NSS – How to setup with Active Directory

NSS AD setup instructions

This document covers how to set up Active Directory for user import and authentication in NetBackup Self Service.

Biomni Ltd, 4 Bloomsbury Square, London, WC1A 2RP -T: +44(0) 20 7557 4200 F +44(0) 20 7557 4201 E: info@biomni.com

Contents

1.0 Overview

Please find below a digest of how to set up Active Directory (AD) import and authentication for NetBackup Self Service (NSS).

There are 2 main activities:

1. Create Active Directory user import tasks
2. Enable Single Sign on via Windows Authentication

2.0 Create AD User import task

2.1 Decide user ID format

Decide how to store user IDs in the system.

<Windows Name> (i.e. john.smith)

Or

<Domain>\<Windows Name> (i.e. BIOMNI-US\john.smith)

If you are importing NSS users from multiple domains, and their Windows Name cannot be guaranteed to be unique, then the latter form should be used to avoid potential duplicate user IDs.

2.2 Set system setting to determine user ID format on import

When using the Active Directory user import functionality, the user ID format is set by the NSS system setting "Set Domain Name rules for User login"

To change:

1. Log into NSS as ADMIN
2. Access Admin -> Settings -> System Configuration
3. Search for "Domain"
4. Set to Yes if you wish to store as <Windows Name> No if you want <Domain>\<Windows Name>

2.3 Create Active Directory OU or Groups

When creating rules to import users into NSS, Active directory groups or organizational units (OUs) are used to map users to NSS tenants and to NSS roles.

Within NSS, users are placed within tenants. Users within a tenant can only action protection, backup and restore to client machines also registered within that tenant.

There are three types of users within NSS.

NSS Administrators

Users who have full access to configure the system. These users are not members of a tenant.

Tenant Users

Standard end-users who will log into NSS and perform actions and view dashboards against client computers registered within the same tenant

Tenant administrators

With the same rights as tenant users, but also with the ability to assign permissions to other users within the tenant limiting their access to perform actions against client computers within that tenant.

These users can also manually create other tenant users, although this ability will likely not be used if AD user import is enabled.

Active directory groups and OUs containing the appropriate users therefore need to be used to represent the tenants and user roles within NSS.

If current active directory groups are not sufficient to map users into NSS tenants and roles, an example set of AD groups created for two tenants and the NSS admins might look like:

..\NetBackupSelfService\Administrators
..\NetBackupSelfService\Tenants\Development
..\NetBackupSelfService\Tenants\Development \Admins
..\NetBackupSelfService\Tenants\Finance\
..\NetBackupSelfService\Tenants\Finance\Admins

If importing users from multiple domains, then these groups may need to be created within each domain as import rules are per domain.

The relevant users should then be placed in each group. Users can not be members of more than one tenant

2.4 Configure Import Rules in NSS

Rules must be configured to import users into NSS. One rule will be required for each domain / user type / tenant.

Rules are processed in order, and the user will inherit the permission of the last rule executed only.

To configure the rules that will import users, log on to NSS as ADMIN and access

Admin -> Organization -> (hover over) User -> Select Import Active Directory

You will be presented with the "Scheduled task details – Import active directory" screen.

Click "New" to create a new import rule

Configure the rule as follows

2.4.1 Details tab - Active Directory Credentials

Name

Description of the users the rule imports (i.e. Development tenant admins)

Domain Name

The domain name of the users being imported with this rule (i.e. BIOMNI-US)

Email Domain

The email domain of the user - what goes after the @ sign in that user's email address e.g. biomni.com

User Name / Password

The user name of the account being used to read from Active Directory to perform the import. This user requires the List Contents and Read All Properties rights at the root level of the domain specified . This will allow NSS to search all organizational units/groups and import all users.

2.4.2 Details tab - Imported User Fields

Users must be given defaults for the information held within NSS but not contained within AD. These include

Access Profile

The access profile represents the access rights given to all AD imported users. For tenant users you must use "Client Administrator" or "Client User". For the NSS administrator, select "Supervisor"

Cost Center

Cost Center corresponds with the tenant the users in this import will be included in.

Select "General – GEN" for the NSS administrator rule to prevent those users being added to a tenant.

Language

Set this to the preferred language of the users in this import.

Status

Set this to "active" to immediately active the user account on import.

Groups

Do not link to any groups. NSS will link the user to the default tenant group automatically.

2.4.3 Filter tab

Add button

Click Add to launch a pop up allowing you search for and specify from what OUs / groups this rule will import users.

Click OK to save the rule.

Add any additional rules required.

Ensure that rules importing supervisor and users with elevated user rights are then executed after importing standard users. The NSS admin users should have their own OU. This rule must be the last in the list. The order of rules can be changed by dragging and dropping the rule.

2.4.4 Enabling the import

On the main Import active directory screen, Click the enable checkbox and specify the time of day the import can be run (usually outside of business hours)

You can click the Run Now button for an immediate import.

After the import has been given sufficient time to run you can view a summary of how many users have been imported and any import errors via the "View Log" button

2.4.5 Notes

The 'Import Active Directory' update schedule is a full 'import and replace' process so all active NSS users must always be present, otherwise their account will be deactivated.

The import task does not import users' passwords. If SSO with Windows Authentication (explained in the following chapter) is not going to be used, users will have to set their passwords via the "forgot my password" link on the home page. In this case passwords will be maintained separately from the user's AD password.

Users with only the Pre-Windows 2000 user logon name against their AD record, not the new user log on name, will NOT be imported.

3.0 Single Sign on via Windows Authentication

NSS can be configured to automatically sign users in by using Windows authentication configured on the web server.

This requires the user to be accessing NSS while authenticated to the Active Directory. It will not work for NSS hosted on the internet.

IMPORTANT: Before enabling, ensure that you have set your user ID (or at least one ID) to the "Supervisor" access profile.
Missing this step will result you will lose access to the admin area (as there is no manual log on option therefore the ADMIN user account cannot be accessed).
If your users are populated by the 'Import active Directory' option as described above, ensure at least one rule is configured to create NSS administrators, and your user account is included within this OU/Group.

3.1.1 Configure IIS Authentication

Access the web server Enable Windows security in IIS Admin as follows

Navigate to the NSS website virtual directory in the web site explorer and click the site to select.

Select the Authentication option, enable the features as follows

- Enable Windows Authentication
- Disable Anonymous Authentication
- Disable Forms Authentication

Repeat for the NetBackupSelfServiceNetBackupPanels virtual directory

The NetBackupSelfServicePublicWebService and NetBackupSelfServiceNetBackupServices security settings should not be changed.

The IIS web server must be on the domain or in a trust relationship with the domain the user is to be authenticated against.

3.1.2 Test access

Completely close your web browser if it has been used to access NSS previously to making this configuration.

Access NSS via Internet Explorer. Providing you are logged in to your domain and a user account exists within NSS that matches your Windows ID, you will be logged on automatically.

If the user is prompted for their Windows credentials, or has any other access issues, ensure that the NSS website is added to their "Intranet sites" in Internet security settings