Administration Guide

Nymi with Evidian Solution
v1.0
2025-08-07

Contents

3 - Preface

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

Purpose

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

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

Audience

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

Revision history

The following table outlines the revision history for this document.

Table 1: Revision history

Version	Date	Revision history
1.0	August 7, 2025	First release of this document to separate Nymi with Evidian Solution administration content from deployment content.

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.
- **Connected Worker Platform with Evidian Installation and Configuration Guide**

  The Nymi with Evidian Solution—Deployment Guide provides information about how to deploy the Nymi with Evidian solution components.
- **Nymi Connected Worker Platform with Evidian Troubleshooting Guide**

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

How to get product help

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

How to provide documentation feedback

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

4 - Using the Solution

This section provides information about administrative tasks that are related to the Nymi Band and the tasks that you perform after you deploy the Nymi with Evidian Solution, including backups and recoveries and the steps you must perform when you add new users, user terminals, and enrollment terminals to the solution.

4.1 - Train Evidian Enterprise SSO for the Application

To complete authentication tasks in an application with a NB tap, you must train Evidian Enterprise SSO to correctly detect and interpret the UI controls within the application.

This section provides information about how to configure Evidian single sign-on support for authentication applications.

Note: Before you perform the steps in this section, install the application on the enrollment terminal according to the instructions provided by the Application Vendor. After you complete the SSO configuration steps, you can uninstall the authentication application.

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

4.1.1 - Adding an SSO definition for a new target application

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

About this task

Perform the following steps from the enrollment terminal.

Note: For a web application, SSO detects the application based on the windows process that runs the application. If you run the application with more than one browser, create a new technical definition for each supported browser that will start the application, for example, Chrome, Microsoft Internet Explorer, Firefox, Opera etc.

Procedure

1. Log in as a user that is a EAM administrator.

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

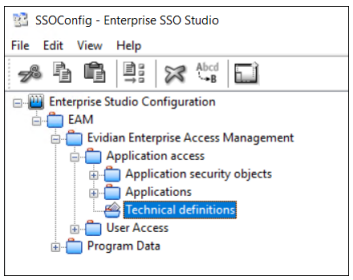


Figure 1: Technical Definition object

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

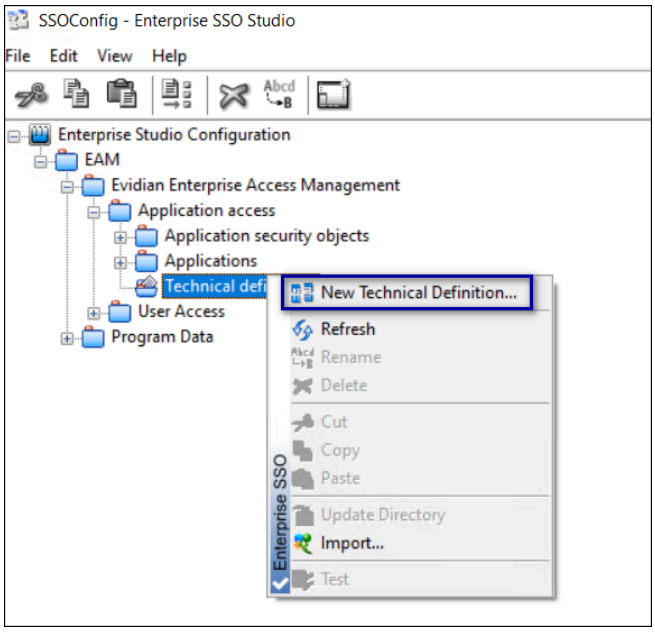
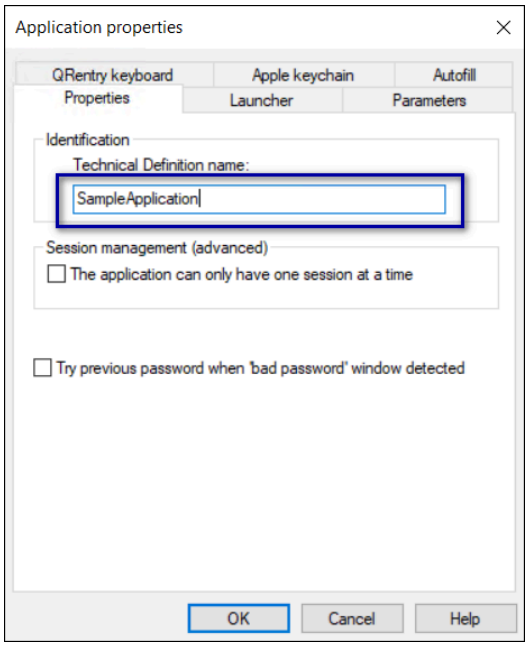


Figure 2: Creating a New Technical Definition

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

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



7. Right-click on the newly created technical definition, and then select **`New Window`**, as shown in the following figure.

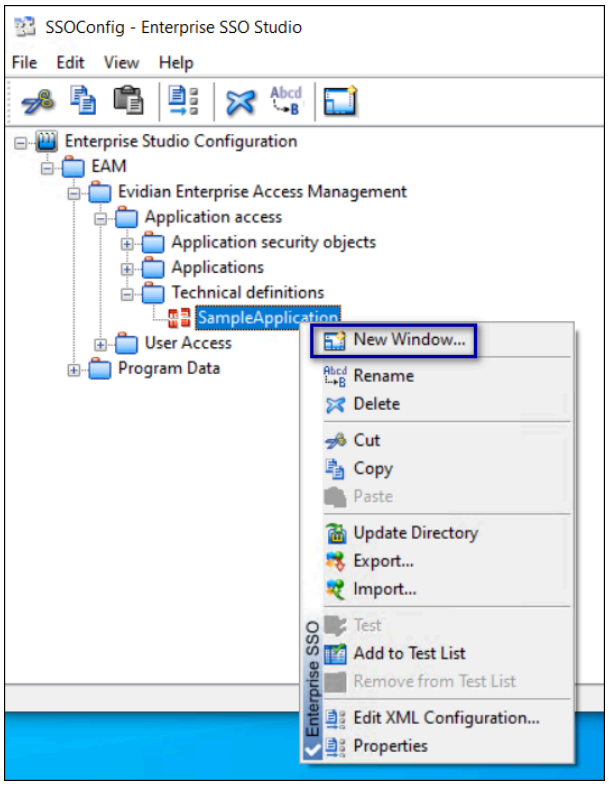


Figure 3: Creating a New Window for the Technical Definition

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.

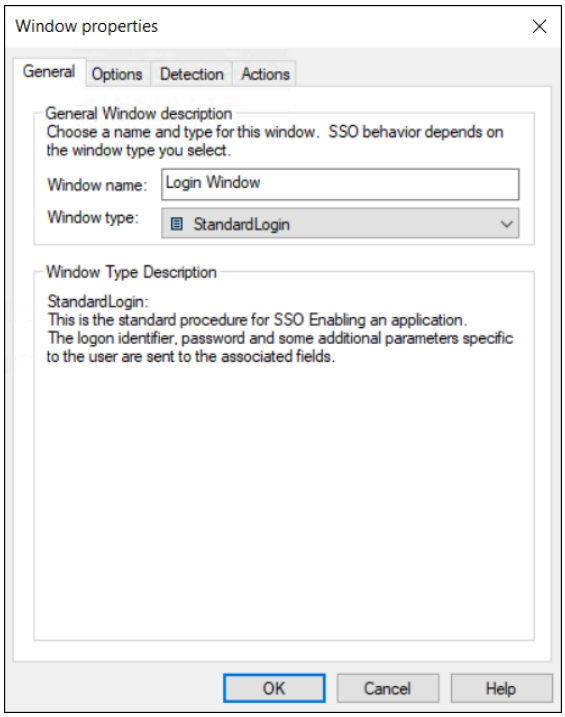


Figure 4: Naming the New Technical Definition Window

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

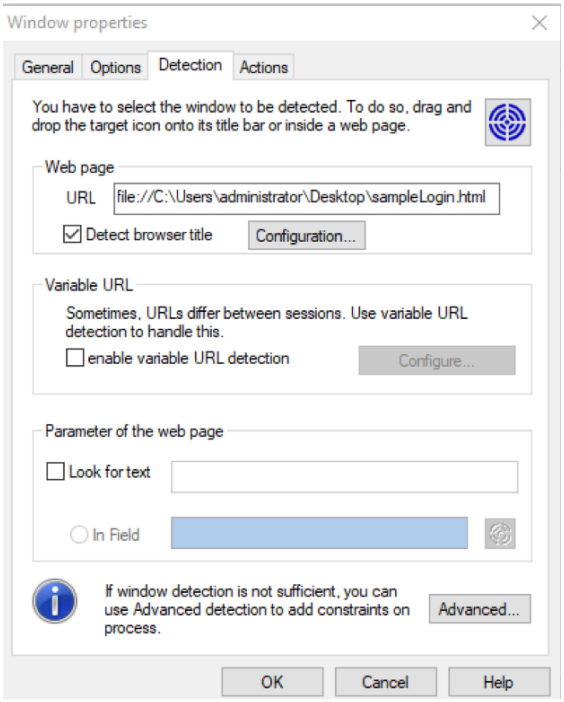


Figure 5: New Technical Definition Detection window

The URL for the webpage appears in the **URL** field.

11. In the **Actions** Tab, perform the following actions:
    a) Click and drag the target icon beside the **Identifier** field onto the **Username** entry field of the application.
    b) Click and drag the target icon beside the **Password** field onto the **Password** entry field of the application.

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

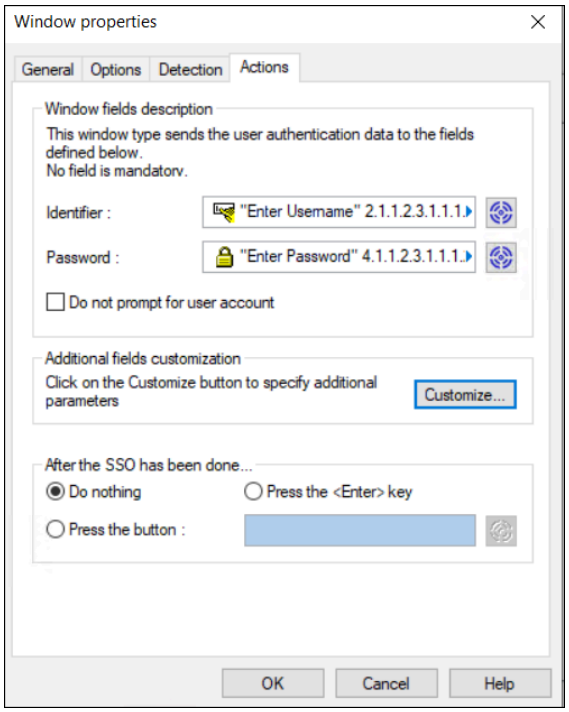


Figure 6: New Technical Definition Actions tab

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

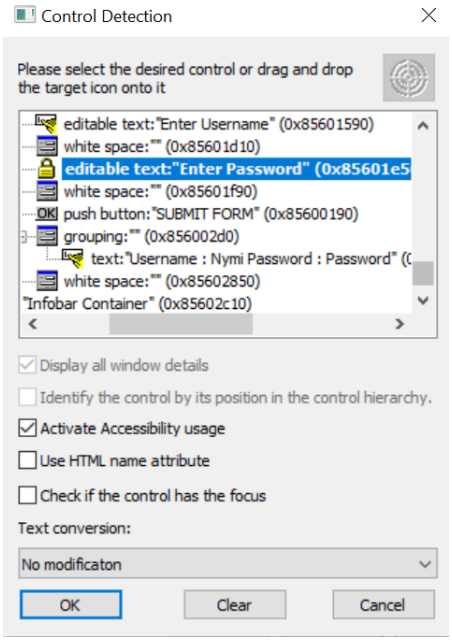


Figure 7: Detection window

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. Optional, for MES applications that require 2 different users to perform an e-signature to complete a task, perform the following actions:
    a) Right-click on the form that requires the sign-offs and then select **`Properties`**, as shown in the following figure.

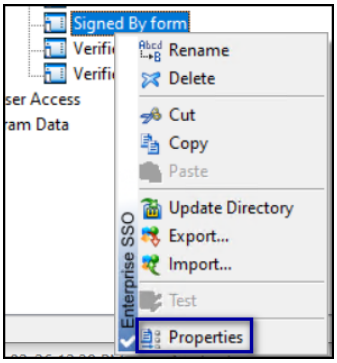


Figure 8: Properties

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

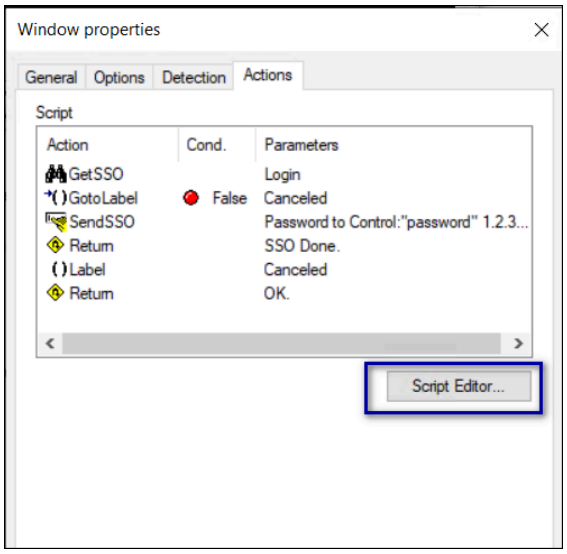


Figure 9: Script Editor option

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

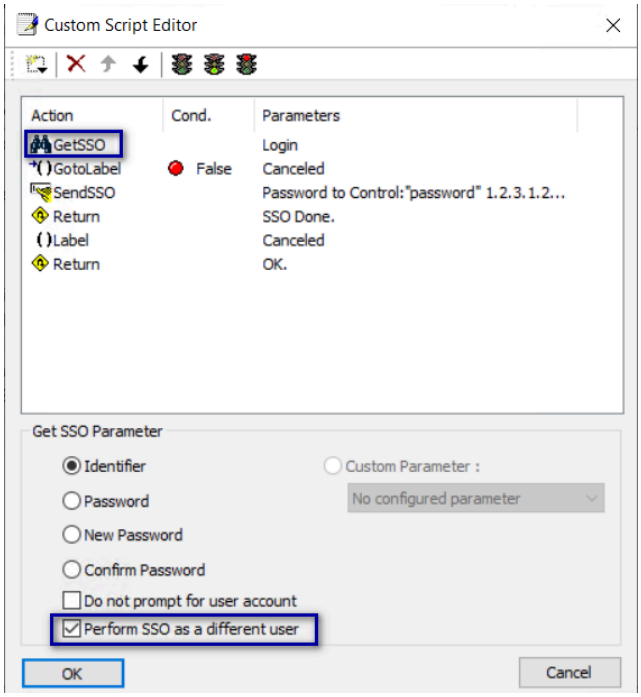


Figure 10: Custom Script Editor window

d) Click **`OK`**.

e) On the `Window properties` window, click **`OK`**.

15. Right-click the newly created technical definition and click **`Update Directory`**, as shown in the following figure.

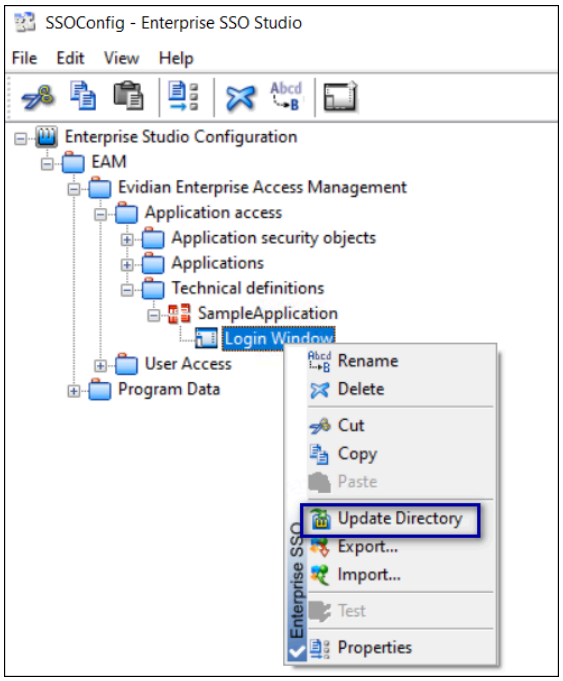


Figure 11: Update Directory with New Technical Definition

16. Close `SSO Builder`.

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

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

About this task

Procedure

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

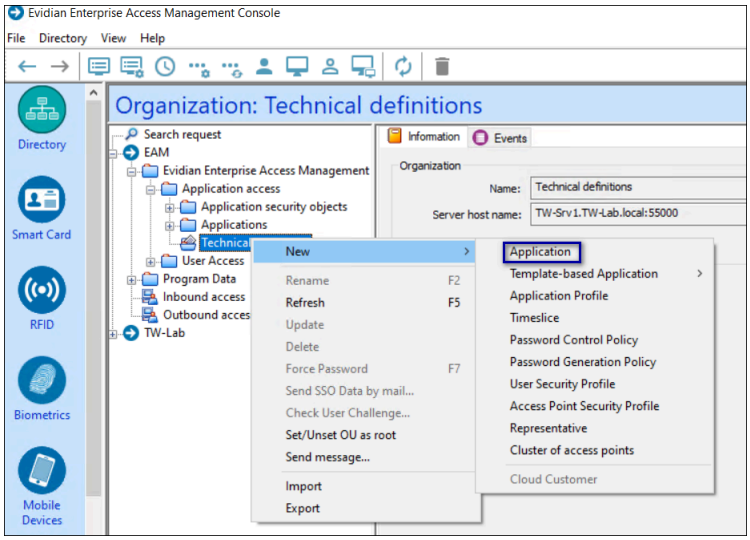


Figure 12: New Application menu option

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

   The following figure provides an example of a new application.

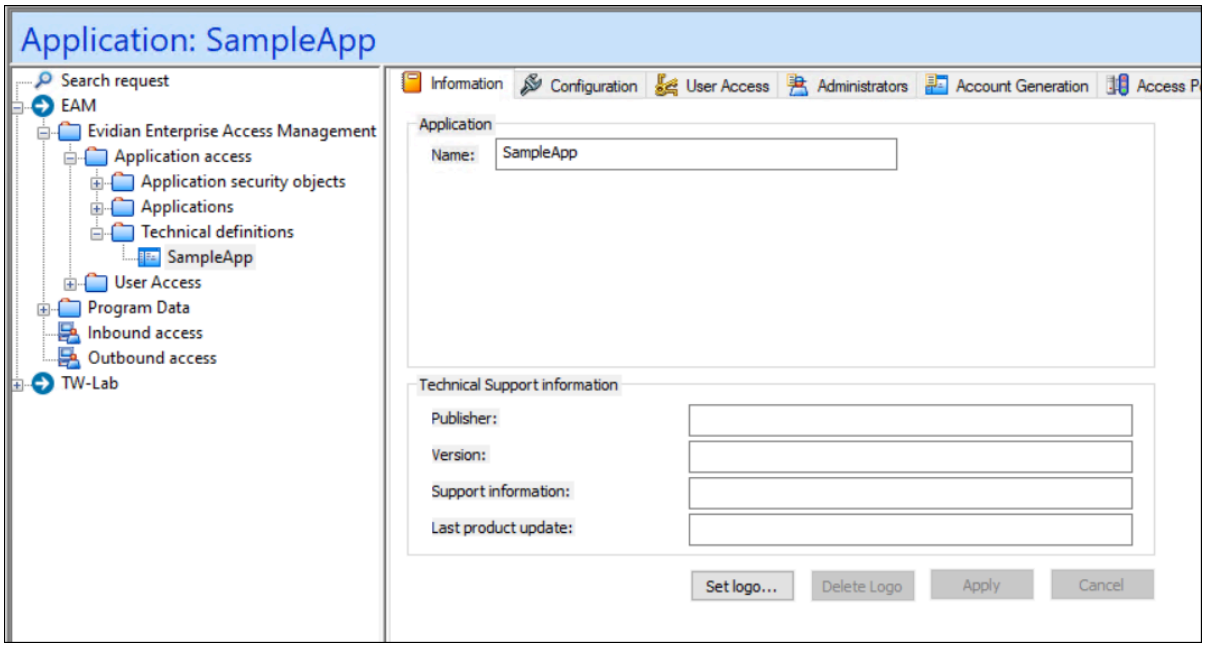


Figure 13: New Application Name

6. If the application uses the credentials of the logged in AD user, perform the following steps:

   a) In the Evidian EAM Management Console, navigate to the technical definition and in the **`Configuration`** tab, select the **`Account Base`** tab.

   b) Select the **`The application uses the primary account`** option.

   c) In the **`Login format`** list, select the login format of the AD credentials.

   d) Click **`Apply`**.

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

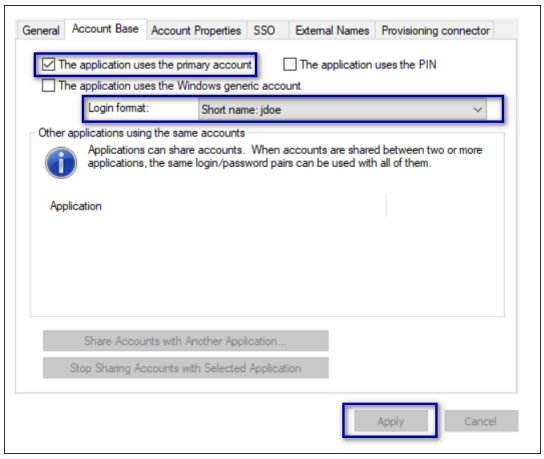


Figure 14: Account Base window

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

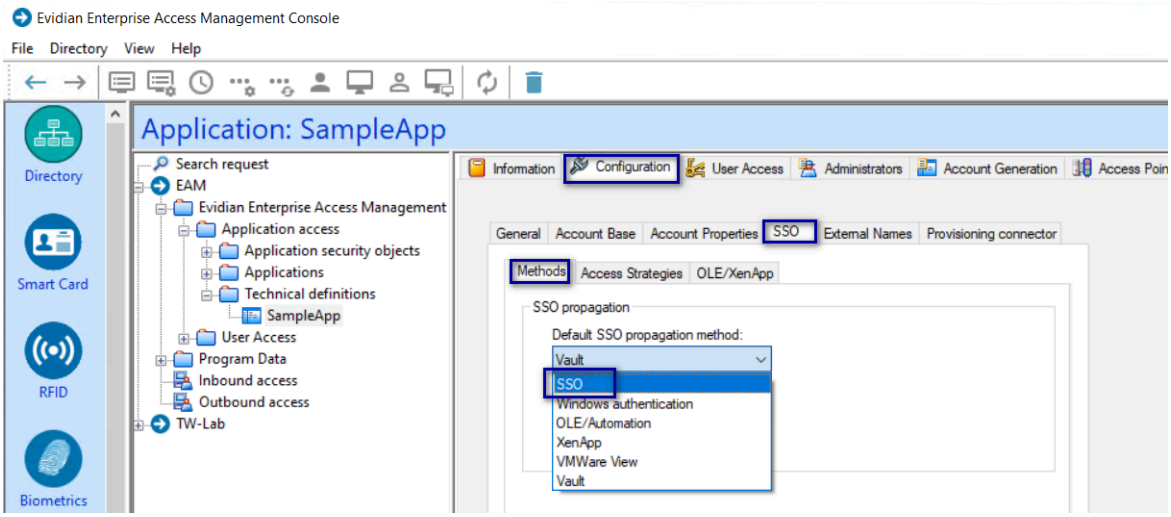
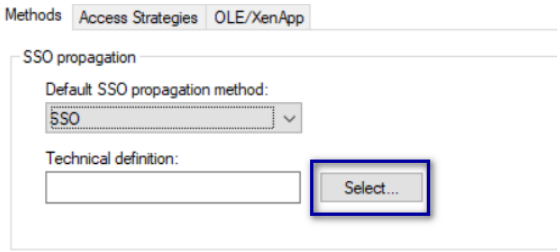


Figure 15: Selecting Default SSO Propagation Method

8. Beside the **`Technical definition`** field, click **`Select`**, as shown in the following figure.

Figure 16: Select button



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.

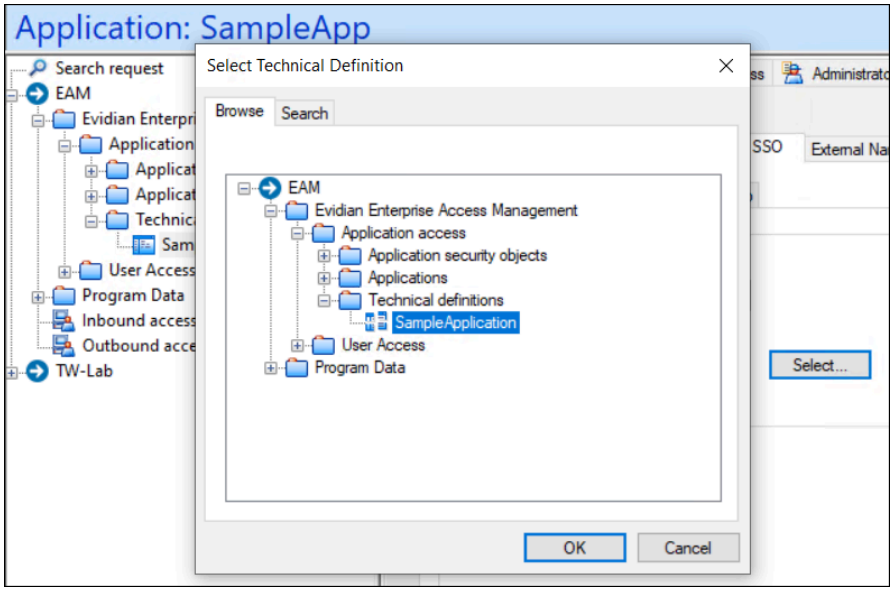


Figure 17: Selecting the Technical Definition

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`**. Select **`User must re-authenticate to perform SSO`**, as shown in the following figure, and then click **`Apply`**.

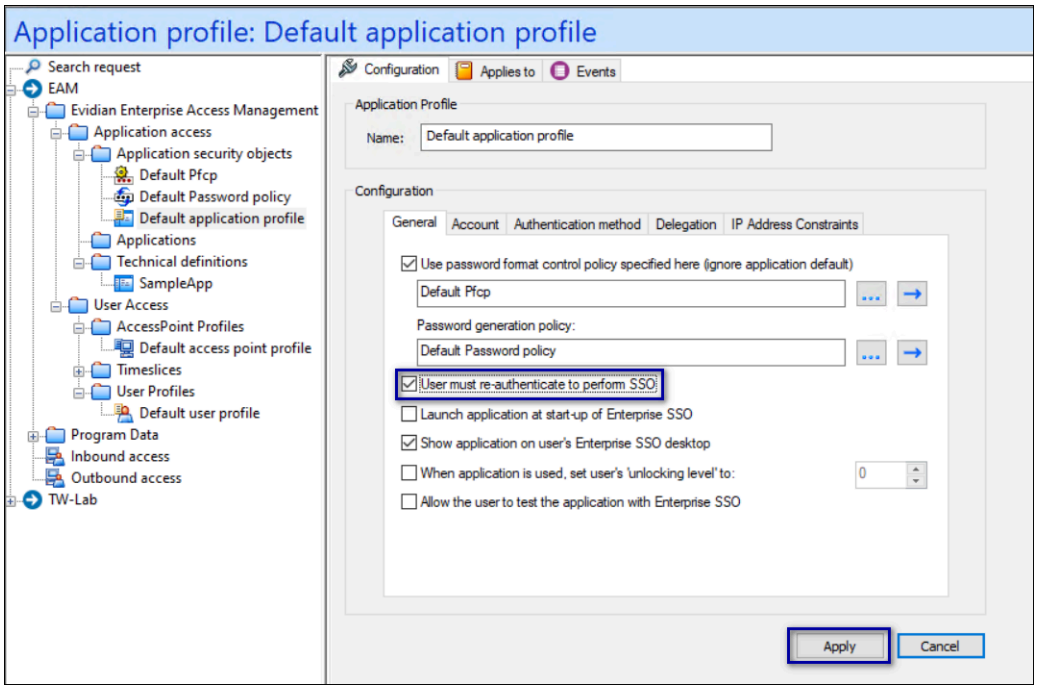


Figure 18: User must re-authenticate to perform SSO

13. Close the Evidian EAM Management Console.

4.1.3 - Removing the Application

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

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

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

Before you begin

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

About this task

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

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

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

Procedure

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

Results

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

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

4.3 - Importing SEOS-Enabled Nymi Band information into NES

Each time you place a order for SEOS-enabled Nymi Bands, Nymi provides you a CSV that contains important information about the Nymi Bands.

About this task

Note: Ensure that you upload the information about the SEOS-enabled Nymi Bands before a user enrolls to the Nymi Band.

Nymi attaches the CSV file to the purchase order email.

Procedure

1. Copy the *CSV* file to a folder on the Nymi Enterprise Server(NES) server.

   Note: Do not modify the *CSV* file. Changes to the *CSV* can prevent successful enrollment.
2. Log into the NES Administrator Console on the NES server with an NES Administrator account.
3. On the menu bar, click **`Search`**.

4. In the Search window, click **Nymi Bands**, and then click **Import**
   The following figure shows the Search window.

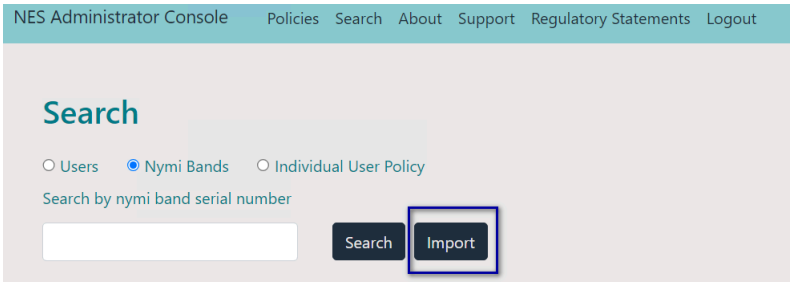


Figure 19: Import option in Search window

5. On the **Import Nymi Bands** window, click **Browse** as shown in the following figure

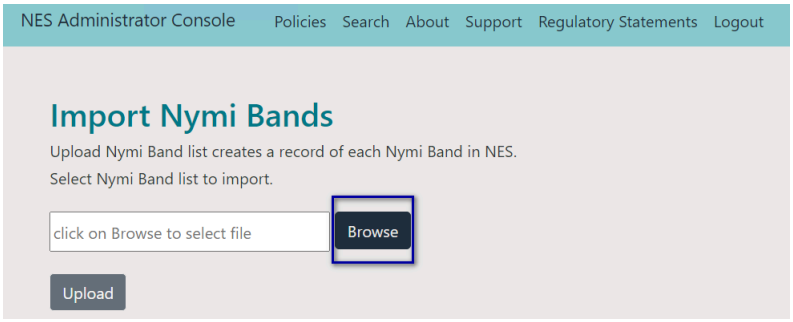


Figure 20: Browse in Import Nymi Bands window

6. In the Open window, navigate to the folder that contains the CSV file, select the *CSV* file, and then click **Open**.
   The path and filename appear in the **Import Nymi Bands** window, as shown in the following figure.

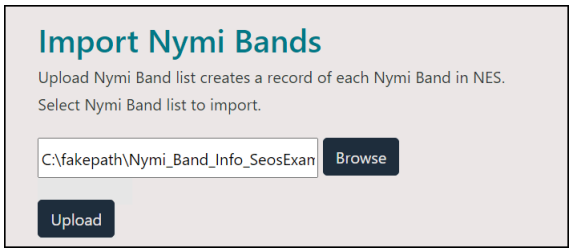


Figure 21: Import file window with filename

Note: Some browsers display the path of the file as *C:\fakepath*. It is not necessary to correct the path.

7. Click **Upload**.
   The import operation completes. The import feature updates the NES database with information for new Nymi Bands. If the import detects existing Nymi Bands, the operation retains existing information and updates the database with new information only.

   If the import operation encounters a problem, the Import Nymi Bands window indicates an error. To review error messages, click **Download records**, as shown in the following figure.

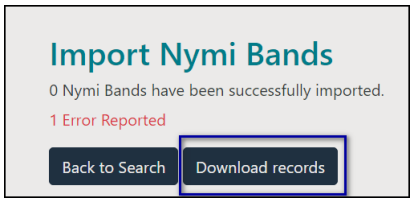


Figure 22: Nymi Band Import error

The NES Administrator Console creates a *CSV* file named *InvalidUploadsData* in the *Downloads* folder. Open the file and review the error message that appears in the last column for each Nymi Band that encountered an issue.

4.4 - (Secure NFC Only) Enrolling a Nymi Band

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

Before you begin

- Plug the Bluetooth Adapter and SEO-capable reader into the Nymi Band Application Terminal.
- Ensure that in the active NES policy, the *Enrollment /Registration Destination* value is set to *NES*. This prevents the enrollment process from adding unnecessary NFC ID entries for the Nymi Band in the Evidian EAM Controller. The *Nymi with Evidian Solution—Deployment Guide* provides more information.
- Ensure that the Nymi Band Application Terminal allows Evidian self-enrollment. The *Nymi with Evidian Solution—Deployment Guide* provides more information.

About this task

Enrollment is a two step process:

1. User logs in to the Nymi Band Application to complete the fingerprint registration and update the Nymi Enterprise Server(NES) database with information about the user and Nymi Band association.
2. User must then perform a Nymi Band tap on the Evidian Enterprise SSO login window, which presents the user with a second screen that prompts the user to supply their domain credentials. When the user supplies their credentials, Evidian associates the RFID serial number of the Nymi Band to the profile of the user in the Evidian EAM Controller.

To enroll the Nymi Band, perform the following actions:

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.
4. Launch the `Evidian Enterprise SSO` application. If the `Evidian Enterprise SSO` application is running, right-click **`Enterprise SSO`**, select **`Stop`**, and then start `Evidian Enterprise SSO` again.
5. On the `Evidan Enterprise SSO` screen, perform a Nymi Band tap.
   The `Evidan Enterprise SSO- Enroll RFID badge` popup appears.
6. On the `Evidan Enterprise SSO- Enroll RFID badge`, type the username and password of the user, and then click **`OK`**.
   The login completes as does the enrollment of the Nymi Band within Evidian.

Results

Before the user can successfully complete authentication tasks with a Nymi Band tap, the user might need to login to the Evidian Enterprise SSO window with their username and password to retrieve information from the Evidian EAM Controller. The user can perform subsequent logins by performing a Nymi Band tap.

4.5 - Migrating Existing Nymi Bands to Evidian

If you introduce Evidian into an existing Connected Worker Platform(CWP) deployment and your users have enrolled their Nymi Bands, Nymi Band users must log in to the Nymi Band Application on the enrollment terminal to complete the enrollment on the Evidian EAM Controller. It is not necessary for the users to delete user data on the Nymi Band and repeat the enrollment process.

Before you begin

The **`Enrollment / Registration Destination`** attribute in the Active NES policy is set to **`NES and Evidian`**.

Procedure

1. Ensure that the user is wearing their authenticated Nymi Band.
2. Log into the Nymi Band Application with the username and password of the user that will enroll the Nymi Band.
3. Close the Nymi Band Application when the enrollment completes.

Results

To confirm that the Nymi Band details appears for the user in the Evidian, perform the following actions:

1. Log into the Evidian EAM Management Console and an EAM Administrator, select the **`Directory panel`**.
2. Select the search request up at the top of the navigation tree.
3. Change the object type to user and then in the **`Filter`** field, type your username.
4. Select your user, and then select the **`RFID`** tab. Confirm that you can see entries for your Nymi Band, the following figure provides an example of what you would see:

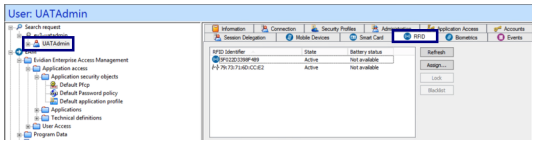


Figure 23: RFID tab for Nymi Band user

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

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

About this task

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

Procedure

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

Results

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

4.6 - Viewing the Nymi Band Associated with a User

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

Procedure

1. In the Evidian EAM Management Console, select the **`Directory`** panel.
2. Select the search request by changing the object type to **`user`**, and then in the **`Filter`** field, type the username.

   The following figure shows the `Search request` window.

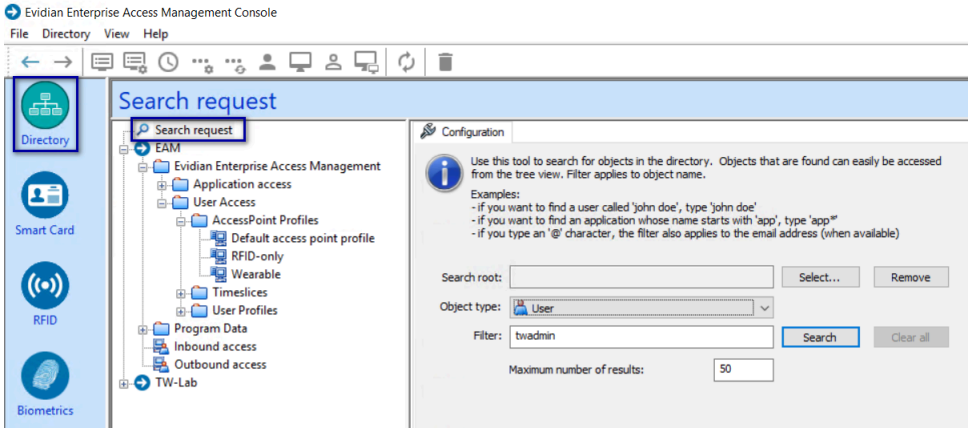
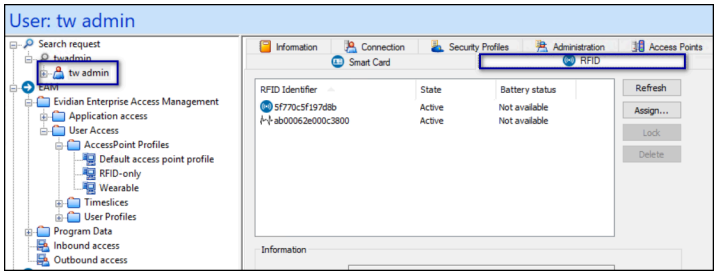
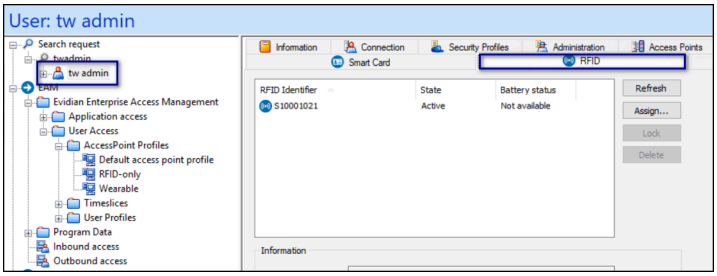


Figure 24: Search request window

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

Deployment	Nymi Band Entries
Wearable / RFID-only Mode	Two entries display, one for the user as an RFID entry and the other is a Wearable entry.  **a.** Select the Wearable entry, and then click **`Blacklist`**. **b.** On the `Confirmation` window, click **`Yes`**. **c.** On the `Confirmation` window, click **`Yes`**.

Deployment	Nymi Band Entries
	d. Once blacklisted, the **`Delete`** button appears. Click **`Delete`**.
Secure NFC Mode	One entry appears.  **a.** Select the Serial Number entry, and then click **`Blacklist`**. **b.** On the `Confirmation` window, click **`Yes`**. **c.** Once blacklisted, the **`Delete`** button appears. Click **`Delete`**.

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

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

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

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

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

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

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

Before you begin

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

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

About this task

Instruct the user to perform the following steps.

Procedure

1. Perform the delete user data operation on the Nymi Band identified for re-enrollment.
2. For Secure NFC only, you must blacklist and delete the RFID entry for the Nymi Band in the Evidian EAM Management Console.
3. Log into the Nymi Band Application and complete the steps for enrollment.

   The steps to complete a re-enrollment and re-registration are identical to the steps that the user follows to complete a new enrollment and registration.
4. For FIDO2 only, when a user enrolls to another Nymi Band, the user must re-create the FIDO2 security key on the newly enrolled Nymi Band.

Results

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

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

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

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

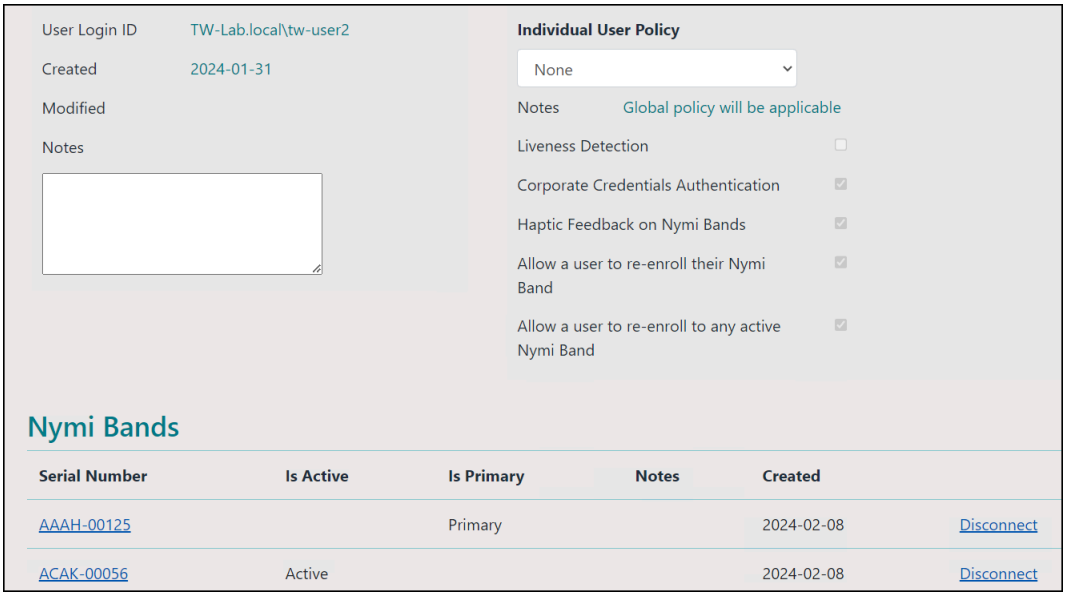
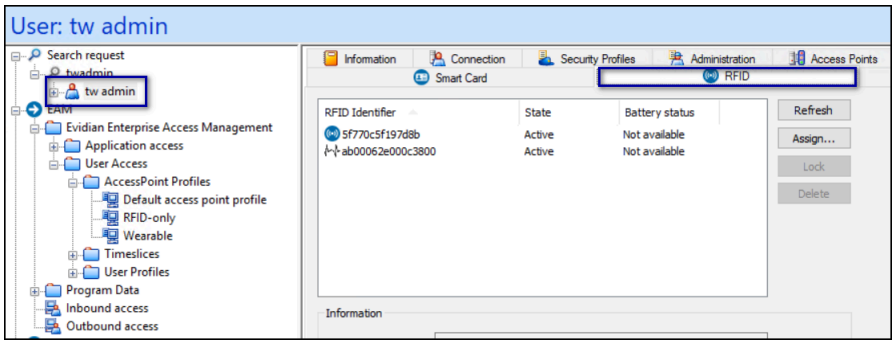
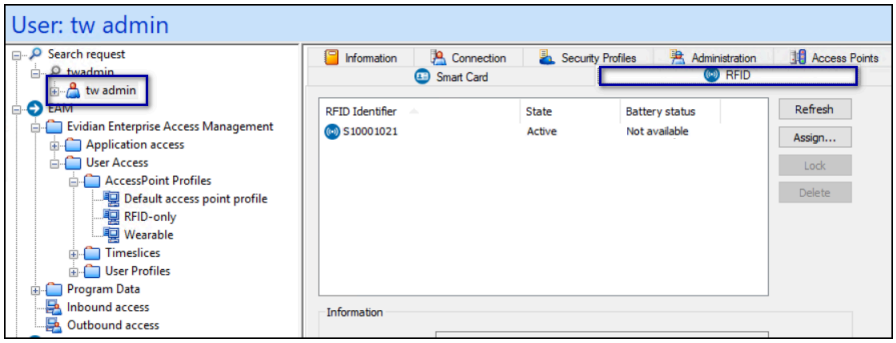


Figure 25: User with multiple Nymi Bands after self-service re-enrollment.

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

The following section describes what you see in the Evidian EAM Management Console after a user completes a self enrollment with a Nymi Band that was already enrolled to them. The result differs depending on the Nymi Band mode.

Nymi Band Mode	Nymi Band entries
Wearable / RFID only mode	The RFID tab for the user displays the entries for NFC UID and MAC address for the new instance of the Nymi Band as well as the MAC address entry for the old Nymi Band. 
Secure NFC mode	The RFID tab for the user displays the entry for the RFID serial number of the Nymi Band. 

Nymi recommends that you do not manually manage Nymi Band entries for a user after self-enrollment.

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

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

Before you begin

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

About this task

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

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

Procedure

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

What to do next

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

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

4.7.3 - Returning a Nymi Band Without Self-Enrollment

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

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

Want to see this a video instead? Go to YouTube

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

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

About this task

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

Procedure

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

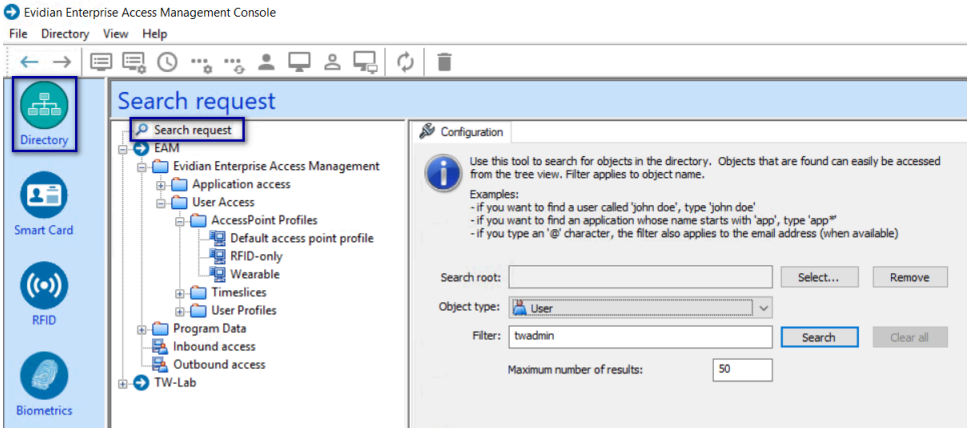
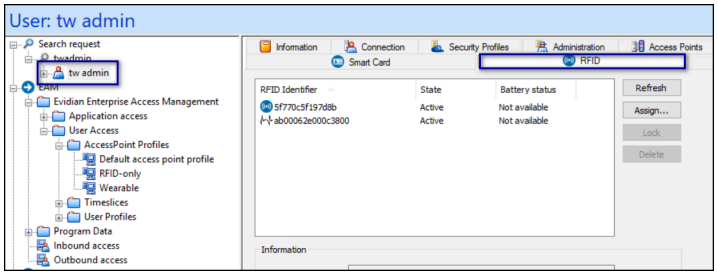
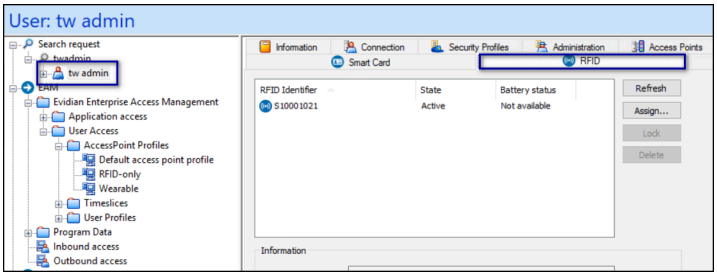


Figure 26: Search request window

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

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

Deployment	Nymi Band Entries
Secure NFC Mode	One entry appears.  **a.** Select the Serial Number entry, and then click **`Blacklist`**. **b.** On the `Confirmation` window, click **`Yes`**. **c.** Once blacklisted, the **`Delete`** button appears. Click **`Delete`**.

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

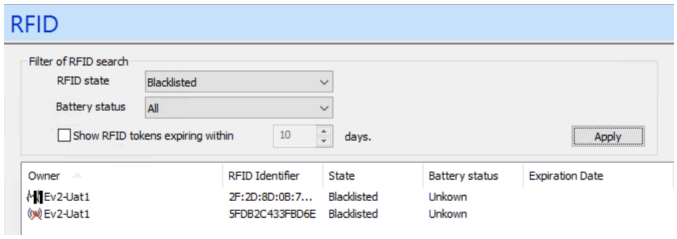


Figure 27: Blacklisted Nymi Band

For Secure NFC mode, only one entry appears.

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

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

Perform the following steps to remove the Nymi Band association to the user in Nymi Enterprise Server(NES).

Procedure

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

6. On the `Disconnect` screen, scroll to the bottom and select **`Disconnect`**.

4.7.3.3 - Deleting User Data on Nymi Band 4

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

About this task

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

Procedure

1. Remove the Nymi Band from the wrist of the user, and then attach the Nymi Band to a charger.
2. Press the Nymi Band fingerprint sensor twice. The Delete User Data message displays on the screen, as shown in the following figure.

Figure 28: Delete User Data

3. Hold your finger on the fingerprint sensor until the Nymi Band vibrates quickly twice and the **Delete** message displays on the screen, as shown in the following figure.

Figure 29: Delete progress screen

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

4. When `Delete User Data Completion` screen appears, remove your finger from the fingerprint sensor, as shown in the following figure

   The following figure shows the `Delete User Data Completion` screen.

Figure 30: Delete User Data Completion

The Delete User Data operation completes.

Results

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

Note: If you delete the user data on a Nymi Band and attempt to re-enroll it when self service enrollment is not enabled in the Nymi Enterprise Server(NES) policy, you will see the following message,

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

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

4.7.3.4 - Deleting User Data on Nymi Band 3

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

About this task

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

Procedure

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

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

   Figure 31: Delete User Data
3. Continue to hold the bottom button until the Nymi Band quickly vibrates twice and the **USER DATA DELETED** message displays on the screen (after about 10 seconds), as show in the following figure.

   Figure 32: User Data Deleted

Results

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

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

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

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

4.7.4 - Handling a Lost Nymi Band Without Self Enrollment

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

About this task

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

Procedure

1. In the Evidian EAM Management Console, select the **`Directory`** panel.
2. Select the search request by changing the object type to **`user`**, and then in the **`Filter`** field, type the username.

   The following figure shows the `Search request` window.

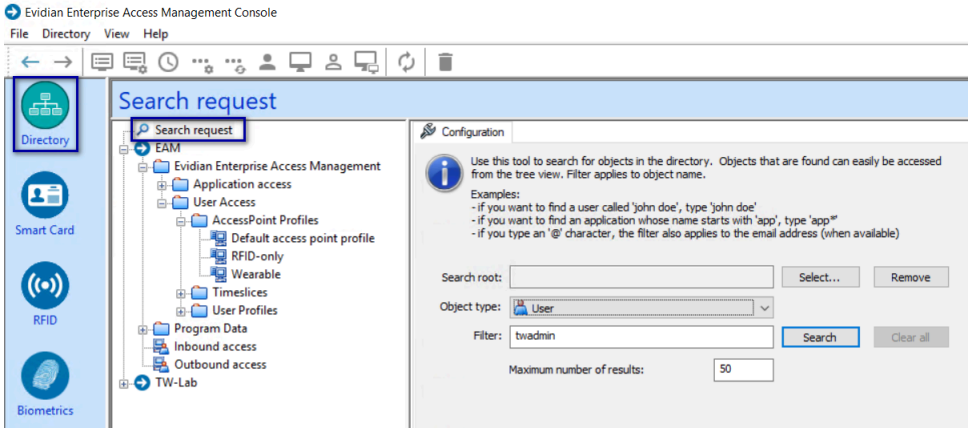
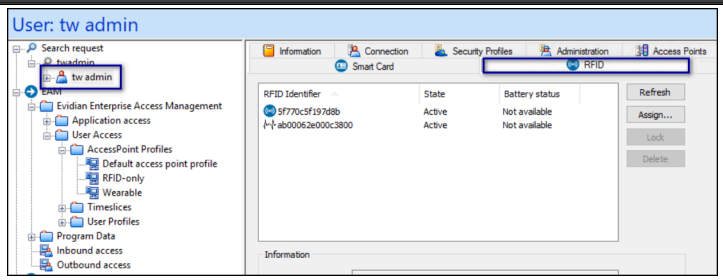
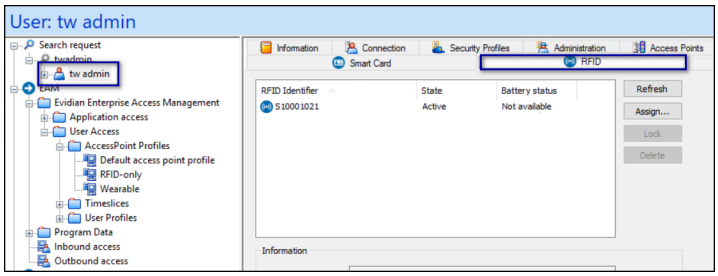


Figure 33: Search request window

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

Deployment	Nymi Band Entries
Wearable / RFID-only Mode	Two entries display, one for the user as an RFID entry and the other is a Wearable entry.

Deployment	Nymi Band Entries
	 **a.** Select the Wearable entry, and then click **`Blacklist`**. **b.** On the `Confirmation` window, click **`Yes`**. **c.** On the `Confirmation` window, click **`Yes`**.
Secure NFC Mode	One entry appears.  **a.** Select the Serial Number entry, and then click **`Blacklist`**. **b.** On the `Confirmation` window, click **`Yes`**.

Results

The Nymi Band is blacklisted in Evidian. 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.

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

Perform the following steps to remove the Nymi Band association to the user in Nymi Enterprise Server(NES).

Procedure

1. In the **`Search`** page, select the **`Users`** Option.
2. In the **`Search`** field, type the full or partial username, first name, or last name of the user.
3. Click **`Search`**. The `Search` page displays the user, or a list of users that match the search criteria.
4. Select the Domain\username link of the user to open the **`User Details`** page.

5. In the Nymi Band table, to the right of the Nymi Band that you want to delete, click **Disconnect**. On the Disconnect page, scroll down and then click **Disconnect**.
6. On the Disconnect screen, scroll to the bottom and select **Disconnect**.

4.7.5 - Handling a found Nymi Band Without Self-Enrollment

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

About this task

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

Procedure

1. In the Evidian EAM Management Console, select the **Directory** panel.
2. Select the search request by changing the object type to **user**, and then in the **Filter** field, type the username.
   The following figure shows the Search request window.

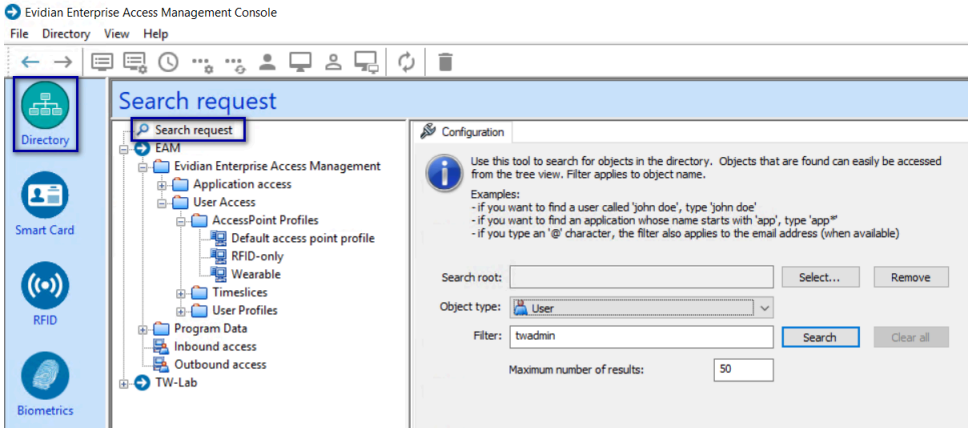


Figure 34: Search request window

3. Click **Search**.
4. Select the user, and then select the **RFID** tab, and the perform one of the following actions:
   - For Wearable and RFID-only modes:
     a. Select the RFID device, and then click **Delete**.
     b. Select the wearable device, and then click **Delete**.
   - For Secure NFC mode, select the serial number, and then click **Delete**.
5. In the left navigation pane, select **RFID**.
6. From the **RFID state** list, select **Blacklisted**, and then click **Apply**.
   For Wearable and RFID-only modes, two blacklisted entries appear for the user, one for the RFID and one for the Wearable entry, as shown in the following figure.

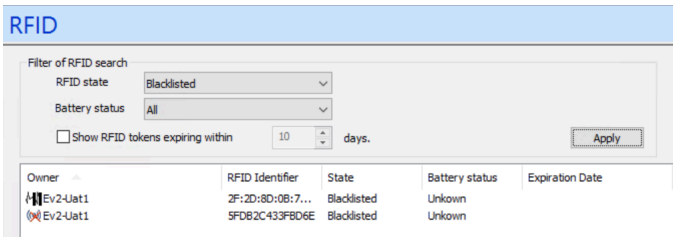


Figure 35: Blacklisted Nymi Band

For Secure NFC mode, only one entry appears.

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

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

Perform the following steps to remove the Nymi Band association to the user in Nymi Enterprise Server(NES).

Procedure

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

4.8 - Adding New Users and Computers to the Solution

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

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

5 - Managing the Nymi with Evidian Solution

Review this section for information about tasks that you perform after you deploy the Nymi with Evidian Solution, such as backups and recoveries.

5.1 - Delegating an Administrator Role to a User

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

Procedure

1. Log into the Evidian EAM Management Console with a user account that is an EAM administrator.
2. Click on the **`Account and Access Rights Management`** icon.
3. In the Evidian EAM Management Console, select the **`Directory`** panel.
4. Select the search request by changing the object type to **`user`**, and then in the **`Filter`** field, type the username.

   The following figure shows the `Search request` window.

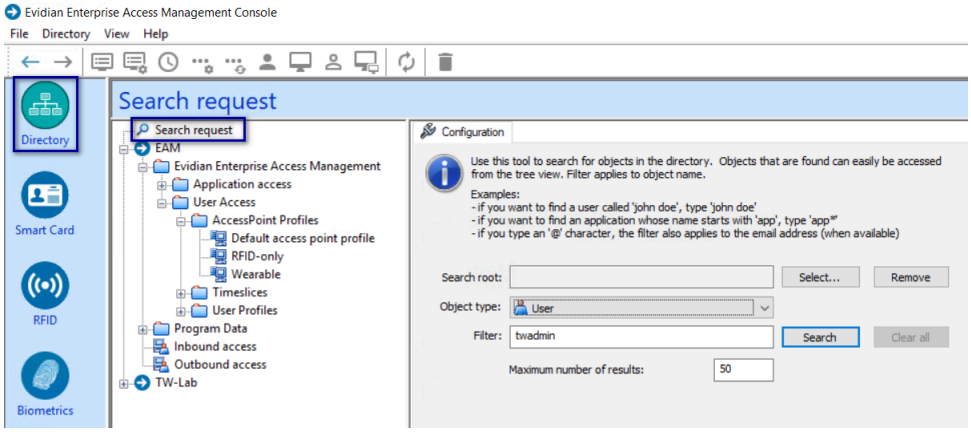


Figure 36: Search request window

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

Figure 37: Delegate option

8. In the **`Administration Profiles`** section, click **`Add`**.

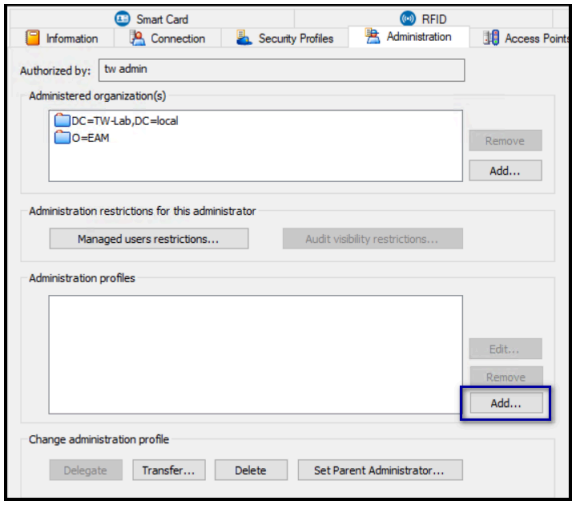


Figure 38: Add Administration Profiles

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

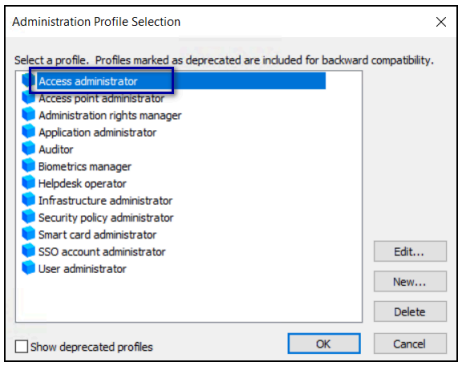


Figure 39: Administration Profiles Selection window

10. Click **OK**.
11. On the **`Administration`** tab, click **`Apply`**.

5.2 - Providing Users Access to Enterprise SSO Studio Only

You can provide user accounts with the ability to access Evidian Enterprise SSO Studio to train applications and manage the technical definition configuration, but you do not provide the user account with administrative access to Evidian EAM Controller.

About this task

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

Procedure

1. In the `Directory` view, use the **`Search Request`** option to search for the user account.
2. On the **`Administration`** tab, in the **`Administration Profiles`** section, click **`Add`**.
   The following figure shows the `Administration` tab.

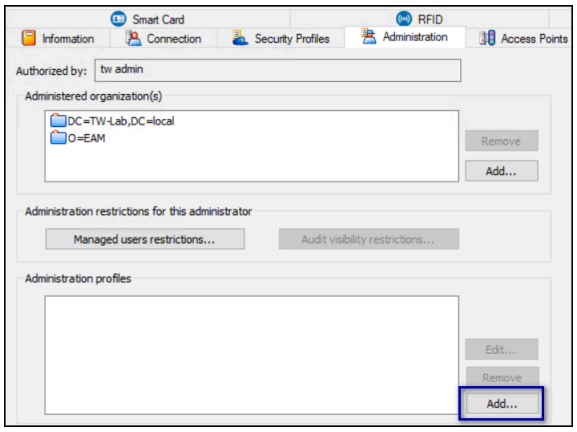


Figure 40: Administration Tab

3. On the `Administration Profile Selection` window, select **`Application Administrator`**, and then click **`OK`**.

   The following figure shows the `Administration Profile Selection` window.

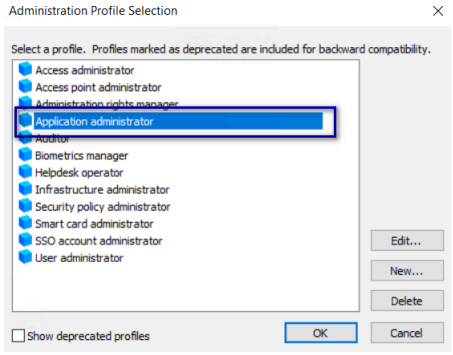


Figure 41: Administration Profile Selection window

4. On the **`Administration`** tab click **`Apply`**.
5. Instruct the user to start Evidian Enterprise SSOStudio and confirm that login succeeds.

5.3 - Managing Service Account Password Changes

Nymi and Evidian both recommend that you configure your configure the service account with a password that never expires.

Before you begin

To change the service account password in Evidian, you must know the passphrase.

About this task

If your organizational procedures require changes to the service account password, perform the following steps on to update Evidian components with the new password.

Procedure

1. On the Evidian EAM Controller, stop the Enterprise Access Management Security Services service.
2. Change the service account password.
3. From the folder that contains the Evidian installation package, navigate to *EAM.x64\TOOLS \WGSrvConfig*.
4. Run *WGSRVConfig.exe* as an administrator.
5. In the `Administrative Tools` window, click **`Configure Security Settings`**, as shown in the following figure.

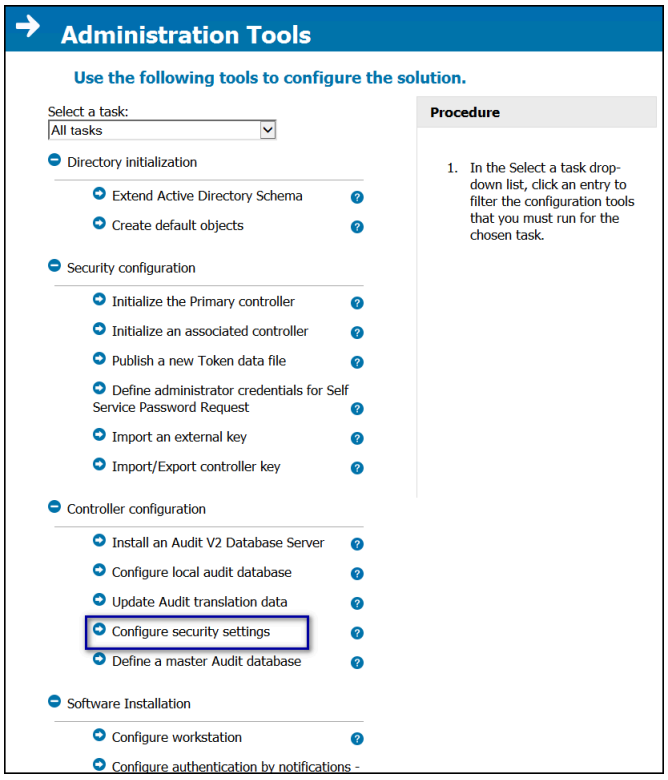


Figure 42: Configure Security Settings option

6. On the `Directory` tab, update the password for the service account, and then click **`OK`**.

   The following figure provides an example of the `Directory` tab.

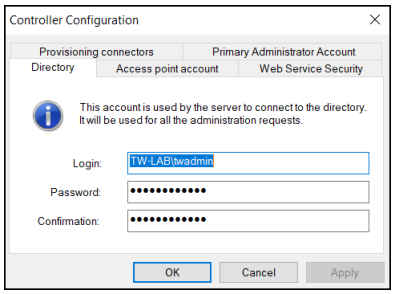


Figure 43: Directory tab

7. Launch `SQL Server Manangement Studio` (SSMS) and connect to the Evidian EAM database server.

5.4 - Managing User Account Password Changes

Review this article for a list of password change scenarios and the expected results.

Nymi recommends that Nymi Band users perform password management from a computer where the Evidian client software is installed. Evidian clients that use Authentication Manager or the Integrate with Windows option will prompt the user to change their password, during Nymi Band tap operations. If the user must manually change their password, it is recommended that they do so on the Evidian client.

Note: If the user changes their password on a machine that does not have the Evidian client software installed, see Nymi Band Taps Populate the Username in the Evidian SSO window only

Scenario 1 — Admin Changes Password in AD for a user and user does not remember old password

1. User performs a Nymi Band tap to log into the computer. The error LDAP error: Bad credentials provided appears.
2. User clicks **OK**. A screen appears that prompts the user to enter type new password.
3. User types their new password, and then clicks **OK**. A screen appears prompting the user for for their old password.
4. User presses the **`Reinitialize`** button. A popup appears that warns the user that it will cause a wipe of Evidian security data.
5. User clicks **OK** and the log in completes.
6. User can use their Nymi Band to perform authentication tasks without further intervention.

Scenario 2 — User is logged into their user terminal and their Password has expired/set to change password at next login in Active Directory

1. User open the MES app and when the SSO window appears, the user perform a Nymi Band tap. A window appears that notifies the user that they must change their password.
2. User clicks **OK**. A window appears that prompts the user to set a new password.
3. User specifies their new password, and then clicks **OK**. Log in completes.
4. User can use their Nymi Band to perform authentication tasks without further intervention.

Scenario 3 — User account is set to change the password at next logon in AD

1. User performs a Nymi Band tap to log into the Windows desktop. A window appears and notifies the user that they must change their password.
2. User clicks **OK**. A window appears that prompts the user to create a new password.
3. User provides a new password that meets the policy requirements, and then clicks **OK**. Desktop appears and SSO engine appears in the system tray.
4. User can use their Nymi Band to perform authentication tasks without further intervention.

Scenario 4 — User is required to change their password but types a password that does not meet the policy requirements

1. User opens the MES application and taps their authenticated Nymi Band when the SSO window appears. A window appears that notifies the user that they must change their password.
2. User clicks **OK**. A window appears that prompts the user to type a new password.
3. User specifies a password that does not meet the requirements, and then clicks **OK**. A window appears that states the password is not valid.
4. User clicks **OK**. A window appears that prompts the user to type a new password.
5. User types a new password that meets the policy requirements, and then clicks **OK**. The MES application login completes.
6. User can use their Nymi Band to perform authentication tasks without further intervention.

5.5 - Collecting Evidian EAM Client Log Files Remotely

To simplify client log file collection, you can use the Evidian EAM Management Console to configure debug mode on clients, and then collect the client side Evidian log files.

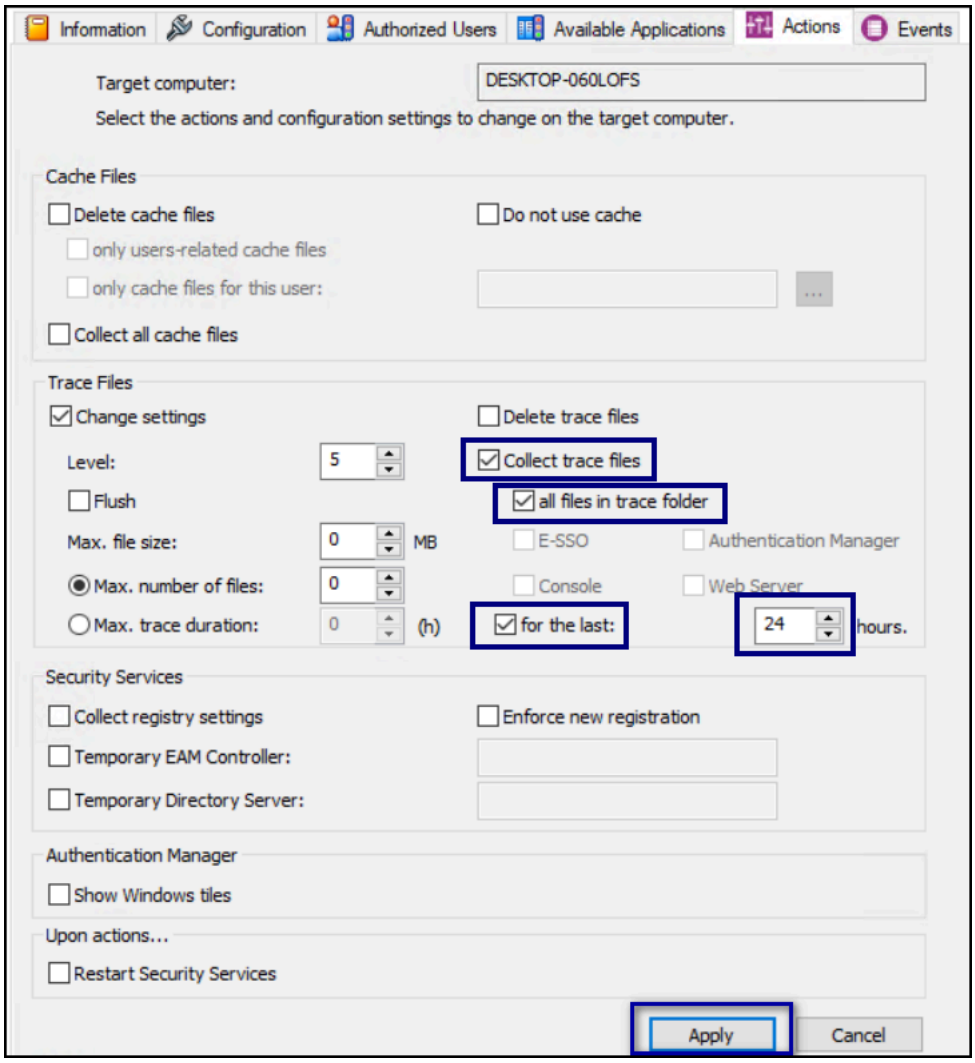
Before you begin

To collect log files remotely, your client computers must allow communication on port 3644.

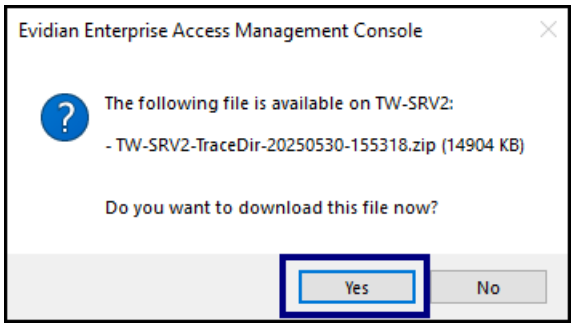
Procedure

1. Connect to the Evidian EAM Management Console with an administrator account.
2. From the **`Directory`** view, in left navigation pane, select **`Search request`**.
3. In the **`filter`** field, type the name of the user terminal, and then click **`Search`**
4. From the search results, click the computer name.
5. In the properties window, on the **`Actions`** tab, perform the following steps in the **`Trace Files`** section:
   a) Select **`Change settings`**.
   b) Set the value in **`Level`** to ***`5`***.
   c) For process crashes, select **`Flush`**.

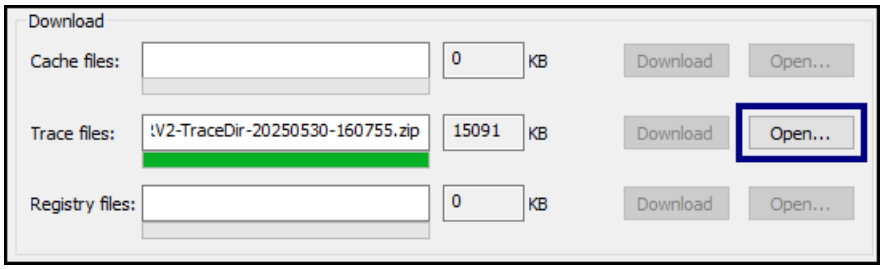
      Note: This option can produce large log files quickly.
   d) Click **`Apply`**. The following figure show the `Trace Files` section.
      The Enterprise Access Management Security Service service on the user terminal restarts and debug mode is disabled.



6. Reproduce the issue on the user terminal.
7. In the EAM Console, on the properties window of the user terminal, on the **`Actions`** tab, perform the following steps in the **`Trace Files`** section:
   a) Enable **`Collect trace files`**, and then select **`all files in trace folder`**.
   b) Select **`For the last`**, and then define the time period in hours, for example, ***24***.
   c) Click **`Apply`**. The following figure show the `Trace Files` section.
   d) On the `Evidian Enterprise Access Management Console` popup window, click **`Yes`**.



e) On the **`Select Folder`** window, navigate to the directory to save the *ZIP* file that contains the logs, and then click **`Select Folder`**.
The **`Downloads`** section displays the location of the *ZIP* file. Click **`Open`** to view the contents of the zip file.



f) Clear the **`Flush`** option.

g) Optionally,to disable debug mode on the user terminal, clear the **`Collect Trace Files`** option, change the **`Level`** value to ***`0`***.

h) Click **`Apply`**.
The Enterprise Access Management Security Service service on the user terminal restarts and debug mode is disabled.

5.6 - Collecting Evidian EAM Client Registry Settings Remotely

To simplify client registry entries, you can use the Evidian EAM Management Console to collect the client side registry settings.

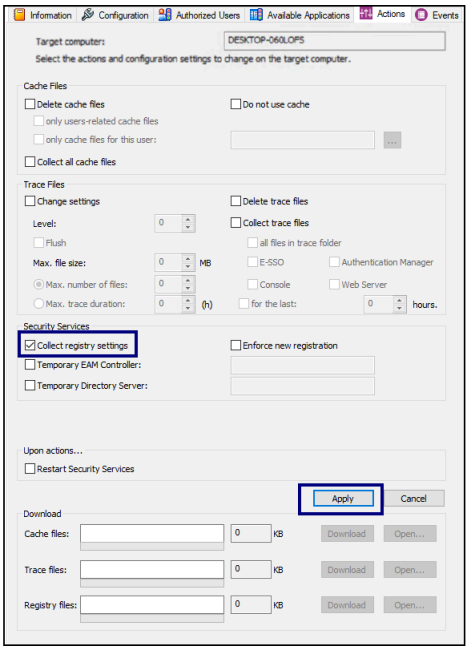
Before you begin

To collect registry settings remotely, your client computers must allow communication on port 3644.

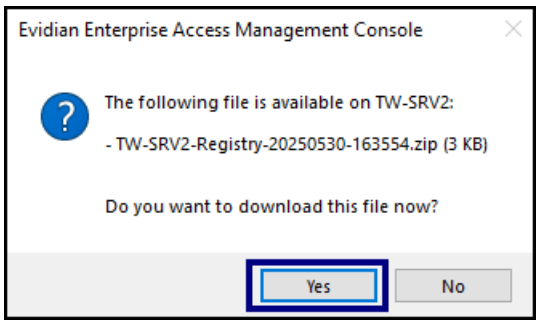
Procedure

1. Connect to the Evidian EAM Management Console with an administrator account.
2. From the **`Directory`** view, in left navigation pane, select **`Search request`**.

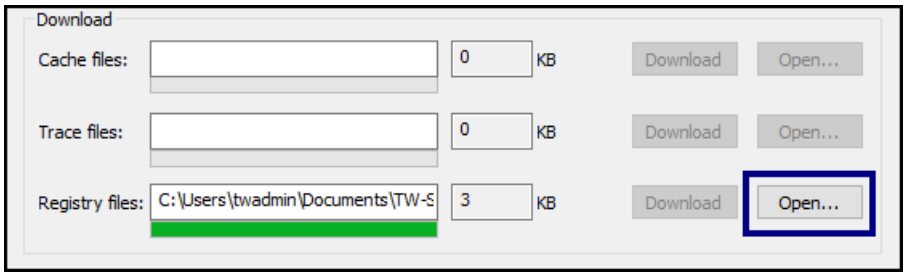
3. In the **`filter`** field, type the name of the user terminal, and then click **`Search`**.
4. From the search results, click the computer name.
5. In the properties window, on the **`Actions`** tab, perform the following steps in the **`Security Services`** section:
   a) Select **`Collect registry settings`**.
   b) Click **`Apply`**. The following figure show the `Security Services` section.



6. On the `Evidian Enterprise Access Management Console` popup window, click **`Yes`**.



7. On the **`Select Folder`** window, navigate to the directory to save the *ZIP* file that contains the registry settings, and then click **`Select Folder`**.
   The **`Downloads`** section displays the location of the *ZIP* file. Click **`Open`** to view the contents of the zip file.



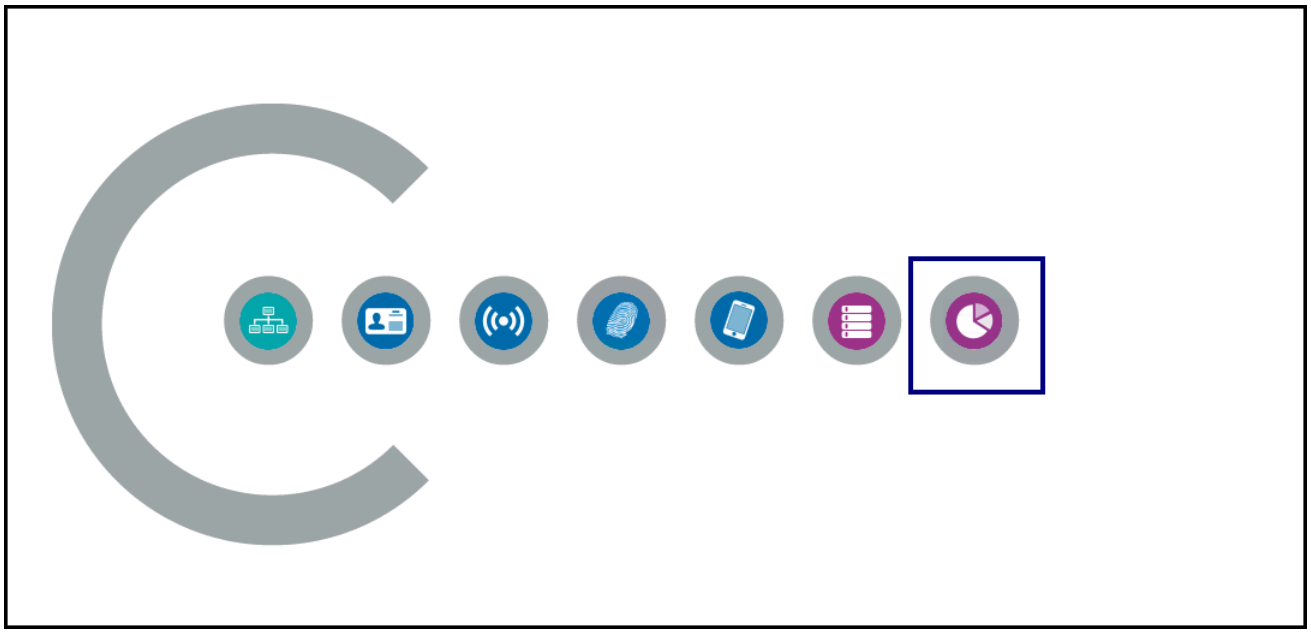
5.7 - Viewing Audit Information for Nymi Band Usage

Evidian stores audit information such as successful authentication, failed authentications, and enrollment information in a SQL database. You can use the Evidian Auditing and Reporting features in the Evidian EAM Management Console to view information about Nymi Band usage.

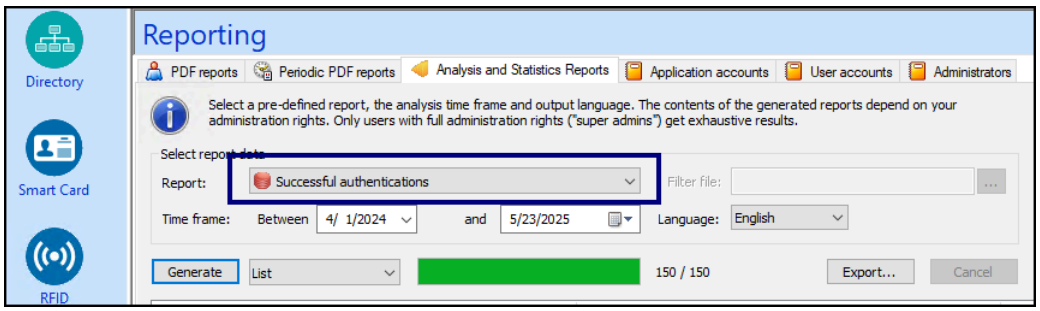
Viewing Successful Authentications

Evidian provides a report that allows you to determine when a user logs into an Evidian login window with their username and password, or a Nymi Band tap.

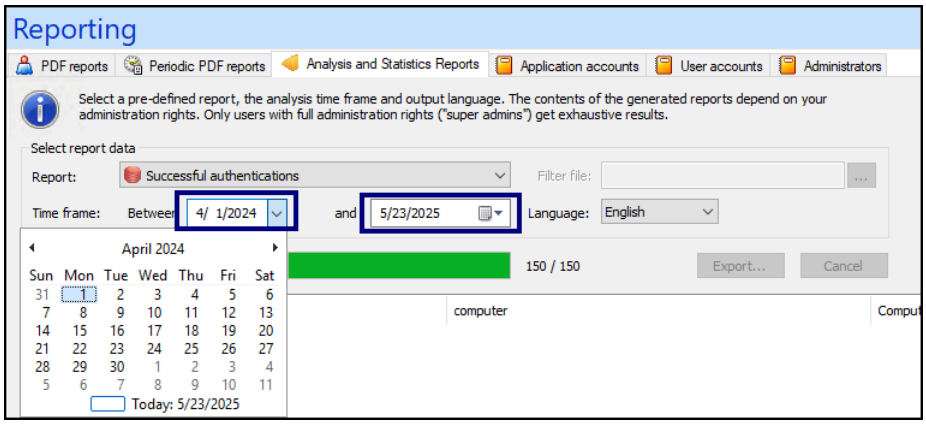
1. Log in to the Evidian EAM Management Console.
2. Click the **`Reporting`** icon, as shown in the following figure.



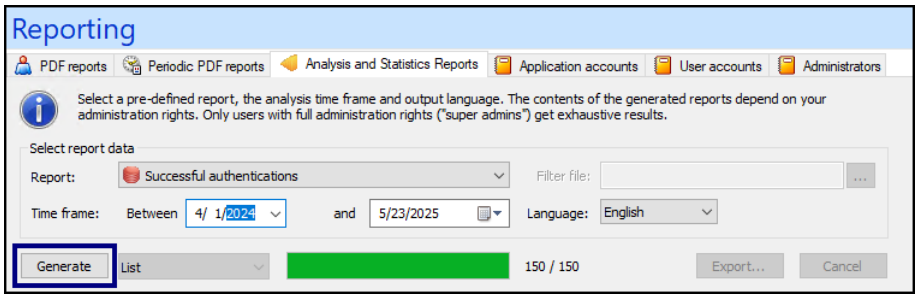
3. On the **`Analysis and Statistics Reports`** tab, from the **`Reports`** list, select **`Successful Authentications`**, as shown in the following figure.



4. In **`Time frame`** fields, use the date selectors to choose the time range on which to report. The following figure provides an example.



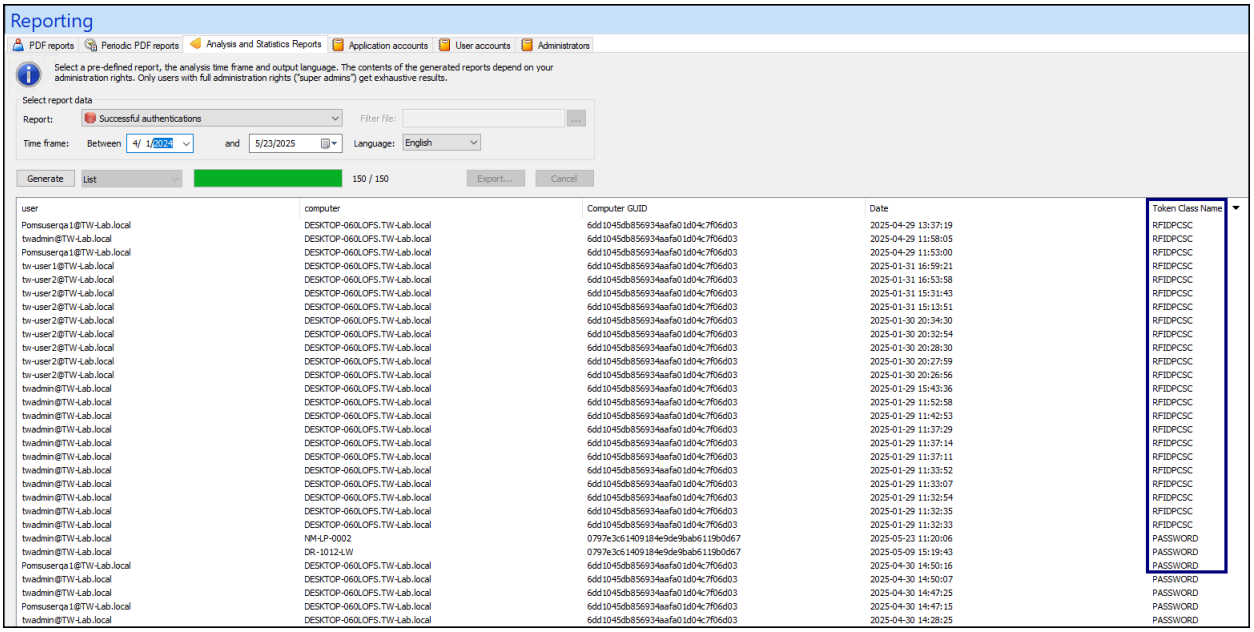
5. Click **`Generate`**, as shown in the following figure.



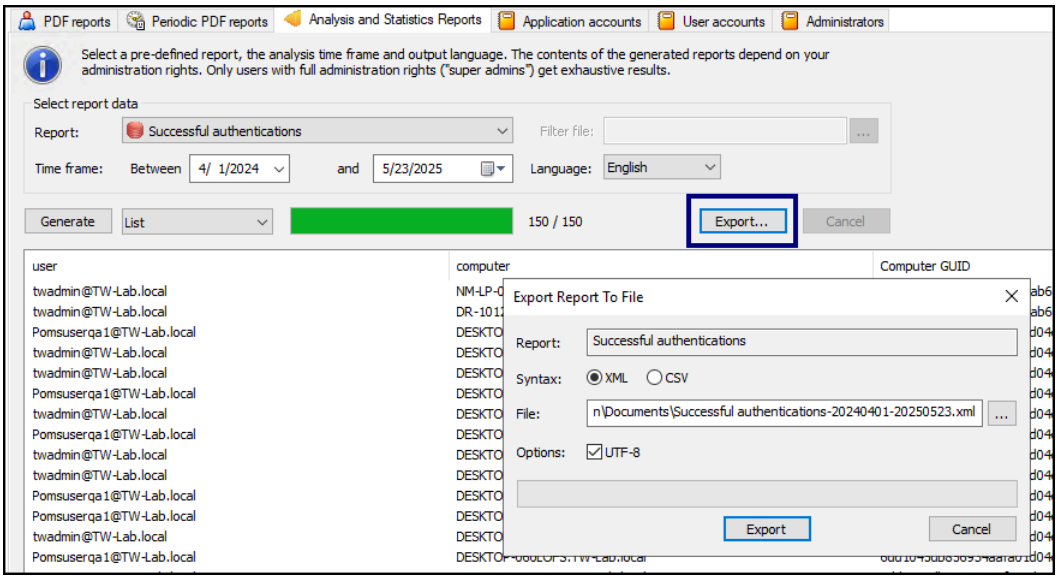
In the output, the value in the **`Token Class Name`** field identifies how the user completed the Evidian username and password window:

- Password—User typed their username and password.
- RFIDPCSC—User performed a Nymi Band tap.

The following figure provides an example of the output window.



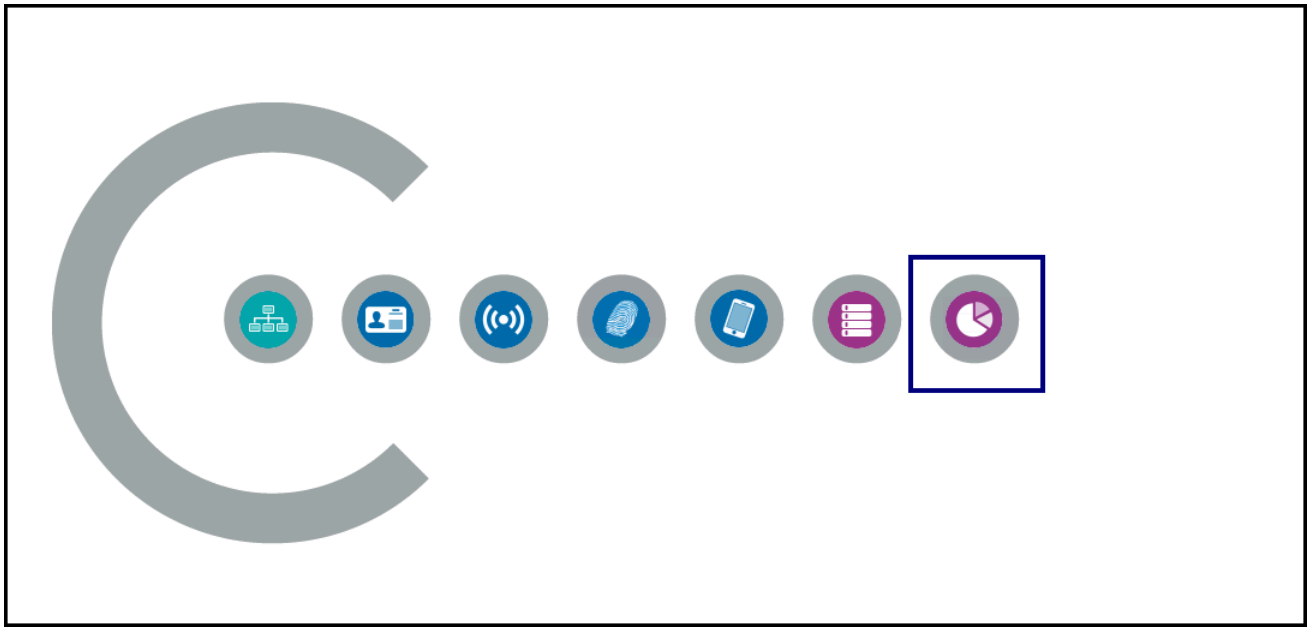
You can use the **`Export`** option to send the list to *XML* or *CSV* format.



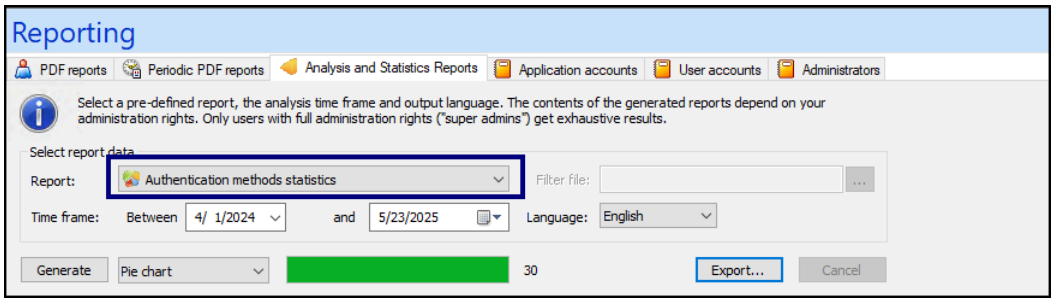
Comparing Total Nymi Band Taps vs Manual Username and Password Login

The Authentication method statistics allows you to determine when a user logs into an Evidian login window with their username and password, or a Nymi Band tap.

1. Log in to the Evidian EAM Management Console.
2. Click the **`Reporting`** icon, as shown in the following figure.



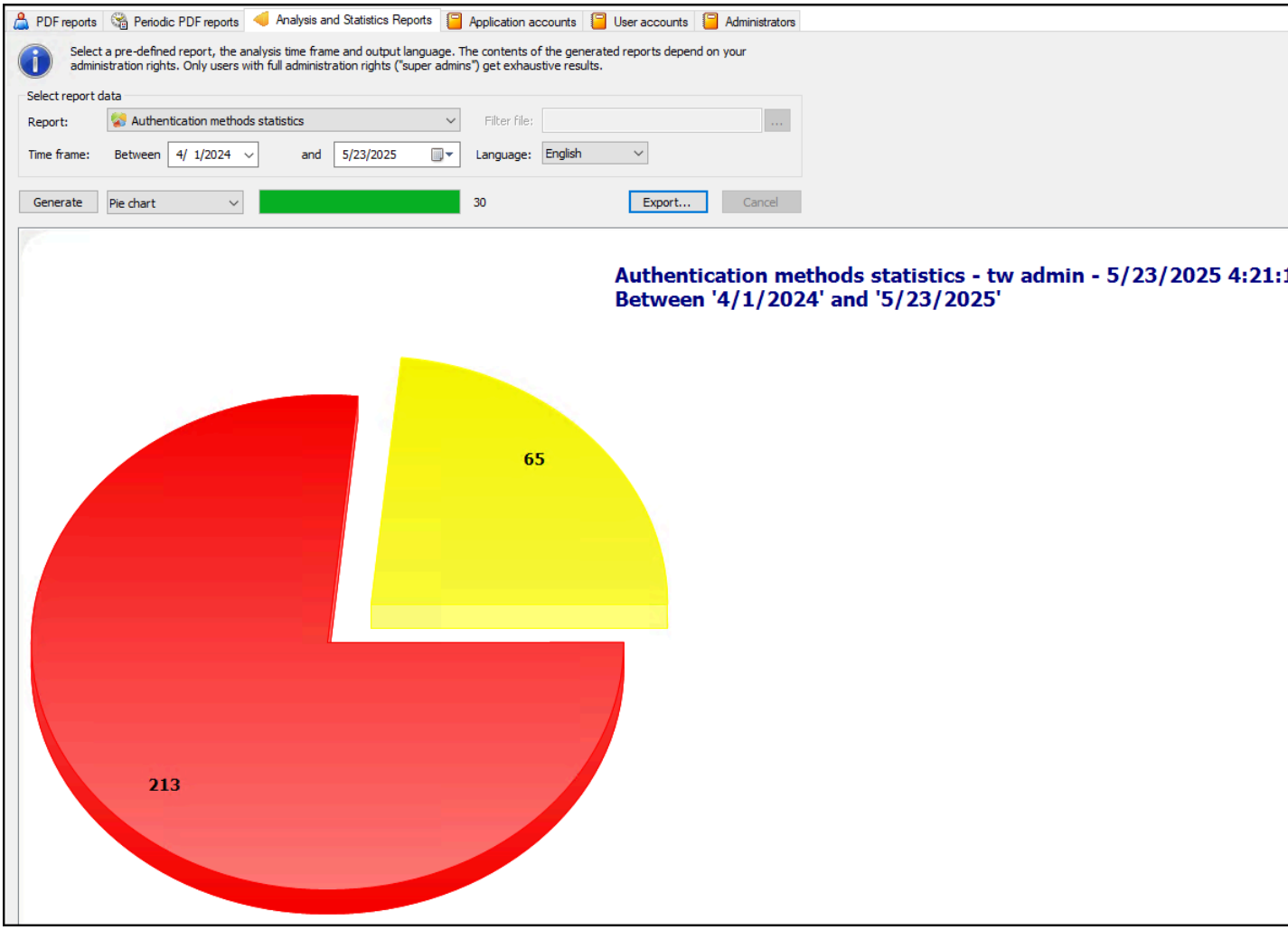
3. On the **`Analysis and Statistics Reports`** tab, from the **`Reports`** list, select **`Authentication method statistics`**, as shown in the following figure.



4. In **`Time frame`** fields, use the date selectors to choose the time range on which to report.
5. Click **`Generate`**.

The following figure provides an example of the pie chart output, where:

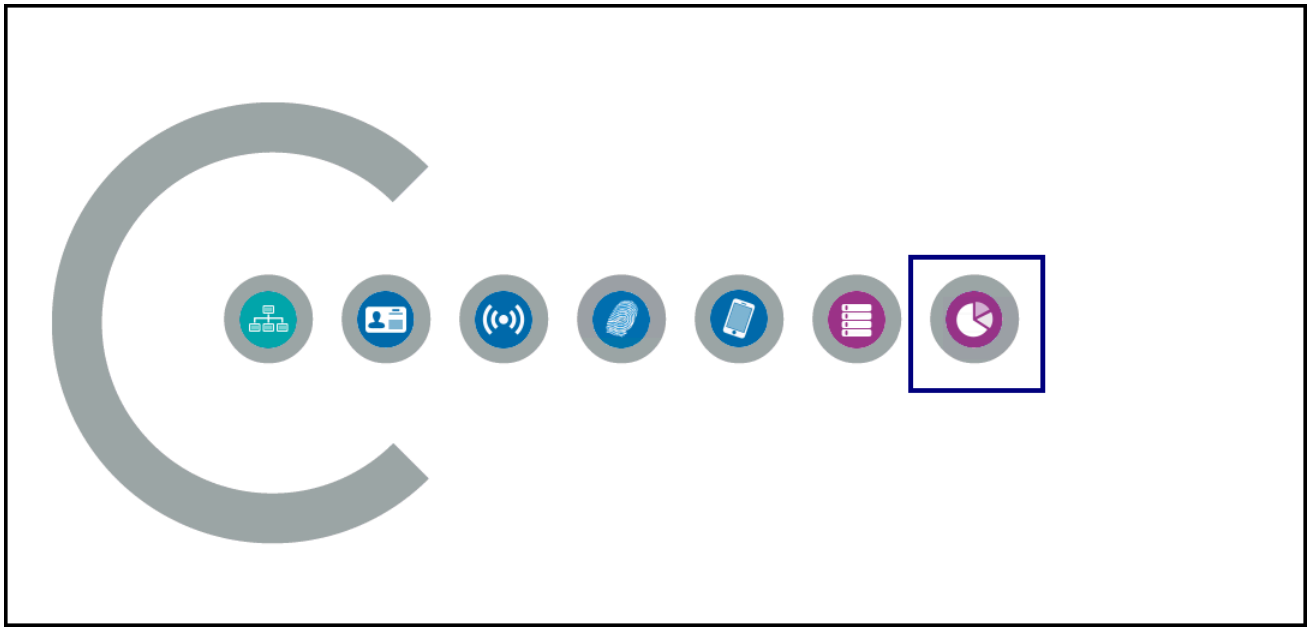
- Password—User typed their username and password.
- RFIDPCSC—User performed a Nymi Band tap.



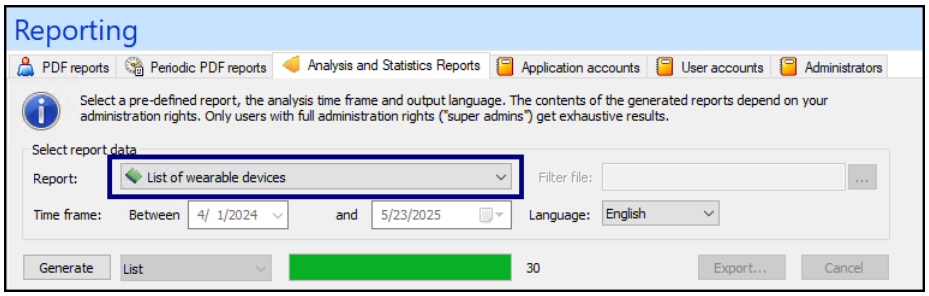
Viewing a list of Nymi Bands Enrolled in Evidian

The `List of Wearable Devices` report provides you with a list of Nymi Bands that have been enrolled to users in Evidian.

1. Log in to the Evidian EAM Management Console.
2. Click the **`Reporting`** icon, as shown in the following figure.



3. On the **`Analysis and Statistics Reports`** tab, from the **`Reports`** list, select **`Authentication method statistics`**, as shown in the following figure.

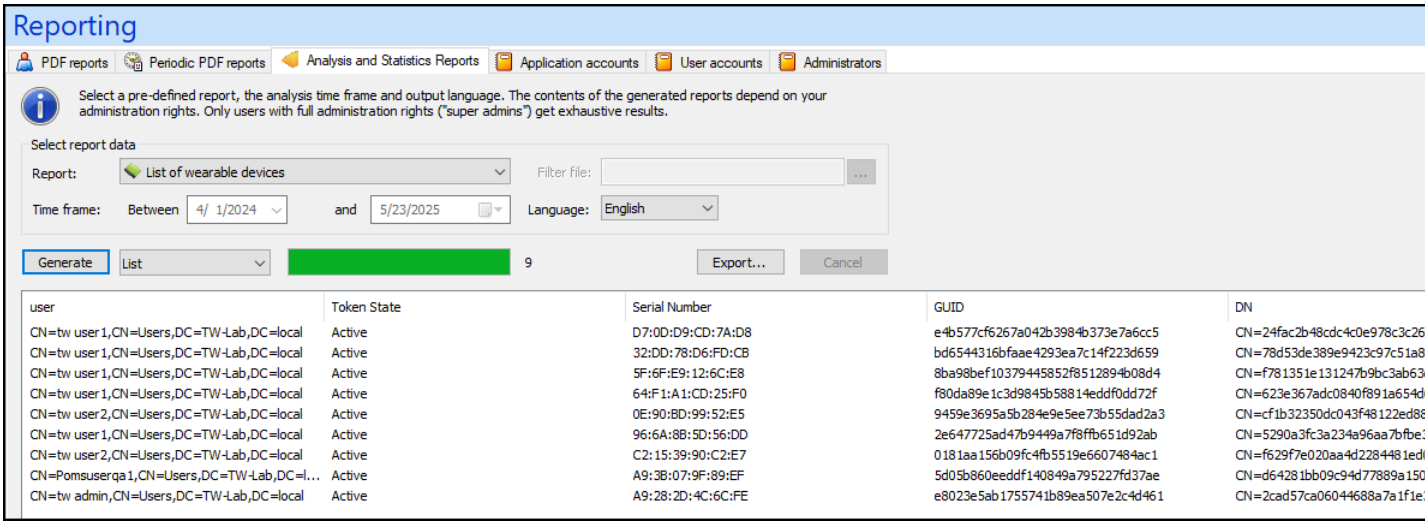


4. In **`Time frame`** fields, use the date selectors to choose the time range on which to report.
5. Click **`Generate`**.

The report provides you with information in the following columns:

- user—AD account associated with the Nymi Band.
- serial number—Serial number of the Nymi Band.
- Creation date (AD)—Date of Nymi Band enrollment.

The following figure provides an example of the output. In this example, users tw user1 and tw user2 have performed self re-enrollment several times and the report displays enrollment information for several different Nymi Bands.



5.8 - Exporting Technical Definitions

In some situations Nymi recommends that you export the technical definitions that are associated with your SSO applications, to allow you to import the technical definition configuration into another EAM Controller. For example, when you move from a Development environment to a QA environment to a Production Environment.

About this task

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

Procedure

1. Launch the `Enterprise SSO Studio` application (*C:\Program Files\Evidian\Enterprise Access Management\ssobuilder.exe*).
2. Expand **`EAM > Evidian Enterprise Access Management > Application access > Technical Definitions.`**.
3. Right-click the technical definition, and then select **`Export`**, as shown in the following figure.

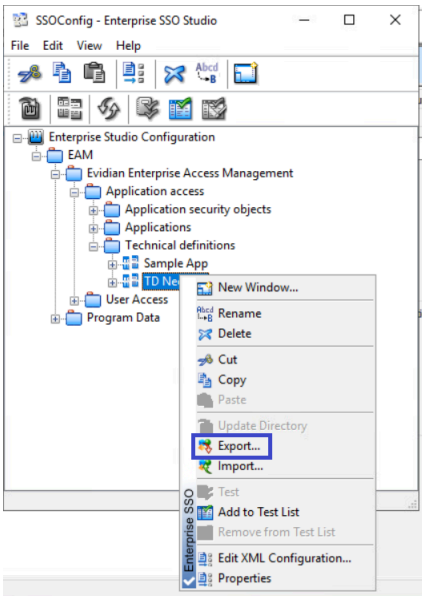


Figure 44: Export option

4. In the **Save as** window, select a directory location and provide the name of the file. Click **Save**.

5.9 - Importing Technical Definitions

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

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

Importing Technical Definitions in Enterprise SSO Studio

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

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

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

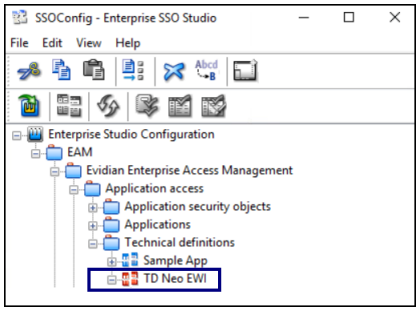


Figure 45: Imported Technical Definition

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

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

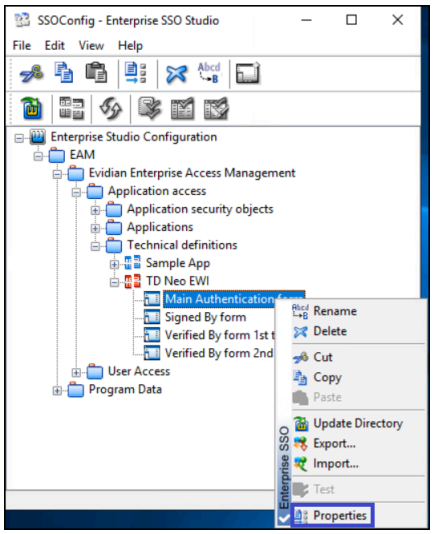


Figure 46: Properties option

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

   c. Click **`OK`**.

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

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

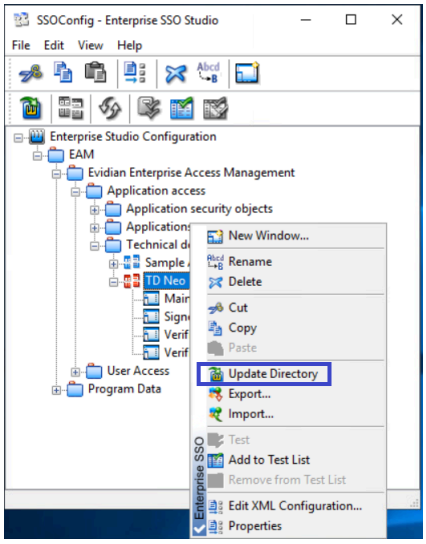
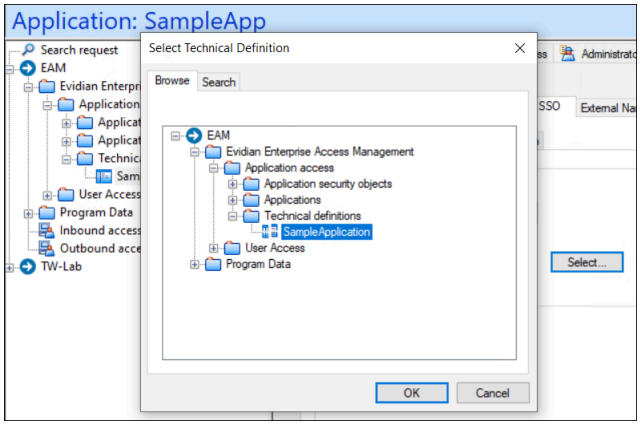


Figure 47: Properties option

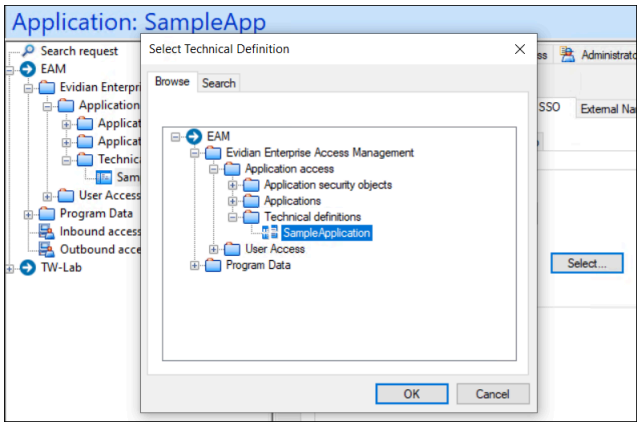
Update Technical Definition in Evidian EAM Management Console

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

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



4. If the technical definition is for an existing application instance, perform the following steps:
   a. Select the application.
   b. On the **SSO** tab, in the `Methods` window, click **`Select`**.
   c. Navigate to **`EAM > Evidian Enterprise Access Management > Application access > Applications`**, select the new technical definition, and then click **`OK`**. The following figure provides an example.



Download Technical Definition to User Terminals

Perform the following steps on each Evidian EAM Client.

1. From the system tray, select **`SSO Enterprise`**.
2. From the left menu pane, click the **`Home`** button, and in the **`Home`** window, click the **`Refresh`** button.
3. For new applications, from the left menu pane, click the **`Account`** button. Confirm that the new application appears and a username does not appear (displays not registered). If the application does not appear, right click in an empty area of the applications table and clear the option **`Hide applications without credential`**.
4. Launch the application and when prompted, log in with a username and password.
5. Perform a task that requires an e-signature and perform a tap to complete the operation.

5.10 - Installing Evidian Licenses

Eviden offers standard and perpetual by seat licenses for the Evidian software.

The following table provides a summary of the installation differences for each license type.

License Type	Renewal Period	Components that require license file
Standard	Annually	Evidian EAM Controller and all Evidian EAM Clients
Perpetual	n/a	Evidian EAM Controller and any Evidian EAM Clients on which you install the Evidian EAM Management Consoles or Evidian SSO Studio components.

The Evidian license file is a text file that you import into the registry by using the WGConfig tool.

To import the license file, perform the following actions:

1. Log into the computer 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 are prompted to replace the license keys, click **`Yes`**.

   On the confirmation window, click **`OK`**.
7. Click **`Cancel`** to close the window.
8. For the Evidian EAM Clients on which you import the perpetual license file only, restart the Evidian Enterprise Access Management Security service.

Note: You can 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.

5.11 - Freeing Up Evidian Licenses

When a user logs into an Evidian login window by performing a Nymi Band tap or typing their username and password, they begin to consume an Evidian license. When you blacklist the Nymi Band entries for a user in Evidian, the SSO data for the user remains. Users with SSO data are considered active users and continue to consume an Evidian license.

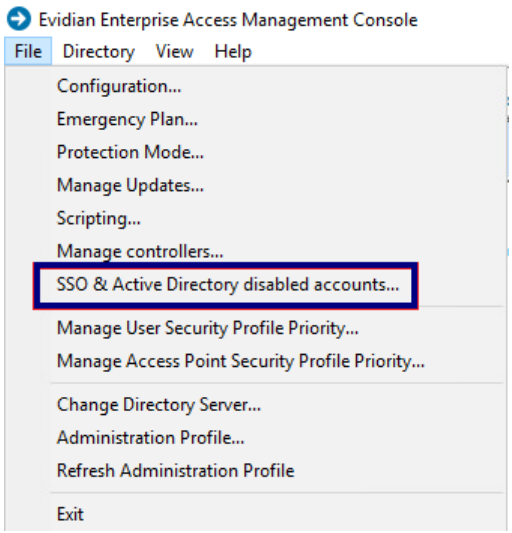
About this task

When the associated user account is disabled in Active Directory, you can free up the Evidian license for a user that no longer uses the Nymi with Evidian solution by performing the following steps.

Note: These steps apply to configurations that use AD LDS only.

Procedure

1. Log into the Evidian EAM Management Console as an EAM Administrator.
2. From the Help menu select About to make note of the number of licenses.
3. From the **`File`** menu, select **`SSO & Active Directory disabled accounts`**, as shown in the following figure.



4. On the **`Disabled accounts with SSO data`** window, select the applicable user, and then click **`Delete SSO data`**.

Results

It might take up to 24 hours for the license count to change. The Evidian controller performs a license calculation daily. The time that the Controller performs this calculation is not configurable. For performance reasons, the value is not calculated by a service restart.

5.12 - Collecting Evidian EAM Client Log Files Remotely

To simplify client log file collection, you can use the Evidian EAM Management Console to configure debug mode on clients, and then collect the client side Evidian log files.

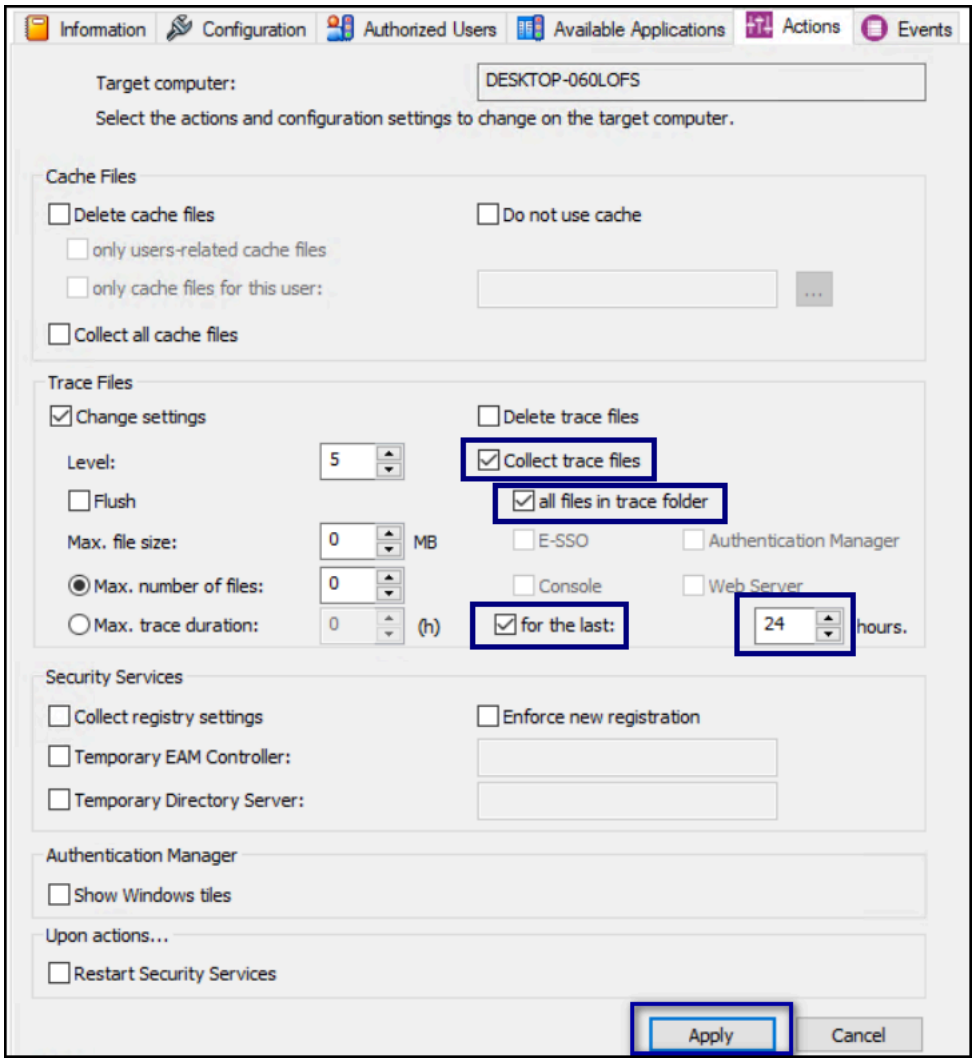
Before you begin

To collect log files remotely, your client computers must allow communication on port 3644.

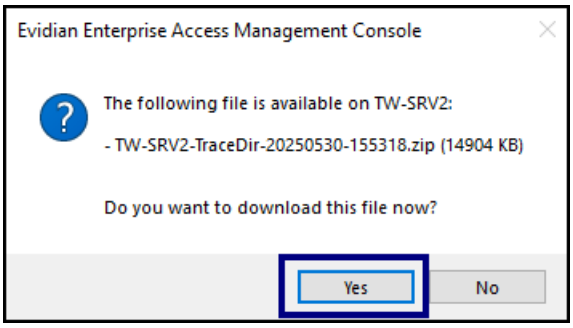
Procedure

1. Connect to the Evidian EAM Management Console with an administrator account.
2. From the **`Directory`** view, in left navigation pane, select **`Search request`**.
3. In the **`filter`** field, type the name of the user terminal, and then click **`Search`**
4. From the search results, click the computer name.
5. In the properties window, on the **`Actions`** tab, perform the following steps in the **`Trace Files`** section:
   a) Select **`Change settings`**.
   b) Set the value in **`Level`** to ***`5`***.
   c) For process crashes, select **`Flush`**.

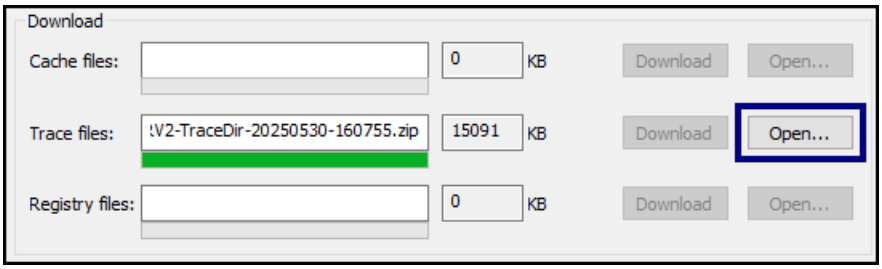
      Note: This option can produce large log files quickly.
   d) Click **`Apply`**. The following figure show the `Trace Files` section.
      The Enterprise Access Management Security Service service on the user terminal restarts and debug mode is disabled.



6. Reproduce the issue on the user terminal.
7. In the EAM Console, on the properties window of the user terminal, on the **`Actions`** tab, perform the following steps in the **`Trace Files`** section:
   a) Enable **`Collect trace files`**, and then select **`all files in trace folder`**.
   b) Select **`For the last`**, and then define the time period in hours, for example, ***24***.
   c) Click **`Apply`**. The following figure show the `Trace Files` section.
   d) On the `Evidian Enterprise Access Management Console` popup window, click **`Yes`**.



e) On the **`Select Folder`** window, navigate to the directory to save the *ZIP* file that contains the logs, and then click **`Select Folder`**.
The **`Downloads`** section displays the location of the *ZIP* file. Click **`Open`** to view the contents of the zip file.



f) Clear the **`Flush`** option.
g) Optionally,to disable debug mode on the user terminal, clear the **`Collect Trace Files`** option, change the **`Level`** value to ***`0`***.
h) Click **`Apply`**.
The Enterprise Access Management Security Service service on the user terminal restarts and debug mode is disabled.

5.13 - Collecting Evidian EAM Client Registry Settings Remotely

To simplify client registry entries, you can use the Evidian EAM Management Console to collect the client side registry settings.

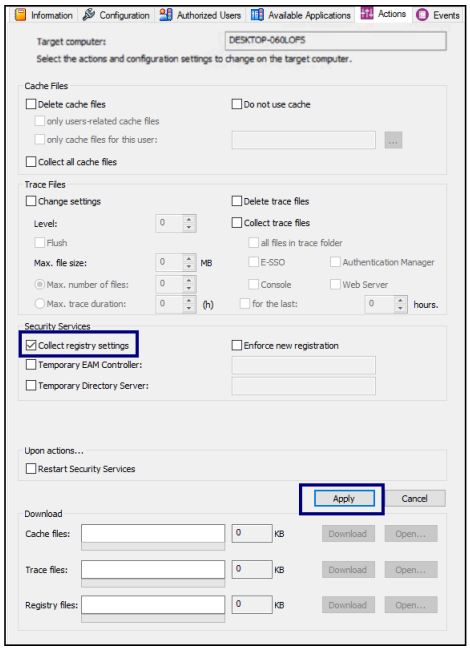
Before you begin

To collect registry settings remotely, your client computers must allow communication on port 3644.

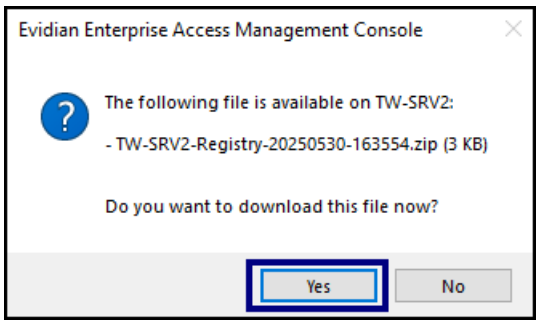
Procedure

1. Connect to the Evidian EAM Management Console with an administrator account.
2. From the **`Directory`** view, in left navigation pane, select **`Search request`**.

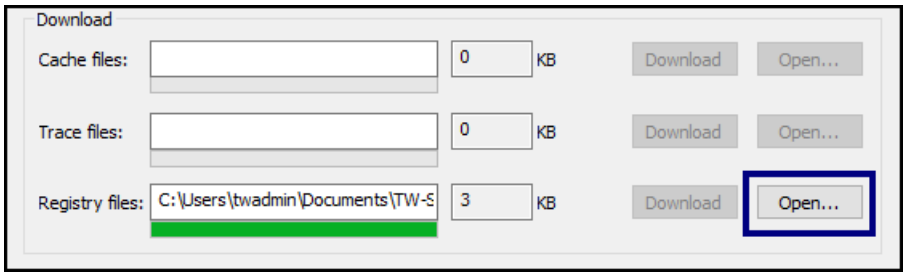
3. In the **`filter`** field, type the name of the user terminal, and then click **`Search`**.
4. From the search results, click the computer name.
5. In the properties window, on the **`Actions`** tab, perform the following steps in the **`Security Services`** section:
   a) Select **`Collect registry settings`**.
   b) Click **`Apply`**. The following figure show the `Security Services` section.



6. On the `Evidian Enterprise Access Management Console` popup window, click **`Yes`**.



7. On the **`Select Folder`** window, navigate to the directory to save the *ZIP* file that contains the registry settings, and then click **`Select Folder`**.
   The **`Downloads`** section displays the location of the *ZIP* file. Click **`Open`** to view the contents of the zip file.



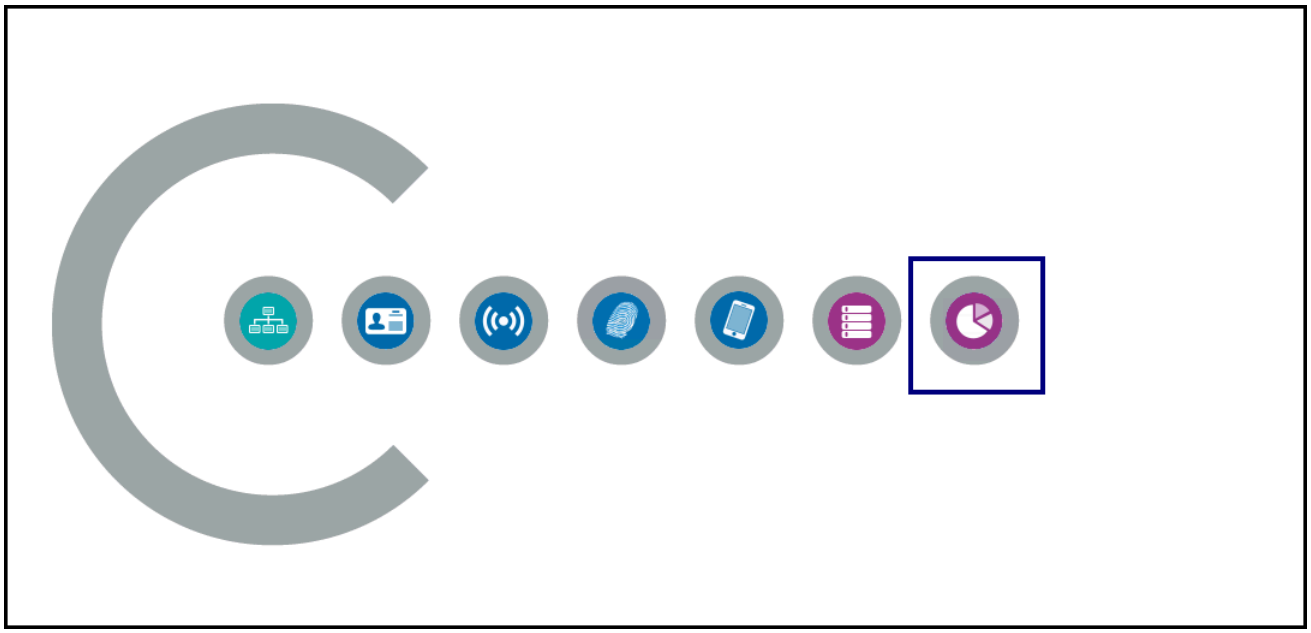
5.14 - Viewing Audit Information for Nymi Band Usage

Evidian stores audit information such as successful authentication, failed authentications, and enrollment information in a SQL database. You can use the Evidian Auditing and Reporting features in the Evidian EAM Management Console to view information about Nymi Band usage.

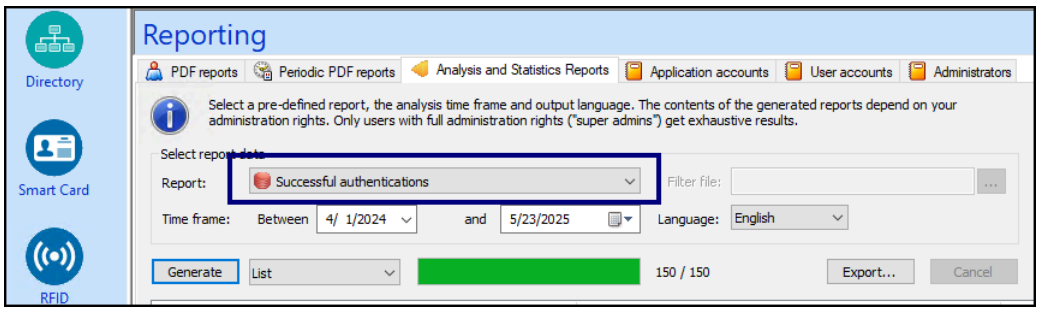
Viewing Successful Authentications

Evidian provides a report that allows you to determine when a user logs into an Evidian login window with their username and password, or a Nymi Band tap.

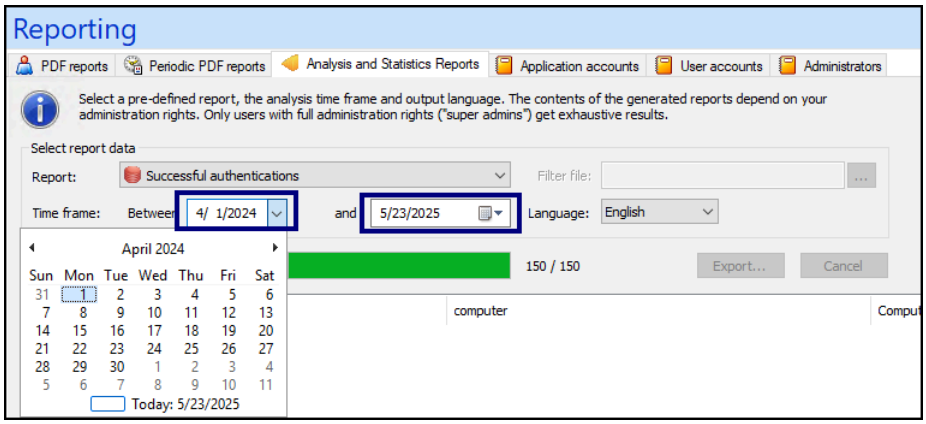
1. Log in to the Evidian EAM Management Console.
2. Click the **`Reporting`** icon, as shown in the following figure.



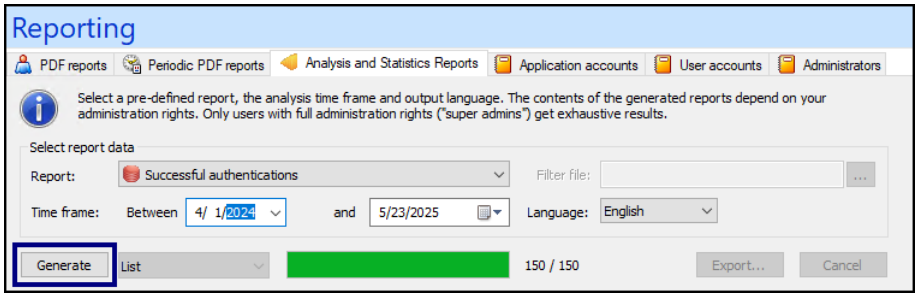
3. On the **`Analysis and Statistics Reports`** tab, from the **`Reports`** list, select **`Successful Authentications`**, as shown in the following figure.



4. In **`Time frame`** fields, use the date selectors to choose the time range on which to report. The following figure provides an example.



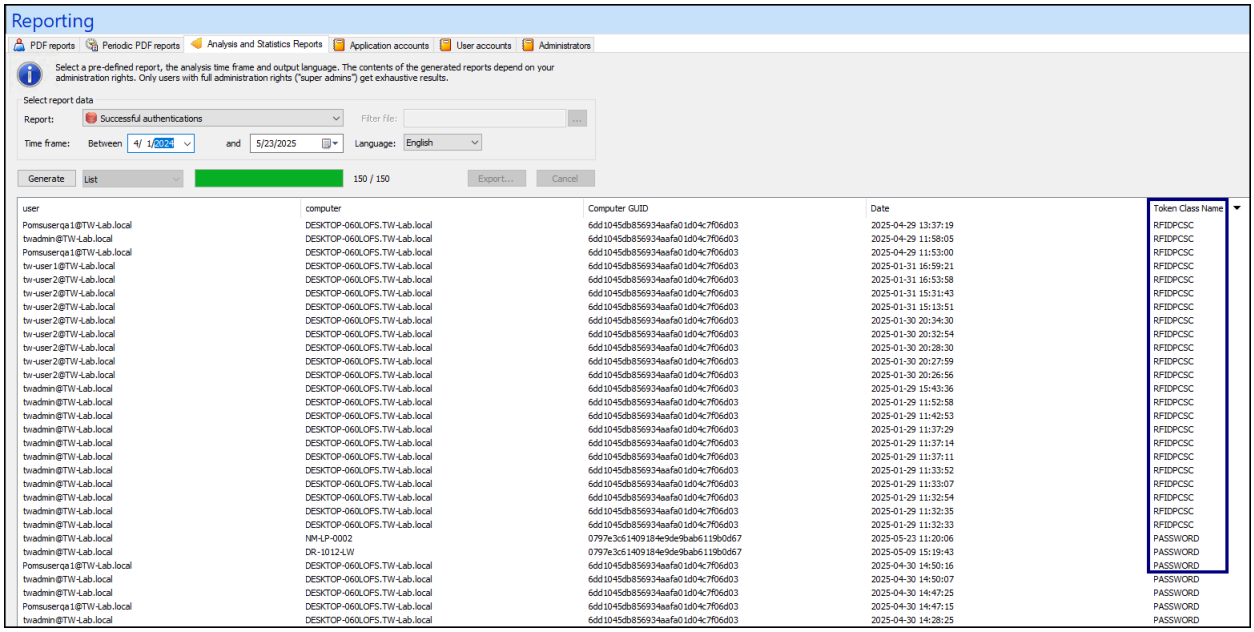
5. Click **`Generate`**, as shown in the following figure.



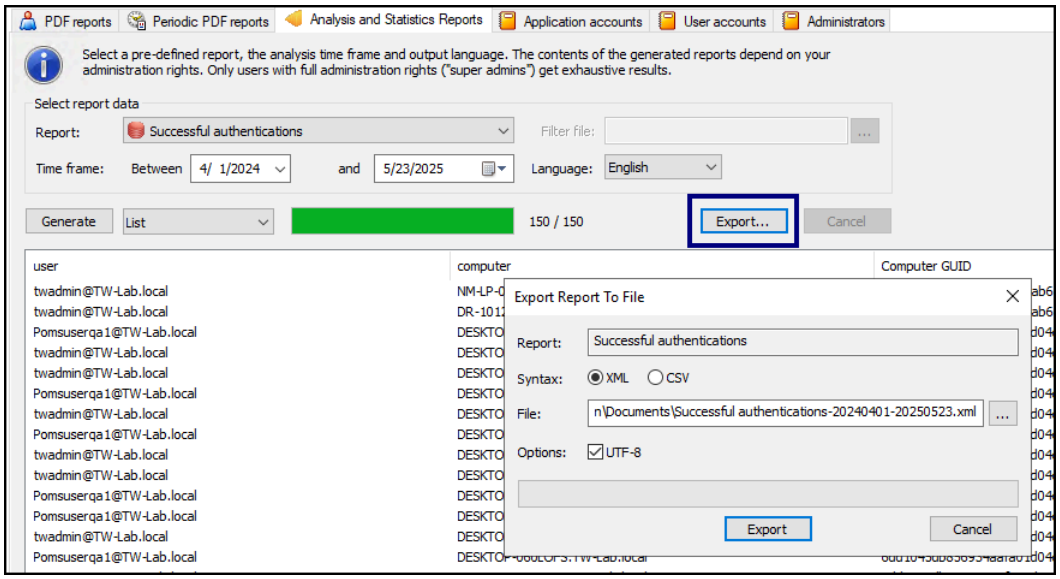
In the output, the value in the **`Token Class Name`** field identifies how the user completed the Evidian username and password window:

- Password—User typed their username and password.
- RFIDPCSC—User performed a Nymi Band tap.

The following figure provides an example of the output window.



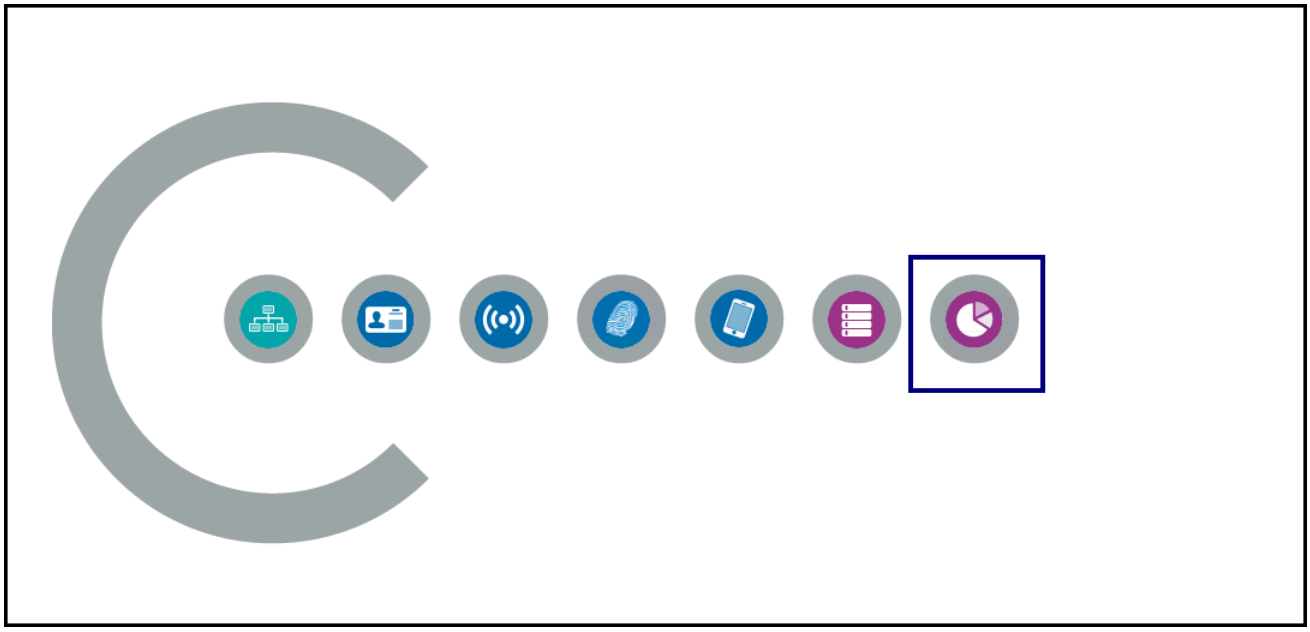
You can use the **`Export`** option to send the list to *XML* or *CSV* format.



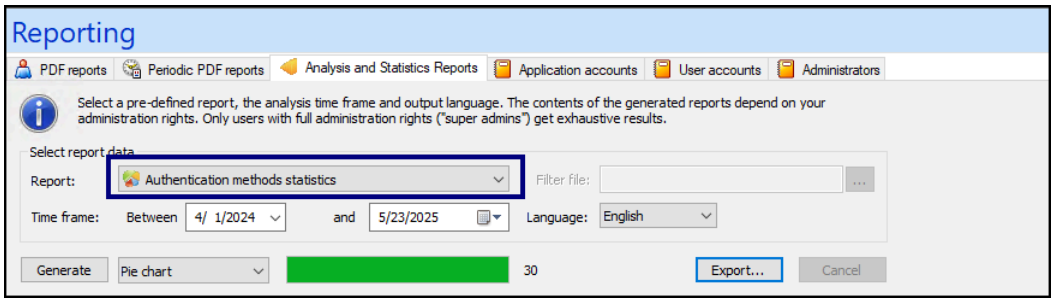
Comparing Total Nymi Band Taps vs Manual Username and Password Login

The Authentication method statistics allows you to determine when a user logs into an Evidian login window with their username and password, or a Nymi Band tap.

1. Log in to the Evidian EAM Management Console.
2. Click the **`Reporting`** icon, as shown in the following figure.



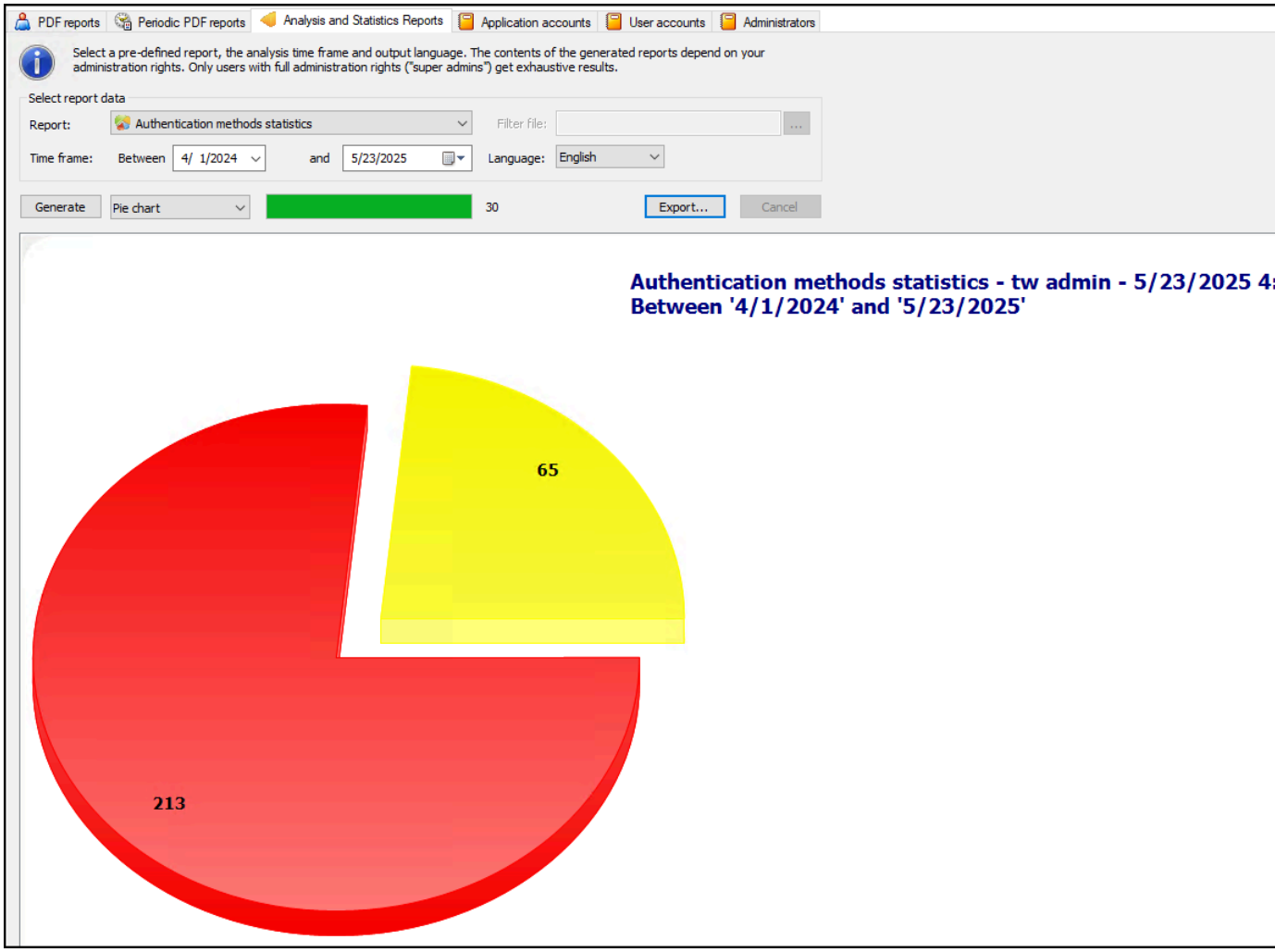
3. On the **`Analysis and Statistics Reports`** tab, from the **`Reports`** list, select **`Authentication method statistics`**, as shown in the following figure.



4. In **`Time frame`** fields, use the date selectors to choose the time range on which to report.
5. Click **`Generate`**.

The following figure provides an example of the pie chart output, where:

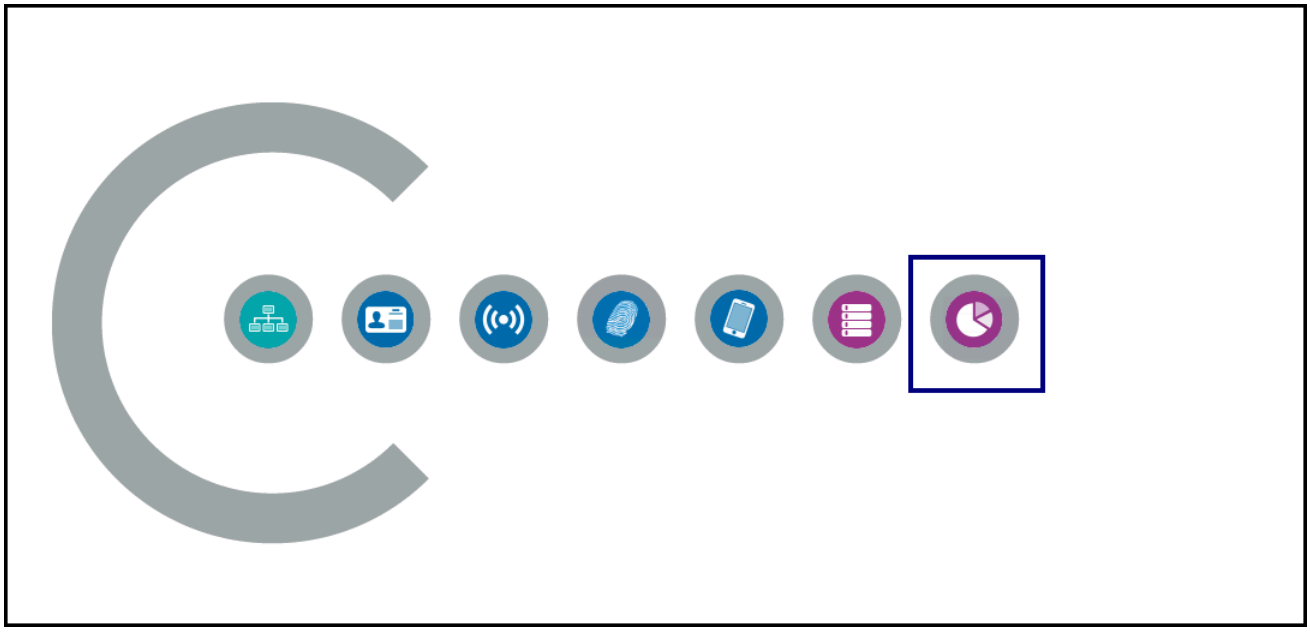
- Password—User typed their username and password.
- RFIDPCSC—User performed a Nymi Band tap.



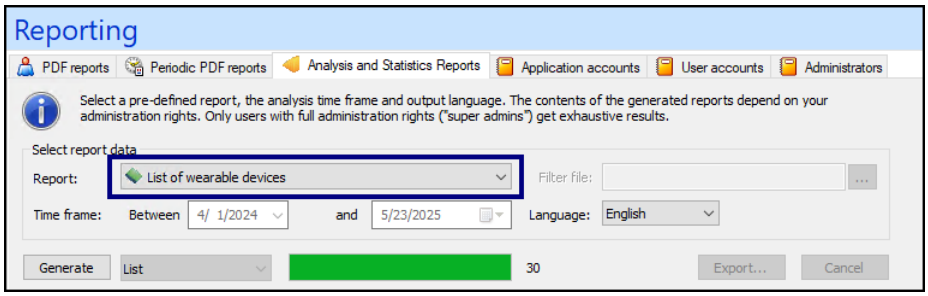
Viewing a list of Nymi Bands Enrolled in Evidian

The `List of Wearable Devices` report provides you with a list of Nymi Bands that have been enrolled to users in Evidian.

1. Log in to the Evidian EAM Management Console.
2. Click the **`Reporting`** icon, as shown in the following figure.



3. On the **`Analysis and Statistics Reports`** tab, from the **`Reports`** list, select **`Authentication method statistics`**, as shown in the following figure.

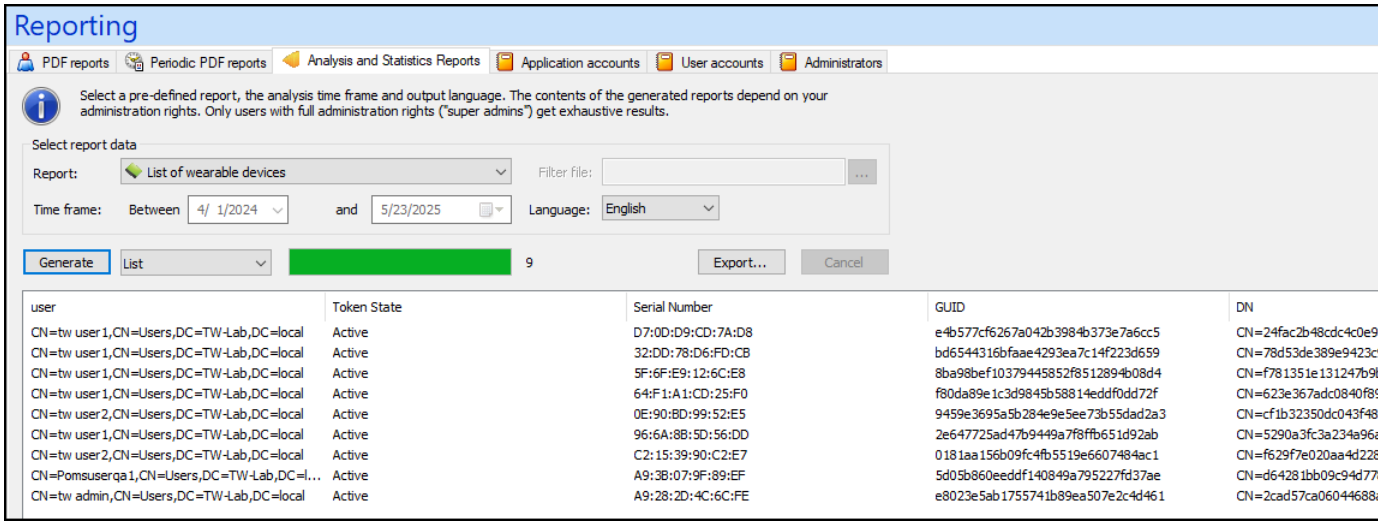


4. In **`Time frame`** fields, use the date selectors to choose the time range on which to report.
5. Click **`Generate`**.

The report provides you with information in the following columns:

- user—AD account associated with the Nymi Band.
- serial number—Serial number of the Nymi Band.
- Creation date (AD)—Date of Nymi Band enrollment.

The following figure provides an example of the output. In this example, users tw user1 and tw user2 have performed self re-enrollment several times and the report displays enrollment information for several different Nymi Bands.



5.15 - NES Backup and Recovery

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

This section assumes that you:

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

5.15.1 - NES Backups

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

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

5.15.2 - NES Database Backups

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

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

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

5.15.3 - NES Server and Database Recoveries

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

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

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

5.16 - Evidian EAM Controller Backup and Recovery

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

This section assumes that you:

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

5.16.1 - Evidian EAM Controller Backups

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

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

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

5.16.2 - Audit Database Backups

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

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

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

5.16.3 - Evidian EAM Controller Server and Audit Database Recoveries

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

Note: You cannot recover the following data:

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

6 - Changing the Evidian Authentication Method

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

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

6.1 - Changing Authentication Method From RFID-only to Wearable

Perform the following steps to change your environment from an RFID-only configuration to Wearable.

6.1.1 - Obtaining the TokenManagerStructure file for the Evidian EAM Controller

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

6.1.2 - Changing the Configuration of the Evidian EAM Controller

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

Procedure

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

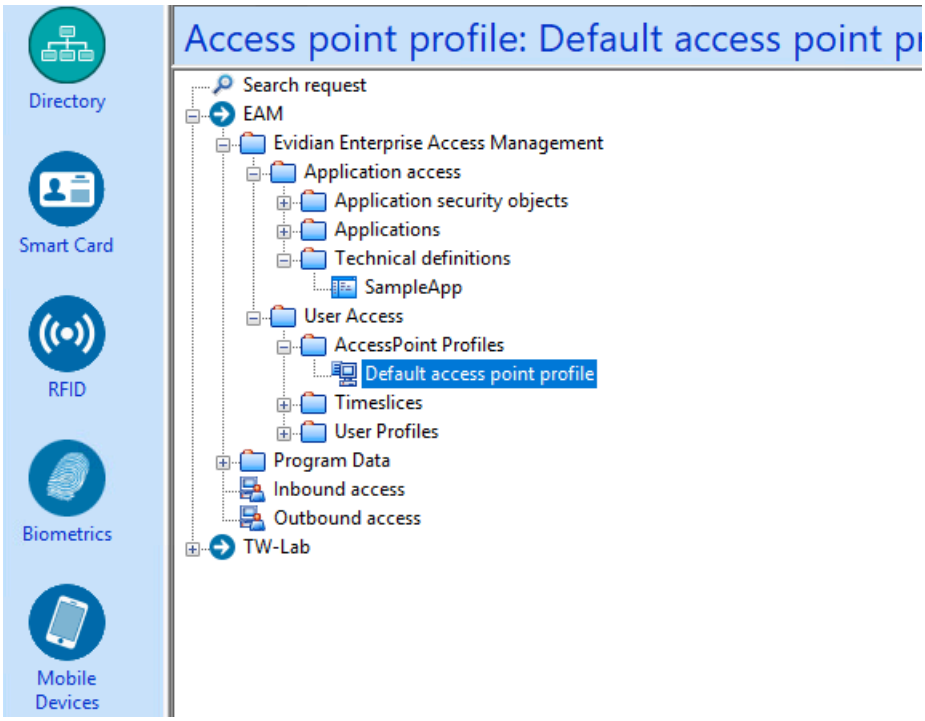


Figure 48: Default Access Point Profile

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

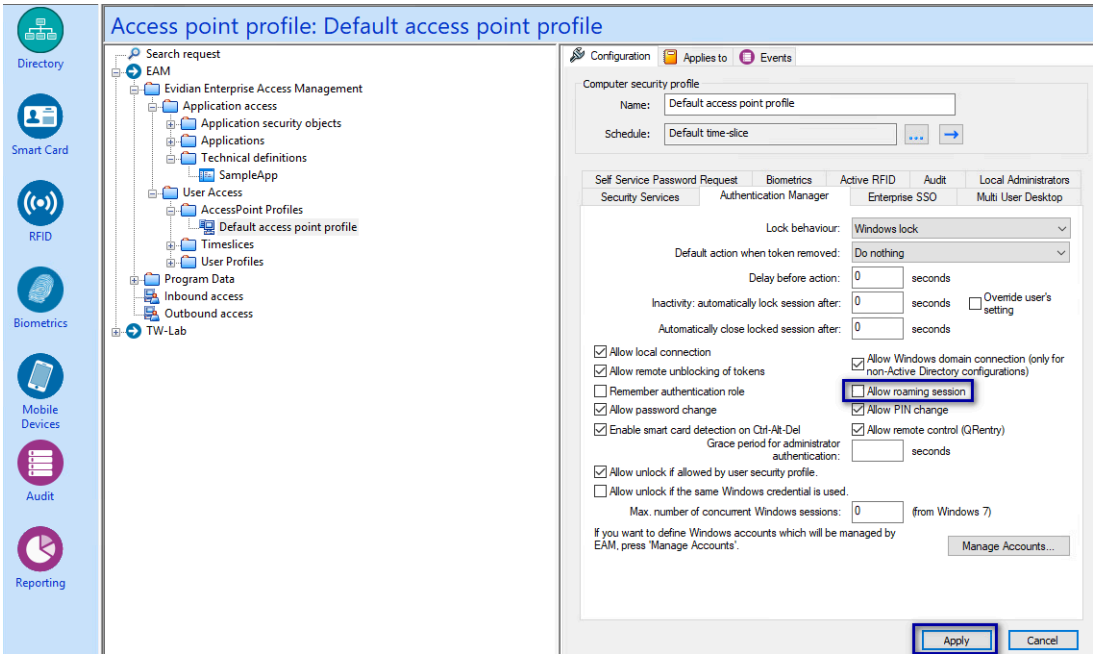


Figure 49: Authentication Manager window

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

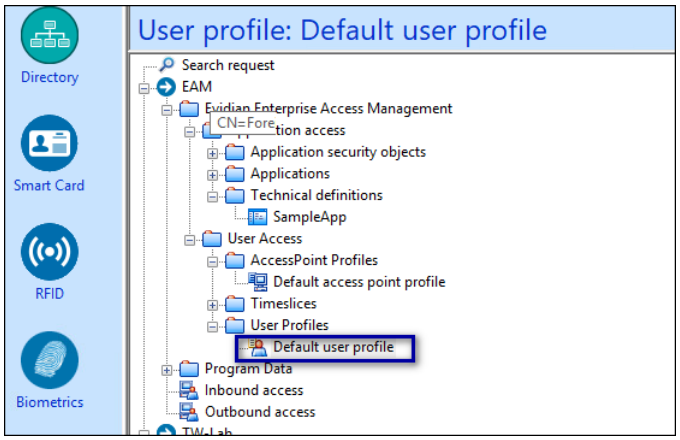


Figure 50: User Profiles

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

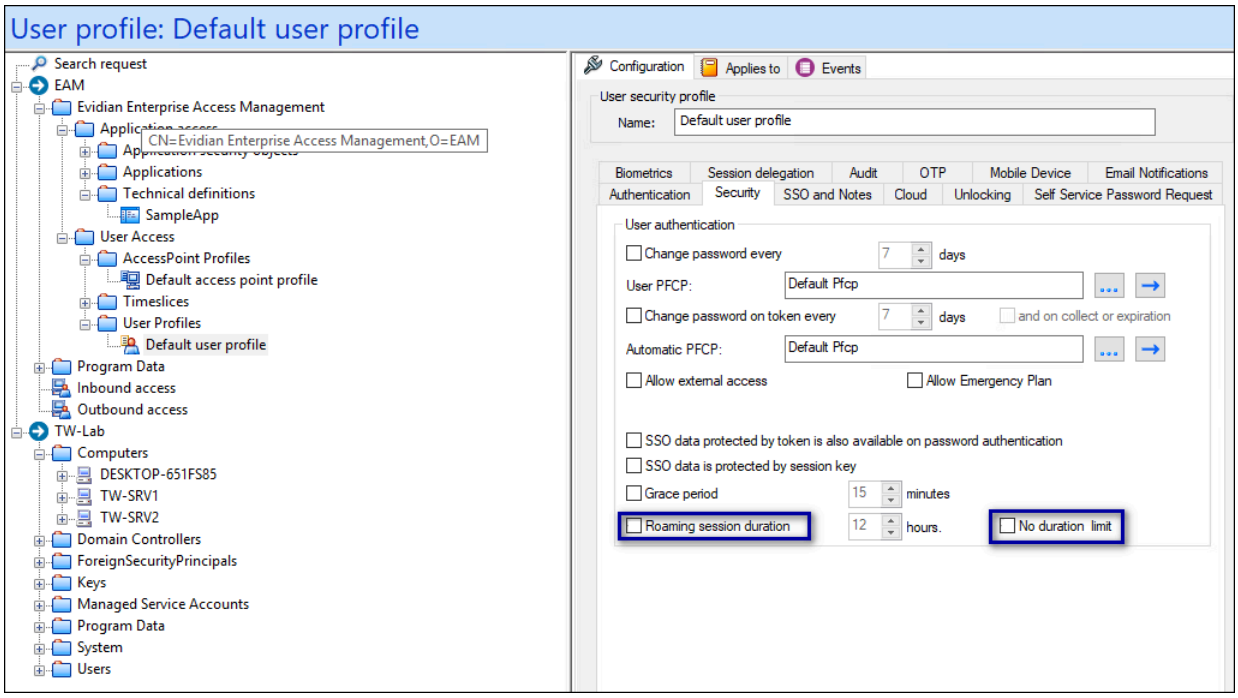
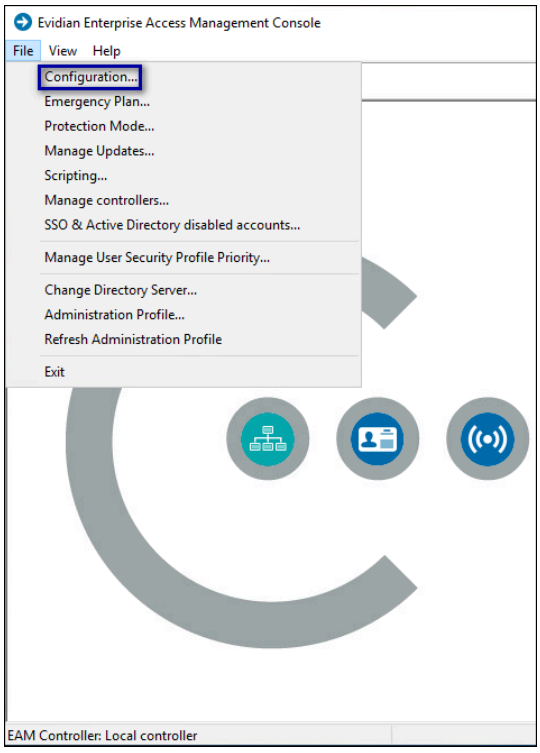
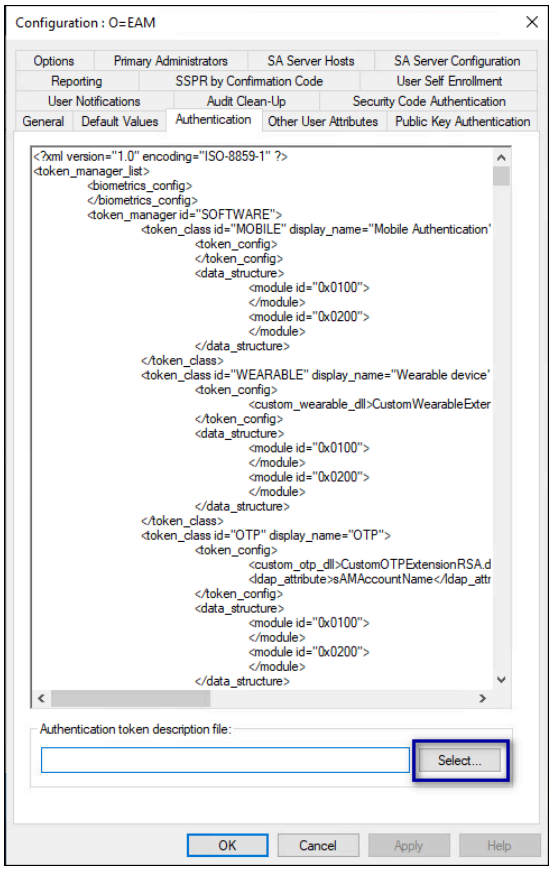


Figure 51: Roaming Session Duration Limit

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



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



9. In the `Open File` dialog, navigate to the directory that contains the Wearable TokenManagerStructure file, select the TokenManagerStructure file, and then click **`Open`**.
10. Click **`Apply`**, which will validate the structure of the file.
11. Click **`OK`**.
12. Close the Evidian EAM Management Console.

6.1.3 - Changing the Evidian EAM Client Configuration on User Terminals

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

About this task

Perform the following steps on each user terminal.

Procedure

1. Run `Registry Editor`.

2. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication*.
3. Right-click *RoamingSessionCached*, and then select **`Delete`**.
4. On the `Confirm Value Delete` window, click **`Yes`**.
5. Right-click the *RoamingSessionAllowedForSSO*, and then select **`Delete`**.
6. On the `Confirm Value Delete` window, click **`Yes`**.
7. Close `Registry Editor`.
8. From `File Explorer`, navigate to *C:\Program Files\Common Files\Evidian\WGSS* folder.
9. If the file exists, rename *TokenManagerStructure.xml* to *TokenManagerStructure_rfid.xml*

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

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

Procedure

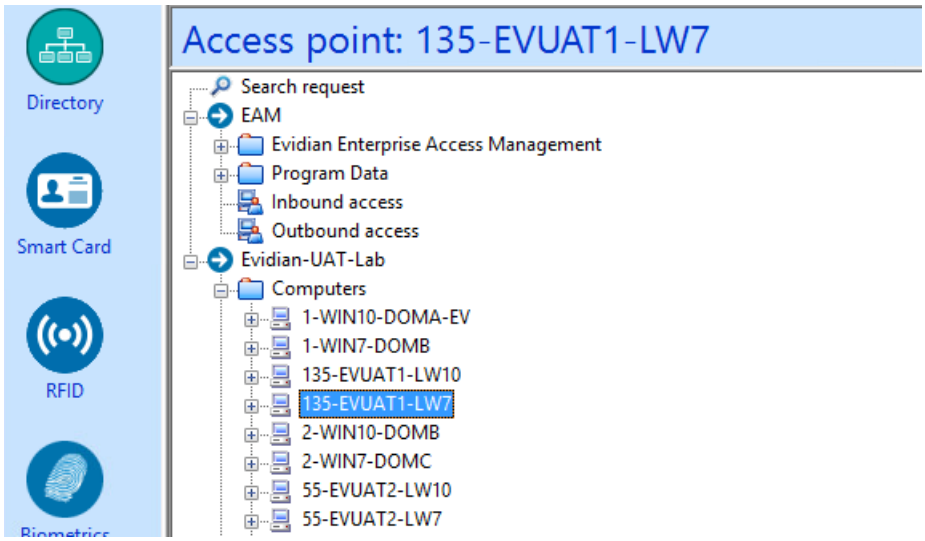
1. From `File Explorer`, navigate to *C:\Program Files\Common Files\Evidian\WGSS* folder.
2. Delete the *TokenManagerStructure.xml* file.
3. Close `File Explorer`.

6.1.5 - Deleting Evidian EAM Client Cache

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

Procedure

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



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

6.2 - Changing the Authentication Method from Wearable to RFID-only

Perform the following steps to change your environment from Wearable to RFID-only.

Your enrollment terminal remains in a wearable configuration.

6.2.1 - Obtaining the TokenManagerStructure files

You require both Token Manager Structure (TMS) files from the extracted Nymi installation package, in the *Evidian-Supplementary-Files* subdirectory.

Copy the following files to the following locations:

- *TokenManagerStructure-Nymi-RFID.xml* file to the Evidian EAM Controller.
- *TokenManagerStructure-Nymi-Wearable.xml* to the enrollment terminal.

6.2.2 - Changing the Configuration of the Evidian EAM Controller

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

Procedure

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

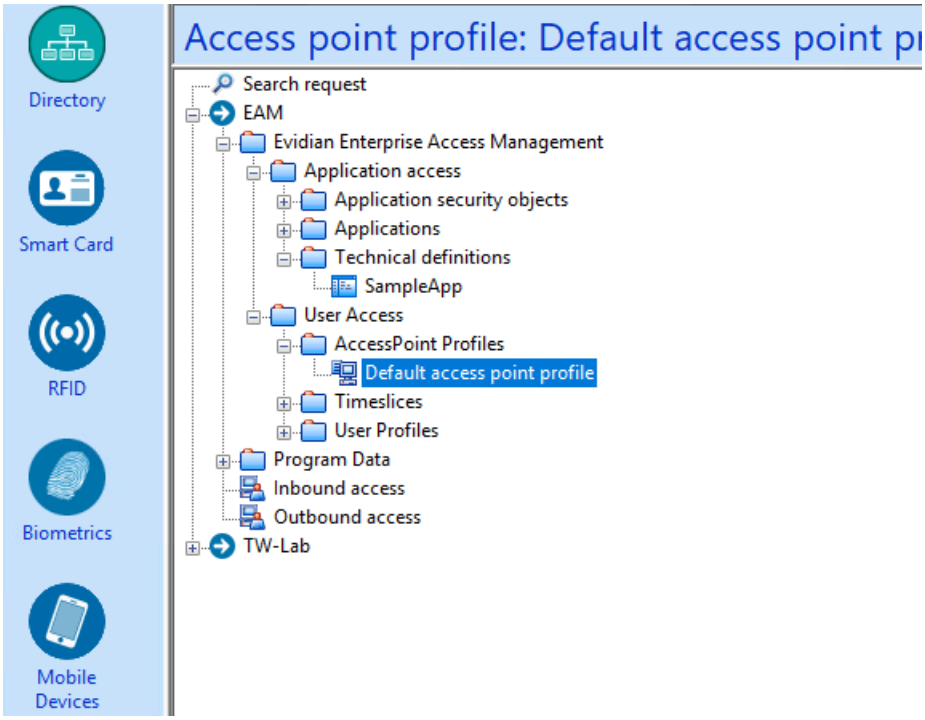


Figure 52: Default Access Point Profile

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

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

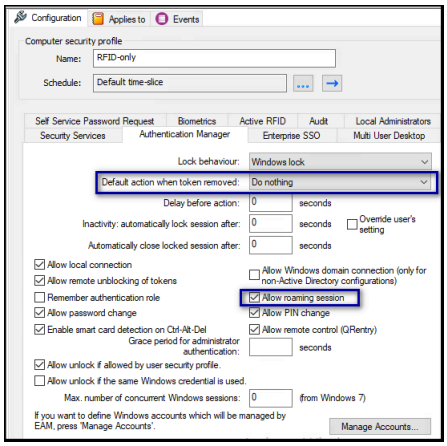


Figure 53: Authentication Manager window

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

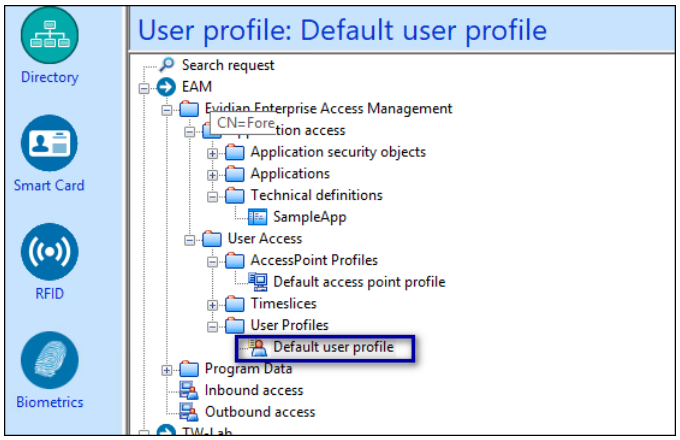


Figure 54: User Profiles

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

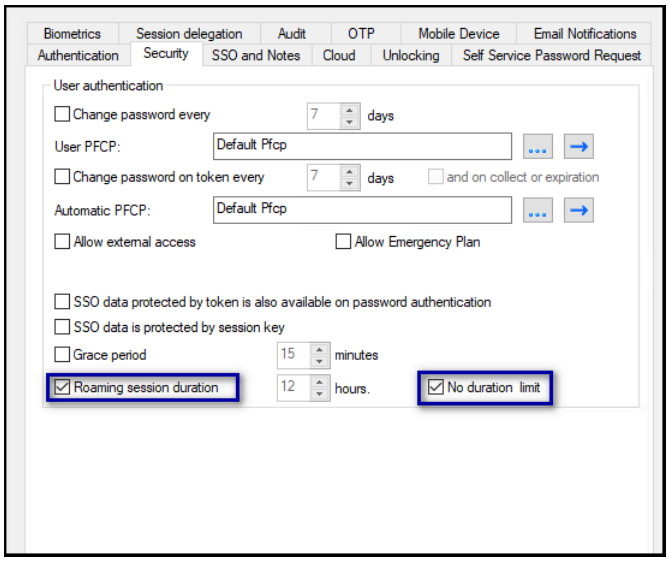
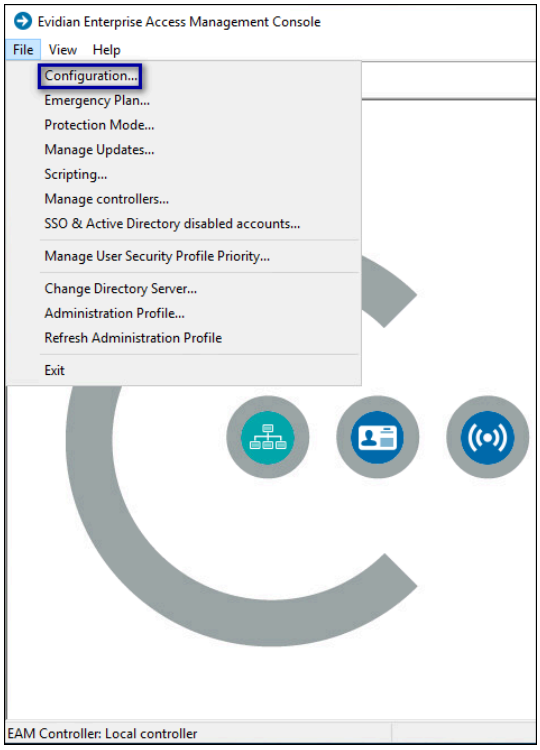
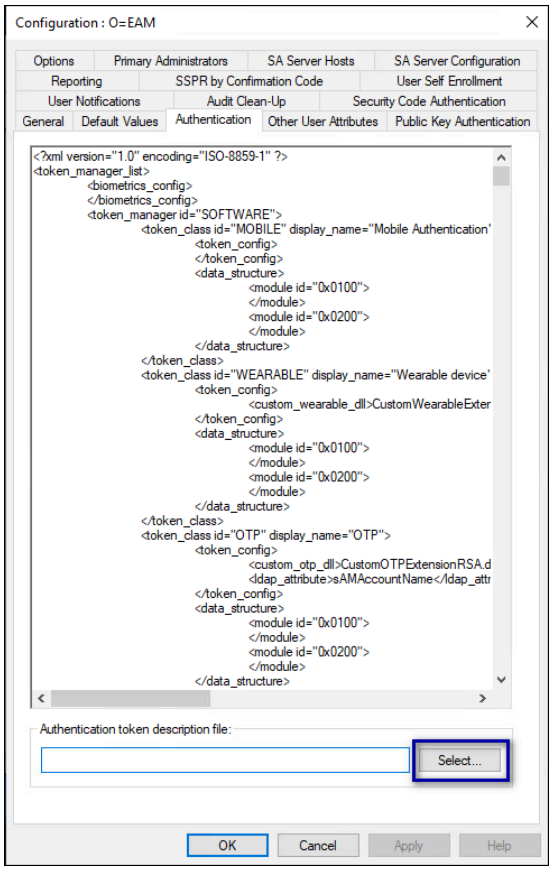


Figure 55: Roaming Session Duration Limit

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



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



9. In the `Open File` dialog, navigate to the directory that contains the RFID-only TokenManagerStructure file, select the TokenManagerStructure file, and then click **`Open`**.
10. Click **`Apply`**, which will validate the structure of the file.
11. Click **`OK`**.
12. Close the Evidian EAM Management Console.

6.2.3 - Changing the Evidian EAM Client Configuration on User Terminals

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

About this task

Perform the following steps on each user terminal.

Procedure

1. Run `Registry Editor`.

2. Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork*, and then perform the following actions.
   a) Right-click *Authentication*, and then select **`New > DWORD (32 bit)`**.
   b) Name the key *RoamingSessionAllowedForSSO*.
   c) Edit the key and in the value field, type ***1***.
   d) Right-click *Authentication*, and then select **`New > DWORD (32 bit)`**.
   e) Name the key *RoamingSessionCached*.
   f) Edit the key and in the value field, type ***1***.
   g) Navigate to *HKLM\SOFTWARE\Enatel\WiseGuard\FrameWork\Authentication*
   h) Right-click **`WearableNeedsRFID`**, and then select **`Delete`**.
   i) On the `Confirm Value Delete` window, click **`Yes`**.
3. Close `Registry Editor`.
4. From `File Explorer`, navigate to *C:\Program Files\Common Files\Evidian\WGSS* folder.
5. If the file exists, rename *TokenManagerStructure.xml* to *TokenManagerStructure_wearable.xml*

6.2.4 - Add Wearable TMS File to Enrollment Terminal

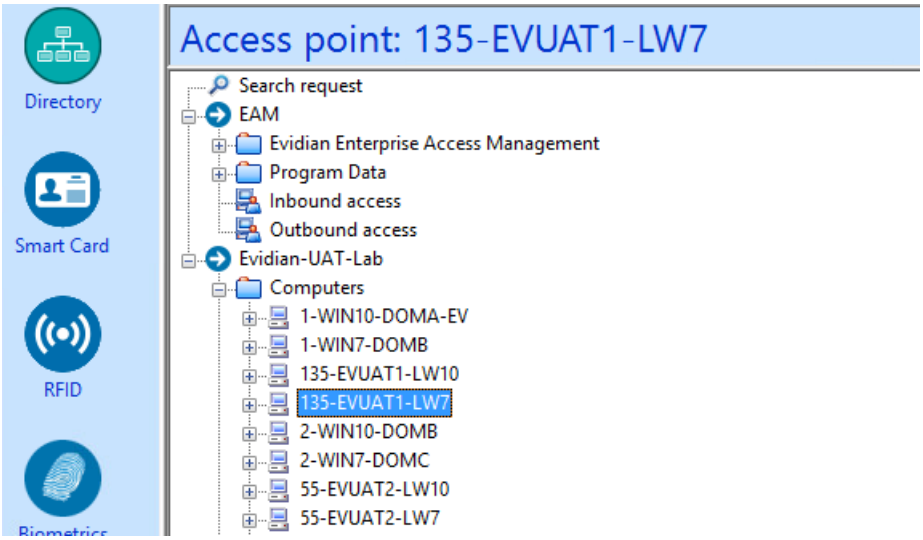
Configure the enrollment terminal to load a wearable token management structure file, when the default authentication method on the Evidian EAM Controller is RFID-only.

About this task

Perform these steps on the Enrollment Terminal.

Procedure

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



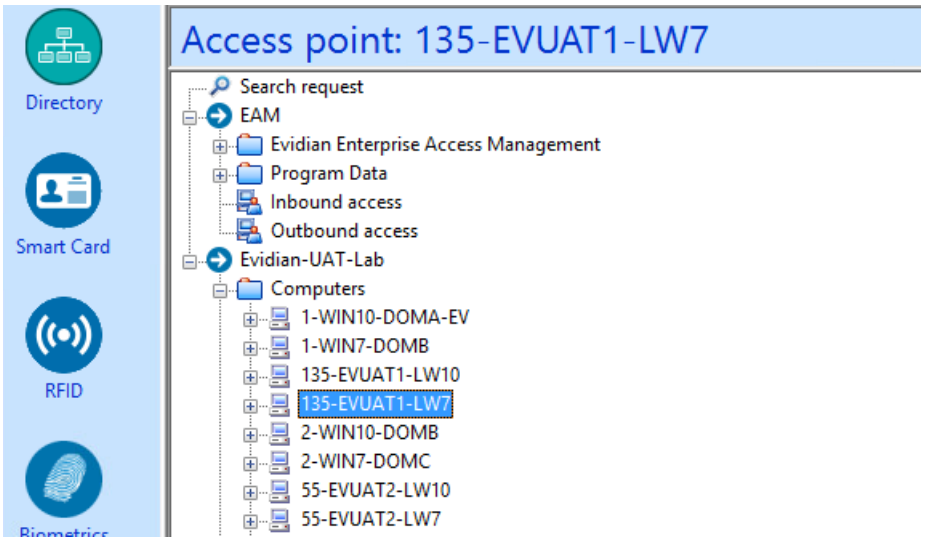
6. On the **`Actions`** tab, select **`Delete cache files`**, and then click **`Apply`**.
   The cache files are deleted on the terminal and the terminal desktop locks.

6.2.5 - Deleting Evidian EAM Client Cache

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

Procedure

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



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

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