

RFID-Only Installation and Configuration Guide

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

Contents

Preface	4
Name Carriera Marken Die Germanisch Fridien Assess Management	
Nymi Connected Worker Platform with Evidian Access Management	
Solution	
Coexistence of Nymi-direct integrations and Evidian integrations	6
Environment Configuration	8
User Terminal Requirements	8
Enrollment Terminal Requirements	9
Using the Nymi Band as an RFID-only Device	10
Nymi-Evidian Architecture	
Obtain the Required Software	
Install Server Software	
Installing and Configuring NES	
Installing the EAM Controller software	
Installing and Configuring Software on the Enrollment Terminal	
Importing the Root CA certificate	27
Installing the Nymi Band Application	29
Installing the EAM Client	29
Configuring the EAM client to use the Nymi Band Application	32
Confirming the Runtime dll versions	33
Overriding the authentication method	34
Logging into the terminal	
Configure the Evidian SSO for an MES Application	
Adding an SSO definition for a new target application	
Configuring the SSO application in the EAM Console	
Configuring SSO to use AD Credentials	
Removing the MES application	
Installing and Configuring Software on the User Terminals and for remote MES application	
integration over RDP or Citrix	
Installing the EAM Client	
Setting the NES URL	
Enabling Roaming Sessions for SSO	
Logging into the terminal	
Installing the MES Application	
Updating User Terminal with new SSO Configuration	50

ii

Configuring Support for Users in Multi Domain Environments	52
Enrolling a Nymi Band	
Manage the Nymi Band	54
Viewing the Nymi Band Associated with a User	
Returning a Nymi Band	
Handling a lost Nymi Band	
Handling a found Nymi Band	
Upgrading Nymi and Evidian Components	60
Upgrading the NES software	
Modifying EAM Settings to Support Coexistence with other Solutions	
Updating the TokenManagerStructure	
Upgrading the Nymi Band Application on the Enrollment Terminal	
Confirming the Runtime dll versions	
Upgrading Nymi Components on the User Terminals and Remote NEA hosts	
Post Upgrade Tasks for Existing Users	
Enrolling Existing Nymi Bands in Evidian	
Re-enrolling existing Nymi Band Users in Evidian	66
Troubleshooting	69
Enabling Evidian Logging	
Troubleshooting Evidian Error Messages	
Evidian Security Services seems to not be running	
Evidian License has Expired	
EAM Security Services are not available	
Nymi Band Enrollment Fails: Failed to Create Security Settings	
User has two Active Bands after Enrollment	
Cannot Unlock the Enrollment Terminal	71
Cannot Perform Authentication events With the Nymi Band After Closing SSO	
Authentication Window	72
ESSO Credential Manager icon does not appear in the system tray	72
Authentication error: you are not allowed to close this user session	73

4

NymiTM provides periodic revisions to the Nymi Connected Worker Platform. Therefore, some functionality that is described in this document might not apply to all currently supported Nymi products. The product release notes provide the most up to date information.

Purpose

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

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
1.0		First release of this document for CWP 1.3.

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 NES Deployment Guide

This document provides the steps that are required to deploy the Nymi Enterprise Server (NES). This installation uses the Nymi Token Service to install certificates that enable communication between components. This document also provides information about deploying the Connected Worker Platform in a Citrix or RDP environment.

• Nymi Connected Worker Platform Administration Guide

5

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 BandTM, and how to use the Nymi Band Application. This document also provides instructions on deploying the Nymi Band Application and Nymi Runtime components.

• Nymi SDK for C Developer's Guide

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

• Nymi SDK for WebSocket Developer's Guide

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

• Nymi Connected Worker Platform Troubleshooting Guide

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

Connected Worker Platform Release Notes

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

How to get product help

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

How to provide documentation feedback

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

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 EAM Controller and the default configuration is pushed by the EAM Controller to the 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.

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.

6

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 EAM Client and 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.

7

Environment Configuration

8

The section outlines the configuration requirements for the enrollment terminal and the user terminals. Refer to the Nymi Connected Worker Platform NES Deployment Guide for details about NES requirements and the Nymi Connected Worker Platform Administration Guide for information about supported NFC readers.

User Terminal Requirements

The user terminal is a Windows 10 machine that operators use to perform MES authentication tasks. User terminals include local machines as well as machines that are connected to 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. 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	EAM Client, with a valid Evidian license fileNymi-supported NFC Reader.

Network Requirements

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

- For an ADLDS 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 EAM Client communicates with the Nymi Agent machine on default port 9120.

9

• For communications between the EAM Client and EAM Controller, communication occurs on port 3644.

Enrollment Terminal Requirements

- Evidian License File
- Nymi Band Application
- EAM Client
- Local Administrator access or Directory Administrator Access
- Connection to the enterprise domain
- BLE Adapter (BLED112)
- Bidirectional communication ports open on the firewall.
 - For an ADLDS configuration, 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 EAM Console, communications occurs on port 3644 on the access point.

Using the Nymi Band as an RFID-only Device

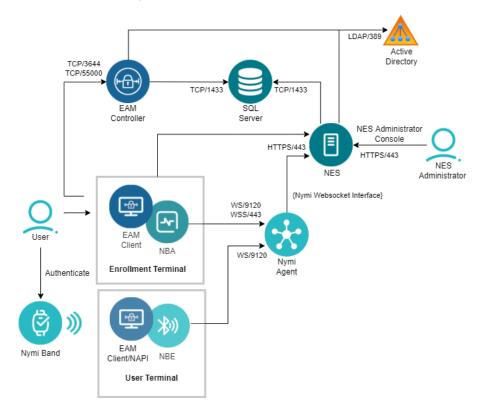
This chapter provides information about deploying the Nymi Band as an RFID-only device in a CWP with Evidian environment.

Note: In an RFID-only configuration, a terminal lock does not occur when an authenticated Nymi Band becomes deauthenticated.

Nymi-Evidian Architecture

In the configuration, two TokenManagerStructure files are used. Upload the RFID-only file to the EAM Controller and then copy the Wearable file to the enrollment terminal

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



Enrollment Terminal

User Terminal

The Windows 7 or Windows 10 machine where users enroll their Nymi Band.

The workstation on which you install Nymi components and the Evidian Access Manager (EAM) client.

Nymi Band Application	A native Windows application that is used to register biometric, employee ID, and Nymi Band with the enterprise. The Evidian version of the Nymi Band Application integrates directly to the Evidian ecosystem and facilitates communication between NES and the Nymi Bands. The Nymi Connected Worker Platform Administration Guide provides more information about the Nymi Band Application.
Enterprise Access Management Client	Also known as the Evidian 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.
	NES includes:
	 Enrollment Service - Authenticates, validates, and authorizes certificate requests from requesters, such as the Nymi Band Application and Nymienabled Application(NEAs. Directory and Policy Service - Maintains the NES database, and provides the IIS web service that allows the NES Administrator Console to access the NES database. Authentication Service - Provides authentication and authorization support for domain users and computers. The service currently uses an Active Directory (LDAP) interface.
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 EAM Console application provides the interface to perform management activities.
Corporate Directory	A server such as Windows domain controller that provides authentication services, such as Active Directory.
NFC Reader	Captures the NFC ID of the Nymi Band, which is used when an operator performs an SSO authentication event.
BLE112 Dongle	Nymi Band uses Blue Tooth Low Energy (BLE) to interact with external components and services. Nymi Band BLE communication does not rely on

Blue tooth security. All security is implemented using strong, standard-based cryptography. A BLE adapter (BLED112) is required on the enrollment terminal.

Obtain the Required Software

Obtain the required software files or the fileshare link for the software package from your field support team member.

When you receive the zip file, download and extract the contents to a machine and folder that is accessible to the NES and EAM Controller hosts.

Install Server Software

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

Installing and Configuring NES

You can install the NES software on the same server on which you plan to install the EAM Controller software. For deployments in a production environment, Nymi recommends that you install the NES and 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 NES 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.

- 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 Destination list, select the option NES and Evidian, as shown in the following figure, and then click Save.

Enrollment Destination	NES and Evidian	
Fingerprint Required		
Corporate Credentials Authentication		
NFC UID Capture	Mandatory	
Display Band Label on Nymi Bands		

Figure 1: NES and Evidian enrollment option

Installing the EAM Controller software

Install the EAM Controller software on a server.

Before you begin

Obtain a valid EAM license file.

About this task

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

Note: The installation of the controller software requires that you restart the server.

Procedure

1. Log in to the server as a local administrator.

For ADLDS deployments, the user must have schema rights to the Active Directory.

- 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. Copy the Evidian license file to the *Downloads* directory on the server.

4. 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.

5. For ADLDS deployments, 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.



- 6. On the User Account Control window, click Yes.
- 7. On the Welcome to the EAM Controller installation assistant window, click Next.
- If the Microsoft Visual C++ 2012 Update 4 redistributable is not installed on this machine, you will see the Prerequisites window, click Next. The Windows Installer window appears.
- 9. On the License keys window, click Import, as shown in the following figure.

	ise Access Management Controlle mse keys		
	Provide EAM license keys to enable s	software features.	
2		fou may not use it if you do not have a sime and conditions of the license agre nually or Import them from a file.	
	Customer ID:		Import
	Feature /	License key	
	Select license:	Enter your license key and press /	\dd:
	Authentication Manager base	·	Add

10. In the open window, select the license file in the *Downloads* directory, and the click Open.

If the file cannot be found, ensure file type is selected as **All Files** *.*

11.On the EAM Controller configuration window, click OK.

12.On the License keys window, click Next.

13.On the Storage for security objects window, click Next.

14.On the Dedicated Directory window, click **Select**.

15. In the Dedicated directory window, type the username and password for a domain account that will act as the dedicated EAM administrator.

The account must have local administrator access to the server.

Note: Select an account that has the option **Password Never Expires** in the AD properties of the user.

16.Click OK.

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

	Install the dedicated directory server		2
Z	The EAM Controller includes its own users accounts. The Controller requirer management operations.		
7	You must select the Windows doma domain account must have the right this account must never expire.		
	Controller Windows account:	NYMI\administrator	Select
	The selected account must be local	ted in the domain of this comp	uter.

17.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.

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

Audit database server Set up a database server for EAM au	idit events.
This wizard creates EAM audit data computer.	base tables in a database server installed on this
It provides automated installation for to documentation when using anoth	r MySQL, PostgreSQL and Microsoft SQL Server. Refer tertype of RDBMS.
🔿 Install a MySQL database se	erver dedicated to EAM audit
	erver dedicated to EAM audit s in an existing database server
O Create audit database table	s in an existing database server Microsoft SQL Server SQLEXPRESS
Create audit database table Select database server:	s in an existing database server Microsoft SQL Server SQLEXPRESS

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

		ou by delega	ated administrators.	
S	ecurity administrator's accou	unt:	NYMI\administrator	Select
A a			n of EAM security. The security as s EAM Console. The passphrase	
S	ecurity passphrase:	1)
C	Confirm:			

Note: Ensure that you make a note of the passphrase as you will need to reference it when starting the EAM Console for the first time.

20.Click Next.

21.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**.

	hentication methods Choose specific authentication methods	you want to enable for the solution.	
7	EAM natively includes the support for p additional authentication methods.	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 configurati	
	Biometrics authentication	Store-On-Server	4
	Biometrics provider	Upek	~
	RFID authentication	Contactless badge	

22.On the Software installation window, click Next.

The Windows Installer window appears, and the installation process begins.

23.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.



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

	Enterprise Access Manage	ement
Login:	••• administrator	~
Password:	•••••	
Log on to:	NYMI	~

25.On the Administration Pass-phrase window, type the 16-character passphrase that you created in the Secrets Initialization window, and then click **OK**. The EAM Console launches, as shown in the following figure.



What to do next

Install the Audit Database for the EAM Controller. Consider the following:

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

The *Evidian EAM Installation Guide* provides detailed information about how to install and configure the audit database.

Obtaining the TokenManagerStructure file for the EAM Controller

Obtain the *TokenManagerStructure-Nymi-RFID.xml* file software package. The file is located in the *Evidian-Supplementary-Files* subdirectory. You will use this file to define the RFID-only as the default authentication method for the environment.

About this task

Defining the Authentication Method

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 EAM Clients.

Procedure

- 1. On the EAM Console, from the File menu, select Configuration.
- 2. On the Authentication Tab, click the Select button, as shown in the following figure.

Options	Primary Ad	Iministrators	SA Server Ho	ata	SA Server Con	ficuration
	orting	SSPR by Confin			User Self Enro	-
	Notifications	Audit Clea		Securi	ty Code Authent	
ieneral		Authentication				
	ersion - "1.0" enco					
	doko	ی م د/data_strue	BILE" display_n fig> nfig> ture> module id="0x0" /module> module id="0x0" /module>	100">	oble Authentica	tion
	<td>en_class> an_class id="WE</td> <td></td> <td>ay_name</td> <td>-'Wearable dev</td> <td></td>	en_class> an_class id="WE		ay_name	-'Wearable dev	
< Auther	doke ntication token de	an_class id="WE		ay_name	-'Wearable dev	>

- **3.** In the Open File dialog, navigate to the directory that contains the TokenManagerStructure file, and then select the TokenManagerStructure file.
- 4. Click Open.
- 5. Click **Apply**, which will validate the structure of the file.
- 6. Click OK.
- 7. Close the EAM Console window.
- **8.** Run *regedit* and navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard* *FrameWork\Config.*
- 9. Edit the ManageAccessPoints key and change the value to 1.

10. Restart the Enterprise Access Management Security Services service.

Modifying EAM Settings to Support Coexistence with other Solutions

With 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 Nymiintegrated MES applications, perform the following steps to modify the settings in the access point profile, to prevent unexpected desktop locks when performing an NFC tap in the Nymi-integrated MES application.

Perform the following steps in the EAM Console

Procedure

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

Results

A user cannot perform an NFC 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.

Configuring roaming sessions

This section describes the EAM Controller configuration changes that are required to use a Nymi Band to perform authentication events on user terminals without Blue tooth communication.

About this task

Procedure

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

Select Account and access rights management

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

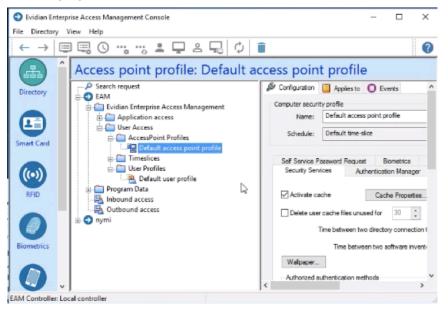


Figure 2: Default Access Point Profile

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

- P Search request	Configuration Applies to Configuration
EAM	Computer security profile Name: Default access point profile
User Access	Schedule: Default time-slice
	Self Service Password Request Biometrics Active RFID Audit Local Administrators Security Services Authentication Manager Enterprise SSO Multi User Desidop
Inbound access	Lock behaviour: Windows lock \checkmark
Evidian-UAT-Lab	Default action when token removed: Lock the session
	Delay before action: 0 seconds
	Inactivity: automatically lock session after:
	Automatically close locked session after: 0 seconds
	Allow Windows domain connection Only for
	Allow remote unblocking of tokens Allow remote unblocking of tokens Remember authentication role Multive reaming session
	Allow password change
	Enable smart card detection on Ctri-Alt-Del Allow remote control (QRentry) Grace period for administrator autheritication seconds
	Allow unlock if allowed by user security profile.
	Allow unlock if the same Windows credential is used.
	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
	Apply Cancel

Figure 3: Authentication Manager window

- 5. Navigate to Evidian Enterprise Access Management > User access > User Profiles > Default user profile.
- 6. Under the Security tab, select Roaming Session Duration and No duration limit, and then click Apply.
- 7. Close the EAM Console.

Configuring Additional EAM Controller Administrators

It is possible to add additional administrators to the EAM Controller.

About this task

By adding a secondary primary user, you have an additional user with access to the EAM Controller in the case where the primary user is locked out of the EAM Controller.

Procedure

- **1.** Log into the EAM Console.
- 2. From the File menu, select Configuration, and then click the Primary Administrators tab.
- 3. Click Add, as shown in the following figure.

Repo	pring	SSPR by Confi	mation Code		User Self I	Enrolment
	Notifications	Audit Clea		Secur	ty Code Aut	nentication
Seneral	Default Values	Authentication	Other User At	ributes	Public Key	Authentication
Options	Primary A	dministrators	SA Server Ho	ds	SA Server	Configuration
	iatrator - CN=Adi y primary adminis	ministrator.CN+Use strators	ara.DC=nymi.DC	-local		
				4dd	Remi	ove
				kdd	Remi	2/18
				kdd	Rema	208

- 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 OK.
- 7. Click Apply.
- 8. Click OK.
- 9. Close the EAM Console.

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 EAM Controller machine, ensure that the SQL service account has the right to log in locally and is a member of the local Administrators group.
- On the SQL server, ensure that the SQL browsing service is running.

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 click **Execute**.

Results

The eamaudit database appears in the **Databases** folder. **Configuring the EAM Controller to Use the Audit Database** Install and configure the ODBC driver for SQL on the EAM Controller.

About this task

Perform the following steps on the EAM Controller

Procedure

- 1. Stop the Enterprise Access Management Security Server service.
- 2. Download and install the Microsoft OLE DB Driver for SQL.
- 3. Start the Enterprise Access Management Security Server service.
- 4. From the EAM installation package, navigate to the ... *EAM.x64 VOOLS WGSrvConfig* folder.
- 5. Hold the Shift key, right-click WGSRVConfig.exe, and select Run as a different user.
- 6. In the Run as a different user window, specify the username and password of the SQL service account.
- 7. Under Controller Configuration, click Configure local audit database, as shown in the following figure.

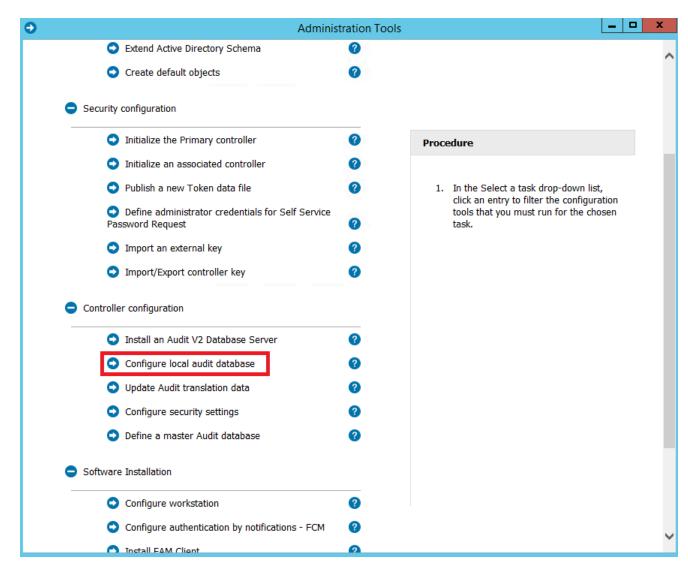


Figure 4: Configure local audit database option

- 8. In the Use existing corporate database section, next to Next to Data Source Name, click the ellipses (...).
- 9. Select Microsoft OLE DB Driver for SQL Server .

10.Click Next.

11. In the Data Link Properties, perform the following actions:

- a) In the **Select or enter a server name** field, type the name of the SQL server.
- b) From the **Enter information to log on to the server** list, select the appropriate authentication method for your configuration.
- c) In Step 3, select Select the database.
- d) From the list, select **eamaudit**.

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

Import an external ke	ny 🛛 🛛 🛜		2
Import/Export contro	Provider Connection Advanced All		
oller configuration	1. Select or enter a server name: ev3-uat-srv2	~	Refresh
Install an Audit V2 D	2. Enter information to log on to the serv		Thursday.
Configure local audi	Windows Authentication	~	
Dupdate Audit transla	Server SPN:		
Configure security s	Password:		
Define a master Auc	Blank password Use strong encryption for data		saving password
are Installation	3. (i) Select the database:	eamaudit	~
Configure workstati	Attach a database file as a database	ase name:	3
Configure authentica	Using the filename		
Install EAM Client	Change Password	Test Co	nnection
Install finger vein bio	ОК	Cancel	Help
Install EAM Controller			

Figure 5: Select the database window

- e) Click Test Connection
- f) On the Test Connection Succeeded window, click $\ensuremath{\text{OK}}$.
- g) Optionally, in Step 2, select the Use strong encryption for data and Trust server certificate options.
- h) Click Test Connection.
- i) On the Test Connection Succeeded window, click $\ensuremath{\text{OK}}$.
- j) In the Credential to access the database window, specify the username and password of the SQL service account, and then click \mathbf{OK} .

The Audit Database Configuration window appears with information about the database, as shown in the following figure.

	Audit Database	e Configuration				
i	The controller must connect to an existing database (through an OLE DB Provider) in order to support Audit and Reporting.					
	O Use an existing SQL Ser	ver instance.				
	Password:	•••••				
	Confirmation:					
	• Use existing corporate of	database				
	Data Source Name:	EV3-UAT-SRV2\SQLEXPRESS				
	Table name:	dbo.v_iamaudit 🗸 🗸				
		Use quotes				
Adva	nced Verify	Apply Close				

Figure 6: Audit Database Configuration window

k) On the Audit Database Configuration window, click **Close**.

l) Click Verify.

m) On the EAM Configuration pop-up, click OK.

12. Close the Administration Tools window.

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 EAM Client software on the enrollment terminal.

Importing the Root CA certificate

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

About this task

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

Procedure

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

The following figure shows the certlm window.

蕕 certlm - [Certificates - Local Compu	ter\Trusted Root Certificat	tion Aut	horities] —	\times
File Action View Help				
🗢 🄿 🙍 🗊 📋 🙆 🛃				
 Certificates - Local Computer Personal Trusted Root Certification Author 	Object Type			
Certificates	Find Certificates			
 Enterprise Trust Intermediate Certification Author 	All Tasks	>	Find Certificates	
 Trusted Publishers Untrusted Certificates 	View	>	Import	
> 🛄 Third-Party Root Certification A	Refresh			
Trusted People Client Authentication Issuers	Export List			
> Preview Build Roots	Help]	

Figure 7: certlm application on Windows 10

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

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 Current User Local Machine
To continue, click Next.
Next Cancel

Figure 8: 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**.
- On the File to Import screen, click Next.
 The following figure shows the File to Import screen.

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 format
Personal Information Exchange-PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)
Microsoft Serialised Certificate Store (.SST)

Figure 9: 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.

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.

Installing the EAM Client

Install the EAM Client on the enrollment terminal.

Before you begin

Before installing the EAM Client software:

- Complete the steps to configure the EAM Controller.
- Ensure that the machine is on the same domain as the EAM Controller.
- Obtain the Evidian license file from the Nymi Solution Consultant.
- Determine the Nymi Band use cases. To use the Nymi Band to unlock user terminals, you will configure the EAM Client with Authentication Manager. To use the Nymi Band for SSO activities only, you will configure the EAM Client with Windows Login.
- •

About this task

Perform the following steps on the enrollment terminal.

Procedure

- 1. Log in to the host as a Domain Administrator.
- 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. Copy the license file to the *Downloads* directory on the host.
- **4.** Double-click the *C:\Downloads\EAM-v10.0xxxxxx\Start.hta* file.

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 directly from *EAM-v10.01xxxxxx/QuickInstall.x64/Client/ESSOClientSetup-Dedicated.exe* Proceed to step 7.

- 5. On the Open File Security warning window, click Run.
- 6. On the Quick Installation window, in the **dedicated ADLDS Directory** section, click **x64** beside **Install a Client**, as shown in the following figure.



- 7. On the User Account Control window, click Yes.
- 8. On the Enterprise Access Management Wizard window, click Next.
- 9. If the Microsoft Visual C++ 2012 Update 4 redistributable is not installed on this machine, you will see the Prerequisites window. Click **Next**. An installation progress window appears and installs the prerequisite software.
- 10.On the What do you want to do window, select including advanced parameters, leave the remaining default selections, and then click Next.
- 11.On the Software Licenses window, click Import.

12.In the Open window, select the license file, and then click Open.

If the file cannot be found, ensure file type is selected as **All Files** *.*

The license stored in the registry is imported.

- 13. On the Enterprise Access Management Wizard screen, click OK.
- 14.On the Storage for Security Objects window, in the **Directory Server** field, type the FQDN and port of the server where the EAM Controller was installed. For example, ev3-uat-srv1.ev3-uat-lab.local:55000.

The following figure provides an example of the window.

Enterpris	ie Access Management Wizard X
	age for Security Objects Belect where Enterprise Access Management security objects are stored.
6	Enterprise Access Management security objects may be stored either in a Dedicated directory, or in the existing Corporate user directory.
	Please indicate where Enterprise Access Management security objects are stored:
	In the Corporate directory
	In a Dedicated directory
	Please indicate the name of the EAM Dedicated directory server. Expected syntax is: server.dns.name.port (default port is 55000)
	Directory server: ev3-uat-srv1.ev3-uat-lab local:55000 v
	< Back Next > Cancel

15.Click Next.

16.On the Detailed Configuration Options window, expand **Authentication**, and then select **Manage access points**, as shown in the following figure.

Ŧ	Tracing		
Ŧ	Directory		
Ξ	Authentication		
	Synchronize keys	Do not synchronize: prompt user for Windows passwo	
	Manage access points	Authenticate computer to the controller	
	New registration	D _{No}	
+ Enterprise SSO			

17.Click Next.

18.On the Enterprise Access Management Client Modules window, perform the following actions:

a) From the Authentication Mode list:

- Select **Authentication Manager** to use the Nymi Band to unlock the desktop and perform SSO authentication tasks on the computer.
- Select **Windows Login** to use the Nymi Band to perform SSO authentication tasks on the computer only.
- b) Optionally, select Administrative Console to install the EAM Console on the enrollment terminal.
- c) Click Next.

The following figure provides an example of the Enterprise Access Management Client Modules window.

Enterpris	se Access Management Wizard		×
9	rprise Access Management Clie Select the Enterprise Access Manager workstation.		9
	Select the Enterprise Access Manag press Next to proceed.	gement Client modules to install on your	workstation and
	Authentication mode:	Authentication Manager	~
	Administrative workstation	SSPR workstation	
	Press Advanced for more installation	options.	Advanced
		< Back Next >	Cancel

- **19.**On the Enterprise Access Management Client installation window, click **Next**. An installation progress window appears and installs the software.
- 20.On the Restart Computer screen, leave the default selection Do not restart the computer, and the click Finish.

Configuring the EAM client to use the Nymi Band Application

Create a registry entry to enable the EAM Client to use the Nymi Band Application to enroll the Nymi Band.

About this task

Perform the following steps in *regedit.exe*.

Procedure

- 1. In the HKLM\Software\Enatel\WiseGuard\AdvancedLogin key, create a new string value
- 2. In the Name field, type WearableEnrollTool.
- **3.** Edit the string and in the value field, type C:\Program Files\Nymi\Nymi Band Application\NEM.exe, as shown in the following figure.

Edit View Favorites Help mputer\HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\A	dvand	edLogin		
HEP_LOCAL_MACHINE HED HED HARDWARE HARDWARE HARDWARE SOFTWARE SOFTTWARE SOFTWARE SOFTTWARE SOFTWARE SOFTWARE	^	Name Action/WhenTokenRemoved Action/WalidationTimer Bit Action/WalidationTimer Bit MiddliometricsTitle MindatIDirectory Bit LockTimer WearableEnrolITool	Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_DWORD REG_SZ	Data (value not set) 6x0000006 (10) 6x00000006 (10) 6x00000000 (1) 6x00000000 (1) 6x0000000 (1) 6x0000012 (200) cl\program files(Mymil/Nymi Band Application\nem.exe

4. Navigate to *HKEY_LOCAL_MACHINE**Software**Nymi**NES*.

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

- 5. In the NES key, create a new string value.
- 6. In the Name field, type URL.
- 7. Edit the string and in the value field, type https://nes server/nes service name

Where:

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

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

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

• Close *regedit.exe*.

Confirming the Runtime dll versions

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

About this task

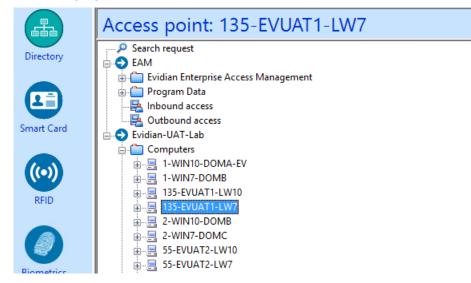
Procedure

- 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. On the EAM Controller, log in to the EAM Console.
- 6.

Select 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.

Overriding the authentication method

When you configure the EAM controller to use the RFID-only *TokenManagerStructure.xml* file, perform the following steps to configure the enrollment terminal to use the wearable authentication method.

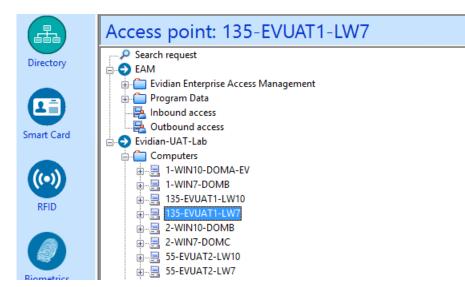
About this task

Procedure

- 1. Obtain the Wearable version of the TokenManagerStructure file, *TokenManagerStructure_WEARABLE.xml* from the software package that you downloaded. The file is located in the *Evidian-Supplementary-Files* subdirectory.
- 2. Rename the *TokenManagerStructure_WEARABLE.xml* to *TokenManagerStructure.xml*.
- **3.** Copy the *TokenManagerStructure.xml* file to the *C:\Program Files\Common Files\Evidian\WGSS* directory.
- 4. On the EAM Controller, log in to the EAM Console.
- 5.

Select 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.

Logging into the terminal

If you installed the EAM Client with the Authentication Manager authentication mode, after you complete the configuration of the EAM Client, when the terminal locks, the Windows login screen appears with new options.

About this task

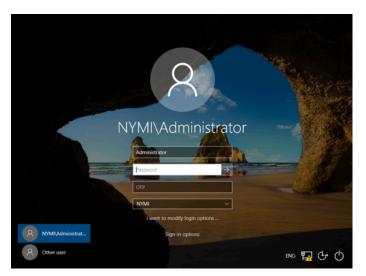
Perform the following steps to log in.

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.
- 3. Restart the terminal.

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.

Adding an SSO definition for a new target application

The SSO definition captures the login screen and credentials for the 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.** Enter the login credentials of an Evidian Administrator.
- 4. In the SSO Config Enterprise SSO Studio, navigate to EAM > Evidian Enterprise Access Management > Application Access > Technical definitions.
- 5. Right-click **Technical Definitions** and select **New Technical Definition**, as shown in the following figure.

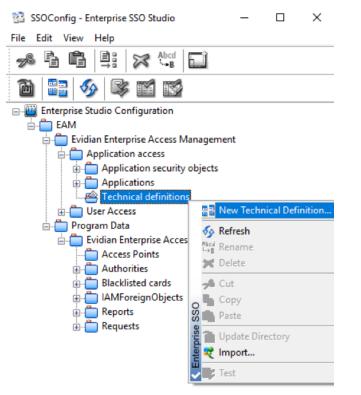


Figure 10: Creating a New Technical Definition

- 6. In the **Properties** tab, provide a name in the **Technical Definition** name field, and then click **OK**.
- 7. Right-click on the new technical definition that you just created and select **New Window**, as shown in the following figure.

🔢 SSOConfig - Enterprise SSO Studio			_		×	
File Edit View Help						
📌 🖥 🛱 📑 🔀 崎	1					
🛍 📰 🍫 🛸 🌃 💕						
Enterprise Studio Configuration						
Evidian Enterprise Access Man	age	eme	ent			
Application access						
Application security objects Applications						
⊕						
Sample Application						
I User Access			New Win	dow		
🖃 🛑 Program Data		Abed	Rename			
Evidian Enterprise Access			Delete			
- Access Points		-				
🖶 🧰 Authorities		1	Cut			
Blacklisted cards		-	Сору			
IAMForeignObjects			Paste			
Reports		7	Update D	irectory		
iaiiii Requests		2	Export			
	0	R	Import			
	SSO		Test			
	ise		Add to Te	et lict		
	ā		Add to h			

Figure 11: 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.

Window p	roperties		×
General	Options	Detection Actions	
Choos	al Window se a name a ndow type	and type for this window. SSO behavior depends on	
Winde	ow name:	Login Window	
Windo	ow type:	🗉 StandardLogin 🗸 🗸	
Stand This is The k	ogon identifi	escription and procedure for SSO Enabling an application. er, password and some additional parameters specific ant to the associated fields.	;

Figure 12: Naming the New Technical Definition Window

9. Open the application that will use Evidian SSO to enter the credentials. Ensure that the SSO builder and application windows are both visible on your desktop.

10.

In the **Detection** tab, click and drag the target icon onto the application window. The following figure provides an example of the Detection window.

Window properties	\times							
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.								
URL file://C:\Users\administrator\Desktop\sampleLogin.html								
Detect browser title Configuration								
Variable URL Sometimes, URLs differ between sessions. Use variable URL detection to handle this. enable variable URL detection Configure								
Parameter of the web page								
Look for text								
🔿 In Field								
If window detection is not sufficient, you can use Advanced detection to add constraints on process.								
OK Cancel Hel	2							

Figure 13: New Technical Definition Detection window

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 Dete	Actions	×
Window fields descrip This window type sen defined below. No field is mandatory.	ds the user authentication data to the fields	
Identifier :	💘 "name"	÷
Password :	🔒 "pass"	
Do not prompt for a	user account	
Additional fields custor Click on the Customize parameters	mization e button to specify additional Customize	
After the SSO has bee	-	
Do nothing	O Press the <enter> key</enter>	
O Press the button :		
	OK Cancel Help	5

Figure 14: 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.

Control Detection X
Please select the desired control or drag and drop the target icon onto it
<pre>editable text: "Enter Username" (0x85601590) white space: "" (0x85601d10) editable text: "Enter Password" (0x85601e5 editable text: "Enter Password" (0x85601e5 white space: "" (0x85601f90) white space: "" (0x85601f90) grouping: "" (0x856002d0) white space: "" (0x856002d0) white space: "" (0x85602d0) white space: "" (0x85602850)</pre>
"Infobar Container" (0x85602c10)
 Display all window details Identify the control by its position in the control hierarchy. Activate Accessibility usage
Use HTML name attribute
Check if the control has the focus
Text conversion:
No modificaton V
OK Clear Cancel

Figure 15: 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 **OK** to save the configuration.
- **14.**Right-click the newly created technical definition and click **Update Directory**, as shown in the following figure.

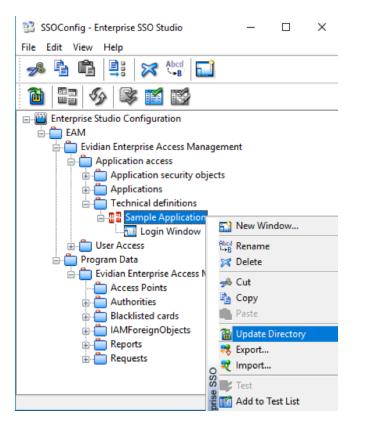


Figure 16: Update Directory with New Technical Definition

Configuring the SSO application in the EAM Console

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

About this task

Procedure

1. Launch the EAM Console, and log in using EAM administrator credentials.

```
2.
```

Click on the Account and Access Rights Management 🔤 icon.

- 3. Navigate to EAM > Evidian Enterprise Access Management > Application Access
- 4. Right-click Technical definitions and then select New > Application.
- 5. Provide an application name, as shown in the following figure, and then click Apply.

Application: New Applicati	on			
P Search request □ • ● EAM	Account Ge	eneration	Accounts	Events
	Application Name: Def Sample	Application		

Figure 17: New Application Name

- 6. In the Configuration tab, select the SSO tab.
- 7. On the **Methods** tab, from the **Default SSO propagation method** list, select **SSO**, as shown in the following figure.

₽.	Account Gene	ration		💅 Accounts		Events
📒 Info	mation	🔊 Conf	iguration	🎉 User /	Access	😤 Administrators
General	Account Base	Account Prop	erties SSO	External Names	Provisioning	connector
Metho SS	Ods Access Str Opropagation Default SSO pro	rategies OLE				
	SSO SSO		~			
	Windows author OLE/Automatic XenApp			Select	Edit	
	VMWare View Vault					

Figure 18: Selecting Default SSO Propagation Method

- 8. Beside the Technical definition field, click 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.

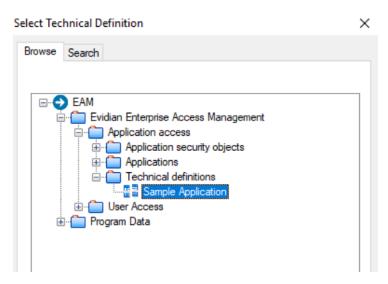


Figure 19: Selecting the Technical Definition

10.Click OK.

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.

13. Select User must re-authenticate to perform SSO, as shown in the following figure.

Application profile: Defau	It application profile
Search request	& Configuration Applies to Events
Comparison of the second	Application Profile Name: Default application profile Configuration
Default Password policy Default application profile Applications Technical definitions User Access User Access Program Data	General Account Authentication method Delegation IP Address Constraints Image: Constraint of the second s
Inbound access Outbound access onymi	Default Password policy → ✓ User must re-authenticate to perform SSO → Launch application at start-up of Enterprise SSO
	Show application on user's Enterprise SSO desktop When application is used, set user's 'unlocking level' to: Allow the user to test the application with Enterprise SSO

Figure 20: User must re-authenticate to perform SSO

14.Click **Apply** to save.

15.Close the EAM Console.

Configuring SSO to use AD Credentials

By default, the configuration for a new technical definition uses separate credentials - not the credentials of the logged in user.

About this task

Perform the following steps to configure SSO to use the logged in AD credentials.

Procedure

- 1. In the EAM Console, navigate to the technical definition and in the **Configuration** Tab, select the **Account Base** tab.
- 2. Select the The application uses the primary account option.
- 3. In the Login format list, select the login format of the AD credentials.

Removing the MES application

After you configure SSO for the MES application on the enrollment terminal, optionally, remove the MES application according to the vendor instructions.

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 API, and the EAM Client software.

The Nymi 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.

Installing the EAM Client

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

Before installing the EAM Client software:

- Complete the steps to configure the EAM Controller.
- Ensure that the machine is on the same domain as the 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 host as a Domain Administrator.
- 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. Copy the license file to the *Downloads* directory on the host.
- **4.** Double-click the *C*:*Downloads**EAM-v10.0xxxxxxx**Start.hta* file.

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 directly from *EAM-v10.01xxxxx/QuickInstall.x64/Client/ESSOClientSetup-Dedicated.exe* Proceed to step 7.

- 5. On the Open File Security warning window, click Run.
- 6. On the Quick Installation window, in the **dedicated ADLDS Directory** section, click **x64** beside **Install a Client**, as shown in the following figure.



- 7. On the User Account Control window, click Yes.
- 8. On the Enterprise Access Management Wizard window, click Next.
- 9. If the Microsoft Visual C++ 2012 Update 4 redistributable is not installed on this machine, you will see the Prerequisites window. Click **Next**. An installation progress window appears and installs the prerequisite software.
- **10.**On the What do you want to do window, select **including advanced parameters**, leave the remaining default selections, and then click **Next**.
- 11.On the Software Licenses window, click Import.

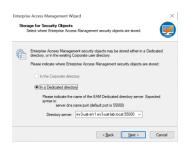
12.In the Open window, select the license file, and then click Open.

If the file cannot be found, ensure file type is selected as **All Files** *.*

The license stored in the registry is imported.

- 13.On the Enterprise Access Management Wizard screen, click OK.
- 14.On the Storage for Security Objects window, in the **Directory Server** field, type the FQDN and port of the server where the EAM Controller was installed. For example, ev3-uat-srv1.ev3-uat-lab.local:55000.

The following figure provides an example of the window.



15.Click Next.

16.On the Detailed Configuration Options window, expand **Authentication**, and then select **Manage access points**, as shown in the following figure.

+	Tracing				
+	Directory				
=	Authentication				
	Synchronize keys	Do not sync	hronize: promp	t user for Wind	ows passwo
	Manage access points	Authenticat	e computer to	the controller	
	New registration	No			
+	Enterprise SSO				
a.	Cache Management				

17.Click Next.

18.On the Enterprise Access Management Client Modules window, perform the following actions:

- a) From the Authentication Mode list:
 - Select **Authentication Manager** to use the Nymi Band to unlock the desktop and perform SSO authentication tasks on the computer.
 - Select **Windows Login** to use the Nymi Band to perform SSO authentication tasks on the computer only.
- b) Optionally, select Administrative Console to install the EAM Console on the enrollment terminal.
- c) Click Next.

The following figure provides an example of the Enterprise Access Management Client Modules window.

Enterpris	se Access Management Wizard		×
9	erprise Access Management Clie Select the Enterprise Access Manager workstation.		Ø
1	Select the Enterprise Access Manag press Next to proceed.	gement Client modules to install on your	workstation and
	Authentication mode:	Authentication Manager	~
	Administrative workstation	SSPR workstation	
	Press Advanced for more installation	options.	Advanced
		< Back Next >	Cancel

- **19.**On the Enterprise Access Management Client installation window, click **Next**. An installation progress window appears and installs the software.
- 20.On the Restart Computer screen, leave the default selection Do not restart the computer, and the click Finish.

Setting the NES URL

Create a registry entry to enable the EAM Client to connect to NES.

About this task

Perform the following steps to define the NES URL.

Procedure

- 1. Open regedit.exe
- 2. Navigate to *HKEY_LOCAL_MACHINE*\Software\Nymi\NES.

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

- 3. In the *NES* key, create a new string value.
- 4. In the Name field, type URL.
- 5. Edit the string and in the value field, type https://nes_server/nes_service_name Where:

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

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

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

• Close regedit.exe.

Enabling Roaming Sessions for SSO

RFID-only terminals use roaming sessions to perform MES authentication tasks with SSO.

About this task

Procedure

- **1.** Open *regedit.exe*
- 2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication*.
- 3. Create a new **REG_DWORD** value named RoamingSessionAllowedForSSO with a value of 1.
- 4. Close regedit.

Logging into the terminal

If you installed the EAM Client with the Authentication Manager authentication mode, after you complete the configuration of the EAM Client, when the terminal locks, the Windows login screen appears with new options.

About this task

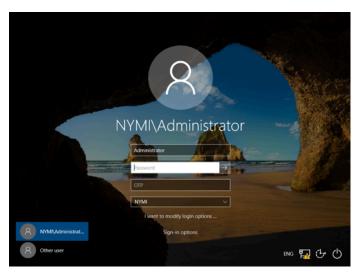
Perform the following steps to log in.

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.
- 3. Restart the terminal.

Installing the MES Application

Install and configure the MES application according to the MES documentation.

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.

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 eSSO application.

About this task

Perform the following steps on the machine on which you installed the MES application and the EAM Client software.

Procedure

- 1. On a User Terminal, open the Enterprise SSO (eSSO) by clicking on the staskbar icon
- 2. Click the **Home** oicon, and then click **Refresh**.

This enables the EAM Client to communicate to the EAM Controller to retrieve new technical definitions.

The following figure shows the eSSO Home window.

🏹 E	interprise SSO : Single Sign-On Engine		-		×	
0	Activate Suspend	C) Refresh	(I)	Stop		^
⊕	Connected User : Administrator	4	U			
	Current role : No selected role	Reload the techni	cal refere	ences		
						~
	<				>	
Ready						.:

Figure 21: 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.

		9	Show password	
7	Enterprise SSO : Single Sig		Delegate	×
			Add to favorites Remove from favorites	
•	B Def Sample Application	~	Hide applications without credential	A
			Open SSOStudio	
			Start application Create shortcut	
			Disable the application Enable the application Enable all applications	

Figure 22: eSSO 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 Enterpri	se 550 Session - Re-aumentication
(Enterprise Single Sign-On
Login:	••• Administrator 🗸
Password:	
Log on to:	NYMI
	OK Cancel

Figure 23: SSO Login screen

6. Close the SSO application.

Existing Enternaine CCO Consistent De author

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.

Configuring Support for Users in Multi Domain Environments

About this task

Perform the following steps when a user has enrolled their Nymi Band in a domain that is different from the domain where the user terminal is run.

Procedure

- 1. Run regedit.
- 2. In the *HKLM**Software**Enatel**WiseGuard**FrameWork**Directory*, right-click **PossibleDomainsList**, and then select **Modify..**
- 3. In the Value Data field, type the NETBIOS name for each domain that contains users, comma separated, that will log in to the user terminal.
- 4. Click OK.

Example

This example shows a user terminal that supports authentication tasks from Nymi Band users that are a member of domains UAT1B-Lab and UAT1A-Lab.

File Edit View Favorites Help Computer\HKEY_LOCAL_MACHINE SOFTWARE Caphyon Classes Clients Clients Dolby Enatel SSOWatch WiseGuard	SOFTWARE\Enatel\WiseGuard\FrameWork\Direct Name BlobCompression DirectoryType EnterpriseUserAuthentication CSSEncryption CSSSignature	Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data (value not set) 0x00000001 (1) 0x00000001 (1) 0x00000001 (1) 0x000000001 (1) 0x00000000 (0) 0x00000000 (0)
Jobug AdvancedLog BioEnroll Debug ExtendedMan FrameWork AccessPoir Audit		REG_SZ REG_SZ	UAT1B-LAB, UAT1A-Lab DC=B,DC=UAT-1,DC=local

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.

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 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.

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.

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 EAM 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.

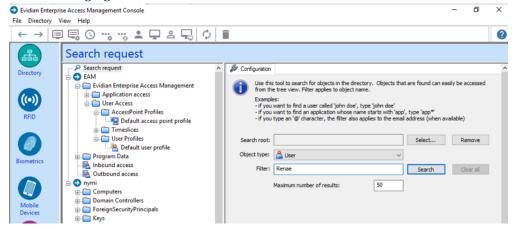


Figure 25: Search request window

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

Figure 26: RFID tab for a user

User: UATAdmin			
Br-Au UATAdmin Brown Construction Construc	Information Active Session Delegation Mobile De PPD Identifie State SF02203396F49 Active F0273771:60:CC:E2	Battery status e Not available	Accounts Events

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

Returning a Nymi Band

When a user no longer requires their Nymi Band, perform the following steps, which allows you to assign another user to the Nymi Band.

About this task

This procedure removes the association between the user and the Nymi Band in EAM and deletes the biometric data from 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 EAM 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.

😔 Evidian Enterpri	se Access Management Console						-	٥	×
File Directory \	/iew Help								
$\leftarrow \rightarrow \equiv$; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;	ĺ	Î.						?
æ	Search request		R						
Directory	Search request EAM EAM Evidian Enterprise Access Management Application access	Â		tool to search for objects in the dire tree view. Filter applies to object n		t are found can ea	sily be ac	cessed	Î
RFID	User Access Care AccessPoint Profiles Default access point profile Default access point profile Default access point profile		- if you v - if you v	want to find a user called 'john doe', want to find an application whose na ype an '@' character, the filter also	me starts with 'app'	, type 'app*' address (when av	ailable)		
	User Profiles		Search root:	0		Select	Rer	nove	
Biometrics	Program Data Dound access Outbound access		Object type: Filter:	🖾 User Renae	~	Search	Cle	ar all	
Mobile Devices	Onymi Omputers Omputers Ononic Controllers OreignSecurityPrincipals Keys		,	Maximum number of results:	50				

Figure 27: Search request window

4. Click Search.

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

Figure 28: RFID tab for a user

Search request ⊨ - P ev3-uatadmin ⊕ - ▲ UATAdmin	Information 🤽 Conne Session Delegation	ction La Security	Profiles 😤 Administ	ration 😹 Application Access 🛷 Accounts RFID O Biometrics O Events
C EAM	RFID Identifier	State	Battery status	Refresh
Evidian Enterprise Access Management	5F022D3398F489	Active	Not available	
- Carl Application access	↓↓ 79:73:71:6D:CC:E2	Active	Not available	Assign
Application security objects				Lock
- 🔗 Default Pfcp				
- 🎒 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 kens expiring with		÷ days.		Apply
Owner All Ev2-Uat1		RFID Identifier 2F:2D:8D:0B:7 5FDB2C433FBD6E	State Blacklisted Blacklisted	Battery status Unkown Unkown	Expiration Date

Figure 29: Blacklisted Nymi Band

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

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

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

- 5. Select the Domain\username link of the user. to open the User Details page.
- 6. 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**.
- 7. On the Disconnect screen, scroll to the bottom and select **Disconnect**.

Handling a lost Nymi Band

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 EAM 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 Enterpris	se Access Management Console			-	٥	\times
File Directory V	fiew Help					
$\leftarrow \rightarrow \equiv$] ⊑ () …, …, ≗ ⊑ ≗ ⊑ ¢	Î				?
æ	Search request					
Directory	- P Search request ^	🖉 Configuration				^
Directory	EAM					
	Evidian Enterprise Access Management		tool to search for objects in the directory. Objects that are four e tree view. Filter applies to object name.	id can easily be ac	cessed	
ത്ര	Application access	Example				
	User Access	- if you	want to find a user called 'john doe', type 'john doe'			
RFID	AccessPoint Profiles		want to find an application whose name starts with 'app', type 'ap type an '@' character, the filter also applies to the email address			
	Ser Profiles	Search root:	Sele	ct Doe	nove	
	Default user profile	Searchroot	300	Ken	iove	
	🕀 🦳 Program Data	Object type:	🚨 User 🗸 🗸			
Biometrics	- 🖶 Inbound access	Filter	Renae	cia.	ar a l	
	- 📑 Outbound access	i nuci .	Sed	ren cies	af all	
	ia-⊙ nymi		Maximum number of results: 50			
	Computers					
Mobile	Domain Controllers					
Devices	ForeignSecurityPrincipals					
	🕀 🛅 Keys					

Figure 30: Search request window

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

Figure 31: RFID tab for a user

Search request		nnection 🛛 👗 Securit		
□-, P ev3-uatadmin	Session Delegation	Mobile Devices	Smart Card	RFID OBiometrics OEver
uATAdmin	[ann the st			
EAM	RFID Identifier	State	Battery status	Refresh
😑 🧰 Evidian Enterprise Access Management	5F022D3398F489	Active	Not available	
Application access	₩79:73:71:6D:CC:E2	Active	Not available	Assign
Application security objects				Lock
- R Default Pfcp				
- 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.

- 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.

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 NES Administrator Console, select Search.
- 2. In the **Search** page, select the **Users** Option.
- 3. In the **Search** field, type the full or partial username, first name, or last name of the user.
- 4. Click **Search**. The Search page displays the user, or a list of users that match the search criteria.
- 5. Select the Domain\username link of the user. to open the User Details page.
- 6. 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**.
- 7. On the Disconnect screen, scroll to the bottom and select **Disconnect**.

Handling a found Nymi Band

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

About this task

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 EAM 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.

Evidian Enterp	rise Access Management Console	- 0	×
File Directory			?
A	Search request		
Directory	Search request EAM Evidian Enterprise Access Management Diano Access Diser Access Diser Access Point Profiles Diser Access Point Profile Diser Access Point Profile Diser Access Point Profile	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 want to find an application whose name starts with 'app', type 'app'' if you want to find an application whose name starts with 'app', type 'app'' if you want to find an application whose name starts with 'app', type 'app'' if you want to find an application whose name starts with 'app', type 'app'' if you want to find an application whose name starts with 'app', type 'app'' if you want to find an application whose name starts with 'app', type 'app'' if you want to find an application whose name starts with 'app', type 'app'' if you want to find an application whose name starts with 'app', type 'app'' if you want to find an application whose name starts with 'app', type 'app'' if you type an '@r' character, the filter also applies to the email address (when available)	^
Biometrics	C User Profiles Default user profile Program Data Inbound access Outbound access	Search root: Select Remove Object type: Liser Filter: Remoe Search Clear al	
Mobile Devices	Prymi Primi Primi Primin Controllers Primin Controlers Primin Controlers Primin Controllers Primin Contr	Maximum number of results: 50	

Figure 32: Search request window

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

Results

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

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 NES Administrator Console, select Search.
- 2. In the **Search** page, select the **Users** Option.
- 3. In the **Search** field, type the full or partial username, first name, or last name of the user.
- 4. Click Search. The Search page displays the user, or a list of users that match the search criteria.
- 5. Select the Domain\username link of the user. to open the User Details page.
- 6. 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**.
- 7. On the Disconnect screen, scroll to the bottom and select **Disconnect**.

Upgrading Nymi and Evidian Components

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

The section describes how to update the components in a Connected Worker Platform with Evidian solution and post update configuration changes that are required to allow existing users to use the Nymi Band to perform authentication events.

Upgrading the NES software

Upgrade the NES according to the instructions in the Nymi Connected Worker Platform Administration Guide.

If you upgrade from an NES 3.2.x or earlier version, 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 Destination list, select the option NES and Evidian, as shown in the following figure, and then click Save.

Enrollment Destination	NES and Evidian	
Fingerprint Required		
Corporate Credentials Authentication		
NFC UID Capture	Mandatory	
Display Band Label on Nymi Bands		

Figure 33: NES and Evidian enrollment option

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 an NFC tap, the desktop locks.

About this task

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

Perform the following steps in the EAM Console

Procedure

- 1. In the Directory view, expand EAM > Evidian Enterprise Access Management > User Access > AccessPoint Profiles > Default Access Point Profile.
- 2. On the Authentication 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 NFC 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.

Updating the TokenManagerStructure

The Connected Worker Platformsoftware package includes new TokenManagerStructure(TMS) files that support wearable and RFID authentication methods. When you upgrade Connected Worker Platform components, it is recommended that you replace any TokenManagerStructure file that you placed on a terminal to override the EAM Controller configuration, and the configuration on the 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 EAM Console as an EAM Administrator.
- 2. From the File menu, select Configuration.
- **3.** On the **Authentication** tab, click **Select**, and then select the appropriate TMS file for your configuration.
- 4. Click Apply.
- 5. Click OK.
- 6. Launch Services.
- 7. Stop the Enterprise Access Management Security Services service.
- **8.** Delete all files under *C*:*Program Files**Common Files**Evidian**WGSS**CacheDir*.

Note: If you get a message that you cannot delete the files, hold the **Shift** key down when you press **Delete**.

9. Start Enterprise Access Management Security Services service.

10.For each terminal in the environment that overrides the 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*.

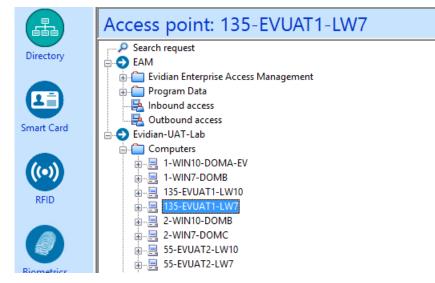
11.On the EAM Controller, log in to the EAM Console.

12.

Select 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.

Upgrading the Nymi Band Application on the Enrollment Terminal

An upgrade 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.

Confirming the Runtime dll versions

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

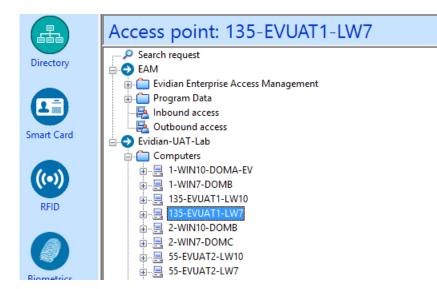
About this task

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. On the EAM Controller, log in to the EAM Console.
- 6.

Select 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.

Upgrading Nymi Components on the User Terminals and Remote NEA hosts

Upgrade the Nymi Runtime. For user terminal that use a wearable configuration.

About this task

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

Procedure

- 1. Log in to the terminal, with an account that has administrator privileges.
- 2. Extract the Nymi SDK distribution package.
- **3.** From the ...*nymi-sdk**windows**setup* folder, run the *Nymi Runtime Installer version.exe* file.
- 4. On the Welcome page, click Install.
- **5.** On the User Account Control page, click **Yes**. The installation wizard appears. If the installation detects missing prerequisites, perform the steps that appear in the prerequisite wizards.
- 6. On the Welcome to the Nymi Runtime Setup Wizard page, click Next.
- 7. On the Nymi Runtime Setup window, click Next.
- 8. On the Service Account window, click Next.
- 9. On the Ready to install page, click Install.

10.Click Finish.

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

12.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.

Post Upgrade Tasks for Existing Users

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

After you upgrade all the components in the Connected Worker Platform with Evidian solution, additional steps are required to allow existing Nymi Band users to use the Nymi Band with Evidian. The procedure differs depending on where the Nymi Band was enrolled prior to upgrade.

Enrolling Existing Nymi Bands in Evidian

After you upgrade all the components in the Connected Worker Platform with Evidian solution, a user with a Nymi Band that was enrolled in NES prior to the upgrade, must log in to the Nymi Band Application on the enrollment terminal.

Before you begin

Ensure that the user is wearing their authenticated Nymi Band.

About this task

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

Procedure

- 1. On the Windows Login screen, log in to the computer.
- 2. In the system tray, right-click the ESSO Credential Manager. The icon may be hidden behind the ^ (caret).

If you do not see the icon, perform the following steps:

- a) Start the **ESSO Credential Manager** by double-clicking *C:\Program Files\Evidian* *Enterprise Access Management\ESSOCredentialManager.exe*
- b) On the Evidian Enterprise SSO Open Session window, log in with credentials of the user.
- c) Check the system tray for the icon.
- 3. Select Manage Wearable Devices..., as shown in the following figure.



Figure 34: Manage Wearable Devices menu option

4. On the Manage wearable devices window, click Add

- 5. On the login window, type the username and password of the user that will enroll the Nymi Band, and then click **OK**.
- 6. On the Authentication Manager window, click **Yes**, and then wait until the Nymi Band Application starts.
- 7. Log into the Nymi Band Application with the username and password of the user that will enroll the Nymi Band.

Results

The Nymi Band Application displays Saving user settings while their enrollment completes in the Evidian database. Close the Nymi Band Application when the enrollment completes.

Re-enrolling existing Nymi Band Users in Evidian

After you upgrade all the components in the Connected Worker Platform with Evidian solution, perform the following steps for all users that have a Nymi Band that was enrolled in Evidian prior to the upgrade.

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

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 EAM 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.

Evidian Enterpri	se Access Management Console	- 0	×
File Directory V		Î	0
æ	Search request		
Directory	Search request Search request Search request EAM Evidian Enterprise Access Management	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.	^
(interview) RFID	Application access Juser Access AccessPoint Profiles Default access point profile	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)	
Biometrics	Timeslices Der Profiles Default user profile Program Data Program Data	Search root: Select Remove	
Mobile Devices	Computers Computers Computers Computers Computers Computers Comparison Controllers Composed Controllers Controllers Composed Controllers Con	Filter: Renae Search Clear all	

Figure 35: Search request window

4. Click Search.

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

Figure 36: RFID tab for a user

- ₽ Search request - ₽ ev3-uatadmin ▲ UATAdmin	Information 🤽 Conn La Session Delegation	ection La Securit	ty Profiles 🛛 😤 Administ	ration 🚂 Application Access 🧭 Account
CALADMIN CALADMIN	RFID Identifier	State	Battery status Not available	Refresh
Chain Chain acces Application acces Application security objects Application security objects Application profile Default Psychol policy Default Psychol policy Default Application profile Default application Technical definitions Default applications Default application	+ - -79:73:71:60:CC:E2	Active	Not available	Assign Lock Bladdist

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 sea RFID state			~		
Battery status	tus		~		
Show RFID tokens expiring within 10 🌲 days.					
Owner 🔶		RFID Identifier	State	Battery status	Expiration Date
WEv2-Uat1		2F:2D:8D:0B:7 5FDB2C433FBD6E	Blacklisted Blacklisted	Unkown Unkown	

Figure 37: Blacklisted Nymi Band

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

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

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.

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 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.

Troubleshooting

This section provides information about how to enable logging and how to troubleshoot common issues.

Enabling Evidian Logging

Perform the following steps to enable logging in Evidian.

About this task

Leaving on the Debug On option is not recommended as it can generate a lot of log entries.

Procedure

- 1. Launch regedit.exe.
- 2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard*.
- **3.** Rename *Debug* to *Debug_*.
- **4.** Rename _*Debug* to >*Debug*.
- 5. Close regedit.exe.

Results

Logs files are generated in C:\Program Files\Common Files\Evidian\WSGG\Logs.

Troubleshooting Evidian Error Messages

Evidian Security Services seems to not be running

This error message appears when you start Manage Wearable Devices.

Cause

This error is a typical error when the EAM Client cannot communicate with the EAM Controller, for one of the following reasons:

- Poor network connection between the EAM Client and EAM Controller
- Technical Admin account has expired.

However, occasionally this can be caused when the password of the technical admin account has expired.

Resolution

To resolve the issue where the password of the technical admin account has expired, perform the following steps to reset the password for the security settings account.

- **1.** Launch *WGSRVConfig.exe*, which is in the EAM Install package in the ...*EAM-v10.X EAM.x64*/*TOOLS* directory.
- 2. On the Administration Tools, select Configure security settings
- 3. Change the Directory and Access point account to the new login and password.

Evidian License has Expired

This message appears when you use EAM.

Cause

The license on the EAM Client and the EAM Controller has expired.

Resolution

Obtain a new license file and perform the following actions:

- 1. Log in to the server with domain admin credentials (example: server = Ev-UAT-Srv1).
- 2. Launch C:Program Files\Common Files\Evidian\WGSS\WGConfig.exe..
- 3. On the Account Control window, click Yes.
- 4. On the Configuration Assistant, select Enterprise Access Management, and then click Next.
- 5. On the Software Licenses window, click Import.
- 6. Navigate to the license file and then click OK.

Note: If you prompt to replace the license keys, click Yes.

- 7. On the confirmation window, click OK.
- 8. Click **Cancel** to close the window.

EAM Security Services are not available

This error message appears on the Window Login screen.

Cause

The EAM Security Services service is not running.

Resolution

Start the service by performing the following actions:

- 1. Log into the machine with your username and password.
- 2. Open the Services applet, double-click Enterprise Access Management Security Services.
- 3. Ensure that the Startup Type is set to Automatic, and then click OK.

4. Start the Enterprise Access Management Security Services service. Ensure that the status of the service displays Running.

Nymi Band Enrollment Fails: Failed to Create Security Settings

Enrollment of the Nymi Band using the Nymi Band Application fails as security settings could not be created.

Cause

Network issues

The Nymi Band is already associated with another user in the EAM Controller.

Resolution

To resolve the issue when the Nymi Band is already associated with anotherr user, follow the instructions in the *Returning a Nymi Band* section to remove the Nymi Band association in the EAM Controller. Retry the enrollment using the Nymi Band Application.

•

User has two Active Bands after Enrollment

After completing enrollment of the Nymi Band using the Nymi Band Application, there are two Active Bands associated to the user in the EAM Console.

Cause

The association between the user and the previously issued Nymi Band was not removed in the EAM Controller.

Resolution

Follow Returning a Nymi Band to remove the outdated Nymi Band association in the EAM Controller.

Cannot Unlock the Enrollment Terminal

An enrolled Nymi Band can lock a user terminal but cannot unlock the terminal.

Cause

The unlock function relies on the Nymi Band Application and the Nymi Band Application version of the *nymi_api.dll* file that is used by Evidian. The DLL used by Evidian must match the Nymi Band Application version.

Resolution

- **1.** Ensure that the *nymi_api.dll* file has been copied from the *C:\Program Files\Nymi\Nymi Band Application* to *C:\Program Files\Common\Evidian\WGSS.*
- 2. Delete the Nymi certificate files by performing the following steps:

- **a.** Navigate to C:\Windows\system32\config\systemprofile\appdata\roaming\Nymi\NSL\hVoGqxl8\.
- **b.** Delete the *ksp* directory.
- c. Change the startup type of the Enterprise Access Management Security Services service to Disabled.
- d. Stop the Enterprise Access Management Security Services service.
- e. Log back into the computer.
- f. Change the startup type of the Enterprise Access Management Security Services service to Enabled.
- g. Start the Enterprise Access Management Security Services service.

Cannot Perform Authentication events With the Nymi Band After Closing SSO Authentication Window

In an Citrix/RDP session, if a user closes the SSO authentication window that appears when the they tap their Nymi Band against the NFC reader while in the MES application, the SSO authentication window does not appear on a subsequent Nymi Band tap.

Cause

The SSO process closes.

Resolution

Restart the Enterprise SSO application. For example:

- From the Windows search field, type Enterprise SSO, and then open the application. On the Evidian Enterprise SSO Open Session window, type your username and password and then click **OK**.
- Log out of the remote session and then log back in. When the Evidian Enterprise SSO Open Session window appears, tap the authenticated Nymi Band against the NFC reader.

ESSO Credential Manager icon does not appear in the system tray

ESSO Credential Manager icon does not appear in the system tray.

Cause

The ESSO Credential Manager application is not running. This can occur after you disable the **Enterprise Access Manager Security Services** service and then stop the service.

Resolution

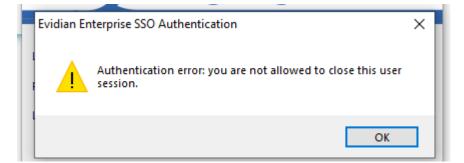
To resolve this issue, perform the following actions:

- **1.** Navigate to C:\Program Files\Evidian\Enterprise Access Management.
- 2. Double-click ESSOCredentialManager.exe.
- 3. When prompted, log in with your username and password.

Authentication error: you are not allowed to close this user session

This error message appears when you tap your Nymi Band against the NFC reader to re-authenticate the SSO session.

The following figure provides an example of the error message.



Cause

The Nymi Band user is logged into the terminal but SSO was started with the EAM administrator username and password, and not the user account that is associated with the Nymi Band that is performing the MES authentication operation.

Resolution

- 1. Right-click SSO on the System Tray and then select Stop.
- 2. Right-click **SSO** on the **System Tray** and then select **Start**. When prompted, type the username and password of the user account that is associated with the Nymi Band that is performing the MES authentication operation.

Copyright ©2022 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