

Installation steps

Installation of PowerConnect for Splunk requires the following steps to be completed in the order listed below.

1. If you wish to use HTTPS / SSL connection between SAP and Splunk please setup the SSL support in the ABAP engine using the steps listed here. (link to Setting up HTTPS / SSL support).
2. Import the agent using TMS / SAINT
3. Activate BC Sets
4. Upload PowerConnect Roles
5. Start the PowerConnect for Splunk control panel in SAP using tcode /BNWVS/MAIN
6. Configure the connection between SAP and Splunk
7. Load HDB Scripts (HANA only)

Setting up HTTPS / SSL support in SAP

By default, Splunk REST API listens on port 8089 and HEC on Port 8088 with SSL active. SAP supports SSL however some basic setup is needed to provide SSL functionality to the native HTTP client built in to the ICM to support HTTPS. You can disable SSL support in Splunk and use HTTP without SSL to communicate between SAP and Splunk however it is not recommended for a production environment, especially where Splunk traffic traverses a shared network or in a public or private cloud hosted solution for SAP or Splunk.

If you wish to enable SSL support in SAP ABAP, please follow the steps below.

Please note that the instructions below are for setting up SSL to Splunk with a default configuration that includes a self-signed certificate that is included into Splunk during installation.

Important Note(s):

If your Splunk Enterprise Server has a custom SSL certificate installed, the process is the same, however names you see in the examples will differ from the screen shots below.

If you connect to a Splunk server via a proxy server then you will need to install any certificates that may sign HTTPS requests that flow through it into SAP.

If you are unsure about how to configure SSL, or you get SSL *chain-verify* or *peer verify* errors in SAP log a support call. You will need a valid license and support agreement to get email and phone support.

Ensure that System environment variable SECUDIR is set, this normally points to the /usr/sap/<SID>/<Instance>/sec directory.

If further details are required for setting environment variables please refer to SAP OSS Note 1827566 - <http://service.sap.com/sap/support/notes/1827566>

Download the latest SAP Crypro library from SAP Marketplace and unpack into the instance executable directory

<http://support.sap.com/swdc> → Support Packages and Patches → My Application Components → SAPCRYPTOLIB

In transaction RZ10 set the following profile parameters into the Default.pfl profile parameters. A restart of you SAP system is required after saving updated profile.

Profile Parameter	Value	Examples
ssl/ssl_lib	Path and file name of the SAP Cryptographic Library	UNIX: /usr/sap/<SID>/SYS/exe/run/libsapcrypto.so Windows NT: <DRIVE>:\usr\sap\<SID>\SYS\exe\run\sapcrypto.dll
sec/libsapsecu	Path and file name of the SAP Cryptographic Library	UNIX: /usr/sap/<SID>/SYS/exe/run/libsapcrypto.so Windows NT: <DRIVE>:\usr\sap\<SID>\SYS\exe\run\sapcrypto.dll
ssf/ssfapi_lib	Path and file name of the SAP Cryptographic Library	UNIX: /usr/sap/<SID>/SYS/exe/run/libsapcrypto.so Windows NT: <DRIVE>:\usr\sap\<SID>\SYS\exe\run\sapcrypto.dll
ssf/name	SAPSECULIB	SAPSECULIB
icm/server_port_<xx>	PROT=HTTPS, PORT=<port>, TIMEOUT=<timeout_in_seconds>	PROT=HTTPS, PORT=1443, TIMEOUT=900

In transaction STRUSTSSO2 activate the following SSL nodes:

- SSL Server Standard
- SSL Client SSL Client (Anonymous)
- SSL Client SSL Client (Standard)

Activate by right clicking on each node and selecting "Create" - The default entry can be used unless specific security policies must be adhered too.

Trust Manager for Single Sign-On with Logon Ticket: Display

68

- System PSE
- SNC SAPCryptolib
- SSL server Standard
- SSL client SSL Client (Anonymo
- SSL client SSL Client (Standar
- SSL client WSSE
- WS Security Standard
- WS Security Other System Encry
- WS Security WS Security Keys
- SMIME Standard
- File
- SSF Collaboration Integration
- SSF E-Learning
- SSF Logon Ticket

System PSE

Own Certificate

Subject CN= (Self-Signed)

Certificate List

Subject
CN=

Veri. PSE Password

Change Mode →

Trust Manager for Single Sign-On with Logon Ticket: Change

68

- System PSE
- SNC SAPCryptolib
- SSL server Standard
- SSL client SSL Client (Anonymo
- SSL client SSL Client (Standar
- SSL client WSSE
- WS Security Standard
- WS Security Other System Encry
- WS Security WS Security Keys
- SMIME Standard
- File
- SSF Collaboration Integration
- SSF E-Learning
- SSF Logon Ticket

System PSE

Own Certificate

Subject CN= (Self-Signed)

Certificate List

Subject
CN=

Veri. PSE Password

Trust Manager for Single Sign-On with Logon Ticket: Change



System PSE

System PSE

Own Certificate

Create PSE

Name

Org. (Opt)

Comp./Org.

Country

CA

Algorithm: RSA with SHA-1

Key Length: 1024

✓ ✎ ✕

Trust Manager for Single Sign-On with Logon Ticket: Change



System PSE

System PSE

Own Certificate

SSL Server

DN of Standard PSE: CN=

Instance-Specific PSEs

Host	Inst...	Status	Distinguished Name
	3	=	CN=
	3	=	CN=
	3	=	CN=
	2	=	CN=

Trust Manager for Single Sign-On with Logon Ticket: Change

68

The screenshot shows the 'Trust Manager for Single Sign-On with Logon Ticket: Change' window. On the left, a tree view lists various PSEs (Policy Security Engines) under 'System PSE'. The 'SSL client SSL Client (Anonymous)' PSE is selected, and a context menu is open over it with 'Create' and 'History' options. The main pane shows details for the selected PSE, including 'Own Certificate' and 'Certificate List'. The 'Subject' field for the certificate is 'CN= (Self-Signed)'. At the bottom, there are buttons for 'Veri. PSE' and 'Password'.

Trust Manager for Single Sign-On with Logon Ticket: Change

68

The screenshot shows the same 'Trust Manager' window, but with a 'Create PSE' dialog box open in the foreground. The dialog box has the following fields:

- DN: CN=anonymous
- Algorithm: RSA with SHA-1
- Key Length: 1024

At the bottom right of the dialog box are 'OK' (green checkmark) and 'Cancel' (red X) buttons. The background shows the same PSE list as the first screenshot, with 'SSL client SSL Client (Anonymous)' still selected.

Trust Manager for Single Sign-On with Logon Ticket: Change

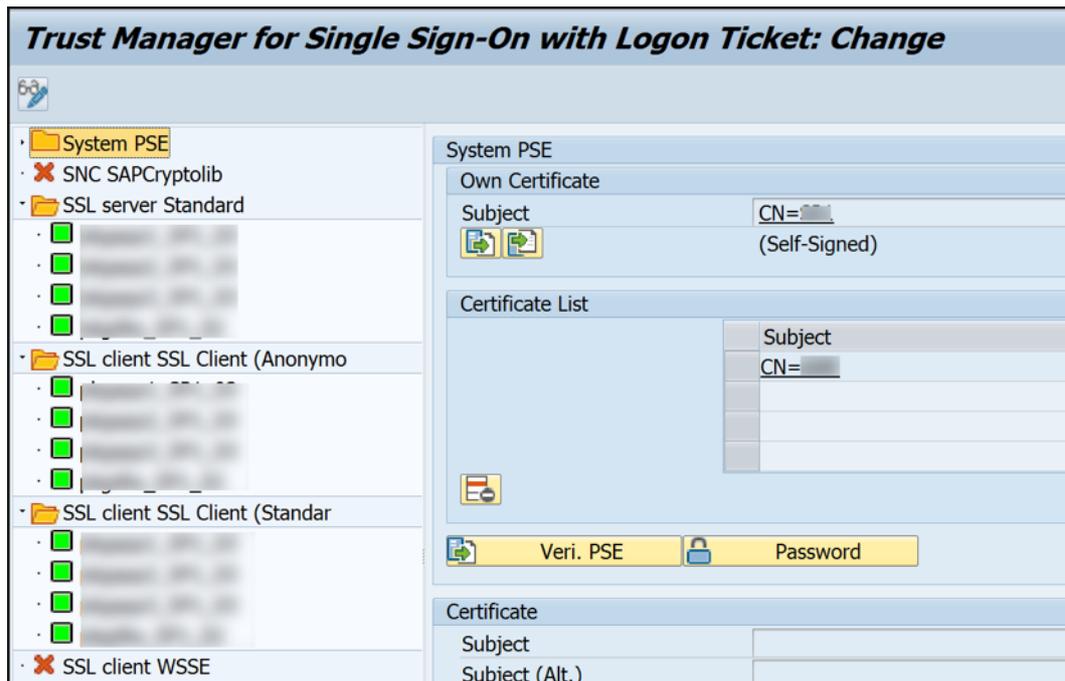
The screenshot shows the 'Trust Manager' interface. On the left, a tree view lists various PSEs (Policy Security Environments) under 'System PSE'. The 'SSL client SSL Client (Standard)' PSE is selected, and a context menu is open over it with 'Create' and 'History' options. The main pane shows the details for the selected PSE, including 'Own Certificate' and 'Certificate List' sections. The 'Subject' field for the certificate is 'CN=...' (Self-Signed). At the bottom, there are buttons for 'Veri. PSE' and 'Password'.

Trust Manager for Single Sign-On with Logon Ticket: Change

The screenshot shows the 'Trust Manager' interface with a 'Create PSE' dialog box open. The dialog box has the following fields and values:

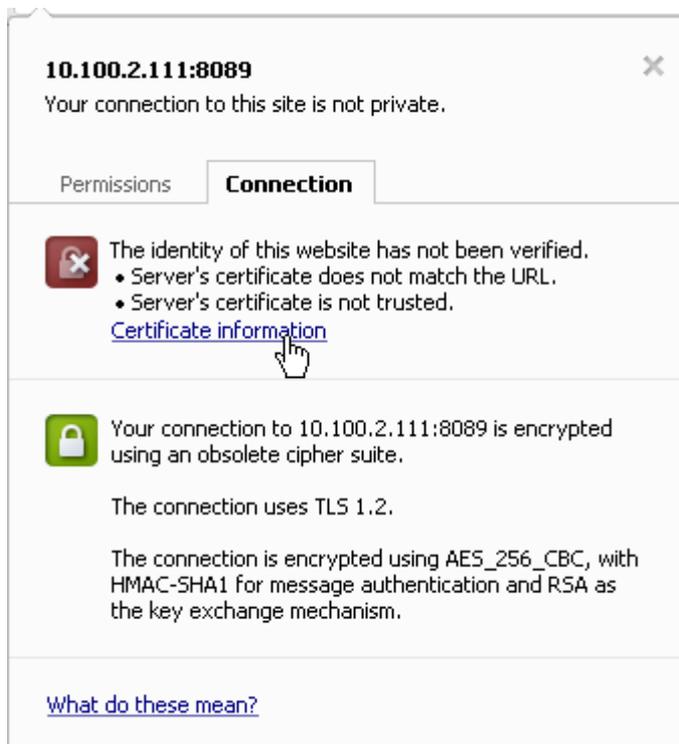
Field	Value
Name	SP1 SSL client SSL Client (Standard)
Org. (Opt)	
Comp./Org.	
Country	
CA	
Algorithm	RSA with SHA-1
Key Length	1024

The dialog box also has a 'Create PSE' button and a close button (X). At the bottom of the dialog, there are three buttons: a green checkmark, a blue pencil, and a red X. The background shows the same PSE list as the first screenshot, with 'SSL client SSL Client (Standard)' selected.

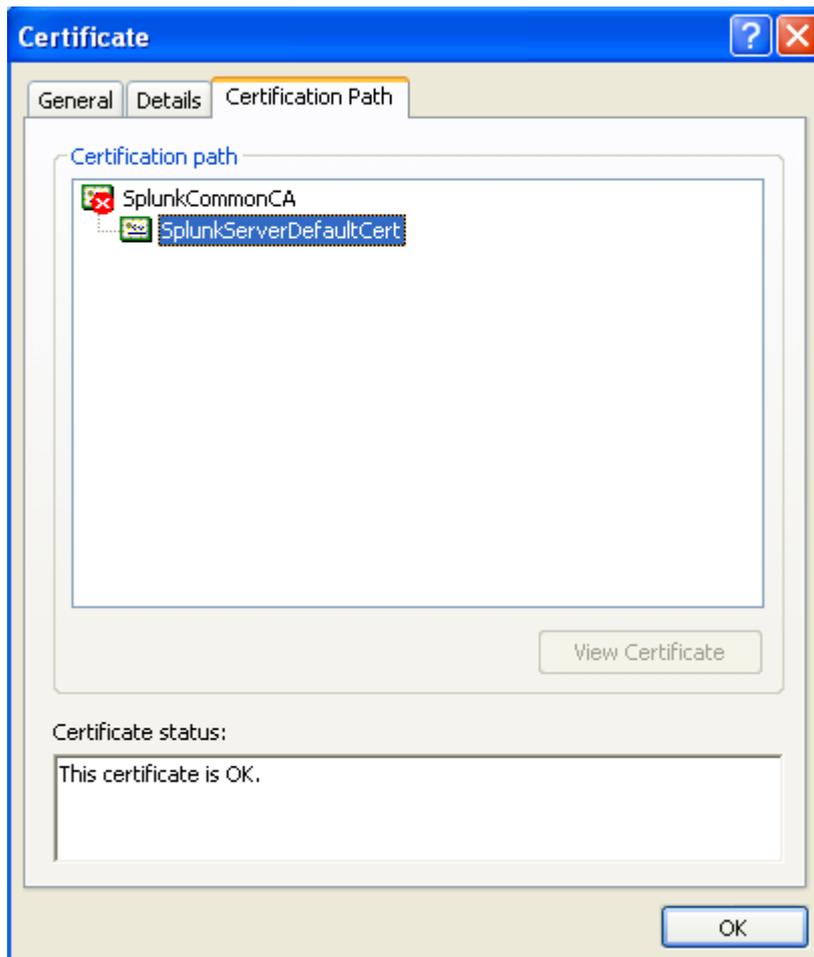


Next we need to ensure the ROOT CA (or server self-signed certificate is installed in the ABAP system)

Start by connecting to the Splunk server on port 8089 using HTTPS this will show you the certificate in use.



Open the **certificate information**



This certificate is signed by the SplunkCommonCA and we need to import this CommonCA certificate into SAP so it trusts the certificate being issued by the Splunk server.

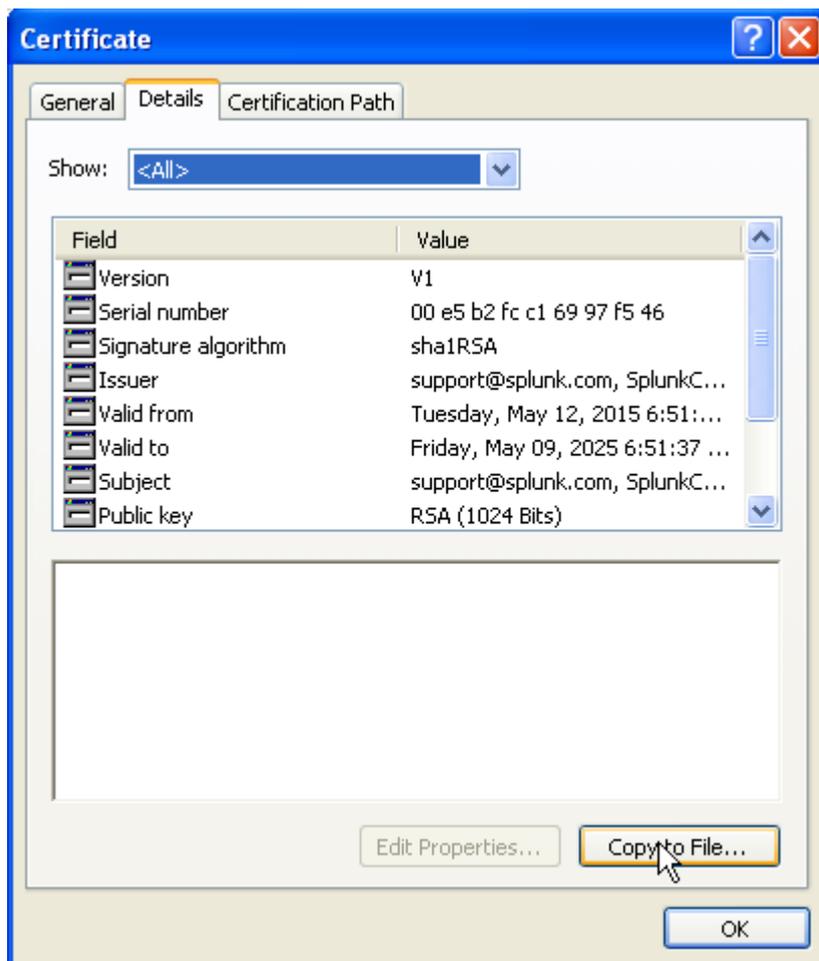
To do this highlight the **SplunkCommonCA** certificate and click **View Certificate**

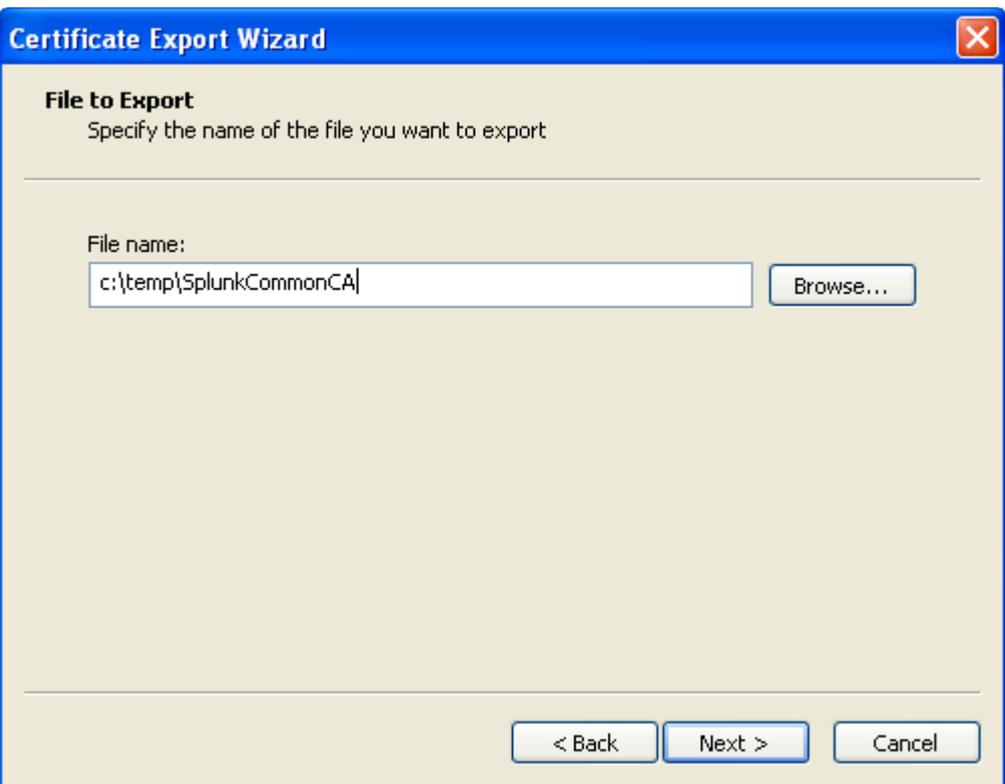


Not we are looking at the SplunkCommonCA certificate that is the issuer of the certificate being sent by Splunk. If we configure SAP to trust this certificate, then it will also trust the certificates it has issued which include the one being sent to SAP by the Splunk Server (SplunkServerDefaultCert).



Next click **Copy to file** to export this certificate







Now we need to import this certificate into SAP. Start tcode **STRUSTSSO2**. Highlight the hostname under node "SSL client SSL Client (Standard)".

Trust Manager for Single Sign-On with Logon Ticket: Change

System PSE

- ✗ SNC SAPCryptolib
- SSL server Standard
- SSL client SSL Client (Anonym...
- SSL client SSL Client (Standa
 - susehana1a_SH1_00
 - ✗ SSL client WSSE Web Service
 - ✗ WS Security Standard
 - ✗ WS Security Other System E
 - ✗ WS Security WS Security Ke
 - ✗ SMIME Standard
 - File
 - ✗ SSF Collaboration Integration

SSL client SSL Client (Standar

Own Certificate

Subject: CN=SH1 SSL client SSL Client (Standard), OU=I0090139180, OU=SAP W...
(Self-Signed)

Certificate List

Subject

Veri. PSE Password

Certificate

Subject:

Subject (Alt.):

Issuer:

Serial Number (Hex.):

Serial Number (Dec.):

Valid From: to

Algorithm: Key Length:

Check Sum (MD5):

Checksum (SHA1):

Add to Certificate List Add to ACL

Click on the import button  in the certificate section

Certificate

Subject:

Subject (Alt.):

Issuer:

Serial Number (Hex.):

Serial Number (Dec.):

Valid From: to

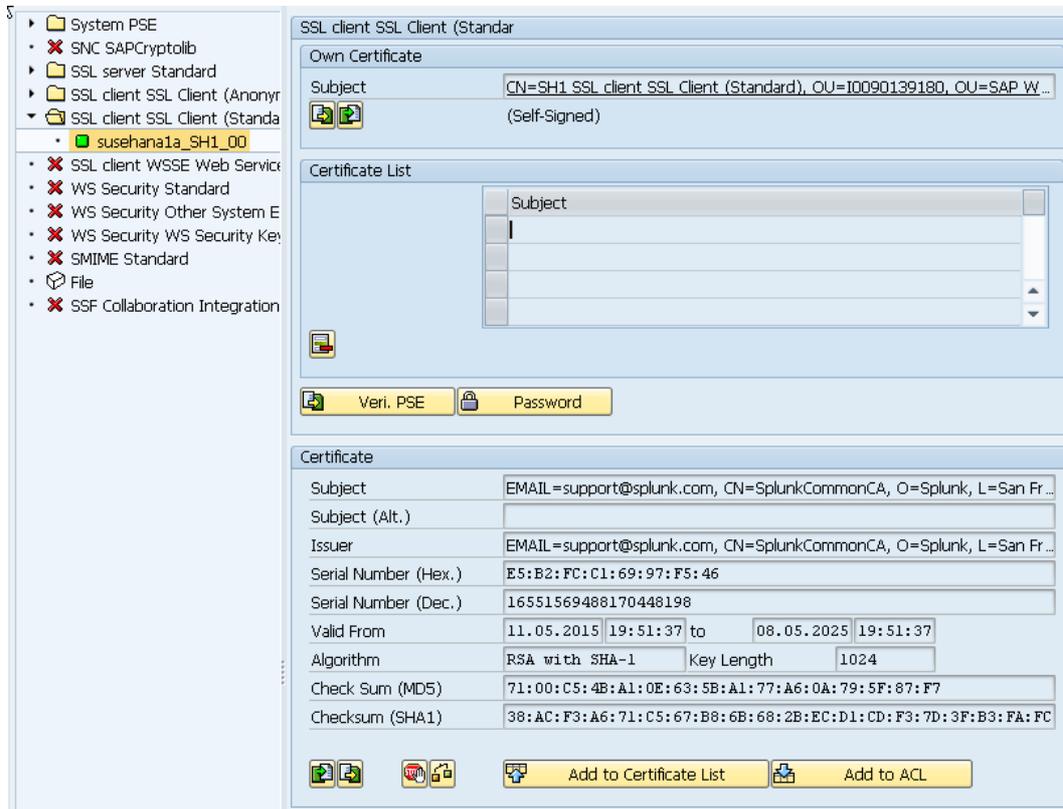
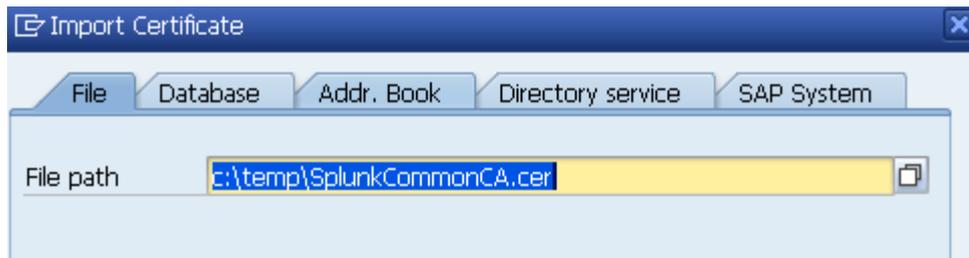
Algorithm: Key Length:

Check Sum (MD5):

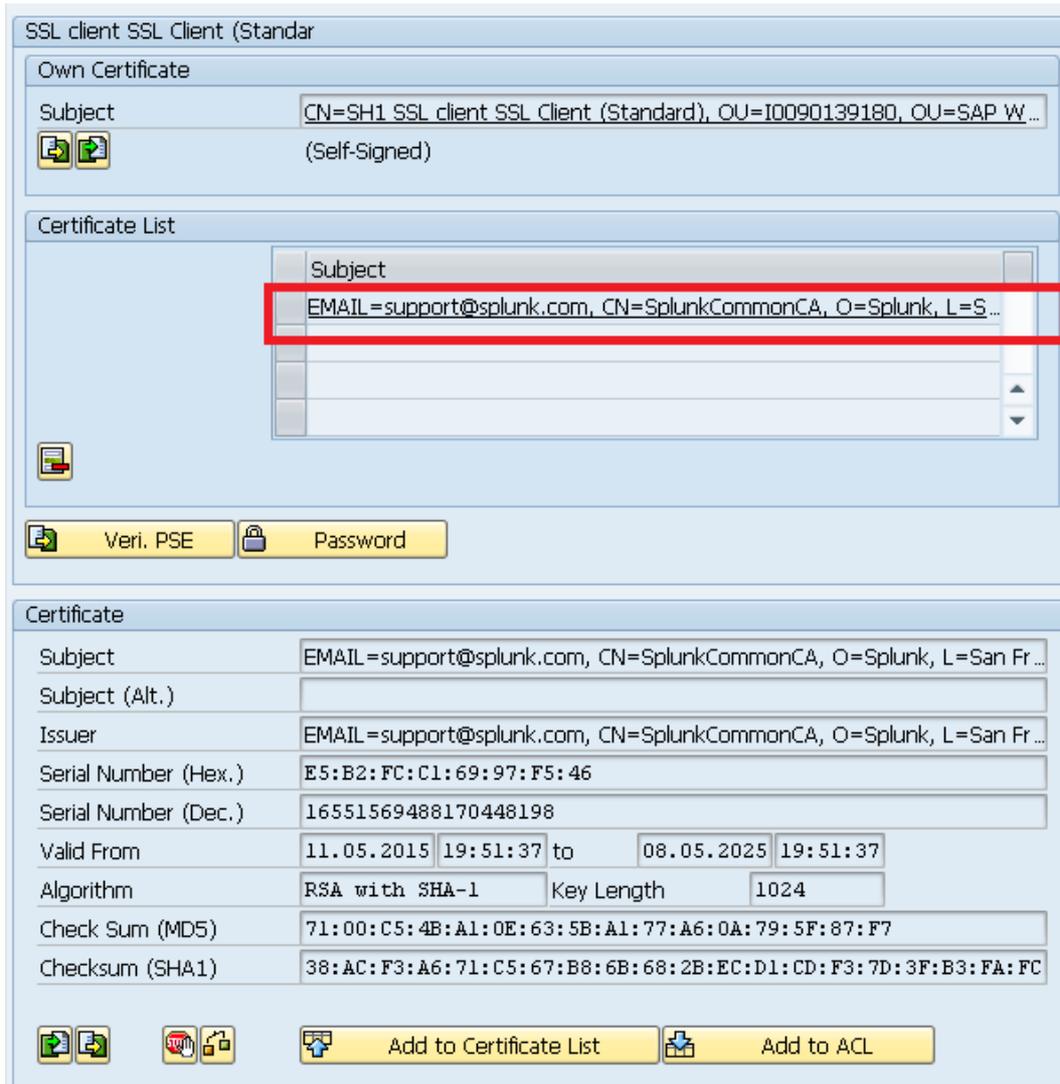
Checksum (SHA1):

 Add to Certificate List Add to ACL

Now enter the file path of the SplunkCommonCertificate saved in the previous step



Now the SplunkCommonCA certificate appears in the **Certificate** section, click on the **Add to Certificate List** button to add it to the **Certificate List**



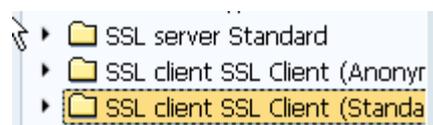
Click **Save** in the toolbar to save this change



Repeat this change for the following 2 nodes

SSL server Standard

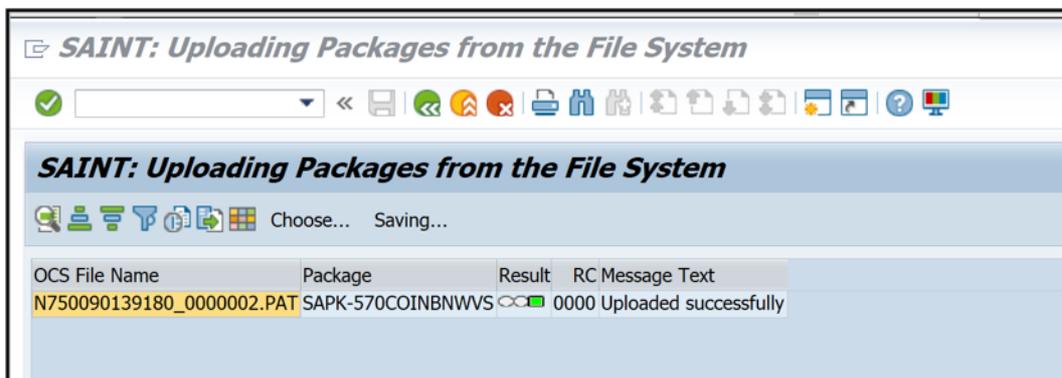
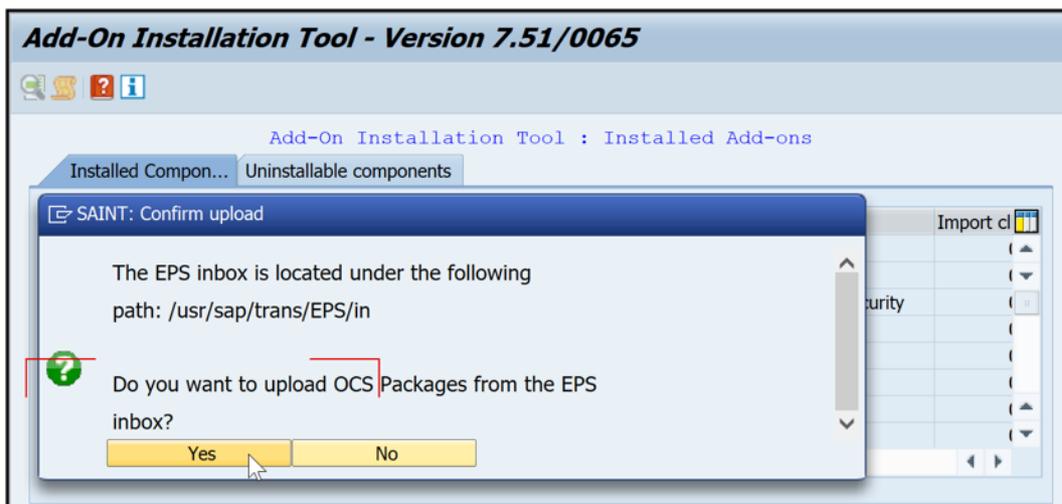
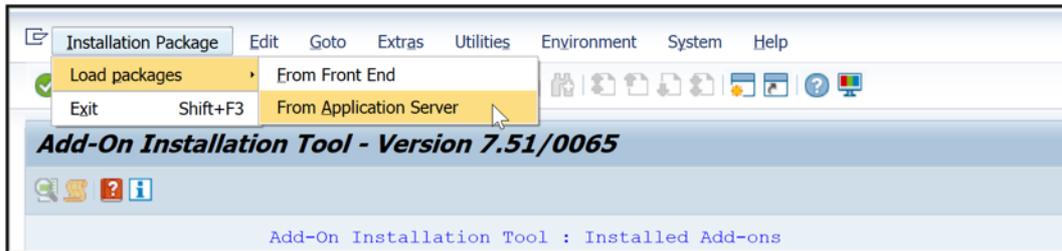
SSL client SSL Client (Anonymous)



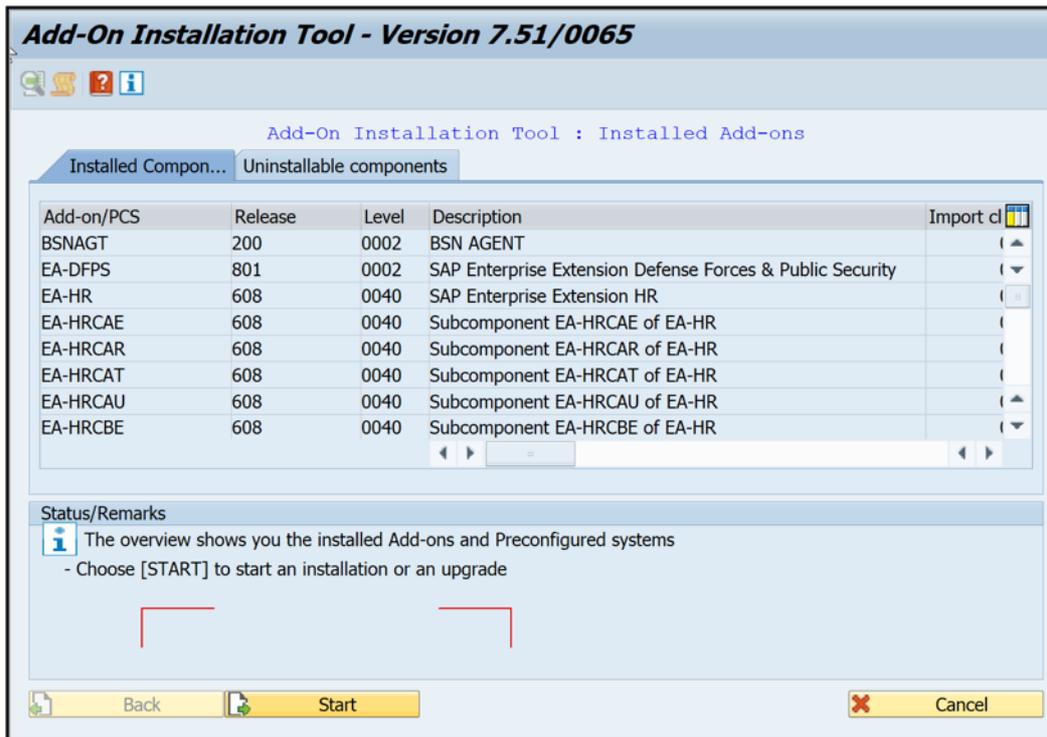
SAINT

Ensure Installation and Support Packages are unpacked into \usr\sap\trans\EPS\in directory

Client 000 → Transaction Saint



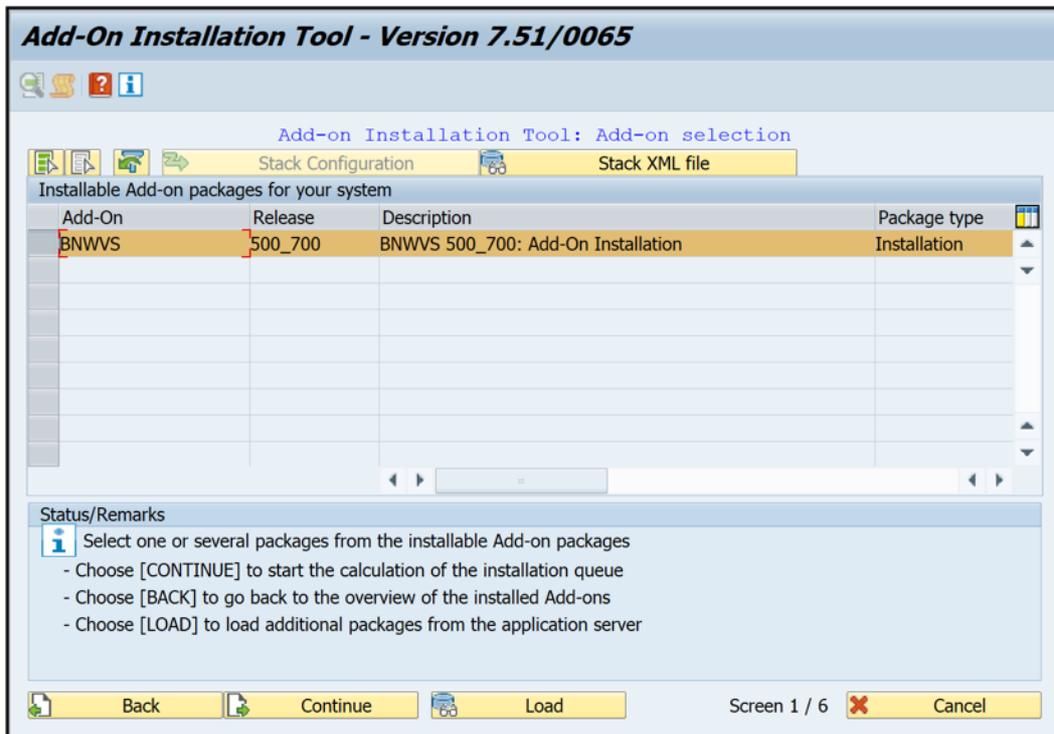
Install add-on



From the main screen in transaction SAINT select “Start”



Highlight the PowerConnect Add-on



Select “Continue”



Add-On Installation Tool - Version 7.51/0065

Installation of several Add-ons : Support Package selection

Installation qu... Support Package select...

Software Comp.	Target Support Package	Level	Calculated Package	Level
BNWVS			SAPK-570COINBNWVS	0000
SAP_BASIS				
SAP_ABA				
SAP_GWFND				
SAP_UI				
ST-PI				
SAP_BW				
GRCFND_A				

Status/Remarks

i You can extend the installation queue with further Support Packages

- Choose the required target Support Package for each component
- Choose [CONTINUE] to start the calculation of the extended installation queue
- Choose [BACK] to go back to the Add-on selection
- The tab page "Installation queue" displays the preliminary installation queue

Back Continue Logs Screen 2 / 6 Cancel

Select "Continue"



You will then see a list all packages being installed.

Add-On Installation Tool - Version 7.51/0065

Installation of several Add-ons : Calculated queue

Installation qu... Software Components

OCS packages for import				
OCS Package	Package type	Software Component	Release	Short description
SAPK-570COINBNWVS	Installation	BNWVS	500_700	BNWVS 500_700

Status/Remarks

i The displayed packages must be imported when installing the Add-on

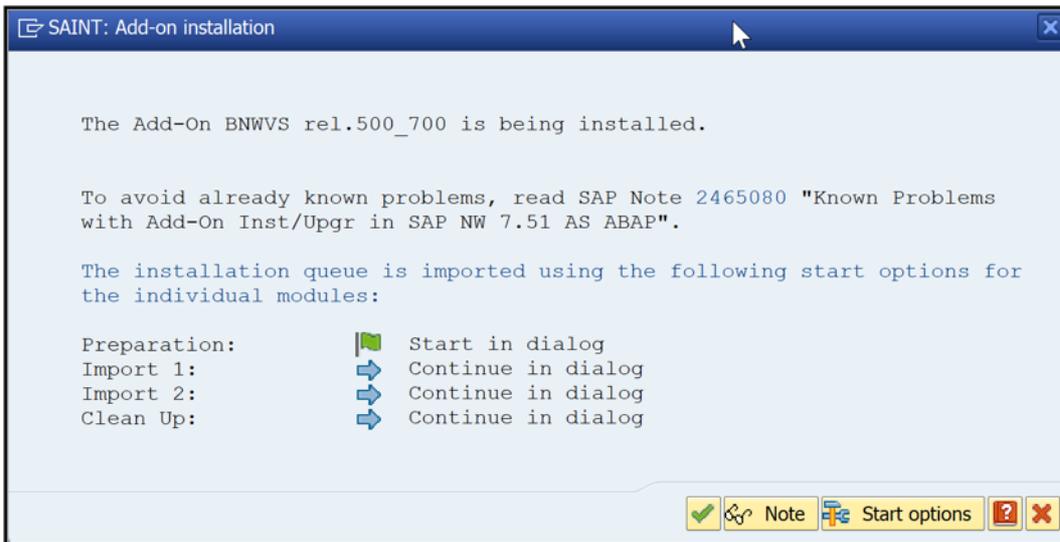
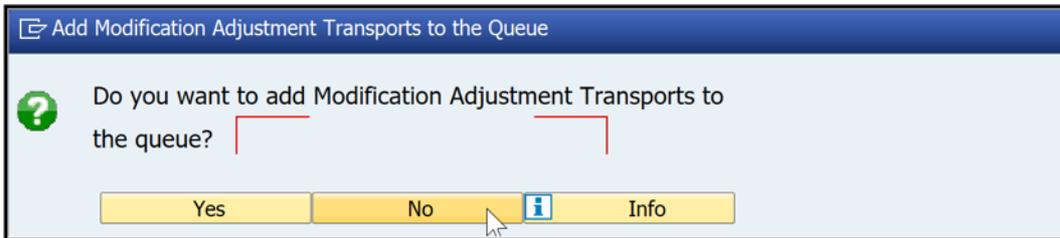
- You have not selected any further Support Packages
- Choose [CONTINUE] to add Modification Adjustment Transports to the queue
- Choose [BACK] to go back to the Support Package selection

Back Continue Logs Screen 3 / 6 Cancel

Select "Continue"



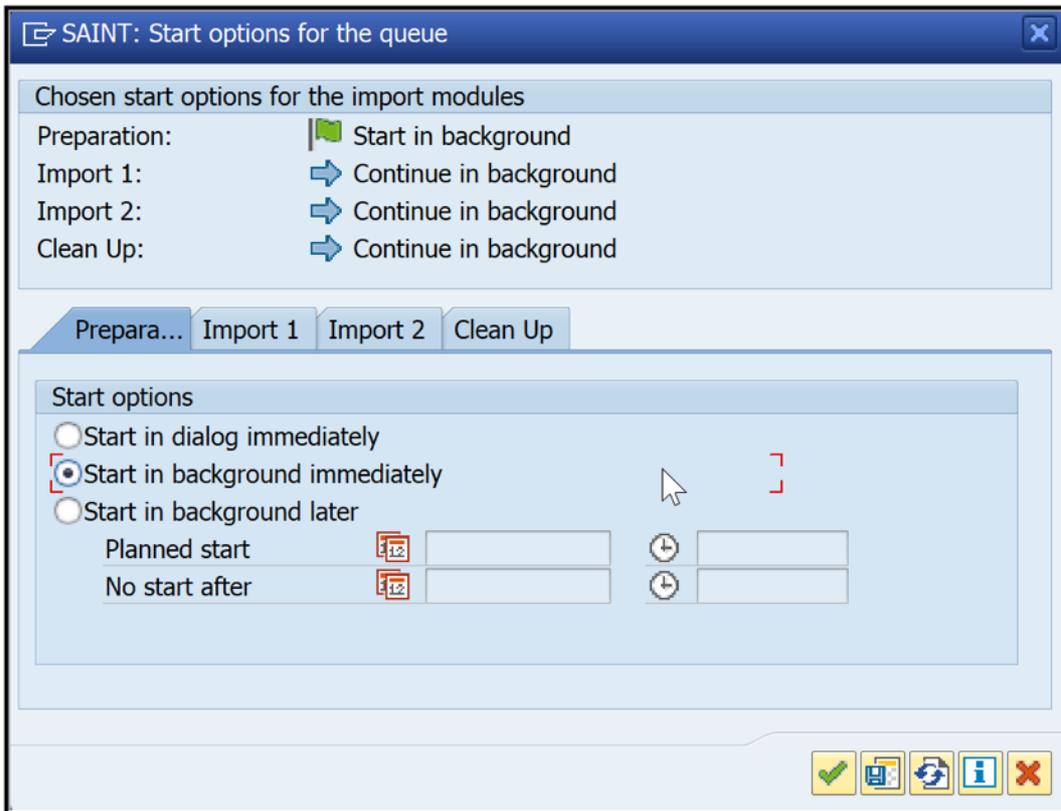
Select "No" for Modification Adjustment transport



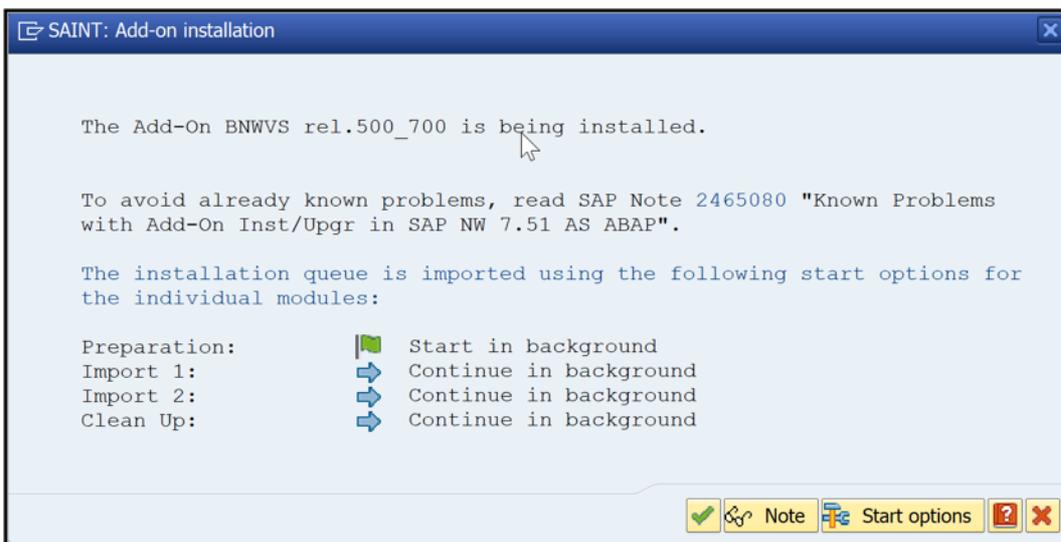
Select the "Start Options" button"



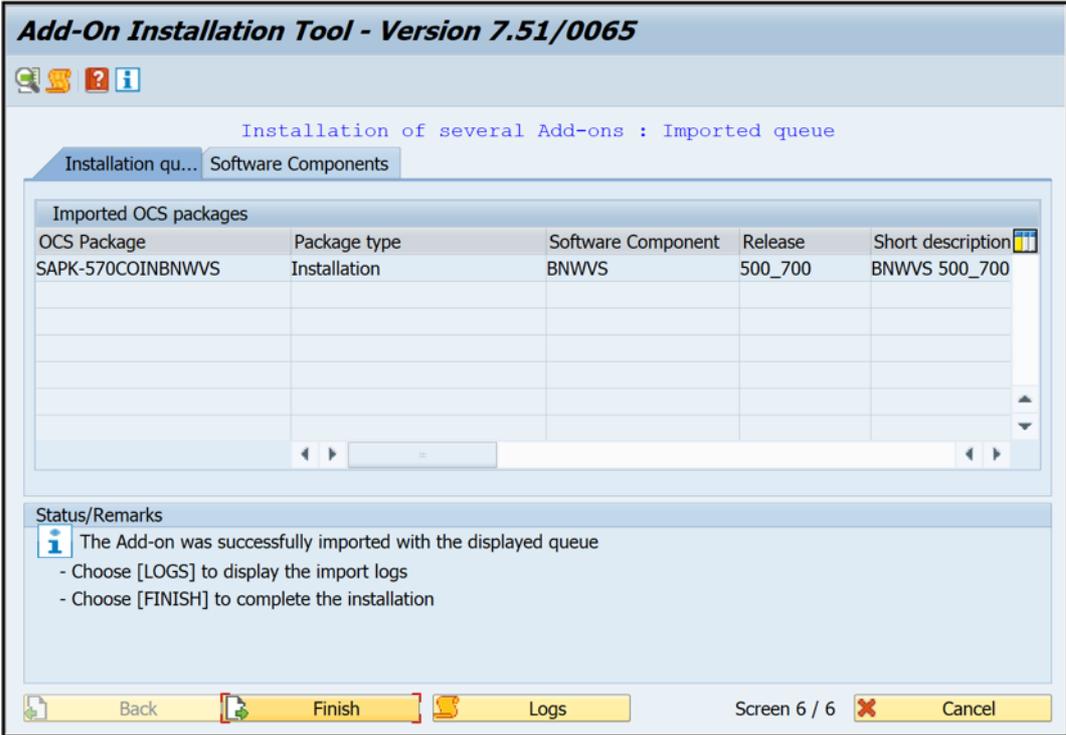
Change to start in background



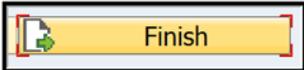
Select the "tick" to continue



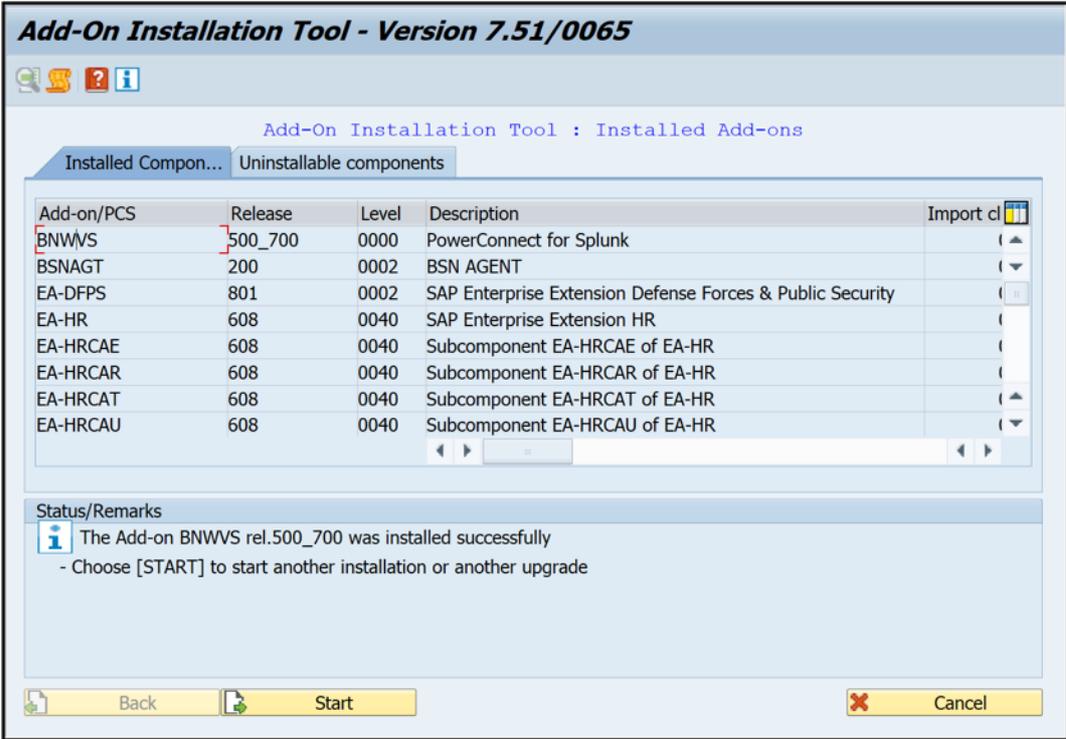
Select the "tick" to start installation



Once installation is complete select “Finish”



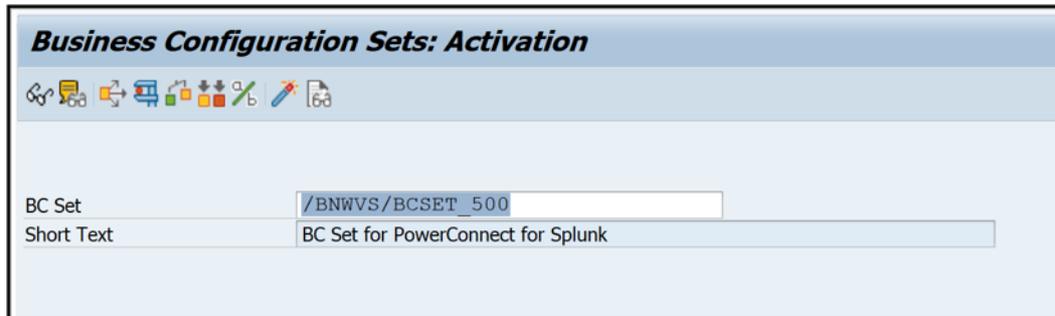
The “BNWVS” add-on will now appear in installed add-on list



Activate BC Sets

Go to transaction SCCR20

In the BC Sets Field enter “\BNWVS\BCSET_500”



Business Configuration Sets: Activation

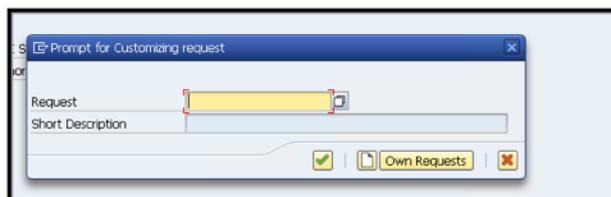
BC Set: /BNWVS/BCSET_500

Short Text: BC Set for PowerConnect for Splunk

BC Set → Activate



Create a transport for the BC Set activation - This transport will be imported into subsequent systems rather than running this transaction again.

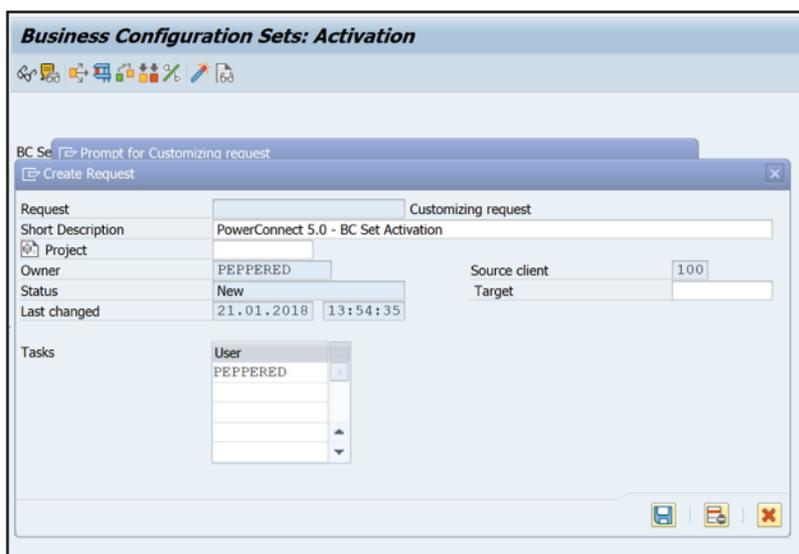


Prompt for Customizing request

Request: [Yellow highlight]

Short Description:

Own Requests



Business Configuration Sets: Activation

BC Set Prompt for Customizing request

Create Request

Request: Customizing request

Short Description: PowerConnect 5.0 - BC Set Activation

Project:

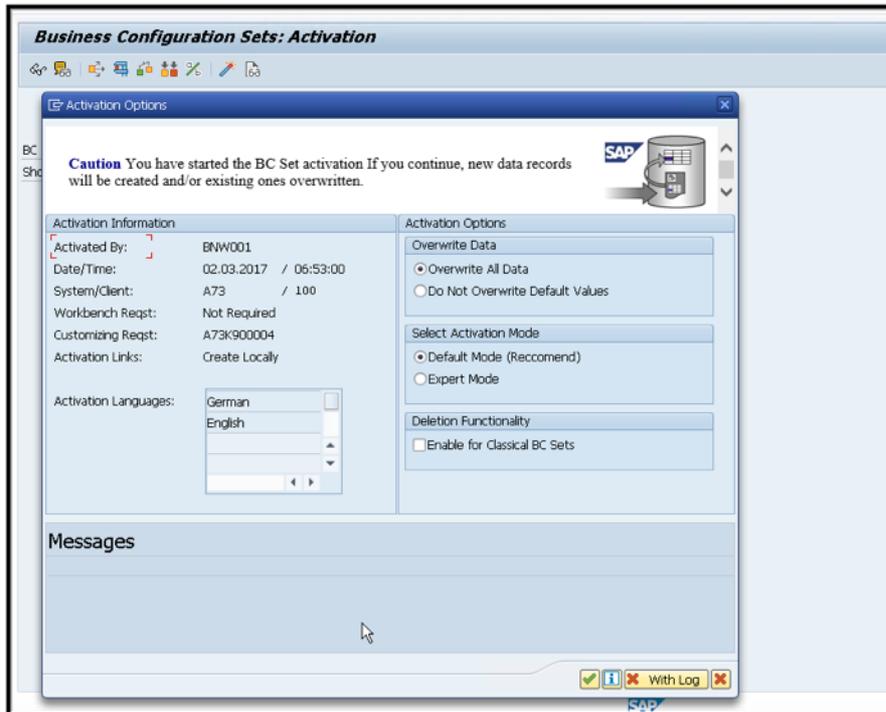
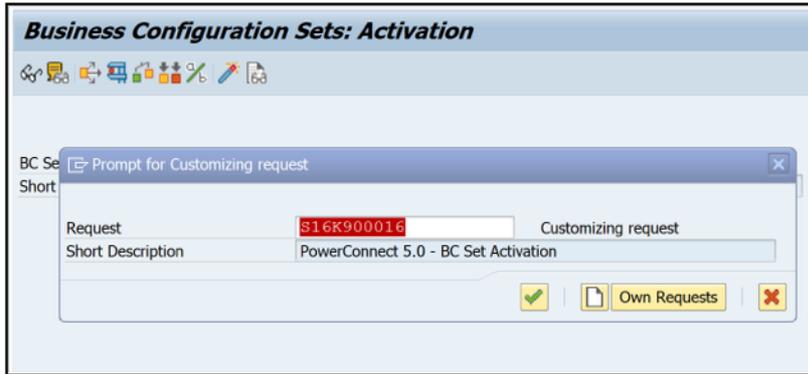
Owner: PEPPERED Source client: 100

Status: New Target:

Last changed: 21.01.2018 13:54:35

Tasks:

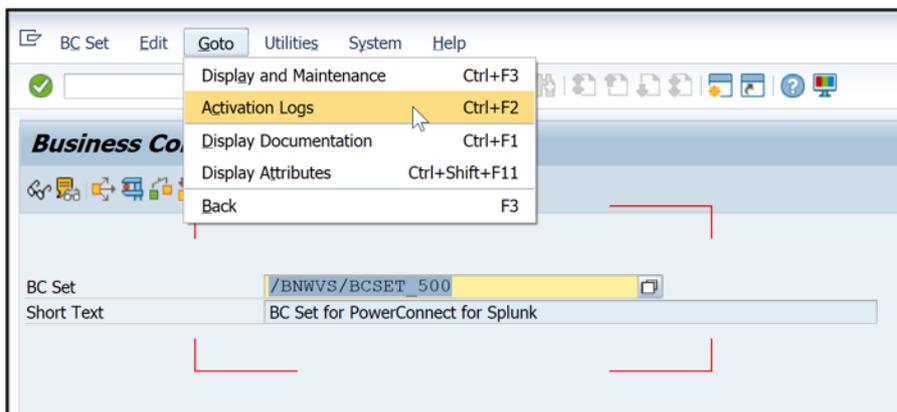
User
PEPPERED



The follow line will appear at the bottom of screen on complete.



To confirm successful activation view the logs by going to Goto → Activation Logs



Business Configuration Sets: Activation Logs

18.01.2018 um 11:10:07

Activation ... Activation Information

- /BNWVS/BCSET_500
 - /BNWVS/CFG
 - /BNWVS/CHG_LOG
 - /BNWVS/GRP_DEF
 - /BNWVS/LOGS_CFG
 - /BNWVS/STC_EXT
 - /BNWVS/TASK_GRP
 - /BNWVS/UP
 - /BNWVS/UP_CFG

Maintain BC Sets BC Set Overall View 17 14 0 0

Type	BC Sets	Object	Message Text	Key Field	Infor
	/BNWVS/BCSET_500		Main Activation Started		
	/BNWVS/BCSET_500		BC Set /BNWVS/BCSET_500 passed to activate		
	/BNWVS/BCSET_500	/BNWVS	Customizing object /BNWVS/CFG passed to activation		
	/BNWVS/BCSET_500	/BNWVS	Customizing object /BNWVS/CHG_LOG passed to activation		
	/BNWVS/BCSET_500	/BNWVS	Customizing object /BNWVS/GRP_DEF passed to activation		
	/BNWVS/BCSET_500	/BNWVS	Customizing object /BNWVS/LOGS_CFG passed to activation		
	/BNWVS/BCSET_500	/BNWVS	Customizing object /BNWVS/STC_EXT passed to activation		
	/BNWVS/BCSET_500	/BNWVS	Customizing object /BNWVS/TASK_GRP passed to activation		
	/BNWVS/BCSET_500	/BNWVS	Customizing object /BNWVS/UP passed to activation		
	/BNWVS/BCSET_500	/BNWVS	Customizing object /BNWVS/UP_CFG passed to activation		
	/BNWVS/BCSET_500	/BNWVS	Table /BNWVS/CFG assigned to customizing object /BNWVS/CFG		
	/BNWVS/BCSET_500	/BNWVS	Table /BNWVS/CHG_LOG assigned to customizing object /BNWVS/CHG_LOG		
	/BNWVS/BCSET_500	/BNWVS	Table /BNWVS/GRP_DEF assigned to customizing object /BNWVS/GRP_DEF		
	/BNWVS/BCSET_500	/BNWVS	Table /BNWVS/LOGS_CFG assigned to customizing object /BNWVS/LOGS_CFG		
	/BNWVS/BCSET_500	/BNWVS	Table /BNWVS/STC_EXT assigned to customizing object /BNWVS/STC_EXT		

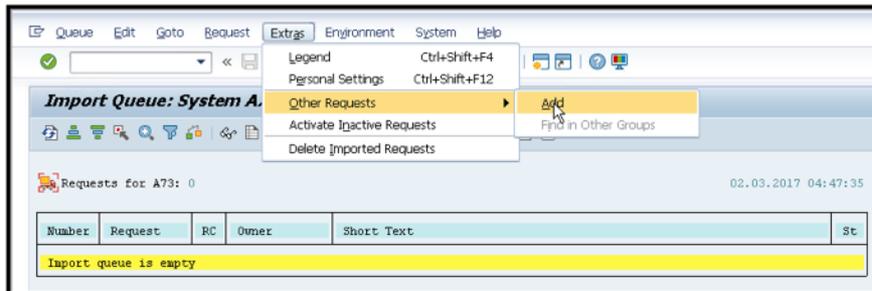
Upload Roles

Add Transport to buffer

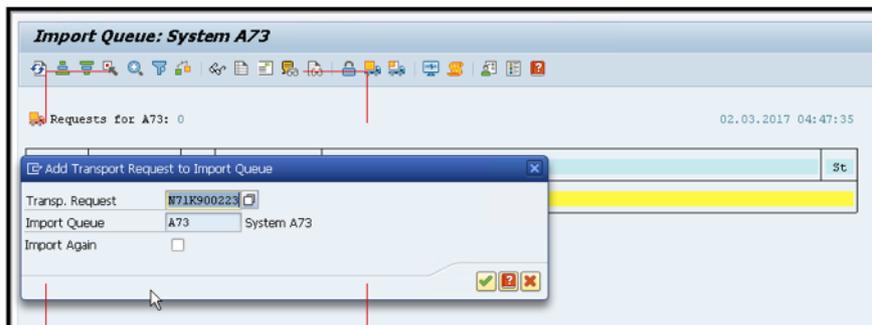
Ensure transport files are loaded into the `usr\sap\trans\cfiles` and `\usr\sap\trans\data` directories.

Transaction STMS

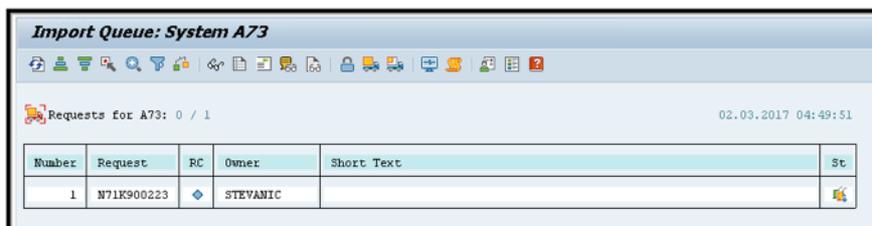
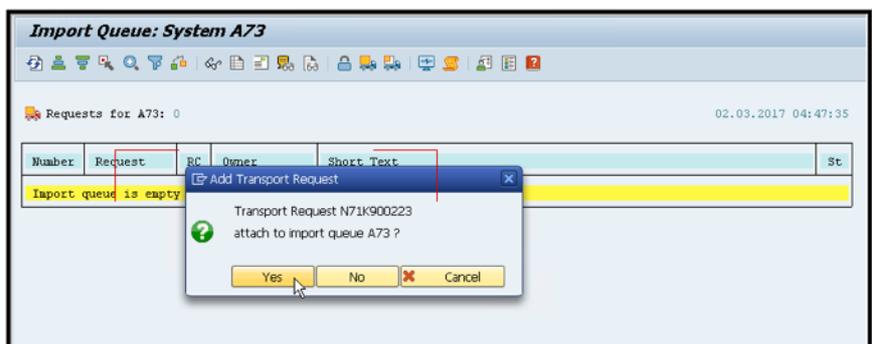
From the buffer of the system select Extras → Other Requests → Add



Select transport “N71K900223”



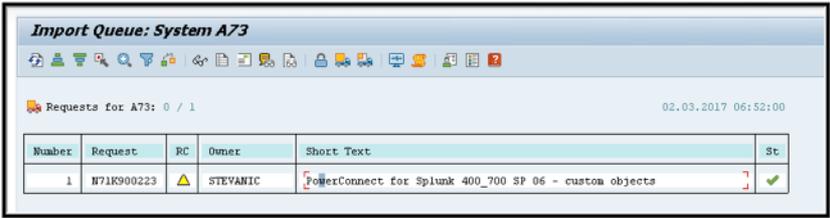
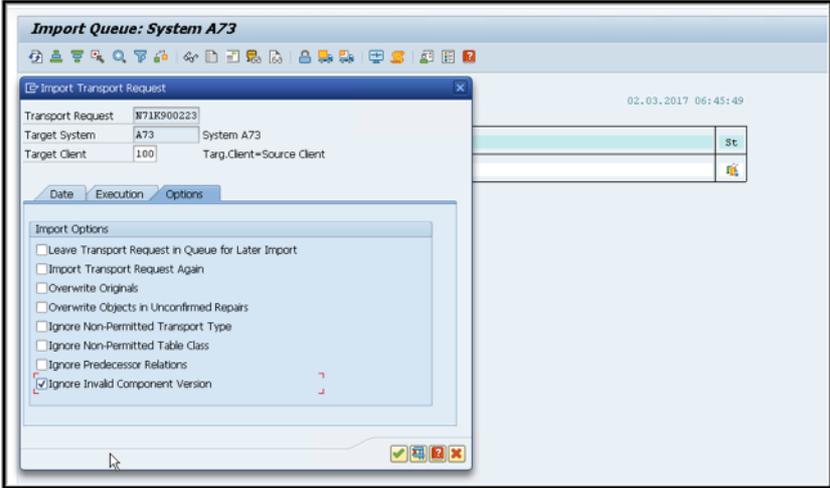
Select the “tick” and then “yes” to add to buffer



Select transport with the mouse and then from menu select Request → Import

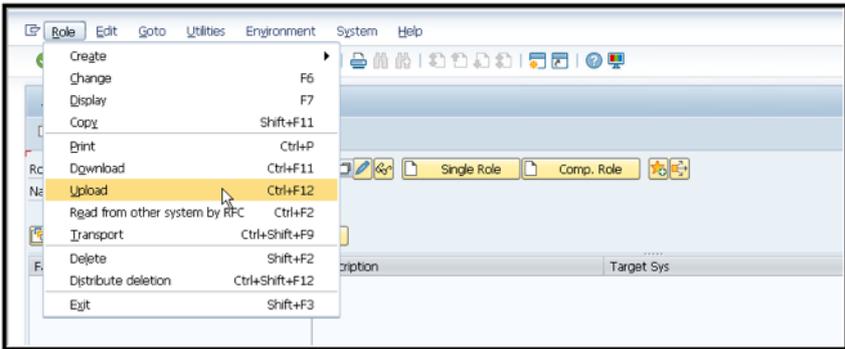


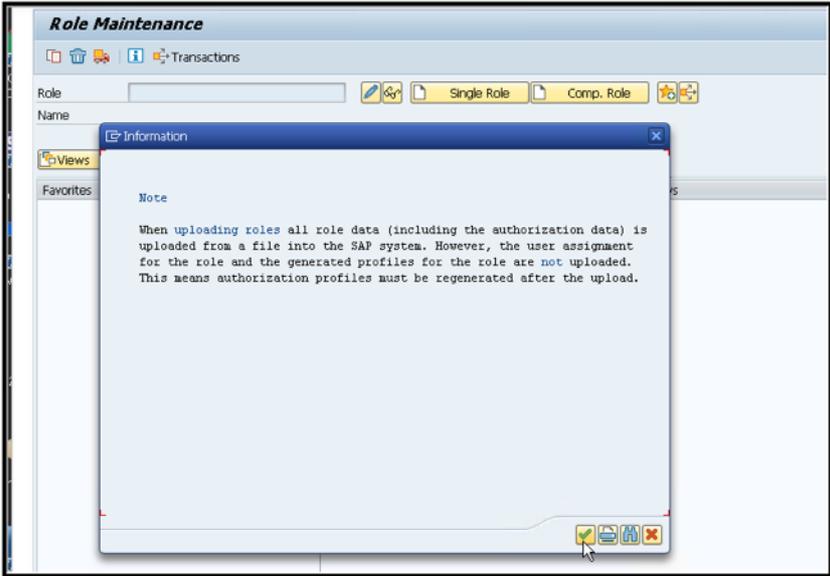
Ensure "Ignore Invalid Component Version" is selected.



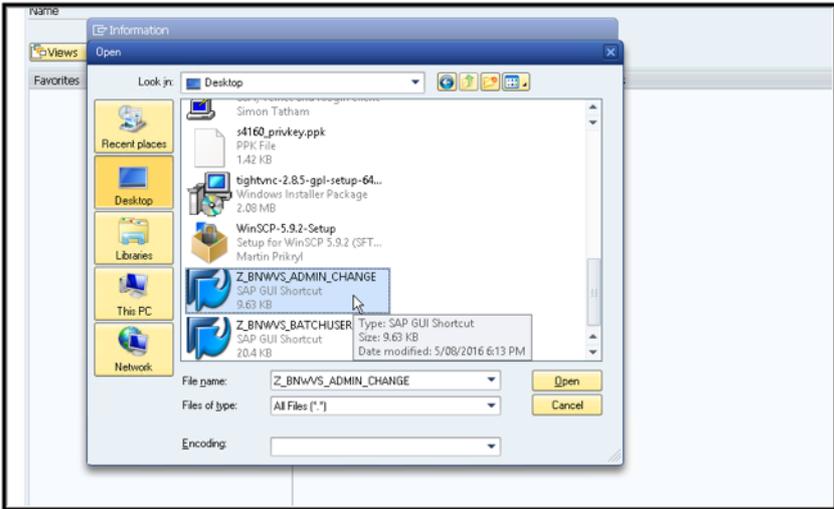
Upload PowerConnect Roles Transaction PFCG

From menu Role → Upload

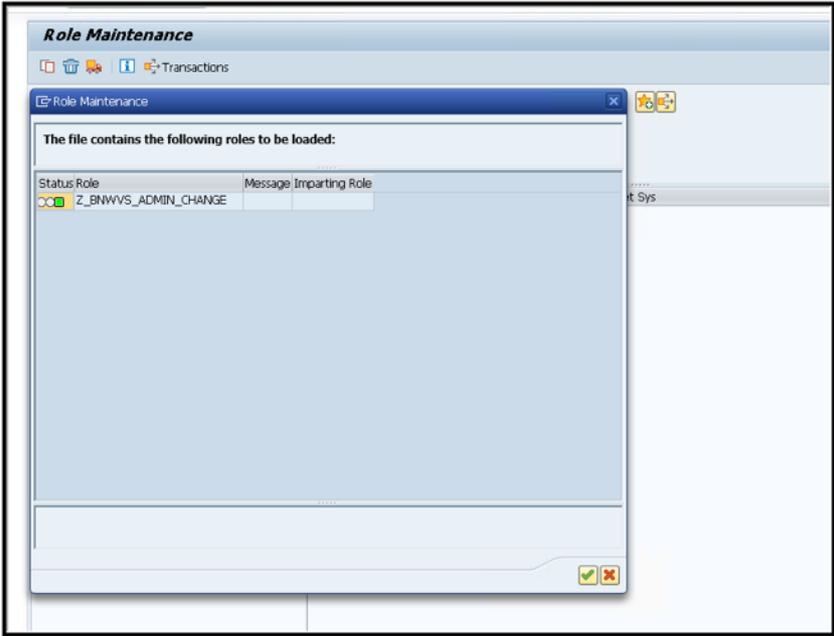




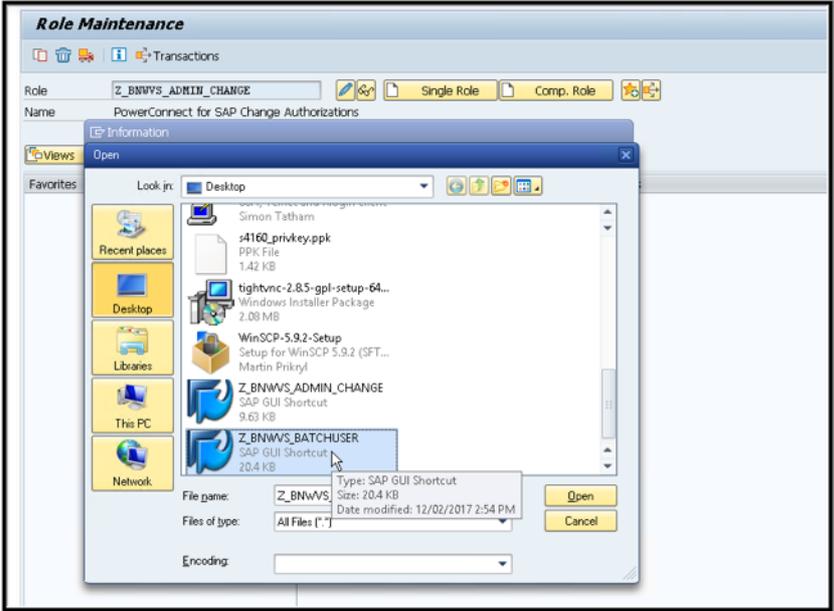
Navigate to the directory where you have saved the roles and select one.

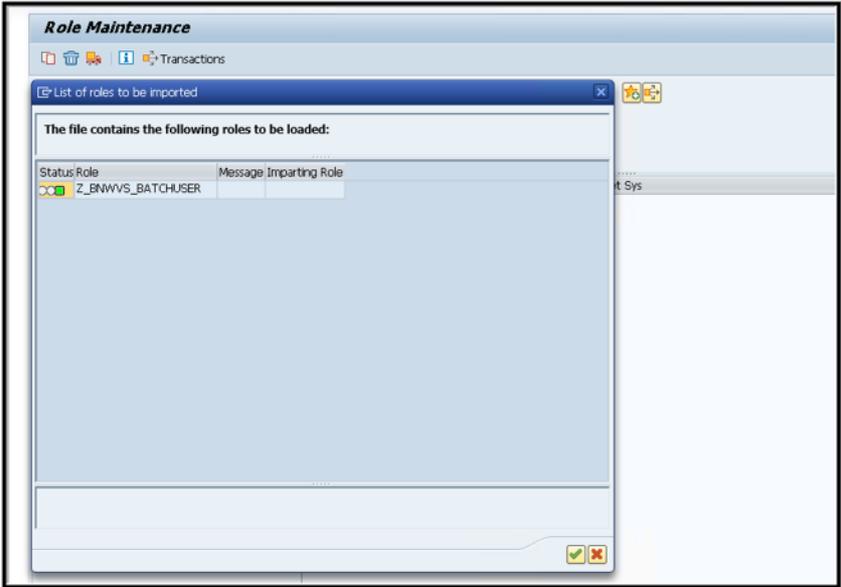


Confirm the import.



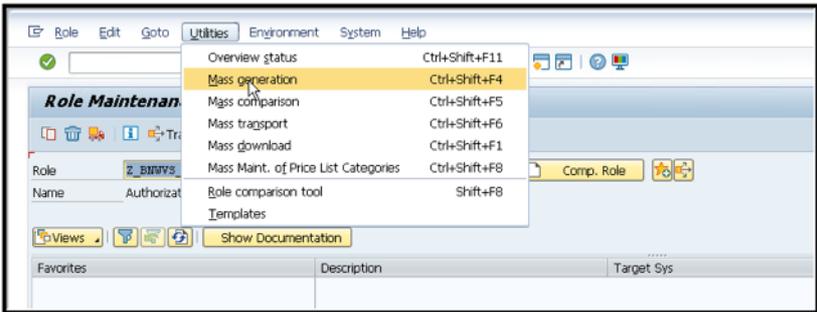
Carry out the same procedure for the other role.



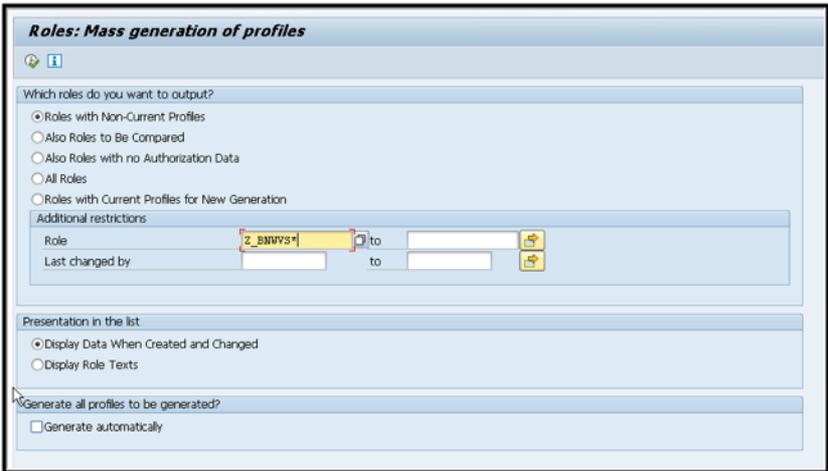


Generation Roles

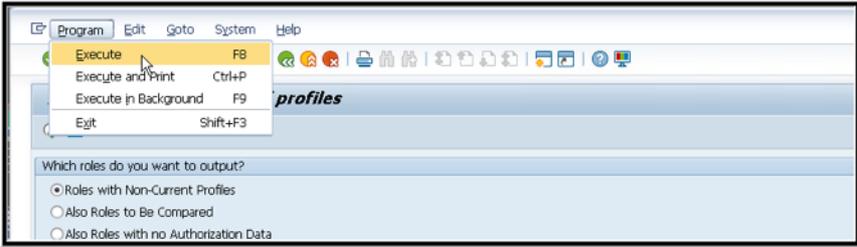
From menu select Utilities → Mass generation



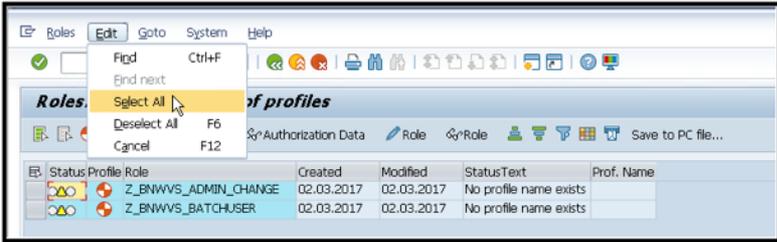
In the role field enter "Z_BNWWVS**"



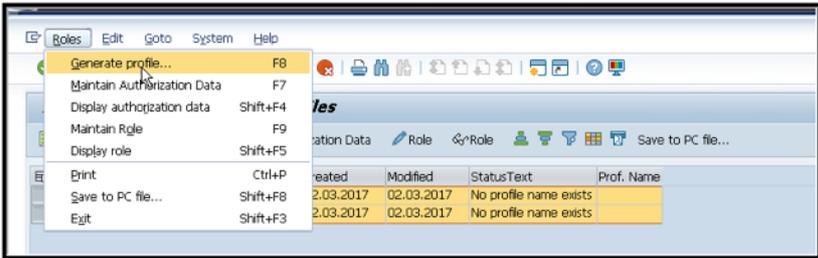
Select Program → Execute



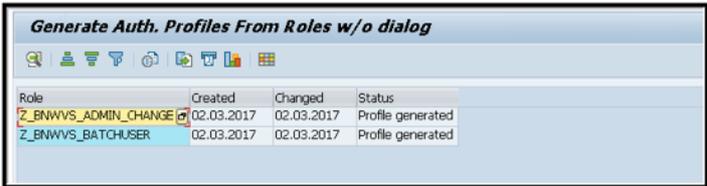
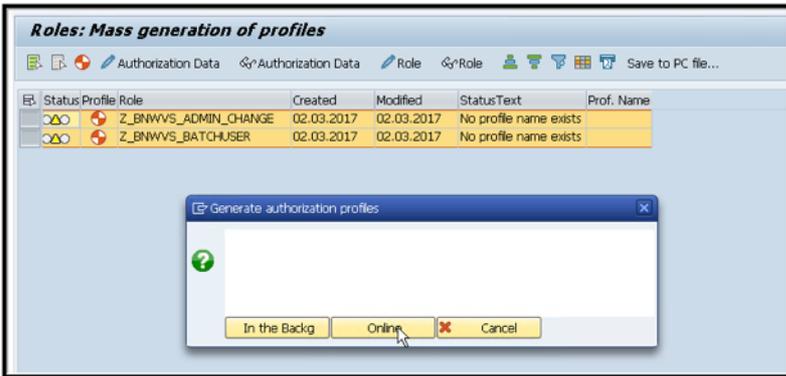
Edit → Select All



Roles → Generate profile



Select "online"



Leave transaction

Status	Prof. Role	Created	Modified	StatusText	Prof. Na...
	Z_BNWVS_ADMIN_CHANGE	02.03.2017	02.03.2017	Profile generated	T-N1070...
	Z_BNWVS_BATCHUSER	02.03.2017	02.03.2017	Profile generated	T-B1690...

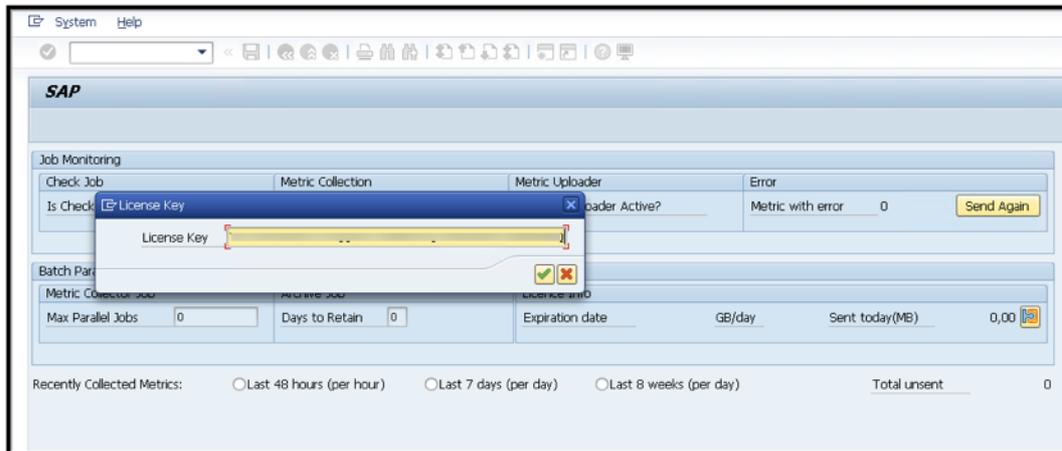
Assign Roles

Assign role Z_BNWVS_ADMIN_CHANGE to user who will administer PowerConnect and Z_BNWVS_BATCHUSER to user that will run the PowerConnect batch jobs.

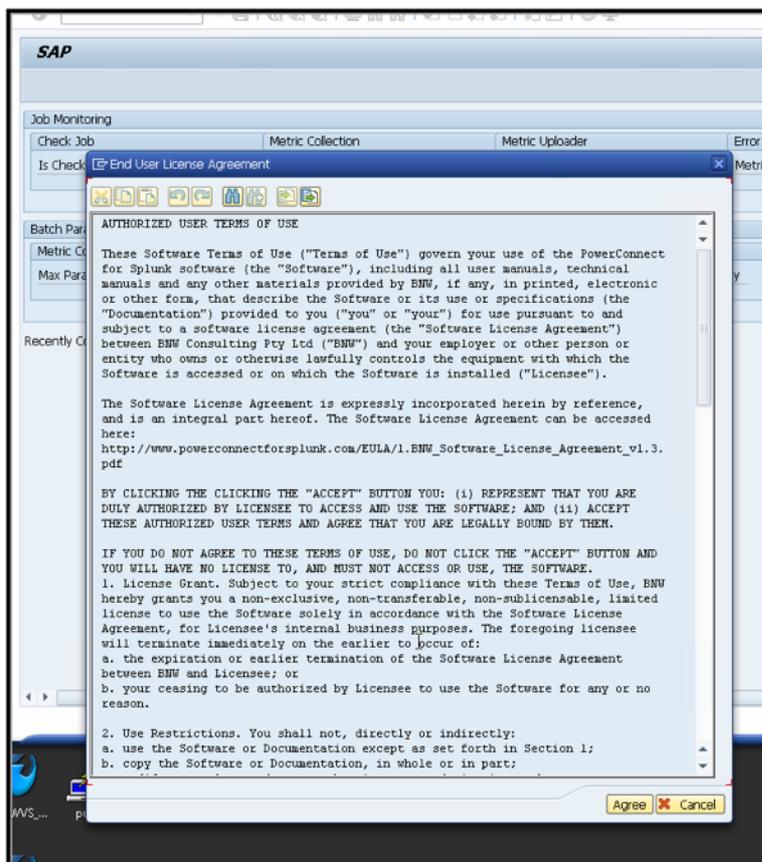
Activate PowerConnect

Transaction /n/bnwvs/main

Enter your PowerConnect license



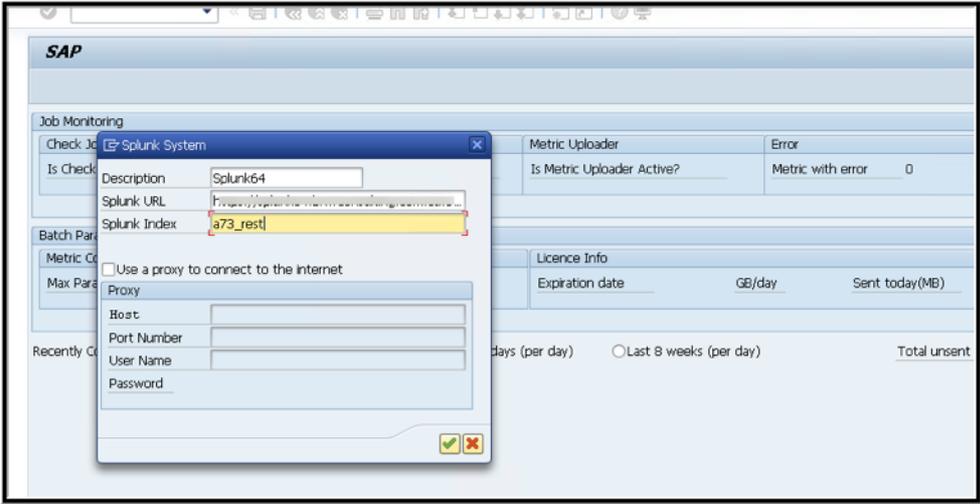
Accept the user terms



Configure Splunk Connection

Enter Splunk Connection details

Enter either the hostname and port to the REST or HEC port and the target index

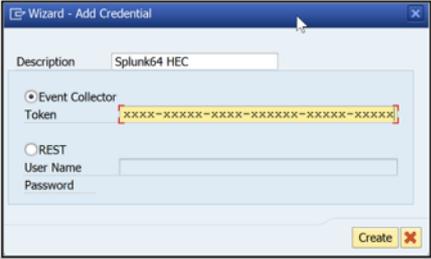


Enter Credentials

One of the two credential methods can be used, but we do recommend using HEC keys.

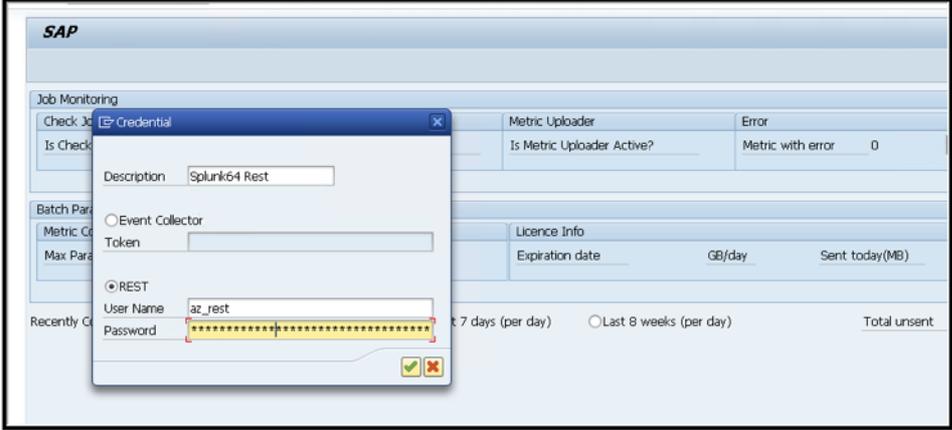
Enter HEC key

If using HEC select the “Event Collector” Radio button and enter the Token associated with your index.



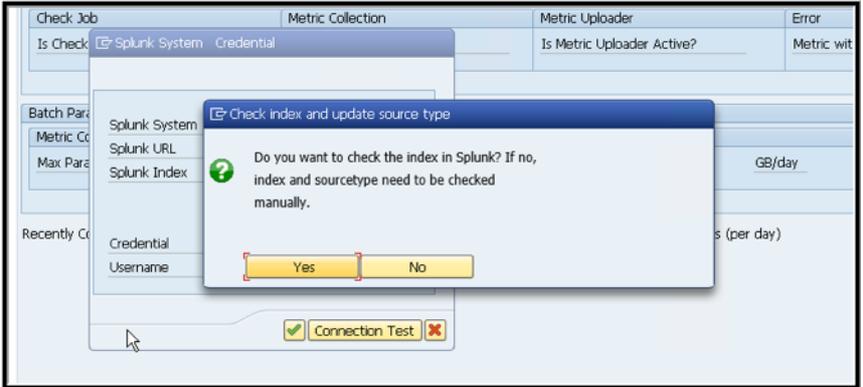
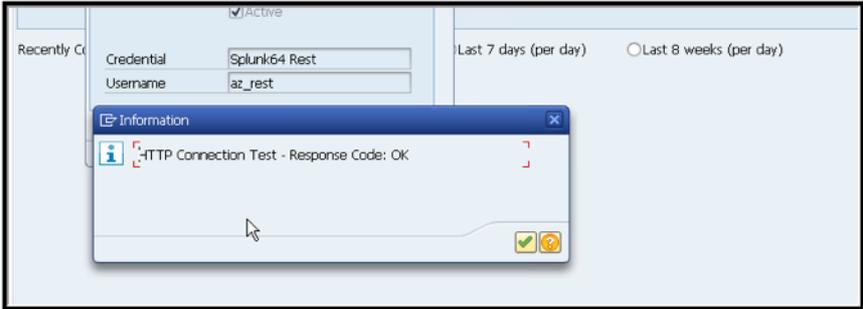
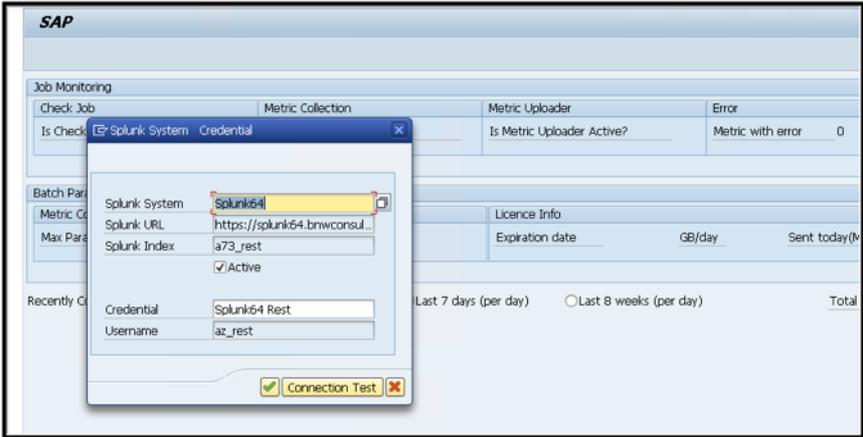
Enter REST user details

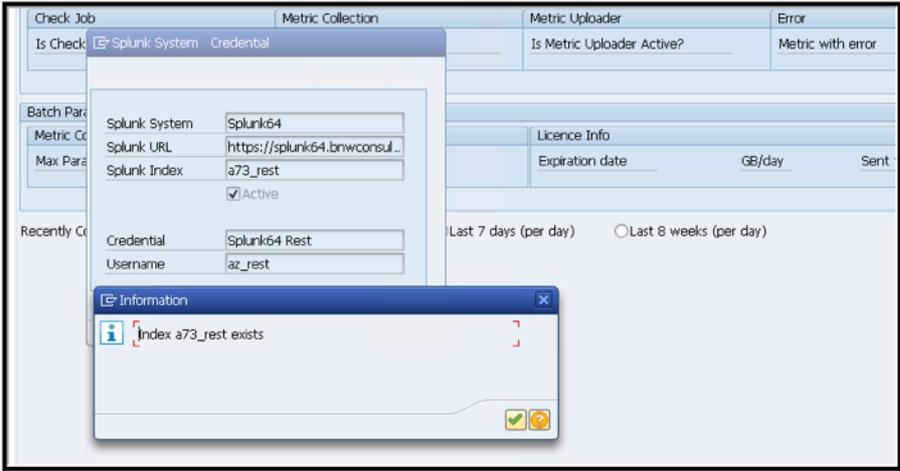
If using REST select the “REST” radio button - specify username and password



Connection Test

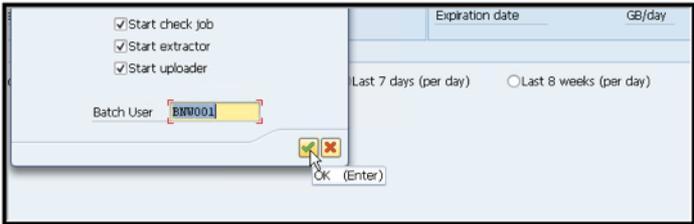
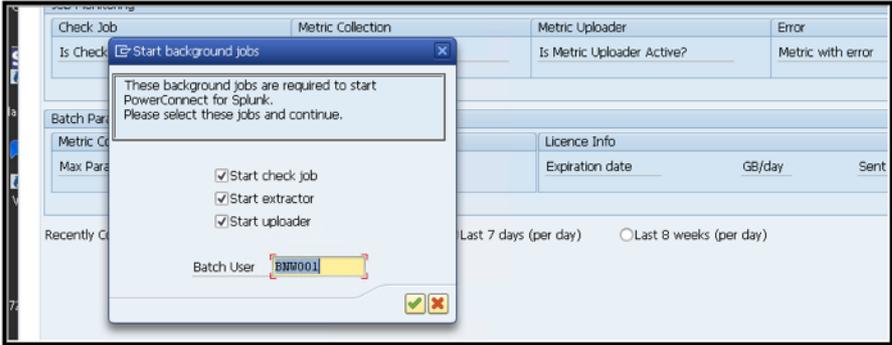
On the next screen you can carry out a connection test to confirm SAP can access Splunk and the index exists.





Start Batch jobs

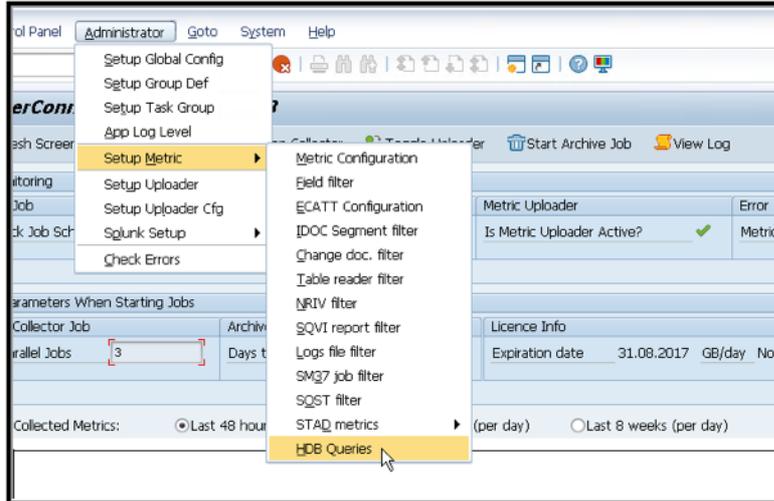
In the “Batch User” field enter the name of your background user and confirm.



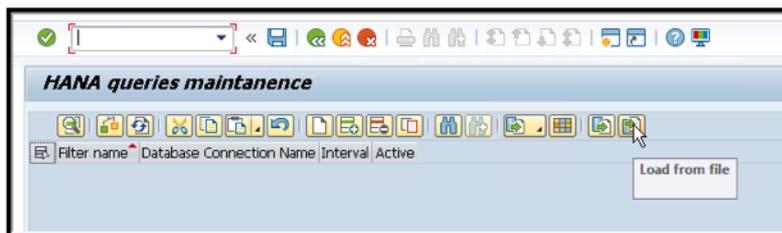
Load HANA Scripts

If your SAP systems run on HANA you will need to upload the scripts to run extended queries.

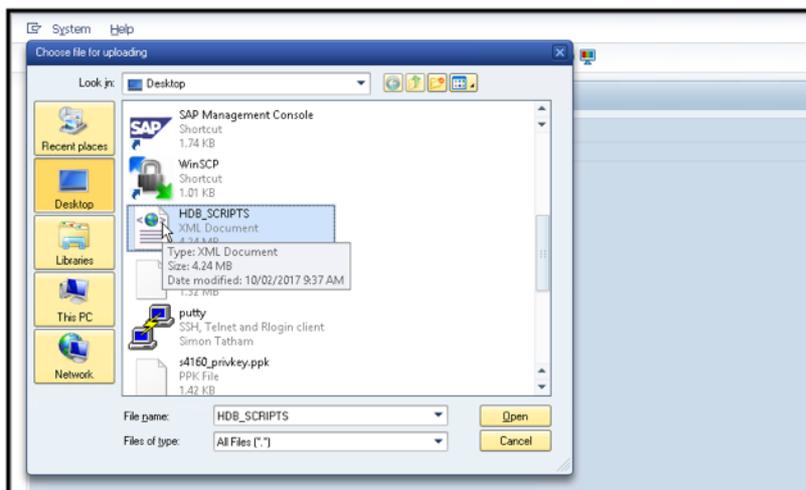
Administrator → Setup Metric → BDB Queries



Select Upload file button



Navigate to where HDB_SCRIPTS.xml file has been save and select



HANA queries maintenance

Filter name	Database Connection Name	Interval	Active
HANA_BACKUPS_BACKUPRUNS		86400	<input type="checkbox"/>
HANA_BACKUPS_CATALOGDELETION_COMMANDGENERATOR		86400	<input type="checkbox"/>
HANA_BACKUPS_CATALOGSIZE		86400	<input type="checkbox"/>
HANA_BACKUPS_LOGBACKUPDELAYS		86400	<input type="checkbox"/>
HANA_BANKANALYZER_INDEXCONSISTENCY		86400	<input type="checkbox"/>
HANA_BW_DATATARGETS		86400	<input type="checkbox"/>
HANA_BW_DSOTYPES		86400	<input type="checkbox"/>
HANA_BW_INCONSISTENTDSOTABLES		86400	<input type="checkbox"/>
HANA_BW_INCONSISTENTDSOTABLES_FALLBACK		86400	<input type="checkbox"/>
HANA_BW_INCONSISTENTFACTTABLES		86400	<input type="checkbox"/>
HANA_CALCULATIONENGINE_CALCULATIONSCENARIOS		86400	<input type="checkbox"/>
HANA_COLUMNS		86400	<input type="checkbox"/>
HANA_CONFIGURATION_HYBRIDLOBACTIVATION_COMMANDGE...		86400	<input type="checkbox"/>
HANA_CONFIGURATION_MINICHECKS_1.00.102.01+		86400	<input type="checkbox"/>
HANA_CONFIGURATION_MINICHECKS_1.00.120+		86400	<input type="checkbox"/>
HANA_CONFIGURATION_MINICHECKS_1.00.70+_SSS		86400	<input type="checkbox"/>
HANA_CONFIGURATION_MINICHECKS_1.00.74+_ESS		86400	<input type="checkbox"/>
HANA_CONFIGURATION_MINICHECKS_1.00.90+_ESS		86400	<input type="checkbox"/>
HANA_CONFIGURATION_MINICHECKS_SSS		86400	<input type="checkbox"/>
HANA_CONFIGURATION_OVERVIEW		86400	<input type="checkbox"/>
HANA_CONFIGURATION_OVERVIEW_1.00.100+		86400	<input type="checkbox"/>
HANA_CONFIGURATION_OVERVIEW_1.00.110+		86400	<input type="checkbox"/>
HANA_CONFIGURATION_PARAMETERS_1.00.69-		86400	<input type="checkbox"/>

Once uploaded select with scripts you want to run and then select “save” from the top menu

HANA queries maintenance

Filter name	Database Connection Name	Interval	Active
HANA_BACKUPS_BACKUPRUNS		86400	<input checked="" type="checkbox"/>
HANA_BACKUPS_CATALOGDELETION_COMMANDGENERATOR		86400	<input checked="" type="checkbox"/>
HANA_BACKUPS_CATALOGSIZE		86400	<input checked="" type="checkbox"/>
HANA_BACKUPS_LOGBACKUPDELAYS		86400	<input checked="" type="checkbox"/>
HANA_BANKANALYZER_INDEXCONSISTENCY		86400	<input checked="" type="checkbox"/>
HANA_BW_DATATARGETS		86400	<input checked="" type="checkbox"/>
HANA_BW_DSOTYPES		86400	<input checked="" type="checkbox"/>
HANA_BW_INCONSISTENTDSOTABLES		86400	<input checked="" type="checkbox"/>
HANA_BW_INCONSISTENTDSOTABLES_FALLBACK		86400	<input checked="" type="checkbox"/>
HANA_BW_INCONSISTENTFACTTABLES		86400	<input checked="" type="checkbox"/>
HANA_CALCULATIONENGINE_CALCULATIONSCENARIOS		86400	<input checked="" type="checkbox"/>
HANA_COLUMNS		86400	<input checked="" type="checkbox"/>
HANA_CONFIGURATION_HYBRIDLOBACTIVATION_COMMANDGE...		86400	<input type="checkbox"/>
HANA_CONFIGURATION_MINICHECKS_1.00.102.01+		86400	<input type="checkbox"/>