Voice Innovate

RSA SecurID Ready Implementation Guide

Last Modified: August 26, 2011

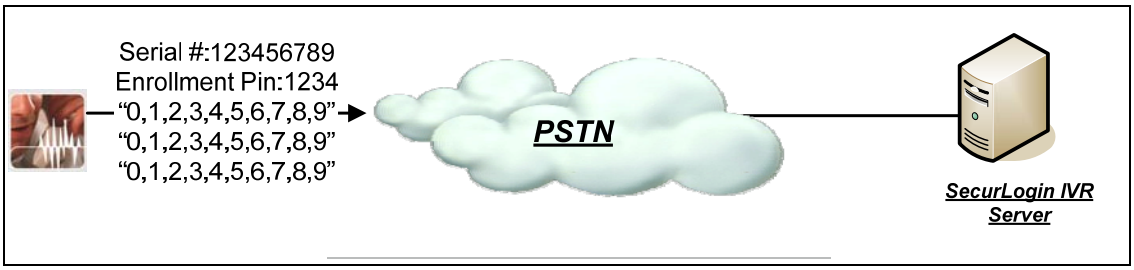
Partner Information

Product Information	
Partner Name	Voice Innovate
Web Site	http://voiceinnovate.com/
Product Name	SecurLogin
Version & Platform	SecurLogin V1.1, Supported on Windows Server 2003 R2
Product Description	The SecurLogin Application is intended to add a third factor of authentication to existing Smart Card login processes using Voice Biometrics. Users typically access a secured web page, provide their RSA SecurID credentials and then are prompted to call the SecurLogin IVR to perform voice authentication. Once voice authenticated, the user is then given access to the secured resource.

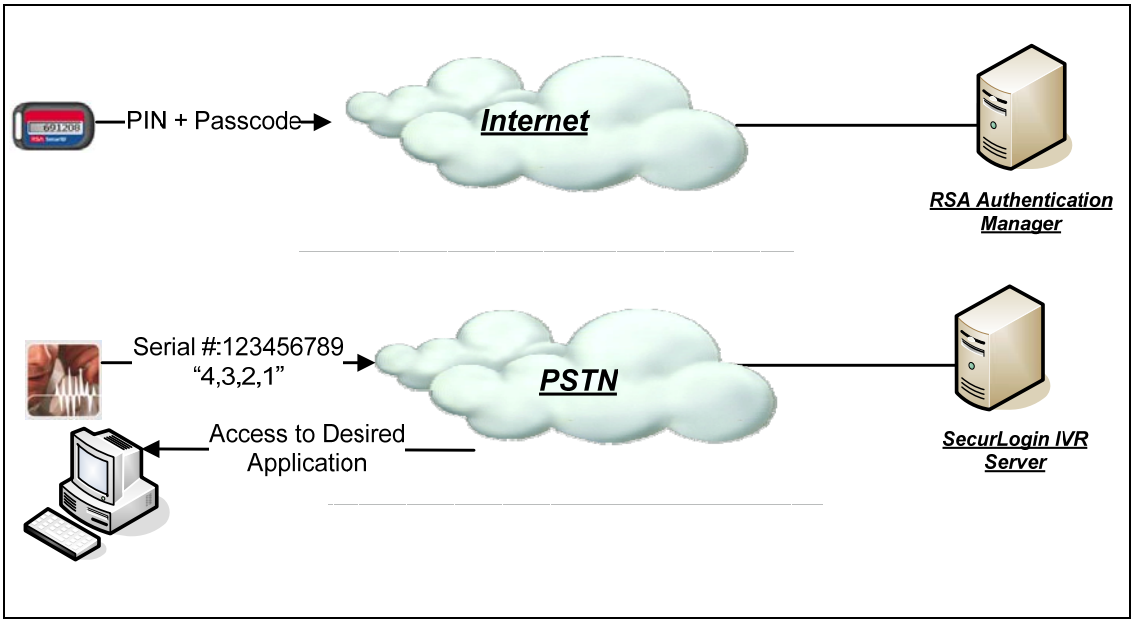
Solution Summary

Voice Innovate's SecurLogin adds a third factor of authentication to the standard RSA SecurID login processes using voice biometrics technology. Utilizing SecurLogin, existing RSA SecurID token users will be required to validate their respective identities with their biometric voice print after each successful SecurID authentication.

Once the system is in place, RSA SecurID token users will be instructed to dial in to an Interactive Voice Response (IVR) service to register their voice prints. The IVR service will prompt each user for his/her RSA SecurID token serial number and a RSA SecurID passcode. After a successful SecurID authentication, each user will be asked to repeat the numbers 0 through 9 to complete enrollment.



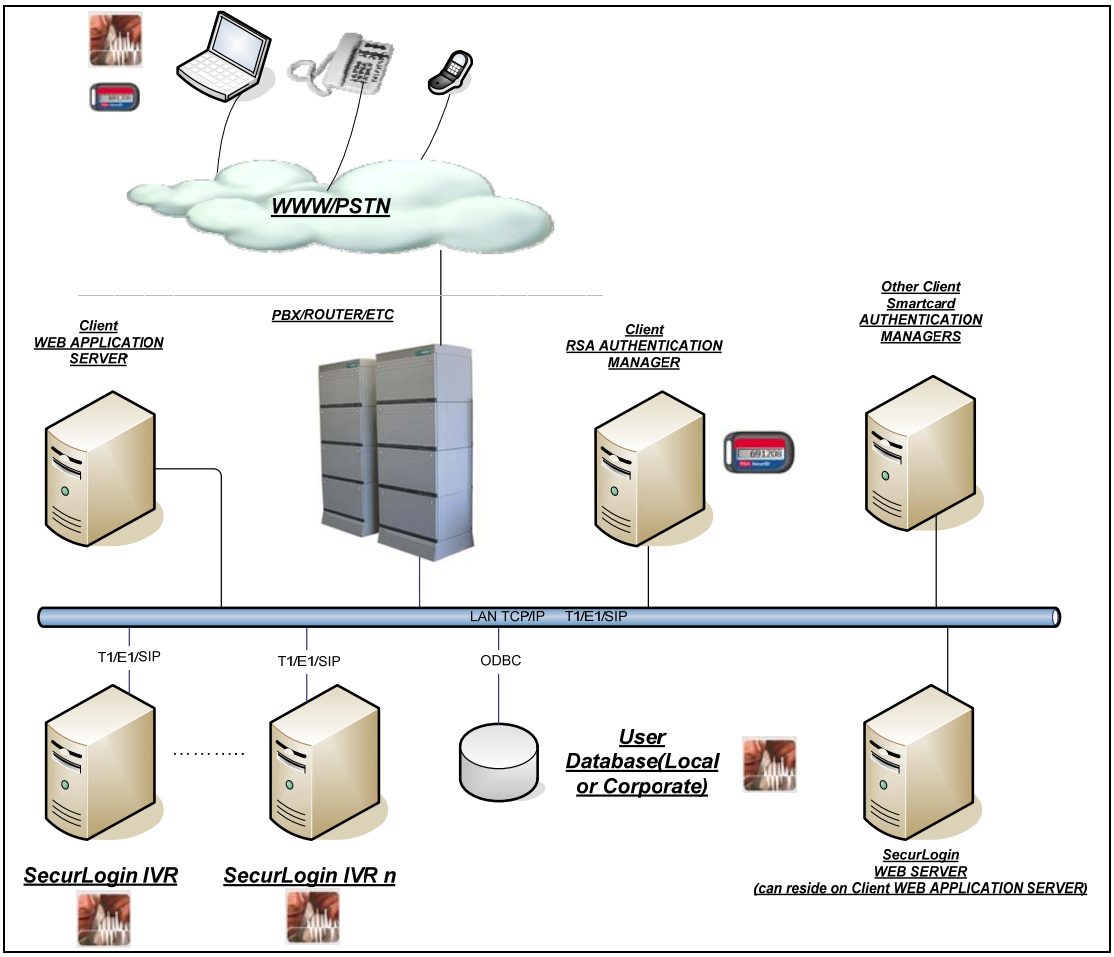
Once enrolled, users will be prompted to key in their PIN the RSA SecurID tokencode at the client's login screen as usual. After successfully completing this step, a page will appear with instructions to call an 800 number for voice authentication. When they dial in, users will be prompted to enter their respective token serial numbers and to repeat 4 or more random digits. SecurLogin will then use this voice sample to authenticate each enrolled user against the appropriate voice print. If successful, the user would be allowed to continue to the requested application. If the voice sample did not pass validation, the user would be denied access.



SecurLogin components are comprised of the following:

- **The SecurLogin Web Application** – an OpenID provider that hosts the SecurLogin web application. The Client Web Application's custom OpenID relying party component will rely on this server for authentication. The SecurLogin Web GUI permits users to authenticate with RSA SecurID and SecurLogin Voice Biometric authentications
- **The SecurLogin IVR** – an interactive voice response system that provides a telephony interface for voice biometric authentication.
- **The Client Web Application** – a client-supplied web application served via HTTP(s) protocol that delivers HTML content that will be protected by SecurLogin.
- **The User Database** – a MySQL database (not required if leveraging an existing corporate database).

The following diagram illustrates a sample deployment of SecurLogin within a corporate infrastructure.



Typically, the web servers and RSA Authentication Manager servers are part of the corporate infrastructure. The SecurLogin application provides the SecurLogin IVR and the mechanisms required to customize the corporate web server. A minimum of one SecurLogin IVR must be implemented, but multiple instances can be used to provide scalability for call volume, load balancing, and fault tolerance.

RSA SecurID supported features	
Voice Innovate SecurLogin V1.1	
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
On-Demand Authentication via API	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	No

Authentication Agent Configuration

Agent Host Records contain information that allows an RSA Authentication Manager server to locate its clients and establish secure communication channels with them. The server's database must contain Agent Host Records to identify the SecurLogin servers in a given environment. In order to create this record, the following information is required for each SecurLogin IVR server and the SecurLogin Web Application server instance:

- 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 SecurLogin 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	%SYSTEM32%\sdconf.rec
Node Secret	In Memory

Partner Product Configuration

Before You Begin

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

Prerequisites

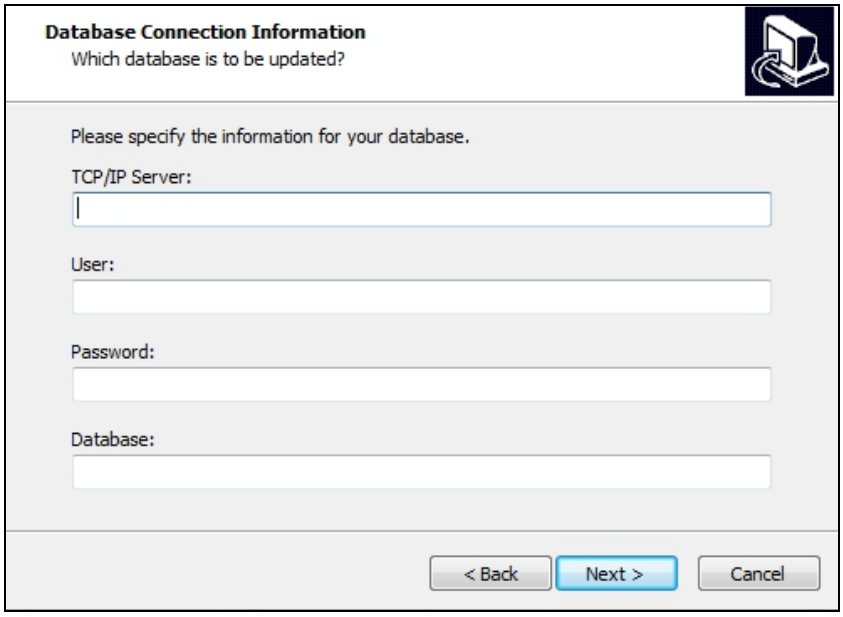
- Direct Inward Dial (DID) phone circuits that will be routed to the SecurLogin IVR server. The DID phone number will be used during the SecurLogin Web Application configuration.
- MySQL can be installed on any server but must be accessible by both the SecurLogin IVR and SecurLogin web applications.
- Windows 2003 R2 Server is required for the SecurLogin IVR application. An additional Windows 2003 R2 Server is required if the SecurLogin web application is to be housed on a standalone server.

Note: The RSA Authentication Manager Windows API library V6.1.3 is automatically installed during the SecurLogin Web Application and SecurLogin IVR installation procedures.

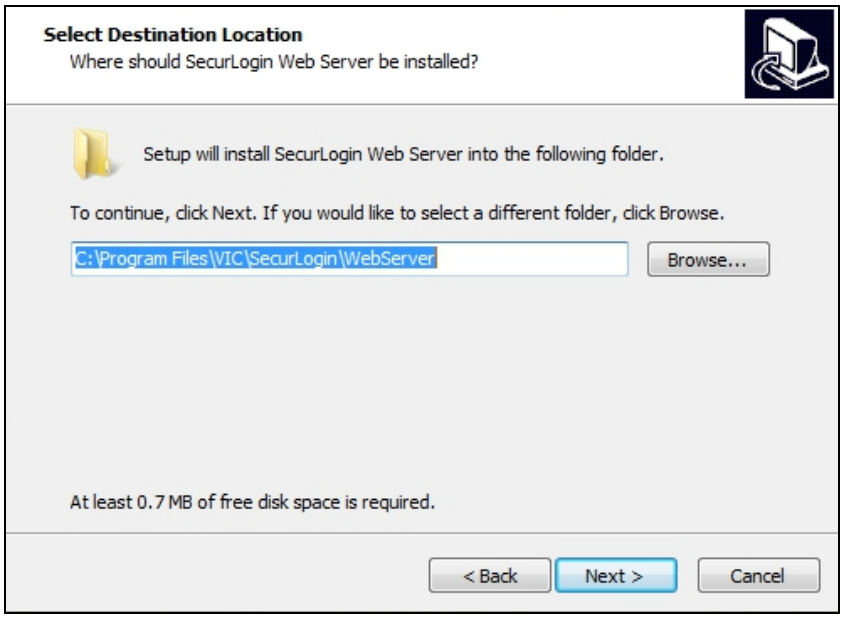
SecurLogin Web Application Installation

1. Launch the SecurLogin Web Server Installation program and click the **Next** button.

2. Enter the following information to create a SecurLogin MySQL database and click the **Next** button.
   - *TCP/IP Server*– the database server's host address
   - *User* – the database Administrator's username
   - *Password* – the above user's password
   - *Database* – a name for the SecurLogin database. Be sure that this name is unique.



3. Accept the default installation folder (or change it as required) and click the **Next** button.



4. Click the **Finish** button when the installation has completed.

SecurLogin Web Application Configuration

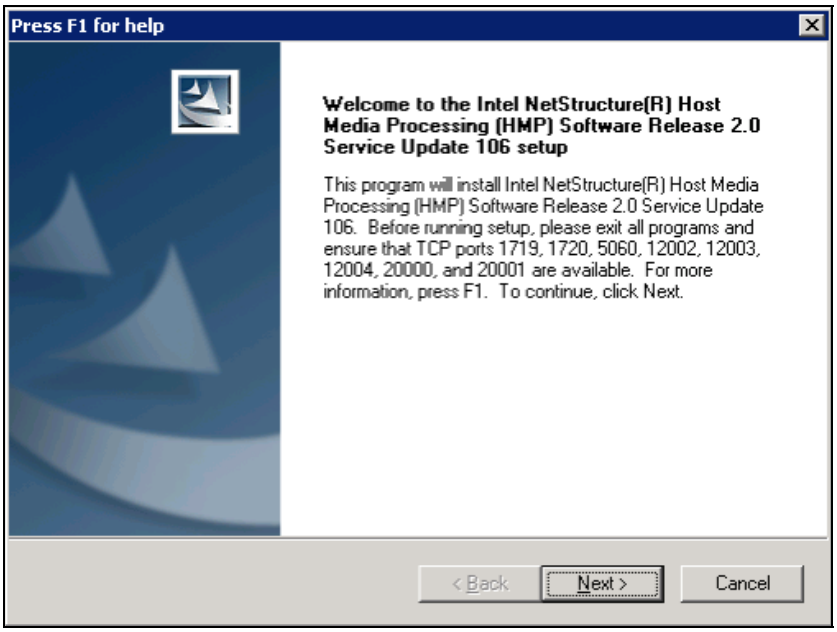
1. Open the SecurLogin web application's *config.ini* and modify the following variables to suit your configuration:
   - *host* and *port* – the host address and port that the SecurLogin web application is bound to
   - *server_url* – the fully-qualified domain name of the SecurLogin web page
   - *phone_auth* – the DID phone number that users will dial to access the SecurLogin IVR
   - *phone_reg* – the phone number that users will dial to enroll with SecurLogin. It can be the same as *phone_auth*.
   - *login_fail_wait* – the number of seconds between failed login attempts
   - *login_max_attempts* – the number of failed login attempts allowed before *log_max_wait* is applied
   - *login_max_wait* – the length of time a user must wait to log in again
   - *cache_dir* – the directory location that the SecurLogin Web Application will use for its cache
2. Open Services from the **Windows Control Panel** and start the **SecurLoginWeb** service.

Dialogic HMP (VoIp drivers) Installation

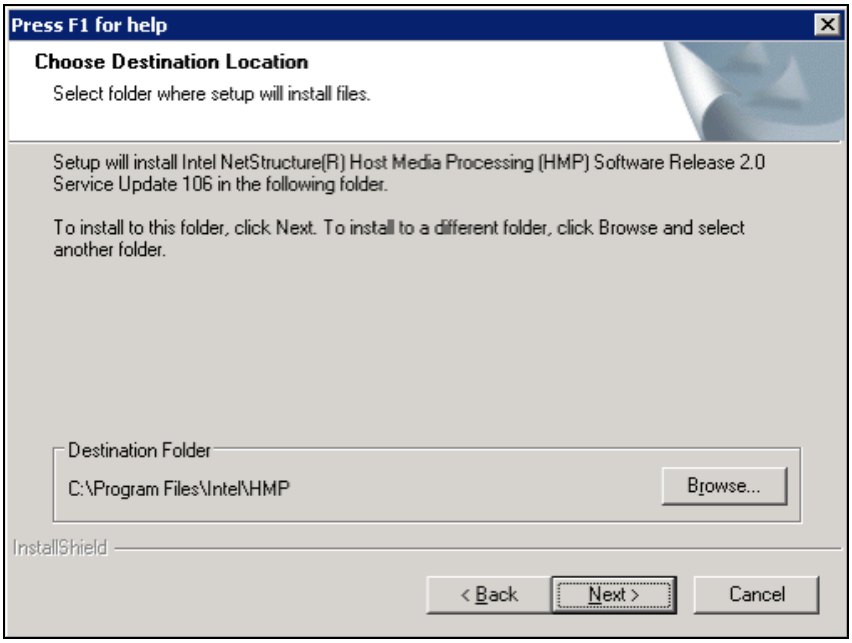
This section contains instructions for installing the Dialogic HMP VoIp drivers. At the time of this writing, the most current release of HMP is 3.0 Build 307. It can be obtained at the following link: **http://www.dialogic.com/products/ip_enabled/download/hmp30/default.htm**

Ensure that you have a valid HMP Software license file prior to proceeding. If you do not have a license, contact Voice Innovate.

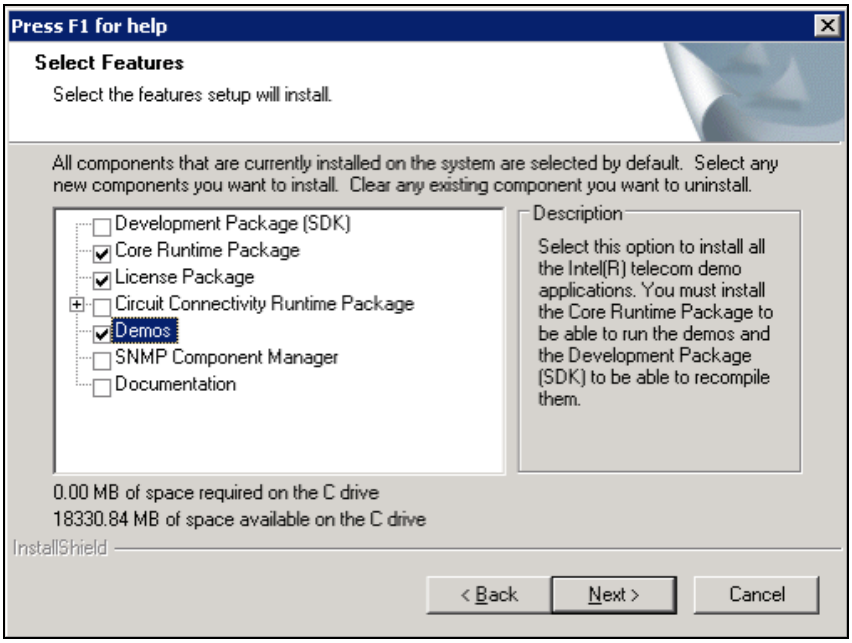
1. After obtaining the Dialog HMP drivers and license file, run the Dialogic installation program and click the **Next** button.



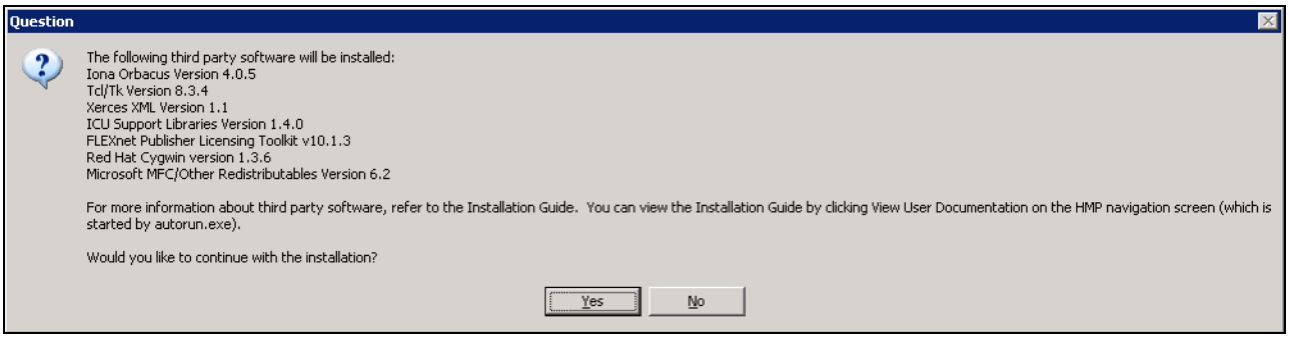
2. Accept the default installation folder (or change it as required) and click the **Next** button.



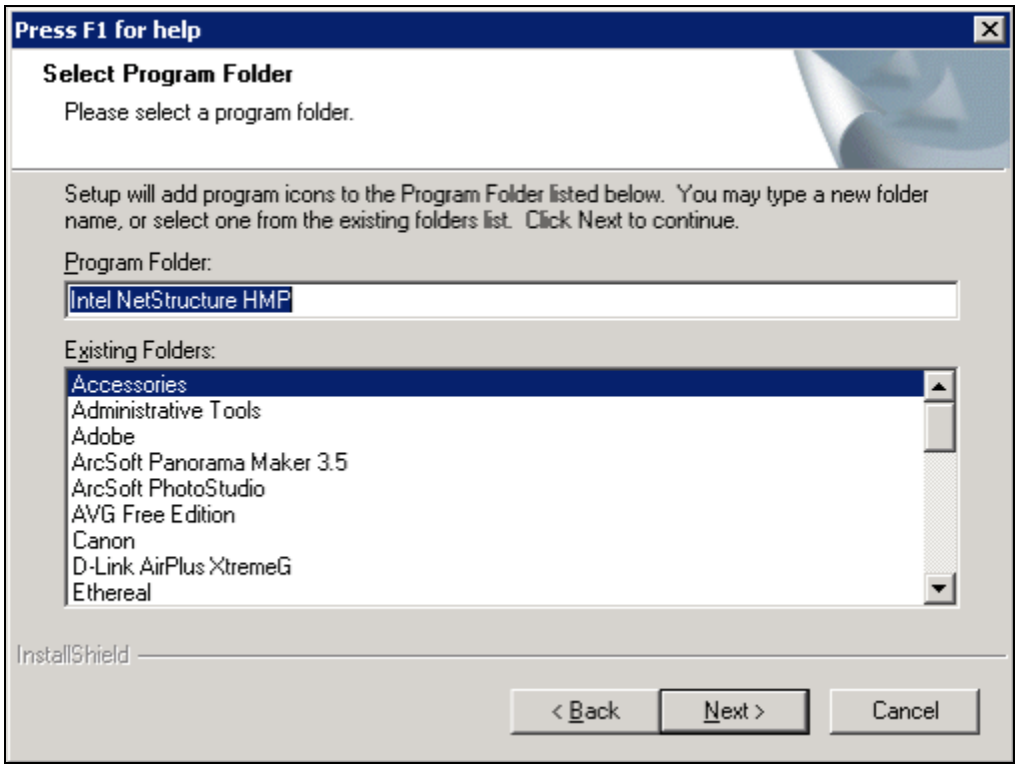
3. Ensure **Core Runtime**, **License Package** and **Demos** are checked and click the **Next** button.



4. Click the **Yes** button to continue the installation.



5. Accept the default program folder (or change it as appropriate) and click the **Next** button.

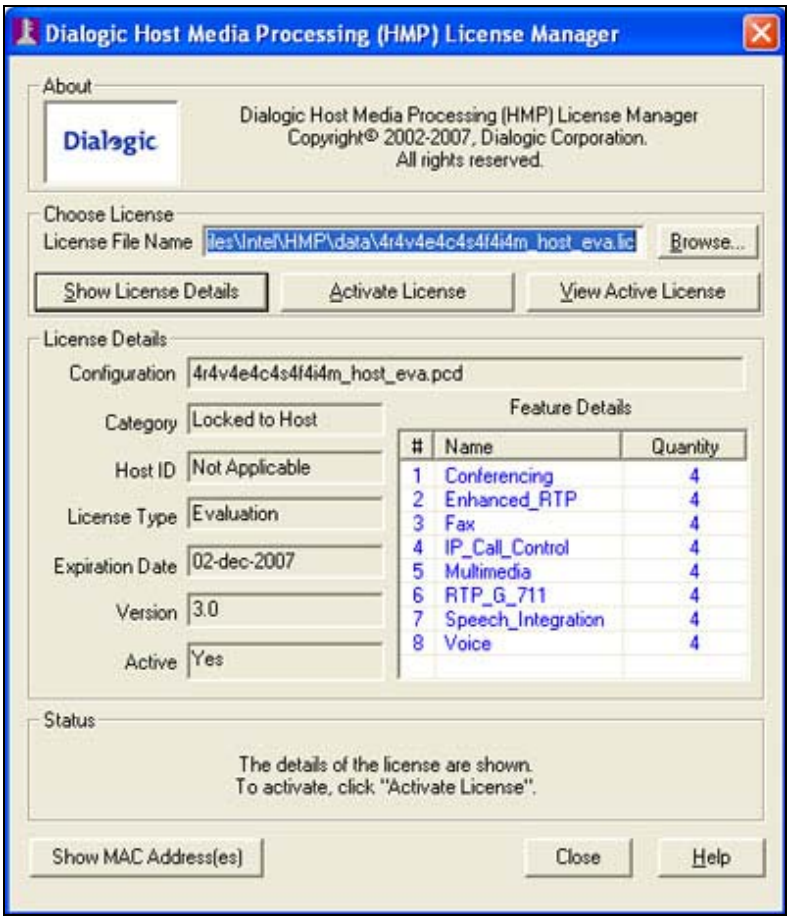


6. Review the settings on the next screen and click the **Next** button.
7. When the installation completes, select the **Yes, I want to restart my computer now** radio button and click the **Finished** button.

Dialogic HMP Drivers License Activation

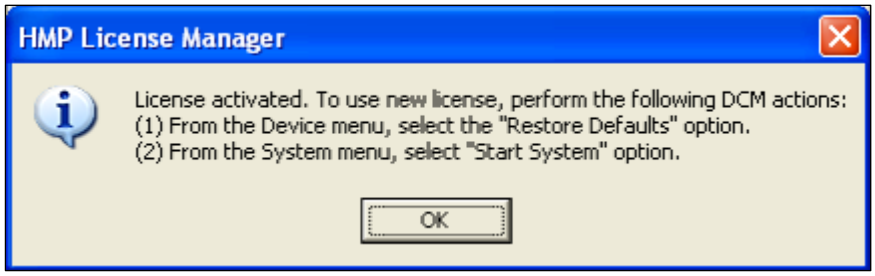
Ensure you have a valid HMP Software license file prior to proceeding. If you do not have a license, contact Voice Innovate with the host ID value, which can be found in the "Host ID" field in the HMP License Manager.

1. Place a copy of the license file the HMP software installation folder's *data* subdirectory (for example, *C:\Program Files\Dialogic\HMP\data*).
2. Go to the Window's **Start** menu and click **All Programs → Dialogic HMP→ HMP License Manager** to launch the licensing utility.
3. Browse to your license in the **License File Name** field and click the **Activate License** button. The license is located in the HMP software's installation folder's *data* subdirectory (for example, *C:\Program Files\Dialogic\HMP\data*).

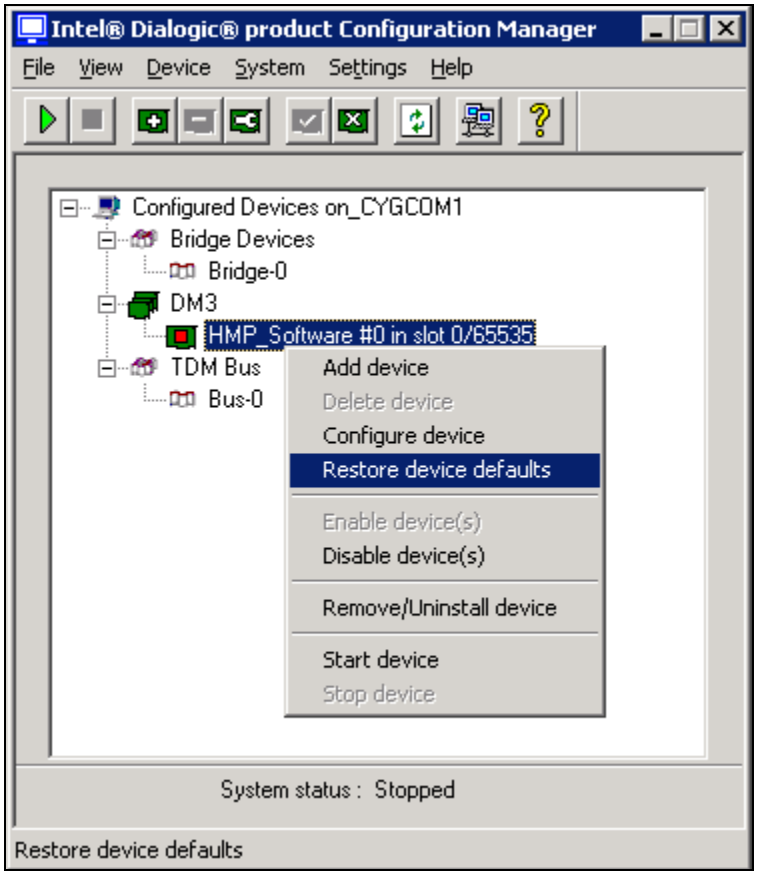


Note: The license file is named according to the number of ports and features licensed. For example, a 37 port license containing the base HMP features as well as enhanced RTP features might be named: *37r37v37e0c37s0f37i_host_pur.lic*.

4. Click the **OK** button and close License Manager.

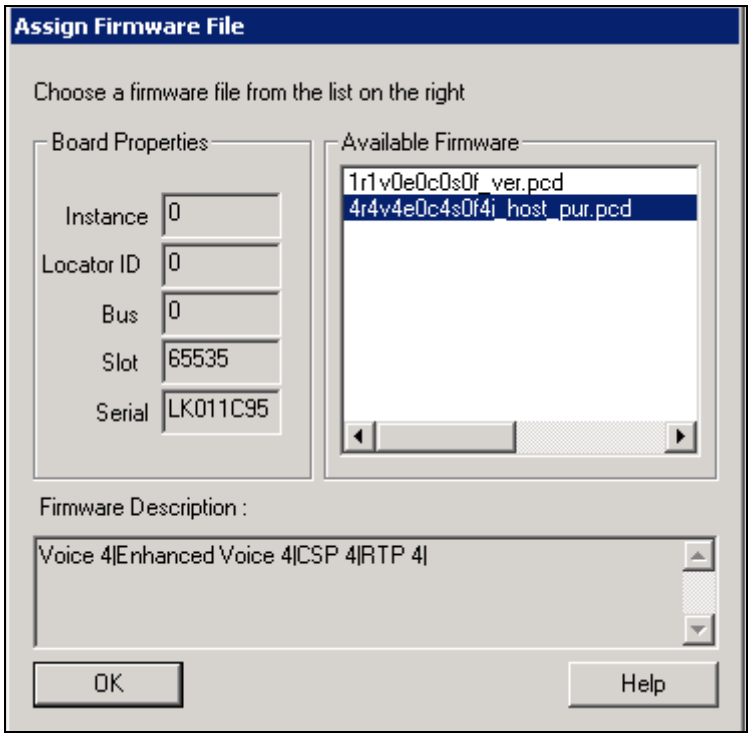


5. Open the Windows **Start** menu and click **All Programs** → **Dialogic HMP** → **Configuration Manager DCM** to launch the configuration utility.
6. Right-click the **HMP_Software** entry and select **Restore device defaults**.

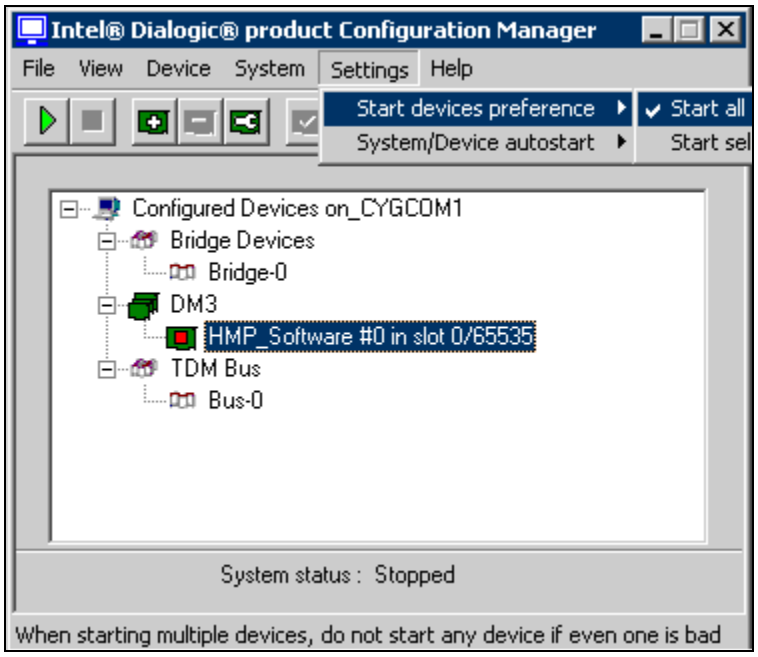


7. Click the **Yes** button on the next screen to restore the device's default values.

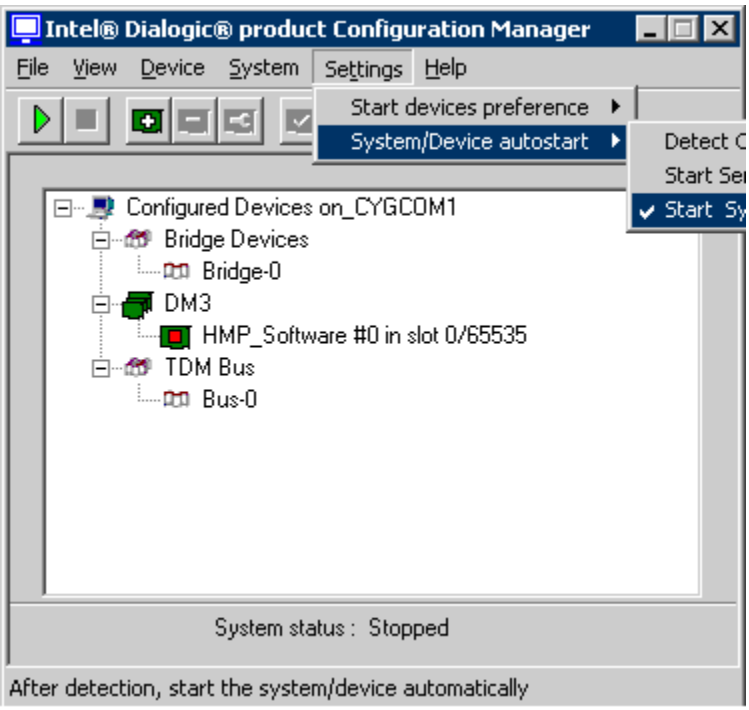
8. Select the license file and click the **OK** button.



9. Click **Settings → Start devices preference → Start all**.



10. Click **Settings → System/Device autostart → Start System**.

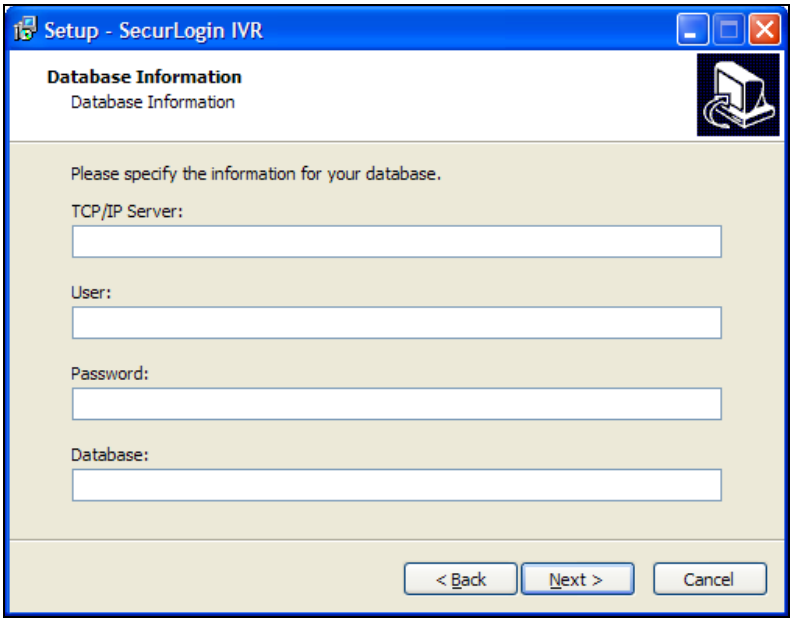


11. Close the DCM window and reboot the system.

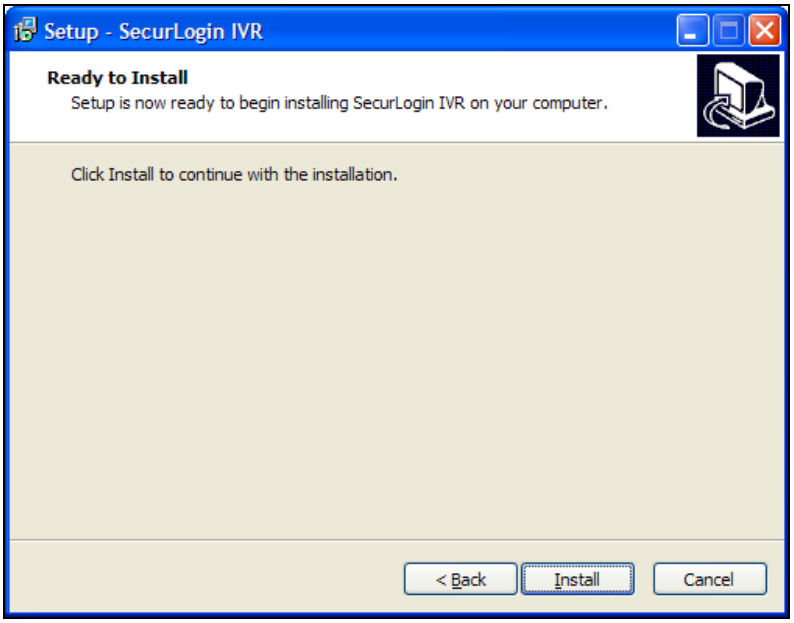
SecurLogin IVR Installation

This section contains instructions for installing SecurLogin IVR.

1. Launch the SecurLogin installer and click the **Next** button.
2. Enter the **SecurLogin MySQL database information** and click the **Next** button.



3. Click the **Install** button.



4. Click the **Finish** button when the installation has completed.

LumenVox ASR Speech Recognizer Installation

The SecurLogin IVR service uses a third party Speech Recognition engine. The information for installing and licensing the LumenVox ASR speech recognizer can currently be found using a web browser at: **http://www.lumenvox.com/help/speechEngine/installation/windowsInstallation.htm**

Note that the LumenVox Engine and Licensing installation files and the LumenVox License file are supplied by Voice Innovate. You will not need to obtain them as described on the web page specified below.

RSA Access Manager User Mapping

Each RSA Authentication Manager user must be mapped to a Voice Innovate SecurLogin user. Voice Innovate provides a convenient utility for provisioning it's users from an RSA Authentication Manager report. Follow the instructions below to use this utility.

Export User Records from RSA Authentication Manager

1. Log into the RSA Authentication Manager Security Console and select **Reporting → Add New**.
2. Select the **Users with Tokens** template and click the **Next** button at the bottom of the page.
3. Enter a name for the report in the **Report Name** field.
4. For simplicity, choose **Output all Columns**. The utility will select the right appropriate values.
5. Choose the **Identity Source** from the select dialog in the **Input Parameter Values Section** and click the **Save** button.
6. Click **Reporting → Manage Existing**, select the new report and click **Run Report Now**.
7. Click **Reporting → Report Output → Completed Reports**, select the latest output for the report and click **Download CVS file**.

Import User Records to SecurLogin

1. Open a Windows command prompt and navigate to the SecurLogin web server root directory.
2. Enter the import.exe command followed by the path to report's CSV file you exported above.

If your import was successful, the utility will display the number of accounts that were updated, inserted or removed. Otherwise, it will display descriptions of any errors in the import process.

Here is an sample execution of the utility:

```
C:\Program Files\VIC\SecurLogin\WebServer>import.exe usertoken.csv
       Success
       Imported 23 Users
```

Client Web Client Configuration

SecurLogin requires that the Client Web Application uses the OpenID standard (**http://openid.net/**) for authentication purposes. OpenID plug-ins for most popular applications are freely available for download via the internet from many sources. If a plug-in is available for your Client Web Application it must be downloaded and installed as per the plug-in instructions. If you require assistance in obtaining an OpenID plug-in for your application contact Voice Innovate.

If a plug-in is not available for your Client Web Application, the tools to create an authentication client for the application are available from OpenID at: **http://openid.net/developers/libraries/**. If you require further assistance regarding OpenID client development contact Voice Innovate.

The installation and configuration process for the OpenID plug-in varies based on the plug-in chosen. The steps for installation and configuration are detailed in the documentation provided with the OpenID Plugin chosen, but can be summarized as:

- Disable the existing authentication modules.
- Install and enable the Plugin.
- Configure your system to rely solely on the SecurLogin web application for authentication.

Certification Checklist for RSA Authentication Manager

Date Tested: July 29, 2011

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP4	Windows 2003 R2
RSA Authentication API Library	6.1.3	Windows 2003 R2
SecurLogin	1.1	Windows 2003 R2

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 Numeric PIN	✓	Deny Numeric 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

JGS/ PAR

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