



Web Dispatcher Installation and Configuration

Table of Contents

1.	About this Document	3
1.1	Overview	3
1.2	Audience	3
2.	Installing Web Dispatcher	3
3.	Configuration	25
2.1	PSE Management.....	25
2.2	Importing CA Response Certificate:	27
i.	Import 3 rd Party Root Certificate:	28
ii.	Import SMP Certificate:.....	29

1. About this Document

1.1 Overview

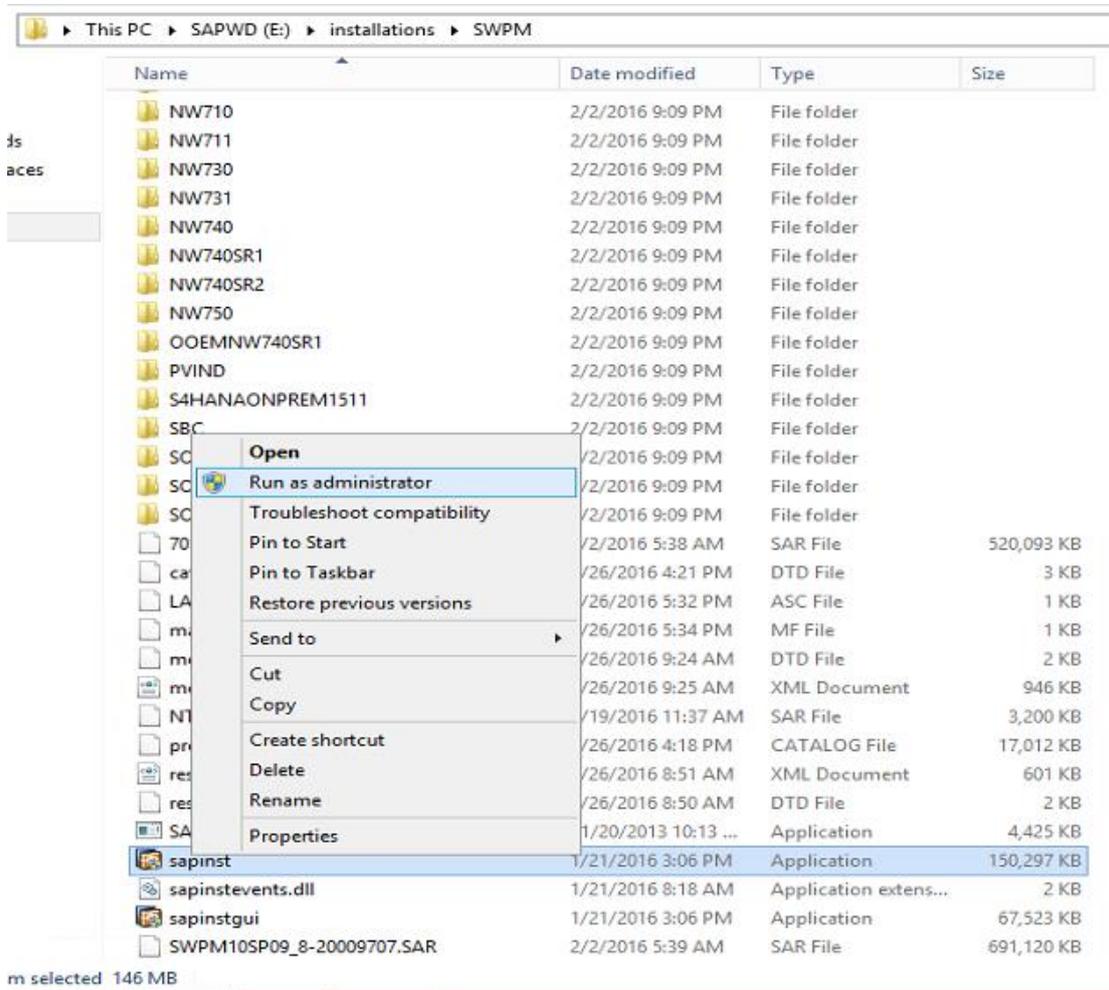
This document consists of Web Dispatcher Installation and Configuration steps.

1.2 Audience

This document is intended for Basis team.

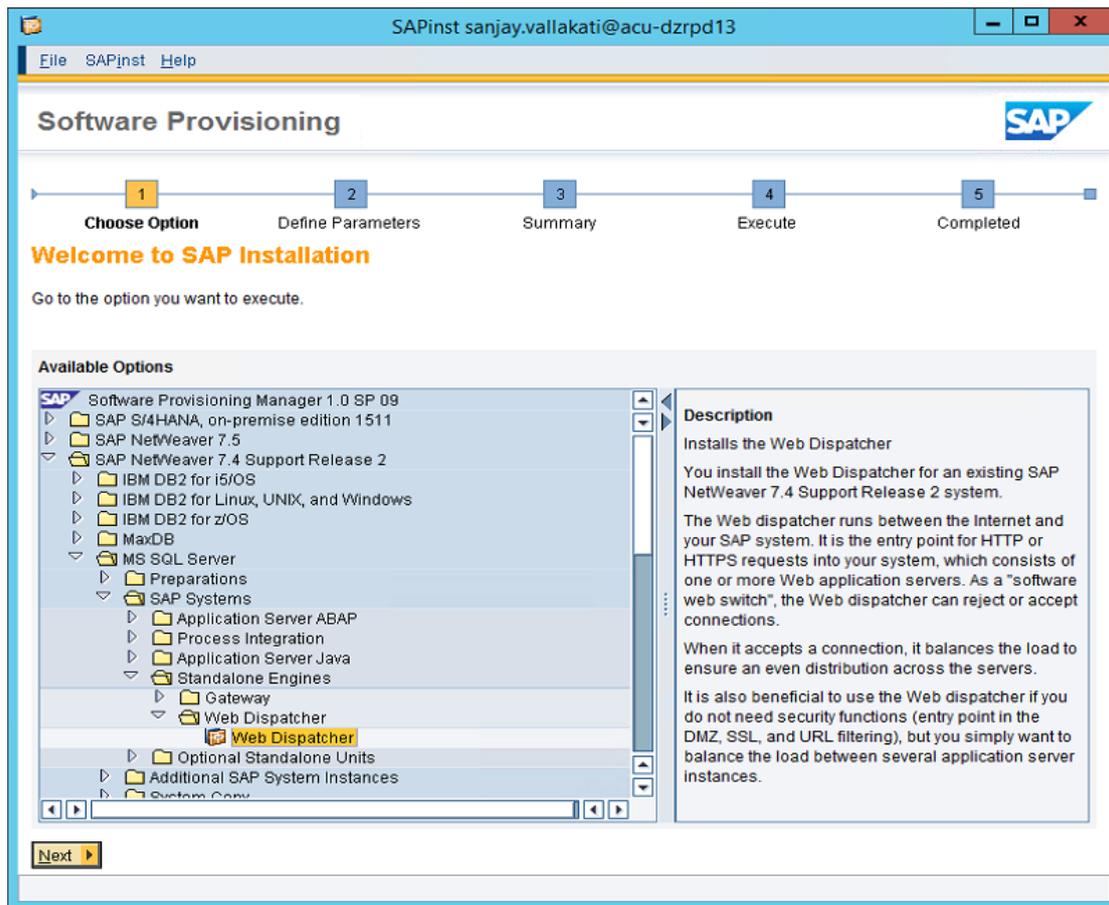
2. Installing Web Dispatcher

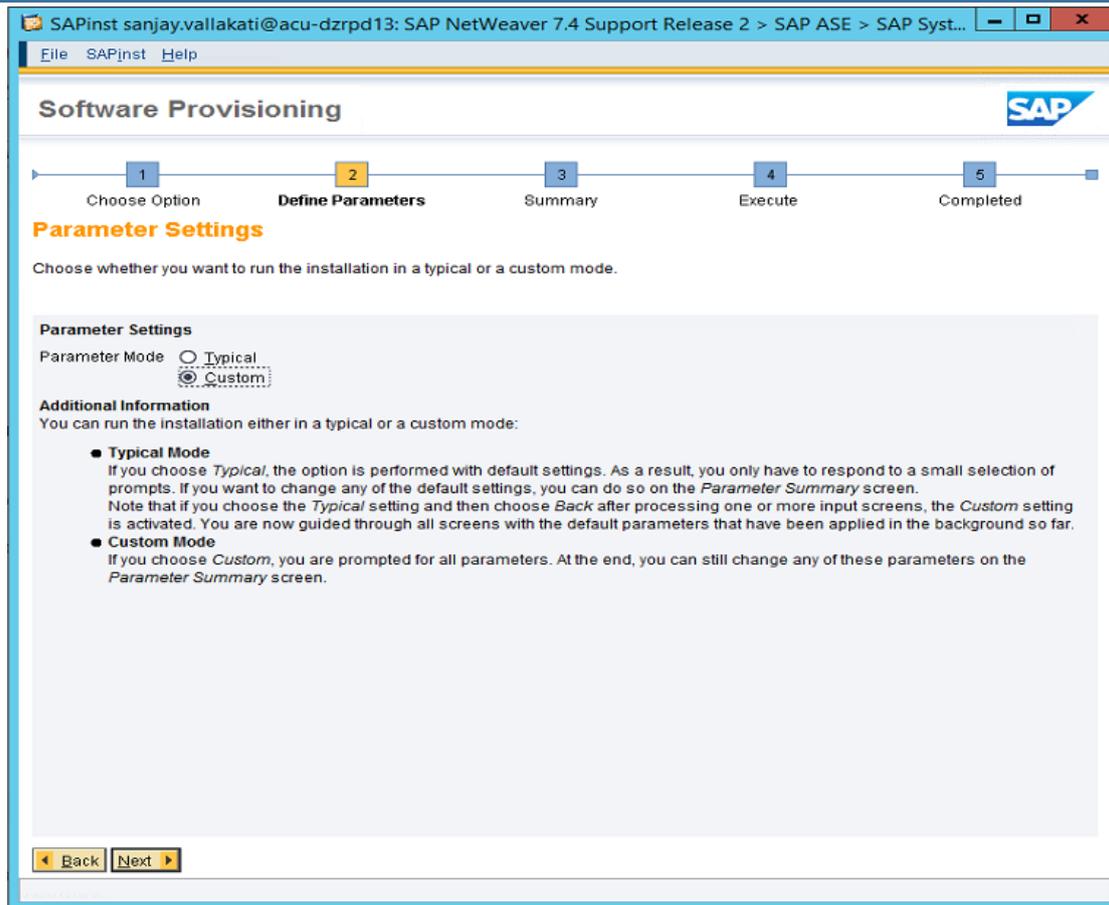
Following are the steps to be followed for Installing Web Dispatcher.



Name	Date modified	Type	Size
NW710	2/2/2016 9:09 PM	File folder	
NW711	2/2/2016 9:09 PM	File folder	
NW730	2/2/2016 9:09 PM	File folder	
NW731	2/2/2016 9:09 PM	File folder	
NW740	2/2/2016 9:09 PM	File folder	
NW740SR1	2/2/2016 9:09 PM	File folder	
NW740SR2	2/2/2016 9:09 PM	File folder	
NW750	2/2/2016 9:09 PM	File folder	
OOEMNW740SR1	2/2/2016 9:09 PM	File folder	
PVIND	2/2/2016 9:09 PM	File folder	
S4HANAONPREM1511	2/2/2016 9:09 PM	File folder	
SBC	2/2/2016 9:09 PM	File folder	
SC	2/2/2016 9:09 PM	File folder	
SC	2/2/2016 9:09 PM	File folder	
SC	2/2/2016 9:09 PM	File folder	
70	2/26/2016 5:38 AM	SAR File	520,093 KB
ca	2/26/2016 4:21 PM	DTD File	3 KB
LA	2/26/2016 5:32 PM	ASC File	1 KB
m	2/26/2016 5:34 PM	MF File	1 KB
m	2/26/2016 9:24 AM	DTD File	2 KB
m	2/26/2016 9:25 AM	XML Document	946 KB
NT	1/19/2016 11:37 AM	SAR File	3,200 KB
pr	2/26/2016 4:18 PM	CATALOG File	17,012 KB
res	2/26/2016 8:51 AM	XML Document	601 KB
res	2/26/2016 8:50 AM	DTD File	2 KB
SA	1/20/2013 10:13 ...	Application	4,425 KB
sapinst	1/21/2016 3:06 PM	Application	150,297 KB
sapinstevents.dll	1/21/2016 8:18 AM	Application extens...	2 KB
sapinstgui	1/21/2016 3:06 PM	Application	67,523 KB
SWPM10SP09_8-20009707.SAR	2/2/2016 5:39 AM	SAR File	691,120 KB

1 item selected 146 MB





The screenshot shows the SAP Software Provisioning interface. At the top, the title bar reads 'SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...'. Below the title bar is a menu bar with 'File', 'SAPinst', and 'Help'. The main header is 'Software Provisioning' with the SAP logo on the right. A progress bar below the header shows five steps: 1. Choose Option, 2. Define Parameters (highlighted in orange), 3. Summary, 4. Execute, and 5. Completed. The main content area is titled 'Parameter Settings' and contains the following text:

Choose whether you want to run the installation in a typical or a custom mode.

Parameter Settings

Parameter Mode Typical
 Custom

Additional Information
You can run the installation either in a typical or a custom mode:

- **Typical Mode**
If you choose *Typical*, the option is performed with default settings. As a result, you only have to respond to a small selection of prompts. If you want to change any of the default settings, you can do so on the *Parameter Summary* screen. Note that if you choose the *Typical* setting and then choose *Back* after processing one or more input screens, the *Custom* setting is activated. You are now guided through all screens with the default parameters that have been applied in the background so far.
- **Custom Mode**
If you choose *Custom*, you are prompted for all parameters. At the end, you can still change any of these parameters on the *Parameter Summary* screen.

At the bottom of the screen, there are 'Back' and 'Next' navigation buttons.

SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > MS SQL Server > SA...

File SAPinst Help

Software Provisioning

1 Choose Option 2 **Define Parameters** 3 Summary 4 Execute 5 Completed

General SAP System Parameters

Enter the system ID and destination drive.

SAP System

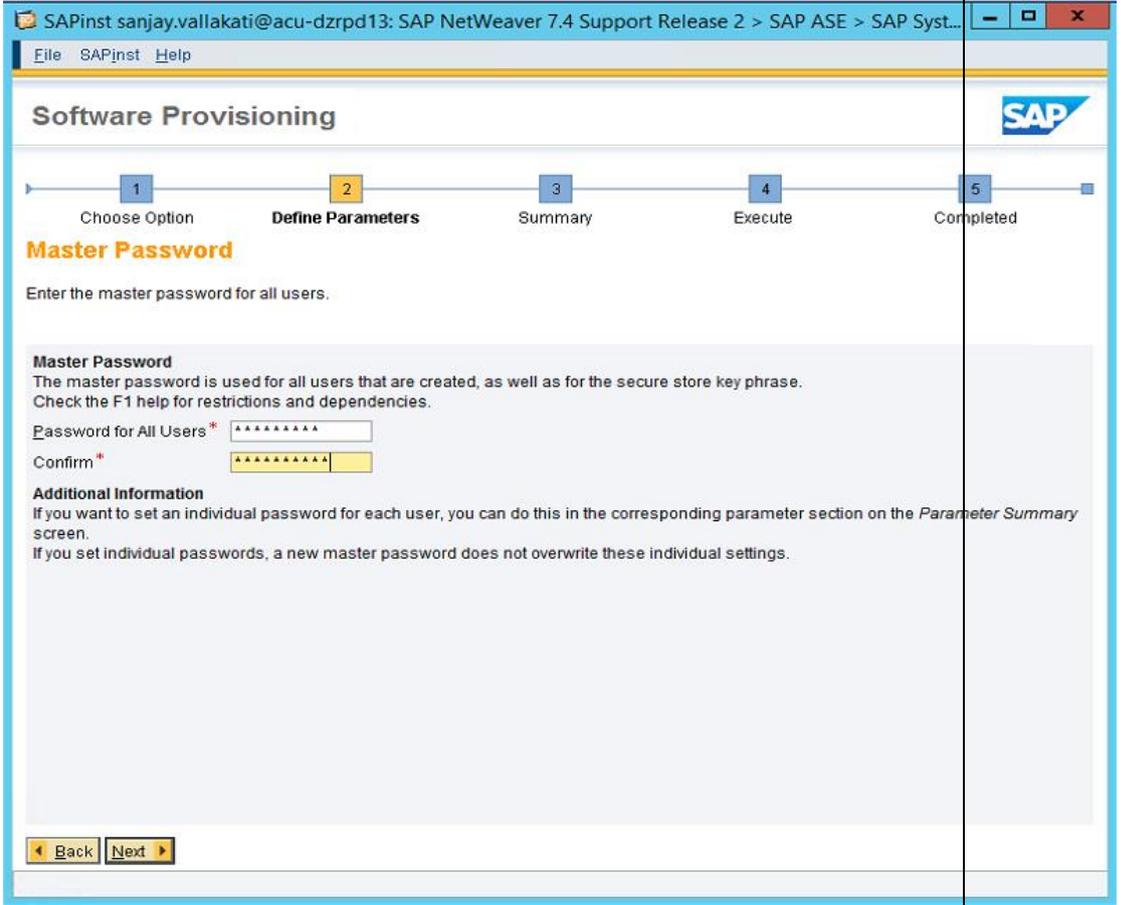
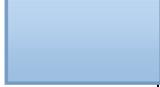
SAP System ID (SAPSID)*

Destination Drive

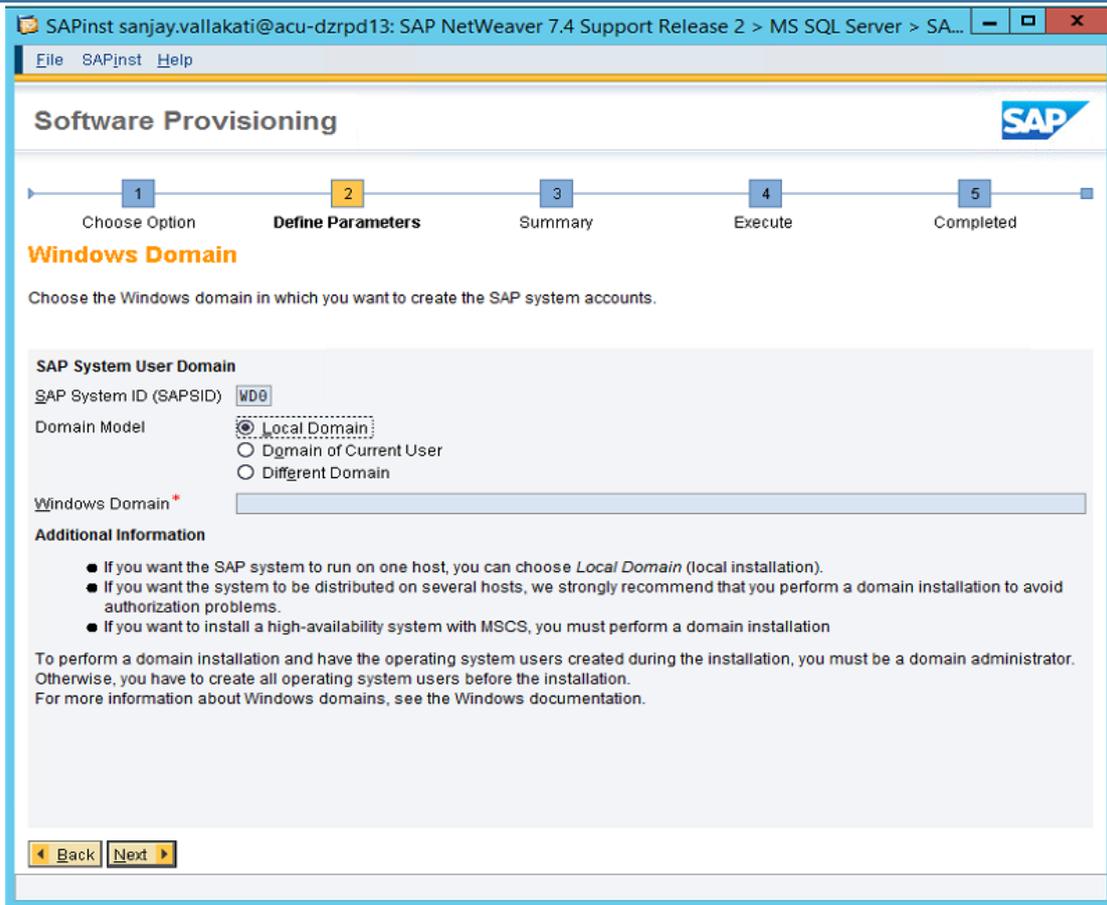
Additional Information
The *SAP System ID* is an identifier for your SAP system. It must be unique throughout your system landscape.
The system is installed under <Destination Drive>:\usr\sap\<SAPSID>\....

Password

:



The screenshot shows the SAP Software Provisioning wizard interface. At the top, the browser title is "SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...". The menu bar includes "File", "SAPinst", and "Help". The main heading is "Software Provisioning" with the SAP logo in the top right corner. A progress bar at the top indicates five steps: 1. Choose Option, 2. Define Parameters (highlighted in yellow), 3. Summary, 4. Execute, and 5. Completed. Below the progress bar, the section is titled "Master Password" in orange. The text reads: "Enter the master password for all users." Below this, there is a sub-section "Master Password" with the following text: "The master password is used for all users that are created, as well as for the secure store key phrase. Check the F1 help for restrictions and dependencies." There are two input fields: "Password for All Users*" and "Confirm*", both containing masked characters (asterisks). Below the input fields, there is "Additional Information" text: "If you want to set an individual password for each user, you can do this in the corresponding parameter section on the *Parameter Summary* screen. If you set individual passwords, a new master password does not overwrite these individual settings." At the bottom of the wizard, there are "Back" and "Next" buttons.



The screenshot shows the SAPinst software provisioning wizard. The window title is "SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > MS SQL Server > SA...". The menu bar includes "File", "SAPinst", and "Help". The main heading is "Software Provisioning" with the SAP logo. A progress bar at the top shows five steps: 1. Choose Option, 2. Define Parameters (highlighted), 3. Summary, 4. Execute, and 5. Completed. The current step is "Windows Domain", which asks the user to "Choose the Windows domain in which you want to create the SAP system accounts." The "SAP System User Domain" section includes a text field for "SAP System ID (SAPSID)" containing "WDD", a "Domain Model" section with radio buttons for "Local Domain" (selected), "Domain of Current User", and "Different Domain", and a "Windows Domain" text field. An "Additional Information" section contains three bullet points and a paragraph of instructions. At the bottom, there are "Back" and "Next" buttons.

SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > MS SQL Server > SA...

File SAPinst Help

Software Provisioning

1 Choose Option 2 Define Parameters 3 Summary 4 Execute 5 Completed

Windows Domain

Choose the Windows domain in which you want to create the SAP system accounts.

SAP System User Domain

SAP System ID (SAPSID)

Domain Model

Local Domain

Domain of Current User

Different Domain

Windows Domain *

Additional Information

- If you want the SAP system to run on one host, you can choose *Local Domain* (local installation).
- If you want the system to be distributed on several hosts, we strongly recommend that you perform a domain installation to avoid authorization problems.
- If you want to install a high-availability system with MSCS, you must perform a domain installation

To perform a domain installation and have the operating system users created during the installation, you must be a domain administrator. Otherwise, you have to create all operating system users before the installation.
For more information about Windows domains, see the Windows documentation.

Back Next

SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...

File SAPinst Help

Software Provisioning

1 Choose Option 2 **Define Parameters** 3 Summary 4 Execute 5 Completed

Operating System Users

Enter the passwords of the operating system users.

SAP System Administrator
Account: *acu-dzrpd13\gd0adm*
Password of SAP System Administrator:
Confirm:

SAP System Service User
Account: *acu-dzrpd13\SAPServiceGDO*
Password of SAP System Service User:
Confirm:

SAPInst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...

File SAPInst Help

Software Provisioning

1 Choose Option

Media Browser

Enter the location of the required

5 Completed

Software Package Request

Medium
Kerne1 NW740 SR2

Additional Information

The required software packages

If you do not want to check the locations of the software packages now, deselect the flag in the Check Location column. Later, you are prompted again to check the locations of the software packages.

Back Next

File Browser

Select the file.

- My Computer
- C:
- E:
- \$RECYCLE.BIN
- System Volume Information
- installations
 - Kernel742
 - 51049724_10
 - DATA_UNITS
 - CDLABEL.ASC
 - CDLABEL.EBC
 - COPY_TM.HTM
 - COPY_TM.TXT
 - LABEL.ASC**
 - LABEL.EBC
 - LABELIDX.ASC
 - MD5FILE.DAT
 - MID.XML
 - SHAFILE.DAT
 - VERSION.ASC
 - VERSION.EBC
 - 51049724_10.zip
 - SAPCAR patch number 510

File LABEL.ASC

OK Cancel

Check Location

Browse...

SAPinst Administrator@INNOGDCSERV: SAP NetWeaver 7.0 including Enhancement Package 3 > Standalone Engines > Web Disp...

File SAPinst Help

Software Provisioning

1 Choose Option

Media Browser > Soft

Enter the location of the required s

Software Package Request

Medium
Kerne1 NW 7.20 / 7.21

Additional Information
 The required software packages :
 If you do not want to check the locations of the software packages now, deselect the flag in the *Check Location* column. Later, you are prompted again to check the locations of the software packages.

Back Next

File Browser

Select the file.

- My Computer
- C:
- D:
- E:
- \$RECYCLE.BIN
- System Volume Information
- mWorklist
- profile_backup
- usr
 - KrnL_7.21_WIN_IA32_IA64_x64_SP09_
 - DATA_UNITS
 - CDLABEL.ASC
 - CDLABEL.EBC
 - COPY_TM.HTM
 - COPY_TM.TXT
 - LABEL.ASC**
 - LABEL.EBC
 - LABELIX.ASC
 - MID.XML
 - SHAFILE.DAT
 - VERSION.ASC
 - VERSION.EBC
 - SWPM_SP08

File LABEL.ASC

OK Cancel

5 Completed

	Check Location
Browse...	<input checked="" type="checkbox"/>

SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...

File SAPinst Help

Software Provisioning

1 Choose Option
 2 **Define Parameters**
 3 Summary
 4 Execute
 5 Completed

Media Browser

Enter the location of the required software packages.

Software Package Request

Medium	Package Location		Check Location
Kerne1 NW740 SR2	E:\installations\Kerne1742\5104972...	Browse...	<input checked="" type="checkbox"/>

Additional Information
 The required software packages available on the medium are detected using the identification files LABEL.ASC or LABELIDX.ASC. If you do not want to check the locations of the software packages now, deselect the flag in the *Check Location* column. Later, you are prompted again to check the locations of the software packages.

SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...

File SAPinst Help

Software Provisioning

1 Choose Option 2 **Define Parameters** 3 Summary 4 Execute 5 Completed

Windows Domain for SAP Host Agent

Select the Windows domain of the SAP system accounts for the SAP Host Agent.

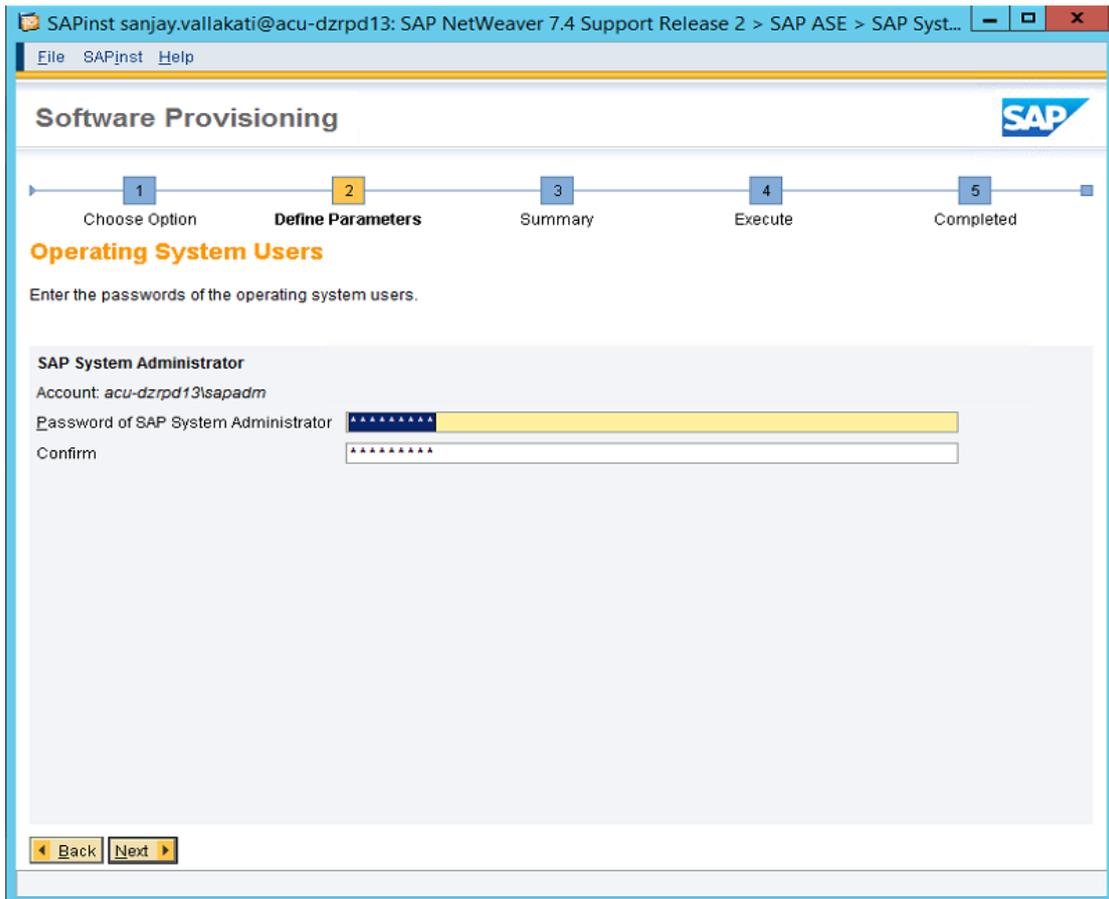
SAP Host Agent User Domain

SAP System ID (SAPSID):

Domain Model

- Local Domain
- Domain of Current User
- Different Domain

Windows Domain*



The screenshot shows the SAPinst Software Provisioning wizard. The title bar indicates the user is 'sanjay.vallakati@acu-dzrpd13' and the system is 'SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...'. The menu bar includes 'File', 'SAPinst', and 'Help'. The main window title is 'Software Provisioning' with the SAP logo in the top right corner. A progress bar at the top shows five steps: 1. Choose Option, 2. Define Parameters (highlighted in yellow), 3. Summary, 4. Execute, and 5. Completed. Below the progress bar, the section 'Operating System Users' is displayed in orange text. The instruction reads: 'Enter the passwords of the operating system users.' The 'SAP System Administrator' section shows the account 'acu-dzrpd13\sapadm'. There are two password input fields: 'Password of SAP System Administrator' and 'Confirm', both containing masked characters (asterisks). At the bottom left, there are 'Back' and 'Next' navigation buttons.

SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...

File SAPinst Help

Software Provisioning

1 Choose Option 2 **Define Parameters** 3 Summary 4 Execute 5 Completed

SAP Web Dispatcher

Enter the required instance parameters for the SAP Web Dispatcher instance

SAP Web Dispatcher Instance

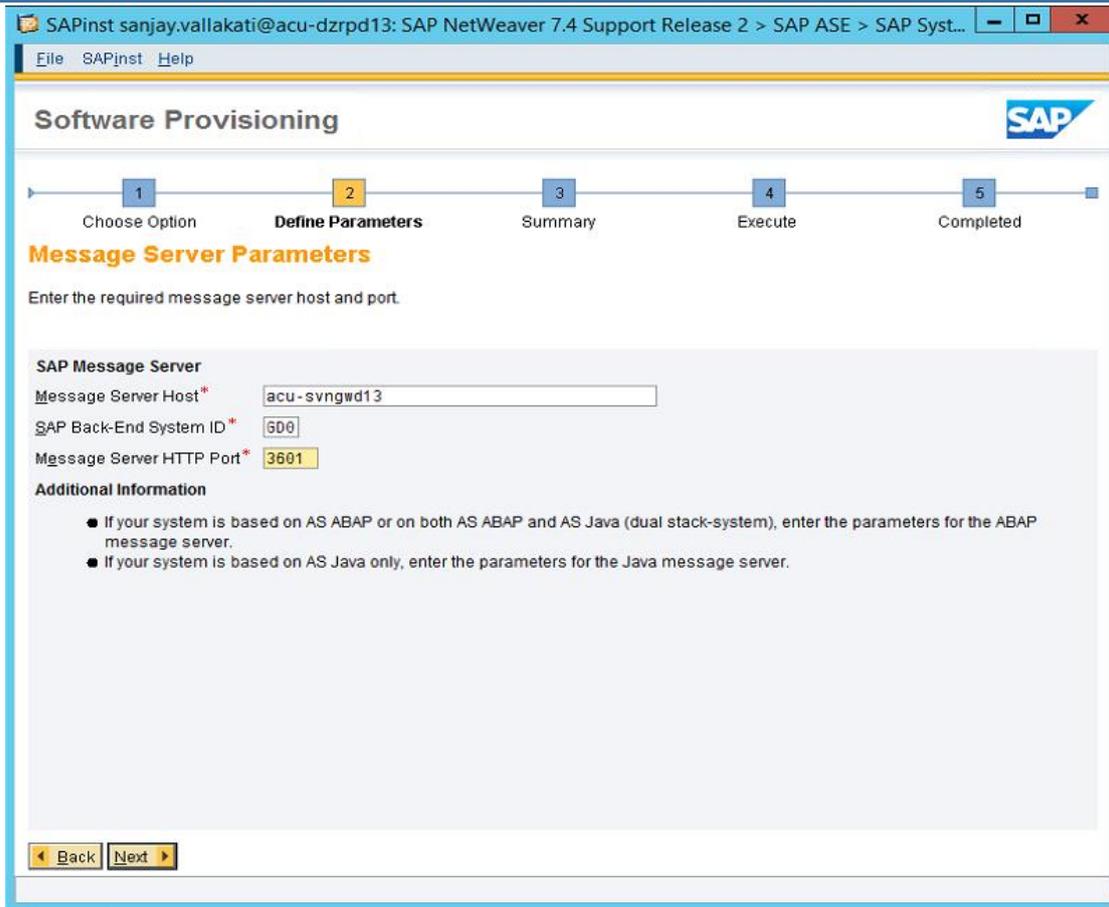
The following SAP system instances already exist on this host:

SAP System ID (SAPSID)	Instance Name	Instance Number
------------------------	---------------	-----------------

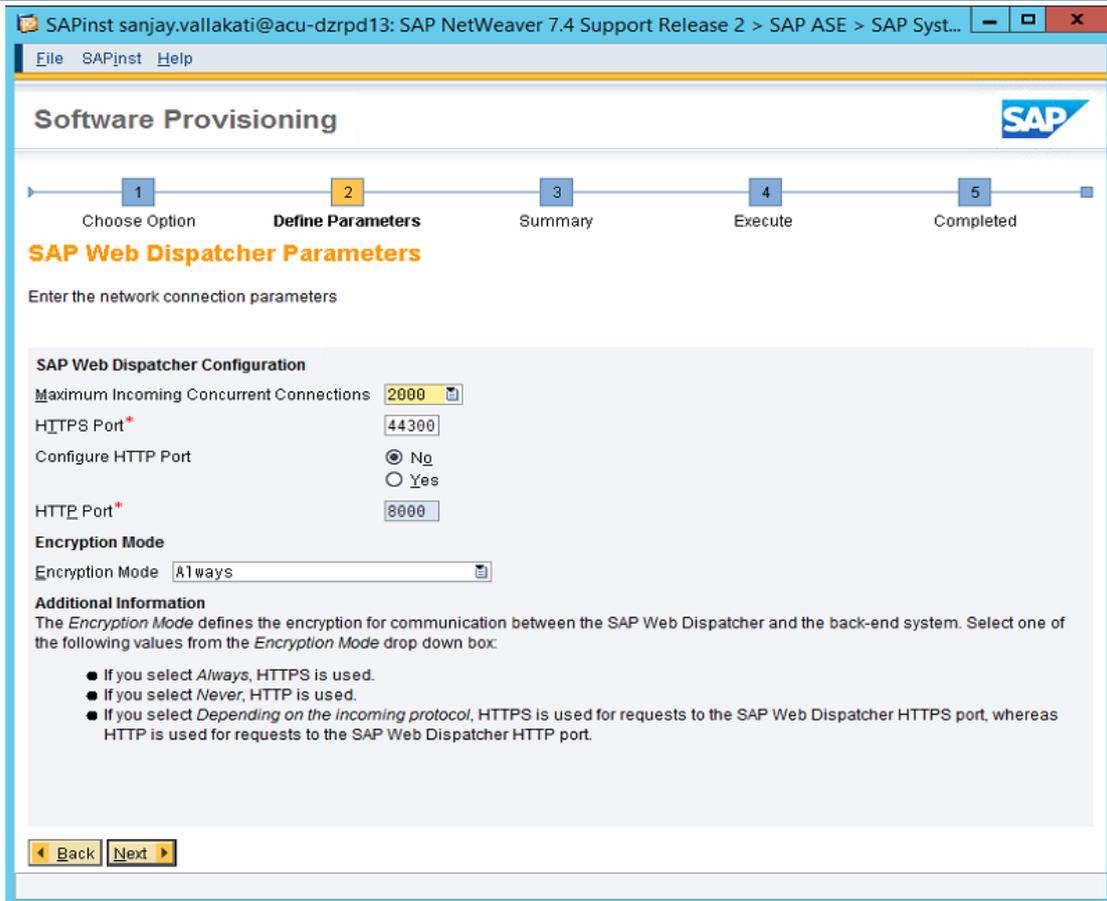
Instance Number*

Virtual Host*

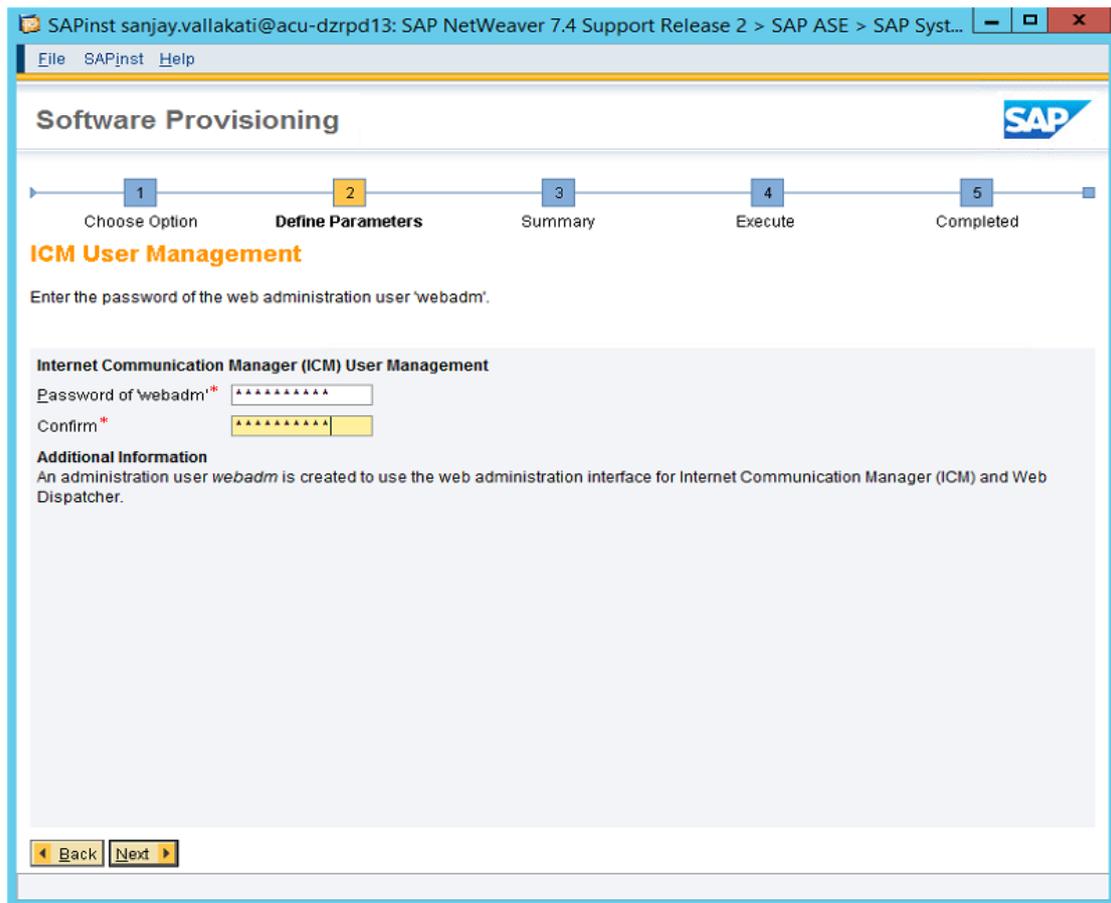
Additional Information
The *Instance Number* and *Virtual Host* for the SAP Web Dispatcher instance are technical identifiers for controlling internal processes, such as assigned memory. They must be unique for this installation host.



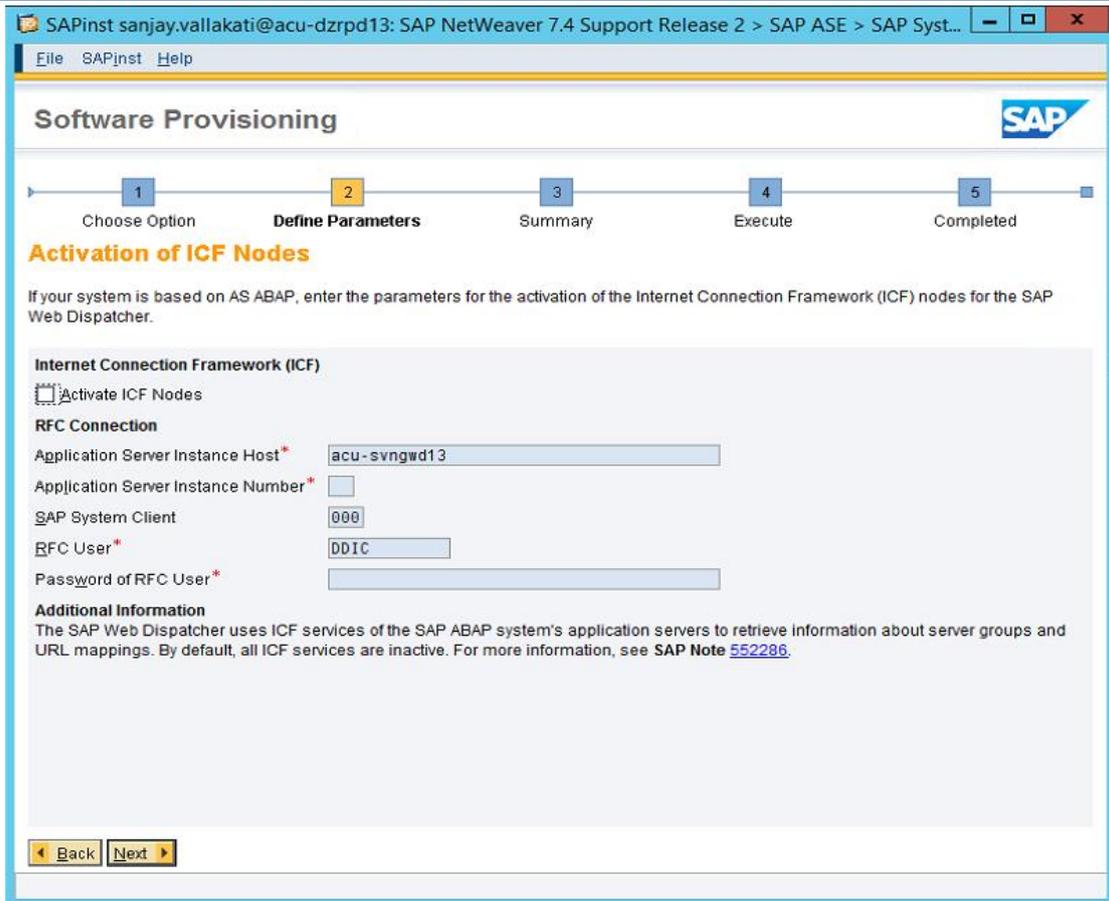
The screenshot shows the SAPinst software provisioning wizard. The window title is "SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...". The menu bar includes "File", "SAPinst", and "Help". The main heading is "Software Provisioning" with the SAP logo in the top right corner. A progress bar at the top indicates five steps: 1. Choose Option, 2. Define Parameters (highlighted in yellow), 3. Summary, 4. Execute, and 5. Completed. Below the progress bar, the section is titled "Message Server Parameters" in orange. A sub-heading reads "Enter the required message server host and port." The "SAP Message Server" section contains three input fields: "Message Server Host*" with the value "acu-svngwd13", "SAP Back-End System ID*" with the value "600", and "Message Server HTTP Port*" with the value "3601". An "Additional Information" section follows, containing two bullet points: "● If your system is based on AS ABAP or on both AS ABAP and AS Java (dual stack-system), enter the parameters for the ABAP message server." and "● If your system is based on AS Java only, enter the parameters for the Java message server." At the bottom left, there are "Back" and "Next" navigation buttons.



The screenshot shows the SAPinst Software Provisioning wizard. The title bar indicates the user is sanjay.vallakati@acu-dzrpd13 and the system is SAP NetWeaver 7.4 Support Release 2. The wizard is currently on step 2, 'Define Parameters', out of five steps: 1. Choose Option, 2. Define Parameters, 3. Summary, 4. Execute, and 5. Completed. The current step is titled 'SAP Web Dispatcher Parameters' and instructs the user to 'Enter the network connection parameters'. The configuration section includes: 'Maximum Incoming Concurrent Connections' set to 2000; 'HTTPS Port*' set to 44300; 'Configure HTTP Port' with radio buttons for 'No' (selected) and 'Yes'; 'HTTP Port*' set to 8000; and 'Encryption Mode' set to 'Always'. An 'Additional Information' section explains that the Encryption Mode defines the encryption for communication between the SAP Web Dispatcher and the back-end system, with three options: 'Always' (uses HTTPS), 'Never' (uses HTTP), and 'Depending on the incoming protocol' (uses HTTPS for HTTPS requests and HTTP for HTTP requests). At the bottom, there are 'Back' and 'Next' navigation buttons.



The screenshot shows a SAP Software Provisioning wizard window. The title bar reads "SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst...". The menu bar includes "File", "SAPinst", and "Help". The main content area is titled "Software Provisioning" and features a progress bar with five steps: 1. Choose Option, 2. Define Parameters (highlighted in yellow), 3. Summary, 4. Execute, and 5. Completed. Below the progress bar, the section "ICM User Management" is displayed. It prompts the user to "Enter the password of the web administration user 'webadm'." and contains two password input fields: "Password of 'webadm'*" and "Confirm*", both masked with asterisks. Below these fields is an "Additional Information" section with the text: "An administration user *webadm* is created to use the web administration interface for Internet Communication Manager (ICM) and Web Dispatcher." At the bottom of the wizard, there are "Back" and "Next" navigation buttons.



The screenshot shows the SAPinst Software Provisioning wizard. The title bar indicates the user is sanjay.vallakati@acu-dzrpd13 and the system is SAP NetWeaver 7.4 Support Release 2. The wizard is currently on step 2, "Define Parameters".

Software Provisioning 

Progress bar: 1 Choose Option, 2 **Define Parameters**, 3 Summary, 4 Execute, 5 Completed

Activation of ICF Nodes

If your system is based on AS ABAP, enter the parameters for the activation of the Internet Connection Framework (ICF) nodes for the SAP Web Dispatcher.

Internet Connection Framework (ICF)

Activate ICF Nodes

RFC Connection

Application Server Instance Host*

Application Server Instance Number*

SAP System Client

RFC User*

Password of RFC User*

Additional Information

The SAP Web Dispatcher uses ICF services of the SAP ABAP system's application servers to retrieve information about server groups and URL mappings. By default, all ICF services are inactive. For more information, see [SAP Note 552286](#).

SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > MS SQL Server > SA...

File SAPinst Help

Software Provisioning

1 Choose Option 2 **Define Parameters** 3 Summary 4 Execute 5 Completed

Unpack Archives

Select the archives you want to unpack.

SAP System Archives
 The installation procedure has determined that the selected archives have to be unpacked. Choose *Next* to unpack the archives automatically from the media to the SAP global host.

Archives to Be Unpacked

Unpack Archive	Codepage	Destination	Downloade...
<input checked="" type="checkbox"/> DBINDEP\SAPEXE.SAR	Non-Unicode	E:\usr\sap\W00\SY5\exe\nuc\NTAMD64	<input type="button" value="Browse..."/>

Additional Information
 If you have downloaded newer versions of these archives from SAP Service Marketplace, enter their locations in the *Downloaded To* column. Deselect *Unpack* for archives that you want to unpack manually: for instance if the destination is located on a network share for which the installation user does not have write permissions.

Additional Information for SAP HANA
 If you are installing a product based on SAP HANA please download the latest SAPEXE.SAR and SAPEXEDB.SAR of your SAP kernel from the SAP Service Marketplace and enter their respective download locations in the *Downloaded To* column. If you are installing a product based on kernel version 7.20 please use the archives of kernel version 7.21.

SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Syst... - [maximize] [close]

File SAPinst Help

Software Provisioning

1 Choose Option 2 **Define Parameters** 3 Summary 4 Execute 5 Completed

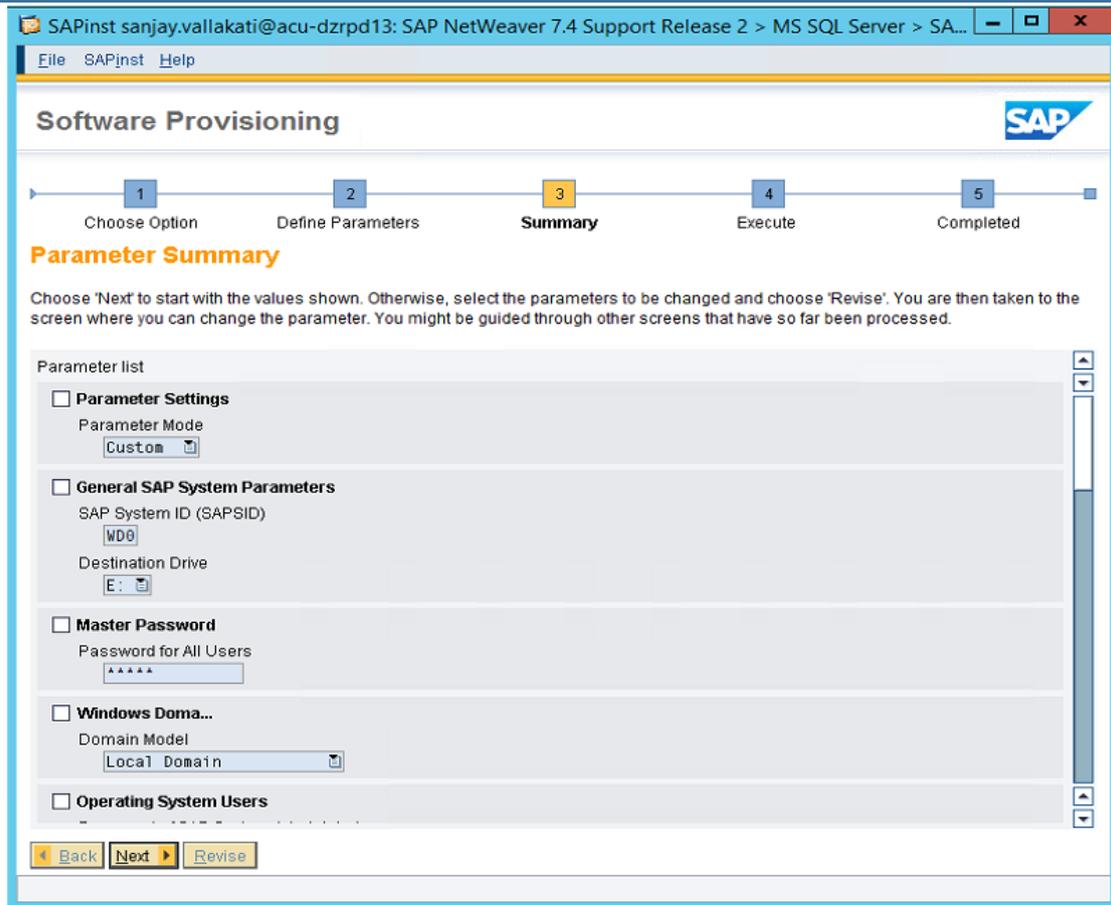
Install Diagnostics Agent

Define your Diagnostics Agent installation strategy and decide whether to install the Diagnostics Agent for diagnostics in SAP Solution Manager.

Diagnostics Agent for Diagnostics in SAP Solution Manager

Install Diagnostics Agent

Additional Information
It is recommended to **not install** the Diagnostics Agent together with the managed system when using *Agents On-the-fly* functionality. Refer to SAP Note [1365123](#) for guidance and details.



The screenshot shows the SAPinst Software Provisioning interface. At the top, the window title is "SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > MS SQL Server > SA...". The main header is "Software Provisioning" with the SAP logo. A progress bar below the header shows five steps: 1. Choose Option, 2. Define Parameters, 3. Summary (highlighted in yellow), 4. Execute, and 5. Completed.

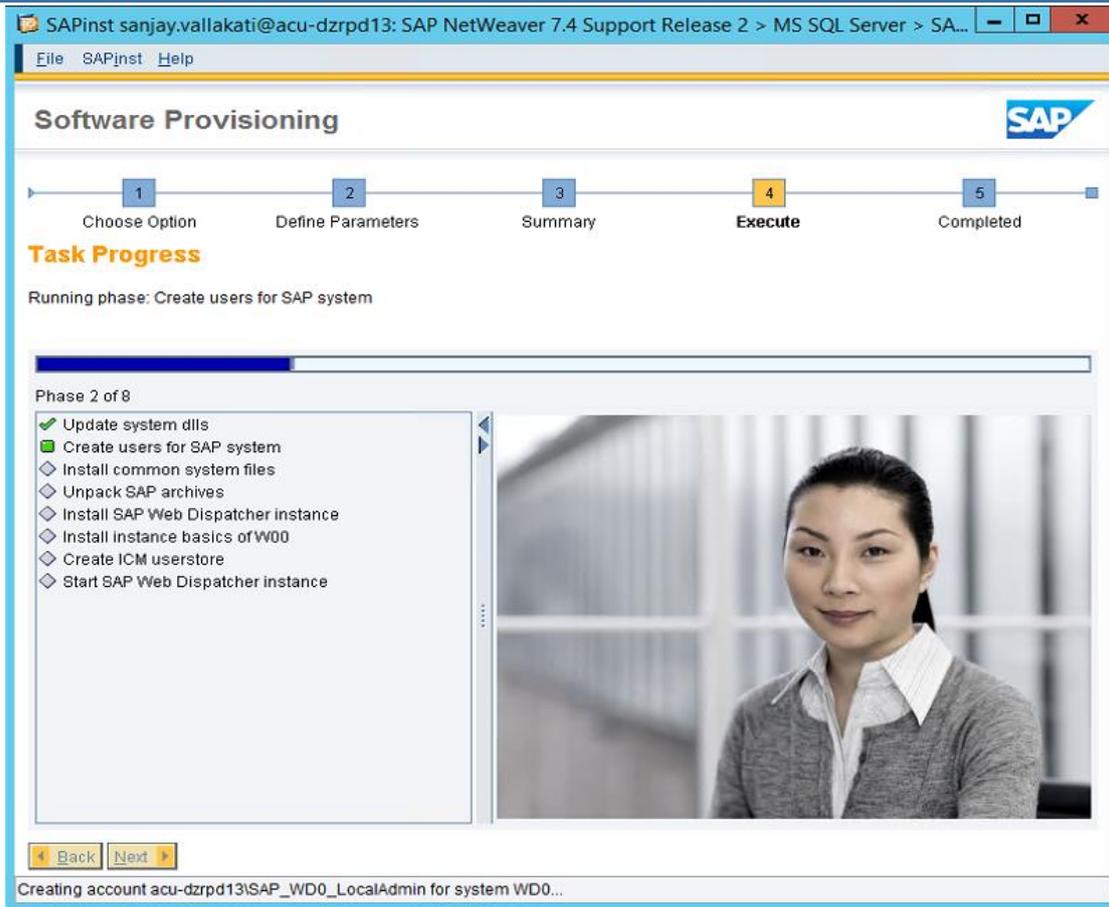
Parameter Summary

Choose 'Next' to start with the values shown. Otherwise, select the parameters to be changed and choose 'Revise'. You are then taken to the screen where you can change the parameter. You might be guided through other screens that have so far been processed.

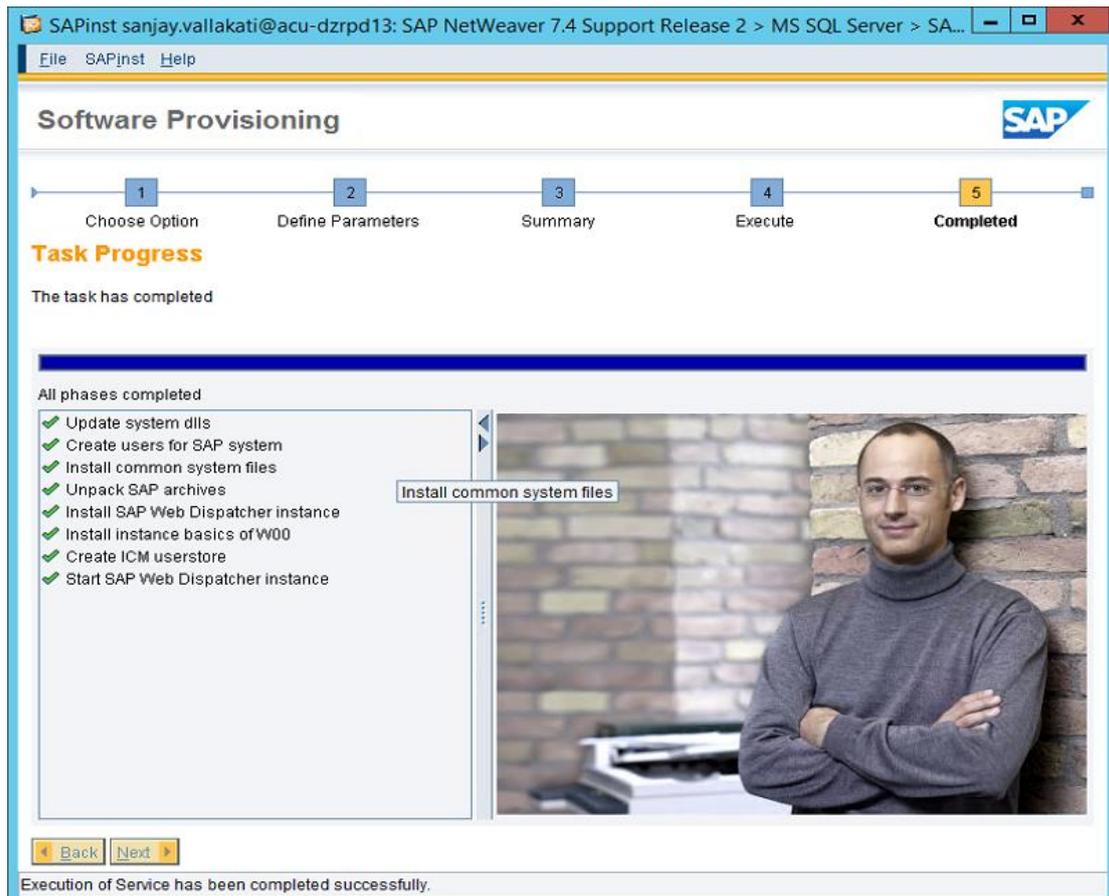
Parameter List

- Parameter Settings**
 - Parameter Mode: Custom
- General SAP System Parameters**
 - SAP System ID (SAPSID): W00
 - Destination Drive: E:
- Master Password**
 - Password for All Users: [masked]
- Windows Doma...**
 - Domain Model: Local Domain
- Operating System Users**

At the bottom, there are three buttons: "Back", "Next", and "Revise".



The screenshot shows the SAPinst software provisioning interface. At the top, the window title is "SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > MS SQL Server > SA...". The main header is "Software Provisioning" with the SAP logo on the right. A progress bar below the header shows five steps: 1. Choose Option, 2. Define Parameters, 3. Summary, 4. Execute (highlighted in yellow), and 5. Completed. Below the progress bar, the text "Task Progress" is displayed in orange, followed by "Running phase: Create users for SAP system". A task list on the left under "Phase 2 of 8" includes: Update system dlls (checked), Create users for SAP system (checked), Install common system files (diamond), Unpack SAP archives (diamond), Install SAP Web Dispatcher instance (diamond), Install instance basics of W00 (diamond), Create ICM userstore (diamond), and Start SAP Web Dispatcher instance (diamond). To the right of the task list is a portrait of a woman. At the bottom, there are "Back" and "Next" buttons, and a status bar at the very bottom reads "Creating account acu-dzrpd13\SAP_WD0_LocalAdmin for system WD0..."



SAPinst sanjay.vallakati@acu-dzrpd13: SAP NetWeaver 7.4 Support Release 2 > MS SQL Server > SA...

File SAPinst Help

Software Provisioning

1 Choose Option 2 Define Parameters 3 Summary 4 Execute 5 Completed

Task Progress

The task has completed

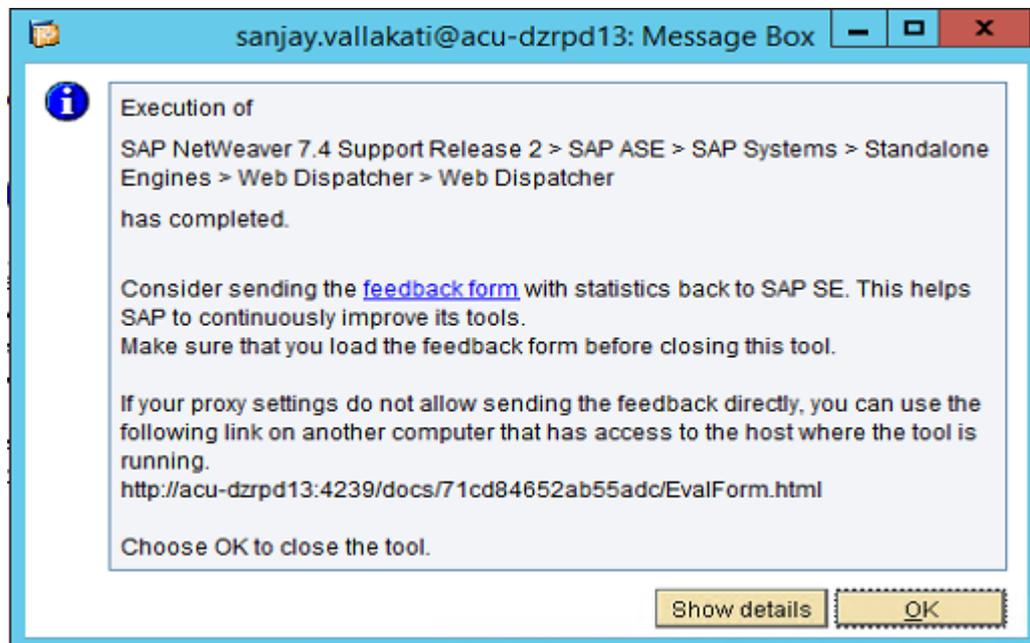
All phases completed

- ✓ Update system dlls
- ✓ Create users for SAP system
- ✓ Install common system files
- ✓ Unpack SAP archives
- ✓ Install SAP Web Dispatcher instance
- ✓ Install instance basics of W00
- ✓ Create ICM userstore
- ✓ Start SAP Web Dispatcher instance

Install common system files

Back Next

Execution of Service has been completed successfully.



sanjay.vallakati@acu-dzrpd13: Message Box

i Execution of
SAP NetWeaver 7.4 Support Release 2 > SAP ASE > SAP Systems > Standalone
Engines > Web Dispatcher > Web Dispatcher
has completed.

Consider sending the [feedback form](#) with statistics back to SAP SE. This helps
SAP to continuously improve its tools.
Make sure that you load the feedback form before closing this tool.

If your proxy settings do not allow sending the feedback directly, you can use the
following link on another computer that has access to the host where the tool is
running.
<http://acu-dzrpd13:4239/docs/71cd84652ab55adc/EvalForm.html>

Choose OK to close the tool.

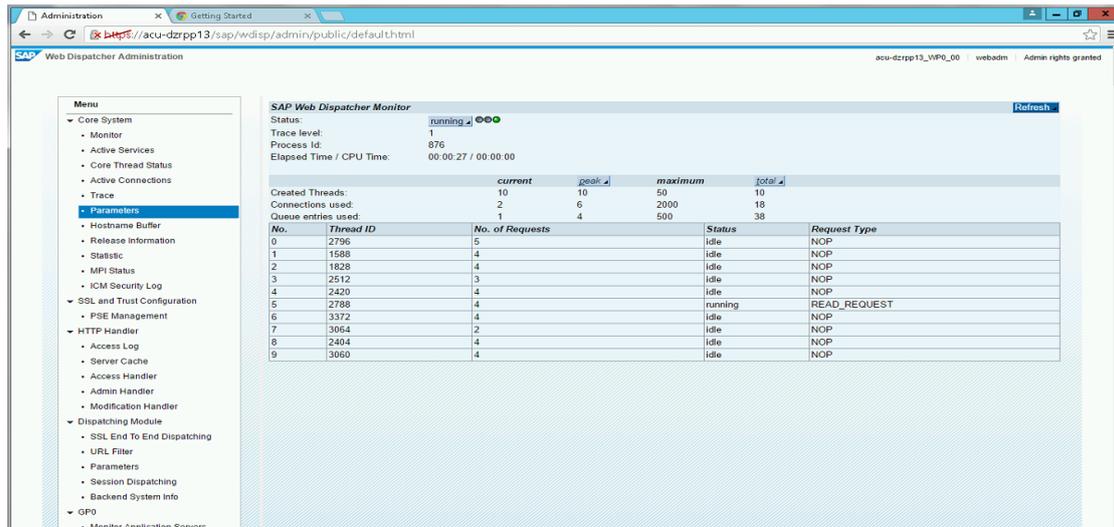
Show details OK

3. Configuration

Please make necessary modifications as per the sample configuration file provided.

Login into Web Dispatcher:

PSE Management:



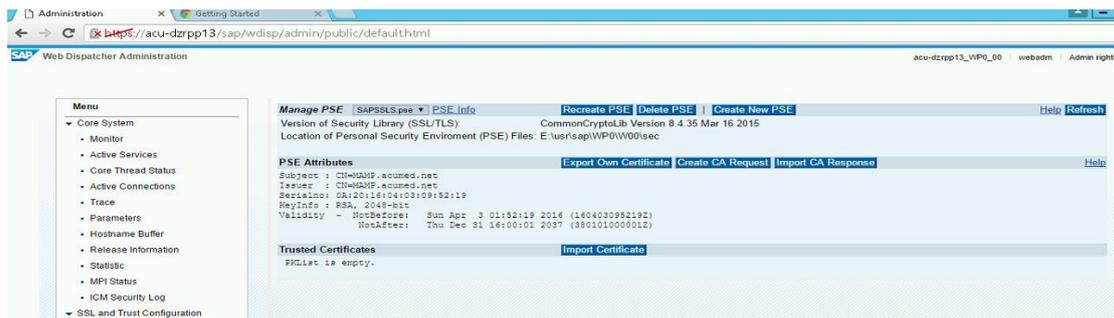
The screenshot shows the SAP Web Dispatcher Administration interface. The main content area displays the 'SAP Web Dispatcher Monitor' status, which is 'running'. Below this, there is a table showing the number of threads and requests. The table has columns for 'No.', 'Thread ID', 'No. of Requests', 'Status', and 'Request Type'.

No.	Thread ID	No. of Requests	Status	Request Type
0	2796	5	idle	NOP
1	1588	4	idle	NOP
2	1828	4	idle	NOP
3	2512	3	idle	NOP
4	2420	4	idle	NOP
5	2788	4	running	READ_REQUEST
6	3372	4	idle	NOP
7	3064	2	idle	NOP
8	2404	4	idle	NOP
9	3060	4	idle	NOP

2.1 PSE Management

Click on PSE Management:

Select Recreate PSE



The screenshot shows the 'PSE Management' section of the SAP Web Dispatcher Administration interface. The 'Manage PSE' section is active, showing details for a Personal Security Environment (PSE). The 'Recreate PSE' button is highlighted in blue. Below this, there are sections for 'PSE Attributes' and 'Trusted Certificates'.



Administration x Getting Started x
 https://acu-dzrpp13/sap/wdisp/admin/public/default.html

Web Dispatcher Administration

Menu

- Core System
 - Monitor
 - Active Services
 - Core Thread Status
 - Active Connections
 - Trace
 - Parameters
 - Hostname Buffer
 - Release Information
 - Statistic

Create new key pair for PSE SAPSSL.pse PSE Info

Distinguished Name:

Algorithm: **RSA with SHA-256** [Algorithm Info](#)

Key Length: **2048**

PIN (optional):

[Back](#) [Create](#)



Web Dispatcher Administration acu-dzrpp13_WP0_00 webadm Admin rights gran

Menu

- Core System
 - Monitor
 - Active Services
 - Core Thread Status
 - Active Connections
 - Trace
 - Parameters
 - Hostname Buffer
 - Release Information
 - Statistic
 - MPI Status
 - ICM Security Log
- SSL and Trust Configuration
 - PSE Management
- HTTP Handler

Created Key Pair for PSE SAPSSL.pse [Manage PSE](#) [PSE Info](#) [Recreate PSE](#) [Delete PSE](#) [Create New PSE](#) [Help](#) [Refresh](#)

Version of Security Library (SSL/TLS): CommonCryptoLib Version 8.4.35 Mar 16 2015
 Location of Personal Security Environment (PSE) Files: E:\usrsap\WP0\W00\sec

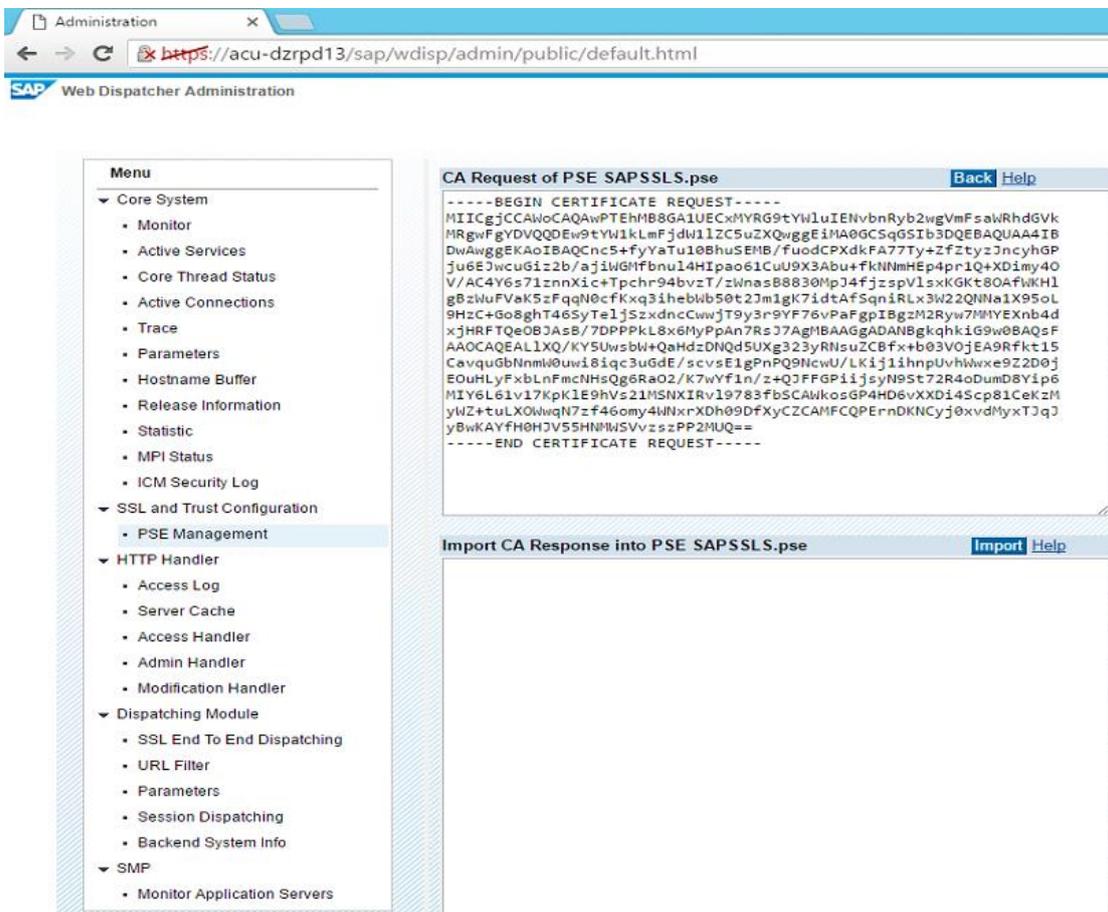
PSE Attributes [Export Own Certificate](#) [Create CA Request](#) [Import CA Response](#) [Help](#)

Subject: CN=MAMP.acumed.net
 Issuer: CN=MAMP.acumed.net
 Serialno: 0A120161040309152119
 KeyInfo - RSA, 2048-bit
 Validity - NotBefore: Sun Apr 3 01:15:21 2016 (1604030952119)
 NotAfter: Thu Dec 31 16:00:01 2037 (3801010000012)

Trusted Certificates [Import Certificate](#)

PKList is empty.

Copy the provided PSE Certificate



Administration x
 https://acu-dzrpd13/sap/wdisp/admin/public/default.html

Web Dispatcher Administration

Menu

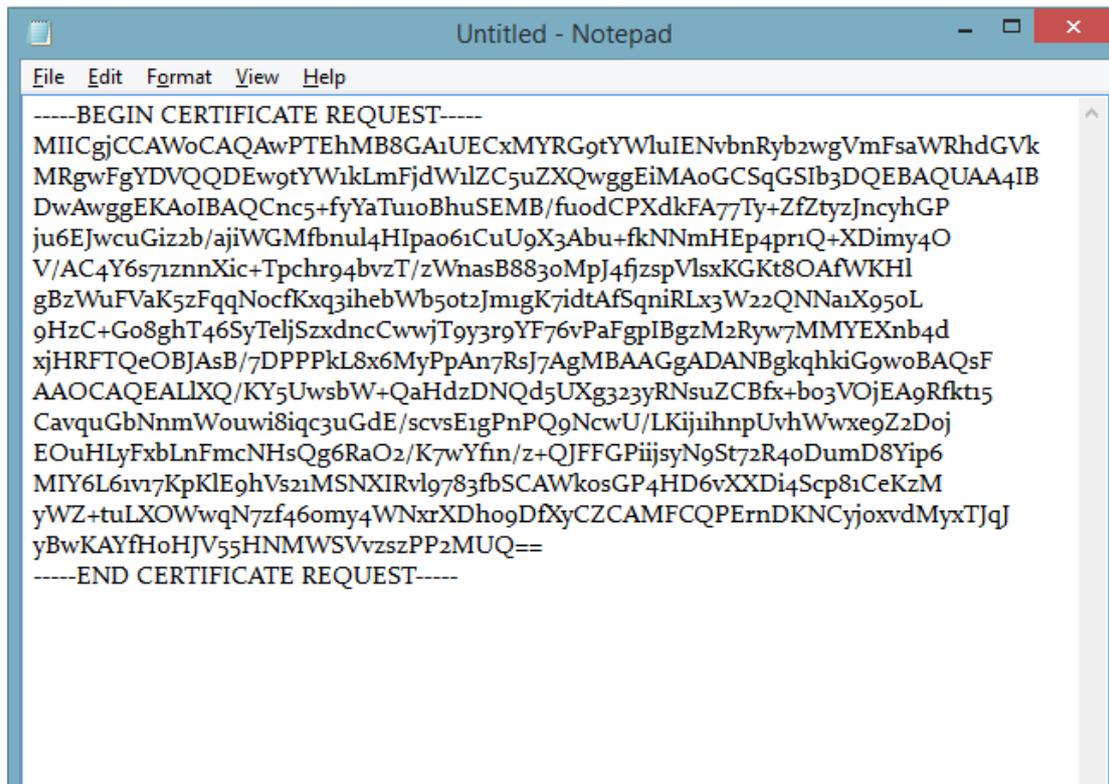
- Core System
 - Monitor
 - Active Services
 - Core Thread Status
 - Active Connections
 - Trace
 - Parameters
 - Hostname Buffer
 - Release Information
 - Statistic
 - MPI Status
 - ICM Security Log
- SSL and Trust Configuration
 - PSE Management
- HTTP Handler
 - Access Log
 - Server Cache
 - Access Handler
 - Admin Handler
 - Modification Handler
- Dispatching Module
 - SSL End To End Dispatching
 - URL Filter
 - Parameters
 - Session Dispatching
 - Backend System Info
- SMP
 - Monitor Application Servers

CA Request of PSE SAPSSL.pse [Back](#) [Help](#)

```

-----BEGIN CERTIFICATE REQUEST-----
MIICgGCCAwoCAQAwPTEhMB8GA1UECwMYRg9tYwluIENvbnRyb2wgVmFsaWRhdGVk
MRgwFgYDQDEw9tYW1kLmFjdW11ZC5uZXQwggEiMA0GCsqG5Ib3DQEBAQUAA4IB
DwAwggEKAAoIBAQCnc5+fYyATu10BhuSEMB/fuodCPXdkFA777Ty+ZfZtyJncyhGP
ju6E3wcuGiz2b/ajjWGHfBnu14HIpao61CuU9X3Abu+fknNmHEp4pr1Q+XDImy4Q
V/AC4Y6s71znnXic+Tpchr94bvzT/zWnasB8830MpJ4fjzspV1sxKGKt80AfWkH1
gBzWuFvK5zFqqN0cfKxq3ihebw50t2Jm1gk7idAfSqniRLx3W22QNNa1X95oL
9HzC+Go8ghT465yTeljSzdncCwwjT9y3r9YF76vPaFgpIBgzM2Ryw7MMYEXnb4d
xjHRFTQeOBJA5B/7DPppkL8x6HyPpAn7RsJ7AgrMBAAGgADANBgkqhkiG9w0BAQsF
AAOCAQEAALXQ/KY5Uwsbw+QaHdzDNQd5UXg323yRNsuzCBf+hb03V0jEA9Rfkt15
CavquGbnmW0uw18iqc3uGdE/scvSE1gPnPQ9NcwU/LKij1ihnpUvhwXex9Z2D0j
EOuHlyFxbLnFmcNHsQg6RaO2/k7wYf1n/z+QJFFGP11jyN95t72R4oDumD8Yip6
MIY6L61v17KpK1E9hVs21MSNXIRv19783fbsCAWkosGP4HD6vXXD145cp81CeKzH
yWZ+tuLX0WwqN7zF46omy4WxRDXh09DFXyCZCAMFCQPErrnDKNcyj0xvdMyxTJq3
yBwKAYFH0H7V55HNW5SVzszsPP2MUQ==
-----END CERTIFICATE REQUEST-----
  
```

Import CA Response into PSE SAPSSL.pse [Import](#) [Help](#)



```
-----BEGIN CERTIFICATE REQUEST-----
MIICgjCCAWoCAQAwPTEhMB8GA1UECxMYRG9tYWluIENvbnRyb2wgVmFsaWRhdGVk
MRgwFgYDVQQDEw9tYWlkLmFjdW1lZC5uZXQwggEiMAoGCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCnc5+fyYaTuioBhuSEMB/fuodCPXdkFA77Ty+ZfZtyzJncyhGP
ju6EJwcuGizzb/ajiWGMfbnul4HIpao61CuU9X3Abu+fkNNmHEp4pr1Q+XDimy4O
V/AC4Y6s71znnXic+Tpchr94bvzT/zWnasB8830MpJ4fjzspVlsxKGKt8OafWKHl
gBzWuFVaK5zFqqNocfKxq3ihebWb5ot2Jm1gK7idtAfSqniRLx3W22QNNa1X95oL
9HzC+Go8ghT46SyTeljSzdncCwwjT9y3r9YF76vPaFgpIBgzM2Ryw7MMYEXnb4d
xjHRFTQeOBJAsB/7DPPPkL8x6MyPpAn7RsJ7AgMBAAGgADANBgkqhkiG9woBAQsF
AAOCAQEALXQ/KY5UwsbW+QaHdzDNQd5UXg323yRNsuZCBfx+bo3VOjEA9Rfkt15
CavquGbNnmWouwi8iqc3uGdE/scvsE1gPnPQ9NcwU/LKijihnpUvhWwxegZ2Doj
EOuHLyFxbLnFmcNHsQg6RaO2/K7wYfin/z+QJFFGPijisyN9St72R4oDumD8Yip6
MIY6L61v17KpKIE9hVs21MSNXIRvl9783fbSCAWkosGP4HD6vXXDi4Scp81CeKzM
yWZ+tuLXOWwqN7zf46omy4WNxrXDho9DfXyCZCAMFCQPErnDKNCyjoxvdMyxTJqJ
yBwKAYfHoHJV55HNMWSVvzsPP2MUQ==
-----END CERTIFICATE REQUEST-----
```

2.2 Importing CA Response Certificate:

Copy 3rd Party Generated SSL Certificates to the below location.

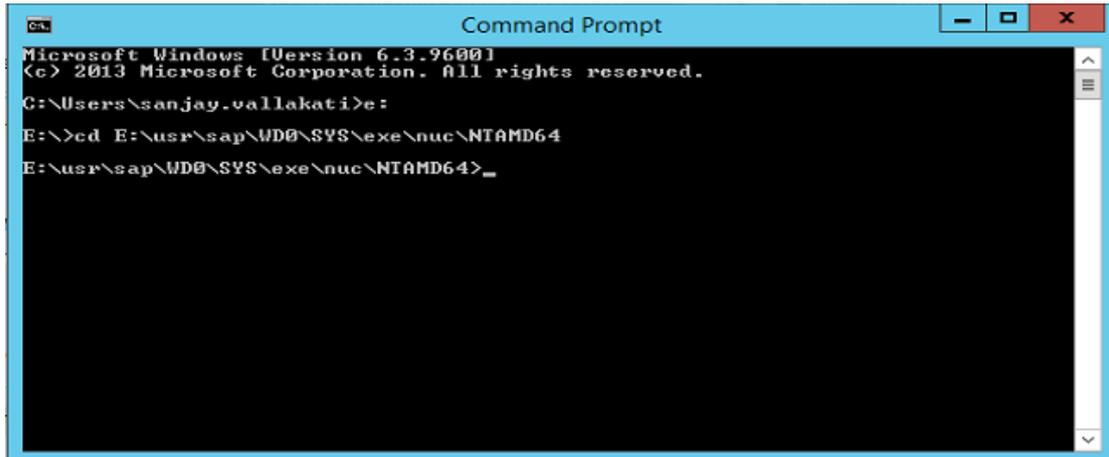
```
E:\usr\sap\WP0\SYS\exe\nuc\NTAMD64
```

Open Command Prompt as Administrator and navigate to below path.

```
E:\usr\sap\WP0\SYS\exe\nuc\NTAMD64
```

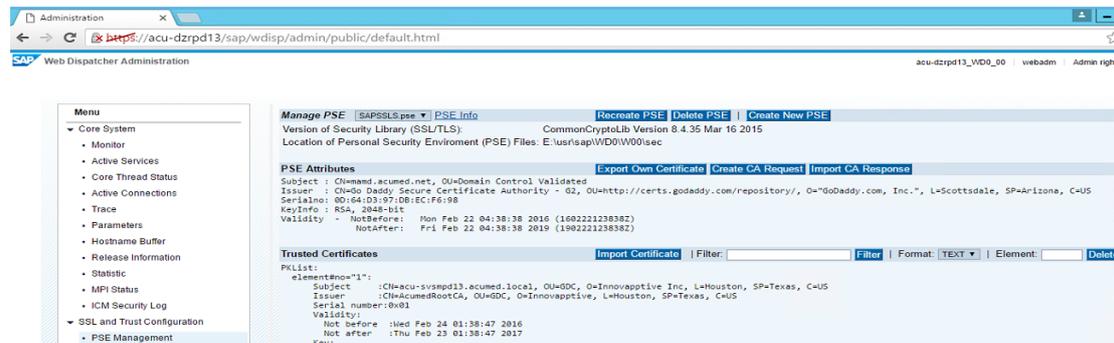
Run below cmd.

```
Sapgenpse import_own_cert -c 2b982dabbd06ce39.crt -r gd_bundle-g2-g1.crt -p
E:\usr\sap\WP0\W00\sec\SAPSSLS.pse
```

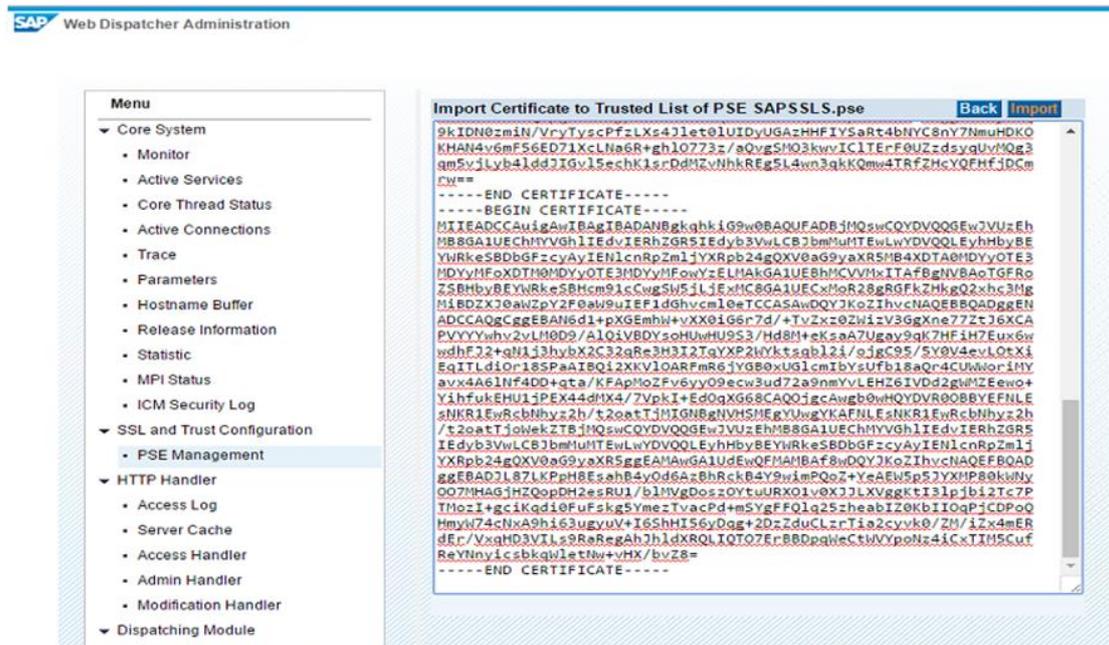


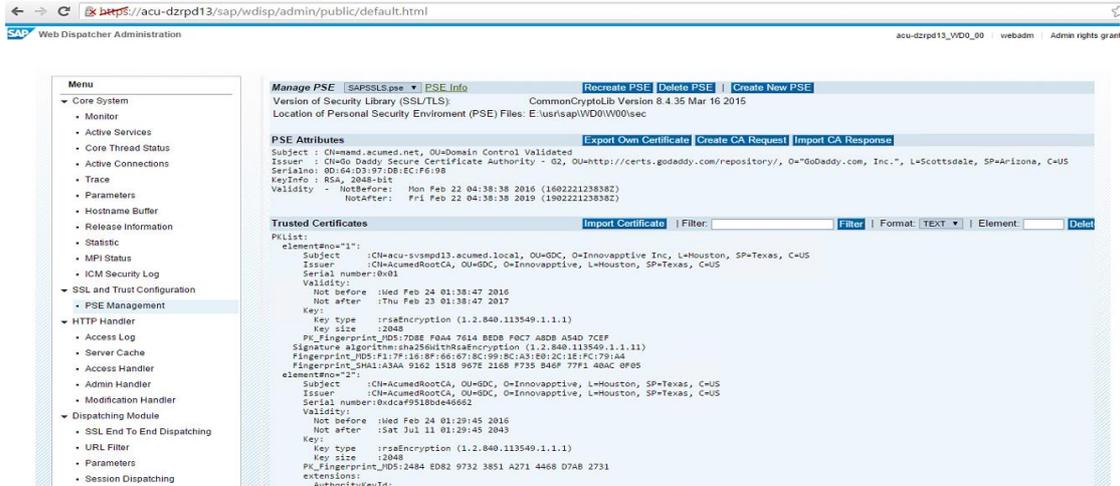
i. Import 3rd Party Root Certificate:

Import 3rd Party Root Certificate:



Click on Import and once Done Restart Web Dispatcher.





The screenshot shows the 'Manage PSE' interface in SAP Web Dispatcher Administration. The left menu is expanded to 'PSE Management'. The main area displays the following information:

- Manage PSE** | SAPSSLS.pse | PSE Info | Recreate PSE | Delete PSE | Create New PSE
- Version of Security Library (SSL/TLS): CommonCryptoLib Version 8.4.35 Mar 16 2015
- Location of Personal Security Environment (PSE) Files: E:\usr\sap\W00\W00\sec
- PSE Attributes**:
 - Subject: CN=amad.acumed.net, OU=Domain Control Validated
 - Issuer: CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, SP=Arizona, C=US
 - Serialno: 80:64:D3:97:DB:EC:1F:98
 - KeyInfo: RSA, 2048-bit
 - Validity: NotBefore: Mon Feb 22 04:38:38 2016 (160222123838Z); NotAfter: Fri Feb 22 04:38:38 2019 (190222123838Z)
- Trusted Certificates**:
 - PKList:
 - element@nov="1":
 - Subject: CN=acu-svsmpd13.acumed.local, OU=GDC, O=Innovapptive Inc, L=Houston, SP=Texas, C=US
 - Issuer: CN=AcumedRootCA, OU=GDC, O=Innovapptive, L=Houston, SP=Texas, C=US
 - Serial number:0x01
 - Validity: Not before: Wed Feb 24 01:38:47 2016; Not after: Thu Feb 23 01:38:47 2017
 - Key: Key size: 2048; Key type: rsaEncryption (1.2.840.113549.1.1.1)
 - PK_Fingerprint_MD5:7D8E F0A4 7614 B8DB F0C7 A8DB A54D 7CEP
 - Signature algorithm:sha256withRsaEncryption (1.2.840.113549.1.1.11)
 - Fingerprint_MD5:F1:7F:18:8F:66:67:8C:99:8C:A3:8B:2C:1E:FC:79:34
 - Fingerprint_SMAL:A3AA 9162 1518 967E 2168 F735 846F 77F1 40AC 0F05
 - element@nov="2":
 - Subject: CN=AcumedRootCA, OU=GDC, O=Innovapptive, L=Houston, SP=Texas, C=US
 - Issuer: CN=AcumedRootCA, OU=GDC, O=Innovapptive, L=Houston, SP=Texas, C=US
 - Serial number:0xdcf9518bde46662
 - Validity: Not before: Wed Feb 24 01:29:45 2016; Not after: Sat Jul 11 01:29:45 2043
 - Key: Key size: 2048; Key type: rsaEncryption (1.2.840.113549.1.1.1)
 - PK_Fingerprint_MD5:2484 ED82 9732 3851 A271 4468 D7AB 2731
 - extensions: AuthorityKeyID:

ii. Import SMP Certificate:

SMP certificate should be imported to - SAPSSLS.pse – Server certificate PSE and SAPSSLC.pse – Client certificate PSE.

We can manage the PSE at “Manage PSE” drop-down menu.

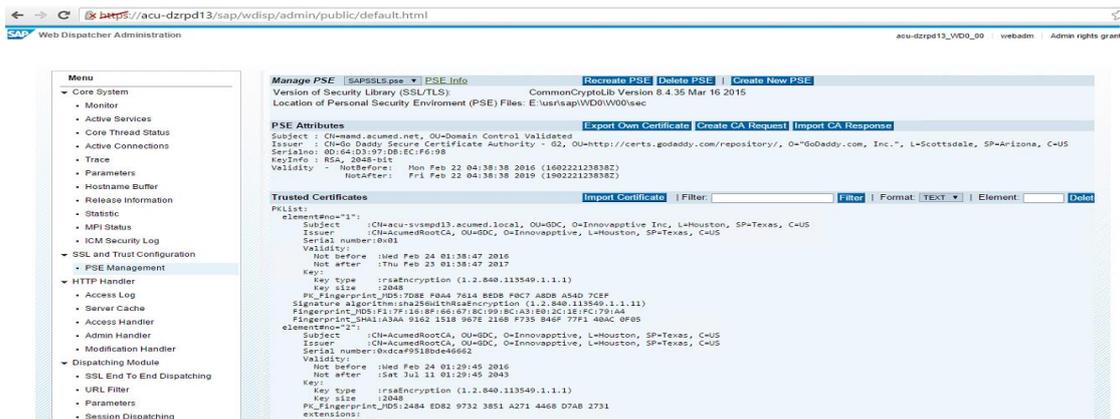
Click on “Import certificate” button and open the certificate using the notepad text editor.

Select all its content in the notepad and copy it.

Paste the content in the empty box which opens after clicking on “Import certificate” button.

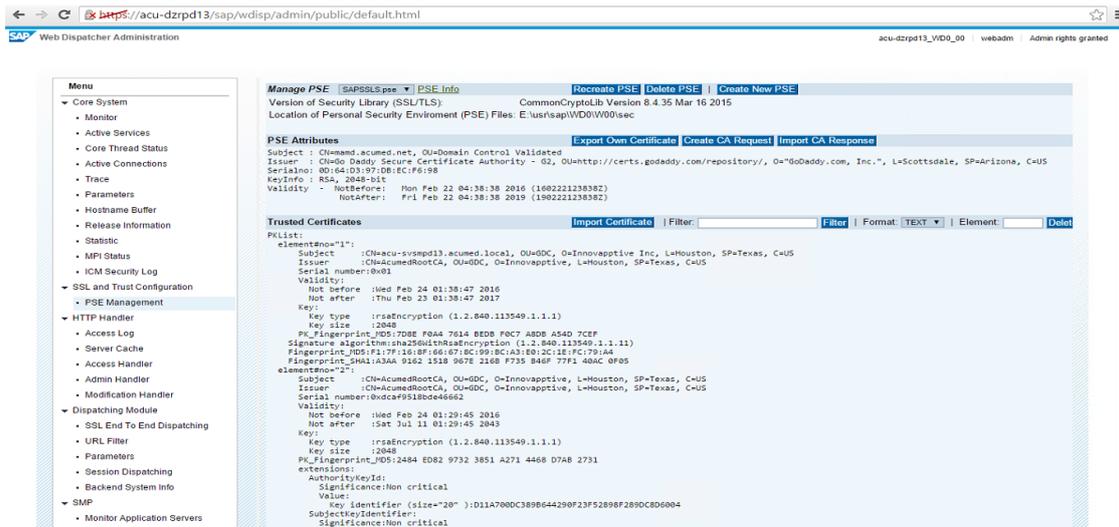
Once you have pasted the content click on import button.

These steps should be performed for both SAPSSLS.pse and SAPSSLC.pse.



This screenshot is identical to the one above, showing the 'Manage PSE' interface in SAP Web Dispatcher Administration. The left menu is expanded to 'PSE Management'. The main area displays the following information:

- Manage PSE** | SAPSSLS.pse | PSE Info | Recreate PSE | Delete PSE | Create New PSE
- Version of Security Library (SSL/TLS): CommonCryptoLib Version 8.4.35 Mar 16 2015
- Location of Personal Security Environment (PSE) Files: E:\usr\sap\W00\W00\sec
- PSE Attributes**:
 - Subject: CN=amad.acumed.net, OU=Domain Control Validated
 - Issuer: CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, SP=Arizona, C=US
 - Serialno: 80:64:D3:97:DB:EC:1F:98
 - KeyInfo: RSA, 2048-bit
 - Validity: NotBefore: Mon Feb 22 04:38:38 2016 (160222123838Z); NotAfter: Fri Feb 22 04:38:38 2019 (190222123838Z)
- Trusted Certificates**:
 - PKList:
 - element@nov="1":
 - Subject: CN=acu-svsmpd13.acumed.local, OU=GDC, O=Innovapptive Inc, L=Houston, SP=Texas, C=US
 - Issuer: CN=AcumedRootCA, OU=GDC, O=Innovapptive, L=Houston, SP=Texas, C=US
 - Serial number:0x01
 - Validity: Not before: Wed Feb 24 01:38:47 2016; Not after: Thu Feb 23 01:38:47 2017
 - Key: Key size: 2048; Key type: rsaEncryption (1.2.840.113549.1.1.1)
 - PK_Fingerprint_MD5:7D8E F0A4 7614 B8DB F0C7 A8DB A54D 7CEP
 - Signature algorithm:sha256withRsaEncryption (1.2.840.113549.1.1.11)
 - Fingerprint_MD5:F1:7F:18:8F:66:67:8C:99:8C:A3:8B:2C:1E:FC:79:34
 - Fingerprint_SMAL:A3AA 9162 1518 967E 2168 F735 846F 77F1 40AC 0F05
 - element@nov="2":
 - Subject: CN=AcumedRootCA, OU=GDC, O=Innovapptive, L=Houston, SP=Texas, C=US
 - Issuer: CN=AcumedRootCA, OU=GDC, O=Innovapptive, L=Houston, SP=Texas, C=US
 - Serial number:0xdcf9518bde46662
 - Validity: Not before: Wed Feb 24 01:29:45 2016; Not after: Sat Jul 11 01:29:45 2043
 - Key: Key size: 2048; Key type: rsaEncryption (1.2.840.113549.1.1.1)
 - PK_Fingerprint_MD5:2484 ED82 9732 3851 A271 4468 D7AB 2731
 - extensions: AuthorityKeyID:



The screenshot shows the SAP Web Dispatcher Administration web interface. The browser address bar displays `https://acu-dzrpd13/sap/wdisp/admin/public/default.html`. The page title is "Web Dispatcher Administration".

The interface is divided into a left-hand menu and a main content area. The menu includes sections like "Core System", "PSE Management", and "Dispatching Module". The "PSE Management" section is currently selected.

The main content area shows the configuration for a Personal Security Environment (PSE). At the top, there are buttons for "Manage PSE", "SAPSSLS pse", "PSE Info", "Recreate PSE", "Delete PSE", and "Create New PSE". Below this, the "Version of Security Library (SSL/TLS)" is listed as "CommonCryptoLib Version 8.4.35 Mar 16 2015".

The "PSE Attributes" section displays the following information:

- Subject: CN=mand.acumed.net, OU=Domain Control Validated
- Issuer: CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O=GoDaddy.com, Inc., L=Scottsdale, SP=Arizona, C=US
- Serial number: 0x81
- Validity: Not before: Mon Feb 22 04:38:38 2016 (1682221238382), Not after: Fri Feb 22 04:38:38 2019 (1902221238382)

Below the PSE attributes, there is a "Trusted Certificates" section with a table of certificates. The table has columns for "elementno", "Filter", "Format", and "Delete". Two certificates are listed:

elementno	Filter	Format	Delete
1		TEXT	
2		TEXT	

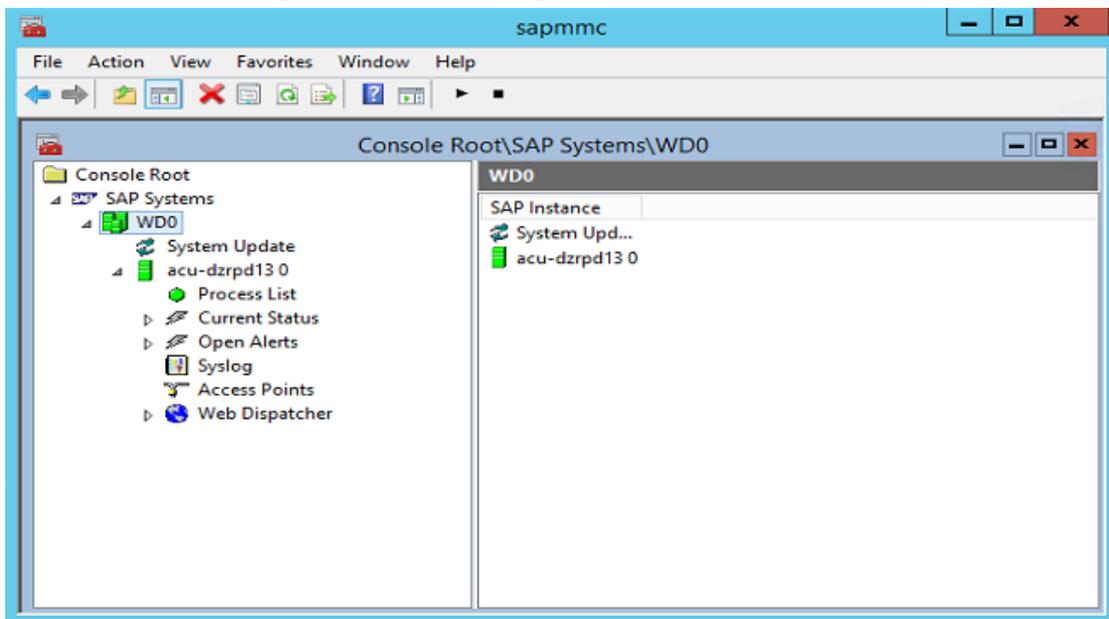
The details for the first certificate (elementno=1) are as follows:

- Subject: CN=acu-sysmp13.acumed.local, OU=ODC, O=Innovapptive Inc, L=Houston, SP=Texas, C=US
- Issuer: CN=AcumedRootCA, OU=ODC, O=Innovapptive, L=Houston, SP=Texas, C=US
- Serial number: 0x81
- Validity: Not before: Wed Feb 24 01:38:47 2016, Not after: Thu Feb 23 01:38:47 2017
- Key: Key type: rsaEncryption (1.2.840.113549.1.1.1), Key size: 2048
- PK_Fingerprint_MD5: 7D8E F044 7614 B8D8 F0C7 AB08 A54D 7CEP
- Signature algorithm: sha256withRSAEncryption (1.2.840.113549.1.1.11)
- Fingerprint_MD5: F17F 182F 686E 78C1 998C A31B 12C1 2E9C 79A4
- Fingerprint_SHA1: 9362 1158 907E 2168 F735 846F 77F1 40AC 0F05

The details for the second certificate (elementno=2) are as follows:

- Subject: CN=AcumedRootCA, OU=ODC, O=Innovapptive, L=Houston, SP=Texas, C=US
- Issuer: CN=AcumedRootCA, OU=ODC, O=Innovapptive, L=Houston, SP=Texas, C=US
- Serial number: 0x0ca99110e46652
- Validity: Not before: Wed Feb 24 01:29:45 2016, Not after: Sat Jul 11 01:29:45 2043
- Key: Key type: rsaEncryption (1.2.840.113549.1.1.1), Key size: 2048
- PK_Fingerprint_MD5: 2484 ED82 9732 3851 A271 4468 D7AB 2731
- extensions: AuthorityKeyId: Significance: Non critical, Value: Key Identifier (size=20): D11A7080DC389B644290F23F52898F2890C8D6004, SubjectKeyIdentifier: Significance: Non critical

Once Certificates are imported Restart WebDispatcher.



The screenshot shows the SAP MMC (Maintenance Console) interface. The window title is "sapmmc". The menu bar includes "File", "Action", "View", "Favorites", "Window", and "Help".

The main area displays a tree view of the system configuration. The "Console Root" is expanded to show "SAP Systems". Under "SAP Systems", the "WDO" system is selected. The right-hand pane shows the configuration for the "WDO" system, including a "SAP Instance" section with the instance name "acu-dzrpd13 0".

The tree view shows the following structure:

- Console Root
 - SAP Systems
 - WDO
 - System Update
 - acu-dzrpd13 0
 - Process List
 - Current Status
 - Open Alerts
 - Syslog
 - Access Points
 - Web Dispatcher

Maintain Profile parameters for WebDispatcher to redirect to SMP.

Path: E:\usr\sap\WDO\SYS\profile

```

WD0_W00_acu-dzrpd13 - Notepad
File Edit Format View Help
SAPSYSTEMNAME = W00
SAPGLOBALHOST = acu-dzrpd13
SAPSYSTEM = 00
INSTANCE_NAME = W00
DIR_CT_RUN = $(DIR_EXE_ROOT)\$(OS_UNICODE)\NTAMD64
DIR_EXECUTABLE = $(DIR_CT_RUN)
DIR_PROFILE = $(DIR_INSTALL)\profile
_PF = $(DIR_PROFILE)\W00_W00_acu-dzrpd13
SETENV_00 = PATH=$(DIR_EXECUTABLE);%PATH%

wdisp/ssl_auth=0

#-----
# Back-end system configuration
#-----

wdisp/system_0 = SID=SMP, SSL_ENCRYPT=1, EXTSRV=https://acu-svsmpd13.acumed.local:8081, SRCSRV=*.443, SRCURL=/, STICKY=true

#-----
# Configuration of maximum number of concurrent connections
#-----
icm/max_conn = 2000
#-----
# Tuning parameters that usually do not need to be adjusted
#-----
icm/max_sockets = ($(icm/max_conn) * 2)
icm/req_queue_len = 500
icm/min_threads = 10
icm/max_threads = 50
mpi/total_size_MB = (min(0.06 * $(icm/max_conn) + 50, 2000))
mpi/max_pipes = ($(icm/max_conn) * 2)
wdisp/HTTP/max_pooled_con = ($(icm/max_conn))
wdisp/HTTPS/max_pooled_con = ($(icm/max_conn))
ssl/server_cache_size = (min($(icm/max_conn) * 4, 100000))
#-----
# SAP Web Dispatcher Ports
#-----
icm/server_port_0 = PROT=HTTPS,PORT=443
icm/server_port_1 = PROT=HTTP,PORT=8000

#-----
# SSL Cipher Suites
#-----
  
```

Import the SAP Mobile Platform Server certificate and Root CA into the Web Dispatcher trust store

1. Start the Web Administration interface for SAP Web Dispatcher.
2. Under SSL and Trust Configuration, choose PSE Management.
3. From the Manage PSE drop-down list, choose the client PSE (SAPSSLC.pse).
4. Under Trusted Certificates, choose Import Certificate.
5. Using a text editor, open the CA certificate used to sign the SAP Mobile
6. Platform server certificate. Copy and paste the contents of the certificate into the box and import the certificate
7. Repeat the same procedure for Trusting SMP certificate also. If you are using a .pfx certificate we need to convert to .cer(base 64 format)
8. Once imported the Root CA/Intermediate Certificates in Web Dispatcher
9. Repeat the same steps to import the certificates in SAPSSLA.pse and a.SAPSSLS.pse
10. Restart the web dispatcher.
11. Now test the Web Dispatcher redirecting to SMP
12. The success full redirecting screen as below



Reference Links:

http://help.sap.com/saphelp_nw73/helpdata/en/48/3d993fb08c72d1e10000000a42189c/content.htm

http://help.sap.com/saphelp_banking60/helpdata/en/03/e301e249744a32adc6d23aff1f287c/content.htm