

ENTERPRISE ACCESS MANAGEMENT



Enterprise Access Management 10.0 Evolution 3 Release Notes

39 A2 25MC 08

March 2024



Copyright © Evidian, 2020-2024

The trademarks mentioned in this document are the property of their respective owners. The terms Evidian, AccessMaster, SafeKit, OpenMaster, SSOWatch, WiseGuard, Enatel, CertiPass and QReentry are trademarks registered by Evidian.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical or otherwise without the prior written permission of the publisher.

Evidian disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customer. In no event is Evidian liable to anyone for any indirect, special, or consequential damages.



The information and specifications in this document are subject to change without notice. Consult your Evidian Marketing Representative for product or service availability.

Preface

- Subject** This document provides information relating to the release of Enterprise Access Management 10.0 Evolution 3.
- Audience**
- System integrators.
 - Administrators.
- Required Software** Enterprise Access Management Services 10.0 Evolution 3 and later versions.

Typographical Conventions

This guide uses the following conventions:

Bold	Indicates: <ul style="list-style-type: none">○ Interface objects such as menu names, labels, buttons and icons.○ File, directory and path names.○ Keywords to which particular attention must be paid.
<i>Italics</i>	Indicates references to other guides.
Monospace	Indicates portions of program codes, command lines, or messages displayed in command windows.
CAPITALIZATION	Indicates specific objects (in addition to standard capitalization rules) within the application.
 Note	Notes contain additional information such as a comment or clarification on the subject.
 Important	Important tags contain warnings or cautions to prevent data loss and essential information to complete the task.
Change bars	Change bars are vertical lines that identify new or revised text from the previous version of the guide.

If you have any comments or questions related to this documentation, please mail us at Institute@Evidian.com

Contents

1. What is new in Enterprise Access Management version 10 evolution 3?	1
1.1 General.....	1
1.2 Web Portal.....	1
1.3 Authentication Manager	1
1.3.1 HID Seos.....	1
1.4 EAM Console	2
1.4.1 Handling of POST method for sending SMS and taking into account Rest API using header.....	2
1.4.2 Improve security for Mobile device	4
1.5 Enterprise SSO	5
1.5.1 Making technical definitions without Internet Explorer	5
1.5.2 Password Vault.....	8
2. What is new in Enterprise Access Management version 10 evolution 2?	10
2.1 Web Portal.....	10
2.1.1 Help-Desk feature.....	10
2.1.2 Customization of Web Portal	10
2.1.3 Web Portal for DMZ.....	10
2.2 Web Service (SOAP) Proxy for DMZ.....	10
2.3 EAM Console	11
2.3.1 Display in the ""Applies to" tab.....	11
2.3.2 Copy in the Other User Attribute Dialog Box.....	11
2.3.3 Navigation inside EAM Console	11
2.3.4 Scripting improvements	11
2.3.5 Wearable reports	11
2.4 Enterprise SSO	12
2.4.1 Support of Edge-Chromium	12

- 2.4.2 Password Vault 12
- 2.4.3 Studio 12
 - 2.4.3.1 Saving dialog box size 12
 - 2.4.3.2 Regular expression 12
 - 2.4.3.3 Deactivate a Window of an application 12
 - 2.4.3.4 Test mode 13
 - 2.4.3.5 4 eyes improvement 13
 - 2.4.3.6 NetWeaver Business Client 6.5 13
 - 2.4.3.7 Focus and Java based application 13
 - 2.4.3.8 Making technical definitions without Internet Explorer 13
- 2.5 Authentication Manager 16
 - 2.5.1 Tiles 16
 - 2.5.1.1 Password Credential provider 16
 - 2.5.1.2 Customization 16
 - 2.5.1.3 Automatic repair 16
 - 2.5.2 Credential Manager 16
 - 2.5.3 SSPR 16
 - 2.5.3.1 Mask answers 16
 - 2.5.3.2 Reset password with QReentry in Web Portal 17
- 2.6 QReentry 17
 - 2.6.1.1 Autofill 17
 - 2.6.1.2 NFC Authentication (Currently Android Only) 17

3. What is new in Enterprise Access Management version 10 evolution 1? 18

- 3.1 Enterprise SSO 18
 - 3.1.1 Firefox Web extension 18
 - 3.1.2 macOS 18
 - 3.1.3 as a Service 18
- 3.2 Authentication Manager 19
 - 3.2.1 Second authentication factor 19
 - 3.2.2 Push notification 19
 - 3.2.3 Nymi band version 2 19
- 3.3 Miscellaneous 19
 - 3.3.1 EAM Monitoring module 19
 - 3.3.2 Audit 19

4. What is new in Enterprise Access Management version 10? 20

- 4.1 Enterprise SSO 20
 - 4.1.1 GUI 20

4.1.2	macOS	20
4.1.3	Chrome	20
4.1.4	as a Service	20
4.2	Authentication Manager	21
4.2.1	Self-Service Password Request (SSPR)	21
4.2.2	QRentry enrollment.....	21
4.2.3	Multi-User Desktop	21
4.2.4	RsUserAuth.....	21
4.3	Miscellaneous	21
4.3.1	EAM Console and administration rights	21
4.3.2	Audit.....	22

5. Technical details 24

5.1	Operating system prerequisites	24
5.1.1	Agents environment.....	24
5.1.2	Controllers environment.....	25
5.1.3	Citrix / XenApp	25
5.1.4	VMWare Horizon Client version.....	25
5.1.5	Hardware prerequisites.....	26
5.1.5.1	Enterprise SSO, Authentication Manager	26
5.1.5.2	Enterprise Access Management Console and controller	26
5.1.5.3	Audit base	26
5.1.5.4	Reporting.....	27
5.1.5.5	Reporting database	27
5.2	LDAP directories and databases versions	27
5.2.1	LDAP directory versions	27
5.2.2	Database versions	29
5.2.3	Link with Identity & Access Manager.....	29
5.3	Supported authentication devices.....	29
5.3.1	Smart cards and USB tokens	29
5.3.2	Biometric devices.....	31
5.3.2.1	Using UPEK	31
5.3.2.2	Using Hitachi	32
5.3.3	RFID/HID devices	32
5.4	Enterprise SSO plug-in requirements	33
5.4.1	General requirements	33
5.4.2	SAP R/3 plug-in requirements	34

- 5.5 Supported HTTP server34
- 5.6 Encryption methods35
- 5.7 Supported Gemalto SA Server version.....35
- 5.8 Configuring the HLLAPI plug-in35
- 5.9 Supported languages36
- 5.10 Reporting service requirements37
- 5.11 Warnings37
 - 5.11.1 Updating Enterprise Access Management modules37
 - 5.11.2 APACHE server update from EAM evolution 2 (or less) to EAM evolution 3.....37
 - 5.11.3 Integrating an application with the HLLAPI plug in.....37
 - 5.11.4 Integrating a third-party Card Management System (CMS).....38
 - 5.11.5 Enterprise SSO with Novell NetWare38
 - 5.11.6 Enterprise SSO Internet Explorer plug-in warnings.....39
 - 5.11.7 Microsoft Edge plug-in warnings.....39
 - 5.11.8 macOS Enterprise SSO web extension.....39
 - 5.11.9 Some features are available in English language only.....39
 - 5.11.10 Reporting functionality & Languages.....39
 - 5.11.11 Reporting functionality & Audit.....39
- 5.12 Restrictions40
 - 5.12.1 Restrictions of Evolution 3 Patch Level 140
 - 5.12.2 Windows Active Directory inter-domain support with Enterprise Access Management in temporary restriction40
 - 5.12.3 Active Directory multi-domain and multi-forest40
 - 5.12.4 eDirectory.....41
 - 5.12.5 LDAP accounts used by Enterprise Access Management controllers must not expire..41
 - 5.12.6 Other limitations41
 - 5.12.7 Java plug-in.....41
 - 5.12.8 QRentry or Enterprise SSO for mobile devices42
 - 5.12.9 Enterprise Access Management Console42
 - 5.12.10 Web Portal: Help-Desk feature42
 - 5.12.11 Verification of the Unique Identifier of the mobile device during enrolment42
- 6. Documentation.....43**

1. What is new in Enterprise Access Management version 10 evolution 3?

1.1 General

EAM is now built using Microsoft Visual Studio 2019. For the proper functioning of the software suite, it is necessary to have at least the redistributable Microsoft Visual C++ 2015-2019 version 14.29.30133.

1.2 Web Portal

QRentry connected mode enrollment (smartphone connected and able to join the EAM web service) by a single QR code to scan from the web portal is now available.

1.3 Authentication Manager

1.3.1 HID Seos

New Seos compatible devices (like HID Seos cards/badges, Nymi bands v.3, etc) can be use with EAM solution as authentication tokens within RFID PCSC authentication method. The configuration thru Quickinstall is not yet available.

To add these token, refer to the Evidian EAM Console Administrator' Guide, chapter 18.1 and uncomment or add the following part to the default configuration file:

```
<!-- HID Seos -->
```

```
<token_atr>
```

```
<token_atr_value>3b80800101</token_atr_value>
```

```
<token_atr_mask> ffffffff</token_atr_mask>
```

```
</token_atr>
```

A special case is the HID Prox card, which is Seos compatible but with a different ATR, that is already defined in the default configuration:

```
<token_atr>  
<!-- HID Prox Seos -->  
<token_atr_value>3B8F8001804F0CA000000306400000000000028</token_atr_value>  
<token_atr_mask>ffffffffffffffffffffffffffffffff</token_atr_mask>  
</token_atr>
```

1.4 EAM Console

1.4.1 Handling of POST method for sending SMS and taking into account Rest API using header

From the EAM Console you can now add header templates for SMS sending configuration.

What is new in Enterprise Access Management version 10 evolution 3?

Configuration : DC=x03,DC=lan

Options	Primary Administrators	SA Server Hosts	SA Server Configuration	
Reporting	SSPR by Confirmation Code	User Self Enrollment		
User Notifications	Audit Clean-Up	Security Code Authentication		
General	Default Values	Authentication	Other User Attributes	Public Key Authentication

User contact name

Import from existing feature:

SMTP Server:

Port:

Default messaging configuration

Secure connection using: TLS SSL

Authenticate to SMTP Server as:

Password:

Sender's (and reply to) address:

Email address LDAP attribute:

Mobile phone LDAP attribute:

URL for SMS:

Proxy:

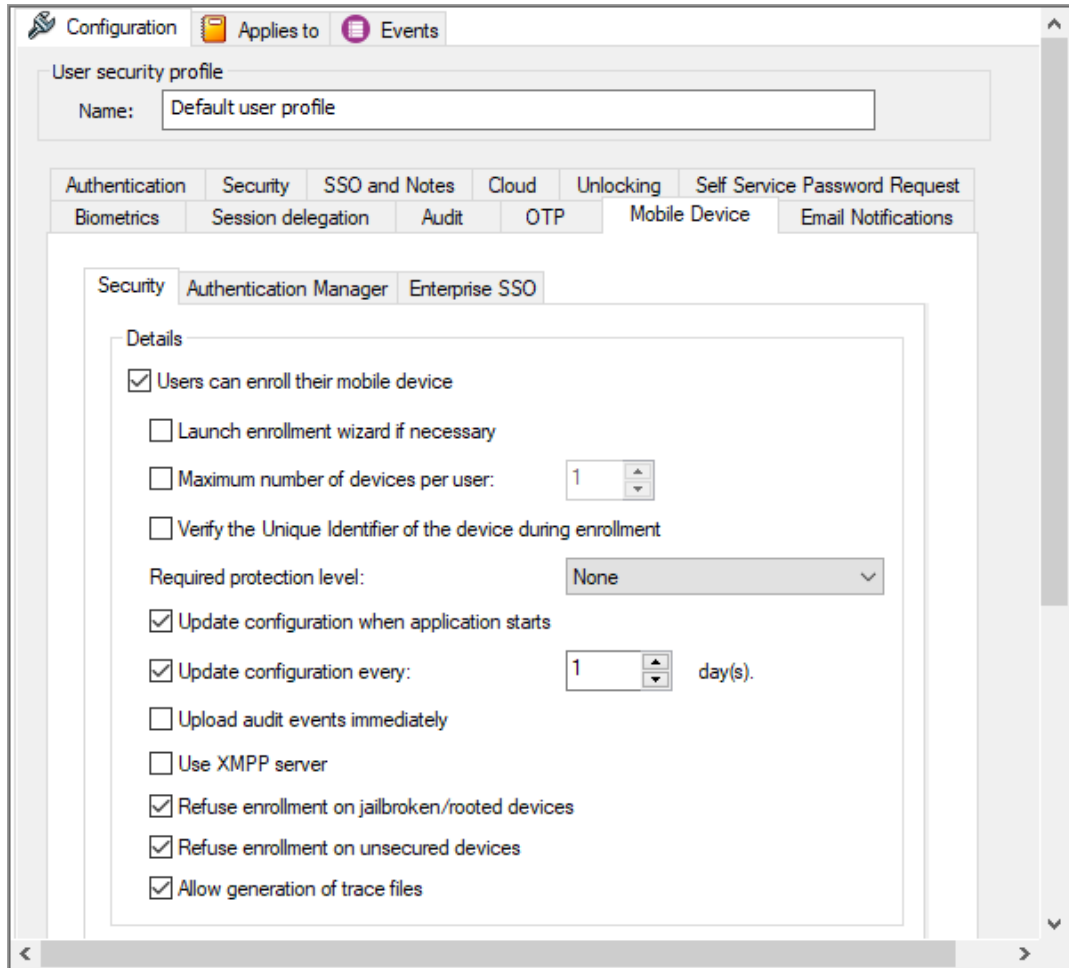
SMS Form data:

Keywords: %PHONENUMBER% %TITLE% %BODY%

Header

1.4.2 Improve security for Mobile device

New options to refuse enrollment on jailbroken, rooted or unsecured devices:



1.5 Enterprise SSO

1.5.1 Making technical definitions without Internet Explorer

Enterprise Access Management's SSO Studio uses Microsoft Internet Explorer 11 to create models of web application authentication screens. EAM uses these models to automate authentication and other password-related interactions in Internet Explorer 11 and, via the Enterprise SSO web extension, in other browsers (Google Chrome, Microsoft Edge and Mozilla Firefox).

As Microsoft retires Internet Explorer 11 on Windows platforms, EAM is providing a new method of enrolling applications for the Enterprise SSO extension. SSO Studio will work with a new, separate web extension, which is to be installed in Google Chrome, Microsoft Edge or Mozilla Firefox.

The new extension will allow operators to continue using the familiar cross-hair drag-and-drop method of identifying user-interface elements. Operators will also be able to choose whether the model is to be used by the SSO web extension or directly by SSO Engine.

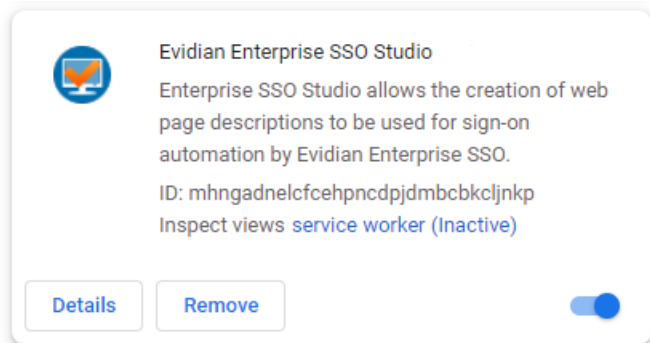
SSO Studio is distributed in the EAM agent package. Administration workstations on which application enrolment is performed will need to be updated to enable the new version of SSO Studio.

End-user workstations on which EAM performs application sign-on will not need to be updated as a result of this change.

To make technical definitions for the SSO extension, it is necessary to install the extension "Evidian Enterprise SSO Studio Extension" to download by <https://chrome.google.com/webstore/detail/mhngadnelcfcehpncdpjdmcbckljnkp> for Chrome and Edge browsers.

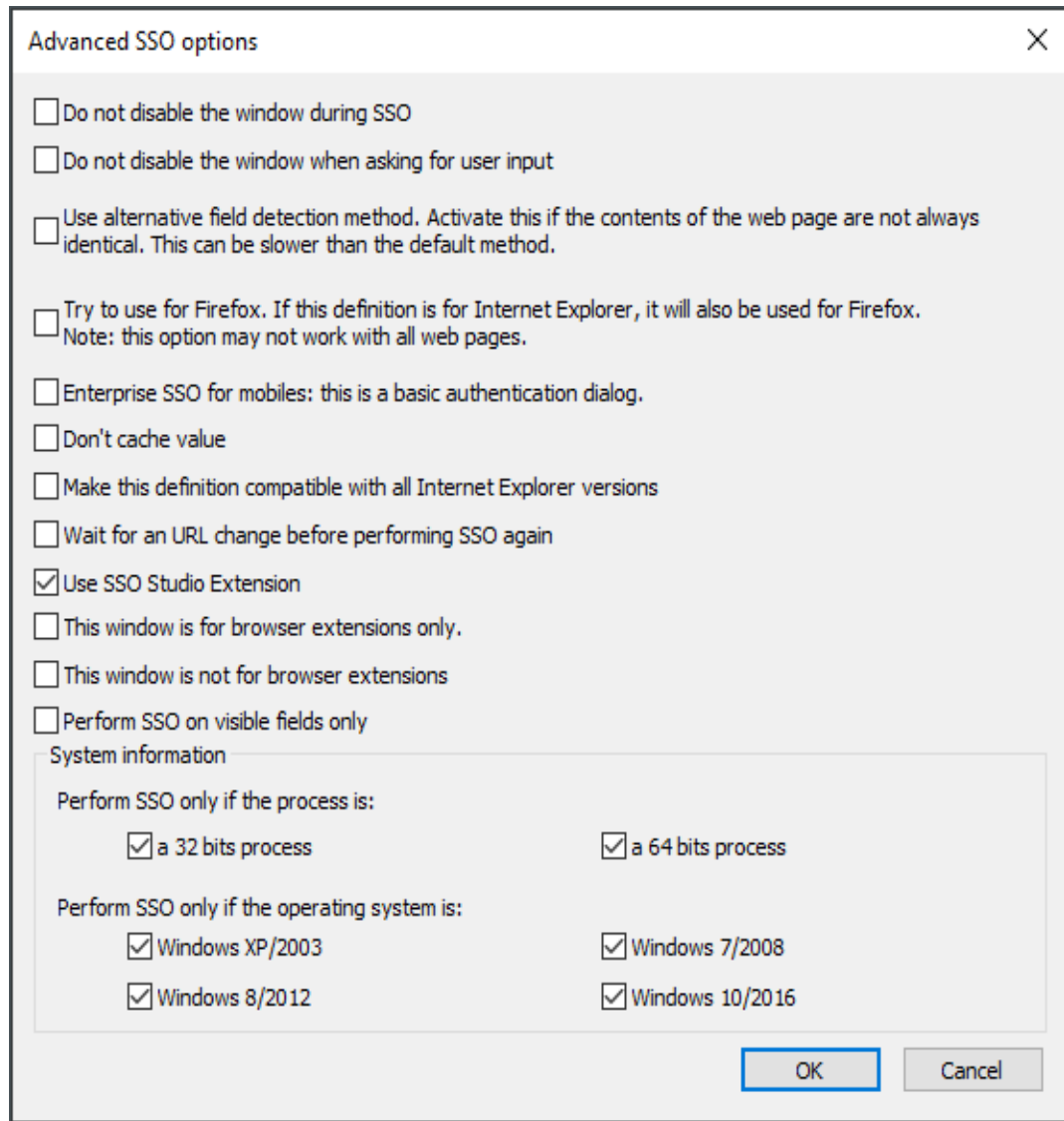
For Firefox, the extension is available to download by https://support.evidian.com/solutions/downloads/firefox/sso_studio.xpi





In the extension part of the browser, we will have:



The image shows a configuration card for "Evidian Enterprise SSO Studio". On the left is a circular icon with a blue background and a white laptop with an orange checkmark. To the right of the icon, the text reads: "Evidian Enterprise SSO Studio", "Enterprise SSO Studio allows the creation of web page descriptions to be used for sign-on automation by Evidian Enterprise SSO.", "ID: mhngadnelcfcehpncdpjdmcbckcljnkp", and "Inspect views [service worker \(Inactive\)](#)". At the bottom left are two buttons: "Details" and "Remove". At the bottom right is a blue toggle switch that is currently turned on.

In the studio, when you define a window, you must check the box "Use SSO Studio Extension" in the Advanced SSO Options window as below:



You must then click on the icon of the Studio extension at the top right of the browser to start the detection. You will have   for a detection in progress. You have to click again on the icon to finish the detection phase and return to  .

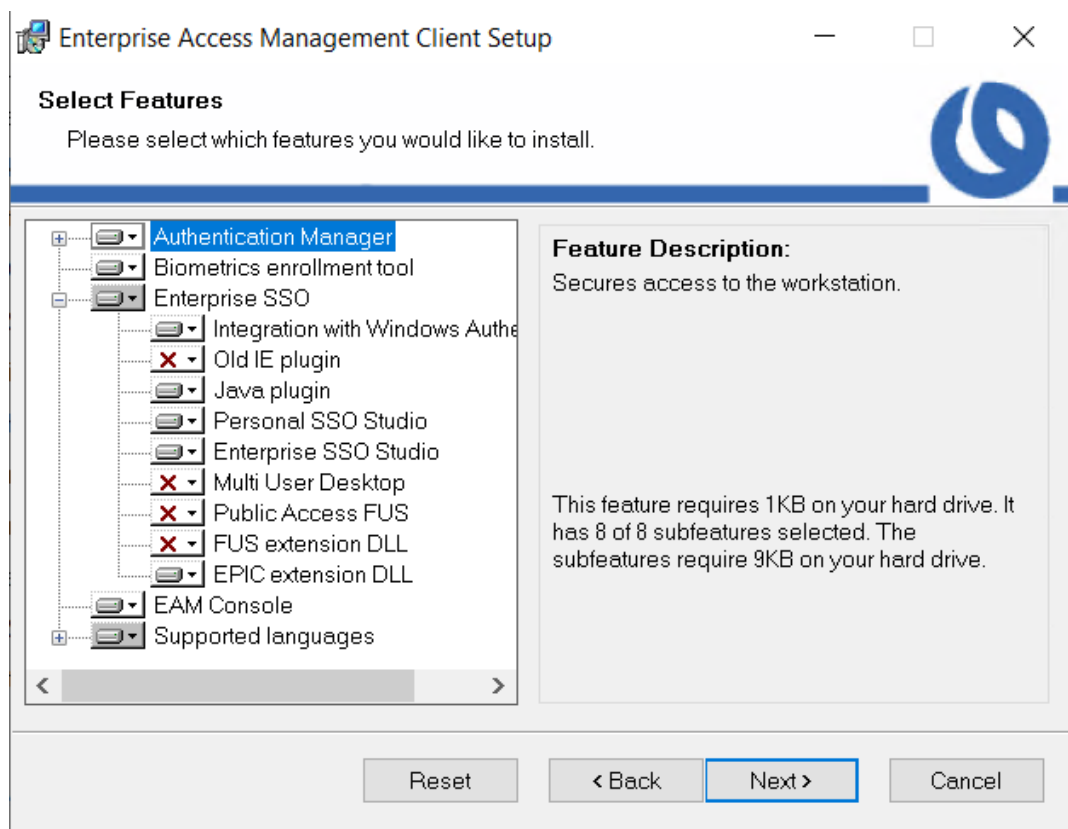
The operations to make a technical definition are the same as before.

1.5.2 Password Vault

- o Application search in Enterprise SSO related to Password Vault functionality is now added.
- o Special characters in complex password generation in Enterprise SSO linked Password Vault functionality is now added.

1.5.3 Support of EPIC application

With the PL3, an “EPIC extension DLL” item has been added in the E-SSO agent to install and register a DLL in order to perform SSO in the EPIC application.



1.6 Nymi Intent

With the PL3, Nymi bands are supported in Intent mode. For more information, see EAM Installation Guide.

1.7 Trivial PIN

With the PL3, Change of PIN have evolved to suppress trivial PIN. For more information, see EAM Installation Guide.

1.8 Oracle OUD

With the PL3, Enterprise Access Management now supports Oracle Unified Directory. For more information, see EAM Installation Guide.

2. What is new in Enterprise Access Management version 10 evolution 2?

2.1 Web Portal

2.1.1 Help-Desk feature

The goal of this feature is to provide the help-desk administrators with a Web Portal to perform frequent administration operations on behalf of EAM users.



You can only use this feature on portal hosted by Apache.

2.1.2 Customization of Web Portal

To customize the EAM Web Portal (SSPR and Self-Admin) you can create a CSS (Cascaded Style Sheet) file named “custom.css”. This file must be located at the root of the EAM Web site.

2.1.3 Web Portal for DMZ

The goal of this feature is to allow the installation of the EAM Web Portal in network DMZ areas where computers cannot access the corporate Directory. When installed in a DMZ, the EAM Web Portal delegates access to EAM data to an EAM “proxy” server.

2.2 Web Service (SOAP) Proxy for DMZ

The goal of this feature is to allow the installation of the EAM Web Service in network DMZ areas where computers cannot access the corporate Directory. When installed in a DMZ, the EAM Web Service Proxy delegates access to EAM data to an EAM Web Service or Controller.

2.3 EAM Console

2.3.1 Display in the “Applies to” tab

When objects have the same name in the “Applies to” tab, the distinguished name is added to all objects to avoid any ambiguity.

2.3.2 Copy in the Other User Attribute Dialog Box

If an administrator presses Ctrl+C when a line is selected in the list, then the value is copied in the clipboard.

2.3.3 Navigation inside EAM Console

By default, when you double-click an object, the object is selected in the navigation tree.

By setting an option, the search function is used instead. This feature should be used when displaying the tree takes times or when there are too many objects in the tree.

2.3.4 Scripting improvements

The limit of 300 lines has been lifted. You can have as many lines as you want in the script file.

A parsing is done before executing the file to check its consistency. No LDAP request is sent if there is a syntax error in a line.

2.3.5 Wearable reports

A new report is available: List of wearable devices.

2.4 Enterprise SSO

2.4.1 Support of Edge-Chromium

As for Google Chrome, the Chrome extension reuses the IE technical definition to perform SSO.



Internet Explorer is not used anymore. See [Section 1.4.3.8 Making technical definitions without Internet Explorer](#) for more information.

2.4.2 Password Vault

Password Vault by Evidian enables you to store and generate complex application passwords securely.

2.4.3 Studio

2.4.3.1 Saving dialog box size

The size of the “Control Detection” dialog box is saved. There is no need to size the window each time you click on the target button.

2.4.3.2 Regular expression

When you write your own regular expression, you can test it easily by double-clicking the URL field.

2.4.3.3 Deactivate a Window of an application

A new option has been added to deactivate a window of an application. Just by selecting this option, Enterprise SSO will ignore the window.

2.4.3.4 Test mode

Until now the “Test application” feature was available only if it was allowed on the application profile. Now this is also allowed if the connected user can access Enterprise SSO Studio.

2.4.3.5 4 eyes improvement

Bad password and new password screens are now compatible with 4 eyes authentication. The account used to perform SSO during 4 eyes is kept in memory until the next SSO. So, if a bad password screen or new password screen is displayed, then the 4 eyes account is used.

2.4.3.6 NetWeaver Business Client 6.5

Support of SSO with the SAP extension on NetWeaver Business Client 6.5 can be performed with a registry value.

2.4.3.7 Focus and Java based application

The advanced option “Check control has focus” in an SSO technical definition is available for Java-based applications with Java plug-in.

2.4.3.8 Making technical definitions without Internet Explorer



This is only true for Enterprise Access Management version 10 evolution 2 PL5.

Enterprise Access Management's SSO Studio uses Microsoft Internet Explorer 11 to create models of web application authentication screens. EAM uses these models to automate authentication and other password-related interactions in Internet Explorer 11 and, via the Enterprise SSO web extension, in other browsers (Google Chrome, Microsoft Edge and Mozilla Firefox).

As Microsoft retires Internet Explorer 11 on Windows platforms, EAM is providing a new method of enrolling applications for the Enterprise SSO extension. SSO Studio will work with a new, separate web extension, which is to be installed in Google Chrome, Microsoft Edge or Mozilla Firefox.

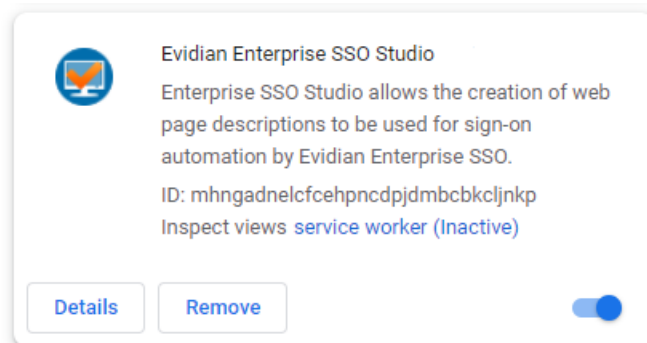
The new extension will allow operators to continue using the familiar cross-hair drag-and-drop method of identifying user-interface elements. Operators will also be able to choose whether the model is to be used by the SSO web extension or directly by SSO Engine.

SSO Studio is distributed in the EAM agent package. Administration workstations on which application enrolment is performed will need to be updated to enable the new version of SSO Studio.

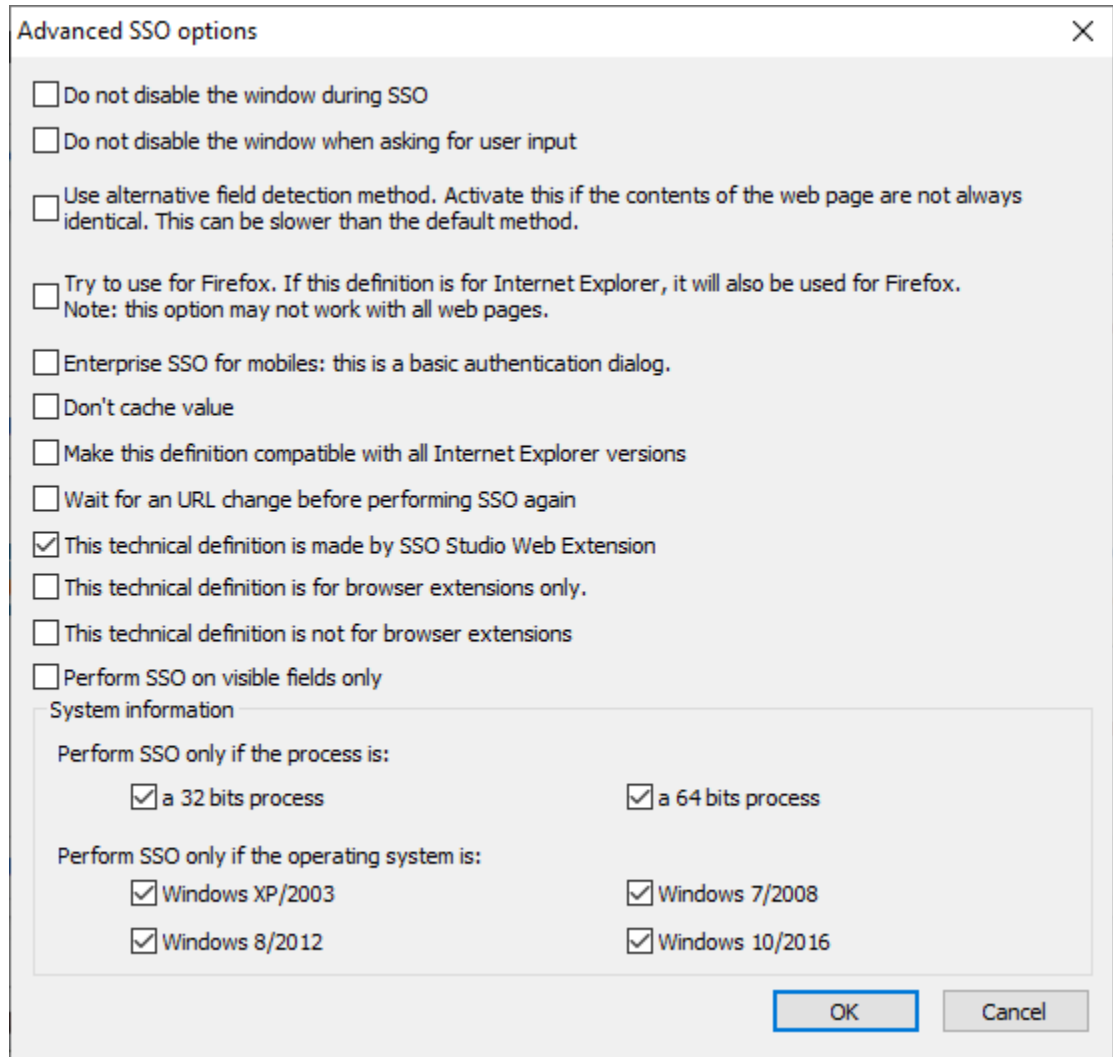
End-user workstations on which EAM performs application sign-on will not need to be updated as a result of this change.





Concretely to make technical definitions for the SSO extension, it is necessary to install the extension "Evidian Enterprise SSO Studio Web Extension" to download by <https://chrome.google.com/webstore/detail/mhngadnelcfcehpncdpjdmcbckljkp>

In the extension part of the browser, we will have:



Then in the studio, when you define a window, you must check the box "This technical definition is made by SSO Studio Web Extension" in the Advanced SSO Options window as below:



You must then click on the icon of the Studio extension at the top right of the browser to start the detection. We will have   for a detection in progress. We will click again on the icon to finish the detection phase and return to  .

The operations to make a technical definition are the same as before.

2.5 Authentication Manager

2.5.1 Tiles

2.5.1.1 Password Credential provider

The password credential provider at change-password can be disabled by setting a registry value. See section 5 Documentation.

2.5.1.2 Customization

The logo of the RFID enrolment process can now be customized as it is for other screens.

2.5.1.3 Automatic repair

Symptom: E-SSO not started upon Windows 10 Update.

FIX: Automatically repair Network Provider and/or Credential Providers and/or Credential Provider filter destroyed by Windows 10 Update.

2.5.2 Credential Manager

Hide "External Certificates..." Credential Manager menu command, unless user has external certificates on the smartcard.

2.5.3 SSPR

2.5.3.1 Mask answers

During answers collect on IIS Web Portal, answers are always visible. Moreover, changing a question resets the collect form. See section 5 Documentation.

2.5.3.2 Reset password with QRentry in Web Portal

Web portal has been extended to allow users to reset their Windows password using QRentry.

2.6 QRentry

2.6.1.1 Autofill

Autofill is the QRentry service that allows users to inject an application's credentials into any native android application.

2.6.1.2 NFC Authentication (Currently Android Only)

You can use your NFC-compatible mobile device to authenticate to Windows or an application. You must select the RFID method during authentication and place your mobile device on a compatible RFID reader (active RFID) with QRentry application running on your smartphone.

3. What is new in Enterprise Access Management version 10 evolution 1?

3.1 Enterprise SSO

3.1.1 Firefox Web extension

A web extension is available for Firefox. As for Google Chrome, this web extension reuses the IE technical definition to perform SSO.

3.1.2 macOS

Enterprise SSO is now available on macOS with a similar interface to Windows (account management, notes and audit visualization).

| SSO is performed in Safari with a Web extension installed automatically by the Enterprise SSO for macOS package.

3.1.3 as a Service

The Enterprise SSO as a Service version supports:

- the shared SSO account feature.
- the use of the enrolment wizard.

3.2 Authentication Manager

3.2.1 Second authentication factor

Any authentication method from Evidian or other vendors can be reused as a second authentication factor to open the Windows session. The trigger of the use of the second factor can be contextual (schedule, network, frequency).

3.2.2 Push notification

By simply validating a notification on their mobile device, users can open a Window session. This feature has been designed to store the security data on-premises.

Currently, Push notification is available on-demand for QRentry iOS.

Push notification shall be available for official release during 2nd semester 2020 for QRentry Android.

3.2.3 Nymi band version 2

The new generation of Nymi bands performing fingerprint authentication for activation is supported.

EAM 10 Evolution 1 version was qualified with Nymi Enterprise Edition version 2.2 and Nymi Band (Gen2 Gold) with firmware version up to version 3.4 Gold.

3.3 Miscellaneous

3.3.1 EAM Monitoring module

A monitoring module is natively available to easily check the health status of EAM controllers.

3.3.2 Audit

Cleaning the audit database (event older than x months) can be managed by the solution with an Oracle Master Database. Events can be archived or deleted.

4. What is new in Enterprise Access Management version 10?

4.1 Enterprise SSO

4.1.1 GUI

Enterprise SSO provides a new interface, more graphical and user-centered. The user can now customize the layout (3 available types), manage his personal notes and view his audit events.

4.1.2 macOS

Enterprise SSO is now available on macOS with a similar interface to Windows (account management, notes and audit visualization).

SSO is performed in Safari with a Web extension installed automatically by the Enterprise SSO for macOS package.

4.1.3 Chrome

The Chrome extension used to perform SSO now supports Custom Script configuration types.

4.1.4 as a Service

The Enterprise SSO as a Service version provides a new authentication method that allows authenticating without a “Cloud” password.

The authentication methods available on the user workstation (Windows Hello) are now used.

Integrated biometric readers available on macOS can also be used.

4.2 Authentication Manager

4.2.1 Self-Service Password Request (SSPR)

When the network is available, the mandatory challenge exchange for the PIN reset can be performed automatically without a call to the help desk.

The user can now reset his PIN on his own.

4.2.2 QRentry enrollment

Two new ways to enroll QRentry are available:

- Directly from the application.
- By scanning a single QR code from the workstation (Windows or macOS).

4.2.3 Multi-User Desktop

The Multi User Desktop can now be configured to use an automatic connection to a remote desktop (RDP, VMWare or Citrix) instead of using the SSO engine.

The Multi User Desktop is not supported on Windows 10 tablets in display mode.

4.2.4 RsUserAuth

The module now takes into account the automatic change of the Windows password.

It also provides SSO to RDP, Citrix and VMWare natively.

4.3 Miscellaneous

4.3.1 EAM Console and administration rights

The EAM Console adapts to the administration rights. Non-useful objects and unavailable features are hidden from the administrator.

It is even easier for administrators using the console to reset passwords or manage authentication tokens.

4.3.2 Audit

Cleaning the audit database (event older than x months) can be managed by the solution. Events can be archived or deleted.



Automatic cleaning of the audit database is not supported with an Oracle Master Database.

5. Technical details

5.1 Operating system prerequisites

5.1.1 Agents environment

Enterprise Access Management agents can be installed on the OS platforms detailed in the tables below. That concerns the following agents:

- Enterprise SSO.
- Authentication Manager (not for macOS).
- Enterprise Access Management Console (not for macOS).

Operating system	Service Packs 32 bits	Service Packs 64 bits
Windows 8 Pro/Windows 8 Enterprise	Original and 8.1	Original and 8.1
Windows 10	Qualified with update 1809	Qualified with update up to 22H2
Windows 11		Qualified with update up to 22H2
Windows Server 2012		Original and R2
Windows Server 2016		Original
Windows Server 2019		Original
Windows Server 2022		Original
macOS	Sierra 10.12.5 and above	



Enterprise Access management agents are supported with the virtualization software such as VMware Workstation or Microsoft Virtual PC.

On macOS, Python3 is a prerequisite. If your version is lower than Catalina (10.15) or Big Sur (11), you must install Python3.

There will be no more hotfixes for Windows Server 2012 and Windows Server 2012 R2 from October 2023.

5.1.2 Controllers environment

Enterprise Access Management Controllers can be installed on the OS platforms detailed in the tables hereafter.

Operating system	Service Packs 32 bits	Service Packs 64 bits
Windows Server 2012	-	Original and R2
Windows Server 2016	-	Original
Windows Server 2019	-	Original
Windows Server 2022		Original



Enterprise Access Management Controllers are supported with the virtualization software such as VMware Workstation or Microsoft Virtual PC. There will be no more hotfixes for Windows Server 2012 and Windows Server 2012 R2 from October 2023.

5.1.3 Citrix / XenApp

Citrix XenApp (Citrix Presentation Server) 4.5, 5.0, 6.0, 6.5, 7.5, 7.6,7.8 and 7.13 are supported using the receiver 4.12.018020 or Citrix Workspace 19.5.0.26, 19.9.0.21 or 19.12.0.119.

5.1.4 VMWare Horizon Client version

Automatic start of VMWare Horizon client has been validated using the version 4.1.0.1487.

5.1.5 Hardware prerequisites

5.1.5.1 Enterprise SSO, Authentication Manager

The Enterprise Access Management agents do not require significant resources on modern computers. The recommended minimal configuration on Windows 8 and 10 is the following:

- 1 GHz Intel processor.
- 1 GB RAM for 32bits, 2GB for 64bits

For macOS workstations, any workstation where Sierra 10.12.5 is running is considered as sufficient.

5.1.5.2 Enterprise Access Management Console and controller

The Enterprise Access Management Console and controller must run on recent hardware to access the audit base with satisfactory performance. The recommended minimal configuration is the following:

- Intel Core 2 Duo processor.
- 2 GB RAM.

5.1.5.3 Audit base

The size of the hard drive hosting the audit database depends on how long you want to keep the log on-line before archiving it. (The audit base does not need to reside on the Enterprise SSO server itself.). For a rough estimate use the following:

- One log entry = 1000 bytes (including database index and other overhead).
- Typical log activity = 20 log entries per user per day.

Performance of the audit database is directly related to the performance of the disk where data is stored. So, high performance disks are recommended.

If the server is virtualized, then a dedicated high-performance disk is highly recommended.

For the master database, virtualization is not recommended.

5.1.5.4 Reporting

The controller hosting reporting must run on recent hardware to generate reports and to use the reporting database with satisfactory performance. The recommended minimal configuration is the following:

- Intel Core 2 Duo processor.
- 8 GB RAM.

5.1.5.5 Reporting database

The size of the hard drive hosting the reporting database depends on usage in terms of concurrent report generation, size of audit database, and number of managed users. The reporting database needs to reside on the Enterprise SSO controller itself.

When using MySQL server, some database parameters must be checked to ensure correct report generation:

- **max_allowed_packet:**
This is the maximum packet length to send/receive from the MySQL server. Its value must be set at least to 32Mb.
- **wait_timeout:**
This is the number of seconds the MySQL server waits for activity on a connection before closing it. Its value must be set to at least the default value of 28800 seconds.



Known Issue

For more information on installing Reporting with MySQL, refer to the Evidian Knowledge Base on the Evidian Support Website:
https://support.evidian.com/knowledge_base/index.php?path=global_area/Q009178.htm

5.2 LDAP directories and databases versions

5.2.1 LDAP directory versions

Enterprise Access Management can access user information located in LDAP directories and use these directories to store SSO and security data. The directories supported by Enterprise Access Management are:

Directories	Operating systems and/or directory versions
Active Directory	<ul style="list-style-type: none"> ○ Windows Server 2012 and R2 ○ Windows Server 2016 ○ Windows Server 2019 ○ Windows Server 2022
AD LDS	<ul style="list-style-type: none"> ○ Windows Server 2012 and R2 ○ Windows Server 2016 ○ Windows Server 2019 ○ Windows Server 2022
Oracle Directory Server	Oracle Directory Server Edition 11g Or Sun Java System Directory Server 5.2
389 Directory Server	389 Directory Server 1.2. on Red Hat Linux Or Fedora Directory Server 1.2 on Red Hat Linux Or Fedora Directory Server 1.0.1 on Red Hat Linux
Novell eDirectory	Version 8.7.3 minimum
Evidian DirX	Version 8.5
OpenLDAP	OpenLDAP Directory 2.4.X IMPORTANT: the configuration of the Enterprise Access Management Service with an OpenLDAP repository requires advanced skills and integration service. Please contact Evidian services: srv-expertise@evidian.com

Enterprise Access Management can use Microsoft AD LDS or ADAM to store SSO and security data.



Cannot find the version you are using? To obtain an up-to-date list of supported LDAP directories versions, please contact your Evidian representative.

5.2.2 Database versions

Enterprise Access Management controller can store a “master” audit base on a relational database. Enterprise Access Management has been validated with the following database versions running on Windows 2012 to 2022 Server Enterprise Edition:

- Oracle from 8.1.7.4. and Oracle Database 18c Express Edition (XE).
- MySQL Server from 5.0.
- Microsoft SQL Server from 2005. The Express edition can be used based on scale limits provided by Microsoft.

The audit cache base can also be one of the database types listed here.

If you want to use another type of relational database, please contact Evidian for the feasibility and a cost evaluation.



Reporting functionality is only available on MySQL and Microsoft SQL Server from 2008 version.



Since the 19.x version of the OLEDB for SQL Server driver of Microsoft, the encryption option with the base is set to Mandatory. If no certificate was installed, you must set this parameter to Optional manually to be able to connect to the data base.

5.2.3 Link with Identity & Access Manager

The link with the Identity & Access Manager requires at least I&AM 9.

5.3 Supported authentication devices

5.3.1 Smart cards and USB tokens

The following middleware and authentication devices are compatible with these specific Enterprise Access Management modules:

- Authentication Manager can use the devices for user authentication.
- Enterprise Access Management Console can manage these devices and use them for the administrators' authentication.

Smart-Card & USB Tokens	Vendor	Middleware
ID Classic 340/341 (Classic TPC)	Gemalto	IDGo 300 (Classic Client) 6.3 patch 1
ID Classic IAS 610/611 (IAS-ECC)	Gemalto	W7, W8.1 - IAS ECC V2.0.20 (ANTS)
IDPrime 510/511 (Cryptoflex .NET V2+)	Gemalto	IDGo 500. The PKCS#11 dll included in our package requires a valid Gemalto support contract.
IDPrime MD830	Gemalto	W7, W8.1, W10, Safenet Authentication Client (SAC) version 10.5
IDPrime MD840	Gemalto	W10, Safenet Authentication Client (SAC) version 10.8 (R2)
IDPrime MD930	Thales	W10, Safenet Authentication Client (SAC) version 10.8 (R2)
IDPrime MD940	Thales	W10, Safenet Authentication Client (SAC) version 10.8 (R2)
IDPrime MD940B	Thales	W10, Safenet Authentication, Client (SAC) version 10.8 (R6) patch 2
IDPrime MD3810	Gemalto	W7, W8.1, W10, Safenet Authentication Client (SAC) version 10.5
Cyberflex 32K or 64K	Gemalto	XP - IDGo 200 (Access Client ACS) 5.6.4 Hot Fix 1
Cyberflex and Oberthur smart cards	ActivIdentity	ActivClient 5.3.1/7.0.2
CPS2ter and CPS3	GIP-CPS	<ul style="list-style-type: none"> version 5.0.42 (ASIP Santé)
Cosmo 64 v5	Oberthur	AWP (Authentic Web Pack) 3.6.2.2
Card OS	Atos	CardOS_API_V5_3_008
Badgeo/Winkeo 2.0	Neowave	AET SafeSign version 3.5.3



To request validation with other types of middleware and devices, please contact Evidian services srv-expertise@evidian.com.



- When using smart cards, you must use PC/SC smart card readers that are compatible with both the cards and the middleware detailed above.
- SAC middleware should be installed with appropriate maintenance.
- IDGo 800 provided in EAM binaries (IDPrimePKCS11.dll version 2.4.0.0) is for test-use only.
- Authentication Manager on Linux module (rsUserAuth) only allows authentication base on smart cards with PKCS#11 middleware linux availability and with smart card assigned to user with directory authentication configuration using stored credentials (<auth_type>stored_cred</auth_type> setting in TokenManagerStructure).

The only Certification Authority that is currently supported is the Microsoft Windows 2003/2008/2012 Certification Authority in an Active Directory configuration. Other Certification Authorities can be used via the PKCS import feature of the Enterprise Access Management Console.

Authentication Manager only supports the default "answer to reset" (ATR) of Gemalto Cryptoflex cards:

- Cryptoflex 32K: 3b 95 XX 40 ff 64 02 01 XX XX.
- Cryptoflex e-gate 32K: 3b 95 XX 40 ff 62 01 02 XX XX.

Customized Cryptoflex cards are not supported.

5.3.2 Biometric devices

5.3.2.1 Using UPEK

Authentication Manager uses BSAPI 4.3.0.289 or PTAPI 3.11.0.236.

These APIs support:

- Intelligent readers based on the following chipsets: TCD21 (TFM), TCD41, TCD42, TCD50A, TCD50D. This includes EIKON, EIKON II and EIKON-To-Go external readers.
- Sensor-only readers based on the following sensors: TCS4B, TCS4C, TCS5B, TCS4K, TCS5D.
- Area sensor readers: TCRU (using ST9 controller), EIKON Touch (using STM32 controller), TCEFC/TCEFD modules (using TCD50D controller).

- ONLY devices with area sensors based on Cypress. (Supported only on Windows).

On Windows, BSAPI.DLL supports also biometry-enabled composite devices manufactured by 3rd parties, if these conditions are met:

- The composite device has AuthenTec sensor embedded, which is supported by BSAPI.
- The manufacturer of the composite device provides original AuthenTec driver, which is modified for use with the composite device (e.g. it is registered for VID and PID of the composite device).

5.3.2.2 Using Hitachi

Authentication Manager 10 supports the Hitachi USB Finger Vein Biometric Scanner - Hitachi Finger Vein H1 Unit.

5.3.3 RFID/HID devices

Authentication Manager has been tested with the following MIFARE Classic, HID iClass, & HID Prox technologies. These components may be embedded, depending on the product release, in:

- SAGEM Ypsid S1 smartcards.
- GEMALTO Classic TPC cards.
- OBERTHUR ID-One Cosmo cards.
- GEMALTO Cyberflex 64k.
- GEMALTO IDPrime Crypto.NET v2+.
- CPS3 cards provided by the GIE CPS.
- Atos CardOS cards.

These tests have been done with the following readers: OMNIKEY HID 5022, 5023 CL, 5025 CL, 5422, ACS ACR122U and Linkeo-NFC. These RFID devices are natively supported (no middleware needed).

Authentication Manager is pre-configured with the following ATR (Answer To Reset):

ATR	Badge
3b8f80010031b86404b0ecc1739401808290000e	CPS3
3b8f8001804f0ca000000306030001000000006a	Mifare Standard 1K
3b8f8001804f0ca0000003060300020000000069	Mifare Standard 4K

3b8f8001804f0ca0000003060a001c000000007e	HID iCLASS
3b8f80010031b8644070151173940180829000a3	IAS ECC Type 1 Contactless
3b8180018080	Mifare DESFire
Start with 3b05	HID Prox 125kHz format H10320
Start with 3b06	HID Prox 125kHz format H10301
Start with 3b07	HID Prox 125kHz format H10302, H10304 and Corp 1k

RFIDeas (www.rfideas.com) is natively supported by Authentication Manager, with SDK mode (Raw Data output) RFIDeas readers. No additional middleware or software development kit is needed.



- pcProx Sonar of RFIDeas is compatible with Authentication Manager and Multi User Desktop.
- Authentication Manager on Linux module (rsUserAuth) doesn't handle reading encrypted information/serial number from DESFire file/application

5.4 Enterprise SSO plug-in requirements

5.4.1 General requirements

Plug-ins are extensions of Enterprise SSO. They provide SSO authentication methods for specific types of applications.

These plug-ins are delivered with Enterprise SSO. Plug-ins are available for:

- Microsoft Edge 90.0.818.42 (using EAM web extension version 1.0.0.27).
- Microsoft Internet Explorer (for Internet Explorer 9.0, 10 and 11).
- Firefox 42, 44, 50, 57, 59, 64 and up to 93. Firefox ESR 10, 17, 24, 31, 38, 52, 60, 68, and up to 102. Firefox ESR is recommended by Evidian because updates are less frequent and have less impact.
- Chrome 46 to 110 (using EAM web extension version 1.0.0.27).
- Edge Chromium up to 110.

- Sun Java SE Runtime Environment (JRE) 10 to 17 as well as OpenJDK Version 8 update 262 b10 (for Adopt OpenJDK, the “JavaSoft (Oracle) registry keys” feature must be installed).
- Lotus Notes versions 4.x, 5.x, 6.x, 7.x ,8.0 and 8.5.
- Microsoft Telnet.
- HLLAPI (see Section 9.1 “Configuring the HLLAPI plug-in” for supported emulators of “Enterprise SSO Administrator's Guide”).
- Script environment for Windows and HTML applications that are not covered by the standard Enterprise SSO process.

5.4.2 SAP R/3 plug-in requirements

The table below shows the supported versions of SAP R/3 components:

Enterprise SSO window type	SAP R/3 client version	SAP R/3 server version (minimum kernel patch level)
SAPGUI Scripting	SAP GUI 6.20	6.10 (360)
	SAP GUI 6.40	4.6D (948)
	SAP GUI 7.10	4.5B (753)
	SAP GUI 7.20	4.0B (903)
	SAP GUI 7.30	3.1I (650)
	SAP GUI 7.40	



Important

The SAP web-based Start Center is compatible with Enterprise SSO, but you need to upgrade to SAPGUI Version 6.40 with Patch Level 23.



Note

The SAPLogin and SAPEXPIRED window types defined in version 3.71 of SSOWatch remain available to ensure the continuity of deployed configurations.

We recommend not using them for new deployments. Existing windows should be ported to SAPGUI Scripting window types.

5.5 Supported HTTP server

The following Enterprise SSO features require an HTTP server:

- Enterprise Access Management Web Service administration API.
- Enterprise Access Management Self Service Password Request feature.

Evidian delivers an HTTP server based on Apache 2.4 (version 2.4.27) and PHP 5.6 (version 5.6.31). This web server is the only server supported by Evidian for providing the Web Service API and the SSPR feature. For cases where only the SSPR feature is needed, it is possible to integrate that feature in an existing Microsoft IIS Server.

Evidian will not provide support for the above-mentioned features when used with any other server. As well, Evidian will not support the bundled server for functions other than those that are strictly necessary for the above Authentication Manager features.

The password reset feature requires you to use a certificate generated by a Certification Authority (CA) in order to activate HTTPS. Evidian delivers a sample CA for testing purposes, but does not provide support for that CA. Please use a supported CA for actual deployments.

5.6 Encryption methods

All calls done to encryption and signature functions (whatever the algorithm: AES, RSA...) are done through OpenSSL version 1.0.2.L. You can configure EAM to use OpenSSL in FIPS 140-2 mode.

5.7 Supported Gemalto SA Server version

The integration between Enterprise Access Management and Gemalto Strong Authentication Server requires the installation of Gemalto SA Server in version 3, 4, or 5.1.

5.8 Configuring the HLLAPI plug-in

The HLLAPI plug-in communicates with a terminal emulator through a DLL. Each emulator provides a different DLL for that purpose.

To tell Enterprise SSO how to communicate with your terminal emulator, you need to edit the Microsoft Windows Registry and enter three values located under **HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\SSOWatch\HLLAPI**.

- **HLLibrary** – the name of the emulator's DLL (file name or full path) that gives access to the HLLAPI feature.

- **HllEntryPoint** – the name of the relevant function in the DLL file.
- **HLLAPI-32bit** – indicates whether the HLLAPI is in 32-bit mode (value=1) or not (value=0).

	HllLibrary	HllEntryPoint	HLLAPI-32bit
Attachmate EXTRA!® Enterprise 2000	ehllapi32.dll	hllapi	0
Values used by the plug-in if the registry entries do not exist.	PCSHLL32.dll	hllapi	1



The Registry entry and associated values are not created during installation. You need to manually create the Registry entry **HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\SSOWatch\HLLAPI** and the three values **HllLibrary**, **HllEntryPoint** and **HLLAPI-32bit**.

5.9 Supported languages

The supported languages are:

- arabic
- czech
- dutch
- english
- finnish
- french
- german
- italian
- japanese
- romanian
- russian
- spanish
- swedish

5.10 Reporting service requirements

The Reporting service is a web service requiring:

- Sun Java SE Runtime Environment (JRE) 1.8. or Java Virtual Machine (JVM) Adopt OpenJDK Version 8 update 272 b10.
- The Java Connector related to the database used.
 - For MySQL Server: Java Connector from 5.1.
 - For Microsoft SQL Server: Microsoft JDBC Driver 4.1 for SQL Server

5.11 Warnings

5.11.1 Updating Enterprise Access Management modules

If the Enterprise Access Management Console and the Authentication Manager modules are installed on a same system, when you update these Enterprise SSO modules, please bear in mind that:

- The Enterprise Access Management controller component must be updated before any other modules.
- You must update all the Enterprise Access Management modules installed on this station to the latest patch level.

5.11.2 APACHE server update from EAM evolution 2 (or less) to EAM evolution 3

Version of APACHE and PHP changed for EAM evolution 3. You cannot make an update of the SSPR portal with an update of the ESSOWebServer.msi package.

You must uninstall the ESSOWebServer.msi package and APACHE. Then you reinstall the SSPR server using the WGSrvConfig tool.

5.11.3 Integrating an application with the HLLAPI plug in

Successfully integrating a terminal application with the HLLAPI module depends on many parameters:

- Which terminal emulator is used?

- Which terminal protocol is used?
- The specific way in which the application implements login.

The HLLAPI plug-in has been tested by Evidian with the following emulators in some basic conditions:

- Attachmate EXTRA! Mainframe Server Edition 8.1.
- Gallagher and Robertson Glink Professional Edition version 8.0.5 and 8.4.
- NetManage RUMBA version 7.4.
- Zephyr PASSPORT PC TO HOST (version 2007-914-S).
- Distinct IntelliTerm 8.1.

However, this does not mean that integrating any application with any terminal protocol will always work with the above emulators. In some cases, the specificities of applications mean that successfully integrating them may require paid services from Evidian or Evidian partners.

5.11.4 Integrating a third-party Card Management System (CMS)

Evidian can integrate a third-party CMS with Enterprise SSO on a service basis. This requires paid professional services from Evidian.

Once integrated, the third-party system replaces the CMS features of Enterprise Access Management Console.

Please be aware that, for this integration to be technically feasible, there are several technical prerequisites on the third-party CMS. Please contact Evidian for a list of those prerequisites.

5.11.5 Enterprise SSO with Novell NetWare

When Enterprise SSO is used in Novell NetWare environments, please make sure that the NetWare password is always the same as the Windows password.

You must use a NetWare option to synchronize the Windows password with the NetWare password.

If this is not done, the user will need to perform a second authentication to Novell NetWare after his or her Windows authentication.

5.11.6 Enterprise SSO Internet Explorer plug-in warnings

The following warning applies to the Internet Explorer 6.0, 7.0, 8.0, 9.0,10 and 11 plug-in: if a frameset contains a secure page that contains a combo box, Enterprise SSO cannot activate that combo box.

5.11.7 Microsoft Edge plug-in warnings

Looking for text is always done on the whole page not for a specific field.

Two custom script features are not available:

- Send javascript command,
- Get text from a control.

5.11.8 macOS Enterprise SSO web extension

SSO on basic authentication dialog is not supported.

5.11.9 Some features are available in English language only

The following will be displayed in English language only in localized versions: Java Virtual Machine (JVM) configuration program (Java plug-in feature of Enterprise SSO).

5.11.10 Reporting functionality & Languages

When Reporting functionality is used on data containing Japanese or Chinese languages, Reporting font has to be modified with one supporting this language. Refer to the documentation for details on how to modify font used by Reporting functionality.

5.11.11 Reporting functionality & Audit

When Reporting functionality is used on audit data, for the current release, the result may fail in timeout depending on the requested period of time. In that case, shorten the period of time to apply to reported data.

5.12 Restrictions

5.12.1 Restrictions of Evolution 3 Patch Level 1

- No FIPS compliance.
- You cannot use the PDF Reporting with Enterprise Access Manager version 10 evolution 3.



This restriction is lifted with the Patch Level 4.

5.12.2 Windows Active Directory inter-domain support with Enterprise Access Management in temporary restriction

When a station is declared in several domains using Enterprise Access Management Console, there are restrictions in access for users who do not belong to the same domains as the station.

	With Authentication Manager	Without Authentication Manager
Users who belong to the same domain as the station	Can authenticate SSO active	Can authenticate SSO active
Users who do not belong to the same domain as the station	Cannot authenticate	Can authenticate SSO not active

This restriction exists:

- o With Controller, if the various domains the user belongs to are not located in the same Active Directory forest.
- o Without Controller, if the middleware does not have a user account. In that case, deploying a user account for the middleware will lift the restriction.

5.12.3 Active Directory multi-domain and multi-forest

The multi-domains functions are managed in one forest only.

5.12.4 eDirectory

An access point security profile cannot be set on a computer. Policy must be set using groups or organizations.

In cooperative mode, the option “Change password at next login” is not supported.

5.12.5 LDAP accounts used by Enterprise Access Management controllers must not expire

The technical LDAP accounts used by Enterprise Access Management controllers does not expire or, if it expires, the account must be different on each controllers. The value of the register key `LdapUserSrvPwdChangeDelay` under `HKLM\Enatel\WiseGuard\Framework\FmkServer` is used. This value must be set for a time over than the expiration delay of the password for the account. This value is in days and the generated password has 12 random base-64 characters.

5.12.6 Other limitations

Import of XML objects may not work depending of the characters set.

5.12.7 Java plug-in

The Java plug-in supports the following object classes:

	AWT classes (and classes derived from these)	Swing classes (and classes derived from these)	Oracle classes (exact classes only)
Buttons	java.awt.Button	javax.swing.JButton	oracle.forms.ui.VButton oracle.apps.fnd.ui.Button oracle.apps.fnd.ui.FormButton oracle.ewt.button.PushButton oracle.ewt.button.ContinuousButton
Text fields	java.awt.TextField	javax.swing.JTextField javax.swing.JPasswordField	oracle.forms.ui.VTextField oracle.ewt.lwAWT.lwText.LWTextArea
Labels	java.awt.Label	javax.swing.JLabel	oracle.ewt.lwAWT.LWLabel oracle.ewt.multiLineLabel.MultiLineLabel

			oracle.ewt.alert.BaseAlertPane\$PreferredAspectLabel
Others	java.awt.Choice java.awt.Checkbox	javax.swing.JComboBox javax.swing.JList javax.swing.JCheckBox	oracle.forms.ui.VComboBox oracle.forms.ui.VCheckbox oracle.ewt.lwAWT.LWCheckbox

If the java plug-in does not work with your application, an extension of the supported classes could be possible.



The configuration of SSO for Java requires advanced skills. To deliver SSO access to Java applications, integration service is required. Please contact Evidian services srv-expertise@evidian.com.

5.12.8 QRentry or Enterprise SSO for mobile devices

QRentry is available on Android (6.0 or later) and iPhone (iOS 12.0 or later).

QRentry manages the enrollment and usage of only one Active Directory account. If you are in a multi-account environment, you need to use Evidian Authenticator.

5.12.9 Enterprise Access Management Console

Windows computers with Large Fonts or Extra Large Fonts configuration are not supported by Enterprise Access Management Console.

5.12.10 Web Portal: Help-Desk feature

Currently, the detailed information about the user are correctly displayed only using Google Chrome or Microsoft Edge Chromium.

5.12.11 Verification of the Unique Identifier of the mobile device during enrolment

Due to Android 10 security update, Unique Identifier (a.k.a IMEI) of the user’s mobile device cannot be checked upon the enrolment process anymore.

6. Documentation

Documentation of Authentication Manager and Enterprise SSO can be found in the Evidian documentation pack delivered with the product, and particularly for the updates on the web site of Evidian Support <https://support.evidian.com> in the documentation area.

Available documents are the following:

Task	Document title	Reference	Modifications
Getting Started	Enterprise Access Management 10.0 Evolution 3 Release Notes	39A2 25MC	§ 1.5.3, 1.6, 1.7, 1.8, 5.1.1, 5.2.2
	Evidian EAM in a Nutshell	39A2 66MB	No modification.
Installing and Configuring	Evidian EAM Installation Guide	39A2 13MC	§ 2.5, annex E, F, G, H
	Evidian EAM as a Service Installation Guide	39A2 24MB	No modification.
	Evidian EAM Quick Installation and Start Guide	39A2 28MC	No modification
	Authentication Manager and Enterprise SSO Directory Replication Guide	39 A2 76MB	No modification.
	Authentication Manager for Linux Installation and Configuration Guide	39 A2 20MB	No modification.
Administering	Evidian EAM Console Administrator's Guide (English and French)	39A(F)2 12MC	§ 9: modification
	Authentication Manager Self Service Password Request Administrator's Guide	39 A2 96MB	No modification.
	QREntry Administrator's and User's Guide (English and French)	39 A(F)2 15MC	No modification.
	Authentication Manager Session Management Administrator's Guide	39A2 65MB	No modification.
	Authentication Manager Cluster Administrator's Guide	39A2 67MB	No modification.

Task	Document title	Reference	Modifications
	Enterprise SSO Administrator's Guide (English and French)	39A(F)2 20MC	§ 10.1.3.2:removal of rubular reference § 3.2.1: new option described
Using	Evidian EAM Portal User's Guide (English and French)	39A(F)2 14MC	No modification.
	Authentication Manager for Windows User's Guide (English and French)	39A(F)2 17MC	No modification.
	Enterprise SSO User's Guide for Windows	39A(F)2 55MB	No modification
	Enterprise SSO User's Guide for macOS	39A(F)2 22MB	No modification.
	Enterprise SSO as a Service - User's Guide for Windows	39A(F)2 56MB	No modification.
	Enterprise SSO as a Service - User's Guide for macOS	39A(F)2 05MB	No modification.
	Enterprise SSO as a Service – User's Guide for Android mobile devices	39A(F)2 06MB	No modification.
	Enterprise SSO as a Service – User's Guide for iOS mobile devices	39A(F)2 07MB	No modification.
	Password Vault User's Guide for Windows (English and French)	39A(F)2 36MB	No modification.
	Wearable Device Authentication - User's Guide	39A2 17MB	No modification.
Customizing	Evidian EAM Customization Guide	39A2 57MB	No modification.
	Evidian EAM API and Web Service Reference Guide	39A2 71MB	No modification.

