



Cloud Connector configuration for Integration Suite Managed Gateway

Bharath Balakrishnan - SAP Ariba Cloud Integration Support

PUBLIC

Confidential Documents:

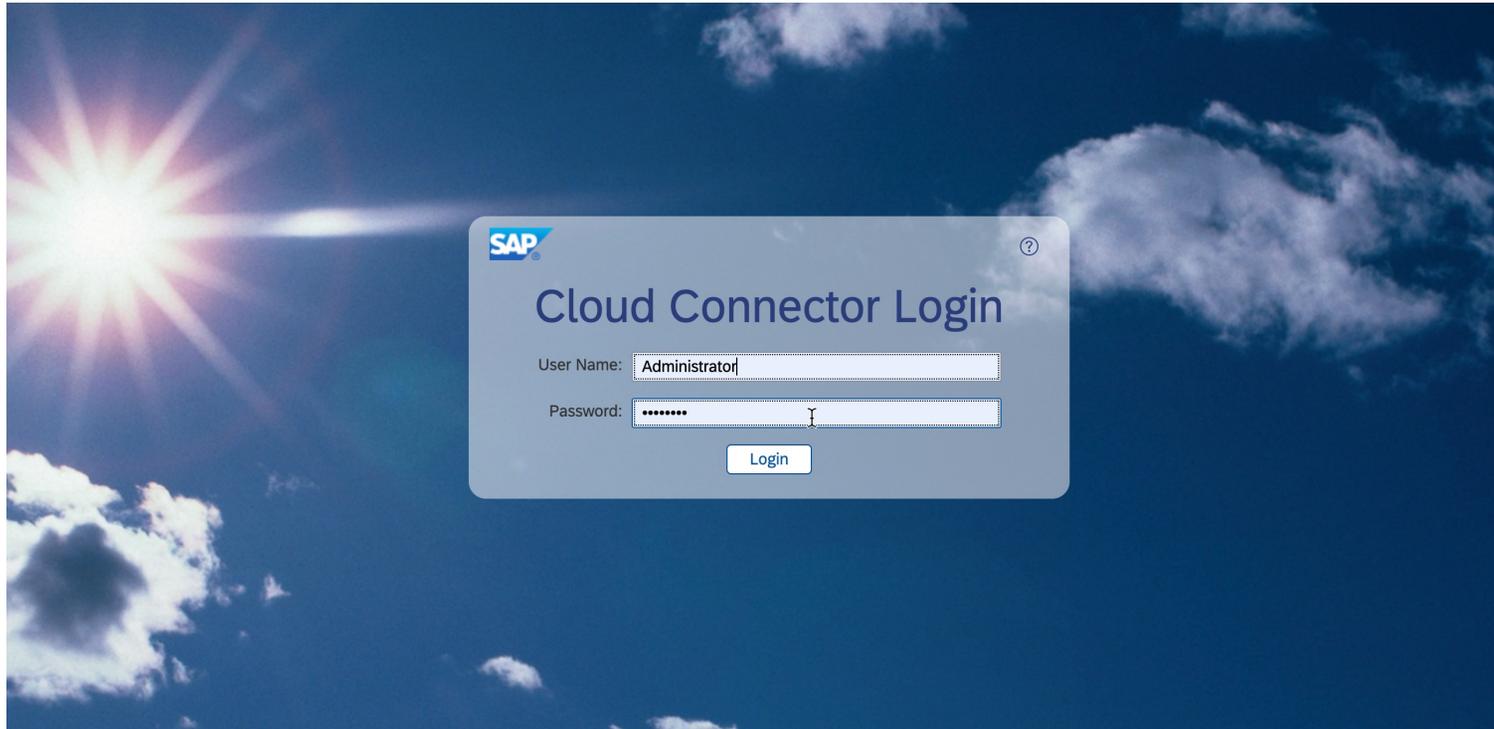
© 2024 Ariba, Inc. All rights reserved. The contents of this document are confidential and proprietary information of Ariba, Inc.



Topics

- Cloud Connector configuration for Integration Suite Managed Gateway
- Whitelist IPs for Integration Suite Managed Gateway -> ERP
- Whitelist IPs for ERP -> Integration Suite Managed Gateway
- Troubleshooting

Once you install cloud connector login with the user credentials provided during the installation. Here I am logging in as administrator



When you login for the first time you will not see any subaccounts in the connector page. You need to add separate sub accounts for test and production system. Click Add Subaccount button.

- Connector
- Security Status
- Alerting
- High Availability
- Hardware Metrics Monitor
- Configuration
- Define Subaccount
- Cloud To On-Premise
- On-Premise To Cloud
- Monitor
- Audits
- Log And Trace Files

Define Subaccount Save ?

Cloud Connector is not configured and remains inoperative unless you define at least one subaccount

First Subaccount

Region: *
Subaccount: *
Display Name:
Subaccount User: *
Password: *
Location ID:
Description:

HTTPS Proxy

Host:
Port:
User:
Password:

- Region Host:** Any customers integrating via Integration Suite Managed Gateway, will use one of the below data centers depending on their location or when the Integration Suite Managed Gateway was activated. If you using Integration Suite Managed Gateway EU, then its **eu1.hana.ondemand.com or EU(Rot)**, if you are using Integration Suite Managed Gateway US, then its **us4.hana.ondemand.com**, if are using Integration Suite Managed Gateway CN, then its **cn1.platform.sapcloud.cn**, If you are using Integration Suite Managed Gateway KSA then its, **sa1.hana.ondemand.com**, If you are using Integration Suite Managed Gateway UAE then its, **ae1.hana.ondemand.com**,

How to know which Integration Suite Managed Gateway data center I am using? Once you enable Integration Suite Managed Gateway in Ariba Network/Ariba Buying/Ariba Sourcing, next to Visit SAP Ariba Cloud Integration Gateway, you will see the data center.

- Subaccount:** We have separate subaccounts for **TEST** and **PRODUCTION** systems for each **DATA CENTER**. Follow the below table to know

Integration Suite Managed Gateway EU (eu1.hana.ondemand.com or EU (Rot))	Integration Suite Managed Gateway US (us4.hana.ondemand.com)	Integration Suite Managed Gateway China (cn1.platform.sapcloud.cn)	Integration Suite Managed Gateway KSA (sa1.hana.ondemand.com)	Integration Suite Managed Gateway UAE (ae1.hana.ondemand.com)
	xf014edd7	r0j327s1ak	vyune65dsw	gxrmsck7oq
aff5426a3	x60abf046	c7rrjwusz0	va2w1i23wr	t5skjep13f
a18a6fc8f				
riph868phi	b3bcoyxwro	v6h7i4po2z	q954q7a4d0	s3wsfj1qe8
a8f3ed22c	x691dbc6d	gegwi7n4kq	w2fi9zn95p	qc7mrw8tvm
ab9e90b64	x1e1a8cfb	g1mgxyvy6e	q8famn5vpc	v011cy26z4
a278d9ec7	x8713dd41	zj358jrvnr		
A508aae51	fnpxlbn69y			
fh7owkbn5n	ald178slao			
t6u5sulpil				
uajqqqv8i3				

3. **Display Name:** You can provide any display name to any value. Here I used Integration Suite Managed Gateway_TEST

4. **Subaccount User/Password:** Provide the Puser value you have received in email when you enable Integration Suite Managed Gateway and the corresponding password.

5. **Location ID:** Provide a location id value here. It can be anything but make sure you provide the same in the Integration Suite Managed Gateway portal connection details and for other subaccounts. Here I am using SAP Integration Suite Managed Gateway

The screenshot shows a web form titled "Add Subaccount". The form contains the following fields and values:

- *Region Host: eu1.hana.ondemand.com
- *Subaccount: aff5426a3
- Display Name: CIG_TEST
- *Subaccount User: P000284
- *Password:
- Location ID: ARIBACIG
- Description: Test CIG connectivity |

At the bottom of the form, there are "Save" and "Cancel" buttons.

In the configuration page, If you want to use any proxy, you can mention that as well. Check with your BASIS/IT consultant if this is required. My proxy is proxy.ariba.com so I used it here. Please use your own proxy server.

The screenshot displays the SAP Cloud Connector Administration interface. The left sidebar contains navigation options: Connector, Security Status, Alerting, High Availability, Hardware Metrics Monitor, Configuration, CIG_PROD, Cloud To On-Premise, On-Premise to Cloud, Monitor, Audits, Log And Trace Files, Important Links, and Legal Information. The main content area is titled 'Configuration' and has tabs for 'USER INTERFACE', 'CLOUD', and 'ON PREMISE'. The 'CLOUD' tab is active. Under 'Connector Info', there is a 'Description' field. The 'HTTPS Proxy' section is highlighted with a red box and contains a configuration popup with the following details: Host: proxy.ariba.com, Port: 8080, and User: (empty). Below this, the 'Cloud User Store' section includes a 'Hosts' table with columns for 'Host Name' and 'Port', and a 'Secure' checkbox. The table currently shows 'No data'. Other fields for 'User Name', 'User Path', and 'Group Path' are also present but empty.

Host Name	Port
No data	

Click on the sub account you created recently and make sure the details you provided in the previous step are reflecting here. This shows a secure tunnel is established between Integration Suite Managed Gateway sub account and the cloud connector.

The screenshot displays the SAP Cloud Connector Administration interface. The top navigation bar includes the SAP logo, the title 'Cloud Connector Administration', and the user 'Administrator'. A left-hand navigation menu lists various options: Connector, Security Status, Alerting, High Availability, Hardware Metrics Monitor, Configuration, and a user profile section with options like Cloud To On-Premise, On-Premise To Cloud, Monitor, Audits, and Log And Trace Files. The main content area shows a subaccount overview for a subaccount named 'ab9e90b64'. The status is 'Operational since August 26, 2022 1:52:08 AM UTC'. The overview includes details such as Region (Europe (Rot)), Region Host (hana.ondemand.com), Subaccount Certificate (Certificate valid until August 26, 2023 1:52:08 AM UTC), and System Certificate. Below this, the 'Disaster Recovery Subaccount' section shows a status of 'Not configured'. The 'Tunnel Information' section at the bottom indicates the tunnel is 'Connected' with a Tunnel ID of 'account:///ab9e90b64/S4CIGPROD' and a Remote Name of 'connectivitynotification.hana.ondemand.com'. Action buttons for Disconnect, Import, Export, and Certificate are visible at the top right of the subaccount overview.

SAP Cloud Connector Administration

Subaccount: [redacted]

Operational since August 26, 2022 1:52:08 AM UTC

Subaccount Overview

Region:	Europe (Rot)	Subaccount:	ab9e90b64
Region Host:	hana.ondemand.com	Initiated By:	[redacted]
HTTPS Proxy:	◇	Location ID:	S4CIGPROD
Subaccount Certificate:	Certificate valid until August 26, 2023 1:52:08 AM UTC	Description:	
System Certificate:	◇		

Disaster Recovery Subaccount

Status:	◇ Not configured	Region Host:	
Subaccount Certificate:	◇	Subaccount User:	

Tunnel Information

Status:	Connected
Tunnel ID:	account:///ab9e90b64/S4CIGPROD
Remote Name:	connectivitynotification.hana.ondemand.com

Important Links

Legal Information

Click Cloud To On-Premise link to provide the virtual mapping to the internal system. When you configure for the first time you will not see any entries here. Click on the '+' sign to add virtual mapping.

SAP Cloud Connector Administration

Subaccount:

Cloud To On-Premise

[ACCESS CONTROL](#) [COOKIE DOMAINS](#) [APPLICATIONS](#) [PRINCIPAL PROPAGATION](#)

Mapping Virtual To Internal System (0)

Status	Virtual Host	Internal Host	Check Result	Protocol	Back-end Type	Actions
No data						

Select the Back-end Type as ABAP System if you are using SAP ECC or S/4 HANA system and click Next

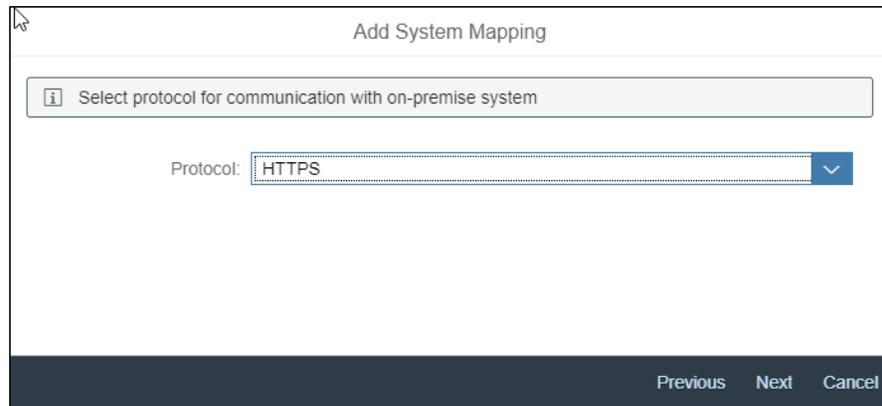
Add System Mapping

Select back-end type of on-premise system

Back-end Type: ABAP System

Previous Next Cancel

Select the Protocol as HTTP or HTTPS. We recommend to choose HTTPS



The image shows a dialog box titled "Add System Mapping". At the top, there is a header bar with the title. Below the header, there is a message box with an information icon and the text "Select protocol for communication with on-premise system". Underneath this, there is a label "Protocol:" followed by a dropdown menu. The dropdown menu is currently open, showing the selected option "HTTPS". At the bottom of the dialog box, there is a dark bar containing three buttons: "Previous", "Next", and "Cancel".

Provide the Internal Host and Port of your SAP Application server. You can get this details from tcode SMICM. SMICM->Goto->Services. Click Next

Add System Mapping

Enter internal (on-premise) host and port

Internal Host:*

Internal Port:*

Previous **Next** Cancel

H87 (1) (400)

Service Edit Goto List Settings System Help

ICM Monitor - Service Display

Active Services

No.	Protocol	Service Name/Port	Host Name	Keep Alive	Proc.Timeo	Actv	External Bind	Address bound	ACL File
1	HTTP	50080	tdclv1000177.tdc.net.sap	90	600	✓			
2	HTTPS	50081	tdclv1000177.tdc.net.sap	90	600	✓			
3	SMTP	25400	tdclv1000177.tdc.net.sap	60	1.800	✓			

Provide the Virtual host and Virtual port details. You can provide any value for virtual host and port but make sure it is a fully qualified domain name and not the same value as the internal host / port. We will provide the virtual host value in the Integration Suite Managed Gateway Portal connection page.

Note: Make sure your virtual host should not have any underscore character otherwise, you will see a 400 error when sending the message from Integration Suite Managed Gateway.

Add System Mapping

 It is recommended to use a virtual (cloud-side) name that is different from internal name

Virtual Host:*

Virtual Port:*

[Previous](#)



[Cancel](#)

Choose the Principal Type as None

Add System Mapping

 Select principal type

Principal Type:

None



Previous

Next

Cancel

Choose the Host In Request Header as Use Virtual Host

Add System Mapping

 Select host for request header field HOST

Host In Request Header:

[Previous](#)

[Next](#)

[Cancel](#)

This is optional. You can provide for your reference.

Add System Mapping

 Optionally enter a description

Description:

I 

Previous **Next** Cancel

Add System Mapping

 Summary

Protocol: HTTPS (None)

Internal: tdclv1000177.tdc.net.sap:50081

Virtual: s4cig.sap.com:8080

Check Internal Host:



Previous

Finish

Cancel

Add System Mapping

 Summary

Protocol: HTTPS (None)

Internal: tdclv1000177.tdc.net.sap:50081

Virtual: s4cig.sap.com:8080

Check Internal Host:

Previous

Finish

Cancel

Add the resource accessible path for the virtual to internal system

The screenshot displays the SAP Cloud Connector Administration interface. The top navigation bar includes the SAP logo, the text 'Cloud Connector Administration', and user information 'Administrator'. A left sidebar contains a 'Connector' menu with options like 'Security Status', 'Alerting', 'High Availability', 'Hardware Metrics Monitor', and 'Configuration'. Below this is a search bar for 'L15001' and a dropdown menu with 'Cloud To On-Premise' selected. The main content area is titled 'Cloud To On-Premise' and features a sub-account 'L15001'. It has four tabs: 'ACCESS CONTROL' (active), 'COOKIE DOMAINS', 'APPLICATIONS', and 'PRINCIPAL PROPAGATION'. Under 'ACCESS CONTROL', there is a section 'Mapping Virtual To Internal System (1)' with a table. The table has columns: Status, Virtual Host, Internal Host, Check Result, Protocol, Back-end Type, and Actions. One row is visible with 's4cig.sap.com:8080' as the Virtual Host, 'tdclv1000177.tdc.net.sap:50081' as the Internal Host, and 'Reachable' as the Check Result. Below this is a section 'Resources Of s4cig.sap.com:8080 (0)' with a table for 'Access Policy' containing columns for Status, URL Path, and Actions. This table is currently empty, showing 'No data'. A red box highlights the '+' icon in the top right of the 'Resources Of s4cig.sap.com:8080 (0)' section, indicating where to click to add a new resource path.

Status	Virtual Host	Internal Host	Check Result	Protocol	Back-end Type	Actions
◇	s4cig.sap.com:8080	tdclv1000177.tdc.net.sap:50081	Reachable	HTTPS	ABAP System	[Icons]

Status	URL Path	Access Policy	Actions
No data			

1. Add the URL path as /sap/
2. Check the Enabled box
3. Choose path and all sub-paths
4. Click Save

Add Resource

URL Path: *

Active:

WebSocket:

Access Policy: Path Only (Sub-Paths Are Excluded)

Path And All Sub-Paths

Description:

Save

Cancel

Now click on the Connector and start adding the remaining sub accounts.

The screenshot displays the SAP Cloud Connector Administration interface. The top navigation bar includes the SAP logo, the title 'Cloud Connector Administration', and user information 'Administrator'. The left sidebar contains a menu with 'Connector' selected, and a sub-menu for 'L15001' with options like 'Cloud To On-Premise' and 'Monitor'. The main content area shows the 'Connector' overview for subaccount 'L15001'. A red arrow points to the 'Connector' menu item. A red box highlights the '+ Add Subaccount' button. The 'Connector Overview' section displays details such as Connector ID, Local Name, Local IP, Security Status (Low risk), High Availability (Disabled), and Alerts (1). Below this is the 'Subaccount Dashboard (6)' table.

Status	Subaccount	Display Name	Location ID	Region	Actions
	a18a6fc8f		S4CIGTEST1	Europe (Rot)	

The Location ID and the Virtual Host, Virtual Port should be same for both test sub accounts like below. Once you add all sub-accounts you will see like below and all secure tunnels are established properly.

Subaccount: 

Connector

[+ Add Subaccount](#) [↓ Backup](#) [↑ Restore](#) 

Connector Overview

Connector ID: 7E936D7018BD11EDC947FBD00AEF47DD
Local Name: tdclv1000177.tdc.net.sap
Local IP: 10.239.71.221

Security Status:  Low risk
High Availability:  Disabled
Alerts:  1

Subaccount Dashboard (6)

Status	Subaccount	Display Name	Location ID	Region	Actions
	a18a6fc8f		S4CIGTEST1	Europe (Rot)	    
	a278d9ec7		S4CIGPROD	Europe (Rot)	    
	a508aae51		S4CIGPROD	Europe (Rot)	    
	a8f3ed22c		S4CIGPROD	Europe (Rot)	    
	ab9e90b64		S4CIGPROD	Europe (Rot)	    
	aff5426a3		S4CIGTEST1	Europe (Rot)	    

Service Channels Overview (0)

We have few optional configuration in SAP cloud connector. In case the secure tunnel between Integration Suite Managed Gateway sub account and the cloud connector is broken for some reason like Integration Suite Managed Gateway outage or network glitches, you will receive an email alert if the below configuration is performed. This alert will tell you in case if the tunnel is broken or recovered successfully and any new version is cloud connector is available.. Usually with SAP CC 12.3.0 or above, the secure tunnel will establish automatically. We always recommend to upgrade to the latest version.

The screenshot shows the SAP Cloud Connector Administration interface. The top navigation bar includes the SAP logo, 'Cloud Connector Administration', and user information 'Administrator'. The left sidebar contains a menu with 'Connector' selected, and sub-items: 'Security Status', 'Alerting', 'High Availability', 'Hardware Metrics Monitor', and 'Configuration'. Below this is another menu with 'Cloud To On-Premise', 'On-Premise To Cloud', 'Monitor', 'Audits', and 'Log And Trace Files'. The main content area is titled 'Alerting' and features two buttons: 'Observation Configuration' and 'E-Mail Configuration' (highlighted with a red box). Below the buttons is a table titled 'Alerts (1)' with the following data:

Status	Alert Message	Origin	Actions
	August 26, 2022 12:59:05 AM UTC — Cloud Connector version 2.14.2 is available. Please upgrade as soon as possible.	Master	

Please update the details and click Save.

E-Mail Configuration

Sending Alert E-Mails Enabled

Common Properties

Send To:

Sent From:

SMTP Server:

SMTP Port:

TLS Enabled:

User:

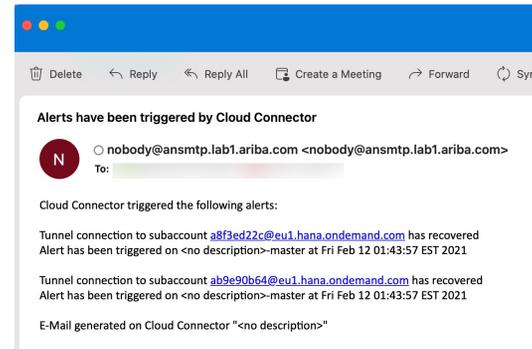
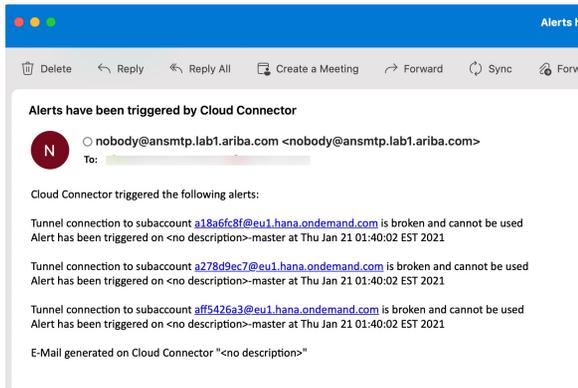
Password:

Additional Properties + -

Key	Value	Actions
No data		

Save Save & Test Cancel

Sample emails



Whitelist IPs for Integration Suite Managed Gateway -> ERP

To receive the transactions from Integration Suite Managed Gateway successfully your cloud connector will need to establish a secure tunnel with the Integration Suite Managed Gateway subaccounts. Based on the region host you are connecting to you need to whitelist the below IP ranges in your firewall. Sometime, BTP updates the IP ranges, so please refer the appropriate DC for latest IPs [here](#)

Data center	Region Host	IPs (Integration Suite Managed Gateway -> Cloud connector / PI -> ERP)
Europe (Rot)	eu1.hana.ondemand.com	130.214.160.64/28 and 130.214.160.80/29
US West (Colorado Springs)	us4.hana.ondemand.com	130.214.184.64/29 and 130.214.184.72/29
China (Shangai)	cn1.platform.sapcloud.cn	121.91.106.64/28 and 121.91.106.72/29
KSA (Riyadh)	sa1.hana.ondemand.com	130.214.223.32/29 and 130.214.223.40/29
UAE (Dubai)	ae1.hana.ondemand.com	130.214.251.32/29 and 130.214.251.40/29

Whitelist IPs for ERP -> Integration Suite Managed Gateway

To send the transactions from ERP/PI to Integration Suite Managed Gateway you need to whitelist the below IP address in your firewall. Based on the Integration Suite Managed Gateway data center you are connecting to this will change.

Data center	Integration Suite Managed Gateway Transaction URL	IPs to whitelist
Europe (Rot)	https://testacig.ariba.com/ https://acig.ariba.com/	3.124.222.77, 3.122.209.241, 3.124.208.223
US West (Colorado Springs)	https://testacig-us.ariba.com/ https://acig-us.ariba.com/	52.4.101.240, 52.23.1.211, 52.23.189.23
China (Shangai)	https://test.cig.cn40.apps.platform.sapcloud.cn/ https://prod.cig.cn40.apps.platform.sapcloud.cn/	139.224.7.71
KSA (Riyadh)	https://aribacloudintegration-test-ksa.ariba.com/ https://aribacloudintegration-ksa.ariba.com/	130.214.209.128/25
UAE (Dubai)	https://aribacloudintegration-uae.ariba.com/ https://aribacloudintegration-test-uae.ariba.com/	130.214.80.128/25

Troubleshooting

- Common errors when using integrating using cloud connector
 - Could not Send Message
 - 503 Service Unavailable
 - Service Unavailable
 - `org.apache.cxf.transport.http.HTTPException: HTTP response '503: Service Unavailable. There is no SAP Cloud Connector (SCC) connected to your subaccount. Requested opening of a tunnel for subaccount 'aff5426a3' and SCC location ID 'XXXXXX'. Check the configuration on SCC and cloud side.'` when communicating with https://ADDRESS_IS_SET_VIA_HEADER
 - 502 Bad Gateway
- Integration Suite Managed Gateway Connection Flow - <https://ga.support.sap.com/dtp/viewer/index.html#/tree/2757/actions/39812>
- Invalid server certificate error after cloud connector upgrade to 2.13.2 - <https://launchpad.support.sap.com/#/notes/0003088349>
- If you see Certificate expired message in screen from slide 8, click on the renew subaccount certificate button in the same screen.

Thank you.

Confidential Documents:

© 2024 Ariba, Inc. All rights reserved. The contents of this document are confidential and proprietary information of Ariba, Inc.