

# Wearable and RFID Installation and Configuration Guide

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

# Contents

Preface	5
Nymi Connected Worker Platform with Evidian Access Management	
Solution	7
Coexistence of Nymi-direct integrations and Evidian integrations	7
Environment Configuration	9
Liser Terminal Requirements	ر و
Enrollment Terminal Requirements	10
Using the Nymi Band in a Mixed Mode Authentication Configuration	11
Obtain the Required Software	11
Install Server Software	11
Installing and Configuring NES	11
Installing the EAM Controller software	12
Installing and Configuring Software on the Enrollment Terminal	26
Importing the Root CA certificate	26
Installing the Nymi Band Application	28
Installing the EAM Client	28
Configuring the EAM client to use the Nymi Band Application	31
Confirming the Runtime dll versions	32
Logging into the terminal	33
Configure the Evidian SSO for an MES Application	34
Adding an SSO definition for a new target application	34
Configuring the SSO application in the EAM Console	40
Configuring SSO to use AD Credentials	42
Removing the MES application	43
(Wearable only) Installing and Configuring Software on User Terminals and for Remote	
MES Applications	43
(Citrix/RDP environments only) Deploy a centralized Nymi Agent	43
Importing the Root CA certificate	45
Installing the Nymi Runtime software	47
Installing the EAM Client	49
Disabling Drive By Authentication	52
Setting the NES URL	53
(Citrix server/RDP session host only) Configuring the EAM client to Communicate	
with the Centralized Nymi Agent	53

(Citrix/RDP environments only) Configuring the User Terminals to Access	
Centralized Nymi Agent	
Confirming the Runtime dll versions	
Logging into the terminal	
Installing the MES Application	
Updating User Terminal with new SSO Configuration	56
Configuring Support for Users in Multi Domain Environments	
(RFID-only) Installing and Configuring Software on RFID-only User Terminal and for	
Remote MES Applications	59
Installing the EAM Client	59
Setting the NES URL	
Overriding the authentication method	63
Enabling Roaming Sessions for SSO	64
Logging into the terminal	64
Installing the MES Application	
Updating User Terminal with new SSO Configuration	65
Configuring Support for Users in Multi Domain Environments	
Enrolling a Nymi Band	67
Manage the Nymi Band	68
Viewing the Nymi Band Associated with a User	68
Returning a Nymi Band	69
Handling a lost Nymi Band	71
Handling a found Nymi Band	
Upgrading Nymi and Evidian Components	74
Upgrading the NES software	74
Modifying EAM Settings to Support Coexistence with other Solutions	75
Updating the TokenManagerStructure	75
Upgrading the Nymi Band Application on the Enrollment Terminal	77
Confirming the Runtime dll versions	77
Upgrading Nymi Components on the User Terminals and Remote NEA hosts	78
Post Upgrade Tasks for Existing Users	79
Enrolling Existing Nymi Bands in Evidian	79
Re-enrolling existing Nymi Band Users in Evidian	80
Troubleshooting	83
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	

Cannot Perform Authentication events With the Nymi Band After Closing SSO	
Authentication Window	86
ESSO Credential Manager icon does not appear in the system tray	86
Authentication error: you are not allowed to close this user session	87

Nymi<sup>TM</sup> 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	May 16, 2022	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

This document provides information about how to use the NES Administrator Console to manage the Connected Worker Platform (CWP) system. This document describes how to set up, use and manage the Nymi Band<sup>TM</sup>, 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.

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.

# **Environment Configuration**

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

# **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.

• 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 in a Mixed Mode Authentication Configuration

Some environments require the Nymi Band to provide authentication as an RFID-only device, and as a Wearable device.

Note: Smart Card functionality is no longer supported for Connected Worker Platform.

This chapter assumes the default deployment of the Nymi Band as a wearable device, with some user terminals requiring wearable or RFID-only authentication.

# **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.

Flovide EAM license keys	to enable software features.
This software is subject to software. You must agree proceed. You may enter each licen	o license. You may not use it if you do not have a license for a with the terms and conditions of the license agreement to use key manually or Import them from a file.
Customer ID:	Impo
Feature /	License key
Select license:	Enter your license key and press 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.

Z	The EAM Controller includes its own users accounts. The Controller requir management operations.	directory dedicated to the s res a Windows domain acc	storage of SSO data and ount to perform password
R	You must select the Windows domain domain account must have the right this account must never expire.	n account used by the EAM to Self Service Password P	A Controller. This Windows Requests. The password of
	Controller Windows account:	NYMI\administrat/	or Select
	The selected account must be locate	ed in the domain of this con	nputer.

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.

Set up a database server for EAM as	udit events.
This wizard creates EAM audit data computer.	abase tables in a database server installed on this
It provides automated installation fo to documentation when using anot	or MySQL, PostgreSQL and Microsoft SQL Server. Refe her type of RDBMS.
O Install a MySQL database s	erver dedicated to EAM audit
<ul> <li>Install a MySQL database a</li> <li>Create audit database table</li> </ul>	erverdedicated to EAM audit. Is in an existing database server
<ul> <li>Install a MySQL database s</li> <li>Create audit database table Select database server:</li> </ul>	erver dedicated to EAM audit as in an existing database server Microsoft SQL Server SQLEXPRESS
<ul> <li>Install a MySQL database a</li> <li>Create audit database table Select database server.</li> <li>Do not install the EAM data</li> </ul>	erver dedicated to EAM audit as in an existing database server Microsoft SQL Server SQLEXPRESS base server on this controller
<ul> <li>Install a MySQL database a</li> <li>Create audit database table Select database server:</li> <li>Do not install the EAM data</li> <li>Press Next to proceed.</li> </ul>	erver dedicated to EAM audit as in an existing database server Microsoft SQL Server SQLEXPRESS base server on this controller

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

Security administrator's account: NYMI\administrator Selecurity administrator's account: NYMI\administrator Selecurity passphrase is the foundation of EAM security. The security administrator asked to enter it the first time he launches EAM Console. The passphrase must be at 16 characters long. Security passphrase:	6	The security administrator is the f administration rights to other user him. They should be performed b	inst user able to run the EAM Console s. Daily administration tasks should n y delegated administrators.	e. He will delegate tot be performed by
The security passphrase is the foundation of EAM security. The security administrator acked to enter it the first time he launches EAM Console. The passphrase must be at 16 characters long. Security passphrase:		Security administrator's account:	NYMI\administrator	Select.
Security passphrase:	2	The security passphrase is the for asked to enter it the first time he 16 characters long.	undation of EAM security. The secur aunches EAM Console. The passph	rity administrator will rase must be at lea
		Security passphrase:	I	
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**.

Auth	nentication 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 configurat	ion of device in
	Biometrics authentication	Store-On-Server	
	Biometrica provider	Upek	

**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**.

Evidian Enterp	rise Access Management - Open Session Enterprise Access Manage	ment
Login: Password:	••• administrator	~
Log on to:	NYME	~
		Cancel

**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

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

#### **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.

Ontions	Primary Ar	iministrators	SA Server Hosts	SA Server Configuration
Ren	orting	SSPR by Confin	mation Code	User Self Econolment
User	Notifications	Audit Clea	n-Up Secur	ity Code Authentication
General	Default Values	Authentication	Other User Attributes	Public Key Authentication
	doken_manag doke	erid="SOFTWAF an_classid="MOI doken_con <th>RE"&gt; BILE" display_name="M fig&gt; htma&gt; module id="0x0100"&gt; module id="0x0200"&gt; module id="0x0200"&gt; module id="0x0200"&gt; ture&gt;</th> <th>oble Authentication</th>	RE"> BILE" display_name="M fig> htma> module id="0x0100"> module id="0x0200"> module id="0x0200"> module id="0x0200"> ture>	oble Authentication
	Citol	en_class> an_class.id=''WE	APARI E' dealar anno	-'Manaphie deuters'
< Auther	ntication token de	scription file:		>
Auther	tication token de	scription file:	novoce doplay_lane	Select
Auther	tication token de	scription file:		Select
Auther	ritation token de	corption file:		Select
Auther	tication token de	scription file:		Select

- **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.

#### (RFID-only) Configuring the EAM Controller Changes for RFID-only

If the configuration includes user terminals that use the Nymi Band as an RFID-only device, perform the following actions.

#### **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.

EAM	Configuration Applies to O Events
Evidian Enterprise Access N     Application access	Name: Default access point profile
Construction     Construction     Construction     Construction	Schedule: Default time-slice
Default access p     Default access p     Default access p     Default access p	Self Service Password Request Biometrics Active RFID Aude Local Administration Security Services Authentication Manager Enterprise SSO Multi User Desktop
- A Inbound access	Lock behaviour: Windows lock 🗸
Outbound access	Default action when token removed: Lock the session
	Delay before action: 0 seconds
	Inactivity: automatically lock session after: 0 seconds conditional setting
	Automatically close locked session after: 0 seconds
	Allow local connection
	Remember authentication role
	Allow password change
	Enable smart card detection on Ctrl-Alt-Del     Grace period for administrator     admentication     seconds
	Allow unlock if allowed by user security profile.
	Allow unlock if the same Windows credential is used.
	Max. number or concurrent vindows sessions: U (rom vindows /) 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.

#### 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 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.

Rep	onting	SSPR by Confin	mation Code		User Self Enrolment		
User	Notifications	Audit Clea	an-Up	Secur	nty Code Authentication		
ieneral	Default Values	Authentication	Other User /	Attributes	Public Key Authentication		
Options	Primary Ad	ministrators	SA Server H	osts	SA Server Configuration		
Drimon							
( Adapted	v doministrator	Children Children		C. In col			
Admir	natrator - CIV=Adm	inistrator, CN+Use	sra.UC=nymi.U	CHOCAL			
				Add	Remove		
				Add	Renove		
				Add	Benove		
				Add	Bendoe		
				Add	Benove		
				Add	Benove		

- 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*\*TOOLS*\*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	v <u>2</u>
Import/Export contro	Data Link Properties Provider Connection Advanced All
-	1 Salact or enter a server name
oller configuration	ev3-uat-srv2 V Refresh
Install an Audit V2 D	2. Enter information to log on to the server:
	Windows Authentication V
Configure local audi	Server SPN:
Update Audit transla	User name
Configure security s	Password
Define a master Auc	Blank password Allow saving password
	Use strong encryption for data Trust server certificate
are Installation	3.  Select the database:
	O Attach a database file as a database name:
Configure workstatic	
Configure authentica	Using the filename
Install EAM Client	Onange Password Test Connection
Install finger vein bio	
	OK Cancel Help

Figure 5: Select the database window

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

1	🖥 certlm - [Certificates - Local Compute	er\Trusted	Root Certificatio	n Aut	thorities] — L		
F	ile Action View Help						
4	• 🔿 🙍 🗊 📋 🧟 🗟						
<b>,</b>	Certificates - Local Computer	^	Object Type				
~	Trusted Root Certification Authority	ties					
	Certificates	Find (	Certificates				
>	🚞 Enterprise Trust		alva	~	Find Cartificator	1	
>	Intermediate Certification Author	All Ta:	SKS		Find Certificates		
>	Trusted Publishers	View		>	Import		
>	Untrusted Certificates						
>	Third-Party Root Certification A	Refre	sh				
>	📔 Trusted People	Expor	t List				
>	Client Authentication Issuers						
>	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.

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.

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.

File to Import					
Specify t	e file you want to	import.			
File name	:				
C:\User:	ddunn \Download	s\Local Lab Roo	t CA.cer		Browse
Note: Mo	re than one certifi	cate can be sto	red in a single file	in the follo	wing formats
Persor	al Information Exc	hange-PKCS #	12 (.PFX,.P12)		
Crypto	graphic Message S	Syntax Standar	d- PKCS #7 Certi	ficates (.P7	в)
Micros	oft Serialised Certi	ficate Store (.S	ST)		

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.
- ٠

#### 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-v10.0xxxxxxx\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-v10.01xxxxxx/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.

Enterprise Access Management Wizard	×
Storage for Security Objects Select where Enterprise Access Management security objects are stored.	
Enterprise Access Management security objects may be stored ether in a Deducted     mesen index where Enterprise Access Management security objects are stored     in the Corporat and Management security objects are stored     in a Deducted directory     Pease index the mann of the EMA Deducted directory server. Expected     mesen are not an enterport liability bot in \$55000     Dentery server: [Includent of a full who has bots to the SMD or stored or server.]	
< Back Next > Car	cel

#### 15.Click Next.

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

<ul> <li>Tracing</li> </ul>	
+ Directory	
Authentication	
Synchronize keys	Do not synchronize: prompt user for Windows passwor
Manage access points	Authenticate computer to the controller
New registration	DN0
+ Enterprise SSO	
E 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			$\times$
Ente	<b>rprise Access Management Clie</b> Select the Enterprise Access Manager workstation.	<b>nt modules</b> ment Client modules to	install on your	Ø
<b></b>	Select the Enterprise Access Manag press Next to proceed.	gement Client modules	to install on you	r workstation and
	Authentication mode:	Authentication Mana	iger	~
	Administrative workstation	SSPR wo	rkstation	
	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.

😭 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\Adv	/anc	edLogin		
V HKEY_LOCAL_MACHINE	^	Name	Туре	Data
CODOCOCO     General Constraints     General Cons		el (Defue) Exclose/Wen Exken@encored Exclose/Wen Exken@encored Exclose/Wen Exken@encored DevadBattaction/Encored Exclose/Exclose/Encored MontalDirectory El LeckTimer el WennableEncolTicol	REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_DWORD REG_SZ	(nale not set) bio000006 (10) bio000000 (10) bio000000 (1) bio000001 (1) cl/Program Files/Biddan/Enterprise Access Management/ bio000012c (00) cl/program files/Mymi/Mymi 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.

#### 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	_		$\times$				
File Edit View Help							
📌 🖥 🛱 📑 🔀 崎	1						
🛍 📰 🔗 🛸 🖬 🖼							
Enterprise Studio Configuration							
🗄 👘 EAM							
🚊 🛑 Evidian Enterprise Access Management							
🖨 📩 Application access							
Application security objects							
👜 📥 Applications							
🖃 🛑 Technical definitions	_						
	-						
🖶 🛑 User Access			New Win	dow			
🚊 🛑 Program Data		Abed B	Rename				
🖮 🛑 Evidian Enterprise Access N		23	Delete				
Access Points		-					
🛓 📋 Authorities		20	Cut				
🖶 📋 Blacklisted cards		-	Сору				
iAMForeignObjects			Paste				
🖶 🧰 Reports		24	Update D	irectory			
iiii Requests			Export	,			
			Import				
	20	×	import				
	ŝ	I.	Test				
	prise	114	Add to Te	st List			

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				
Gener Choos the wi	al Window se a name a ndow type y	description and type for this window. SSO behavior depends on you select.				
Winde	Window name: Login Window					
Windo	Window type: 🗉 StandardLogin 🗸					
Windo Stand This is The lo to the	ow Type De ardLogin: the standa ogon identifi user are se	escription ard procedure for SSO Enabling an application. er, password and some additional parameters specifi ant to the associated fields.	c			

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 drop the target icon onto its title bar or inside a web page. Web page	and
URL [file://C:\Users\administrator\Desktop\sampleLog	gin.html
Detect browser title Configuration	
Sometimes, URLs differ between sessions. Use variable detection to handle this.  enable variable URL detection  Config  Parameter of the web page	URL
D Look for text	
🔿 In Field	Ċ
If window detection is not sufficient, you can use Advanced detection to add constraints on process.	Advanced
OK Cancel	Help

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	$\times$
General Options Detection Actions	
Window fields description This window type sends the user authentication data to the fields defined below	
No field is mandatory.	
Identifier :	
Password :	
Do not prompt for user account	
Additional fields customization Click on the Customize button to specify additional parameters Customize	
After the SSO has been done Do nothing     O Press the <enter> key</enter>	
O Press the button :	
OK Cancel Help	

Figure 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 ×
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 white space: "" (0x85601f90) white space: "" (0x85601f90) white space: "" (0x856002d0) white space: "" (0x856002d0) white space: "" (0x856022s50) "Infobar Container" (0x85602c10) </pre>
✓ 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 $\checkmark$
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 Applicat	ion			
Search request	Account Ge	neration	Accounts	Events
<ul> <li>Evidian Enterprise Access Management</li> <li>Application access</li> <li>Application security objects</li> <li>Applications</li> <li>Technical definitions</li> <li>User Access</li> <li>Program Data</li> <li>Inbound access</li> <li>Outbound access</li> <li>Ontbound access</li> </ul>	Application Name: Def Sample J	(pplication	SC User Access	Aoministrators

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.

<b>P</b> -	Account Gene	ration		🔗 Accounts		Events
📒 Info	mation	🔊 Configu	ration	🛃 User /	Access	😤 Administrators
General	Account Base	Account Propert	ies SSO	External Names	Provisioning	connector
Metho	Access Str	rategies OLE/Au	tomation			
- 00						
	o propagation					
	Default SSO pro	pagation method				
	SSO		$\sim$			
	SSO					
	Windows authe	entication				
	OLE/Automatic	n		Select E	Edit	
	XenApp					
	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	t application profile
Search request	🖉 Configuration 🧧 Applies to 🏮 Events
EAM     Evidian Enterprise Access Management     Application access     Application security objects     Application security objects     Application security objects     Application profile	Application Profile           Name:         Default application profile           Configuration         General
	Use password format control policy specified here (ignore application default)           Default Picp
<ul> <li>Program Data</li> <li>Inbound access</li> <li>Outbound access</li> <li>Tymi</li> </ul>	Password generation policy: Default Password policy ↓ User must re-suthenticate to perform SSO
	☐ Launch application at start-up of Enterprise SSO
	When application is used, set user's 'unlocking level' to: 0
	Allow the date to test the application with this relief insection.

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.

# (Wearable only) Installing and Configuring Software on User Terminals and for Remote MES Applications

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.

On user terminals that use the Nymi Band as a wearable device, perform the following actions

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

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

#### About this task

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

#### **Procedure**

- 1. Log in to the terminal, with an account that has administrator privileges.
- 2. 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, expand Nymi Runtime.

8. Select Nymi Bluetooth Endpoint, and then select Entire feature will be unavailable.

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

🛃 Nymi Runtime 5.0	.5.46 Setup	ē	—	
Nymi Runtime S Select the way yo	etup ou want features to be installe	ed.		-^-
Click the icons in t	he tree below to change the	way features will be	e installed.	
	ymi Runtime ■ Vymi Agent Nymi Bluetooth Endpoir Will be installed on lo B Entire feature will be Feature will be install	nt ocal hard drive installed on local led when required	hard drive	
<	× Entire feature will be	unavailable		
				Browse
Reset	Disk Usage	Back	Next	Cancel

Figure 21: Nymi Bluetooth Endpoint feature will be unavailable

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

🞲 Nymi Runtime 5.0.	5.46 Setup		ē			
Nymi Runtime Se	etup					
Select the way you	u want features to be inst	alled.				94
Click the icons in t	ne tree below to change t	ne way	features v	vill be instal	led.	
	/mi Runtime ■	oint	This feat hard driv	ure require e.	s OKB	on your
						Browse
Reset	Disk Usage		Back	Next		Cancel

Figure 22: Nymi Bluetooth Endpoint feature is not available

10.On the Service Account window, click Next.

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

## 12.Click Finish.

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

## 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.

ertlm - [Certificates - Local Computer	Trusted Root Certification Au	ithorities] — 🗆	$\times$
File Action View Help			
🗢 🄿 🙍 📰 📋 🔯 🕞	1		
<ul> <li>Certificates - Local Computer</li> <li>Personal</li> <li>Trusted Root Certification Authoritie</li> </ul>	Object Type	_	
Certificates	Find Certificates		
>      Enterprise Trust     Difference Certification Author	All Tasks	Find Certificates	
> Trusted Publishers	View >	Import	
<ul> <li>Untrusted Certificates</li> <li>Third-Party Root Certification A</li> </ul>	Refresh		1
> 🚞 Trusted People	Export List		
Client Authentication Issuers     Preview Build Roots	Help		

Figure 23: 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
To continue, dick Next.
Next Cancel

Figure 24: Welcome to the Certificate Import Wizard screen

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

File	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 25: 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 Runtime software

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

## About this task

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

#### **Procedure**

- 1. Log in to the terminal, with an account that has administrator privileges.
- 2. 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, perform one of the following actions:
  - If the user will perform authentication tasks in a local MES application, click **Next**.
  - If the user will perform authentication tasks in an MES application on a Citrix server or RDP session host:
    - a. Select Nymi Agent, and then select Entire feature will be unavailable, as shown in the following figure.

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

Figure 26: Nymi Agent feature will be unavailable

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

Wymi Runtime 5.0.5.4	6 Setup				_	· .	×
Select the way you w	ant features to be instal	ed.				6	5
Click the icons in the	tree below to change the	way	features	will be in:	stalled.		
Nymi	Runtime Nymi Agent Nymi Bluetooth Endpoi	nt	This feat hard driv	ture requ ve.	uires OK	B on your	
μ						Browse	
Reset	Disk Usage		Back	Ne	ext	Cancel	

Figure 27: Nymi Agent feature is not available

c. 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.

## 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-v10.0xxxxxx*\*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-v10.01xxxxx/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 synchronize: pr	rompt user for Windows passv	10
	Manage access points	Authenticate compute	er to the controller	
	New registration	D <sub>No</sub>		
+	Enterprise SSO			
à	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			$\times$	
Ente	<b>rprise Access Management Clie</b> Select the Enterprise Access Manager vorkstation.	nt modules nent Client modules to	install on your	<b>e</b>	
	Select the Enterprise Access Manag press Next to proceed.	ement Client modules	to install on your	workstation and	
	Authentication mode:	Authentication Mana	ger	~	
	Administrative workstation	SSPR wo			
	Press Advanced for more installation	s Advanced for more installation options.			
		< 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.

## **Disabling Drive By Authentication**

Perform the following steps on each user terminal to prevent a user from logging into a user terminal with a blank password.

## About this task

## **Procedure**

- **1.** Open *regedit.exe*
- 2. Navigate to *HKEY\_LOCAL\_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork*.
- 3. Right-click Authentication, and then select New > DWORD (32-bit) value
- 4. In the *Value* field, type WearableNeedsRFID.
- 5. Edit the value, and then in the Value data field, type 1.
- 6. Click OK.
- 7. Close Registry Editor.

#### 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.

# (Citrix server/RDP session host only) Configuring the EAM client to Communicate with the Centralized Nymi Agent

On the Citrix server/RDP session host, configure the EAM Client to communicate with the Nymi Agent server by performing the following steps.

#### **Procedure**

- 1. Run regedit.exe and navigate to HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork \Authentication.
- 2. Create a new string named NymiAgentUrl, and then edit the string.
- 3. Update the Value data field with the port used to connect the centralized Nymi Agent over a WebSocket connection, in the following format:

ws://agent\_fdqn:9120/socket/websocket

## (Citrix/RDP environments only) Configuring the User Terminals to Access Centralized Nymi Agent

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

## About this task

#### **Procedure**

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

## **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, 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 file 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.

## 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 taskbar 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.

7	Enterprise SSO : Sing	le Sign-On Engine		-		×	2
	Activate	Suspend	C Refresh	ባ	Stop		^
	Connected User : Current role :	Administrator No selected role	Reload the techni	cal refere	ences		
							~
	<					>	
Ready							

Figure 28: eSSO application Home Window

3.

On the **Account** tab (1), 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.

_	,	<i>,</i>	Show password	
2	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 29: 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 SSO Session - Re-authentication
	Enterprise Single Sign-On
Login:	•••• Administrator V
Password:	
Log on to:	NYMI ~
	OK Cancel

Figure 30: SSO Login screen

**6.** Close the SSO application.

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

#### **Results**

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

If you change the technical definition at a later time, it is necessary to right-click the technical definition and select **Update Directory** and delete the Evidian cache.

## **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.



# (RFID-only) Installing and Configuring Software on RFID-only User Terminal and for Remote MES Applications

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.

On user terminals that use the Nymi Band as an RFID-only device, perform the following actions

## **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-v10.0xxxxxx\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-v10.01xxxxx/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 synchronize: pr	rompt user for Windows passv	10
	Manage access points	Authenticate compute	er to the controller	
	New registration	D <sub>No</sub>		
+	Enterprise SSO			
à	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			$\times$
Ente	<b>rprise Access Management Clie</b> Select the Enterprise Access Manager vorkstation.	nt modules ment Client modules to	install on your	9
<b></b>	Select the Enterprise Access Manag press Next to proceed.	gement Client modules	to install on you	r workstation and
	Authentication mode:	Authentication Mana	ger	~
	Administrative workstation	SSPR wo		
	Press Advanced for more installation	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.

## Overriding the authentication method

Copy the *TokenManagerStructure-Nymi-RFID.xml* file to RFID-only user terminals and Citrix Server/RDP session hosts, to support the use of an RFID-only Nymi Bands.

## **Procedure**

- 1. Obtain the RFID-only version of the TokenManagerStructure file, *TokenManagerStructure-Nymi-RFID.xml* from the software package that you downloaded. The file is located in the *Evidian-Supplementary-Files* subdirectory.
- 2. Rename the *TokenManagerStructure-Nymi-RFID.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





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.

## **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 **Z** taskbar 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.



Figure 32: 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.

Enterprise SSO : Single Sig     Enterprise SSO : Single Sig     Def Sample Application		~	Delegate Add to favorites Remove from favorites Hide applications without credential Open SSOStudio		×
			Start application Create shortcut		
			Disable the application Enable the application Enable all applications		
		_		_	

Figure 33: 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 Enterprise SSO Session - Re-authentication

	Enterprise Single Sign-On	
Login:	•••• Administrator 🗸 🗸	
Password:		
Log on to:	NYMI	
	OK Ca	ncel

Figure 34: SSO Login screen

6. Close the SSO application.

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

#### **Results**

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

If you change the technical definition at a later time, it is necessary to right-click the technical definition and select **Update Directory** and delete the Evidian cache.

## **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.



## **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 36: Search request window

3. Click Search.

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

Figure 37: RFID tab for a user

User: UATAdmin						
⊨ P Search request	📔 Information 🛛 📜 C	onnection 🛛 👗 Security	Profiles 🛛 😤 Admi	inistration 🛛 😹 App	lication Access	8 <sup>nd</sup> Accounts
evs-uatadmin	Bession Delegation	Mobile Devices	Smart Card	RFID	Biometrics	Events
EAM	RFID Identifier	State	Battery status	Refresh		
Evidian Enterprise Access Management	SF022D3398F489	Active	Not available		-	
Application access	ሎ+79:73:71:6D:CC:E2	Active	Not available	Assign	•	
Application security objects				Lock		
- 🧟 Default Pfcp						
- 👜 Default Password policy				Biacoss		
Default application profile						
B- Applications						
Technical definitions						
User Access						
Program Data						

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

## **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.



Figure 38: Search request window

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

Figure 39: RFID tab for a user

User: UATAdmin					
□- P Search request	Co	nnection 🕹 Security	Profiles 🧏 Admin	istration	Accounts
⊨_P ev3-uatadmin	Session Delegation	Mobile Devices	Smart Card	RFID     Biometrics	O Events
🗄 📇 UATAdmin		•			•
E SAM	RFID Identifier	State	Battery status	Refresh	
Evidian Enterprise Access Management	SF022D3398F489	Active	Not available		
- Carl Application access	かた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					
H- C 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 v		✓ davs.		Anniv
Owner REID Identifier			State	Battery status	Expiration Date
WEv2-Uat1		2F:2D:8D:0B:7 5FDB2C433FBD6E	Blacklisted Blacklisted	Unkown Unkown	

Figure 40: 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.



Figure 41: Search request window

## 3. Click Search.

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

```
Figure 42: RFID tab for a user
```

User: UATAdmin					
Search request     Borner P ev3-ustadmin     Borner P ev3-ustadmin     Borner P ev3-ustadmin     Dev3-ustadmin     Dev3-ustadmin	Information     Account of the session Delegation     RFID Identifier     GF0:2203398F489     H-1-79:73:71:60:CC:E2	Inection Active	Profiles Adm Smart Card Battery status Not available Not available	inistration Access  Application Access  Application Access Bornetics Bornetics  Assign Lock Blackist	er Accounts
🖶 🧰 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.

## 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 Enterpris	e Access Management Console	- 0	×
File Directory V	iew Help		
$\leftarrow \rightarrow   \equiv$	□ ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;		?
A	Search request		
Directory	Search request     Access Management	Ø Configuration Use this tool to search for objects in the directory. Objects that are found can easily be accessed	^
	Application access      User Access      Demonstrate Constraints	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 araPitettion whome name starts with 'ann', tune 'ann''	
RFID	Default access point profile	- if you type an '@' character, the filter also applies to the email address (when available)	
	User Profiles     User Profile     Program Data	Search root: Select Remove	
biometrics	Inbound access     Outbound access	Filter: Renae Search Clear al	
Mobile	Computers Compu	Maximum number of results: 30	
Devices	General Control C		

Figure 43: 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 44: 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 and replace the *nymi\_api.dll* for the NEA.

### **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 45: 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 Enterp	rise Access Management Console		- 0	×
File Directory	View Help			
$\leftarrow \rightarrow  $	▋▝▋़ ۞ …, …, ≗ ♀ ≗ ♀ ♀ ↓ ↓	1		?
E C	Search request			
Directory	← ♀ Search request , ➡ ➔ EAM	S Configuration		^
(co) RFID	Vidian Enterprise Access Management     Der Application access     User Access     AccessPoint Profiles	Use this tool to search for objects in the directory. Objects that are found can easi the other than the constraint of the object name. Examples: - Fyou 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 use to find 'dwratert, the filter ada analies to the email address (when was	ilable)	
	Timeslices     User Profiles     User Profiles     Default user profile     Default user profile     Program Data	Search root: Select Object type: Auguster	Remove	1
Biometrics	Inbound access     Outbound access     Outbound access	Filter: Renae Search	Clear all	
Mobile Devices	Pyrini     Computers     Domain Controllers     P     ForeignSecurityPrincipals     P     Keys	Maximum number of results: 50		

Figure 46: Search request window

### 4. Click Search.

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

Figure 47: RFID tab for a user

User: UATAdmin					
Beach request	Information     A. Conn       A. Session Delegation     RFID Identifier       ● 570220397-499     A. Print Pr	Active	Profiles Admir Smart Card Battery status Not available Not available	Refresh Lock Bladdst	Accounts     Events

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	Blacklisted		~		
Battery sta	tus All	All			
Show RFID tokens expiring within			🔹 days.		Apply
Owner		RFID Identifier	State	Battery status	Expiration Date
WEv2-Uat1		2F:2D:8D:0B:7 5FDB2C433FBD6E	Blacklisted Blacklisted	Unkown Unkown	

Figure 48: 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