

Wearable Installation and Configuration Guide

Nymi Connected Worker Platform v12.0 2025-01-23

Contents

3 - Preface	5
4 - Nymi Connected Worker Platform with Evidian Access	40
Management Solution	.12
4.1 - Coexistence of Nymi-direct integrations and Evidian integrations	13
5 - Environment Configuration	14
5.1 - Active Directory Requirements	. 14
5.2 - Evidian EAM Controller Requirements	. 14
5.3 - User Terminal Requirements	15
5.4 - Enrollment Terminal Requirements	15
5.5 - Bluetooth Tap Support	16
6 - Using the Nymi Band as a Wearable device	17
6.1 - Nymi-Evidian Architecture - Wearable Device	17
6.2 - Obtain the Required Software	. 19
6.3 - Install Server Software	20
6.3.1 - Installing and Configuring Nymi Enterprise Server	20
6.3.2 - Installing and Configuring the Evidian EAM Controller software	21
6.3.3 - Install the Audit Database	40
6.4 - Installing and Configuring Software on the Enrollment Terminal	. 49
6.4.1 - Importing the Root CA certificate	49
6.4.2 - Installing the Nymi Band Application	51
6.4.3 - (Optional) Configuring the Communication Protocol	. 51
6.4.4 - Installing the Evidian EAM Client	52
6.4.5 - Installing the Evidian SSO Agent	56
6.4.6 - Defining Evidian EAM Client Registry Keys	64
6.4.7 - Enabling LDAPS Support on the Enrollment Terminal	69
6.4.8 - Replacing the Nymi DLL File	. 70
6.4.9 - Logging into the terminal	71
6.4.10 - Validating the EAM Client Installation	. 72
6.5 - Configure the Evidian SSO for an MES Application	73
6.5.1 - Adding an SSO definition for a new target application	73
6.5.2 - Configuring the SSO application in the Evidian EAM Management	
Console	82
6.6 - Installing and Configuring Software on the User Terminals and for remote MES	
application integration over RDP or Citrix	86

6.6.1 - (Citrix/RDP environments only) Deploy a centralized Nymi Agent	87
6.6.2 - Importing the Root CA certificate.	91
6.6.3 - Installing the Nymi Runtime software	93
6.6.4 - IGEL Only - Handling Slow Tap Response in Remote Session	96
6.6.5 - Installing the Evidian EAM Client	96
6.6.6 - Installing the Evidian SSO Agent	100
6.6.7 - Defining Evidian EAM Client Registry Keys	107
6.6.8 - Silent Installations of Evidian EAM Client and SSO Engine	113
6.6.9 - (Citrix/RDP environments only) Configuring Citrix/RDP Clients to	
Access the Centralized Nymi Agent	113
6.6.10 - Replacing the Nymi DLL File	114
6.6.11 - Enabling LDAPS Support	115
6.6.12 - Logging into the terminal	115
6.6.13 - Validating the EAM Client Installation	116
6.6.14 - Updating User Terminal with new SSO Configuration	117
6.7 - Configuring Support for Selective Trust Environments	119
6.8 - Silent Installations of Evidian EAM Client and SSO Engine	120
6.9 - Enrolling a Nymi Band	120
7 - Post Deployment Considerations	122
7.1 - Adding New Users and Computers to the Solution	122
7.2 - NES Backup and Recovery	122
7.2.1 - NES Backups	123
7.2.2 - NES Database Backups	123
7.2.3 - NES Server and Database Recoveries	123
7.3 - Evidian EAM Controller Backup and Recovery	123
7.3.1 - Evidian EAM Controller Backups	124
7.3.2 - Audit Database Backups	124

	•		
7.3.3 - Evidian EAM	Controller Serve	r and Audit Database Re	coveries124

8 - Manage the Nymi Band	125
8.1 - Migrating Existing Nymi Bands to Evidian	125
8.1.1 - (Updates from NEE 3.3.1 and earlier only) Modifying EAM Setting	s to
Support Coexistence with other Solutions	125
8.2 - Viewing the Nymi Band Associated with a User	
8.3 - Replacing, Re-Enrolling or Re-Registering the Nymi Band for a User	127
8.3.1 - Managing Nymi Band Re-Enrollments and Re-registrations with S	elf-
Service	128
8.3.2 - Re-enrolling/Re-registering a User to the Same Nymi Band withou	ıt
Self-Service	130
8.3.3 - Returning a Nymi Band Without Self-Enrollment	131
8.3.4 - Handling a Lost Nymi Band Without Self Enrollment	134
8.3.5 - Handling a found Nymi Band Without Self-Enrollment	

9 - Updating Nymi and Evidian Components	138
9.1 - Updating the NES Software	.138
9.1.1 - (Updates from NEE 3.3.1 and earlier only) Modifying EAM Settings to	
Support Coexistence with other Solutions	139
9.2 - Updating the Evidian EAM Controller	139
9.2.1 - (Updates from CWP 1.15.X and earlier only) Updating the	
TokenManagerStructure	142
9.3 - Update the Centralized Nvmi Agent	143
9.4 - Update the Enrollment Terminal	.147
9.4.1 - Updating the Nymi Band Application	.147
9.4.2 - Updating Registry Key Settings	147
9.4.3 - Updating the Evidian SSO Agent	.147
9.4.4 - Confirming the Runtime dll versions	151
9.4.5 - (Optional) Configuring the Communication Protocol	152
9.5 - Update User Terminals	.153
9.5.1 - Updating Nymi Runtime	153
9.5.2 - Updating Registry Key Settings	154
9.5.3 - Updating the Evidian SSO Agent	.154
9.5.4 - Configuring the Connected Worker Platform Communication Protocol	157
9.5.5 - Optimizing NFC Taps	.158
9.5.6 - Confirming the Runtime dll versions	159
9.6 - Updating from Nymi Enterprise Edition 3.2.1 and Earlier	160
9.6.1 - (Updates from CWP 1.15.X and earlier only) Updating the	
TokenManagerStructure	160
9.6.2 - Re-enrolling existing Nymi Band Users	.161
9.7 - Updating Technical Definitions.	165

10.1 - Obtaining the TokenmanagerStructure life for the Evidian EAM Controller	100
10.2 - Changing the Configuration of the Evidian EAM Controller	166
10.3 - Changing the Evidian EAM Client Configuration on User Terminals	170
10.4 - Changing the Evidian EAM Client Configuration on the Enrollment Terminal	171
10.5 - Deleting Evidian EAM Client Cache	172



Nymi[™] provides periodic revisions to the Nymi Connected Worker Platform. Therefore, some functionality that is described in this document might not apply to all currently supported Nymi products. The *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 Connected Worker Platform with Evidian Guides provides information about installing the Evidian components and configuration options based on your deployment. Separate guides are provided for Wearable, RFID-only, and mixed Wearable and RFID-only deployments.

Audience

This guide provides information to NES and Evidian Access Management Administrators. An NES and Evidian Access Management Administrator is the person in the enterprise that manages the Connected Worker Platform 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
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 <i>Install Audit Database</i> 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.

Version	Date	Revision history
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.
8.0	February 26, 2024	 Eighth release of this document for the CWP 1.3 and later releases. Updates include: 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 <i>Post Deployment Considerations</i> 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:
		 reate 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—Deployment Guide

This document provides the steps that are required to deploy the Connected Worker Platform solution.

Separate guides are provided for authentication on iOS and Windows device.

Nymi Connected Worker Platform—Administration Guide

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

• Nymi SDK Developer Guide—NymiAPI(Windows)

This document provides information about how to develop Nymi-enabled Applications by using the Nymi API(NAPI).

Nymi SDK Developer Guide—Webapi(Windows)

This document provides information about how to understand and develop Nymi-enabled Applications (NEA) on Windows by utilizing the functionality of the Nymi SDK, over a WebSocket connection that is managed by a web-based or other application.

Nymi Connected Worker Platform—Troubleshooting Guide

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

• Nymi Connected Worker Platform with Evidian Troubleshooting Guide

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

Nymi Connected Worker Platform—FIDO2 Deployment Guide

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

• Connected Worker Platform with POMSnet Installation and Configuration Guide

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

• Nymi Band Regulatory Guide

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

• Third-party Licenses

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

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

The Nymi-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-Evidian solution.

The Nymi Band supports two authentication methods in an Evidian environment:

- Wearable (NFC with Bluetooth)—During communications, tapping the Nymi Band on an NFC reader initiates the authentication, and then the Nymi Band is cryptographically authenticated over Bluetooth. This is the default authentication method.
- RFID-only—During communications, the Nymi Band is identified by using only the NFC UID without cryptographic authentication.

Nymi provides you with one or more *TokenManagerStructure.xml* files, based on your configuration needs. The *TokenManagerStructure.xml* file defines the supported authentication types and modules that implement the authentication modules. The contents of the TokenManagerStructure file are loaded on the Evidian EAM Controller and the default configuration is pushed by the Evidian EAM Controller to the Evidian EAM Clients. To override the default authentication method on a terminal, place a different version of the TokenManagerStructure file locally on the terminal.

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

There are several supported deployment configurations in the Nymi-Evidian solution.

- Nymi Band configured as a wearable device
- Nymi Band configured as an RFID-only device
- Nymi Band configured as a mixed use device

Note: This document is specific to an Evidian configuration that uses Active Directory Lightweight Directory Services to provide data storage and retrieval support for directory-enabled applications.

4.1 - Coexistence of Nymi-direct integrations and Evidian integrations

The Connected Worker Platform now supports the co-existence of Nymi-direct integration, and Evidian integration, within the same environment.

Nymi-direct integration supports:

- Nymi-enabled Application (NEAs) that make use of the Nymi SDK to perform application logons and electron signatures.
- Operating systems and applications that support the FIDO2 standard, to perform OS logon / unlock, application logon, and electronic signature.

Evidian integration supports:

- Evidian-integrated applications, which leverage Evidian Single Sign-on (SSO) support to perform application logins and/or electronic signatures.
- Evidian Windows logon, which makes use of Evidian to perform Windows session logon, unlock, and relock when the user is away from the Windows terminal.

In these Evidian integration scenarios, Nymi Bands are integrated with the Evidian EAM Client and Evidian EAM Controller.

You can configure Connected Worker Platform to support either Nymi-direct integration only (default), or to support both Nymi-direct integration and Evidian integration simultaneously.

5 - Environment Configuration

The section outlines the configuration requirements for the enrollment terminal and the user terminals.

Refer to the *Nymi Connected Worker Platform—Deployment Guide* for details about NES requirements and Support NFC Readers for information about supported NFC readers.

5.1 - Active Directory Requirements

To prevent Active Directory(AD) accounts from using the Evidian Enterprise Access Management(EAM) solution and using one Evidian license, create one AD group that contains:

- · AD user accounts that use the Nymi Band to complete authentication tasks
- AD user accounts that requires administrator access to Evidian EAM Management Console.

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

The first time that a user whose account is in the inclusion group logs into an Evidian EAM Client, the user is allocated one Evidian license.

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

5.2 - 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.

5.3 - 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. User terminals include local machines as well as machines that are connected remotely through an RDP session or on a Citrix server.

The user terminal requirements differ depending on the type of user terminal:

User Terminal Type	Requirements
Local Wearable User Terminal	 Nymi Bluetooth Endpoint and the Nymi Agent software to support MES operations. Evidian Enterprise Access Management (EAM) Client, with a valid Evidian license file. Nymi-supported NFC Reader. BLE Adapter (BLED112).
Remote Wearable User Terminal	 Nymi Bluetooth Endpoint software to support MES operations. Evidian EAM Client on the Citrix server or remote session host, with a valid Evidian license file. Network access to the centralized Nymi Agent.
Local RFID-only User Terminal	 Evidian EAM Client, with a valid Evidian license file Nymi-supported NFC Reader.

Network Requirements

User Terminals require a connection to the enterprise domain and bidirectional communication through the following firewall ports:

- For an AD LDS configuration, The user terminal communicates with the listening port of the AD LDS service. When you use the Evidian quick installer as described in this document, the port defaults to 55000.
- For a centralized Nymi Agent, the Evidian EAM Client communicates with the Nymi Agent machine on default port 9120.
- For communications between the Evidian EAM Client and Evidian EAM Controller, communication occurs on port 3644.

5.4 - Enrollment Terminal Requirements

• Windows 10 (minimum build version 1607) or Windows 11 operating system

- Evidian License File.
- Nymi Band Application.
- Evidian EAM Client.
- Local Administrator access or Directory Administrator Access.
- Connection to the enterprise domain.
- BLE Adapter (BLED112)
- Bidirectional communication ports open on the firewall.
 - The enrollment terminal communicates with the listening port of the AD LDS service. When you use the Evidian quick installer as described in this document, the port defaults to 55000.
 - For a centralized Nymi Agent, the enrollment terminal communicates with the Nymi Agent machine on port 9120.
 - For management of access points from the Evidian EAM Management Console, communications occurs on port 3644 on the access point.

5.5 - 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.

BLE tap support is enabled by default when you deploy the following versions of software in your environment: requirements:

- Connected Worker Platform 1.8.1 or later
- Evidian Access Management version 10.03b8573-hotfix-2

6 - Using the Nymi Band as a Wearable device

This chapter provides information about deploying the Nymi Band as a wearable device in an CWP with Evidian environment.

Nymi recommends deploying Nymi Band as a wearable device in a CWP with Evidian environment.

6.1 - Nymi-Evidian Architecture -Wearable Device

The following image represents the components in a Nymi-Evidian solution where the Nymi Band is used as a wearable device.



	Guide provides more information about the Nymi Band Application.
Enterprise Access Management Client	The client-side Evidian software that provides users with a single sign-on (SSO) experience at the user terminal.
Nymi Enterprise Server	Management software for the Nymi Bands within the Nymi ecosystem. Nymi Enterprise Server (NES) ensures the validity of the hardware in the system. NES includes the NES Administrator Console, a web application that administrators can use to manage the Nymi Bands within the ecosystem.
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.
Corporate Directory	An Active Directory server that provides authentication services.
NFC Reader	Captures the NFC UID of the Nymi Band, which is used when an operator performs and SSO authentication event.
BLED112 Dongle	Nymi Band uses Bluetooth Low Energy (BLE) to interact with external components and services. Nymi Band BLE communication does not rely on Bluetooth security. All security is implemented using strong, standard-based cryptography. A BLE adapter (BLED112) is required on the enrollment terminal and user terminals.

6.2 - 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 NES and Evidian EAM Controller hosts.

6.3 - Install Server Software

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

6.3.1 - Installing and Configuring Nymi Enterprise Server

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.

The NES software is in the folder of software package that you obtained from the Nymi Solution Consultant. The Nymi Connected Worker Platform—Deployment Guide provides more information about installing NES.

Enabling Evidian Enrollments

Enrollment in an Evidian environment requires you to enable the option **NES** and Evidian in the active NES policy. In CWP 1.18.0 and later in 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 1: NES and Evidian enrollment option

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

6.3.2 - 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.xxxxxx.zip* to a directory on the server, (for example, the *Downloads* directory).
- 3. Double-click the C:\Downloads\EAM-v10.0x.xxxxxx\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, in the in a dedicated ADLDS directory section, click x64 beside 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.

Enterprise Access Management Controller		×
License keys Provide EAM license keys to enable soft	ware features.	
This software is subject to license. You software. You must agree with the terms proceed. You may enter each license key manua	may not use it if you do not have a lice s and conditions of the license agreem illy or Import them from a file.	ense for this ent to Import
Feature /	License key	
Select license:	Enter your license key and press Add	:
Authentication Manager base $~~$		Add
	< Back Next >	Cancel

- 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 or.

The domain account displays in the **Controller Windows account** field, as shown in the following figure.

Enterprise	Access Management Controller			×
Dedica Inst	ted directory all the dedicated directory server			
In as ma	e EAM Controller includes its own directo ers accounts. The Controller requires a W anagement operations.	ry dedicated to /indows domain	the storage of SS account to perfor	O data and m password
Yo do thi	ou must select the Windows domain acco main account must have the right to Self is account must never expire.	unt used by the Service Passwo	EAM Controller. T ord Requests. The	his Windows password of
Co	ontroller Windows account:	TW-LAB\uat	admin	Select
Th	ne selected account must be located in th	e domain of this	s computer.	
		< Back	Next >	Cancel

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.

8	The security administrator is the fir administration rights to other users him. They should be performed by	st user able to Daily administ delegated ad	run the EAM Console tration tasks should no ministrators.	. He will delegate t be performed by
	Security administrator's account:	T	V-LAB\uatadmin	Select
2	The security passphrase is the fou asked to enter it the first time he is 16 characters long.	undation of EA aunches EAM	M security. The securit Console. The passphra	ty administrator will be ase must be at least
	Security passphrase:	•••••	•••••	•
	Confirm:	•••••		•

Note: 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**.

	chouse apecinic autrioritication mechous	you want to enable for the autoion.	Y
6	EAM natively includes the support for p additional authentication methods. Plain password authentication	lain password authentication. You c	an select
	The following authentication methods in drivers on client workstations: Smart card authentication Wearable device authentication	equire the installation and configurat Mobile phone authentication	ion of device on
	Biometrics authentication	Store-On-Server	.v
	Biometrica provider	Upek	
	RFID authentication	Contactless badge	~

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.

Enterprise Access Manageme	nt Controller	×
Enterprise Access Management	The EAM Controller is now installed.	
Evidian	Start EAM Console	
	< Back Finish Cancel	

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

Evidian Enterp	orise Access Management - Open Session
0	Enterprise Access Management
Login:	🚥 uatadmin 🗸
Password:	••••••
Log on to:	TW-LAB ~
	OK Cancel

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.

Adminis	tration Pass-phrase	×
1	Either this is the first time you start the Console, or your password has been changed. Please enter the administration pass-phrase.	
Pass-phr	ase:	
•••••	•••••	
	OK Cancel	

Results

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

Evidian Enterprise Access Management Console	- 0	×
File View Help		
0		
	Enterprise Access Management	~
	S Evidian	~
AM Controller: Local controller	Ready	100

6.3.2.1 - Obtaining the TokenManagerStructure file for the Evidian EAM Controller

Copy the *TokenManagerStructure-Nymi-Wearable.xml* file from the extracted Nymi installation package, in the *Evidian-Supplementary-Files* subdirectory. You will use this file to define the wearable as the default authentication method for the environment.

6.3.2.2 - Defining the Authentication Method and Enabling Manage Access Points

The Nymi Band uses an authentication method to communicate with the Evidian Authentication Manager and perform authentication tasks.

About this task

Perform the following steps to define the default authentication method that is used by the Evidian EAM Clients.

Procedure

1. On the Evidian EAM Management Console, 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.

Rep	Prima	ry Administrators	SA Server	Hosts	SA Server Configuration
nep	orting	SSPR by Co	nfirmation Code		User Self Enrollment
User	Notifications	Audit (Clean-Up	Secu	rity Code Authentication
General	Default Valu	es Authenticati	on Other Use	r Attributes	Public Key Authenticatio
doken_	manager_list chiometric <token_m< th=""><th>> oonfig> soonfig> magerid="SOFTV tokenclass id="1 token tokenclass tokenclass id="1 token tokenclass id="1 tokenclass id="1 tokenclass id="1 tokenclass id="1 tokenclass id="1</th><th>VARE"> MOBILE" display config> ructure> (module id="0 (module) tructure> (module) tructure> (config) (config) (</th><th>v_name="N kx0100"> kx0200"> splay_name rable_dll>C kx0100"> kx0200"> dll>Custom s>SAMAcco kx0100"> kx0200"></th><th>Iobile Authentication' s="Wearable device" ustomWearableExter '> OTPExtensionRSA.d puntName</th></token_m<>	> oonfig> soonfig> magerid="SOFTV tokenclass id="1 token tokenclass tokenclass id="1 token tokenclass id="1 tokenclass id="1 tokenclass id="1 tokenclass id="1 tokenclass id="1	VARE"> MOBILE" display config> ructure> (module id="0 (module) tructure> (module) tructure> (config) (config) (v_name="N kx0100"> kx0200"> splay_name rable_dll>C kx0100"> kx0200"> dll>Custom s>SAMAcco kx0100"> kx0200">	Iobile Authentication' s="Wearable device" ustomWearableExter '> OTPExtensionRSA.d puntName
<	r	<td>structure></td> <td></td> <td>></td>	structure>		>

- **3.** In the Open File dialog, navigate to the directory that contains the TokenManagerStructure file, select the TokenManagerStructure file, and then click Open.
- 4. Click Apply, which will validate the structure of the file.
- 5. Click or.
- 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.

Registry Editor			
Computer\HKEY LOCAL MACHINE	SOFTWARE\Enatel\WiseGuard\Fram	eWork\Config	
Computer/HKEY_LOCAL_MACHINE Computer Computer Computer HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CLASAL_MACHINE BCD00000000 HKEY_LOCAL_MACHINE SECURITY SGFTWARE Caphyon Classes Clients Cli	 Name (Default) (ClientModuleList (ClientServiceList (ClientSe	eWork\Config Type REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD Cdit DWORD (32- Value name: ManageAccessPc Value data: 1	Data (value not set) FmkAUDIT FmkAuth FmkSSO FmkADM FmkAP FmkSvcBase FmkSvcCln C:\Program Files\Evidian\Enterprise Access Manag C:\Program Files\Common Files\Evidian\WGSS\ 0x00000000 (0) 0x00000000 (0) 0x00000000 (0) -bit) Value FmkAP F Base I Hexadecimal Decimal OK Cancel

Figure 2: Manage Access Points Registry Setting

9. Click or.

10.Restart the Enterprise Access Management Security Services service.

6.3.2.3 - Creating the Access Point Profile for Wearable Mode

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

About this task

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.

- 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.



Figure 3: New Access Point Profile menu option

- 3. In the Name field, type Wearable-only.
- 4. 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 4: Access Point Profile Configuration tab

- 5. Click Apply.
- 6. >On the Configuration tab, select the Authentication Manager tab, and then click Manage Accounts.
- 7. Click Add.
- 8. In the Select Group window, expand you domain, select **Users**, and then select the AD inclusion group, and then click OK.
- **9.** In the **Group** table, select the inclusion group, 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.

lanage Accounts				×
Password authentication groups are passed to th	n requests for members of e operating system. EAM :	the excluded g authentication	roups or non membe is not performed.	r of included
Group name	Group SID	Meaning	Scope	
http://www.action_group	S-1-5-21-44452223	Included	All	
Add Re	move	Change	meaning Ch	nange scope
Add Re	move /stem authentication for log	Change	meaning Ch	nange scope
Add Re Perform operating sy Perform operating sy	move /stem authentication for low /stem authentication when	Change cal administrato EAM authentic	meaning Ch ors ration fails	nange scope

Figure 5: 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.

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 or.

12.Click Apply.

Assigning the Access Point Profiles to User Terminals

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

Before you begin

Assign the wearable profile to the enrollment terminal machine.

About this task

Perform the following steps in the Evidian EAM Management Console.

- 1. 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.

- P Search request	Information 🔊 Configuratio	Authorized Users	Available Applications	Actions 🔘 Events		
EAM Constant Enterprise Access Manager Application access Durate Profiles Program Data Change Access	Access point profile Default access point profile Origin: Default Yalue Available Security services Origin: This computer is not an EAM Controller.					
Outbound access						
Outbound access TW-Lab Computers	Windows generic account					
Computers	Windows generic account Domain'Login:			Delete		
➡ Outbound access ➡ TW-Lab ➡ ➡ ➡ ■ ■ ■	Windows generic account Domain kogin: Password:			Delete		
Outbound access Outbound acce	Windows generic account Domain Login: [Password: [Confirmation:]			Delete		
Curbound access (→ TW-Lab (→ TW-Lab (→ TW-Sw1 (→ = 105×10 ⁻⁰ 050L0F5 (→ = 17W-Sw2 (→ = 36×10 ⁻⁰ 050L0F5 (→ = 36×10 ⁻⁰ 0	Windows generic account Domain\Login: Password: Confirmation:	Z User can open other W	/indows account sessions	Delete		
Contpound access TW-Lab Computers B Computers B Computers B Computers B Computers Computers D Computers	Windows generic account Domain'Login: Password: Confirmation:	User can open other W	/indows account sessions n is never automatically dos	Delete		
Outbound access Outbound access Ornputer	Windows generic account Domain'Login: Password: Confirmation:	∑ User can open other W Generic account sessio	Indows account sessions n is never automatically dos	Delete		

3. In the Select Access Point pop-up, expand EAM > Evidian Enterprise Access Management > User Access > Access Point Profiles, and then select the access point profile that you created.

Select Access Point Profile X Browse Search
EAM EAM Construction EAM Construction Constructio
OK Cancel

- 4. Click or.
- 5. On the Configuration tab, click Apply.

6.3.2.4 - Creating 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 on all user profiles for users that use their Nymi Bands in the wearable configuration.

- 1. From the Directory window, navigate to EAM > Enterprise Access Management.
- 2. Right-click User Profiles, and then select New > User Security Profile.
- 3. In the Name field, type Wearable-only.
- 4. On the Authentication tab, in the User authentication methods section, ensure that only the following methods are selected:
 - Password

- 6 Using the Nymi Band as a Wearable device
 - RFID Pcsc
 - Wearable

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

Biometrics Session dele	gation Au	dit	OTP	Mobile	e Device	Email Notifications
Authentication Security	SSO and Note	s Clo	bud	Unlocking	Self Servi	ce Password Request
User authentication method	s					
Methods	Conf	iguratior	ı		^	
Service Service	Defa	ult confi	guration		*	Select Configuration
Timeslice: Defa	ault time-slice					→
Use cache		Cache o	data vali	dity (in hours	s):	0
Session duration (in hours):		0	*			
Allow temporary password	access for:	0	‡ di	ay(s) when r	esetting use	er's password
		0	‡ da	ay(s) when g	enerating d	hallenge
Allow on all access points				Can unloc	k a worksta	tion
Open Windows session w	ith smartcard lo	gon cert	ificate if	available		
Primary password is stored	l as an SSO ac	count, e	ncrypte	d by:		
User a	nd administrato	rs				~

Figure 6: User Profile Authentication tab

5. Click Apply.

Assigning Users to the Wearable User Profile

Perform the following steps for each user that will use their Nymi Band in Wearable mode.

- 1. In the left navigation pane of the Evidian EAM Management Console, navigate to your_domain > Users, and then select the user.
- 2. On the security Profiles tab, click the ellipses(...), as shown in the following figure.
- 3. On the Select User Profile pop up, expand EAM > Evidian Enterprise Access Management > User Access > User Profiles, and the select the user profile, as shown in the following figure.

User: tw user1	
Users ^	Accounts 🤮 Session Delegation 🕘 Mobile Devices 😐 Smart Card 🚳 RFID 🥥 Biometrics
Administrator	📔 Information 🛛 🖺 Connection 🛛 🚢 Security Profiles 🛛 📇 Administration 🔢 Access Points 😹 Applie
Guest	User security profile
H	Dafault uppr grafia
	Derault user prome
H-m lest	
	Select User Profile X
twuser	
H- agent	Browse Search
Allewed RODC Deservered Per	Cancel
Cart Publishers	Concol
Coneshle Domain Controlle	
Denied RODC Password Ren	Evolan Enterprise Access Management
	Approximation access
DnsUpdateProxy	AccessPoint Profiles
A Domain Admins	mesices
Domain Computers	🖨 🧰 User Profiles
A Domain Controllers	
Domain Guests	Relinent
- 🦰 Domain Users	
- 🤏 eam exclusion	
- 🦰 eam_inclusion	
Enterprise Admins	
- 🦰 Enterprise Key Admins	
- A Group Policy Creator Owners	OK Cancel
- 🤏 Key Admins	

Figure 7: Select Wearable User Profile

- 4. Click or.
- 5. On the security Profiles tab, click Apply.
- 6. In the left navigation pane of the Evidian EAM Management Console, navigate to your_domain > Users, and then select the user.

6.3.2.5 - Modifying EAM Settings to Support Coexistence with other Solutions

If Evidian Authentication Manager is enabled, when an Evidian-integrated MES 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 MES 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.

6.3.2.6 - Configuring Additional EAM Primary Administrators

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

About this task

By adding at least one additional auxiliary primary user, 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 cannot use Active Directory groups, you can only add individual users.

6. Select the user, and then click or.

The following figure provides an example of the screen with one auxiliary primary administrator.
Rep	orting	SSPR by Confin	mation Code		User Self Enrollment	
User Notifications		Audit Clea	an-Up Secur		rity Code Authentication	
General	Default Values	Authentication	Other User Attributes		Public Key Authentication	
Options	nmary Ac	aministrators	s SA Server Hos		ts SA Server Configuration	
Primar	y administrator					
tw ad	lmin - CN=tw admir	n,CN=Users,DC=	TW-Lab,DC=	ocal		
A						
Auxilia	ry primary administ	trators				
/ At	w user1					
				Add	Remove	
				Add	Remove	
				Add	Remove	
				Add	Remove	
				Add	Remove	
				Add	Remove	
				Add	Remove	
				Add	Remove	
				Add	Remove	

- 7. Click Apply.
- 8. Click or.
- 9. Close the Evidian EAM Management Console.

6.3.2.7 - Delegating an Administrator Role to a User

You can delegate the privileges to a user, to allow them limited access to the Evidian EAM Management Console.

Procedure

- **1.** Log into the Evidian EAM Management Console with a user account that is a primary EAM administrator.
- 2. Click on the Account and Access Rights Management licon.
- 3. In the Evidian EAM Management Console, select the Directory panel.
- 4. 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 8: Search request window

- 5. Click Search.
- 6. Select the user from the search results.
- 7. On the Administration tab, click Delegate, as shown in the following figure.

🙂 Smart Card 📒 Information 🛛 🤽 Set	ecurity Profiles	💿 RFID 🗎 🗎	Access Points
uthorized by:			
Administered organization(s)			
			Remove
			Add
			- ddin
Administration restrictions for this administrator			
Managed users restrictions	Audit visit	ality restrictions	
Administration profiles			
			Edit
			Remove
			Add
Change administration profile			
Delegate Transfer Delete	Set Pare	ent Administrator	
Audit			
All events	O Events m	atching filter:	
○ No events			Select
		Apply	Cancel

Figure 9: Delegate option

8. In the Administration Profiles section, click Add.



Figure 10: Add Administration Profiles

9. In the Administration Profiles Selection window, select Access administrator, as shown in the following figure.



Figure 11: Administration Profiles Selection window

10.Click or.

11.On the Administration tab, click Apply.

6.3.2.8 - Enabling LDAPS Support on the Evidian EAM Controller

Evidian Authentication Manager and Enterprise SSO 10.0 evolution 2 patch level 3 and later supports LDAPS on AD LDS.

Before you begin

Install LDAPS on AD LDS. Microsoft provides more information.

About this task

Perform the following steps on the Evidian EAM Controller.

Procedure

- 1. Run regedit.exe.
- 2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork.
- 3. Right-click WGDirectory, and then select New > DWORD (32-bit) value
- 4. In the Value file, type SSL.

- 5. Double-click the SSL key, and in the Value data field, type 1.
- 6. In the *ServerList* key, confirm that the path to the AD LDS instance with the secure port appears. For example, *srv-ssl.ssl.lan:636.*.
- 7. Close Registry Editor.

6.3.3 - Install the Audit Database

EAM stores audit information in an audit database.

Consider the following:

- You can install the Audit Database on the same SQL server that you use for 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.
- Assign the Evidian service account db_owner rights to the Audit Database.
- On the SQL server, ensure that the SQL browsing service is running.

6.3.3.1 - Creating the EAM Audit Database

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

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

Ensure that the SQL service account has db_create access to the audit database.

6.3.3.2 - 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 or.
 - 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 domain user has local administrator privileges.
- **8.** Under Controller Configuration, click Configure local audit database, as shown in the following figure.

dministration Tools	
Administration Tools	
Use the following tools to configure	the solution.
Select a task:	Procedure
 Directory initialization 	1 In the Select a task dron-
Extend Active Directory Schema (2)	down list, click an entry to filter the configuration tools
• Create default objects	that you must run for the chosen task.
Security configuration	
 Initialize the Primary controller 	
 Initialize an associated controller 	
Publish a new Token data file	
 Define administrator credentials for Self Service Password Request 	
 Import an external key 	
Import/Export controller key	
Controller configuration	
 Install an Audit V2 Database Server 	
Configure local audit database	
 Update Audit translation data 	
Configure security settings	

Figure 12: 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.

🗊 Data	Link Propert	es			×
Provider	Connection	Advanced	All		
Select	he data you v	ant to conne	ct to:		
OLE	DB Provider	(s)			
Mic Mic Mic Mic Mic Mic MSI OLE	rosoft OLE DE rosoft OLE DE rosoft OLE DE rosoft OLE DE rosoft OLE DE rosoft OLE DE DataShape E DB Provider	Driver 19 fo Provider for Provider for Provider for Provider for Simple Prov	r SQL S Analysi ODBC Search SQL Se vider	erver is Services 14.(Drivers) erver ry Services)
					Next>>
		ОК		Cancel	Help

Figure 13: 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 FDQN of the SQL server.
- b) From the **Enter information to log on to the server** list, select one of the following options; 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.

📰 Data Link Properties	×
Provider Connection Advanced Al	1
1. Select or enter a server name:	
tw-srv1	✓ Refresh
2. Enter information to log on to the ser	ver:
Windows Authentication	\sim
Server SPN:	
Username:	
Password:	
Blank password	Allow saving password
3. Select the database:	eamaudit 🗸 🗸
O Attach a database file as a data	base name:
Using the filename:	
	Browse
Change Password	Test Connection
OK	Canaal Holp
OK	Cancer Help

Figure 14: Select the database window

- e) Click Test Connection.
- f) On the Test Connection Succeeded window, click OK.
- g) Click or.
- 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.

Audit Datab	ase Configuration		×
The an	controller must conne OLE DB Provider) in ord	ect to an existing data der to support Audit a	base (through and Reporting.
Credential	to access to the dat	abase	×
Enter the cr	edential to use to conn	ect to the database:	
loș	Login format mus gin: tw-lab\twadmin	t be DOMAIN\user]
Passwo	ird:	']
		ОК	Cancel
	Table		\sim
		Use quotes	
Advanced	Verify	Apply	Close

Figure 15: 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.

Audit D	atabase Configuration		×
1	The controller must connect an OLE DB Provider) in ord	t to an existing da er to support Audit	tabase (through and Reporting.
	OUse an existing SQL Set	ver instance.	
	Password:	•••••	
	Confirmation:	•••••	
	• Use existing corporate of	latabase	
	Data Source	tw-srv1 (OLE DB)
	Table	dbo.auditevents	~
		Use quotes	
Adva	nced Verify	Apply	Close

Figure 16: Audit Database Configuration window

- j) On the EAM Configuration pop-up, click ox.
- k) Click Close.
- **13.**On the Administration Tools window, in the click Update Audit translation data, as shown in the following figure.



Figure 17: 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.

Please select the directory i	n which the	e metadata	files	can	be found:	
EAM-V10.03B8573.4\EAI	M.X64\TOC	LS\WGSrv	Conf	ig\Me	taData	Select
Translated resources for s	supported a	udit categ	ories			
The following metadata Select a category to see addition to the category	will be imp which erro descriptior	oorted/upd ors or reso n.	ated. urce	s will	be imported	in
Category		Resource	5	^	Errors	^
Monitoring		sv			sv	
Admin		ru			ru	
SSO		ro			ro	
Authentication		nl			nl	
System		ja			ja	
		it			it	
		fr			fr	
		fi			fi	
		es		\sim	es	
		<	>		en	\sim
✓ Import translations in loc	cal databas	e	tw-	srv2 (OLE DB)	
Import translations in maste	er database		tw-	srv2 (OLE DB)	

Figure 18: 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.

Customizing Audit Report Output

By default, Evidian audit queries and reports display user identification with a object GUID to protect user privacy. You can configure the audit queries and reports to display the AD username instead of the object GUID.

About this task

Perform the following steps in the Evidian EAM Management Console.

Procedure

- 1. From the File menu, select Configuration.
- 2. On the Other User Attributes tab, change the value in the Audit Attribute field from *ObjectGUID* to *SAMAccountName*, as shown in the following figure.

optiona miniary /	dministrators	SA Server Hosts	SA Se	rver Configuration	
Reporting	SSPR by Conf	imation Code	User	Self Enrollment	
User Notifications	Audit Cle	ean-Up Sec	curity Code	nty Code Authentication Public Key Authentication	
General Default Values	Authentication	Other User Attribute	es Public		
Attributes					
Description	Туре	LD	AP Attribute	,	
				Delete	
Attribute description :					
Autobite description.					
	Integer		\sim		
Attribute type:					
Attribute type: LDAP name:				Add	
Attribute type: LDAP name: Audit identifier				Add	
Attribute type: LDAP name: Audt identifier Unless explici another LDA	tły set, a GUID id P attribute to iden	lentifies users in audit e tify users in events.	events. You	Add I may select	
Attribute type: LDAP name: Audt identifier Unless explici another LDAI For better per	tty set, a GUID id P attribute to iden formances, make	lentifies users in audit e tify users in events. sure this attribute is in	events. You	Add I may select I Directory.	

Figure 19:

3. Click **Test**. A popup appears with 10 random usernames in your directory, as shown in the following figure.



Figure 20:

- 4. Click or.
- 5. Click Apply.
- 6. Click or.
- 7. Stop the Enterprise Security Services service.
- 8. Navigate to the C:\Program Files\Common Files\Evidian\WGSS\CacheDir folder.
- 9. Select all the files, hold the **shift** key down, and then select **Delete**, when prompted, click **Yes** to delete all files.

10.Start the Enterprise Security Services service.

6.4 - Installing and Configuring Software on the Enrollment Terminal

The enrollment terminal is the machine that you use to enroll Nymi Bands. This machine requires a connected Bluegiga Bluetooth Adapter(BLED 112).

This section provides information about installing the Evidian Nymi Band Application and the Evidian EAM Client software on the enrollment terminal.

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

6.4.1 - 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. For example, on Windows 10, perform the following steps:

Procedure

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

The following figure shows the certlm window.

ᡖ certlm - [Certificates - Local Computer	Trusted Root Certificatio	on Auth	orities] —	\times
File Action View Help				
🗢 🔿 🙍 🗊 📋 🙆 📴				
🙀 Certificates - Local Computer	^ Object Type			
> 🧮 Personal	Certificate	c		
 Trusted Root Certification Authoritie 		·		
Certificates	Find Certificates			
> 🧮 Enterprise Trust				
> 🧮 Intermediate Certification Autho	All lasks	~	Find Certificates	
> 🧮 Trusted Publishers	View	>	Import	
> 🧮 Untrusted Certificates		T		
> 🧮 Third-Party Root Certification A	Refresh			
> 🧮 Trusted People	Export List			
> Client Authentication Issuers				
> Preview Build Roots	Help			

Figure 21: certIm application on Windows 10

- 3. On the Welcome to the Certificate Import Wizard screen, click Next.
 - The following figure shows the Welcome to the Certificate Import Wizard screen.

×
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
To continue, dick Next.
Nex

Figure 22: Welcome to the Certificate Import Wizard screen

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

Fil	le to Import
	Specify the file you want to import.
	File name:
	C:\Users\ddunn\Downloads\Local Lab Root CA.cer Browse
	Note: More than one certificate can be stored in a single file in the following formats:
	Personal Information Exchange- PKCS #12 (.PFX,.P12)
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (,P7B)
	Microsoft Serialised Certificate Store (.SST)

Figure 23: File to Import screen

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

6.4.2 - Installing the Nymi Band Application

For information about installing the Nymi Band Application, see the Nymi Connected Worker *Platform—Administration Guide*.

Note: On the Completing the Nymi Band Application Setup Wizard screen, before you click Finish, clear the Launch Nymi Band Application option.

6.4.3 - (Optional) Configuring the Communication Protocol

If you use the enrollment terminal to also access NEAs, 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.

New System Variable		×
Variable name:	NYMI_NEA_SUPPORT_LEGACY_MODE	
Variable value:	0	
Browse Directory	Browse File	OK Cancel

Figure 24: New System Variable window

c) Click or.

6.4.4 - Installing the Evidian EAM Client

Install the Evidian EAM Client on the enrollment terminal.

Before you begin

Before installing the Evidian EAM Client software:

- 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.

About this task

Perform the following steps on the enrollment terminal.

Procedure

- 1. Log in to the user terminal with an account that has Local Administrator access.
- 2. Download and extract the Evidian software package, *EAM-v10.0x.xxxxxx.zip* to a directory on the host, for example, the *Downloads* directory.
- **3.** Double-click the C:\Downloads\EAM-v10.0xxxxxxx\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.

Lincolp	orise Access Management Cont	troller	×
Lic	ense keys Provide EAM license keys to enal	ble software features.	
	This software is subject to licens software. You must agree with th proceed. You may enter each license key	e. You may not use it if you do not have a line terms and conditions of the license agree manually or Import them from a file.	cense for this ment to
	Customer ID:		Import
	Feature /	License key	
	Select license:	Enter your license key and press Ac	id:

- 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.

Configuration Assistant	×
Installation mode Allows you to choose whether a Controller is needed by the workstation.	
Please choose the Security Services operating mode:	
O without a Controller	
Security Services run on the user workstation only.	
with a Controller Security Services use a Controller for advanced features.	
< Back Next >	Cancel

Figure 25: 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.

ed		
icu.		<u> </u>
story :		
	ied. tory :	ied. tory :

Figure 26: 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.

nfiguration Assistant Security repository Choice of security data storage.	
	ų
Stand-alone: the directory is used stored in flat files and in Windows	for user authentication only. The security data is registry.
Integrated with Active Directory: the This requires customization of the	he security data is stored in the domain directory. A.D. schema.
Integrated with AD LDS: the security	rity data is stored in an AD LDS server.

Figure 27: 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.

figuration Assistan	t			
DAP Configuratio Configuration of p	n arameters for acces	s to the LDAP server.		
Name or address of	the LDAP server an	d any replicas :		
Name/Address :	tw-srv1.tw-lab.loc	al	Port : 55000	
			Add	+
			Remove/Edit	
Enterprise naming c	ontext :			\sim
Use a dedicated	naming context for	Evidian Enterprise Acce	ess Management dat	ta
Evidian Enterprise A Management namin	g context :			~
		(De el	Marcha	Cara
		< Back	Next >	Car

Figure 28: 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.

Configuration Assistant	×
Access-point management Choose whether to enable different security policies for different workstations.	9
Access-point management	
If you select this option you will be able to define security policies for individual workstations and groups of workstations.	
Manage access-points Note: EAM Controllers and workstations must be configured to use the same value for this parameter.	
< Back Next >	Cancel

Figure 29: 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 30: Restart Computer window

15.

6.4.5 - Installing the Evidian SSO Agent

The Evidian SSO Agent 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.

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

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking C: \Downloads\EAM-v10.0xxxxxxx\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-v10.0xxxxxxx\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 31: 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 32: 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.

🕼 Enterprise Acces	s Management Client Set	up	-		×
Select Installation Select the desired	Type I installation type.			_(9
O Typical	The most common applic is recommended for most	ation features will be t users.	installed. This	option	_
○ Complete	All application features wi recommended for the bes	ll be installed. This op st performance.	otion is		
• Custom	Use this option to choose installed and where they v advanced users.	which application fea will be installed. Reco	tures you want mmended for	t	
		< Back	Next >	Can	cel

Figure 33: 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.
	Reset (Back Next) Cancel
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.
	Enterprise Access Management Client Setup - X Select Features Please select which features you would like to install.
	Authentication Manager Austrantial Authentication And OTP authentication And Authentication And Comparison of the password and OTP authentication And Comparison of the password and other particulation And Comparison of the password and other particulation Authentication Authentic
	Reset <back next=""> Cancel</back>
	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.

🛃 Enterprise Access Management Client Setu	Ar - dr
Select Features Please select which features you would like to	install.
Authentication Manager Password and OTP authe Smart card authentication RFID authentication Biometrics authentication Cluster and transparent lo Mobile authentication SSPR authentication InWebo authentication Enterprise SSD EAM Console Supported languages	Feature Description: Enable users to enroll their biometrics authentication data. This feature requires 0KB on your hard drive.
Reset	< Back Next > Cancel

Figure 34: 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.

🔀 Enterpri	se Access Management Client Setup - 🗌 🗙
Select Fe Please	atures select which features you would like to install.
	Authentication Manager Biometrics enrollment tool Enterprise SSO x Integration with Windows Authe Will be installed on local hard drive.
	Bentire feature will be installed on local hard drive. Will be installed to run from network. Bentire feature will be installed to run from network. ur hard drive.
	Feature will be installed when required. Entire feature will be unavailable.
	Reset <back next=""> Cancel</back>

Figure 35: 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. # Enterprise Access Management Client Setup Select Features Please select Which features you would like to install # Authentication Manager Please select Which features you would like to install # Contemprise SSO Studio # Contemprise SSO Stud
Use the Nymi Band for Windows login only	Leave the default Enterprise SSO configuration, 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 36: Install EAM Console Feature

12.Click Next.

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

🕼 Enterprise Access Management Client Setup	—		\times
Ready to Install the Application			
Click Next to begin installation.			S.
Click the Back button to reenter the installation information or click the wizard.	k Cancel to exi	it	
< Back	Next>	Can	cel

Figure 37: Ready to install the application

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



Figure 38: User account control

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



Figure 39: Evidian Client Installation Success window

¹⁶ In the Windows System Tray, click on the Enterprise SSO (eSSO) **16** icon.

17.Click the Home Oicon, 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 40: eSSO application Home Window

6.4.6 - Defining 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.

Purpose	Affected Components	Registry Setting	
Required Registry Key Se	try 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: <i>HKLM\Software\Nymi\NES</i> Type: String Name: URL Value: <i>https://nes_server/instance</i> 	
		Where:	
		 nes_server is the Fully Qualified Domain name of the NES host. instance is the convised mapping name 	
		• 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
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
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:: <i>HKLM\SOFTWARE \Enate\\WiseGuard\SSOWatch \CommonConfig</i> Type: DWORD 32-bit Name: <i>Allow4EyesAndSameUser</i> Value: 1 Edit DWORD (32-bit) Value

Purpose	Affected Components	Registry Setting
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: <i>HKLM\Software</i> \<i>Enate\Wiseguard\FrameWork</i> <i>Authentication</i> Type: DWORD 32-bit Name: <i>RFIDSelfEnrollAllowed</i> 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: <i>HKLM\Software\Enatel \WiseGuard\AdvancedLogin</i> Type: String Name:WearableEnrollTool Value: <i>C:\Program Files\Nymi\Nymi</i> Band Application\NEM.exe Edit String Value data: C:\Program Files\NymiNymi Band Application\NEM.exe C:\Program Files\NymiNymi Band Application\NEM.exe C:\Program Files\NymiNymi Band Application\NEM.exe C:\Program Files\NymiNymi Band Application\NEM.exe C:\Program Files\NymiNymi Band Application\NEM.exe C:\Program Files\NymiNymi Band Application\NEM.exe C:\Program Files\NymiNymi Band Appl
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
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
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 \Enate\WiseGuard\FrameWork \Authentication Type: DWORD 32-bit Name: WearableNeedsRFID Value: 1
Registry Key Settings Spec Configure the Evidian EAM Client to communicate with the Nymi Agent server.	ific to Citrix/RDP environmen All Citrix/RDP servers	ts Create the following registry key: • Location: HKLM\SOFTWARE \Enate\\WiseGuard\FrameWork \Authentication\CommonConfig • 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: <i>HKLM\SYSTEM</i> \ <i>CurrentControlSet\Control\Citrix</i> \ <i>Wfshell\TWI</i> • Type: String • Name: LogoffCheckSysModules • Value: ssoengine.exe, ESSOCredentialManager.exe Registry Key #2 • Location: <i>HKLM\SOFTWARE\Policies</i> \ <i>Enatel\SSOWatch\CommonConfig</i> or <i>HKLM\SOFTWARE\Enatel</i> \ <i>SSOWatch\CommonConfig</i> • 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 <i>nymi_api.dll</i> 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

6.4.7 - Enabling LDAPS Support on the Enrollment Terminal

Evidian Authentication Manager and Enterprise SSO 10.0 evolution 2 patch level 3 and later supports LDAPS on AD LDS.

Before you begin

Install LDAPS on AD LDS. Microsoft provides more information.

About this task

Perform the following steps on the Enrollment Terminal.

Procedure

- 1. Run regedit.exe.
- 2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork.
- 3. Right-click WGDirectory, and then select New > DWORD (32-bit) value
- 4. In the Value file, type SSL.
- 5. Double-click the SSL key, and in the Value data field, type 1.
- 6. In the *ServerList* key, confirm that the path to the AD LDS instance with the secure port appears. For example, *srv-ssl.ssl.lan:636.*.
- 7. Close Registry Editor.

6.4.8 - 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.

6.4.9 - Logging into the terminal

If you installed the Evidian SSOAgent with the Authentication Manager authentication mode, 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 an NFC 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.

6.4.10 - Validating the EAM Client Installation

After you log into the computer, validate that the Evidian EAM Client can connect to the Evidian EAM Controller and that the EAM client can retrieve certificates from NES.

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



Figure 41: 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.

• Navigate to C:\Windows\System32\config\systemprofile\AppData\Roaming\Wymi\WSL \random_string\ksp, and confirm that you see at least 20 files, as shown in the following figure. If you see 9 files only, refer to the Nymi Connected Worker Platform with Evidian Troubleshooting Guide for more information.
« Local Disk (C:) > Windows > System32 > co	onfig > systemprofile > AppData	 Roaming > 	Nymi > NSL > Yr2hs4Og > ksp
Name	 Date modified 	Туре	Size
📑 АААВ	2023-03-08 4:54 PM	File	1 KB
📑 AAAC	2023-03-08 4:54 PM	File	1 KB
📑 AAAF	2023-03-08 4:54 PM	File	1 KB
📑 AAAG	2023-03-08 4:54 PM	File	1 KB
📑 АААН	2023-03-08 4:54 PM	File	1 KB
AAAI	2023-03-08 4:54 PM	File	1 KB
f3HdCDshM9mGTPvL	2023-03-08 4:54 PM	File	1 KB
f3HdCDshM9mGTPvL-ext	2023-03-08 4:54 PM	File	1 KB
📑 g79C1qzPGjzdmE9R	2023-03-08 4:54 PM	File	1 KB
📑 g79C1qzPGjzdmE9R-ext	2023-03-08 4:54 PM	File	1 KB
hZi-s1zzMi35h6Yi	2023-03-08 4:54 PM	File	1 KB
hZi-s1zzMi35h6Yi-ext	2023-03-08 4:54 PM	File	1 KB
📑 hzIUAUPcMUjnBSPu	2023-03-08 4:54 PM	File	1 KB
hzIUAUPcMUjnBSPu-ext	2023-03-08 4:54 PM	File	1 KB
QsreoP9t7qycffDk	2023-03-08 4:54 PM	File	1 KB
QsreoP9t7qycffDk-ext	2023-03-08 4:54 PM	File	1 KB
T60b91aL3RqMIr90	2023-03-08 4:54 PM	File	1 KB
T60b91aL3RqMIr90-ext	2023-03-08 4:54 PM	File	1 KB
wMEzycZsMSPIfpWz	2023-03-08 4:54 PM	File	1 KB
wMEzycZsMSPIfpWz-ext	2023-03-08 4:54 PM	File	1 KB

Figure 42: Certificates Folder

6.5 - Configure the Evidian SSO for an MES Application

The following information provides setup and configuration information about how to configure single sign-on for MES applications.

Note: Before you perform the steps in this chapter, install the MES application on the enrollment terminal according to the instructions provided by the MES application vendor. After you complete the SSO configuration steps, you can uninstall the MES application.

Important: Follow each step in the order in which they appear.

6.5.1 - Adding an SSO definition for a new target application

To use the Nymi Band with Evidian to perform authentication tasks, use Enterprise SSO Studio to create SSO technical definition and training Evidian SSO to operate with the MES application. The SSO definition captures the login screen and credentials for the MES application.

About this task

Perform the following steps from the enrollment terminal.

Note: For a web application, SSO detects the application based on the windows process that runs the application. If you run the application with more than one browser, create a new

technical definition for each supported browser that will start the application, for example, Chrome, Microsoft Internet Explorer, Firefox, Opera etc.

Procedure

- 1. Log in as a user that is a EAM administrator.
- 2. Navigate to C:\Program Files\Evidian\Enterprise Access Management and double-click SSOBuilder.exe.
- **3.** On the Enterprise SSO Studio login window, type the login credentials of an EAM Administrator.
- 4. In the SSO Config Enterprise SSO Studio, navigate to EAM > Evidian Enterprise Access Management > Application Access > Technical definitions, as shown in the following figure.



Figure 43: Technical Definition object

5. Right-click Technical Definitions and select New Technical Definition, as shown in the following figure.



Figure 44: Creating a New Technical Definition

6. In the **Properties** tab, provide a name in the **Technical Definition** name field, and then click OK.

ication properties			
QRentry keyboard	Apple k	eychain	Autofill
Properties	Launcher		Parameters
dentification			
Technical Definition	name:		
Sample Application			
Session management (a	dvanced)		
The application can	only have one	session at a t	ime
	,		
	,		
Try previous password	l when bad pas	sword' windo	w detected
Try previous password	l when 'bad pas	sword' windo	w detected
Try previous password	l when bad pas	sword" windo	w detected
Try previous password	l when bad pas	sword" windo	w detected
Try previous password	l when 'bad pas	sword" windo	w detected
Try previous password	l when 'bad pas	sword" windo	w detected
] Try previous password	when 'bad pas	isword' windo	w detected
] Try previous password	l when 'bad pas	isword' windo	w detected
Try previous password	I when bad pas	isword' windo	w detected
] Try previous password	l when 'bad pas	sword' windo	w detected
] Try previous password	I when 'bad pas	isword' windo	w detected
] Try previous password	I when 'bad pas	isword' windo	w detected
Try previous password	I when 'bad pas	isword' windo	w detected

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

7. Right-click on the new technical definition that you just created and select New Window, as shown in the following figure.



Figure 45: Creating a New Window for the Technical Definition

8. In the Window properties window, enter a name for the window, for example, *Login Window*, and from the Window Type list, select the appropriate windows type.

	propertie			>
General	Options	Detection Action	าร	
Gene Choo the w	ral Windov se a name indow type	description and type for this wi you select.	indow. SSO behavior	r depends on
Wind	ow name:	Login Window		
Wind	ow type:	StandardLog	in	~

Figure 46: Naming the New Technical Definition Window

- **9.** Open the application that will use Evidian SSO to enter the credentials. Ensure that both the SSO Builder and MES application windows are visible on your desktop.
 - The following figure provides an example of the SSO Builder and an MES application window.
- **10.** On the **Detection** tab, click and drag the target icon **one on the application** window. The following figure provides an example of the Detection window.

Vindow properties X
General Options Detection Actions
You have to select the window to be detected. To do so, drag and drop the target icon onto its title bar or inside a web page.
Web page
URL file://C:\Users\administrator\Desktop\sampleLogin.html
Detect browser title Configuration
detection to handle this. enable variable URL detection Parameter of the web page
Look for text
O In Field
If window detection is not sufficient, you can use Advanced detection to add constraints on process.
OK Cancel Help

Figure 47: New Technical Definition Detection window

The URL for the webpage appears in the URL field.

11.In the Actions Tab, perform the following actions:

- a) Click and drag the target icon beside the **Identifier** field onto the **Username** entry field of the application.
- b) Click and drag the target icon beside the **Password** field onto the **Password** entry field of the application.

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

Window properties	×
General Options Detection Actions	
Window fields description	
This window type sends the user authentication data to the fields defined below. No field is mandatorv.	
Identifier : Enter Username" 2.1.1.2.3.1.1.1.	
Password : 🔒 "Enter Password" 4.1.1.2.3.1.1.1. 🔊	
Do not prompt for user account	
Additional fields customization Click on the Customize button to specify additional parameters Customize	
After the SSO has been done	
Do nothing O Press the <enter> key</enter>	
O Press the button :	
OK Cancel Help	

Figure 48: New Technical Definition Actions tab

Note: If the target icon does not detect the field, double-click the Target icon (instead of clicking and dragging) to open a Control Detection window, and then select the desired target control, for example, an editable text option.



Figure 49: Detection window

- 12.In the After the SSO has been done section, select an option to perform after the SSO action has completed, for example, select Press the button, and then drag and drop the Target icon onto the button in the application that completes the login action such as a Submit button.
- **13.**Click or to save the configuration.
- **14.**Optional, for MES applications that require 2 different users to perform an e-signature to complete a task, perform the following actions:
 - a) Right-click on the form that requires the sign-offs and then select **Properties**, as shown in the following figure.



Figure 50: Properties

b) On the Window properties window, from the Actions tab, click Script Editor, as shown in the following figure.

Script Action Ac	Con	d. Parame Login	ters	
Action Action Action GetSSO →()GotoLab Free SendSS	Con	d. Parame Login	ters	
GetSSO ⁺()GotoLab	el 🥥 I	Login		
 Return Label Return 	0	False Cancel Passwo SSO Do Cancel OK.	ed ind to Control:"passwone. ed	vord" 1.2.3
٢			Scrip	> t Editor

Figure 51: Script Editor option

c) On the Custom Script Editor window, select GetSSO, and then select the option Perform SSO as a difference user, as shown in the following figure.

Custom Script I	Editor		×
🛱 🗙 🕹 🕇	888	5	
Action Action Action CostoLabel CostoLabel CostoLabel Return ()Label Return	Cond.	Parameters Login Canceled Password to Control:"password" 1.2.3.1.2 SSO Done. Canceled OK.	
Get SSO Paramete	r		
 Identifier 		O Custom Parameter :	
O Password		No configured parameter	\sim
O New Passw	vord		
O Confirm Pa	ssword		
Do not pro	mpt for user a	account	
Perform SS	60 as a differ	ent user	

Figure 52: Custom Script Editor window

- d) Click or.
- e) On the Window properties window, click ox.
- **15.**Right-click the newly created technical definition and click **Update Directory**, as shown in the following figure.



Figure 53: Update Directory with New Technical Definition

16.Close SSO Builder.

6.5.2 - Configuring the SSO application in the Evidian EAM Management Console

After creating the technical definition for an MES application in SSO Builder, configure the Evidian EAM Controller to propagate the technical definition to user terminals in the environment.

About this task

Procedure

- 1. Launch the Evidian EAM Management Console, and log in as an EAM administrator.
- ^{2.} Click on the Account and Access Rights Management de icon.
- 3. Navigate to EAM > Evidian Enterprise Access Management > Application Access
- 4. Right-click **Technical definitions** and then select **New > Application**, as shown in the following figure.

Evidian Enterprise Access Management Cor	sole			
File Directory View Help				
← → 🗏 🗒 🕓 …, …,	1 🖵 2 🖵	\$		
Ganization:	Technical o	definitior	is	
Search request		Information	O Events	
EAM				
Evidian Enterprise	Access Management	Organization		
Application ac	cess		Name:	Technical definitions
Applicatio	n security objects	Server	host name:	TW-Srv1.TW-Lab.local:55000
Smart Card	ns			
User Access	New	;	Ap	plication
Program Data	Rename	F2	Ten	nplate-based Application >
Inbound access	Refresh	E5	Ap	plication Profile
REID Outbound acces	Undate		Tim	neslice
iu ib i ◆ TW-Lab	Delete		Pas	sword Control Policy
	Delete		Pas	sword Generation Policy
	Force Password	F7	Use	er Security Profile
	Send SSO Data by	/ mail	Acc	cess Point Security Profile
Biometrics	Check User Chall	enge		
	Set/Unset OU as	root	Kep	bresentative
	Send message		Clu	ister of access points
	Import		Clo	ud Customer
Mobile	Export			
Devices.				

Figure 54: New Application menu option

5. Provide an application name, and then click Apply.

The following figure provides an example of a new application.

Application: SampleApp	
Search request Search request Application access Application security objects Applications Control Control Contro	Information & Configuration & User Access Administrators Application Application Name: SampleApp
	Technical Support information Publisher: Version: Support information: Last product update: Set logo Delete Logo Apply Cancel

Figure 55: New Application Name

- 6. If the MES use the credentials of the logged in AD user, perform the following steps:
 - a) In the Evidian EAM Management Console, navigate to the technical definition and in the Configuration tab, select the Account Base tab.
 - b) Select the The application uses the primary account option.
 - c) In the Login format list, select the login format of the AD credentials.
 - d) Click Apply.

General Ac	count Base Accou	int Properties SSC	External Names	Provisioning connector
The a	application uses the p application uses the 1	orimary account Windows generic ac	The application	uses the PIN
- Other apr	Login format:	Short name: jdo	e	~
	Applications can sh applications, the sa	are accounts. Whe me login/password p	n accounts are share pairs can be used with	ed between two or more h all of them.
Applica	ation			
	Share Accounts with	Another Application	٦	
Sto	op Sharing Accounts	with Selected Appli	cation	
				Apply Cancel

The following figure provides an example of the Account Base window.

Figure 56: Account Base window

7. In the Configuration tab, select the SSO tab, and then on from the Methods tab, from the Default SSO propagation method list, select SSO, as shown in the following figure.

😔 Evidian E	interprise Access Management Console	
File Directo	ory View Help	
$\leftarrow \rightarrow$	▣ ▣ ○ …, …, ≗ ᄆ ≗ 모	l ¢ 🗎
Æ	Application: SampleApp	
Directory	Search request	📔 Information 🖉 Configuration 🎉 User Access 🖹 Administrators 🔝 Account Generation 🔢 Access Poin
Smart Card	Evidian Enterprise Access Management Application access Application security objects Applications Applications Technical definitions Implications	General Account Base Account Properties SSO External Names Provisioning connector Methods Access Strategies OLE/XenApp SSO propagation
RFID	User Access Der Carlos Inbound access Outbound access Outbound access TW-Lab	Default SSO propagation method: Vault SSO Windows authentication OLE/Automation
Biometrics		Vender View Vault

Figure 57: Selecting Default SSO Propagation Method

8. Beside the Technical definition field, click Select, as shown in the following figure. Figure 58: Select button

Methods	Access Strategies	OLE/XenApp		
SSO pr	opagation			
Def	ault SSO propagation	method:		
55	0	~		
Tec	hnical definition:			
			Select	

9. In the select Technical Definition window, expand EAM > Evidian Enterprise Access Management > Application Access > Technical definitions, and then select the new technical definition that was created with SSOBuilder, as shown in the following figure.



Figure 59: Selecting the Technical Definition

10.Click or.

- 11.On the sso tab, click Apply to save the configuration.
- 12.Navigate to EAM > Evidian Enterprise Access Management > Application Access > Application security objects > Default application profile. Select User must re-authenticate to perform SSO, as shown in the following figure, and then click Apply.



Figure 60: User must re-authenticate to perform SSO **13.**Close the Evidian EAM Management Console.

6.6 - Installing and Configuring Software on the User Terminals and for remote MES application integration over RDP or Citrix

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 SDK, and the Evidian EAM Client software.

The Nymi with Evidian solution supports the use of the Nymi Band to perform authentication events on an MES 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.

6.6.1 - (Citrix/RDP environments only) Deploy a centralized Nymi Agent

Citrix and RDP environments make use of a centralized Nymi Agent .

About this task

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

Procedure

- 1. Log in to the terminal, with an account that has administrator privileges.
- **2.** Create a backup copy of the C:\Wymi\Bluetooth_Endpoint\nbe.toml file.
- **3.** Extract the Nymi SDK distribution package.
- **4.** From the ...*\nymi-sdk\windows\setup* folder, right-click the *Nymi Runtime Installer version.exe* file, and select **Run as administrator**.
- 5. On the Welcome page, click Install.
- 6. On the User Account Control page, click Yes. The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
- 7. On the Welcome to the Nymi Runtime Setup Wizard page, click Next.
- 8. On the Nymi Runtime Setup window, expand Nymi Runtime.
- 9. Select Nymi 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.

🛃 Nymi Runtime 5.0.5	5.46 Setup		_	
Nymi Runtime Se Select the way you	t up want features to be installe	ed.		-^-
Click the icons in th	e tree below to change the mi Runtime - Nymi Agent - Nymi Bluetooth Endpoir Will be installed on lo	way features wi	ll be installed.	
	 Feature will be install Entire feature will be 	led when requi	red	
				Browse
Reset	Disk Usage	Back	Next	Cancel

Figure 61: Nymi Bluetooth Endpoint feature will be unavailable

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

🞲 Nymi Runtime 5.0.	5.46 Setup		₽	_			\times
Nymi Runtime Se Select the way you	e tup u want features to be instal	led.				(~
Click the icons in th	e tree below to change the	way	features	will be install	ed.		
	mi Runtime Vymi Agent Vymi Bluetooth Endpoi	nt	This feat hard driv	ture requires /e.	: OKB	on your	
						Browse	
Reset	Disk Usage		Back	Next		Cano	el

Figure 62: Nymi Bluetooth Endpoint feature is not available

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

Service Account	.3	
Account to run syste	m services as	66
Service Account	tt: Local Service	

Figure 63: Nymi Runtime Service Account window

12.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.

13.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*. Refer to Appendix—Record the CWP Variables for the service account name.

The following figure shows the Nymi Infrastructure Service Account window.



Figure 64: Nymi Infrastructure Service Account window

The installer creates the following files in the C: Wymi/WymiAgent\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.

14.On the Ready to install page, click Install.

15.Click Finish.

```
16.On the Installation Completed Successfully page, click Close.
```

6.6.2 - Importing the Root CA certificate

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

Before you begin

Install the Root CA on the following machines:

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

About this task

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

Procedure

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

The following figure shows the certlm window.



Figure 65: certIm application on Windows 10

3. On the Welcome to the Certificate Import Wizard screen, click Next. The following figure shows the Welcome to the Certificate Import Wizard screen. 6 - Using the Nymi Band as a Wearable device



Figure 66: Welcome to the Certificate Import Wizard screen

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

The following figure shows the File to Import screen.

Specify the file y	ou want to import.			
- 1				
C:\Users\ddunr	1\Downloads\Local Lab R	oot CA.cer		Browse
Note: More thar Personal Info	n one certificate can be s rmation Exchange-PKCS	stored in a single file 5 #12 (.PFX,.P12)	in the follow	wing formats:
Cryptographi	Message Syntax Stand	lard- PKCS #7 Certi	ficates (.P7E	3)
Microsoft Seri	alised Certificate Store ((.SST)		

Figure 67: File to Import screen

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

6.6.3 - Installing the Nymi Runtime software

The Nymi Runtime software is contained in the Nymi API C Interface distribution package and includes two separate components, the Nymi Agent and the Nymi Bluetooth Endpoint.

About this task

The Nymi Runtime components that a user terminal requires differs depending on how a user connects to the MES application, remotely or locally.

Procedure

- 1. Log in to the terminal, with an account that has administrator privileges.
- 2. Create a backup copy of the C:\Wymi\Bluetooth_Endpoint\nbe.toml file.
- 3. Extract the Nymi SDK distribution package.
- 4. From the ... *Inymi-sdk* windows setup folder, right-click the Nymi Runtime Installer version.exe file, and select Run as administrator.
- 5. On the Welcome page, click Install.
- 6. On the User Account Control page, click Yes. The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
- 7. On the Welcome to the Nymi Runtime Setup Wizard page, click Next.
- 8. On the Nymi Runtime Setup window, perform one of the following actions:
 - If the user will perform authentication tasks in a local MES application, click Next.
 - If the user will perform authentication tasks in an MES application on a Citrix server or RDP session host:
 - a. Select Nymi Agent, and then select Entire feature will be unavailable, as shown in the following figure, and then click Next.

记 Nymi Runtime 5.1.1.439 Setup - 🗆 🗙
Nymi Runtime Setup
Select the way you want features to be installed.
Click the icons in the tree below to change the way features will be installed.
Nymi Runtime
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Feature will be installed when required
× Entire feature will be unavailable
Browse
Reset Disk Usage Back Next Cancel

Figure 68: Nymi Agent feature will be unavailable

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

₩ Nymi Runtime 5.0. Nymi Runtime Se Select the way yo	5.46 Setup E tup u want features to be ins	talled.			_	(×
Click the icons in t	ne tree below to change	the way	features	will be in	stalled.		
	/mi Runtime 【 ▼ <mark>Nymi Agent</mark> ③ ▼ Nymi Bluetooth End	point >	This fea hard dri	iture req ve.	uires 0K	B on your	
						Browse	
Reset	Disk Usage		Back	Ne	ext	Can	cel

Figure 69: Nymi Agent feature is not available

c. 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**.

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

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

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

12.Click Finish.

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

What to do next

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

6.6.4 - 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.

6.6.5 - Installing the Evidian EAM Client

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

About this task

- When the user accesses an MES application that you installed on the user terminal, install the Evidian EAM Client on the user terminal.
- When the user accesses an MES application on an RDP sessions host or Citrix server, install the Evidian EAM Client on the RDP sessions host or Citrix server.
- When a user uses the Nymi Band to unlock the user terminal, install the Evidian EAM Client on the user terminal.

Before installing the Evidian EAM Client software:

- 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.

Procedure

- 1. Log in to the user terminal with an account that has Local Administrator access.
- 2. Download and extract the Evidian software package, *EAM-v10.0x.xxxxxx.zip* to a directory on the host, for example, the *Downloads* directory.
- **3.** Double-click the C:\Downloads\EAM-v10.0xxxxxxx\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.

ЦС	ense keys Provide EAM license keys to ena	able software features.	
0	This software is subject to licen: software. You must agree with t proceed. You may enter each license key	se. You may not use it if you do not have a he terms and conditions of the license agree y manually or Import them from a file.	icense for this ement to
	Customer ID:		Import
	Feature /	License key	
	Select license:	Enter your license key and press A	

- 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.

Configuration Assistant	×
Installation mode Allows you to choose whether a Controller is needed by the workstation.	
Please choose the Security Services operating mode:	
 without a Controller Security Services run on the user workstation only. 	
with a Controller Security Services use a Controller for advanced features.	
< Back Next > (Cancel

Figure 70: 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.

ed		
icu.		<u> </u>
story :		
	ied. tory :	ied. tory :

Figure 71: 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.

Configuration Assistant	×
Security repository Choice of security data storage.	
Stand-alone: the directory is used for stored in flat files and in Windows reg	user authentication only. The security data is jistry.
 Integrated with Active Directory: the This requires customization of the A.I Integrated with AD LDS: the security 	security data is stored in the domain directory. D. schema. data is stored in an AD LDS server.
	< Back Next > Cancel

Figure 72: 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.

figuration Assistan	t			
DAP Configuratio Configuration of p	n arameters for acces	s to the LDAP server.		
Name or address of	the LDAP server an	d any replicas :		
Name/Address :	tw-srv1.tw-lab.loc	al	Port : 55000	
			Add	+
			Remove/Edit	
Enterprise naming c	ontext :			\sim
Use a dedicated	naming context for	Evidian Enterprise Acce	ess Management dat	ta
Evidian Enterprise A Management namin	g context :			~
		(De el	Marcha	Cara
		< Back	Next >	Car

Figure 73: 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.

Configuration Assistant	×
Access-point management Choose whether to enable different security policies for different worksta	tions.
Access-point management	
If you select this option you will be able to define security policies for indi- workstations and groups of workstations.	vidual
Manage access-points Note: EAM Controllers and workstations must be configured to us same value for this parameter.	e the
< Back Next >	Cancel

Figure 74: 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 75: Restart Computer window

6.6.6 - Installing the Evidian SSO Agent

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

About this task

Procedure

1. Install the required version of the Microsoft Visual C++ redistributable by double-clicking C: \Downloads\EAM-v10.0xxxxxxx\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-v10.0xxxxxxx\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 76: License Agreement window

5. On the Destination Folder window, accept the default, and then click Next. The following figure shows the Destination Folder window.

🕼 Enterprise Access Management Client Setup		_		×
Destination Folder Select a folder where the application will be installe	ed.			0
The Installation Wizard will install the files for Enterprise Access Management Client in the following folder. To install into a different folder, click the Browse button, and select another folder. You can choose not to install Enterprise Access Management Client by clicking Cancel				
to exit the Installation Wizard. Destination Folder C:\Program Files\Evidian\Enterprise Access Management\ Browse]
	< Back	Next >	Ca	ancel

Figure 77: 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.

Enterprise Access	Management Client Setup		-		×
Select Installation Select the desired	Type installation type.			_(9
O Typical	The most common application feat is recommended for most users.	ures will be ins	talled. This (option	
○ Complete	All application features will be installed. This option is recommended for the best performance.				
• Custom	Use this option to choose which application features you want installed and where they will be installed. Recommended for advanced users.				
	< E	Back N	lext >	Car	icel

Figure 78: 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.		
	Enterprise Access Management Client Setup - X Select Features Please select which features you would like to install.		
	Auffenticetion Manager Fanture Description: Will be installed on local hard drive. orkstation. Image: Entire feature will be installed when required. image: Entire feature will be unavailable. Image: Entire feature will be unavailable. This feature requires 1KB on your herd drive. It has 8 of 8 subfeatures selected. The subfeatures require 42MB on your hard drive. Reset K Back Next> Cancel K		
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.	
	Enterprise Access Management Client Setup - X Select Features Please select which features you would like to install.	
	Authentication Manager Authentication Manager Authentication do CTP authentication AriD Biometrics enrollment tool Arid Biometrics enrollment tool Arid Console Arid Console Arid Console Arid Console Arid Arid Arid Arid Arid Arid Arid A	
	Reset < Back Next> Cancel	
	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.

🛃 Enterprise Access Management Client Setu	Ar — dr
Select Features Please select which features you would like to	install.
Authentication Manager Password and OTP authe Smart card authentication RFID authentication Biometrics authentication Cluster and transparent lo Mobile authentication SSPR authentication InWebo authentication Enterprise SSD EAM Console Supported languages	Feature Description: Enable users to enroll their biometrics authentication data. This feature requires 0KB on your hard drive.
Reset	< Back Next > Cancel

Figure 79: 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.

🔀 Enterpri	se Access Management Client Setup - 🗌 🗙		
Select Fe Please	atures select which features you would like to install.		
	Authentication Manager Biometrics enrollment tool Enterprise SSO To Integration with Windows Auther Will be installed on local hard drive.		
Image: Second			
	 Feature will be installed when required. Entire feature will be unavailable. 		
	Reset <back next=""> Cancel</back>		

Figure 80: 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. # Enterprise Access Management Client Setup Select Features Please select Which features you would like to install # Authentication Manager Please select Which features you would like to install # Contemprise SSO Studio # Contemprise SSO Stud
Use the Nymi Band for Windows login only	Leave the default Enterprise SSO configuration, 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 81: 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 82: Ready to install the application

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



Figure 83: User account control

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



Figure 84: Evidian Client Installation Success window

16-In the Windows System Tray, click on the Enterprise SSO (eSSO) 2 icon.

17.Click the Home Oicon, 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 85: eSSO application Home Window

6.6.7 - Defining 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.

Purpose	Affected Components	Registry Setting	
Required Registry Key Settings The Nymi with Evidian solution			

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: HKLM\Software\Enatel \SSOWatch\CommonConfig • Type: DWORD 32-bit • Name: DisplayErrorMessageAtStartup • Value: 0
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:: <i>HKLM\SOFTWARE \Enatel\WiseGuard\SSOWatch \CommonConfig</i> Type: DWORD 32-bit Name: <i>Allow4EyesAndSameUser</i> Value: 1 Edit DWORD (32-bit) Value Value name: Name: Base Name: Cancel CK Cancel
Purpose	Affected Components	Registry Setting
--	--	---
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: <i>HKLM\Software</i> \<i>Enate\Wiseguard\FrameWork</i> <i>Vauthentication</i> Type: DWORD 32-bit Name: <i>RFIDSelfEnrollAllowed</i> 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: <i>HKLM\SOFTWARE</i> \<i>Enatel\WiseGuard\FrameWork</i> <i>Vauthentication</i> Type: DWORD 32-bit Name: <i>WearableNeedsRFID</i> Value: 1
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

Purpose	Affected Components	Registry Setting
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: <i>HKLM\Software\Wymi\NES</i> Type: String Name: URL Value: <i>https://nes_server/instance</i>
		Where:
		 nes_server is the Fully Qualified Domain name of the NES host. <i>instance</i> 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 C	trix/RDP environments	
Configure the Evidian EAM Client to communicate with the Nymi Agent server.	All Citrix/RDP servers	Create the following registry key: • Location: <i>HKLM\SOFTWARE</i> \ <i>Enate\WiseGuard\FrameWork</i> \ <i>Authentication\CommonConfig</i> • Type: String • Name: <i>NymiAgentUrl</i> • Value: <i>ws://agent_fdqn:9120/</i> <i>socket/websocket</i> Where <i>agent_fdqn</i> is the Fully Qualified Domain Name of the centralized Nymi Agent server.

Purpose	Affected Components	Registry Setting
Configure Citrix roaming	All Citrix servers	Create/Update the following registry keys:
sessions, to ensure that when a published MES		Registry Key #1
application closes, the Citrix session is logged off.		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	
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

Purpose	Affected Components	Registry Setting
Support multiple domains, where users enroll their Nymi Bands in a domain	All Evidian EAM Clients including Citrix/RDP servers and the enrollment	Edit the HKLM\Software\Enatel \WiseGuard\FrameWork\Directory \PossibleDomainList.
user terminal domain.		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.
		Edit String X Value name: PossibleDomainsList Value data: TW-LAB TW2-LAB OK Cancel
For use with DeltaV	All Evidian EAM Clients, including the enrollment terminal Citrix/RDP servers.	Create the following registry keys in <i>HKLM\Software\Enatel\SSOWatch</i> <i>\CommonConfig</i> : Key #1 • Type: DWORD 32-bit • Name: <i>NoCacheFields</i> • Value: 1 Key #2 • Type: DWORD 32-bit • Name: <i>CheckUIAutomationFieldPresence</i> • Value: 2 Key #3 • Type: DWORD 32-bit • Name: <i>DoNotStopCustomScriptOnCancel</i> • Value: 1 Key #4 • Type: DWORD 32-bit • Name: <i>SupportMultipleDesktops</i> • 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
Performance Registry Key S	Settings	
Increase the time that the Evidian EAM Client waits for the initialization of the <i>nymi_api.dll</i> 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

6.6.8 - Silent Installations of Evidian EAM Client and SSO Engine

For environments with a large number of user terminals, you can use enterprise tools to deploy the software and registry key settings from a central location.

When designing your strategy, export the following registry keys:

- HKEY_LOCAL_MACHINE\Software\Nymi\NES, which defines the <u>NES_URL</u>.
- *HKEY_LOCAL_MACHINE\Software\Enatel*, which defines the Evidian EAM Client configuration.
- *HKEY_LOCAL_MACHINE\Software\Evidian*, which contains Evidian license information.

6.6.9 - (Citrix/RDP environments only) Configuring Citrix/RDP Clients to Access the Centralized Nymi Agent

On the user terminals that access the MES 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

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

6.6.10 - 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.
- 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.

6.6.11 - Enabling LDAPS Support

Perform the following steps on each terminal in the environment when you configure the Evidian EAM Controller to use LDAPS.

About this task

Consider using Group Policy Objects (GPO) to make this change.

Procedure

- 1. Run regedit.exe.
- 2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork.
- 3. Right-click WGDirectory, and then select New > DWORD (32-bit) value
- 4. In the Value file, type SSL.
- 5. Double-click the SSL key, and in the Value data field, type 1.
- 6. In the *ServerList* key, confirm that the path to the AD LDS instance with the secure port appears. For example, *srv-ssl.ssl.lan:636.*.
- 7. Close Registry Editor.

6.6.12 - Logging into the terminal

If you installed the Evidian SSOAgent with the Authentication Manager authentication mode, 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 an NFC 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.

6.6.13 - Validating the EAM Client Installation

After you log into the computer, validate that the Evidian EAM Client can connect to the Evidian EAM Controller and that the EAM client can retrieve certificates from NES.

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



Figure 86: 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.

• Navigate to C:\Windows\System32\config\systemprofile\AppData\Roaming\Wymi\WSL \random_string\ksp, and confirm that you see at least 20 files, as shown in the following figure. If you see 9 files only, refer to the Nymi Connected Worker Platform with Evidian Troubleshooting Guide for more information.

K Local Disk (C:) > Windows > System32 > config	› systemprofile › AppData	> Roaming > N	lymi > NSL > Yr2hs4Og > ksp
Name	✓ Date modified	Туре	Size
📑 AAAB	2023-03-08 4:54 PM	File	1 KB
📑 AAAC	2023-03-08 4:54 PM	File	1 KB
AAAF	2023-03-08 4:54 PM	File	1 KB
📑 AAAG	2023-03-08 4:54 PM	File	1 KB
📑 АААН	2023-03-08 4:54 PM	File	1 KB
AAAI	2023-03-08 4:54 PM	File	1 KB
f3HdCDshM9mGTPvL	2023-03-08 4:54 PM	File	1 KB
f3HdCDshM9mGTPvL-ext	2023-03-08 4:54 PM	File	1 KB
📑 g79C1qzPGjzdmE9R	2023-03-08 4:54 PM	File	1 KB
📑 g79C1qzPGjzdmE9R-ext	2023-03-08 4:54 PM	File	1 KB
📑 hZi-s1zzMi35h6Yi	2023-03-08 4:54 PM	File	1 KB
hZi-s1zzMi35h6Yi-ext	2023-03-08 4:54 PM	File	1 KB
📑 hzIUAUPcMUjnBSPu	2023-03-08 4:54 PM	File	1 KB
hzlUAUPcMUjnBSPu-ext	2023-03-08 4:54 PM	File	1 KB
QsreoP9t7qycffDk	2023-03-08 4:54 PM	File	1 KB
CsreoP9t7qycffDk-ext	2023-03-08 4:54 PM	File	1 KB
T60b91aL3RqMIr90	2023-03-08 4:54 PM	File	1 KB
T60b91aL3RqMIr90-ext	2023-03-08 4:54 PM	File	1 KB
mtezycZsMSPIfpWz	2023-03-08 4:54 PM	File	1 KB
wMEzycZsMSPIfpWz-ext	2023-03-08 4:54 PM	File	1 KB

Figure 87: Certificates Folder

6.6.14 - Updating User Terminal with new SSO Configuration

To enable the user terminal to use SSO and the Nymi Band with the MES application, refresh the Enterprise SSO application.

Before you begin

Install the MES application. If the MES 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 MES application.

Procedure

- 1. In the Windows System Tray, click on the Enterprise SSO (eSSO) 2 icon.
- 2. Click the Home Oicon, 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 88: eSSO application Home Window

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

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

	Properties Change Password New account Delete Show password Delegate Add to favorites Remove from favorites	
~	Hide applications without credential Open SSOStudio	
Enterprise SS	Start application Create shortcut	- 🗆 X
Application	Disable the application Enable the application Enable all applications	Account

Figure 89: 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

Evidian Enterp	e SSO Session - Re-authentication	
	Enterprise Single Sign-On	
Login:	••• Administrator	
Password:		
Log on to:	NYMI ~	
	OK Cancel	

Figure 90: SSO Login screen

6. Close the SSO application.

If a Nymi Band is authenticated, you can now use your Nymi Band to perform authentication events in the SSO application.

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, it is necessary to right-click the technical definition and select **Update Directory** and delete the Evidian cache.

6.7 - Configuring Support for 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.

6.8 - Silent Installations of Evidian EAM Client and SSO Engine

For environments with a large number of user terminals, you can use enterprise tools to deploy the software and registry key settings from a central location.

When designing your strategy, export the following registry keys:

- HKEY_LOCAL_MACHINE\Software\Wymi\NES, which defines the NES_URL.
- *HKEY_LOCAL_MACHINE\Software\Enatel*, which defines the Evidian EAM Client configuration.
- HKEY_LOCAL_MACHINE\Software\Evidian, which contains Evidian license information.

6.9 - Enrolling a Nymi Band

Before a new user or an existing user (enrolled in NES prior to an Evidian intergation) can use a Nymi Band to perform authentication events with Evidian and Evidian-integrated MES 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 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.

7 - Post Deployment Considerations

Review this section for information about tasks that you perform after you deploy the with Evidian solution, such as backup and recoveries and the steps you must perform when you add new users, user terminals, and enrollment terminals to the solution.

7.1 - Adding New Users and Computers to the Solution

After you deploy the Nymi with Evidian solution, you must perform the following tasks when you add new computers or users to the solution.

- When you add new users to the solution, ensure that you:
 - Add their Active Directory user account to the Active Directory inclusion group.
 - Assign the appropriate user profile to their user account in the Evidian EAM Management Console.
- When you add new computers to the solution, ensure that you assign the appropriate access point profile to the computer in the Evidian EAM Management Console.

7.2 - NES Backup and Recovery

Review this section for information about how to perform backups and recoveries of the NES host and NES database.

This section assumes that you:

- · Deployed NES on a virtual machine
- The SQL instance resides on a server that differs from the NES server.
- Maintain the same FQDN and IP address for the NES virtual machine at the time of backup and the time of restore.
- Maintain the same FQDN and IP address for the SQL server virtual machine at the time of backup and the time of restore.

7.2.1 - NES Backups

To protect the Connected Worker Platform and certificate data on the NES machine, perform a backup of the NES virtual machine after you complete the initial installation and each time you change the NES or IIS configuration.

Use VMware vMotion or perform snapshots to backup the virtual machine.

7.2.2 - NES Database Backups

NES stores Nymi Band information, Nymi Band user information, and audit events securely in a SQL database named Nymi.<u>NES_service_name</u>, where <u>NES_service_name</u> is the NES service mapping name that you configured in the NES Setup wizard. For example, **Nymi.nes**

Use your corporate backup and recovery software to back up the SQL database. The recovery point objective (RPO) determines the frequency of the NES database backup.

See Microsoft for more information about how to protect the SQL server.

7.2.3 - NES Server and Database Recoveries

Use your corporate backup and recovery software to restore the NES database on the SQL server and use VMware vMotion or snapshots to restore the virtual machine.

Note: You cannot recover the following data from a database restore:

- Any NES database changes, such as Nymi Band enrollments, Nymi Band re-enrollments, Nymi Band disassociations, and application policy changes that you perform after the last backup and prior to the failure.
- NES audit events that were recorded after the last backup and prior to the failure.

7.3 - Evidian EAM Controller Backup and Recovery

Review this section for information about how to perform backups and recoveries of the Evidian EAM Controller host and audit database.

This section assumes that you:

- Deployed the Evidian EAM Controller on a virtual machine
- Created the audit database a server that differs from the Evidian EAM Controller server.
- Installed ADLDS on the same virtual machine as the Evidian EAM Controller.
- Maintain the same FQDN and IP address for the Evidian EAM Controller server virtual machine at the time of backup and the time of restore.
- Maintain the same FQDN and IP address for the SQL server virtual machine at the time of backup and the time of restore.

7.3.1 - Evidian EAM Controller Backups

Use Virtual Machine(VM) snapshots to backup the Evidian EAM Controller virtual machine.

Perform a VM snapshot of the Evidian EAM Controller virtual machine:

- After you complete the initial installation.
- On a regular basis, as defined by your backup policy and your recovery point objective(RPO).

7.3.2 - Audit Database Backups

Evidian EAM Controller stores audit information in a SQL database named eamaudit.

Use your corporate backup software to back up the SQL database. The recovery point objective (RPO) determines the frequency of the audit database backup.

See Microsoft for more information about how to protect the SQL server.

7.3.3 - Evidian EAM Controller Server and Audit Database Recoveries

Use your corporate backup and recovery software to restore the audit database on the SQL server and use snapshot recovery to restore the virtual machine.

Note: You cannot recover the following data:

- Any ADLDS changes, such as Nymi Band enrollments, Nymi Band re-enrollments and Nymi Band disassociations that you perform after the last backup of the Evidian EAM Controller virutal machine and prior to the failure.
- Evidian EAM Controller audit events that were recorded after the last database backup and prior to the failure.

8 - Manage the Nymi Band

This section provides information about administrative tasks related to the Nymi Band, that an EAM administrator can perform, including what to do when a user no longer needs the Nymi Band, what to do when a user loses their Nymi Band, how to assign a temporary Nymi Band to a user, and what do to when a user finds their lost Nymi Band.

8.1 - Migrating Existing Nymi Bands to Evidian

If you introduce Evidian into an existing Nymi direct integration environment, such as POMSnet, existing Nymi Band users must log in to the Nymi Band Application on the enrollment terminal to complete the enrollment on the Evidian EAM Controller.

Before you begin

Ensure that the user is wearing their authenticated Nymi Band.

About this task

Procedure

- 1. Log into the Nymi Band Application with the username and password of the user that will enroll the Nymi Band.
- 2. Close the Nymi Band Application when the enrollment completes

Results

The Nymi Band Application detects that the user enrollment exists in the NES database and automatically updates the Evidian database with enrollment information.

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 MES 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 MES 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 - Viewing the Nymi Band Associated with a User

Perform the following steps to view information about the Nymi Band that is enrolled to a user.

Procedure

- 1. In the Evidian EAM Management Console, select the **Directory** panel.
- 2. 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.

	Evidian Enterpri	se Access Management Console Fiew Help		
*******	$\leftarrow \rightarrow \equiv$	□ 📮 🖸 💘 💘 💄 📮 🛎 📮 ⊄		
	A	Search request		
	Directory Smart Card	Search request Search request EAM EAM	Configuration Use this tool to search for objects in the directory. Objects that are found can easily be accessed from the tree view. Filter applies to object name. Examples: if you want to find a user called 'john doe', type 'john doe' if you want to find an application whose name starts with 'app', type 'app'' if you type an '@' character, the filter also applies to the email address (when available) 	
	((•)) RFID		Search root: Select Remove Object type: User Filter: twadmin Search Clear all	
	Biometrics	TW-Lab	Maximum number of results: 50	

Figure 91: Search request window

- 3. Click Search.
- 4. Select the user, and then select the **RFID** tab.

Figure 92: RFID tab for a user

User: UATAdmin				
	Homaton Amon Deligation Homaton Hamaton Hamat	ection Associate	Profiles Advanced	International Accordance Accords of PADO O Bonetics O Events

Two entries display, one for the user as an RFID entry and the other is a wearable entry.

8.3 - Replacing, Re-Enrolling or Re-Registering the Nymi Band for a User

After a user enrolls to a Nymi Band, there are several reasons that a user might need to repeat enrollment:

- User might need to temporarily enroll to another Nymi Band when they have forgotten their Nymi Band at home.
- User might need to permanently enroll to another Nymi Band when they have lost their Nymi Band or the Nymi Band does not function correctly.
- User might need to re-enroll their Nymi Band when the characteristics of their fingerprint change, for example, when their finger has a cut.
- ٠

Nymi provides you with configuration options that allow users to perform self-service reenrollment without the assistance of an CWP Administrator. Alternatively, you can ensure that users only complete re-enrollment with the assistance of a CWP Administrator.

The steps to replace or re-enroll a Nymi Band differ depending on your configuration.

8.3.1 - Managing Nymi Band Re-Enrollments and Re-registrations with Self-Service

When you enable the self-service enrollment and self-service registration feature in the active Nymi Enterprise Server(NES) administration policy, users can re-enroll and re-register their own Nymi Band or optionally a Nymi Band that is currently assigned to another user without the assistance of an CWP Administrator.

Before you begin

Customizing Self-Service Re-Enrollment and Self_service Re-Registration provides detailed information about how to configure the NES active policy to allow a user to self-enroll and self-register their own Nymi Band or to the Nymi Band of another user.

Note: User with SEOS-enabled Nymi Bands cannot use self-service re-enrollment to re-enroll a Nymi Band that was previously assigned to a another user.

About this task

Instruct the user to perform the following steps.

Procedure

- 1. Perform the delete user data operation on the Nymi Band identified for re-enrollment.
- Log into the Nymi Band Application and complete the steps for enrollment. The steps to complete a re-enrollment and re-registration are identical to the steps that the user follows to complete a new enrollment and registration.
- **3.** For FIDO2 only, when a user enrolls to another Nymi Band, the user must re-create the FIDO2 security key on the newly enrolled Nymi Band.

Results

If the user re-enrolls/re-registers their own Nymi Band, the same Nymi Band appears in the User Properties window in the NES Administrator Console.

If a user re-enrolls/re-registers a Nymi Band that was assigned to another user, the following changes appear in the User Properties window in the NES Administrator Console of the Enrollment NES and Registration NES:

- The original Nymi Band appears for the user is not active but remains as the primary Nymi Band.
- The newly enrolled Nymi Band appears for the user and is set to active.

The following figure provides an example where a user named tw-user2 enrolled to a Nymi Band with serial number AAAH-00125, and then performed a self-service enrollment to second Nymi Band with serial number ACAK-00056.

User Login ID	TW-Lab.local\tw-user2	Individu	ial User Policy		
Created	2024-01-31	None		~	
Modified		Notes	Global policy	will be applicable	
Notes		Liveness	Detection		
		Corpora	te Credentials Authe	ntication 🛛	
		Haptic F	eedback on Nymi Ba	inds 🛛	
	/	Allow a Band	user to re-enroll thei	r Nymi 🛛	
		Allow a Nymi Ba	user to re-enroll to a nd	ny active 🛛	
Nymi Band	ls				
Serial Number	Is Active	Is Primary	Notes	Created	
AAAH-00125		Primary		2024-02-08	Discon
ACAK-00056	Active			2024-02-08	Discon

Figure 93: User with multiple Nymi Bands after self-service re-enrollment.

8.3.1.1 - Evidian Behaviour with Self-Enrollments

The following section describes what you see in the Evidian EAM Management Console after a user completes a self enrollment.

If a user re-enrolls to a Nymi Band that was assigned to another user or an unassigned Nymi Band, the RFID tab for the user displays the entries for NFC UID and MAC address for the newly enrolled Nymi Band as well as the NFC UID and MAC address entry for the previously enrolled Nymi Band.

Note: The user can use both Nymi Bands to complete authentication tasks in Evidian windows.

The following figure provides an example.

- P Search request	information	Connection	Security P	rofies 🖹	Administration	18 Access Points
⊕. P qs5		Smart Card			RFID	
🔅 🚔 Srikanth Annam	RFID Identifier		State	Battery status		Refresh
QA-Lab	97EA003F0 12	SEE .	Active	Not available		Assign
	SPDA76EDCC	181	Active	Not available		Lock
	Interpretation (10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	AC/E2	Active	Not available		Delete

Figure 94: RFID tab for User with multiple Nymi Bands after self-service re-enrollment.

Managing Nymi Band self-enrollments with Evidian

Nymi recommends that you do not manually manage Nymi Band entries for a user after selfenrollment.

If the user re-enrolled to a new Nymi Band because their original Nymi Band was not available, for example the Nymi Band was lost or forgotten at home, perform the following steps:

1. Instruct the user to continue to use their newly enrolled Nymi Band.

- **2.** Instruct the user to perform a delete user data operation on the originally enrolled Nymi Band.
- **3.** Use the originally enrolled Nymi Band as a spare or provide it to a another user for enrollment.

8.3.2 - Re-enrolling/Re-registering a User to the Same Nymi Band without Self-Service

User might require re-enrollment and re-registration of their current Nymi Band in the event of multiple fingerprint authentication failures or when must use a different fingerprint for authentication, for example, due to a cut.

Before you begin

Perform a delete user data process of the Nymi Band. See section Deleting User Data for more information.

About this task

To re-enroll and re-register a user to their Nymi Band, the NES Administrator must delete the Nymi Band to user association in NES and the user or administrator must delete the user data on the Nymi Band.

Perform the following steps in the NES Administrator Console to assign a Nymi Band to a different user. In an IT/OT configuration perform these steps on the Enrollment NES and Registration NES.

Procedure

- 1. In the search page, select the Users Option.
- 2. In the search field, type the full or partial username, first name, or last name of the user.
- 3. Click search. The Search page displays the user, or a list of users that match the search criteria.
- 4. Select the Domain\username link of the user to open the User Details page.
- 5. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **Disconnect**. On the Disconnect page, scroll down and then click **Disconnect**.

What to do next

Contact the user to enroll the Nymi Band with the Enrollment Terminal. In IT/OT configurations, instruct the user to register with the Registration Terminal.

When the enrollment and if required, registration succeeds, in the NES Administrator Console of the Enrollment NES and Registration NES, search for the user in the NES Administrator Console, open the User Details page and confirm that in the Nymi Band table, the Nymi Band is Active.

8.3.2.1 - Evidian Behaviour with Self-Enrollments (Same Nymi Band)

The following section describes what you see in the Evidian EAM Management Console after a user completes a self enrollment.

If the user re-enrolls their own Nymi Band, the RFID tab for the user displays the entries for NFC UID and MAC address for the new instance of the Nymi Band as well as the MAC address entry for the old Nymi Band.

The following figure provides an example.



Figure 95: RFID tab for User re-enrolls their Nymi Bands with self-service re-enrollment.

Nymi recommends that you do not manually manage Nymi Band entries for a user after selfenrollment.

8.3.3 - Returning a Nymi Band Without Self-Enrollment

When a user no longer requires their Nymi Band, you must delete the Nymi Band association in NES and Evidian, and then perform a delete user data operation on the Nymi Band.

After you complete these steps, you can assign another user to the Nymi Band.

8.3.3.1 - Removing the User Association to the Nymi Band in Evidian Enterprise Access Management

This procedure removes the association between the user and the Nymi Band in Enterprise Access Management (EAM) and deletes the biometric data from the Nymi Band.

About this task

Log into the Evidian EAM Management Console with an account that is an EAM Administrator.

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 96: Search request window

- 4. Click Search.
- 5. Select the user, and then select the **RFID** tab.

Figure 97: RFID tab for a user

User: UATAdmin				
	Environ Constant Session Delegation	ection 🛛 👗 Securi 👩 Mobile Devices	ty Profiles 🛛 😤 Administ	ntion Mathematica Application Access PRID Benetics O Events
IN O LAM	RFID Identifier	State	Battery status	Refresh
in Carl Evidian Enterprise Access Management	\$F022D3390F409	Active	Not available	
Application access	F-179:73:71:60:00:82	Active	Not available	Assign
Application security objects				Lock
- & Default Pfcp				
- fip Default Password policy				Blacklist
Default application profile				
Applications				
Technical definitions				
· User Access				
🕫 🧰 Program Data				

Two entries display, one for the user as an RFID entry and the other is a wearable entry.

- 6. Select the Wearable entry, and then click **Blacklist**.
- 7. On the Confirmation window, click Yes.
- 8. On the Confirmation window, click Yes. The RFID and Wearable entries are blacklisted.
- 9. Select the wearable entry, and then click Delete.
- 10.On the Confirmation window, click Yes.
- **11.**Select the RFID entry, and then click **Delete**.
- 12.In the left navigation pane, select RFID.
- 13. From the RFID state list, select Blacklisted, and then click Apply.

Two blacklisted entries appear for the user, one for the RFID and one for the Wearable, as shown in the following figure

RFID						
Filter of RFID search RFID state	Blacklisted			~		
Battery status	All ~		~			
Show RFID to	okens expiring wit	hin	10	🗘 days.		(Apply)
Owner		RFID Ide	ntifier	State	Battery status	Expiration Date
₩∎Ev2-Uat1 (₩Ev2-Uat1		2F:2D:80 5FDB2C4	0:08:7 133FBD6E	Blacklisted Blacklisted	Unkown Unkown	

Figure 98: Blacklisted Nymi Band

14.Select the RFID entry, and then click **Delete**.

15.Select the Wearable entry, and then click **Delete**.

8.3.3.2 - Removing the user association to the Nymi Band in NES

Perform the following steps to remove the Nymi Band association to the user in NES.

Procedure

- 1. In the search page, select the users Option.
- 2. In the search field, type the full or partial username, first name, or last name of the user.
- 3. Click search. The Search page displays the user, or a list of users that match the search criteria.
- 4. Select the Domain\username link of the user to open the User Details page.
- 5. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **Disconnect**. On the Disconnect page, scroll down and then click **Disconnect**.
- 6. On the Disconnect screen, scroll to the bottom and select Disconnect.

8.3.3.3 - Deleting User Data on Nymi Band 3.0

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 if the **Haptic Feedback on Nymi Bands** is not enabled for the user or active group policy.



Figure 99: 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 100: 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.

8.3.4 - Handling a Lost Nymi Band Without Self Enrollment

When a user loses their Nymi Band, perform the following steps to disable the Nymi Band in EAM and prevent another user from using the Nymi Band.

About this task

After completing these steps, enroll and assign a new Nymi Band to the user.

Procedure

- 1. In the Evidian EAM Management Console, select the Directory panel.
- 2. 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.

Fi	Evidian Enterpri	se Access Management Console /iew Help					
	$\leftarrow \rightarrow \square$:■ © …, …, ≗ ⊑ ≗ ⊑ ⊄					
		Search request	Sconfiguration				
5	Smart Card	EAM Evidian Enterprise Access Management Application access User Access Default access point Profile Default access point profile RFID-only	Use thi from th Exampl - if you - if you - if you	tool to search for objects in the directory. O te tree view. Filter applies to object name. ss: want to find a user called 'john doe', type 'jol want to find an application whose name start type an '@' character, the filter also applies t	bjects that are fo nn doe' s with 'app', type ' to the email addres	und can easily 'app*' ss (when avail	y be accessed able)
	((•)) RFID	Timeslices Timeslices Timeslices Torgaran Data	Search root: Object type:	User	Sei	lect	Remove
	Biometrics	Inbound access Gutbound access ⊕- ◆ TW-Lab	Hiter:	twadmin Maximum number of results:	j0	earch	Clear all

Figure 101: Search request window

- 3. Click Search.
- 4. Select the user, and then select the RFID tab.

Figure 102: RFID tab for a user

User: UATAdmin					
P Search request P e/3-ustadmin A UATAdmin	Homation 📙 Con	nection 🛛 👗 Security 🗿 Mobile Devices	Profiles 📃 😤 Administ	Inition Mc Application Access RFID O Bornetrics	Accounts O Events
IN CO LAM	RFID Identifier	State	Battery status	Refresh	
🖟 🦳 Evidian Enterprise Access Management	SF02203390F409	Active	Not available		
Application access	H-79:73:71:60:00:82	Active	Not available	Assign	
Application security objects				Lock	
- & Default Pfcp					
- Mp Default Password policy				Blackfist	
Default application profile					
B Applications					
Technical definitions					
🛞 🧰 User Access					
🕸 🧰 Program Data					

Two entries display, one for the user as an RFID entry and the other is a wearable entry.

- 5. Select the Wearable entry, and then click Blacklist.
- 6. On the Confirmation window, click Yes.
- 7. Select the wearable entry, and then click Delete.
- 8. On the Confirmation window, click Yes.

Results

The Nymi Band is blacklisted in EAM. If the another user attempts to use the Nymi Band for authentication tasks result in an error stating that the certificate on the Nymi Band has been revoked.

Note: After blacklisting the Nymi Band, do not delete Nymi Band from the user. If you delete the Nymi Band, another user can enroll the Nymi Band.

8.3.4.1 - Removing the user association to the Nymi Band in NES

Perform the following steps to remove the Nymi Band association to the user in NES.

Procedure

- 1. In the search page, select the Users Option.
- 2. In the search field, type the full or partial username, first name, or last name of the user.
- 3. Click search. The Search page displays the user, or a list of users that match the search criteria.

- 4. Select the Domain\username link of the user to open the User Details page.
- 5. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **Disconnect**. On the Disconnect page, scroll down and then click **Disconnect**.
- 6. On the Disconnect screen, scroll to the bottom and select Disconnect.

8.3.5 - Handling a found Nymi Band Without Self-Enrollment

When you find a lost Nymi Band, perform the following steps to allow another user to use the Nymi Band.

About this task

Log into the Evidian EAM Management Console with an account that is an EAM Administrator.

Procedure

- 1. In the Evidian EAM Management Console, select the **Directory** panel.
- 2. 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 103: Search request window

- 3. Click Search.
- 4. Select the user, and then select the **RFID** tab.
- 5. Select the RFID device, and then click Delete.
- 6. Select the wearable device, and then click Delete.

Results

The Nymi Band is available for enrollment and assignment to a new user.

8.3.5.1 - Removing the user association to the Nymi Band in NES

Perform the following steps to remove the Nymi Band association to the user in NES.

Procedure

- 1. In the **Search** page, select the **Users** Option.
- 2. In the search field, type the full or partial username, first name, or last name of the user.
- 3. Click search. The Search page displays the user, or a list of users that match the search criteria.
- 4. Select the Domain\username link of the user to open the User Details page.
- 5. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **Disconnect**. On the Disconnect page, scroll down and then click **Disconnect**.
- 6. On the Disconnect screen, scroll to the bottom and select Disconnect.

9 - Updating Nymi and Evidian Components

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

The section describes how to update the components in a Connected Worker Platform with Evidian solution.

9.1 - 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.

Enrollment / F	Registration Settings
Enrollment / Registration Permission	Enrollment Only
Enrollment / Registration Destination	NES and Evidian
Display Band Label on Nymi Bands	
Allow a user to re-enroll / re-register their Nymi Band	

Figure 104: NES and Evidian enrollment option

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

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

By default, when an Evidian-integrated MES 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 MES 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.

9.2 - Updating the Evidian EAM Controller

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

Before you begin

If you use LDAPS, before you perform the following steps you must first to revert the configuration to LDAP.

- 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.

Registry Editor			- 0
File Edit View Favorites Help			
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\	WiseGuard\FrameWork\WG	Directory	
Authentication Cache Config Directory ESSO DEDICATED STOF	Name DirectoryType NootLdapDN	Type REG_SZ REG_DWORD REG_SZ	Data (value not set) 0x00000007 (7) O=EAM
FinkServer FinkServer WGDirectory Evidian		REG_SZ REG_DWORD	1W-5tV2.1W-Lab.local:55000 0x00000000 (0)

Figure 105: WGDirectory changes

4. Restart the Enterprise Access Management Security Services service.

Procedure

- 1. Log in to the server as a local administrator.
- 2. Download and extract the Evidian software package, *EAM-v10.0x.xxxxxx.zip* to a directory on the server, (for example, the *Downloads* directory).
- 3. Double-click the C:\Downloads\EAM-v10.0xxxxx.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 Dedicated 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.

Enterprise Access Management Controller		
Enterprise Access Management	The EAM Controller is now installed.	
Evidian	☑ Start EAM Console	
	< Back Finish Cancel	

13.For LDAPS deployments only, perform the following steps:

- **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 ox.

Evidian Enterprise Access Management - Open Session				
0	Enterprise Access Management			
Login:	••• uatadmin 🗸			
Password:	••••••			
Log on to:	TW-LAB \checkmark			
	OK Cancel			

Results

The Evidian EAM Management Console appears.

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

The Connected Worker Platformsoftware 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 or.
- 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.

9.3 - 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.

Nymi Runtime 5.0.5.46 Setup
Image: marked block installed.
Image: marked block installed.
Image: marked block installed.



Entire feature will be unavailable

Reset Disk Usage Back Next Cancel

Figure 106: 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**.

Browse...
🛃 Nymi Runtime 5.0.5.46	Setup		Ð		_		(
Nymi Runtime Setup Select the way you wan	t features to be insta	alled.				-~)
Click the icons in the tre	e below to change th	e way	features w	ill be ins	stalled.		
Nymi Ru	ıntime Nymi Agent Nymi Bluetooth Endpo	pint	This featu hard drive	ure requ e.	iires OKE	on your	
<		>				Browse	
Reset	Disk Usage		Back	Ne	xt	Cancel	

Figure 107: 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.

Nymi Runtime 5.13.0.3			×
Account to run system services as			6
Service Account:			
NT Authority Local Service		~	
The service account must be allowed to Service" or an error will occur.	Logon as		
	Back	Next	Cancel

Figure 108: 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*. Refer to Appendix—Record the CWP Variables for the service account name.

The following figure shows the Nymi Infrastructure Service Account window.

(Optional) Hymi infrastructure service account If you are installing a hymi Agent on a dent machine, leave the service account username and password blank. If you are installing a centralized Nymi Agent on a server, type the username and password for the service account that communicates with NES. Service account username twi-ab/nymi_infra_service Service account password If work account password Back Next Cancel	17	Nymi Runtime 5.20.1.5 Setup	;
If you are installing a Nymi Agent on a client machine, leave the service account username and password blank. If you are installing a centralized Nymi Agent on a server, type the username and password for the service account that communicates with NES. Service account username [vt-dab'nymi_infn_service Service account password Back Next Cancel		(Optional) Nymi infrastructure service account	
If you are installing a centralized Nym Agent on a server, type the username and password for the service account that communicates with NES. Service account username [tw-lab(nymi_infra_service Service account password Back Next Cancel		If you are installing a Nymi Agent on a client machine, leave the service account username and password blank.	
Service account username [tv-lab/nymi_infra_service Service account password Back Next Cancel		If you are installing a centralized Nymi Agent on a server, type the username and password for the service account that communicates with NES.	
tv-lab'nymi_infra_service Service account password Back Next Cancel		Service account username	
Service account password Back Next Cancel		tw-lab \nymi_infra_service	
Back Next Cancel		Service account password	
Back Next Cancel		••••••	
Back Next Cancel		·	
Back Next Cancel			
		Back Next	Cancel

Figure 109: Nymi Infrastructure Service Account window

The installer creates the following files in the C: Wymi/WymiAgent/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.

9.4 - Update the Enrollment Terminal

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

9.4.1 - 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.

9.4.2 - 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\Enate\WiseGuard\FrameWork\Authentication* and then delete the *WearableNeedsRFID* registry key.
- **3.** Navigate to *HKLM\SOFTWARE\Enate\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 ox.
- 5. Close Registry Editor.

9.4.3 - 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-v10.0xxxxxxx\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-v10.0xxxxxxx\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 end we are	, 11001100	- 119±0	- cinc.	
🛃 Enterprise Access Management Client Setup	ρ	_		×
License Agreement You must agree with the license agreement belo	ow to proceed.			9
End User License Tern for Evidian License 2017-	ms and Conditi ed Products 06	ons	_	^
Installation, operation and use of all E this one, are exclusively governed by conditions of this Agreement, except to license agreement that is legally Agreement"), has been signed and ap wish to install. In the event that a c	vidian Licensed and subject to the extent the binding on oplies to the Li urrently valid	d Products to, all the at a separa Evidian censed Pr Separate	s includ terms a ate writ ("Separ oduct y Agreem	ing and ten ate /ou ent ~
 I accept the licer I do not accept the 	ise agreement he license agreeme	nt		
	< Back	Next >	Can	

The following figure shows the License Agreement window.

Figure 110: License Agreement window

5. On the Destination Folder window, accept the default, and then click Next. The following figure shows the Destination Folder window.

🕼 Enterprise Access Management Client Setup —		×
Destination Folder Select a folder where the application will be installed.		9
The Installation Wizard will install the files for Enterprise Access Managemen the following folder. To install into a different folder, click the Browse button, and select another fol You can choose not to install Enterprise Access Management Client by click to exit the Installation Wizard.	t Client in Ider. ing Cancel	
C\Program Files\Evidian\Enterprise Access Management\	owse	
< Back Next >	Can	cel

Figure 111: 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.

🛃 Enterprise Access	Management Client Setup -	×
Select Installation Select the desired	Type installation type.	0
O Typical	The most common application features will be installed. This option is recommended for most users.	
○ Complete	All application features will be installed. This option is recommended for the best performance.	
● Custom	Use this option to choose which application features you want installed and where they will be installed. Recommended for advanced users.	
	<back next=""> Ca</back>	ancel

Figure 112: 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 113: Ready to install the application

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



Figure 114: User account control

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



Figure 115: Evidian Client Installation Success window

9.4.4 - 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.

9.4.5 - (Optional) Configuring the Communication Protocol

If you use the enrollment terminal to also access NEAs, 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.

New System Variable		×
Variable name:	NYMI_NEA_SUPPORT_LEGACY_MODE	
Variable value:	0	
Browse Directory	Browse File	OK Cancel

Figure 116: New System Variable window

c) Click or.

9.5 - Update User Terminals

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

9.5.1 - 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. Create a backup copy of the C:\Wymi\Bluetooth_Endpoint\nbe.toml file.
- 3. Extract the Nymi SDK distribution package.
- 4. From the ... *Inymi-sdk* windows setup folder, right-click the Nymi Runtime Installer version.exe file, and select Run as administrator.
- 5. On the Welcome page, click Install.
- 6. On the User Account Control page, click Yes. The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
- 7. On the Welcome to the Nymi Runtime Setup Wizard page, click Next.
- 8. On the Nymi Runtime Setup window, 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**.

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.**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.

9.5.2 - 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\Enate\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 ox.
- 6. Close Registry Editor.

9.5.3 - 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-v10.0xxxxxxx\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-v10.0xxxxxxx\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 117: License Agreement window

5. On the Destination Folder window, accept the default, and then click Next. The following figure shows the Destination Folder window.

🕼 Enterprise Access Management Client Setup	_		×
Destination Folder Select a folder where the application will be installed.			9
The Installation Wizard will install the files for Enterprise Access Ma the following folder. To install into a different folder, click the Browse button, and select You can choose not to install Enterprise Access Management Clie to exit the Installation Wizard.	anagemen another fol nt by clicki	t Client in der. ng Cancel	
Destination Folder C:\Program Files\Evidian\Enterprise Access Management\	Br	owse	
<back 1<="" td=""><td>Vext ></td><td>Can</td><td>cel</td></back>	Vext >	Can	cel

Figure 118: 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.

🕼 Enterprise Access	Management Client Setup		-		×
Select Installation Select the desired	Type installation type.			_(9
○ Typical	The most common application featur is recommended for most users.	es will be ins	talled. This (option	
Complete	All application features will be installe recommended for the best performar	ed. This optic nce.	ın is		
● Custom	Use this option to choose which appl installed and where they will be instal advanced users.	ication featur led. Recomr	es you want nended for	:	
	< Ba	ick N	lext >	Car	icel

Figure 119: 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.

🛃 Enterprise Access Management Client Setup	-		×
Ready to Install the Application Click Next to begin installation.			9
Click the Back button to reenter the installation information or click (the wizard.	Cancel to ex	it	
< Back	vext >	Can	cel

Figure 120: Ready to install the application

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



Figure 121: User account control

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



Figure 122: Evidian Client Installation Success window

9.5.4 - 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.

New System Variable		×
Variable name:	NYMI_NEA_SUPPORT_LEGACY_MODE	
Variable value:	0	
Browse Directory	. Browse File	OK Cancel

Figure 123: New System Variable window

c) Click or.

9.5.5 - 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.

9.5.6 - 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





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.

9.6 - 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 Connected Worker Platform with Evidian solution, perform the following actions:

- Replace the token structure configuration on the Evidian EAM Controller and any 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.

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

The Connected Worker Platformsoftware 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 or.
- 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.

9.6.2 - Re-enrolling existing Nymi Band Users

After you update all the components in the Connected Worker Platform 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

9.6.2.1 - 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 124: Search request window

- Click Search.
- 5. Select the user, and then select the **RFID** tab.

Figure 125: RFID tab for a user

User: UATAdmin

Two entries display, one for the user as an RFID entry and the other is a wearable entry.

- 6. Select the Wearable entry, and then click **Blacklist**.
- 7. On the Confirmation window, click Yes.
- 8. On the Confirmation window, click Yes. The RFID and Wearable entries are blacklisted.
- 9. Select the wearable entry, and then click Delete.

10.On the Confirmation window, click Yes.

- **11.**Select the RFID entry, and then click **Delete**.
- **12.**In the left navigation pane, select **RFID**.
- **13.**From the **RFID** state list, select **Blacklisted**, and then click **Apply**.

Two blacklisted entries appear for the user, one for the RFID and one for the Wearable, as shown in the following figure

RFID					
Filter of RFID search RFID state	Blacklisted		~		
Battery status	All kens expiring with	nin 10	ç days.		Apply
Owner		RFID Identifier 2F:2D:8D:0B:7	State Blacklisted	Battery status Unkown	Expiration Date

Figure 126: Blacklisted Nymi Band

14.Select the RFID entry, and then click **Delete**.

15.Select the Wearable entry, and then click **Delete**.

9.6.2.2 - Deleting User Data on Nymi Band 3.0

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 if the **Haptic Feedback on Nymi Bands** is not enabled for the user or active group policy.



Figure 127: Delete User Data

 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 128: 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.

9.6.2.3 - Enrolling a Nymi Band

Before a new user or an existing user (enrolled in NES prior to an Evidian intergation) can use a Nymi Band to perform authentication events with Evidian and Evidian-integrated MES 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 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.

9.7 - 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) Z icon.
- 5. Click the Home Oicon, 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 129: eSSO application Home Window

10 - Appendix - Changing Evidian Authentication Method

Changing the authentication method from RFID to Wearable requires the following steps:

- Changing configuration settings on the Evidian EAM Controller
- Changing registry key entries on the Evidian EAM Clients
- Clearing the Evidian cache on the Evidian EAM Clients

10.1 - Obtaining the TokenManagerStructure file for the Evidian EAM Controller

Copy the *TokenManagerStructure-Nymi-Wearable.xml* file from the extracted Nymi installation package, in the *Evidian-Supplementary-Files* subdirectory. You will use this file to define the wearable as the default authentication method for the environment.

10.2 - Changing the Configuration of the Evidian EAM Controller

Perform the following steps in the Evidian EAM Management Console with an EAM Administrator account.

Procedure

- 1. Log into the Evidian EAM Management Console as an Evidian administrator.
- 2.



3. Expand EAM > Evidian Enterprise Access Management > User Access > Access Point Profiles > Default access point profile, as shown in the following figure.



Figure 130: Default Access Point Profile

4. On the Authentication Manager tab, clear Allow Roaming Session, and then click Apply, as shown in the following figure.

A	Access point profile: Default access point pr	ofile
Directory	P Search request	Seconfiguration 🗧 Applies to 🕕 Events
	EAM Enterprise Access Management	Computer security profile
	Condication access	Name Default access point profile
(±≞)	Application access	
	Applications	Schedule: Default time-slice →
Smart Card	- Technical definitions	
	SampleApp	Self Service Password Request Biometrics Active RFID Audit Local Administrators
	🖶 🧰 User Access	Security Services Authentication Manager Enterprise SSO Multi User Desktop
	AccessPoint Profiles	
RFID		Lock behaviour: Windows lock ~
	Imesices	Default action when token removed: Do nothing \vee
	Deer Promes	Delay before action: 0 seconds
	📮 Outbound access	Inactivity: automatically lock session after:
Biometrics	TW-Lab	Automatically close locked session after: 0 seconds
		Allow local connection
		Allow remote unblocking of tokens
		Remember authentication role
Mobile		Allow PIN change
Devices		Enable smart card detection on Ctrl-Alt-Del
		Grace period for administrator seconds
		Allow unlock if allowed by user security profile
Audit		Allow unlock if the same Windows credential is used.
Audit		Max, number of concurrent Windows sessions; 0 (from Windows 7)
		If you want to define Windows accounts which will be managed by
		EAM, press 'Manage Accounts'. Manage Accounts
Reporting		
		Apply Cancel
Figure 1	31: Authentication Manager window	1

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



Figure 132: User Profiles

6. Under the Security tab, clear the Roaming Session Duration and No duration limit options, as shown in the following figure, and then click Apply.

User profile: Default user profile	
Search request Search request Applications Applications	Configuration Applies to Events User security profile Name: Default user profile Biometrics Session delegation Audit OTP Mobile Device Email Notifications Authentication Change password every 7 change password every 7 change password on token every 7 days and on collect or expiration Automatic PFCP: Default Pfcp Allow external access Allow Emergency Plan SSO data protected by token is also available on password authentication SSO data is protected by session key Grace period 15 initutes Roaming session duration 12 hours. No duration limit

Figure 133: Roaming Session Duration Limit

7. From the File menu, select Configuration, as shown in the following figure.



8. On the Authentication Tab, click the select button, as shown in the following figure.

	Primary A	dministrators	SA Server H	losts	SA Server Configuration
Rep	ortina	SSPR by Confi	mation Code		User Self Enrollment
User	Notifications	Audit Clea	an-Up	Securi	tv Code Authentication
General	Default Values	Authentication	Other User	Attributes	Public Key Authentication
	diometrics_c /biometrics_ doken_mana dol dol 	onfig> config> gerid="SOFTWAI (and the soft) (and t	RE"> BILE" display_ fiftp> nnfig> wndule id="0x /module> cture> cture> cture> cture> cture> module id="0x /module> cture> module id="0x /module> module id="0x /module> p* display_nan fiftp> custom_otp_d ldap_attribute: nfig> ture> p* display_nan fiftp> custom_otp_d ldap_attribute: nfig> ture>	_name="Mi 0100"> 0200"> blay_name bble_dll>Cu 0100"> 0200"> ne="OTP" sAMAcco 0100">	obile Authentication' =''Wearable device' stomWearableExter >)TPExtensionRSA.d urtName

9. In the Open File dialog, navigate to the directory that contains the Wearable TokenManagerStructure file, select the TokenManagerStructure file, and then click Open.

10.Click **Apply**, which will validate the structure of the file.

11.Click or.

12.Close the Evidian EAM Management Console.

10.3 - Changing the Evidian EAM Client Configuration on User Terminals

To change the Evidian EAM Client configuration from RFID-only to Wearable, remove the roaming sessions registry key, and then rename the token management structure file, if the file exists.

About this task

Perform the following steps on each user terminal.

Procedure

- 1. Run Registry Editor.
- 2. Navigate to HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication.
- 3. Right-click the *RoamingSessionAllowedForSSO*, and then select **Delete**, as shown in the following figure.



Figure 134: Delete RoamingSessionAllowedForSSO

- 4. On the Confirm Value Delete window, click Yes.
- 5. Close Registry Editor.
- 6. From File Explorer, navigate to C:\Program Files\Common Files\Evidian\WGSS folder.
- 7. If the file exists, rename TokenManagerStructure.xml to TokenManagerStructure_rfid.xml

10.4 - Changing the Evidian EAM Client Configuration on the Enrollment Terminal

Remove the wearable token management structure file from the Enrollment Terminal, to ensure that the Enrollment Terminal retrieves the wearable configuration from the Evidian EAM Controller.

Procedure

- **1.** From File Explorer, navigate to C:\Program Files\Common Files\Evidian\WGSS folder.
- 2. Delete the *TokenManagerStructure.xml* file.
- **3.** Close File Explorer.

10.5 - Deleting Evidian EAM Client Cache

Perform the following steps to delete the cache files on 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.

Copyright ©2024 Nymi Inc. All rights reserved.

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

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

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

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