



PUBLIC

Document Version: 1.0 – 2026-03-17

SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Onboarding Guide

Content

1	Onboarding Guide for SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud.	3
2	Overview.	4
2.1	Unsupported Features.	5
3	Provisioning.	7
4	Join the SAP ASE Service Account in IBM Cloud.	8
5	Authorize Additional Users to Access the SAP ASE Instances.	13
6	Setting Up a Connection to IBM Cloud.	16
7	Connecting to the SAP ASE Cloud Portal.	18
8	Connecting to Administration and Management Console (AMC).	19
9	SSH Into the Management VSI (Optional).	21
10	Connect to SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud.	23
11	Managing SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Instances.	25
11.1	Monitoring SAP ASE Instances.	25
11.2	Transferring a DEK.	26
11.3	Uploading a Backup to IBM Cloud.	27
11.4	Backup and Restore.	28
12	Glossary of Terms.	29

1 Onboarding Guide for SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud

This guide introduces the concepts of SAP Adaptive Server Enterprise, cloud edition by IBM Cloud, describes how you access it and use it on IBM Cloud.

2 Overview

SAP Adaptive Server Enterprise, cloud edition by IBM Cloud is a cloud managed service for SAP ASE hosted on IBM Cloud.

SAP ASE cloud edition by IBM Cloud runs the same code line as on-premises SAP ASE. You can quickly move your application to run on IBM Cloud without any code changes. SAP ASE cloud edition offers lower cost of ownership, enterprise-level services, and faster deployment time. The start-up costs of running on IBM Cloud are also much lower than purchasing and maintaining your own hardware.

SAP ASE on IBM Cloud provides nearly the same functionality as the on-premises version and offers enhanced security and administration features. You retain most administrative access.

SAP ASE clients connect to SAP ASE running on IBM Cloud the same way they do with an on-premises SAP ASE.

Network Architecture

The SAP ASE service utilizes a multi-tiered network architecture.

- **Edge Virtual Private Cloud (VPC)** – All inbound and outbound traffic to and from IBM Cloud passes through this VPC. This environment groups IBM Cloud resources needed for on-premises integration, including bastion hosts (jump servers), VPN servers, gateways, and public gateways.
- **Management VPC (Optional)** – This is an optional environment where you can use SAP ASE client tools and run customer-specific scripts for managing your SAP ASE locally within the IBM Cloud.
- **Workload VPC** – This environment hosts your databases and contains the IBM Cloud resources for SAP ASE instances.

Security

All access to SAP ASE cloud edition instances is through secure SSL connections on SQL ports. Your data is always stored encrypted using SAP ASE's full database encryption. In addition, all network communication and all storage in IBM Cloud is also encrypted.

To ensure a clear separation of duties, the SAP ASE security model is updated. This change allows IBM Cloud to operate the SAP ASE server and perform regular activities like backups and patching while still protecting your data. The IBM Cloud team cannot access your schemas or data. As a customer, your "sa" account has slightly reduced capabilities. IBM Cloud now handles certain administrative tasks that the "sa" account previously performed.

For more information, see [SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Security Guide](#).

Backup and Restore

SAP ASE cloud edition provides automatic backups to help protect your databases. In the high availability (HA) service, these backups are provided by default. Full database backups run daily and are retained for seven days, five weeks, and three months. If you need longer backup retention, you can request it. Transaction log backups run every hour. If you use the non-HA service, backups are not provided by default, but you can request them. You can also request ad-hoc backups and ad-hoc restores through the self-service.

2.1 Unsupported Features

This topic lists features that you can use in the on-premises version of SAP ASE but are not available in SAP Adaptive Server Enterprise, cloud edition by IBM Cloud. These features are in addition to those already documented as unavailable in SAP Note [2922454 - SAP Adaptive Server Enterprise \(SAP ASE\) on Cloud Platforms](#).

Feature	Unsupported Components/Functions/Utilities
SAP ASE High Availability (HA) – External Vendor	- installhasvss - sybha
Process mode kernel	sp_configure "kernel mode", process
XP Server	- XP Server utility - Extended stored procedures - Start XP Server - xp_cmdshell - xp_logevent - xp_enumgroups - create procedure with the as external name parameter - create xpserver - drop xpserver - set xpserver port - show xpserver
Disk Mirroring	Disk mirror commands: - disk mirror - disk unmirror - disk remirror - waitfor mirrorexit
Simplified Native Access Plan (SNAP)	sp_configure 'simplified native access plan'

Feature	Unsupported Components/Functions/Utilities
Audit Records	Sending audit records to syslog using <code>sp_configure 'audit trail type'</code> .

3 Provisioning

SAP Adaptive Server Enterprise, cloud edition by IBM Cloud instances are provisioned on IBM Cloud based on the scope and timing agreed during the pre-sale and sizing process. Instances can also be provisioned on request by raising a support ticket.

HA-enabled SAP ASE instances are created as an always-on pair. The primary SAP ASE runs in data center 1, and the standby SAP ASE runs in data center 2 to provide high availability and disaster recovery (HADR). In addition, the Fault Manager component is located in data center 3.

Non-HA SAP ASE instances are created as single instances in a single data center.

4 Join the SAP ASE Service Account in IBM Cloud

After your SAP ASE service account is set up, the primary customer contact receives an email invitation to join the account in IBM Cloud.

Context

The SAP ASE service account is a dedicated IBM Cloud account that your enterprise uses only for SAP ASE. You can create your own IBM Cloud account and connect it to the SAP ASE service account.

Procedure

1. Click the Join now link in the email.
2. If you are new to IBM Cloud, you are prompted to set up two-factor authentication. Click [Start](#) to begin.

Two Factor Authentication - Setup

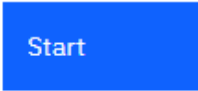
Setup Multi-Factor Authentication

At least one of your IBM Cloud accounts requires an additional authentication factor:

- Account name: **SAP-TEST-ACCOUNT**
Account owner: 

First you have to verify your identity or setup a verification method. After that, you have to setup one of the following authentication factors:

- TOTP MFA
- Security Key MFA



Start

3. In the Two Factor Authentication - Setup window, select your first verification method from the following:
 - SMS
 - E-mail
 - Voice call

Two Factor Authentication - Setup

☒ Create Veri... ☐ Create Verif... ☐ Setup Auth...

Create Verification Method (1/2)

Before you can enroll for an authentication factor, you must provide two verification methods to identify yourself.

Please select your first verification method:

☒ SMS ☐ E-Mail ☐ Voice Call

Full qualified number (e.g. +123456789) or valid mail address (e.g. name@domain.com)

Name for this verification method

Send SMS to *****

Send

One-Time Password

2822 - Enter the one-time password

Complete

4. Enter the one-time password you receive from the selected method and click Complete to finish the authentication for the first method.
5. Repeat step three and step four to complete the authentication for the second verification method.
6. Once you have completed two separate verification methods, proceed to set up a time-based one-time password (TOTP).

Two Factor Authentication - Setup

☒ Validate yo... ☒ Validate yo... ☒ Setup Auth...

Setup Authentication

After successfully validating your identity, you can now enroll one authentication factor.

Please select one authentication factor:

☒ TOTP ☐ Security Key

Please scan this QR code with your authenticator app or enter the shared secret under the code into your application:



UOIWFPJL35XR74C26RBLFZHADGFQXKGC

Name for this authentication factor

TOTP Verification Code

6 Digit Verification Code

Enter the 6 digit verification code

Complete

7. Scan the QR code to add the TOTP to your preferred authentication app.
8. Use the app to generate a code, enter it in the 6 Digit Verification Code field, and click Complete.
9. Click [Start](#) to authenticate yourself again to log in to IBM Cloud.

Two Factor Authentication - Setup

Success!

You will now be able to authenticate using the factor that you just created.

Start

10. Review your account details and join the account.

Results

You are now logged in to the IBM Cloud Management Console.

5 Authorize Additional Users to Access the SAP ASE Instances

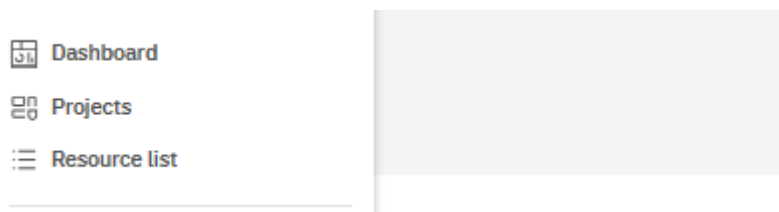
Use the App ID dashboard to authorize access to the SAP ASE Cloud Portal, such as database administrators and application developers.

Context

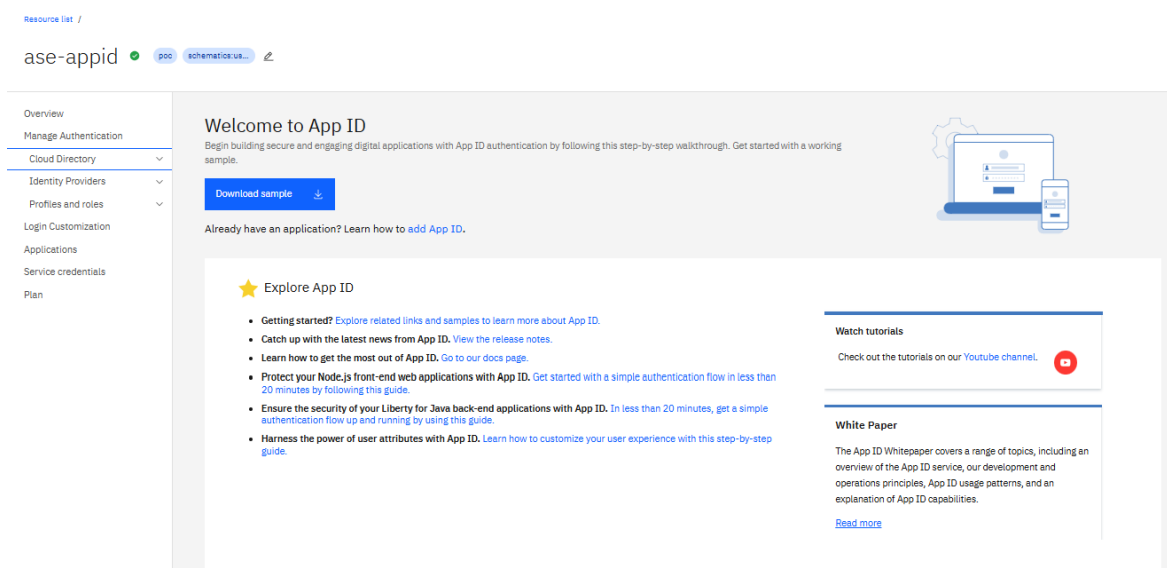
Only the primary customer contact has access to the App ID dashboard.

Procedure

1. Log in to IBM Cloud.
2. Click the *Navigation Menu* in the upper left corner and select *Resource List*.



3. In the *Resource List*, double-click *ase-appid* under the Security category to open the App ID dashboard.



4. Go to the **Cloud Directory** > **Users** tab, click *Create User*.

Resource list / ase-appid pool schematic.us...

Overview
Manage Authentication
Cloud Directory ^
Settings
Password Policies
Email Templates
Multi-factor authentication
Single Sign-on
Users
Identity Providers ^
Profiles and roles ^
Login Customization
Applications
Service credentials
Plan

Cloud Directory users

With Cloud Directory, you can manage your users in a scalable registry by using pre-built functionality that enhances security and self-service. For more information, see the [docs](#).

Total numbers of Cloud Directory users: 10

Last refreshed: 13 April 2026 11:04
Create User

☐	Email	First Name	Last Name	Last Login	Status	
☐				10 April 2026 19:07	Verified	
☐					Verified	
☐				7 April 2026 21:17	Verified	
☐					Verified	
☐				16 March 2026 17:11	Verified	
☐				10 April 2026 15:53	Verified	
☐					Verified	
☐				7 April 2026 15:35	Verified	
☐				9 April 2026 17:58	Verified	
☐				26 March 2026 15:54	Verified	

Items per page | 10 | 1-10 of 10 items
1 1 of 1 page

- In the Add User window, enter Username, Email, and Password and click [Save](#) to create the user.

Add a user to test your application

First Name:
Demo

Last Name:
User

Username:*

demouser@sap.com

Email:*

demouser@sap.com

Password:*

Re-enter Password:*

Note: Users created in the dashboard are signed up and validated when they are added. They do not receive an email verification.

Show password

Cancel

Save

- In the users table, click on the newly created user and scroll down to Custom Attributes and click [Edit](#).

Edit custom attributes

Custom attributes are additional pieces of information about your users that you can associate with their profile.

1 { "access_to_cloud_services": "allow" }

Cancel Save

7. Paste the following into the custom attributes and click [Save](#).

```
{
  "access_to_cloud_services": "allow"
}
```

Results

You can now securely communicate the username and password to the DBA or application developers and they will be able to register for IBM Cloud access and set up their own 2FA. They will now be able to access Secret Manager (as per next steps in the documentation) and follow the instructions to access the service using this guide.

6 Setting Up a Connection to IBM Cloud

IBM Cloud provides three options for connecting from your workstation to the SAP ASE cloud edition.

Context

Client-to-Site VPN

This is the default option and enables quick onboarding. Install a VPN client on your computer to connect to the SAP ASE service. You also need to send a signed (by your security authority) individual client certificate to the service owner for authentication.

Site-to-Site VPN

This option requires your team to set up a generic VPN server. After configuration, users connect to the SAP ASE service through this server. You need to send a signed server certificate to the service owner. All users needing access to the service require the service passphrase.

Direct Connection

This option requires a dedicated connection to be installed and configured within your network, which allows you to connect to the SAP ASE Service.

This topic shows you how to set up a client-to-site VPN. Before you begin, install OpenVPN. See [Supported VPN client software](#)  for VPN client software versions that work with your platform.

Procedure

1. Log in to IBM Cloud.
2. Click the [Navigation Menu](#) in the upper left corner and select [Resource List](#).
3. In the [Resource List](#), double-click to open the `<base_environment_prefix>-secrets-manager` instance under the Security category.
4. Click `<base_environment_prefix>-vpn-server-config` to open the secret.
5. Click the Overflow menu button (three vertical dots) next to the secret and select [View Secret](#).
6. Confirm that you are in a safe environment, then copy the secret value.
7. Create an OpenVPN (.ovpn) file on your computer (for example, `vpn.ovpn`) and paste the contents of the secret into the new file.
8. Open the OpenVPN client.
Make sure you close other VPNs running on your machine before you open the OpenVPN client. Use a 5G wireless connection or better if you connect to OVPN wirelessly.
9. In the OpenVPN window, click the button in the upper left corner and select [Import Profile](#).

10. On the UPLOAD FILE tab, browse for and select the ovpn file you created previously.
11. For *Username*, enter your IBM Cloud username and click *Connect*.
12. When prompted for a password, retrieve a temporary one-time password from [this link](#) . If prompted to log in, enter your IBM Cloud email and password. If necessary, complete multi-factor authentication (MFA) requirements when prompted.
13. Click *OK* to connect. When the connection is successful, the toggle is enabled next to the configured profile.

→ Tip

For future connections, click the toggle next to the desired profile to connect.

7 Connecting to the SAP ASE Cloud Portal

Once connected to IBM Cloud, you can access the SAP ASE Cloud Portal to manage your SAP ASE instances.

Context

After your SAP ASE instance is provisioned, you receive an email notification that includes the link to your SAP ASE Cloud Portal. In the portal, you can:

- Upload and install database encryption keys
- Run ad-hoc backups and restores
- View important SAP ASE configuration files
- Access SAP ASE log files
- Access and download SAP ASE backup files

Procedure

1. Log in to IBM Cloud.
2. Go to the [Resource List](#) and launch the Secrets Manager instance as described earlier.
3. Select [View Secret](#) for the `<base_environment_prefix>-dba-initial-login` secret.
4. Confirm you are in a safe environment and copy the secret value.
5. Open the SAP ASE Cloud Portal link from the confirmation email in your internet browser.
6. Log in using your IBM Cloud email and the initial password from Secrets Manager.

Results

You have logged in to the SAP ASE Cloud Portal and can view your SAP ASE instances.

8 Connecting to Administration and Management Console (AMC)

The AMC for SAP ASE is a web-based tool that helps you manage and administer your SAP ASE servers.

Procedure

Retrieve Credentials and the Public Certificate from Secrets Manager

1. Log in to IBM Cloud.
2. Go to the [Resource List](#) and open the `<base_environment_prefix>-secrets-manager` instance.
3. Find the SAP ASE user login credentials (`<base_environment_prefix>-<ase_instance_prefix>-user-login`). Select **View secret**. Confirm you are in a safe environment, and copy the username and password to a secure location.
4. Find and download the AMC public certificate (`<ase_instance_prefix>-amc-public-cert`).

Import the AMC Public Certificate

5. Unzip the AMC public certificate you downloaded from Secrets Manager.
6. Open the Settings page of your web browser.
7. Under the Security options, select **Manage certificates** **>** **Local certificates** **>** **Manage imported certificates from Windows**.
8. In the Certificates window, click **Import...**
9. In the Certificate Import Wizard, browse to and import the `<ase_instance_prefix>-amc-public-cert.pem` certificate.

You will receive the message `The import was successful` when the import is complete.

Connect to AMC

10. Log in to the IBM Cloud.
11. Click the hamburger icon in the upper left corner and select **Infrastructure** **>** **Network** **>** **Load Balancers**.
12. In the Load Balancers to VPC table, choose the region.
13. Copy the hostname for either the primary or companion load balancer.
 - primary: `<base_environment_prefix>-<primary>-amc-lb-b`
 - companion: `<base_environment_prefix>-<companion>-amc-lb-b`
14. Start the OpenVPN Client and connect to the VPN.
15. When you are prompted to "Enter password," retrieve a temporary one-time passcode from [IBM Cloud](#). If prompted, log in with your IBM Cloud email and password.
16. Open a new browser window or tab.
17. Enter the AMC load balancer hostname in the address bar using the format `https://<amc_load_balancer_hostname>:8443`.

18. On the AMC login page, enter your SAP ASE user login credentials.

9 SSH Into the Management VSI (Optional)

Your organization may have chosen to have root access to a virtual server instance (VSI) hosted in your IBM Cloud account. This setup lets you connect using SSH and run commands such as `isql` from within IBM Cloud instead of on your machine.

Generate Your SSH Keys

You need an SSH key pair to establish an SSH or SFTP connection to IBM Cloud (bastion host and file exchange host). You can use an existing SSH key pair or generate a new one. To generate an SSH key pair:

Open a terminal window and create your key pair. SAP recommends that you use a passphrase when creating your SSH key pair and that you store the password in a password manager.

```
% ssh-keygen -t rsa -b 4096 -C "<your_email_address>"
```

For details about generating SSH keys, see [Getting started with SSH keys](#) .

Validate your SSH key

When you generate an SSH key pair, you create two files: a public key (`~/.ssh/id_rsa.pub`) and a private key (`~/.ssh/id_rsa`). Use the following command to check the password and confirm that your SSH key pair matches. If the passphrase and keys match, the command returns your public key.

```
% ssh-keygen -y
```

SSH into the Management VSI

Before you begin, your public key must be installed on the IBM Cloud server to let you connect with SSH over the VPN. Share your public key (`~/.ssh/id_rsa.pub`) with your cloud operator so that they can install it for you. Do not share or upload your private key. The cloud operator will notify you when your public key is installed.

1. Add your private key to the key chain.

```
ssh-add ~/.ssh/id_rsa
```

On Windows, navigate to the folder where your private key is and run:

```
start-ssh-agent
```

2. Open a case with IBM to add your generated `id_rsa.pub` to the edge node and management VSI. Provide the generated `id_rsa.pub` file with the case.
Do not proceed until you receive confirmation that your key is installed.

3. Connect to the management tools VSI using the bastion server as the jump host. For example:

```
ssh -J root@10.10.0.13 root@10.20.0.9
```

Follow the prompts until you see the success message below:

ATTENTION! Your session is being recorded!

[root@sap-ase-management-tools-vsi ~]#

10 Connect to SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud

This topic shows you how to connect to an SAP ASE cloud edition instance with different client applications.

Before connecting to the SAP ASE instance in IBM Cloud, verify that your connection to IBM Cloud is configured and that you have access to an SAP ASE database with credentials and privileges to connect and run commands.

Open Client Applications

1. Copy or download the SSL `trusted.txt` certificate from Secrets Manager.
2. Append the contents of the `trusted.txt` file to the `$SYBASE/config/trusted.txt` file on your client system.
3. Connect to the SAP ASE cloud edition instance from the command prompt or terminal:

```
isql -U<ase_username> -P<password> -S'<host_domain>:<ase_port>  
ssl="CN=SAPASEService.ibm.cloud"
```

- `<ase_username>` – Your SAP ASE login name
- `<password>` – The password needed to log in to the SAP ASE instance
- `<host_domain>` – The fully qualified domain name of the SAP ASE server in IBM Cloud. You can find the domain name in the ASE Cloud Portal.
- `<ase_port>` – The port number for the SAP ASE Server that accepts requests. The default value is 5000.

Include the single quotes (') and double quotes (") exactly as shown. This is required for the SSL connection to work correctly. Interfaces entries of the form can be made as:

```
<SERVER>  
master tcp ether <host><port> ssl="CN=SAPASEService.ibm.cloud"  
query tcp ether <host><port> ssl="CN=SAPASEService.ibm.cloud"
```

JAVA jConnect Applications

1. Copy or download the SSL `trusted.txt` certificate from Secrets Manager.
2. Append the certificate of the `trusted.txt` file to the Java keystore using the Java keytool:

```
keytool -import -trustcacerts -file trusted.txt -alias <anyalias> -keystore  
<keystore>
```

3. To enable existing applications, set the `ENABLE_SSL=true` connection property when you create a connection and add the following JVM directives when you invoke the application:

```
-Djavax.net.ssl.trustStore="<keystore>"  
-Djavax.net.ssl.trustStorePassword="<keystore password>"
```

Note

Newer JVMs require the keystore type to be PKCS12 format.

See [Using the jConnect JDBC Driver with SSL](#) for more information.

11 Managing SAP Adaptive Server Enterprise, Cloud Edition by IBM Cloud Instances

The ASE Cloud Portal allows you to monitor the SAP ASE cloud edition instances, migrate database encryption keys, and upload database backups to IBM Cloud Object Store.

11.1 Monitoring SAP ASE Instances

You can get an overview of all SAP ASE instances provisioned in the ASE Cloud Portal.

The SAP ASE Instances page lists all SAP ASE instances provisioned in the base environment. For each instance, you can review the instance name, workload type (high availability or non-high availability), size, and status. Select the instance name to view its details.

Nodes

The Nodes tab lists the node name, domain, and status of each node.

Databases

The Databases tab summarizes all databases within the SAP ASE instance. You can perform an ad hoc backup of all user databases from this tab.

Backups

The Backups tab lists all backups for the SAP ASE instance. By default, all user databases are backed up once a day. The database backups are retained for seven days (daily backup), five weeks (weekly backup), and three months (monthly backup). Transaction log backups are taken once an hour. This tab also lists all ad hoc backups and backups taken on-premises.

Critical Files

The Critical Files tab lists all critical files for an SAP ASE instance, such as log files and configuration files. You can download these files to your local storage.

Database Restores

The Database Restores tab displays the most recent ad hoc restore of a specific database. You can check the restore status, duration, and view error message for a failed restore.

Data Encryption Key (DEK) Transfers

The DEK Transfers tab lists all data encryption key transfer requests for the SAP ASE instance. You can check the transfer status on this tab.

11.2 Transferring a DEK

To ensure the source database (on-premises) and the target database (in the cloud) use the same database encryption key (DEK), you need to transfer your DEK from the on-premises database to IBM Cloud.

Prerequisites

Encrypt the on-premises SAP ASE database that you want to migrate with a DEK.

Context

You can find all DEKs transferred to IBM Cloud on the DEK Transfers tab in your SAP ASE instance.

Procedure

1. Export the DEK encrypted with your user password from the on-premises SAP ASE by using the `transfer encryption key` command. For example:

```
transfer encryption key <dek_name> for database encryption with password  
'<password>'  
go  
0x0100011000001000001080000000000000000000001bc572fba81246b2934a7541e675cf06  
7e54396202e90604c540184f3f8cc595e17d73ccf4299fb7c6e635752f31002d1f76900c13175c  
e5
```

2. Log in to the ASE Cloud Portal.
3. On the Database Encryption Keys page, click [Upload a DEK](#).
4. In the Upload a DEK window, enter a name for the DEK.
5. Enter the same password you used during the export in step 1 and paste the encryption key generated from the same step into the relevant field.
6. Click [Confirm](#) to upload the encryption key.
7. In the Customer Encryption Keys list, locate the encryption key you just uploaded and click the [Transfer](#) button at the right-hand side of the list to install the encryption key on your SAP ASE instance.
8. In the Install DEK window, select your SAP ASE instance to install the DEK and click [Confirm](#).
9. If your SAP ASE instance is part of an Always On/HADR cluster, repeat steps seven and eight for each SAP ASE in the cluster.

Results

The DEK is installed on your SAP ASE instance and ready to encrypt the database to be stored on IBM Cloud.

11.3 Uploading a Backup to IBM Cloud

You can follow the instructions on the [About Uploading Backup Items](#) page to upload a backup to IBM Cloud Object Store (COS).

Prerequisites

- Install Python 3.
- Install IBM Aspera Transfer SDK.
- Obtain access to the SAP ASE common services IBM Schematics Workspace.
- Obtain an IBM Service ID API Key with the following access policies:
 - **Schematics:Service Access: Manager**

- Secrets Manager: Service Access: SecretsReader
- Generate and download the `upload_to_cos.py` script from the [About Uploading Backup Items](#) page in the ASE Cloud Portal.

Procedure

1. Open the downloaded IBM Aspera Transfer SDK folder in your IDE.
2. Move the `upload_to_cos.py` script to the `/connectors/python` folder in the IBM Aspera SDK.
3. Move the dump files that you want to upload to COS into the `/connectors/python` directory in the IBM Aspera SDK.
4. Navigate to the python directory in the SDK and then run the following command to install all dependencies:

```
pip3 install -r requirements.txt
```

5. Update the following variable on line 94 of the `upload_to_cos.py` script:
FILE_NAME: Specify the name of the dump file (including extension) to upload to COS. The file must exist in the `/connectors/python` directory.
6. In the root directory of the IBM Aspera SDK folder, start the Aspera Transfer SDK daemon:

```
./bin/asperatransferd
```

7. In a separate terminal window, after the daemon is running, navigate to the python directory and run the following command:

```
python3 upload_to_cos.py
```

Results

Your dump files are successfully uploaded to COS.

11.4 Backup and Restore

You can perform an ad hoc backup or restore of any SAP ASE user database on IBM Cloud.

To perform an ad hoc backup of a user database, locate the database on the Databases tab of the instance. In the same row, click the [Backup](#) button to back up the database. After the backup completes, you can find it in the list on the Backups tab.

To perform an ad hoc restore of a user database, locate the database on the Backups tab of the instance. Click the [Restore](#) button to restore the database to the required state. You can also click the [Download](#) button to save the backup to your local storage.

12 Glossary of Terms

This glossary describes terms that are specific to SAP Adaptive Server Enterprise, cloud edition by IBM Cloud.

Administration and Management Console (AMC)	A web-based tool that provides centralized management and administration of SAP ASE servers running in IBM Cloud.
data center	A physical building that hosts the power, cooling, compute, network, and storage resources used for services and apps in IBM Cloud.
base environment	The IBM Cloud deployment environment that hosts SAP ASE cloud edition instances and their associated resources, including the Secrets Manager, VPN server, and load balancers.
base environment prefix	A customer-specific identifier prepended to the names of IBM Cloud resources to uniquely identify resources within a base environment.
companion	The standby SAP ASE instance in an Always On or HADR cluster, hosted in Data Center 2. The companion takes over database operations if the primary instance fails.
data encryption key (DEK)	An encryption key used to encrypt an SAP ASE database. In IBM Cloud, a DEK can be transferred from an on-premises SAP ASE instance to IBM Cloud to ensure the source and target databases use the same encryption.
disaster recovery (DR)	A service capability provided by the SAP ASE Always On or HADR cluster in which a primary SAP ASE instance hosted in Data Center 1 and a companion instance hosted in Data Center 2 are deployed across separate infrastructure, with automatic failover managed by the Fault Manager, to restore database operations in the event of a failure and maximize service continuity.
fault manager (FM)	A component of the SAP ASE Always On or HADR cluster hosted in a dedicated data center that monitors the primary and companion instances and triggers automatic failover when the primary becomes unavailable.
high availability (HA)	A service configuration in which a primary SAP ASE instance and a standby instance are deployed in separate Availability Zones, with automatic failover managed by the Fault Manager to maximize uptime and support disaster recovery.
managed service provider (MSP)	A service provider responsible for provisioning and managing SAP ASE cloud edition instances on IBM Cloud on behalf of a customer.
primary	The active SAP ASE instance in an Always On or HADR cluster, hosted in Data Center 1, that handles all database read and write operations under normal conditions.

SAP ASE Cloud Portal	A web-based portal deployed on a private network that allows authorized users to manage SAP ASE cloud edition instances, including uploading encryption keys, running backups and restores, and accessing log and configuration files.
virtual private cloud (VPC)	An isolated, logically defined network environment within IBM Cloud that groups related resources and controls network access between them. The SAP ASE service uses three VPCs: the Edge VPC, the Management VPC, and the Workload VPC.
virtual private network (VPN)	A secure, encrypted network connection that allows users or systems to access the SAP ASE service in IBM Cloud over the internet. The SAP ASE service supports three connection types: client-to-site VPN, site-to-site VPN, and direct connection.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

© 2026 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.

