TACACS+ User Guide

General Information

A TACACS+ user can login on:

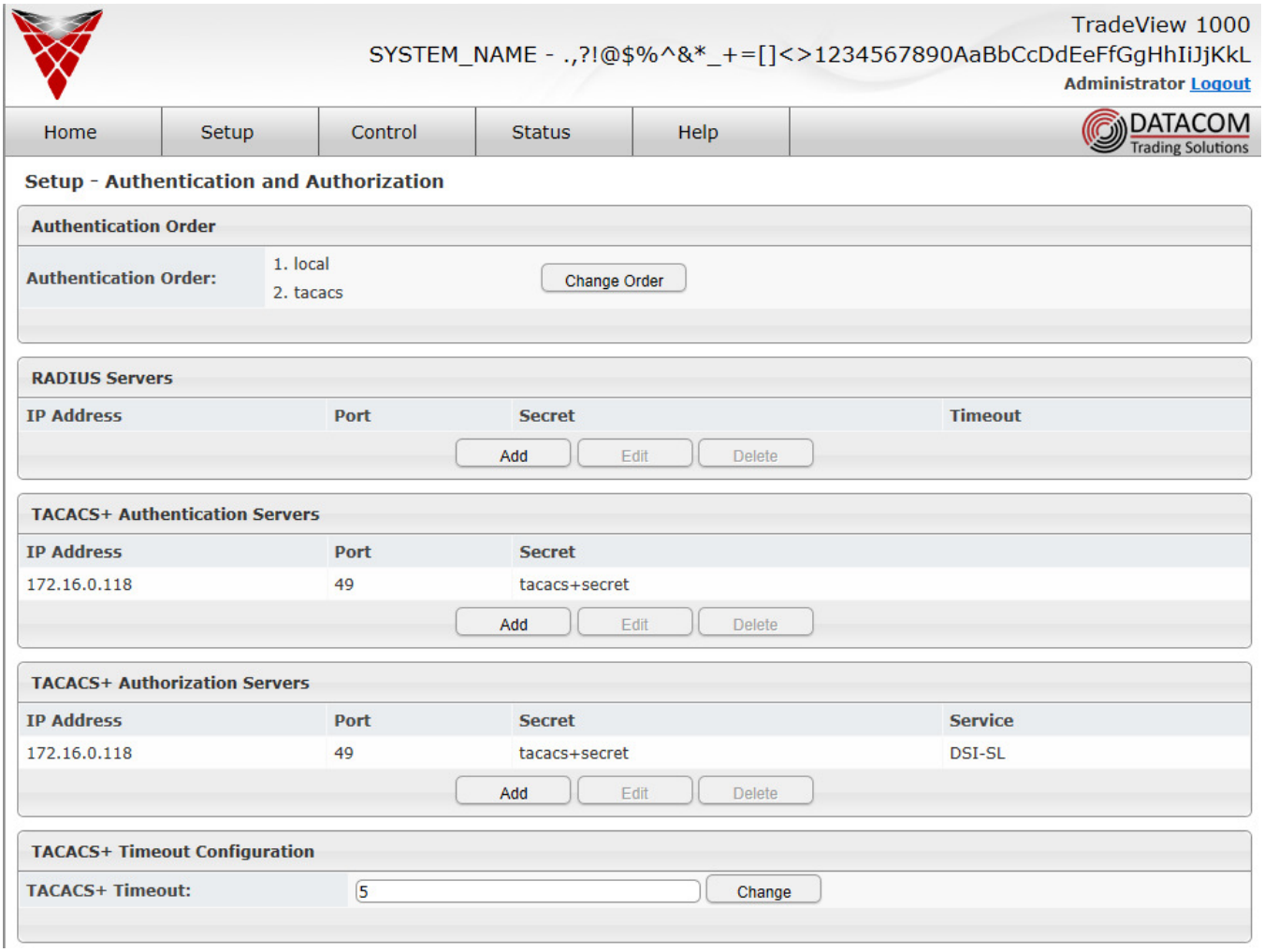
- Serial Console
- SSH
- GUI - Web Server

If telnet is enabled, local authentication ONLY is available. No TACACS+ authentication is implemented at this time (i.e., 8/24/12)Client Side Configuration

Client Configuration

GUI Configuration

1. Define a TACACS+ Authentication Server
2. Define a TACACS+ Authorization Servers
3. Optionally you can change the default TACACS+ Timeout.
4. Set the Authentication Order to your preference: TACACS only, TACACS/Local or Local/TACACS.



CLI Configuration

1. Add the TACACS+ Server using the IP:Port and the defined TACACS+ Secret.
   eg. ADD TACACS LOGIN 172.16.0.118:49 tacacs+secret

2. Add the TACACS+ user rights as defined on the TACACS+ Server
   eg. ADD TACACS RIGHTS 172.16.0.118:49 tacacs+secret DSI-SL

3. Set Authentication order selecting whether to attempt TACACS or LOCAL authentication first.
   SE AU OR LO (Authenticate locally)
   SE AU OR TA (Authenticate using Tacacs only)
   SE AU OR LO TA (Attempt local authentication. If fails, attempt Tacacs authentication)
   SE AU OR TA LO (Attempt Tacas authentication, if NONE of the Tacacs servers respond, attempt local

TACACS+ Server Configuration

The DSI right is represented as one of the known right names as identified in the TACACS+ Dictionary. This "right" must be set to an integer value of :

87 for Full Access

82 for Read-only access.

78 for No Access

The default is No Access. Consequently, if a particular right is not to be either Full or Read-Only access, do not include the right in the Authorization Service. Add a TACACS+ Authorization Server (RIGHTS) using the known TACACS+ IP address, the shared secret, and the authorization service name created for you on the TACACS+ authorization server. (NOTE: The Authorization server can be different than the Authentication server.)

NOTE :The server settings are dependent on the TACACS+ Server . The Examples bellow are for TACACS.net server.

1. Define the Clients Client Group

```
<ClientGroup Name="INTERNAL">
    <Secret ClearText="tacacs+secret" DES=""></Secret>
    <Clients>
        <Client>192.168.12.*</Client>
        <Client>192.168.13.*</Client>
        <Client>10.0.0.0/8</Client>
        <Client>172.16.0.0/12</Client>
        <!--<Client>192.168.0.0/16</Client> -->
    </Clients>
</ClientGroup>
```

clients.xml

2. Define the Users and the User Group

```
<UserGroup>
    <Name>QA Testing</Name>
    <AuthenticationType>File</AuthenticationType>
        <Users>
            <User>
                <Name>Username</Name>
                <LoginPassword ClearText="Password#123" DES=""> </LoginPassword>
                <EnablePassword ClearText="" DES=""></EnablePassword>
                <CHAPPassword ClearText="" DES=""> </CHAPPassword>
                <OutboundPassword ClearText="" DES=""> </OutboundPassword>
            </User>
            <User>
                <Name>UserTACACS</Name>
                <LoginPassword ClearText="Password#123" DES=""> </LoginPassword>
                <EnablePassword ClearText="" DES=""></EnablePassword>
                <CHAPPassword ClearText="" DES=""> </CHAPPassword>
                <OutboundPassword ClearText="" DES=""> </OutboundPassword>
            </User>

        </Users>
</UserGroup>
```

authentication.xml

3. Define the authorization service using the Datacom Systems Inc. dictionary.

authorisation.xml

```
<?xml version="1.0" encoding="utf-8"?>
<Authorizations xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <Authorizations>
    <Authorization>
        <!--This entry will only be processed in the times given below-->
        <!--<Time>MTWRFSN,04:00-21:00</Time>-->
        <!--This authorization section applies to the following user groups. In case of conflicting authorization entries for the same grou
        <UserGroups>
            <UserGroup>QA Testing</UserGroup>
        </UserGroups>
        <Users>
            <User>TestUser</User>
            <User>UserTACACS</User>
        </Users>
        <!--This authorization section applies to the following client groups. In case of conflicting authorization entries for the same cl
            <!--If no client groups are specified then the settings are applied to the specified usergroups irrespective of the clients the
        <ClientGroups>
            <ClientGroup>LOCALHOST</ClientGroup>
            <ClientGroup>INTERNAL</ClientGroup>
            <ClientGroup>QA Clent Group</ClientGroup>
        </ClientGroups>
        <AutoExec>
        <!--The next entry allows telnet to certain ip addresses for the group-->
        <Shell> <!--note that the login and exit commands are always permitted-->
        <Services>
            <!-- <Service>
                <!--these groups can run IP over PPP only if they use one of the following mandatory addresses. If they supply no address,
                <!--<Set>addr=10.1.1.1</Set>--> <!--mandatory argument-->
                <!--Their  mandatory input access list number is 5-->
                <!--<Set>inacl=5</Set>-->
                <!--We will suggest an output access list of 10 but the NAS may choose to ignore or override it-->
                <!--<SetOptional>outacl=10</SetOptional>-->
                <!--These are examples of vendor specific attributes(VSAs)-->
                <!--<Set>foundry-privlvl=5</Set>-->
            <!-- </Service> -->

            <!--
            <Service>
                <Set>service=DSI-SL</Set>
                <!-- No protocol specified here will allow ALL protocols to work <Set>protocol=lcp</Set> -->
                <Set>protocol=lcp</Set>

                <Set>DSI-Admin=87</Set> <!-- Full CLI Administrative Rights -->
                <Set>DSI-SL-Management=87</Set>
                <Set>DSI-SL-Users=87</Set>
                <Set>DSI-SL-Port-Settings=87</Set>
                <Set>DSI-SL-System=87</Set>
                <Set>DSI-SL-Port-Steering=87</Set>
                <Set>DSI-SL-Filter-Def-Appl=87</Set>
                <Set>DSI-SL-Counters = 87</Set>
                <Set>DSI-SL-System-Health=87</Set>
                <Set>DSI-SL-Logs=87</Set>
                <Set>DSI-SL-Help=87</Set>
                <Set>DSI-SL-SNMP=87</Set>
                <Set>DSI-SL-Group-Management=87</Set>
                <Set>DSI-SL-Load-Balancing=87</Set>
                <Set>DSI-SL-Analytics=87</Set>
                <Set>DSI-SL-Radius=87</Set>
                <Set>DSI-SL-Radius=87</Set>

            </Service>
            <Service>
                <Set>service=DSI-ATTR</Set>
                <!-- No protocol specified here will allow ALL protocols to work <Set>protocol=lcp</Set> -->
                <Set>protocol=lcp</Set>

                <Set>DSI-Admin=87</Set> <!-- Full CLI Administrative Rights -->
                <Set>DSI-SL-Management=87</Set>
                <Set>DSI-SL-Users=87</Set>
                <Set>DSI-SL-Port-Settings=87</Set>
                <Set>DSI-SL-System=87</Set>
                <Set>DSI-SL-Port-Steering=87</Set>
                <Set>DSI-SL-Filter-Def-Appl=87</Set>
                <Set>DSI-SL-Counters = 87</Set>
                <Set>DSI-SL-System-Health=87</Set>
                <Set>DSI-SL-Logs=87</Set>
                <Set>DSI-SL-Help=87</Set>
                <Set>DSI-SL-SNMP=87</Set>
                <Set>DSI-SL-Group-Management=87</Set>
                <Set>DSI-SL-Load-Balancing=87</Set>
                <Set>DSI-SL-Radius=87</Set>
            </Service>
```