SECURE AREA HELP
This document provides an overview about the Secure Area and the key functions of the application.
TABLE OF CONTENTS

1. Value of the Secure Area ................................................................. 3
2. Access options to Secure Area ......................................................... 3
3. Authorization Concept .................................................................. 4
4. Visibility Settings .......................................................................... 5
5. Incident Restricted View ............................................................... 5
6. Secure Area Application ............................................................... 6
6.1 Main elements of the Secure Area ............................................... 7
6.2 Creation of new logon data set ..................................................... 9
1. Value of the Secure Area

- Save storage for logon data.
- Logon data needs to be created only once per system and can then be used for incident processing or other purposes, e.g. consulting, service Delivery, etc.
- The visibility of and the access to the logon data can be restricted by access reason or accessing parties (e.g. SAP or partners)
- Logon data can be changed anytime
- An incident indicates if logon data is stored for the system or not
- All operations on the logon data are tracked in the compliance log

2. Access options to Secure Area

- From an Incident

296529 / 2018 Test Message for Secure Area

System: AP1 - Dublette von Installation 0020659001
Installation: 0020659687 - ERP Standard Support
Component: Test messages for IV / Do not use, SAP internal only (SV-SMG-SUP-TST-IV)
Customer: 1208936 - aPaul Pharma

Access Data Maintained
Connection Closed

296529 / 2018 Test Message for Secure Area

System: AP1 - Dublette von Installation 0020659001
Installation: 0020659687 - ERP Standard Support
Component: Test messages for IV / Do not use, SAP internal only (SV-SMG-SUP-TST-IV)
Customer: 1208936 - aPaul Pharma

Access Data Missing
Connection Closed
• From the Remote Connections Launchpad Application

Open the application and choose a system. In the next screen you can reach the Secure Area via the Maintain Access Data Button in the upper right corner.

3. Authorization Concept

• S-users with authorization 'Edit my Logon Data' can store, display, and change logon data they had previously stored. However, they cannot see the passwords specified by other users and they cannot change logon data stored by other users. SAProuter Passwords can be overridden.

• S-users (e.g. super-administrators) with authorization 'Edit all Logon Data' have full access to create/change/display/delete all stored logon data.

• An authorized S-user can assign specific logon data sets (aka credentials) to a certain incident when creating or working on an incident to restrict the view of user passwords for SAP message processors.
4. Visibility Settings

**Please note.** The initial values for a new record are set that the visibility is not limited. If visibility is to be restricted, the customer must do this individually via the checkboxes.

- The visibility, and usability can be restricted. There are four main features:
  - The option to set the usability for the logon data concerning the incident processing. There are 3 choices:
    - **Unrestricted Incidents** – the logon data can be used for incident processing
    - **No Incidents** – the logon data cannot be used for incident processing
    - **Only Assigned Incidents** – the logon data is only usable for processing of assigned incidents. Unassigned incidents cannot use the logon data.
  - The purpose of logon data sets is to define access reasons, that have access to logon data. Access reason can be Incident Processing, Consulting, Support Service Delivery, Custom Development, Cloud Operation, or Others (free-text field). Access reasons will be recorded in the Log.
  - The overall visibility can be restricted to SAP and/or to SAP 3rd parties (aka partners)
  - Usability is restricted and can be temporary. The Customer can set a timeframe where the logon data is usable. After expiration the logon data will be deleted. The customer can subscribe a notification e-mail

5. Incident Restricted View

When creating or working on an incident, you can assign specific users to an incident. Thus, you can restrict the logon data visible to a specific incident for SAP message processors:
- The message processor can select from the list of currently stored logon data, the ones that are needed to process the incident. Also, logon data from other systems or installations can be selected.
- The restriction refers to credentials only. SAProuter passwords cannot be restricted.
- The restriction allows an SAP employee or a partner to see only the logon data that was assigned the incident, but an indication is available for the SAP employee, that logon data was stored, even when nothing is visible.
- If no user is explicitly assigned to the incident, all logon data that is set to be visible for ‘All incidents’ and ‘SAP’ is visible to the SAP employee

With this modification it is possible that customers can restrict the access of login data to a certain incident by assigning specific logon data. The restriction is valid for the incident. When logon data is assigned to an incident, it will only be visible to incidents that are assigned.
6. Secure Area Application

The application can be used by customers to maintain and provide customer data for "User", "SAP-Routers", "Servers", "Contacts", and "Info" for SAP Support when necessary. It is possible to maintain logon data for all the systems assigned to the same customer. No cross-customer visibility is provided.
6.1 Main elements of the Secure Area

1. **System** shows information about the system that logon data is maintained for.
2. **Incident** - shows information of the incident from which the Secure Area was called.
3. In the free-text field **System Info** general information about the system can be stored.
4. **Credentials** is a table with the stored credentials grouped by Service type

If the Service Type is filled with "Imported: Please Check!" the service type was imported automatically during the migration to UI5, but the Service Type could not be determined automatically. Open the logon data set and enter the edit mode. Here the Service Type can be chosen from a dropdown list. The Service Type maintained in the old Secure Area is visible in the Info section of the credential view.

5. **SAProuter** – Area where SAProuter passwords can be stored. The SAProuters passwords can be maintained after the following scheme:

   I. Main SAProuter
   II. Additional SAProuter
   III. Server SAProuter

   ![SAProuter table]

6. **Switch System** button opens a list of available customer systems. For switching to another system select an item from the list.
7. **Show Log** button The Secure Area Log section displays the logs which can be filtered using date ranges. Logs can also be downloaded from here.

After the migration to UIS it is possible, and strongly recommended, to download the logs of the old Secure Area application. In the new version of the secure area the log format has changed, as there are new features like the new access reasons.

8. **Maintain View Restriction** button

Maintain View Restriction button
Opens a new view where credentials can be assigned to an incident.
6.2 Creation of new logon data set

Entry over the button on the landing page in the Credentials area.

1. Under Logon Data the Service Type can be selected from the dropdown list. Depending on the Service Type the required attributes can be entered.

2. In the section Visibility the usability/visibility of the credential can be defined, as described in chapter 4. Visibility Settings.

3. In the field Contact a contact person can be specified.

4. In the Info box additional info specifically for these credentials can be provided as free-text.