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.

Authentication Manager Session Management Administrator’s Guide
Updated - November 2017
Version - 9.0.2
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
- 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.

*CAPITALIZATION* 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.
Overview

Session Management Functions

This section gives an overview of the features offered by the Session Management option.

Fast User Switching (FUS)

Fast User Switching (FUS) simplifies the access to computers used by several employees.

FUS modifies the Microsoft session unlocking method by allowing users to unlock or close an other user’s session, by using one of the following methods:

- **Hierarchized access FUS**: users are only authorized to unlock or close the session of other users whose level is below or equal to their own level.
- **Shared access FUS**: several users have in their Windows account list the one that has open the session, so they can unlock or close the session of all other users who have the same account.
- **Public access FUS**: the workstation session remains open and is the same for all users, but the SSO context and application opening/closing are handled individually for each user.

This function is particularly used in retail store workstations where salespersons want to check stocks or register orders before their customers change their minds.

Fast User Switching can work with Roaming Session Mode or with Cluster Mode.

To know how to configure and use the Fast User Switching, see The Fast User Switching (FUS) Feature.
Multi-User Desktop

Description

The Multi-User Desktop feature provides advanced Fast User Switching features for workstations used simultaneously by a large number of users, such as kiosk computers or computers used by medical staff in hospitals.

To provide Fast User Switching and save computer resources, the Multi-User Desktop uses a single Windows Desktop to display all the user applications and launches a single instance of Enterprise SSO engine.

Requirements

- To be compatible with Multi-User Desktop, applications must support several instances running simultaneously.
- Specific configuration is needed with Internet Explorer: for more information, please contact the Expertise Evidian Center.
- The Multi-User Desktop is designed for computers where the Windows session is always and automatically opened and never locked. Do not enable the screensaver.

Session Management

Session authentication/disconnection

Upon a successful authentication, the Enterprise SSO engine loads the user's set of accounts. It can then automatically start the user's applications and perform the SSO.

Upon disconnection, Enterprise SSO closes the user's set of accounts and some of his applications if necessary. Multi-User Desktop then hides the applications started by the user.

If no user authenticates, the welcome dialog box appears. If another user authenticates, his own session is created or re-connected.

Session termination

Upon termination of a session, Enterprise SSO closes the user's set of accounts and his applications. Multi-User Desktop then terminates all applications started by the user before displaying the welcome dialog box.

NOTE: Multi-User Desktop can automatically disconnect an active session and terminate a disconnected session.
When a new user session must be created, Multi-User Desktop can automatically terminate the oldest disconnected session if a maximum number of concurrent sessions has been set in Enterprise SSO Console.

To know how to configure and use the Multi-User Desktop feature, see The Multi-User Desktop Feature.

## Roaming Session

The **Roaming Session mode** simplifies the successive authentication to several computers.

When a user needs to access several computers during the day, he/she only has to authenticate once on the first computer; then he/she only needs his/her device to open the other computers sessions.

This function is particularly used in hospitals emergency desks, where nurses and doctors need immediate access to information.

It can be combined with Fast User Switching, and can be used on Clusters of computers.

To know how to configure and use the Roaming Session mode, see The Roaming Session Mode.

## Double-Login Prevention

By default, when a user authenticates on a computer, the computer session on which he/she was previously connected (by password, passive RFID or biometrics) remains open.

The **Double-Login Prevention** function ensures that, when a user is authenticating on a computer, the session opened on the previously used computer is locked.

To know how to configure and use the Double-Login Prevention feature, see The Double-Login Prevention Feature.

## Session Management Authentication Methods

The following table lists the authentication methods that can be used for each of the Session Management functions.
### Table 1: Session Management Authentication Methods

<table>
<thead>
<tr>
<th>Function</th>
<th>Password</th>
<th>Smart Card</th>
<th>Active RFID</th>
<th>Passive RFID</th>
<th>Biometrics</th>
<th>Mobile device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchized Access FUS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Shared Access FUS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Public Access FUS</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Multi-User Desktop</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Roaming Session Mode</td>
<td>Not relevant</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Not relevant</td>
<td>-</td>
</tr>
<tr>
<td>Double-Login Prevention</td>
<td>✓</td>
<td>Not relevant</td>
<td>Not relevant</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
</tbody>
</table>

### Required EAM Modules

The following table lists the EAM (Enterprise Access Management) modules that you must install to use each of the Session Management functions.

### Table 2: EAM Modules

<table>
<thead>
<tr>
<th>Function</th>
<th>EAM Client</th>
<th>EAM Console</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enterprise SSO</td>
<td>Authentication Manager</td>
</tr>
<tr>
<td>Hierarchized Access FUS</td>
<td>Optional</td>
<td>✓</td>
</tr>
<tr>
<td>Shared Access FUS</td>
<td>Optional</td>
<td>✓</td>
</tr>
<tr>
<td>Public Access FUS</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Multi-User Desktop</td>
<td>✓</td>
<td>Not compatible</td>
</tr>
<tr>
<td>Roaming Session Mode</td>
<td>Optional</td>
<td>✓</td>
</tr>
<tr>
<td>Double-Login Prevention</td>
<td>Optional</td>
<td>✓</td>
</tr>
</tbody>
</table>
The Fast User Switching (FUS) Feature

Fast User Switching - Overview and Use

Definition

EAM Fast User Switching (FUS) is a functionality that allows multiple users to easily share the same workstation, by allowing them to change the SSO context quickly, without closing the Windows session.

Fast User Switching Modes

The Fast User Switching function works in three modes so that it can perfectly fit your needs. These modes are detailed in the following sub-sections.

In Hierarchized Access FUS and Shared Access FUS, the access to the Windows session is protected: the Windows session locking and unlocking is managed by Authentication Manager. All authentication methods can be used, but if an authentication device is used, it ensures that when a user removes his/her device, the session is automatically locked. If the same user comes back to the same workstation, he/she will find his/her applications still open.

In Public Access FUS, the access to the Windows session is not protected: the session is the same for all users, but each user can access his/her own applications.

You can also use FUS with AutoLogon. You can configure Windows to automate the logon process by storing authentication data in the registry database. This feature allows any user to start a workstation in public access and use the account configured for automatic logon.

This enables a user to gain time when:
- Opening a Windows session for the first time.
- The network is not available for your first authentication.

Turn on automatic logon:

- For Hierarchized Access FUS and Shared Access FUS by using E-SSO registry keys as explained in Authentication Manager pour Windows - Guide de l’utilisateur.
- For Public Access FUS by using the Windows registry keys as explained in the following web page: http://support.microsoft.com/?scid=kb%3Ben-us%3B315231&x=10&y=13 (URL valid in Thursday, November 30, 2017).

  IMPORTANT: You are strongly advised to use a generic account that has no particular right on its own to keep the Windows session open for all users.

Hierarchized Access FUS

In hierarchized Access FUS, users are associated with an "unlocking level" and a "closing level". They are only authorized to unlock or close the session of other users whose level is below or equal to their own level.

Figure 1: Hierarchized Access FUS
In the above illustration, the Windows user is still User A, and the Enterprise SSO user is User B.
To configure this FUS mode, see Configuring Hierarchized Access FUS.

**Shared Access FUS**

In Shared Access FUS, all users who need to authenticate to the same workstation have the same Windows account. All these users have in their account list the one that has open the session. This way, they can unlock the session open by another user of the same group.

**Figure 2: Shared Access FUS**

To configure this FUS mode, see Configuring Shared Access FUS.

**Public Access FUS**

The Public Access FUS is adapted to computers used in public access. In this mode, the access to the Windows session is not protected: the workstation session remains open, but the SSO context and application opening/closing are handled individually for each user, as illustrated in the following figure:
Upon detection of a smart card or an active RFID device, Enterprise SSO starts and prompts the user for his/her PIN (smart card) or password (RFID). Once the user is authenticated, he/she can access his/her own applications. When the device is removed, Enterprise SSO is closed. The Windows session can use a generic account that has no particular right of its own.

**NOTE:** If the roaming session is allowed on the access point (see The Multi-User Desktop Feature), each time an RFID device is presented or a smart card is inserted, Public Access FUS checks if a roaming session can be used before prompting for the password or the PIN to the user.

To install and configure this FUS mode, see Installing and Configuring Public Access FUS.

**Configuring Hierarchized Access FUS**

Evidian provides hierarchized access Fast User Switching with Authentication Manager. The functionality is managed from EAM Console.
Authorizing FUS on Workstations

Subject

You must authorize the use of FUS on all computers on which you plan to set up hierarchized access FUS, as explained in the following procedure.

Procedure

1. In EAM Console, from the Directory panel, click the access point security profile that applies to computers that will be used for hierarchized Fast User Switching.
2. In the Authentication Manager tab, select Allow unlock if allowed by user security profile:

   Figure 4: Authenticatin Manager tab

   ![Authentication Manager tab](image)

   - Lock behaviour
     - Default action when token removed
     - Delay before action
     - Automatically lock after
       - [ ] Automatically logoff after
     - [ ] Allow local connection
     - [ ] Allow remote unlocking of tokens
     - [ ] Remember authentication role
     - [ ] Allow password change
     - [ ] Enable smart card detection on Ctrl+Alt+Del
     - [ ] Allow unlock if allowed by user security profile
     - [ ] Allow unlock if the same Windows credential is used
     - Max. number of concurrent Windows sessions:
       - [ ] 0
       - [ ] from Windows Server

3. Click Apply.
Activating Hierarchized Access FUS

Subject

You activate hierarchized access FUS from the user security profile, as explained in the following procedure.

Before Starting

- Make sure Authentication Manager is installed on the workstation you want to be used for Fast User Switching.
- Make sure you have the following administration role:
  - In classic administration mode: "Security object administrator".
  - In advanced administration mode, your role must contain the following rights: "User security profile: Creation/Modification", "Application profile: Creation/Modification" and "Access point security profile: Creation/Modification".

**NOTE:** For more details on administration roles, see *Evidian EAM Console - Guide de l'administrateur*.

Procedure

1. In EAM Console, from the **Directory** panel, click the user security profile that applies to users that will use the hierarchized Fast User Switching.
2. Click the **Unlocking** tab.
   The **Unlocking** tab appears.
3. Fill-in the tab as explained in the following Unlocking Tab Description section.

Unlocking Tab Description

**Figure 5: Unlocking Tab**
Table 3: Unlocking tab

<table>
<thead>
<tr>
<th>Tab Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User level</strong></td>
<td>Enter a user hierarchy level (0 is the lowest level, and 50000 is the highest). We recommend to set a big interval between levels (for example 10; 20; 30 and so on), so that you can add sub-levels in between if needed.</td>
</tr>
<tr>
<td><strong>User can unlock sessions of users below level</strong></td>
<td>Select this check-box to allow a user to unlock a session locked by another user whose level is below the specified level.</td>
</tr>
<tr>
<td><strong>User can close sessions of users below level</strong></td>
<td>Select this check-box to allow a user to close a session opened by another user whose level is below the specified level.</td>
</tr>
</tbody>
</table>

**NOTE:** When a user tries to perform a FUS on a workstation, EAM refers to the unlocking level before the closing level.
Overriding the User "Unlocking Level" (Optional)

Subject

In the application security profile, you can define a different user level than the one specified in the user security profile. In this case, when a user launches an application that is associated with this application security profile, the user "unlocking level" is overridden with the level set in the application security profile (usually set to a higher level).

Procedure

1. In EAM Console, from the Directory panel, click the application security profile that applies to applications for which you want to override the user unlocking level.
2. Click the Configuration/General tab.
   The General tab appears.

   Figure 6: Configuration/General tab

   ![Configuration/General tab](image)

3. Select the When application is used, set user's "unlocking level" to: select the check-box and set the level number.
4. Click Apply.
Configuring Shared Access FUS

The shared access FUS is used when no hierarchy can be set between employees that need to access a workstation.

Authorizing FUS on Workstations

You must authorize the use of FUS on all computers on which you plan to set up shared access FUS, as explained in Authorizing FUS on Workstations.

Associating Users with a Shared Windows Account

Subject

In shared access FUS, all users who need to access the same workstation have in their account list the one that has open the session. The easiest way to configure this is to gather these users in a group of users. The following procedure explains how to associate a group of users with a shared windows account.

Before Starting

To perform the task described in this section, you must have at least the following administration role:

- In classic administration mode: "Security object administrator"
- In advanced administration mode, your role must contain the following right: "Application: Creation/Modification".

Procedure

1. In EAM Console, from the Directory panel, right-click the Organizational Unit that must contain your Application and select New/Template-based Application/Windows.
   The Windows Application window appears.
2. Fill-in the window by typing the application name and Windows domain.

3. In the group of users that you want to make share the same Windows account, add the application and define it as shared, as follows:
   a. Click the group of users and select the Application Access tab. The Application Access tab appears.
   b. In the Application Access tab, add the application you have just created, and set the Account type to Shared.

4. In the group of users, assign an owner for the application, as follows:
   a. Click the group of users and select the Accounts tab. The Accounts tab appears.
b. Click the application and click the **Properties** button.
   The **Account Properties** window appears.

c. In the **SSO Data** tab, create credentials for the account.
d. In the **Ownership** tab, you can assign an owner for the account. In this case, this owner becomes the only user authorized to modify the account password.

**NOTE:** EAM allows you to manage password modification of a shared application account: if you do not set ownership, all users who are part of the group of users sharing the same application account are authorized to modify the shared account password. The other users automatically retrieve the new password.

## Activating Shared Access FUS on Dedicated Access Points (Optional)

### Subject

By default, FUS is authorized on all access points, without need of any configuration. This section explains how to reserve some workstations only for shared access FUS users. The configured workstations will only be accessible to shared access FUS users.
Procedure

1. In EAM Console, from the **Directory** panel, click the access point security profile that applies to computers reserved for shared access FUS users.

2. In the **Authentication Manager** tab, select **Allow unlock if the same Windows credential is used**:

   ![Authentication Manager](image)

   **Figure 11: Authentication Manager**

   - **IMPORTANT:** If you select both **Allow unlock if allowed by user security profile** and **Allow unlock if the same Windows credential is used** check-boxes, you must take into account that **FUS** will be applied to users from a same Windows account, at the same hierarchy level.

3. Click **Apply**.
Installing and Configuring Public Access FUS

Subject

Evidian provides Fast User Switching at the session level with Enterprise SSO, with the "Session Management" extra license.

The process listens for incoming events from activated authentication devices. These devices are:

- Smart cards managed from Evidian.
- Smart cards managed externally for which the PKA authentication is activated in Evidian.
- Active RFID devices.

In Public Access FUS, the Windows session is the same for all users. The Windows session used is the one of the first user who has open a Windows session on the workstation. Then users use their authentication device to access their own SSO context and applications.

NOTE: You can set a generic Windows account that has no particular right on its own, to keep the Windows session open for all users.

Procedure

1. Log-on as system administrator.
2. Run the EAM installation wizard and follow the displayed instructions with the following guidelines:
   a. If you use the EAM Quick installation, select the Public access authentication mode in the EAM Client modules selection window:
Figure 12: Enterprise Access Management Wizard

NOTE: For more details on EAM quick installation, see *Evidian EAM Quick Installation Guide*.

- If you use the EAM advanced installation, select **Public Access FUS** in the features selection window:

Figure 13: Public Access FUS
**IMPORTANT:**
- Make sure the **Authentication Manager** and **Integration with Windows** features are not selected for installation.
- For more details on EAM advanced installation, see *Evidian EAM Installation Guide*.

## Configuring Keyboard and Mouse Locking

**IMPORTANT:**
- The following configuration settings are unique to Public Access FUS for smart cards or RFID devices.
- For compatibility reasons with **Windows Vista/2008** and later versions, do one of the following:
  - Add the string value (REG_SZ type) named `C:\%EAM installation folder\SSOFus.exe` with the VISTARTM value. The registry key is located in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers`.
  - Deactivate the User Account Control after having set the following keys.

## Locking Keyboard and Mouse if Enterprise SSO is Stopped

### Subject

This section explains how to lock keyboard and mouse when Enterprise SSO is stopped and no Authentication Manager authentication is asked.

### Procedure

- Set the **FUSBockInput** registry key (DWORD) to 1. (default value: 0).

  This registry key is located in `HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\SSOWatch\CommonConfig`
Locking Keyboard and Mouse at Startup

Subject

By default, at startup keyboard and mouse are not locked. If you want to lock keyboard and mouse at startup (because you are using the automatic logon in Windows for example) then you have to set the following registry key.

Procedure

- Set the `FUSBlockInputAtStartup` registry key (DWORD) to 1. (default value: 0).
  This registry key is located in `HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\SSOWatch\CommonConfig`

Configuring the Keyboard and Mouse Locking Timer

Subject

When a badge or a smart card is detected, keyboard and mouse are released to allow the user to type his secret. If no secret is entered after 300 seconds, then the authentication window is automatically closed and keyboard and mouse are locked. You can configure this timer as follows.

Procedure

- Set the `FUSAuthenticationDelay` registry key (DWORD) to the number of seconds you want before the authentication window closes. Default value is 300. 0 means deactivated.
  This registry key is located in `HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\SSOWatch\CommonConfig`
Configuring the Inactivity Timer

Subject

By default, if no user activity is detected during a while, Enterprise SSO goes into secure mode; a new authentication is then needed to perform SSO.

If you want to lock keyboard and mouse on inactivity timer, then the following registry key must be used. When this option is activated, Enterprise SSO is closed on inactivity timer. So Public Access FUS locks automatically keyboard and mouse since Enterprise SSO is not running.

Procedure

- Set the StopSSOEngineOnSecurityEvent registry key (DWORD) to 1. (default value: 0).
  
  This registry key is located in HKEY_LOCAL_MACHINE\SOFTWARE\Enatel\SSOWatch\CommonConfig

Configuring Application Closing

When a user locks a session (for Hierarchized and Shared Access FUS) or withdraws his/her device (for Public Access FUS), Enterprise SSO is closed but the user’s running applications remains open. To force Enterprise SSO to automatically close the user’s applications before switching context, an extension DLL must be written.

Tips for Writing and Using an Extension DLL

Description

The extension DLL exports the following functions:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnSessionLocked</td>
<td>Enterprise SSO calls these functions when it switches to the lock state (upon a smart card)</td>
</tr>
<tr>
<td>OnSessionUnLocked</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>removal or an elapsed inactivity timeout).</td>
</tr>
<tr>
<td>EngineStarted</td>
<td>Enterprise SSO calls these functions when it is started, stopped or when its configuration is reset. For more information: see Special Case 1 below and for more information on the EngineStartedV2 function, see Special Case 2.</td>
</tr>
<tr>
<td>EngineStartedV2</td>
<td></td>
</tr>
<tr>
<td>EngineStopped</td>
<td></td>
</tr>
<tr>
<td>EngineRestarted</td>
<td></td>
</tr>
<tr>
<td>OnWindowsSessionLocked</td>
<td>Enterprise SSO calls these functions when the Windows session is locked or unlocked</td>
</tr>
<tr>
<td>OnWindowsSessionUnlocked</td>
<td></td>
</tr>
<tr>
<td>OnWindowsSessionReconnected</td>
<td></td>
</tr>
<tr>
<td>OnWindowsSessionDisconnected</td>
<td></td>
</tr>
</tbody>
</table>

**Special Case 1**

When a user unlocks his/her workstation using an authentication device which is not the same as the device used to log on the workstation (for example, John Smith logs on the workstation at 8.00am using his smart card, then unlocks it using his RFID card at 02.00pm), Authentication Manager proceeds as follows:

1. It sets the **HKCU\SOFTWARE\Enatel\SSOWatch\WillRestartForUPN** registry value with the Windows user name
2. It stops Enterprise SSO.

**NOTE:** During shutdown, Enterprise SSO calls the EngineStopped function only if the WillRestartForUPN registry value is not set.

3. It starts Enterprise SSO.

**NOTE:** During startup, Enterprise SSO calls the EngineRestarted function only if WillRestartForUPN is set with the Windows user name. Else, Enterprise SSO calls the EngineStarted function and the registry value is deleted.

**Format**

The functions must be written according to the following format:

```c
typedef struct __CUSTOMPARAMETERS
{
    LPCSTR szUser;
} CUSTOMPARAMETERS, *PCUSTOMPARAMETERS;

BOOL APIENTRY OnSessionLocked(HWND hParent, const PCUSTOMPARAMETERS pcapParameters)
```
BOOL APIENTRY OnSessionUnLocked(HWND hParent, const PCUSTOMPARAMETERS pcapParameters)
{
    return TRUE;
}

BOOL APIENTRY EngineStarted(HWND hParent, const PCUSTOMPARAMETERS pcapParameters)
{
    return TRUE;
}

BOOL APIENTRY EngineStopped(HWND hParent, const PCUSTOMPARAMETERS pcapParameters)
{
    return TRUE;
}

BOOL APIENTRY EngineRestarted(HWND hParent, const PCUSTOMPARAMETERS pcapParameters)
{
    return TRUE;
}

BOOL APIENTRY OnWindowsSessionLocked(HWND hParent, const PCUSTOMPARAMETERS pcapParameters)
{
    return TRUE;
}

BOOL APIENTRY OnWindowsSessionUnLocked(HWND hParent, const PCUSTOMPARAMETERS pcapParameters);
{
    return TRUE;
}

BOOL APIENTRY OnWindowsSessionReconnected(HWND hParent, const PCUSTOMPARAMETERS pcapParameters);
{
    return TRUE;
}

BOOL APIENTRY OnWindowsSessionDisconnected(HWND hParent, const PCUSTOMPARAMETERS pcapParameters);
{
return TRUE;
}

**DLL location**

Enterprise SSO calls the extension DLL using the path set in the `HKLM\Software\Enatel\SSOWatch\ExternalCall\CustomDLLName` registry value. Example: `CustomDLLName = C:\SSO\MyDll.dll`

**Special Case 2**

The EngineStartedV2 function provides the authentication method used, as follows:

<table>
<thead>
<tr>
<th>Method</th>
<th>Returned Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>PWD</td>
</tr>
<tr>
<td>Non-EAM card</td>
<td>EXTCARD</td>
</tr>
<tr>
<td>Biometrics</td>
<td>BIO</td>
</tr>
<tr>
<td>Temporary password</td>
<td>TPA</td>
</tr>
<tr>
<td>EAM card</td>
<td>CARD</td>
</tr>
<tr>
<td>Badge</td>
<td>RFID</td>
</tr>
<tr>
<td>Session mode</td>
<td>SESSION</td>
</tr>
<tr>
<td>OTP</td>
<td>OTP</td>
</tr>
</tbody>
</table>

This function must be written according to the CUSTOMV2 definition as follows:

```c
typedef struct _CUSTOMPARAMETERSV2
{
    LPCSTR szUser;
    LPCSTR szAuthMethod;
} CUSTOMPARAMETERSV2, *PCUSTOMPARAMETERSV2;
typedef BOOL (APIENTRY *CUSTOMV2)(HWND hParent, const PCUSTOMPARAMETERSV2 pcapParameters);
```
Using the FUS Extension DLL Tool

Subject

The FUS Extension DLL once installed (see Installing the DLL), enables you to use the Configuration of FUS DLL tool. This tool is designed to help you configure automated actions on running applications when Enterprise SSO starts or stops on a workstation configured for Fast User Switching without Authentication Manager installed.

Description

The Configuration of FUS DLL tool is located here: %EAM installation folder%\UAConfFUSDll.exe and looks like this:

Figure 14: Configuration of FUS DLL

This tool enables you to execute the following actions:

- Mandatory step : activate the call to the FUS library : see Activating the call to the FUS library.
- Configure the window detection: see Configuring the window detection.
Execute specific commands at a given time: see Executing specific commands at a given time.

Configure the browsers: see Configuring the browsers.

Activate the Citrix Receiver (PNAgent): see Activating the Citrix Receiver (PNAgent).

Configure the forced stop of a process: see Configuring the forced stop of a process.

Call a FUS client library: see Calling a FUS client library.

Other actions: see Other actions.

IMPORTANT: Once you have finished the configuration, you must save it by clicking Save configuration. You must then select the directory where the configuration file is to be saved under the following form: UAConfFus_<Date>_<Time>.reg) Example: UAConfFus_01082014_17h23.reg).

Installing the DLL

1. Log-on as system administrator.
2. Run the EAM installation wizard and follow the instructions displayed in the wizard with the following guideline: at the features selection step, select FUS extension DLL.

IMPORTANT: Make sure the Authentication Manager and Integration with Windows features are not selected for installation. Replace this text with a notation that requires the reader's attention.

For more details on EAM advanced installation, see Evidian EAM Installation Guide.

Activating the call to the FUS library

IMPORTANT: You must activate the call to use the UAConfFUSDII.exe tool.
1. Execute **UAConfFUSDll.exe**.
   The tool opens.

2. Select the **Activate the call to the library FUS** check box.
   The **name** of the library is automatically filled in the corresponding field. Depending on your environment (32 or 64 bits), the name can be:
   - 32 bits: `<FUS library installation directory>\ExtSessionMgr.dll`
   - 64 bits: `<FUS library installation directory>\ExtSessionMgr64.dll`

3. Click **Change** if the name or path are not correct and select the correct name/path.
4. Click **Save configuration**.

### Configuring the window detection

This window enables you to configure the actions executed by the SSOEngine on the window detection. You can configure up to 32 window detections.

1. Execute **UAConfFUSDll.exe**.
   The tool opens.

2. Click **Actions on window detection**.
   The following window appears:
3. Configure the window and click **Ok**.
   
   **NOTE:** You must fill-in the **Title** field.

4. Click **Save configuration**.

### Executing specific commands at a given time

You can configure up to 32 commands.

1. Execute **UAConfFUSDII.exe**.
   
The tool opens.

2. Click **Command execution**.
   
The following window appears:
3. Click the button corresponding to the moment when you want the command to be executed.
   The following window appears (example: when SSOEngine is stopped):

4. Configure the window and click **Ok**, then **Quit**.

5. Click **Save configuration**.
Configuring the browsers

You can configure IE and Firefox to stop at the same time as the SSOEngine.

1. Execute **UAConfFUSDII.exe**.
   The tool opens.
2. Click **Treatment on browsers when the SSOEngine stops**.
   The following window appears:

   ![Treatment window](image)

   3. Configure the window and click **Ok**.
   4. Click **Save configuration**.

Activating the Citrix Receiver (PNAgent)

The actions will be executed on the Citrix Receiver. If you activate this configuration, the:

- PNAgent will be started due to SSOEngine start.
- PNAgent will be stopped due to SSOEngine stop (execution of 'PNAgent /disconnect' then 'PNAgent /logoff' and finally 'PNAgent /Terminate').
- 'PNAgent /disconnect' action is also executed during Windows session lock.
- 'PNAgent /reconnect' action is executed during Windows session unlock.

1. Execute **UAConfFUSDII.exe**.
   The tool opens.
2. Click **PNAgent (CITRIX)**.
The following window appears:

Figure 18: Citrix

If needed, execute the following actions:

a. Modify the title or the class defined by default if they are incorrect.
b. Fill-in the fields of the Parameters for PNAgent area to execute the PNAgent (SSOEngine start) with commands.
c. Click the Removing Citrix shortcuts button to define the shortcuts to delete when PNAgent stops and therefore when SSOEngine stops.
   You can delete up to 20 shortcuts.

3. Click Ok.
4. Click Save configuration.

Configuring the forced stop of a process

You can configure a process to stop at the same time as the SSOEngine stops. You can enter up to 32 process names.

1. Execute UAConfFUSDII.exe.
   The tool opens.
2. Click Killed process when the SSOEngine stops.
   The following window appears:
3. Enter the name of the processes and click Ok.
4. Click Save configuration.

**Calling a FUS client library**

1. Execute `UAConfFUSDII.exe`.
   The tool opens.
2. Click Call Customer DLL.
   The following window appears:

   ![Calling a client library](image)

   3. Select the library and click Ok.
   4. Click Save configuration.

**Other actions**

1. Execute `UAConfFUSDII.exe`.
   The tool opens.
2. Click **Various**.
   
The following window appears:

   **Figure 21: Miscellaneous**

3. If needed, select the following check boxes and click **Ok**:
   
   - **If the client "RemoteApp" This menu then select "Disconnect all connections"**: when SSOEngine stops, if the RemoteApp client of Microsoft is detected on the workstation, then all the connections are disconnected.
   
   - **Use "SplashScreen.exe" (No with MUD ou Authentication Manager)**: when SSOEngine stops, a **SplashScreen** window type is displayed on the whole of the screen for 5 seconds to warn the new user that a user switch is occurring.
     
     This mode does not work if the MUD or Authentication Manager are installed on the workstation.

4. Click **Save configuration**.
The Multi-User Desktop Feature

Overview and Use

Presentation

The Multi-User Desktop allows hosting several secure sessions in the same Windows session.

Welcome Screen

Multi-User Desktop is automatically started when the Windows session opens. A Welcome screen displays the list of available authentication methods and the list of disconnected user sessions. Authentication methods that are not authorized by the Access Point Security Profile are hidden, as shown hereunder for the contactless badge authentication method.
NOTE:

- To use the **Press if you have forgotten your password** tile, you must have previously chosen a set of questions and recorded the associated answers using the SSPR wizard, which is available in the Enterprise SSO popup menu.

- When a user authenticates in Multi-User Desktop mode with an unassigned RFID badge, he will be able to assign it with his credentials. He will have to choose a PIN if the RFID+PIN authentication method is activated.

This welcome screen either hides:

- The whole screen: **Kiosk** mode: see Kiosk Mode.
- Part of the screen, as a dialog box: **Control** mode: see Control Mode. In this mode, the welcome screen moves automatically or can be moved using the arrow keys. This enables the user to see the running applications in the background.

**NOTE:** The Multi-User Desktop feature is not compatible with a multi-screen display.

**Virtual Desktops**

When a user authenticates, only his applications are displayed. All other applications are automatically hidden and are unavailable for this user. When this user disconnects, his applications are automatically hidden and the welcome screen appears.

**NOTE:** You can exclude a set of these hidden applications to make them always visible for any user who authenticates.
Multi-User Desktop Authentication Modes

IMPORTANT: To use the mobile device authentication mode, you must have previously enrolled your mobile device from a workstation that does not use the Multi-User Desktop mode.

Kiosk Mode

This is the default mode. In Kiosk mode, the welcome screen of Multi-User Desktop uses the whole desktop space and hides the content of the Windows desktop.

In Kiosk mode, all authentication methods are allowed, including password, SSPR and mobile device. However, users cannot move/hide/terminate the welcome screen. To configure this mode, go to Configuring the Kiosk Mode.

Control Mode

In Control mode, the welcome screen appears in the center of the desktop.

The welcome screen changes position: it automatically moves clockwise on the desktop.

As an alternative to this automatic move, you can allow users to move the welcome screen using the arrow keys. Even if the keyboard is locked, the following keys are enabled:

<table>
<thead>
<tr>
<th>Key</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left arrow</td>
<td>10 pixels to the left</td>
</tr>
<tr>
<td>Right arrow</td>
<td>10 pixels to the right</td>
</tr>
<tr>
<td>Up arrow</td>
<td>10 pixels up</td>
</tr>
<tr>
<td>Down arrow</td>
<td>10 pixels down</td>
</tr>
<tr>
<td>Home</td>
<td>Top-left corner</td>
</tr>
<tr>
<td>End</td>
<td>Bottom-right corner</td>
</tr>
<tr>
<td>Page up</td>
<td>Top</td>
</tr>
<tr>
<td>Page down</td>
<td>Bottom</td>
</tr>
</tbody>
</table>

The mouse and keyboard can be locked: users cannot use these devices outside the welcome screen.

The welcome screen can be resized manually with the + and - keys and displays the following elements depending on its size:
• Full screen:
  • Customizable bitmap.
  • Authentication method buttons and texts.
  • List of users.
For more information on the customizable bitmap, please refer to Evidian EAM Customization Guide.
• Normal screen:
  • Title.
  • Authentication method buttons and texts.
  • List of users.
• No user:
  • Title.
  • Authentication method buttons and texts (no list of users).
• Minimum: only authentication method buttons.
• Invisible. To make it visible again, press the + key.
To configure this mode, go to Configuring the Control Mode.

Installing the Multi-User Desktop

1. Log-on as system administrator.
2. Run the EAM installation wizard and select the Custom installation mode.
3. Select the Multi User Desktop feature.
   • Make sure the Authentication Manager and Integration with Windows features are not selected for installation.
   • For more details on EAM advanced installation, see Evidian EAM Installation Guide.

Figure 23: Multi User Desktop
4. Click **Next** and follow the rest of the Wizard instructions.

5. Depending on your Windows version, execute one of the following actions:
   - Windows **XP/2003**: restart the workstation.
   - Windows **7/2008**: close the session.

   The Multi-User Desktop feature has been installed.

## Configuring the Multi-User Desktop Modes

### Configuring the Kiosk Mode

1. In EAM Console, from the **Directory** panel, click the access point security profile that applies to computers that is used for Multi-User Desktop.

2. In the **Multi User Desktop** tab, **Welcome screen** area, select **Full screen mode**.
3. Click the ▼ to specify the background color of the welcome screen (default color: white).

4. Click Apply.

**Configuring the Control Mode**

1. In EAM Console, from the **Directory** panel, click the access point security profile that applies to computers that is used for Multi-User Desktop.

2. In the **Multi User Desktop** tab, **Welcome screen** area, select **Transparent mode**:

---

**Figure 24: Multi User Desktop:Full screen mode**

![Configuration](image)

---

**Figure 25: Multi User Desktop:Transparent Mode**

![Welcome screen](image)
3. Configure the following elements:
   - **Lock keyboard and mouse** check box: users cannot use these devices outside the welcome screen.
   - **Move information window every**:
     - **Seconds field**: enter the number of seconds after which the welcome screen changes position.
     - **Manually check box**: enables users to move the welcome screen manually with the arrow keys.
   - **Information window is resizable** check box: enables users to resize the welcome screen by pressing the:
     - + key to increase the size.
     - - key to reduce the size.
   - **Allow reboot** check box: enables users to restart the workstation by clicking the **Reboot** button in the Welcome screen.
   - **Show help url** check box and field: enter a help URL in the field and select the check box to display a link in the Welcome screen.

4. Click **Apply**.

| NOTE: | Fore more information on the keys, please refer to **Control Mode**.

### Configuring the Exclusion of Applications

When switching between user sessions, Multi-User Desktop hides, displays or terminates applications unless they are listed in the **Always display windows of these processes** field. Applications in this list are ignored by Multi-User Desktop and are always displayed on the desktop.

1. In EAM Console, from the **Directory** panel, click the access point security profile that applies to computers that is used for Multi-User Desktop.
2. In the **Multi User Desktop** tab, **Welcome screen** area, enter the list of applications as named in the windows process list in the **Always display windows of these processes** field:
Figure 26: Multi User Desktop: Welcome Screen

NOTE:
- Separate the applications by commas or spaces.
- Some applications are automatically ignored by Multi-User Desktop: the Multi User Desktop itself, Enterprise SSO and the Windows task manager.

3. To activate this option for all opened applications, enter the * character in the process field. The windows of the opened application will always be displayed.
4. Click Apply.

Configuring Multi-User Desktop Session Management

Configuring Session Lock

Multi-User Desktop automatically locks a user session, i.e. disconnects it when the session has been inactive (neither keyboard nor mouse event) for a given period of time. The user is also automatically disconnected if another user authenticates. However, you can allow users to disconnect themselves manually. They can either:

- Use the Multi-User Desktop icon in the notification area and click Disconnect.
- Press the Win + K keys.
- Swipe their finger or withdraw their smart card or tap/withdraw their badge.

The default configuration is as follows:
- No automatic lock.
- No countdown.
Users can disconnect manually.

1. In EAM Console, from the Directory panel, click the access point security profile that applies to computers that is used for Multi-User Desktop and select the Multi User Desktop tab, Session Management area.

![Figure 27: Multi User Desktop:Session Management](image)

2. Configure the following elements:
   - **Automatically disconnect users after** field: enter the number of seconds after which the user is automatically disconnected.
   - **Show count down for last ... seconds before lock**: select this check box and enter a non null value to display a pop-up window which indicates the remaining seconds before automatic lock.
   - **Users can disconnect manually** check box: users can use the Multi-User Desktop icon in the notification area to lock their session.

3. Click **Apply**.

### Configuring Session Log Off

Multi User Desktop automatically logs off a disconnected session after a given period of time.

However, you can allow users to logoff manually. They can either:

- Use the Multi-User Desktop icon in the notification area and click **Logoff**.
- Press the **Win + Q** keys.

The **default configuration** is as follows:

- No automatic logoff.
- Users can log off manually.

1. In EAM Console, from the Directory panel, click the access point security profile that applies to computers that is used for Multi-User Desktop and select the Multi
User Desktop tab, Session Management area.

Figure 28: Multi User Desktop:Session Management

2. Configure the following elements:
   - **Automatically logoff users after** field: enter the number of seconds after which the user is automatically logged off.
   - **Users can logoff manually** check box: users can use the Multi-User Desktop icon in the notification area to log off.

3. Click **Apply**.

Configuring Concurrent Sessions

You can define the maximum number of concurrent sessions managed by Multi-User Desktop.

When a new user authenticates and creates a new session, Multi-User Desktop terminates the oldest session if needed, i.e. the session that has been locked for the longest period of time.

1. In EAM Console, from the **Directory** panel, click the access point security profile that applies to computers that is used for Multi-User Desktop and select the **Multi User Desktop** tab, **Session Management** area.

Figure 29: Multi User Desktop:Session Management
2. Set the **Max. number of concurrent sessions** field to configure the maximum number or concurrent sessions.
   Set this field to 0 (default value) to disable this feature.
3. Click **Apply**.

---

### Configuring Biometrics Enrolment

For a user to enroll his fingerprints, you must configure the Biometric enrolment parameter in E-SSO Console to enable the **Enroll** button in the **User Identification** window.

1. In EAM Console, from the **Directory** panel, click the access point security profile that applies to computers that is used for Multi-User Desktop and select the **Multi User Desktop** tab, **Session Management** area.

   ![Figure 30: Multi User Desktop:Session Management](image)

2. Check the **Allow biometrics enrolment** check box.
   Default behavior: biometrics enrolment is allowed.
3. Click **Apply**.

---

### Configuring the Information Display

You can display information about the connected user either directly on the Windows desktop wallpaper or on a toolbar that appears on the desktop.

**NOTE:** In addition to displaying information about the connected user, the toolbar provides a lock and a disconnect button.

1. In EAM Console, from the **Directory** panel, click the access point security profile that applies to computers that is used for Multi-User Desktop and select the **Multi User Desktop** tab, **Session Management** area.
2. Select the **Show infos** check box and select either **On the wallpaper** or **As a toolbar** in the drop down list. To customize the available information, see *Evidian EAM Console - Guide de l'administrateur*. 
The Roaming Session Mode

Roaming Session Mode - Overview and Use

Definition

The roaming session mode allows users to open a session (using Authentication Manager) on one or several computer(s) with their physical authentication token, without having to type a secret, during a defined period of time.

Mechanism Description

Figure 32: Mechanism Description
The administrator configures the roaming session mode on appropriate access points, and for a number of users for a defined duration.

A user authenticates on a computer on which the roaming session mode is available, whatever the authentication method is (login/password, smart card, active or passive RFID device, biometry).

This automatically creates a roaming session in the EAM Controller. If no EAM Controller is available, the roaming session is not created.

When the computer (on which the roaming session mode is activated) detects a physical authentication token (smart card, active or passive RFID), the roaming session is retrieved from the EAM Controller and the user is authenticated without having to type the secret associated with the token. The session duration time is displayed to the user in a task bar balloon help. If the roaming session expires when it is open on a computer, or
Phase Description

if the user password expires or is changed, the session remains open, but the user will have to authenticate at next session opening.

Prerequisites

- Make sure you have the "Session Management" license key.
- If users authenticate with a smart card for the roaming session, the smart card must meet the following requirements:
  - The smart card configuration must allow the owner name to be read without typing the PIN.
  - The smart card contains only one account.
  - No SSO account is stored on the smart card.

Restriction

In a roaming session, users cannot change their password or PIN with Authentication Manager.

Configuring the Roaming Session Mode

Subject

To make available the roaming session mode, you must activate it for concerned users, and on appropriate access points, as explained in the following sections.

Before Starting

To perform the tasks described in this section, you must have at least the following administration role:

- In classic administration mode: "Security object administrator".
- In advanced administration mode, your role must contain the following right: "User security profile: Creation/Modification" and "Access point security profile: Creation/Modification".
Activating the Roaming Session Mode for Users

Subject

You must activate the roaming session mode in the user security profile. For users associated with this profile, a roaming session will be automatically created after they have authenticated themselves with Authentication Manager on a computer that authorizes roaming sessions.

Procedure

1. In EAM Console, from the Directory panel, click the user security profile that applies to users that will use the roaming session mode.
2. Click the Security tab.
   The Security tab appears.
3. Select the Roaming session check-box and define the duration:
   - *x hours*: number of hours you want the session to be active. The roaming session is created as soon as the user authenticates on an authorized access point, and the session duration time starts from that moment. At the end of the duration time, the user will have to type a secret.
   - **No duration limit**: if you select this check-box the roaming session is created as soon as the user authenticates on an authorized access point, with no duration time. The user will never have to type a secret again.
Figure 33: Roaming Session

**IMPORTANT:** If you change the duration time parameter once the roaming session has started, the new value will only be taken into account once the session in progress has expired, or has been deleted by the user (see Administering Current Roaming Session From the User’s Workstation) or by the administrator (see Administering User’s Roaming Sessions From EAM Console).

4. Click **Apply**.

**Activating the Roaming Session Mode on Computers**

**Subject**

You must activate the roaming session mode in the access point security profile. For computers associated with this profile:

- A roaming session is automatically created when authorized users authenticate on these computers.
- The roaming session is automatically retrieved when an authorized user presents a physical authentication token; this automatically opens the user session if it exists.
To optimize the session opening time, we recommend to allow the roaming session mode only on access point that will actually use it.

Procedure

1. In EAM Console, from the **Directory** panel, click the access point security profile that applies to computers on which activating the roaming session mode is necessary.

2. In the **Authentication Manager** tab, select the **Allow roaming session** check-box.

![Figure 34: Authentication Manager](image)

3. Click **Apply**.

Administering User’s Roaming Sessions

From EAM Console, you can display information on users’ roaming session duration, and decide to delete it for a selected user: see Administering User’s Roaming Sessions From
EAM Console
From his/her workstation, the user can also display information on his/her own roaming session duration, and also delete it: see Administering Current Roaming Session From the User’s Workstation.

Administering User’s Roaming Sessions From EAM Console

Subject
You can see information on user roaming sessions from EAM Console, as explained in the following procedure.
You can decide to delete a roaming session. In this case, the current user session remains open, but this forces the user to authenticate again at next session opening. This also allows you to disable the roaming session in case a user has lost his/her token.

Before Starting
To perform the task described in this section, you must work in advanced administration mode, and your role must contain the following right: "Roaming: Delete user’s sessions".
For more information on administration modes, see Evidian EAM Console - Guide de l'administrateur.

Procedure

1. In EAM Console, from the Directory panel, click the user for whom you want to display the roaming session information.
2. In the Connection tab, select the Authentication tab.
   The roaming session duration time left for the selected user appears.
3. To delete the displayed roaming session, click the **Delete roaming session** button. The current user session remains open on the computer, but he/she will have to authenticate again at next session opening.

---

**Administering Current Roaming Session From the User’s Workstation**

**Subject**

From his/her workstation, a user can administer his/her own roaming session: he can decide to delete a roaming session. In this case, the current user session remains open.

The functionality described in this section is not available if the user has authenticated with his password, or with Biometrics.
Procedure

1. On the workstation, in the notification area, right-click the Authentication Manager icon and click **Roaming Session**.
   The following window appears, it displays the roaming session duration time left.

   **Figure 36: Roaming Session Management**

   ![Roaming Session Management](image)

   Your current roaming session expires on:
   Tuesday, June 25, 2013 4:45:36 PM

   Once your roaming session expires or is terminated, you will have to enter your password or PIN to access your workstation.

   You can press the Terminate button to stop the roaming capability of your current session.

   [Terminate] [Cancel]

2. To delete the roaming session, click **Terminate**.
   The current user session remains open.
The Double-Login Prevention Feature

Double-Login Prevention - Overview and Use

Definition

The **Double-Login Prevention** feature ensures that when a user is authenticating on a computer, the session opened on the previously used computer is locked.
Mechanism Description

Figure 37: Double-Login Prevention

The administrator configure the Double-Login Prevention function for a number of users.

A user authenticates on a computer by password, passive RFID or biometrics.

The session opens.

The user authenticates on another computer by password, passive RFID or biometrics, without having locked his/her previous session.

The session opens on the current computer, and the session which was open on the previous computer is locked.

Table 8: Double-Login Prevention

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The administrator configure the Double-Login Prevention function for a number of users.</td>
</tr>
<tr>
<td>2</td>
<td>A user authenticates on a computer by password, passive RFID or biometrics. The session opens.</td>
</tr>
<tr>
<td>3</td>
<td>The user authenticates on another computer by password, passive RFID or biometrics, without having locked his/her previous session. The session opens on the current computer, and the session which was open on the previous computer is locked.</td>
</tr>
</tbody>
</table>
Prerequisites

- EAM must be configured in "manage-access-point" mode.
- An EAM Controller must be available.
- For this functionality to work properly, the computers must be connected to the network.
- Port 3644 must be open on computers so that SSO Clients can communicate.

Configuring EAM Controllers (Optional)

Subject

As Double-Login Prevention information is stored in the directory, directory architecture and replication time (in case several servers are replicated) must be taken into account. The Double-Login Prevention feature can only work if the time it takes for the user to change computer is longer than the time it takes to replicate data between all directory servers.

If replication time is too long, you can configure EAM Controllers to make them use a list of directory servers according to their availability, as detailed in the following procedure.

Procedure

- If EAM is installed in Corporate directory mode (in this mode, security objects are stored in the company directory), set the following registry key (REG_SZ. or Policies type):
  Enatel\WiseGuard\FrameWork\Directory\UniquenessSessionServerList

  **NOTE:** With this key, the Double-Login Prevention feature does not work in case of inter-domain (e.g. the user authenticates on a computer that is not part of his/her domain).

- If EAM is installed in Dedicated directory mode (in this mode, security objects are stored in a dedicated directory), set the following registry key (REG_SZ. or Policies type):
  Enatel\WiseGuard\FrameWork\WGDirectory\UniquenessSessionServerList

  **NOTE:** With this key, inter-domain can work.
Activating Double-Login Prevention From EAM Console

Subject

You must activate the Double-Login Prevention function in the user security profile, as explained in the following procedure. For users associated with this profile, Double-Login Prevention function will be automatically active after they have authenticated themselves with Authentication Manager.

Procedure

1. In EAM Console, from the Directory panel, click the user security profile that applies to users that will use the Double-Login Prevention function.
2. Click the Authentication tab.
3. Select the User can have only one active Windows session check-box.
4. Click **Apply**.
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