



# Cloud Connector configuration for Integration Suite Managed Gateway

Bharath Balakrishnan - SAP Ariba Cloud Integration Support

PUBLIC

**Confidential Documents:**

© 2026 Ariba, Inc. All rights reserved. The contents of this document are confidential and proprietary information of Ariba, Inc.

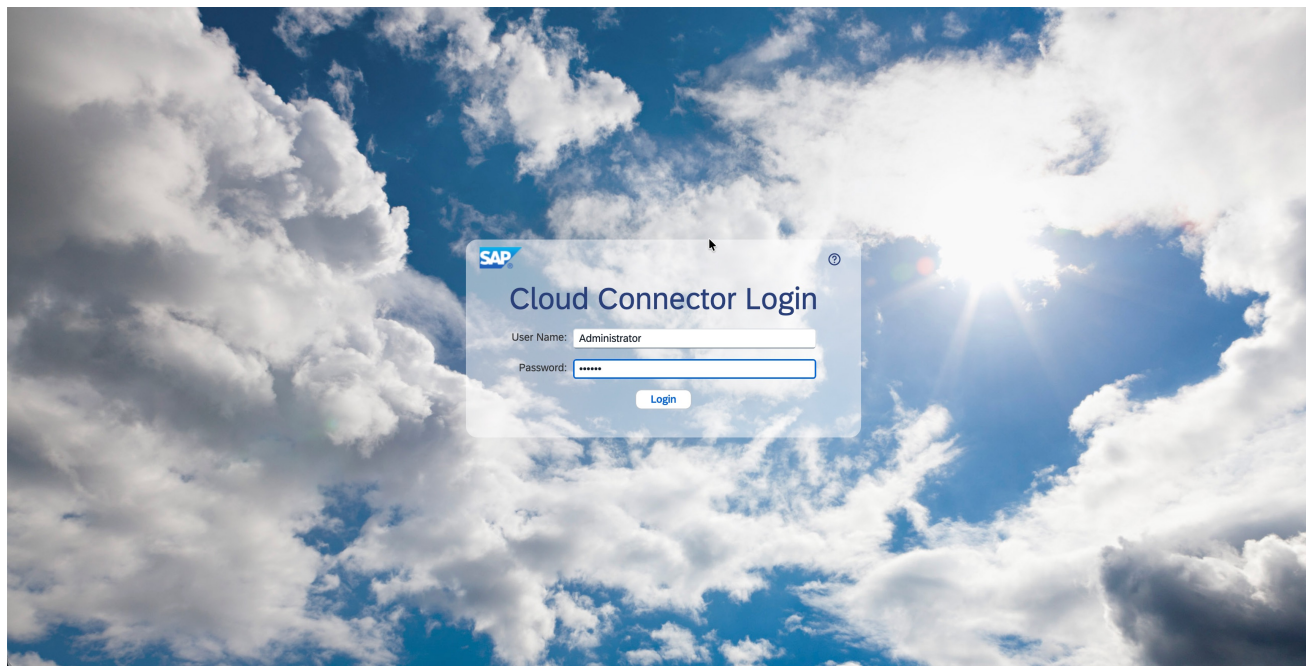


# Topics

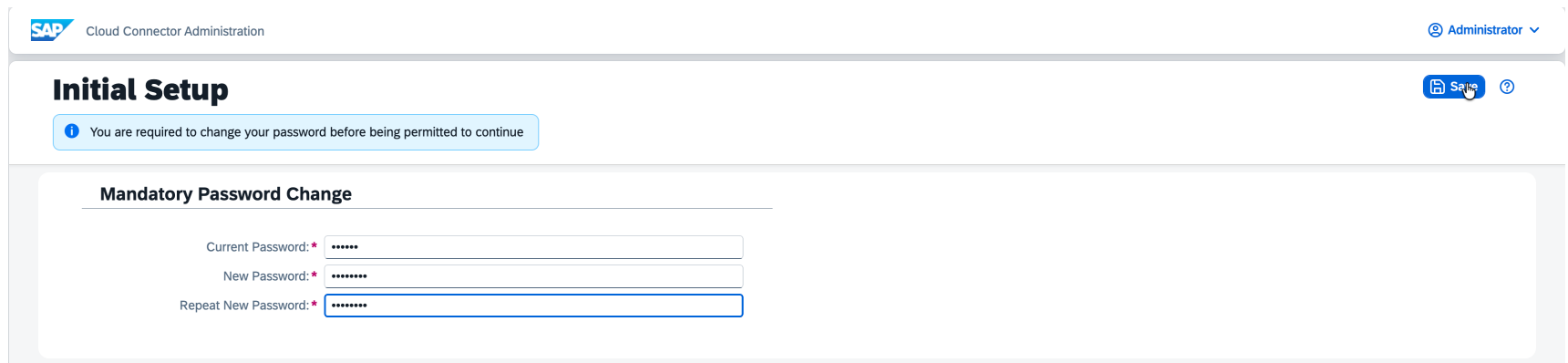
- Cloud Connector configuration for Integration Suite Managed Gateway
- Whitelist IPs for Integration Suite Managed Gateway -> ERP
- Whitelist IPs for ERP -> Integration Suite Managed Gateway
- Troubleshooting

After installing the cloud connector, you can launch it by using startcloudconnector.bat if you're on Windows, or go.sh script if you're on Linux or macOS.

Open your browser and enter the hostname of the machine where the cloud connector is installed, along with the port number you specified during installation like https://<hostnamewithdomain>:8443. I am signing in as the **Administrator**. The initial default password for your first login is **manage**.



After the first login, SAP CC will prompt you to change the default password.



The screenshot displays the SAP Cloud Connector Administration interface during its initial setup phase. The top header includes the SAP logo and the text "Cloud Connector Administration" on the left, and a user profile labeled "Administrator" with a dropdown arrow on the right. Below the header, the main section is titled "Initial Setup". A light blue information banner states: "You are required to change your password before being permitted to continue". Underneath this, a section titled "Mandatory Password Change" contains three password input fields. The first field is labeled "Current Password: \*" and contains seven asterisks. The second field is labeled "New Password: \*" and also contains seven asterisks. The third field is labeled "Repeat New Password: \*" and contains seven asterisks. To the right of the "Initial Setup" title, there are two icons: a "Save" button with a floppy disk icon and a help icon with a question mark.

SAP Cloud Connector Administration

Administrator

## Initial Setup

**You are required to change your password before being permitted to continue**

### Mandatory Password Change

Current Password: \*


New Password: \*

Repeat New Password: \*

Save ?




When you setup cloud connector as initial setup you will be prompted to choose if this is a Master or Shadow instance. Choose Master here and click Save

 Cloud Connector Administration

Administrator ▾

## Initial Setup

Save ⓘ

 You are required to select the installation type before being permitted to continue

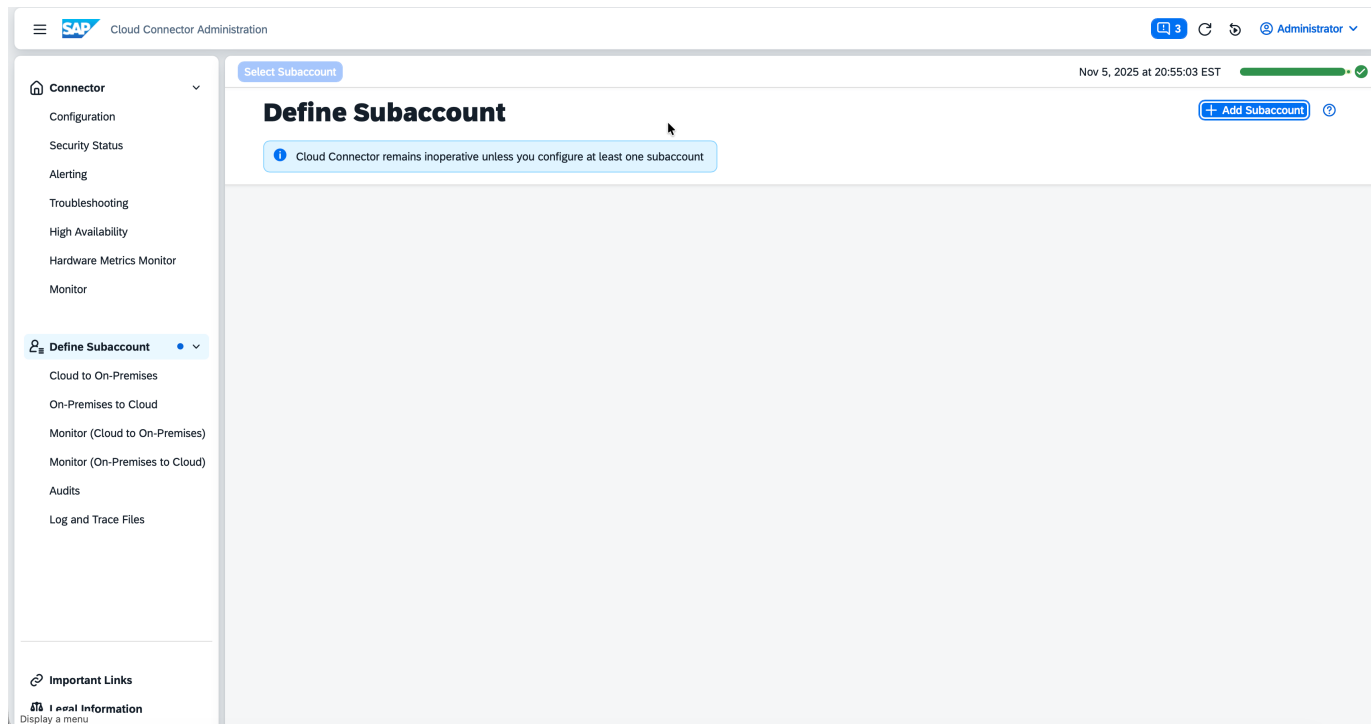
### Choose Installation Type

☒ Master (Primary Installation)

☐ Shadow (Backup Installation)

Description:

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. In case if you already have other subaccounts added or if you already added Managed Gateway Neo Subaccount and wanted to add managed gateway cloud foundry subaccounts, proceed with + Add Subaccount button.



If you connecting to the subaccount host using a proxy server, you can enter the details here.

The screenshot displays the SAP Cloud Connector Administration web interface. On the left is a sidebar menu with categories: **Connector** (containing Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor) and **Define Subaccount** (containing Cloud to On-Premises, On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, and Log and Trace Files). The main area is titled 'Define Subaccount' and includes a '+ Add Subaccount' button. A modal dialog box titled 'Add Subaccount' is open, featuring an information banner that reads 'Configure HTTPS proxy to connect to the Internet (if required)'. Below this, there are four input fields labeled 'Host:', 'Port:', 'User:', and 'Password:'. At the bottom of the dialog are three buttons: 'Previous', 'Next' (highlighted in blue), and 'Cancel'. The top of the interface shows the SAP logo, 'Cloud Connector Administration', a user profile for 'Administrator', and a timestamp 'Nov 5, 2025 at 20:56:08 EST'.

SAP Cloud Connector Administration

Administrator

Nov 5, 2025 at 20:56:08 EST

Select Subaccount

## Define Subaccount

+ Add Subaccount

### Add Subaccount

Configure HTTPS proxy to connect to the Internet (if required)

Host:

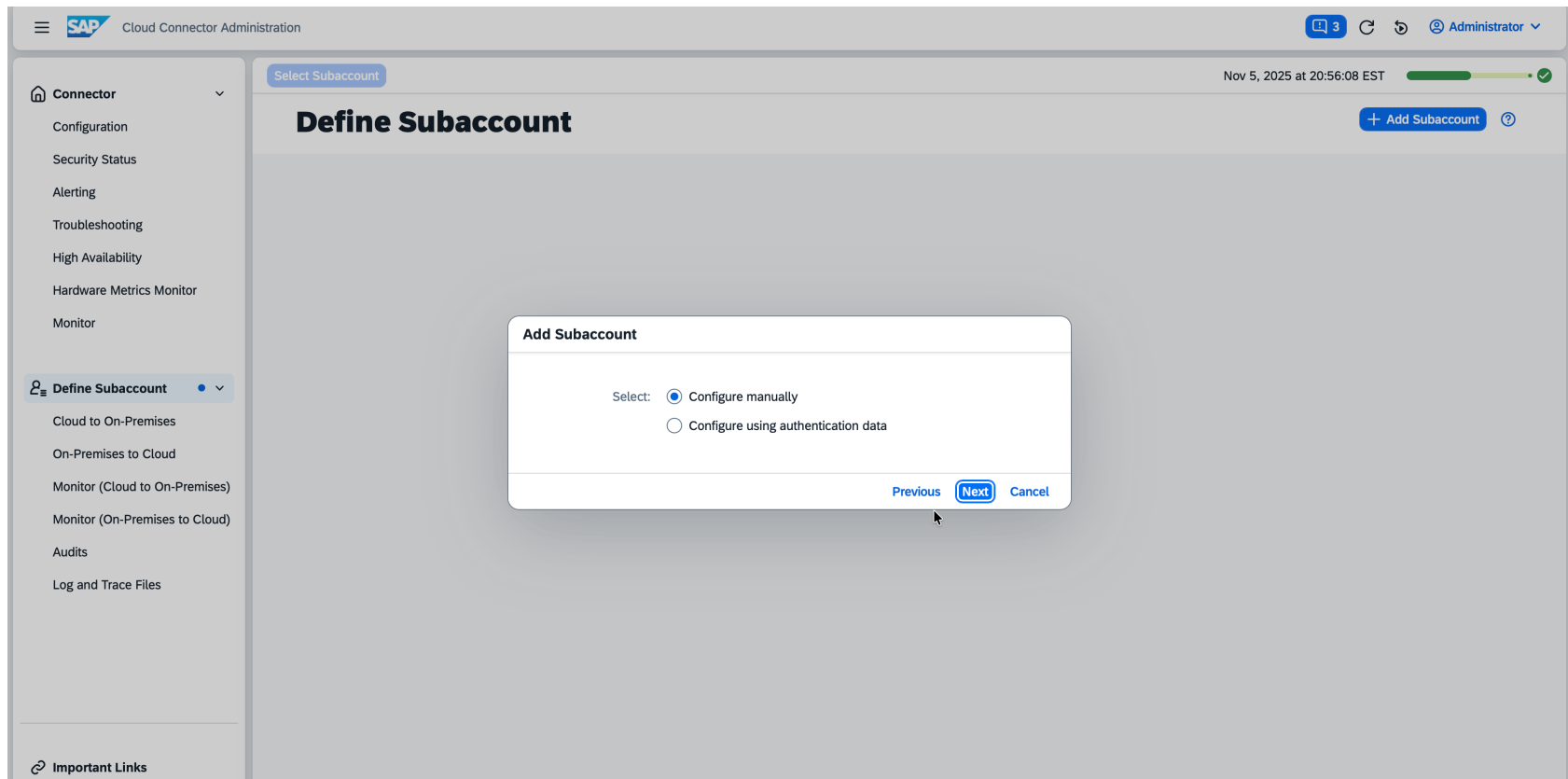
Port:

User:

Password:

Previous **Next** Cancel

Choose configure manually and click Next



Enter the following details in the Add subaccount screen.

**Region host:** Customers integrating via **SAP Integration Suite Managed Gateway** will connect through one of the following data centers, based on their geographic location or the time of activation:

**Subaccount:** We have separate subaccounts for **TEST** and **PRODUCTION** systems for each **DATA CENTER**. Below are the Sub accounts we have for each regions for SAP Managed Gateway.

**Subaccount User:** Enter “\$SAP-CP-SSO-PASSCODE\$” (without double quotes)

**Password:** Open the Passcode link for each of the subaccount corresponding do your region. Login with your email address linked to your Managed Gateway account and the Puser password to get the Onetime Passcode. If you are not sure of your email of your Managed Gateay account, Open the Managed Gateway application and navigate to My Configurations -> Authorizations where you can find the email address.

**Description:** This is an optional field just to give some reference.

*If you are unsure of the P-user password, you would need to reset it. SAP support teams do not have any way to recover your old password.*

*Repeat this until you add all of the subaccount for your corresponding datacenter and instance (test/production)*

## Add Subaccount

Provide the region host name of your managed gateway

Depending on  
your region host,  
enter the  
appropriate  
subaccount id.

Region: \*

Subaccount: \*

Display Name:

SAP MG TEST Subaccount1

Subaccount User: \*

\$SAP-CP-SSO-PASSCODE\$

This value is same for  
all subaccounts

Enter the passcode  
generated using the

Password: \*

.....

Location ID:

ARIBA MG1

Enter any value that is unique to  
your company like  
<CompanyName>MGTEST1

Description:

Previous

Finish

Cancel

Managed Gateway Region	Region Host Name	Sub Account Details
China	China (Shanghai) cf.cn40.platform.sapcloud.cn	<a href="#">SAP MG China Subaccount</a>
Europe Access Union (EUA)	Europe (Frankfurt) cf.eu10.hana.ondemand.com	<a href="#">SAP MG EUA Subaccount</a>
United States of America (USA)	US East (VA) cf.us10.hana.ondemand.com	<a href="#">SAP MG US Subaccount</a>
United Arab Emirates (UAE)	United Arab Emirates (UAE) cf.ae01.hana.ondemand.com	<a href="#">SAP MG UAE Subaccount</a>
Kingdom of Saudi Arabia (KSA)	KSA (Dammam regulated) - GCP cf.sa30.hana.ondemand.com	<a href="#">SAP MG KSA Subaccount</a>
	KSA (Dammam non-regulated) - GCP cf.sa31.hana.ondemand.com	
India (IN)	in30.hana.ondemand.com	<b>Test:</b> e8a1937f-7f45-4629-b3b9-ecc0a8c68b6e c9232e08-2ea4-4a3b-844c-1d40e0dd7ebb
		<b>Production:</b> b5c6fdd4-1992-4fb3-95ed-ad3c80ae1a86 ea5cf7cd-b2f6-4250-a8be-66e9f313410d
Europe Union (EU)	Europe (Frankfurt) – AWS cf.eu10.hana.ondemand.com	<a href="#">SAP MG EU Subaccount</a>



SAP

Cloud Connector Administration

7

Administrator

Connector

Configuration

Security Status

Alerting

Troubleshooting

High Availability

Hardware Metrics Monitor

Monitor

CIGUSZ

Cloud to On-Premises

On-Premises to Cloud

Monitor (Cloud to On-Premises)

Monitor (On-Premises to Cloud)

Audits

Log and Trace Files

Select Subaccount

Cross-Subaccount

Feb 2, 2026, 22:42:46 EST

Connector

Connector ID: CD2A39EE7AB74FC6BD6407F932BA581B

Local Name:

Local IP:

Security Status: 

Low risk

High Availability: 

Disabled

Alerts: 

1

Add Subaccount

Backup

Restore

Subaccount Dashboard (4)

Status	Subaccount	Display Name	Location ID	Region	Actions
	a4eca8c4-328d-492a-8ee0-cfb14a5d751c	CIGEU_NEW		Europe (Frankfurt) - AWS	
	c2cd9a88-7143-472a-a358-ac050eacdc39	CIGEU1		Europe (Frankfurt) - AWS	
	2fdff90d-496d-4c6d-9f21-26d1bb9f37b5	CIGEU2		Europe (Frankfurt) - AWS	
	c7845fda-254d-42ef-9069-70bde1d2b647	CIGEU3		Europe (Frankfurt) - AWS	

Service Channels Overview (0)

Status	Port	Type	Subaccount	Details	Actions
				No data	

When you open one of the sub account from the connector page, it should look like below where the tunnel status should show as **Connected**.

Cloud Connector Administration

7

Administrator

Connector

Configuration

Security Status

Alerting

Troubleshooting

High Availability

Hardware Metrics Monitor

Monitor

CIGEU\_NEW

Cloud to On-Premises

On-Premises to Cloud

Monitor (Cloud to On-Premises)

Monitor (On-Premises to Cloud)

Audits

Log and Trace Files

Important Links

Legal Information

Select Subaccount

CIGEU\_NEW

Feb 2, 2026, 22:49:35 EST

Disconnect

Import

Export

Certificate

CIGEU\_NEW

Connected since 2026-02-03 03:07:56 +0000 — no active resources available (check Cloud to On-Premises/Access Control)

Subaccount Overview

Region: Europe (Frankfurt) - AWS

Subaccount: a4eca8c4-328d-492a-8ee0-cfb14a5d751c

Region Host: cf.eu10.hana.ondemand.com

Display Name: CIGEU\_NEW

HTTPS Proxy:

Initiated By:

Subaccount Certificate: Valid

Location ID:

Auto Renewal: Off

Description:

Tunnel Information

Status: Connected

Tunnel ID: account:///a4eca8c4-328d-492a-8ee0-cfb14a5d751c/CIGEUTRAINING

Remote Name: connectivitynotification.cf.eu10.hana.ondemand.com

Cloud Connections

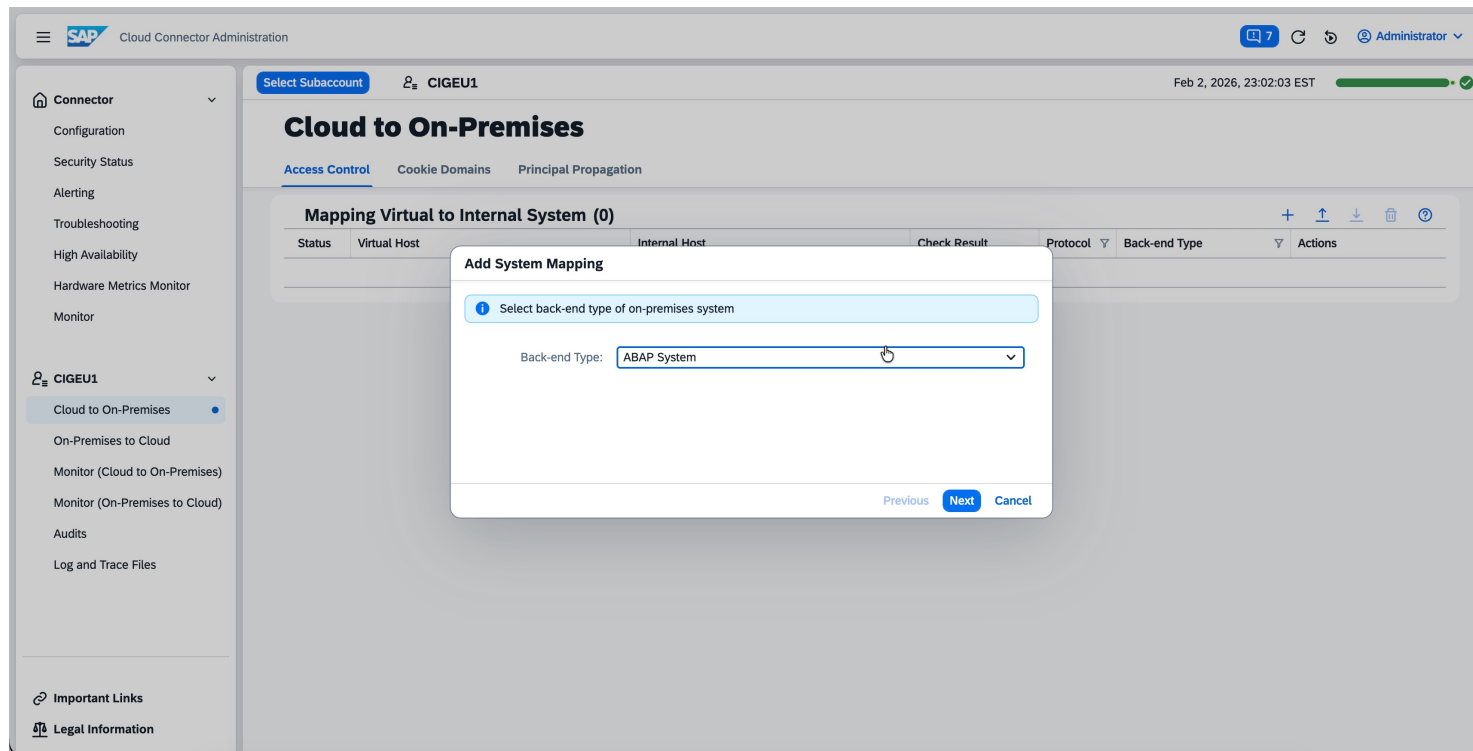
Application	Connections	Connected Since	Peer Labels	Actions
No data				

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. This needs to be done for each of the managed gateway subaccounts added to your cloud connector.

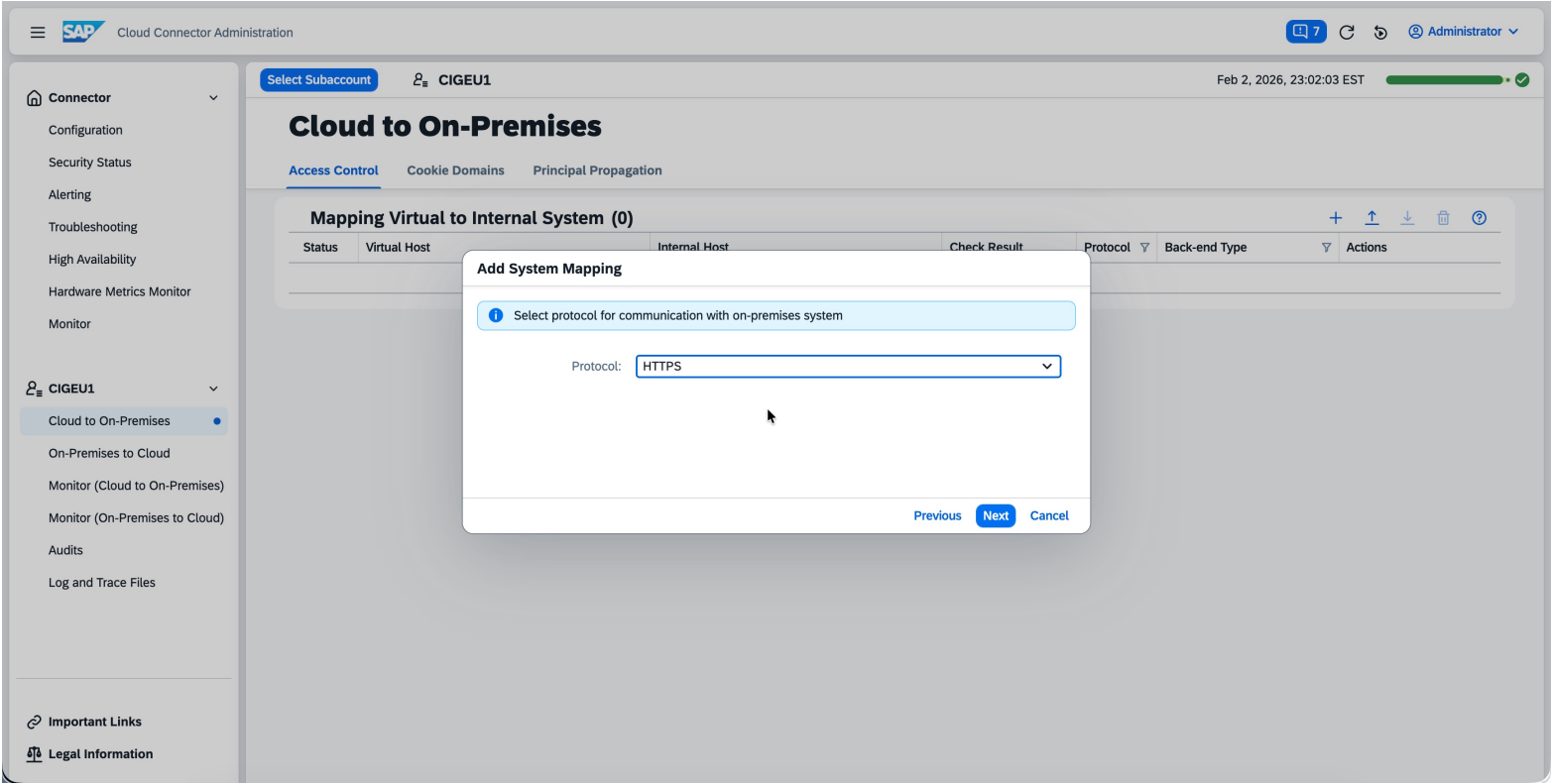
The screenshot displays the SAP Cloud Connector Administration interface. The left sidebar shows the navigation menu with 'Connector' expanded, listing options like Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor. Below this, the 'CIGEU1' subaccount is selected, and 'Cloud to On-Premises' is highlighted. The main content area is titled 'Cloud to On-Premises' and includes tabs for 'Access Control', 'Cookie Domains', and 'Principal Propagation'. The 'Access Control' tab is active, showing a table titled 'Mapping Virtual to Internal System (0)'. The table has columns for Status, Virtual Host, Internal Host, Check Result, Protocol, and Back-end Type. A red box highlights the '+' icon in the top right corner of the table, indicating where to click to add a new mapping. The table currently shows 'No data'.

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

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



Choose the protocol as HTTPS



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

The screenshot displays the SAP Cloud Connector Administration web interface. The left sidebar contains navigation options under 'Connector' (Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, Monitor) and under 'CIGEU1' (Cloud to On-Premises, On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, Log and Trace Files). The main area is titled 'Cloud to On-Premises' and shows 'Access Control' as the active tab. A modal dialog titled 'Add System Mapping' is open, prompting the user to 'Enter internal (on-premises) host and port'. The dialog contains two input fields: 'Internal Host: \*' with a placeholder 'ipaddressofonpremisesdestination' and 'Internal Port: \*' with the value '44350'. At the bottom of the dialog are 'Previous', 'Next', and 'Cancel' buttons. The background interface shows a table header for 'Mapping Virtual to Internal System (0)' with columns: Status, Virtual Host, Internal Host, Check Result, Protocol, Back-end Type, and Actions. The top of the interface includes the SAP logo, 'Cloud Connector Administration', a user menu for 'Administrator', and a timestamp 'Feb 2, 2026, 23:02:03 EST'.

SMICM screen shows the hostname of your SAP application server.

The screenshot shows the SAP ICM Monitor interface. The title bar indicates it's a Windows application. The menu bar includes Service, Edit, Goto, List, Settings, System, and Help. Below the menu is a toolbar with various icons for navigation and actions. The main area displays "Active Services" as a table.

No.	Protocol	Service Name/Port	Host Name	Keep Alive	Proc.Timeo	Actv	External Bind	Address bound	ACL File
<input type="checkbox"/>	1 HTTP	8050	[REDACTED]	300	300	✓			
<input type="checkbox"/>	2 HTTPS	44350	[REDACTED]	300	300	✓			



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 this 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.

The screenshot displays the SAP Cloud Connector Administration web interface. The left sidebar contains navigation links for 'Connector' (Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, Monitor) and 'CIGEU1' (Cloud to On-Premises, On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, Log and Trace Files). The main area is titled 'Cloud to On-Premises' and shows a table for 'Mapping Virtual to Internal System (0)'. A modal dialog titled 'Add System Mapping' is open, featuring a warning message: 'We recommend using a virtual (cloud-side) name that is different from internal name'. The dialog has two input fields: 'Virtual Host' with the value 'msna.sap.com' and 'Virtual Port' with the value '1234'. At the bottom of the dialog are 'Previous', 'Next', and 'Cancel' buttons.

Status	Virtual Host	Internal Host	Check Result	Protocol	Back-end Type	Actions
--------	--------------	---------------	--------------	----------	---------------	---------

**Add System Mapping**

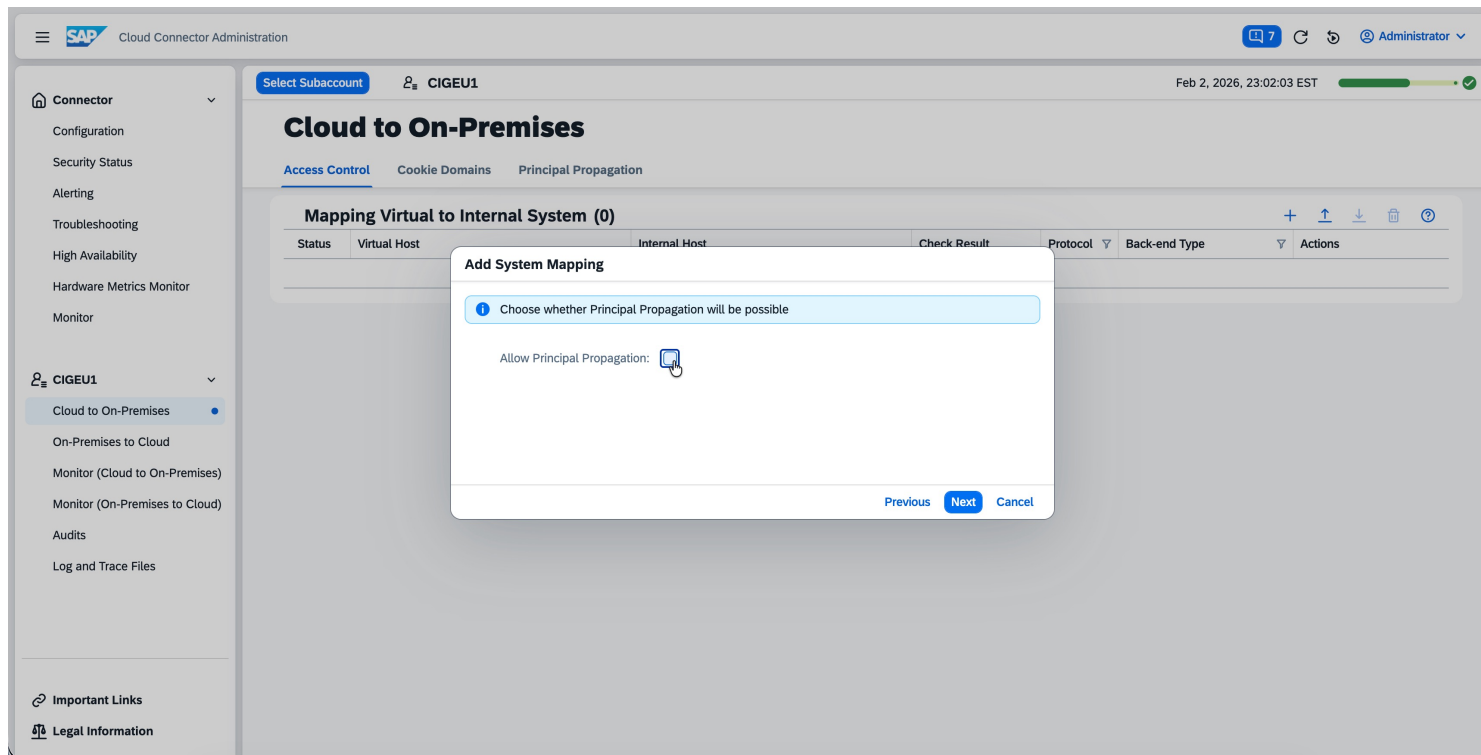
ⓘ We recommend using a virtual (cloud-side) name that is different from internal name

Virtual Host: \* msna.sap.com

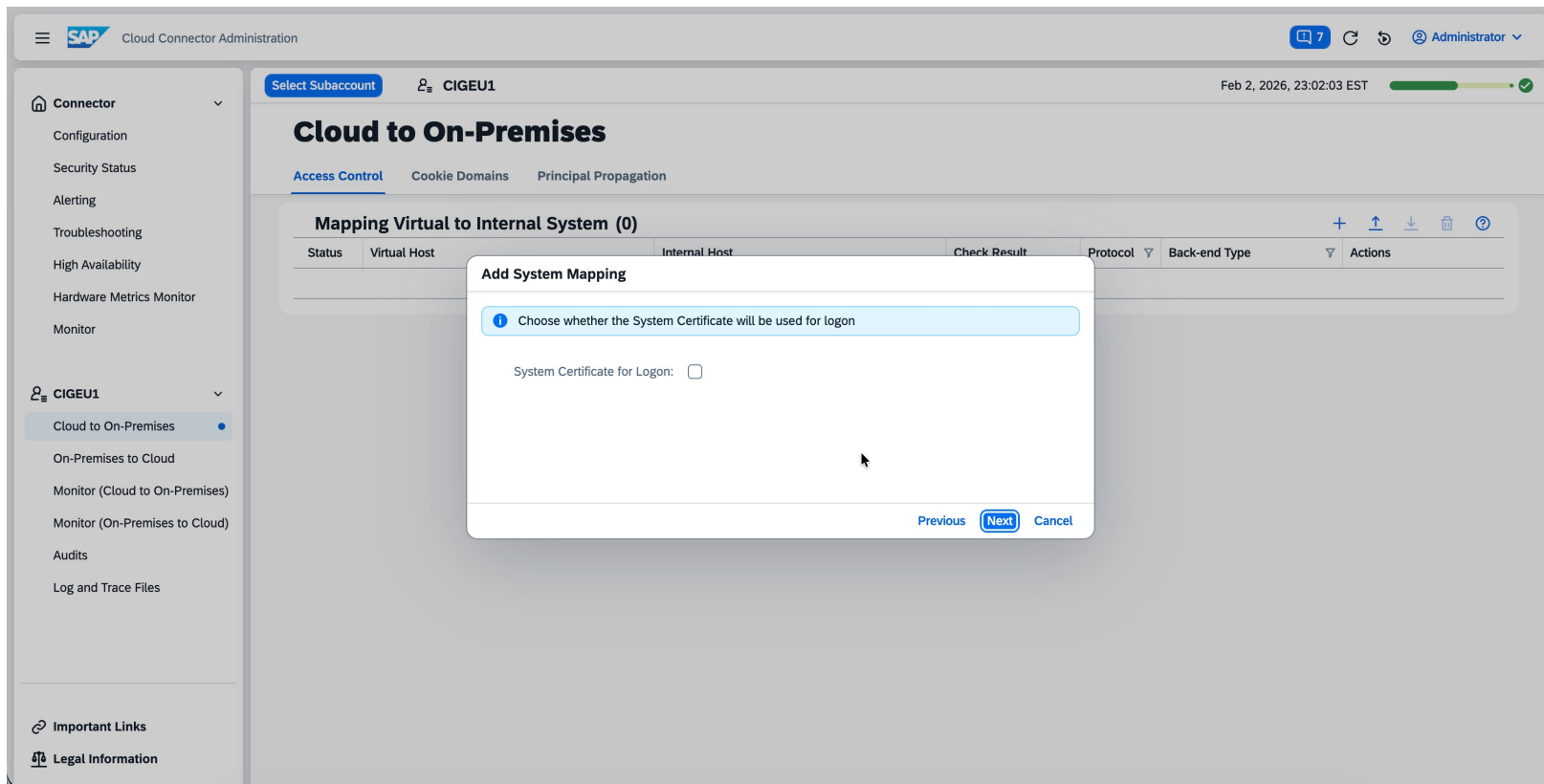
Virtual Port: \* 1234

Previous Next Cancel

## Uncheck the Allow Principal Propagation



## Uncheck the System Certificate for Logon



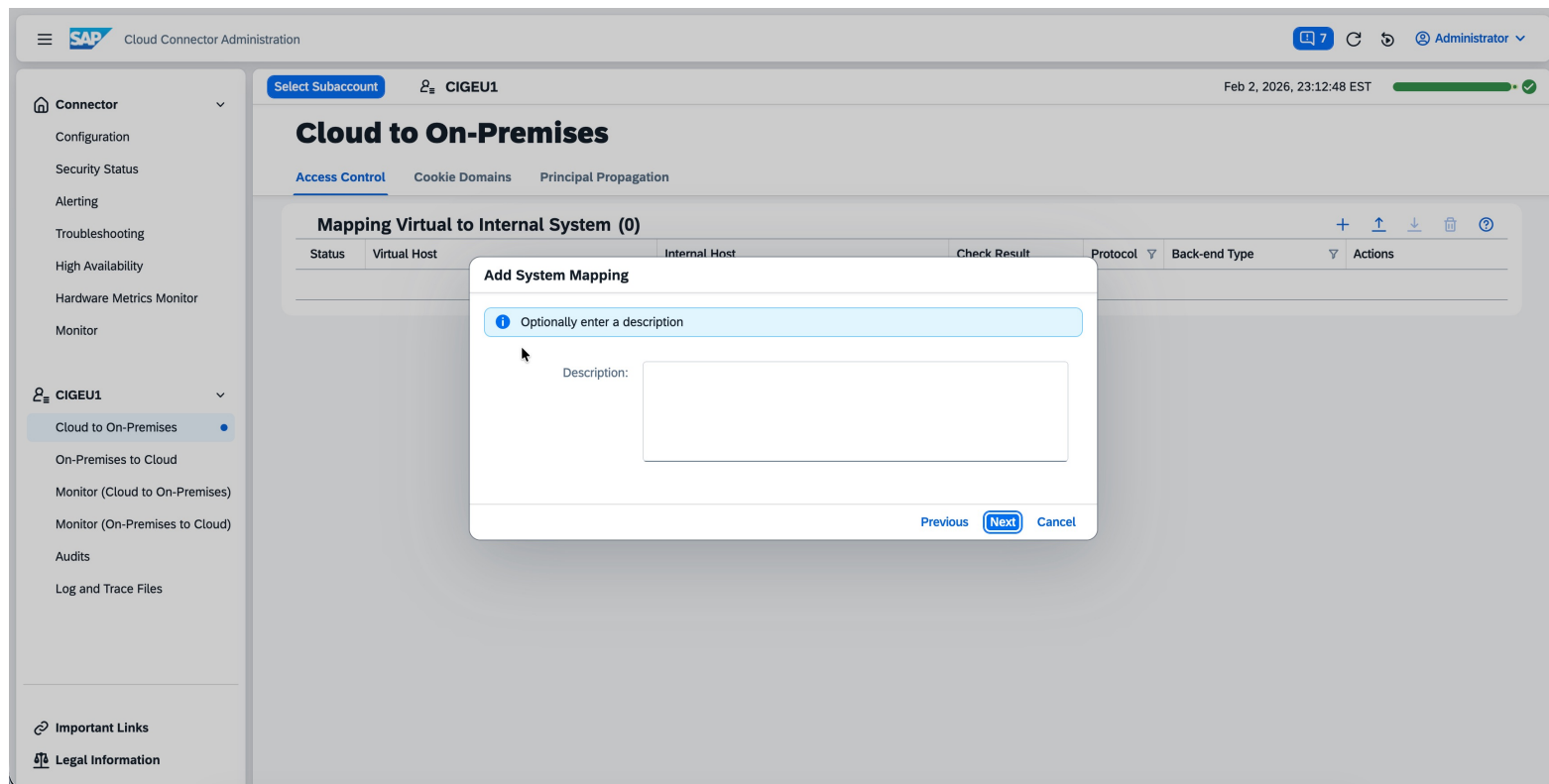
Select **Use Virtual host** as Host in Request Header

The screenshot displays the SAP Cloud Connector Administration web interface. The left sidebar contains navigation menus for 'Connector' (Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, Monitor) and 'CIGEU1' (Cloud to On-Premises, On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, Log and Trace Files). The main area is titled 'Cloud to On-Premises' and includes tabs for 'Access Control', 'Cookie Domains', and 'Principal Propagation'. A table titled 'Mapping Virtual to Internal System (0)' is visible, with columns for Status, Virtual Host, Internal Host, Check Result, Protocol, Back-end Type, and Actions. Overlaid on this is a modal dialog box titled 'Add System Mapping'. Inside the dialog, there is an information icon and the text 'Select host for request header field HOST'. Below this, a label 'Host in Request Header:' is followed by a dropdown menu currently showing 'Use Virtual Host'. At the bottom of the dialog are three buttons: 'Previous', 'Next' (highlighted with a blue border), and 'Cancel'. The top of the interface shows the SAP logo, 'Cloud Connector Administration', a user profile 'Administrator', and a timestamp 'Feb 2, 2026, 23:02:03 EST'.

Enter the System ID. This is an optional field

The screenshot displays the SAP Cloud Connector Administration web interface. The left sidebar contains a navigation menu with sections: 'Connector' (Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, Monitor), 'CIGEU1' (Cloud to On-Premises, On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, Log and Trace Files), 'Important Links', and 'Legal Information'. The main area is titled 'Cloud to On-Premises' and includes tabs for 'Access Control', 'Cookie Domains', and 'Principal Propagation'. Below these is a table titled 'Mapping Virtual to Internal System (0)' with columns: Status, Virtual Host, Internal Host, Check Result, Protocol, Back-end Type, and Actions. A modal dialog titled 'Add System Mapping' is open in the center. It contains an informational message 'Optionally enter a system ID' and a text input field labeled 'System ID:' with the value 'EUP'. At the bottom of the dialog are three buttons: 'Previous', 'Next' (which is highlighted with a mouse cursor), and 'Cancel'. The top of the interface shows the SAP logo, 'Cloud Connector Administration', a user profile 'Administrator', and a timestamp 'Feb 2, 2026, 23:12:48 EST'.

This is an optional field entered for your reference.



Select the Check Internal Host box and click Finish

The screenshot displays the SAP Cloud Connector Administration web interface. The left sidebar contains navigation menus for 'Connector' (Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, Monitor) and 'CIGEU1' (Cloud to On-Premises, On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, Log and Trace Files). The main area is titled 'Cloud to On-Premises' and includes tabs for 'Access Control', 'Cookie Domains', and 'Principal Propagation'. A table titled 'Mapping Virtual to Internal System (0)' is visible, with columns for Status, Virtual Host, Internal Host, Check Result, Protocol, Back-end Type, and Actions. Overlaid on this is a modal dialog box titled 'Add System Mapping'. The dialog has a 'Summary' section with the following details: Protocol: HTTPS (None), Internal: (empty field), Virtual: msna.sap.com:1234, and Check Internal Host: ☒. At the bottom of the dialog are 'Previous', 'Finish', and 'Cancel' buttons.



Click the add resource option option.

The screenshot displays the SAP Cloud Connector Administration web interface. The left sidebar contains navigation menus for 'Connector' (Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, Monitor) and 'CIGEU1' (Cloud to On-Premises, On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, Log and Trace Files). The main content area is titled 'Cloud to On-Premises' and includes tabs for 'Access Control', 'Cookie Domains', and 'Principal Propagation'. The 'Access Control' tab is active, showing a table for 'Mapping Virtual to Internal System (1)' with columns: Status, Virtual Host, Internal Host, Check Result, Protocol, Back-end Type, and Actions. Below this is a table for 'Resources of msna.sap.com:1234 (0)' with columns: Status, URL Path, Access Policy, and Actions. A red arrow points to the '+' icon in the Actions column of the Resources table. A 'Changes were saved' notification is visible at the bottom.

**Cloud to On-Premises**

**Mapping Virtual to Internal System (1)**

Status	Virtual Host	Internal Host	Check Result	Protocol	Back-end Type	Actions
	msna.sap.com:1234		✓ Reachable	HTTPS	ABAP System	

**Resources of msna.sap.com:1234 (0)**

Status	URL Path	Access Policy	Actions
No data			

Changes were saved

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

The screenshot displays the SAP Cloud Connector Administration web interface. The main header shows 'Cloud Connector Administration' with a user profile 'Administrator' and a timestamp 'Feb 2, 2026, 23:18:15 EST'. The left sidebar contains navigation options under 'Connector' (Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, Monitor) and 'CIGEU1' (Cloud to On-Premises, On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, Log and Trace Files). The main content area is titled 'Cloud to On-Premises' and includes tabs for 'Access Control', 'Cookie Domains', and 'Principal Propagation'. A modal dialog box titled 'Add Resource' is open in the center. It contains the following fields and options: 'URL Path' with the value '/sap/', 'Active' checked, 'Upgrade Allowed' unchecked, 'Access Policy' with 'Path and All Sub-Paths' selected, and a 'Description' text area. The dialog has 'Save' and 'Cancel' buttons at the bottom right. In the background, a table titled 'Resources of msn' is partially visible, showing columns for 'Status', 'URL Path', 'Protocol', 'Back-end Type', and 'Actions'.

- Connector
  - Configuration
  - Security Status
  - Alerting
  - Troubleshooting
  - High Availability
  - Hardware Metrics Monitor
  - Monitor
- CIGEU1
  - Cloud to On-Premises
  - On-Premises to Cloud
  - Monitor (Cloud to On-Premises)
  - Monitor (On-Premises to Cloud)
  - Audits
  - Log and Trace Files

- Important Links
- Legal Information

Select Subaccount

CIGEU1

## Cloud to On-Premises

Access Control Cookie Domains Principal Propagation

### Mapping Virtual to Internal System (1)

Status	Virtual Host	Internal Host	Check Result	Protocol	Back-end Type	Actions
✓	msna.sap.com:1234		✓ Reachable	HTTPS	ABAP System	

### Resources of msna.sap.com:1234 (1)

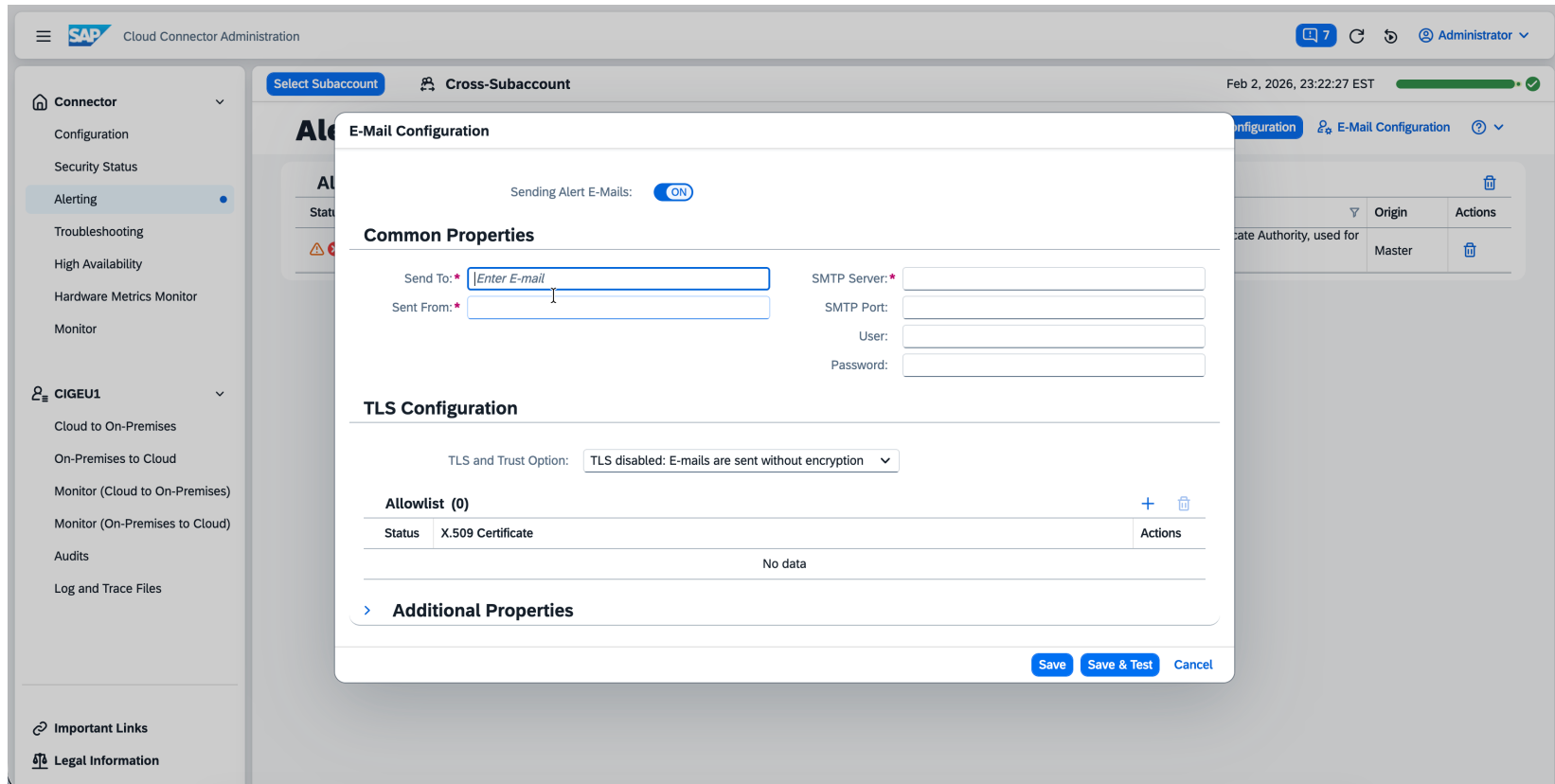
Status	URL Path	Access Policy	Actions
✓	/sap/	Path and All Sub-Paths	

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 displays the SAP Cloud Connector Administration web interface. The left sidebar contains a navigation menu with options: Connector, Configuration, Security Status, Alerting (selected), Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor. Below this, a section for 'CIGEU1' lists various monitoring and audit options. At the bottom, there are links for 'Important Links' and 'Legal Information'. The main content area is titled 'Alerting' and includes tabs for 'Observation Configuration' (highlighted with a red arrow) and 'E-Mail Configuration'. Below the tabs, a table titled 'Alerts (1)' shows a single alert entry. The table has columns for Status, Date, Alert Message, Origin, and Actions. The alert message states: 'Message from cloud: Please make sure to check the following two notes, which describe an upcoming change in the Certificate Authority, used for issuing the TLS certificates of the BTP endpoints. Action may be required. Notes: https://me.sap.com/notes/3583377 & https://me.sap.com/notes/3566727'. The Origin is listed as 'Master'.

Status	Date	Alert Message	Origin	Actions
	2026-02-02 21:10:00 +0000	Message from cloud: Please make sure to check the following two notes, which describe an upcoming change in the Certificate Authority, used for issuing the TLS certificates of the BTP endpoints. Action may be required. Notes: <a href="https://me.sap.com/notes/3583377">https://me.sap.com/notes/3583377</a> & <a href="https://me.sap.com/notes/3566727">https://me.sap.com/notes/3566727</a>	Master	

Please update the details and click Save.



The screenshot shows the SAP Cloud Connector Administration interface. A modal window titled "E-Mail Configuration" is open, displaying settings for sending alert emails. The "Sending Alert E-Mails" toggle is turned ON. The "Common Properties" section includes fields for "Send To" (with a placeholder "Enter E-mail"), "Send From", "SMTP Server", "SMTP Port", "User", and "Password". The "TLS Configuration" section shows the "TLS and Trust Option" set to "TLS disabled: E-mails are sent without encryption". Below this is an "Allowlist (0)" table with one entry: "X.509 Certificate". The "Additional Properties" section is currently collapsed. At the bottom of the modal are three buttons: "Save", "Save & Test", and "Cancel".

**E-Mail Configuration**

Sending Alert E-Mails: ☒ ON

**Common Properties**

Send To:

Send From:

SMTP Server:

SMTP Port:

User:

Password:

**TLS Configuration**

TLS and Trust Option:

**Allowlist (0)**

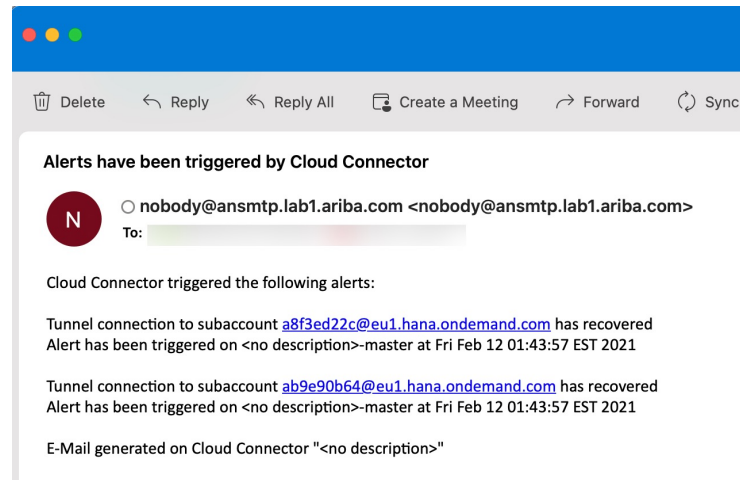
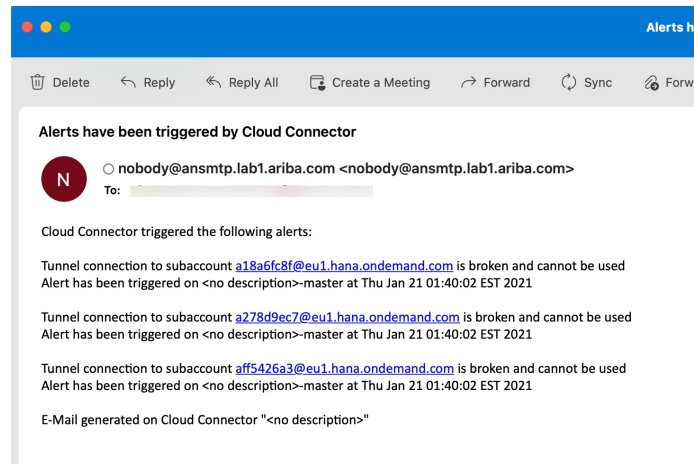
Status	Details	Actions
X.509 Certificate		

No data

**Additional Properties**

[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](#). See **IP AllowList Updating** section for your respective data center.



## 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. You can also whitelist the hostname mentioned in the Integration Suite Managed Gateway Transaction URL column. 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 (Frankfurt) <b>cf-eu10</b>	<a href="https://test-integration.eu.managedgateway.cloud.sap/">https://test-integration.eu.managedgateway.cloud.sap/</a> <a href="https://integration.eu.managedgateway.cloud.sap/">https://integration.eu.managedgateway.cloud.sap/</a>	Refer the column LB IPs (ingress, for incoming request) from <a href="#">Regions and API Endpoints Available for the Cloud Foundry Environment</a>
US West (Colorado Springs) <b>cf-us10</b>	<a href="https://test-integration.us.managedgateway.cloud.sap/">https://test-integration.us.managedgateway.cloud.sap/</a> <a href="https://integration.us.managedgateway.cloud.sap/">https://integration.us.managedgateway.cloud.sap/</a>	
China (Shanghai) <b>cf-cn40</b>	<a href="https://test-integration.managedgateway.sapcloud.cn/">https://test-integration.managedgateway.sapcloud.cn/</a> <a href="https://integration.managedgateway.sapcloud.cn/">https://integration.managedgateway.sapcloud.cn/</a>	
KSA (Riyadh)	<a href="https://test-integration.ksa.managedgateway.cloud.sap/">https://test-integration.ksa.managedgateway.cloud.sap/</a> <a href="https://integrationportal.eu.managedgateway.cloud.sap/">https://integrationportal.eu.managedgateway.cloud.sap/</a>	
UAE (Dubai) <b>cf-ae01</b>	<a href="https://integration.uae.managedgateway.cloud.sap/">https://integration.uae.managedgateway.cloud.sap/</a> <a href="https://test-integration.uae.managedgateway.cloud.sap/">https://test-integration.uae.managedgateway.cloud.sap/</a>	

# 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](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:**

© 2026 Ariba, Inc. All rights reserved. The contents of this document are confidential and proprietary information of Ariba, Inc.