SAP Ariba

Cloud Connector configuration for Integration Suite Managed Gateway

Bharath Balakrishnan - SAP Ariba Cloud Integration Support

PUBLIC

Confidential Documents:

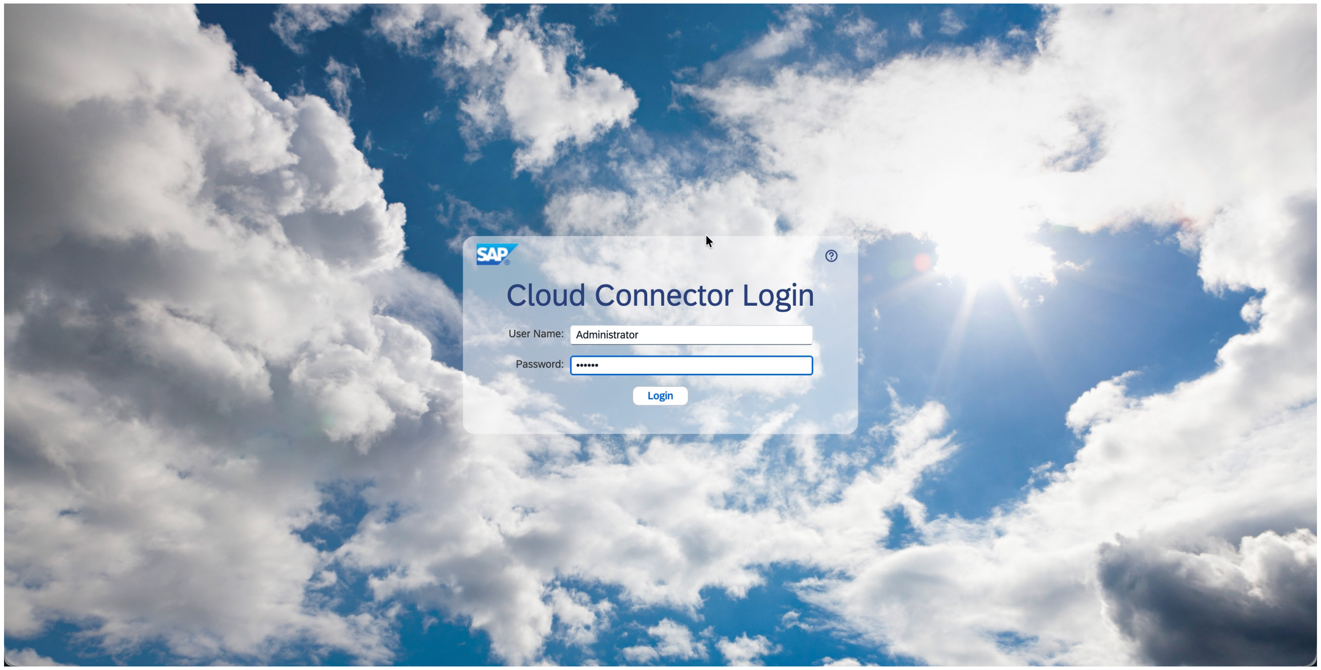
THE BEST RUN SAP

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**.

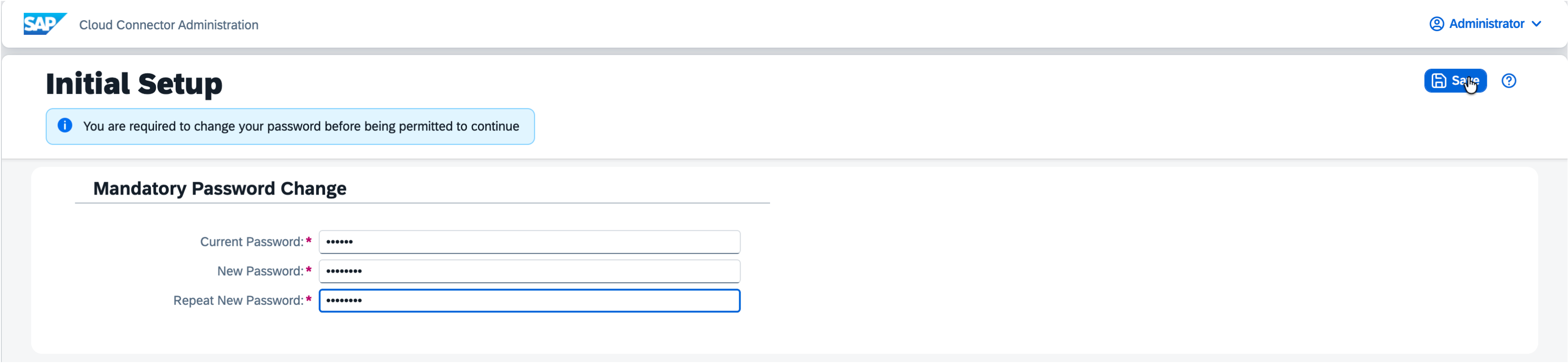


Cloud Connector Login

User Name: Administrator

Password: ••••••

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



Initial Setup

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

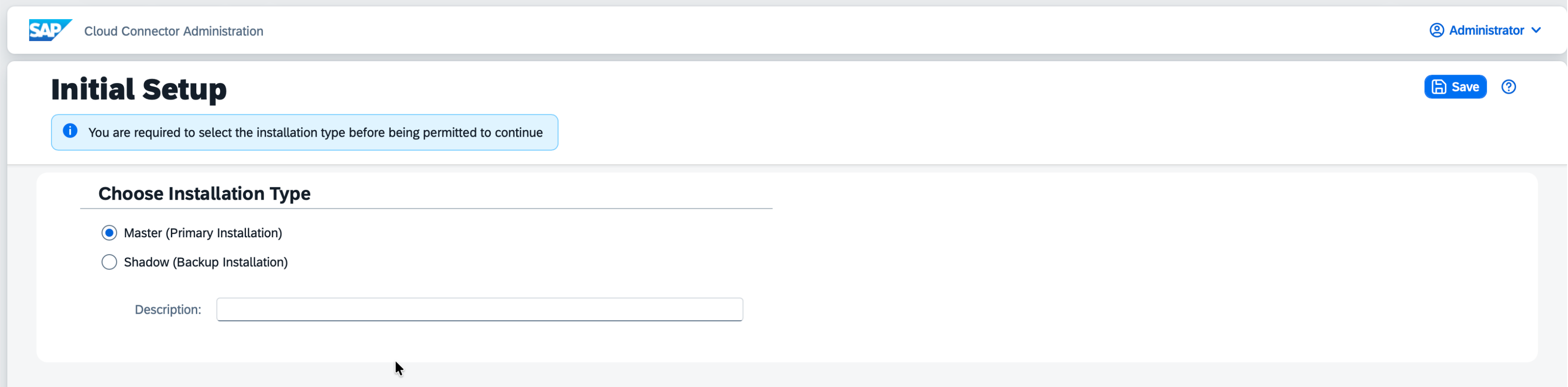
Mandatory Password Change

Current Password:* ••••••

New Password:* ••••••••

Repeat New Password:* ••••••••

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



Initial Setup

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

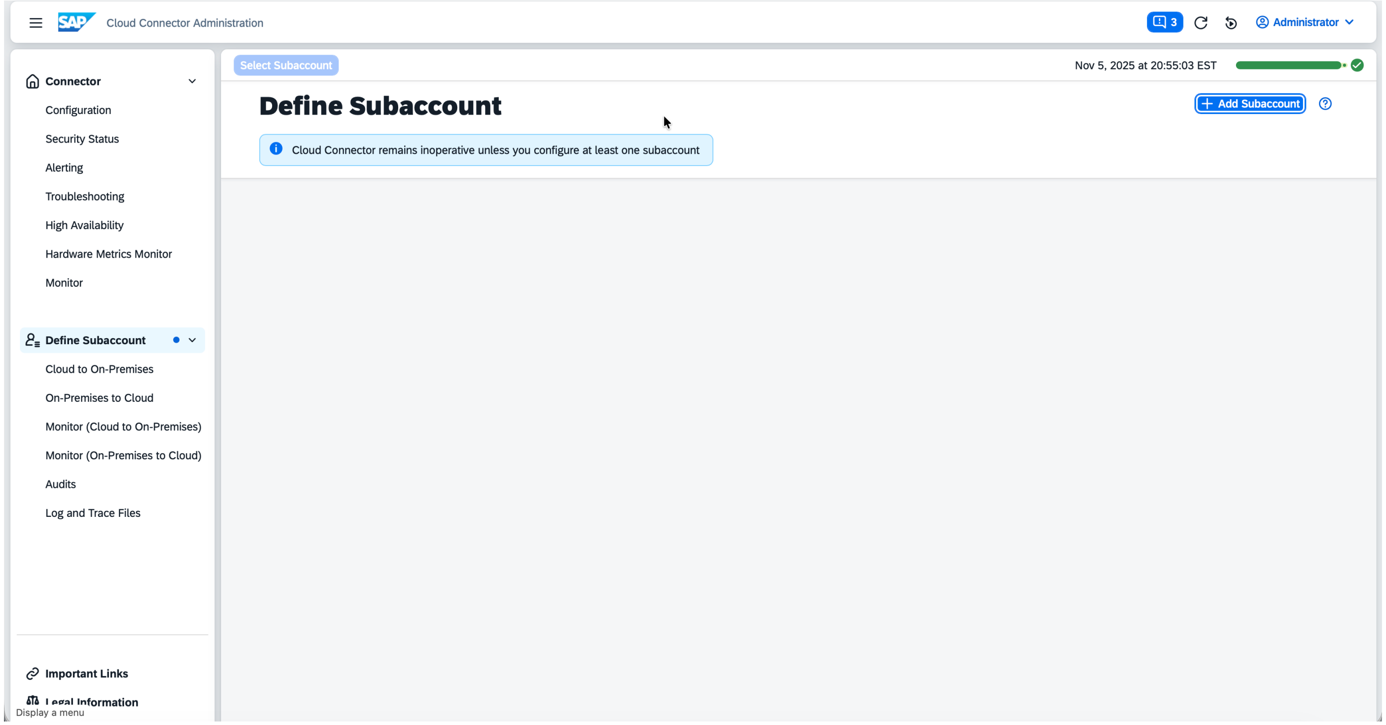
Choose Installation Type

● Master (Primary Installation)

○ Shadow (Backup Installation)

Description:

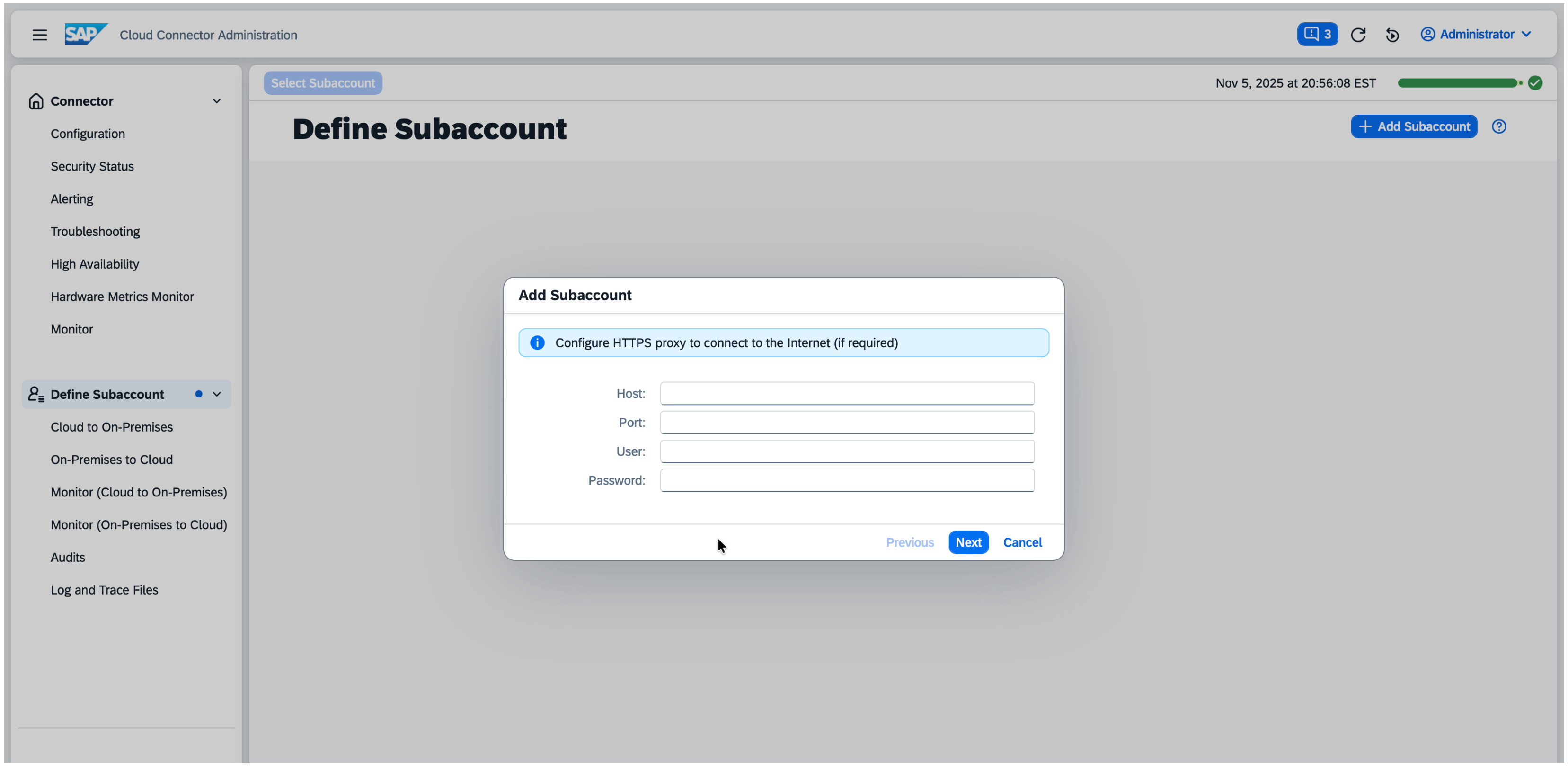
When you login for the first time you will not see any subaccounts in the connector page. You need to add separate sub accounts for test and production system. Click + Add Subaccount button. In case if you already have other subaccounts added or if you already added Managed Gateway Neo Subaccount and wanted to add managed gateway cloud foundry subaccounts, proceed with + Add Subaccount button.



Define Subaccount

Cloud Connector remains inoperative unless you configure at least one subaccount

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



Nov 5, 2025 at 20:56:08 EST

Define Subaccount

Add Subaccount

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

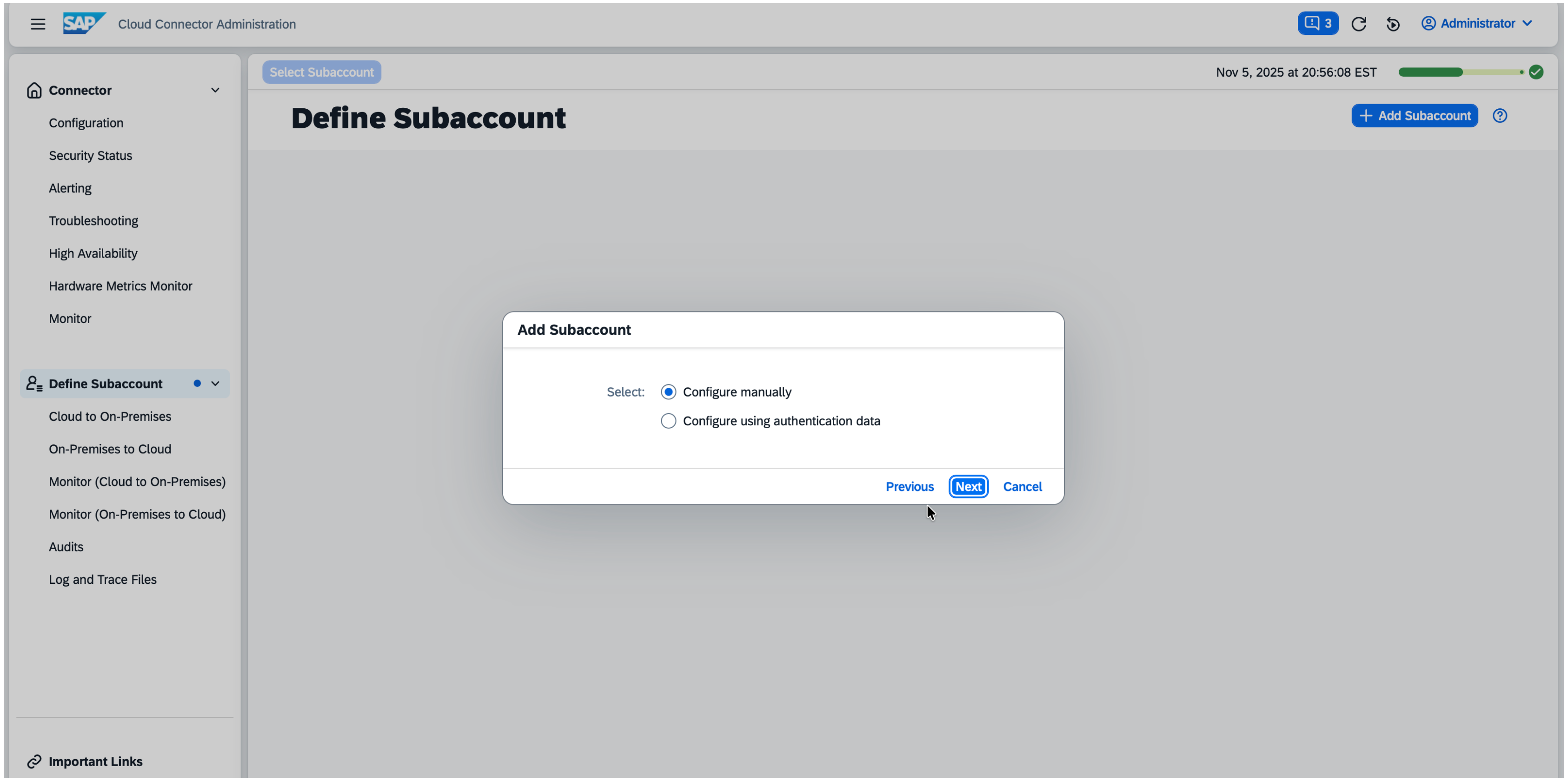
Host:

Port:

User:

Password:

Choose configure manually and click Next



Add Subaccount

Select: ● Configure manually
○ Configure using authentication data

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.

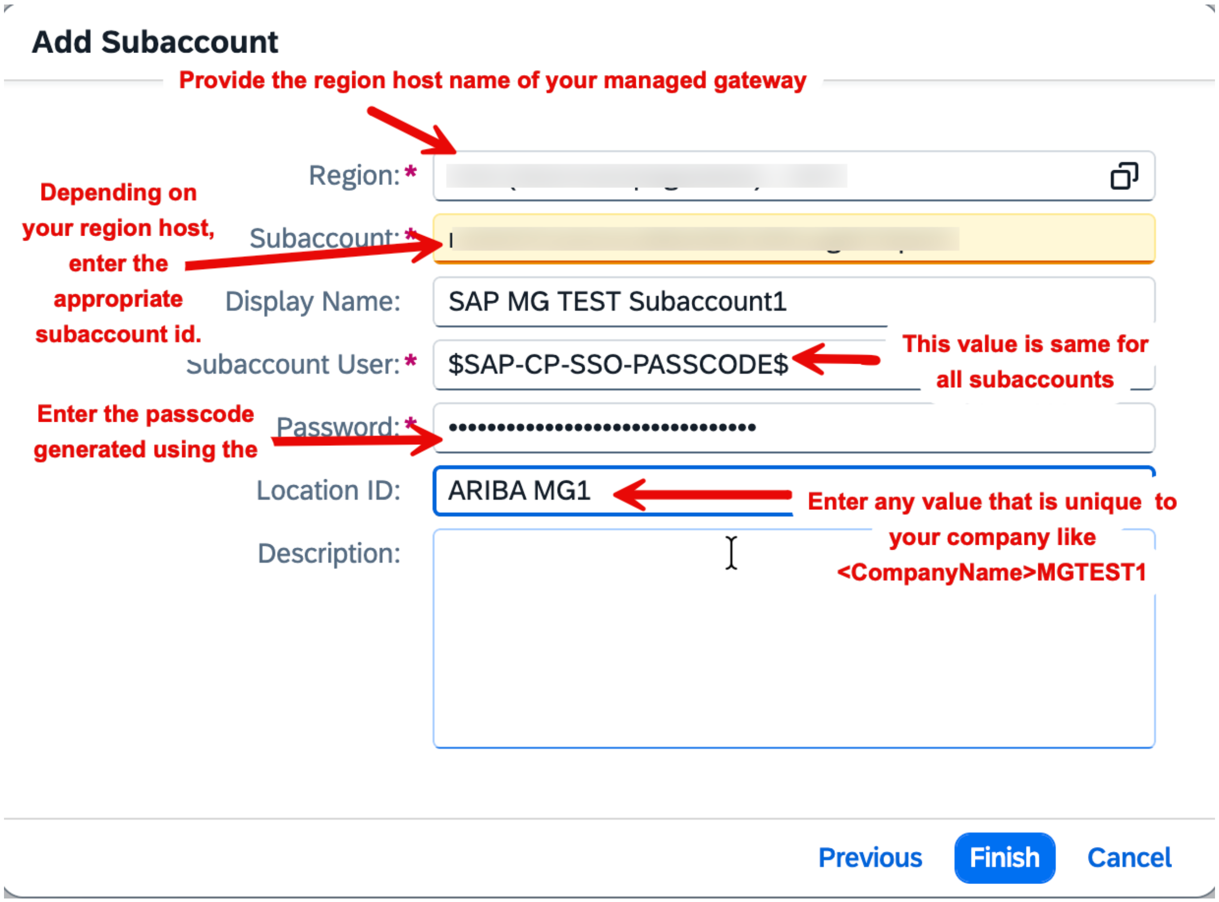
Subaccount User: Enter “$SAP-CP-SSO-PASSCODE$” (without double quotes)

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

Region:* [redacted]

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

Subaccount:* [redacted]

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:* ••••••••••••••••••••••••••••••••

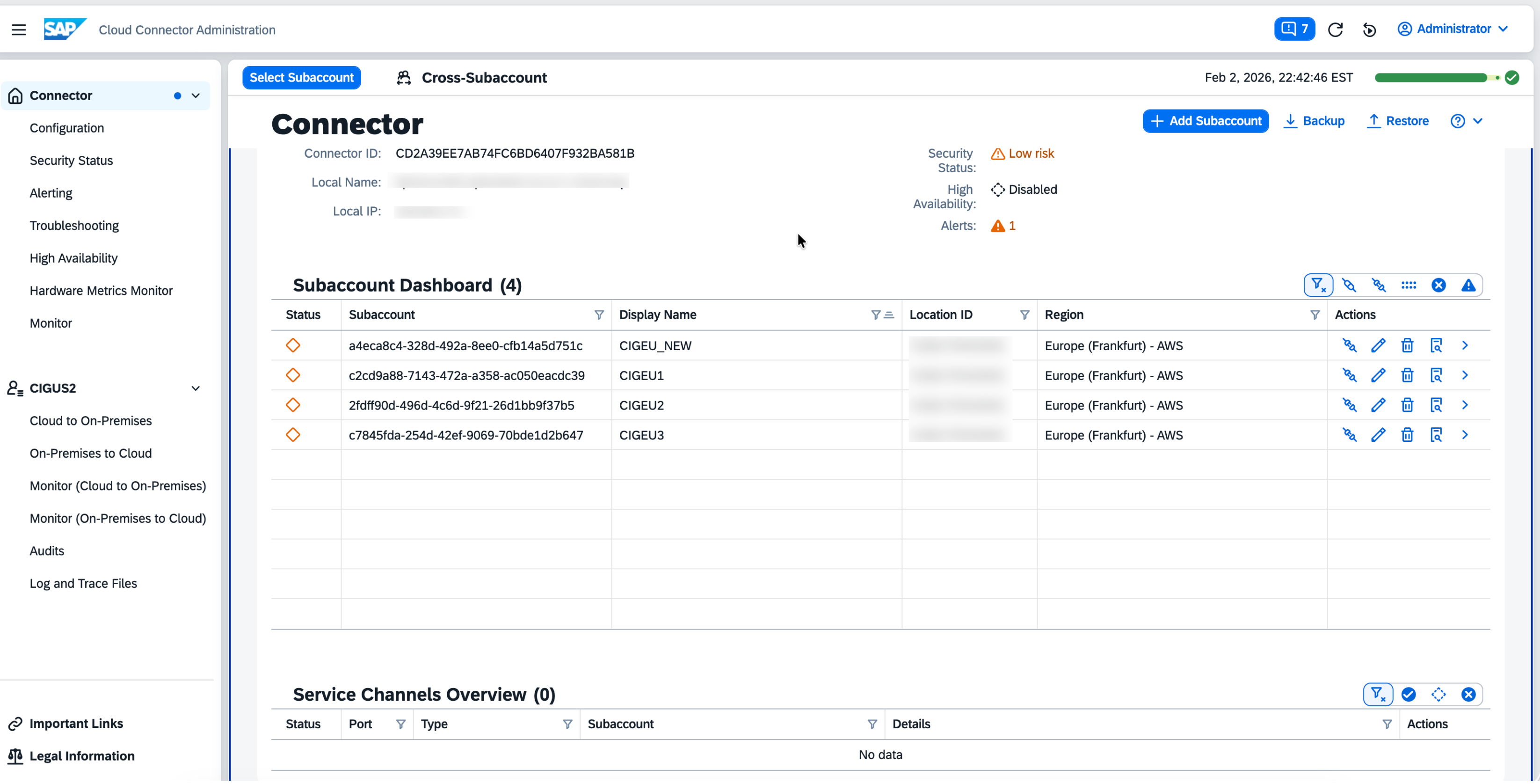
Location ID: ARIBA MG1

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

Description:

Managed Gateway Region	Region Host Name	Sub Account Details
China	China (Shangai) 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.



Feb 2, 2026, 22:42:46 EST

Connector

Connector ID: CD2A39EE7AB74FC6BD6407F932BA581B

Local Name: [redacted]

Local IP: [redacted]

Security Status: Low risk

High Availability: Disabled

Alerts: 1

Subaccount Dashboard (4)

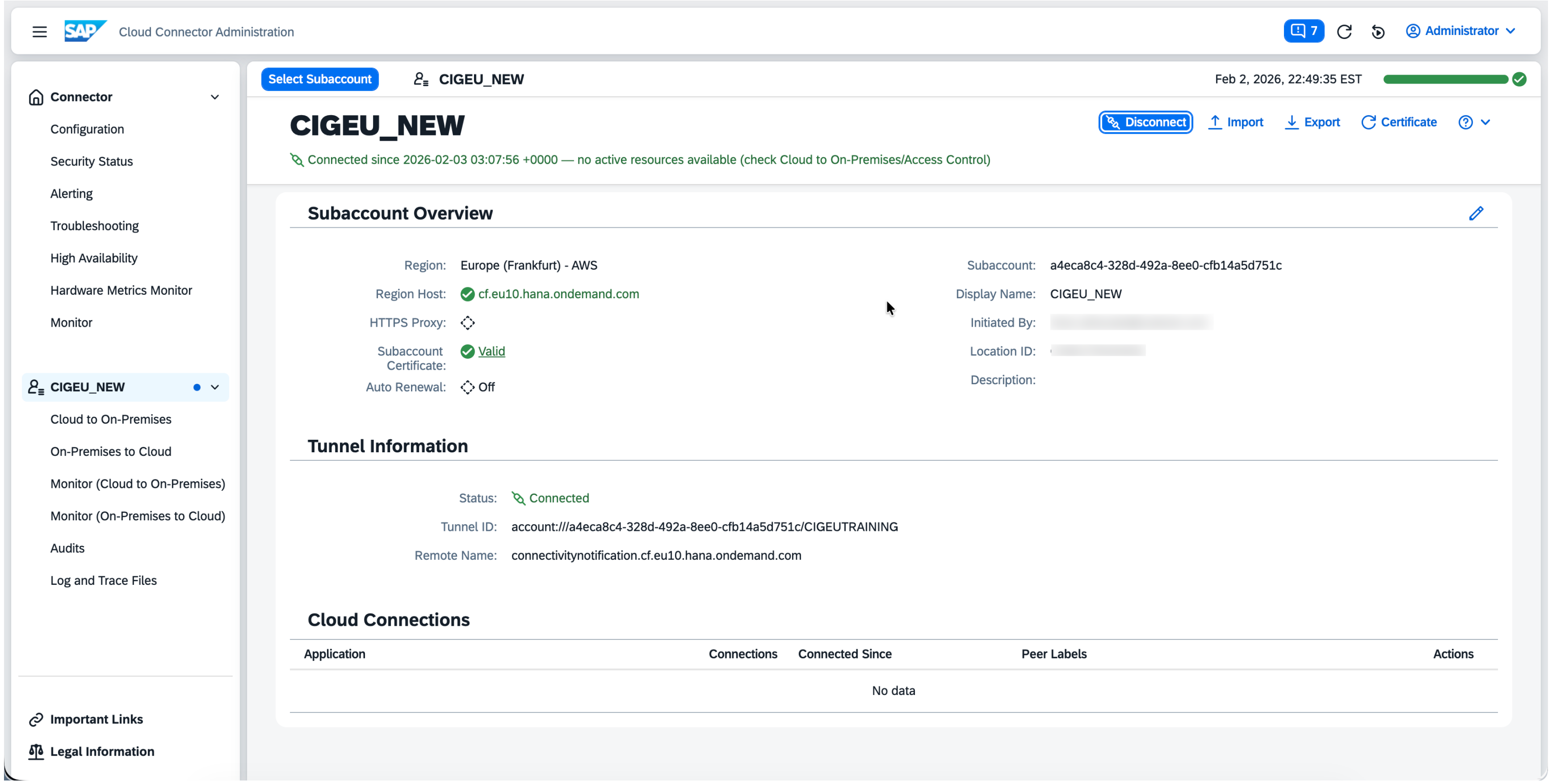
Status	Subaccount	Display Name	Location ID	Region	Actions
◇	a4eca8c4-328d-492a-8ee0-cfb14a5d751c	CIGEU_NEW	[redacted]	Europe (Frankfurt) - AWS	
◇	c2cd9a88-7143-472a-a358-ac050eacdc39	CIGEU1	[redacted]	Europe (Frankfurt) - AWS	
◇	2fdff90d-496d-4c6d-9f21-26d1bb9f37b5	CIGEU2	[redacted]	Europe (Frankfurt)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



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
Region Host: cf.eu10.hana.ondemand.com
HTTPS Proxy:
Subaccount Certificate: Valid
Auto Renewal: Off

Subaccount: a4eca8c4-328d-492a-8ee0-cfb14a5d751c
Display Name: CIGEU_NEW
Initiated By: [redacted]
Location ID: [redacted]
Description:

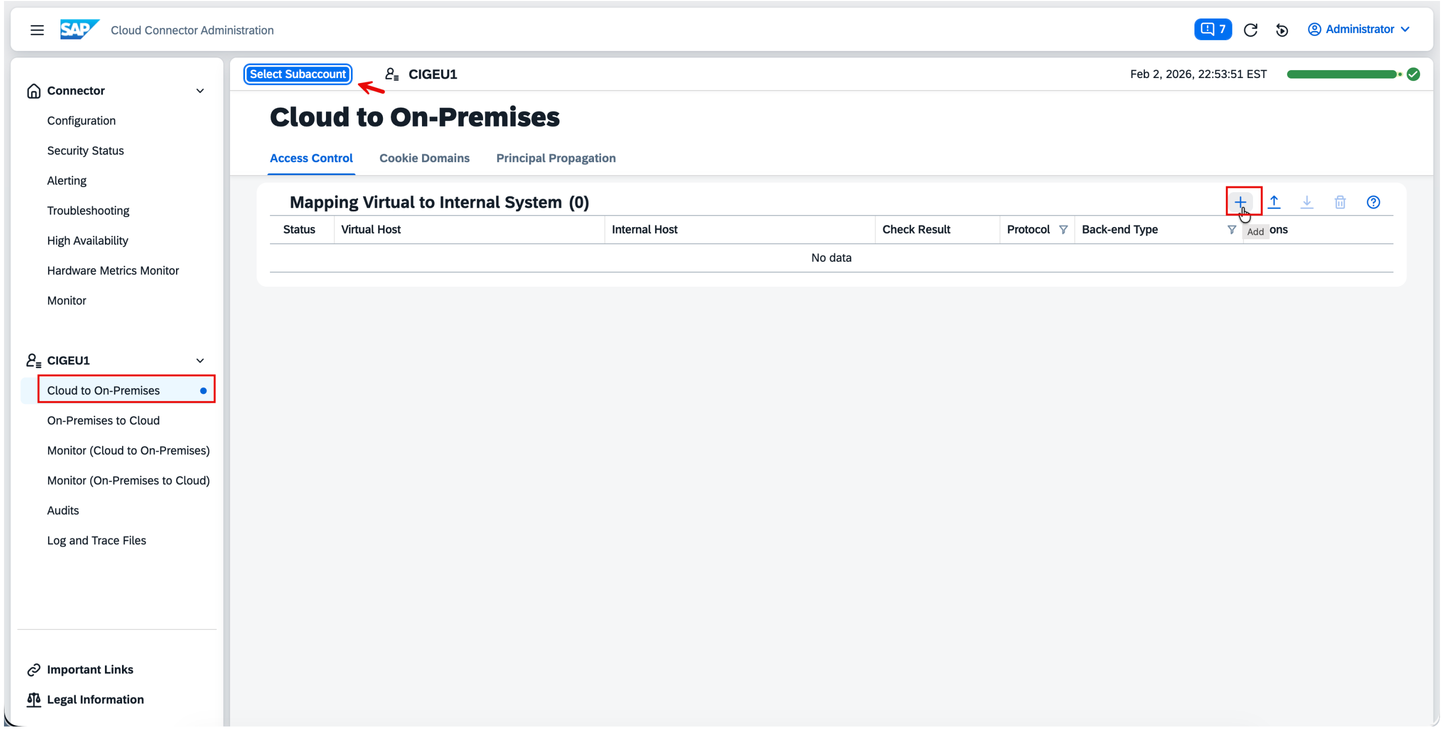
Tunnel Information

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				

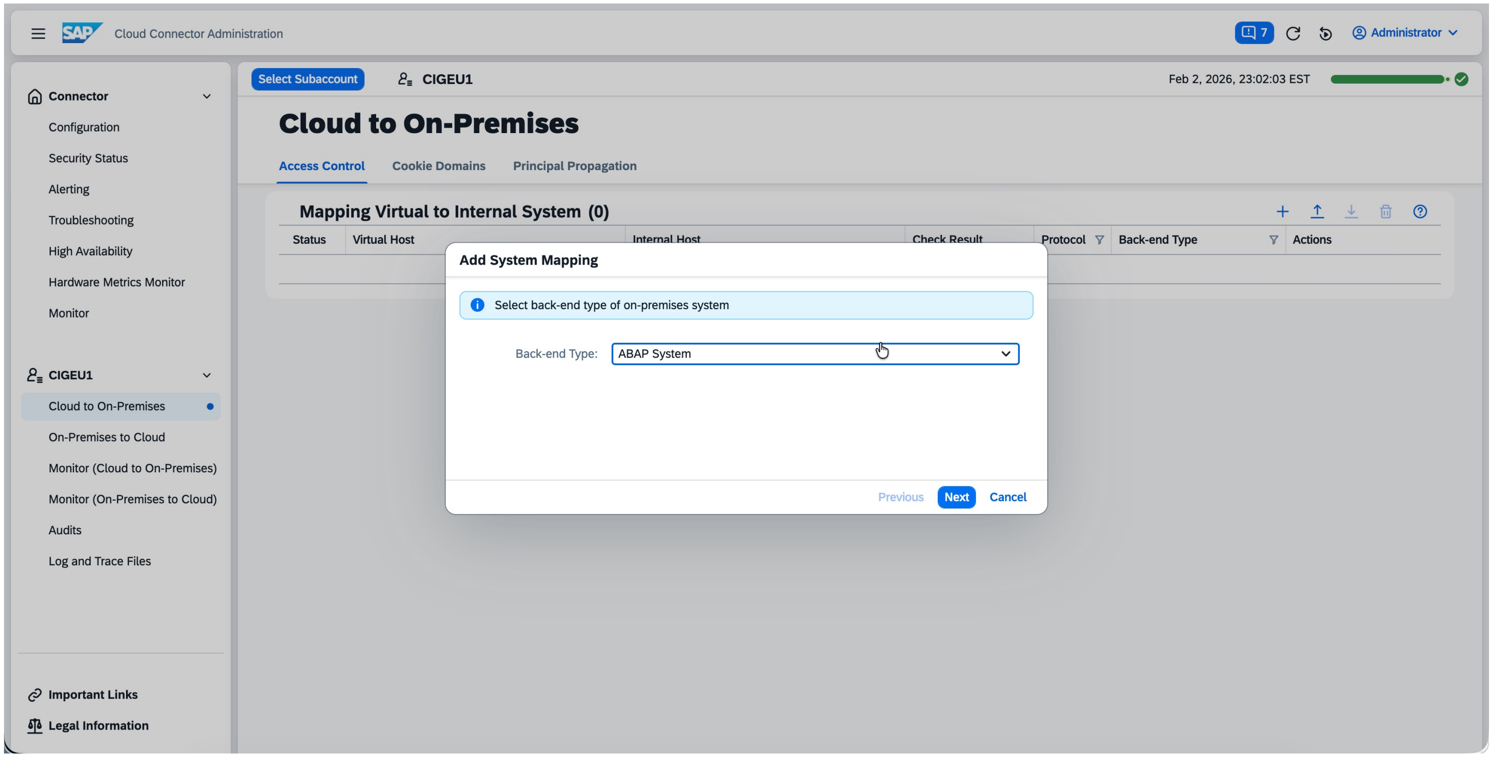
Click Cloud To On-Premise link to provide the virtual mapping to the internal system. When you configure for the first time you will not see any entries here. Click on the ‘+’ sign to add virtual mapping. This needs to be done for each of the managed gateway subaccounts added to your cloud connector.



Mapping Virtual to Internal System (0)

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

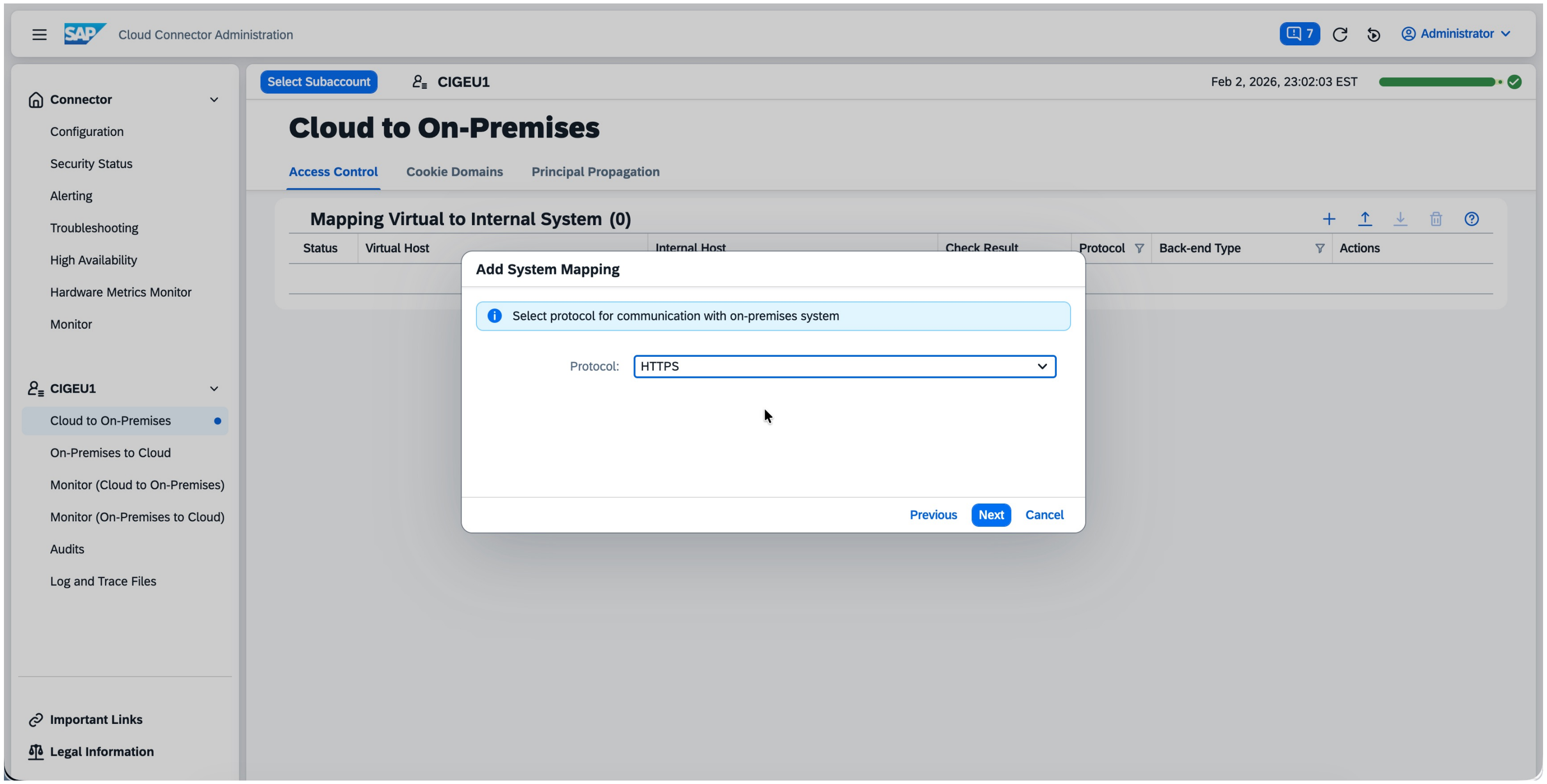
Select the Back-end Type as ABAP System if you are using SAP ECC or S/4 HANA



Select back-end type of on-premises system

Back-end Type: ABAP System

Choose the protocol as HTTPS

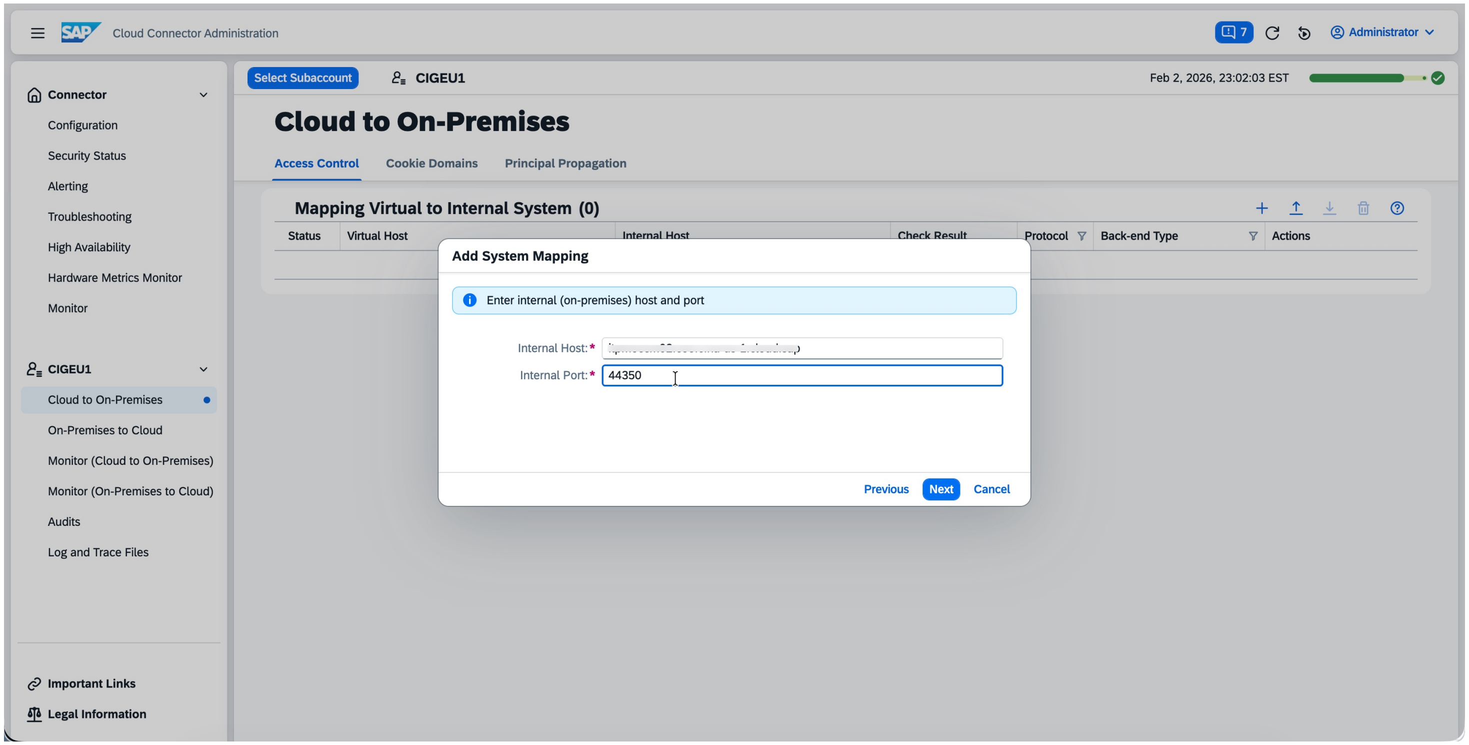


Add System Mapping

Select protocol for communication with on-premises system

Protocol: 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



Feb 2, 2026, 23:02:03 EST

Cloud to On-Premises

Mapping Virtual to Internal System (0)

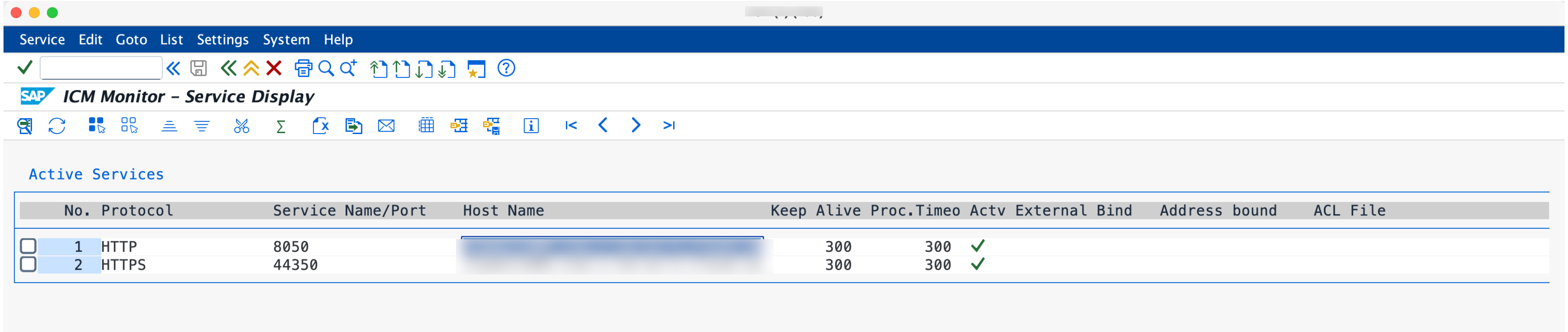
Add System Mapping

Enter internal (on-premises) host and port

Internal Host:* [redacted]

Internal Port:* 44350

SMICM screen shows the hostname of your SAP application server.



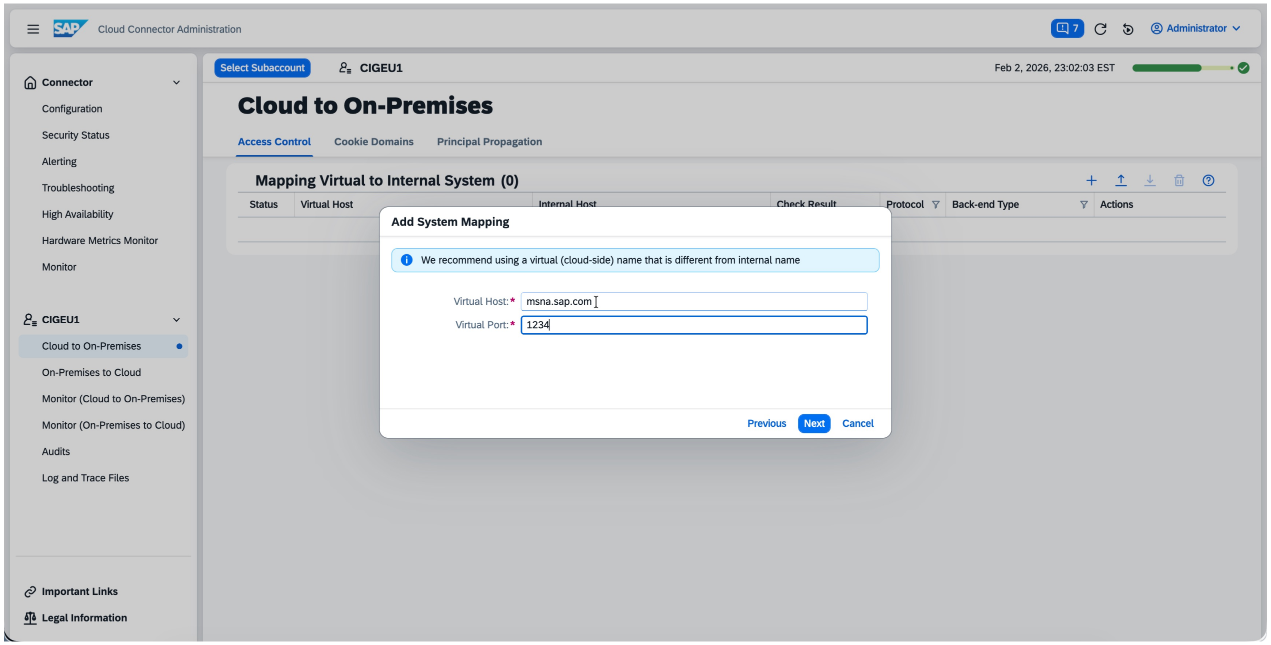
ICM Monitor – Service Display

Active Services

No.	Protocol	Service Name/Port	Host Name	Keep Alive	Proc.Timeo	Actv	External Bind	Address bound	ACL File
□ 1	HTTP	8050	[redacted]	300	300	✓			
□ 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.



Cloud to On-Premises

Mapping Virtual to Internal System (0)

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

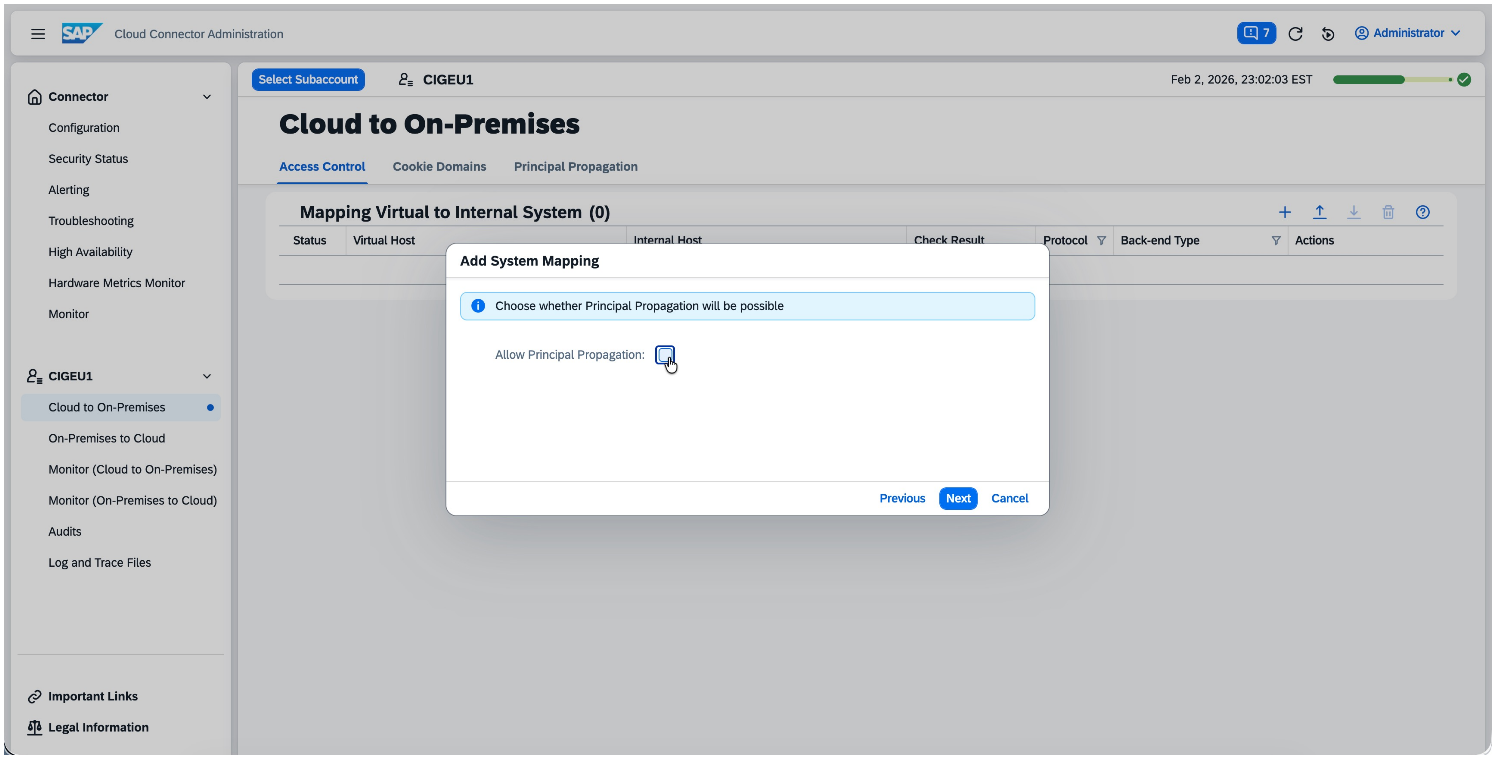
Add System Mapping

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

Virtual Host:* msna.sap.com

Virtual Port:* 1234

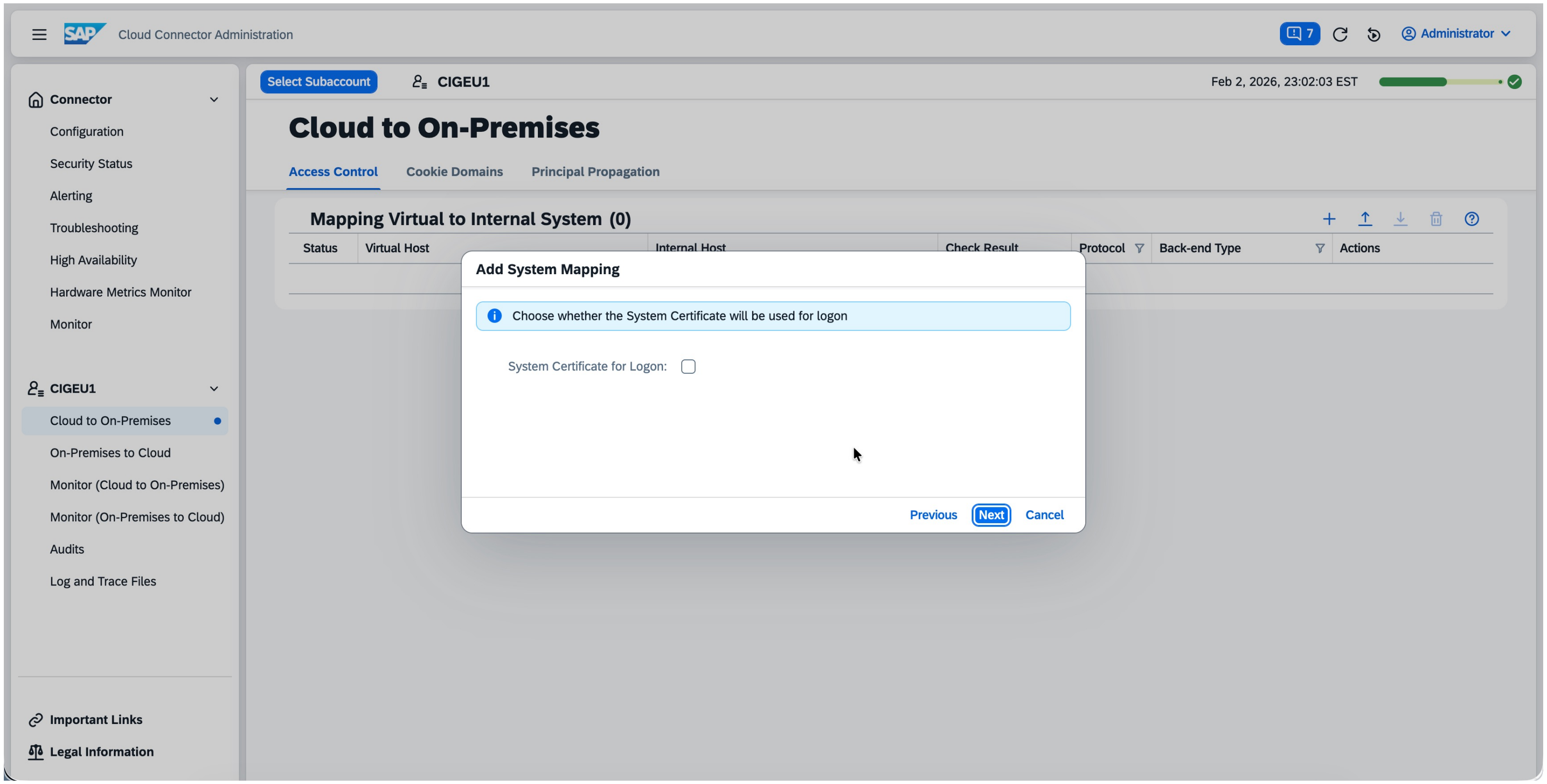
Uncheck the Allow Principal Propagation



Choose whether Principal Propagation will be possible

Allow Principal Propagation: □

Uncheck the System Certificate for Logon



Cloud to On-Premises

Mapping Virtual to Internal System (0)

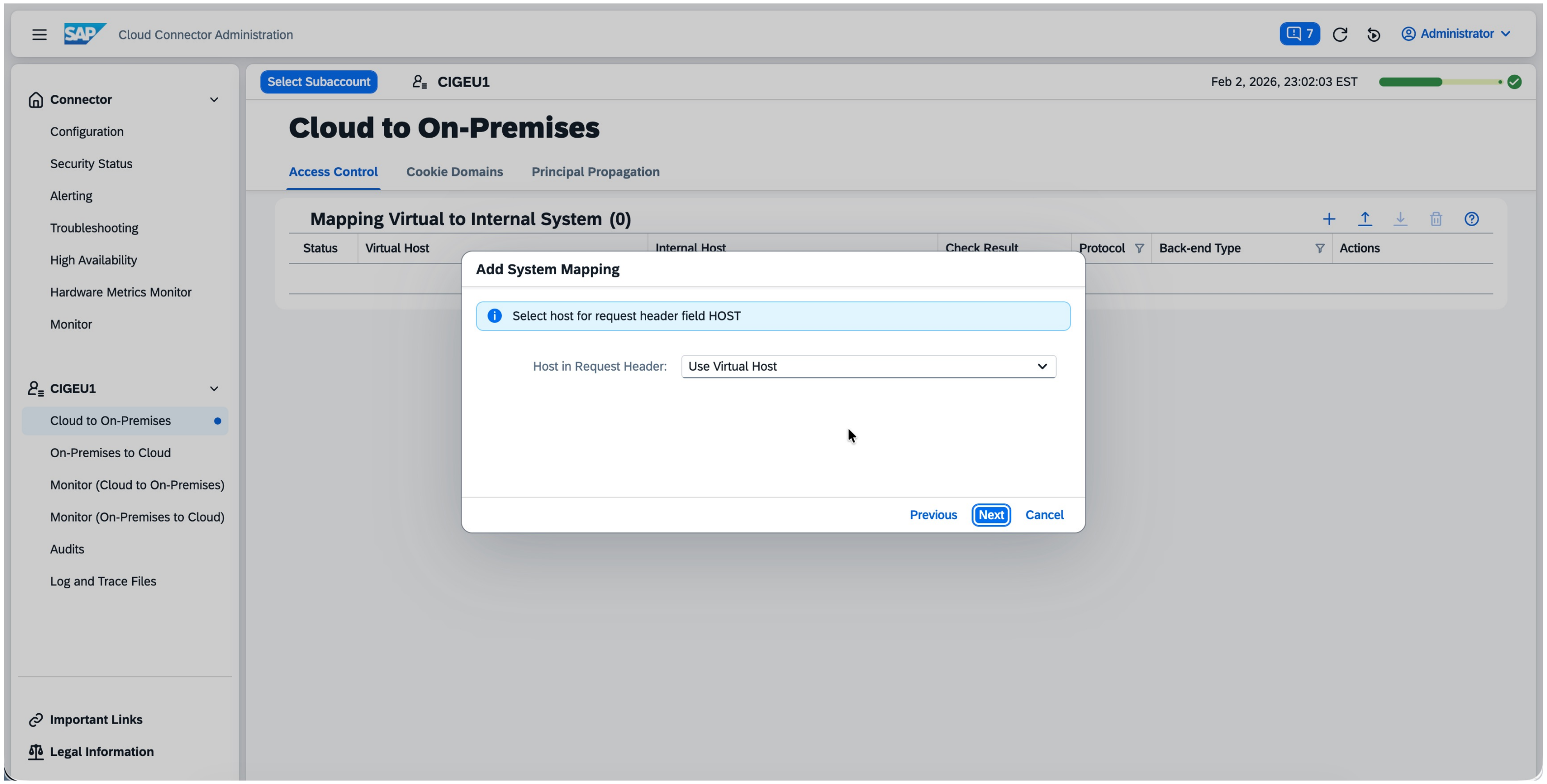
Status	Virtual Host	Internal Host	Check Result	Protocol	Back-end Type	Actions

Add System Mapping

Choose whether the System Certificate will be used for logon

System Certificate for Logon: □

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

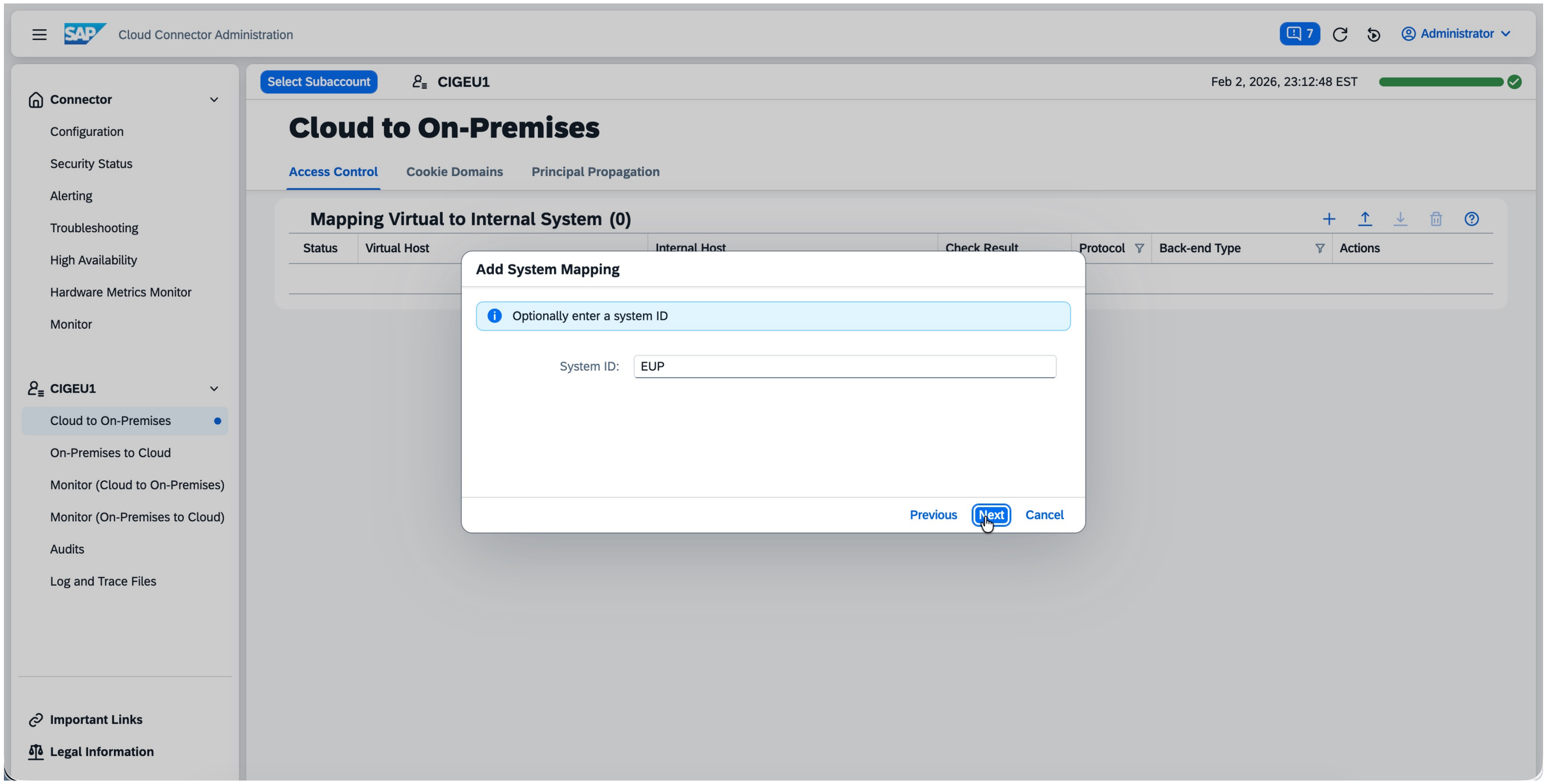


Add System Mapping

Select host for request header field HOST

Host in Request Header: Use Virtual Host

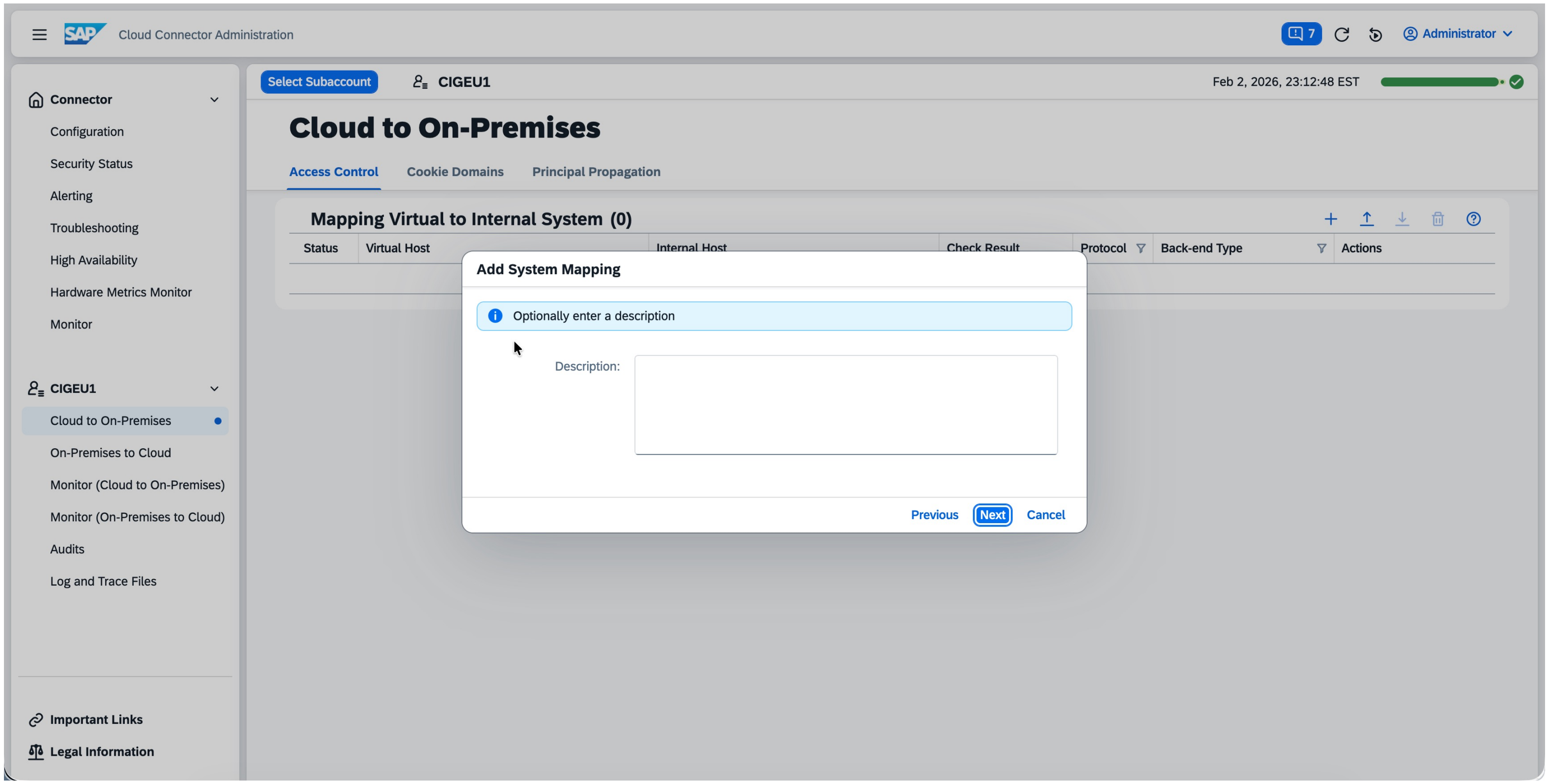
Enter the System ID. This is an optional field



Optionally enter a system ID

System ID: EUP

This is an optional field entered for your reference.

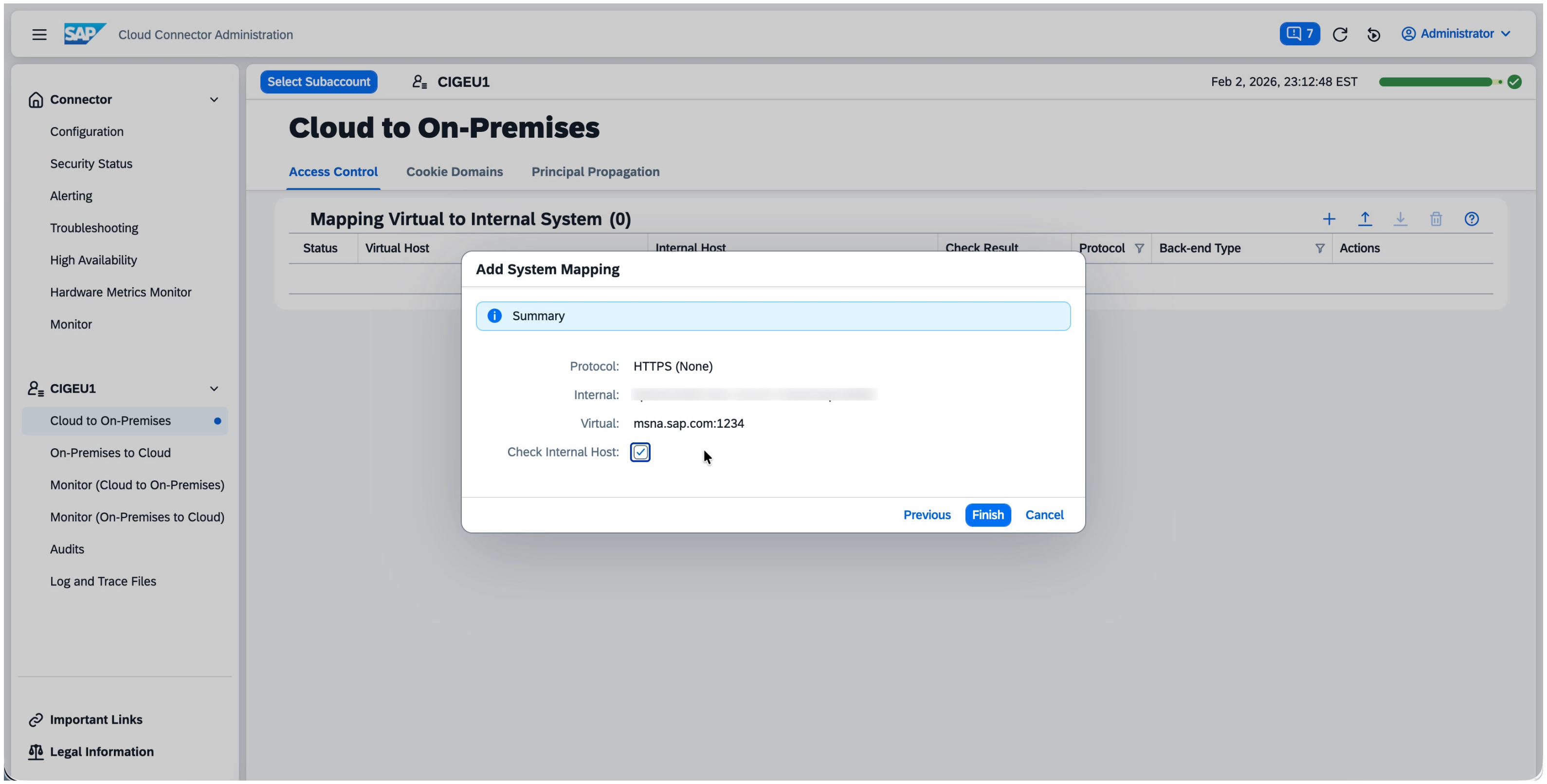


Add System Mapping

Optionally enter a description

Description:

Select the Check Internal Host box and click Finish



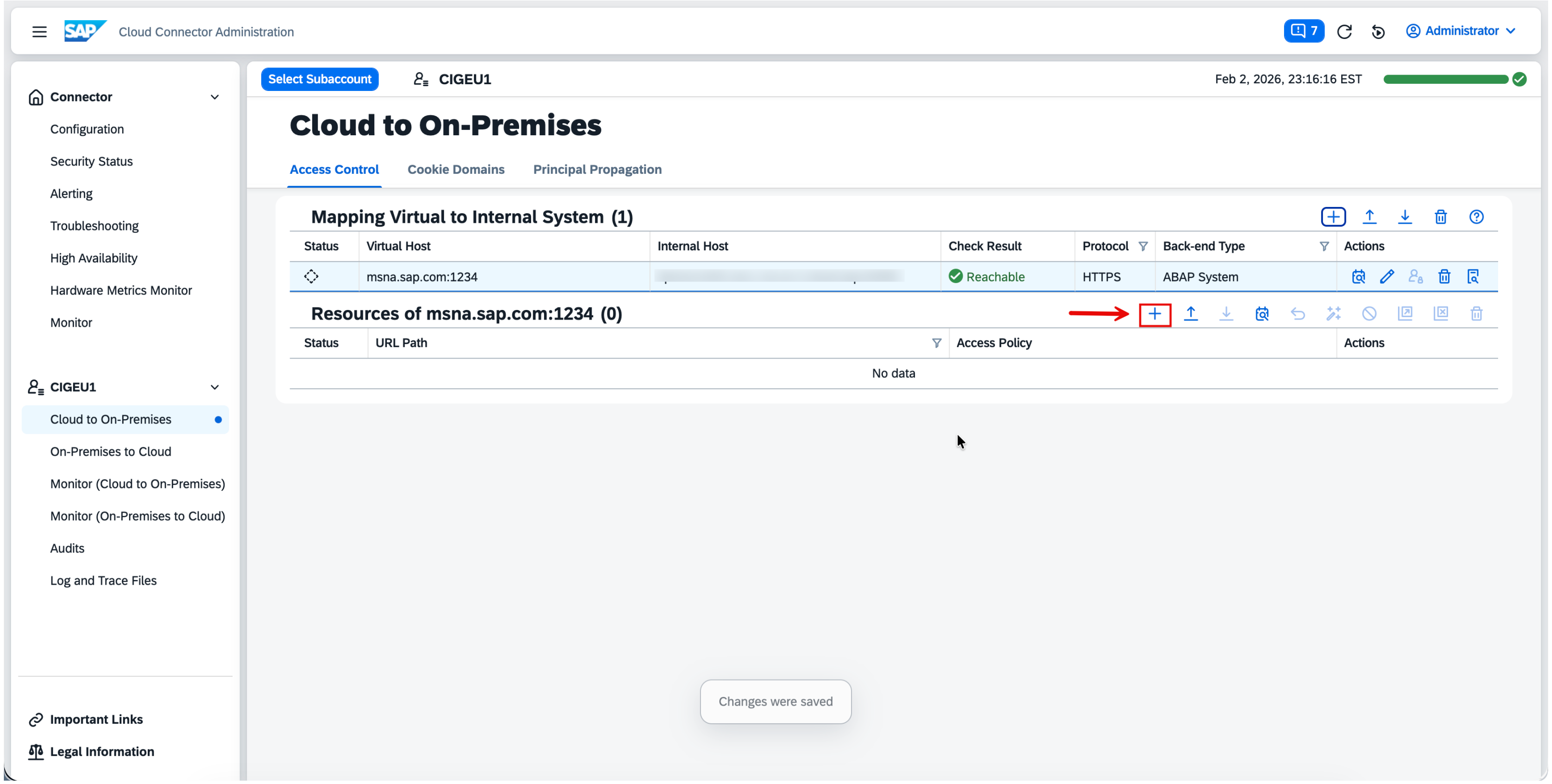
Protocol: HTTPS (None)

Internal: [redacted]

Virtual: msna.sap.com:1234

Check Internal Host: ☑

Click the add resource option option.



Cloud to On-Premises

Mapping Virtual to Internal System (1)

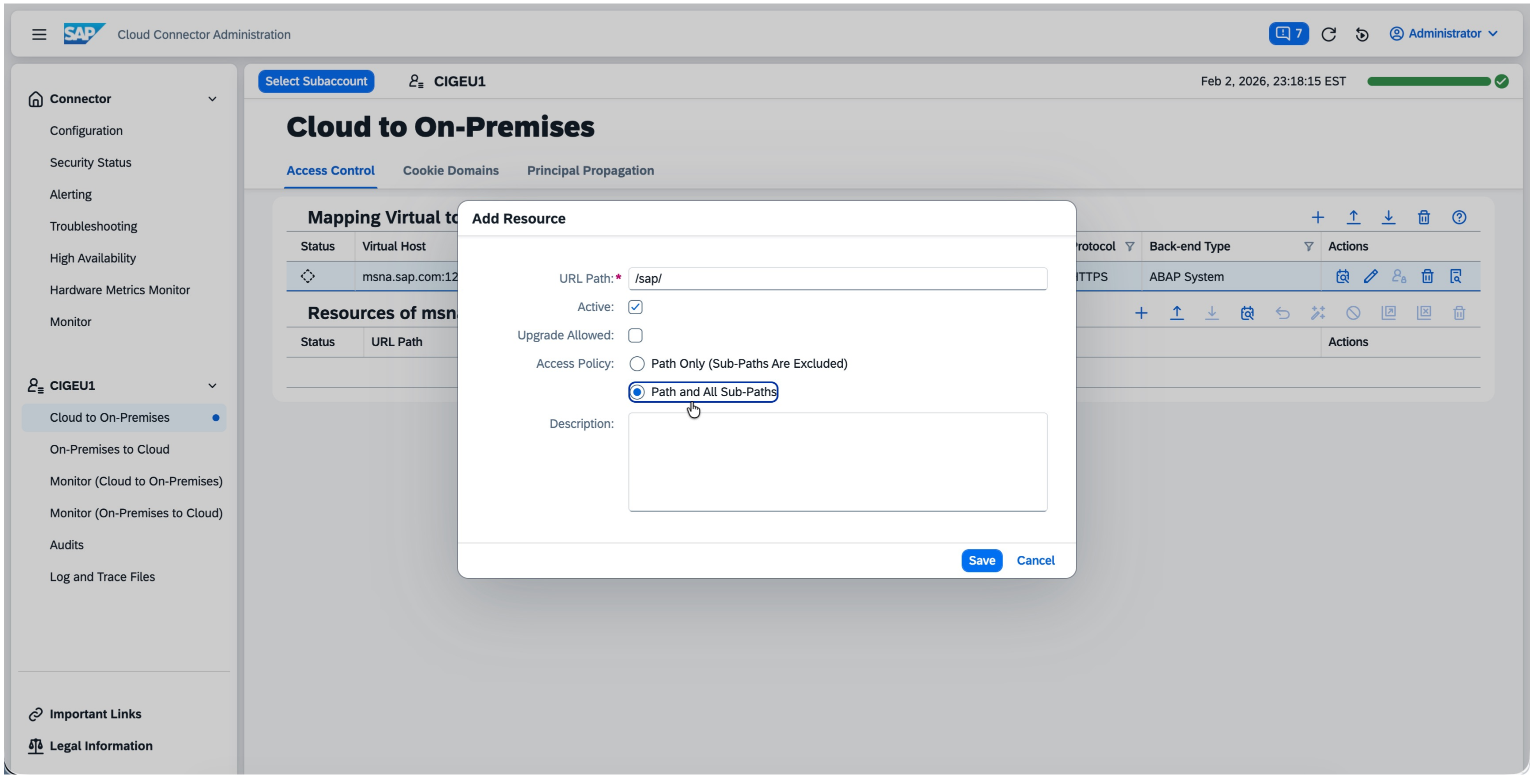
Status	Virtual Host	Internal Host	Check Result	Protocol	Back-end Type	Actions
	msna.sap.com:1234	[redacted]	✓ Reachable	HTTPS	ABAP System	

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



Add Resource

URL Path:* /sap/

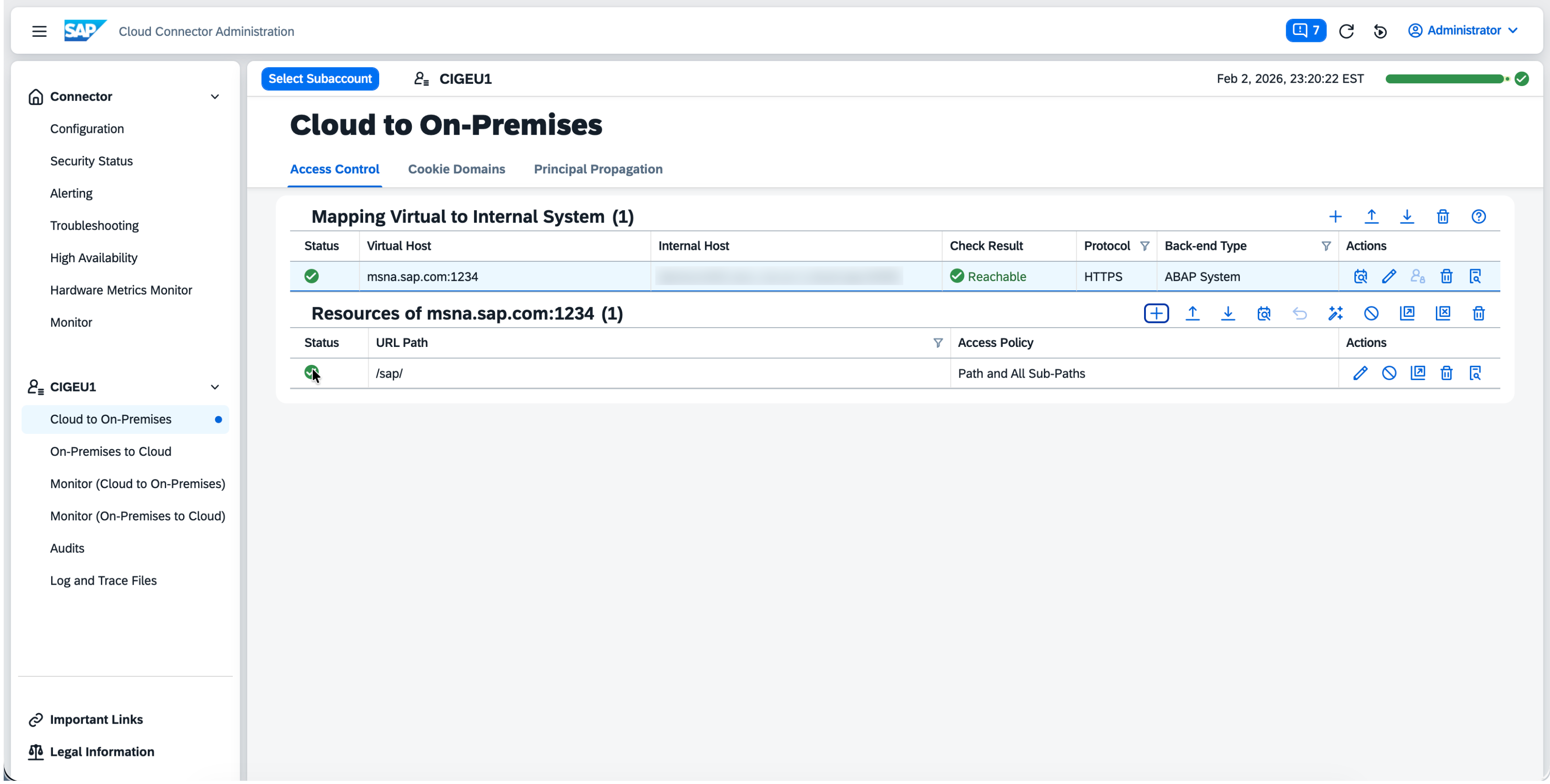
Active: ☑

Upgrade Allowed: □

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

● Path and All Sub-Paths

Description:



Cloud to On-Premises

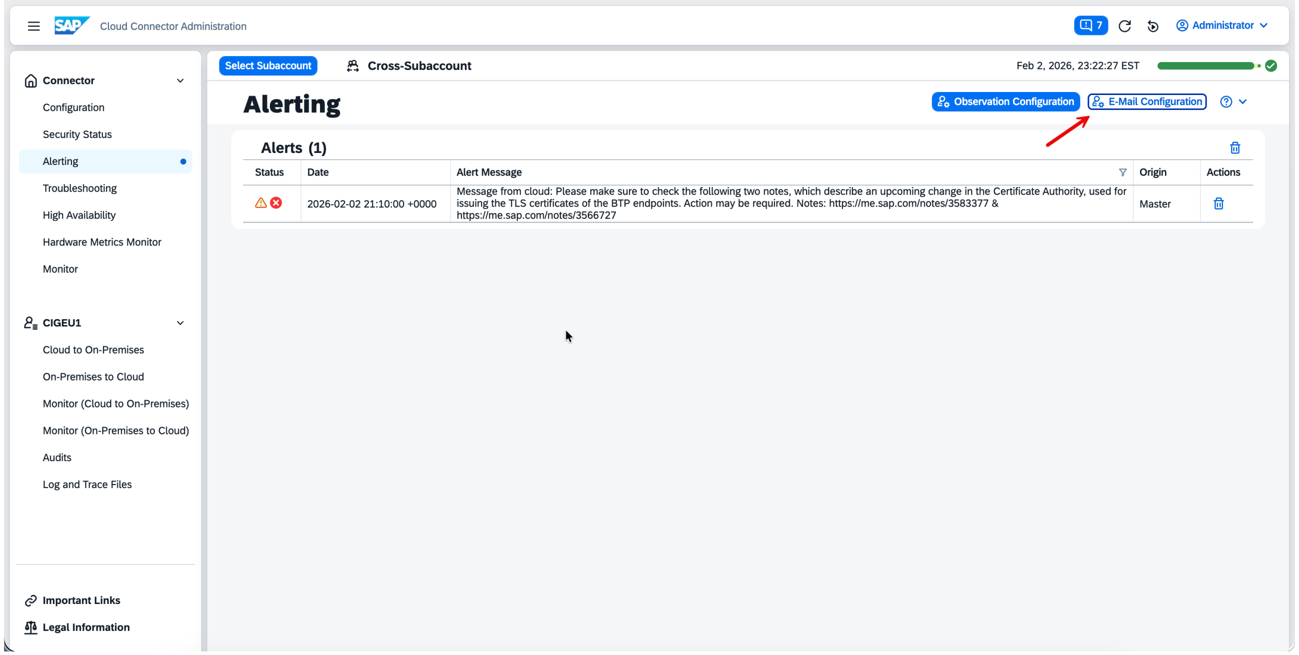
Mapping Virtual to Internal System (1)

Status	Virtual Host	Internal Host	Check Result	Protocol	Back-end Type	Actions
✓	msna.sap.com:1234	[redacted]	✓ 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.



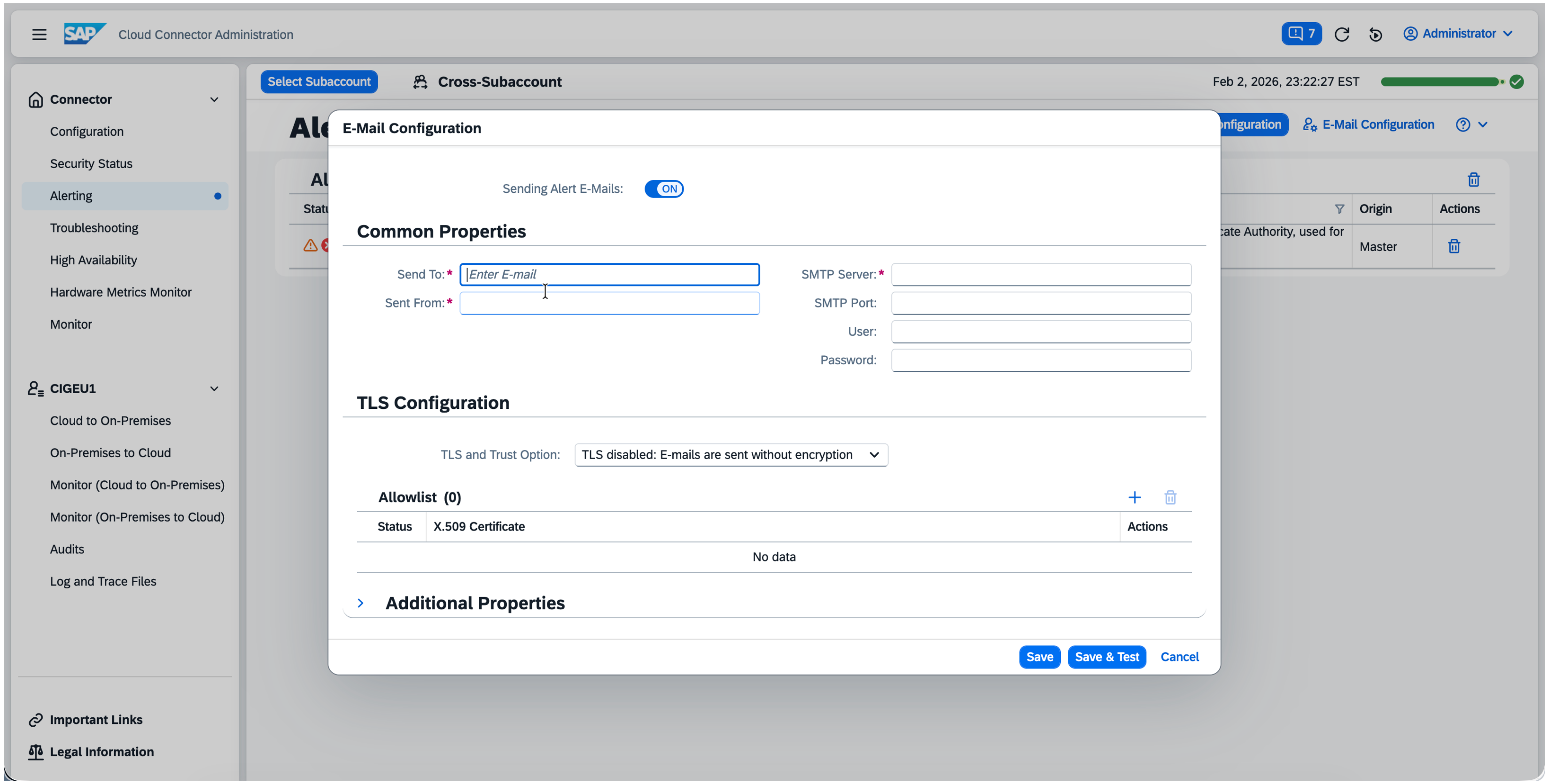
Feb 2, 2026, 23:22:27 EST

Alerting

Alerts (1)

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	🗑

Please update the details and click Save.



E-Mail Configuration

Sending Alert E-Mails: ON

Common Properties

Send To:*	Enter E-mail	SMTP Server:*	
Sent From:*		SMTP Port:	
		User:	
		Password:	

TLS Configuration

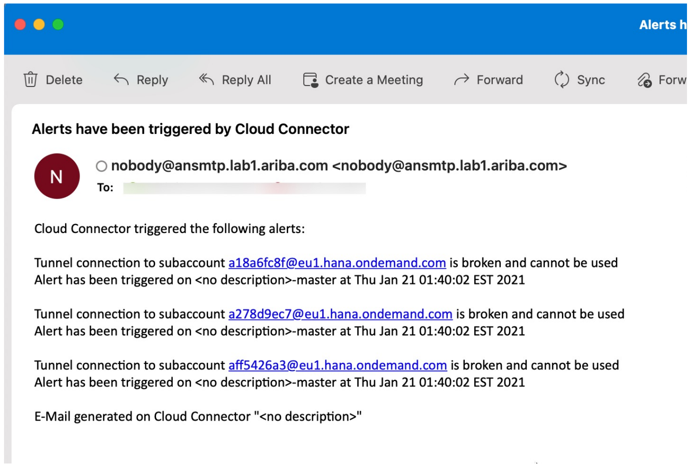
TLS and Trust Option: TLS disabled: E-mails are sent without encryption

Allowlist (0)

Status	X.509 Certificate	Actions
	No data	

› **Additional Properties**

Sample emails



Alerts have been triggered by Cloud Connector

N ○ nobody@ansmtp.lab1.ariba.com <nobody@ansmtp.lab1.ariba.com>

To: [redacted]

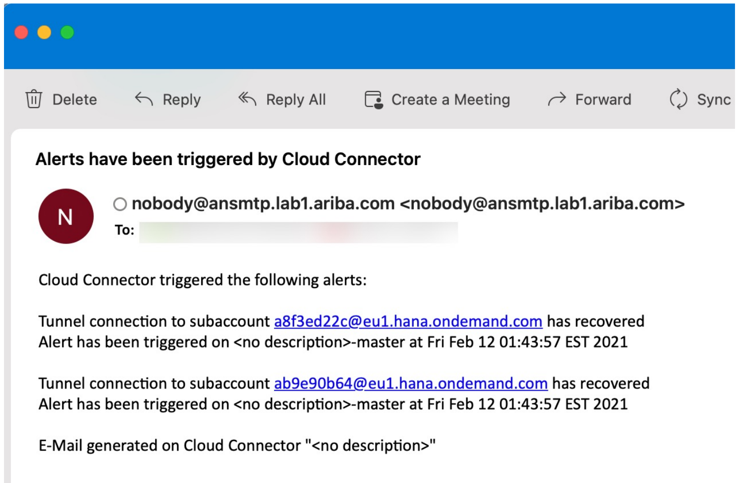
Cloud Connector triggered the following alerts:

Tunnel connection to subaccount a18a6fc8f@eu1.hana.ondemand.com is broken and cannot be used
Alert has been triggered on <no description>-master at Thu Jan 21 01:40:02 EST 2021

Tunnel connection to subaccount a278d9ec7@eu1.hana.ondemand.com is broken and cannot be used
Alert has been triggered on <no description>-master at Thu Jan 21 01:40:02 EST 2021

Tunnel connection to subaccount aff5426a3@eu1.hana.ondemand.com is broken and cannot be used
Alert has been triggered on <no description>-master at Thu Jan 21 01:40:02 EST 2021

E-Mail generated on Cloud Connector "<no description>"



Alerts have been triggered by Cloud Connector

N ○ nobody@ansmtp.lab1.ariba.com <nobody@ansmtp.lab1.ariba.com>

To: [redacted]

Cloud Connector triggered the following alerts:

Tunnel connection to subaccount a8f3ed22c@eu1.hana.ondemand.com has recovered
Alert has been triggered on <no description>-master at Fri Feb 12 01:43:57 EST 2021

Tunnel connection to subaccount ab9e90b64@eu1.hana.ondemand.com has recovered
Alert has been triggered on <no description>-master at Fri Feb 12 01:43:57 EST 2021

E-Mail generated on Cloud Connector "<no description>"

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 (Shangai) **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 &apos;503: Service Unavailable. There is no SAP Cloud Connector (SCC) connected to your subaccount. Requested opening of a tunnel for subaccount &amp;quot;aff5426a3&amp;quot; and SCC location ID &amp;quot;XXXXXX &amp;quot;. Check the configuration on SCC and cloud side.&apos; 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.

SAP Ariba

Thank you.

THE BEST RUN SAP