One Time Password

A one-time password (OTP) is a unique, temporary code used for a single login session or transaction. Unlike traditional passwords, which remain the same until changed, OTPs are dynamic and can only be used once.

Using a third party authenticator, such as Google Authenticator, 2FAS, Authy etc, your TapeTrack login, once activated, will need your user name, password and a one time code to be successful.

Ensure your computer, server and device is set to the correct geographical location and time zone to have accurate one time passwords created

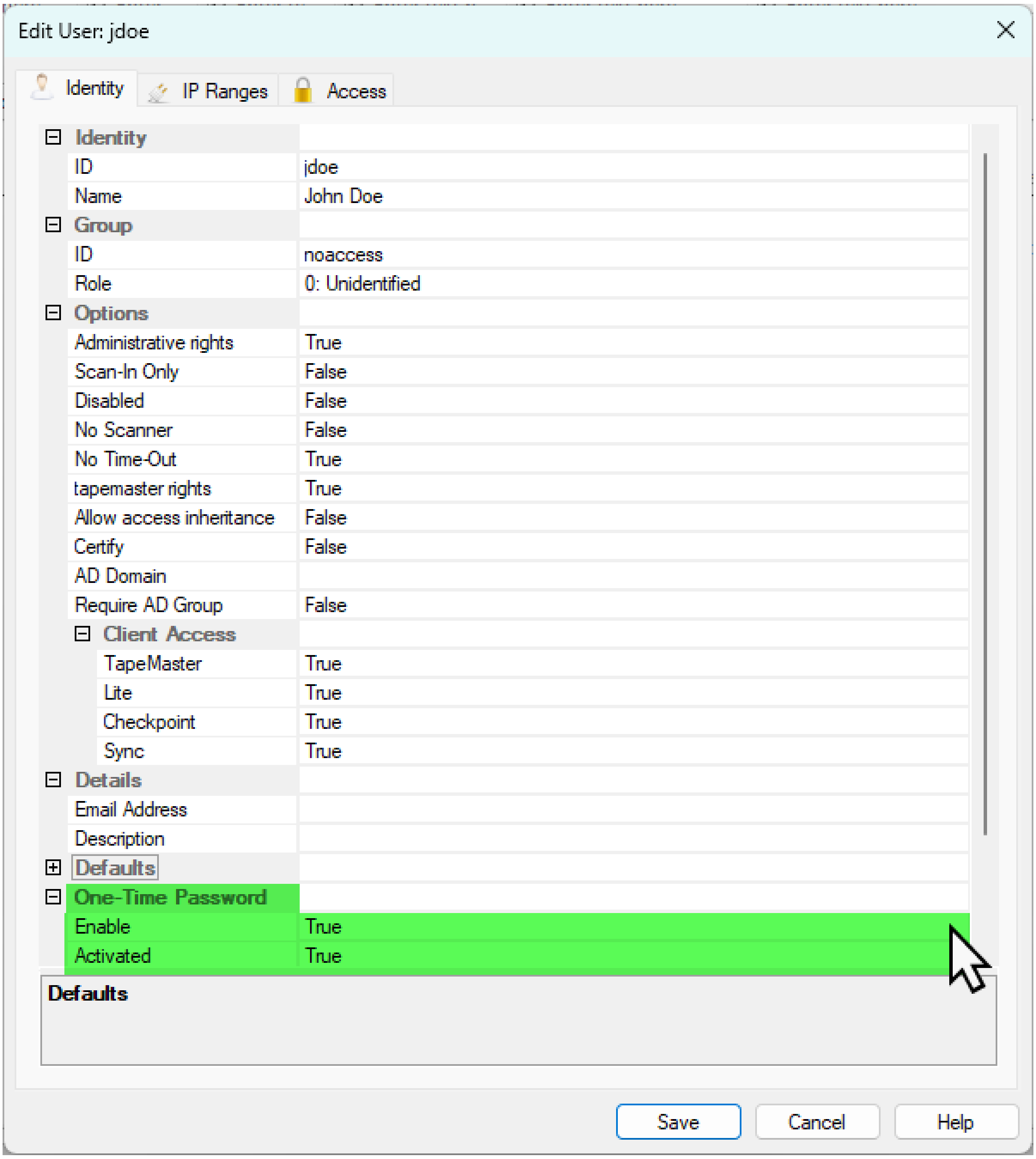
Enabling One Time Password

Open the user's profile you want to enable the OTP option via TapeMaster `Administration` > `Group User Administration`

Open the user-id by right clicking and selecting `Properties`, or double clicking.

Select the `Identity` tab.

Set the field `One Time Password` to `True`. This will display an extra field `Activated`, set to `False`. Once the user has successfully set up the one time password and logged in using a successful code this field will display `True` to signify the one time password is now required for all future login attempts with TapeTrack desktop software.



⊟ **Identity**	
ID	jdoe
Name	John Doe
⊟ **Group**	
ID	noaccess
Role	0: Unidentified
⊟ **Options**	
Administrative rights	True
Scan-In Only	False
Disabled	False
No Scanner	False
No Time-Out	True
tapemaster rights	True
Allow access inheritance	False
Certify	False
AD Domain	
Require AD Group	False
⊟ **Client Access**	
TapeMaster	True
Lite	True
Checkpoint	True
Sync	True
⊟ **Details**	
Email Address	
Description	
⊞ **Defaults**	
⊟ **One-Time Password**	
Enable	True
Activated	True

Defaults

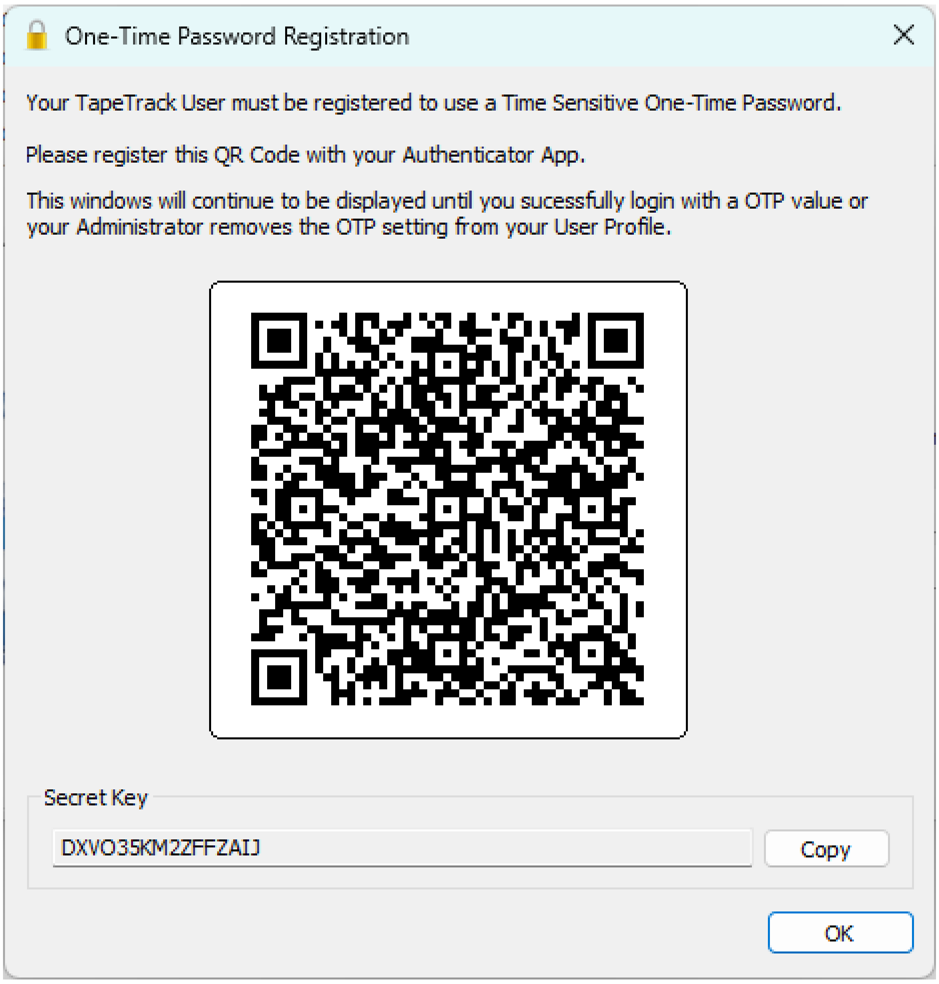
Once a user has activated the one time password function, all desktop software they use (eg TapeMaster, Checkpoint, Lite etc) will need to be a current version with the OTP function to be able to login.

Setting Up Authenticator

Load your choice of authenticator app on your device. The decision of what authenticator app to use is down to personal preference and your companies IT polices and approved apps.

Log into to your choice of TapeTrack desktop software (TapeMaster, Checkpoint or Lite) with your current user-id and password. Click OK

Yow will be presented with a QR code to add your key to the authenticator app, scan to add the code or use the `Secret` Key value to enter it manually.



One-Time Password Registration

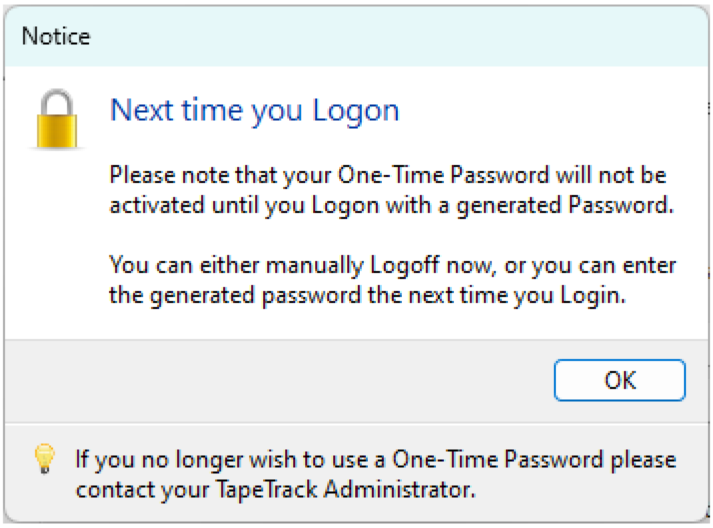
Your TapeTrack User must be registered to use a Time Sensitive One-Time Password.

Please register this QR Code with your Authenticator App.

This windows will continue to be displayed until you sucessfully login with a OTP value or your Administrator removes the OTP setting from your User Profile.

Secret Key: DXVO35KM2ZFFZAIJ

This QR code will be displayed each time you login until you have logged in successfully using the OTP.



Notice

Next time you Logon

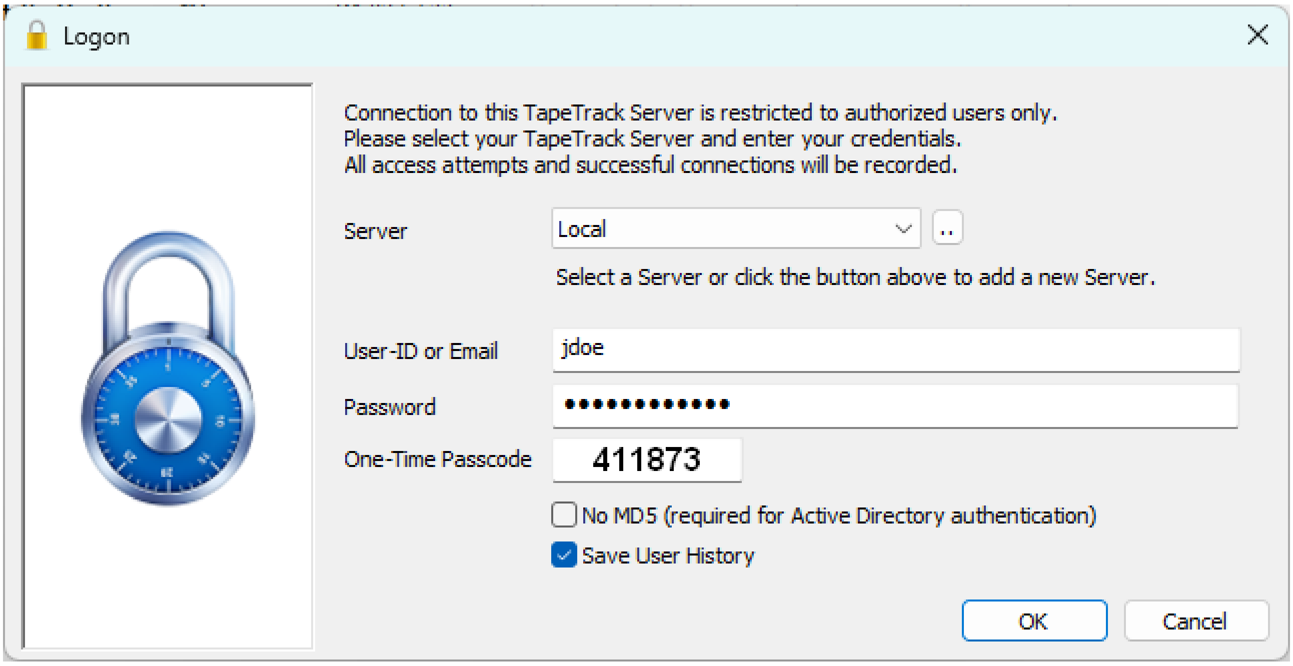
Please note that your One-Time Password will not be activated until you Logon with a generated Password.

You can either manually Logoff now, or you can enter the generated password the next time you Login.

If you no longer wish to use a One-Time Password please contact your TapeTrack Administrator.

Activate One Time Password

Log out of TapeTrack and log back in, this time using your user-id, password and OTP.



Connection to this TapeTrack Server is restricted to authorized users only.
Please select your TapeTrack Server and enter your credentials.
All access attempts and successful connections will be recorded.

Server: Local

Select a Server or click the button above to add a new Server.

User-ID or Email: jdoe

Password: ●●●●●●●●●●●●●

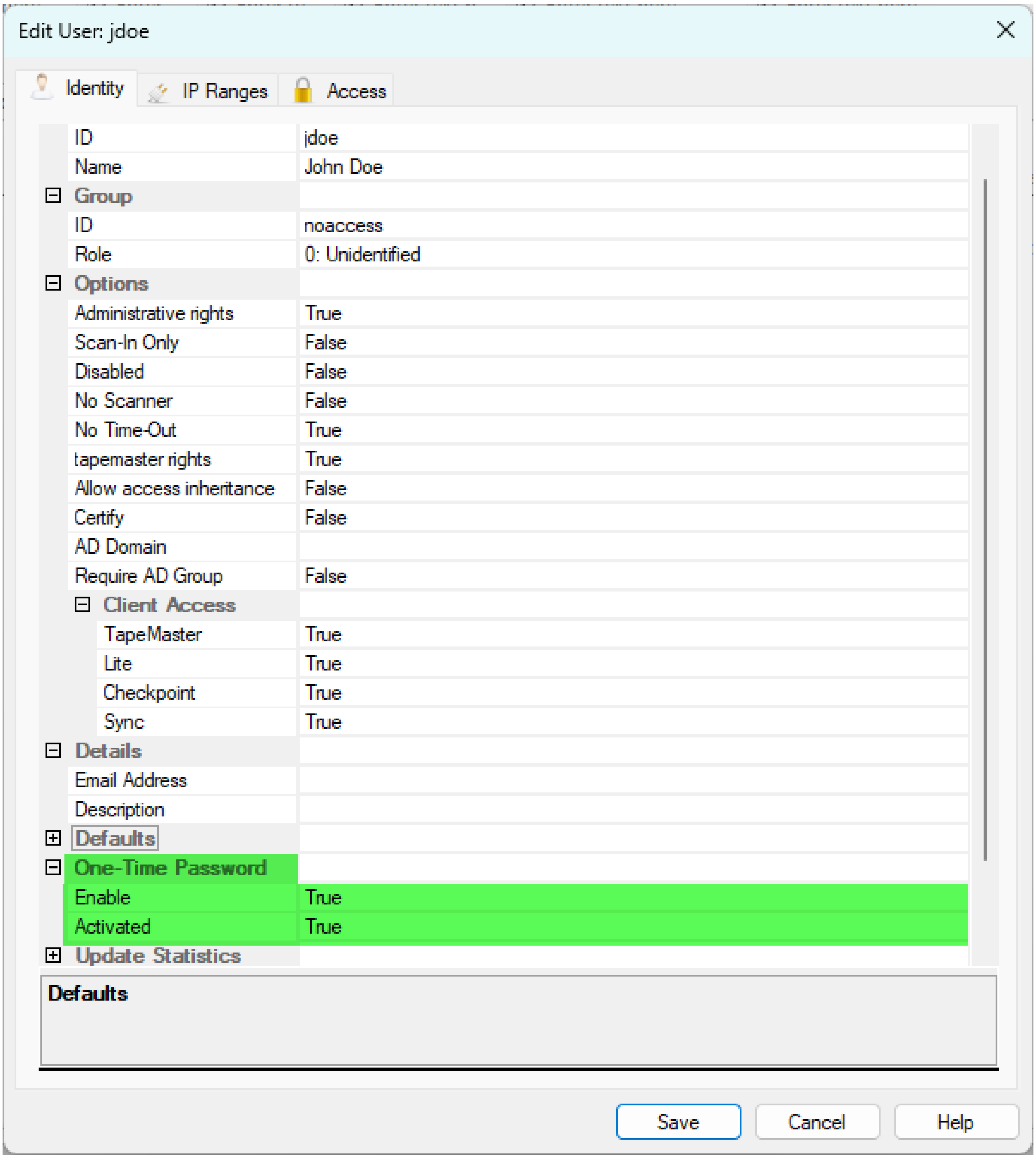
One-Time Passcode: 411873

☐ No MD5 (required for Active Directory authentication)

☑ Save User History

As you have not activated the OTP feature until after a successful login using the OTP value, the QR code will display again. Simply click `OK` on both the popups and continue for connection. Once you have logged in the OTP is now activated and the QR popup will no longer be displayed on login.

Once the user-id has activated the OTP function, the user-id `identity` tab will now display the OTP activated field as `True`.



ID	jdoe
Name	John Doe
⊟ Group	
ID	noaccess
Role	0: Unidentified
⊟ Options	
Administrative rights	True
Scan-In Only	False
Disabled	False
No Scanner	False
No Time-Out	True
tapemaster rights	True
Allow access inheritance	False
Certify	False
AD Domain	
Require AD Group	False
⊟ Client Access	
TapeMaster	True
Lite	True
Checkpoint	True
Sync	True
⊟ Details	
Email Address	
Description	
⊞ Defaults	
⊟ One-Time Password	
Enable	True
Activated	True
⊞ Update Statistics	

Defaults

Lost One Time Password Access

If a user that has the OTP activated loses access to their authenticator (lost or damaged device etc), setting the One Time Password `Enabled` field to `False` will turn off the requirement to enter a OTP when logging in.

Setting the One Time Password `Enabled` field to `True` will restart the adding OTP process for the user upon login. The secret key will have changed and will need to be added to the new device and then used to login to activate the OTP function.