



PUBLIC – Remote Connectivity Program

## **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

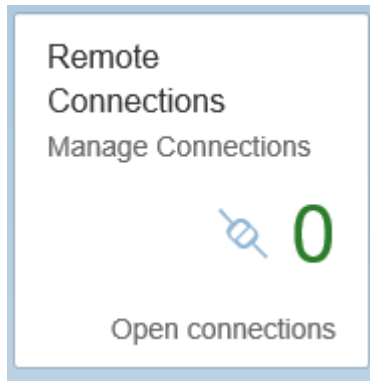
Component: Test messages for IV / Do not use, SAP internal only (SV-SMG-SUP-TST-IV)

Customer: 1208936 - aPaul Pharma

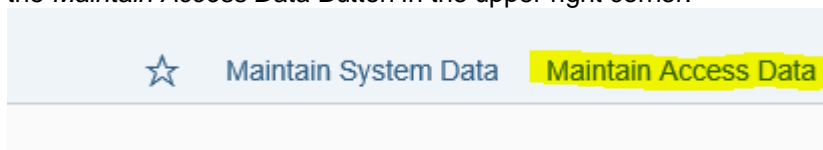
Access Data Missing

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 3<sup>rd</sup> parties (aka partners)
  - Usability is restricted and can be temporary. The Customer can set a timeframe where the logon data is useable. 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.

SAP Secure Area Knowledge Base Enter search term Test Cloud (S0018132424)

Test eines HANA Systems (HN1) Authorized to edit all logon data Switch System Show Log

**System**  
Customer Number: 1208936 System Name: Test eines HANA Systems  
Installation Number: 20689660 System ID: HN1  
Installation Product: SAP ERP System Number: 311669898  
Installation Name: ERP ESsupport System Type: TEST

**Incident**  
Subject: Test Secure Area Password Storage Restricted View  
Incident State: In Processing by SAP  
Incident Priority: Medium  
Component: Test messages to SAP (SV-SMG-SUP-TST)

Visibility: Not Restricted  
Maintain View Restriction

6 7

1 2

System Info Credentials SAProuter

**System Info** Edit Delete  
Endless Info Text.  
TextText.  
Just a text.

3

**Credentials** Add

Service Type	User	Password	Visibility	Delete At	Created By	Last Changed By	Last Changed On
Imported: Please Check!	wtuser	asterix	Not Restricted	31.12.2018, 09:30:59	John Hybrid	Test Hybrid	31.08.2018, 08:05:48
R/3 Support	Zweihundert	200	Not Restricted	25.09.2019, 21:45:00	Test Hybrid	Test Hybrid	10.09.2018, 08:02:59
	Ein hundred	100	Not Restricted	25.09.2018, 21:45:00	Test Hybrid	Test Hybrid	10.09.2018, 08:02:44
	Test	test	Not Restricted	26.09.2018, 11:38:07	Tim S-Buchholz	Tim S-Buchholz	19.09.2018, 11:38:17

**SAProuter** Maintain SAProuters

Router Type	Host Name	IP Address	Port	Password	Delete At	Created By
Main	B1000312154295	111.111.111.124	3242	MainRouter1	24.10.2018, 21:45:01	John Hybrid

SAP Secure Area Knowledge Base Enter search term Christian Bresch (D073552)

Test eines HANA Systems (HN1) Switch System

**System**  
Customer Number: 1208936 System Name: Test eines HANA Systems  
Installation Number: 20689660 System ID: HN1  
Installation Product: SAP ERP System Number: 311669898  
Installation Name: ERP ESsupport System Type: TEST

**Incident**  
Subject: Test Message for Secure Area  
Incident State: Sent to SAP Partner  
Incident Priority: Medium  
Component: Test messages for IV / Do not use, SAP internal only (SV-SMG-SUP-TST-IV)

Visibility: Not Restricted

2

1

System Info Credentials

**System Info**  
Endless Info Text.  
TextText.  
Just a text.

3

**Credentials**

Service Type	User	Server	Created By	Last Changed By	Last Changed On
Imported: Please Check!	Test		Test Hybrid	Test Hybrid	19.09.2018, 17:42:36
R/3 Support	Banana	adminconsole-1	Tim S-Buchholz	Tim S-Buchholz	24.09.2018, 11:19:06
	Wunderbar		Test Hybrid	Test Hybrid	24.09.2018, 11:24:08

4

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.

Logon Data

\*Service Type:

\*User:

AS/400-5250 Connection

\*Password:

Citrix Metaframe

DB-Connect

EarlyWatch

\*Delete At:

HTTP Connect - URLAccess

Incident Processing:

HTTP-based Tools

Useable for:

JDBC/ODBC Connection

R/3 Support





Visibility

- 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

Maintain SAProuters

Router Type	Host Name	IP Address	Port	Password	Delete At	Created By	
Main	B1000312154295	111.111.111.124	3242	MainRouter1	24.10.2018, 21:45:01	John Hybrid	 
Additional	addrouter	2001:0db8:85a3:08d3:1319:8a2e:0370:7344	3299	AddRouter	31.12.2018, 22:45:01	John Hybrid	 

Server SAProuter

Server Host Name	Host Name	IP Address	Port	Password	Delete At	Created By	
dbtest	dbthirdrouter		3299				 
adminnnnnnn.1	AdditionalIP	111 111 111	3299				 

- 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** 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.

**Secure Area Log**

System

Customer Number: 1208936 System Name: Test eines HANA Systems  
 Installation Number: 20689660 System ID: HN1  
 Installation Product: SAP ERP System Number: 311669898  
 Installation Name: ERP ESupport System Type: TEST

**Secure Area Log** **Old Secure Area Log**

Access Log (125/292) Date Range: dd.MM.yyyy - dd.MM.yyyy Search

Accessed By	Last Accessed On (UTC)	Type	Operation	Service Type	User	Incident Number	Access Reason
SAP Support	19.09.2018, 12:23:19	Logon Data	Read	Main SAProuter	B1000312154295		
SAP Support	19.09.2018, 12:23:19	Logon Data	Read	Additional SAProuter	addrouter		

- ! After the migration to UI5 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** *Maintain View Restriction* button  
 Opens a new view where credentials can be assigned to an incident.

**Assign Credentials To Incident 121821 2018**

Not Restricted Incident


Subject: Test Secure Area Password Storage Restricted View Incident State: In Processing by SAP  
 Customer: 1208936 - aPaul Pharma Incident Priority: Medium  
 Installation: 0020689660 - ERP ESupport Component: Test messages to SAP (SV-SMG-SUP-TST)  
 System: HN1 - Test eines HANA Systems

0 Credentials Assigned Search

User	Service Type	System ID	Visibility	Last Changed By	Last Changed On	Delete At
<input type="checkbox"/> DDIC	R/3 Support	AP1	Assigned	Test Hybrid	23.07.2018, 07:28:42	31.12.9999, 23:45:01 >



## 6.2 Creation of new logon data set

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

**New Entry**

Credential	System
Last Changed By:	Customer Number: 1208936
Last Changed On:	Installation Number: 20689660
Created By:	Installation Product: SAP ERP
Created On:	Installation Name: ERP ESupport
	System Name: Test eines HANA Systems
	System ID: HN1
	System Number: 311669898
	System Type: TEST

**Logon Data**

1

\*Service Type:

\*User:

\*Password:

**Visibility**

2

\*Delete At:

Incident Processing: ☒ All Incidents ☐ No Incidents ☐ Only Assigned Incidents

Useable for: ☒ Consulting ☒ Support Service Delivery ☒ Custom Development

☒ Cloud Operation ☒ Others

\*Visibility: ☒ SAP ☒ SAP 3rd parties

**Contact**

3

User ID:

**Info**

4

Additional Info:

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.

[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. See [www.sap.com/copyright](http://www.sap.com/copyright) for additional trademark information and notices.

**THE BEST RUN**

