Novell
Identity Assurance Solution

3.0

www.novell.com

INSTALLATION GUIDE

December 20, 2006

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on theNovell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide provides an overview of the Identity Assurance Solution. It includes instructions on how to install, configure, and manage the solution.

Audience

This guide is written primarily for network administrators and system integrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Identity Assurance Solution Installation Guide*, visit the Identity Assurance Solution Documentation Web site (http://www.novell.com/documentation/ias/index.html).

Documentation Conventions

In Novel®l documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Overview

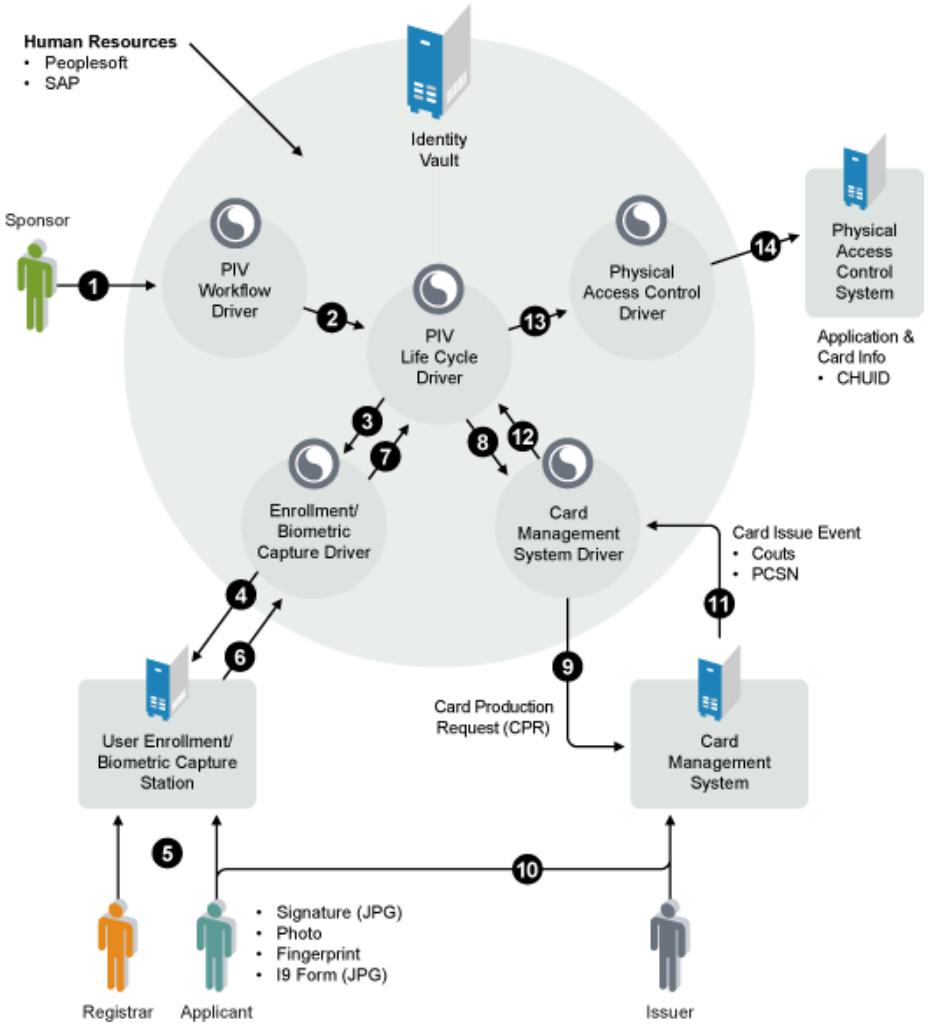
1

Novell® has partnered with third-party companies to build a solution that offers an integrated logical and physical control system that complies with Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 directs the implementation of a new standardized badging process, which is designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification.

Identity Assurance Solution provides a complete system for managing the enrollment, issuance, access control, and retirement of Personal Identification Verification (PIV) cards. This solution is in compliance with the Federal Information Processing Standards Publication 201 (FIPS 201) and provides components such as an Identity Management System (IDMS), a User Enrollment/ Biometric Capture system, a Card Management System (CMS), and Logical and Physical Access Control Systems (LACS/PACS).

Figure 1-1 shows the different components of the solution and how the workflow is designed.

Figure 1-1 *Identity Assurance Solution Workflow Overview*



1.1 Identity Assurance Solution Components

Table 1-1 describes the basic components and the specific products in this solution.

Table 1-1 *Identity Assurance Solution Components and Products*

Component	Product
Identity Management System / Identity Vault	Novell eDirectory™
	Novell Identity Manager
	Novell iManager
User Enrollment/Biometric Capture system	Enrollment Driver for Honeywell* SmartPlus* System
Card Management System (CMS)	CMS Driver for ActivIdentity* ActivID*
Logical Access Control System (LACS)	Novell Enhanced Smart Card Method (NESCM)
Physical Access Control System (PACS)	PACS Integration Driver for Honeywell SmartPlus System

A more detailed list of components and products is provided in Chapter 2, “Planning the Identity Assurance Solution Installation,” on page 13.

1.2 Identity Assurance Solution Drivers

Key components of this solution are the drivers. For information on what each driver does, see Section 4.1, “Driver Overviews,” on page 29.

1.3 Identity Assurance Solution Workflow

Figure 1-1 on page 9 describes the basic workflow of this solution.

1. From a workstation, the sponsor accesses the user application associated with the PIV Workflow Driver and submits a request for a PIV card for the applicant.
2. The PIV Workflow Driver sends the request to the PIV Life Cycle driver.
3. The PIV Life Cycle driver checks to make sure the request is valid and complete. If it is a valid request, it routes the request to the Enrollment/Biometric Capture driver.
4. The Enrollment/Biometric Capture driver routes the request to the biometric engine, accessible by the Registrar’s workstation.
5. The applicant meets with the Registrar and provides the following information:
   - Signature. This is captured as a JPEG file.
   - Photo
   - Fingerprint
   - I9 Form. This is scanned and saved as a JPEG file.

   A background check is also conducted on the applicant.

6 After the enrollment data is captured, the registrar submits it back to the Enrollment/Biometric Capture driver.

7 The Enrollment/Biometric Capture driver sends the enrollment data to the PIV Life Cycle driver.

8 The PIV Life Cycle driver checks to make sure the data is valid and complete. If the data is valid and complete, it routes the request to the Card Management System driver.

9 The Card Management System driver sends a Card Production Request (CPR) to the Card Management System.

10 The Issuer creates the PIV card for the applicant.

The Applicant meets with the Issuer to receive the PIV card. The applicant provides a fingerprint scan to confirm his or her identity and to finalize the PIV card creation and issuance. When this is successfully completed, the Issuer hands over the card.

11 After the card is physically issued, the Issuer sends a Card Issue Event back to the Card Management System driver. The Card Issue Event contains all the card data.

12 The Card Management System driver notifies the PIV Life Cycle driver of the Card Issue Event.

13 The PIV Life Cycle driver stores the card data and verifies that everything is in order. If so, the applicant can now use his or her card for logical access to the network. The PIV Life Cycle driver notifies the Physical Access Control driver of the card issuance.

14 The Physical Access Control driver sends the information to the Physical Access Control System. The card is activated for physical access based on the sponsor's chosen settings.

1.4 What's Next

- To prepare for the installation, see Chapter 2, "Planning the Identity Assurance Solution Installation," on page 13.
- To begin the installation, see Chapter 3, "Installing Identity Assurance Solution," on page 17.

Planning the Identity Assurance Solution Installation

2

This section describes the minimum requirements that must be met for each machine before starting the Identity Assurance Solution installation. It also describes the contents of each CD distributed with this solution.

2.1 Minimum Requirements

The following minimum requirements apply to this release:

2.1.1 Identity Vault Server

The Identity Vault server must be running one of the following:

- Windows 2003 Server SP1 or later

2.1.2 User Enrollment/Biometric Capture Station

See the minimum requirements for the Honeywell SmartPlus Enrollment software.

2.1.3 Card Management System

See the minimum requirements for the ActivIdentity CMS software.

2.1.4 Physical Access Control System

See the minimum requirements for the Honeywell SmartPlus Integration software.

2.1.5 Workstations

Each workstation must meet the following minimum requirements:

- Windows XP SP2 or later installed.
- PIV card reader is connected and PIV card middleware is installed.
- Use supported PIV cards.
- Use supported middleware:

2.1.6 Web Browser

The administration of the Identity Management Solution is supported using the following browsers on Windows only:

- Firefox* 1.5.x or later
- Mozilla* 1.7.5 or later
- Internet Explorer 6.0 SP2 or later

2.2 Preparing the Software

Identity Assurance Solution is made up of several software components:

- Novell® products that need to be downloaded and installed (Novell eDirectory™, Novell Identity Manager, Novell Audit).
- Third-party products that need to be installed (Honeywell SmartPlus Enrollment, ActivIdentity CMS, Honeywell SmartPlus Integration).
- IAS CD images (the configuration files, drivers, and workstation setup software).

  After downloading the IAS `.iso` files and verifying the MD5 values, create a CD for each `.iso` file you downloaded. Label each CD as outlined in the following table:

Filename	CD label
ias_modules_3_0.iso	CD 1-IAS Modules
ias_client_3_0.iso	CD 2-IAS Client

The CDs are referenced according to these labels throughout the installation.

2.3 Contents of Each Identity Assurance Solution CD

The Identity Assurance Solution software is contained on two CDs. The following table can serve as a reference as you go through the installation of each component.

CD Name	CD Contents
CD 1–IAS Modules CD	◆ iManager 2.6 (standard iManager structure, plug-ins, custom utilities, and Web applications) ◆ Installs for IDM drivers specific to IAS CMS Driver for ActivIdentity ActivID Enrollment Driver for the Honeywell SmartPlus System PACS Integration Driver for Honeywell SmartPlus System PIV Life Cycle Driver ◆ Pre-config files for all IAS IDM drivers ◆ Novell Designer 2.0 for IDM
CD 2–IAS Client CD	◆ IAS Client Umbrella Install ◆ Novell Client™ 4.9.1 SP3 NICI 2.7.0.1 and NMAS™ Client 3.1.1.0 ◆ Novell Enhanced Smart Card Method (NESCM) 3.0 ◆ Novell Audit Platform Agent 2.0.2

2.4 What's Next

To begin the installation, follow the instructions in Chapter 3, “Installing Identity Assurance Solution,” on page 17.

Installing Identity Assurance Solution

3

This section describes or points to information on how to install all software components for the Identity Assurance Solution.

3.1 Installing the User Enrollment Biometric Capture Station

The software being utilized for the User Enrollment Biometric Capture station for this release is Honeywell SmartPlus Enrollment software. Order this software and install it on the machine you are designating for this function.

For information on installing the Honeywell SmartPlus Enrollment software, see the installation documentation provided by Honeywell.

3.2 Installing the Card Management System

The software being utilized for the Card Management System for this release is the ActivIdentity CMS software. Order this software and install it on the machine you are designating for this function.

For information on installing the ActivIdentity CMS software, see the installation documentation provided by ActivIdentity.

3.3 Installing the Physical Access Control System

The software being utilized for the Physical Access Control System for this release is the Honeywell SmartPlus Integration software. Order this software and install it on the machine you are designating for this function.

For information on installing the Honeywell SmartPlus Integration software, see the installation documentation provided by Honeywell.

3.4 Installing the Identity Vault Server

Install the Identity Vault server components *in the order they are presented in this section*. Each section lists the product to install and the CD the product is on.

3.4.1 Novell eDirectory 8.8.1

Purchase, download, and install Novell® eDirectory™ 8.8.1 from the Novell Download Web site (http://download.novell.com/index.jsp).

For information on installing Novell eDirectory, see the *Installing or Upgrading Novell eDirectory on Windows* section of the *Novell eDirectory Installation Guide* (http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html).

By installing Novell eDirectory 8.8.1, you will also install the following components:

- NICI 2.7.0-1
- Novell Certificate Server™ 3.1.1.0
- NMAS™ 3.1.0.1

TIP: Consider the following as you install eDirectory:

- Do not re-install the Novell Client™ if prompted.
- If the eDirectory server is being installed on a Windows 2000 AD Domain Controller, you must change the ports to avoid a conflict with the AD LDAP server. We recommend changing the ports to 390 for clear text and 637 for SSL/TLS.
- You don’t need to install any NMAS login methods. The NESCM method is installed as a separate component.

3.4.2 iManager 2.6

CD: CD 1 - IAS Modules

Install Location: `\imanager\installs\win`

Install Documentation: *Novell iManager 2.6 Installation Guide* (http://www.novell.com/documentation/imanager26/imanager_install_26/data/alw39eb.html)

1. Run `imanagerinstall.exe`.
2. Accept the license agreement.
3. Configure iManager to use the following:

Web Server:	Apache

Servlet Container:	Tomcat
JVM:	Sun* JRE

4 Accept the default installation folder.

5 Specify the Tree name and Admin username.

6 Complete the installation.

TIP: When logging in to iManager, use the fully distinguished Admin user DN (for example, admin.ias). If the tree can't be located, use the IP address or DNS name of the Identity Vault server.

3.4.3 Novell Identity Manager 3.0.1

Purchase, download, and install Novell Identity Manager 3.0.1 from the Novell Download Web site (http://download.novell.com/index.jsp).

For information on installing Novell Identity Manager, see the Installation section of the Novell Identity Manager 3.0.1 Documentation Web site (http://www.novell.com/documentation/idm/index.html).

3.4.4 Novell Identity Manager 3.0.1 on Connected Systems

Each of the three connected systems (User Enrollment/Biometric Capture Station, Card Management System, and Physical Access Control System) needs to have Novell Identity Manager 3.0.1 Connected System installed on it.

For information on installing Novell Identity Manager on connected systems, see the Installing the Connected Systems Option section of the *Identity Manager 3.0.1 Installation Guide* (http://www.novell.com/documentation/idm/install/data/abaa35l.html).

3.4.5 Novell Enhanced Smart Card Method (NESCM) Server Component

CD: CD 2 - IAS_Client
Location: `\nmasmethods\novell\enhancedsmartcard.zip`

The NESCM method's server component is installed using iManager.

You must complete the procedures for installing and configuring the NESCM method on a server as provided in the *Novell Enhanced Smart Card Method Installation Guide* (http://www.novell.com/documentation/ias/index.html?page=/documentation/ias/nescm_install/data/bookinfo.html).

3.5 Installing Drivers

Identity Assurance Solution contains five separate drivers. The following table describes which driver is installed on which system:

Table 3-1 *Driver/System Installation*

Driver Type	Driver Brand Name	System to Install Driver On
PIV card control center driver	PIV Life Cycle driver	Identity Vault server
PIV card user application driver	PIV Workflow driver	Identity Vault server
Enrollment driver	Enrollment Driver for Honeywell SmartPlus System	User Enrollment/Biometric Capture Station
Card Management System driver	CMS Driver for ActivIdentity ActivID	Card Management System
Physical Access Control driver	PACS Integration Driver for Honeywell SmartPlus System	Physical Access Control System

TIP: The driver installation programs shut down eDirectory if eDirectory is installed on the system.

If the eDirectory shutdown attempt fails, the installer stops and must be run again. In order to avoid the inconvenience of re-running the installer, you can stop the eDirectory service before launching each installer.

3.5.1 PIV Life Cycle Driver

CD: CD 1 - IAS_Modules
Location: `\idmdriver`

The PIV Life Cycle driver must be installed on the Identity Vault server.

1. Double-click *IAS_MODULES_3.0:IDMDriver\PIV Life Cycle Driver.exe* to install the driver.
2. Read the welcome page, then click *Next*.
3. Read the license agreement and select *I accept the terms of the license agreement*, then click *Next*.
4. Specify the name of an eDirectory user who has sufficient administrative rights to the root of the tree to extend the schema, then click *Next*.

   The user name must be entered using the leading dot-delimited notation. Then click Next.
5. Read the summary page, then click *Install* to begin the installation.
6. Click *Finish* to exit the installation wizard.

3.5.2 PIV Workflow Driver

CD: CD 1 - IAS_Modules
Location: No installation program

The PIV Workflow driver doesn't have an installation program. It is installed using iManager and works with the User Application for Provisioning.

For more information on importing and configuring the PIV Workflow Driver, see Section 4.2.2, "Configuring the PIV Workflow Driver in iManager," on page 35.

3.5.3 Enrollment Driver for Honeywell SmartPlus System

CD: CD 1 - IAS_Modules
Location: `\idmdriver`

To install the Enrollment driver, you need to complete the following three tasks:

1. "Install Identity Manager 3.01 for Connected System on the Enrollment Biometric Capture System" on page 21
2. "Install the Driver" on page 21
3. "Configure the Connected System (Remote Loader)" on page 21

Install Identity Manager 3.01 for Connected System on the Enrollment Biometric Capture System

For information on installing Novell Identity Manager on connected systems, see the Installing the Connected Systems Option section of the *Identity Manager 3.0.1 Installation Guide* (http://www.novell.com/documentation/idm/install/data/abaa35l.html).

Install the Driver

The driver is installed on the same machine where the Honeywell SmartPlus Enrollment system is installed. Make sure that the Identity Manager Connected System is installed before proceeding with the installation of the driver.

1. Double-click *IAS_MODULES_3.0:IDMDriver\Honeywell SmartPlus Enrollment Driver.exe* to install the driver.
2. Read the welcome page, then click *Next*.
3. Read the license agreement and select *I accept the terms of the license agreement*, then click *Next*.
4. Browse to and select where you have the Remote Loader installed on the Honeywell SmartPlus Enrollment system, then click *Next*.
5. Read the summary page, then click *Install* to begin the installation.
6. Click *Finish* to exit the installation wizard.

To configure the driver, see Chapter 4, "Configuring Identity Assurance Solution," on page 29.

Configure the Connected System (Remote Loader)

To configure the connected system (remote loader):

1. Launch the Remote Loader Console.
2. Click *Add* to add a remote driver.
3. Specify a description for the remote driver.
4. Select *com.novell.nds.dirxml.driver.soap.SOAPDriver* in the driver drop-down list.

   If the driver is not listed, it means the driver has not been installed. You must first install the driver. See "Install the Driver" on page 21.
5. Specify a filename and location for the remote loader configuration file.

6 Select *All* for the Remote Loader service to listen for communication on all IP addresses for the ActivIdentity server.

   6a Leave the connection port at the default of 8090.

   6b Leave the command port at the default of 8000.

7 Specify the remote loader password.

8 Specify the driver object password.

9 Select *Use an SSL Connection*.

   9a Browse to and select a trusted root file.

   See Providing for Secure Data Transfer (http://www.novell.com/documentation/idm/index.html?page=/documentation/idm/admin/data/bs35pi6.html#bs35pi6) for information on how to create a trusted root file.

10 Set the trace level to zero.

   Increase this only during troubleshooting of the driver.

11 Select *Establish a Remote Loader service for this driver instance*.

12 Click *OK* to save the information.

To configure the driver, see Chapter 4, "Configuring Identity Assurance Solution," on page 29.

3.5.4 CMS Driver for ActivIdentity ActivID

CD: CD 1 - IAS_Modules
Location: *idmdriver*

To install the CMS driver, you need to complete the following three tasks:

1. "Install Identity Manager 3.0.1 for Connected Systems on the Card Management System" on page 22
2. "Install the Driver" on page 22
3. "Configure the Connected System (Remote Loader)" on page 23

Install Identity Manager 3.0.1 for Connected Systems on the Card Management System

For information on installing Novell Identity Manager on connected systems, see the Installing the Connected Systems Option section of the *Identity Manager 3.0.1 Installation Guide* (http://www.novell.com/documentation/idm/install/data/abaa35l.html).

Install the Driver

The driver is installed on the same machine where the Card Management System for ActivIdentity is installed.

1 Double-click *IAS_MODULES_3.0:IDMDriver\CMS Driver for ActivIdentity ActivID.exe* to install the driver.

2 Read the welcome page, then click *Next*.

3 Read the license agreement and select *I accept the terms of the license agreement*, then click *Next*.

4 Browse to and select where you have the Remote Loader installed on the ActivIdentity Card Management system, then click *Next*.

5 Read the summary page, then click *Install* to begin the installation.

6 Click *Finish* to exit the installation wizard.

Configure the Connected System (Remote Loader)

To configure the connected system (remote loader):

1 Launch the Remote Loader Console.

2 Click *Add* to add a remote driver.

3 Specify a description for the remote driver.

4 Select *com.novell.nds.dirxml.driver.aicmsshim.AICMSDriverShim* in the driver drop-down list.

If the driver is not listed, it means the driver has not been installed. You must first install the driver. See "Install the Driver" on page 22.

5 Specify a filename and location for the remote loader configuration file.

6 Select *All* for the Remote Loader service to listen for communication on all IP address for the ActivIdentity server.

6a Leave the connection port at the default of 8090.

6b Leave the command port at the default of 8000.

7 Specify the remote loader password.

8 Specify the driver object password.

9 Select *Use an SSL Connection*.

9a Browse to and select the CMS CA Root certificate.

10 Set the trace level to zero.

Increase this only during troubleshooting of the driver.

11 Select *Establish a Remote Loader service for this driver instance*.

12 Click *OK* to save the information.

To configure the driver, see Chapter 4, "Configuring Identity Assurance Solution," on page 29.

3.5.5 PACS Integration Driver for Honeywell SmartPlus System

CD: CD 1 - IAS_Modules
Location: *idmdriver*

To install the PACS driver, you need to do the following three tasks:

1. "Install Identity Manager 3.0.1 for Connected Systems on the Physical Access Control System" on page 24
2. "Install the Driver" on page 24
3. "Configure the Connected System (Remote Loader)" on page 24

Install Identity Manager 3.0.1 for Connected Systems on the Physical Access Control System

For information on installing Novell Identity Manager on connected systems, see the Installing the Connected Systems Option section of the *Identity Manager 3.0.1 Installation Guide* (http://www.novell.com/documentation/idm/install/data/abaa35l.html).

Install the Driver

The driver is installed on the same machine where the Honeywell SmartPlus Integration system is installed.

1. Double-click *IAS_MODULES_3.0:IDMDriver\Honeywell SmartPlus Integration Driver.exe* to install the driver.
2. Read the welcome page, then click *Next*.
3. Read the license agreement and select *I accept the terms of the license agreement*, then click *Next*.
4. Browse to and select where you have the Remote Loader installed on the Honeywell SmartPlus Integration system, then click *Next*.
5. Read the summary page, then click *Install* to begin the installation.
6. Click *Finish* to exit the installation wizard.

To configure the driver, see Chapter 4, "Configuring Identity Assurance Solution," on page 29.

Configure the Connected System (Remote Loader)

To configure the connected system (remote loader):

1. Launch the Remote Loader Console.
2. Click *Add* to add a remote driver.
3. Specify a description for the remote driver.
4. Select *com.novell.nds.dirxml.driver.soap.SOAPDriver* in the driver drop-down list.

   If the driver is not listed, it means the driver has not been installed. You must first install the driver. See "Install the Driver" on page 24.
5. Specify a filename and location for the remote loader configuration file.
6. Select *All* for the Remote Loader service to listen for communication on all IP address for the ActivIdentity server.
   - **6a** Leave the connection port at the default of 8090.
   - **6b** Leave the command port at the default of 8000.
7. Specify the remote loader password.
8. Specify the driver object password.
9. Select *Use an SSL Connection*.
   - **9a** Browse to and select a trusted root file.

     See Providing for Secure Data Transfer (http://www.novell.com/documentation/idm/index.html?page=/documentation/idm/admin/data/bs35pi6.html#bs35pi6) for information on how to create a trusted root file.

10 Set the trace level to zero.

   Increase this only during trouble shooting of the driver.

11 Select *Establish a Remote Loader service for this driver instance*.

12 Click *OK* to save the information.

To configure the driver, see Chapter 4, "Configuring Identity Assurance Solution," on page 29.

3.6 Post-Installation Tasks

After installation, you need to enable the iManager plug-ins:

1 Launch iManager.

2 Click the Configure icon  .

3 Install the IAS plug-ins

   3a Click Module to select all available modules.

   3b Click Install.

4 Close iManager.

5 Restart Tomcat by either rebooting the server or doing the following:

   5a Click Start > Settings > Control Panel.

   5b Double-click Administrative tool > Services.

   5c Right-click Tomcat, then click Restart.

3.7 Installing Workstations

CD: CD 2 - IAS_Client
Location: Auto launch

Each applicant's workstation should meet the minimum requirements. See Section 2.1.5, "Workstations," on page 13.

Each applicant's workstation that will be authenticating using a PIV card must be installed in the following way:

1 Insert the CD 2 - IAS Client into the workstation's CD drive.

   The client installation should auto launch.

   If not, browse to the root of CD 2 - IAS Client and double-click `setup.exe`.

2 Read the welcome page, then click *Next*.

3 Read the license agreement and select *I accept the terms of the license agreement*, then click *Next*.

4 Select *Novell Client and Enhanced Smart Card Method*.

   (Optional) If you also want to audit Workstation Only logins, select *Novell Audit Platform Agent*.

5 Click *Next*.

6 Click *Install*.

7. Read the Novell Enhanced Smart Card Method welcome page, then click *Next*.
8. Read the license agreement and select *I accept the terms of the license agreement*, then click *Next*.
9. On the Disconnected Support page, select *Yes, I Want Disconnected Support*, then click *Next*.

   This feature allows you to authenticate to the workstation only using the Smart Card login method.
10. On the ID Plugin Support page, select whether or not you want to use the ID plug-in support. feature.

    This feature allows the ID plug-in to query the database for the smart card's associated username.

    If you select *Yes*, you must also supply the IP addresses and port numbers for all LDAP servers you want to query.
11. Click *Next*.
12. Choose whether or not to customize the password field description on the login screen, then click *Next*.

    If you choose to customize the login screen's password field, you must type in the new text for the field.

    TIP: If you use Alt-P to access the password field when logging in, you lose this functionality when you customize the password field description. To keep this functionality, you must include an ampersand (&) in front of a letter P in the new text you enter in the password field.

    For example, if your new text reads Password, you should enter it as &Password so that Alt-P continues to function as usual.

    ---
13. Select either *PC/SC* or *PKCS#11*, then click *Next*.

    PC/SC and PKCS#11 are technical standards used to communicate between a server and PKI-enabled applications. PC/SC is a standard used for integrating smart cards and smart card readers. PKCS#11 is a standard for public key message exchanges.

    Select the standard that best supports your hardware. For more information, see the manufacturer's specifications.

    If you select PKCS#11, you must also select a provider that best suits your needs.
14. Review the summary page, then click *Install*.
15. (Conditional) If you decided to install the Novell Audit Platform Agent in Step 4, click *Next* on the Novell Audit Platform Agent page. If not, skip to Step 21.
16. Accept the License Agreement, then click *Next*.
17. Fill in the customer information, then click *Next*.
18. Type the IP address or DNS name of the Secure Logging Server, then click Next.

    This is the IP address or DNS name of the Novell Audit server (the Identity Vault server that was set up previously).
19. Select *Complete*, then click *Next* > *Install*.
20. Click *Finish*.
21. Click *Finish*.
22. Restart the workstation.

You must complete the instructions for installing and configuring the NESCM method on a workstation as provided in the *Novell Enhanced Smart Card Installation Guide* (http://www.novell.com/documentation/ias/index.html?page=/documentation/ias/nescm_install/data/bookinfo.html).

3.7.1 Installing the Novell Client Patch

CD: CD 2 - IAS_Client
Location: `\novellclient\winnt\i386\491_SP3_update`

After installing the Novell Client, you need to install the Novell Client Patch.

1. On CD 2 - IAS Client, browse to the `\novellclient\winnt\i386\491_sp3_update` directory.
2. Right-click the `_491psp3_nwsso.inf` file, then click *Install*.
3. If files are in use, reboot the workstation when prompted to.

3.7.2 Workstation Configuration

For information about configuring NESCM on a workstation, see the *Novell Enhanced Smart Card Installation Guide* (http://www.novell.com/documentation/ias/index.html?page=/documentation/ias/nescm_install/data/bookinfo.html).

3.8 What's Next

Configure the Identity Assurance Solution drivers by following the instructions in Chapter 4, "Configuring Identity Assurance Solution," on page 29.

Configuring Identity Assurance Solution

4

This section describes each driver for Identity Assurance Solution. It also describes how to configure the drivers using iManager.

Review Section 4.1, “Driver Overviews,” on page 29 for detailed information about the drivers. Then see Section 4.2, “Configuring the Drivers using iManager,” on page 34 for information on configuring the drivers.

4.1 Driver Overviews

Each driver was installed previously in Chapter 3, “Installing Identity Assurance Solution,” on page 17. The following sections provide information about each driver:

4.1.1 PIV Life Cycle Driver Overview

The PIV Life Cycle driver acts as a sort of traffic director for the solution. It verifies that all expected attributes are included in each step of the process and either allows the process to continue if all requirements are met or halts the process if requirements are not met.

4.1.2 PIV Workflow Driver Overview

The PIV Workflow driver provides a means for the Sponsor to perform tasks related to requesting and provisioning PIV cards for users.

4.1.3 Enrollment Driver Overview

The Enrollment driver for the Honeywell SmartPlus system does the following tasks in the PIV provisioning scenario:

- Creates application user accounts in the Honeywell SmartPlus Enrollment system.
- Provisions sponsor-approved appellation information from the Identity Manager system to the Honeywell SmartPlus Enrollment system.

- Publishes biometric data and vetting confirmation from the Honeywell SmartPlus Enrollment system to the Identity Manager system.
- Deletes cardholder biometric data from the Honeywell SmartPlus Enrollment system upon termination of the user.

The driver contains policies to detect events that indicate when data should be provisioned to or deprovisioned from the Honeywell SmartPlus Enrollment system. It also contains an event "listener" capability that allows it to receive data transmissions from the Honeywell SmartPlus Enrollment system.

In order to maintain a simple interface with Identity Manager, the driver is configured to only respond to state changes in the fipsBioStatus attribute.

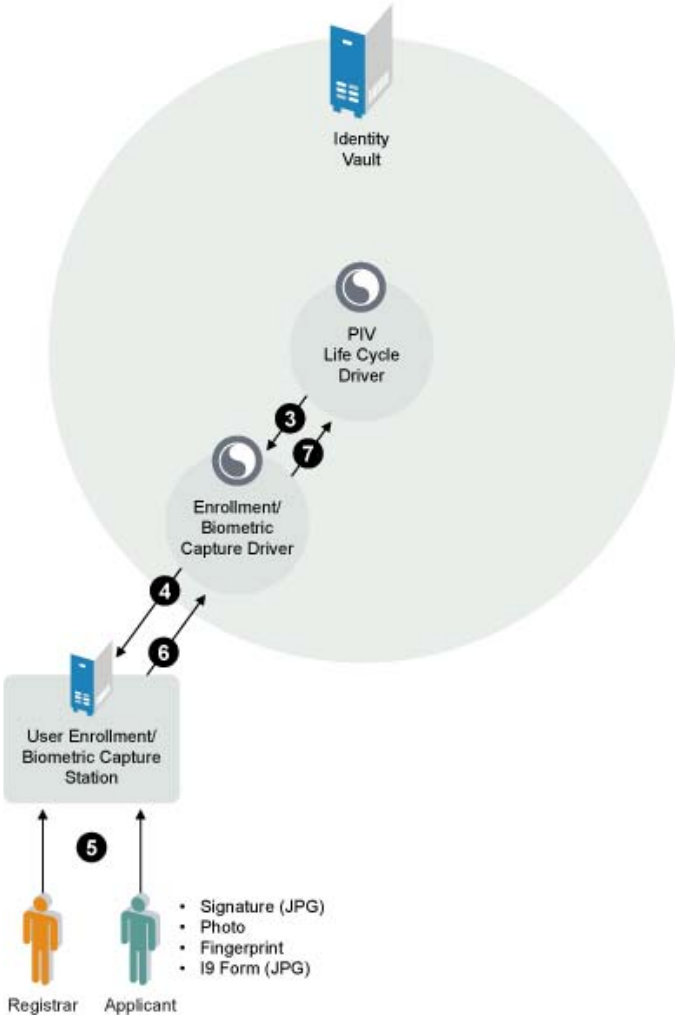
The value of this attribute is modified only by the Enrollment driver or PIV Life Cycle driver. After the initial provisioning information is added by the sponsor to the user through the PIV Workflow, the PIV Life Cycle driver sets the fipsBioStatus attribute to a value of Biometric Enrollment Ready.

This modification event triggers the driver to send the account creation and sponsor enrollment data to the Biometric Enrollment server. If the information is sent and provisioned successfully, the fipsBioStatus attribute is set to Biometric Enrollment in Progress. If the information failed to be sent to the server, fipsBioStatus is set to Biometric Enrollment Failure and the fipsBioStatusReason and fipsBioStatusExplanation attributes contain the reason for the failure.

The PIV Life Cycle driver receives the modify event for the fipsBioStatus attribute and updates the PIV provisioning state attributes. If the information was submitted successfully to the Honeywell

SmartPlus Enrollment server, the Registrar notifies the applicant to report to the biometric enrollment station, as indicated in Figure 4-1.

Figure 4-1 *Enrollment Driver*



After the information is entered into the Honeywell SmartPlus Enrollment server, the Registrar sends the completed biometric data package to the driver for storage in the Identity Vault. The driver stores the biometric data and updates the fipsBioStatus attribute with a value of either Biometric Enrollment Complete or Biometric Enrollment Failure. The fipsBioStatusReason and fipsBioStatusExplanation attributes can be updated with relevant success or failure information.

The role of the Enrollment driver is finished at this point in the Identity Assurance Solution.

4.1.4 CMS Driver Overview

The CMS driver for ActivIdentity Active ID is used for the following tasks in the PIV provisioning scenario:

- Creates applicant user accounts in the Card Management System.

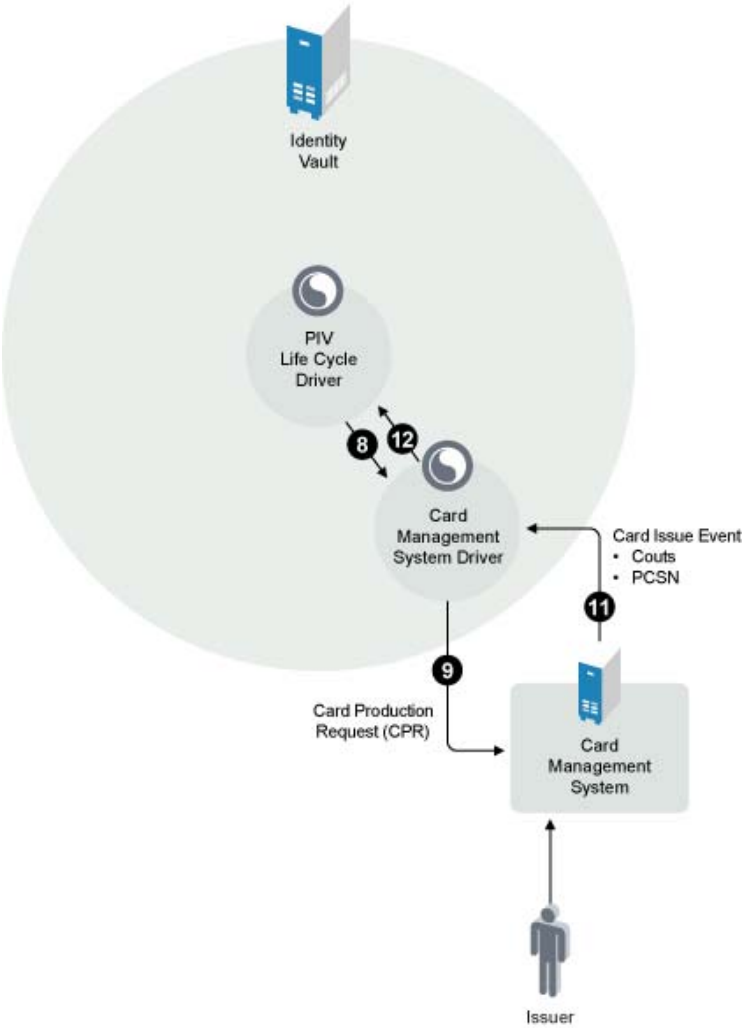
- Sends a Card Production Request (CPR) containing all required data to the Card Management System.
- Notifies Identity Manager of a Card Issued or a Credential Issued event from the Card Management System.
- Sends card information (card serial number, FIPS 201 required certificate, CHUID) back to Identity Manager.
- Sends a Card Termination Request to the Card Management System.

The driver contains policies to detect events that indicate when data should be provisioned to or deprovisioned from the Card Management System.

In order to maintain a simple interface with Identity Manager, the driver is configured to only respond to state changes in the fipsCMSStatus attribute.

The value of this attribute is modified only by the CMS driver or by the PIV Life Cycle driver. After the enrollment process is completed successfully, the PIV Life Cycle driver sets the fipsCMSStatus attribute to a value of PIV Card Production Request Ready and then to CMS User Provisioning Ready. See Figure 4-2.

Figure 4-2 *Card Management System Driver*



If the sponsor approves the PIV issuance, the CMS driver sends a User Add request to the Card Management System. If the User Add request is successful, the fipsCMSStatus attribute is set to CMS User Provisioning Complete. If the Add request fails, the fipsCMSStatus attribute is set to CMS User Provisioning Failed and the fipsCMSStatusReason attribute and fipsCMSStatusExplanation attribute explain why the process failed.

When the CMS User Provisioning is complete, the PIV Life Cycle driver sets the fipsPIVStatus attribute to CMS User Provisioning Complete and ensures that all attributes for a Card Provisioning Request (CPR) are present for the user. If so, the PIV Life Cycle driver sets the fipsCMSStatus attribute and the fipsPIVStatus attribute to PIV Card Production Request Ready.

The CMS driver gathers all available attributes, builds the Card Production Request, and submits it to the Card Management System. If the sponsor approves the Card Production Request, the PIV Life Cycle driver sets the fipsCMSStatus attribute and the fipsPIVStatus attribute to PIV Card Production Approved. The Card Management System driver, then sends a production request to the Card Management System and sets the fipsCMSStatus attribute to PIV Card Issuance Ready.

The CMS driver forwards the results of the card issuance procedure. It sets the fipsCMSStatus attribute to PIV Card Issued and the fipsCMSPhysicalCardSN attribute to the card's serial number value. It also retrieves and stores the card's certificates from the Card Management System in Identity Manager.

4.1.5 PACS Integration Driver Overview

The PACS Integration driver for the Honeywell SMartPlus system is used for the following tasks in the PIV provisioning scenario:

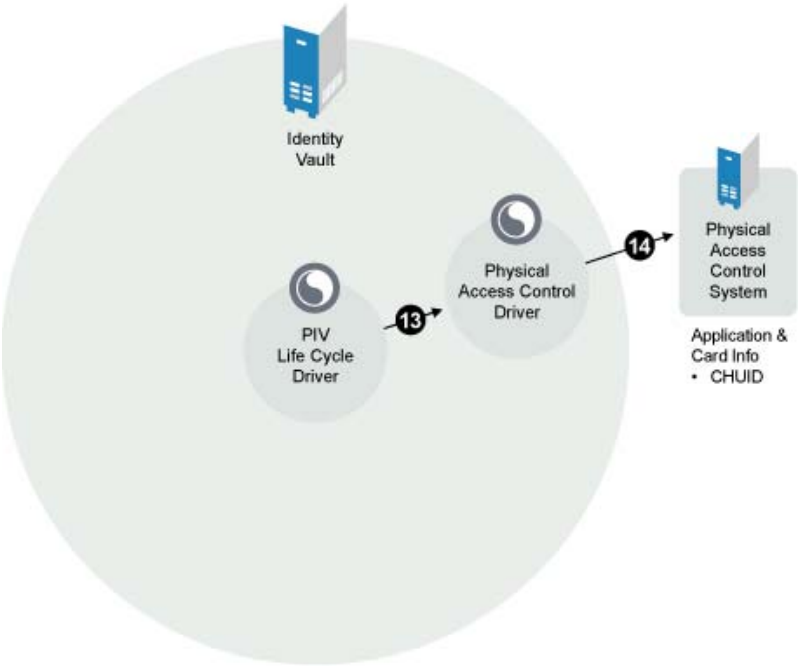
- Creates applicant user accounts in the Physical Access Control system (PACS).
- Sends information to the Honeywell SmartPlus PACS system stating what locations the user has access to.
- Deletes the user from the Honeywell SmartPlus PACS system upon termination.

The driver contains policies to detect events that indicate when data should be provisioned to or deprovisioned from the Honeywell SMartPlus PAC system.

In order to maintain a simple interface with Identity Manager, the driver is configured to only respond to state changes in the fipsPACSStatus attribute.

The value of this attribute is modified only by the PACS Integration driver or by the PIV Life Cycle driver. After the PIV card is issued to the applicant, the PIV Life Cycle driver sets the fipsPACSStatus attribute to a value of PACS Activation Ready. See Figure 4-3.

Figure 4-3 *Physical Access Control System Driver*



This modification event triggers the driver to send the applicant's PIV card information to the Honeywell SmartPlus PACS system. If the information is sent and provisioned successfully, the fipsPACSStatus attributes is set to PACS Activation Ready. If the information failed to be sent to the system, the fipsPACSStatus is set to PACS Activation Failed and the fipsPACSStatusReason and fipsPACSStatusExplanation attributes contain the reason for the failure.

The Honeywell SmartPlus PAC system receives the applicant's information and allows the applicant physical access to the place of employment.

4.2 Configuring the Drivers using iManager

You can manually configure the drivers using iManager. This method of configuring the drivers requires you to complete the following tasks:

- Section 4.2.1, "Configuring the PIV Life Cycle Driver in iManager," on page 35
- Section 4.2.2, "Configuring the PIV Workflow Driver in iManager," on page 35
- Section 4.2.3, "Configuring the Enrollment Driver in iManager," on page 38
- Section 4.2.4, "Configuring the Honeywell SmartPlus Enrollment System," on page 40
- Section 4.2.5, "Configuring the CMS Driver in iManager," on page 40
- Section 4.2.6, "Configuring the ActivIdentity Card Management System," on page 42
- Section 4.2.7, "Configuring the PACS Integration Driver in iManager," on page 44

4.2.1 Configuring the PIV Life Cycle Driver in iManager

When the PIV Life Cycle driver is installed on the Identity Vault server, it is ready to use. You installed the PIV Life Cycle driver previously. See Section 3.5.1, “PIV Life Cycle Driver,” on page 20. No further configuration is required.

4.2.2 Configuring the PIV Workflow Driver in iManager

To import and configure the PIV Workflow Driver, you need to complete the following four tasks in the order listed:

- “Create a Sponsors group in the Identity Vault and add all users who you want to designate as Sponsors” on page 35
- “Configure the PIV Workflow driver to point to the Identity Vault server” on page 35
- “Install User Application for Provisioning” on page 37
- “Assign rights to each of the provisioning requests” on page 37

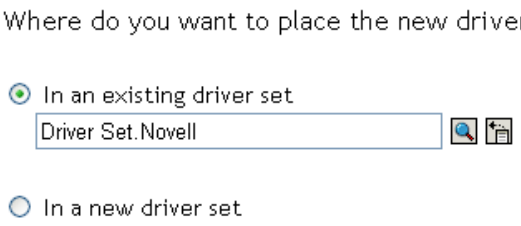
Create a Sponsors group in the Identity Vault and add all users who you want to designate as Sponsors

This is the recommended method for assigning rights. You can also assign trustee rights to individual users also. See “Assign rights to each of the provisioning requests” on page 37.

1. Launch iManager.
2. From the Roles and Tasks menu, select Directory Administration > Create Object.
3. Select Group, then click OK.
4. Specify the group name as Sponsors and specify the context, then click OK > OK.
5. Select Directory Administration > Modify Object.
6. Browse for and select the Sponsors group, then click OK.
7. Click the Members tab, browse and select the users you want in this group, then click OK.

Configure the PIV Workflow driver to point to the Identity Vault server

1. In iManager, select *Identity Manager* > *New Driver*.
2. Select an existing driver set or select a new driver set.



3. If you selected an existing driver set, continue with Step 4.

   or

   If you selected to place the driver in a new driver set, skip to Step 6.
4. If you select an existing driver set, browse to and select the driver set, then click *Next*.

5 Browse to and select the server the driver is associated with, click *Next*, then skip to Step 8.

6 If you selected to place the driver in a new driver set, click *Next*.

7 Define the properties of the new driver set, then click *Next*.

7a Specify the name of the driver set.

7b Browse to and select the context where the driver set will be created.

7c Browse to and select the server you want the driver set associated with.

7d Leave the *Create a new partition on this driver set* option selected.

7e Click *Next*.

We recommend that you create a partition for the driver object. For Identity Manager to function, the server that is associated with the driver set must hold a real replica of the Identity Manager objects. If the server holds a Master or Read/Write replica of the context where the objects are to be created, then the partition is not required.

8 Select *Import a configuration from the server*, browse to and select the `IAS_PIVWorkflow_3_0_1-IDM3_0_1-V1.xml` driver configuration file, then click *Next*.

9 If the driver configuration file is not listed, select *Import a configuration from the client*, then click *Browse*.

9a Browse to and select the driver configuration file from `IAS_MODULES_3.0:\IDMDriver\configs\IAS_PIVWorkflow_3_0_1-IDM3_0_1-V1.xml` from the IAS modules ISO, then click *Open*.

9b Click *Next*.

10 Configure the driver by filling in the configuration parameters, then click *Next*.

10a Specify the name of the driver.

10b Specify the Sponsors group DN.

This is the DN of the Sponsors group you created in "Create a Sponsors group in the Identity Vault and add all users who you want to designate as Sponsors" on page 35

10c Specify the IP address and port number of the server where you will install the User Application in "Install User Application for Provisioning" on page 37.

10d Specify the User Application Administrator's DN.

This is the DN of a user who exists in the Identity Vault that you will designate as the User Application Administrator.

10e Specify the User Application Administrator's password.

11 Select *Define Security Equivalences*.

11a Click *Add*, then browse to and select a user object that has the rights the driver needs to have on the server.

Many administrators use the Administrator User object in the Identity Vault for this task. However, you might want to create another object, such as a DriversUser, and assign sufficient rights to that user for the driver to function. Whatever rights the driver needs to have on the server, the DriversUser object must have the same rights.

11b Click *OK* twice.

12 Select *Exclude Administrative Roles.*

12a Click *Add*, then browse to and select all objects that represent administrative roles and exclude them from replication with the driver.

Exclude the User object in the Identity Vault (for example, DriversUser) that you specified in Step 11. If you delete the User object, you have removed the rights from the driver. Therefore, the driver can't make changes to Identity Manager.

If there are objects that are currently excluded, they do not appear in the *Excluded users* list unless you select *Retrieve Current Exclusions*.

12b Click *OK* twice.

13 Click *Next*.

14 View the summary, then click *Finish with Overview*.

Install User Application for Provisioning

User Application for Provisioning is included in the Novell Identity Manager 3.0.1 build.

For installation instructions, see Installing User Application section of the *Identity Manager 3.0.1 Installation Guide* (http://www.novell.com/documentation/idm/install/data/i1064071.html).

TIP: During the User Application configuration, you need to enter the PIV Workflow driver's distinguished name in the field next to *Provisioning Driver DN*.

Assign rights to each of the provisioning requests

Assign rights to each of the provisioning requests.

There are a set of tasks for PIV Sponsors, and a single task for PIV Applicants. See Table 4-1. You can create groups for PIV Sponsors and PIV Applicants and assign rights to the groups or you can assign rights to individual users or containers.

Table 4-1 *PIV Roles and Tasks*

Roles	Tasks
PIV Sponsors	◆ Request Card for an Applicant ◆ Approve Issuance Request ◆ Suspend Card ◆ Resume Card ◆ Terminate Card ◆ Collect PIV Card ◆ Create Default Settings Object ◆ Edit Default Settings Object ◆ Assign Default Settings Object ◆ Enable User for Re-issuance
PIV Applicants	◆ Request card for yourself

1 Launch iManager.

2 From the *Roles and Tasks* menu, select *Provisioning Request Configuration* > *Provisioning Requests*.

3 Browse for and select the PIV Workflow driver.

4 Click *OK*.

5 Select a workflow task.

6 Click *Actions* > *Define Rights with iManager*.

7 Click *Add Trustee*.

8 Browse for and select the Sponsors group you created in "Create a Sponsors group in the Identity Vault and add all users who you want to designate as Sponsors" on page 35, then click *OK* > *OK*.

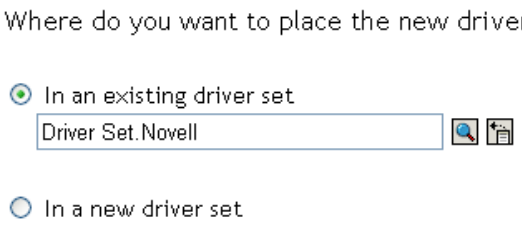
9 Repeat Steps 5 through 8 for all the workflow tasks.

4.2.3 Configuring the Enrollment Driver in iManager

After the driver is installed, it is configured through iManager. (See Section 3.5.3, "Enrollment Driver for Honeywell SmartPlus System," on page 21 for instructions on how to install the driver.) The Enrollment driver configuration file creates the policies that govern how the information is synchronized. If you used the IAS Designer project, you do not need to configure the driver.

1 In iManager, select *Identity Manager* > *New Driver*.

2 Select an existing driver set or select a new driver set.



3 If you selected an existing driver set, continue with Step 4.

or

If you selected to place the driver in a new driver set, skip to Step 6.

4 If you select an existing driver set, browse to and select the driver set, then click *Next*.

5 Browse to and select the server the driver is associated with, click *Next*, then skip to Step 8.

6 If you selected to place the driver in a new driver set, click *Next*.

7 Define the properties of the new driver set, then click *Next*.

7a Specify the name of the driver set.

7b Browse to and select the context where the driver set will be created.

7c Browse to and select the server you want the driver set associated with.

7d Leave the *Create a new partition on this driver set* option selected.

7e Click *Next*.

We recommend that you create a partition for the driver object. For Identity Manager to function, the server that is associated with the driver set must hold a real replica of the

Identity Manager objects. If the server holds a Master or Read/Write replica of the context where the objects are to be created, then the partition is not required.

8 Select *Import a configuration from the server*, then browse to and select the `IAS_IWBioEnrollent-IDM3_0_1-V1.xml` driver configuration file, then click *Next*.

9 If the driver configuration file is not listed, select *Import a configuration from the client*, then click *Browse*.

9a Browse to and select the driver configuration file from `IAS_MODULES_3.0:\IDMDriver\configs\IAS_IWBioEnrollment-IDM3_0_1-V1.xml` from the IAS modules ISO, then click *Open*.

9b Click *Next*.

10 Configure the driver by filling in the configuration parameters, then click *Next*. See Table 4-2 on page 39 for description of each field.

11 Select *Define Security Equivalences*.

11a Click *Add*, then browse to and select a user object that has the rights the driver needs to have on the server.

Many administrators use the Administrator User object in the Identity Vault for this task. However, you might want to create another object, such as a DriversUser, and assign sufficient rights to that user for the driver to function. Whatever rights the driver needs to have on the server, the DriversUser object must have the same rights.

11b Click *OK* twice.

12 Select *Exclude Administrative Roles*.

12a Click *Add*, then browse to and select all objects that represent administrative roles and exclude them from replication with the driver.

Exclude the User object in the Identity Vault (for example, DriversUser) that you specified in Step 11. If you delete the User object, you have removed the rights from the driver. Therefore, the driver can't make changes to Identity Manager.

If there are objects that are currently excluded, they do not appear in the *Excluded users* list unless you select *Retrieve Current Exclusions*.

12b Click *OK* twice.

13 Click *Next*.

14 View the summary, then click *Finish with Overview*.

Table 4-2 *Enrollment Driver Configuration Parameters*

Parameter	Description
Driver name	Specify the name of the driver.
Remote host name and port	Specify the hostname or IP address and port of the Honeywell SmartPlus Enrollment System.
Driver password	Specify the driver object password. It is the same password as specified in Step 8 on page 22 of Install Identity Manager 3.01 for Connected System on the Enrollment Biometric Capture System.

Parameter	Description
Remote password	Specify the Remote Loader password. It is the same password as specified in Step 7 on page 22 of Install Identity Manager 3.01 for Connected System on the Enrollment Biometric Capture System.
KMO Name	Specify the name of the KMO object. See Providing for Secure Data Transfer (http://www.novell.com/documentation/idm/index.html?page=/documentation/idm/admin/data/bs35pi6.html#bs35pi6) for steps on how to create a KMO.
URL of the Biometric Enrollment Server	Specify the URL of the Honeywell Smartplus Enrollment server.
Listening Hostname and Port	Specify the IP address and port of the server where the Remote Loader is installed. It should be the IP address of the Honeywell SmartPlus Enrollment server. See "Install Identity Manager 3.01 for Connected System on the Enrollment Biometric Capture System" on page 21 for more information.

4.2.4 Configuring the Honeywell SmartPlus Enrollment System

The Enrollment/Biometric Capture driver runs on the Honeywell SmartPlus Enrollment system. (For installation instructions, see Section 3.1, "Installing the User Enrollment Biometric Capture Station," on page 17.) The `iws.cfg` file must be modified to communicate with the Identity Manager server.

1. Locate the Tomcat directory where the Honeywell SmartPlus Enrollment Web service is running.
2. Open the *`tomcat_directory`*`/webapps/PIV/WEB-INF/iws.cfg` file in a text editor.
3. Add the following two lines at the bottom of this file:
   - `IDMS=NOVELL`
   - `IDMS_NovellEnrollURL = http://Identity_Manager_server_IP:Publisher_Port_Number`

   The Publisher port number is located on the properties of the Enrollment driver. It can be any port that is not in use on the Identity Manager server.

   3a. In iManager, click *Identity Manager* > *Identity Manager Overview*, then click *Search* to find the driver set objects in the Identity Vault.

   3b. Click the upper right corner of the driver, then select *Edit properties*.

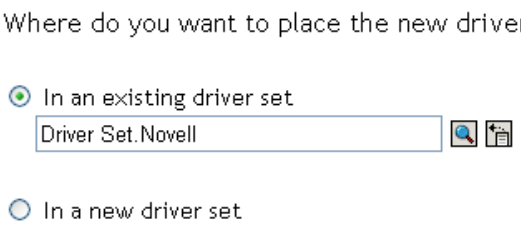
   3c. The Publisher port number is listed under *Driver Configuration* > *Driver Parameters* *Publisher Options* > *Listening IP address and port*.
4. Restart Tomcat.

4.2.5 Configuring the CMS Driver in iManager

After the driver is installed, it is configured through iManager. (See Section 3.5.4, "CMS Driver for ActivIdentity ActivID," on page 22 for instructions on how to install the driver.) The CMS driver configuration file creates the policies that govern how the information is synchronized. If you used the IAS Designer project, you do not need to configure the driver.

1. In iManager, select *Identity Manager* > *New Driver*.

2 Select an existing driver set or select a new driver set.



3 If you selected an existing driver set, continue with Step 4.

or

If you selected to place the driver in a new driver set, skip to Step 6.

4 If you select an existing driver set, browse to and select the driver set, then click *Next*.

5 Browse to and select the server the driver is associated with, click *Next*, then skip to Step 8.

6 If you selected to place the driver in a new driver set, click *Next*.

7 Define the properties of the new driver set, then click *Next*.

7a Specify the name of the driver set.

7b Browse to and select the context where the driver set will be created.

7c Browse to and select the server you want the driver set associated with.

7d Leave the *Create a new partition on this driver set* option selected.

7e Click *Next*.

We recommend that you create a partition for the driver object. For Identity Manager to function, the server that is associated with the driver set must hold a real replica of the Identity Manager objects. If the server holds a Master or Read/Write replica of the context where the objects are to be created, then the partition is not required.

8 Select *Import a configuration from the server*, browse to and select the `IAS_AICMSDriver-IDM3_0_1-V1.xml` driver configuration file, then click *Next*.

9 If the driver configuration file is not listed, select *Import a configuration from the client*, then click *Browse*.

9a Browse to and select the driver configuration file from `IAS_MODULES_3.0:\IDMDriver\configs\IAS_AICMSDriver-IDM3_0_1-V1.xml` from the IAS modules ISO, then click *Open*.

9b Click *Next*.

10 Configure the driver by filling in the configuration parameters, then click *Next*. See Table 4-3 on page 42 for description of each field.

11 Select *Define Security Equivalences*.

11a Click *Add*, then browse to and select a user object that has the rights the driver needs to have on the server.

Many administrators use the Administrator User object in the Identity Vault for this task. However, you might want to create another object, such as a DriversUser, and assign sufficient rights to that user for the driver to function. Whatever rights the driver needs to have on the server, the DriversUser object must have the same rights.

11b Click *OK* twice.

12 Select *Exclude Administrative Roles*.

12a Click *Add*, then browse to and select all objects that represent administrative roles and exclude them from replication with the driver.

Exclude the User object in the Identity Vault (for example, DriversUser) that you specified in Step 11. If you delete the User object, you have removed the rights from the driver. Therefore, the driver can't make changes to Identity Manager.

If there are objects that are currently excluded, they do not appear in the *Excluded users* list unless you select *Retrieve Current Exclusions*.

12b Click *OK* twice.

13 Click *Next*.

14 View the summary, then click *Finish with Overview*.

Table 4-3 *CMS Driver Configuration Parameters*

Parameter	Description
Driver name	Specify the name of the driver.
Remote host name and port	Specify the hostname or IP address and port number where the Remote Loader Service has been installed for this driver.
Driver Password	Specify the driver password. It is the same password as specified in Step 8 on page 23 of the Install Identity Manager 3.0.1 for Connected Systems on the Card Management System.
Remote Password	Specify the remote password. It is the same password as specified in Step 7 on page 23 of the Install Identity Manager 3.0.1 for Connected Systems on the Card Management System.
KMO name	Specify the KMO name.
Client certificate	Specify the path to a client certificate that can be used to initiate an SSL connection with CMS.
Client certificate password	Specify the password to unwrap the client certificate.
Trusted root certificate	Specify the path to a trusted root certificate.
Card Policy	Specify the name of the CMS policy that will be used to issue PIV cards.
CMS users parent AD context	Specify the name of the container in Active Directory where the driver will create CMS users.
Default email domain for CMS users	Specify the default e-mail domain for CMS users.

4.2.6 Configuring the ActivIdentity Card Management System

For this deployment scenario, ActivIdentity Card Management System is being used for the card management system. The CMS driver runs on the ActivIdentity Card Management System. The

installation of the Card Management System was done previously. See Section 3.2, "Installing the Card Management System," on page 17.

You must complete the following steps:

1. Stop IIS.
2. Locate the `/cmsevent` directory located inside the Remote Loader directory created by the CMS Driver Install.
3. Copy the following files from the `/cmsevent` directory to the *`CMS Directory`*`/cms_portal/WEB-INF/lib` directory:
   - `novellplugin.jar`
   - `aims-spi.jar`
4. Copy the following files from the /cmsevent directory to the *`CMS Directory`*`/cms_portal/WEB-INF/conf` directory:
   - `novellplugin.properties`

   NOTE: This file contains a path to `c:\novell\remoteloader\cmsevent\event`. This path must match the event files directory that is configured for the CMS driver. If you accepted all of the default settings during the CMS driver installation, then the paths will match.
5. Edit the *`CMS Directory`*`/cms_portal/WEB-INF/conf/eventnotificationplugins.properties` file.
   - **5a** Locate the `plugins =` line near the top of the file. Add `,novell_plugin` at the end of this line.

     For example, `plugins = piv_notify,novell_plugin`
   - **5b** Add the following two lines at the end of the file:

```
# Novell Event Notification Plugin
novell_plugin.class=com.novell.nds.dirxml.novellplugin.Novel
  lCMSEventPlugin
```

6. Edit the *`CMS Directory`*`/cms_portal/WEB-INF/conf/log4j.properties` file.
   - **6a** Add the following lines at the end of the `List categories for logging` section of this file:

```
log4j.category.com.novell.nds.dirxml.novellplugin =INFO,
  novellplugin
log4j.additivity.com.novell.nds.dirxml.novellplugin = false
```

   - **6b** Add the following lines at the end of this file (replace occurrences of *CMS Dir* below with the directory where CMS is installed):

```
# NOVELL
#--------------------------
log4j.appender.novellplugin =
  org.apache.log4j.RollingFileAppender
log4j.appender.novellplugin.File = CMS Dir/logs/
  novell_plugin.log
log4j.appender.novellplugin.MaxFileSize = 10MB
```

```
log4j.appender.novellplugin.MaxBackupIndex = 20
log4j.appender.novellplugin.layout =
  org.apache.log4j.PatternLayout
log4j.appender.novellplugin.layout.ConversionPattern =
  %d{ISO8601} %-5p [%t] %c{1} %M - %m%n
log4j.appender.credProviders.File=CMS Dir/logs/
  credProviders.log
log4j.appender.InitializationManager.File=CMS Dir/logs/
  InitializationManager.log
```

7 Start IIS.

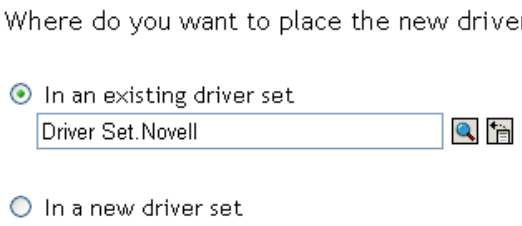
TIP: In order for CMS notification events, such as Suspend/Resume, to be properly propagated to the IDM system, the CMS system needs to have card binding properly configured. For example, where the CMS directory is Microsoft* Active Directory* in the CMS Portal, the setting for Card Binding under the *Configuration/Customization/Directories* section should be set to distinguishedName.

4.2.7 Configuring the PACS Integration Driver in iManager

After the driver is installed, it is configured through iManager. (See Section 3.5.5, "PACS Integration Driver for Honeywell SmartPlus System," on page 23 for instructions on how to install the driver.) The PACS Integration driver configuration file creates the policies that govern how the information is synchronized. If you used the IAS Designer project, you do not need to configure the driver.

1 In iManager, select *Identity Manager* > *New Driver*.

2 Select an existing driver set or select a new driver set.



3 If you selected an existing driver set, continue with Step 4.

or

If you selected to place the driver in a new driver set, skip to Step 6.

4 If you select an existing driver set, browse to and select the driver set, then click *Next*.

5 Browse to and select the server the driver is associated with, click *Next*, then skip to Step 8.

6 If you selected to place the driver in a new driver set, click *Next*.

7 Define the properties of the new driver set, then click *Next*.

- **7a** Specify the name of the driver set.
- **7b** Browse to and select the context where the driver set will be created.
- **7c** Browse to and select the server you want the driver set associated with.

7d Leave the *Create a new partition on this driver set* option selected.

7e Click *Next*.

We recommend that you create a partition for the driver object. For Identity Manager to function, the server that is associated with the driver set must hold a real replica of the Identity Manager objects. If the server holds a Master or Read/Write replica of the context where the objects are to be created, then the partition is not required.

8 Select *Import a configuration from the server*, then browse to and select the `IAS_HoneywellPACS-IDM3_0_1-V1.xml` driver configuration file, then click *Next*.

9 If the driver configuration file is not listed, select *Import a configuration from the client*, then click *Browse*.

9a Browse to and select the driver configuration file from `IAS_MODULES_3.0:\IDMDriver\configs\IAS_HoneywellPACS-IDM3_0_1-V1.xml` from the IAS modules ISO, then click *Open*.

9b Click *Next*.

10 Configure the driver by filling in the configuration parameters, click *Next*. See Table 4-4 on page 45 for description of each parameter.

11 Select *Define Security Equivalences*.

11a Click *Add*, then browse to and select a user object that has the rights the driver needs to have on the server.

Many administrators use the Administrator User object in the Identity Vault for this task. However, you might want to create another object, such as a DriversUser, and assign sufficient rights to that user for the driver to function. Whatever rights the driver needs to have on the server, the DriversUser object must have the same rights.

11b Click *OK* twice.

12 Select *Exclude Administrative Roles*.

12a Click *Add*, then browse to and select all objects that represent administrative roles and exclude them from replication with the driver.

Exclude the User object in the Identity Vault (for example, DriversUser) that you specified in Step 11. If you delete the User object, you have removed the rights from the driver. Therefore, the driver can't make changes to Identity Manager.

If there are objects that are currently excluded, they do not appear in the *Excluded users* list unless you select *Retrieve Current Exclusions*.

12b Click *OK* twice.

13 Click *Next*.

14 View the summary, then click *Finish with Overview*.

Table 4-4 *PACS Integration Driver Configuration Parameters*

Parameter	Description
Driver name	Specify the name of the driver.
Remote host name and port	Specify the hostname or IP address and port of the Honeywell SmartPlus PACS Integration system.

Parameter	Description
Driver password	Specify the driver object password. It is the same password as specified in Step 8 on page 24 of the Install Identity Manager 3.0.1 for Connected Systems on the Physical Access Control System.
Remote password	Specify the Remote Loader password. It is the same password as specified in Step 7 on page 24 of the Install Identity Manager 3.0.1 for Connected Systems on the Physical Access Control System.
KMO Name	Specify the name of the KMO object. See Providing for Secure Data Transfer (http://www.novell.com/documentation/idm/index.html?page=/documentation/idm/admin/data/bs35pi6.html#bs35pi6) for steps on how to create a KMO.
URL of the Honeywell SmartPlus PAC Server	Specify the URL of the Honeywell Smartplus PACS Integration server.
Listening Hostname and Port	Specify the IP address and port of the server where the Remote Loader is installed. It should be the IP address of the Honeywell SmartPlus Enrollment server. See "Install Identity Manager 3.0.1 for Connected Systems on the Physical Access Control System" on page 24 for more information.

4.3 Customizing Your Implementation Using Designer

Designer is a powerful graphical toolset that you can use to customize, test, and document the drivers after you have configured them in iManager. You can import the driver set or drivers from the Identity Vault to create a project in Designer. After you have customized, tested, and documented the drivers in Designer, you can deploy the changes using Designer.

Designer is included on CD 1 - IAS Modules in the `\designer` directory.

For more information on using Designer, see the Designer 1.2 for Identity Manager Documentation Web site (http://www.novell.com/documentation/designer12/index.html).

Troubleshooting Identity Assurance Solution

5

This section provides troubleshooting information for the Identity Assurance Solution installation.

5.1 Known Issues

- COULD_NOT_FIND_USER: Error while retrieving userAIMS_NO_SUCH_WALLET

  If you receive the above message in the Remote Loader trace when attempting to suspend a card in the CMS system and the card is not being suspended in the other systems, you must properly configure the card binding.

Installation Security Guide

A

This section provides information on securely installing and configuring the products included in the Identity Assurance Solution.

Some products have specific security considerations called out in the documentation. Other products have security information dispersed throughout the documentation.

A.1 Novell Products

For additional information on securely installing the Novell products in this solution, see the following resources:

- *Novell eDirectory Installation Guide* (http://www.novell.com/documentation/edir88/edirin88/data/a2iii88.html)
- *Novell iManager 2.6 Installation Guide* (http://www.novell.com/documentation/imanager26/imanager_install_26/data/alw39eb.html)
- *Novell Identity Manager 3.0.1 Installation Guide* (http://www.novell.com/documentation/idm/install/data/front.html)
- *Novell Enhanced Smart Card Method Installation Guide* (http://www.novell.com/documentation/ias/index.html?page=/documentation/ias/nescm_install/data/bookinfo.html)
- *Novell Client for Windows Installation and Administration Guide* (http://www.novell.com/documentation/noclienu/index.html).
- Novell Audit 2.0.2 Installation Guide (http://www.novell.com/documentation/novellaudit20/install/data/bktitle.html).

A.2 Third-Party Products

For information on securely installing the third-party products in this solution, see the documentation provided with the third-party software.