Parallels RAS Multi-Factor RADIUS Authentication Setup[1]

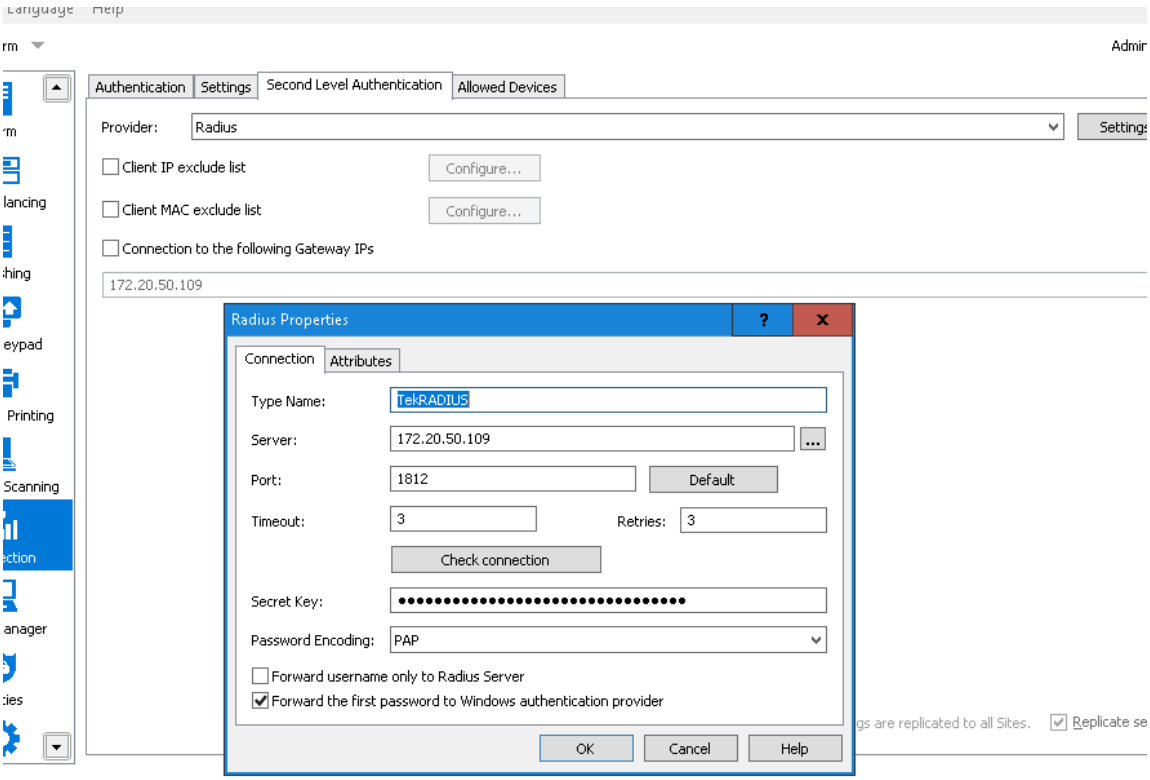
You can deploy TekRADIUS with Parallels RAS for Multi-Factor RADIUS Authentication. Parallels RAS allows you to use multi-factor authentication for access control by configuring a second level authentication.

Parallels Configuration

Parallels RAS allows you to use multi-factor authentication for access control by configuring multiple levels of authentication.

When multi-level authentication is used, users will have to authenticate through two or more successive stages to get the application list. While the first level authentication will always use native authentication (Active Directory / LDAP), other levels can use supported authentication providers like Google Authenticator.

Multi-level of authentication is more secure because instead of using a standard username and password, it uses a static username and a one-time password generated by a token.
Multi-Level Authentication can be configured from the Second Level Authentication tab in the Connection category.



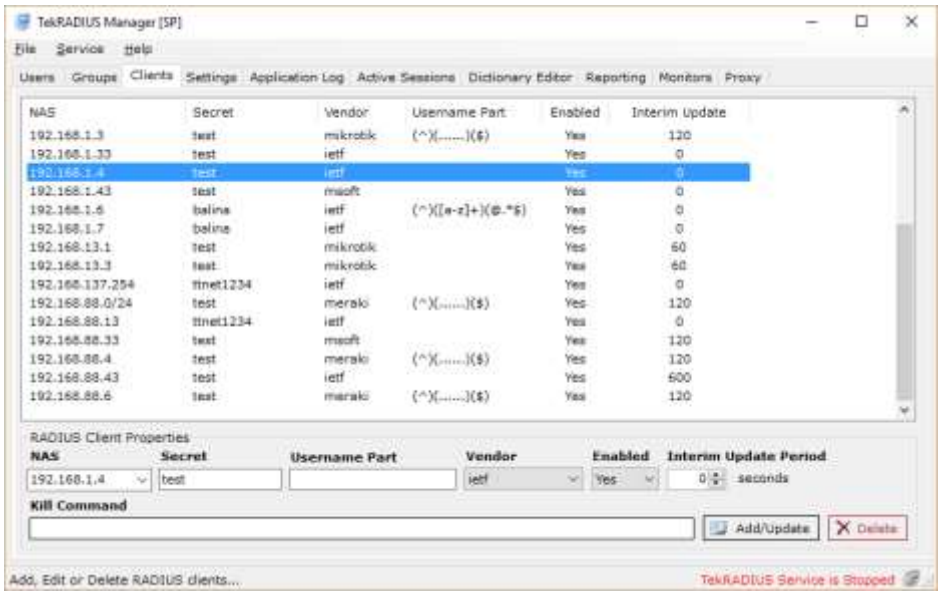
[1] Contributed by Frans Rampen (Frans.Rampen@yoda-ict.nl)

TekRADIUS Configuration

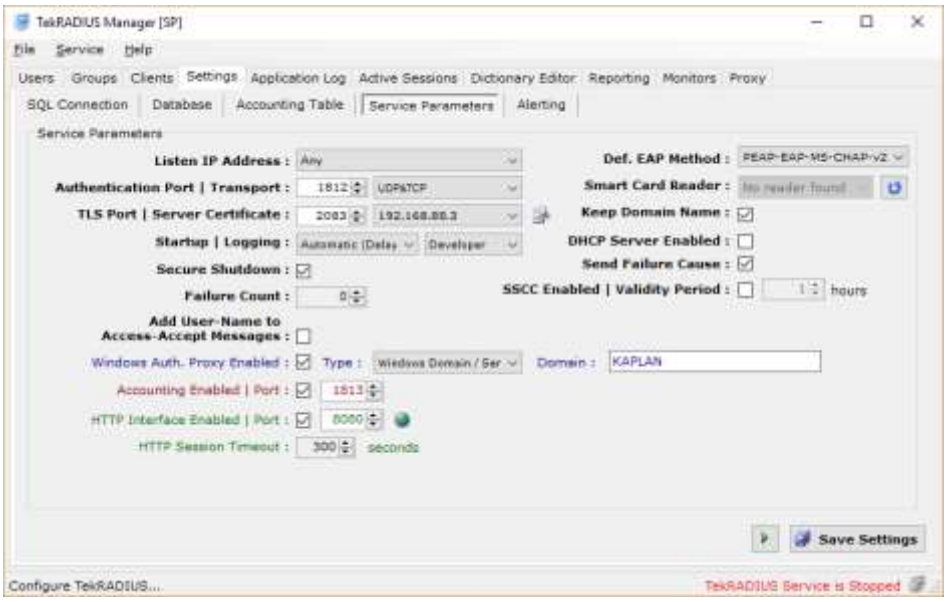
Using second level authentication within Parallels basically replaces standard Authentication provider with TekRADIUS. So TekRADIUS determines if Multi-Level authentication is required or not.

You can authenticate built-in user profiles or Active Directory users *(Commercial editions only)* with TekRADIUS. Google Authenticator will be used as Second Level Authentication in this example. Please note that Google Authenticator is supported only in commercial editions of TekRADIUS.

Add a client entry for Parallels in TekRADIUS Manager / Clients tab. Enter IP address of the Parallels RAS and a secret key.



Windows Auth. Proxy feature will be used in this sample configuration. You can enable Windows Auth. Directory Proxy at Settings / Service Parameters. TekRADIUS must be installed on domain member server for proper operation.



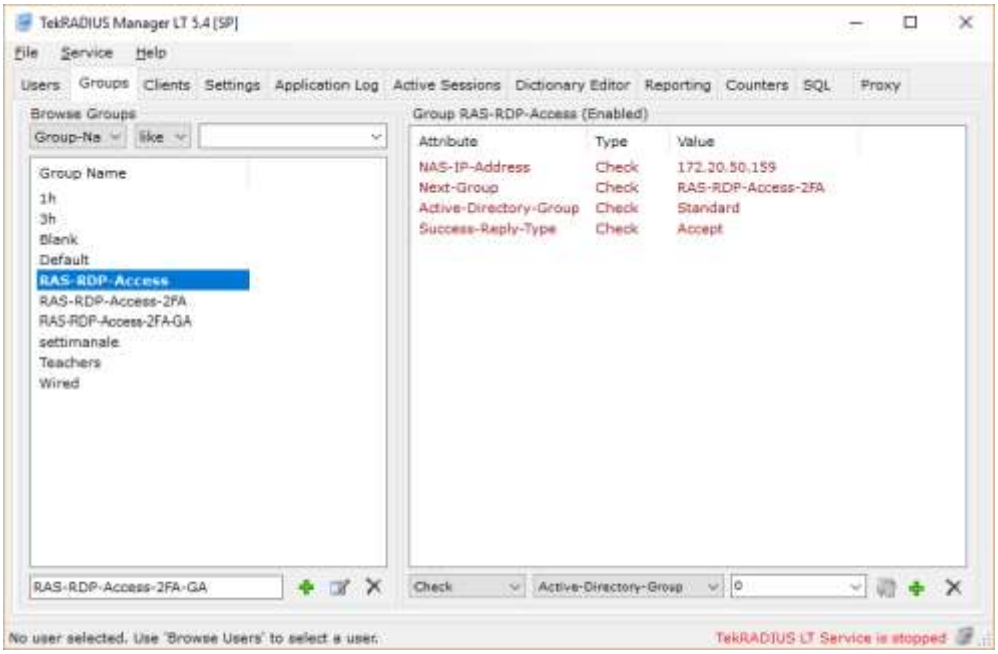
Some of users do not want to have extra authentication; only username/password. In TekRADIUS we have two group profiles matching active directory groups with or without OTP. You need two extra AD groups in your AD; Standard for plain Active Directory authentication, Access-2FA for Google-Authenticator after AD authentication and a dummy group called “TekRADIUS-Default”. Group profile configuration in TekRADIUS;

TekRADIUS Group "Default" *(This is entry group)*

- Active-Directory-Group = TekRADIUS-Default *(Check)*
- Next-Group = RAS-RDP-Access *(Check)*

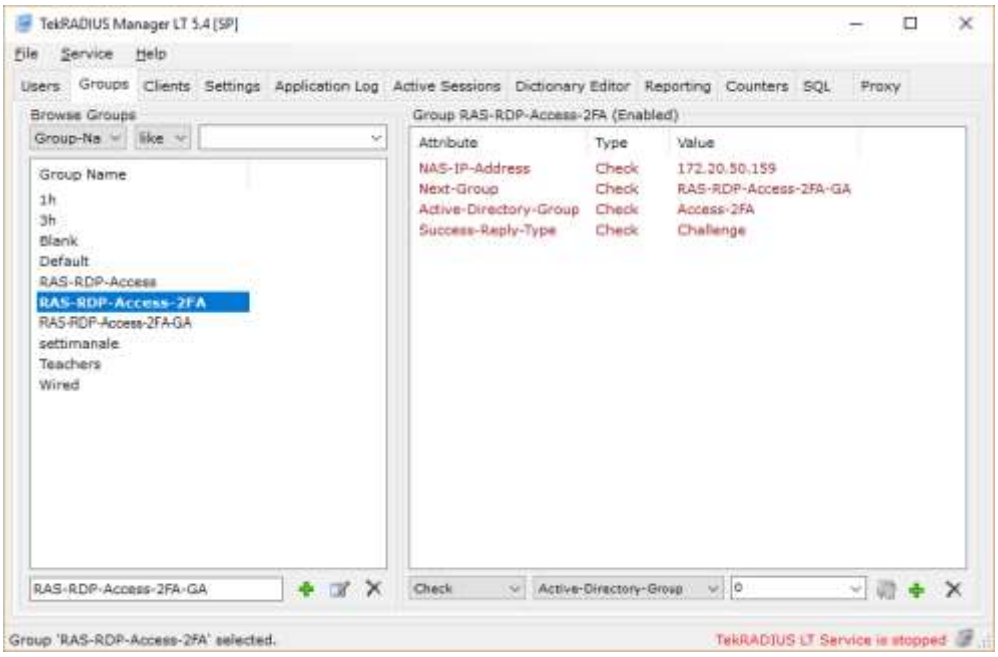
TekRADIUS Group "RAS-RDP-Access" *(This one authenticates plain AD users, falls back to RAS-RDP-Access-2FA if authentication fails)*

- Active-Directory-Group = Standard *(Check)*
- Success-Reply-Type = Accepts *(Check)*
- Next-Group = RAS-RDP-Access-2FA



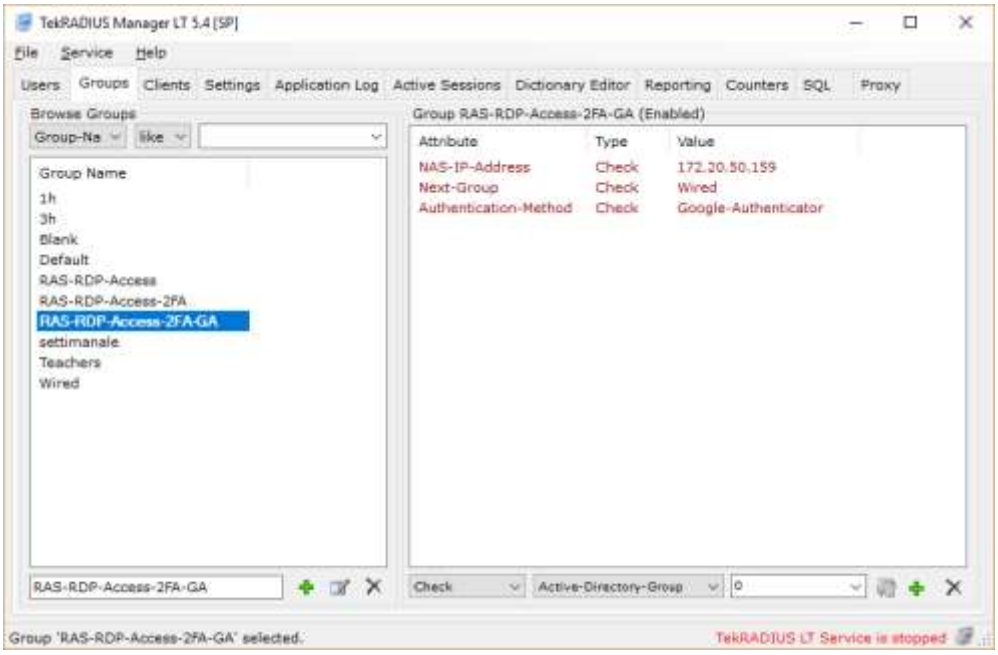
TekRADIUS Group "RAS-RDP-Access-2FA" *(Sends challenge for Google-Authenticator phase if AD authentication is successful)*

- Active-Directory-Group = Access-2FA *(Check)*
- Next-Group = RAS-RDP-Access-2FAGA *(Check)*
- Success-Reply-Type = Challenge *(Check)*



TekRADIUS Group "RAS-RDP-Access-2FAGA" *(This is the final phase for Google-Authenticator)*

- Authentication-Method = Google-Authenticator *(Check)*



Primary group for a user must be Access-2FA in this configuration and TekRADIUS HTTP interface should display GA initiator icon when a user logins to TekRADIUS HTTP interface with AD credentials.

TekRADIUS sends an Accept Reply-Type after authentication of the credentials and successful active directory membership:

RAS Log:

```
[I 06/0000000E/T00001058] Tue Mar 20 11:11:12 2018 - User (user@company.domain) connected
from client (10.10.11.9:51501), machine (CLIENT)(14-DD-A9-2B-CB-4D) mode Gateway SSL,
using OS: Microsoft Windows 10 Enterprise Edition (x64) , Client version: 16.2 (build
19160).
[I 0E/00000000/T00001058] Tue Mar 20 11:11:13 2018 - Radius 172.20.50.109: User
user@company.domain from machine CLIENT access allowed.
[I 06/0000000E/T00001058] Tue Mar 20 11:11:13 2018 - Logon successful user
'user@company.domain' client IP '188.92.60.180' gateway IP '172.21.50.109' [47 31 0 0]
[I 06/00000040/T00001058] Tue Mar 20 11:11:13 2018 - Client Rules: rule 'Default Policy'
matched. User: user_domain Gateway: 172.21.50.109 Mac Address: 14-DD-A9-2B-CB-4D
```

TekRADIUS log:

```
20.03.2018 11:11:12.549 - RadAuth req. from : 172.20.50.109:51592 [UDP]
Size              : 64 / 64
Identifier        : 1
Attributes        :

NAS-IP-Address = 172.20.50.109
User-Name = user@company.domain

20.03.2018 11:11:12.550 - Authentication query; for user 'user@company.domain'; SELECT
Attribute, Val from Users where UserName = 'user@company.domain' and AttrType = 0
20.03.2018 11:11:12.587 - Active Directory Authentication commencing for user
'user@company.domain'
20.03.2018 11:11:12.814 - Check items control for user 'user@company.domain' - Start
(Group: Default) [ActiveDirectory].
20.03.2018 11:11:12.829 - Validating Active Directory group membership for user
'user@company.domain' (TekRADIUS-Default, company.domain).
20.03.2018 11:11:12.829 - Getting Active Directory group membership information for user
'user@company.domain' (TekRADIUS-Default, company.domain [company.domain]).
20.03.2018 11:11:13.038 - Active Directory group membership validation failed for user
'user@company.domain'. No group information obtained.
20.03.2018 11:11:13.038 - Active Directory group does not match (TekRADIUS-Default).
20.03.2018 11:11:13.038 - Check items control for user 'user@company.domain' - Stop
(Default).
20.03.2018 11:11:13.056 - Check items control for user 'user@company.domain' - Start
(Group: RAS-RDP-Access) [ActiveDirectory].
20.03.2018 11:11:13.073 - Validating Active Directory group membership for user
'user@company.domain' (Standard, company.domain).
20.03.2018 11:11:13.073 - Getting Active Directory group membership information for user
'user@company.domain' (Standard, company.domain [company.domain]).
20.03.2018 11:11:13.138 - Active Directory group membership validation successful for
user 'user@company.domain'.
20.03.2018 11:11:13.138 - Check items control for user 'user@company.domain' - Stop (RAS-
RDP-Access).
20.03.2018 11:11:13.138 - Active Directory authentication successfull for user
'user@company.domain'
20.03.2018 11:11:13.138 - Fetching Success-Reply items for user 'user@company.domain' -
Start.
20.03.2018 11:11:13.139 - Fetching Success-Reply items for user 'user@company.domain' -
Stop.
```

TekRADIUS sends challenge back top RAS if windows authentication was successful followed by Google Authentication.

RAS Log:

```
[I 06/0000000E/T00000F24] Tue Mar 20 11:19:32 2018 - User (rastest@company.domain)
connected from client (10.10.11.9:51760), machine (CLIENT)(14-DD-A9-2B-CB-4D) mode
Gateway SSL, using OS: Microsoft Windows 10 Enterprise Edition (x64) , Client version:
16.2 (build 19160).
[I 0E/00000000/T00000F24] Tue Mar 20 11:19:32 2018 - Radius 172.20.50.109: User
rastest@company.domain from machine CLIENT is challenged.
[I 0E/00000000/T00000F24] Tue Mar 20 11:19:41 2018 - Radius 172.20.50.109: User
rastest@company.domain from machine CLIENT access allowed.
[I 06/0000000E/T00000F24] Tue Mar 20 11:19:41 2018 - Logon successful user
'rastest@company.domain' client IP '188.92.60.180' gateway IP '172.21.50.109' [47 31 0 0]
[I 06/00000040/T00000F24] Tue Mar 20 11:19:41 2018 - Client Rules: rule 'YodaCLoud
Default Policy' matched. User: rastest_domain Gateway: 172.21.50.109 Mac Address: 14-DD-
A9-2B-CB-4D
```

TekRADIUS Log:

```
20.03.2018 11:19:32.147 - RadAuth req. from : 172.20.50.109:63709 [UDP]
Size              : 58 / 58
Identifier        : 1
Attributes        :

NAS-IP-Address = 172.20.50.109
User-Name = rastest@company.domain

20.03.2018 11:19:32.147 - Authentication query; for user 'rastest@company.domain'; SELECT
Attribute, Val from Users where UserName = 'rastest@company.domain' and AttrType = 0
20.03.2018 11:19:32.173 - Active Directory Authentication commencing for user
'rastest@company.domain'
20.03.2018 11:19:32.195 - Check items control for user 'rastest@company.domain' - Start
(Group: Default) [ActiveDirectory].
20.03.2018 11:19:32.207 - Validating Active Directory group membership for user
'rastest@company.domain' (TekRADIUS-Default, company.domain).
20.03.2018 11:19:32.207 - Getting Active Directory group membership information for user
'rastest@company.domain' (TekRADIUS-Default, company.domain [company.domain]).
20.03.2018 11:19:32.316 - Active Directory group membership validation failed for user
'rastest@company.domain'. No group information obtained.
20.03.2018 11:19:32.316 - Active Directory group does not match (TekRADIUS-Default).
20.03.2018 11:19:32.316 - Check items control for user 'rastest@company.domain' - Stop
(Default).
20.03.2018 11:19:32.330 - Check items control for user 'rastest@company.domain' - Start
(Group: RAS-RDP-Access) [ActiveDirectory].
20.03.2018 11:19:32.342 - Validating Active Directory group membership for user
'rastest@company.domain' (Access-2FA, company.domain).
20.03.2018 11:19:32.342 - Getting Active Directory group membership information for user
'rastest@company.domain' (Access-2FA, company.domain [company.domain]).
20.03.2018 11:19:32.412 - Active Directory group membership validation failed for user
'rastest@company.domain'. No group information obtained.
20.03.2018 11:19:32.412 - Active Directory group does not match (Access-2FA).
20.03.2018 11:19:32.412 - Check items control for user 'rastest@company.domain' - Stop
(RAS-RDP-Access).
20.03.2018 11:19:32.425 - Check items control for user 'rastest@company.domain' - Start
(Group: RAS-RDP-Access-2FA) [ActiveDirectory].
20.03.2018 11:19:32.437 - Validating Active Directory group membership for user
'rastest@company.domain' (Access-2FA).
20.03.2018 11:19:32.437 - Getting Active Directory group membership information for user
'rastest@company.domain' (Access-2FA, company.domain [company.domain]).
20.03.2018 11:19:32.504 - Active Directory group membership validation successful for
user 'rastest@company.domain'.
20.03.2018 11:19:32.504 - Check items control for user 'rastest@company.domain' - Stop
(RAS-RDP-Access-2FA).
```

```
20.03.2018 11:19:32.504 - Active Directory authentication successful for user
'rastest@company.domain'
20.03.2018 11:19:32.504 - Fetching Success-Reply items for user 'rastest@company.domain'
- Start.
20.03.2018 11:19:32.504 - Fetching Success-Reply items for user 'rastest@company.domain'
- Stop.
20.03.2018 11:19:32.504 - Generating Reply Packet - Start.
20.03.2018 11:19:32.505 - Generating Reply Packet - Stop.

20.03.2018 11:19:32.505 - RadAuth reply to  : 172.20.50.109:63709 (Failure)
Size              : 54
Identifier        : 1
Attributes        :

State = 5417647261A3D24A94B9E8C5E445FF08

20.03.2018 11:19:41.779 - RadAuth req. from : 172.20.50.109:63709 [UDP]
Size              : 92 / 92
Identifier        : 1
Attributes        :

State = 5417647261A3D24A94B9E8C5E445FF08
NAS-IP-Address = 172.20.50.109
User-Name = rastest@company.domain

20.03.2018 11:19:41.782 - GoogleAuthenticator Authentication commencing for user
'rastest@company.domain'
20.03.2018 11:19:41.782 - Check items control for user 'rastest@company.domain' - Start
(Group: RAS-RDP-Access-2FA-GA) [GoogleAuthenticator].
20.03.2018 11:19:41.782 - Check items control for user 'rastest@company.domain' - Stop
(RAS-RDP-Access-2FA-GA).
20.03.2018 11:19:41.782 - Google Authenticator authentication successful for user
'rastest@company.domain'
20.03.2018 11:19:41.782 - Fetching Success-Reply items for user 'rastest@company.domain'
- Start.
20.03.2018 11:19:41.782 - Fetching Success-Reply items for user 'rastest@company.domain'
- Stop.
```

If a third level authentication is required; just return ‘Challenge’ as Reply-Type on Google Authenticator and configure another authentication method using groups.