impero
education pro

PIN Group User Guide V3.0

Impero learning series

English

impero

table of contents

the challenge

With the proliferation of mobile devices in recent years, the challenge of managing these devices has increased in complexity. Whilst retaining Impero Education Pro's focus on cross-platform compatibility, and retaining enough flexibility to meet the needs of a school's individual requirements, we have introduced our **PIN Group** feature, a cross-platform, multi-device grouping feature enabling end users to quickly group and view devices (including user information).

As a classroom teacher I want to be able to quickly provision a PIN number to group and view multiple devices within the Impero console and, if appropriate, force users to enter user details and/or their Active Directory credentials. The Impero console will show all the devices being used by my students within my lesson, and who is using which device, so that I can oversee students use of these devices to ensure they are safe and on-task. This applies to whether the student devices are Windows, Chromebook or iOS devices and owned by the school or by a pupil (subject to the installation of an Impero Client).

Two types of PIN groups are available, either Static or Dynamic, to address the differing needs of individual schools and teaching staff. Experience shows that teachers often forget to wipe their block/allow policy settings at the end of a lesson which then causes difficulties for subsequent lessons as the previous teacher's settings are still active.

Static Groups give staff the ability to apply policies that remain for the duration of the group or class and Dynamic Groups are designed to support the application of specific policies for the duration of that lesson or session.

If a Server user (administrator) selects the 'No access to PIN groups' radio button for a specific user, they will not be able to create or view PIN groups or the PIN icon and the Static PIN group list will not be displayed in their console.

If a server user selects the 'Allow dynamic PIN group options' only, then the user selected in the Access Rights List pane will be able to only create dynamic PIN groups.

the basics

This section provides information on the layout and identifies key PIN Group areas within the Impero Console and in the Server application. All relevant PIN Group Session data is mapped to the Dates, Users, Computers and Groups categories within the Log viewer in line with standard existing functionality.

opening the Impero Console

To begin using Impero, locate the 'Impero Console' shortcut icon (Image 1) on a Windows or Mac desktop and double click.

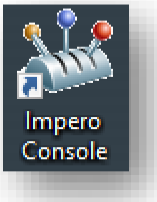


Image 1 – Desktop Icon

The first time you launch the Console you may be prompted with the password entry box* (Image 2). If you are permitted access, the Impero Console will then open. You will see the password prompt the first time you launch the Console for every log in session.

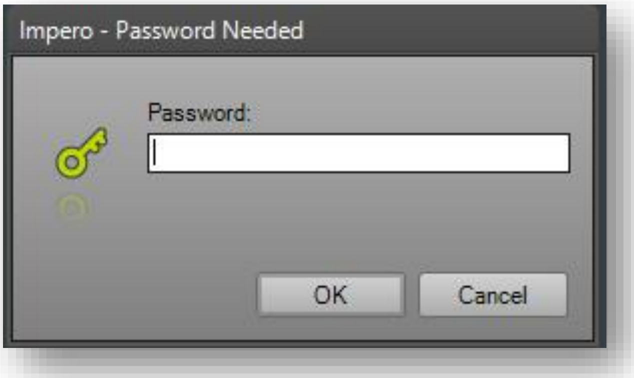


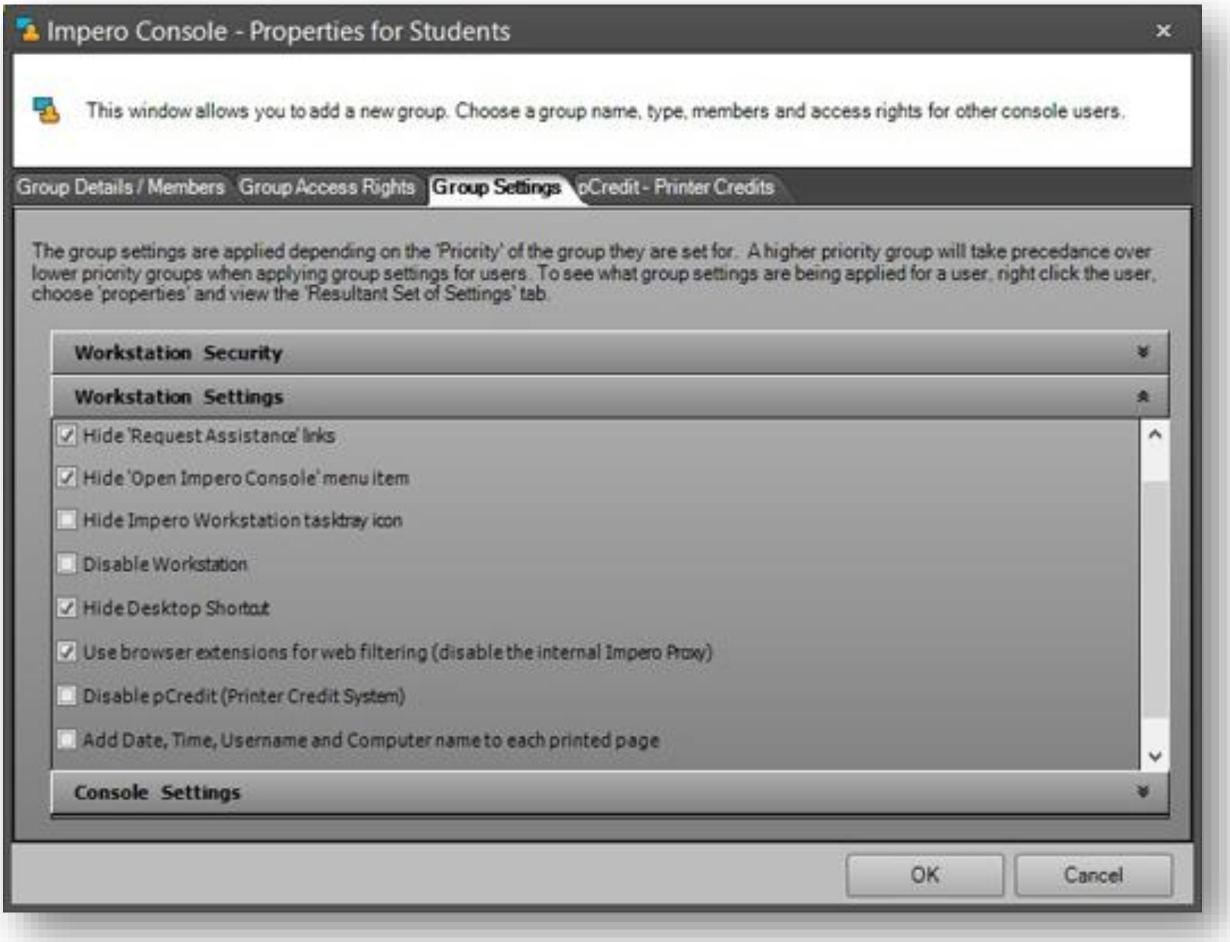
Image 2 – Password entry box

*Please Note: If you are not sure of your password please ask your network administrator.

The Principals of Impero Groups.

It is important when setting up your Groups within Impero that you understand how the 'Priority' of the group affects the behaviour of Impero.

Every Impero Group has a number of settings that can be applied. Right-click on a group in the Console, and select '**Properties**'. Click the '**Group Settings**' tab across the top of this window.



This window allows you to add a new group. Choose a group name, type, members and access rights for other console users.

The group settings are applied depending on the 'Priority' of the group they are set for. A higher priority group will take precedence over lower priority groups when applying group settings for users. To see what group settings are being applied for a user, right click the user, choose 'properties' and view the 'Resultant Set of Settings' tab.

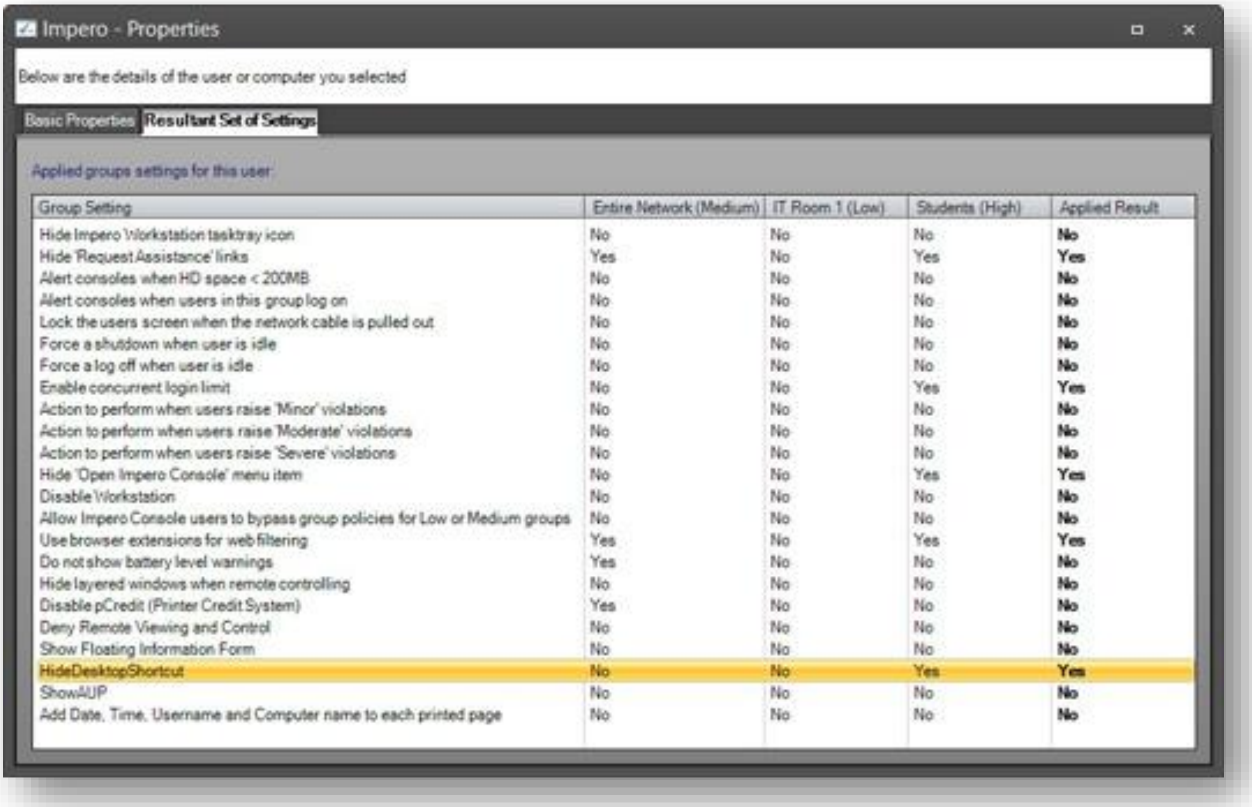
☑ Hide 'Request Assistance' links
☑ Hide 'Open Impero Console' menu item
☐ Hide Impero Workstation tasktray icon
☐ Disable Workstation
☑ Hide Desktop Shortcut
☑ Use browser extensions for web filtering (disable the internal Impero Proxy)
☐ Disable pCredit (Printer Credit System)
☐ Add Date, Time, Username and Computer name to each printed page

The 'Group Settings' tab contains all these settings that can be applied on a group-by-group basis, for example, '**Hide Desktop Shortcut**' – which will hide the Impero Console desktop icon for members of the selected group.

One user can easily belong to multiple groups. For example, a student user could potentially belong to the 'Entire Network' group, a 'Students' user group, and a 'Classroom' computer group.

The 'Group Setting' that will apply to this user will be the setting from the group with the **highest priority** that the user belongs to.

To identify which setting applies to a user right-click a user in the Console and select ‘**Properties**’. Now, click the ‘**Resultant Set of Settings**’ tab.



Below are the details of the user or computer you selected

Applied groups settings for this user

Group Setting	Entire Network (Medium)	IT Room 1 (Low)	Students (High)	Applied Result
Hide Impero Workstation tasktray icon	No	No	No	**No**
Hide 'Request Assistance' links	Yes	No	Yes	**Yes**
Alert consoles when HD space < 200MB	No	No	No	**No**
Alert consoles when users in this group log on	No	No	No	**No**
Lock the users screen when the network cable is pulled out	No	No	No	**No**
Force a shutdown when user is idle	No	No	No	**No**
Force a log off when user is idle	No	No	No	**No**
Enable concurrent login limit	No	No	Yes	**Yes**
Action to perform when users raise 'Minor' violations	No	No	No	**No**
Action to perform when users raise 'Moderate' violations	No	No	No	**No**
Action to perform when users raise 'Severe' violations	No	No	No	**No**
Hide 'Open Impero Console' menu item	No	No	Yes	**Yes**
Disable Workstation	No	No	No	**No**
Allow Impero Console users to bypass group policies for Low or Medium groups	No	No	No	**No**
Use browser extensions for web filtering	Yes	No	Yes	**Yes**
Do not show battery level warnings	Yes	No	No	**No**
Hide layered windows when remote controlling	No	No	No	**No**
Disable pCredit (Printer Credit System)	Yes	No	No	**No**
Deny Remote Viewing and Control	No	No	No	**No**
Show Floating Information Form	No	No	No	**No**
HideDesktopShortcut	No	No	Yes	**Yes**
ShowAUP	No	No	No	**No**
Add Date, Time, Username and Computer name to each printed page	No	No	No	**No**

In this window you can see all the groups that the user belongs to, the priority of each group, the setting applied to the user from each group they belong to, and the ‘**Applied Result**’ of those settings to this user based on the priorities.

Please Note: If a user belongs to two groups with matching priority, the applied setting could vary – it is important to ensure that users belong to only one group of a higher priority.

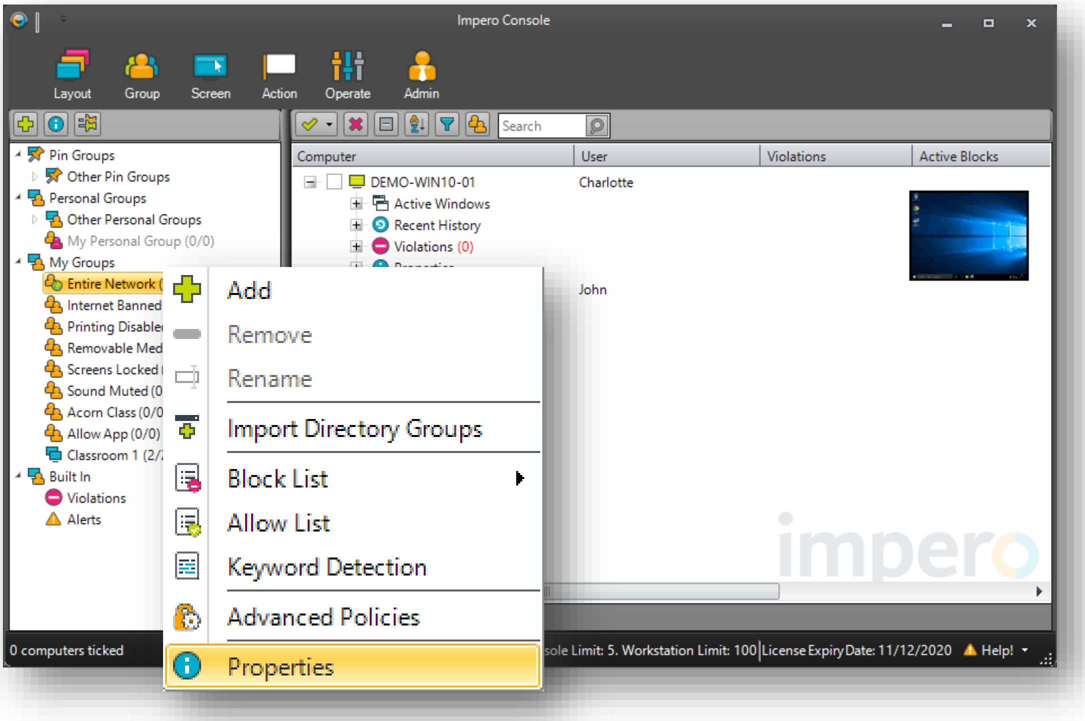
The setup that Impero recommends is to have user groups set to higher priorities. For example:

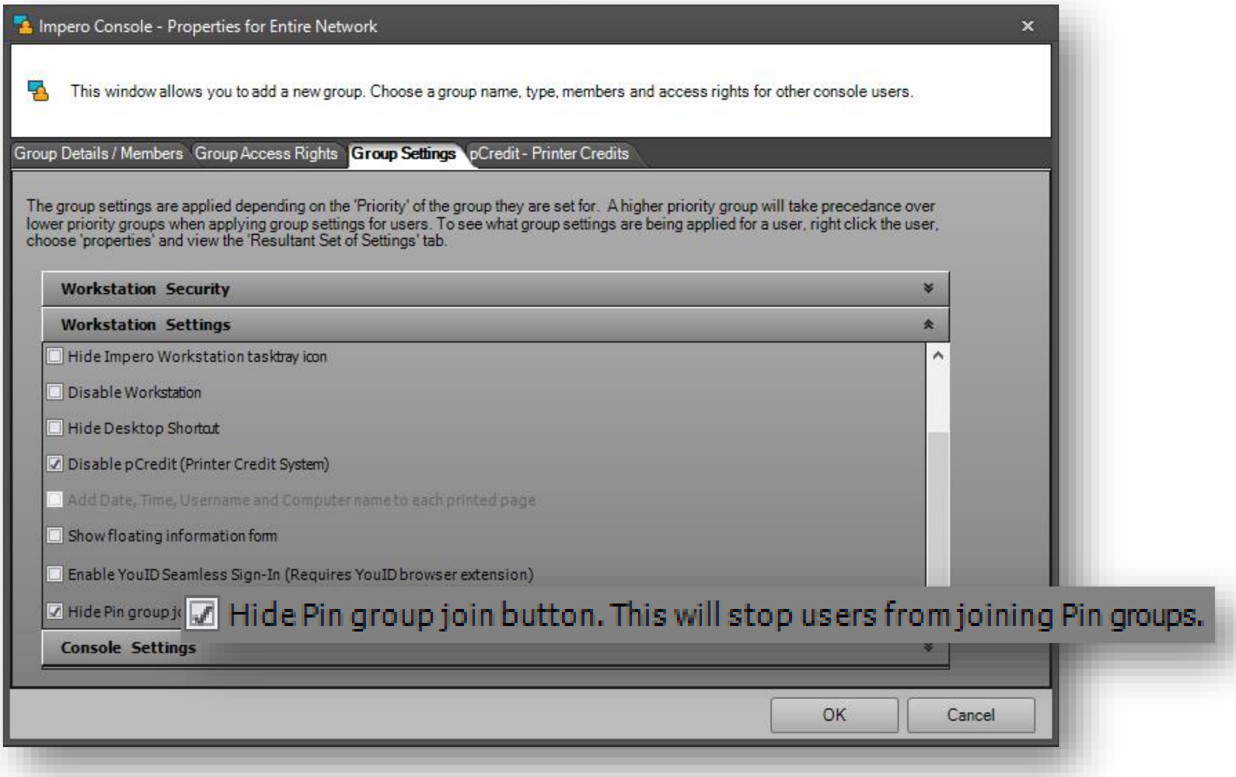
Group Name	Group Priority
Entire Network	Low/Medium
Admin Staff [User Group]	High
Teaching Staff [User Group]	High
Year 11 Students [User Group]	High
Year 12 Students [User Group]	High
IT Suite [Computer Group]	Low
Science Lab [Computer Group]	Low

This configuration ensures all users belong to one high priority group only with no overlap, and whatever setting is applied to the user group will apply to its members regardless of where they login. For example, 'Hide Desktop Shortcut' will apply to all students wherever they login, but all staff members will still see the Impero Console desktop shortcut regardless of where they login.

adding and removing the PIN Group feature for end users (within the Impero Education Pro Console)

Right click the ‘Entire Network’ group within the Impero Console and select Properties. Add or remove (turn on or off) the button from users’ desktops within the Workstation Settings section of the Group Settings tab (Images 3 and 4).




Impero Console - Properties for Entire Network
Group Details / Members
Group Access Rights
Group Settings
pCredit - Printer Credits
OK
Cancel

This window allows you to add a new group. Choose a group name, type, members and access rights for other console users.

The group settings are applied depending on the 'Priority' of the group they are set for. A higher priority group will take precedance over lower priority groups when applying group settings for users. To see what group settings are being applied for a user, right click the user, choose 'properties' and view the 'Resultant Set of Settings' tab.

Workstation Security

Workstation Settings

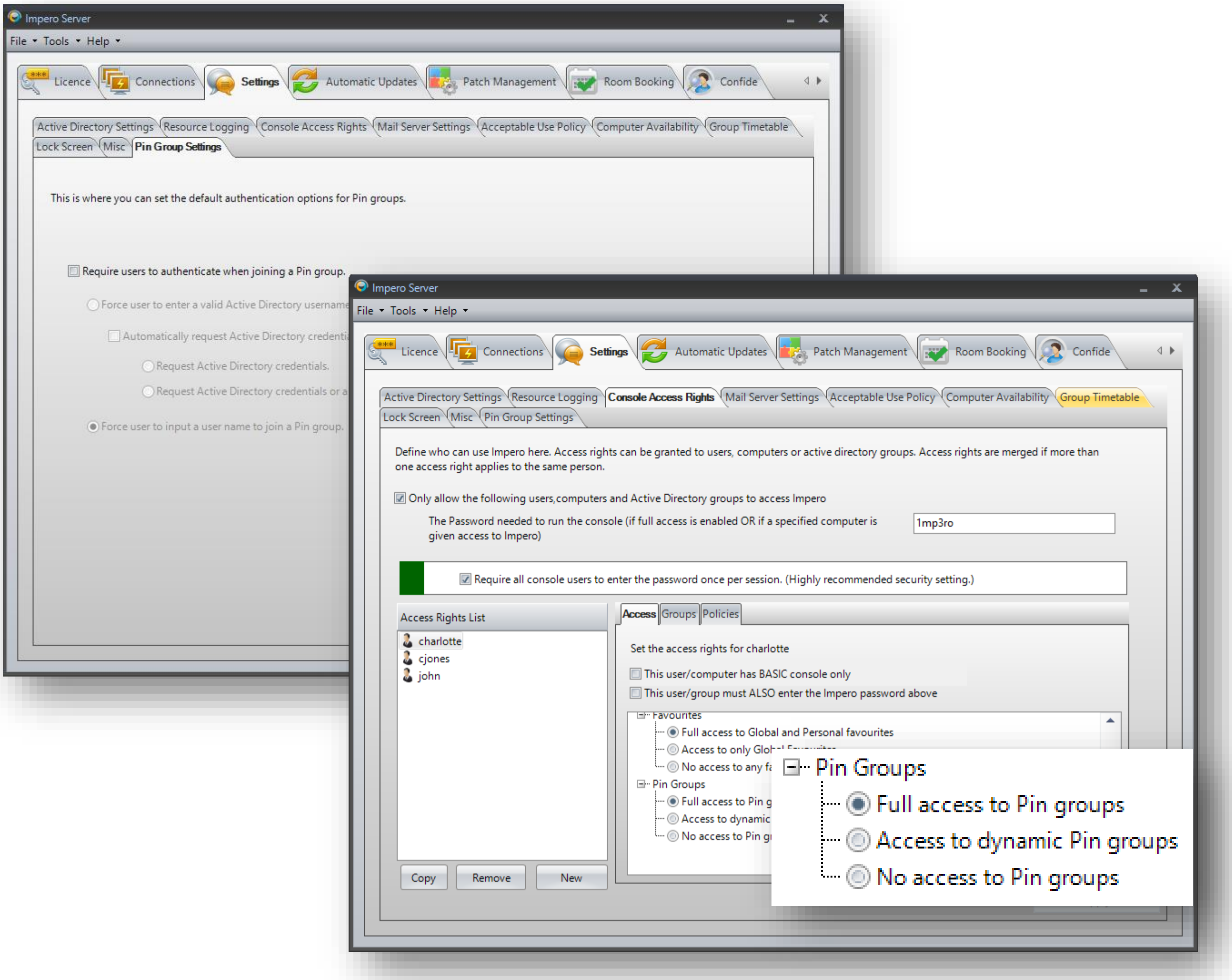
- □ Hide Impero Workstation tasktray icon
- □ Disable Workstation
- □ Hide Desktop Shortcut
- ☑ Disable pCredit (Printer Credit System)
- □ Add Date, Time, Username and Computer name to each printed page
- □ Show floating information form
- □ Enable YouID Seamless Sign-In (Requires YouID browser extension)
- ☑ Hide Pin group join button. This will stop users from joining Pin groups.

Console Settings

© 2016 Impero Solutions Ltd

setting PIN Group defaults (within the Server application)

At a server level, admin users can select user requirements during the process to join a PIN Group/Session, including forcing users to authenticate when joining. Users can be forced to authenticate by entering their Active Directory (AD) username and password or by automatically requesting their AD credentials if the user has already authenticated on their device. Users can also be asked to enter a username during this process, either alongside their AD credentials or in place of.



This is where you can set the default authentication options for Pin groups.

□ Require users to authenticate when joining a Pin group.

○ Force user to enter a valid Active Directory username

□ Automatically request Active Directory credenti

○ Request Active Directory credentials.

○ Request Active Directory credentials or a

● Force user to input a user name to join a Pin group.

Define who can use Impero here. Access rights can be granted to users, computers or active directory groups. Access rights are merged if more than one access right applies to the same person.

☑ Only allow the following users,computers and Active Directory groups to access Impero

The Password needed to run the console (if full access is enabled OR if a specified computer is given access to Impero) 1mp3ro

☑ Require all console users to enter the password once per session. (Highly recommended security setting.)

charlotte
cjones
john

Set the access rights for charlotte

□ This user/computer has BASIC console only

□ This user/group must ALSO enter the Impero password above

Favourites
- ● Full access to Global and Personal favourites
- ○ Access to only Glob
- ○ No access to any fa

Pin Groups
- ● Full access to Pin g
- ○ Access to dynamic
- ○ No access to Pin g

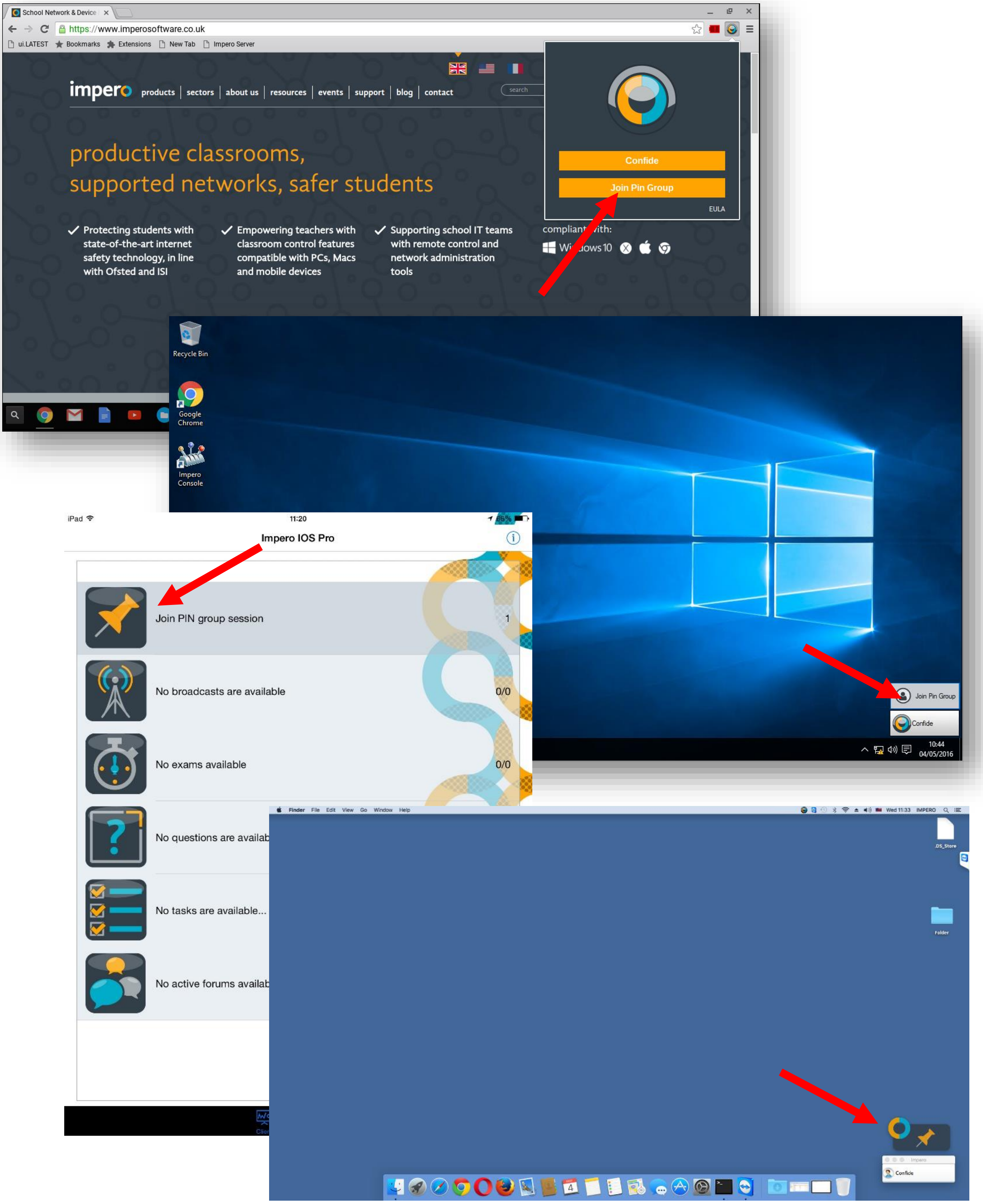
Pin Groups
- ● Full access to Pin groups
- ○ Access to dynamic Pin groups
- ○ No access to Pin groups

Image 5 – Setting PIN Group options in the Impero Server

Additionally, admin users can, on a user level basis, add or remove access to PIN group functionality, whereby an end user **cannot create or view PIN groups** and the PIN icon and Static PIN Group list **will not be displayed** in the console for the selected user.

If an admin user selects the ‘Allow access to dynamic PIN groups’ option only, then the user selected in the Access Rights List panel will be able to only create Dynamic PIN groups, and the advanced options on the Dynamic PIN group session window within the console will be greyed out and un-selectable.

accessing PIN Groups on Windows, iOS, Mac and Chrome



School Network & Device

https://www.imperosoftware.co.uk

productive classrooms, supported networks, safer students

✓ Protecting students with state-of-the-art internet safety technology, in line with Ofsted and ISI

✓ Empowering teachers with classroom control features compatible with PCs, Macs and mobile devices

✓ Supporting school IT teams with remote control and network administration tools

Join PIN group session	1
No broadcasts are available	0/0
No exams available	0/0
No questions are availab	
No tasks are available...	
No active forums availab	

creating a PIN Group (Session Name with Session PIN Code)

When you first start using the Impero Console there are a number of predefined default User Groups created. It is then necessary to create/modify new Computer/User/PIN groups as required by your organisation (Image 6).

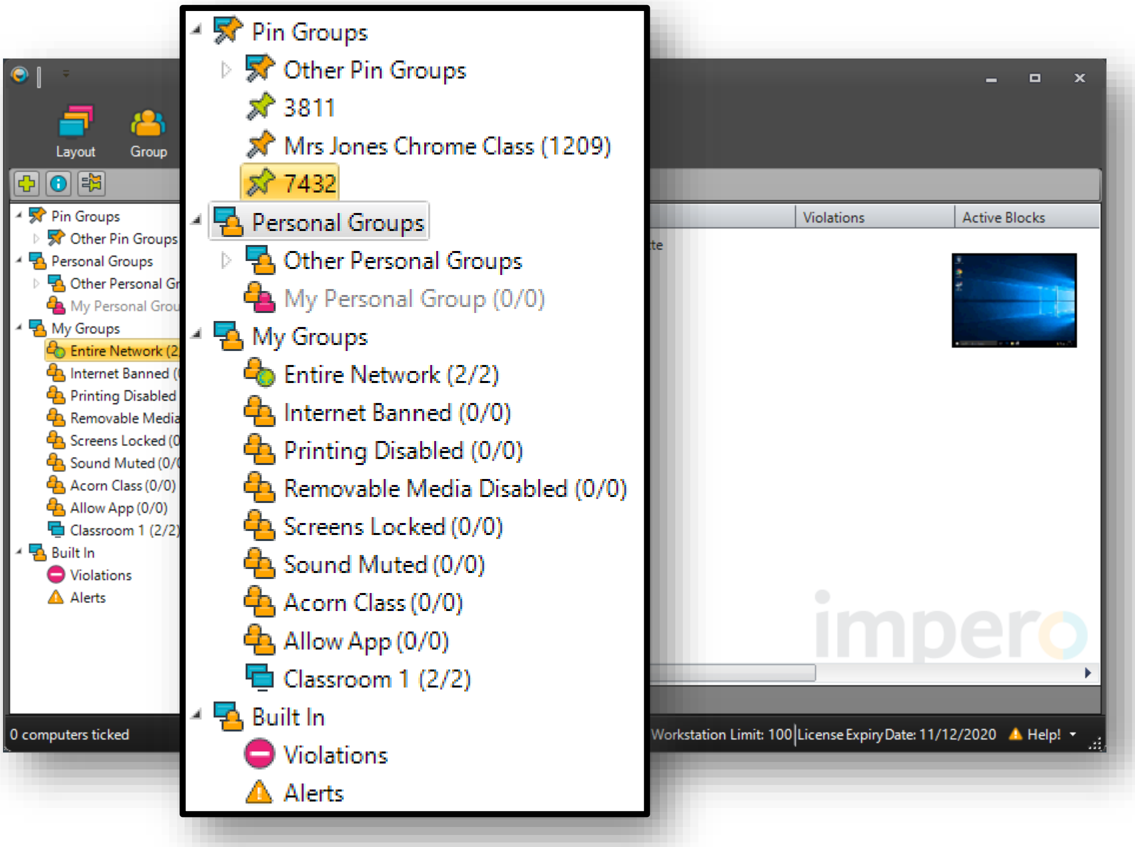


Image 6 - Default Groups/Created Groups/PIN Groups

To create a new PIN Group, click on the PIN icon that appears above the Group Lists (Image 7).

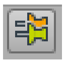
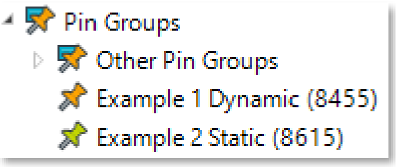


Image 7 - New PIN Group Icon

This will open the 'New PIN Group' window which allows you to begin the creation of the group. There are a number of options within this window that govern how your new PIN group is created and policies being applied to said group, which are explored in the next section. Different types of PIN Group are identified by the colour of the PIN icon (Image 8):



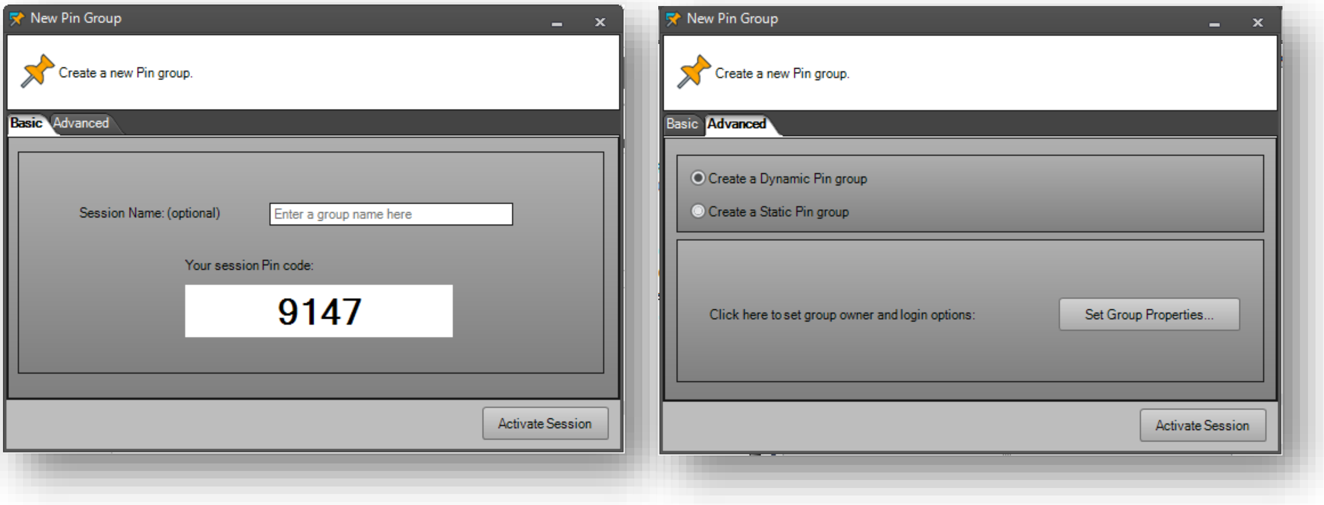
Orange pins are Dynamic Groups / Sessions.

Green pins are Static Groups / Sessions.

Image 8 – Pin group classifications

new PIN Group options

These options are spread over two tabs, Basic and Advanced, and allow you to set basic properties of your new group (Images 9 and 10).



Images 9 and 10 – Basic and Advanced tabs when creating a new PIN Group

creating a PIN Group – Basic options

Basic PIN Groups are usually the default type of PIN Group (determined by the server-based PIN group options).

- **Session Name (optional)**: the name of the group is how it will then be displayed in the PIN Grouplist

- **Your Session PIN code**: a pre-defined number, so as to ensure there are no duplications of PIN Group numbers by users

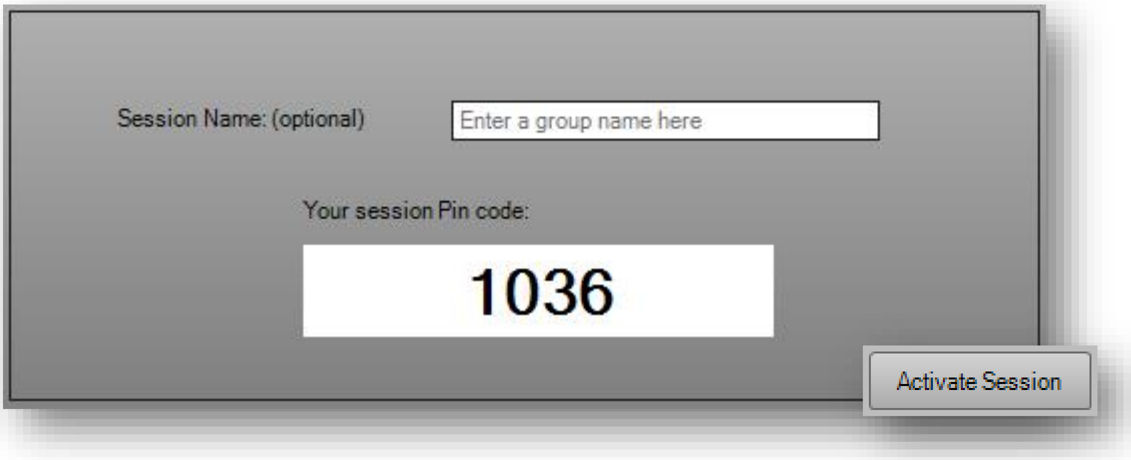


Image 11 – Static PIN Group options

By selecting the Activate Session button, rules for policies are the same as for all other groups. PIN groups will inherit policies from 'Entire Network' and any other groups the user is a member of.

creating a PIN Group – Advanced options

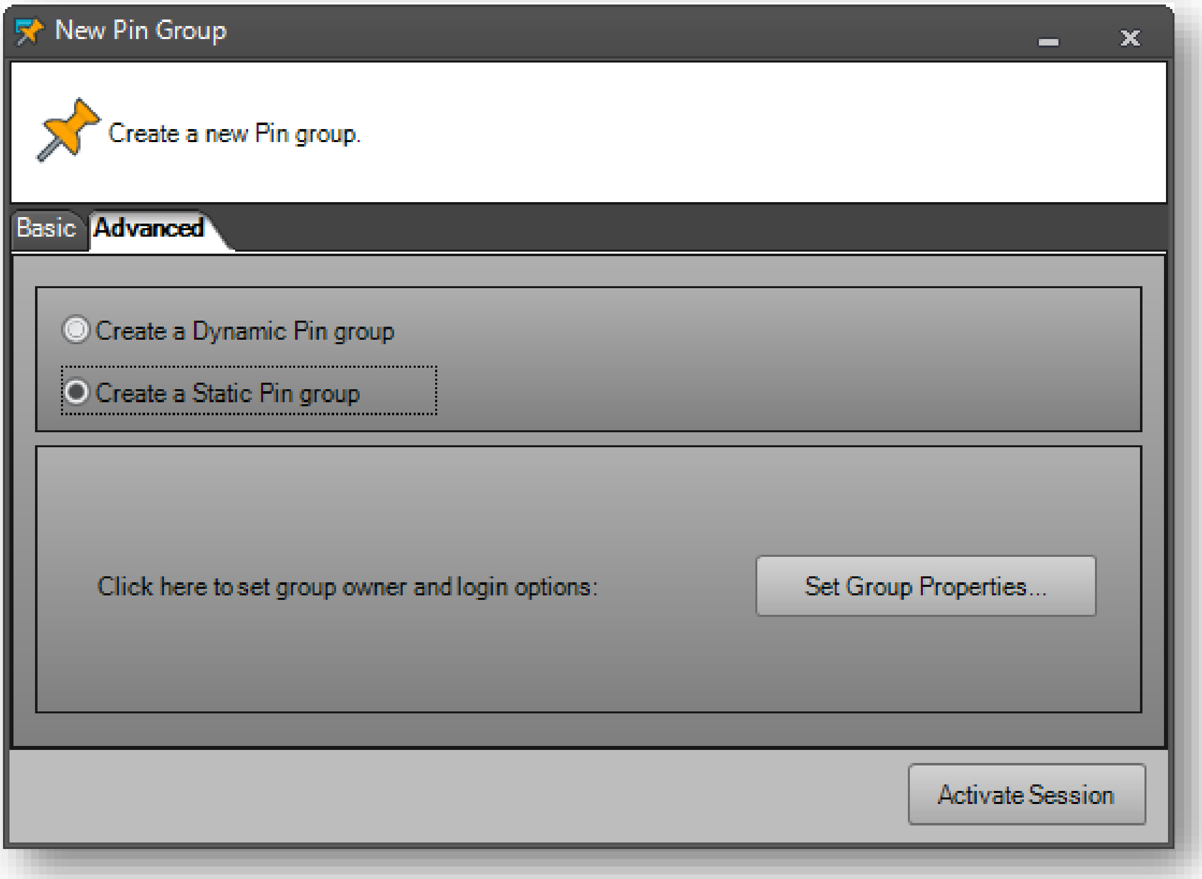

New Pin Group
Create a new Pin group.
Basic
Advanced
○ Create a Dynamic Pin group
○ Create a Static Pin group
Click here to set group owner and login options:
Set Group Properties...
Activate Session

Image 12 – Advanced Tab

Under the 'Advanced' tab (Image 12), users have two options:

create a Dynamic PIN Group

This is a one-off, live group session, linking devices based on a shared PIN number, so that when logged in using the session PIN code the end user's devices can be visible as one group within the live thumbnail, list and room layout views in the Impero admin console. Dynamic PIN Groups will be automatically removed when users close their Impero Console.

Dynamic groups are the default type and offer one-click creation.

create a Static PIN Group

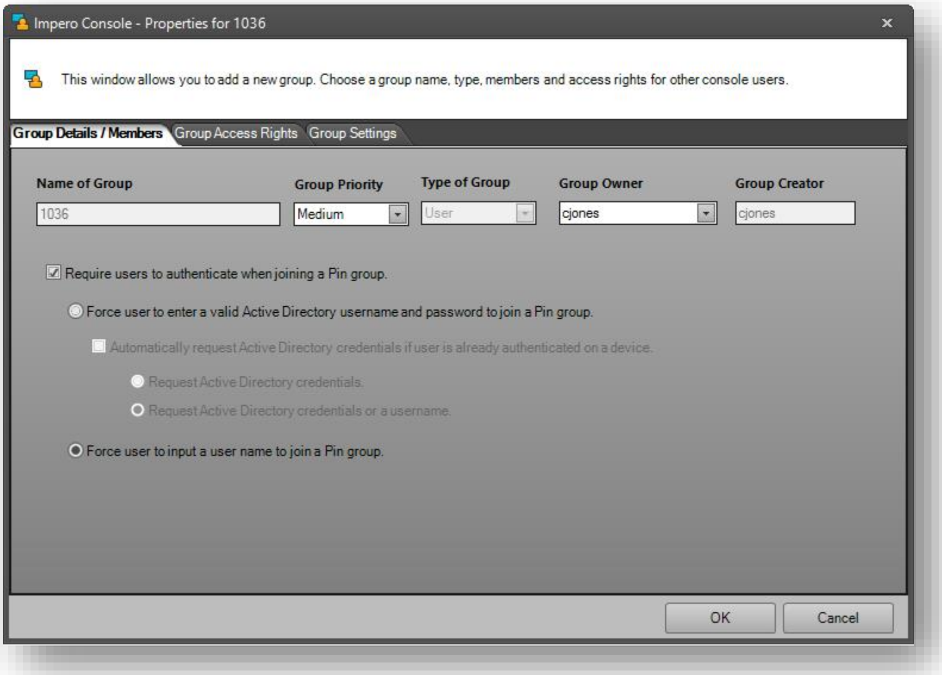
This is a live group session, linking devices based on a shared PIN number, so that when logged in using this number the end user's devices can be visible as one group within the live thumbnail, list and room layout views in the admin console. Unlike the Dynamic PIN Groups, the Static PIN Group and its settings can be saved in the console for future use by a teacher/console user.

‘Set Group Properties’ button

Users have the option to set group properties either during the setup process or retrospectively if required. The ‘Set Group Properties’ button enables you to choose the group’s priority and owner, as well as determining authentication requirements for when end users join the group. This includes forcing users to enter a valid Active Directory username and password.

These settings also determine the authentication screens that a student is presented with when they join a PIN Group session. The authentication options are automatically populated to reflect the choices selected in the PIN Groups settings on the server, but can also be edited on an individual basis.

‘Group Details/Members’ tab



Impero Console - Properties for 1036

This window allows you to add a new group. Choose a group name, type, members and access rights for other console users.

Name of Group	Group Priority	Type of Group	Group Owner	Group Creator
1036	Medium	User	cjones	cjones

☑ Require users to authenticate when joining a Pin group.

○ Force user to enter a valid Active Directory username and password to join a Pin group.

□ Automatically request Active Directory credentials if user is already authenticated on a device.

○ Request Active Directory credentials.

○ Request Active Directory credentials or a username.

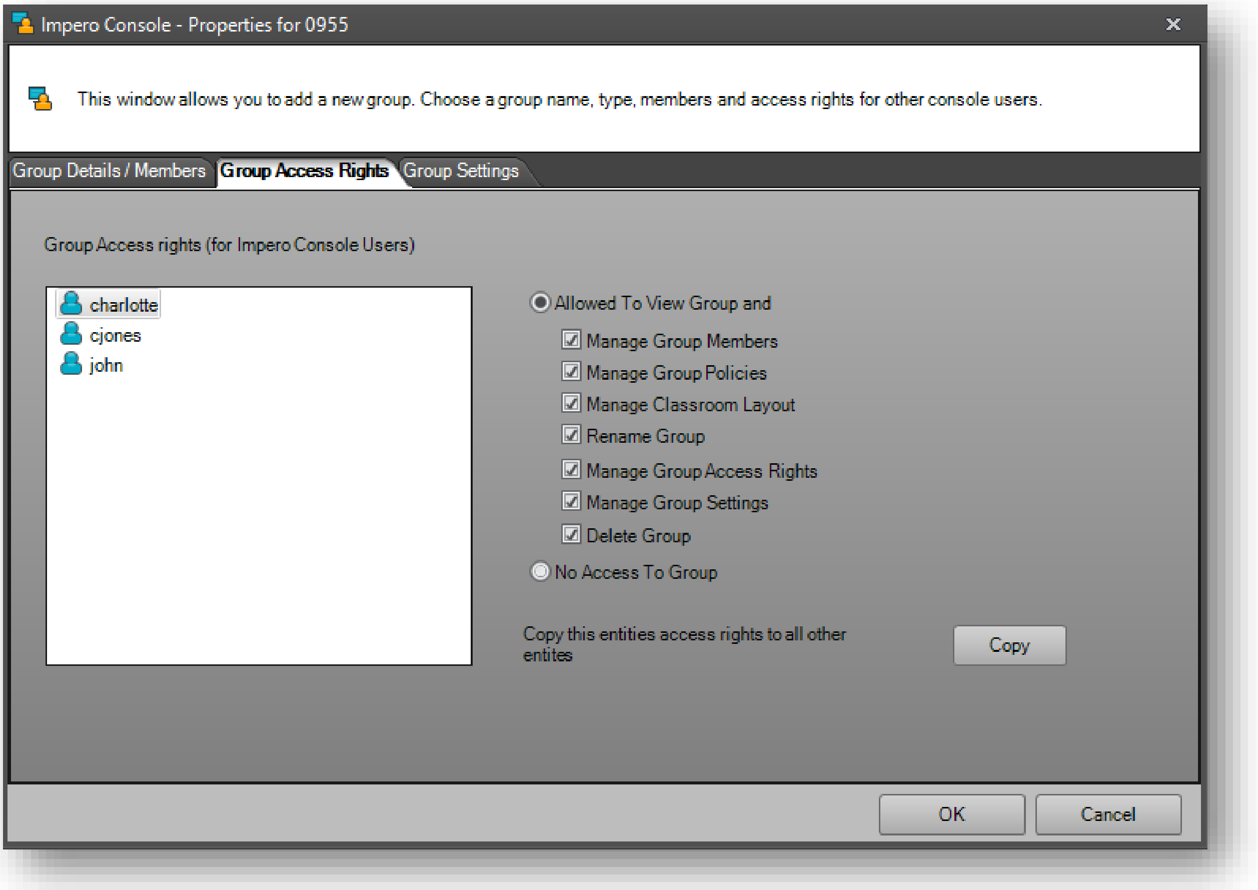
● Force user to input a user name to join a Pin group.

Image 13 – Group Details/Members tab

- **‘Group Priority’ option** - this refers to the properties of the group (Group Settings options) and **not** the Policies of the group. The entire network level is set as ‘Medium’ by default although users are recommended to set PIN Group priorities as low.

‘Group Access Rights’ tab

The 'Group Access Rights' tab (Image 14) allows you to configure the access privileges that Impero Console users have to the group that you are creating.



Impero Console - Properties for 0955

This window allows you to add a new group. Choose a group name, type, members and access rights for other console users.

Group Details / Members | Group Access Rights | Group Settings

Group Access rights (for Impero Console Users)

- charlotte
- cjones
- john

● Allowed To View Group and

- ☑ Manage Group Members
- ☑ Manage Group Policies
- ☑ Manage Classroom Layout
- ☑ Rename Group
- ☑ Manage Group Access Rights
- ☑ Manage Group Settings
- ☑ Delete Group

○ No Access To Group

Copy this entities access rights to all other entites

Image 14 - Group Access Rights

- **Group Access rights (for Impero Console Users)**
  This displays a list of the users that have been granted Console access via the Impero Server. Select the user that you wish to modify the access rights for by clicking on them. In Image X, user ‘Charlotte’ is selected. Mark the relevant checkboxes to determine access levels for the selected user.

- **Allowed To View Group and**
  The console user has access to view the group, as well as perform any further selected options.

- **Manage Group Members**
  The console user has the ability to add/remove users to this group.

- **Manage Group Policies**
  The console user is able to add/modify/remove any policies (Block List/Allow List/Keyword Detection/Advanced Policies) applied to the group.

- **Manage Classroom Layout**
  The console user is able to modify the Room Layout of the group (Computer Groups only).

- **Rename Group**
  The console user has access to change the name of the group.

- **Manage Group Access Rights**
  The console user is able to make changes to Group Access Rights (this window) for this group.

- **Manage Group Settings**
  The console user can make changes to the Group Settings (the third tab in 'Add Group').

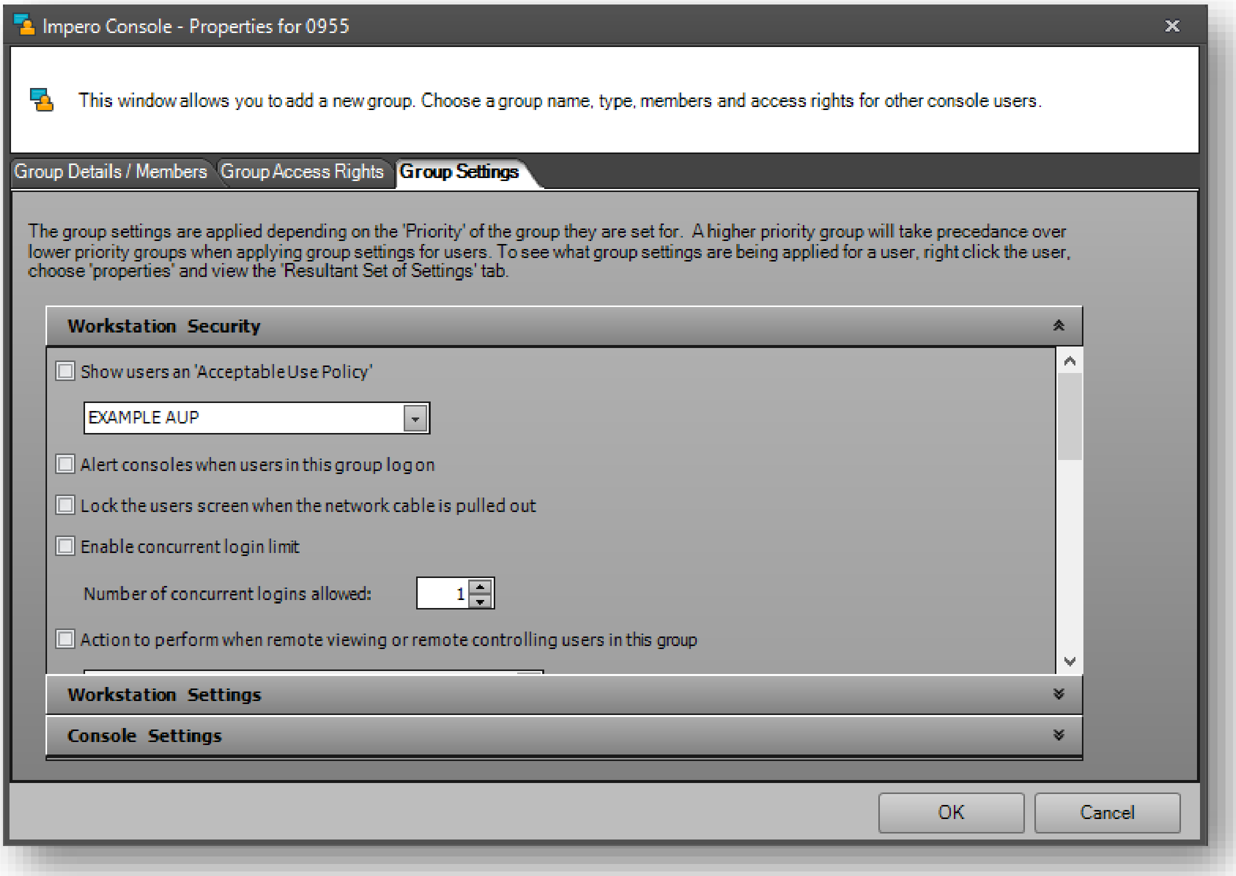
- **Delete Group**
  The console user is allowed to delete this group.

- **No Access To Group**
  The console user does not have any access rights to the group.

- **Copy**
  Clicking the 'Copy' button will copy the access rights of the selected console user to the rest of the console users in the list. For example, if user 'Becky' has access to only 'Rename Group' and 'Delete Group', you can select 'Becky', click the 'Copy' button, and then the rest of the console users will then have access to the same two options.

‘Group Settings’ tab

The 'Group Settings' tab (Image 15) allows you to apply a range of functions to the group you are creating.



Impero Console - Properties for 0955

This window allows you to add a new group. Choose a group name, type, members and access rights for other console users.

The group settings are applied depending on the 'Priority' of the group they are set for. A higher priority group will take precedance over lower priority groups when applying group settings for users. To see what group settings are being applied for a user, right click the user, choose 'properties' and view the 'Resultant Set of Settings' tab.

Workstation Security

□ Show users an 'Acceptable Use Policy'

EXAMPLE AUP

□ Alert consoles when users in this group log on

□ Lock the users screen when the network cable is pulled out

□ Enable concurrent login limit

Number of concurrent logins allowed: 1

□ Action to perform when remote viewing or remote controlling users in this group

Workstation Settings

Console Settings

Image 15 - Group Settings

Workstation Security

- **Show users an 'Acceptable Use Policy'**
  You have the option to show users an 'Acceptable Use Policy' either the first time they log in, or each time they log in. You can set up different AUPs for different groups of users.

  Note: The Acceptable Use Policies are set up in the Impero Server.

- **Alert consoles when users in this group logon**
  This will alert any console users that a user within this group has logged onto the system.

- **Lock the users screen when the network cable is pulled out**
  If network cable is removed from the remote computer, the screen will be locked.

- **Enable concurrent login limit**
  Set the number of concurrent logon sessions that one username can have active at any one time within this group.

- **Action to perform when remote viewing or remote controlling users in this group**
  If this is set then you can choose what happens when the user is being remotely controlled.

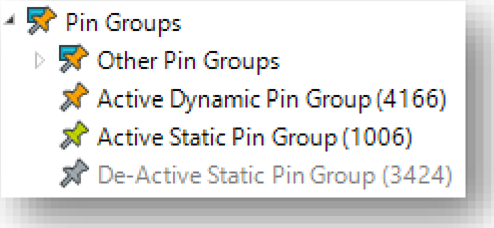
  - **Allow** - Allow remote controlling of these users.
  - **Deny** - Do not allow remote controlling of these users. If this option is selected, the Thumbnail View for this group will display only a black window with the text 'Access Denied'.
  - **Ask if Allowed (Auto ALLOW after 10 seconds)** - Ask the remote user's permission to take control. Control is automatically allowed after 10 seconds if no response is given.
  - **Ask if Allowed (Auto DENY after 10 seconds)** - Ask the remote user's permission to take control. Control is automatically denied after 10 seconds if no response is given. If this option is selected, the Thumbnail View for this group will display only a black window with the text 'Access Denied'.

- **Force a log off when user is idle for more than**
  This option allows Impero to log the current user off when a machine has been idle for a specified number of minutes.

- **Force a shutdown when user is idle for more than**
  This option allows Impero to shut the machine down when a machine has been idle for a specified number of minutes.

- **Action to perform when users raise 'Minor'/'Moderate'/'Severe' violations**
  You can perform an action after a violation is triggered a specified number of times at each of the different levels. The actions you can set are to have the screen locked, the internet disabled, log the user off or to move the user to a specific group, all for a specified amount of time. Once the time has expired they are automatically removed from that group.

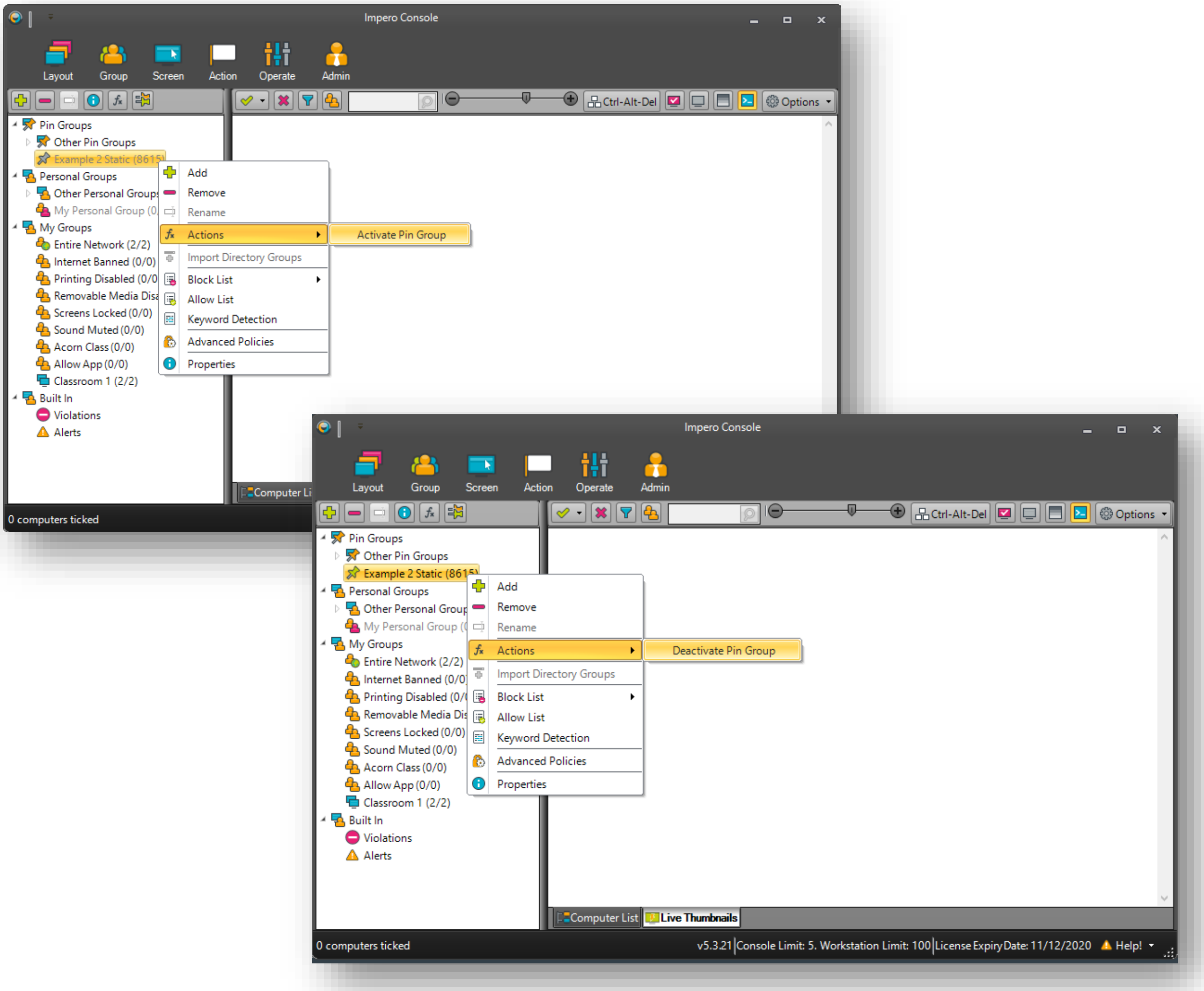
activating and deactivating PIN Groups



Pin Groups
Other Pin Groups
Active Dynamic Pin Group (4166)
Active Static Pin Group (1006)
De-Active Static Pin Group (3424)

A grey PIN signifies that the current PIN Group/Session is in-active. To activate and deactivate a PIN group, users need to right click the relevant PIN, hover over 'Action' and select either activate or deactivate group.

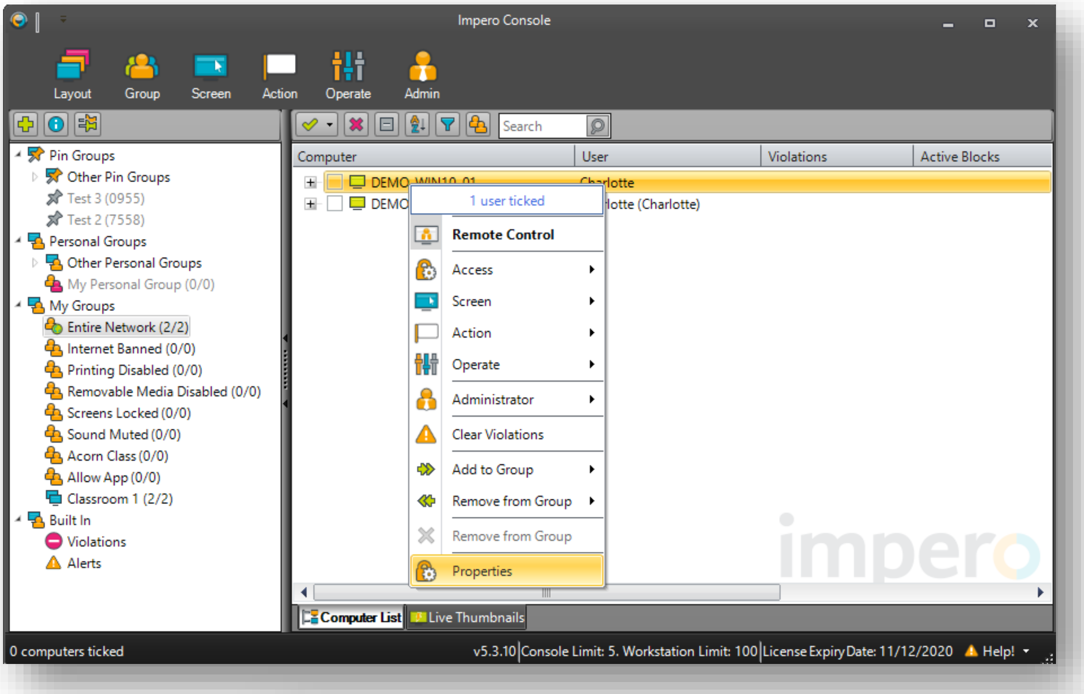
Please note: You cannot deactivate a dynamic group which by its very nature is only active for that session.

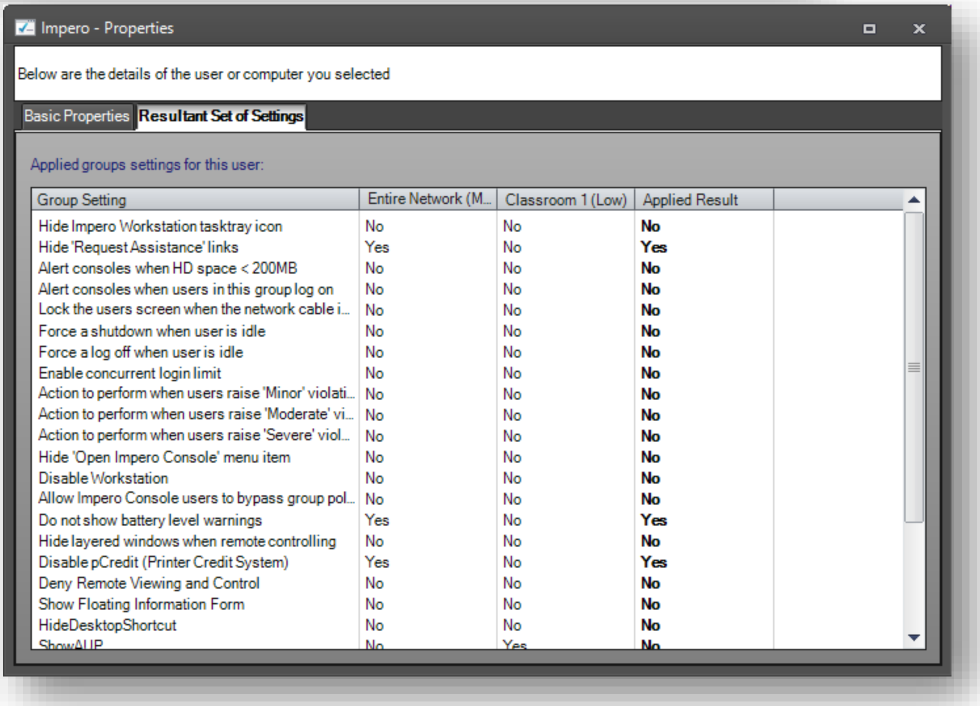


Images 16 and 17 – Activating and deactivating PIN Groups

identifying which settings take precedence 'Resultant Set of Settings'

As explained above, group settings are applied depending on the 'Priority' of the group they are set for. A higher priority group will take precedence over lower priority groups when applying group settings for users. To see what group settings are being applied for a user, from the Impero Console right click a user, choose 'Properties' and view the 'Resultant Set of Settings' tab.





Below are the details of the user or computer you selected

Applied groups settings for this user:

Group Setting	Entire Network (M...	Classroom 1 (Low)	Applied Result
Hide Impero Workstation tasktray icon	No	No	**No**
Hide 'Request Assistance' links	Yes	No	**Yes**
Alert consoles when HD space < 200MB	No	No	**No**
Alert consoles when users in this group log on	No	No	**No**
Lock the users screen when the network cable i...	No	No	**No**
Force a shutdown when user is idle	No	No	**No**
Force a log off when user is idle	No	No	**No**
Enable concurrent login limit	No	No	**No**
Action to perform when users raise 'Minor' violati...	No	No	**No**
Action to perform when users raise 'Moderate' vi...	No	No	**No**
Action to perform when users raise 'Severe' viol...	No	No	**No**
Hide 'Open Impero Console' menu item	No	No	**No**
Disable Workstation	No	No	**No**
Allow Impero Console users to bypass group pol...	No	No	**No**
Do not show battery level warnings	Yes	No	**Yes**
Hide layered windows when remote controlling	No	No	**No**
Disable pCredit (Printer Credit System)	Yes	No	**Yes**
Deny Remote Viewing and Control	No	No	**No**
Show Floating Information Form	No	No	**No**
HideDesktopShortcut	No	No	**No**
ShowAUP	No	Yes	**No**

Images 18 and 19 – Properties and Group Settings

PIN Groups on Chromebooks

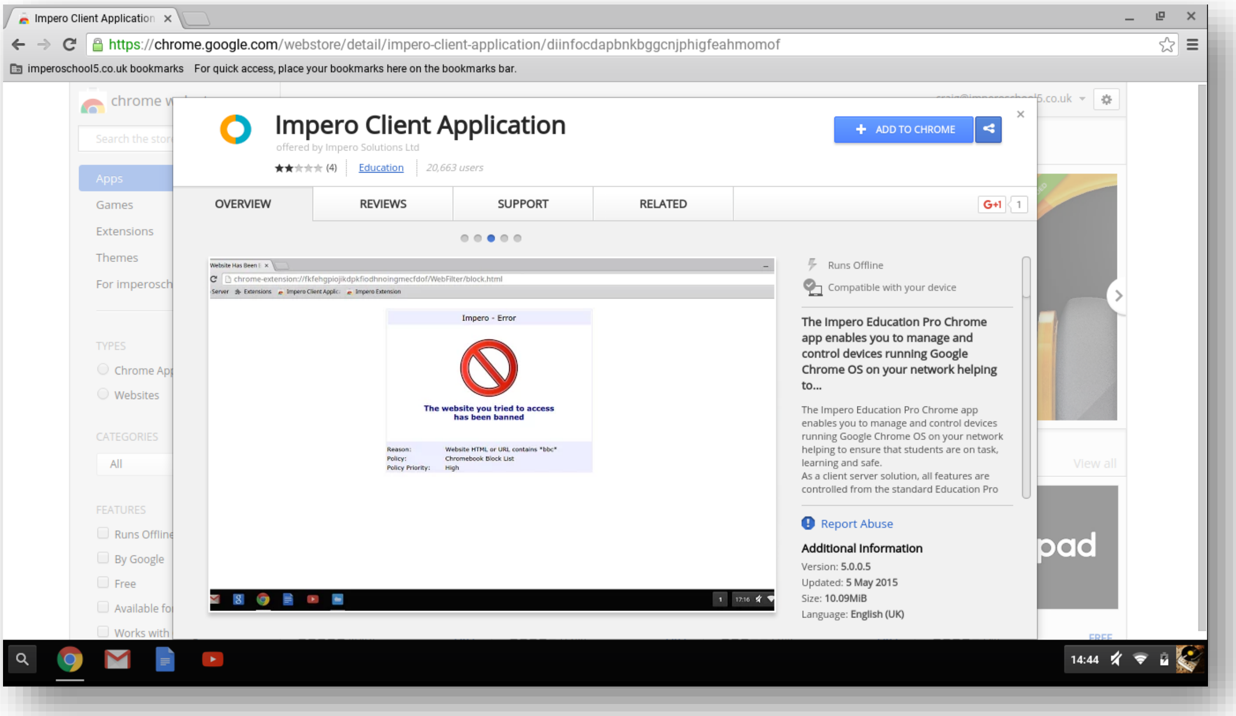
introduction

The Impero Client Application and Impero Client Extension for Chromebook allow you to integrate your Chromebook devices with your Impero Education Pro network. There are two applications that you need to download from the Chrome Web Store in order to join your Chromebook device to your network. You are required to be running Impero version 4.2.20 or later in order to view Chromebook screens from your Impero Console.

Once installed on your device, the applications can be configured to connect to your Impero Server and become viewable from your Impero Console.

application Download

In order to configure your Chromebook, you will need to download the Impero Client Application and Impero Client Extension from the Chrome Web Store. Click on the 'FREE' button in order to download and install the two applications.



https://chrome.google.com/webstore/detail/impero-client-application/diinfocdapbnkbggcnjphigfeahmomof

Impero Client Application

offered by Impero Solutions Ltd

(4) | Education | 20,663 users

The Impero Education Pro Chrome app enables you to manage and control devices running Google Chrome OS on your network helping to...

The Impero Education Pro Chrome app enables you to manage and control devices running Google Chrome OS on your network helping to ensure that students are on task, learning and safe.
As a client server solution, all features are controlled from the standard Education Pro

Additional Information

Version: 5.0.0.5
Updated: 5 May 2015
Size: 10.09MiB
Language: English (UK)

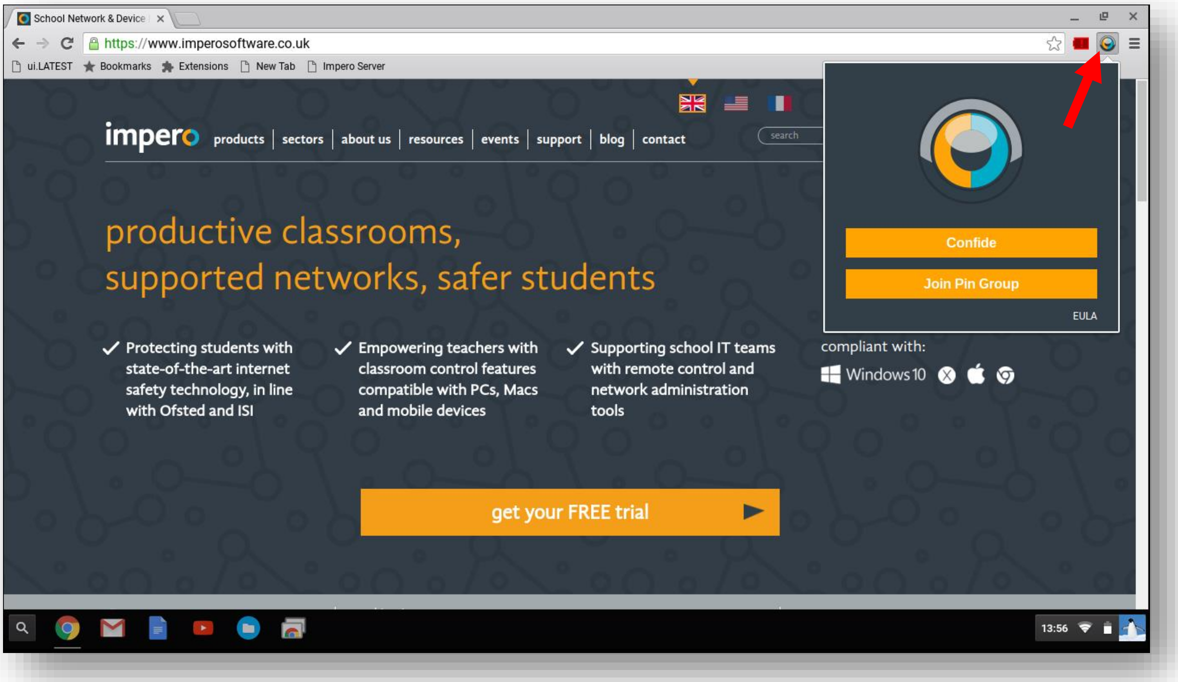
Impero Client Application
imperoschool5.co.uk bookmarks
For quick access, place your bookmarks here on the bookmarks bar.
ADD TO CHROME
OVERVIEW
REVIEWS
SUPPORT
RELATED
G+1
Apps
Games
Extensions
Themes
TYPES
CATEGORIES
FEATURES
Runs Offline
Compatible with your device
Impero - Error
The website you tried to access has been banned
Reason: Website HTML or URL contains *bbc*
Policy: Chromebook Block List
Policy Priority: High
Report Abuse
14:44

When prompted to confirm the new applications, click on the 'Add to Chrome' button.

To verify that your applications have installed, launch your Google Chrome browser and navigate to 'chrome://extensions'.

Ensure that 'Impero Client Application' and 'Impero Client Extension' both appear in your list of browser extensions and are both set to 'Enabled'.

connecting to a PIN Group from a Chromebook

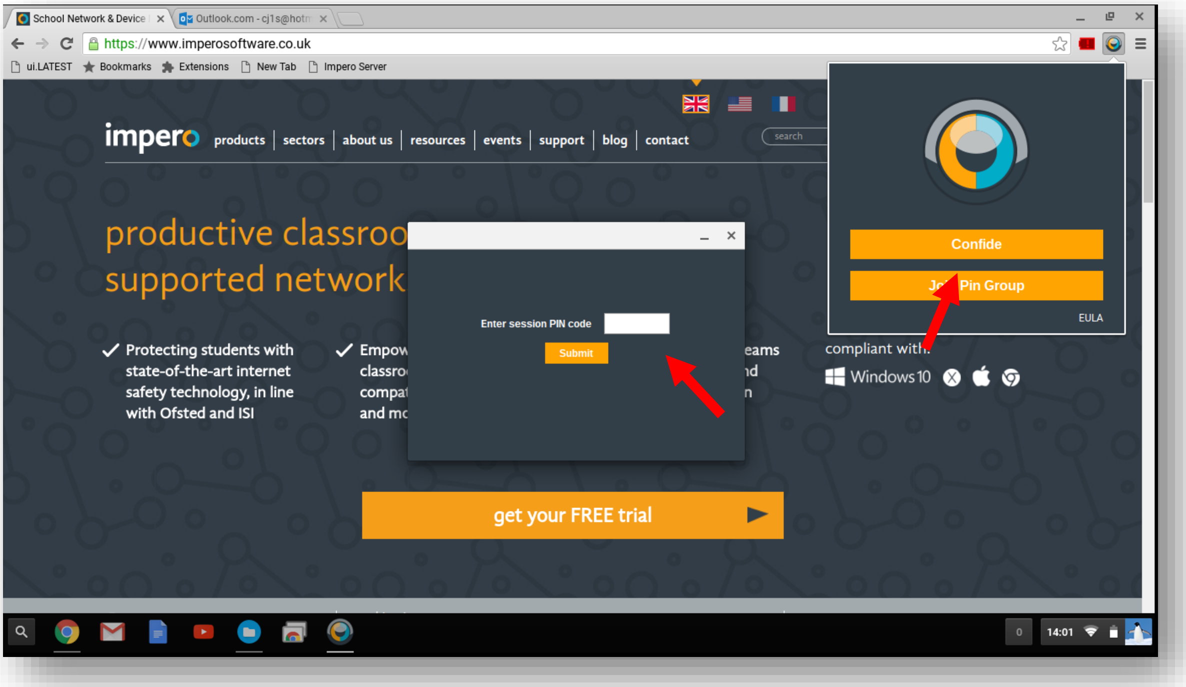


productive classrooms, supported networks, safer students

✓ Protecting students with state-of-the-art internet safety technology, in line with Ofsted and ISI

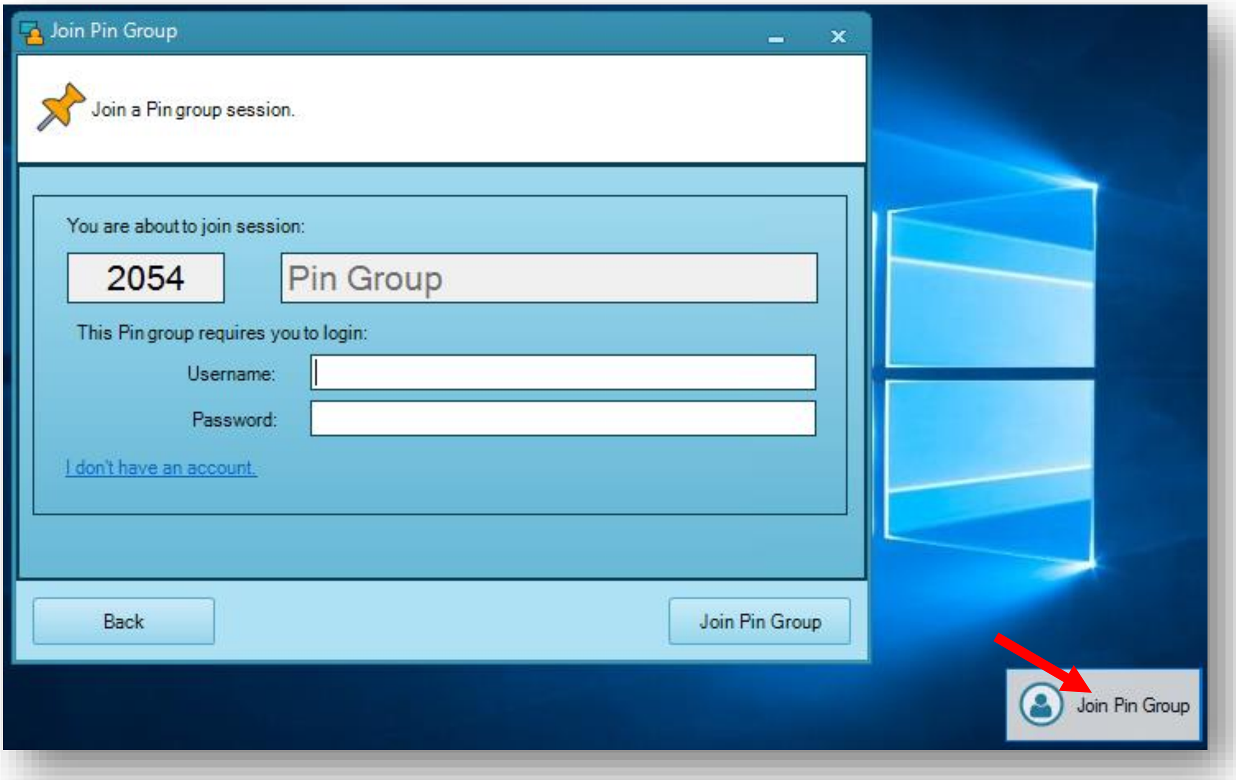
✓ Empowering teachers with classroom control features compatible with PCs, Macs and mobile devices

✓ Supporting school IT teams with remote control and network administration tools



Enter session PIN code

connecting to a PIN Group from a Windows Device


Join Pin Group

Join a Pin group session.

You are about to join session:

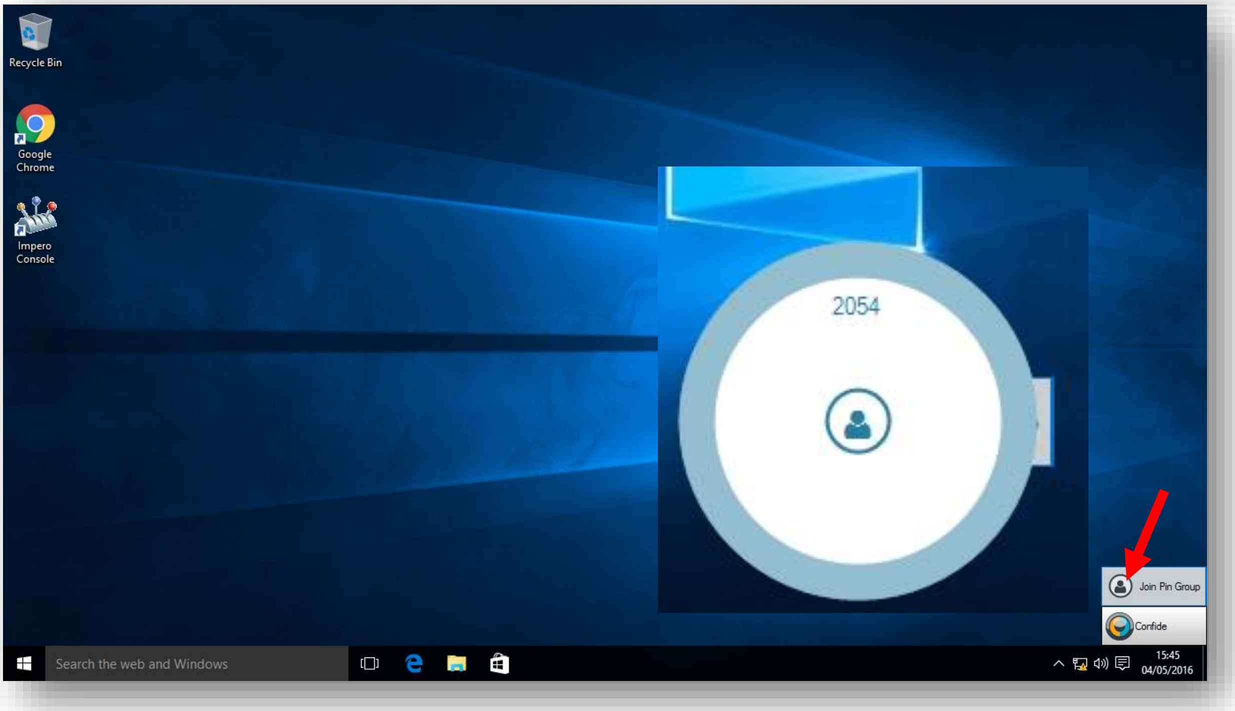
2054 Pin Group

This Pin group requires you to login:

Username:

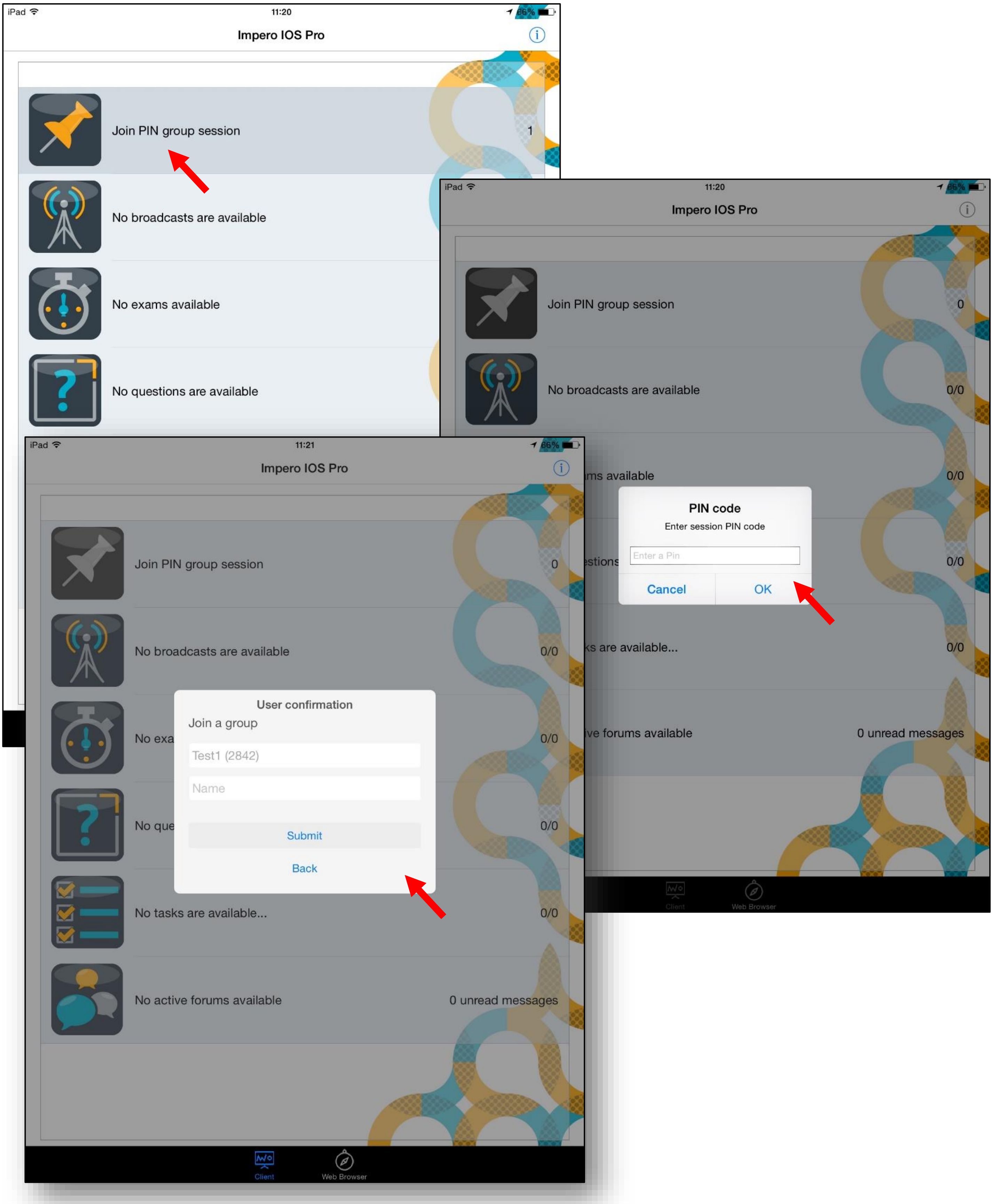
Password:

I don't have an account.



By selecting the Circle button within the 'Join PIN Group' box, you can quickly identify which PIN group session the end user is a member of and if required leave the PIN group session.

connecting to a PIN Group from an iPad



Join PIN group session 1

No broadcasts are available

No exams available

No questions are available

Join PIN group session 0

No broadcasts are available 0/0

ms available 0/0

PIN code

Enter session PIN code

Enter a Pin

estions 0/0

ks are available... 0/0

ve forums available 0 unread messages

Join PIN group session 0

No broadcasts are available 0/0

User confirmation

Join a group

Test1 (2842)

Name

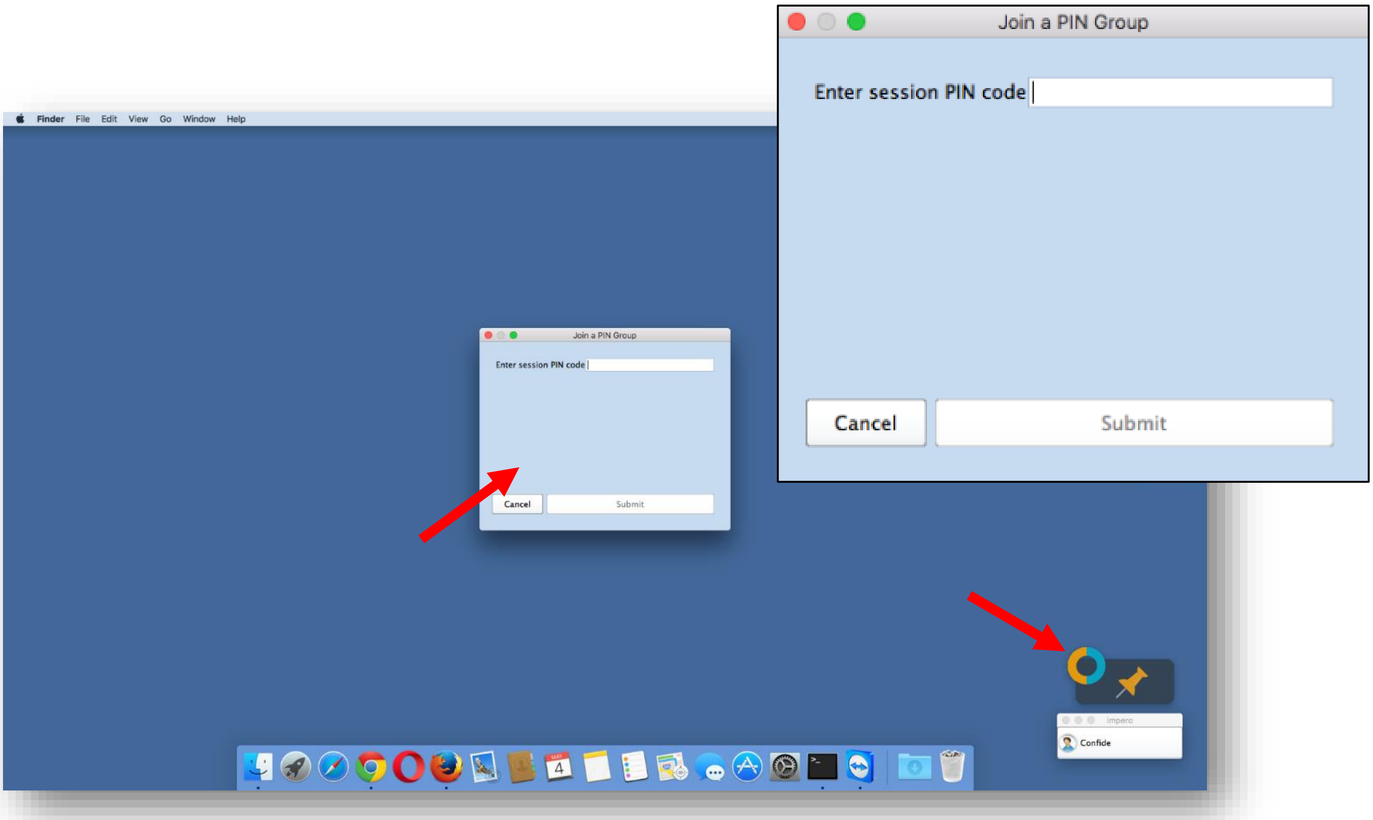
No exa 0/0

No que 0/0

No tasks are available... 0/0

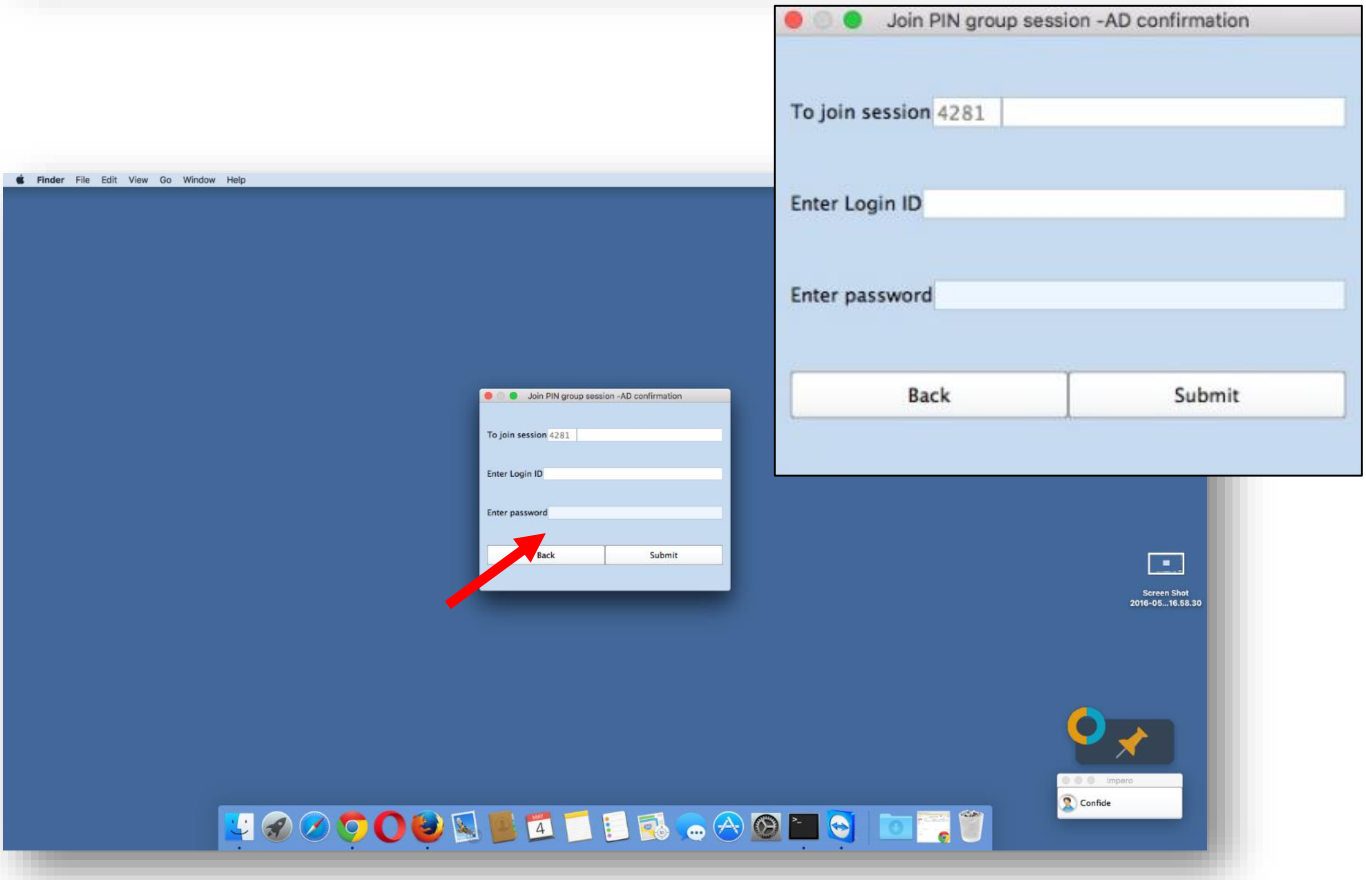
No active forums available 0 unread messages

connecting to a PIN Group from a Mac



Join a PIN Group

Enter session PIN code



Join PIN group session -AD confirmation

To join session 4281

Enter Login ID

Enter password

Back
Submit
Finder File Edit View Go Window Help
Screen Shot 2016-05...16.58.30
Impero
Confide

info@imperosoftware.com

www.imperosoftware.co.uk

www.imperosoftware.com

+44 (0) 1509 606582 UK

877-883-4370 USA