confidential RESTRICTED

amadeus

Amadeus Security Management (ASM)

User Guide

Edition 18.3 For Amadeus Security Management (ASM) 18.3
Job Number 4412 FE 0714

Published by :

Amadeus Learning Services
email: learning@amadeus.com

July 2018

Table of Contents

Chapter 13

Chapter 14

Chapter 15

Before You Start

Purpose of This Document

This guide describes how to use Amadeus Security Management (ASM).

Audience

This guide is intended for administrators who are responsible for managing security and access to Amadeus applications within their organization.

Related Reference Material

For more information on Amadeus Security Management (ASM), refer to the e-Learning videos available on Amadeus Service Hub (e-Support Centre):

- Amadeus Security Management (ASM) - eLearning Videos.

Feedback on This Document

Your feedback is important and will help us to improve this document.

Please email your comments to Amadeus Learning Services at learning@amadeus.com.

What's New in This Document

For further information about product changes in each release, refer to the Product Release notes.

This edition includes the following changes:

Change	Topic
New features	• It is now possible to automatically delete login areas that have been inactive for a specified period. See *Explanation: PCI-compliant Lock-out Management Settings* on page 27. • There is now an check box option allowing users to be informed by email before their account is locked or deleted. See *Explanation: PCI-compliant Lock-out Management Settings* on page 27. • It is now possible to display the list of cryptic entries allowed to each user. See *How to List the Cryptic Entries Allowed to a User* on page 64. • In the **List of ACLs** panel, you can now click on the column headings to sort ACLs. See *How to Display the ACLs Assigned to a Consumer* on page 98. • Users PCs can now be secured using Digital DNA (DDNA) based on user hardware components. See *Defining Your Security Policy* on page 25. • Two-factor authentication (TFA) has been replaced by Multi-factor authentication (MFA). See *Defining Your Security Policy* on page 25. • You can now create metagroups for applying permission across organizations. See *Working With Metagroups* on page 48. • You can now create Security Badges for users containing Roles and ACLs. See *Working With Security Badges* on page 105.
Updated features	• An additional option **SMS and Mail** has been added to the choices for receiving a one-time password. See *Applying Application Security* on page 30. • You can now search across organization description when adding an organization. See *How to Add an Organisation to Your List* on page 15. • When Multi-Factor Authentication is activated, it is now possible to choose what happens when the maximum number of locations is reached and a user tries to register a new location. See *Applying Application Security* on page 30. • When creating or updating a user profile, the phone number must now be entered in international standard format. See *How to Create a User* on page 56. • It is now possible to add permissions with the same label in one role, if they are from different applications or sub-applications. See *How to Create a Unitary Role* on page 86.

Latest Version of This Document

For Travel Agencies:

1. Click here to view the User Guide in Amadeus Service Hub.
   - If you are asked to log in, select **Travel Agency**, then either:

- Enter the **Office ID**, **Agent sign** (or **User ID**), and **Password** that you use to access Amadeus applications, then click on **Sign in**.

  Or:

- If you are a first-time user, click on **Register**.

Note: For more information on how to register, click on the **How to register** link.

- Click on to view the guide in full screen.
- Click on to download the .DOC (Word) version.
- Click on or Subscribe to bookmark the page and receive notification emails when the page is updated. (To set notification preferences, click on your name at the top of the screen then **My Account** > **Notification Preferences** tab.).

For Airlines:

For the latest version of this document, and other reference material:

2. Click here to view the User Guide in Amadeus Service Hub.

   - If you are asked to log in, select **Airline**, then either:

- Enter your Service Hub (Airline Extranet) user name and password, then click on **Sign in**.

  Or:

- If you are a first-time user, click on **Register** to get access to Service Hub.

  - Click on to view the guide in full screen.
  - Click on to download the .DOC (Word) version.
  - Click on or Subscribe to bookmark the page and receive notification emails when the page is updated. (To set notification preferences, click on your name at the top of the screen then **My Account** > **Notification Preferences** tab.)

For Ground Handlers:

For the latest version of this document, and other reference material:

- Click here to view the User Guide in Amadeus Service Hub.
- If you are asked to log in elect **Ground Handler & Airport**, then :

a) Enter either the **User ID**, **Organization ID**, and **Password** that you use to access Amadeus Altéa Flight Management and Customer Management applications, or enter the **Office ID**, **Agent sign**, and **Password** that you use to access Amadeus reservations applications.

b) Click on **Sign in**.

- If you are a first-time user, enter all missing mandatory information in the fields of the ASH self-registration pop-up window, and click on **Register**.

Note: For more information on the self-registration process, click on the **How to login** link.

- Click on to view the guide in full screen.
- Click on to download the .DOC (Word) version.
- Click on or Subscribe to bookmark the page and receive notification emails when the page is updated. (To set notification preferences, click on your name at the top of the screen then **My Account** > **Notification Preferences** tab.)

Product Release

This document explains how to use the features available in ASM Version 18.1.

Chapter 1

Overview of the Amadeus Security Model

What Is the Amadeus Security Model?

The Amadeus security model provides a common solution for security administration across Amadeus products.

The security model consists of two separate processes:

- **User Authentication**

  This is the process by which a user is identified and acknowledged as having the right to access the system. This process is run the first time the user tries to connect to an application.

- **Access control**

  This checks that a user has the right to use a specific function, and to manipulate specific data, within an application. This check is run every time a user tries to perform some task in an application.

You use the Amadeus Security Management (ASM) application to administrate these two processes.

Understanding Access Control

What Are Permissions and Data Types?

For each Amadeus application, the application team defines generic objects that are used to grant the rights to use certain functions of the application and manipulate data related to the application. These objects are:

- **Permissions**

  A permission grants the right to carry out one particular function in the application. Permissions are not assigned individually to a user, office or organization, but are grouped together into roles. A permission is linked to a particular data type.

- **Data types**

  A data type is a definition of a particular type of data operated on by the functions of an application. In ASM, you create **data values**, which are instances of these data types with specific values. By linking permissions to data values you restrict the user's ability to use an application function to manipulate information to only those values.

For each application, Amadeus teams also create preference types that are used to set a number of non-security parameters linked to the general behaviour of the application.

What Are Roles and ACLs?

- **Roles**

  In order to grant multiple permissions in one step, permissions are aggregated into **roles**. Roles are analogous to job functions, and allow you to grant users access to the complete set of functions that they need to perform their job tasks. Roles can also contain other roles.

  To help you create your own roles, Amadeus application teams create generic roles for each application. These are preset, typical roles containing all the permissions needed to use a function of the application. Generic roles can be used by any organization.

- **Access Control Lists**

  In addition to the right to use an application function granted by a permission contained in a role, the user must also have the right to manipulate the data used by that function. This is enabled through **Access Control Lists** (ACLs). ACLs define the data values a role can operate on.

What Are the System Components of the Amadeus Security Model?

The Amadeus security model is managed through interaction between the following systems:

- **Logon and Security Server (LSS)**

  LSS is the master database where most security and access control data is defined. Security administrators define and maintain this data in ASM in order to authenticate users and control access to each application. LSS performs the user authentication and provides a library for applications to check the user rights.

- **The Services Integrator (SI)**

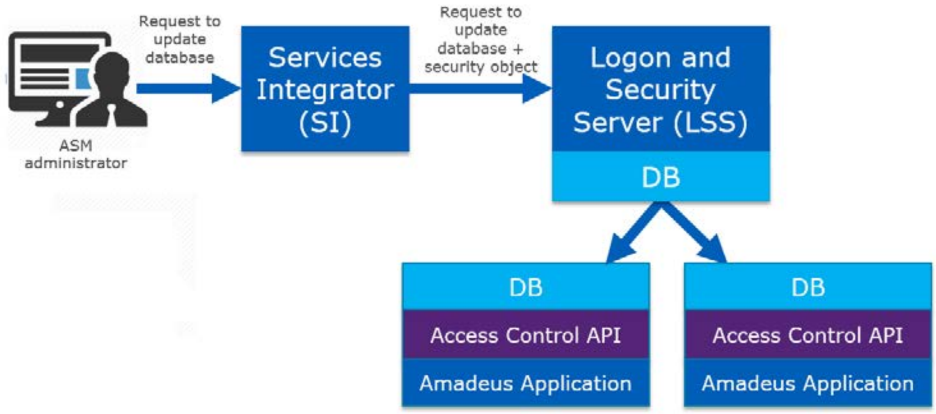
  The SI is a gateway that acts as the single entry point to Amadeus applications. It coordinates communication between users, LSS and Amadeus applications. It stores user-related security objects for complete work sessions.

- **Amadeus Applications**

  Each application uses the authentication information sent by the system to identify the owner of a task request, along with that person's location. The application then checks in its own database to verify whether the user has the right to perform the requested task and manipulate the requested data.

The security administrator uses Amadeus Security Management (ASM), which is the LSS administration user interface, to create and maintain the security data for an application. ASM is available from Amadeus Retailing Platform (ARP). For other Amadeus products, access to ASM functions is controlled by settings within LSS.

Every hour, LSS replicates the security information to other applications so that it can be used in real time to verify user rights using the LSS library.



What Are the Security Modes?

Hosted Mode

The hosted mode is the default mode. When an organization is set up in hosted mode, LSS fully manages both user authentication and access control (authorisation). The security data is stored in LSS. The user is authenticated by LSS and identified by entering unique authentication credentials, such as:

- User ID, Log-in or Sign.
- Organization.
- Office ID.
- Password.

Trusted Mode

When an organization is set up in trusted mode, the organization's own system is used for user authentication, and LSS is used for access control. As a result:

- The security policy and the full user profiles are not available in LSS.
- The roles, ACLs and partnerships are created and assigned in LSS, as in hosted mode.

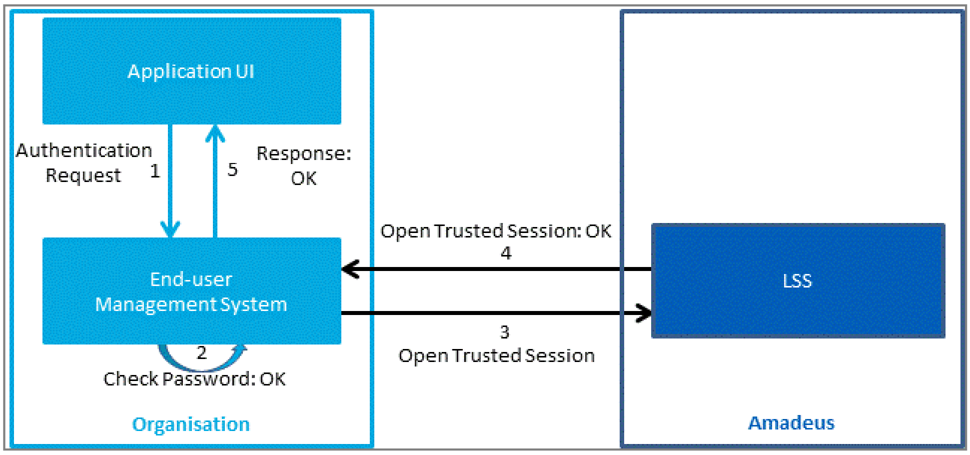
With trusted mode, the organization follows one of the two authentication flows: either the trusted authentication or the delegated authentication. This flow depends on the location of the application user interface.

Trusted Authentication

The application user interface is on the organization's side. The organization uses their own end-user management system to authenticate users. After having checked the password, the organization requests LSS to open a trusted session on a secured link.

The change password requests are also handled by the organization's end-user management system, not by LSS.

Image: Trusted Authentication

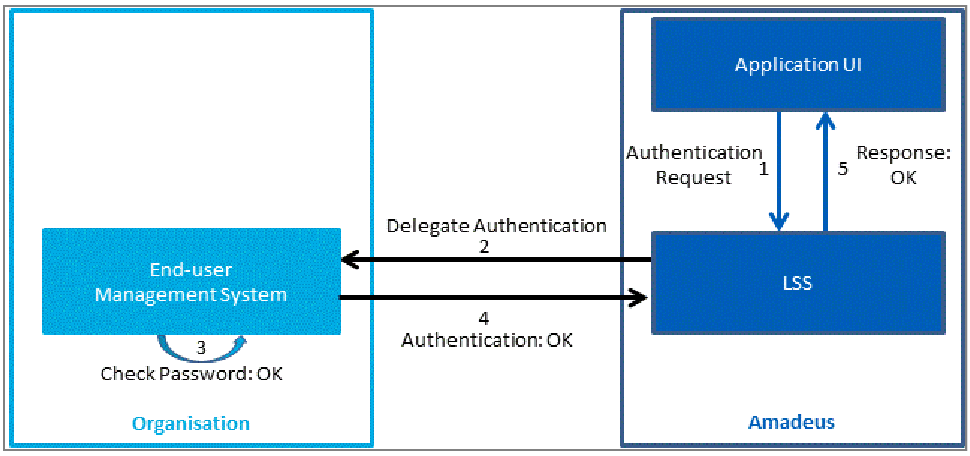


Delegated Authentication

The application user interface is on Amadeus' side. The authentication request initially reaches LSS, which delegates the authentication to the organization's end-user management system.

LSS also delegates the password change requests to the organization's end-user management system.

Image: Delegated Authentication

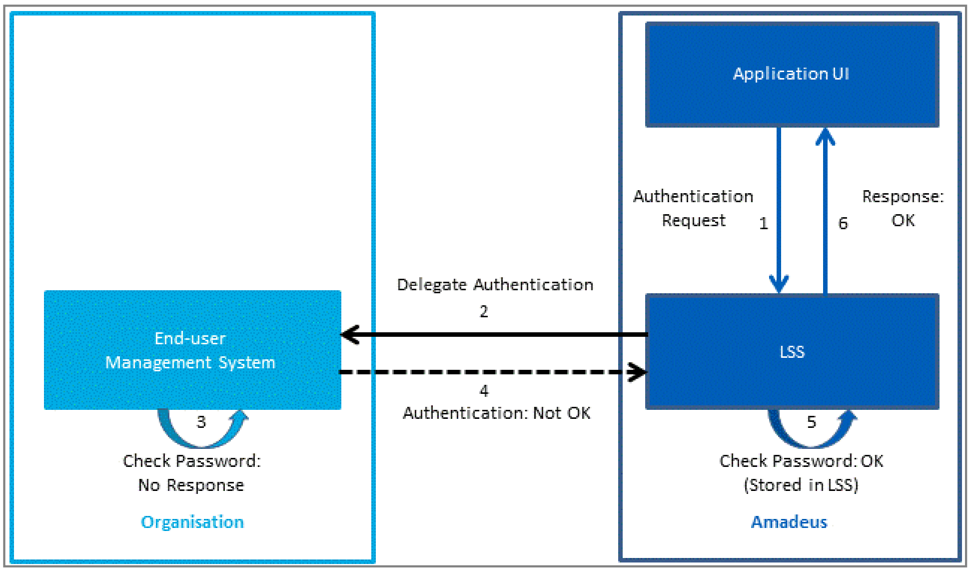


Resilience for Delegated Authentication

The resilience feature can be activated only for the trusted mode using delegated authentication. It is used if the organization's end-user management system does not respond when LSS delegates authentication. LSS performs the password check using the password it has stored the last time the user was successfully authenticated. If the user has never been successfully authenticated, resilience is not possible.

Note: The resilience feature cannot be used for a password change request. If the organization's end-user management system does not respond, both the authentication and password change requests fail. The user must sign in again with their current password, without attempting to change it.

Image: Resilience of Authentication



Understanding Security Administrators' Responsibilities

Implementing the Amadeus security model requires administrators to complete certain tasks both in Amadeus and on the organization's side.

What Are the Amadeus Security Administrator's Tasks?

The Amadeus administrator is responsible for the following tasks in Amadeus Security Management (ASM):

- Defining the root for the organization's tree in the Organization domain.
- Allocating appropriate rights to the organization's security administrators to work in ASM.
- Creating the following data for your organization:
  - The applications and sub-applications.
  - The permissions and the data types for each application.
  - The generic roles and the preferences for each application.

What Are the Organisation Security Administrator's Tasks?

The organization's security administrator is responsible for the following tasks in Amadeus Security Management (ASM).

Table: Implementing the Amadeus Security Model

Step	Task	See...
1	Set up the organization: • Create the organization tree (ORG tree). • Assign office IDs to the appropriate unit in the ORG tree. • Set up the security policy of the organization (not in Trusted mode).	*Managing Your Organisation* on page 23.
2	Create users for the organization.	*Managing Users* on page 55. *Defining Sign Profiles* on page 67.
3	Define the data that users of the various roles can access.	*Managing Data* on page 76.
4	Define roles that correspond to job functions in the organization, or use generic roles for the application if appropriate.	*Defining Roles* on page 81.
5	Create Access Control Lists (ACLs) for each role, to define which data can be accessed by the user who has been assigned a role.	*Defining Access Control Lists* on page 91.
6	Assign roles and ACLs to each user, either directly or at a higher level in the ORG tree, so that a user benefits from both a role and an ACL.	*Assigning Roles and Access Control Lists* on page 95.
7	Optionally, allocate preferences, which customise how a feature is used in an application.	*Assigning Preferences* on page 102.
8	Create and maintain partnerships: If two organizations have an agreement to work together and delegate certain tasks from one organization or organization unit to another.	*Working With Partnerships* on page 111.

Step	Task	See...
9	Generate user, sign bank, administration history details, office, ACL, role, and preference reports for administration purposes.	*Working With Reports* on page 133.

To retrieve the list of administrators in your organization or organization unit, see *How to Display the List of Administrators of an Organisation* on page 40 and *How to Display the List of Administrators of an Organisation Unit* on page 42.

Chapter 2

Navigating Amadeus Security Management

The Amadeus Security Management (ASM) screens are composed of:

- Main part of the screen: Contains the major ASM functions.

  See *Overview of the Home Tab* on page 14.

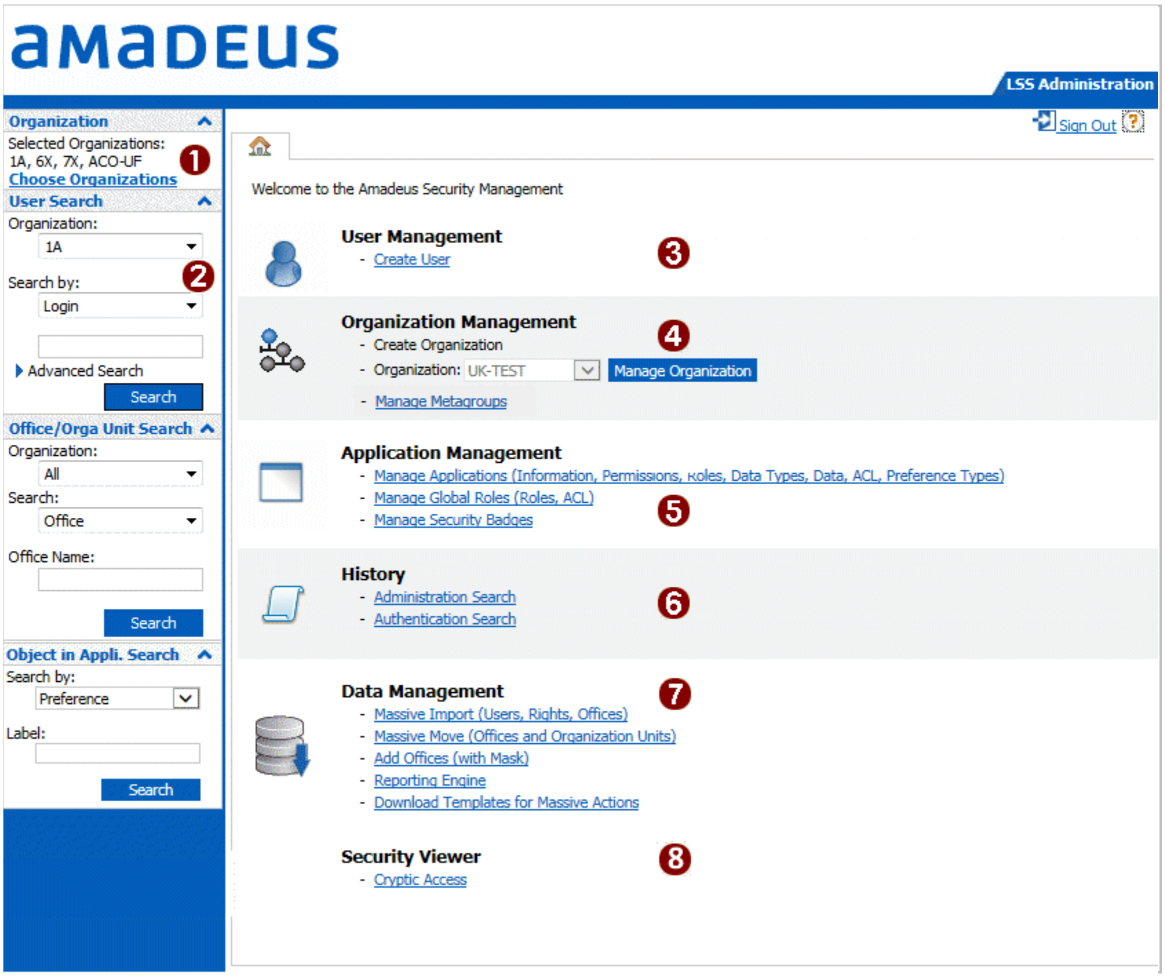
- Left menu bar: Contains search tools that enable you to find users and nodes in the organization tree. The left menu bar is always visible.

  See *Searching Across Organisations and Applications* on page 16.

Overview of the Home Tab

The **Home** tab is displayed when you launch the application, and remains open when you are working in the system.

Image: Amadeus Security Management Home Tab



❶ Organization selection. See *Creating Your List of Organisations* on page 15.

❷ User and office or organization unit search boxes. See *How to Search for a User* on page 16 and *How to Search for an Organisation Unit or an Office* on page 16.

❸ **User Management**. See *How to Create a User* on page 56.

❹ **Organization Management** (organization tree). See *How to Display an Organisation* on page 39.

❺ **Application Management** (for example roles, ACLs and preferences). See:

- *Defining Data for an Application* on page 75.
- *Defining Roles* on page 81.
- *Defining Access Control Lists* on page 91.
- *Assigning Roles and Access Control Lists* on page 95.

❻ **History**. See *Displaying the Administration History* on page 18 and *Displaying the Authentication History* on page 19.

❼ **Data Management**. See:

- *Managing Multiple Offices* on page 44.
- *Adding Offices to Your Organisation* on page 46.
- *How to Create or Update Multiple Users (Airlines)* on page 63.
- *How to Create Multiple Data Instances and Datalists (Airlines)* on page 78.
- *How to Create Multiple Roles (Airlines)* on page 87 and *How to Assign Multiple Roles (Airlines)* on page 97.
- *How to Create Multiple ACLs (Airlines)* on page 93 and *How to Assign Multiple ACLs (Airlines)* on page 99.
- *How to Assign Multiple Preferences (Airlines)* on page 103 and *Working With Reports* on page 133.
- *Working With Reports* on page 133.

❽ **Security Viewer** See *How to List the Cryptic Entries Allowed to a User* on page 64.

Note: Depending on your user rights in the system, you may not be able to see all these options, and you may not be authorised to perform certain tasks.

Creating Your List of Organisations

Why Do You Need a List of Organisations?

You need to create your list of organizations before you can manage them. The organizations you have selected appear in all the **Organization** drop-down lists.

Your list can contain up to 15 organizations.

How to Add an Organisation to Your List

3. In the left menu bar, click on **Choose organizations**.

   The list of organizations you have already selected is displayed.

4. Enter the name or organization code that you want to add.

   Note: ASM searches by default within organization code. Optionally select the check box **Search also within organization Description** to extend the search.

5. Click on **Add**.

   The new organization is added to the list.

6. Repeat the previous two steps, to add other organizations.
7. Click on **Save**.

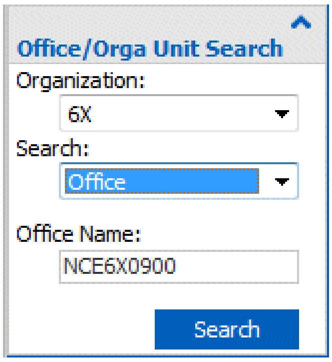
Searching Across Organisations and Applications

How to Search for an Organisation Unit or an Office

Note: The search is limited to one organization at a time.

1. In the left menu bar, expand the **Office/Unit Search** menu.
2. From the **Organization** drop-down list, select the organization to which the organization unit or office belongs.

   Note: If the appropriate organization is not in the list, you must add it. See *Creating Your List of Organisations* on page 15.
3. From the **Search** drop-down list, select **Unit** or **Office**.
4. Enter the **Unit name** or the **Office ID**.
5. Click on **Search**.



6. In the **Search Results** window, click on **View office** or **View organization unit**.

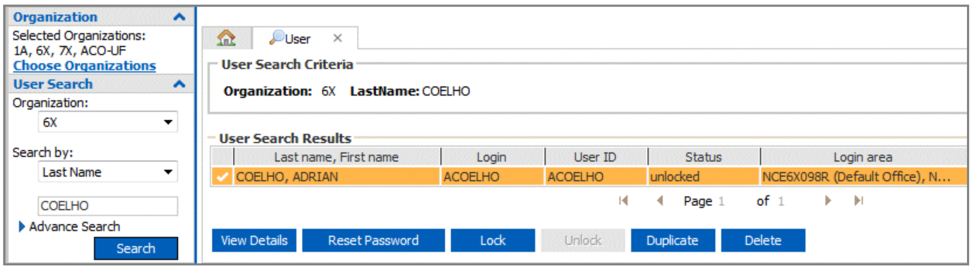
How to Search for a User

1. In the left menu bar, expand the **User Search** menu.
2. From the **Organization** drop-down list, select the organization to which the user belongs.

   Note: If the appropriate organization is not in the list, you must add it. See *Creating Your List of Organisations* on page 15.
3. From the **Search by:** drop-down list, select **Login**, **User ID**, **Sign, Last name**, or **Email**.
4. Enter the required information in the empty field. You can use the asterisk (*****) wildcard as part of your search entry.

   To search by additional criteria, expand the **Advanced Search** icon to display more search options.
5. Click on **Search**.
6. If there are several users in the search results, select the one with which you want to work.
7. Click on **View details**.

Image: Search for a User

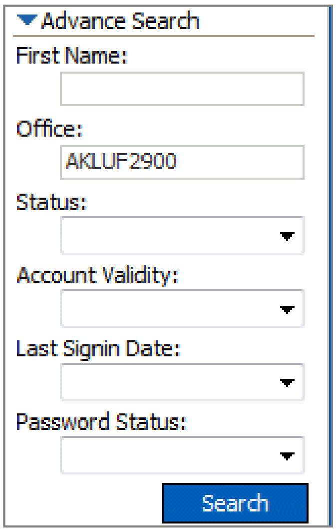


How to Display a List of Users in an Office

1. In the left menu bar, expand the **User Search** menu.
2. From the **Organization** drop-down list, select the organization to which the user belongs.

   Note: If the appropriate organization is not in the list, you must add it. See *Creating Your List of Organisations* on page 15.

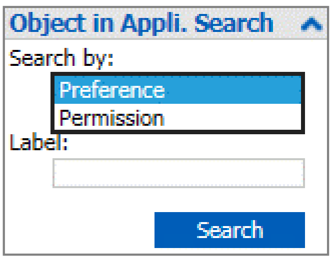
3. Expand the **Advanced Search** icon to display more search options.



4. Enter the office ID in the **Office** field.
5. Click on **Search**.

How to Search for an Application Preference or Permission

1. In the left menu bar, expand the **Search in Applications** menu.
2. From the **Search by** drop-down list, select **Preference** or **Permission**.



3. Enter a **Label**.
4. Click on **Search**.

   The **Search Results** window shows a list of all permissions or preferences matching your search criteria and the corresponding application path and value type.

   - For more information on a permission, select the permission and click on **View Permission Usage**.
   - For more information on a preference, select the preference and click on **View Values and Consumers**.

   Note: The displayed preferences can only be those that the Administrator has the right to see.

Displaying the Administration History

What Is Administration History?

All changes to data stored in the system are logged and can be displayed using the **History** feature. Data is stored in the system for two years.

You can display history for:

- Users: Creation, deletion, update, freezing, unlocking, login areas, security settings and default office.
- Organization tree: Organizations, units or offices and office masks.
- Applications and sub-applications: Roles, permissions, ACLs, preference types, preferences, data types and data sets.
- Role and ACL access-rights allocation.

  Note: On the history display, allocation of a role is called a **Role Context** and allocation of an ACL is called an **ACL Context**.

- Partnerships: Creation, validation, suspension, reactivation and deletion, and delegation of roles and ACLs.

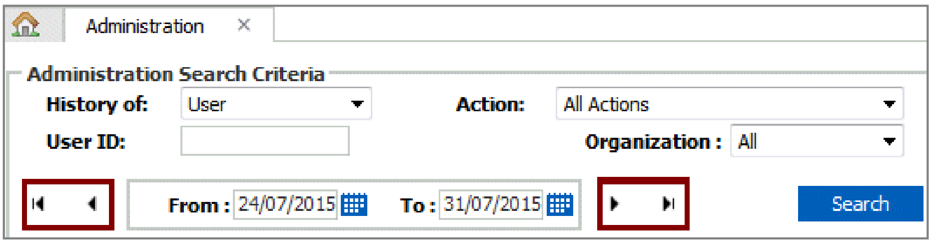
The history records are displayed for each type of object handled by the system. The history display contains information such as the date and time the change was made (**Time Stamp**), the name of the item for which you requested a history display (**History of**), the change that was made (**Action**) and the security object that was changed (**Object**).

How to Display Administration History

1. Click on **Administration search** in the **History** section of the **Home** tab, or on the **View History** link from any of the tabs.
2. In the **Administration Search Criteria** pane, select the item you want to display from the choices in the **History of** drop-down list.
3. Optionally, use the other search criteria fields to further specify what you want to see in the history display.

   For example, enter a user ID when searching for a user, or a role name when searching for role history, an application or a type of action.

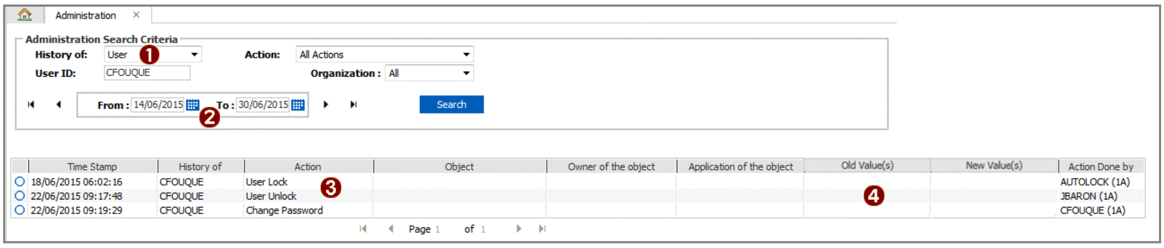
4. Enter a date range in the date fields (up to 30 consecutive days). Use the arrows to shift the date range by one day or one week either side of the selected dates.



5. Click on **Search**.

Example: Administration History Display

Image: History of User Changes



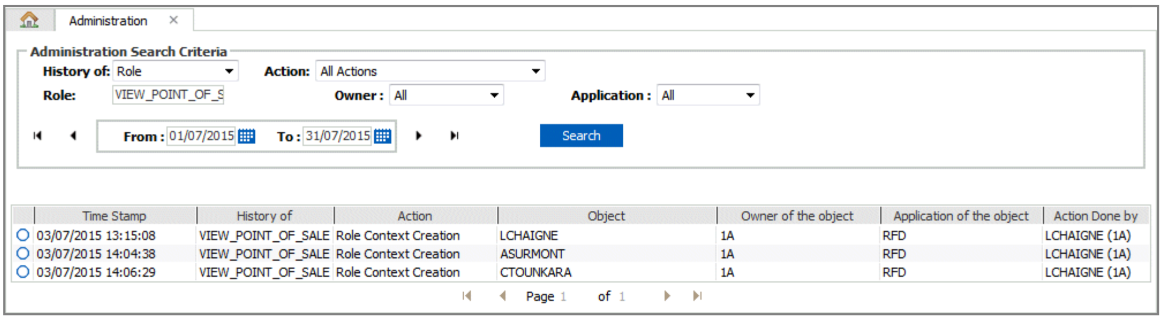
❶ Type of administration history requested.

❷ Date range for the history search.

❸ Actions performed on this item during the date range.

❹ Previous value before the change.

Image: History of Role Changes



Displaying the Authentication History

What Is Authentication History?

You can search for the history of actions such as login attempts, logouts, and password changes.

- You can run a search on the following levels: **User**, **Office** and **Organization**.
- Actions are one of: **Sign-in**, **Sign-out**, **Authentication factor management** or **Impersonation**.

The range of dates for which you can retrieve information depends on the search type. You can retrieve authentication events logged within the last two months. To retrieve authentication events within the last three years, you must open a work order (WO) and assign it to **MHDORM** (**DB End User Maintenance**).

Authentication history is only available for the hosted mode related events. The feature enables the LSS audit log, thereby enforcing PCI compliance.

How to Display Authentication History

1. Click on **Authentication Search** in the **History** section of the **Home** tab.
2. On the **Authentication** tab, select or enter your search criteria.
3. Optionally, use the other search criteria fields to further specify what you want to see in the history display.

   For example, enter a user ID when searching for a user, or a role name when searching for role history, an application or a type of action.
4. Enter a date range in the date fields. Use the arrows to shift the data range by one day or one week either side of the selected dates.
5. Click on **Search**.

   All the events corresponding to your search criteria are displayed.

   Note: **Full Location** corresponds to the full workstation location. See *Table: Full Location Parameters* on page 147.

What Are Location Type and Location Value?

Location type corresponds to the possession factor in multi-factor authentication (MFA). If the organization is set up and the application user interface is correctly configured for it, ASM displays **MAC** for the MAC address, **AIP** for the IP address or **SCO** for the cookie (used for web applications only).

Location value gives the value of the **Location type**, which is used only in MFA.

For more information on MFA, see *Applying Application Security* on page 30.

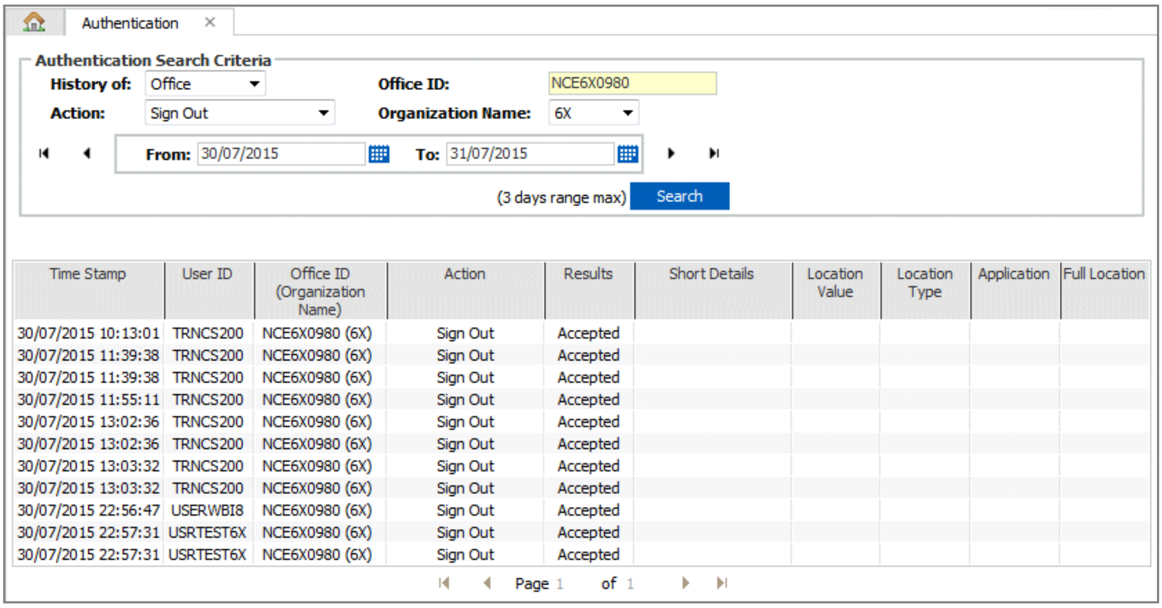
Table: Formats of Location Value

Location Type	Location Value Format
MAC address	A series of six pairs of hexadecimal characters optionally separated by a colon (:). Example: 00:60:94:25:51:4B

Location Type	Location Value Format
IP address	LSS supports both IPv4 and IPv6 values: - IPv4: A series of four sets of numbers ranging from 1 to 255 separated by periods (.). - IPv6: A series of eight sets of four characters separated by a colon (:). Example of IPv6: `2001:0db8:85a3:0042:1000:8a2e:0370:7334` - Additionally, the network mask can be added, corresponding to a slash (/) and a positive decimal value. Example for IPv4: `172.16.204.234 / 255.255.255.0`
Cookie	A string of 64 characters.

Example: Authentication History Display

Image: History of Password Changes in Office



Time Stamp	User ID	Office ID (Organization Name)	Action	Results	Short Details	Location Value	Location Type	Application	Full Location
30/07/2015 10:13:01	TRNCS200	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 11:39:38	TRNCS200	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 11:39:38	TRNCS200	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 11:55:11	TRNCS200	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 13:02:36	TRNCS200	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 13:02:36	TRNCS200	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 13:03:32	TRNCS200	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 13:03:32	TRNCS200	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 22:56:47	USERWBI8	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 22:57:31	USRTEST6X	NCE6X0980 (6X)	Sign Out	Accepted					
30/07/2015 22:57:31	USRTEST6X	NCE6X0980 (6X)	Sign Out	Accepted					

Chapter 3

Managing Your Organisation

What Is an Organisation?

Each organization using secured Amadeus applications is defined in ASM as a unique organization.

An organization is represented in the system as a hierarchical tree. This organization tree consists of nodes, as follows:

- **Organization (ORG)**

  This is the top node of the organization tree. The organization is created by Amadeus.

- **Organization Units (OGUs)**

  You can create any number of OGUs within an ORG, forming a hierarchical tree that reflects the organization's internal structure. This structure can be based on criteria such as business or geographical units. Each OGU must have a name that is unique within the organization tree.

- **Offices**

  Amadeus Office IDs are used to identify an office. Offices are created outside of Logon and Security Server (LSS), in the Amadeus Central System. However, they must be attached to ORGs or OGUs using Amadeus Security Management (ASM).

  The office ID is mandatory in an organization tree. Each office ID is unique within ACS. Office IDs always represent the lowest level in an organization tree.

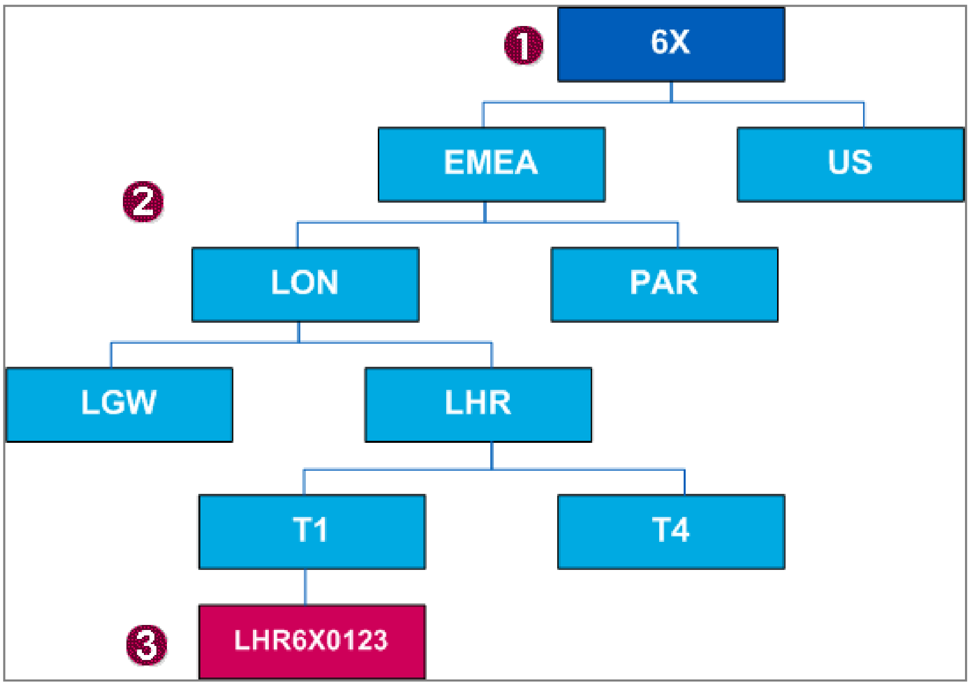
  Each user is linked to an office through their login area.

  Note: One user can be linked to several offices. However, a user can only have one sign per office.

  Note: Guidelines on how to design an organization for Amadeus ACOs are available from LSS Distribution product management.

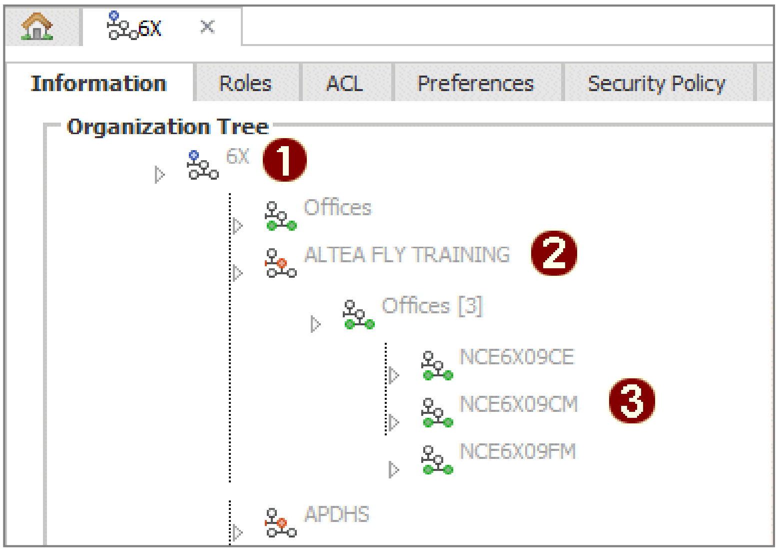
Example: Organisation Tree Structure (Airlines)

The organization of airline 6X is based on geographical criteria.



- ❶ Organization
- ❷ Organization units
- ❸ Offices

Example: Organisation Tree (Airlines)



- ❶ Organization
- ❷ Organization unit
- ❸ Office

Defining Your Security Policy

What Are Security Policy Settings?

Security policy settings are set at organization level and are inherited by all the organization units, offices, and users within the organization.

These settings include:

- **Payment Card Industry (PCI)-compliance**, through:
  - Password management.
  - Lock-out management.

  See *Specifying a PCI-compliant Security Policy* on page 26.
- **Multi-factor authentication (MFA) management**.

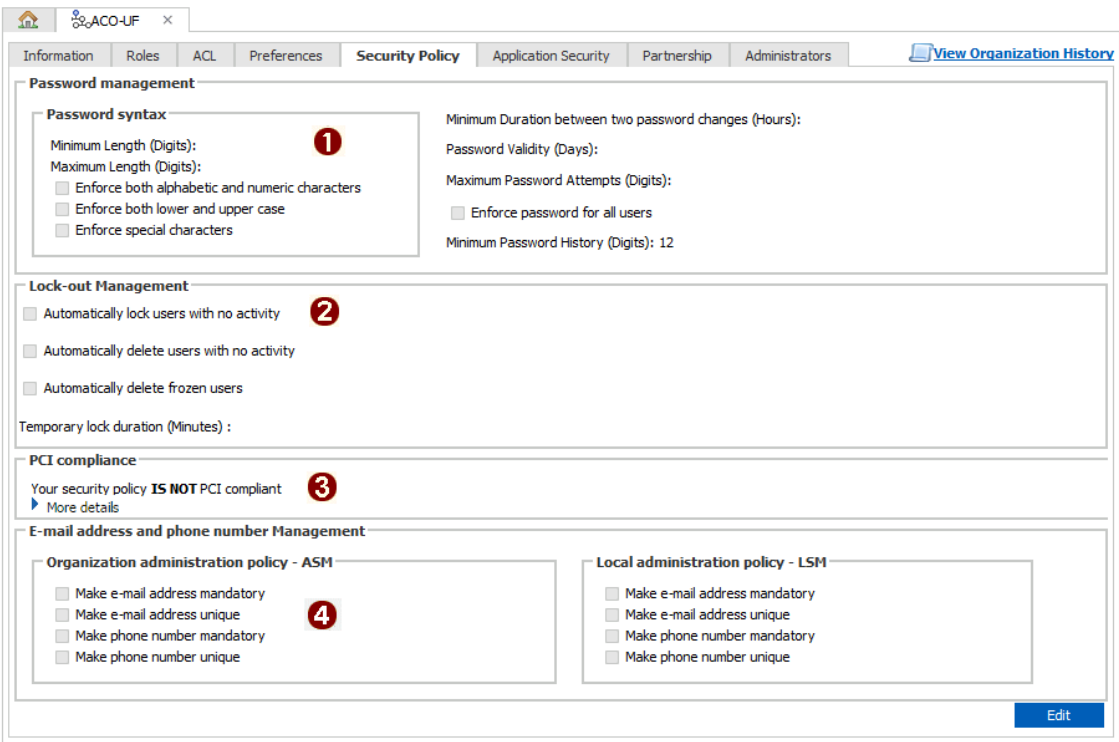
  See *Applying Application Security* on page 30.

How to View Your Organisation's Security Policy

1. In the **Organization Management** section of the **Home** tab, select your organization from the drop-down list, then click on **Manage organization**.
2. Select the **Security Policy** tab.

   This tab displays the various security settings for your organization.

Image: Security Policy Tab



❶ **Password Management**

See *Explanation: PCI-compliant Password Management Settings* on page 27.

❷ **Lock-out Management**

See *Explanation: PCI-compliant Lock-out Management Settings* on page 27.

❸ **PCI Compliance**

If ASM determines your settings are not PCI-compliant, the message **Your security policy is not compliant** is displayed. Click on the arrow to see more details.

❹ **E-mail and Phone Number Management**

Specifying a PCI-compliant Security Policy

What is a PCI-compliant Security Policy?

A PCI-compliant security policy prevents credit card fraud, hacking, and other security issues.

A company that processes credit-card payments must be PCI-compliant. To have a PCI-compliant security policy, you must protect and restrict access to sensitive data such as payment-card information. Your password and lock-out settings must follow, or be even more restrictive than, the rules below:

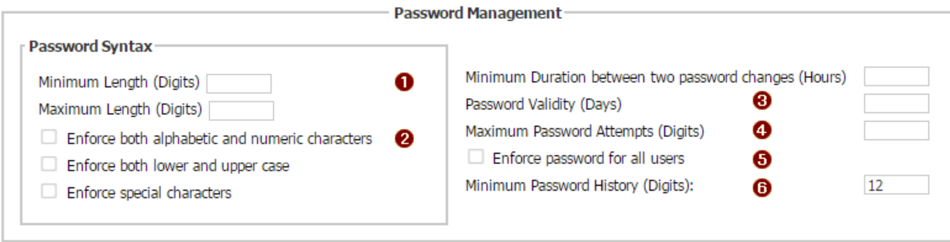
Table: Values for a PCI-compliant Security Policy

Setting	Required for PCI-compliance
Password management	
Password validity (days)	90
Minimum length (digits)	7
Enforce both alphabetic and numeric characters	Yes
Enforce password for all users	Yes
Maximum password attempts	6
Lock-out management	
Automatically lock users with no activity	Yes
Notification to be sent	14 days before lock/deletion
Number of inactive days before lock	90 or less
Temporary lock duration (minutes)	30

See also *How to Specify a PCI-compliant Security Policy* on page 29.

On your organization's **Security Policy** tab, the **PCI Compliance** pane shows whether the security settings of your organization are PCI-compliant.

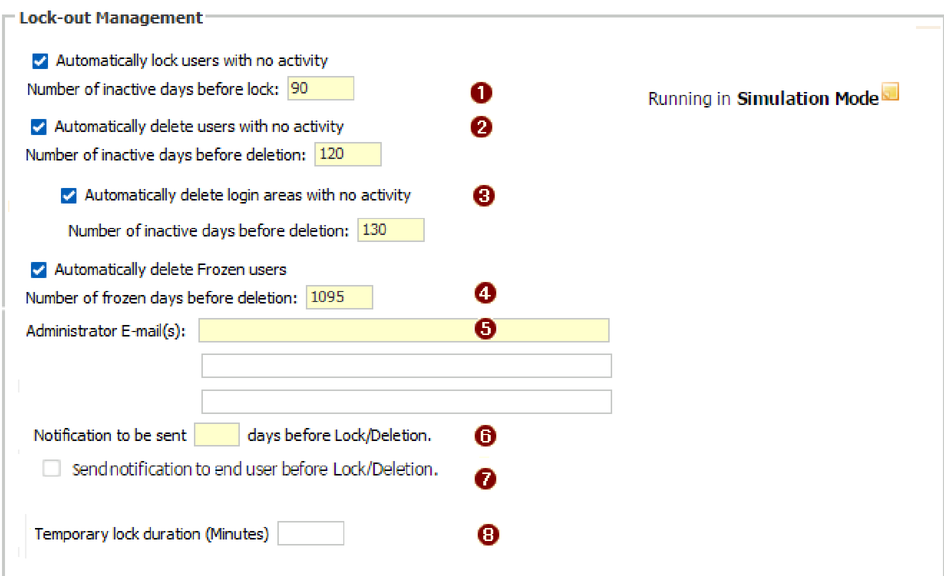
Explanation: PCI-compliant Password Management Settings



1. The number of characters that are needed to compose a password.
2. The password must contain alphanumeric characters.
3. The number of days a password is valid. When this period is over, a new password must be defined.
4. The number of consecutive, unsuccessful password attempts before the user account is temporarily locked.
5. If selected, all users of the organization are forced to use a password. Compulsory for PCI compliance.

   Note: It is strongly recommended to notify your Amadeus point of contact before you use the **Enforce password for all users** feature in the production environment.
6. This is mandatory for PCIDSS compliancy. The PCI minimum value is 4.

Explanation: PCI-compliant Lock-out Management Settings



1. Lock out inactive users after a defined number of days of inactivity. Inactivity means the user has not logged in or the account has been created but never used. Compulsory for PCI compliance and must be set to 90 days or less.
2. Delete inactive users after a defined number of days of inactivity or if the account has never been used. Not compulsory for PCI compliance but highly recommended.

❸ Delete login areas which have not been active for a defined number of days.

Note: You can only activate this option in Real Mode if the option **Automatically delete users with no activity** is also activated in Real Mode. This option does not apply to robotic, emergency, frozen, test-only or Skilling system-only users.

❹ Automatically delete users who have been frozen for a defined number of days.

❺ Email addresses of the organization's security administrators. These administrators receive daily email notifications of accounts to be deleted.

You can specify up to three email addresses.

❻ Send an email notification to the security administrators the specified number of days (for example, 14 days) before the automatic lock or deletion of an account or deletion of a login area.

❼ Send a notification to the end-user when an account or login area is to be automatically locked or deleted. Users will receive a first notification the specified number of days before lock or deletion, then a second notification the day before lock or deletion.

Note: This option is only available in Real Mode, when either or both of the automatic lock or deletion options are activated.

❽ The time, in minutes, during which a user is locked when the maximum number of unsuccessful password attempts has been reached. After this delay, the user can try to log in again.

Note: For automatic deletion of users, there is an additional optional check box in the **Lock-out Management** section: **Notify Users by e-mail about their account deletion**. The option has to be activated by OSR, so only the ORG who requested it can see the check box.

What Is Simulation Mode?

Lock-out management settings are first implemented in **Simulation Mode**.

While your security policy is in **Simulation Mode**, the administrators indicated in the **Security Policy** tab receive daily email notifications on the specified number of days before the automatic lock or deletion of accounts. The administrators can verify that the accounts indicated should be locked/deleted. However, as long as the policy remains in **Simulation Mode**, the system does not actually lock or delete accounts.

To exit Simulation Mode once you have verified your security policy, see *Process Flow: PCI Compliance in ASM* below.

Process Flow: PCI Compliance in ASM

1. Specify PCI-compliant settings on your organization's **Security Policy** tab. See *How to Specify a PCI-compliant Security Policy* below.

   The lock-out management policy is then put in Simulation Mode. See *What Is Simulation Mode?* above.

2. Open a work order (WO), select the **ADP Activation** template under **Security > Logon and Security Server (LSS) > Middleware** and assign it to **DSASSOS (Security Maintenance & Support)**.

3. Amadeus checks with your organization that your user setup is satisfactory. For example, a check is made that robotics are flagged correctly in LSS, so that they are excluded from the auto-lock and auto-delete processes.

4. Amadeus enables user lock-out and deletion. Lock-out management is now in Real Mode.

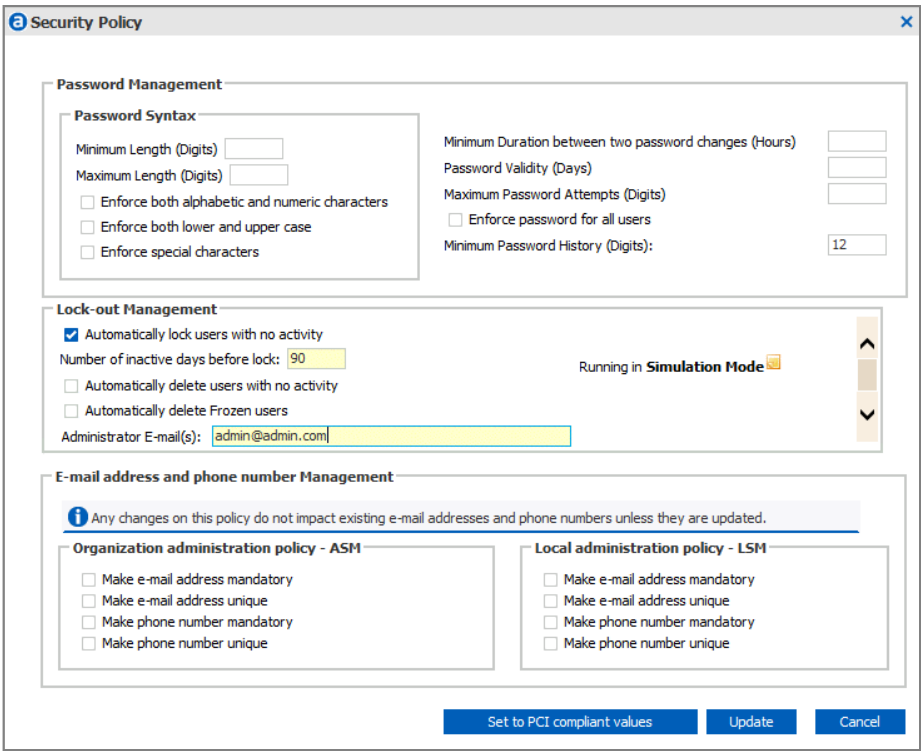
Note: This is permanent, unless you modify the number of inactive days. In this case, the lock-out management policy reverts to **Simulation Mode**, and you must open another WO.

How to Specify a PCI-compliant Security Policy

Note: It is strongly recommended that you notify your Amadeus point of contact before you use the **Set to PCI-compliant values** feature in the production environment.

1. In the **Organization Management** section of the **Home** tab, select your organization from the drop-down list, then click on **Manage organization**.
2. Select the **Security Policy** tab.
3. If required, in the **PCI Compliance** pane, click on the arrow next to **More details** to review the settings required for PCI compliance and see which areas of your policy are not compliant.
4. Click on **Edit**.

   The **Security Policy** dialog box displays the current settings.



5. Click on **Set to PCI-compliant values**.

   The **Security Policy** window is updated with PCI-compliant settings. For example, inactive accounts are locked after 90 days.
6. If required, modify the password and lock-out settings, ensuring they remain PCI-compliant.
7. To ensure that security emails reach individual end-users, you can specify in the **Email address and phone number management** section that an email address is mandatory and unique when a user is created.

   If the **Make email address unique** option is set, a new user cannot be created or updated with an email address already associated to another user.

You can also specify that a phone number is mandatory and unique.

8. Click on **Update**.

   The security policy rules are set to those required for PCI compliance.

   The **Lock-out Management** pane of the **Security Policy** tab indicates that the policy is in **Simulation Mode**. See *What Is Simulation Mode?* on page 28.

Applying Application Security

What Is Multi-Factor Authentication?

Multi-factor authentication is an authentication method that requires the presentation of multiple known factors for the system to grant a user access to an application.

- **A knowledge factor:** Something the user knows, such as a password.
- **A possession factor:** Something the user has, such as a MAC address, IP address or browser cookie.

There are two MFA methods available in ASM:

- **Location-based:** Authentication is secured through a one-time password and the identification of your computer through an address or cookie.
- **DDNA-based:** Authentication is secured through a one-time password and a hash value computed by a plug-in on your computer.

How Does Location-Based MFA Work?

When a user logs in to an application for the first time, Logon and Security Server (LSS) stores the user's MAC or IP address, or generates a browser cookie. This corresponds to the possession factor.

If, after the first successful login, the user logs in from a workstation with an unknown possession factor, LSS sends the user a one-time password by email or SMS. When the user has successfully logged in with the one-time password, this possession factor is added to the list of known authentication factors for that user. Subsequent log-in attempts from that workstation will not trigger the sending of another one-time password.

Example: Logging In to an Application with MFA Applied

Successful Login Attempt	From a Workstation with IP Address	IP Addresses Stored in ASM for this User	One-Time Password Sent?
First	123.XX.XXX.X	None	Yes
Second	456.YY.YYY.Y	123.XX.XXX.X	Yes
Third	789.ZZ.ZZZ.Z	123.XX.XXX.X 456.YY.YYY.Y	Yes
Fourth	123.XX.XXX.X	123.XX.XXX.X 456.YY.YYY.Y 789.ZZ.ZZZ.Z	No

In ASM, you can define how many possession factors can be stored in LSS for each user, and for how long each possession factor is stored.

What is DDNA?

Digital DNA (DDNA) is a Multi-Factor Authentication (MFA) system that is used to verify whether a user can be granted secure access to an application.

DDNA is a unique key computed by a plugin that an LSM administrator installs on a user's computer. The plugin computes the hash value of the attributes of the computer, and devices such as USB keys that are connected to it. The hash value is unique and does not change with time or use.

Once the plugin is installed on a computer, any users needing to use the device will need to be registered on that device, either by the LSM administrator (Admin enrolment) or through self-enrolment.

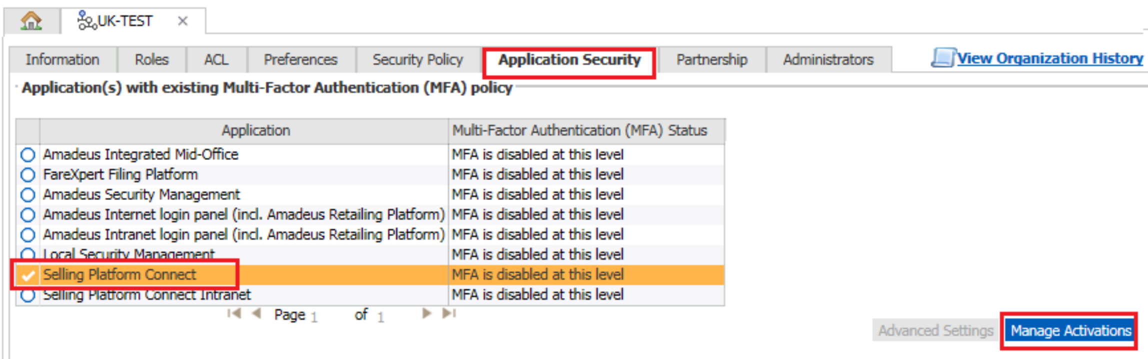
In LSM, this process of computing the hash value is called Registering the Digital DNA - see the *Amadeus Local Security Management User Guide*.

LSS compares this hash value against a list of registered computer/devices that the user is allowed to use. If the hash value is in the list, the user is granted access to the application. If a user tries to login from a device that has not been registered to their User ID, the request will be rejected.

How to Apply Application Security for Your Organisation

1. On the **Home** tab, under **Organization Management**, select your organization and click on **Manage Organization**.
2. Select the **Application Security** tab.

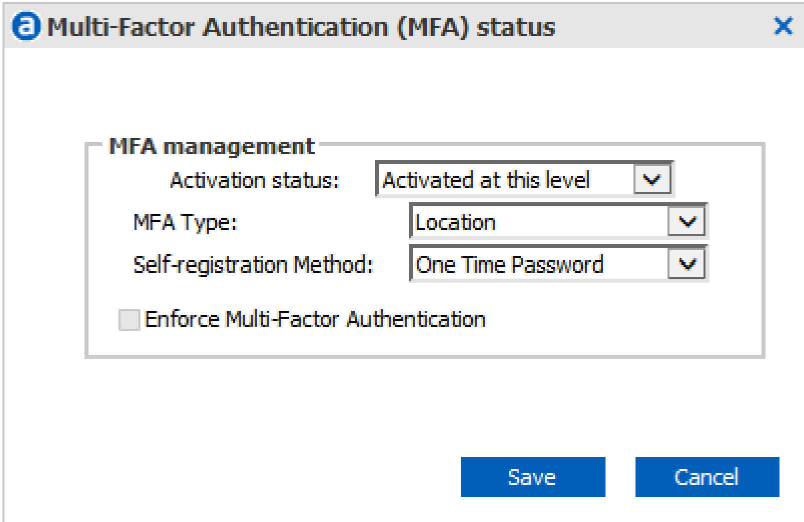
   This tab is available at ORG level, OGU level, Office level, or User level. For example, if you want to setup application security for an office only, you must view the office details and select the **Application Security** tab of the office.
3. Chose the application in the drop-down list and select **Manage Activations**.



   The **Multi-Factor Authentication (MFA) status** dialog box opens.
4. By default, **Activation status** is set to **Deactivated at this level**. Select **Activated at this level** from the drop-down list.

   Note: For any level lower than ORG, there is also the option **Inherited from upper level**.

   The fields **MFA Type** and **Self-registration method** become available.



5. For **MFA type**:
   - If you select **Location**, then for **Self-registration method** the only option is **One Time Password**.
   - If you select **DDNA**, then for **Self-registration method** select either **One-Time Password** or **Approved by Admin**.
6. Optionally select the check box **Enforce Multi-Factor Authentication** parameter to prevent anyone changing the MFA activation at lower levels.

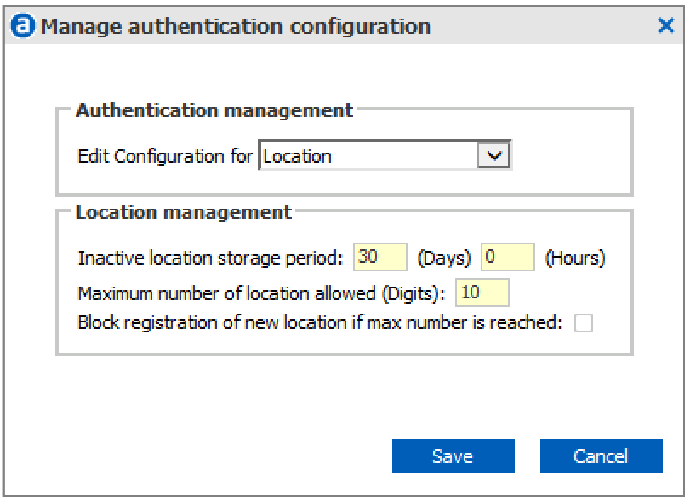
If you set **MFA Type** to:

- **Location**, then you need to also make some additional location settings. See *How to Set Location Settings* below.
- **DDNA**, then you need to set up DDNA. See *How to Set Up DDNA* on page 35.

How to Set Location Settings

1. On the **Home** tab, under **Organization Management**, select your organization and click on **Manage Organization**.
2. Select the **Application Security** tab.
3. Select **Advanced Settings**.

   The **Manage authentication configuration** dialog box appears.
4. Select **Location** from the drop-down list to specify your location management settings.



5. **Inactive location storage period**: Enter the period that LSS will store an inactive location before it is considered obsolete. The maximum days allowed is 90.

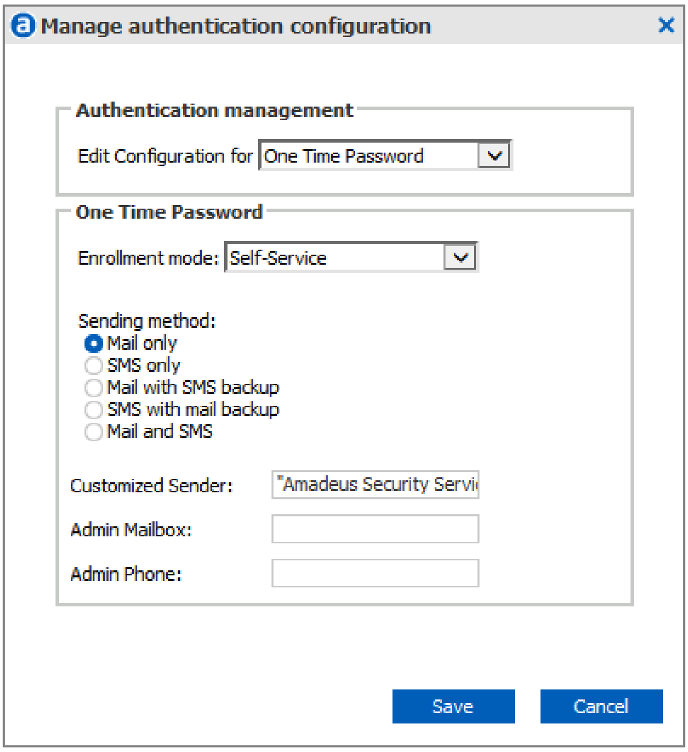
6. **Maximum number of locations allowed**: Enter the number of possession factors that LSS can store for each user. The maximum allowed is 10.

   By default, if the maximum number of locations for the active rule is reached, and the user tries to register a new location, the oldest location currently stored for this application is deleted. To prevent any new locations being stored when the maximum is reached, select the check box **Block registration of new location if max number is reached**. If this option has been selected, one or more existing locations must be revoked before new locations can be registered.

   If the maximum number of locations is set to 0, ASM does not check if the location is registered already and the one-time password is sent for each authentication request.

   Note: The locations are stored at user level and can be viewed in the **Location** tab for each user.

7. Select **One-time Password** from the drop-down list to specify the enrolment mode and sending method.



8. For **Enrolment Mode**, select one of the following options:

   - **Self-service**

     Indicates that the user can register new locations themselves.

   - **Approved by Administrator**

     Indicates that self-registration is restricted. In this case, the administrator will receive the one-time password. You must enter the administrator's email in the **Admin Mailbox** field.

   In both cases, you must select one of the **Sending method** options to indicate how the one-time password is sent.

Table: Sending Methods and Backup Details

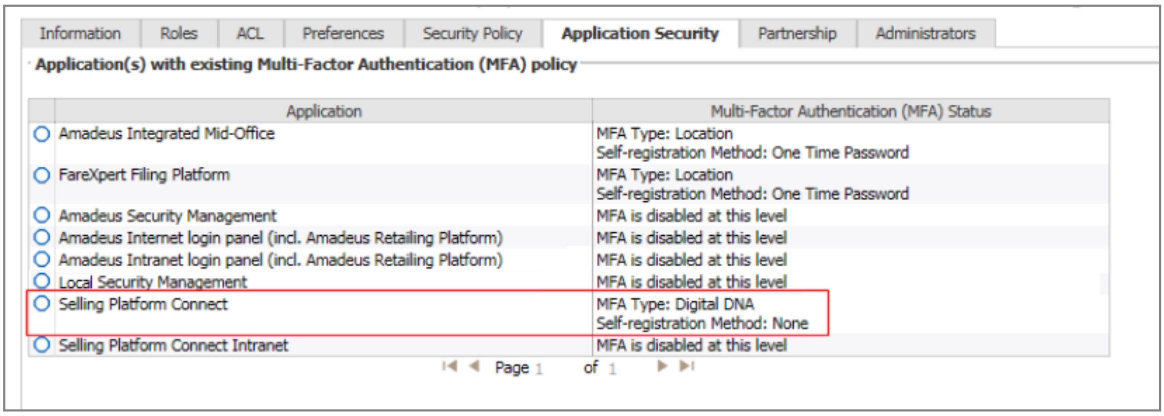
Sending Method	Backup Details
Mail only	No backup. If there is no email address in the user profile, the one-time password is not sent.
SMS only	No backup. If there is no phone number in the user profile, the one-time password is not sent.
Mail with SMS backup	If there is no email address in the user profile, an SMS is sent. If there is no phone number in the user profile, the one-time password is not sent.
SMS with mail backup	If there is no phone number in the user profile, an email is sent. If there is no email address in the user profile, the one-time password is not sent.
Mail and SMS	No backup. If there is no phone number or email address in the user profile, the one-time password is not sent.

Note: The one-time password is valid for 15 minutes.

Note: When a one-time password is sent, ASM checks the enrolment mode and sending method from the most restrictive rule in the organization tree that applies for the authentication request on the identified product.

9. Click on **Save**.

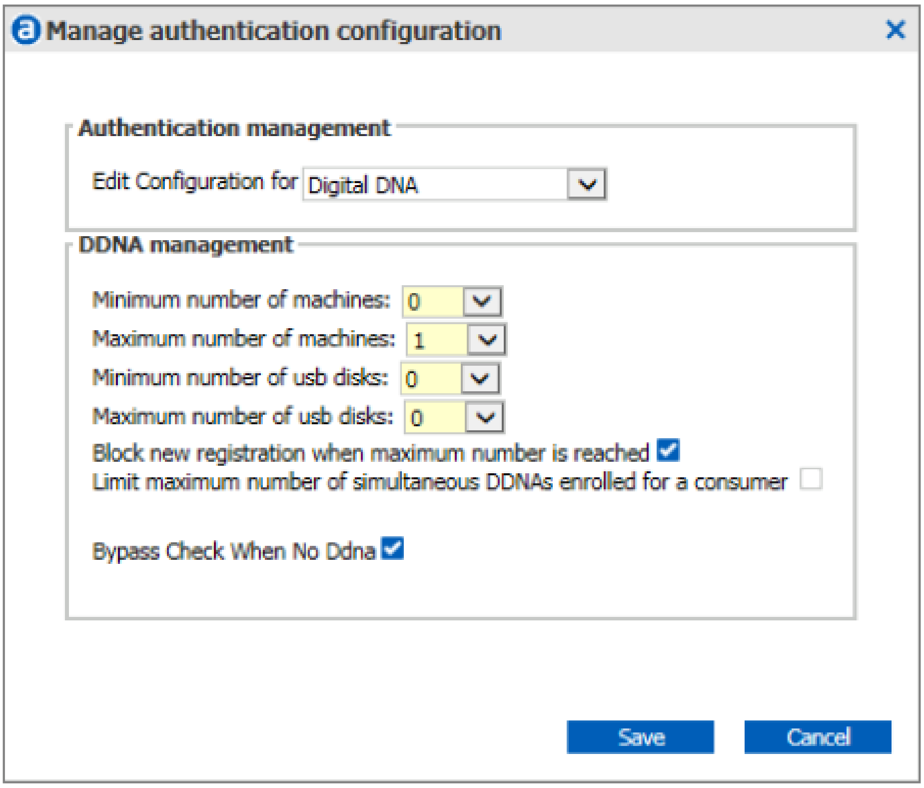
   The new security settings are applied to the application:



How to Set Up DDNA

1. On the **Home** tab, under **Organization Management**, select your organization and click on **Manage Organization**.
2. Select the **Application Security** tab.
3. Select **Advanced Settings**.

   The **Manage authentication configuration** dialog box appears.
4. Select **DDNA** from the drop-down to specify your location management settings.



5. Set the DDNA management settings:
   - Specify the minimum and maximum numbers of machines and USB disks.
   - Optionally specify whether to block new registrations when the maximum number set above is reached.
   - Optionally specify whether to limit the maximum number of simultaneous DDNAs enrolled for a consumer.
6. While performing the DDNA setup, it is suggested to select the check box **Bypass the DDNA check**. Once the setup is completed and all users are registered, this can be switched off.

Users can now be registered by the LSM admin on each machine. For details see the *Amadeus Local Security Management User Guide*.

Inheritance Rules Applied to an Organisation

What Inheritance Rules Apply to an Organisation?

Offices in an organization inherit most of their data security information from the organization unit to which they belong. However, preferences and action types of permissions assigned at user level override the ones assigned at higher levels.

Reference: Inheritance Rules

LSS Security Element	Inheritance
General security information	From the organization to which the office belongs.

LSS Security Element	Inheritance
Roles	From the organization units higher in the branch.
ACLs	From the organization units higher in the branch.
Preferences Action types of permissions	Preferences and action types of permissions assigned at user level prevail. Inheritance from the top level applies only if no preference or permission has been assigned at a lower level.

What Is an Office Mask?

Office masks are filters that are used to define the format of offices that can be linked to an organization or an organization unit. An office mask is composed of three parts: office ID, vendor code and country code.

Amadeus defines the office mask at organization level, and you cannot modify it. However, you can create office masks at lower levels in the organization tree.

When you are trying to link an office to an organization or organization unit, the system checks that the link attempt is compliant with the office mask set for that node. If no office mask has been set for the node, the system checks the parent hierarchy until it finds an office mask against which to validate the link attempt.

Office ID

The office ID consists of nine characters, as follows:

1. IATA city or airport code - first three characters.
2. Corporate ID - next three characters, composed of:
   - Corporate code - two characters.
   - Corporate qualifier - one character from 0 to 9.
3. Office identifier - final three characters.

When setting office masks, you can replace some of the characters by asterisks (*), which are wildcard characters. The following rules apply:

- City code: In full or only as asterisks: cannot be a combination of both. For example, you can enter `LON` or `***` but you cannot use `L**`.
- Corporate ID: In full or as a combination of asterisks and characters. However, the corporate code (the first two characters) must be either in full or only as asterisks. For example:
  - `6X*`
  - `6X0`
  - `**2`
  - `UF*`
  - `UF2`
- Office identifier: Any combination of characters and asterisks allowed.

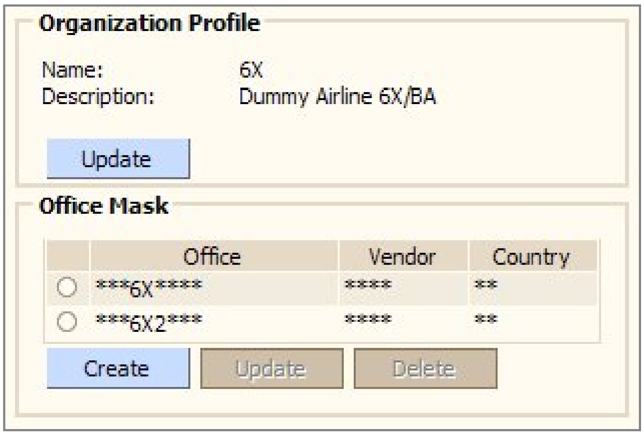
Vendor Code

A vendor code identifies the owning market of an office ID and its associated data. The vendor code associated with an office is stored in the **UVC** field of the office profile in the Amadeus central system (ACS). It is composed of four characters. It can be represented in the office mask by four alphanumerical characters or four asterisks, but it cannot be a combination of both.

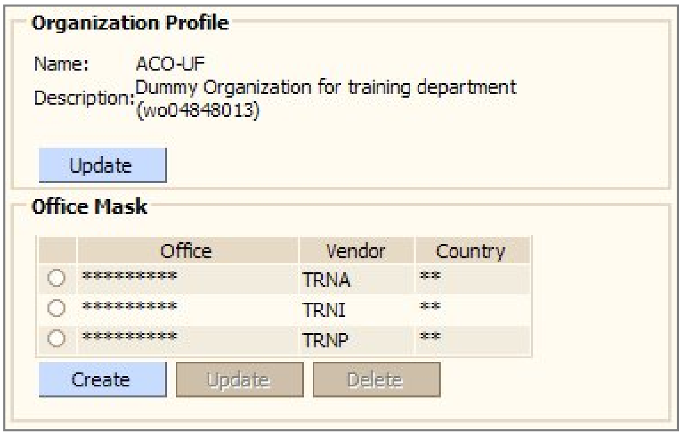
Country Code

A country code is composed of two characters. It can be two alphanumerical characters or two asterisks, but it cannot be a combination of both.

Example: Office Mask at Organisation Level (Airlines)



Example: Office Mask at Organisation Level (ACOs)



Assigning Access Rights to an Organisation Unit

You can assign access rights and preferences to an organization unit or office ID, so that all users under the organization unit inherit the rights.

For more information, see:

- *How to Assign a Role* on page 96.
- *How to Assign Multiple Roles (Airlines)* on page 97.
- *How to Assign an ACL to a Consumer* on page 98.

- *How to Assign Multiple ACLs (Airlines)* on page 99.
- *How to Assign a Preference* on page 102.
- *How to Assign Multiple Preferences (Airlines)* on page 103.

Working at Organisation Level

How to Display an Organisation

1. In the **Organization Management** pane of the **Home** tab, select the organization you want to display from the drop-down list.
2. Click on **Manage Organization**.

   The **Information** tab of the organization is displayed. This tab contains the **Organization Tree**.

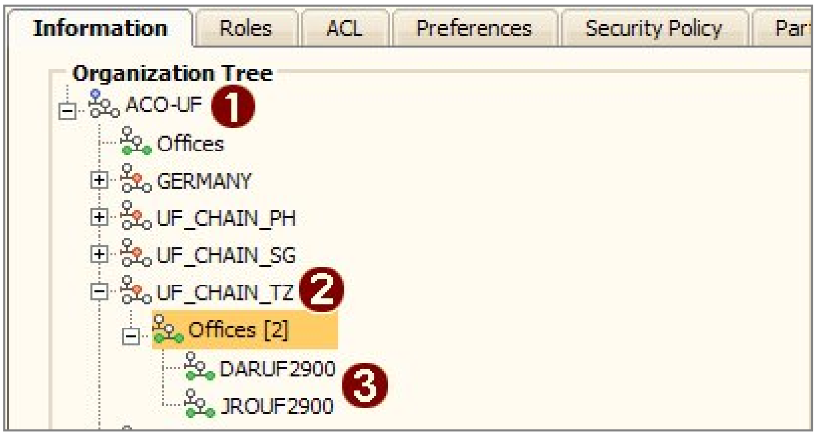
Example: Organisation Tree (Airlines)

❶ Organization

❷ Organization unit

❸ Offices

Example: Organisation Tree (ACOs)



❶ Organization

❷ Organization unit

❸ Offices

If you are allowed to administer more than one organization, you can display the list of organizations in the **Organization Management** pane.

By default, only your organization is listed. Add the other organizations using the organization search in the left menu bar. See *How to Add an Organisation to Your List* on page 15.

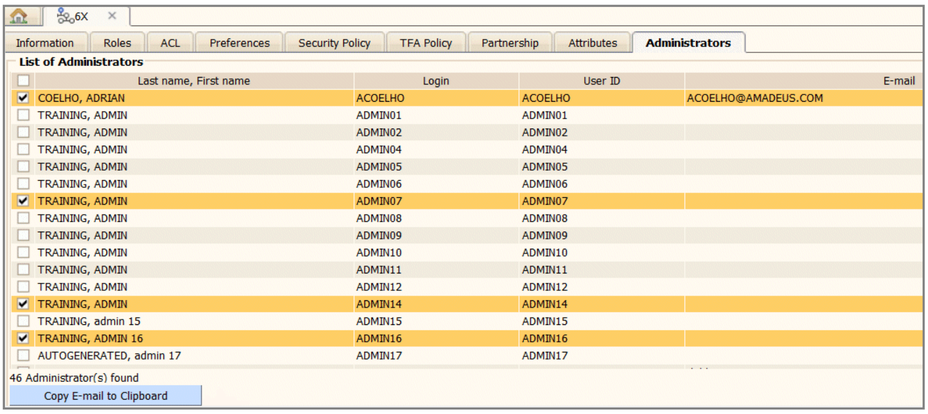
Note: Hover the mouse over any organization unit to display its full name.

Note: You can display up to 10 organizations at the same time, in 10 separate tabs, provided you have not opened any other types of tab.

How to Display the List of Administrators of an Organisation

1. On the **Home** tab, select your organization and click on **Manage organization**.
2. Select the **Administrators** tab.

   The list of all administrators who have the generic role `LSS_FULL_SECURITY_ADMIN` and the corresponding ACL for the organization is displayed.



How to Update an Organisation's Profile

1. Create a generic work order (WO) with your request.
2. Assign your WO to **MHDORM** (**DB End User Maintenance**).

Working With Organisation Units

How to Create an Organisation Unit

1. On the **Home** tab, select the organization and click on **Manage organization**.
2. Click on **Create OGU**.
3. Follow the steps of the pop-up wizard to create the organization unit (OGU).

   Remember that each OGU must have a name that is unique to all other organization units, regardless of where each appears in the organization tree.
4. Select your newly created OGU in your organization tree and click on **View details**.
5. Optionally, create office masks specific to the OGU.

   If you do not create an office mask, the OGU inherits the office masks of its parent OGU or the office masks set for the entire organization.

   See *How to Create an Office Mask for an Organisation Unit* below.
6. Create any child OGUs if necessary.

   To create an OGU below an existing OGU, select the existing OGU and follow the same steps.
7. Add offices to the OGU.

   See *How to Add an Office to the Organisation Tree* on page 43.

How to Create an Office Mask for an Organisation Unit

1. In the **Home** tab, select the organization and click on **Manage Organization**.
2. Expand the organization tree, click on the organization unit to which you want to apply an office mask, then click on **View details**.
3. In the **Office Unit Office Mask** pane, click on **Create**.
4. Enter the office mask values.

   For more information, see *What Is an Office Mask?* on page 37.
5. Click on **Finish**.

How to Move a Unit in an Organisation

1. In the **Home** tab, select your organization and click on **Manage organization**.
2. In the **Information** tab, expand the organization tree and select the organization unit (OGU) or office ID.
3. Click on **Move**.
4. Select the targeted position.
5. Click on **Save**.

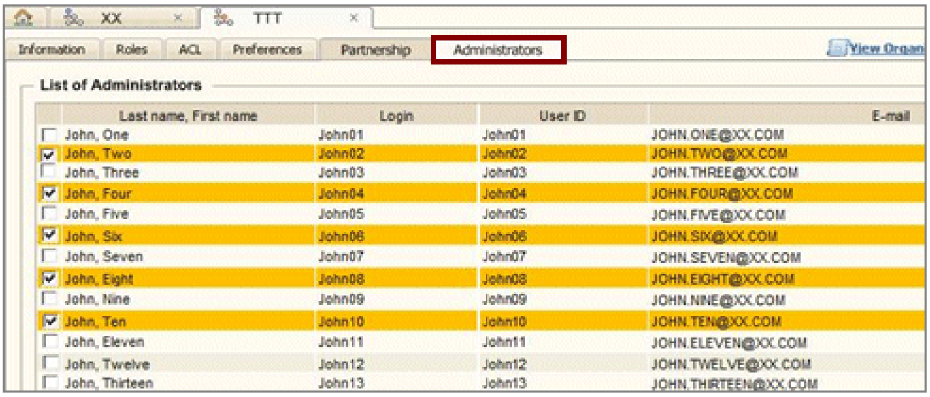
If you have selected an OGU, all of the OGUs and offices beneath this OGU are also moved to the new location. If partnerships had been defined at OGU level, they are automatically removed.

To move multiple offices, see *Managing Multiple Offices* on page 44.

How to Display the List of Administrators of an Organisation Unit

1. In the **Home** tab, select your organization and click on **Manage organization**.
2. Expand the organization tree and select the organization unit (OGU).
3. Click on **View details**.
4. Click on the **Administrators** tab.

   The list of all administrators who have the generic role `LSS_FULL_SECURITY_ADMIN_ON_OGU` and the corresponding ACL for the OGU is displayed.



How to Modify an Organisation Unit

1. In the **Home** tab, select your organization and click on **Manage organization**.
2. Expand the organization tree and select the organization unit (OGU).
3. Click on **View details**.

   On the OGU's **Information** tab, you can update the OGU's profile and add, modify or delete office masks.

Note: If you update the name of an OGU, and there are roles or ACLs assigned to the OGU, the rights inherited by users become unavailable until a database synchronization has been completed. You will receive a warning message to confirm this.

Remember that each OGU must have a name that is unique within the organization tree.

How to Delete an Organisation Unit

1. On the **Home** tab, select your organization and click on **Manage organization**.

2. Expand the organization tree and select the organization unit you want to delete.
3. If there are any linked child organization units or offices, you must remove them before you can delete the unit.

   Follow the steps below for all child organization units.

   See *How to Remove an Office from the Organisation Tree* on page 44.
4. Click on **View details**.
5. Remove all the roles and ACLs from the organization unit.

   For more information, see the following topics:

   - *How to Remove a Role* on page 97.
   - *How to Remove an ACL from a Consumer* on page 100.
6. Return to the **Information** tab for the organization, and click on **Remove**.

Working With Offices

Managing Individual Offices

How to Add an Office to the Organisation Tree

1. In the **Home** tab, select your organization and click on **Manage organization**.
2. In the **Information** tab, click on **Add office**.
3. Expand the organization tree to find the appropriate organization unit.
4. Click on **Next**.
5. Enter the **Office ID**.

   Confirm that the office ID matches one of the **Office masks** at the selected level.
6. Click on **Finish**.

How to Display the User Login Areas in an Office

1. In the **Home** tab, select your organization and click on **Manage organization**.
2. Expand the organization tree and select the office for which you want to display a list of users.
3. Click on **View details**.
4. Select the **Login Areas** tab.

   To sort the results in alphabetical order, click on any of the column headings.

   To filter the results, select a filter criteria, enter a string in the **Value** field and click on **Search**.

   Note: You can also display a list of users in an office from the **User Search** menu. See *How to Display a List of Users in an Office* on page 17.

How to Remove an Office from the Organisation Tree

1. In the **Home** tab, select your organization and click on **Manage organization**.
2. Expand the organization tree and select the office you want to remove.
3. Click on **View details**.
   a) Select the **ACL** tab and remove all ACLs.

      See *How to Remove an ACL from a Consumer* on page 100.

   b) Select the **Roles** tab and remove all roles.

      See *How to Remove a Role* on page 97.
4. Return to the **Information** tab for the organization and click on **Remove**.

   Note: All the login areas linked to the office are automatically deleted when the office is removed from the organization tree. However, the office is not removed from Amadeus Central System. You can add the office back to the organization tree in the future if necessary.

How to Lock or Unlock an Office

1. In the **Home** tab, select your organization and click on **Manage organization**.
2. Expand the organization tree and select the office you want to lock or unlock.
3. Click on **View details**.
4. Select the **Information** tab.
5. Click on **Lock** or **Unlock**.

   The lock status is shown in the **Status** line in the profile. When an office is locked, no users can log in to that office.

Note: If any user is already signed in while the office is being locked, that user will be forcefully signed out and they will not be able to log in again.

Managing Multiple Offices

What Is Massive Move for Offices and Organisation Units?

Massive Move (Offices And Organization Units) allows you to move multiple offices within an organization (ORG) in a single operation. Typically, you do this when the offices have been imported into your organization by Amadeus, but you need to move them into organization units (OGUs) as you reorganise your organization tree.

The possible move operations are:

- Multiple offices from an ORG root to multiple OGUs.
- Offices within OGUs to other OGUs.
- Multiple OGUs and their offices to other OGUs.

To perform a massive move, you define the source offices and/or OGUs and their destinations, in a downloadable template. See *How to Move Multiple Offices* on page 45.

Note: You cannot move offices that are in partnership. You must move the whole OGU, and the partnership is removed as a consequence.

To move individual offices and OGUs, see *How to Move a Unit in an Organisation* on page 41.

How to Move Multiple Offices

1. Go to **Home > Data Management > Download Templates for Massive Actions**.
2. In the **List of Templates** pane, select the **Move Offices & Organization Units** template, then click on **Download template**.
3. Enter the source and destination information in the Excel file template on the **Move Office** or **Move Organization Unit** tabs, as appropriate.

   See *Explanation: Move Office and OGU Template Fields* below.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management >Massive Move (Offices and Organization Units)**.
6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, then click on **Upload**.

   The move is performed. The **List of Requests** pane indicates the status.
7. If there is an error, select the file, then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.
8. Check the report sent to the email address indicated in the first line of the file.

   See *Explanation: Massive Office Move Email Report* below.

Explanation: Massive Office Move Email Report

Email subject line:	`[status]` Mass Import Report. File name `[Mail x of n]` `(environment)`
For example:	`[Failure]` Mass Import Report. LSS_SYNCHRO_DF_1A_UAT_120916.csv [Mail 1 of 1] (UAT)

Possible errors include:

- Invalid organization.
- Invalid office ID.
- Office ID does not match the office mask of the target organization unit.

Explanation: Move Office and OGU Template Fields

You use the **Move Office** template to specify the offices to be moved and their source and destination OGUs.

Table: Move Offices Template Fields Explanation

Field	Tabs	Explanation
Organization label	• Move Office • Move Organization Unit	Source organization. 1 to 10 alphanumeric characters and hyphen (-). Same as **Organization Label of Destination**.
Office label	Move Office	Enter the office ID of every office you want to move. 9 alphanumeric characters. Wildcards characters are not allowed.
Organization unit label	Move Organization Unit	Source organization unit.
Organization label of destination	• Move Office • Move Organization Unit	Destination organization. 1 to 10 alphanumeric characters and hyphen (-). Same as **Organization Label**.
Organization unit label of destination	• Move Office • Move Organization Unit	Optional. 1 to 20 alphanumeric characters, and hyphen (-) and underscore (_).
WIN@proach item type:	Options	For example, work order (WO).
WIN@proach item number:	Options	For example, WO number.
Comment	Options	Any relevant remarks.
Email	Options	Administrator's email address. This is the address to which the report will be sent.

Adding Offices to Your Organisation

What Features Can Help You Add Multiple Offices to Your Organisation?

Two features allow you, in a single operation, to move multiple offices that have no organization assigned to them into an organization (ORG) in LSS:

- **Add Offices (With Mask)**.This feature is available only upon request to Amadeus. See *How to Add Multiple Offices Using Office Masks* on page 47.
- **Massive Import (Users, Rights, Offices)**. This feature is available to ACOs only. See *How to Add Multiple Offices Using Templates for Massive Actions (Airlines)* on page 47.

Access to these features depends on your LSS rights.

To add offices individually, see *How to Add an Office to the Organisation Tree* on page 43.

How to Add Multiple Offices Using Office Masks

Note: This feature is available only upon request to Amadeus. For airlines, all new offices with the corporate qualifier 0 or 1 are added to the default OGU automatically.

1. Go to **Home > Data Management > Add Offices (With Mask)**.
2. In the **Add Offices (With Mask)** tab, enter the destination organization, then click on **Select**.

   The **Organization Profile** pane displays a summary of the organization.
3. If required, click on **Office Masks** to view the office masks you can use as selection criteria.
4. In the **Enter Offices Selection Criteria** pane, enter the masks for **Office ID**, **Vendor** and **Country**. For example, `NCE1A0***, ****, **`.

   Note: You must include a **Corporate ID** in the **Office ID**.
5. Click on **Offices List** to display and, in the **List of Matching Offices** pane, check the offices that will be added using your criteria.
6. Click on **Next**.

   The tab displays two panes: **Offices Selection Criteria** and **Choose Destinations**.
7. In the **Choose Destinations** pane, select the organization or organization unit to which you want to add the offices, then click on **Add Offices**.

   The **List of Requests** is refreshed, and indicates the status of the addition. The addition can take a few minutes. When the offices have been added, an email notification is sent to the administrator.
8. To view details of a request or check any errors, select the request from the list, then click on **View Details**.

   The **Request Details** pop-up window is displayed.

How to Add Multiple Offices Using Templates for Massive Actions (Airlines)

1. Go to **Home > Data Management > Download Templates for Massive Actions**.
2. In the **List of Templates** pane, select the **Manage Offices** template, then click on **Download Template**.
3. Enter the appropriate information in the **Add Offices** tab of this template.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.
6. In the **File Path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, then click on **Upload**.

   The offices are added. The **List of Requests** pane indicates the status.
7. If there is an error, select the file, then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.
8. Check the report sent to the email address indicated in the first line of the file.

Creating Offices

How Are Offices Created?

You create office IDs in ACE. Administrators with the appropriate rights can access a version of ACE from the **Amadeus Retailing Platform** menu. The ACE link is displayed only when access rights are granted.

Note: ACE in ARP will be available to new airlines to be implemented in Altèa Reservation/Inventory/Ticketing and who will be using ARD Web and has NOT been implemented with the TN3270 panel. Airlines with existing access to ACE from the ARD Classic TN3270 panel should continue to use this until they are informed by Amadeus that they can move to access ACE from the Amadeus Retailing Platform.

How to Access ACE

1. Open a work order (WO) and assign it to **MHDORM** (**DB End User Maintenance**).
2. Copy the following info to ask for the rights to access ACE:
   - Application: RFD/RFD_MDW/ACE.
   - Permission: VIEW_ACE_PANEL.
   - Generic Role: ACE_PANEL_USER.
3. When the WO is completed, go to **Amadeus Retailing Platform > Security Portfolio > ACE**.

   The ACE cryptic window is displayed.
4. Enter `CICSP` and press **Enter**.
5. Sign in with your credentials, then create offices according to the standard ACE procedure.

   For further information, see the *ACE User Guide*.

Working With Metagroups

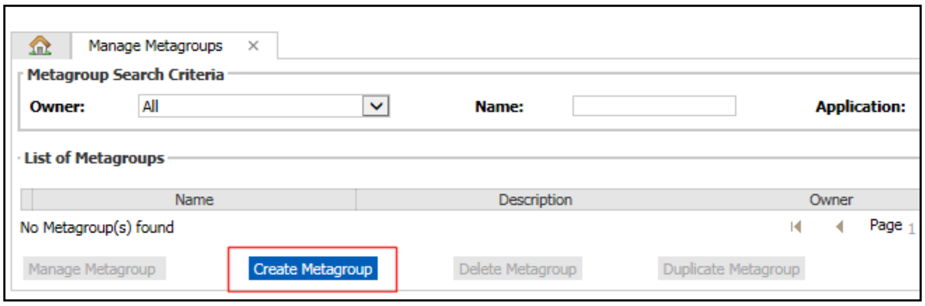
Note: This feature is not available for airlines.

A metagroup is an LSS object that gathers a list of Offices, OGUs and ORGs from different LSS Organizations.

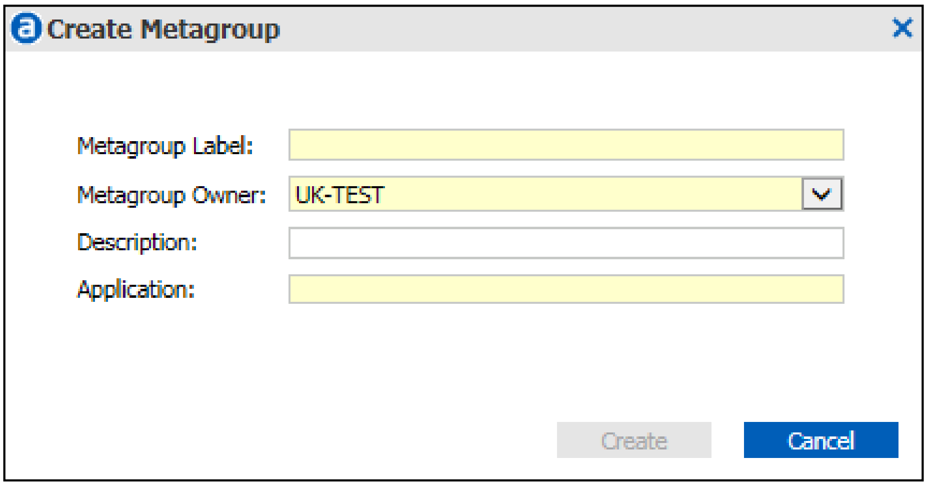
A metagroup can then be used by Amadeus applications to apply a unique security setting across a pool of Office IDs.

How to Create a Metagroup

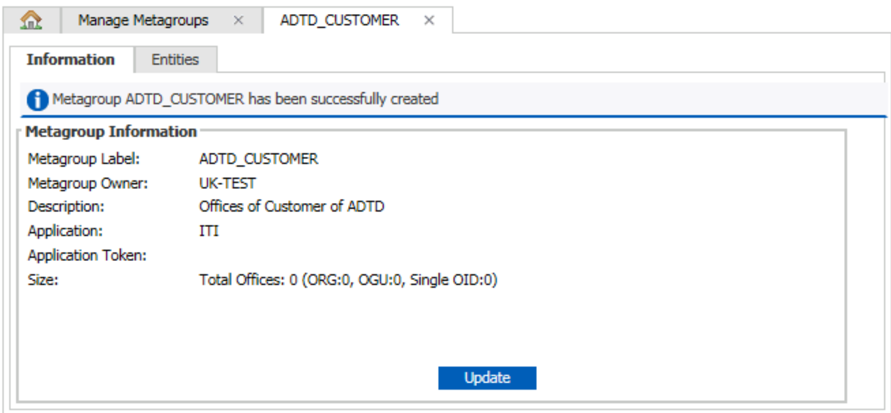
1. In the **Home** tab, under **Organization Management**, click on **Manage Metagroups**.
2. In the **Metagroups** tab, click on **Create Metagroup**.



3. Enter a label for the metagroup, select the owning organization from the drop-down list, specify the application to which it applies, then click on **Create**.

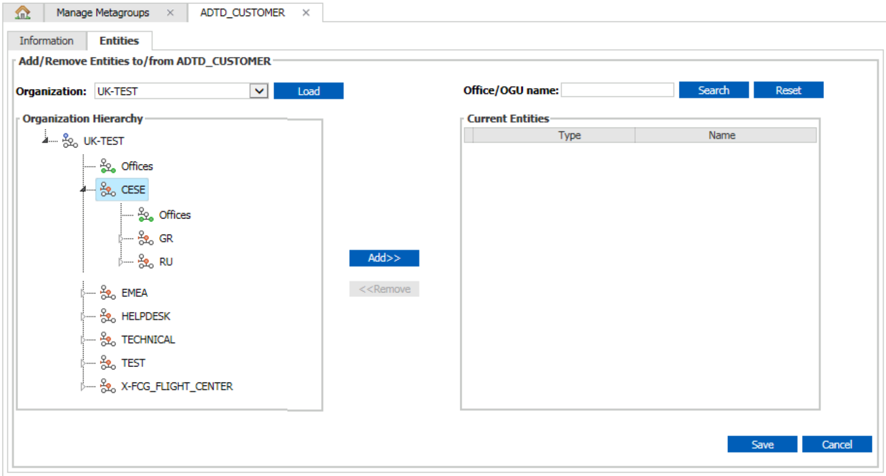


The metagroup is created.



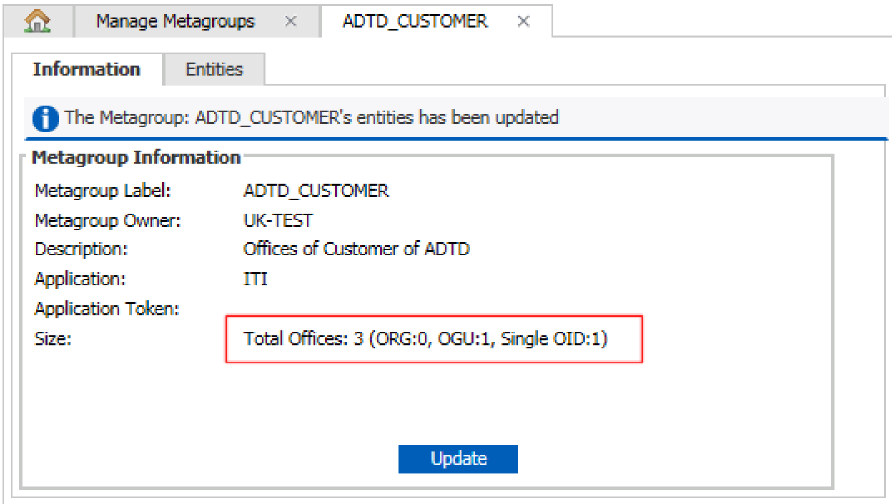
4. To add entities, such as offices or OGUs, to this metagroup, select the **Entities** tab, then click on **Add/Remove Entities**.

5. Select the entities you which to add into the metagroup and click on **Add** to move them to the panel on the right-hand side.



6. After you have added all entities, click on **Save**.

   The metagroup is created and the **Entities** tab displays key information such as the total number of Offices, and the number of ORGs, OGU and single Office IDs.



How to Update a Metagroup

1. In the **Home** tab, under **Organization Management**, click on **Manage Metagroups**.
2. In the **Metagroups** tab, select the metagroup you wish to update and click on **Manage Metagroup**.
3. In the **Update Metagroup Information** dialog box, you can change the description.
4. To modify the entities contained in the metagroup, select the **Entities** tab then click on **Add/Remove Entities**.
5. Select the entities you wish to add or remove from the metagroup and click on **Save**.

Adding Entities From Another Organisation to a Metagroup

What Are the Prerequisites?

It is possible to include entities from an organization other than your own in a metagroup. However in order to enable this:

- A partnership must exist between the two organizations. For more details see *Working With Partnerships* on page 111.
- The metagroup manager on the receiving ORG must be delegated certain ACLs from the delegating ORG. See *What ACLs Must be Delegated by the Delegating ORG?* below.
- The LSS administrator of the receiving ORG must have certain ACLs assigned. See *What Rights Must the LSS Administrator of the Receiving ORG Have?* below.

What ACLs Must be Delegated by the Delegating ORG?

The delegating ORG must delegate certain ACLs to the receiving organization's metagroup manager, depending on the desired scenario:

Scenario 1: To allow the receiving Organization to add any Offices from the delegating ORG, delegate the ACLs:

- (ORG) for LSS_MANAGE_METAGROUP_ENTITIES_**ORG**
- (ORG) for LSS_ORGANIZATION_VIEW

Scenario 2: To allow the receiving Organization to add any Offices of a given OGU from the delegating ORG, delegate the ACLs:

- (OGU) for LSS_MANAGE_ METAGROUP_ENTITIES_**OGU**
- (ORG) for LSS_ORGANIZATION_VIEW

Scenario 3: To allow the receiving Organization to add a specific Office from the delegating ORG, delegate the ACLs:

- (OFF) for LSS_MANAGE_ METAGROUP_ENTITIES_**OFF**
- (ORG) for LSS_ORGANIZATION_VIEW

Note: Depending on the entities the delegate wishes to allow, the right ACLs must first be created and delegated.

What Rights Must the LSS Administrator of the Receiving ORG Have?

To be able to assign delegated ACLs to a user, the Local Security Administrator of the receiving ORG must have the following role+ACL:

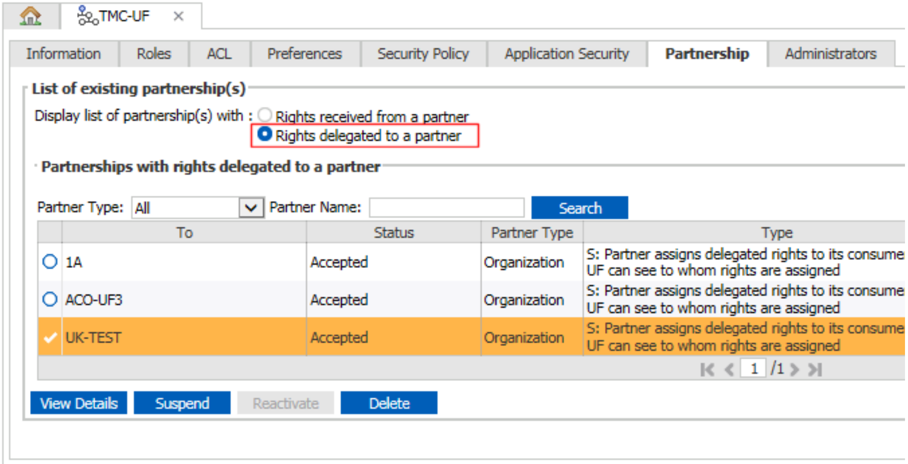
- <PTS name> for PTS_ALLOC

Example: <TMC-UF_TO_UK-TEST_S> for PTS_ALLOC

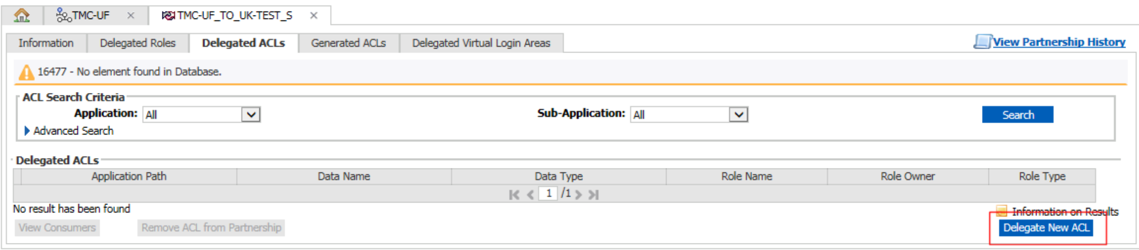
How to Add Entities From Another Organisation to a Metagroup

Delegating the ACLs on the Delegating Side

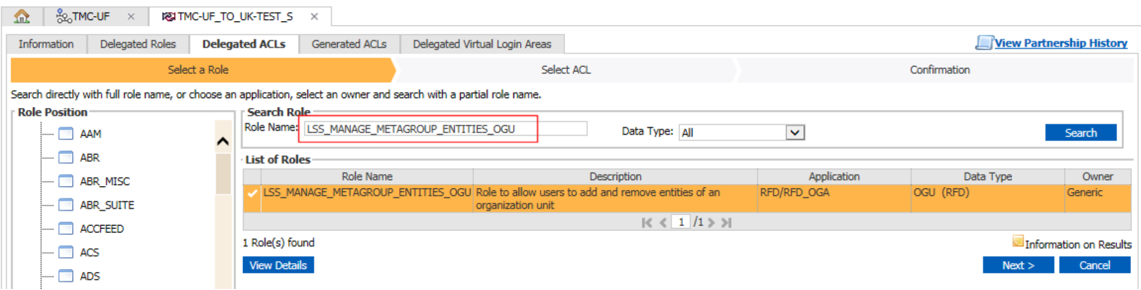
1. On the **Partnership** tab, display the list of partnerships with rights delegated to a partner.



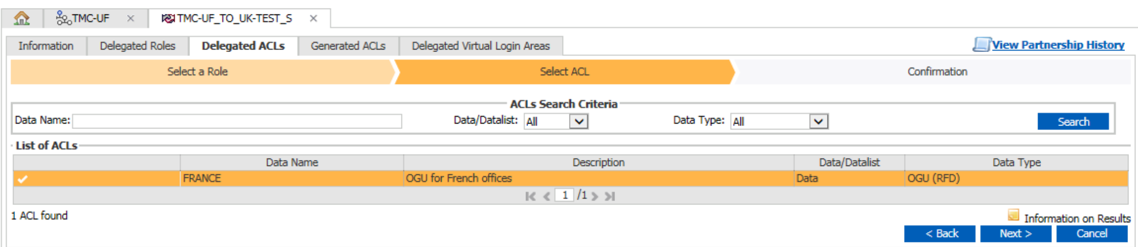
2. Select the partnership you wish to update and click on **View Details**.
3. Select the **Delegated ACLs** tab and click on **Delegate New ACL**.



4. In the **Select a Role** page, select the first role under RFD_OGA and click on **Next**.



5. In the **Select ACL** page, select the correct ACL and click on **Next**.



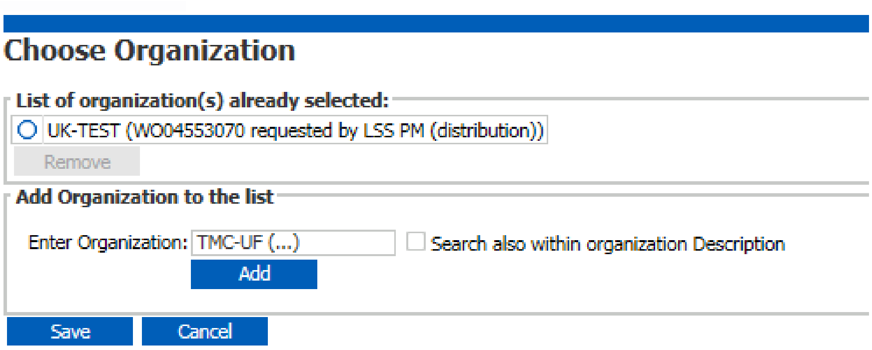
If no ACL is displayed, it means that the ACL was not created. Make sure the ACL is created first by going to **Application Management**.

6. In the **Confirmation** page, click on **Delegate**.

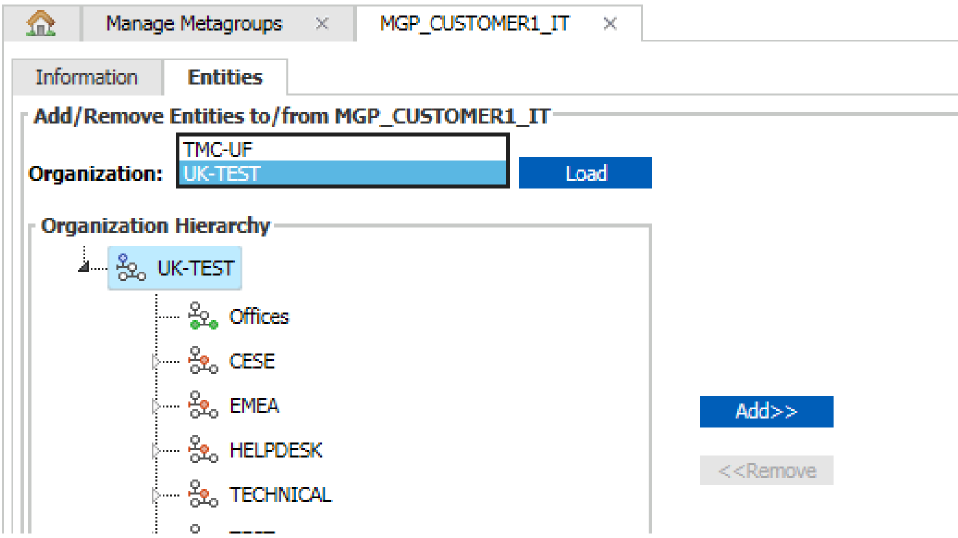
Perform Steps 3 to 6 for the second ACL.

Assigning the Delegated ACLs on the Receiving Side

1. On the ASM Home page, click on **Choose Organizations** in the top-left corner.



2. Type in the name of the Organization you need to view and click on **Add** then **Save**.
3. Click on **Manage Metagroups**.
4. Select the metagroup you wish to update, select the **Entities** tab and then click on **Add/Remove Entities**.
5. Select the ORG and click on **Load**.



The metagroup administrator for the receiving organization can now add the entities corresponding to the delegated ACL from the other organization. See *How to Update a Metagroup* on page 50.

For details on assigning metagroups to users, see the *Amadeus Local Security Management User Guide*.

Chapter 4
Managing Users

Working With User Authentication Settings

What Is the Purpose of the Information Tab?

The **Information** tab displays user profile attributes. It consists of one pane, **User's Profile**, divided into the following sections:

- **General Information**

  These fields contain personal information used to identify and communicate with the user. Mandatory fields are highlighted in yellow.

- **Security Information**

  Security settings at the user level provide user rights and the password policy that applies to the user. This allows you to manage the user's access to the system. Users inherit the security policy of the organizations to which they belong. The password policy is generally set at organization level.

Note: For convenience, this tab also contains some sign profile attributes. See *Defining Sign Profiles* on page 67.

What Is a Robot User?

A robot user is an automated process that accesses the system and carries out tasks on applications.

Robot users require rights to access the system, and must be identified as robots, to allow for special security handling. Robots have the following attributes:

- Robots cannot be automatically locked.
- Robots cannot be deleted.
- Robots do not have a password validity check.

What Is a Training-only User?

A training-only user is a user that can only access Amadeus Training Environment (SKL).

Training-only users have the following attributes:

- They are locked in the production environment.
- They are assigned a default password, which is reset each week. No activation email is sent, even if an email address is specified.

- They are not automatically deleted, although they are always inactive in the production environment.
- Only the profiles and rights saved in the production environment are kept after the weekly refresh of LSS.

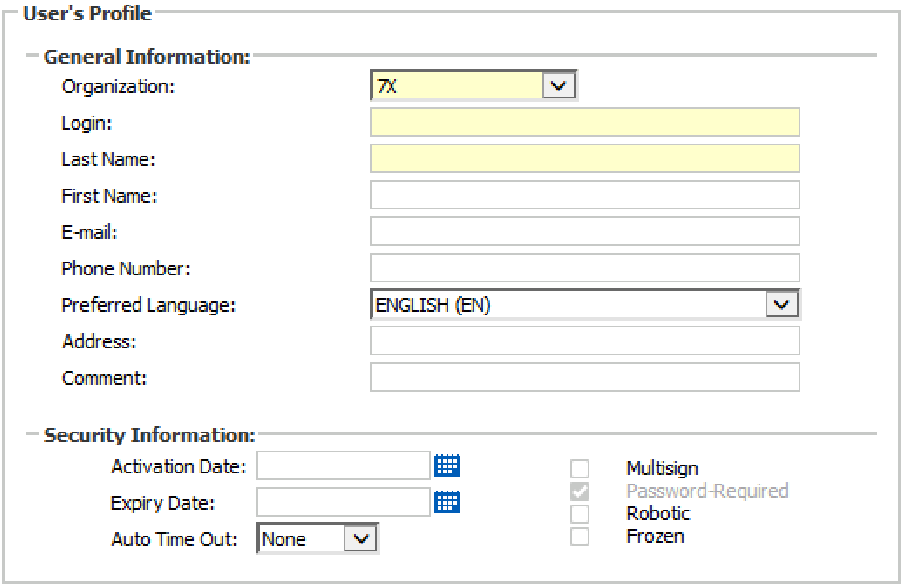
Managing User Accounts

How to Create a User

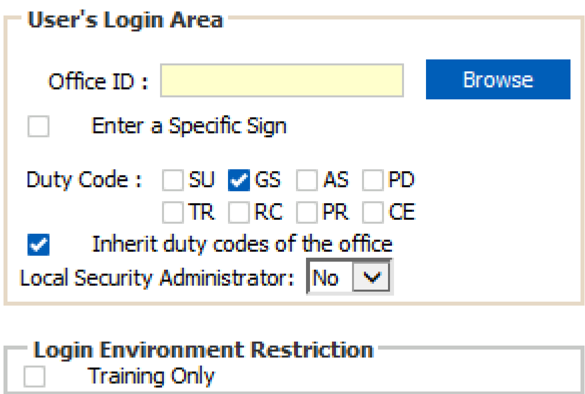
6. On the **Home** tab, click on **Create user**.

   The **Create User** tab opens.

7. In the **User's Profile** panel, complete the fields in the **General Information** and **Security Information** sections. For details on these fields, see *Explanation: Create User Tab Fields and Settings* on page 57.



8. In the **User's Login Area** panel, enter the **Office ID** to which the user belongs.



To search for an office ID:

a) Click on **Browse**.

b) In the **Office Mask** field, enter part of the office ID and enter the remaining characters as asterisks (wildcards), for example: `BKK6X0***`, then click on **Search**.

c) Select an office from the list displayed and click on **Use selected office**. The location of the office in the organization tree is displayed in the **Path** column.

For details on this and the other fields in this panel, see *Explanation: Create User Tab Fields and Settings* below.

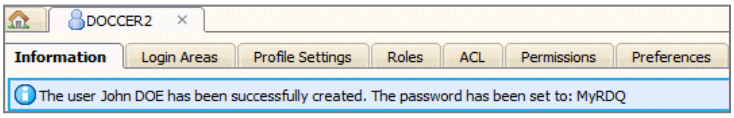
9. Optionally, select the **Training-only** check box in the **Login Environment Restriction** panel if you want to create a training-only user. See *What Is a Training-only User?* on page 55.

10. Click on **Create**.

Note: Once you have created a user, you can add additional login areas. See *How to Update a User* on page 61.

Explanation: Create User Tab Fields and Settings

User's Profile Panel: General Information Section

Field	Explanation
Login	The unique login of the user within the organization. If modified, it does not update the **User ID** field of the corresponding signs. This field is mandatory.
Last name	Updates to this attribute made directly in the Amadeus central system are **not** synchronised with LSS. This field is mandatory.
Email	Email address of the user. If you enter an email address, an activation email is automatically sent to the user, who can define their own password. You also give the user the possibility to reset their password at any time, without needing to contact their security administrator. If you do not enter an email address, the user is automatically created. A random password is generated and displayed in ASM.  You must communicate this password to the user. The user will be required to change the password at the first login attempt with the random password. **Note:** If you enter an email address after the user has been created, no email is automatically sent to this address.
Phone number	Phone number of the user. Updates to this attribute made directly in the Amadeus central system are not synchronised with LSS. The phone number must be entered in the international standard format: +<country code><local phone number>

Field	Explanation
Preferred language [LNG]	English (EN) by default.

User's Profile Panel: Security Information Section

Field	Explanation
Status (only after user creation)	Indicates whether a user ID is locked or unlocked. If it is locked, it cannot be used by an agent to log in. If the user is already logged into an application at the time of the locking of their account, they are not logged out of the system immediately. The lock takes effect the next time they attempt to log in.
Activation date	User authentication is refused before this date. To enter the date, click on the calendar icon, or enter it directly using the format *DD/MM/YYYY* (Day, Month, Year).
Expiry date	User authentication is refused after this date. If the field it is left blank, the user account remains active indefinitely. To enter the date, click on the calendar icon, or enter it directly using the format *DD/MM/YYYY*.
Auto Time Out [ATO]	Applies only to users of ARD Classic and Sell Connect. Represents the elapsed time (in minutes) after which an unused login area is either suspended or signed out. In the text field, enter a value greater than 0 minutes and lower than or equal to 1440 minutes. Then, select **Sign out** or **Suspend** from the drop-down list. **Security Policy Note:** The user will either be timed out by the **Auto time out** setting, or by the application time-out, whichever comes first. If **Credit card display** is selected: • **Auto Time Out** must be set to a maximum of 15 minutes. Or: • The application screensaver or desktop system lock must be set to a maximum of 15 minutes.
Multisign [MUL]	Not selected by default. If not selected: • **ARD Classic** users can sign into only one login area. • **Altéa DC CM** and **FM** users cannot sign in simultaneously on more than one workstation, thereby preventing credentials from being shared across multiple workstations. • **Sell Connect** users can only log in under the same Office ID.
Password-required [PWR]	Selected by default. Indicates whether a password is required. In PCI-compliant organizations, the **Password required** setting is defined at organization level. It cannot be changed for an individual user. If this setting has been selected and saved at user level, it cannot be removed.

Field	Explanation
Robotic	For web services and other application users. Identifies the user account as a robot user account, which is used for automated processes. When selected, the password policy of the user is modified so that the password validity check is bypassed. The user cannot be locked in case of multiple login attempts with the wrong password. The user is ignored in the auto-lock and auto-delete processes, which are activated in the **Security Policy** tab at organization level. See also *What Is a Robot User?* on page 55.
Frozen	Helps manage users on a temporary leave of absence, for example. When selected, the user cannot log in, as if their account has been locked. However, the user is ignored in the auto-lock and auto-delete processes, which are activated in the **Security Policy** tab at organization level. The user is not deleted from the application after the inactivity period. When the user returns to work, the security administrator needs to unfreeze the account to allow the user to log in again.

User's Login Area Panel

Field	Explanation
Office ID	Nine-character field. The format is XXXYYYZZZ where: • XXX = The city code. • YYY = The corporation code. • ZZZ = The office attribute. **Note:** A user can have only one sign per office. When updating a user, you can add more office IDs and signs if the user needs access to several offices. You can use the same sign across all offices. When a user has a access to several offices, one office can be defined as the default office. This office ID is taken by default when the user selects **Login and Organization** or **User ID and Organization** in the login window.

Field	Explanation
Enter a specific sign	Allows you to enter a specific sign. Cleared by default. In this case, the sign is automatically chosen by the system according to the environment: • In the production environment (PRD), the sign is randomly chosen in the range 0000 to 9000. If there is no available sign, the sign is chosen in the range 9001 to 9950. • For all other environments, the sign is randomly chosen in the range 9001 to 9950. If there is no available sign, the sign is chosen in the range 0000 to 9000. • If the office profile indicator UNI is set to **Y** in the Amadeus central system, then the chosen sign must contain initials that are different to all existing initials in that office. For example, the initials AA cannot be used if there is already a sign with those initials. In all cases, sign 4567 and signs from 9950 to 9999 are reserved by Amadeus and are not chosen automatically. For details on sign profiles, see *Defining Sign Profiles* on page 67. If this option is selected, the **Sign** field is displayed, and the options: • **Create new sign**. • **Associate existing sign**.
Sign	Displayed only if you select **Enter a specific sign**. Six-character field. The format is XXXXYY where: • XXXX = A number. • YY = Two letters. **Note:** It is possible to create users with the generic signs 0001xx or 0000xx (e.g., 0001AA or 0000LS). The organization must be PCI-DSS compliant to enable this.
Create new sign	Displayed only if you select **Enter a specific sign**. This is selected by default. Select if the sign does not already exist in the office. The new sign is created when a new login area is added.
Associate existing sign	Displayed only if you select **Enter a specific sign**. Select if the sign already exists in the office ID provided in the corresponding field. The sign is associated to the user when the new login area is added. If you choose this option, the **Duty code** check boxes are not displayed.

Login Area Details

Field	Explanation
Duty Code	By default the duty code **GS** is selected. Select at least one duty code: • **AS**: Agent sell (travel agents only). • **CE**: Customer engineer. • **GS**: General sales agent. • **PD**: Pre/post departure agent. • **PR**: Programmer. • **RC**: Space control. • **SU**: Supervisor. • **TR**: TTY reject agency.

Field	Explanation
Inherit duty codes of the office	Applies all duty codes set at office ID level to the sign. This option is not displayed if you have selected both **Enter a specific sign** and **Associate existing sign**.
Local security administrator [LSA]	This field has a specific security check. Only an administrator logged with a login area set to **Local security administrator** is allowed to select the **Local security administrator** attribute of another sign. This option is not displayed if you have selected both **Enter a specific sign** and **Associate existing sign**.

Login Environment Restrictions Panel

Field	Explanation
Training only	Allows you to create users who only have access to Amadeus Training Environment (SKL). These users have a locked status in the production environment (PRD). See also *What Is a Training-only User?* on page 55.

How to Create a User by Duplication

1. Select the existing user on which to base the duplication, using the **User Search** under the correct organization.
2. Click on **Duplicate**.
3. Complete the user's profile, security information and login areas.

   See *How to Create a User* on page 56.
4. Click on **Create**.

   Note: The new user is created with the same roles, ACLs and application preferences as the existing user.

How to Update a User

1. Select the user, using the **User Search** under the correct organization.
2. Click on **View details**.
3. Click on **Edit** on the **Information** tab.
4. In the **Update User Profile** pop-up window, update the user's general information and security information settings.
5. Click on **Save**.
6. If you want to update duty codes of one of the user's offices:
   a) Select the **Login Areas** tab.
   b) Select the office you want to update from the list displayed, and then click on **Edit**.
   c) Update the duty codes and options as appropriate, and then click on **Save**.
7. If you want to add another office to the user's login areas:

a) Select the **Login Areas** tab.

b) Click on **Add new login area**.

The **Add a Login Area** pop-up window is displayed.

c) Enter the office ID, and then select the appropriate duty codes and options.

d) Click on **Add**.

8. Optionally, if the user has a sign in several offices, define the default office:

a) Select the appropriate office from the list displayed in the **Login Areas** tab.

b) Click on **Set as default**.

Note: This office ID is taken by default when, in the login screen, the user selects **Login and organization** or **User ID and organization**.

How to Duplicate User Rights to an Existing User

1. Select the user, using the **User Search** under the correct organization.
2. Click on **View details**.
3. On the **Information** tab, click on **Duplicate** and select **Duplicate To an Existing User**.
4. In the **Select User** screen, search for the user(s) in the same organization to whom you want to copy the rights.

   If more than 300 users are found matching the search criteria, a message is displayed asking you to refine your search.
5. Select the user(s) to whom you want to copy the rights, and click on **Next**.

   You can select up to 15 users.
6. In the **Select Rights** page, select either **Duplicate All Rights**, or **Duplicate Rights of Selected Application**.

   If you want to duplicate rights from selected applications, search for the specific applications by typing in the **Application or Sub-Application Name** field, and click on **Add** to move them to the **Current Applications** box.
7. Click on **Next**.
8. In the **Confirmation** page, review the proposed changes, then click on **Duplicate** and select one of the options.

How to Duplicate User Rights From an Existing User

1. Select the user, using the **User Search** under the correct organization.
2. Click on **View details**.
3. On the **Information** tab, click on **Duplicate** and select **Duplicate From an Existing User**.
4. In the **Select User** screen, search for the user(s) in the same organization from whom you want to copy the rights.

   If more than 300 users are found matching the search criteria, a message is displayed asking you to refine your search.

5. Select the user(s) from whom you want to copy the rights, and click on **Next**.

   You can select up to 15 users.

6. In the **Select Rights** page, select either **Duplicate All Rights**, or **Duplicate Rights of Selected Application**.

   If you want to duplicate rights from selected applications, search for the specific applications by typing in the **Application or Sub-Application Name** field, and click on **Add** to move them to the **Current Applications** box.

7. Click on **Next**.

8. In the **Confirmation** page, review the proposed changes, then click on **Duplicate** and select one of the options.

How to Create or Update Multiple Users (Airlines)

1. Go to **Home > Data Management > Download Templates for Massive Actions**.

2. In the **List of Templates** pane, select the **Manage Users** template, and then click on **Download template**.

3. Enter the appropriate information in the **Manage Users** tab of this template.

4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.

5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.

6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, and then click on **Upload**.

   The users are created or updated, depending on your requests. The **List of Requests** pane indicates the status.

7. If there is an error, select the file, and then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.

8. Check the report sent to the email address indicated in the first line of the file.

How to Sign a User Out of All Their Active Sessions

Note: You need appropriate rights to perform this action. If necessary, you can sign yourself out.

1. Select the user, using the **User Search** under the correct organization.

2. In the **Information** tab, check that the **Currently signed-in** field of the **Security Information** panel indicates **Yes**.

   This means that the user is currently signed in to at least one Amadeus application in the same environment as you (for example, the production environment or SKL).

3. Click on **Sign-out user**.

   The user is immediately signed out of all their active sessions in the environment from which you have triggered the action. All login areas and all Amadeus applications in this defined environment are impacted.

Note: For security reasons, you should lock or delete the user just after having signed them out.

How to Lock a User Manually

1. Select the user, using the **User Search** under the correct organization.
2. Click on **Lock**.

   Note: If the user is already logged into an application at the time of the locking of their account, they are not logged out of the system immediately. The lock takes effect the next time they attempt to log in.

How to Delete a User Manually

1. Select the user, using the **User Search** under the correct organization.
2. Click on **Delete**.

   All roles, application preferences and login areas assigned to the user are deleted.

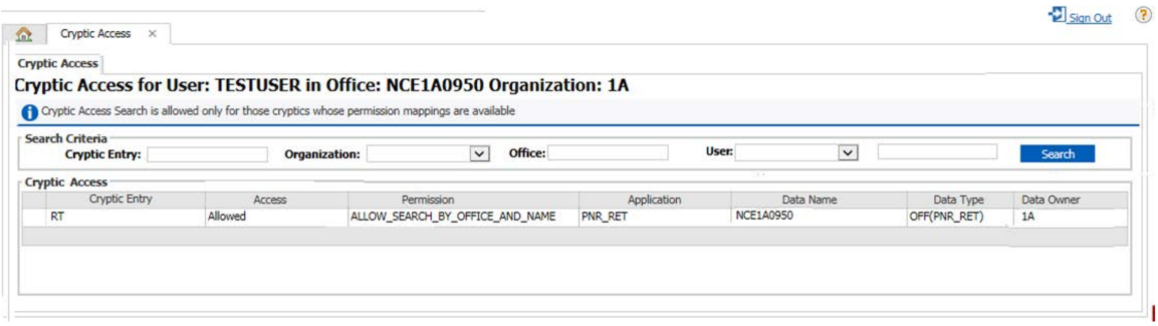
   Note: If the user you are deleting has rights across additional applications that you do not have permission to see, a warning message is displayed informing you of the number of applications in which the user has role contexts or preferences.

How to List the Cryptic Entries Allowed to a User

1. In the main panel click on **Cryptic Access** in the **Security Viewer** section.

   Note: This section is restricted to security administrators who have the right to view cryptic access.

   The **Cryptic Access** panel for that user is displayed.



2. Enter a cryptic command and click on **Search**.

How to Send Credentials or a Password Reset Link to a User

1. Select the user using the **User Search** under the correct organization.

2. Click on **View details**.
3. Click on **Notify user**.

   An email is sent to the user. The content of the email depends on the activation status of the user.

   - **User created, not yet activated:** The email contains the user's full credentials and a dedicated link for password activation. This link is valid for 48 hours.
   - **User already activated:** The email contains a permanent link to the LSS Password Changer tool.

Chapter 5

Defining Sign Profiles

What Are Profile Settings?

Profile settings allow you to control the agents' office environment. They correspond to agents' sign profile attributes in the Amadeus central system (ACS).

Currently, LSS contains only the sign attributes most frequently needed by security administrators. Most attributes are available in ASM from the **Profile Settings** tab, some from the **User Information** tab.

For explanations of the attributes, see:

- *Explanation: Create User Tab Fields and Settings* on page 57.

How Are Sign Profiles Synchronised with the Amadeus Central System?

All sign profile attributes can be managed in ACS, which is the master database. The sign attributes most frequently needed by security administrators can also be managed in ASM.

Except where noted in the tables, profile updates made in ASM or the Amadeus central system synchronise automatically. Normally, this happens immediately. However, it can take a few minutes if the user has hundreds of signs associated with their user ID.

Explanation: Sign Profile Settings

Super administrators (**MHDORM - DB End-User Maintenance**) have access to all attributes in the **Sign Profile** tab. Organization's administrators have access to a restricted number of attributes. Some attributes are airline- or ACO-specific, as noted in the key.

Key:

[NNN] Amadeus-cryptic sign attribute.

* Attribute available to airlines only.

Attribute available to ACOs only.

Table: Explanations of Sign Profile Attributes

Name	Explanation
General Duties	
Credit card display [CCD]	Select to allow the user to view credit card information in all the associated login areas. This option can be selected only if the **Password required** check box on the **Information** tab is selected. **Note:** If **Credit card display** is selected: • In the **User's Profile** pane of the user's **Information** tab, **Auto time out** must be set to a maximum of 15 minutes. Or: • The application user's screensaver or desktop system lock must be set to a maximum of 15 minutes.
Profile credit card [PCD]	Determines whether the credit card details are displayed or concealed in profiles.
Remote office [RMO]	Select to access the login areas in **Remote office** mode. If this field is not selected, the **Ticketing in remote office** field is also not selected.
Ticketing in remote office [RMT]	Select to allow the user to perform ticketing functions when in **Remote office** mode. This field is active only if **Remote office** is selected.
Security matrix name* [PST]	Used when there is security in place to access customer profiles. This field contains the security matrix name that allows the sign access to customer profiles.
Reference Data	
Display non-IATA locations [DNI]	Controls whether all locations, or only IATA official locations are displayed in the result of a DAN entry.
Customer Profile#	
Duties	
Profile reassociation [CPA]	Select to allow the users to maintain the **Traveller profile / company profile** association in their login areas.
Profile modification [CPM]	Select to allow the users to maintain **Customer profiles** in their **Login Areas**.
Profile renaming [CPN]	Select to allow the users to rename **Customer profiles** in their **Login areas**.
Display	

Name	Explanation
Air travel choice [CSA]	The display formats you can choose from are: • **Enriched neutral (E)**. Default. Neutral availability enriched with information on the policies and preferences in the profile. • **Preferential display (P)**. Policy-compliant availability only. • **Twin display (T)**. Displays policy-compliant and neutral availability in a split window.
Profile merge [PMG]	You can request a merged display of a company and a traveller profile. This can be either a merge of a traveller profile and its associated company, or a traveller with a guest company. A guest company is a company that the traveller is not associated to. When displaying a traveller profile merged with a guest company, the traveller profile can be unassociated, or associated to a different company. The advantage of the guest merged display is that you can specify any company profile name for a traveller without physically associating the traveller. Possible values are: • **No merged display (N)**. Default. The system does not merge traveller and company displays unless you specifically request it using the merge display entries. • **Merged display with company (C)**. By default, the system automatically merges the traveller profile with the associated company profile. • **Merged display with all associations (A)**. • **Guest merged display (G)**. When a guest company is included in the entry, the system merges the traveller profile with the profile of the guest company. • **Booking merged display (B)**. This is intended for use with organization profiles and **Amadeus Travel Preferences Manager**.

How to Update Sign Profile Settings

1. Create the user.

   See *How to Create a User* on page 56.
2. Select the **Profile Settings** tab.
3. Click on **Edit**, and then update the settings.
4. Click on **Save**.

Chapter 6
Accessing Virtual Offices

Note: This feature is only available for Distribution customers, and is not available for Airlines.

Managing Virtual Login Areas

What Is a Virtual Login Area?

The Virtual Login Area feature allows Distribution customers to streamline the authentication to Amadeus Selling Platform Connect by allowing agents to access multiple office IDs with same credentials.

Users can thereby access an office even if they do not have a sign within that Office ID; that is, no Login Area is defined for that Office ID.

A Virtual Login Area can represent an office, a selection of offices, an entire OGU or an entire organization. For example, a user with a Virtual Login Area at OGU level can log into all offices of this OGU.

When users logs into a virtual office, they have not only the rights assigned directly to their user ID, but also inherit any rights assigned to the virtual office or its parent (OGU or organization).

Virtual Login Areas can also be shared between organizations using partnerships. See *Delegating Virtual Login Areas* on page 72.

How to Add a New Virtual Login Area for a User

1. Search for a user. See *How to Search for a User* on page 16.
2. In the **User details** tab, click on the **Login Areas** tab.
3. In the **Virtual Login Area** panel, click on **Add New Virtual Login Area**.

   This button is disabled if the user does not have a default Login Area.
4. In the **Add New Virtual Login Area** screen, select an organization from the drop-down list.

   Note: By default your own organization is selected. You can select another organization only if it has been delegated through a partnership. See *Delegating Virtual Login Areas* on page 72.
5. Select the desired login areas, such as offices, from the left panel and move them to the right panel.

6. Click on **Save**.

   The Virtual Login Area is created.

Notes:

- When the first Virtual Login Area is created for a user, the VLA is associated with the Default Login Area of the user.
- If you are creating a Virtual Login Area with an organization or OGU, and the user already has some regular Login Areas with offices under it, then the regular Login Areas will still remain while Virtual Login Areas will also be created.
- You cannot create a Virtual Login Area with an office if the user already has a normal Login Area with that office, and vice-versa.
- If the Virtual Login Area represents an entire OGU or ORG, and if an Office ID is added to the OGU or ORG, this is automatically passed on to the Virtual Login Area. In other words, the setup is dynamic so you do not have to maintain the Virtual Login Areas. If the Virtual Login Area only contains a selection of Office IDs of a given OGU or ORG, then the addition of an Office ID in the LSS hierarchy is not passed on in the Virtual Login Areas.

How to Add or Remove Offices in an Existing Virtual Login Area

1. Search for a user. See *How to Search for a User* on page 16.
2. In the **User details** tab, click on the **Login Areas** tab.
3. In the **Virtual Login Area** panel, click on **Add View/Edit**.
4. In the **View/Edit Virtual Login Area** screen, make the desired changes to the login areas, such as adding or removing objects.
5. Click on **Save**.

How to Remove an Existing Virtual Login Area

1. Search for a user. See *How to Search for a User* on page 16.
2. In the **User details** tab, click on the **Login Areas** tab.
3. In the **Virtual Login Area** panel, click on **Remove Virtual Login Area**.
4. Click on **Confirm**.

Delegating Virtual Login Areas

You can enable users to log into office IDs outside their own organization, by creating Virtual Login Areas for them in another organization. This assumes there is a partnership (type S) with the other organization and the offices/organization units/organization are delegated through the partnership.

Conversely, you can choose to delegate part of your hierarchy to be used as Virtual Login Area, thereby allowing access to offices from outside your organization.

How to Delegate a Virtual Login Area

1. Access the **Partnership** tab. See *How to Display a Partnership* on page 112.

- Click on the **Delegated Virtual Login Areas** tab.

- Click on **Delegate New Virtual Login Area**.

  The hierarchy of Office IDs you are allowed to manage is displayed.

2. Select Office IDs, OGUs or the entire Organization to be delegated to the receiving Partner.

   Note: Partnerships can be set between two Organizations, between two OGUs from different Organizations, or between an Organization and an OGU.

3. Click on **Save**.

How to Remove a Virtual Login Area From a Partnership

- Access the **Partnership** tab. See *How to Display a Partnership* on page 112.
- Click on the **Delegated Virtual Login Areas** tab.
- If necessary, click on **View Consumers** to see which users are assigned to this area.
- Click on **Remove Virtual Login Area From Partnerships**.
- Click on **Confirm**.

Chapter 7

Defining Data for an Application

How Is Data Linked to an Application?

Access control is used to secure the use of applications and the information controlled by applications. To open rights to access application data, Amadeus application teams create data types and link them to permissions created for the application.

The data type is what links the ACLs through the data set and the roles through the permissions.

Note: Some applications define permissions that do not require any data type.

What Are Data Types?

All the secured access to data in an application is based on data types. Data types are created by application teams at application or sub-application level.

A data type has a predefined layout, such as an integer, a list, a range, a city or airport code.

You work with data types by creating data instances or datalists that are specific to the needs of your users.

What Are Data and Datalists?

A data instance is created to define which data values can be accessed in an application by the user of a role, through the ACL.

The data type is generic to an application.

Note: The global data types OFF, OGU and ORG are defined under the RFD application, but are available to all LSS applications for data management.

A data instance can either be specific to an organization and defined by the organization's security administrator, or it can be generic. Generic data (that is, data defined within a LSS application but available for all LSS organizations) can only be created and modified by Amadeus security administrators.

A data instance can be a single value, or a list of values called a datalist. You can group data instances of the same data type into datalists. You must create the individual data instances before you create the datalist.

Note: You cannot delete an individual data instance if it has been grouped in a datalist. You must first delete the datalist.

Example: Data Values (Airlines)

In **Amadeus Altéa Inventory**, a data type has been defined as **FLI** (**flight range**). The layout defined for the **FLI** data type is: **Integer or range of integers Separated by -**. The permission **View flight inventory** is associated to the data type **FLI**.

Some users need to view the inventory of flights within the range 1500 to 2000, while others only need to view the inventory for flight number 2500 or 2000. In this case, you define the following data values: 1500-2000, 2000 and 2500.

Application	Data Type	Data Instances
Altéa Inventory	Flight range (FLI)	`1500-2000`
		`2000`
		`2500`

Example: Datalist (Airlines)

In **Amadeus Altéa Departure Control Customer Management** (**CM**), a data type has been defined as **BPT** (**boarding point of the departing flight**). The layout for **BPT** is a three-character airport code that corresponds to the departure of the flight. For example, `LHR`, `JFK` or `CDG`.

You have users whose job is to manage catering at all London airports. You can define a datalist called **London airports** and include the boarding points **LHR**, **LGW** and **LCY**.

Application	Data Type	Datalist	Data Instances
CM	Boarding point (BPT)	London airports	LHR
			LGW
			LCY

Managing Data

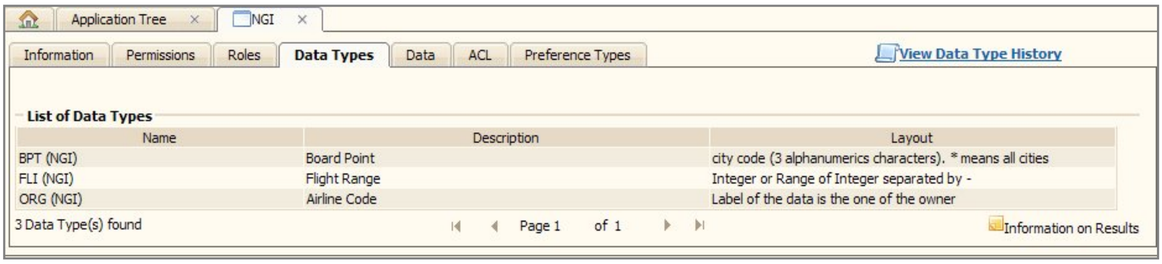
For a description of data, see *How Is Data Linked to an Application?* on page 75.

How to Display Data Types

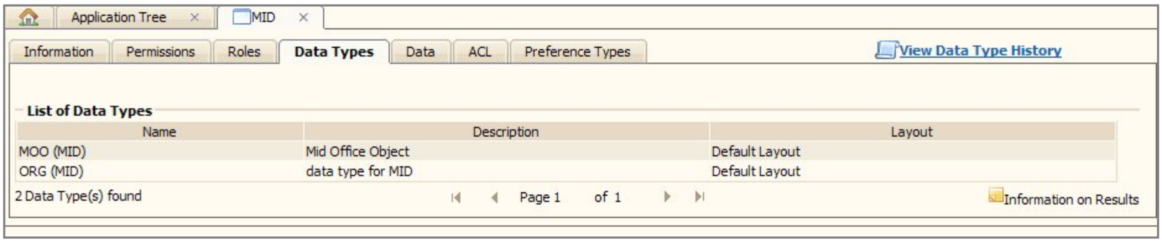
1. On the **Home** tab, click on **Manage Applications**.
2. Select the application or sub-application in the application tree, and then click on **Manage application**.
3. Select the **Data Types** tab.

Image: Data Types

Application: **Amadeus Altéa Inventory** (**NGI**)



Application: **Amadeus Integrated Mid Office** (**MID**)



How to Display Data and Datalists

1. On the **Home** tab, click on **Manage applications**.
2. Select the application or sub-application in the application tree, and then click on **Manage application**.
3. Select the **Data** tab.

How to Create Data

1. On the **Home** tab, click on **Manage applications**.
2. Select the application or sub-application in the application tree, and then click on **Manage application**.
3. Select the **Data** tab.
4. Click on **Create a new data**.
5. Enter the name of the data, following the convention of the selected data type.
6. Enter a description.
7. Click on **Create**.

How to Create a Datalist

1. On the **Home** tab, click on **Manage applications**.
2. Select the application or sub-application in the application tree, and then click on **Manage application**.
3. Click on the **Data** tab.
4. Click on **Create a new datalist**.

5. Enter the details of the datalist, such as name and description, and choose the data type.

   Note: Within an application, it is not possible to create two datalists with the same name and the same owner, even if they do not share the same data type. However, it is possible to create two or more datalists that have the same label and the same data type(s) but different owners.

6. Click on **Next**.
7. In the **Available Data** pane, select all the data that you want to add to the datalist, and then click on **Add** to move them to the **Current Data** pane.
8. Click on **Create**.

How to Create Multiple Data Instances and Datalists (Airlines)

Note: In a single operation, you can also create and assign roles, create, assign and delegate ACLs, and assign preferences. To do this, use the other tabs available in this template.

1. Go to **Home > Data Management > Download Templates for Massive Actions**.
2. In the **List of Templates** pane, select the **Manage Rights** template, and then click on **Download Template**.
3. Enter the appropriate information in the **Create DataSet** tab of this template.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.
6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, and then click on **Upload**.

   The new data and datalists are created. The **List of Requests** pane indicates the status.

7. If there is an error, select the file, and then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.

8. Check the report sent to the email address indicated in the first line of the file.

How to Modify Data or a Datalist

1. On the **Home** tab, click on **Manage applications**.
2. Select the application or sub-application in the application tree, and then click on **Manage application**.
3. Select the **Data** tab.
4. Select the data or datalist that you want to modify, and then click on **Update**.
5. Make the modifications, and then click on **Update**.

How to Delete Data or a Datalist

1. On the **Home** tab, click on **Manage applications**.
2. Select the application or sub-application in the application tree, and then click on **Manage application**.
3. Select the **Data** tab.
4. Select each line of data or datalist that you want to delete, and then click on **Delete**.

   A confirmation dialog box is displayed. If any of the selected data or datalists are used in an ACL, you cannot delete them. You must first remove them from the ACL definition.
5. Click on **Delete**.

Chapter 8
Defining Roles

What Are Permissions?

Permissions are defined for each application by Amadeus application teams. They are used to give users access rights to the functions of specific applications.

A permission is mapped to each function of an application and groups of permissions are known as unitary roles. The action-type attribute of the permission either allows or disallows the user access to a feature or entry of an application. Action types set at the user level override those set at higher organizational levels. For example, a specific user can be denied access to a function that the rest of their office can access.

Unitary roles can be combined, called composite roles, to provide or prevent access to a fuller range of functions.

In most cases, each permission is also linked to one of the data types defined for the application; this data type is also present in the related Access Control List (ACL). This further secures the application by making sure each user is also restricted to manipulating only certain data through this use of data types.

Note: In some cases, permissions can be created without being associated with a data type. Permissions without a data type work with roles without data types.

For detailed instructions on how to grant or forbid access to a function using a permission, see *How to Create a Unitary Role* on page 86.

How to Display Permissions

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, and then select the application for which you want to display the associated permissions.
3. Click on **Manage application**.
4. Select the **Permissions** tab.

   The name, description and data type of each permission is displayed.

   You can filter the list of permissions using the **Permission Search Criteria** fields.
5. To display the roles to which the permissions pertain, select a permission and click on **View permission usage**.
6. Do one of the following:

- Click on **Close** to return to the **Permissions** tab.

Or:

- Select a role, then click on **Manage role** to display more information about the role, and optionally add, remove or update the permissions granted with this role. See *How to Create a Unitary Role* on page 86.

What Are Roles?

Roles are the security counterpart of job functions. Roles are defined according to tasks that need to be completed. They are composed of the permissions that either allow or forbid a user to perform these tasks. Roles can also be composed of other roles, thus inheriting their permissions.

Roles can be assigned to any consumer. Users can work with all the roles they have been assigned directly, as well as the roles that have been assigned at the organization level.

Each role can be assigned to several users and each user can be attributed several roles.

Several types of roles are available.

For more information, see:

- *Types of Roles* below.
- *Examples of Roles* on page 84.
- *What Are Permissions?* on page 81.

Types of Roles

Unitary Role

Unitary roles are composed exclusively of permissions. They belong to a single organization and are associated with one application.

A unitary role can be defined in two ways:

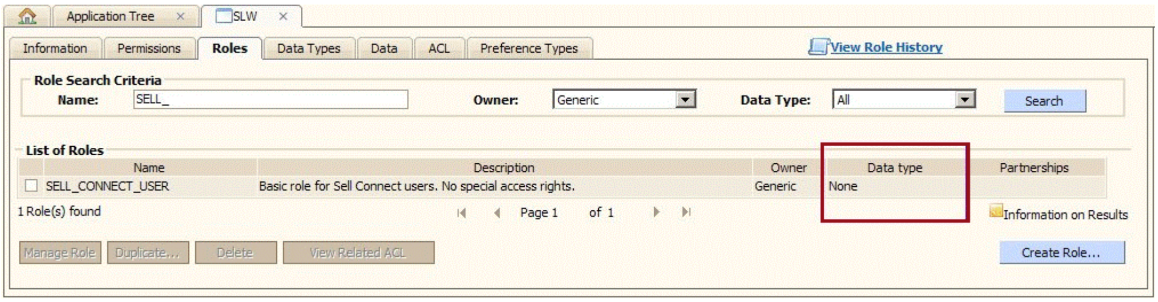
- With no restrictions. These roles are not associated with a data type. These are Boolean permissions that are used for functions requiring low-level security.

  These roles do not need to be associated with an ACL to grant rights.

- Restricted to a single data type. All the permissions included in the role must be secured by the same data type.

Note: Permissions can be linked to several data types. However, when they are used in a unitary role, they are activated by only one data type.

Example: Unitary Role with no Data Type (Selling Platform Connect)



Composite Role

A composite role is composed only of other roles, called sub-roles.

The following is true of sub-roles:

- Sub-roles can be any type of roles except global roles.
- Sub-roles in a composite role can be defined for an application as a generic role, or defined by you in an organization.
- Sub-roles can be linked to different data types, but there can be a maximum of one data type per sub-role.
- All of the sub-roles in a composite role must belong to the same organization and the same application as the composite role.

Global Role

A global role is a special type of composite role used to group sub-roles created for several applications or belonging to different organizations. A global role cannot include another global role.

Generic Role

Generic roles are standardised security profiles defined by Amadeus for each application. They are available to all customers of the application, regardless of the organization they belong to.

Generic roles can be either unitary roles or composite roles. However, a generic composite role can only be composed of generic roles.

Table: Characteristics of Each Type of Role

Role	Defined by	Composed of	Data Type	Application	Organization
Unitary	An organization	Permissions.	All permissions in the role must be of the same data type (or none).	For a single application.	For a single organization.
Composite	An organization	Sub-roles (belonging to the organization, or generic).	The permissions in the sub-roles can be for different data types.	For a single application.	For a single organization.

Role	Defined by	Composed of	Data Type	Application	Organization
Global	An organization	Sub-roles (belonging to the organization, or generic).	The sub-roles can be for different data types.	Can be for multiple applications.	For a single organization (but can include sub-roles of another organization delegated by partnership).
Generic	Amadeus	Permissions, if a unitary role.	All permissions in the role must be of the same data type (or none).	For a single application.	Independent from an organization.
		Sub-roles, if a composite role. All sub-roles must be generic roles.	The sub-roles can be for different data types.		

See also *Examples of Roles* below.

Examples of Roles

Unitary Role

Role	Permissions	Application	Organization
7X_NGI_SKD PUBLICATION FLI	MANAGE SCHEDULE CONTENT	NGI	7X
	PUBLISH FULL SCHEDULE		
	REDRESS FLIGHT		
	REPLAY INV UPDATE ERROR		
	SEND SCHEDULE RECAP		

Role	Permissions	Application	Organization
MID_ADMIN_USER	AIMO_MID_ACCESS MANAGE_BOF MANAGE_EXCHANGE_RATE MANAGE_FEE_RULE	MID	ACO-UF

Composite Role

Role	Sub-roles	Application	Organization
7X_NGI_INV_VIEW	7X_NGI_VIEW_FLIGHT	NGI	7X
	7X_NGI_VIEW_ORG		

Role	Sub-roles	Application	Organization
FULL_ITINERARY_PACK	DELIVER_EML_ONLY	ITI	ACO-UF

Role	Sub-roles	Application	Organization
	DELIVER_FAX_ONLY		
	DELIVER_PNT_ONLY		
	DELIVER_SMS_ONLY		
	DISPLAY_ONLY		

Global Role

Role	Sub-roles	Application	Organization
7X_HELPDESK_AGENT	7X_NGI_ADMIN_FLIGHT	NGI	7X
	7X_NGD_ADMIN_CM_ADVANCED	NGD	

Generic Role

Role	Sub-roles	Application	Organization
CHECK-IN AGENT	CHECK-IN_DISPLAY CHECK-IN_UPDATE	NGD	Any

Role	Permissions	Application	Organization
FULL_ITINERARY_PACK	DELIVER_EML DELIVER_FAX DELIVER_PNT DELIVER_SMS DISPLAY	ITI	Any

Displaying Roles

How to Display Unitary, Composite and Generic Roles

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, then select the application for which you want to display existing roles.
3. Click on **Manage application**.
4. Select the **Roles** tab.

   Use the **Owner** filter to display generic roles, or roles by organization. Use the **Data type** filter to display roles with a specific data type, or composite roles.
5. Select the role you want to display, and then click on **Manage role**.
6. Select the following tabs to display more detailed information about the role:

- **Sub-roles** or **Parent-roles**, to view the structure of the role. If you select a sub-role in the **Role structure** tree, the data displayed in the other tabs is displayed for this role only.
- **Permissions**, to view a list of permissions available in the role. Use the filter to display permissions for a specific application or of a specific data type.
- **Consumers**, to view which users, offices, organization units or organizations have been assigned this role.
- **Partnerships**. If **Delegated** is displayed in the **Partnership** column on the **Roles** tab, the **Partnership** tab lists all partnerships that benefit from this role.

  Or:
- Click on the **View Related ACL** tab to display the ACLs that have been created for this role.

How to Display Global Roles

1. On the **Home** tab, click on **Manage global roles**.
2. Select the role you want to display, and then click on **Manage role**.
3. Select the following tabs to display more detailed information about the role:
   - **Sub-roles**, to view the structure of the role. If you select a sub-role in the Role Structure tree, the data displayed in the other tabs is displayed for this role only.
   - **Permissions**, to view a list of permissions available in the role. Use the filter to display permissions for a specific application or of a specific data type.
   - **Consumers**, to view which consumers have been assigned this role.

   Or:
   - Click on the **View Related ACL** tab to display the ACLs that have been created for this role.

Managing Unitary and Composite Roles

For a definition of these types of roles, see *Types of Roles* on page 82.

Note: When you have created a role, you must then create the ACL for it. For more information, see *Defining Access Control Lists* on page 91.

How to Create a Unitary Role

Note: If you are an airline, you can also create multiple roles in a single operation. See *How to Create Multiple Roles (Airlines)* on page 87.

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, and then select the application for which you want to create a role.
3. Click on **Manage application**.

4. Select the **Roles** tab and click on **Create role**.
5. In the **Enter Role Details** window, enter the name and description of the role, and select the owning organization.
6. In the **Role Type** pane, select **Unitary** and select the data type that will be associated with this role.
7. Click on **Next**.

   The **Available Permissions** pane displays all permissions available for this application or sub-application, and the data type selected in the previous window.

   If you selected data type **None**, the system displays only the permissions that can be used with no data type.
8. For each permission that you want to include in the role, select that permission in the **Available Permissions** pane, then click on either:
   - **Allow** to enable users to use the associated function.

     Or:
   - **Disallow** to forbid users to use the associated function.
9. If you want to change the action type of a current permission, select this permission in the **Current Permissions** pane, then click on **Change action type**.
10. Click on **Create**.

How to Create a Composite Role

Note: If you are an airline, you can also create multiple roles in a single operation. See *How to Create Multiple Roles (Airlines)* below.

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, then select the application for which you want to create a role.
3. Click on **Manage application**.
4. Select the **Roles** tab, then click on **Create role**.
5. In the **Enter Role Details** window, enter the name and description of the role, and select the owning organization.
6. In the **Role Type** pane, select **Composite**, then click on **Next**.
7. In the **Add/Remove Roles** window, expand the tree of available unitary and composite roles for the application or sub-application.
8. Select a role in the **Available Roles** pane and click on **Add**, to move it to the **Current Roles** pane.
9. Repeat the previous step for each role that you want to include in the composite role.
10. Click on **Create**.

How to Create Multiple Roles (Airlines)

1. Go to **Home > Data Management > Download Templates for Massive Actions**.

2. In the **List of Templates** pane, select the **Manage Rights** template, then click on **Download template**.
3. Enter the appropriate information in the **Create Role** tab of this template.

   Note: If you want to assign these roles to consumers in the same operation, enter the appropriate information in the **Allocate Role** tab. See *How to Assign Multiple Roles (Airlines)* on page 97.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.
6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, then click on **Upload**.

   The new roles are imported. The **List of Requests** pane indicates the status.
7. If there is an error, select the file, then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.
8. Check the report sent to the email address indicated in the first line of the file.

Note: In a single operation, you can also create data and datalists, assign roles, create, assign and delegate ACLs, and assign preferences. To do this, use the other tabs available in this template.

How to Modify a Unitary or Composite Role

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, then select the application for which you want to create a role.
3. Click on **Manage application**.
4. Select the **Roles** tab.
5. Select the role you want to modify, and then click on **Manage role**.
   - To modify the name or description of the role, click on **Update** on the **Information** tab.
   - To add or remove sub-roles, select the **Sub-roles** tab, then click on **Add/remove sub-roles**.
   - To update, add or remove permissions, select the **Permissions** tab, then click on **Add/remove permissions**.

     See *How to Create a Unitary Role* on page 86.
6. Make the necessary changes, then click on **Save** or **Update** (depending on the tab in which you are working) to save the changes.

How to Delete a Unitary or Composite Role

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, and then select the application for which you want to create a role.
3. Click on **Manage application**.

4. Select the **Roles** tab.
5. Select the roles that you want to delete (up to 15), and then click on **Delete**.

   The system confirms which roles will be deleted, and which roles cannot be deleted.

   If a role has associated ACLs, you cannot delete it until you have deleted all of the ACLs. To do this, click on **View related ACL**, and use the **Delete** function in this tab.
6. Click on **Delete**.

   See also *Managing Global Roles* below.

Managing Global Roles

See also *Types of Roles* on page 82.

How to Create a Global Role

Note: If you are an airline, you can also create multiple roles in a single operation. See *How to Create Multiple Roles (Airlines)* on page 87.

1. On the **Home** tab, click on **Manage global roles**.
2. Click on **Create global role**.
3. In the **Enter Role Details** window, enter the name and description of the global role, and select the owning organization.
4. Click on **Next**.

   The **Add/Remove Roles** window allows you to select the unitary and composite roles that you want to add to the global role.
5. In the **Available Roles** pane, expand the application tree to display the existing roles for your organization.
6. Select a role and click on **Add**, to include it in the **Current Roles** pane.
7. When you have included all the relevant roles in the **Current Roles** pane, click on **Create**.

   When you have created the global role, you must then create the ACL for it.

   For more information, see *Defining Access Control Lists* on page 91.

How to Modify a Global Role

1. On the **Home** tab, click on **Manage global roles**.
2. Select the global role that you want to modify.
3. To modify the role name or description:
   a) Click on **Update** on the **Information** tab.
   b) Enter a new name and description, then click on **Update**.
4. To add or remove sub-roles, select the **Sub-roles** tab.
5. Click on **Add/remove sub-role**.

6. To add a role, expand the application tree to display existing roles, select the role you want and click on **Add** to include it in the **Current Roles** pane.
7. To remove a role, select it in the **Current Roles** pane, then click on **Remove**.
8. When you have added or removed all the relevant roles, and the **Current Roles** pane displays only the roles you want in the global role, click on **Save**.

How to Delete a Global Role

1. On the **Home** tab, click on **Manage global roles**.
2. Select the global role that you want to delete (up to 15 at the same time).
3. Click on **Delete**.

   The system confirms which roles will be deleted, and which roles cannot be deleted.

   If a role has associated ACLs, you cannot delete it until you have deleted all of the ACLs. To do this, click on **View related ACL**, and use the **Delete** function in this tab.
4. Click on **Delete**.

Chapter 9

Defining Access Control Lists

What Are ACLs?

Access Control Lists (ACLs) define the access rights granted to a role and its permissions, by activating the role for a specific data set only. ACLs are defined for a role and are used to create a link between the role and a data set. They determine the data values for which a permission is granted.

The link between permissions and data types is defined by Amadeus application teams.

Before you can create an ACL, you must have already created the data elements that you want to use for the data type, the application and the organization. You build an ACL by selecting a role and the data values or datalists you have created for the data type needed for the role.

When you create an ACL, the permissions in the role inherit the data restrictions from the ACLs associated to the role. The role and the data associated to the ACL must belong to the same organization (unless the role is a generic role).

You must create ACLs for each role that you want to assign to a role consumer, including any generic roles that you choose, provided this role is made of permissions associated to data types.

How Are ACLs Assigned?

ACLs can be assigned directly to a user, or to a node in the organization tree and inherited by the user. This is described in *Assigning Roles and Access Control Lists* on page 95.

Managing ACLs

Note: If a role contains sub-roles (composite, global or composite generic roles) with permissions associated to data types, it is recommended that you create the ACLs at the level of the master role.

See also *What Are ACLs?* on page 91

How to Create an ACL for a Role

Note: If you are an airline, you can also create multiple ACLs in a single operation. See *How to Create Multiple ACLs (Airlines)* on page 93.

For a Unitary, Composite or Generic Role

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, then select the application for which you want to create a role.
3. Click on **Manage application**.
4. Select the **ACL** tab.
5. Click on **Create ACL**.
6. Select the role for which you want to create the ACL, then click on **Next**.
7. In the **Available Data/Datalists** pane, expand the application tree and select the application, data type, owning organization and data or datalist.
8. Click on **Add**, to move your selection to the **ACL to Create** pane.
9. Repeat the previous two steps, as necessary.
10. Click on **Create**.

    The system displays a list of the ACLs that will be created, and any that cannot be created, with the relevant explanation.
11. Click on **Create**.

For a Global Role

1. On the **Home** tab, click on **Manage global roles**.
2. Select the **ACL** tab.
3. Click on **Create ACL**.
4. Select the role for which you want to create the ACL, then click on **Next**.
5. In the **Available Data/Datalists** pane, expand the application tree and select the application, data type, owning organization and data or datalist.
6. Click on **Add**, to move your selection to the **ACL to Create** pane.
7. Repeat the previous two steps, as necessary.
8. Click on **Create**.

    The system displays a list of the ACLs that will be created, and any that cannot be created, with the relevant explanation.
9. Click on **Create**.

How to Delete an ACL for a Role

For a Unitary, Composite or Generic Role

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, then select the application for which you want to delete a role.
3. Click on **Manage application**.
4. Select the **ACL** tab.
5. Select the ACLs you want to delete (up to 15), then click on **Delete**.

   The system displays a list of the ACLs that will be deleted, and any that cannot be deleted, with the relevant explanation.
6. Click on **Delete**.

For a Global Role

1. On the **Home** tab, click on **Manage global roles**.
2. Select the **ACL** tab.
3. Select the ACLs you want to delete (up to 15), then click on **Delete**.

   The system displays a list of the ACLs that will be deleted, and any that cannot be deleted, with the relevant explanation.
4. Click on **Delete**.

How to Create Multiple ACLs (Airlines)

Note: In a single operation, you can also create and assign roles, assign and delegate ACLs, and assign preferences. To do this, use the other tabs available in this template.

1. Go to **Home > Data Management > Download Templates for Massive Actions**.
2. In the **List of Templates** pane, select the **Manage Rights** template, then click on **Download Template**.
3. Enter the appropriate information in the Excel file template located in the **Create ACL** tab.

   Note: If you want to assign these ACLs at the same time, enter the appropriate information on the **Assign ACL** tab. See *How to Assign Multiple ACLs (Airlines)* on page 99.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.
6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, then click on **Upload**.

   The new ACLs are created. The **List of Requests** pane indicates the status.
7. If there is an error, select the file, then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.

8. Check the report sent to the email address indicated in the first line of the file.

Guidelines for ACLs for Composite and Global Roles

When assigning composite or global roles (roles composed of sub-roles), ensure that the user has the correct role and ACLs.

We recommend that you create the ACLs for composite or global roles at the level of the master role. An ACL at this level will activate all the sub-roles (of the same data type).

Example: Composite Role With Three Sub-roles (of Two Different Data Types) and Two ACLs

Composite Role	Sub-roles	Data Type	Data Set
7X_NGI_INV_ADMIN	7X_NGI_VIEW_FLIGHT	FLI	
	7X_NGI_UPDATE_FLIGHT	FLI	
	7X_NGI_MANAGE_OVERBOOKING	ORG	
ACLs	1-500 FOR 7X_NGI_INV_ADMIN	FLI	1-500
	7X FOR 7X_NGI_INV_ADMIN	ORG	7X

To benefit from *all* sub-roles in the role 7X_NGI_INV_ADMIN, a user must be assigned (either directly or through inheritance):

- The role 7X_NGI_INV_ADMIN.
- The role ACL 1-500 FOR 7X_NGI_INV_ADMIN (to activate the permissions in the sub-roles with the FLI data type for flights 1-500).
- The role ACL 7X FOR 7X_NGI_INV_ADMIN (to activate the permissions in the sub-role with the ORG data type for organization 7X).

However, if a user had been assigned the ACLs for the composite (master) role, and had been assigned the individual sub-roles (rather than the master composite role), the ACL at the master level would not activate the individual sub-roles. The user would not be able to work in the application.

Chapter 10

Assigning Roles and Access Control Lists

What Are the Different Methods of Assigning Roles and ACLs?

You can:

- Assign a role and the relevant ACLs to a role consumer in two separate steps.

  Do this if you want to assign the role and ACLs at different levels in the organization.

  See *How to Assign a Role* on page 96 and *How to Assign an ACL to a Consumer* on page 98.

- Assign an ACL and its associated role to a role consumer in one step.

  Do this to save time if you want to assign the role and ACLs at the same level. Start by assigning the ACL, and select the role to be assigned at the same time.

  See *How to Assign an ACL to a Consumer* on page 98.

- Assign multiple ACLs and multiple roles to one or multiple role consumers in a single operation.

  See *How to Assign Multiple Roles (Airlines)* on page 97 and *How to Assign Multiple ACLs (Airlines)* on page 99.

Assigning Roles

How to Display the Consumers of a Role

For Unitary, Composite or Generic Roles

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, then select the application to which the role belongs.
3. Click on **Manage application**.

4. Select the **Roles** tab.
5. Select the role you want, then click on **Manage role**.
6. Select the **Consumers** tabs.

   These tabs show which consumers have been assigned this role.

For Global Roles

1. On the **Home** tab, click on **Manage global roles**.
2. Select the role you want, then click on **Manage role**.
3. Select the **Consumers** tab.

   These tabs show you which consumers have been assigned this role.

How to Display the Roles Assigned to a Consumer

1. Select the consumer to which the role has been assigned, and then click on **View details**.
2. Select the **Roles** tab.

   Either a list of assigned roles is displayed, or, if there are too many roles to display, you must enter search criteria.
3. In the **Roles Search Criteria** pane, you must select the level where the roles have been assigned to the consumer.
4. Optionally, select the application.
5. Click on **Search**.
6. In the **Roles Search Criteria** pane, select to display roles assigned to the consumer, and then click on **Search**.
7. From the list of roles assigned, select a role and click on **View details**.
8. Click on **Return to list of roles**.

How to Assign a Role

1. Display the consumer to whom you want to assign a role.
2. Click on the **Roles** tab.
3. Click on **Assign new role**.
4. Do one of the following:
   - For a global role, expand the folder called **Global Roles** at the top of the application tree, and then move to step 6.

     Or:
   - Select the application to which the role belongs in the application tree, and then select your organization if the role was created by your organization; **Generic** if the role is a generic role, or **Delegated** if the role has been delegated to you through a partnership.

     The list of roles is displayed in the **List of Roles** pane. You can filter it using the **Search Role** pane.

     Or:

- Enter the full name of the role in the **Search Role** pane, then click on **Search**.

  If roles having the same name exist for separate applications, a pop-up window is displayed with the list of roles.

5. Select the role from the list.

   Note: Click on **View details** to display more information on the role.

6. Click on **Next**.
7. In the **Confirmation** pane, enter the dates that determine the role's validity period for the consumer.

   Note: The expiry date for the assignation of the role to the consumer is not compulsory, but is recommended to provide more controlled security access.

8. Select **Test only** if you want to use the role only in a test environment.
9. Click on **Assign**.

How to Assign Multiple Roles (Airlines)

1. Go to **Home > Data Management > Download Templates for Massive Actions**.
2. In the **List of Templates** pane, select the **Manage Rights** template, then click on **Download template**.
3. Enter the appropriate information in the **Allocate Role** tab of this template.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.
6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, then click on **Upload**.

   The roles are assigned to consumers. The **List of Requests** pane indicates the status.

7. If there is an error, select the file, then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.

8. Check the report sent to the email address indicated in the first line of the file.

How to Remove a Role

1. Display the consumer to which the role has been assigned.
2. Click on the **Roles** tab.
3. Select the role that you want to remove.
4. Click on **Remove role**.
5. Click on **Remove role**.

Assigning ACLs

How to Display the Consumers of an ACL

1. On the **Home** tab, click on **Manage applications**.
2. Expand the application tree or use the **Find** filter, then select the application to which the ACL belongs.
3. Click on **Manage application**.
4. Select the **ACL** tab.
5. Select an ACL, then click on **Display consumers**.

   These tabs show you which consumers have been assigned this ACL.

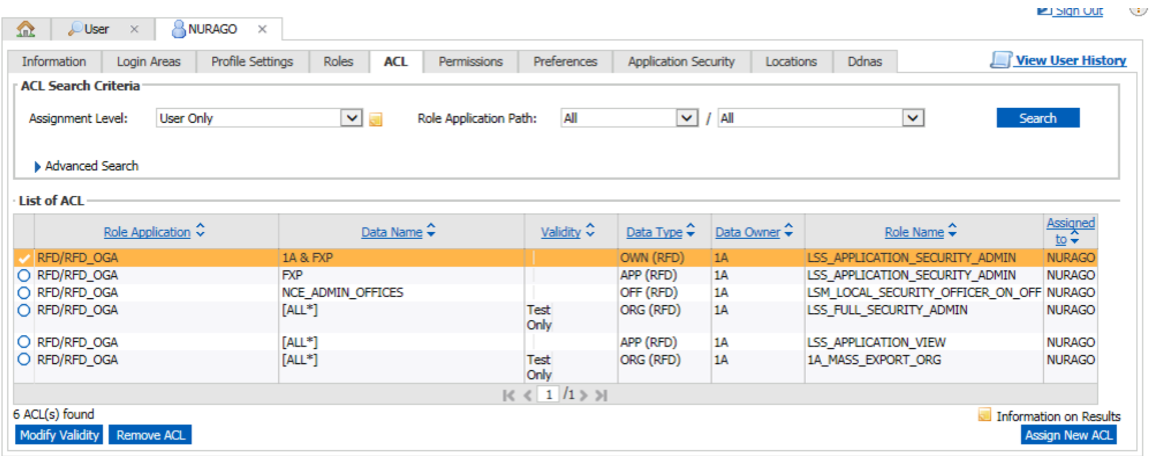
Note: If an ACL has been directly assigned to a role, these tabs do not list the consumers who benefit from the ACL that is directly assigned to a role.

How to Display the ACLs Assigned to a Consumer

1. Select the consumer to which the ACL has been assigned, and then click on **View details**.
2. Click on the **ACL** tab.

   Either a list of ACLs assigned is displayed, or, if there are too many ACLs to display, you must enter search criteria.

3. In the **ACL Search Criteria** pane, you must select the level where the ACLs have been assigned to the consumer.
4. Optionally, select the application or additional filters in the **Advanced Search** fields.
5. Click on **Search.**



6. To sort the displayed ACLs, click on the column headings.

How to Assign an ACL to a Consumer

a) Open the account of the consumer to whom you want to assign a role.

1. Click on the **ACL** tab, and then click on **Assign new ACL**.
2. For a global role:
   - Expand the folder called **Global Roles** at the top of the application tree, and then move to step 6.

     Or:
   - In the application tree, select the application and the role for which you want to assign an ACL.
3. Select the source of the role for which you need an ACL:
   - Your organization, if the role was created in your organization.
   - **Generic**, if the role is a generic role.
   - **Delegated**, if it is a role delegated to you through a partnership.

   The list of roles is displayed.
4. Select the role from the list.

   Note: Click on **View details** to display more information on the role.
5. Click on **Next**.
6. Select the ACL.

   Note: You can use the search fields to find an ACL in the list returned.
7. Click on **Next**.
8. Select whether you want to assign to the consumer the role related to the ACL at the same time as you assign the ACL.

   b) If **Yes**:
   - Set the validity period for the role.

   Note: The expiry date for the assignation of the role to the assignee is not compulsory, but is recommended to provide more controlled security access.
   - Select **Test only** if you want to use the role only in a test environment.

   c) If **No**, move to the next step.
   - Select **Test only** if you want to use the role only in a test environment.
9. Click on **Assign**.

How to Assign Multiple ACLs (Airlines)

1. Go to **Home > Data Management > Download Templates for Massive Actions**.
2. In the **List of Templates** pane, select the **Manage Rights** template, then click on **Download template**.
3. Enter the appropriate information in the Excel file template in the **Assign ACL** tab.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.

6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, then click on **Upload**.

   The ACLs are assigned to consumers. The **List of Requests** pane indicates the status.

7. If there is an error, select the file, then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.

8. Check the report sent to the email address indicated in the first line of the file.

How to Remove an ACL from a Consumer

1. Display the consumer to which the ACL has been assigned.
2. Click on the **ACL** tab.
3. Select the ACL that you want to remove.
4. Click on **Remove ACL**.
5. Click on **Remove ACL**.

Chapter 11

Customising Applications Using Preferences

What Are Preferences?

Preferences are attributes of an application. They are defined by the Amadeus application team, and you can customise them. Preferences are not used for security. Rather, they allow you to influence how the information from the application is presented, and how the application behaves.

The *preference type* is the generic attribute that is created at application level and set with a default value. The *preference* is defined by giving a specific value to a preference type for an organization, organization unit, office or user. When you are defining a preference for an application, you can either keep the default value set by the Amadeus application team, or choose another value.

If a preference is set for several levels of the hierarchy, the preference at the lowest level is applied.

Example: Preference (Airlines)

In **Altéa Departure Control Customer Management (CM)**, the Amadeus application administrator has created the preference type DEF_APPL to specify the default module an agent will access when logging in. The possible values are: BAG, BRD, CRY, CUS, DEV, FLT, LOG, MSG and STM.

For this preference type, the Amadeus application administrator has set the default value to Blank.

To use this preference type across the whole organization, you, as security administrator, set the preference type DEF_APPL to your organization (that is, the root of your organization tree). You then override the default value and replace it with the value required by the agents of your organization, for example, CUS. As a result, all users in your organization directly access the **Customer** module when first logging in to the application.

Example: Preference (ACOs)

The default currency in **Amadeus Integrated Mid Office Solution**.

Assigning Preferences

See also *What Are Preferences?* on page 101.

How to Display Preference Types and Preference Values

1. Select the application or sub-application in the application tree, and click on **Manage Application**.
2. Select the **Preference Types** tab.
3. Select the preference type for which you require more information, then click on **View preference type values**.

   A list of defined preference values is displayed, with a default value if appropriate.
4. To view the consumers of a preference type, select it and click on **View consumers**.

   The tabs indicate how many consumers of each type have this preference assigned to them.
5. Click on **Close** to return to the **View Preferences** tab.

How to Display the Consumers of a Preference

1. Select the application or sub-application in the application tree, and then click on **Manage application**.
2. Select the **Preference Types** tab.
3. Select the preference type for which you require more information, and then click on **View preference type values**.

   A list of defined preference values is displayed, with a default value if appropriate.
4. To view the consumers of a preference value, select it and click on **View consumers**.

   The tabs indicate how many consumers of each type have this preference type and value assigned to them.
5. Click on **Close**.

How to Assign a Preference

Note: A preference set at one level of the organization tree overrides all the inherited preferences set for the same preferences type.

1. Display the consumer (user, office, organization unit or organization) to which you want to assign a preference.
2. Select the **Preferences** tab.
3. Click on **Assign preference**.
4. Find the application to which the preference is related in the application tree.
5. Select the preference from the list.
6. Click on **Assign preference**.

7. In the pop-up dialog box, enter a value for the preference.

   The value you enter must comply with the value type, for example text string or range of integers.

8. Click on **Save**.

How to Assign Multiple Preferences (Airlines)

1. Go to **Home > Data Management > Download Templates for Massive Actions**.
2. In the **List of Templates** pane, select the **Manage Rights** template, then click on **Download template**.
3. Enter the appropriate information in the Excel file template in the **Allocate Preferences** tab.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.
6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, then click on **Upload**.

   The preferences are assigned to consumers. The **List of Requests** pane indicates the status.

7. If there is an error, select the file, then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.

8. Check the report sent to the email address indicated in the first line of the file.

How to Remove a Preference

1. Display the consumer (user, office, organization unit or organization) whose preference you want to remove.
2. Select the **Preferences** tab.
3. Select the preference you want to remove.
4. Click on **Remove preference**.
5. Click on **Remove preference**.

Chapter 12

Working With Security Badges

What is a Security Badge?

A security badge is a mechanism that allows you to group roles, ACLs and preferences into a single object that you can then assign to different consumers. Once security badges are created in ASM, local security administrators (LSAs) can use LSM to assign them to users in their organization. For details see the *Amadeus Local Security Management User Guide*.

Note: In this release of ASM, the following limitations apply:

- Preferences cannot be added to badges.
- It is not currently possible to assign badges to consumers in ASM. Only a local security administrator using LSM can currently assign a badge to a user.
- If changes are made to a badge that has already been assigned to users, the changes are not updated to the badge's existing consumers. The badge must be reassigned.

These features will become available in a subsequent release of ASM.

What Is an Adaptive ACL?

In many cases, ACLs are required for a role to work properly, and so must be created before the role can be assigned to a user. This creates extra work for an organization administrator, and can be very time consuming, especially for Office ID ACLs.

To facilitate the creation and assignation of roles requiring an ACL on a precise Office ID, ASM introduces the concept of an Adaptive ACL.

Whenever an LSM user assigns a Badge containing an Adaptive ACL, the ACL is automatically created and assigned to the user. The assignment process allows the LSM user to choose up to 10 Offices.

Note: Adaptive ACLs are only available where the required datatype is Office ID.

How to Create a Badge

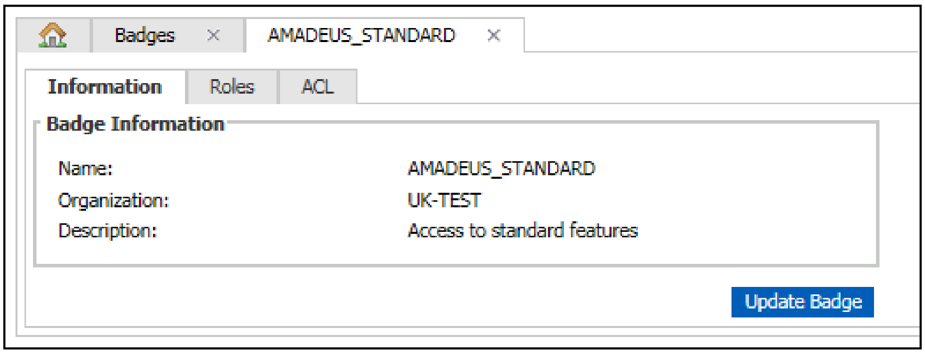
1. From the **Home** page, under **Application Management**, click on **Manage Security Badges**.

   The **Badges** tab opens, displaying a list of existing badges.

2. Click on **Create Badge**.

Alternatively, to duplicate an existing badge, click on **Duplicate Badge**.

3. In the **Create Badge** dialog box, enter a name, select your organization, and enter an optional description and click on **Create**.
4. The details of the badge are displayed in a new tab.



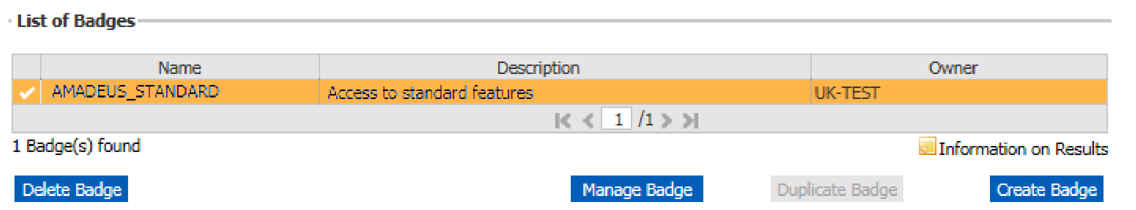
Note: The description will be visible in LSM. You can update the description at any time by clicking on **Update Badge**.

You can now add a role to the badge.

How to Add a Role to a Badge

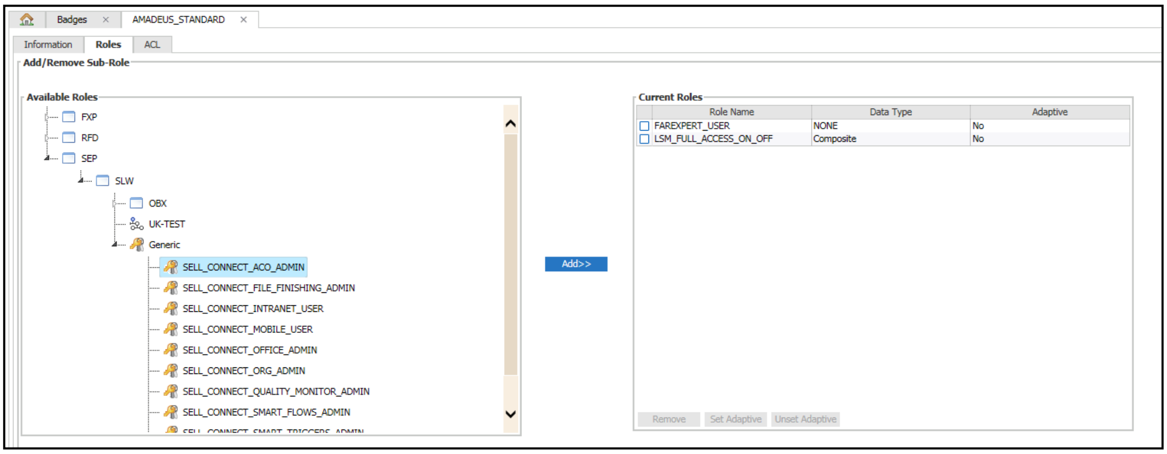
1. From the **Home** page, under **Application Management**, click on **Manage Security Badges**.

   The **Badges** tab opens, displaying a list of existing badges.



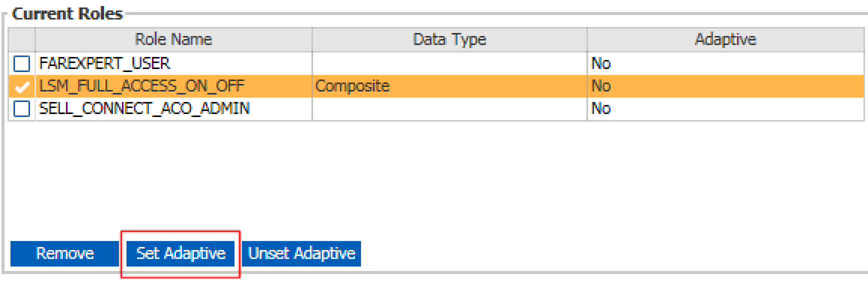
2. Select a badge and click on **Manage Badge**.
3. Click on the **Roles** tab.

   A list of roles contained in this badge is displayed.
4. Click on **Add New Role**.
5. Search for the specific roles you wish to add and click on **Add** to move them to the right-hand panel.



6. Specify the roles you wish to mark as adaptive by selecting them and clicking on **Set Adaptive**.

Note: Adaptive ACLs only work when data type is OFF (Office ID). Make sure you review the corresponding LSS catalogues to be sure which data type is required for each role you insert in a given badge.



7. Click on **Save** to save your changes.

If you added any roles that require ACLs that are not adaptive, you must add the ACLs to the badge explicitly. See *How to Add an ACL to a Badge* below.

How to Add an ACL to a Badge

Note: This step only applies to roles that require an ACL that is not adaptive.

1. From the **Home** page, under **Application Management**, click on **Manage Security Badges**.

   The **Badges** tab opens, displaying a list of existing badges.

2. Select a badge and click on **Manage Badge**.
3. Click on the **ACL** tab.

   A list of ACLs contained in this badge is displayed.

4. Click on **Add new ACL**.
5. Search for a role by entering the full role name and clicking on **Search**, or by selecting an application and owner in the tree then entering a partial role name.

   Note: Look for roles that require data type ORG or OGU.

   For roles requiring multiple ACLs including OFF + ORG, make sure you flag the role as adaptive and add the ACL on ORG for that role.

6. Select the role in the **List of Roles** pane and click on **Next**.
7. Choose the ACL and click on **Next**.
8. In the **Confirmation** page, click on **Assign**.

How to Add a Preference to a Badge

1. From the **Home** page, under **Application Management**, click on **Manage Security Badges**.

   The **Badges** tab opens, displaying a list of existing badges.
2. Select a badge and click on **Manage Badge**.
3. Click on the **Preferences** tab.

   A list of Preferences contained in this badge is displayed.
4. Click on **Add Preferences**.
5. Find the application to which the preference is related in the application tree.
6. Select the preference from the list.
7. Click on **Add preference**.
8. In the pop-up dialog box, enter a value for the preference.

   The value you enter must comply with the value type, for example text string or range of integers.
9. Click on **Save**.

How to Delete a Badge

1. Search for the badge you wish to delete.
2. Click on **Delete Badge**.
3. Confirm or cancel the deletion.

   The association between the badge and its contents (roles, ACLs, and preferences) is removed. Any ACLs associated with the badge label and the data are removed.

Granting Badge Rights to LSM Users

What Roles and ACLs Does the LSM User Require?

Depending on the scenario you wish to achieve, you can grant LSM users the rights to display or assign:

- All badges created by your organization.
- A list of badges available to a specific customer.
- A specific badge.

In this section:

- ORG is the organization in which the Office ID is placed.
- OFF is the Office ID.

- BDG is the name of a badge.
- USR is the name of a user.

Prerequisites

To be able to assign badges to all users of a given Office ID, the LSM user must have the following role:

- LSM_FULL_ACCESS_ON_OFF

and the related ACLs:

- (ORG) for LSM_FULL_ACCESS_ON_OFF
- (OFF) for LSM_FULL_ACCESS_ON_OFF

Displaying badges

To display badges, the LSM user must have the following role:

- LSM_BADGE_VIEW

The ACL for this role can be set in either of the following ways:

- To display all badges in the organization, the ACL should be on ORG.
- To display a specific badge, the ACL should be on BDG.

Displaying and assigning badges

To display and assign badges, the LSM user must have the following role:

- LSM_BADGE_ASSIGN

This role needs two ACLs, which can each be set in two ways:

- ACL1 determines which badges are visible:
  - To display all badges in the organization, the ACL should be on ORG.
  - To display a specific badge, the ACL should be on BDG.
- ACL2 determines on which consumers the LSM user can assign a badge:
  - To assign a badge to all users of a given Office ID, the ACL should be on OFF.
  - To assign a badge to a specific users, the ACL should be on USR.

Examples

Scenario 1

Allow LSM user to	Assign the user these rights
Display all badges available in an organization.	(ORG) for LSM_BADGE_VIEW

Scenario 2

Allow LSM user to	Assign the user these rights
Display a single badge.	(BDG) for LSM_BADGE_VIEW

Scenario 3

Allow LSM user to	Assign the user these rights
Display all badges available in an organization.	(ORG) for LSM_BADGE_ASSIGNMENT
Assign any visible badge to all users in a given Office ID.	(OFF) for LSM_BADGE_ASSIGNMENT

Scenario 4

Allow LSM user to	Assign the user these rights
Display a specific badge.	(BDG) for LSM_BADGE_ASSIGNMENT
Assign any visible badge to all users in a given Office ID.	(OFF) for LSM_BADGE_ASSIGNMENT

Scenario 5

Allow LSM user to	Assign the user these rights
Display a list of all badges.	(BDG) for LSM_BADGE_ASSIGNMENT (Add 1 for each badge you wish to make visible or 1 Datalist containing all badges to be shown)
Assign any visible badge to all users in a given Office ID.	(OFF) for LSM_BADGE_ASSIGNMENT

Note: You can give rights on several Office IDs either by assigning several ACLs or by creating a Datalist of Offices.

Note: If an LSM user has rights on several Office IDs, and can assign a badge containing an adaptive ACL, he will be prompted to add more Offices for which the badge can apply. The Office IDs available are based on the Office listed as per the role LSM_FULL_ACCESS_ON_OFF.

Chapter 13

Working With Partnerships

What Are Partnerships?

What Is the Purpose of a Partnership?

By default, you can access only your own business information. However, if you need to share data with another organization, partnerships allow you to delegate access rights in a controlled environment to that organization.

For example:

- An airline that delegates its customer management activities to a ground handling company.
- A global travel management company that delegates limited access rights to one of its national organization units.

Partnerships between two organizations are created and maintained by the organizations themselves without any intervention from Amadeus.

Between Which Organisation Levels Do Partnerships Operate?

You can delegate access rights as follows:

- From Organization to Organization.
- From Organization to Organization Unit.
- From Organization Unit to Organization Unit (for ACOs only).

In relation to partnerships, unless otherwise mentioned, the terms organization and organization unit and are used interchangeably.

What Organisations Are in a Partnership?

The organizations linked by a partnership are:

- A delegating organization that:
  - Creates the partnership.
  - Delegates the roles and ACLs to the receiving organization for use with their data.
  - Keeps ownership of these roles and ACLs.
- A receiving organization that validates the partnership.

What Is Partnership Type?

The partnership type is defined when the partnership is created. It determines whether:

- The delegating or receiving organization assigns access rights to consumers.
- The delegating organization is allowed to see which consumers have been assigned the delegated roles.

Table: Partnership Types

Partnership Type	Who Assigns Access Rights?	Can the Delegating Organization Display the Consumers of Delegated Roles and ACLs?
D	Delegating organization	Yes
R	Receiving organization	No
S	Receiving organization	Yes

Types of Partnership Status

Partnership status is displayed in the **Information** tab for each partnership.

Table: Types of Partnership Status

Status	Explanation
Pending validation	The partnership has been created by the delegating organization, but the receiving organization has not accepted, or has refused, the partnership.
Accepted	The partnership has been accepted by the receiving organization. The partnership is active and can be used to delegate rights and share data.
Suspended	The partnership has been suspended. The partnership can no longer be used for delegating rights between the two partner organizations, but the partnership has not been deleted from the system. All assignments of delegated roles and ACLs to consumers in the receiving organization are removed, but the roles and ACLs remain delegated; they can be reassigned if the partnership is reactivated.
Refused	A partnership has been refused by the receiving organization.

How to Display a Partnership

1. On the **Home** tab, select an organization, and then click on **Manage Organization**.
2. Do either of the following:
   - Select the **Partnership** tab to display partnerships at organization (ORG) level.

     Or:

a) Select an organization unit (OGU) from the **Organization tree** list, then click on **View Details** > **Partnership** to display partnerships at OGU level.

b) In the **List of existing partnership(s)** pane, select the **Rights received from a partner** check box or the **Rights delegated to a partner** check box.

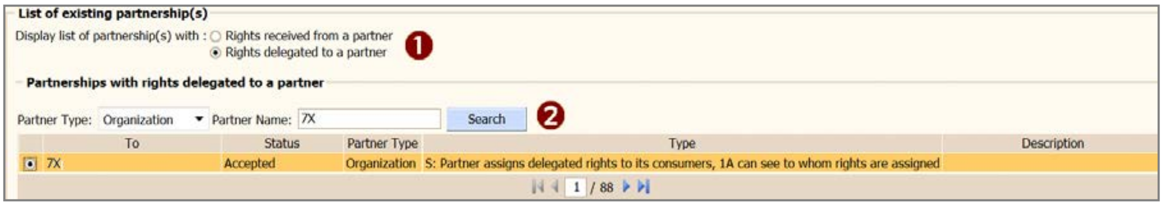
c) To limit the list of results, select the **Partner type** and, optionally, enter the **Partner name**, then click on **Search**.

3. Select the partnership you want to display from the list, then click on **View details**.

   The **Information** tab provides the **Partnership details** and **Partnership status** panes. The other tabs describe the delegated roles, delegated ACLs generated ACLs, and delegated virtual login areas.

   For more information, see *What Are Partnerships?* on page 111.

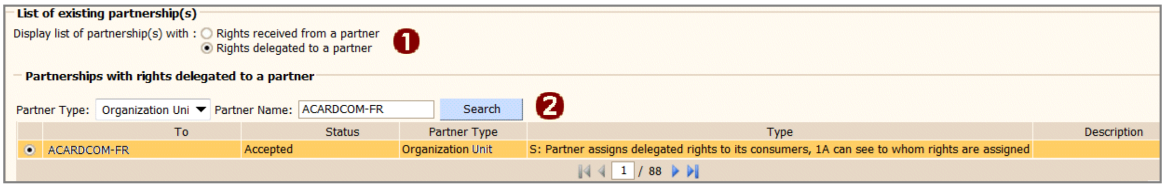
Example: Displaying a Partnership (Airlines)



❶ Ensure that you display the partnership in the appropriate list, depending on whether you have delegated or received access rights.

❷ If you have many partnerships, use the filter to search by organization.

Example: Displaying a Partnership (ACOs)



❶ Ensure that you display the partnership in the appropriate list, depending on whether you have delegated or received access rights.

❷ If you have many partnerships, use the filter to search by organization or organization unit.

Workflow: Setting Up a Partnership

Step	Done By	Task
1	Delegating organization	Create the partnership. See *How to Create a Partnership* on page 114.

Step	Done By	Task
2	Receiving organization	Accept the partnership. See *How to Accept a Partnership* on page 120.
3	Partnership type D: Delegating organization	Assign the auto-generated ACLs to the security administrator in your organization. See *How to Assign the Auto-generated ACLs and Generic Roles for Partnership Management (Delegating Organisation)* on page 116.
	Partnership types R and S: Receiving organization	Assign the auto-generated ACLs to the security administrator in your organization. See *How to Assign the Auto-generated ACLs and Generic Roles for Partnership Management (Receiving Organisation)* on page 121.
4	Delegating organization	Delegate the relevant roles and ACLs to the receiving organization. **Note:** The roles and ACLs must have already been created in the normal way. See *How to Delegate an ACL and Its Related Role to the Receiving Organisation* on page 117.
5	Partnership type D: Delegating organization	Assign the delegated roles and ACLs to the consumers in the receiving organization. See *How to Assign Delegated ACLs and Related Roles (Delegating Organisation)* on page 119.
	Partnership types R and S: Receiving organization	Assign the delegated roles and ACLs to the consumers in your organization. See *How to Assign Delegated ACLs and Related Roles to Consumers (Receiving Organisation)* on page 122.

Tasks for the Delegating Organisation

How to Create a Partnership

Note: ACOs can create partnerships at organization unit level on the delegating organization side.

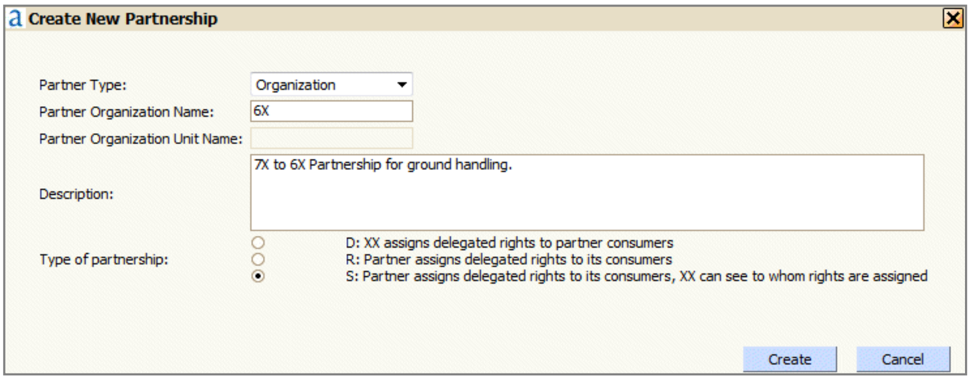
1. On the **Home** tab, select the delegating organization, and then click on **Manage Organization**.
2. If applicable, select an organization unit, then click on **View details**.
3. Select the **Partnerships** tab.
4. Click on **Create a new partnership**.
5. From the **Partner type** drop-down list, select whether the rights will be delegated to an **Organization** or **Organization unit**.

   See *What Are Partnerships?* on page 111.
6. In the **Partner organization name** field, enter the organization code of the receiving organization.

   For example, for an airline, enter its IATA code.
7. Enter a description of the partnership.
8. Select the type of partnership: **D**, **R** or **S**.

   See *What Is Partnership Type?* on page 112.

Image: Create Partnership



9. Click on **Create**.

   The partnership is displayed in the **Partnerships with rights delegated to a partner** list. It has the status **Pending validation** until the receiving organization accepts it.

   For more information on setting up a partnership, see *Workflow: Setting Up a Partnership* on page 113.

What Are the Auto-generated ACLs and Generic Roles for Partnership Management?

When a partnership is validated by the receiving organization, the system automatically generates ACLs in the partnership management application (**RFD/RFD_OGA/PTS**) with data type **NPS** (partnerships).

These ACLs must be assigned to the security administrator, along with the relevant generic roles, to allow the administrator to assign delegated roles to consumers, and view the consumers of these roles.

The generic roles are:

- PTS_VIEW_CONSUMER, which allows the consumer to display the consumers of delegated roles and ACLs.
- PTS_ALLOC, which allows the consumer to assign delegated roles and ACLs in a partnership.

When your organization is the data owner, you must assign the ACLs and roles to the security administrators (including yourself).

Table: Auto-generated ACLs and Generic Roles

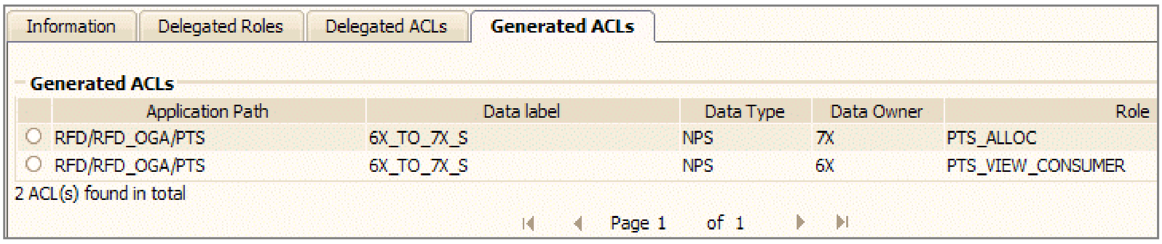
Partnership Type	Generic Role	ACL Name	Data Owner	Assigned to Security Administrator By:
D	PTS_VIEW_CONSUMER	AA_TO_BB_D	AA	Delegating organization (AA)
	PTS_ALLOC			
R	PTS_ALLOC	AA_TO_BB_R	BB	Receiving organization (BB)
S	PTS_VIEW_CONSUMER	AA_TO_BB_S	AA	Delegating organization (AA)
	PTS_ALLOC		BB	Receiving organization (BB)

(**AA** = Delegating organization, **BB** = Receiving organization)

How to Display the Auto-generated ACLs and Generic Roles for Partnership Management (Delegating Organisation)

1. On the **Home** tab, select your organization, and then click on **Manage Organization**.
2. Click on the **Partnerships** tab.
3. Select the partnership, and then click on **View details**.
4. Select the **Generated ACLs** tab.

Image: Generated ACLs and Generic Roles



Application Path	Data label	Data Type	Data Owner	Role
RFD/RFD_OGA/PTS	6X_TO_7X_S	NPS	7X	PTS_ALLOC
RFD/RFD_OGA/PTS	6X_TO_7X_S	NPS	6X	PTS_VIEW_CONSUMER

How to Assign the Auto-generated ACLs and Generic Roles for Partnership Management (Delegating Organisation)

Note: This task is only required by the delegating organization when the partnership type is D or S.

1. Display the security administrator (consumer) to whom you wish to assign the ACLs. Do one of the following:
   - Use the **User Search** if you know any of the search criteria.

     Or:
   - Display the consumer details (see *How to Display the Consumers of a Role* on page 95), then use the **User Search**.

   The consumers are displayed in the **User** tab. The administrator is normally yourself, and any other security administrators in your organization. However, it is also possible to assign the ACLs at a higher level, such as the office level, if appropriate.
2. In the results list, select the administrator, then click on **View details**.
3. Select the **ACL** tab.

   Note: If you want to display existing delegated ACLs, you must use the **Search Criteria** fields and select an application.
4. Click on **Assign new ACL**.
5. Select the role. Expand the application tree to display the roles under **RFD/RFD_OGA/PTS**, then click on **Generic** to display the generic roles.
6. Select the role to assign:
   - For partnership type D, you must assign **PTS_ALLOC** *and* **PTS_VIEW_CONSUMER** (in separate steps).
   - For partnership type S, you assign only **PTS_VIEW_CONSUMER**.

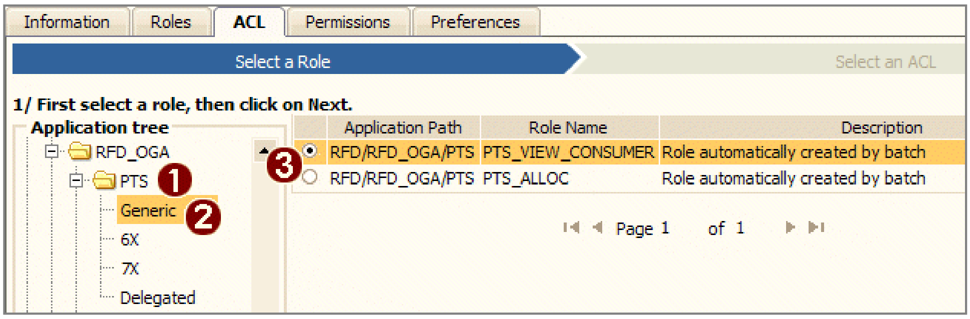
For more information about these roles, see *What Are the Auto-generated ACLs and Generic Roles for Partnership Management?* on page 115.

7. Click on **Next**.
8. Select the ACL for the partnership.

   Example: **AA_TO_BB_D** for partnership type D, or **AA_TO_BB_S** for partnership type S. The data type is **NPS**.

   Use the **Search** filters to reduce the list of ACLs displayed, if necessary.
9. Click on **Assign**.
10. In the **Assign ACL** dialog box, select the option to assign the related role.
11. Click on **OK**.

Example: Selecting the Auto-generated Role



❶ Application **RFD/RFD_OGA/PTS**.

❷ Generic roles.

❸ Select the role to assign (one or both, depending on the partnership type).

How to Delegate an ACL and Its Related Role to the Receiving Organisation

Note: Before you can perform this task, you must have already created the roles and ACLs that you want to delegate. A delegated ACL can be related to either a generic role or to a role belonging to your organization. See *Defining Roles* on page 81 and *Defining Access Control Lists* on page 91.

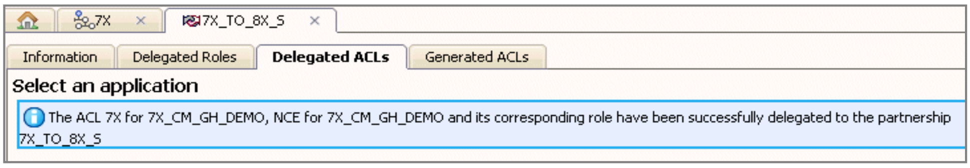
1. On the **Home** tab, select your organization, and then click on **Manage Organization**.
2. Select the **Partnership** tab.
3. Select the partnership to which you want to delegate an ACL, then click on **View details**.
4. Select the **Delegated ACLs** tab.

   Note: To display existing delegated ACLs, you must select an application in the **Search Criteria** fields.
5. Click on **Delegate new ACL**.
6. Select the related role: Expand the application tree and select the role related to the ACL.

This can be a role belonging to your organization, or a generic role.

7. Click on **Next**.
8. Select the ACLs you want to delegate to the partnership.
9. Click on **Delegate**.
   - If the role related to the ACL is a generic role, only the ACL is delegated.
   - If the role related to the ACL belongs to your organization and has not yet been delegated, both the ACL and the role are delegated.
   - If the role related to the ACL belongs to your organization and has already been delegated with another ACL, only the ACL is delegated.

Image: Delegated ACL and Role Confirmation Message



How to Delegate Multiple ACLs and Their Related Roles (Airlines)

1. Go to **Home > Data Management > Download Templates for Massive Actions.**
2. In the **List of Templates** pane, select the **Manage Rights** template, then click on **Download template**.
3. Enter the appropriate information in the **Delegate ACL** tab of this template.
4. When you have completed all the fields, select the **Options** tab and click on **Convert to CSV**.
5. Go to **Home > Data Management > Massive Import (Users, Rights, Offices)**.
6. In the **File path** field of the **Upload File** pane, enter the template file name, or click on **Browse** to select it, then click on **Upload**.

   The ACLs and associated roles are delegated. The **List of Requests** pane indicates the status.
   - If the role related to the ACL is a generic role, only the ACL is delegated.
   - If the role related to the ACL belongs to your organization and has not yet been delegated, both the ACL and the role are delegated.
   - If the role related to the ACL belongs to your organization and has already been delegated with another ACL, only the ACL is delegated.
7. If there is an error, select the file, then click on **View details**.

   The **Request Details** pop-up window is displayed containing the error description. For example, the user is not authorised to perform the action.
8. Check the report sent to the email address indicated in the first line of the file.

How to Remove Delegated Roles and ACLs From the Receiving Organisation

1. On the **Home** tab, select your organization, then click on **Manage organization**.
2. Select the **Partnership** tab.
3. Select the partnership from which you want to remove an ACL and a role, and then click on **View details**.
4. Click on the **Delegated ACLs** tab.
5. Select the delegated ACL that you want to remove from the partnership.
6. Click on **Remove ACL from partnership**.
7. Click on **Remove** to confirm.

   Any allocation of the ACL to consumers in the receiving organization is removed.

   If the related role is also delegated and the ACL is the only ACL related to the role in the partnership, then any assignation of the role to consumers is deleted. The role is also removed from the partnership.

   If the related role is a generic role, only the ACL is removed from the partnership.

How to Assign Delegated ACLs and Related Roles (Delegating Organisation)

Note: When the partnership type is D, the delegating organization delegates and then directly assigns access rights to consumers in the receiving organization.

1. If the receiving organization does not belong to your list of organizations, click on the **Choose organizations** link at the top of the left panel to select this organization.

   For detailed instructions, see *How to Add an Organisation to Your List* on page 15.

2. Using the left search pane, display the consumer in the receiving organization to whom you want to assign a delegated ACL and role.
3. Display the details of the consumer.
4. Click on the **ACL** tab.
5. Click on **Assign new ACL**.
6. Expand the application tree and select the delegated role.

   This can be a role belonging to your organization, or a generic role.

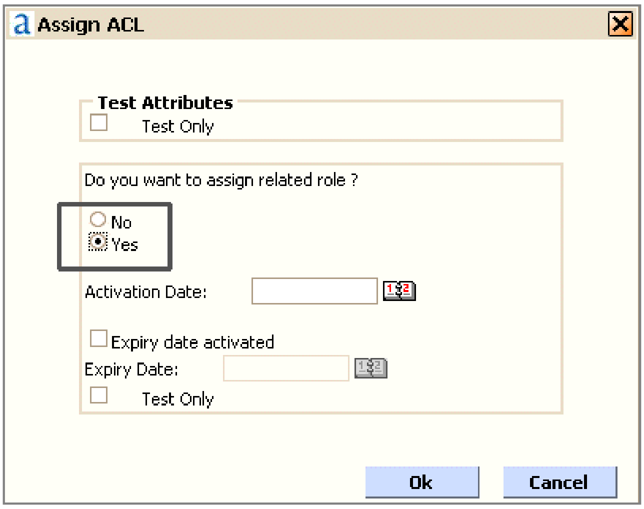
7. Click on **Next**.
8. Select the delegated ACL to assign.

   The data owner of the ACL is your organization.

   Note: To display the available delegated ACLs, you must select an application in the fields of the **ACL Search Criteria** pane.

9. Click on **Assign**.

10. Select the option to assign the role at the same time as the ACL, then click on **OK**.



For more information on assigning ACLs, see *How to Assign an ACL to a Consumer* on page 98.

How to Display the Consumers of a Delegated Role and ACL

Note: This task applies to partnership types D and S.

1. On the **Home** tab, select your organization, and then click on **Manage organization**.
2. Select the **Partnership** tab.
3. Select the partnership to which you have delegated access rights, and then click on **View details**.
4. Select the **Delegated ACLs** tab.
5. Use the fields of the **ACL Search Criteria** pane to display the delegated ACLs for an application.
6. Select a delegated ACL, then click on **View consumers**.

Tasks for the Receiving Organisation

How to Accept a Partnership

Note: Perform this task when another organization has created a partnership with your organization as the receiving organization. The status of the partnership is **Pending validation**.

1. On the **Home** tab, select your organization, then click on **Manage organization**.
2. Select the **Partnership** tab.
3. In the section **Partnerships requests pending validation**, select the partnership that you want to accept.
4. Click on **Accept**.

The partnership is now active and its status is set to **Accepted**. It is added to the list of existing partnerships.

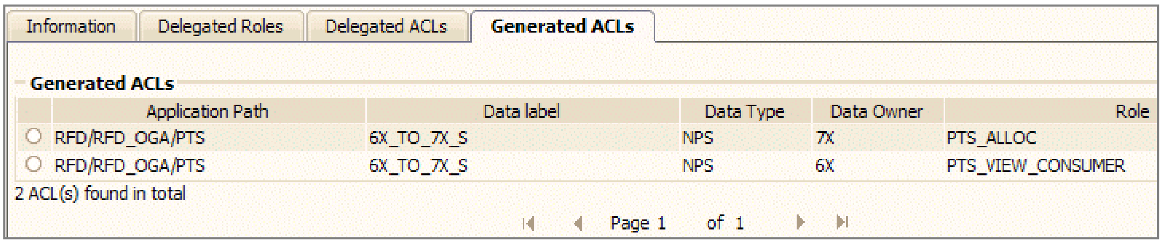
Note: If you refuse a partnership, it is removed from the **Pending validation** list and added to the **List of existing partnerships**, with its status set to **Refused**.

How to Display the Auto-generated ACLs and Generic Roles for Partnership Management (Receiving Organisation)

See also *What Are the Auto-generated ACLs and Generic Roles for Partnership Management?* on page 115.

1. On the **Home** tab, select your organization, and then click on **Manage Organization**.
2. Select the **Partnership** tab.
3. Select the partnership for which you are the receiver, then click on **View details**.
4. Click on the **Generated ACLs** tab.

Example: Generated ACLs and Generic Roles


Information | Delegated Roles | Delegated ACLs | Generated ACLs

Generated ACLs

Application Path	Data label	Data Type	Data Owner	Role
RFD/RFD_OGA/PTS	6X_TO_7X_S	NPS	7X	PTS_ALLOC
RFD/RFD_OGA/PTS	6X_TO_7X_S	NPS	6X	PTS_VIEW_CONSUMER

2 ACL(s) found in total

Page 1 of 1

How to Assign the Auto-generated ACLs and Generic Roles for Partnership Management (Receiving Organisation)

Note: This task applies to the receiving organization, when the partnership type is R or S.

1. Select the security administrator (consumer) in your organization to whom you wish to assign the ACLs.

   This will normally be yourself and any other security administrators in your organization. However, it is also possible to assign the ACLs at a higher level, such as the office level, if appropriate.
2. Click on **View details**.
3. Select the **ACL** tab and click on **Assign new ACL**.
4. Select the role: Expand the application tree to display the roles under `RFD/RFD_OGA/PTS`, and then click on **Generic** to display the generic roles.
5. Select the role `PTS_ALLOC`.

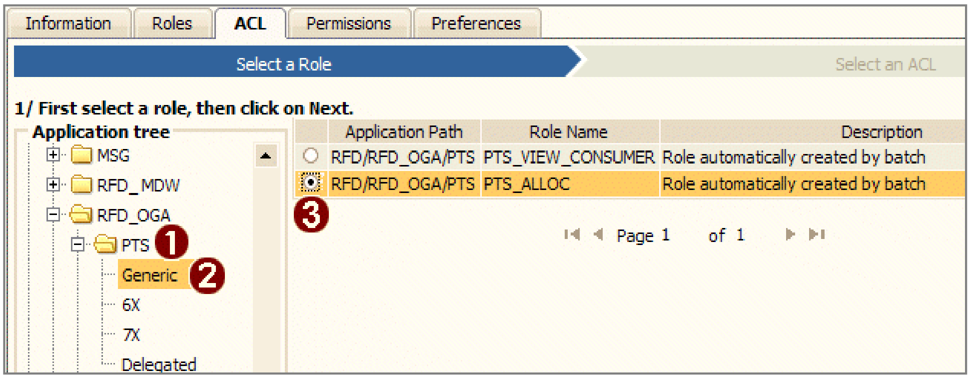
   For more information on this role, see *What Are the Auto-generated ACLs and Generic Roles for Partnership Management?* on page 115.
6. Click on **Next**.
7. Select the ACL for the partnership.

Example: `AA_TO_BB_R` for partnership type R or `AA_TO_BB_S` for partnership type S, where AA is the delegating organization and BB is the receiving organization. The data type is **NPS**.

Use the **Search** filters to reduce the list of ACLs displayed, if necessary.

8. Click on **Assign**.
9. In the **Assign ACL** dialog box, select the option to assign the related role.
10. Click on **OK**.

Example: Selecting the Auto-generated Role



❶ Application **RFD/RFD_OGA/PTS**

❷ Generic roles

❸ Role `PTS_ALLOC`

How to Assign Delegated ACLs and Related Roles to Consumers (Receiving Organisation)

Note: When the partnership type is **R** or **S**, the receiving organization assigns access rights to consumers in their own organization.

1. Display the consumer in your organization to whom you want to assign a delegated ACL and role.
2. Display the details of the consumer.
3. Select the **ACL** tab.
4. Click on **Assign new ACL**.
5. Select the related role: Expand the application tree then click on **Delegated** or **Generic**, to display the delegated roles available.

   The role must belong to the delegating organization (listed under **Delegated**) or be a generic role (listed under **Generic**).
6. Click on **Next**.
7. Select the ACL to assign.

   The data owner of the ACL is the delegating organization.

   Use the **Search** filters to reduce the list of ACLs displayed, if necessary.
8. Click on **Assign**.

9. Select the option to assign the role at the same time as the ACL, and then click on **Assign**.

   For more information on assigning ACLs, see *How to Assign an ACL to a Consumer* on page 98.

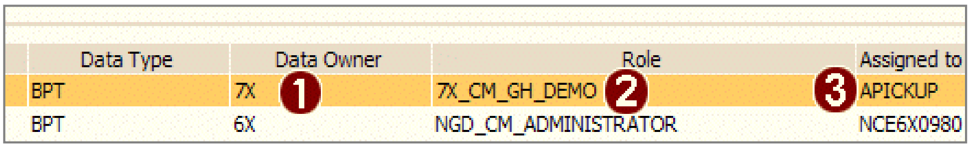
How to Display the Delegated Access Rights of a Consumer

1. Select the consumer in your organization for whom you want to display delegated access rights, and then click on **View details**.
2. Select the **ACL** tab.
3. In the fields or from the drop-down lists of the **ACL Search Criteria** pane, enter or select the application, then click on **Search**.

   The system displays all ACLs directly assigned to the consumer.
4. Modify the display, as necessary, by selecting a higher level (for example, office or organization unit) in the **ACL for** field of the **ACL Search Criteria** pane.
5. On the resulting display, check the **Data Owner** column.

   Delegated ACLs and roles show the delegating organization as the data owner.

Example: ACL Delegated from 7X to 6X, Assigned to a 6X User



Data Type	Data Owner	Role	Assigned to
BPT	7X	7X_CM_GH_DEMO	APICKUP
BPT	6X	NGD_CM_ADMINISTRATOR	NCE6X0980

1. The data owner is the delegating organization.
2. In this example, the role belongs to the delegating organization.
3. The ACL has been assigned directly to a user in organization 6X.

Suspending and Deleting a Partnership

How to Suspend a Partnership

Note: A partnership can be suspended by either the delegating or the receiving organization. This prevents data being shared for as long as the partnership is suspended. However, the structure of the partnership is maintained and can be reactivated by the delegating organization, at any time.

1. On the **Home** tab, select your organization, then click on **Manage organization**.
2. Select the **Partnership** tab.
3. Select the partnership that you want to suspend, then click on **Suspend**.
4. Click on **Suspend**.

What Happens When a Partnership Is Suspended?

When you suspend a partnership:

- ACLs automatically generated to manage the partnership have their assignation to consumers removed, and are deleted.
- Assignation of delegated ACLs is removed from the consumers.
- Assignation of roles belonging to the delegating organization is removed from the consumers.
- Assignation of rights to partner consumers is no longer possible.

However, delegated roles and ACLs no longer assigned to consumers are maintained in the suspended partnership.

Note: The suspension of a partnership has no impact on generic roles, as generic roles exist independently of the partnership. The role assignation in the receiving organization is maintained, but the related ACLs delegated through the partnership can no longer be used.

How to Reactivate a Suspended Partnership

Note: Only the security administrator of the *delegating* organization can reactivate a suspended partnership.

1. On the **Home** tab, select your organization, and then click on **Manage organization**.
2. Select the **Partnership** tab.
3. Select the suspended partnership that you want to reactivate, and then click on **Reactivate**.
4. Click on **Reactivate** to confirm the reactivation of the partnership.
   - The partnership becomes active and its status is set to **Accepted**.
   - The auto-generated ACLs for partnership management that were deleted when the partnership was suspended are generated again.

To reactivate access rights in the receiving organization, you must:

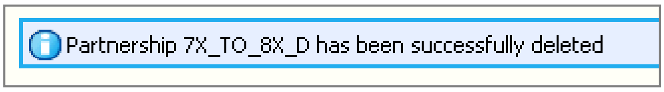
- Assign the auto-generated ACLs for partnership management.
- For partnership type D, assign delegated ACLs and roles to consumers in the receiving organization.
- For partnership types S and R, ask the security administrator in the receiving organization to assign PTS_ALLOC and the ACL to themselves, and to assign delegated ACLs and roles to the consumers.

How to Delete a Partnership

Note: Only the security administrator of the delegating organization can delete a partnership.

1. On the **Home** tab, select your organization, and click on **Manage organization**.
2. Select the **Partnership** tab.

3. Select the partnership that you want to delete, and then click on **Delete**.
4. Click on **Delete**.



What Happens When a Partnership Is Deleted?

- ACLs for partnership management that were created automatically when the partnership was set up are deleted.
- Assignation of ACLs are removed from consumers.
- ACLs with no assignations are removed from the partnership.
- Assignation of roles belonging to the delegating organization are removed from the consumers.
- Delegated roles belonging to the delegating organization with no assignations are removed from the partnership.
- Generic roles are maintained with the receiving organization, and if they are assigned to a consumer, the assignation is maintained.

Chapter 14

Managing Guest Authentication

Note: This feature is only available for Travel Channels customers, and is not available for Airlines.

Understanding Guest Authentication

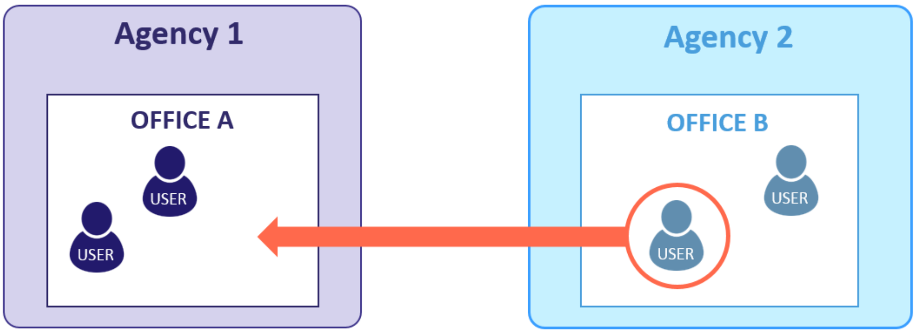
What is Guest Authentication?

The Guest Authentication feature allows Amadeus Selling Platform Connect customers to streamline authentication by allowing agents to use the same credentials to access multiple office IDs.

Agents can thereby access an office even if they do not have a sign within that Office ID; that is, no Login Area is defined for them in that Office ID.

How is Guest Authentication set up?

To illustrate the concept, suppose an office in Agency 1 wishes to allow an agent in an office in Agency 2 to be able to log in as a guest user. (This is equivalent to a remote jump.)



To achieve this:

- The administrator in Office A creates a **guest user** with various rights and preferences, and a so-called **agreement** with Office B, linked to that guest user.

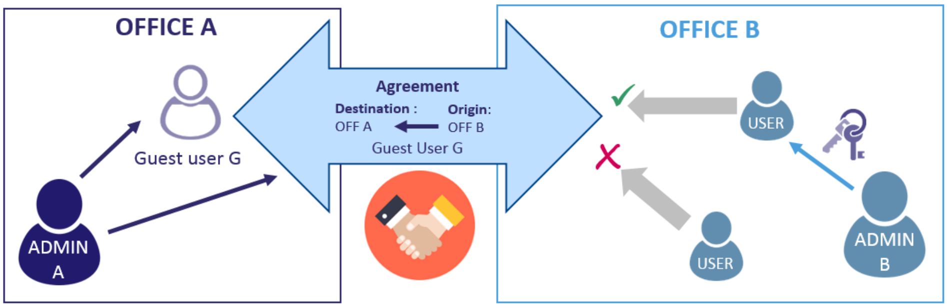
  An agreement can be between:

  - Two offices: To allow users from the origin Office to access the destination Office

- An origin Office and a destination OGU: To allow users from the origin Office to access all the offices of the destination OGU.
- An origin OGU and a destination Office: To allow users from the origin OGU to access the destination Office.
- An origin User and a destination Office (or OGU): To allow a specific User to access the destination Office (or all the offices of the destination OGU).

- The administrator in Office B creates a **guest login area** for an existing agreement and assigns that login area to a user. When that user logs in to the guest login area (and hence the guest office), he inherits the same rights given to the guest user. This includes not only the rights assigned directly to the guest user ID, but also any rights assigned to its office or parent (OGU or ORG).

  Users in Office B without access to the guest login area are blocked from logging in to Office A.



Notes

- The guest user (and its associated profile) is determined from the agreement, as set by the destination administrator. The origin user/administrator cannot choose the guest user used for authentication.
- The security policy and application security (that is, the password policy and TFA/DDNA security policies) are controlled through the origin user's default login area.
- Authentication is logged for both the user in his default office, and the associated guest in the destination office.

What is a Guest User?

A guest user is a special LSS user of type *Guest User*, that:

- is identified by a guest name.
- has a duty code.
- belongs to an organization.
- is associated to one or more definition areas: ORG, OGU, OFF.

What is an Agreement?

An agreement is defined by the combination of:

- Origin Area (ORG, OGU, OFF or USER)
- Destination Area (ORG, OGU or OFF)

- Guest User ID

A maximum of one agreement can exist between a given Origin-Destination office pair. Only one agreement can be exist between a given pair, so it is not possible to have one agreement between office A and office B for guest 1 and then try to create another agreement for guest 2 between the same office pair. If a user in office A needs to access office B with different rights than the guest at office level, then a new agreement needs to been created between the specific user and office B with a different guest profile.

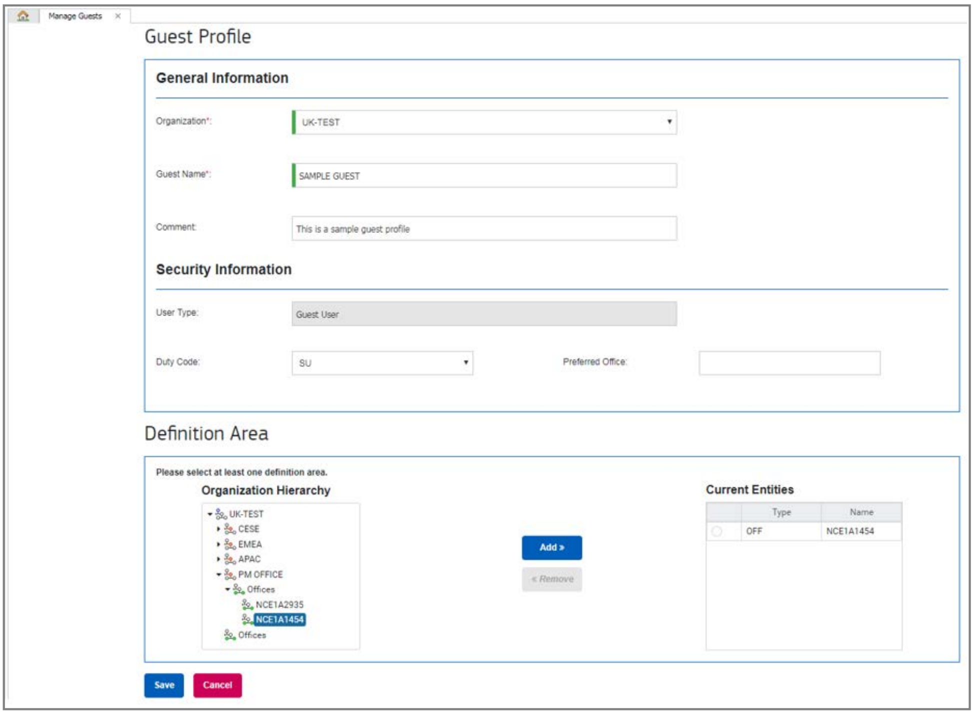
Each agreement has:

- an origin status, managed by the administrator of the origin area. The value can be Locked or Active.
- a destination status, managed by the administrator of the destination area. The value can be Locked, Suspended or Active.

Destination Administration Tasks

How to add a Guest Profile

1. On the Home page under **User Management**, click on **Manage Guest**.
2. On the **Manage Guests** page, click on **Create Guests**.
3. In the **Guest Profile** area, select the **Organization** and enter a **Guest name**.
4. In the **Security Information** area, optionally specify a **Duty Code** and **Preferred Office**. The preferred office is the office from which the guest user's sign profile attributes are initialized.
5. In **Definition Area**, select an organization level such as OGU or office, and click on **Add** to move it to the list of entities.



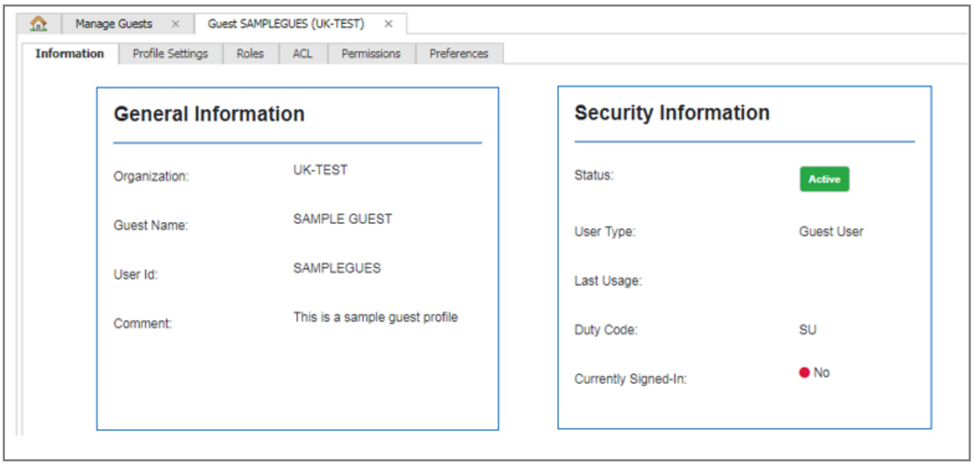
6. Click on **Save** to return to the Home page.

The new **Guest User** is shown in the list.

You can now define the Guest User's profile by defining its access rights.

How to define the access rights of a Guest User

1. On the Home page under **User Management**, click on **Manage Guest**.
2. In the **Manage Guests** page, click on **View Guest Details**.
3. Click on any of the tabs to set the roles, ACLs, and so on for the user.



4. Optionally, in the **Definition** area, add or remove any definition areas if necessary.

How to search for an Agreement

1. On the Home page under **User Management**, click on **Manage Agreement**.
2. On the **Manage Agreements** tab, select the organization and entity type, and whether you are looking for an **Incoming** or **Outgoing** agreement.

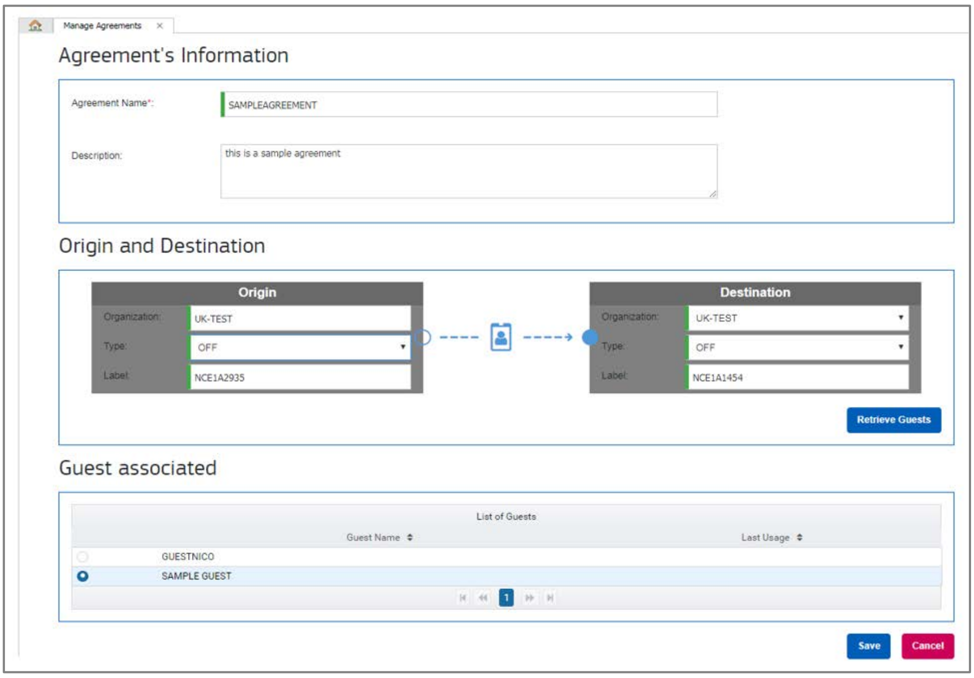
3. Click on **Search**.
4. To view details of the agreement, select it from the list.

How to create an Agreement

Note: Before you can create an agreement you must first create a Guest User and define its profile.

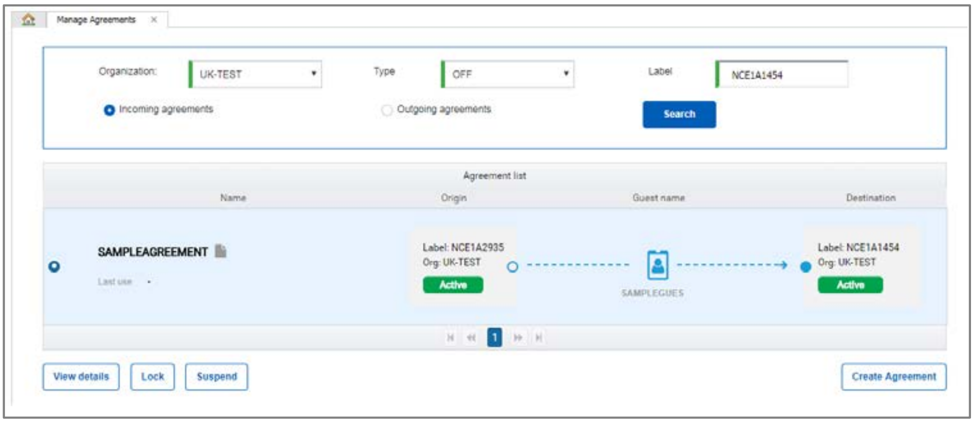
1. On the Home page under **User Management**, click on **Manage Agreement**.
2. On the **Manage Agreements** tab, click on **Create Agreement**.

3. On the **Agreement Information** area, enter a name for the agreement.
4. In the **Origin and Destination** area specify the origin and destination entities then click on **Retrieve Guests**.
5. A list of all Guest Users is displayed in the **Guest associated** area.
6. Select the Guest User.
7. Click on **Save**.



How to view details of an Agreement

1. On the Home page under **User Management**, click on **Manage Agreement**.
2. Fill in the **Organization**, **Type** and **Label**, and select if it is an incoming or outgoing agreement.



A list of matching Agreements is displayed.

3. Select an Agreement from the list and click on **View details**.

How to lock or suspend Guest User access

1. View the details of an Agreement. See *How to view details of an Agreement* above.

2. Click on:
   - **Lock**

     In this case, the agreement is taken into account, but access is denied)
   - **Suspend**

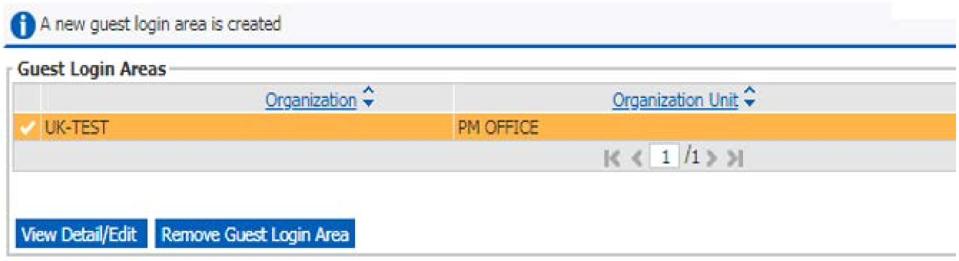
     In this case, the agreement is ignored as if it did not exist.

Origin Administration Tasks

How to assign a Guest Login Area

1. Search for a user and view the user's details.
2. On the user's details page, in the **Guest Login Areas** area, click on **Add New Guest Login**.

   The **Login Areas** tab shows the definition areas for which there is an existing agreement.
3. Select the login area you wish to add and click on **Add**, then click on **Save**.
4. The new Guest Login Area is listed.



Note: If you added all offices of an OGU, the **Organization Unit** column will show the entry **All**.

5. Click on **View Details** to view the full details.

How to remove a user's access to a Guest Login Area.

1. Search for a user and view the user's details.
2. On the user's details page, in the **Guest Login Areas** area, select the login area from the list and click on **Remove New Guest Login**.

Chapter 15
Working With Reports

What Are Reports?

The reporting engine allows security administrators to create up to 10 reports per week per organization. These reports are in CSV format. They can contain:

- A list of users and their profiles for an organization. Depending on your rights, you can extract your own and partners' user profiles.
- A list of all the signs, including those without a LSS login, contained in the sign bank of an office belonging to an organization.
- A list of all ACLs for one or several consumers.
- A list of roles for one or several consumers.
- A list of preferences for one or several consumers.
- A list of offices within an organization.
- A list of applications and sub-applications, with all their details.
- A list of administration history details for all the actions performed in an organization.
- A list of authentication history details.

For more information on the reports, see:

- *Where Are Reports Stored?* below
- *What Are Report Templates?* on page 136
- *What Are Report Schedules?* on page 136
- *Reference: Codes in Administration History Reports* on page 149.

Where Are Reports Stored?

The **Reports** tab lists all reports created by LSS administrators of the organization during the previous 60 days. Any administrator can see the reports. For example, all 1A administrators can see reports created by the 1A organization administrator.

The reporting engine cache is refreshed once a day at 06:00 GMT in the test environments (PDT, UAT, MIG) and Amadeus Training Environment (SKL), and at 05:00 GMT in the production environment (PRD). Changes to user profiles made after this time do not appear in reports until the next refresh.

See also *How to Create a Report* on page 134.

Creating Reports

How to Create a Report

1. Go to **Home > Reporting Engine**.
2. Click on the appropriate tab, depending on the type of data you want in your report: Data on users, sign banks, rights and preferences, offices, applications or administration history details.
3. Select an organization from the **Organization** drop-down list.
4. Do one of the following:

   - If you have already created a template that suits your needs, select it from the **Template** drop-down list, then click on **Load**.

     To create a template, see *How to Create a Report Template* on page 136.

     Or:

   - Select the required data from the **Data to export** pane, and then from the **Filters** pane select any filter attributes or enter values in any of the filter fields, as appropriate.

     See *How to Restrict the List of Data in Your Report* below.

   a) For administration history reports, enter a date range in the **Date** pane of the **Admin History** tab.

   You can go back to a maximum of 12 months in the past.

5. Click on **Submit**.

   When the report is ready, it is added to the list on the **Reports** tab.

6. Click on the **Reports** tab, select the organization, then click on **Select**.

   The **Reports** list is refreshed. There is one report per type of data, for example, user, office, sign bank.

   Note: It can take a few minutes for a report to appear in the **Reports** list.

7. In the **Reports** list, select the report, then click on **Open file**.
8. Open or save the CSV report.

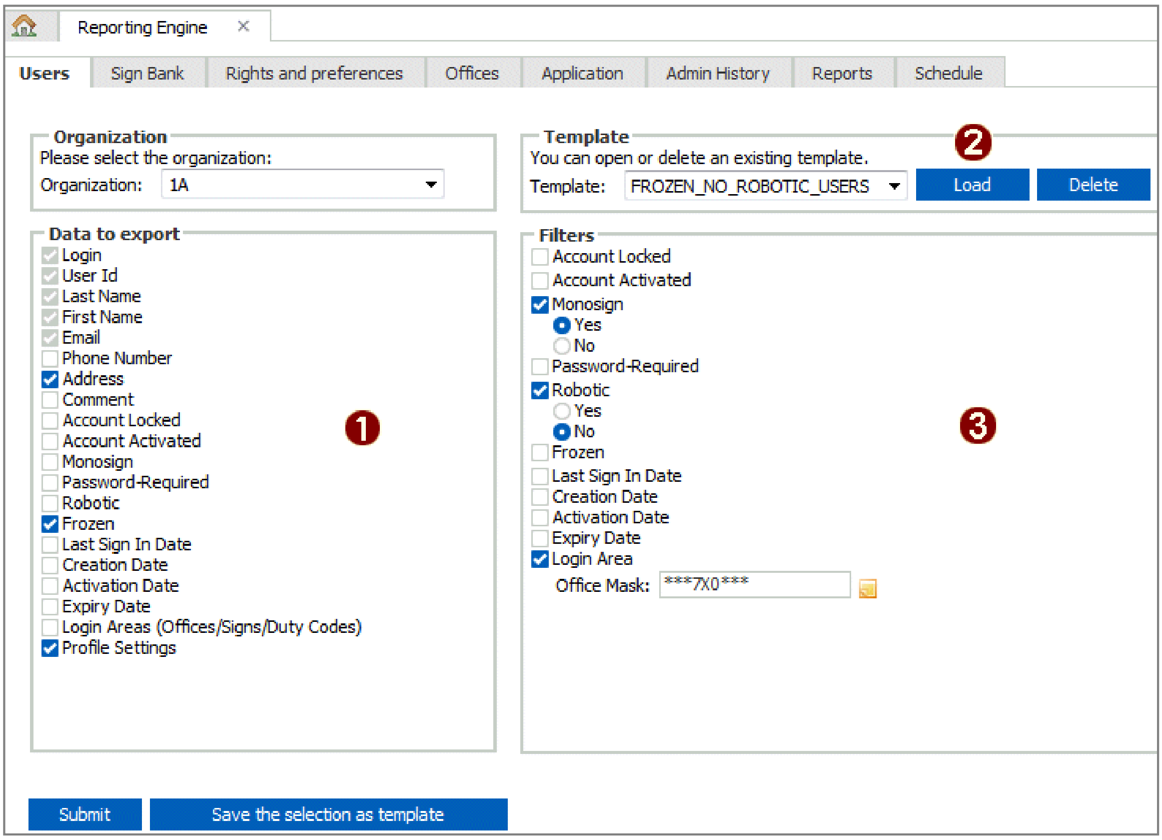
   For an explanation of the codes used in administration history reports, see *Reference: Codes in Administration History Reports* on page 149.

How to Restrict the List of Data in Your Report

Apply filters to restrict the list of data in your report. These filters are available in the **Filters** pane of all the data tabs, for example, the **Rights and Preferences** tab or the **Admin History** tab.

Note: Alternatively, create a report with all data and then apply filters to the CSV report in your own application.

Example: Restricting the List of Data in User Reports



1. **Data to export** pane: Five parameters are selected by default and cannot be removed. You can select others as required, such as user address and frozen account attributes. If you select **Profile Settings**, you obtain a report with the profile settings attributes, duty codes and the preferred language of each user.

   Explanation: Create User Tab Fields and Settings on page 57.

2. **Template** pane. See *Managing Report Templates* on page 136.

3. **Filters** pane: You can create a user data report that only lists robotic users for an organization, or one that only lists accounts with login areas corresponding to a specific office mask.

Example: Restricting the List of Data in Rights and Preference Reports

You can limit your ACL, role and preference reports by specifying up to 10 values for each of the three filters: **Application**, **Office** and **Organization Unit**. If you specify an office or an OGU, your report will also list the rights of the nodes above in the organization tree (OGU and organization for the office, organization for the OGU).

Example: Restricting the List of Data in Office Reports

You can limit your office reports by specifying up to 10 values for each of the three filters: **Office ID**, **Organization Unit** and **Country**.

Managing Report Templates

What Are Report Templates?

For reports you run frequently, you can save a series of criteria in a template. You load the template whenever you want to create the report.

You can also use templates to schedule reports on a regular basis. See *Working With Report Schedules* below.

How to Create a Report Template

Note: You can create templates for all reports except administration history reports.

1. Go to **Home > Reporting Engine**.
2. Click on the appropriate tab, depending on the type of data you want in your report: data on users and their profiles, sign banks, roles, ACLs, preferences, offices, applications or administration history details.
3. Select an organization from the **Organization** drop-down list.
4. Select the required data from the **Data to export** pane, and any filter attributes from the **Filters** pane.

   See *Explanation: Create User Tab Fields and Settings* on page 57.
5. Click on **Save the selection as template**.
6. Enter a name for the template, then click on **Save**.

How to Delete a Report Template

1. Go to **Home > Reporting Engine**.
2. Click on the appropriate tab, depending on the report template you want to delete.
3. In the **Template** pane, select the template, then click on **Load**.
4. Check that the attributes correspond to the template you want to delete, then click on **Delete**.

Working With Report Schedules

What Are Report Schedules?

The **Schedule** tab allows you to run reports on a regular basis. They run as a batch in the background. You can view them on the **Reports** tab.

You can schedule reports as follows:

- On a specific day of the week, for up to 52 weeks.
- On any day of the month from the 1st to the 28th, for up to 12 months.

Scheduled reports are based on templates. See *How to Create a Report Template* above.

How to Schedule Reports

1. Go to **Home > Reporting Engine > Schedule**.
2. Select the organization from the drop-down list.
3. Click on **New**.

   The **New Schedule** pop-up window is displayed.
4. Select a template.

   See *How to Create a Report Template* on page 136.
5. Define a weekly or monthly schedule, and the number of iterations.

   Note: At the end of the specified period you will have to recreate the schedule.
6. Click on **Save**.

   The schedule is added to the **Schedule** list.

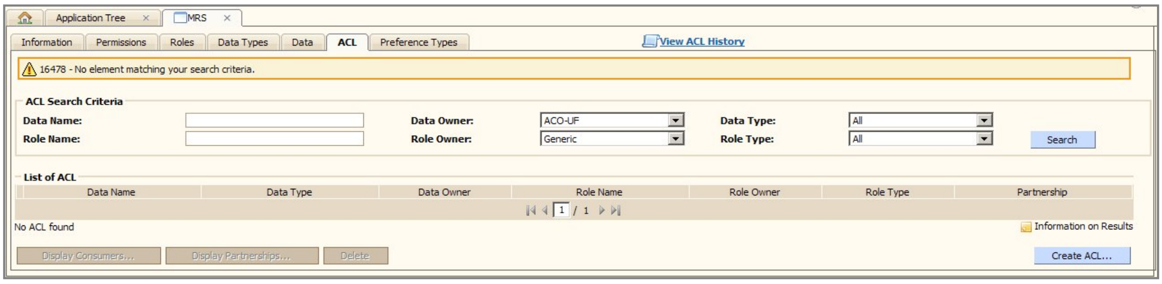
Appendix A

Examples

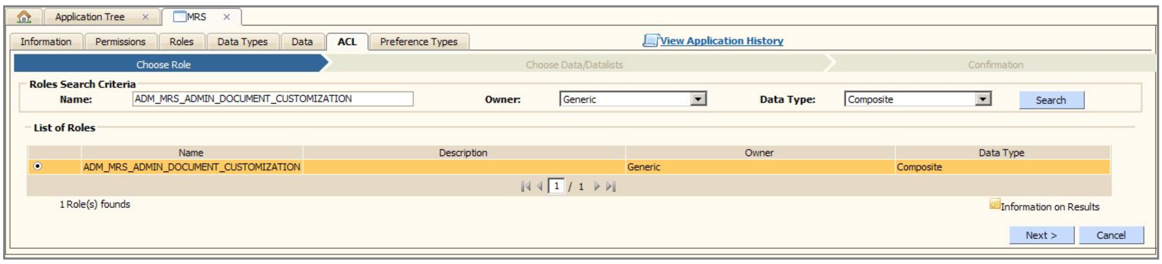
This section shows how to create three ACLs of different data types for a generic role in the **CustomizeIT** application (**UFD/MRS** in the application tree) for organization ACO-UF, and then how to assign it to office MUCUF2900.

Creating ACLs for a Generic Role

1. Display the application **UFD/MRS** in the application tree, then click on the **ACL** tab to display any existing ACLs.
2. Click on **Create ACL**.



3. Search for and select the generic role `ADM_MRS_ADMIN_DOCUMENT_CUSTOMIZATION`, then click on **Next**.

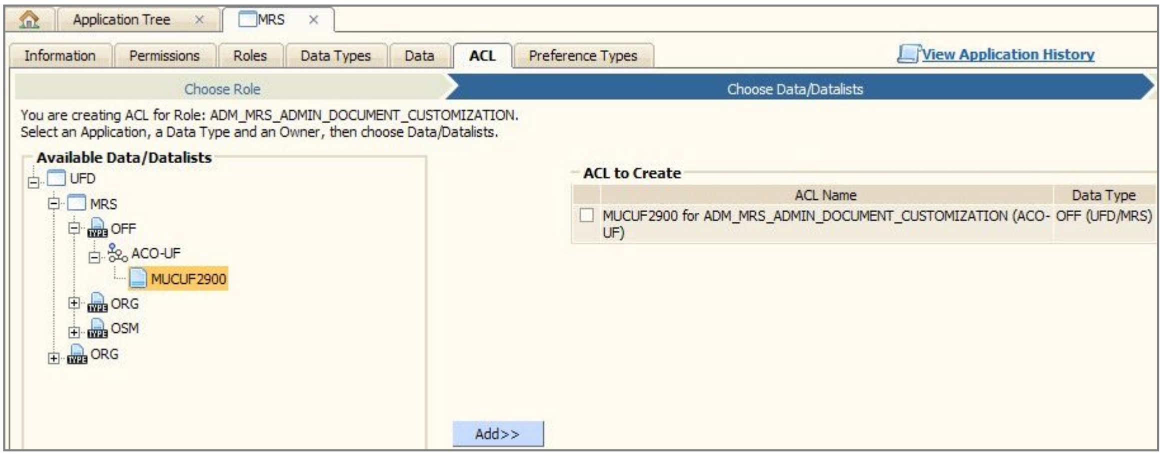


This role is a composite role and has three data types: **OFF** (office), **ORG** (organization) and **OSM** (object security mode).

4. Expand the tree of available data under data type **OFF**, then select the office **MUCUF2900** under owner organization **ACO-UF**.

   MUCUF2900 has already been created as data for data type **OFF** and owner organization **ACO-UF**.

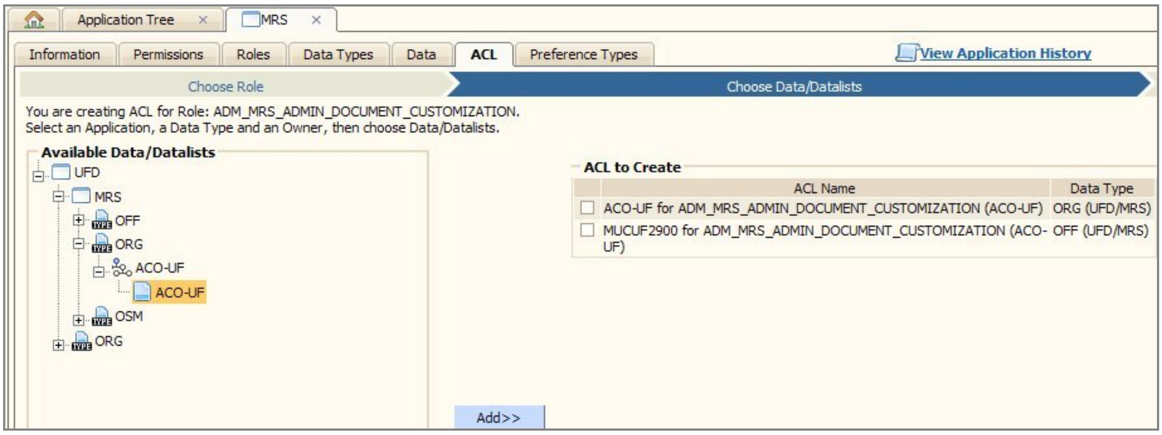
5. Click on **Add** to move this data into the **ACL to Create** box.



6. Expand the tree of available data under data type **ORG**, then select the organization **ACO-UF** under owner organization **ACO-UF**.

   ACO-UF has already been created as data for data type **ORG** and owner **ACO-UF**.

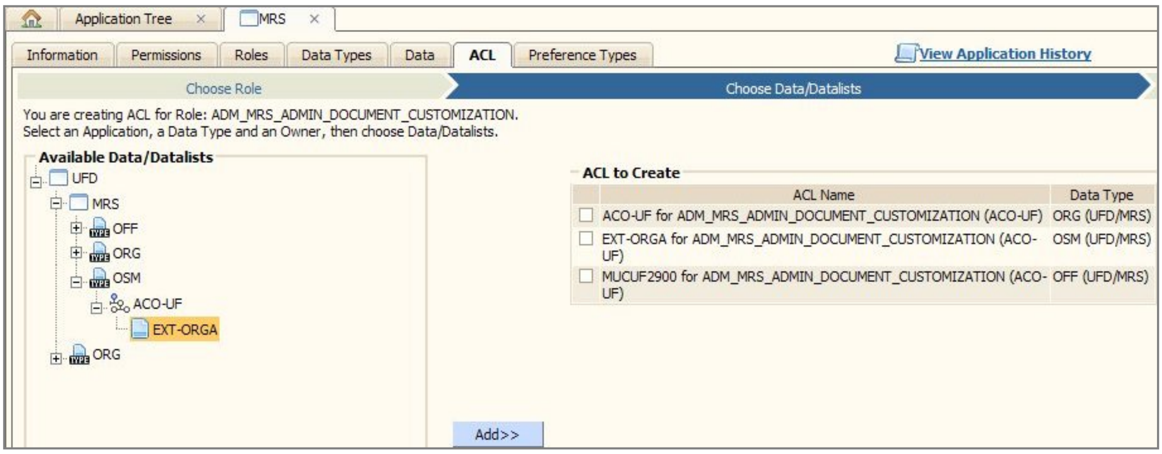
7. Click on **Add** to move this data into the **ACL to Create** box.



8. Expand the tree of available data under data type **OSM**, then select the value **EXT-ORGA** under owner organization **ACO-UF**.

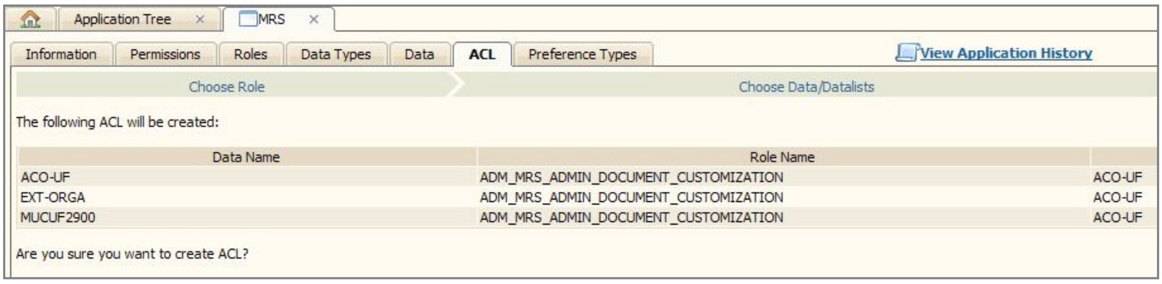
   EXT-ORGA has already been created as data for data type **OSM** and owner **ACO-UF**.

9. Click on **Add** to move this data into the **ACL to Create** box.



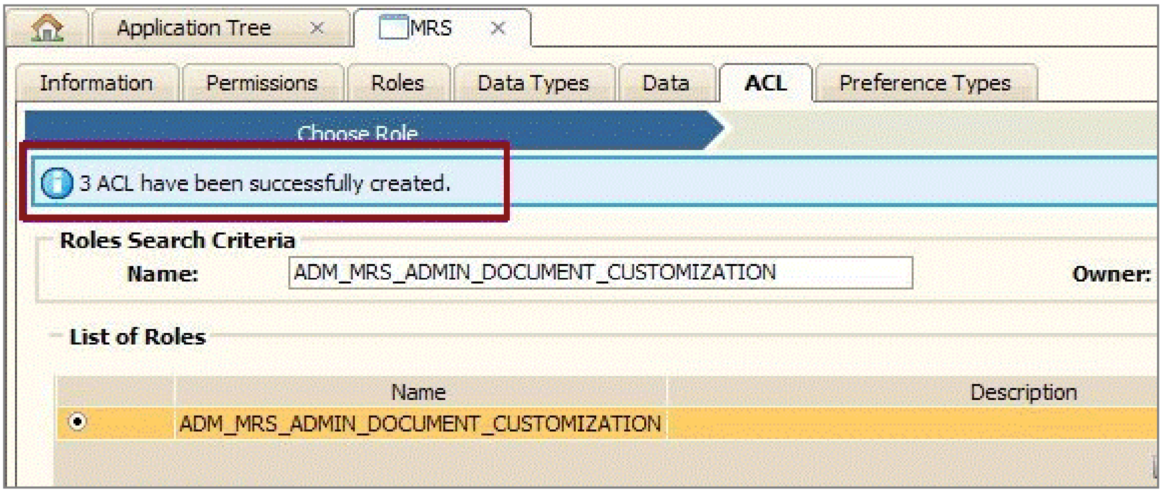
10. Click on **Create**.

    The ACLs to create are displayed.



11. Click on **Create**.

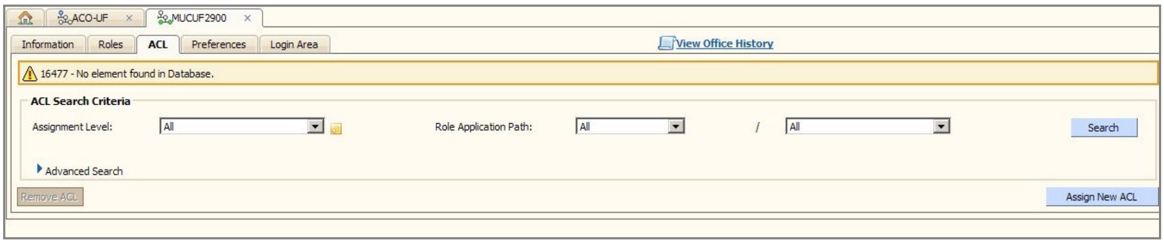
    A confirmation message is displayed.



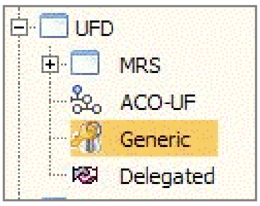
Assigning ACLs and a Role to an Office in One Step

1. Search for the office in the organization tree, using the **Office/Unit** search fields in the left menu bar. When the office is displayed, click on **View office**.

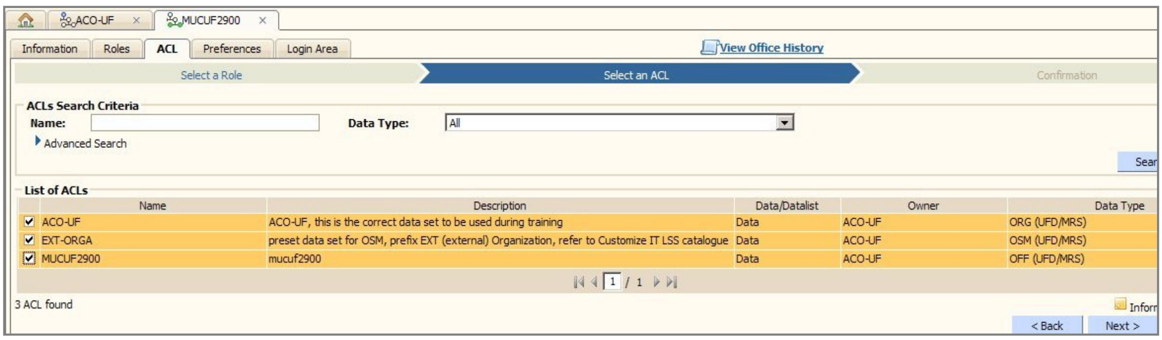
2. Select the ACL tab, to display ACLs assigned to this office.



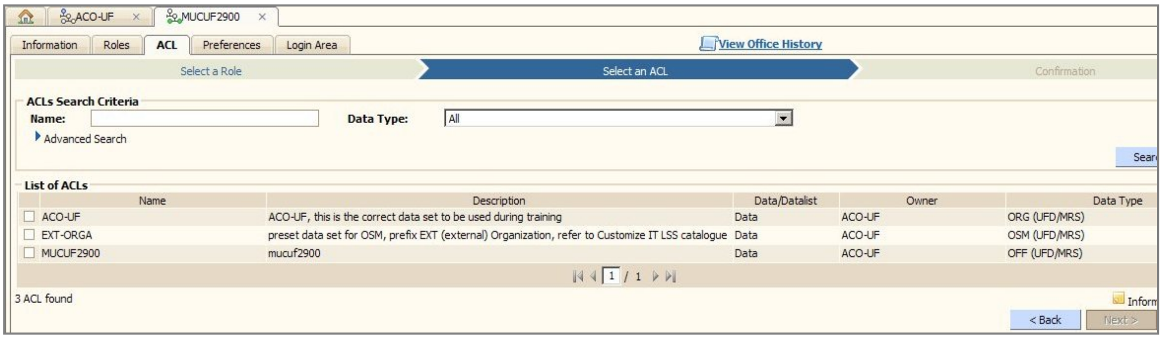
3. Click on **Assign New ACL**.
4. Expand the application tree and find application **UFD/MRS**; then click on **Generic** under this application to display a list of roles.



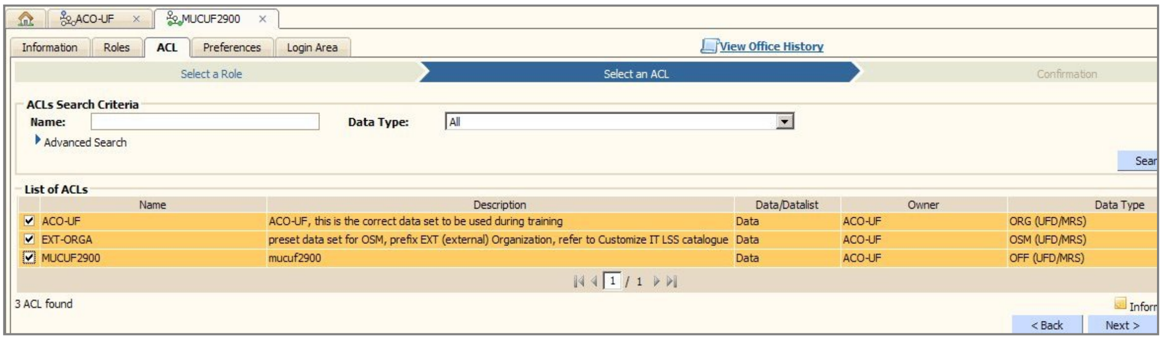
5. Select the role **ADM_MRS_ADMIN_DOCUMENT_CUSTOMIZATION**, then click on **View details**.



The ACLs you created for this role are displayed.



6. Select each ACL, then click on **Next**.



7. To assign the role and the ACLs in one step, select **Assign Related Role**.

8. Click on **Assign**.

A confirmation message is displayed.

Appendix B

Sign Profile Synchronisation

This table indicates changes to attribute characters, or the non-synchronization of specific attributes, when they are exchanged between **ASM** and the Amadeus central system (ACS). The attributes are displayed in the **User Information** tab.

See also:

- *Working With User Authentication Settings* on page 55.
- *Defining Sign Profiles* on page 67.

Table: ASM-TPF Sign Profile Synchronization Details

Information Tab Field Names	System Notes
Last name	The **Last name** and **First name** are used to update the **Sign profile attribute USN** on ACS, but the update of the **USN** attribute directly on ACS is not synchronised with LSS. Some special characters are changed in the JGA/JGU cryptic entry sent by LSS to ACS: • Hyphen (-) is kept on LSS side but is changed into a space character in the JGA/JGU request on ACS. • Period (.) is kept on LSS side but is changed into a space character for the JGA/JGU request on ACS.
First name	Some special characters are changed in the JGA/JGU cryptic entry sent by LSS to ACS: • Letters with and without accents are kept on LSS side but are changed in upper case letters without accent for the JGA/JGU request on the Amadeus central system (example: à is kept on LSS side but becomes **A** in the JGA/JGU request). • Hyphen (-) is kept on LSS side but must be changed into a space character in the JGA/JGU request on the Amadeus central system. • Period (.) is kept on LSS side but must be changed into a space character in the JGA/JGU request on ACS.

Information Tab Field Names	**System Notes**
Phone number	Updates of the UPC attribute directly on ACS are *not* synchronised with LSS. The **Phone number** field is limited to 15 characters (ACS constraint). Some **Special characters** are changed in the JGU request on ACS: • Open-square bracket **[** is kept on LSS side but must be changed to open-parenthesis **(** for the JGA/JGU request on ACS. • Close-square bracket **]** is kept on LSS side but must be changed to close-parenthesis **)** for the JGA/JGU request on ACS. • Slash (**/**) is kept on LSS side but must be changed to period (**.**) for the JGA/JGU request on ACS. • Hyphen (**-**) is kept on LSS side but must be changed to period (**.**) for the JGA/JGU request on ACS. • Underscore (_) is kept on LSS side but must be changed to period (**.**) for the JGA/JGU request on ACS.

Appendix C
Full Locations

Full Locations define the physical location of each workstation and each device in the network.

Full Location Parameters

The concept of a full location is used to describe where a device or a workstation is located. The following convention is used, with the components separated by a slash (/):

Location type/Location code/Site type/Site code/Location category code/Location category index

For example:

A/SYD/T/1/GTE/25

C/NCE/B/A/ADM/105

This example shows a full location when you are working with **Altéa Reservation Desktop** for the office ID NCE6X098R:

C/NCE/B/6X/TRN/098R

Table: Full Location Parameters

Full Location Parameter	Comments	Example
Location type	A - airport code C - city code	A
Location code	The 3-letter airport or city code.	SYD
Site type	If the location type is A, the site type is T (terminal) or B (building). If the location type is C, the site type can only be B (building). **Note:** You cannot use the wildcard character * when you are creating a full location.	T
Site code	Contains a terminal code or a building code. **Note:** You cannot use the wildcard character * when you are creating a full location.	1

Full Location Parameter	Comments	Example
Location category code	Contains the type of location considered. This is an optional parameter. For example: gate. **Note:** You cannot use the wildcard character * when you are creating a full location.	GTE
Location category index	Optional if the location category type is included.	25

Note: You can use the wildcard character ***** when you are searching for full locations, except for the location type and location code, which are always mandatory.

Appendix D

Reference: Codes in Administration History Reports

Code	Description
ACL	Access Control List
AD	Activation date
APP	Application
AR	Address
ATT	Data type
AUT	Authentication type
CT	Comment
DAL	Datalist
DAV	Data value
DSC	Description of the organization
ED	Expiry Date
EM	Email
FN	First name
FR	Freeze
LBL	Label
LG	Login
LN	Last name
MO	Monosign value
OFF	Office
OGU	Organization unit
ORG	Organization
PCD	Delegate change password from login panel value
PEC	Password encryption value
PH	Phone
PP	Password-protected value
PRE	Preference

Code	Description
PTS	Partnership
PWL	Display a change password link value
RFD	Referential data
RLC	Composite role
RLG	Global role
RLU	Unitary role
RO	Robotic value
ROL	Role
RSL	Resiliency value
URL	Change password link value
USR	User

For more information on how to create reports, see *Creating Reports* on page 134.

Glossary

[A](#) [C](#) [D](#) [G](#) [H](#) [I](#) [L](#) [M](#) [O](#) [P](#) [R](#) [S](#) [T](#) [U](#) [V](#)

A

Access control list (ACL)
: The part of a role that determines which data within an application can potentially be accessed by a user who has been assigned the role.

  An ACL must be created under a role, then assigned to a user (or another level of an organization) to provide access to the data within the application.

  Several ACLs can be created for the same role, to provide access to different data sets.

  A user must be assigned both a role and an ACL, to be able to work in an application.

ACE
: **Amadeus Centralised End-user** (**ACE**) maintenance system is an internal Amadeus tool that is used by organizations to create and maintain the following definitions in the Amadeus central system (ACS): office ID and profile, printers, terminals, terminal and printer cross-references, and certificates for Amadeus Selling Platform.

ACL context
: The term used on the history display to indicate an assignment of an ACL.

Amadeus central system (ACS)
: A global distribution system (GDS). It allows users to book and sell tickets for multiple travel-related companies, including airlines, trains, car rentals, cruises, ferries and hotels.

Application
: Amadeus applications that have the access control and authentication controlled by Amadeus Logon and Security Server (LSS).

C

Composite role
: This role type is composed only of sub-roles. It is for a specific application and for one organization, but each of the sub-roles can contain permissions related to a different data type. When a role is created from several sub-roles, it automatically includes all the permissions of each of the sub-roles.

  See also: *Role*.

Consumer
: Any entity in an organization tree to which security rights can be assigned: organization, organization unit, office or user.

D

Datalist
: A type of data set. A grouping of several data values. For example, New York airports, composed of JFK, EWR and LGA.

Data set Data that is defined by an organization's security administrator, which will be used to control which data a user can access. It is specific to an Amadeus application and data type.

For example, it can be flight number ranges in Amadeus Altéa Inventory, or airport board points in Amadeus Altéa Departure Control Customer Management.

A data set can be a data value or a datalist.

Data type A data type defines a type of data that can be accessed within an application. It is defined by the Amadeus application team.

Examples include flight number (FLI) in Amadeus Altéa Inventory, or airport board point (BPT) in Amadeus Altéa Departure Control Customer Management.

Each permission for an application is associated to a data type.

Data value A type of data set. A single item of data, such as LHR (for the board point data type) or 1-200 (for the flight number data type).

Default office When a user has a sign in several offices, one office can be defined as the default office. This office ID is taken by default when the user selects Login and Organization or User ID and organization in the login screen.

Delegated ACL An ACL that has been delegated to another organization as part of a partnership.

Delegated role A role that has been delegated to another organization as part of a partnership.

Delegating organization An organization initiating a partnership.

See also: *Partnership, Receiving Organization.*

G

Generic role A role defined by Amadeus for a generic job description within an application. It can be used by any organization.

A generic role can be unitary (composed of permissions) or composite (composed of generic sub-roles).

See also: *Role*.

Global role A role created by an organization, which is composed of sub-roles only. The sub-roles can be for multiple applications. A global role is for a single organization, but can include roles from a different organization if they have been delegated in a partnership.

See also: *Role*.

H

Hosted model The authentication mode whereby an organization uses the Amadeus Logon and Security Server for both authentication and access control.

See also: *Trusted Mode*.

I

Inheritance Both roles and ACLs can be inherited. That is, if a role or an ACL is assigned to a level in an organization higher than a user, all levels underneath will inherit the role or ACL.

For example, if a role is assigned to an office ID, all users with the office ID have the role assigned to them by inheritance.

L

Login area The list of offices to which a user is linked.

LSS Logon and Security Server. Amadeus' security application (RFD).

M

MHDORM This is the Security & Access Management team (previously known as the Order Management & Security team) to whom you assign LSS requests. They administer credentials for all new customers and participate, define and coach the security setup for new and existing customers. They also ensure that all offices, terminals and users are correctly configured and maintained for all customers.

O

Office An Amadeus office, identified by its office ID. For example, LONBA0100. Each user in an organization is linked at user creation time to an office ID. A single user can be linked to several office IDs if this is required for a user's job function.

Office mask A filter set up at organization level, and optionally at organization units, in an organization tree to control the offices that are added to an organization when creating the organization tree. It consists of three parts: The office code (nine characters), the vendor code (four characters) and the country code (two characters).

At organization level, the office mask is created by Amadeus and cannot be modified or removed later. At organization unit level, the office mask is created by a security administrator belonging to the organization. It can be modified or removed later.

Organization (ORG) A company, such as an airline, a hotel chain or a travel company, that is using one or several Amadeus applications. It is the top node of the organization tree.

Organization unit (OGU) A level in the organization tree hierarchy, below the organization and above the offices.

In relation to partnerships, unless otherwise mentioned, the terms 'organization' and 'organization unit' and are used interchangeably.

P

Partnership An agreement between two organizations that want to share data and job functions for a specific Amadeus application. For example, an airline wishes to delegate its ground handling to another company at certain airport locations.

Partnerships are created and maintained by the organizations involved, without the intervention of Amadeus.

Password Changer tool Used to change your LSS password for one or several specific environments. Requires a valid email address in the LSS user profile. Also depends on the security policy of your organization.

PCI-DSS Payment Card Industry Data Security Standard.

A standard developed by major credit card companies to help organizations that process card payments prevent credit card fraud, hacking and other security issues. A company that processes credit card payments must be PCI-compliant.

Permission A permission corresponds to a specific function within an application. Each permission is defined by the Amadeus application team and is associated to a specific data type. You can set the action-type attribute of the permission to either **Allow** to allow access to the function, or **Disallow** to forbid access to the function.

Permissions must be added to a role so that the permission will be granted to the person who has been assigned the role.

Preference The value of a preference type, which are defined by the security administrator.

Preference type Attributes of an application that can be set so that the application behaves in a certain way. Preference types are defined by the Amadeus application team.

An example is the password attempt default value.

R

Receiving organization An organization benefiting from roles and ACLs created by the delegating organization in a partnership.

See also: *Delegating Organization*, *Partnership.*

Resilience A feature provided only with the delegated flow of the trusted authentication mode. It allows a user who has already been successfully authenticated once to sign in even if the organization's end-user management system is down.

See also: *Trusted Mode*.

RFD LSS application.

Robot user A process set up to access the system and carry out automated tasks on applications. Robot users require rights to access the system, but must be identified to allow for special security handling. They cannot be automatically deleted or locked.

Role A role corresponds to a job function within an organization. A role can be created by the organization, or a generic role (created by the Amadeus application team) can be used. A role is composed of permissions or sub-roles.

A role must be assigned to a user (or a higher level in the organization tree) to grant the permissions in the role to the user.

A user must benefit from both a role and an ACL to be able to work in an application.

See also: *Composite Role*, *Generic Role*, *Global Role*, and *Unitary Role*.

Role context The term used on the history display to indicate an assignment of a role.

S

Services Integrator (SI) The gateway that provides a single entry point into Amadeus applications. It coordinates communication between users and Amadeus applications.

Sign Also called Agent Sign. A 6-character code (four numbers and two letters) that identifies an agent in an office, in the Amadeus central system (ACS). In Amadeus Security Management (ASM), the sign is displayed in the user's **Login Areas** tab.

Single sign on (SSO) A process that enables authenticated users to log on once to have access to multiple applications.

T

Trusted mode The authentication mode whereby an organization uses its own end-user management system for user authentication, and LSS for access control. Two authentication flows exist: the trusted authentication and the delegated authentication.

The trusted authentication flow is used when the application user interface is on the organization's side. The end-user management system checks the password and then requests LSS to open a trusted session.

The delegated authentication flow is used when the application user interface is on Amadeus' side. LSS receives the authentication request, delegates the password check to the organization's end user management system, and then opens a trusted session.

See also: *Hosted Mode, Resilience*.

U

Unitary role A role composed solely of permissions, for a single data type or no data type. It is for a specific application and for one organization.

See also: *Role*.

User Users are the people who use the Amadeus applications. A user is defined within an organization and has a unique user ID. Each user is defined for a specific organization and is linked to an office ID. A user can belong to several offices within the same organization.

See also: *Robot User*.

V

Vendor code A four-character code that identifies the owning market of an office ID and its associated data. The vendor code is stored in the **UVC** field of the office profile in the Amadeus central system (ACS).

Index