RSA Ready Implementation Guide for

RSA SecurID

HelpSystems Safestone DetectIT Security Manager 14.4.6

Daniel R. Pintal, RSA Partner Engineering
Last Modified: April 15, 2016

RSA READY

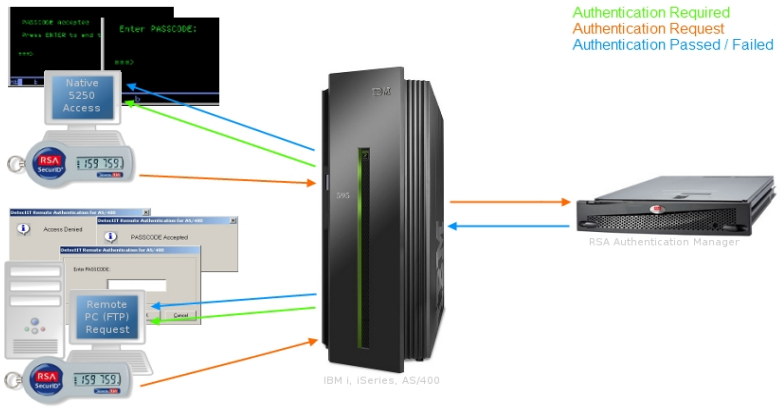
Solution Summary

The DetectIT Agent for RSA SecurID brings confidence to everyday transactions, providing secure access for employees, customers and partners while striking the right balance between risk, cost and convenience. It dramatically increases security by providing RSA SecurID's market-leading two-factor authentication to users of IBM i on Power Systems (AS/400, iSeries, System i). The DetectIT Agent for RSA SecurID is a targeted implementation that can be configured with extra controls if and when they are required, both minimizing disruption and costs.

DetectIT provides two kinds of authentication for IBM i:

- Native authentication for users working within the traditional 5250 screen environment.
- Remote authentication for client/server-based requests such as FTP.

RSA Authentication Manager supported features Safestone DetectIT Security Manager 14.4.6	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	No
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes



RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between the DetectIT Security Manager and the RSA Authentication Manager an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the DetectIT Security Manager and contains information about communication and encryption.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Important: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with DetectIT Security Manager will occur.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the DetectIT Security Manager with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All appropriate DetectIT Security Manager components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Safestone DetectIT Security Manager Configuration

Configure DetectIT and IBM i LPAR for RSA SecurID Authentication

1. Install/upgrade DetectIT Security Manager as outlined within the DetectIT Deployment instructions.

> **Important: Please refer to the DetectIT Deployment Guide for further details.**

2. Configure SecurID Authentication service port. Sign on to IBM i LPAR using the ALERT profile.

   - Sign on to IBM i LPAR using the ALERT profile.
   - Run the **CFGTCP** command.
   - Select **Configure related tables**.

```
CFGTCP                          Configure TCP/IP
                                                        System:    SST8001
Select one of the following:

     1. Work with TCP/IP interfaces
     2. Work with TCP/IP routes
     3. Change TCP/IP attributes
     4. Work with TCP/IP port restrictions
     5. Work with TCP/IP remote system information

    10. Work with TCP/IP host table entries
    11. Merge TCP/IP host table
    12. Change TCP/IP domain information

    20. Configure TCP/IP applications
    21. Configure related tables
    22. Configure point-to-point TCP/IP


Selection or command
===> 21

F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel
```

   - Select **Work with service table entries**.

```
                      Work with Service Table Entries
                                                        System:    SST8001
Type options, press Enter.
  1=Add    4=Remove    5=Display

Opt  Service                                 Port  Protocol
 1   securid                                 5500  udp
 _   as-admin-http                           2001  tcp
 _   as-admin-http                           2001  udp
 _   as-admin-https                          2010  tcp
 _   as-admin-https                          2010  udp
 _   as-central                             8470  tcp
 _   as-central-s                           9470  tcp
 _   as-database                            8471  tcp
 _   as-database-s                          9471  tcp
 _   as-debug                               4026  tcp
 _   as-dtaq                                8472  tcp
 _   as-dtaq-s                              9472  tcp
                                                              More...
Parameters for options 1 and 4 or command
===>
F3=Exit    F4=Prompt    F5=Refresh    F6=Print list    F9=Retrieve    F12=Cancel
F17=Top    F18=Bottom
```

3. Select the option to add details for a service entry and enter the required values. The SecurID defaults are:

```
Service = “securid”
Port = “5500”
Protocol = “udp”
Text  = “SecurID authentication”
```

4. Install/apply SecurID configuration file, sdconf.rec.

   - Obtain a copy of the appropriate **sdconf.rec** from the Authentication Manager Administrator.
   - Log on the IBM i LPAR host with an ftp client, using the ALERT profile.
   - Copy the **sdconf.rec** file to **/var/ace/.**
   - For example:

```
ftp <%IBM i LPAR%>
bin
cd /
put   < sdconf.rec >  /var/ace/sdconf.rec
quit
```

5. Configure the TCP/IP connection for the DetectIT server.

   - Sign on to IBM i LPAR using the ALERT profile.
   - Run the **WRKDTICFG** command.
   - Click the **F6** key to add a product.
   - Select **SECURID** in the product list.

```
MSPT5961                                                        6/11/13
                    Product selection screen (TCP/IP)           09:22:02

                                      Position to product . . . . _________
Type options, press Enter
  1=Select

Opt   Product       Port    Description
__    DTIGEN        07880   General Server
__    RMTSDIAUT     07878   SecurID authentication for remote access
1_    SECURID       15500   SecurID authentication main server

F3=Exit    F5=Refresh    Enter=Continue    Roll
```

   - Enter/accept the port number.

> **Important: The port number entered here will be used by the requesting user's job to connect to the DetectIT server, ALERTDS06. This port should not be confused with the one used by the actual RSA Authentication Manager server.**

   - Click the Enter key on each remaining screen.

6. Start the DetectIT server for RSA SecurID.

   - Sign on to IBM i LPAR using the ALERT profile.
   - Use STRDTISVR if the DetectIT subsystems (ALERT and TIMPGM) are currently active, and STRALERT if they are not.

> **Important: The DetectIT server for RSA SecurID job runs in the TIMPGM subsystem under the name ALERTDS06.**

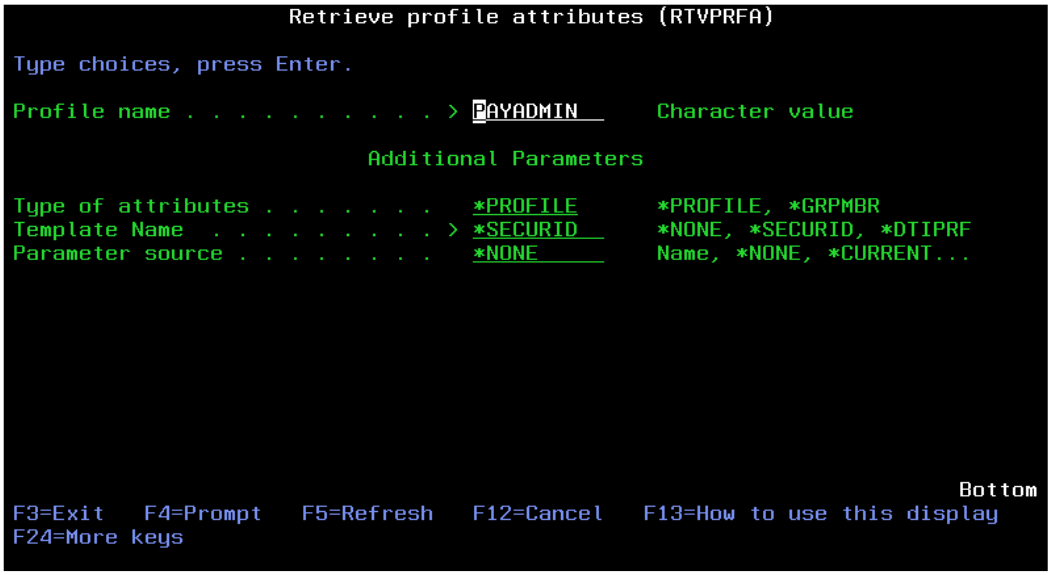
7. Configure native and/or remote authentication types. As mentioned above, this integration supports both types of integration for IBM i:

   - **Native** authentication for users working within the traditional 5250 screen environment.
   - **Remote** authentication for client/server-based requests such as FTP.

Both types can be configured using either the DetectIT interface or the ATHPRF command.

- The following steps outline how to configure DetectIT to provide native authentication:
  - Sign on to IBM i LPAR using the ALERT profile.
  - Prompt the RTVPRFA command using the F4 key followed by F9 key.
  - Enter the required profile name.
  - Enter ***SECURID** as the template name.

> **Important: It is most likely that programming changes will need to be made in order to have run ATHPRF with external routines.**



- The following steps outline how to configure DetectIT to provide remote authentication:
  - Sign on to IBM i LPAR using the ALERT profile.
  - Run the **WRKDTITCP** command.
  - Click the **F6** key to add a product.
  - Select ***RMTSDIAUT*** from the product list.

```
MSP5961     0000              Safestone Technologies                25/03/10
                      Product selection screen (TCP/IP)               15:58:13

                                        Position to product . . . .  _________
Type options, press Enter
  1=Select

Opt    Product        Port    Description
1_     RMTSDIAUT      07878   SecurID authentication for remote access
__     SECURID        15500   SecurID authentication main server
__     SSC            07871   TCP/IP port for link to SSC

F3=Exit     F5=Refresh     Enter=Continue     Roll
```

- Enter/accept the port number.
- Using the **Work With Client App. Availability** menu option, set the **Authentication requests** parameter to one of the following values:
  - Enter ***S*** to authenticate only those profiles configured for SecurID authentication.
  - Enter ***A*** to authenticate all profiles that attempt to use the client/server application.

```
MSP7852     0000              Safestone Technologies                25/03/10
                      Maintain PC Support Availability Header

                                                                     Amend
Enter detail below, and select the appropriate action.

Exit Point Name  . . . . . : QIBM_QTMF_SVR_LOGON
Exit Point Format  . . . . : TCPL0100
Application Name . . . . . : *FTPSLOG   FTP Server Logon - TCPL0100

Availability Criteria  . . . . *ALL    *ALL, *DEF
Monitor Client Requests  . . . 2       0 = Unsuccessful Requests Only
                                       1 = Successful Requests Only
                                       2 = Both Unsuccessful/Successful Reqs.
Request Checking Type  . . . . 2       ' '=Profile Only, '1'=IP Only, '2'=Both
Authentication requests  . . . S       Blank = No authentication
                                           A = Authenticate all profiles
                                           S = Authenticate specific profiles
Bypass Generic Checking? . . . _       ' '=Do not bypass, 'Y'=Bypass
Exit point processing program. _________
Library  . . . . . .  _________

    Enter=Continue       F23=Delete          F12=Cancel
```

- Ensure that all of the appropriate profiles and TCP/IP authorities are configured for the client/server application.
- Ensure that DetectIT Client / Server checking has been activated.
- Using the **Client/Server & Internet Control** menu option entitled **Maintain Remote Authentication**, select the profiles that are to be challenged for remote authentication.
- The following steps outline how to configure DetectIT Agent for RSA SecurID to provide remote authentication:

Important: Profiles configured for Native authentication will also be challenged for Remote authentication.

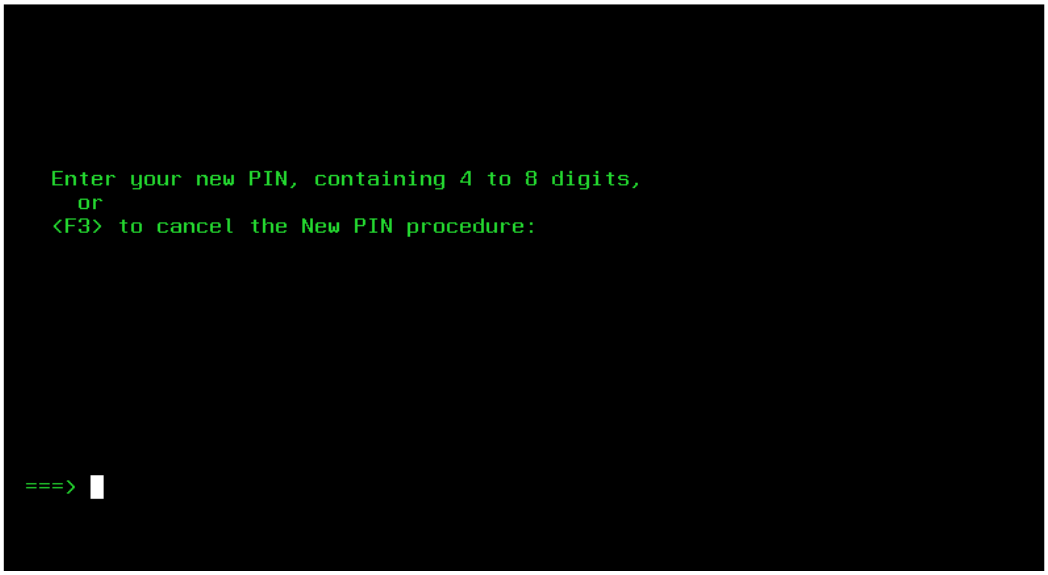
Important: For Remote Authentication, additional software must be installed on the Windows PC / laptop to be used to make the remote access. Please refer to the DetectIT Interfaces Guide, see the Section entitled, "Installing DetectIT Remote Authentication for AS/400".

RSA SecurID Login Screens

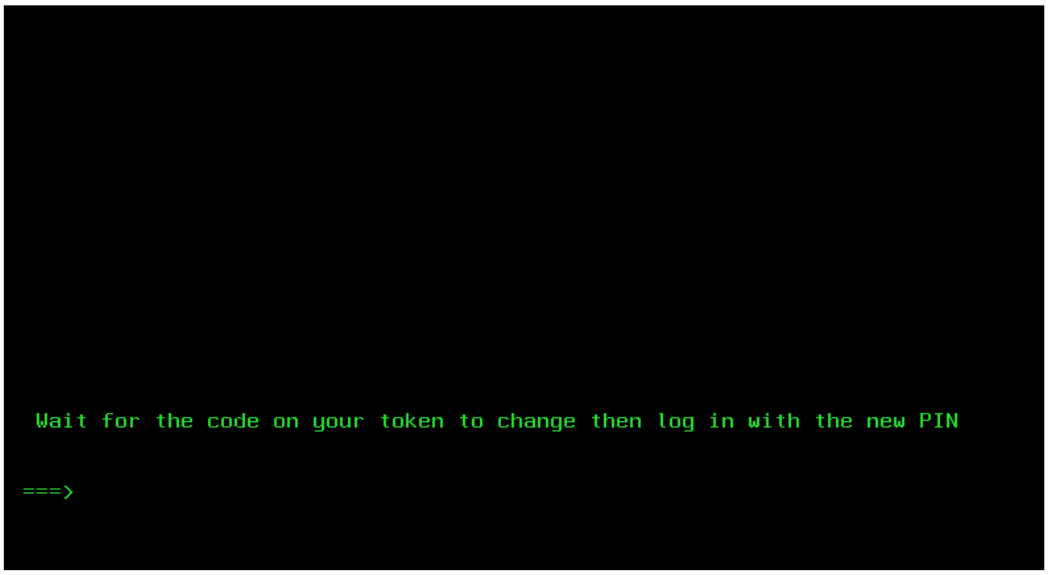
Native Authentication

Login screen:

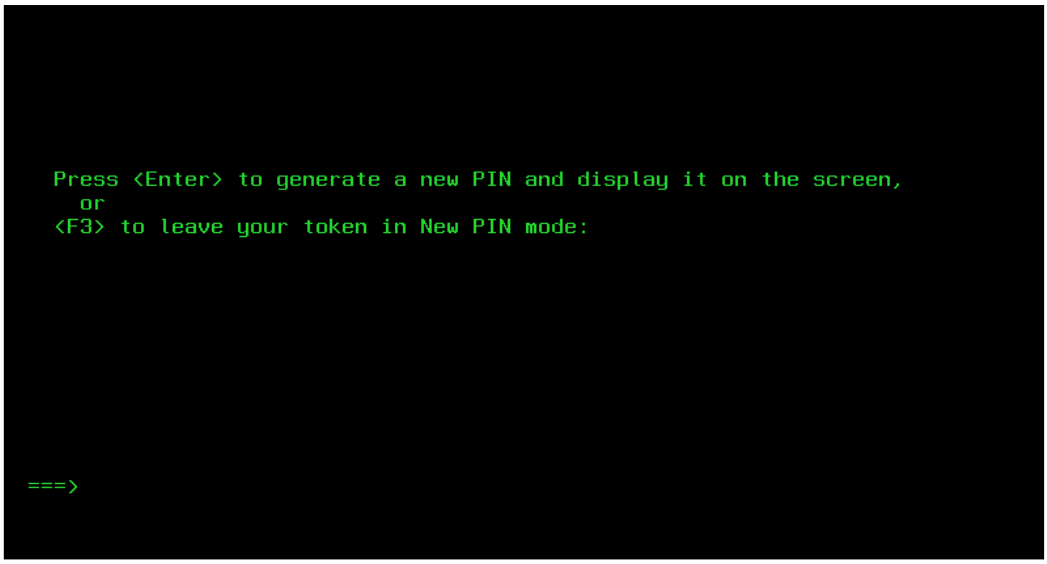
User-defined New PIN:

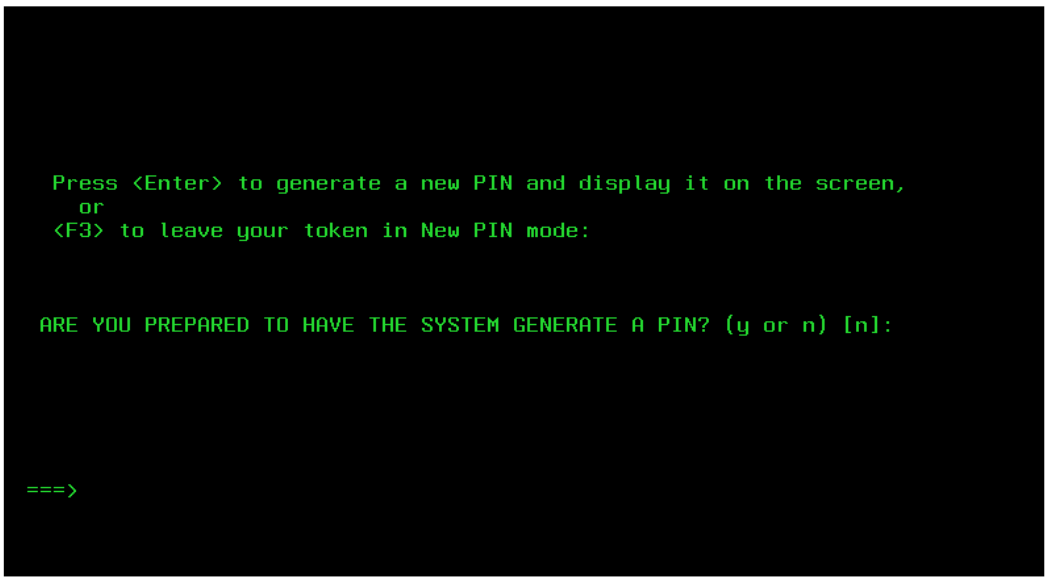


User-defined New PIN (Continued):

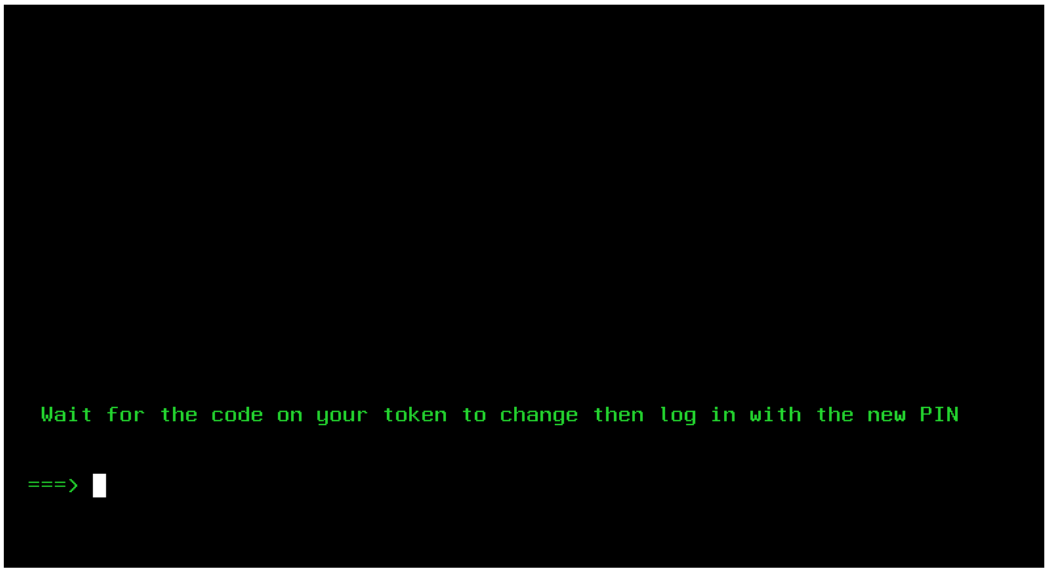


System-generated New PIN:





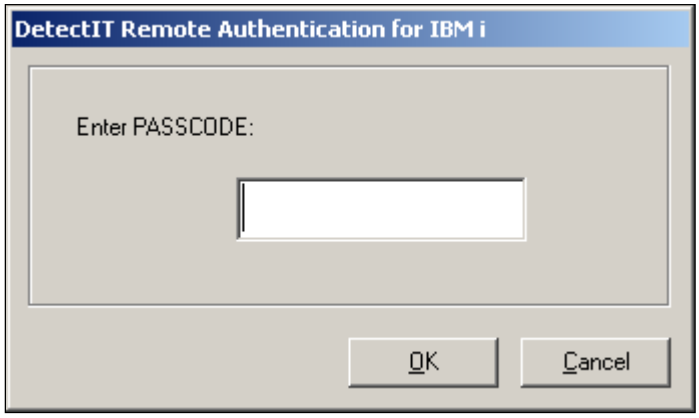
System-generated New PIN (Continued):



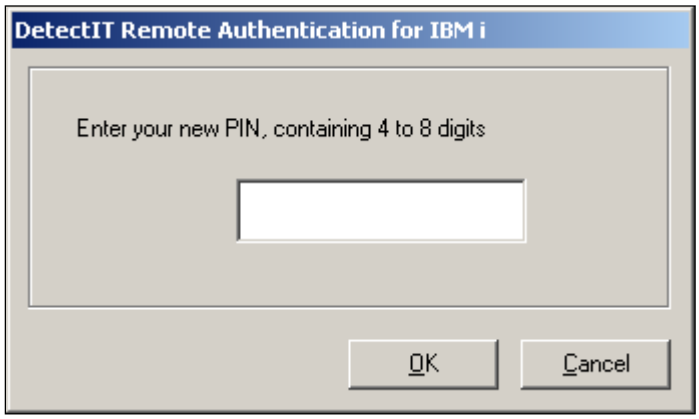
Next Tokencode:

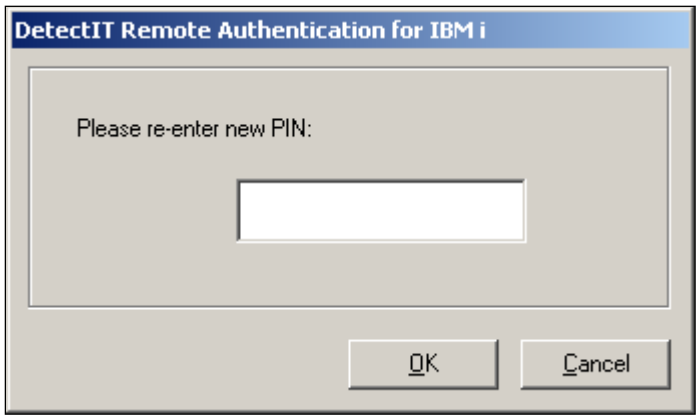
Remote Authentication

Login screen:

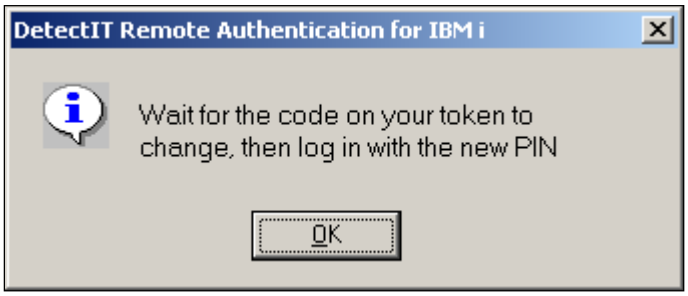


User-defined New PIN:



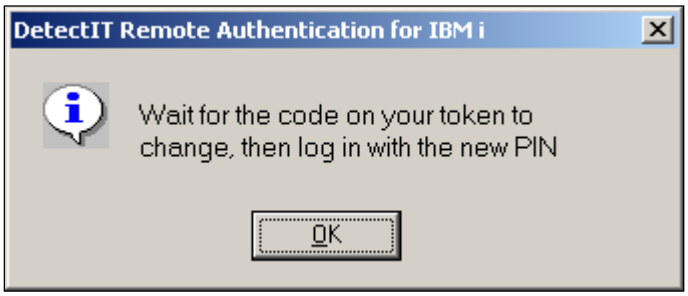


User-defined New PIN (Continued):

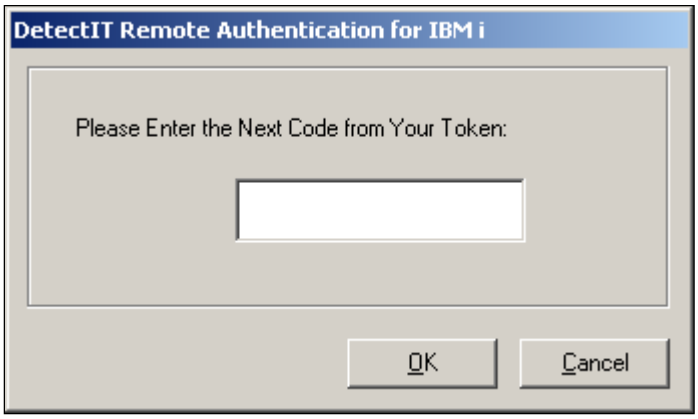


System-generated New PIN:

System-generated New PIN (Continued):



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: April 16, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
RSA Authentication Agent	Standard Agent	IBM i
RSA Software Token	N/A	N/A
RSA Remote Authentication Client	N/A	N/A
DetectIT Security Manager	14.4.6	IBM i

RSA SecurID Authentication

Date Tested: April 15, 2016

Mandatory Functionality	Native UDP	Native TCP	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	✓	N/A	N/A
System Generated PIN	✓	N/A	N/A
User Defined (4-8 Alphanumeric)	✓	N/A	N/A
User Defined (5-7 Numeric)	✓	N/A	N/A
Deny 4 and 8 Digit PIN	✓	N/A	N/A
Deny Alphanumeric PIN	✓	N/A	N/A
Deny PIN Reuse	✓	N/A	N/A
Passcode			
16 Digit Passcode	✓	N/A	N/A
4 Digit Fixed Passcode	✓	N/A	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	N/A	N/A
On-Demand Authentication			
On-Demand Authentication	✓	N/A	N/A
On-Demand New PIN	✓	N/A	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	N/A	N/A
No RSA Authentication Manager	✓	N/A	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

Installing / upgrading DetectIT 'objects' within Portable Application Solutions Environment (PASE).

Depending on the type of functionality required by DetectIT users, it may be necessary to perform a DetectIT upgrade on the IBM i system in "Restricted State". Unfortunately, this means it is not possible for the upgrade routine to carry out any processing within PASE. In order to update PASE, the required processing is performed when the DetectIT subsystems (ALERT and TIMPGM) are started.

Therefore, after a DetectIT installation (or upgrade), it is recommended to start and then end the DetectIT subsystems to ensure the required PASE directories and files exist:

- Sign on to IBM i LPAR using the ALERT profile.
- Run the STRALERT command.
- Run the ENDALERT command.

Using sdopts.rec

If sdopts.rec is created under the Windows Operating System, each entry will have 'carriage return / line feed' combination at the end i.e. characters X'0D' and X'0A' respectively. This ending combination should be avoided by configuring sdopts.rec directly within IBM Portable Application Solutions Environment (PASE). The AIX 'echo' command can be used to provide the correct syntax.

For example:

```
echo "CLIENT_IP=172.28.52.27" > /var/ace/sdopts.rec
```

Important: The echo command must be run within IBM PASE. Do NOT use IBM QSHELL / QSH.

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	/var/ace/sdconf.rec
sdopts.rec	/var/ace/sdopts.rec
Node secret	/var/ace/securid
sdstatus.12 / jastatus.12	/var/ace/sdstatus.12

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	Custom Build based on 5.0.3 (AIX)
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No but can display contents of sdconf.rec
Perform Test Authentication	No
Agent Tracing	Yes

API Details:

The SecurID related files (sdconf.rec, Node secret, sdstatus.12 and sdopts.rec) are all processed, by DetectIT, from within the Portable Application Solutions Environment (PASE). If needed, there are a number of ways to manually remove these files. They are:

- Run the IBM i **WRKLNK OBJ('/var/ace/*')** command.
- By accessing PASE and calling AIX commands such as **cd, rm**, etc.
- Using a mapped drive on a PC that has access to the /var/ace/ directory within the IBM i Integrated File System (IFS).

The DetectIT CLNTCHK command can be used to review the configuration details stored within sdconf.rec. To run the command:

1. Sign on to IBM i LPAR using the ALERT profile.
2. Run the **CLNTCHK** command.

> **Important: If the DetectIT Security Manager Agent for RSA SecurID had been used prior to the compatible release for Authentication Manager 8.1, it is possible that an earlier version of sdconf.rec may still exist on the system. When the CLNTCHK command is run, it will display the details from all versions of sdconf.rec that are available.**

Node Secret:

/var/ace/securid

sdconf.rec:

/var/ace/sdconf.rec

sdopts.rec:

/var/ace/sdopts.rec

sdstatus.12:

/var/ace/sdstatus.12

Agent Tracing:

1. Sign on to the IBM i LPAR using the ALERT profile
2. Ensure the IBM syslog daemon, syslogd is running within PASE.

This can be done by accessing PASE and running the AIX **ps –ef | grep /usr/sbin/syslogd** command.

If this daemon is NOT running:

- Run the **WRKDTITCP** command.
- Click the **F6** key to add a product.
- Select **SYSLOGD** from the product list.
- Accept the default port number.
- Click the Enter key on each remaining screen.

> **Important: When the syslog daemon is configured to run via DetectIT, it runs under a job in the TIMPGM subsystem, named ALERTDS07.**

Add RSA SecurID related environmental variables at the system (*SYS) level:

- RSATRACEDEST

```
ADDENVVAR ENVVAR(RSATRACEDEST) VALUE('/< Your_Directory_Path >/< Your_File >')
LEVEL(*SYS)
```

Where:

- < Your_Directory_Path > full path within the Integrated File System (IFS)
- < Your_File > name of your log/trace file

> **Important: < Your File > must exist for the trace processing to generate output into the file.**

- RSATRACELEVEL

```
ADDENVVAR ENVVAR(RSATRACELEVEL) VALUE('< Trace_Level_Value >') LEVEL(*SYS)
```

Where:

< Trace_Level_Value > numeric value for one of the following:

SDITRACEING_OFF	00000000
SDITRACEING_ON	00000001
SDITRACEING_ENTRY	00000002
SDITRACEING_EXIT	00000004
SDITRACEING_FLOW	00000008

End and re-start the DetectIT server for RSA SecurID

- Run the **ENDALERT** command.
- Run the **STRALERT** command.