Client authentication with Duo Mobile Push notification and RADIUS

An additional User Validation option has been introduced in NetSupport Manager 14.00 to allow the use of Duo Mobile Push notifications with RADIUS to authenticate the NetSupport Manager Control Console user when connecting to a NetSupport Manager 14.00 Client machine.

This provides per-Client machine connection authentication and allows enhanced validation to confirm that the Control Console user attempting to connect to the Client machine is authorised.

As well as being a standalone authentication method, RADIUS can also be used in conjunction with one of the following User Validation options to apply additional authentication to the Control Console user:

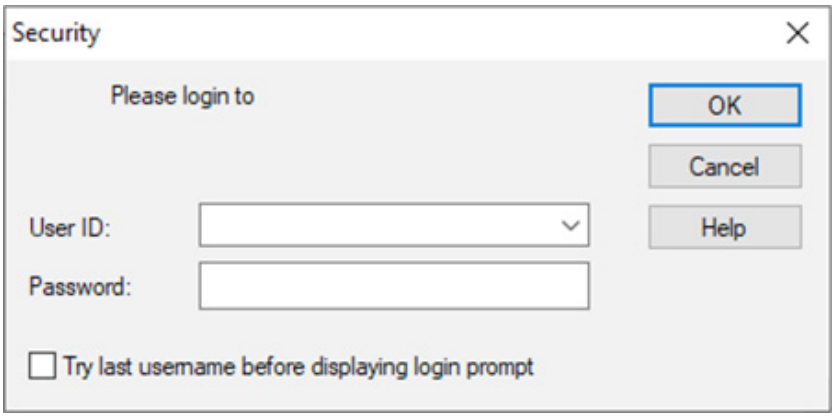
- NT Options (including Smart Card)
- Active Directory Options

For the Duo Mobile with RADIUS authentication feature to work, there are several pre-requisites that need to be in place in your environment:

1. You have installed and configured the Duo Authentication Proxy/RADIUS server on a machine within your network. Full instructions on how to install and configure the Duo Authentication Proxy/RADIUS server can be found in this document:
   https://duo.com/docs/radius
2. You have pre-enrolled your list of Duo users that will be used by the Client machine to authenticate the connection request from the Control Console. Full instructions on how to create the Duo users or synchronise the Duo users from your Active Directory can be found in this document:
   https://duo.com/docs/enrolling-users
3. You have a record of the FQDN of the machine where the Duo Authentication Proxy/RADIUS server is installed, along with the unencrypted value of the secret key.

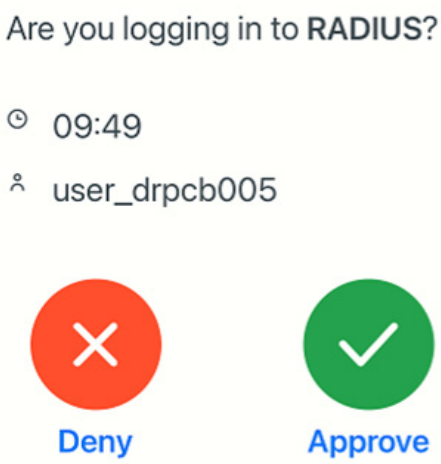
Example of Client RADIUS authentication using Duo Mobile Push notification

1. The NetSupport Manager Control Console user attempts to connect to a NetSupport Manager Client machine.
2. The Client machine initiates the user validation check, and the Control Console user is prompted to enter their username and password, which have been configured in the RADIUS infrastructure.



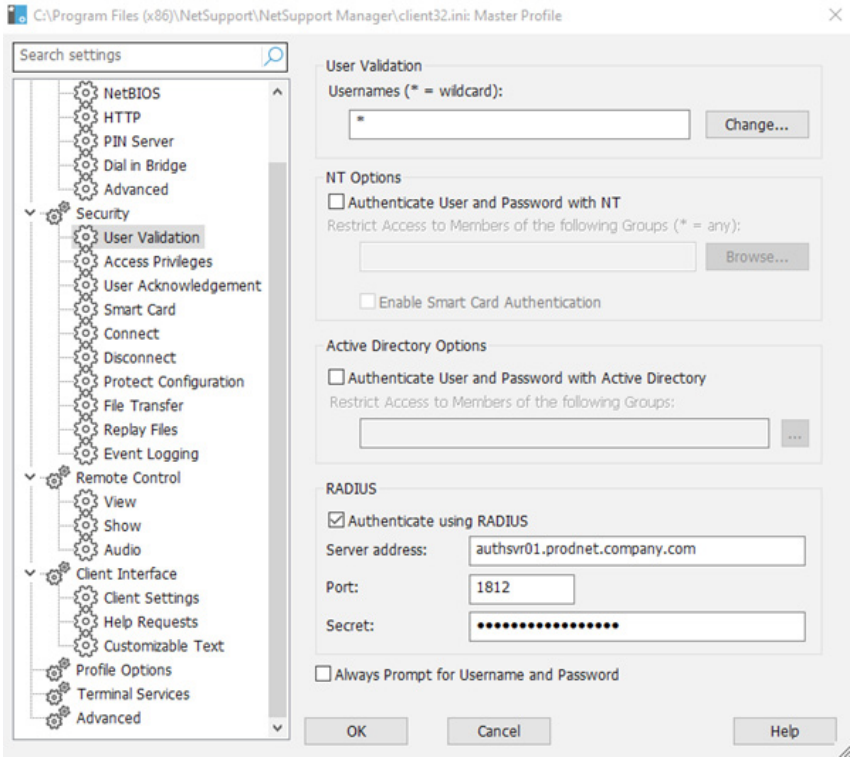
3. The user authentication request is sent by the Client machine to the RADIUS server and the Control Console user sees a message saying that the Client connection is waiting for the RADIUS authentication.

4. The Control Console user receives a push authentication request from RADIUS on the Duo Mobile app that they have registered on their mobile phone or tablet device.



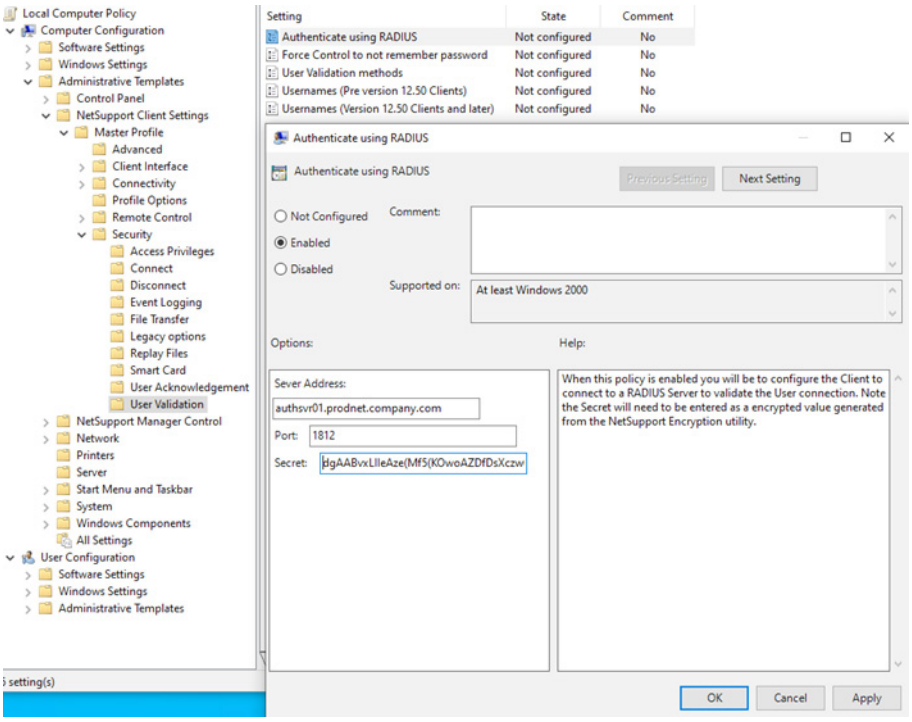
5. The Control Console user can then approve the connection to the Client machine or deny it if they were not the user who initiated it.
6. If the NT Options or Active Directory Options are also configured on the Client machine for user validation, the Control Console user may need to complete extra two-factor authentication processes before the connection to the Client machine is completed.

Client configuration
Local Client files configuration



1. Open the NetSupport Manager Client Configurator.
2. Select **Advanced**.
3. Double-click **Master Profile**.
4. Select **Security** - **User Validation**.
5. Enable the **Authenticate using RADIUS** option.
6. Enter the FQDN of the Duo Authentication Proxy/RADIUS server machine in the **Server address** field.
7. Enter the connection port number (or leave as the default 1812).
8. Enter the unencrypted value of the secret key. Due to the complexity of the secret key, we recommend that this is copied and pasted into the field to avoid any mistyping.
   Note: *Once entered, the secret key is stored as an encrypted value in the Client configuration file.*
9. Click **OK** to accept the changes and **Save** to save the changes to the local Client client32.ini and client32u.ini configuration files (C:\Program Files (x86)\NetSupport\NetSupport Manager by default).
10. The Client configuration file can then be deployed to the other Client machines in the environment to apply the required settings.

Group Policy configuration



1. Use the instructions in the following technical article to add the ADMX and ADML files to the Group Policy Management server: *How to apply the NetSupport Manager ADMX files*.
2. Create a new Group Policy using the Group Policy Management Console.
   Note: *We recommend that a machine-based Group Policy is configured to apply the same Client configuration to all users who log onto the Client machines.*
3. Select the **Security** | **User Validation** section shown in the above screenshot.
4. Double-click the **Authenticate using RADIUS** entry.
5. Select **Enabled** and enter the FQDN of the Duo Authentication Proxy/RADIUS server machine in the S**erver Address** field.
6. Enter the connection port number (or leave as the default 1812).
7. Enter the encrypted value of the secret key.
   Note: *The encrypted secret key value can be copied from the RADIUSSecret= entry in the client32.ini and/or client32u.ini file on a Client machine where the RADIUS authentication configuration has been applied locally.*
8. Click **Apply** and **OK** to save the setting.
9. Configure any additional settings for the Client configuration and close the Policy window.
10. Link the Group Policy to the OU(s) that contain the NetSupport Manager Client machine computer accounts.

Additional information

The **Authenticate using RADIUS** option can be configured on the Client machines as a per-Client Profile setting. This means that the Master Profile can be configured to require RADIUS authentication, as it can use all the features of the NetSupport Manager Control Console, and a different profile with more restricted Client features can be configured not to require RADIUS authentication.

In short, any Client profile that does not require enhanced user authentication should have more restricted Client features once they are connected, with the more advanced Client features reserved for the profiles of Control Console users who have had their identities more rigorously validated.

Instructions on how to create multiple Client profiles can be found in the following technical article: *Creating multiple Client profiles within NetSupport Manager.*