TACACS.net TACACS+ Server
Quickstart Setup Guide

TACACS.net is designed to be very easy to setup and use.
In most cases, you should be up and running in minutes!

1) Installation

a) Run the TACACSSetup_v*.exe installation wizard. This wizard will walk you through the software installation on your server.

b) You will be prompted to enter the TACACS+ shared secret during the wizard setup. If you would like to change this, you can do so in clients.xml.

c) The wizard will install the configuration and log files to different locations depending on your OS. See Readme.rtf in the Program Menu for the location of installed files.

2) Create Test Users

Create test users to verify operation of the server. Authentication settings are in the authentication.xml file. Before you change any files, make a backup of the original files in case you need to restore them.

a) Create a File User

File users are created in the authentication.xml file itself. Here is an example of a file user named "steve" with the ClearText password "password". You can start with the commented examples in the authentication.xml file. Uncomment them and make your changes. Use cleartext passwords for testing. These can be replaced with hashed passwords using TACDES after the server has been fully tested and before it goes into production.

```
<User>
     <Name>steve</Name>
     <LoginPassword ClearText="password" DES=""> </LoginPassword>
     <EnablePassword ClearText="" DES=""></EnablePassword>
     <CHAPPassword ClearText="" DES=""> </CHAPPassword>
     <OutboundPassword ClearText="" DES=""> </OutboundPassword>
 </User>
```

b) The DEFAULT Group

The default group is installed by default. This is the fallback group and includes all administrators on the local machine. It should be commented out when the server is deployed in production.

You do not need to restart/reload the server when you modify the configuration files. The server monitors for changes to the configuration files and reloads them automatically.

3) Verification

a) Run TACVerify

This utility will check your configuration for syntax errors. It can be found in the Program Menu. If the tool detects any errors, go back and fix them and run the utility again.

b) Run TACTest

Before you attempt to run TACACS+ on any external Clients in a lab or production environment, it is critical that you first run TACTest to verify that the system is working correctly. If TACTest fails,

your external Clients will fail also. Run tactest /? from the command line for options. Here is a simple example:

```
C:\> tactest -k mykey -u myuser -p mypassword
```

4) Configure the NAS

After you have verified that the TACACS+ server is up and running and working properly, then configure the network device (router/switch/firewall.etc.) for TACACS+ and repeat these steps by authenticating to the NAS. Refer to the manual for the device you are using for TACACS+ configuration. After you have confirmed that basic TACACS+ operation is working between the client and server, then you can move on to configuring different authentication methods and authorization policies. Review the configuration files and documentation for further instructions.

5) Troubleshooting

If you experience any problems, try the following steps:

a) Ping and traceroute from the client to the server and from the server to the client to verify connectivity between the systems.
b) Telnet to the TACACS+ server from the client to ensure connectivity on the TACACS+ port (#telnet IP.address.of.server 49).
c) Ensure that there are no firewalls or ACLs blocking the traffic between the NAS and the server. Disable any firewalls (including Windows firewall) on the local machine.
d) Review the logs for errors. The logs can be found in the TACACS.net program menu and in the readme.rtf.
e) Run the TACVerify test tool from the program menu.
f) Run TACTest to ensure that you can authenticate from the local machine.
g) Restore the configuration files from the original installation.
h) Turn up the logging levels in tacplus.xml to debug and review the output.
i) If more than one network interface is available on the server (physical or virtual), or if you are receiving any type of socket errors in TACTest, manually configure the IP address of the server in tacplus.xml.
j) Disconnect all open sessions and restart the service using the Services applet in Administrative Tools.
k) Disable other services or programs on the local server.
l) Run Wireshark on the server to review incoming requests.

6) Advanced Configurations

- Please refer to the Configuration Guide for additional options including:
- Creating DES hashed passwords for local file users
- Authentication using Windows Users & Groups
- Authentication using Windows Active Directory
- Authentication using LDAP
- Clients & client groups
- Authorization policy
- Logs & logging levels