One Identity Quick Connect for Mainframes 2.3.0

Installation and Configuration Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Quick Connect for Mainframes Installation and Configuration Guide
Updated - October 2017
Version - 2.3.0

Contents

Installing and Configuring One Identity Quick Connect for Mainframes

This document describes how to install, create and configure the Quick Connect for Mainframes connector into an existing One Identity Quick Connect system. This enables Quick Connect to connect to IBM RACF®, CA ACF2™ and CA Top Secret® databases on the mainframe using the Quick Connect for Mainframes (bridge).

Please refer to the One Identity Quick Connect documentation on http://software.oneidentity.com for additional information and guidance on One Identity Quick Connect.

Prerequisites

Prerequisites

Ensure that the following installation prerequisites are met before installing One Identity Quick Connect for Mainframes:

- Quick Connect Sync Engine version 5.4 must be fully installed and functional.
- The Quick Connect for Mainframes (bridge) must be installed and configured for the database that will be accessed (IBM RACF®, CA ACF2™ or CA Top Secret®). Please refer to the Quick Connect for Mainframes 2.3.0 (bridge 3.5.5) LDAP Bridge Installation Guide.
- An administrative account must be set up for the database with the appropriate permissions to administer user and group information.

For additional information and guidance on Quick Connect Sync Engine version 5.4, please refer to the ActiveRoles Quick Connect documentation on http://support.oneidentity.com/.

How to install and configure the CA Top Secret® Connector

The CA Top Secret® Connector is distributed in a standard Microsoft® MSI format which contains the required files to install and configure the CA Top Secret Connector in an existing One Identity Quick Connect environment.

The following sections describe:

- Installing the One Identity Quick Connect for Mainframes (CA Top Secret®) Connector software
- Adding a new CA Top Secret® Connector
- Modifying an existing connection to CA Top Secret®
- Configuring CA Top Secret® Connector attributes
- Creating a workflow
- Configuring CA Top Secret® password synchronization

Installing the One Identity Quick Connect for Mainframes (CA Top Secret®) Connector software

This section describes how to install the CA Top Secret® Connector on Windows Server® 2008 or above, or on an existing installation of One Identity Quick Connect.

To install One Identity Quick Connect for Mainframes (Top Secret) connector software

1. To start the installation for:
    a. 32-bit systems; double click the **QuickConnectForMainframes(TOPS)_x86.msi** installation routine.

b. 64-bit systems; double click the **QuickConnectForMainframes(TOPS_x64.msi** installation routine.

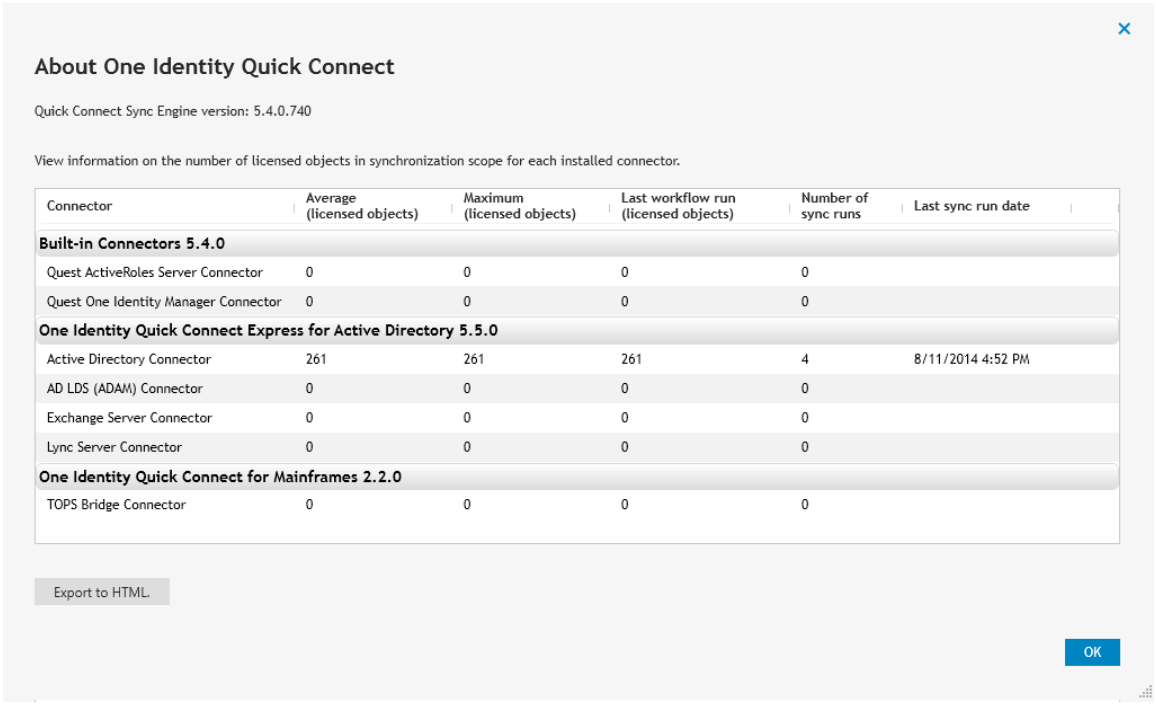
2. The **Welcome Wizard** starts. Click **Next**.
3. Read the license agreement, select the **I accept the terms in the License Agreement** box, and then click **Next**.
4. Enter your name and organization.
5. Click **Next**.
6. Click **Install**.

The files will be copied to your system. On completion of the installation, you will be prompted to restart your One Identity Quick Connect Service.

Verifying the Connector installation

To verify the CA Top Secret® Connector installation, click the information icon in the top right-hand corner of the Quick Connect Console. The **About Quick Connect** screen is displayed. If the installation was successful, the Top Secret Connector is included in the list of installed connectors.

Figure 1: About Quick Connect

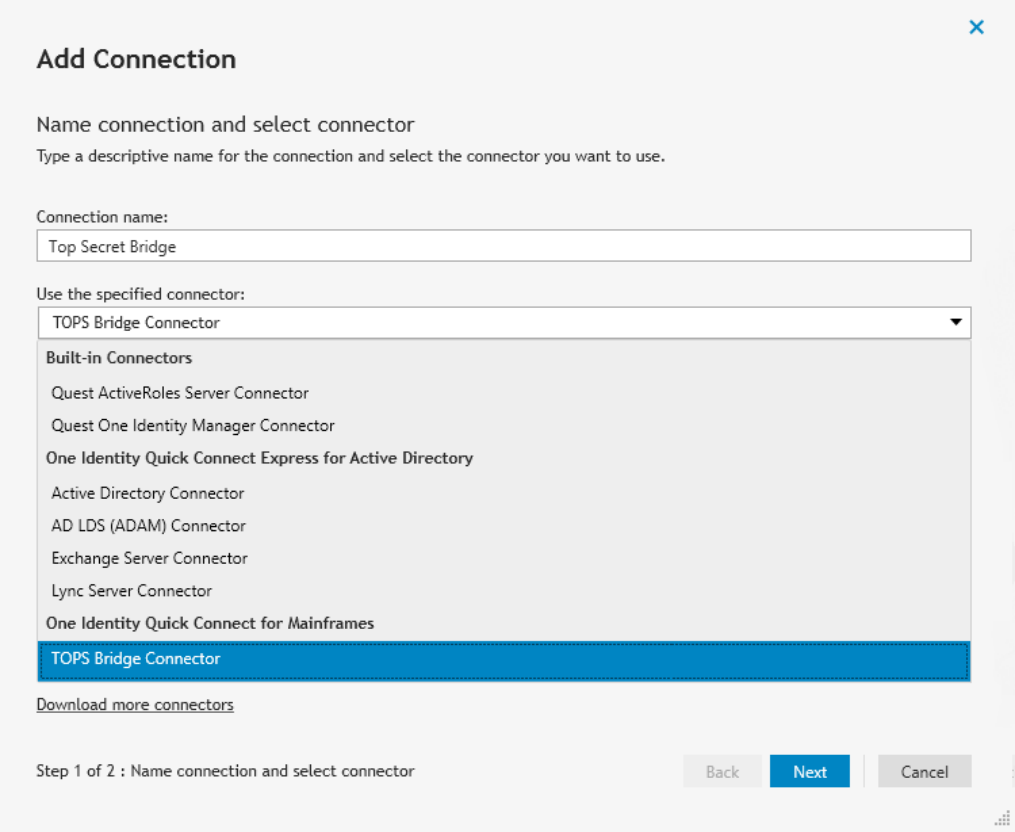


Adding a new CA Top Secret® Connector

The Quick Connect Sync Engine provides an Add Connected System wizard. The wizard adds a specific external data source to the One Identity Quick Connect environment, and configures a connection to that connected data system. You can manually start the wizard using the following procedure:

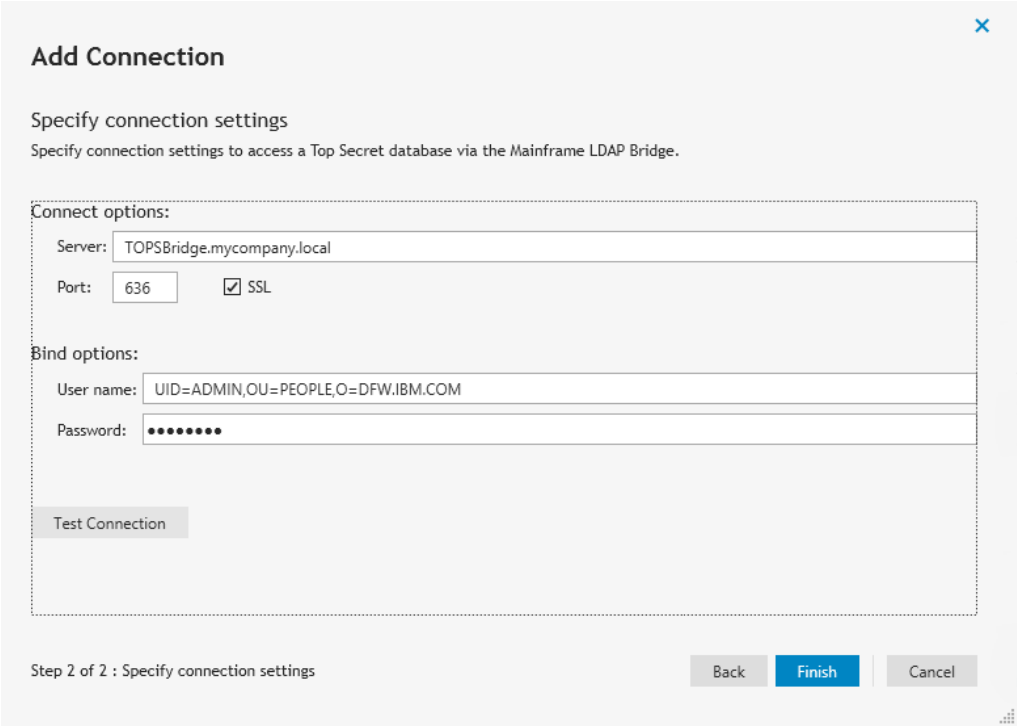
To start the Add Connected System wizard

1. In the **Quick Connect Administration Console**, select **Connections**.
2. Click the **Add Connection** link. The **Name connection and select connector** page is displayed, as shown below.



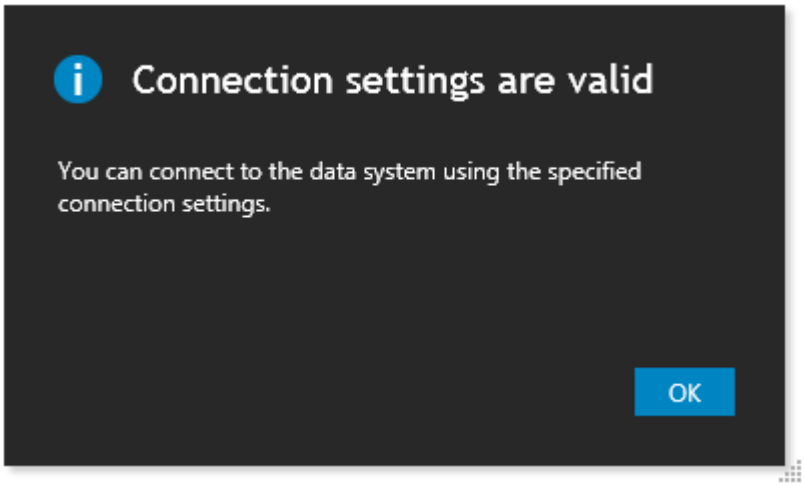
3. Enter a **Connection name**.
4. In the **Use the specified connector** field, choose the **Rocket TOPS Connector** from the drop down list, and click **Next**.
5. On the **Specify connection settings** page, specify the CA Top Secret® LDAP service to connect to and the account that the application will use to access the Top Secret LDAP service.

   The **Specify connection settings** page is similar to the following example.

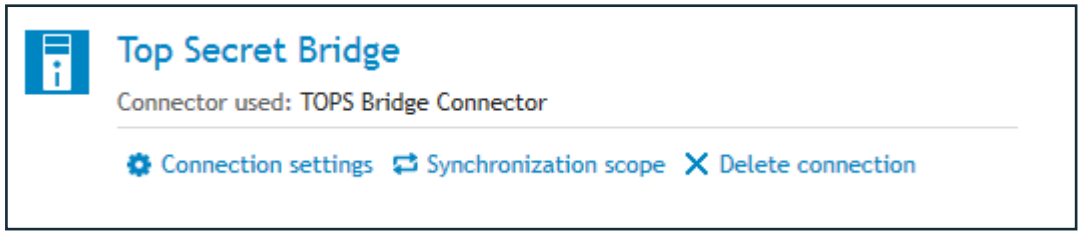


To specify connection settings to access a Top Secret LDAP directory service

1. Open the **Specify connection settings** page.
2. In the **Server** field, type the fully qualified DNS name of the IBM RACF® server running the LDAP service.
3. In the **Port** field, type the Top Secret LDAP communication port number in use by the service. (The default port numbers are 389 for non SSL and 636 for SSL encrypted data).
4. In the **User name** field, specify the fully distinguished name (DN) of the account that the application will use to access the Top Secret LDAP directory service. In the **Password** field, specify the password of the user account that the application will use to access the Top Secret LDAP directory service.
5. Optionally, click **Test Connection** to verify that the credentials provided can access the Top Secret LDAP service.



6. Click **Finish**.
7. The connection should appear in the list of available connections with the Top Secret icon:



NOTE: Consider the following restrictions imposed by Top Secret:

- The maximum length of the values you specify for user name (saved in the Top Secret attribute uid), user password (saved in the Top Secret attribute tssPassword), and group name (saved in the Top Secret® attribute uid) cannot exceed 8 characters.
- Values of the attributes that identify objects in Top Secret cannot include any of these characters: , = + < > # ; \ " SPACE
- To create objects in Top Secret (for example, when provisioning objects from the managed Active Directory® domain to Top Secret), you must specify an existing department ID (saved in the Top Secret attribute **tssDeptAcid**) for the objects being created.

Modifying an existing connection to CA Top Secret®

To modify connection settings

1. In the **Quick Connect Administration Console**, open the **Connections** tab.
2. Click **Connection settings** below the existing CA Top Secret® connection you want to modify.
3. Expand **Specify connection settings** and use the following options to modify the settings:
    a. **Server** - Specify the fully qualified domain name (FQDN) of the computer running the LDAP Bridge that provides access to the Top Secret system.
    b. **Port** - Specify the number of the LDAP communication port used by the LDAP Bridge. For more information, see the Quick Connect for Mainframes (bridge) PDF document supplied with the Quick Connect for Mainframes package.
    c. **Access Quest One Quick Connect for Mainframes (bridge) using** - Specify the user name and password with which you want to access the LDAP Bridge.
    d. **Advanced** - Click to specify additional connection options.
    e. **Test Connection** - Click to verify the connection settings you have specified.
4. Click **Save**.

Configuring CA Top Secret® Connector attributes

The following attributes have been verified for one-way synchronization from Active Directory® and CA Top Secret® in addition to the password synchronization attribute. Other attributes can be synchronized by Quick Connect as long as the attribute types are maintained between platforms.

Table 1: CA Top Secret Connector attributes

Type of attribute	Active Directory attribute	Top Secret attribute
User	sAMAccountName	uid

Creating a workflow

Workflows are designed in three key areas:

- Provision
- Update
- Deprovision

Provision – creates objects in the target connected data systems based on the changes made to specific objects in the source connected system. When creating a new object, One Identity Quick Connect assigns initial values to the object attributes based on the attribute population rules you have configured.

Update – changes the attributes of objects in the target connected data systems based on the changes made to specific objects in the source connected system. To define the objects that will participate in the update operation you can use object mapping rules.

Deprovision – modifies or removes objects in the target connected data systems after their counterparts have been disconnected from the source connected system. One Identity Quick Connect can be configured to remove objects permanently or change them to a specific state.

Example – creating a workflow

This example demonstrates how to create a workflow from Active Directory® to CA Top Secret®.

Provisioning (users)

To synchronize the Active Directory® users to Top Secret

1. Navigate to the **Workflow** tab.
2. Click Add synchronization.
3. Click **Provision**, and then **Next**.
4. From the **Source connected system** section, click **Specify**…
5. A new Wizard starts.
6. Select your Active Directory connector and click **Finish**.
7. The **Source object type**: is currently set to **User (user)**. Do not change this value.
8. Specify any **Provisioning Criteria** (for example only members of a specific OU are synchronized).
9. Click **Next**.

10. In the **Target connected system** field, click **Specify**…, then locate your Top Secret connector and click **Finish**.
11. The **object type** in the **Target object system** field should be set to **tssUser**.
    a. The **Target Container** should be set to **People**.
    b. In the **Rules to generate a unique object name** section select **Attribute**. Then select the **SAMAccountName** attribute.
    c. Click **OK**.
12. Click **Next**.
13. In the **Initial Attribute Population Rules** section, click **Forward Sync Rule...**
14. In the **Source item** field, click **Attribute**…, locate **sAMAccountName** and click **OK**.
15. In the **Target item** field, click **Attribute** then Select **uid** and click **OK**.
16. Click **OK** again.
    a. Click **Forward Sync Rule...** again.
    b. In the **source item** section, click on the drop down box and select **Text...**
    c. In the **source item** box, enter the name of your **Department Name** (for example, SYSDEPT).
    d. In the **Target item** field, click on **Attribute...** and select **tssDeptAcid**
    e. Click **OK**.
17. Specify an initial password for the newly created users (this is mandatory for Top Secret).
18. Click **Finish** to complete this synchronization step.

When you have successfully completed the steps in Creating a workflow, all new users in your Active Directory system will be synchronized through One Identity Quick Connect to Top Secret.

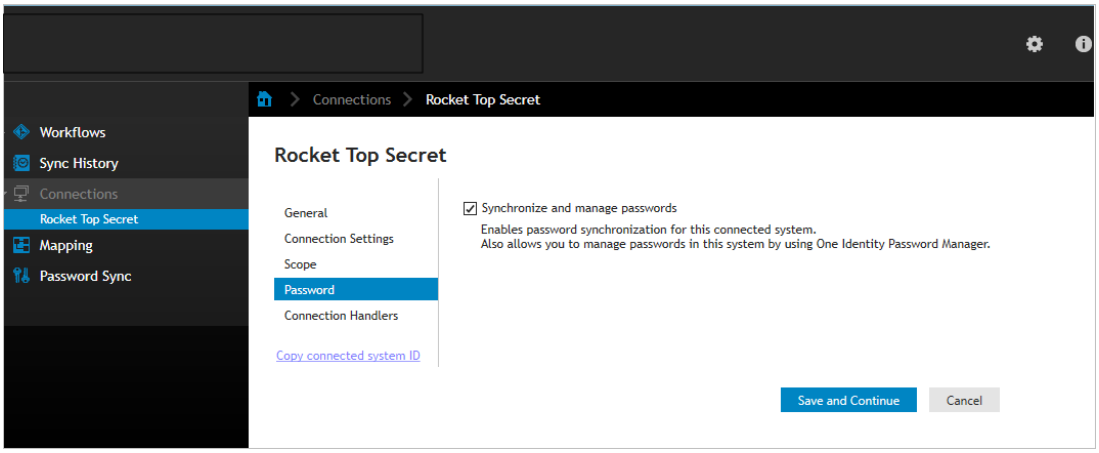
Configuring CA Top Secret® password synchronization

Passwords are only captured from Active Directory® when the Quick Connect capture module is installed.

To enable password synchronization from Active Directory® to CA Top Secret®

1. Navigate to the **Quick Connect Administration Console**.
2. Select the **Connections** tab.
3. In the **Connected systems** section, select the required system.

4. Select the **Password** tab.
5. Click **Synchronize and manage passwords**.



How to install and configure the CA ACF2™ Connector

The CA ACF2™ Connector is distributed in a standard Microsoft® MSI format which contains the required files to install and configure the ACF2 Connector in an existing One Identity Quick Connect environment.

The following sections describe:

- Installing the One Identity Quick Connect for CA ACF2™ Connector software
- Adding a new CA ACF2™ Connector
- Modifying an existing connection to CA ACF2™
- Configuring CA ACF2™ Connector attributes
- Creating a workflow
- Configuring CA ACF2™ password synchronization

Installing the One Identity Quick Connect for CA ACF2™ Connector software

This section describes how to install the CA ACF2™ Connector on Windows Server® 2008 or above, or on an existing installation of One Identity Quick Connect.

To install One Identity Quick Connect for ACF2 connector software

1. To start the installation for:
    a. 32-bit systems; double click the **QuickConnectForMainframes(ACF2)_ x86.msi** installation routine.
    b. 64-bit systems; double click the **QuickConnectFor Mainframes(ACF2)_ x64.msi** installation routine.
2. The **Welcome Wizard** starts. Click **Next**.

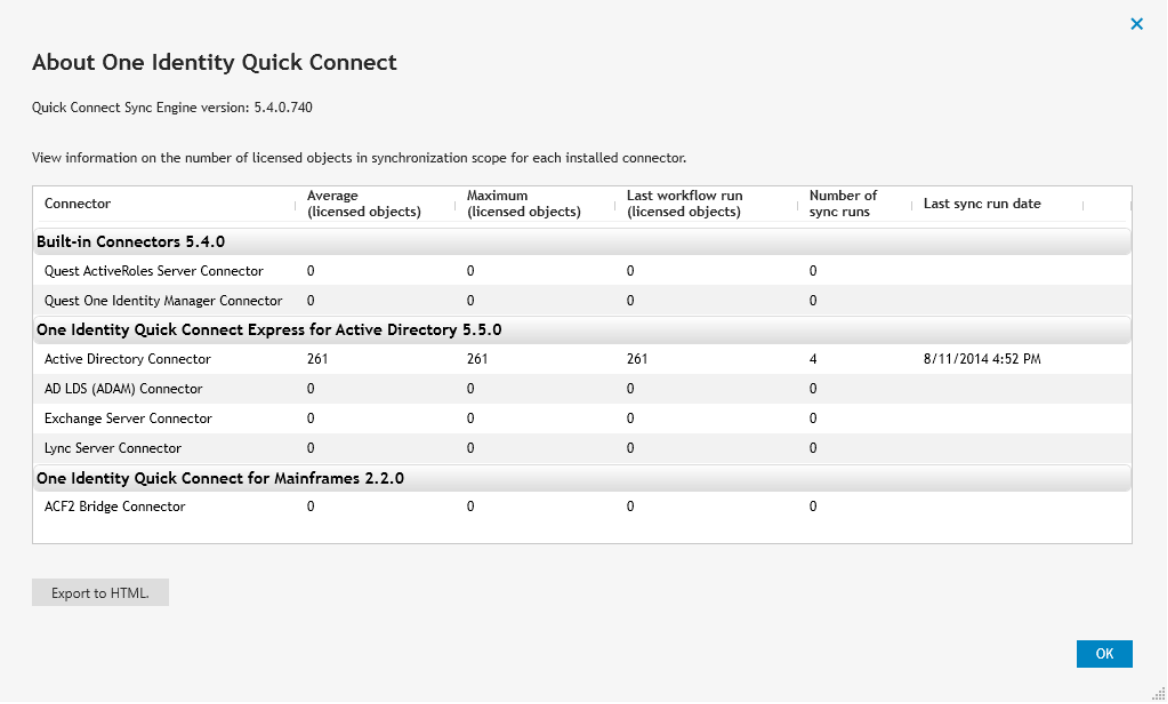
3. **Read the license agreement, select the I accept the terms in the License Agreement** box, and then click Next.
4. Enter your name and organization.
5. Click **Next**.
6. Click **Install**.

The files will be copied to your system. On completion of the installation, you will be prompted to restart your One Identity Quick Connect Service.

Verifying the Connector installation

To verify the CA ACF2™ Connector installation, click the information icon in the top right-hand corner of the Quick Connect Console. The **About Quick Connect** screen is displayed. If the installation was successful, the CA ACF2™ Connector is included in the list of installed connectors.

Figure 2: About Quick Connect



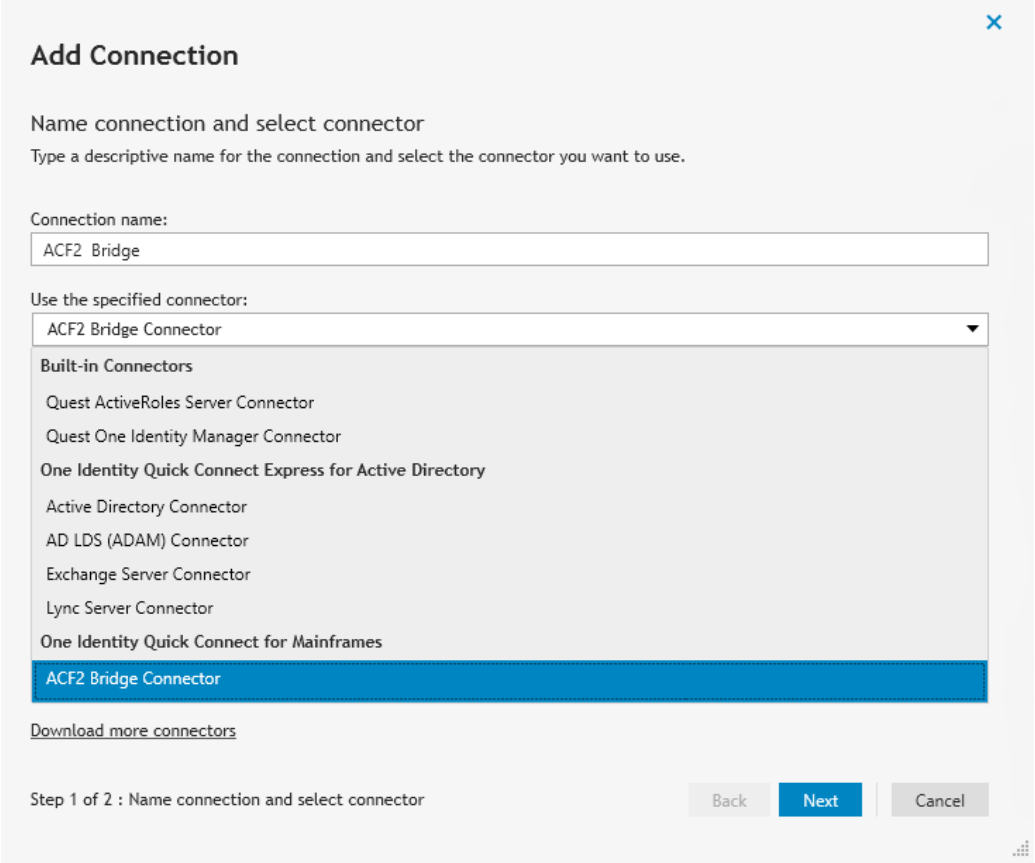
Adding a new CA ACF2™ Connector

The Quick Connect Sync Engine provides an **Add Connected System** wizard. The wizard adds a specific external data source to the One Identity Quick Connect environment, and

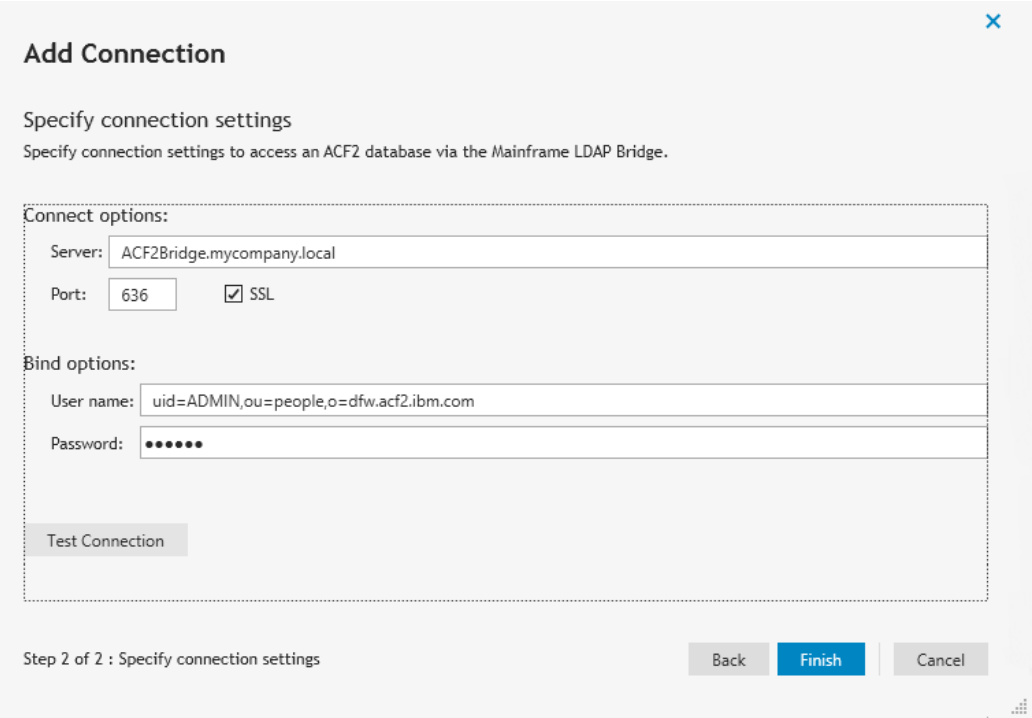
configures a connection to that connected data system. You can manually start the wizard using the following procedure:

To start the Add Connected System wizard

1. In the **Quick Connect Administration Console**, select **Connections**.
2. Click the **Add Connection** link. The **Name connection and select connector** page is displayed, as shown below.

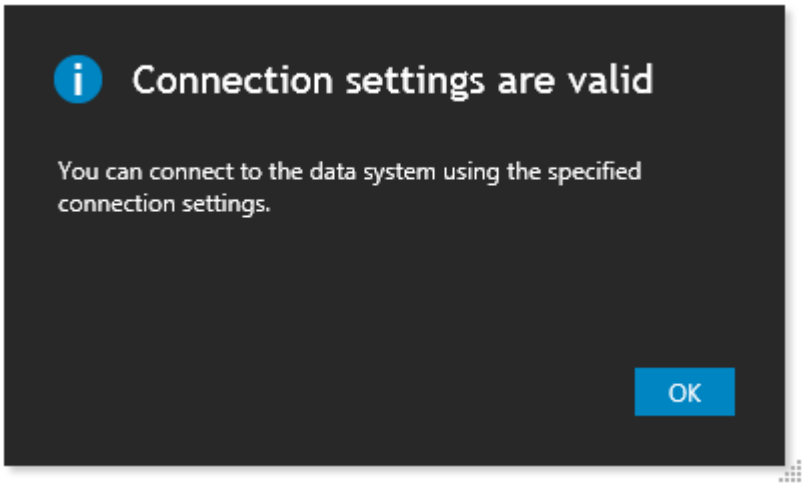


The **Specify connection settings** page is similar to the following example.

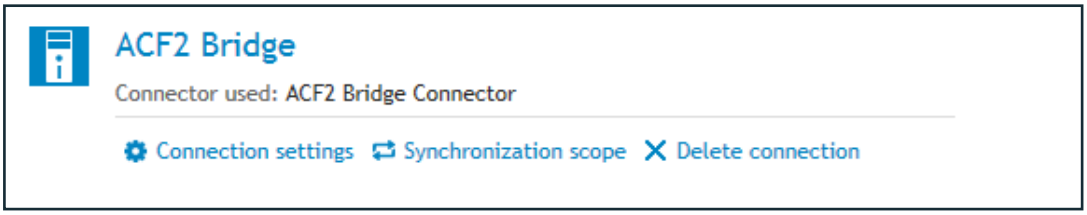


To specify connection settings to access a ACF2 LDAP directory service

1. Open the **Specify connection settings** for ACF2 page.
2. In the **Server** field, type the fully qualified DNS name of the ACF2 server running the LDAP service.
3. In the **Port** field, type the ACF2 LDAP communication port number in use by the service. (The default port numbers are 389 for non SSL and 636 for SSL encrypted data).
4. In the **User name** field, specify the fully distinguished name (DN) of the account that the application will use to access the ACF2 LDAP directory service. In the **Password** field, specify the password of the user account that the application will use to access the ACF2 LDAP directory service.
5. Optionally, click **Test Connection** to verify that the credentials provided can access the ACF2 LDAP service.



6. Click **Finish**.
7. The connection should appear in the list of available connections with the ACF2 icon:



NOTE: Consider the following restrictions imposed by ACF2:

- The maximum length of the values you specify for user name (saved in the ACF2 attribute uid) and user password (saved in the ACF2 attribute **acf2Password**) cannot exceed 8 characters.
- Values of the attributes that identify objects in ACF2 cannot include any of these characters: , = + < > # ; \ " SPACE

Modifying an existing connection to CA ACF2™

To modify connection settings

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Connection settings** below the existing CA ACF2™ connection you want to modify.
3. Expand **Specify connection settings** and use the following options to modify the settings:

a. **Server** - Specify the fully qualified domain name (FQDN) of the computer running the LDAP Bridge that provides access to the ACF2 system.

b. **Port** - Specify the number of the LDAP communication port used by the LDAP Bridge. For more information, see the Quick Connect for Mainframes (bridge) PDF document supplied with the Quick Connect for Mainframes package.

c. **Access One Identity Quick Connect for Mainframes (bridge) using** - Specify the user name and password with which you want to access the LDAP Bridge.

d. **Advanced** - Click to specify additional connection options.

e. **Test Connection** - Click to verify the connection settings you have specified.

4. Click **Save**.

Configuring CA ACF2™ Connector attributes

The following attributes have been verified for one-way synchronization from Active Directory® and CA ACF2™ in addition to the password synchronization attribute. Other attributes can be synchronized by Quick Connect as long as the attribute types are maintained between platforms.

Table 2: CA ACF2 Connector attributes

Type of attribute	Active Directory attribute	ACF2 attribute
User	sAMAccountName	uid

Creating a workflow

Workflows are designed in three key areas:

- Provision
- Update
- Deprovision

Provision – creates objects in the target connected data systems based on the changes made to specific objects in the source connected system. When creating a new object, One Identity Quick Connect assigns initial values to the object attributes based on the attribute population rules you have configured.

Update – changes the attributes of objects in the target connected data systems based on the changes made to specific objects in the source connected system. To define the objects that will participate in the update operation you can use object mapping rules.

Deprovision – modifies or removes objects in the target connected data systems after their counterparts have been disconnected from the source connected system. One Identity Quick Connect can be configured to remove objects permanently or change them to a specific state.

Example – creating a workflow

This example demonstrates how to create a workflow from Active Directory® to CA ACF2®.

Provisioning (users)

To synchronize Active Directory® groups to ACF2

1. Navigate to the **Workflows** tab on the main menu.
2. Click **Add workflow**.
3. Enter a description for your workflow, for example **Sync Active Directory to ACF2** and click **OK**.
4. Click the **Sync Active Directory to ACF2 workflow step** hyperlink.
5. Click **Add synchronization step**.
6. Click **Provision**, and then **Next**.
7. From the **Source connected system** section, click **Specify**…
8. A new wizard starts.
9. Select your Active Directory connector and click **Finish**.
10. The **Source object type:** is currently set to **User (user)**. Do not change this **value**.
11. Specify any **Specific Provision Criteria** (for example only members of a specific OU are synchronized).
12. Click **Next**.
13. In the **Target connected system** field, click **Specify**…, then locate your ACF2 connector and click **Finish**.
14. The object type in the Target object system field should be set to **acf2person**.
    a. In the target **Containers:** section click on **Browse...**
    b. Select the container called **people**.
    c. Click **OK**.
    d. In the **Rules to generate unique object name** click on **Attribute...**
    e. Select the **SAMAccountname** attribute.
    f. Click **OK**.
15. Click **Next**.

16. In the Initial **Attribute Population Rules** section, click **Forward Sync Rule...**
17. In the **Source item** field, click **Attribute...**, locate **sAMAccountName** and click **OK**.
18. In the **Target item** field, click **Attribute...**, then locate **uid** and click **OK**.
19. Specify an initial password for the newly created users (this step is mandatory).
20. Click **Finish** to complete this synchronization step.

When you have successfully completed the steps in Creating a workflow, all new users or groups in your Active Directory system will be synchronized through One Identity Quick Connect to ACF2.

Deprovisioning (users)

To deprovision users

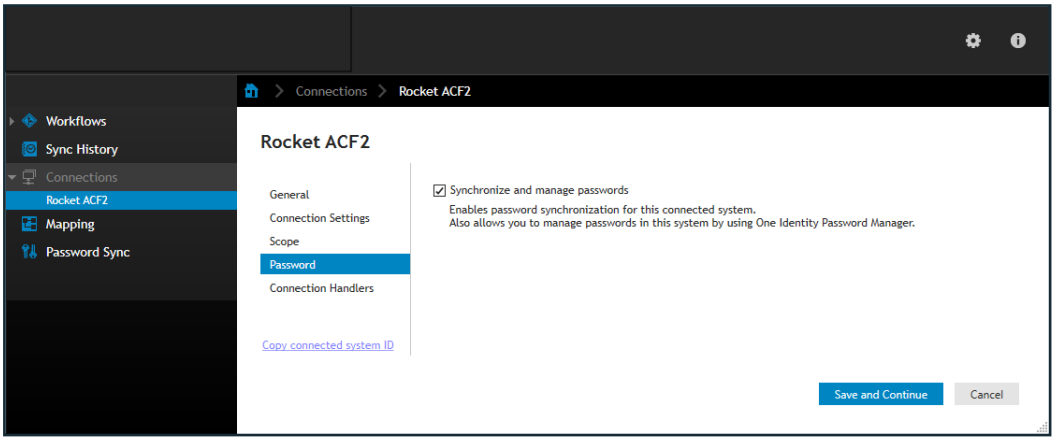
1. Navigate to the **Workflow** tab.
2. Click **Add synchronization** step.
3. Click **Deprovision**, and then **Next**.
4. In the **Source connected system section**, click **Specify**…
5. Select your **Active Directory Connector** and click **Finish**.
6. Verify the **Source object type** is set to **user**.
7. In the **Deprovision target if: section, select the Source object is deleted or is out of synchronization scope check box.**
8. Alternatively, configure the **Source object meets the following criteria** if required.
9. Click **Next**.
10. In the **Target connected system:** field, click **Specify...**.
11. Locate your ACF2 connector and complete the steps in the wizard.
12. The **Target object type** will be prefilled automatically to acf2person.
13. Click **Next**.
14. Select **Delete target object**.
15. Click **Finish** to complete this synchronization step.

Configuring CA ACF2™ password synchronization

Passwords are only captured from Active Directory® when the Quick Connect capture module is installed.

To enable password synchronization from Active Directory® to CA ACF2™

1. Navigate to the **Quick Connect Administration** Console.
2. Select the **Connections** tab.
3. In the **Connected systems** section, select the required system.
4. Select the **Password** tab.
5. Click **Synchronize and manage passwords**.



4

How to install and configure the Quick Connect for Mainframes (IBM RACF®) Bridge Connector

The IBM RACF® Connector is distributed in a standard Microsoft® MSI format which contains the required files to install and configure the RACF Connector in an existing One Identity Quick Connect environment.

The following sections describe:

- Installing the One Identity Quick Connect for IBM RACF® Connector software
- Adding a new IBM RACF® Connector
- Modifying an existing connection to IBM RACF®
- Configuring IBM RACF® Connector attributes
- Creating a workflow
- Configuring IBM RACF® password synchronization

Installing the One Identity Quick Connect for Mainframes (IBM RACF®) Connector software

This section describes how to install the IBM RACF® Connector on Windows Server 2008® or above, or on an existing installation of One Identity Quick Connect.

To install One Identity Quick Connect for Mainframes (RACF) connector software

1. To start the installation for:
    a. 32-bit systems; double click the **QuickConnectForMainframes(RACF)_x86.msi** installation routine.

b. 64-bit systems; double click the **QuickConnectForMainframes(RACF)_x64.msi** installation routine.

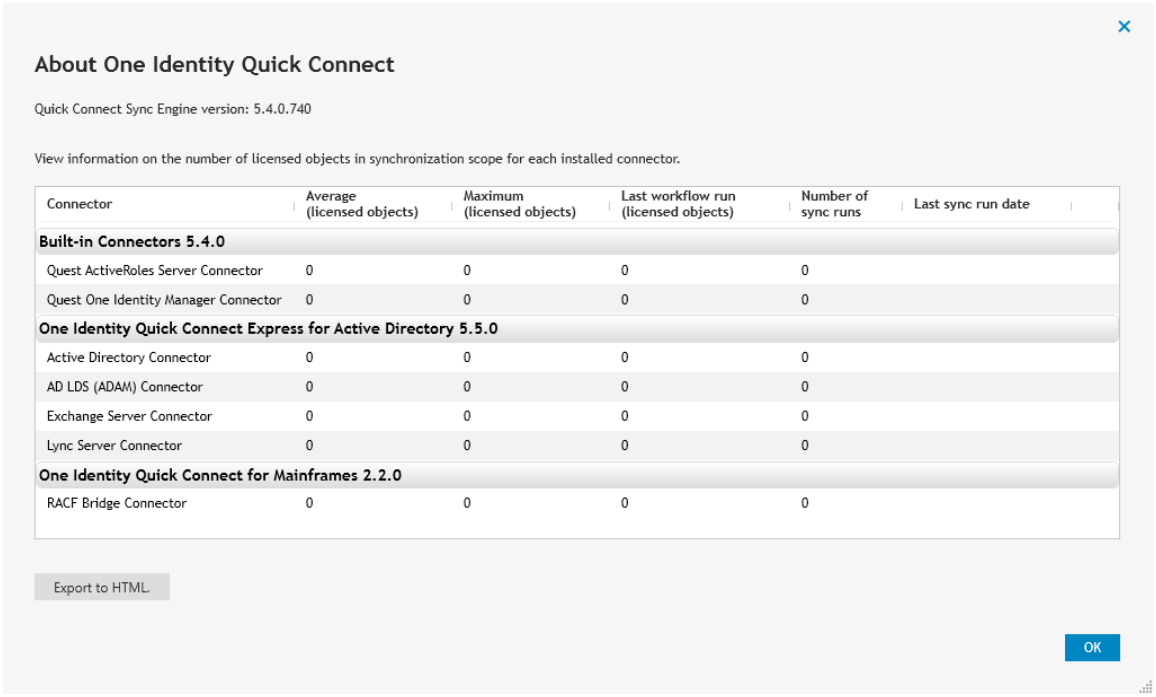
2. The **Welcome Wizard** starts. Click **Next**.
3. Read the license agreement, select the **I accept the terms in the License Agreement** box, and then click **Next**.
4. Enter your name and organization.
5. Click **Next**.
6. Click **Install**.

The files will be copied to your system. On completion of the installation, you will be prompted to restart your One Identity Quick Connect Service.

Verifying the Connector installation

To verify the Quick Connect for Mainframe Connector installation, click the information icon in the top right-hand corner of the Quick Connect Console. The **About Quick Connect** screen is displayed. If the installation was successful, the IBM RACF® Connector is included in the list of installed connectors.

Figure 3: About Quick Connect

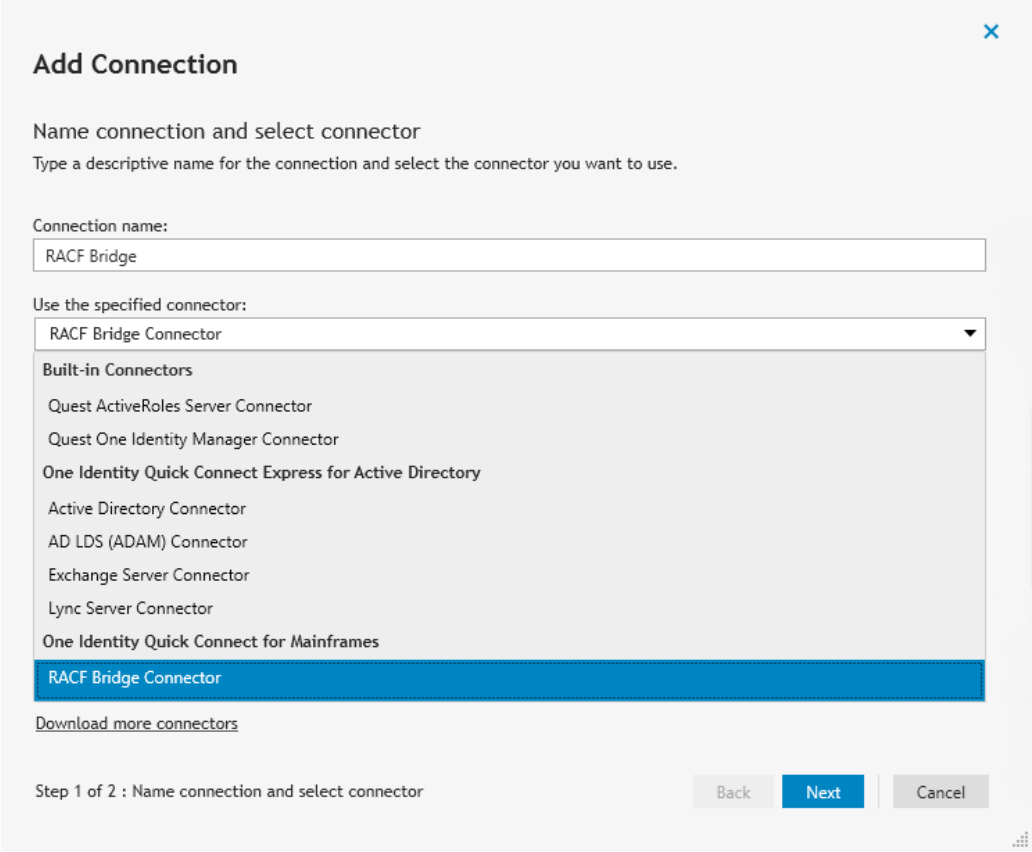


Adding a new IBM RACF® Connector

The Quick Connect Sync Engine provides an Add Connected System wizard. The wizard adds a specific external data source to the One Identity Quick Connect environment, and configures a connection to that connected data system. You can manually start the wizard using the following procedure:

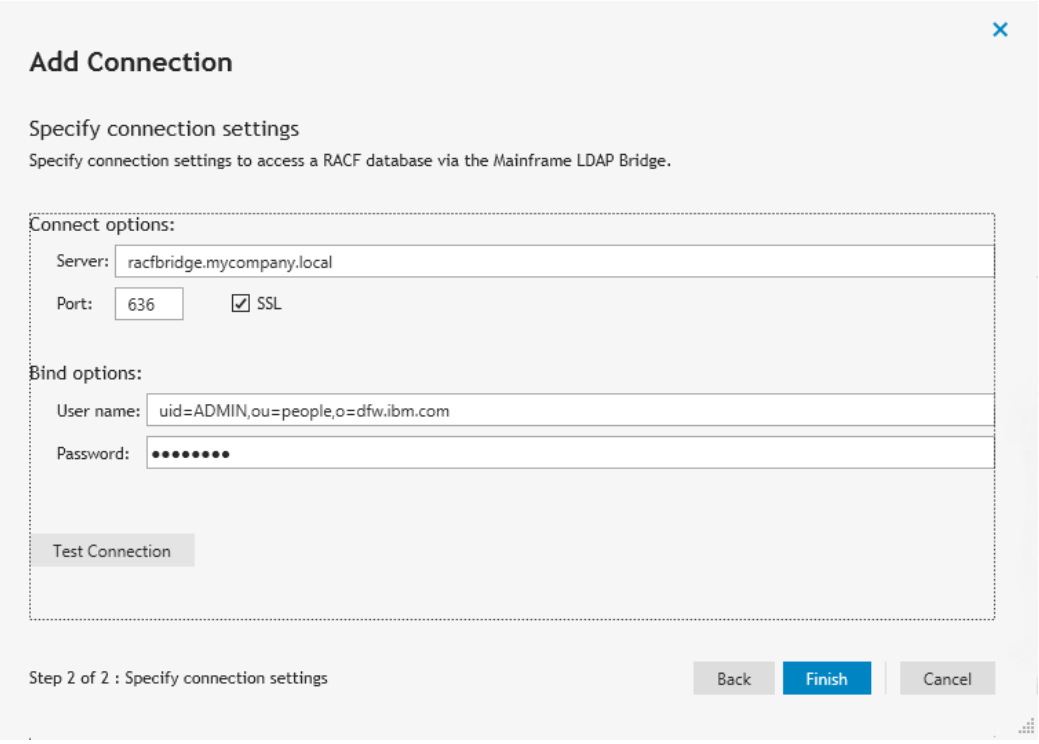
To start the Add Connected System wizard

1. In the Quick Connect Administration Console, select **Connections**.
2. Click the **Add connection** link. The **Name connection and select connector** page is displayed, as shown below.



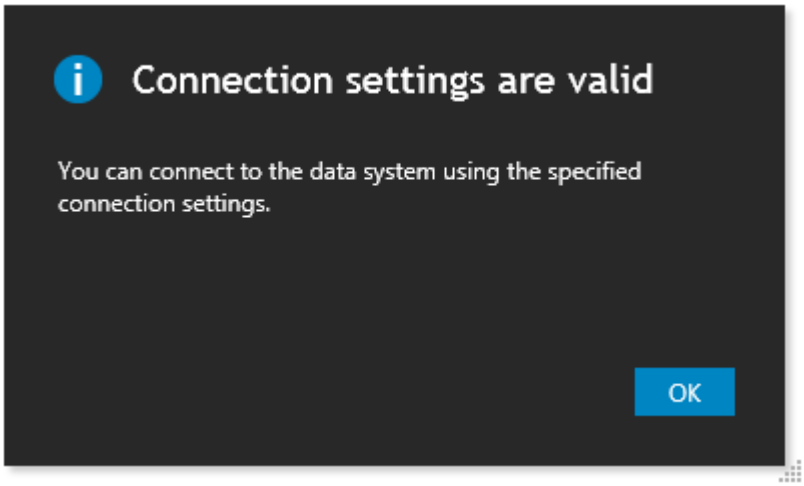
3. Enter a **Connection name**.
4. In the **Use the specified connector** field, choose the IBM RACF® Connector from the drop down list, and click **Next**.
5. On the **Specify connection settings** page, specify the Bridge LDAP service to connect to and the account that the application will use to access the Bridge LDAP service.

   The **Specify connection settings** page is similar to the following example.

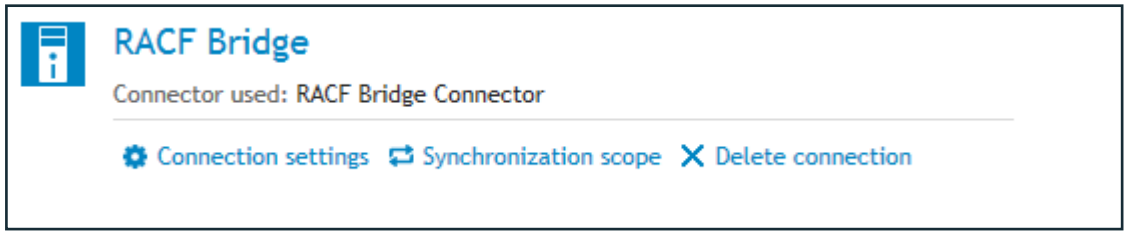


To specify connection settings to access a RACF LDAP directory service

1. Open the **Specify connection settings** for RACF page.
2. In the **Server** field, type the fully qualified DNS name of the server running the LDAP bridge that provides access to the RACF system.
3. In the **Port** field, type the communication port number in use by the service. (The default port numbers are 389 for non SSL and 636 for SSL encrypted data).
4. In the **User name** field, specify the fully distinguished name (DN) of the account that the application will use to access the RACF LDAP directory service. In the **Password** field, specify the password of the user account that the application will use to access the RACF LDAP directory service.
5. Optionally, click **Test Connection** to verify that the credentials provided can access the RACF LDAP service.



6. Click **Finish**.
7. The connection should appear in the list of available connections with the RACF icon:



NOTE: Consider the following restrictions imposed by RACF:

- The maximum length of the values you specify for user name (saved in the RACF attribute uid), user password (saved in the RACF attribute **racfPassword**), and group name (saved in the RACF attribute cn) cannot exceed 8 characters.
- Values of the attributes that identify objects in RACF cannot include any of these characters: , = + < > # ; \ " SPACE

Modifying an existing connection to IBM RACF®

To modify connection settings

1. In the **Quick Connect Administration Console**, open the **Connections** tab.
2. Click **Connection settings** below the existing IBM RACF® connection you want to modify.
3. Expand **Specify connection settings** and use the following options to modify the settings:

a. **Server** - Specify the fully qualified domain name (FQDN) of the computer running the LDAP Bridge that provides access to the RACF system.

b. **Port** - Specify the number of the LDAP communication port used by the LDAP Bridge. For more information, see the Quick Connect for Mainframes (bridge) PDF document supplied with the Quick Connect for Mainframes package.

c. **Username and password** - Specify the user name and password with which you want to access the LDAP Bridge.

d. **Test Connection** - Click to verify the connection settings you have specified.

4. Click **Save**.

Configuring IBM RACF® Connector attributes

The following attributes have been verified for one-way synchronization from Active Directory® to IBM RACF® in addition to the password synchronization attribute. Other attributes can be synchronized by Quick Connect as long as the attribute types are maintained between platforms.

Table 3: IBM RACF Connector attributes

Type of attribute	Active Directory attribute	RACF attribute
User	sAMAccountName	uid
Group	sAMAccountName	cn
Group	member	member

Creating a workflow

Workflows are designed in three key areas:

- Provision
- Update
- Deprovision

Provision – creates objects in the target connected data systems based on the changes made to specific objects in the source connected system. When creating a new object, One Identity Quick Connect assigns initial values to the object attributes based on the attribute population rules you have configured.

Update – changes the attributes of objects in the target connected data systems based on the changes made to specific objects in the source connected system. To define the objects that will participate in the update operation you can use object mapping rules.

Deprovision – modifies or removes objects in the target connected data systems after their counterparts have been disconnected from the source connected system. One Identity Quick Connect can be configured to remove objects permanently or change them to a specific state.

Example – creating a workflow

This example demonstrates how to create a workflow from Active Directory® to IBM RACF® using the RACF LDAP Bridge.

Provisioning (groups)

To synchronize Active Directory® groups to RACF

1. Navigate to the **Workflows** tab on the main menu.
2. Click **Add workflow**.
3. Enter a description for your workflow, for example **Sync Active Directory to RACF**, and click **OK**.
4. Click the **Sync Active Directory to RACF workflow step** hyperlink.
5. Click **Add synchronization step**.
6. Click **Provision** and then click **Next**.
7. From the **Source connected system** section, click **Specify**…
8. A new wizard starts.
9. Select your Active Directory connection and click **Finish**.
10. The **Active Directory source** object type: should be set to Group (group).
11. Specify any **Provisioning Criteria** (for example only members of a specific OU are synchronized).
12. Click **Next**.
13. In the **Target connected system:** field, click **Specify...** then locate your RACF connector and click **Finish**.
14. The **Target** object type in the Connected System should be set to racfGroup.
    a. In the **Target container:** section, click **Browse...**
    b. Select the container called groups and click **OK**.

c. In the **Rules to generate unique object name** section click on **Attribute...**

d. Select **sAMAccountName** and click **OK.**

15. Click **Next**.
16. In the **Specify provisioning rules** section, click **Forward Sync Rule...**
17. In the **Source item:** field, click **Attribute...**, locate **sAMAccountName** and click **OK**.
18. In the **Target item:** field, click **Attribute...**, then **Select**, locate **cn** and click **OK**.
19. Click **Finish** to complete this synchronization step.

Provisioning (users)

To synchronize the Active Directory® users to RACF using the RACF LDAP Bridge

1. Navigate to the **Workflow** tab.
2. Click **Add synchronization**.
3. Click **Provision**, and then **Next**.
4. From the **Source connected system:** section, click **Specify...**
5. A new wizard starts.
6. Select your Active Directory connector and click **Finish**.
7. **The Source object type:** is currently set to **User (user)**. Do not change this value.
8. Specify any **Provisioning Criteria** (for example only members of a specific OU are synchronized).
9. Click **Next**.
10. In the Target connected system: field, click **Specify...**, then locate your RACF connector and click **Finish**.
11. The **object type** in the **Target object system** field should be set to **racfUser**.
    a. In the **Target Container:** section, click **Browse...**
    b. Select the container called **people,** and click **OK.**
    c. In the **Rules to generate unique object name** section click on **Attribute...**
    d. Select **sAMAccountName** and click **OK.**
12. Click **Next**.
13. In the **Specify provisioning rules** section, click **Forward Sync Rule...**
14. In the Source: field, click **Attribute**, locate **sAMAccountName** and click **OK**.
15. In the **Target item:** field, click **Attribute**, locate **uid** and click **OK**.
16. Specify an initial password for the newly created users (this step is mandatory).
17. Click **Finish** to complete this synchronization step.

When you have successfully completed the steps in Creating a workflow, all new users or groups in your Active Directory system will be synchronized through One Identity Quick Connect to RACF.

Updating (groups)

To synchronize users Active Directory® attribute(s) group membership to RACF

1. Navigate to the **Sync Active Directory to RACF workflow**.
2. Click **Add synchronization step**.
3. Click **Update**, and then click **Next**.
4. From the **Source connected system** section, click **Specify...**
5. A new wizard starts.
6. Select your Active Directory Connector and click **Finish**.
7. The **Source object type:** is currently set to **User (user)**. Change this to **Group (group)**.
8. Specify any **Updating Criteria** (for example, only members of an OU are synchronized).
9. Click **Next**.
10. In the **Target connected system:** field, click **Specify...**, and then locate your RACF connector.
11. Click **Finish**.
12. The **Target object type** should be set to **racfGroup**.
13. Click **Next**.
14. In the **Specify updating rules** section, click **Forward Sync Rule...**
15. A new **Forward Sync Rule...** screen is displayed. In the **Source item:** field, click **Attribute...**, locate member and click **OK**.
16. Set the **Target item:** field to **member**.
17. Click **OK**.
18. Click **Finish** to complete this synchronization step.

On successful completion of these update steps, any modifications to your existing users or groups will be synchronized with your RACF database.

Deprovisioning (users)

To deprovision users

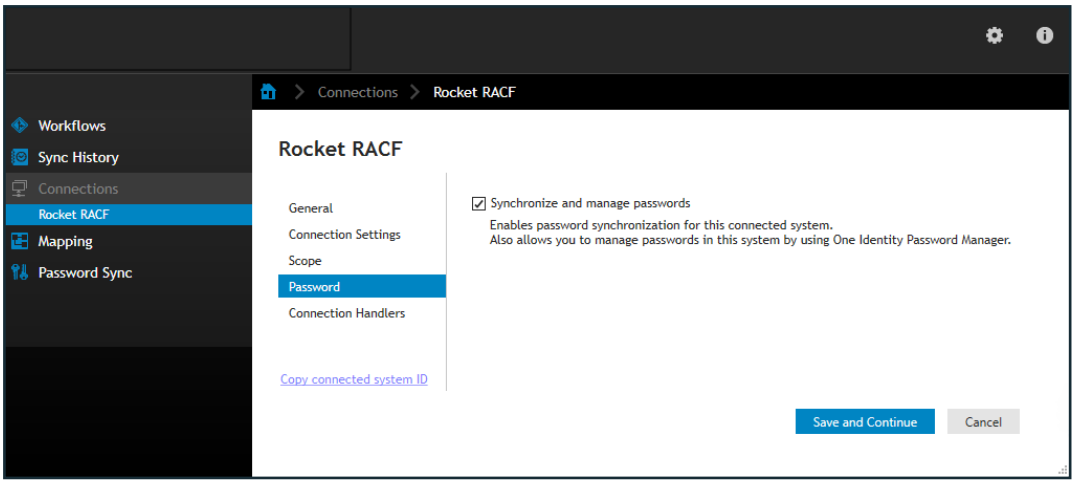
1. Navigate to the **Sync Active Directory to RACF workflow**.
2. Click **Add synchronization step**.
3. Click **Deprovision**, and then **Next**.
4. In the **Source connected system** section, click **Specify...**
5. Select your **Active Directory Connector** and click **Finish**.
6. Verify the **Source object type** is set to **user**.
7. In the **Deprovision target if:** section, select the **Source object is deleted or is out of synchronization scope** check box.
8. Alternatively, configure the **Source object meets these criteria** if required.
9. Click **Next**.
10. In the **Target connected system:** field, click **Specify...**.
11. Locate your RACF connector and click **Finish**.
12. The Target object type should be changed to **racfUser**.
13. Click **Next**.
14. Select **Delete target objects**.
15. Click **Finish** to complete this synchronization step.

Configuring IBM RACF® password synchronization

Passwords are only captured from Active Directory® when the Quick Connect capture module is installed.

To enable password synchronization from Active Directory® to IBM RACF® using the RACF LDAP Bridge

1. Navigate to the **Quick Connect Administration Console**.
2. Select the **Connections** tab.
3. In the **Connected systems** section, select the required system.
4. Select the **Password** tab.
5. Click **Synchronize and manage passwords**.


Connections
Rocket RACF
Workflows
Sync History
Connections
Rocket RACF
Mapping
Password Sync
Rocket RACF
General
Connection Settings
Scope
Password
Connection Handlers
Copy connected system ID
Synchronize and manage passwords
Enables password synchronization for this connected system.
Also allows you to manage passwords in this system by using One Identity Password Manager.
Save and Continue
Cancel

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product