

# ID Mapping – Simplifying Heterogeneous File Sharing

## Contents

1. Introduction .....	1	5.2 Mapping a New ID Manually.....	3
2. Overview of Windows Domain Integration.....	1	5.3 Removing a Mapping.....	3
2.1 Windows Integration Options.....	1	5.4 Remove all Mapping.....	3
2.2 Interoperability with Active Directory Authentication .....	2	6. How ID Mapping Affects Other GuardianOS Features.....	3
3. Overview of UNIX NIS Integration.....	2	6.1 ID Mapping and Quotas.....	3
3.1 Handling UID/GID Assignments.....	2	6.2 ID Mapping and Share Access.....	4
4. Predefined and Default GuardianOS Users and Groups .....	2	6.3 ID Mapping and Group Membership .....	4
4.1 UID and GID Assignments.....	2	7. Best Practices for ID Mapping .....	4
5. Mapping UNIX UIDs/GIDs to Windows Users and Groups.....	2		
5.1 Using the Auto Map Feature .....	2		

### 1. Introduction

This whitepaper is intended to detail how the latest GuardianOS release can be integrated into enterprises that support the authentication infrastructures for both Windows Domains and UNIX NIS Domains.

Snap Servers powered by GuardianOS can supply file-sharing services to both Windows via the Common Internet File System (CIFS) and UNIX derivatives via the Network File System (NFS). Since Snap Servers serve both of these client types simultaneously, it is important to be able to support the authentication mechanisms in both environments.

Windows/CIFS clients in an enterprise typically belong to a Windows NT Domain or a Windows Active Directory Domain. UNIX/NFS clients can be authenticated using the Network Information Service (NIS).

In versions of GuardianOS prior to v4.0.228, Windows users and groups and NIS user identifiers (UIDs) and group identifiers (GIDs) were managed separately and considered different users and groups regardless of the intentions of the administrator. The ability to map UIDs and GIDs that exist in NIS to a Windows user and group, respectively, has been added to GuardianOS v4.0.228 through the ID Mapping feature.

This whitepaper will cover the following topics related to this new feature:

- Overview of Windows Domain integration
- Overview of UNIX NIS integration
- Predefined and default GuardianOS users and groups

- Mapping UNIX UIDs/GIDs to Windows users and groups
- How ID mapping affects other GOS features
- Best practices for ID mapping

### 2. Overview of Windows Domain Integration

Snap Servers running GuardianOS can support integration into Windows Domain environments as a member server. Windows Workgroup or Domain authentication is configured on the **Network > Windows** screen of the Web Browser Administration Tool. Specific instructions on how to join a Windows Workgroup or Domain can be found in the Snap Server Administration Guide for GuardianOS or the online help of a GuardianOS-powered Snap Server.

#### 2.1 Windows Integration Options

Windows networks use a Domain Controller to store user credentials. The Domain Controller can validate all authentication requests on behalf of other systems in the domain. In GuardianOS there are two options for configuring authentication with Windows; **workgroup** and **domain**.

**Workgroup** – In a workgroup environment, users and groups are stored and managed separately on each server in the workgroup.

**Domain (NT or ADS)** – When operating in a Windows NT or Active Directory Domain environment, the Snap Server is a member of the domain and the Domain Controller is the repository of all account information. Client machines are also members of the domain and users log into the domain through their Windows-based client machines. Windows or Active Directory Domains resolve user authentication and group membership through the Domain Controller.

## 2.2 Interoperability with Active Directory Authentication

The Snap Server supports the Microsoft Windows 2000/2003 family of servers that run in native ADS mode or in mixed NT/ADS mode. Snap Servers can join Active Directory Domains as member servers. References to the Snap Server's shares can be added to organizational units (OU) as shared folder objects.

## 3. Overview of UNIX NIS Integration

The Snap Server can join an NIS Domain and function as an NIS client. It can then read the users and groups maintained by the NIS Domain. Thus, you must use the NIS server to make modifications. NIS Domain authentication is configured on the **Network > NIS** screen of the Web Browser Administration Tool. Specific instructions on how to join a NIS Domain can be found in the Snap Server Administration Guide for GuardianOS or the online help of a GuardianOS-powered Snap Server. Changes you make on the NIS server do not immediately appear on the Snap Server; it may take up to 10 minutes for changes to be replicated.

### 3.1 Handling UID/GID Assignments

Unless UID/GID assignments are properly handled, NIS users and groups may fail to display properly. For guidelines on integrating compatible Snap Server UIDs, see **UID and GID Assignments** below.

*Tip: NIS identifies users by UID, not user name, and although it is possible to have duplicate user names, Adaptec does not support this configuration.*

## 4. Predefined and Default GuardianOS Users and Groups

There are some predefined users and groups within GuardianOS to be aware of. It is important to understand the protected ranges and how those ranges will incorporate within your existing environment. The protected ranges and other rules to consider will be described below.

### 4.1 UID and GID Assignments

The Snap Server uses the POSIX standard to assign a UID and GID, in which each user and group must have an ID. This requirement applies to all users and groups on the Snap Server, including local, Windows, and NIS users and groups.

If you join the Snap Server to a Windows or NIS Domain, IDs are automatically assigned. UIDs and GIDs are now assigned on a "first come, first served" basis. This means that whichever authentication service claims the UID/GID first gets to use the ID for the user or group.

Consider the following when creating users and groups:

- UIDs and GIDs from 0 - 100 are unavailable for use if you try to use a UID or GID less than 101, you will get an error message.

- If you try to assign a UID or GID that is in use by NIS or the Windows Domain, you will get an error message.
- When local users are created, automatic generation of IDs starts at 18,000. This can be modified manually via the Web Browser Administration Tool.
- When adding a Snap Server to a Windows Domain, the automatic generation of IDs for Windows users and groups will start populating initially at 30,000.
- When the server automatically generates UIDs and GIDs for imported Windows Domain users and groups, UIDs or GIDs that are in the range that would normally be assigned to Windows users, but are already in use by local or NIS users will be skipped.
- When NIS Domain users and groups are imported, the Snap Server will discard any users or groups that have UIDs or GIDs less than 101 or are in conflict with UIDs already in use by local or Windows Domain users and groups.
- The NIS user ID 'nobody' (UID 65534) is reserved. It is not mappable to another ID, nor is another ID mappable to 'nobody'.
- The combined limit for total number of UIDs and GIDs on the Snap Server is 60,000 UIDs and 60,000 GIDs.

*Note: During an OS upgrade to 4.0.228, any previously assigned UIDs/GIDs will be preserved.*

## 5. Mapping UNIX UIDs/GIDs to Windows Users and Groups

GuardianOS v4.0 offers a new ID Mapping feature, which allows mapping of Windows users to local or NIS users to provide unified permission assignments to users of different protocols. Access to the ID Mapping feature is done via the Web Browser Administration Tool in the **Security > ID Mapping** screen.

Prior to mapping any IDs make sure you have joined your NIS Domain and/or Windows Domain so that all of the available groups will be seen in the ID Mapping screen.

If there is existing data on the Snap Server from local or NIS users AND Windows users, the ID Mapping function will propagate and modify the permissions of any existing data to match any new ID mappings that have been created.

*Note: During an OS upgrade to 4.0.228, any previously assigned UIDs/GIDs will be preserved.*

### 5.1 Using the Auto Map Feature

Use the Auto Map feature to generate a list of ID mappings that have the same name as your local or NIS users and groups.

Follow these steps to map names that are an exact match:

- Click on the **Auto Map** button
- A screen will display asking if you want to generate and view the auto ID mappings. Click the **Yes** button.

- Domain, local, and NIS user and group lists are compared. The matches are automatically queued for your review. Any local or NIS user and group names that match Windows user and group names exactly will be mapped. Review the mappings, remove any unwanted mappings, and click the **OK** button to continue.
- The main page will be displayed summarizing all users and groups and any associated mappings. When you are satisfied with the changes, click the **OK** button to save your changes.
- A summary screen will be displayed to verify all changes before starting the propagation process. When satisfied with the changes, click the **OK** button.
- A notice screen will be displayed letting you know that the changes you are requesting will update the file system. Click the **Yes** button to accept and commit the changes to the file system.

*Tip: The propagation process may take a long time, depending upon the number of files and folders you have on your server.*

The next section describes how you can manually adjust the mappings where the names are not an exact match.

### 5.2 Mapping a New ID Manually

In the event that the Auto Map functionality does not map all of your users and groups because the names are not an exact match, you can manually map any remaining users or groups. Within the main ID Mapping screen you have options to manually map users and groups.

Follow these steps to map names that are an **NOT** exact match:

- Within the ID Mapping screen, select a Windows user or group from the list and click the **Map** button.
  - If the desired user or group does not appear in the list, use the **Search** field to locate the desired user or group. Select a domain to search, then click either the “Binocular” button to see a subset of all users and groups in that domain, or the “World” button to display all users and groups in that domain.
- Once you have selected the user or group to map and clicked the **Map** button, select the local or NIS user or group you want to which you want to map the Windows user or group. When finished, click the **OK** button.
- The main page will be displayed summarizing all users and groups and any associated mappings. When you are satisfied with the changes, click the **OK** button to save your changes.
- A summary screen will be displayed to verify all changes before starting the propagation process. When satisfied with the changes click the **OK** button.
- A notice screen will be displayed letting you know that the changes you are requesting will update the file system. Click the **Yes** button to accept and commit the changes to the file system.

### 5.3 Removing a Mapping

Any mappings that you would like to be removed can be done within the main ID Mapping screen.

Follow these steps to remove any individual ID mappings:

- Select the user you wish to un-map and click the **Remove Mapping** button.
- The main page will be displayed summarizing all users and groups and any associated mappings. When you are satisfied with the changes, click the **OK** button to save your changes.
- A summary screen will be displayed to verify all changes before starting the propagation process. When satisfied with the changes click the **OK** button.
- A notice screen will be displayed letting you know that the changes you are requesting will update the file system. Click the **Yes** button to accept and commit the changes to the file system.

### 5.4 Remove all Mapping

In the event that you would like to remove all user and group mappings there is a simple one button process located in the main ID Mapping screen to facilitate this action.

Follow these steps to completely remove all ID mappings:

- Within the main ID Mapping screen, click the **Remove all Mapping** button.
- The main page will be displayed showing that no users or groups are mapped. When you are satisfied with this change, click the **OK** button to save your changes.
- A summary screen will be displayed to verify all changes before starting the propagation process. When satisfied with the changes click the **OK** button.
- A notice screen will be displayed letting you know that the changes you are requesting will update the file system. Click the **Yes** button to accept and commit the changes to the file system.

## 6. How ID Mapping Affects Other GuardianOS Features

As one would expect, the mapping of IDs between UNIX and Windows has some effect on other aspects of the GuardianOS operating system. This section will go through and outline the affected features.

### 6.1 ID Mapping and Quotas

Since ID mapping allows users and groups that exist on Windows Domains to share user IDs with local or NIS users and groups, the same permissions and quota consumption applies to both the Windows Domain user and the local or NIS user. If a quota is set for either the Windows user or the NIS/local user both usernames will display in the Quotas screen

*Example of Quota consumption:*

*John Smith is a local user on a Snap Server, as well as having a*

user ID on a Windows domain. John's quota for the Snap Server has been set to 200MB. The administrator of the Snap Server maps the Windows domain user identification for John Smith to the local identification for John Smith, giving both IDs access to John's 200MB.

## 6.2 ID Mapping and Share Access

When share access is configured for a user that has been mapped, the Windows Domain identity will always be used in the share access list. Since NFS users utilize exports and not the Share Access list, there is no impact on NIS users. However, it does have an effect when Windows Domain users are mapped to local users. Specifically, if the mapped users differ in name or password, and you set a share such that only the mapped identity has access, the Windows Domain version of the identity will be able to access the share, but the local version of the identity will get access denied. This is because GuardianOS performs Share Access checks by user/group name and not UID/GID.

There are two main strategies for dealing with this aspect of ID Mapping:

1. Ensure that the local user/group and the domain user/group have the same username and password, and that all of the group memberships are also mapped and/or;
2. Set access restrictions using file system ACLs (that determine access based on UID/GID) rather than Share Access lists.

## 6.3 ID Mapping and Group Membership

When you map Windows users to NIS or local users you are really only making the UIDs the same. This does not resolve any differences between the two authentication methods with regard to group membership.

For example, if you have a Windows Domain user "DOMAIN\jdoe" with UID 32302 and a NIS Domain user "nis\jdoe" with UID 850, you can use the ID Mapping feature to make both identities use UID 850. However, assume that "DOMAIN\jdoe" is also a member of the Windows group "DOMAIN\Domain Users" (GID 30001) and "DOMAIN\ExcelGroup" (GID 30042). Also assume that "nis\jdoe" is a member of "nis\NisUsers" (GID 800) and "nis\OfficeGroup" (GID 825). The ID Mapping created previously does not merge these group memberships. In order to take care of this, you must also create a custom mapping for the

group memberships as appropriate. In this example, you would map the group "DOMAIN\Domain Users" to "nis\NisUsers" and "DOMAIN\ExcelGroup" to "nis\OfficeGroup" (assuming they are equivalent groups). This way, the group memberships are consistent across all protocols from which the user may log in.

## 7. Best Practices for ID Mapping

For the best results in integrating all local, NIS and Windows Domain users onto a Snap Server, it is important to go about preparing the system for the ID Mapping very carefully. Since each user type operates independently, you can only map local users and groups OR NIS users and groups to Windows users and groups. You cannot map local users to NIS users because this feature was designed to allow mapping between Windows Domain users and UNIX users.

In order to ensure the best possible result for integrating into an NIS Domain and a Windows Domain and subsequently mapping users from both environments it is best to follow these steps in order:

### Step 1: Join NIS Domain

### Step 2: Add any local users and groups

### Step 2: Join Windows Domain

### Step 3: Auto Map any users and groups that have exact matches

### Step 4: Add additional mappings that are not exact name matches

Remember the following two important points as well:

1. Create the appropriate share access when mapping local users to Windows Domain users. For example you may need to create identical share access permissions for the local user "jdoe" as well as for the Windows Domain user "DOMAIN\jdoe". Best practice would be to allow all share level access and to create and maintain all access permissions through the file and folder level ACLs managed from an administrative Windows box on the domain. A combination of both share access and file/folder permissions may be preferable to some.
2. Make sure to not only map users but also groups, so that all permissions and file accesses are appropriately maintained.



**Adaptec, Inc.**  
691 South Milpitas Boulevard  
Milpitas, California 95035  
Tel: (408) 945-8600  
Fax: (408) 262-2533

#### Literature Requests:

US and Canada: 1 (800) 442-7274 or (408) 957-7274  
World Wide Web: <http://www.adaptec.com>

**Pre-Sales Support:** US and Canada: 1 (800) 442-7274 or (408) 957-7274  
**Pre-Sales Support:** Europe: Tel: (44) 1276-854528 or Fax: (44) 1276-854505

Copyright 2005 Adaptec, Inc. All rights reserved. Adaptec, the Adaptec logo, Snap Appliance, the Snap Appliance logo, Snap Server, Snap Disk, GuardianOS, SnapOS, and Storage Manager are trademarks of Adaptec, Inc., which may be registered in some jurisdictions. Microsoft and Windows are registered trademarks of Microsoft Corporation, used under license. All other trademarks used are owned by their respective owners.

Information supplied by Adaptec, Inc., is believed to be accurate and reliable at the time of printing, but Adaptec, Inc., assumes no responsibility for any errors that may appear in this document. Adaptec, Inc., reserves the right, without notice, to make changes in product design or specifications. Information is subject to change without notice.