

Configuring Net2 Checkpoint Control

Requirements

- Net2 Access control v6.05 or higher
- Requires Net2 Pro software
- System Engineer or Supervisor operator permissions
- Logical anti-passback is not supported when using Checkpoint Control
- See <http://www.paxton.info/720> for the minimum PC specifications and compatibility statement

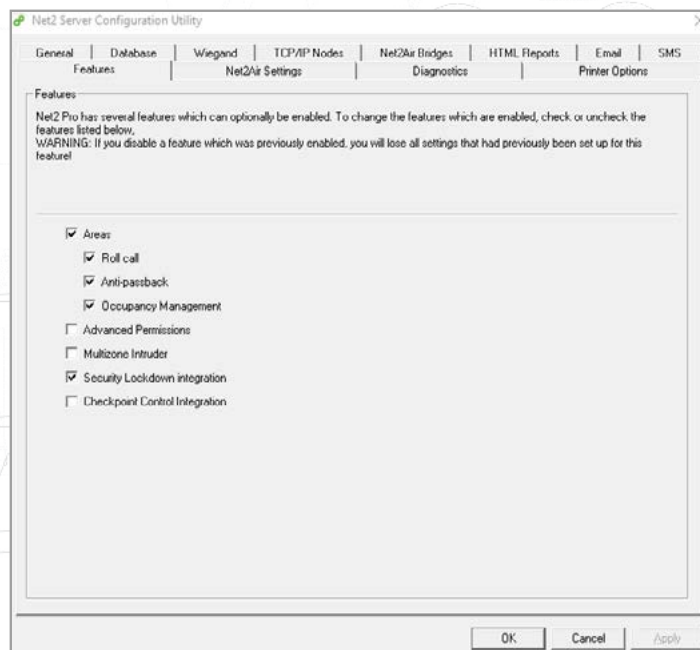


About

Net2 Checkpoint Control allows a site to assign temporary access levels to one or more users that will remain in place until they have either been manually validated or badged through a specific door. This will allow you to ensure all staff have to pass through a specific area at a designated time to be validated. It also offers the flexibility to split staff between multiple checkpoints to maintain social distancing and not overrun an area.

Activating the feature

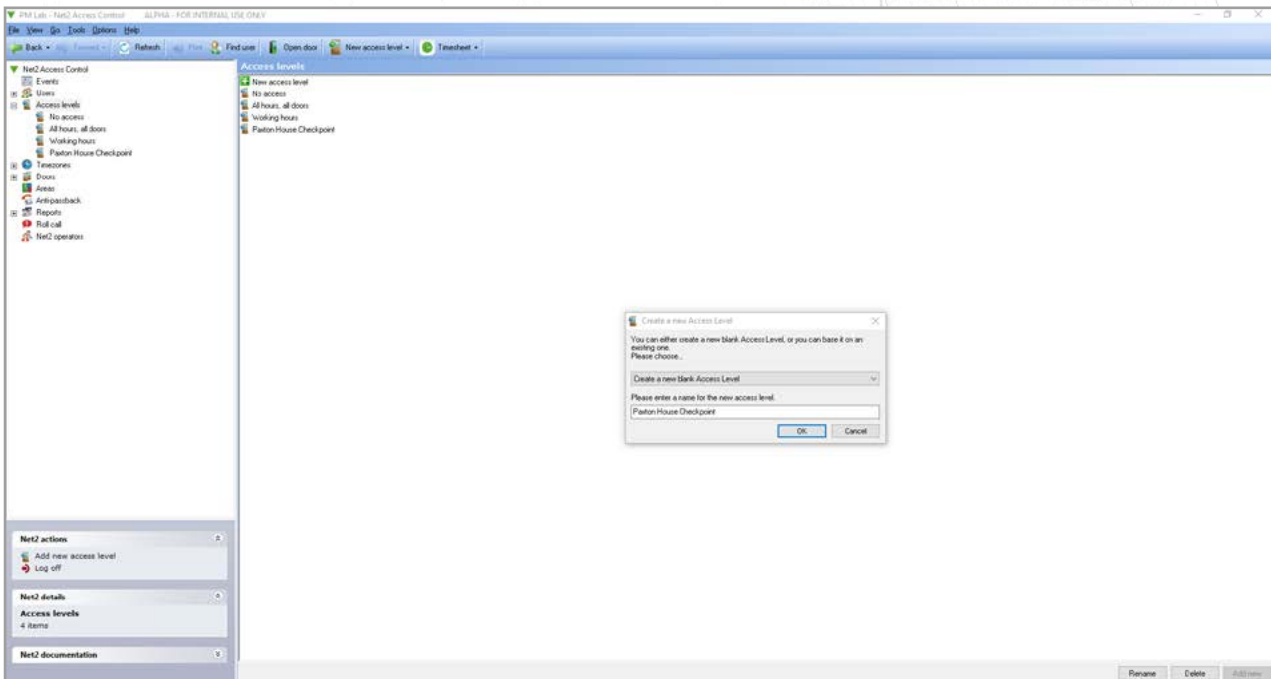
1. Open the Net2 Configuration utility
2. Select the features tab and check the '**Checkpoint Control**' box
3. Now select '**Apply**' for the feature to be activated, followed by OK to close the utility



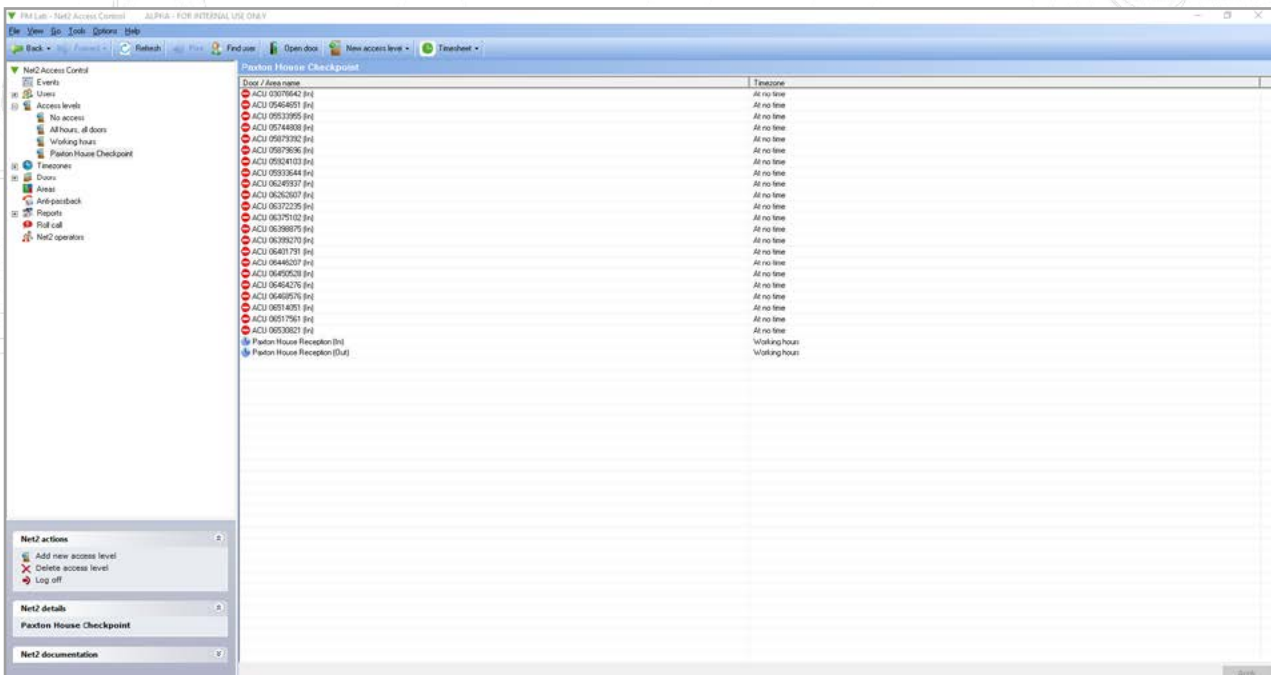
Setting up the Checkpoint Access Level

The first step is to setup your Checkpoint Control Access Levels. These are the access levels you would like a user to have before they have been validated at their nominated checkpoint.

1. Open the Net2 Pro software
2. Select 'Access Levels' shown in the left tree menu
3. Now double click on the 'New access level' option in the main window
4. Name your new Checkpoint Control access level



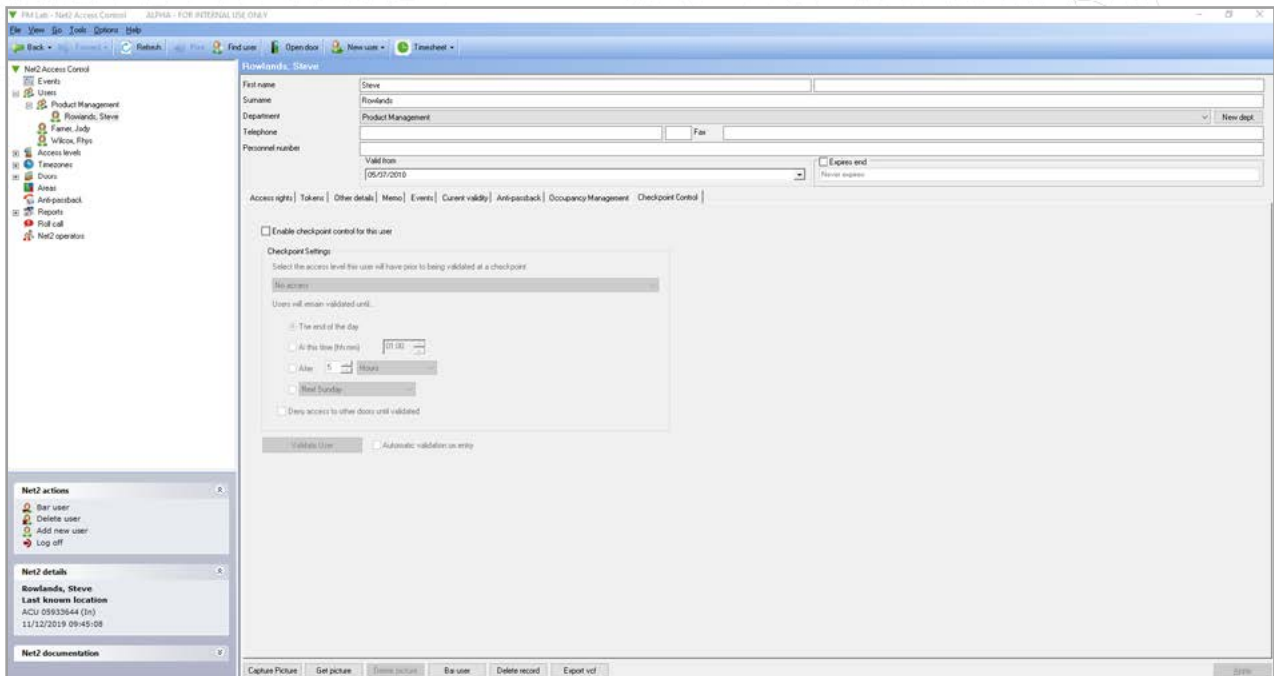
5. Setup the access level as appropriate to that Checkpoint location and click Apply



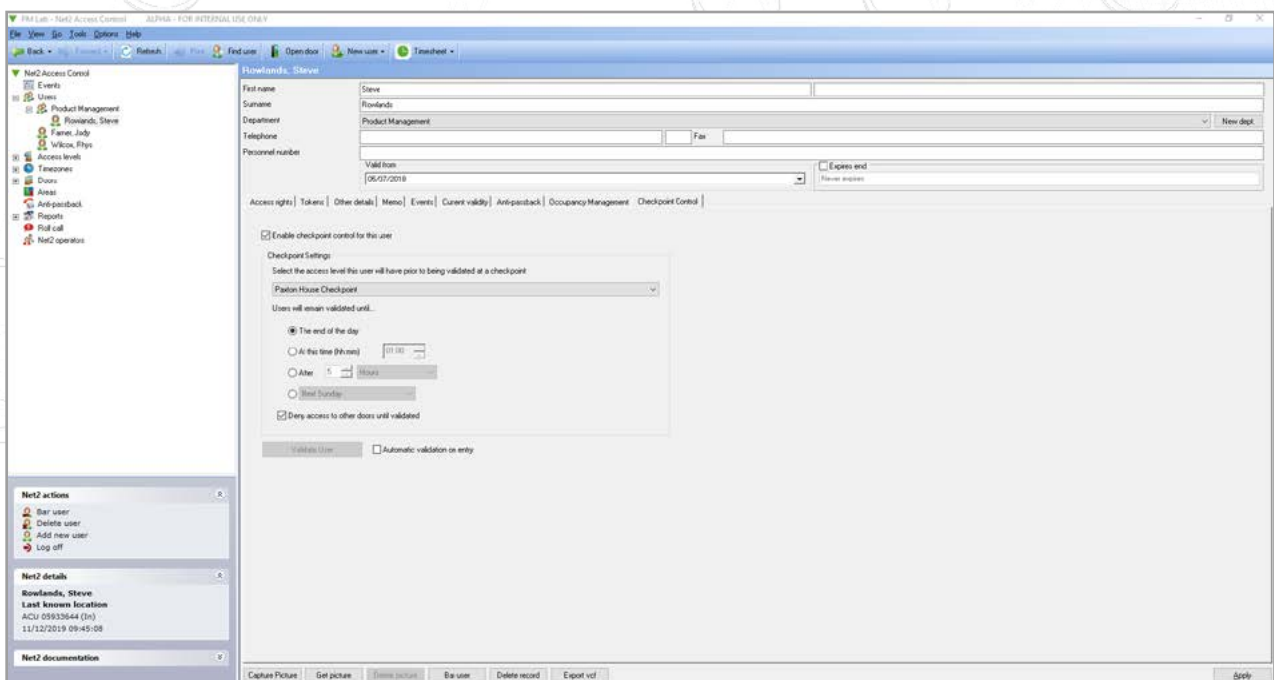
Setting up Checkpoint Users

You now need to assign your users to the Checkpoints you wish them to use.

1. Select **'Users'** in the left-hand tree menu and choose the user you wish to setup Checkpoint Control for



2. Check the box to enable Checkpoint Control for that user
3. Now choose the access level that you would like the user to have, prior to being validated at a checkpoint



4. Next, you will need to choose how long you would like a user to remain validated for when they have successfully passed through their checkpoint

5. **'Deny access to other doors until validated'** – Deselecting this box will enable that user to continue to gain access to doors permitted under their standard permissions. When doing so, if they are not validated, an event will be returned 'User not validated at a checkpoint'

By default, this is selected, meaning a user will only receive their standard permissions once they have successfully passed through their nominated checkpoint.

Setting up users by department

If you wish to setup Checkpoint Control for multiple users within a department, simply do the following.

1. Right click on the department you wish to setup and select Properties

Properties

Set the properties for all users in Product Management

Activation date
To apply a common activation date to this department, click the 'Set' button Set

Expiration date
To apply a common expiration date to this department, click the 'Set' button.
To remove the expiry date, click the 'Remove' button Set Remove

Access level
Set the access level for the entire department Unchanged ▾

Checkpoint Control
Set the Checkpoint Control settings for the entire department Set

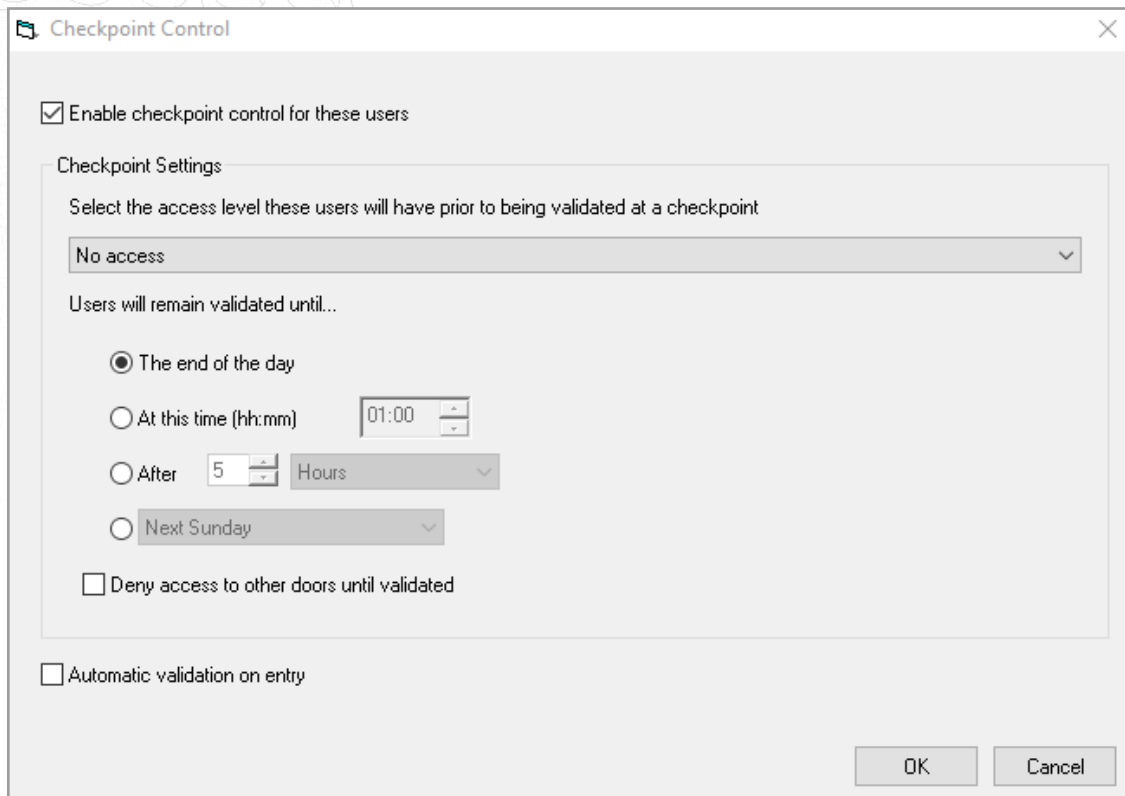
Anti-passback
 The users obey anti-passback rules

Security Lockdown
 Users are exempt from Lockdown rules.

Card template
Choose a card template for entire department Unchanged ▾

OK Cancel

2. Now select the **'Set'** button under Checkpoint Control
3. Check the box to enable Checkpoint Control for that user
4. Now choose the access level that you would like the user to have, prior to being validated at a checkpoint



5. Select OK when you're done to apply the changes

Manual and automatic validation

Manual (software) – Using this option you will need a member of staff to be present in the Checkpoint area to check and manually validate staff in the Net2 software as they enter the building.

Additionally if the desktop reader is in Checkpoint mode, the user will simply need to present their token to the desktop reader and the Net2 software will automatically navigate to their Checkpoint page, where the 'Validate User' button can be selected.

Auto – When this option is selected, users entering the building simply need to pass through their nominated Checkpoint area and present their token to that reader. Doing so will then validate them and introduce their standard permissions.

Note: The Checkpoint Control feature requires a live connection with the Net2 server to be present. If this connection is lost, all ACUs within a controlled area will resume standard, permission-based operation.

Desktop reader - Checkpoint Control Mode

If you have manual validation setup on a site, to make the validation process more convenient you can enable the desktop reader checkpoint control mode.

This will take you straight to the relevant user validation page in the Net2 software when a user presents their token to a desktop reader.

The image shows a screenshot of the 'Options' dialog box in a software application. The dialog has a title bar with a gear icon and the text 'Options' and a close button. It features a tabbed interface with the following tabs: 'Token types', 'Token data formats', 'Custom days', 'Camera integration', 'Landlord Tenant permissions', 'Card printing', 'Activation', 'Security', 'Net2Online', 'Paxton Telemetry', 'General', 'Departments', 'Door groups', 'Report groups', and 'Field names'. The 'General' tab is selected. Under 'General settings', there are four items: 'Week starts on' (Monday), 'Desktop reader' (No desktop reader selected), 'Desktop reader should sound buzzer' (unchecked), and 'Desktop reader checkpoint control mode' (checked). Under 'Default pictures', there is a 'Select token type' dropdown set to 'Default', a text box for the picture, and 'Get picture' and 'Delete picture' buttons. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Token types	Token data formats	Custom days	Camera integration	Landlord Tenant permissions
Card printing	Activation	Security	Net2Online	Paxton Telemetry
General	Departments	Door groups	Report groups	Field names

General settings

Week starts on: Monday

Desktop reader: No desktop reader selected

Desktop reader should sound buzzer:

Desktop reader checkpoint control mode:

Default pictures

Select token type: Default

Choose the default picture you would like to use for this token type. This can be changed on the user record.

Get picture

Delete picture

OK Cancel Apply