Disclaimer

DISCLAIMER OF WARRANTY

THIS SOFTWARE AND MANUAL ARE SOLD "AS IS" AND WITHOUT WARRANTIES AS TO PERFORMANCE OF MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. BECAUSE OF THE VARIOUS HARDWARE AND SOFTWARE ENVIRONMENTS INTO WHICH THIS PROGRAM MAY BE PUT, NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE IS OFFERED. GOOD DATA PROCESSING PROCEDURE DICTATES THAT ANY PROGRAM BE THOROUGHLY TESTED WITH NON-CRITICAL DATA BEFORE RELYING ON IT. THE USER MUST ASSUME THE ENTIRE RISK OF USING THE PROGRAM. ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR REFUND OF PURCHASE PRICE.

Table of Contents

Introduction

TACACS Server is a NLM based server that responds to username/password requests via the Extended TACACS (XTACACS) protocol. It is specifically designed to work with cisco terminal servers, but should work with any TACACS client.

How it works

When a user authenticates into a cisco server, they enter username@machine.name followed by a password. The cisco server then authenticates the username/password with the machine specified via the TACACS protocol. If the username/password is valid the cisco server allows the connection. At certain times after this connection is opened, the cisco server may send or request additional information to the authorizing machine. Once TACACS Server is installed on the NetWare server and the NetWare server is specified as a valid host within the cisco servers, users can authenticate with their NDS or bindery usernames. No Un*x host is required.

Requirements

TACACS Server for NetWare requires either a NetWare 4.1 or NetWare 3.12 file server. Under NetWare 4.1 a single server can service requests for an entire NDS tree.

The server memory requirements for TACACS Server for NetWare vary. The base NLM requires 500K of memory. Each handler requires an additional 50K and each queue requires 5K. Therefore, in the default configuration the memory requirement would be Base (500K) + Handlers (5 * 50K) + Queues (20 * 5K) for a total of 850K.

NetWare Directory Services

Installation

1. Configure your cisco servers to allow requests from your NetWare servers registered DNS name. Please consult your printed cisco manuals, UniverCD, or http://www.cisco.com for assistance.

    - Make a note of the IP addresses that you want to allow TACACS authentication from.

2. With NWAdmin (Windows) or NetAdmin (DOS) create a user for TACACS Server to login as. A suggested name is TACACS.

    - For this user, make sure to set login restrictions so that the user can only login from the NetWare server. Do so by specifying the NetWare servers internal network number as the network number, and 1 as the node number. You should see something like 00004000:000000000001 as the complete network address when completed.
    - Set the user to have unlimited number of logins.
    - A password is not required and is not recommended. If you choose to use a password please record it, as it will need to be entered into the TACACS.RSP file.

3. Copy TACACS.NLM and TACACS.RSP to SYS:SYSTEM.
4. Copy your license file, TACACS.LIC to either SYS:SYSTEM or SYS:ETC. SYS:ETC is recommended for better security.
5. Edit TACACS.RSP. See **OPTIONS** for details.
6. Installation is now complete. To start TACACS Server, type LOAD TACACS.NLM @TACACS.RSP on NetWare server console.

Access Control

Granting and removing TACACS access is extremely easy as all management is done through tools you already know, either NWAdmin for Windows users or NetAdmin for DOS users.

Access control for a user is determined by the TACACS user NDS rights. To authorize a user grant the TACACS user **Read** rights to **[All Properties Rights]** for the user your want to authorize. Unless the TACACS user has these rights users will not be authenticated and requests will always be denied.

With Directory Services powerful flow down and inheritance filters you can configure just about any combination of user access. For example: To grant everybody in a container TACACS authorization, make the TACACS user a trustee of the container itself. The trustee rights will flow down to all users in that container and all sub-containers. If you later want to disallow access to a guest user then make the TACACS user a trustee of the guest user, but set the **[All Properties Rights]** to **None**.

Setting up your first user (Windows)

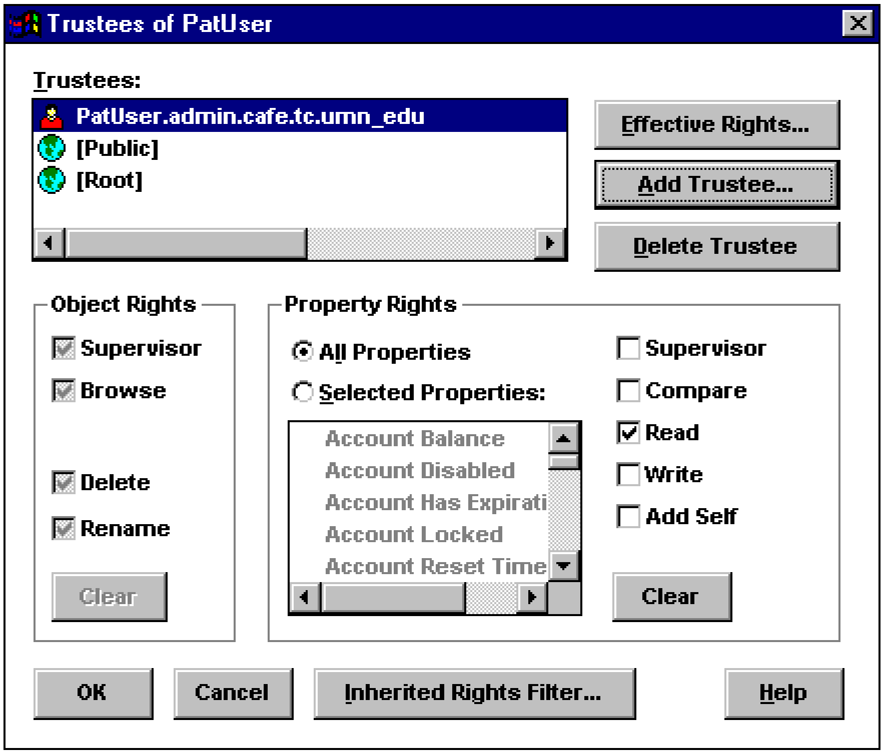
If you are not already logged in as a user with sufficient rights to manipulate the Access Control Lists of objects, do so now. If in doubt, login as Admin.

In the following screen images the TACACS user is tacacs.cafe.tc.umn_edu and the user we are giving authorization to is PatUser.admin.cafe.tc.umn_edu.

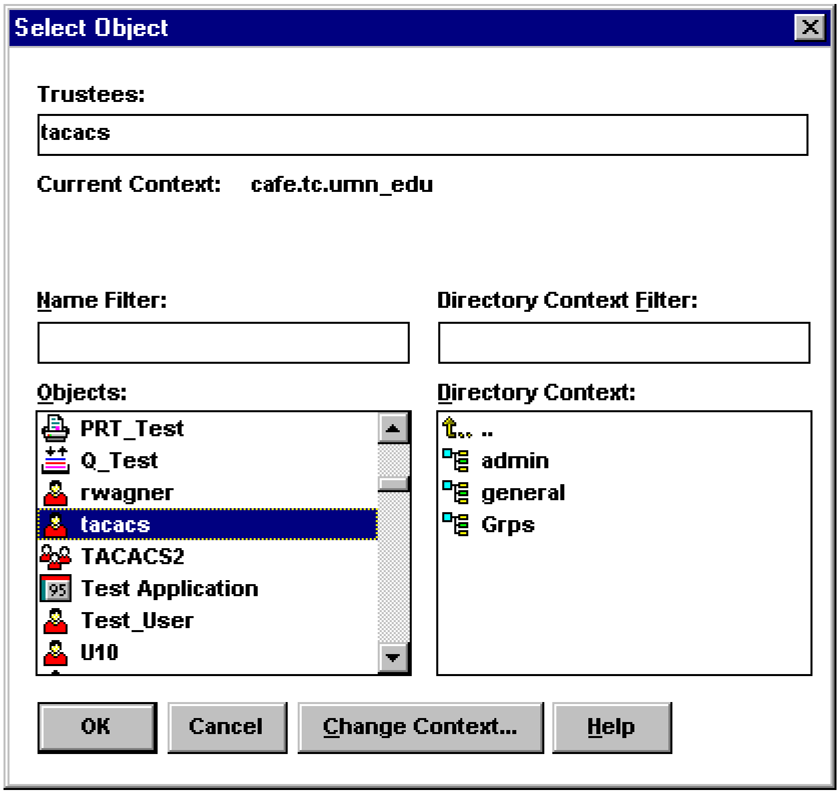
1. Start NWAdmin. This should be located in SYS:PUBLIC.

2. Locate the user to grant TACACS access and highlight them. From the **Object** menu select **Trustees of this Object**.

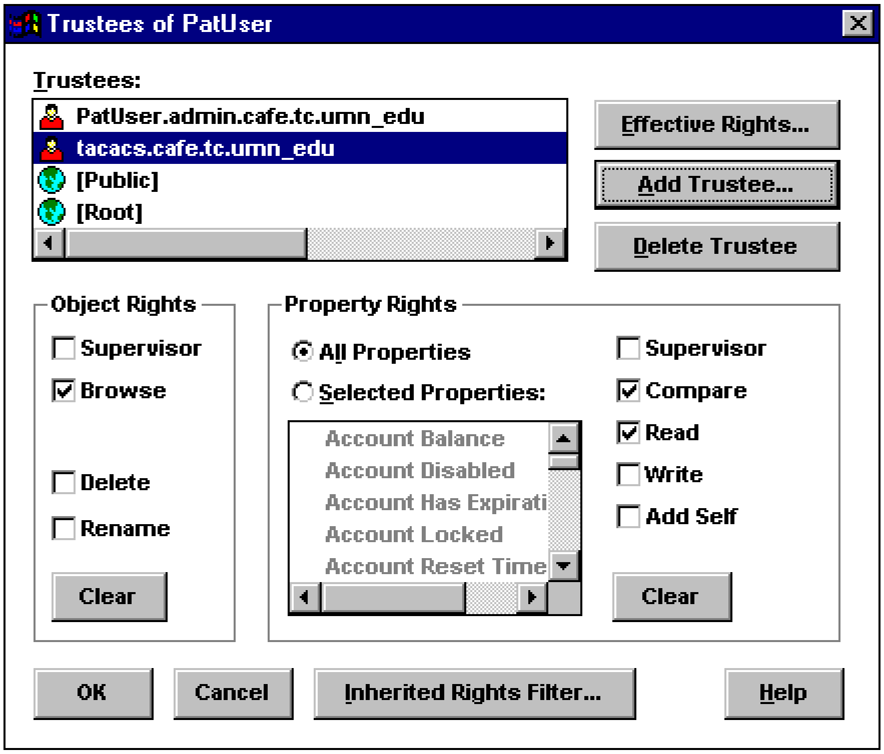
3. Grant the TACACS user rights to the user by pressing the **Add Trustee** button.



4. Walk the tree and locate the TACACS user. Highlight the TACACS user and press the **OK** button.



5. By default the TACACS user is assigned **Object Rights-Browse** and **All Properties-Compare/Read**. Verify that the rights are correct.



6. Click OK. The user is now authorized to use the TACACS server.

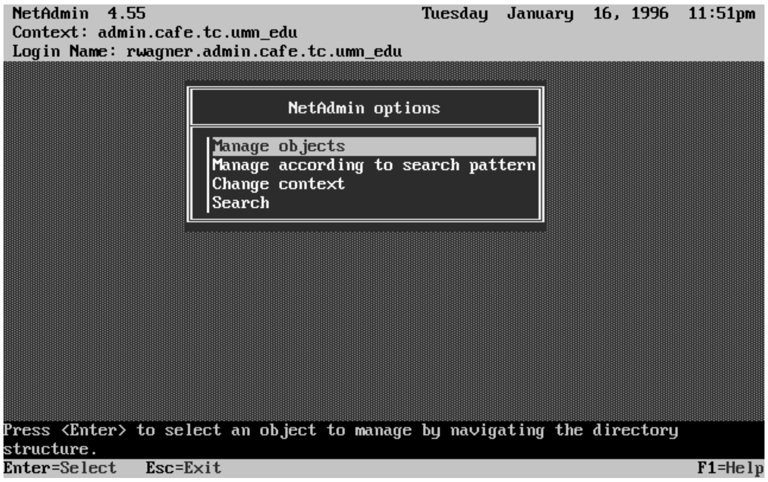
Setting up your first user (DOS)

If you are not already logged in as a user with sufficient rights to manipulate the Access Control Lists of objects, do so now. If in doubt, login as Admin.

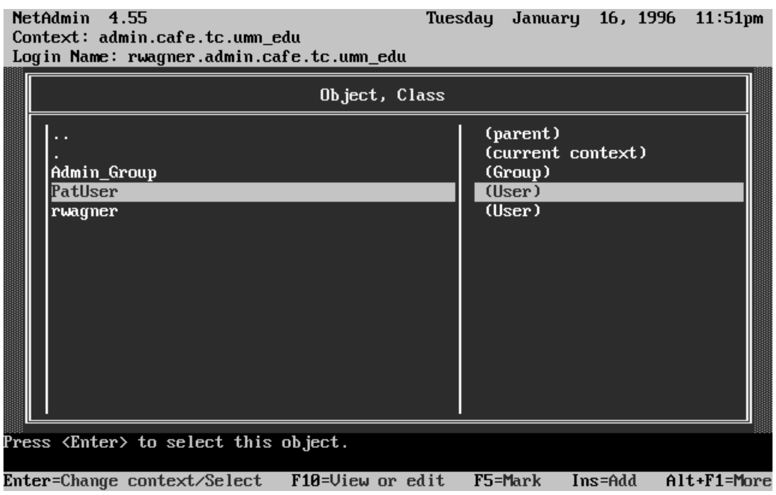
1. Start NetAdmin by typing

   `NETADMIN`

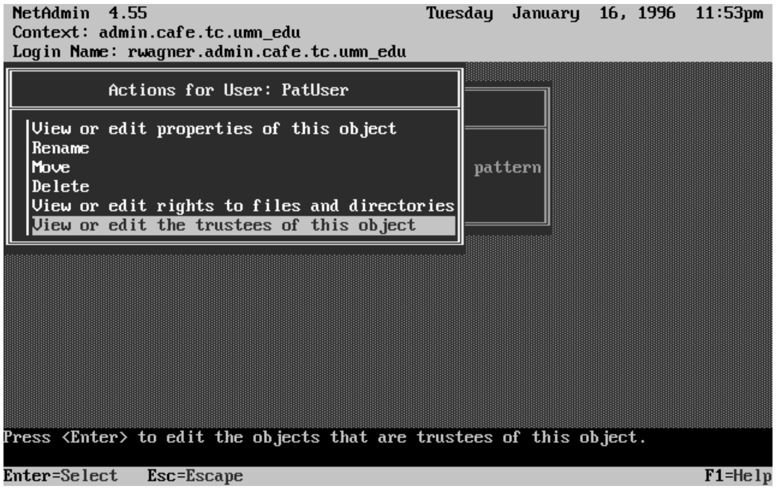
2. From NetAdmin menu select **Manage Objects**.



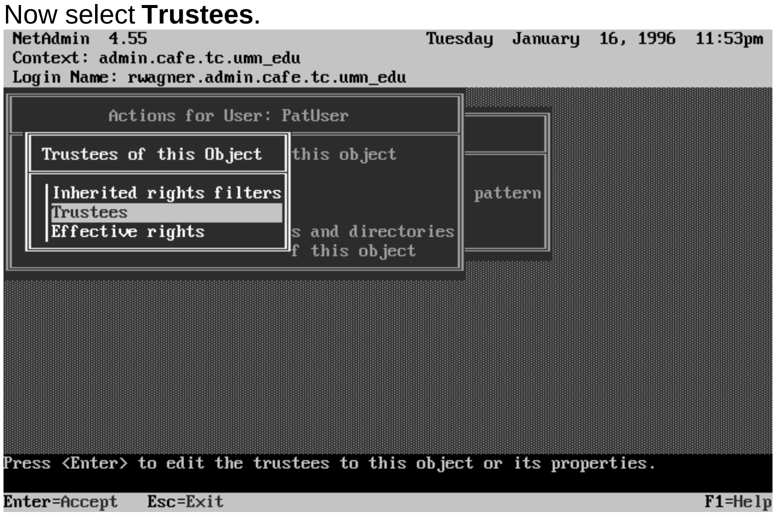
3. You will be presented with a list of the objects in your current context. Locate and highlight the user that you wish to have access.
   *Note: You may also type **Insert** again and walk the tree to locate the user.*



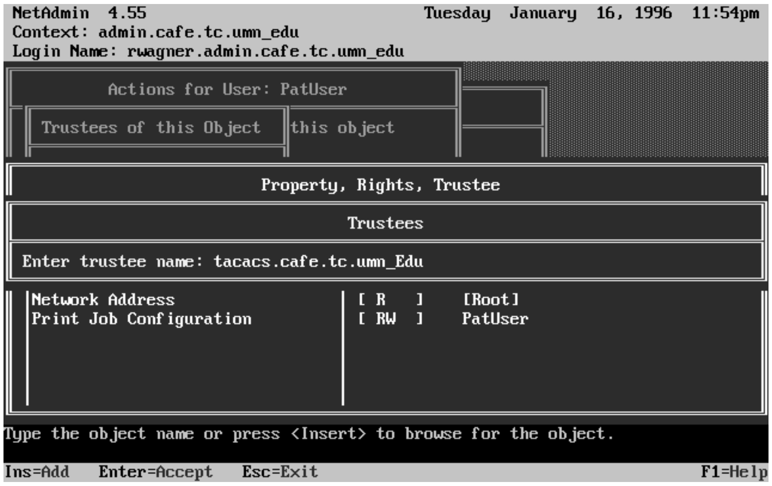
4. Once you have located your user, hit **Enter** to edit the user and select **View or edit the trustees of this object**.



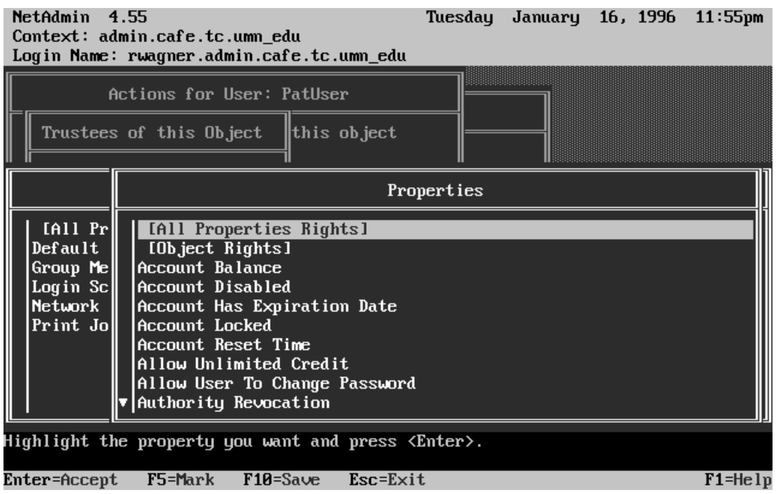
5. Now select **Trustees**.



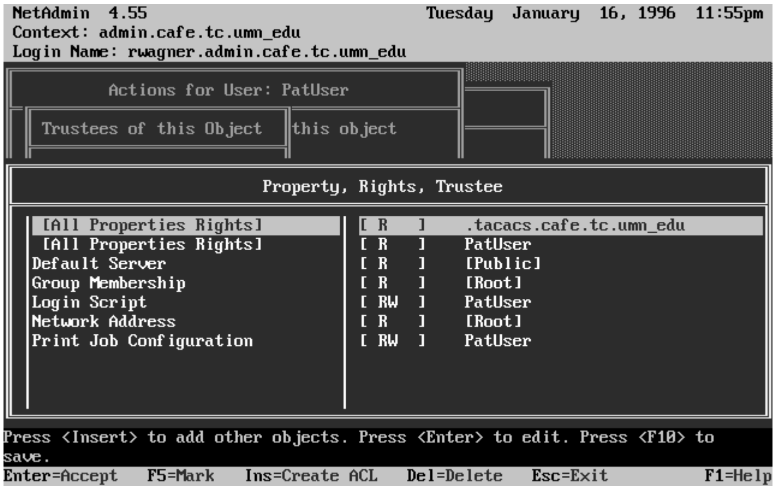
6. You are now presented with a list of the current trustees for the user. Hit **Insert** and enter the complete name of the TACACS Server user.
Note: You may also type ***Insert*** *again and walk the tree to locate the TACACS user.*



7. Highlight **[All Properties Rights]** and hit **Enter**.



8. By default the new trustee assignment contains **Read**. This is all the rights that are required!



9. You may now exit or repeat this procedure for additional users.

Authentication

When the user connects to the cisco server they must enter their full context name. (e.g., rwagner.dept.umn) unless using shortcuts (see below).

With multiple authorized TACACS servers, users must also enter a machine name (e.g., rwagner.dept.umn@nw41.is.umn.edu). It's recommended in these situations to add an additional DNS name for your Novell server (e.g., nds.umn.edu).

Shortcuts

Shortcuts are a method of simplifying the user names that are entered for authentication (see **Options** below for syntax). With shortcuts, you can configure your system so users can just enter their Common Name instead of their full context names.

When the username is received by the server it is first treated as a full context name. If that user does not exist then each shortcut is appended to the user name and checked for existence. The first user object located with that name is the user that will be processed.

Example:

To shorten the login names for Provo.Utah.Company.USA users, define a shortcut of Provo.Utah.Compary.USA. With that set the user Pat.Provo.Utah.Company.USA can just enter Pat for the username.

Note: To guarantee adequate performance with shortcuts, ensure that the server running TACACS Server has replicas of all the partitions that have shortcuts defined.

Bindery Servers

Installation

1. Configure your cisco servers to allow requests from your NetWare servers registered DNS name. Please consult your printed cisco manuals, UniverCD, or http://www.cisco.com for assistance.

    - Make a note of the IP addresses that you want to allow TACACS authentication from.

2. Copy TACACS.NLM and TACACS.RSP to SYS:SYSTEM on the destination server.
3. Copy your license file, TACACS.LIC to either SYS:SYSTEM or SYS:ETC. SYS:ETC is recommended for better security.
4. Edit TACACS.RSP. See OPTIONS for details.
5. Create either a TACACS or NOTACACS group as defined below.
6. Installation is now complete. To start TACACS Server, type LOAD TACACS.NLM @TACACS.RSP on the NetWare server console.

Authentication

When the user connects to the cisco server they must enter their normal bindery username.

With multiple authorized TACACS servers, users must also enter a machine name (e.g., rwagner@nw312.is.umn.edu). In these situations I highly recommend adding an additional DNS name for each Novell server that is easy for people to remember.

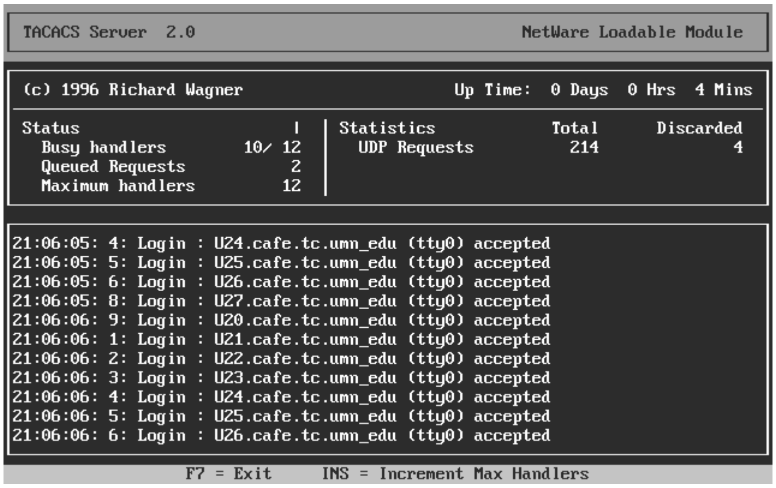
Group Membership

Authentication is based on one of two methods.

1. **Only explicitly authorized users**. To utilize this method create a TACACS group (with SYSCON). You may then authorize individual users by making them group members.
2. **Everybody except those explicitly denied**. To utilize this method create a NOTACACS group (with SYSCON). At this point everybody on your server is authorized. To revoke users (such as GUEST or PUBLIC) add those users to the NOTACACS group.

Please note that only one of the two groups may exist. If you decide at some point to switch methods, you must delete the initial group before creating the new group.

Operation



The Status Window

- **Busy Handlers** consists of two numbers. The first number is the number of handlers that are currently busy handling requests. The second number is the number of handlers that are available. New handlers are started when there are no available handlers for a newly arrived request.

- **Queued Requests** is the number of requests waiting for an available handler. When the buffers are full, new requests are discarded.

- **Maximum handlers** is the maximum number of handlers that will be allocated. You may increase this number while running by pressing the **INSERT** key.

Statistics Window

- **Total** is the total number of requests that have been serviced since TACACS Server was last started.

- **Discarded** is the number of requests that have been thrown away due to no queue buffers available. If this is larger consider increasing the number of queues and the number of handlers. If it continues to be a problem then either the NetWare server is under powered or it is time to add another server running TACACS Server.

Online Log

- This window contains the running long. The information displayed here is identical to the log files contents. You can watch authentication requests as they are received, processed and responded to.

Options

TACACS Server has a powerful set of options available. Any of the options can be given in the response file (TACACS.RSP) or on the command line during the LOAD. When entering parameters do not include *[ ]*.

/Min=[n]	The initial number of authentication handlers. Default = 2, Maximum = 64
/Max=[n]	The maximum number of handlers that will be allocated. Default = 5, Maximum=64
/M=[n]	Log level. Normal = 1, Warnings only = 2, Errors only = 3. Default = 1.
/User=[text]	The DS user that TACACS Server will use. This username must be the full context name.
/PW=[text]	Sets the password for the TACACS Server user. Make sure to keep the response file secure.
/IP=[ipaddress]	Authorized TACACS client. This may be either of the form 128.98.97.1 for a single station or 128.98.97.255 for a complete subnet. Multiple addresses may be entered with multiple '/IP's.
/AllowNULLPasswords	Normally, accounts with no passwords are always denied access. This parameter will enable accounts with no passwords to be used.
/Shortcut=[NDS context]	Sets a shortcut (see section for details).
/Log=[path]	Path on server where the log files will be written. Must be in VOL:PATH\ format (i.e.: SYS:TACACS\LOGS). Default is SYS:SYSTEM
/QueueLength=[n]	Sets the size of the request queue. Default = 20.

Tips

- Whenever in doubt about whether a user is authorized or not, check Effective Rights through either NWAdmin or NetAdmin.
- If you use shortcuts, ensure that usernames are unique within defined shortcuts. No attempt is made to continue checking other contexts if the first user located with that name fails authentication.
- TACACS Server will not allow anybody to authenticate with the same user as the server is currently using.
- In situations where many authentication's are being performed from replicas on other servers, to increase performance set the number of handlers to at least 15.
- If the statistics screen shows that packets are being lost, increase the size of the queue. 50 has been shown to be a good number for heavily loaded servers.

Problems

- You may see reports about unsupported scrambled passwords (CHAP and ARAP). If so, you must set your cisco servers to use normal passwords (this is the default).
- NDS does not handle low memory situations very well. You may see many failures to authenticate when NetWare runs out of memory.
- For NetWare 4.1, make sure you're running the latest version of DS.NLM and appropriate patches (41PT*.EXE). There are many problems with earlier versions of DS.NLM that may cause abends, especially in high load situations.

Technical Support

Technical support is currently available via email to rwagner@tc.umn.edu or through the address and phone number given below.

Richard Wagner
14600 34th Avenue N, Suite 211
Plymouth, MN 55447

You may also reach the author at (612) 559-4591. Please be aware that I have a day job but will return messages promptly.

Uninstalling

- Delete TACACS.NLM, TACACS.RSP, TACACS.LIC and TAC*.LOG from your SYS:SYSTEM directory. TACACS.LIC may be installed in SYS:ETC instead.