Checklist for Support Backbone Update
For SAP Solution Manager 7.2 SPS 10 with Multiple Customer Scenarios
Content

1  Introduction ................................................................. 5
2  Step-by-Step Checklist .................................................... 6
  2.1  Request a Technical Communication User ................................. 8
  2.2  Check the Required Kernel Version ........................................... 9
  2.3  Check and Install CommonCryptoLib ........................................ 10
  2.4  Check and Adjust the TLS/SSL Protocol Version .......................... 12
  2.5  Configure and Activate HTTPS/SSL .......................................... 13
  2.6  Check the Application Server ............................................... 14
  2.7  Install SSL Certificates .................................................. 15
  2.8  Execute Task List SAP_SUPPORT_HUB_CONFIG .......................... 16
    Check the SAP-SUPPORT_PORTAL Connection ............................ 18
    Check the SAP-SUPPORT_PARCELBOX Connection ......................... 19
  2.9  Prepare Note Assistant ................................................... 20
  2.10  Set Customizing Parameter to Allow for Automatic Customer Number Updates .......................... 22
  2.11  Activate BAdl AT.SDK.SP.RFC.RP ....................................... 23
  2.12  VAR: Verify SAP Customer Number ....................................... 24
  2.13  VAR: Set Up One Connection to SAP for All Customers .................. 25
  2.14  Adjust Your User Logon Information for Specific Users .................. 26
  2.15  VAR: Configure Partner/VAR Communication Channels .................... 27
  2.16  Finalize Support Hub Connectivity ..................................... 29
  2.17  Check Jobs Using the New Connections .................................. 31
  2.18  Apply Final Corrections ................................................ 33
<table>
<thead>
<tr>
<th>Document Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-06-10</td>
<td>Added the Service Connections section to Apply Final Corrections [page 33].</td>
</tr>
<tr>
<td>2020-04-28</td>
<td>Updated the recommendation regarding SAPOSS in Adjust Your User Logon Information.</td>
</tr>
<tr>
<td>2020-02-27</td>
<td>Check Jobs Using the New Connections [page 31] erroneously stated that the job REFRESH_ADMIN_DATA_FROM_SUPPORT had been deactivated. This has been corrected to SEND_SYSTEM_RELATIONSHIP_TO_SUPP.</td>
</tr>
<tr>
<td>2020-02-18</td>
<td>Added information about the discontinuation of jobs SM:UPLOAD_SYSTEM_DATA and REFRESH_ADMIN_DATA_FROM_SUPPORT. See Check Jobs Using the New Connections [page 31].</td>
</tr>
<tr>
<td>2020-01-16</td>
<td>Updated IT Service Management [page 33]</td>
</tr>
</tbody>
</table>
Who Is This Guide For?

This checklist is relevant for you if either of the following situations applies to you:

- You manage multiple customers but require only one connection to the support backbone. For instance, you may be a service provider such as a PartnerEdge Sell partner (also known as a “value-added reseller” or “VAR”) or a customer with multiple customer numbers under the corporate group function (Customer Competence Center or Customer Center of Excellence), which may be for different regions or branches. We will point out information that is specific to you throughout this document.
- You manage multiple customers and you require multiple connections to the support backbone. You require one connection to the backbone for each of your customer numbers. This may include SAP Solution Manager as a Managed System (SMaaMS) customers, who are also known as “SAP Partners” or “SAP Hosting” customers.

Special Cases

1. You are a Partner Edge Sell partner in a corporate group but you don’t want to download or receive data from other partners in the same group.
   Your scenario is handled as the “one connection” scenario above. In this case, see SAP Note 2626887 and request that your customer number be removed from the corporate group. Once it has been removed, you can continue to configure the system as described here.

2. Your SAP Solution Manager system manages multiple PartnerEdge Sell subsidiaries.
   In this case, you must use a corporate group (CCC or CCoE) function. See SAP Note 2459283 and include all customer numbers from your subsidiaries as part of the corporate group. The updated support backbone doesn’t allow a PartnerEdge Sell partner to download or receive customer data from another partner without a valid business reason. Therefore, if the partner is not maintained contractually (by SAP) as the “support provider” of an end-customer installation, the partner will not be able to download the customer’s data.

Restriction

This document doesn’t contain detailed information about delta configurations. If you have upgraded to Support Package Stack 10, please work through all of the following steps and check whether your configuration is still valid.
1 Introduction

The support backbone is the infrastructure that we use to provide you with technical support. Your systems connect to the support backbone to exchange information, such as support incident data, maintenance planner data, and SAP EarlyWatch Alert data.

Due to the increasing demand placed on the support backbone, we have updated the infrastructure so that we can continue to provide you with the support you require. As part of this process, the way in which systems connect to SAP has been redesigned to include the following changes:

- The HTTPS protocol is now used instead of RFC.
- A technical communication user handles the data transfer instead of generic users.
- There is no generic inbound interface.
- Applications send data asynchronously unless the data is sent manually.

To help you transition smoothly to the updated support backbone, the legacy infrastructure will remain in place until January 8, 2020.

This document provides step-by-step tasks to help you retain connectivity to the support backbone after this date.

Before you start to work through this checklist, please familiarize yourself with the following information:

- SAP Support Backbone Update: How the SAP Support Backbone Update Affects SAP Solution Manager and Focused Run (including a list of affected SAP Solution Manager scenarios)
- Configuration and Upgrade Guide for Service Providers and Channel Partners on SAP Support Portal
  
This guide contains the required Customizing settings that you must configure before you can run your partner scenarios.
2 Step-by-Step Checklist

Before You Begin

This document is based on a readily customized partner scenario and is intended to help you convert from SAPOSS to the updated support backbone connections.

If you have a newly installed system, you must first configure your partner scenario. For more information, see the Configuration and Upgrade Guide for Service Providers and Channel Partners on SAP Support Portal.

We recommend that you work through the configuration steps with a user that has extended basic authorizations, as well as authorizations for SAP Solution Manager Configuration. For the latest updates to SAP Solution Manager authorizations, see SAP Note 2250709. Download the latest version from this SAP Note. Specifically, you require authorization for the roles SAP_SETUP_SYSTEM_PREP (to run the System Preparation procedure steps) and SAP_SM_BATCH (to allow for the smooth running of technical user SOLMAN_BTC). In addition, implement SAP Notes 2816890 and 2781686.

⚠ Caution

Information about the changes you need to make to connect to the updated support backbone is provided in this checklist, documentation in SAP Solution Manager Configuration (transaction SOLMAN_SETUP), and task list documentation in transaction STC01. If, despite our best efforts, you find discrepancies between these sources, please treat them with the following order of priority:

1. This checklist
2. Task list documentation
3. Documentation in SAP Solution Manager Configuration

If you have not already done so, implement SAP Note 2830316 to update the relevant parts of SAP Solution Manager Configuration (transaction SOLMAN_SETUP).

For the purposes of this checklist, call SOLMAN_SETUP only in English.

If You Need Help

Throughout this document, we provide some hints that you can use to resolve any problems that you may encounter. However, if your system does not run as expected after you have migrated to the updated support backbone, please refer to the central point of call for troubleshooting at Support Hub Connectivity: Guided Answers.

If you have configured all of the settings described in this document but you continue to experience connectivity issues, please open a message on component SV-SMG-INS-CFG and prefix your message title with “Backbone Update:” to simplify processing.
If you have a question about the technical infrastructure of the new communication channels, please open an incident on component XX-SER-NET-HTL. If you require more background about the relationship between the support backbone and SAP Solution Manager, see Connectivity to SAP’s Support Backbone.

Procedure

Use the following overview to work through the steps required to retain communication with the updated support backbone.

1. **Request a Technical Communication User** [page 8]
   Where: SAP ONE Support Launchpad | Useful SAP Notes: 2174416, 2740667, 2805811, 2911301
2. **Check the Required Kernel Version** [page 9]
   Where: SAP Solution Manager system
3. **Check and Install CommonCryptoLib** [page 10]
   Where: transaction STRUST | Useful SAP Notes: 2390726
4. **Check and Adjust the TLS/SSL Protocol Version** [page 12]
   Where: transaction SM69, RZ11 | Useful SAP Notes: 510007
5. **Configure and Activate HTTPS/SSL** [page 13]
   Where: transaction SMICM | Useful SAP Notes: 510007
6. **Check the Application Server** [page 14]
   Where: system OS
7. **Install SSL Certificates** [page 15]
   Where: transaction STRUST | Useful SAP Notes: 2631190
8. **Execute Task List SAP_SUPPORT_HUB_CONFIG** [page 16]
   Where: transactions STC01, SM59 | Useful SAP Notes: 2500061, 2454045
9. **Prepare Note Assistant** [page 20]
   Where: transactions SOLMAN_SETUP, SA38, SNOTE | Important SAP Notes: 2537133, 2721941, 2836302
10. **Set Customizing Parameter to Allow for Automatic Customer Number Updates** [page 22]
    Where: transaction SM30
11. **Activate BAdi AI_SDK_SP_RFC_RP** [page 23]
    Where: transaction SOLMAN_SETUP
12. **VAR: Verify SAP Customer Number** [page 24]
    Where: transaction SM30
13. **VAR: Set Up One Connection to SAP for All Customers** [page 25]
    Where: transaction SOLMAN_SETUP
14. **Adjust Your User Logon Information for Specific Users** [page 26]
    Where: transaction AISUSER | Useful SAP Notes: 2000132, 2174416
15. **VAR: Configure Partner/VAR Communication Channels** [page 27]
    Where: transaction SOLMAN_SETUP
16. **Finalize Support Hub Connectivity** [page 29]
    Where: transaction SOLMAN_SETUP | Useful SAP Notes: None at present
17. **Check Jobs Using the New Connections** [page 31]
    Where: transaction SM37 | Useful SAP Notes: 2250709, 2525987
18. Apply Final Corrections [page 33]

After you have completed the upgrade tasks, there are handful of SAP Notes that you must implement and some related activities to work through.

### 2.1 Request a Technical Communication User

**Where:** SAP ONE Support Launchpad | **Useful SAP Notes:** 2174416, 2740667, 2805811, 2911301

Technical communication users allow machine-to-machine communication and data exchange. Only super administrators and user administrators have access to the Technical Users app, where they can create, activate, and delete technical communication users.

**i Note**

Depending on your current release, you may already have at least one technical communication user (although you can request more if required). Technical communication users were introduced with SAP Solution Manager 7.2. They are also occasionally referred to as “technical S-users”, “support hub users”, or “users for support hub communication”.

Make sure that you request your technical communication users in good time. It can take up to 24 hours to receive them.

The number of technical communication users that you require depends on your company policy. It is possible to use one technical communication user for all systems. However, this may lead to connectivity issues if the user gets locked.

**→ Recommendation**

We recommend that you request one technical communication user per installation / system track (for example, DEV-QAS-PRD). The highest level of flexibility and security can be reached by using one technical communication user per system.

**i Note**

You can decide whether you require one technical user for one connection to the support backbone, or whether you require more than one connection to the support backbone for multiple customer numbers.

### Procedure

1. Request your technical communication user as described in SAP Note 2174416 and create client certificates for it as described in 2805811 (initial creation) and 2911301 (automated renewal).
2. Replace generic users with the technical communication user(s) as instructed in SAP Note Request your technical communication user as defined in SAP Note 2740667.
3. Make sure that you activate your technical communication user as described in SAP Note 2174416.

For a list of frequently asked questions about technical communication users, see the User Handling section at Update of SAP’s Support Backbone: Frequently Asked Questions (FAQ).
Check

You can check whether your technical communication user has been activated successfully at https://launchpad.support.sap.com/#/techuser.

Your Notes

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

Parent topic: Step-by-Step Checklist [page 6]

Next: Check the Required Kernel Version [page 9]

Related Information

SAP Note 2174416
Creation and activation of users in the Technical Users application - SAP ONE Support Launchpad

SAP Note 2740667
RFC connection SAPOSS to SAP Service & Support backbone will change (latest) in January 2020

SAP Note 2805811
How to enable client certificate authentication for technical communication users

SAP Note 2911301
SAP Support Portal connection - Renew client certificate of technical S-user

2.2  Check the Required Kernel Version

Where: SAP Solution Manager system

To retain communication with the support backbone, you must make sure that your SAP Solution Manager system is running on the correct kernel version and patch level.
Valid kernel versions and patch levels are:
- Kernel release 742, patch level 401 and above
- Kernel release 745, patch level 400 and above
- Kernel release > 745

**Procedure**

1. In your SAP Solution Manager system, choose **System > Status...**
2. Click (Other kernel info.) or press **SHIFT + F5**.

Your kernel release and patch level are shown in the **Kernel Information** area. If they are below the required levels, patch to the level specified above.

**Your Notes**

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

Parent topic: Step-by-Step Checklist [page 6]

Previous: Request a Technical Communication User [page 8]

Next: Check and Install CommonCryptoLib [page 10]

### 2.3 Check and Install CommonCryptoLib

**Where:** transaction **STRUST** | **Useful SAP Notes:** 2390726

You require at least version 8.4.48 of the CommonCryptoLib library to retain your connection to the support backbone.

→ **Recommendation**

We recommend that you always upgrade to the latest version of CommonCryptoLib.
Procedure

1. In your SAP Solution Manager system, call transaction STRUST and choose ![Environment ![Display SSF Version](image) from the menu.
2. Check the installed version of CommonCryptoLib.

![Version Image]

3. If you have to update your version of CommonCryptoLib, go to the Software Downloads area of SAP Support Portal and search for CommonCryptoLib in the Support Packages and Patches area.

For more information, see the Prerequisites section of Support Hub Connectivity Configuration in SAP Solution Manager 7.2 SP05 or Higher.

Your Notes

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

Parent topic: Step-by-Step Checklist [page 6]

Previous: Check the Required Kernel Version [page 9]

Next: Check and Adjust the TLS/SSL Protocol Version [page 12]

Related Information

**SAP Note 2390726**

Fixes in CommonCryptoLib 8.5.7
2.4 Check and Adjust the TLS/SSL Protocol Version

Where: transaction SM69, RZ11 | Useful SAP Notes: 510007

The connection to the support backbone requires SSL protocol version TLS1.1 or higher for outbound HTTP connections. TLS versions 1.0, 1.1, and 1.2 are enabled by the `ssl/client_ciphersuites` parameter value.

To communicate properly with the support backbone, make sure that SSL profile parameter `ssl/client_ciphersuites` for outgoing HTTP connections is set correctly. We recommend a value of 150:PFS:HIGH::EC_P256:EC_HIGH provided that you have implemented the correction instructions and manual activities in SAP Note 2781565. For detailed, expert information, see SAP Note 510007. You can also use the value 918:PFS:HIGH::EC_P256:EC_HIGH for SAP Solution Manager (in which case, SAP Note 2781565 is not required). However, this will not work with TLS protocol versions above 1.2.

Also make sure that you are using the most recent version of CommonCryptoLib (8.4.31 or higher).

Procedure

1. Check the value of parameter `ssl/client_ciphersuites`:
   1. Call transaction RZ11 and enter `ssl/client_ciphersuites`.
   2. Note the current value of parameter `ssl/client_ciphersuites`.

2. Check the TLS version:
   1. Call transaction SM69, select the command SAPGENPSE and choose Execute.
   2. Enter the first three digits from the `ssl/client_ciphersuites` value in the Additional Parameters field.
3. Execute the command and make sure that at least TLS 1.1 is listed under Configured protocol versions.

Your Notes

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

Parent topic: Step-by-Step Checklist [page 6]

Previous: Check and Install CommonCryptoLib [page 10]
Related Information

SAP Note 510007
Setting up SSL on Application Server ABAP

2.5 Configure and Activate HTTPS/SSL

Where: transaction SMICM | Useful SAP Notes: 510007

Check that the communication between your Web browser and your SAP Solution Manager system is handled using the HTTPS protocol.

→ Recommendation

Allow yourself plenty of time to complete this step. It may take a few hours.

The connection to the updated support backbone concerns only ABAP systems, although we recommend that you use HTTPS in your Java systems as well.

Procedure

1. Check whether HTTPS communication is used in your SAP Solution Manager system by calling transaction SMICM and choosing Goto Services. Check whether the HTTPS protocol is listed under Active Services.

   i Note

   If both HTTP and HTTPS are used in your system, consider using HTTPS only.

   If you want to configure the support backbone connection in a sandbox/test environment, HTTPS is not mandatory and this step can be skipped.

2. If an HTTPS connection is not used, see the SAP NetWeaver Security Guide on SAP Help Portal and pay particular attention to the following topics:

   Transport Layer Security
   Configuring SAP NetWeaver AS for ABAP to Support SSL
   Configuring Transport Layer Security on SAP NetWeaver AS for Java

3. After you have configured the HTTPS connection, enter it in SAP Solution Manager Configuration (transaction SOLMAN_SETUP) in the System Preparation scenario. Navigate to the Check Prerequisites step and maintain the activity Check Secure Web Browser Comm. (HTTPS).
2.6 Check the Application Server

Where: system OS

Make sure that the SAP Solution Manager application server can reach a server outside your network (that is to say, check your network access at OS level). In particular, the following servers must be reachable:

- apps.support.sap.com
- documents.support.sap.com
- notesdownloads.sap.com
- servicepoint.sap.com

External access can be managed in any of the following ways:

- The application server has direct access to the Internet via HTTPS
- The application server has indirect access to the Internet via HTTPS and a Web proxy.
- The application server has indirect access to external networks via HTTPS and the SAP proxy “SAProuter”.

For more information, see the guided answer Check All Prerequisites.
2.7 Install SSL Certificates

Where: transaction STRUST | Useful SAP Notes: 2631190

Context

The following certificates are required for the support backbone:

- VeriSign Class 3 Public Primary Certification Authority - G5
- DigiCert Global Root CA
- DigiCert Global Root G2
- DigiCert High Assurance EV Root CA

Procedure

1. Call transaction STRUST and check that SSL client SSL Client (Standard) and SSL client SSL Client (Anonymous) are correct.
2. Check that the status is green and that all of the above certificates are present for both the anonymous and standard PSEs. If this is the case, no further action is required. Otherwise, proceed with step 3 [page 15].
3. Download the required certificates from SAP Note 2631190.
4. In transaction STRUST, choose Certificate > Import to add the certificates to SSL client SSL Client (Standard) and SSL client SSL Client (Anonymous).
Task overview: Step-by-Step Checklist [page 6]

Previous: Check the Application Server [page 14]

Next: Execute Task List SAP_SUPPORT_HUB_CONFIG [page 16]

Related Information

SAP Note 2631190
Download location of SSL certificates required for Support Hub Connectivity configuration

2.8 Execute Task List SAP_SUPPORT_HUB_CONFIG

Where: transactions STC01, SM59 | Useful SAP Notes: 2500061, 2454045

**Note**
This step is only to be done **once** for your technical communication user (that is, the technical communication user for your own customer number as a PartnerEdge Sell partner or your SMaaMS scenario).

Task list SAP_SUPPORT_HUB_CONFIG contains a number of tasks, some of which you may have already set up. In this case, you can use the task list to check your setup.

The task list also creates connections SAP-SUPPORT_PORTAL, SAP-SUPPORT_PARCELBOX, and SAP-SUPPORT_NOTE_DOWNLOAD, which are required for the updated support backbone.

All of the relevant information is provided in the task list itself.

**Note**
The user and password defined in this task list must be correct. User RFC_OSS is no longer supported for any of the new connections. Make sure that you have the correct users and that they are correctly assigned.

Use your technical communication user **only** for communication with the support backbone. Do not use it for any other connections. If you try to log in to a system such as SAP ONE Support Launchpad using the technical communication user, you risk locking it.

If you change the password, wait for 30 minutes so that the new password can be propagated to all of the relevant SAP systems. During this time, avoid testing the channels, starting jobs, and uploading data (for example, via LMDB). The technical communication user will be locked after five failed logon attempts.

If your technical communication user does become locked (“SAP service point ping error: 401 Unauthorized”), please see SAP Note 2392726 for instructions on how to unlock it.
**Procedure**

1. Call transaction **STC01**.  
   If you are unfamiliar with this transaction, see this wiki page for more information.
2. Enter the name of the task list.
3. Run all of the activities described here.
4. Call transaction **STC02** to check that the task list ran successfully.

**Troubleshooting**

For information about changing the technical communication user, password, SAProuter string, or proxy settings for the support backbone, see this guided answer.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>The step “Check connectivity and credentials to SAP Support Portal” fails with the error message SAP portal connection error 404 : Proxy Connection Refused.</td>
<td>See the guided answer at Check if Relevant HTTP Proxy or SAProuter Is Reachable from SAP Solution Manager 7.2.</td>
</tr>
<tr>
<td>All applications that use a synchronous communication channel return an error message even though configuration was successful.</td>
<td>See the guided answer at Delete the Value in Field Path Prefix in HTTP Destination SAP-SUPPORT_PORTAL and Save the Entry.</td>
</tr>
</tbody>
</table>

**Your Notes**

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

**Parent topic:** Step-by-Step Checklist [page 6]

**Previous task:** Install SSL Certificates [page 15]

**Next:** Prepare Note Assistant [page 20]
2.8.1 Check the *SAP-SUPPORT_PORTAL* Connection

After you have executed task list `SAP_SUPPORT_HUB_CONFIG`, connection `SAP-SUPPORT_PORTAL` (*HTTP Connection to ABAP System* [type H]) should be fully operational. You can verify this in transaction `SM59`.

### Procedure

1. Call transaction `SM59` and open the connection `SAP-SUPPORT_PORTAL`.
2. Enter the path prefix `/sap/bc/bsp/svt/sapping` and run the connection check.
3. If the check is successful, delete the prefix from the connection and reenter the credentials for the technical communication user.

### Troubleshooting

<table>
<thead>
<tr>
<th>Issue</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>You test destination <code>SAP-SUPPORT_PORTAL</code> or ping the Web service for the asynchronous channel in <code>SOAMANAGER</code> and you get the error 407 Proxy Authentication Required.</td>
<td>See the guided answer at Check the Proxy Settings and Password.</td>
</tr>
<tr>
<td>Although the support hub channels were configured successfully, the connection test for destination <code>SAP-SUPPORT_PORTAL</code> finished with <code>HTTPIO_PLG_CANCELED</code>.</td>
<td>See the guided answer at Activate the HTTPS Service.</td>
</tr>
<tr>
<td>Access to target host <code>servicepoint.sap.com</code> fails with the error <code>SAP service point ping error : 404 Connection Refused</code>.</td>
<td>See the guided answer at Ensure That SAProuter String Was Entered and Is Correct.</td>
</tr>
<tr>
<td>Access to target hosts <code>servicepoint.sap.com</code> or <code>apps.support.sap.com</code> fails with the error <code>NIECONN_REFUSED(-10)</code>.</td>
<td>See the guided answer at Ensure That SAProuter String Was Entered in STC01.</td>
</tr>
</tbody>
</table>
2.8.2 Check the SAP-SUPPORT_PARCELBOX Connection

After you have executed task list SAP_SUPPORT_HUB_CONFIG, connection SAP-SUPPORT_PARCELBOX (HTTP Connection to External Serv. [type G]) should be fully operational. You can verify this in transaction SM59.

Procedure

1. Call transaction SM59 and open the connection SAP-SUPPORT_PARCELBOX.
2. Check that the path prefix /parcel/ is entered and run the connection checks.

Your Notes

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

2.8.3 Check the SAP-SUPPORT_NOTE_DOWNLOAD Connection

After you have executed task list SAP_SUPPORT_HUB_CONFIG, connection SAP-SUPPORT_NOTE_DOWNLOAD (HTTP Connection to External Serv. [type G]) should be fully operational. You can verify this in transaction SM59.
Procedure

1. Call transaction SM59 and open the connection SAP-SUPPORT_NOTE_DOWNLOAD.
2. Enter the path prefix `/note/0040000000874972019` and run the connection check.
3. If the check is successful, delete the prefix from the connection and reenter the credentials for the technical communication user.

Your Notes

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

2.9 Prepare Note Assistant

Where: transactions SOLMAN_SETUP, SA38, SNOTE | Important SAP Notes: 2537133, 2721941, 2836302

i Note

This section applies only to systems to which you want to download SAP Notes (such as development or quality assurance environments). If you are transporting SAP Notes to your SAP Solution Manager system, this section is not relevant.

Note Assistant requires that you use the SAP NetWeaver Download Service or the HTTPS protocol to download SAP Notes. Download Service is the recommended option.

Procedure

To implement the SAP NetWeaver download service, proceed as follows:

1. Open SAP Solution Manager Configuration (transaction SOLMAN_SETUP) and in the System Preparation scenario, navigate to the Check Prerequisites step.
2. Execute the activity Check Secure Web Browser Comm. (HTTPS).
Check

You can check that Note Assistant now connects to the updated support backbone by running the report *Defining Procedure for Downloading SAP Note* (RCWB_SNOTE_DWNLD_PROC_CONFIG) and checking the settings there.

- If an RFC connection is used to download SAP Notes, the outdated support backbone is being used unless a redirect is in place.
- If an HTTP connection is used to download SAP Notes, the updated support backbone is being used.
- If the download service is used, it will connect to the updated support backbone.

Tip

Regardless of which procedure you use to download SAP Notes, you can check the log of the downloaded SAP Note to see whether it is digitally signed. The log also includes the procedure that was used for the download.

Your Notes


Parent topic: Step-by-Step Checklist [page 6]

Previous: Execute Task List SAP_SUPPORT_HUB_CONFIG [page 16]

Next: Set Customizing Parameter to Allow for Automatic Customer Number Updates [page 22]

Related Information

- **SAP Note 2537133**
  FAQ - Digitally Signed SAP Notes
- **SAP Note 2576306**
  Transport-Based Correction Instruction (TCI) for Download of Digitally Signed SAP Notes
- **SAP Note 2721941**
  Download of digitally signed note - changes to configuration report and other minor changes
- **SAP Note 2836302**
2.10 Set Customizing Parameter to Allow for Automatic Customer Number Updates

Where: transaction SM30

In this step, you set a parameter that automatically updates and refreshes any new customer numbers with an S-user assignment from the support backbone.

Procedure

1. Call transaction SM30.
2. Open the view DNOC_USERCFG (Service Desk Customizing) in maintenance mode.
3. Create a new entry using the following data:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>&lt;blank&gt;</td>
</tr>
<tr>
<td>Field Name</td>
<td>AI_SC_GET_NEW_CUSTOMERS</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>0</td>
</tr>
<tr>
<td>Description</td>
<td>&lt;free text&gt;</td>
</tr>
<tr>
<td>Field Value</td>
<td>X</td>
</tr>
</tbody>
</table>

Your Notes

Parent topic: Step-by-Step Checklist [page 6]

Previous: Prepare Note Assistant [page 20]

Next: Activate BAdI AI_SDK_SP_RFC_RP [page 23]
2.11 Activate BAdI AI_SDK_SP_RFC_RP

Where: transaction SOLMAN_SETUP

You will need to send data to cross-customer destinations at SAP. BAdI AI_SDK_SP_RFC_RP activates the general, multiple-customer configuration steps.

Procedure

1. Call transaction SOLMAN_SETUP.
2. In the Mandatory Configuration scenario, choose System Preparation and navigate to step 2 (Check Prerequisites).
3. Run the activity VAR: BAdI: Manage Several SAP Customer Numbers.
4. Activate the BAdI implementation.

Check

Activating this BAdI enables you to extend table AISUSER in transaction AISUSER. Call this transaction and check that the customer number column is displayed.

When you activate the BAdI, the system automatically adds the following activities to step 3.2 of the System Preparation scenario:

- VAR: Verify SAP Customer Number
- VAR: Set Up One Connection to SAP for All Customers
- VAR: Configure Partner Communication Channels

Your Notes

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

Parent topic: Step-by-Step Checklist [page 6]

Previous: Set Customizing Parameter to Allow for Automatic Customer Number Updates [page 22]
2.12 VAR: Verify SAP Customer Number

**Where:** transaction SM30

**i Note**
- If you are a PartnerEdge Sell partner, enter only your own customer number.
- If you are an SMaaS provider, enter all of your customers' numbers.

**Procedure**

1. Call transaction **SOLMAN_SETUP**.
2. In the **Mandatory Configuration** scenario, choose **System Preparation** and navigate to step 3.2 (**Support Hub Connectivity**).
3. Run the activity **VAR: Verify SAP Customer Number**.
4. Open the view **V_AISAPCUSTNOS** (**SAP Customer Numbers**) in maintenance mode.
5. Check that your SAP customer number(s) are maintained correctly.
   - The customer name can be empty. It is filled by batch job **REFRESH_ADMIN_DATA_FROM_SUPPORT**.

**Your Notes**

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

**Parent topic:** Step-by-Step Checklist [page 6]

**Previous:** Activate BAdI Al_SDK_SP_RFC_RP [page 23]

**Next:** VAR: Set Up One Connection to SAP for All Customers [page 25]
2.13  VAR: Set Up One Connection to SAP for All Customers

Where: transaction SOLMAN_SETUP

**i Note**

This step is relevant only if you use one destination (synchronous) for all your customer numbers.

In this step, you set up one connection to the support backbone for several customer numbers and remove the previous parameter.

**Procedure**

1. **Add field** ONE_RFC_TO_SAP_FOR_ALL_CUST:
   1. Call transaction SOLMAN_SETUP.
   2. In the Mandatory Configuration scenario, choose System Preparation and navigate to step 3.2 (Support Hub Connectivity).
   3. Run the activity VAR: Set Up One Connection to SAP for All Customers.
   4. Open the view DNOC_USERCFG (Service Desk Customizing) in maintenance mode.
   5. Set the field value for field ONE_RFC_TO_SAP_FOR_ALL_CUST to **X**.
      If the field doesn’t exist, create a new entry using the following data:

      | User Name     | <blank> |
      | Field Name    | ONE_RFC_TO_SAP_FOR_ALL_CUST |
      | Sequence Number | 1 |
      | Description   | RFC connection to SAP Support Global Backbone |
      | Field Value   | X |

2. **Set the field value for parameter AI_SC_GET_NEW_CUSTOMERS to **X**:**
   1. Click New Entries, enter field AI_SC_GET_NEW_CUSTOMERS and set the field value to **X**.
      For other possible values, see SAP Note 2182476.
   3. **Remove field** AI_SC_REFRESH_OSS:
      1. In the same table, select the row containing field AI_SC_REFRESH_OSS.
      2. Delete the entry and save your changes.

**Your Notes**
2.14 Adjust Your User Logon Information for Specific Users

Where: transaction AISUSER | Useful SAP Notes: 2000132, 2174416

An S-user is a user in the support backbone with actual authorizations and must be assigned to SAP Solution Manager system users in table AISUSER. Specifically, it must be assigned to the following users:

- SOLMAN_BTC
- SOLMAN_ADMIN
- SAPSUPPORT

The assigned system users can then perform specific activities with the support backbone (such as sending an incident to SAP). Table AISUSER contains your S-user, not your technical communication user. The technical communication user is intended only to establish the connection to the support backbone and does not have any authorizations itself.

Procedure

1. Call transaction AISUSER and check that the correct contact person (S-user number) is correctly assigned to the users:
   - SOLMAN_BTC
   - SOLMAN_ADMIN
   - SAPSUPPORT

2. If the contact person is incorrect, enter the correct S-user (not the technical communication user).

   **Note**
   You may need to press **ENTER** twice to correctly add entries to the table.
Check

Check the entries for your dialog users and the S-user assignments in transaction AISUSER.

If you require more than one destination for your customers, you must have an entry for each customer number and user. Check that the entries are correctly maintained and that the S-user in the Contact Person column belongs to the relevant customer number. This is especially relevant for users who send incidents to SAP. Each user requires a separate entry.

Your Notes

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

Parent topic: Step-by-Step Checklist [page 6]

Previous: VAR: Set Up One Connection to SAP for All Customers [page 25]

Next: VAR: Configure Partner/VAR Communication Channels [page 27]

Related Information

SAP Note 2000132
Configuring RFC connections to the SAPNet R/3 front end (OSS) correctly

SAP Note 2174416
Creation and activation of users in the Technical Users application

Secure Configuration Security Guide

2.15 VAR: Configure Partner/VAR Communication Channels

Where: transaction SOLMAN_SETUP

In this step, you create all required connections for the new support backbone. The connections that you created earlier (such as SAP-SUPPORT_PORTAL, SAP-SUPPORT_PARCELBOX, or port channels) are copied and
assigned to the relevant technical communication user(s). These copied connections are created by the system with the naming convention: SM_SP_<customer number>_*.

You set up the following communication channels:

- **SAP-SUPPORT_PORTAL**: Destinations in the format SM_SP_<customer number>_H
- Asynchronous: Logical ports in the format SM_SP_<customer number>_H
- **SAP-SUPPORT_PARCELBOX**: Destination in the format SM_SP_<customer number>_G

**Note**

**If you require only one connection to the support backbone:**

If you require only one connection (PartnerEdge Sell partner or CCC), run this activity only once. Transaction SM59 will then contain your original connections and the copied connections with the format SM_SP_<customer number>_*.

**If you require multiple connections:**

If you require multiple connections to the support backbone (SMaaS), run this activity for each of your customer numbers.

**Procedure**

1. Call transaction SOLMAN_SETUP.
2. In the System Preparation scenario, navigate to step 3.2 (Support Hub Connectivity).
3. Select the activity VAR: Configure Partner/VAR Communication Channels.
   The navigation of this activity links you to a specific activity. The help text for contains the information that you require to complete this step.

   **Tip**
   The required user here is the technical communication user from Request a Technical Communication User [page 8].

**Check**

Call transaction SM59 and check that the new connections are displayed.

Check the naming conventions have been applied correctly:

- SM_SP_<customer number>_H for SAP-SUPPORT_PORTAL
- SM_SP_<customer number>_G for SAP-SUPPORT_PARCELBOX
2.16 **Finalize Support Hub Connectivity**

**Where:** transaction SOLMAN_SETUP | **Useful SAP Notes:** None at present

“Finalize Support Hub Connectivity” is an automatic activity in SAP Solution Manager Configuration. It creates logical ports and checks whether the communication channels (both synchronous and asynchronous) are operational. Specifically, it creates logical port LP_SISE_SUPPORTHUB for the following consumer proxies:

- CO_SISEHUB_MI_O_AS_PUT_EXTERNA
- CO_SISEHUB_MI_O_S_SHB_GET_EX
- CO_SISEHUB_MI_O_S_SHB_LIST
- CO_SISEHUB_MI_O_S_SHB_REMOVE

**Procedure**

1. Open SAP Solution Manager Configuration (transaction SOLMAN_SETUP) and navigate to step 3.2 (Support Hub Connectivity) in the System Preparation scenario.
2. Execute the automatic activity Finalize Support Hub Connectivity.

**Check**

1. Open SOA Management (transaction SOAMANAGER) and click Web Service Configuration.
2. Change the selection filter for the object name from is to contains and search for object names that contain *HUB*.
The search returns the consumer proxies mentioned above.

3. Click each of the consumer proxies in turn to open their details and ping logical port LP_SISE_SUPPORTHUB by clicking (Ping Web Services).

For more information, see How to Check the Asynchronous Channel.

Troubleshooting

For troubleshooting information, see Error Messages in Task “Check Connectivity and Credentials to SAP Support Portal”.

Your Notes

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

Parent topic: Step-by-Step Checklist [page 6]

Previous: VAR: Configure Partner/VAR Communication Channels [page 27]

Next: Check Jobs Using the New Connections [page 31]

Related Information

SAP Note 2522789
How to check error ‘Web service ping failed for logical port LP_SISE_SUPPORTHUB’ in Solution Manager 7.2 as of SP05
### 2.17 Check Jobs Using the New Connections

Where: transaction SM37 | Useful SAP Notes: 2250709, 2525987

User SOLMAN_BTC runs a number of jobs that connect to the support backbone. These are:

<table>
<thead>
<tr>
<th>Job Name</th>
<th>Job Frequency</th>
<th>Relevant for Systems...</th>
</tr>
</thead>
<tbody>
<tr>
<td>REFRESH_ADMIN_DATA_FROM_SUPPORT</td>
<td>Daily</td>
<td>Production only</td>
</tr>
<tr>
<td>SEND_SYSTEM_RELATIONSHIP_TO_SUPPP</td>
<td>Daily</td>
<td>All</td>
</tr>
<tr>
<td>SERVICE_CONNECTION_LISTENER</td>
<td>Every minute</td>
<td>Production only</td>
</tr>
<tr>
<td>SM:AGS_SISE_SUPHUB_OUTBOX_PROCES</td>
<td>Hourly</td>
<td>All</td>
</tr>
<tr>
<td>SM:EXEC_SERVICES</td>
<td>Daily</td>
<td>All</td>
</tr>
<tr>
<td>SM:GET_PPMS_DATA_FROM_OSS</td>
<td>Daily</td>
<td>Production only</td>
</tr>
<tr>
<td>SM:GET_CSN_COMPONENTS</td>
<td>Weekly</td>
<td>Production only</td>
</tr>
<tr>
<td>SM:LMDB GENERIC_UPLOAD</td>
<td>Hourly</td>
<td>Production only</td>
</tr>
<tr>
<td>SM:LONG_FILE_EXTDOWNLOAD</td>
<td>Weekly</td>
<td>Production only</td>
</tr>
<tr>
<td>SM:RCD_CHECK_UPDATES</td>
<td>Weekly</td>
<td>All</td>
</tr>
<tr>
<td>SM:REFRESH_MESSAGE_STATUS</td>
<td>Hourly</td>
<td>Production only</td>
</tr>
<tr>
<td>SM:SELFDIAGNOSIS</td>
<td>Daily</td>
<td>All</td>
</tr>
<tr>
<td>SM:SELFDIAGNOSIS_SEND_TO_SAP</td>
<td>Monthly</td>
<td>All</td>
</tr>
<tr>
<td>SM:SERVICE_CONNECTION_MIGRAT_SPP</td>
<td>Run once only</td>
<td>All</td>
</tr>
<tr>
<td>SM:SERVICE_CONTENT_UPDATE</td>
<td>Daily</td>
<td>All</td>
</tr>
<tr>
<td>SM:SYNC_SAP_SESSIONS</td>
<td>Daily</td>
<td>All</td>
</tr>
<tr>
<td>SM:SYNC_SERVICE_REQUESTS</td>
<td>Hourly</td>
<td>Production only</td>
</tr>
<tr>
<td>SM:SYSTEM_RECOMMENDATIONS</td>
<td>Weekly</td>
<td>All</td>
</tr>
<tr>
<td>SM:TOP_ISSUE_TRANSFER</td>
<td>Daily</td>
<td>Production only</td>
</tr>
<tr>
<td>SM:UPDATE_RULES</td>
<td>Daily</td>
<td>All</td>
</tr>
<tr>
<td>SM:UPLOAD_SYSTEM_DATA</td>
<td>Daily</td>
<td>All</td>
</tr>
</tbody>
</table>

#### Note

The background job SM:UPLOAD_SYSTEM_DATA has been deactivated as of January 27, 2020. For more information, see SAP Note 2863831. Tasks that were handled by this job are now handled by job SM:LMDB GENERIC UPLOAD.

The SM:LMDB GENERIC UPLOAD job updates your SAP customer numbers and downloads S-users from the support backbone. This adds the relevant customer numbers and S-users to table AISUSER. We recommend that you regularly check these updates and assign the correct data.
You may also need to schedule report `AI_SDK_SP_GENERATE_BP_V2` to enable business partner creation.

Background job `SM:REFRESH_RFCDEST` (not listed above) is now completely obsolete (see SAP Note 894279) and can be deleted (using transaction SM37).

**Check**

1. Call transaction SM37 and make sure that there are no errors or references to old destinations in the logs for the jobs mentioned above.
   
   Note that some jobs use legacy destinations (such as `SAPOSS`) as a fallback if communication with SAP fails using a new destination. The overall status of a job can therefore be misleading, and so we recommend that you check the job logs and not just the overall status of a job in SM37.

2. If a job runs infrequently and a scheduled run hasn’t taken place since you migrated your system to the updated support backbone, wait for the first scheduled run to take place and then check your system.

**Troubleshooting**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>General issues regarding the job log.</td>
<td>See the guided answer at <a href="#">Check the Job Log</a>.</td>
</tr>
<tr>
<td>When you check the response from SAP, the job fails with the message Internal Server Error <code>SRT_CORE 122</code> or Timeout error (<code>ICM_HTTP_TIMEOUT</code>).</td>
<td>See SAP Note 2525987.</td>
</tr>
<tr>
<td>Logical port <code>LP_SISE_SUPPORTHUB</code> isn’t available for proxy class <code>CO_SISEHUB_MI_O_S_SHB_LIST</code>.</td>
<td>See SAP Note 2665368.</td>
</tr>
</tbody>
</table>

**Your Notes**

____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________
____________________________________________________________________________________________________

**Parent topic:** [Step-by-Step Checklist [page 6]]

**Previous:** [Finalize Support Hub Connectivity [page 29]]
Related Information

SAP Note 2250709
Solution Manager 7.2: End-User Roles and Authorizations Corrections as of SP01 and higher

SAP Note 2525987
Internal Server Error, SoapFaultCode:5 Server Error or Timeout error (ICM_HTTP_TIMEOUT) in jobs using the asynchronous channel

2.18 Apply Final Corrections

After you have completed the upgrade tasks, there are handful of SAP Notes that you must implement and some related activities to work through.

Service Data Control Center (SDCCN) – Universally Relevant (for Example, for SAP EarlyWatch Alert)

If your SAP Solution Manager 7.2 SP 10 system is running together with ST-PI 740 SP11 (it cannot be running on a lower SP), implement the following SAP Note:

2802999 – SDCCN activation fails without errors or red icons in Migrate tab

Then call transaction SDCCN and check whether the Migrate tab appears. If so, follow the instructions there. Also implement SAP Note 2744825 (Self-Diagnosis: Alert 211 - Changes for SDCC_OSS Shutdown) to avoid false positives in the SAP Solution Manager Self-Diagnosis framework.

Service Connections

If you are using the Service Connections application (transaction SOLMAN_CONNECT), implement the following SAP Note:

• 2928430 – Open R/3 connection without using SAPOSS

IT Service Management

If you are using IT Service Management (ITSM), schedule report AI_CRM_IM_UPDATE_FROM_SAP_WS to run instead of AI_CRM_IM_UPDATE_FROM_SAP so that incidents can be exchanged with SAP.
Also implement the following SAP Note:

- **1483276** – Use of Customizing Parameters in DNO_CUST04, AGS_WORK_CUSTOM, and ICT_CUSTOM
  This is relevant not only for IT Service Management. Please pay particular attention to parameter SAP_INCIDENT_EXCHANGE

Parent topic: Step-by-Step Checklist [page 6]

Previous: Check Jobs Using the New Connections [page 31]

Related Information

SAP Note **2880999**

SAP Backbone connectivity update - Alert 00188 in Self-Diagnosis is no longer valid
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.

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.

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.