ONE IDENTITY™

Wearable Device Authentication 9.0.2

User's Guide

Copyright 2017 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity do not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

⊗ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

⚠ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⓘ IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Wearable Device Authentication User's Guide
Updated - November 2017
Version - 9.0.2

Contents

Preface

Subject

This guide describes how to use the Primary account, Access to applications and Self Enrollment menus of the Enterprise Access Management (EAM) portal.

Audience

This guide is intended for end-users.

Required Software

EAM 9.0 evolution 2 and later versions. For more information about the versions of the required operating systems and software solutions quoted in this guide, please refer to One Identity EAM Release Notes.

Typographical Conventions

Bold Indicates:

- Interface objects, such as menu names, buttons, icons and labels.
- File, folder and path names.
- Keywords to which particular attention must be paid.

Italics - Indicates references to other guides.

`Code` - Indicates portions of program codes, command lines or messages displayed in command windows.

CAPITALIZATI ON Indicates specific objects within the application (in addition to standard capitalization rules).

< > Identifies parameters to be supplied by the user.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Documentation support

The information contained in this document is subject to change without notice. As our products are continuously enhanced, certain pieces of information in this guide can be incorrect. Send us your comments or suggestions regarding the documentation on the One Identity support website.

1

Wearable Device Overview

The IoT (Internet of Things) has allowed daily common devices, such as wearable devices, to communicate with each other to make our life easier and help us in our active lifestyle. The Nymi Band is one of them; a simple wrist band that can be easily worn for your daily activities. However, combined with the Enterprise Access Management solution of One Identity, the Nymi Band offers you much more.

Indeed, once you have activated your Nymi Band and followed the next steps of this guide, you will be able to log on to your Windows session securely and "hands-free".

Description

The Nymi Band as a solution for accessing your computer or tablet

Activate your Nymi Band and complete the enrollment procedure. Your wearable device is ready for computer access.

There is nothing to memorize, no Windows password to remember. Just select and validate the Password tile and you will be automatically authenticated wearing your activated Nymi Band.

The Nymi Band, for people who need a quick and secure access to their computer

The Nymi Band is a strong authentication device, ideal for retailers or bank branches that use tablets to authenticate and accelerate their daily tasks.

The Nymi Band is a biometric device that uses your ECG, unique to each person, to identify and authenticate you.

Before Starting

You need the following devices:

- A computer/tablet to log on.
- A smartphone with the Nymi Companion app installed.
- Your Nymi Band activated.

IMPORTANT: For more information on the Nymi Companion app and activating your Nymi Band, go to **https://nymi.com/**.

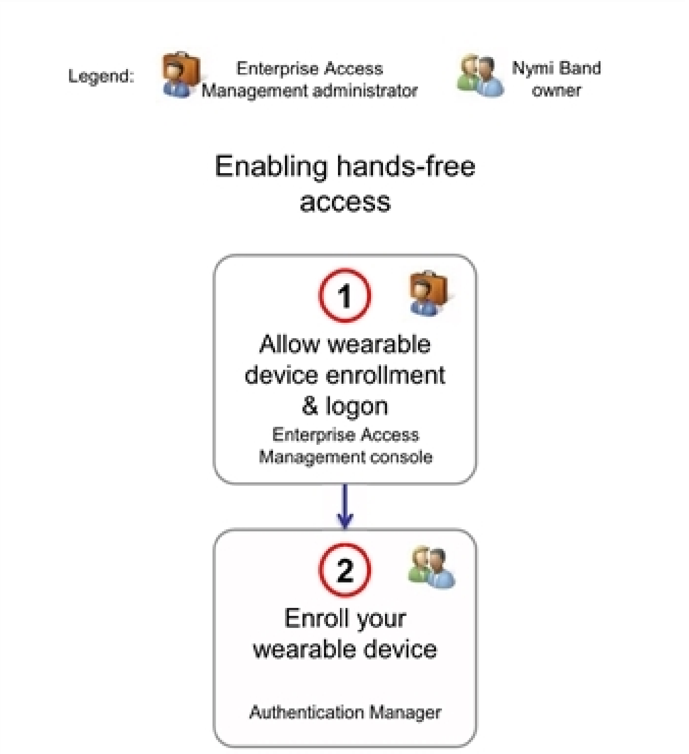
You must execute the following steps:

- Install the Nymi Bluetooth dongle on all the computers/tablets on which you want to log on.
- Install the following service on the same computer:
  Setup-Nymi Bluetooth Service.exe (contact a Nymi representative for more information).

Preparing the Wearable Device for Authentication Manager

The following schema shows the different steps to prepare a wearable device for Authentication Manager, which are:

1. Allowing Users to Enroll and Log on with a Wearable Device.
2. Enrolling your Wearable Device.


Legend:
Enterprise Access Management administrator
Nymi Band owner
Enabling hands-free access
1
Allow wearable device enrollment & logon
Enterprise Access Management console
2
Enroll your wearable device
Authentication Manager

Allowing Users to Enroll and Log on with a Wearable Device

Subject

This section is intended to Enterprise Access Management administrators. It explains how to configure the Enterprise Access Management console to allow users to use their wearable device with Authentication Manager.

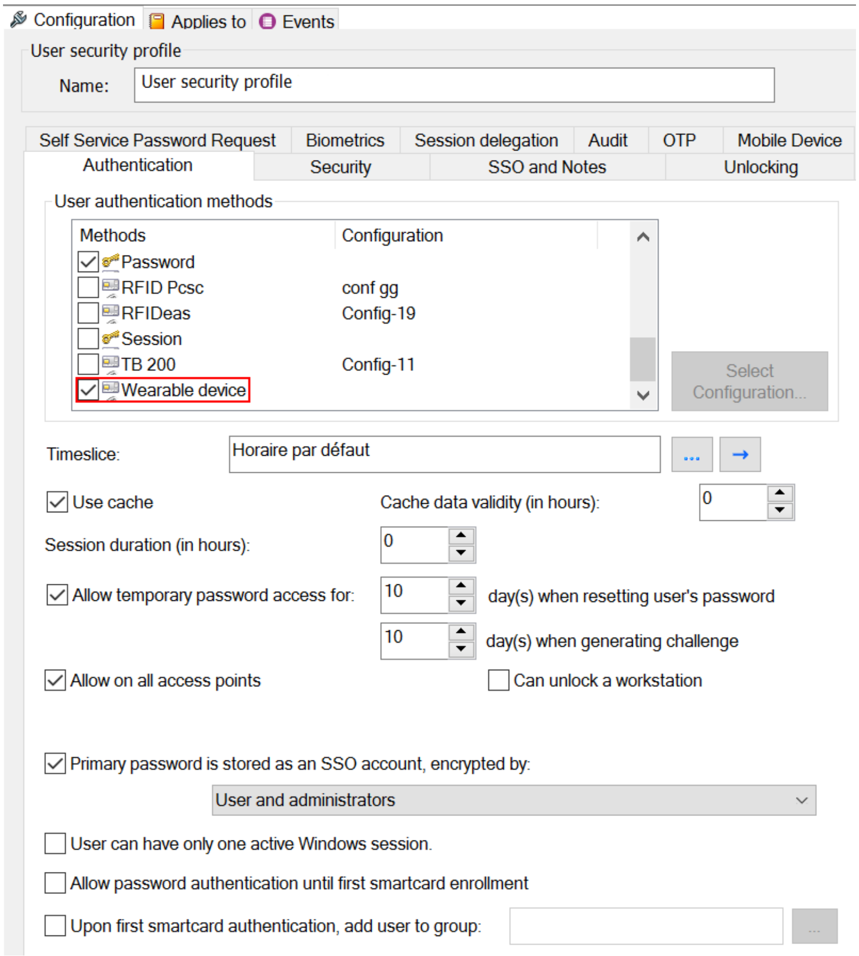
Before starting

You have the following administration role:

- In classic administration mode: **Smart Card administrator**.
- In advanced administration mode, your role must contain the following rights:
  - **User Security Profile: creation/modification**.
  - **Token: Modification**.

Procedure

1. In the Enterprise Access Management console, click the User Security Profile that contains the users for whom you want to allow the use of wearable devices for authentication.
2. In the **Authentication** tab, select the **Wearable device** method and **Apply**.



User security profile

Name: User security profile

User authentication methods

Methods	Configuration
☑ Password	
☐ RFID Pcsc	conf gg
☐ RFIDeas	Config-19
☐ Session	
☐ TB 200	Config-11
☑ Wearable device	

Timeslice: Horaire par défaut

☑ Use cache

Cache data validity (in hours): 0

Session duration (in hours): 0

☑ Allow temporary password access for: 10 day(s) when resetting user's password

10 day(s) when generating challenge

☑ Allow on all access points

☐ Can unlock a workstation

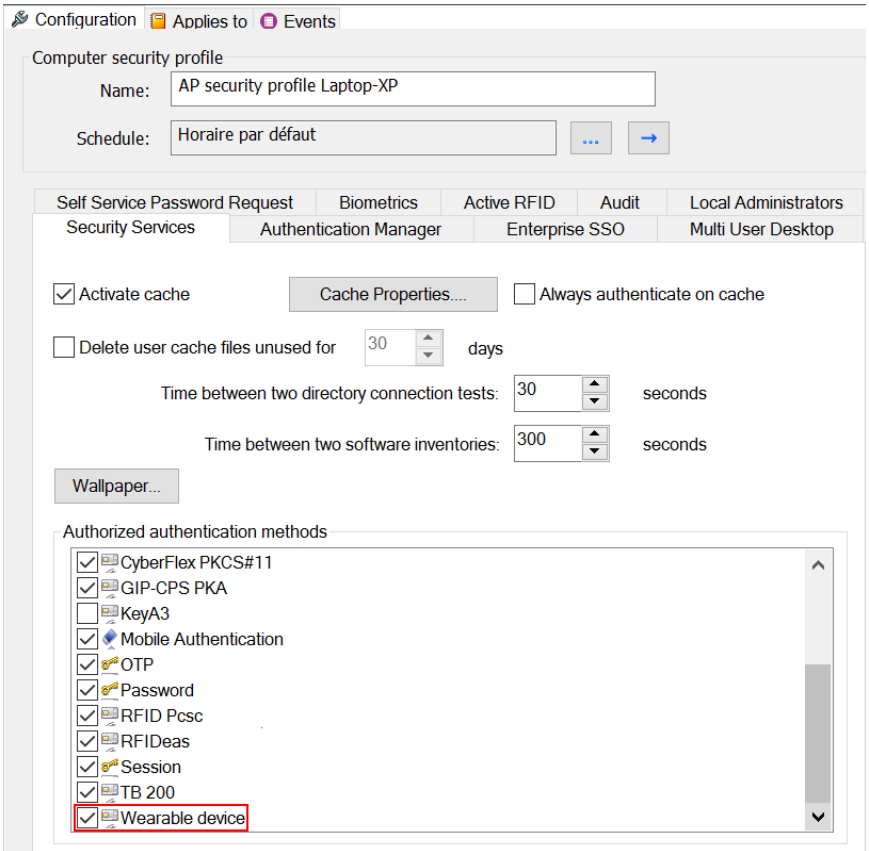
☑ Primary password is stored as an SSO account, encrypted by: User and administrators

☐ User can have only one active Windows session.

☐ Allow password authentication until first smartcard enrollment

☐ Upon first smartcard authentication, add user to group:

3. Click the Access Point Security profile that contains the access points for which you want to allow the use of wearable devices for authentication.
4. In the **Security Services** tab, select the **Wearable device** method and **Apply**.



Configuration | Applies to | Events

Computer security profile

Name: AP security profile Laptop-XP

Schedule: Horaire par défaut

Self Service Password Request | Biometrics | Active RFID | Audit | Local Administrators

Security Services | Authentication Manager | Enterprise SSO | Multi User Desktop

☑ Activate cache   Cache Properties....   □ Always authenticate on cache

□ Delete user cache files unused for 30 days

Time between two directory connection tests: 30 seconds

Time between two software inventories: 300 seconds

Wallpaper...

Authorized authentication methods

- ☑ CyberFlex PKCS#11
- ☑ GIP-CPS PKA
- □ KeyA3
- ☑ Mobile Authentication
- ☑ OTP
- ☑ Password
- ☑ RFID Pcsc
- ☑ RFIDeas
- ☑ Session
- ☑ TB 200
- ☑ Wearable device

The users are now authorized to enroll their wearable device.

Enrolling your Wearable Device

Subject

The enrollment of a wearable device is done through Authentication Manager.

Before starting

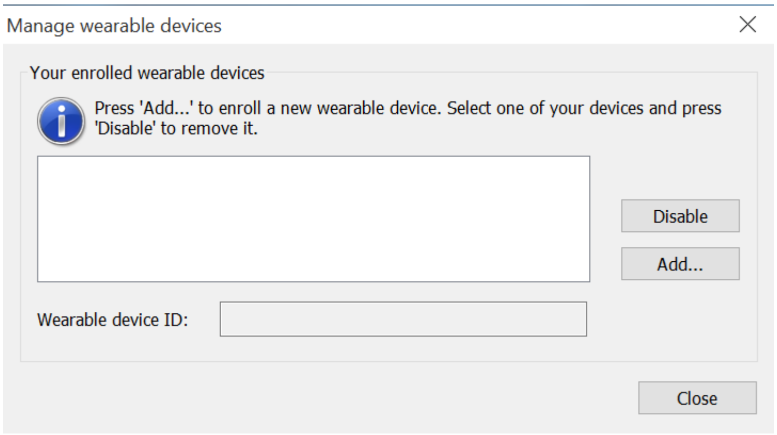
Your Nymi Band is activated.

Procedure

1. Right-click the **Authentication Manager** icon located in the notification area, and select **Manage Wearable Devices**.

NOTE: For security reasons, you will have to authenticate during the enrollment of your wearable device. It is a normal behavior.

The following window appears:



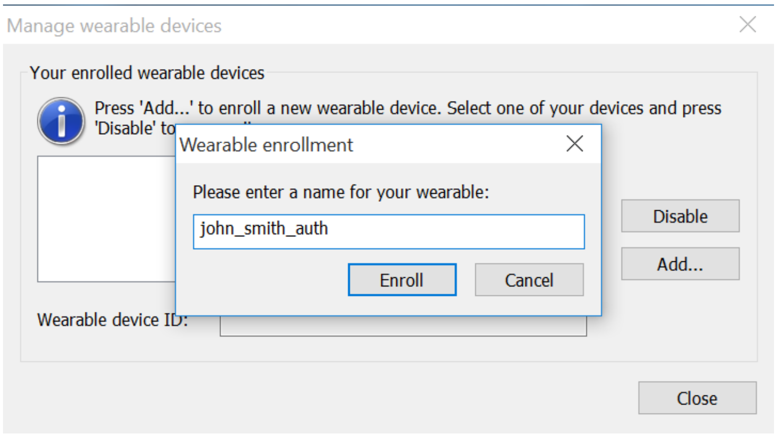
Manage wearable devices

Your enrolled wearable devices

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

Wearable device ID:

2. Click **Add**.
3. Enter a name for your wearable device.



Wearable enrollment

Please enter a name for your wearable: john_smith_auth

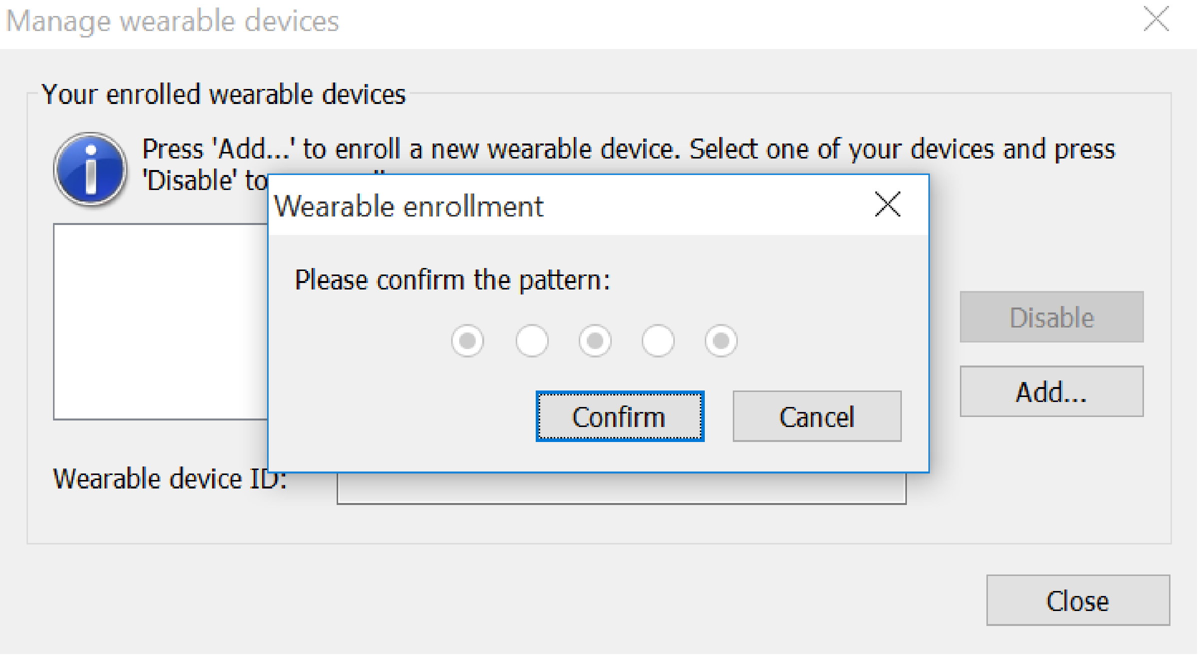
Manage wearable devices
Your enrolled wearable devices
Press 'Add...' to enroll a new wearable device. Select one of your devices and press 'Disable' to
Wearable device ID:
Enroll
Cancel
Disable
Add...
Close

4. Click **Enroll**.

   You Nymi Band is being searched.

5. To activate the enrollment of your Nymi Band, tap the top of your Nymi Band four times.

   An enrollment pattern appears.



Manage wearable devices

Your enrolled wearable devices

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

Wearable enrollment

Please confirm the pattern:

○ ○ ○ ○ ○

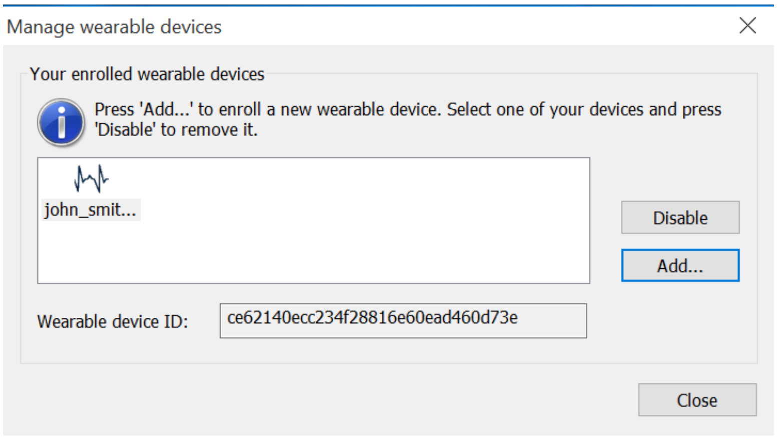
Wearable device ID:

At the same time, the corresponding pattern appears on your Nymi Band.

NOTE: If the enrollment patterns do not match, check to see whether another Nymi Band is being enrolled next to yours.

6. Click **Confirm**.

   Your Nymi Band is enrolled.



Manage wearable devices

Your enrolled wearable devices

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

john_smit...

Wearable device ID: ce62140ecc234f28816e60ead460d73e

IMPORTANT: When your wearable device is enrolled, you are ready to log on for hands-free access on all computers where the One Identity solution and the Nymi Bluetooth dongle are installed.

3

Authenticating with your Wearable Device

Subject

You can use your Nymi Band to log on to Windows or to log on to an application, as detailed in the following procedures.

Before starting

Your wearable device is enrolled and activated.

Logging on to Windows

Procedures

1. If required, press **Ctrl**+**Alt**+**Del**.

   The log on screen of the last authenticated user appears.

2. Click on **Other user** (or press **Esc**) to display the welcome screen.
3. Enter your user name and press **Enter**.

   Your Windows session starts.

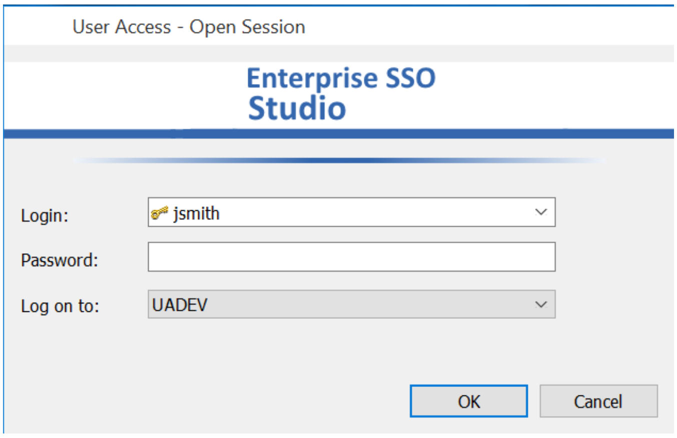
Logging on to an Application

The following procedure details how to log on to One Identity Enterprise SSO using your Nymi Band when starting manually this application.

1. In the **Start** menu, click **Programs/One Identity User Access/Enterprise SSO**.

   The authentication window appears.

2. In the **Login** field, select the password authentication method and press **Enter**.



User Access - Open Session

Login: jsmith

Password:

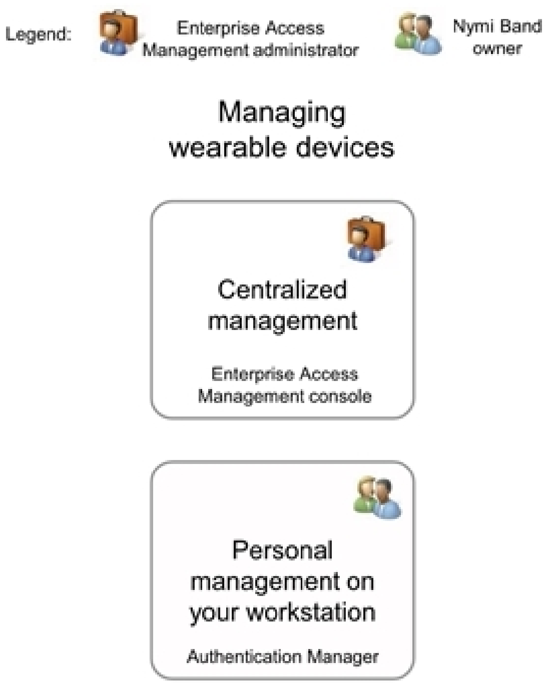
Log on to: UADEV

Enterprise SSO starts.

Managing Wearable Devices

This section describes all the tasks related to wearable devices management. Some tasks are restricted to the Enterprise Access Management administrator, while others can be performed by any Nymi Band user. These tasks are:

- Managing Wearable Devices from the Enterprise Access Management console.
- Managing wearable devices from the Authentication Manager tools.


Legend:
Enterprise Access Management administrator
Nymi Band owner
Managing wearable devices
Centralized management
Enterprise Access Management console
Personal management on your workstation
Authentication Manager

Managing Wearable Devices from the Enterprise Access Management console

Using the RFID management module

Subject

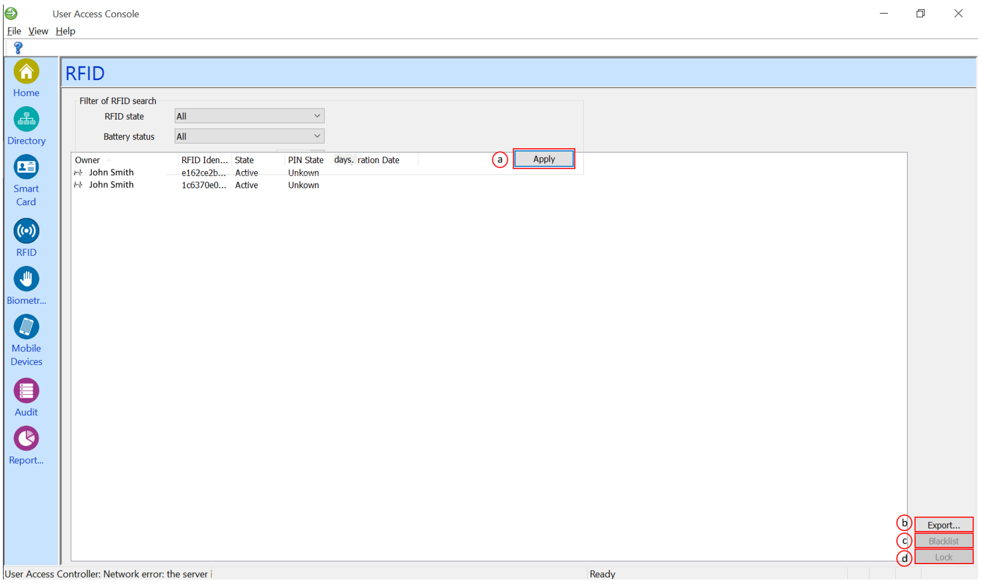
The Enterprise Access Management console includes an RFID management module, which is available from the welcome page. The wearable devices are managed from this module and allows you to:

- Display the list of the wearable devices already enrolled.
- Display the properties of each wearable device (owner, RFID identifier, device state).
- Export the list of wearable devices into a CSV file.
- Lock or unlock a wearable device.
- Blacklist or delete a wearable device form your configuration.

> NOTE: The wearable devices can be recognized by the ECG icon ⟿ in front of the owner's name..

Procedure

1. From the User Access console welcome page, click the **RFID management** button.
2. Click the **Apply** button to display the list of enrolled wearable devices:



Filter of RFID search

RFID state: All

Battery status: All

Owner	RFID Iden...	State	PIN State	days. ration Date
⟿ John Smith	e162ce2b...	Active	Unkown	
⟿ John Smith	1c6370e0...	Active	Unkown	

User Access Controller: Network error: the server i

Ready

a. To filter the wearable devices to display, select the filter you want and click **Apply**.

b. To export the list of wearable devices, click **Export**.

c. To blacklist/delete a device, select it in the list and click **Blacklist**/**Delete**.

d. To lock/unlock one or more wearable devices, select them and click **Lock**/**Unlock**.

Hint

Double-click a listed wearable device to browse to the wearable device.

Using the directory management module

Subject

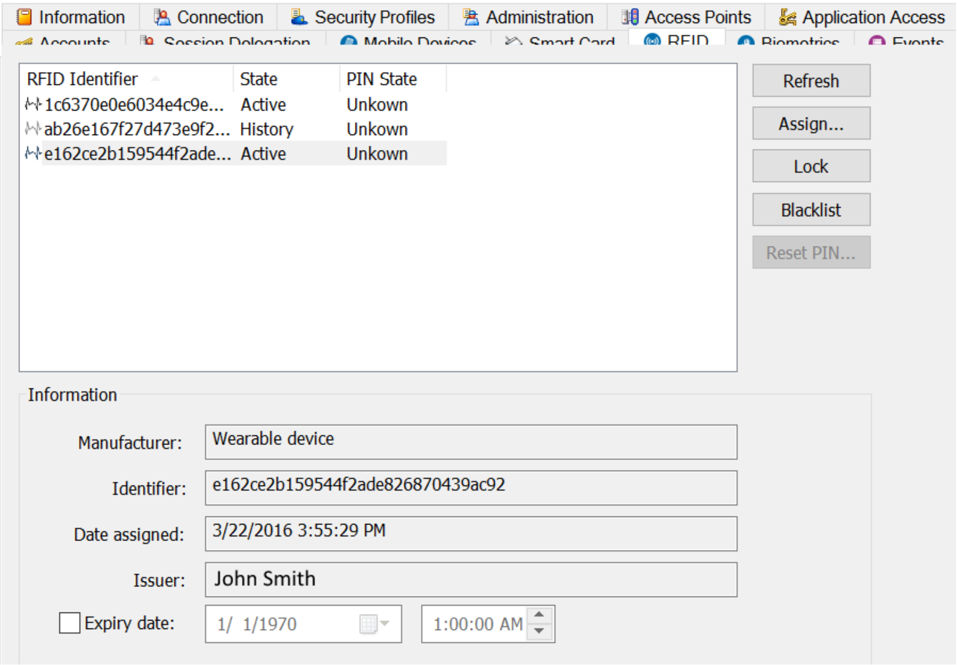
For a selected user, the **RFID** tab contains his wearable device(s) and by selecting one, the following information is displayed:

- The wearable devices enrolled for computer access.
- The properties of each wearable device (RFID Identifier, State...).
- You can also use this tab to lock or disable a user’s wearable device.

Window description

ℹ NOTE:To display the following tabbed panel, browse or search the tree structure of the **Directory** panel to the wanted user object and select it to display the **RFID** tab.

RFID Tab



RFID Identifier	State	PIN State
1c6370e0e6034e4c9e...	Active	Unkown
ab26e167f27d473e9f2...	History	Unkown
e162ce2b159544f2ade...	Active	Unkown

Information

Manufacturer: Wearable device

Identifier: e162ce2b159544f2ade826870439ac92

Date assigned: 3/22/2016 3:55:29 PM

Issuer: John Smith

□ Expiry date: 1/ 1/1970 1:00:00 AM

Table 1: RFID tab

Button	Description
Refresh	Updates the list of displayed wearable devices.
Assign	Not applicable.
Lock/Unlock	Locks or unlocks a wearable device.
Blacklist/Delete	Blacklists or deletes a wearable device form the configuration.
Reset PIN	Not applicable.

Managing wearable devices from the Authentication Manager tools

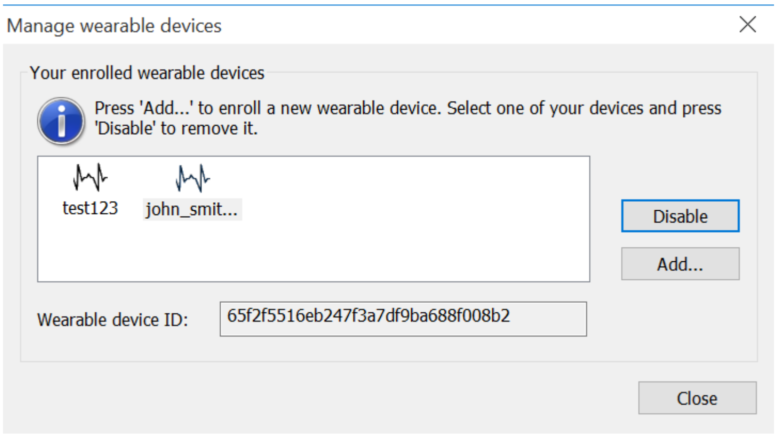
Subject

You can manage by yourself your wearable device(s) enrollment directly from your computer, using the Authentication Manager tools. A dedicated interface allows you to:

- Enroll a new wearable device. This feature is detailed in Enrolling your Wearable Device.
- Disable a wearable device.
- Display information about your wearable devices.

Window description

NOTE: To display the following window, right-click the Authentication Manager icon located in the notification area and select **Manage Wearable Devices**.



Manage wearable devices

Your enrolled wearable devices

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

Wearable device ID: 65f2f5516eb247f3a7df9ba688f008b2

Table 2: Manage wearable devices

Item	Description
Your enrolled wearable devices area	This area displays the wearable devices associated with this user.
Disable button	Disables the selected wearable device. The user can no longer use this device to log on.
Add button	Starts the enrollment for a new wearable device. For details, see Enrolling your Wearable Device.
Wearable device ID	Private key ID of the selected wearable device, used only for debugging purposes.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product