Identity Assurance Solution Readme

February 8, 2008

- Section 1, “Overview,” on page 1
- Section 2, “Known Issues,” on page 5
- Section 3, “Documentation,” on page 6
- Section 4, “Documentation Conventions,” on page 6
- Section 5, “Legal Notices,” on page 6

1 Overview

Identity Assurance Solution by Novell® (IAS) enables federal agencies to comply with the credential issuance, physical and logical access requirements of Homeland Security Presidential Directive 12 (HSPD-12). This solution provides convenient yet controlled access to disparate logical IT systems and physical facilities by using combinations of biometrics, passwords, personal identification numbers, smart cards, X.509 digital certificates, and other forms of advanced authentication.

It is fully integrated with Novell Identity Manager and meets FIPS 201 workflow, identity management, and card life cycle requirements. Personal Identity Verification (PIV) cards issued using this solution enable users to have physical and logical access to facilities and IT systems. This solution enables convergence of IT and physical systems to provide a complete end-to-end and seamless control system.

NOTE: Because eDirectory is restarted during the installation of the `Identity Assurance Life Cycle Driver Patch 3011.exe`, take care of any critical processes that are dependent upon eDirectory before running this installer. Other applications that depend on eDirectory (such as the Identity Manager User Application, NetMail®, etc.) also must be restarted in order to function correctly.

1.1 Installing Commercial Drivers for 3.0.2

IAS 3.0.2 contains commercial driver configurations for the Card Management System (CMS) driver and the Null driver. The Null driver configuration is referred to as the User Notification Driver (UND) in this document.

The commercial driver configurations are for customers who want integration with the ActivIdentity* CMS without configuring the entire Homeland Security Presidential Directive (HSPD-12) solution. If you plan to install such a configuration, then you should follow the steps outlined in Section 1.2, “Installing A New System,” on page 2.

If you plan to install a full HSPD-12 solution, then you should follow instructions in the *Novell IAS 3.0.2 Installation Guide* (http://www.novell.com/documentation/ias302/ias_install/data/bookinfo.html).

The following driver preconfigurations are part of the commercial driver configuration:

- `IAS-Com_AICMS-Driver-IDM3_5_0-V1.xml`
- `IAS-Com_UND-Driver-IDM3_5_0-V1.xml`

The following driver preconfigurations are part of the HSPD-12 driver configuration:

- `IAS_AICMSDriver-IDM3_5_0-V1.xml`
- `IAS_HoneywellPACS-IDM3_5_0-V1.xml`
- `IAS_IWBioEnrollment-IDM3_5_0-V1.xml`
- `IAS_PIVLifeCycle-IDM3_5_0-V1.xml`
- `IAS_PIVWorkflow-IDM3_5_0-V2.xml`

If you already have an HSPD-12 system or are planning to configure one, do not install the preconfigurations from the commercial driver configuration. Likewise, do not use the HSPD-12 preconfigurations with a commercial configuration.

1.2 Installing A New System

Use the following procedure to install a new system using the 3.0.2 commercial configuration with the Card Management System (CMS) driver and User Notification Driver (UND):

1. In the CMS screen, click *Configuration* > *Customization*, then set the following attributes:
   - **1a** On the *Directories* screen, set the User Attribute for Card Binding to userPrincipalName.
   - **1b** On the *Directories* screen, set the User Attribute to Store Card Serial Number as telexNumber. This is a single-value attribute.
   - **1c** On the *User Attributes* screen, map all instances of User ID to the "userPrincipalName" attribute.
2. If your users authenticate to the CMS My Digital ID Card portal using their Active Directory passwords when activating their cards, you must do the following:
   - **2a** In CMS, select *Configuration* > *Security Settings*.
   - **2b** Select LDAP Password from the *Authentication Method when Presented Smart Card is Blank but not Bound* drop-down list.
3. On the CMS server, run the Identity Manager installation, then select "Connected System."

   This installs the IDM Remote Loader.
4. On the CMS server, run the CMS Driver for `ActivIdentity ActivID.exe` InstallShield* executable from IAS 3.0.2.
5. Configure a Remote Loader for CMS as instructed in the *IAS 3.0.2 Installation Guide* (see "Configure the Connected System (Remote Loader)") (http://www.novell.com/documentation/ias302/ias_install/data/b7b8p52.html).
6. On your eDirectory server, run the `PIV Life Cycle Driver.exe` InstallShield executable from IAS 3.0.2.
7. Perform the following steps in iManager:
   - **7a** Create a new driver set in your Identity Vault.
   - **7b** Create a new driver in this driver set using the `IAS-Com_AICMS-Driver-IDM3_5_0-V1.xml` preconfiguration file.

7c Fill out the information to configure the driver as promted.

Fill out this information as instructed. Also, give the driver security equivalence to admin, or another user that has write rights to your user objects.

7d Start the CMS driver and make sure that it connects to its Remote Loader.

It is critical that the CMS driver is running and connected to its Remote Loader before proceeding. The UND driver does not install properly if the CMS driver is not running.

7e Create a new driver using the `IAS-Com_UND-Driver-IDM3_5_0-V1.xml` preconfiguration file.

7f Fill out the information to configure the driver as prompted.

Give the driver security equivalence to admin, or another user that has write rights to your user objects.

7g Start the UND driver.

1.3 Configuring Commercial Mode

When configuring the class filter Scope for the Scan for Eligible CMS Users and Expiring Cards job in the UND driver, be aware that only effective classes can be specified in the class filter. Consequently, auxiliary classes, for example, cannot be used for filtering, so you would need to set the class filter to User instead of setting it to fipsComCMSAux.

The UND driver depends on the CMS driver to perform rights assignments during its configuration. Therefore, the CMS driver must be installed, configured, running, and connected to the Remote Loader on the CMS system before you attempt to configure the UND driver. Failure to meet these conditions results in an error message when you attempt to manually launch the Scan for Eligible CMS Users and Expiring Cards job, even if the UND driver appears to be successfully configured:

```
"The following error occurred trying to run the job, Scan for Eligible
CMS Users and Expiring Cards.User Notification
Driver.CommercialDriverSet.PIV_SSP: Insufficient rights to driver
object..."
```

To resolve this problem, see Section 1.5, “Troubleshooting Issues,” on page 4.

After creating and configuring the UND Driver object, eDirectory must be restarted again or manually launching the Scan for Eligible CMS Users and Expiring Cards job will fail. See Section 1.5, “Troubleshooting Issues,” on page 4 for details on the error that is encountered.

1.4 Submitting Binding Issuance User Requests

The CMS driver automatically submits binding issuance requests for users when the following attributes are populated:

- **fipsPhysicalCardIdentifier:** Contains the card serial number with no spaces.
- **fipsComCMSUPN:** Contains the user's User Principal Name in Active Directory.
- **fipsComCMSATR:** Contains the card Answer to Reset (ATR) string. Cannot contain spaces.
- **Surname:** Family name.
- **Given Name:** The given name.

Fips-prefixed attributes used by the commercial configuration are part of the `fipsComCMSAux` auxiliary class.

If one of the above fips-prefixed attributes is removed from a user, the user's card is terminated. If a user's `fipsPhysicalCardIdentifier` changes, the user's old card is terminated and a binding issuance request is automatically submitted for the new card.

If a user's `fipsComCMSUPN` attribute changes, the user's card is terminated. A binding issuance request is automatically submitted when the card is recycled.

The UND driver is designed to run at scheduled intervals. Use the *Jobs* tab on the iManager driver to schedule times when this driver runs.

When the UND driver runs, it performs the following functions:

- Scans for users who have all of the above listed attributes, but for whom a card issuance request has not yet been submitted. The UND driver submits issuance requests for these users. Users who received the above listed attributes before the CMS driver was installed are in this state.
- Scans for users whose cards are about to expire. If a user's card expiration date falls within the Card Expiration Threshold, then the user is notified via e-mail, and a card renewal request is submitted to CMS. The Card Expiration Threshold can be set in the Global Configuration Values for the UND driver. The default value is 42 days.

1.5 Troubleshooting Issues

- In the UND driver preconfiguration, there are many important instructions that are listed in all capital letters.You should review and follow these instructions carefully.
- The Scan for Eligible CMS Users and Expiring Cards job fails to start with an Insufficient rights to driver object message.

  If the CMS driver is not installed, configured, running, and connected to the Remote Loader on the CMS system before attempting to configure the UND driver, the Scan for Eligible CMS Users and Expiring Cards object does not have sufficient rights to the UND Driver object to perform its job. Use the following procedure to resolve this problem:

  1. In iManager, go to the *Modify Trustees* screen of the UND driver object.
  2. Select *Add as Trustee*, for the Scan for Eligible CMS Users and Expiring Cards object.
  3. Assign Compare, Read, and Write rights to the DirXML-AccessSubmitCommand attribute.
- The Scan for Eligible CMS Users and Expiring Cards job reports that it ran successfully, but fails to act on eligible users. In the Debug output from Identity Manager, a stack trace and an error message similar to the following is encountered:

  `"Code(-9140) Error processing DirXML sub-verb DSVR_START_JOB"`

  After installing and configuring the UND Driver object, eDirectory must be restarted again. If eDirectory is not restarted or if the Scan for Eligible CMS Users and Expiring Cards object is not edited and then saved in iManager, then when a user manually launches the Scan for Eligible CMS Users and Expiring Cards job, a message will indicate that it has run successfully, but there were problems parsing the data in the XmlData attribute, causing it to fail to run the job and send the binding card issuance requests for the eligible users.
- The Identity Manager plug-in hangs when attempting to access the Overview page of a Driver object.

  If your iManager uses Identity Manager 3.5 plug-ins and has the Novell Enhanced Smart Card Method (NESCM) or another plug-in that bundles a recent version of the Shared Content V1 plug-in installed, the error is because of an incompatability between the old 3.5 Identity

Manager plug-ins and the new Shared Content V1 plug-in. To correct the problem, install the Novell Identity Manager 3.5.1 plug-in for iManager 2.6 (http://download.novell.com/SummaryFree.jsp?buildid=90nyRAz-JW0~) or later.

- You might encounter an arrayIndexOutOfBounds error in the IDM Debug trace information when an elegibility attribute is removed from a user who has not had a card issued to him or her. By default, the elegibility attributes are fipsPhysicalCardIdentifier, fipsComCMSUPN, fipsComCMSATR, surname, Given Name. This is normal and does not indicate a failure.
- You will encounter "Unable to Locate ATR" or similar errors in ActivIdentity CMS if there are spaces in either the Card ATR value (of the fipsComCMSATR attribute) or the Card Serial Number value (fipsPhysicalCardIdentifier attribute) for the user. ActivIdentity CMS by default does not handle spaces in these values.

2 Known Issues

Do Not Use the Enter Key When Requesting an Applicant Card

When requesting a card for an applicant, you can type information in the *Delivery Place Info* and *Physical Characteristics* fields, but do not use the Enter key. A hotfix is available for this problem. Contact Novell Support (http://support.novell.com).

Required Browsers for IAS Workflow

Use Firefox* 1.5.x or Internet Explorer* 6x or later when running IAS Workflow.

LDAP Special Characters Not Allowed in User Distinguished Names or Contexts

The following LDAP special characters are not permitted in user distinguished names or contexts:

, + " \ < > ;

Using these characters causes forms to not be auto-populated with default values, and they fail to be submitted.

An error similar to the following will be displayed if any of the above characters are used:

```
Sponsor: Script error in idvault.globalQuery(): Service returned
error. Return code=500, Message=Error encountered while executing the
service globalquery: {1}., Throwable=Ldap error querying for results.
Error: javax.naming.InvalidNameException: O=IasTest: [LDAP: error code
34 - NDS error: illegal ds name (-610)]; remaining name 'O=IasTest'
```

Reset User Workflow Displays Blank Values in the No Fingerprint Field

When an authorized user accesses the Reset User workflow, the No Fingerprints field displays a blank value, indicating that the attribute is unpopulated, even though the fipsNoFingerprints attribute has a value of either TRUE or FALSE.

User Selection Box in the Sponser New Applicant Workflow Displays 'Undefined' When Multiple Usernames are Found by the Search

When using a Firefox browser to search for a user in the Sponsor New Applicant workflow, the selection box displays "undefined" for each username found. This selection box should allow you to select a user by his or her username when the search returns more than one candidate user. Being

unable to see usernames in the box requires the sponsor to choose each user individually and view the user's data in order to find the desired user.

3 Documentation

The following sources provide information about the Identity Assurance Solution:

- Installation: *Identity Assurance Solution Installation Guide* (http://www.novell.com/documentation/ias/index.html?page=/documentation/ias302/ias_install/data/bookinfo.html)
- Online product documentation:

  For Identity Assurance Solution documentation, visit the Identity Assurance Solution Documentation Web site (http://www.novell.com/documentation/ias302/index.html).

  For Novell product documentation, visit the Novell Documentation Web site (http://www.novell.com/documentation).
- Third-party documentation:

  For documentation about third-party software included in this solution, see the documentation provided by the vendor.

4 Documentation Conventions

In this 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

5 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. Please refer to 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.