

How-to: LDAP Security

Document version: 1.00

This document describes how to configure roles and permissions when NDAS (the Nirva Directory Access Service) is used to authenticate users with an LDAP server.

NDAS provides an alternative to Nirva's default user authentication. When NDAS is used, the normal Nirva application roles are unavailable. Instead, NDAS provides its own mechanism for assigning permissions to a user session.

Overview

When an application is configured with its "Application for security" set to "(NDAS)", Nirva sends all its requests for userid/password validation to NDAS. NDAS processes such a request by querying an LDAP server.

If the LDAP server indicates that the userid/password combination is valid, NDAS can assign permissions to the user session. NDAS provides a number of different methods of configuring roles and permissions. Before beginning configuration, the administrator must decide which method will be used.

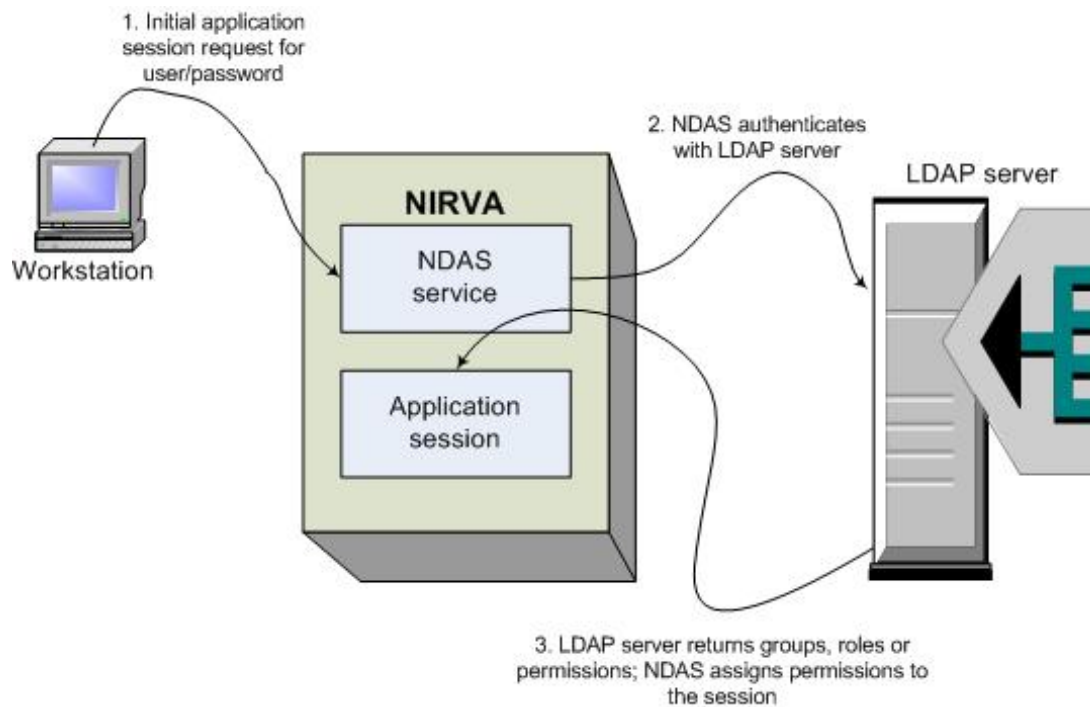


Figure 1 NDAS security overview

This document focuses on NDAS roles and permissions. It does not cover other aspects of NDAS configuration. It assumes that NDAS has been configured with at least one LDAP server.

The following points should be noted:

- The goal is to assign permissions to an authenticated user session. A role is simply a collection of permissions. Using roles makes it easier to manage permissions.
- Each LDAP server can be configured with a different method of assigning permissions to users.

- A server can be specified as the security server for more than one application. Roles and permissions must be configured in NDAS for each application for which NDAS has been specified.
- Some understanding of LDAP servers is required, in particular the naming of LDAP objects using Common Names (CN), Organisational Units (OU) and Domain Components (DC)¹.

Deciding on the permissions method

Before starting to configure NDAS roles and permissions, decide on the method that you will use. Each LDAP server configured within NDAS can have its own method. Section [Available permissions methods](#) below describes the methods available. Each method has its own section in this document where the rationale and method for implementing it is described.

In each case, the method is specified on the NDAS server [Permissions processing](#) tab. To reach this, begin with the NDAS service configuration page. This lists the configured servers.

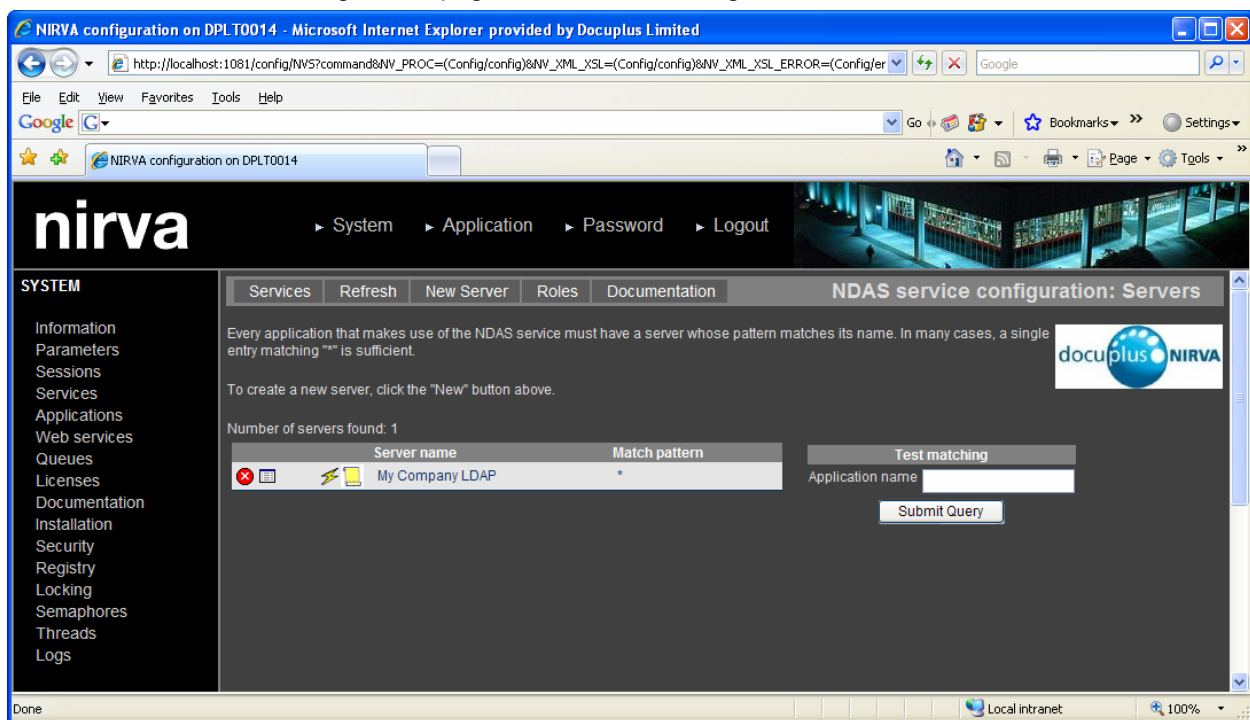


Figure 2 NDAS list of LDAP servers

Click the configuration icon for the server being configured. This displays a page with multiple tabs. Each tab displays a set of values configured for the selected server. Click on the [Permissions processing](#) tab to proceed.

¹ There are various products available for free download that will display the contents and structure of an LDAP server, e.g. Softerra LDAP Browser 2.6 available from <http://www.ldapbrowser.com/download.htm>. These may be useful in providing the information required to configure NDAS.

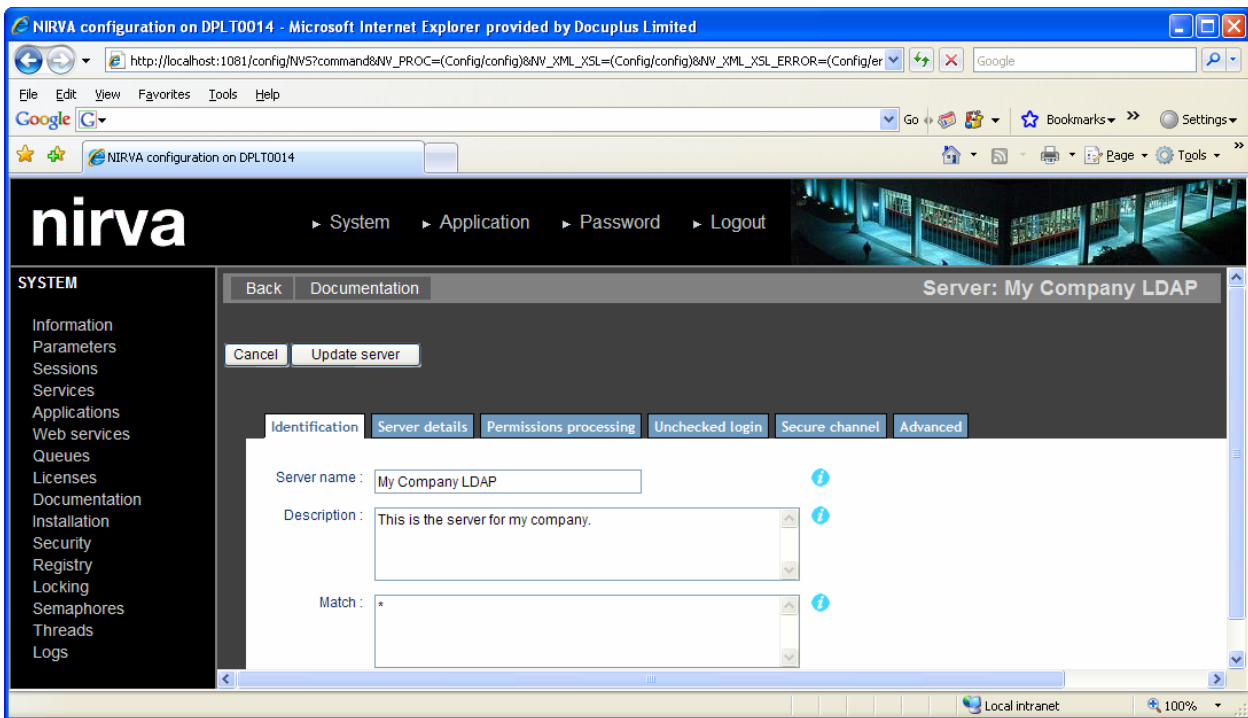


Figure 3 NDAS: LDAP configured servers

Available permissions methods

Following is a list of the methods that NDAS makes available for assigning permissions to an authenticated user session:

1. NDAS will never assign any permissions to any user session. See the section entitled [NDAS assigns no permissions](#).
2. The LDAP server assigns each user to a named group. NDAS maps each server group to an NDAS role. See the section entitled [Group supplied by the server](#).
3. The LDAP server provides the names of the NDAS roles. See the section entitled [NDAS role names supplied by the server](#).
4. The LDAP server provides the names of the Nirva permissions. See the section entitled [Nirva permissions supplied by the server](#).

Method 1: NDAS assigns no permissions

Rationale

NDAS can be configured to assign no permissions to a user session. It will still check that the user has supplied a valid userid/password combination but the session will begin with no permissions at all.

On the face of it, this may not appear very useful; once a user has logged on, their session will have no permissions assigned. However, there may be situations in which an application has been written to assign its own permissions each time a session begins. But remember that NDAS can handle the security for multiple applications and other applications might require NDAS to assign permissions. In this case, this would not be the correct choice.

When NDAS assigns no permissions, NDAS roles are not used.

How to configure

Ensure that the server's **Permissions processing** tab is displayed.

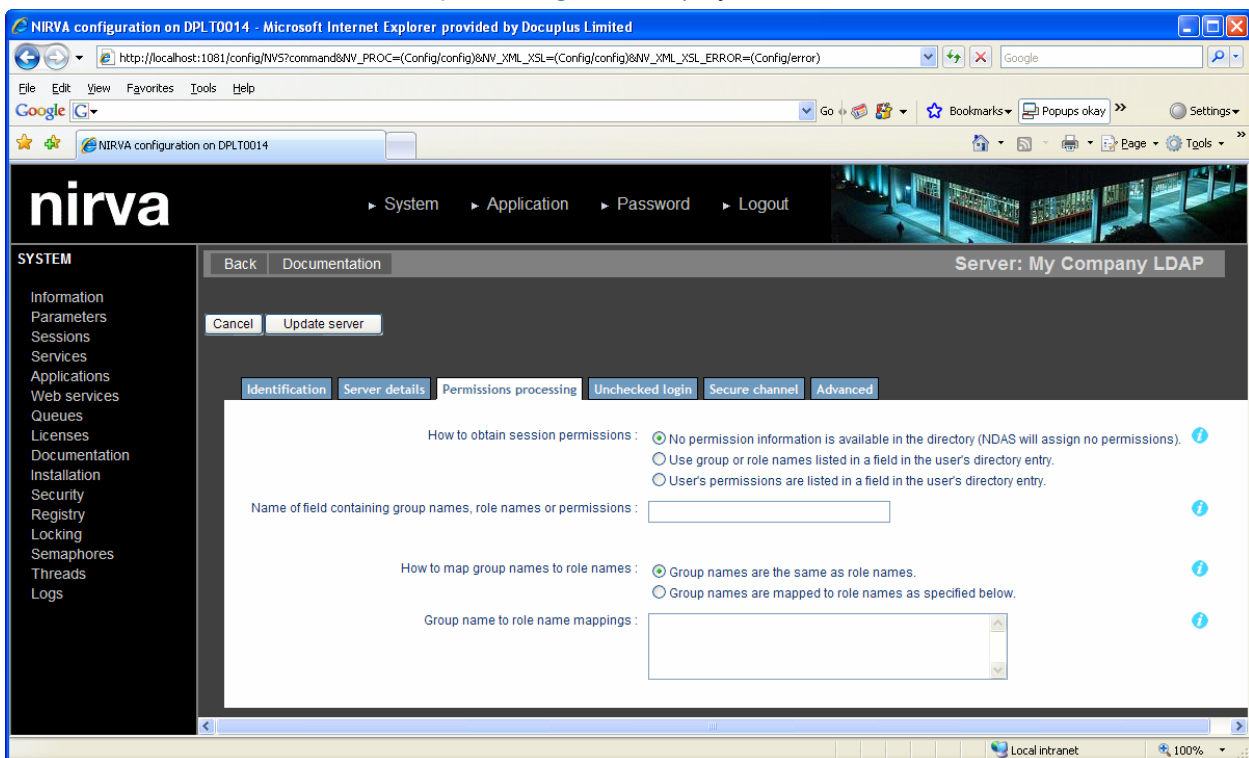


Figure 4 NDAS Permissions processing tab: No permissions processing

For How to obtain session permissions select No permission information is available in the directory (NDAS will assign no permissions). Click the Update server button to save any changes. In this case, NDAS will ignore all other values on this tab.

Method 2: Group names supplied by the server

Rationale

Each user's entry in an LDAP server contains a number of fields. One of the fields can be specified as containing the names of a number of groups to which the user belongs (it is a multi-valued field). The user is assigned to these groups by means of the LDAP server's administration functions.

When NDAS has authenticated a user, it reads the set of group names assigned to the user and maps each to the name of an NDAS role. NDAS assigns all the permissions specified by all the specified roles to the session.

This is a good choice when the Nirva application(s) are stable. When a new user joins the organisation, they can be added to the LDAP server and assigned to one or more groups. They are then automatically authorised to use the functionality of the Nirva application(s) that they require.

It is also a good choice because it requires no structural change (such as addition of a new field) to the LDAP server.

For this to work, a number of NDAS roles will be required. See section [NDAS Roles](#) for information on configuring NDAS roles.

How to configure

Ensure that the server's [Permissions processing](#) tab is displayed.

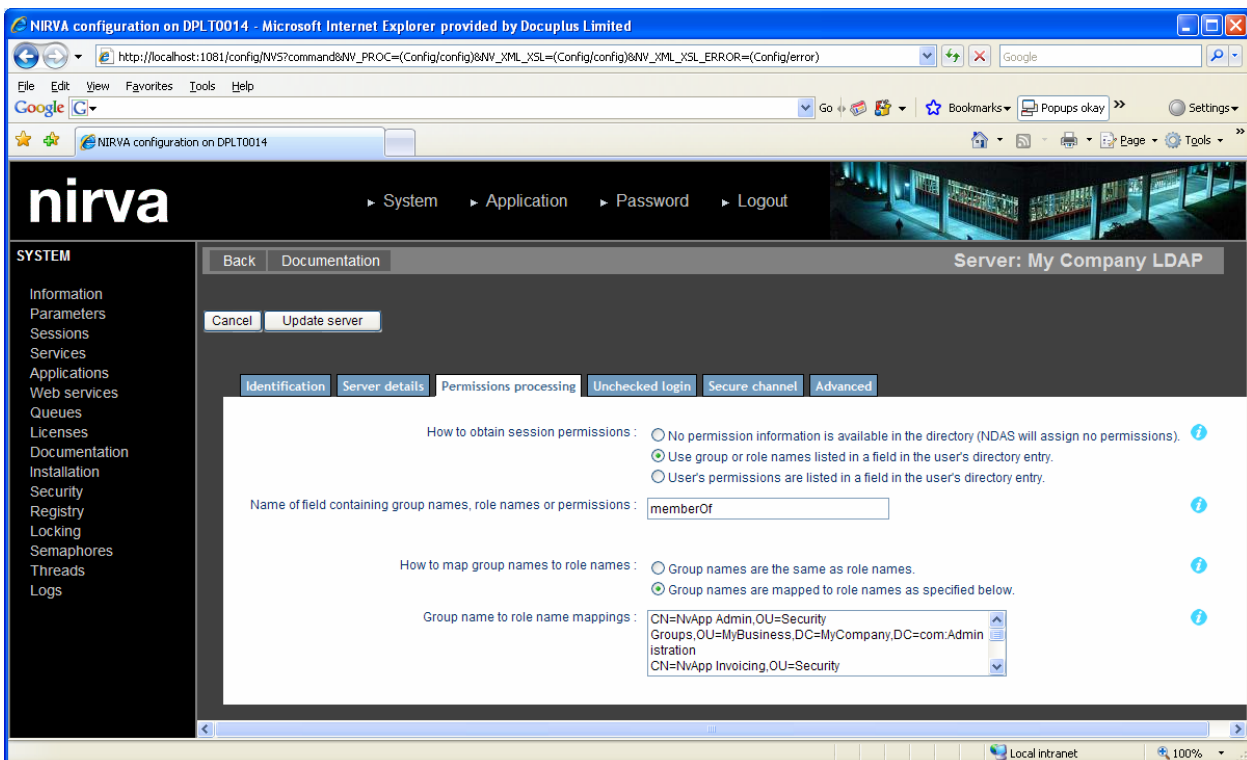


Figure 5 NDAS Permissions processing tab: group names supplied by the server

Choose the following options:

- For **How to obtain session permissions** select **Use group or role names listed in a field in the user's directory entry**.
- For **Name of field containing group names, role names or permissions** enter the name of the field in the user record where the LDAP server stores the user's group names. For a Microsoft Active Directory server, this name is "memberOf".
- For **How to map group names to role names** select **Group names are mapped to role names as specified below**.

- For [Group name to role name mappings](#) specify one or more lines of text. Each line must contain a server group name followed by a colon followed by the name of an NDAS role. For example:

```
CN=NvApp Admin,OU=Security Groups,OU=MyBusiness,DC=MyCompany,DC=com:Administration  
CN=NvApp Invoicing,OU=Security Groups,OU=MyBusiness,DC=MyCompany,DC=com:Invoicing  
CN=NvApp Reporting,OU=Security Groups,OU=MyBusiness,DC=MyCompany,DC=com:Reporting
```

In the example above:

- User1 might be assigned to the groups `NvApp Invoicing` and `NvApp Reporting` on the LDAP server. When NDAS authenticates User1, the Nirva session will be assigned all the permissions specified by NDAS roles `Invoicing` and `Reporting`.
- User2 might be assigned to the groups `NvApp Admin` on the LDAP server. When NDAS authenticates User1, the Nirva session will be assigned all the permissions specified by NDAS roles `Administration`.

Method 3: NDAS role names supplied by the server

Rationale

Each user's entry in an LDAP server contains a number of fields. One of the fields can be specified as containing the names of a number of NDAS roles (it is a multi-valued field). The values (role names) in this field must be specified by means of the LDAP server's administration functions.

When NDAS has authenticated a user, it reads the set of NDAS role names assigned to the user and assigns all the permissions specified by those roles to the session.

This method will rarely be used because it would probably require some specific modifications to the LDAP server to add the field before it can be used. Its advantage is that it transfers some of the user administration tasks from Nirva to the LDAP server where users are normally added and removed. However, before using this method, you should be certain that using server groups is not a satisfactory option (see section [Group names supplied by the server](#)).

For this to work, a number of NDAS roles will be required. See section [NDAS Roles](#) for information on configuring NDAS roles.

How to configure

Ensure that the server's **Permissions processing** tab is displayed.

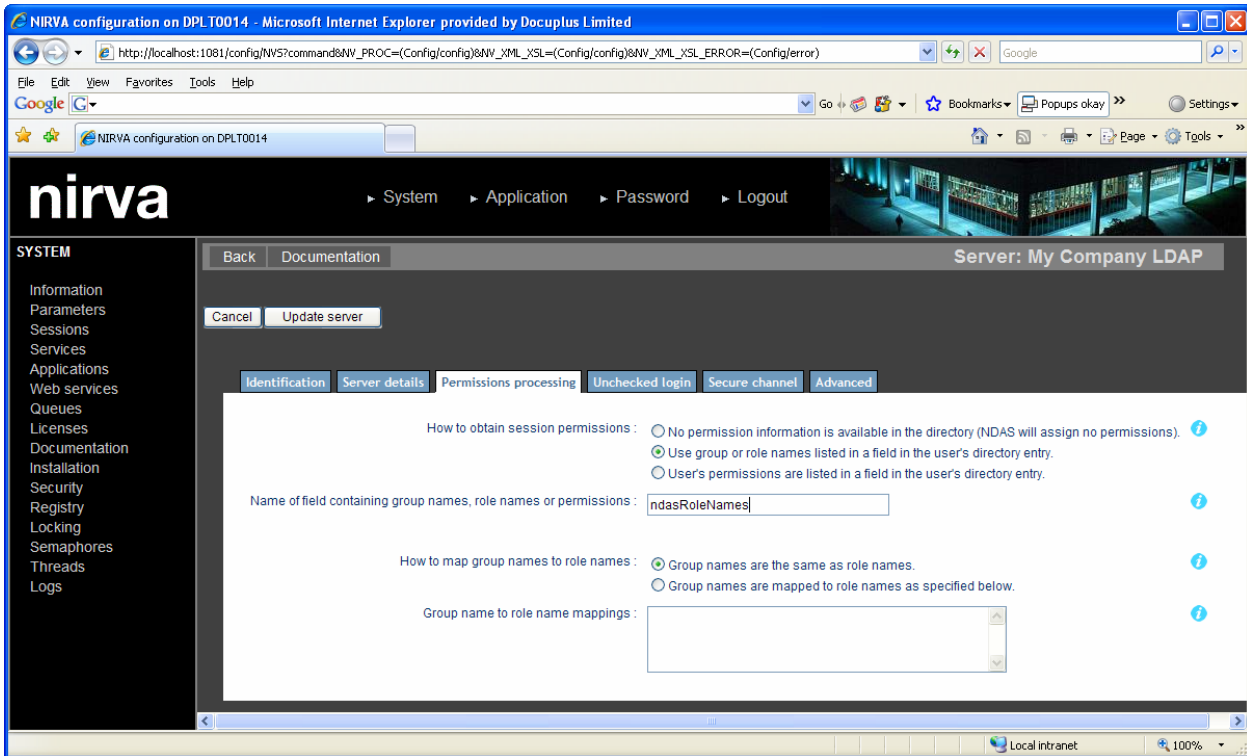


Figure 6 NDAS Permissions processing tab: role names supplied by the server

Choose the following options:

- For How to obtain session permissions select Use group or role names listed in a field in the user's directory entry.
- For Name of field containing group names, role names or permissions enter the name of the field in the user record where the LDAP server stores the user's NDAS role names. The screen shot above shows the name `ndasRoleNames` but this will be different in each case and depends upon how the LDAP server is configured.
- For How to map group names to role names select Group names are the same as role names.
- Leave the field Group name to role name mappings empty (NDAS ignores any value entered here).

Method 4: Nirva permissions supplied by the server

Rationale

Each user's entry in an LDAP server contains a number of fields. One of the fields can be specified as containing the names of a number of Nirva permissions (it is a multi-valued field). The values (permissions) in this field must be specified by means of the LDAP server's administration functions.

When NDAS has authenticated a user, it reads the set of Nirva permissions assigned to the user and assigns each to the session.

This method will rarely be used because it would probably require some specific modifications to the LDAP server to add the field before it can be used. It will also require a lot of administration because there is no mechanism for keeping the user's permissions in line with those available on the Nirva server.

When NDAS obtains the permissions from the LDAP server, NDAS roles are not used.

Permission formats

Each value in the LDAP server's permissions field specifies a single permission (one field can contain multiple values). The format of a permission is one of the following:

- For an application permission, `app::permission` where `app` is the name of the Nirva application and `permission` is the name of the permission (note: the two colons separating `app` and `permission`).
- For a service permission, `:serv:permission` where `serv` is the name of the Nirva service and `permission` is the name of the permission (note: one colon precedes `serv` and one colon separates `serv` and `permission`).
- For a Nirva system permission, `::permission` (note: two colons precede `permission`).
- For a web service permission, `:(webserv):permission` where `webserv` is the name of the Nirva web service and `permission` is the name of the permission (note: (i) one colon precedes `webserv` and one colon separates `webserv` and `permission`; (ii) `webserv` is enclosed in parentheses).

How to configure

Ensure that the server's **Permissions processing** tab is displayed.

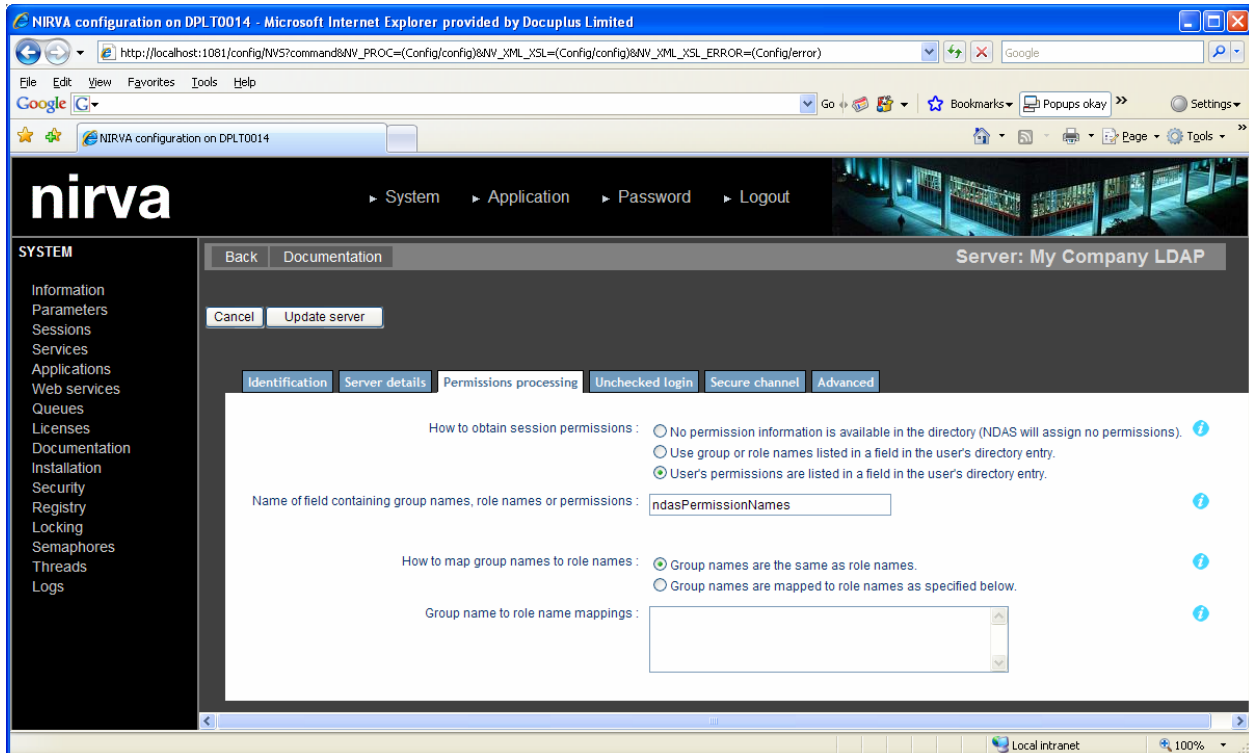


Figure 7 NDAS Permissions processing tab: permissions supplied by the server

Choose the following options:

- For **How to obtain session permissions** select **User's permissions are listed in a field in the user's directory entry**.
- For **Name of field containing group names, role names or permissions** enter the name of the field in the user record where the LDAP server stores the user's permissions. The screen shot above shows the name `ndasPermissionNames` but this will be different in each case and depends upon how the LDAP server is configured.
- NDAS ignores the value selected for **How to map group names to role names**.
- NDAS ignores anything in the field **Group name to role name mappings**.

NDAS Roles

Multiple Nirva applications can have NDAS specified for their security. A single NDAS role can specify the permissions for multiple applications.

Each NDAS role consists of a name to identify it, a description and a set of permissions.

To configure an NDAS role, begin by opening the NDAS configuration page.

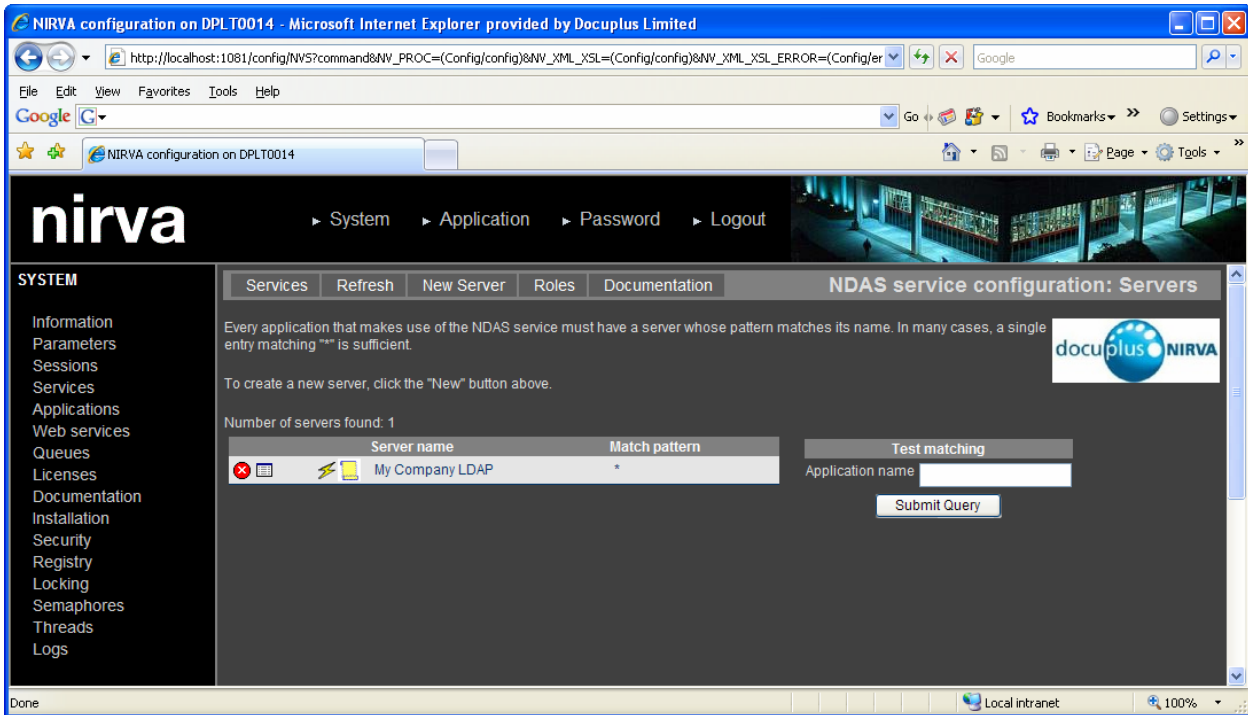


Figure 8 NDAS list of LDAP servers

Then click the Roles button at the top of the page. NDAS displays a list of roles already configured.

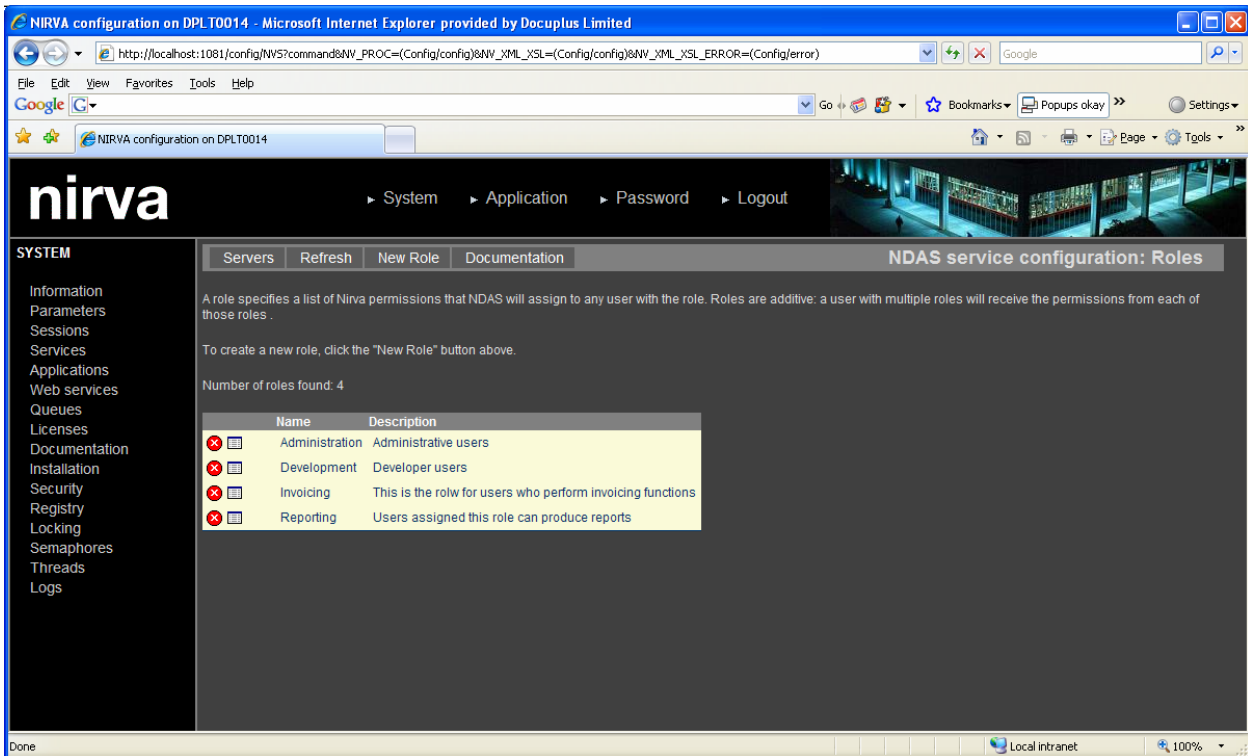




Figure 9 NDAS list of roles

Clicking  next to a role will remove it.

To update a role, click  next to its name in the list. To add a new role, click the **New Role** button at the top of the page.

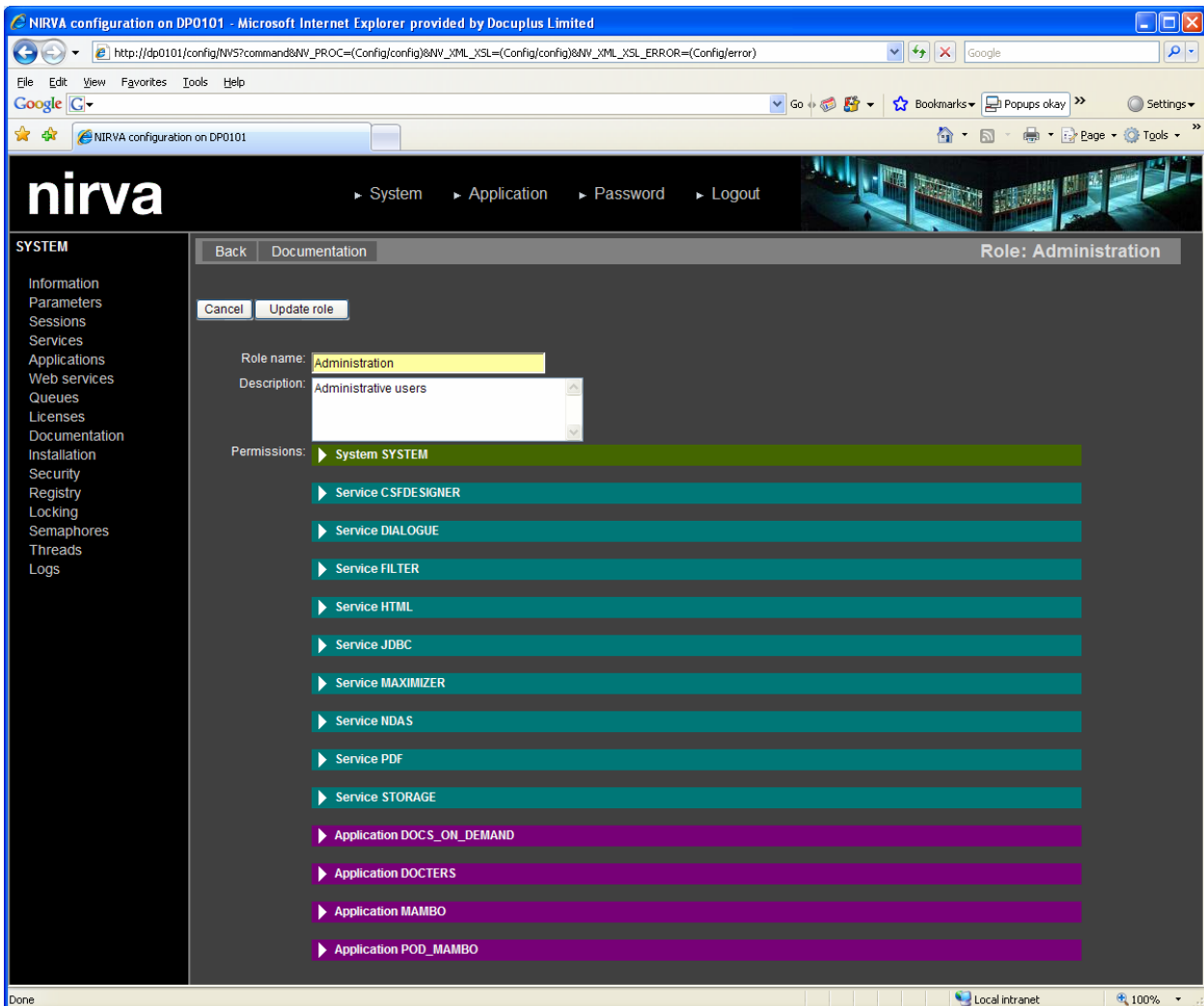


Figure 10 NDAS role configuration page

The role's configuration page shows:

- its name
- its description
- a section for the Nirva system
- a section for each service
- a section for each application
- a section for each web service (none shown in the example above)

If this is a new role, you must supply its name and, optionally, its description. For an existing role, you can change its name or description if necessary.

Click on the triangle at the start of each row to show the permissions for that section.

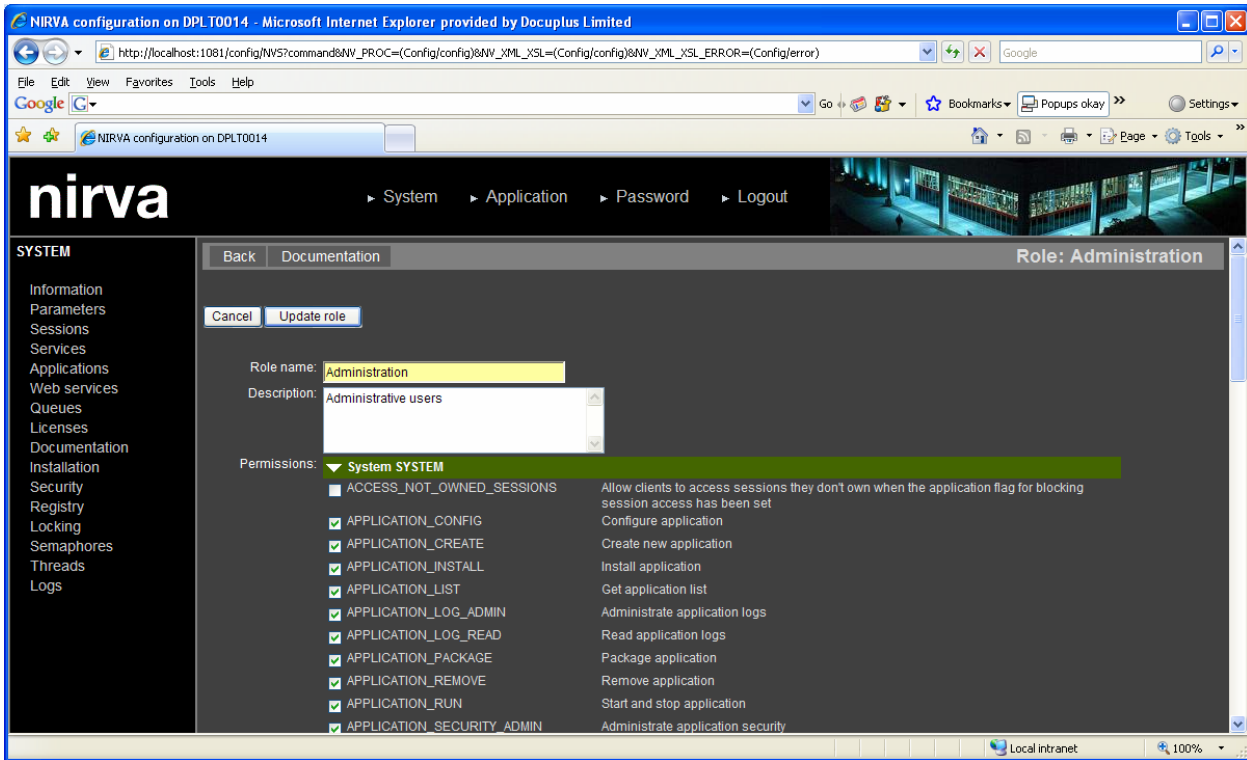


Figure 11 NDAS role configuration page with permissions

Tick a checkbox to add the permission to the role or clear the tick to remove the permission from the role. When all the permissions have been set, click Update role to save the changes.

When you have set the permissions correctly, click the Update role button (or Add role for a new role).

Active Directory Administration

This section provides an overview of administering Active Directory in readiness for use with NDAS.

The example assumes that [Method 2: Group names supplied by the server](#) has been chosen in the NDAS configuration. This means that all that needs to be done in the Active Directory administration is to ensure that the correct users exist and are members of the correct groups. It may also be necessary to create the groups.

Depending upon the version of Windows Server, the administration tools you have available may vary from what is shown here. On a given version of Windows Server, you may have more than one tool available in which case your choice of tool is down to personal preference. The examples shown here use the Server Management tool provided with Microsoft Windows Server 2003 for Small Business Server Service Pack 2.

Figure 12 shows the Server Management tool as it initially starts up.

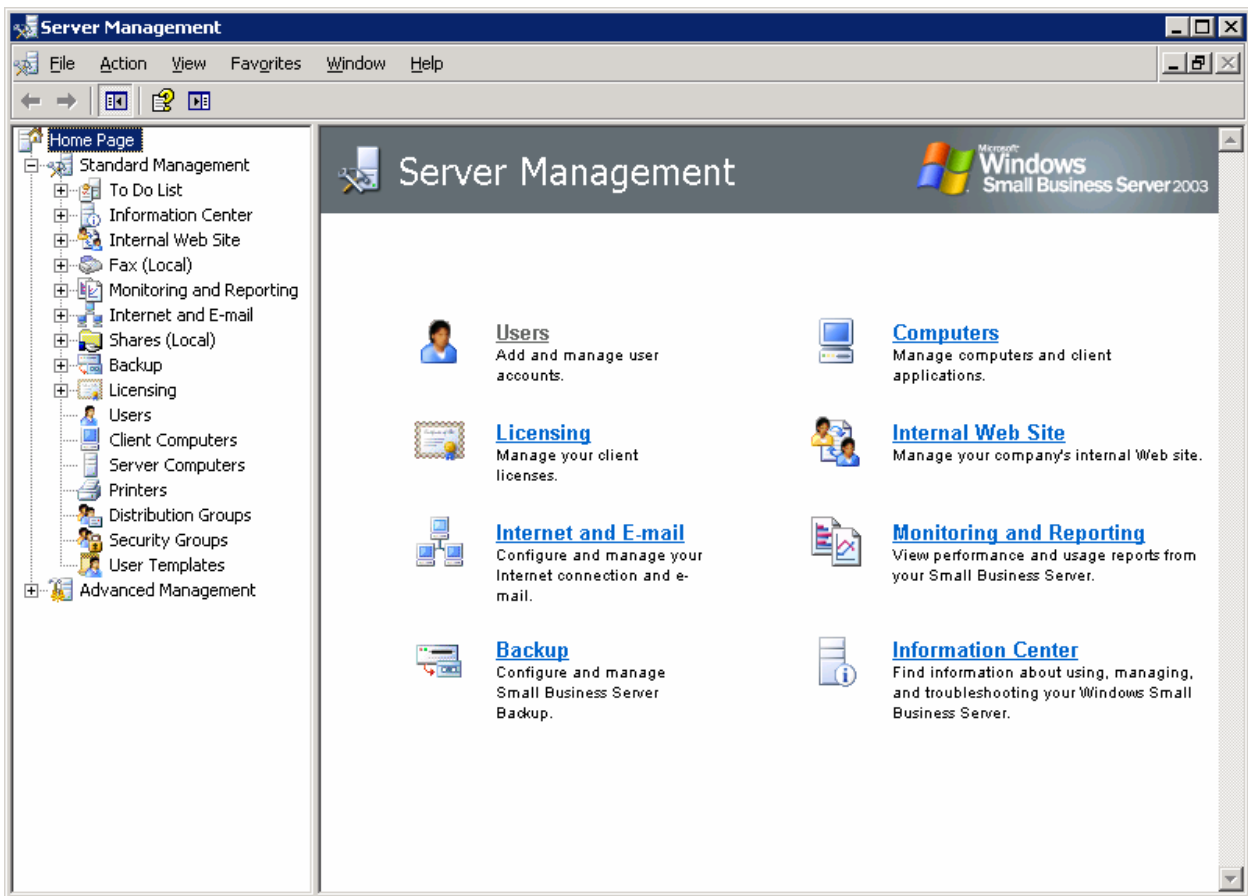


Figure 12 Windows Server Management tool - initial startup

Active Directory: Add a Security Group

In the tree in the left hand pane, click on Security Groups (see Figure 13).

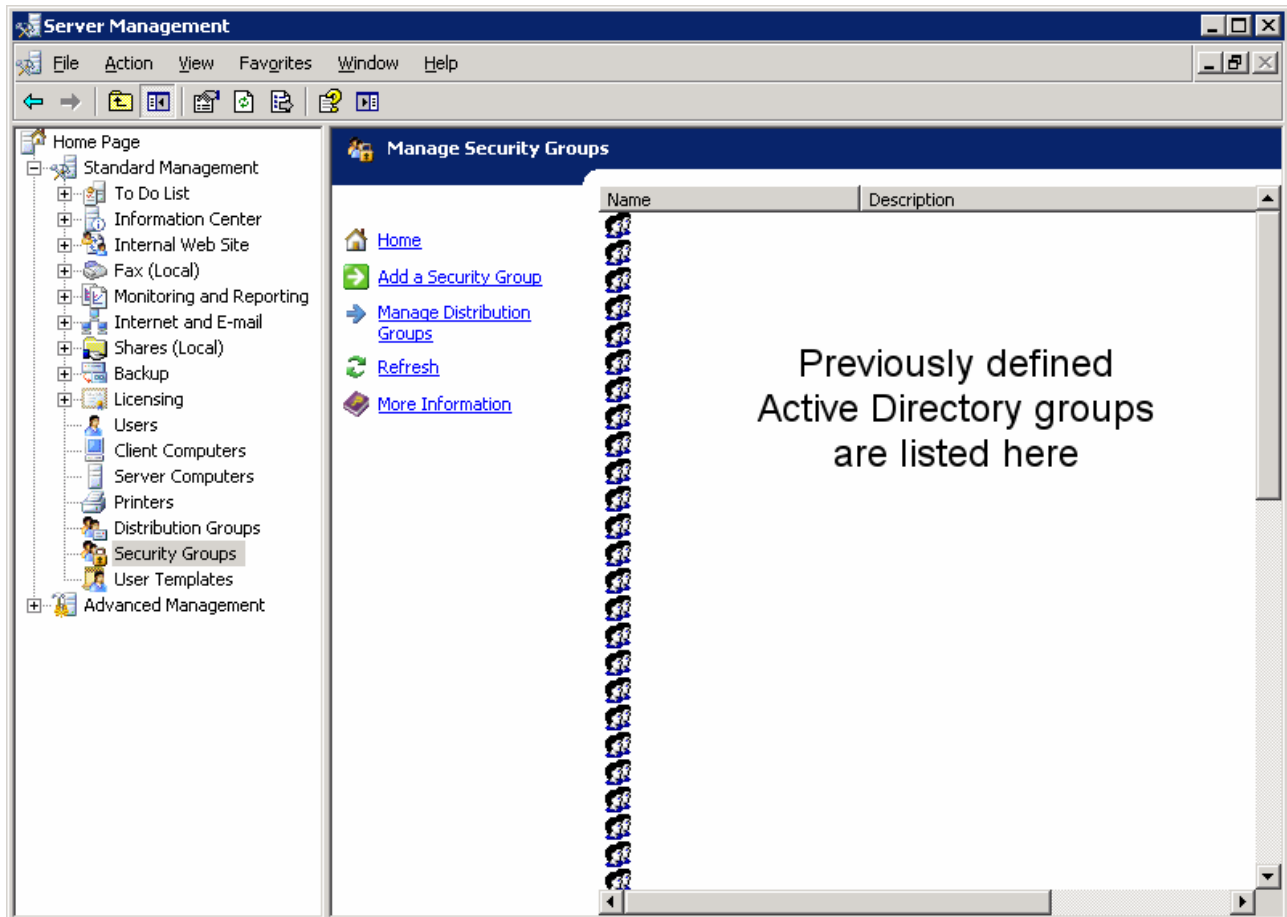


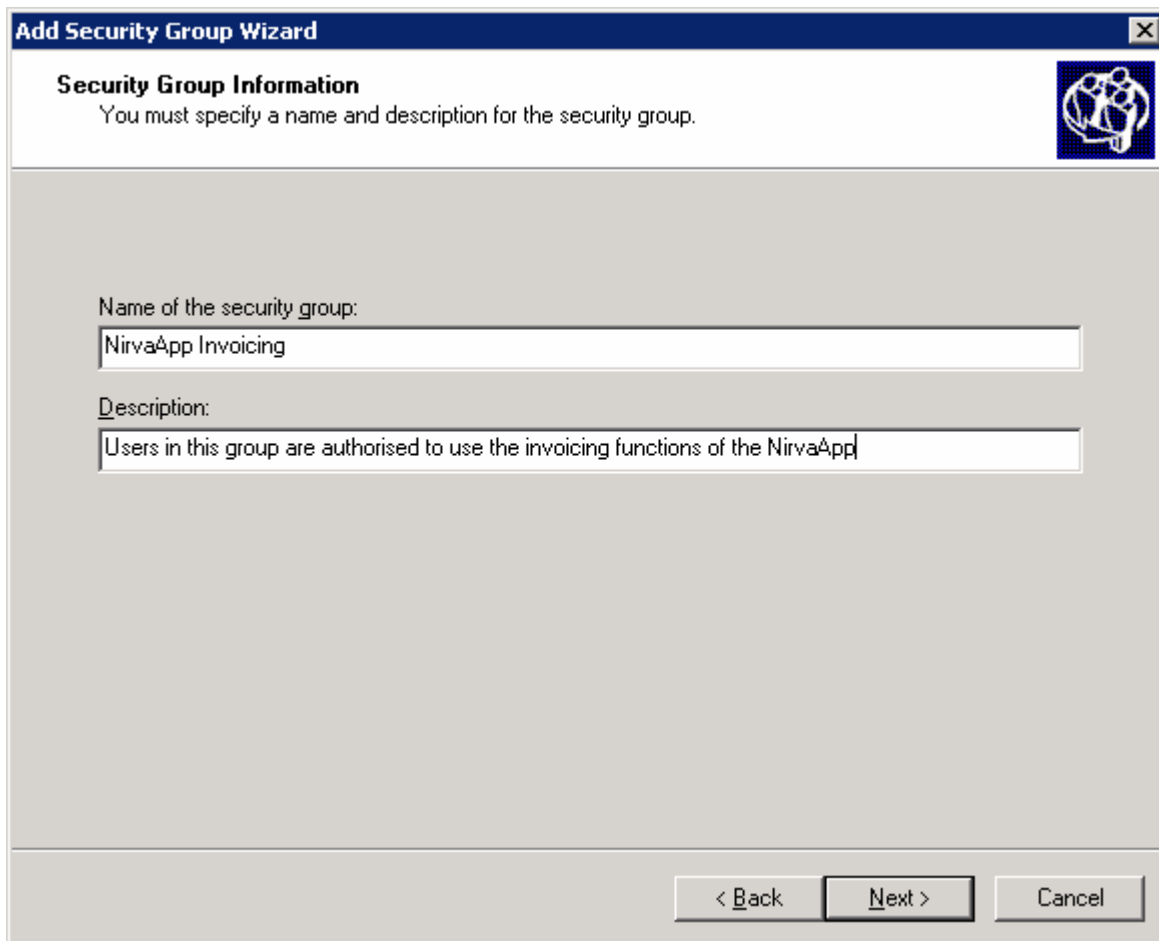
Figure 13 Windows Server Management tool – Manage Security Groups

Click on Add a Security Group to begin the Security Group wizard. See Figure 14.



Figure 14 Add Security Group Wizard – first page

Click Next. You will be presented with a form where you can enter the name of the group (mandatory) and its description (optional). See Figure 15.



Add Security Group Wizard

Security Group Information
You must specify a name and description for the security group.

Name of the security group:
NirvaApp Invoicing

Description:
Users in this group are authorised to use the invoicing functions of the NirvaApp

< Back Next > Cancel

Figure 15 Security Group Information

Having filled in the Security Group Information form, click Next. The Group Membership page is displayed (see Figure 16). On the left is a list of previously defined Active Directory users and groups. Select those users and groups that will have membership of the new group and click the Add button (a group can be a member of another group – in this case the added group’s members will become members of the new group). Then click Next. If you have not yet created the required users, you can click Next without adding any users or groups to create an empty group.

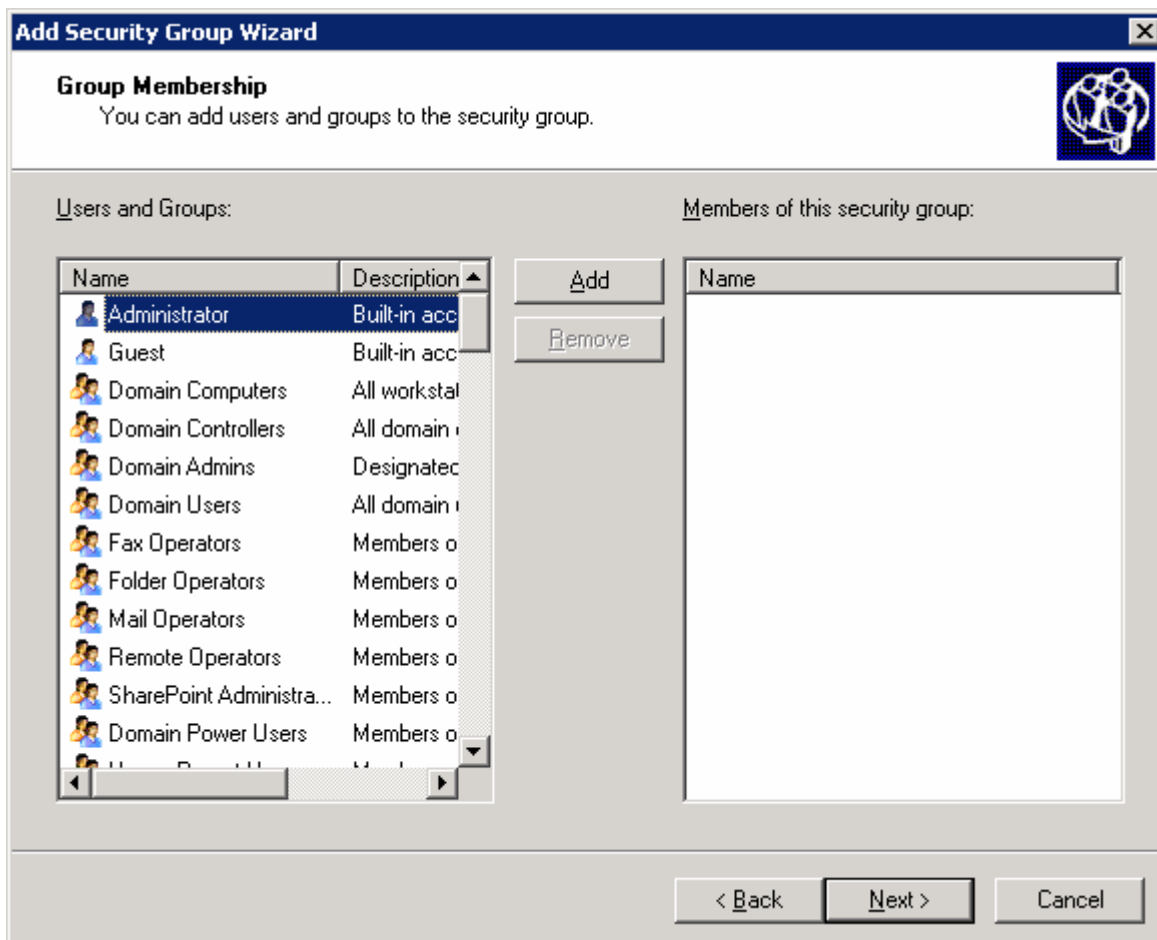


Figure 16 Group Membership

When you click Next, the final page of the wizard is displayed. See Figure 17.



Figure 17 Add Security Group Wizard – last page

Click Finish on the last page of the wizard to save the new security group.

Active Directory: Add a User to a Group

Click on Users in the main window pane.

This section assumes that you do not need to add a new user; the user who will use the Nirva Application already exists in the Active Directory database. If this is not the case, click on the Add a User or the Add Multiple User link. A wizard will start and guide you through the process of creating a new user.

To add a current user to an existing security group (if the group does not exist, create it first as described in the earlier in [Active Directory: Add a Security Group](#)).

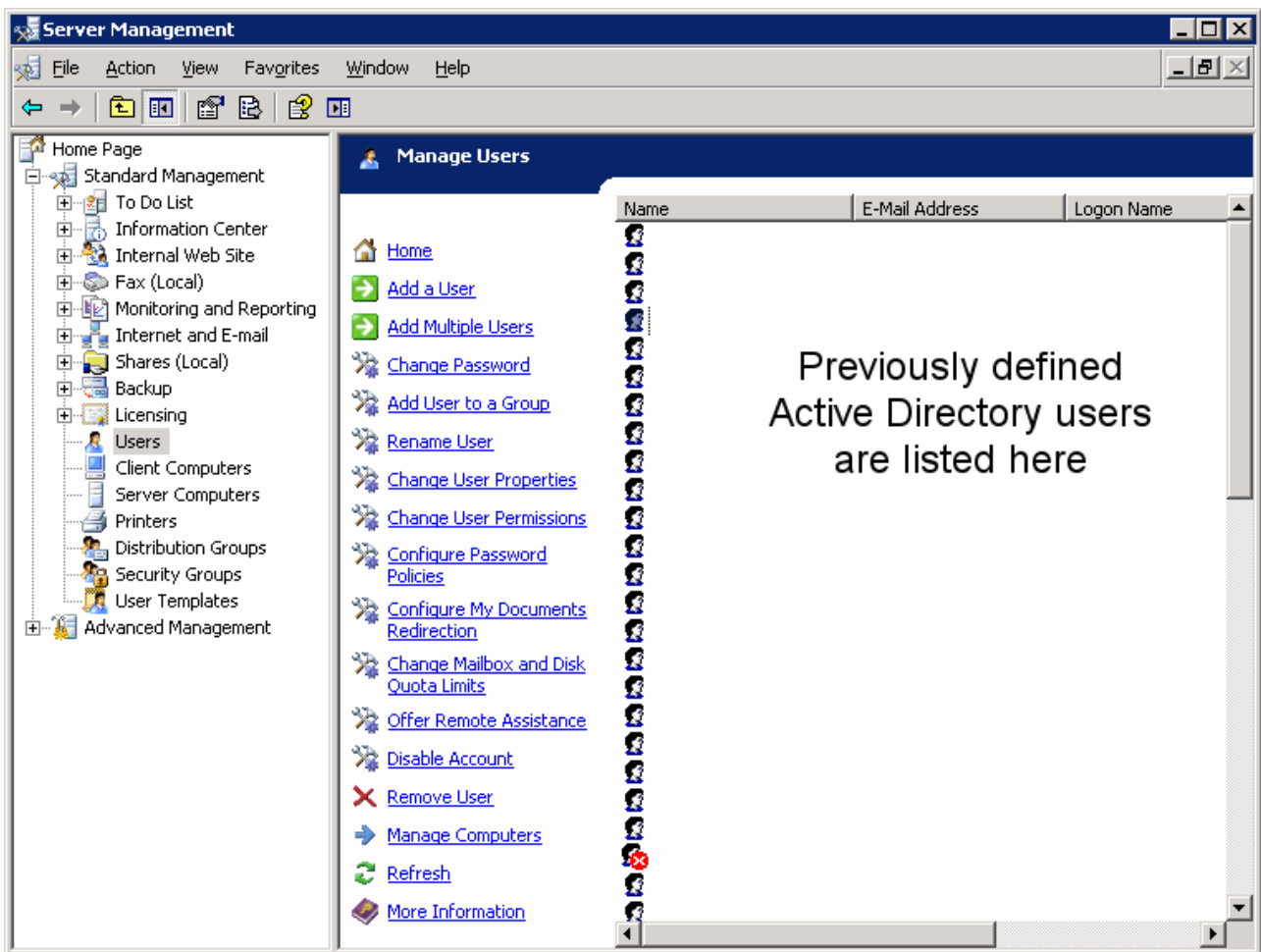


Figure 18 Active Directory Manage Users page

If the Nirva user does not already exist, click on Add a User. This opens a wizard that takes you step by step through the process of creating a user. In this document, it is assumed that the required user already exists. In this case, double click the name of the user to be added to Nirva. A window similar to that shown in Figure 19 will open.

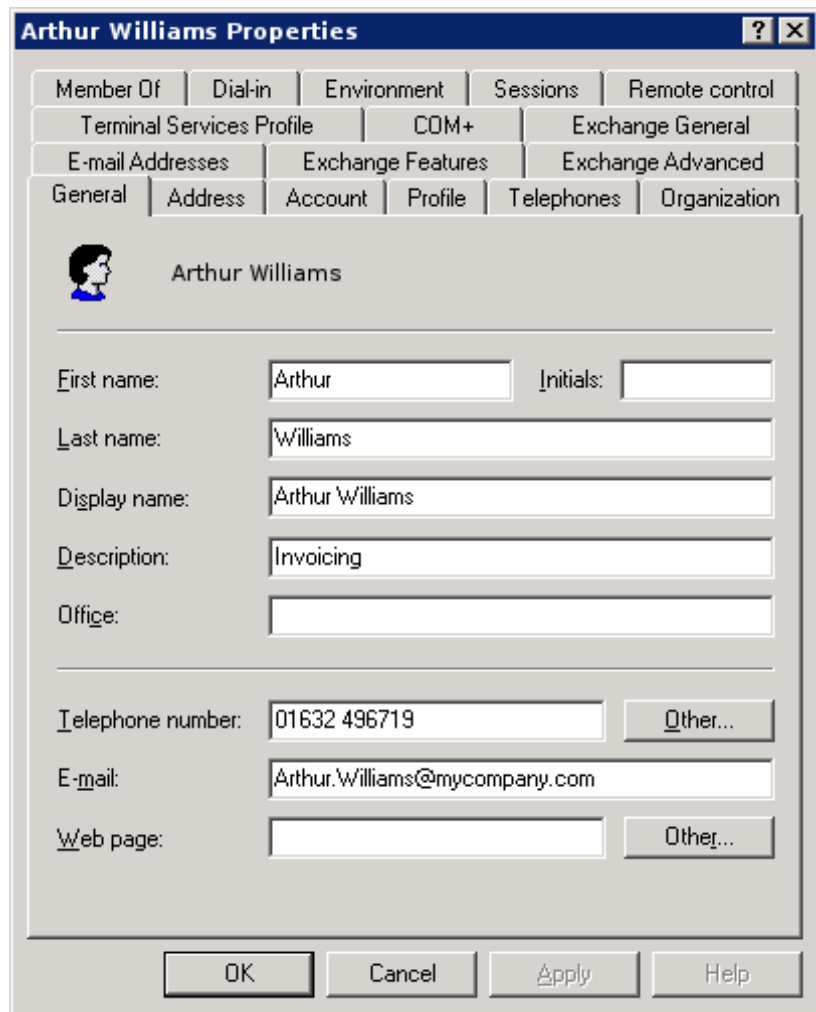


Figure 19 Active Directory User Properties

Click on the Member Of tab. Any groups of which the user is already a member are displayed. See Figure 20.

Click the Add... button. The Select Groups dialog box is displayed. See Figure 21. Type the name of the Active Directory security group. Then click the Check Names button. If the group name is valid, Active Directory will underline it. If you are not sure of the name, you can click the Advanced button to perform a search.

Once you have entered a valid group name, click OK to return to the User Properties box. Then click OK to save and close.

The group will now be returned to NDAS when the user logs on.

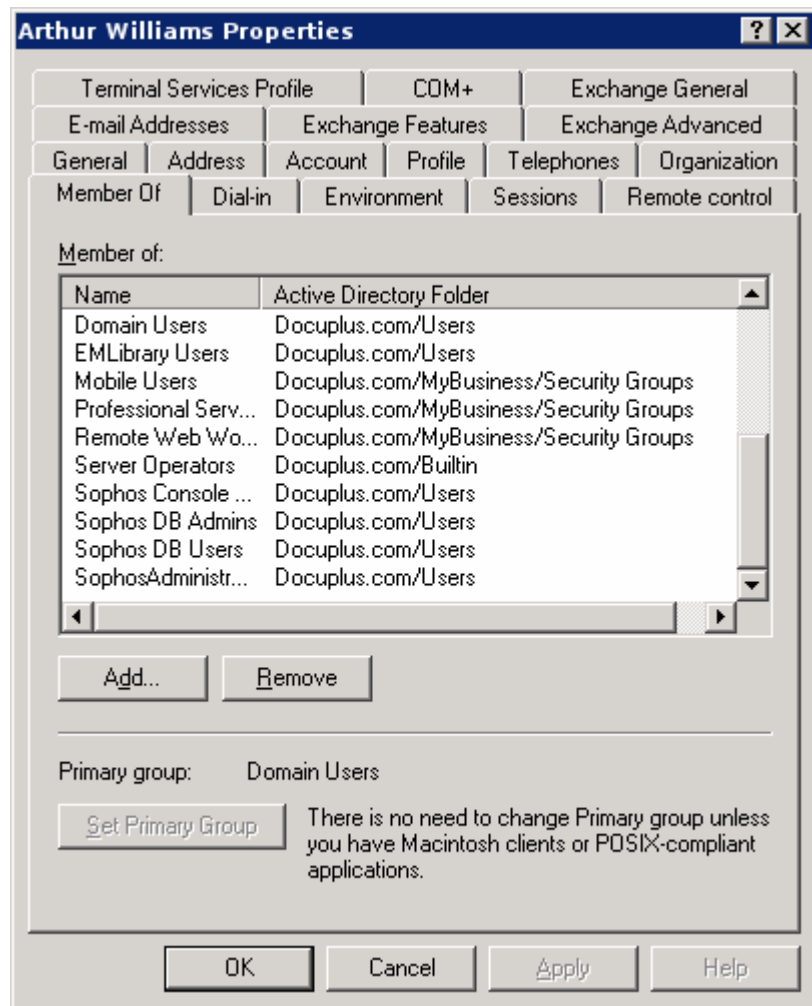


Figure 20 Active Directory User Group Membership

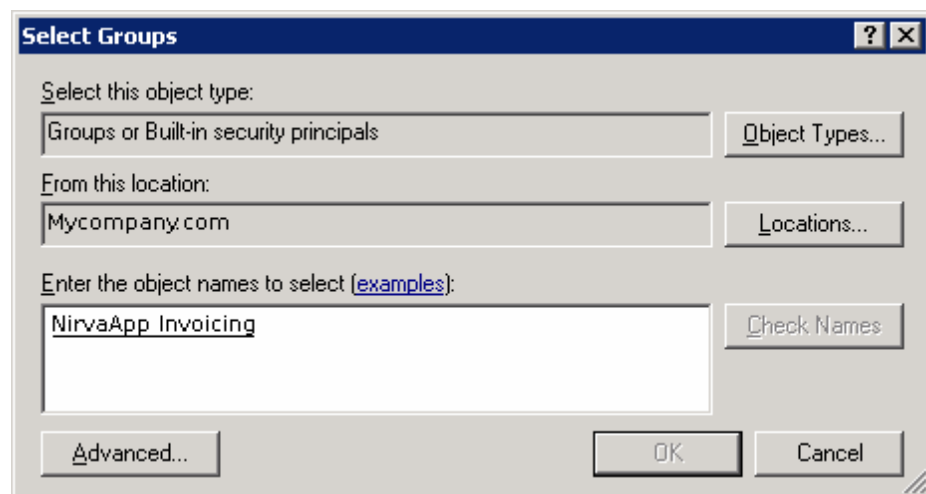


Figure 21 Active Directory Select Groups