



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.

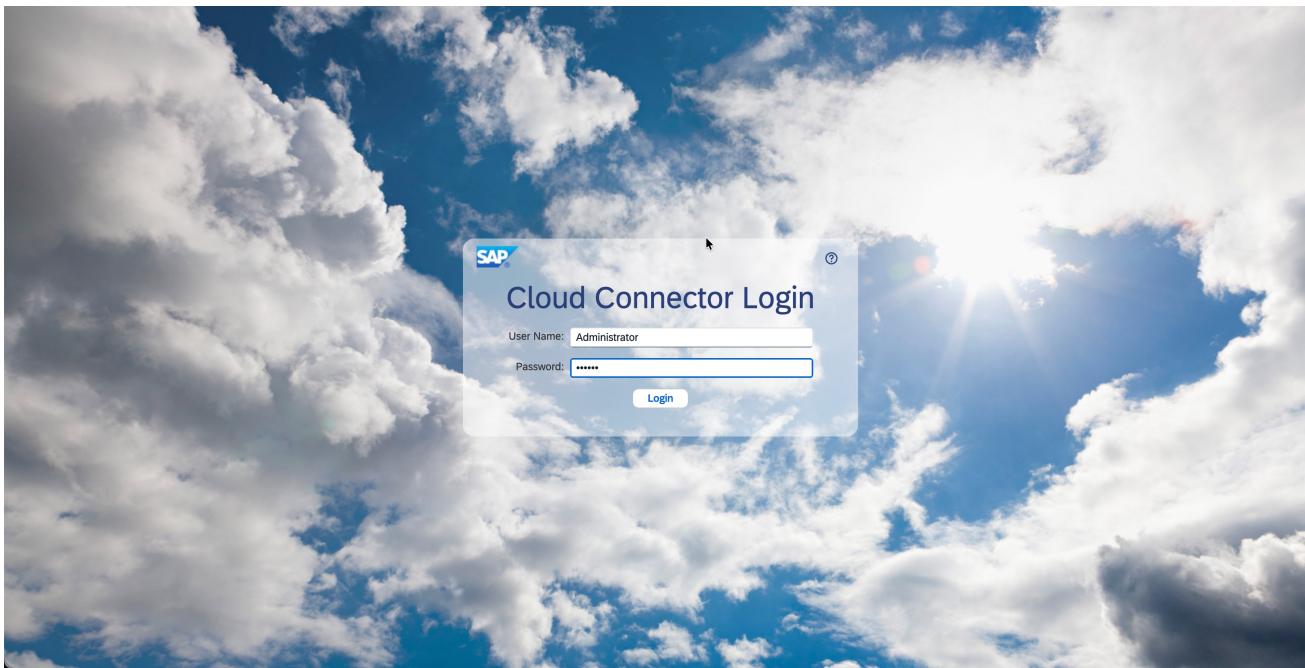
THE BEST RUN  SAP

Topics

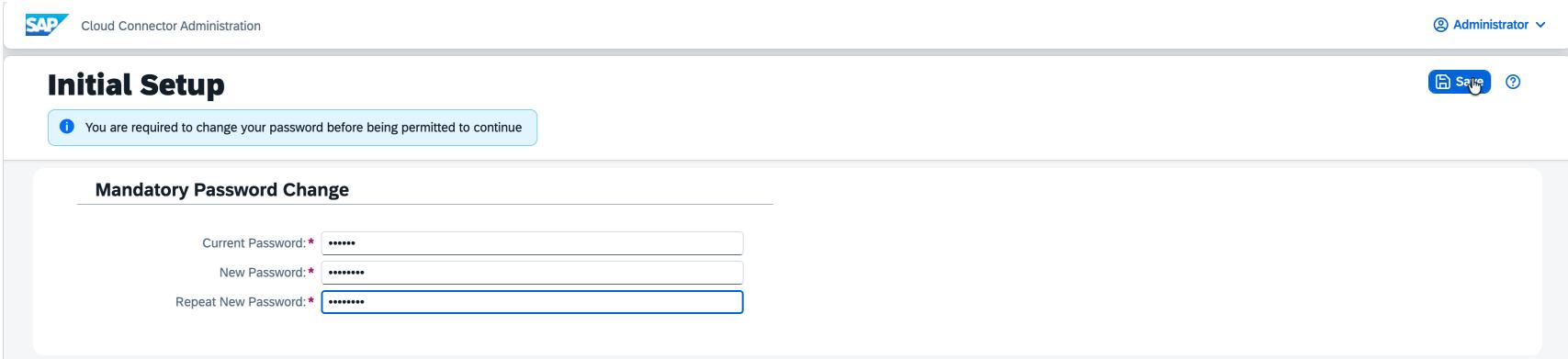
- Cloud Connector configuration for Integration Suite Managed Gateway
- Whitelist IPs for Integration Suite Managed Gateway -> ERP
- Whitelist IPs for ERP -> Integration Suite Managed Gateway
- Troubleshooting

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 shows the SAP Cloud Connector Administration interface. At the top, there is a header with the SAP logo, the text "Cloud Connector Administration", and a user dropdown for "Administrator". Below the header, the page title is "Initial Setup". A callout box contains the message: "You are required to change your password before being permitted to continue". The main content area is titled "Mandatory Password Change" and contains three input fields: "Current Password" (containing "*****"), "New Password" (containing "*****"), and "Repeat New Password" (containing "*****"). The "Save" button is highlighted with a blue border, and a help icon is also present.

Initial Setup

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

Mandatory Password Change

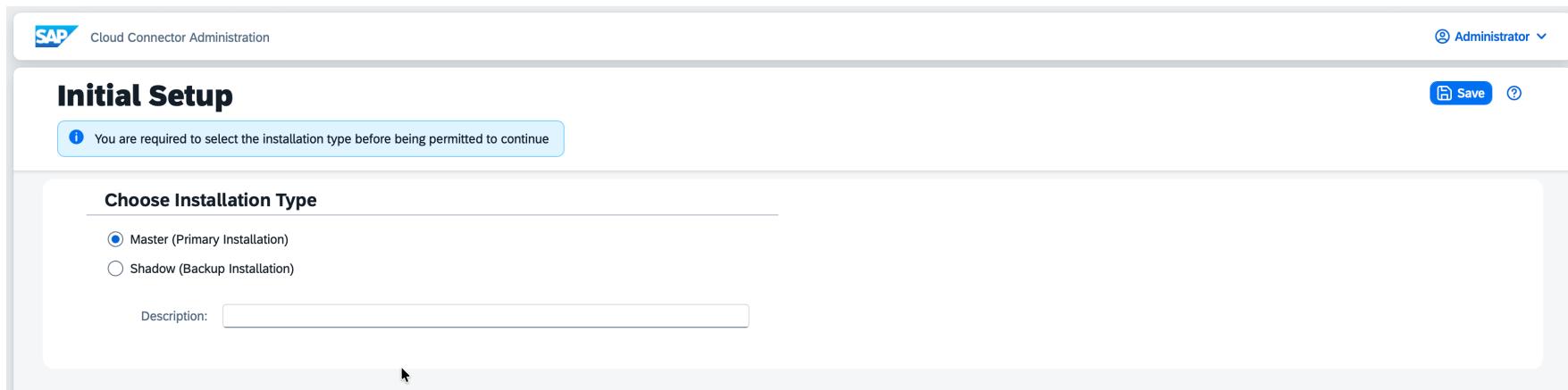
Current Password: *

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



SAP Cloud Connector Administration

Administrator

Initial Setup

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

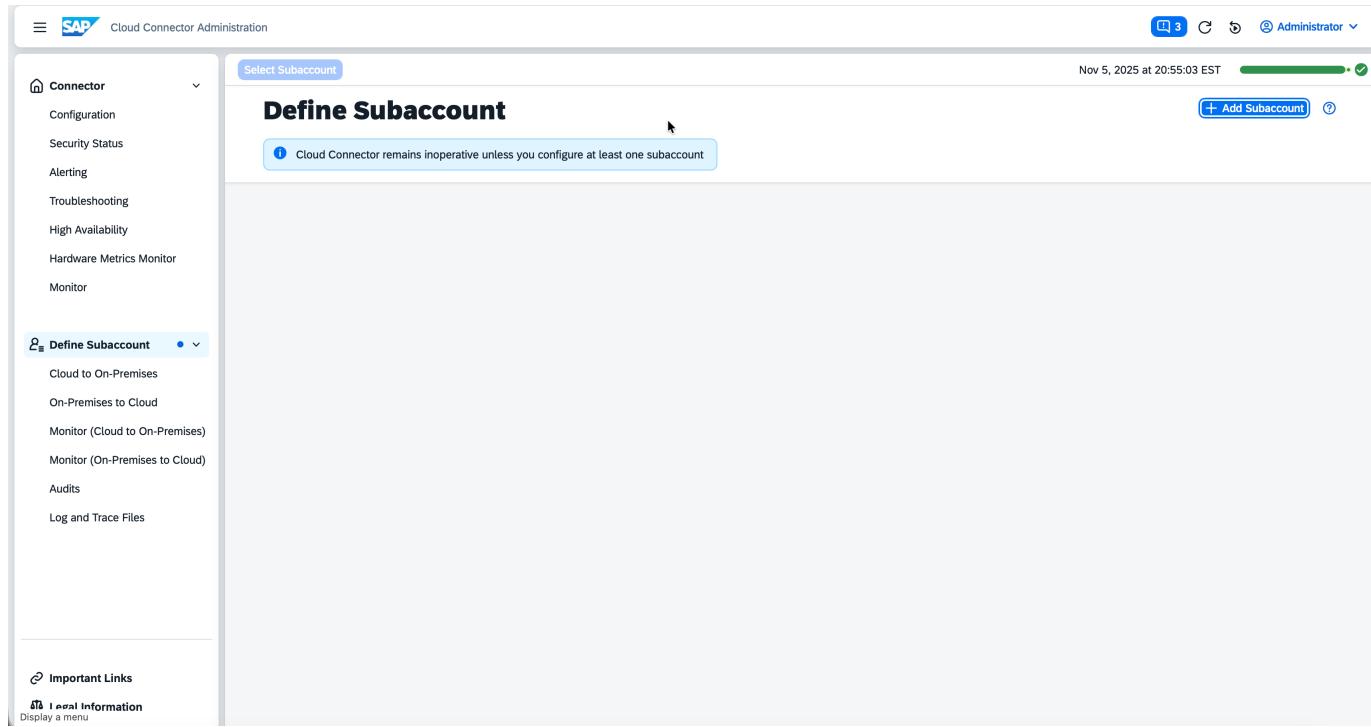
Choose Installation Type

Master (Primary Installation)
 Shadow (Backup Installation)

Description:

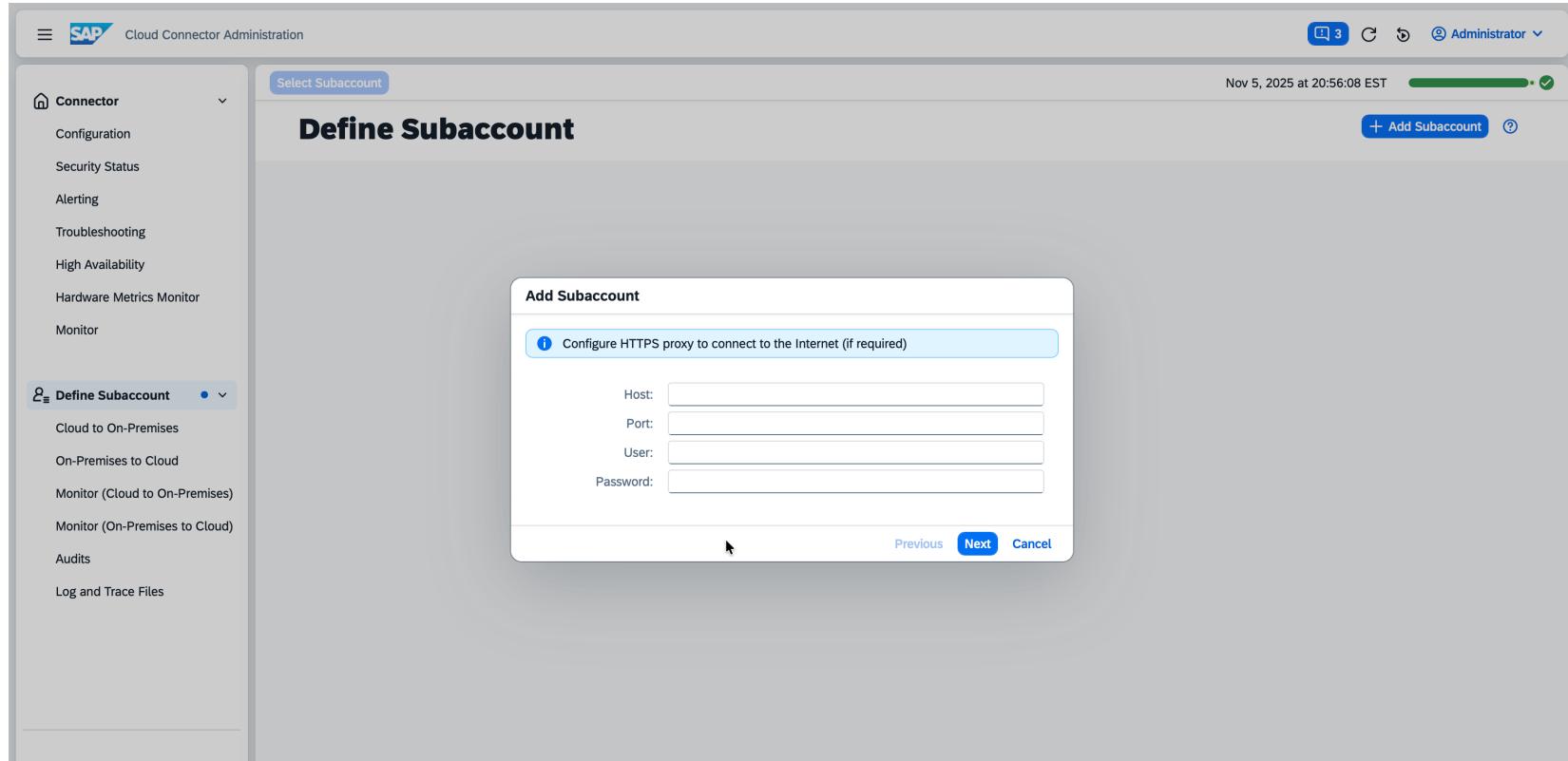
Save

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.



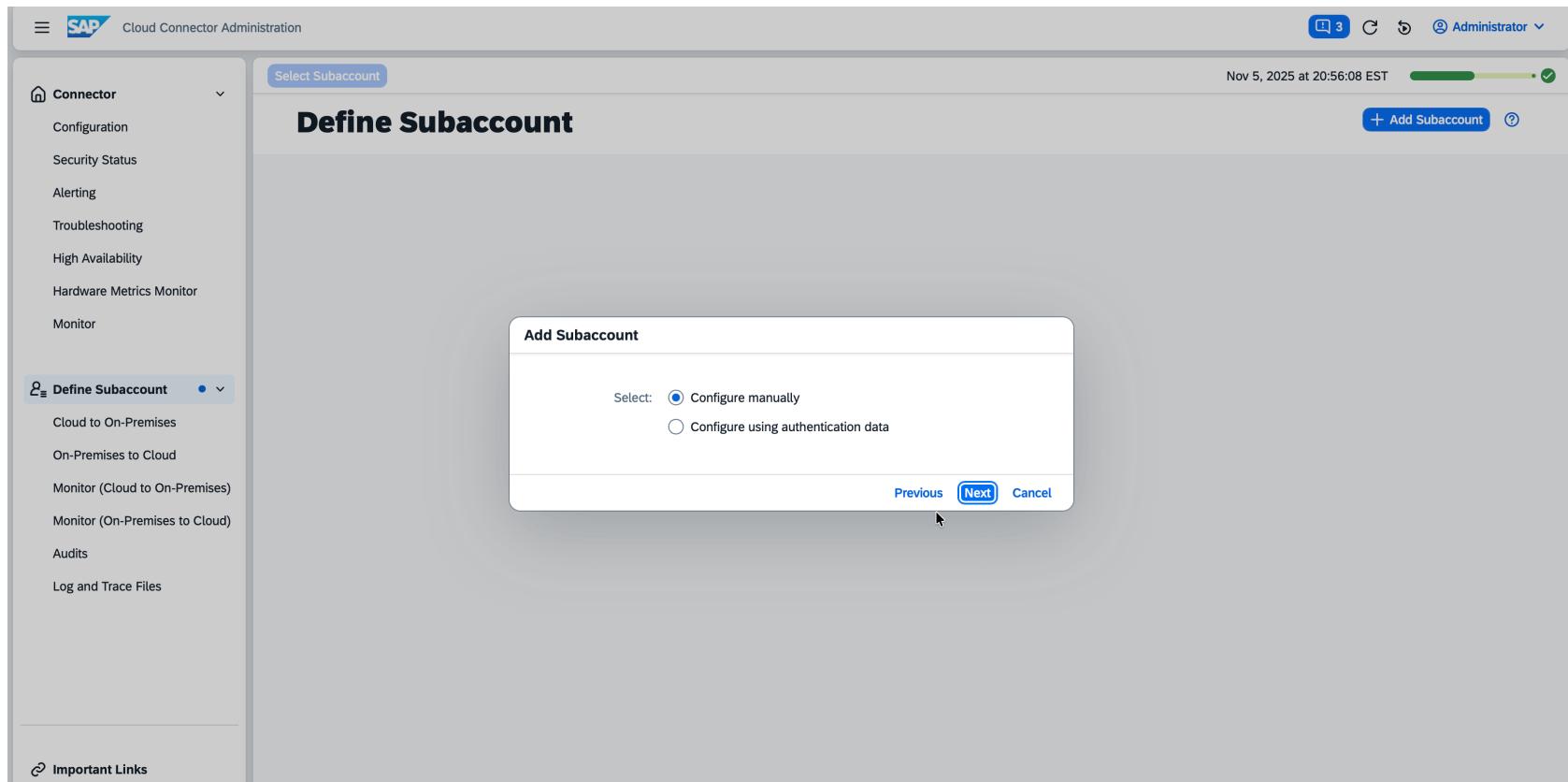
The screenshot shows the SAP Cloud Connector Administration interface. The top navigation bar includes the SAP logo, the title 'Cloud Connector Administration', a notification badge with '3', a search icon, and a user dropdown for 'Administrator'. The main content area is titled 'Define Subaccount' with a sub-header 'Select Subaccount'. A message box states: 'Cloud Connector remains inoperative unless you configure at least one subaccount'. On the left, a sidebar menu under 'Connector' lists: Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor. Under 'Define Subaccount', the 'Cloud to On-Premises' option is selected, with other options like On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, and Log and Trace Files listed. At the bottom of the sidebar are 'Important Links' and 'Local Information'.

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



The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with 'Configuration', 'Security Status', 'Alerting', 'Troubleshooting', 'High Availability', 'Hardware Metrics Monitor', and 'Monitor'. Below that is a 'Define Subaccount' section with '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 content area has a 'Select Subaccount' header and a 'Define Subaccount' sub-header. A modal dialog titled 'Add Subaccount' is open, containing a note to 'Configure HTTPS proxy to connect to the Internet (if required)' and four input fields: 'Host', 'Port', 'User', and 'Password'. At the bottom of the dialog are 'Previous', 'Next' (highlighted in blue), and 'Cancel' buttons. The top right of the screen shows the date 'Nov 5, 2025 at 20:56:08 EST' and a progress bar.

Choose configure manually and click Next



SAP Cloud Connector Administration

Nov 5, 2025 at 20:56:08 EST

Administrator

Connector

Configuration

Security Status

Alerting

Troubleshooting

High Availability

Hardware Metrics Monitor

Monitor

Define Subaccount

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

Select Subaccount

Define Subaccount

+ Add Subaccount

Add Subaccount

Select: Configure manually

Configure using authentication data

Previous Next Cancel

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

Description:

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

Previous

Finish

Cancel

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

Once you enter all the subaccount, the connector page will looks like this.

The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with 'Configuration', 'Security Status', 'Alerting', 'Troubleshooting', 'High Availability', 'Hardware Metrics Monitor', and a 'Monitor' section. Below that is a 'CIGUS2' section with 'Cloud to On-Premises', 'On-Premises to Cloud', 'Monitor (Cloud to On-Premises)', 'Monitor (On-Premises to Cloud)', 'Audits', and 'Log and Trace Files'. At the bottom are 'Important Links' and 'Legal Information'.

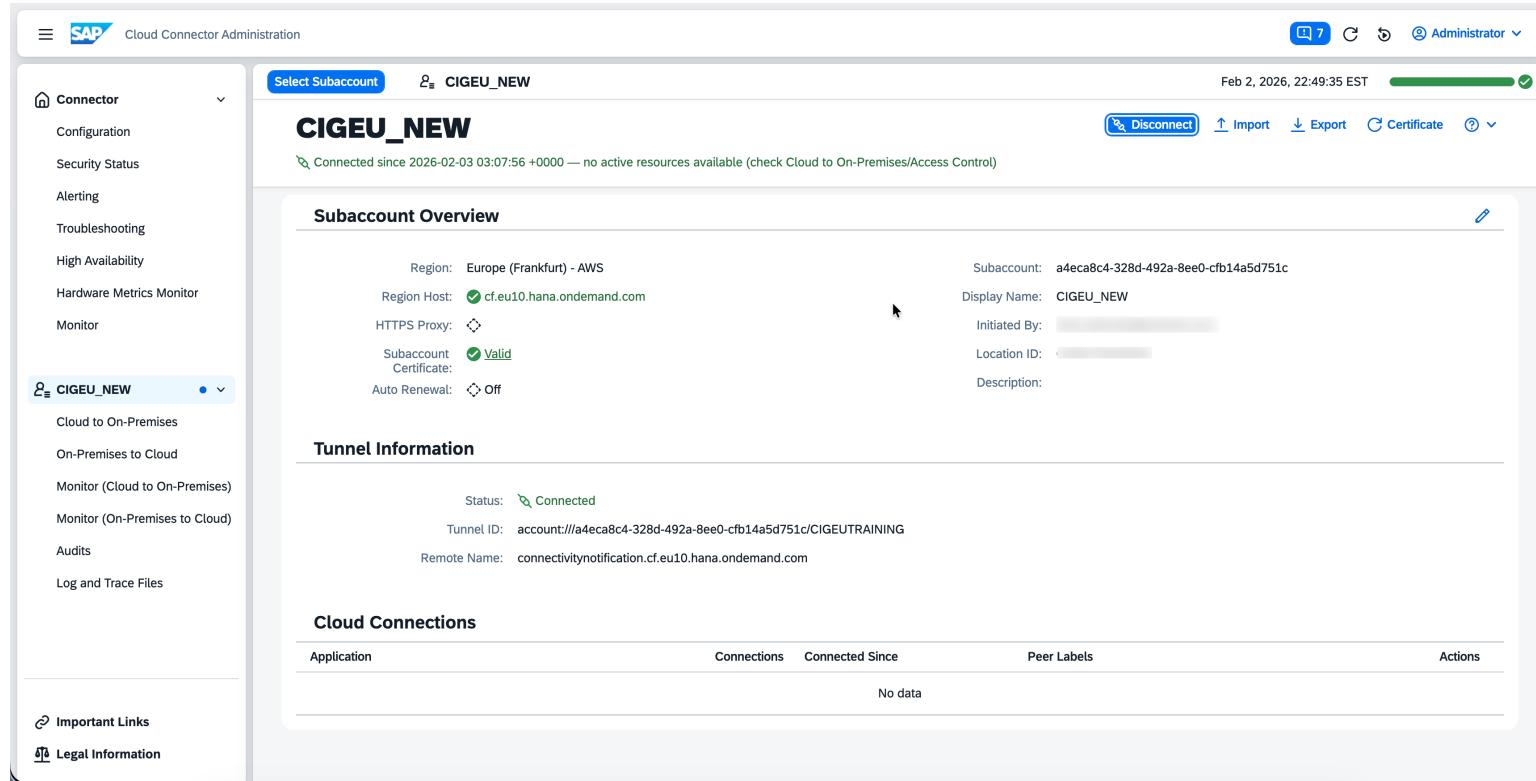
The main content area has a 'Select Subaccount' tab and a 'Cross-Subaccount' tab. The 'Connector' section shows a Connector ID: CD2A39EE7AB74FC6BD6407F932BA581B, Local Name: [REDACTED], and Local IP: [REDACTED]. It also displays security status (Low risk), status (Disabled), availability (High), and alerts (1).

The 'Subaccount Dashboard (4)' table lists four subaccounts:

| Status | Subaccount | Display Name | Location ID | Region | Actions |
|----------------|--------------------------------------|--------------|-------------|--------------------------|---------|
| Orange diamond | a4eca8c4-328d-492a-8ee0-cfb14a5d751c | CIGEU_NEW | [REDACTED] | Europe (Frankfurt) - AWS | > |
| Orange diamond | c2cd9a88-7143-472a-a358-ac050eacdc39 | CIGEU1 | [REDACTED] | Europe (Frankfurt) - AWS | > |
| Orange diamond | 2fdf90d-496d-4c6d-9f21-26d1bb9f37b5 | CIGEU2 | [REDACTED] | Europe (Frankfurt) - AWS | > |
| Orange diamond | c7845fda-254d-42ef-9069-70bde1d2b647 | CIGEU3 | [REDACTED] | Europe (Frankfurt) - AWS | > |

The 'Service Channels Overview (0)' table is empty, showing '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**.



The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar is collapsed, and the main content area is for the subaccount **CIGEU_NEW**. The top navigation bar includes the SAP logo, the title "Cloud Connector Administration", a "Select Subaccount" dropdown set to "CIGEU_NEW", a timestamp "Feb 2, 2026, 22:49:35 EST", and a user "Administrator".

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: Off | Initiated By: [redacted] |
| Subaccount Certificate: Valid | Location ID: [redacted] |
| Auto Renewal: Off | Description: [redacted] |

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 | | | | |

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

The screenshot shows the SAP Cloud Connector Administration interface. The top navigation bar includes the SAP logo, 'Cloud Connector Administration', a search bar, and a user dropdown for 'Administrator'. The main content area is titled 'Cloud to On-Premises' and displays a table for 'Mapping Virtual to Internal System (0)'. The table has columns for 'Status', 'Virtual Host', 'Internal Host', 'Check Result', 'Protocol', 'Back-end Type', and 'Add-ons'. A red box highlights the 'Select Subaccount' button at the top left of the main content area. The left sidebar shows a tree structure with 'Connector' selected, and under 'Connector', 'Cloud to On-Premises' is selected, indicated by a red box. Other options in the sidebar include 'On-Premises to Cloud', 'Monitor (Cloud to On-Premises)', 'Monitor (On-Premises to Cloud)', 'Audits', and 'Log and Trace Files'. At the bottom of the sidebar are links for 'Important Links' and 'Legal Information'.

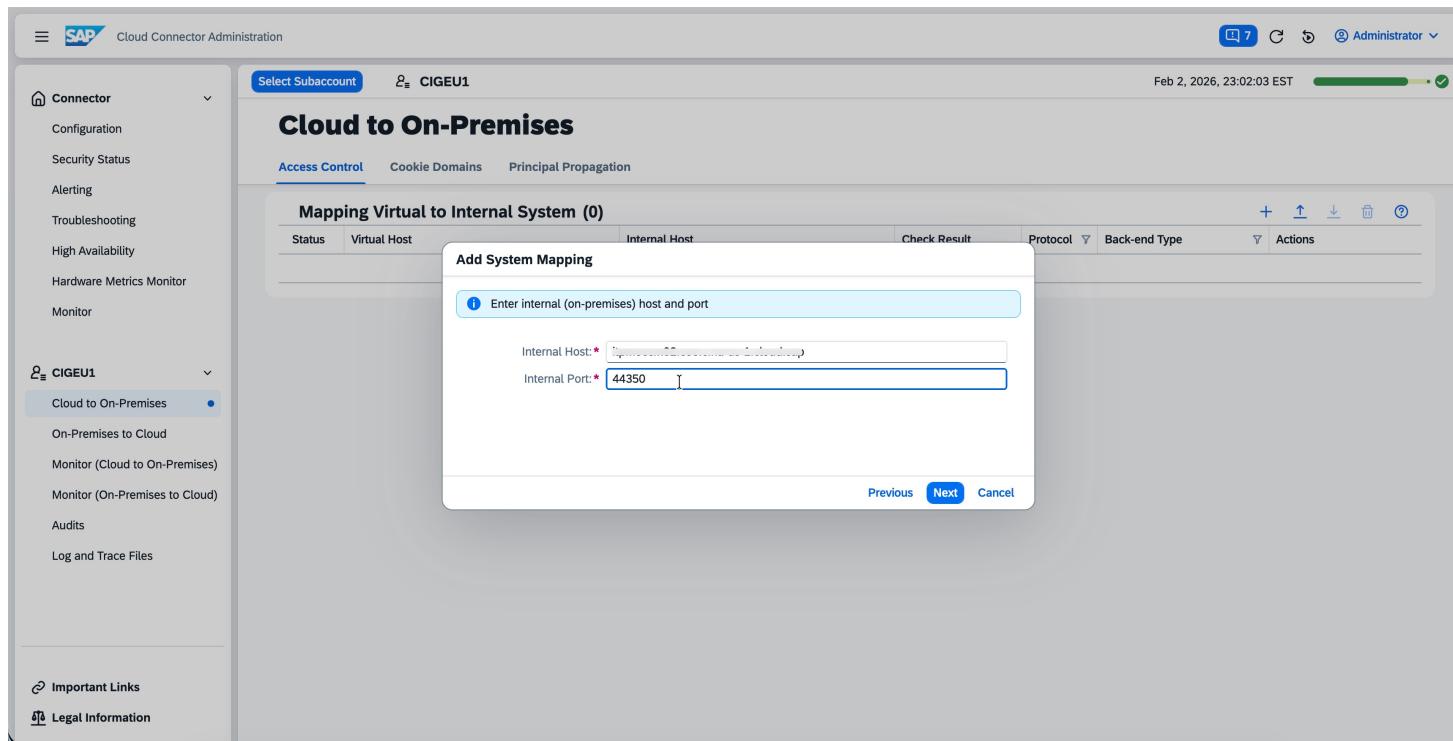
Select the Back-end Type as ABAP System if you are using SAP ECC or S/4 HANA

The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has sections 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 shows 'Access Control', 'Cookie Domains', and 'Principal Propagation'. A modal dialog is open titled 'Add System Mapping' with the instruction 'Select back-end type of on-premises system'. A dropdown menu shows 'ABAP System' selected. The background table 'Mapping Virtual to Internal System (0)' has columns for Status, Virtual Host, Internal Host, Check Result, Protocol, Back-end Type, and Actions. The status bar at the bottom shows 'Feb 2, 2026, 23:02:03 EST' and a battery icon.

Choose the protocol as HTTPS

The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with 'Cloud to On-Premises' selected. The main content area is titled 'Cloud to On-Premises' and shows the 'Access Control' tab is active. A modal dialog is open, titled 'Add System Mapping', with a note 'Select protocol for communication with on-premises system'. A dropdown menu shows 'Protocol: HTTPS' selected. The background shows a table for 'Mapping Virtual to Internal System' with one row. The top right of the screen shows the date 'Feb 2, 2026, 23:02:03 EST' and a green progress bar.

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



SAP Cloud Connector Administration

Select Subaccount: CIGEU1

Feb 2, 2026, 23:02:03 EST

Administrator

Cloud to On-Premises

Access Control Cookie Domains Principal Propagation

Mapping Virtual to Internal System (0)

| Status | Virtual Host | Internal Host | Check Result | Protocol | Back-end Type | Actions |
|--|--------------|---------------|--------------|----------|---------------|---------|
| Add System Mapping | | | | | | |
| <p>Enter internal (on-premises) host and port</p> <p>Internal Host: * <input type="text" value="http://192.168.1.100:44350"/></p> <p>Internal Port: * <input type="text" value="44350"/></p> <p>Previous Next Cancel</p> | | | | | | |

Connector

- Configuration
- Security Status
- Alerting
- Troubleshooting
- High Availability
- Hardware Metrics Monitor
- Monitor

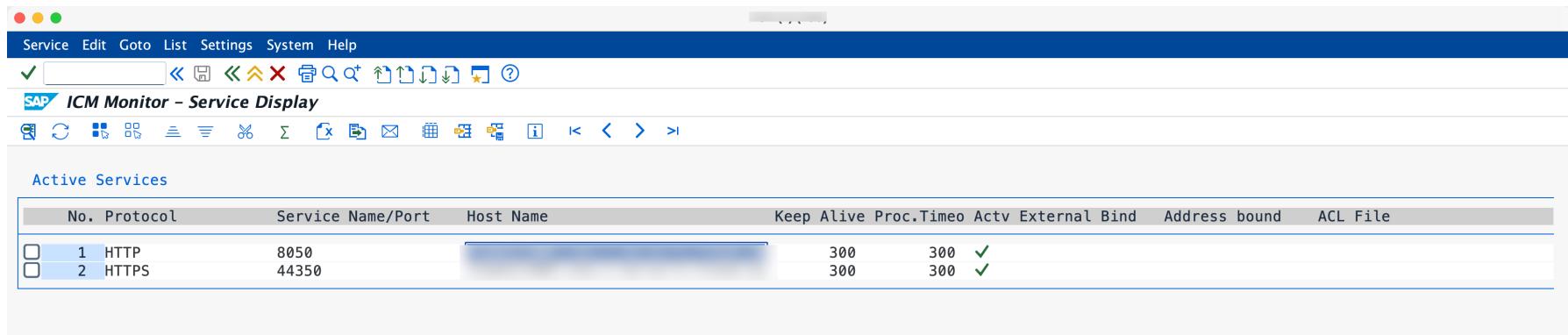
CIGEU1

- 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

SMICM screen shows the hostname of your SAP application server.

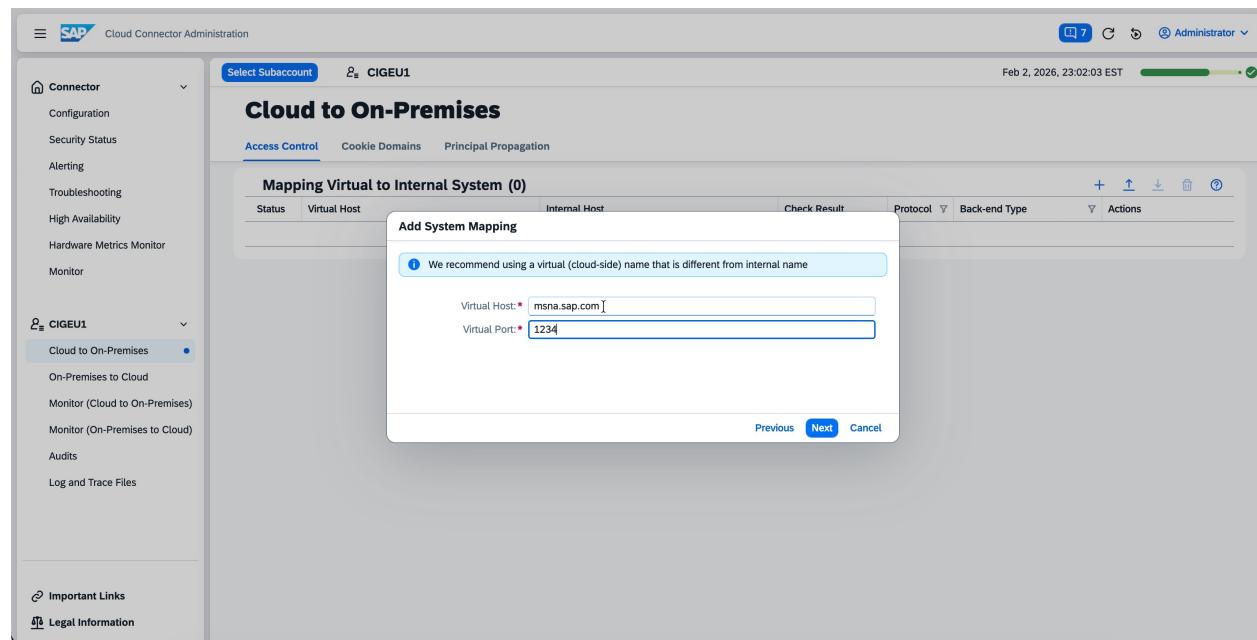


The screenshot shows the SAP ICM Monitor - Service Display interface. The top navigation bar includes Service, Edit, Goto, List, Settings, System, and Help. Below the navigation bar is a toolbar with various icons for search, refresh, and navigation. The main title is "SAP ICM Monitor - Service Display". The interface is divided into sections: "Active Services" and "Service Details". The "Active Services" section contains a table with the following data:

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

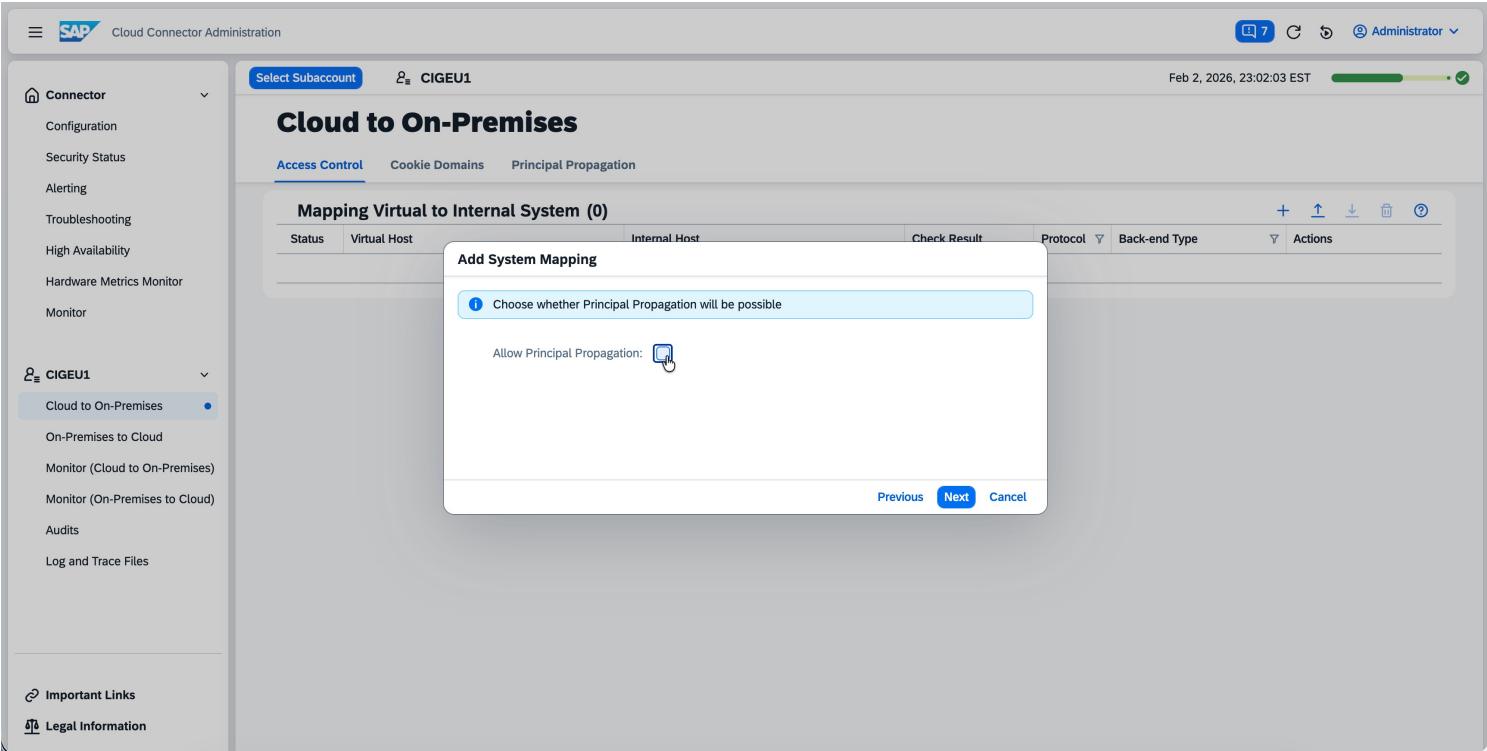


The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar is titled 'Connector' and includes options like Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor. The subaccount 'CIGEU1' is selected, with 'Cloud to On-Premises' highlighted. The main content area is titled 'Cloud to On-Premises' and shows the 'Mapping Virtual to Internal System (0)' table. A modal dialog is open, titled 'Add System Mapping', with the following fields:

| Virtual Host | Virtual Port |
|--------------|--------------|
| msna.sap.com | 1234 |

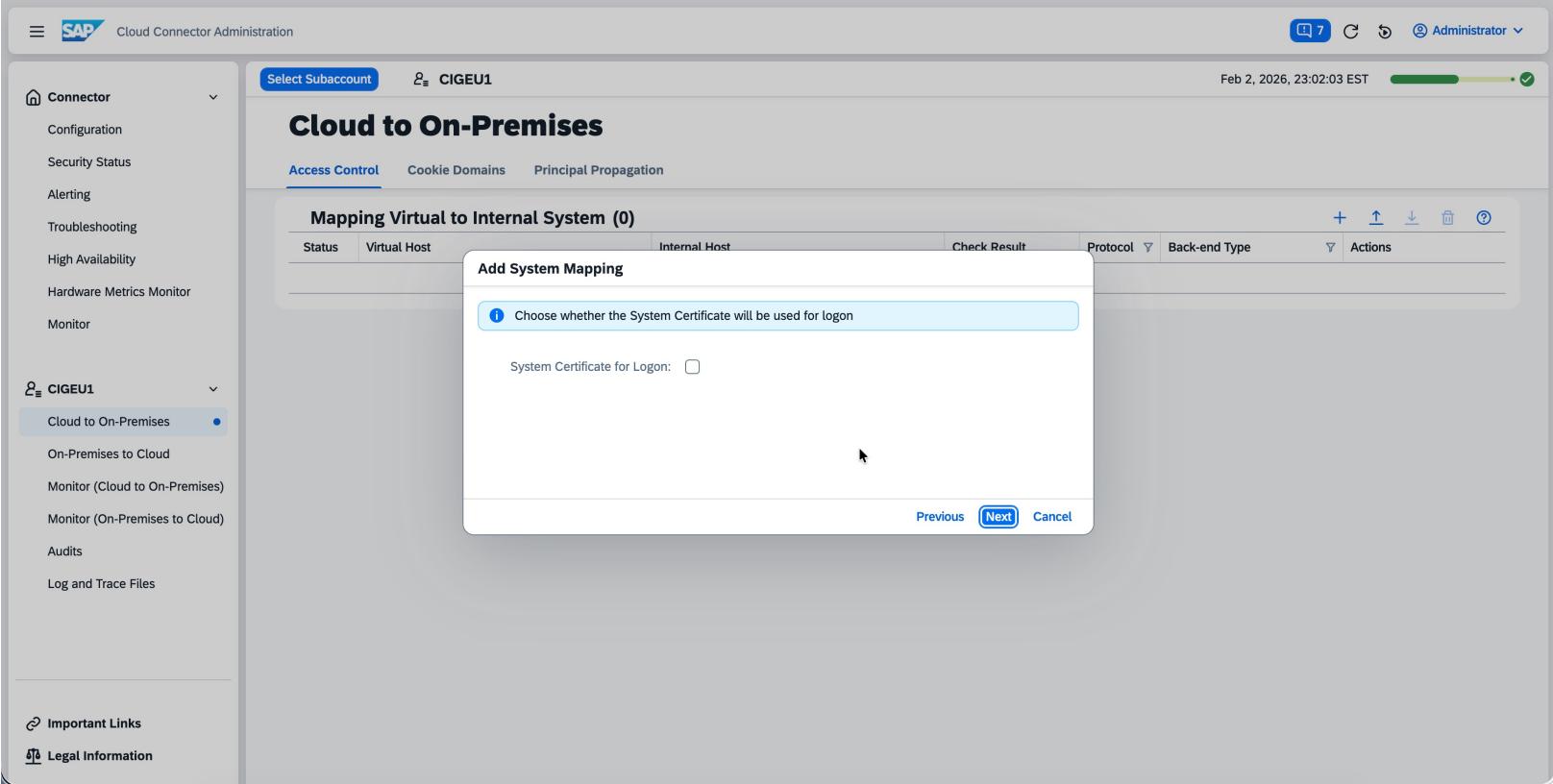
A tooltip in the dialog box says: "We recommend using a virtual (cloud-side) name that is different from internal name".

Uncheck the Allow Principal Propagation



The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar is titled 'Connector' and includes options like Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor. The main navigation bar shows 'Cloud to On-Premises' is selected. The main content area is titled 'Cloud to On-Premises' and has tabs for Access Control, Cookie Domains, and Principal Propagation. The 'Principal Propagation' tab is active, showing a sub-section titled 'Mapping Virtual to Internal System (0)'. A modal window titled 'Add System Mapping' is open, containing a note: 'Choose whether Principal Propagation will be possible' and a checkbox labeled 'Allow Principal Propagation:'. The checkbox is currently checked. At the bottom of the modal are buttons for Previous, Next, and Cancel.

Uncheck the System Certificate for Logon



The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with 'Cloud to On-Premises' selected. The main content area is titled 'Cloud to On-Premises' and shows the 'Access Control' tab is active. A sub-section titled 'Mapping Virtual to Internal System (0)' is displayed. A modal window titled 'Add System Mapping' is open, containing the instruction 'Choose whether the System Certificate will be used for logon' and a checkbox labeled 'System Certificate for Logon:'. The checkbox is currently checked. At the bottom of the modal are 'Previous', 'Next', and 'Cancel' buttons. The top right of the screen shows the date 'Feb 2, 2026, 23:02:03 EST' and a progress bar.

Select Use Virtual host as Host in Request Header

The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with 'Configuration', 'Security Status', 'Alerting', 'Troubleshooting', 'High Availability', 'Hardware Metrics Monitor', and 'Monitor'. Below it is a 'CIGEU1' section with 'Cloud to On-Premises' (selected), 'On-Premises to Cloud', 'Monitor (Cloud to On-Premises)', 'Monitor (On-Premises to Cloud)', 'Audits', and 'Log and Trace Files'. At the bottom are 'Important Links' and 'Legal Information'. The main content area is titled 'Cloud to On-Premises' and shows 'Mapping Virtual to Internal System (0)'. It has tabs for 'Access Control', 'Cookie Domains', and 'Principal Propagation'. A table header includes 'Status', 'Virtual Host', 'Internal Host', 'Check Result', 'Protocol', 'Back-end Type', and 'Actions'. A modal window titled 'Add System Mapping' is open, with a step '1 Select host for request header field HOST' and a dropdown menu showing 'Use Virtual Host'. The bottom of the modal has 'Previous', 'Next' (highlighted in blue), and 'Cancel' buttons. The top right of the interface shows the date 'Feb 2, 2026, 23:02:03 EST' and a progress bar.

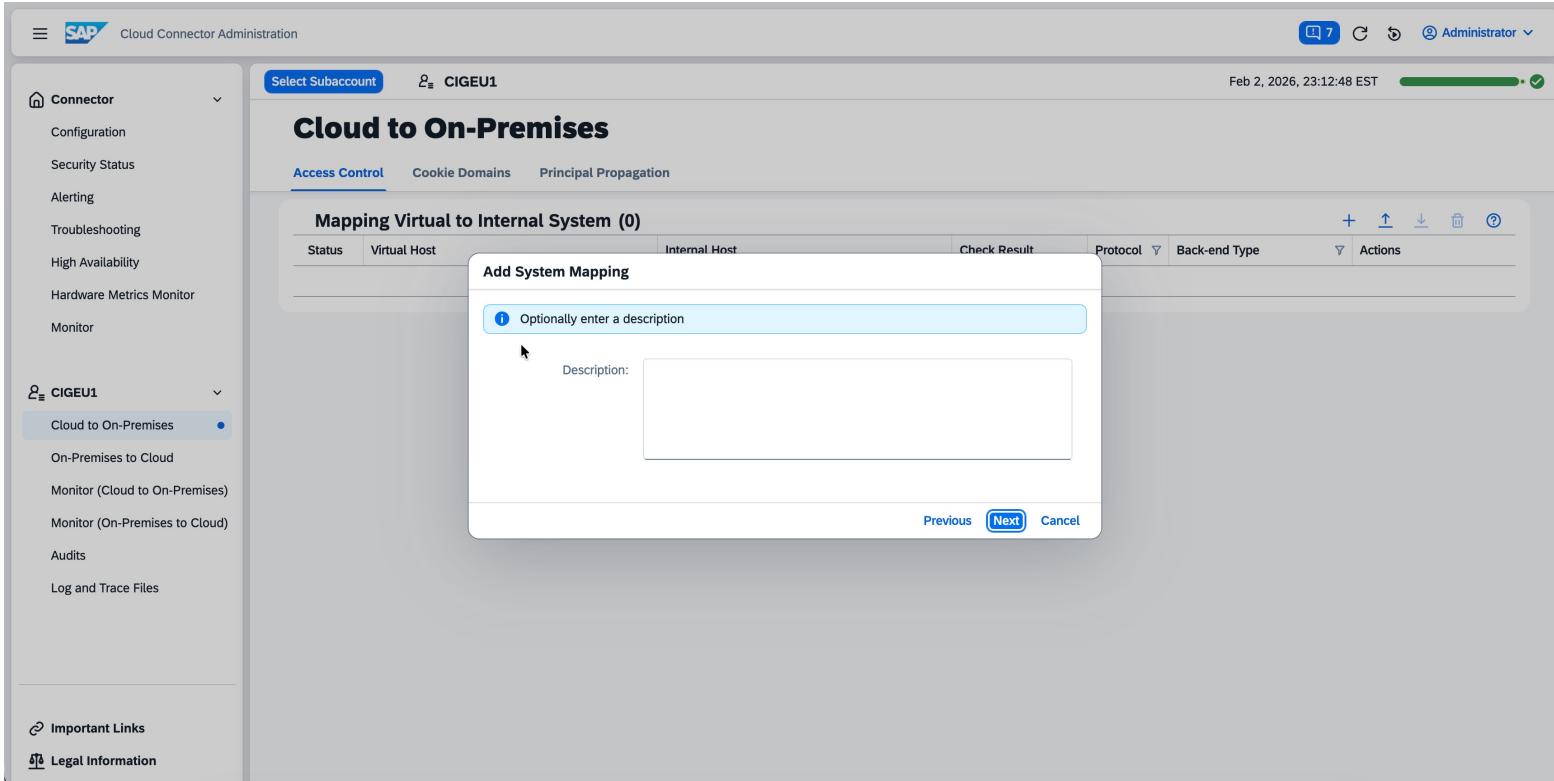
Enter the System ID. This is an optional field

The screenshot shows the SAP Cloud Connector Administration interface. The top navigation bar includes the SAP logo, 'Cloud Connector Administration', a message center with 7 notifications, a user dropdown for 'Administrator', and a timestamp 'Feb 2, 2026, 23:12:48 EST'.

The left sidebar has a 'Connector' section with links: Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor. Below that is a 'Cloud to On-Premises' section with 'Cloud to On-Premises' (selected), On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, and Log and Trace Files. At the bottom are links for Important Links and Legal Information.

The main content area is titled 'Cloud to On-Premises' and shows the 'Access Control' tab is selected. Below it 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, containing a note 'Optional: enter a system ID' and a text input field with the value 'EUP'. The modal has buttons for 'Previous', 'Next' (highlighted in blue), and 'Cancel'.

This is an optional field entered for your reference.



The screenshot shows the SAP Cloud Connector Administration interface. The top navigation bar includes the SAP logo, the title "Cloud Connector Administration", a "Select Subaccount" dropdown set to "CIGEU1", a timestamp "Feb 2, 2026, 23:12:48 EST", and a user "Administrator". The left sidebar has a "Connector" section with links for Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor. Below that is a "CIGEU1" section with "Cloud to On-Premises" selected, followed by On-Premises to Cloud, Monitor (Cloud to On-Premises), Monitor (On-Premises to Cloud), Audits, and Log and Trace Files. At the bottom are links for "Important Links" and "Legal Information". The main content area is titled "Cloud to On-Premises" and "Mapping Virtual to Internal System (0)". It features tabs for Access Control, Cookie Domains, and Principal Propagation. A table header for "Mapping Virtual to Internal System (0)" includes columns for Status, Virtual Host, Internal Host, Check Result, Protocol, Back-end Type, and Actions. A modal window titled "Add System Mapping" contains a text input field with placeholder "Description:" and a note "Optionally enter a description". The modal has "Previous", "Next", and "Cancel" buttons at the bottom.

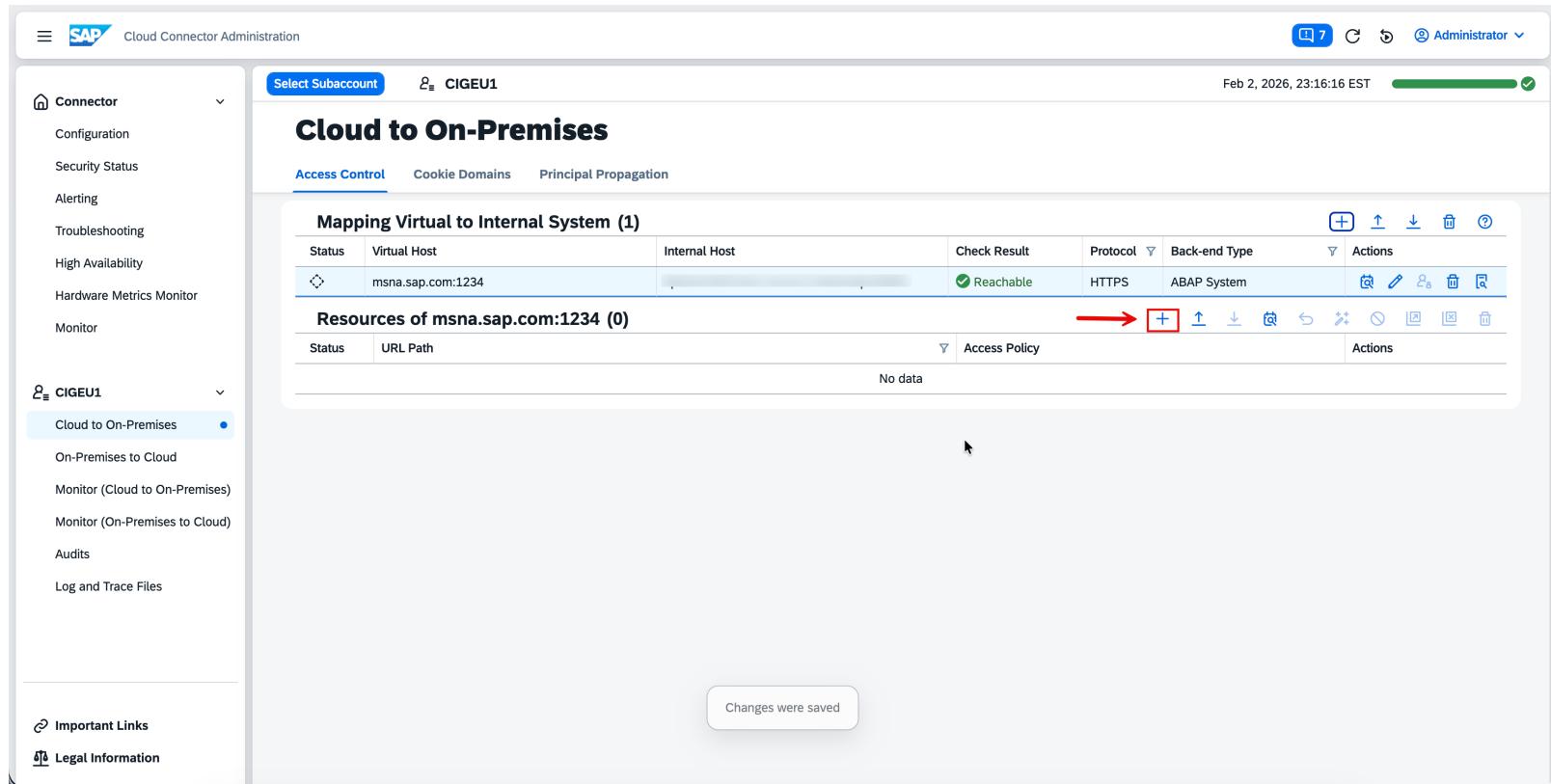
Select the Check Internal Host box and click Finish

The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with 'Cloud to On-Premises' selected. The main content area is titled 'Cloud to On-Premises' and shows a table for 'Mapping Virtual to Internal System (0)'. A modal dialog is open, titled 'Add System Mapping', with a 'Summary' tab selected. The summary shows:

- Protocol: HTTPS (None)
- Internal: [redacted]
- Virtual: msna.sap.com:1234
- Check Internal Host:

At the bottom of the dialog are 'Previous', 'Finish', and 'Cancel' buttons. The top right of the interface shows the date 'Feb 2, 2026, 23:12:48 EST' and a status bar with a green progress bar and a checkmark.

Click the add resource option option.



SAP Cloud Connector Administration

Select Subaccount: CIGEU1

Feb 2, 2026, 23:16:16 EST

Administrator

Cloud to On-Premises

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

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 shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with various sub-options like Configuration, Security Status, Alerting, Troubleshooting, High Availability, Hardware Metrics Monitor, and Monitor. Below that is a 'Cloud to On-Premises' section with 'Cloud to On-Premises' selected. The main content area is titled 'Cloud to On-Premises' and shows 'Access Control', 'Cookie Domains', and 'Principal Propagation' tabs. A modal window titled 'Add Resource' is open, showing a table with a single row for 'msna.sap.com:12000'. The modal has fields for 'URL Path' (set to '/sap/'), 'Active' (checked), 'Upgrade Allowed' (unchecked), 'Access Policy' (radio button selected for 'Path and All Sub-Paths'), and a 'Description' field. In the background, there's a list of resources with columns for 'Protocol', 'Back-end Type', and 'Actions'. One item in the list is 'HTTPS ABAP System'. At the bottom of the modal are 'Save' and 'Cancel' buttons.

SAP Cloud Connector Administration

Select Subaccount **CIGEU1** Feb 2, 2026, 23:20:22 EST

Administrator

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

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 | |

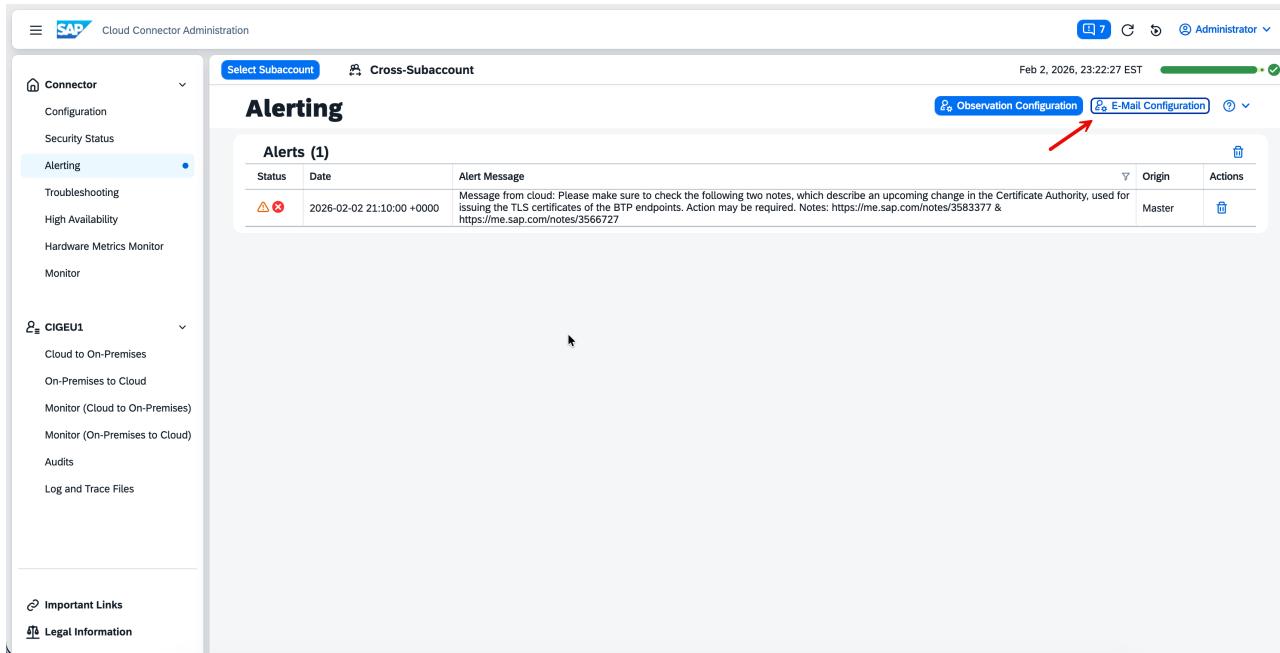
Resources of msna.sap.com:1234 (1)

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

Important Links

Legal Information

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.

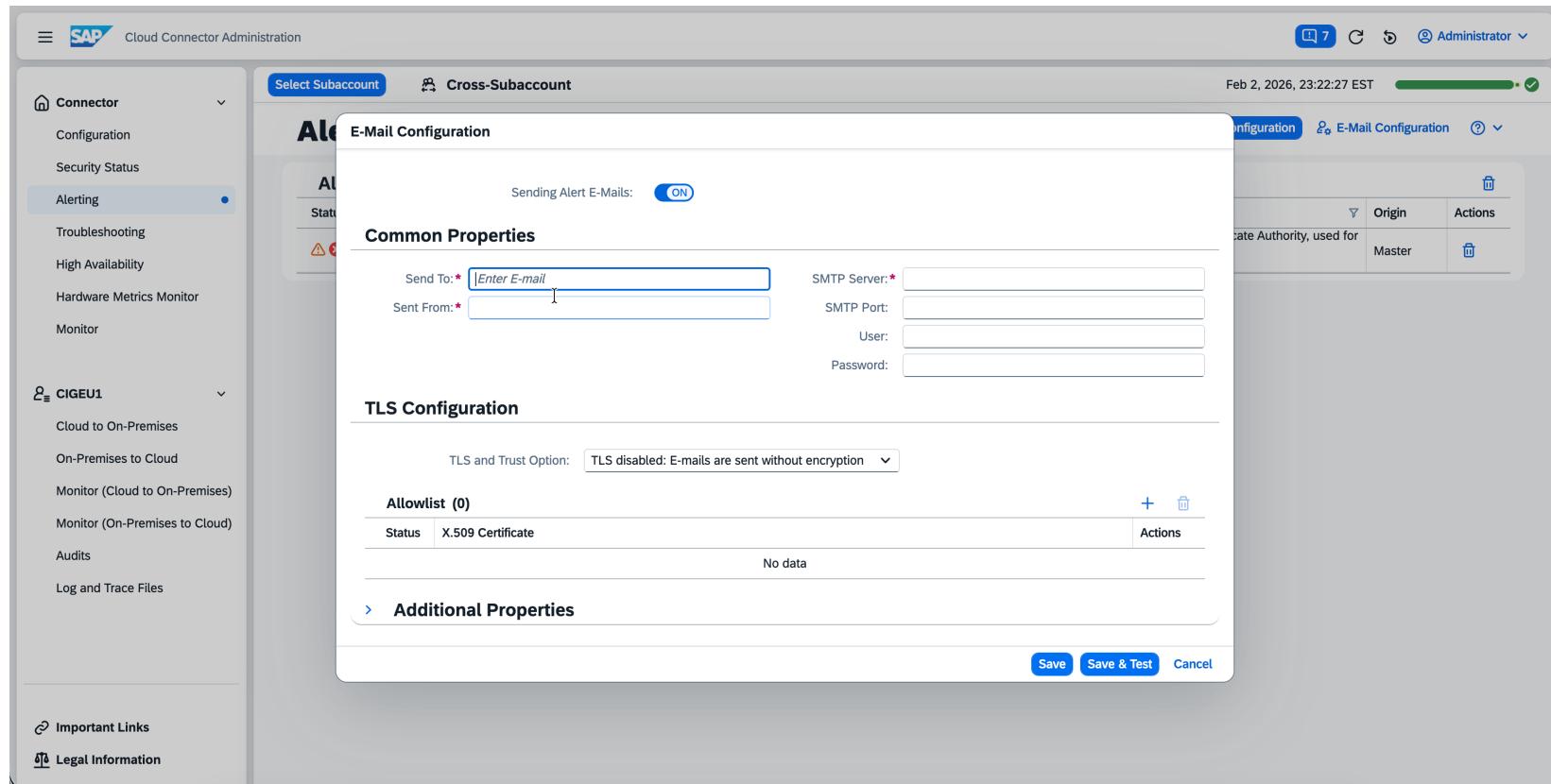


The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with 'Alerting' selected. The main content area is titled 'Alerting' and shows 'Alerts (1)'. One alert is listed with the following details:

| 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: https://me.sap.com/notes/3583377 & https://me.sap.com/notes/3566727 | Master | 🔗 |

At the top right of the alert details, there are two links: 'Observation Configuration' and 'E-Mail Configuration'. A red arrow points to the 'E-Mail Configuration' link.

Please update the details and click Save.

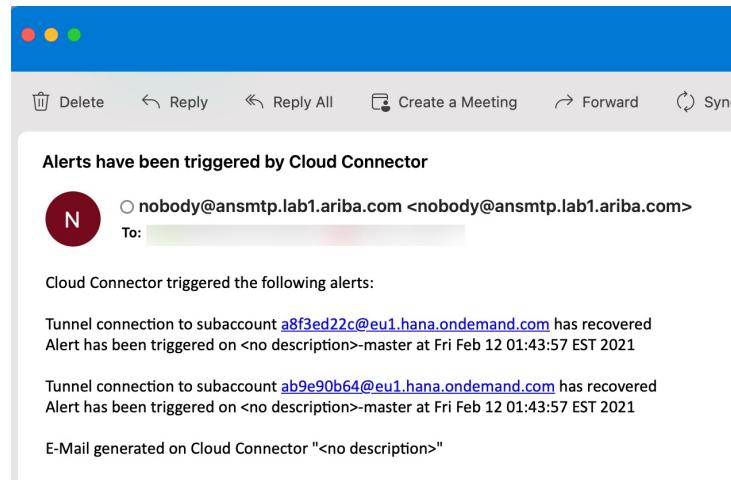
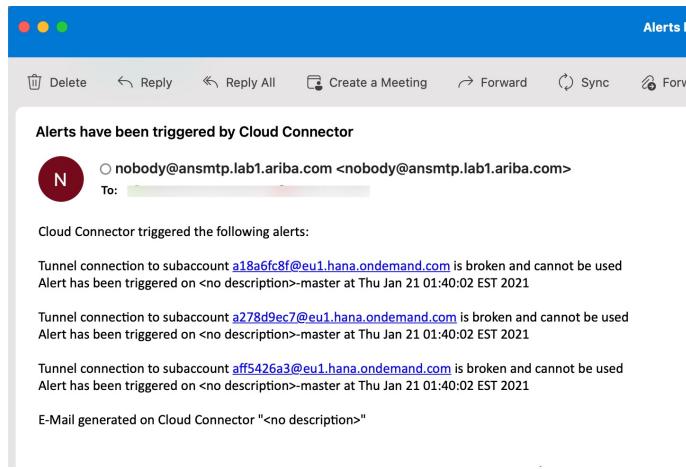


The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has a 'Connector' section with 'Alerting' selected, and a 'CIGEU1' section with 'Cloud to On-Premises' selected. The main content area is titled 'E-Mail Configuration' and contains the following sections:

- Common Properties:** Includes fields for 'Send To:' (with placeholder 'Enter E-mail'), 'Sent From:' (with placeholder 'Enter E-mail'), 'SMTP Server:', 'SMTP Port:', 'User:', and 'Password:'.
- TLS Configuration:** Shows 'TLS and Trust Option: TLS disabled: E-mails are sent without encryption'.
- Allowlist (0):** A table with columns 'Status' and 'Actions'. It shows one entry: 'X.509 Certificate'.
- Additional Properties:** A section with a plus sign icon.

At the bottom right are buttons for 'Save', 'Save & Test', and '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) cf-eu10 | https://test-integration.eu.managedgateway.cloud.sap/ https://integration.eu.managedgateway.cloud.sap/ | Refer the column LB IPs (ingress, for incoming request) from Regions and API Endpoints Available for the Cloud Foundry Environment |
| US West (Colorado Springs) cf-us10 | https://test-integration.us.managedgateway.cloud.sap/ https://integration.us.managedgateway.cloud.sap/ | |
| China (Shanghai) cf-cn40 | https://test-integration.managedgateway.sapcloud.cn/ https://integration.managedgateway.sapcloud.cn | |
| KSA (Riyadh) | https://test-integration.ksa.managedgateway.cloud.sap/ https://integrationportal.eu.managedgateway.cloud.sap/ | |
| UAE (Dubai) cf-ae01 | https://integration.uae.managedgateway.cloud.sap/ https://test-integration.uae.managedgateway.cloud.sap/ | |

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:

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