AUTHORIZED DOCUMENTATION

Driver for Google Apps Implementation Guide

Novell®
Identity Manager

4.0.1

February 1, 2011

www.novell.com

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.
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 explains how to install and configure the Identity Manager 4.0.1 Driver for Google Apps.

This guide includes the following information:

- Chapter 1, “Overview,” on page 7
- Chapter 2, “Installing the Driver Files,” on page 11
- Chapter 3, “Creating a New Driver,” on page 13
- Chapter 4, “Customizing the Driver,” on page 27
- Chapter 5, “Managing the Driver,” on page 33
- Chapter 6, “Troubleshooting the Driver,” on page 35
- Appendix A, “Driver Properties,” on page 39

Audience

This guide is for Identity Manager and Google Apps administrators who are using the Identity Manager Driver for Google Apps.

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 this document, see the Identity Manager 4.0 Drivers Documentation Web site (http://www.novell.com/documentation/idm40drivers/index.html).

Additional Documentation

For information on Identity Manager, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/idm40).

Overview

1

Identity Manager 4.0 offers automatic provisioning and synchronization of users to cloud applications. The new Google Apps driver for Novell Identity Manager can seamlessly provision and de-provision users, groups, organizational units, and contacts to the Google Apps cloud application keeping the user identity information consistent across the Identity Vault and the cloud application. The Google Apps driver supports secure password synchronization across Identity Vault and Google Apps. The Google Apps driver for Identity Manager is a Subscriber channel only driver and offers out-of-the box random password generation policy for the newly provisioned users. The Google Apps driver uses a combination of language and protocols to enable identity provisioning and data synchronization between an Identity Vault with Google Apps Driver.

This section contains the following information:

- Section 1.1, “Driver Concepts,” on page 7
- Section 1.2, “Support for Standard Driver Features,” on page 8

1.1 Driver Concepts

- Section 1.1.1, “Data Transfer between Systems,” on page 7
- Section 1.1.2, “How the Driver Works,” on page 8
- Section 1.1.3, “Understanding The Goggle API’s,” on page 8

1.1.1 Data Transfer between Systems

IDM drivers support two data transfer channels between the IDV and the connected system, called the Publisher and Subscriber channels. The Publisher channel handles data and events from the connected system into the IDV. The Subscriber channel handles data and events from the IDV into the connected system.

The Google Apps driver only supports data transfers from the IDV into Google Apps. Communication is one-way only.

- “The Publisher Channel” on page 7
- “The Subscriber Channel” on page 7

The Publisher Channel

The Publisher Channel is not currently supported by this driver.

The Subscriber Channel

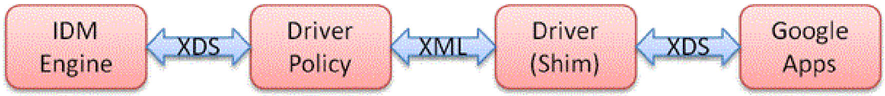
- Monitors the IDV for new objects and changes to existing objects.
- Any relevant changes are sent to the shim to be executed in the Google Apps system.

Through the use of filters and policies, the driver can be configured to control and manage what changes are detected and sent to Google Apps.

1.1.2 How the Driver Works

The following diagram illustrates the data flow between Identity Manager and Google APS API’s:

Figure 1-1 *Google Apps Driver Data Flow*



The Identity Manager engine uses XDS, a specialized form of XML, to represent events in the Identity Vault. Identity Manager passes the XDS to the driver policy, which can consist of basic policies, DirXML Script, and XSLT style sheets.

After driver policy has been applied, the driver shim communicates securely over https to the Google Apps API's for your domain. The results are then communicated back to the driver. The driver then processes that information converting it into an appropriate XDS that is reported back to the Identity Manager engine.

1.1.3 Understanding The Goggle API’s

Google has many different API's available for managing data into and out of the many different Google applications. The 4.0.1 driver supports the following API's:

- Provisioning API - The provisioning API is responsible for creating users and group objects. It is required to turn this API on inside the Google Apps control panel.
- Profile API* - The profile API allows extended attributes to be added to user objects. These include but are not limited to Title, Manager, Phone, Cell, Location, Company. These attributes will be displayed to all domain users in the Address Book (Contacts).
- Contact API* - The contact API is similar to the Profile API with the exception that it will create a Shared Contact inside of the Address Book (Contacts).
- EMail Settings API - The email API allows modification to the default behavior (as set in your Google apps domain) for items related to email.

* The Contact and Profile API Add events do not show in the Google Apps Control Panel and Address Book (Contacts) for up to 24 hours. Modify events will show immediately.

1.2 Support for Standard Driver Features

The following sections provide information about how the Google APPS driver supports these standard driver features:

- Section 1.2.1, “Local Platforms,” on page 8
- Section 1.2.2, “Remote Platforms,” on page 9
- Section 1.2.3, “Supported Operations,” on page 9

1.2.1 Local Platforms

A local installation is an installation of the driver on the Metadirectory server. The Goggle driver can be installed on the operating systems supported for the Metadirectory server.

For information about the operating systems supported for the Metadirectory server, see “Metadirectory Server” in “System Requirements” in the *Identity Manager 4.0 Framework Installation Guide*.

1.2.2 Remote Platforms

The Goggle Apps driver can use the Remote Loader service to run on a server other than the Metadirectory server. The Goggle Apps driver can be installed on the operating systems supported for the Remote Loader.

For information about the supported operating systems, see “Remote Loader” in “System Requirements” in the *Identity Manager 4.0 Framework Installation Guide*.

1.2.3 Supported Operations

The basic configuration files for the Goggle Apps driver are capable of performing the following operations.

- User Objects - Add, Modify, Delete, Query, Rename, set/change password, and Move
- Group Objects - Add, Modify, Delete, Query
- Contact Objects - Add, Modify, Delete, Query

Additional Packages add support for:

- Entitlements: User-Account and Group Membership.
- User Placement: Mirrored and Entitlement based placement..

Installing the Driver Files

2

You must install the Google Apps driver on a server that has direct access to the Google Apps domain. The driver does not support running behind an http proxy server at this time. The Google Apps driver can be installed on multiple systems and platforms. To verify the system requirement list, see "System Requirements" in the *Identity Manager 4.0 Framework Installation Guide*.

This section contains the following information:

- Section 2.1, "Getting the .iso file from the Download Site," on page 11
- Section 2.2, "New Installation by Using a Physical Media or ISO," on page 11

2.1 Getting the .iso file from the Download Site

1. After you have purchased Identity Manager 4.0, log in to the *Novell Customer Center* (http://www.novell.com/center).
2. In the Product or Technology menu, select Novell Identity Manager, then click *Search*.
3. On the Novell Identity Manager Downloads page, click *Download* next to a file you want.
4. Follow the on-screen prompts to download the file to a directory on your computer.
5. Repeat from Step 2 until you have downloaded all the files you need.

If you haven't already verified that the media you burned is valid, you can check it by using the Media Check option; otherwise, refer to the Getting the .iso file from the Download Site section.

2.2 New Installation by Using a Physical Media or ISO

Insert the disc of the Identity Manager 4.0.1 installation media that you created into the CD-ROM or DVD drive of the computer that you want to be your Identity Manager 4.0.1 server.

1. From the CD root folder \Additional_Drivers\GoogleApp, start the installation by executing the correct program for your workstation's platform.
   - **Windows:** `Novell Identity Manager Google Apps Driver-4.0.1-Setup.exe`
   - **Linux:** `rpm -ivh novell-DXMLGoogleApps.rpm`
   - **Solaris:** `pkgadd -d novell-DXMLGoogleApps.pkg`
2. In order to use the pre-config package within Designer, you will need to extend the eDirectory schema using the following steps:
   - **Windows:**
     1. Click Start > Settings > Control Panel > Novell eDirectory Services
     2. Click install.dim, then click Start
     3. Click Install Additional Schema files, then click Next
     4. Log in as a user with administrative rights, then click OK

5. Specify the schema file path and name (<InstallDirectory>\Novell_Google_Schema.sch)
6. Click Finish

- **Linux/Unix:**
  1. /opt/novell/eDirectory/bin/ndssch -h <localhost:524> -t <MyTreename> <admin_fdn> /opt/novell/eDirectory/lib/nds-schema/Novell_Google_Schema.sch

3 It may be necessary to restart eDirecory once the driver binary and schema have been updated.

- **Windows:** Use services to restart your eDirectory Instance.
- **Linux/Unix:**

```
/etc/init.d/ndsd restart
```

NOTE: The admin_fdn is in dot format and not ldap format i.e. admin.novell

Creating a New Driver

3

After the Google Apps driver files are installed on the server where you want to run the driver (see Chapter 2, “Installing the Driver Files,” on page 11), you can create the driver in the Identity Vault. You do so by importing the driver configuration file and then modifying the driver configuration to suit your environment.

The following sections provide instructions to create the driver:

- Section 3.1, “Creating the Driver in Designer,” on page 13
- Section 3.2, “Activating the Driver,” on page 21
- Section 3.3, “Google Apps Requirements,” on page 22

3.1 Creating the Driver in Designer

You create the Goggle Apps driver by importing the driver’s configuration file and then modifying the configuration to suit your environment. After you have created and configured the driver, you need to start it.

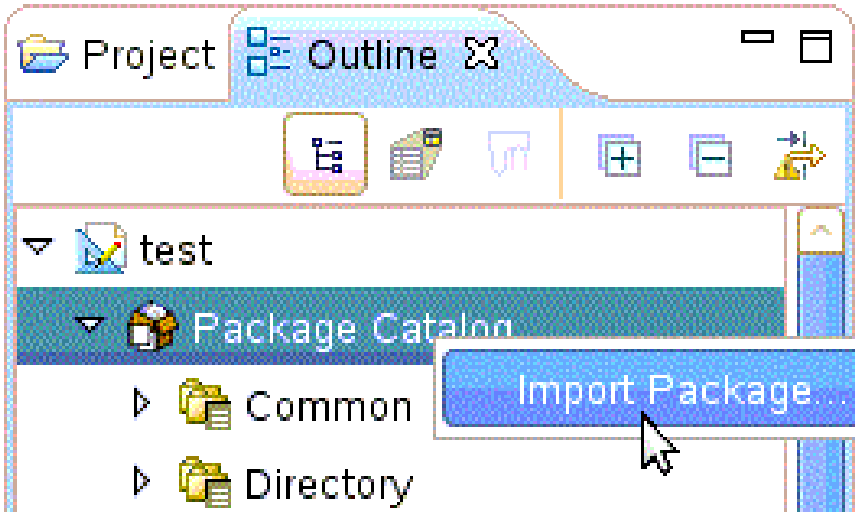
- Section 3.1.1, “Installing the Current Driver Packages,” on page 13
- Section 3.1.2, “Installing the Driver Packages,” on page 14
- Section 3.1.3, “Configuring the Driver,” on page 19
- Section 3.1.4, “Deploying the Driver,” on page 21
- Section 3.1.5, “Starting the Driver,” on page 21

3.1.1 Installing the Current Driver Packages

The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer and can be updated after they are initially installed. You must have the most current version of the packages in the Package Catalog before you can create a new driver object.

To verify that you have the most recent version of the driver packages in the Package Catalog:

1. Open Designer
2. In the toolbar, Left Click Help > Check for Package Updates
3. Left Click OK to update the packages or Left Click OK if the packages are up-to-date
4. In the Outline view, Right Click the Package Catalog
5. Left Click Import Package



6 Select any Google Apps driver packages

Or

Left Click Select All to import all of the packages displayed.

NOTE: By default, only the base packages are displayed. Deselect Show Base Packages Only to display all packages.

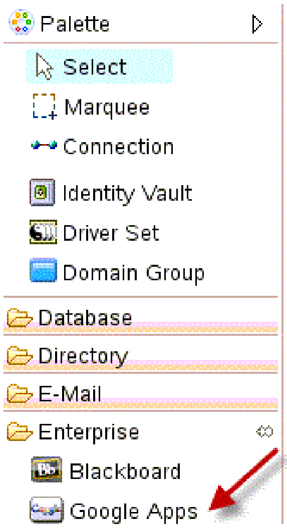
7 Click OK to import the selected packages, and then click OK in the successfully imported packages message.

8 After the current packages are imported, then continue with section,Section 3.1.2, "Installing the Driver Packages," on page 14

3.1.2 Installing the Driver Packages

1 In Designer, open your project.

2 From the Palette, drag-and-drop the Google Apps driver to the desired driver set in the Modeler.

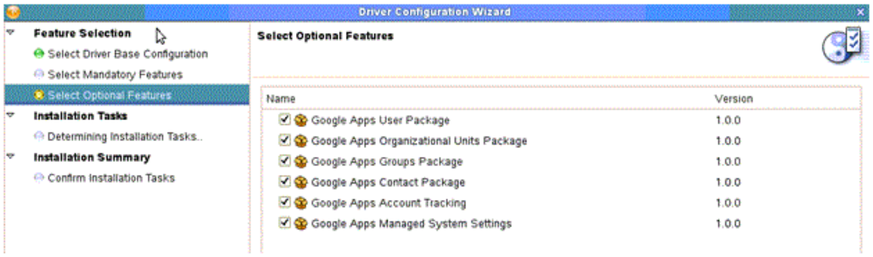


3. Select Google Apps Base, and then Left Click next.
4. Select the optional features to install for the Google Apps driver.

NOTE: By default “show Only applicable packages versions” will be selected as expected.

The Options are:

- Google Apps User Package
- Google Apps Organizational Units Package
- Google Apps Groups Package
- Google Apps Contact Package
- Google Apps Account Tracking
- Google Apps Managed System Settings

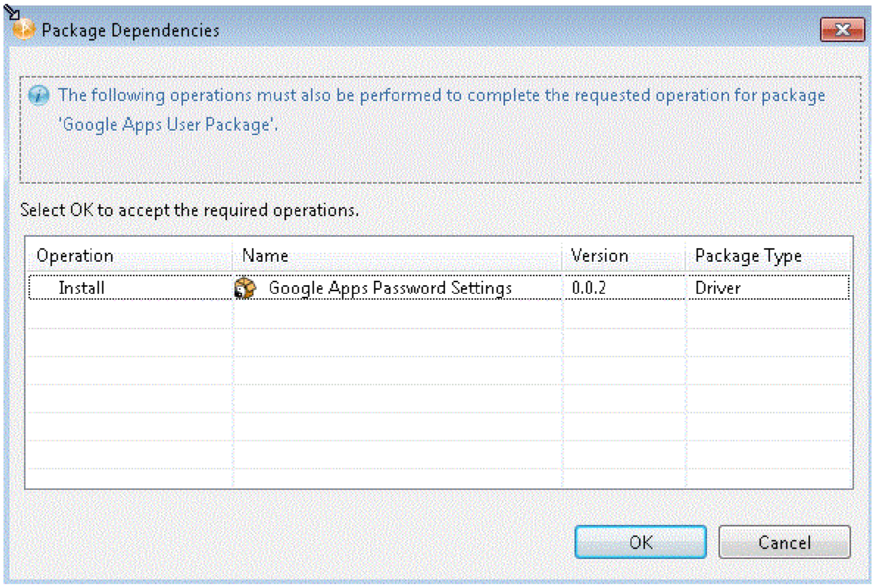

Driver Configuration Wizard
Feature Selection
Select Driver Base Configuration
Select Mandatory Features
Select Optional Features
Installation Tasks
Determining Installation Tasks..
Installation Summary
Confirm Installation Tasks

Select Optional Features

Name	Version
☑ Google Apps User Package	1.0.0
☑ Google Apps Organizational Units Package	1.0.0
☑ Google Apps Groups Package	1.0.0
☑ Google Apps Contact Package	1.0.0
☑ Google Apps Account Tracking	1.0.0
☑ Google Apps Managed System Settings	1.0.0

5. Left Click Next
6. (Conditional) If there are package dependencies for the packages you selected to install, you must install them to install the selected package. Left Click OK to install Package Dependencies.

NOTE: There will be mutable instance of this; one for each option selected.



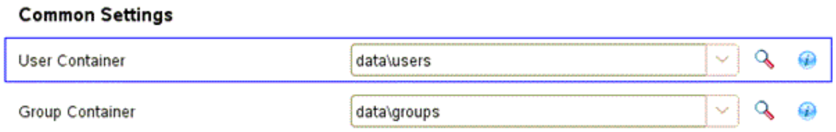
Package Dependencies

The following operations must also be performed to complete the requested operation for package 'Google Apps User Package'.

Select OK to accept the required operations.

Operation	Name	Version	Package Type
Install	Google Apps Password Settings	0.0.2	Driver

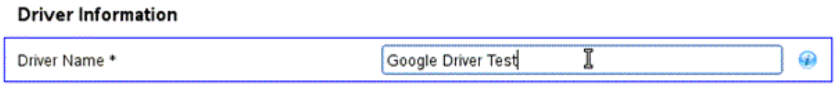
7 Once all dependencies selected are installed, the components will have to be configured. The first will be the common settings for User and Group.



Common Settings

User Container	data\users
Group Container	data\groups

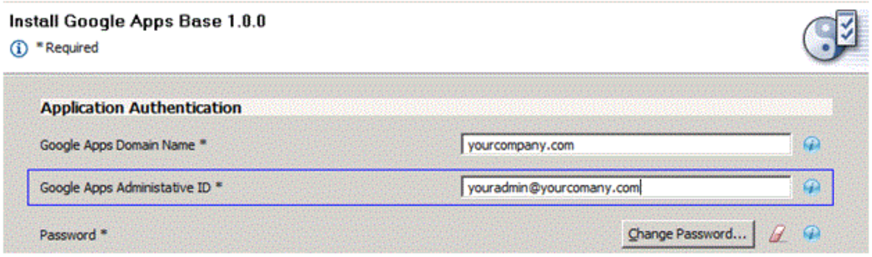
8 On the “Install Google Apps Base” page, specify a name for the driver that is unique within the driver set, and then click next.



Driver Information

Driver Name *	Google Driver Test

9 Configure the suthentication of the application.



Install Google Apps Base 1.0.0

* Required

Application Authentication

Google Apps Domain Name *	yourcompany.com
Google Apps Administative ID *	youradmin@yourcomany.com
Password *	Change Password...

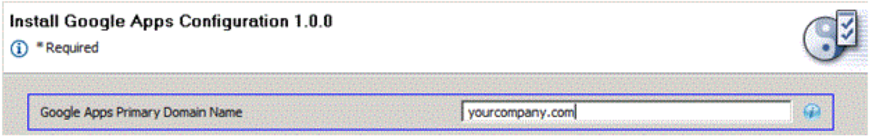
- **Google Apps Domain Name:** Specify the Googel Apps Primanry Doman Name. (example- yourcompany.com)
- **Google Apps Administrative ID:** Specify the email address of a Google Apps administrator.

- **Password:** Specify the password of the accoungt referenced. Select Next when finished.

10 (Optional) Remote loader configuration: Complete this section if and only if a remote loader is being used.

11 (Optional) Verify Realm information, then select Next.

12 (Optional) Specify the name of the Primary Google Apps domain managed by the driver.

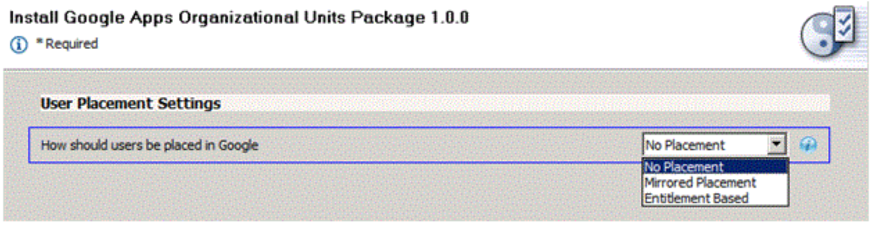


Install Google Apps Configuration 1.0.0

* Required

Google Apps Primary Domain Name: yourcompany.com

13 (Optional) "Installing Google Apps Organizational Units package." This will configure the placement of users.



Install Google Apps Organizational Units Package 1.0.0

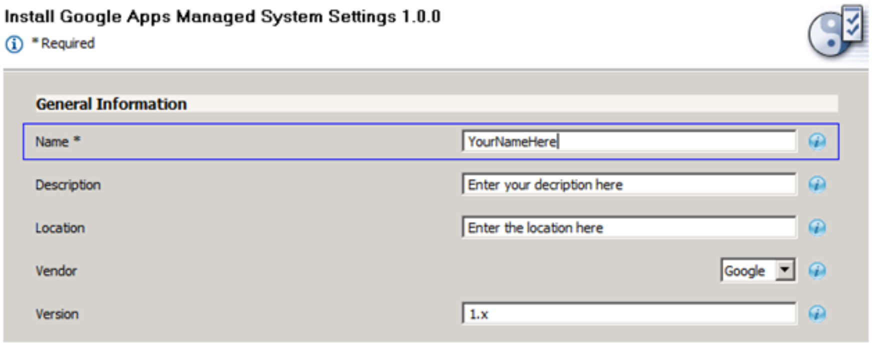
* Required

User Placement Settings

How should users be placed in Google: No Placement

1. **No Placement:** All user accounts will show up in the base of the domain in the Google Management Interface.
2. **Mirror Placement:** The starting base container for all OUs are synchronized to Google and the user's dn will match from that point forward.
3. **Entitlement Based:** Allows you to select the container in Google that a user will be placed in. It will also grant the location with an Entitlement using RBPMS or Legacy.

14 (Optional) "Installing Google Apps Managed System Setting"



Install Google Apps Managed System Settings 1.0.0

* Required

General Information

Name *: YourNameHere

Description: Enter your decription here

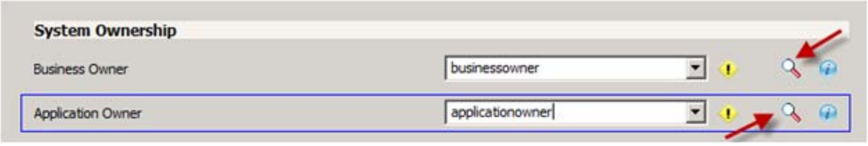
Location: Enter the location here

Vendor: Google

Version: 1.x

1. **Name:** Specify a descriptive name for the managed system.
2. **Description:** Specify a brief description of the managed system.
3. **Location:** Specify the location of the managed system.
4. **Vendor:** Specify the Vendor of the managed system.
5. **Version:** Specify the version of the managed system.

15 (Optional) Install Google Apps Managed System Settings - System Ownership.



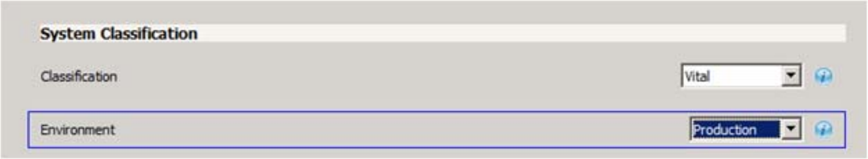
System Ownership

Business Owner	businessowner
Application Owner	applicationowner

NOTE: Select the Search icon and enter login information to browse to selections.

- **Business Owner:** Specify the business owner of the managed system. Select a user object (not a role, group or container).
- **Application Owner:** Specify the application owner of the managed system. Select a user object (not a role, group or container).

16 (Optional) Install Google Apps Managed System Settings - System Classification.

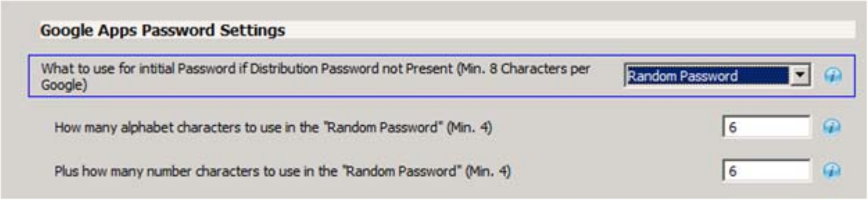


System Classification

Classification	Vital
Environment	Production

- **Classification:** Specify one of the following: Mission Critical, Vital, Not Critical, or Other.
- **Environment:** Specify one of the following: Development, Test, Staging, Production, or Other.

17 (Optional) Install Google Apps Password Settings - Random Selected.

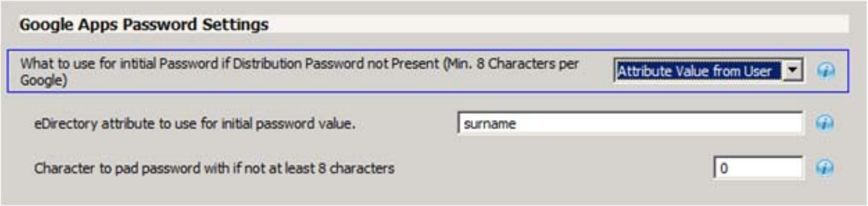


Google Apps Password Settings

What to use for intitial Password if Distribution Password not Present (Min. 8 Characters per Google)	Random Password
How many alphabet characters to use in the "Random Password" (Min. 4)	6
Plus how many number characters to use in the "Random Password" (Min. 4)	6

- **Initial Password:** If the system is not set up for Universal Password syncronization or if the user doesn't have a password set, this will determine the password.
- **Number of Alphabetic Characters:** This determines the number of letters in the random password. This will be combined with the number selected for "number characters".
- **Number of Number Characters:** This determines the number of number characters in the random password. This will be combined with the number selected for "alphabetic characters". (Example: if the number 6 is selected for both numbers and letters, a a random password will have a length of 12.)

18 (Optional) Install Google Apps Password Settings - Attribute

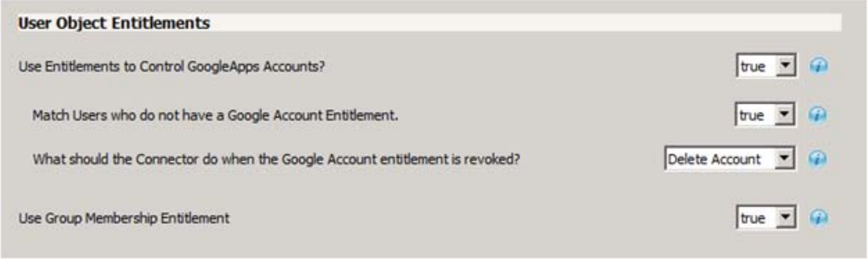


Google Apps Password Settings

What to use for intitial Password if Distribution Password not Present (Min. 8 Characters per Google)	Attribute Value from User
eDirectory attribute to use for initial password value.	surname
Character to pad password with if not at least 8 characters	0

- **eDirectory Attribute:** Enter the name of the attribute in eDirectory that the Google Driver will use for the initial password.
- **Character to pad:** Enter the value to be added to the end of the password if the length of the specified attribute value is less than the minimum number of characters.

19 Install Google Apps User Package



User Object Entitlements

Use Entitlements to Control GoogleApps Accounts?	true
Match Users who do not have a Google Account Entitlement.	true
What should the Connector do when the Google Account entitlement is revoked?	Delete Account
Use Group Membership Entitlement	true

- **Use Entitlements to control Google Apps accounts?** Select either True or False. If set to true, then the entitlement connector must be installed and entitlement must be set to create users in Google Apps.
  - **Match users who do not have a Google account entitlement.** When set to True, users that have not been given an entitlement will be matched to Google users. When set to False, the connector will not attempt to match users without a Google user entitlement and will be blocked at the matching rule.
  - **What should the Connector do when the Google Account entitlement is revoked?** You can choose the default behavoir from *Do Nothing*, *Disable Account*, or *Delete Account*
- **Use Group Membership Entitlement** Select either True or False.

20 Review the Summary.

21 Select *Finish*.

3.1.3 Configuring the Driver

After importing the driver configuration file, you need to configure the driver before it can run. You should complete the following tasks to configure the driver:

- **Configure the driver properties:** There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to review the Driver Parameters located on the Driver Configuration page. The Driver Parameters and the Global Configuration Values let you configure the Google Apps login information and security credentials, and other parameters associated with the Publisher channel. These settings must be configured properly for the driver to start and function correctly. If you do not have the Driver Properties page displayed in Designer:

1. Open your project.
2. In the Modeler, right-click the driver icon or the driver connection, then select Properties.
3. Make any desired changes, then click OK to save the changes.
4. After the driver is created in Designer, it must be deployed to the Identity Vault. Proceed to Section 3.1.4, “Deploying the Driver,” on page 21

- **Authentication:** This panel contains the user account and connection details for your Google Apps subscription. It also contains additional Remote Loader configuration. The driver will require an account with Google Apps which is an administrator for your Google Apps subscription. It is recommended that a new account be created in your Google Apps domain specifically for this purpose. Make sure that this new account is set to administer your Google Apps domain. These values are set during the default import of the driver.

Google Apps Driver Properties

Property	Description	Example Value
Authentican ID	Google Apps Admin Account	idm@yourdomain.com
Connection Information	Your Google Apps Domain	yourdomain.com

Be sure to set the account password in the Application Authentication section of the driver properties.

Driver Configuration

- **Configure the driver parameters:** The driver parameters panel contains driver-specific configuration.

  1. **Driver Options** The Google Apps driver does not use any Driver Options. This panel is intentionally blank.
  2. **Subscriber Options:**
     - **Hash Password** Select *True* to have the Google driver apply an MD5 hash to passwords prior to sending them to Google.
  3. **Publisher Options:**
     - **Heartbeat Interval:** Specify the length of time in seconds the between heartbeats emitted by the Google driver’s publisher channel.

If this GCV is set to true then Groups that have not been given a Google Group Create entitlement will be matched to existing Google Groups. Otherwise the connector will not attempt to match Groups without a Google Group Create entitlement they will just be blocked at the matching rule.

- **Global Configuration Values (GCVs)**

  The GCVs are defined in Table A-6 on page 43

After completing the configuration tasks, continue with Section 3.1.4, “Deploying the Driver,” on page 21.

3.1.4 Deploying the Driver

After the driver is created in Designer, it must be deployed into the Identity Vault.

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon or the driver connection, then select Live > Deploy.

3 Read through the deployment summary, and then click Deploy.

4 Read the success message, and then click OK.

5 Click Define Security Equivalence to assign rights to the driver.

 The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user. Any Rights the driver needs to have on the server need to be assigned to the DriversUser object.

 5a Click Add, then browse to and select the object with the correct rights.

 5b Click OK twice.

6 Click Exclude Administrative Roles to exclude users that should not be synchronized.

 6a Click Add, then browse to and select the user object you want to exclude.

 6b Click OK.

 6c Repeat Step 6a and 6b for each object you want to exclude.

 6d Click OK.

7 Click OK

3.1.5 Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs.

To start the driver:

1 In Designer, select the project view.

2 Click on the Google Apps driver.

3 Click the green start icon.

3.2 Activating the Driver

If you created the Google Apps driver in a driver set that has not been activeate, you must activate the driver with a Google Apps Driver activation within 90 days. If you do not apply a Google Apps Driver activation within 90 days, the driver will stop working.

For more information on activation, refer to "Activating Novell Identity Manager Products" in the Identity Manager 4.0 Framework Installation Guide.

The drivers that are included in the Integration Module for Tools are:

- Driver for Delimited Text
- Driver for SOAP

For information on activation, refer to “Activating Novell Identity Manager Products” in the *Identity Manager 4.0 Framework Installation Guide*.

3.3 Google Apps Requirements

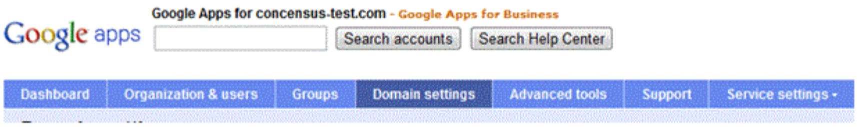
In order for the driver to interact with your domain, the following steps are required:

3.3.1 Enabling the Google Provisioning API Access

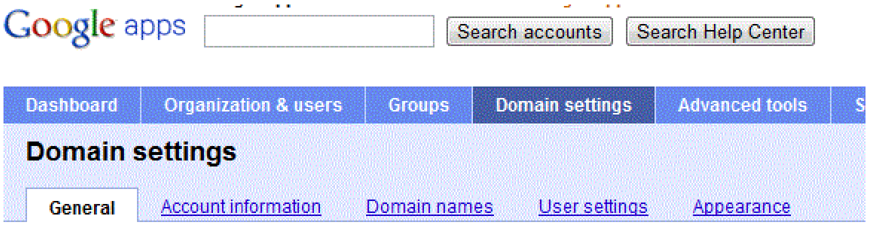
The driver will provision users into Google Apps for Business or Google Apps for Education edition services. It is necessary to enable the Google Provisioning API of your Google Apps subscription before the driver can interoperate with Google Apps.

To enable Google’s API access:

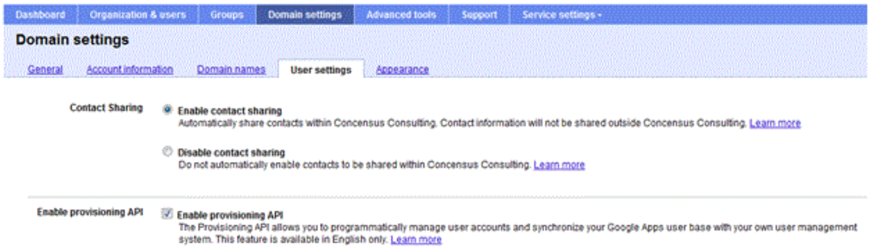
1. Using a web browser, log into the Google Apps Administration Console, typically found at http://www.google.com/a/yourdomainname, where yourdomainname is the Google Apps domain for your subscription. For example, if your Google Apps accounts take the form of username@mydomain.com, then your domain name is mydomain.com.
2. From the Dashboard, select "Domain Settings".



3. From the Domain Settings management page, select "User Settings".



4. Scroll down the Settings page and check the box labeled "Enable Provisioning API".



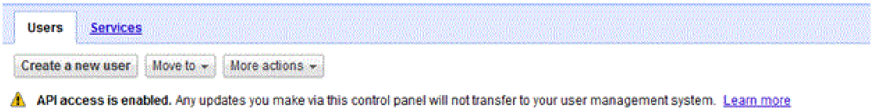
Contact Sharing
● Enable contact sharing
Automatically share contacts within Concensus Consulting. Contact information will not be shared outside Concensus Consulting. Learn more

○ Disable contact sharing
Do not automatically enable contacts to be shared within Concensus Consulting. Learn more

Enable provisioning API
☑ Enable provisioning API
The Provisioning API allows you to programmatically manage user accounts and synchronize your Google Apps user base with your own user management system. This feature is available in English only. Learn more

5. Save the settings by clicking the "Save Changes" button at the bottom of the page.

You can confirm that the API has been enabled by clicking the "Organizations and Users" button at the top of the management console.



API access is enabled. Any updates you make via this control panel will not transfer to your user management system. Learn more

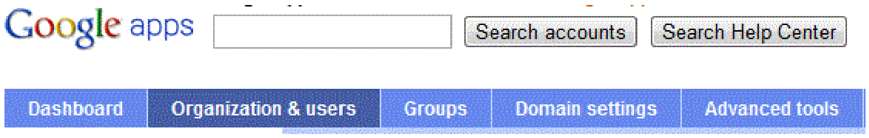
This enables the Provisioning API interface for your Google Apps subscription. This interface provides the access methods which the driver will use to provision and manage users and groups in Google Apps.

3.3.2 Creating a Google Administrative Account

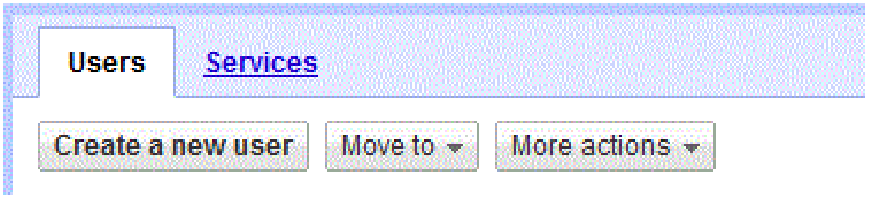
In order for the Google Driver to access the Google Domain and perform administrative functions such as creating users, the driver must log in to the domain using a Google account with Administrative Privileges.

To access the Google Domain:

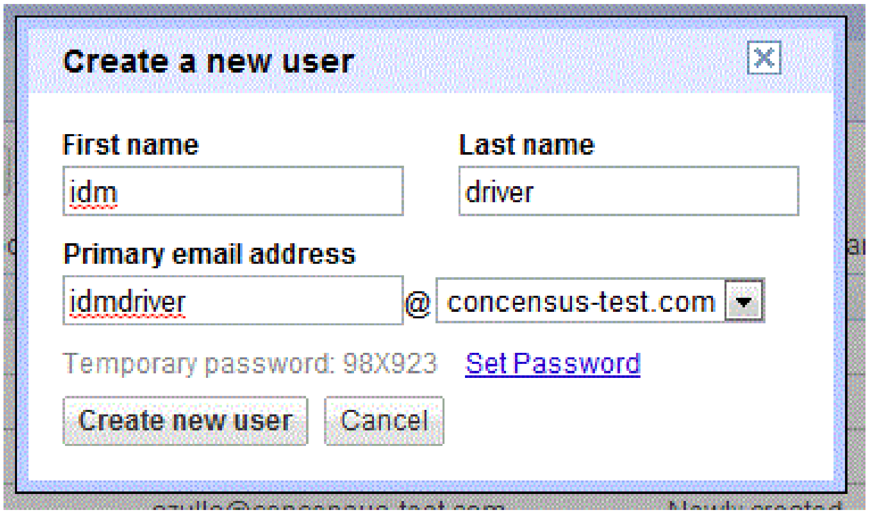
1. Using a web browser, log into the Google Apps Administration Console, typically found at http://www.google.com/a/yourdomainname, where yourdomainname is the Google Apps domain for your subscription. For example, if your Google Apps accounts take the form of username@mydomain.com, then your domain name is mydomain.com.
2. From the Dashboard, select "Organization & Users".



3. Click the Create a New User button.



4. Enter a First Name, Last Name and email address.



Create a new user

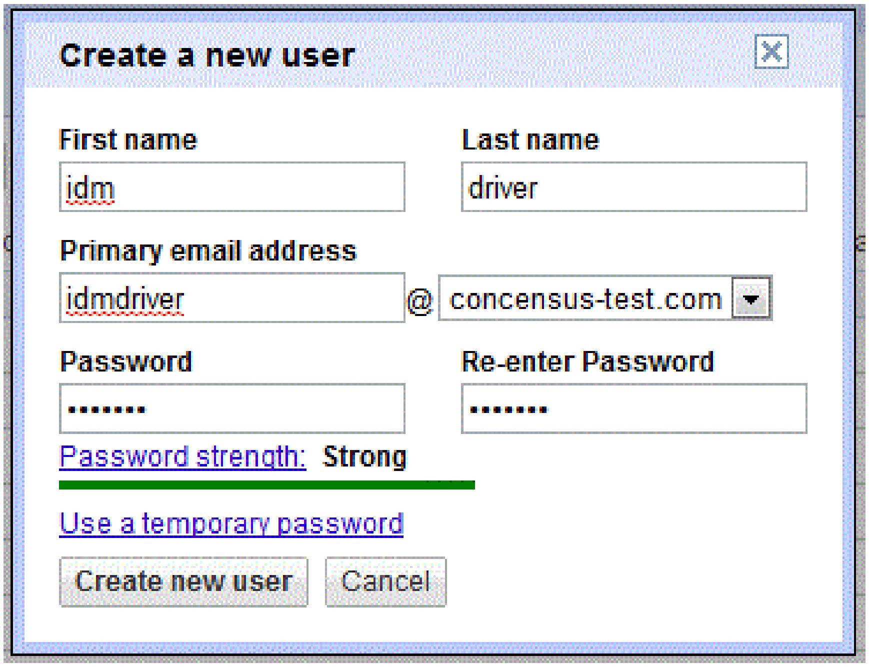
First name: idm

Last name: driver

Primary email address: idmdriver @ concensus-test.com

Temporary password: 98X923

5 Click on the Set Password link and set the password you desire to user for the driver ID.



Create a new user

First name: idm

Last name: driver

Primary email address: idmdriver @ concensus-test.com

Password: •••••••

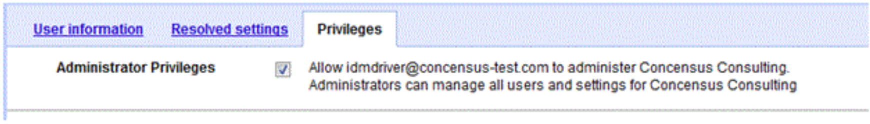
Re-enter Password: •••••••

Password strength: Strong

6 Click Create new user.

7 Find your new Driver ID in the list of Users and select it.

8 Click on the Privileges tab and check the Administrator Privileges box and click Save Changes



Administrator Privileges ☑ Allow idmdriver@concensus-test.com to administer Concensus Consulting. Administrators can manage all users and settings for Concensus Consulting

9 Log out of the Google console and log back in using the new Driver ID.

10 Accept the Google Terms of Service.

Now this ID can be used by the driver to manage the Google domain.

Customizing the Driver

4

The following sections provide information to help you understand what the driver does and what customization you might need to make to the driver:

- Section 4.1, “Managing the Driver,” on page 27
- Section 4.2, “Schema Mapping,” on page 27

4.1 Managing the Driver

As you work with the Google Apps driver, there are a variety of management tasks you might need to perform, including the following:

- Starting, stopping, and restarting the driver
- Viewing driver version information
- Using Named Passwords to securely store passwords associated with the driver
- Monitoring the driver’s health status
- Backing up the driver
- Inspecting the driver’s cache files
- Viewing the driver’s statistics
- Using the DirXML Command Line utility to perform management tasks through scripts
- Securing the driver and its information

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *Identity Manager 4.0 Common Driver Administration Guide*.

4.2 Schema Mapping

This section details the default schema mapping of the driver. The schema map details how IDV attributes and classes are translated into Google Apps attributes and classes.

The section includes:

- Section 4.2.1, “User Attributes Mapping,” on page 27
- Section 4.2.2, “Group Attribute Mapping,” on page 30
- Section 4.2.3, “Organizational Unit Attribute Mapping,” on page 30
- Section 4.2.4, “Contact Attribute Mapping,” on page 30

4.2.1 User Attributes Mapping

IDVault	Google Apps
User	UserEntry

IDVault	Google Apps
	Agreed to terms
Assistant	Assistant
assistantPhone	AssistantPhoneNumber
	Birthday
	Brother
	CallbackPhoneNumber
	ChangePasswordAtNextLogin
	Child
	CompanyMainPhoneNumber
	DomesticPartner
Surname	FamilyName
	Father
	Friend
	Gender
	General
Given Name	GivenName
	GmailSettingsEnableIMAP
	GmailSettingsEnablePOP
	GmailSettingsForwarding
	GmailSettingsLabel
Language	GmailSettingsLanguage
	GmailSettingsSendAs
	GmailSettingsSignature
Groups Memberships	Groups
	HomeFaxPhoneNumber
Home Phone	HomePhoneNumber
	InternalExtensionPhoneNumber
	IpWhiteListed
	IsAdmin
internationalISDNNumber	ISDNPhoneNumber
Login Disabled	IsSupended
	MaidenName

IDVault	Google Apps
	MainPhoneNumber
manager	Manager
mobile	MobilePhoneNumber
	Mother
preferredName	NickNames
	Occupation
OU	OrgDepartment
	OrgJobDescription
L	OrgLocation
company	OrgName
	OrgSymbol
Title	OrgTitle
otherPhoneNumber	OtherPhoneNumber
Pager	PagerPhoneNumber
	Parent
	Partner
nspmDistributionPassword	Password
	ProfileAdditionalName
	ProfileFamilyName
	ProfileFullName
	ProfileGivenName
	ProfileNamePrefix
	ProfileNameSuffix
	Quota
	RadioPhoneNumber
	ReferredBy
	Sister
	Spouse
TelexNumber	TelexPhoneNumber
	TTY_TDDPhoneNumber
CN	UserName
Fascimile Telephone Number	WorkFaxPhoneNumber

IDVault	Google Apps
	WorkMobilePhoneNumber
	WorkPagerPhoneNumber
	WorkPhoneNumber

4.2.2 Group Attribute Mapping

IDVault	Google Apps
Group	Group
Description	Description
DirXML-GAGroupEmailAddress	EmailAddress
Member	Members
CN	Name
Owner	Owners

4.2.3 Organizational Unit Attribute Mapping

IDVault	Google Apps
Organizational Unit	Organizational Unit
	BlockInheritance
Description	Description
OU	Name

4.2.4 Contact Attribute Mapping

The driver does not map directly to a class in eDirectory. The schema can be extended (or mapped to the user object class). The driver contains a sample GoogleContact.sch file that can be used to extend the eDirectory schema. The following table lists the available attributes within Google Apps.

IDVault (EXAMPLE)	Google Apps
GoogleContact	ContactEntry
Assistant	Assistant
assistantPhone	AssistantPhoneNumber
	Birthday
	Brother
	CallbackPhoneNumber

IDVault (EXAMPLE)	Google Apps
	CarPhoneNumber
	Child
	CompanyMainPhoneNumber
	DomesticPartner
	Father
	Friend
	Gender
	General
Given Name	GivenName
	HomeEmailAddress
	HomeFaxPhoneNumber
Home Phone	HomePhoneNumber
internationalISDNNumber	ISDNPhoneNumber
	MaidenName
	MainPhoneNumber
Manager	Manager
mobile	MobilePhoneNumber
	Mother
	Occupation
OU	OrgDepartment
	OrgJobDescription
L	OrgLocation
company	OrgName
	OrgSymbol
Title	OrgTitle
	OtherFaxPhoneNumber
otherPhoneNumber	OtherPhoneNumber
Pager	PagerPhoneNumber
	Parent
	Partner
	ProfileAdditionalName
	ProfileFamilyName

IDVault (EXAMPLE)	Google Apps
	ProfileFullName
	ProfileGivenName
	ProfileNamePrefix
	ProfileNameSuffix
	RadioPhoneNumber
	ReferredBy
	Sister
	Spouse
TelexNumber	TelexPhoneNumber
	TTY_TDDPhoneNumber
CN	UserName
Facsimile Telephone Number	WorkFaxNumber
mobile	WorkMobilePhoneNumber
pager	WorkPagerPhoneNumber
Telephone Number	WorkPhoneNumber

5 Managing the Driver

As you work with the Google Apps driver, there are several management tasks you might need to perform, including the following:

- Starting, stopping, and restarting the driver
- Viewing driver version information
- Using Named Passwords to securely store passwords associated with the driver
- Monitoring the driver’s health status
- Backing up the driver
- Inspecting the driver’s cache files
- Viewing the driver’s statistics
- Using the DirXML Command Line utility to perform management tasks through scripts
- Securing the driver and its information

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *Identity Manager 4.0 Common Driver Administration Guide*.

Troubleshooting the Driver

6

You can log Identity Manager events by using Novell Event Auditing Service. Using this service in combination with the driver log level setting provides you with tracking control at a very granular level.

This section contains the following information on error messages:

- Section 6.1, "Reporting Errors to Identity Manager," on page 35
- Section 6.2, "Google Error Codes," on page 36
- Section 6.3, "Common Driver Issues," on page 37
- Section 6.4, "Troubleshooting Driver Processes," on page 37

6.1 Reporting Errors to Identity Manager

The driver reports errors occurring in both the driver and the Google Domain. All errors reported by the driver follow the Identity Manager Driver error reporting scheme of Status Level and Status Type.

Status Level	Description
Success	The operation succeeded
Warning	The operation succeeded with a warning
Retry	The operation failed because of an error not related to invalid data or a memory or execution error. These are transient errors. For instance, the Google driver issues a Retry when Google reports a Server Busy error.
Error	The operation failed due to an error in xml formatting or a data error.
Fatal	The operation failed as a result of an unrecoverable condition, such as an OutOfMemoryException.

The Status Type provides a way for a driver to indicate the category of the error. For instance, the driver can use Status Type to indicate if a Retry has been issued as a result of application connectivity error. When handling an exception or an error as a result of a transient condition the driver will disconnect from the Google domain and then send a retry request to the Identity Manager engine.   The default retry interval is 30 seconds. Once 30 seconds has elapsed the IDM engine will send the event to the driver again. The driver will detect that it is no longer connected to the Google domain and establish a fresh connection.

The driver will report invalid xml conditions such as invalid class names, attribute names or values with an Error status level.

All other errors will be reported with a Java exception or a Google API exception along with the Status Level and Status Type.

6.2 Google Error Codes

Exception	Cause	Status Level
Java.io.IOException	Interrupted I/O operations	Retry
com.google.gdata.util.ServiceException	An error occurred in Google while processing a request	Error
com.google.gdata.util.AuthenticationException	This is a connection exception received from Google after the driver has successfully authenticated.	Retry
com.google.gdata.util.InvalidEntryException	The Google Entry ID requested is invalid	Error
com.google.gdata.util.ResourceNotFoundException	This exception indicates that a query failed to retrieve a valid object	If the exception is a result of a query the status level is Success, since a query that doesn't resolve to an object is not an error. If the exception is a result of requesting a Google object based on an Association value the Status Level will be Error.
com.google.gdata.util.ServiceException with an error description of "Internal Server Error"	The Google APIs encountered an undefined server error when processing a request.	Retry
Java.net.MalformedURLException	Indicates a malformed URL was received	Error
com.google.gdata.data.AppsForYourDomainException	An exception thrown by AppsForYourDomainService, which is the service which implements Google Provisioning.	The Status Level is dependent on the error code associated with the exception.
Invalid Domain Edition	The Google domain doesn’t support the client library	Fatal
Unknown Error	The provisioning API is reporting an unknown error condition. This is routinely a transient condition.	Retry
Entity does not exist	An exception occurred looking up or querying for an object.	Success if the operation was a query operation. Error if the operation was a lookup based on an association value.
Entity Exists	An attempt to create an object in Google has failed because an object of that name already exists.	Error
All other Apps ForYourDomainException Error Codes		Error

6.3 Common Driver Issues

Issue	Example
User Placement. Do not use a leading "\" to place users or Organization Units.	To place a user in the root container, the dest-dn should only contain the Username. If you are placing a user in the google Sales\Marketing container your dest-dn should look like: <add class-name="User" dest-dn="Sales\Marketing\ddare"/> Organization Units use the same format for dest-dn.
Group Placement: Do not use a placement rule on groups as Google does not support placing groups in organizations.	
Group renames are not supported.	The naming attribute of a group in Google is the email address. Google does not support changing this address after the group has been created. It is up to the deveoper as to how best to capture this event. If the group in eDirectory is renamed the driver will continue to manage the group in Google, but the Google group won't be renamed.
Unique naming: It is important that Nicknames, Group names and usernames be unique in the Google apps domain.	When developing a matching rule be sure to check for nicknames and usernames to ensure proper matching. Further, naming must be unique across all Google Organization units. It is not legal to have Sales\Marketing\ddare and Engineering\ddare since ddare needs to be unique across the domain.

6.4 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see "Viewing Identity Manager Processes" in the *Identity Manager 4.0 Common Driver Administration Guide*.

Driver Properties

A

This section provides information about the Driver Configuration and Global Configuration Values properties for the Google Apps driver. These are the only unique properties for drivers. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to "Driver Properties" in the *Identity Manager 4.0 Common Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with an icon.

- Section A.1, "Driver Configuration," on page 39
- Section A.2, "Global Configuration Values," on page 42
- Section A.3, "Special Attributes," on page 44

A.1 Driver Configuration

In iManager:

1 Click to display the Identity Manager Administration page.

2 Open the driver set that contains the driver whose properties you want to edit:

2a In the *Administration* list, click *Identity Manager Overview*.

2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.

2c Click the driver set to open the Driver Set Overview page.

3 Locate the driver icon, then click the upper right corner of the driver icon to display the *Actions* menu.

4 Click *Edit Properties* to display the driver's properties page.

By default, the Driver Configuration page is displayed.

In Designer:

1 Open a project in the Modeler.

2 Right-click the driver icon or line, then select click *Properties* > *Driver Configuration.*

The Driver Configuration options are divided into the following sections:

A.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.

Table A-1 *Driver Module*

Option	Description
Java	Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the `classes` directory as a class file, or in the `lib` directory as a `.jar` file. If this option is selected, the driver is running locally. The Java class name is: `com.novell.nds.dirxml.driver.gmailshim.GMailDriverShim`
Native	This option is not used with the Google Apps driver.
Connect to Remote Loader	Used when the driver is connecting remotely to the connected system. Designer includes two suboptions: ◆ *Driver Object Password*: Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim. ◆ *Remote Loader Client Configuration for Documentation*: Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.

A.1.2 Driver Object Password

Table A-2 *Driver Object Password*

Option	Description
Driver Object Password	Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page or the remote driver does not run. This password is used by the Remote Loader to authenticate itself to the remote driver shim.

A.1.3 Authentication

The authentication section stores the information required to authenticate to the connected system.

Table A-3 *Authentication*

Option	Description
Authentication ID or *User ID*	This is a User ID on the target Google domain that has administrative rights on the domain. The driver will authenticate to Google Apps using this User ID. If your domain is mydomain.com, then this user id would be in the form: admin@mydomain.com

Option	Description
Authentication Context or ● *Connection Information*	This is the name of the Google domain to be managed by the driver. If your Google domain is named mydomain.com, then you would enter mydomain.com in the Authentication Context.
Remote Loader Connection Parameters or ● *Host name* ● Port ● *KMO* ● *Other parameters*	Used only if the driver is connecting to the application through the remote loader. The parameter to enter is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, when the host name is the IP address of the application server running the Remote Loader server and the port is the port the remote loader is listening on. The default port for the Remote Loader is 8090. The `kmo` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine. Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`
Driver Cache Limit (kilobytes) or ● *Cache limit (KB)*	Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited. ● Click *Unlimited* to set the file size to unlimited in Designer.
Application Password or ● *Set Password*	This option is not used with the Google Apps driver.
Remote Loader Password or ● *Set Password*	Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.

A.1.4 Startup Option

The Startup Option section allows you to set the driver state when the Identity Manager server is started.

Table A-4 *Startup Option*

Option	Description
Auto start	The driver starts every time the Identity Manager server is started.
Manual	The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.
Disabled	The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.

Option	Description
Do not automatically synchronize the driver	This option only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

Table A-5

Parameter Name	Description
Hash Passwords	Setting this subscriber parameter to True tells the driver to apply an MD5 hash to the password before passing it to Google.
Heartbeat Interval	This publisher parameter tells the publisher how frequently to emit a heartbeat document to the IDM engine.

A.2 Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The Google Apps driver includes several predefined GCVs. You can also add your own if you discover you need additional ones as you implement policies in the driver.

To access the driver’s GCVs in iManager:

1 Click to display the Identity Manager Administration page.

2 Open the driver set that contains the driver whose properties you want to edit.

2a In the *Administration* list, click *Identity Manager Overview*.

2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.

2c Click the driver set to open the Driver Set Overview page.

3 Locate the driver icon, click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.

or

To add a GCV to the driver set, click *Driver Set*, then click *Edit Driver Set properties*.

To access the driver’s GCVs in Designer:

1 Open a project in the Modeler.

2 Right-click the driver icon or line, then select *Properties* > *Global Configuration Values*.

or

To add a GCV to the driver set, right-click the driver set icon , then click *Properties* > *GCVs*.

Table A-6 Global Configuration Values

Name	Description	Example Value
Google Apps Domain Name	Specify the name of the Google Apps domain managed by this driver.	mydomain.com
Base Container for users in eDirectory	Only users in or below this container will be synchronized to the connected Google System.	yourorg\users
Use Entitlement for User Account Creation	If this GCV is set to true then users will only be created in Google when the entitlement is granted.	True
Match Users who do not have a Google Account Entitlement.	If this GCV is set to true then users who have not been given an entitlement will be matched to existing Google Accounts. Otherwise the connector will not attempt to match users without a Google Account Entitlement they will just be blocked at the matching rule.	False
What should the Connector do when the Google Account entitlement is revoked?	This GCV determines how the connector will handle a user account who has their Account Entitlement revoked. Do Nothing: This means that if an Account Entitlement is revoked, then the driver will do nothing. The account will remain in the state it was in when it was revoked. Disable Account: If this is selected then when the entitlement is revoked. The account in Google will be disabled.Delete Account: This will tell the connector to Delete the account in Google when the entitlement is revoked.	Do Nothing
Base Container for Groups in eDirectory	Only Groups in or below this container will be synchronized to the connected Google System.	Yourorg/groups
Default visibility for Google Groups.	This GCV sets the default visibility for groups created in GoogleApps. If all your groups will be used as a distribution list available to users on the internet you will need to set the Value to Anyone-Internet Enabled. Note that by using the Policy Builder you can change the permissions on any group during add or modify events.	Owner, Member, Domain, Anyone
Base Container for Organizational Units in eDirectory	Only OU's in or below this container will be synchronized to the connected Google System. If placement is done with mirroring package this GCV is also used as the root container for where the mirror will start.	Myorg

Name	Description	Example Value
What to use for intitial Password if Distribution Password not Present	If the system is not set up for universal password synchronization or the user account just doesnt have a distribution password set yet, then an initial password has to be set. This GCV tells the system whether to use an attribute off of the user account for an initial password or to use a random generated password. If the accounts are going to use SAML for authentication then a Random Password would be fine. Otherwise an attribute value should be selected.	Random Password Attribute Value from User
eDirectory attribute to use for initial password value.	This is the name of the attribute in edirectory that the Google driver should use for an initial password if no Distribution password is available on creation.	Surname
Number of letters to use in the Random Password	This is the number of Letters to use in the random password. when added to the value of the "Random password numbers" GCV It will determine the number of characters in the total Length	6
Number of numbers to use in the Random Password	This is the number of numbers to use in the random password. when added to the value of the "Random password letters" GCV It will determine the number of characters in the total Length.	6

A.3 Special Attributes

Several attributes are exposed for the Goggle Schema that update a users default email settings within a Goggle Domain. these attributes are not mapped to an eDirectory attribute but can be sent on modify or add events. These attributes are:

- GmailSettingsEnableIMAP
- GmailSettingsEnablePop
- GmailSettingsForwarding
- GmailSettingsLabel
- GmailSettingsEnableLanguage
- GmailSettingsSendAs
- GmailSettingsSignature

Table A-7 Special Attributes

Setting	Example
GmailSettingsEnableIMAP Turns on or off IMAP for the Account. Set to True or False.	<add-attr attr-name="GmailSettingsEnableIMAP"> <value type="string">true</value> </add-attr>

GmailSettingsEnablePOP
Turns on or off POP for the Account.
	<add-attr attr-name=”GmailSettingsEnablePOP”>
	    <value type=”structured”>
	        <component name=”EnableFor”>Don DaRe</
	component>
	        <component name=”Action”>don@idmtest.org</
	component>
	        <component name=”Enable”>true</component>
	    </value>
	</add-attr>

GmailSettingsForwarding
Sets a forwarding email address. Note the API only allows setting this to an account inside of the Google Apps Domain. External addresses will cause an error.
	<add-attr attr-name=”GmailSettingsForwarding”>
	    <value type=”structured”>
	        <component name=”ForwardAddress”>Don DaRe</
	component>
	        <component name=”Action”>don@idmtest.org</
	component>
	        <component name=”Enable”>true</component>
	    </value>
	</add-attr>

GmailSettingsLabel This is a set of labels that will be automatically set on the account. The labels will be available in gmail to the end user. .	<add-attr attr-name=”GmailSettingsLabel”> <value type=”string”MyProject</value> </add-attr>
GmailSettingsLanguage This sets the default language for the user.	<add-attr attr-name=”GmailSettingsLanguage”> <value type=”string”Eng</value> </add-attr>

GmailSettingsSendAs
Set this structured value to setup a send as alias. Useful when there are multiple domains or subdomains in Google Apps..
	<add-attr attr-name=”GmailSettingsSendAs”>
	    <value type=”structured”>
	        <component name=”Name”>Don DaRe</component>
	        <component name=”SendAs”>don@idmtest.org</
	component>
	        <component name=”ReplyTo”>Don@idmtest.org</
	component>
	        <component name=”IsDefault”>true</
	component>
	    </value>
	</add-attr>

GmailSettingsSignature Set a default email signature on the user. This is at the user level and can be overridden by the end user.	<add-attr attr-name=”GmailSettingsSignature”> <value type=”string”>Signature Data</value> </add-attr>

Table A-8 Password Configuration

Option	Description
Connected system name	Specify the name of the connected system. This name is used for password sync failure notifications.
Notify the user of password synchronization failure via e-mail	Select this option if you want to notfiy the Google Apps user through e-mail.
Application accepts passwords from Identity Manager	Select whether the application accepts passwords from Identity Manager. Selecting this option to True allows the passwords to flow from the Identity Manager data store to connected system.

Table A-9 Password Configuration

Option	Description
Connected system name	Specify the name of the connected system. This name is used for password sync failure notifications.
Notify the user of password synchronization failure via e-mail	Select this option if you want to notfiy the Google Apps user through e-mail.
Application accepts passwords from Identity Manager	Select whether the application accepts passwords from Identity Manager. Selecting this option to True allows the passwords to flow from the Identity Manager data store to connected system.