ESKER Tun® Plus

Web Administrator Guide

ESKER®

Document Process Automation

Tun Plus 2009
Issued May 2008

Esker S.A., 10 rue des Émeraudes, 69006 Lyon, France
Tel: +33 (0)4.72.83.46.46 ♦ Fax: +33 (0)4.72.83.46.40 ♦ info@esker.fr ♦ www.esker.fr

Esker, Inc., 1212 Deming Way, Suite 350, Madison, WI 53717 USA
Tel: +1.608.828.6000 ♦ Fax: +1.608.828.6001 ♦ info@esker.com ♦ www.esker.com

Esker Australia Pty Ltd. (Lane Cove - NSW) ♦ Tel: +61 (0)2 8596 5100 ♦ info@esker.com.au ♦ www.esker.com.au
Esker GmbH (München) ♦ Tel: +49 (0) 89 700 887 0 ♦ info@esker.de ♦ www.esker.de
Esker Italia SRL (Milano) ♦ Tel: +39 02 57 77 39 1 ♦ info@esker.it ♦ www.esker.it
Esker Ibérica, S.L. (Madrid) ♦ Tel: +34 91 552 9265 ♦ info@esker.es ♦ www.esker.es
Esker UK Ltd. (Derby) ♦ Tel: +44 1332 54 8181 ♦ info@esker.co.uk ♦ www.esker.co.uk

Table of Contents

1

LDAP introduction

LDAP (Lightweight Directory Access Protocol) is a protocol that lets you access information via a directory system. LDAP is the Internet's standard directory services protocol. It allows directory searches and updates and includes authentication and network resource access control.

A directory is a special kind of database that gives the user a static view of its data. It allows users to view and update its data easily.

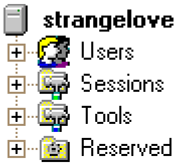
A directory system is an object-oriented database that represents users and network resources as objects. Each object contains information that's specific to a given user or resource. The objects are stored hierarchically in a directory tree that constitutes the work environment. This tree can be organized according to users' needs. A directory system allows secure access to data using a double mechanism of identification and authorization; each user must identify himself to access directory services. He then only has access to the network resources for which he has the required access rights.

There are many advantages to using this system for network administration:

- Unique user identification independent of network location: the user begins by connecting to the system using a login ID and password. He can then access all the network resources for which he has access rights. He uses the same ID regardless of the machine from which he connects.
- Centralized network data administration: network maintenance and administration are simplified and can be carried out on a single machine (avoiding the repetition of some operations). Administration can be carried out centrally or it can be partially delegated without risk to data coherence.
- Data protection: this system makes it possible to associate a level of security to each branch of the directory tree. This security level applies to each of the objects in the branch.
- Customization: the directory tree structure can be adapted to user requirements.
- Adaptability: The system can be adapted to any network size and type.

Administrator structure

The Administrator contains four main directories:



strangelove
- Users
- Sessions
- Tools
- Reserved

- Users: all the users and groups of users. (Default directory)
- Sessions: All the sessions, network access configurations, etc., referenced on the LDAP server. (Default directory)
- Tools: all the objects required to create configurations (buttons, function-key panels, bitmaps, backgrounds, default configurations, etc.). This directory is hidden by default, and may be displayed for viewing or modification by changing the properties of the LDAP database at the root.
- Reserved: services registered on the LDAP server. This directory is hidden by default, and may be displayed for viewing or modification by changing the properties of the LDAP database at the root.

General Administrator principles

To understand fully the functioning and use of Administrator, a number of concepts must be explained.

User and user group

A user is a specific resource, identified by a user name and password. In the resource tree below a user, we find his privileges (or his profile if you're using Netscape Directory Server), and his private and favorite resources.

A user group is a collection of users and/or subgroups of users. In the resource tree below a user group, we find the groups privileges and the users and/or user subgroups that belong to the group.

Private and Tun Plus resources

A resource is any element registered in a directory on the LDAP server, except for services.

Tun Plus resources refers to all the resources sharable by all the network users. Each user has only access in his Tun Plus resources directory to the resources defined in his privileges. The network administrator, by default, can view all the resources defined on the network in his Tun Plus resources directory. A user can only create, modify or delete a resource in his directory if he has write access rights to this resource.

Private resources refers to all the resources that belong to a user. Each user only has access to the resources in his private resources directory that he himself has put there. A user can always create, modify or delete a resource from his private resources directory.

Reserved

This is a resource tree directory that includes basic elements from the LDAP server. The File service provides the hard disk directory tree of the LDAP server. The Template service contains all the object classes on the LDAP server.

Privileges

This is a resource tree directory that's specific to a user or user group. It contains all the resources to which the user or user group has been access rights. This directory is unavailable when using Netscape Directory Server.

Configuration

A configuration is the association of a program and the elements that constitute the program, considered from both functional and interface viewpoints. You can create numerous configurations (sessions, FTP sessions, etc.) in the resource tree. This simplifies the use of these programs and lets the network administrator adapt them to the needs of the end users.

Tools

This is a resource tree directory that contains all the objects used to construct configurations for the end users: Bitmaps for buttons, complete toolbars, emulation function-key panels, keyboard configurations, help files, etc.

Object classes and classes

An object class is the general description of an object. A class describes the characteristics of an object, but an instance of this class is required to produce the object itself. In Administrator, the description of object classes is provided by the Template service. Instances of these classes, that is, objects, can be created in each user's Resources and Private Resources directories.

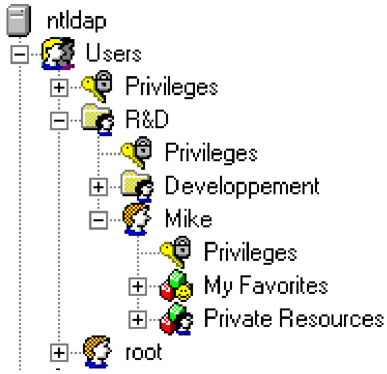
DN (Distinguished Name)

In the LDAP directory system, the DN is a name that identifies uniquely each entry in the resource tree (that is, each directory, subdirectory or object that appears in the hierarchy).

Each entry has a name which, associated with the key representing the type of entry, forms the RDN (Relative Distinguished Name). From this relative DN, you obtain the full DN by successively adding the different RDNs of the entry's parent directories upward through the directory tree. A DN is a sequence of relative DNs separated by commas: The RDN furthest to the left is that of the entry identified by the DN.

Example:

For example, let's take the user Mike, who appears in the resource tree:



The relative DN of the entry for this user is "uid=Mike". "uid" is the key used for user-type entries, and "Mike" is the name of the entry.

You obtain the entry's full DN by adding the relative DNs of Mike's R&D group, the Users directory, the directory for the ntldap server, and finally the domain identifiers. This produces the DN:

"uid=Mike,gn=R&D,sn=Users,sv=ldapsvr,o=Esker,c=FR".

Note:
This example is based on the Users directory as it appears if you use the Tun LDAP server.

Starting the Administrator

To start the LDAP-based administration tool Administrator, do the following:

1. Start your Internet browser and enter the URL of the Administrator tool (by default, this is webadm.htm) to connect to the HTTP server with Tun Plus.
2. Enter your user name and your password, and then click Login. Administrator displays as a directory tree, known as the resource tree. The appearance of the resource tree differs depending on the access rights associated with the user name used to log on.
3. Click Advanced to change your password or define the default language.

Note:
If you use a Netscape Directory Server LDAP host instead of the Tun LDAP host, you will have to enter into the User field the user identifier followed by the "Directory suffix" defined on installation of Netscape Directory Server. For instance:

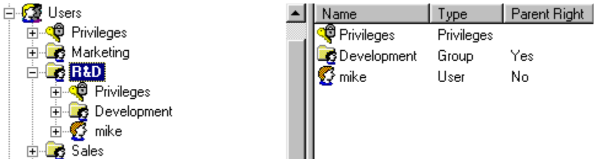
```
uid=Mike, o=Esker, c=fr
```

Once you connect, you can change the password linked with your user name. You use this password when you log on to the LDAP server. To do that, choose Change Password from the server's context menu. A dialog box opens to let you change your password.

Viewing the contents of an object

There are two ways to view the contents of an object:

1. Click the object in the left pane to highlight it; its contents are displayed in the right pane.
2. Double-click the object in the left pane; its contents appear below the object in the same pane.



Name	Type	Parent Right
Privileges	Privileges	
Development	Group	Yes
mike	User	No

Viewing the directory tree

There are three ways to view the subtree of a given object:

1. Click the plus sign (+) beside the object in the left pane to display the directory tree below the object in the same pane, and the minus sign (-) to hide it.
2. Double-click the object in the left pane.
3. Use the command Expand in the context menu.

Displaying the properties associated with an object

To display the properties of an object, click Properties in the context menu associated with the object.

Updating the display

The command Refresh in the context menu updates the display of the object's contents. The update is automatic.

Deleting an object

There are two ways to delete an object:

- Select Delete from the context menu.
- Select the object and use the Del key on the keyboard.

Renaming an object

There are two ways to rename an object:

- Select Rename from the context menu.
- Select the object by clicking it (it's then highlighted), and then click again (the cursor appears).

Copying objects

To copy an object, you can use drag and drop. Depending on the operation you want to perform, do one of the following:

- To move an object without copying it; select it first, hold the mouse button down and drag the object to the desired location. Then release the mouse button.
- To create a copy of an object; press the Ctrl key while you click the object, hold the mouse button down and drag the object to the desired location. Then release the mouse button.
- To create a link on an object; press the Shift and Ctrl keys at the same time and select the object. Hold the mouse button down and drag the object to the desired location. Then release the mouse button. Once the link is created, any changes made to the source object are also made to the copies of the object.

You can also use one of the following methods to copy the object:

1. Click the object (which is then highlighted).
   Either:

- Select Copy from the context menu.

  OR

- Use the keyboard shortcut Ctrl C.

2. Click the target object (highlight it).
   Use one of the following methods to paste the object selected:

- Choose Paste from the context menu.
- Use the keyboard shortcut Ctrl V.

Selecting several objects

1. To select a group of successive objects, click the first object and hold the Shift key down while clicking the last of the desired objects. The intermediary objects are also selected.
2. To select several objects that aren't adjacent, hold the Ctrl key down and click the desired objects.

   When you've made your selection, you can use a context menu (displayed using the right mouse button) to perform operations on the selected objects.

Ordering of objects in a directory

By default, all the elements in a directory are displayed in the hierarchy in alphabetic order. However, you can change the order of a directory's components by moving them up or down the tree.

To do this, choose Move from the context menu of the object you want to move. If this option doesn't appear in the context menu, you must activate ordering at the parent directory level. To do that, choose Properties from the parent directory's context menu. Select the Index check box.

The Move option will then appear in the context menus of all the objects in the directory.

Publishing a configuration

From Administrator, copy the configuration from the directory under /Sessions in which you created it, to the user's or user group's Privileges directory. The user or users can then access the session by clicking the session icon on their Desktop page, as long as you have given them Read or All access rights.

▸ Retrieving a session access URL

Right-click on a session in the Sessions directory, and select Properties. The URL generated for the session appears in the URL field under the URL Access tab. You can then copy this to a webpage, email, etc.

User access to Tun Plus resources

Users can use Tun Plus to access their resources in two different ways.

- Connecting to a particular HTML page called the Desktop. Each user can use this page to access a personal working environment containing all resources and configurations for which the administrator has given him rights.
- Using a particular URL to run a session directly. This URL is generated when the configuration is created. For example, it could be placed on an HTML page on an intranet site.

The Desktop page

The Desktop is a client tool that lets end users browse available sessions as well as other resources like web pages, FTP sites, programs, documents, and more. Access it from the Tun Plus home page on the Tun Plus HTTP server by clicking the Users option.

Note:
Resources on the Desktop are also accessible from other HTML pages, allowing users to connect to them automatically (without having to enter the login and the password for the session or other resource). Access to resources in automatic connection mode is described in the Automatic Connection section in this chapter.

Administrators and users with LDAP privileges may access the Administrator tool and the LDAP database by clicking on the Administrator option on the Tun Plus home page. Users may access sessions created by the administrator by clicking Users on the Tun Plus home page to open the Desktop page. A log on window displays in your browser. Users must enter a valid name and password to access configurations from the LDAP database, and then click on the Login button.

The Desktop page contains sessions and other resources created by the administrator for the end users to access. For resources to appear on the Desktop page, they must be:

- Accessible with Read or All rights.
- Associated with one or more actions; for example, a printer can be installed or uninstalled, an FTP session can be opened, a URL can be contacted, a data source can be opened or queried, etc. However, you can't use a toolbar resource type if it's not linked to a configuration. Therefore, you can't access this resource type directly from the Desktop page.

Advanced login parameters

When logging into the Administrator, you can access other connection parameters by clicking on the Advanced button. These parameters include the language in which the Desktop will be started, firewall parameters, and security settings.

New password/Confirm password
Enter and confirm the new password for the Administrator here.

Use a proxy server (socks protocol)
To configure the firewall, select this check box.

Name of the proxy server
Enter the name or IP address of the server that is used as firewall (only enter a name if your system uses a DNS).

Port number
By default, the port number corresponding to the Socks protocol is 1080. If your configuration uses another port, enter the new value in this field.

Do not use for local addresses
By default, access to all the machines on the LAN will be via the firewall configured in this way. If you want to avoid this for connection to a local address, select this check box.

Use SSL
You may choose whether you will use a real certificate or a test certificate.

URL access

You can use the URL access mechanism to generate URLs for running sessions starting only from data stored on the HTTP server (without using LDAP queries). These URLs are intended particularly for use by an Intranet site administrator, to be included in his customized HTML pages. Users can then start sessions directly from these pages by clicking on these URLs.

You can also adapt the size and number of components downloaded to the customer station to suit your needs through the URL access. By default, all components are downloaded the first time that the configuration is started. A user who simply needs to access a terminal in pure emulation without any specific functions will not use all these components. With a URL access, he will be able to run a "light" session, with limited functions but less expensive in terms of size and therefore faster.

Note:
When using a URL to provide access to a session, all necessary data are retrieved in a storage file on the HTTP server. Therefore, no LDAP query is necessary when starting a session through URL access, unless you enable users to customize configurations; the modifications made are then saved in his private resources on the LDAP base.

Retrieve a session's URL from the URL Access tab in its Properties.

Automatic connection

Tun Plus offers several automatic connection modes where the user does not need to pass through a login screen to access the resources available from the Administrator or the Desktop. The user will still need to login to the Administrator or Desktop pages. These automatic connection modes use the following methods:

- A connection mode using the Windows user name without a password.
- A connection mode using NT connection parameters.

If you want to use these various automatic connection modes, start by connecting to the Tun Plus HTTP server using pages other than those proposed by default.

Automatic Windows connection without a password

If you want to enable the user to connect to resources using an automatic Windows connection, define the user in the LDAP base with the following parameters:

- Name: the Windows user name that he uses when the machine starts
- Password: an empty string.

When the user accesses a resource via URL, he can do so without entering a login name or password for the resource.

Windows NT automatic connection

You must import an NT user base into the Tun Plus LDAP base before you can use this connection mode.

In this case, imported NT users can connect directly to resources using URL access with their NT connection parameters as their login information.

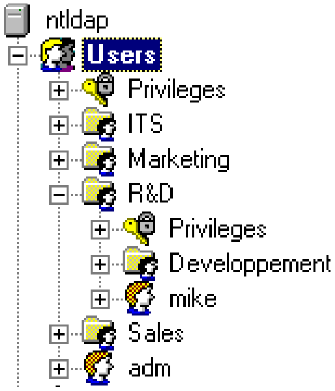
2

Administrating users

Note:
If you use a Netscape Directory Server LDAP host instead of the Tun LDAP host, the functionalities described in this chapter will differ. For more details, refer to the section Administrating users with the Netscape LDAP host, at the end of the chapter.

The Users directory hierarchy

The users are organized in the Users directory in groups and subgroups as shown in the figure below:



Each user and group has specific access rights that are defined in the user's or group's Privileges directory.

The access rights are the permissions given to the user to allow him to administer an object (resource, service or group of users). The permissions are attributed to the user by dragging and dropping the object into the user's Privileges directory. When a user connects to the administration tool, he only sees the objects he is allowed to view or administrate in the resource hierarchy. The management of users and access rights makes it possible to provide shared administration.

In the user's resource hierarchy, you can do the following:

- Create or delete a user or group of users.
- View and/or edit a user or group of user's properties.
- Associate access rights with a user or group of users.

Creating a user

As administrator, you can create as many user names as you want on the LDAP server.

To create a user, choose New > User from the context menu of the directory where you want to place the user.

Creating a user group

As administrator, you can create as many groups and subgroups of users on the LDAP server as you want.

To create a group of users, choose New from the context menu of the directory in which you want to create it, and then choose Group.

Note:
A user can belong to several groups. In this case, when the user connects to the LDAP server, he will be able to access all the resources that are accessible through each occurrence of his user name.

Deleting a user

To delete a user, right-click the user to display his context menu. Then:

Choose Delete from this group if you only want to delete the user from the current group.

Choose Delete from all groups to delete the user from all the groups he belongs to.

Deleting a group

To delete a group of users, click the group with the right mouse button to display the context menu. Then, Choose Delete. This deletes groups, not groups of users and all user occurrences.

Viewing and/or editing the properties of a user or a group of users

To view or edit the properties of a user or a group of users, right-click the user or group of users to display the context menu and choose Properties. The user or group's dialog box opens. The fields in this dialog box are described in the sections "Creating a user" and "Creating a user group".

Attributing access rights to a user or a group of users

You can drag and drop a resource or group of resources to a user or a group. The user, or group of users, can then access the resource from his resource hierarchy or the Desktop.

Access to resources and directories on the LDAP server depends on the access rights the administrator attributes to the users. There are three levels of access rights:

- All: Full rights (read, create, modify, and delete resource or directory).
- Read:: The user can only read the contents of the resource or directory.
- Hidden Read: The user can't view the hierarchy above the object (resource or directory) covered by the access rights (except if an object below the resource can be accessed with All or Read rights). However, the user can use the object if, for example, he uses a configuration that calls it.

Attributing resource access rights to a user or group of users

Select the resource for which you want to allow access rights to a given user (or group). Drag and drop the resource to the user's Privileges directory.

The user or group then has the default level access rights for this resource. There's always one level of access rights by default that applies to every new object (resource, directory, or service) the user is allowed to access. To change the default level of access rights, you can do one of two things:

Double-click as necessary the value of the access rights level in the Level column.

Double-click the resource name in the Type column. In the dialog box that opens, select the option you want in the Level section.

Changing the default access rights of an object

You can change the default value of the access rights level that is attributed to every new object a user is allowed to access.

To do that, display the context menu from your server directory and click Properties. In the Default Privileges section, choose the Rights Level you want to attribute by default: Hidden Read, Read or All.

The default level of access rights applies to all the users.

Checking user's access rights

To check user access rights, right click the User group icon to display the context menu, and then select Check > Rights.

This option makes it possible to check the coherence of rights within the LDAP base (for instance, in the case of rights on resources that do not exist any more).

Administrating users with the Netscape LDAP host (Netscape Directory Server)

You can use Tun Plus with the Netscape LDAP host: Netscape Directory Server. In this case, user administration is different from that described previously and corresponds to the use of the Tun LDAP host. This section describes the organization of units with the Netscape LDAP host, and shows you how to:

- Create users, groups and organizations.
- Attribute or create permissions regarding resources.

The Netscape users resources tree

If you use the Netscape Directory Server,, the user resources tree includes:

- A main organization () and sub-organizations (). For instance, the main organization may correspond to your company or group and each sub-organization to a company subsidiary.
- All the users () and user groups () are directly under the root of the organization (or of a sub-organization). Users belonging to a group are defined in the properties of that group.
- Under each user are the following items: his/her Profile, Favorites and Private resources.

The use of the Favorites and Private resources directories of a user is similar to that of the Tun Plus LDAP host (see Ergonomics and general principles of Administrator, General concepts of Administrator, Users in the chapter entitled Presentation of Administrator). To add a resource to one of these directories, simply select it in the resources tree and copy or move it into the directory. To create a resource in one of these directories, from the directory context menu, select New > Resource.

On the other hand, the method of attributing rights operates inversely to that of the use of the Tun Plus LDAP host. To attribute rights to a user (the term used is “permission” regarding a resource or “target”), you must select the user and move him/her onto the resource. In this way, you create permission indicating the attributed rights and the parties to whom those rights are attributed (“Attributing permission to a resource” on page 19).

Creating a sub-organization

To create a sub-organization, from the context menu of an organization, select New > Organization. Then, complete the following fields in the dialog box that appears.

- Organization: Name of the organization, as it will appear in the resources tree.
- Description: Enter any optional text describing the organization.

Creating a user

To create a user, select the option New then User from the context menu of an organization or sub-organization. Then, complete the following fields in the dialog box that appears.

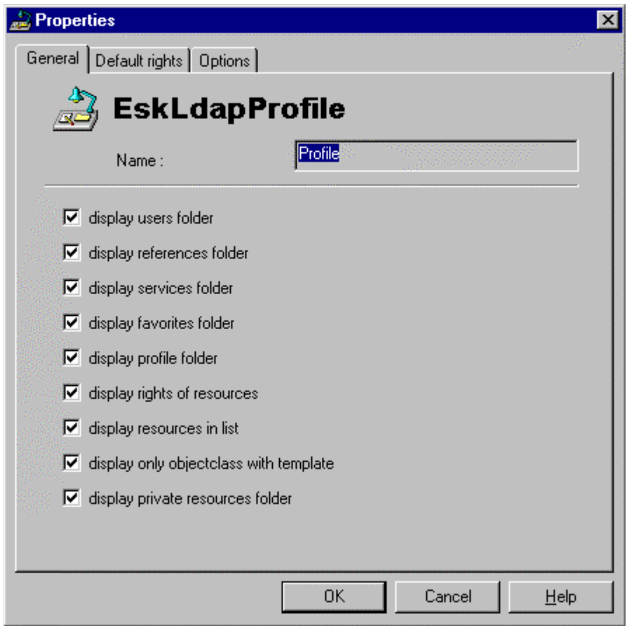
- UID: User name as it will appear in the resources tree.
- Given name: Given name or first name of user.
- Surname: User family name (mandatory).
- Full name: The full name of the user, often used to designate him/her (mandatory). In most cases, it is the given name followed by the surname.
- Title: Description of user title.
- Mail: E-mail address of user.
- Telephone number: User’s telephone number.
- Password: Password with which the user can access his/her resources.

Changing a user profile

A user profile specifies for the user involved:

- The directories displayed in the Administrator resources tree,
- The default rights,
- The display options and the language used.

To modify a user profile, select the Profile sub-directory for the user and choose the Properties option from the context menu of the directory.



EskLdapProfile

Name : Profile

☑ display users folder

☑ display references folder

☑ display services folder

☑ display favorites folder

☑ display profile folder

☑ display rights of resources

☑ display resources in list

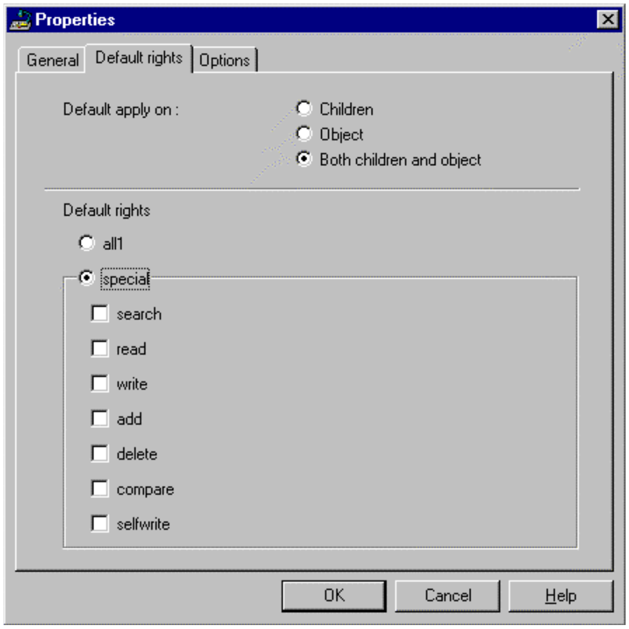
☑ display only objectclass with template

☑ display private resources folder

Select the directories which will be displayed in the user resources tree: users, references, services, favorites, profiles, private resources.

The Display rights of resources and Display resources in list options enable you to indicate the data, which will be displayed in the resource directory "list view.”

The Display only object class with template option enables you to display in the Reserved\Templates directory only the objects that have a template. If you deselect this check box, the object classes without a template will appear (gray) in the Templates directory.



Default apply on : ○ Children ○ Object ● Both children and object

Default rights

○ all1

● special

□ search

□ read

□ write

□ add

□ delete

□ compare

□ selfwrite

This tab enables you to define the default rights of the user when a resource is attributed to him/her.

Default apply on

By default, limit each user's rights to a resource to:

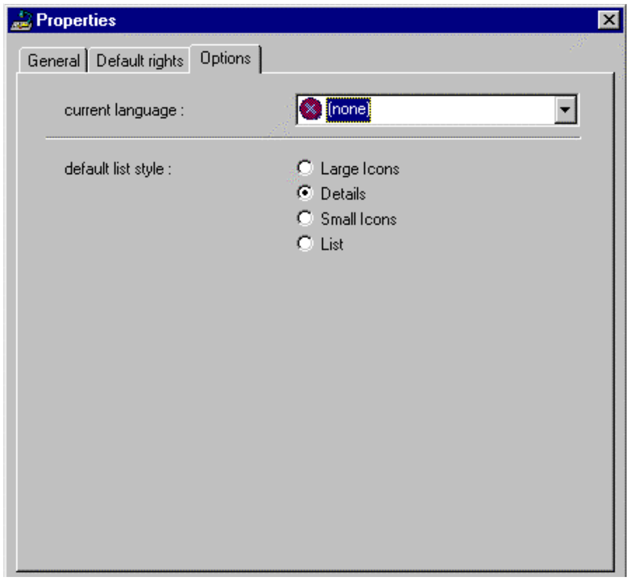
- The resource's sub-objects only (Children),
- The resource only (Object),
- The resource and its sub-objects (Both children and object).

Default rights

Select the type of rights granted by default. You can choose to assign all the rights or simply select some of them among the following:

- Search: enables the user to carry out search requests in the resource directory (note: to see the results of a search, the users must also have read rights for that resource).
- Read: used for the reading of data contained in the resource directory.
- Write: enables the user to add attributes to the resource, to modify attributes or to delete them.
- Add: enables the user to add resources.
- Delete: enables the user to delete resources.
- Compare: enables comparison requests to be made on the resource directory (the response to a comparison request is of the Yes/No type).

- Selfwrite: enables the user to add or delete himself to or from a group.



current language : (none)

default list style :
○ Large Icons
● Details
○ Small Icons
○ List

Current language

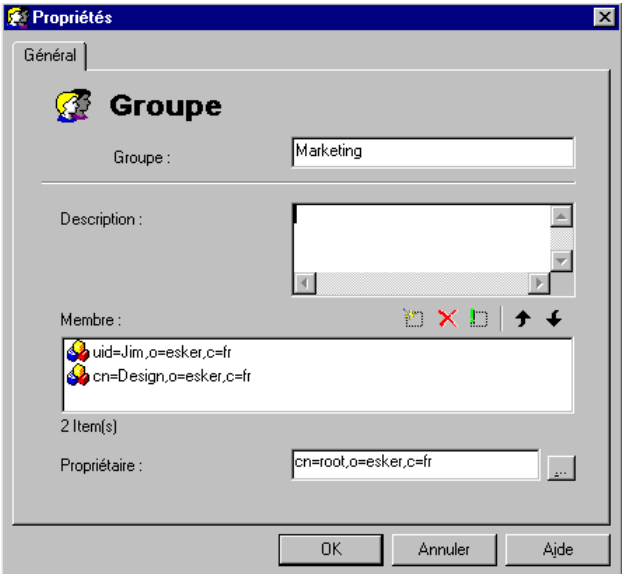
Select the language for the user interface display.

Default list style

Select the data display style in the "list view" of the Administrator: large or small icons, list, detailed list.

Create a users group

To create a users group, from the context menu for an organization or sub-organization select New > Group.



Groupe

Groupe : Marketing

Description :

Membre :
uid=Jim,o=esker,c=fr
cn=Design,o=esker,c=fr
2 Item(s)

Propriétaire : cn=root,o=esker,c=fr

Group

Group name as it will appear in the resources tree.

Description

Optional text describing the group.

Member

Indicate the various members of the group:

- To add a user or a group, click □.
- To delete a user or a group, select it and click ✕.
- To modify the DN of a user or member group, or to replace it, select it and click □.

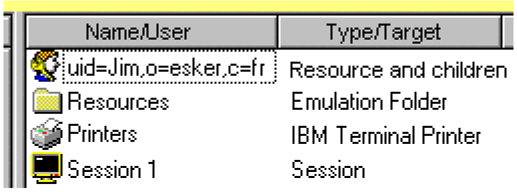
Owner

Name of group administrator. click the … button to select a user in the users list.

Attributing permission to a resource

To attribute resource access permission to an organization, user, or user group, select the organization, user, or group, and then drag and drop the organization, user, or group onto the resource.

A permission icon (symbolized by a key) will then appear in the "list view" of the resource:

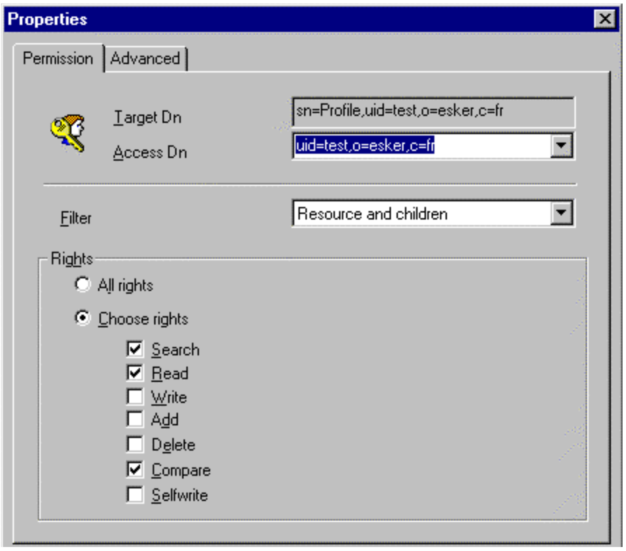


Name/User	Type/Target
uid=Jim,o=esker,c=fr	Resource and children
Resources	Emulation Folder
Printers	IBM Terminal Printer
Session 1	Session

Note:
Permissions are displayed in the "list view" of the resources tree if the Display rights of resources check box is selected in the user profile under the name by which you are connected (see above Modifying a user profile).

The Target field indicates which resources include the permission: the resource alone, the resource's sub-objects, or the resource and its sub-objects.

To display the permission properties, right click the permission in the "list view" and select Properties. The following dialog box appears:



Target Dn: sn=Profile,uid=test,o=esker,c=fr

Access Dn: uid=test,o=esker,c=fr

Filter: Resource and children

Rights

○ All rights

● Choose rights

☑ Search
☑ Read
☐ Write
☐ Add
☐ Delete
☑ Compare
☐ Selfwrite

Target Dn

This non-editable field displays the DN of the resource for which permission is granted.

Access Dn

This field indicates the organization DN, that of the group or user to whom permission is granted. You can change the value of this field by selecting one of the options in the dropdown list:

- all: permission for the resources granted to all the authenticated users in the database.
- anyone: permission to the resource is granted to anybody (anonymous user).
- self: permission to the user type resource is granted to the user itself. This option applies only to a user type resource.
- parent: permission to a user type resource is granted to the user parent directory (e.g. the organization to whom the user belongs). This option only applies to a user type resource.

Filter

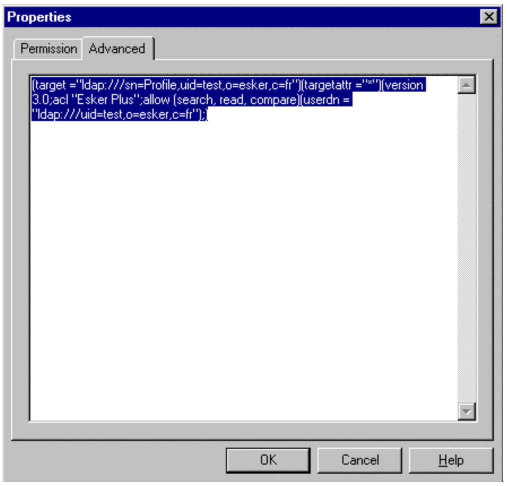
Select the resources and sub-resources to which the permission applies:

- Resource and children: permission concerns the resource and all the children in the resources tree.
- Resource only: permission concerns the resource alone.
- Children only: permission concerns one of the children of the resource only.

All rights/Choose rights

Select the type of rights granted. You can choose to assign all the rights or simply select some of them among the following:

- Search: enables the user to carry out search requests in the resource directory (note: to see the results of a search, the users must also have read rights for that resource).
- Read: used for the reading of data contained in the resource directory.
- Write: enables the user to add attributes to the resource, to modify attributes or to delete them.
- Add: enables the user to add resources.
- Delete: enables the user to delete resources.
- Compare: enables comparison requests to be made on the resource directory (the response to a comparison request is of the Yes/No type).
- Selfwrite: enables the user to add or delete himself to or from a group.



```
(target ="ldap:///sn=Profile,uid=test,o=esker,c=fr")(targetattr ="*")(version
3.0;acl "Esker Plus";allow (search, read, compare)(userdn =
"ldap:///uid=test,o=esker,c=fr");)
```

This tab displays permission according to the Netscape syntax. It enables you to configure advanced permissions while modifying the code yourself. Consult the Netscape Directory Server documentation for more details about permission syntax.

Creating permission for a resource

To create permission for a resource, from the resource context menu select New > Permission. Then, fill in the fields described in the section Attributing permission to a resource.

Allowing the users to change their passwords

By default, Netscape Directory Services does not allow users to change their passwords users are not allowed to change their passwords.

To authorize a user, or each user of a group or an organization to modify his password, select the parent directory under which this right will be granted. Then, from the context menu of this directory select New > Permission. Under the Advanced tab, enter the following permission with the Netscape Directory Server syntax:

```
(target ="ldap:///<EntryDn>")(targetattr ="userpassword")(version 3.0;acl"User Password
managment";allow (write)(userdn = "ldap:///self");)
```

Where <EntryDn> corresponds to the parent object, under the permission directory, from which a user will be able to change his password (for instance, an organization or sub-organization).

Or :

```
(target ="*")(targetattr ="userpassword")(version 3.0;acl"User Password manag-
ment";allow (write)(userdn = "ldap:///self");)
```

In this case, the permission will automatically relate to all the sub-objects of its directory.

3

Creating Configurations

You can create a new session using the New Session Wizard. This wizard helps administrators create new sessions by requesting the parameters for the session in a navigable, wizard format.

▸ Creating a new session

1. Click (the New Session Wizard button) in the Adminstrator toolbar.

   The first New Session Wizard dialog appears.
2. Select the type of emulation for this session then click Next. The second screen of the New Session wizard appears.

Note:
When creating FTP file transfer sessions and Other asynchronous sessions, the Next button is replaced by the Finish button and there is no second wizard screen.

3. Select the client type (either ActiveX or Java) and click Finish. The remaining dialogs ask for more specific emulation information. Complete these dialogs.
4. Click Finish on the last dialog to create the new session

   Tun Plus stores new sessions in the Sessions directory on the LDAP tree.

▸ Modifying a session

To change a session's parameters, right-click it, then select Properties.

You may also change a session by changing the parameters in its Terminal, Preferences, and Advanced directories. In these directories, you can set most of the preferences, including the color schemes, keyboard mapping, fonts, hotspots, and panels.

Running a Windows application from an emulation session

Tun Plus permits you to run Windows and host applications simultaneously on your PC. To run a Windows application from an emulation session, you can do any of the following:

- Create a button to this effect in a function-key panel.
- Create a hotkey for the task.
- Attribute an escape sequence to the task and include it in an application menu.
- Link the operation to a mouse event.

A function-key panel is a fully customizable tool for which you can create buttons that perform individual tasks. For example, a button can send a specific character string or execute a macro.

Using macros to run an emulation session automatically

In standard networks it's fairly common to have to go through one or more gateways and enter one or more passwords before accessing an application. This type of login procedure isn't very practical if you access these applications frequently.

Tun Plus provides a macro-language that lets you create macros to automate certain tasks. For example, the different stages of starting an application or disconnecting can be made transparent (login and password request, starting an application, etc.).

A macro is a text file containing a sequence of instructions required by the server.

Note:
In the case of Java emulations, the macro language used is TCL.

▸ Creating a macro in the ActiveX version

From the Administrator, open the directory containing the UNIX or IBM emulation macros. This directory is located below the directory Tools (/Tools/Host Access References/UNIX Emulations/Specific Data/Macros or /Tools/Host Access References/IBM Emulations/Specific Data/Macros). Choose New from the context menu of the Macros directory and then choose Macro. The Windows text editor Notepad opens for you to enter the macro text.

▸ Creating a macro in Java version

From the Administrator, open the directory containing the Java emulation macros. This directory is located below the directory Tools (/Tools/Host Access References/Java Emulations/Macros). Choose New from the context menu of the Macros directory and then choose Macro. A creation Wizard opens for you to enter the macro text.

Running a macro on login

The advantage of a macro is that it automates specific tasks. It's common practice to automate login and application startup for users.

To do that, you can associate a macro with a session, just like you associate terminal settings (emulation settings files) and display settings (colors, background, function-key panel, etc.). A macro can be associated with a session at the start (login macro) and/or at the end (the macro runs when you exit the session).

When you create a session, you can associate a start and/or end macro with the session. These macros are characteristics of the session preferences.

▸ Associating a macro to a session

From the Administrator, open the Preferences directory of the relevant session (Preferences > Macro > Properties). Click the Macro tab. The list shows the macros that are stored in the Sessions directory of the configuration in question. To add a new macro to the configuration, click Browse and select the macro from those registered on the LDAP server.

Printing with templates in 3270 or 5250 emulation

Printing pages from an emulation session can sometimes be a long and tedious task. You have to print each screen separately. Tun Plus' 3270 and 5250 provide template printing to simplify this operation: This lets you create reusable print templates for your print jobs.

To print from templates, you must first define the template: Screen area to print (so you don't print the whole screen unnecessarily), choice of keys to scroll the pages, print start and finish text, etc.

There are two ways to create printing templates:

- Use the appropriate button, if the administrator has included one to this effect, in the application.
- Use Administrator (administrator only).

▸ Creating a new printing template

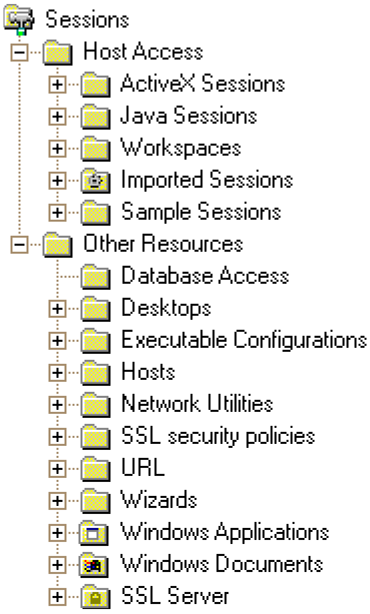
From the Administrator, open the directory containing the printing templates below the Tools directory (/Tools/Host Access References/IBM Emulations/Specific Data/Print Templates). Choose New from the directory's context menu and then choose Print Template type.

4

Administrating Resources

Resources are parameters or configuration files used by Tun Plus' client applications. They display in a hierarchy or tree that the administrator may structure as needed.

The default resources are listed in either the Tools or Sessions directory:



- Sessions
  - Host Access
    - ActiveX Sessions
    - Java Sessions
    - Workspaces
    - Imported Sessions
    - Sample Sessions
  - Other Resources
    - Database Access
    - Desktops
    - Executable Configurations
    - Hosts
    - Network Utilities
    - SSL security policies
    - URL
    - Wizards
    - Windows Applications
    - Windows Documents
    - SSL Server

The Sessions directory contains:

- Host Access: This folder contains sessions for servers on the network.
- Other Resources: This folder contains links, useful documents and programs provided as examples. Users may adapt these examples to suit individual needs.

The Other Resources directory contains:

- URL: Web site addresses.
- Hosts: Servers on the network.
- Windows Applications: Windows applications.
- Windows Documents: Documents that can be used from the Windows client PC.
- Network Utilities: These include FTP sessions.

In addition to the Sessions directory, there is the Tools directory. This is a special directory that contains all the reference elements used to construct emulation, network applications and database configurations (images, HTML reference pages, toolbars and application-specific configuration elements). The Tools directory is hidden by default. You can display this directory by changing the properties of the LDAP database root.

Note:
The list of resources in this directory is not exhaustive. It can be completed according to needs.

It also contains links, useful documents and programs provided as examples. The user should adapt these examples to suit his needs.

Tools

The Tools directory is represented by the icon . This directory can contain all the objects required to construct configurations for the end users: images for the buttons, complete toolbars, emulation function-key panels, keyboard configurations, etc. This directory is hidden by default. To display this directory, right-click on the server name (root) in the LDAP tree, then select Properties admin. On the dialog that appears, select Display Tools folder, then click OK.

By default, Tun provides the following predefined references:

- Host Access References: Tools used to create sessions.
- Color Styles: Color and style definitions for the HTML pages the applications are started from.
- Countries: This directory contains a list of all country codes for use by Tun Plus emulations.
- Database Access References: Tools for using databases.
- Help: Help files.
- Language: Language files.
- Network Access References: Tools used to configure the network applications (FTP).
- Desktop styles: Pre-configured Desktop configurations.
- Tun Plus options: This provides additional information on the Tun Plus version number.

However, you may organize this directory as desired. You can create subdirectories for storing the different objects you use to build your configurations. You can also create as many new references as you want, or modify existing ones.

Host Access References

The Host Access References directory contains the elements used to define sessions. The Bitmaps, Hotspots and Panels subdirectories contain elements that can be used in any ActiveX session. The Unix Emulations, IBM Emulations, and Java Emulations subdirectories contain elements that can be used to create those specific sessions. All directories include:

- A Buttons directory () containing the buttons you can place on the toolbars referenced in the Toolbars directory. Each button is defined by a name, an image and an action (JavaScript code) entered in its Properties box.
- A References Pages directory () containing the HTML pages you can start the configuration from.
- A Toolbars directory () containing the different toolbars used with the configuration. Each toolbar consists of a group of buttons placed on the toolbar.
- A Specific Data directory containing data that are specific to the type of emulation.
- The 3270 Default Access, Unix Default Access, 5250 Default Access, and Default 3287 Printer and subdirectories are the default IBM 3270, Unix, IBM 5250, and IBM 3287 emulations. These directories contain the directories defined when you create a new session.

IBM Emulations

This directory provides all the elements needed to create an IBM session. It includes the Buttons, Toolbars and References Pages subdirectories as well as the Specific Data directory which contains the following IBM emulation elements:

- Charsets: Character tables.

- Color Schemes: Descriptions of the colors used for the different emulation attributes.
- Keyboards: Emulation keyboards.
- Macros: Macro files.
- Print Templates: Printing templates.

Unix Emulations

This directory contains the elements used to create asynchronous sessions. In addition to Buttons, Toolbars, and References Pages, the Specific Data directory contains:

- Contexts: Predefined display settings. Display settings are a collection of all the parameters used in an emulation session in a single entity: Font, emulation window dimensions, attribute colors, background bitmap, function-key panel and mouse parameters.
- Control Codes: Files describing the actions provoked by the control characters (like line feed and carriage return).
- Escape Sequences: Files containing the escape sequences that provoke special actions (like clearing the screen or cursor positioning).
- Host to PC conversions: This directory contains : files to convert the host codes to the values displayed on the PC.
- Key Functions: Files defining the values associated with the function-keys.
- Keyboards: Keyboard definitions. The codes sent by the keyboard refer to a piece of information (character to send, reference to another filter, action to perform, dead key).
- Macros: Macro files.
- National Keyboards: Files defining the language-specific values returned by the keyboard.
- PC Keyboard Layout: Files defining the available PC keyboard types.
- PC to Host conversions: This directory contains files to convert special PC characters to the host's character set.
- Terminal Keyboard Layout: Files defining the available terminal keyboard types.
- Terminal Setups: Terminal configuration files.
- Terminals: Terminal definitions with the different settings files for the session.

Java Sessions

This directory provides all the elements needed to create a Java session. It includes the Buttons, Toolbars, References Pages, and Macros subdirectories as well as the Specific Data directory, which contains the following Java emulation elements in folders specific to an emulation:

- Charsets: Character tables.
- Keyboards: Emulation keyboards.

- Color Configurations: Color palettes and combinations.

Database Access References

The Database Access References directory contains the Datamart Application and Query Application subdirectories with all the elements needed to define SQL data sources.

The Datamart Application directory contains the following subdirectories:

- A Buttons directory () containing the buttons you can place on the toolbars referenced in the Toolbars directory. Each button is defined by a name, an image, and an action (JavaScript code) entered in its Properties box.
- A References Pages directory () containing the HTML pages you can start the configuration from.
- A Toolbars directory () containing the different toolbars used with the configuration. Each toolbar consists of a group of buttons placed on the toolbar.
- An example of a standard data source template configuration.

The Query Application directory contains the following subdirectories:

- A Reference Pages directory () containing the HTML pages you can start the configuration from.
- An example of a query.

Network Access References

The Network Access References directory contains the elements needed to define FTP application configurations. The FTP Application subdirectory contains everything you need to create FTP file transfer configurations:

- A Buttons directory () containing the buttons you can place on the toolbars referenced in the Toolbars directory. Each button is defined by a name, an image and an action (JavaScript code) entered in its Properties box.
- An HTML generation directory containing JavaScripts () and JavaScript event handlers ().
- A Profiles directory ( ) with predefined FTP profiles.
- A References Pages directory () containing the HTML pages you can start the configuration from.
- A Toolbars directory () containing the different toolbars used with the configuration. Each toolbar consists of a group of buttons placed on the toolbar.

Color Styles

This directory contains style and color settings that can be used in the HTML pages the users access from their Desktop.

The elements defined in these settings are:

- The color and background image of the HTML page.
- The color of the font used.
- Page margins.
- The hyperlink colors.

You can modify these color/style settings by choosing Properties from their context menus.

Help

This directory contains help files, which can be called up from various Tun Plus applications. These help files may be in HLP or HTML format.

Languages

This directory contains all the language files used by the Tun Plus application. Each language is identified by a number. By default, the available languages are as follows:

- English: 00
- French: 01
- German: 02
- Spanish: 03
- Italian: 04

Each file ends with two numbers that represent the language of that particular file.

Creating new tools

You can create as many new Tools as you want. This can be a simple operation (create a new default asynchronous session) or more complicated if it requires some programming (create a new button).

By default, a reference directory lets you create some types of new Tools. You must first familiarize yourself with the list of types and then change it if necessary if it doesn't suit your needs. You can then create the new reference for the type you want.

▸ Discovering which objects you can create in a Tools subdirectory

From Administrator, you can do one of the following:

- Display the directory's context menu: Choose New to see the possible objects.
- Display the directory's properties (choose Properties from the context menu): The Allowed Children tab shows all the objects you can create in this directory.

Example:

Right-click the directory /Tools/Host Access References and choose New from the context menu: As you can see from the list, you can create a new directory, link or session.

Choose New from the context menu for the directory /Tools/Host Access References/Bitmap: You can see that you can only create objects from the Bitmap class. If you look at the Allowed Children tab in Bitmap directory's properties, you'll see that only the Bitmap object class is selected.

▸ Modifying the list of objects you can create in a Tools directory

From Administrator, choose Properties from the context menu for the directory in question. Click the Allowed Children tab. Select or clear the object classes you want. You can use the Check All or Clear All buttons to select or clear all the classes at once.

▸ Creating a new reference

From Administrator, choose New from the context menu of the parent directory. Select the object class for the new reference. Complete the tabs that are displayed.

Note:
Esker provides a set predefined default Tools. These Tools are sufficient in most cases to organize the LDAP server and create the configurations required by the end users. You can, of course, create as many new Tools as you want or edit existing ones. To do this, you need to understand how LDAP and the components supplied by Esker work. For more details, see the Administrator Reference guide.

Example of creating a new toolbar

This example shows you how to create a new toolbar for IBM emulations. You can then use the same procedure to create as many toolbars as you want.

In the Tools subtree, there are:

- An Host Access References directory: Contains all the references used by the sessions.
- A subdirectory of this directory called IBM Emulations: Contains all the references used by IBM sessions.
- Below this subdirectory, the directory Toolbars: Contains the toolbar objects used by IBM sessions.

From this directory, choose New from the context menu, and then Toolbar.

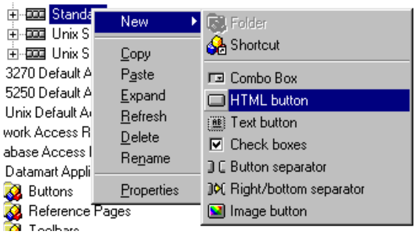
Note:
If the Toolbar option doesn't appear, choose Resource and select the Toolbar object class. This means that you can create different types of object than toolbars in the Toolbars directory. If neither the Toolbar option or the Resource option appears, you can't create Toolbar class objects, for the moment at least. In this case, make sure that the Toolbars directory is the one in which you want to add a toolbar. If this is the case, display the directory's properties and select the Toolbar object class on the Allowed Children tab.

The tabbed dialog box appears with the definition parameters of the new toolbar: toolbar name (enter "Standard"), width and height of the buttons in millimeters, button appearance and width and height of the toolbar separators (keep the default values proposed).

These parameters are defined in what's known as an object class, in this case the toolbar object class.

Once you've created the new toolbar, you can then copy an existing object (for example, by creating a link to a button in the Buttons directory).

You can add tools to the new toolbar. To do that, choose New from the toolbar's context menu: The list of objects you can create on this toolbar appears.



For example, you can create on the Standard toolbar:

- HTML buttons.
- Text buttons.
- Separators.
- Image buttons (buttons with bitmaps).

Example of creating a new button in a toolbar

This example follows on from the previous one: This time we're going to create a button in the Standard toolbar you've just created.

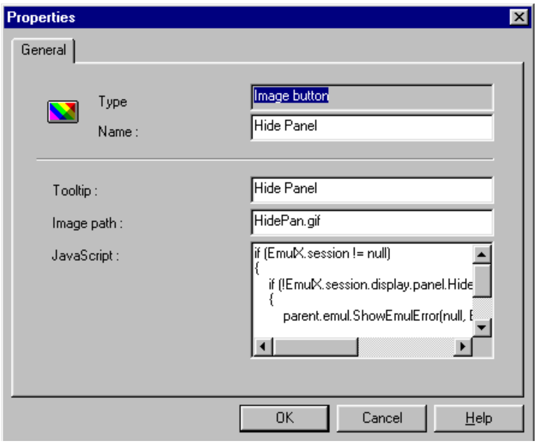
Choose New from the context menu of the Standard toolbar, and then the type of element you want to add to the toolbar. For example, create a new image button.

Enter the button settings. For an image button, these are:

- Name
- Tooltip
- The bitmap file for the button's image
- The JavaScript code that associates a method to the button

A button starts a specific action when the user clicks it. The action, in fact, is started by the JavaScript code.

For example, the Hide Panel button in the Standard toolbar has these properties:



Type: Image button

Name : Hide Panel

Tooltip : Hide Panel

Image path : HidePan.gif

JavaScript :

```
if (EmulX.session != null)
{
   if (!EmulX.session.display.panel.Hide
   {
      parent.emul.ShowEmulError(null, E
```

This button masks the function-key panel in an emulation session. The Javascript code used to create this button is written from Tun Plus' various APIs. A description of these APIs can be found in the programmer's guide supplied by Esker.

Javascript code for the Hide Panel button:

```
if (EmulX.session != null)
{
    if (!EmulX.session.display.panel.Hide())
    {
        parent.emul.ShowEmulError(null, EmulX.session.display.panel.GetLastError());
    }
}
EmulX.SetActive();
```

The function-key panel (panel) is a display settings item (display), which is a session item (session), which, in turn, is an emulation application item (emulX). This object has a Hide Panel method which masks the function-key panel.

Creation of the JavaScript and Java toolbar

For your configurations, you can create customized toolbars as well as buttons and items contained in these toolbars. In the Tools/Host Access References directory, select a parent directory for the new toolbar, button, or other item.

- For toolbars, select the Toolbars directory in IBM Emulations, Unix Emulations, or Java Emulations.
- For buttons, select the Buttons directory in IBM Emulations, Unix Emulations, Java Emulations/JavaScript, or Java Emulations/Buttons/Java.

- For other items, select the appropriate directory in the Specific Data directory of IBM Emulations, Unix Emulations, or Java Emulations.

▸ Creating a JavaScript toolbar

From the context menu of a toolbar directory in Tools/Host Access References, select New > Toolbar. Complete the fields on the dialog that appears.

▸ Creating a JavaScript image button

Select New > Image Button from the context menu of a JavaScript toolbar or a reference button directory. Then, complete the following fields on the dialog that appears.

▸ Creating an HTML button or a JavaScript text button

An HTML button is a button appearing as a button with a label. A text button appears as an URL (underlined text).

To create an HTML button or a JavaScript text button, select New > HTML Button or Text Button from the context menu of a JavaScript toolbar or a directory of reference buttons. Then, complete the following fields on the dialog box that appears.

▸ Creating a JavaScript button separator

A separator is a space between two consecutive elements in a toolbar.

To create a button separator, select New > Button separator from the context menu of a JavaScript toolbar or a reference button directory. Then, complete the following fields on the dialog that appears.

▸ Creating a right/bottom JavaScript separator

A right/bottom separator is a way of aligning all the elements located after the separator in the toolbar directory on the right or bottom edge of the toolbar.

To create a right/bottom separator, select New > Right/bottom separator from the context menu of a JavaScript toolbar or a reference button directory. Then, on the dialog box that appears, enter a Name (or DN) of the right/bottom separator as it will appear in the resources tree.

▸ Creating a Java toolbar

Select New > Java toolbar from the context menu of the directory Java Sessions/Toolbars. Then, complete the fields on the dialog that appears.

▸ Creating a button or a Java toggle button

A toggle button is a button which can have two positions: a “depressed” position and a “released” button. To change from one position to the other, click on the button.

Select New > Button or Toggle button from the context menu of the Java Sessions/Buttons/Java Sessions directory of the resources tree, or from the context menu of a Java toolbar. Then, complete the fields on the dialog that appears.

▸ Creating a Java line feed

A line feed indicates that all the elements located after this item in the toolbar directory will be moved to a new line in the toolbar.

Select New > Line Feed from the context menu of the Java Sessions/Buttons/Java Sessions directory of the resources tree, or from the context menu of a Java toolbar. Then, on the dialog that appears, enter a Name (or DN) for carriage return as it will appear in the resources tree.

▸ Creating a Java separator

A separator is one or more line(s) separating two consecutive elements in a toolbar.

Select New > Separator from the context menu of the Java Sessions/Buttons/Java directory of the resources tree, or from the context menu of a Java toolbar. Then, complete the fields on the dialog that appears.

Creating a TCL Java macro

To create a TCL Java macro, from the context menu of the Java Sessions\Macros directory, select New > Java Macro. Then, complete the fields on the dialog that appears.

Creating an emulation reference page

An emulation reference page is a reference to an HTML page on the HTTP server in which a session can be put into action.

To create a reference page, from the context menu of the References Pages directory in the Unix Emulations, IBM Emulations, or Java Emulations directory, select New > Reference page. Then, complete the fields on the dialog that appears.

Creation of color page style

To create a new color page style, from the context menu of the Tools\Color styles directory, select New > Color page style. Then, complete the fields on the dialog that appears.

Object classes

Each object defined on the LDAP server is an instance of an object class. There are lots of examples: There are object classes for toolbars, buttons, emulation, FTP Sessions, data sources, revamped databases, function-key panels, etc.

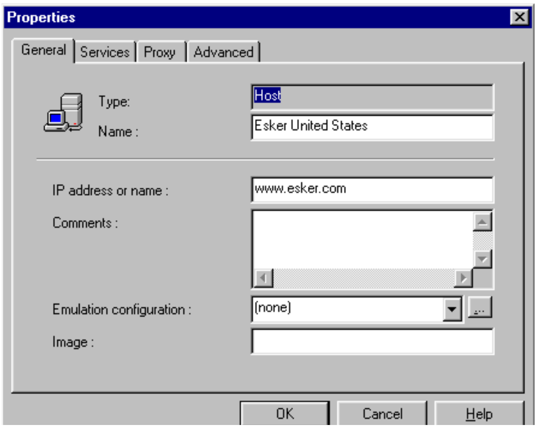
The object classes are listed in the Template service on the server.

Note:
By default, the Reserved directory isn't displayed the first time you connect to the LDAP server. To change the list of directories shown in the directory tree, choose Properties from the LDAP server's context menu and then select or clear the check boxes you want.

For each object class, there is a corresponding set of attributes. For example, a Host object is defined by the following attributes:

- IP address or name.
- Type of server (Telnet, 3270, 5250, PC).
- Comment (optional).
- A default configuration that's started on connection with the server.

In practical terms, when a Host object type is created in the /Sessions/Other Resources/Hosts directory, for example, each attribute defined in the object class becomes a property of the object:



Type: Host

Name : Esker United States

IP address or name : www.esker.com

Comments :

Emulation configuration : (none)

Image :

The tabs defined in the object class that are used to classify the attributes thematically appear as defined in the object's properties.

Note:
Esker provides a set of predefined classes. In most cases, these classes are sufficient to organize the LDAP server and create configurations for the end user. Of course, you can create as many new object classes as you want or modify the existing classes. This operation, however, requires a good understanding of LDAP functioning and the components provided by Esker.

Delegating LDAP server administration

One of the features of an Intranet is that the Web server can be divided into several smaller sites that can be administrated separately. Each project leader or head of department can use just a part of the Intranet with a few simple tools: Marketing can supply information about forthcoming campaigns, sales can publish its results, computing can publish technical bulletins, etc.

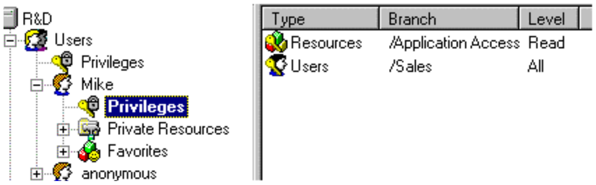
The Tun Plus administration tool was designed to allow delegated administration of the LDAP server. The super administrator has an overall view of the Intranet and the access rights to the objects on the server. He can also authorize individual users (or delegate administrators) to administrate their own part of the server.

Delegation works on the following principle: Any user can connect to Administrator using the user name given him by the administrator. In this case, the Administrator tree shows the resources the administrator has authorized the user to access. These resources can be the configurations the user is allowed to access from his Desktop page (for example, a session), Tools used by configurations, or even a group of users.

Example:

User mike has access to the following resources:

- *Read access to the configurations in /Sessions/Host access.*
- *Full access (All) to the users in the Sales group.*



Type	Branch	Level
Resources	/Application Access	Read
Users	/Sales	All

When the user connects to the Desktop page with the user name mike, he can access all the configurations in the directories in the subtree /Sessions/Host Access (sessions).

When he connects to Administrator with the user name mike, he has Read access to the /Sessions/Host Access sub-

tree. He can change the settings for the users in the Sales group. In particular, he can change their access rights within the limits of his own (in this case, he can give the Sales group users access rights to the resources in the /Sessions/Host Access subtree.)

▸ Delegating administration to a user

From Administrator, attribute the resource access rights desired to a user (resources, users, services, etc.). To do that, see the previous sections that deal with this operation. Indicate to the user how to connect to Administrator with his user name.

▸ Connecting to Administrator

Connect to the Administrator HTML page (webadm.htm by default). Enter the user name with which you want to log on and the associated password.

Network Utilities

A Network utility is the hardware or software installed on the network that lets users perform different operations:

- A host is a resource for storing data or applications, running applications, etc.
- A streamer is a resource for performing backup and restoring data.

For network users, these resources represent enormous potential: The working environment is no longer reduced to a single PC and the devices connected to it directly (like a printer) but includes the entire network.

Transferring data between two machines (PCs or servers)

Data transfer between two machines can take different forms depending on your intentions and your work environment:

- From a terminal emulation session: You can transfer files in either direction between a PC and a host machine. The PC emulates a terminal for that particular host.
- Using the FTP protocol: FTP was largely developed through the Internet. You can use FTP for file transfer and to transform your PC into a file server.
- Using a macro to automate the transfer: You can exploit EMUL's or FTP's macro languages.

Transfers between FTP client on PC and an FTP server

You can transfer files between a PC and an FTP server using the FTP protocol (standard UNIX servers, IBM/MVS servers, AS400 servers, PC server). The FTP protocol ensures the security of transferred data with login ID and password procedures for each connection established with the server.

The transfer mode is either binary (no data conversion) or ASCII (carriage returns and line feeds handled).

The FTP server may also be a PC running an FTPD server program.

In addition to the basic FTP protocol which allows file downloading and uploading, Tun FTP offers the following advantages:

- File and directory transfer using drag and drop in a 100% Windows environment.
- File conversion with filters (binary or ASCII transfer mode). These filters convert Windows files with carriage return characters into UNIX text files with line feed (LF) and no carriage returns (CR). They also convert PC format accented characters into UNIX format (and vice-versa).
- Multi-session implementation allowing transfers between two servers without using temporary files on the PC.
- Session automation using the built-in macro language.

▸ Transferring data via FTP

From the Administrator, open the directory containing the FTP Session you want to use. Choose Connect from the context menu to connect to the server defined in the configuration or choose Open as Administrator if you only want to start the FTP application.

Notes:
If you started Tun FTP by clicking Open as Administrator, the connection isn't automatic. In this case, you must click the New connection icon to establish the connection or else open the configuration again by clicking the Open connection icon.

Transfers between two FTP servers

You can transfer data between two FTP servers from a PC using the FTP protocol. There's no need to create temporary files on the PC. You simply connect via the PC client to the relevant servers and drag and drop the files or directories from one server window to the other.

If the two servers are in the same type of environment, you can transfer the files in binary mode: You don't have to worry about line feeds as with Windows PC - UNIX server transfers.

▸ Transferring data between two FTP servers

From the Administrator, open the directory containing the FTP Session you want to use. Choose Connect from the context menu to connect to the server defined in the configuration, or choose Open as Administrator if you only want to start the FTP application. Repeat the operation for the second server.

Creating an FTP profile

Most servers are standard UNIX servers. You need only read this section if you have a different configuration. Tun Plus provides a number of predefined profiles (MVS, AS400 and standard UNIX).

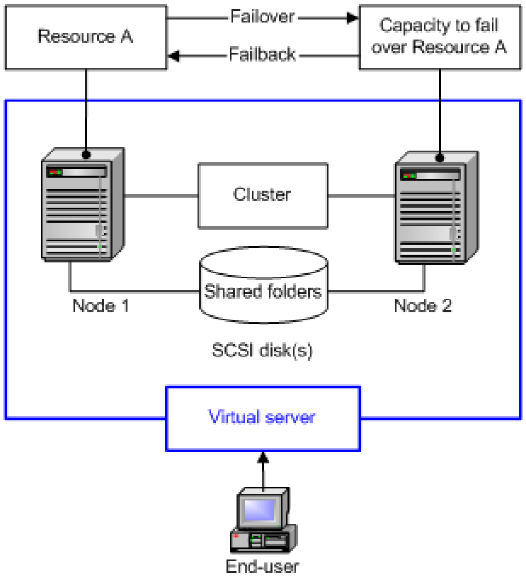
▸ Creating a new profile

From the Administrator, open the subdirectory containing the FTP profiles below the Tools directory (/Tools/Network Access References/FTP Application/Profiles). Choose New from this subdirectory's context menu, and then FTP Session.

Clustered Environment

This chapter explains the installation and configuration of Tun in a clustered environment.

The concept of a cluster is to take two or more computers and organize them to work together to provide higher availability, reliability, and scalability than can be obtained by using a single system. As shown in the figure below, to the end-user's viewpoint, it makes no difference. The various servers - or nodes - are joined together in such a way that they appear as a single environment (a virtual server).



Clustering computers ensures that in case of failure of the node hosting the shared SCSI disk, or in case you want to upgrade your system without interrupting end-user access, operations can be taken over by another node in the cluster thanks to a process called failover.

If a cluster node/resource is unavailable or has failed due to hardware or software problems, its workload is handled by other nodes in the cluster until the failed node/resource is brought back online. Typically the end-user will only experience a limited failure.

Note: The end-user may experience no disruption at all - if they do not access the cluster until the failover is complete. If the user accesses the cluster during the failover, they will receive an I/O or connection-lost error message. All the end-user must do is to click "retry" to refresh or re-establish the connection to the cluster.

Clustering Main Concepts

A server in the cluster is called a **node**.

A cluster node may be **active** (running and participating in cluster operations) or **inactive** (running but not participating in cluster operations).

Clustering is a means of sharing resources between different nodes.

A **resource** is any physical or logical component that can be managed. Examples of resources are disks, network names, IP addresses, databases, Web sites, application programs, services and any other entity that can be brought **online** and taken **offline**.

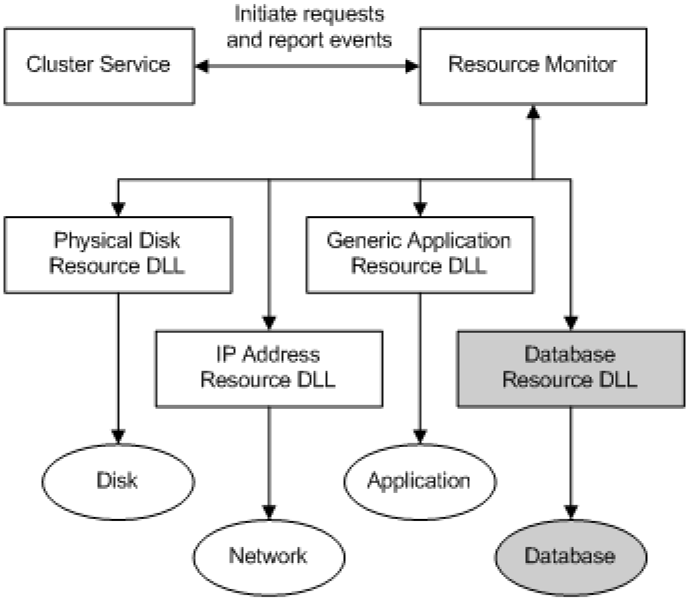
In a cluster, resources are handled in **groups**. Typically a group contains all resources needed to run a specific application or service.

When a failure occurs on a resource, another node in the cluster takes ownership of the whole group that owns the failed resource (this process is known as **failover**). When the failed resource is later brought back online, resources and client requests can be redistributed appropriately (this process is known as **failback**).

A **virtual server** is a group containing a Network Name resource, an IP Address resource, and additional resources necessary to run one or more applications or services. Clients can use the network name to access the resources in the group, analogous to using a computer name to access the services on a physical server. However, because a virtual server is a group, it can be failed over to another node without affecting the underlying name or address.

MSCS stands for Microsoft® Cluster Service.

- Microsoft Cluster Service (MSCS) is composed of three key components:
- The **Cluster Service** that controls cluster activities, by periodically calling resource DLLs to check if the resource is still alive.
- The **Resource Monitor** that is an interface between the Cluster Service and the cluster resources.
- **Resource and Cluster Administrator extension DLLs** that are used by the Resource Monitor to check the status of the resource and to bring resources online and offline.



For more information on Microsoft® Cluster Service, refer to `http://www.microsoft.com/windowsserver2003/technologies/clustering/default.mspx`

Tun Cluster Model

Tun cluster model provides high availability and performance. In a Tun cluster, Tun is installed on every node and a shared SCSI disk is used to store:

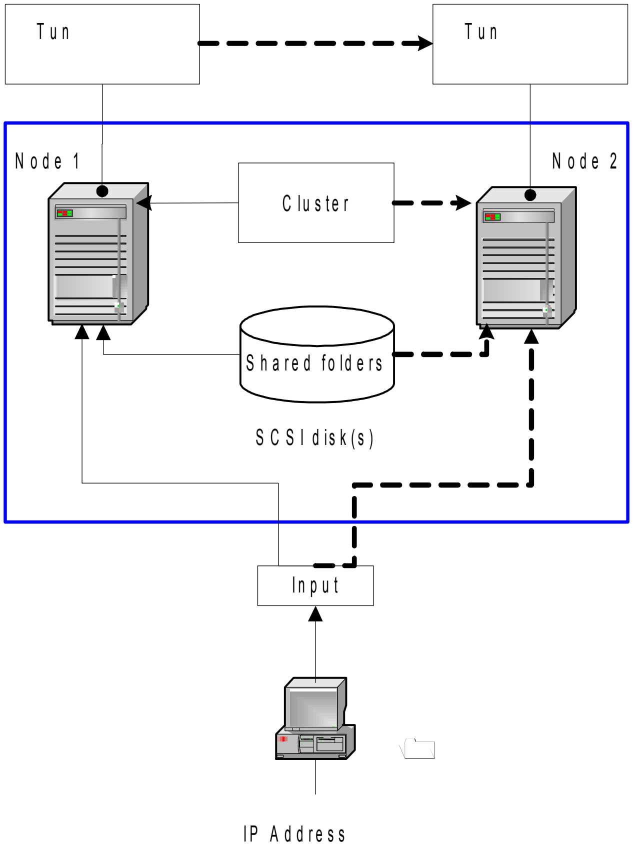
- HTML pages and active components (ActiveX and Java classes)
- LDAP
- SSL Proxy files

Each node has a preferred set of resources to handle. One of the nodes makes its set of resources available to the network in the form of a virtual server, which can be detected and accessed by clients, while the other nodes are used as “rescuing” servers in case of failure.

One node processing operating mode

Tun processes run in a “one node processing mode”. This means that only one node handles Tun processes at a time. The other nodes remain available to take over the processes each time the node currently handling them fails.

The following figure illustrates the one node processing mode:



Clients access the cluster server via the Tun cluster IP address and network name. One Tun application treats all clients input requests, and the same Tun application on the other node(s) is just used in case of failover.

Microsoft Cluster Service (MSCS) Installation

Tun uses Microsoft® Cluster Service (MSCS) to deliver higher levels of service and availability.

MSCS allows multiple Microsoft Windows NT® operating system-based servers to be connected together, making them appear to network clients as a single, highly available system providing failover support.

For more information on Microsoft® Cluster Service, refer to
`http://www.microsoft.com/windowsserver2003/technologies/clustering/default.mspx`

MSCS handles Tun as three types of logical entities:

- The service executables
- The datafiles and components stored on the shared SCSI disk.
- The virtual server that hides both nodes behind a single IP address and network share.

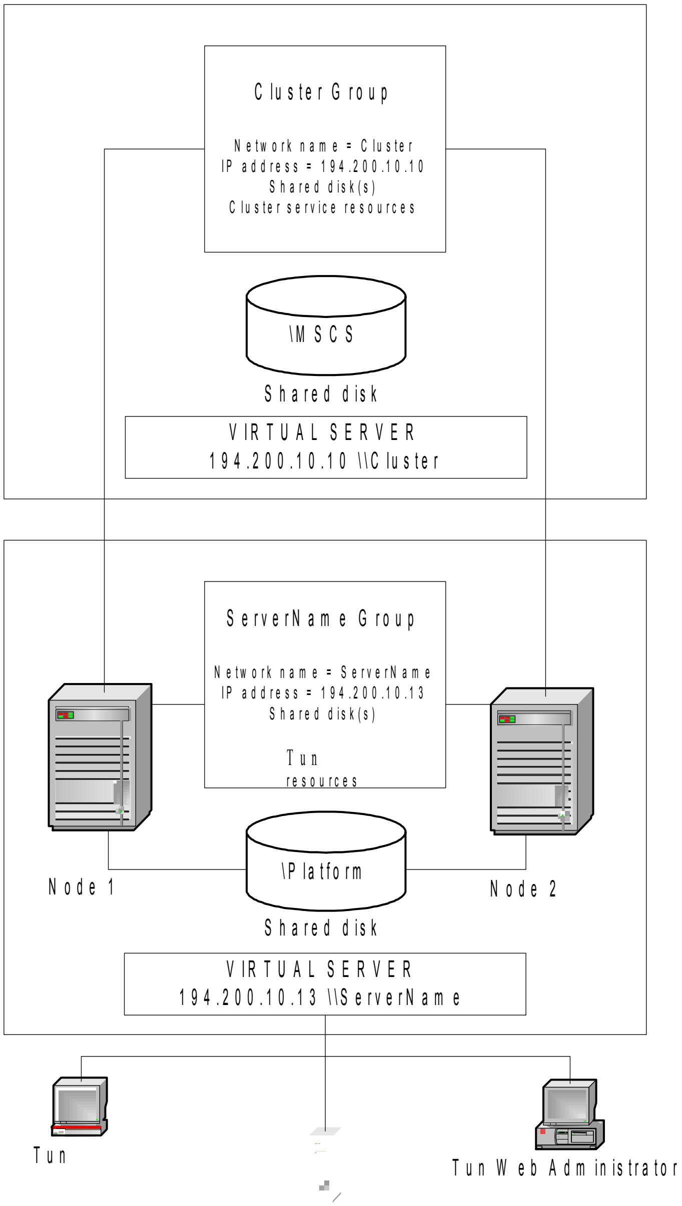
Tun Cluster system requirements

Before installing Tun in a Cluster, you must first meet the following requirements:

- 2-node hardware cluster with RAID-5 disk array
- Server nodes are running Windows Server 2003 Enterprise edition, including latest security updates, and IIS v6.0 is installed.
- Cluster Service is configured and operational on each node.
- Active/Passive configuration will be used

A cluster configuration is composed of two or more servers, storage, and networking.

The following figure shows a Tun cluster composed of two servers:



The operating system of each server can be Windows Server 2003 Enterprise Edition installed on your computer, with Cluster Service and with Microsoft Internet Explorer 6.0 or later.

Here are some important elements you should remember when installing a cluster on which you will install Tun:

- Each server needs to be attached to a shared, external SCSI bus that is separate from the system disk bus. Data that will migrate between the nodes is stored on one or more shared disks attached to this bus.

- Each server needs at least two network cards. Typically, one card is used for public/corporate network communications, and the other is used for private network communications between the cluster nodes.
- End-user clients have access to all the cluster resources, such as shared disks, file shares, and applications without having to know the names of the individual servers in the cluster.
- Ensure that each node meets the Tun system minimum requirements as listed in the Tun *Installation Guide*.
- Your cluster system should be as homogeneous as possible since you will perform a similar Tun installation on all nodes.

Important: When installing Tun on the cluster, you must install Tun Plus on ALL cluster nodes (first node and secondary nodes). If the node that owns the Tun Plus resource fails, the Cluster Service randomly selects another cluster node, to which it fails over Tun Plus's activity.

Installing Microsoft Cluster Service

1. Install Microsoft Cluster Service on all nodes to set them up as cluster nodes.
2. Create at least one cluster group with an associated physical SCSI disk resource.

Note: In your cluster configuration, we recommend that you have separate groups for the cluster and for clustered applications like Tun.

For more information on Microsoft® Cluster Service, refer to
`http://www.microsoft.com/windowsserver2003/technologies/clustering/default.mspx`

Installing Tun in a clustering environment

Before installing Tun in a cluster, you need to understand the basic concepts of Clustering and Server Administration and you should have already set up a Cluster Group in the Cluster Administrator as described in the previous pages.

Before installing Tun in a Clustering environment

1. Log on to the first node of the cluster you are going to set up with Tun.
2. Launch Cluster Administrator.
3. Create a resource group for Tun under groups by right-clicking Groups and selecting New>Group.
4. Provide a Name and click Next.
5. Select the available nodes (from what you set before in Cluster Administrator--refer to the previous section) and click Add and then Finish.
6. Create resources for the new group by right-clicking the group's name and selecting New>Resource.
   a. Create the shared SCSI disk resource.
   b. Create the cluster IP Address and Network Name resources: These resources will be used by clients connecting to the Tun cluster; they define the Tun cluster virtual server.
   c. Bring the resources for the shared SCSI disk, the virtual IP address, and the virtual network name online singly or as a group.

Note:
Do not add service resources to the Tun group until after Tun is installed.

At this point, you'll need to install Tun before continuing with cluster configuration.

Install Tun on the First Node

The next step is to launch the Tun installation program on the first node.

Note:
It is very important that you should not have any Tun components on the node before installation. Verify the Esker folder on the shared SCSI disk is empty. If at any time during the installation, a screen appears asking you if you wish to upgrade, cancel setup and uninstall Tun from the node. Once the machine is free from any Tun components, re-launch the installation program.

1. Insert the Tun CD-ROM in the first node's CD-ROM drive. The Autorun program starts automatically.
2. Proceed with installation normally until reaching the Choose Destination Directories screen. On this screen, change the default drive letter for the Tun PLUS Destination Directory and the HTML pages and components to the drive letter assigned to the shared SCSI disk, and proceed.
3. On the Server Information screen, enter either the virtual IP address or the virtual network name instead of the IP address or host name of the node.
4. On the last installation screen, deselect Start LDAP Server now, and Finish installation.

Set the Service to Manual

Launch the Services MMC and change the Esker LDAP Server Service to Manual start. Do not start the service.

Complete Tun configuration on the first node

After installing Tun on the first node, relaunch the Cluster Administrator to create resource types for the services.

1. Launch the Cluster Administrator.
2. Create a generic service resource for the Esker LDAP Service. The service name is SLAPD. Specify dependencies including the shared SCSI disk and the virtual IP address.
3. Create a generic service resource for the World Wide Web Service. The service name is W3SVC. Specify dependencies including the shared SCSI disk, the virtual IP address, and the Esker LDAP service.
4. If the SSL component is to be installed, create a generic service resource for the Esker SSL Server Connector. The service name is EskerSSL. Specify dependencies including the shared SCSI disk, the virtual IP address, and the Esker LDAP service.
5. Bring the entire Tun resource group online.
6. Launch the Internet Information Services (IIS) Manager. Right-click the Default Web Site and select New Virtual Directory from the context menu.
7. Name the new virtual directory “wwwEsker” and make it point to the directory of the same name installed on the shared SCSI disk. The access permissions for the virtual directory should be set to “Read.”
8. Test connections to the server using the virtual IP address and virtual network name before proceeding.

Tun cluster installation and configuration on subsequent nodes

1. Log on to the next node where Tun is to be installed and launch the Cluster Administrator.
2. Take the entire Tun resource group offline.
3. Move the Tun resource group to the secondary node.
4. Bring the resources for the shared SCSI disk, the virtual IP address, and the virtual network name online.
5. On the server, navigate to the shared SCSI disk and delete all of the Tun folders and components that were installed during setup of the first node.

6. Install Tun on the second node using all the same options chosen when installing it on the first node.
7. Launch the Services MMC and change the Esker LDAP Server Service to Manual start. Do not start the service here.
8. Launch the Cluster Administrator and bring the entire Tun resource group online.
9. Launch the Internet Information Services (IIS) Manager. Right-click on Default Web Site and select New Virtual Directory from the context menu. Name the new virtual directory 'wwwEsker' and make it point to the directory of the same name installed on the shared SCSI disk. The access permissions for the virtual directory should be 'Read'.
10. Test connections to the server using the virtual IP address and virtual network name.

Uninstalling Tun from a cluster

This section describes how to uninstall Tun from all cluster nodes.

Note:
Uninstalling Tun from the cluster does not delete what is under \wwwEsker or \LDAP Server on the shared disk so that you do not lose your data files and configurations. If you wish to delete these, they must be deleted manually after running the uninstaller.

1. Move the Tun resource group to the node from which you wish to uninstall Tun.
2. Take the Tun resource group offline. This will prevent failover at the end of uninstall when the server reboots.
3. If SSL was installed, bring the shared SCSI disk resource back online so that the uninstaller is able to locate the SSL proxy files.
4. Run the uninstaller from Control Panel > Add or Remove Programs to uninstall Tun from the server.
5. Repeat these procedures for each node from which Tun is to be uninstalled.

Administrating Tun Cluster Groups

Administrating the Tun cluster groups means handling cluster resources.

This section describes the resource groups and resources that you are to handle with Tun Cluster, and it explains how you can manage these groups and resources using the Cluster Administrator.

Tun cluster resource groups and resources

The Tun cluster relies on the following groups:

- One group for Tun Plus (for example, "Esker Group") containing:

  - Resources defining the cluster virtual server (Physical Disk, IP Address, Network Name)

  - "Generic Service" type resources for all Tun services that run in one node processing mode (Esker LDAP service, Esker SSL Connector service, and the World Wide Web service)

Managing cluster nodes, groups, and resources

This section describes some actions you may want/need to perform on resources, resource groups, and cluster nodes.

The Cluster Administrator was installed when you installed the Cluster Service. It is a cluster management application that allows you to configure, control, and monitor clusters.

You can use the Cluster Administrator to manage the Tun cluster objects, establish groups, initiate failover, handle maintenance, and monitor the cluster activity.

For more information on Microsoft® Cluster Service, refer to
`http://www.microsoft.com/windowsserver2003/technologies/clustering/default.mspx`

Identifying failovers

Failover within the Tun cluster can occur when an entire node in the Tun cluster fails.

It is important to use Cluster Administrator to routinely monitor the status of the Tun cluster and check for failover activities that diminish either the performance or the availability of Tun resources.

Failover within the Tun cluster should be easily tolerated. Your workflow should not suffer if all Tun applications are working, and you have provided sufficient capacity for all situations.

Serious failover situations can affect performance and availability.

If a node fails and no other node is able to serve clients efficiently, the situation must be resolved immediately.

Important: Remember that you must have installed Tun on ALL cluster nodes for failover support. In case of failure, if the Cluster Service cannot fail over Tun’s activity to the node it has randomly selected, it deletes all incoming network requests until the failed application is brought back online.

If groups persistently fail over and fail back without surviving on either node for very long, availability to clients is completely lost.

Failover will not occur if the failure is in Tun’s application or Tun’s services.

Handling Tun cluster’s resources

All Tun cluster’s resources should always be online, which means, available to the cluster. However you may need to manually activate or deactivate online Tun Service resources (for example, if you want to force the cluster to use a particular node for support of a given service). For this, you use the Cluster Administrator.

Handling Tun cluster’s resource groups

Actions you may need to perform on Tun cluster’s resource groups from Cluster Administrator include:

- Assigning a preferred owner to the “Esker Group”
- Configuring automatic failback for the ‘Esker Group’
- Moving a resource group from one node to another (for maintenance)
- Taking a resource group offline (for maintenance)

See the instructions below for more information.

Assigning a preferred owner to the “Esker Group”

Assigning a preferred owner to a cluster resource group means forcing the cluster to failback the group to a specific node after a failover.

By default, no preferred node is assigned to the "Esker Group". If your cluster system is heterogeneous, it may be adviseable to set the most powerful machine as preferred owner for the "Esker Group".

To assign a preferred node to the "Esker Group":

1. From Cluster Administrator’s left pane, right-click the "Esker Group", and select Properties.
2. In the dialog box that appears, click the Modify button.
3. In the Modify Preferred Owners dialog box, place the cluster node(s) you want to set as preferred owner(s) for the "Esker Group" in the right pane.
4. Click OK.
5. On the initial dialog box, click Apply, and OK.

6. Now that you have specified a preferred owner for the "Esker Group", configure automatic failback for this group by following the next procedure.

Configuring automatic failback for the “Esker Group”

This step is associated to the definition of a preferred owner for the "Esker Group". The objective is to force the cluster to restore the "Esker Group" to the specified preferred owner either immediately or between a given time interval after the failed node is brought back online.

1. From Cluster Administrator’s left pane, right-click the “Esker Group” and select Properties.
2. On the Failback tab, select Allow failback and configure the failback time as needed.

Moving a resource group from one node to another

If you need to perform some maintenance that requires reboot on one of the cluster nodes (for example, installing or upgrading an anti-virus software), you should first force the resource group(s) owned by this node to move to another node. Thus you ensure that the reboot will not affect the Cluster Service. For this, follow the procedure below.

1. From the Cluster Administrator’s left pane, right-click the group and select Move Group.

   As a result, the Cluster Service takes the group offline, then it moves it, and it takes the group online again on the other node.

   If your cluster contains two nodes, the group switches to the other node.

   If your cluster contains more than two nodes, the group switches to its preferred owner (if different from the original owner), or it switches to the first node available.
2. When your maintenance is finished, move the group back to its original owner.

Taking a resource group offline

When you have to perform maintenance on one of the cluster nodes, another solution is to take the group(s) owned by the node offline. Thus the cluster does not monitor the group(s) any longer and the node's maintenance cannot affect the Cluster Service in any way.

Notes:
This solution is more drastic than group moving. We recommend that you move resource groups rather than to take them offline.

Taking the "Esker Group" offline stops all activities of the Tun cluster!

1. To take a group offline, from Cluster Administrator’s left pane, right-click the cluster group and select Take Offline.
2. To bring the group back online when your maintenance is finished, right-click it again and select Bring online.

Handling Tun cluster nodes

The Cluster Administrator allows you to perform different actions on cluster nodes. These include the possibility to stop all resources owned by a node simultaneously.

Stopping all resources of a node simultaneously

From the Cluster Administrator, right-click the node and select Stop Cluster Service.

As a result, the Cluster Service does not monitor the node any longer; all dependent resources are brought offline.

For more information on Microsoft® Cluster Service, refer to
`http://www.microsoft.com/windowsserver2003/technologies/clustering/default.mspx`

Appendix: Clustering Glossary

active A node that is running and participating in cluster operations.

failback Process of moving a group back to its preferred node when the node becomes active after a failure.

failed Describes a node or resource that has ceased operating and is unavailable to the cluster. Node or resource failure can trigger failover.

failover Process of moving a group to another node in response to a node or resource failure.

group A collection of resources managed as a single cluster object. Typically a group contains all of the resources needed to run a specific application or service.

high availability Refers to the ability to provide end-user access to a service a high percentage of scheduled time while attempting to reduce unscheduled outages.

high reliability Refers to the ability to reduce the frequency of system failure, while attempting to provide fault tolerance in case of failure. A solution is highly reliable if it minimizes the number of single points of failure and reduces the risk that failure of a single component/system will result in the outage of the entire service offering.

high scalability Refers to the ability to add resources and computers while attempting to improve performance. A solution is highly scalable if it can be scaled up and out. Individual systems in a service offering can be scaled up by adding more resources (for example, CPUs, memory, disks). The service can be scaled out by adding additional computers.

inactive A node that is running but not participating in cluster operations.

node A Microsoft Windows NT Server/Windows 2000 system that is an active or inactive member of a server cluster.

offline A state describing a resource or group as unavailable to the cluster.

online A state describing a resource or group as available to the cluster.

quorum resource The quorum-capable resource selected to maintain essential cluster data. The quorum resource stores a synchronized version of the cluster database as well as critical recovery information in a recovery log. The quorum resource guarantees that all nodes have access to the most recent database changes.

resource A physical or logical entity that is capable of being owned by a node, brought online and taken offline, moved between nodes, and managed as a cluster object. A resource can be owned by only a single node at any point in time. A resource is an instance of a resource type.

resource type A cluster object used to categorize and manage resources sharing similar characteristics. A resource type is implemented in a resource DLL that manages all the resources of that type in the cluster.

virtual server A group containing a Network Name resource, an IP address resource, and additional resources necessary to run one or more applications or services. Clients can use the network name to access the resources in the group, analogous to using a computer name to access the services on a physical server. However, because a virtual server is a group, it can be failed over to another node without affecting the underlying name or address.

Macro Principles

Tun Plus includes a high-level script-language (EScript) which serves to create scripts that replace the keyboard and totally or temporarily control an emulation session. You can call such a script when you start the emulator, and/or when you exit emulation.

For example, you can use EScript to:

- Send a character string over the connection.
- Wait for a particular character string from the host within a specified time.
- Wait for a period of time expressed in seconds.
- Retries.
- Test return codes of certain instructions.
- Test characters received.
- End an emulation session.
- Return to an emulation session.
- Show or hide characters sent by the host.
- Prompt the user to enter information.
- Handle variables.

Syntax

You can create macros with an ordinary text editor. You don't have to compile them since they're directly interpreted by Tun Plus.

One of the most common ways to use macros is to associate with the session start and end macros, used respectively when you connect and disconnect the session.

Sample macro

The following script example automates logon to a server and launches a Unix application (scoadmin).

```
Module scoadmin
# Variable used to store the number of the matched
# string:
Dim Matched as Int

# Characters sent by Host computer not displayed:
Dialog.SetTitle("SCOADMIN")
SetDisplayOff()

# Start:
Label BEGIN

# Read login and password: Dim USER as String

Dim PASSWD as String
USER = Dialog.Read("Enter your user name: ")
PASSWD = Dialog.ReadPasswd("Enter your password: ")
```

```
# Make connection:
Repeat 3
          # Send carriage-return character:
          Repeat 5
          SendString("\n")
          If Receive(1000,"ogin") > 0 Then Break Endif
EndRepeat
If Error() Then Goto NOCONNECTION Endif

# Send login:
SendString(USER + "\n")
Matched = Receive(15000,"assword","# ","$ ")
If Error() Then continue Endif
If Matched >=  2 Then Break Endif    # "#" or "$" matched
SendString(PASSWD + "\n")
Receive(15000, "$ ", "# ", "ogin:", "TERM =")
If Error() Then Continue Endif
If StringFound() = "# " Then Break Endif
If StringFound() = "$ " Then Break Endif
# Return to start of program if login incorrect:
If StringFound() = "ogin:" Then Goto BEGIN Endif

          # Set the TERM variable if necessary:
          SendString("\n")
          If Receive(15000,"# ", "$ ")>0
                Then Break
                Else Continue
          Endif
EndRepeat

# Start application:
SendString("scoadmin\n")
# Display received characters:
SetDisplay()
# Return to the emulator:
Return

# No login:
Label NOCONNECTION
Dim ANSWER
ANSWER = MsgBox("Communication failed\nDo you want to quit Emul?","SCOADMIN",4)
If ANSWER = 6
          Then  exit   # Exit the emulator
Endif
CloseSession
```

The same type of program can be designed to establish more complex connections, such as sending modem commands, connecting through an X.25PAD, navigating within a Unix application, etc.

The preceding model can also be used to run Unix applications other than "scoadmin". For example, you can replace the line SendString("scoadmin\n") by a SendString method using another Unix command or shell script as parameter.

Language syntax

An EScript macro must always begin with the word "module" followed by the macro's name.

The macro can then contain the following elements:

- Control structures : loops with stop and continue conditions, conditional blocked instructions, jumps from one place in a script to another.
- Variables of the following types: integer (Int) or character string (String).
- Macro parameters (used when you specify start and end macros from the emulator).

- Comparison, arithmetical and boolean operators.
- Predifined functions and methods.

Notes:
In this manual, instruction names are combinations of upper- and lowercase letters: This is only to simplify reading. It's of no importance with respect to programming, and either upper- or lowercase letters can be used to write instructions (for example, "*SendAndReceive* can be written "*SENDANDRECEIVE*" or "*sendandreceive*").

If the first character of a line is "#", the entire line is treated as a comment.

EScript functions

Chr	(language)	Returns the character associated with a given character code.
Error	(language)	Returns the number of the last error encountered.
Str	(language)	Changes a number to a character string.
Val	(language)	Returns the first number encountered in a character string.
Connected	3270, 5250, Unix	Returns a boolean value indicating if the terminal is connected or not.
Convert	Unix	Converts the specified string to the host character set.
Decrypt	Unix	Decrypts a character string.
Dialog.Read	3270, 5250, Unix	Lets the user enter a string in a dialog box.
Dialog.ReadPasswd	3270, 5250, Unix	Lets the user enter a password in a dialog box.
LicenseString	Unix	Retrieves the application's license string.
MsgBox	3270, 5250, Unix	Displays a message dialog box. Returns the clicked button.
ProductNumber	Unix	Retrieves the application's product number.
Receive	Unix	Waits to receive one or more strings.
SearchString	3270, 5250, Unix	Searches a character string on the screen.
SearchStringInRect	3270, 5250, Unix	Searches for a string of characters in a rectangular area of the screen.
SerialNumber	Unix	Retrieves the application's serial number.
StringFound	Unix	Returns the last string received by the Receive command.

EScript methods

ChangeKey	3270, 5250	Attributes a new string of characters, a macro or a function to a key.
ClosePanel	3270, 5250	Unloads the current function-key panel.
CloseSession	3270, 5250, Unix	Closes the current session.
Connect	3270, 5250	Connects to a server.
CopyClipboard	3270, 5250	Defines a screen area and copies the contents to the clipboard.
Dialog.Clear	3270, 5250, Unix	Clears messages contained in a dialog box.
Dialog.Hide	3270, 5250, Unix	Prevents dialog from being displayed.
Dialog.Message	3270, 5250, Unix	Displays character strings in a dialog box.
Dialog.SetButtons	3270, 5250, Unix	Displays/hides the cancel button in a dialog box.
Dialog.SetTitle	3270, 5250, Unix	Assigns a title to a dialog box.
Dialog.Show	3270, 5250, Unix	Displays the dialog field.
Disconnect	3270, 5250	Disconnects from a server previously connected.
DisplayAVI	3270, 5250	Clears the screen and displays an AVI file (only under 32-bits windows).

DisplayMessage	3270, 5250	Clears the screen and displays a message on the emulator screen.
ExecDosProg	3270, 5250	Executes an MS-DOS command.
Exit	3270, 5250, Unix	Unconditional exit from a macro and also the emulator.
ExitIfDisconnect	3270, 5250, Unix	Triggers an exit from emulation if disconnection is detected.
HidePanel	3270, 5250	Hides the current function-key panel.
HideScreen	3270, 5250	Hides the display of the characters received by the emulator.
LoadCharset	3270, 5250	Loads a charset file.
LoadKeyboard	3270, 5250	Loads a keyboard file.
Modem.Dial	Unix	Dials a telephone number on a Hayes-compatible modem.
Modem.Hangup	Unix	Ends modem communication.
MoveCursor	3270, 5250	Moves a cursor to a position.
MoveCursorToString	3270, 5250	Moves the cursor to the last position found.
MsgBox	3270, 5250, Unix	Displays a message dialog box.
OpenPanel	3270, 5250	Loads a function-key panel.
PrintScreen	3270, 5250	Prints the screen.
PrintTemplate	3270, 5250	Prints using a template.
Receive	Unix	Waits until a string is received.
ReceiveFile	3270	Receives a file from the remote server.
ResizeSession	3270, 5250, Unix	Sets a value indicating the visual state of the session window.
RestoreBackground	3270, 5250	Restores the normal screen background if it has been changed with the command SetBackgroundBitmap.
SendCryptedString	3270, 5250, Unix	Sends a crypted character string over the communication channel
SendFile	3270	Sends a local file to the remote server.
SendFunKey	3270, 5250	Sends a function key code to the remote server.
SendString	3270, 5250, Unix	Sends a character string over the communication channel.
SetBackgroundBitmap	3270, 5250	Loads a bitmap file.
SetHelpFile	Unix	Specifies the help file to use.
SetPanelText	3270, 5250	Changes the text linked to the current function-key panel.
SetSessionTitle	3270, 5250, Unix	Assigns a name to the emulation session.
ShowPanel	3270, 5250	Displays a function-key panel previously opened.
ShowScreen	3270, 5250	Displays the characters received by the emulator again.
Sleep	3270, 5250, Unix	Wait a specified period of time (in milliseconds).
Wait	3270, 5250	Puts the system on hold until the end of a timeout.
WaitCursor	3270, 5250	Waits for the cursor to be placed in a certain position.

For asynchronous emulation, you have to add other methods to this list. A description of these methods is given in EScript.hlp (English only) available on the CD in \Pc2host\Win_32\DOCS\MISC.

9

Advanced Use of Asynchronous Emulator

Tun's asynchronous emulator lets you define and customize every aspect of an emulation session, including keyboards, escape sequences, and character tables.

The emulation parameters are grouped together in an entity called the terminal. Each type of terminal (file .ter) is associated with various files containing the information necessary for communications between the PC and the server: keyboard file .key, function keys file .fun, escape sequences file .seq, and so on.

Data from the PC to the server goes through the following filters. The filters perform different operations on the data depending on the type of data and the filter settings.

- Keyboard filter (for .key files): each code sent from the keyboard (each key is identified by a code known as the scan code) refers to a piece of information. This information can be:

  A character (or a string of characters) to send.

  A script or a macro of type .mac to be executed.

  A function key (link with the function keys file .fun).

  A mnemonic for which the various lists can be found in the Using the emulators chapter, Keyboard customization, Asynchronous Emulation section. If the mnemonic is "nat", this means that you should refer to a specific national feature (national file .nat).

- Function-key filter (.fun file): Each function-key is assigned a value.
- Code conversion filter (.snd file): Converts ASCII files in some types of emulation.
- National filter (file .nat): the scan code sent by the keyboard can be re-routed by the .key file to a value of the .nat file specific to the language used.

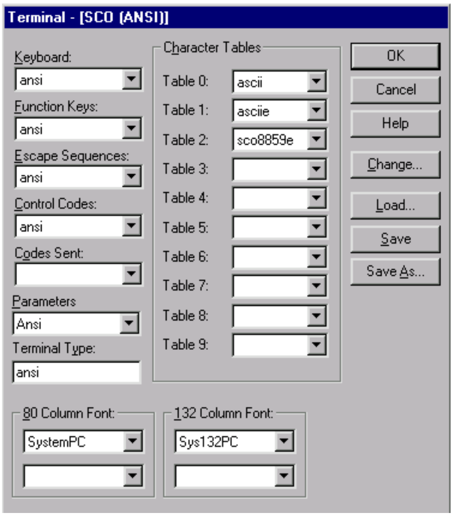
In the next stage, the data reaches the host. The host processes the data and sends a reply to the PC. The reply is also filtered:

- Escape sequence filter (for .seq files): The emulator processes the escape sequences sent by the Unix host and links them to one or more actions (clear the screen, move the cursor, start an application, etc.).
- Control code filter (for .cod files): When the host sends special characters known as control codes (the decimal values 0 through 31 and 128 through 159), Tun Plus looks up the actions mapped to the characters in a table).
- Character table filter (for .tab files): Displays the characters correctly on the screen. It ensures Unix host codes are correctly interpreted by the emulator.).

You can modify the .key, .fun and .seq files for particular sessions. You seldom need to modify the .nat, .snd, .cod and .tab files.

All the configuration files are text files which can be opened in a Notepad-type utility and then modified.

You can however access these files and configure them using the configuration window of the terminal settings. This window is accessible from the Administrator tool, when you choose Properties in the Terminal context menu in an asynch session. The following window opens:



Terminal - [SCO (ANSI)]

Keyboard: ansi
Function Keys: ansi
Escape Sequences: ansi
Control Codes: ansi
Codes Sent:
Parameters: Ansi
Terminal Type: ansi

Character Tables
Table 0: ascii
Table 1: asciie
Table 2: sco8859e
Table 3:
Table 4:
Table 5:
Table 6:
Table 7:
Table 8:
Table 9:

80 Column Font: SystemPC
132 Column Font: Sys132PC

The corresponding filename of the terminal type for the current session appears in the dialog's title bar. All displayed files correspond to the parameters associated with this type of terminal (for example: keyboard file ansi.key, function keys file ansi.fun).

To load another terminal type, click Load and select a .ter extension file.

Files in any field can be edited from this dialog by selecting them and clicking Modify. For a .key file (Keyboard field), a model of the keyboard appears. For all other file types, the file opens in Notepad.

Escape sequences

The asynchronous emulator uses ".seq" files to interpret the flow of data from the host machine. The ".seq" files associate one or more actions (cursor movement, clear screen...) with the reception of character strings (typically called escape sequences).

Opening an existing .seq file from the Administrator reference directory

A .seq file is a text file that can be read by any text editor. The escape sequence files supplied by Tun can be found in the Tools\Applications Access\Unix Emulations\Specific Data\Escape Sequences directory of the resources tree. To edit a .seq file, select Properties from its context menu.

Opening an existing .seq file from a session in the Administrator

Select the Properties option in the context menu of the Terminal element of a session.

Click on the .seq file chosen from the drop-down menu of Escape sequences then click on the Modify button. The .seq file opens in the default test editor.

Content of an escape sequences file

A .ses escape sequences file comprises three separate parts:

- Terminal initialization, which enables the terminal to be set to the initial status needed for establishing communication between the server and the terminal. This part can be described in the first line(s) of the file.
- The escape sequences header, when common to all the sequences (optional part).
- Definition of the escape sequences.

Here, for example, is an extract from file vt52.seq:

```
195(2)
\033
H s 92
A s 93
B s 94
C s 95
D s 96
Y%p0%{32}%-%c%p1%{32}%-%c p 91
I s 112
J s 49
K s 52
F s 211
```

Escape sequence files may need editing in the following cases:

- If the current initialization strings are not appropriate.
- If the action associated with an escape sequence is not appropriate.
- If you want to add escape sequences for particular actions.

Syntax

The escape sequences and the initialization strings are described by actions specific to the Tun asynchronous emulator. Each action is identified by its number or label and its parameters, if any. The list of asynchronous emulator actions is given in the Escript.hlp file, copied into the installation directory.

Note:
If an emulation session has been customized or newly defined, the File Reception feature (with <Alt><F8> and <Alt><F9>) will help you to capture and analyze escape sequences and display characters sent by the host (using a Debug utility).

Terminal initialization

The first line of an escape sequence file contains the list of actions necessary for the terminal to function properly. You can add or replace actions according to your needs (see following paragraphs for information on obtaining online help with escape sequences).

The Initialization line contains different actions separated by spaces. Parametered actions must be written with the appropriate parameters enclosed in parentheses and separated by commas. If there are a lot of actions, you can divide the initialization sequence into several lines, terminating each line, except the last one, with the backslash character \ (for example, the 2nd line in the file wyse60.seq).

Here, for example, is an initialization line:

```
195(0)1195(0) 196(2) 197(2) 216
```

or with the actions label:

```
TabAsG1(0) TabAsG2(2) TabAsG3(2) G2IntoGR
```

These actions are defined as follows:

Action	Description
195(0)	Assignment of character table 0 as G1
196(2)	Assignment of character table 2 as G2
197(2)	Assignment of character table 2 as G3
216	Lock G2 in GR

Sequence headers

If all the sequences in an emulation begin with the same characters, it's best to enter them on the second line of the ".seq" file. This line serves as a header for every line that follows, and allows the emulator to treat sequences sent by the server more rapidly. The escape character (\033) is very often used a header.

If you don't use a Sequence Header, you must leave the second line blank.

Defining escape sequences

The remaining fields define the actions that are related to a particular sequence. There are two types of sequences:

- Simple sequences that don't change.
- Parametered sequences that may vary.

Simple sequences

A simple sequence is a character string that doesn't contain a variable zone, and may be directly associated with one or more actions.

For example, here's a string of three characters that move the cursor one position to the left:

```
\E[D s 96
```

or with the actions label:

```
\E[D s MoveCursorLeft
```

Parametered sequences

A parametered sequence is composed of a succession of strings beginning with the character %, which serves to identify the presence of a variable. A sequence can contain several parameters, defined in three parts:

- Definition of the parameters themselves.
- Calculations and controls to be carried out on the parameter.
- Parameter format.

Parametered actions

In the case of a parametered action, there are two possibilities:

- The escape sequence is simple: the action parameters are constants.

  Example:

  ```
  c s 270("vt100")
  ```

  (or `c s ChangeTerminal("vt100")`)

  Escape sequence \033c executes the 270 ChangeTerminal action (dynamic terminal change) whose parameter value is vt100.
- The escape sequence is parametered: the parameters are in the order expected by the action, which then recovers the values taken from the sequence.

  Example:

  ```
  Y%p0%{32}%-%c%p1%{32}%-%c p 91
  ```

  (or `Y%p0%{32}%-%c%p1%{32}%-%c p MoveCursor)`

  Escape sequence \033Y executes the 91 MoveCursor action by recovering the values of two parameters (p0 for columns and p1 for rows).

In addition, after the action retrieves the parameter value, operations can be performed on this parameter before it is used by the action.

Example:

```
31(-30)[30,37]
```

- Check whether parameter value is between 30 and 37. If not, the action will not be carried out.
- Subtract 30 from the parameter value before it is used by the action.

Defining parameters

Note:
In the following notations, [ ] indicates an optional range.

Parameter definition uses the following syntax:

- %[?value by default]p[0-9] Allocation of a parameter
- *Example* %?1p2 Third parameter with a default value = 1
- %[?value by default]pi Allocation of several parameters
- *Example* %?1pi
- %g[a-z] Allocation of a variable
- *Example* %gh Allocation of the variable h

Calculations and controls

In conventional mathematic notation, the operands are separated by the operators and a particular significance forced by using parentheses. In RPN, the operands and operators are simply stacked and ‘popped’ and ‘pushed’ accordingly.

Operator	Function	Example
%[min,max]	Checks the contents in the range	%[0x40,0x7f] The variable must be between 0x40 and 0x7f
%'c'	Stacks a constant	%'b'
%"string"	Push the string *string* on the string stack	%"green"
%{nn}	Stacks a decimal constant	%{64}
%g[a-z]	Pops a variable off the stack	%gh
%P[a-z]	Stacks a variable	%Ph
%V	Push the vertical position of the cursor on to the integer stack	
%H	Push the horizontal position of the cursor onto the integer stack	
%+	Add	
%-	Subtract	
%*	Multiply	
%/	Divide	
%m	Modulo (remainder)	
%&	Bitwise AND	
%|	Bitwise OR	
%^	Bitwise Exlusive OR	
%=	Equality	
%>	Greater than	

Operator	Function	Example
%<	Less than	
%A	Logical AND	
%O	Logical OR	
%!	Logical NOT	
%~	Bitwise NOT	
%I	Bitwise Inverse	(01100010 becomes 01000110)

Parameter format

This is shown as follows:

%c	Single character
%s	Character string delimited by " or "
%S(string)	Character string ending by string. string isn't stacked, and must be less than 10 characters. The decimal, hexadecimal and octal notations must begin with the character \\. The character) mustn't be used within string, and must be coded \0x29. Note: %S() represents a character string ended by the first received character.

% [[:]flag] [dim[.precision]][type]	
flag	Can have the values - + or #
-	The result is centered to the left
+	The result always includes the sign + or -
Blank	If the first character of a conversion with a sign does not have a sign, a space precedes the result. This implies that if the flags **blank** and **+** are listed, the blank flag isn't taken into account.
#	This flag means that the value has to be converted to a format depending upon the type of the corresponding argument. This flag has no effect on the type d. In the case of a conversion of type o, it raises the precision in such a way as to force the first digit of the result to 0. In the case of a conversion of type x or X, a result other than zero is prefixed as 0x or 0X.
dim	Gives the minimum number of characters occurring in the parameter. If this dimension begins with '0', the number is padded on the left by zeros and not blanks.
precision	Indicates the required number of digits (and not characters) corresponding to the parameter.
type	Can have the following values: d, o, x or X.
d	A signed decimal is converted into a integer
o	An octal notation is converted into an integer
x	A non-signed hexadecimal is converted into an integer (use the lowercase letters a, b, c, d, e and f).
X	A non-signed hexadecimal is converted into an integer (use the uppercase letters A, B, C, D, E and F).

Example: setting the mouse for ansi emulation

```
\033Mm%p0%d;%p1%dX
```

There are two parameters in this sequence:

- %p0%d : first parameter
- %p1%dX : second parameter

These parameters are a succession of digits indicating an integer (d).

Example: reassignment of a keyboard key for ansi emulation

```
\033Q%p0%[0,9]%{59}%+%d%p1%S()
```

There are two parameters in this sequence:

- `%p0%[0,9]%{59}%+%d` : first parameter
- `%p1%S()` : second parameter

The first parameter is an integer expressed in decimal format, while the second is a character string bounded by the first character received.

For the first parameter, the following processing is required:

%[0,9]	Controls that the character is in the range of decimal values 0 through 9
%{64}	Stacks the value 59
%+	Addition in Reverse Polish Notation: (car59+) is equivalent to (car+59)

Function keys

The emulator uses the .fun files to define each of the function keys used by an emulation.

▸ Opening an existing .fun file from the Administrator reference directory

A .fun file is a text file that can be read by a Notepad-type text editor. You can therefore open a .fun file from this type of editor. The function key files supplied by Tun can be found in the Tools\Applications Access\Unix Emulations\Specific Data\Function keys directory of the resources tree. To edit a .fun file, select Properties in its context menu.

▸ Opening an existing .fun from an session in the Administrator

Select the Properties option in the context menu of the Terminal element of an session.

Click on the .fun file chosen from the Function keys drop-down menu and then click on the Modify button. The .fun file opens in the default text editor.

Content of a function keys file

A .fun function keys file associates each function key on the terminal with the character string to be sent when it is struck.

Here, for example, is an extract from file vt100.fun:

```
[fKeyActions]
fKey1=\033OP
fKey2=\033OQ
fKey3=\033OR
fKey4=\033OS
fKey5=brk
fKey6=\033[17~
fKey7=\033[18~
fKey8=\033[19~
fKey9=\033[20~
fKey10=\033[21~
```

...

If necessary, you can change the value associated with each of the function keys. Character string encoding follows the same rules as those defined for the character strings of the .key keyboard files.

Integration of function keys in the emulator

The function keys can be invoked when striking a key on the keyboard or at a mouse event. Reference to the function keys file can thus be made in the keyboard and mouse definitions.

The emul.fky file is used to display simple labels for the various terminal function keys in the keyboard and mouse configuration boxes.

Example:

Function key fKey22 has label Shift F10: when a keyboard key or mouse event is associated with function key Shift F10, the keystroke or mouse activation corresponds to function key fKey22 whose value is defined in the function keys file (for example fKey22=\033[34~ in vt100 emulation).

Terminal configuration

You can associate a terminal configuration file (extension .ses), whose contents interact with the ".seq" and ".cod" files, with each type of terminal. A number of configuration files are supplied with Tun's emulator so that standard configuration parameters for the chosen terminal can be associated with each session.

▸ Opening an existing .ses file from the Administrator reference directory

A .ses file is a text file that can be read in a Notepad-type text editor. You can therefore open a .ses file from this type of editor. The terminal configuration files supplied by Tun can be found in the Tools\Applications Access\Unix Emulations\Specific Data\Terminals of the resources tree. To edit a .ses file, select Properties in its context menu.

▸ Opening an existing .ses file from an session in the Administrator

Select the Properties option in the context menu of the Terminal element of an session.

Click on the .ses file chosen from the Parameters drop-down menu, then click on the Modify button. The .ses file opens in the default test editor.

Content of a terminal configuration file

Here, for example, is an extract from the vt220.ses file:

```
[Intro]
ID=19971009
ParamNb=5
Param1=Cursor
Param2=Wrap
Param3=KeyMode
Param4=Keyboard
Param5=AbortEsc

[Cursor]
Label=SetupCursorStyle
ItemNb=2
Item1=SetupCursUnderline
Item2=SetupCursBlock
Action1=127(12,14)
Action2=127(0,14)
InitDefault=1
InitAction=%gS136%{16}%/%{5}%>%{2}%{1}%@

[Wrap]
```

```
Label=SetupAutowrap
ItemNb=2
Item1=SetupON
Item2=SetupOFF
Action1=62
Action2=63
InitDefault=1
InitAction=%gS4%{2}%{1}%@
...
```

A .ses file is used to define the different terminal configuration parameters (for example, cursor style, keyboard type, sequence abort or not, etc.). Each section of the .ses file describes the various possible options for a parameter which can be selected by the user in the terminal configuration box.

Details

Identifiers

The names of combo-boxes and the listed items are stored in the emulator's language files (".lg"). The file ".ses" contains the related name file identifiers (SetupCursorStyle, SetupAutoWrap, etc. in the example) as parameters.

Order of the combo-boxes

The combo-boxes appear in the order of their definition in the section [Intro]. The items listed in a combo-box appear in the order of their definition.

Actions

The field InitAction must contain a number from 1 through N. This number is the initial choice in the combo-box when it's opened in an active session. In other cases, the field InitDefault is used. InitDefault is set in accordance with the initialization parameters of the ".seq" file. That way, the ".ses" and ".seq" files aren't contradictory.

If the dialog box relates to the active session, the actions linked to the options in the combo-box (Action1...ActionN) are executed when the dialog box is validated (OK is pressed).

Loading order of the ".ses" file

The .ses file is loaded after the ".seq" file but before the configuration file containing the users' choices.

National keyboards

In highly-specific multi-lingual environment situations, the emulator enables national filters to be employed, for example so that particular accents can be used. Using the nat mnemonic, it is then possible to assign a particular value to a keyboard key, as referenced in the .nat file. The values referenced in a .nat file are simple characters or mnemonics.

Example:

You are working in a French environment (azerty keyboard). However, a user temporarily wants to use a US keyboard configuration (qwerty keyboard). After selecting the US keyboard from the National keyboard option, the user can then redefine the keyboard by associating the nat mnemonic with key «a» on the PC keyboard. This indicates that the emulator has to refer to the .nat file to find out the value of this key in a qwerty environment (in fact, striking the «a» key will display a «q» on the screen, as if a qwerty keyboard were being used).

Reading a .nat file

When a PC keyboard key refers to the nat mnemonic, the character or mnemonic associated with it is located on the row corresponding to the key's scan code. The first column of the row gives the scan code, while the eight other columns give the value assigned to the key, in the following order:

- Key without combination (basic)
- Shift
- Ctrl
- Ctrl/Shift
- Alt
- Alt Shift
- Alt Ctrl
- Alt Ctrl Shift

Example:

The keyboard key with scan code 16 refers to row 16 of the .nat file. The value of this key, when combined with the Shift key, is defined in the third column of row 16.

▸ Opening an existing .nat file

A .nat file is a text file that can be read in a Notepad-type text editor. You can therefore open a .nat file from this type of editor. The national files supplied by Tun can be found in the Tools\Applications Access\Unix Emulations\Specific Data\National Keyboards directory of the Administrator resources tree. To edit a .nat file, select Properties in its context menu.

Control codes

Characters whose decimal values range from 0 through 31, and from 128 through 159 are called control codes. Control codes often directly trigger particular actions. In Tun's emulator, control codes are configured in files with a ".cod" extension.

Here, for example, are the contents of the file ansi.cod:

```
nul       0
soh       0
stx       0
etx       0
eot       0
enq       0
ack       261
bel       250
bs        96
ht        99
lf        113
vt        0
ff        51
cr        97
so        0
si        0
dle       0
dc1       0
dc2       0
dc3       0
dc4       0
```

```
nak       0
syn       0
etb       0
can       0
em        0
sub       0
esc       0
fs        0
gs        0
rs        0
us        0
```

The first column contains the control code mnemonic and the second column contains the number of the action to be carried out on reception of the corresponding code. Three options can be used in the second column:

- Leave the value blank (the character is displayed on the terminal).
- Respond with 0 (no action is carried out, and the character isn't listed).
- Select an action from the list in the Escript.hlp file.

A control code can only execute a simple action.

Opening an existing .cod file from the Administrator reference directory

A .cod file is a text file that can be read in a Notepad-type text editor. You can therefore open a .cod file from this type of editor. The control code files supplied by Tun can be found in the Tools\Applications Access\Unix Emulations\Specific Data\Control codes directory of the resources tree. To edit a .cod file, select Properties in its context menu.

Opening an existing .cod file during an emulation session

Select the Properties option in the context menu of the Terminal element of an session.

Click on the .cod file chosen from the Control codes drop-down menu then click on the Modify button. The .cod file opens in the default text editor.

Code conversion

In some emulations, ASCII characters need to be converted before they can be sent correctly to the server. This conversion is managed by the .snd sent code files.

Here, for example, is an extract from file vt220.snd:

```
-       \0xa1
›       \0xa2
œ       \0xa3
_       \0xa5
¦       \0xaa
®       \0xab
ø       \0xb0
ñ       \0xb1
ý       \0xb2
þ       \0xb3
æ       \0xb5
ã       \0xb6
```

The left-hand column contains ASCII characters and the right-hand column contains the codes to be sent to the host machine.

Opening an existing .snd file from the Administrator reference directory

A .snd file is a text file that can be read in a Notepad-type text editor. You can therefore open a .snd file from this type of editor. The sent codes files provided by Tun can be found in the Tools\Applications Access\Unix Emulations\Specific Data\PC to host conversions directory of the resources tree. To edit a .snd file, select Properties in its context menu.

Opening an existing .snd file from an session in the Administrator

Select the Properties option in the context menu of the Terminal element of an session.

Click on the .snd file chosen from the Sent codes drop-down menu and then click on the Modify button. The .snd file opens in the default text editor.

Character tables

The character tables act as filters for displaying characters on the screen: An 8-bit character has 256 possible values. IBM-compatible micro-computers have their own encoding of these 256 characters. Certain characters are standard: 65 is represented as 'A', 66 as 'B', 48 as 'O', etc. Other characters, such as control characters, have a particular meaning for IBM. Different terminals have different character sets.

The objective is to define the tables for character representation. A representation is always encoded with 7 bits, that is, with the values 0 through 127.

The tables ascii.tab and asciie.tab (ASCII and the extended ASCII character set) represent the micro-computer codes 0 through 127 (ascii.tab) and 128 through 255 (asciie.tab). Other tables are:

UK.TAB	Britain
DECSU.TAB	DEC supplementary
DECSP.TAB	DEC special graphics

A character table file looks like this:

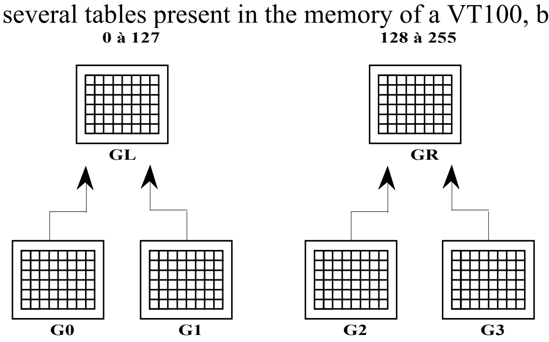
```
80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f
90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f
a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af
b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf
c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf
d0 d1 d2 d3 d4 d5 d6 d7 d8 d9 da db dc dd de df
e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef
f0 f1 f2 f3 f4 f5 f6 f7 f8 f9 fa fb fc fd fe ff
```

There are 128 fields corresponding to the 128 possible arrangements of 7 bits. The horizontal axis shows the first four bits and the vertical axis shows the last three bits. This table only contains hexadecimal codes.

To change a particular character, its hexadecimal code must first be looked up in the ASCII table and then entered in the ".tab" file.

Internal character table management

To manage these tables during an emulation session, Tun's emulator uses a model based on VT100 emulation. There are several tables present in the memory of a VT100, but only 4 tables are available at any given time:



By default, one of the tables G0, G1, G2, or G3 is loaded into GL and GR. GL represents all the characters from 0 through 127, and GR, the characters from 128 through 255.

In Tun's emulator, there are four actions related to this procedure:

Actions	Description
194	Assigns a character table to G0
195	Assigns a character table to G1
196	Assigns a character table to G2
197	Assigns a character table to G3

These actions are defined by a table number corresponding to those indicated in the terminal configuration box (Terminal option of the Session menu).

In Tun's emulator, eight actions allow you to fill GL and GR:

Actions	Description
210	lock G0 in GL
211	lock G1 in GL
212	lock G2 in GL
213	lock G3 in GL
214	lock G0 in GR
215	lock G1 in GR
216	lock G2 in GR
217	lock G3 in GR

Finally, four other simple actions let you access the next character in the tables G0, G1, G2, or G3 without using GL or GR:

Actions	Description
218	Selective use of G0
219	Selective use of G1
220	Selective use of G2
221	Selective use of G3

This organization of 4 active tables (two of which are available by default) is complex. Most emulations have two permanent tables (GL and GR). The configuration file lets you use 10 alternative tables. You load one of these tables into GR or GL as follows:

Example:

```
194(4) 214
```

or with the action label:

```
TabAsG0(4) G0IntoGR
```

loads the 5th table into G0, then locks G0 into GR.
This organization lets you set the parameters to match virtually all existing terminal emulations.

Alternate character font

By default, PCs are only able to display 256 characters simultaneously. This limit poses some problems when trying to create emulations for more complex terminals that offer four or five different fonts.

In MS-DOS with a VGA or SVGA card, or in Windows, Tun's emulator can display 2 x 256 characters simultaneously by using an alternate font.

For a ".tab" file to be able to use an alternate font, simply replace the desired hexadecimal value by the number 1.

For example, the value 182 refers to the 130th position (82nd in hexadecimal) of the alternate font.

Eastern European character sets

TunPlus supports Eastern European character sets for Czech, Croatian, Estonian, Latvian, and Lithuanian in the IBM3151, VT320, and VT220 emulations. To enable these character sets:

1. Click File > New.
2. Select Asynchronous Emulation.
3. Set the terminal and display type.

Terminal	Display Type
IBM3151	• For Czech or Croatian, set the Terminal and Display to IBM3151_2e • For Estonian, Latvian, and Lithuanian, set the Terminal and Display to IBM3151_13e
VT220	• For Czech or Croatian, set the Terminal to VT220_2e. Set the Display to VT320_2e. (VT220 and VT320 use the same display file.) • For Estonian, Latvian, and Lithuanian, set the Terminal to VT220_13e. Set the Display to VT320_13e. (VT220 and VT320 use the same display file)
VT320	• For Czech or Croatian, set the Terminal to VT320_2e. Set the Display to VT320_2e. • For Estonian, Latvian, and Lithuanian, set the Terminal to VT320_13e. Set the Display to VT320_13e.

4. Connect to the host.

- For IBM3151 or VT320, confirm that the terminal settings are correct by clicking on Session>Terminal.
- For IBM3151, change the Extended Page to 8859.
- For VT320, ensure that the VT default character set is Dec Multinational.

5. Click on Tools > Display Editor > Fonts tab. The "Use Ansi to Oem Conversion" must be disabled.
6. Save the workspace.

Index