Novell
Identity Assurance Solution

3.0.1

www.novell.com

ADMINISTRATION GUIDE

July 17, 2007

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 the Novell 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 information on performing basic administration tasks for the Identity Assurance Solution.

Audience

This guide is intended for system 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 Administration Guide*, visit the Identity Assurance Solution Documentation Web site (http://www.novell.com/documentation/ias301/index.html).

Documentation Conventions

In Novell 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 users who are 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).

During the installation of the Identity Assurance Solution, several roles are created. These roles, and their associated tasks, are based on the General Services Administration (GSA) standards. Those users who are assigned to these roles can perform their tasks by using the User Application for Provisioning through a Web browser.

This document outlines the roles and tasks performed by each role for the Identity Assurance Solution.

1.1 System-Wide Roles

This solution includes the following system-wide roles:

Table 1-1 *System-Wide Roles*

System-Wide Role	Description	Tasks
System Role Administrator	Responsible for adding and removing other users from roles in the system. Can add or remove users from all system-wide roles and from the agency role administrator's role for each agency. Cannot add or remove users from agency-specific roles.	◆ Add a User to a System-Wide Role ◆ Remove a User from a System-Wide Role
System Security Officer	Responsible for viewing and managing the audit log. Does not have any specific workflow tasks but is responsible to enforce the rules and policies related to PIV card requests, activations, and issuances.	◆ No workflow tasks

System-Wide Role	Description	Tasks
Activator	Runs the CMS system. Responsible for activating an applicant's PIV card after it comes back from the card production facility. Verifies the applicant's identity by using a biometric scan and oversees the personalization of the card by generating keys, loading certificates onto the card, and initializing the card's PIN number. Sends all this information to the Identity Vault and notifies the system that the card has been issued.	◆ No Applicant Match for Shipped Cards ◆ Wrong Cards Shipped to Valid Address
Registrar	Runs the biometric enrollment system. The registrar does the identity-proofing and captures the applicant's identification information and biometric data. This information is forwarded to the Idenitity Vault.	◆ No workflow tasks

1.2 Agency-Specific Roles

This solution includes the following agency-specific roles:

Table 1-2 *Agency-Specific Roles*

Agency-Specific Role	Description	Tasks
Agency Sponsor	Responsible for initiating a PIV card request on behalf of an applicant and is the only user that can initiate a PIV card request. Updates an applicant's employment status (terminated, active, or suspended) and modifies information about the applicant in the system (change the applicant's name, job title, etc.).	◆ Card Destruction ◆ Create a New User ◆ Delete a User ◆ Display Applicant Info ◆ Request Card Reissuance ◆ Request Card Reprint ◆ Sponsor New Applicant ◆ Update Applicant Employment Status
Agency Adjudicator	Responsible for performing background checks on applicants. At the end of the biometric enrollment process, initiates an Automated Fingerprint Identification System (AFIS) check and the manually performs a National Agency Check with Inquiries (NACI) check or FBI check. Based on the results of these checks, determines if the card request can proceed.	◆ Change the Adjudication Record (Manual)

Agency-Specific Role	Description	Tasks
Agency Security Officer	Responsible to ensure that the agency is following all policies regarding the use of PIV cards. If a PIV card is terminated, the agency security officer collects the card from the user.	◆ Card Destruction ◆ Change PIV Card Status ◆ Invalid Address ◆ Invalid Source Documents ◆ Impersonation Check ◆ Request Card Reprint
Agency Role Administrator	Responsible for adding and removing other users from agency-specific roles.	◆ Add a User to an Agency-Specific Role ◆ Remove a User from an Agency-Specific Role

1.3 What's Next

To view information on performing tasks assigned to system-wide roles, see Chapter 2, "Managing System-Wide Roles," on page 13.

To view information on performing tasks assigned to agency-specific roles, see Chapter 3, "Managing Agency-Specific Roles," on page 15

Managing System-Wide Roles 2

This section outlines the system-wide roles and tasks performed by each role for the Identity Assurance Solution.

When you are working with the workflow forms, all fields with an asterisk (*) are required fields.

2.1 System Role Administrator

A system role administrator can perform the following tasks:

2.1.1 Add a User to a System-Wide Role

This task allows the system role administrator to add a user to a system-wide role.

1. Log in to IAS Workflow as a system role administrator with the appropriate rights.
2. Click *Requests & Approvals* > *Request Resources*.
3. Click *Continue*.
4. Click *Add a User to a System-Wide Role*.
5. Select the system-wide role you want to assign a user to.
6. In the *Search by* field, select a value from the drop-down menu.

   You can search for the user by either typing the user’s last name and date of birth or by typing the user’s Social Security number and date of birth.
7. Select the user.
8. Click *Submit*.

2.1.2 Remove a User from a System-Wide Role

This task allows the system role administrator to remove user from a system-wide role.

1. Log in to IAS Workflow as a system role administrator with the appropriate rights.
2. Click *Requests & Approvals* > *Request Resources*.
3. Click *Continue*.
4. Click *Remove a User from a System-Wide Role.*
5. In the *Search by* field, select a value from the drop-down menu.

You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.

6 Select the user.

7 Click *Remove*.

2.2 System Security Officer

The system security officer is responsible for administering the audit system and does not have any specific workflow tasks.

2.3 Activator

An activator can perform the following tasks:

- Section 2.3.1, "No Applicant Match for Shipped Cards," on page 14
- Section 2.3.2, "Wrong Cards Shipped to Valid Address," on page 14

2.3.1 No Applicant Match for Shipped Cards

If an applicant doesn't claim his or her PIV card, the activator can create an audit log for the event.

1 Log in to IAS Workflow as an activator with the appropriate rights.

2 Click *Requests & Approvals > Request Resources*.

3 Click *Continue*.

4 Click *No Applicant Match for Shipped Cards*.

5 Type a note explaining that the applicant has not claimed his or her card.

6 Select the *Warning and Usage Statement,* then click *Sign Approval*.

7 Click *Submit*.

2.3.2 Wrong Cards Shipped to Valid Address

If the wrong cards are shipped to a valid address, the activator can create and audit log for the event.

1 Log in to IAS Workflow as an activator with the appropriate rights.

2 Click *Requests & Approvals > Request Resources*.

3 Click *Continue*.

4 Click *Wrong Cards Shipped to Valid Address*.

5 Type a note explaining that the wrong cards were shipped.

6 Select the *Warning and Usage Statement,* then click *Sign Approval*.

7 Click *Submit*.

2.4 Registrar

The registrar interacts directly with the biometric enrollment system and does not have any specific workflow tasks.

Managing Agency-Specific Roles 3

This section outlines the agency roles and tasks performed by each role for the Identity Assurance Solution.

When you are working with the workflow forms, all fields with an asterisk (*) are required fields.

3.1 Agency Sponsor

The agency sponsor can perform the following tasks:

3.1.1 Card Destruction

This task allows the sponsor to create an audit trail when a card is destroyed.

1. Log in to IAS Workflow as a sponsor with the appropriate rights.
2. Click *Requests & Approvals* > *Request Resources*.
3. Click *Continue*.
4. Click *Card Destruction*.
5. In the *Search type* field, select a value from the drop-down menu.

   You can search for the user by either typing the user’s last name and date of birth or by typing the user’s Social Security number and date of birth.
6. Click *Search*.
7. Select the user.

   The user and card information are automatically filled in.
8. Select the *Warning and Usage Statement*, then click *Sign Approval*.
9. Ensure that all required fields are filled in, then click *Submit*.

3.1.2 Create a New User

The Identity Assurance Solution has two ways that users are created:

- Human Resources adds the user to the Identity Vault at the time the user is hired.
- The sponsor uses IAS Workflow to add a user to the Identity Vault.

Human Resources Adds the User to the Identity Vault at the Time the User is Hired

In the first instance, Human Resources creates the User object in the Users container with the following attributes populated:

- fipsDateOfBirth (use YYYYMMDD format)
- fipsFirstName
- fipsFirstNameAndMiddleInitial
- fipsMiddleName
- fipsLastName
- fipsFullName
- fipsSSNumber (Use xxx-xx-xxxx format)
- fipsSSNLastFour (last four digits of the SSN)

Human Resource then creates a Card object in the Agency container with the following attributes populated:

- fipsCardAgencyDN (points to the fipsAgency object in the Agency container)
- fipsCardOwnerDN (points to the corresponding user object in the Users container)
- fipsFASCNAgencyCode (four digit agency code for the agency in this container. This can be read from the Agency object.)

After creating the Card object, set the following attribute on the User object you created:

- fipsAgencyCardDNs (Adds a value that points to the card object you created)

The Sponser Uses IAS Workflow to Add a User to the Identity Vault

In the second instance, the sponsor uses this workflow to add a user:

1. Log in to IAS Workflow as a sponsor with the appropriate rights.
2. Click *Requests & Approvals > Request Resources*.
3. Click *Continue*.
4. Click *Create a New User*.
5. Fill in the required fields, then click *Submit*.

3.1.3 Delete a User

When a sponsor deletes a user, the user is removed from the Identity Vault.

1. Log in to IAS Workflow as a sponsor with the appropriate rights.
2. Click *Requests & Approvals > Request Resources*.

3 Click *Continue*.

4 Click *Delete a User*.

5 In the *Search type* field, select a value from the drop-down menu.

You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.

6 Click *Search*.

7 Select the user.

The user information is automatically filled in.

8 Click *Submit*.

3.1.4 Display Applicant Information

This task allows the sponsor to view the applicant's user and card information.

1 Log in to IAS Workflow as a sponsor with the appropriate rights.

2 Click *Requests & Approvals > Request Resources*.

3 Click *Continue*.

4 Click *Diplay Applicant Information*.

5 In the *Search type* field, select a value from the drop-down menu.

You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.

6 Click *Search*.

7 Select the user.

The user and card information are automatically filled in.

8 Click *OK*.

3.1.5 Request Card Reissuance

This task allows the sponsor to force a re-enrollment and have a new PIV card reprinted, if something happens to the original card.

1 Log in to IAS Workflow as a sponsor with the appropriate rights.

2 Click *Requests & Approvals > Request Resources*.

3 Click *Continue*.

4 Click *Request Card Reissuance*.

5 In the *Search type* field, select a value from the drop-down menu.

You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.

6 Click *Search*.

7 Select the user.

The user and card information are automatically filled in.

8. Select a reason why the card is being reissued. The options are:
   - Biometrics no longer valid
   - Damaged
   - Lost
   - Stolen
9. Select the *Warning and Usage Statement*, then click *Sign Approval*.
10. Ensure that all required fields are filled in, then click *Submit*.

3.1.6 Request Card Reprint

This task allows the sponsor to request a reprint of a PIV card without requiring a re-enrollment. A sponsor might use this task if an applicant's name has changed or if a bad card was identified during the application process.

1. Log in to IAS Workflow as a sponsor with the appropriate rights.
2. Click *Requests & Approvals > Request Resources*.
3. Click *Continue*.
4. Select *Request Card Reprint*.
5. In the *Search type* field, select a value from the drop-down menu.

   You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.
6. Click *Search*.
7. Select the user.

   The user and card information are automatically filled in.
8. Select the *Warning and Usage Statement*, then click *Sign Approval*.
9. Ensure that all required fields are filled in, then click *Reprint*.

3.1.7 Sponsor New Applicant

This workflow allows a sponsor to request a PIV card for the following types of applicants:

- **New Applicant:** When a new applicant is entered in the system for the first time, the sponsor fills in any required data fields that don't have a value.
- **Unaffiliated Applicant:** An unaffiliated applicant is a person who has been sponsored before, but whose sponsorship has been terminated or expired. This person is not currently sponsored by an agency. When an agency wants to sponsor an unaffiliated applicant, it can use the Social Security number or last name/date of birth to look up the applicant. All the applicant information will pre-populate in the sponsorship screen and link the applicant to the sponsor's agency.

To start the Sponsor New Applicant workflow:

1. Log in to IAS Workflow as a sponsor with the appropriate rights.
2. Click *Requests & Approvals > Request Resources*.
3. Click *Continue*.

4. Click *Sponsor New Applicant*.
5. For an existing applicant, select a value from the *Search by* drop-down menu, then click *Search*.

   You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.

   For a new applicant, fill in the information for each required field.
6. Select the *Warning and Usage Statement*, then click *Sign Approval.*
7. Ensure that all required fields are filled in, then click *Submit*.

3.1.8 Update Applicant Employment Status

A sponsor can update the employment status of an applicant to one of the following:

- **Active:** This status indicates that the applicant is an active employee in the system. An Active status is required to issue a card and credentials. By changing an applicant's status to Active, you can reactivate a suspended card. Also, if an agent on one of the connected systems reactivates a card, our system will update the card status to *Reactivated*, but the event is not propagated to any other systems until the sponsor sets the user's employee status to *Active*.
- **Suspended:** This status indicates that the employee is temporarily placed on inactive duty. While the employee is in the suspended state, the PIV Card credentials are automatically suspended as well.
- **Terminated:** This status indicates that the employee is terminated and no longer requires the PIV Card credentials. A terminated employment status automatically revokes the PIV Card credentials.

The employment status only impacts the card to which the sponsorship is linked.

To start the Update Applicant Employment Status workflow:

1. Log in to IAS Workflow as a sponsor with the appropriate rights.
2. Click *Requests & Approvals > Request Resources*.
3. Click *Continue*.
4. Click *Update Applicant Employment Status*.
5. In the *Search type* field, select a value from the drop-down menu.

   You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.
6. Click *Search*.
7. Select the user.

   The user information is automatically filled in.
8. In the *Change Employee Status* field, select a new status.
9. Select the *Warning and Usage Statement*, then click *Sign Approval.*
10. Ensure that all required fields are filled in, then click *Submit*.

3.2 Agency Adjudicator

The agency adjudicator performs background checks on the applicants and makes changes to the adjudication record.

3.2.1 Change To Adjudication Record (Manual)

This task allows the adjudicator to enter the results of background checks by the FBI and NACI. If the result is negative, the card and all active credentials are revoked.

This task describes how to use the workflow to manually change the adjudication record. Normally, this task is an auto-started task.

1. Log in to IAS Workflow as an adjudicator with the appropriate rights.
2. Click *Requests & Approvals* > *Request Resources*.
3. Click *Continue*.
4. Click *Change to Adjudication Record (Manual)*.
5. In the *Search type* field, select a value from the drop-down menu.

   You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.
6. Click *Search*.
7. Select the user.

   The user, card, and adjudication record information are automatically filled in.
8. Select a new NACI status.
9. Select a new FBI status.
10. Enter a comment.
11. Ensure that all required fields are filled in, then click *Submit*.

3.3 Agency Security Officer

The agency security officer can perform the following tasks:

- Section 3.3.1, "Card Destruction," on page 20
- Section 3.3.2, "Change PIV Card Status," on page 21
- Section 3.3.3, "Invalid Address," on page 21
- Section 3.3.4, "Invalid Source Documents," on page 22
- Section 3.3.5, "Impersonation Check," on page 22
- Section 3.3.6, "Request Card Reprint," on page 23

3.3.1 Card Destruction

This task allows the agency security officer to create an audit trail when a card is destroyed.

1. Log in to IAS Workflow as an agency security officer with the appropriate rights.
2. Click *Requests & Approvals* > *Request Resources*.

3 Click *Continue*.

4 Click *Card Destruction*.

5 In the *Search type* field, select a value from the drop-down menu.

You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.

6 Click *Search*.

7 Select the user.

The user and card information are automatically filled in.

8 Select the *Warning and Usage Statement*, then click *Sign Approval.*

9 Ensure that all required fields are filled in, then click *Submit*.

3.3.2 Change PIV Card Status

This task allows an agency security officer to change the status of a user's PIV card.

1 Log in to IAS Workflow as an agency security officer with the appropriate rights.

2 Click *Requests & Approvals > Request Resources*.

3 Click *Continue*.

4 Click *Change PIV Card Status*.

5 In the *Search type* field, select a value from the drop-down menu.

You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.

6 Click *Search*.

7 Select the user.

The user and card information are automatically filled in.

8 Select a new PIV Status.

9 Select the *Warning and Usage Statement*, then click *Sign Approval.*

10 Ensure that all required fields are filled in, then click *Submit*.

3.3.3 Invalid Address

If PIV cards are shipped to an invalid address, the agency security officer is responsible to investigate and correct the shipping address.

This task allows the agency security officer to create a signed audit trail if PIV cards are shipped to an invalid address.

1 Log in to IAS Workflow as an agency security officer with the appropriate rights.

2 Click *Requests & Approvals > Request Resources*.

3 Click *Continue*.

4 Click *Invalid Address*.

5 In the *Search type* field, select a value from the drop-down menu.

You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.

6. Click *Search*.
7. Select the user.

   The user and card information is automatically filled in.
8. Type in information about why the address is invalid.
9. Select the *Warning and Usage Statement*, then click *Sign Approval.*
10. Ensure that all required fields are filled in, then click *Submit*.

3.3.4 Invalid Source Documents

This is an auto-started task.

When the registrar validates the authenticity of the source documents and has reasons to believe that one or both documents could be falsified, he or she sets a flag with a message on the enrollment system. This workflow then sends a notice for the agency security officer to investigate.

1. Log in to IAS Workflow as an agency security officer with the appropriate rights.
2. Click *Requests & Approvals > Request Resources*.
3. Click *Continue*.
4. Click *Invalid Source Documents*.
5. Review the provided information.
6. Select the *Warning and Usage Statement*, then click *Sign Approval.*
7. Ensure that all required fields are filled in, then click *Submit*.

3.3.5 Impersonation Check

This is an auto-started task.

When the registrar validates the authenticity of the source documents and has reasons to believe that an applicant is impersonating another user, he or she sets a flag with a message on the enrollment system. This workflow then sends a notice for the agency security officer to investigate.

1. Log in to IAS Workflow as an agency security officer with the appropriate rights.
2. Click *Requests & Approvals > Request Resources*.
3. Click *Continue*.
4. Click *Impersonation Check*.
5. Review the provided information.
6. Select the *Warning and Usage Statement*, then click *Sign Approval.*
7. Ensure that all required fields are filled in, then click *Submit*.

3.3.6 Request Card Reprint

This task allows the agency security officer to request a reprint of a PIV card without requiring a re-enrollment. An agency security officer might use this task if an applicant's name has changed or if a bad card was identified during the application process.

1. Log in to IAS Workflow as an agency security officer with the appropriate rights.
2. Click *Requests & Approvals* > *Request Resources*.
3. Click *Continue*.
4. Select *Request Card Reprint*.
5. In the *Search type* field, select a value from the drop-down menu.

   You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.
6. Click *Search*.
7. Select the user.

   The user and card information are automatically filled in.
8. Select the *Warning and Usage Statement*, then click *Sign Approval*.
9. Ensure that all required fields are filled in, then click *Reprint*.

3.4 Agency Role Administrator

The agency role administrator can perform the following tasks:

- Section 3.4.1, "Add a User to an Agency-Specific Role," on page 23
- Section 3.4.2, "Remove a User from an Agency-Specific Role," on page 24

3.4.1 Add a User to an Agency-Specific Role

This task allows the agency role administrator to add an agency adjudicator.

1. Log in to IAS Workflow as an agency role administrator with the appropriate rights.
2. Click *Requests & Approvals* > *Request Resources*
3. Click *Continue*.
4. Click *Add a User to an Agency-Specific Role*.
5. Select the system-wide role you want to assign a user to.
6. In the *Search by* field, select a value from the drop-down menu.

   You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.
7. Select the user.
8. Click *Submit*.

3.4.2 Remove a User from an Agency-Specific Role

This task allows the agency role administrator to remove user from a system-wide role.

1. Log in to IAS Workflow as an agency role administrator with the appropriate rights.
2. Click *Requests & Approvals > Request Resources*.
3. Click *Continue*.
4. Click *Remove a User from an Agency-Specific Role.*
5. In the *Search by* field, select a value from the drop-down menu.

   You can search for the user by either typing the user's last name and date of birth or by typing the user's Social Security number and date of birth.
6. Select the user.
7. Click *Remove*.

Troubleshooting

4

This section provides Identity Assurance Solution troubleshooting information.

4.1 Known Issues

- 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 Technical Support (http://support.novell.com).
- Use Firefox* 1.5.x or later, Internet Explorer 6 or 7 when running IAS Workflow. IAS Workflow will not work properly with earlier versions of these browsers.

IAS Administration Security

A

This section provides information on security issues related to Identity Assurance Solution and the products that make up the solution.

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

A.1 Identity Assurance Solution

The following issues relate to Identity Assurance Solution:

A.1.1 Signed Workflows

The certificates used in the signed workflows provide non-repudiation, but they do not provide for data integrity or accountability. To ensure the secure transfer of data, you should configure mutual authentication on the User Application server. For more information, see the *Install User Application for Provisioning* section of the *IAS Installation Guide*.

A.2 Novell Products

See the following documents for security information about Novell® products:

- *Novell eDirectory 8.8.1 Administration Guide* (http://www.novell.com/documentation/edir88/edir88/data/a2iii88.html)
- *Novell iManager 2.6 Administration Guide* (http://www.novell.com/documentation/imanager26/imanager_admin_26/data/hk42s9ot.html)
- Security: Best Practices in the *Novell Identity Manager 3.0.1 Administration Guide* (http://www.novell.com/documentation/idm/admin/data/b1bsw73.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 Administration Guide* (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html)

A.3 Third-Party Products

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