Troubleshooting Guide

Nymi Connected Worker Platform
v11.0
2024-07-20

Contents

Preface

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

Purpose

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

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

Audience

This guide provides information to NES and Evidian Access Management Administrators. An NES and Evidian Access Management Administrator is the person in the enterprise that manages the Connected Worker Platform with Evidian solution in their workplace.

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
11.0	July 30, 2024	Twelth release of this document. Updates include: • New error message **Evidian error 0x82003505 Impossible to retrieve administration rights** • Instructions about how to disable Desktop locks with a Nymi Band tap.
10.0	March 5, 2024	Tenth release of this document.
9.0	December 18, 2023	Ninth release of this document.
8.0	November 22, 2023	Eighth release of this document.
7.0	November 13, 2023	Seventh release of this document.
6.0	September 29, 2023	Sixth release of this document.

Version	Date	Revision history
5.0	September 11, 2023	Fifth release of this document.
4.0	August 21, 2023	Fourth release of this document.
3.0	May 8, 2023	Third release of this document.
2.0	March 20, 2023	Second release of this document.
1.0	January 9, 2023	First release of this document.

Related documentation

- **Nymi Connected Worker Platform—Overview Guide**

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

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

  Separate guides are provided for authentication on iOS and Windows device.
- **Nymi Connected Worker Platform—Administration Guide**

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

  This document provides information about how to develop Nymi-enabled Applications by using the Nymi API(NAPI).
- **Nymi SDK Developer Guide—Webapi(Windows)**

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

  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.
- **Nymi Connected Worker Platform—Troubleshooting Guide**

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

- **Nymi Connected Worker Platform—FIDO2 Deployment Guide**

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

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

  This guide provides regulatory information for the Generation 3 (GEN3) Nymi Band.
- **Third-party Licenses**

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

How to get product help

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

How to provide documentation feedback

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

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 Application Crashes

To reduce filesystem write operations, the Evidian Enterprise Access Management Solution stores log file messages in memory, and then writes the messages to the log files. When an application crash occurs, any messages that were stored in memory are lost.

When an Evidian EAM process crashes, fault messages appear in the Evidian EAM log files.

For example, when the Evidian Enterprise SSO process crashes, an error similar to the following appears:

```
Faulting application name: ssoengine.exe, version: 10.3.8573.4, time stamp: 0x64ddfb1d
Faulting module name: ucrtbase.DLL, version: 10.0.14393.2990, time stamp: 0x5caeb96f
Exception code: 0xc0000409
Fault offset: 0x000000000006e00e
Faulting process id: 0x853c
Faulting application start time: 0x01da26ab55d523e5
Faulting application path: C:\Program Files\Evidian\Enterprise Access Management\
ssoengine.exe
Faulting module path: C:\Windows\SYSTEM32\ucrtbase.DLL
Report Id: b6e04f81-92a9-11ee-8192-005056aac3f3
Faulting package full name:
```

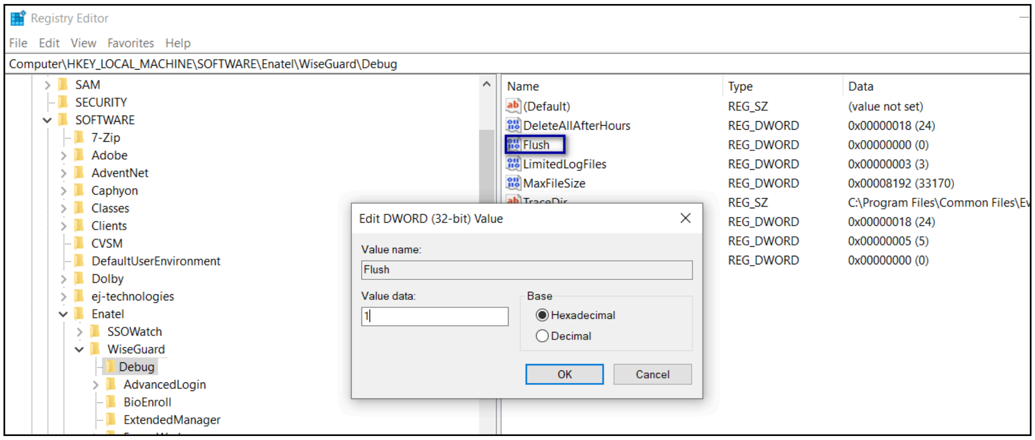
Faulting package-relative application ID:

Fault messages also appear the Window Event log files.

To assist in troubleshooting, perform the following steps to temporarily disable the storage of messages in memory to ensure that each message appears in the log file in real time:

1. Open `Registry Editor`
2. Navigate to **`HKLM > Software > Enatel > Wiseguard > Debug`**
3. Right-click **`Flush`**, and then select **`Modify`**.
4. Change the value in the **`Value data`** field to ***1***.

   The following figure provides an example of the registry key.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\Debug

SAM
SECURITY
SOFTWARE
7-Zip
Adobe
AdventNet
Caphyon
Classes
Clients
CVSM
DefaultUserEnvironment
Dolby
ej-technologies
Enatel
SSOWatch
WiseGuard
Debug
AdvancedLogin
BioEnroll
ExtendedManager

Name	Type	Data
(Default)	REG_SZ	(value not set)
DeleteAllAfterHours	REG_DWORD	0x00000018 (24)
Flush	REG_DWORD	0x00000000 (0)
LimitedLogFiles	REG_DWORD	0x00000003 (3)
MaxFileSize	REG_DWORD	0x00008192 (33170)
TraceDir	REG_SZ	C:\Program Files\Common Files\Ev
	REG_DWORD	0x00000018 (24)
	REG_DWORD	0x00000005 (5)
	REG_DWORD	0x00000000 (0)

Edit DWORD (32-bit) Value

Value name: Flush

Value data: 1

Base: ● Hexadecimal ○ Decimal

Figure 1: Flush Registry Key

5. Click **`OK`**.

After you reproduce the issue, return to `Registry Editor`, ensure that you change the value for the **`Flush`** registry key back to ***0*** to avoid continued frequent write operations.

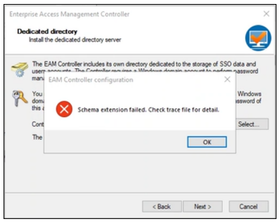
Evidian Installation Issues

Review this section for errors and issues that are related to the installation of the Evidian EAM Controller and Evidian EAM Client software.

Evidian stores the installation trace log files in the *C:\users\*`username`*\AppData\Local\Temp\Evidian\Traces* directory.

Schema extension failed Check trace file for details

This error message appears when you install/update the Evidian EAM Controller software.


Enterprise Access Management Controller
Dedicated directory
Install the dedicated directory server
EAM Controller configuration
Select...
OK
< Back
Next >
Cancel

The EAM Controller includes its own directory dedicated to the storage of SSO data and users accounts. The Controller requires a Windows domain account to perform password

Schema extension failed. Check trace file for detail.

Cause 1

The *C:\Program Files\Common Files\Evidian\WGSS\Logs\ESSOControllerSetup-Dedicated log* file displays the following errors:

```
=> Connecting to "localhost:55000"
        =>
        ServerSetupGenericPropertiesPage.cpp0160: Output:
        => The connection cannot be established
        => The error code is 8224
```

Which indicates the ESSOServer service exists but the service is stopped.

Resolution

Cancel the Evidian EAM Controller software installation, start the ESSOServer service, and the install the Evidian EAM Controller software again.

Cause 2

The *C:\Program Files\Common Files\Evidian\WGSS\Logs\ESSOControllerSetup-Dedicated log* file displays the following errors:

```
MS ldap_connect returned 0x8c060bf8 (0x00000000)

CAdsiHandler::InternalMSPing returned: 0x81020029

[PING] ERROR: InternalMSPing could not reach the server

CldapConfiguration::GetNextServerandRotate

CldapConfiguration::GetNextServerandRotate returned 0x81010009
.
.
[PING] Ping for domain O=EAM returned: 0x81020029
```

Which indicates that there is a connectivity issue between the Evidian EAM Controller and the Active Directory server.

Resolution 2

Resolve connectivity issues.

Evidian EAM Management Console Errors

This section provides information about informations that you might encounter logging into or using the Evidian EAM Management Console.

Console Login Fails with "Error during connection with the security services"

This issue appears when you attempt to log into the Evidian EAM Management Console.

You will also see the following error information: Network error: the EAM Security Services are unavailable. The Windows Service "EAM Security Services" is probably stopped. Please contact your administrator. Error code: 0x81011005

This message can appear for several reasons

Cause 1

The Evidian EAM Controller does not have connectivity to the Active Directory server.

Resolution 1

1. Confirm that the Evidian EAM Controller can communicate with the AD server. For example, confirm that you can ping the AD server.
2. On the AD server, review the properties of the account. Re-enable the account.

Cause 2

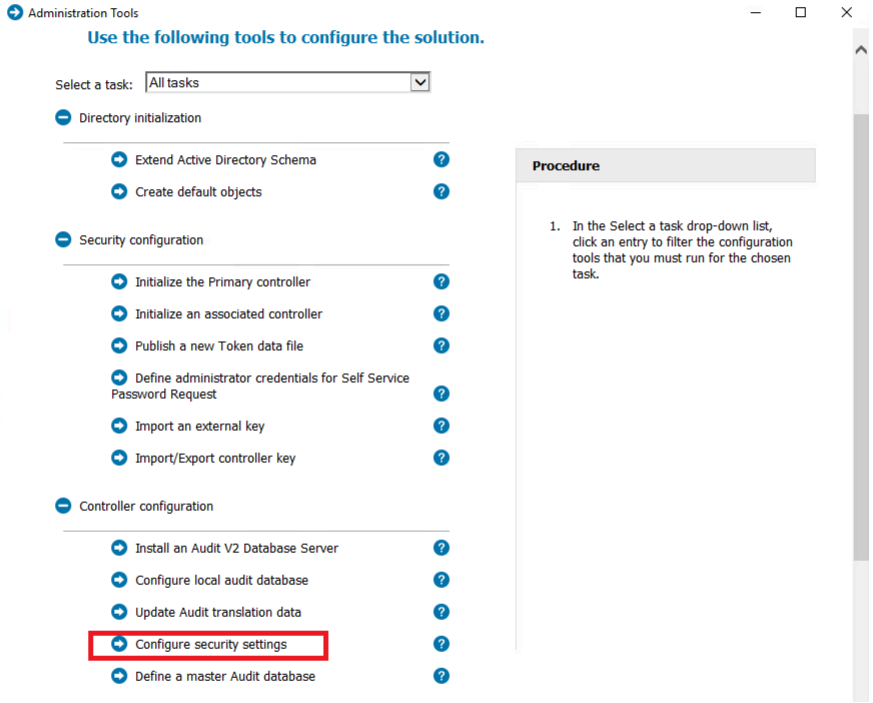
The password for the primary administrator account for the Evidian EAM Controller has changed or the account is disabled.

Resolution 2

Perform the following steps to update the password in the Evidian EAM Controller:

1. Log in with a domain administrator account.
2. From the EAM installation package navigate to the *..\EAM-v10.X\EAM.x64\TOOLS\WGSRVConfig* directory.
3. Double-click *WGSRVConfig.exe*.
4. On the `User Account Control` window, click **Yes**.

5. On the `Controller Configuration` select, select **`Configure security settings`**, as shown the following figure.

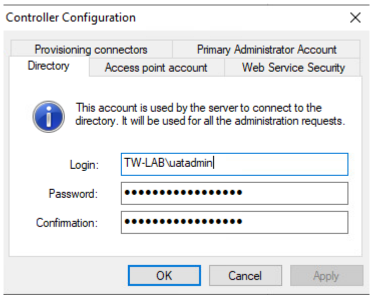

Administration Tools
Select a task:
All tasks
Directory initialization
Extend Active Directory Schema
Create default objects
Security configuration
Initialize the Primary controller
Initialize an associated controller
Publish a new Token data file
Define administrator credentials for Self Service Password Request
Import an external key
Import/Export controller key
Controller configuration
Install an Audit V2 Database Server
Configure local audit database
Update Audit translation data
Configure security settings
Define a master Audit database
Procedure

Use the following tools to configure the solution.

1. In the Select a task drop-down list, click an entry to filter the configuration tools that you must run for the chosen task.

Figure 2: Configure Security Settings option

6. On the `Directory` tab, in the **`Password`** and **`Confirmation`** fields, specify the new password.



This account is used by the server to connect to the directory. It will be used for all the administration requests.

Login: TW-LAB\uatadmin

Password: ••••••••••••••••

Confirmation: ••••••••••••••••

7. Click **`OK`**.
8. Close the EAM `Administration Tools` window.
9. Restart the **`Enterprise Access Management Security Services`** service.

Cause 3

The Evidian EAM Controller is configured to use LDAPS but the environment uses LDAP.

In this situation, the following errors also appear in the wgss log files:

```
AdsiHandler.cpp          :0715:   [PING] : No new server found (0x81010009)
AdsiHandler.cpp          :0716: CAdsiHandler::Ping returned: 0x81020029
LdapBaseRequests.cpp        :2761:[PING] Ping for domain O=EAM returned: 0x81020029
```

```
FrameworkServer.cpp          :0202:Wait 5 secs for services to start...
```

Resolution 3

Perform the following steps to configure the Evidian EAM Controller to use LDAP:

1. Run *regedit.exe*
2. Navigate to *HKLM\Software\Enatel\Framework\WGDirectory*.
3. Edit the SSL key and change the value from 1 to 0.
4. Restart the **`Enterprise Access Management Security Service`** service.

Console Login Fails with "Evidian error 0x82003505 Impossible to retrieve administration rights"

This issue appears when you attempt to log into the Evidian EAM Management Console.

Cause

The user account is a member of the Evidian inclusion group but does not have EAM administrator rights.

Resolution

Configure the user as a Primary Administrators, which gives them full adminstrator access to the EAM Console or assign a specific administrator role to the user account. The *Evidian EAM Console Administrator's Guide* provides more information about assigning roles to users.

Configuring Additional EAM Primary Administrators

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

About this task

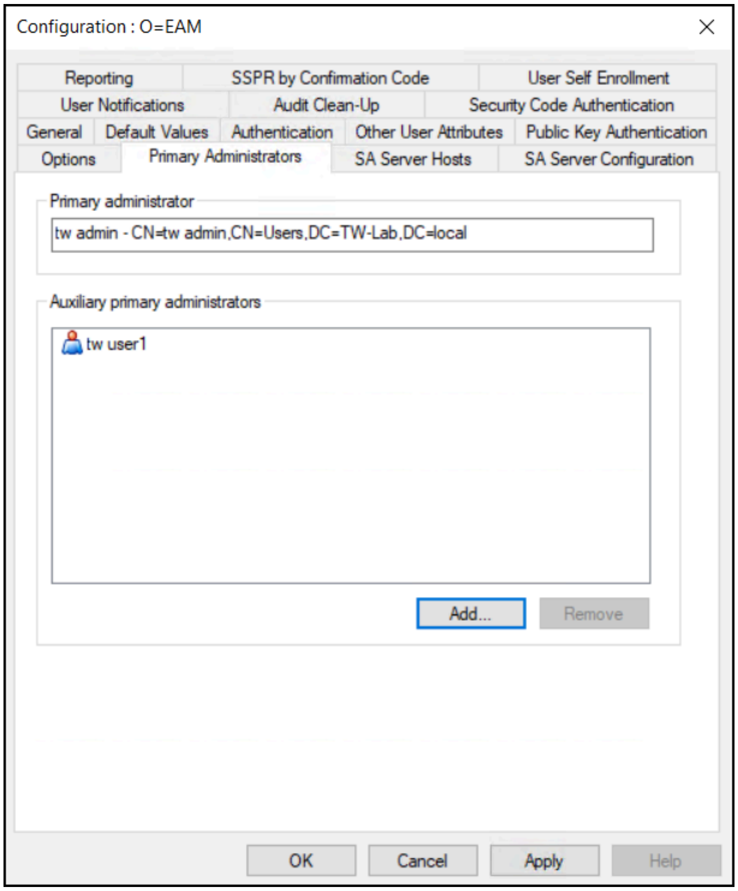
By adding at least one additional auxiliary primary user, you ensure that you have access to the Evidian EAM Controller in the case where the primary administrator is locked out of the Evidian EAM Controller, for example, if the password of the primary administrator changes.

Procedure

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

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

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



Primary administrator: tw admin - CN=tw admin,CN=Users,DC=TW-Lab,DC=local

Auxiliary primary administrators: tw user1

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

Authentication Error: you are not allowed to logon. You account is in the exclusions list

This issue appears when you attempt to log into the Evidian EAM Management Console.

Cause

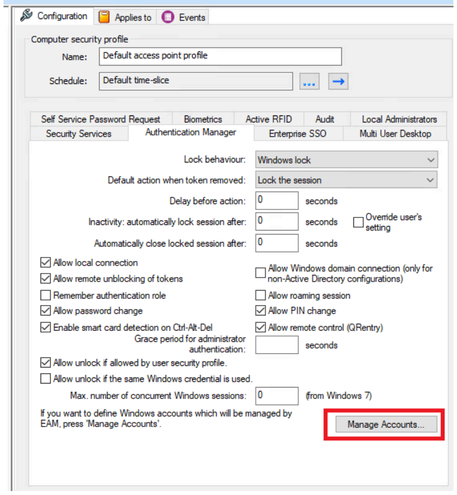
The Access Point Profiles on the Evidian EAM Controller are configured to use inclusion groups and the account is not a member of the associated Active Directory group.

Resolution

Add the user account to the appropriate Active Directory group.

To determine the name of the inclusions group, log into the Evidian EAM Management Console with an EAM administrator account and perform the following steps.

1. From the Evidian EAM Management Console, expand **`EAM > Evidian Enterprise Access Management > User Access > AccessPoint Profiles > Default Access Point Profile`**.
2. On the **`Configuration`** tab, select the **`Authentication Manager`** tab, and then click **`Manage Accounts`**.



Computer security profile

Name: Default access point profile

Schedule: Default time-slice

Lock behaviour: Windows lock

Default action when token removed: Lock the session

Delay before action: 0 seconds

Inactivity: automatically lock session after: 0 seconds □ Override user's setting

Automatically close locked session after: 0 seconds

☑ Allow local connection

☑ Allow remote unblocking of tokens

□ Allow Windows domain connection (only for non-Active Directory configurations)

□ Remember authentication role

□ Allow roaming session

☑ Allow password change

☑ Allow PIN change

☑ Enable smart card detection on Ctrl-Alt-Del

☑ Allow remote control (QRentry)

Grace period for administrator authentication: seconds

☑ Allow unlock if allowed by user security profile.

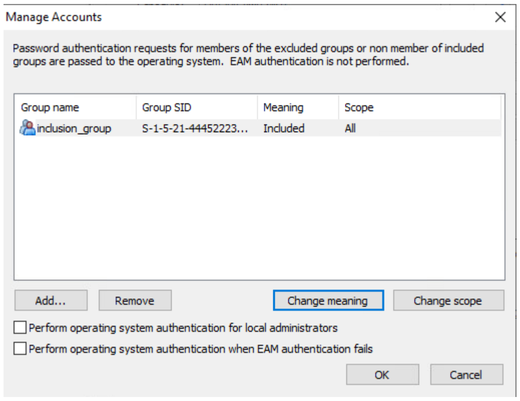
□ Allow unlock if the same Windows credential is used.

Max. number of concurrent Windows sessions: 0 (from Windows 7)

If you want to define Windows accounts which will be managed by EAM, press 'Manage Accounts'.

Figure 3: Manage Accounts

The `Manage Accounts` window displays the inclusion groups.



Manage Accounts

Password authentication requests for members of the excluded groups or non member of included groups are passed to the operating system. EAM authentication is not performed.

Group name	Group SID	Meaning	Scope
inclusion_group	S-1-5-21-44452223...	Included	All

☐ Perform operating system authentication for local administrators

☐ Perform operating system authentication when EAM authentication fails

Figure 4: Inclusion Group table

Evidian License has Expired

This message appears when you use EAM.

Cause

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

Note: You can also perform these steps to increase the number of Evidian licenses.

Resolution

Obtain a new license file and perform the following actions:

1. Log in to the Evidian EAM Controller with a user account that has access to install software.
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`**. Change the extension to **.txt.*
6. Navigate to the license file and then click **`OK`**.

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

   On the confirmation window, click **`OK`**.
7. Click **`Cancel`** to close the window.
8. Confirm the license update completed successfully by logging into the Evidian EAM Management Console and reviewing the license count and expiration date under the **About** menu.
9. Add the license file to each Evidian EAM Client machine by using the same steps that you performed on the Evidian EAM Controller server or you can export the license registry key on the Evidian EAM Controller, and then use group policies to push the registry key to each client.

Unable to connect to audit server

This error message appears when attempting to query the audit database in the Evidian EAM Management Console.

The wgss log file displays an error message similar to the following:
AutoImpersonator.cpp :0071: LogonUser Failed (user: *`username`* - domain: *`domain_name`*) with error: 0x00000569

Connecting to the SQL server with SSMS as the user in the error message fails with the error: Logon failure: the user has not been granted the requested logon type at this computer.

Cause

The EAM service account does not have the rights to log into SQL Server.

Resolution

Edit local or group policies to allow the EAM service account with log on local privileges on the SQL server.

Cannot Create New Access Point Profile

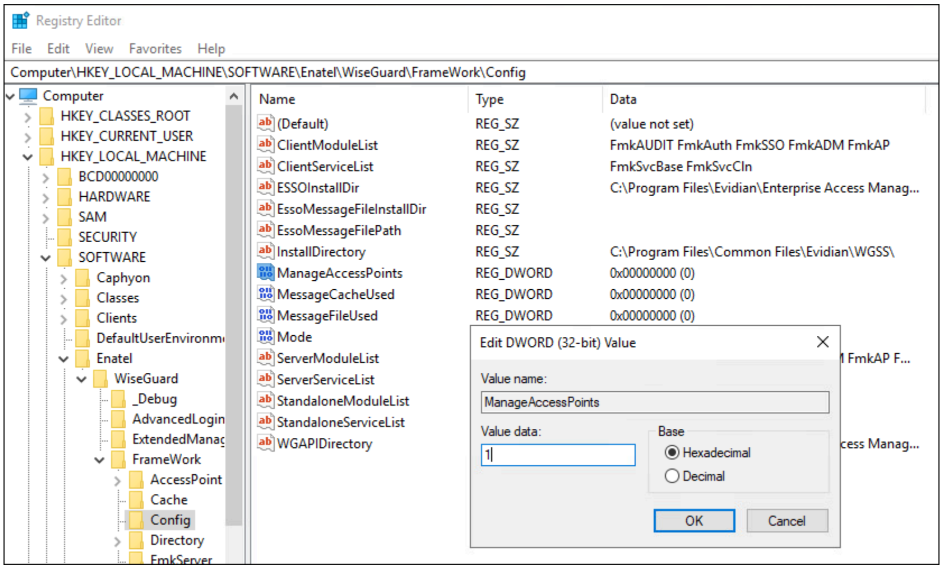
In the Evidian EAM Management Console, when you right-click **`Access Point Profiles`** and select **`New`**, the Access Point Security Profile option does not appear.

Cause

The ability to manage access point profiles is not enabled.

Resolution

1. Run *regedit* and navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork\Config*.
2. Edit the **`ManageAccessPoints`** key and change the value to ***1***, as shown in the following figure.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork\Config

Name	Type	Data
(Default)	REG_SZ	(value not set)
ClientModuleList	REG_SZ	FmkAUDIT FmkAuth FmkSSO FmkADM FmkAP
ClientServiceList	REG_SZ	FmkSvcBase FmkSvcCln
ESSOInstallDir	REG_SZ	C:\Program Files\Evidian\Enterprise Access Manag...
EssoMessageFileInstallDir	REG_SZ	
EssoMessageFilePath	REG_SZ	
InstallDirectory	REG_SZ	C:\Program Files\Common Files\Evidian\WGSS\
ManageAccessPoints	REG_DWORD	0x00000000 (0)
MessageCacheUsed	REG_DWORD	0x00000000 (0)
MessageFileUsed	REG_DWORD	0x00000000 (0)
Mode		
ServerModuleList		l FmkAP F...
ServerServiceList		
StandaloneModuleList		
StandaloneServiceList		
WGAPIDirectory		cess Manag...

Edit DWORD (32-bit) Value

Value name: ManageAccessPoints

Value data: 1

Base: ● Hexadecimal ○ Decimal

OK Cancel

Figure 5: Manage Access Points Registry Setting

3. Click **OK**.
4. Restart the **`Enterprise Access Management Security Services`** service.

LDAP server is not operational

This error appears when you perform an operation in the EAM console, such as adding a user account to the primary administrators list.

The WGSS log file contains the following errors:

```
        AdsiHandler.cpp      :8735:          -> CAdsiHandler::GetAvailableServer
        AdsiHandler.cpp      :8751:            [PING] No server is currently known as available
        WindowsTools.cpp      :2069:            -> GetDCNameFromDomainName
        WindowsTools.cpp      :2092:              Calling DsGetDcName with domain=xxx
        WindowsTools.cpp      :2119:              Using additional DS_WRITABLE_REQUIRED flag to get a
RWDC
        WindowsTools.cpp      :2128:              Using flags: 1073812240
        WindowsTools.cpp      :2138:             ::DsGetDcName returned: 0x0000054b
        WindowsTools.cpp      :2178:            <- GetDCNameFromDomainName returned: 0x81020029
        AdsiHandler.cpp      :8765:          <- CAdsiHandler::GetAvailableServer returned: 0x81020029
        AdsiHandler.cpp      :0234:        <- CAdsiHandler::Init returned: 0x81020029
        LdapBaseRequests.cpp    :3105:          -> CLdapBaseRequests::SetDirectoryNotAvailable
        LdapBaseRequests.cpp    :3222:            [PING] An LDAP request failed on domain
DC=xxx,DC=nymi,DC=com (directory server not reachable)
        LdapBaseRequests.cpp    :3124:          <- CLdapBaseRequests::SetDirectoryNotAvailable returned:
0x00000000
        LdapBaseRequests.cpp    :0592:        <- CLdapBaseRequests::LdapBaseInitEx returned: 0x81020029
        AutoLock.cpp        :0178:       CS Unlock(LdapBaseInitEx)
        AdsiHandler.cpp      :3137:      <- CAdsiHandler::OpenObjectDN returned: 0x81020029
        AdsiHandler.cpp      :4131:      Unable to open object DC=xxx,DC=nymi,DC=com, error: 0x81020029
        AdsiHandler.cpp      :4132:    <- CAdsiHandler::GetClassFromDN returned: 0x81020029
        FmkLdapBaseRequests.cpp :1738:     ERROR: unable to find out the class of DC=xxx,DC=nymi,DC=com -
0x81020029
```

```
        FmkLdapBaseRequests.cpp  :1943:   <- CFmkLdapBaseRequests::InterpretCooperativeRequest returned: 
0x81020029
        FmkLdapBaseRequests.cpp  :2288:<- CFmkLdapBaseRequests::Execute returned: 0x81020029
```

Cause

The *DsGetDcName returned: 0x0000054b* error indicates that the specified domain either does not exist or could not be contacted.

Resolution

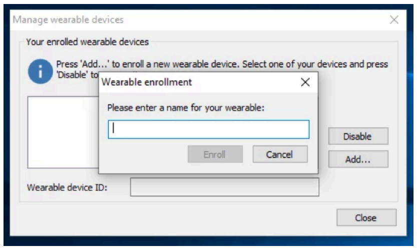
Correct DNS configuration issues.

Enrollment Errors

The section provides more information about errors that you might experience during Nymi Band enrollment.

Wearable enrollment screen appears instead of the Nymi Band Application

When you click **>Add** in **`Wearable Device Manager`** and log in with your username and password, the `Wearable enrollment` window appears instead of the Nymi Band Application, as shown in the following figure.



Press 'Add...' to enroll a new wearable device. Select one of your devices and press 'Disable' to

Please enter a name for your wearable:

Figure 6: Wearable Enrollment window

Cause

Ensure that the registry key for the WearableEnrollTool is defined.

Resolution

1. Launch *regedit.exe*.
2. Navigate to *HKLM\Software\Enatel\WiseGuard\AdvancedLogin*.
3. Edit the *WearableEnrollTool* key and update the value with the correct path and file name for the *nem.exe*. For example, *C:\Program Files\Nymi\Nymi Band Application\nem.exe.*

Wearable devices services are not available

This error message appears when you attempt to launch the Nymi Band Application.

Cause

The value for the ***WearableEnrollTool*** registry setting is incorrect.

Resolution

1. Launch *regedit.exe*.
2. Navigate to *HKLM\Software\Enatel\WiseGuard\AdvancedLogin*.
3. Edit the *WearableEnrollTool* key and update the value with the correct path and file name for the *nem.exe*. For example, *C:\Program Files\Nymi\Nymi Band Application\nem.exe.*

Failed to External Authenticator

This error message appears during enrollment in the Nymi Band Application.

The following errors appear in the *nem.log* file:

```
        Band error: (2000) Request made with invalid parameters
        [18] ERROR  Band operation error:
MessageType=Nymi.Model.BandMessage.Response.CreateExternalAuthBandResponse ErrorCode: 2000
ErrorDescription: Request made with invalid parameters. ErrorSpecifics: MalformedFraming
        [31] ERROR  Failed Create External Authenticator on real band on retry #1
        NEM.Services.ExternalAuthenticatorException Band error 2000:
        Request made with invalid parameters.
        MalformedFraming
```

Cause

Blacklisted entries for a previous Nymi Band were not deleted for the Nymi Band user in the Evidian EAM Management Console.

Resolution

To resolve this issue, perform the following steps:

1. Log into the Evidian EAM Management Console with an EAM administrator account.
2. Click the **`Directory`** icon.
3. In the left navigation pane, click **`RFID`**.
4. From the **`RFID state`** list, select **`Blacklisted`**, and then click **`Apply`**.
5. Select each blacklisted entry that appears for the user and click **`Delete`**.
6. On the **`Please confirm RFID state change`** prompt, click **`Yes`**.

Failed to create security settings. Try again or contact the Administrator to restart the enrollment

This error appears in the Nymi Band Application during enrollment and includes the message Evidian error: (0x81011004) The server is unreachable.

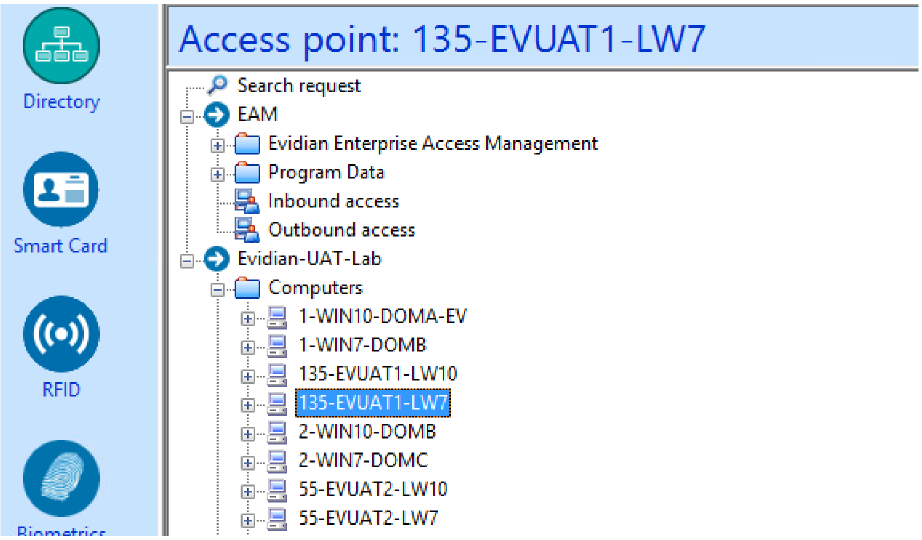
Cause 1

Issues with Evidian cache.

Resolution 1

Delete the Evidian cache files on the enrollment terminal.

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



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

Cause 2

There is a Nymi Band to user association in the Evidian EAM Controller, or the Nymi Band is blacklisted but not deleted.

When the Nymi Band is blacklisted but not deleted, the following error appears in the *nem.log* file:

```
            [9] ERROR  Band operation error: 
MessageType=Nymi.Model.BandMessage.Response.CreateExternalAuthBandResponse
            ErrorCode: 2000 ErrorDescription: Request made with invalid parameters. ErrorSpecifics: MalformedFraming
            [27] ERROR  Failed Create External Authenticator on real band on retry #0
            NEM.Services.ExternalAuthenticatorException Band error 2000: Request made with invalid 
parameters.MalformedFraming
```

Resolution

To resolve the issue, remove the Nymi Band association in the Evidian EAM Controller. Retry the enrollment using the Nymi Band Application. The *Nymi Connected Worker Platform with Evidian Guide* provides more information.

.

Failed to create security settings. Try again or contact the Administrator to restart the enrollment

This error appears in the Nymi Band Application during enrollment and includes the message Evidian error (Authentication error: you are not allowed to log on. You account is in the exclusion list. Error code: 0x82002060) Failed to open session.

Cause

The user account is not a member of the EAM inclusion group.

Resolution

Add the user account to the EAM Inclusion group.

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 theEvidian EAM Controller.

Resolution

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

Enrollment Succeeds But Nymi Band Does Not Appear in Manage Wearable Window

Enrollment completes but device does not appear in the `Manage Wearable` window. On the Evidian EAM Management Console in the properties of the user, the RFID tab does not display the device. In NES, in the properties of the user, the Nymi Band appears.

Cause

The Enrollmen Destination is not set to "Nes and Evidian" in the NES active policy.

Resolution

To resolve this issue, perform the following steps:

1. Log in to the NES Administrator Console and edit the active policy.
2. Select the "Nes and Evidian" option for the **`Enrollment Destination`**.
3. Sign into the Nymi Band Application and complete the enrollment.

User Cannot Re-enroll their Nymi Band After Removal from Evidian Access Management Database

A user cannot re-enroll their Nymi Band after performing a delete user data operation and the blacklisting and deleting the Nymi Band in the Evidian Accesss Management (EAM) database.

Cause

The Nymi Band to user association was not removed from the Nymi Enterprise Server (NES) database.

In Nymi Enterprise Edition 3.2 and earlier, the user to Nymi Band association was recorded in the EAM database only. In NEE 3.3 and later and Connected Worker Platform(CWP), enrollments in an Evidian environment write Nymi Band information to both the NES and EAM database.

Resolution

After the user performs the delete user data operation, the NES Administrator deletes the Nymi Band association with the user in the NES Administrator Console.

Enhancement INTAKE-500 has been filed to change the enrollment behaviour in the Nymi Band Application to support re-enrollments that do not require administrator intervention.

Nymi Band Tap Issues

This section provides information about the errors and issues you might see when you perform tap operations with the Nymi Band.

Cannot Unlock the User Terminal

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

Cause

The unlock function relies on the Nymi SDK. The *nymi_api.dll* file that is used by Evidian must match the version that is included in the Nymi SDK package for the deployed Nymi solution..

Resolution

1. Copy the *nymi_api.dll* file from the *C:\Program Files\Nymi\Nymi Band Application* directory to the *C:\Program Files\Common\Evidian\WGSS* folder on the user terminal.
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 Tap to Lock User Terminal

The desktop does not lock when a user taps an authenticated Nymi Band on the NFC reader.

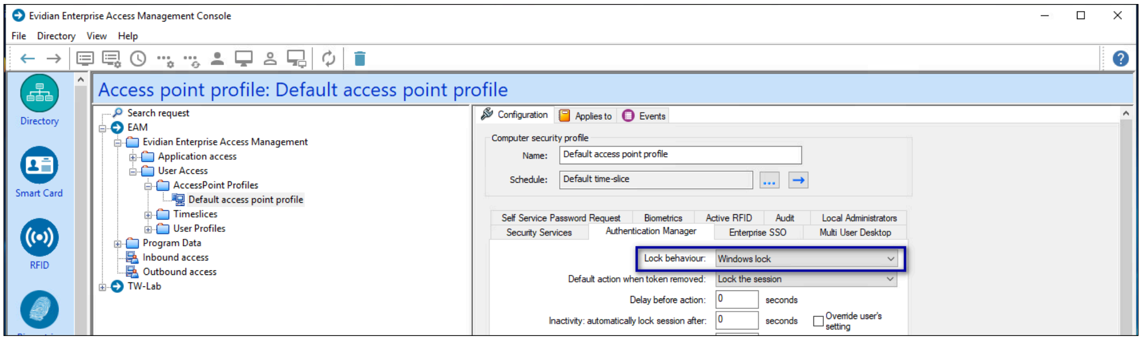
Cause

The Access Point Profile configuration for lock behaviour is set to Do Nothing.

Resolution

1. Log into the Evidian EAM Management Console, and click the **`Accounts and access rights management`** icon.
2. Expand **`EAM > Evidian Enterprise Access Management > User Access > AccessPoint Profiles > Default Access Point Profile`**, or the applicable profile.
3. On the **`Authentication Manager`** tab, from the **`Default action when token removed list`**, select **`Lock the session`**.
4. Click **`Apply`**.

   The following figure provides an example of the **`Default action when token removed list`** option.



Access point profile: Default access point profile

- Search request
- EAM
  - Evidian Enterprise Access Management
    - Application access
    - User Access
      - AccessPoint Profiles
        - Default access point profile
      - Timeslices
      - User Profiles
  - Program Data
  - Inbound access
  - Outbound access
- TW-Lab

Computer security profile

Name: Default access point profile

Schedule: Default time-slice

Lock behaviour: Windows lock

Default action when token removed: Lock the session

Delay before action: 0 seconds

Inactivity: automatically lock session after: 0 seconds □ Override user's setting

Nymi Band Tap Not Detected

When a user performs a Nymi Band tap, the Evidian SSO window does not detect the tap.

Cause 1

The connection between the Evidian EAM Client and Evidian EAM Controller on Port 3644 is blocked.

The following errors appear in the WGSS log file at the time of the Nymi Band tap:

```
           AccessPointAuthCln.cpp :1432:-> VOLUNTEER Disconnection from WG SERVER
           AccessPointAuthCln.cpp :1433:->
           AccessPointAuthCln.cpp :0366:-> SetServerStatus: 0x81011009
           AutoLock.cpp :0272:CS Lock(AP Infos)
           AccessPointAuthCln.cpp :0386:->
           AccessPointAuthCln.cpp :0387:-> WG SERVER :3644 for domain xyz IS DOWN OR
UNREACHABLE
           AccessPointAuthCln.cpp :0388:->
```

Resolution 1

Ensure that firewall allows TCP connections from the Evidian EAM Client and Evidian EAM Controller on port 3644.

Cause 2

The user terminal has multiple network adapters and the network connection has switched from one network adapter to another.

In this situation, the *nymi_blueooth_endpoint.log* files does not report the error Nymi Bluetooth Endpoint is missing and also displays messages that show that the Nymi Bluetooth Endpoint reconnects to the Nymi Agent and the subscribes to a topic with a different IP address.

Resolution 2

Log out (not just disconnect) of the current Citrix / RDP session, and then relaunch the session, which starts a new application session and triggers Nymi API to start and subscribe to the new IP address.

Nymi Band Tap Inadvertantly Locks Desktop

When you enable Authentication Manager on a user terminal, if a user taps their authenticated Nymi Band on an NFC reader or the Bluetooth Adapter, and an Enterprise SSO window is not in focus on the desktop, the desktop locks.

Resolution

To prevent this behaviour, perform the following steps:

1. Log into the user terminal and create an empty text file in the a directory of your choice. For example, *C:\Program Files\Common Files\Evidian\no_lock.text*.
2. Run *regedit.exe*.
3. Navigate to **`HKEY_Local_Machine > SOFTWARE > Enatel > WiseGuard`**.
4. Right-click **`AdvancedLogin`**, and then select **`New > String Value`**.
5. In the **`Value Name`** field type ***IgnoreCardEventIfFileExists***.
6. Edit the **`IgnoreCardEventIfFileExists`** key, and in the **`Value Data`** field, type the path to the empty text file, and then click **`OK`**.
7. Close `Registry Editor`.

Wearable device is unreachable. Please make sure it is on or activated

This error message appears when you attempt to tap to unlock a user terminal with an enrolled Nymi Band or when attempting to perform an SSO action.

Cause

- The ManageAccessPoint registry key is not configured correctly on the client.
- The environment uses a centralized Nymi Agent but the Nymi Agent URL definition is incorrect.

Resolution

To resolve this issue, perform one of the followings on the Evidian EAM Client and the Evidian EAM Controller:

- Correct the **`ManageAccessPoint`** registry key Evidian EAM Client and the Evidian EAM Controller:

  1. Run *regedit.exe*.
  2. Navigate to *HKLM\Software\Enatel\Wiseguard\FrameWork\Config\*.
  3. Edit the *`ManageAccessPoints`* registry key is set to ***1***.
  4. Restart the **`Enterprise Access Management Security Services`** service.
- On the client, perform one of the following actions:

  - Correct the **`NymiAgentUrl`** registry key:

    1. Run **regedit.exe** and navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork \Authentication*.
    2. Ensure that the value in the *`NymiAgentUrl`* is correct. The format of the *`NymiAgentUrl`* is ***ws://`agent_server_FQDN`:9120/socket/websocket***
  - Correct the *nbe.toml* file.

    1. Edit the *C:\Nymi\Bluetooth_Enpoint\nbe.toml* file.
    2. Ensure that the *`agent_url`* value is correct. The format of the *`agent_url`* is ***agent_url='ws://`agent_server_FQDN`:9120/socket/websocket'***

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.

Nymi Band Tap Populates Username Field Only

On a user terminal that is configured for RFID-only, when the user taps their authenticated Nymi Band to log into Enterprise SSO, the login screen displays the username but does not fill in the password. When the user performs an authentication task in the MES application, the Enterprise SSO login window does not appear.

The *ssoengine* log file displays the following message:

Try roaming session ? RoamingSessionAllowed: 1; DontUseRoamingSession:1, RoamingSessionOnlyFromRFID: 0; m_bHasWearable: 1 AuthMethod (): RoamingSessionAble:0; RoamingSessionTried: 0; WearableAble: 0; MobileRFID: 0; MobileRFID: 0; MobileRFIDAllowed: 0;

Cause

The `RoamingSessionAllowedForSSO` registry key is not configured or misconfigured on the user terminal.

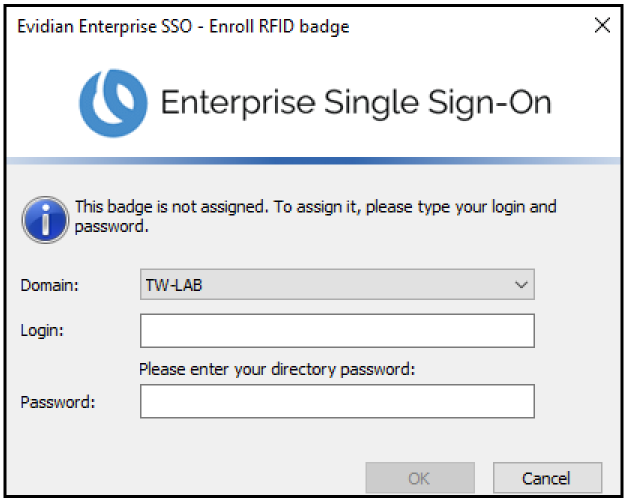
Resolution

Set the `RoamingSessonsAllowedForSSO` registry key to 1 and then restart the Enterprise Access Management Security Service.

This badge is not assigned. To assign it, please type your username and password

This error message appears when you perform a tap on the Evidian software login window.

The following image provides an example of the pop-up window:



Evidian Enterprise SSO - Enroll RFID badge

This badge is not assigned. To assign it, please type your login and password.

Domain: TW-LAB

Login:

Please enter your directory password:

Password:

Figure 7: This badge is not assigned. To assign it please type your username and password

Cause

By default the Evidian software allows users to perform self-enrollments of recognized NFC devices.

This issue can occur for one of the following reasons

- A non-Nymi device comes into close proximity of the NFC reader at a user terminal. The Evidian software detects the device.

Note: When the user provides their username and password and completes the badge assignment, users can tap the same device or a device with the same internal identifier on an NFC reader to complete authentication tasks with the identity of the user that completed the self-enrollment.

- A user taps an authenticated Nymi Band that was enrolled in a different Nymi with Evidian datazone on the NFC reader at a user terminal. The Evidian software detects the Nymi Band.

  Note: When the user provides their username and password and completes the badge assignment, users can use Nymi Band to complete authentication tasks with a Nymi Band tap in both datazones.

- A user performs a Nymi Band enrollment in the Nymi Band Application in the same Nymi with Evidian datazone, but the enrollment did not occur in the Evidian EAM database. For example, when the user performed the Nymi Band enrollment in the Nymi Band Application, but the NES policy was not configured with the **`NES and Evidian`** enrollment destination value.

  Note: When the user provides their username and password and completes the badge assignment, the user can use Nymi Band to complete authentication tasks with their identity.

Resolution

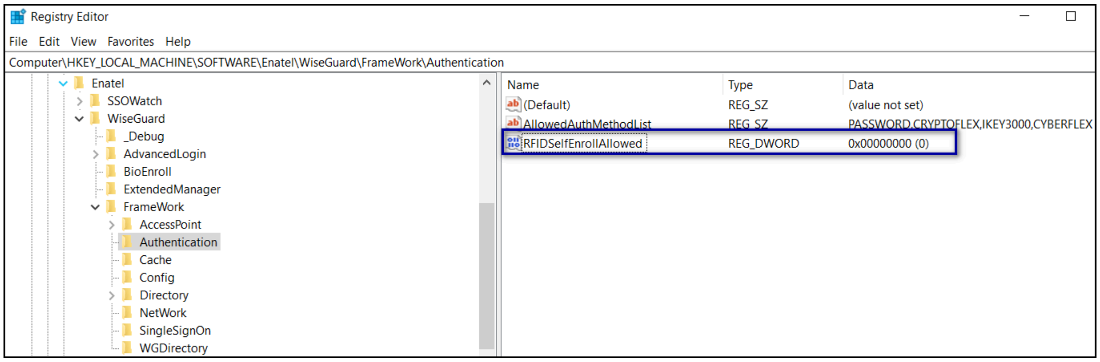
1. Create the following registry key on all user terminals, including all Citrix/RDP servers, to disable the Self Enrollment feature.

   a. Run *regedit.exe*

   b. Navigate to **`HKLM > SOFTWARE > Enatel > WiseGuard > FrameWork`**.

   c. Right-click**`Authentication`**, and then select **`> DWORD (32-bit) value`**.

   d. In the **`Value Name`** field, type ***RFIDSelfEnrollAllowed***. Leave the default **`Data`** value (0).The following figure provides an example of the ***RFIDSelfEnrollAllowed*** key.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowedAuthMethodList	REG_SZ	PASSWORD,CRYPTOFLEX,IKEY3000,CYBERFLEX
RFIDSelfEnrollAllowed	REG_DWORD	0x00000000 (0)

Figure 8: RFIDSelfEnrollAllowed Registry Key

   e. Close `Registry Editor`.Restart the **`Enterprise Access Management Security Service`**.

   f. Restart the **`Enterprise Access Management Security Service`**.

2. Ensure that you configure the NES policy to perform NES and Evidian enrollments.

a. Connect to the NES Administrator Console.
b. Edit the active policy.
c. From the **`Enrollment Destination`** list, select **`NES and Evidian`**.
d. Save the policy.
e. Instruct the user to log into the Nymi Band Application while they wear their authenticated Nymi Band. Nymi Band Application completes the enrollment on the Evidian EAM Controller.

How to Remedy Self Enrollments of Non-Nymi Devices

Determine which users have a non-Nymi device, and remove the non-Nymi device association with the user.

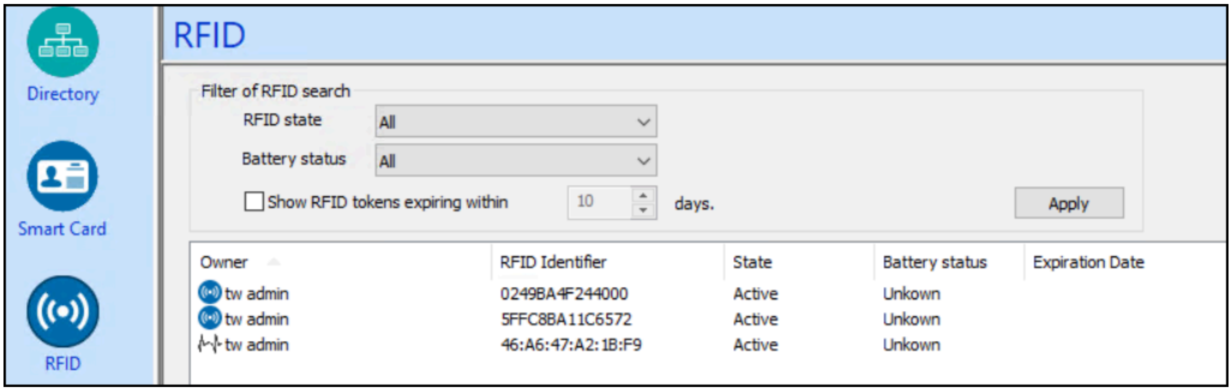
About this task

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

Procedure

1. In the left navigation pane, select **`RFID`**.
2. On the `RFID` window, leave the default settings and then click **`Apply`**.
3. Review the output for users that have 2 or more RFID identifiers that are associated with their account. The following figure shows user *twadmin* that has two RFID identifiers, one for their Nymi Band and one for a non-Nymi device.

   Note: The RFID identifier for a Nymi Band device always starts with the alphanumeric characters **5F**.



RFID

Filter of RFID search

RFID state: All

Battery status: All

☐ Show RFID tokens expiring within 10 days.

Apply

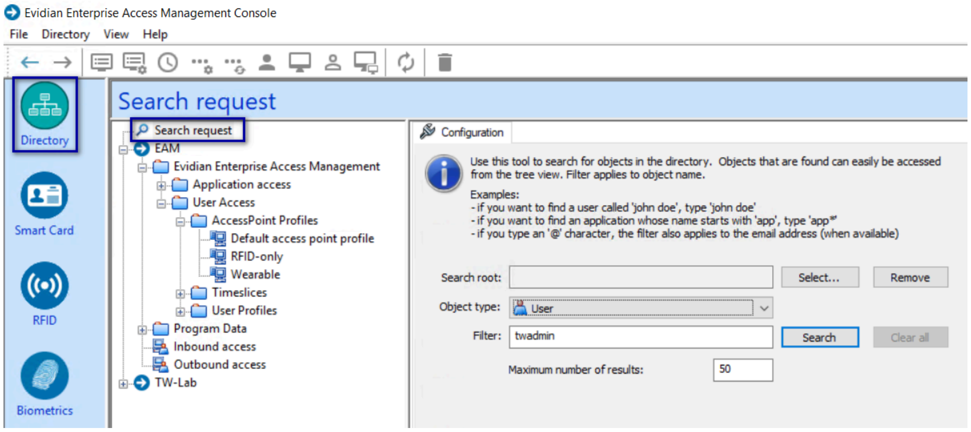
Owner	RFID Identifier	State	Battery status	Expiration Date
tw admin	0249BA4F244000	Active	Unkown	
tw admin	5FFC8BA11C6572	Active	Unkown	
tw admin	46:A6:47:A2:1B:F9	Active	Unkown	

Figure 9: User with multiple RFID devices

In this example, the RFID identifier of the Nymi Band that is assigned to twadmin is *5FFC8BA11C6572* and the RFID identifier for the non-Nymi device is *02498A4F244000*.

4. In the left navigation pane, click **`Directory`**.
5. 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.



Use this tool to search for objects in the directory. Objects that are found can easily be accessed from the tree view. Filter applies to object name.

Examples:
- if you want to find a user called 'john doe', type 'john doe'
- if you want to find an application whose name starts with 'app', type 'app*'
- if you type an '@' character, the filter also applies to the email address (when available)

Search root:

Object type: User

Filter: twadmin

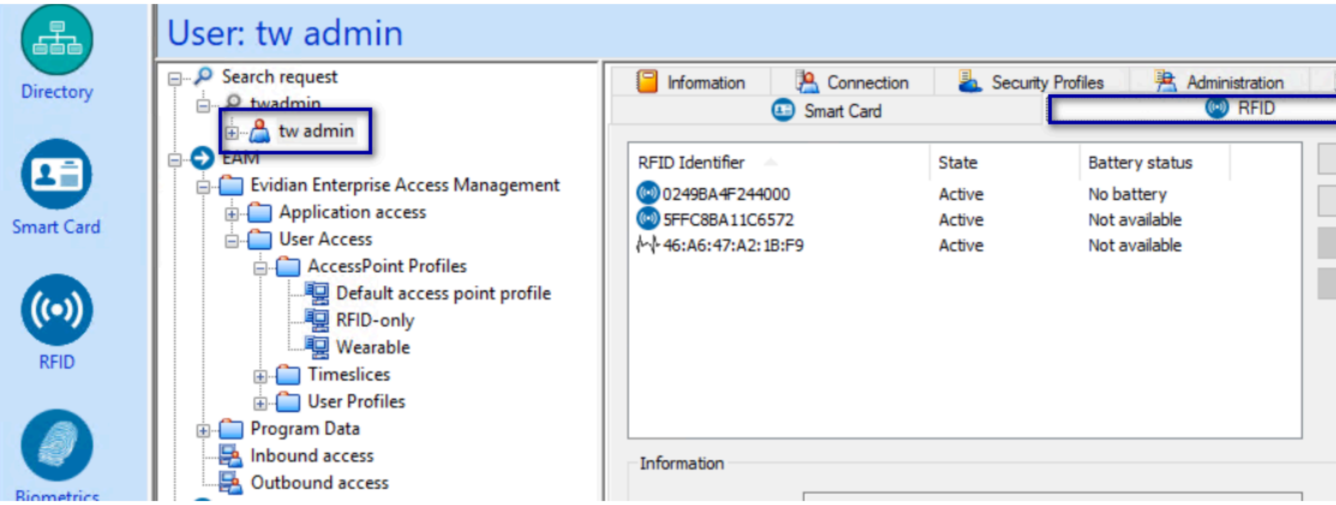
Maximum number of results: 50

Figure 10: Search request window

6. Click **`Search`**.

7. From the search results, select the user, and then in the `User` properties window, select the **`RFID`** tab.

Figure 11: RFID tab for a user

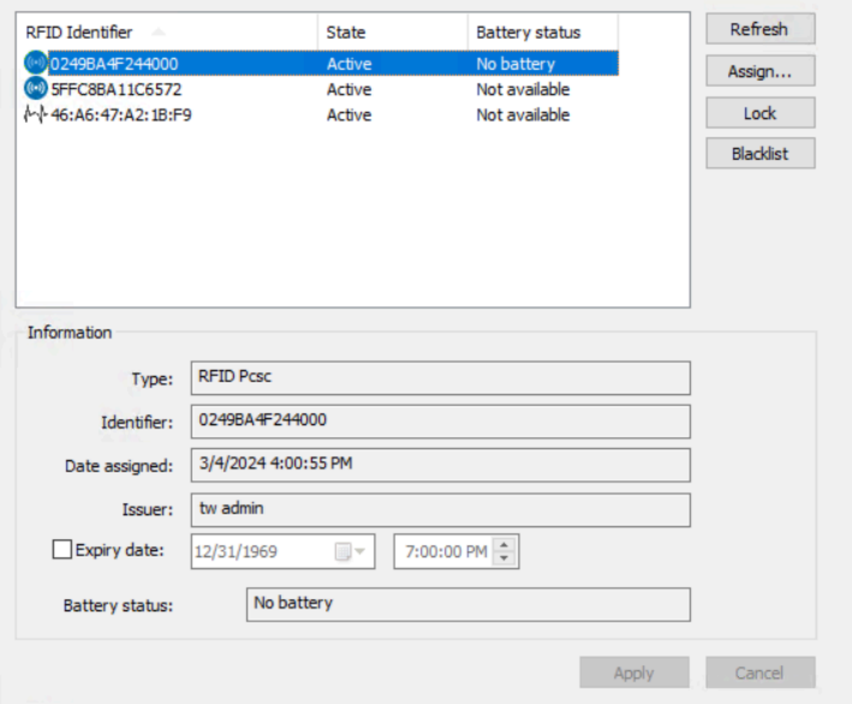


RFID Identifier	State	Battery status
0249BA4F244000	Active	No battery
5FFC8BA11C6572	Active	Not available
46:A6:47:A2:1B:F9	Active	Not available

One or more RFID entries appear for the non-Nymi devices that are assigned to the user, in addition to the RFID and associated wearable entry for the Nymi Band.

8. Select the RFID entry for the non-Nymi device, and then click **`Blacklist`**.

The following figure highlights the non-Nymi device that is assigned to the user.



RFID Identifier	State	Battery status
0249BA4F244000	Active	No battery
5FFC8BA11C6572	Active	Not available
46:A6:47:A2:1B:F9	Active	Not available

Type: RFID Pcsc

Identifier: 0249BA4F244000

Date assigned: 3/4/2024 4:00:55 PM

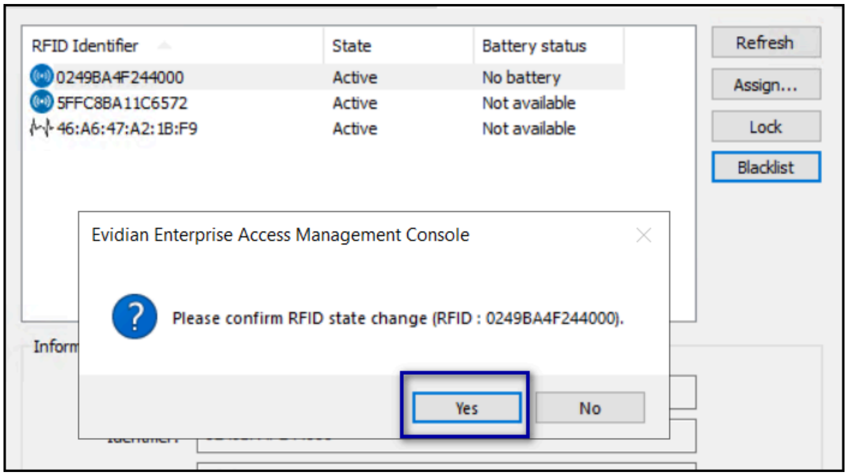
Issuer: tw admin

☐ Expiry date: 12/31/1969 7:00:00 PM

Battery status: No battery

Figure 12: Devices assigned to the user

9. On the `Please confirm RFID state change` window, click **`OK`**, as shown in the following figue.



RFID Identifier	State	Battery status
0249BA4F244000	Active	No battery
5FFC8BA11C6572	Active	Not available
46:A6:47:A2:1B:F9	Active	Not available

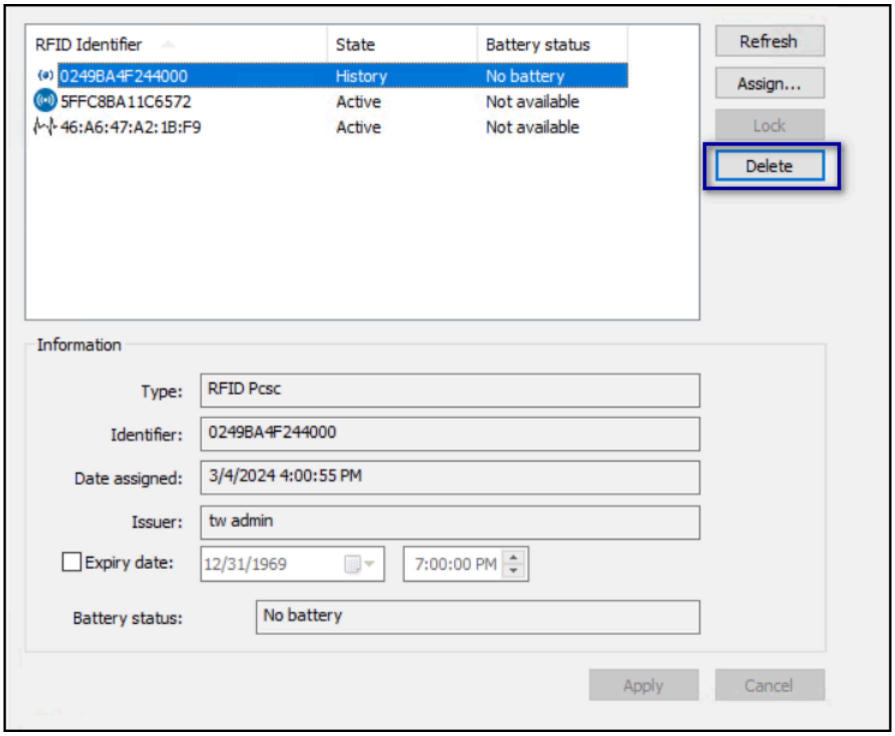
Evidian Enterprise Access Management Console

Please confirm RFID state change (RFID : 0249BA4F244000).

Figure 13: RFID State Change prompt

The state of the non-Nymi device changes to *History*.

10. Select the entry for the non-Nymi device, and then click **`Delete`**, as shown in the following figure.



RFID Identifier	State	Battery status
0249BA4F244000	History	No battery
5FFC8BA11C6572	Active	Not available
46:A6:47:A2:1B:F9	Active	Not available

Information

Type:	RFID Pcsc
Identifier:	0249BA4F244000
Date assigned:	3/4/2024 4:00:55 PM
Issuer:	tw admin
□ Expiry date:	12/31/1969 7:00:00 PM
Battery status:	No battery

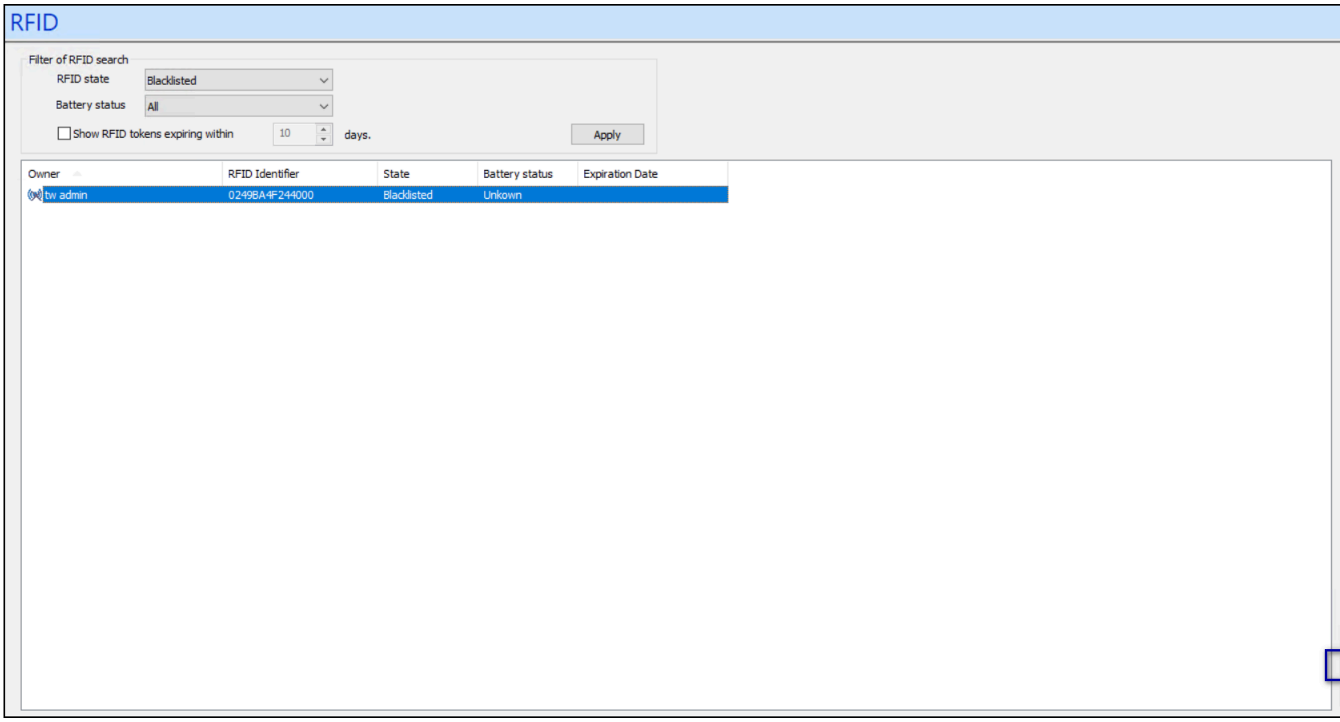
Figure 14: Delete Non-Nymi Device

11. On the `Please confirm RFID state change` window, click **`OK`**.

12. In the left navigation pane, select **`RFID`**.

13. From the **`RFID state`** list, select **`Blacklisted`**, and then click **`Apply`**.
The window displays the deleted non-Nymi device.

14. Select the non-Nymi device, and then click **`Blacklist`** as shown in the following figure.



RFID

Filter of RFID search

RFID state: Blacklisted

Battery status: All

□ Show RFID tokens expiring within 10 days.

Owner	RFID Identifier	State	Battery status	Expiration Date
tw admin	0249BA4F244000	Blacklisted	Unkown	

Figure 15: Blacklist Non-Nymi Device

15. On the `Please confirm RFID state change` window, click **`OK`**.

Nymi Band Tap Fails with error 0x82002081

When a user performs a Nymi Band tap on the `Enterprise SSO Login` window, the error 0x82002081 appears.

Cause

The user account is a member of too many Active Directory groups and the Local Security Authority(LSA) cannot generate the token that NES requires to allow the login to complete.

Resolution

Reduce the group membership for the user account to 1009 or less. Refer to Microsoft for more information.

Authentication error, invalid directory account, initialize using collect mode

This error appears on a user terminal that is in a wearable configuration, when the user taps their authenticated Nymi Band to log into Enterprise SSO. Before this error appears, the login screen displays the username but does not fill in the password.

Cause

Changes were made to the user terminal that require the reinitialization of Enterprise SSO.

Resolution

1. On the `Enterprise SSO` window, log in with your username and password.
2. In the System Tray, right click the Enterprise SSO icon and then select **`Stop`**.
3. From the start menu search for and select **`Enterprise SSO`**.
4. On the `Enterprise SSO` window, perform a Nymi Band tap.

Nymi Band Taps Populate the Username in the Evidian SSO window only

When performing a Nymi Band tap when the SSO login window appears, the action populates the username field but not the password field, and the tap does not complete. When the user types the password, and then click OK, they are prompted to specify their old password.

Cause

The user changed their Active Directory password on a computer that does not have the Evidian client software installed.

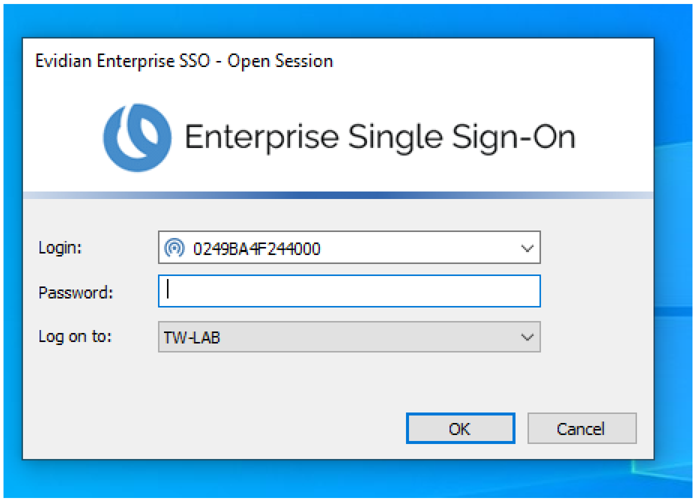
Resolution

Instruct users to change their Active Directory password from a computer with the Evidian client software installed, to ensure that the Evidian software infrastructure is aware of the change.

Nymi Band Taps Populate the Username in the Evidian Window With a Device Identifier

When performing a Nymi Band tap on an Evidian window, the action populates the username field with an identifier, and the tap does not complete.

The following figure provides an example of an Evidian window with a device identifier in the username field.



Evidian Enterprise SSO - Open Session

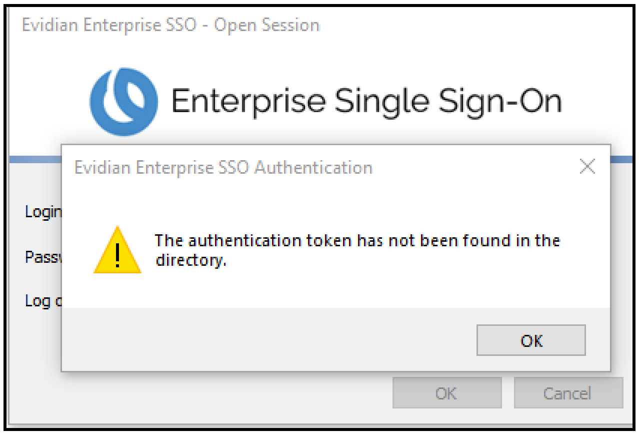
Enterprise Single Sign-On

Login: 0249BA4F244000

Password:

Log on to: TW-LAB

If the user types their password in the **`Password`** field, and then click **`OK`**, the login fails with the following error: *The authentication token has not been found in the directory*.



Evidian Enterprise SSO - Open Session

Enterprise Single Sign-On

Evidian Enterprise SSO Authentication

The authentication token has not been found in the directory.

Cause

This issue appears for the following reasons:

- A non-Nymi device was in close proximity of the NFC reader at the time of the Nymi Band tap. The Evidian software detected the non-Nymi device and not the Nymi Band.
- A user taps a Nymi Band that is not enrolled in the Evidian EAM Controller.

Note: This issue appears when you disable the Evidian self enrollment feature. See *This badge is not assigned. To assign it, please type your username and password* for the behaviour that appears you enable the self-enrollment feature and a user taps a non-Nymi device or a Nymi Band that is not enrolled in the Evidian EAM Controller.

Resolution

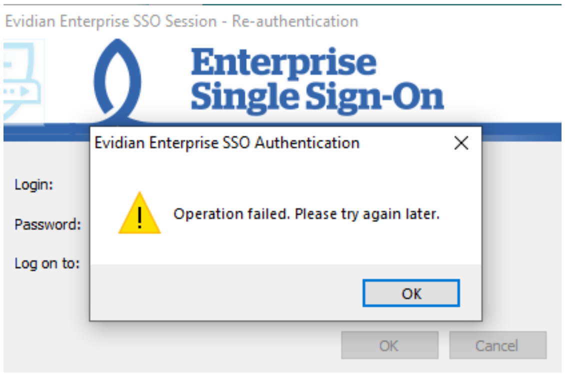
To resolve this issue, perform the following actions:

1. Move any non-Nymi device away from the NFC reader.
2. Perform a Nymi Band tap.

Operation Failed. Please try again later

This error message appears when you perform a tap to perform an SSO action.

The following image provides an example of the error message.



Evidian Enterprise SSO Session - Re-authentication
Enterprise Single Sign-On
Login:
Password:
Log on to:
OK
Cancel
Evidian Enterprise SSO Authentication
OK

Operation failed. Please try again later.

Figure 16: Operation Failed. Please try again later

Cause

The initialization of the *nymi_api.dll* and retrieval of authentication token from Nymi AgentNES is taking longer than expected and does not complete within the default time period.

Resolution

To resolve this issue, install the latest supported version of EAM 10.02 PL2 or EAM 10.01.7125.10 and then define the following registry key on each machine that runs the MES application.

1. Run *regedit.exe*.
2. Navigate to *HKLM\Software\Enatel\Wiseguard\FrameWork\Authentication\*.

3. Create a new DWORD (32 bit value) registry key named *WearableDelay* with a value set to more than ***2000*** ms. Nymi recommends a value of 10000.

Your badge must be initialized with a PIN. Please type your password and then choose a pin for your badge

This error message appears when you attempt to tap to unlock the user terminal with an authenticated Nymi Band.

Cause

Misconfigured TokenManagerStructure file.

Resolution

Correct the TokenManagerStructure configuration on the Evidian EAM Controller or replace the *TokenManagerStructure.xml* on the terminal, and then delete the Evidian cache files.

Slow Authentication with Nymi Band Tap

This problem appears when you use a Nymi Band in a Nymi-Evidian integration and you use the Evidian EAM Controller to manage password changes.

Cause

When the Evidian EAM Controller manages the password changes and the environment includes a distributed Active Directory configuration, Evidian uses the `LsaLogonUser` function to determine the Active Directory Domain Controller(DC) name, and then uses the DC that is closest to the access point for a user to manage password changes. Due to an issue with the `LsaLogonUser` function, the process takes longer than expected.

Resolution

Manage password changes outside of the Evidian EAM Controller and configure the Evidian EAM Client to avoid the use of the `LsaLogonUser` function.

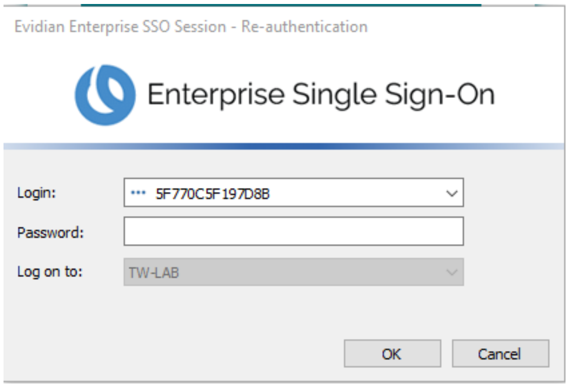
To disable the `LsaLogonUser` function, perform the following actions on each Evidian EAM Client:

1. Run **regedit.exe**, and navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\Framework \Directory*
2. Create a new DWord (32bit) key named **CallLsaLogonUserAfterLogon**.
3. Edit the key, and in the value field, type ***0***.
4. Close *regedit.exe*.
5. Restart the Evidian EAM Client.

Nymi Band tap displays the NFC UID in the Enterprise SSO window in the Login field

When a user performs Nymi Band tap, NFC UID of the Nymi Band appears in the **`Login`** field instead of the username. The SSO authentication never completes, and you cannot change the value in the **`Login`** field.

The following image provides an example of this issue.



Evidian Enterprise SSO Session - Re-authentication

Enterprise Single Sign-On

Login: 5F770C5F197D8B

Password:

Log on to: TW-LAB

Figure 17: eSSO window displays the NFC UID of the Nymi Band

Cause

The Nymi Band that is associated with the user has been blacklisted in Evidian.

Resolution

Delete the Nymi Band entries for the user in Evidian and NES, perform a Delete User Data operation on the Nymi Band, and then repeat the enrollment.

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**.

SSO Engine icon does not appear in the system tray

SSO Engine ☑ icon does not appear in the system tray.

Cause

The SSO Engine 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, reboot the computer.

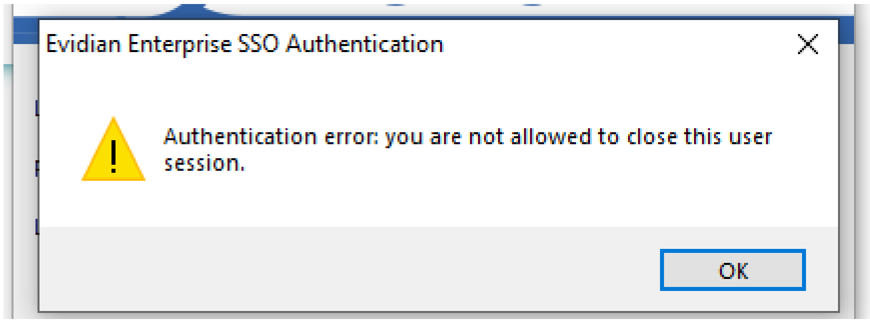
If you cannot reboot the computer, perform the following actions

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.



Evidian Enterprise SSO Authentication

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

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.

Evidian Access Management Security Services service is running but there is no communication

This issue appears after you start `Manage Wearable Devices`.

Cause

This problem typically occurs when the Evidian EAM Client cannot communicate with the Evidian EAM Controller, for one of the following reasons:

- Poor network connection between the Evidian EAM Client and Evidian EAM Controller
- 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. Stop the *Enterprise Access Management Security Services* service.

2. Right-click the *WGSRVConfig.exe* file, which is in the EAM Install package in the *..\EAM-v10.X\EAM.x64\TOOLS\* folder, and then select **`Run as administrator`**.
3. On the `Administration Tools`, select **`Configure security settings`**
4. Change the Directory and Access point account to the new login and password.
5. Start the *Enterprise Access Management Security Services* service.

Enterprise SSO Login window does not appear when performing an e-signature in a Java-based MES application.

The `Enterprise SSO Login` window appears for actions that are not in the Java-based MES application, for example, SSO startup.

Cause 1

The required version of Visual C++ is not installed on the Evidian EAM Client computer.

Resolution 1

To resolve this issue, Install the Visual C++ Redistributable package on the machine that runs the MES application. You can get the required installation file from the EAM installation package in the *..\EAM\Install* directory.

Cause 2

Evidian Java plugin is not enabled or a newer version of JRE was installed after the installation of Evidian Java plugin Evidian EAM Client.

Resolution 2

Install the Java plugin on the Evidian EAM Client by typing the following command:

C:\Program Files\Evidian\Enterprise Access Management>ssojsecfg/install path_to_jre

where *path_to_jre* is the directory location of the Java Runtime Environment (JRE) application.

Nymi Band Tap Fails Because PAS-X Username is Case Sensitive

When a user launches PAS-X and performs a Nymi Band tap on the Evidian Enterprise SSO log in, the Evidian Enterprise SSO application populates the username in the format that appears in Active Directory(AD). PAS-X requires the username in a particular format, for example in all capital letters, and the tap to complete the authentication does not complete successfully.

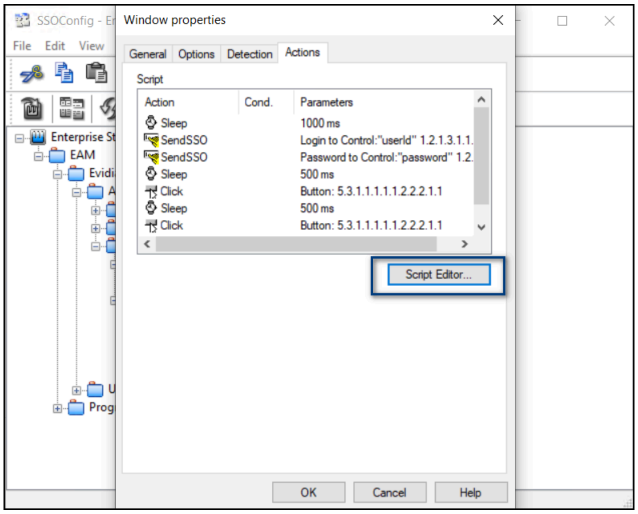
Cause

PAS-X usernames are case sensitive and the format of the username that Evidian Enterprise SSO receives from AD is not the format that PAS-X requires.

Resolution

Perform the following step to edit the properties of a window in the Technical Definition to automatically convert the username into the format that PAS-X requires.

1. From an Evidian EAM Client computer, start `Enterprise SSO Studio`(*ssobuilder.exe*), and log in with an EAM administrator account.
2. Expand **`Enterprise Studio Configuration > EAM > Evidian Enterprise Access Management > Application access > Technical definitions`**.
3. Expand your technical definition, and then right-click on the affected window and select **`Properties`**.
4. On the **`Actions`** tab, click **`Script Editor`**, as shown in the following figure.



Action	Cond.	Parameters
Sleep		1000 ms
SendSSO		Login to Control:"userId" 1.2.1.3.1.1.
SendSSO		Password to Control:"password" 1.2.
Sleep		500 ms
Click		Button: 5.3.1.1.1.1.1.2.2.2.1.1
Sleep		500 ms
Click		Button: 5.3.1.1.1.1.1.2.2.2.1.1

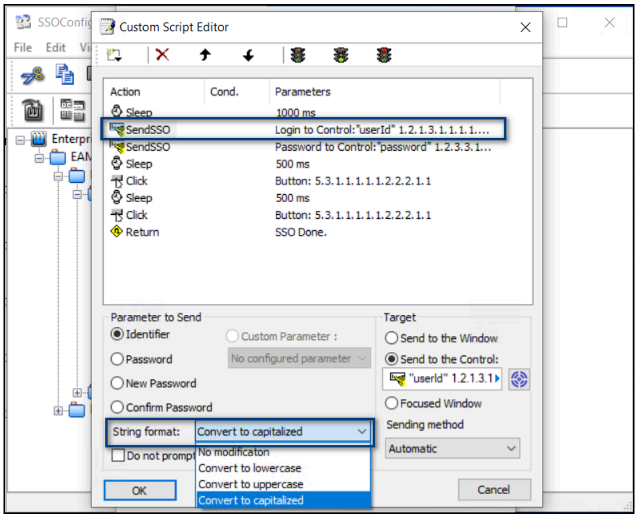
Figure 18: Script Editor option

5. On the `Custom Script Editor` window, select the **SendSSO** option with the parameter **`Login to Control`**.
6. In the `Parameter to Send` section that appears, from the **`String format`** list, select one of the following options:

   - Convert to lowercase—To populate the value in the Username field in all lowercase letters.
   - Convert to uppercase—To populate the value in the Username field in all uppercase letters.

- Convert to capitalized—To populate the value in the Username field with first letter capitalization.

  The following figure provides an example of the `Custom Script Editor` window.



Action	Cond.	Parameters
Sleep		1000 ms
SendSSO		Login to Control:"userId" 1.2.1.3.1.1.1.1....
SendSSO		Password to Control:"password" 1.2.3.3.1...
Sleep		500 ms
Click		Button: 5.3.1.1.1.1.1.2.2.2.1.1
Sleep		500 ms
Click		Button: 5.3.1.1.1.1.1.2.2.2.1.1
Return		SSO Done.

Parameter to Send
● Identifier
○ Custom Parameter :
No configured parameter
○ Password
○ New Password
○ Confirm Password
String format: Convert to capitalized
□ Do not prompt
No modificaton
Convert to lowercase
Convert to uppercase
Convert to capitalized

Target
○ Send to the Window
● Send to the Control:
"userId" 1.2.1.3.1
○ Focused Window
Sending method
Automatic

Figure 19: Custom Script Editor window

- Click **OK**.

7. On the `Window Properties` window, click **OK**.
8. From the `Toolbar`, click **`Save changes`**.

Object not found

This error message appears when a user performs an NFC tap with their Nymi Band, for example, to log into Evidian SSO.

Object not Found is a generic error, and requires log file investigation for additional error messages to narrow down the specific reason for the failure.

Note: Ensure that the Evidian software is in debug mode. *Enabling Debug Mode in Evidian* provides more information.

To narrow down a cause, review the Evidian log files for additional error messages that appear before the *Object not found* error.

For example, review the WGSS(nymi) log file and search for the error code 0x81010009. This is the error code that is associated with *Object Not Found* error.

Review the error messages that appear before the 0x81010009 error.

Cause

Potential causes include:

- The user terminal cannot establish a connection to the NES server due to network issues.
- The BLE adapter is not plugged into the user terminal at the time the Nymi Band tap is performed on an NFC reader.
- SPNs are not correctly configured in the environment for NES.
- The NEA certificates have expired on the user terminal and the user terminal cannot retrieve NEA certificates from the NES server.

  In the sample log output below, we can see that the message *WearableExtension.cpp :0440: Ext::GetListOfVisibleDevices returns: 0x8101201c* appears before the *Object not Found* error.

```
                704:(22/03/17 06:13:14.149):CHttpClient.cpp :0402: -> CHttpClient::GetHttpStatus
                704:(22/03/17 06:13:14.149):CHttpClient.cpp :0411: <- CHttpClient::GetHttpStatus
                704:(22/03/17 06:13:14.149):NesClient.cpp :0114: Error from token request--code: 0 - message: 'The
operation is complete"
                '
                704:(22/03/17 06:13:14.149):NesClient.cpp :0122: <- nymi::NesClient::AuthenticateWithToken
                704:(22/03/17 06:13:14.149):Listener.cpp :0411: Unable to get token with USER creds
                5bc:(22/04/04 13:31:31.469):WearableExtension.cpp :0440: Ext::GetListOfVisibleDevices returns:
0x8101201c
                5bc:(22/04/04 13:31:31.469):WearableExtension.cpp :0441: 0 visible devices
                5bc:(22/04/04 13:31:31.469):AutoChrono.cpp :0029: [TIME] Wearable::FreeListOfDevices() : 0 ms
                5bc:(22/04/04 13:31:31.469):WearableExtension.cpp :0495: <-
CWearableExtension::ValidateProvisions returned: 0x81010009
                5bc:(22/04/04 13:31:31.469):AutoLock.cpp :0178: CS Unlock(WEProtectDll)
                5bc:(22/04/04 13:31:31.469):WearableContext.cpp :0460: <-
CWearableContext::ConnectUserWearableDevice returned: 0x81010009
```

The `Evidian Errors and Events application` provides the following error message for the 0x8101201c error code: *FMK_E_SECURITY_CERTIFICATECHAINNOTTRUSTED*

Inspection of the *C:\Windows\System32\config\systemprofile\AppData\Roaming\Nymi\NSL\string\ksp* directory shows that there are only the 8 locally-generated certificate files.

The *nymi_api.log* file displays the following errors:

```
                WARN - Verifying NEA certs without an NES connection. Some checks will be skipped.
                ERROR - NSL: nsl_verify_nea_cert_chain, 2227, 5
                ERROR - Error: ErrorWithMessage { error: MissingCerts, specifics: "Missing NES connection
parameters. Please call `init` with additional fields \'nes_url\' and \'token\'" }
                INFO - sending update to nea {"operation":"init","exchange":"30809","status":8000,"payload":
{},"error":{"error_description":"NEA missing certificates.","error_specifics":"Missing NES connection parameters.
Please call `init` with additional fields 'nes_url' and 'token'"}}
```

The user terminal cannot retrieve the NEA certificates from the NES server over port 443 (by default). NEA certificates are used to secure communications between the Nymi Band and the BLE adapter. The NEA certificates are a combination of 8 locally-generated certificates files and 12 NES-generated certificate files. By default, the NEA certificates on a user terminal expire every 14 or 90 days by default, depending on the Connected Worker Platform(CWP) version. When the certificates expire, the user terminal initiates a request to retrieve certificates from the NES server when the Evidian Enterprise Access Management Security Service restarts or when an action occurs that requires certificates.

Resolution

Perform the following sequence of actions to determine the cause of the communication issue:

- Review the IIS log file in the *C:\inetpub\logs* directory on the IIS server that hosts the NES instance to confirm that communication between the user terminal and NES server occurs over http/https.
- Confirm that user terminal can successfully request authentication by token with the NES server.
- Review *Troubleshooting Basic Connectivity Issues* to confirm that the client can communicate with the NES server.
- Inspect firewall logs to confirm that bi-directional communication occurs between the client and server over http/https.
- Ensure that the BLE adapter is inserted into a USB port on the user terminal. If the adapter is in the USB port, reseat the adapter in the port, or try a different port.
- Review the article *Troubleshooting SPN Issues*.

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