SECURITY GUIDE | PUBLIC
Document Version: 2.1 – 2020-03-25

Security Guide for SAP Focused Run

THE BEST RUN SAP

Content

1 SAP Focused Run Security Guide

Introduction to the Security Guide

> ⚠ Caution
>
> This guide has a security focus. It does not replace this product's Master Guide or other available guides for productive operation.

Target Audience

- Technical consultants
- System administrators

The security concept of SAP Focused Run is designed to provide a secure infrastructure within IT environments. IT environments discussed here typically have a central administration network and managed systems in separate network segments.

We recognize that systems, networks, and IT security infrastructures are unique according to each customer's needs and specifications. This means that this guide can only describe the features of SAP Focused Run based on past experiences and best practices.

This guide contains many answers to general questions about how to apply customer security policies. If you would like an in-depth discussion about how to apply specific customer security policies, please contact us directly at focused.solutions@sap.com. In most cases, we find this direct contact to be more efficient than an exchange via customer tickets. We can arrange a short face-to-face discussion with our experts or set up "SAP Focused Run Architecture and Project Setup Workshop" to discuss your unique security-relevant questions in detail.

Table of Contents

Related Information

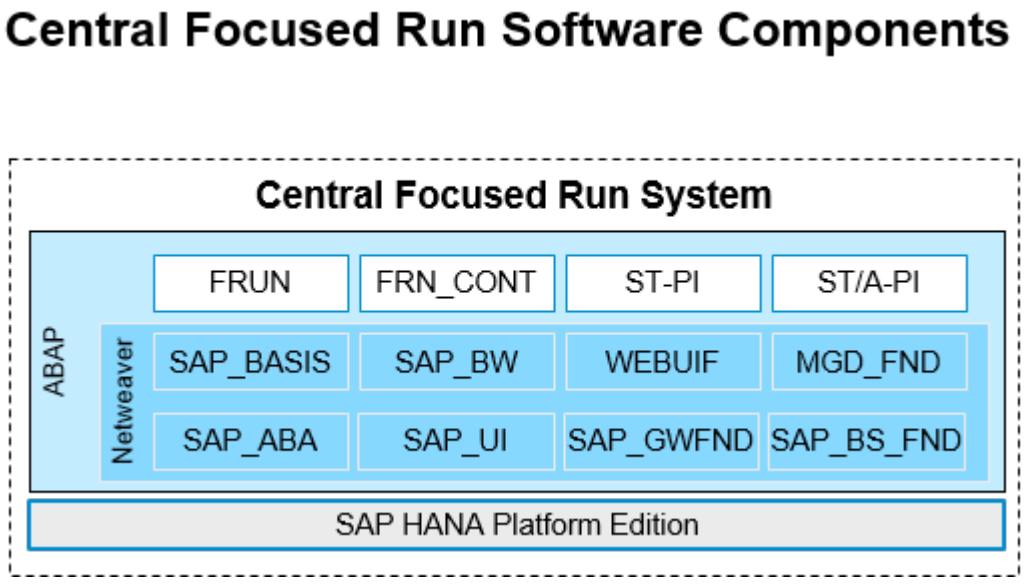
SAP NetWeaver Security Guide

2 Technical System Landscape

Overview of technical components relevant for SAP Focused Run

Central SAP Focused Run (ABAP on SAP HANA)

SAP Focused Run is a suite of ABAP applications running on a NW ABAP application server. The ABAP system receives and processes all incoming managed system metrics and other collected data. This central ABAP application service also provides all SAP Focused Run application user interfaces. SAP Focused Run is optimized for SAP HANA. The SAP HANA DB saves all managed system metrics and other collected data, as well as SAP Focused Run administrative data.



Central SAP Focused Run software components

For further information, see the product page for SAP Focused Run: https://support.sap.com/en/solution-manager/focused-solutions/focused-run.html

See also Technical Operations for SAP NetWeaver in SAP Help Portal: https://help.sap.com/viewer/DRAFT/3a49a58accb3464ca80d4bb309312204/latest/en-US

SAP Hostagent

Short form: SHA

SHA is installed on every host of a managed system. It acts as proxy for all requests sent to the simple diagnostics agent. SHA installs and upgrades the simple diagnostics agent on hosts of a managed system, and provides runtime control (start/stop). SHA provides the outside discovery in SAP Focused Run.

While not delivered as part of SAP Focused Run, SHA is used by SAP Focused Run and is necessary for SAP Focused Run operations.

For more information, see SAP Host Agent in SAP Help Portal: https://help.sap.com/viewer/3ce0859db2164fe19541dda577d29020/latest/en-US

Simple Diagnostics Agent

Short form: SDA

SDA is installed as a java plug-in of SHA on every host of a managed system. SDA is the runtime container of SAP Focused Run data collection applications.

SDA is part of the SAP Focused Run delivery.

For more information, see Simple Diagnostics Agent in SAP Focused Run Expert Portal: https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/simple-system-integration-ui-user-guide.html

System Landscape Data Router

Short form: SLDR

SLDR distributes SLD DS payloads. It is an agent application, available in each SDA. The SLDR is activated and configured centrally in the Agent Administration.

For more information, see SLD in the SAP Focused Run Expert Portal: https://support.sap.com/en/solution-manager/focused-solutions/focused-run-expert-portal/managed-systems-maintenance-guide/preparing-system-landscape-data-router.html

Managed System

Also known as: Managed Object (MO)

MOs are hosts, databases, instances, and systems. As associated with SAP Focused Run infrastructure, MOs have varying security requirements for users and other security-relevant features.

This guide contains information about determining authorizations when creating users for SAP Focused Run.

Customer Cloud Account

Also known as: Managed Cloud

SAP Focused Run provides cloud monitoring. SAP Focused Run connects with a technical user, provided that user exists in the customer's cloud account.

For the creation of this kind of user, please see the relevant cloud product documentation.

Support Tool Plug-In

Short forms: ST-PI, ST/A-PI

In general, function modules and roles/authorizations are developed for support with SAP Solution Manager. Certain function modules and roles/authorizations are developed specifically for SAP Focused Run. For this reason, ST-PI and ST/A-PI in the managed ABAP systems must be kept up to date. This updated information is released with SAP Focused Run feature pack.

CA Application Performance Measurement Enterprise Manager

Short form: CA APM EM

> **i** Note
>
> Outdated forms: Wily, Wily Introscope. (In March 2006, CA purchased Wily Technology, Inc.)

CA APM EM is temporary staging data collected by the different bytecode injection agents. CA APM EM sends this data to SAP Focused Run based on central configuration of SAP Focused Run.

CA APM EM OEM license is part of SAP Solution Manager.

For more information, see RCA Introscope Home: https://wiki.scn.sap.com/wiki/display/TechOps/RCA_Introscope_Home

Open Source Statistical Language R (optional)

Short form: R

SAP Focused Run application *System Anomaly Prediction* is implementing advanced statistical models written in R. This requires R runtime on dedicated hosts and integration of this R runtime with the SAP HANA DB

For more information, see SAP HANA R Integration Guide for System Anomaly Prediction: https://support.sap.com/content/dam/support/en_us/library/ssp/sap-solution-manager/focused-solutions/frun-r-setup-system-anomaly-prediction-100-suse-linux-sles-12-sp03.pdf

See also SAP HANA R Integration Guidehttps://help.sap.com/viewer/a78d7f701c3341339fafe4031b64f015/latest/en-US/dbad714484d242789688a551fbdf5573.html

Reverse Proxy (function can be provided by SAP Web Dispatcher)

The reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers.

In SAP Focused Run infrastructure, a reverse proxy retrieves resources on behalf of the agents and managed systems from SAP Focused Run. SAP Focused Run uses proxy functions for header modification to grant strong data separation.

SAP Web Dispatcher can provide such reverse proxy functionality. SAP Web Dispatcher provides access to SAP Fiori UI and can be used as reverse proxy.

There are other different third-parties providing the needed reverse proxy functionality. Of these, the best known is the Apache HTTP server.

For more information, see SAP Web Dispatcher in SAP Help Portal: https://help.sap.com/viewer/683d6a1797a34730a6e005d1e8de6f22/latest/en-US/4899d142ee2b73e7e10000000a42189b.html

See also Apache Http Server Project: https://httpd.apache.org/

Load Balancer (function can be provided by SAP Web Dispatcher)

Short form: LB

SAP Focused Run is commonly installed with multiple-application servers for high-availability and load-distribution purposes.

SAP Focused Run supports third-party hardware and software load balancer (see vendor documentation). SAP Web Dispatcher can provide software load balancing functionality.

for more information, see SAP Web Dispatcher in SAP Help Portal:https://help.sap.com/viewer/683d6a1797a34730a6e005d1e8de6f22/latest/en-US/4899d142ee2b73e7e10000000a42189b.html

HTTP Proxy

In SAP Focused Run infrastructure, a HTTP proxy server acts as an intermediary for requests from SAP Focused Run central system to SHA (optional, depending on customer network security implementation).

There are different third-party proxies. SAP Web Dispatcher does not support the HTTP request command *connect* and therefore cannot not act as a proxy in the common meaning.

There are other third-parties providing the needed reverse proxy functionality. Of these, the best known is the Apache HTTP server.

For more information, see Apache HTTP Server Project: https://httpd.apache.org/

Other Network Appliance

Examples: (smart) Firewall, NAT, VPN

SAP Focused Run incoming and outgoing communication with a MO is conducted via HTTP application protocol only. This means relates to IP/TCP setting, like hostname resolution and open ports. Lower-level network appliances (VPN, NAT, Firewall) are supported.

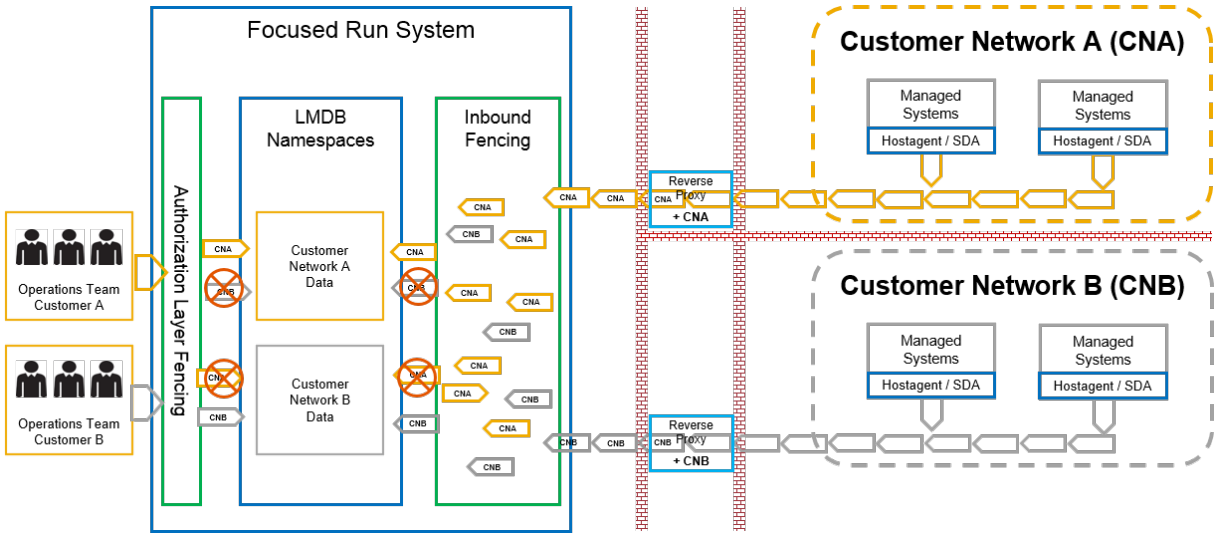
3 Data Separation

Use

In a segmented network environment, it is common that different networks have different security policies. For example, a host provider might entrust the security policy for the hosted systems to the hosted customer. To support this, SAP Focused Run provides strong data-separation capabilities. If a customer network is compromised, the central component that is SAP Focused Run ensures that no other connected network/ system can be compromised. Data separation is a main pillar to protect customer data against threats such as information disclosure and data tampering.

Brief Architecture

The below figure illustrates the idea behind data separation in SAP Focused Run. All managed object configurations are network/customer specific. All reported metrics and data can only be sent specifically to one network/customer. The reverse proxy plays an important role in this concept. The reverse proxy **must not** be open to the customer network. All ports except HTTP(S) are assumed to be closed by firewall. On the reverse proxy, an "inbound fencing" string is added to all requests from that network. This inbound fencing string is mapped to the customer-network identification. SAP Focused Run checks whether a configuration exists for this metric and network for each incoming request, if not, the request is rejected.



SAP Focused Run Data Separation

> ### Note
>
> Without the reverse proxy, no inbound fencing is possible in SAP Focused Run, and no data separation can be applied. SAP Focused Run also has a special customer network that does not require a reverse proxy: *LOCALNETWORK*. Though initially intended to be used for self-monitoring of SAP Focused Run and other IT tools, *LOCALNETWORK* can also be used if no data separation is desired.

- Service for HTTP Inbound of Monitoring Data [page 11]
  Lists SICF services' URLs and functions, as background for the rewriting rules.
- Enable Strong Data Separation at Data Collection Time [page 12]
  Explains the reverse proxy functionality.
- SAP Web Dispatcher [page 13]
  Provides samples for SAP Web Dispatcher configurations.
- Apache [page 15]
  Samples for Apache configurations

3.1 Service for HTTP Inbound of Monitoring Data

Use

Familiarize yourself with the SICF services and their purposes.

SICF Service

The listed SICF services, if utilizing data separation, must be configured on the reverse proxies to enable strong data separation.

URL	Function	Description
/lmdb/ds	Entry point for SLD DS	SLD DS payload transmits directly to SAP Focused Run using this service.
/sld/ds	Entry point for SLD DS	SLD DS payload transmits directly to SAP Focused Run using this service. Same service as /lmdb/ds with a different alias.
/sap/srsm_mai/push_metrics	Entry point for all monitoring and RCA metrics	Metrics collected by the simple DA monitoring aglet and the CA APM EM are sent to this service.
/sap/bc/rest/cof/COF_SEND_TO_SRSM/	Entry point for all configuration and security analysis data	Configuration data from the different configurations stores are collected as snapshot every 24 hours and sent to this service.
/sap/bc/sdf/sdcc/	Entry point for all ABAP EWA data	The ABAP SDCC data collector sends data collected for ABAP EWA to this service (among all non-ABAP EWA

URL	Function	Description
		data, it is calculated from the monitoring data).
/sap/bc/rest/e2e_ta_col	Entry point of data that is collected for E2E trace analysis	E2E trace data collected by the simple diagnostics agent is sent to this service.
/sap/srsm/E2E_trace_upl	Entry point for E2E TA recordings by SAPUI5 diagnostics	Recorded SAPUI5 sessions are uploaded to SAP Focused Run by this service.
/sap/bc/rest/rumdataservice	Entry point for real user monitoring data	Header data as well as statistical recode data of recorded user requests are uploaded to SAP Focused Run by this service.
/sap/bc/rest/aimdataservice	Entry point for advanced interface monitoring data	Header data as well as statistical recode data of recorded electronic requests are uploaded to SAP Focused Run by this service.
/sap/bc/rest/statraggdatasrv	Entry point for collection of aggregated statistical data from ABAP	Collected for long-term analysis and predictions.
/sap/bc/rest/sumdataservice	Entry point for synthetic user monitoring data	Script executions are reported to SAP Focused Run by this service.
/sap/bc/rest/rcadataservice	Entry point for system analytics data	Collection of "ABAP work process overview" and "SAP HANA thread samples" if enabled for system analytics.
/sap/bc/rest/rca_gs	Entry point for root cause analysis generic storage	Collection of generic data (such as from Dynatrace or custom scripts)

For more information about web service activation, see the SAP Focused Run Master Guide 2.0.

3.1.1 Enable Strong Data Separation at Data Collection Time

Configure header modification operations in the reverse proxy.

To enable strong data separation with reverse proxy, the inbound fencing parameter must be set as part of the reverse path configuration. Adding this inbound fencing parameter to the URL requires a modification of the HTTP request header by the reverse proxy.

> ⚠ Caution
>
> The inbound fencing URI parameter `?smgwa` is case-sensitive.

<AdmReqParam> (in the script below) is equal to the *Admin Request Parameter* as set at creation of a customer network.

The syntax of the modification rule are specific to the vendor of the proxy:

For full documentation of SAP Web Dispacher, see:https://help.sap.com/viewer/683d6a1797a34730a6e005d1e8de6f22/latest/en-US/488fe37933114e6fe10000000a421937.html.

For SAP Web Dispatcher sample configurations, see: SAP Web Dispatcher [page 13]

For full documentation of Apache HTTP server, see: http://httpd.apache.org/docs/2.4/howto/reverse_proxy.html

For Apache HTTP server sample configurations, see: Apache [page 15]

3.1.1.1 SAP Web Dispatcher

Configure SAP Web Dispatcher as reverse proxy for SAP Focused Run

Procedure

1. Declare SAP Focused Run in the SAP Web Dispatcher with profile parameter: `wdisp/system_<nr>`

   Syntax

   ```
   wdisp/system_<X>= SID=<SID>, SRCURL=/, SSL_ENCRYPT=0, CLIENT=<default
   client>, EXTSRV=<FOCUSED RUN Host>:<FOCUSED RUN HTTP Port>
   ```

   → Tip

   The parameter is `webdisp/system_<X>` for SAP Focused Run after applying settings for Web Assistance. The`webdisp/system_2` lower numbers and `webdisp/system_0`, `webdisp/system_1` are needed for the Web Assistance of the SAP Fiori applications of SAP Focused Run.

   Example incl. `wdisp/system_<X>` for in-application help.

   Sample Code

   Example incl. in in-application help

   ```
   wdisp/system_0 = SID=FR0, EXTSRV=https://cp.hana.ondemand.com,
   SRCURL=/sap/dfa/help/, SRCSRV=*:*, PROXY=proxy:8080,
   STANDARD_COOKIE_FILTER=OFF
   wdisp/system_1 = SID=FR1, EXTSRV=https://xray.hana.ondemand.com, SRCURL=/
   resources/sap/dfa/help/, SRCSRV=*:*, PROXY= proxy:8080,
   STANDARD_COOKIE_FILTER=OFF
   wdisp/system_2 = SID=FRP, MSHOST=myhost, MSPORT=8143, SSL_ENCRYPT=1,
   SRCURL=/, CLIENT=<default client>, EXTSRV=<FOCUSED RUN Host>:<FOCUSED RUN
   HTTP Port>
   ```

2. Configure the rewriting rules to be applied for the URLs in a dedicated file. The parameter is `icm/HTTP/mod_<Nr>`. You need to create a file **rules.txt** in your profile directory.

   Example

   ```
   icm/HTTP/mod_0 = PREFIX=/, FILE=$(DIR_PROFILE)/rules.txt
   ```

   Or

   Sample Code

   ```
   icm/HTTP/mod_0=PREFIX=/,FILE=/usr/sap/WEB/W01/rules.txt
   ```

   a. Create the **rules.txt** at the destination defined with parameter `icm/HTTP/mod_<X>`.

      The file **rules.txt** contains rules to be applied for the modification of user requests.

      Replace the <AdmReqParam> in the sample code with the admin request parameter as defined at customer network creation.

      Sample Code

      ```
      # allow Web Admin UI
      if %{PATH} regimatch ^/sap/wdisp/admin
      nop [break]
      # Rewrite rules
      RegIRewriteRawUrl ^/sap/bc/sdf/sdcc/$ /sap/bc/sdf/sdcc/?
      smgwa=<AdmReqParam> [qsreplace,break]
      RegIRewriteRawUrl ^/sld/ds$ /sap/bc/cim/ds?smgwa=<AdmReqParam>
      [qsreplace,break]
      RegIRewriteRawUrl ^/sap/srsm_mai/push_metrics/$ /sap/srsm_mai/
      push_metrics?smgwa=<AdmReqParam> [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/cof/COF_SEND_TO_SRSM/$ /sap/bc/rest/cof/
      COF_SEND_TO_SRSM?smgwa=<AdmReqParam> [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/e2e_ta_col/AgentCollector$ /sap/bc/rest/
      e2e_ta_col/AgentCollector?smgwa=<AdmReqParam> [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/rumdataservice/records$ /sap/bc/rest/
      rumdataservice/records?smgwa=<AdmReqParam>  [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/aimdataservice/data$ /sap/bc/rest/
      aimdataservice/data?smgwa=<AdmReqParam>  [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/statraggdatasrv/records$ /sap/bc/rest/
      statraggdatasrv/records?smgwa=<AdmReqParam>  [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/sumdataservice/records$ /sap/bc/rest/
      sumdataservice/records?smgwa=<AdmReqParam>  [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/rcadataservice$ /sap/bc/rest/
      rcadataservice?smgwa=<AdmReqParam>  [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/rca_gs$ /sap/bc/rest/rca_gs?
      smgwa=<AdmReqParam>  [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/ajmruntimesrv/data$ /sap/bc/rest/
      ajmruntimesrv/data?smgwa=<AdmReqParam> [qsreplace,break]
      RegIRewriteRawUrl ^/sap/bc/rest/ajmmetadatasrv/data$ /sap/bc/rest/
      ajmmetadatasrv/data?smgwa=<AdmReqParam> [qsreplace,break]
      # Reject all other URLs
      #RegForbiddenUrl ^(.*) - [break]
      ```

   You can define multiple customer networks with one SAP Web Dispatcher. To do so, configure different ports. Port-dependent rewrite rules are in the same rules.txt:

   Sample Code

   ```
   # Rewrite rules
   ```

```
if %{SERVER_PORT} = 8080
begin
RegIRewriteRawUrl ^/sap/bc/sdf/sdcc/$ /sap/bc/sdf/sdcc/?
smgwa=<AdmReqParam> [qsreplace,break]
RegIRewriteRawUrl ^/sld/ds$ /sap/bc/cim/ds?smgwa=<AdmReqParam>
[qsreplace,break]
RegIRewriteRawUrl ^/sap/srsm_mai/push_metrics/$ /sap/srsm_mai/
push_metrics?smgwa=<AdmReqParam> [qsreplace,break]
RegIRewriteRawUrl ^/sap/bc/rest/cof/COF_SEND_TO_SRSM/$ /sap/bc/rest/cof/
COF_SEND_TO_SRSM?smgwa=<AdmReqParam> [qsreplace,break]
RegIRewriteRawUrl ^/sap/bc/rest/e2e_ta_col/AgentCollector$ /sap/bc/rest/
e2e_ta_col/AgentCollector?smgwa=<AdmReqParam> [qsreplace,break]
RegIRewriteRawUrl ^/sap/bc/rest/rumdataservice/records$ /sap/bc/rest/
rumdataservice/records?smgwa=<AdmReqParam>  [qsreplace,break]
RegIRewriteRawUrl ^/sap/bc/rest/aimdataservice/data$ /sap/bc/rest/
aimdataservice/data?smgwa=<AdmReqParam>  [qsreplace,break]
RegIRewriteRawUrl ^/sap/bc/rest/statraggdatasrv/records$ /sap/bc/rest/
statraggdatasrv/records?smgwa=<AdmReqParam>  [qsreplace,break]
RegIRewriteRawUrl ^/sap/bc/rest/sumdataservice/records$ /sap/bc/rest/
sumdataservice/records?smgwa=<AdmReqParam>  [qsreplace,break]
RegIRewriteRawUrl ^/sap/bc/rest/rcadataservice$ /sap/bc/rest/
rcadataservice?smgwa=<AdmReqParam>  [qsreplace,break]
if %{SERVER_PORT} = 8081
begin
…
end
RegForbiddenUrl ^(.*) - [break]
```

⚠ Caution

Please note that the service implementation of `sdcc` requires a slash before the question mark. `/sdcc/?smgwa`. In general, the syntax is sensible for unintended <cr>, <space>, or hidden characters you might not see in your editor.

→ Tip

You can also create other rewriting rules not based on listening ports of the reverse proxy. Customer rewriting rules can be based on elements in the distinguished name in the client certificate or based on the IP subnet.

3.1.1.2 Apache

Context

Configure Apache HTTP Server as reverse proxy for SAP Focused Run.

Procedure

1. In your **http_conf**, load at least the module: `rewrite_module`.

   > **i Note**
   >
   > Which modules (mods) to load and how to configure Apache HTTP server as reverse proxy with logging and SSL termination is not covered by this SAP Focused Run security guide. Please see Apache documentation here: https://httpd.apache.org/docs/2.4/ .

   > **Sample Code**
   >
   > In **http_conf**

   ```
   ...
   LoadModule rewrite_module modules/mod_rewrite.so
   ...
   ```

2. In your **http_conf**, consider defining a virtual host configuration file to have a dedicated location for your rewriting rules. This is a best practice recommendation, rather than a mandatory requirement. The path given in the **http_conf** is relative to the Apache installation directory.

   > **Sample Code**
   >
   > In **http_conf**

   ```
   ...
   # Virtual hosts
   Include vhosts/myServer_proxy.conf
   Include vhosts/myServer_reverse_proxy.conf
   ...
   ```

3. Create the rewriting rules in `vhosts/myServer_proxy.conf`.

   Replace the <AdmReqParam> in the sample code with the Admin request parameter as defined at customer network creation. Below example is for two customer networks with two listening ports: 8001 and 8002.

   > **Sample Code**
   >
   > `vhosts/myServer_proxy.conf`

   ```
    Define SRVROOT "C:/Apache24"
   ServerRoot "${SRVROOT}"
   Listen 8001
   Listen 8002
   <VirtualHost *:8001>
       ServerName MyServer
       LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost_common
       LogLevel alert rewrite:trace3
       ErrorLog logs/8001.error.log
       CustomLog logs/8002.access.log vhost_common
       ProxyTimeout 1200
       Timeout 1200
       <IfModule mod_rewrite.c>
           ReWriteEngine            on
       # RewriteCond %{QUERY_STRING} ^(.*|\?|&|%26|%20)smgwa(=|%3D)[^&]+(.*)$
       ReWriteRule ^/sld/ds$ http://<host>:<port>/sld/ds?smgwa=<AdmReqParam>
   [P,NC,L]
   ```

```
    ReWriteRule ^/lmdb/ds$ http://<host>:<port>//lmdb/ds?
smgwa=<AdmReqParam> [P,NC,L]
    ReWriteRule ^/sap/srsm_mai/push_metrics/$ http://<host>:<port>//sap/
srsm_mai/push_metrics?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/cof/COF_SEND_TO_SRSM/$ http://
<host>:<port>//sap/bc/rest/cof/COF_SEND_TO_SRSM?smgwa=<AdmReqParam>
[P,NC,L]
    ReWriteRule ^/sap/bc/sdf/sdcc/$ http://<host>:<port>//sap/bc/sdf/sdcc/?
smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/e2e_ta_col/AgentCollector/$ http://
<host>:<port>//sap/bc/rest/e2e_ta_col/AgentCollector?smgwa=<AdmReqParam>
[P,NC,L]
    ReWriteRule ^/sap/srsm/E2E_trace_upl$ http://<host>:<port>//sap/srsm/
E2E_trace_upl?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/rumdataservice$ http://<host>:<port>/sap/bc/
rest/rumdataservice?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/aimdataservice/data$ http://
<host>:<port>/sap/bc/rest/aimdataservice/data?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/statraggdatasrv/records$  http://
<host>:<port>/sap/bc/rest/statraggdatasrv/records?smgwa=<AdmReqParam>
[P,NC,L]
    ReWriteRule ^/sap/bc/rest/sumdataservice$ http://<host>:<port>/sap/bc/
rest/sumdataservice?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/rcadataservice/data$  http://
<host>:<port>/sap/bc/rest/rcadataservice/data?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/rca_gs$  http://<host>:<port>/sap/bc/rest/
rca_gs?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/ajmruntimesrv/data$ http://
<host>:<port>/sap/bc/rest/ajmruntimesrv/data?smgwa=<AdmReqParam> [P,NC,L]
    ReWriteRule ^/sap/bc/rest/ajmmetadatasrv/data$ http://
<host>:<port>/sap/bc/rest/ajmmetadatasrv/data?smgwa=<AdmReqParam> [P,NC,L]
<VirtualHost *:8002>
    ServerName MyServer
    LogFormat "%v %h %l %u %t \"%r\" %>s %b" vhost_common
    LogLevel alert rewrite:trace3
    ErrorLog logs/8002.error.log
    CustomLog logs/8002.access.log vhost_common
    ProxyTimeout 1200
    Timeout 1200
    <IfModule mod_rewrite.c>
        ReWriteEngine            on
    # RewriteCond %{QUERY_STRING} ^(.*|\?|&|%26|%20)smgwa(=|%3D)[^&]+(.*)$
    ReWriteRule ^/sld/ds$     http://<host>:<port>/sld/ds?
smgwa=<AdmReqParam> [P,NC,L]
    ReWriteRule ^/lmdb/ds$       http://<host>:<port>//lmdb/ds?
smgwa=<AdmReqParam> [P,NC,L]
    ReWriteRule ^/sap/srsm_mai/push_metrics/$   http://<host>:<port>//sap/
srsm_mai/push_metrics?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/cof/COF_SEND_TO_SRSM/$   http://
<host>:<port>//sap/bc/rest/cof/COF_SEND_TO_SRSM?smgwa=<AdmReqParam>
[P,NC,L]
    ReWriteRule ^/sap/bc/sdf/sdcc/$     http://<host>:<port>//sap/bc/sdf/
sdcc/?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/e2e_ta_col/AgentCollector/$ http://
<host>:<port>//sap/bc/rest/e2e_ta_col/AgentCollector?smgwa=<AdmReqParam>
[P,NC,L]
    ReWriteRule ^/sap/srsm/E2E_trace_upl$  http://<host>:<port>//sap/srsm/
E2E_trace_upl?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/rumdataservice$  http://<host>:<port>/sap/bc/
rest/rumdataservice?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/aimdataservice/data$  http://
<host>:<port>/sap/bc/rest/aimdataservice/data?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/statraggdatasrv/records$  http://
<host>:<port>/sap/bc/rest/statraggdatasrv/records?smgwa=<AdmReqParam>
[P,NC,L]
    ReWriteRule ^/sap/bc/rest/sumdataservice$  http://<host>:<port>/sap/bc/
rest/sumdataservice?smgwa=<AdmReqParam>  [P,NC,L]
```

```
    ReWriteRule ^/sap/bc/rest/rcadataservice/data$  http://
<host>:<port>/sap/bc/rest/rcadataservice/data?smgwa=<AdmReqParam>  [P,NC,L]
    ReWriteRule ^/sap/bc/rest/rca_gs$  http://<host>:<port>/sap/bc/rest/
rca_gs?smgwa=<AdmReqParam>  [P,NC,L]
```

⚠ Caution

Please note that the service implementation of `SDCC` requires a slash before the question mark `/sdcc/?smgwa`. In general, the syntax is sensible for unintended <cr>, <space>, or hidden characters you might not see in your editor.

→ Tip

You can also create other rewriting rules not based on listening ports of the reverse proxy. Customer rewriting rules can be based on elements in the distinguished name in the client certificate or based on the IP subnet.

4 Network and Communication Security

Use

Your network infrastructure is extremely important in protecting your *technical system landscape*. Your network must support the communication necessary for your business and your needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the SAP system database or files. Additionally, if users are not able to connect to the server LAN, they cannot exploit well-known bugs and security holes in network services on the server machines.

Again, your strategy and your priorities are the most important factors in deciding which level of security is necessary for your network infrastructure. We offer general recommendations when establishing your network topology, which includes using a firewall and other intermediary devices. SAP Focused Run implements **SAP Web Dispatcher** and **SAProuter** to **SAP Backbone** for protecting your local network. The use of an SAP Web Dispatcher enables you to conceal the host name and ports of your application server as well as enable SAP Focused Run data separation.

To protect SAP system communications at the transport layer, SAP NetWeaver products support the use of the Secure Sockets Layer (SSL) protocol and Secure Network Communications (SNC).

> **i** Note
>
> Depending on your current situation, you may not be able to implement the described secure network setup. However, we offer suggestions and recommendations at various security levels. If the plan described here does not fit your needs, contact our consultants, who are available to assist you in setting up your network securely.

4.1 Channel Simplification

Simplify communication between the central SAP Focused Run ABAP application server and the agent, the managed ABAP system and the CA APM EM, by using as application protocol HTTP only.

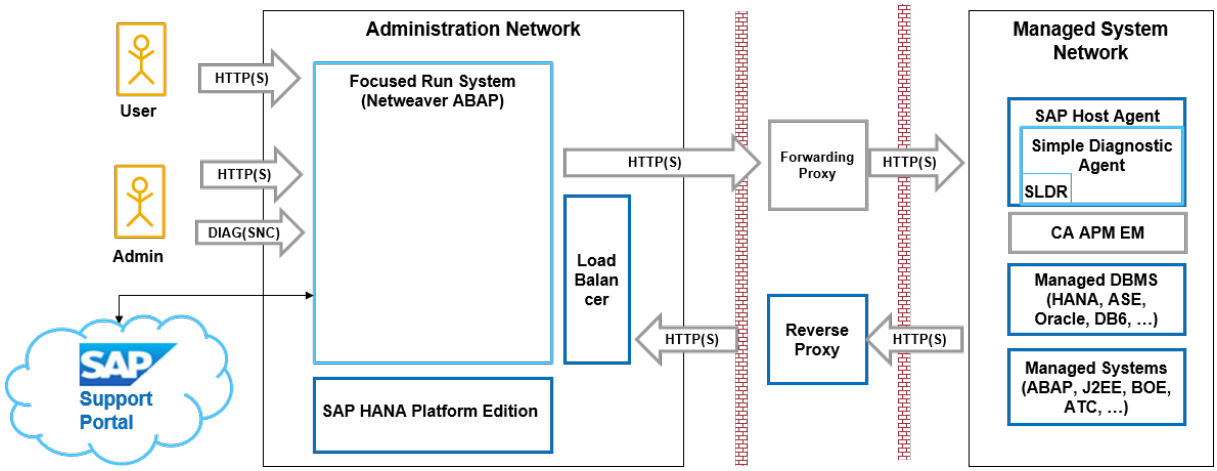
> **i** Note
>
> The communication of SAP Focused Run with the managed system networks is bi-directional.

This means you need to open only two ports in your firewall. From SAP Focused Run to the managed system network, open the port to call the SAP Host Agent. From the managed system to SAP Focused Run, open the port to call SAP Focused Run load balancer. Details are implementation-dependent.

Communication involving SAP Focused Run and the managed system support, by default, most common features for improving network security. Below, you can find a list of the most common features we face during

the rollout of SAP Focused Run. This list and the accompanying figure include common features, but not all supported features. For more information, please contact us with technical inquiries via a support ticket on component SV-FRN-*.

- Physical and Logical Separation of Network Segments
- Forwarding-, Reverse-, Reverse Invocation Proxy
- Separation of Domain Name Server (DNS)
- Name Address Translation (NAT)
- Firewalls on Network and Application layer
- Virtual Private Networks (VPN)



Communication Channel Simplification

> ⚠ Caution
>
> Please consider SAP Focused Run infrastructure landscape management for hostname resolution. For standards on resolving hostnames, see:
>
> - 611361 Hostnames of ABAP platform servers
> - 962955 Use of virtual or logical TCP/IP host names

4.2 Transport Layer Security

Use

This involves documenting client/server relationships, which communicate via the simplified channels or on the local on the managed hosts, and determining what is security-relevant. An understanding of this is necessary to decide which of the communications you would like to secure by encryption.

Connection Type and Communication Between SAP Focused Run and Managed Systems

All communication between SAP Focused Run and managed systems uses HTTP, as described here: Channel Simplification [page 19]. Communication can be encrypted via supporting TLS 1.2 protocols. This is commonly known as HTTPS. During customer network creation in **Global Settings & Network Configuration**, you can set all URLs generated for the incoming and outgoing communication of SAP Focused Run to use HTTPS.

Connection Type and Communication Between Agents and Managed Systems

The local RFC communication between the SDA and the managed ABAP systems can be encrypted supporting TLS 1.2 protocols. The encrypted RFC is named SNC. The `Simple System Integration` for ABAP system supports the central configuration for SNC.

The local HTTP communication between the SDA and the managed systems using HTTP can be encrypted supporting TLS 1.2 protocols, then named HTTPS. The central HTTPS configuration for monitoring data collection by the SDA is not yet integrated in `Simple System Integration`. This HTTPS is planned for a later release. This HTTPS configuration can be made in the monitoring application. Please see details in the relevant monitoring application documentation.

The local P4 communication between SDA and the managed java system can be encrypted. The encrypted P4 is named P4S. With SAP Focused Run, `Simple System Integration` does not support the central automated configuration of P4S. The SDA provides a configuration interface for configuring P4S. Please open a ticket on SV-FRN-INF-SDA, if needed. `Simple System Integration` is expected to support this central automated configuration of P4S in a coming release.

Encryption Enabling

SAP Focused Run provides features for encrypted communication configuration. These include automated generation or manual creation of connection credentials for encrypted communication (general HTTPS URLs). SAP Focused Run features do **not** include central **enabling** of network encryption in the clients and servers by providing function for central certificate distribution.

Distribution and maintenance of certificate stores, as well as the configuration parameters for validation and preferred encryption algorithm, need to be done following component-specific documentation. For your convenience, see links below to the most common components.

> → Tip
>
> For the TLS pass-through, TLS termination, please consider which components certificates need to be requested and how these certificates must be distributed and stored, which impacts overall effort and costs.

Client/Server Relations in the SAP Focused Run Technical System Landscape

See below for a list of all client-server communications within the SAP Focused Run infrastructure. The subsection numbers are the legend for the ball numbers. All encryption is optional, but recommended. Encryption of SAP Focused Run communication between ABAP and SAP HANA DB is also possible (though not part of the graphic).

1 Remote communication from SAP Focused Run (client) to the customer cloud account (server)

- The connection credentials for the customer cloud account are provided in **Cloud Service Configuration** at cloud monitoring setup.
- Message contains cloud exception and errors.
- For communication encryption for customer cloud account, see cloud product documentation.

2 Remote communication from SAP Focused Run (client) to the Simple Diagnostics Agent (SDA), using SAP Host Agent (SHA) as an authentication proxy server.

This communication is opened on SAP Focused Run using destination `SM59`, type: *HTTP Connections to External Servers*.

The properties for the *Technical Settings* and *Logon & Securities* settings are provided in *Global Settings & Network Configuration* at customer network creation.

A proxy is possible here, but a TLS handshake is not. For this reason it is excluded from the graphic below.

Encryption is supported using HTTPS.

The messages may contain configurations with user/password which are then stored in a secure store of SDA.

For more information regarding communication encryption for SAP NetWeaver as client and server, see SAP NetWeaver Security Guide: https://help.sap.com/viewer/621bb4e3951b4a8ca633ca7ed1c0aba2/latest/en-US/5f0f558b8a7841049139f0fb558ac62c.html

For more information regarding communication encryption for SAP Host Agent Server as server, see: https://help.sap.com/viewer/141cbf7f183242b0ad0964a5195b24e7/113/en-US/6aac42c2e742413da050eaecd57f785d.html

3 Remote communication from all SLD data suppliers, including client Outside Discovery (OD) to server SAP Focused Run via reverse proxy and load balancer

The connection credentials "`sldhost`"," `sldport`, "`sld-user` ","`sld-user-passwd`". "http/https" depends where you like to send of the SLD payload to. SLD payload can be send to the following receivers:

1. 1. Directly to SAP Focused Run: no data separation, all data gets assigned to the namespace "localnetwork" (Direct send is not shown on the graphic below)
2. Directly to the revers proxy in front of the SAP Focused Run for data separation, see Data Separation [page 10]
3. To a System Landscape Data Router `SLDR` for further distribution to 1 or multiple receivers
4. To a SLD on Netweaver Java for further distribution to 1 or multiple receivers (SLD on Netweaver Java is not in graphic belwo)

The preparation tool provides a scriptable interface for most SLD DS configurations.

Encryption is supported using HTTPS.

The messages contain SLD payload with hostnames, IP addresses, OS version, and CPU information.

For more information regarding communication encryption for SLDREG (OD and SAPSTARSERV-integrated SLD DS), see 2307051 TLS1.2 support for `sldreg`.

For all other SLD DS, please see product-specific security guides.

4 Remote communication from the SDA and the CA EPM EM (client) to SAP Focused Run (Server), via reverse proxy and load balancer (Client & Server).

URLs are generated automatically with HTTPS by Simple System Integration (SSI) when configured in **Global Settings & Network Configuration** at customer network creation.

Encryption is supported using HTTPS.

The messages may contain landscape data like hostnames, OS version and patches, and information about default users on managed system not locked. Messages contain usage data (RUM) and business data (AIM) if customized.

For more information regarding communication encryption for Simple Diagnostic Agent as client, see https://support.sap.com/en/solution-manager/focused-solutions/focused-run-expert-portal/simple-diagnostic-agent-tls-configuration.html

For more information regarding communication encryption for CA APM EM (you need to create an account on the CA side to see the documentation), see https://support.ca.com/cadocs/0/CA%20Application%20Performance%20Management%209%206-ENU/Bookshelf_Files/HTML/APM--Configuration%20Administration%20Guide/index.htm

5 Remote communication from all SLD data supplier, including client OD to the server System Landscape Data Router (SLDR). (Optional marked by dotted line)

The `sldhost` and `sldport` are here the host and port of the SLDR.

Encryption is supported using HTTPS.

The messages contain SLD payload with hostnames, IP addresses, OS version and CPU information.

For more information regarding communication encryption for Simple Diagnostic Agent as client & server SLDR, see https://support.sap.com/en/solution-manager/focused-solutions/focused-run-expert-portal/simple-diagnostic-agent-tls-configuration.html

6 Local communication from the proprietary DB-client delivered with the SHA to the database server

Encryption of the proprietary DB protocol is supported, depending on the DB vendor.

For more information regarding communication encryption for SAP HANA DB server, see https://help.sap.com/viewer/DRAFT/b3ee5778bc2e4a089d3299b82ec762a7/latest/en-US/de15ffb1bb5710148386ffdfd857482a.html

For more information regarding SAP Host Agent proprietary DB-client to hana database server, see 2514150 SAP Host Agent for SAP HANA: SSL Connection to SAP HANA.

For more information regarding communication encryption for ASE DB, see 2667773 SYB: saphostctrl - enable SSL for existing systems.

7 Local communication calls from SDA (client) to the managed systems (server)

Encryption is supported for SNC, HTTPS, P4S, depending on the managed system type.

The messages may contain landscape data like host names, OS version and patches, and information about default users on managed system not locked. Messages contain usage data (RUM) and business data (AIM) if customized.

For more information regarding communication encryption for your managed system, please see the security guide of your product version.

For more information regarding communication encryption for Simple Diagnostic Agent as HTTP client, see https://support.sap.com/en/solution-manager/focused-solutions/focused-run-expert-portal/simple-diagnostic-agent-tls-configuration.html

For more information regarding communication encryption for Simple Diagnostic Agent as SNC client, see 2633417 Set up secure communication with SDA using certificates from PKCS12 stores (such as PSE).

8 Remote communication from managed ABAP systems (client) to SAP Focused Run (server) via reverse proxy and load balancer (client & server)

Encryption is supported using HTTPS.

The message contains ABAP EWA data.

For more information regarding communication encryption for NetWeaver ABAP, please see the security guide of your SAP NetWeaver version.

9 Remote communications forwarded by the reverse proxy, the load balancer.

The reverse proxy must terminate the encryption to apply forwarding rules for data separation. Therefore it acts as server for the incoming requests and as client for the outgoing requests. The load balancer can be configured to terminate or to pass through the encrypted messages. Then it's not relevant for the TLS handshake. If the load balancer terminates the encryption, it acts a server for the incoming requests and as client for the outgoing requests.

Encryption is supported using HTTPS.

The messages may contain landscape data like hostnames, IP addresses, OS version and patches, and information about default users on managed system not locked. Messages contain usage data (RUM) and business data (AIM) if customized.

For more information regarding communication encryption for SAP Web Dispatcher as reverse proxy and/or load balancer, see https://help.sap.com/viewer/bd78479f4da741a59f5e2a418bd37908/latest/en-US/48477e7fe9d771b9e10000000a421937.html

For more information regarding communication encryption for APACHE HTTP server as reverse proxy, see https://httpd.apache.org/docs/current/mod/mod_ssl.html .

Remote communication from the UI (client) to SAP Focused Run (server)

All end user UIs are SAP Fiori UIs encrypted by default using HTTPS.

Admin UIs are implemented as the following:

- SAP Fiori UIs encrypted by default, using HTTPS.
- `Webdynppro` encryption is supported, using HTTPS.
- WebGui encryption is supported, using HTTPS

- SAPGui encryption is supported, using SNC.
  For more information regarding communication encryption for SAP NetWeaver as server, see SAP NetWeaver Security Guide https://help.sap.com/viewer/621bb4e3951b4a8ca633ca7ed1c0aba2/latest/en-US/5f0f558b8a7841049139f0fb558ac62c.html

The message may contain many kinds of data. Especially at logon, the message can contain user/password information. Therefore, SAP Fiori uses HTTPS by default.

Remote communication between SAP Focused Run (client) and the customer account in the SAP Support Backbone

Encrypted by default as in SAP Focused Run Master Guide.

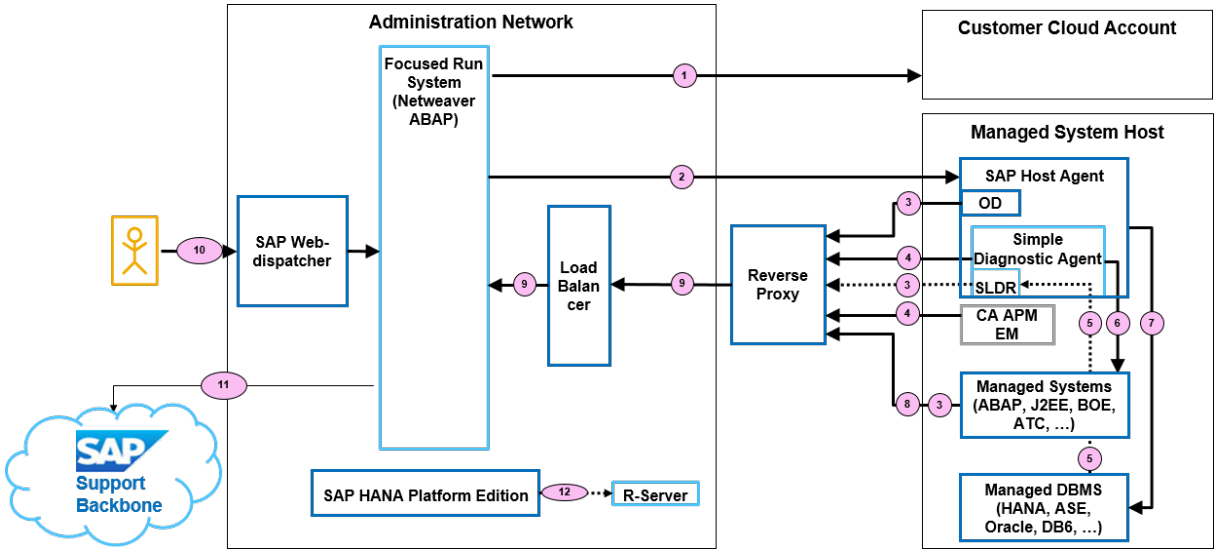
For more information regarding communication encryption for SAP Focused Run and customer account in SAP Support Backbone, see the SAP Focused Run Master Guide https://help.sap.com/viewer/p/FRUN

11 Remote communication from SAP Focused Run Hana DB (cient) to the R-server for System Anomaly Prediction (optional marked by dotted line)

Encryption is supported using QAP1 via Secure Socket Layer (SSL).

The messages contain monitoring metrics for statistical analysis.

For more information regarding communication encryption for SAP Focused Run SAP HANA DB and the R-server, see https://support.sap.com/content/dam/support/en_us/library/ssp/sap-solution-manager/focused-solutions/frun-r-setup-system-anomaly-prediction-100-suse-linux-sles-12-sp03.pdf and https://help.sap.com/viewer/a78d7f701c3341339fafe4031b64f015/2.0.03/en-US/d8487d07f6804248834b0e0153c3ee45.html



Client/Server Relations in SAP Focused Run 2.0 Technical System Landscape

4.2.1 Background for TLS Handshakes

Use

Describe the different phases of the TLS handshake. This is important to understand for implementing strong encryption and certificate-based authentication. Although documentation on TLS and encryptions is available, this documentation is tailored to SAP Focused Run. Here, certificates refer to X509 certificates.

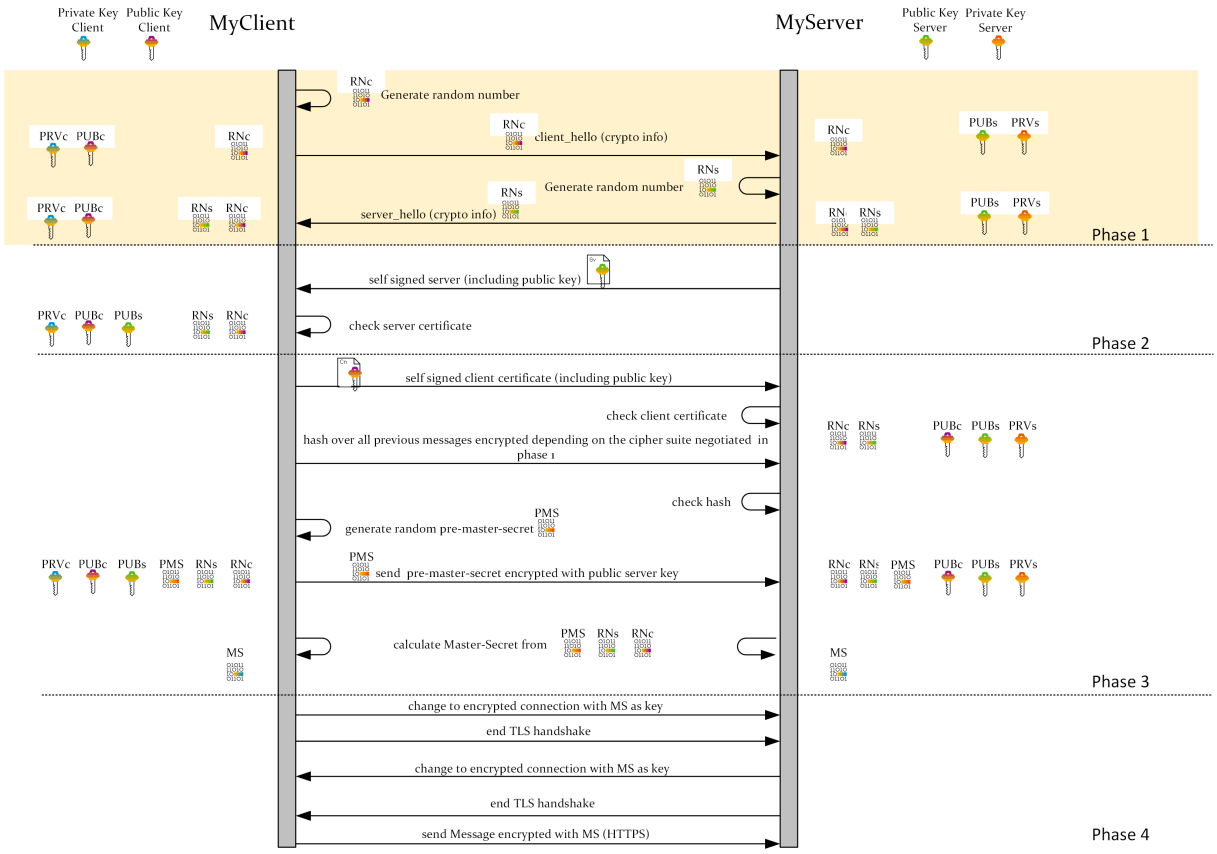
Weak Encryption

This encryption is called weak here because the client and server self-authenticate with self-signed certificates.

You do not need to issue and distribute certificates.

Such encryption is vulnerable for **man-in-the-middle attacks**. The man in the middle pretends to be the server/client and provides his own random numbers and public keys. The communication can be intercepted.

The generation of private and public key is handled by the crypto provider implementation. Latest at the creation of key-stores (*pse for Common Crypto Lib), they are created transparent for the user.

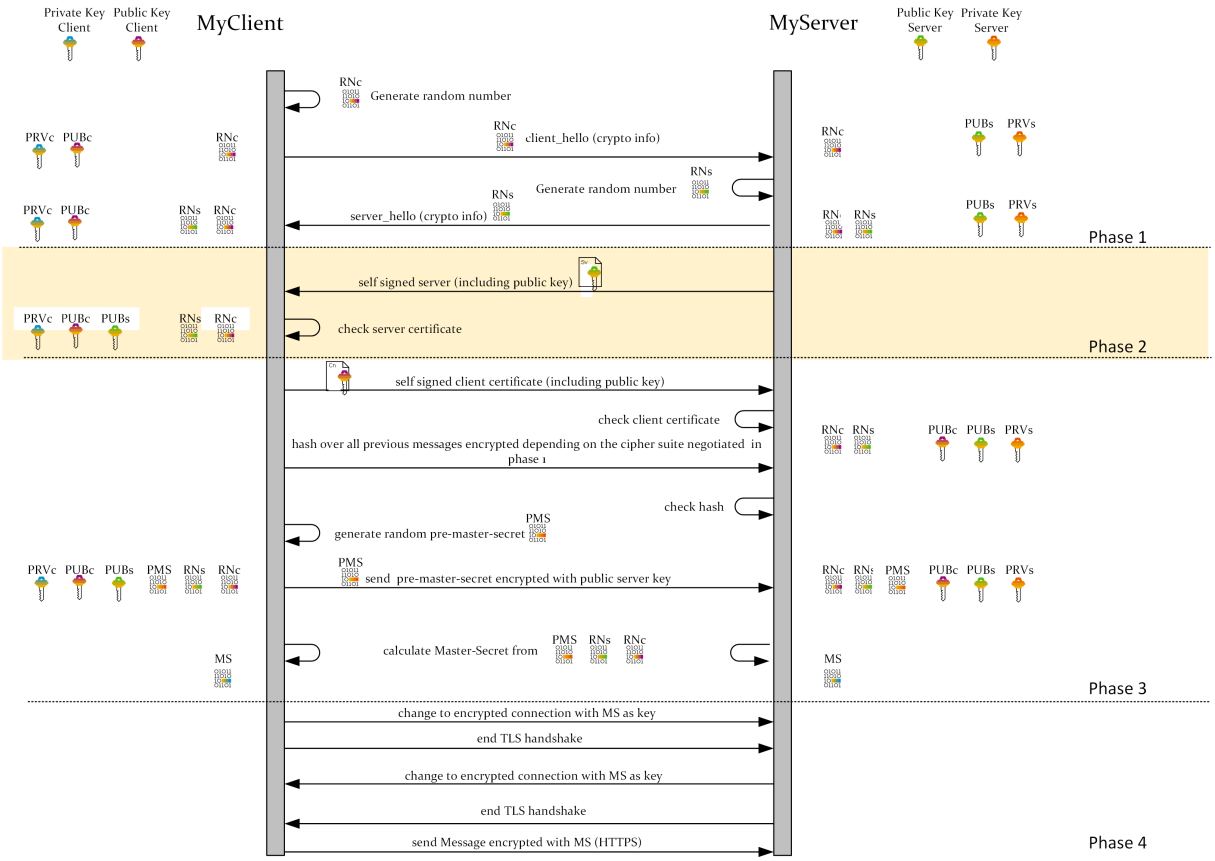


TLS Handshake w/n Server and w/n Client Verification

Encryption with Server Authentication

Such encryption with server authentication is most common in intranet usage.

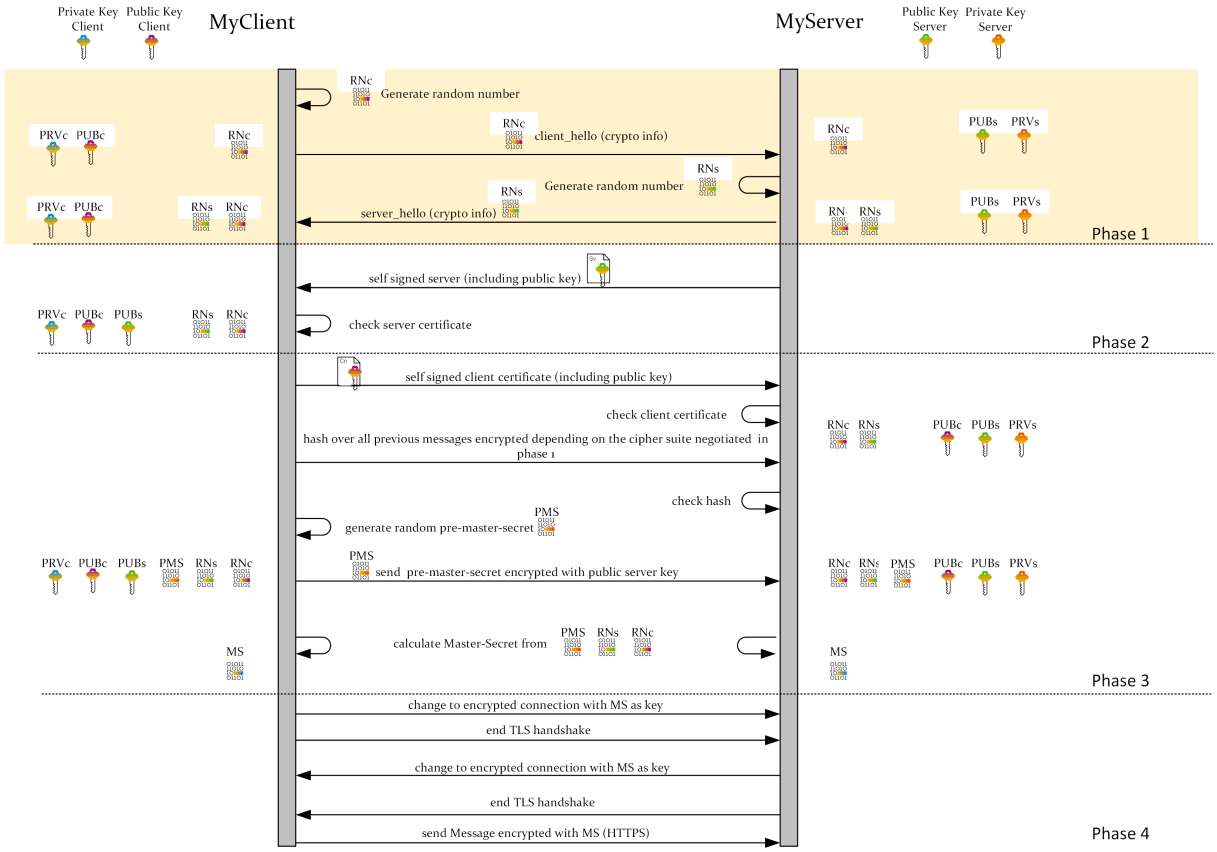
> ⚠ Caution
>
> If the human end-user HTTP browser does not trust the server certificate because it is not in the certificate store of the user, the browser returns a warning about untrusted communication. The end-user can decide to accept the communication or not. The technical user for authenticating the communications to and from SAP Focused Run and the managed systems cannot make such a choice. Therefore, if the server certificate is untrusted, the TLS handshake will fail and communication can not be established.



TLS Handshake w/ Server and w/n Client Verification

Encryption with Server and Client Authentication

Such encryption with client authentication takes the most effort to fully implement, because you also need to issue and distribute client certificates. It is mandatory if you like to implement certificate-based authentication.



TLS Handshake w/ Server and w/ Client Verification

Phase 1 Exchange of Crypto Info

During this phase, the crypto info (such as cyptographic methods and random numbers) are exchanged.

> → Tip
>
> Even if you choose most modern and secure chiphers, the security does not become strong without client & serve authentication with CA-signed certificates.

- The version of TLS protocol and chipher suites you like to support for this communication. With a higher TLS version, you can make the communication more secure.
  This is a disadvantage when clients or server are not able to support the configured TLS version. Then the TLS handshake will fail. It is not uncommon to configure the TLS accordingly.
  - The central SAP Focused Run, SAP NetWeaver 7.5, SAP HANA, the SHA, SAP Web-dispatcher, and most of other managed systems running SAP products implement the **Common Crypto Lib** (formally known as SAP Crypto lib) as crypto provider. For more information about how the Common Crypto Lib is fully supporting TLS 1.2 and sophisticated chipher suites, see 1848999 Central Note for CommonCryptoLib 8. The TLS version and chipher suites can be set by profile parameter `ssl/ciphersuites` , namely, `ssl/client_ciphersuites`. For more information, see 550007 Setting up SSL on Application Server ABAP.
  - Simple Diagnostics Agent, using sapjvm, and CA APM EM are implementing oracle Java Cryptographic Extension (JCE) as crypto provider. JCE is fully supporting TLS 1.2 and sophisticated chipher suite. For

more information regarding how to configure TLS version and cypher suites, see https://www.java.com/en/configure_crypto.html

- R server is implementing OpenSSL as crypto provider. As reference implementation, it already supports TLS 1.3, but as all other components are using other crypto provider, the highest TLS version you can configure is TLS 1.2. For more information regarding how to configure TLS version and cypher suites, see https://wiki.openssl.org/index.php/SSL/TLS_Client
- Apache is implementing Apache Common Crypto as cryptopm provider. It wraps to OpenSSL or JCE, which implement the algorithm. For more information regarding how to configure TLS version and cypher suites, see https://httpd.apache.org/docs/current/mod/mod_ssl.html .

- Random number generation and exchange will be used later for the generation of the pre-master-secret. As this is not further explained here, please take it as given or discuss with a security expert.
- Session ID is not further discussed here. Please take it as standard functionality
- FQHN for Server Name Indication. SNI support is planned for a later release. The FQHN is remains important. For more information, see phase 2.

Phase 2 Server Authentication

The server authenticates itself to the client. That means if the client sends a HTTPS request to

```
myserver.acme.com
```

and the server authenticates itself as

```
 myserver.acme.global.com
```

This is a completely different string. The TLS handshake will be rejected. This issue can occur with self-signed certificates of the server (unsecure) as well as with CA-signed certificates. In the example above, the CN must contain

```
CN= myserver.acme.com
```

for successful TLS handshake. All certificates with other CN will be rejected.

The setting of a wild-card (*) for one element in the CN is supported.

To do

1. Issue a CA-signed certificate for the server and import it into the server certificate store.
2. Distribute the CA root certificate to the client to verify the certificate send by the server.

For more information on how to maintain the certificate stores, request and import certificates, see Transport Layer Security [page 20]

> ⚠ Caution
>
> The SDA is delivered without the CA root certificate of your company. After you have imported the CA root certificate into the SDA trust store to *Establish Trust on SDA*, see https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/simple-diagnostic-agent-tls-configuration.html#section
>
> > ⚠ Caution
> >
> > You need to activate the server certificate verification. For more information, see 2632984

Enable/Disable verification of server certificates

→ Tip

In SAP Focused Run, each SHA on each host is a server and needs such a CA certificate. The distribution of the certificates is often automated by customers using O-scripts.

The server can request a client certificate.

- The SHA as server requests by default a CA-signed client certificate. The client is normally only SAP Focused Run or a SAP LAMA. So only one client certificate needs to be issued and distributed.
- Web-dispatcher: the central SAP Focused Run ABAP as server can be configured to request a client certificate with

  ```
  icm/server_port_<xx>
  ```

  sub-parameter

  ```
  VCLIENT
  ```

  For more information, see https://help.sap.com/viewer/bd78479f4da741a59f5e2a418bd37908/201809.000/en-US/483ae05299c172d0e10000000a42189c.html
- For more information regarding the SLDR as server can request, see https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/simple-diagnostic-agent-tls-configuration.html#section
- For more information regarding R-server implementing OpenSSL - how to request client certificate, see https://wiki.openssl.org/index.php/SSL/TLS_Client
- For more information regarding Apache reverse proxy mod_ssl - how to request client certificate, see https://httpd.apache.org/docs/current/mod/mod_ssl.html
- All other servers of managed system, please see the product security documentation.

Phase 3 Client Authentication and Exchange of Per-Master-Secret

To do

1. Issue a CA-signed certificate for the server and import it into the server certificate store.
2. Distribute the CA root certificate to the server to verify the certificate send by the client.
3. Issue a CA-signed certificate for the client and import it into the client certificate store.
4. Distribute the CA root certificate to the client to verify the certificate send by the server.

The issuing and distribution of certificates for the client is in principle not different than the one for the server, therefore please find the links mentioned above.

The creation of the hash of all previous messages and the generation of the pre-Master-Secret are implementation details depending on encryption methods. As this is not further explained here, please take it as given or discuss with a security expert.

> **i Note**
>
> The DN is same important for certificate-based authentication as it is for server authentication. If the client certificate is unsecured for
>
> ```
> DN = "CN=xyz.sap.corp, O=SAP AG, C=DE"
> ```
>
> then this string is mapped to an authorization. If another string is provided, the authorization will not be granted.

4.3 UCON Usage with SAP Focused Run

Use

In the technical system landscape where UCON is used, an administrator decides which remote-enabled function modules (RFMs) are to be exposed to the outside.

In SAP Focused Run, Simple Diagnostics Agents call RFMs via RFC, depending on the different use cases. RFMs need to be maintained as UCON white list in the managed systems to grant feature completeness and proper data collection with SAP Focused Run.

This topic provides you the RFMs called by the Simple Diagnostics Agent.

> **→ Tip**
>
> If you record RFC calls for Synthetic User Monitoring or Trace Anaylsis, you might need to enhance the UCON white list accordingly.

The list remote function modules below are gathered for the different development teams with the greatest care. If you face any problems due to missing function modules below or any other questions regarding the called function modules, please open a ticket using the component SV-FRN-INF-SSI.

The remote-enabled function modules are listed as sample code for you to copy and paste, as needed.

Simple System Integration and License Management

Ticket component: SV-FRN-INF-SSI

> **‹≡› Sample Code**
>
> ```
> RFC_SYSTEM_INFO
> /SDF/LICENSE_KEY_INSTALL
> ```

Preparation Tool

Ticket component: SV-FRN-INF-SDA

Sample Code

```
/SDF/PRGN_COPY_AGR_WITH_MESSAG
/SDF/UPDATE_AUTH_ROLES
BAPI_USER_CREATE1
BAPI_USER_EXISTENCE_CHECK
DEST_HTTP_EXT_CREATE
DEST_HTTP_EXT_UPDATE
DEST_SET_PASSWORD
SLDAG_RUN_COLLECTOR
SLDAG_SET_CONFIG
SLDAG_START_COLLECTOR
```

Advanced System Management System Monitoring

Ticket Component: SV-FRN-INF-CNT

Sample Code

```
/SDF/E2E_BATCHJOB_INFO
/SDF/E2E_CCMS_MTE
/SDF/E2E_CCMS_MTE_CURRENT
/SDF/E2E_DUMP_INFO
/SDF/E2E_DUMP_STATS
/SDF/E2E_EFWKE_DATA_CONNECTOR
/SDF/E2E_ICM_INFO
/SDF/E2E_INSTANCE_STATUS
/SDF/E2E_LICENSE_CHECK
/SDF/E2E_LOGON_GROUPS
/SDF/E2E_MEMORY_INFO
/SDF/E2E_ODQ_INFO
/SDF/E2E_Q_BGRFC
/SDF/E2E_RFC_CHECK
/SDF/E2E_RFC_RESOURCES
/SDF/E2E_RFC_STATS
/SDF/E2E_SYSLOG_STATS
/SDF/E2E_TRFC
/SDF/E2E_UPDATE_INFO
/SDF/E2E_USER_CHECK
/SDF/E2E_USER_INFO
/SDF/E2E_USER_SESSION
/SDF/E2E_WP_INFO
RFCPING
```

Advanced Configuration Monitoring

Ticket component: SV-FRN-APP-CSA

Sample Code

```
/SDF/COF_PERFORM_EXTR
```

Advanced Integration Monitoring and Exception Management

Ticket component: SV-FRN-APP-AIM

Sample Code

```
/SDF/E2EEM_GET_DATA
/SDF/IMA_DC_BDOC
/SDF/IMA_DC_BGRFC_Q
/SDF/IMA_DC_BGRFC_T
/SDF/IMA_DC_IDOC
/SDF/IMA_DC_PI_ABAP
/SDF/IMA_DC_QRFC
/SDF/IMA_DC_TRFC
/SDF/IMA_VH
/SDF/IMA_WS_ABAP
CTE_FND_COMM_MONITOR_GET_DATA (concur only)
(concur only)
```

Real User Management and Synthetic User Management

Ticket component: SV-FRN-APP-RUM

SUM and RUM have an integrated function to activate transaction analysis. For this reason, the TA remote-enabled function modules are mentioned here.

Sample Code

```
/SDF/GET_ALL_ATRA_FILE_NAMES
/SDF/GET_DUMP_LOG
/SDF/GET_SSR_FESR
/SDF/SMD_E2E_TRACE/
SACC_TRACE_SUMMARY_ALL
SWNC_GET_AGGREGATES_FRAME
SWNC_GET_DIRECTORY_FRAME
SWNC_GET_STATRECS_FRAME
```

Advanced Root Cause Analysis with System Analysis

Ticket component: SV-FRN-APP-SYA

Sample Code

```
/SDF/MON_GET_ANALYSES
/SDF/SMON_START_CM
/SDF/SMON_STOP_CM
/SDF/SMON_WPINFO_AGGR
SWNC_GET_AGGREGATES_FRAME
SWNC_GET_DIRECTORY_FRAME
```

Advanced Root Cause Analysis with System Analysis and Transaction Analysis

Ticket component: SV-FRN-APP-TA

Sample Code

```
/SDF/GET_ALL_ATRA_FILE_NAMES
/SDF/GET_DUMP_LOG
SACC_TRACE_SUMMARY_ALL
SWNC_GET_STATRECS_FRAME
```

Guided Procedure

Ticket component: SV-FRN-APP-CP-CNT

Sample Code

```
/SDF/E2E_BUFFER_INFO
/SDF/E2E_IDOC
/SDF/E2E_MEMORY_INFO
/SDF/GET_DUMP_LOG
/SDF/GET_SYS_LOG
/SDF/GET_SYS_LOG_INST
/SDF/GET_SYS_LOG_INST_EPP
/SDF/GPC_CALL_METRIC_COLLECTOR
/SDF/GPC_DP_GET_DATA
/SDF/GPC_GET_TRFC_ERRORS
ENQUEUE_REPORT
GET_CCM_DATA
RSLG_FILEINFO_INIT_ALV
RSLG_READ_FILE_ALV
RSLG_TAB_CACHE_ACCESS
SACC_TRACE_SUMMARY_ALL
SWNC_COLLECTOR_GET_AGGREGATES
THUSRINFO
```

All

Use to enable all functions of SAP Focused Run.

Sample Code

```
/SDF/E2E_BATCHJOB_INFO
/SDF/COF_PERFORM_EXTR
/SDF/E2E_BUFFER_INFO
/SDF/E2E_CCMS_MTE
/SDF/E2E_CCMS_MTE_CURRENT
/SDF/E2E_DUMP_INFO
/SDF/E2E_DUMP_STATS
/SDF/E2E_EFWKE_DATA_CONNECTOR
/SDF/E2E_ICM_INFO
/SDF/E2E_IDOC
/SDF/E2E_INSTANCE_STATUS
/SDF/E2E_LICENSE_CHECK
/SDF/E2E_LOGON_GROUPS
/SDF/E2E_MEMORY_INFO
/SDF/E2E_ODQ_INFO
/SDF/E2E_Q_BGRFC
/SDF/E2E_RFC_CHECK
/SDF/E2E_RFC_RESOURCES
/SDF/E2E_RFC_STATS
/SDF/E2E_SYSLOG_STATS
/SDF/E2E_TRFC
/SDF/E2E_UPDATE_INFO
/SDF/E2E_USER_CHECK
/SDF/E2E_USER_INFO
/SDF/E2E_USER_SESSION
/SDF/E2E_WP_INFO
/SDF/E2EEM_GET_DATA
/SDF/GET_ALL_ATRA_FILE_NAMES
/SDF/GET_DUMP_LOG
/SDF/GET_SSR_FESR
/SDF/GET_SYS_LOG
/SDF/GET_SYS_LOG_INST
/SDF/GET_SYS_LOG_INST_EPP
/SDF/GPC_CALL_METRIC_COLLECTOR
/SDF/GPC_DP_GET_DATA
/SDF/GPC_GET_TRFC_ERRORS
/SDF/IMA_DC_BDOC
/SDF/IMA_DC_BGRFC_Q
/SDF/IMA_DC_BGRFC_T
/SDF/IMA_DC_IDOC
/SDF/IMA_DC_PI_ABAP
/SDF/IMA_DC_QRFC
/SDF/IMA_DC_TRFC
/SDF/IMA_VH
/SDF/IMA_WS_ABAP
/SDF/LICENSE_KEY_INSTALL
/SDF/PRGN_COPY_AGR_WITH_MESSAG
/SDF/SMD_E2E_TRACE/
/SDF/UPDATE_AUTH_ROLES
BAPI_USER_CREATE1
BAPI_USER_EXISTENCE_CHECK
CTE_FND_COMM_MONITOR_GET_DATA
DEST_HTTP_EXT_CREATE
DEST_HTTP_EXT_UPDATE
DEST_SET_PASSWORD
ENQUEUE_REPORT
GET_CCM_DATA
RFC_SYSTEM_INFO
RFCPING
RSLG_FILEINFO_INIT_ALV
```

```
RSLG_READ_FILE_ALV
RSLG_TAB_CACHE_ACCESS
SACC_TRACE_SUMMARY_ALL
SLDAG_RUN_COLLECTOR
SLDAG_SET_CONFIG
SLDAG_START_COLLECTOR
SWNC_COLLECTOR_GET_AGGREGATES
SWNC_GET_AGGREGATES_FRAME
SWNC_GET_DIRECTORY_FRAME
SWNC_GET_STATRECS_FRAME
THUSRINFO
```

Related Links:

https://help.sap.com/viewer/1ca554ffe75a4d44a7bb882b5454236f/7.5.13/en-US/ab35e1c69f744d69a4fcf4ca93284e0c.html Unified connectivity in help.sap.com

2098702 Composite note for UCON RF

2219467 UCON blocks RFC calls of function modules assigned to a communication assembly

5 User Administration and Authentication

Use

This section covers how to create users and authorization needed for SAP Focused Run operations. In addition, it provides information about authentication methods supported by the different components.

> ⚠ Caution
>
> We strongly recommend creating all users and maintaining authorization as described, while in an early phase of your SAP Focused Run implementation project.

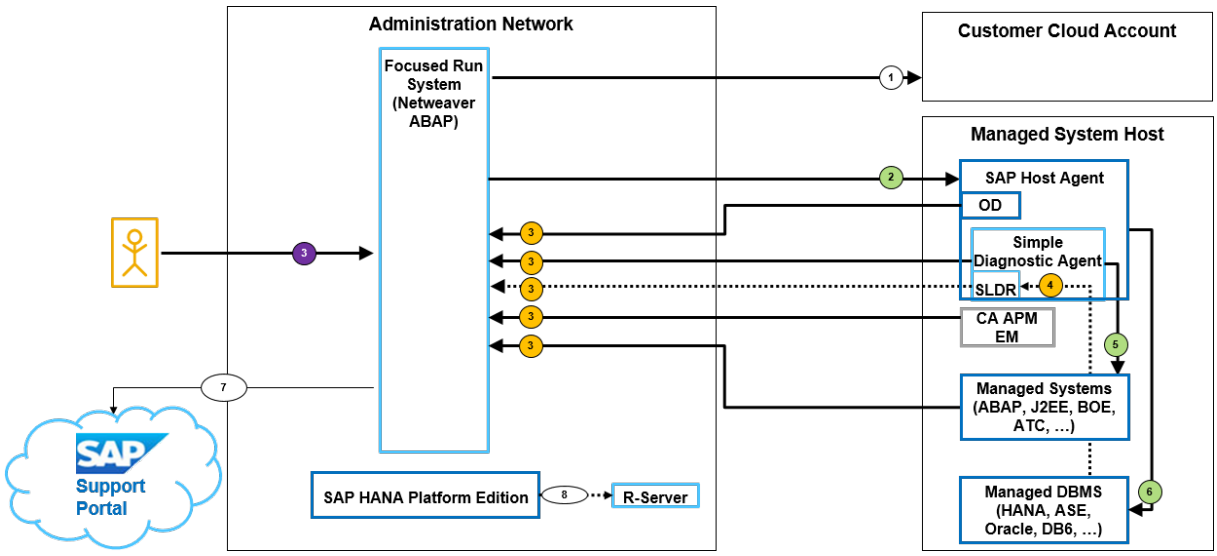
5.1 User Authentication

Use

Understand where user authentication is required in SAP Focused Run technical system landscape.

Components in the Technical System Landscape to Authenticate to

1. Customer Cloud Account
2. Central SAP Focused Run System
3. SAP Host Agent
4. System Landscape Data Router (SLDR)
5. Managed System
6. Managed DB
7. SAP Support Backbone
8. R Server



User Authentication

5.1.1 Basic Authentication

Use

This section describes how user and password for basic authentication are configured and stored in the technical system landscape of SAP Focused Run. It includes links for additional related information.

> ⚠ Caution
>
> Basic authentication sends the user and password, and if the communication is not encrypted, the user and password are sent in plain text.
>
> Therefore, we recommend implementing encrypted communications for SAP Focused Run. For more information, see Transport Layer Security [page 20]
>
> Also for encrypted communication reasons, SAP Fiori launchpad supports logon with HTTPS only.

(1) At the Customer Cloud Account

The cloud product for collecting monitoring data supports a technical user and password created at the customer cloud account.

In SAP Focused Run, this user and password is provided at *Cloud Service Management Configuration*, and stored in the secure store of SAP NetWeaver. Reference in-app help for more information.

(2) At SAP Host Agent

When using basic authentication, SAP Focused Run supports the OS user `sapadm` for all requests sent to SHA web service methods.

The OS user `sapadm` is created according to OS user management and password policies. Neither SAP Focused Run nor the Simple Diagnostics Agent (SDA) supports OS user management operations.

Simple System Integrations (SSI) support the basic authentication configuration with user `sapadm` and password as provided at customer network creation. SSI uses this password for the automated creation of `SM59` destinations to SAP Host Agent.

> ⚠ Caution
>
> With basic authentication, SAP Focused Run has full administrator authorization on SHA.
>
> This should be considered when used in parallel with SAP Lama is or when in hosting provider scenarios:
>
> - SAP Lama for system management with full admin authorization on SHA
> - SAP Focused Run for system monitoring and root-cause analysis with limit authorization on SHA
>   For this scenario, we recommend using certificate authentication at SHA. For more information, see Certificate Authentication [page 41]

(3) At Central SAP Focused Run

Dialog User

Dialog users enter user and password in the logon screen for SAP Fiori launchpad, WebGui, or SAPGui.

User-ID policies and password policies can be set as provided by SAP NetWeaver 7.5.

For more information regarding SAP NetWeaver 7.5 ABAP, seehttps://help.sap.com/viewer/621bb4e3951b4a8ca633ca7ed1c0aba2/latest/en-US/4a112f1a2228101ee10000000a42189b.html

Technical User

Technical users that authenticate incoming HTTP requests from SDA, CA APM EM, or SLD DS are generated at customer network creation from template users. For this technical user, a random password is generated, except FRN_LDDS_<CID>, FRN_LDSR_<CID>, FRN_EWA_<CID> and FRN_SLDS_<CID>. The user ID and the password are sent to the SDA (also for CA APM EM) as part of agent configuration, namely SSI of CA APM EM. The user ID and password are then stored in the secured store of the SDA. For more information, see Technical Users to Authorizing Incoming HTTP Requests 2.1 [page 52].

Technical users FRN_LDDS_<CID>, FRN_LDSR_<CID>, FRN_EWA_<CID>, are created at the customer network creation as well, but the passwords need to be set in the SAP Focused Run in transaction `SE38` with report `RSSI_CHANGE_NETWORK_PASSWORD.`. These users and passwords must then be entered when configuring the SLD DS.

For more information regarding the user and password for FRN_LDDS_<CID>, FRN_LDSR_<CID> that needs to be provided when configuring the SLD DS, please see the product-specific documentation.

Only SHA provides web method `ConfigureOutsideDiscovery` for scriptable automated configuration

The preparation tool provides a web method for configuring other SLDR. For more information, see 2641304 Using SAP Focused Run 2.0 System Preparation Tool for Managed System Preparation

For more information regarding the optional SLDR outbound connection to SAP Focused Run if SLDR is used, see https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/managed-systems-maintenance-guide/preparing-system-landscape-data-router.html Preparing System Landscape Data Router

Technical user FRN_EWA_<CID>, same as above. This user and password needs to be entered in the managed ABAP during the `SM59` destination creation for EWA.

(4) At the System Landscape Data Router (Optional)

One technical user per SLDR **inbound port** to authenticate incoming data from SLD DS if used. Standard user ID is FRN_SLDS_<CID>. The user ID and password is set when configuring the SLDR. For more information, see https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/managed-systems-maintenance-guide/preparing-system-landscape-data-router.html Preparing System Landscape Data Router.

The user does not have any other purpose than to authenticate the incoming request from the SLD DS. There are no password policies to be defined on the SLDR. The user ID and password are stored in the secure store of the SDA.

The user and password need to be provided when configuring the SLD DS. For more information, please see the product-specific documentation.

Only the SHA provides web method `ConfigureOutsideDiscovery` for scriptable automated configuration.

The preparation tool provides a web method for configuring other SLDR. For more information, see 2641304 Using SAP Focused Run 2.0 System Preparation Tool for Managed System Preparation

(5) At Managed DBMS

For more information regarding the technical user that connects to the managed databases, see Databases [page 97]

(6) At the Managed Systems

For more information regarding the technical user that connects to the managed systems and collects monitoring data, see Technical Users in Managed Systems [page 92]

For user management and password policies, please see your product documentation.

The user and password are provided at SSI of the managed system. They are transmitted as part of the configuration to the SDA, where they are stored in the secure store.

(7) At the SAP Support Backbone

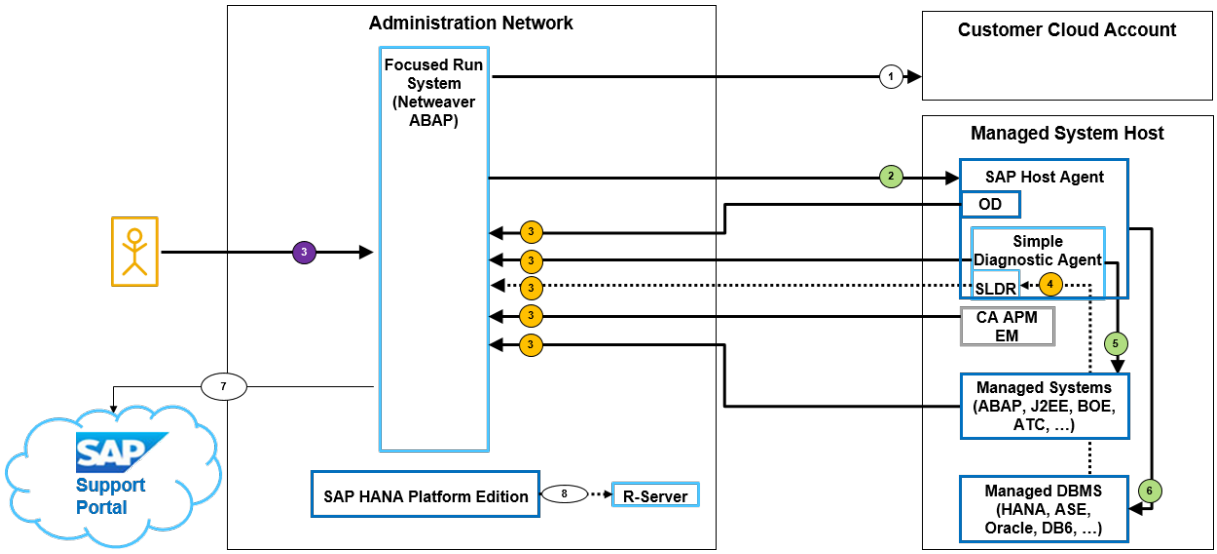
This regards an S-user provided during SAP Focused Run setup. It regards uploading landscape data to SAP Support Backbone for the maintenance planner and uploading monitoring metrics for EWA report creation. For more information, see https://help.sap.com/viewer/p/FRUN Master Guide, chapter 5.2.9 Setup Communication with SAP Support Backbone.

(8) At the R-Server (optional)

The R-server supports basic authentication only. R-server documentation recommends creating a non-privileged OS user to authenticate the QAPI call at the R-server. For more information, see https://support.sap.com/content/dam/support/en_us/library/ssp/sap-solution-manager/focused-solutions/frun-r-setup-system-anomaly-prediction-100-suse-linux-sles-12-sp03.pdf Chapter 3.1 Create a non-privileged user.

The OS user `sapadm` is created according to the OS user management with password policies.

The user and password need to be configured in the SAP HANA DB.



5.1.2 Certificate Authentication

Use

This section describes how X509 certificate DNs are mapped to user for certificate authentication in SAP Focused Run's technical system landscape. It includes links to related documentation.

> **i Note**
>
> This chapter describes the mapping of the certificate to the existing user with authorization. Transport layer security needs to be already implemented and client certificates need to be issued and distributed to

the clients. For more information, see Transport Layer Security [page 20]. See also Background for TLS Handshakes [page 26] as prerequisite.

(1) At the Customer Cloud Account

No cloud products support certificate authentication. Basic authentication and OAuth are supported by cloud products and SAP Focused Run. For more information, please see the cloud product documentation.

(2) At SAP Host Agent

SAP Host Agent supports two kinds of certificate-based authentication:

- Inherited from `SAPSTARTSRV`, configured by parameter `service/sso_admin_user_<X>` , set in `host_profile` of SAP Host Agent.

  Sample Code

  ```
  service/sso_admin_user_0 = CN=D??????, O=SAP-AG, C=DE
  ```

  For more information, see the full documentation in 1439348 Extended security settings for `SAPSTARTSRV`

  ⚠ Caution

  Requests authenticated with certificates matching the value of `service/sso_admin_user_<X>` are executed with full authorization on SAP Host Agent. Therefore, this certificate authentication type is not recommended for system management with SAP Focused Run because it grants more authentication than needed.

- Designed for SAP Focused Run requests, the `SAPSSLC.pse resp <CUSTOM>.pse` containing the certificate for authentication is provided at customer network creation and used for the automated creation of the `SM59` destination to Sap Host Agent.
  An additional configuration file needs to be created on the managed host.
  - Windows

    ```
    C:\Program Files\SAP\hostctrl\exe\config.d\http.server.settings
    ```

  - Unix

    ```
    /usr/sap/hostctrl/exe/config.d/http.server.settings
    ```

  ⚠ Caution

  On Unix, the owner of file *http.server.settings* must be root or `sapadm`, and the file must not be writable for group/others. Otherwise the settings file is ignored.

  The DN as in the certificate is then provided in this file in this syntax.

Sample Code

```
URL: /SMDAgent/deploy {
    authentication {
        DN : "CN=abc.sap.corp, O=SAP AG, C=DE"
    }
    start: no
}
URL: /lmsl/sda {
    authentication {
        DN : "CN=xyz.sap.corp, O=SAP AG, C=DE"
        DN : "CN=abc.sap.corp, O=SAP AG, C=DE"
    }
}
```

- The SSO DN "CN=abc.sap.corp, O=SAP AG, C=DE" is able to deploy the SDA. It will not be started after deployment.
- The SSO DN "CN=xyz.sap.corp, O=SAP AG, C=DE" is able to access the SDA.
- On access, SDA will be started automatically if it is not already running.

The settings can be activated without the need to restart SAP HostAgent with the web service *ReloadConfiguration*.

```
<sha-dir>/saphostctrl -function ReloadConfiguration
```

For more information regarding, additional possible variants of this SHA functionality, see https://wiki.scn.sap.com/wiki/display/ATopics/SDA+deployment+using+SSO

(3) At Central SAP Focused Run

Configure central SAP Focused Run to accept the X509 certificate for user authentication. For more information, see https://help.sap.com/viewer/6ba510f3be2945e19e497bfb1065b022/2.0/en-US/789188ebf9cc42d7b112cf31e6405f8d.html

Map the client certificate (via transaction) distributed from SDA to the SAP Focused Run user with the requisite authorization.

→ Recommendation

CERTRULE

see https://help.sap.com/viewer/d528eef3dca14679bcb47b069aa17a9d/7.5.13/en-US/54f1104ea9834be7be12282f10042327.html

(4) At SLDR (optional)

SLDR can be configured to map a certificate provided by the SLD DS to one or more inbound ports.

SLDR supports SDA configurations: JSON format sends to a REST API. You can use any HTTP client supporting REST. The configuration API is scriptable. The example below is for using **curl** as client.

1. Create a small text file

   Sample Code

   ```
   sldr.conf
   ```

   containing this JSON

   Sample Code

   ```
   {
       "active":{"value":"true"},
       "secure.1":{"value":"true"},
       "basic-auth.1":{"value":"false"},
       "port.0":{"value":"8888"},
       "user.1":{"value":"<accepted-certificate-DN>"}
   }
   ```

2. Send this JSON structure as body the host of SLDR with **curl**

   Sample Code

   ```
   cat sldr.conf | curl --user sapadm:<password>  --request POST --url http://
   <sldrhost>:1128/lmsl/sda/default/?service=configuration&json-
   types=SecureProperties&application=t-connector&solution-manager=<SID>
   ```

As a result, you have configured SLDR to accept at port 8888 SLD DS payload authenticated with DN = <accepted-certificate-DN>.

For full configuration possibilities, please see https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/simple-diagnostic-agent-tls-configuration.html section **Configure SLDR**.

(5) At the Managed System

Supported as by the product of the managed system. For more information, please see the product-specific documentation.

For Managed System ABAP. Simple System Integration support central configuration of SDA as SNC client with certificate authentication.

(6) At the Managed DB

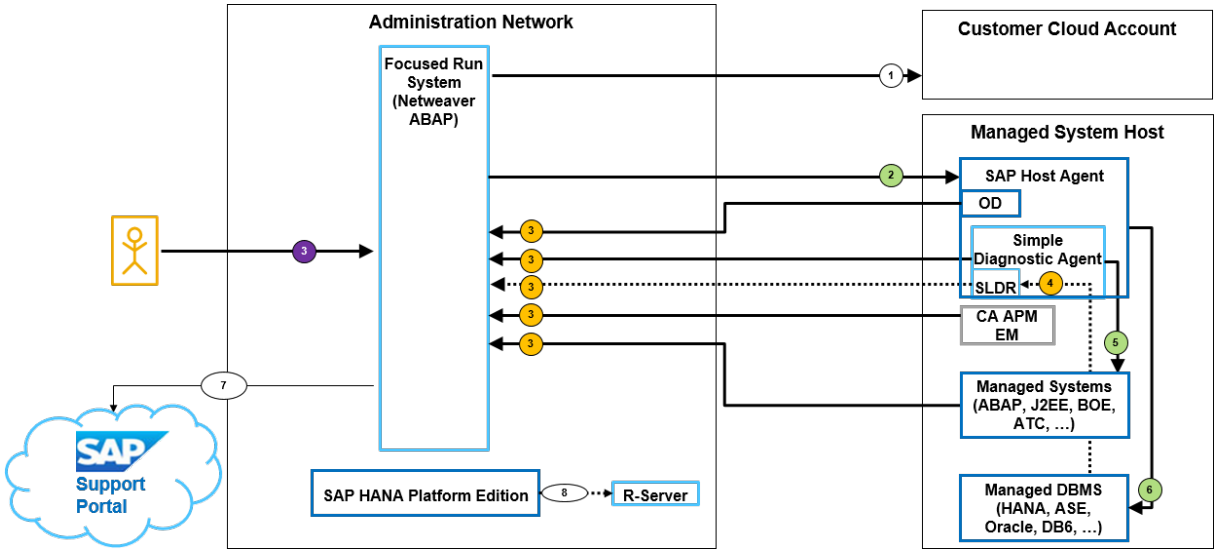
Not supported.

(7) At the Support Backbone

Not supported.

(8) At the R-server

Not supported.



5.2 User Management

Use

This section provides an overview of users in a SAP Focused Run infrastructure.

> **i** Note
>
> To better understand this topic, please familiarize yourself with the concept of Data Separation [page 10].

> **→** Tip
>
> Apply latest version of roles for SAP Focused Run 2.0 SP00 delivered with 2730623 Role updates for SAP Focused Run: FRUN 200
>
> To learn more about a limitation with composite roles, see 2538787 2538787 - Catalogs in composite role cannot be seen by end user

> ⚠ Caution
>
> For security reasons, we deliver SAP standard roles with empty authorization object values. Your first tasks when configuring SAP Focused Run should be to create customer roles and maintain the values.

External User Management

SAP Focused Run supports external user management solutions. For inquiries regarding integration of external user management, please create a customer ticket (component: FRN-SV-INF-SSI).

User Management Types

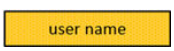
- **Technical users** with specific authorizations need to be created in the central SAP Focused Run ABAP itself.
  - Technical Users to Authorizing Incoming HTTP Requests 2.1 [page 52]
  - Technical Users Authorizing Batch Processing (2.1) [page 56]
  - Technical User to Authorize Internal RFC Calls (2.1) [page 63]

  For more information regarding users and authorization needed for these managed object types, see Proposed Workflow to Assign Authorizations to Technical Users [page 51].

User Overview graphic element (below): Green boxes

- **Technical Users in managed systems** are users you need to create in the managed systems. SAP Focused Run differs from SAP Solution Manager in this regard, given that the latter supports central user creation. The Preparation Tool (PT) delivered with the SDA supports a scriptable creation and integration in SAP LAMA.
  For more information regarding users and authorization needed for the following managed object types, see the documentation below:
  - SAP NetWeaver ABAP [page 93]
  - SAP NetWeaver Java [page 95]
  - SAP Mobile Platform [page 97]
  - Databases [page 97]
  - Hosts / OS [page 99]

User Overview graphic element (below): Yellow boxes



- **Technical User in SAP Focused Run** for Batch processing need to be created manually in SAP Focused Run during the SAP Focused Run initial configuration. See also Technical Users Authorizing Batch Processing (2.1) [page 56]
- **Technical User in SAP Focused Run** for authentication of incoming calls are automatically created from Template User see also Technical Users to Authorizing Incoming HTTP Requests 2.1 [page 52]

- The distribution of technical user credentials to the Simple Diagnostics Agent (SDA) and the CA APM is centrally automated by Simple System Integration (SSI).
- The distribution of technical user credentials for the SLD data supplier for authentication of post request of SLD payload need to be configured without central support by SAP Focused Run.
  The distribution of technical user credentials for the ABAP EWA data collection for authentication of post request of EWA raw data need to be configured without central support by SAP Focused Run.
- The PT delivered with the SDA supports a scriptable configuration of SLD data supplier and ABAP EWA HTTP destination.
  For more information regarding the PT, see 2641304 Using SAP Focused Run System Preparation Tool for Managed System Preparation

User Overview graphic element (below): Pink boxes

Indicating where the user credentials are stored.

User Overview graphic element (below): Light violet boxes

Dialog users must be created in the central SAP Focused Run. SAP Focused Run provides roles for SAP Fiori UI and application authorization.

For more information regarding dialog users and the needed authorizations, see the documentation below:

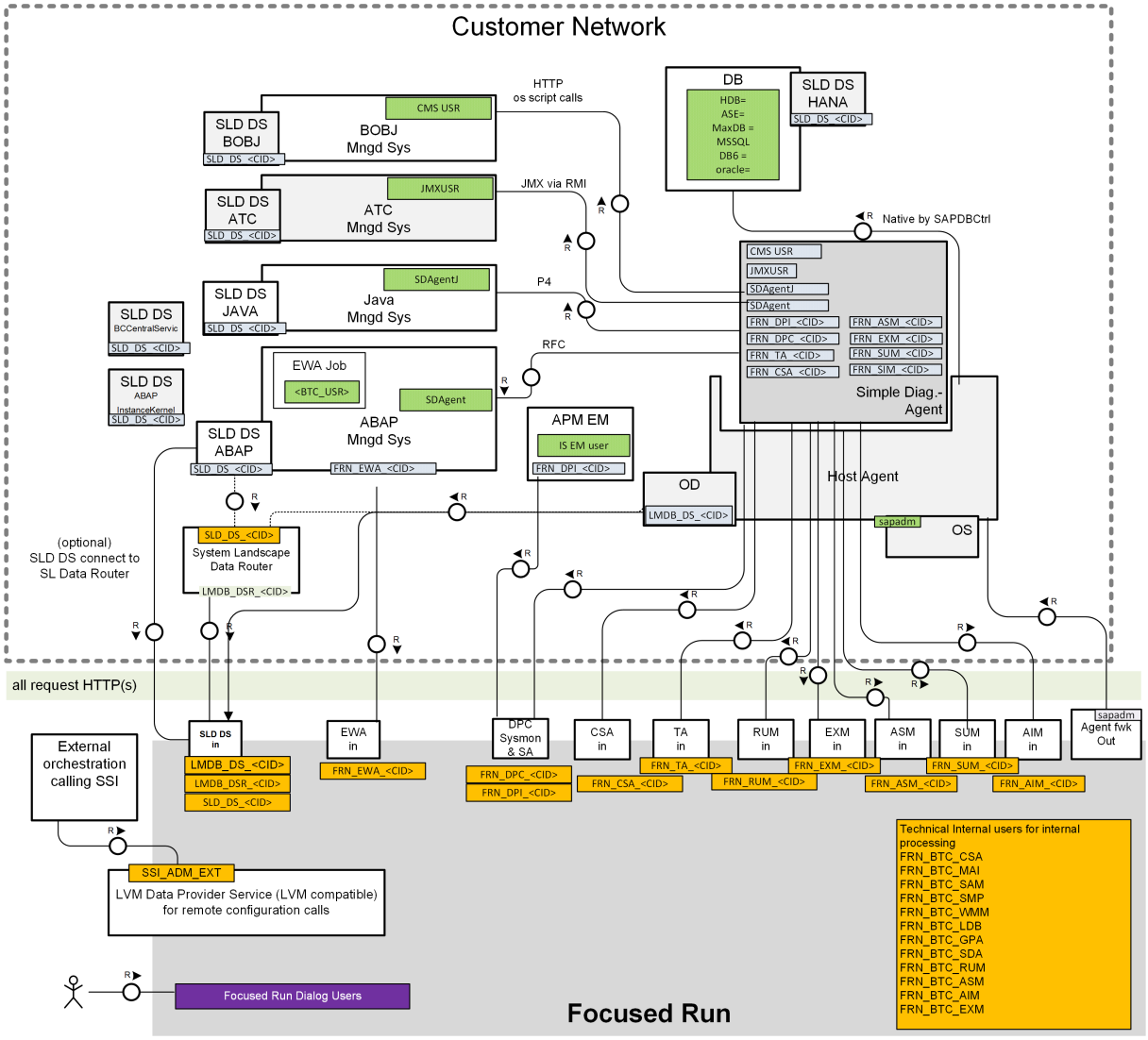
- Proposed Workflow to Assign Authorizations for Dialog Users [page 65]
- Dialog User Roles with Cross-Application Authorizations [page 67]
- Dialog User Roles with SAP Fiori Authorizations [page 70]
- Dialog User Roles with Application Authorization [page 74]
- Roles for Setup Admin and Dev Support [page 91]

Not in the graphic below

S-users can see EWA reports in SAP ONE Support Launchpad, as generated from data uploaded from SAP Focused Run:

S-User Authorizations in SAP ONE Support Launchpad [page 100]

User Overview Graphic



User Management Tools

- The central SAP Focused Run ABAP uses the SAP NetWeaver standard tools. For more information, see https://help.sap.com/viewer/621bb4e3951b4a8ca633ca7ed1c0aba2/latest/en-US/4a114fce13271018e10000000a42189b.html
- For more information regarding managed systems using product-specific user management tools, please see the managed systems documentation.
- The SAP Host Agent does not implement user management. It supports authentication of OS users. For more information regarding OS user management, please see the relevant documentation of your OS provider.
- The Simple Diagnostics Agent does not implement user management. It stores user credentials in secure stores to authenticate requests.

- The SLDR provides simple user management without roles. It allows for edit functions for user IDs (with password) to authenticate incoming SLD payload post-request. For more information, see https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/simple-diagnostic-agent-tls-configuration.html#section
- SSI provides web services to integrate external user management during SSI configurations of managed network and systems for automation purposes. If you plan to automate managed system integration with remote external user management, please send any inquiries via customer tickets (component: SV-FRN-INF-SSI).

Mass Role Generation and Mass User Comparison

After installation of the latest SAP Focused Run version, or after an upgrade to a newer FP, we recommend that you run Tx `PFCC` → Utilities → Mass Generation and → Mass Comparison for roles **SAP_FRN*** in central SAP Focused Run.

Run this as well after an upgrade of **ST-PI** and **ST/A-PI Z_SAP_FRN*** in managed ABAP systems. As a result, you avoid authorization problems due to missing profiles.

5.2.1 New, Changed, and Obsolete Roles with SAP Focused Run

Use

This section offers simple lists of roles (new, changed, obsolete) in SAP Focused Run 2.1. After an upgrade to SAP Focused Run 2.1, this helps your security team to easily search through current custom roles. Update and apply changes to custom roles as necessary.

> ⚠ Caution
>
> New customers or teams implementing SAP Focused Run for the first time should not use this chapter. Please work completely through the other chapters instead.

Changed Roles with SAP Focused Run 2.1

Role Name	Short Description
SAP_FRN_AAD_SUM_ALL	All authorizations for SUM configuration
SAP_FRN_AAD_SUM_MAINT	Maintenance authorizations for SUM configuration
SAP_FRN_APP_MOAL_ALL	All authorizations for System Monitoring & Alert Management

Role Name	Short Description
SAP_FRN_APP_CSA_DISP	Authorizations for CSA APP in display mode
SAP_FRN_APP_CSA_MAINT	Authorizations for CSA APP in maintenance mode
SAP_FRN_APP_CSA_PROTECTED	Authorizations for CSA APP in display mode, including protected results
SAP_FRN_AAD_CSA_ALL	All authorizations for CSA administration
SAP_FRN_BTC_GPA	Authorizations for GPA specific background processing
SAP_FRN_LDB_NOTIF_SSI	Authorizations: Execute for SSI admin application in BTC by FRN_BTC_LDB
SAP_FRN_SSI_ALL	All authorizations - Super Admin - for SSI admin application
SAP_FRN_SSI_MAINT	Authorizations: Execute for SSI admin application
SAP_FRN_BTC_SMP	Authorizations for SPM specific background processing
SAP_FRN_APP_GP_ALL	Full access to Guided Procedures application
SAP_FRN_APP_GP_EXE	Execute access to Guided Procedures application
SAP_FRN_IADM_SSI_USER	Role to authorize int. admin for SSI in FRUN: User
SAP_FRN_AEM_COV_ALL	Admin AEM configuration & consumer variants
SAP_FRN_AEM_COV_DISP	Display AEM configuration & consumer variants
SAP_FRN_AAD_AVM_ALL	All authorizations to configure application Open Component Monitoring Config
SAP_FRN_BTC_AIM	Authorizations for AIM specific background processing
SAP_FRN_BTC_LDB	Authorizations for LMDB specific background processing
SAP_FRN_BTC_CSA	Authorizations for CSA specific background processing
SAP_FRN_UI5_PERS_PUB	Authorizations to create public UI5 custom pages
SAP_FRN_AAD_MOAL_ALL	All authorizations for System Monitoring & Alert Management Administration
SAP_FRN_APP_MOAL_ALL	All authorizations for System Monitoring & Alert Management
SAP_FRN_APP_MOAL_DISP	Display authorizations for System Monitoring & Alert Management
SAP_FRN_AAD_SUM_DISP	Display authorizations for SUM configuration
SAP_FRN_AAD_SUM_ALL	All authorizations for SUM configuration
SAP_FRN_AAD_SUM_MAINT	Maintenance authorizations for SUM configuration
SAP_FRN_BTC_EWA	Authorizations for EWA specific background processing
SAP_FRN_BTC_ASM	Authorizations for ASM specific background processing
SAP_FRN_FI_TACTICAL	Access to tactical dashboards

New Roles with SAP Focused Run 2.1

Role Name	Short Description
SAP_FRN_AJM:	Role for technical user FRN_AJM_<CID>
SAP_FRN_APP_AJM_DISP	Display authorizations for Job Monitoring application
SAP_FRN_APP_AJM_ALL	All authorizations for Job Monitoring application
SAP_FRN_AAD_AJM_ALL	All authorizations to configure Job Monitoring application
SAP_FRN_BTC_AJM	Authorizations for AJM specific background processing
SAP_FRN_APP_EWA_DISP	Display authorizations for application EWA Admin
SAP_FRN_APP_EWA_ALL	Full authorizations for application EWA Admin

Obsolete Roles with SAP Focused Run 2.1

Not applicable	Not applicable

5.2.2 Technical User Creation in Central SAP Focused Run

Use

This section concerns creating technical users in SAP Focused Run, in an early phase of your project.

- Proposed Workflow to Assign Authorizations to Technical Users [page 51]
- Technical Users to Authorizing Incoming HTTP Requests 2.1 [page 52]
- Technical Users Authorizing Batch Processing (2.1) [page 56]
- Technical User to Authorize Internal RFC Calls (2.1) [page 63]

5.2.2.1 Proposed Workflow to Assign Authorizations to Technical Users

Context

For technical users, create a custom role according to your specific needs.

> → Remember
>
> Generate all roles and execute user comparison.

Procedure

1. Go to role maintenance Tx `PFCCG`
2. Create a copy of SAP-standard delivered role `SAP_FRN_*` to your customer namespace (such as Z_SAP_FRN).
3. Choose *Authorization* tab and select *Change*.
4. From menu: *Utilities* → *Technical Names On*
5. Maintain all activity values for each authorization object. The roles delivered with **authorization objects to be maintained** are marked below with an asterisk (*).
6. Save and generate the profile.
7. Select *User* tab. If the user is already assigned, execute *User Comparison*.

   > → Tip
   >
   > You can assign users directly here, if they are already created.
8. Save.

5.2.2.2 Technical Users to Authorizing Incoming HTTP Requests 2.1

Use

Create template users as preparation for customer network creation with Simple System Integration (SSI). SSI generates technical users from these template users, with the expectation that template users already exist.

Each customer namespace has its own set of users most with a three-character customer ID <CID> as post-fix in their names. These users are used to authorize processing of incoming data. Even if there is only one network/namespace LOCALNETWORK and no data separation in SAP Focused Run, there is at least one <CID> of the LOCALNETWORK. These technical users are of type **system**, and are created automatically by SSI at customer network creation. As a prerequisite to achieve this automatic user creation, the below-mentioned template users are to be created.

Template Users

> **i** Note
>
> Template users are of type **reference**.

Template Users and Users Created from Template in SAP Focused Run

Template User	ABAP Role	Technical User Generated by SSI	Description
TPL_FRN_LDDS	**SAP_FRN_LDB_DS**	FRN_LDDS_<CID>	FRN_LDDS_<CID> user is for the authentication of data suppliers sending SLD payloads directly to SAP Focused Run 2.0 (LMDB). FRN_LDSR_<CID> user is for authentication of data suppliers sending SLD payloads via an SLDR. The SLDR has its own user to easily identify the SLD payload sent via SLDR. Both are considered special users in SAP Focused Run.
TPL_FRN_LDSR	All roles indicating **emphasis** have authorization objects that need to be maintained. The following sub-chapter explains the values.	FRN_LDSR_<CID>	
TPL_FRN_CSA	SAP_FRN_CSA	FRN_CSA_<CID>	User to authenticate configuration-analysis requests sent from the SDA to SAP Focused Run (collection of configuration data).
TPL_FRN_DPC	SAP_FRN_DPC	FRN_DPC_<CID>	User to authenticate monitoring requests sent from the SDA to SAP Focused Run (collection of host, DB, system monitoring, and analysis data).
TPL_FRN_DPI	SAP_FRN_DPI	FRN_DPI_<CID>	User to authenticate monitoring requests sent from the CA APM EM to SAP Focused Run (collection of host, DB, system monitoring, system analysis data and open component monitoring data).

Template User	ABAP Role	Technical User Generated by SSI	Description
TPL_FRN_EWA	SAP_FRN_EWA	FRN_EWA_<CID>	User to authenticate EWA requests sent from the ABAP-managed system to SAP Focused Run (collection of ABAP EWA data).
TPL_FRN_TA	SAP_FRN_TA SAP_FRN_LDB_OB_DISP	FRN_TA_<CID>	User to authenticate TA requests sent from the SDA-managed system to SAP Focused Run (collection of TA data).
TPL_FRN_RUM	SAP_FRN_RUM	FRN_RUM_<CID>	User to authenticate RUM requests sent from the SDA-managed system to SAP Focused Run (collection of RUM data).
TPL_FRN_AIM	SAP_FRN_AIM	FRN_AIM_<CID>	User to authenticate AIM requests sent from the SDA-managed system to SAP Focused Run (collection of AIM data).
TPL_FRN_ASM	SAP_FRN_ASM	FRN_ASM_<CID>	User to authenticate STATRAG requests sent from the SDA-managed system to SAP Focused Run (collection of STATRAG data).
TPL_FRN_EXM	SAP_FRN_EXM	FRN_EXM_<CID>	User to authenticate EXM requests sent from the SDA-managed system to SAP Focused Run (collection of EXM data).
TPL_FRN_SUM	**SAP_FRN_SUM**	FRN_SUM_<CID>	User to authenticate SUM requests sent from the SDA-managed system to SAP Focused Run (collection of SUM data).

Template User	ABAP Role	Technical User Generated by SSI	Description
TPL_FRN_SLDS	no role	SLD_DS_<CID>	This user is special. It's only generated at network generation as a preparation of an external user-management effort. This user is intended for authentication of send requests to the SLDR (java application of the SDA) from the SLD DS. This user has no role and no password in ABAP. Do not enter user and password at: RSSI_CHANGE_NETWORK_PASSWORD. If you have no integration with external user management for the SLD DS, enter this user password when you configure the SLDR itself.
TPL_FRN_AJM	SAP_FRN_AJM	FRN_AJM_>CID>	User to authenticate AJM requests sent from the SDA-managed system to SAP Focused Run (collection of AJM data).

SAP_FRN_LDB_DS

The role SAP_FRN_LDB_DS contains authorization objects delivered by SAP with no authorization. Please maintain as shown below.

Authorization Objects of role SAP_FRN_LDB_DS to be maintained

Authorization Object	Authorization Field	Recommended Value	Comment
S_BTCH_JOB	JOBGROUP	*	Job management requirement
AI_LMDB_DS	LMDB_DOMA	LDB	Only the domain LDB (landscape management database) is currently available.

Authorization Object	Authorization Field	Recommended Value	Comment
AI_LMDB_DS	LMDB_NAMES	*	The technical users FRN_LDDS_ FRN_LDSR_ write into the customer namespaces identified internally by namespace hashes. These users are created from template user. The namespace hashes are randomly generated. After the namespaces are operative, consider creating a dedicated role for each namespace and add the namespace with the known namespace hash.
S_BTCH_NAM	BTCUNAME	FRN_BTC*	SAP Focused Run Batch Users

SAP_FRN_SUM

The role SAP_FRN_SUM contains authorization objects delivered by SAP with no authorization. Please maintain as shown below

Authorization Object	Authorization Field	Recommended Value	Comment
S_SUM_AUT	SUM_SCOPE	*	Could be used to separate authorizations by Robot, Script, Network
	SUM_GUID	*	GUID is random-generated

5.2.2.3 Technical Users Authorizing Batch Processing (2.1)

Use

This section describes technical users needed to be created and roles to be maintained for SAP Focused Run internal batch processing.

Batch User in SAP Focused Run

> ⚠ Caution
>
> User type **System** must be assigned to all technical users, as required for batch processing.
>
> Roles marked **<bold>** are delivered with authorization objects that need to be maintained in your custom roles. Find details for each such role in the collapsed sub-sections.
>
> Please maintain the authorization objects carefully. Missing authorizations have caused most troubleshooting sessions in the past.

User ID	Role	Description of Role
FRN_BTC_CSA	SAP_FRN_BTC_CSA	Authorizations to run configuration and security analysis-specific batch processing
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
FRN_BTC_EWA	**SAP_FRN_BTC_EWA**	Authorizations to run SAP EarlyWatch Alert-specific batch processing
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
	SAP_FRN_LDB_OB_DISP	Authorizations to access all LMDB objects
FRN_BTC_LDB	SAP_FRN_BTC_LDB	Authorizations to run LMDB-specific batch processing
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
	SAP_FRN_LDB_NOTIF_SSI	Authorizations to start SSI procedures like *Agent installation* or *Redistribution of templates at DB switchover* triggered by LMDB notification
	SAP_FRN_LDB_OB_DISP	Authorizations to access all LMDB objects
FRN_BTC_MAI	**SAP_FRN_BTC_MAI**	Authorizations to run Monitoring and Alerting Infrastructure-specific batch processing
	SAP_FRN_BTC_GPA	Authorization needs to integrate monitoring alert into guide procedure
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
	SAP_FRN_SND_SNMP_TRAP	Authorizations to create SNMP traps out of alerts
FRN_BTC_RUM	SAP_FRN_BTC_RUM	Authorizations to run Real User Monitoring-specific batch processing

User ID	Role	Description of Role
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
	SAP_FRN_AEM_UMD_ALR	Authorizations to create unmodeled alerts
	SAP_FRN_CNM_SND_NOTIF	Authorizations to send notifications
FRN_BTC_SAM		Authorizations to run Service Level Monitoring-specific batch processing. No role needed
FRN_BTC_SMP	SAP_FRN_BTC_SMP	Authorizations to run service marketplace-specific batch processing, like upload technical system data
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
FRN_BTC_WMM	SAP_FRN_BTC_WMM	Authorizations to run Workmode Management-specific batch processing
FRN_BTC_TA	SAP_FRN_BTC_TA	Authorizations to run TA-specific batch processing
FRN_BTC_CNM	**SAP_FRN_CNM_ALL**	Authorizations to run Central Notification Management-specific batch processing
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
FRN_BTC_AIM	SAP_FRN_BTC_AIM	Authorizations to run Advanced Integration Monitoring-specific batch processing
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network.
	SAP_FRN_AEM_UMD_ALR	Authorizations to create unmodeled alerts
	SAP_FRN_LDB_OB_DISP	Authorizations to access all LMDB objects
	SAP_FRN_CNM_SND_NOTIF	Authorizations to send notifications
FRN_BTC_SRA	**SAP_FRN_BTC_SRA**	Authorizations to the scheduling, replication and aggregation FWK to start data aggregation jobs for various applications and collections of cloud monitoring data
	SAP_FRN_AIM	Authorizations to run Advanced Integration Monitoring-specific batch processing
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
	SAP_FRN_AAD_SYA_ALL	All authorizations for system analytics application administration

User ID	Role	Description of Role
	SAP_FRN_AEM_UMD_ALR	Authorizations to create unmodeled alerts
	SAP_FRN_SUM_ALRT_ENG	Authorizations to execute Synthetic User Monitoring alerts
	SAP_FRN_BTC_RUM	Authorizations to run Real User Monitoring-specific batch processing
	SAP_FRN_CNM_SND_NOTIF	Authorizations to send notifications
	SAP_FRN_AAD_AIM_ALL	All Authorizations for AIM Administration
FRN_BTC_AEM	SAP_FRN_BTC_AEM	Authorizations to run Advanced Event Management-specific batch processing
FRN_BTC_ASM	SAP_FRN_BTC_ASM	User with authorizations to run ASM-specific batch processing
	SAP_FRN_LDB_OB_DISP	Authorizations to access all LMDB objects
FRN_BTC_GPA	**SAP_FRN_BTC_GPA**	User with authorizations to run guided procedure- specific batch processing
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
FRN_BTC_PAS	SAP_FRN_BTC_PAS	User with authorizations to run batch processing for system anomaly prediction
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
	SAP_FRN_LDB_OB_DISP	Authorizations to access all LMDB objects
FRN_BTC_AJM	SAP_FRN_BTC_AJM	Authorizations for AJM specific background processing
	SAP_FRN_CNW_ACCESS_ADMIN	Enable data separation controlled by customer network
	SAP_FRN_LDB_OB_DISP	Authorization to access all LMDB objects
	SAP_FRN_CNM_SND_NOTIF	Authorizations to send notifications

SAP_FRN_BTC_EWA

The role SAP_FRN_BTC_EWA contains authorization objects with no authorization, delivered by SAP. Please maintain as shown below:

SAP_FRN_BTC_EWA authorization objects to be maintained

Authorization Objects	Authorization Field	Recommended Value	Comment
S_RFC_ADM	ICF_VALUE	*	See online documentation
	RFCTYPE	*	Depends on connection type not known at installation. Consider entering the known destination type of destination created with SDCCN
S_BTCH_JOB	JOBGROUP	*	Job management requirement
S_RFC_ADM	ACTVT	03	Necessary for step execution of job SAP_FRN_EWA_SEND_REPORT (report FRUN_DOWNLOADS_REPORT) Please see SAP Note 2758118
	RFCDEST	SAP-SUPPORT_PARCELBOX	
		SAP-SUPPORT_PORTAL	
		SDCC_OSS	
		SM_SP_*	

SAP_FRN_CNM_ALL

The role SAP_FRN_CNM_ALL contains authorization objects with no authorization, delivered by SAP. Please maintain as shown below:

SAP_FRN_CNM_ALL Authorization Objects to be Maintained

Authorization Objects	Authorization Field	Recommended Value	Comment
S_RFC_ADM	ICF_VALUE	*	See online documentation
	RFCDEST	*	Depends on the name(s) of the destination to SLD. For content sync not known at installation, consider entering the known destination name
S_LDAP	LDAP_SERV	<empty> or customer-specific	If external LDAP is used
S_USER_GRP	CLASS	* or IDs of users for notification from SU01	In case user IDs from SU01 should be used to create notification groups
SM_CNM_AUT	CNM_APPACT	WMM	Only possible value

SAP_FRN_BTC_MAI

The role SAP_FRN_BTC_MAI contains authorization objects with no authorization, delivered by SAP. Please maintain as shown below:

SAP_FRN_BTC_MAI Authorization Objects to be Maintained

Authorization Objects	Authorization Field	Recommended Value	Comment
S_RFC_ADM	ICF_VALUE	*	See online documentation
	RFCDEST	*	Destination names to all SAP host agents needed in case of mass update of configurations. It is advised to keep this as "*" due to the high effort to maintain
S_USER_GRP	CLASS	*	See online documentation
AI_LMDB_AD	LMDB_NAMES	*	The technical users FRN_BTC_MAI must have access to all LMDB namespaces (filter here is only advised for dialog user, to restrict access)
AI_LMDB_OB	LMDB_MTYPE	*	The technical users FRN_BTC_MAI must have access to all LMDB objects (a filter here is only advised for dialog user, to restrict access)
	LMDB_NAMES	*	
	LMDB_OBJID	*	
	LMDB_STYPE	*	

SAP_FRN_SND_SNMP_TRAP

The role SAP_FRN_SND_SNMP_TRAP contains authorization objects with no authorization, delivered by SAP. Please maintain as shown below:

SAP_FRN_SND_SNMP_TRAP Authorization Objects to be Maintained

Authorization Objects	Authorization Field	Recommended Value	Comment
S_LOG_COM	HOST	<hostname>	Hostname of SAP Focused Run application server, which should create SNMP traps for alert-forwarding with SNMP

SAP_FRN_BTC_SRA

The role SAP_FRN_BTC_SRA contains authorization objects with no authorization, delivered by SAP. Please maintain as shown below:

SAP_FRN_BTC_SRA Authorization Objects to be Maintained

Authorization Objects	Authorization Field	Recommended Value	Comment
AI_LMDB_OB	LMDB_MTYPE	*	The technical users FRN_BTC_MAI must have access to all LMDB objects (a filter here is only advised for dialog user, to restrict access)
	LMDB_NAMES	*	
	LMDB_OBJID	*	
	LMDB_STYPE	*	

SAP_FRN_AAD_SYA_ALL

The role SAP_FRN_AAD_SYA_ALL contains authorization objects with no authorization, delivered by SAP. Please maintain as shown below:

SAP_FRN_AAD_SYA_ALL Authorization Objects to be Maintained

Authorization Objects	Authorization Field	Recommended Value	Comment
S_BTCH_JOB	JOBGROUP	*	Job management requirement
S_DATASET	FILENAME	*	File name not known at configuration time

SAP_FRN_BTC_GPA

The role SAP_FRN_BTC_GPA contains authorization objects with no authorization, delivered by SAP. Please maintain as shown below:

SAP_FRN_BTC_GPA Authorization Objects to be Maintained

Authorization Objects	Authorization Field	Recommended Value	Comment
S_ICF_ADM	ICF_NODE	*	A randomly-generated hash, created at GP generation. The batch user must have access to all GPs (for housekeeping, for example)
S_DATASET	FILENAME	*	File name not known at configuration time
S_BTC_JOB	JOBGROUP	*	Job management requirement

Authorization Objects	Authorization Field	Recommended Value	Comment
S_DEVELOP	DEV_CLASS	*	Customer package name for logos to be included in HTML reports generated as part of the GPs
	OBJNAME	*	Customer object name for logos to be included in HTML reports generated as part of the GPs
	P_GROUP	*	Customer programs to be included in the GPs
AI_LMDB_OB	LMDB_NAMES	*	The technical users FRN_BTC_GPA must have access to all LMDB objects (a filter here is only advised for dialog user, to restrict access)
	LMDB_OBJID	*	
	LMDB_STYPE	*	
SM_SETUP	SCENARIOS	*	GP scenario name not known before GP creation
	STEPS	*	GP step name not known before GP creation

5.2.2.4 Technical User to Authorize Internal RFC Calls (2.1)

User

This section describes the automated creation of users from template users, if no external user management solution is available at customer site.

Internal RFC User in SAP Focused Run

> ⚠ Caution
>
> Technical user should be of type: **System**

User ID	Role	Description
FRN_IADM_SSI	SAP_FRN_IADM_SSI_COMP Composite role including roles: **SAP_FRN_IADM_SSI_USER** SAP_FRN_IADM_SSI_USER_DELETE	The user having this role is used in the local SM59 RFC destination: SSI_USER_ADMIN_CONNECTION

SAP_FRN_IADM_SSI_USER

The role SAP_FRN_IADM_SSI_USER contains authorization objects with no authorization, delivered by SAP. Please maintain as shown below:

SAP_FRN_IADM_SSI_USER Authorization Objects to be Maintained

Authorization Objects	Authorization Field	Delivered Value	Comment
S_USER_AGR	ACT_GROUP	SAP_FRN* Z_SAP_FRN*	Grant authorizations to assign the roles you have assigned to the template users. If you have created custom roles you need to maintain this group with your **custom role names (such as Z_SAP_FRN*)**
S_USER_SAS	SUBSYSTEM	*	Receiving system for central user administration
	ACT_GROUP	SAP_FRN* Z_SAP_FRN*	Grant authorizations to assign the roles you have assigned to the template users. If you have created custom roles, you need to maintain this group with your **custom role names (such as Z_SAP_FRN*)**

5.2.3 Dialog User Creation in Central SAP Focused Run

Use

Create dialog users in SAP Focused Run.

Role User Types

There are three different kinds of roles delivered with SAP Focused Run:

- Roles with cross-application authorizations: To define the cross UI-features you can use in SAP Fiori UIs (some are mandatory).
- Roles with SAP Fiori authorizations: To define the SAP Fiori tiles you see and how they are grouped in the SAP Fiori launchpad
- Roles with application authorizations: To define what you can do in the application.

- Proposed Workflow to Assign Authorizations for Dialog Users [page 65]
- Dialog User Roles with Cross-Application Authorizations [page 67]
- Dialog User Roles with SAP Fiori Authorizations [page 70]
- Dialog User Roles with Application Authorization [page 74]
- Roles for Setup Admin and Dev Support [page 91]

5.2.3.1 Proposed Workflow to Assign Authorizations for Dialog Users

Context

Create dialog users and custom roles for your specific needs in central SAP Focused Run.

> → Tip
>
> Execute the task flow below for one team member with defined responsibility to get an impression about the function of the cross-application and SAP Fiori roles.

> → Remember
>
> Generate all roles and execute user comparison.

Procedure

1. Define operation team responsibilities and team members. For guests and customers, define supported self-services.
2. Create named dialog user in SAP Focused Run for each team member. Similarly, create a dialog user for guests and customers.
3. Create custom **cross-application** roles from Dialog User Roles with Cross-Application Authorizations [page 67] as delivered. Maintain the authorization fields with empty values according to defined

responsibilities. Maintain this authorization for granting visibility to systems, custom networks, customers, and others. This grants functionality to applications roles.

> → Tip
>
> Use the role `SAP_FRN_CNW_ACCESS` to manage and limit access to objects in customer networks. The LMDB role`SAP_FRN_LDB_OB_DISP` you can use to grant access only to databases, or only to ABAP systems with SID starting with P*.
>
> If you like to grant access to all system types in on Managed System you maintain * as values in the fields of `SAP_FRN_LDB_OB_DISP`
>
> Other cross-application roles can be assigned as they are, if your security policy does not say otherwise. This are technical roles and do not need to be adapted in Z*# roles.

   a. Assign custom **cross-application** roles to dialog users.

4. Assign the delivered SAP Focused Run Dialog User Roles with SAP Fiori Authorizations [page 70] according to your utilized SAP Focused Run user cases and dialog user team functions.
5. **(Optional)** If you like to hide certain SAP Fiori tiles from users or to organize the SAP Fiori tiles in custom groups, please create your own SAP Fiori groups in the launchpad designer and add tiles **https://<server>:<port>/sap/bc/ui5_ui5/sap/arsrvc_upb_admn/main.html**. For documentation of the SAP Fiori launchpad and the launchpad designer, see: https://help.sap.com/viewer/a7b390faab1140c087b8926571e942b7/latest/en-US/2d98610a5bcf43dfad588e755459dc42.html
   a. Create custom ABAP roles to grant access to your custom SAP Fiori Groups.

> → Tip
>
> Use the delivered SAP Focused Run roles for SAP Fiori catalogs to see how to create custom roles. As this role does not contain ABAP authorizations, you assign navigation targets in the `PFCG` role menu tab *Menu*.

6. Create custom application roles from the delivered Dialog User Roles with Application Authorization [page 74]. According to defined responsibilities, maintain the authorization object of the role for granting operations. Authorization objects of these roles must be maintained before you can use the roles.

> ⚠ Caution
>
> Various roles are delivered with authorization fields containing empty values. Create custom roles upfront for this role and maintain the empty values. Do not miss a field or a role for generating user comparison. Such oversight accounts for most troubleshooting issues.

   a. Assign SAP Focused Run custom application roles to the dialog user.

5.2.3.2 Dialog User Roles with Cross-Application Authorizations

Use

This section describes delivered cross-application roles and authorization objects to be maintained to create custom roles.

Roles Types

There are two groups of cross-application roles:

- Roles that enable you to control display and operational access to managed objects in your IT landscape in SAP Focused Run with different severities.
- Roles that grant access to tools, which work across applications.

Managed Objects Access Control

All managed objects including customer networks in SAP Focused Run are modeled in the LMDB. By granting access to the different objects in the LMDB, the data separation in SAP Focused Run is controlled. With the **customer roles** created from the roles in the table below, you can control access to managed objects.

MO Access Control Roles

Role Name	Comment	Assign custom role to
`SAP_FRN_SCOPE_SEL`	Role to get the tool **scope selection** in SAP Fiori UIs. Mentioned here also because the **scope selection** is a tool needed to select managed objects in all SAP Fiori UIs of SAP Focused Run. Without having it, you cannot apply the authorizations on managed objects granted by the roles below	All
`SAP_FRN_CNW_ACCESS_ADMIN`	Grants access to all managed objects in all customer networks, customers, or data centers	Only administrators and technical users where you not limit the access by customer network
`SAP_FRN_CNW_ACCESS` to be maintained	By maintaining the authorization fields values, you manage the access to managed objects on the level of customer networks, customer ID, or data center	All that don't have the following: `SAP_FRN_CNW_ACCESS_ADMIN`

Role Name	Comment	Assign custom role to
SAP_FRN_LDB_OB_DISP optional to be maintained	By maintaining the authorization fields values, you manage the access to managed objects on the level of technical system and host	All. This role is created for LMDB access when using operations. You must have access to LMDB objects emedded from a applications UI. There is another role "SAP_FRN_LDB_DISP" needed when using the LMDB UI directly

SAP_FRN_CNW_ACCESS

The role SAP_FRN_CNW_ACCESS contains authorization object LMDB_CN, delivered by SAP with field value LMDB_CN. Please maintain in your **customer roles**, the object LMDB_CN to grant access to dedicated LMDB namespaces.

Role SAP_FRN_CNW_ACCESS

Authorization object	Field	Value
LMDB_CN	LDB_CUSNET	Name of Customer Network (Name)
	LDB_CUST	Customer ID (CID
	DB_DCL	Data center ID (DC-ID)

SAP_FRN_LDB_OB_DISP

The role SAP_FRN_LDB_OB_DISP contains authorization objects delivered with no authorization values by SAP. For AI_LMDB_OB. Maintain the listed authorization values in your customer roles as below, if you want to manage authorization to dedicated LMDB objects.

Role SAP_FRN_LDB_OB_DISP

Authorization object	Field	Value as delivered	Comment
AI_LMDB_OB	LDB_NAMES	*	See documentation (maintain this field as an exception only; namespace access is granted with SAP_FRN_CNW_ACCESS).
	LMDB_STYPE	ABAP	Maintain to grant access to dedicated object type
		ATC	
		SAP BusinessObjects	
		CLOUD_CONN	
		DBSYSTEM	
		DIAGNAGENT	
		EXT_SRV	
		HANADB	
		IS_EM	
		IS_MOM	
		JAVA	

Authorization object	Field	Value as delivered	Comment
		LIVE_CACHE	
		MDM	
		MSIISINST	
		MS_.NET	
		Sybase Unwired Platform	
		TREX	
		UNSP3TIER	
		UNSPAPP	
		UNSPECIFIC	
	LMDB_OBJID	*	See documentation. Maintain this field as an exception only if you want to grant access on by object ID **LMDB GUID**

Tool Roles

The tools roles grant access to certain tools that can be reused in different SAP Fiori UIs.

> → Tip
>
> If it does not conflict with your security policies, consider assigning the tools roles as delivered.

Tool Roles

Role Name	Description	Assign to
SAP_FRN_FLP_EMBEDDED	Role to enable the SAP Fiori launchpad. Mentioned here because the SAP Fiori launchpad is the tool to access all SAP Focused Run end user UIs	Mandatory all
SAP_FRN_SCOPE_SEL	Role to get the tool **scope selection** in SAP Fiori UIs. Scope selection is needed to select managed objects in all SAP Fiori UIs of SAP Focused Run. The scope selection provides sophisticated features to create and manged prede-fined filters	Mandatory all
SAP_FRN_SCOPE_SEL_PUB_FILTER	Authorizations to create public filters for scope selection	Key users
SAP_FRN_UI5_PERS_PUB	Authorizations to create public SAPUI5 customization in the granted SAP Focused Run application	Key users

Role Name	Description	Assign to
SAP_FRN_CNM_SND_NOTIF	Role to get the tool **send notification** from within SAP Fiori UIs. The **send notification** provided sophisticated features to send notifications with content from SAP Fiori UI to recipients maintain in central notification management	Optional all. Prerequisite is to maintain recipients in CNM
SAP_FRN_APP_AEM_ALR_INB_DISP	Role to get the tool **alert inbox in** SAP Fiori UIs. This enables you to jump context sensitive into the alert inbox	Only groups working with alerts
SAP_FRN_APP_AEM_ALR_TIC	Role to get the tool **alert ticket** in SAP Fiori UIs. This enables the alert ticket in SAP Fiori UIs	Only groups working with alerts

5.2.3.3 Dialog User Roles with SAP Fiori Authorizations

Use

Description of delivered SAP Fiori groups, SAP Fiori catalogs, and mapped ABAP roles. Assign the roles directly to dialog users and create custom roles.

Background

SAP Fiori authorizations are effective on SAP Fiori catalogs and SAP Fiori groups. For SAP Focused Run use cases, analog SAP Fiori groups are delivered. SAP Focused Run applications tiles are included in delivered SAP Fiori catalogs.

Each SAP Focused Run application provides for end user SAP Fiori tiles in the SAP Fiori launchpad to access the application UIs. The application *Real User Monitoring* has its UI with tile name *Real User Monitoring*. This tile is included in `SAP Fiori catalog`, FRN Real User Monitoring.

The access to this SAP Fiori catalog is granted by the standard role `SAP_FRN_FLP_CAT_AAD_SYM`. The access is granted in the role like access to a transaction. Check the role to see that this is only a navigation target.

The tiles are part of the SAP Fiori group `FRN_AdvancedUserManagement` analog to the SAP Focused Run use case.

The access to this SAP Fiori Group is granted by the role SAP_FRN_FLP_2_AUM. The access is granted in the role like access to a transaction.

> → Tip
>
> SAP Fiori catalogs are included in SAP Fiori Groups, not the other way around.
>
> For more information regarding how to maintain custom SAP Fiori Catalogs and SAP Fiori Groups, please reference **SAP Fiori launchpad Designer** in the official SAP Fiori Documentation at https://help.sap.com/viewer/cc1c7615ee2f4a699a9272453379006c/latest/en-US/f951b50a07ce41deb08ced62711fe8b5.html.

SAP Focused Run Home

SAP Fiori Group technical name =`FRUNHome`

ABAP Role on SAP Fiori Group = `SAP_FRN_FLP_0_FRNH`

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
SAP Focused Run	FRUNHome	Home Page	`SAP_FRN_FLP_0_FRNH`
		Help Portal	
		Expert Portal	
		White Paper	

Advanced Dashboarding & Intelligence

SAP Fiori Group technical name =`FRN_AdvancedDashboardingIntelligence`

ABAP Role on SAP Fiori Group = `SAP_FRN_FLP_1_1_ADI`

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
Tactical Dashboards	`FRN_Insights`	<empty>	`SAP_FRN_FLP_CAT_FI_TAC`
OCC Dashboards	`FRN_Insights`	<empty>	`SAP_FRN_FLP_CAT_FI_TAC`

Advanced System Management

SAP Fiori Group technical name =`FRN_AdvancedSystemManagement`

ABAP Role on SAP Fiori Group = `SAP_FRN_FLP_1_ASM`

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
System Monitoring	`FRN_SystemMonitoring`	<empty>	`SAP_FRN_FLP_CAT_APP_SYM`
System Monitoring Administration	`FRN_SystemMonitoring`	Template Maintenance	`SAP_FRN_FLP_CAT_AAD_SYM`
		Individual Maintenance	
		Content Update	
Open Component Monitoring	`FRN_AdvancedMonitoring`	<empty>	`SAP_FRN_FLP_CAT_AVM`
System Management	`FRN_GuidedProcedureASM`	Guided Procedure Catalog	`SAP_FRN_FLP_CAT_GPB`
		Guided Procedure Reporting	

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
IT Calendar & Work Mode Management	FRN_IT_CalendarWorkModeManagement	<empty>	SAP_FRN_FLP_CAT_APP_ITC
Service Availability Management	FRN_ServiceAvailabilityManagement	<empty>	SAP_FRN_FLP_CAT_APP_SAM
License Management	FRN_LicenseManagement	<empty>	SAP_FRN_FLP_CAT_LICM
SAP EarlyWatch Alert Status	FRN_EWA_Reports	<empty>	SAP_FRN_FLP_CAT_EWA
SAP EarlyWatch Alerts Reports	FRN_EWA_Reports	S- User required	SAP_FRN_FLP_CAT_EWA
SAP EarlyWatch Workspace	FRN_EWA_Reports	S- User required	SAP_FRN_FLP_CAT_EWA
Maintenance Planner	FRN_MaintenancePlanner	SAP ONE Support Cloud	SAP_FRN_FLP_CAT_MPL

Advanced User Monitoring and ABAP role

Fiori Group technical name =FRN_AdvancedUserManagement

ABAP Role on SAP Fiori Group = SAP_FRN_FLP_2_AUM

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
Real User Monitoring	FRN_RealUserMonitoring	<empty>	SAP_FRN_FLP_CAT_APP_RUM
Synthetic User Monitoring	FRN_SyntheticUserMonitoring	<empty>	SAP_FRN_FLP_CAT_APP_SUM
		Configuration	

Advanced Integration Monitoring

SAP Fiori Group technical name =FRN_AdvancedIntegrationMonitoring

ABAP Role on SAP Fiori Group = SAP_FRN_FLP_3_1_AIM

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
Integration & Cloud Monitoring	FRN_AdvancedIntegrationMonitoring	<empty>	SAP_FRN_FLP_CAT_APP_AIM
	FRN_AdvIntegrMonAdministration	Configuration	SAP_FRN_FLP_CAT_AAD_AIM
Cloud Service Management		Configuration	

Advanced Event & Alert Management

SAP Fiori Group technical name =`FRN_AdvancedEventAlertManagement`

ABAP Role on SAP Fiori Group = `SAP_FRN_FLP_3_AEM`

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
Alert Management	FRN_AdvancedEventAlert-Management	<empty>	SAP_FRN_FLP_CAT_APP_AEM
	FRN_AdvEventAlertMgmtAdministration	Alerting Consumer Settings	SAP_FRN_FLP_CAT_AAD_AEM
	FRN_GuidedProcedureAEM	Guided Procedure Catalog	SAP_FRN_FLP_CAT_GPR
		Guided Procedure Reporting	

Advanced Configuration Monitoring

SAP Fiori Group technical name =`FRN_ConfigurationSecurityAnalytics`

ABAP Role on SAP Fiori Group = `SAP_FRN_FLP_4_CSA`

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
Configuration & Security Analytics	FRN_ConfigurationSecurityAnalytics	<empty>	SAP_FRN_FLP_CAT_APP_CSA
	FRN_ConfigurationSecurityAnalyAdmin	Administration	SAP_FRN_FLP_CAT_AAD_CSA

Advanced Root Cause Analysis

SAP Fiori Group technical name =`FRN_AdvancedRootCauseAnalysis`

ABAP Role on SAP Fiori Group = `SAP_FRN_FLP_5_5_RCA`

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
System Analysis	SAP_FRN_FLP_CAT_APP_SYA	<empty>	SAP_FRN_FLP_CAT_APP_SYA
		Configuration	
Trace Analysis	FRN_TraceAnalysis	<empty>	SAP_FRN_FLP_CAT_APP_TA
File System Browser	FRN_Filesystem_Browser	<empty>	

Infrastructure Administration

SAP Fiori Group technical name =`FRN_InfrastructureAdministration`

ABAP Role on SAP Fiori Group = `SAP_FRN_FLP_5_ISA`

Tile Title	Catalog Name	Tile Subtitle	ABAP Role for the SAP Fiori Catalog
LMDB	FRN_InfrastructureAdministration	Object Maintenance	SAP_FRN_FLP_5_ISA
		Administration	
Global Settings & Network Configuration		<empty>	
Simple System Integration		<empty>	
Agent Administration		<empty>	
Self-Monitoring		<empty>	
Self-Monitoring		Dashboard	
Expert Scheduling Management Cockpit		<empty>	
Central Notification Management		<empty>	

5.2.3.4 Dialog User Roles with Application Authorization

Use

This section describes delivered ABAP application roles. Create customer roles based on team functions.

All roles listed together with the applications have full function in the relative application, even if the role belongs to a different application. Cross-application roles are no longer redundantly listed.

Background

SAP Focused Run applications are written in ABAP with ABAP authorization objects. Authorizations on those objects are incorporated in roles. SAP Focused Run applications are grouped by SAP Focused Run use cases.

> ⚠ Caution
>
> Please maintain the authorization objects carefully. Missing authorization issues typically cause the most troubleshooting sessions.

Roles Delivered with Authorization Fields with Empty Values. To be Maintained!

SAP_FRN_CNW_ACCESS

Create a custom role for each customer namespace. Mentioned here redundantly. You should have already maintained this as part off the cross-application roles

Authorization object	Field	Proposed Value	Comment
LMDB_CN	LDB_CUSNET	<custom>	Customer network attributes to separate customer-specific read access
	LDB_CUST		
	LDB_DC		

SAP_FRN_AAD_AVM_ALL

Authorization object	Field	Proposed Value	Comment
FRN_CUSTOP	CUSTOM_OPE	<custom>	Default value is SAPHostAgent.Ping. Please enter list of custom operations user is allowed to execute

SAP_FRN_AAD_MOAL_ALL

Authorization object	Field	Proposed Value	Comment
S_BTCH_JOB	JOBGROUP	*	Required by job management
S_BTCH_NAM	BTCUNAME	FRN_BTC_*	SAP Focused Run batch users
S_DEVELOP	OBJNAME	*	Display all objects and groups as in the defined package
	P_GROUP		
S_SYS_RWBO	DESTSYS	<custom>	Customer specific how to transport the templates
	DOMAIN		
S_DATASET	FILENAME	*	File names not known

SAP_FRN_AAD_SYA_ALL

Authorization object	Field	Proposed Value	Comment
S_BTCH_JOB	JOBGROUP	*	Required by job management
S_DATASET	FILENAME	*	File name not known

SAP_FRN_APP_GP_DISP

Authorization object	Field	Proposed Value	Comment
S_DEVELOP	DEVCLASS	<custom>	Customer-specific for LOGO integrated in HTML report
	OBJNAME		
	P_GROUP		

SAP_FRN_APP_GP_ALL

Authorization object	Field	Proposed Value	Comment
S_BTCH_JOB	JOBGROUP	*	Required by job management
S_DATASET	FILENAME	*	File names not known
S_DEVELOP	DEVCLASS	<custom>	Customer-specific for LOGO integrated in HTML report
	OBJNAME		
	P_GROUP		
S_DOKU_AUT	DOKU_DEVCL	<custom>	Customer-specific document class
S_SYS_RWBO	DESTSYS	<custom>	Customer-specific where to transport GPs
	DOMAIN		
S_APPL_LOG	ALG_OBJECT	*	Various application log objects
	ALG_SUBOBJ		
SM_SETUP	SCENARIOS	*	Scenarios and steps not known
	STEPS		

SAP_FRN_AAD_RUM_ALL

Authorization object	Field	Proposed Value	Comment
S_BTCH_JOB	JOBGROUP	*	Required by job management

SAP_FRN_APP_CSA_DISP

Authorization object	Field	Proposed Value	Comment
SRSM_CA_AP	CA_AREA	VALIDATION	The display authorization for the different applications (areas) allows the user to display the data. The areas of CSA are validation, changes, search, and store browser. The field CA_AREA *Name of Application* controls the areas for which the user can display data
		POLICY	
		CHANGES	
		SEARCH	
		STOREBROWSER	
SRSM_CV_TS	CV_TARDEF	*	Target system and user where the CS&A should be effective
	CV_TARUSR		

SAP_FRN_APP_CSA_MAINT

Authorization object	Field	Proposed Value	Comment
SRSM_CA_AP	CA_AREA	VALIDATION	Security object ready for coming releases to separate access to different CSA functions
		POLICY	
		CHANGES	

Authorization object	Field	Proposed Value	Comment
		SEARCH	
		STOREBROWSER	
SRSM_CV_TS	CV_TARDEF	*	Target system and user where the CS&A should be effective
	CV_TARUSR		

SAP_FRN_APP_CSA_PROTECTED

Authorization object	Field	Proposed Value	Comment
SRSM_CA_AP	CA_AREA	VALIDATION	Security object ready for coming releases to separate access to different CSA functions
		POLICY	
		CHANGES	
		SEARCH	
		STOREBROWSER	
SRSM_CV_TS	CV_TARDEF	*	Target system and user where the CS&A should be effective
	CV_TARUSR		

SAP_FRN_LDB_OB_DISP

Authorization object	Field	Value as delivered	Comment
AI_LMDB_OB	LDB_NAMES	*	See documentation (maintain this field as an exception only; namespace access is granted with SAP_FRN_CNW_ACCESS).
	LMDB_STYPE	ABAP	Maintain to grant access to dedicated object type
		ATC	
		BOBJ	
		CLOUD_CONN	
		DBSYSTEM	
		DIAGNAGENT	
		EXRT_SERV	
		HANADB	
		IS_EN	
		IS_MOM	
		JAVA	
		LIVE_CACHE	
		mdm	
		MSIISINST	
		MS_.NET	

Authorization object	Field	Value as delivered	Comment
		SUP	
		TREX	
		UNSP3TIER	
		UNSPAPP	
		UNSPECIFIC	
	LMDB_OBJID	*	See documentation. Maintain this field as an exception only if you want to grant access on by object ID **LMDB GUID**

SAP_FRN_LDB_ALL

Authorization object	Field	Proposed Value	Comment
S_BTCH_JOB	JOBGROUP	*	Demanded by job management
AI_LMDB_AD	LMDB_NAMES	*	LMDB names are random hashes
AI_LMDB_OB	LMDB_NAMES	*	LMDB names and object IDs are random hashes
	LMDB_OBJID	*	
	LMDB_MTYPE	*	Limitation possible depending on functional team roles or customer specific
	LMDB_STYPE		
AI_LMDB_PS	LMDB_NAMES	*	LMDB names are random hashes
	PS_NAME		
AI_LMDB_TM	LMDB_DOMA	LDB	LMDB domain, only LMDB is supported
	LMDB_NAMES	*	LMDB names are random hashes

SAP_FRN_LDB_DISP

Authorization object	Field	Proposed Value	Comment
AI_LMDB_OB	LMDB_NAMES	*	LMDB names and object IDs are random
	LMDB_OBJID	*	
	LMDB_STYPE	as delivered or limit to Systems Types only, for example	As delivered, unless limited access desired
	LMDB_STYPE	*	LMDB names and object IDs are random hashes
AI_LMDB_PS	LMDB_NAMES	*	LMDB names and object IDs are random

Authorization object	Field	Proposed Value	Comment
	PS_NAME	*	LMDB names and object IDs are random
AI_LMDB_TM	LMDB_DOMA	LDB	LMDB domain, only LMDB is supported

SAP_FRN_LDB_MAINT

Authorization object	Field	Proposed Value	Comment
S_BTCH_JOB	JOBGROUP	*	Required by job management
AI_LMDB_AD	LMDB_NAMES	*	LMDB names are random hashes
AI_LMDB_OB	LMDB_NAMES	*	LMDB names and object IDs are random hashes
	LMDB_OBJID	*	
	LMDB_MTYPE	*	Limitation possible depending on functional team roles or customer-specific
	LMDB_STYPE		
AI_LMDB_PS	LMDB_NAMES	*	LMDB names are random hashes
	PS_NAME		
AI_LMDB_TM	LMDB_DOMA	LDB	LMDB domain, only LMDB is supported
	LMDB_NAMES	*	LMDB names are random hashes

SAP_FRN_SDA_ALL

Authorization object	Field	Proposed Value	Comment
S_BTCH_JOB	JOBGROUP	*	Required by job management

SAP_FRN_CNM_DISP

Authorization object	Field	Proposed Value	Comment
S_RFC_ADM	ICF_VALUE	*	Depend on customer SCOTsettings
	RFCDEST	*	
S_LDAP	LDAP_SERV	<empty> or customer specific	If external LMDB is used
S_USER_GRP	CLASS		If user IDs from SU01 should be used to create notification groups
SM_CNM_AUT	CNM_APPACT	WMM	Only possible value

SAP_FRN_CNM_ALL

Authorization object	Field	Proposed Value	Comment
S_RFC_ADM	ICF_VALUE	*	Depends on customer SCOTsettings
	RFCDEST		

Authorization object	Field	Proposed Value	Comment
S_LDAP	LDAP_SERV	<empty> or customer specific	If external LDAP is used
S_USER_GRP	CLASS	* or IDs of users for notification from SU01	In case user IDs from SU01 should be utilized to create notification groups
SM_CNM_AUT	CNM_APPACT	WMM	Only possible value

SAP_FRN_TECH_MON_TOOL

Authorization object	Field	Proposed Value	Comment
S_DEVELOP	DEVCLASS	*	Role recommended for dev support
	OBJNAME		
	OBJTYPE		
	P_GROUP		
S_DATASET	FILENAME	*	
	FILENAME		
S_PROGRAM	P_GROUP	*	
S_TRANSLAT	TLANGUAGE	*	
S_APPL_LOG	ALG_OBJECT	*	
	ALG_SUBOBJ		

SAP_FRN_OPR_ALL

Authorization object	Field	Proposed Value	Comment
S_DATASET	FILENAME	*	File names not known

SAP_FRN_SSI_ALL

Authorization object	Field	Proposed Value	Comment
S_DATASET	FILENAME	*	File names not known
S_DEVELOP	DEVCLASS	<empty>	<empty>
	OBJNAME		
	OBJTYPE		
	P_GROUP		
S_RFC_ADM	RFCDEST	*	Value are the SM59 destination to external servers (SAPHOSTAGENT) to be created by SSI, convention is HOSTNAME_NAMESPACE. As such needs to be created for all hosts connected to SAP Focused Run * is recommended

Authorization object	Field	Proposed Value	Comment
	ICF_VALUE	<empty>	Not used by SSI but need to exist in role
S_BTCH_JOB	JOBGROUP	*	Demanded by Job Management
AI_LMDB_OB	LMDB_NAMES LMDB_OBJID	*	LMDB names and Object ID's are random hashes
AI_LMDB_OB	LMDB_STYPE		Customer specific

SAP_FRN_SSI_APMAINT

Authorization object	Field	Proposed Value	Comment
S_DATASET	FILENAME	*	File names not known
S_DEVELOP	DEVCLASS OBJNAME OBJTYPE P_GROUP	<empty>	<empty>
S_RFC_ADM	RFCDEST	*	Value are the SM59 destination to external servers (SAPHOSTAGENT) to be created by SSI, convention is HOSTNAME_NAMESPACE. As such needs to be created for all hosts connected to SAP Focused Run, * is recommended
	ICF_VALUE	<empty>	Not used by SSI but need to exist in role
S_BTCH_JOB	JOBGROUP	*	Demanded by Job Management

SAP_FRN_SSI_MAINT

Authorization object	Field	Proposed Value	Comment
S_DATASET	FILENAME	*	File names not known
S_DEVELOP	DEVCLASS OBJNAME OBJTYPE P_GROUP	<empty>	<empty>

Authorization object	Field	Proposed Value	Comment
S_RFC_ADM	RFCDEST	*	Value are the SM59 destination to external servers (SAPHOSTAGENT) to be created by SSI, convention is HOSTNAME_NAMESPACE. As such needs to be created for all hosts connected to SAP Focused Run, * is recommended
	ICF_VALUE	<empty>	Not used by SSI but need to exist in role
S_BTCH_JOB	JOBGROUP	*	Demanded by Job Management

SAP_FRN_SSI_DISP

Authorization object	Field	Proposed Value	Comment
S_DATASET	FILENAME	*	File names not known
S_DEVELOP	DEVCLASS OBJNAME OBJTYPE P_GROUP	<empty>	<empty>

Role Name Conventions (Info Only)

Role	Short Description	Intended for
SAP_FRN_SSI_WSEXEC	Dedicated role to execute SSI via web service calls.	Administrators, technical users
SAP_FRN_*_ALL, *_ ADMIN	All authorizations on the applications incl. personal data and business data where monitored	Administrators, key users
SAP_FRN_RUM_WOD SAP_FRN_SIA_WOD SAP_FRN_AIM_ WOD SAP_FRN_APP_AIM_WOD	Administrator access without special protected data like personal data (UID) in RUM or Business payload in AIM (collected only if dedicated customizing exists)	Administrators who should not see personal data or business payload data, administrators should not see business data, do not assign *_ALL
SAP_FRN_*_ EXE	Execute the applications	Key users, operators
SAP_FRN_*_ MAINT	Maintain content	Operators
SAP_FRN_ *_ REVIEW, REV	Review certain content	Key users, customers
SAP_FRN_*_DISP	Display data	Customers, guests

Role	Short Description	Intended for
SAP_FRN_CSA_PROTECTED	Access to critical data in CSA (has user SAP_ALL, etc.)	Key users

Advanced Dashboarding & IntelligenceADI)

Application	Role name	Short description
Tactical Dashboard	SAP_FRN_FI_TACTICAL	Access to tactical dashboards
	SAP_FRN_APP_PAS_DISP	Display authorizarions for predictive analytics
	SAP_FRN_APP_MOAL_DISP	Display authorizations for system monitoring and alert management

Advanced System Management (ASM)

Application	Role Name	Short description
System Monitoring	SAP_FRN_APP_MOAL_DISP	Display authorizations for system monitoring and alert management
	SAP_FRN_AAD_MOAL_MOC	Authorize MO individual monitoring and alert configuration
	SAP_FRN_APP_MOAL_ALL	All authorizations for system monitoring and alert management
	SAP_FRN_AAD_MOAL_ALL	All authorizations for system monitoring and alert management administration
	SAP_FRN_APP_PAS_DISP	Display authorizarions for predictive analytics
Open Component Monitoring	SAP_FRN_APP_AVM_ALL	All authorizations for open component monitoring
	SAP_FRN_SDA_DISP	Display authorizations for SDA admin application (needed to check the agent executing the configured OCM)
	SAP_FRN_AAD_AVM_ALL	All authorizations to administer application advanced monitoring
	SAP_FRN_SDA_MAINT	Administration function on SDA (needed to configure OCM)
Job Monitoring	SAP_FRN_APP_AJM_ALL	All authorizations to configure Application Job Monitoring

Application	Role Name	Short description
	SAP_FRN_APP_AJM_DISP	Display Authorization for JobMonitoring Application
	SAP_FRN_AAD_AJM_ALL	All Authorization for JobMonitoring Application
Guided Procedure Catalog/Reporting	SAP_FRN_APP_GP_DISP	Display access to guided procedures and GP reports
	SAP_FRN_APP_GP_EXE	Execution right of guided procedures
	SAP_FRN_APP_GP_ALL	Full access to guided procedures application
IT Calendar & Work Mode Management	SAP_FRN_APP_ITC	Authorization displaying IT-calendar (the maintenance is in the WMM
	SAP_FRN_APP_WMM_DISP	Work mode management display authorizations
	SAP_FRN_APP_WMM_ALL	Work mode management full authorizations
Service Availability Management	SAP_FRN_APP_SAM_DISP	Service availability management display authorizations
	SAP_FRN_APP_SAM_OUTAGE	Authorizations for service availability management application: manage outages
	SAP_FRN_APP_SAM_OUTAGE_REV	Authorizations for service availability management application: review outages
	SAP_FRN_APP_SAM_DEF	Authorizations for service availability management application: Manage service definitions
	SAP_FRN_APP_SAM_ALL	All authorizations for service availability management application
License Management	SAP_FRN_LICM_ALL	Full access to license management application
	SAP_FRN_LICM_DISP	Display access to license management application
SAP EarlyWatch Alert Status	SAP_FRN_APP_EWA_ALL	Full authorizations for application EWA Admin
	SAP_FRN_APP_EWA_DISP	Display authorizations for application EWA Admin

Advanced User Monitoring (AUM)

Application	Role name	Short description
Real User Monitoring	SAP_FRN_APP_RUM_WOD	All authorizations for App RUM, but no user data
	SAP_FRN_APP_RUM_ALL	All authorizations for App RUM
	SAP_FRN_SDA_MAINT	Maintenance authorizations for SDA admin application
	SAP_FRN_AEM_COV_DISP	Display AEM consumer variants
	SAP_FRN_AEM_COV_ALL	Administrate AEM consumer variants
	*SAP_FRN_AAD_RUM_ALL	All authorizations for RUM administration
Synthetic User Monitoring	SAP_FRN_APP_TA_DISP	Display authorizations for APP trace analysis (needed when trace is enabled in Synthetic User Monitoring)
	SAP_FRN_APP_SUM_ALL	All authorizations for App Synthetic User Monitoring: This role needs to be assigned to any user configuring SUM application
	SAP_FRN_SDA_DISP	Display authorizations for SDA admin application (needed to check the agent executing the configured Synthetic User Monitoring scripts)
	SAP_FRN_SDA_MAINT	Administration function on SDA (needed to configure Synthetic User Monitoring)
	SAP_FRN_AAD_SUM_DISP	Display authorizations for SUM Configuration: This role needs to be assigned to any user running SUM application
	SAP_FRN_AAD_SUM_MAINT	Maintenance Authorizations for Synthetic User Monitoring script configuration
	SAP_FRN_AEM_COV_DISP	Display AEM consumer variants
	SAP_FRN_AEM_COV_ALL	Administration AEM consumer variants
	SAP_FRN_AAD_SUM_ALL	All authorizations for Synthetic User Monitoring configuration
	SAP_FRN_SUM_ALRT_ENG	Authorization to execute Synthetic User Monitoring Alerts (needed to integrated Synthetic User Monitoring into alerting)

* SAP_FRN_AAD_RUM_ALL role is special security-relevant. The owner of this role is able to see the user ID of the user sending a request monitored by RUM. This authorization is mandatory for investigating subjective complaints (such as "slow response times") by an end user. If the application is monitored by RUM, find the user request by searching for the user ID. View the measured response time and where the time is spent. This

authorization is also mandatory for SAP dev support. Grant this authorization to selected users only. For more information, see also section **Special protected tables**.

Advanced Integration Monitoring (AIM)

Application	Role name	Short description
Integration & Cloud Monitoring	SAP_FRN_APP_AIM_DISP	Display authorizations for integration monitoring
	SAP_FRN_APP_AIM_ALL	All authorizations for integration monitoring
	SAP_FRN_APP_AIM_WOD	All authorizations for integration monitoring, but no total records display
	SAP_FRN_SRA_ALL	All authorizations for the scheduling aggregation & replication FWK
	*SAP_FRN_AAD_RUM_ALL	All authorizations for RUM administration (reuse of RUM data HTTP /HTTPS channels in integration monitoring)
	SAP_FRN_AAD_MOAL_ALL	All authorizations for system monitoring and alert management administration (for integration into alerting)
	SAP_FRN_AEM_COV_DISP	Display AEM consumer variants
	SAP_FRN_AEM_COV_ALL	Administrate AEM consumer variants
	**SAP_FRN_AAD_AIM_ALL	All authorizations for AIM administration
	SAP_FRN_SRA_DISP	All authorizations for the scheduling aggregation & replication FWK
Cloud Service Management	SAP_FRN_SRA_ALL	All authorizations for the scheduling aggregation & replication FWK
	*	
	SAP_FRN_AAD_RUM_ALL	All authorizations for RUM administration (reuse of RUM data HTTP and HTTPS channels in cloud service management)
	SAP_FRN_AAD_MOAL_ALL	All authorizations for system monitoring and alert management administration (for integration into alerting)
	**SAP_FRN_AAD_AIM_ALL	All authorizations for AIM administration
	SAP_FRN_SRA_DISP	Display authorization for the scheduling aggregation & replication FWK

* SAP_FRN_AAD_RUM_ALL role is special security-relevant. The owner of this role is able to see the user ID of the user sending a request monitored by RUM. This authorization is mandatory for investigating subjective complaints (such as "slow response times") by an end user. If the application is monitored by RUM, find the

user request searching by the user ID to see the measured responsive and where the time is spent. This authorization is also mandatory for SAP dev-support. Grant this authorization to selected users only. For more information, see also section **Special protected tables**.

****This role is special security-relevant. The owner of this role is able to see the business payload of the electronic document monitored by AIM, if payload data monitoring is customized. This authorization is mandatory for investigating problem with processing of certain payload, if the endpoint and document type is monitored by AIM. This authorization is mandatory for SAP dev support. Grant this authorization to selected users only. For more information, see also section **Special protected tables**.

Advanced Event & Alert Management (AEM)

Application	Role name	Short description
Alert Management	SAP_FRN_APP_MOAL_ALL	All authorizations for system monitoring & alert management
	SAP_FRN_AAD_MOAL_ALL	All authorizations for system monitoring & alert management administration
Guided Procedure Catalog/Reporting	SAP_FRN_APP_GP_EXE	Execute access to guided procedures application (integrate GP in alert management)
	SAP_FRN_APP_GP_ALL	Full access to guided procedures application (integrate GP in alert management)
	SAP_FRN_APP_GP_DISP	Display access to guided procedures application (integrate GP in alert management)

Advanced Configuration Management (ACM)

Application	Role name	Short description
Configuration & Security Analytics	SAP_FRN_APP_CSA_DISP	Display authorization for CSA
	SAP_FRN_APP_CSA_MAINT	Maintenance authorization for CSA
	SAP_FRN_APP_CSA_PROTECTED	Display authorization for CSA, including protected personal data
	SAP_FRN_AAD_CSA_DISP	Display authorization for CSA administration
	SAP_FRN_AAD_CSA_MAINT	Maintenance authorization for CSA without authorization for security template
	SAP_FRN_AAD_CSA_ALL	All authorizations for CSA Administration

Application	Role name	Short description
	Authorizations to transport policies are required	

Advanced Root Cause Analysis (ARCA)

Application	Role name	Short description
System Analysis	SAP_FRN_APP_SYA_ALL	Display authorizations for system analysis
	SAP_FRN_APP_PAS_DISP	Display suthorizations for predictive analytics
	SAP_FRN_APP_SYA_WOD	All authorizations for system analysis without authorization to change predictive analytics settings
	SAP_FRN_AAD_SYA_ALL	All authorizations for system analytics application administration
Trace Analysis	SAP_FRN_APP_TA_DISP	Display authorizations for APP trace analysis
	SAP_FRN_APP_TA_ALL	All authorizations for APP trace analysis
File System Browser	SAP_FRN_APP_FSB_ALL	Authorizations for APP file system browser

Infrastructure Administration

Application	Role name	Short description
LMDB	SAP_FRN_LDB_DISP	Display authorization on LMDB objects, This role is created for LMDB from LMDB UI. Please don't mistake with the other role "SAP_FRN_LDB_OB_DISP" needed to have access to LMDB objects from within a application UI
	SAP_FRN_LDB_MAINT	Maintenance authorization on LMDB objects
	SAP_FRN_LDB_ALL	Full authorization on LMDB
Global Settings & Network Configuration For access with read-only/display permissions mentioned roles must be assigned	SAP_FRN_LDB_DISP	Display authorization on LMDB objects
	SAP_FRN_SDA_DISP	Display authorizations for SDA admin application
	SAP_FRN_LDB_DISP	Display authorization on LMDB objects

Application	Role name	Short description
Global Settings & Network Configuration With full administrative permissions, the user can change global use case settings and global security settings, and he can create and modify customer networks, including changing network level security settings. Mentioned roles must be assigned.	SAP_FRN_SSI_ALL	All authorizations for SSI applications
	SAP_FRN_SDA_ALL	All authorizations for SDA admin application
	SAP_FRN_LDB_ALL	All authorizations on LMDB objects
Simple System Integration For access with read-only/display permissions mentioned roles must be assigned.	SAP_FRN_SSI_DISP	Display authorizations for SSI admin application
	SAP_FRN_SDA_DISP	Display authorization for SDA admin application
	SAP_FRN_LDB_DISP	Display authorization on LMDB objects
Simple System Integration Regular maintenance permissions allow to operate the full feature set of the Simple System Integration application. Mentioned roles must be assigned.	SAP_FRN_SSI_MAINT	Regular maintenance authorization for SSI applications
	SAP_FRN_SDA_MAINT	Maintenance authorization for SDA admin application
	SAP_FRN_LDB_MAINT	Maintenance authorization on LMDB objects
Simple System Integration Application-admin maintenance permissions, are somewhat stronger than the regular maintenance permissions. They add authorizations to use the “Configure Manually” functionality. We recommend to reserve these permissions for experienced Simple System Integration application-admins. Mentioned roles must be assigned.	SAP_FRN_SSI_APMAINT	Application-admin maintenance authorization for SSI applications
	SAP_FRN_SDA_MAINT	Maintenance authorization for SDA admin application
	SAP_FRN_LDB_MAINT	Maintenance authorization on LMDB objects
Agent Administration	SAP_FRN_LDB_DISP	Display authorization on LMDB objects
	SAP_FRN_SDA_DISP	Display authorizations for SDA admin application
	SAP_FRN_SSI_DISP	Display authorizations for SSI admin application
	SAP_FRN_SDA_MAINT	Maintenance authorizations for SDA admin application
	SAP_FRN_SDA_ALL	All authorizations for SDA admin application

Application	Role name	Short description
	SAP_FRN_SSI_MAINT	Execute for SSI admin application. Manual execution of SSI tasks. Decommissioning of technical systems
Agent Mass Update	SAP_FRN_LDB_DISP	Display authorization on LMDB object
	SAP_FRN_SDA_DISP	Display authorizations for SDA admin application
	SAP_FRN_SDA_MAINT	Maintenance authorizations for SDA admin application
	SAP_FRN_SDA_ALL	All authorizations for SDA admin application
Self-Monitoring / Self-Monitoring Dashboard	SAP_FRN_APP_MOAL_DISP	Display authorizations for system monitoring and alert management
Central Notification Management	SAP_FRN_CNM_DISP	Display authorization for CNM
	SAP_FRN_CNM_ALL	Full authorizations for notification management
Expert Scheduling Management Cockpit	SAP_FRN_SRA_DISP	Display authorizations for application Scheduling aggregation and replication FWK
	SAP_FRN_SRA_ALL	All authorizations for application scheduling Aggregation and replication FWK

Transaction "mai_tools"

Application	Role name	Short description
MAI Tools	SAP_FRN_AAD_MOAL_ALL	All authorizations for system monitoring and alert management administration
	SAP_FRN_APP_MOAL_ALL	All authorizations for system monitoring and alert management
	SAP_FRN_LDB_ALL	All authorizations for LMDB
	SAP_FRN_SDA_ALL	All authorizations for SDA admin application

Partner Reporting

Application	Role name	Short description
Partner Reporting	SAP_FRN_OPR_ALL	All authorizations for partner reporting

5.2.3.5 Roles for Setup Admin and Dev Support

Use

For your convenience to create the first administrator user or user for development support before your authorization concept is released.

Please also grant access to SAP Basis transactions such as SE16, SE80, SM37, SM59, SICF, and STC01.

→ Tip

There is a note describing authorization needed. 2042794 SAP Note 2042794 Prerequisites for Efficient Incident Processing

‹≡› Sample Code

SAP Focused Run 2.0 admin role collection for cut and paste

```
SAP_FRN_FLP_EMBEDDED
SAP_FRN_SCOPE_SEL
SAP_FRN_UI5_PERS_PUB
SAP_FRN_SCOPE_SEL_PUB_FILTER
SAP_FRN_CNW_ACCESS_ADMIN
SAP_FRN_FLP_1_ASM
SAP_FRN_FLP_2_AUM
SAP_FRN_FLP_3_1_AIM
SAP_FRN_FLP_3_AEM
SAP_FRN_FLP_4_CSA
SAP_FRN_FLP_5_5_RCA
SAP_FRN_FLP_5_ISA
SAP_FRN_FLP_6_AAD
SAP_FRN_FLP_CAT_AAD_AEM
SAP_FRN_FLP_CAT_AAD_AIM
SAP_FRN_FLP_CAT_AAD_CSA
SAP_FRN_FLP_CAT_AAD_RUM
SAP_FRN_FLP_CAT_AAD_SUM
SAP_FRN_FLP_CAT_AAD_SYM
SAP_FRN_FLP_CAT_APP_AEM
SAP_FRN_FLP_CAT_APP_AIM
SAP_FRN_FLP_CAT_APP_CSA
SAP_FRN_FLP_CAT_APP_FSB
SAP_FRN_FLP_CAT_APP_ITC
SAP_FRN_FLP_CAT_APP_RUM
SAP_FRN_FLP_CAT_APP_SAM
SAP_FRN_FLP_CAT_APP_SUM
SAP_FRN_FLP_CAT_APP_SYA
SAP_FRN_FLP_CAT_APP_SYM
SAP_FRN_FLP_CAT_APP_TA
SAP_FRN_FLP_CAT_ASHC
SAP_FRN_FLP_CAT_AVM
```

```
SAP_FRN_FLP_CAT_EWA
SAP_FRN_FLP_CAT_GPB
SAP_FRN_FLP_CAT_GPR
SAP_FRN_FLP_CAT_LICM
SAP_FRN_FLP_CAT_MPL
SAP_FRN_AAD_AIM_ALL
SAP_FRN_AAD_AVM_ALL
SAP_FRN_AAD_CSA_ALL
SAP_FRN_AAD_MOAL_ALL
SAP_FRN_AAD_RUM_ALL
SAP_FRN_AAD_SUM_ALL
SAP_FRN_AAD_SYA_ALL
SAP_FRN_APP_AAD_ADM_ALL
SAP_FRN_APP_AIM_WOD
SAP_FRN_APP_AVM_ALL
SAP_FRN_APP_FSB_ALL
SAP_FRN_APP_GP_ALL
SAP_FRN_APP_MOAL_ALL
SAP_FRN_APP_RUM_WOD
SAP_FRN_APP_SAM_ALL
SAP_FRN_APP_SUM_ALL
SAP_FRN_APP_SYA_ALL
SAP_FRN_APP_TA_ALL
SAP_FRN_APP_WMM_ALL
SAP_FRN_CNM_ALL
SAP_FRN_LDB_ALL
SAP_FRN_LICM_ALL
SAP_FRN_OPR_ALL
SAP_FRN_SDA_ALL
SAP_FRN_SRA_ALL
SAP_FRN_SSI_ALL
SAP_FRN_WMM_ALL
SAP_FRN_TECH_MON_TOOL
SAP_FRN_FI_TACTICAL
SAP_FRN_FLP_CAT_FI_TAC
```

5.2.4 Technical Users in Managed Systems

Use

Create technical users in managed systems during an early phase of your project.

SAP Focused Run ABAP central system does not create these technical users. They must be created by different tools, according to customer policies and as part of the preparation. The user credentials must be provided to SSI at configuration call.

With your simple diagnostics agent, the delivered preparation tool supports the creation of users. The preparation tool is scriptable and easy to integrate in LAMA.

For more information regarding the starting point for the preparation tool, see 2641304

OS-level technical users are required for the communication between SAP Focused Run and the agents.

Not all managed system types need mandatory monitoring users to be created (such as the Apache Tomcat monitoring with default templates).

Monitoring user creation is only one task of preparing managed systems.

For more information regarding the entry point for all preparation tasks, see **Infrastructure Preparations** in the SAP Focused Run expert portal at https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal.html

- SAP NetWeaver ABAP [page 93]
- SAP NetWeaver Java [page 95]
- SAP BusinessObjects [page 96]
- SAP Mobile Platform [page 97]
- Databases [page 97]
- Hosts / OS [page 99]

5.2.4.1 SAP NetWeaver ABAP

Use

This section concerns the creation of an ABAP user as part of system preparation. The ABAP user must exist in the ABAP client(s), to which the simple diagnostics agent connects via local RFC, to authenticate data collection.

The user and password need to be provided as execution of SSI.

A good practice is to name the user SDAGENT_<SAP Focused Run 2.0 SID>, especially if you connect the managed system to more than one SAP Focused Run system. In this case, you can detect easy where a wrong password is set.

The roles below are delivered with latest version of ST-PI. In addition, the most recent version of the roles is attached to SAP Note 2450740 - Roles to authorize access in managed Systems to collect data for SAP Focused Run 2.0.

Common practice is to create Z_* roles out of the delivered standard roles.

> **i** Note
>
> Please create the user with user type **System**

> **→** Tip
>
> Grant the authorization only if you use the usecase/metric.

Roles and Users for Monitoring ABAP-Managed System

User	Use case	Description	Role
SDAGENT	ASM	Authorization to collect data for system monitoring	SAP_FRN_SDAGENT_MAI_MS
		Authorization to collect data for system analysis and advanced rootcaucse analysis	SAP_FRN_SDAGENT_ASM_MS

User	Use case	Description	Role
		Authorization to collect data for job monitoring	SAP_FRN_SDAGENT_AJM_MS
		Authorisation to execute operations though the Guided Procedure plugin	SAP_FRN_SDAGENT_GPA_MS
	AIM	Authorization to collect data for Advanced Integration Monitoring	SAP_FRN_SDAGENT_AIM_MS
		Authorization to collect data for system monitoring	SAP_FRN_SDAGENT_MAI_MS
		For a S/4 Hana on-premise system, please follow Note 2450740 - Roles to authorize access in managed Systems to collect data for FRUN	
	AUM	Authorization to collect data for Real User Monitoring	SAP_FRN_SDAGENT_RUM_MS
		Authorization to collect data for system monitoring	SAP_FRN_SDAGENT_MAI_MS
		Authorization to collect data for Advanced Integration Monitoring	SAP_FRN_SDAGENT_AIM_MS
	ARCA	Authorization to collect data for Trace Analysis	SAP_FRN_SDAGENT_TA_MS
	CSA	Authorization to collect data for Configuration & Security Analysis	SAP_FRN_SDAGENT_CSA_MS
		Authorization to collect data for Configuration & Security Analysis for special users (such SAP*)	SAP_FRN_SDAGENT_CSA_SEC_MS
	AJM	Authorization to collect data for Job Management	SAP_FRN_SDAGENT_AJM_MS
<customer> the userid can be freely chosen		Execute SDCCN Job	SAP_SDCCN_ALL

Convenience Role List for easy Copy & Paste

⚠ Caution

Copy *AIM_MS and *RUM_MS if you plan to implement these SAP Focused Run use cases. Otherwise, grant more authorizations as needed.

Sample Code

```
SAP_FRN_SDAGENT_MAI_MS
SAP_FRN_SDAGENT_CSA_MS
SAP_FRN_SDAGENT_CSA_SEC_MS
SAP_FRN_SDAGENT_TA_MS
SAP_FRN_SDAGENT_AIM_MS
SAP_FRN_SDAGENT_RUM_MS
SAP_FRN_SDAGENT_ASM_MS
SAP_FRN_SDAGENT_AJM_MS
```

5.2.4.2 SAP NetWeaver Java

Use

this section concerns the creation of a Java user as part of system preparation. The Java user must exist in the Java UME store of the J2EE engine to authenticate data collection.

The SDAGENTJ/password needs to be provided when executing SSI in SAP Focused Run.

The following roles and actions must be assigned if the described functionality or metric is planned to be used in SAP Focused Run.

A good practice is to name the user SDAGENTJ_<Focused SID>, especially if you connect the managed system to more than one SAP Focused Run system. In this case, you can easily detect where a wrong password is set.

i Note

Please create the user with user type: **Technical User**

→ Tip

Grant the authorization only if you use the use case/metric.

Roles and Action for Monitoring Java Managed System

Technical User ID	Use case/ description	Category	Name
SDAGENTJ	ASM / Needed to collect common monitoring metrics	Java Role	○ NWA_READONLY

Technical User ID	Use case/ description	Category	Name
	ASM / Needed to collect monitoring metrics of Java jobs		`SAP_JAVA_WSNAVIGATOR`
	AIM / Needed to collect PI Monitoring Data		`SAP_XI_MONITOR_J2EE`
	AIM / Needed to collect message payload in AIM (only possible if relevant customizing is done in the PI).		`XI_FRUN_GET_MSG` Available with • PI 7.31 SP17+ • PI 7.40 SP12+ • PI 7.50 SP05+
	CSA& ASM / Needed to collect data of "Java PSE Certificates" for validation check and monitoring		`Administrator`
	CSA& ASM / Needed to collect data for security check if default users like "Administrator" are disabled. Needed to collect monitoring metric "Java Named Users"	Action	`Spml_Read_Action`

5.2.4.3 SAP BusinessObjects

Use

This section concerns the creation of an SAP BusinessObjects user as part of system preparation to authenticate data collection.

The user and password need to be provided when executing SSI in SAP Focused Run.

Roles for Monitoring SAP BusinessObjects Managed System

Technical User ID	Use case/ Description	Roles
<customer> User ID can be chosen	ASM & ARCA & CSA / Needed to collect data for system monitoring Needed to enable tracing Needed to configure store snapshot creations	`SMAdmin`, for XI 4.1 + see note below `CMS Admin` for older release

For more information, see 2266873 How to configure XI4.1 CMS built-in user SMAdmin for BI/Job Monitoring.

5.2.4.4 SAP Mobile Platform

Use

This section concerns the creation of a Sybase Unwired Platform user as part of system preparation to authenticate data collection.

The user and password need to be provided when executing SSI in SAP Focused Run.

Roles for Monitoring SAP Mobile Platform Managed System

Technical User ID	Use case/ Description	Roles
<customer>	ASM & ARCA & CSA /	`Help Desk`
User ID can be chosen	Needed to collect data for system monitoring	
	Needed to enable tracing	
	Needed to configure store snapshot creations	

Related Information

http://scn.sap.com/community/developer-center/mobility-platform/blog/2015/04/26/granting-role-based-access-in-sap-mobile-platform-30

5.2.4.5 Databases

Use

Understand where a dedicated DB user for the database is needed, provided a DB user authenticates connections from SAP Host Agent. Find links to related documentation.

SAP host agent offers the web service method `SetDatabaseProperty` for the creation of the DB monitoring user for SAP HANA, ASE, and MaxDB. For other DBs, the creation of a DB user is not needed.

> ⚠ Caution
>
> This preparation is mandatory for outside discovery on all DBs except SAP HANA, which has a built-in SLD data supplier.
>
> Do not execute the creation of the monitoring users unaligned with your other IT departments. The same functionality might be used by SAP LAMA or custom scripts.

Notes Describing the Proprietary User Creation for Managed Databases

DB / authentication	SAP Note
SAP HANA Authentication with a DB user. When requesting monitoring data from the SAP HANA DB the SHA looks in the OS `hdbuserstore` for the Key `<SID>SAPDBCTRL<TenantDBName>`.	2023587 Maintaining "`hdbuserstore`" using "`setProperty`" for SAP Host Agent
SAP Adaptive Server Enterprise (ASE) DB Authentication with a DB user. When requesting monitoring data from the ASE DB the SHA looks in the OS `rsecssfs store` for the key `<SID>SAPDBCTRL`.	2236137 SYB: saphostctrl/sapdbctrl - enable discovery for native ASE database installations 1797040 SYB: SAP Host Agent - Using global or local secure storage
MSSQL Authentication with an OS user. The SAP Host Agent runs as Windows Service with internal build in OS account **System**. When requesting monitoring data from the MS SQL the SHA authenticate as **System** at the MSSQL.	1877727 `sapdbcntrl`: not member of `sysadmin` 1564275 How to Install SAP Systems Using Virtual Host Names on Windows
Oracle Database Authentication with an OS user. SAP host agent utilizes secure built-in functions to request monitoring data	No note. In case of issues, please see SAP Host Agent Troubleshooting Guide https://wiki.scn.sap.com/wiki/display/ATopics/SAP+Host+Agent+Troubleshooting+Guide#SAPHostAgentTroubleshootingGuide-OracledatabasescannotbedetectedonUnix
IBM DB2 for LUW Authentication with an OS user. SAP host agents utilize secure built-in functions to request monitoring data	No note. In case of issues, please see SAP Host Agent Troubleshooting Guide https://wiki.scn.sap.com/wiki/display/ATopics/SAP+Host+Agent+Troubleshooting+Guide#SAPHostAgentTroubleshootingGuide-OracledatabasescannotbedetectedonUnix
SAP Max DB Authentication with a MaxDB `X-Server` user. Allow the `sapadm` of SAP Host Agent to call `X-Server` to log on to MaxDB when collecting Monitoring data secure built-in functions to request monitoring data	SAP Focused Run 2.0 Expert Portal https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/managed-systems-maintenance-guide/preparing-databases.html#section_352923295 2018919 SAP MaxDB/SAPHost Agent: Setting connect information as SetDatabaseProperty

DB / authentication	SAP Note
SAP IQ DB Authentication with a DB user. When requesting monitoring data from the SAP IQ DB the SHA looks in the OS `rsecssfs store` for the Key `<SID>SAPDBCTRL` .	SAP Focused Run 2.0 Expert Portal https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/managed-systems-maintenance-guide/preparing-databases.html#section_352923295

5.2.4.6 Hosts / OS

Use

Understand and create a password for the OS user `sapadm`

The OS user `sapadm` is mandatory to install the SAP Host Agent. As the SAP Host Agent (SHA) is a mandatory component in the FRUN infrastructure, the user is mentioned in this guide.

For more information from SAP Host Agent Installation guide, see https://help.sap.com/viewer/DRAFT/141cbf7f183242b0ad0964a5195b24e7/115/en-US/ba5e83bd129e4932a4a7726fcea01c4f.html

You can install SAP Host Agent manually or as a task of the `Software Provisioning Manager`.

- Running the command-line tool `saphostexec`. The existence of OS user `sapadm`is checked. If it exists: OK. If not: It is created, but **without** a password set. Before you can use this SHA with SAP Focused Run 2.0 you need to set a password.
- Running the `Software Provisioning Manager`. The existence oOS user `sapadm` is checked. If it exists: OK. If not: It is created, **with** a password set.

> ⚠ Caution
>
> For automation purposes the password of the `sapadm`must be the same on all hosts within a customer network when using basic authentication.

> → Tip
>
> When using certificate-based authentication for calls from SAP Focused Run 2.0 to SHA, `sapadm` does not need a password.

5.2.5 CA APM EM Users

Use

Understand and create custom CA APM EM Users.

Background

SAP Focused Run is not delivered with OEM licenses for CA APM EM. SAP customers commonly already own such an OEM license, however, because the license is included with SAP Solution Manager and its support contract. SAP Focused Run is a consumer of monitoring metrics collected in the CA APM EM. Self Monitoring checks the availability of CA APM EM and provides a generated JumIn URL for further analysis. The logon to the CA APM EM needs to be authenticated. This is possible with built-in standard users.

CA APM EM Standard User Passwords

User Name (case sensitive)	Password
Admin	Admin89
Guest	guest12

Consider changing standard user and passwords. For more information, please see the CA APM EM documentation: https://docops.ca.com/ca-apm/10-5/en/administrating/apm-security .

5.2.6 S-User Authorizations in SAP ONE Support Launchpad

Use

Assign authorization to S-users for viewing SAP EarlyWatch Alert (EWA) reports.

EWA reports are not generated in SAP Focused Run. SAP Focused Run sends EWA data to the SAP Support Backbone for EWA report creation. To view the EWA reports, log on to SAP ONE Support Launchpad with an authorized S-user.

Assign to your S-user the required authorization `Service Reports and Feedback` to see EWA reports in SAP ONE Support Launchpad.

For more information, see 2319793 How to check service messages in SAP ONE Support Launchpad.

Due to the planed SAP Support Backbone Update you will need to switch the communication to Support Backbone to HTTPS after the 31.12.2019 and will need an additional communication user. Please see further details here https://support.sap.com/en/alm/solution-manager/sap-support-backbone-update.html herehttps://support.sap.com/en/release-upgrade-maintenance/maintenance-information/connectivity-to-sap.html and here 2174416 Creation and activation of users in the Technical Communication User application

6 Data Protection and Privacy

Personal data protection

The purpose of SAP Focused Run is to support organizations (IT departments, host providers) that run technical operations on business systems.

As part of technical operations, SAP Focused Run collects monitoring data such as metrics, configurations, traces, and exceptions from designated business systems. This monitoring data can contain personal data such as user IDs when exposed by the business systems.

Taking the consent to store and process personal data in business operations and expose them in monitoring data is to be done by the managed business system. Part of the monitoring operation personal data is stored together with the operational data. This personal data in the monitoring data is to be deleted in SAP Focused Run on demand, and as part of regular housekeeping.

SAP Focused Run requires personal data of its dialog users for administrative purposes. In other cases, SAP Focused Run stores personal data for the productive operations of IT departments.

SAP Focused Run users effectively consent to SAP Focused Run storing and processing personal data when conducting SAP Focused Run transactions that require personal data to complete.

This chapter describes where the personal data is stored and used in SAP Focused Run.

SAP Focused Run Dialog Users and Business Partners

All dialog users and business partners in SAP Focused Run are created and maintained with SAP NetWeaver 7.5 standard functionality. For more information, reference SAP NetWeaver documentation: https://help.sap.com/viewer/p/SAP_NETWEAVER_750.

Landscape Objects and Business Partners

Landscape objects include customer networks, technical systems, instances, databases, and hosts. Landscape objects are maintained in the LMDB. It is not uncommon in the LMDB, being part of productive IT operations, to map technical objects to the business partners who are responsible for them. If business partners are deleted using SAP NetWeaver functions (see above 8.1), this mapping is invalidated.

Depending on individual organizational policies, personal data can be maintained and deleted in the LMDB's technical system editor, in the additional attributes (such as system owner).

Delete landscape objects in the LMDB's technical system editor. Please note, however, that deleting landscape objects can lead to orphaned configurations, which complicate clean-up efforts if the landscape object is already deleted. A safe option is to decommission landscape objects using the report `RSRSM_SSI_CLEANUP_NETWORK`. For more information, see the relevant documentation in the SAP Focused Run Expert Portal in the section **Decommissioning** https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal.html

For a safe deletion of documents that contain user ID, depending on the use case, you can use the following tools:

- To delete change log documents, execute `RLMDB_CLEAR_CHANGELOG`. The report documentation explains how to execute the report and schedule a periodical job.
- To delete customized additional attributes, use transaction `SM34` with view cluster `VC_LMDB_ADD_ATTR`. For more information about deletion of changelog entries containing personal data, see https://help.sap.com/viewer/bdd095d01c7941c8b5d4c27e04da7315/latest/en-US/6fcbda6e22f24a78af60888b1ca2fb2c.htm

Real User Monitoring

User IDs collected by real user monitoring are stored in these protected tables:

`/RUM/AGGRECIN`

`/RUM/AGGRECOUT`

`/RUM/SNGLRECIN`

`/RUM/SNGLRECOUT`

To delete all data older than a given number of days, execute report `/rum/housekeeping`. The time period is configurable.

To delete a single user ID outside of executing the housekeeping function, manually delete the ID from the tables listed above.

Advanced Integration Monitoring

To check for stored personal data in the application, use transaction `SE16` for all the tables mentioned in the below section and on the selection screen, filter by columns mentioned for respective tables.

Below a list of tables hold personal data (USERID), on who changed configuration information in the application. The personal data in the below tables can be deleted by executing the report `/IMA/AIM_CONF_PERS_DATA_DELETE`. The execution of the above report is logged as ABAP Trace see Tx `SLG1` using object `/IMA/`.

- `/IMA/TSCONFIG` in column LAST_CHANGE_BY
- `/IMA/COLLCONFIG` in column LAST_CHANGE_BY
- `/IMA/ISCENARIO` in column LAST_CHANGE_BY
- `/IMA/ALERTTYPE` in column LAST_CHANGE_UNAME
- `EXM_FILTERS` in column CHANGED_BY
- `EXM_AL_TYPES` in column LAST_CHANGE_UNAME

Tables listed below hold personal data (USERID), while collecting monitoring data for BDocs and IDocs. The personal data in the tables is deleted by housekeeping job `SAP_FRN_AIM_HOUSEKEEPING` (Program name: `/IMA/HOUSEKEEPING`).

- `/IMA/BDOC_HEADER` in columns SND_USER, CRE_USER, UPD_USER
- `/IMA/IDOCINBOX` in column LAST_CHANGE_BY
- `/IMA/EDIDC` in columns RCVPRN, SNDPRN

The mentioned reports are delivered with 2645276

Below a list of tables hold personal data (USERID), while collecting cloud monitoring data. The personal data in the table is deleted by a housekeeping task scheduled by expert scheduler framework named *cloud monitoring housekeeping job*.

- `/IMA/CLD_CORE` in column *CREATED_BY*.

Tables listed below hold personal data (USERID), while collecting cloud monitoring data. The personal data in the tables is deleted by a housekeeping task scheduled by expert scheduler framework named *ExM housekeeping job*.

- `EXM_CORE` in column CREATED_BY

Scheduling, Replication and Aggregation Framework

The tables `SRAF_CONF_STORE` holds personal data (USERID) on who created or changed configuration information for a scheduled task.

The report `ESM_PERS_DATA_USAGE` could be executed to check if personal data (USERID) is stored in the application.

The personal data (USERID) stored in the application can be deleted by running the report `ESM_PERS_DATA_DELETE`. This report will be made available by SAP Note. 2644382

The execution of the above reports is logged in `SLG1` using object `SRAF`.

Synthetic User Monitoring

A best practice for synthetic user monitoring is to remove all personal data in the synthetic user monitoring script editor when parameterizing scripts. As a result, data of technical tests users replaces all personal data. This is the standard recommendation for creating scripts for automatic execution in SUM

Trace Analysis

If a user records a trace for their own activity, this action collects the user ID. The user can delete their trace manually from the trace application.

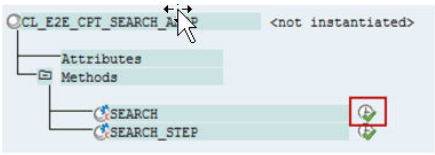
To delete all data older than a given number of hours, execute report `E2E_TRACE_DELETE`. The time period is configurable.

To delete a single user ID outside of executing the housekeeping function, manually delete the ID from the trace tables as follows:

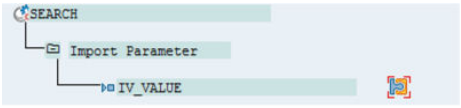
Go top Tx SE24 and choose CL_E2E_CPT_SEARCH_AMDP.

Execute class (F8).

Select **Search.**

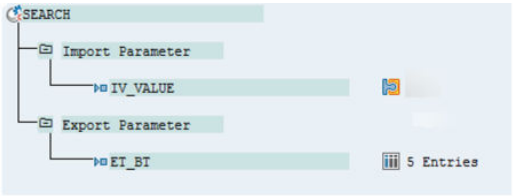


Enter the user name in field IV_VALUE

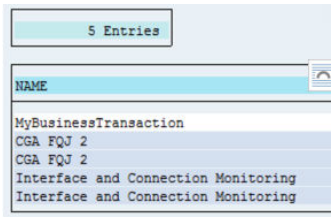


Execute the method.

If the result ET_BT is empty, no trace is available or it contains traces of the entered user name only.



The following entries from ET_BT can be deleted in the trace application.



System Analytics

The tables WEA_EXTR_CONFIG and WEA_VARIANTS holds personal data (USERID) on who created or changed configuration information for the application.

The report SYSANA_PERS_DATA_USAGE could be executed to check if personal data (USERID) is stored in the application.

The personal data (USERID) stored in the application can be deleted by running the report SYSANA_PERS_DATA_DELETE.

The reports are available via. 2643875

The execution of the above reports is logged in SLG1 using object SYS_ANA.

Additional personal data in System Analytics are User IDs of back-end systems collected if the collection for a system is configured for:

- **ABAP Statistic records**
- **ABAP work process overview**
- **SAP HANA Thread samples**

If you have enabled the collection of *ABAP Statistical Records*" all data older than a given number of days can be deleted by executing the report`AI_STATRAGG_HOUSEKEEPING` . The time period is configurable.

If you have enabled the collection of *ABAP work process overview* and *SAP HANA Thread samples*, all data older than a given number of days can be deleted by executing the report `RCA_HOUSEKEEPING`.

To delete a single user ID outside of executing the housekeeping function, manually delete it from the tables.

- `STATDBUSERTCODE` where ACCOUNT = the user ID
- `STATDBUSERWORKLO`where USERNAME = the user ID
- `RCA_SMON_WP_AGGR` where USER_NAME = the user ID
- `RCA_HANA_TS_AGGR` where APPLICATION_USER_NAME = the user ID

Root Cause Analysis Generic Storage

RCA Generic Storage is designed for the storage of technical monitoring data only and does not provide function's for the protection of personal data in the generice storage. It is also not planned to provide such function in later release. The sending of personal data to `/sap/bc/rest/rca_gs` is contrarily the application design and strongly not recommended. It might it might result in a vialotation of data protect and privacy laws.

Predictive Applications

Predictive Applications persist user id in 2 tables.

- `PAS_SA_MODEL_VER`
- `PAS_SA_VARIANT`

The report `PAS_PERS_DATA_USAGE` could be executed to check if personal data is stored in the application.

The personal data stored in the application can be deleted by running the report `PAS_PERS_DATA_DELETE`.

The execution of the above reports is logged in Tx `SLG1`using object `PAS`.

The reports are shipped for SAP Focused Run 2.0 FP3 with 2643513

Advanced Event Management

`AEM_ACTION_LOG` table stores user IDs of users who have performed any action on an alert. This data gets deleted when the AEM housekeeping program `AEM_HOUSEKEEPING` is set up to run periodically.

IT Calendar

`ITCAL_EVENTS` table stores the CREATED and CHANGED user IDs of work modes. This is deleted when the work mode housekeeping report`WMM_HOUSEKEEPING` is run and delete per default personal data after 365 days. To configure a custom period for the deletion of personal data and to log the deletion of personal data in Tx `SLG1` please implement 2658030.

Central Notification Management

In central notification management (CNM), recipient groups are maintained to send alerts and other notifications to recipients. Notification groups can be populated by selecting registered users from the SAP Focused Run SAP NetWeaver user management (see 8.1) or by entering external recipients. Register an external recipient can be entered with their name, telephone numbers, and e-mail addresses. You can maintain and delete this entry in CNM. The tables of the CNM are as follows:

- `CNM_CID` stores the e-mail and phone number
- `CNM_RECIPIENT`
- `CNM_RL`
- `CNM_RL_CN`
- `CNM_RL_MAP`

If schedules, templates, and configurations are deleted, they are marked as *deleted* and retained in the database. Housekeeping job `CNM_SYNC_SYSTEM_USERS` can be scheduled to delete items from database.

- `CNM_SCHEDULES`
- `CNM_TEMPLATES`
- `CNM_CONFIGS`

Advanced Configuration Monitoring

Configuration & Security Analytics can monitor critical authorizations (such as **SAP_ALL, J2EE_Administrator**). When this special monitoring is active, the user ID containing the critical authorization is recorded.

Configuration & Security Analytics uses its collector framework to transfer technical data of the connected managed systems into the configuration and change database (CCDB). CCDB is a set of tables stored in SAP Focused Run's database. This transferred technical configuration data does contain user IDs. Other personal and sensitive data is not extracted or stored.

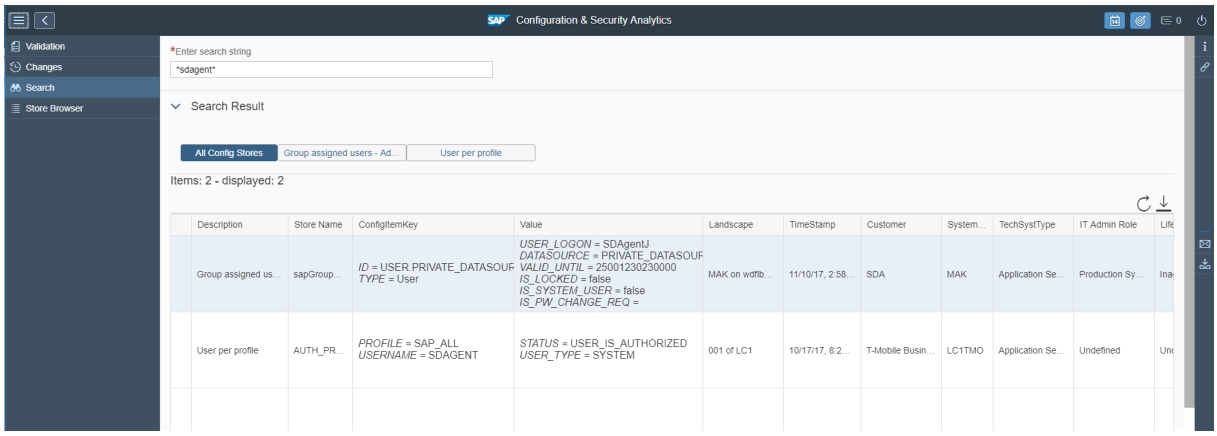
How to display data stored in the configuration and change database

To display of user-dependent data:

Start application `Configuration & Security Analytics`.

For your scope, select systems or use an asterisk on the extended system ID for all systems.

Select the panel **Search**, enter the user ID bracketed by asterisks (for example, `*sdagent*`), confirm the selection as shown in the screenshot below:



> ## Note
>
> - Data deletion takes place in two steps, both logically and physically. As soon as data is deleted logically it is not displayed anymore by the above search. The physical deletion of data is performed periodically. The physical data deletion is performed within a few hours of the logical deletion.
> - The display of data is protected by authorizations. The CCDB authorization to display all data, including the protected data, is required here. In addition, you must ensure you have authorization for all customer networks.
> - The search does not display configuration items that are marked as deleted in CCDB. These are elements which have not been delivered by the last snapshot of the corresponding data transfer. Such deleted configuration items can be found and displayed by the data deletion utility only.

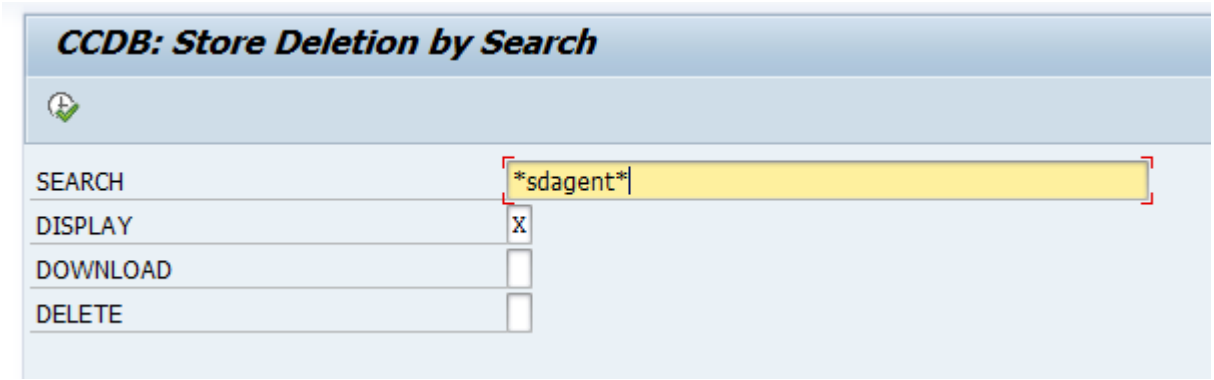
How to delete user-dependent data from configuration and change database

The CSA checks configuration data of managed systems. Due to its technical configuration, data is transferred into the CCDB of the SAP Focused Run system (such as configuration data of RFC connections or authorization data containing user IDs).

For deletion of CCDB data on SAP Focused Run, use report `CCDB_SEL_DATA_DELETION`. For an installation reference, see 2562443 Collective Corrections for CSA Collector Framework in SAP Focused Run.

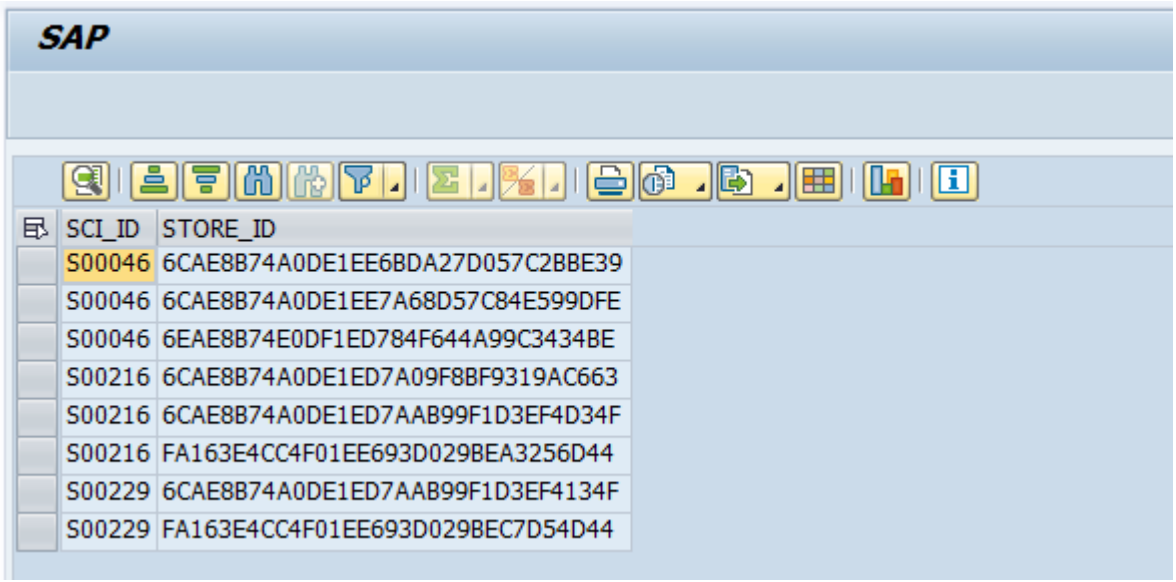
Data Display

Execute Report `CCDB_SEL_DATA_DELETION`CCDB_SEL_DATA_DELETION.



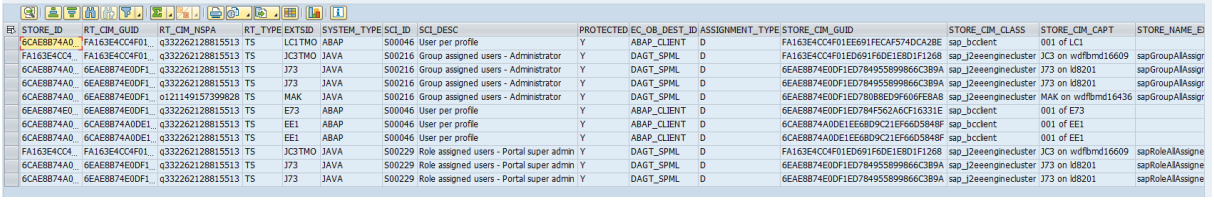
Enter the user between asterisks with *DISPLAY* enabled, *DELETE* disabled, and execute.

As a result, a screen displays the technical store IDs that match the search pattern (case insensitive search). Depending on the number of connected systems with which the user is working, the number of stores displayed will vary. If the list is empty, there is no user data regarding the search pattern in CCDB.



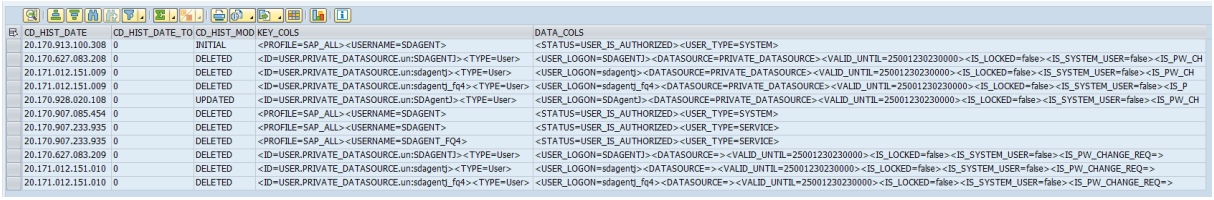
SCI_ID	STORE_ID
S00046	6CAE8B74A0DE1EE6BDA27D057C2BBE39
S00046	6CAE8B74A0DE1EE7A68D57C84E599DFE
S00046	6EAE8B74E0DF1ED784F644A99C3434BE
S00216	6CAE8B74A0DE1ED7A09F8BF9319AC663
S00216	6CAE8B74A0DE1ED7AAB99F1D3EF4D34F
S00216	FA163E4CC4F01EE693D029BEA3256D44
S00229	6CAE8B74A0DE1ED7AAB99F1D3EF4134F
S00229	FA163E4CC4F01EE693D029BEC7D54D44

Choosing the back icon displays a second screen containing additional data.



STORE_ID	RT_CIM_GUID	RT_CIM_NSPA	RT_TYPE	EXTSID	SYSTEM_TYPE	SCI_ID	SCI_DESC	PROTECTED	EC_OB_DEST_ID	ASSIGNMENT_TYPE	STORE_CIM_GUID	STORE_CIM_CLASS	STORE_CIM_CAPT	STORE_NAME_EX
6CAE8B74A0...	FA163E4CC4F01...	q332262128815513	TS	LC1TMO	ABAP	S00046	User per profile	Y	ABAP_CLIENT	D	FA163E4CC4F01EE691FECAF574DCA2BE	sap_bcclient	001 of LC1	
FA163E4CC4...	FA163E4CC4F01...	q332262128815513	TS	JC3TMO	JAVA	S00216	Group assigned users - Administrator	Y	DAGT_SPML	D	FA163E4CC4F01ED691F6DE1E8D1F1268	sap_j2eeenginecluster	JC3 on wdfbmd16609	sapGroupAllAssigr
6CAE8B74A0...	6EAE8B74E0DF1...	q332262128815513	TS	J73	JAVA	S00216	Group assigned users - Administrator	Y	DAGT_SPML	D	6EAE8B74E0DF1ED784955899866C3B9A	sap_j2eeenginecluster	J73 on ld8201	sapGroupAllAssigr
6CAE8B74A0...	6EAE8B74E0DF1...	q332262128815513	TS	J73	JAVA	S00216	Group assigned users - Administrator	Y	DAGT_SPML	D	6EAE8B74E0DF1ED784955899866C3B9A	sap_j2eeenginecluster	J73 on ld8201	sapGroupAllAssigr
6CAE8B74A0...	6EAE8B74E0DF1...	q121149157399828	TS	MAK	JAVA	S00216	Group assigned users - Administrator	Y	DAGT_SPML	D	6EAE8B74E0DF1ED780B8ED9F606FE8A8	sap_j2eeenginecluster	MAK on wdfbmd16436	sapGroupAllAssigr
6EAE8B74E0...	6EAE8B74E0DF1...	q332262128815513	TS	E73	ABAP	S00046	User per profile	Y	ABAP_CLIENT	D	6EAE8B74E0DF1ED784F562A6CF16331E	sap_bcclient	001 of E73	
6CAE8B74A0...	6CAE8B74A0DE1...	q332262128815513	TS	EE1	ABAP	S00046	User per profile	Y	ABAP_CLIENT	D	6CAE8B74A0DE1EE6BD9C21EF66D5848F	sap_bcclient	001 of EE1	
6CAE8B74A0...	6CAE8B74A0DE1...	q332262128815513	TS	EE1	ABAP	S00046	User per profile	Y	ABAP_CLIENT	D	6CAE8B74A0DE1EE6BD9C21EF66D5848F	sap_bcclient	001 of EE1	
FA163E4CC4...	FA163E4CC4F01...	q332262128815513	TS	JC3TMO	JAVA	S00229	Role assigned users - Portal super admin	Y	DAGT_SPML	D	FA163E4CC4F01ED691F6DE1E8D1F1268	sap_j2eeenginecluster	JC3 on wdfbmd16609	sapRoleAllAssigne
6CAE8B74A0...	6EAE8B74E0DF1...	q332262128815513	TS	J73	JAVA	S00229	Role assigned users - Portal super admin	Y	DAGT_SPML	D	6EAE8B74E0DF1ED784955899866C3B9A	sap_j2eeenginecluster	J73 on ld8201	sapRoleAllAssigne
6CAE8B74A0...	6EAE8B74E0DF1...	q332262128815513	TS	J73	JAVA	S00229	Role assigned users - Portal super admin	Y	DAGT_SPML	D	6EAE8B74E0DF1ED784955899866C3B9A	sap_j2eeenginecluster	J73 on ld8201	sapRoleAllAssigne

Scroll to the right to find the searched data if it is not in the initial view.



CD_HIST_DATE	CD_HIST_DATE_TO	CD_HIST_MOD	KEY_COLS	DATA_COLS
20.170.913.100.308	0	INITIAL	<PROFILE=SAP_ALL><USERNAME=SDAGENT>	<STATUS=USER_IS_AUTHORIZED><USER_TYPE=SYSTEM>
20.170.627.083.208	0	DELETED	<ID=USER.PRIVATE_DATASOURCE.un:SDAGENTJ><TYPE=User>	<USER_LOGON=SDAGENTJ><DATASOURCE=PRIVATE_DATASOURCE><VALID_UNTIL=25001230230000><IS_LOCKED=false><IS_SYSTEM_USER=false><IS_PW_CH
20.171.012.151.009	0	DELETED	<ID=USER.PRIVATE_DATASOURCE.un:sdagentj><TYPE=User>	<USER_LOGON=sdagentj><DATASOURCE=PRIVATE_DATASOURCE><VALID_UNTIL=25001230230000><IS_LOCKED=false><IS_SYSTEM_USER=false><IS_PW_CH
20.171.012.151.009	0	DELETED	<ID=USER.PRIVATE_DATASOURCE.un:sdagentj_fq4><TYPE=User>	<USER_LOGON=sdagentj_fq4><DATASOURCE=PRIVATE_DATASOURCE><VALID_UNTIL=25001230230000><IS_LOCKED=false><IS_SYSTEM_USER=false><IS_P
20.170.928.020.108	0	UPDATED	<ID=USER.PRIVATE_DATASOURCE.un:SDAgentJ><TYPE=User>	<USER_LOGON=SDAgentJ><DATASOURCE=PRIVATE_DATASOURCE><VALID_UNTIL=25001230230000><IS_LOCKED=false><IS_SYSTEM_USER=false><IS_PW_CH
20.170.907.085.454	0	DELETED	<PROFILE=SAP_ALL><USERNAME=SDAGENT>	<STATUS=USER_IS_AUTHORIZED><USER_TYPE=SYSTEM>
20.170.907.233.935	0	DELETED	<PROFILE=SAP_ALL><USERNAME=SDAGENT>	<STATUS=USER_IS_AUTHORIZED><USER_TYPE=SERVICE>
20.170.907.233.935	0	DELETED	<PROFILE=SAP_ALL><USERNAME=SDAGENT_FQ4>	<STATUS=USER_IS_AUTHORIZED><USER_TYPE=SERVICE>
20.170.627.083.209	0	DELETED	<ID=USER.PRIVATE_DATASOURCE.un:SDAGENTJ><TYPE=User>	<USER_LOGON=SDAGENTJ><DATASOURCE=><VALID_UNTIL=25001230230000><IS_LOCKED=false><IS_SYSTEM_USER=false><IS_PW_CHANGE_REQ=>
20.171.012.151.010	0	DELETED	<ID=USER.PRIVATE_DATASOURCE.un:sdagentj><TYPE=User>	<USER_LOGON=sdagentj><DATASOURCE=><VALID_UNTIL=25001230230000><IS_LOCKED=false><IS_SYSTEM_USER=false><IS_PW_CHANGE_REQ=>
20.171.012.151.010	0	DELETED	<ID=USER.PRIVATE_DATASOURCE.un:sdagentj_fq4><TYPE=User>	<USER_LOGON=sdagentj_fq4><DATASOURCE=><VALID_UNTIL=25001230230000><IS_LOCKED=false><IS_SYSTEM_USER=false><IS_PW_CHANGE_REQ=>

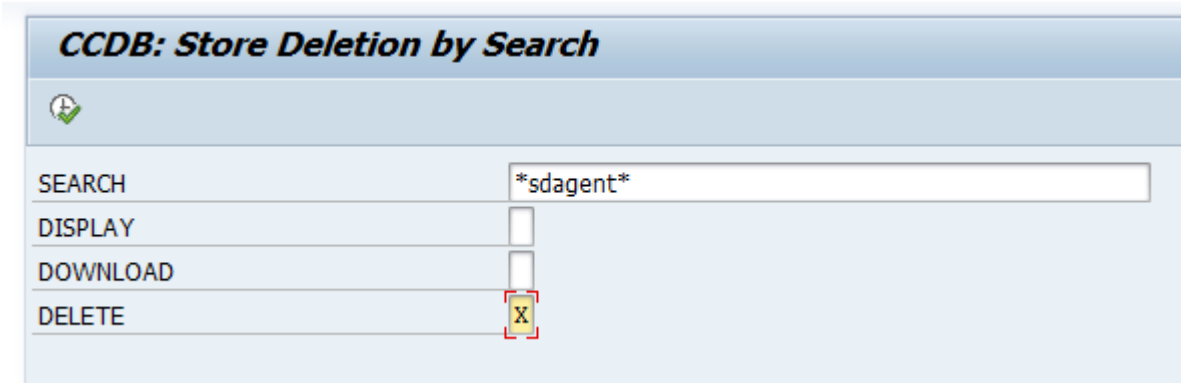
Choose the back icon to end the report.

Data Deletion

> **i Note**
>
> - During data deletion, the whole content of stores containing the user ID is deleted. This means all other data in the store and his history is removed as well. It takes approximately 24 hours until current data is reloaded. The possibility to reload the current data makes the process not critical, but the history of data that is not user-dependent is lost.
>
> Until the current data is re-transferred to CCDB, applications like configuration validation and SAP EarlyWatch Alert, which use the CCDB data, may run into an error or report incorrect or missing data.

- Depending on the user ID, stores are selected for deletion that contain text rather than the specific user ID to match the search. Such deletions cannot be avoided technically
- The data is deleted logically only. The physical deletion takes place within a few hours automatically. As soon as the data is deleted logically it cannot be accessed further by applications.
- Before performing the deletion process, consider that the user data must be deleted in the managed systems at first. Otherwise, the periodic data push may transfer the user data again into the CCDB.

To perform the deletion, enter the user between asterisks with *DISPLAY* disabled and *DELETE* enabled:



Execute the report and wait until it has finished. The report is designed for user data deletion only, and therefore a high number of search hits are not expected.

Additional authorization needed for the deletion from Configuration and Change Database

Authorization to run a report.

Authorization to Run a Report

Authorization Object	Field Name	Value
S_TCODE	TCD	SA38
S_PROGRAM	P_ACTION	SUBMIT
	P_GROUP	<empty>

Authorization to display, download and delete configuration data:

Authorization to Display, Download and Delete Configuration Data

Authorization Object	Field Name	Value
SR_CCDB	CCDB_COMP	READAPI
		STORE_DATA
	CCDB_SUB	READ
		PROTECT
	ACTVT	03

Authorization Object	Field Name	Value
SR_CF_ADM	CF_COMP	PROC
		SYST
	SUBCOMP	PROC
		SYST
	ACTVT	02
		06
LMDB_SCOPE	LDB_SCOPE	ADMIN
	ACTVT	03
S_GUI	ACTVT	61

Service Availability Management

These tables store the **CREATED** and **CHANGED** user IDs. Since outage and service definition are seen as audit relevant data, there are no deletion possible from the user interface.

The data SE16

- SAM_DEF
- SAM_OUT
- SAM_OUT_CHNLOG

Work Mode Management

WMM_PLAN_HEADER table stores the **CREATED** and **CHANGED** user IDs of work modes. This is deleted when the work mode housekeeping report WMM_HOUSEKEEPING is run and delete per default personal data after 365 days. To configure a custom period for the deletion of personal data and to log the deletion of personal data in ABAP trace SLG1 please implement: 2658030

Simple System Integration (SSI)

SSI stores the **USER ID** of operators who set up the behavior of SSI or configure a certain managed object in Simple System Integration or Diagnostics Agent Administration.

General Log View

The **USER ID** is displayed in the Simple System Integration UI and in the Diagnostics Agent Administration UI, in the log viewer section. In this log viewer, you can filter on the **USER ID** to see the respective entries.

To delete log entries containing a **USER ID** from the SAP Focused Run system, SSI provides an archiving functionality described here.

https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/ssi-log-archiving.html

Scheduled background processing

The initiator of background processing in the SSI is logged as *CREATED_BY* in database table `ATK_MATE_ACTN_`. To check for stored user data, use report `P_ATK_MATE_DPP_INFO`. The report displays a text if personal data are stored for the user in Scheduled Background Processing.

The deletion of user data is performed by an automated cleanup process. With following persisted configuration parameters it's possible to control the behavior of the cleanup process. The configuration database table is `ATK_MATE_CONFIG`.

ATK_MATE_CONFIG Configuration Keys

KEY	VALUE	Description
CLEANUP.LOGS.AFTER	<integer>	The period after that status and logs are deleted; default = 2.419.200 (= 4 weeks)
CLEANUP.LOGS.EXECUTE	0|1	Control whether the cleanup log task is active; default = 1 (= true)

Configuration of LMDB event handling by SSI

The configuration tracks users who maintained the LMDB event handling in the SSI. The user data is stored in table `SSI_EVENT_CONF` in column **CHANGE_USER**. To check for stored user data, use report `P_SSI_DPP_INFO`. The report displays a text if personal data are stored for the user in *LMDB event handling in SSI*.

Agent administration

The agent administration traces all configurations made to the agents in table `SRSM_CONFIG_INF`, together with the **USER ID**.

The personal data can be deleted in the host cleanup procedure using program `RSRSM_SSI_CLEANUP`.

The table `AMA_SETUP_BINARY` stores the latest binaries, that are uploaded by the report `SRSM_AMA_UPLOAD_BINARY`. The **USER ID** will be overwritten when another user uploads the same type of binary for the same platform.

For both tables, the stored user IDs can be returned by report `P_AMA_DPP_INFO` .

Open Component Monitoring

To delete personal data referring to a specific user ID, you have to check whether there is data in the following database tables. Then delete the records containing the user ID, using transaction `SE16`:

- ADMON_MTYP_DEFC default settings for each metric type specified by customer
- ADMON_MTUSR_DEF default settings for metric type and user
- ADMON_MT_TP_DEFC default value for threshold parameter specified by customer
- ADMON_MTU_TP_DEF default value for threshold parameter specified by user

License Management

License Management stores user data in the *Log Messages* tab in the License Management UI. The column *User Name* contains the user ID of the user who generated the log message. In the *Log Messages* tab, the *User Name* can be used as filter criteria.

To delete log entries containing a*User Name* from the SAP Focused Run system, see

https://support.sap.com/en/alm/focused-solutions/focused-run-expert-portal/ssi-log-archiving.html

Rapid Content Delivery

The tables below contain personal data (USERID), regarding which users downloaded and imported SAP Focused Run content as described in SAP Note 2695734. This is configuration information.

- `CSU_DWLD_CONT`
- `CSU_DWLD_PACK`
- `CSU_CONFIGURATIN`

The report `RCD_PERS_DATA_USAGE` could be executed to check if personal data (USERID) is stored in the application.

The personal data (USERID) can be deleted using the report `RCD_DELETE_PERSONAL_DATA`.

The execution of the above reports is logged in `SLG1`SLG1 using object `SOLAR`.

The deletion reports are delivered with 2643443.

S-User Handling

Report `AI_SC_REFRESH_READ_ONLY_DATA` downloads S-user data, including the details of the persons (name, gender, telephone number, e-mail, country, language, etc.) and their authorities of Maintain System Data (INSTPROD) at SAP. These data are used as the value help of S-user selection in transaction `AISUSER` and pre-check before communicating with SAP.

Case 1: You are managing customer number(s) in view V_AISAPCUSTNOS

When individual S-user is obsolete at SAP, the above data in Focus Run will be deleted by report AI_SC_REFRESH_READ_ONLY_DATA accordingly. However, when the whole installation/customer is obsolete, you have to run report SOLMAN_DELETE_CUSTOMER_DATA to manually delete the data by selecting *Systems of a Customer* or *Systems of an Installation*.

Case 2: View V_AISAPCUSTNOS is empty.

As the customer number is unknown in Focus Run, report AI_SC_REFRESH_READ_ONLY_DATA cannot refresh the S-user data automatically. Therefore, you have to delete the S-users via report AI_SC_DISPLAY_CONTACT_DATA manually.

In addition, the entries in transaction AISUSER can be deleted manually.

Job Monitoring

The tables that hold personal data (UNAME, LAST_CHANGE_UNAME, LAST_CHANGED_BY & CREATED_BY) on who created or changed configuration information for the application are as follows:

- AJM_MO_STATUS
- AJM_ABAP_IDENT
- AJM_GRP_DETAILS
- AJM_METADATA
- AJM_ALERTTYPE

The report, AJM_DISP_DEL_PERSONAL_DATA, could be executed in *Test Mode* to check if personal data (UNAME, LAST_CHANGE_UNAME, LAST_CHANGED_BY & CREATED_BY) is stored in the application and which tables contain the personal data.

Same Report, AJM_DISP_DEL_PERSONAL_DATA, when run in *Production Mode* will allow the user to mask or delete all the personal data stored in the tables.

The execution of the above report is logged in SLG1 under object AJM and sub-objects SETUP, RUNTIME, and HOUSEKEEPING.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

www.sap.com/contactsap

THE BEST RUN SAP