Novell
Identity Assurance Solution

3.0

December 20, 2006

ADMINISTRATION GUIDE

Novell®

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html)](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. It is written primarily for network administrators and system integrators.

- Chapter 1, "Managing Sponsor Workflow Tasks," on page 9
- Chapter 2, "Applicant Workflow Tasks," on page 13
- Chapter 3, "Troubleshooting," on page 15

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.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment 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).

Managing Sponsor Workflow Tasks

1

This section describes the procedures performed by the Sponsor for Identity Assurance Solution.

1.1 Creating a User

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

- ◆ Human Resources adds users to the Identity Vault at the time the user is hired.
- ◆ The Sponsor adds a user to the Identity Vault using IAS Workflow.

In the first instance, the user already exists and is available to select for PIV card issuance. However, if the user existed in the Identity Vault before the Identity Assurance Solution was installed and configured, the sponsor will need to enable the user before they can be issued a PIV card.

To enable an existing user:

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

2 Click *Requests & Approvals* > *Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

4 Click *Enable a User for Re-Issuance*.

5 Search for and select a user who you want to reissue a card to, then click OK.

In the second instance, the Sponsor adds a user using IAS Workflow:

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

2 Click *Requests & Approvals* > *Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

4 Click *Create a User*.

5 Fill in the required fields, then click OK.

1.2 Requesting a Card for an Applicant

The Sponsor can request a PIV card for an applicant:

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

2 Click *Requests & Approvals* > *Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

4 Click *Request Card for an Applicant*.

5 Search for and select a user, then click OK.

As a Sponsor, you need to check *My Tasks* regularly, as you will need to perform other tasks relating to issuing a card.

6 From the left-hand menu, click *My Tasks* > *Submit Request Data*.

7 Click *Claim* and fill in all required fields, then click *Submit*.

This action creates the Applicant in the Enrollment system. The Registrar proceeds with the enrollment process (collects the Applicant's biometric data) and, when the process is completed successfully, submits the enrollment request.

8 From the left-hand menu, click *My Tasks > Adjudicate*.

9 Click *Claim*, then click *Approve* or *Deny*.

If you click *Approve*, a Card Production Request is generated and sent to the Card Management System and the Issuer produces the card, gives it to the Applicant and submits the card information back into the Identity Vault. The data needed by the Physical Access Control System is sent and the card is now active.

If you click *Deny*, the card issuance process is terminated.

1.3 Suspending a Card

As a Sponsor, you can suspend a card. This action puts the card on hold but does not terminate the card.

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

2 Click *Requests & Approvals > Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

4 Click *Suspend Card*.

5 Search for and select a user whose card you want to suspend.

6 Select a reason and type in an explanation, then click *OK*.

1.4 Resuming a Card

As a Sponsor, you can resume the use of a suspended card.

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

2 Click *Requests & Approvals > Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

4 Click *Resume Card*.

5 Search for and select a user whose card you want to resume, then click *OK*.

1.5 Terminating a Card

It might be necessary to terminate the use of a card.

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

2 Click *Requests & Approvals > Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

4 Click *Terminate Card*.

5 Search for and select a user whose card you want to terminate. Select a reason and type in an explanation. Then click *OK*.

After terminating a card, the card must be collected. When you collect the card, you are asked if you want to reissue a new card to the user. If you select *true*, the user is automatically enabled for reissuance, and you can run the *Request Card for an Applicant* workflow. If you select *false*, you are specifying that the user should not receive another PIV card. In this case, you must run the *Enable a User for Re-Issuance* workflow before the user can be issued a new card.

1.6 Collecting a PIV Card

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

2 Click *Requests & Approvals* > *Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

4 Click *Collect PIV Card*.

5 Search for and select a user whose card you want to collect. Select whether or not you want to reissue the card, then click OK.

1.7 Enabling a User for Re-Issuance

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

2 Click *Requests & Approvals* > *Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

4 Click *Enable a User for Re-Issuance*.

5 Search for and select a user who you want to reissue a card to, then click *OK*.

1.8 PIV Card Default Settings Tasks

The following PIV Card Default Settings tasks can be performed using IAS Workflow:

1.8.1 Create Default Settings Object

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

2 Click *Requests & Approvals* > *Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card Default Settings*. Then click *Continue*.

4 Click *Create Default Settings Object*.

5 Choose a name and a location for the new Default Settings Object. Then click *OK*.

1.8.2 Assign or Remove Assignment of Default Settings Object

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

2 Click *Requests & Approvals* > *Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card Default Settings*. Then click *Continue*.

4 Click *Assign Default Settings Object*.

5 Select a Default Settings Object. Select either *Assign Object* or *Remove Assignment* from the drop-down list. Specify either a user or a container to assign the Default Settings Object to. Then click *OK*.

1.8.3 Edit Default Settings Object

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

2 Click *Requests & Approvals > Request Resources*.

3 From the drop-down menu next to *Resource Category*, select *PIV Card Default Settings*. Then click *Continue*.

4 Click *Edit Default Settings Object*.

5 Browse for and select the Default Settings Object. Then click *OK*.

6 Make the necessary changes, then click *OK*.

Applicant Workflow Tasks

2

This section describes the Identity Assurance Solution task performed by an applicant user.

2.1 PIV Card Tasks

The following PIV Card tasks can be performed using IAS Workflow:

2.1.1 Request Card for an Applicant

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

  2 Click *Requests & Approvals* > *Request Resources*.

  3 From the drop-down menu next to *Resource Category*, select *PIV Card*. Then click *Continue*.

  4 Click *Request Card for Yourself*.

  5 Search for and select your User object, then click OK.

Troubleshooting

3

This section provides Identity Assurance Solution troubleshooting information.

3.1 Known Issues

- The *Request Card for an Applicant* or *Request Card for Yourself* may fail for users who were created before the PIV Life Cycle driver was installed. You can fix this problem by running the *Enable User for Re-Issuance* workflow for these users.

- When requesting a card for an applicant, in the *Delivery Place Info* and *Physical Characteristics* fields, you can type in information, but do not use the <Enter> key. A hotfix is available for this problem. Contact Novell Technical Services.

- Use Firefox* 1.5.x or later when running IAS Workflow. IAS Workflow will not work properly with Internet Explorer.

Administration Security Guide

A

This section provides information on securely managing 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

- *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.2 Third-Party Products

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