Configuring Duo two-factor authentication in NetSupport Manager

This document explains how to enable and configure two-factor authentication (2FA) within NetSupport Manager via Duo. It is assumed that you have already installed the NetSupport Manager Gateway component and have Controls and Clients configured to use this.

System prerequisites:

- The Gateway needs to be running NetSupport Manager version 14.00 or above.
- All Controls and Clients you wish to use 2FA on must be running version 14 or above.
- A paid Duo subscription is required. The free evaluation account is not supported as there is no Admin API for evaluation accounts.

Obtaining the required Duo information

In order to enable Duo 2FA, the Gateway Server requires the following information from your Duo account:

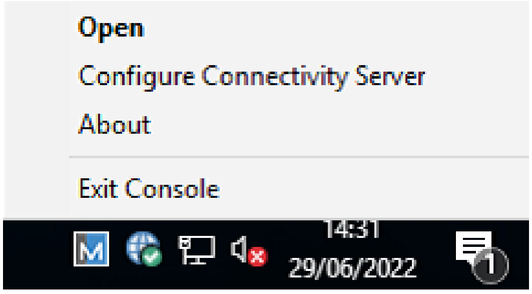
- API hostname
- Auth API integration key
- Auth API secret key
- Admin API integration key
- Admin API secret key

These details can be obtained from your Duo Admin panel and are located under **Dashboard** > **Applications**.

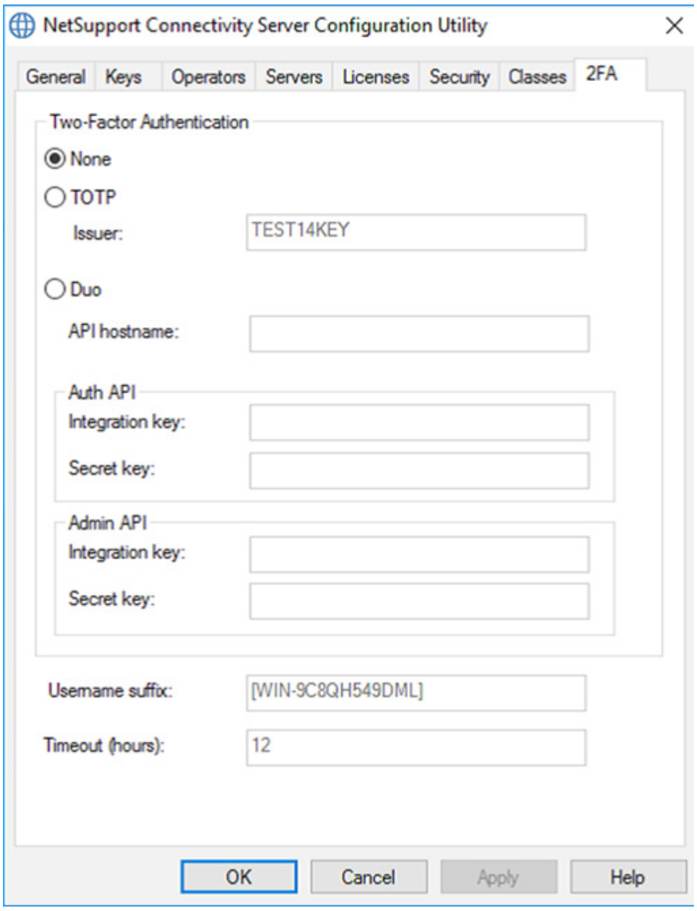
Note: *An 'Owner' level Duo administration account is required to obtain the Admin API information.*

Configuring Duo 2FA on the Gateway Server

To access the Gateway configuration, right-click the **Gateway Server** icon in the system tray and select **Configure Connectivity Server**.



The NetSupport Connectivity Server Configuration Utility will appear. Select the 2FA tab.



NetSupport Connectivity Server Configuration Utility

Two-Factor Authentication

● None

○ TOTP

Issuer: TEST14KEY

○ Duo

API hostname:

Auth API

Integration key:

Secret key:

Admin API

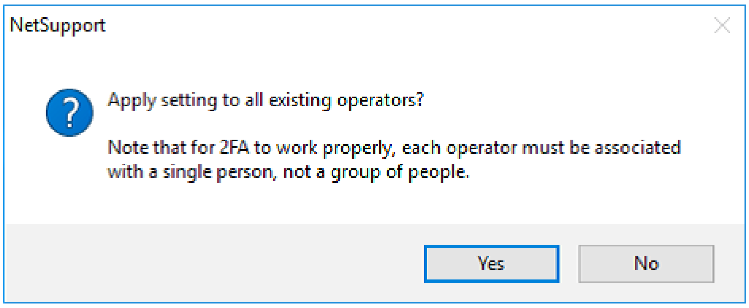
Integration key:

Secret key:

Username suffix: [WIN-9C8QH549DML]

Timeout (hours): 12

Select **Duo**. If you have existing Gateway operators that you wish to enable 2FA for, click **Yes** on the following prompt.

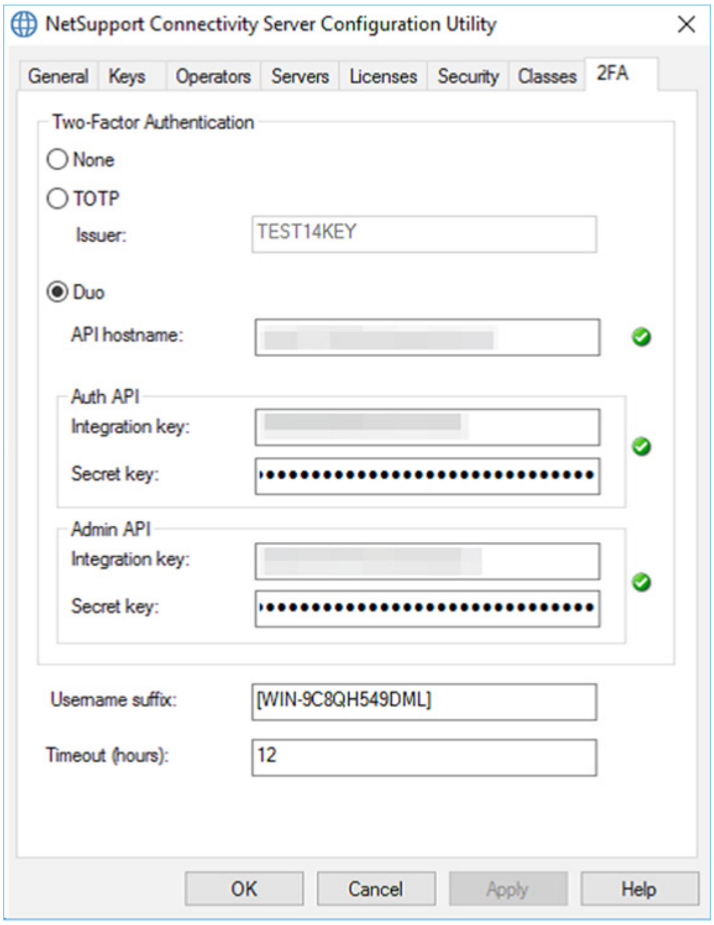


NetSupport

Apply setting to all existing operators?

Note that for 2FA to work properly, each operator must be associated with a single person, not a group of people.

Next, you need to populate the API fields with your Duo information obtained earlier in this document. A green tick indicates that the information entered is correct. Any red crosses mean the Gateway has not been able to validate the information provided, either due to the details being incorrect or the Gateway being unable to reach the Duo API host on port 443.



Two-Factor Authentication

○ None

○ TOTP

Issuer: TEST14KEY

● Duo

API hostname: [redacted] ✓

Auth API

Integration key: [redacted] ✓

Secret key: •••••••••••••••••••••••••••••••

Admin API

Integration key: [redacted] ✓

Secret key: •••••••••••••••••••••••••••••••

Username suffix: [WIN-9C8QH549DML]

Timeout (hours): 12

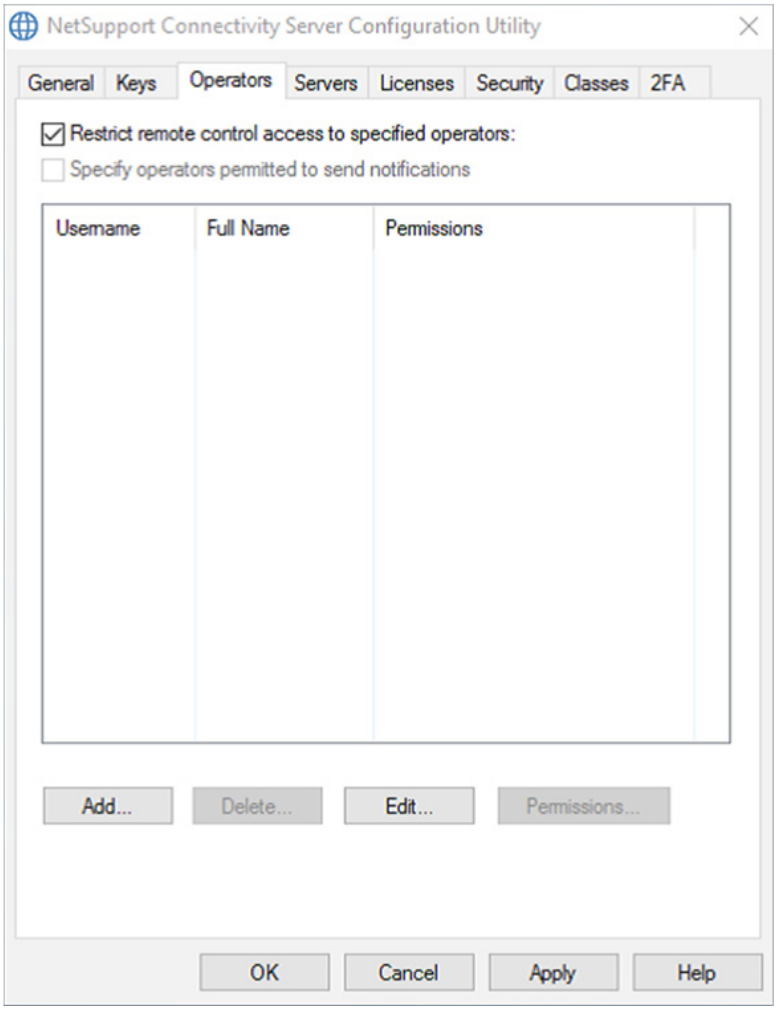
By default, after a user has successfully authenticated, their session will stay active for 12 hours or until the NetSupport Manager Control is closed. If required, you can set a different timeout period here. Setting this value to 0 means that you must authenticate for every Client you attempt to connect to.

Click **Apply** and the changes will be applied to the configuration.

Creating operators on the Gateway Server

Now that the Duo integration has been configured, you need to create operators on the Gateway Server (if you haven't already done so).

Select the Operators tab in the NetSupport Connectivity Server Configuration Utility and click **Restrict remote control access to specified operators**.



☑ Restrict remote control access to specified operators:

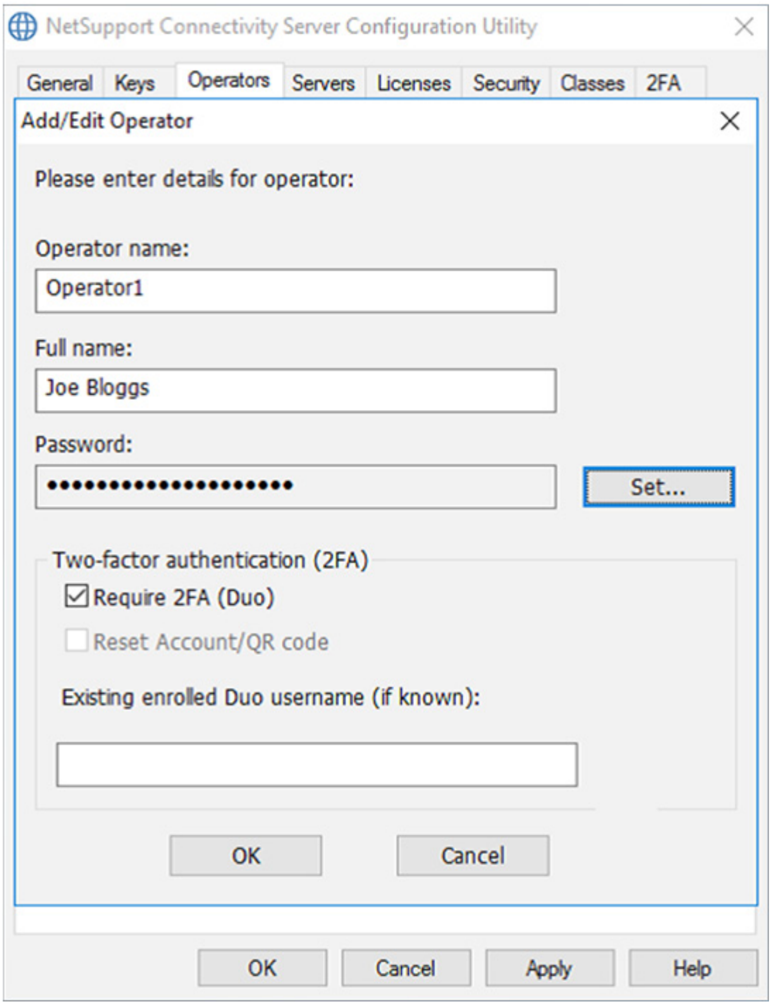
□ Specify operators permitted to send notifications

Click **Add** to create a new operator and enter a name and password for the operator.

Make sure you select **Require 2FA (Duo)**. This will already be selected if you chose to apply 2FA to existing operators when enabling it in the 2FA tab.

If you already have an enrolled Duo user account that you would like to associate the operator with, enter the Duo username in the **Existing enrolled Duo username** field. You can use a Duo user alias.

Existing operators who already have Duo user accounts should be edited to use their existing enrolled Duo username. Otherwise, they will get new automatic usernames created within Duo when they first attempt to use 2FA via NetSupport Manager.



Please enter details for operator:

Operator name: Operator1

Full name: Joe Bloggs

Password: ••••••••••••••••••••

Two-factor authentication (2FA)

☑ Require 2FA (Duo)

□ Reset Account/QR code

Existing enrolled Duo username (if known):

Click **OK** to apply the changes and create the operator. Repeat the steps to add any additional operators.

Click **Apply** to save the changes to the Gateway.

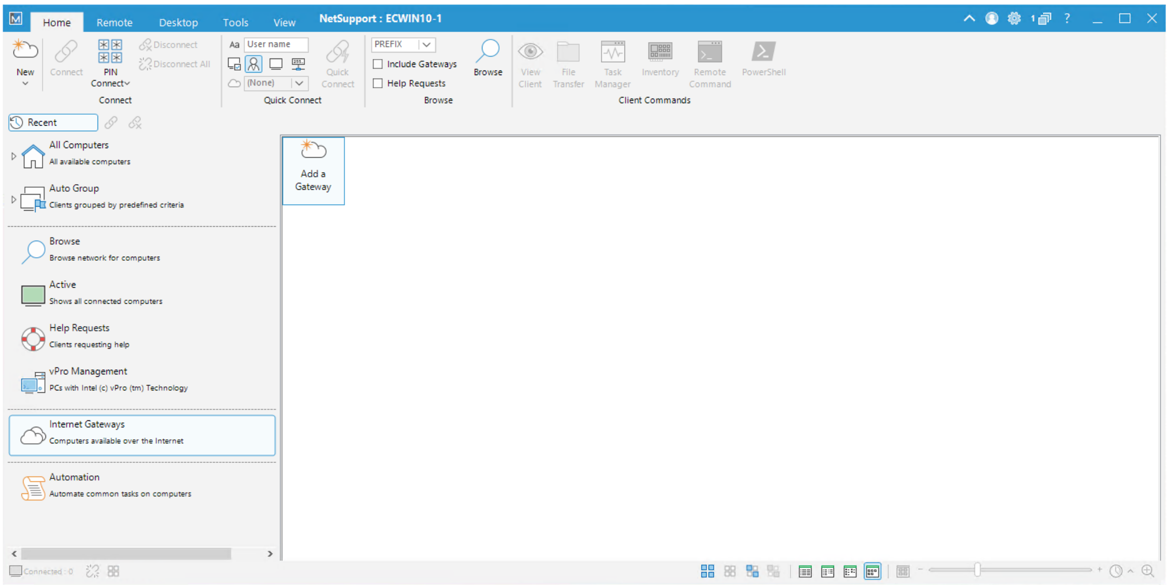
Important!

- Deleting an operator from the NetSupport Manager Gateway will also delete the Duo account that was automatically created when the operator first authenticated via NetSupport Manager. However, if you used the option to associate the operator with an existing Duo account, the pre-existing Duo account will not be deleted.
- If an operator user replaces their authenticating device, you can edit the operator within the Gateway using the **Reset Account/QR Code** option. The next time this operator attempts to connect to a Client, a new QR code will appear, prompting them to enrol their new device. Doing so would follow the same process as above, whereby the Duo account would be deleted if NetSupport Manager automatically created it. Pre-existing Duo accounts would not be deleted.

Using 2FA within the NetSupport Manager Control

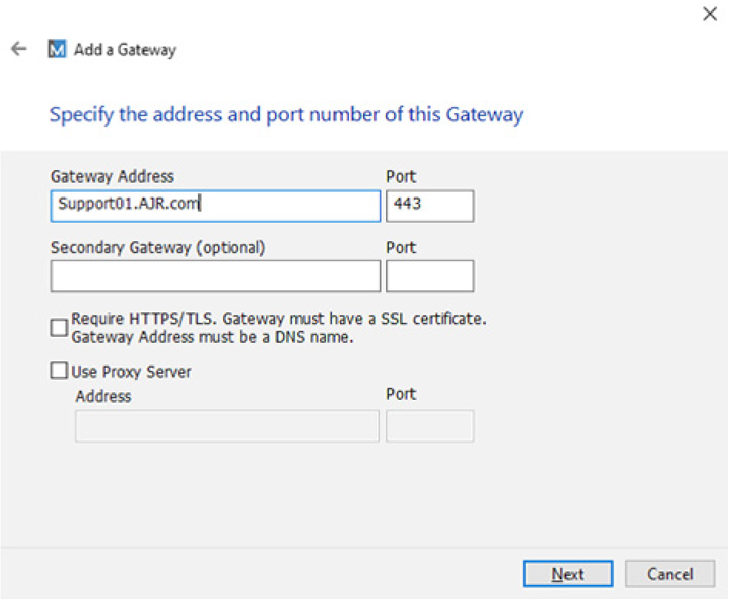
Now that the Gateway is configured to use Duo, you can now configure the NetSupport Manager Control to use this authentication.

Launch the NetSupport Manager Control and select **Internet Gateways** from the Tree view.



Double-click **Add a Gateway**, enter a name and description and click **Next**.

Enter your Gateway connection details and click **Next**.



Specify the address and port number of this Gateway

Gateway Address: Support01.AJR.com
Port: 443

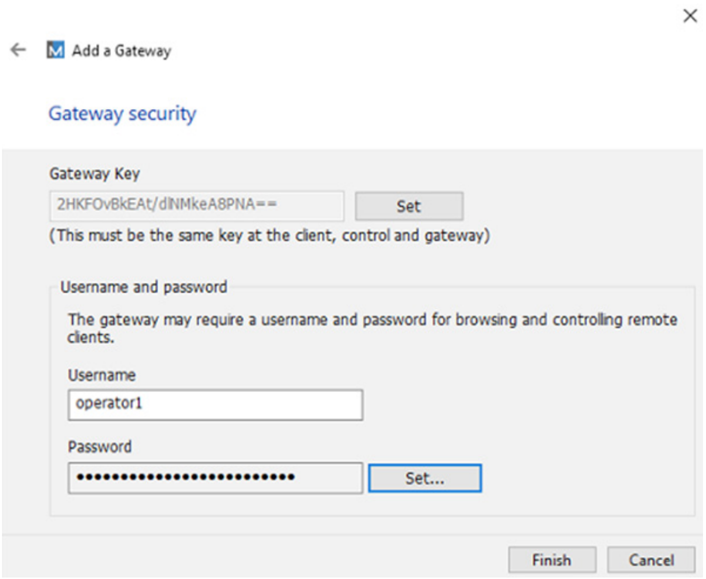
Secondary Gateway (optional):
Port:

☐ Require HTTPS/TLS. Gateway must have a SSL certificate. Gateway Address must be a DNS name.

☐ Use Proxy Server
Address:
Port:

Specify the Gateway key for your Gateway Server and the operator credentials for the operator you have created on the Gateway Server.

Note: *The operator credentials need to be the credentials you created on the Gateway Server when creating your operator, not the Duo credentials.*



Add a Gateway

Gateway security

Gateway Key

2HKFOvBkEAt/dlNMkeA8PNA== Set

(This must be the same key at the client, control and gateway)

Username and password

The gateway may require a username and password for browsing and controlling remote clients.

Username

operator1

Password

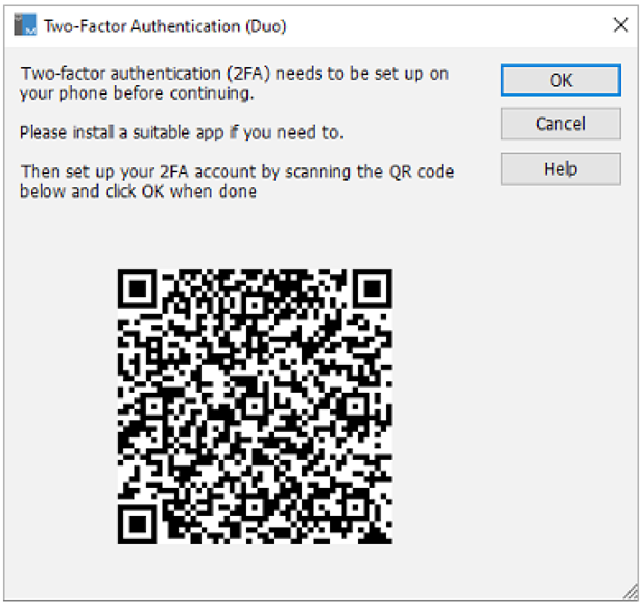
•••••••••••••••••••••••• Set...

Finish Cancel

Click **Finish** to add the Gateway. The new Gateway will be added to the List view.

Double-click the Gateway to browse it. Any connected Clients will appear in the List view.

Double-click a Client to connect to it. A dialog showing a QR code will appear.



Two-Factor Authentication (Duo)

Two-factor authentication (2FA) needs to be set up on your phone before continuing.

Please install a suitable app if you need to.

Then set up your 2FA account by scanning the QR code below and click OK when done

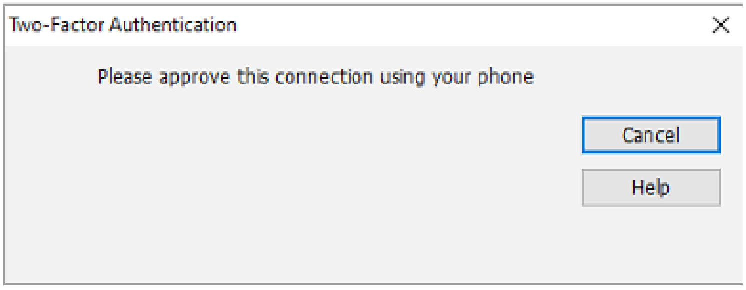
OK Cancel Help

Scan this QR code using the Duo Mobile app.

Note: *If you linked your operator with an existing Duo user account, the QR code will not appear and a push notification will be sent straight away.*

Once you have scanned the QR code in the Duo Mobile app and added the user, click **OK** in the NetSupport Manager Two-Factor Authentication (Duo) dialog.

This will proceed to connect to the Client and a push notification will be sent to your authenticator app. The NetSupport Manager Control will display the following dialog while waiting for you to approve the request.



Two-Factor Authentication

Please approve this connection using your phone

Approve the request in the Duo Mobile app and you will connect to the Client.

You have now successfully configured 2FA using Duo within NetSupport Manager.

Please contact our *Support team* if you need any further help.