One Identity Quick Connect for IBM RACF 1.3

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 IBM RACF Installation and Configuration Guide
Updated - October 2017
Version - 1.3

Contents

Installing and Configuring One Identity Quick Connect for IBM RACF®

This document describes how to install, create and configure the IBM RACF® Connector into an existing One Identity Quick Connect system.

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

Pre-requisites

Ensure that the following installation pre-requisites are met before installing One Identity Quick Connect for IBM RACF®:

- Quick Connect Sync Engine version 5.5 must be fully installed and functional.
- The IBM mainframe must have LDAP directory services installed and configured.
- An LDAP service account must be created on your RACF server which has the appropriate permissions to administer users and groups on this platform.

For additional information and guidance on Quick Connect Sync Engine version 5.5, please refer to the One Identity Quick Connect documentation on https://support.oneidentity.com/.

Platform support

- The IBM RACF® connector has been verified for synchronization against the IBM mainframe running z/OS 1.8 (and RACF 1.8) or later.
- The RACF connector should be installed on Microsoft® Windows Server® 2008 or later.
- The RACF connector is not supported on earlier releases of the Quick Connect Sync Engine, i.e. 5.3 or earlier.

Operating constraints

- There is an 8 character limit for user and group names on IBM RACF®.
- There is an 8 character limit for passwords on RACF.

Pre-installation information

Please read the information in this section before you install the IBM RACF® Connector.

User and group identifier

The LDAP implementation for IBM RACF® uses the `racfid` attribute to store the user name in a user object and the group name in a group object. The object containing the attribute defines whether it is referring to a user or a group.

Group membership

The group attribute `racfGroupUserids` contains a list of all users who belong to a group. If a group has no members, this attribute is not present (rather than present, but empty). To map an Active Directory® group's members to an IBM RACF® group's members, the AD attribute member must be mapped to `racfGroupUserids` for the RACF group. The connector has been written to support this mapping.

IBM RACF® system users

IBM RACF® creates three special or system users that are stored in the RACF database and which can be listed with an LDAP call. They are called iicerta, iimulti and iisitec.

These users cannot (and must not) be altered by the Connector through an LDAP call, so are filtered out by the Connector, i.e. when returning a list of all users in the database, these three special users will not be shown.

How to install and configure the IBM RACF® 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
- Configuring IBM RACF® Connector attributes

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

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

To install the One Identity Quick Connect for RACF connector software

1. To start the installation for:
    a. 32-bit systems; double click the **QuickConnectForRACF_x86.msi** installation routine.
    b. 64-bit systems; double click the **QuickConnectForRACF_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.

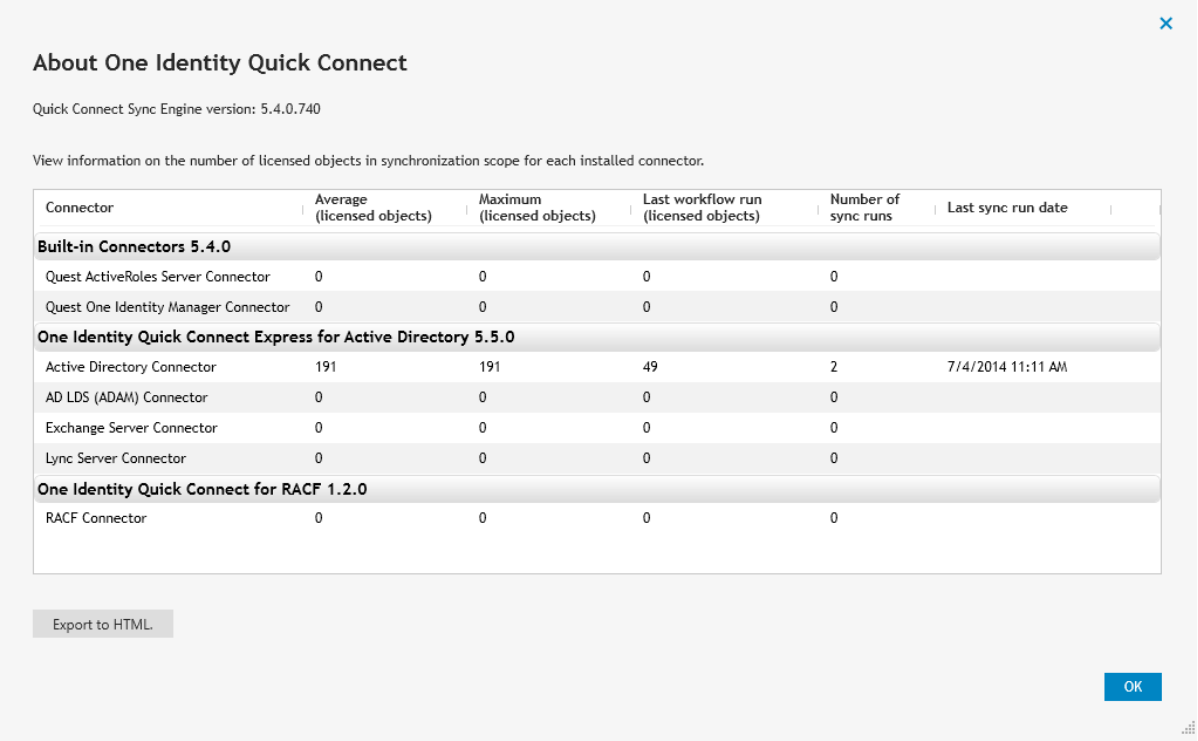
5. Click **Next**.
6. Click **Install**.

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 IBM RACF® 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 RACF Connector is included in the list of installed connectors.

Figure 1: About Quick Connect

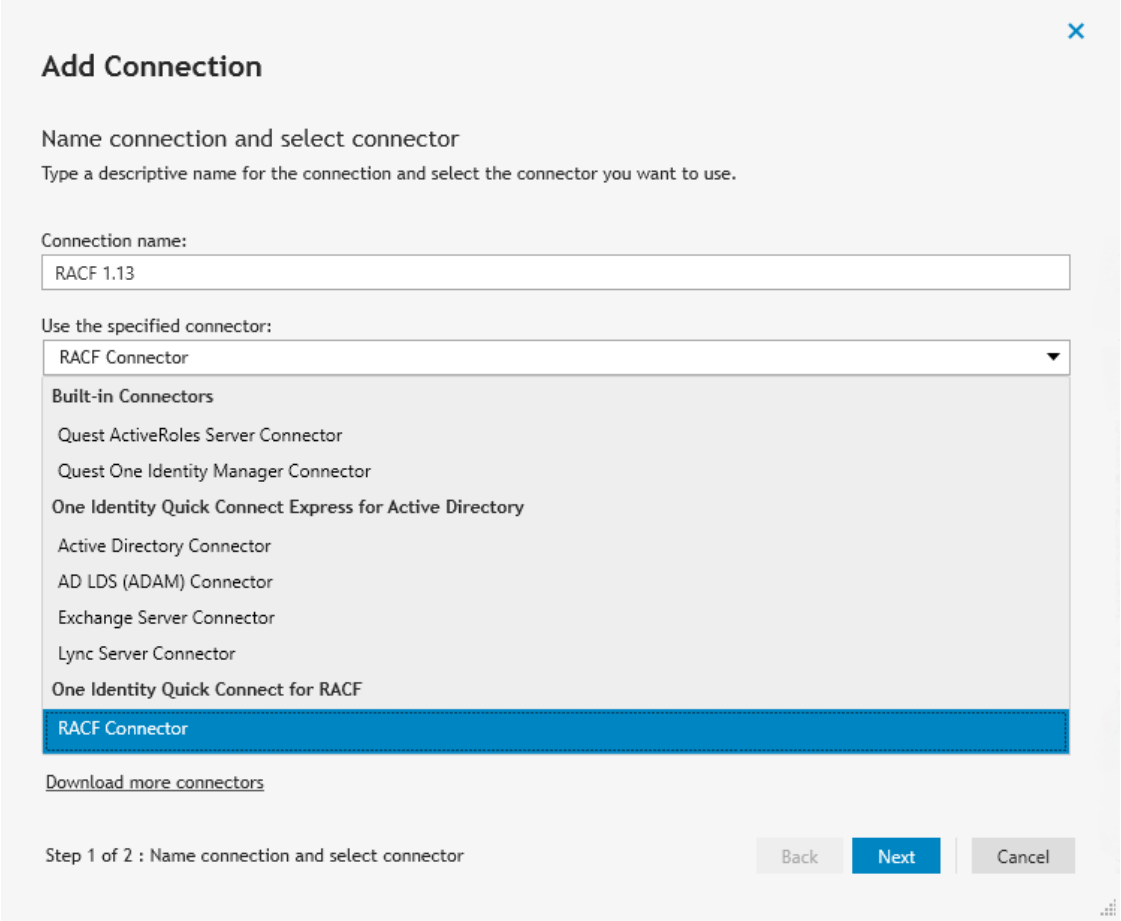


Adding a new IBM RACF® Connector

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:

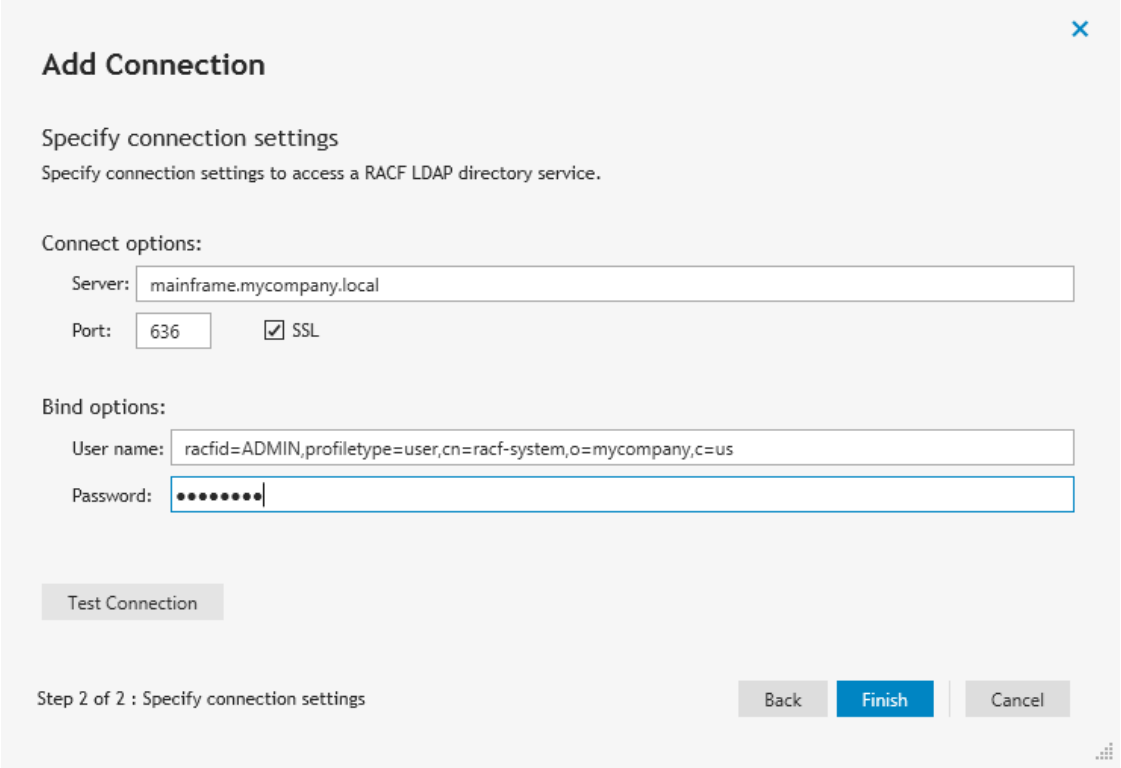
To start the Add Connected System wizard

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.



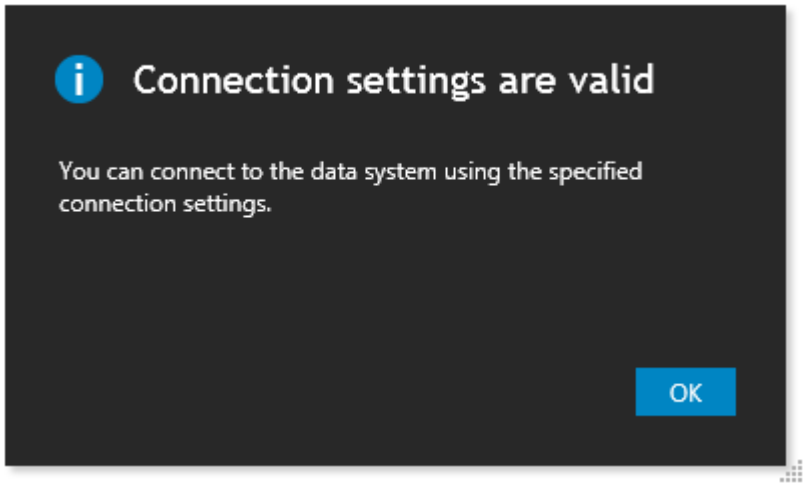
3. Enter a **Connection name**.
4. In the **Use the specified connector** field, choose the **RACF Connector** from the drop down list, and click **Next**.
5. On the **Specify connection settings** page, specify the RACF LDAP service to connect to and the account that the application will use to access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

This Specify connection settings page is similar to the following example.

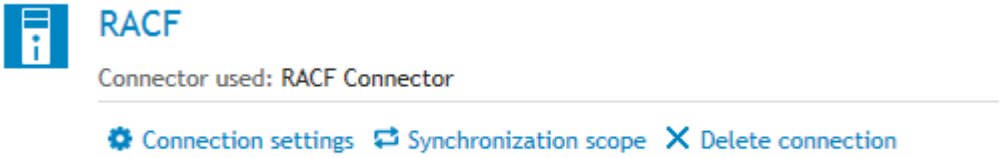


To specify connection settings to access a RACF LDAP directory service

1. Open the **Specify connection settings** for RACF page.
2. In the **Server** field, type the fully qualified DNS name of the RACF server running the LDAP service.
3. In the **Port** field, type the RACF 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 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:



Configuring IBM RACF® Connector attributes

The following attributes have been verified for one-way synchronization from Active Directory® and 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 (see Operating constraints).

Table 1: IBM RACF Connector attributes

Type of attribute	Active Directory attribute	RACF attribute
User	sAMAccountName	racfId
Group	sAMAccountName	racfId
Group	member	racfGroupUserids

Creating the One Identity Quick Connect mappings

You will need to create two mappings to enable user and group synchronization between Active Directory® and IBM RACF®.

For user synchronization

To create mappings for user synchronization

1. Firstly, define the RACF Connector as described in Adding a new RACF Connector, then click the Mapping tab.
2. Click the **Active Directory Connection** in the list of connectors.
3. Click **Add mapping pair** at the top of the screen.
4. A new Wizard starts.
5. Your Active Directory connector is automatically selected as the source.
6. Verify that the **System object type** is defined as **User (user)**, and then click **Next**.
7. In the **Target Connect System** section, click **Specify**…
8. Select your RACF connector from the list.
9. Click **Finish**.
10. Verify that the **system object type** is **racfUser**, then click **Finish**.
11. On the main **Mapping** screen, select your newly created pair.
12. Click **Add mapping rule**. The **Define Mapping Rule** wizard starts.
13. Click **Attribute**… for your Active Directory and select the **sAMAccountName** attribute for your Active Directory Attribute.
14. Click **OK**.
15. Click **Attribute**… for your RACF connector and select the **racfid** attribute for your RACF attribute.
16. Click **OK**.
17. Click **Map now**.

For group synchronization

To create mappings for user synchronization

1. Firstly, define the RACF Connector as described in Adding a new RACF Connector, then click the Mapping tab.
2. Click the **Active Directory Connection** in the list of connectors.

3. Click **Add mapping pair** at the top of the screen.
4. A new Wizard starts.
5. Your Active Directory connector is automatically selected as the source.
6. Click **Finish**.
7. Change the **system object type** to **Group (group)**, and then click **Next**.
8. In the **Target Connect System** section, click **Specify**…
9. Select your RACF connector from the list.
    a. In the **Connected System object type**: section, click **Select**…
    b. From the displayed list, select **racfGroup**.
    c. Click **OK**.
10. Click **Finish**.
11. On the main **Mapping** screen, select your newly created pair.
12. Click **Add mapping rule**. The **Define Mapping Rule** wizard starts.
13. Click **Attribute**… for your Active Directory and select the s**AMAccountName** attribute for your Active Directory attribute.
14. Click **OK**.
15. Click **Attribute**… for your RACF connector and select the **racfid** attribute for your RACF attribute.
16. Click **OK**.
17. On the main **Mapping** screen, click **Add mapping rule**. The **Define Mapping Rule** wizard starts.
18. Click **Attribute**… for your Active Directory connector and select the member attribute for your Active Directory attribute.
19. Click **OK**.
20. Click **Attribute**… for your RACF connector and select the **racfGroupUserids** attribute for your RACF attribute.
21. Click **OK**.
22. Click **Map now**.
23. When you have completed these steps, your mapping is complete.

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®.

Provisioning (groups)

To synchronize Active Directory® groups to IBM RACF®

1. Navigate to the **Workflow** tab on the main menu.
2. Click **Add workflow**.
3. Enter a description for your workflow, for example Sync Active Directory to RACF.
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 Connector and click **Finish**.
10. The Active Directory source object type: is currently set to **User (user)**. Change this to **Group (group)** by entering the word group.
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**…, and then locate your RACF connector and click **Finish**.
14. The object type in the **Target object system** field should be prefilled by One Identity Quick Connect to **racfGroup**.

15. Click **Next**.
16. In the **Specify provisioning rules** section, click **Attribute**.
17. In the **Source attribute**: field, click **Select**…, locate **sAMAccountName** and click **OK**.
18. In the **Target attribute**: field, click **Attribute**, then Select, locate **racfid** and click **OK**. (*)
19. Click **OK**.
20. Specify an initial password for the newly created group.
21. Click **Finish** to complete this synchronization step.

Provisioning (users)

To synchronize the Active Directory® users to IBM RACF®

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 Active Directory source object type**: is currently set to **User (user)**. Do not change this value.
8. Specify any **Specific Provision Criteria**, for example only members of a specific OU are synchronized.
9. Click **Next**.
10. In the **Target connected system**: field, click **Specify**…, and then locate your RACF connector and click **Finish**.
11. The object type in the **Target object system** field is prefilled by One Identity Quick Connect to **racfUser**.
12. Click **Next**.
13. In the **Specify provisioning rules** section, click **Attribute**.
14. In the **Source attribute**: field, click **Select**… locate **sAMAccountName** and click **OK**.
15. In the **Target attribute**: field, click **Attribute**, then **Select**, locate **racfid** and click **OK**. (*)
16. Click **OK**.
17. Specify an initial password for the newly created group.
18. 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 IBM RACF®

1. Navigate to the **Workflow** tab.
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)** and click **OK**.
8. Check that the **ActiveRoles Server object type**: is User (user). Change this to **Group (group)** by typing the word **group**.
9. Specify any **Updating Criteria** (for example only members of an OU are synchronized).
10. Click **Next**.
11. In the **Target connected system** field, click **Specify**…, and then locate your RACF connector.
12. Click **Finish**.
13. The **Target object type** should be set to **racfGroup**.
14. Click **Next**.
15. In the **Specify updating rules** section, click **Attribute**. (*)
16. A new **Direct Synchronization** screen is displayed. In the Source attribute: field, click **Select**, locate member and click **OK**.
17. Set the Target attribute: field to racfGroupUserids.
18. Click **OK**.
19. Click **Finish** to complete this synchronization step.

(*) At this stage in the process, you can configure as many attribute mappings between RACF and Active Directory as required for your infrastructure. The items specified in this guide are just an example.

For more information, please refer to the Operating constraints.

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

Deprovisioning (groups)

To deprovision groups

1. Navigate to the **Workflow** tab.
2. Click **Add synchronization step**.
3. Click **Deprovision**, and then click **Next**.
4. In the **Source connected system** section, click **Specify**…
5. Select your **Active Directory Connector** and click **Finish**.
6. Click **Select**….
7. Search for group and click **OK**.
8. Select the following check boxes in the Initiate deprovisioning if: section:
    - **Source object is deleted or is out of synchronization scope**
    - **Source object deprovisioning is initiated by ActiveRoles Server**
9. Optionally, configure the **Source object meets the following criteria** if required.
10. Click **Next**.
11. In the **Target connected system**: field, click **Specify**….
12. Locate your RACF connector and complete the wizard.
13. The **Target object type** will be prefilled automatically to **racfGroup**.
14. Click **Next**.
15. Select **Delete target object**.
16. Click **Finish** to complete this synchronization step.

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.

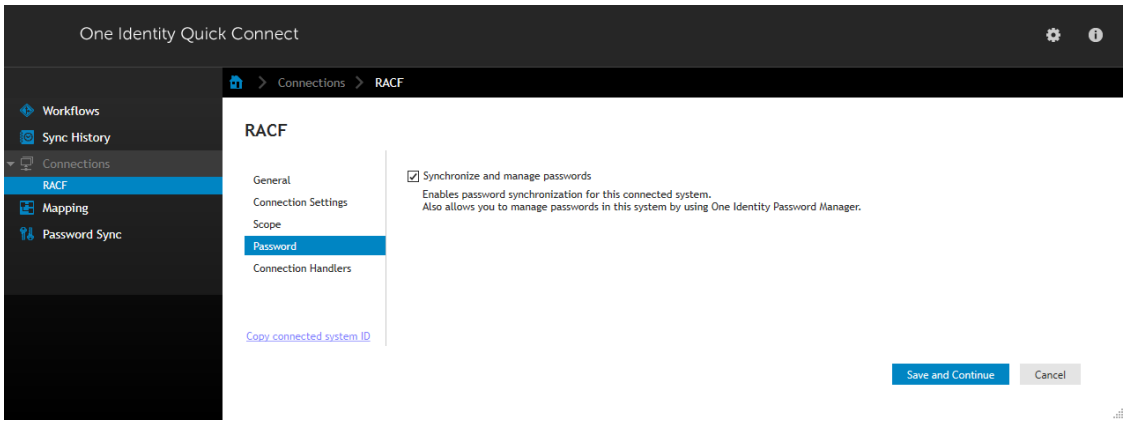
9. Click **Next**.
10. In the **Target connected system**: field, click **Specify**….
11. Locate your RACF connector and complete the steps in the Wizard.
12. The **Target object type** will be prefilled automatically to **racfUser**.
13. Click **Next**.
14. Select **Delete target object**.
15. Click **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®

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**.



Database attributes

This section describes any changes made by One Identity Quick Connect for IBM RACF® when writing data to or reading data from an IBM OS/390® mainframe with the RACF database.

The section consists of two tables:

- changes made when writing attribute values to a RACF database
- changes made when reading attribute values from a RACF database

Writing data to the IBM RACF® database

IBM RACF attribute	Description	Changes made by the Connector
racfAttributes	Attributes associated with a profile	None
racfAuthorizationDate	Authorization date - not modifiable	N/A
racfClassName	Class name	None
racfConnectGroupAuthority	Connect group authority	None
racfConnectGroupUACC	Connect group UACC	None
racfConnectGroupName	Connect group name	None
racfDatasetModel	Dataset model	None
racfDefaultGroup	A user's default group	None
racfGroupNoTermUAC	Group number terminal UACC	None
racfGroupUniversal	Universal group	None
racfGroupUserAccess	Group user access	None
racfGroupUserids	Group userIDs	None
racfhavePasswordEnvelope	Determines whether or not a user's password has been enveloped - not modifiable	N/A
racfid	User or group name	None
racfInstallationData	Installation data	None
racfLastAccess	Date of last access - not modifiable	N/A
racfLogonDays	Day of last log in	None
racfLogonTime	Time of last log in	None
racfOwner	Account owner	None
racfPassPhrase	User's pass phrase	None
racfPassPhraseChangeDate	The date the user's pass phrase was last changed - not modifiable	N/A

IBM RACF attribute	Description	Changes made by the Connector
racfPassword	User's password	None
racfPasswordChangeDate	The date the user's password was last changed - not modifiable	N/A
racfPasswordEnvelope	Password envelope - not modifiable	N/A
racfPasswordInterval	Password interval - not modifiable	N/A
racfProgrammerName	Programmer name	None
racfResumeDate	Account resume date	None
racfRevokeDate	Account revoke date	None
racfSecurityCategoryList	Security category list	None
racfSecurityLabel	Security label	None
racfSecurityLevel	Security level	None
racfSubGroupName	Sub group name	None
racfSuperiorGroup	Superior group	None

Reading data from the IBM RACF® database

IBM RACF attribute	Description	Data type returned
racfAttributes	Attributes associated with a profile	String
racfAuthorizationDate	Authorization date	Date/time
racfClassName	Class name	String
racfConnectGroupAuthority	Connect group authority	String
racfConnectGroupUACC	Connect group UACC	String
racfConnectGroupName	Connect group name	String
racfDatasetModel	Dataset model	String
racfDefaultGroup	A user's default group	String
racfGroupNoTermUAC	Group number terminal UACC	String
racfGroupUniversal	Universal group	String

IBM RACF attribute	Description	Data type returned
racfGroupUserAccess	Group user access	String
racfGroupUserids	Group user IDs	String
racfhavePasswordEnvelope	Determines whether or not a user's password has been enveloped	String
racfid	User or group name	String
racfInstallationData	Installation data	String
racfLastAccess	Date of last access	Date/time
racfLogonDays	Day of last log in	Integer
racfLogonTime	Time of last log in	String
racfOwner	Account owner	String
racfPassPhrase	User's pass phrase	String
racfPassPhraseChangeDate	The date the user's pass phrase was last changed	Date/time
racfPassword	User's password	String
racfPasswordChangeDate	The date the user's password was last changed	Date/time
racfPasswordEnvelope	Password envelope	Binary
racfPasswordInterval	Password interval	String
racfProgrammerName	Programmer name	String
racfResumeDate	Account resume date	Date/time
racfRevokeDate	Account revoke date	Date/time
racfSecurityCategoryList	Security category list	String
racfSecurityLabel	Security label	String
racfSecurityLevel	Security level	String
racfSubGroupName	Sub group name	String
racfSuperiorGroup	Superior group	String

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