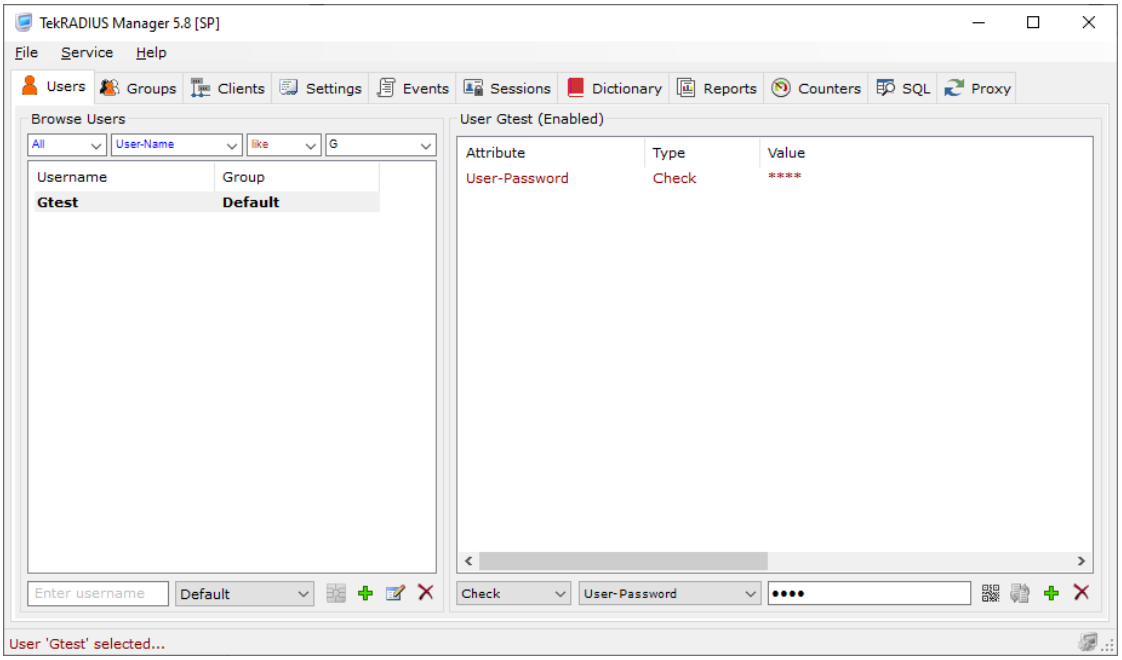
Policy Matching

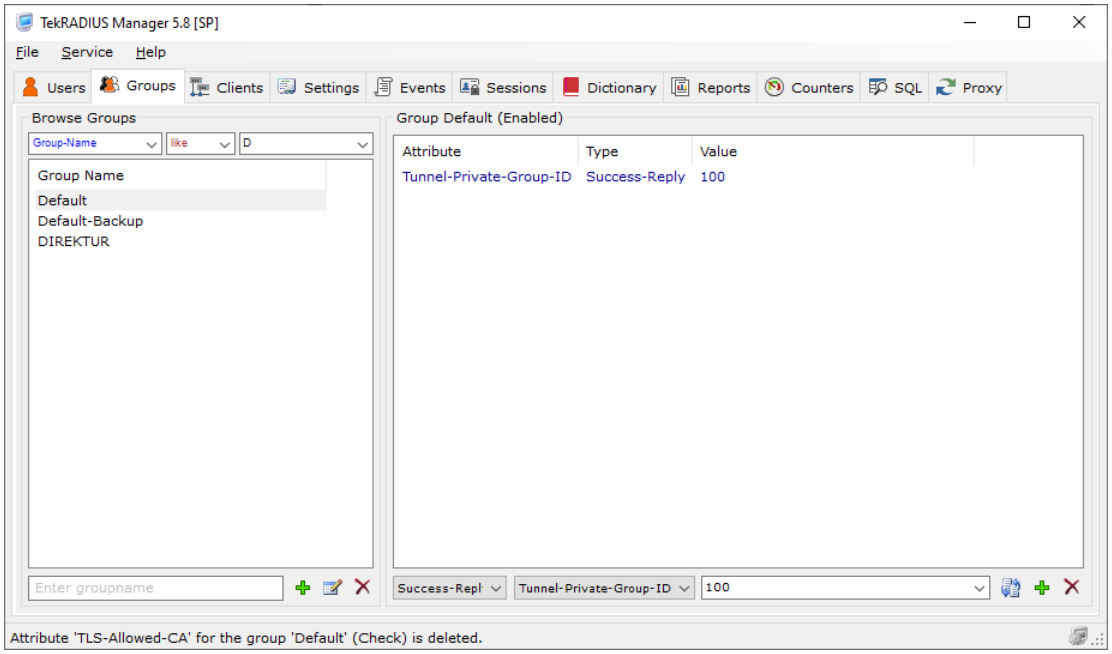
Every user profile in TekRADIUS is associated with a group profile. Group profiles enable you to group common check / reply attributes for a group of users. TekRADIUS allows you to authenticate with a different set of group attributes chained with Next-Group attribute in the primary group. Policy matching allows you to specify an alternative primary user group for an incoming authentication request when user is assigned to the default user group in TekRADIUS. Policy matching is also used to determine local user group for AD/Windows user accounts when there is not a corresponding local user group for the user's primary AD group. Matching based on policy attributes added as check attributes to the group profiles:

- Client-Label
- NAS-IP-Address
- NAS-Identifier
- Service-Type
- Framed-Protocol
- Called-Station-Id
- NAS-Port-Type
- Authentication-Method

User GTest has User-Password attribute as a check attribute and assigned to Default user group:



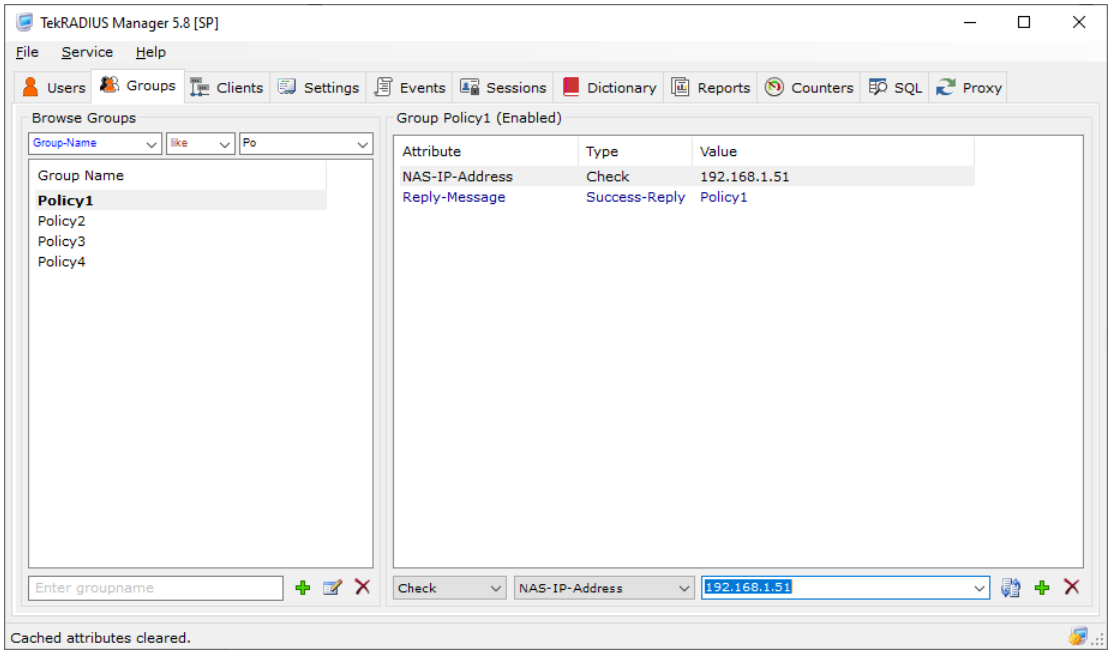
Defautl user group has only Tunnel-Private-Group-ID attribute as a success-reply attribute:




```
23.05.2024 18:58:32.714 - RadAuth req. from 127.0.0.1:61859 [UDP]

 Size            : 64
 Identifier      : 2
 Attributes      :

 User-Name = gtest
 NAS-IP-Address = 192.168.1.51
 Framed-Protocol = 1 (PPP)
 Service-Type = 2 (Framed)

23.05.2024 18:58:32.734 - No group check attribute is configured for user 'gtest' - (default).

23.05.2024 18:58:32.734 - CHAP authentication commencing for user 'gtest'

23.05.2024 18:58:32.734 - CHAP authentication commencing for user 'gtest' (default).

23.05.2024 18:58:32.737 - CHAP authentication is successful for user 'gtest' (default).

23.05.2024 18:58:32.739 - Check items control for user 'gtest' - Start (CHAP) [Group: 'default'].

23.05.2024 18:58:32.739 - Check items control for user 'gtest' - Stop [Group: 'default'].

23.05.2024 18:58:32.739 - Authentication is successful for user 'gtest'

23.05.2024 18:58:32.740 - Fetching Success-Reply items for user 'gtest' - Start.

23.05.2024 18:58:32.744 - Fetching Success-Reply items for user 'gtest' - Stop.

23.05.2024 18:58:32.744 - Generating Reply Packet for user 'gtest' - Start.

23.05.2024 18:58:32.745 - Generating Reply Packet for user 'gtest' - Stop.

23.05.2024 18:58:32.747 - RadAuth reply to 127.0.0.1:61859 (Success)

 Size            : 25
 Identifier      : 2
 Attributes      :

 Tunnel-Private-Group-ID = 100
```

User GTest will be authenticated and authorized by processing attributes in local user profile and Default user group as shown above.

You can create a policy group with NAS-IP-Address = 192.168.1.51 and use as primary group for the authentication requests comes from 192.168.1.51

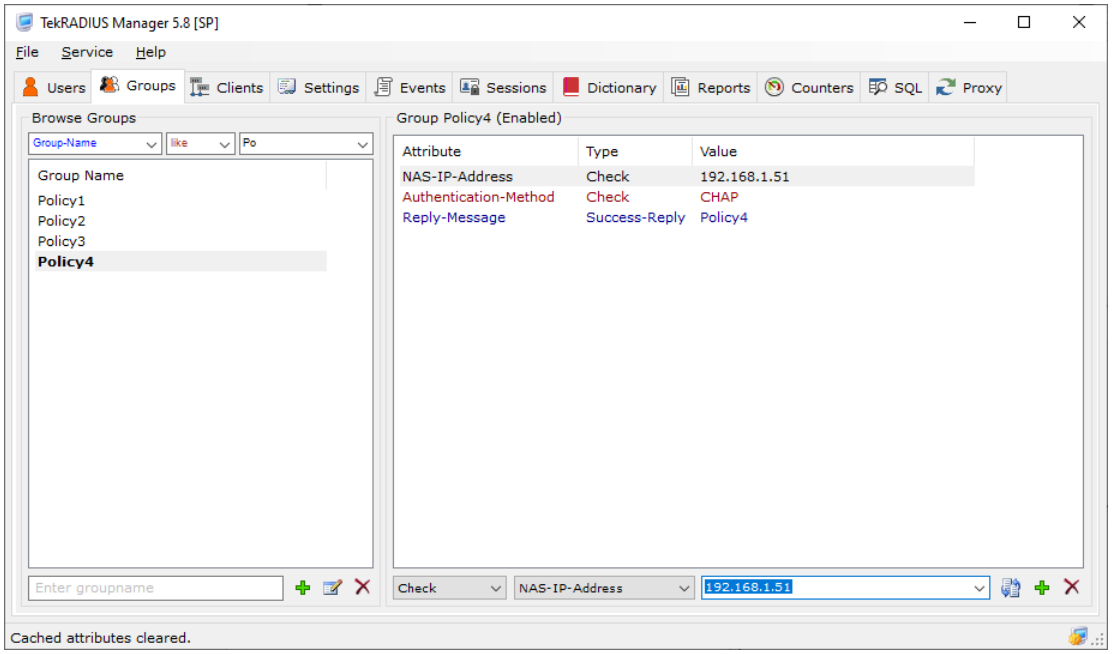



```
23.05.2024 19:01:24.225 - RadAuth req. from 127.0.0.1:55920 [UDP]

 Size              : 64
 Identifier        : 3
 Attributes        :

 User-Name = gtest
 NAS-IP-Address = 192.168.1.51
 Framed-Protocol = 1
 Service-Type = 2

23.05.2024 19:01:24.231 - Group check attribute(s) obtained for user 'gtest' - (Policy1).

23.05.2024 19:01:24.231 - CHAP authentication commencing for user 'gtest'

23.05.2024 19:01:24.231 - CHAP authentication commencing for user 'gtest' (Policy1).

23.05.2024 19:01:24.231 - CHAP authentication is successful for user 'gtest' (Policy1).

23.05.2024 19:01:24.232 - Check items control for user 'gtest' - Start (CHAP) [Group: 'Policy1'].

23.05.2024 19:01:24.232 - Check items control for user 'gtest' - Stop [Group: 'Policy1'].

23.05.2024 19:01:24.232 - Authentication is successful for user 'gtest'

23.05.2024 19:01:24.232 - Fetching Success-Reply items for user 'gtest' - Start.

23.05.2024 19:01:24.234 - Fetching Success-Reply items for user 'gtest' - Stop.

23.05.2024 19:01:24.234 - Generating Reply Packet for user 'gtest' - Start.

23.05.2024 19:01:24.234 - Generating Reply Packet for user 'gtest' - Stop.

23.05.2024 19:01:24.234 - RadAuth reply to 127.0.0.1:55920 (Success)

 Size              : 29
 Identifier        : 3
 Attributes        :

 Reply-Message = Policy1
```

User GTest will be authenticated and authorized by processing attributes in local user profile and Policy1 user group as shown above.

You can also specify a more specific policy. You can match authentication requests from

192.168.1.51 with CHAP authentication method to group named Policy4.




```
23.05.2024 19:04:18.352 - RadAuth req. from 127.0.0.1:58791 [UDP]

 Size              : 64
 Identifier        : 4
 Attributes        :

 User-Name = gtest
 NAS-IP-Address = 192.168.1.51
 Framed-Protocol = 1
 Service-Type = 2

23.05.2024 19:04:18.357 - Group check attribute(s) obtained for user 'gtest' - (Policy4).

23.05.2024 19:04:18.357 - CHAP authentication commencing for user 'gtest'

23.05.2024 19:04:18.357 - CHAP authentication commencing for user 'gtest' (Policy4).

23.05.2024 19:04:18.357 - CHAP authentication is successful for user 'gtest' (Policy4).

23.05.2024 19:04:18.358 - Check items control for user 'gtest' - Start (CHAP) [Group: 'Policy4'].

23.05.2024 19:04:18.358 - Check items control for user 'gtest' - Stop [Group: 'Policy4'].

23.05.2024 19:04:18.358 - Authentication is successful for user 'gtest'

23.05.2024 19:04:18.358 - Fetching Success-Reply items for user 'gtest' - Start.

23.05.2024 19:04:18.361 - Fetching Success-Reply items for user 'gtest' - Stop.

23.05.2024 19:04:18.361 - Generating Reply Packet for user 'gtest' - Start.

23.05.2024 19:04:18.361 - Generating Reply Packet for user 'gtest' - Stop.

23.05.2024 19:04:18.361 - RadAuth reply to 127.0.0.1:58791 (Success)

 Size              : 29
 Identifier        : 4
 Attributes        :

 Reply-Message = Policy4
```

TekRADIUS always select the group with the most matched attributes. If multiple groups are matched TekRADIUS will fall back to the Default group.