

Compliance Now

CN Suite Add-on Installations Guide

Table of Contents

INTRODUCTION	4
ADD-ON COMPATIBILITY	5
INSTALLATION REQUIREMENTS.....	5
INSTALLATION PLAN	6
COMMON INSTALLATION TASKS	7
Install add-on.....	7
Signed and Unsigned Packages	8
Configure profile parameters	9
Single Sign-On	9
Other parameters	10
Activate ICF services	10
Selection screen	10
Activate services	11
Generate roles.....	12
CONNECTING SAP TO THE COMPLIANCENOW SERVER	14
Using HTTPS for communication	14
SAP Cryptolib	14
Check installed cryptographic software.....	14
Installation	15
Configure STRUST	16
Create SSL Server PSE	16
Create SSL Client (Standard) PSE.....	16
Create APM identity.....	16
Create APM PSE	16
Add web server certificate to APM PSE	16
Activate HTTPS	19
Restart ICM.....	19
Start HTTPS service	19
Add profile parameter for HTTPS service	20
Obtain required information.....	21
Configure RFC destination.....	21
Technical Settings tab	21
Logon & Security tab.....	22
Special Options tab	23
Connection test.....	24

CONNECTION TO SAP USING HTTP OR HTTPS.....	25
APM Destination table.....	25
Add an entry.....	26
Implemented BAdIs and exits for Access Control	27
BAdI.....	27
New BAdI for 7.31+	27
Exits.....	27
BACKGROUND JOB PROGRAMS.....	28
The data collector execution.....	28
Schedule data collector jobs	28
Programs for every system.....	29
UM ONLY - Usage Monitor dashboard generation	30
AC ONLY – Access Control dashboard generation	30
Additional programs.....	30
Reset after client copy or ad hoc	30
Monitoring.....	30
AC ONLY - Enable role assignment after AC workflow approval.....	31
OPTIONAL CONFIGURATION TASKS.....	32
Alternative tcodes	32
Create new transaction code	32
Add record to /APPLISOL/APMTCD table	32
Remote logon	34
Special configuration parameters	35
UM_NO_EMAIL_ADDRESS	35
ADD-ON UNINSTALLATION.....	36
Backup	36
Uninstall add-on.....	36
RFC destination APM_WEB	36
Entries in SSM_CUST.....	37

Introduction

This documentation guides you through the required installation steps and tasks that are common to all implementation scenarios.

Any comments or questions Mail: support@compliancenow.eu or call: +45 8817 8118.

Add-on Compatibility

The compatibility between SAP versions and the ComplianceNow Add-on is shown in the table below.

Add-on file name	SAP_BASIS version / Add-on description	7.00	7.01	7.02	7.31	7.40	7.50	7.51	7.52	7.53	7.54	7.55
APPLIAPM_520_06-BASIS_700-Install.sar	Add-on 5.2 SP06 for SAP_BASIS 7.0x	X	X	X								
APPLIAPM_520_06-BASIS_731-Install.sar	Add-on 5.2 SP06 for SAP_BASIS 7.31				X							
APPLIAPM_520_06-BASIS_740-Install.sar	Add-on 5.2 SP06 for SAP_BASIS 7.40 & 7.5x					X	X	X	X	X	X	X

SAP_BASIS 7.00 requires SP 27 or higher.

SAP_BASIS 7.02 requires SP 12 or higher.

Installation requirements

SPAM version at least 55 must be installed on the SAP system before installing

CRITICAL: If installing a new add-on or upgrading from an SP earlier than SP09, the first step is to install or upgrade to SP09.

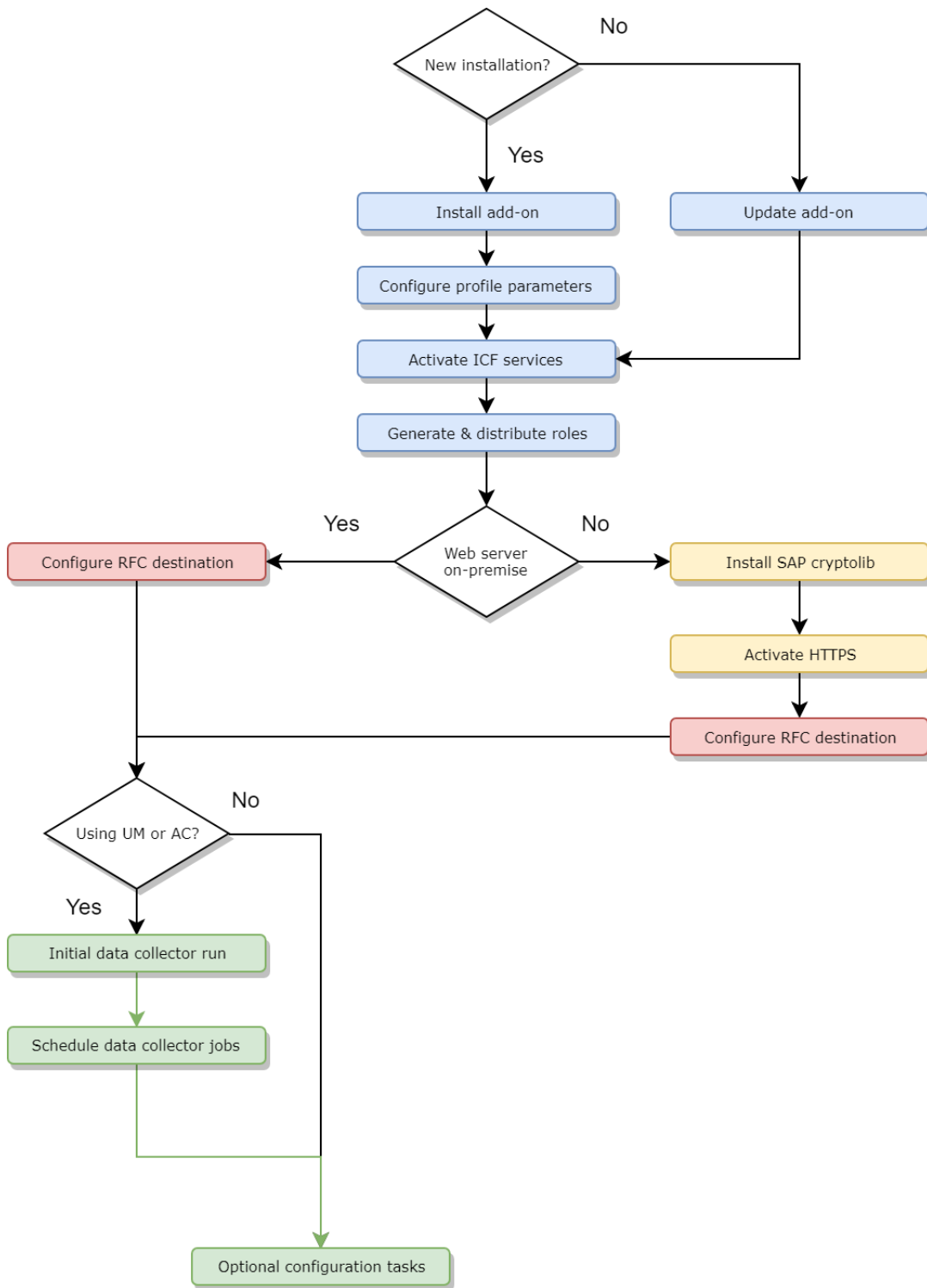
Afterwards, perform a separate upgrade to SP12. Do not perform the complete upgrade in one step!

Please consult the software download site for latest installation/upgrade details:

<https://compliancenow.eu/en/software-download/>

Installation Plan

Consult the below flow-chart to determine which sections of this installation guide are relevant for your installation.



Common installation tasks

This section describes the required installation tasks that are common to all implementation scenarios.

Install add-on



The technical name of the ABAP add-on is APPLIAPM. It is provided in a .SAR file with the following naming convention:

```
APPLIAPM_xxx_yy-BASIS_zzz-Install.sar
```

where *xxx* is the version of the add-on, *yy* is the support package level of the add-on, and *zzz* is the SAP_BASIS version required by the add-on.



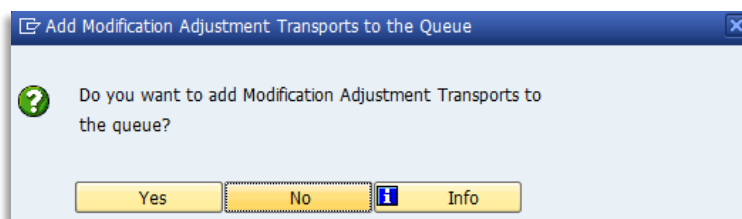
Install the add-on via transaction SAINT in client 000 of the SAP system. Use the provided .SAR file corresponding to the system's SAP_BASIS version.



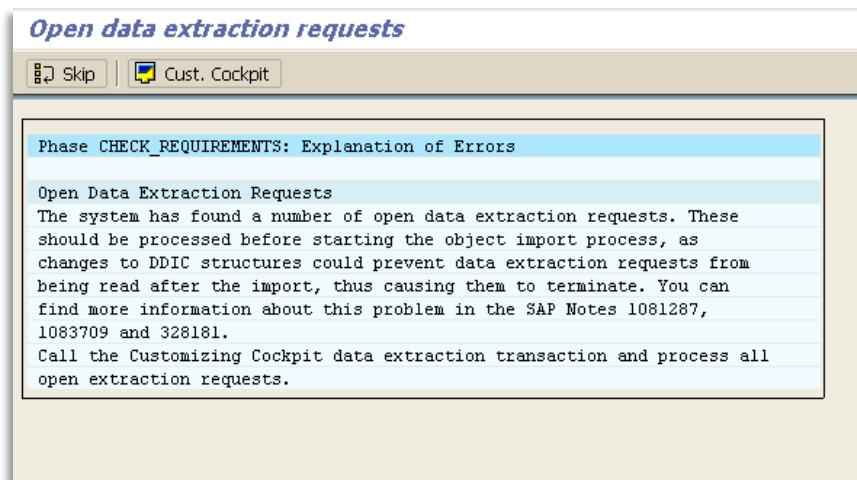
Always install the highest support package available in the .SAR file.



If you are asked if you want to add Modification Adjustment Transports to the queue, then answer "No":



During the CHECK_PREREQUISITES phase of the add-on installation, a warning may be displayed indicating potential problems with open BW/BI QRFC queues or Open Data Extraction Requests:



This is a generic warning, but since the APM add-on does not interact with any such queues or requests, the warning may be safely ignored. Choose “Skip”.

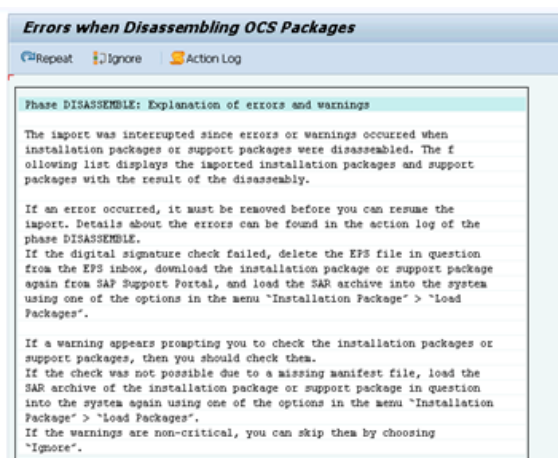
Signed and Unsigned Packages

Applications are now checked for the digital signature during installation and updates as of 2017 or SPAM/SAINT version 66.

1. Signed Packages → Packages having digital signatures
2. Unsigned packages → These have been archived or do not have new releases

The digital signature on each package that SAP releases will be checked during the DISASSEMBLE phase.

During installation or upgrading, you will receive the following error if you have any unsigned packages.



Refer <https://me.sap.com/notes/2687814> for resolution.

Configure profile parameters

Single Sign-On

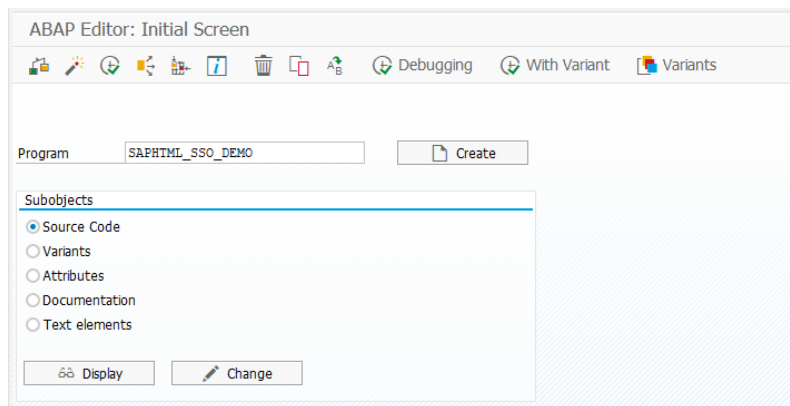


Set the following profile parameter values in order to enable internal single sign-on between the SAPGUI session and the browser which is embedded in the APM transactions.

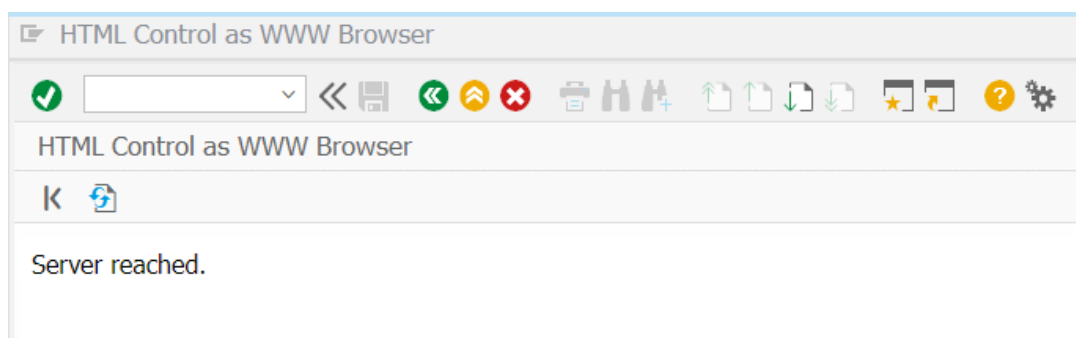
```
login/create_sso2_ticket = 2
```

```
login/accept_sso2_ticket = 1
```

Test the SSO configuration by executing the program SAPHTML_SSO_DEMO in transaction SE38.



The program should execute and display the following without prompting for additional credentials:



Refer to SAP Note [817529 Checking the SSO configuration](#) for further troubleshooting information.

Other parameters



Check the setting of the following profile parameters in transaction RZ10.

auth/new_buffering = 4

This must be set to 4 for APM's test container functionality to function correctly.

login/ticket_only_to_host = 1

If this parameter is not set correctly, users may receive additional logon prompts when switching between multiple APM sessions involving different SAP systems.

Activate ICF services

The ICF services associated with the APPLIAPM add-on must be activated in SICF for the CCSuite transactions to work.

Selection screen



Start transaction SICF and fill in the selection screen as follows:

Filter for Calling ICF Hierarchy	
Hierarchy Type	SERVICE
Virtual Host	
Service Path	
Service Name	APPLIAPM
Reference Service	
Description	
Language	English

Then press Execute.

Activate services



In the following screen, right-click the appliapm entry under default_host and choose “Activate Service” from the menu:

The screenshot shows the 'Define Services' window. At the top, there are buttons for 'Create Host/Service', 'External Aliases', and 'System Monitor Inactive'. Below is the 'Filter Details' section with fields for 'Virtual Host', 'Service Path', 'ServiceName' (containing 'APPLIAPM'), and 'Description'. There are also buttons for 'Apply', 'Reset', and 'Fine-Tune'. The main area shows a tree view of 'Virtual Hosts / Services' with 'default_host' expanded to 'appliapm'. A context menu is open over 'appliapm', listing various actions. The 'Activate Service' option is highlighted with a green box.



In the following dialog, click the second “Yes” button to activate the service as well as the underlying services:

The screenshot shows a dialog box titled 'Activation of ICF Services'. The main text asks 'Do you want to activate service /default_host/appliapm?'. At the bottom, there are four buttons: 'Yes', 'Yes' (highlighted with a green box), 'Info', and 'Cancel'.

Generate roles



A number of roles are delivered as part of the APPLIAPM add-on. These roles need to be generated in each client where the suite is to be used.



Start transaction PFCG and choose Utilities -> Mass generation from the menu. Enter /APPLISOL/* in the "Role" field and check the "Generate automatically" field:

Roles: Mass generation of profiles

Which roles do you want to output?

- Roles with Non-Current Profiles
- Also Roles to Be Compared
- Also Roles with no Authorization Data
- All Roles
- Roles with Current Profiles for New Generation

Additional restrictions

Role	/APPLISOL/*	to		
Last changed by		to		

Presentation in the list

- Display Data When Created and Changed
- Display Role Texts

Generate all profiles to be generated?

- Generate automatically

Click "Execute" and click "Online" in the dialog:

Generate authorization profiles

No. of profiles: 1

In the Backg Online Cancel

No. of profiles may vary.

Generate Authorization Profiles from Roles (No Dialog)

Role	created	changed	Status
/APPLISOL/DATAADMIN	07.11.2018	31.05.2023	Profile generated

You should see the following confirmation screen:

Generate Auth. Profiles From Roles w/o dialog			
Role	Created	Changed	Status
/APPLISOL/APMCOCKPIT	09.01.2013	20.11.2013	Profile generated
/APPLISOL/APMPROJ	25.09.2007	20.11.2013	Profile generated
/APPLISOL/APMSU53	09.01.2013	20.11.2013	Profile generated
/APPLISOL/APM_ALL	00.00.0000	20.11.2013	Profile generated
/APPLISOL/APM_DISP	12.08.2010	20.11.2013	Profile generated
/APPLISOL/APM_TC	25.09.2007	20.11.2013	Profile generated
/APPLISOL/APM_TC_PARENT	25.09.2007	20.11.2013	Profile generated
/APPLISOL/APM_TC__SASRE	18.10.2011	20.11.2013	Profile generated

Connecting SAP to the ComplianceNow server

Using HTTPS for communication

This section describes the steps required to set up the communication between the APPLIAPM add-on and the ComplianceNow web server.

If you require the communication between SAP and the ComplianceNow server to be encrypted and communicate using HTTPS, please follow these instructions to either ensure HTTPS is possible or to install and configure HTTPS.

SAP Cryptolib



A secure, encrypted connection is required when connecting your SAP system to ComplianceNow Solutions' SaaS web server. This is accomplished using HTTPS. In order to enable HTTPS, you must make sure the SAP Cryptographic Library (SAPCRYPTOLIB) is installed or install it yourself.

In newer SAP systems this library is installed by default.

Check installed cryptographic software



Check the currently installed cryptographic software by executing program SSF02 in SE38 with Function selection = Determine version:

SSF Test Program

Function selection:

- Determine version
- Determine properties
- Signing
- Add signature
- Verify
- Encrypt
- Decrypt
- Calculate hash value



When SAPCRYPTOLIB is correctly installed, the program will display the following:

```

SSF Test Program
-----
SSF Test Program
-----
Version          (on application server)
-----
Result:  SSF_API_OK

Version information:
-----
SSFLIB Version 1.840.40 ; CommonCryptoLib (SAPCRYPTOLIB) Version 8.4.41 (+MT) ##Copyright (c) SAP, 2011-2015##compiled for windows-x86-64##
    
```

Installation



Refer to the following SAP Notes to obtain the correct version of SAPCRYPTOLIB for your server platform:

- [397175 - SAP Cryptographic Software - Export control](#)
- [1375378 - Select the right version of an SAP security toolkit](#)



Complete steps 1 and 2 in [SAP Note 510007](#) to install and configure SAPCRYPTOLIB. Most of the remaining steps described in this note are not necessary, and those that are described in detail in the following.

Configure STRUST

The certificate generated by/for the ComplianceNow server must be trusted by SAP and must be imported into STRUST. You can either create a specific PSE for the ComplianceNow server or use an existing PSE. The steps for uploading the certificate are the same.

Create SSL Server PSE

If the SSL Server PSE has not already been created, it will be displayed as follows:



• ✖ SSL server Standard

In this case, right-click the PSE and choose Create. Accept the values suggested by the system. Afterwards, the PSE should be displayed as follows:

▼ 📁 SSL server Standard
• 🟢 ecc604_I64_00

Create SSL Client (Standard) PSE



Create the SSL Client (Standard) PSE in the same way as the SSL Server PSE, accepting the values suggested by the system. Here it is also possible to use an existing PSE.

Create APM identity



Select Environment -> SSL Client Identities from the menu.

Create a new entry with the following field values:

SSL Client	APM
Description	APM
Active	<input checked="" type="checkbox"/>



Save changes. You will be prompted to add the change to a transport request.

Create APM PSE



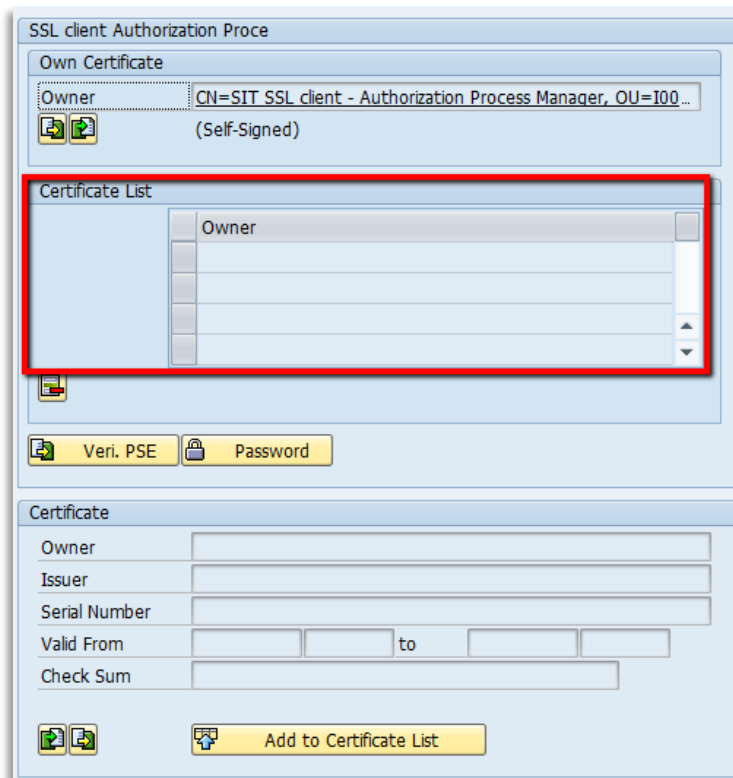
When you return to the main STRUST screen, a new APM PSE will be displayed in the tree. Right-click this and choose Create.


Once again, accept the values suggested by the system.

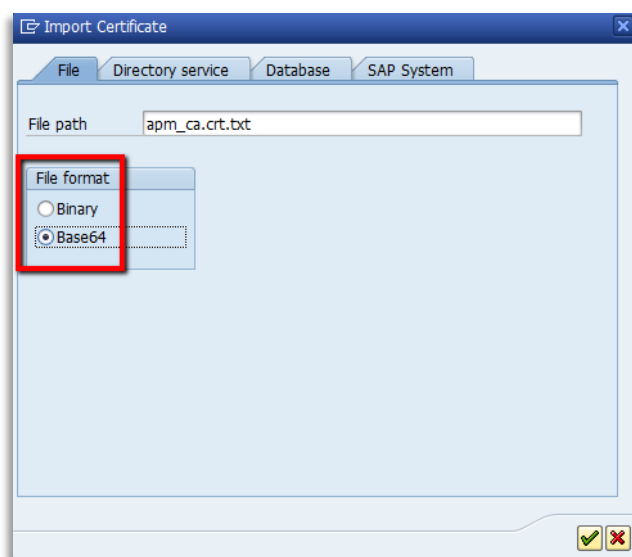
Add web server certificate to APM PSE



Double-click the APM PSE. It should display the PSE with an empty certificate list on the right-hand side of the screen:



Press the Import Certificate  button in the lower left-hand corner and browse to the path of the certificate file provided by ComplianceNow Solutions, set File format to Base64, and press Enter:



The certificate is now shown in the lower right-hand side of the screen:

SSL client Authorization Proce

Own Certificate

Owner: CN=SIT SSL client - Authorization Process Manager, OU=I00... (Self-Signed)

Certificate List

Veri. PSE Password

Certificate

Owner	CN=thawte Primary Root CA, OU="(c) 2006 thawte, Inc. - Fo...
Issuer	CN=thawte Primary Root CA, OU="(c) 2006 thawte, Inc. - Fo...
Serial Number	344ED55720D5EDEC49F42FCE37DB2B6D
Valid From	17.11.2006 00:00:00 to 16.07.2036 23:59:59
Check Sum	8C:CA:DC:0B:22:CE:F5:BE:72:AC:41:1A:11:A8:D8:...

Add to Certificate List



Press the Add to Certificate List button to add the certificate to the PSE. It is now displayed in the middle right-hand side of the screen:

SSL client Authorization Proce

Own Certificate

Owner: CN=SIT SSL client - Authorization Process Manager, OU=I00... (Self-Signed)

Certificate List

Owner	CN=thawte Primary Root CA, OU="(c) 2006 thawte, Inc. - Fo...
-------	--

Veri. PSE Password

Certificate

Owner	CN=thawte Primary Root CA, OU="(c) 2006 thawte, Inc. - Fo...
Issuer	CN=thawte Primary Root CA, OU="(c) 2006 thawte, Inc. - Fo...
Serial Number	344ED55720D5EDEC49F42FCE37DB2B6D
Valid From	17.11.2006 00:00:00 to 16.07.2036 23:59:59
Check Sum	8C:CA:DC:0B:22:CE:F5:BE:72:AC:41:1A:11:A8:D8:...

Add to Certificate List

Save changes and exit STRUST.

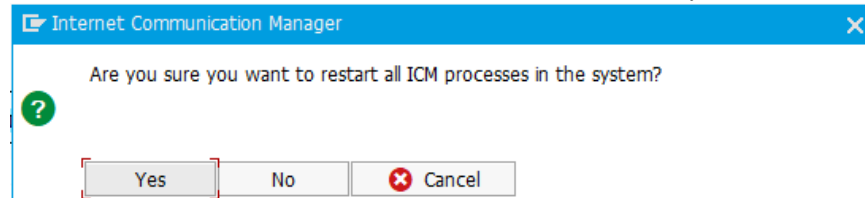
Activate HTTPS

Start transaction SMICM.

Restart ICM



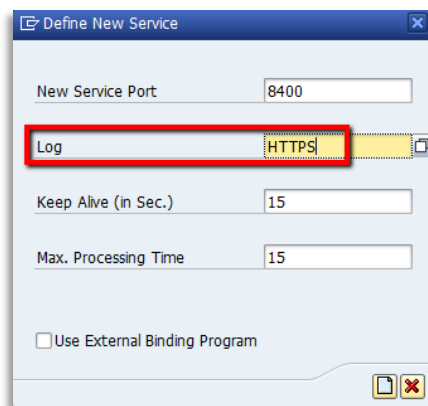
If you have made changes to STRUST, restart the ICM by choosing Administration -> ICM -> Exit Soft -> Global from the menu. Answer Yes when asked if you want to restart ICM processes:



Start HTTPS service



Choose Goto -> Services then Service -> Create from the menu. Define the HTTPS service as follows:



Usually, you can use the Service Port number that the system suggests. Make a note of this port number.

The Service Display screen should now display the active HTTPS service:

No.	Log	Service Name/Port	Host Name	Keep Alive	Proc.Timeo	Actv	External Bind
1	HTTP	8000	apm-demo.applicon.lo	30	60	✓	
2	SMTP	0	apm-demo.applicon.lo	30	60	✓	
3	HTTPS	8400	apm-demo.applicon.lo	30	60	✓	

Make a note of the service number (No.) assigned to the HTTPS service.

Note: When the SAP services are restarted, the SMICM modifications will be undone. Ensure that the profile parameter that is listed in the next step has been maintained.

Add profile parameter for HTTPS service



In order for the HTTPS service to start each time the SAP system starts, a profile parameter must be created containing the parameters of the service.



Go to RZ10 and add a profile parameter named:

`icm/server_port_n`

where *n* is one less than the service number assigned to the HTTPS service in the previous step, e.g. `icm/server_port_2`. Set the parameter's value to:

```
PROT=HTTPS,PORT=pp$$
```

where *pp* are the first 2 digits of the service port assigned to the HTTPS service in the previous step, e.g. 84\$\$.

Obtain required information

Obtain the following information from the web server administrator. If the server is hosted by a third party or by ComplianceNow, this information will be delivered by them.



<host> - host name of the web server

<port> - port number that the web server is listening on, usually 80 (HTTP) or 443 (HTTPS)

<path> - path to the ComplianceNow Suite application on the web server, usually "/" but it should reflect the actual application path within the Apache Home directory.

Configure RFC destination

Start transaction SM59 and create a new RFC destination with the following configuration values.



Technical Settings tab

Field	Value
RFC Destination	APM_WEB
Connection Type	G
Description	APM web server
Target Host	<host>
Service No.	80 or 443
Path Prefix	<path>

RFC Destination APM_WEB

Connection Test

RFC Destination:

Connection Type: HTTP Connection to External Serv Description

Description

Description 1:

Description 2:

Description 3:

Administration | **Technical Settings** | Logon & Security | Special Options

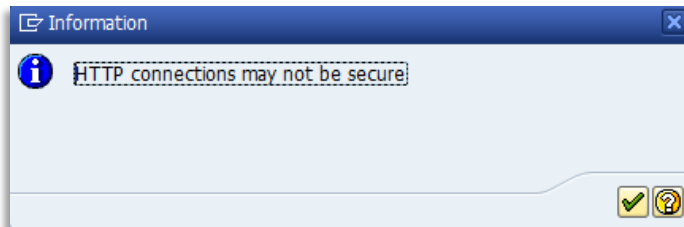
Target System Settings

Target Host: Service No.:

Path Prefix:



Press Enter after entering Connection Type and Description 1, and ignore the following warning:



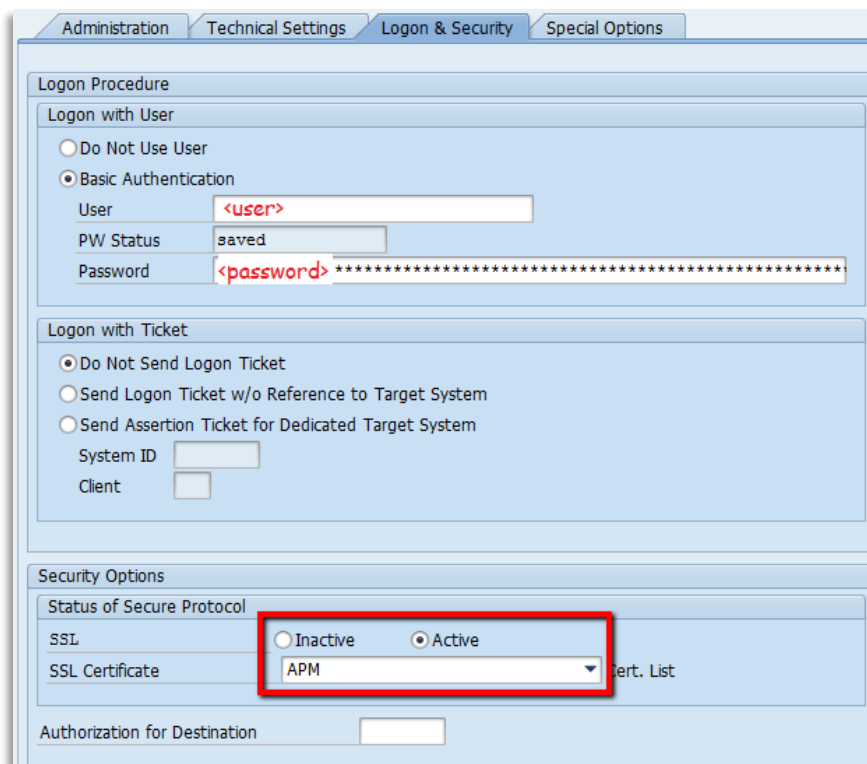
Logon & Security tab



Choose Basic Authentication and fill in the User and Password fields using the information provided by the server team.

If you communicate using HTTPS and have configured a certificate in the STUST PSE, activate SSL and choose APM in the Certificate List.

Otherwise leave SSL inactive



Special Options tab



Administration Technical Settings Logon & Security **Special Options**

Timeout

ICM Default Timeout
 No Timeout
 Specify Timeout Timeout in Seconds (1 to 9999999)

HTTP Setting

Status of HTTP Version

HTTP Version HTTP 1.0 HTTP 1.1

Compression Status

Compression Inactive
 Active (Depends on MIME Type)
 Active (Whole Document)

Status of Compressed Response

Compressed Response Yes No

HTTP Cookies

Type of Cookies Acceptance

Accept Cookies No
 Yes (All)
 Input Prompt
 Trigger Event

Connection test



Perform a connection test and verify that the Response Body tab displays something like the following:

Connection Test HTTP Destination APM_WEB

Destination: APM_WEB
Ty.: HTTP Connection to External Server

Test Result | Response Header Fields | **Response Body** | Response Text

Authorization Process Manager[®]

Version	3.3.6 (1176)
Web username	[REDACTED]
Database status	ok
Licensed to	[REDACTED]
APM license	Expires never
UM license	Expires never
Request time (ms)	177.023
Server local time	2013-11-11 19:33:03



To troubleshoot errors, check the ICM trace file in transaction SMICM.

Connection to SAP using HTTP or HTTPS

When users are executing the ComplianceNow applications, The applications are accessing SAP through the HTTP or HTTPS services. By default, the connection is established on the HTTP service. In these instances, it might conflict with the authentication in SAP and the use of SAP logon tickets.

To activate the connection through the HTTPS service, the following steps are required.

APM Destination table

When the application determines which destination for the server it uses, the table /APPLISOL/APMDST is queried.

Table to be searched	/APPLISOL/APMDST	APM Destination
Number of hits	3	
Runtime	0	Maximum no. of hits 500

char120	RFC Destination	Single-Character Indicator	Flag	URL
*	APM_WEB	A	X	https://demo.ccs.ciber.com/appliapm/proxy/
DEFRE-NB16015	APM_WEB_HEALTHCHECK	A	X	https://demo.ccs.ciber.com/appliapm/proxy/
DKCPH-NB17023	APM_WEB_HEALTHCHECK	D	X	

1. The Column “char120” indicates the terminal of the user logged on to the application. If a user’s terminal ID is entered here it is possible to assign a different behaviour than the standard connection. If a wildcard is entered all connections are assigned the base URL.
2. The Column “**RFC Destination**” indicates the name of the SM59 RFC destination to use to connect to the web server. The default RFC destination name is APM_WEB, but this can be changed by assigning a different RFC name.
3. The Column “**Single-Character Indicator**”/”**GUI**” indicates the type of connection from SAP.
 - A Alternate specified base URL as specified in column “URL”.
 - D Direct connection based on RFC destination as specified in the column “RFC Destination”.
 - P ICF proxy from browser
4. The Column “**Flag**”/”**SSO**” should always be assigned an “X”
5. The Column “**URL**”/”**Alternate**” indicates the base URL for the application. The format of the URL is:

<https://<host>:<port>/appliapm/proxy/>

<host> and <port> should be replaced by the actual values of the application listening for connections or a possible web dispatcher.

The default URL used is for the ICF service PROXY.

Virtuelle Hosts / Services	Documentation	Referenz Service
default_host	VIRTUAL DEFAULT HOST	/default_host/sap/bc/bsp/sap/zcrossdomain
appliamp	Authorization Process Manager AppliCon S...	
att	Auto tcode test service	
auth_check	APM Authorization Check	
bootstrap	UI bootstrap	
ping	APM ping	
proxy	APM proxy	
client	Empty node	
Apps	Provides public access to static app content	
tc	APM Test Container Service	
watchdog	APM watchdog	
wf_status	Ciber Access Control Access approval work...	

Add an entry

You will need to manually add an entry to the table /APPLISOL/APMDST.

FIELD	VALUE	
TERMINAL / CHAR20	*	
DESTINATION	APM_WEB	Default RFC destination
GUI / INDICATOR	A	
SSO / FLAG	X	
ALTERNATE / URL	https://<host>:<port>/appliamp/proxy	



Implemented BAdIs and exits for Access Control

The preventive checks in Access Control are implemented via a number of BAdIs and exits in the SAP system.

BAdI

The classic BAdI /APPLISOL/SODUSERCHK for definition HRBAS00INFTY implements preventive checks on assignment of roles to users in SU01 and SU10.

New BAdI for 7.31+

In addition to the above, the new BAdI /APPLISOL/CL_SOD_IDENTITY_CHK for definition BADI_IDENTITY_CHECK implements preventive checks on role assignment changes from SAP_BASIS 7.31 and onwards.

Exits

The following exits must be defined in table SSM_CUST. These exits implement the various preventive checks that are performed when users or roles are changed and/or assigned in SU01/SU10/PFCG.

If using Access Control these entries MUST be added to the SSM_CUST table.

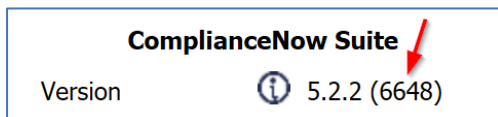
Name	Value
Z_AFTER_PROF_GEN	/APPLISOL/SOD_PFCG_GEN_CHK
Z_BEFORE_BATCH_GEN	/APPLISOL/SOD_PFCG_BATCH_GEN
Z_BEFORE_PROF_GEN	/APPLISOL/SOD_PFCG_BEFORE_GEN
Z_EXIT_USERS_SAVE	/APPLISOL/SOD_PFCG_ASSIGN_CHK
Z_GRC_COLL_ROLE	/APPLISOL/SOD_PFCG_SAVE_CHK

Background Job Programs



This section describes how to set up the background jobs to execute the data collector programs required by Usage Monitor (UM) and Access Control (AC).

This part refers to applications with revision 5507 or higher.



If you have not licensed Usage Monitor or Access Control, please disregard this section entirely.

The data collector execution

The first time the data collector is executed in an SAP system/client, the data collection can be run manually, if you want to collect the data right away. Otherwise schedule it for a recurring execution and wait until the first run has completed.



In SE38, execute the program /APPLISOL/APMUM_URT_COLLECTOR without any parameter values



Since the program may run for some time, we recommend executing it in the background.



This data collector must be performed in each client, from which you wish to collect data.



Always check the result of background jobs and contact your support team or ComplianceNow if any errors are indicated.

Schedule data collector jobs



The data collector programs are intended to run each night in order to ensure that up-to-date data is always available to the applications.

The required authorizations for the user executing the background jobs are contained in the role /APPLISOL/DC_BATCH which is included in the add-on.

Programs for every system

These programs must be scheduled on every system/client from which UM & AC data is to be collected.



In SM36, create a new job to execute the following 2 programs in sequence once each night:

```
/APPLISOL/APMUM_USAGE_COLL
/APPLISOL/APMUM_URT_COLLECTOR
```



The programs do not require any parameters, so no variants should be selected.



There are filters available for the URT (Users, Roles & Transactions) collector which enables specifying which users are to be transferred to the web server for reporting purposes. Any users filtered out in this way will still be analyzed during the Access Control risk analysis.

Create a variant for the program and specify which users or user groups that you want to include in the data collector job.

User selection			
User group	<input type="text"/>	to	<input type="text"/>
User	<input type="text"/>	to	<input type="text"/>

UM ONLY - Usage Monitor dashboard generation

To trigger the necessary background processing for UM that is performed on the ComplianceNow application server, an additional program can be executed manually on an ad hoc basis.



For UM, execute the following program:

```
/APPLISOL/APMUM_DASHBOARD_LOAD
```

No parameters or variant is needed.



Do not schedule this program as a part of the recurring background job as this program is already part of the program /APPLISOL/APMUM_URT_COLLECTOR

AC ONLY – Access Control dashboard generation

To trigger the necessary background processing for AC that is performed on the ComplianceNow application server, an additional program can be executed manually on an ad hoc basis.



For AC, execute the following program:

```
/APPLISOL/AC_DASHBOARD_LOAD
```

No parameters or variant is needed.



Do not schedule this program as a part of the recurring background job as this program is already part of the program /APPLISOL/APMUM_URT_COLLECTOR

Additional programs

Reset after client copy or ad hoc



Whenever a client copy is performed and the SAP system/client data has been overwritten, it is very important to reset the data collector tables in the target client by executing the program. This can also be done on a regular basis to ensure master data is consistent

```
/APPLISOL/APMUM_URT_RESET
```

If this programs has been executed in a system/client, the master data will be resynchronized the next time the program /APPLISOL/APMUM_URT_COLLECTOR is executed.

Monitoring



It is important to monitor the data collector jobs and respond appropriately to any errors that might occur. If the data collector jobs are not executed regularly, there may be gaps in the data available in the UM application, which could result in inaccurate analyses.

Please contact ComplianceNow Solution Center at support@compliancenow.eu for help with problem resolution.

AC ONLY - Enable role assignment after AC workflow approval

This is for Access Control only. In order to assign roles after the AC role assignment workflow has been approved, a program must be executed once the approval has been registered.



For AC, schedule the following program to run as a periodic job after an event is triggered:

`/APPLISOL/AC_ASGN_APPRVD_ROLES`

Schedule the program to run after the following event in SAP:

`/APPLISOL/AC_WF_APPROVED`

General Data	
Job Name	<input type="text" value="/APPLISOL/AC_ASGN_APPRVD_ROLES"/>
Job Class	<input type="text" value="A"/>
Status	<input type="text" value="Finished"/>
Exec. Target	<input type="text"/> <input type="button" value="Spool List Recipient"/>
Job Start	
After Event	
Event	<input type="text" value="/APPLISOL/AC_WF_APPROVED"/>
Parameters	<input type="text"/>
Job Frequency	
Event	<input type="text" value="periodic"/>
	<input type="text"/>
	<input type="text"/>
	<input type="text"/>



The job must be run with a user with right to assign roles and profiles to users.



The program must be setup on **EACH** system/client where Access Control is going to be used to provision rights to users.

Optional Configuration Tasks

This section describes various optional configuration tasks which may or may not be required for your usage scenario. Please discuss the necessity of these with your end users.

Alternative tcodes

It is possible to define custom transaction codes as replacements for the supplied APM transaction codes. For instance, this could be done to allow users to enter ZSU53 instead of /n/APPLISOL/APMSU53 to report an authorization issue.



Create new transaction code

Start SE93 and press the Copy icon:



Enter the name of the existing and new transaction codes, and press Copy:

Select a package and transport request or select Local Object if you do not wish to transport the new transaction code.

Add record to /APPLISOL/APMTCD table





The APM needs to know which standard transaction code a given custom transaction code is a substitute for in order to react correctly when the custom transaction code is started.





Start SE16, enter the table name /APPLISOL/APMTCD and press the Create Entries icon:

Data Browser: Initial Screen




Table Name

Enter the custom and standard transaction codes, and press the Save icon:






    

Table /APPLISOL/APMTCD Insert

Reset

ALTERNATE

APM

Remote logon






Within the APM Authorization Cockpit it is possible to work on issues, tasks and projects across the entire APM system landscape. Actions to be executed in a different system/client from where the Authorization Cockpit is running are initiated via remote logon, where the user is prompted to logon to the remote system.



In order to enable this remote logon functionality, RFC destinations must be maintained in each system from which the Authorization Cockpit is to be executed. The RFC destinations used are of type 3 (R/3 connection) and observe the naming convention

`APM_sid_cli`, where *sid* is the 3-character system id of the remote system and *cli* is the 3-digit client number.

While the RFC destinations may be maintained manually, they can also be maintained automatically from the Authorization Cockpit using the following procedure, provided the user has the required basis authorizations.

1. On each of the target systems *to* which remote logon will be enabled
 - a. logon to any client of the target system
 - b. start the APM Authorization Cockpit (transaction /APPLISOL/APMCOCKPIT)
 - c. in the System Overview, click the server icon () for the system *you are currently logged on to*
 - d. in the right-hand pane (Maintenance of System xyv) click “Add clients to APM landscape” (this has the side-effect of transferring the necessary technical data about this system to the APM server for use in step 2) – no further actions are necessary here
 - e.
2. On each of the source systems *from* which remote logon will be enabled
 - a. logon to any client of the source system
 - b. start the APM Authorization Cockpit (transaction /APPLISOL/APMCOCKPIT)
 - c. in the System Overview, click the server icon () for the system *you are currently logged on to*
 - d. in the right-hand pane (Maintenance of System xyv) click “Manage remote logon connections”
 - e. select the target system(s) to which remote logon is required and click “Create/update RFC destinations” – this will create the RFC destinations, which will subsequently be visible in transaction SM59
 - f. The created RFC connections can be tested by clicking on their test icon ()



In some cases, it may be desirable to modify the settings of the automatically created RFC destinations, e.g. to enable load-balancing or single sign-on.



Special configuration parameters

The configuration table /APPLISOL/APMCFG holds name/value pairs that affect the operation of the APM in different ways. The table is maintained via SE16 or SM30.

The following parameters are available.

UM_NO_EMAIL_ADDRESS

Setting this parameter to 'X' tells the UM data collector *not* to transfer users' e-mail addresses to the APM web server. Consequently, the e-mail addresses will not be available in UM reports.

Add-on Uninstallation

Prior to uninstalling the Add-On, please contact us.



The Add-On can be uninstalled in a standard way as described in SAP Add-On Assembly Kit documentation <https://help.sap.com> → AAK 5.0 → Add-On Uninstallation.

Backup

Perform a system copy in advance and/or to create a backup

Uninstall add-on

Uninstall the add-on **APPLIAPM** via transaction SAINT in client 000 of the SAP system - see installation section “Install add-on”.

The screenshot shows the 'Add-On Installation Tool - Version 7.51/0063' window. It has two tabs: 'Installed Components' and 'Deinstallable components'. The 'Deinstallable components' tab is active, displaying a table with the following data:

Add-On	Release	Level	Hinweis	Beschreibung
APPLIAPM	510_750	0000	1883223	ComplianceNow Suite
GBX01HR	600	0006	2180598	FIORI X1 HCM
GBX01HR5	605	0003	2180598	FIORI X1 HCM
SRA004	600	0009	2131183	Create Travel Request OData Integration

Below the table is a 'Status/Remarks' section with an information icon and the following text:

The overview shows the Add-Ons which can be deinstalled

- Mark the Add-Ons, which you want to deinstall
- Choose [START] to start the deinstallation

At the bottom of the window, there are three buttons: 'Back', 'Start', and 'Cancel'.

RFC destination APM_WEB

Please delete APM_WEB RFC destination in SM59 – see installation section “Configure RFC destination”

Entries in SSM_CUST

Delete the following entries from table SSM_CUST - see installation section "Exits"

Name	Value
Z_AFTER_PROF_GEN	/APPLISOL/SOD_PFCG_GEN_CHK
Z_BEFORE_BATCH_GEN	/APPLISOL/SOD_PFCG_BATCH_GEN
Z_BEFORE_PROF_GEN	/APPLISOL/SOD_PFCG_BEFORE_GEN
Z_EXIT_USERS_SAVE	/APPLISOL/SOD_PFCG_ASSIGN_CHK
Z_GRC_COLL_ROLE	/APPLISOL/SOD_PFCG_SAVE_CHK