FORTRA

Powertech RSA SecurID Agent for IBM i 9.13

Installation Guide

Copyright Terms and Conditions

202403280759

Installing RSA SecurID Agent

Use the following instructions to install Powertech RSA SecurID Agent for IBM i.

For information regarding installation of SecurID Remote Authentication, see Installing SecurID Remote Authentication.

Before You Begin

Read this section before you install Powertech RSA SecurID Agent for IBM i.

System Requirements

- **Disk Space:** The amount of disk space required to accommodate the software will be approximately 60MB.
- **Data Requirements:** The amount of disk space required to accommodate the necessary information is dependent on the number of profiles to have authentication. A journal technique has been introduced as from version 9.8.2, to provide auditing of the configuration details. Beginning with version 9.8.3.1 additional journal processing has been included for user/job activity relating to 'Emergency Access'. Therefore, as a rule of thumb, you should ensure that there is a minimum of 100MB of DASD available for the initial installation. It is certainly anticipated that no where near this amount of space will in fact be used, but this will give you sufficient space to start using RSA SecurID Agent.
- **OS:** The minimum level of IBM i operating system software that is required to support RSA SecurID Agent, is IBM i 7.3 (V7R3M0). Contact your local supplier if you are concerned whether your version of RSA SecurID Agent will function correctly with your version of IBM i.
    - In order to prevent multiple RSA SecurID Agent challenges for a series of DDM (not DRDA) requests from a specific IBM i job, an IBM PTF is required to have been applied. Check with your IBM i administrator to make sure your database group PTF levels are up to date.

      GET_JOB_INFO

      IBM i 7.3 SF99703 Level 3
- **Profiles:** There are three profiles required by this software: PTADMIN, PTUSER, and a product administrator profile (to be designated by the security officer) that is a member of the PTSECURID authorization list. For proper functioning of the system, do not delete these profiles. Should you designate additional product administrator

profiles, they must be included in the PTSECURID authorization list.

> **IMPORTANT:** These profiles are shared with other Powertech products, and consideration must be made before uninstalling SecurID or any of the products that use these profiles. SecurID will become unusable if these profiles are removed. Do not uninstall Powertech Central Administration and care must be taken when removing any Powertech products that share these common profiles. Be sure to discuss any plans with Fortra Support before proceeding.

- **Error Logs:** If errors occur which cannot be transmitted to the operator, the system will dump the error to the output queue (QEZDEBUG) on the system on which it has occurred.
- **PASE:** Portable Application Solutions Environment, option 33.

> **NOTE:** Installation of SecurID does not change any major system settings.

Installation Considerations

- Ensure that the system value QALWOBJRST has a value of *ALL i.e.

  ```
  CHGSYSVAL SYSVAL(QALWOBJRST) VALUE('*ALL')
  ```

- The QSECOFR security officer profile is referenced within these instructions for use during the installation process. However, a different profile may be used but MUST have all the Special Authorities that are associated with QSECOFR, on your release level of IBM i. Make sure that you have access to the appropriate profile, ideally the QSECOFR security officer profile. Do not attempt to load the software with any other profile that does not have all the required Special Authorities.

Installing RSA SecurID Agent

Ensure the following servers are available and running prior to installation:

- FTP Server
- Remote Command Server

Do the following to perform the installation or update:

1. Download the Powertech RSA SecurID Agent for IBM i installer (**setupAgentForRSASecurID.exe**) to your PC from the Powertech RSA SecurID Agent for IBM i Downloads page.
2. On the Choose Components panel, select which components you want to install. You can choose to install the Manuals and the Software for IBM i. Click **Next**.

3. If you are installing the Manuals only, the process completes and the installer closes. The Manuals have been installed. You can skip the rest of these steps.

   > **NOTE:** The manuals are installed to the following location: C:\Program Files\PowerTech\RSA SecurID Agent for IBM i\manuals

4. On the IBM i Details panel:
   a. Select or enter the IBM i system.
   b. Enter a user profile and password that is a member of the user class *SECOFR and has at least the following special authorities: *ALLOBJ, *SECADM, *JOBCTL, *IOSYSCFG, and *AUDIT. The user profile should have Limit capabilities set to *NO.
   c. (Optional) In the Advanced Settings section:
      - Enter a port number or use the arrows if you want to change the FTP port number to something other than the default of 21.
      - Select **Secure File Transfer** if you want to use FTPS (FTP over SSL) during the file transfer. The default FTPS secure port is 990, but it can be changed to the required secure port for your environment.
      - In the **Timeout (seconds)** field, enter the number of seconds the session should be kept active during an FTP transfer. You can choose anywhere between 25 and 1800 seconds (30 minutes).

        > **NOTE:** If the transfer takes longer than the amount of time specified, the session will expire.

   d. Click **Next**.
5. You have two options on the Product Load Options panel:
   a. Click **Immediate Load** if you'd like to load the product on the IBM i now.
   b. Click **Staged Load** if you'd like to transfer the objects now and load them on the IBM i at a later time.

      > **NOTE:** See "Loading Staged Objects on the IBM i" (below) for instructions on how to load the staged objects on your selected IBM i system.

6. The Product Load Progress panel for Powertech RSA SecurID Agent for IBM i launches.

   If the Product Load Progress panel ends with an overall Failed message, the product upload could not complete properly. To find the reason the upload failed, click **View Logs** and review your logs. You can also use **Download** at the top of the logs to save the information for future review.

   When the processing is complete, you have two choices:

- If this is the only installation or update of Powertech RSA SecurID Agent for IBM i that you're doing, click **Finish**.
- If you have installs or updates to do on other IBM i systems, click **Restart**. Then, return to step 4.

Loading Staged Objects on the IBM i

If you chose to stage your objects during step 5b of the installation or update process, do the following to manually load them on the IBM i you identified above.

1. On the IBM i, execute the following command to display the Work with Loads panel:

   HSLOADMGR/HSWRKLOAD
2. Enter option **1**, Load, next to the Load Name for Powertech RSA SecurID Agent for IBM i and press Enter.

   The installation program installs Powertech RSA SecurID Agent for IBM i, including the required user profiles and libraries (see table below for details).

The installation process displays the job log name, user, and job log number. Use the WRKSPLF command to display the job log for complete information on the Powertech RSA SecurID Agent for IBM i install.

After You Are Done

Congratulations! RSA SecurID Agent is now installed. Read the following for additional information regarding installed objects.

Objects Installed on System

Installed on System	Description
Product Library	@ACE
User Profiles	PTADMIN, which has special authorities *ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL, *SAVSYS, *SECADM, *SERVICE, and *SPLCTL PTUSER, which has no special authorities
Authorization List	PTSECURID - for product administrators
Subsystem	ACEDTI
Job Queue Entries	@ACE/ACEDTI01 & @ACE/ACEDTI02 added to ACEDTI

Removing Install / Upgrade Objects

When you install/upgrade, a couple of installation only libraries are created as follows:

- Install/Upgrade Object Library. The default library is called @APYACE. This library contains objects required to install/upgrade the SecurID software.
- Save File Library. The default library is called @ACESAVF. This library contains save files containing the actual SecurID software.

After a successful install/upgrade, you can remove these libraries from the system.

Remote Authentication Software

If you now wish to install the Remote Authentication Software, proceed to Installing SecurID Remote Authentication.

Upgrading RSA SecurID Agent

Important Considerations before Upgrading

- The process to upgrade **Powertech RSA SecurID Agent for IBM i to version 9.10 or higher will attempt to delete the user profile ACEDTI, as well as all objects owned by this profile, and the contents of the @ACEOLD library (if found).Before upgrading, you must backup the existing @ACE library**
  - Before upgrading, you must backup the existing @ACE library.
  - After this upgrade, the @ACEOLD library can no longer be restored to the revert to the prior version.

    > **NOTE:** The ACEDTI profile will not be deleted in some cases. This does not interfere with the proper functioning of the SecurID Agent.

- **RSA SecurID Agent objects are now owned by one of two User Profiles:**
  - **PTUSER** - Standard object owner User Profile with IBM i Special Authority set to *NONE.
  - **PTADMIN** - Administrator level owner User Profile, which includes all available IBM i Special Authority values.

  (Previously, all objects were owned by a single User Profile named, ACEDTI.)

  > **IMPORTANT:** These profiles are shared with other Powertech products, and consideration must be made before uninstalling SecurID or any of the products that use these profiles. Be sure to discuss any plans to remove Powertech Central Administration, Command Security, SecurID, or other products that make use of these common profiles with Fortra Support prior to doing so.

- **The installation must be in a dedicated mode.** Ensure that all users who are controlled by SecurID are already signed off.

  To ensure that you are in a dedicated mode, use the commands:

  ```
  WRKOBJLCK QSYS/@ACE *LIB

  WRKOBJLCK @ACE/MSFT770 *FILE

  WRKOBJLCK @ACE/MSFT094 *FILE
  ```

No one should be using this library. Also check that the libraries @ACE and other prefixed @ACE* libraries are not in the system library list or in the user library list. Check this by using the WRKSYSVAL command.

If in doubt, you may want to ensure that the machine is in a restricted state before continuing.

- Ensure that the system value QALWOBJRST has a value of *ALL i.e.

```
CHGSYSVAL SYSVAL(QALWOBJRST) VALUE('*ALL')
```

- The QSECOFR security officer profile is referenced within these instructions for use during the upgrade process. However, a different profile may be used but MUST have all the Special Authorities that are associated with QSECOFR, on your release level of IBM i. Make sure that you have access to the appropriate profile, ideally the QSECOFR security officer profile. Do not attempt to load the software with any other profile that does not have all the required Special Authorities.
- Ensure that the software is compatible with your IBM i operating system release level. If the release of your IBM i operating system is below that of the permitted release level, you will have to upgrade your operating system to the correct level. Consult your system administrator for further details.
- Ensure that your current SecurID system is properly backed up. The libraries to back up are all the @ACE* prefixed libraries. Also, for Agent version 9.7.0 (and later), back up the IFS directory: /var/ace . Complete these backups first before proceeding further.
- The installation time may vary between 0.5 hours to 1 hour depending on the size and usage of SecurID.
- Remove all reports (if any) in the @ACE/ACEDTI output queue. The output queue should be empty. If the queue is not empty, the job to remove the previous version of the @ACE library (@ACEOLD) may terminate abnormally.
- Also, ensure that there are no outstanding jobs waiting in any of the SecurID job queues. If there are any, you must ensure that they are either processed or deleted accordingly.

Important Consideration for the SecurID Authentication

Upgrading from version 9.8.0 or earlier

The following applies if the current version of the SecurID Agent is prior to 9.8.1 and had been used for authentication:

a. After installing or upgrading to version 9.8.1 (or later), access the Authentication Manager to clear the Node Secret from the IBM i agent.
b. The Node Secret should also be deleted from the actual IBM i agent.

The above notes also apply if any other product had been used, on the IBM i System to perform SecurID authentication with the same Authentication Manager.

Software Availability

The RSA SecurID Agent download is available via the Fortra Support Portal.

Native Software Upgrade Procedure

Follow the same instructions as the installation procedure. See Installing RSA SecurID Agent.

Removing Install/Upgrade Objects

When you install/upgrade SecurID, a couple of installation only libraries are created as follows:

- Installation Object Library. The default library is called @APYACE. This library contains objects required to install/upgrade the SecurID software.
- Save File Library. The default library is called @ACESAVF. This library contains save files containing the actual SecurID software.

After a successful install/upgrade you can remove these libraries from the system.

> **NOTE:** If you wish to install the Remote Authentication Software, proceed to the section entitled Installing the Remote Authentication Software.

Installing SecurID Remote Authentication

The following instructions describe how to install SecurID Remote Authentication. See the *Powertech RSA SecurID Agent for IBM i User Guide* on the FortraSupport Portal.

Important Considerations Before Installing

- The Administrator account should be used during the installation process so make sure that you have access to the Administrator account. **Do not use any other account to load the software.**
- The Remote Authentication software is only available for Microsoft Windows based PC's.

Available Software

The SecurID Remote Authentication download is available among the RSA SecurID Agent downloads on the Fortra Support Portal. It is an executable file that deploys the installation package onto your Windows PC.

The file "setupSecurIDRemoteAuthentication.exe" contains the setup routine to install software that allows users to input the data required for SecurID authentication. The installed software is activated when "Remote Authentication" has been configured for client / server based requests and the user makes such a request. For example, when an FTP request is performed by the user. See the Configuring SecurID Remote Authentication section in the *Powertech RSA SecurID Agent for IBM i User Guide*.

Software Install Procedure

The whole installation process (including download) should not take more than 0.5 hour to complete.

PC

1. Locate the file containing the Remote Authentication Installation file: "setupSecurIDRemoteAuthentication.exe". The SecurID Remote Authentication Software download is available on the Fortra Support Portal.
2. Run "setupSecurIDRemoteAuthentication.exe".
3. Follow the instructions within the installation windows.

Configuring the RSA SecurID Agent

Important Considerations

1. These instructions are compatible with Authentication Manager Version 8.4, or above when processing using RSA SecurID Replicas.
2. Ensure your IBM machine is running IBM i 7.3 (V7R3M0) or above.

System Preparation

Server Machine

1. Sign on as the Administrator profile.
   Example: "root" on UNIX or “Administrator” on Windows.
2. Register the IBM i client as a "host" on the server.
   Either edit the server’s local host table or add the machine, running IBM i within the DNS.

Client Machine (IBM i)

1. Sign on as QSECOFR.
2. Access the command line.
3. Enter the command CFGTCP.
4. Select the option to "Work with TCP/IP Interfaces". Select the option to add details of local machine:
   - Internet address: INTNETADR
   - Line description: LIND
   - Subnet mask: SUBNETMASK
5. Select the option to "Work with TCP/IP host table entries". Select the option to add details of server & local system.
   - Internet address: INTNETADR
   - Host names: HOSTNAME
   - Text: TEXT

6. Select the option to "Change local domain & host names".
    - Local domain name
    - Local host name
7. Select the option to "Configure related tables". Select the option to "Work with service table entries". Select the option to add details for service entry. The SecurID Agent defaults are:
    - Service: securid
    - Port: 5500
    - Protocol: udp
    - Text: SecurID authentication

Check System Configuration

Server Machine

Ensure the machine to host the RSA Authentication Manager is ‘up and running’.

Client Machine (IBM i)

1. Start TCP/IP jobs.
   Use STRTCP command from command line.
2. Check configuration.
   Ping "server" (either TCP/IP address or name).

Server Machine

Check configuration

Ping "IBM i client" (either TCP/IP address or name)

Software Installation

Server Machine

1. Install the RSA Authentication Manager product on designated server machine as outlined within the appropriate documentation.
2. Add the IBM i client into the RSA Authentication Manager database.
3. Activate appropriate users for the IBM i client.
4. Generate the required sdconf.rec configuration file.

Refer to the appropriate Authentication Manager documentation for details of the above.

Client Machine (IBM i)

1. Sign on as QSECOFR profile.
2. Install the SecurID Agent software.
3. Start TCP/IP jobs.

   ```
   STRTCP
   ```

4. FTPRMTSYS (server name).

   ```
   binary
   lcd     /
   cd      VAR_ACE     (data directory)
   get     sdconf.rec  /var/ace/sdconf.rec
   ```

Troubleshooting the Installation

To help you troubleshoot any problems that may occur during, or after, the installation, we have put together a series of frequently asked questions regarding SecurID authentication for an IBM i agent.

Q: How do I register an IBM i agent?
A: The IBM i agents are registered in the same manner as existing SecurID Agents. To do this you must use the Administration facility on the Authentication Manager (ACE/Server). For an IBM i agent the type must be specified as:

> “Standard Agent”

Q: Where is the "sdconf.rec" record stored?
A: The "sdconf.rec" record is held within the IBM i Portable Application Solutions Environment (PASE). It is located under /var/ace/sdconf.rec

Q: How can I move the @ACE/SDCONF file into PASE as sdconf.rec?
A: After upgrading the RSA SecurID Agent, the @ACE/SDCONF file can be moved using fip with binary mode transfer.

For example:

a. Sign on to the IBM as QSECOFR
b. ftp < local IBM i >
c. cd /
d. bin
e. namefmt 1
f. put /qsys.lib/@ace.lib/sdconf.file /var/ace/sdconf.rec

Q: How can I get the sdconf.rec file to the IBM i?

A: After installing RSA SecurID Agent, the sdconf.rec file can be installed using fip with binary mode transfer.

For example:

a. Sign on to the IBM i as QSECOFR
b. ftp < server name >
c. bin
d. lcd /

e. cd VAR_ACE (data directory)
f. get sdconf.rec /var/ace/sdconf.rec

Q: Where is the node secret stored?
A: The node secret is stored within the IBM i Portable Application Solutions Environment (PASE). It is located under /var/ace/securid

Q: How do I remove the node secret?
A: The node secret can be removed using one of the following:

1. Calling IBM i command:

   ```
   WRKLNK  OBJ('/var/ace/*')
   ```

2. Accessing PASE and calling AIX commands such as cd. rm etc
3. Using a mapped drive on a PC that has access to the /var/ace/ directory within IBM i Integrated File System (IFS)

Q: Why do I keep receiving the message "Cannot initialize client-server communications"?
A: There are several areas that need to be reviewed:

1. The TCP/IP host name for the machine running IBM i (on the IBM i) must:
   a. begin with the system name of the machine running IBM i
   b. have the domain name as the suffix. For example:
      - System name: MYIBMI
      - Domain name: XYZ.COM
      - Host name must be: MYIBMI.XYZ.COM

   > **NOTE:** If any changes are made within the TCP/IP configuration, on IBM i, TCP/IP must be re-started. The IBM i line description may also need to be "varied off" and "varied on".

   When registering the IBM i agent with the RSA Authentication Manager (AM) the AM will be expecting the name and IP address for the IBM i to be the same as that referenced within the host table entries that are accessible by the AM. If, however, the IBM i entry in the main host table, for example, DNS is NOT correct, a local entry may be required to be configured, for the IBM i within the AM itself.

   Alternatively, configuration file /var/ace/sdopts.rec may be required on the IBM i.

   The entry to be used is:

   CLIENT_IP=< IP Address expected by AM >

where:
< IP Address expected by AM > is the IPV4 address that the AM is expecting the IBM i will be sending data from, for example, 192.168.23.5

Such a situation may occur if using virtual address configuration and the IBM i data is being sent and/or routed using a different network interface to the one that is used to identify the IBM i.

> **NOTE:** When creating or updating /var/ace/sdopts.rec ensure to use the 'echo' command within PASE. Maintaining the file on a platform such as Windows will most likely use different record line endings that are not expected by UNIX based systems such as IBM's PASE.

2. The Authentication Manager (ACE/Server) services are not started. Refer to the appropriate documentation for your Authentication Manager
3. The SecurID sever job, ACEDTIDS01 is not active
    - Review subsystem, ACEDTI
    - If the ACEDTI subsystem is currently active, run ENDACEDTI
    - To start the ACEDTI subsystem, run command, STRACEDTI

Q: How do I activate server job, ACEDTIDS01 ?
A: Use the SecurID "Work with TCP/IP port connections" menu option to configure the required port number.

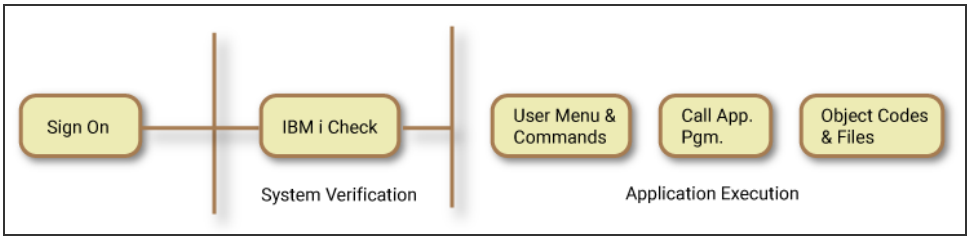
Q: How do I activate SecurID authentication for IBM i sign on?
A: The authentication is activated at the profile level using one of the following for each profile:

1. Use Powertech RSA SecurID Agent Maintenance to activate SecurID authentication
2. Include the ATHPRF command within the initial program of the IBM i profile

Q: No changes have been made to the profiles but the authentication screen does not appear!
A: For the SecurID authentication screen to be displayed the SecurID product installation must be valid. If the software key has expired, the authentication routine is no longer active.

Important Considerations for the SecurID Authentication

Implementation type

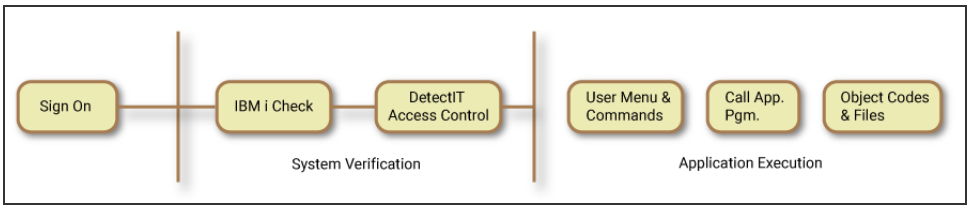


The above diagram shows normal IBM i processing of a sign-on request. The user enters their profile name and password and the IBM i operating system verifies the entries. If the entries are valid, the IBM i passes control to the initial program as specified in the user profile control record. This initial program can be a menu or a program. In normal circumstances, this is most likely to be a menu. The menu allows the user to select the next step of their processing requirement. This is usually the execution of a selected option that then calls an application program. The application program will execute the appropriate object codes and maintain the appropriate database accordingly.

If you use this type of security set up, it will be your responsibility to ensure that the programs, objects, and live data files are properly configured to protect against unauthorized access, unauthorized use of programs, and unauthorized changes of live data. An experienced security officer will know that by using the basic IBM i commands they can fulfil most of the security requirements, but maintaining the integrity of a secured environment can be a major task. Furthermore, the retrieval of pertinent information is not quick enough, meaningful enough, or consolidated in a useful fashion for easy reference.

SecurID is designed to be flexible. It has built in 'switches' to allow you to implement security at your own pace. The more profiles challenged with SecurID authentication, the more secure your environment will be. In the following section, we will discuss how you can introduce SecurID in your system up to the user profile level. This process makes use of DetectIT access control. We call this a 'SIMPLE INSTALLATION'.

Simple installation



A simple installation allows you to introduce DetectIT access control using SecurID into your IBM i. SecurID complements and enhances existing IBM i facilities. What is more important, it will manage your security more efficiently, with the introduction of integrated and enhanced features over standard IBM i. User profiles can be managed in a controlled manner.

For using Powertech RSA SecurID Agent for IBM i refer to the User Guide on the Fortra Support Portal. You will be required to have the system available when you go through the illustrations. Program names or commands will be referred to rather than menu option numbers.

Designating a SecurID Security Officer

Profiles to be authorized to administer Powertech RSA SecurID Agent for IBM i must be added to the PTSECURID authorization list. No specific Special Authority values are required as all necessary authority is provided by the appropriate product object owner profiles (PTUSER or PTADMIN).

> **NOTE:** When upgrading from Powertech RSA SecurID Agent for IBM i version 9.9 or earlier, the ACEDTI profile is removed. Objects previously owned by ACEDTI are now owned by one of two other profiles, PTUSER or PTADMIN.

You can use the following command to add a profile to the PTSECURID authorization list (with *USE authority), where *myuser* is the administrator profile to add.

ADDAUTLE AUTL(PTSECURID) USER(*myuser*) AUT(*USE)

QSECOFR

QSECOFR is the IBM supplied security officer. This profile could easily be misused and therefore the risk associated is extremely high. Access to the password of this profile should be carefully controlled. The password must be authorized by management, and its use should be carefully logged.

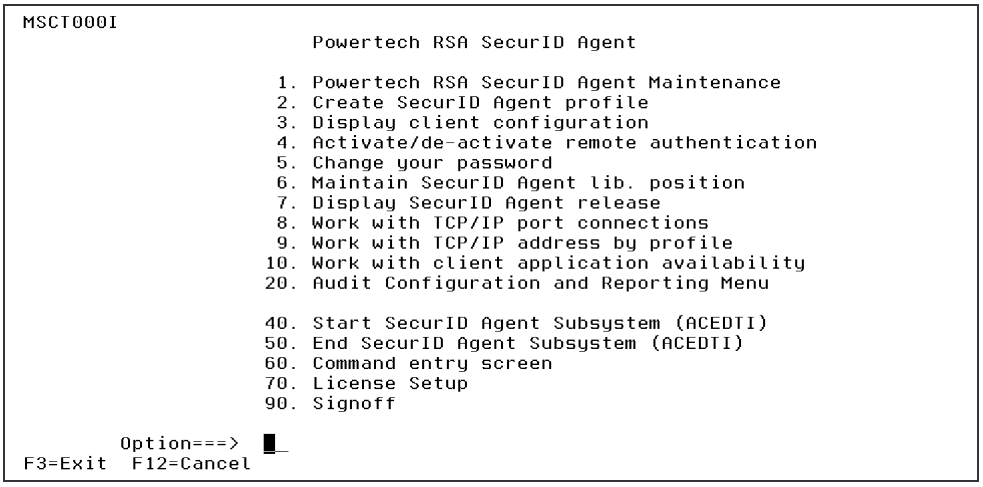
It is recommended that the IBM i security officer QSECOFR does not have SecurID authentication activated via SecurID. This will ensure that in the unlikely event that any changes made by IBM to their operating system that may affect QSECOFR, it will not inhibit your ability to work properly as the security officer.

The QSECOFR profile should never be used in the daily running of the computer. The QSECOFR password should be sealed in an envelope and only used in exceptional circumstances. These circumstances may include applying IBM software or SecurID upgrades, changing system values, or controlling object authority. You may even consider introducing dual control or key locks on the QSECOFR password so that there should always be two persons involved in the use of this profile. You should create a substitute security officer adopting the QSECOFR group profile. By doing this, you can still continue to perform with the authority of the security officer and can monitor the activities of QSECOFR. This should rarely happen except when the sealed password is used. Otherwise someone must have breached the security officer's password!

When you are creating the substitute security officer, you should avoid using a name similar to QSECOFR. In this way, you should 'lose' the identity of the new security officer amongst your other users. You should make the name as normal as your other users. The reason behind this is to keep the potential hacker guessing, as surely one of the hacker's main objectives is to retrieve QSECOFR and its password. Since that is not easily available, the next target is to retrieve profiles adopting QSECOFR.

Accessing the Powertech RSA SecurID Agent menu

The installation places command WRKSECURID into libraries QGPL and @ACE, which can be used to access the Powertech RSA SecurID Agent menu, if authorized:



Activating RSA SecurID Agent authentication

From the Master Menu, select option **1**. The Powertech RSA SecurID Agent Maintenance screen appears, which permits you to perform the following:

a. Configure TCP/IP network between IBM i and RSA Authentication Manager server.
b. Activate SecurID authentication against any of your profiles.

See the *Powertech RSA SecurID Agent for IBM i User Guide* on the Fortra Support Portal for more information.

Other Considerations

Saving the SecurID Agent

The SecurID libraries and associated Integrated File System (IFS) directory should be backed up on a regular basis as part of your normal operational procedures. The libraries to be saved are as follows:

-@ACE

-@ACE* (Language libraries. The actual library names will depend on the languages that were installed with your SecurID system).

The Integrated File System (IFS) directory to backup is:

/var/ace

The @ACE library contains the most critical data, and should be backed up at least daily.

It is recommended that, where possible, the libraries should be backed up in a dedicated mode:

- Ensure all users using SecurID are signed off.
- Perform Backup.
- Allow users back onto the system.

Where this procedure is not practical, the SecurID libraries can be backed up using other backup functions available within IBM i such as the "save-while-active" technique.

SecurID Agent in the live environment

SecurID offers you a unique facility to determine how you wish to position its libraries within the user's library list. On the relevant menu, there is an option entitled 'Maintain Powertech Agent lib. position'.

This allows you to define where to place the SecurID libraries: in the system portion or the user's portion of their library list. If the libraries are placed in the system portion, the users cannot change their library list entries using the normal ADDLIBLE or RMVLIBLE or CHGLIBL commands. This is because the CHGSYSLIBL command has a default public authority of *EXCLUDE. Thus, your users can not use this command to change the library in their system portion library list. You could change the authority to allow your users to use this

command but that would not be advisable. You should not allow your users to change the system portion of their library lists.

For optimum security, you should place the SecurID libraries in the system portion of the user's library list. This will stop them from removing them from their library list to stop you from monitoring their activities.

Note the language libraries (@ACE*) must always reside in the system portion of the user's library list. Do not change this entry as it will affect the integrity of the system.

The default setting within the program is *SYSLIBL. This places the SecurID libraries into the user's system portion of their library list.

The following entries are valid:

***SYSLIBL**	The SecurID libraries will be added to the system library list of the user.
***USRLIBL**	The SecurID libraries will be added to the user library list.
***NONE**	No library will be added. Libraries will be added using the normal commands. Warning; This method may cause an abnormal functioning of SecurID.

NOTE: SecurID will incorporate the above activities during execution time. DO NOT enter SecurID libraries in the Initial library list of a job description, or QUSRLIBL and QSYSLIBL system values.

Contacting Fortra

Please contact Fortra for questions or to receive information about Powertech RSA SecurID Agent for IBM i. You can contact us to receive technical bulletins, updates, program fixes, and other information via electronic mail, Internet, or fax.

Fortra Portal

For additional resources, or to contact Technical Support, visit the Fortra Support Portal at https://support.fortra.com.