



One Identity Authentication Manager
Cluster 9.0.2

Administrator's Guide

Copyright 2017 One Identity LLC.

ALL RIGHTS RESERVED.

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

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS 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.

Preface

| | |
|---------------------------|--|
| Subject | This guide explains how to configure and use the Cluster feature. |
| Audience | This guide is intended for: <ul style="list-style-type: none">• EAM (Enterprise Access Management) administrators who know how to use EAM Console.• 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 | <p>Bold Indicates:</p> <ul style="list-style-type: none">• Interface objects, such as menu names, buttons, icons and labels.• File, folder and path names.• Keywords to which particular attention must be paid. <p><i>Italics</i> - Indicates references to other guides.</p> <p>Code - Indicates portions of program codes, command lines or messages displayed in command windows.</p> <p>CAPITALIZATION Indicates specific objects within the application (in addition to standard capitalization rules).</p> <p>< > Identifies parameters to be supplied by the user.</p> <p> WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.</p> <p> CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.</p> <p> IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.</p> |
| 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. |

Contents

| | |
|---|-----------|
| Preface | 3 |
| Overview | 7 |
| Cluster of Access Points - Mechanism | 7 |
| Definitions | 7 |
| Behavior of Workstations Included in a Cluster | 8 |
| Session Delegation - Mechanism | 10 |
| Definitions | 10 |
| Behavior of Delegated Workstations | 11 |
| Required EAM Modules | 11 |
| Administering Clusters From EAM Console | 12 |
| Creating and Configuring a Cluster of Access Points | 12 |
| Managing Users' Permissions on a Cluster | 16 |
| Authorizing Users to Access Workstations of the Cluster | 17 |
| Displaying the Cluster Composition Made by Authorized Users | 18 |
| Configuring and Administering Session Delegation | 18 |
| Authorizing Users to Delegate Their Windows Session | 18 |
| Authorizing Users to Delegate Their Session to other Users | 19 |
| Authorizing Users of the same Group to Delegate Their Session to Members of their Group | 22 |
| Displaying Delegated Sessions | 23 |
| Displaying Cluster Event Logs ('Events' Tab) | 24 |
| Renaming Clusters | 25 |
| Deleting Clusters | 26 |
| Customizing the Data Displayed on the Desktop | 26 |
| Managing a Cluster from your Workstation | 28 |
| Creating and Configuring your Cluster | 29 |
| Managing the Cluster Composition | 29 |
| Attaching a Workstation to Your Cluster | 29 |
| Subject | 29 |
| Before starting | 29 |

| | |
|---|-----------|
| Procedure | 29 |
| Releasing a Workstation from your Cluster | 31 |
| Before starting | 31 |
| Procedure | 32 |
| Renaming your Workstation | 32 |
| Executing Maintenance Operations on Your cluster | 34 |
| Removing Temporarily a Workstation from the Cluster | 34 |
| Rebooting your Cluster | 34 |
| Refreshing the Displayed Data | 35 |
| Managing Session Delegation | 37 |
| Configuring Session Delegation | 37 |
| Configuring Session Delegation in a Cluster | 37 |
| Setting a Temporary Session Delegation | 38 |
| Subject | 38 |
| Procedure | 38 |
| Ending a Temporary Session Delegation | 41 |
| Subject | 41 |
| Procedure | 41 |
| Setting a Permanent Session Delegation | 42 |
| Subject | 42 |
| Procedure | 42 |
| Ending a Permanent Session Delegation | 43 |
| Subject | 43 |
| Procedure | 43 |
| Configuring Session Delegation outside a Cluster | 44 |
| Setting a Session Delegation | 44 |
| Procedure | 44 |
| Ending a Session Delegation | 45 |
| Procedure | 45 |
| Accessing a Colleague's Workstation | 46 |
| Accessing a Colleague's Workstation in a Cluster | 46 |
| Taking control over another workstation | 47 |
| Ending the control over a Workstation | 48 |
| Accessing a Colleague's Workstation outside a Cluster | 48 |
| Taking control over another workstation | 48 |

Ending the control over a Workstation49

Overview

The Cluster mode is intended to employees who have on their desk several computers and need to use them simultaneously. This function is particularly used in financial institution trading rooms or control rooms.

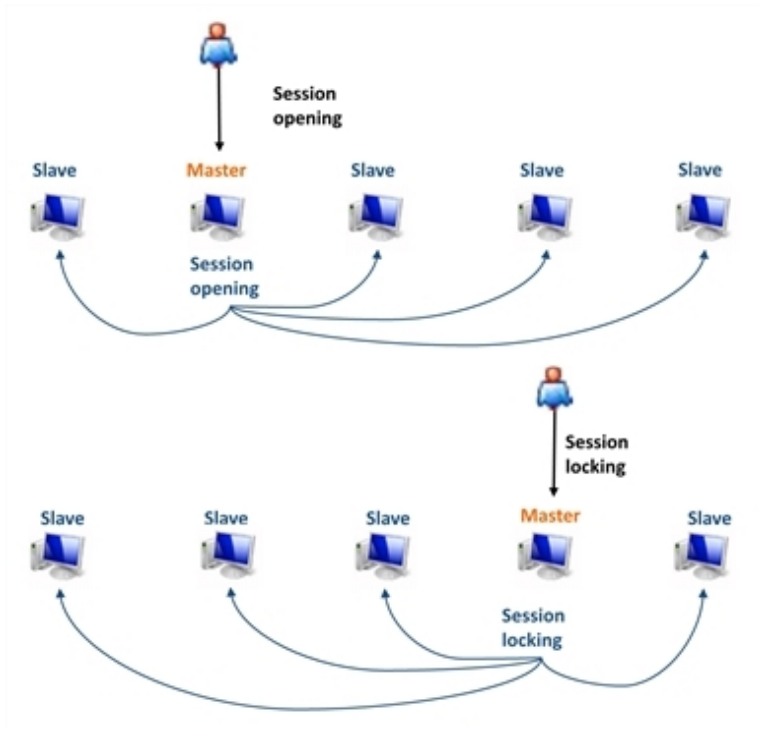
The cluster mode can be combined with Session Management functionalities. For details, see [Authentication Manager Session Management Administrator's Guide](#).

Cluster of Access Points - Mechanism

Definitions

A cluster of access points is a set of computers on which the Windows sessions are synchronized by EAM. Operations that a user performs on the Windows session (opening, closing, locking, unlocking) of a computer that belongs to the cluster are automatically and simultaneously performed on all the other computers that form the cluster, as illustrated in the following figure:

Figure 1: Cluster of Access points



The number of workstations you can include in a cluster is not limited.

In a cluster of access points, the computer on which the user performs an operation on the Windows session is called the master computer. The same action is simultaneously performed on the other computers of the cluster, called slaves.

IMPORTANT: An EAM Controller does not work in Cluster mode.

Behavior of Workstations Included in a Cluster

When a user performs an operation (opening, closing, locking, unlocking) on a computer, this computer becomes the master computer and periodically informs the slave computers of the operation performed. This allows the management of slave computer behaviors.

- **Session Opening/Session Unlocking**
 - The cluster function is compatible with all available EAM authentication methods (password, smart card, passive and active RFID, biometrics). When a user opens a session on a computer of the cluster, all the sessions of other computers of the cluster open with the same user account.

- If a slave computer is not reachable at session opening on the master computer, the session opening operation on this slave computer will be performed as soon as the network is restored.
 - If a slave computer restarts, and if the last operation performed on the master computer is a session opening, a session will be opened on this slave computer as soon as it is available.
 - If the session of a slave computer is locked by another user, the session is unlocked only if the Fast User Switching (FUS) option is activated for the user (for more details on FUS, see *One Identity Authentication Manager Session Management Administrator's Guide*).
If a user performs a FUS on a computer, all the other computers of the cluster perform the FUS.
 - If an "Excluded Account" opens a session on a computer that is part of the cluster, this computer is automatically excluded from the cluster.
For more information on excluded accounts, see *One Identity EAM Console Administrator's Guide*.
- **Session Locking**
 - When a computer is locked, all the other computers are locked according to their defined lock mode (see [Creating and Configuring a Cluster of Access Points](#)).
 - If a slave computer with an open session does not receive any information from the master for a period of 30 seconds, it is automatically locked according to its defined lock mode (see [Creating and Configuring a Cluster of Access Points](#))

- **Session Closing**

When the user closes a computer, all the other computers of the cluster are closed

NOTE: A slave computer can only accept orders from the master computer if they are compatible with its current session. For example, if a user locks a computer session while all the other cluster computer sessions are closed, these sessions will remain closed.

- **Screensaver**

When a computer screensaver is activated, the computer is not locked. It becomes locked at the end of the screensaver period: it then becomes the master and locks all computers of the cluster.

You must configure the screensaver according to the wanted computer behavior.

- **Reboot**

The user can decide to reboot one or several workstations of his/her choice or the whole cluster at once.

Session Delegation - Mechanism

Definitions

Subject

If for any reason a user has to leave his/her cluster, he/she can delegate his/her Windows session to one or more delegate(s) to monitor or intervene in any of his/her ongoing operations.

Delegation Types

The session delegation can be temporary or permanent:

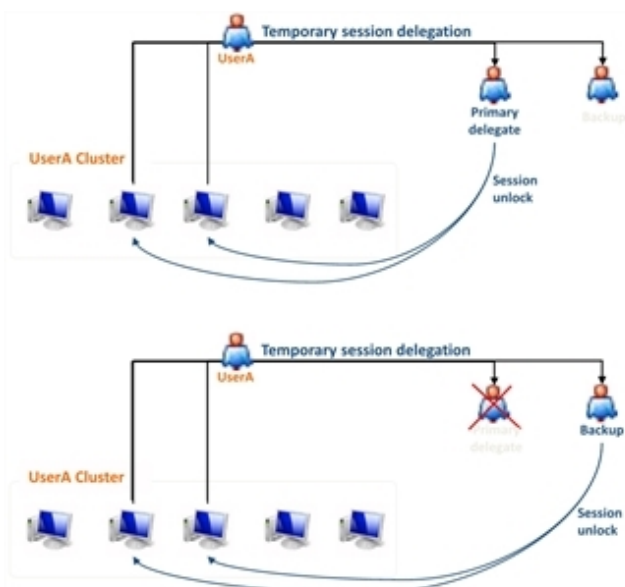
- **Temporary Session Delegation**

To setup a temporary delegation, a user defines a Primary delegate and (if any) a Backup who can access one or several of his/her Windows sessions when he/she is away.

The delegation ends when the user authenticates again.

The following figure illustrates the temporary delegation:

Figure 2: Temporary Session Delegation



In a temporary delegation, there are two delegates:

- The Primary delegate is the main person to whom the user delegates his/her session(s).
 - The Backup delegate is the person monitoring the user workstation if the Primary delegate is not available.
- **Permanent Session Delegation**

To setup a permanent delegation, a user defines one delegate who can access one or several of his/her Windows sessions when he/she is away.

The delegation does not end when the user authenticates again. He/she must explicitly remove it to cancel it.

Behavior of Delegated Workstations

A delegated workstation is not entirely included in the cluster of the delegate, but the operations performed on the cluster have consequences on the delegated workstation. If the delegate:

- Locks his/her cluster, the delegated workstation locks.
- Closes his/her cluster, the delegated workstation locks.
- Locks or closes the delegated workstation, these operations are not propagated to his/her cluster.

Required EAM Modules

To use the Cluster function, the following EAM modules must be installed :

- EAM Console: mandatory.
- Authentication Manager: mandatory.
- Enterprise SSO: optional.

For more information on installation of EAM (Enterprise Access Management) modules, see *One Identity EAM Installation Guide*.

Administering Clusters From EAM Console

EAM Console allows you to create and configure clusters of access points, and to authorize users to manage their own cluster.

Creating and Configuring a Cluster of Access Points

Subject

The following procedure explains how to create a new cluster of access points, and configure it:

- You can authorize users to temporarily remove a computer from the cluster.
- You can define a locking behavior for each computer of the cluster.
- You can define reboot options for the cluster.

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: "Cluster: Creation/Modification".

NOTE: For more information on administration modes, see [One Identity EAM Console Administrator's Guide](#).

- Make sure that none of the computer you want to place in the cluster is an EAM Controller.
- Make sure all the computers you want to gather in a cluster are connected to each other, and configured according to your needs (automatic screen-saver launching, locking).

- DNS resolution must work properly so that orders sent from the master can be easily transmitted to slaves.
- Port 3644 must be open on all computers you want to gather in a cluster.
- EAM must be configured in "manage-access-point" mode.
- The "Cluster Server" license keys must be installed on the EAM Controller and the "Cluster Client" license keys must be installed on all EAM workstations on which you want to use the Cluster feature.

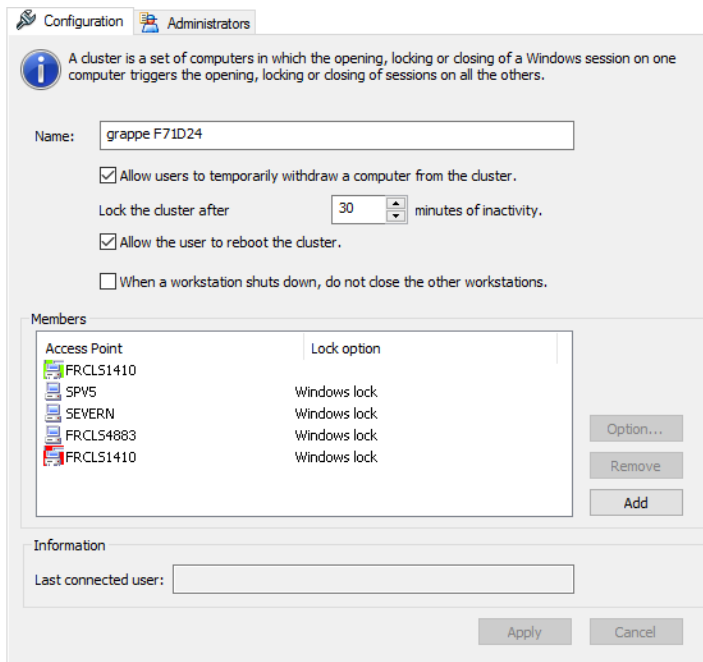
Procedure

1. In EAM Console, in the tree structure of the **Directory** panel, right-click the Organizational Unit that must contain your Cluster of access points and select **New\Cluster of access points**.
The **Configuration** tab appears.
2. Fill in the **Name** field.
3. Click the Add button to select the access points you want to add to the cluster. Use the Browse tab to browse the directory tree structure or use the **Search** tab to find the access point by typing its name.
4. Define the cluster properties as explained in the following ["Configuration" Tab Description](#) section.
5. Click Apply.

The Cluster object is created and configured.

"Configuration" Tab Description

Figure 3: Configuration Tab



- Allow users to temporarily withdraw a computer from the cluster check box
If this check box is selected, users allowed to access one of the cluster computer will be able to temporarily exclude a computer from the cluster, from the Authentication Manager application module: see [Removing Temporarily a Workstation from the Cluster](#) for more details.
- **Lock the cluster after x minutes of inactivity**
This option allows you to define the period of inactivity after which all the computers of the cluster will be automatically locked.
The computers are locked according to the locking behavior you have defined in the Cluster Lock Mode window: see [Option button](#) below.
 - ❗ **IMPORTANT:** For this function to work properly, you must deactivate the Windows locking and screensaving mechanisms on all the computers of the cluster.
- Allow the user to reboot the cluster check box
Check box selected: users allowed to access one of the cluster computer can simultaneously restart all the computers of the cluster by launching a command menu from the Authentication Manager application module: see [Managing the Cluster Composition](#).
Check box cleared: users are not allowed to reboot all the computers of the cluster.




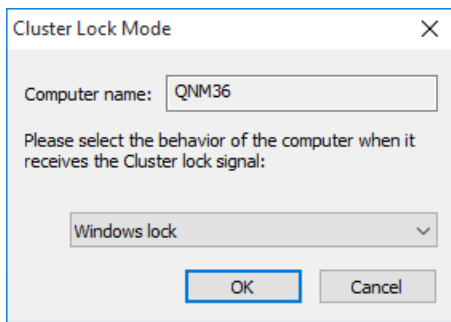
- When a workstation shuts down, do not close the other workstations check box
 Check box selected: if a user restarts a computer of the cluster, the sessions of the other computers remain in the state they were before the reboot operation.
 Check box cleared: if a user restarts a computer of the cluster, the sessions of the other computers are closed.
- Members table
 This area displays the list of access points that are part of the current cluster and their defined lock mode (see the following [Option button](#)).
 If you have authorized a list of users to add/remove access point of the current cluster to/from their own cluster (see [Authorizing Users to Access Workstations of the Cluster](#)), this area gives information on how authorized users have composed their own cluster (for more details, see [Managing the Cluster Composition](#)), by the use of colored icons:
 -  : the access point is not originally part of the cluster. It has been added to the cluster by an authorized user.
 -  : the access point is originally member of the cluster and has been separated from it by an authorized user who has included it in his/her own cluster.
 -  : the access point is originally member of the cluster and has not been separated from or added to it by a user.
- Option button
 Gives access to the Cluster Lock Mode window.

Figure 4: Cluster Lock Mode



For each computer of the cluster, this button allows you to define its behavior as a slave in the following cases:

- When it receives a locking order from the master computer.
- When it is directly locked.
- When it does not receive any order from the master for more than 30 seconds.
- **Transparent lock with logo**

The keyboard and mouse of the selected computer are disabled and a logo appears on top of the screen.

Information displayed on screen remains visible.

To modify the logo displayed on screen, save a WGLock.bmp file (500x72px) corresponding to the wanted logo in the EAM Client installation folder (the default folder is Program Files\One Identity\Enterprise Access Management).

Pressing **Ctrl+Alt+Del** on this computer displays the standard unlock window.

- **Transparent lock**

The keyboard and mouse of the selected computer are disabled.

Information displayed on screen remains visible.

Pressing Ctrl+Alt+Del on this computer displays the standard unlock window.

- **Windows lock**

The selected computer is locked. The standard lock window appears on the screen.

- Remove button

Removes the selected computer from the cluster.

- Add button

Allows you to select the access points you want to add to the cluster.

The Browse tab allows you to browse the directory tree structure and the **Search** tab allows you to find the access point by typing its name.

- Information area

This area displays the name of the last user who connected to the cluster of access points.

Managing Users' Permissions on a Cluster

This section explains how to give more autonomy to users of clusters by allowing them to manage their own cluster: you can authorize them to add to their own cluster some access points that are originally part of another cluster.

If a user adds an access point to his/her own cluster, the access point stays linked to the original cluster. When the user decide to release the access point, it is automatically associated back to its original cluster.

For more details on the conditions under which a user can attach a new access point to its cluster, see [Attaching a Workstation to Your Cluster](#)

Authorizing Users to Access Workstations of the Cluster

Subject

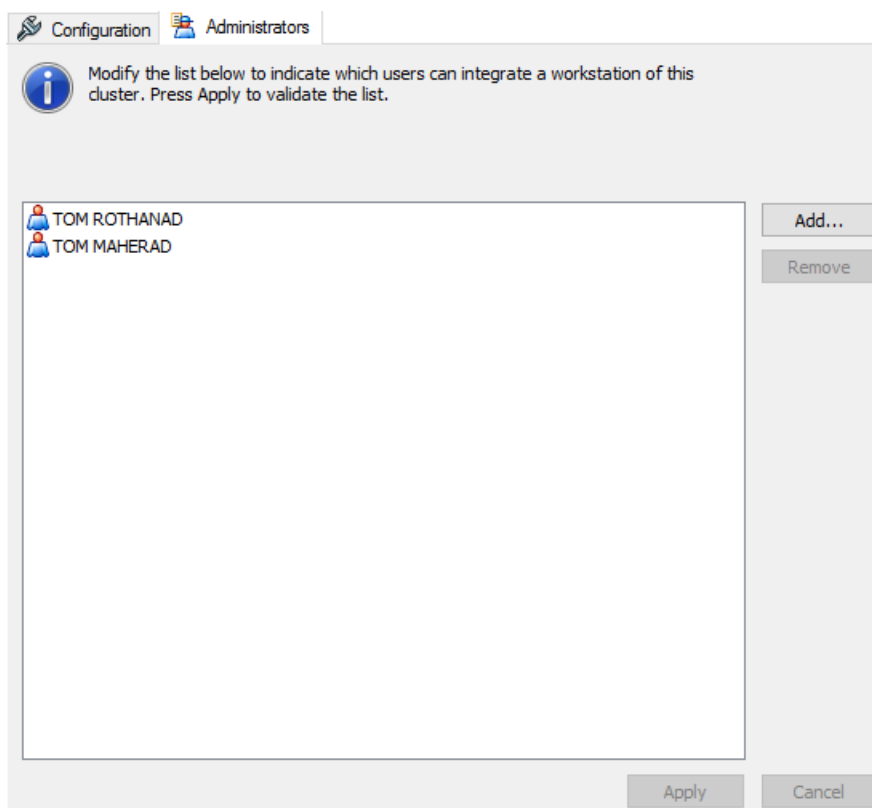
You can authorize some users to add (and remove) access points to their own cluster (see [Managing the Cluster Composition](#)).

For that, you need to define the list of users allowed to appropriate access points of the cluster.

Procedure

1. In the tree structure of the **Directory** panel, click the Cluster of access points that you want to make accessible to users of other clusters.
2. Click the **Administrators** tab:

Figure 5: Administrators tab



3. Click the **Add** button and select the users that you want to authorize to extend their own cluster with the access points included in this cluster.
Use the **Browse** tab to browse the directory tree structure or use the Search tab to find the user by typing its name.
4. Click **Apply**.
The list of users displayed in the tab is allowed to add the access points contained in the cluster into their own cluster.

Displaying the Cluster Composition Made by Authorized Users

Once you have authorized some users of other clusters to access workstations of the selected cluster, they are free to add or remove available access points to their own cluster (as described in [Managing the Cluster Composition](#)).

The Configuration tab allows you to visualize the user-made composition of the cluster. You cannot modify this temporary composition.

In this tab, the Members table displays the list of access points composing the cluster, and colored icons give information on their state. For more information on the meaning of colors, see [Members table](#) in [Creating and Configuring a Cluster of Access Points](#).

Configuring and Administering Session Delegation

For a general overview of the session delegation mechanism, see [Session Delegation - Mechanism](#).

For more details on the conditions under which a user can delegate a session, see [Managing Session Delegation](#).

Authorizing Users to Delegate Their Windows Session

To authorize users to delegate their Windows session, you can:

- Set delegation permissions to users in and outside clusters in their user security profile, so that they can delegate their Windows session to other users that you can define: see [Authorizing Users to Delegate Their Session to other Users](#).

- Set delegation permissions to a group of cluster users, so that they can delegate their Windows session to members of the same group: see [Authorizing Users of the same Group to Delegate Their Session to Members of their Group](#).

Authorizing Users to Delegate Their Session to other Users

Subject

The Session delegation tab of a user security profile allows you to authorize users to delegate their Windows session to another user.


Procedure

1. In the tree structure of the **Directory** panel, click the user security profile that applies to users for which you want to authorize session delegation.
2. Click the **Session Delegation** tab.
The tab appears.
3. In the **Session delegation type** field, select **Temporary** and define the delegation parameters for temporary delegation as described in the following "[Session delegation](#)" [Tab Description](#).
4. In the **Session delegation type** field, select **Permanent** and define the delegation parameters for permanent delegation as described in the following "[Session delegation](#)" [Tab Description](#).
5. Click **Apply**.

"Session delegation" Tab Description

Figure 6: Session Delegation tab

| Authentication | Security | SSO and Notes | Cloud | Unlocking |
|-------------------------------|------------|--------------------|-----------|---------------|
| Self Service Password Request | Biometrics | Session delegation | Audit OTP | Mobile Device |

 These options enable administrators to authorize/forbid session delegation. Allowed users can delegate their Windows session to another user. This user can then unlock the Windows session if needed.

Properties

Session delegation type:

Re-authentication is needed

Temporary delegation needs an approval

Delegate has seconds to accept/decline the delegation demand.

Authorize delegation to all users

Authorize delegation to members of the same group

Authorize delegation to members of the same organizational entity

Advanced mode (build the list of authorized users/groups/organizational entities):

- **Session delegation type**

The user can decide to delegate his/her session temporarily or permanently. Both options are available to the user, so you must configure each of them.

- Temporary: when a user delegates his/her session, the session is delegated until he/she re-authenticates.
- Permanent: when a user delegates his/her session, the session is delegated until he/she ends the delegation authorization through the **Manage Session Delegation** menu in **Authentication Manager**.

- **Re-authentication is needed** check box

This check-box allows you to define whether users must re-authenticate when they want to access the Cluster wizard (from which they can delegate their session) or the Set temporary session delegation shortcut command. See [Managing a Cluster from your Workstation](#) for more details on how users can access these tools. For Session delegation **outside a cluster**, this check box must be selected.

- Check box selected: when the user launches one of the delegation tool, an authentication window appears on his/her workstation.
- Check box cleared: the user does not need to authenticate again on his/her workstation when he/she launches one of the delegation tool.

- **Temporary delegation needs an approval** check box

This check box is only available if the Temporary session delegation type is selected.

- Check box selected: a user who wants to delegate his/her session needs the approval of the delegate.

In this case, when a user selects a user to whom he/she wants to delegate his/her session, a delegation proposal window appears on the delegate's

workstation. The delegate can accept or reject the proposal. The asking user window is frozen until all selected users have given an answer.

Delegate has x seconds to accept/decline the delegation demand

Period of time during which the delegation proposal window appears on the delegate's workstation. If no answer is given during this period of time, the delegation demand is either sent to the Backup delegate (if any), or declined.

- Check box cleared: a user can delegate his/her session to another user without collecting his/her approval. An information window appears on the delegate's workstation to inform him/her that a delegation has been set.

For Session delegation, one of the following check boxes must be selected:

- **Authorize delegation to all users** check box
 - Check box selected: users are authorized to delegate their Windows session to all users of the directory.
 - Check box cleared: users are not authorized to delegate their Windows session to all users of the directory.
- **Authorize delegation to members of the same group** check box
 - Check box selected: users are only authorized to delegate their Windows session to members of the same group of users.
 - Check box cleared: users are not authorized to delegate their Windows session to members of the same group of users.
- **Authorize delegation to members of the same organizational entity** check box
 - Check box selected: users are only authorized to delegate their Windows session to members of the same organizational unit.
 - Check box cleared: users are not authorized to delegate their Windows session to members of the same organizational unit.
- **Advanced mode** (build the list of authorized users/groups/organizational entities) check box
 - Check box selected: users are only authorized to delegate their Windows session to the users listed in the [Advanced Mode area](#) (see below).

Advanced Mode area

Displays the list of users to whom users of the profile are authorized to delegate their session.

- Add button: opens the user selection window, which allows you to add users to the list.
Use the Browse tab to browse the directory tree structure or use the Search tab to find the user by typing its name.
- Remove button: removes the selected user/group/organizational unit from the list.
- **Check box cleared:** no specific of authorized users is defined.

Authorizing Users of the same Group to Delegate Their Session to Members of their Group

Subject

You can define additional security policy parameters on groups of users. These parameters are added to the user security profiles applied to the members of the group.

The Policies tab (only available from a group object) is dedicated to Cluster users and allows you to authorize members of the group to delegate their Windows session to another member of the group.

Before Starting

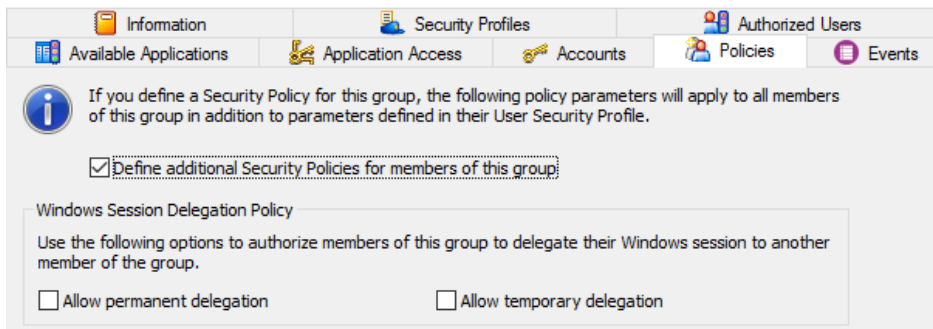
- This section only applies to groups of users who use cluster of access points.
- To perform the task described in this section, you must have at least the following administration role:
 - In classic administration mode: "Security object administrator".
 - In advanced administration mode: your role must contain the following right: "Group policy: Modification".

i **NOTE:** For more information on administration roles, see *One Identity EAM Console Administrator's Guide*.

Procedure

1. In the tree structure of the **Directory** panel, select the wanted group of users.
2. Click the **Policies** tab:

Figure 7: Policies tab



3. Select the **Define additional Security Policies for members of this group** check box.
4. In the **Windows Session Delegation Policy** area, select the check box corresponding to the type of delegation you want to authorize to members of the group:
 - Allow permanent delegation: when a user delegates his/her session, the session is delegated until he/she ends the delegation authorization through the Cluster wizard.
 - Allow temporary delegation: when a user delegates his/her session, the session is delegated until he/she re-authenticates.
5. Click **Apply**.

Displaying Delegated Sessions

Subject

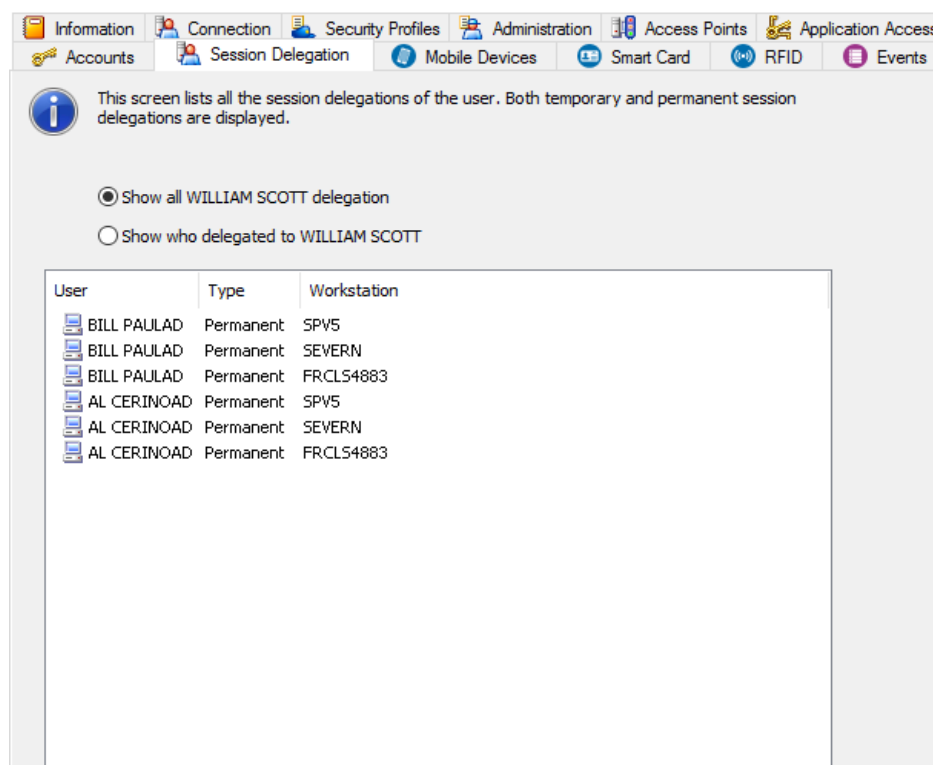
You can display the list of delegations made by users but you cannot modify them.

NOTE: To configure the session delegation parameters for users, see [Authorizing Users to Delegate Their Windows Session](#).

Procedure

1. In the tree structure of the **Directory** panel, click the user for which you want to display session delegations.
2. Click the **Session Delegation** tab.

Figure 8: Session Delegation tab



3. Click **Show all <user name> delegation** to display the list of users to whom the selected user has delegated his Windows session, the type of delegation (permanent or temporary) and the workstation it concerns.
4. Click **Show who delegated to <user name>** to displays the list of users who have delegated their session to the selected user, the type of delegation (permanent or temporary) and the workstation it concerns.

Displaying Cluster Event Logs ('Events' Tab)

Subject

The **Events** tab allows you to display all the events that are directly or indirectly linked to the selected object, for a defined period (the last two days by default). This report contains both User action and administration log entries.

Restriction

The **Events** tab appears only if you have at least the following administration role:

- In classic administration mode: "Auditor".
- In advanced administration mode, your role must contain the following right: "Audit: Visualization".

i **NOTE:** For more details on administration roles, see *One Identity EAM Console Administrator's Guide*.

Procedure

1. In the tree structure of the **Directory** panel, select the wanted Cluster.
2. Click the **Events** tab.
The **Events** tab appears.
3. In the **Filter** area, define a period of time to filter the log entries and click **Apply** (for more information on event logs, see *One Identity EAM Console Administrator's Guide*).

Renaming Clusters

Subject

This section describes how to rename a Cluster.

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: "Cluster: Creation/Modification".

i **NOTE:** For more details on administration roles, see *One Identity EAM Console Administrator's Guide*.

Procedure

1. In the tree structure of the **Directory** panel, right-click the Cluster and select **Rename**.
2. In the **Configuration** tab, type the new name of the object and press **Enter**.

Deleting Clusters

Subject

This section describes how to delete Clusters.

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: "Cluster: Deletion".

i | **NOTE:** For more details on administration roles, see *One Identity EAM Console Administrator's Guide*.

Procedure

In the tree structure of the **Directory** panel, right-click the Cluster to delete and select **Delete**.

The Cluster is deleted.

Customizing the Data Displayed on the Desktop

Subject

This section describes how to customize the information that appears in the foreground of the user's desktop.

Procedure

1. In the tree structure of the **Directory** panel, select the Access Point security profile associated with the access points that are members of the cluster.
2. In the **Security Services** tab, click the **Wallpaper** button.

The following window appears:

Figure 9: Wallpaper information

Wallpaper Information

Position (in pixels)

From top: 50

From right: 50

Width: 250

Font and colors

Font: Tahoma Sample Text

Size: 14

Color: FFFFFFFF

Large size: 20

Shadow color: 808080

Information

Show product name

Show product version

Show user display name

Show authentication time

Add user directory attribute: mail

Multi User Desktop

Show connected users

Connection times

Cluster

Show cluster name

Show members

OK Cancel

3. Check or modify the following areas:
 - **Position (in pixels)**
 - **Font and colors**
 - **Information**
 - **Cluster**
4. Apply the modifications to the security profile.

Managing a Cluster from your Workstation

Subject

The Cluster mode enables you to access several workstations simultaneously. When you:

- Authenticate yourself on a workstation, sessions on other workstations you are using are also unlocked.
- Lock or switch off a workstation, all other workstations you are using are also locked or switched off.
- Reboot, you can reboot one or several workstations of your choice or the whole cluster at once.
- Attach or release a workstation, you can add a workstation from an existing cluster or an entire cluster to your own cluster and then release it.

To manage your cluster, use the **Cluster Wizard** in the **Authentication Manager** dialog box.

You can customize the way the workstations of a cluster are displayed on your screen: see *One Identity EAM Customization Guide*.

Before starting

- All the actions you can perform from your workstations are only available if they have previously been authorized by the EAM Console administrator: see *Authentication Manager Cluster Administrator's Guide*.
- The **Cluster Client** license keys must be installed on all EAM workstations on which the Cluster feature is used.

Creating and Configuring your Cluster

Managing the Cluster Composition

If you are authorized to access workstations of a cluster, you can attach one or more workstations from an existing cluster to your cluster. The workstation(s) is(are) detached when you release it(them) from your cluster or if another user authenticates on the original cluster.

Attaching a Workstation to Your Cluster

Subject

Attaching a workstation to your cluster is not a permanent action, you can release a workstation whenever you want. You can attach only the workstations authorized by the administrator.

Before starting

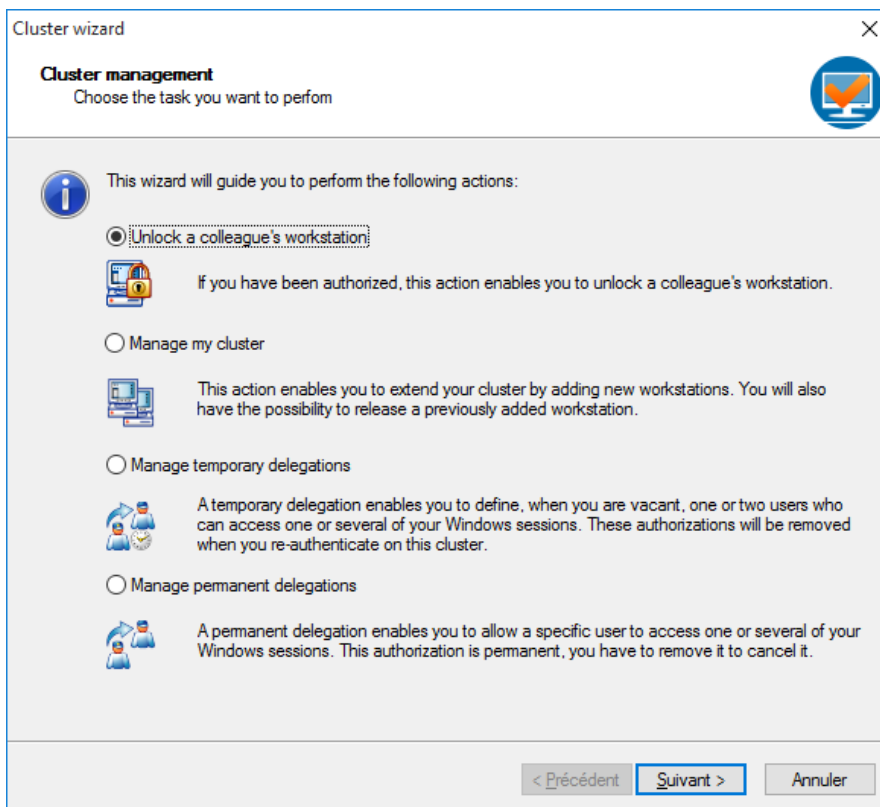
The Windows session of the workstation you want to attach to your cluster must be closed.

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Manage Cluster**.
2. Re-authenticate if needed.

The **Cluster wizard** window appears.

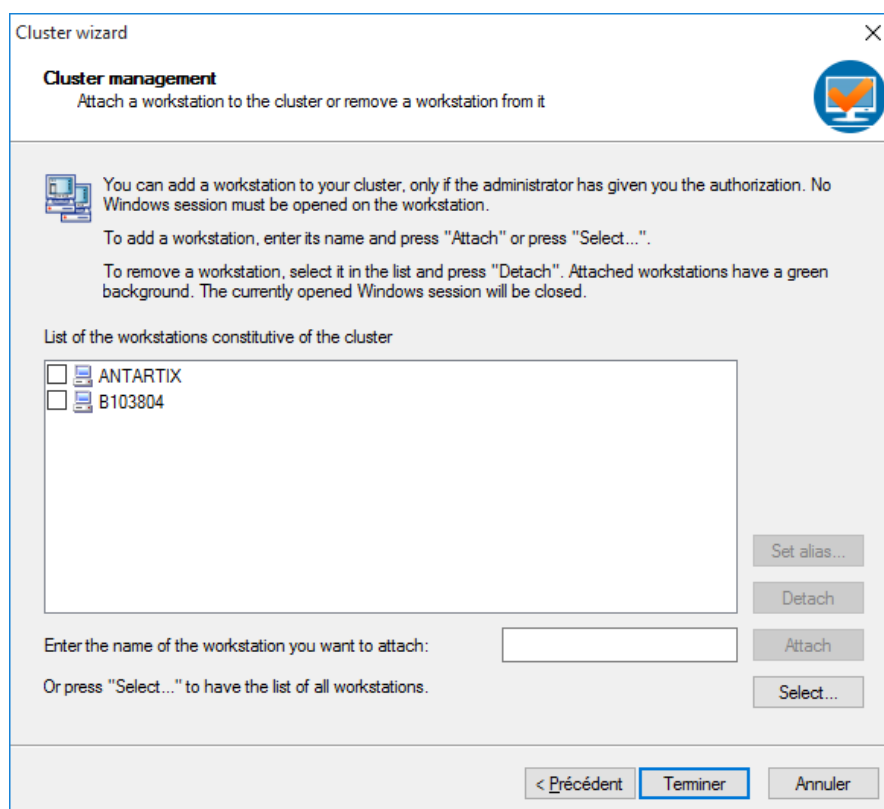
Figure 10: Cluster wizard



3. Select **Manage my cluster** and click **Next**.

The following window appears:

Figure 11: Cluster Management



4. Do one of the following actions to add a workstation to your cluster:
 - Type in the name of the workstation you want to attach in the corresponding field and click the **Attach** button.
 - Click the **Select** button and select a workstation in the list displayed by the wizard.
- !** **IMPORTANT:** Only the workstations authorized by the administrator are displayed.
5. Click **Finish**.

The workstation is now attached to your cluster and its session opens automatically.

Releasing a Workstation from your Cluster

Before starting

You can release a workstation/cluster only if you have added it to your cluster beforehand. The released workstation is automatically reattached to its original cluster.

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Manage Cluster**.
2. Re-authenticate if needed.
The **Cluster wizard** window appears.
3. Select **Manage my cluster** and click **Next**.
4. The **Attach/Detach workstation** window appears.
5. Select the workstation you want to detach from your cluster and click the **Detach** button.
6. Click **Finish**.
The workstation is now released from your cluster and its session closes automatically.

Renaming your Workstation

Subject

You can rename your workstation, i.e. give it an **alias** that is displayed:

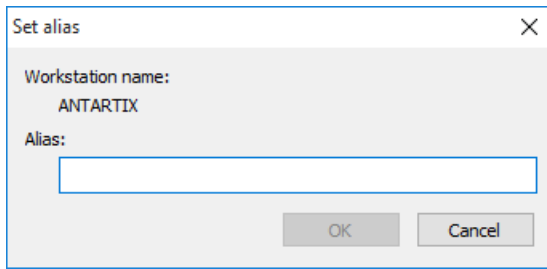
- In the cluster management windows.
- On the desktop (if configured).

Setting an Alias

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Manage Cluster**.
2. Re-authenticate if needed.
The **Cluster wizard** window appears.
3. Select **Manage my cluster** and click **Next**.
The **Attach/Detach workstation** window appears.
4. Select one or more of the displayed workstations and click the **Set alias** button.
The **Set alias** dialog box appears.

Figure 12: Set Alias



5. In the **Alias** field, enter the alias you want to give to your workstation and click the **OK** button.

Since the alias must be unique, a check is made to see if it does not already exist.

The alias of your workstation has been set.

Modifying an Alias

Procedure

Repeat the procedure of [Setting an Alias](#) and at step **5**, modify the alias that is set.

Deleting an Alias

Procedure

Repeat the procedure of [Setting an Alias](#) and at step **5**, delete the text in the **Alias** field.

Executing Maintenance Operations on Your cluster

Removing Temporarily a Workstation from the Cluster

Subject

From your workstation, you can temporarily remove another workstation from the cluster. This can be useful for maintenance operations: the workstation can be rebooted independently from the others.

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Deactivate cluster mode**.
The workstation is excluded from the cluster. It remains excluded even when you restart it.
2. To include the computer back into the cluster, click **Activate cluster mode**.

Rebooting your Cluster

Subject

This action enables you to restart all the workstations in the cluster at once.

Before starting

There are two station behaviors:

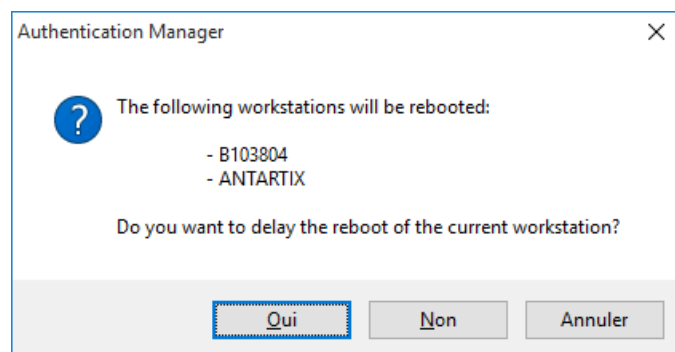
- The **master** station can accept, decline or delay its reboot.
- The **slave** station can only accept or decline its reboot.

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Reboot Cluster**.

The following dialog box appears:

Figure 13: Authentication Manager



IMPORTANT: If the station is a **slave** station, you can only accept or decline the reboot.

2. Do one of the following:
 - Click **Yes** to reboot the cluster **except** your current workstation.
The cluster is rebooted and locked: go to step **3**.
 - Click **No** to reboot the cluster **including** your current workstation.
The cluster is rebooted.
3. Do one of the following:
 - Click **Yes** to reboot your current workstation.
Your current station is rebooted and the other workstations of the cluster stay locked.
 - Click **No** to unlock the cluster without rebooting your current workstation.

Refreshing the Displayed Data

Subject

If you change your desktop wallpaper, the cluster data disappears from the desktop. To re-display this data, execute the following procedure.

Procedure

Right-click the **Authentication Manager** icon in the notification area and select **Redraw wallpaper**.

The cluster data is re-displayed on the desktop.

Managing Session Delegation

Configuring Session Delegation

If for any reason you have to leave your workstation or cluster, you can delegate your Windows session to your **delegate** to monitor or intervene in any of your ongoing operations.

You can configure session delegation either:

- Inside a cluster: see [Configuring Session Delegation in a Cluster](#).
- Outside a cluster: see [Configuring Session Delegation outside a Cluster](#).

Configuring Session Delegation in a Cluster

In cluster mode, you can delegate your workstation to your **Primary delegate** or your **Backup**:

- The **Primary delegate** is the main person to whom you are delegating your session.
- If the Primary delegate is not available, the **Backup** is the one monitoring your workstation.

For more information on cluster configuration, go to [Managing a Cluster from your Workstation](#).

There are two types of session delegation:

- **Temporary**: the session is delegated only once, until the next time you re-authenticate yourself. For more details, refer to:
 - [Setting a Temporary Session Delegation](#).
 - [Ending a Temporary Session Delegation](#).
- **Permanent**: the session is delegated permanently, until you stop delegating the workstation. For more details, refer to:

- [Setting a Permanent Session Delegation.](#)
- [Ending a Permanent Session Delegation.](#)

Setting a Temporary Session Delegation

Subject

- If the administrator has activated the approval function, your Primary delegate or your Backup must be at his workstation to accept the session delegation, i.e. with an unlocked workstation.
- Once you have delegated your session, if your Primary delegate leaves and locks his workstation, your delegated workstations are not part of his cluster anymore. If he/she wants to include them back into his/her cluster he/she must follow the procedure described in [Accessing a Colleague's Workstation in a Cluster.](#)

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Set temporary session delegation.**
2. Re-authenticate if needed.
The **Cluster wizard** window appears.

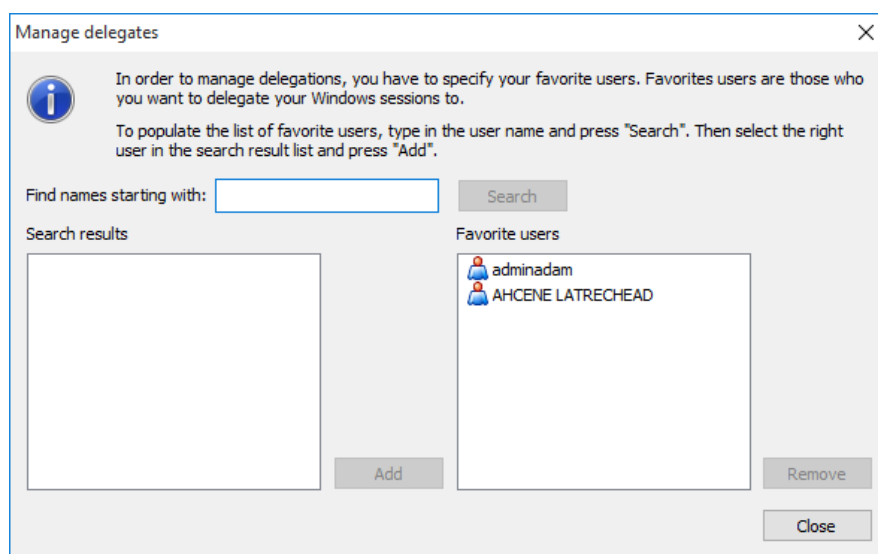
Figure 14: Cluster wizard

The screenshot shows a window titled "Cluster wizard" with a close button (X) in the top right corner. Below the title bar, the text reads "Set/Remove a temporary delegation" followed by "Select your delegate and if necessary your backup and press 'Delegate' to set up a temporary delegation". To the right of this text is a blue circular icon with a white checkmark. Below this is a section with a small icon of two people and the text "A temporary delegation enables you to define one or two users that can unlock one or several of your Windows sessions." The main area contains two dropdown menus: "Primary delegate:" and "Backup". Both dropdown menus currently show "AHCENE LATRECHHEAD". To the right of the "Primary delegate:" dropdown is a "Manage delegates..." button. Below the "Backup" dropdown is a "Delegate" button. To the left of the "Primary delegate:" dropdown is a checkbox labeled "Backup" which is currently unchecked. Below the "Primary delegate:" dropdown is an "Advanced Delegation" button. At the bottom of the window are three buttons: "< Précédent", "Terminer", and "Annuler".

3. Click the **Manage delegates** button to select your **Favorite users** and fill-in the **Primary delegate** and **Backup** drop-down lists. If you have already done so, go directly to step **7**.

The **Manage delegates** window appears.

Figure 15: Manage Delegates



4. Select your favorite users by typing their name in the **Find names starting with** field and click the **Search** button.

A list of the names appears in the **Search Results** area.

5. Select your favorite users and click the **Add** button to add the names to your favorite users list.
6. Click **Close**.
7. In the **Primary delegate** drop-down list, select your Primary delegate.
8. If you want a Backup, select the **Backup** check box and select him/her in the drop-down list.
9. Click the **Advanced Delegation** button to delegate more than one workstation from your cluster.
10. Click the **Delegate** button.

Your temporary session delegation is now set and the selected workstation(s) from your cluster is(are) delegated, pending approval from the Primary delegate/Backup.

NOTE:

- If you retrieve your smart card, your cluster locks itself except your delegated workstations.
- For more information on accessing a delegated session, go to [Accessing a Colleague's Workstation](#).

Ending a Temporary Session Delegation

Subject

There are different ways to end a temporary session delegation. If the master workstation is delegated, you have to end the delegation and lock the workstation by inserting your smart card and re-authenticate yourself.

Procedure

Do one of the following:

- Reauthenticate yourself.
- Use Authentication Manager:
 - a. Right-click the **Authentication Manager** icon in the notification area and select **Set temporary session delegation**.
 - b. Reauthenticate if needed.

The **Cluster wizard** window appears.
 - c. Click the **Remove delegation** button.

The session delegation has ended.
- Ask the Primary delegate or Backup to end the delegation (see [Ending the control over a Workstation](#)).

Table 1: Ending a Temporary Session Delegation

| If... | Then... |
|---|--|
| the Primary delegate or Backup ends the delegation... | the delegated workstation(s) is/are locked. |
| you lock a cluster containing a delegated workstation... | the workstation locks itself. |
| you shut down a cluster containing a delegated workstation... | the workstation is released from the cluster and locks itself. |

Setting a Permanent Session Delegation

Subject

You can delegate as many workstations to as many delegates as you want.

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Manage Cluster**.

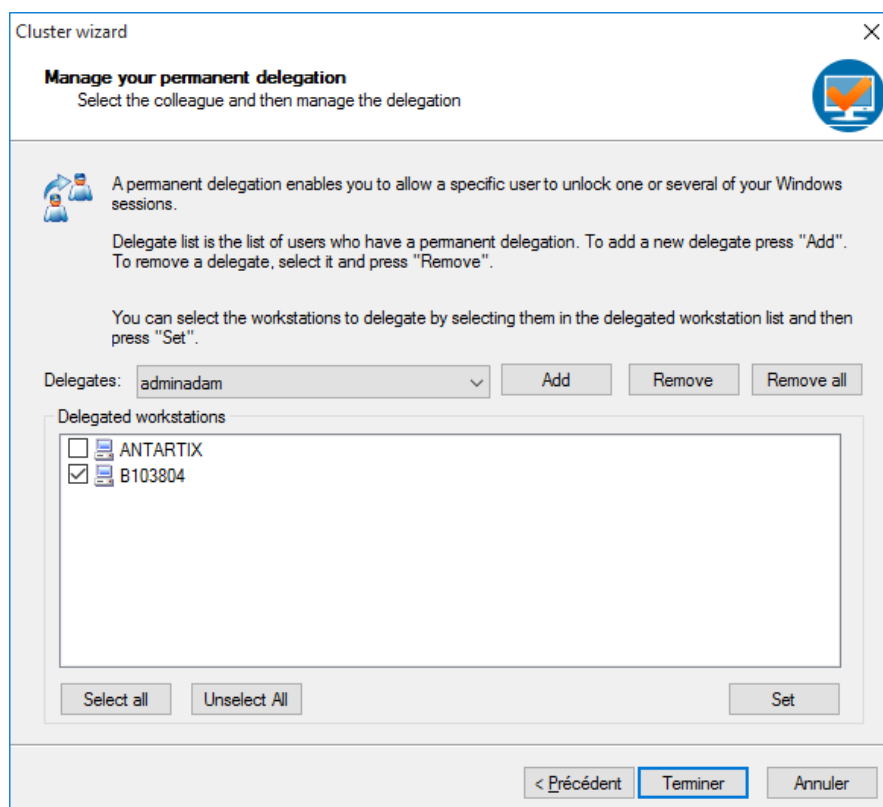
2. Reauthenticate if needed.

The **Cluster wizard** window appears.

3. Select **Manage permanent delegations** and click **Next**.

The following window appears:

Figure 16: Manage permanent delegations



4. Select a delegate in the drop-down list or click the **Add** button to add users to your delegates list.

5. Do one of the following:
 - In the Delegated workstations area, select the workstations you want to delegate to the selected delegate.
 - Click the **Select all** button to select all the workstations at once.
6. Click the **Set** button.

The next time you lock your workstation(s), your selected delegate will be able to take control over your selected workstation(s).

NOTE: For more information on accessing a delegated session, go to [Accessing a Colleague's Workstation](#).

Ending a Permanent Session Delegation

Subject

There are different ways to end a permanent session delegation. If the master workstation is delegated, you have to end the delegation and lock the workstation by inserting your smart card and re-authenticate yourself.

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Manage Cluster**.
2. Reauthenticate if needed.

The **Cluster wizard** window appears.
3. Select **Manage permanent delegations** and click **Next**.

The **Manage your permanent delegation** window appears.
4. Clear the check box(es) corresponding to the workstation(s) for which you want to end the delegation.
5. Select the delegate for whom you want to end the delegation and click the **Remove** button.

NOTE: Click the **Remove all** button to remove all the delegations at once.
6. Click the **Set** button.

The session delegation has ended.

Table 2: Ending a permanent session delegation

| If... | Then... |
|---|--|
| the Primary delegate or Backup ends the delegation... | the delegated workstation(s) is/are locked. |
| you shut down a cluster containing a delegated workstation... | the workstation is released from the cluster and locks itself. |

Configuring Session Delegation outside a Cluster

There is only one type of session delegation outside a cluster: **permanent** delegation. For more information, refer to the following sections:

- [Setting a Session Delegation.](#)
- [Ending a Session Delegation.](#)

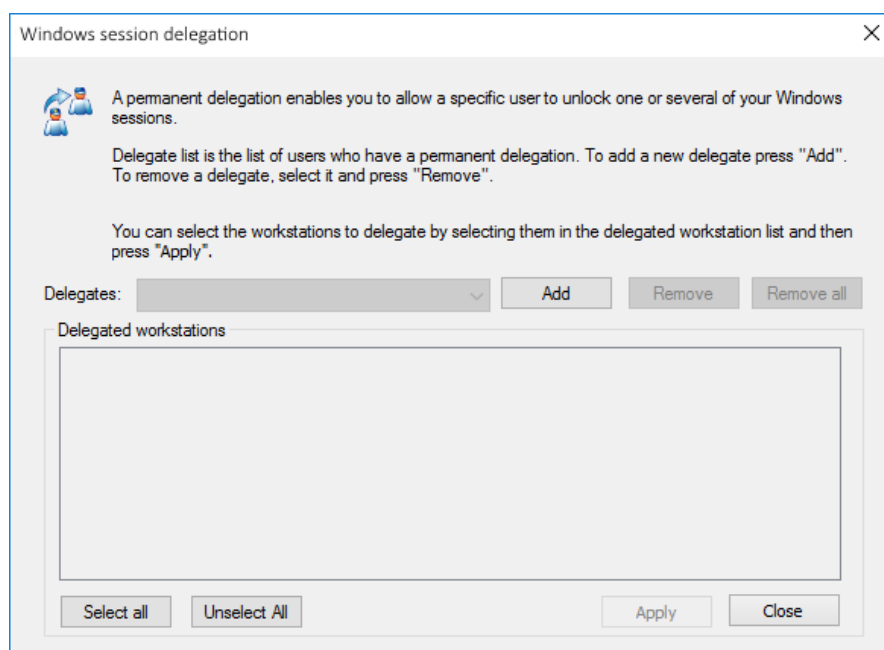
Setting a Session Delegation

You can delegate several workstations to one of your delegates.

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Manage Session Delegation**.
2. Reauthenticate yourself.
The **Windows session delegation** window appears.

Figure 17: Windows session delegation



3. Select a delegate in the drop-down list or click the **Add** button to add users to your delegates list.
4. Do one of the following:
 - In the **Delegated workstations** area, select the workstations you want to delegate to the selected delegate.
 - Click the **Select all** button to select all the workstations at once.
5. Click **Apply**.

The next time you lock your workstation(s), your selected delegate will be able to take control over your selected workstation(s).

Ending a Session Delegation

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Manage Session Delegation**.
2. Reauthenticate yourself.

The **Windows session delegation** window appears.

3. Clear the check box(es) corresponding to the workstation(s) for which you want to end the delegation.
4. Select the delegate for whom you want to end the delegation and click the **Remove** button.

NOTE: Click the **Remove all** button to remove all the delegations at once.

5. Click **Apply**.

The session delegation has ended.

NOTE: If the delegate ends the delegation, the delegated workstation(s) is(are) locked.

Accessing a Colleague's Workstation

Subject

If you are a delegate (temporary or permanent), you can take control over one of your colleague's locked workstation(s) to monitor or intervene in any of his ongoing operations.

The Windows context is the one of the user who has opened the session and the SSO engine (if any) is suspended.

You can access a colleague's workstation whether you are:

- Inside a cluster: [Accessing a Colleague's Workstation in a Cluster](#).
- Outside a cluster: [Accessing a Colleague's Workstation outside a Cluster](#).

Accessing a Colleague's Workstation in a Cluster

The delegated workstations are not attached to the delegate cluster and the operations performed on these workstations are not propagated to the cluster.

NOTE: By double-clicking the Authentication Manager icon, you directly access the **Access a colleague's workstation** feature.

Taking control over another workstation

Before starting

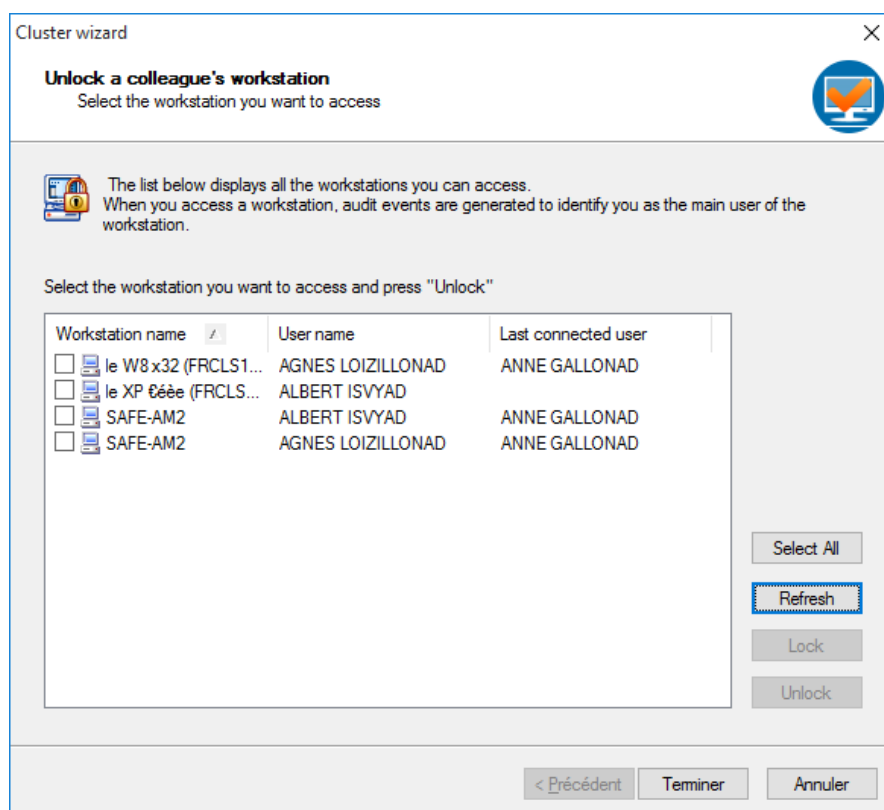
- Your colleague must have designated you as his Primary delegate or his backup.
- Your colleague's workstation(s) must be locked.

Procedure

1. Double-click the **Authentication Manager** icon in the notification area.
2. Reauthenticate if needed.

The following window appears with the list of workstations you are authorized to take control over.

- NOTE:** If you are allowed a permanent session delegation, all the workstations are displayed whether they are delegated temporarily or permanently.



3. Select the workstation(s) you want to take control over and click the **Unlock** button.

- NOTE:** Click the **Select all** button to select all the displayed workstations.

You now have the control over the selected workstation(s).

Ending the control over a Workstation

Subject

There are two ways to end the control over a delegated workstation.

- If you do not lock the workstation, it will be locked when you lock your cluster.
- To take back the control over your delegated workstation, the latter must be locked.

When the delegate unlocks his cluster, the previously controlled workstation does not unlock itself. To take the control back, he must follow the same procedure as described in [Accessing a Colleague's Workstation in a Cluster](#).

Procedure

Do one of the following operations:

- On the delegated workstation, press **Windows+L** to lock it.
- The delegate ends the control by following this procedure:
 - a. Double-click the **Authentication Manager** icon in the notification area.
 - b. Reauthenticate if needed.
The **Access a colleague's workstation** window appears.
 - c. Select the workstation(s) you want to end control over and click the **Lock** button.

The workstation is not under your control anymore.

Accessing a Colleague's Workstation outside a Cluster

Taking control over another workstation

Before starting

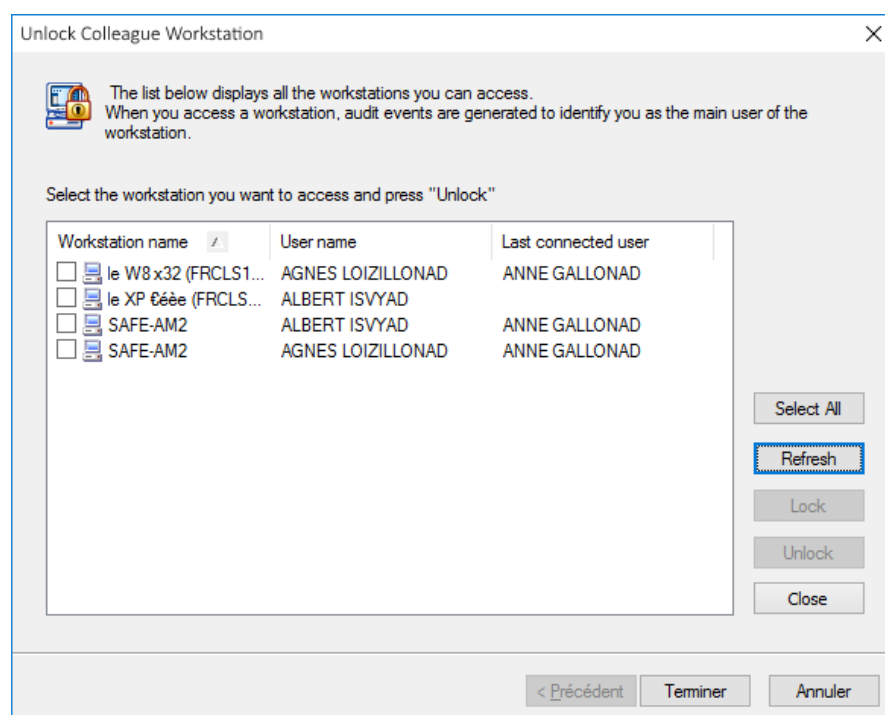
- Your colleague must have designated you as his delegate.
- Your colleague's workstation(s) must be locked.
- On Windows 7 workstations, set the following key to support unlock request: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DisableCAD**

Procedure

1. Right-click the **Authentication Manager** icon in the notification area and select **Access a Colleague's Workstation**.
2. Reauthenticate yourself.

The following window appears with the list of workstations you are authorized to take control over.

Figure 18: Accessing Workstation outside cluster



3. Select the workstation(s) you want to take control over and click the **Unlock** button.

NOTE: Click the **Select all** button to select all the displayed workstations.

You now have the control over the selected workstation(s).

Ending the control over a Workstation

Subject

To take back the control over your delegated workstation, the latter must be locked.

Procedure

Do one of the following operations:

- On the delegated workstation, press **Windows+L** to lock it.
- The delegate ends the control by following this procedure:
 - a. Right-click the **Authentication Manager** icon in the notification area and select **Access a Colleague's Workstation**.
 - b. Reauthenticate yourself.
The **Unlock Colleague Workstation** window appears.
 - c. Select the workstation(s) you want to end control over and click the **Lock** button.
The workstation is not under your control anymore.