kConnect DUO® Setup

For the IBM i

Kisco Connect

Version 2.0

How to contact us

Direct all inquiries to:

Kisco Systems LLC
54 Danbury Road
Suite 439
Ridgefield, CT 06877

Phone: (518) 897-5002

Kisco Website: www.kisco.com

Table of Contents

CHAPTER 1 – KCONNECT - TWO-FACTOR AUTHENTICATION USING DUO® 1-1

Kisco Connect DUO 2FA Overview 1-1
Setup Kisco Connect with DUO 1-2
Validating your new DUO account 1-5
Setting up a kConnect DUO User 1-7
Activating a User in DUO and sending a TEST Push Notification 1-9

CHAPTER 2 - VIEWING THE DUO LOG FILE 2-15

CHAPTER 3 - IMPROVING DUO PERFORMANCE 3-1

Changes required to use new QSYS2 SQL functions with DUO and SMS messaging 3-2
Using an Alternate Digital Certificate store for kConnect 3-3
Certificates needed for DUO and SMS 3-5

CHAPTER 4 - PROGRAMMING EXAMPLES 4-1

Using kConnect's DUO 2FA in IBM i applications 4-1

Chapter 1 – kConnect - Two-Factor Authentication using DUO®

Kisco Connect DUO 2FA Overview

By using kConnect Two-Factor Authentication along with SafeNet/i and i2Pass, you can secure access to your IBM i services using industry leading multi-factor authentication software your users may already be familiar with, such as DUO and Microsoft Authenticator.

Kisco's kConnect 2FA module, along with Kisco's i2Pass and SafeNet/i products, allows you to set up network and user authentication rules for 5250 sign-on services (Telnet), FTP sessions and SQL access.

Regardless of whether you use kConnect with or without SafeNet/i and i2Pass, you can imbed our DUO authentication module into an existing application for an even stronger layer of protection.

kConnect 2FA uses popular multi-factor authentication services such as DUO to provide the added security.

kConnect 2FA using DUO can be used with or without an associated IBM i user profile. If you need DUO authentication for your IBM i website or web service or even an external application, you can use a DUO user name to provide 2FA for non-IBM i users.

This IBM i software utility routes messages through a 3rd party SMS service instead of using the outdated email-to-text method. It works natively within the operating system and does not require any special software or system configuration.

Setup Kisco Connect with DUO

It's this Easy!

1. If you haven't already done so, install the kConnect product following the instructions at the Kisco Systems website Kisco.com.

2. Go to www.duo.com and create a new DUO account. Follow the instructions at the link below on how to create your first DUO account. At the time of this writing, you can open a DUO account for FREE for up to ten (10) users. You can start with a free basic account first and then you can upgrade the account to a full account later. Full accounts are sold in blocks of 10 users.

3. You will need to obtain:
   a. A DUO Account ID
   b. An Integration Key
   c. A Host Key
   d. A Secret Key

4. You will also need to authorize your new DUO account to use the "Auth" API.

   This can be done on the DUO Admin Panel:

   Navigate to *Applications* and select *Protect an Application*

   This is the same page where you will get the needed keys for the DUO account you created. https://duo.com/trial

5. Configuring kConnect DUO

   After you have obtained the required items listed in Step 3 above, you are ready to configure kConnect for 2FA using DUO.

   Before you begin, you may want to add the KCONNECT library to your library list so you can use kConnect commands - A**DDLIBLE KCONNECT**

   - On a 5250 command line, enter the following command:

     GO KCONNECT/KCDUO

   - Select **Option 2 - Work with DUO Service Accounts**

- If this is a new installation, you will be prompted to *Add a New Account*. Please enter the requested information. You can use the account ID of *DEFAULT at this time. The invite timeout determines how long the invitation is valid. 86400 seconds = 1 day.

- The information entered under the “Invite Content” will be included in the DUO invitation sent to the user.

- When finished, exit the program.

6. Set the method to send the DUO Invitation to the user.

   You can send the invitation to the end user using one of these methods:

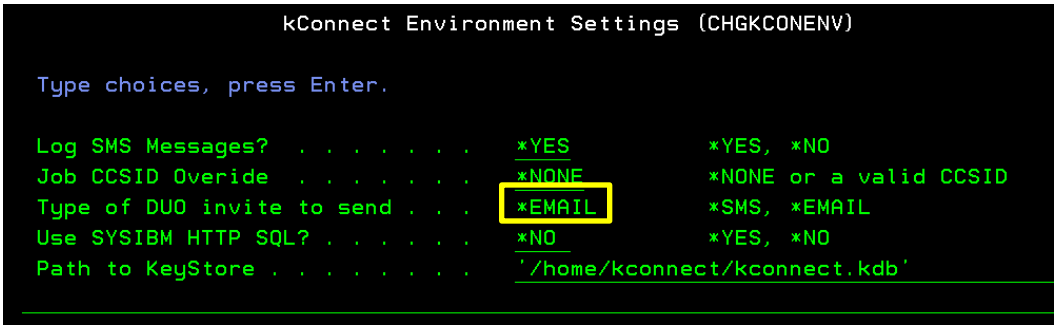
   - Use *SMS if you have the *SMS messaging module of kConnect configured and ready
   - Use a standard email via the SMTP server on the IBM i

   There are two considerations:

   - For *SMS you must have the kConnect SMS module configured for Twilio or Telesign SMS service.

   - For *EMAIL invites, you must have the SafeNet/i product installed and the 2FA module of SafeNet/i installed and configured. See the SafeNet/i documentation for more information.

You can change this setting by using the **CHGKCONENV** command and the *DUOINVTYP* parameter.



Validating your new DUO account

Once you have entered your DUO account information, you will need to verify it is accurate and active.

- From the DUO Main Menu (KCDUO) select **Option 70 – DUO Actions** or type **GO KCDUO2** from the command line

- From the DUO Actions Menu (KCDUO2) select **Option 1 – DUOPING or use the DUOPING** command.

  This option will verify that your system can communicate with the external DUO Host. If you are using the **DEFAULT* DUO account, just press enter and watch for the response.

  If you receive this message, you can proceed with account validation

  If you receive any other message, then you must investigate why.

  The DUO host name may have been entered incorrectly or your system network firewall is blocking the communications path. Check with your system administrator for further assistance.

  If the ping test is successful, proceed with a **DUO CHECK** to check the account signature.

- From the DUO Actions Menu (KCDUO2) select **Option 2 – DUO Check**.

  Change the account name if required and **ENTER**.

- You should receive a message indicating the account signature is validated.

If not, you must verify you entered the information correctly from the DUO website into the *kConnect DUO Service Provider* option.

Setting up a kConnect DUO User

Steps needed to create a DUO user in kConnect:

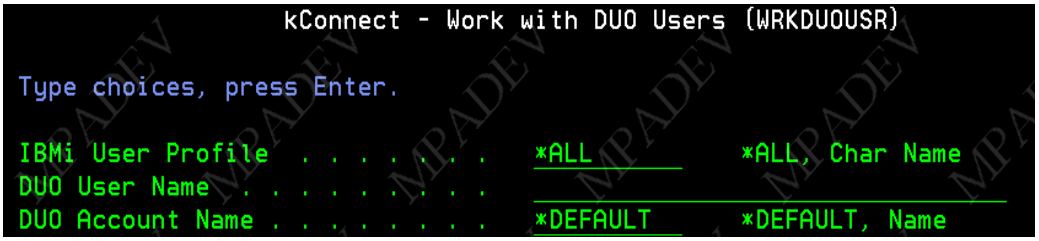
- If you have not already done so, add the KCONNECT library to your library list:

  ADDLIBLE KCONNECT

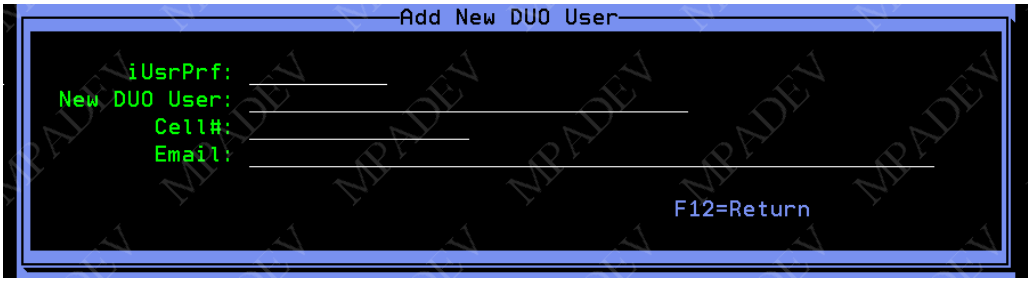
- On the command line type **GO KCDUO** to access the kConnect DUO Main Menu
- Select **Option 1 - Work with DUO Users**

  Set *IBM i User Profile* to **ALL* and the *DUO Account Name* to **Default*

  Leave *DUO User Name* blank for now and **ENTER**



- For each user, **press F6** to add a user and then fill in the pop-up window



  - Enter an *IBM i User Profile* name in the *iUsrPrf* field
  - Enter any name in *New DUO User* (no special characters). This name is not important when using IBM i profiles but it is required for DUO. DUO 2FA software recognizes and uses this as the user ID.
  - Enter the cellphone number of the user's device where the DUO application will be installed. It must be a smartphone capable of SMS and be able to receive PUSH notifications.

- Enter an email address of the user. This is required if you are not using kConnects SMS messaging service and will be using regular email to send the user the invite notification.

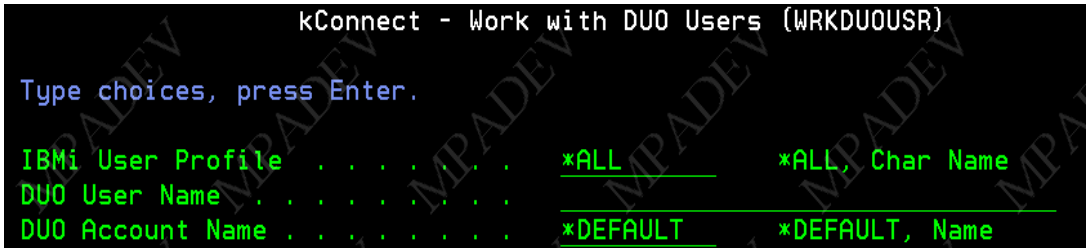
- Press **ENTER** and repeat for each DUO user.

Activating a User in DUO and sending a TEST Push Notification

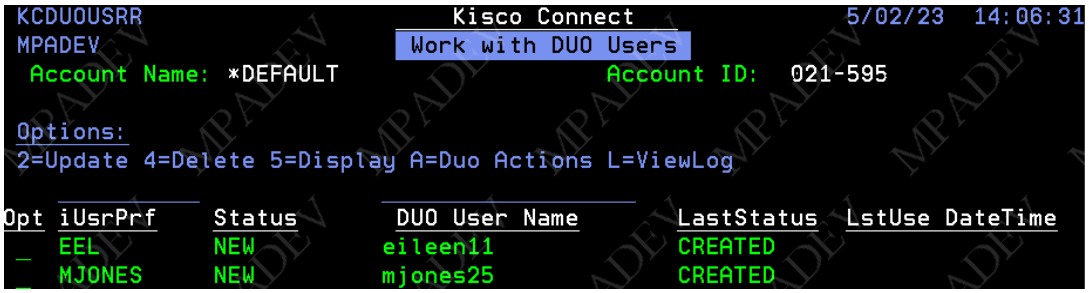
Steps needed to enroll and activate a new DUO user:

- From the kConnect Main Menu (KCDUO) select **Option 1 - Work with DUO Users**

  Use the default of **ALL* users and the **Default Account Name*. Leave the *DUO User Name* blank for now. Then press **ENTER**.



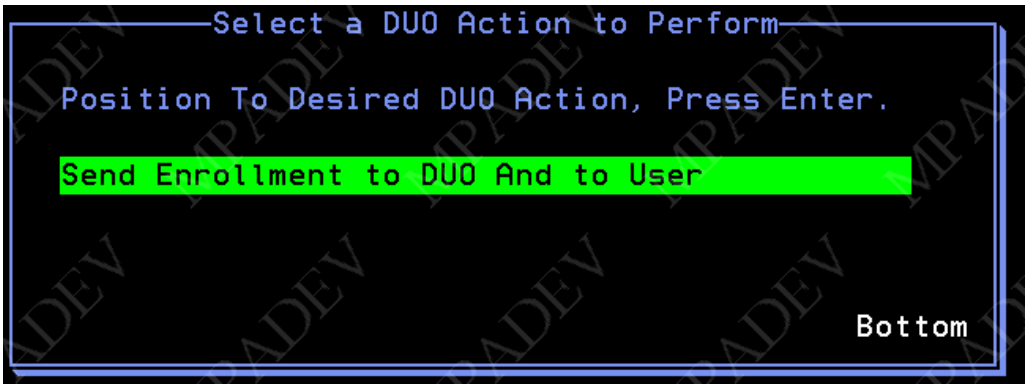
  You will see a list of your DUO users



- At this point you can send an invitation to any user in *CREATED* status to have them download and install the DUO mobile app.

  Type A in the *Option* column in front of a *User Profile* to view a list of available DUO actions

Select/highlight *Send Enrollment to DUO and to User* and press **ENTER**

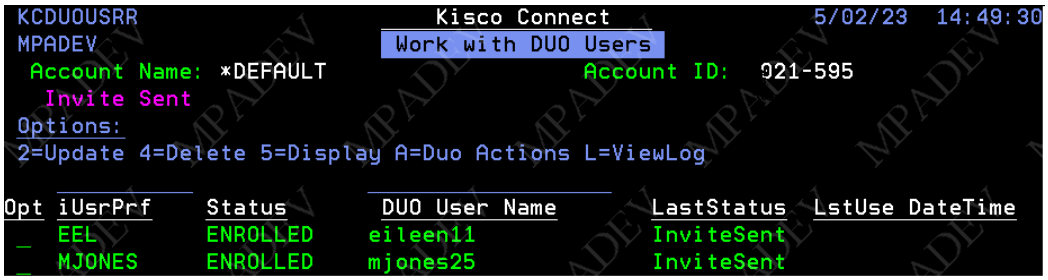


When you see the confirmation screen press **ENTER**

Next you will see a confirmation screen that the invite has been sent.

The user will receive either an SMS text message or an email with a link for the URL to download the DUO mobile app. The user should accept the link and install the DUO app.

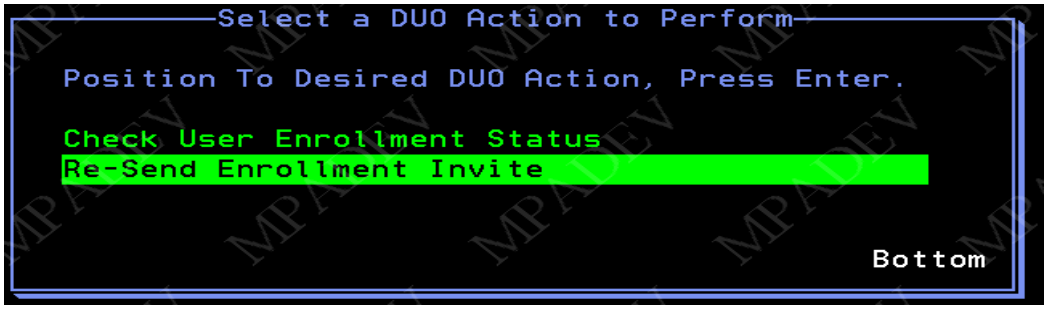
You should now see the user as *ENROLLED* and their last status is *InviteSent*.



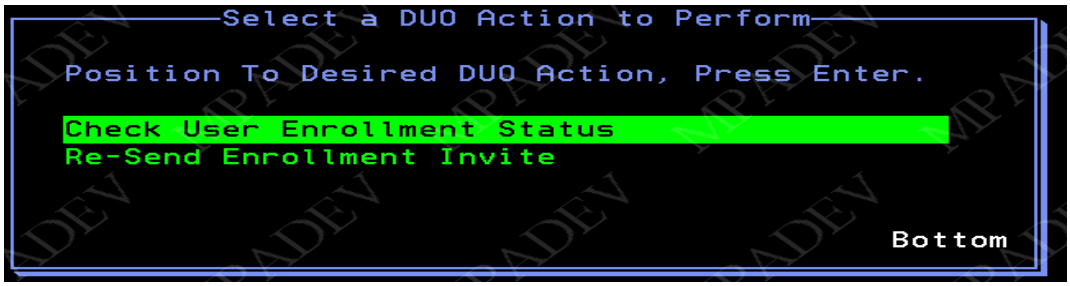
If the user indicates that they **DID NOT** receive the invitation:

Select *Option A* again

Select *Re-Send Enrollment Invite* and **ENTER**



Use O*ption A* again for that user to view the available DUO actions.



At this point you can check the status or re-send the invitation.

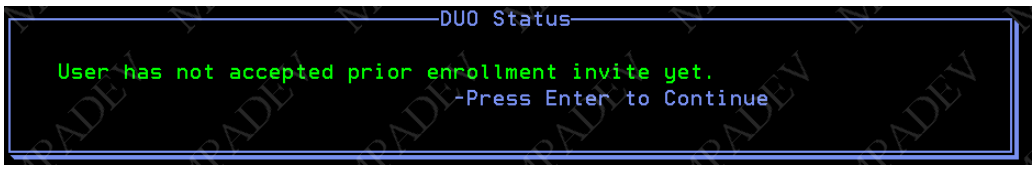
Be aware that the status will not be changed/updated until after the user accepts the invite. Also, the invite time-out is defined in the DUO service provider record. If the user doesn't accept within that time frame, then invite is considered EXPIRED.

IMPORTANT NOTE: If the status of the invitation has EXPIRED, you cannot re-send the invitation. You must follow these steps:

1. DELETE the user from the local kConnect DUO users table using the WRKDUOUSR command
2. Recreate a NEW kConnect DUO user. You must also use a DIFFERENT DUO User Name.
3. You must go to the DUO Website and remove the original DUO user from your DUO account. Removing the DUO user locally does NOT remove the user from the DUO website.

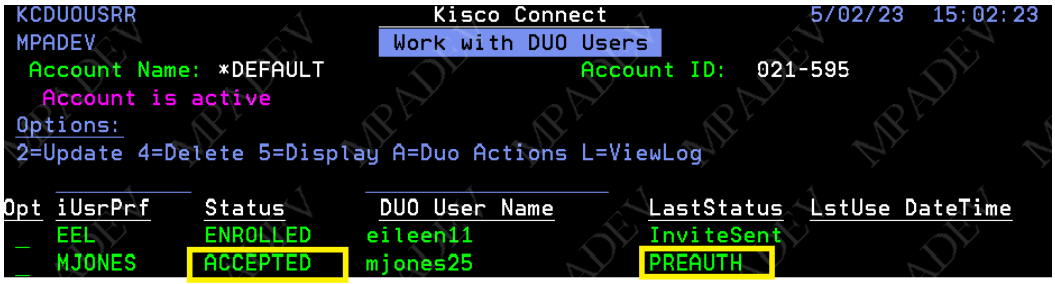
Select *Check the User Enrollment Status* option and press enter.

If you see this text it means the user has not completed the mobile app install. You may want to re-send the invitation using the steps described on the previous page.



If you see this text, you are ready to continue:

You should now see the user with a *Status* of ACCEPTED and *LastStatus* of PREAUTH (preauthorized).

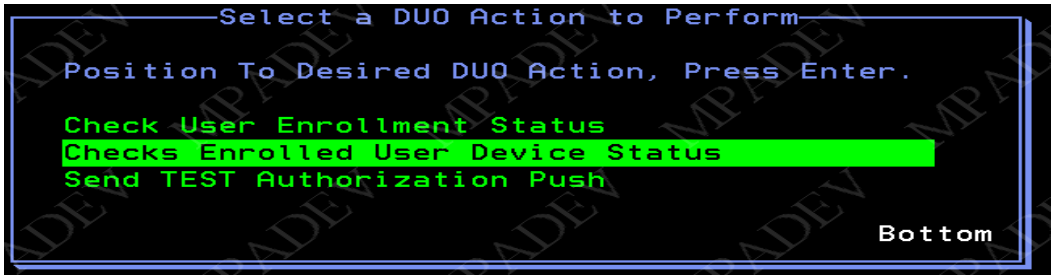


Select *Option A - Duo Actions* again and press **ENTER**.

There will now be more *Actions* to choose from.

You can choose to check enrollment status or check the user's device status. These options could be used to further check the current status of the user account.

Select *Checks Enrolled User Device Status* and press **ENTER**.

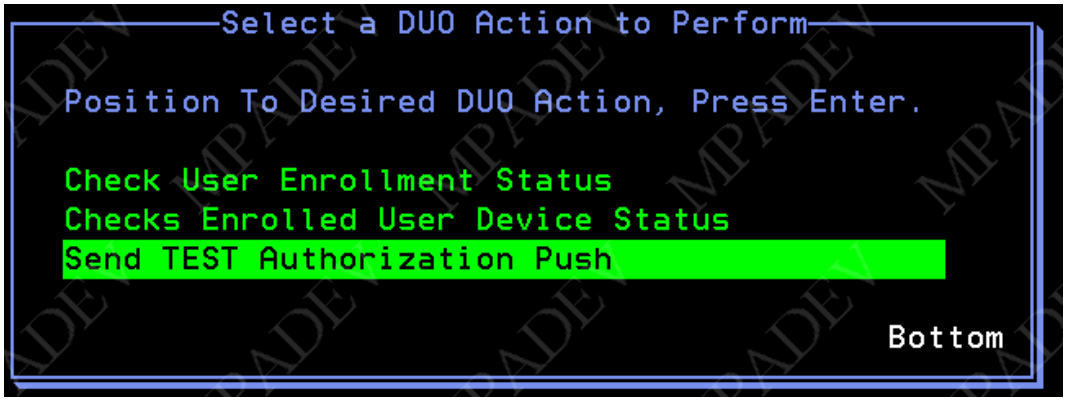


If you see this message, the account is ready to use.

As a final step, send the user a *TEST Push Notification*.

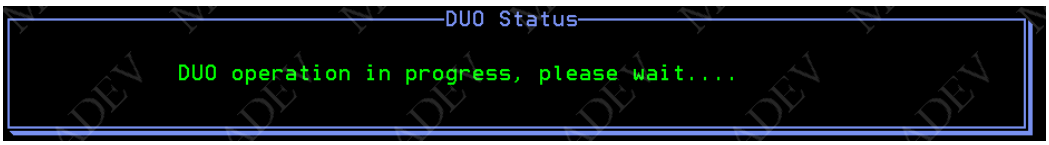
On the *WRKDUOUSR* screen, **type A** next to the user name and press **ENTER**.

You should see the *DUO Action* pop up window.



Using your up/down keys, select *Send TEST Authorization Push* and press **ENTER**.

You will see a screen waiting for the user to Accept or Decline the TEST.



If the User accepts you will see >

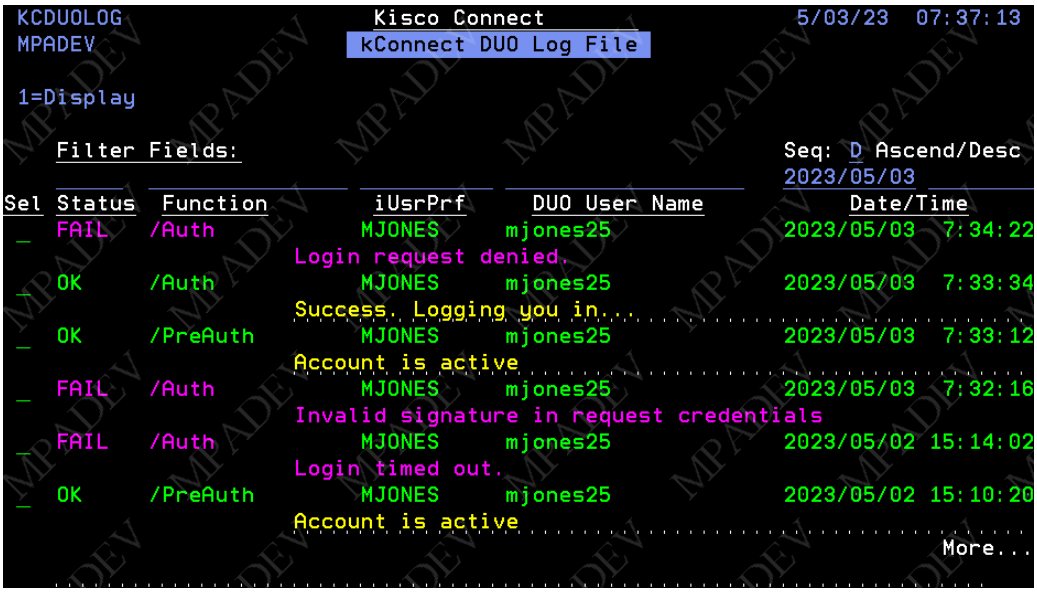
If the user Declines the request or does not respond to the request you will see >

NOW YOU ARE READY TO USE DUO.

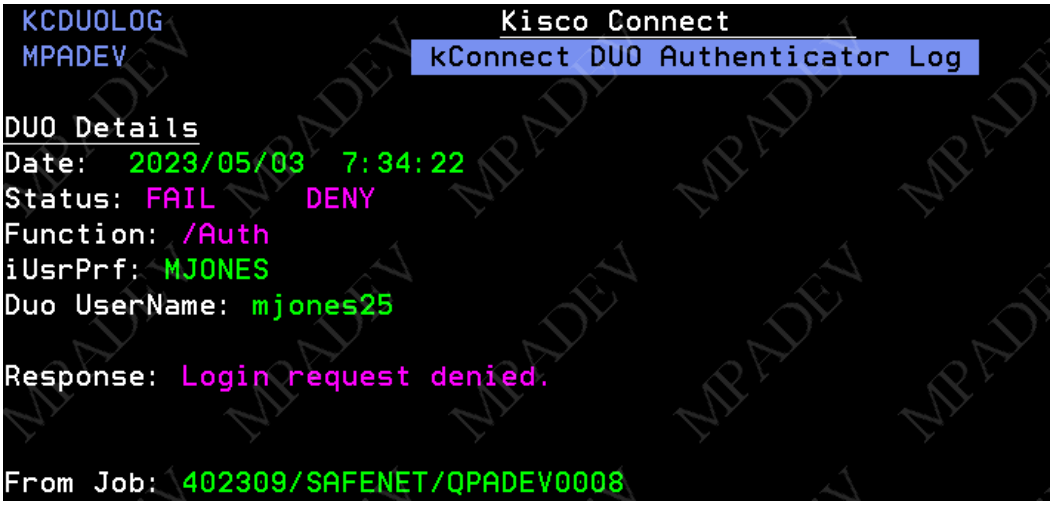
You must also configure Kisco's i2Pass and/or SafeNet/i to be able to use DUO for 2FA with those products. See documentation for i2Pass and SafeNet 2FA modules for this information.

Chapter 2 - Viewing the DUO Log file

To view log entries, use **Option 6 – Display DUO Log File** on the kConnect Main Menu (KCDUO) or use the **DSPDUOLOG** command.

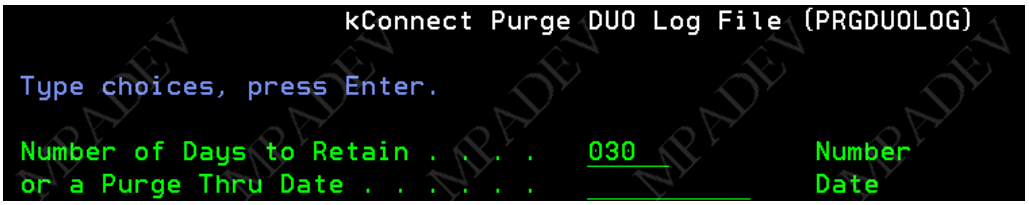


Type 1 in the *Option* column to view specific details about the *DUO Action* message or any error messages.



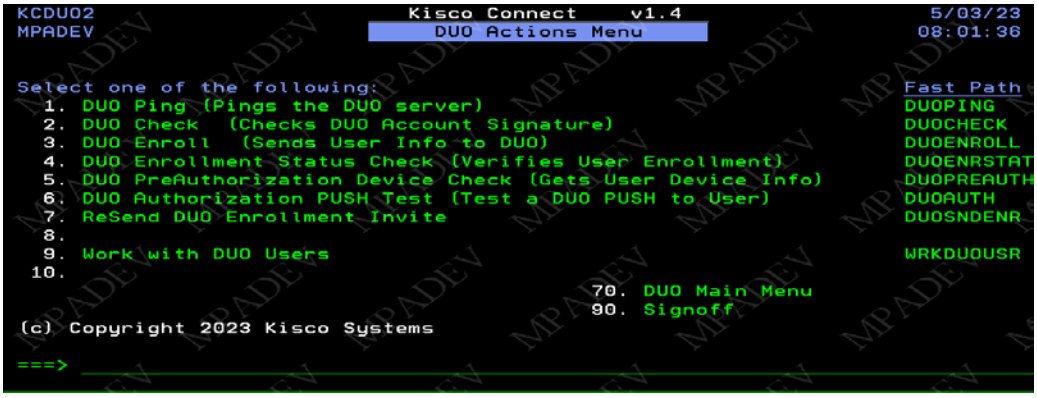
Purging the DUO Log file

At some point you may want to purge the log file as it may grow quite large over time. Use **Option 7 – Purge DUO Log File** from the KCDUO menu or use command **PRGDUOLOG**. You can enter a purge thru date or the number of days to retain.



Using Menu KCDUO2 for all the individual DUO commands

All the individual kConnect DUO commands are listed on the DUO Actions Menu (KCDUO2). You may use these commands individually or within your own applications. All the commands can also be accessed via the **WRKDUOUSR** command and using **Option A** for *DUO Actions*.



1. DUOPING - Checks your system and network capability to access the remote DUO Host
2. DUOCHECK - Validates your DUO account operability
3. DUOENROLL - Enrolls a User into the DUO website DB
4. DUOENRSTAT - Checks status of an enrolled user to see if they have installed the DUO App
5. DUOPREAUTH - Checks and retrieves the device status the user installed DUO mobile on
6. DUOAUTH - Sends the PUSH notification to user asking if they Accept or Decline a connection
7. DUOSNDENR - Resends the invite to the DUO User

Chapter 3 - Improving DUO Performance

There are two ways to connect to the DUO service providers.

ORIGINAL METHOD uses legacy SYSIBM SQL functions and a local Java Virtual Machine (JVM). This method, although very reliable, can be a bit slow to start since it has to start a local JVM.

NEWER METHODS for connections are available only on IBM i V7R3 and later with the latest Technology Refresh PTFs. They are much faster and utilize QSYS2 SQL functions that don't rely on a local job JVM to start.

By default kConnect is set to use the original SYSIBM SQL functions. To use the newer functions you must review these steps:

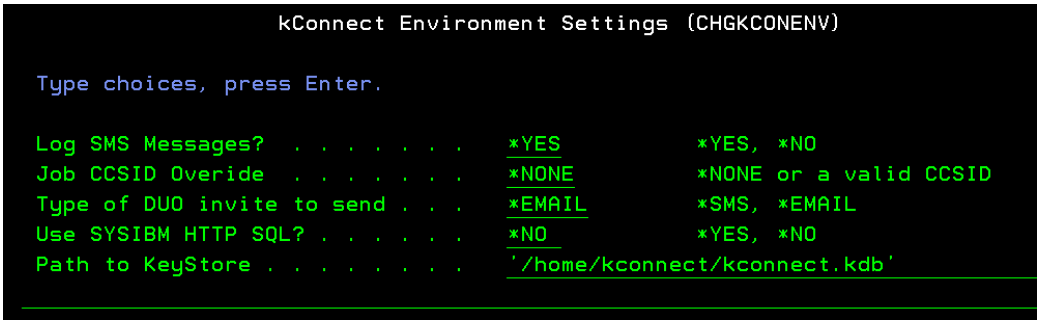
- Populate your DCM Certificate Authorities as described on the following pages in this chapter

- Make sure you are on V7R3 or above with the latest Technology Refresh PTFs installed

- Activate the newer QSYS2 SQL functions.

  From the kConnect Main Menu, use **Option 5 – Change kConnect Environment Settings** or the following command to change the kConnect Environment:

  CHGKCONENV USESYSIBM(*NO)



- Test a DUO push to a user. If this doesn't work, review the above steps and the JOBLOG for further information.

- You can revert back to the original method with this command:

  CHGKCONENV USESYSIBM(*YES)

Changes required to use new QSYS2 SQL functions with DUO and SMS messaging

IBM gives you two choices to connect to the remote servers needed for SMS messaging and DUO authentication.

The newer and better performing method requires some additional setup and configuration.

Note: If you choose to NOT make the changes listed below you can use the legacy method by making sure kConnect is set properly. Use **CHGKCONENV USESYSIBM(*YES)**

If you DO choose to use the new QSYS2 SQL Functions with DUO you need to do the following:

1. Make sure you have the new certificate store and the required Certificates are added to the keystore. (see below)

2. Give *Public authority to lookup the CAs in the keystore for SSL processes by issuing the proper commands listed below.

3. Issue this command to set kConnect's DUO & SMS support to use the new SQL functions:

   CHGKCONENV USESYSIBM(*NO)

If you receive SQL **38501** errors when attempting to use kSndSMS or DUO you need to check the following:

1. Are the two required Certificates populated in your keystore?

2. Does *Public have *RX rights to the above directory and the default.kdb file in the directory?

If you continue to have the problem, try changing kConnect back to using the legacy SYSIBM SQL functions by issuing the following command:

CHGKCONENV USESYSIBM(*YES)

Contact Kisco Systems for additional support.

Using an Alternate Digital Certificate store for kConnect

If you want to use a separate keystore for kConnect, you can either use one provided by Kisco or create your own.

Use the keystore provided by Kisco

Check to see if there is a directory and files in the IFS using

WRKLNK '/home/kconnect'

Inside the directory you should find two files - **kconnect.kdb** and **kconnect.RDB**

If the directory or files **ARE NOT** present, you can contact Kisco for instructions on how to restore them OR follow the directions below to create them.

If the directory and files **ARE** present, you will need to re-sync the DCM passwords to the new certificate store using the following steps:

1. Open your DCM web app and open an "other" keystore

2. The "other" keystore path is **/home/kconnect/kconnect.kdb**

   The password is **kconnect**

3. Choose the option to change the keystore password and set it to **kconnect2**

4. You will now have to log back into the "other" keystore and then select to change the password again. Change it back to **kconnect**.

5. Change the authority for the certificate store:

   CHGAUT OBJ('/home/kconnect') USER(*PUBLIC) DTAAUT(*RX) SUBTREE(*ALL)

Passwords are now re-synced and security updated. You can continue.

Creating your own certificate store for kConnect

Make a new directory to store the new keystore by issuing this command:

MKDIR '/home/kconnect'

1. Open the System DCM at *http://hostname:2006/dcm*
2. Click on ***Create Certificate Store***
    - Select a store type of ***Other***
    - For PATH enter **/home/kconnect/kconnect.kdb**
    - For password enter "**kconnect**" or something of your choice.
3. Click on ***Create***

You should receive a message that the keystore was created and the new keystore name will be displayed on the top of the screen.

If the new keystore name is **NOT** shown, please back up until you can select ***Open Certificate Store*** and then open the new store at path

/home/kconnect/kconnect.kdb

1. Click on ***Populate With CAs*** > ***Select All*** > ***Populate***
2. Exit the DCM
3. On a command line enter

CHGAUT OBJ('/home/kconnect') USER(*PUBLIC) DTAAUT(*RX) SUBTREE(*ALL)

Your new kConnect keystore is ready for use.

Certificates needed for DUO and SMS

You may have to add Certificate Authorities to the keystore if they are not already populated.

To View or Add the CA's to your keystore

Open the keystore you are using with kConnect in DCM.

You can get to your Digital Certificate Manager normally thru Navigator for i under the ***Bookmarks*** navigation link or directly via: http://*yourhost*:2006/dcm/login

1. Sign in and select ***Open Certificate Store***
2. Click ****SYSTEM store*** or ***Other*** if you are not using the default keystore.
3. Click ***Server/Client Certificate*** > ***Populate with CAs*** > ***Select All***

   Note: you can select only specific CAs but only you can decide which are required thru trial and error.

4. Click on ***Populate***

Chapter 4 - Programming Examples

Using kConnect's DUO 2FA in IBM i applications

Sample RPG program to call the kConnect DUO Authenticator:

This code is not a complete RPG program.
Insert sample code snippets where needed.

```
//*************************************************************
// DUOAUTHUSR  - kConnect DUO User authenticator Procedure
//*************************************************************
     Dcl-Pr DUOAUTHUSR   ExtPgm('KCONNECT/AUTHUSRCL');
       @IUsrPrf     Char(10)  Const; // IBMi user id to send DUO push
       @DUsrNam     Char(32)  Const;  // not used with iUsrPrf.
       @DActNam     Char(10)  Const; // defines which DUO account to use.
       @AppNam      CHAR(32)  Const;  // Application or Reference name
       @DStat       Char(20); // Return Status code from DUO
       @DMsg        Char(75); // Return Messages from DUO
     End-Pr;

// Parameters for the DUO authenticator
  Dcl-s @UserID     Char(10);
  Dcl-s @DUOUsrNam  Char(32) inz(*blank);
  Dcl-s @DUOAccount Char(20) Inz('*DEFAULT');
  Dcl-s @ThisApp    Char(20) inz('MyAppName'); // Choose an App Name to show End user
  Dcl-S @DUOStat    Char(20) inz(' ');
  Dcl-s @DUOMsg     Char(75) inz(' ');

  // Fill in the @UserId variable from current user.
   @UserId = SomeUser;

  // Call the DUO authentication process and waits for response
  Callp DuoAuthUsr(@UserId:@DUOUsrNam:@DUOAccount:@ThisApp:@DUOStat:@DUOMsg);

   If @DUOStat = 'OK';
     // Success! User Accepted DUO 2FA, Allow Connection.
     @RtnStatus = '1'; // Allow
   Else;
      // FAILED! User Rejected DUO 2FA, Reject Connection.
      @RtnMsg = @DUOMSG; // return error message to caller
      @RtnStatus = '0'; // Reject
   ENDIF;
```

```
// End RPG Sample Code
//*************************************************************************


//*************************************************************************
 Sample CL program to call the kConnect DUO Authenticator:
 Program will return variable &DUOStat with either 'OK' or 'FAIL'
 Variable &DuoMsg will contain additional information.
//*************************************************************************

Pgm  Parm(&UserId &DUOStat &DuoMsg)

  Dcl &UserID    Char 10 /* IBMi User Profile to authenticate */
  Dcl &DUOUsrNam  Char 32 Value(' ') /* Not used with IUsrPrf - Duo User Name */
  Dcl &DUOAccount Char 20 Value('*DEFAULT') /* DUO Account to use */
  Dcl &ThisApp Char 20 Value('MyAppName') /* Choose an App Name to show End user */
  Dcl &DUOStat Char 20 Value(' ') /* Return Status from DUO Call */
  Dcl &DUOMsg  Char 75 Value(' ') /* Reurn Message from DUO call */

Call kConnect/DuoAuthUsr(&UserId &DUOUsrNam &DUOAccount &ThisApp &DUOStat
&DUOMsg)

   If Cond(@DUOStat *EQ 'OK') Then(do)
     // Success! User Accepted DUO 2FA, Allow Connection.
     // Allow – Continue
   Enddo
   If Cond(@DUOStat *NE  'OK') Then(do)
     // FAILED! User Rejected DUO 2FA, Reject Connection.
     // Reject -Stop Connection
   Enddo

EndClPgm: EndPgm
```