KeyNexus DB2

Integration Guide

v1.2

08/2018

.

Copyright Notice

Table of Contents

Introduction

Many organizations are looking to Key Management Services to help protect their sensitive data. Often, that data exists in different environments and different platforms, each with its own native encryption solution. Ideally, the best approach is to have one KMS that can integrate with many different environments and platforms and manage the encryption keys for all of them. The difficulty is finding a product that can effectively integrate with all the different systems that make up your data environment and manage the keys for them all. KeyNexus has the ability to integrate with many different systems, providing a complete Unified Key Management Service.

This guide provides instructions for configuring KeyNexus and integrating it with IBM DB2. Once successfully integrated, KeyNexus acts as a centralized key store when using DB2 native encryption.

KeyNexus is a Unified Key Management Service that provides a centralized platform for the management of encryption keys throughout their lifecycle. With KeyNexus, you can create or import keys, store and rotate keys, and control key access by assigning them to a specific group or user. KeyNexus can manage encryption keys from many different environments and platforms.

IBM DB2 is a Relational Database Management System (RDBMS), designed to store, analyze and retrieve data efficiently. DB2 is extended with the support of Object-Oriented features and non-relational structures with XML.

This guide was created using Windows 10, KeyNexus v1.9.2 and IBM DB2 v.11.1. If the environment and products you currently use are different from the ones used to create this document, your workflow may be different.

Prerequisites

Before you can successfully integrate KeyNexus and DB2, make sure the following tasks have been performed:

- Download, initialize and configure your KeyNexus instance. To integrate KeyNexus with DB2, KeyNexus version1.9.2 or higher is required. Information regarding the installation and configuration of KeyNexus can be found in the *KeyNexus Web Portal User Guide*.

- Download and install IBM DB2. When DB2 is installed, the Global Security Kit (GSKit version 8) should install at the same time. The GSKit is a library and command-line toolbox that provides SSL implementation, cryptographic features and key management functionality. GSKit is required for creating and configuring the DB2 keystore where the KeyNexus certificates are stored.

  Note: GSK version 8.0.50.67 bundled with DB2 FB1 and FB2 does not work properly with KeyNexus. Confirm your version of GSKit before proceeding.

- Export the root certificate authority from KeyNexus. To properly integrate with KeyNexus, DB2 requires the KeyNexus Root CA to be added to the key store.

Export Root Certificate Authority from KeyNexus

DB2 requires the root-CA certificate from KeyNexus to add to its key store. There are many different methods to export this certificate from KeyNexus. This section provides instructions for exporting the root-CA using OpenSSL, and an example of exporting the root-CA through a browser.

Note: Before you can export the root certificate, make sure KeyNexus has been properly initialized and activated, and is accessible through your browser.

OpenSSL

OpenSSL is an open source implementation of the SSL protocol. With it, you can connect to your KeyNexus instance and output the KeyNexus certificate authority.

1. Install OpenSSL on your system and add it to the system path. For download links and documentation, visit http://www.openssl.org.

2. Open a command line window and enter:

   ```
   openssl s_client -showcerts -connect <keynexus_IP>:443
   ```

   This command opens a connection to the KeyNexus IP and outputs the full certificate chain.

   - The -`showcerts` parameter displays all certificates in the chain.
   - Replace `<keynexus_IP>` with the IP address of your KeyNexus instance.
   - Port 443 is the default port for websites that use SSL.

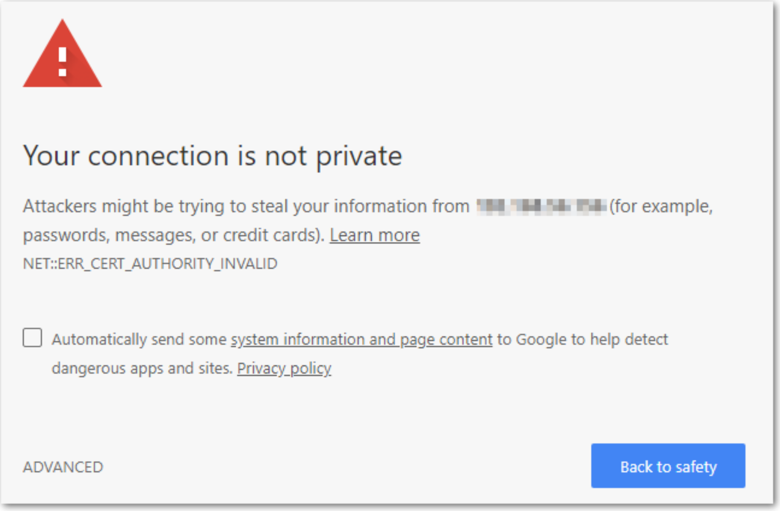
3. Copy the KeyNexus-CA certificate data and save it into a text file. In most cases this is the second certificate displayed.

Browsers

It is possible to export the root-CA through your browser. Depending on the browser, the OS it operates on, and the version, the workflow for exporting the root-CA can be very different. In this example, the Windows 10 version of Chrome is used to extract the KeyNexus-CA.

To export the KeyNexus-CA using another browser, consult that browser’s documentation.

1. Open Chrome and enter the IP address of your KeyNexus instance. The **Your connection is not private** page appears.



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

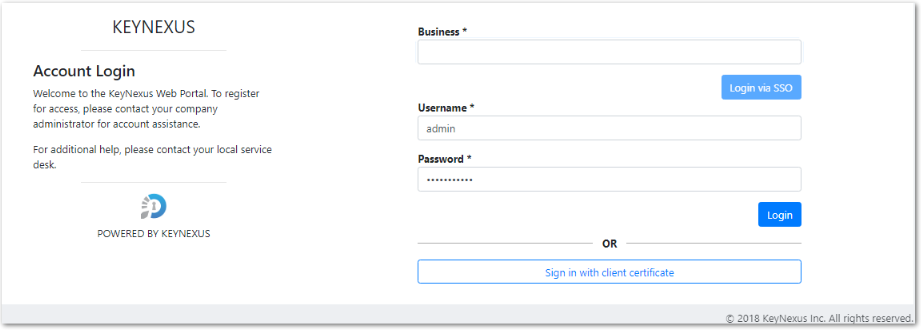
NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

2. Click **Not Secure** in the browser address bar.
3. Click **Certificate**. The **Certificate** dialog appears.
4. Click the **Certification Path** tab and double-click the KeyNexus-CA. A second **Certificate** dialog appears.
5. Click the **Details** tab in the second **Certificate** dialog.
6. Click **Copy to File**. The Certificate Export Wizard dialog appears.
7. Click **Next**
8. Select **Base-64 encoded X.509**.
9. Enter a file name and click **Browse** to select the file download location.
10. Click **Next**.
11. Click **Finish**.

Configuring KeyNexus

1. Go to `https://<your.ip>/login` and log in with your Business ID, Username and Password. Click **Login**. This advances you to the Dashboard page.



Welcome to the KeyNexus Web Portal. To register for access, please contact your company administrator for account assistance.

For additional help, please contact your local service desk.

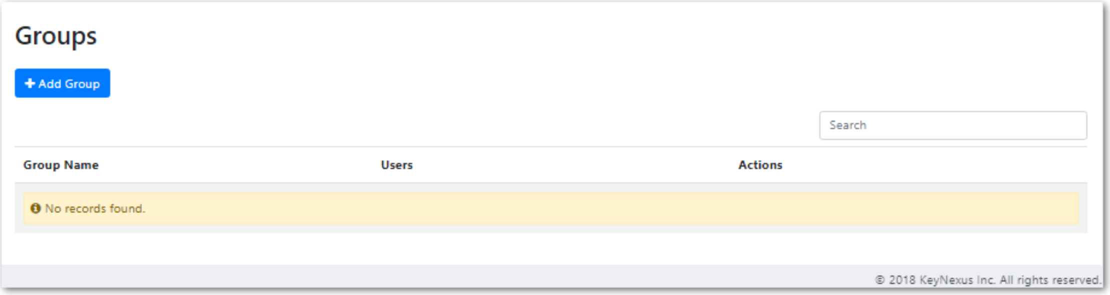
Business *

Username * admin

Password * •••••••••••

© 2018 KeyNexus Inc. All rights reserved.

Use the **Groups** feature to create a new group. The user account that is associated with DB2 access must be associated with a default group. Click the **Groups** tab to navigate to the **Groups** page.

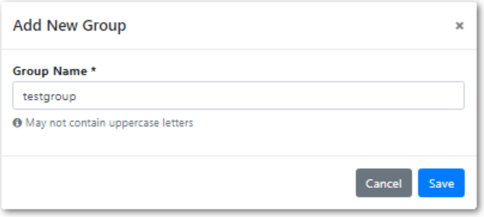


Group Name	Users	Actions
No records found.		

© 2018 KeyNexus Inc. All rights reserved.

1. Click **+Add Group**. The **Add New Group** dialog appears.

2. Enter the name of the key group in the **Group Name** field. This name should follow a naming convention to assist with the logical grouping of your keys.



Group Name * testgroup

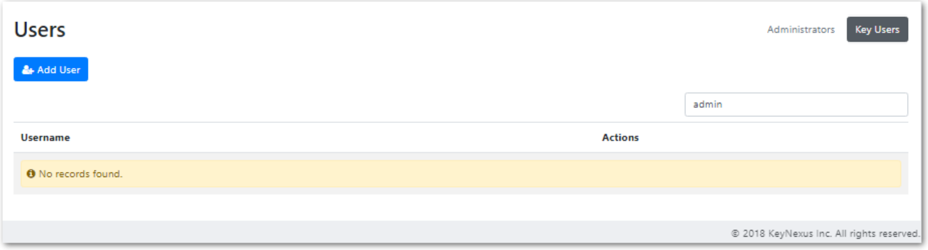
May not contain uppercase letters

Note: Group names cannot use uppercase letters.

3. Click **Save**. A message indicating that the new group was created appears in the top right corner.

When you have completed the group creation task, use the **Users** feature to create the account that is associated with DB2 for KeyNexus authentication and key creation.

1. Click the **Users** tab. This advances you to the Users page.



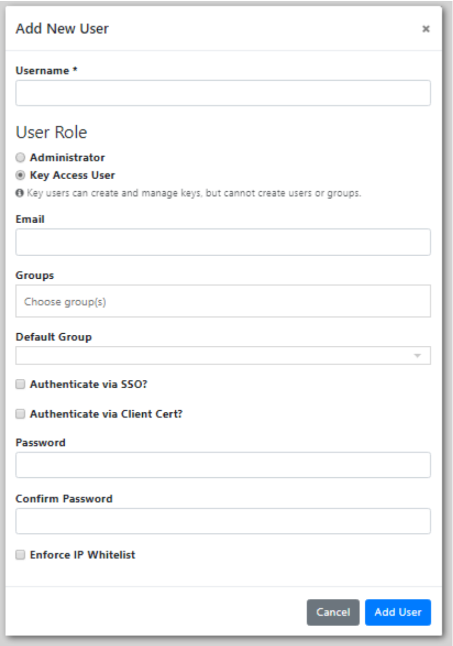
admin

Username	Actions
No records found.	

© 2018 KeyNexus Inc. All rights reserved.

2. Click **Add User**. The Add New User dialog appears.

   This account is set up to generate an authentication certificate, which DB2 requires to integrate with KeyNexus.



Username *

User Role

○ Administrator

● Key Access User

Key users can create and manage keys, but cannot create users or groups.

Email

Groups

Choose group(s)

Default Group

□ Authenticate via SSO?

□ Authenticate via Client Cert?

Password

Confirm Password

□ Enforce IP Whitelist

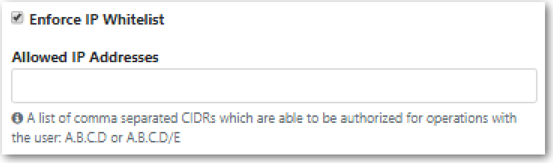
3. Enter the information required in the Add New User dialog:

Field name	Value/Description
Username	Enter the username. This username is used by DB2 when authenticating to KeyNexus.
User Role	Select **Key Access User**
Group	Select a group or groups from the list of available groups.
Default Group	Select a group to act as the default group. Make sure that you are a member of the selected group.

Email	Enter the email associated with this account (optional).
Authenticate via Client Cert	Select this option to generate a certificate used to authenticate this user. You can download the certificate after the new user is created. See Authentication Certificate for more information.
Password	Password must have a minimum length of 10 characters. KeyNexus provides feedback relating to the strength of your password. **Note**: When authenticating via Client Cert, a password is not required.
Confirm Password	Re-enter your password

4. (Optional) Click the **Enforce IP Whitelist** checkbox to restrict API requests for this account to IP address contained in this range. Enter the IP addresses in the fields provided. To enter multiple IP addresses, enter the IP addresses in a comma separated value format (a.b.c.d, a.b.c.d, etc).

   Note: Ensure that the whitelist contains the DB2 server IP.



☑ **Enforce IP Whitelist**

Allowed IP Addresses

ℹ A list of comma separated CIDRs which are able to be authorized for operations with the user: A.B.C.D or A.B.C.D/E

5. Click **Add User**.

Authentication Certificate

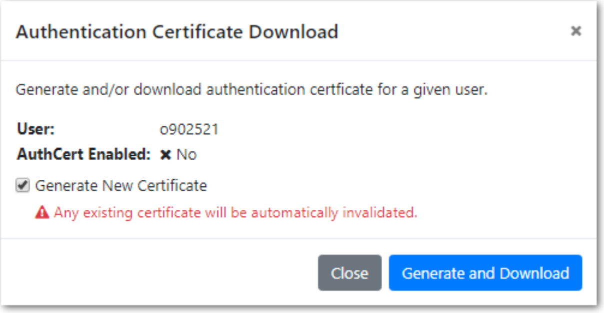
Instead of using a username and password to authenticate a KeyNexus user, you can generate and download an authentication certificate associated with a specific KeyNexus account and use it in lieu of login credentials. This certificate can be generated in several different ways:

a. During the initial user creation process, select the **Authenticate via Client Cert** option.

b. After the user has been created, locate the user in the Users list and click **AuthCertificate** beside the user name.

c. After the user has been created, locate the user in the Users list, click **Edit** beside the user name, select the **Authenticate via Client Cert** option and click **Apply Changes**.

In each case the **Authentication Certificate Download** dialog opens.



Authentication Certificate Download

Generate and/or download authentication certficate for a given user.

User: o902521

AuthCert Enabled: ✖ No

☑ Generate New Certificate

▲ Any existing certificate will be automatically invalidated.

Click **Download** to download the existing authentication certificate or select the **Generate New Certificate** option and click **Generate and Download** to generate and download a new authentication certificate.

Note: If there is no existing authentication certificate associated with the user, the dialog displays a message indicating you must generate a new certificate.

Note: Generating a new certificate automatically invalidates any existing certificate for that user. Make sure the certificate is stored in location that the creator of the Db2 database can access.

Once KeyNexus has been activated, the account used to connect to Db2 has been created and the Authentication Certificate has been successfully generated and downloaded, the next step is setup the keystore for DB2.

Configuring DB2 and GSKit

Once KeyNexus has been configured, the account used to connect to DB2 has been created and the Authentication Certificate has been successfully generated and downloaded, the next step is to setup the DB2 keystore. This keystore contains the root ca certificate and the KeyNexus authentication certificate. These are required for integration with KeyNexus.

1. Open the DB2 command-line window.

2. Locate the GSKCapiCmd tool executable.

   The default location for the 32-bit GSKCapiCmd tool executable is `C:\Program Files(x86)\IBM\gsk8\bin\gsk8capicmd.exe`.

   The default location for the 64-bit GSKCapiCmd tool executable is `C:\Program Files\IBM\gsk8\bin\gsk8capicmd_64.exe`.

3. Create the DB2 keystore, set the keystore's password and store the obfuscated password in a stash file for easier access using the command:

```
gsk8capicmd_64 -keydb -create -db c:\keystore\demokeystore.p12 -
pw password -type pkcs12 -stash
```

Option name	Description
keydb	Object – actions in this command are performed on the keydb object.
create	Creates the keystore.
db <location and name>	Keystore full path name and location
pw <password>	Sets required password
type <type>	Indicates the type of keystore to create. In this case, pkc12.
stash	Creates a stash file containing the obfuscated password.

4. Add the root ca certificate into the DB2 keystore, and label it as a trusted certificate using the command:

```
gsk8capicmd_64 -cert -add -db c:\keystore\demokeystore.p12  -
stashed -label "trustedCA" -file c:\keystore\keynexus.cer -format
ascii -trust enable
```

Option name	Description
cert	Identifies the file as a certificate.
add	Add this cert to the keystore.
label	Name given to certificate stored in the keystore. This name should make it easier to identify the certificate.
format	Specifies whether the format of the certificate is binary or Base 64 ASCII
trust	flag that marks the certificate as being trusted by the DB2 database and can be used for validation purposes.

5. Add the authentication certificate generated by KeyNexus into the DB2 keystore and label it as a client certificate using the command:

```
gsk8capicmd_64 -cert -add -db c:\keystore\demokeystore.p12  -
stashed -label "clientcert" -file c:\keystore\kn-db2user-cert.pem
-format ascii
```

Option name	Description
cert	Identifies the file as a certificate
add	Add this cert to the keystore.
label	Name of the certificate. This name should be easily identifiable
format	Specifies whether the format of the certificate is binary or Base 64 ASCII
trust	flag that marks the certificate as being trusted by the db2 database and can be used for validation purposes.

6. Confirm the certificates have been successfully added to the keystore with a command using the `-validate` option:

   ```
   gsk8capicmd_64 -cert -validate -db c:\keystore\demokeystore.p12 -
   stashed
   ```

7. Configure the KMIP configuration file shown below and save it in a location that the DB2 database user can access:

   ```
   VERSION=1
   PRODUCT_NAME=OTHER
   ALLOW_KEY_INSERT_WITHOUT_KEYSTORE_BACKUP=TRUE
   ALLOW_NONCRITICAL_BASIC_CONSTRAINT=TRUE
   SSL_KEYDB=c:\keystore\demokeystore.p12
   SSL_KEYDB_STASH=c:\keystore\demokeystore.sth
   SSL_KMIP_CLIENT_CERTIFICATE_LABEL=clientcert
   MASTER_SERVER_HOST=node1.keynexus.local
   MASTER_SERVER_KMIP_PORT=5696
   CLONE_SERVER_HOST=node2.keynexus.local
   CLONE_SERVER_KMIP_PORT=5696
   CLONE_SERVER_HOST=node3.keynexus.local
   CLONE_SERVER_KMIP_PORT=5696
   ```

Where:

- `PRODUCT_NAME:` can be set to any name that easily identifies what it is.
- `ALLOW_KEY_INSERT_WITHOUT_KEYSTORE_BACKUP:` is set to true
- `ALLOW_NONCRITICAL_BASIC_CONSTRAINT:` is set to true
- `SSL_KEYDB=:` is the location of the keystore set in Step 3
- `SSL_KEYDB_STASH:` is the location of the stash file
- `SSL_KMIP_CLIENT_ CERTIFICATE_LABEL:` is the client certificate label set in Step 5.
- `MASTER_SERVER_HOST:` is the KeyNexus node DB2 is connected to.
- `MASTER_SERVER_KMIP_PORT:` is set to port 5696.
- `CLONE_SERVER_HOST and CLONE_SERVER_KMIP_PORT:` can also be set, but these are optional.

Note: DB2 requires the hostname to match the ssl certificate presented by the KeyNexus node. Make sure to either modify the hosts file on the DB2 server or add a DNS entry in the DNS server.

8. Open the DB2 command window and enter the commands:

   ```
   update dbm cfg using keystore_location c:\keystore\keyconfig.conf
   ```

   ```
   update dbm cfg using keystore_type kmip
   ```

9. After any change to the config file it is recommended that you stop and start the DB2 database by entering the commands:

   ```
   db2stop
   ```

   ```
   db2start
   ```

10. In order to test the kmip configuration and connection with KeyNexus, use the command:

    ```
    create db testdb encrypt
    ```

To confirm that the key was successfully created, log in to KeyNexus, look at the user associated with DB2 and confirm the key was created. You can view additional information relating to the key by clicking **View** beside the key name and reviewing the Operations History.

Additionally, you can use the db2diag program on the DB2 server to see the operation status.

11. Remove the testdb with the command:

    ```
    drop db testdb
    ```

Additional Links

For additional information relating to IBM DB2 encryption and IBM's Global Security Kit (GSKit), visit the links below:

https://www.ibm.com/developerworks/data/library/techarticle/dm-1504-master-encrypted-keys/index.html.

https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.admin.sec.doc/doc/c0061758.html

KeyNexus DB2 Integration Guide v1.2

KeyNexus Inc.
205 2657
Wilfert Road
Victoria, B.C.
V9B 5Z3