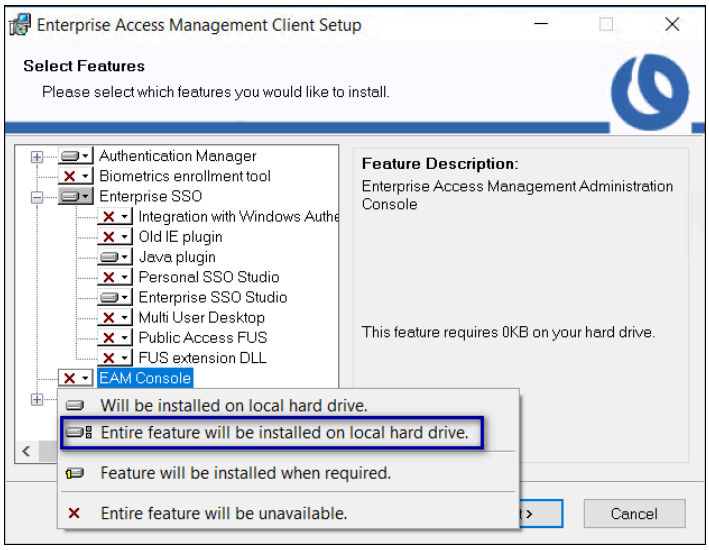


Figure 158: Install EAM Console Feature

12. Click **`Next`**.
13. On the `Ready to install the application` window, click **`Next`**, as shown in the following figure.

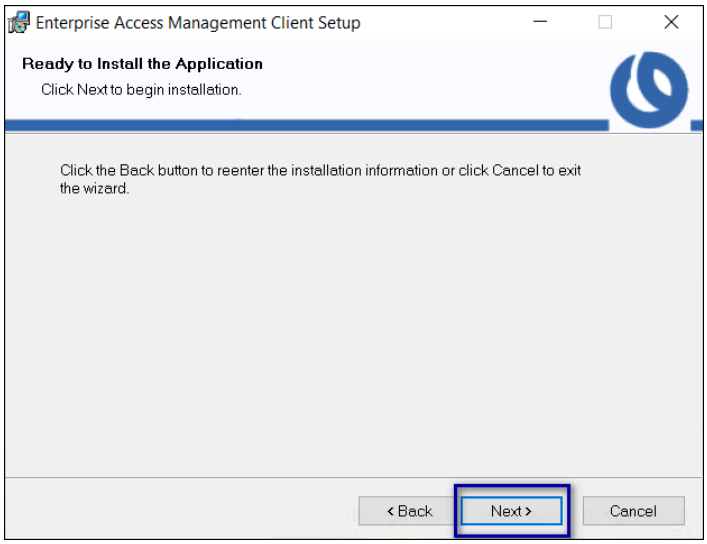


Figure 159: Ready to install the application

14. On the `User account control` pop-up, click **`Yes`**, as shown in the following figure.

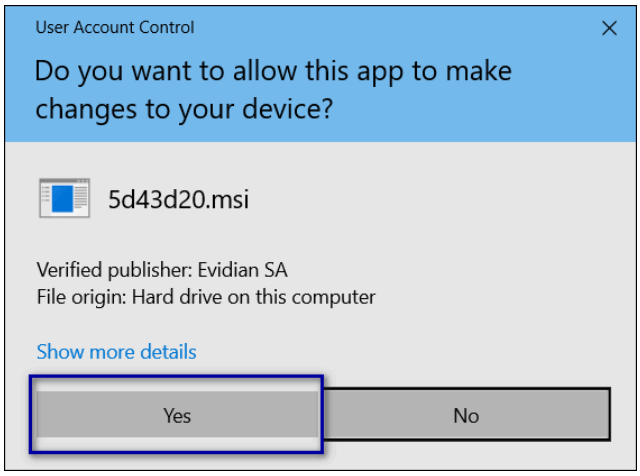


Figure 160: User account control

15. On the `Enterprise Access Management Client has been successfully installed` window, click **`Finish`**, as shown in the following figure.

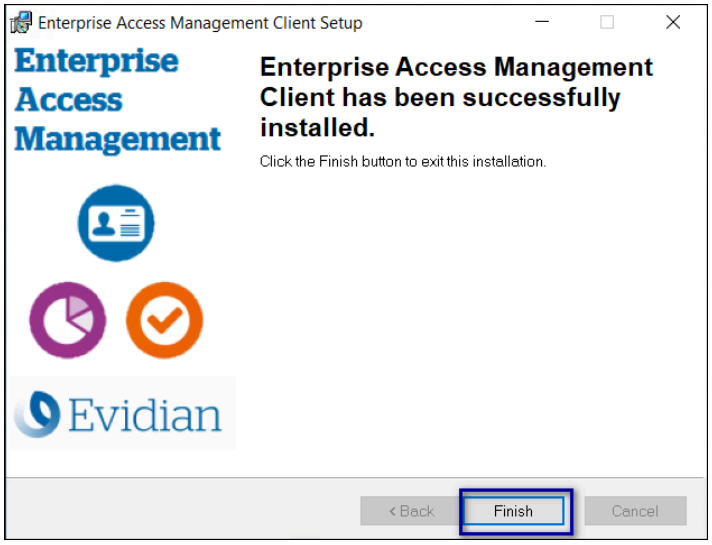


Figure 161: Evidian Client Installation Success window

16. In the Windows System Tray, click on the Enterprise SSO (eSSO) icon.
17. Click the **`Home`** icon, and then click **`Refresh`**, as shown in the following figure.

    The Evidian EAM Client contacts the Evidian EAM Controller to retrieve new technical definitions.

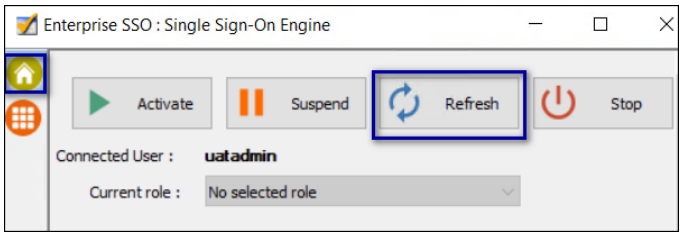


Figure 162: eSSO application Home Window

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\LocalService, 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.

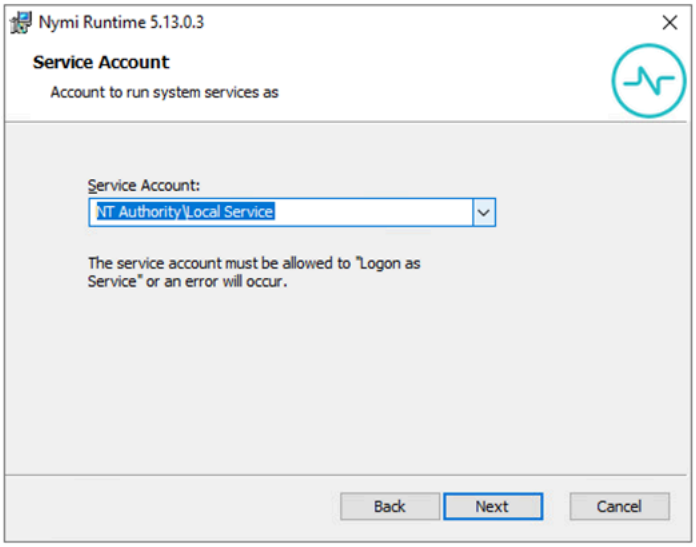


Figure 163: Nymi Runtime Service Account window

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.

7.3.1.4 - 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.

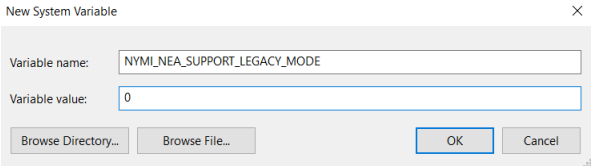


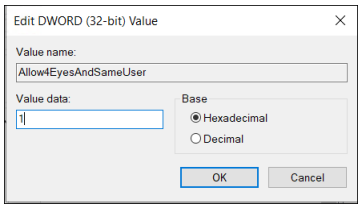
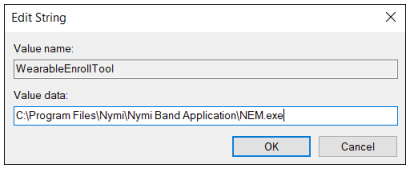
Figure 164: New System Variable window

   c) Click **OK**.

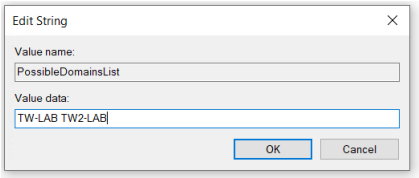
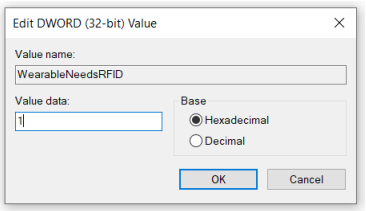
7.3.2 - Defining EAM Registry Keys on the Enrollment Terminal

The Nymi with Evidian Solution requires several registry keys on the Evidian EAM Clients to configure features and optimize performance.

Purpose	Affected Components	Registry Setting
Required Registry Key Settings for the Nymi with Evidian solution		
Enable the Evidian EAM Client to connect to Nymi Enterprise Server(NES)	All Evidian EAM Clients, including Citrix/RDP servers.	Create the following registry key on all Evidian EAM Clients, including Citrix/RDP servers. • **Location:** *HKLM\Software\Nymi\NES* • **Type:** String • **Name:** URL • **Value:** ***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.

Purpose	Affected Components	Registry Setting
Configure the user terminal to prevent the SSO login screen from populating the username field with the user that logged into the user terminal.	All Evidian EAM Clients where users log into the user terminal with a generic account and when the work flows require sign offs by more than one user.	Create the following registry key • **Location:**: *HKLM\SOFTWARE\Enatel\WiseGuard\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name: *Allow4EyesAndSameUser*** • **Value: *1*** 
Prevent user self-enrollment of a Nymi Band and other NFC devices	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.	Create the following registry key: • **Location:** *HKLM\Software\Enatel\Wiseguard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name: *RFIDSelfEnrollAllowed*** • **Value: *0***
Configure the Evidian EAM Client to avoid the use of the LsaLogonUser function and improve Nymi Band tap response times.	All Evidian EAM Clients, including Citrix/RDP servers and the enrollment terminal.	Create the following registry key: • **Location:** *HKLM\SOFTWARE\Enatel\WiseGuard\Framework\Directory* • **Type:** DWORD 32-bit • **Name: *CallLsaLogonUserAfterLogon*** • **Value: *0***
Configure enrollment terminal to access Nymi Band Application	Enrollment terminal	Create the following registry key: • **Location:** *HKLM\Software\Enatel\WiseGuard\AdvancedLogin* • **Type:** String • **Name:**WearableEnrollTool • **Value:** *C:\Program Files\Nymi\Nymi Band Application\NEM.exe* 

Purpose	Affected Components	Registry Setting
Use Case Specific Registry Key Settings		
Optimize NFC taps	All Evidian EAM Clients including Citrix/RDP servers and the enrollment terminal, where you perform Nymi Band taps on an NFC reader. **Note:** Ensure that you define these registry keys with Evidian EAM 10.03b8573 Hotfix 12 and later.	Key #1 • **Location:HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication** • **Type:** DWORD 32-bit • **Name:** ***NymiIntentDiscardNfc*** • **Value:** 0 Key #2 • **Location:HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication** • **Type:** DWORD 32-bit • **Name:** ***NymiIntentDiscardPcsc*** • **Value:** 1
When Integrate with Windows option is enabled on Windows 11 24H2	All Windows 11 24H2 Evidian EAM Clients.	• **Location:***HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*. • **Type:** DWORD 32-bit • **Name:** ***EnableMPR*** • **Value:** ***1*** **Note:** To push this change out through Group Policy Objects (GPO), this configuration is **`Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Logon Options`**. The setting name is *Configure the transmission of the user's password in the content of MPR notifications sent by winlogon*. To make this parameter available, you might require the *WinLogon.admx* from the Administrative Templates (.admx) for Windows 11 2024 Update (24H2), which you can obtain from Microsoft.

Purpose	Affected Components	Registry Setting
Support multiple domains, where users enroll their Nymi Bands in a domain that is different from the user terminal domain.	All Evidian EAM Clients including Citrix/RDP servers and the enrollment terminal.	Edit the *HKLM\Software\Enatel\WiseGuard\FrameWork\Directory\PossibleDomainList.* In the **`Value Data`** field, type the NETBIOS name for each domain that contains users, that will log in to the user terminal. **Note:** Separate each domain with a space, as shown in the following example. 
Prevent a user from logging into the machine by specifying a username without specifying a password, to avoid the situation where a user types the username of another user into the login window, and the other user is nearby an wearing an authenticated Nymi Band. The user can log in without requiring the password of the other user.	All Evidian EAM Clients where a user taps to login. **Note:** Do not set registry key with Evidian EAM 10.03b8573 Hotfix 12 and later. If you set this registry key with Evidian EAM 10.03b8573 Hotfix 12 and later, you cannot use the BLE Tap functionality.	Create the following registry key: • **Location:** *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name:** ***WearableNeedsRFID*** • **Value:** ***1*** 
Registry Key Settings Specific to Citrix/RDP environments		
Configure the Evidian EAM Client to communicate with the Nymi Agent server.	All Citrix/RDP servers	Create the following registry key: • **Location:** *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication* • **Type:** String • **Name:** ***NymiAgentUrl*** • **Value:** ***ws://`agent_fdqn`:9120/socket/websocket*** Where *`agent_fdqn`* is the Fully Qualified Domain Name of the centralized Nymi Agent server.

Purpose	Affected Components	Registry Setting
Configure Citrix roaming sessions, to ensure that when a published MES application closes, the Citrix session is logged off.	All Citrix servers	Create/Update the following registry keys: Registry Key #1 Edit the following registry key and append the following files to the ValueData field. • **Location:** *HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI* • **Type:** String • **Name:** ***LogoffCheckSysModules*** • **Value:** ***ssoengine.exe, ESSOCredentialManager.exe*** Registry Key #2 • **Location:** *HKLM\SOFTWARE\Policies\Enatel\SSOWatch\CommonConfig* or *HKLM\SOFTWARE\Enatel\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***DoNotManageProcList*** • **Value:** ***1***
Performance Specific Registry Key Settings		
Increase the time that the Evidian EAM Client waits for the initialization of the *nymi_api.dll* and retrieval of authentication token from NES to complete.	All Evidian EAM Clients, including Citrix/RDP servers and the enrollment terminal.	Create the following registry key: • **Location:** *HKLM\Software\Enatel\Wiseguard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name:** ***WearableDelay*** • **Value:** ***10000*** • **Base:** **`Decimal`**

Purpose	Affected Components	Registry Setting
Prevent the appearance of the `Enterprise SSO` Login window for user who are not in the inclusion group.	All Evidian EAM Clients, including the Citrix/RDP servers. **Note:** Do not set this registry key with the Evidian EAM 10.03b8573 Hotfix 9 and later.	If the *Integrate with Windows Authentication* module is enabled and a generic account is not used for Windows login, set the following registry keys: Key #1: • **Location:** *HKLM\Software\Enatel\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***StopSSOEngineOnOTPFailed*** • **Value:** 1 Key #2: • **Location:**: *HKLM\Software\Enatel\WiseGuard\AdvancedLogin* • **Type:** DWORD 32-bit • **Name:** ***StartSSOEngine*** • **Value:** 1 If the *Integrate with Windows Authentication* and *Authentication Manager* modules are not enabled, set the following registry key: • **Location:**: *HKLM\Software\Enatel\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***DisplayErrorMessageAtStartup*** • **Value:** 0

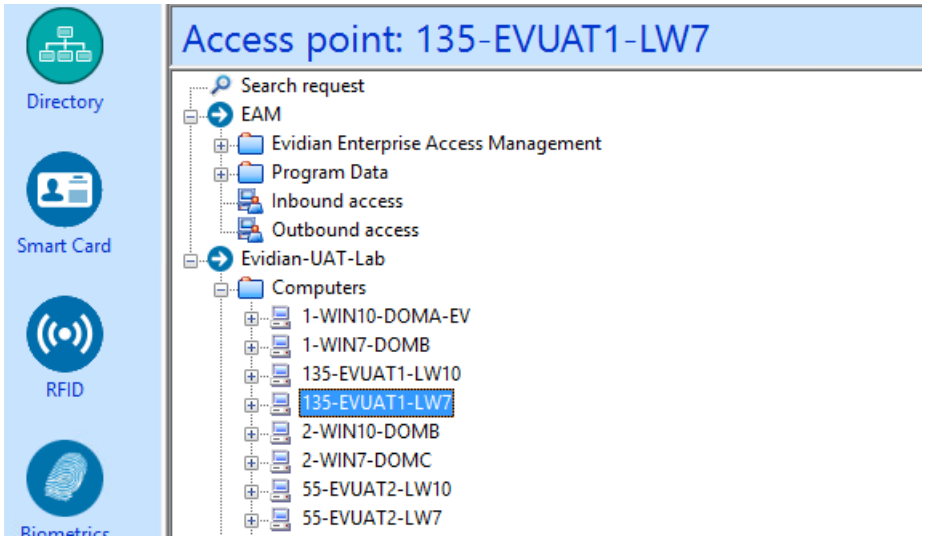
7.3.3 - Replacing the Nymi DLL File

Replace the *nymi_api.dll* file that the Evidian EAM Client uses with the version used by the Nymi Band Application.

Procedure

1. Rename the *nymi_api.dll* file in *C:\Program Files\Common Files\Evidian\WGSS*.
2. Copy the *C:\Program Files\Nymi\Nymi Band Application\nymi_api.dll* file to *C:\Program Files\Common Files\Evidian\WGSS*.
3. Log in to the Evidian EAM Management Console.
4. Click **`Account and access rights management`**  .

5. In the left navigation pane, expand **`Domain > Computers`**, and then select the terminal, as shown in the following figure.



6. On the **`Actions`** tab, select **`Delete cache files`**, and then click **`Apply`**.
   The cache files are deleted on the terminal and the terminal desktop locks.

7.3.4 - Logging into the terminal

If you installed the Evidian SSOAgent with the Authentication Manager, when the terminal locks, the Windows login screen appears with new options.

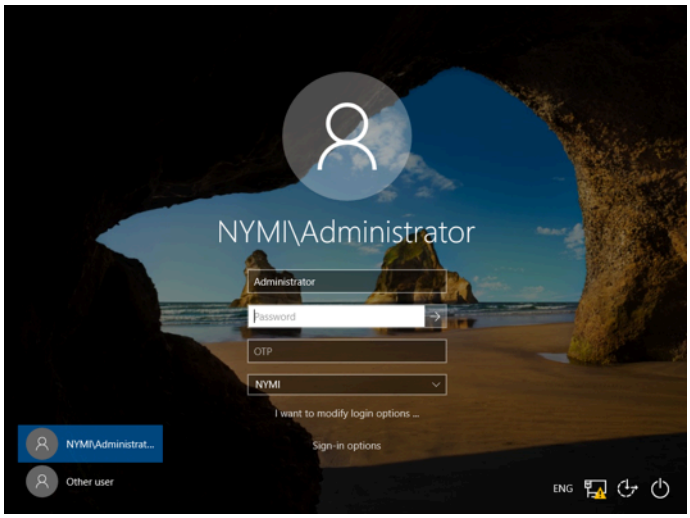
About this task

Perform the following steps to log in.

Note: On the first login, you cannot log in with a Nymi Band tap.

Procedure

1. Press Ctrl-Alt-Delete.
   The `Windows Login` screen appears with additional options. The following figure provides an example of the login screen.



2. Log in to the computer with your username and password.
   The desktop appears.

7.3.5 - Add Wearable TMS File to Enrollment Terminal

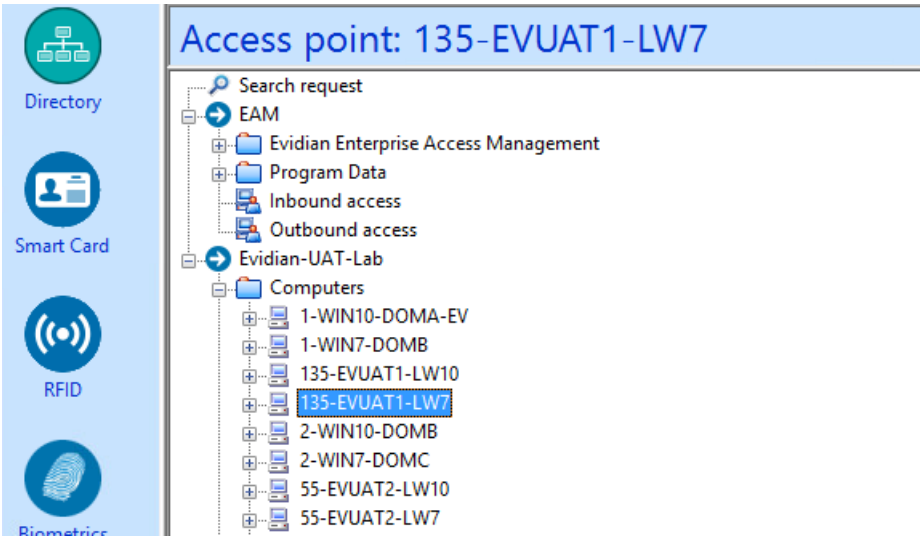
Configure the enrollment terminal to load a wearable token management structure file, when the default authentication method on the Evidian EAM Controller is RFID-only.

About this task

Perform these steps on the Enrollment Terminal.

Procedure

1. Copy the *TokenManagerStructure-Wearable.xml* file. to *C:\Program Files\Common Files\Evidian\WGSS* folder.
2. Rename *TokenManagerStructure-Wearable.xml* file to *TokenManagerStructure.xml*.
3. Log in to the Evidian EAM Management Console.
4. Click **`Account and access rights management`**  .
5. In the left navigation pane, expand **`Domain > Computers`**, and then select the terminal, as shown in the following figure.



6. On the **`Actions`** tab, select **`Delete cache files`**, and then click **`Apply`**.
   The cache files are deleted on the terminal and the terminal desktop locks.

7.3.6 - Validating the Evidian EAM Client Installation

After you log into the computer, validate that the Evidian EAM Client can connect to the Evidian EAM Controller.

Open the system tray and confirm hover over the **`ESSO Credential Manager`** icon. Confirm that the status appears as **Connected Mode**, as shown in the following figure.

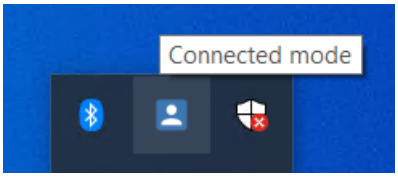


Figure 165: ESSO Credential Manager connected mode

If the status that appears is **Disconnected Mode**, the Evidian EAM Client cannot establish a connection with the Evidian EAM Controller, refer to the *Nymi Connected Worker Platform with Evidian Troubleshooting Guide* for more information.

7.3.7 - Importing Technical Definition

In some situations you might import the technical definitions that are associated with your SSO applications,for example, when you move from a Development environment to a QA environment to a Production Environment.

You will use Enterprise SSO Studio and the EAM Console to importing the technical definition.

Importing Technical Definitions in Enterprise SSO Studio

Perform the following steps on a user terminal on which you installed `Enterprise SSO Studio`.

1. Download the *.sse* file to the computer.
2. Launch the `Enterprise SSO Studio` application (*C:\Program Files\Evidian\Enterprise Access Management\ssobuilder.exe*).
3. Expand **`EAM > Evidian Enterprise Access Management > Application access > Technical Definitions.`**.
4. Right-click the technical definition, and then select **`Import`**.
5. Navigate to the directory that contains the *.sse* file and then double-click the file.

   The technical definition appears in the **`Technical Definitions`** folder, as shown in the following figure.

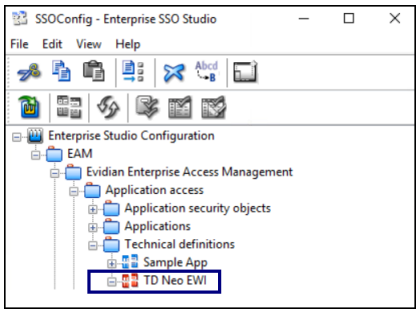


Figure 166: Imported Technical Definition

6. For technical definitions that are related to web-based applications, expand the new application and then perform the following steps for each window that appears in the application:

   a. Right-click the first window that appears in the application, and then select **`Properties`**, as shown in the following figure.

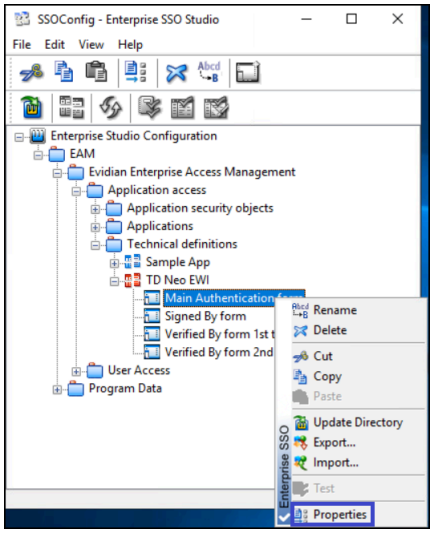


Figure 167: Properties option

b. On the **`Detection`** tab, update that the URL address that appears in the URL field if it is not correct for your environment.

c. Click **`OK`**.

7. Right-click the new application and then select **`Update directory`**.

The application icon changes from red to blue. The following figure shows the **`Update directory`** option.

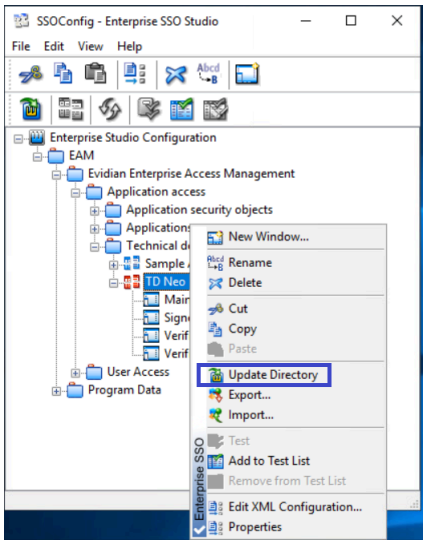
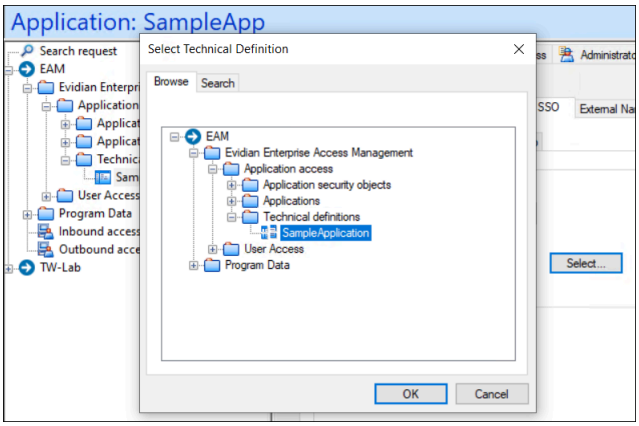


Figure 168: Properties option

Update Technical Definition in Evidian EAM Management Console

Perform the following steps while logged into the Evidian EAM Management Console as an administrator:

1. Click the **Account and access right management** button  .
2. Expand **EAM > Enterprise Access Management > Application**.
3. Right-click **Applications** and then select **New Application**.
4. On the **Information** tab, in the **Name** field, specify a name of the application. Click **Apply**.
5. On the **Configuration** tab, click the **SSO** tab, and then select **SSO**. In the **Methods** window, from the **Default SSO Propagation method** list, select **SSO**. The technical definition field appears.
6. Navigate to **EAM** > **Evidian Enterprise Access Management** > **Application access** > **Applications > Technical Definitions**, select the new technical definition, and then click **OK**. The following figure provides an example.



7.4 - Install User Terminal Components

Review this section for detailed information about how to install the client software on user terminal, including Citrix/RDP servers and the Nymi Band Management Console.

The client software that you install and the configuration steps depend on the authentication mode and environment configuration. The following table provides a high-level overview of the client applications to install on each component, in each configuration.

Table 7: Applications to Install on Each Component

Configuration	Component	Client Applications
Wearable mode with application on RDP/Citrix Servers	Thin User Terminals	Nymi Runtime (Nymi Bluetooth Endpoint only)
	RDP/Citrix Application Server	Evidian EAM Client
	RDP/Citrix Enrollment Server	Nymi Band Application
	Centralized Nymi Agent	Nymi Runtime (Nymi Agent only)

Configuration	Component	Client Applications
RFID mode with application on RDP/Citrix Servers	Thin User Terminals	n/a
	RDP/Citrix Application Server	Evidian EAM Client
	Nymi Band Application Terminal	Nymi Band Application (which installs Nymi Runtime)
Wearable Mode with Local application	Thick client	Evidian EAM Client Nymi Runtime (Nymi Bluetooth Endpoint and Nymi Agent)
	Nymi Band Application Terminal	Nymi Band Application (which installs Nymi Runtime)
RFID-only Mode with Local application	Thick client	Evidian EAM Client
	Nymi Band Application Terminal	Nymi Band Application (which installs Nymi Runtime)

7.4.1 - Installing and Configuring Software on User Terminals

An Operator uses a user terminal to perform an authentication event, such as an e-signature in an MES application that was developed with the Nymi API, and the Evidian EAM Client software.

The Nymi with Evidian Solution supports the use of the Nymi Band to perform authentication events on an application that is local to the user terminal or on a Citrix server/RDP session host that a user terminal connects to.

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.

7.4.1.1 - 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`**.

7.4.1.2 - Installing the Nymi Runtime software

Install the Nymi Runtime on each Wearable mode thick client user terminal in the environment. In an RFID-only environment, you must have at least one Wearable mode thick client, on which you install the Nymi Runtime to enable access to the Nymi Band Application.

About this task

Note:

The Nymi Runtime components that a user terminal requires differs depending on how a user accesses the application.

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` window, perform one of the following actions:
   - If the user will perform authentication tasks in an application that you install on the thick client, click **`Next`**.
   - If the user will perform authentication tasks in an application that a user accesses on a RDP/Citrix session host, then perform the following actions:

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

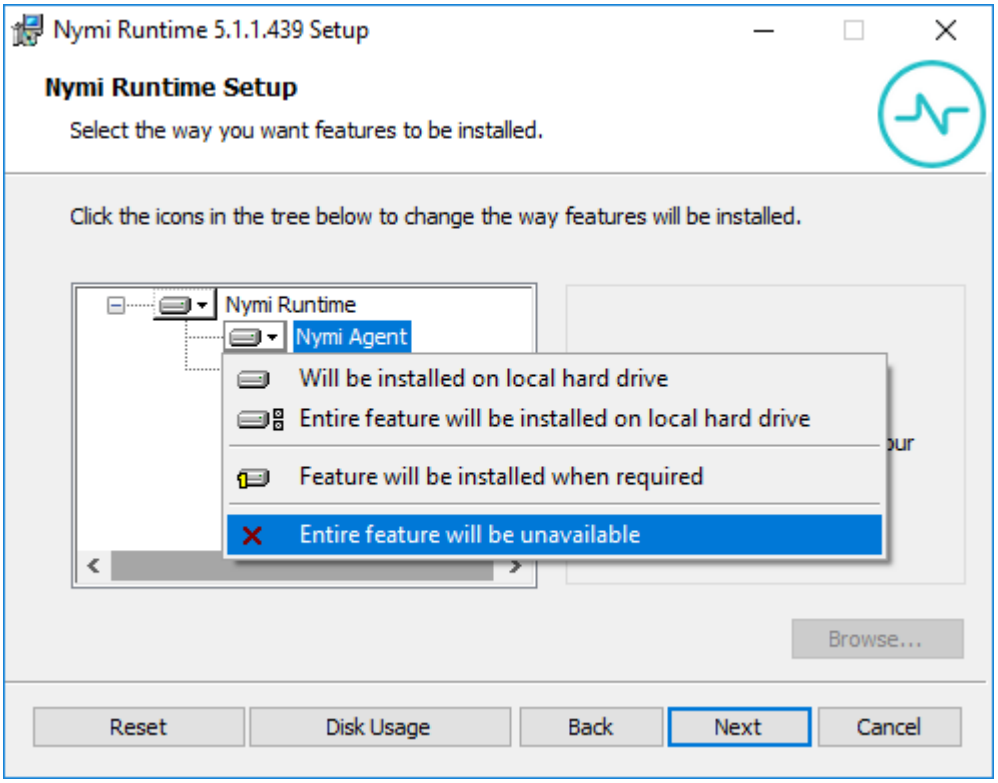


Figure 169: Nymi Agent feature will be unavailable

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

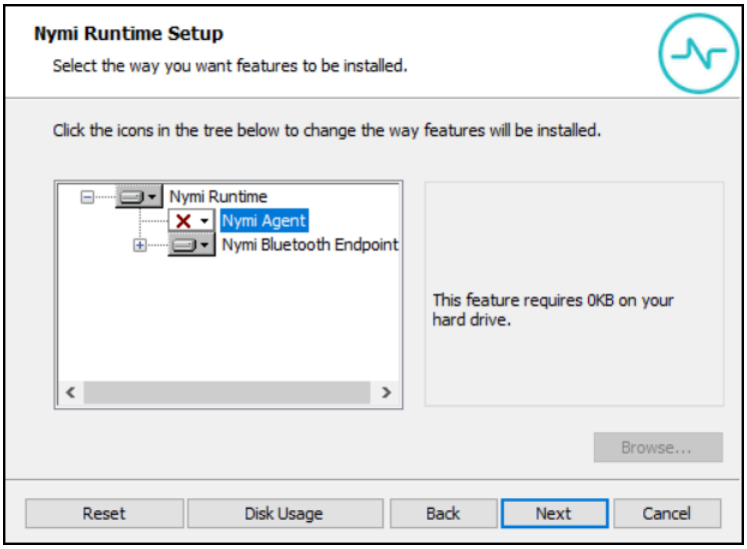


Figure 170: Nymi Agent feature is not available

c. Click **`Next`**.

8. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
   - Accept the default service account NTAuthority\LocalService, click **`Next`**.
   - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.
9. 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.
10. On the `Ready to install` page, click **`Install`**.
11. Click **`Finish`**.
12. On the `Installation Completed Successfully` page, click **`Close`**.

What to do next

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

(Wearable Mode Only) Configuring Citrix/RDP Clients to Access the Centralized Nymi Agent

On the user terminals that access the authentication application on Citrix servers or RDP session hosts, configure the Nymi Bluetooth Endpoint to communicate with the Nymi Agent server by performing the following steps.

Procedure

1. Create a text file named *nbe.toml* in the *C:\Nymi\Bluetooth_Endpoint* directory, with the following line, which defines the centralized Nymi Agent: ***agent_url='ws://agent_FQDN:9120/socket/websocket'***
2. Restart the Nymi Bluetooth Endpoint service.

7.4.1.3 - Configuring the Evidian EAM Client

The machines on which you install and configure the Evidian EAM Client depends on how the user accesses the application and how the user uses the Nymi Band.

Before you begin

- Complete the steps to configure the Evidian EAM Controller.
- Ensure that the machine is on the same domain as the Evidian EAM Controller.
- Obtain the Evidian license file from the Nymi Solution Consultant.
- For RDP session hosts and Citrix servers, ensure that the host is configured with the FQDN.

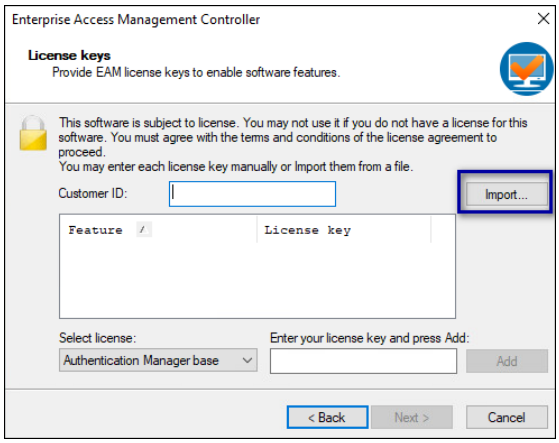
About this task

Configure and install the Evidian EAM Client on the following components:

Use Case	Install
User accesses an application that you installed on the user terminal	Configure and install the Evidian EAM Client on the user terminal.
User accesses an application on an RDP/Citrix session hos	install the Evidian EAM Client on the RDP sessions host or Citrix server.
User uses the Nymi Band to unlock their user terminal	Configure and install the Evidian EAM Client on the user terminal.

Procedure

1. Log in to the machine with an account that has Local Administrator access.
2. Download and extract the Evidian software package, *EAM-v10.0x.xxxxxxx.zip* to a directory on the host, for example, the *Downloads* directory.
3. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\Tools\WGConfig\WGConfig.exe* file.
4. On the `User Access Control` window, click **`Yes`**.
5. On the `Welcome to the Configuration Assistant` window, click **`Next`**.
6. If the required Microsoft Visual C++ Redistributable software is not installed on the server, the `Prerequisites` window appears. Click **`Next`** to install the software.
   The Windows Installer window appears.
7. On the `License keys` window, click **`Import`**, as shown in the following figure.



8. In the `Open` window, select the license file in the *Downloads* directory, and the click **`Open`**.
   If you do not see the file, select **`All Files *.*`** from the file type list.
9. On the `Installation mode` window, leave the default option **`with a controller`** selected, and then click **`Next`**.
   The following figure provides an example of the `Installation mode` window.

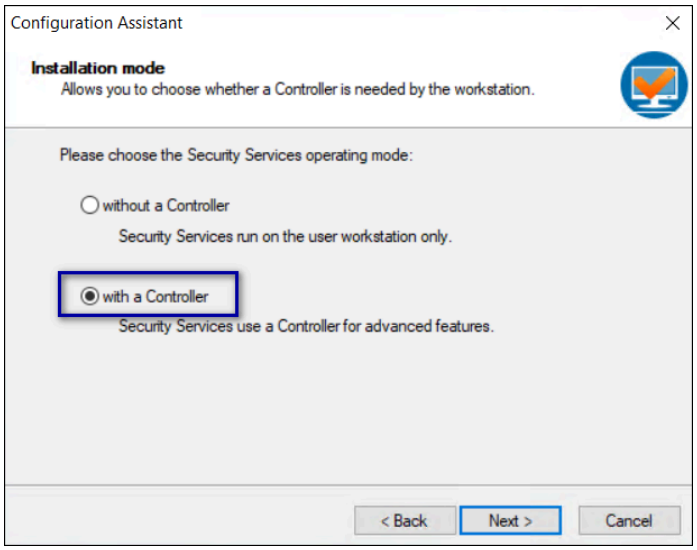


Figure 171: Installation mode window

10. On the `Users directory` window, leave the default option **`Microsoft Active Directory`** selected, and then click **`Next`**.

    The following figure provides an example of the `Users directory` window.

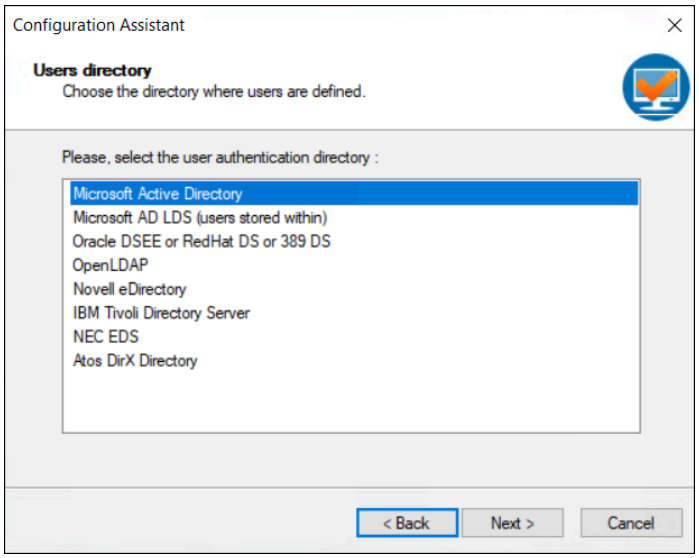


Figure 172: Users directory window

11. On the `Security repository` window, select the option **`Integrated with AD LDS: the security data is stored in an AD LDS server`**, and then click **`Next`**.

    The following figure provides an example of the `Security repository` window.

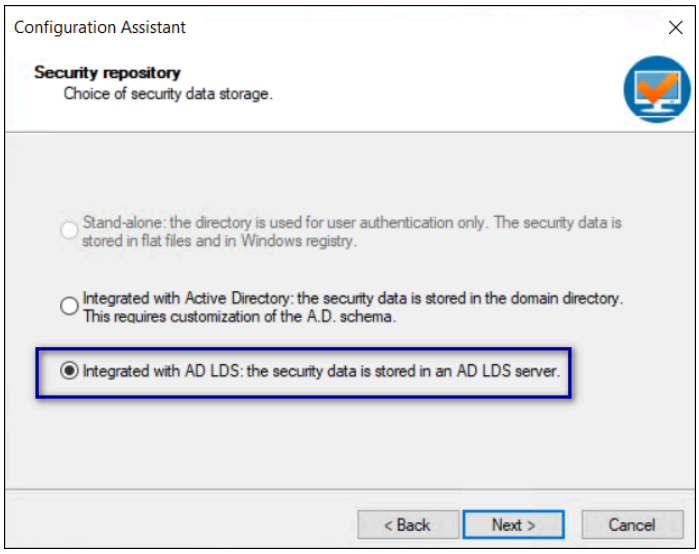


Figure 173: Security repository window

12. On the `LDAP Configuration` window, perform the following action:

a) In the **`Name/address`** field, type the FQDN of the Evidian EAM Controller, and in the **`Port`** field, type ***55000***.

b) Click **`Add`**.

c) Leave the default option **`Use a dedicated naming context for the Evidian Enterprise Access Management data`** selected, and then in the **`Evidian Enterprise Access Management data context`** field, type ***O=EAM***.

The following figure provides an example of the `LDAP Configuration` window.

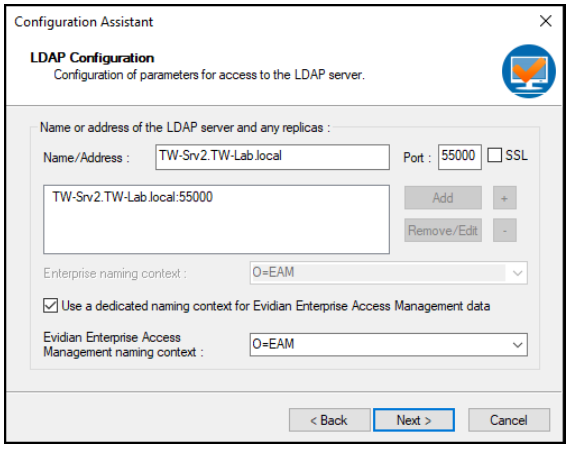


Figure 174: LDAP Configuration

d) Click **`Next`**.

13. On the `Access-point management` window, select **`Manage access points`**, as shown in the following figure, and then click **`Next`**.

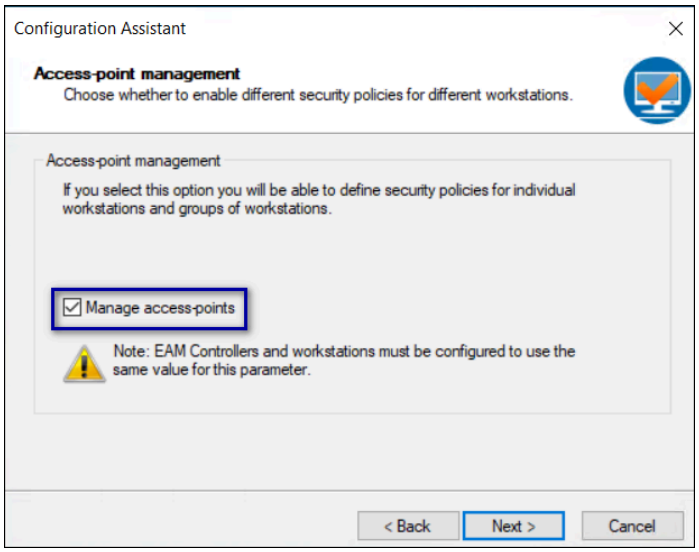


Figure 175: Access-point management window

14. On the `Restart Computer` window, leave the default selection **`Do not restart the computer`**, as shown in the following figure, and the click **`Finish`**.

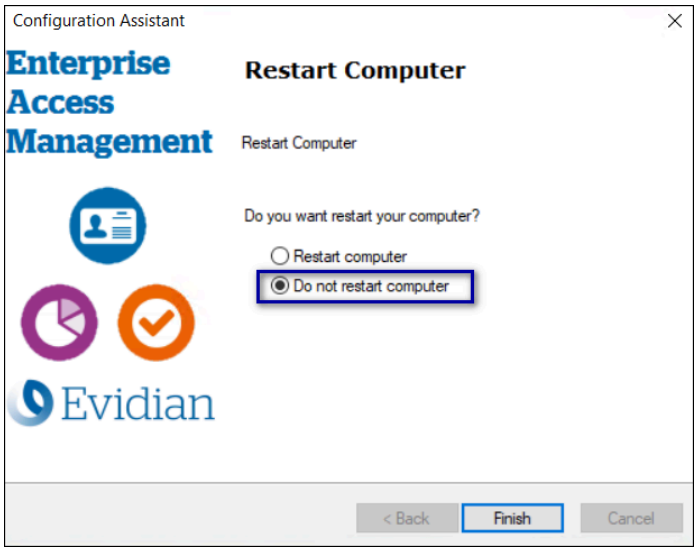


Figure 176: Restart Computer window

7.4.1.4 - Installing the Evidian EAM Client

Perform the following steps on the user terminal to install the Evidian Single Sign On (SSO) Agent.

About this task

For Centralized Nymi Agent deployments, you will install the Evidian EAM Client on each Citrix server / RDP session host. For decentralized Nymi Agent deployments, install the Evidian EAM Client on each thick client user terminal.

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\VCRedist_x64.msi*.

   Note: If the required version of Microsoft Visual C++ redistributable is already installed on the server, a pop-up screen briefly appears, and then disappears.
2. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\ESSOAgent.msi* file.
3. On the `Enterprise Access Management Client Installation`, click **`Next`**.
4. On the `License Agreement` window, click **`I accept the license agreement`**, and then click **`Next`**.

   The following figure shows the `License Agreement` window.

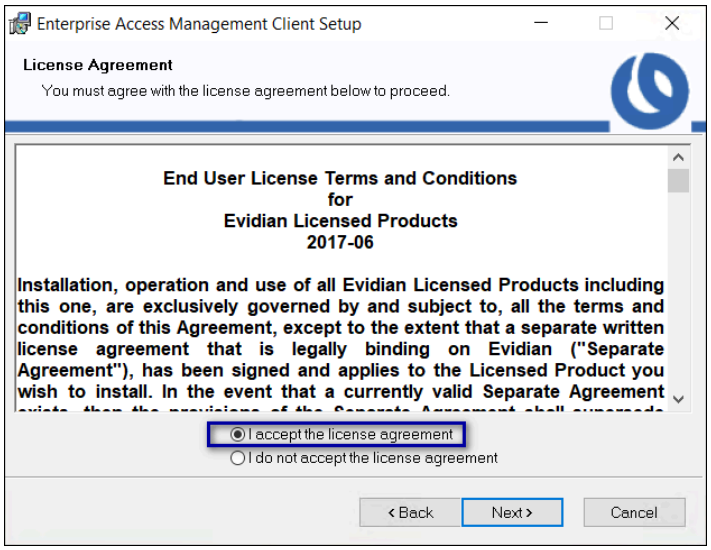


Figure 177: License Agreement window

5. On the `Destination Folder` window, accept the default, and then click **`Next`**.

   The following figure shows the `Destination Folder` window.

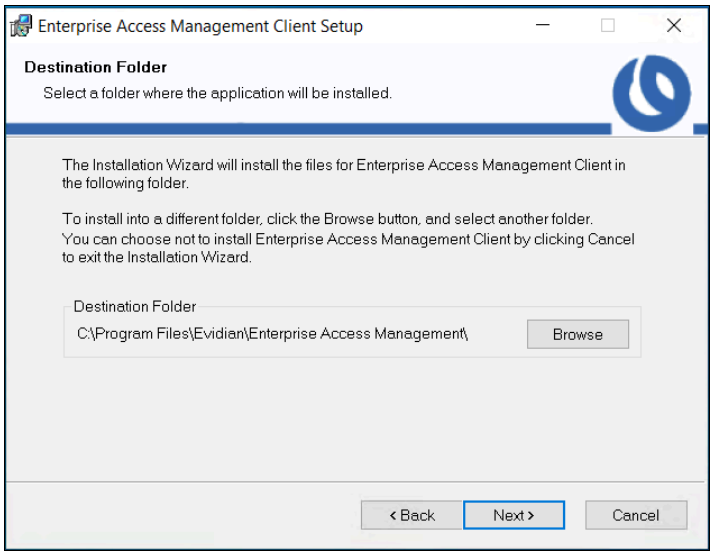


Figure 178: Destination Folder window

6. On the `Select Installation Type` window, select **`Custom`**, and then click **`Next`**.

   The following figure shows the `Select Installation Type` window.

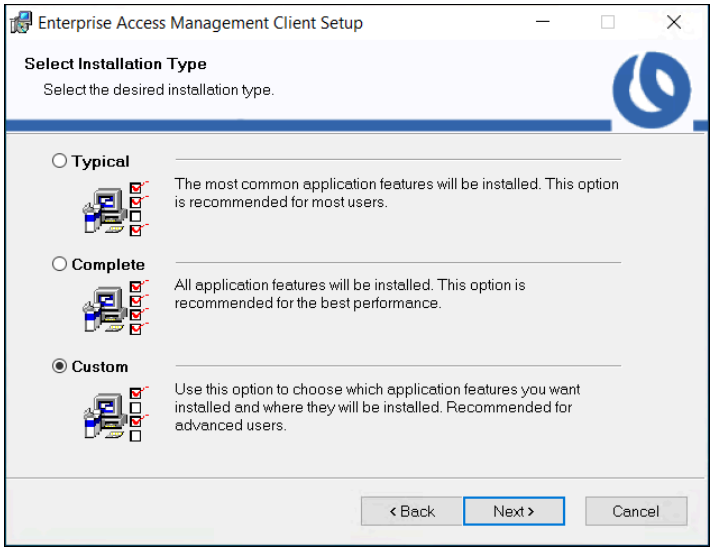
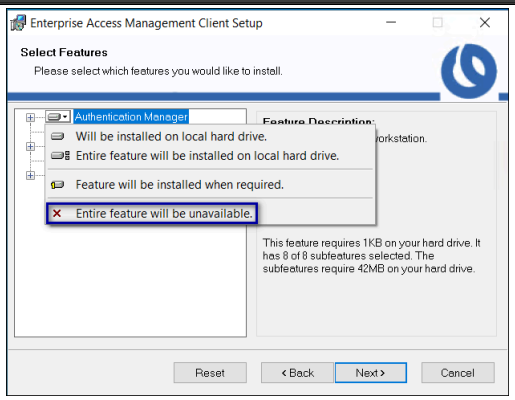
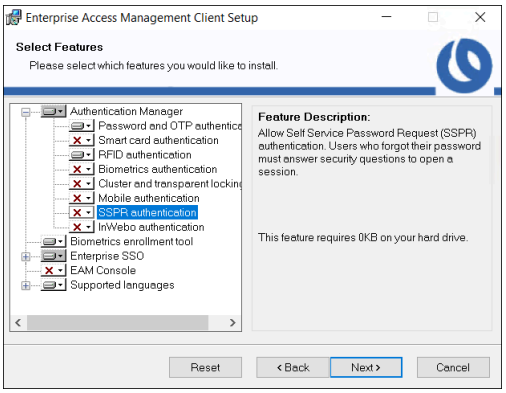


Figure 179: Select Installation Type window

7. On the `Select features` window, for **`Authentication Manager`** perform one of the following actions based on your Nymi Band use case:

   Note: Unless otherwise noted, leave the default option for a feature.

Option	Description
Do not use the Nymi Band to log into terminal.	Select **`Authentication Manager`**, and then select **`Entire feature will be unavailable`**.

Option	Description
	
Use the Nymi Band to log into terminal	Expand **`Authentication Manager`**. For each of the following features: • Smart card authentication • Biometrics authentication • Cluster and transparency • Mobile authentication • SSPR authentication • InWebo authentication Select the feature, and then select **`Entire feature will be unavailable`**, as shown in the following figure.  The only features to install are **`Password and OTP authentication`** and **`RFID authentication`**.

8. Click **`Biometric enrollment tool`**, and then select **`Entire feature will be unavailable`**, as shown in the following figure.

   The following figure shows the `Select Features` window.

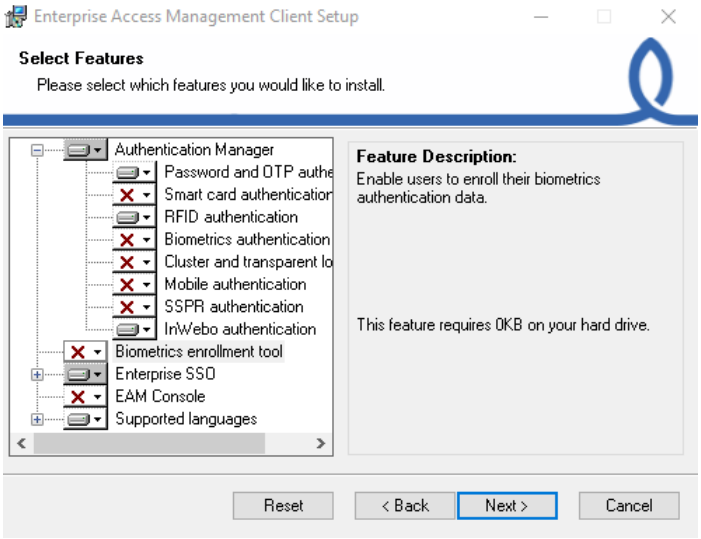


Figure 180: Select Features - Authentication Manager options and without Biometric enrollment tool

9. If you removed the **`Authentication Manager`** feature, and want the SSO Login window to open with the username of the user that logged into Windows, select **`Integrate with Windows`**, and then select **`Entire feature will be installed on local hard drive`**, as shown in the following figure.

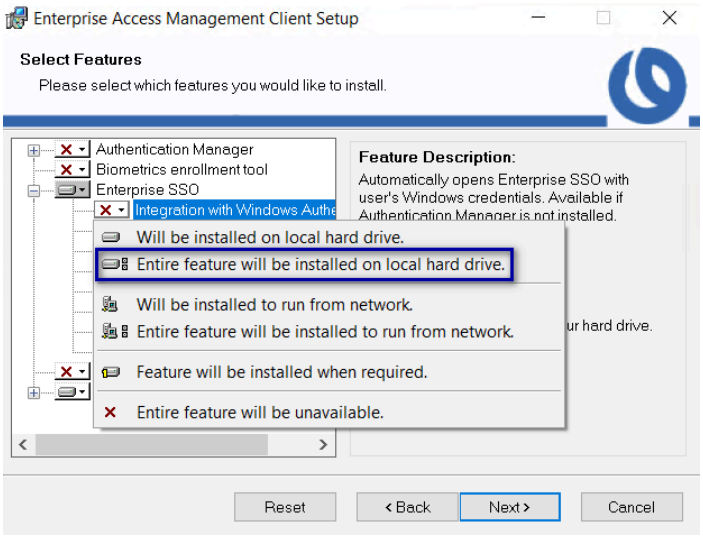
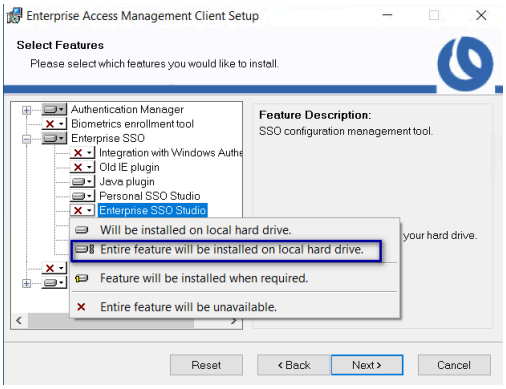
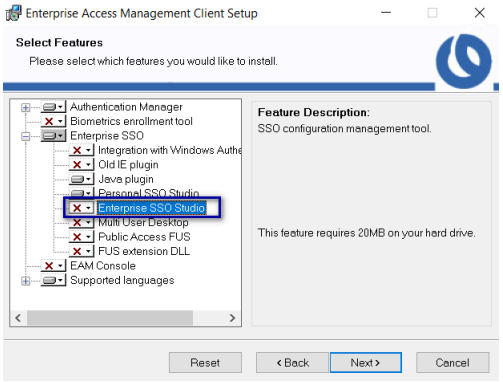
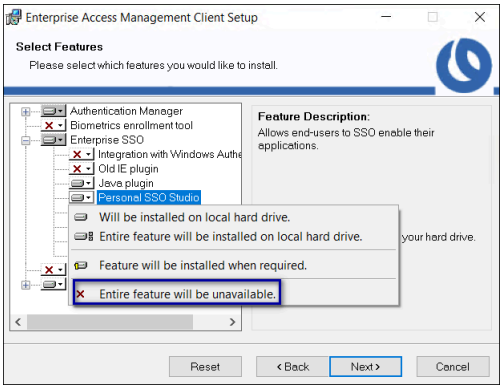


Figure 181: Integrate with Windows

10. For **`Enterprise SSO`**, perform one of the following actions based on your Nymi Band use case:

Note: Unless otherwise noted, leave the default option for a feature.

Option	Description
Use the Nymi Band for SSO	Click **`Enterprise SSO Studio`**, and then select **`Entire feature will be`**

Option	Description
	`installed on local hard drive`, as shown in the following figure. 
Use the Nymi Band for Windows login only	Leave the default **`Enterprise SSO`** configuration, as shown in the following figure. 
All use cases	Click **`Personal SSO Studio`**, and then select **`Entire feature will be unavailable`**, as shown in the following figure. 

11. Select **`EAM Console`**, and then select **`Entire feature will be installed on local hard drive`**, as shown in the following figure.

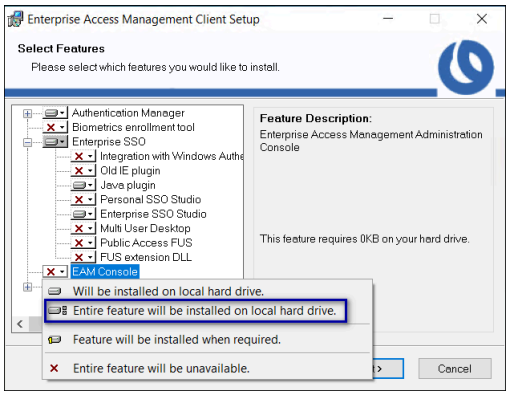


Figure 182: Install EAM Console Feature

12. Click **`Next`**.
13. On the `Ready to install the application` window, click **`Next`**, as shown in the following figure.

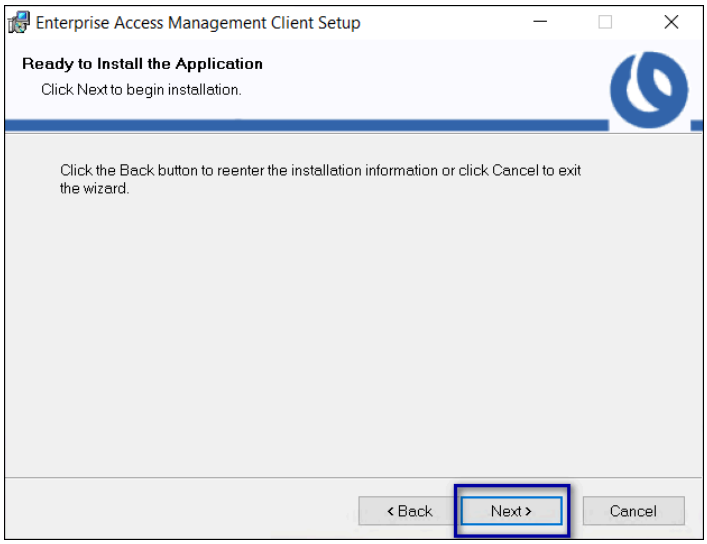


Figure 183: Ready to install the application

14. On the `User account control` pop-up, click **`Yes`**, as shown in the following figure.

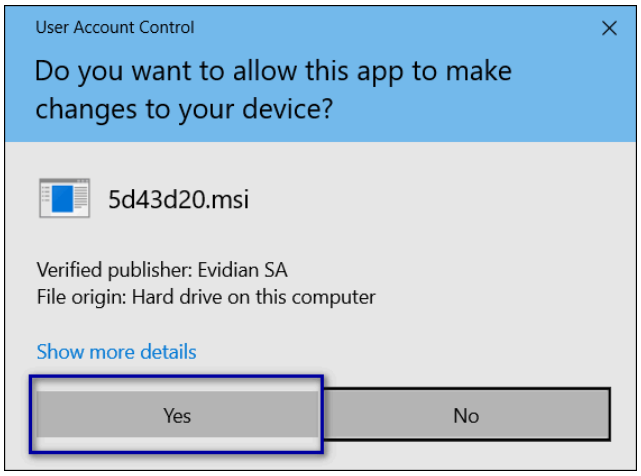


Figure 184: User account control

15. On the `Enterprise Access Management Client has been successfully installed` window, click **`Finish`**, as shown in the following figure.

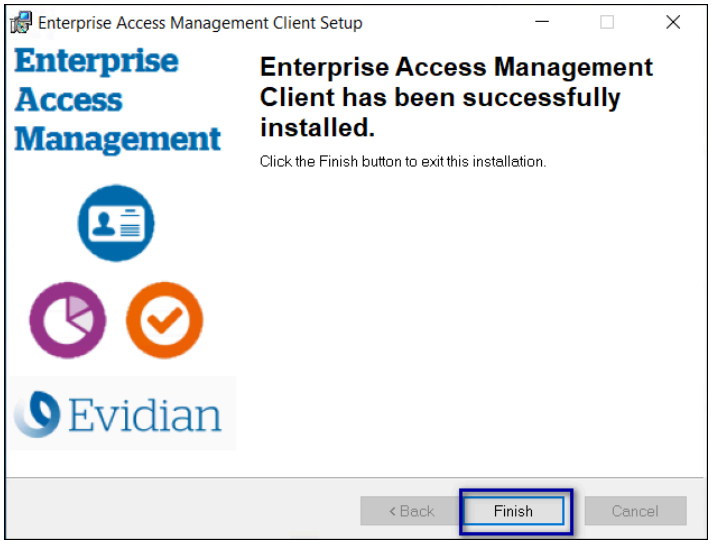


Figure 185: Evidian Client Installation Success window

16. In the Windows System Tray, click on the Enterprise SSO (eSSO) icon.
17. Click the **`Home`** icon, and then click **`Refresh`**, as shown in the following figure.

    The Evidian EAM Client contacts the Evidian EAM Controller to retrieve new technical definitions.

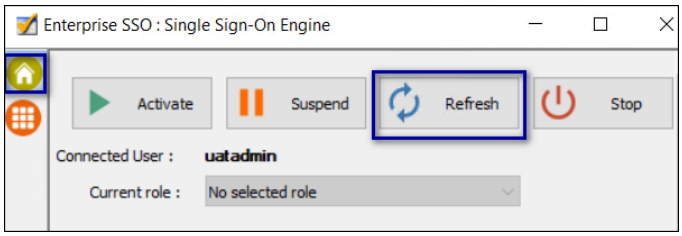
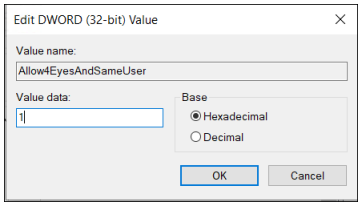


Figure 186: eSSO application Home Window

7.4.1.5 - (NFC-only Mode Only) Defining the EAM client Registry Keys

The Nymi with Evidian Solution requires several registry keys on the Evidian EAM Clients to configure features and optimize performance.

After you define the registry keys, restart the Evidian Enterprise Access Management Security service on the computer.

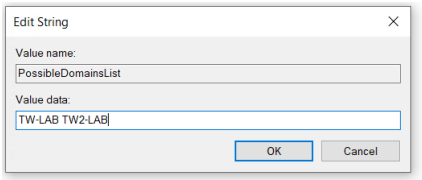
Purpose	Affected Components	Registry Setting
Required Registry Key Settings for the Nymi with Evidian Solution		
Configure the user terminal to prevent the SSO login screen from populating the username field with the user that logged into the user terminal.	All Evidian EAM Clients where users log into the user terminal with a generic account and when the work flows require sign offs by more than one user.	Create the following registry key • **Location:**: *HKLM\SOFTWARE\Enatel\WiseGuard\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***Allow4EyesAndSameUser*** • **Value:** ***1*** 

Purpose	Affected Components	Registry Setting
Configure the Evidian EAM Client to use and cache the Evidian roaming session.	all Evidian EAM Clients, including Citrix/RDP servers.	Create the following registry keys: Key #1 • **Location:** *HKLM\Software\Enatel\Wiseguard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name:** ***RoamingSessionAllowedForSSO*** • **Value:** ***1*** Key #2 • **Location:** *HKLM\Software\Enatel\Wiseguard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name:** ***RoamingSessionCached*** • **Value:** ***1***
Prevent user self-enrollment of a Nymi Band and other NFC devices	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.	Create the following registry key: • **Location:** *HKLM\Software\Enatel\Wiseguard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name:** ***RFIDSelfEnrollAllowed*** • **Value:** ***0***
Configure the Evidian EAM Client to avoid the use of the LsaLogonUser function and improve Nymi Band tap response times.	All Evidian EAM Clients, including Citrix/RDP servers and the enrollment terminal.	Create the following registry key: • **Location:** *HKLM\SOFTWARE\Enatel\WiseGuard\Framework\Directory* • **Type:** DWORD 32-bit • **Name:** ***CallLsaLogonUserAfterLogon*** • **Value:** ***0***
Prevent the EAM client from retrieving Cloud-related configuration data.	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.	Create the following registry key: • **Location:**: *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Directory* • **Type:** DWORD (32-bit) • **Name:** ***GetCloudConfigDataOnlyInCloudMode*** • **Value:** ***1***

Purpose	Affected Components	Registry Setting
Configure validity period of cache credentials when client cannot communicate with AD LDS	All Evidian EAM Clients, including Citrix/RDP.	• **Location:***HKLM\Software\Enatel\WiseGuard\Framework\Cache* • **Type:** DWORD 32-bit • **Name:** ***CriticalDataOfflineDelay*** • **Value:** ***43200***
Registry Key Settings specific to Citrix/RDP environments		
Configure the Evidian EAM Client to communicate with the Nymi Agent server.	All Citrix/RDP servers	Create the following registry key: • **Location:** *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication* • **Type:** String • **Name:** ***NymiAgentUrl*** • **Value:** ***ws://agent_fdqn:9120/socket/websocket*** Where *agent_fdqn* is the Fully Qualified Domain Name of the centralized Nymi Agent server.
Configure Citrix roaming sessions, to ensure that when a published MES application closes, the Citrix session is logged off.	All Citrix servers	Create/Update the following registry keys: Registry Key #1 Edit the following registry key and append the following files to the ValueData field. • **Location:** *HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI* • **Type:** String • **Name:** ***LogoffCheckSysModules*** • **Value:** ***ssoengine.exe, ESSOCredentialManager.exe*** Registry Key #2 • **Location:** *HKLM\SOFTWARE\Policies\Enatel\SSOWatch\CommonConfig* or *HKLM\SOFTWARE\Enatel\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***DoNotManageProcList*** • **Value:** ***1***
LDAPS Registry Key Settings		

Purpose	Affected Components	Registry Setting
Support LDAPS for the communication with an AD LDS instance.	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers. **Note:** Requires Evidian Authentication Manager and Enterprise SSO 10.0 evolution 2 patch level 3 or later.	Create the following registry keys: Key #1 • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\WGDirectory* • **Type:** DWORD 32-bit • **Name:** ***SSL*** • **Value:** ***1*** Key #2 If some of your Active Directory(AD) Domain Controllers(DCs) do not use SSL or are not reachable, perform the following steps to define which AD DCs the Evidian software should use for LDAPS: • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\WGDirectory* • **Type:** DWORD 32-bit • **Name:** ***ServerList*** • **Value:** ***fqdn1:55001 fdqn2:55001*** where: • *fqdn1* and *fqdn2* are the fully qualified domain names of the LDAP Directory Servers. • *55001* is the LDAPS port number. For Example: srvad1.mycompany.lan:55001 srvad2.mycompany.lan:55001 **Note:** You can separate the server entries with a comma or space. Ensure that the *GSSEncryption* and *GSSSignature* registry keys are deleted in the following location: *HKEY_LOCAL_MACHINE\SOFTWARE \Enatel\WiseGuard\FrameWork \WGDirectory*

Purpose	Affected Components	Registry Setting
Support LDAPS for the communication with an Active Directory instance.	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers. **Note:** Requires Evidian Authentication Manager and Enterprise SSO 10.0 evolution 2 patch level 3 or later.	Create the following registry keys: Key #1 • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\Directory* • **Type:** DWORD 32-bit • **Name:** ***SSL*** • **Value:** ***1*** Key #2 If some of your AD DCs do not use SSL or are not reachable, perform the following steps to define which AD DCs the Evidian software should use for LDAPS: • **Location:***HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\Directory* • **Type:** DWORD 32-bit • **Name:** ***ServerList*** • **Value:** ***fqdn1:port fdqn2:port*** where: • *fqdn1* and *fqdn2* are the fully qualified domain names of the LDAP Directory Servers. • *port* is the LDAPS port number and is not required if LDAPS communications occur over the default port 636. For Example: srvad1.mycompany.lan srvad2.mycompany.lan **Note:** You can separate the server entries with a comma or space. Ensure that the *GSSEncyption* and *GSSSignature* registry key values are set to 0 in the following location: *HKEY_LOCAL_MACHINE\SOFTWARE \Enatel\WiseGuard\FrameWork\Directory*
Use Case Specific Registry Key Settings		

Purpose	Affected Components	Registry Setting
When Integrate with Windows option is enabled on Windows 11 24H2	All Windows 11 24H2 Evidian EAM Clients.	• **Location:***HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows \CurrentVersion\Policies\System*. • **Type:** DWORD 32-bit • **Name:** ***EnableMPR*** • **Value:** ***1*** **Note:** To push this change out through Group Policy Objects (GPO), this configuration is **`Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Logon Options`**. The setting name is *Configure the transmission of the user's password in the content of MPR notifications sent by winlogon*. To make this parameter available, you might require the *WinLogon.admx* from the Administrative Templates (.admx) for Windows 11 2024 Update (24H2), which you can obtain from Microsoft.
Support multiple domains, where users enroll their Nymi Bands in a domain that is different from the user terminal domain.	All Evidian EAM Clients including Citrix/RDP servers and the enrollment terminal.	Edit the *HKLM\Software\Enatel \WiseGuard\FrameWork\Directory \PossibleDomainList.* In the **`Value Data`** field, type the NETBIOS name for each domain that contains users, that will log in to the user terminal. **Note:** Separate each domain with a space, as shown in the following example. 

Purpose	Affected Components	Registry Setting
For use with DeltaV	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.	Create the following registry keys in *HKLM\Software\Enatel\SSOWatch \CommonConfig*: Key #1 • **Type:** DWORD 32-bit • **Name:** ***NoCacheFields*** • **Value:** ***1*** Key #2 • **Type:** DWORD 32-bit • **Name:** ***CheckUIAutomationFieldPresence*** • **Value:** ***2*** Key #3 • **Type:** DWORD 32-bit • **Name:** ***DoNotStopCustomScriptOnCancel*** • **Value:** ***1*** Key #4 • **Type:** DWORD 32-bit • **Name:** ***SupportMultipleDesktops*** • **Value:** ***1***
Set when the Integrate with Windows Authentication and Authentication Manager modules are not enabled on the client	All Evidian EAM Clients, including the enrollment terminal.	• **Location:***HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\SSOWatch \CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***DisplayErrorMessageAtStartup*** • **Value:** ***0***

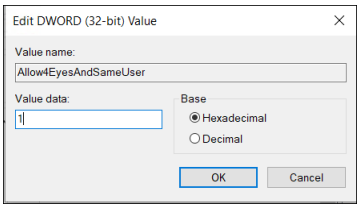
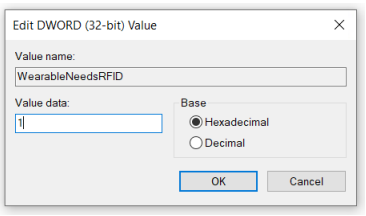
Purpose	Affected Components	Registry Setting
Prevent the appearance of the `Enterprise SSO` Login window for user who are not in the inclusion group.	All Evidian EAM Clients, including the Citrix/RDP servers. **Note:** Do not set this registry key with the Evidian EAM 10.03b8573 Hotfix 9 and later.	If the *Integrate with Windows Authentication* module is enabled and a generic account is not used for Windows login, set the following registry keys: Key #1: • **Location:** *HKLM\Software\Enatel\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***StopSSOEngineOnOTPFailed*** • **Value:** 1 Key #2: • **Location:**: *HKLM\Software\Enatel\WiseGuard\AdvancedLogin* • **Type:** DWORD 32-bit • **Name:** ***StartSSOEngine*** • **Value:** 1 If the *Integrate with Windows Authentication* and *Authentication Manager* modules are not enabled, set the following registry key: • **Location:**: *HKLM\Software\Enatel\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***DisplayErrorMessageAtStartup*** • **Value:** 0

7.4.1.6 - (Wearable Mode Only) Defining the Evidian EAM Client Registry Keys

The Nymi with Evidian Solution requires several registry keys on the Evidian EAM Clients to configure features and optimize performance.

After you define the registry keys, restart the Evidian Enterprise Access Management Security service on the computer.

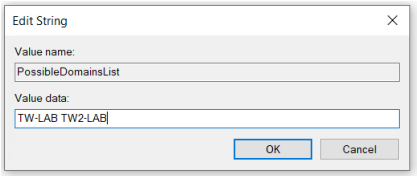
Purpose	Affected Components	Registry Setting
Required Registry Key Settings for the Nymi with Evidian Solution		

Purpose	Affected Components	Registry Setting
Configure the user terminal to prevent the SSO login screen from populating the username field with the user that logged into the user terminal.	All Evidian EAM Clients where users log into the user terminal with a generic account and when the work flows require sign offs by more than one user.	Create the following registry key • **Location:**: *HKLM\SOFTWARE\Enatel\WiseGuard\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name: *Allow4EyesAndSameUser*** • **Value: *1*** 
Prevent user self-enrollment of a Nymi Band and other NFC devices	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.	Create the following registry key: • **Location:** *HKLM\Software\Enatel\Wiseguard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name: *RFIDSelfEnrollAllowed*** • **Value: *0***
Prevent a user from logging into the machine by specifying a username without specifying a password, to avoid the situation where a user types the username of another user into the login window, and the other user is nearby an wearing an authenticated Nymi Band. The user can log in without requiring the password of the other user.	All Evidian EAM Clients where a user taps to login. **Note:** Do not set registry key with Evidian EAM 10.03b8573 Hotfix 12 and later. If you set this registry key with Evidian EAM 10.03b8573 Hotfix 12 and later, you cannot use the BLE Tap functionality.	Create the following registry key: • **Location:** *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name: *WearableNeedsRFID*** • **Value: *1*** 

Purpose	Affected Components	Registry Setting
Configure the Evidian EAM Client to avoid the use of the LsaLogonUser function and improve Nymi Band tap response times.	All Evidian EAM Clients, including Citrix/RDP servers and the enrollment terminal.	Create the following registry key: • **Location:** *HKLM\SOFTWARE\Enatel\WiseGuard\Framework\Directory* • **Type:** DWORD 32-bit • **Name:** ***CallLsaLogonUserAfterLogon*** • **Value:** ***0***
Enable the Evidian EAM Client to connect to Nymi Enterprise Server(NES)	All Evidian EAM Clients, including Citrix/RDP servers.	Create the following registry key on all Evidian EAM Clients, including Citrix/RDP servers. • **Location:** *HKLM\Software\Nymi\NES* • **Type:** String • **Name:** URL • **Value:** ***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.
Prevent the EAM client from retrieving Cloud-related configuration data.	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.	Create the following registry key: • **Location:**: *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Directory* • **Type:** DWORD (32-bit) • **Name:** ***GetCloudConfigDataOnlyInCloudMode*** • **Value:** ***1***
Registry Key Settings for Citrix/RDP environments		

Purpose	Affected Components	Registry Setting
Configure the Evidian EAM Client to communicate with the Nymi Agent server.	All Citrix/RDP servers	Create the following registry key: • **Location:** *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication* • **Type:** String • **Name:** ***NymiAgentUrl*** • **Value:** ***ws://agent_fdqn:9120/socket/websocket*** Where *agent_fdqn* is the Fully Qualified Domain Name of the centralized Nymi Agent server.
Configure Citrix roaming sessions, to ensure that when a published MES application closes, the Citrix session is logged off.	All Citrix servers	Create/Update the following registry keys: Registry Key #1 Edit the following registry key and append the following files to the ValueData field. • **Location:** *HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI* • **Type:** String • **Name:** ***LogoffCheckSysModules*** • **Value:** ***ssoengine.exe, ESSOCredentialManager.exe*** Registry Key #2 • **Location:** *HKLM\SOFTWARE\Policies\Enatel\SSOWatch\CommonConfig* or *HKLM\SOFTWARE\Enatel\SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***DoNotManageProcList*** • **Value:** ***1***
Use Case Specific Registry Key Settings		

Purpose	Affected Components	Registry Setting
Optimize NFC taps	All Evidian EAM Clients including Citrix/RDP servers and the enrollment terminal, where you perform Nymi Band taps on an NFC reader. **Note:** Ensure that you define these registry keys with Evidian EAM 10.03b8573 Hotfix 12 and later.	Key #1 • **Location:HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication** • **Type:** DWORD 32-bit • **Name:** ***NymiIntentDiscardNfc*** • **Value:** 0 Key #2 • **Location:HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication** • **Type:** DWORD 32-bit • **Name:** ***NymiIntentDiscardPcsc*** • **Value:** 1
When Integrate with Windows option is enabled on Windows 11 24H2	All Windows 11 24H2 Evidian EAM Clients.	• **Location:***HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*. • **Type:** DWORD 32-bit • **Name:** ***EnableMPR*** • **Value:** ***1*** **Note:** To push this change out through Group Policy Objects (GPO), this configuration is **`Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Logon Options`**. The setting name is *Configure the transmission of the user's password in the content of MPR notifications sent by winlogon*. To make this parameter available, you might require the *WinLogon.admx* from the Administrative Templates (.admx) for Windows 11 2024 Update (24H2), which you can obtain from Microsoft.

Purpose	Affected Components	Registry Setting
Support multiple domains, where users enroll their Nymi Bands in a domain that is different from the user terminal domain.	All Evidian EAM Clients including Citrix/RDP servers and the enrollment terminal.	Edit the *HKLM\Software\Enatel\WiseGuard\FrameWork\Directory\PossibleDomainList.* In the **`Value Data`** field, type the NETBIOS name for each domain that contains users, that will log in to the user terminal. **Note:** Separate each domain with a space, as shown in the following example. 
For use with DeltaV	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.	Create the following registry keys in *HKLM\Software\Enatel\SSOWatch\CommonConfig*: Key #1 • **Type:** DWORD 32-bit • **Name:** ***NoCacheFields*** • **Value:** ***1*** Key #2 • **Type:** DWORD 32-bit • **Name:** ***CheckUIAutomationFieldPresence*** • **Value:** ***2*** Key #3 • **Type:** DWORD 32-bit • **Name:** ***DoNotStopCustomScriptOnCancel*** • **Value:** ***1*** Key #4 • **Type:** DWORD 32-bit • **Name:** ***SupportMultipleDesktops*** • **Value:** ***1***

Purpose	Affected Components	Registry Setting
Set when the Integrate with Windows Authentication and Authentication Manager modules are not enabled on the client	All Evidian EAM Clients, including the enrollment terminal.	• **Location:***HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\SSOWatch \CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***DisplayErrorMessageAtStartup*** • **Value:** ***0***
Define list of Domain Controllers to contact for LDAP authentication processes. **Note:** Not required when you use LDAPS.		• **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\Directory* • **Type:** DWORD 32-bit • **Name:** ***ServerList*** • **Value:** ***fqdn1 fdqn2*** where: • *fqdn1* and *fqdn2* are the fully qualified domain names of the LDAP Directory Servers. For Example: srvad1.mycompany.lan srvad2.mycompany.lan **Note:** You can separate the server entries with a comma or space.

Purpose	Affected Components	Registry Setting
Prevent the appearance of the `Enterprise SSO` Login window for user who are not in the inclusion group.	All Evidian EAM Clients, including the Citrix/RDP servers. **Note:** Do not set this registry key with the Evidian EAM 10.03b8573 Hotfix 9 and later.	If the *Integrate with Windows Authentication* module is enabled and a generic account is not used for Windows login, set the following registry keys: Key #1: • **Location:** *HKLM\Software\Enatel \SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***StopSSOEngineOnOTPFailed*** • **Value:** 1 Key #2: • **Location:**: *HKLM\Software\Enatel \WiseGuard\AdvancedLogin* • **Type:** DWORD 32-bit • **Name:** ***StartSSOEngine*** • **Value:** 1 If the *Integrate with Windows Authentication* and *Authentication Manager* modules are not enabled, set the following registry key: • **Location:**: *HKLM\Software\Enatel \SSOWatch\CommonConfig* • **Type:** DWORD 32-bit • **Name:** ***DisplayErrorMessageAtStartup*** • **Value:** 0
LDAPS Registry Key Settings		

Purpose	Affected Components	Registry Setting
Support LDAPS for the communication with an AD LDS instance.	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers. **Note:** Requires Evidian Authentication Manager and Enterprise SSO 10.0 evolution 2 patch level 3 or later.	Create the following registry keys: Key #1 • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\WGDirectory* • **Type:** DWORD 32-bit • **Name:** ***SSL*** • **Value:** ***1*** Key #2 If some of your Active Directory(AD) Domain Controllers(DCs) do not use SSL or are not reachable, perform the following steps to define which AD DCs the Evidian software should use for LDAPS: • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\WGDirectory* • **Type:** DWORD 32-bit • **Name:** ***ServerList*** • **Value:** ***fqdn1:55001 fdqn2:55001*** where: • *fqdn1* and *fqdn2* are the fully qualified domain names of the LDAP Directory Servers. • *55001* is the LDAPS port number. For Example: srvad1.mycompany.lan:55001 srvad2.mycompany.lan:55001 **Note:** You can separate the server entries with a comma or space. Ensure that the *GSSEncryption* and *GSSSignature* registry keys are deleted in the following location: *HKEY_LOCAL_MACHINE\SOFTWARE \Enatel\WiseGuard\FrameWork \WGDirectory*

Purpose	Affected Components	Registry Setting
Support LDAPS for the communication with an Active Directory instance.	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers. **Note:** Requires Evidian Authentication Manager and Enterprise SSO 10.0 evolution 2 patch level 3 or later.	Create the following registry keys: Key #1 • **Location:** *HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\Directory* • **Type:** DWORD 32-bit • **Name:** ***SSL*** • **Value:** ***1*** Key #2 If some of your AD DCs do not use SSL or are not reachable, perform the following steps to define which AD DCs the Evidian software should use for LDAPS: • **Location:***HKEY_LOCAL_MACHINE \SOFTWARE\Enatel\WiseGuard \FrameWork\Directory* • **Type:** DWORD 32-bit • **Name:** ***ServerList*** • **Value:** ***fqdn1:port fdqn2:port*** where: • *fqdn1* and *fqdn2* are the fully qualified domain names of the LDAP Directory Servers. • *port* is the LDAPS port number and is not required if LDAPS communications occur over the default port 636. For Example: srvad1.mycompany.lan srvad2.mycompany.lan **Note:** You can separate the server entries with a comma or space. Ensure that the *GSSEncyption* and *GSSSignature* registry key values are set to 0 in the following location: *HKEY_LOCAL_MACHINE\SOFTWARE \Enatel\WiseGuard\FrameWork\Directory*
Performance and Security Registry Key Settings		

Purpose	Affected Components	Registry Setting
Increase the time that the Evidian EAM Client waits for the initialization of the *nymi_api.dll* and retrieval of authentication token from NES to complete.	All Evidian EAM Clients, including Citrix/RDP servers and the enrollment terminal.	Create the following registry key: • **Location:** *HKLM\Software\Enatel\Wiseguard\FrameWork\Authentication* • **Type:** DWORD 32-bit • **Name:** ***WearableDelay*** • **Value:** ***10000*** • **Base:** **`Decimal`**

Use Kerberos GSS Encryption to enhance the security of the component communications	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.
	Note: Do not set this registry key when you use LDAPS.
		Create or edit the following key:
		• **Location:**
		  • AD LDS Instances — *HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork\WGDirectory*
		  • AD Instances — *HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork\Directory*
		• **Type:** DWORD 32-bit
		• **Name:** ***GSSEncryption***
		• **Value:** ***1***

7.4.1.7 - 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.

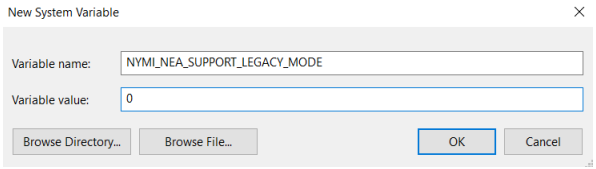


Figure 187: New System Variable window

   c) Click **OK**.

7.4.1.8 - (Wearable Mode Only) Replacing the Nymi DLL File

Replace the *nymi_api.dll* file that the Evidian EAM Client uses with Nymi Runtime version that you installed.

About this task

These steps apply to user terminals and Citrix servers/RDP session hosts in a wearable configuration only.

Procedure

1. Rename the *nymi_api.dll* in *C:\Program Files\Common Files\Evidian\WGSS*.
2. From Windows explorer, navigate to Nymi SDK installation package.
3. Copy the *..\nymi-sdk\windows\x86_64\nymi_api.dll* file to *C:\Program Files\Common Files\Evidian\WGSS*.

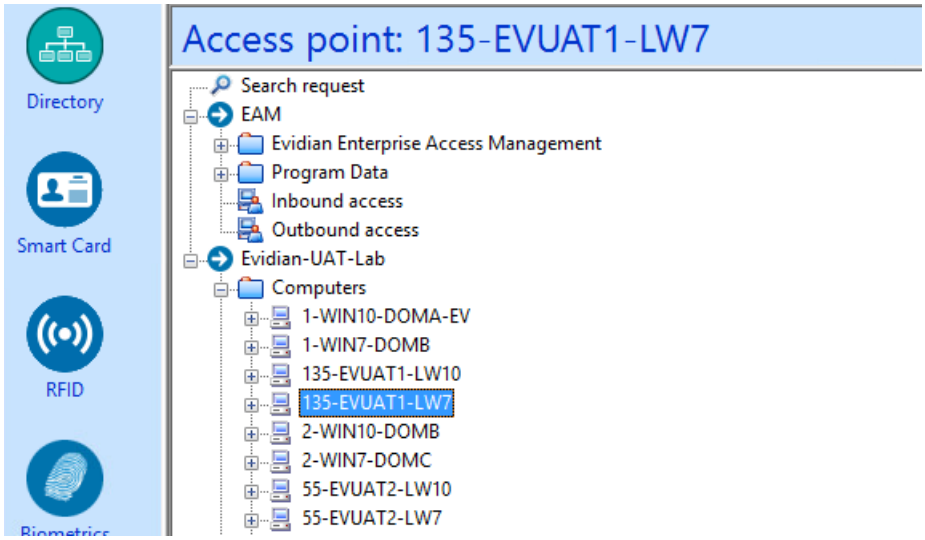
7.4.1.9 - Overriding the authentication method

In a mixed-mode environment, you must copy the appropriate the *TokenManagerStructure* file to each user terminal and Citrix Server/RDP session hosts that uses a non-default authentication mode.

Procedure

1. Obtain the appropriate TokenManagerStructure file, from the extracted Nymi installation software package that you downloaded. The file is located in the *Evidian-Supplementary-Files* subdirectory.
   - If wearable mode is your default authentication method, copy the *TokenManagerStructure-Nymi-Wearable.xml* file.
   - If RFID-only is your default authentication method, copy the *TokenManagerStructure-Nymi-RFID.xml* file.
2. Copy the TMS file to the *C:\Program Files\Common Files\Evidian\WGSS* directory.
3. Rename the file to *TokenManagerStructure.xml*.
4. Log in to the Evidian EAM Management Console.

5. Click **Account and access rights management**  .
6. In the left navigation pane, expand **Domain > Computers**, and then select the terminal, as shown in the following figure.



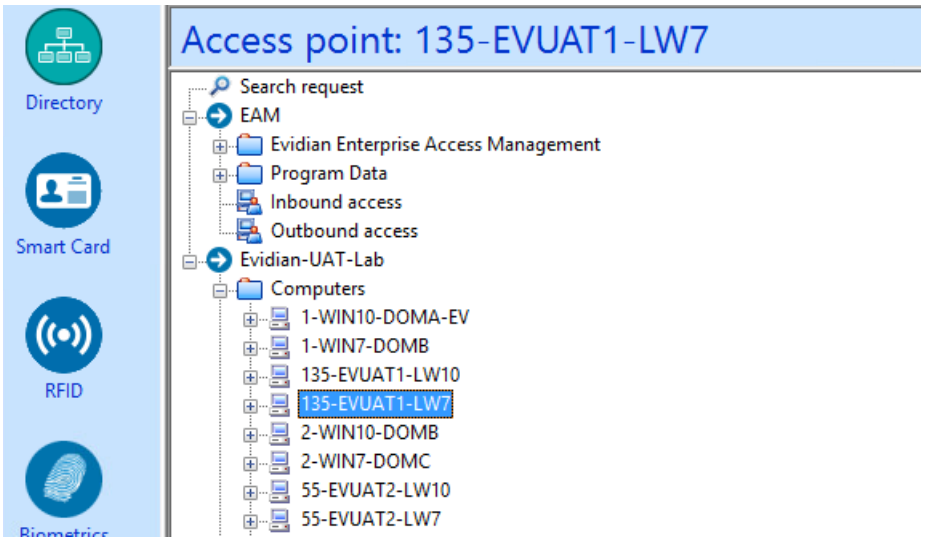
7. On the **Actions** tab, select **Delete cache files**, and then click **Apply**.
   The cache files are deleted on the terminal and the terminal desktop locks.

7.4.1.10 - Deleting Evidian EAM Client Cache

Perform the following steps to delete the cache files on the user terminal and the enrollment terminal.

Procedure

1. Log in to the Evidian EAM Management Console.
2. Click **Account and access rights management**  .
3. In the left navigation pane, expand **Domain > Computers**, and then select the terminal, as shown in the following figure.



4. On the **`Actions`** tab, select **`Delete cache files`**, and then click **`Apply`**.
   The cache files are deleted on the terminal and the terminal desktop locks.

7.4.1.11 - Using the Solution in Selective Trust Environments

Review this information for information about a multi-domain environment where there is a full trust from the client (computer) domain to the server (primary) domain, and a selective trust from the server (primary) domain to the client (computer) domain.

About this task

In a selective two-way trust:

- Primary domain trusts the Evidian EAM Client computers in the computer domain.
- Computer domain trusts the users and the Evidian EAM Controller/Nymi Enterprise Server(NES) in the primary domain.

To support SSO operations on the Evidian EAM Client computer, perform the following actions:

Procedure

1. On the user terminals, ensure that a service account on the primary domain runs the EAM security service.
2. On the user terminals, ensure that the service account has write permissions on the *HKLM \Software\Enatel* registry key.
3. In AD LDS, ensure that the service account has access privileges.
4. Ensure that the user logs into the user terminal with their account in the primary domain.

7.4.1.12 - Logging into the terminal

If you installed the Evidian SSOAgent with the Authentication Manager, when the terminal locks, the Windows login screen appears with new options.

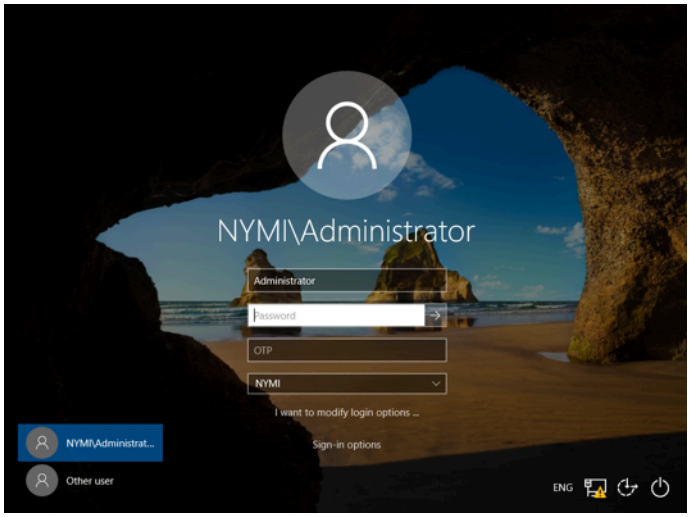
About this task

Perform the following steps to log in.

Note: On the first login, you cannot log in with a Nymi Band tap.

Procedure

1. Press Ctrl-Alt-Delete.
   The `Windows Login` screen appears with additional options. The following figure provides an example of the login screen.



2. Log in to the computer with your username and password.
   The desktop appears.

7.4.1.13 - Validating the Evidian EAM Client Installation

After you log into the computer, validate that the Evidian EAM Client can connect to the Evidian EAM Controller.

Open the system tray and confirm hover over the **`ESSO Credential Manager`** icon. Confirm that the status appears as **Connected Mode**, as shown in the following figure.

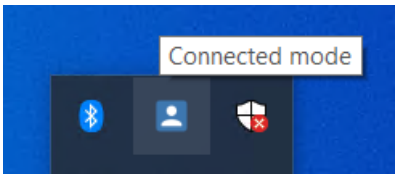


Figure 188: ESSO Credential Manager connected mode

If the status that appears is **Disconnected Mode**, the Evidian EAM Client cannot establish a connection with the Evidian EAM Controller, refer to the *Nymi Connected Worker Platform with Evidian Troubleshooting Guide* for more information.

7.4.1.14 - Updating User Account with new SSO Configuration

To enable a new user to use SSO and the Nymi Band with the Evidian-integrated application, refresh the Evidian Enterprise SSO application.

Before you begin

Install the application. If the application instructs you to copy the *nymi_api.dll* file to a directory location, ensure that you copy the version from the Nymi SDK distribution package.

About this task

Perform the following steps on each user terminal that accesses the application.

Procedure

1. In the Windows System Tray, click on the Enterprise SSO (eSSO) icon.
2. Click the **Home** icon, and then click **Refresh**, as shown in the following figure.

   The Evidian EAM Client contacts the Evidian EAM Controller to retrieve new technical definitions.

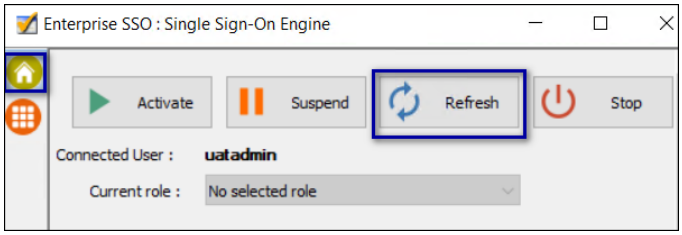


Figure 189: eSSO application Home Window

3. On the **Account** tab, a new entry appears. If the entry does not appear, right-click the table, and then clear the **Hide application without credential** option.

   The following figure shows the **Account** tab.

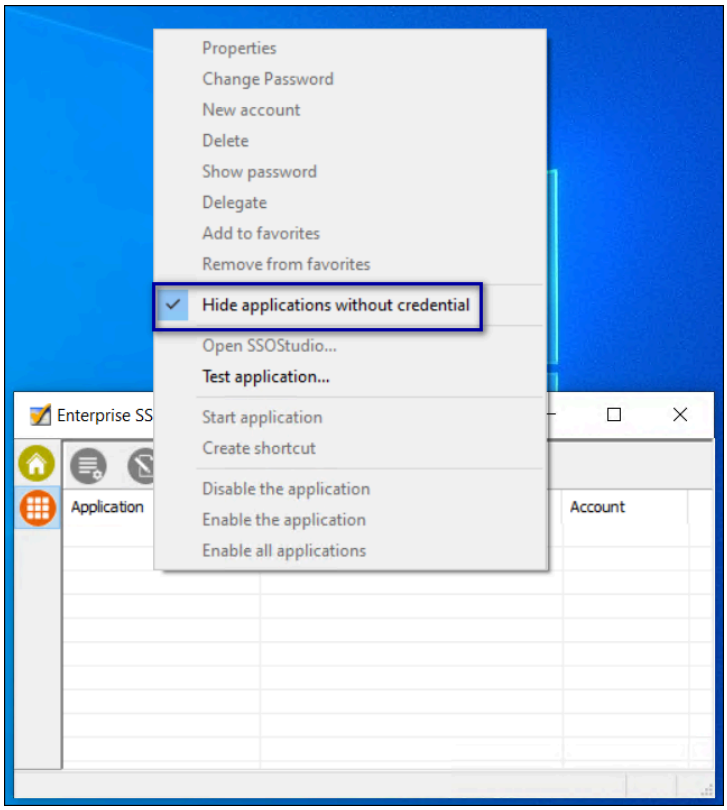


Figure 190: Enterprise SSO Account tab

4. Navigate to your login page of the application.
5. If your application uses credentials that are separate from the LDAP credentials or Windows login, the `Enterprise SSO – Security Data Collect` window appears. In the **`Username`** and **`Password`** fields, type the credentials that are required by the application, and the click **`OK`**.

   The following figure provides an example of the login screen

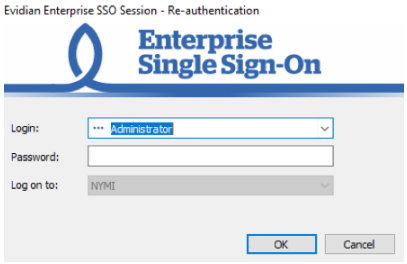


Figure 191: SSO Login screen

6. Close the Evidian Enterprise SSO application.
   For wearable-mode, the user can tap their Nymi Band to complete authentication events in the Evidian-integrated application.

   For NFC-only mode, the user must type their username and password the first time that they see the Evidian Enterprise SSO window on a user terminal, to create a roaming session. After the first manual sign on, the user can tap their Nymi Band to complete authentication tasks.

Results

Note: Sometimes it may take several attempts to get the behaviour of the detect to work as desired. To update the configuration, on the User Terminal you can modify the Detection tab to be more generic using wildcards, or more specific using regex detection. Detection is application-specific. Depending upon your application, you may need to modify settings that are not specified in this document.

If you change the technical definition at a later time, you must right-click the technical definition and select **`Update Directory`** and delete the Evidian cache.

7.4.1.15 - (IGEL Only) Handling Slow Tap Response in Remote Session

In some scenarios users might experience delayed responses to Nymi Band taps on an NFC reader in a Nymi-Evidian configuration.

To resolve this issue, on the IGEL edit the *All_Regions.ini* file and decrease the value defined for the `ReadersStatusPollPeriod` variable.

8 - Updating Nymi and Evidian Components

The Connected Worker Platform provides enhancements that support coexistence of Evidian-integrated applications and Nymi-enabled Applications.

The section describes how to update the components in the Nymi with Evidian Solution.

8.1 - Updating the NES Software

Update the NES according to the instructions in the *Nymi Connected Worker Platform—Deployment Guide*.

If you update from NES 3.3.1 or earlier, perform the following steps to update the active policy to support Evidian enrollments.

1. Log in to the NES Administrator Console with an account that is an NES Administrator.
2. Click **`Policies`**.
3. Edit the active policy.
4. From the **`Enrollment / Registration Destination`** list, select the option **`NES and Evidian`**, as shown in the following figure, and then click **`Save`**.

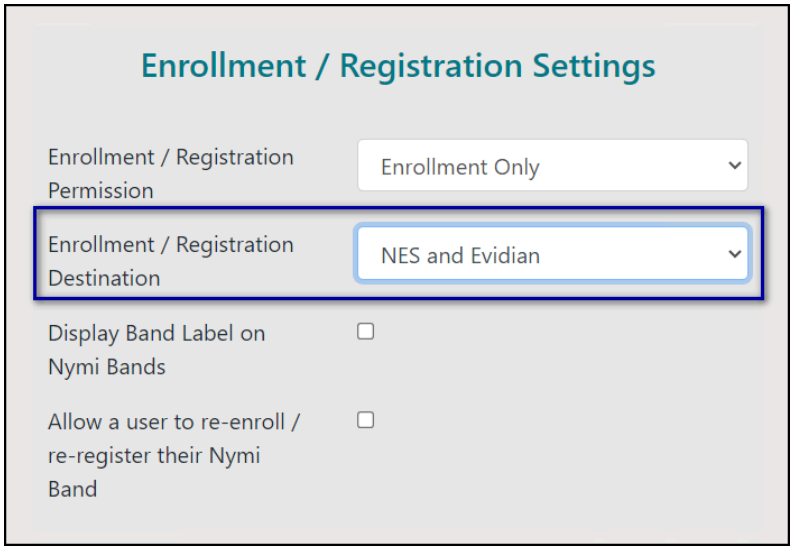


Figure 192: NES and Evidian enrollment option

Note: In CWP 1.17.0 and earlier the list name is **`Enrollment Destination`**.

8.1.1 - (Updates from NEE 3.3.1 and earlier only) Modifying EAM Settings to Support Coexistence with other Solutions

By default, when an Evidian-integrated application is not waiting for an SSO operation and a user performs a tap, the desktop locks.

About this task

If user terminals need to simultaneously support Evidian-integrated applications and Nymi-integrated MES applications, perform the following steps in the Evidian EAM Management Console to modify the settings in the access point profile, to prevent unexpected desktop locks when performing a Nymi Band tap in the Nymi-integrated MES application.

Procedure

1. In the `Directory` view, expand **`EAM > Evidian Enterprise Access Management > User Access > AccessPoint Profiles > Default Access Point Profile`**.
2. On the **`Authentication Manager`** tab, from the **`Default action when token removed`** list, select **`Do nothing`**.
3. Click **`Apply`**.
4. Right-click **`Default Access Point Profile`** and select **`Update`**.

Results

A user cannot perform an tap to lock the Windows session; however, the Windows session still locks when the Nymi Band deauthenticates or when the user is away from the user terminal.

8.2 - Update the Evidian EAM Controller

Update the Evidian EAM Controller software on each Evidian server in the environment.

LDAPS Considerations

In an LDAPS configuration, you must temporarily revert to LDAP before you start the Evidian software update. Perform the following steps on the Evidian EAM Controller.

1. Open Registry Editor and navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork \WGDirectory* .
2. Edit **`ServerList`**, and in the **`ValueData`** field, change the port number from ***50001*** to ***55000***.
3. Edit **`SSL`**, and in the **`ValueData`** field, change the value from ***1*** to ***0***.

   The following figure provides an example of changes in the *WGDirectory*.

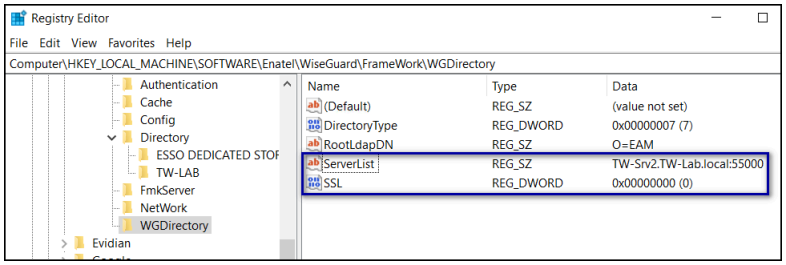


Figure 193: WGDirectory changes

4. Restart the *Enterprise Access Management Security Services* service.

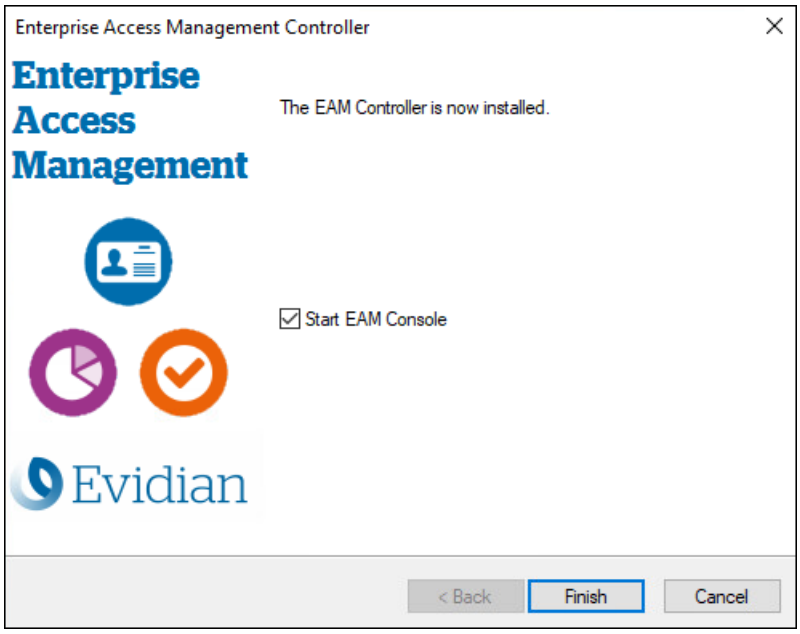
8.3 - Updating the Evidian EAM Controller

Perform the following steps to update the Evidian EAM Controller software.

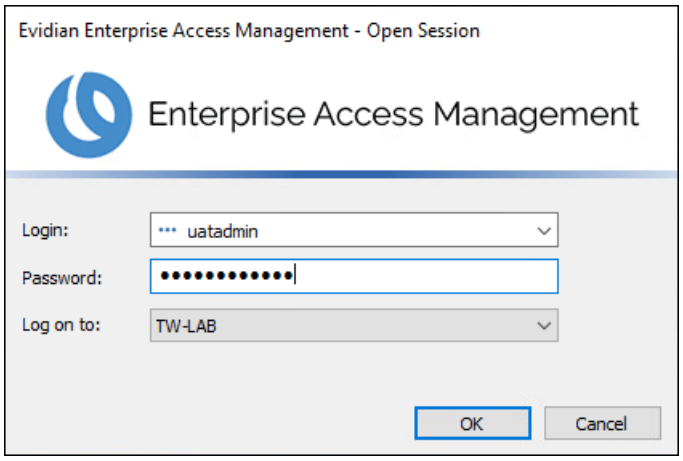
Procedure

1. Log in to the server as a local administrator.
2. Download and extract the Evidian software package, *EAM-v10.0x.xxxxxxx.zip* to a directory on the server, (for example, the *Downloads* directory).
3. Double-click the *C:\Downloads\EAM-v10.0xxxxxx.xx\EAM.x64\INSTALL \ESSOcontroller.msi* file.
4. On the `Windows protected your PC`, window, click **`More info`**, and then click **`Run anyway`**.
5. On the `Welcome to the EAM Controller installation assistant` window, click **`Next`**.
6. On the `License keys` window, click **`Next`**.
7. On the `Directory` window, click **`Next`**.
8. On the `Audit database server` window, click **`Next`**.
9. On the On the `Secrets Initialization` window, click **`Next`**.
10. On the `Authentication methods` window, click **`Next`**.
11. On the `Software installation` window, click **`Next`**.

    The Windows Installer window appears, and the installation process begins.
12. On the window that displays **`The EAM Controller is now installed`**, select **`Start EAM Console`**, as shown in the following figure, and then click **`Finish`**.



13. Optional - for LDAPS deployments only, perform the following steps to change the configuration back to LDAPS:
    a. Open Registry Editor and navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork \WGDirectory* .
    b. Edit **`ServerList`**, and in the **`ValueData`** field, change the port number from ***55000*** to ***55001***.
    c. Edit **SSL**, and in the **`Data Value`** field, change the value from ***0*** to ***1***.
    d. Restart the *Enterprise Access Management Security Service* service.
14. Replace the *nymi_api.dll* file:
    a. Rename the *nymi_api.dll* in *C:\Program Files\Common Files\Evidian\WGSS*.
    b. In Windows explorer, navigate to Nymi SDK installation package.
    c. Copy the *..\nymi-sdk\windows\x86_64\nymi_api.dll* file to *C:\Program Files\Common Files \Evidian\WGSS*.
    d. Restart the *Enterprise Access Management Security Services* service.
15. On the `Evidian Enterprise Access Management – Open Session` window, type your login and password and then select the domain to which you want to log on, as shown in the following figure. Click **`OK`**.



Results

The Evidian EAM Management Console appears.

8.3.1 - (Updates from CWP 1.15.X and earlier only) Updating the TokenManagerStructure

The Connected Worker Platform software package includes new TokenManagerStructure(TMS) files that support wearable and RFID authentication methods. When you update Connected Worker Platform components from Nymi Enterprise Edition, Nymi recommends that you replace any TokenManagerStructure file that you placed on a terminal to override the Evidian EAM Controller configuration, and the configuration on the Evidian EAM Controller.

About this task

The Evidian Supplementary Files directory in the Connected Worker Platform software package includes the following TMS files:

- *TokenManagerStructure-WEARABLE.xml*-To configure Nymi Bands to use wearable authentication.
- *TokenManagerStructure-RFID.xml*-To configure Nymi Bands to use RFID authentication.

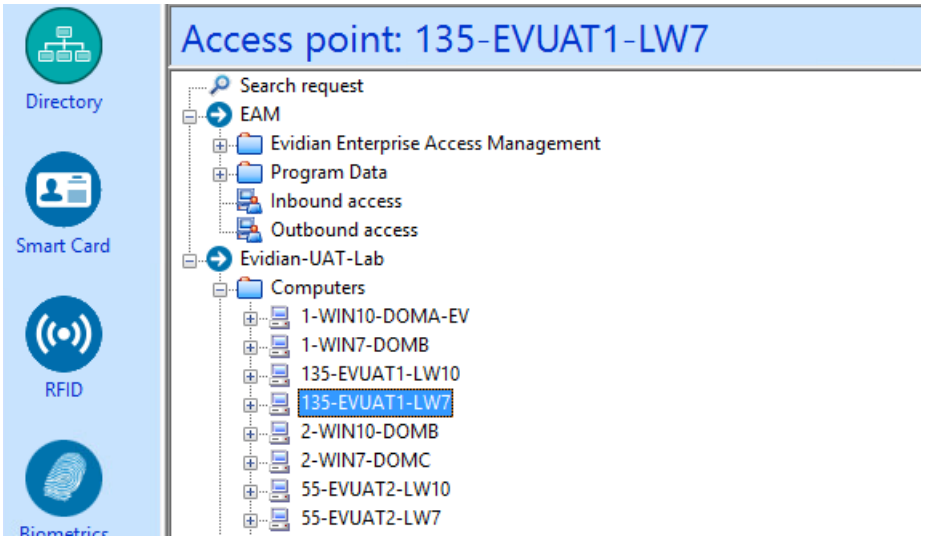
Perform the following steps to replace the TMS configuration in your environment.

Procedure

1. Log in to the Evidian EAM Management Console as an EAM Administrator.
2. From the **`File`** menu, select **`Configuration`**.
3. On the **`Authentication`** tab, click **`Select`**, and then select the appropriate TMS file for your configuration.
4. Click **`Apply`**.

5. Click **OK**.
6. Launch **Services**.
7. Stop the Enterprise Access Management Security Services service.
8. Delete all files under *C:\Program Files\Common Files\Evidian\WGSS\CacheDir*.

   Note: If you get a message that you cannot delete the files, hold the **Shift** key down when you press **Delete**.
9. Start Enterprise Access Management Security Services service.
10. For each terminal in the environment that overrides the Evidian EAM Controller authentication configuration, perform the following steps:
    a) Log in to the terminal.
    b) Rename the *TokenManagerStructure.xml* file in the *C:\Program Files\Common\Evidian\WGSS* directory.
    c) Copy the new TMS file from the Connected Worker Platform package into the *C:\Program Files\Common\Evidian\WGSS* directory.
    d) Rename the TMS file to *TokenManagerStructure.xml*.
11. Log in to the Evidian EAM Management Console.
12. Click **Account and access rights management**  .
13. In the left navigation pane, expand **Domain > Computers**, and then select the terminal, as shown in the following figure.



14. On the **Actions** tab, select **Delete cache files**, and then click **Apply**.
    The cache files are deleted on the terminal and the terminal desktop locks.

8.4 - Update the Centralized Nymi Agent

Perform the following steps if your environment uses a centralized Nymi Agent.

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.

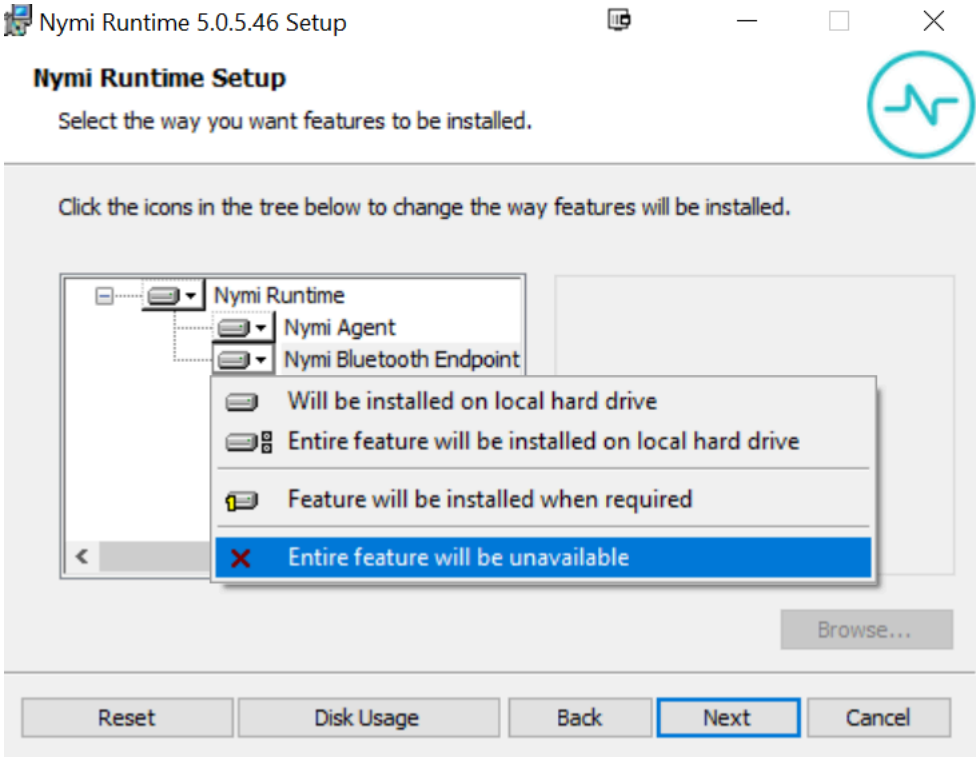


Figure 194: Nymi Bluetooth Endpoint feature will be unavailable

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

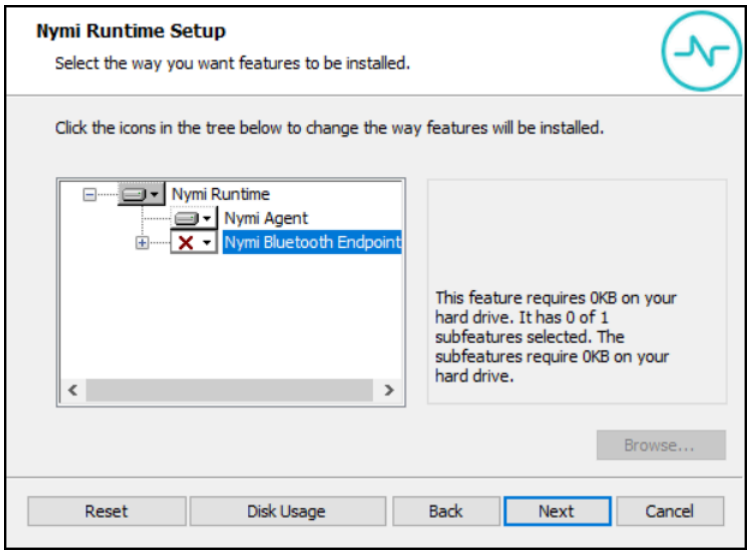


Figure 195: Nymi Bluetooth Endpoint feature is not available

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\LocalService, 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.

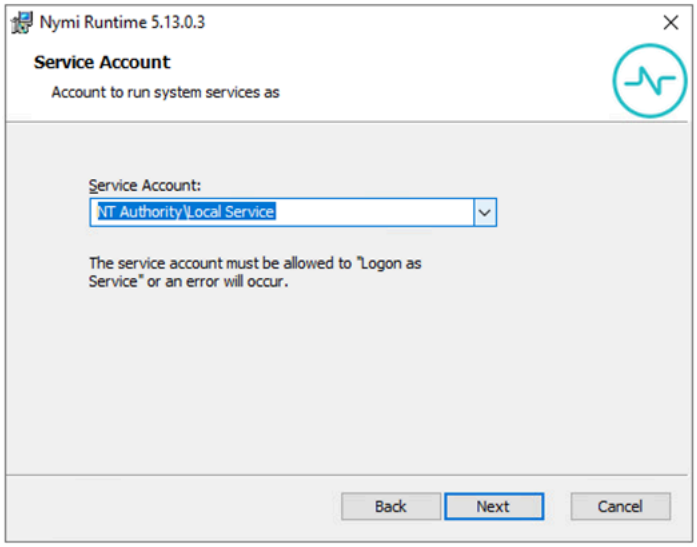


Figure 196: Nymi Runtime Service Account window

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.

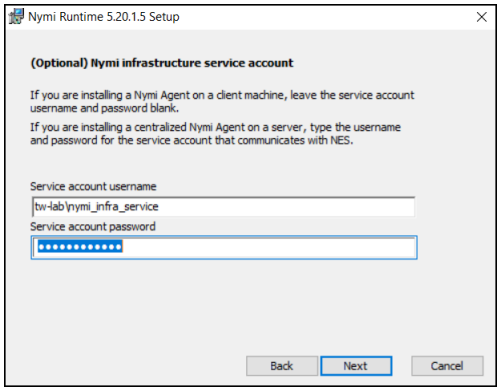


Figure 197: Nymi Infrastructure Service Account window

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`**.

8.5 - Update the Enrollment Terminal

On the Enrollment Terminal, update the Nymi Band Application, the Evidian EAM Client and replace the *nymi_api.dll* file.

8.5.1 - Updating the Nymi Band Application

An update of the Nymi Band Application does not require you to remove the previous version of the software.

About this task

Perform the following steps on the enrollment terminal.

Procedure

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

8.5.2 - Updating Registry Key Settings

Review the registry key settings on the enrollment terminal and update as required.

Procedure

1. Run Registry Editor.
2. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication* and then delete the *WearableNeedsRFID* registry key.
3. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Directory*, and then create a new **`DWORD (32-bit) Value`** named *GetCloudConfigDataOnlyInCloudMode*.
4. Edit the *GetCloudConfigDataOnlyInCloudMode* key, and in the **`Value data`** field type ***1***. Click **`OK`**.
5. Close Registry Editor.

8.5.3 - Updating the Evidian SSO Agent

Perform the following steps with an account that has permission to install software on the machine.

About this task

Obtain the Evidian software package from Nymi Solution Consultant or Nymi Support.

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\VCRedist_x64.msi*.

   Note: If the required version of Microsoft Visual C++ redistributable is already installed on the server, a pop-up screen briefly appears, and then disappears.
2. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\ESSOAgent.msi* file.
3. On the `Enterprise Access Management Client Installation`, click **`Next`**.
4. On the `License Agreement` window, click **`I accept the license agreement`**, and then click **`Next`**.

   The following figure shows the `License Agreement` window.

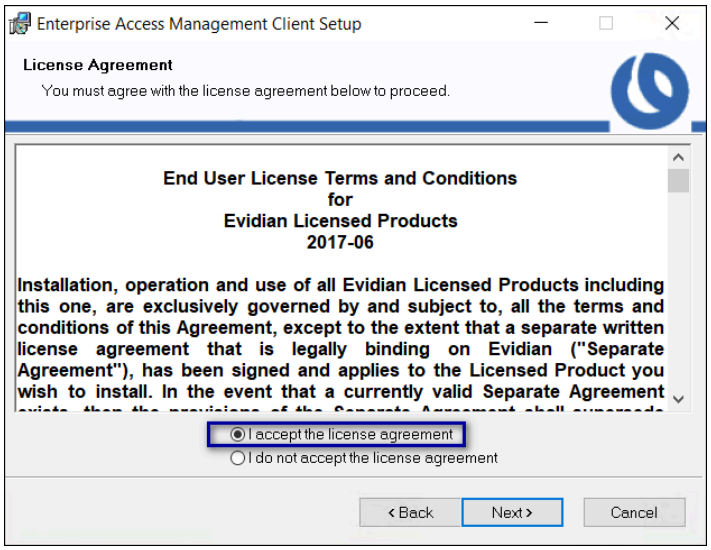


Figure 198: License Agreement window

5. On the `Destination Folder` window, accept the default, and then click **`Next`**.

   The following figure shows the `Destination Folder` window.

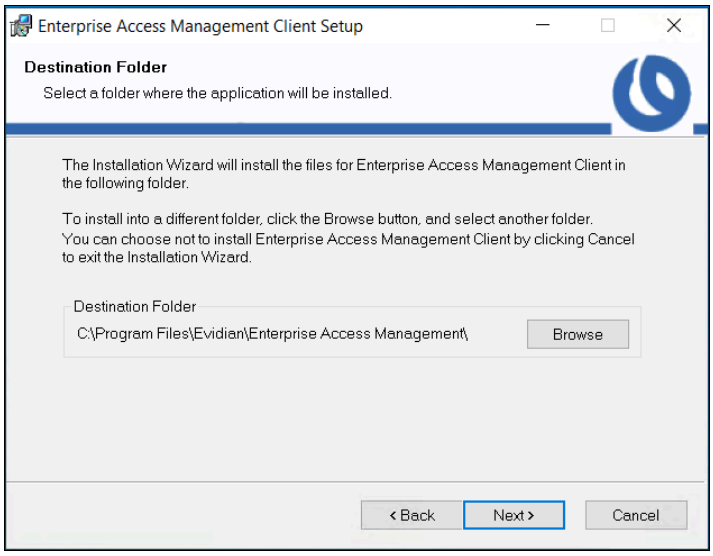


Figure 199: Destination Folder window

6. On the `Select Installation Type` window, select **`Custom`**, and then click **`Next`**.
   The following figure shows the `Select Installation Type` window.

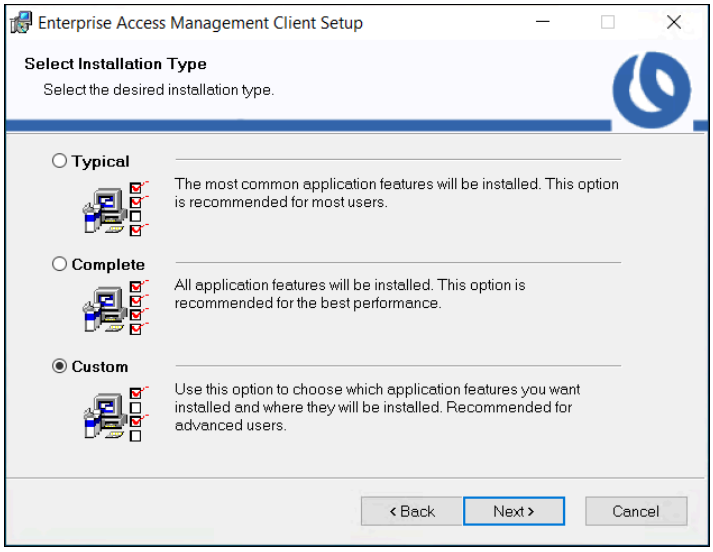


Figure 200: Select Installation Type window

7. On the **`Select Features`** window, click **`Next`**.
   The **`Select Features`** window contains the existing configuration options.
8. On the `Ready to install the application` window, click **`Next`**, as shown in the following figure.

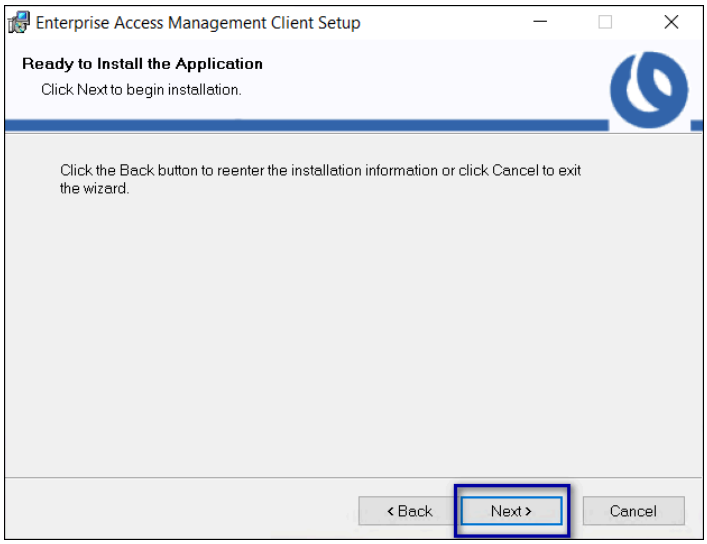


Figure 201: Ready to install the application

9. On the `User account control` pop-up, click **`Yes`**, as shown in the following figure.

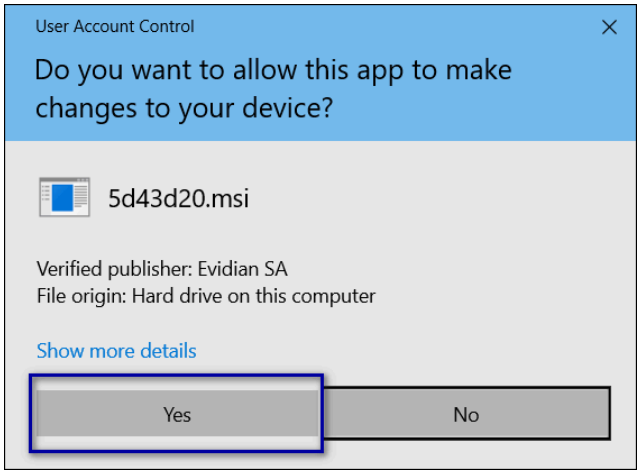


Figure 202: User account control

10. On the `Enterprise Access Management Client has been successfully installed` window, click **`Finish`**, as shown in the following figure.

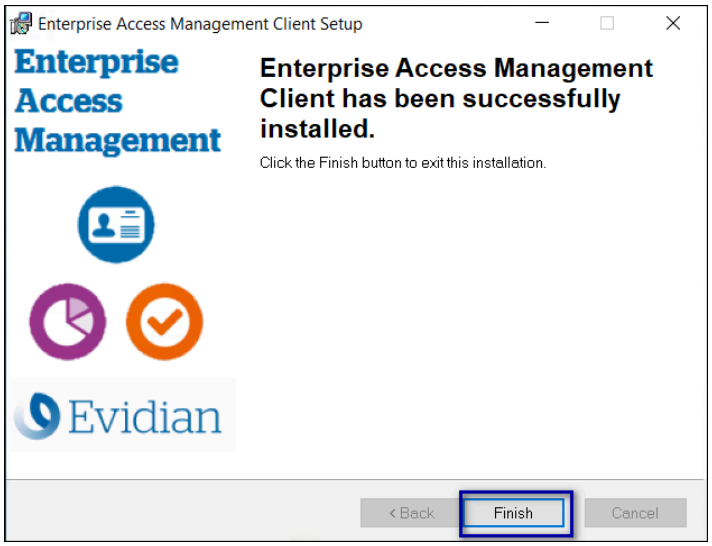


Figure 203: Evidian Client Installation Success window

8.5.4 - Confirming the Runtime dll versions

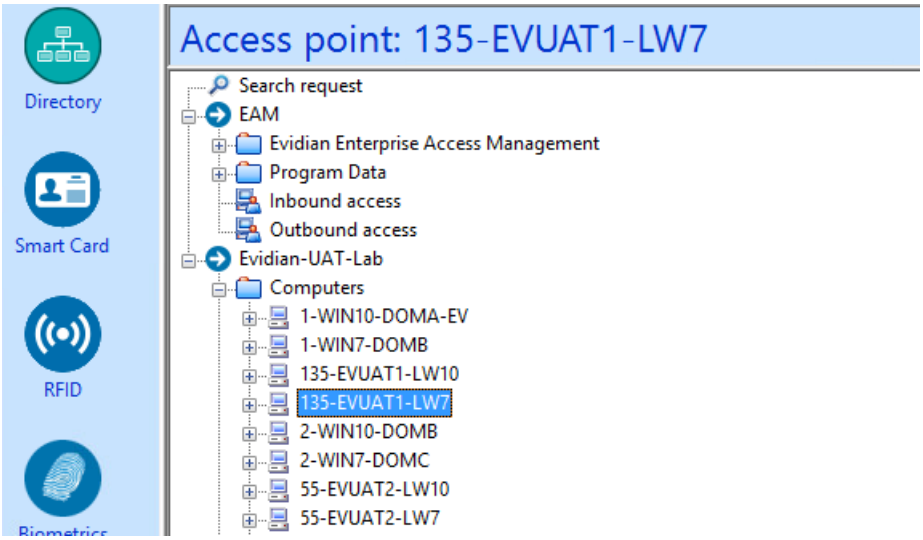
Review the Connected Worker Platform and Evidian EAM Client versions of the Nymi Runtime file to ensure that they are the same.

About this task

Perform the following steps on the client machine.

Procedure

1. From the `Windows Apps and Feature` applet, search for the Nymi Runtime application and make note of the version.
2. From Windows explorer, navigate to *C:\Program Files\Common Files\Evidian\WGSS*.
3. Right-click *nymi_api.dll* and select **`Properties`**. On the **`Details`** tab, confirm that the value in the product version matches the Nymi Runtime installation.
4. If the versions do not match, perform the following steps:
   a) Rename the *nymi_api.dll* in *C:\Program Files\Common Files\Evidian\WGSS*.
   b) Copy the *C:\Program Files\Nymi\Nymi Band Application\nymi_api.dll* to *C:\Program Files \Common Files\Evidian\WGSS*.
5. Log in to the Evidian EAM Management Console.
6. Click **`Account and access rights management`**  .
7. In the left navigation pane, expand **`Domain > Computers`**, and then select the terminal, as shown in the following figure.



8. On the **Actions** tab, select **Delete cache files**, and then click **Apply**.
   The cache files are deleted on the terminal and the terminal desktop locks.

8.5.5 - 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.

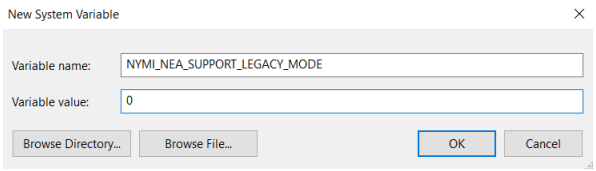


Figure 204: New System Variable window

   c) Click **OK**.

8.6 - Update Wearable User Terminals

Update the Nymi Runtime, the Evidian EAM Client and the *nymi_api.dll* file on each user terminal.

8.6.1 - Updating Nymi Runtime

Update the Nymi Runtime on the user terminal and RDP/Citrix servers that use a wearable configuration.

About this task

Perform the following steps after internal testing has verified the compatibility of the NEA with upgraded versions of the Nymi Components.

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` window, click **`Next`**.
8. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
   - Accept the default service account NTAuthority\LocalService, click **`Next`**.
   - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.
9. 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.
10. On the `Ready to install` page, click **`Install`**.
11. Click **`Finish`**.
12. On the `Installation Completed Successfully` page, click **`Close`**.
13. Replace the *nymi_api.dll* file that is used by the MES application with the version of the file that is in the Nymi API C Interface distribution package.

8.6.2 - Updating Registry Key Settings

Review the registry key settings on the user terminal and update as required.

Procedure

1. Run Registry Editor.
2. Navigate to *HKLM\Software\Enatel\SSOWatch\CommonConfig*, and then delete the *StopSSOEngineOnOTPFailed* registry key.
3. Navigate to *HKLM\Software\Enatel\WiseGuard\AdvancedLogin*, and then delete the *StartSSOEngine* registry key.
4. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Directory*, and then create a new **`DWORD (32-bit) Value`** named *GetCloudConfigDataOnlyInCloudMode*.
5. Edit the *GetCloudConfigDataOnlyInCloudMode* key, and in the **`Value data`** field type ***`1`***. Click **`OK`**.
6. Close Registry Editor.

8.6.3 - Updating the Evidian SSO Agent

Perform the following steps with an account that has permission to install software on the machine.

About this task

Obtain the Evidian software package from Nymi Solution Consultant or Nymi Support.

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\VCRedist_x64.msi*.

   Note: If the required version of Microsoft Visual C++ redistributable is already installed on the server, a pop-up screen briefly appears, and then disappears.
2. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\ESSOAgent.msi* file.
3. On the `Enterprise Access Management Client Installation`, click **`Next`**.
4. On the `License Agreement` window, click **`I accept the license agreement`**, and then click **`Next`**.

   The following figure shows the `License Agreement` window.

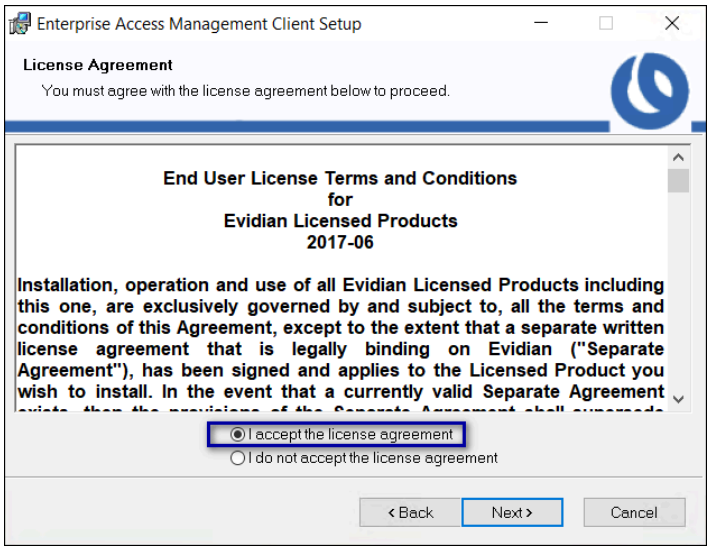


Figure 205: License Agreement window

5. On the `Destination Folder` window, accept the default, and then click **`Next`**.

   The following figure shows the `Destination Folder` window.

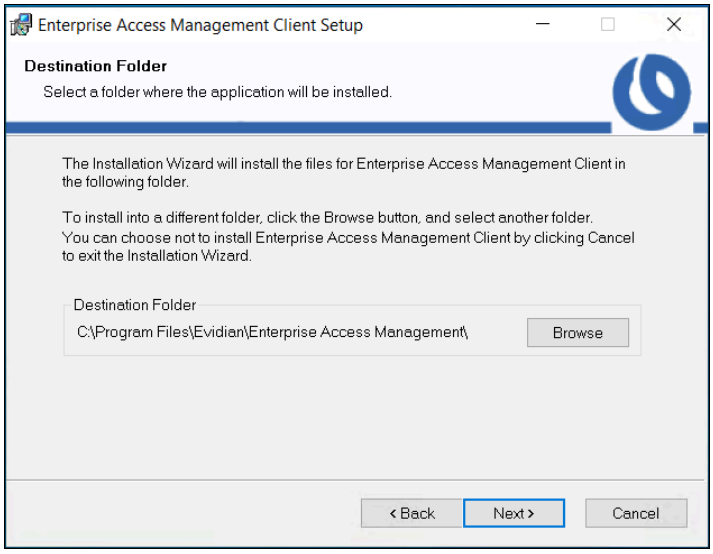


Figure 206: Destination Folder window

6. On the `Select Installation Type` window, select **`Custom`**, and then click **`Next`**.

   The following figure shows the `Select Installation Type` window.

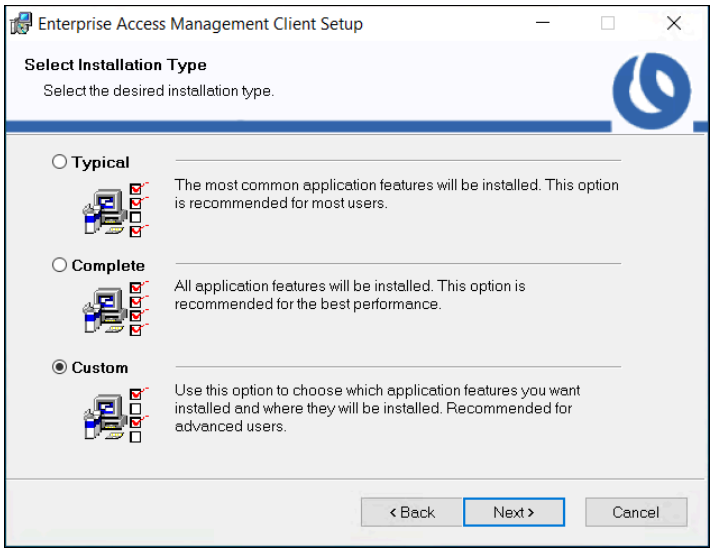


Figure 207: Select Installation Type window

7. On the **`Select Features`** window, click **`Next`**.

   The **`Select Features`** window contains the existing configuration options.

8. On the `Ready to install the application` window, click **`Next`**, as shown in the following figure.

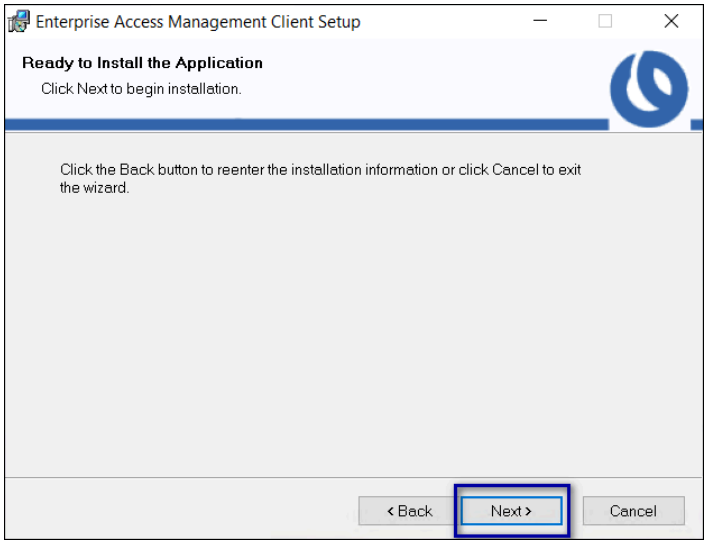


Figure 208: Ready to install the application

9. On the `User account control` pop-up, click **`Yes`**, as shown in the following figure.

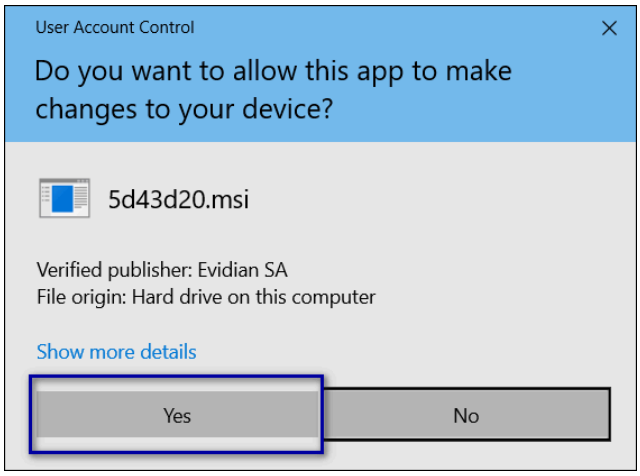


Figure 209: User account control

10. On the `Enterprise Access Management Client has been successfully installed` window, click **`Finish`**, as shown in the following figure.

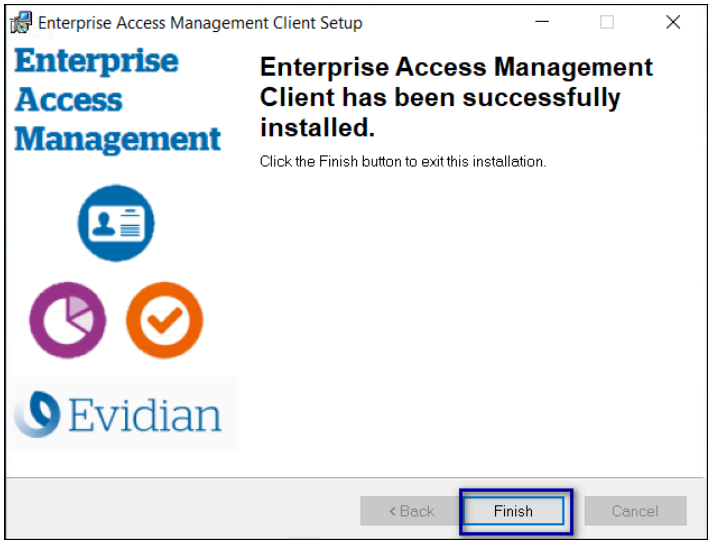


Figure 210: Evidian Client Installation Success window

8.6.4 - 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.

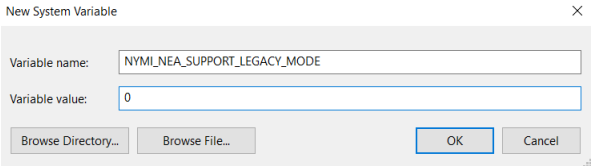


Figure 211: New System Variable window

   c) Click **`OK`**.

8.6.5 - Optimizing NFC Taps

The Evidian Access Management version EAM-v10.03b8573.4 optimizes the Evidian EAM Client configuration for Nymi Band taps on a Bluetooth adapter by default.

About this task

When you use an NFC reader to perform Nymi Band taps, perform the following steps on each Citrix or RDP server.

Note: EAM-v10.03b8573.4 does not support use cases that require Authentication Manager.

Procedure

1. Run *regedit.exe*.
2. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication*.
3. Create a new DWord(32-bit) key named **`NymiIntentDiscardNfc`**.
4. Edit **`NymiIntentDiscardNfc`**, change the value in the **`Value data`** field to ***0***, and then click **`OK`**.
5. Create a new DWord(32-bit) key named **`NymiIntentDiscardPcsc`**. Leave the default value ***1***.
6. Close `Registry Editor`.
7. Restart the `Enterprise Access Management Security Services` service.

8.6.6 - Confirming the Runtime dll versions

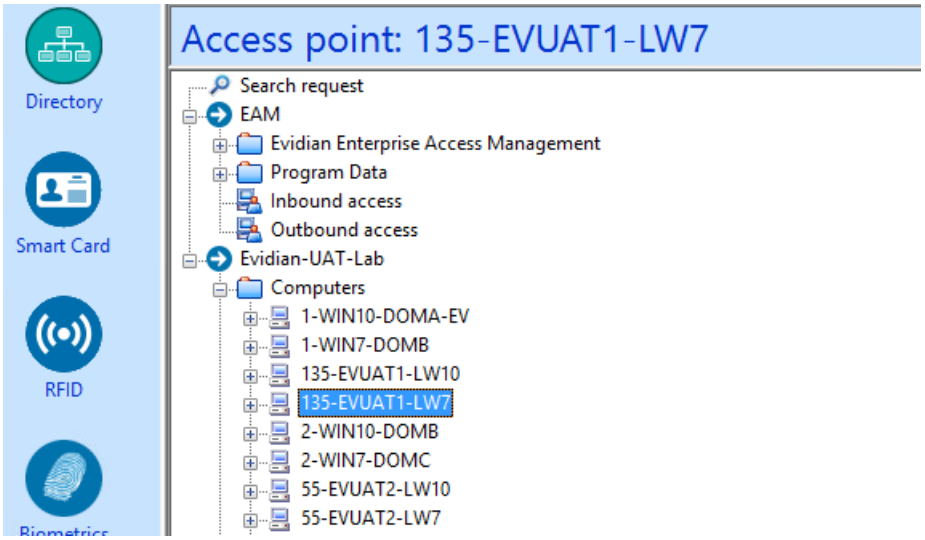
Review the Connected Worker Platform and Evidian EAM Client versions of the Nymi Runtime file to ensure that they are the same.

About this task

Perform the following steps on the client machine.

Procedure

1. From the `Windows Apps and Feature` applet, search for the Nymi Runtime application and make note of the version.
2. From Windows explorer, navigate to *C:\Program Files\Common Files\Evidian\WGSS*.
3. Right-click *nymi_api.dll* and select **`Properties`**. On the **`Details`** tab, confirm that the value in the product version matches the Nymi Runtime installation.
4. If the versions do not match, perform the following steps:
   a) Rename the *nymi_api.dll* in *C:\Program Files\Common Files\Evidian\WGSS*.
   b) Copy the *C:\Program Files\Nymi\Nymi Band Application\nymi_api.dll* to *C:\Program Files \Common Files\Evidian\WGSS*.
5. Log in to the Evidian EAM Management Console.
6. Click **`Account and access rights management`**  .
7. In the left navigation pane, expand **`Domain > Computers`**, and then select the terminal, as shown in the following figure.



8. On the **`Actions`** tab, select **`Delete cache files`**, and then click **`Apply`**.
   The cache files are deleted on the terminal and the terminal desktop locks.

8.7 - Update RFID-only User Terminals

Update the Evidian EAM Client on each user terminal that is in an RFID-only configuration.

8.7.1 - Updating Registry Key Settings

Review the registry key settings on the user terminal and update as required.

Procedure

1. Run Registry Editor.
2. Navigate to *HKLM\Software\Enatel\SSOWatch\CommonConfig*, and then delete the *StopSSOEngineOnOTPFailed* registry key.
3. Navigate to *HKLM\Software\Enatel\WiseGuard\AdvancedLogin*, and then delete the *StartSSOEngine* registry key.
4. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Directory*, and then create a new **`DWORD (32-bit) Value`** named *GetCloudConfigDataOnlyInCloudMode*.
5. Edit the *GetCloudConfigDataOnlyInCloudMode* key, and in the **`Value data`** field type ***1***. Click **`OK`**.
6. Close Registry Editor.

8.7.2 - Updating the Evidian SSO Agent

Perform the following steps with an account that has permission to install software on the machine.

About this task

Obtain the Evidian software package from Nymi Solution Consultant or Nymi Support.

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\VCRedist_x64.msi*.

   Note: If the required version of Microsoft Visual C++ redistributable is already installed on the server, a pop-up screen briefly appears, and then disappears.
2. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\ESSOAgent.msi* file.
3. On the `Enterprise Access Management Client Installation`, click **`Next`**.
4. On the `License Agreement` window, click **`I accept the license agreement`**, and then click **`Next`**.

   The following figure shows the `License Agreement` window.

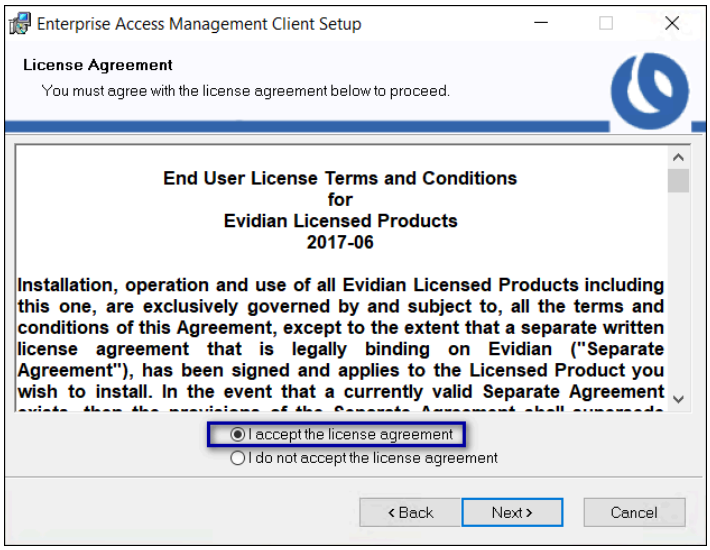


Figure 212: License Agreement window

5. On the `Destination Folder` window, accept the default, and then click **`Next`**.

   The following figure shows the `Destination Folder` window.

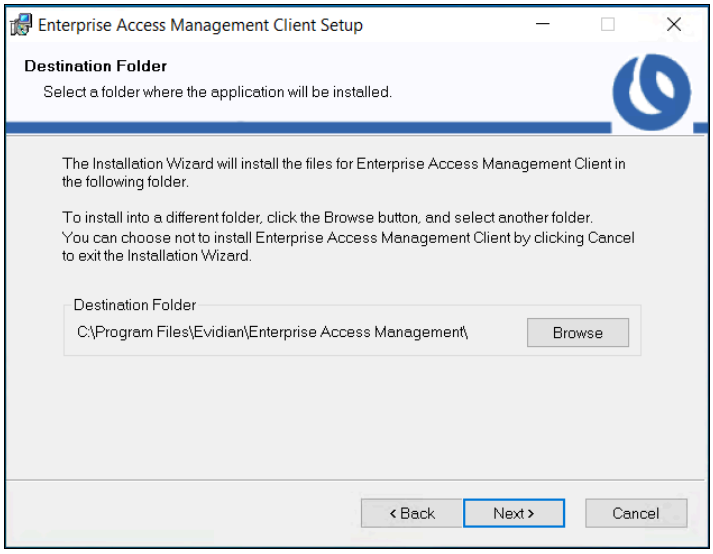


Figure 213: Destination Folder window

6. On the `Select Installation Type` window, select **`Custom`**, and then click **`Next`**.

   The following figure shows the `Select Installation Type` window.

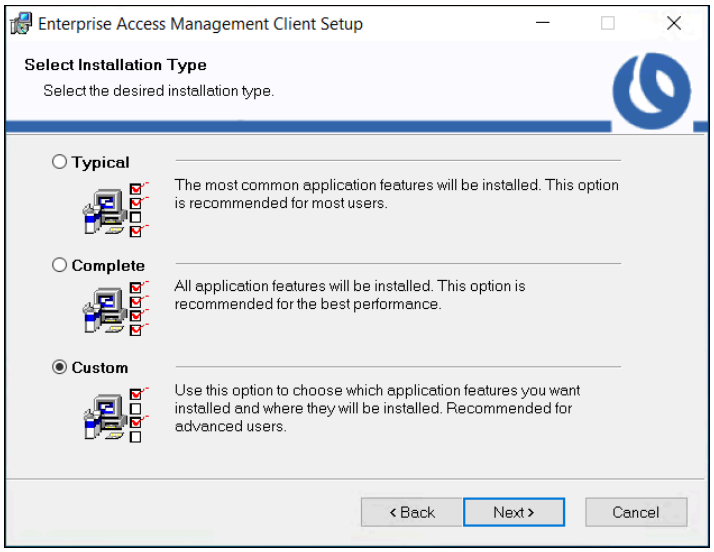


Figure 214: Select Installation Type window

7. On the **`Select Features`** window, click **`Next`**.

   The **`Select Features`** window contains the existing configuration options.

8. On the `Ready to install the application` window, click **`Next`**, as shown in the following figure.

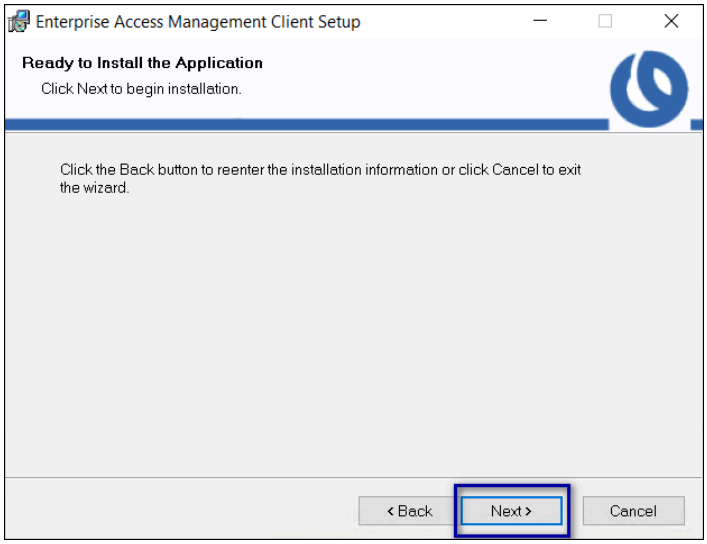


Figure 215: Ready to install the application

9. On the `User account control` pop-up, click **`Yes`**, as shown in the following figure.

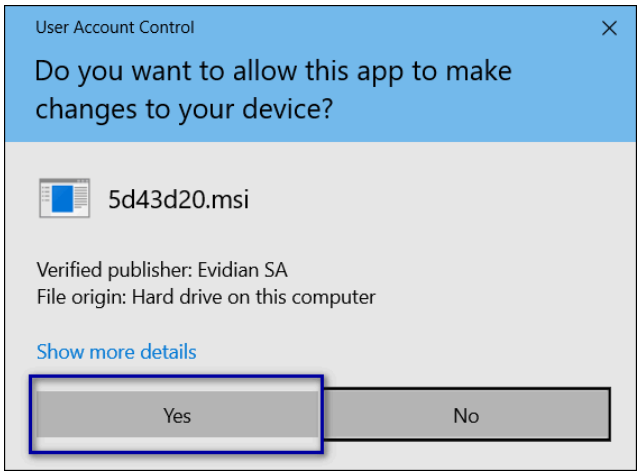


Figure 216: User account control

10. On the `Enterprise Access Management Client has been successfully installed` window, click **`Finish`**, as shown in the following figure.

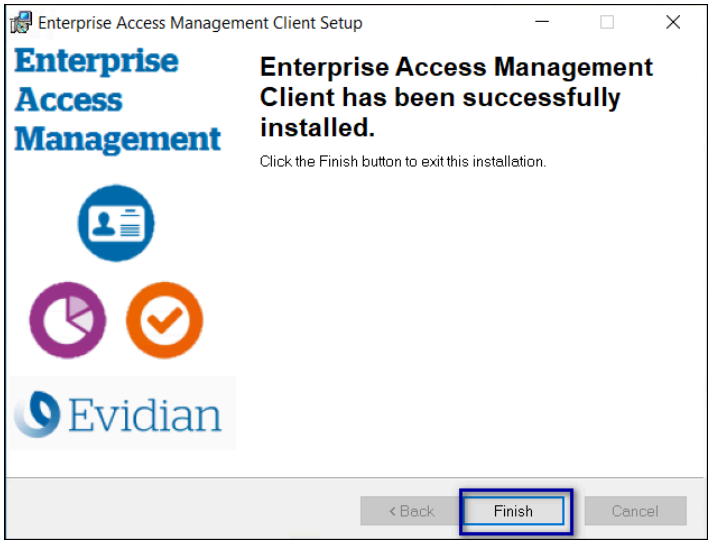


Figure 217: Evidian Client Installation Success window

8.8 - Updating User Terminals

The update procedures differ for user terminals that are in a Wearable and RFID-only configuration.

8.8.1 - Update Wearable User Terminals

Update the Nymi Runtime, the Evidian EAM Client and the *nymi_api.dll* file on each user terminal.

8.8.1.1 - Updating Nymi Runtime

Update the Nymi Runtime on the user terminal and RDP/Citrix servers that use a wearable configuration.

About this task

Perform the following steps after internal testing has verified the compatibility of the NEA with upgraded versions of the Nymi Components.

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` window, click **`Next`**.
8. On the `Service Account` window, perform one of the following actions to choose the account that starts the service:
   - Accept the default service account NTAuthority\LocalService, click **`Next`**.
   - For non-English Windows Operating Systems, choose the LocalSystem account from the drop list, and then click **`Next`**.
9. 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.
10. On the `Ready to install` page, click **`Install`**.
11. Click **`Finish`**.
12. On the `Installation Completed Successfully` page, click **`Close`**.
13. Replace the *nymi_api.dll* file that is used by the MES application with the version of the file that is in the Nymi API C Interface distribution package.

8.8.1.2 - Updating Registry Key Settings

Review the registry key settings on the user terminal and update as required.

Procedure

1. Run Registry Editor.
2. Navigate to *HKLM\Software\Enatel\SSOWatch\CommonConfig*, and then delete the *StopSSOEngineOnOTPFailed* registry key.

3. Navigate to *HKLM\Software\Enatel\WiseGuard\AdvancedLogin*, and then delete the *StartSSOEngine* registry key.
4. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Directory*, and then create a new **`DWORD (32-bit) Value`** named *GetCloudConfigDataOnlyInCloudMode*.
5. Edit the *GetCloudConfigDataOnlyInCloudMode* key, and in the **`Value data`** field type ***1***. Click **`OK`**.
6. Close Registry Editor.

8.8.1.3 - Updating the Evidian SSO Agent

Perform the following steps with an account that has permission to install software on the machine.

About this task

Obtain the Evidian software package from Nymi Solution Consultant or Nymi Support.

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\VCRedist_x64.msi*.

   Note: If the required version of Microsoft Visual C++ redistributable is already installed on the server, a pop-up screen briefly appears, and then disappears.
2. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\ESSOAgent.msi* file.
3. On the `Enterprise Access Management Client Installation`, click **`Next`**.
4. On the `License Agreement` window, click **`I accept the license agreement`**, and then click **`Next`**.

   The following figure shows the `License Agreement` window.

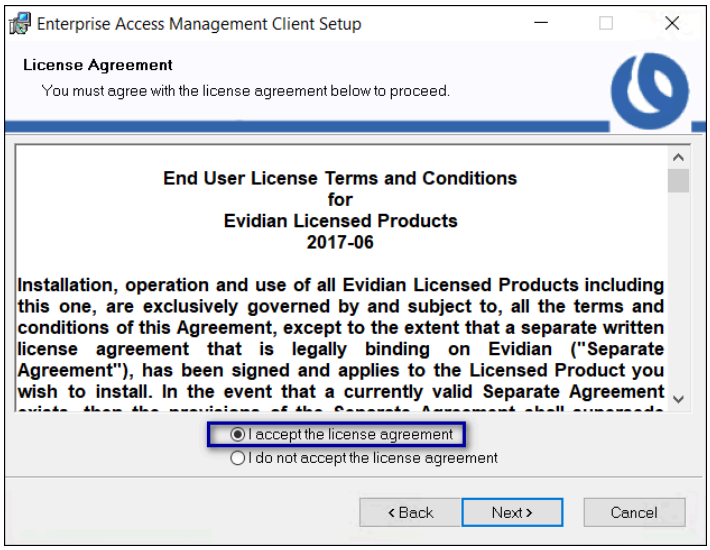


Figure 218: License Agreement window

5. On the `Destination Folder` window, accept the default, and then click **`Next`**.

The following figure shows the `Destination Folder` window.

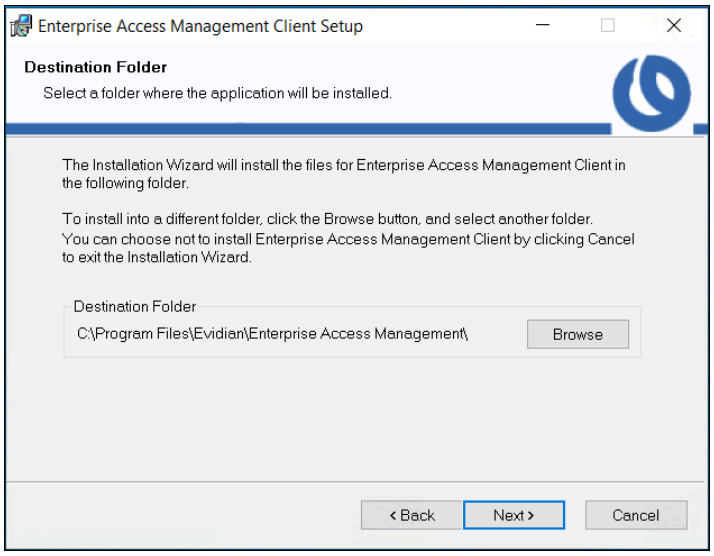


Figure 219: Destination Folder window

6. On the `Select Installation Type` window, select **`Custom`**, and then click **`Next`**.

   The following figure shows the `Select Installation Type` window.

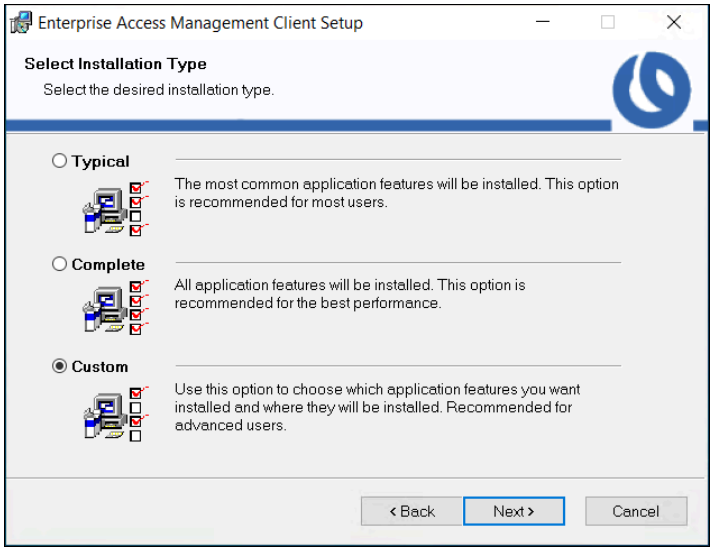


Figure 220: Select Installation Type window

7. On the **`Select Features`** window, click **`Next`**.

   The **`Select Features`** window contains the existing configuration options.

8. On the `Ready to install the application` window, click **`Next`**, as shown in the following figure.

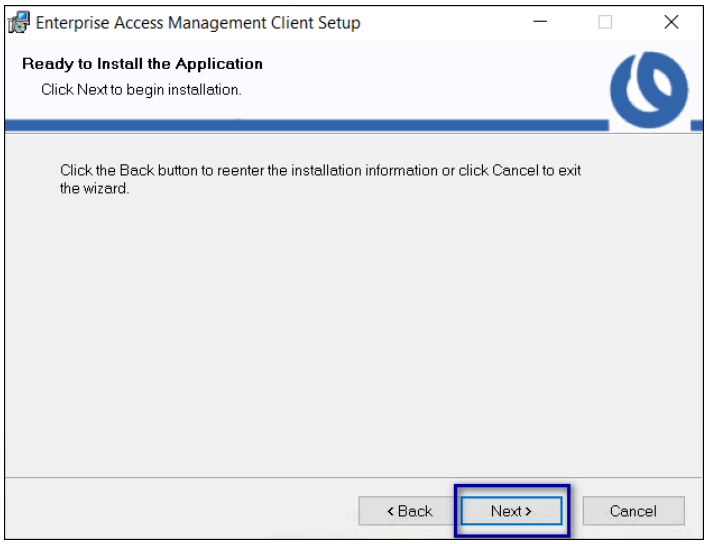


Figure 221: Ready to install the application

9. On the `User account control` pop-up, click **`Yes`**, as shown in the following figure.

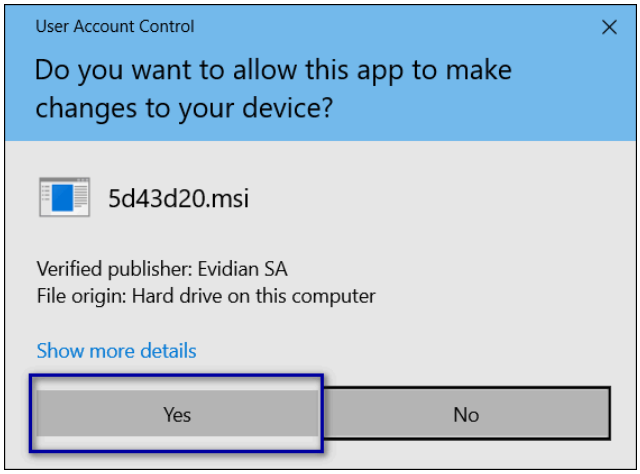


Figure 222: User account control

10. On the `Enterprise Access Management Client has been successfully installed` window, click **`Finish`**, as shown in the following figure.

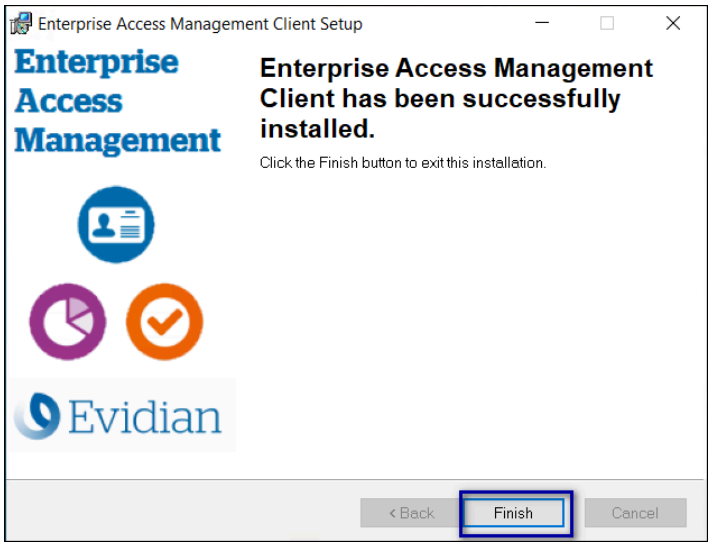


Figure 223: Evidian Client Installation Success window

8.8.1.4 - 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.

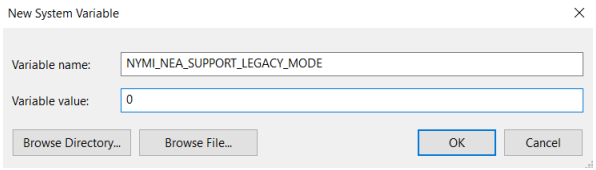


Figure 224: New System Variable window

c) Click **OK**.

8.8.1.5 - Optimizing NFC Taps

The Evidian Access Management version EAM-v10.03b8573.4 optimizes the Evidian EAM Client configuration for Nymi Band taps on a Bluetooth adapter by default.

About this task

When you use an NFC reader to perform Nymi Band taps, perform the following steps on each Citrix or RDP server.

Note: EAM-v10.03b8573.4 does not support use cases that require Authentication Manager.

Procedure

1. Run *regedit.exe*.
2. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication*.
3. Create a new DWord(32-bit) key named **`NymiIntentDiscardNfc`**.
4. Edit **`NymiIntentDiscardNfc`**, change the value in the **`Value data`** field to ***0***, and then click **`OK`**.
5. Create a new DWord(32-bit) key named **`NymiIntentDiscardPcsc`**. Leave the default value ***1***.
6. Close `Registry Editor`.
7. Restart the `Enterprise Access Management Security Services` service.

8.8.1.6 - Confirming the Runtime dll versions

Review the Connected Worker Platform and Evidian EAM Client versions of the Nymi Runtime file to ensure that they are the same.

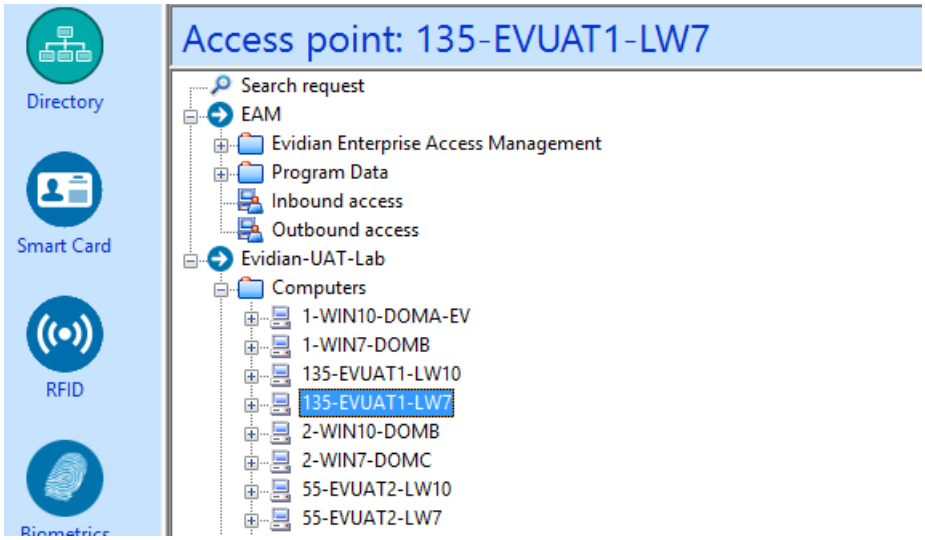
About this task

Perform the following steps on the client machine.

Procedure

1. From the `Windows Apps and Feature` applet, search for the Nymi Runtime application and make note of the version.
2. From Windows explorer, navigate to *C:\Program Files\Common Files\Evidian\WGSS*.
3. Right-click *nymi_api.dll* and select **`Properties`**. On the **`Details`** tab, confirm that the value in the product version matches the Nymi Runtime installation.

4. If the versions do not match, perform the following steps:
   a) Rename the *nymi_api.dll* in *C:\Program Files\Common Files\Evidian\WGSS*.
   b) Copy the *C:\Program Files\Nymi\Nymi Band Application\nymi_api.dll* to *C:\Program Files \Common Files\Evidian\WGSS*.
5. Log in to the Evidian EAM Management Console.
6. Click **`Account and access rights management`**  .
7. In the left navigation pane, expand **`Domain > Computers`**, and then select the terminal, as shown in the following figure.



8. On the **`Actions`** tab, select **`Delete cache files`**, and then click **`Apply`**.
   The cache files are deleted on the terminal and the terminal desktop locks.

8.8.2 - Update RFID-only User Terminals

Update the Evidian EAM Client on each user terminal that is in an RFID-only configuration.

8.8.2.1 - Updating Registry Key Settings

Review the registry key settings on the user terminal and update as required.

Procedure

1. Run Registry Editor.
2. Navigate to *HKLM\Software\Enatel\SSOWatch\CommonConfig*, and then delete the *StopSSOEngineOnOTPFailed* registry key.
3. Navigate to *HKLM\Software\Enatel\WiseGuard\AdvancedLogin*, and then delete the *StartSSOEngine* registry key.
4. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Directory*, and then create a new **`DWORD (32-bit) Value`** named *GetCloudConfigDataOnlyInCloudMode*.

5. Edit the *GetCloudConfigDataOnlyInCloudMode* key, and in the **`Value data`** field type ***1***. Click **`OK`**.
6. Close Registry Editor.

8.8.2.2 - Updating the Evidian SSO Agent

Perform the following steps with an account that has permission to install software on the machine.

About this task

Obtain the Evidian software package from Nymi Solution Consultant or Nymi Support.

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\VCRedist_x64.msi*.

   Note: If the required version of Microsoft Visual C++ redistributable is already installed on the server, a pop-up screen briefly appears, and then disappears.
2. Double-click the *C:\Downloads\EAM-v10.0xxxxxxxx\EAMx64\INSTALL\ESSOAgent.msi* file.
3. On the `Enterprise Access Management Client Installation`, click **`Next`**.
4. On the `License Agreement` window, click **`I accept the license agreement`**, and then click **`Next`**.

   The following figure shows the `License Agreement` window.

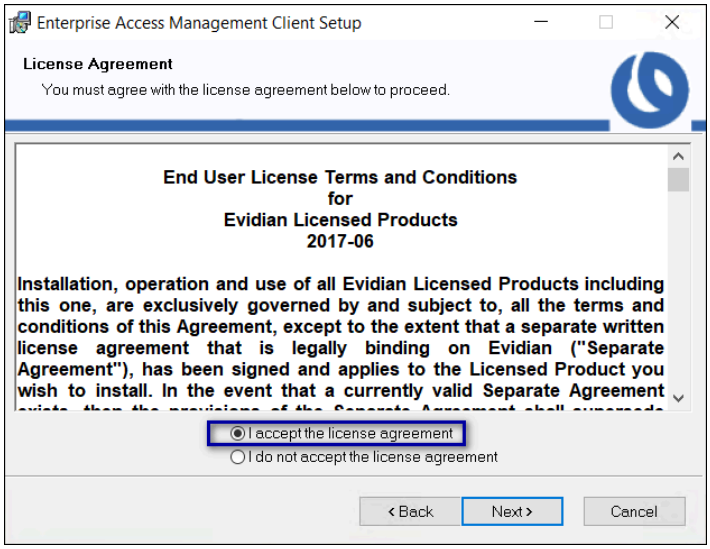


Figure 225: License Agreement window

5. On the `Destination Folder` window, accept the default, and then click **`Next`**.

   The following figure shows the `Destination Folder` window.

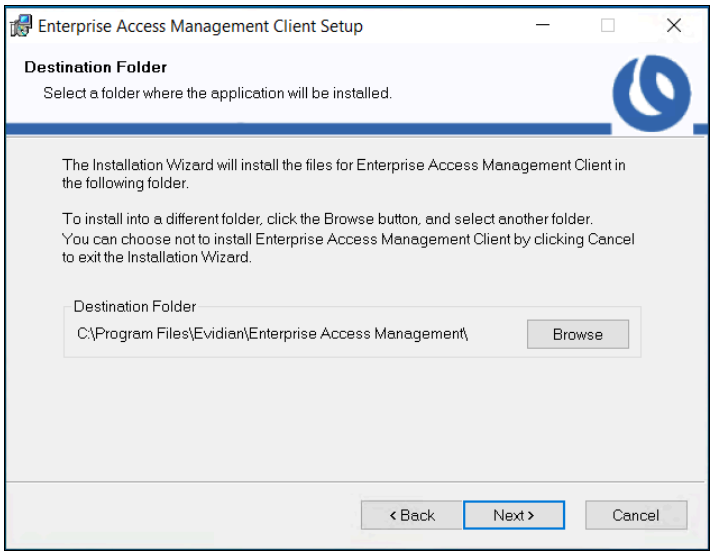


Figure 226: Destination Folder window

6. On the `Select Installation Type` window, select **`Custom`**, and then click **`Next`**.

   The following figure shows the `Select Installation Type` window.

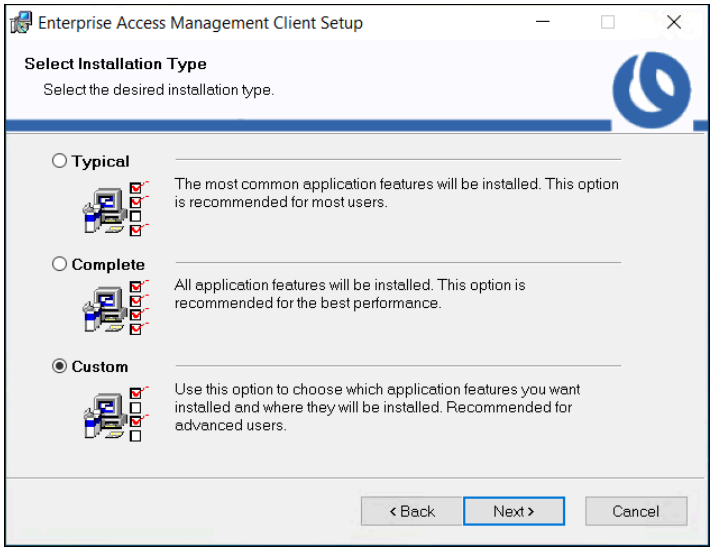


Figure 227: Select Installation Type window

7. On the **`Select Features`** window, click **`Next`**.

   The **`Select Features`** window contains the existing configuration options.

8. On the `Ready to install the application` window, click **`Next`**, as shown in the following figure.

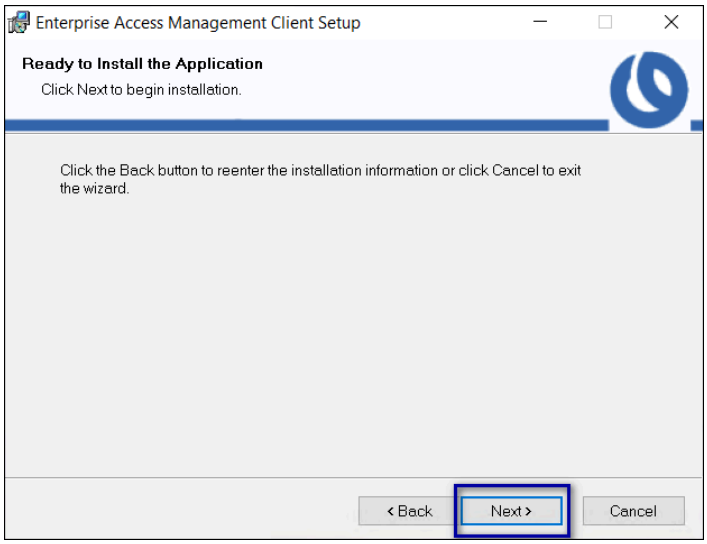


Figure 228: Ready to install the application

9. On the `User account control` pop-up, click **`Yes`**, as shown in the following figure.

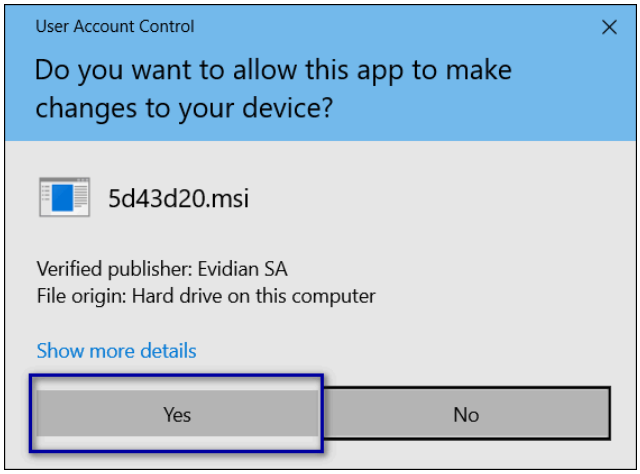


Figure 229: User account control

10. On the `Enterprise Access Management Client has been successfully installed` window, click **`Finish`**, as shown in the following figure.

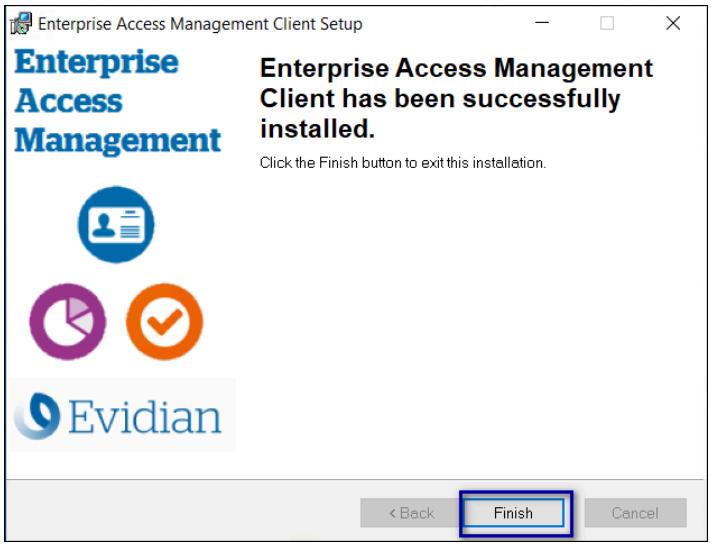


Figure 230: Evidian Client Installation Success window

8.9 - Updating from Nymi Enterprise Edition 3.2.1 and Earlier

This steps in this section only apply to updates from NES 3.2.1 and earlier.

After you update all the components in the Nymi with Evidian Solution, perform the following actions:

- Replace the token structure configuration on the Evidian EAM Controller and any Evidian EAM Client that has a TMS file.
- Re-enroll all existing users to ensure that the Nymi Band to user association appears in the NES and EAM databases.

8.9.1 - (Updates from CWP 1.15.X and earlier only) Updating the TokenManagerStructure

The Connected Worker Platform software package includes new TokenManagerStructure(TMS) files that support wearable and RFID authentication methods. When you update Connected Worker Platform components from Nymi Enterprise Edition, Nymi recommends that you replace any TokenManagerStructure file that you placed on a terminal to override the Evidian EAM Controller configuration, and the configuration on the Evidian EAM Controller.

About this task

The Evidian Supplementary Files directory in the Connected Worker Platform software package includes the following TMS files:

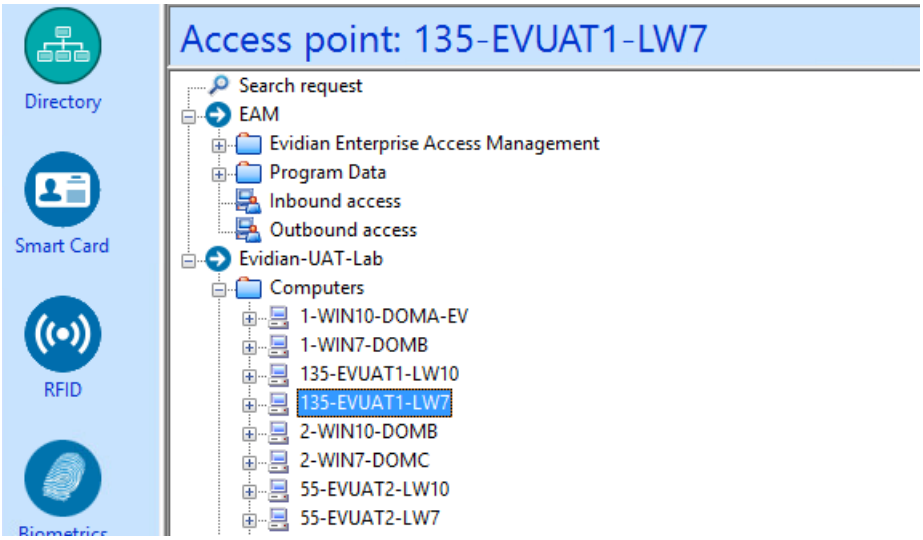
- *TokenManagerStructure-WEARABLE.xml*-To configure Nymi Bands to use wearable authentication.
- *TokenManagerStructure-RFID.xml*-To configure Nymi Bands to use RFID authentication.

Perform the following steps to replace the TMS configuration in your environment.

Procedure

1. Log in to the Evidian EAM Management Console as an EAM Administrator.
2. From the **File** menu, select **Configuration**.
3. On the **Authentication** tab, click **Select**, and then select the appropriate TMS file for your configuration.
4. Click **Apply**.
5. Click **OK**.
6. Launch **Services**.
7. Stop the Enterprise Access Management Security Services service.
8. Delete all files under *C:\Program Files\Common Files\Evidian\WGSS\CacheDir*.

   Note: If you get a message that you cannot delete the files, hold the **Shift** key down when you press **Delete**.
9. Start Enterprise Access Management Security Services service.
10. For each terminal in the environment that overrides the Evidian EAM Controller authentication configuration, perform the following steps:
    a) Log in to the terminal.
    b) Rename the *TokenManagerStructure.xml* file in the *C:\Program Files\Common\Evidian\WGSS* directory.
    c) Copy the new TMS file from the Connected Worker Platform package into the *C:\Program Files\Common\Evidian\WGSS* directory.
    d) Rename the TMS file to *TokenManagerStructure.xml*.
11. Log in to the Evidian EAM Management Console.
12. Click **Account and access rights management**  .
13. In the left navigation pane, expand **Domain > Computers**, and then select the terminal, as shown in the following figure.



14. On the **Actions** tab, select **Delete cache files**, and then click **Apply**.
    The cache files are deleted on the terminal and the terminal desktop locks.

8.9.2 - Re-enrolling existing Nymi Band Users

After you update all the components in the Nymi with Evidian Solution from Nymi Enterprise Edition 3.3.1 or earlier, perform the following steps for all users that have a Nymi Band that was enrolled in Evidian prior to the update.

- Delete the Nymi Band association for the user on the Evidian EAM Controller
- Delete the user data from the Nymi Band
- Re-enroll the Nymi Band

8.9.2.1 - Deleting an RFID or Wearable Nymi Band

Perform the following steps to delete the association between and user and the Nymi Band.

Procedure

1. Put the Nymi Band on a charger and then hold the bottom button down until the **User Data Deleted** icon appears.
   The biometric data of the user is removed from the Nymi Band.
2. In the Evidian EAM Management Console, select the **Directory** panel.
3. Select the search request by changing the object type to **user**, and then in the **Filter** field, type the username.
   The following figure shows the Search request window.

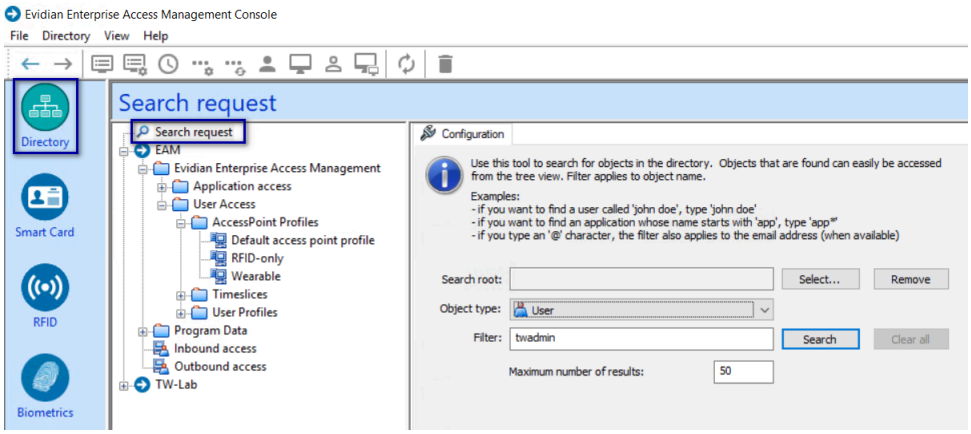
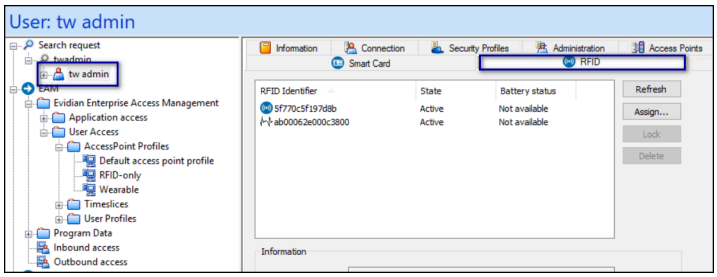
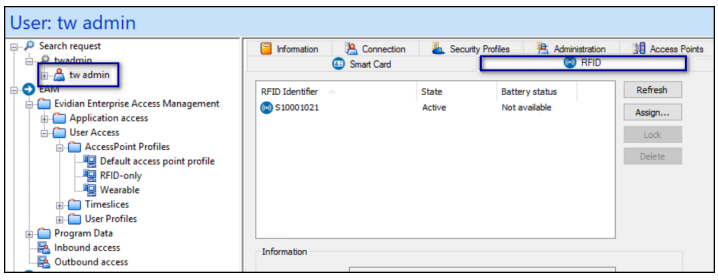


Figure 231: Search request window

4. Select the user, and then select the **RFID** tab. What appears on the **RFID** tab and the actions that you perform, depend on the deployment.

Deployment	Nymi Band Entries
Wearable / RFID-only Mode	Two entries display, one for the user as an RFID entry and the other is a Wearable entry.  **a.** Select the Wearable entry, and then click **Blacklist**. **b.** On the Confirmation window, click **Yes**. **c.** On the Confirmation window, click **Yes**. **d.** Once blacklisted, the **Delete** button appears. Click **Delete**.
Secure NFC Mode	One entry appears.  **a.** Select the Serial Number entry, and then click **Blacklist**. **b.** On the Confirmation window, click **Yes**. **c.** Once blacklisted, the **Delete** button appears. Click **Delete**.

5. In the left navigation pane, select **RFID**.
6. From the **RFID state** list, select **Blacklisted**, and then click **Apply**.
   For Wearable and RFID-only modes, two blacklisted entries appear for the user, one for the RFID and one for the Wearable entry, as shown in the following figure.

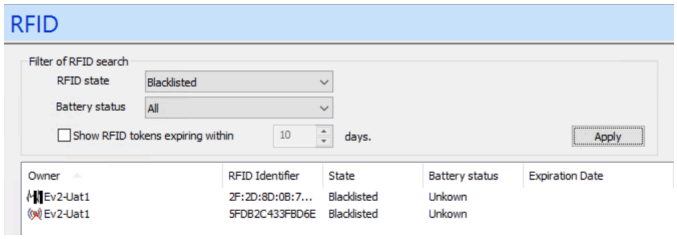


Figure 232: Blacklisted Nymi Band

   For Secure NFC mode, only one entry appears.
7. Delete the blacklisted Nymi Band.
   - For Wearable and RFID-only modes, delete both blacklisted entries.
   - For Secure NFC mode, delete the single blacklisted entry.

8.9.2.2 - Deleting User Data on Nymi Band 3

The Delete User Data process clears personal information, such as the fingerprint template and credentials, from the Nymi Band that is currently enrolled to a user. This process also clears the lockout during a failed authentication lockout.

About this task

Before you can re-enroll a Nymi Band, you must perform the delete user data operation.

Procedure

1. Remove the Nymi Band from the wrist of the user, and then attach the Nymi Band to a charger.
2. On the Nymi Band, hold the bottom button. The Delete User Data message displays on the screen, as shown in the following figure.

   Note: The Nymi Band does not vibrate when you disable **Haptic Feedback on Nymi Bands** for the user or active group policy in Nymi Enterprise Server(NES).

Figure 233: Delete User Data

3. Continue to hold the bottom button until the Nymi Band quickly vibrates twice and the **USER DATA DELETED** message displays on the screen (after about 10 seconds), as show in the following figure.

Figure 234: User Data Deleted

Results

Biometric authentication does not work for the user after you perform a delete user data operation. To use the Nymi Band again, the user must enroll the Nymi Band by using the Nymi Band Application.

Note: If you delete the user data on a Nymi Band and attempt to re-enroll it, you will see the following message,

A Nymi Band has been assigned to (user name), however it cannot be found.

To proceed, you need to delete the Nymi Band association with the user in the NES Administrator Console.

8.9.2.3 - (Wearable and RFID Only Mode) Enrolling a Nymi Band

Before a new user or an existing user (enrolled in NES prior to an Evidian integration) can use a Nymi Band to perform authentication events with Evidian and Evidian-integrated applications, the user must enroll a Nymi Band by using the Nymi Band Application.

Before you begin

Before the user enrolls, ensure that an EAM administrator logs into the Evidian EAM Management Console and adds the user account to the appropriate user profile.

About this task

During the enrollment process for a new user, the process updates the Nymi Enterprise Server(NES) and Evidian databases with enrollment information.

For a user account with a Nymi Band already enrolled on the NES server prior to an Evidian integration, the NES enrollment information is preserved and the process updates the Evidian database with enrollment information.

The user that will enroll the Nymi Band performs the following steps on the enrollment terminal.

Procedure

1. On the Windows Login screen, log in to the computer.
2. Log into the Nymi Band Application with the username and password of the user that will enroll the Nymi Band.
3. Follow the prompts in the Nymi Band Application to enroll the Nymi Band.

Results

Before the user can successfully use the Nymi Band, the user might need to login to the terminal with their username and password to retrieve information from the Evidian EAM Controller. The user can perform subsequent logins by using the Nymi Band.

Note: After enrollment, Nymi recommends that each user authenticate to the Nymi Band 10 times with success. If the number of authentication attempts that are required to get 10 successful authentications exceeds 15, review the information in the *Nymi Connected Worker Platform—Troubleshooting Guide* for more information about how to troubleshoot Nymi Band authentication issues.

8.10 - Updating Technical Definitions

After you make changes to a technical definition, perform the following steps to propagate the change to the Evidian EAM Client.

Procedure

1. In `SSO Builder`, from the **`File`** menu, select **`Manage updates`**.
2. Select **`Post an update`**.
3. Close `SSO Builder`.
4. In the Windows System Tray, click on the Enterprise SSO (eSSO) icon.
5. Click the **`Home`** icon, and then click **`Refresh`**, as shown in the following figure.
   The Evidian EAM Client contacts the Evidian EAM Controller to retrieve new technical definitions.

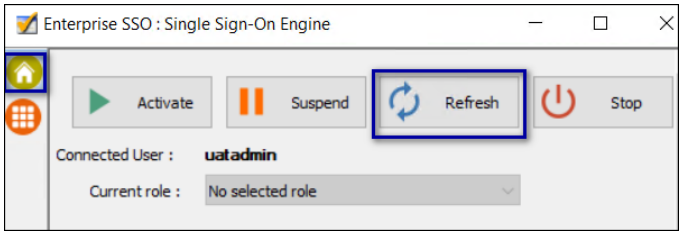


Figure 235: eSSO application Home Window

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