Safestone Technologies Limited

Safestone Agent for RSA SecurID

RSA SecurID Ready Implementation Guide

Last Modified: March 26, 2014

Partner Information

Product Information	
Partner Name	Safestone Technologies Limited
Web Site	www.safestone.com
Product Name	Safestone Agent for RSA SecurID
Version & Platform	V 9.8 IBM i on Power Systems (IBM i)
Product Description	Two factor user identification and authentication providing enhanced security, ensuring that access to sensitive data is protected both at sign-on, on demand and when accessed via the network.

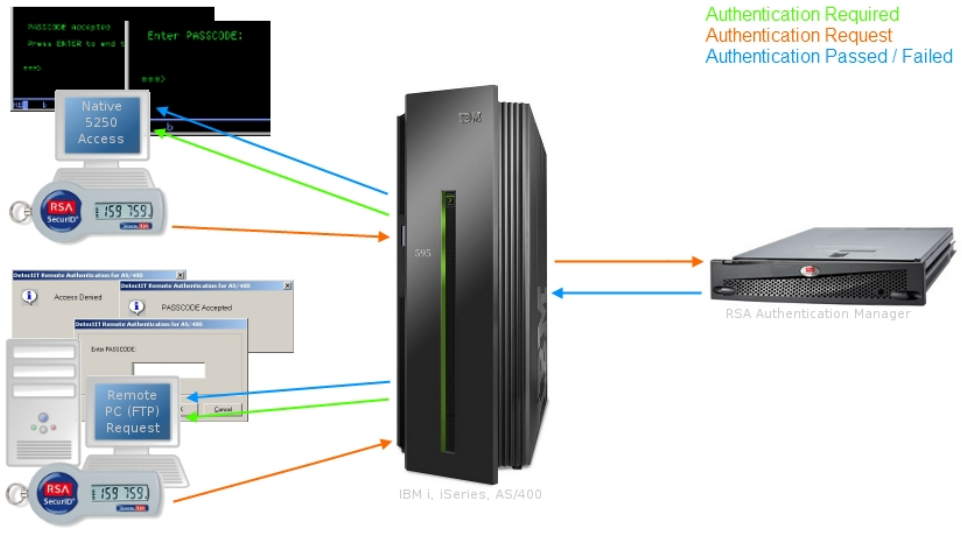
Solution Summary

The Safestone 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 Safestone 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.

Safestone Agent for RSA SecurID 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 Agent for SecurID 9.8	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	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



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

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 Safestone Agent for RSA SecurID will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	/var/ace/sdconf.rec
Node Secret	/var/ace/securid
sdstatus.12	/var/ace/sdstatus.12
sdopts.rec	/var/ace/sdopts.rec

Note: The appendix of this document contains more detailed information regarding these files.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Safestone Agent for RSA SecurID 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 Safestone Agent for RSA SecurID components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

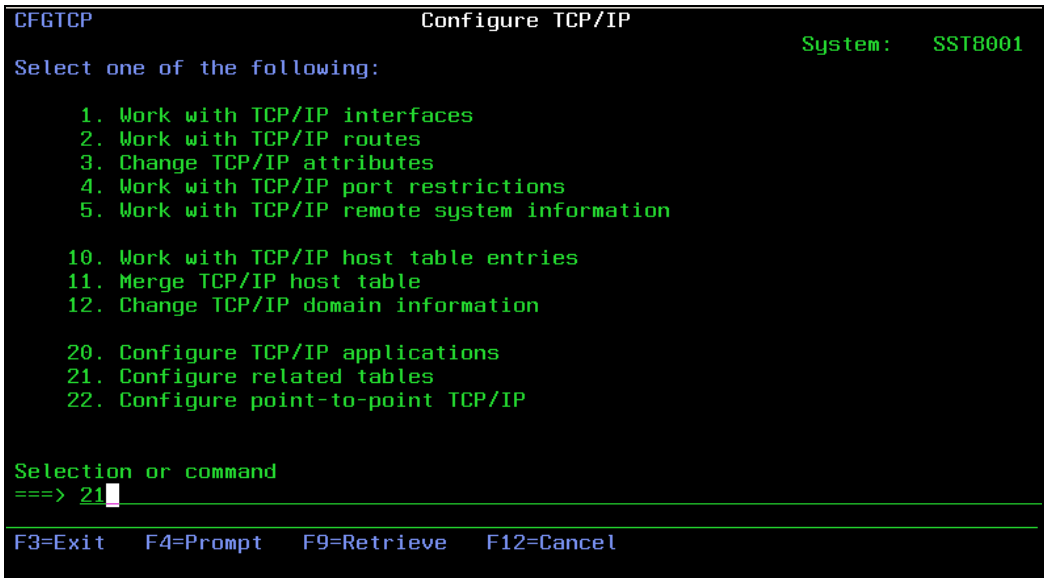
Configure Safestone Agent for RSA SecurID and IBM i LPAR for RSA SecurID Authentication

1. Install/upgrade Safestone Agent for RSA SecurID as outlined within the Safestone Agent for RSA SecurID Deployment instructions.

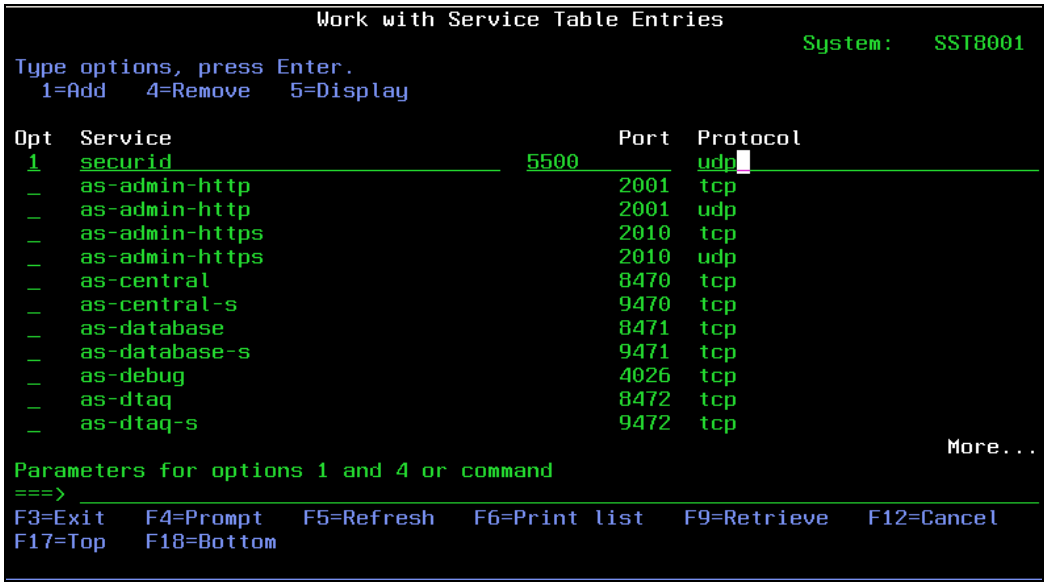
   Note: Refer to the Deployment Guide for further details.

2. Configure RSA SecurID Authentication service port.

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



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



- Select the option to **Add** details for a service entry and enter the required values. The RSA SecurID defaults are:
    - Service = "*securid*"
    - Port = "*5500*"
    - Protocol = "*udp*"
    - Text = "*SecurID authentication*"

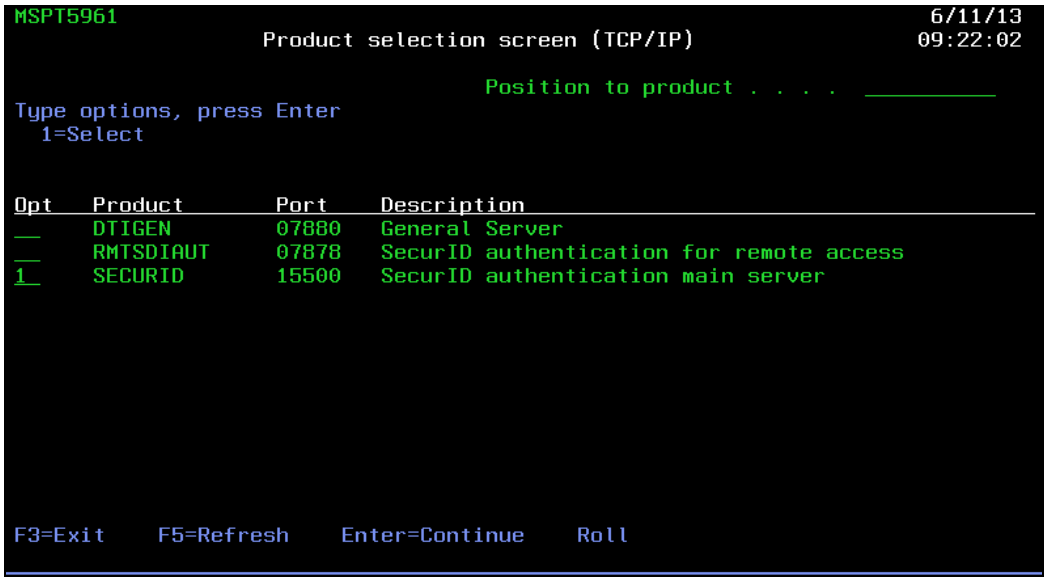
3. Install/apply RSA SecurID configuration file, **sdconf.rec.**

- 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 ACEDTI 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
```

4. Configure the TCP/IP connection for the Safestone Agent for RSA SecurID server for RSA SecurID.

   - Sign on to IBM i LPAR using the ACEDTI profile.
   - Select **Work with TCP/IP port connections**.
   - Click the **F6** key to add a product.
   - Select **SECURID** in the product list.



   - Enter/accept the port number.

> **Important:** The port number entered here will be used by the requesting user's job to connect to the Safestone Agent for RSA SecurID server for RSA SecurID, ACEDTIDS01. 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.

5. Start the Safestone Agent for RSA SecurID server for RSA SecurID.

   - Sign on to IBM i LPAR using the ACEDTI profile.
   - Use **ENDACEDTI** if the ACEDTI subsystem is currently running.
   - Run the **STRACEDTI** command to start the subsystem.

> **Note:**The Safestone Agent for RSA SecurID server for RSA SecurID job runs in the ACEDTI subsystem under the name ACEDTIDS01.

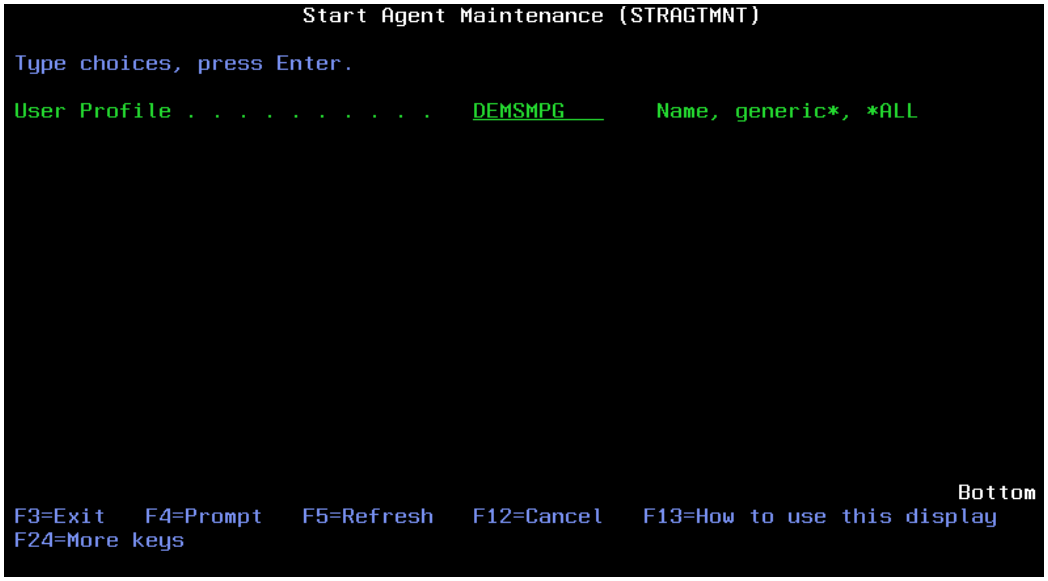
6. Configure native and/or remote authentication types. As mentioned above, this integration supports both types of integration for IBM i:

   - **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 Safestone Agent for RSA SecurID interface or the **ATHPRF** command.

- The following steps outline how to configure Safestone Agent for RSA SecurID to provide **native authentication**:
  - Sign on to IBM i LPAR using the ACEDTI profile.
  - Select **DetectIT Agent for SecurID Maintenance**.
  - Click **Enter** on the first screen**.**
  - Enter the required profile name or leave the default of ***ALL.**

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



- Use the **Position to Profile** prompt or scroll to the required profile**.**
- Select ***2=Activate*** against the required profile.

```
MSPT1041                                                        6/11/13
                  Work with Profiles for DetectIT Agent         09:37:32

                                 Position to Profile  . . . . . _________
Type options, press Enter.
 2=Activate  4=Deactivate   5=Profile Details

Opt User Name  Grp Prf  SecurID  Description
2_  DEMSMPG    *NONE       N    A demonstration profile

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

```
MSPT1041                                                        6/11/13
                  Work with Profiles for DetectIT Agent         09:37:32

                                 Position to Profile  . . . . . _________
Type options, press Enter.
 2=Activate  4=Deactivate   5=Profile Details

Opt User Name  Grp Prf  SecurID  Description
__  DEMSMPG    *NONE       Y    A demonstration profile

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

- The following steps outline how to configure Safestone Agent for RSA SecurID to provide **remote authentication**:
    - Sign on to IBM i LPAR using the ACEDTI profile.
    - Select **Work with TCP/IP port connections**.
    - Click the **F6** key to add a product.
    - Select "***RMTSDIAUT***" from the product list.

```
MSPT5961                                                        6/11/13
                  Product selection screen (TCP/IP)             09:45:36

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

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

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

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

```
MSPT7852                                                        6/11/13
                    Maintain PC Support Availability

                                                                 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

Authentication requests  . . . S      Blank = No authentication
                                          A = Authenticate all profiles
                                          S = Authenticate specific profiles
Exit point processing program. __________
Library  . . . . . .  __________

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

- Ensure that Safestone Agent for RSA SecurID Client / Server checking has been activated.

> **Note:** Profiles configured for Native authentication will also be challenged for Remote authentication.

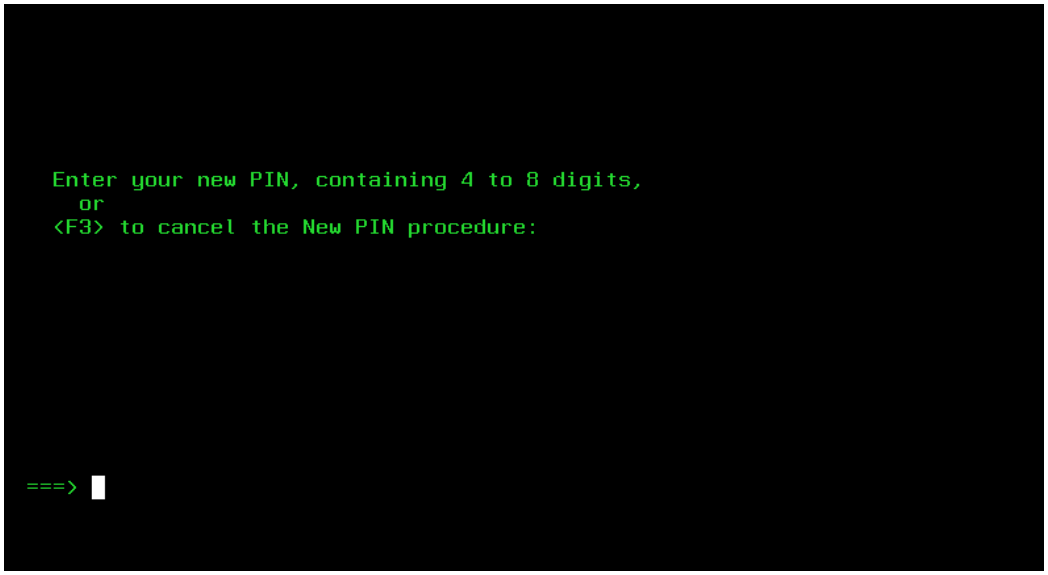
> **Important:** For Remote Authentication additional software must be installed on the Windows PC / laptop to be used for remote access. Please refer to the Deployment Guide, see the Section entitled,"Installing the Remote Authentication Software".

RSA SecurID Login Screens

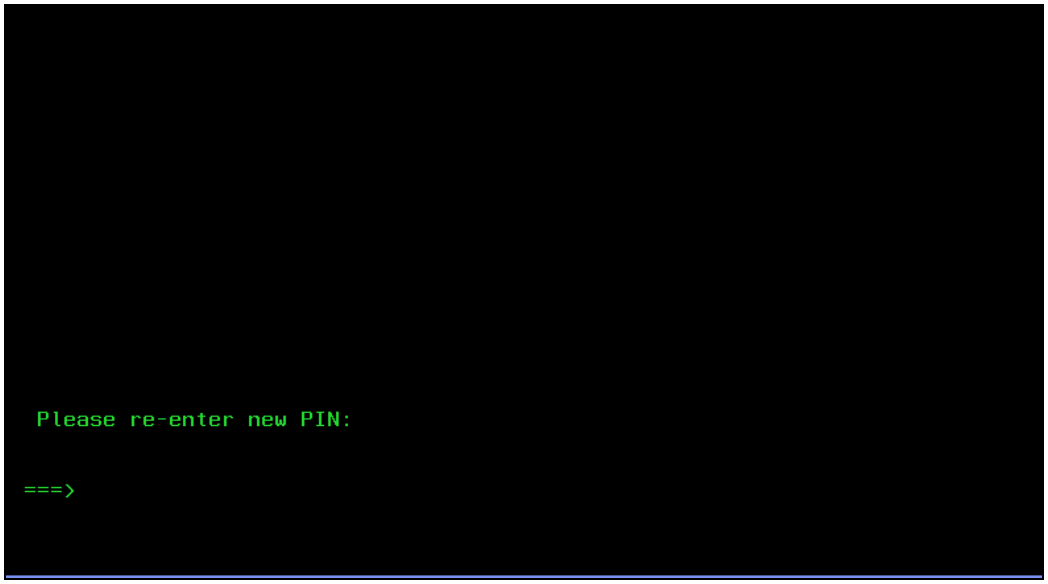
Native Authentication

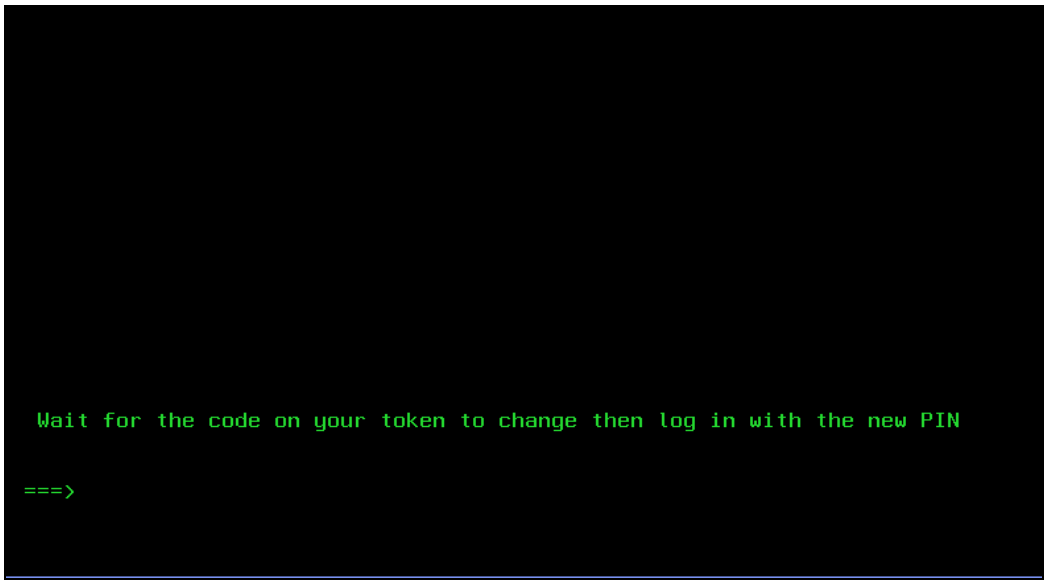
Login screen:

User-defined New PIN:

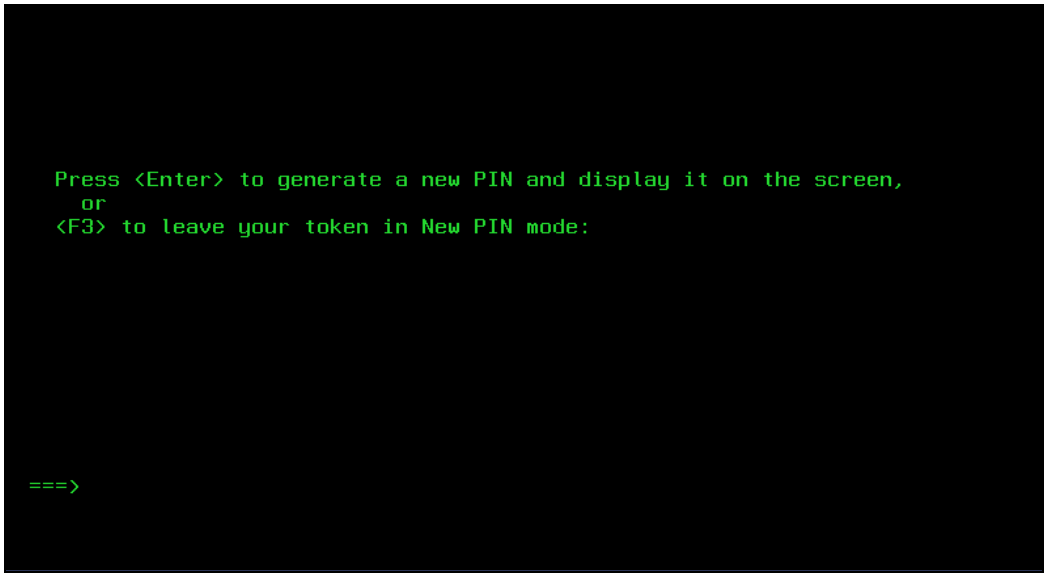


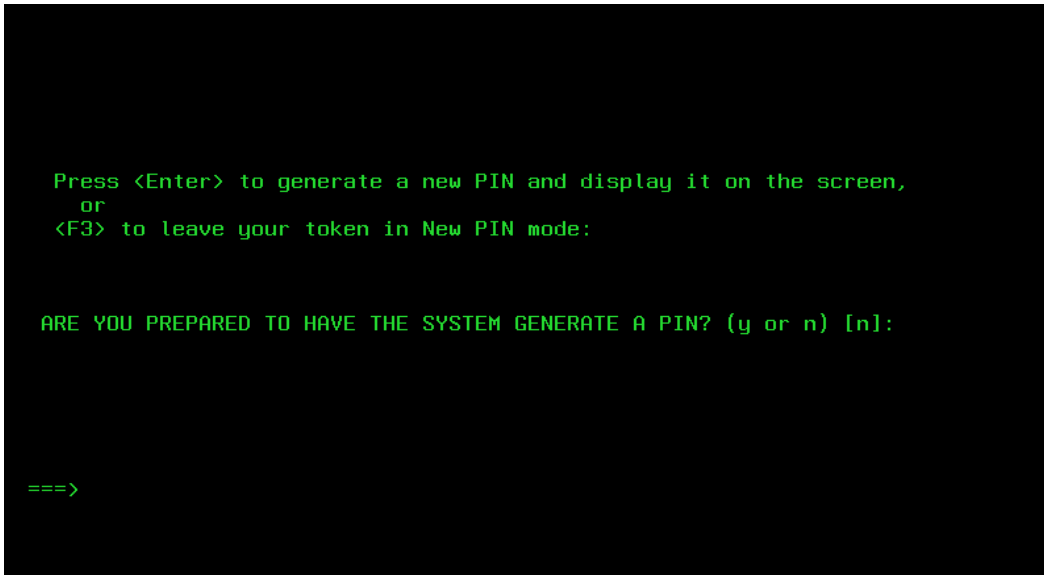
User-defined New PIN (Continued):



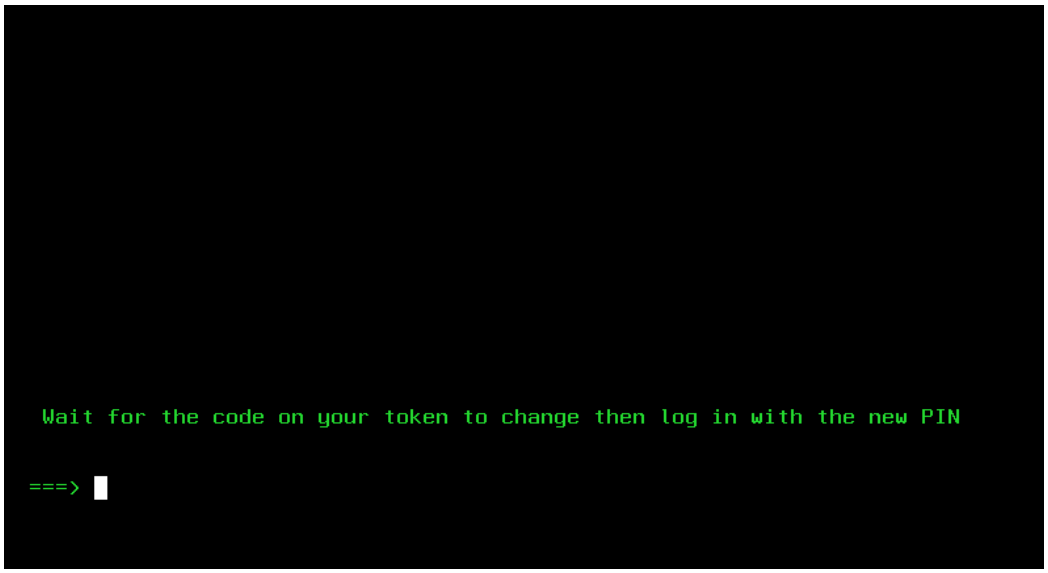


System-generated New PIN:

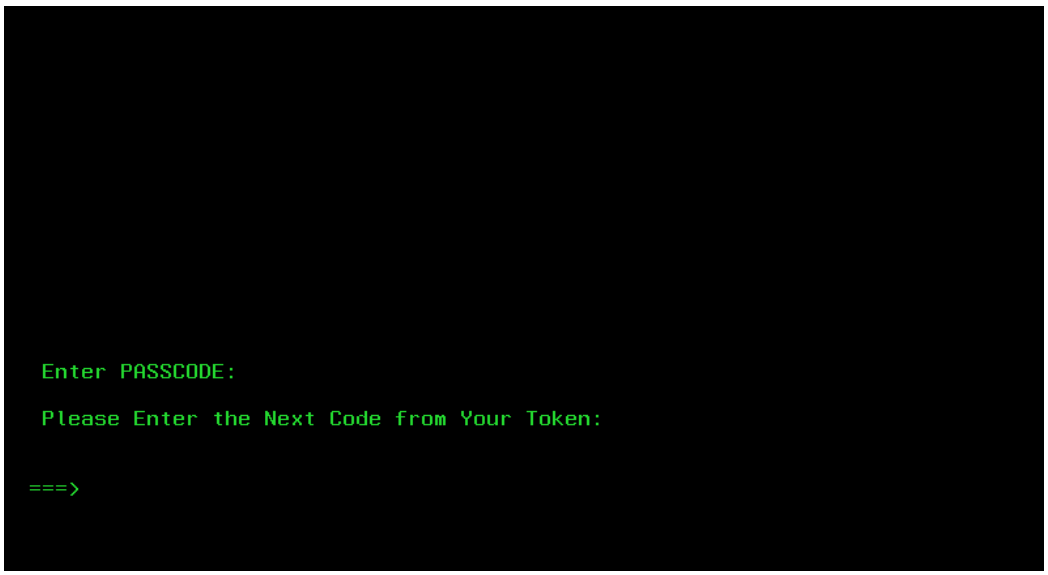




System-generated New PIN (Continued):

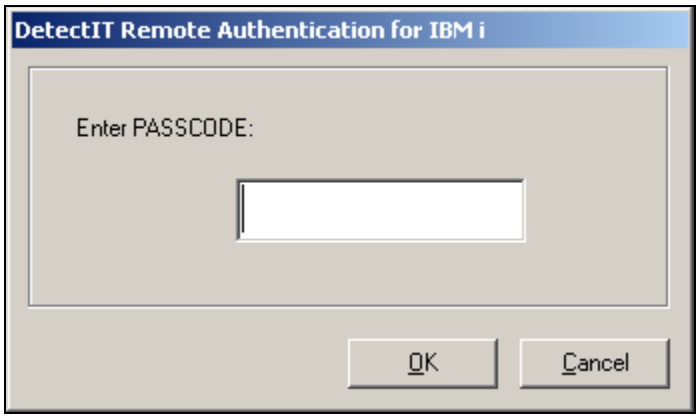


Next Tokencode:

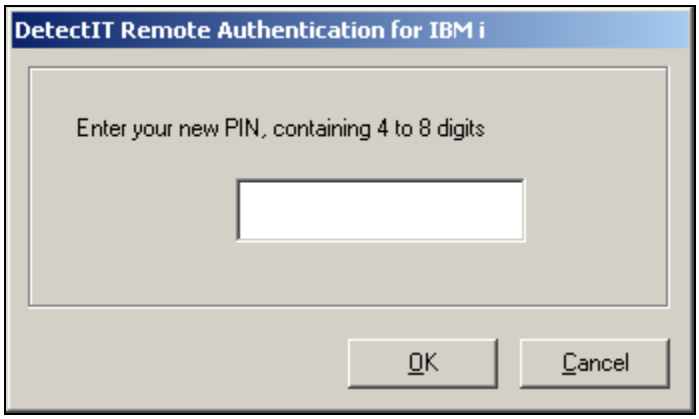


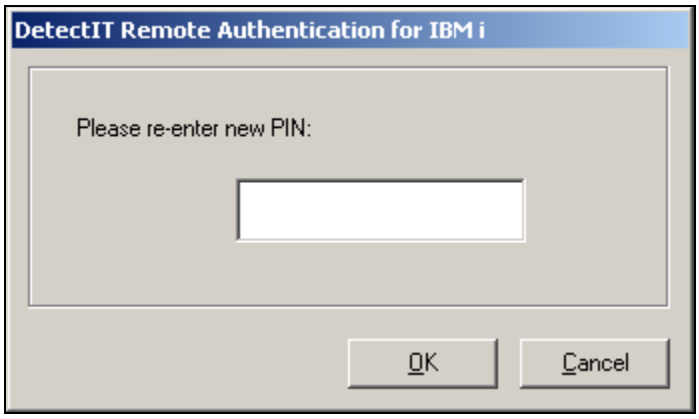
Remote Authentication

Login screen:

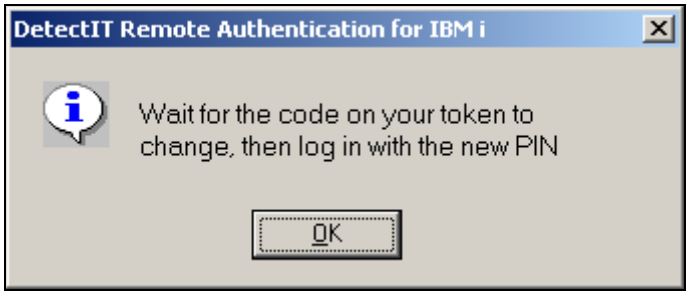


User-defined New PIN:

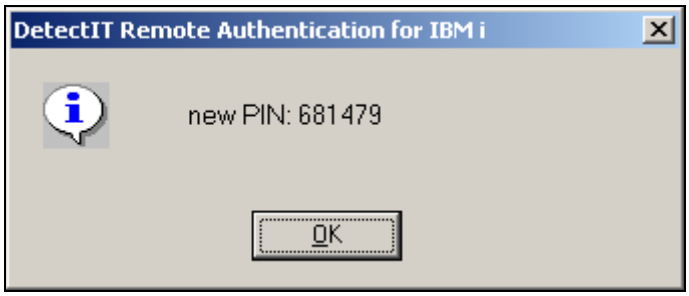




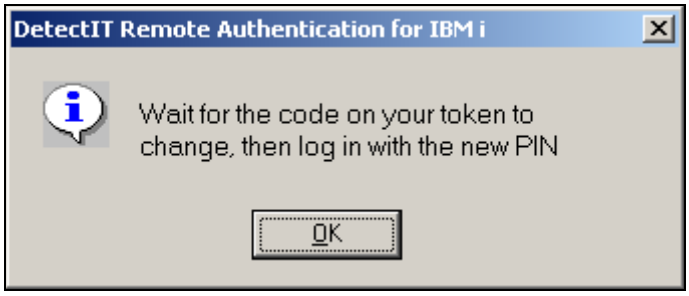
User-defined New PIN (Continued):



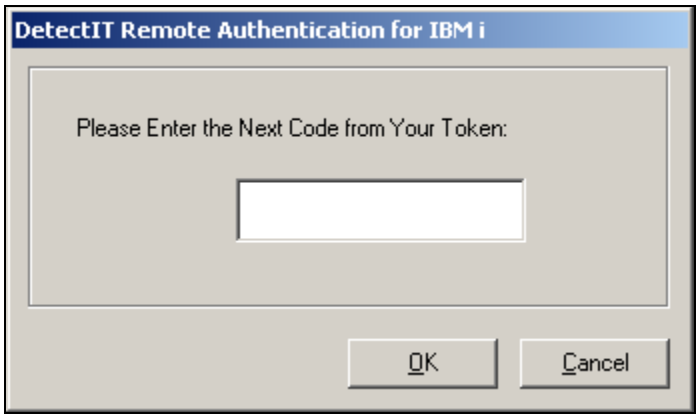
System-generated New PIN:



System-generated New PIN (Continued):



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: March 26, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
Safestone Agent for RSA SecurID	9.8	IBM i

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

DRP / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Known Issues

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

Partner Integration Details	
RSA SecurID API	5.0.3 (AIX)
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	Yes
Perform Test Authentication	No
Agent Tracing	Yes

RSA SecurID Files

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

- By calling the IBM i command:

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

- 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 Safestone Agent for RSA SecurID 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 ACEDTI profile.
2. Run the command:

```
CLNTCHK
```

Note: If the Safestone Agent for RSA SecurID had been used prior to the compatible release for RSA 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.