MULTI-FACTOR AUTHENTICATION

MULTI-FACTOR AUTHENTICATION ENROLLMENT PROCESS FOR PRIVILEGED DEVICE

What is happening?

We are introducing MFA for devices which have privileged application access.

Why is it happening?

NHS Digital has a high priority security directive for all trusts to enforce MFA.

- must enforce MFA on all remote user access to all systems; and
- must enforce MFA on all privileged user1 access to externally hosted systems; and
- should enforce MFA on all privileged user access to all other systems.

If you would like more information, please visit the link: NHS Guidelines

Who is in scope?

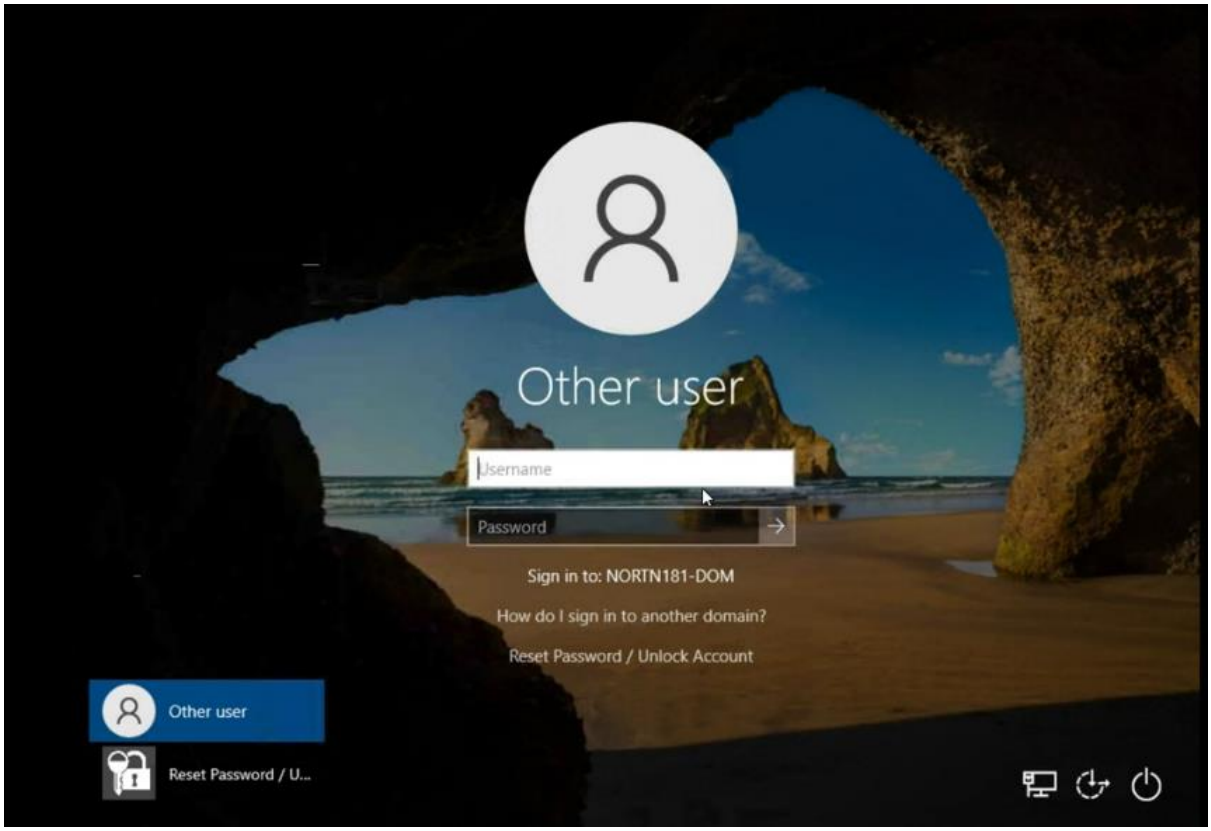
Any device which has privileged applications or has privileged access will be enforced to enrol MFA.

Please follow the Instructions below to enrol:

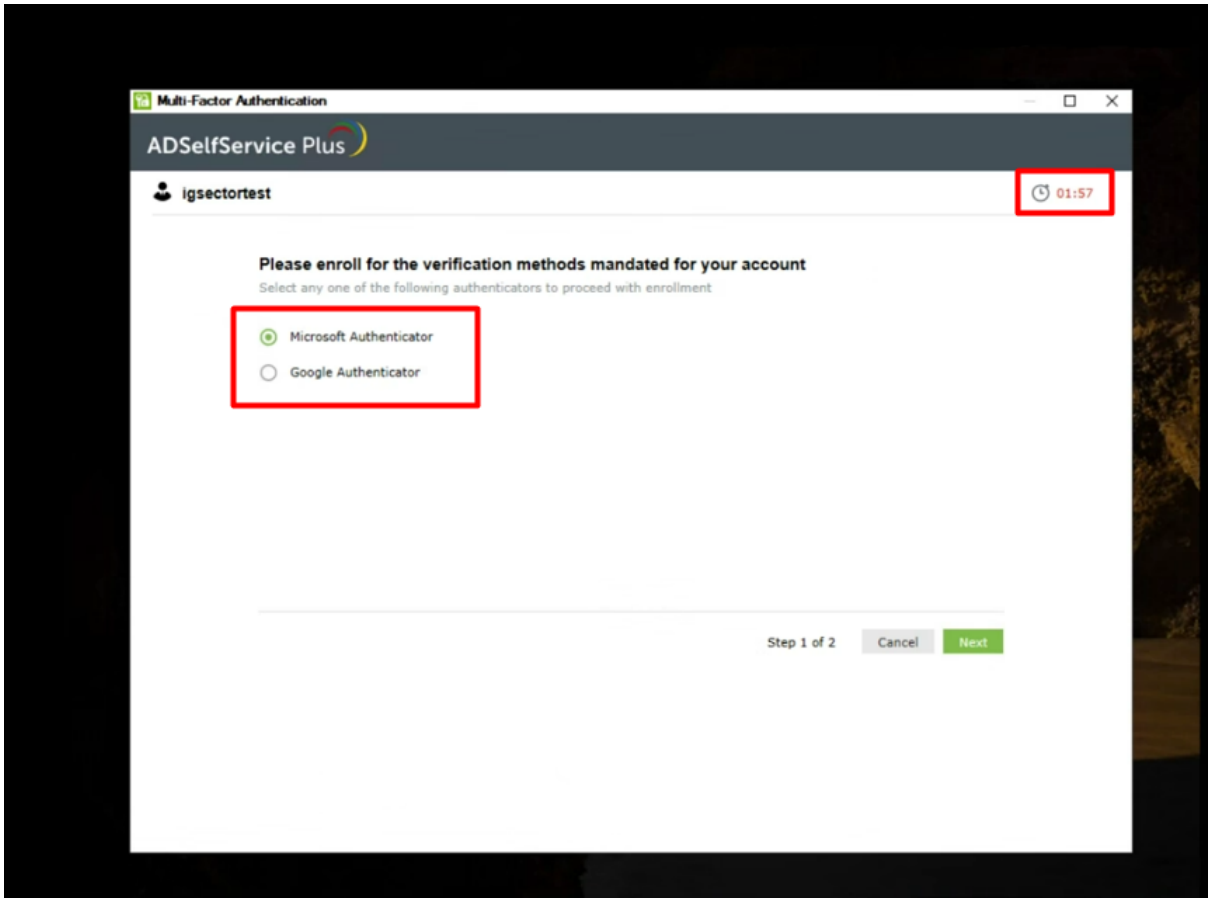
Access to Device

Logging onto the device

1. Press Alt+Ctrl+Del



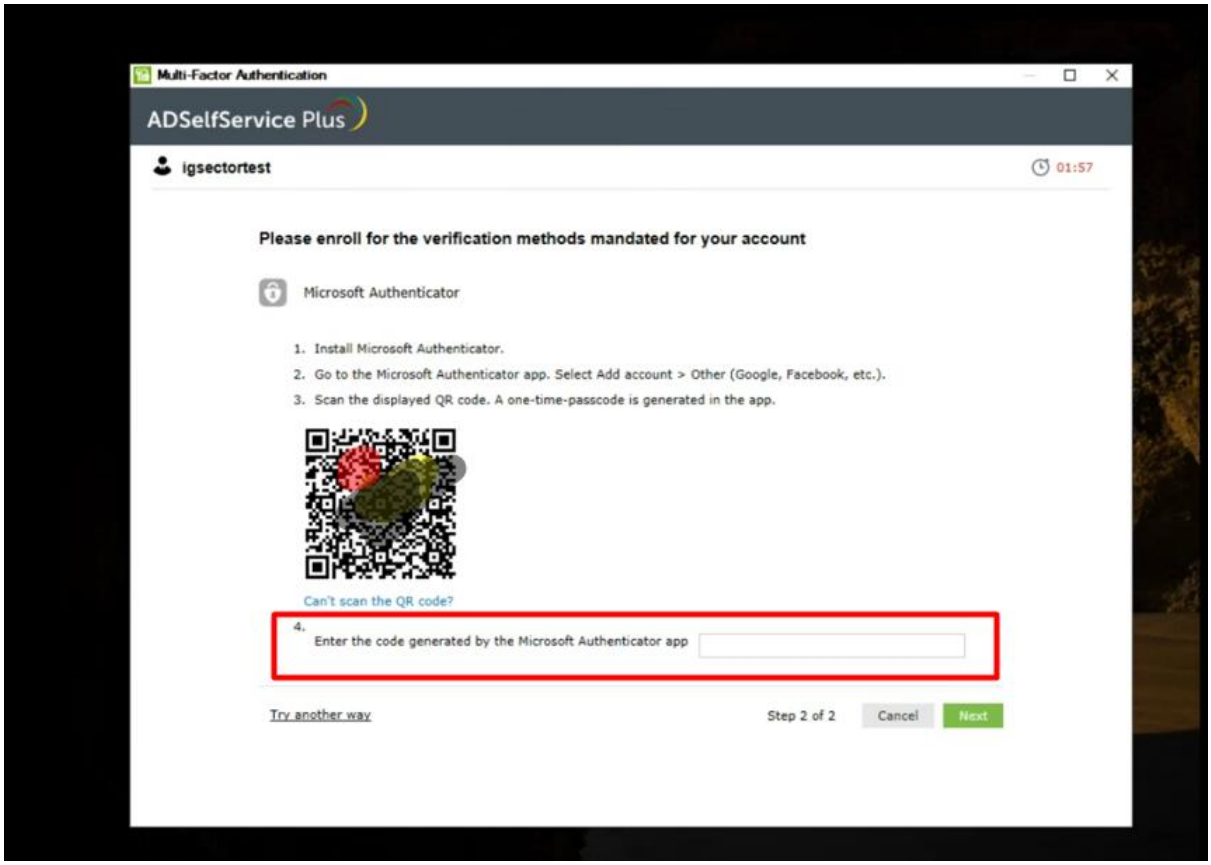
2. Login using your Network credentials.
3. Once authenticated with your network login credentials, the portal will prompt you to enrol for multi-factor authentication, with a choice between Microsoft Authenticator or Google Authenticator.



4. Choose one of the applications and download on your phone.
5. There is no preference which authenticator is downloaded

Please Note: There is a 2 min window to complete this action.

6. Scan the QR code on the application screen.
7. Once authentication is completed, please enter the Authentication code on the application.



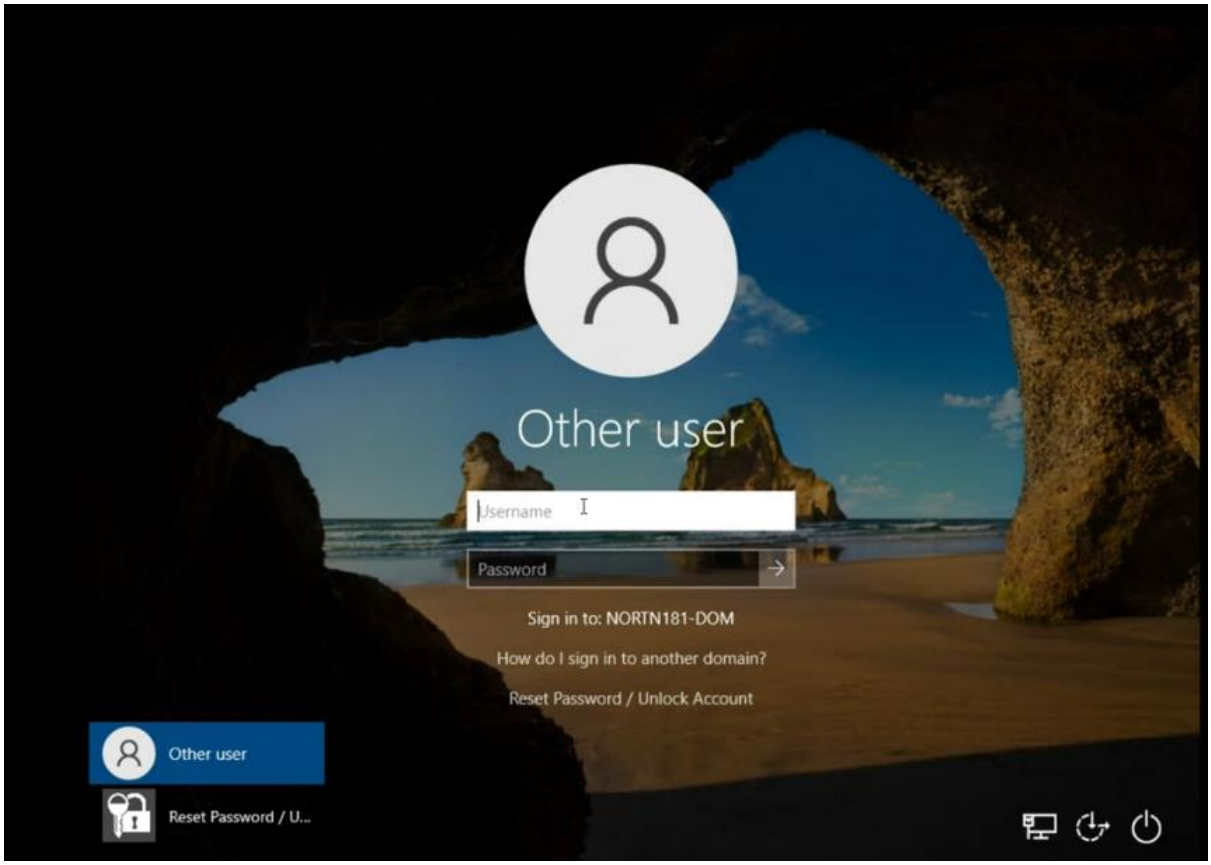
8. This completes the enrolment for MFA and once authenticated you will have access to the device

You will only need to use MFA to access your device once every 24 hours no matter how many times you log in.

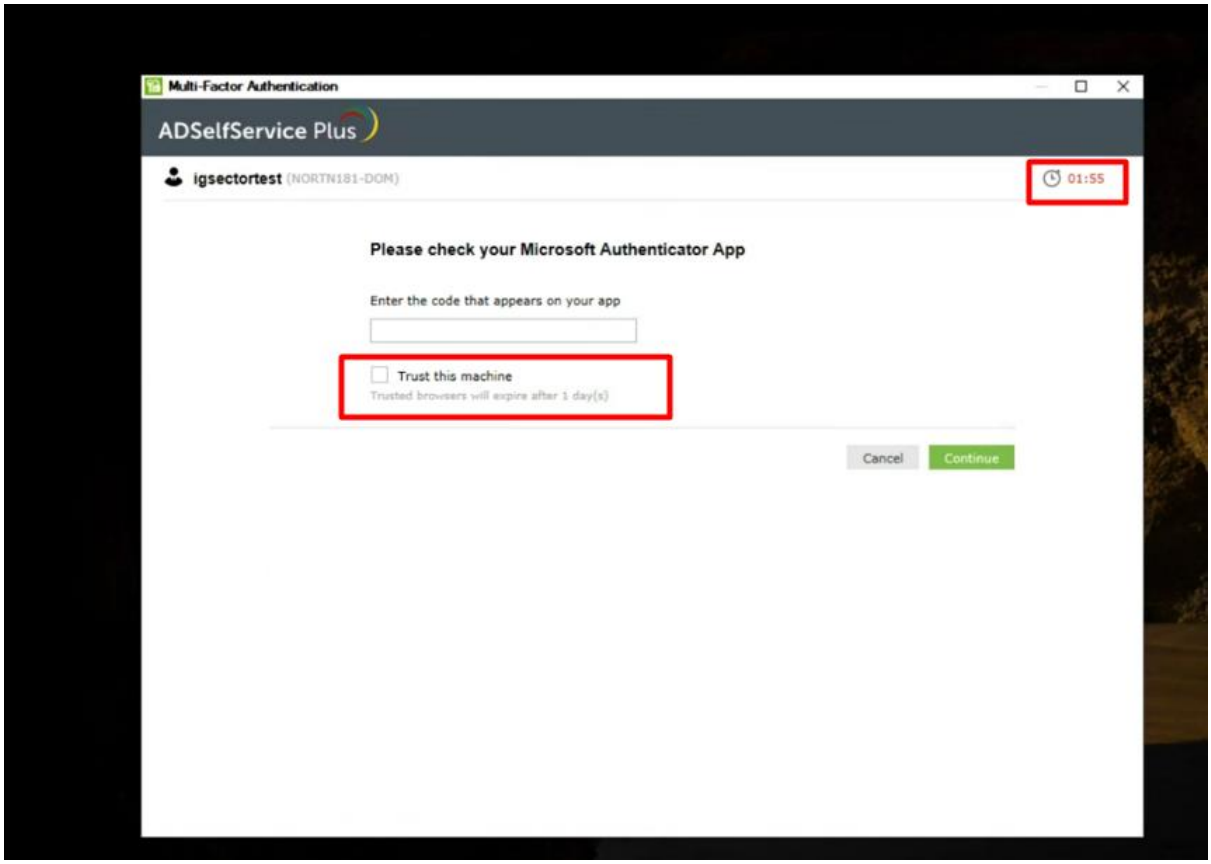
Device Authentication Example

Please follow the steps below:

1. On every next login to a device, you will need to enter the MFA authentication code.
2. Authenticate using your network login credentials.



3. Authenticate with the one-time password which is advertised to you on the authenticator application.



Please note: User will have 2 mins to complete this activity.

4. If you click on the "**Trust this machine"** checkbox on the same device, you will be requested to authenticate again after 24 hours lapse, which is optional.
5. Once authenticated you will have full access to the device.