



Extreme Networks Extreme Management Center[®]

Policy Control Console User Guide

Copyright © 2016 Extreme Networks, Inc. All Rights Reserved.

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.,
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800

Toll-free: +1 888-257-3000



Extreme Networks® Software License Agreement

This Extreme Networks Software License Agreement is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc. ("Extreme"), on behalf of itself and its Affiliates (as hereinafter defined and including its wholly owned subsidiary, Enterasys Networks, Inc. as well as its other subsidiaries). This Agreement sets forth Your rights and obligations with respect to the Licensed Software and Licensed Materials. BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.
2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications

and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.

3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. **YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.**
4. LICENSE TYPES.
 - *Single User, Single Computer.* Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).
 - *Client.* Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.
5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to

Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.

6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED

MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme's prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS

- a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers.

This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

- b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Extreme

of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.
10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.
 - a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.
 - b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.
11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.
12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in

accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.
- NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.
- Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply

to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.
15. GENERAL.
 - a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.
 - b. This Agreement may not be changed or amended except in writing signed by both parties hereto.
 - c. You represent that You have full right and/or authorization to enter into this Agreement.
 - d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme's assignees, licensors, and licensees.
 - e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.
 - f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.
 - g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.
 - h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other

communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134 United States
ATTN: General Counsel

Table of Contents

- Legal Notices i
- Trademarks i
- Support i
- Contact i
- Extreme Networks® Software License Agreement ii
- Table of Contents x
- Extreme Management Center® Policy Control Console Help 1
 - Policy Control Console Features 1
 - Document Version 2
- Policy Control Console Concepts 3**
 - Overview 3
 - Location Hierarchy 5
 - User Groups 6
 - Policy Groups 7
 - Enforcing 9
- Getting Started with Policy Control Console 11**
 - Setting Up PCC 11
 - Explore PCC Features 11
 - Getting Started-Plan your Locations, User Groups, and Policy Groups13
 - Getting Started-Create the Locations Tree16
 - Getting Started-Create Your Policy Groups17
 - Getting Started-Create Your User Groups19
 - Getting Started-Configure Locations23
 - Getting Started-Check Consistency25
 - Getting Started-Accessing the PCC Web Page27

How To Use Policy Control Console	29
How to Change Messaging Credentials on the PCC Engine	30
How to Configure the PCC Web Server	32
LDAP Authentication Configuration	32
Modify Port Values	33
Change the Default Login	34
Customize the PCC Web Page	35
Customizing the PCC Web Page Header	35
Customizing the PCC Web Page Footer	36
Customizing the Policy-Management Table	36
How to Initialize PCC Database Components	38
How to Set PCC Options	39
How to Use Scripts	40
Writing and Storing Scripts	40
Adding Scripts to Policy Groups	41
Assigning Scripts to Locations	42
How to Use the PCC Web Page	43
Policy Management	44
Administration	46
Options	47
NetSight Server	48
PCC Log	48
Change Password	48
Scheduling	49
Policy Control Console Right-Panel Tabs	52
Locations Tab	53

Properties Tab (Folder)	54
Properties Tab (Location)	55
User Groups Tab	57
User Groups	57
Users	58
Ports Tab	60
Policy Control Console Windows	62
Activity Report Window	63
Add Ports Window	65
Add User Window	67
Login Users	67
Static IP Users	68
Appliance Events Window	71
Assign Policy Groups Window	74
Assign User Groups Window	76
Assign Users Window	78
Assigned Ports Window	80
Check Consistency Window	82
Allowed Policies not created on Devices Tab	83
Default Policies not allowed in Location Tab	84
Default Policies that differ Tab	86
Edit User Window	88
Login Users	88
Static IP Users	89
Policy Control Console Main Window	91
Menu Bar	92

File Menu	92
Tools Menu	93
Help Menu	94
Right-click Menu Options	94
Toolbar	95
Event View	96
Events Tab	96
Right-click Menu Options	98
Appliances Tab	98
Manage Policy Groups Window	100
All Policy Groups View	100
Properties Tab	101
Policies Tab	102
Policy Properties Tab	104
Manage Users Window	106
All User Groups View	106
Properties Tab - User Group	107
Allowed Locations Tab - User Group	108
Allowed Policy Groups Tab - User Group	109
Assigned Users Tab - User Group	111
Mapped Authorization Groups Tab - User Group	112
All Users View	113
Properties Tab - User	115
Scheduling Details	118
Details	118
Enable Recurrence	119

Extreme Management Center® Policy Control Console Help

Policy Control Console (PCC) is a tool that allows IT to delegate control of network usage to less technical personnel, and is accessed from the NetSight Console Tools menu. Using a simple web interface, authorized users select from a predefined set of network usage policies (created via Policy Manager) to regulate network access for specified locations in the network. This provides personnel such as administrative assistants, department managers, and professors, with the ability to permit or deny access to the Internet, e-mail, and other network services that might otherwise disrupt a meeting or lecture.

Policy Control Console Features

Integrated with NetSight Console for centralized management

Policy Control Console management is easily accessed from the NetSight Console Tools menu.

Leverages NetSight Policy Manager

Further extends the power and flexibility of NetSight Policy Manager to create and enforce network usage policies.

Extends network control to less technical personnel

Delegates network control to less technical personnel by allowing authorized users the ability to determine network access in specific locations.

Easy-to-use Web Interface

Provides a highly flexible and customizable set of controls through a simple web interface that enables authorized users to turn services on and off with just a click.

Maintains overall security

Limits control to simple tasks applied to specific rooms or work spaces within a facility. Only authorized users as defined by IT have control, so security is not compromised.

Benefits the IT staff

Creates a more self-sufficient enterprise and frees IT from the time-consuming task of applying and changing usage policies.

Document Version

The following table displays the revision history for the Policy Control Console Help documentation.

Date	Revision Number	Description
06-16	7.0 Revision -00	Extreme Management Center (NetSight) 7.0 release
07-15	6.3 Revision -00	NetSight 6.3 release
01-15	6.2 Revision -00	NetSight 6.2 release
06-14	6.1 Revision -00	NetSight 6.1 release
02-14	6.0 Revision -00	NetSight 6.0 release

PN: 9034987-01

Policy Control Console Concepts

This Help topic explains some of the concepts you'll need to understand in order to make the most effective use of Policy Control Console (PCC).

Information on:

- [Overview of Policy Control Console](#)
- [Location Hierarchy](#)
- [User Groups](#)
- [Policy Groups](#)
- [Enforcing](#)

Overview

PCC allows IT organizations to extend the power and capability of a secure network to non-technical users of network resources. This is accomplished through the use of the PCC management tool and an easy-to-use web interface where PCC end users perform the enforcement actions.

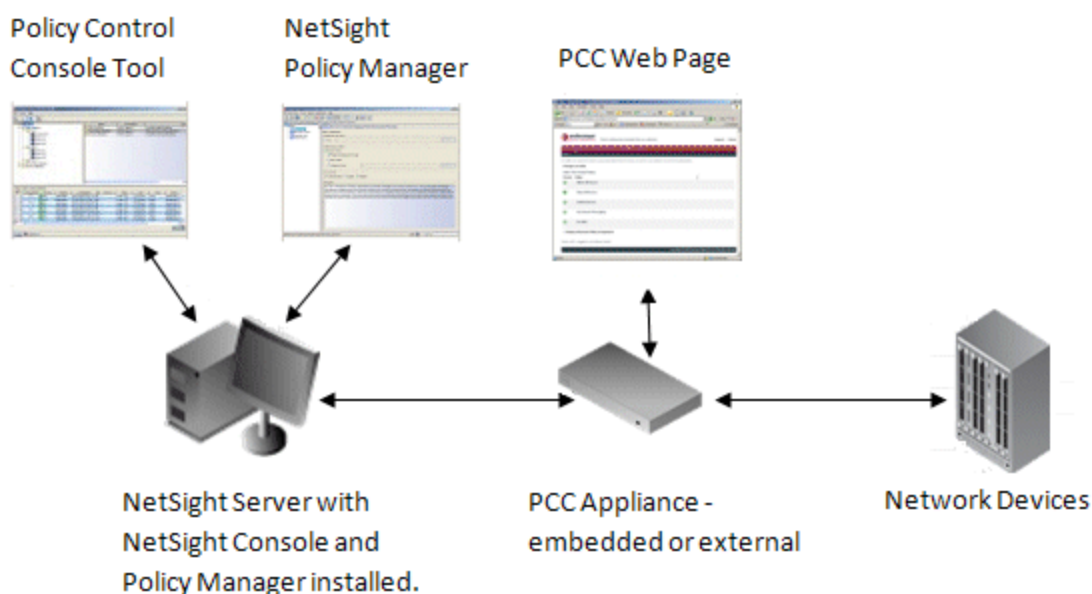
Using a simple web interface, PCC end users select from a predefined set of network usage policies (the actual policy roles are created via NetSight Policy Manager) to regulate network access for specified locations (such as a classroom or conference room) in the network. This provides personnel such as administrative assistants, department managers, and professors, with the ability to permit or deny access to the Internet, e-mail, and other network services that might otherwise disrupt a meeting or lecture.

When a PCC end user sets a usage policy for a location, PCC applies the selected policy as the default policy for the ports that have been configured as a location. This default policy specifies the network access that will be available for the location. For example, Professor Smith could set a policy for his classroom that denies e-mail and internet access while he is giving an exam.

The primary Policy Control Console components are:

- **Policy Control Console Tool** - the PCC management interface accessed from the NetSight Console Tools menu. PCC administrators use this tool to configure the PCC functionality.

- **PCC Appliance** - provides the web user interactions and sets default policy on the ports. The PCC appliance is provided by default as an embedded virtual appliance on the NetSight Server. Optionally, an external hardware appliance (SNS-PCC-WBA) can be used.
- **PCC Web Interface** - provides a web page where PCC end users configure network access for allowed locations.
- **Policy Manager** - used to create the policy roles and enforce them to network devices.



When setting up Policy Control Console, there are three main areas of functionality that the PCC administrator needs to configure:



- **Location Hierarchy and Configuration**- Create and organize the locations where network usage will be controlled. Define the ports that will be included in each location, and assign the PCC users (as part of a user group) that will be able to control the location and the policies that can be set.
- **User Groups** - Create and configure the PCC end users that will be setting the network usage policies via the PCC web page. Assign the users to user

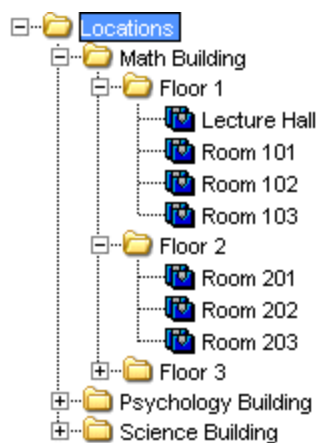
groups that determine the locations they will be able to control and the policies they will be able to set.

- **Policy Groups**- Create the groups that will contain the usage policies available for end users to set.

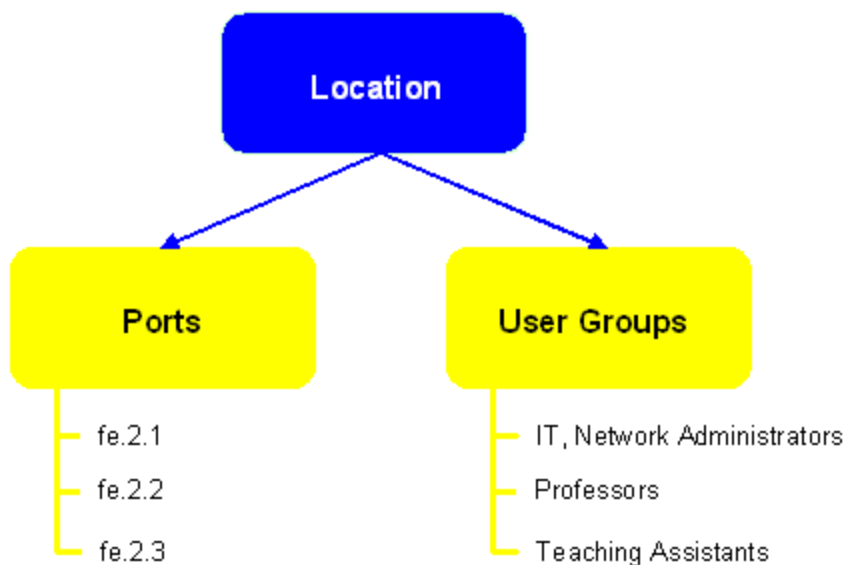
When these three areas have been configured, a PCC end user will be able to access the PCC Web page and set network usage policy for their allowed locations. For complete steps in how to configure this functionality, see [Getting Started](#).

Location Hierarchy

PCC uses a Locations tree to represent the campus, buildings, floors, rooms or other location-based entities where PCC end users will be able to control network usage. The Locations tree is displayed in the left-panel of the Policy Control Console main window. The folders and location icons in the tree represent the work spaces and specific rooms within a facility, and let you organize configurable ports into a hierarchy that can be easily managed by end users. Here is an example of what a Location tree might look like.



Each location in the tree has its assigned ports (the configurable ports for that location) and its assigned user groups (made up of the PCC end users that are allowed to set network usage policies for the ports in that location).



User Groups

PCC users are the authorized end users that will be able to set network usage policies on the ports in the locations. From the user's perspective, they will be managing a room or similar work space. Each end user is assigned to a user group that determines the locations that they can configure and policies they can select from.

There are two types of users:

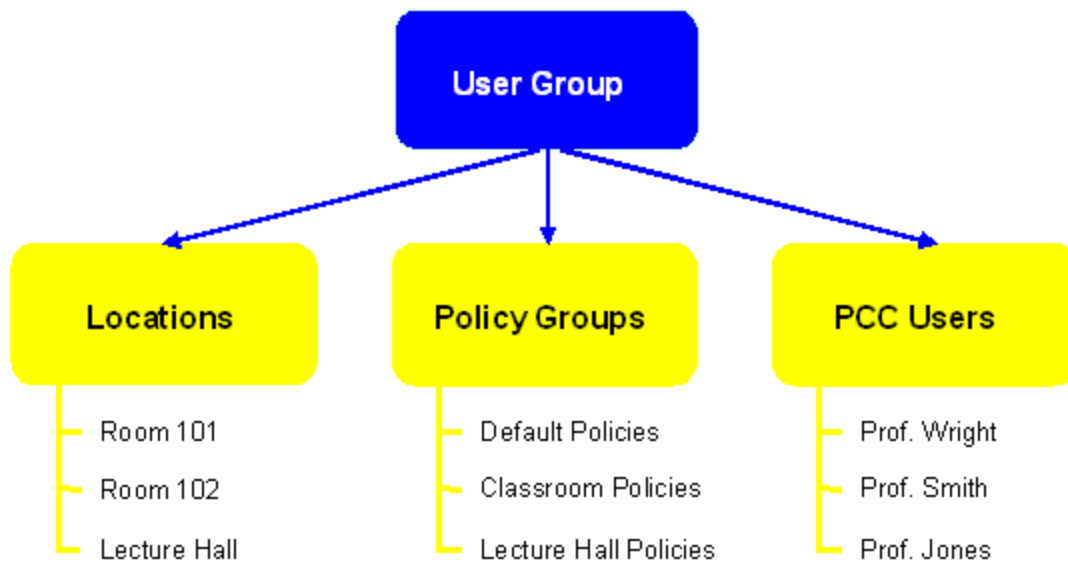
- Login Users- The user authenticates to access the PCC web page and set policies for their allowed locations.
- Static IP Users- This is a static system such as a "podium computer" that provides open access to the PCC web page to set policies for allowed locations (usually for that location only).

A login user can be configured with either Admin or Basic authorization; static IP users are always configured with Basic authorization.

- Admin - Provides access to the PCC web page to:
 - define and schedule policy for allowed locations.
 - configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
 - view a PCC activity log.

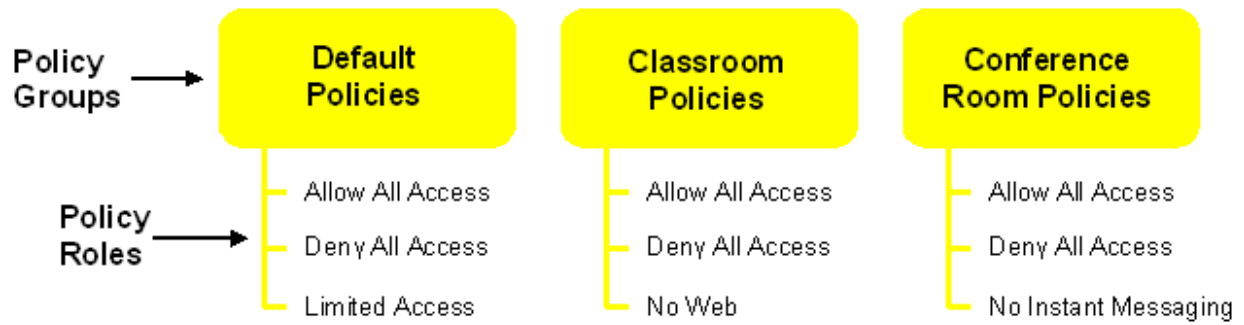
- Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - schedule policy for allowed locations (if access to the scheduling functionality was granted).

End users are grouped into user groups to simplify the assignment of allowed policy groups and locations. Each user group is assigned a set of allowed locations and allowed policy groups, along with the end users that will be allowed to set them.



Policy Groups

Policy groups let you group together the network usage policies that will be set as default policy for the ports in your locations. The actual policy roles themselves must be created and enforced to your network devices using NetSight Policy Manager. Policy groups let you organize your policy roles into logical groups that can be quickly assigned to your user groups. For example, you may create a "Classroom policy group" and a "Conference Room policy group" that contain the appropriate policy roles to allow or deny certain aspects of network usage for that type of location.



NOTE: In networks where access layer devices are non-policy enabled switches, PCC supports the use of scripts to set default policy on ports. For information on using scripts, see [How to Use Scripts](#).

Policy groups provide the PCC network administrator with the ability to organize their network usage policies. From the PCC end user's perspective however, there are only allowed policies. As you can see in the sample PCC Web page below, only the actual allowed policies are displayed for a location.

Extreme networks There's nothing more important than our customers. [Support](#) | [About](#)

[Policy-Management](#) | [Administration](#) | [Change-Password](#) | [Scheduling](#) | [Logout](#)

[Help](#)

To modify your classroom's network access, please select the level of access you wish for your students to have from the settings below.

Change Location ▾

Select the Desired Policy

Status	Policy
<input checked="" type="radio"/>	Allow All Access Allow access to local network and internet.
<input type="radio"/>	Deny All Access Deny access to local network and internet.
<input type="radio"/>	Limited Access Allow local network access only.
<input type="radio"/>	No Instant Messaging No access to messaging services.
<input type="radio"/>	No Web Deny internet access.

Revert to default policy in minutes

V Hide Advanced Policy Assignment

Select the Desired Policy for any Port in this Location


Port	Policy
[17.57.77.127] Port ge.1.2	Allow All Access
[17.57.77.127] Port ge.1.3	Allow All Access

Lecture Hall 1 / Logged in as DCarell

Copyright © 2014 Extreme Networks, Inc. All rights reserved.

Enforcing

In Policy Control Console, enforcing means writing PCC configuration information from the database to the PCC appliances (embedded virtual appliance and/or external appliances.) Whenever database changes need to be enforced, the **Enforce to Appliances** button on the PCC toolbar changes to

orange , indicating that you must enforce the changes to the appliances. You should also enforce any time you make changes to your device credentials

(via Console). Device credentials are stored on the appliance; if the credentials are changed, you must enforce the new credentials to the appliance so it can communicate with the ports on the device. To enforce, use the toolbar button or the Tools > Enforce to Appliances menu option.

Getting Started with Policy Control Console

Getting Started provides a summary of the basic steps you must perform to begin using Policy Control Console (PCC) in your network. The PCC Getting Started steps assume that you have already:

- Used Policy Manager to create and enforce appropriate policy roles to your network devices.
- Installed and configured the PCC appliance and web server, if you are using an external hardware PCC appliance. For more information, see your SNS-PCC-WBA Installation Guide.

It is recommended that you review the information in the [Concepts](#) Help topic before you begin these steps, to get an overview of the basic features in PCC.

Setting Up PCC

The steps are listed in the order in which they should be performed. Click on each step to open a help topic with detailed instructions.

- [Plan your Locations, User Groups, and Policy Groups](#)
- [Create the Locations Tree](#)
- [Create Your Policy Groups](#)
- [Create Your User Groups](#)
- [Configure Your Locations](#)
- [Check for Consistency](#)
- [Accessing the PCC Web Page](#)

Explore PCC Features

Now that you have set up your locations, user groups, and policy groups, you can start exploring some of PCC's features:

- [Activity Report](#) The Activity Report window lets you view policy change activity for the PCC users and locations in your network. It displays event messages received from the PCC appliance for a single location or user during a specified period of time.
 - [Appliance Events](#) The Appliance Events window displays all event messages received from the PCC appliance (embedded virtual appliance and/or external appliance) during a specified period of time. You can access the window from the Tools menu (Tools > Appliance Events).
 - [Current Default Policies](#) The Current Default Policies window lets you view the policies currently active for each port assigned to a location. To access this window, right click on a location in the Locations tree and select View Current Default Policies.
 - [Find Assigned Ports](#) The Assigned Ports window lets you view and search all the ports that are currently assigned to locations. You can access the window from the Tools menu (Tools > Assigned Ports).
-

-Getting Started-

Plan your Locations, User Groups, and Policy Groups

Before you begin configuring Policy Control Console, be sure to read the [PCC Concepts](#) help topic to get a basic understanding of how PCC works. Now, use the steps in this help topic to do some initial planning of your:

- Locations hierarchy - Outline the organization of folders and locations for your Locations tree, and identify the ports that will be assigned to each location.
- Policy Groups - Determine the network usage policies you will be using and the best way to group them.
- User Groups - Identify your user groups, their properties, allowed locations and policy groups, and their assigned PCC end users.
- Location Configuration - Determine each location's allowed user groups.

Outline your Locations hierarchy:

1. On a separate sheet of paper, create a hierarchy of folders and locations to represent the campus, buildings, floors, rooms or other location-based entities. Refer to the [Concepts file](#) for an example of what a location hierarchy might look like.
2. Write down a name and description for each folder and location.
3. Identify the ports that will be assigned to each location.

Determine your Policy Groups:

1. Make a list of the policy roles you will be using in PCC.
2. Verify that the policy roles have been created in Policy Manager and enforced to the appropriate devices.
3. Group the policy roles into policy groups to facilitate assignment to user groups.
4. Write down a name and description for each policy group.

Define your User Groups:

1. Make a list of your PCC [login users](#) and write down the following information for each user:
 - The name the user will use to log in to the PCC web page.
 - The user's display name for the PCC web page.
 - [Authorization Type](#) - Admin or Basic.
 - Will PCC handle user authentication? If so, what is the user's password?
 - What locations should the user have access to?
 - What policy groups should the user have access to?
2. Make a list of your PCC [static IP users](#) and write down the following information for each user:
 - The system's IP address.
 - The system's display name for the PCC web page.
 - What location should the system have access to?
 - What policy groups should the system have access to?
3. Group the users into user groups to facilitate assignment to locations.
 - Write down a name and description for each user group.
 - Determine the users that will be in this group.
 - Determine the locations where the users in this group will be allowed to set policy.
 - Determine the policy groups that the users in this group will be allowed to set.

Configure Locations:

1. For each location, identify the user groups that should be assigned to the location with the ability to set default policy.

Return to [Getting Started](#) for your next step.

Related Information

For information on related windows:

- [PCC Concepts](#)
- [Manage Users Window](#)


- [Manage Policy Groups Window](#)

-Getting Started-


Create the Locations Tree

The [Locations tree](#) is displayed in the left-panel of the Policy Control Console main window. When you did your [Location hierarchy planning](#) in the Getting Started step 1, you outlined the organization of folders and locations for your Locations tree. Use the following steps to create a Locations tree hierarchy according to those plans.

To create your folders:

1. Right-click the Locations folder and select **New Folder** from the menu. The New Folder window opens.
2. Enter a name and description for the folder. Click OK or Apply to add the folder to the tree.
3. Repeat these steps to create a hierarchy of folders for your tree.
4. Enforce to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

To create your locations:

1. Right-click the folder that will contain the location and select **New Location** from the menu. The New Location window opens.
2. Enter a name and description for the location. Click OK or Apply to add the location to the tree.
3. Create all the necessary locations for your tree.
4. Enforce to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.
5. Return to [Getting Started](#) for your next step.

Related Information


For information on related windows:


- [PCC Main Window](#)
- [Properties Tab](#)

-Getting Started- Create Your Policy Groups

Policy groups are predefined sets of network usage policies that PCC users select from when setting network access for locations. The actual policy roles themselves must be created and enforced to your network devices using NetSight Policy Manager. When you did your [Policy Group planning](#) in the Getting Started step 1, you defined your PCC policy groups. Use the following steps to create and define your policy groups according to those plans.

NOTE: Usage policies can be either actual policy roles that have been created and enforced to your network devices using NetSight Policy Manager or they can be scripts that are written to set default policy on ports. This depends on whether your network access layer is composed of policy-enabled switches (use policy roles) or non policy-enabled switches (use scripts). The steps here describe how to set up your policy groups using policy roles for policy-enabled switches. For information on using scripts, see [How to Use Scripts](#).

1. Click the **Manage Policies** button  on the PCC toolbar. The [Manage Policy Groups window](#) opens.
2. Select the All Policy Groups folder in the left panel. Click the Add Policy Group button. The Add Policy Group window opens.
3. Enter a name and description for the group. Click OK.
4. Select the group in the tree and then select the Policies tab in the right panel.
5. Click Add Policies. The Add Policies window opens.
6. Select one or more devices or device groups in the tree and click Retrieve Policy Information.
7. Select the policies you wish to add to the policy group. Click OK.
8. Back in the Manage Policy Groups window click Apply.
9. Select a policy in the tree. In the right-panel Policy Properties tab, enter a description for the policy. The description is what will be displayed on the PCC web page for PCC end user selection. Click Apply.
10. Repeat these steps to create all your policy groups and add descriptions for your policies.

11. Enforce to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

12. Return to [Getting Started](#) for your next step.

Related Information


For information on related windows:

- [Manage Policy Groups Window](#)

-Getting Started-

Create Your User Groups

PCC users are the authorized users who access the PCC web page to regulate network access for specified locations in the network. End users are grouped into user groups to simplify the assignment of allowed policy groups and locations. When you did your [User Group planning](#) in the Getting Started step 1, you defined your PCC user properties and your user groups. Use the following steps to create your PCC users and user groups according to those plans.

1. Click the **Manage Users** button  in the PCC toolbar. The [Manage Users window](#) opens.
2. Select the All Users folder in the left panel tree. Click the Add Users button. The [Add User window](#) opens.
3. Select the user type:
 - Login User - Login users are PCC users that will log in to the PCC web page. As part of a user group, each login user will be assigned certain locations and policy groups that they are allowed to configure. When the user logs in to the PCC web page, they will only have access to those assigned locations and policies.
 - Static IP User - Static IP Users are created for specific locations such as lecture halls or conference rooms where there would be a dedicated computer that anyone could use to access a PCC web page and set policies for that location.

The window's fields will change according to the selected user types. Proceed to either [Define Login User](#) or [Define Static IP User](#) depending on your selection.

Define Login User:

1. Enter the User Name, which is the name the user will use to log in to the PCC web page.
2. Enter the Display Name, which is the user's name that will be displayed on the PCC web page after they log in.

3. Use the drop-down list to select the user's authorization type:
 - Admin - Provides access to the PCC web page to:
 - define and schedule policy for allowed locations.
 - configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
 - view a PCC activity log.
 - Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - schedule policy for allowed locations if the Allow Scheduling option is selected.
4. Select the "Allow Scheduling" checkbox to grant the user access to the scheduling functionality on the PCC web page. This enables the user to schedule policy changes for their allowed locations.
5. Select the "Create User Group" checkbox if you would like a user group to be automatically created based on the user name, with the user as a member of the group. This feature is most commonly used for Static IP users.
6. Select the "Use PCC Login" checkbox if PCC is handling user authentication to the PCC web page. Enter and confirm the password. If PCC Login is not selected, LDAP must be configured.

NOTE: Spaces are not allowed in passwords and will be ignored.
7. Click OK.
8. Return to [step 2](#) at the beginning of the help topic and repeat the steps to define all your PCC users. When you have defined all your users, proceed to [Define User Groups](#).

Define Static IP User:

1. Enter the IP address of the dedicated system that will be the user.
2. Enter the Display Name, which is the system's name that will be displayed on the PCC web page.
3. The system's authorization type is set to Basic, providing access to the PCC web page to define policy for allowed locations and to schedule policy for allowed locations, if the Allow Scheduling option is selected.

4. Select the "Allow Scheduling" checkbox to grant the user access to the scheduling functionality on the PCC web page. This enables the user to schedule policy changes for their allowed locations.
5. Select the "Create User Group" checkbox if you would like a user group to be automatically created based on the user name, with the user as a member of the group.
6. Click OK.
7. Return to [step 2](#) at the beginning of the help topic and repeat all the steps to define all your PCC users. When you have defined all your users, proceed to Define User Groups.

Define User Groups:

1. Select the All User Groups folder in the left panel tree. Click the Add User Groups button. The Add User Group window opens.
2. Enter a name and description for the user group. Click OK.
3. Select the user group in the left panel and select the Allowed Locations tab in the right panel.
4. Click the Add Locations button. The Add Locations window opens.
5. Expand the Locations tree and select the folder(s) or single location(s) where the users in this user group will be allowed to assign policies. Click OK.
6. The locations will be added to the Allowed Locations tab.
7. Select the Allowed Policy Groups tab in the right panel.
8. Click the Add Policy Groups button. The [Assign Policy Groups window](#) opens.
9. Select the appropriate policy group(s) that include the policies the users in the group will be allowed to assign to a location. Click OK.
10. The policy groups will be added to the Allowed Policy Groups tab.
11. Select the Assigned Users tab in the right panel.
12. Click the Assign User button. The [Assign Users window](#) opens.
13. Select one or more users to assign to the user group. Click OK.
14. Return to [step 1](#) at the beginning of this section and repeat the steps to define all your user groups. Click OK.

15. Enforce to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

Return to [Getting Started](#) for your next step.

Related Information


For information on related windows:

- [Manage Policy Groups Window](#)
- [Manage Users Window](#)

-Getting Started- Configure Locations


For each location you must define the allowed user groups and add the ports that will be included in that location.

Assign User Groups to a Location:

1. Select a location in the left-panel Locations tree.
2. Click on the right-panel [User Groups tab](#).
3. The tab lists all the user groups that were configured with this location as an allowed location. You can expand each group to see the users in that group. To add another user group, click **Assign**. The [Assign User Groups window](#) opens.
4. Select the user groups that you want to add. Click **OK**.
5. The user groups are added to the User Groups tab. Click **Save** at the bottom of the tab.
6. Enforce to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

Add Ports to a Location:

1. Select a location in the left-panel Locations tree.
2. Click on the right-panel [Ports tab](#).
3. Click **Add**. The [Add Ports window](#) opens.
4. The left panel displays a device tree of your network devices. Expand the device tree and select a device from which to retrieve ports.
5. When you select a device in the tree, its ports are displayed in the right-panel Available Ports table. Because only access ports should be added to a location, only access ports are displayed in the table. All CDP, backplane, and logical ports are filtered out. Select the ports you want to add to a location, and click **Add**.
6. The right-panel Ports to Add table displays the ports you have selected to add to a location. Click **OK** to add the ports to the location.
7. The ports are listed in the Ports tab. Click **Save** at the bottom of the tab.

8. Enforce to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

Return to [Getting Started](#) for your next step.

Related Information

For information on related windows:

- [User Groups Tab](#)
- [Ports Tab](#)
- [Assign Users Window](#)
- [Assign Policy Groups Window](#)
- [Add Ports Window](#)


-Getting Started- Check Consistency

Now that you have created your user groups and policy groups, and configured your locations, use the Check Consistency feature to verify your PCC configuration and ensure that your policies will be correctly applied to your locations.

Check Consistency checks the following three things for each location:

- Have all the policies assigned to the location (as part of a user group) been enforced (via Policy Manager) to the associated devices? A policy must be enforced to a device via Policy Manager before it can be set as the default policy for a location via PCC.
- Have all the default policies currently configured on the ports in the location been assigned to the location (via PCC)? A policy must be assigned to a location (as part of a user group) before it can be set as a default policy via PCC.
- Is a default policy configured for all the ports in the location? Do all the ports in the location have the same default policy currently configured? In most instances, all the ports in a location should have the same configured default policy.

When inconsistencies or problems are found, the information is displayed so you can easily see what needs to be fixed or changed. Use the following steps to run the Check Consistency feature and verify your PCC configuration.

1. Select the Locations folder in the left-panel Locations tree. Right-click and select **Check Consistency** from the menu. The Check Consistency window opens.
2. The left panel displays the Locations tree. If there are no problems, the right panel displays the default policies currently configured on the ports in the selected folder or location. However, if a folder or location has inconsistencies that would prevent a default policy from being applied, the location and all the folders in its path are displayed with a red X icon . Select a folder or location in the tree and use the right-panel tabs to see the problems. For more information on each tab:
 - [Allowed Policies not created on Devices Tab](#)
 - [Default Policies not allowed in Location Tab](#)

- [Default Policies that differ Tab](#)

Return to [Getting Started](#) for your next step.

Related Information

For information on related windows:

- [Check Consistency Window](#)

-Getting Started-

Accessing the PCC Web Page

PCC end users use the PCC web page to set the network access for their allowed locations. The web page is accessed using the PCC appliance's IP address or hostname, assuming that the hostname is known on the network. The PCC appliance is provided by default as an embedded virtual appliance on the NetSight Server. Optionally, you may be running PCC as an external hardware appliance (SNS-PCC-WBA). For the embedded appliance, the IP address and host name are the same as the device where the NetSight Server is running. For the external appliance, the PCC Administrator configured the appliance's IP address and hostname when the appliance was installed. (For more information, see the PCC appliance hardware installation guide.)

1. Open a browser window and enter the PCC web page URL in either of the following formats:

`http://<address>:8080/pcc`

or

`https://<address>:8443/pcc`

where <address> is the PCC appliance's IP address or hostname, and 8080 or 8443 is the required port number. For example,

`https://10.20.30.40:8443/pcc`

2. Enter your user name and password in the Policy Control Login Page.
3. The PCC web page opens. At the top of the web page, users can access links to Policy-Management, Administration, Change-Password, and Scheduling functions. PCC end users configured with Admin authorization will be able to access all pages. PCC end users configured with Basic authorization will only be able to access the Policy-Management page and Scheduling page (if the Allow Scheduling checkbox is selected with the user is added). The Change Password page is only available to PCC login users. For more information, refer to [How to Use the PCC Web Page](#).

Return to [Getting Started](#) for information on other PCC functions.

Related Information

For information on related windows:

- [How to Use the PCC Web Page](#)

How To Use Policy Control Console

The **How To** help section contains help topics that give you instructions for performing tasks in Policy Control Console.

How to Change Messaging Credentials on the PCC Engine

If the Extreme Management Center messaging credentials are changed, configure your PCC engines to use the new credentials. Use the following steps to change the messaging credentials on your PCC engines.

1. Obtain the current messaging credentials from the Client Connections options view in the suite-wide options (Tools > Options). Check "Show Credentials" to display the current password.
2. On the PCC engine, stop the PCC server using the command: `pccctl stop`
3. Edit the file `/opt/pcc/serverconfig.xml`.

- a. Within the object element, add a void element for the `jmsUserPassword` property as follows:

```
<void property="jmsUserPassword">  
<string>abc123</string>  
</void>
```

Use the contents of the string element for the new password. In the example above, the password is "abc123".

If there is already a void element for the `jmsUserPassword` property, update the string element for the new password.

- b. Save your changes to the file.
4. Start the PCC server using the command: `pccctl start`
5. Repeat steps 2 through 4 on each PCC engine.

Here is an example of a `serverconfig.xml` file with the messaging password configured:

```
<?xml version="1.0" encoding="UTF-8"?>  
<java version="1.6.0_21" class="java.beans.XMLDecoder">  
<object  
class="com.enterasys.netsight.pcc.web.util.PccProperties">  
  <void property="jmsUserPassword">  
    <string>J;]p]VP^lB]GZH1S@-x[DbMQ[p~Yl+6u</string>  
  </void>  
  <void property="netsightServerAddress">
```

```
<string>10.20.30.40</string>  
  </void>  
</object>  
</java>
```

How to Configure the PCC Web Server

The PCC appliance is provided by default as an embedded virtual appliance on the NetSight Server. The appliance software includes a PCC web server. The web server provides the web interface where authorized users select from a predefined set of network usage policies to regulate network access. This Help topic provides information on how to set up or change certain PCC web server configuration settings.

NOTE: These instructions are for the embedded PCC appliance only. If you are running PCC as an external hardware appliance (SNS-PCC-WBA) refer to the PCC appliance hardware installation guide for information on configuring the web server.

Information on:

- [LDAP Authentication Configuration](#)
- [Modify Port Values](#)
- [Change the Default Login](#)
- [Customize the PCC Web Page](#)

LDAP Authentication Configuration

PCC leverages the LDAP authentication configured on the NetSight server as a way to authenticate PCC users using an LDAP server. When a user logs into the PCC web application, their user information is sent to the NetSight server for LDAP authentication. When the user is authenticated, they are assigned a NetSight authorization group. If the authorization group is mapped to a PCC user group, the user is created as a dynamic user and allowed access to the PCC web application. These dynamic users are not stored in the database and only exist as long as their session exists. You can see dynamic users that are created in the event log.

All dynamic users are assigned the Basic authorization type unless they are a member of the NetSight Administrator authorization group, in which case they will be given the Admin authorization type.

Use the following steps to configure the PCC web server to use the NetSight server for LDAP authentication.

1. Make sure that LDAP authentication has been configured as the Authentication Method for NetSight authorization/device access.
2. On the NetSight server, open the following file:
`<install directory>/NetSight/jboss/server/default/conf/login-config.xml`
3. Locate the PCC LDAP Login Module. Uncomment the section and place it under the "JAASLogin2" application-policy section. The order of the login modules in this file controls the order in which each module is executed. If you want LDAP authentication to run first, place it at the top of the application-policy section.
`<login-module
code="com.enterasys.netsight.pcc.web.auth.loginmod.PccLDAPLoginModule"
flag="sufficient">
</login-module>`
4. Map your NetSight authorization groups to the appropriate PCC user group by selecting a user group in the [Manage Users window](#) and using the Mapped Authorization Groups tab. Be sure to enforce your changes to your PCC appliances.

Modify Port Values

To change the HTTP port value:

1. On the NetSight server, open the following file:
`<install directory>/NetSight/appdata/NSJBoss.properties`
2. Locate the following line and change the port value to the desired port.
`enterasys.tomcat.http.port=8080`

To change the HTTPS port value:

1. On the NetSight server, open the following file:
`<install directory>/NetSight/jboss/server/default/deploy/jbossweb-tomcat55.sar/server.xml`
2. Locate the following sections and change the number "8443" to the desired port.

```
<Connector port="{enterasys.tomcat.http.port}"  
address="{jboss.bind.address}"  
maxThreads="250" strategy="ms" maxHttpHeaderSize="8192"  
emptySessionPath="true"
```



```
enableLookups="false" redirectPort="8443"
acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>

<Connector port="8443" address="{jboss.bind.address}"
minSpareThreads="5" maxSpareThreads="15" scheme="https"
secure="true" clientAuth="false"
securityDomain="java:/jaas/nsSSL"
SSLImplementation="org.jboss.net.ssl.JBossImplementation"
/>
```

Change the Default Login

The web server is configured with a default login that can be used to login to the PCC web page. The default login username/password is admin/admin. This provides a "backdoor login" for administrators in the event the NetSight server goes down and the appliance is unable to authenticate PCC end users attempting to login to the PCC web page. To change the default login:

1. On the NetSight server, open the following file:
`<install directory>NetSight/jboss/bin/pcc-user.txt`
2. Locate the following string:
`admin:21232f297a57a5a743894a0e4a801fc3:admin`

which uses the format:

`username:hashed_password:role` where role specifies the user's authorization type of admin or basic.

3. Replace the hashed password entry with an MD5 hashed password. To generate a hashed password, type **md5sum** at the server CLI and press **Enter**. Type the password to be hashed and press **Ctrl D** twice. The hashed password will be displayed right next to the password you entered, followed by a dash. Disregard the dash and use just the hashed password value for your new password. (The **md5sum** command is not available by default on Windows. Windows users will need to install an equivalent program.)

NOTE: The `pcc-user.txt` filename is configurable in the `login-config.xml` file.

Customize the PCC Web Page

You can customize the PCC web page by changing the default header (the Extreme Networks banner), the default footer (the Extreme Networks copyright statement), and the Policy-Management table.

Customizing the PCC Web Page Header

The default PCC web page header is the Extreme Networks logo, along with links to the Extreme Networks Support page and About page.

To use a different logo, edit the header.jsp file. If you are running the embedded PCC server, this file is located in the following directory:

`<install directory>/NetSight/jboss/server/default/deploy/NetSight/pcc.war/header.jsp`. If you are running the external PCC appliance, the file is located in the `opt/pcc/webapps/pcc` directory.

Open the file using a text editor such as WordPad. In the file you will see some lines that have been commented out using the `<!--` and `-->` symbols. These lines can be used to display an alternate Policy Control Console logo (`pcc-banner.gif`). To use them, uncomment these lines by removing the `<!--` and `-->` symbols. Then comment out (using the `<!--` and `-->` symbols) or delete the lines at the top of the file that are used to display the Extreme Networks logo. The `pcc-banner.gif` file name can be replaced with any `.gif` file desired. Put the new `.gif` file in the images directory:

`<install directory>/NetSight/jboss/server/default/deploy/NetSight/pcc.war/images`

```
<!-- *** To use another gif file for the header, comment out
the text above and uncomment
*** the lines below. The pcc-banner.gif file can be
replaced with the image of your choice.
-->
```

```
<!--
<t:panelGrid columns="1" border="0" cellpadding="0"
cellspacing="0">
<t:panelGroup >
<t:graphicImage url="../../../Resources/Images/pcchelp/pcc-
banner.gif" border="0"/>
</t:panelGroup>
</t:panelGrid>
-->
```

Customizing the PCC Web Page Footer

The default PCC web page footer is the Extreme Networks copyright statement.

To change the footer, edit the footer.jsp file. If you are running the embedded PCC server, this file is located in the following directory:

```
<install directory>/NetSight/jboss/server/default/deploy/NetSight/pcc.war/footer.jsp.
```

If you are running the external PCC appliance, the file is located in the opt/pcc/webapps/pcc directory.

Open the file using a text editor such as WordPad. Comment out or delete the existing code in the file and add the desired image or text. To replace text that is displayed in the footer image, the default footer.jsp code can be edited. To do this, replace the quoted text highlighted in red.

```
<t:div id="footer" forceId="true">
<t:div id="copyright" forceId="true">
<h:outputText value="#{bundle['header.copyright']} #{bundle
['header.companyname']}
#{bundle['header.rightsreserved']}"/>
</t:div>
</t:div>
```

Customizing the Policy-Management Table

The PCC Policy-Management web page displays each policy as two table rows under the policy title. The first row shows the policy name and the second row shows the policy description.

You can change the row data displayed under the Policy title by editing the policycontrol.jsp file. If you are running the embedded PCC server, this file is located in the following directory:

```
<install directory>/NetSight/jboss/server/default/deploy/NetSight/pcc.war/user/policycontrol.jsp.
```

If you are running the external PCC appliance, the file is located in the opt/pcc/webapps/user directory.

The policycontrol.jsp file has the following comment that describes how to change the row data. The number of rows displayed can be controlled by the number of "outputText" lines. The content of the row can be changed by editing the value of the "outputText" line (shown in red in the following example). The

possible values are: row.policy.name, row.policy.description, or row.policy.webDisplayString. The webDisplayString displays the policy description unless a description has not been entered in which case it will display the policy name.

```
<!-- The following lines determine what is displayed in the
policy table.
```

```
    The possible choices are row.policy.name,
row.policy.description, or
    row.policy.webDisplayString. The webDisplayString will
select
    the policy description if it exists. If it is empty, it
will display the policy name.
-->
```

```
<h:outputText styleClass="licAppTitle" value="#
{row.policy.name}"/>
<h:outputText styleClass="licAppDescription" value="#
{row.policy.description}"/>
```

For example, to display the policy webDisplayString to show the policy description or the policy name, the following code would be used:

```
<h:outputText styleClass="licAppTitle" value="#
{row.policy.webDisplayString}"/>
```

Related Information

For information on related windows:

- [Accessing the PCC Web Page](#)
- [How to Use the PCC Web Page](#)

How to Initialize PCC Database Components

Policy Control Console provides a way for you to initialize only the PCC components in the NetSight Database. The initialize operation removes **all** PCC data elements from the database including configured PCC users, policy groups, and locations.

Using this operation instead of the Restore Initial Database function (accessed in the Server Information window) allows you to initialize your PCC components while retaining your NetSight Console and other NetSight application data elements in the database.

NOTE: As a precaution, it is recommended that you make a backup of your NetSight Database prior to performing the initialize operation using the Backup Database window accessed from the Server Information window.

1. Make a backup of your database using the Backup Database window accessed from Database tab in the Server Information window (in the Console main window, select **Tools > Server Information**).
 2. In the PCC main window, select **File > Database > Initialize PCC Components** to begin the initialize operation. You will see a message asking if you want to delete all Policy Control Console data in the server's database. Click **OK**.
-

How to Set PCC Options

The Policy Control Console options let you define the SNMP polling parameters and authorization group for PCC. Use the Console Options window (**Tools > Options** in the Console menu bar) to set PCC options.

1. Select **Tools > Options** in the Console menu bar. The Options window opens.
2. In the left-panel tree, expand the Console folder and select Policy Control Console. The right-panel Policy Control Console view is displayed.
3. In the SNMP section, specify SNMP polling parameters for PCC.
 - a. Set the **Number of SNMP Retries**. This is the number of attempts that will be made to contact a device when an attempt at contact fails. The default setting is 3 retries, which means that PCC retries a timed-out request three times, making a total of four attempts to contact a device.
 - b. In the **Length of SNMP Timeout** field, enter the amount of time (in seconds) that PCC waits before re-trying to contact a device.
4. In the Appliance Authorization section, use the drop-down list to select the Authorization Group with the correct profile for the PCC appliance (embedded virtual appliance and/or external appliances) to use when communicating with devices. Profiles define the level of device access granted to users that are members of that Authorization Group. Profiles and Authorization Groups are defined in the Authorization/Device Access window (**Tools > Authorization/Device Access** in the Console menu bar).
5. Click **OK** to set options and close the window. Click **Apply** to set options and leave the window open.

How to Use Scripts

Policy Control Console supports the use of scripts as a way to set policy on ports in networks where access devices are **not** policy-enabled. Scripts are stored on the NetSight Server and are associated to policies and policy groups just like policy roles. When a PCC end user sets a default policy that is associated to a script, the PCC appliance runs the script for the ports that have been configured for that location.

NOTE: The ability to use scripts is not supported on NetSight Servers installed on a Windows platform system, unless you are using the external PCC appliance.

Information on:

- [Writing and Storing Scripts](#)
- [Adding Scripts to Policy Groups](#)
- [Assigning Scripts to Locations](#)

Writing and Storing Scripts

PCC includes a demo script called `demo_script.pl`. The script is written in Perl, although scripts can be written in any language. You can view the demo script in the following directory on the NetSight Server:

`<install directory>\NetSight\appdata\PolicyControlConsole\scripts`. You can use this demo script as an example to create your own scripts.

Each script is passed the following command line arguments:

- *command* - tells the script whether it is being called to get the current policy state (GETSTATE) or set the policy state (SETSTATE).
- *policy* - the name of the policy with which the script is associated.
- *location* - the location where the PCC end user is setting the policy.

The script can return two values as standard output:

- TRUE - In the case of SETSTATE, this means the set operation completed successfully. In the case of GETSTATE, it indicates that the *policy* is currently in force in the *location*.

- FALSE - In the case of SETSTATE, this means the set operation failed. In the case of GETSTATE, it indicates that the *policy* is not in force in the *location*.

The demo script uses a log file to track the progress of the script. It also uses a temporary file to track which policy was last in force at a given location. When a script writes to STDERR, the web server interprets it as a failure.



Once you have created your scripts, you must store them on the NetSight server in the <install directory>\NetSight\appdata\PolicyControlConsole\scripts directory. They will then be available for selection in the Manage Policy Groups window where you will add the scripts to your policy groups.

Adding Scripts to Policy Groups

After you have written your scripts and stored them in the scripts directory, you can add the scripts to your policy groups, just as you would add a policy role. When you add a script to a policy group, you associate the script to a policy name that will be used as the *policy* command argument.

The same script can be used multiple times in a policy group, however each use must have a unique policy name. Policy groups can contain policy roles or policy scripts, but not a combination of the two. Once a script is added to a policy group, the PCC appliance assumes that all policies in the group are scripts.

Use the following steps to add a script to a policy group.

1. Click the **Manage Policies** button  on the PCC toolbar. The [Manage Policy Groups window](#) opens.
2. Select the desired policy group in the tree and then select the Policies tab in the right panel.
3. Click **Add Script**. The Associate a Script as a Policy window opens where you can create the policy that you want to associate with the script.
4. Enter a name and description for the policy. The policy name will be used as the *policy* command argument in the script, and the description is what is displayed on the PCC web page for PCC end user selection.
5. Select the script from the list of available scripts. This list includes all the scripts stored on the NetSight server in the scripts directory. Click **OK**.
6. Back in the Manage Policy Groups window click **OK**.
7. Enforce to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

Assigning Scripts to Locations

Once you have added scripts to a policy group, the policy group can be assigned to a user group and a location using the [Manage Users window](#). For each location that requires the use of scripts to set policy, you must select the "Use Scripts at this location" checkbox on the location's [Properties tab](#). In addition, you can use the location's Properties tab to enter custom arguments that will be appended to a script command line each time it is invoked for that location.

Related Information

For information on related windows:

- [Manage Policy Groups Window](#)
- [Manage Users Window](#)

How to Use the PCC Web Page

PCC end users use the PCC web page to set the network access for their allowed locations. The web page is accessed using the PCC appliance's IP address or hostname, assuming that the hostname is known on the network. The PCC appliance is provided by default as an embedded virtual appliance on the NetSight Server. Optionally, you may be running PCC as an external hardware appliance (SNS-PCC-WBA). For the embedded appliance, the IP address and host name are the same as the device where the NetSight Server is running. For the external appliance, the PCC Administrator configured the appliance's IP address and hostname when the appliance was installed. (For more information, see the PCC appliance hardware installation guide.)

The PCC web page URL uses either of the following formats:

`http://<address>:8080/pcc`

or

`https://<address>:8443/pcc`

where <address> is the PCC appliance's IP address or hostname, and 8080 or 8443 is the required port number. For example,

`https://10.20.30.40:8443/pcc`

This Help topic provides information on how PCC end users will use the PCC web page. At the top of the web page, users can access links to Policy-Management, Administration, Change-Password, and Scheduling functions. PCC end users configured with Admin authorization will be able to access all pages; users configured with Basic authorization can access all pages except the Administration page. The Change Password page is only available to PCC login users.

Information on:

- [Policy Management](#)
- [Administration](#)
- [Change Password](#)
- [Scheduling](#)

Policy Management

The Policy-Management web page allows PCC end users to set policy for their allowed locations. It shows the current location and policy selections, and allows users to select a new location and policy. It also lets them set a schedule to revert to the location's default policy (if a default policy has been defined for the location) and set policy on a port-by-port basis if

Advanced Policy Control has been configured for the selected location. As soon as policy changes are made on this web page, the policy changes will be made for the location.

The screenshot shows the Extreme Networks PCC web interface. At the top left is the Extreme Networks logo with the tagline "There's nothing more important than our customers." and links for "Support" and "About". A navigation bar contains "Policy-Management", "Administration", "Change-Password", "Scheduling", and "Logout". Below this is a "Help" link. A message states: "To modify your classroom's network access, please select the level of access you wish for your students to have from the settings below." The main section is titled "Change Location" with a dropdown arrow. Underneath, "Select the Desired Policy" is followed by a table of policy options:

Status	Policy
<input checked="" type="radio"/>	Allow All Access Allow access to local network and internet.
<input type="radio"/>	Deny All Access Deny access to local network and internet.
<input type="radio"/>	Limited Access Allow local network access only.
<input type="radio"/>	No Instant Messaging No access to messaging services.
<input type="radio"/>	No Web Deny internet access.

Below the table is a checkbox "Revert to default policy in 60 minutes". A section titled "Hide Advanced Policy Assignment" contains "Select the Desired Policy for any Port in this Location" and a table:

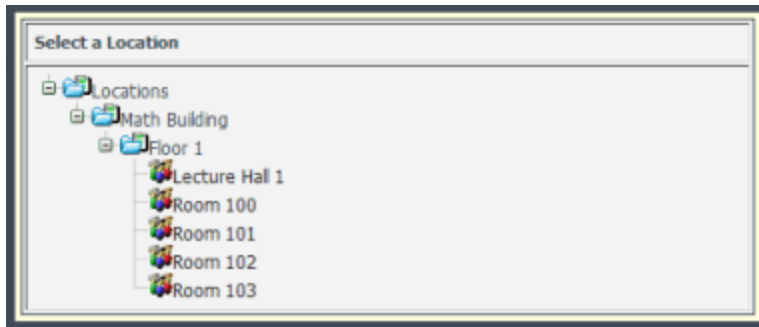
Port	Policy
[17.57.77.127] Port ge.1.2	Allow All Access
[17.57.77.127] Port ge.1.3	Allow All Access

At the bottom of this section are "Submit" and "Cancel" buttons. The footer shows "Lecture Hall 1 / Logged in as DCarell" and "Copyright © 2014 Extreme Networks, Inc. All rights reserved."

Change Location

Clicking on the Change Location drop-down arrow displays the Locations Tree where the end user can select a different location. Only the user's allowed locations are displayed in the tree. If the user has only one allowed location, the Change Location link is not shown at all.

Sample Location Tree.



Select the Desired Policy

This section lists the allowed policies for the selected location and lets the end user specify the desired policy using the radio buttons.

Revert to default policy in minutes

When the "Revert to default policy" checkbox is selected, the location's policy will revert to its default policy in the specified number of minutes. This checkbox only appears if a default policy has been configured for the location in the location's [Properties tab](#).

NOTE: You must select the checkbox and enter a time interval **before** setting a policy for the location. A scheduled revert is lost when a new policy is set. In addition, all reverts are lost if the PCC appliance is restarted.

Advanced Policy Assignment

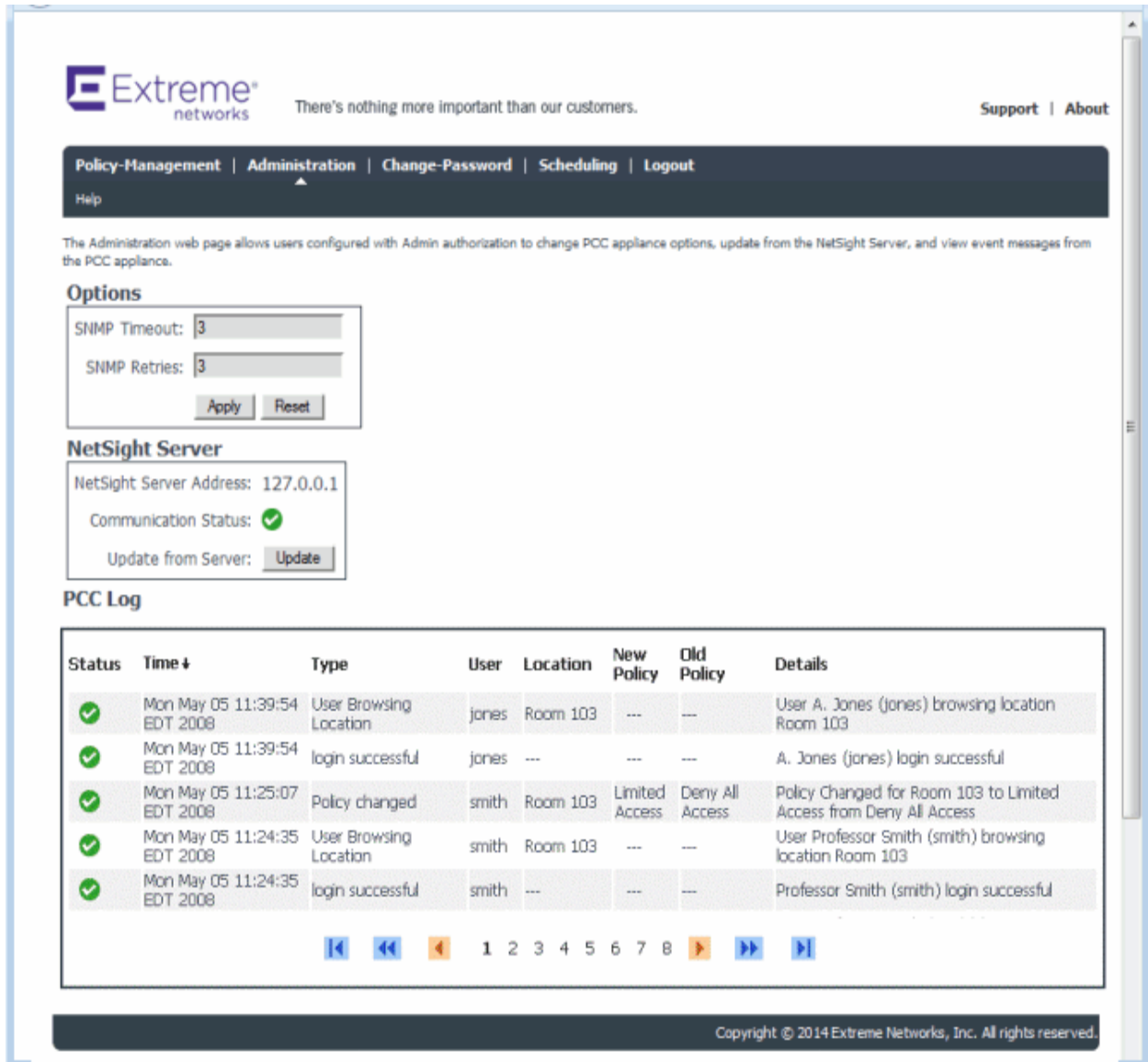
This section allows the end user to set policy for the location on a port-by-port basis. It is only displayed if the Advanced Policy Control option has been configured for the location in the location's [Properties tab](#). The policy drop-down lists can be used to assign a policy for each port. The end user must click **Submit** to change the policy. The advanced policy assignment for a port will override the policy set for the location.

Location/Display Name

The currently selected location and the name of the current PCC end user.

Administration

The Administration web page allows users configured with Admin authorization to change PCC appliance options, update from the NetSight server, and view event messages from the PCC appliance.



Options

These options define how the PCC appliance communicates with network devices when reading current settings and applying policy, and let you change the IP address of the NetSight server, if you are running PCC as an external hardware appliance.

SNMP Timeout

The amount of time (in seconds) that the PCC appliance waits before re-trying to contact a device.

SNMP Retries

The number of attempts that will be made to contact a device when an attempt at contact fails. The default setting is 3 retries, which means that the PCC appliance retries a timed-out request three times, making a total of four attempts to contact a device.

NetSight Server Address

This field is only displayed if you are running PCC as an external hardware appliance. You can use the field to change the IP address of the NetSight server, if desired.

Apply Button

Applies any changes made to the options.

Reset Button

Resets the options to the previously set values.



NetSight Server

This section lets you view the NetSight server communication status and update the PCC appliance with the latest configuration data from the NetSight server.

NetSight Server Address

The IP address of the NetSight server.

Communication Status

The communication status of the NetSight server:  or 

Update from Server

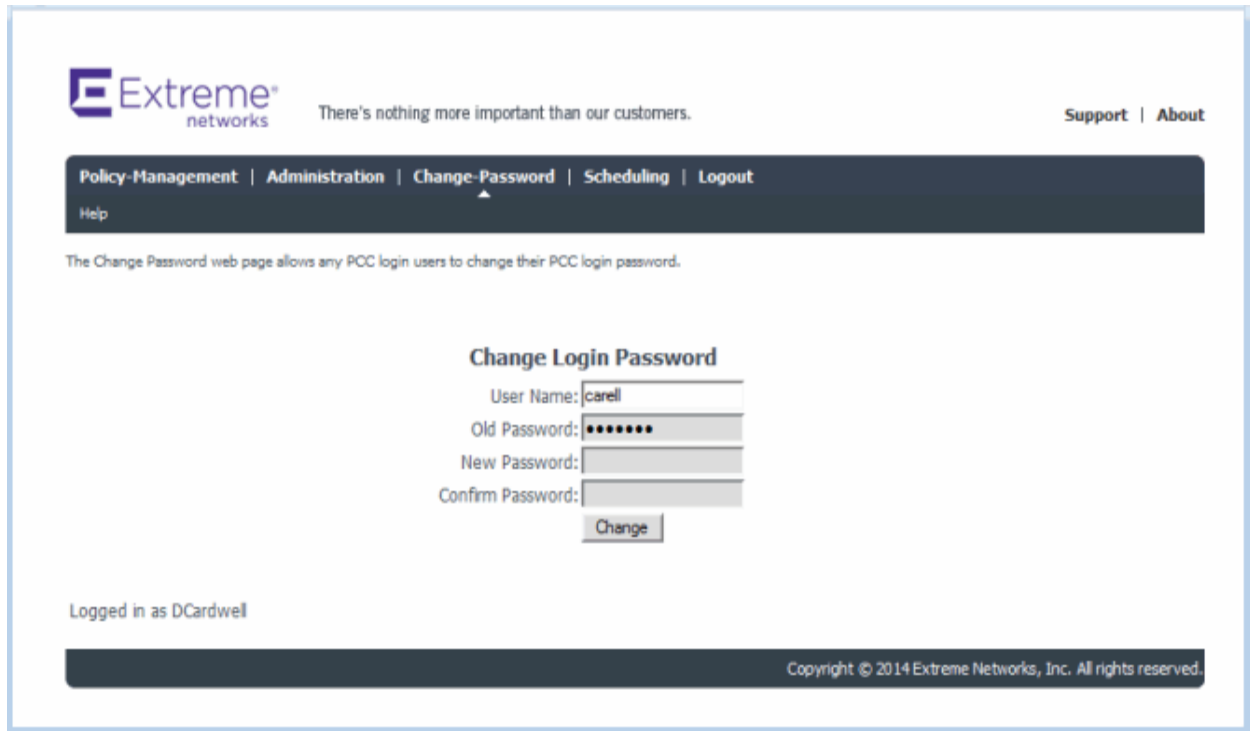
Use the Update button to update the PCC appliance with the latest configuration data from the NetSight server.

PCC Log

This section displays event messages received from the PCC appliance. It displays the same information as the [Appliance Events window](#).

Change Password

The Change Password web page allows any PCC login users to change their PCC login password.



Scheduling

The Scheduling web page allows users to schedule policy management for their allowed locations. Users must be granted access to this web page using the Allow Scheduling checkbox in the [Add User](#) or [Edit User](#) windows. The calendar can be displayed in different formats: day, week, work week, or month using the selections in the upper right corner. When selected, calendar events that have yet to take place are highlighted in blue, while calendar events that have passed are highlighted in red. Recurring events will be highlighted in green, and all associated recurring events are highlighted when one entry is selected. Holding your cursor over an entry will display a tool tip with any comments that were entered when the entry was added.

Extreme networks There's nothing more important than our customers. [Support](#) | [About](#)

[Policy-Management](#) | [Administration](#) | [Change-Password](#) | [Scheduling](#) | [Logout](#)

Help

Use the Scheduling web page to schedule policy management for your allowed locations. The calendar can be displayed in different formats: day, week, work week, or month using the selections in the upper right corner. When selected, calendar events that have yet to take place are highlighted in blue if non-recurring, green if recurring, while all calendar events that have passed are highlighted in red. Holding your cursor over an entry will display a tool tip with any comments that were entered when the entry was added. This page also lets you set a schedule to revert to the location's default policy (if a default policy has been defined for the location).

Scheduling

March. 2014

<- Add Entry... Edit Entry... Delete Entry... ->

1 7 5 31

February 24, 2014	February 25, 2014	February 26, 2014	February 27, 2014	February 28, 2014	March 01, 2014
					March 02, 2014
March 03, 2014	March 04, 2014	March 05, 2014	March 06, 2014	March 07, 2014	March 08, 2014
					March 09, 2014
March 10, 2014	March 11, 2014	March 12, 2014	March 13, 2014	March 14, 2014	March 15, 2014
					March 16, 2014
March 17, 2014	March 18, 2014	March 19, 2014	March 20, 2014	March 21, 2014	March 22, 2014
2:00 PM-5:00 PM: Calculus Lecture	2:00 PM-4:00 PM: Algebra 101 Final				March 23, 2014
					Algebra 101 Final Professor Smith Room 103
March 24, 2014	March 25, 2014	March 26, 2014	March 27, 2014	March 28, 2014	March 29, 2014
		9:00 AM-11:00 AM: Geometry 212 Final			March 30, 2014



Use this icon to select the calendar display format: day (1), week (7), work week (5), or month (31).

Add Entry

Opens the [Scheduling Details page](#) where you can add an entry to the calendar.

Edit Entry

Select a calendar entry and click Edit Entry to open the [Scheduling Details page](#) where you can edit the entry. Only the user that added the entry (or a user with Admin authorization) can edit an entry.

Delete Entry

Select a calendar entry and click Delete Entry to delete the entry. Only the user that added the entry (or a user with Admin authorization) can delete an entry.

Policy Control Console Right-Panel Tabs

When a single **folder** is selected in the left-panel tree, there are three right-panel tabs that provide detailed information for that folder.

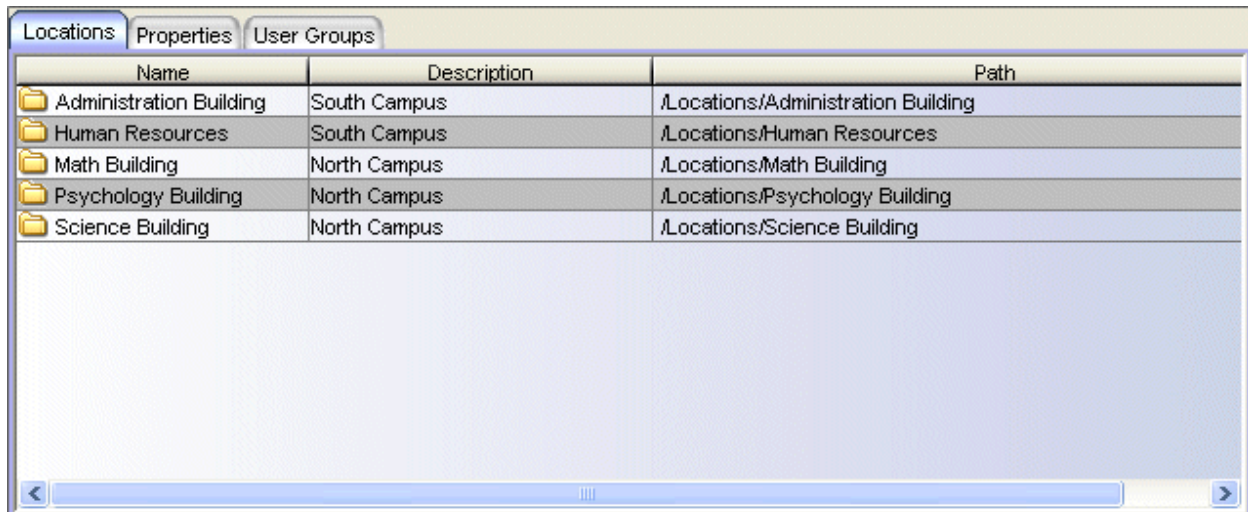
- [Locations Tab](#) - view the contents of the folder.
- [Properties Tab](#) - view and change the folder's name and description.
- [User Groups Tab](#) - add and remove user groups assigned to the folder.

When a single **location** is selected in the left-panel tree, there are three right-panel tabs that provide detailed information for that location.

- [Properties Tab](#) - view and change location properties such as name, description, and default policy.
- [User Groups Tab](#) - add and remove user groups assigned to the location.
- [Ports Tab](#) - add and remove ports assigned to the location.

Locations Tab

This tab displays the contents of the folder selected in the left-panel Locations tree. To access this tab, select a folder in the left-panel tree, then click the Locations tab in the right panel.



The screenshot shows a software interface with three tabs: 'Locations', 'Properties', and 'User Groups'. The 'Locations' tab is active and displays a table with the following data:

Name	Description	Path
Administration Building	South Campus	/Locations/Administration Building
Human Resources	South Campus	/Locations/Human Resources
Math Building	North Campus	/Locations/Math Building
Psychology Building	North Campus	/Locations/Psychology Building
Science Building	North Campus	/Locations/Science Building

Name

The locations or folders contained in the selected folder.

Description

A description of the locations or folders.

Path

The path to the locations or folders.

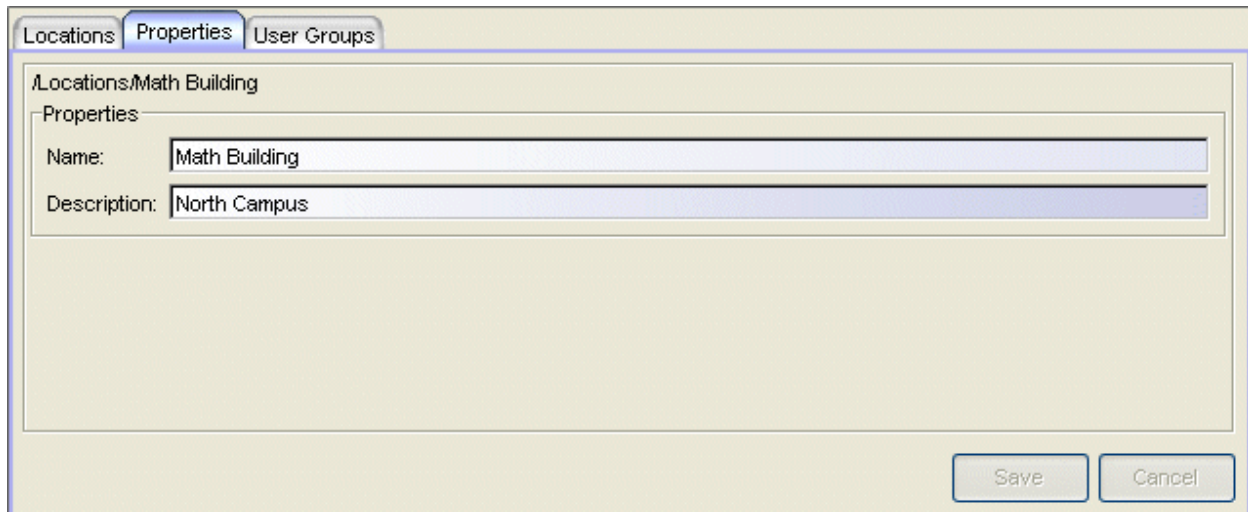
Related Information

For information on related windows:

- [Properties Tab \(Folder\)](#)
- [User Groups Tab](#)

Properties Tab (Folder)

This tab lets you view and change the name and description of a folder in the left-panel Locations tree. To access this tab, select a location in the left-panel tree, then click the Properties tab in the right panel.



The screenshot shows a software interface with three tabs: 'Locations', 'Properties', and 'User Groups'. The 'Properties' tab is active. The path shown is '/Locations/Math Building'. Below the path, there is a 'Properties' section with two text input fields: 'Name' containing 'Math Building' and 'Description' containing 'North Campus'. At the bottom right of the window, there are two buttons: 'Save' and 'Cancel'.


Name

The location name.

Description

A description of the location.

Save

Saves your changes to the PCC database. Be sure to enforce these changes to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

Cancel

Cancels any changes you have made and restores the original properties.

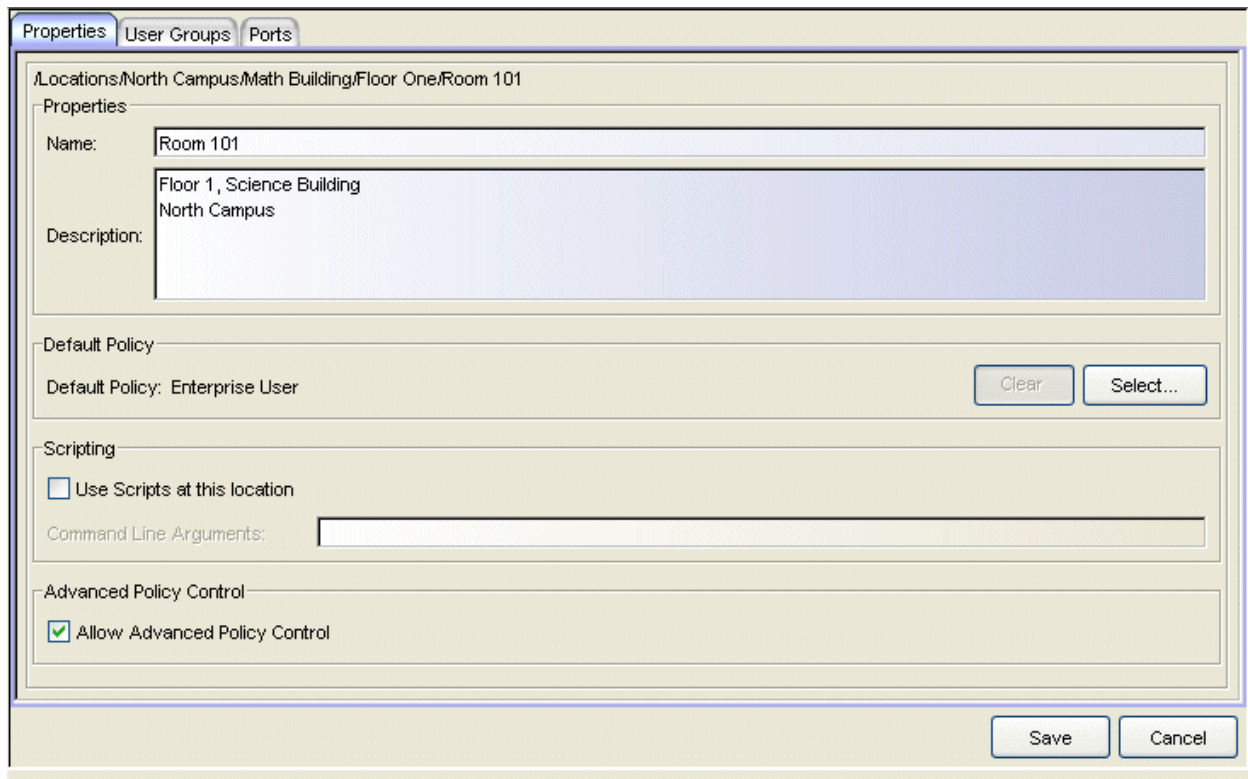
Related Information

For information on related windows:

- [Locations Tab](#)
- [User Groups Tab](#)

Properties Tab (Location)

This tab lets you view and change the name and description of a location, and lets you define a default policy for the location. It also lets you specify whether you will be using scripts to set policy on the ports assigned to this location. To access this tab, select a location in the left-panel tree, then click the Properties tab in the right panel.



The screenshot shows a configuration window titled "Properties" with three tabs: "Properties", "User Groups", and "Ports". The "Properties" tab is active. The window displays the path "/Locations/North Campus/Math Building/Floor One/Room 101". The "Properties" section contains a "Name" field with the value "Room 101" and a "Description" field with the value "Floor 1, Science Building North Campus". The "Default Policy" section shows "Default Policy: Enterprise User" with "Clear" and "Select..." buttons. The "Scripting" section has an unchecked checkbox for "Use Scripts at this location" and a "Command Line Arguments" field. The "Advanced Policy Control" section has a checked checkbox for "Allow Advanced Policy Control". "Save" and "Cancel" buttons are at the bottom right.

Name

The location name.

Description

A description of the location.

Default Policy

The default policy for this location. When policy is set for a location via the PCC web page, it can be configured to expire in a certain amount of time. When the policy expires, the location reverts to the default policy assigned here (if one has been specified). Use the **Select** button to open a window where you can select a policy as a default policy. Only policies from the

user groups assigned to the location are available for selection. Use the **Clear** button to set the default policy to <None>.

Scripting

If you are using scripts to set policy on the ports assigned to this location, you must select the "Use Scripts at this location" checkbox. Use the Command Line Arguments field to enter custom arguments that will be appended to a script command line each time it is invoked for this location. For more information on using scripts to set policy, see [How to Use Scripts](#).

Advanced Policy Control

Selecting this option allows PCC users to set policy for this location on a port-by-port basis. The Advanced Policy Assignment is configured in the [Policy Management PCC web page](#).


Clear

Clears the default policy set for this location and sets it to <None>.

Select

Opens the Select Default Policy window where you can either clear the default policy for the location (set the default policy to <None>) or select a new default policy for the location. Only policies from the user groups assigned to the location are available for selection.

Save

Saves your changes to the PCC database. Be sure to enforce these changes to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

Cancel

Cancels any changes you have made and restores the original properties.

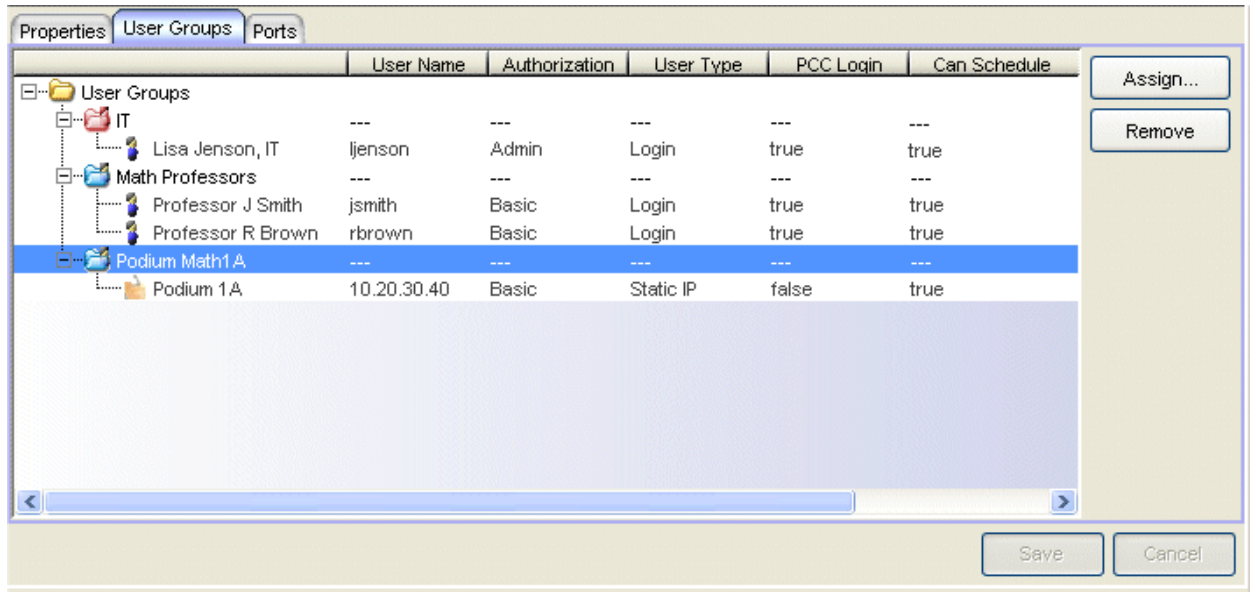
Related Information

For information on related windows:

- [Ports Tab](#)
- [User Groups Tab](#)

User Groups Tab

This tab lists the user groups and users assigned to a specific folder or location, and lets you add and remove user groups, if desired. To access this tab, select a folder or location in the left-panel tree, then click the User Groups tab in the right panel. Expand the user group folders to view the users in each group.





User Groups

The following information is listed for each user group.

Description

The description of the user group that was entered when the group was created. You can edit this description in the Properties tab for the user group in the [Manage Users window](#).

Assignment

Indicates whether the user group was assigned directly to this location or whether the location inherited the user group when it was assigned to a parent folder in the Locations tree. Direct-assigned user groups are indicated with blue folders  and inherited user groups are indicated with pink folders . You cannot remove inherited user groups in this tab; they must be removed from the parent folder where they were directly assigned.

Users

When you expand the user groups folders, you will see the following information listed for each assigned user. Users are listed by their display name, which is the name that will be displayed on the PCC web page after they log in.

User Name

The name the user will use to log in to the PCC web page.

Authorization

A login user can be configured with either of the following two authorization types; static IP users are always configured with Basic authorization.

- Admin - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
 - view a PCC activity log.
- Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.

User Type

A user can be created as one of two types:

- Login - The user authenticates to access the PCC web page and set policies for their allowed locations.
- Static IP - A "podium" computer provides open access to the PCC web page to set policies for allowed locations (usually for that location only).

PCC Login

Whether the user is required to log in to the PCC web page using the PCC login password specified when the user was created: true or false.

Can Schedule

Whether the user has access to the scheduling functionality on the PCC web page: true or false.


Assign

Opens the [Assign User Groups window](#) where you can assign user groups to the location.

Remove

Select a user group and click **Remove** to delete the group from the location. You cannot remove inherited user groups in this tab; they must be removed from the parent folder where they were directly assigned.

Save

Saves your changes to the PCC database. Be sure to enforce these changes to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

Cancel

Cancels any changes you have made and restores the original list of user groups.


Related Information

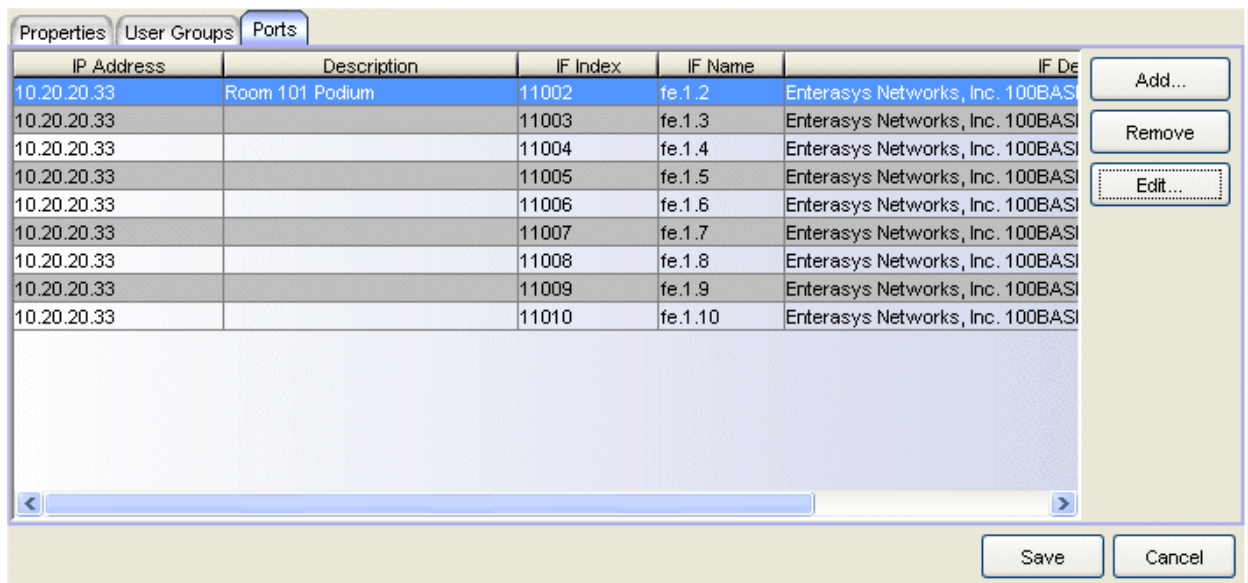
For information on related windows:

- [Assign User Groups Window](#)
- [Manage Users Window](#)
- [Properties Tab](#)

Ports Tab

This tab lists the ports assigned to a specific location, and lets you add and remove ports, if desired. To access this tab, select a location in the left-panel tree, then click the Ports tab in the right panel.

NOTE: Invalid ports (indicated with a ) are ports where policies can no longer be applied because the device has been deleted from Console. You must remove these ports using the Remove button on this tab. Errors will occur when enforcing to PCC appliances until these ports are removed.



The screenshot shows a software interface with three tabs: Properties, User Groups, and Ports. The Ports tab is active, displaying a table with the following columns: IP Address, Description, IF Index, IF Name, and IF De. The table contains ten rows of data. To the right of the table are three buttons: Add..., Remove, and Edit... (with a dotted border). At the bottom right of the interface are Save and Cancel buttons.

IP Address	Description	IF Index	IF Name	IF De
10.20.20.33	Room 101 Podium	11002	fe.1.2	Enterasys Networks, Inc. 100BAS
10.20.20.33		11003	fe.1.3	Enterasys Networks, Inc. 100BAS
10.20.20.33		11004	fe.1.4	Enterasys Networks, Inc. 100BAS
10.20.20.33		11005	fe.1.5	Enterasys Networks, Inc. 100BAS
10.20.20.33		11006	fe.1.6	Enterasys Networks, Inc. 100BAS
10.20.20.33		11007	fe.1.7	Enterasys Networks, Inc. 100BAS
10.20.20.33		11008	fe.1.8	Enterasys Networks, Inc. 100BAS
10.20.20.33		11009	fe.1.9	Enterasys Networks, Inc. 100BAS
10.20.20.33		11010	fe.1.10	Enterasys Networks, Inc. 100BAS

IP Address

The IP address of the device where the port resides.

Description

A description of the port. You can add or edit the port description by selecting the port and clicking the **Edit** button.

IF Index

The interface value assigned to the port index.

IF Name

The port interface name.

IF Descriptor

A description of the interface.

Add

Opens the [Add Ports window](#) where you can add ports to the location. You can also right-click a port in the tab and select Add from the menu.


Remove

Select a port and click **Remove** to delete the port from the table.

Edit

Select a port and click **Edit** to open the Port Properties window where you can view certain port properties and add or edit the port description. You can also right-click a port in the tab and select Edit from the menu.

Save

Saves your changes to the PCC database. Be sure to enforce these changes to the PCC appliances using the **Enforce to Appliances** button  on the PCC toolbar.

Cancel

Cancels any changes you have made and restores the original list of ports.

Related Information

For information on related windows:

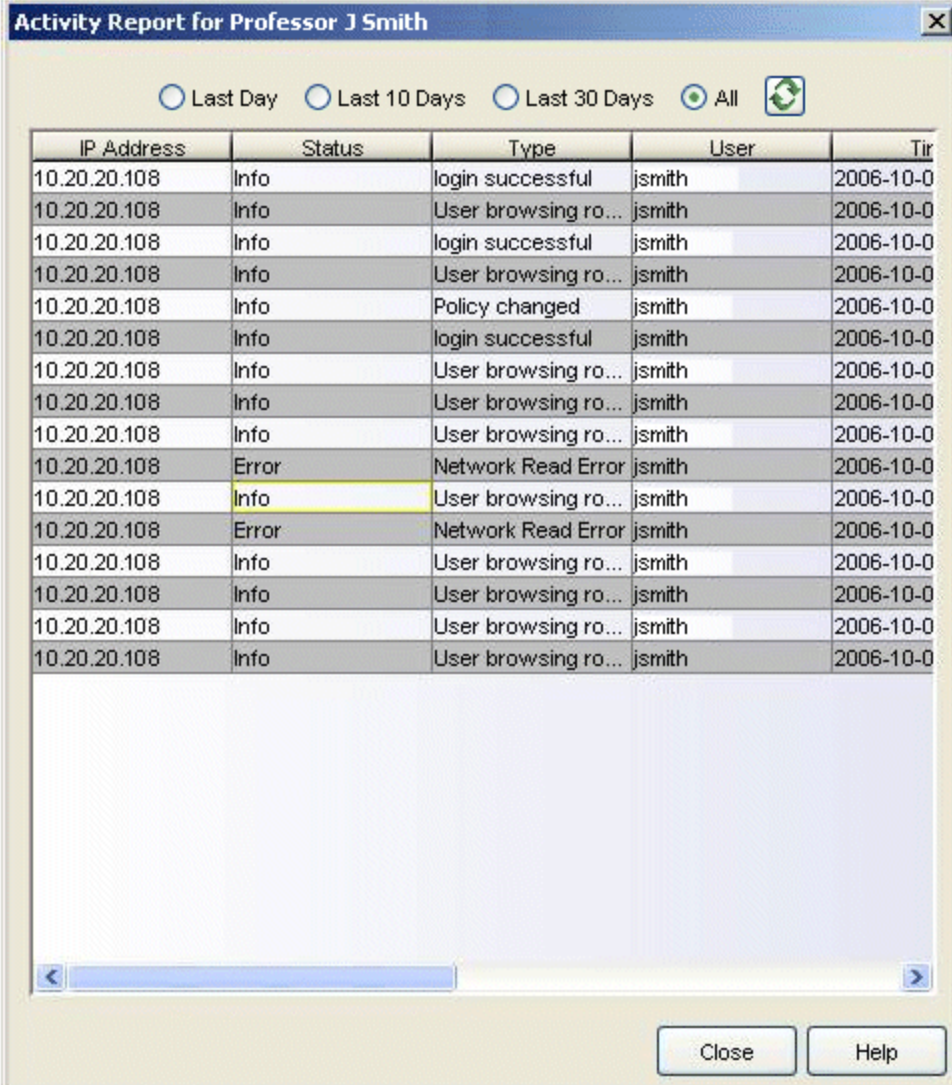
- [Properties Tab](#)
- [User Groups Tab](#)

Policy Control Console Windows

The **Windows** help section contains help topics describing Policy Control Console windows and their field definitions.

Activity Report Window

The Activity Report window lets you view policy change activity for the PCC users and locations in your network. It displays event messages received from the PCC appliance (embedded virtual appliance or external appliance) for a single location or user during a specified period of time. To access the window, right-click a location in the left-panel Locations tree or a user in the [Manage Users window](#) (Tools > Manage Users) and select **Activity Report** from the menu. Use the buttons at the top of the window to specify the time period of activity that you want to view.



IP Address	Status	Type	User	Time
10.20.20.108	Info	login successful	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Info	login successful	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Info	Policy changed	jsmith	2006-10-0
10.20.20.108	Info	login successful	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Error	Network Read Error	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Error	Network Read Error	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0
10.20.20.108	Info	User browsing ro...	jsmith	2006-10-0

IP Address

The IP address of the appliance (embedded virtual appliance or external appliance) that was the source of the event.

Status

The event's severity (e.g. Info, Warning, Error).

Type

The type of event.

User

The user's login name (for a Login User) or IP address (for a Static IP User).

Time

The date and time the event took place.

Location

The location where the event took place.

New Policy

The new policy that was set.

Old Policy

The old policy that was changed.

Details

More detailed information about the event, if available.



Refresh

Refreshes the information in the activity report.

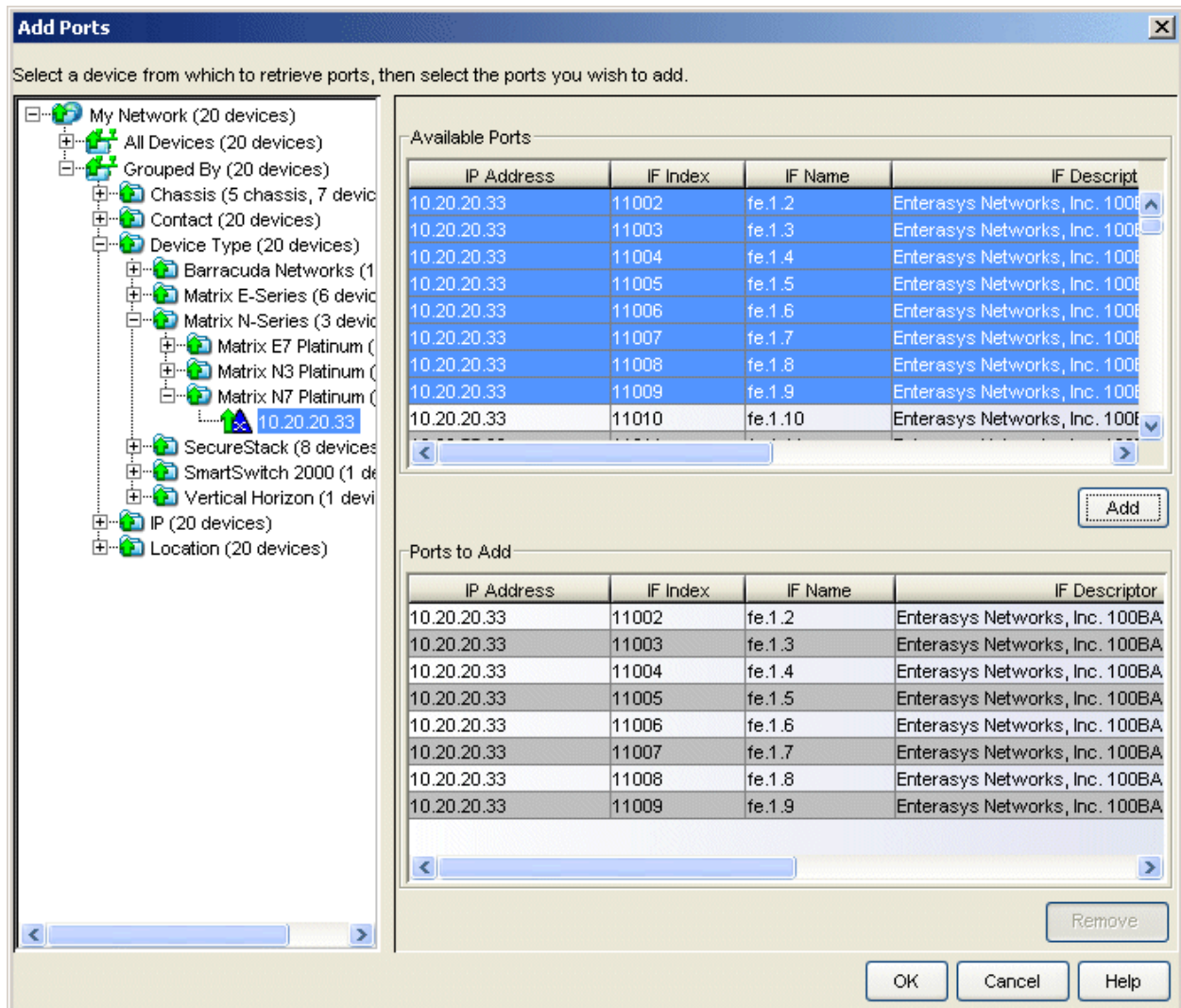
Related Information

For information on related windows:

- [Appliance Events Window](#)
- [Events View](#)

Add Ports Window

The Add Ports window lets you select a device, retrieve its ports, and then select one or more ports to add to a location. The window is accessed from the right-panel [Ports tab](#) when a location is selected in the left-panel tree.



Device Tree

The left panel displays a device tree of your network devices. Expand the device tree and select a device from which to retrieve ports.

Available Ports Table

When you select a device in the tree, its ports are displayed in the top right-panel table. Each port displays the IP address of the device where the port resides, the interface value assigned to the port index, the port interface name, and a description of the interface. There is also a column that displays whether the port is currently assigned to a location and the path to the location where it is assigned. Because only access ports should be added to a location, only access ports are displayed in the table. All CDP, backplane, and logical ports are filtered out. Select the ports you want to add to a location, and click **Add**.

Ports to Add Table

This table displays the ports you have selected to add to a location. Each port displays the IP address of the device where the port resides, the interface value assigned to the port index, the port interface name, and a description of the interface. There is also a column that displays whether the port is currently assigned to a location and the path to the location where it is assigned. To delete a port, select the port in the table and click **Remove**. Click **OK** to add the ports to the location.

Add

In the Available Ports table, select the ports you want to add to a location and click **Add**. The ports are listed in the Ports to Add table.

Remove

To delete a port from the Ports to Add table, select the port and click **Remove**.

OK

Adds the selected ports to the location and closes the window.

Cancel

Closes the window without adding any ports to the location.

Related Information

For information on related windows:

- [Ports Tab](#)

Add User Window

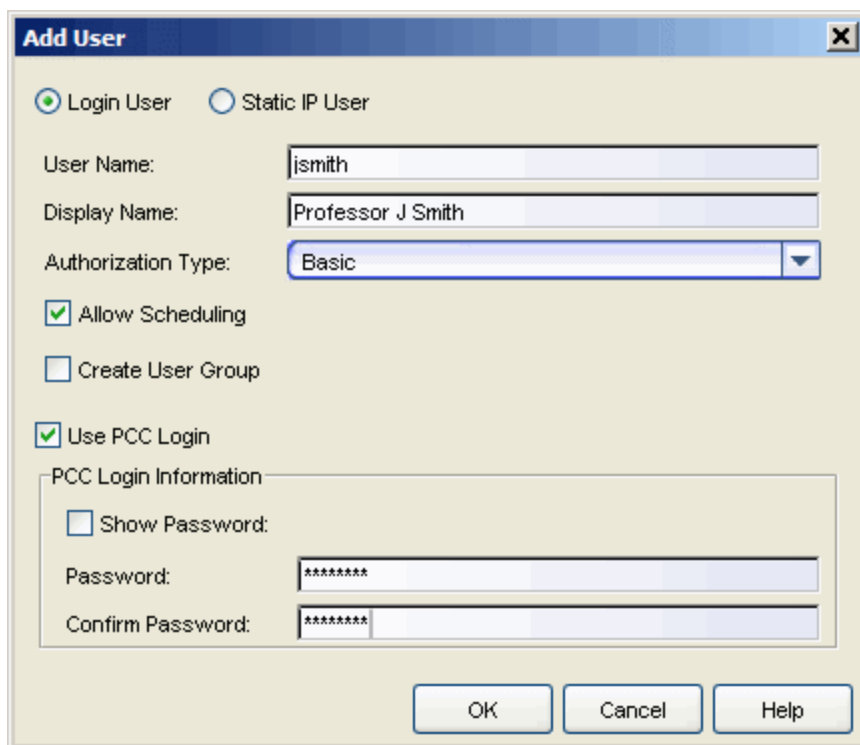
Use this window to add your PCC users to the [Manage Users window](#). You can add two kinds of users: Login Users and Static IP Users. After you have added your users, you must assign them to the appropriate user groups.

Information on:

- [Login Users](#)
- [Static IP Users](#)

Login Users

Login users are PCC users that must authenticate to access the PCC web page.



The screenshot shows the 'Add User' dialog box with the following details:

- Radio Buttons:** Login User, Static IP User
- User Name:** jsmith
- Display Name:** Professor J Smith
- Authorization Type:** Basic (dropdown menu)
- Checkboxes:**
 - Allow Scheduling
 - Create User Group
 - Use PCC Login
- PCC Login Information:**
 - Show Password:
 - Password:** [masked with asterisks]
 - Confirm Password:** [masked with asterisks]
- Buttons:** OK, Cancel, Help

User Name

The name the user will use to log in to the PCC web page.

Display Name

The user's name that will be displayed on the PCC web page.

Authorization Type

A login user can be configured with either of the following two authorization types:

- Admin - Provides access to the PCC web page to:
 - define and schedule policy for allowed locations.
 - configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
 - view a PCC activity log.
- Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - schedule policy for allowed locations if the Allow Scheduling option is selected.

Allow Scheduling

Select this checkbox to grant the user access to the scheduling functionality on the PCC web page. This enables the user to schedule policy changes for their allowed locations.

Create User Group

When this checkbox is selected, a user group will be automatically created based on the user name, and will list the user as a member of the group. This feature is most commonly used for Static IP users.

Use PCC Login

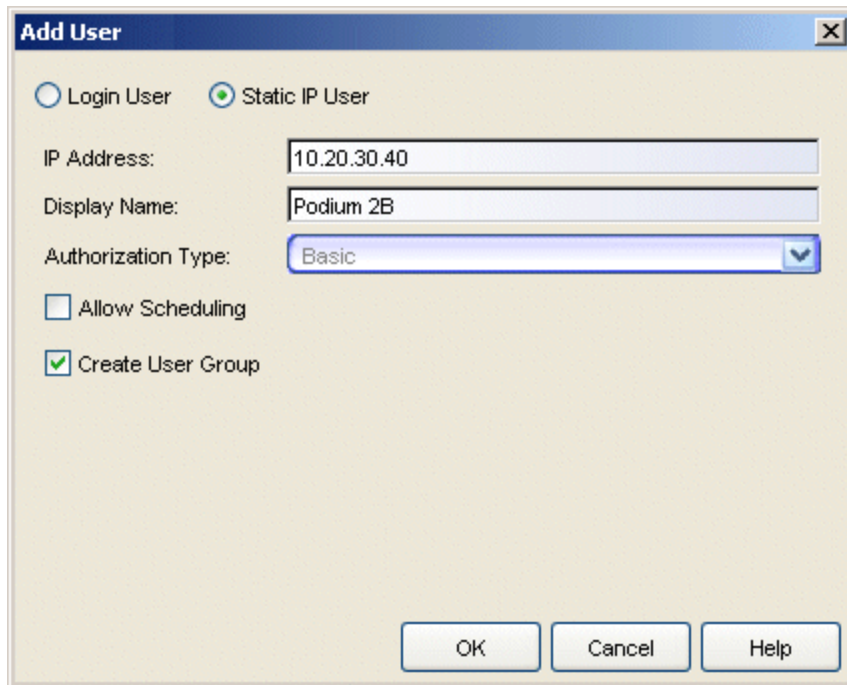
Select this checkbox if PCC is handling user authentication to the PCC web page. Enter and confirm the password. If PCC Login is not selected, LDAP must be configured. When the Show Password option is checked, the password is shown in text. When unchecked, the password is shown as a string of asterisks.

NOTE: Spaces are not allowed in passwords and will be ignored.

Static IP Users

Static IP Users are created for specific locations such as lecture halls or conference rooms where there would be a dedicated computer that anyone could use to access a PCC web page and set policies for that location. For example, if there was a room used by several professors, it might be difficult to

schedule internet access for that room. If a professor needed to turn off web access for the room, they would have to turn it off at the dedicated computer.



The screenshot shows a dialog box titled "Add User". At the top, there are two radio buttons: "Login User" (unselected) and "Static IP User" (selected). Below these are three input fields: "IP Address:" with the value "10.20.30.40", "Display Name:" with the value "Podium 2B", and "Authorization Type:" with a dropdown menu showing "Basic". There are two checkboxes: "Allow Scheduling" (unchecked) and "Create User Group" (checked). At the bottom, there are three buttons: "OK", "Cancel", and "Help".

IP Address

The IP address of the dedicated system for that location.

Display Name

The name that will be displayed on the PCC web page.

Authorization Type

Static IP users are always configured with Basic authorization which provides access to the PCC web page to:

- define policy for allowed locations.
- schedule policy for allowed locations if the Allow Scheduling option is selected.

Allow Scheduling

Select this checkbox to grant the user access to the scheduling functionality on the PCC web page. This enables the user to schedule policy changes for allowed locations.

Create User Group

When this checkbox is selected, a user group will be automatically created based on the IP address, and will list the Display Name as a member of the group.

Related Information

For information on related windows:

- [Manage Users Window](#)

Appliance Events Window

The Appliance Events window displays all event messages received from the PCC engines (embedded virtual engine and/or external engines) during a specified period of time. You can access the window from the Tools menu (Tools > Appliance Events). Use the buttons at the top of the window to specify the time period of activity that you want to view.

NOTE: For external PCC engines: If you compare an event in the Appliance Events window to the same engine event in the [PCC Events tab](#), you may notice a difference in the timestamp. This is because events in the Appliance Events window display the timestamp of the engine, while events in the PCC Events tab display the timestamp of the Extreme Management Center server. Run NTP (Network Time Protocol) on the PCC engine to synchronize its clock with the Extreme Management Center Server.

IP Address	Status	Type	User	Time
	Warn	Contact with serv...	---	2006-1
	Info	Contact with serv...	---	2006-1
	Info	PCC Appliance ca...	---	2006-1
10.20.20.172	Info	PCC Appliance st...	---	2006-1
10.20.20.172	Info	Contact with serv...	---	2006-1
10.20.20.172	Info	PCC Appliance ca...	---	2006-1
10.20.20.172	Info	login successful	jsmith	2006-1
10.20.20.172	Info	User browsing ro...	jsmith	2006-1
10.20.20.172	Info	login successful	ljenson	2006-1
10.20.20.172	Info	User browsing ro...	jsmith	2006-1
10.20.20.172	Info	Policy changed	jsmith	2006-1
10.20.20.172	Info	login successful	rbrown	2006-1
10.20.20.172	Info	User browsing ro...	ljenson	2006-1
10.20.20.172	Info	User browsing ro...	rbrown	2006-1
10.20.20.172	Info	User browsing ro...	jsmith	2006-1
10.20.20.172	Error	Network Read Error	jsmith	2006-1
10.20.20.172	Info	User browsing ro...	ljenson	2006-1
10.20.20.172	Error	Network Read Error	rbrown	2006-1
10.20.20.172	Info	User browsing ro...	jsmith	2006-1
10.20.20.172	Info	PCC Appliance ca...	---	2006-1
10.20.20.172	Info	User browsing ro...	jsmith	2006-1
10.20.20.172	Info	PCC Appliance ca...	---	2006-1
10.20.20.172	Info	User browsing ro...	jsmith	2006-1
10.20.20.172	Info	User browsing ro...	rbrown	2006-1
10.20.20.172	Info	User browsing ro...	141.141.90.141	2006-1

IP Address

The IP address of the engine that was the source of the event.

Status

The event's severity (Info, Warning, Error).

Type

The type of event.

User

The user's login name (for a Login User) or IP address (for a Static IP User).

Time

The date and time the event took place.

Location

The location where the event took place.

New Policy

The new policy that was set.

Old Policy

The old policy that was changed.

Details

More detailed information about the event, if available.



Refresh

Refreshes the information in the Appliance Events window.

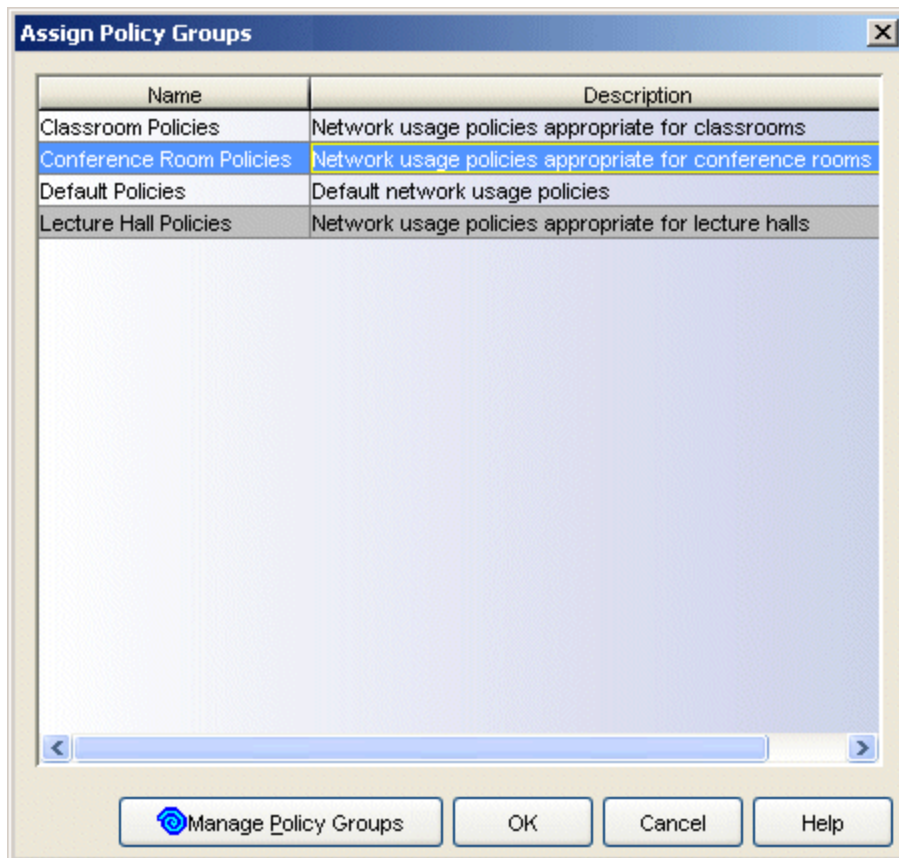
Related Information

For information on related windows:

- [Activity Report Window](#)
- [Events View](#)

Assign Policy Groups Window

The Assign Policy Groups window displays all the policy groups you have created via the [Manage Policy Groups window](#) and lets you select one or more groups to assign to a user group. To access this window, select a user group in the [Manage Users window](#), and click the Add Policy Groups button in the right-panel Allowed Policy Groups tab.



Name

The name of the policy group.

Description

A description of the policy group.

Manage Policy Groups

Opens the [Manage Policy Groups window](#) where you can create and define policy groups.

OK

Assigns the selected policy groups to the user group and closes the window.

Cancel

Closes the window without assigning any policy groups to the user group.

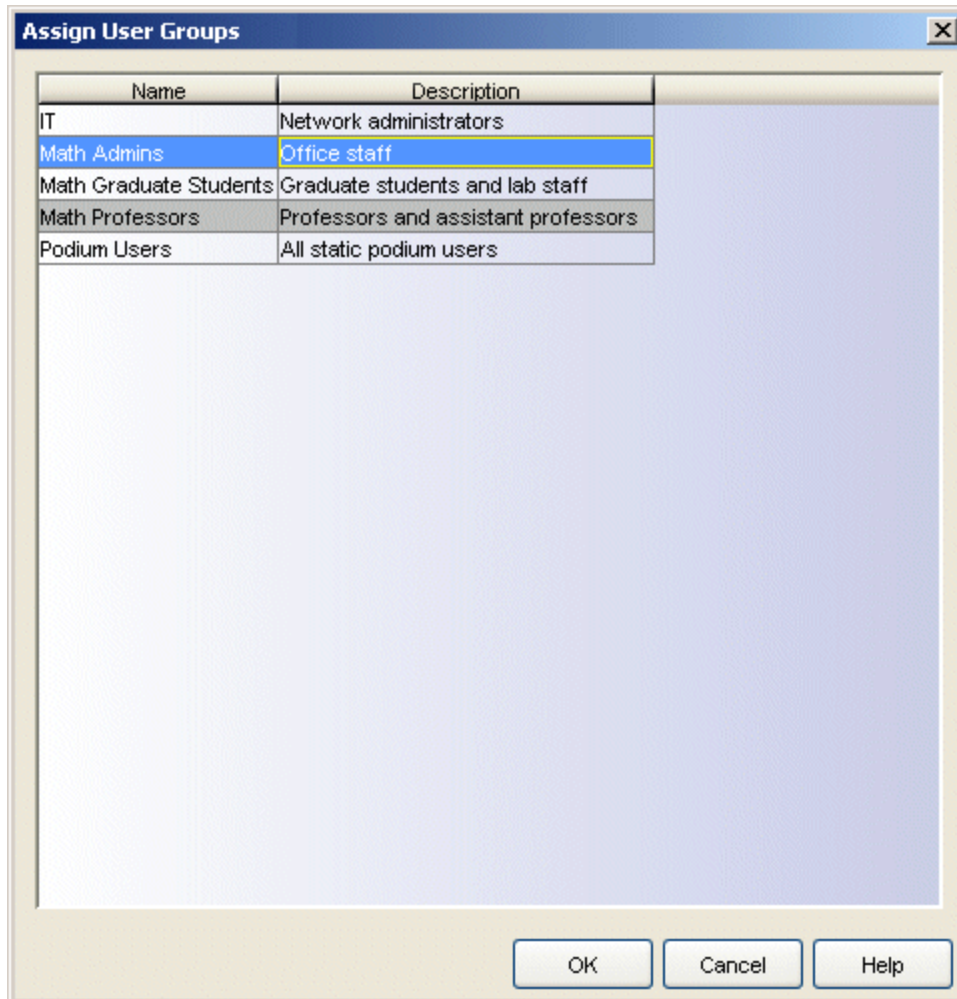
Related Information

For information on related windows:

- [Manage Policy Groups Window](#)
- [Manage Users Window](#)

Assign User Groups Window

The Assign User Groups window displays the user groups you have created via the [Manage Users window](#) and lets you select one or more user groups to assign to a location. The window is accessed from the right-panel [User Groups tab](#) when a location or folder is selected in the left-panel tree.



Name

The name of the user group.

Description

A description of the user group.

OK

Assigns the selected user groups to the location and closes the window.

Cancel

Closes the window without assigning any user groups to the location.

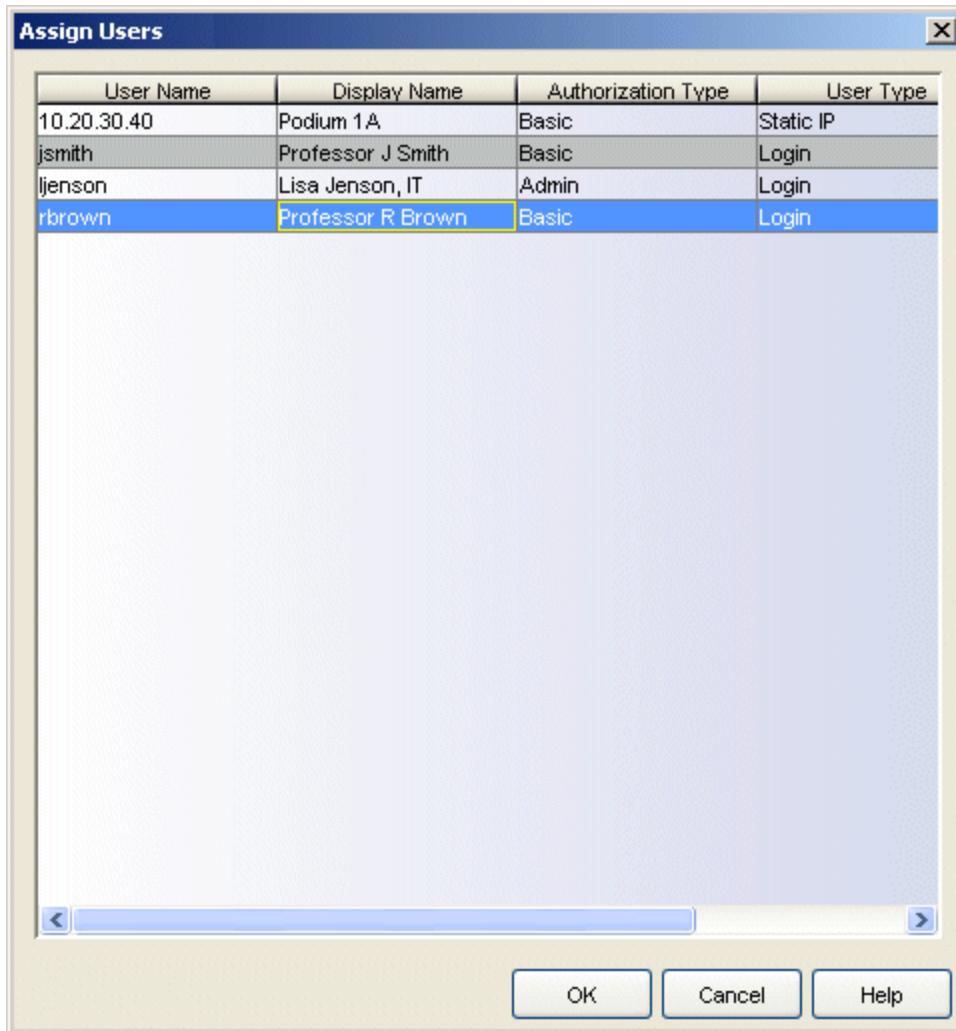
Related Information

For information on related windows:

- [Manage Users Window](#)
- [User Groups Tab](#)

Assign Users Window

The Assign Users window displays the users you have created via the [Manage Users window](#) and lets you select one or more users to assign to a user group. To access this window, select a user group in the Manage Users window, and click the Assign Users button in the right-panel Assigned Users tab.



User Name

The name the user will use to log in to the PCC web page.

Display Name

The user's name that will be displayed on the PCC web page.

Authorization Type

A login user can be configured with either of the following two authorization types; static IP users are always configured with Basic authorization.

- Admin - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
 - view a PCC activity log.
- Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.

User Type

A user can be created as one of two types:

- Login - The user authenticates to access the PCC web page and set policies for their allowed locations.
- Static IP - A "podium" computer provides open access to the PCC web page to set policies usually for that location only.

PCC Login

Indicates whether the user is required to log in to the PCC web page using the PCC login password specified when the user was created: true or false.

OK

Assigns the selected users to the user group and closes the window.

Cancel

Closes the window without assigning any users to the user group.


Related Information

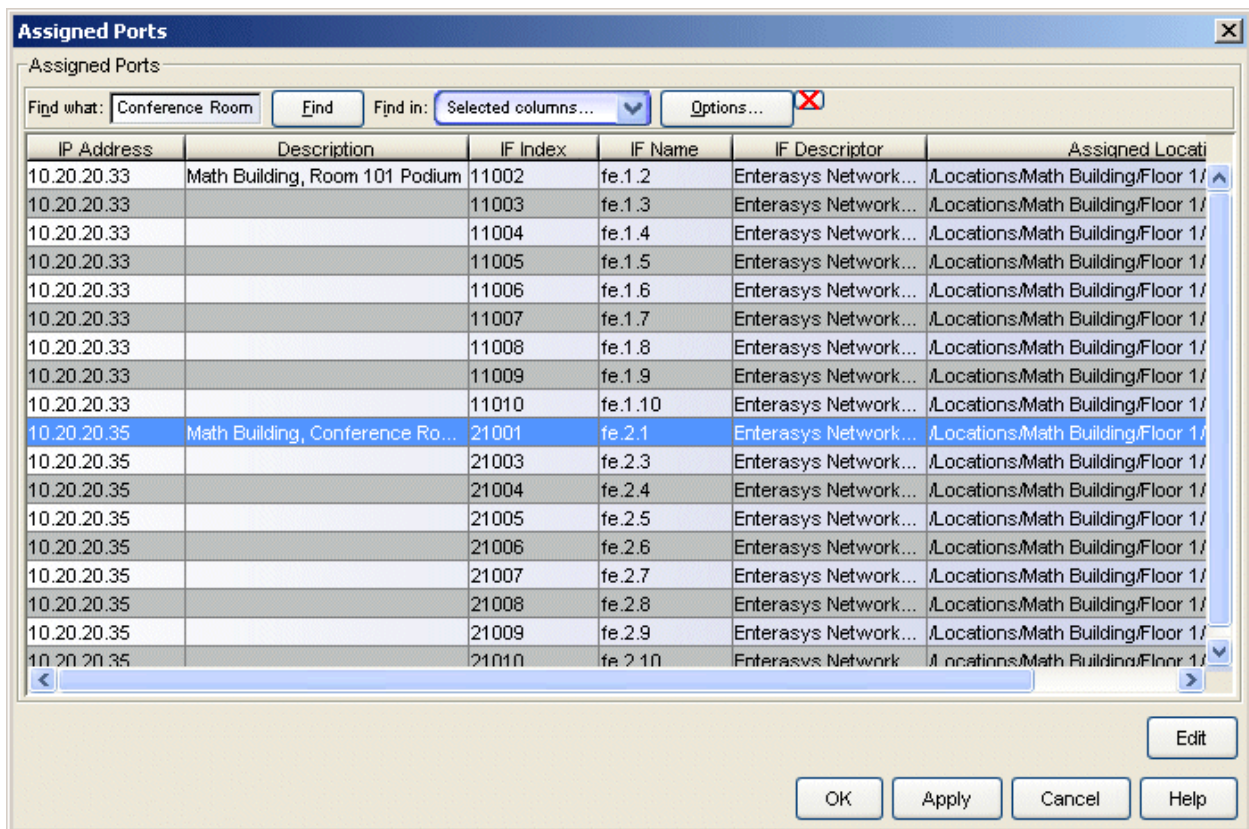
For information on related windows:

- [Manage Users Window](#)
- [User Groups Tab](#)

Assigned Ports Window

This window lets you view and search all the ports that are currently assigned to locations. To access the window, select any folder or location in the Locations

tree, and then select Tools > Assigned Ports or click the  button on the toolbar. The window opens displaying all the ports currently assigned to locations. You can search for a port by using the Find or Filter table tools available through a right-mouse click on a column heading or anywhere in the table body. For more information, see Table Tools.



The screenshot shows the 'Assigned Ports' window with a search toolbar and a table of network ports. The search toolbar includes a 'Find what:' field with 'Conference Room' entered, a 'Find' button, a 'Find in:' dropdown menu set to 'Selected columns...', and an 'Options...' button with a close icon. The table below has six columns: IP Address, Description, IF Index, IF Name, IF Descriptor, and Assigned Location. The row for IP 10.20.20.35 is highlighted in blue.

IP Address	Description	IF Index	IF Name	IF Descriptor	Assigned Location
10.20.20.33	Math Building, Room 101 Podium	11002	fe.1.2	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.33		11003	fe.1.3	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.33		11004	fe.1.4	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.33		11005	fe.1.5	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.33		11006	fe.1.6	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.33		11007	fe.1.7	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.33		11008	fe.1.8	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.33		11009	fe.1.9	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.33		11010	fe.1.10	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35	Math Building, Conference Ro...	21001	fe.2.1	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35		21003	fe.2.3	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35		21004	fe.2.4	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35		21005	fe.2.5	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35		21006	fe.2.6	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35		21007	fe.2.7	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35		21008	fe.2.8	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35		21009	fe.2.9	Enterasys Network...	/Locations/Math Building/Floor 1/
10.20.20.35		21010	fe.2.10	Enterasys Network...	/Locations/Math Building/Floor 1/

Find Toolbar

The Find toolbar lets you locate a specific port in the table. You can search in a single column or in all columns and you can search forward or backward from your current position. You access the Find toolbar by right-clicking on a column header and selecting Find. The toolbar appears at the top of the table.

IP Address

The IP address of the device where the port resides.

Description

A description of the port. You can add or edit the port description by selecting the port and clicking the **Edit** button.

IF Index

The interface value assigned to the port index.

IF Name

The port interface name.

IF Descriptor

A description of the interface.

Assigned Location

The path to the location where the port is assigned.

Edit

Select a port and click **Edit** to open the Port Properties window where you can view certain port properties and add or edit the port description.

OK

Saves any changes to the port descriptions and closes the window.

Apply

Saves any changes to the port descriptions and leaves the window open.

Cancel


Closes the window without saving any port description changes.

Related Information

For information on related windows:

- [Ports Tab](#)

Check Consistency Window

The Check Consistency window verifies your PCC configuration so that policy can be correctly applied to your locations. To access the window, select a folder or single location in the Locations tree, right-click and select **Check Consistency** from the menu. The left panel displays your selection in the Locations tree. The right panel displays the default policies currently configured on the ports in the selected folder or location. If a folder or location has inconsistencies that would prevent a default policy from being applied, it is displayed with a red X icon . Select the folder or location in the tree and use the right-panel tabs to see the problems.

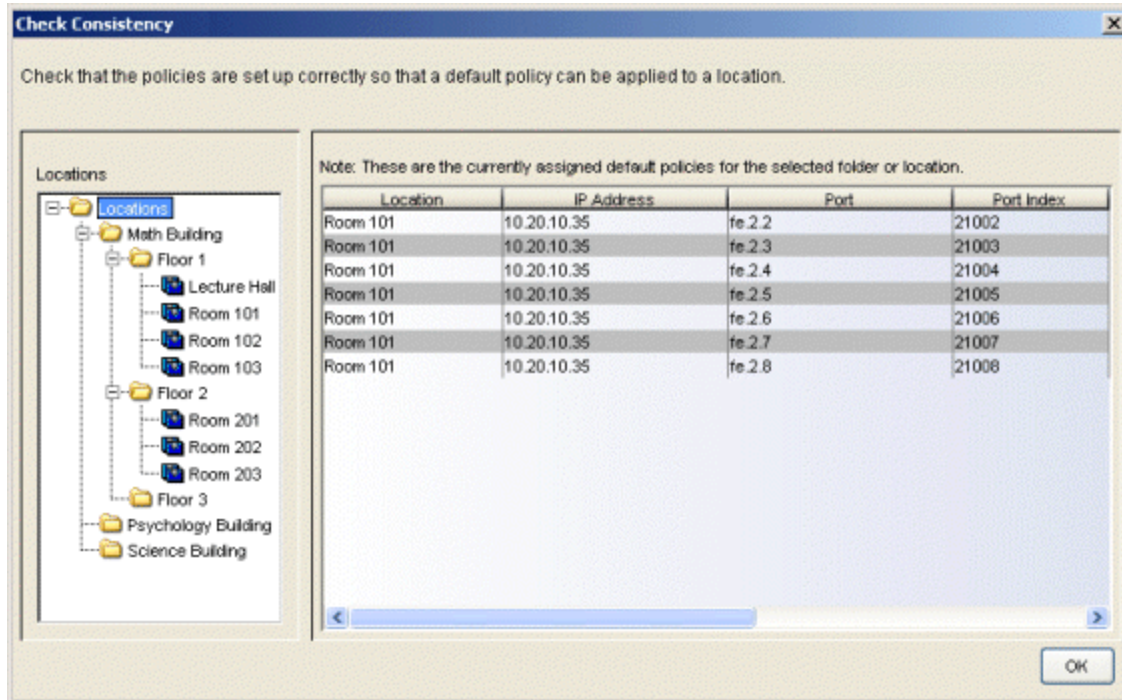
The Check Consistency window checks the following three things for each location:

- Have all the policies assigned to the location been enforced (via Policy Manager) to the associated devices? A policy must be enforced to a device via Policy Manager before it can be set as the default policy for a location via PCC.
- Have all the default policies currently configured on the ports in the location been assigned to the location (via PCC)? A policy must be assigned to a location before it can be set as a default policy via PCC.
- Is a default policy configured for all the ports in the location? Do all the ports in the location have the same default policy currently configured? In most instances, all the ports in a location should have the same configured default policy.

When inconsistencies or problems are found, they are displayed in the right-panel tabs for each location. When no problems are found, the right panel displays a table listing the default policy configured on each port in the selected folder or location (as shown below).

Information on the right-panel tabs:

- [Allowed Policies not created on Devices](#)
- [Default Policies not allowed in Location](#)
- [Default Policies that differ](#)



Location

The name of the location where the default policy is assigned.

IP Address

The IP address of the device where the port resides.

Port

The port interface name.

Port Index

The interface value assigned to the port index.

Default Policy

The default policy configured on the port.

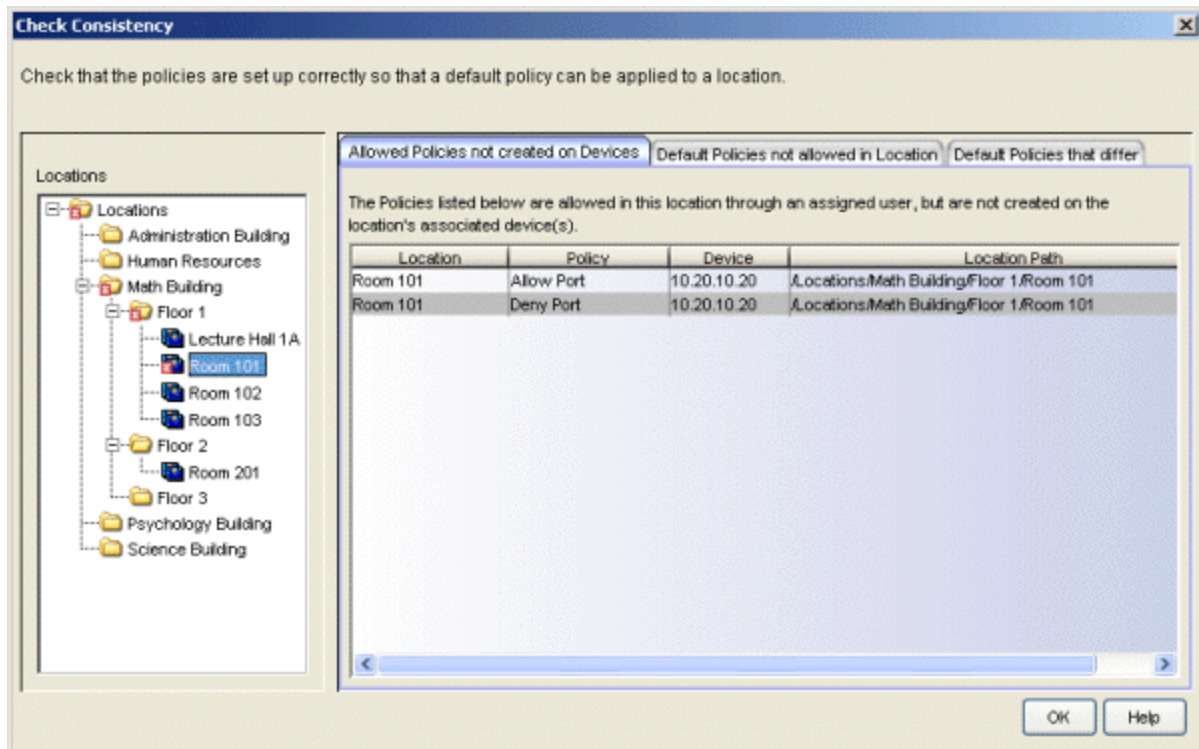
Location Path

The path to the location in the Locations tree.

Allowed Policies not created on Devices Tab

This tab lists any policies that have been assigned to a location (as part of a user group) but have not been enforced to the associated device via Policy Manager. A policy must be enforced to a device via Policy Manager before it can be set as the default policy for a location via PCC. To correct this problem you must either remove the assigned policy from the location (by removing it from the user

group) or use Policy Manager to create and enforce the policy to the associated device.



Location

The name of the location where the policy is assigned through an assigned user group.

Policy

The name of the policy that is assigned to the location as part of a user group but not enforced on the associated devices.

Device

The IP address of the associated device where the policy has not been enforced.

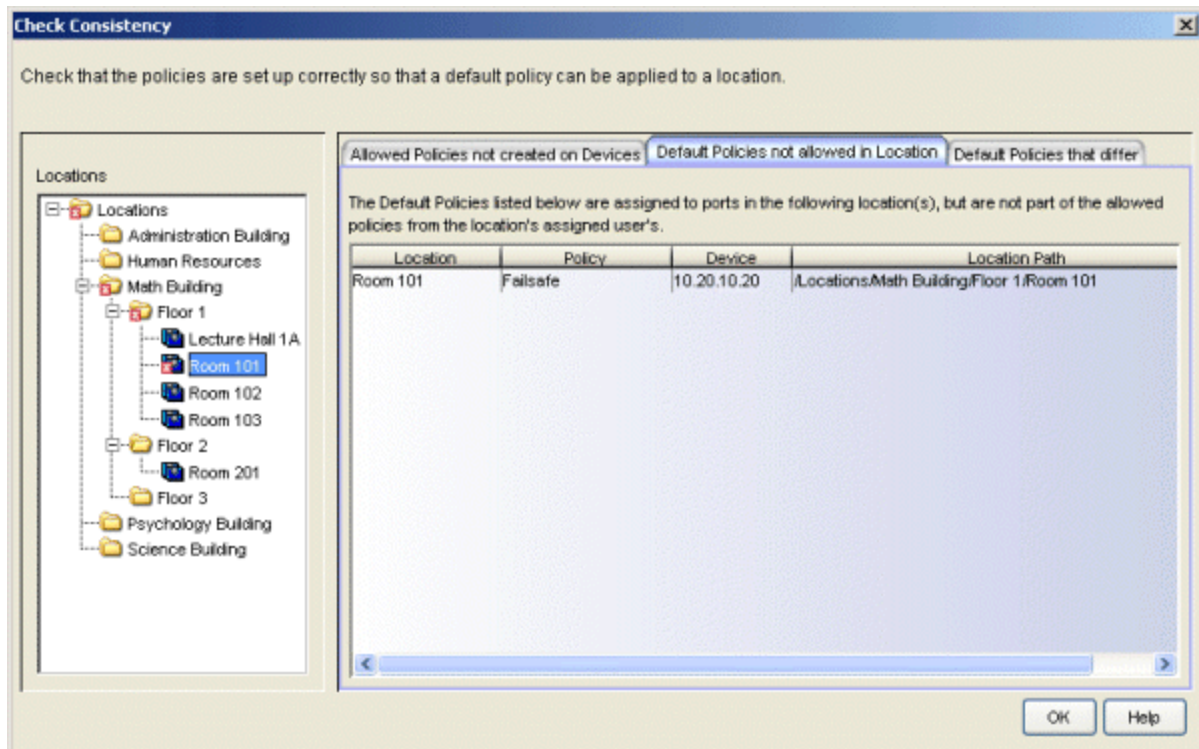
Location Path

The path to the location in the Locations tree.

Default Policies not allowed in Location Tab

This tab lists any policies that are configured as the default policy on a port but are not one of the associated location's assigned policies (as part of a user group). For example, if a port in Location A has been configured (via Policy

Manager or Console) with the default policy "Allow Limited Access" but the "Allow Limited Access" policy has not been assigned to Location A as part of a user group (via PCC), then the default policy "Allow Limited Access" will be listed here. To correct this problem you must either assign the policy to the location (as part of a user group) or change the default policy configured on the port.



Location

The name of the location where the policy needs to be assigned through an assigned user group.

Policy

The name of the policy that needs to be assigned to the location as part of a user group.

Device

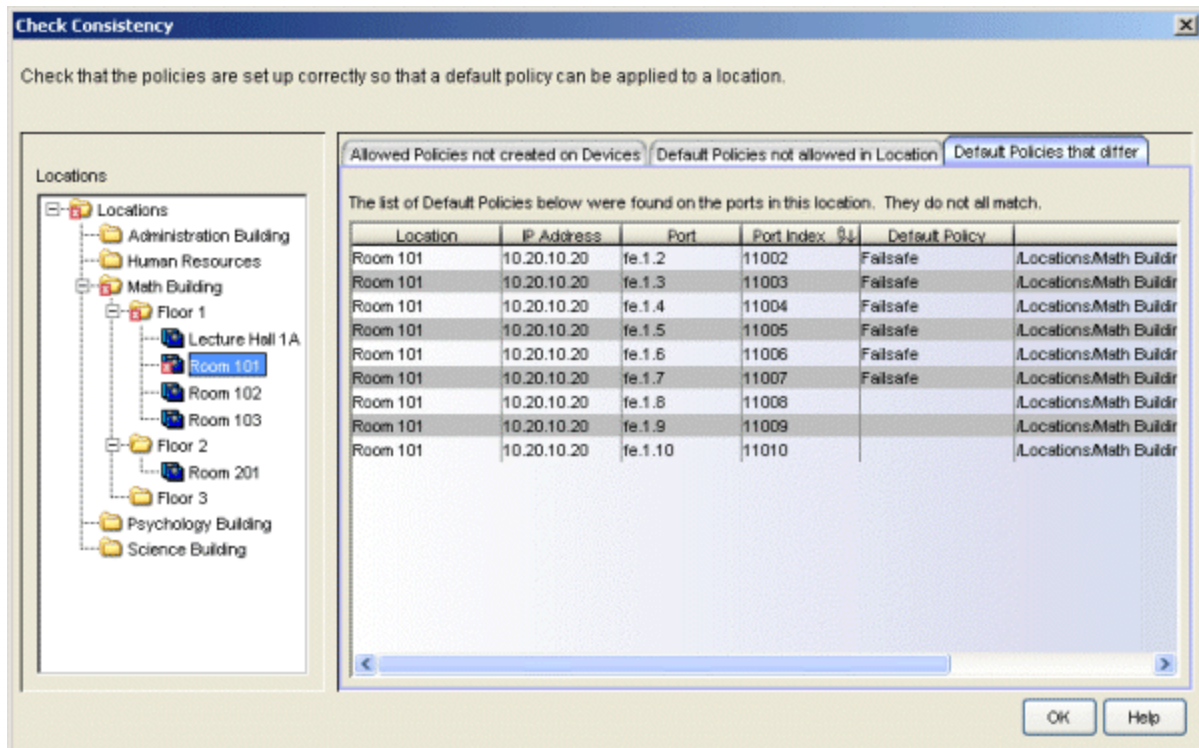
The IP address of the device which has the port with the configured default policy.

Location Path

The path to the location in the Locations tree.

Default Policies that differ Tab

Typically, all the ports included in a location should have the same configured default policy. If some of the ports have different default policies, then this tab will list all the default policies found on all the ports in this location. It also lists the ports that have no default policy configured. This situation might happen if the default policy for a port has been changed using CLI, Policy Manager, or Console, or if a device is down and one of the ports couldn't be set.



Location

The name of the location where the port is added.

IP Address

The IP address of the device where the port resides.

Port

The port interface name.

Port Index

The interface value assigned to the port index.

Default Policy

The default policy configured on the port.

Location Path

The path to the location in the Locations tree.

Related Information

For information on related windows:

- [Manage Policy Groups Window](#)
- [Manage Users Window](#)
- [User Groups Tab](#)
- [Ports Tab](#)

Edit User Window

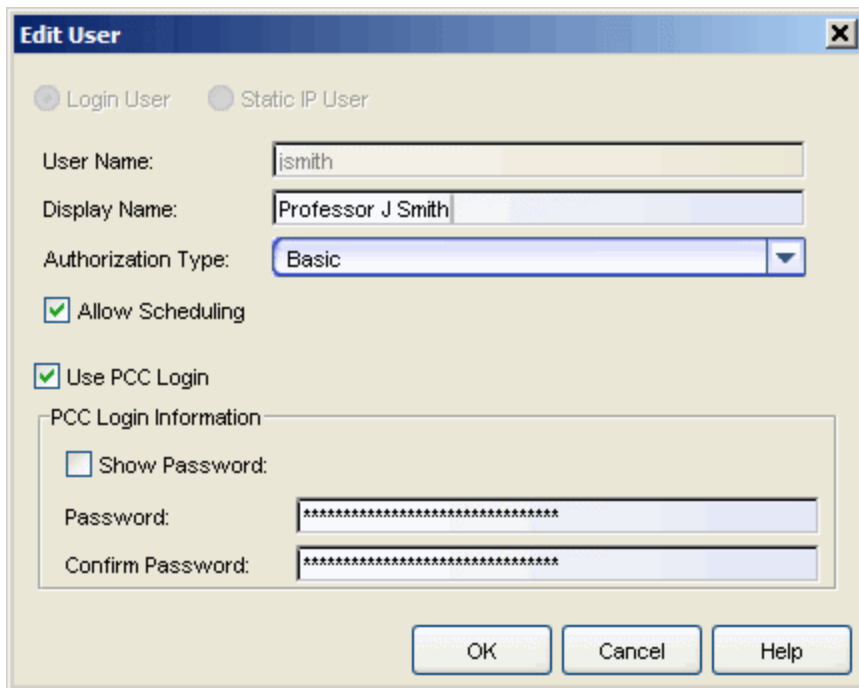
Use this window to edit your PCC users' properties. You can access this window by selecting a user in the [Manage Users window](#) and clicking the Edit Properties button in the right-panel Properties tab. There are two kinds of users: Login Users and Static IP Users.

Information on:

- [Login Users](#)
- [Static IP Users](#)

Login Users

Login users are PCC users that must authenticate to access the PCC web page.



The screenshot shows the 'Edit User' dialog box with the following details:

- Radio buttons: Login User, Static IP User
- User Name:
- Display Name:
- Authorization Type:
- Allow Scheduling
- Use PCC Login
- PCC Login Information section:
 - Show Password:
 - Password:
 - Confirm Password:
- Buttons: OK, Cancel, Help

User Name

The name the user will use to log in to the PCC web page. The user name cannot be edited.

Display Name

The user's name that will be displayed on the PCC web page.

Authorization Type

A login user can be configured with either of the following two authorization types:

- Admin - Provides access to the PCC web page to:
 - define and schedule policy for allowed locations.
 - configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
 - view a PCC activity log.
- Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - schedule policy for allowed locations if the Allow Scheduling option is selected.

Allow Scheduling

Select this checkbox to grant the user access to the scheduling functionality on the PCC web page. This enables the user to schedule policy changes for their allowed locations.

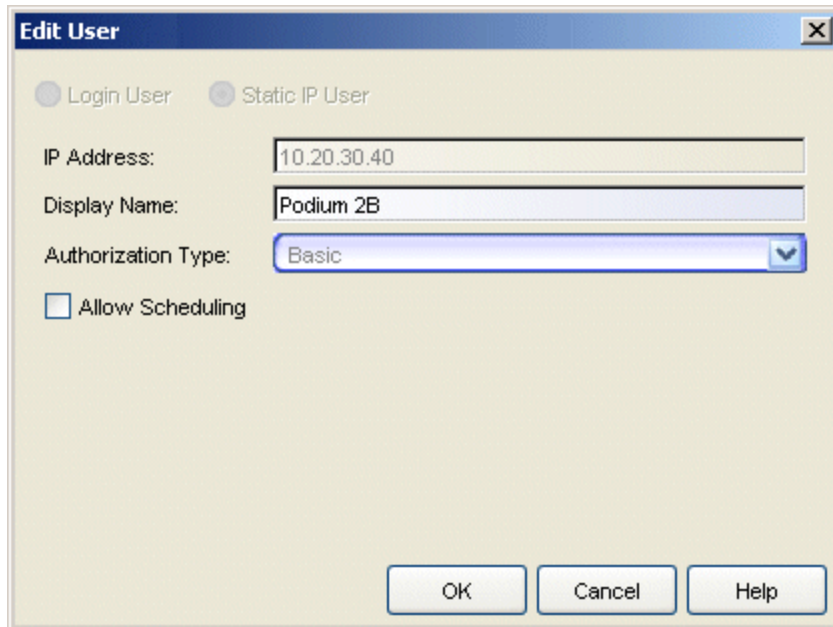
Use PCC Login

Select this checkbox if PCC is handling user authentication to the PCC web page. Enter and confirm the password. If PCC Login is not selected, LDAP must be configured. When the Show Password option is checked, the password is shown in text. When unchecked, the password is shown as a string of asterisks.

NOTE: Spaces are not allowed in passwords and will be ignored.

Static IP Users

Static IP Users are created for specific locations such as lecture halls or conference rooms where there would be a dedicated computer that anyone could use to access a PCC web page and set policies for that location. For example, if there was a room used by several professors, it might be difficult to schedule internet access for that room. If a professor needed to turn off web access for the room, they would have to turn it off at the dedicated computer.



IP Address

The IP address of the dedicated system for that location. The IP address cannot be edited.

Display Name

The name that will be displayed on the PCC web page.

Authorization Type

Static IP users are always configured with Basic authorization which provides access to the PCC web page to:

- define policy for allowed locations.
- schedule policy for allowed locations if the Allow Scheduling option is selected.

Allow Scheduling

Select this checkbox to grant the user access to the scheduling functionality on the PCC web page. This enables the user to schedule policy changes for allowed locations.

Related Information

For information on related windows:

- [Manage Users Window](#)

Policy Control Console Main Window

The Policy Control Console (PCC) main window is divided into a left-panel that displays a Locations tree, a right panel that displays PCC management information, and an Events View. The Locations tree represents specific locations, rooms, or work spaces within a facility or campus. The right-panel displays detailed information about the folder or location selected in the tree. The Events View displays alarm and event information for PCC and PCC appliances (embedded virtual appliance and/or external appliances.) PCC events are also displayed in the Console Event View.

When a single **folder** is selected in the left-panel tree, there are three right-panel tabs that provide detailed information for that folder.

- [Locations Tab](#) - view the contents of the folder.
- [Properties Tab](#) - view and change the folder's name and description.
- [User Groups Tab](#) - add and remove user groups assigned to the folder.

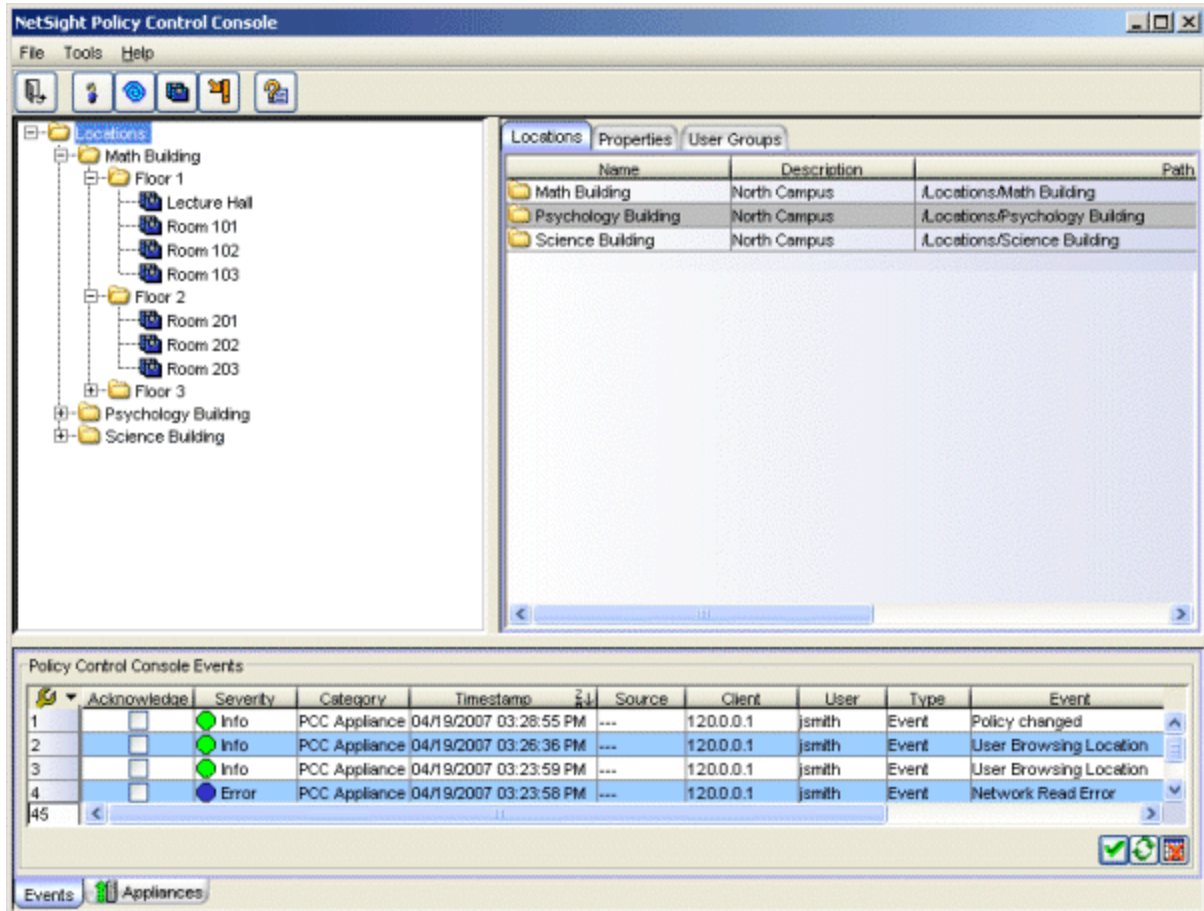
When a single **location** is selected in the left-panel tree, there are three right-panel tabs that provide detailed information for that location.

- [Properties Tab](#) - view and change location properties such as name, description, and default policy.
- [User Groups Tab](#) - add and remove user groups assigned to the location.
- [Ports Tab](#) - add and remove ports assigned to the location.

TIP: Use the table options and tools to find, filter, sort, print, and export information in Policy Control Console tables, and customize table settings. You can access the Table Tools through a right-mouse click on a column heading or anywhere in the table body.

Information on the Main window features:

- [Menu Bar](#)
- [Toolbar](#)
- [Events View](#)



Menu Bar

The menu bar on the Policy Control Console main window provides access to PCC features and functions. For information on menu options available from right-click menus, see [Right-click Menu Options](#).

File Menu

File > Database > Initialize PCC Components

Provides a way for you to initialize only the PCC components in the NetSight Database. The initialize operation removes **all** PCC data elements from the database including configured PCC users, user groups, policy groups, and locations.

File > Exit

Exits the Policy Control Console application. This menu option serves the same function as the **Exit** button  on the toolbar.

*Tools Menu***Tools > New Folder**

Opens the New Folder window where you can enter a name and description for a new folder in the Locations tree.


Tools > New Location

Opens the New Location window where you can enter a name and description for a new location in the Locations tree.


Tools > Delete

Deletes the location or folder selected in the Locations tree. When you delete a folder, any locations residing in the folder will be deleted as well.


Tools > Manage Users

Opens the [Manage Users window](#) where you can add your PCC users and user groups and configure their properties. This menu option serves the same function as the **Manage Users** button  on the toolbar.

Tools > Manage Policy Groups


Opens the [Manage Policy Groups window](#) where you can create and define your policy groups. This menu option serves the same function as the **Manage Policy Groups** button  on the toolbar.

Tools > Assigned Ports

Opens the [Assigned Ports window](#) where you can view and search all ports that are currently assigned to locations. This menu option serves the same function as the **Assigned Ports** button  on the toolbar.

Tools > Enforce to Appliances

Enforces your current PCC configuration from the database to the PCC appliances (embedded virtual appliance and/or external appliances). Whenever you make changes to the configuration, you must enforce the changes to the appliances. You must also enforce any time you make changes to your device credentials (via Console). Device credentials are stored on the appliance; if the credentials are changed, you must enforce the new credentials to the appliance so it can communicate with the ports

on the device. This menu options serves the same function as the **Enforce to Appliances** button  on the toolbar.

Tools > Appliance Events

Opens the [Appliance Events window](#) where you view all event messages received from the PCC appliances (embedded virtual appliance and/or external appliances) during a specified period of time.

Help Menu

Help > Help Topics

Opens the Policy Control Console Help system.

Help > Getting Started

Displays the Getting Started help topic that provides the basic steps you must perform to begin using Policy Control Console in your network.

Help > About This Window

Displays information about the PCC main window.

Right-click Menu Options

The following menu options are only available from right-click menus in the Locations tree.

View Current Default Policies

Opens the Current Default Policies window where you can view the policies currently active for each port assigned to a location.

Activity Report

Opens the [Activity Report window](#) where you can view PCC usage and policy changes for a location. To view an activity report for a user, access this window by right-clicking a user in the [Manage Users window](#) (Tools > Manage Users).

Check Consistency

Opens the [Check Consistency window](#) where you can verify if your policies are correctly configured so that a default policy can be applied to a location.

Related Information

For information on related windows:

- [Main Window](#)
- [Toolbar](#)

Toolbar

The toolbar on the Policy Control Console main window provides easy access to certain PCC functions.



Exit

Exits the Policy Control Console application. This button serves the same function as the **File > Exit** menu option.



Manage Users

Opens the [Manage Users window](#) where you can add your PCC users and user groups and configure their properties. It also lets you specify which locations each user group is allowed to manage and the policies they are allowed to assign. This button serves the same function as the **Tools > Manage Users** menu option.



Manage Policy Groups

Opens the [Manage Policy Groups window](#) where you can create and define your policy groups. This button serves the same function as the **Tools > Manage Policy Groups** menu option.



Assigned Ports

Opens the [Assigned Ports window](#) where you can view and search all ports that are currently assigned to locations. This button serves the same function as the **Tools > Assigned Ports** menu option.



Enforce to Appliances

Enforces your current PCC configuration from the database to the PCC appliances (embedded virtual appliance and/or external appliances.) Whenever you make changes to the configuration, the Enforce button changes to orange, indicating that you must enforce the changes to the appliances. You should also enforce any time you make changes to your device credentials (via Console). Device credentials are stored on the

appliance; if the credentials are changed, you must enforce the new credentials to the appliance so it can communicate with the ports on the device. This button serves the same function as the **Tools > Enforce to Appliances** menu option.



Help

Launches the Policy Control Console Help, and displays information about the PCC main window. This button serves the same function as the **Help > About This Window** menu option.

Related Information

For information on related windows:

- [Main Window](#)
- [Menu Bar](#)

Event View

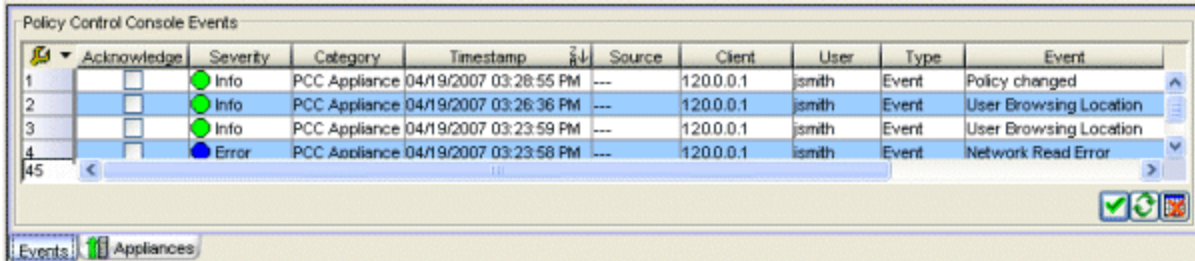
The Event View at the bottom of the Policy Control Console main window displays error and informational messages about PCC operations and also provides information about PCC appliances (embedded virtual appliance and/or external appliances). There are two tabs:

- [Events Tab](#)
- [Appliances Tab](#)

Events Tab

The Events tab displays error and informational messages about PCC system operations. The log displays the most recent 10,000 entries. The current log file is automatically archived when its size reaches 5 megabytes and a new log file is opened. Use the Event Logs view in the Suite-Wide Options window (**Tools > Options**) to configure the number of event logs to save and the number of entries to display in the table.


NOTE: If you compare an appliance event in the PCC Events tab to the same event in the [Appliance Events window](#), you may notice a difference in the timestamp. This is because the events in the PCC Events tab display the timestamp of the NetSight server, while the events in the Appliance Events window display the timestamp of the appliance. It is recommended that you run NTP (Network Time Protocol) on the PCC appliance to synchronize its clock with the NetSight Server.



The screenshot shows a window titled "Policy Control Console Events" with a table of event logs. The table has columns for Acknowledge, Severity, Category, Timestamp, Source, Client, User, Type, and Event. There are four rows of data visible, with a scrollbar on the right indicating more events are present.

	Acknowledge	Severity	Category	Timestamp	Source	Client	User	Type	Event
1	<input type="checkbox"/>	Info	PCC Appliance	04/19/2007 03:28:55 PM	---	120.0.0.1	jsmith	Event	Policy changed
2	<input type="checkbox"/>	Info	PCC Appliance	04/19/2007 03:26:36 PM	---	120.0.0.1	jsmith	Event	User Browsing Location
3	<input type="checkbox"/>	Info	PCC Appliance	04/19/2007 03:23:59 PM	---	120.0.0.1	jsmith	Event	User Browsing Location
4	<input type="checkbox"/>	Error	PCC Appliance	04/19/2007 03:23:58 PM	---	120.0.0.1	jsmith	Event	Network Read Error

Acknowledge:

This checkbox lets you acknowledge an event and also hide items that have been acknowledged. Click the checkbox to acknowledge the item and then click the Show Acknowledged Events button  to hide or show the checked items.

Severity

The event's severity.

Category

The category of event.

Timestamp

The date and time when the event occurred.

Source

The IP address of the host that was the source of the event.

Client

The name of the client host machine that triggered the event.

User

The name of the user that triggered the event.

Type

The type of information: Event.


Event

The type of event.

Information

Information about the event.

Right-click Menu Options

The Events View right-click menu lets you *Acknowledge* and *Unacknowledge* events. It also provides options and a standard set of table tools to help you find, filter, sort, print, and export information in a table and customize table settings. You can access the menu options through a right-mouse click on a column heading or anywhere in the table body, or by clicking the Table Tools  button in the upper left corner of the table (if you have the row count column displayed).

Show/Hide Acknowledged Events

This button hides or shows items in the table that have been acknowledged by a check in the Acknowledge column.

Refresh

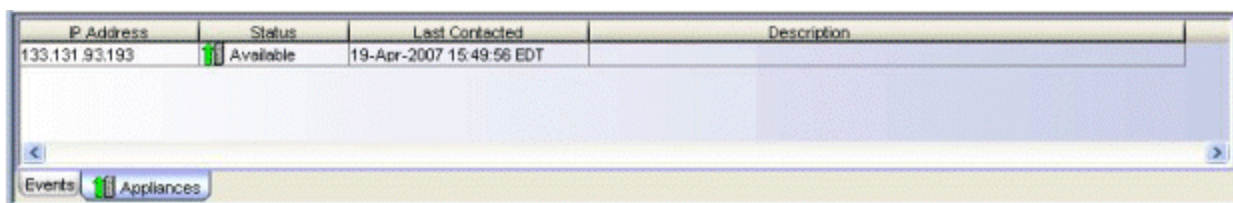
Refreshes the log.


Clear Current View

Clears entries from the current table.

Appliances Tab

This tab lists all PCC appliances (embedded virtual appliance and/or external appliances) and their last successful contact time. It displays appliance activity since the client was launched.



IP Address	Status	Last Contacted	Description
133.131.93.193	 Available	19-Apr-2007 15:49:56 EDT	

IP Address

The appliance's IP address.

Status

The appliance's status.

Last Contacted

The last time PCC successfully contacted the appliance.

Description

A description of the appliance.

Related Information

For information on related windows:

- [Appliance Events Window](#)

Manage Policy Groups Window

The Manage Policy Groups window lets you create and define your policy groups. Policy groups let you group together the network usage policies that will be set as default policy for the ports in your locations. Policy groups are assigned to user groups, and this determines which policies a user group will be allowed to set.

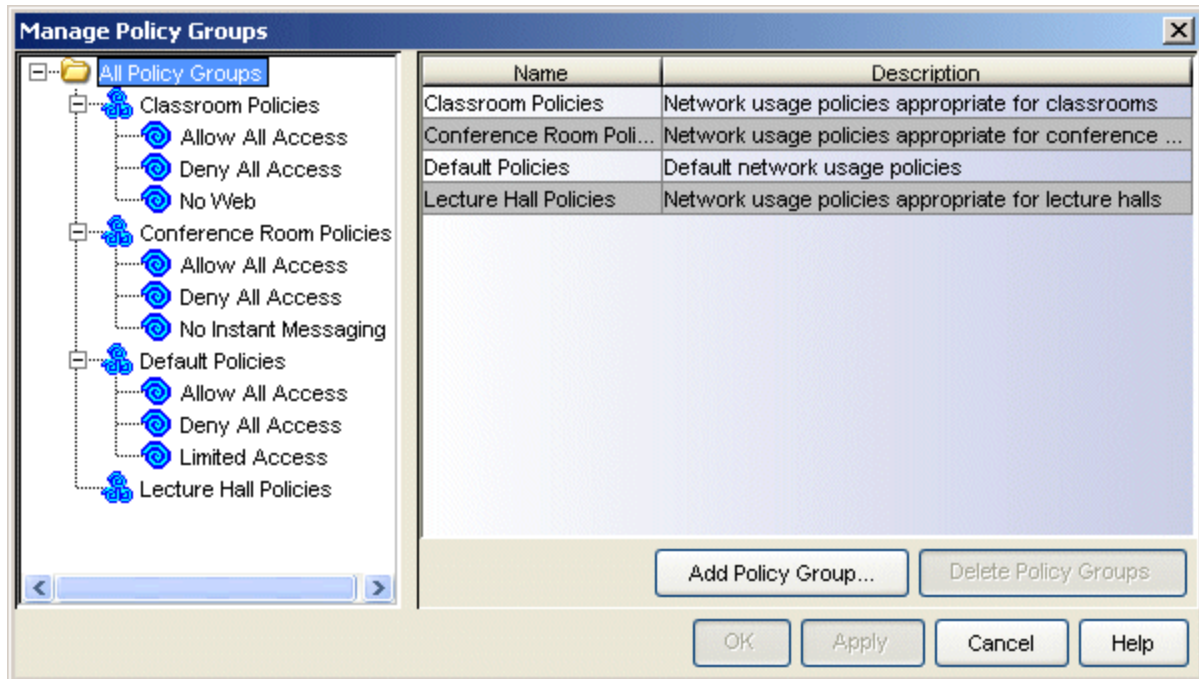
When you open the window, the left panel displays the All Policy Groups tree, which lists your current policy groups. The right panel displays a table of the policy groups and their descriptions. When you select an individual group in the tree, the right panel displays two tabs. You can use these tabs to view and change each group's configuration. When you select an individual policy in the tree, the right panel displays a tab where you can add a definition for the policy.

Information on:

- [All Policy Groups View](#)
- [Properties Tab](#)
- [Policies Tab](#)
- [Policy Properties Tab](#)

All Policy Groups View

Select the All Policy Groups folder in the left panel of the Manage Policy Groups window to view your defined policy groups. To add a new group, click the **Add Policy Group** button. To delete one or more groups, select the groups in the table and click **Delete Policy Groups**.

**Name**

The name of the policy group.

Description

A description of the policy group.

Add Policy Group Button

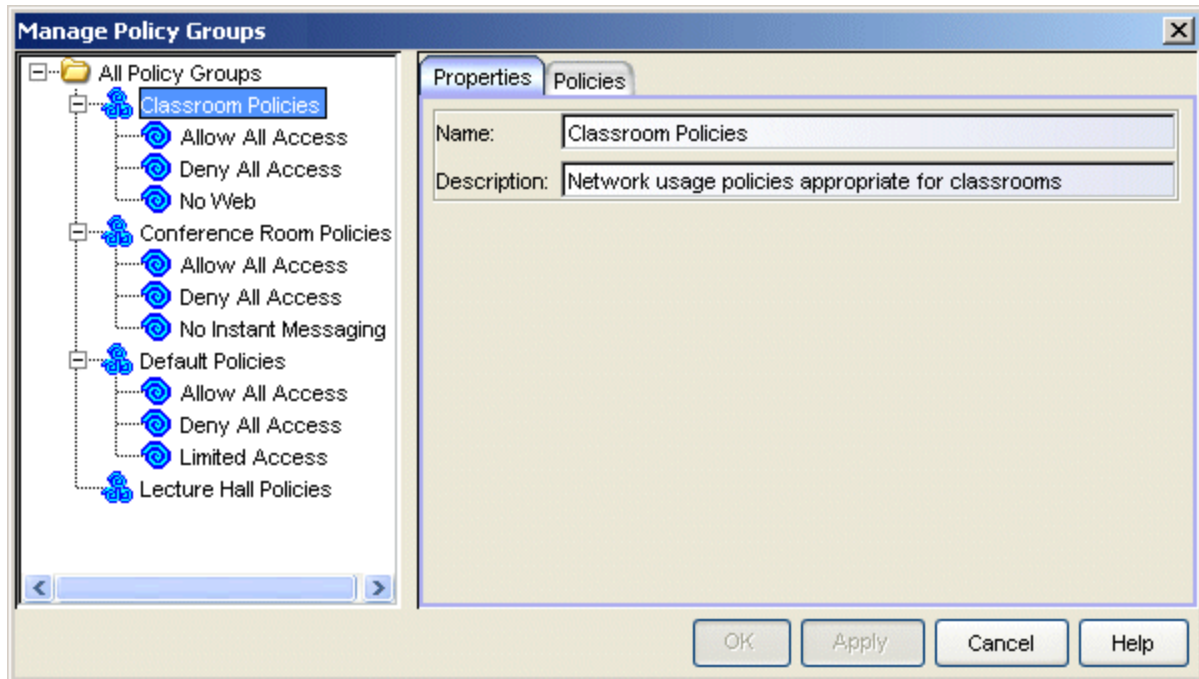
Opens the Add Policy Group window where you can create a new policy group.

Delete Policy Groups Button

Select one or more policy groups in the table and click this button to delete the groups.

Properties Tab

Select a policy group in the left panel and use the Properties tab to view and change the group's name and description.



Name

Use this field to change the name of the policy group.

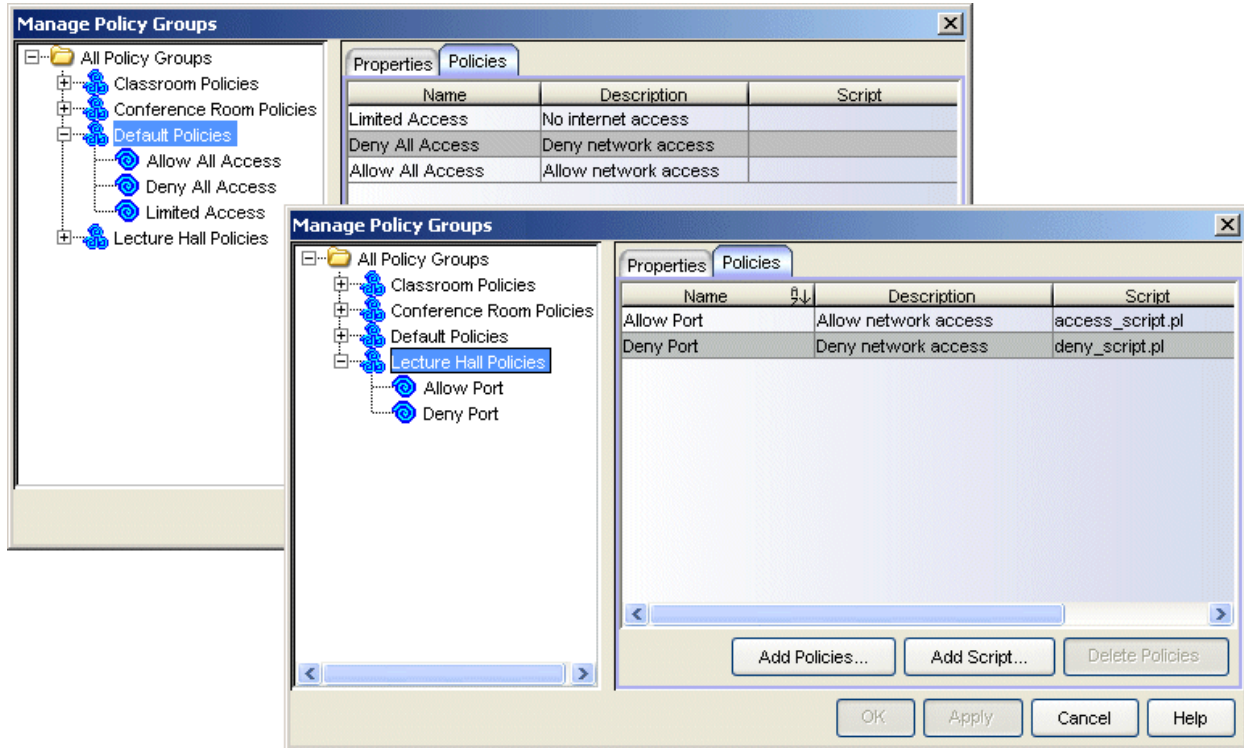
Description

Use this field to add or change a description of the policy group.

Policies Tab

Select a policy group in the left panel and use the right-panel Policies tab to view the usage policies included in that group. Usage policies can be either actual policy roles that have been created and enforced to your network devices using NetSight Policy Manager or they can be scripts that are written to set default policy on ports. This depends on whether your network access layer is composed of policy-enabled switches (use policy roles) or non policy-enabled switches (use scripts). A policy group can contain either policy roles or scripts; it cannot be a combination of the two. For more information on scripts, see [How to Use Scripts](#).

To add a new usage policy based on a policy role, click the **Add Policies** button. To add a new usage policy that is associated with a script, click the **Add Script** button. To remove one or more usage policies, select the policies in the table and click **Delete Policies**.



Name

The name of the usage policy.

Description

A description of the usage policy. You can add or edit a description of the policy by selecting a policy and using the right-panel Properties tab. This description is what is displayed on the PCC web page for PCC end user selection.

Script

If the usage policy is associated with a script, the name of the script is listed here.

Add Policies Button

Opens the Add Policies window where you select the policy roles from your network devices that you wish to add to the group.

Add Script Button

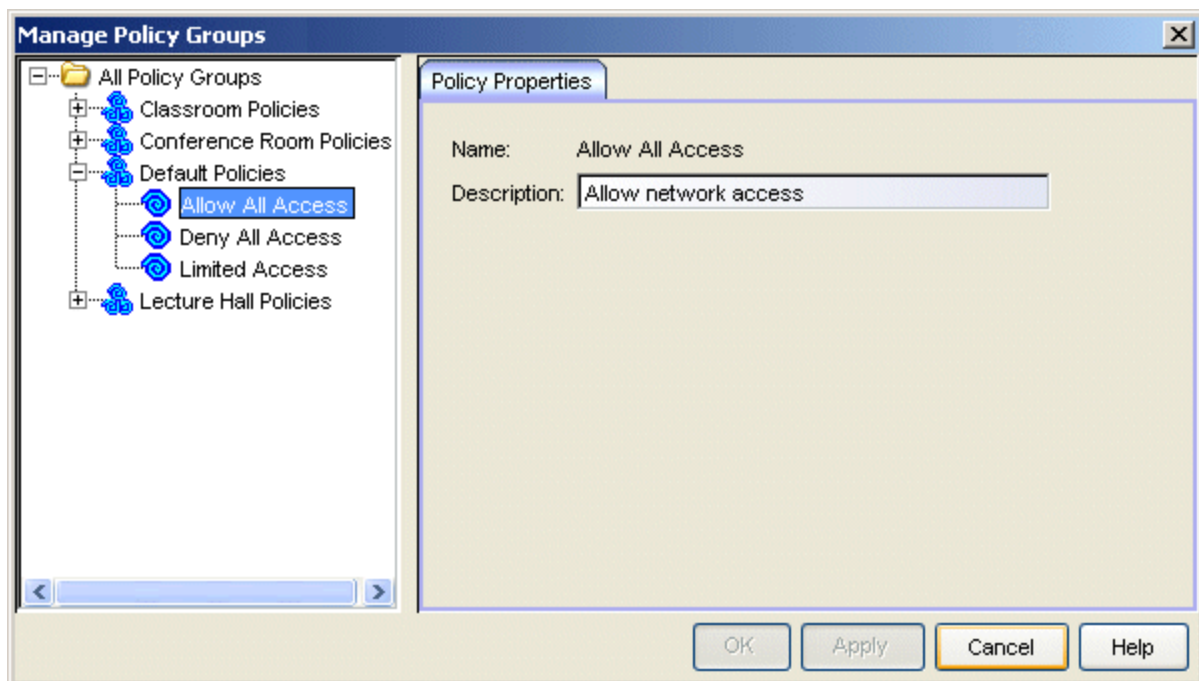
Opens the Associate a Script as a Policy window where you can select a script to associate to a usage policy. Enter a name and description for the usage policy; the description is what is displayed on the PCC web page for PCC end user selection. For more information on scripts, see [How to Use Scripts](#).

Delete Policies Button

Select one or more policies in the table and click this button to delete the policies.

Policy Properties Tab

Select a policy in the left panel and use the right-panel Policy Properties tab to add or change a description of the policy. The policy description is displayed on the PCC web page in the section where PCC end users select a policy to set.



Name


The name of the policy.

Description

Use this field to enter or change the description of the policy. The description is what will be displayed on the PCC web page for PCC end user selection.

OK

Saves your changes to the PCC database and closes the window. Be sure to enforce any changes to the PCC appliances using the **Enforce to**

Appliances button  on the PCC toolbar.

Apply

Saves your changes to the PCC database and leaves the window open.

Cancel

Closes the window without saving any changes.

Related Information

For information on related windows:

- [Manage Users Window](#)

Manage Users Window

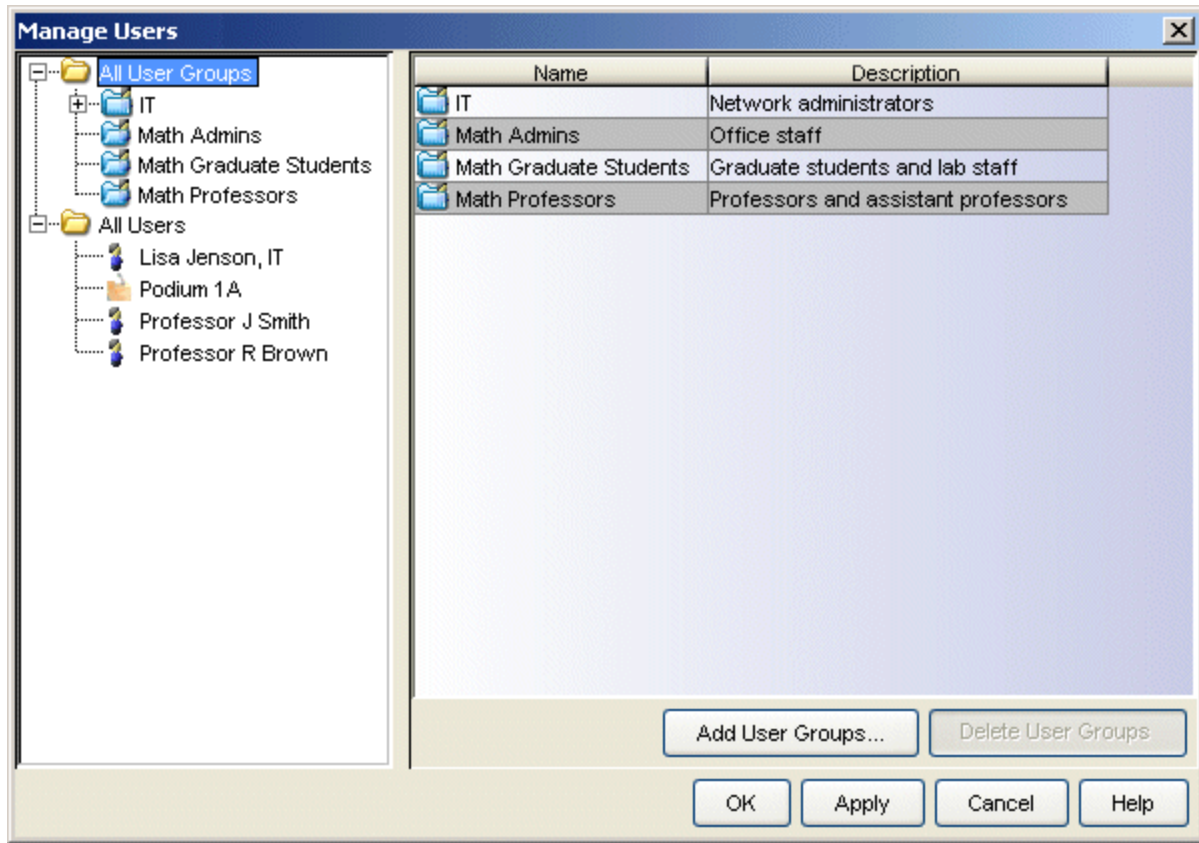
The Manage Users window lets you add your PCC users and user groups and configure their properties. It also lets you specify which locations each user group is allowed to manage and the policies they are allowed to assign. When you open the window, the left panel displays the Manage Users tree, which lists your current PCC user groups and users. The right panel displays detailed information about the user group or user selected in the tree. When you select an individual user group in the tree, the right panel displays four tabs. You can use these tabs to view and change each user group's configuration.

Information on:

- [All User Groups View](#)
 - [Properties Tab](#)
 - [Allowed Locations Tab](#)
 - [Allowed Policy Groups Tab](#)
 - [Assigned Users Tab](#)
 - [Mapped Authorization Groups Tab](#)
- [All Users View](#)
 - [Properties Tab](#)

All User Groups View

Select the All Users Groups folder in the left panel of the Manage Users window to view a list of your user groups and their descriptions. To add a new user group, click the **Add User Groups** button. To delete one or more user groups, select the user group(s) in the table and click **Delete User Groups**.



Name

The name of the user group.

Description

The description of the user group that was added when the group was created. You can change the name and description of the group in the [User Group Properties tab](#).

Add User Groups Button

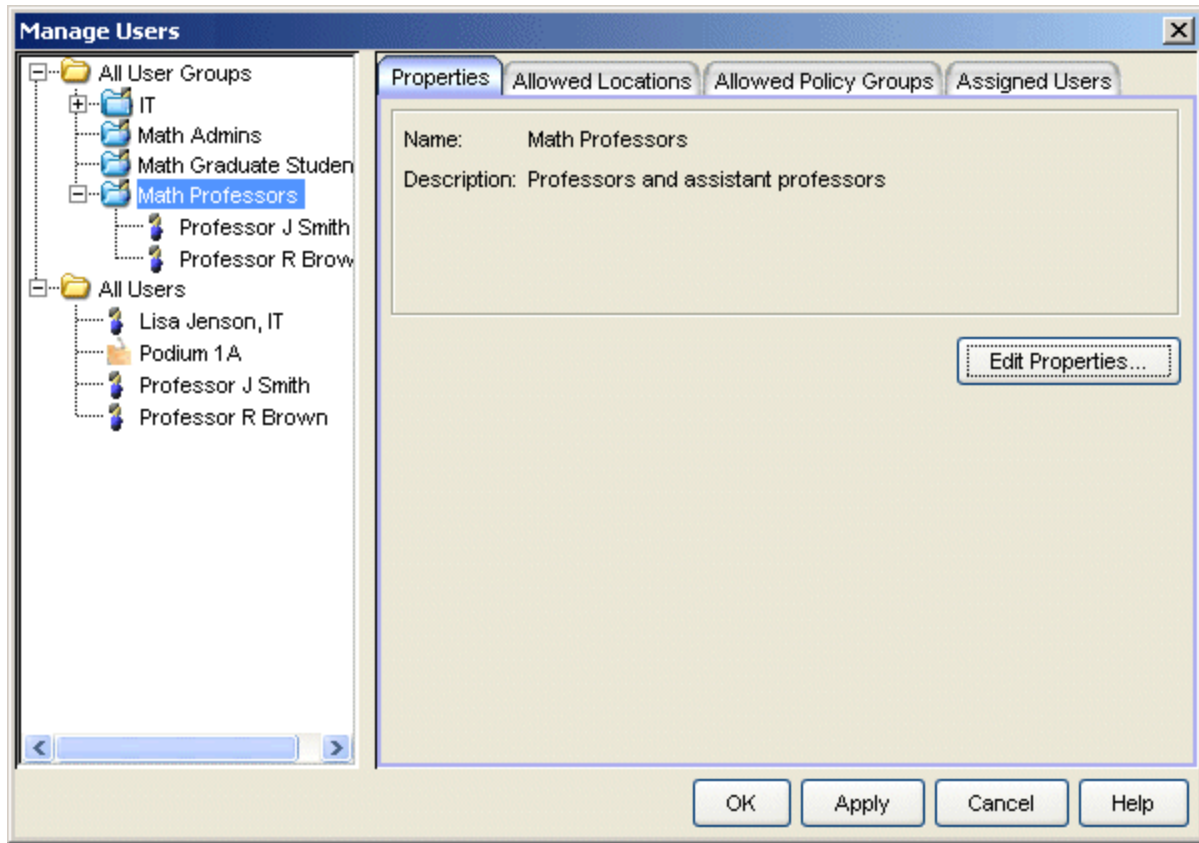
Opens the Add User Group window, where you can add a user group name and description.

Delete User Groups Button

Select one or more user groups in the table and click this button to delete the groups.

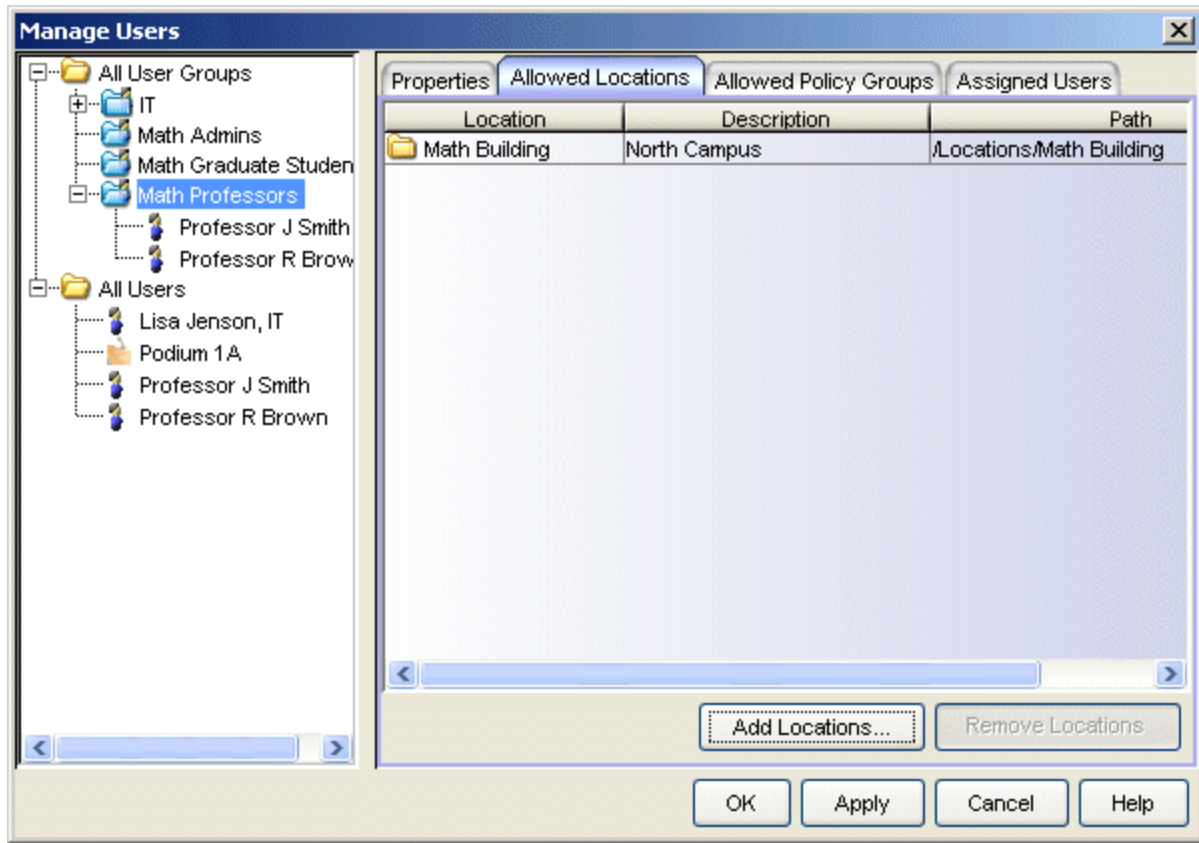
Properties Tab - User Group

Select a math group in the tree and use the Properties tab to view and change the group's name and description by selecting the Edit Properties button.



Allowed Locations Tab - User Group

Select a user group in the tree and use the Allowed Locations tab to view the locations where the user group is allowed to configure default policy. To add a new location, click the **Add Locations** button. To remove one or more locations, select the location(s) in the table and click **Remove Locations**.



Location

The name of the allowed location.

Description

A description of the allowed location.

Path

The path in the Locations tree to the allowed location.

Add Locations Button

Opens the Add Locations window where you can select locations to add to the user's allowed locations.

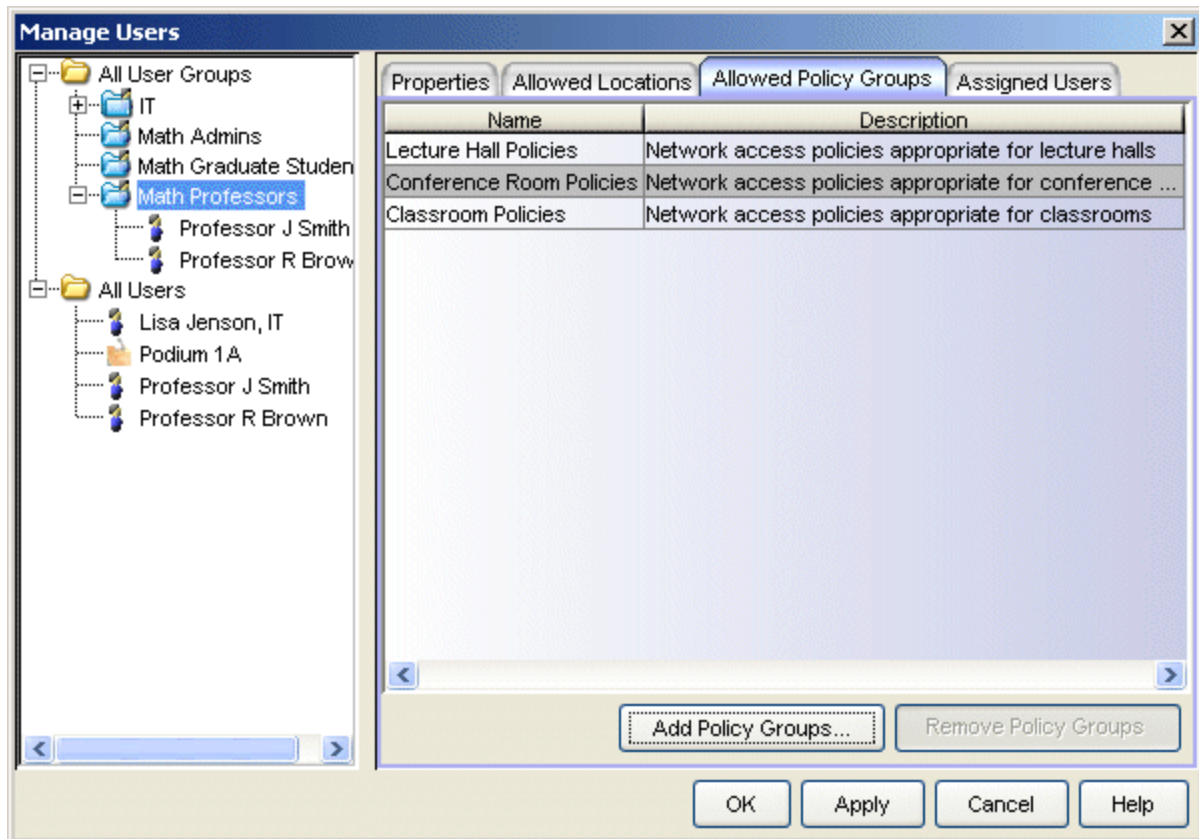
Remove Locations Button

Select one or more locations in the table and click this button to remove the locations.

Allowed Policy Groups Tab - User Group

Select a user group in the tree and use the Allowed Policy Groups tab to view the policy groups from which the user group is allowed to assign a policy. To

add a new policy group, click the **Add Policy Groups** button. To remove one or more policy group, select the group(s) in the table and click **Remove Policy Groups**.



Name

The name of the allowed policy group.

Description

A description of the allowed policy group.

Add Policy Groups Button

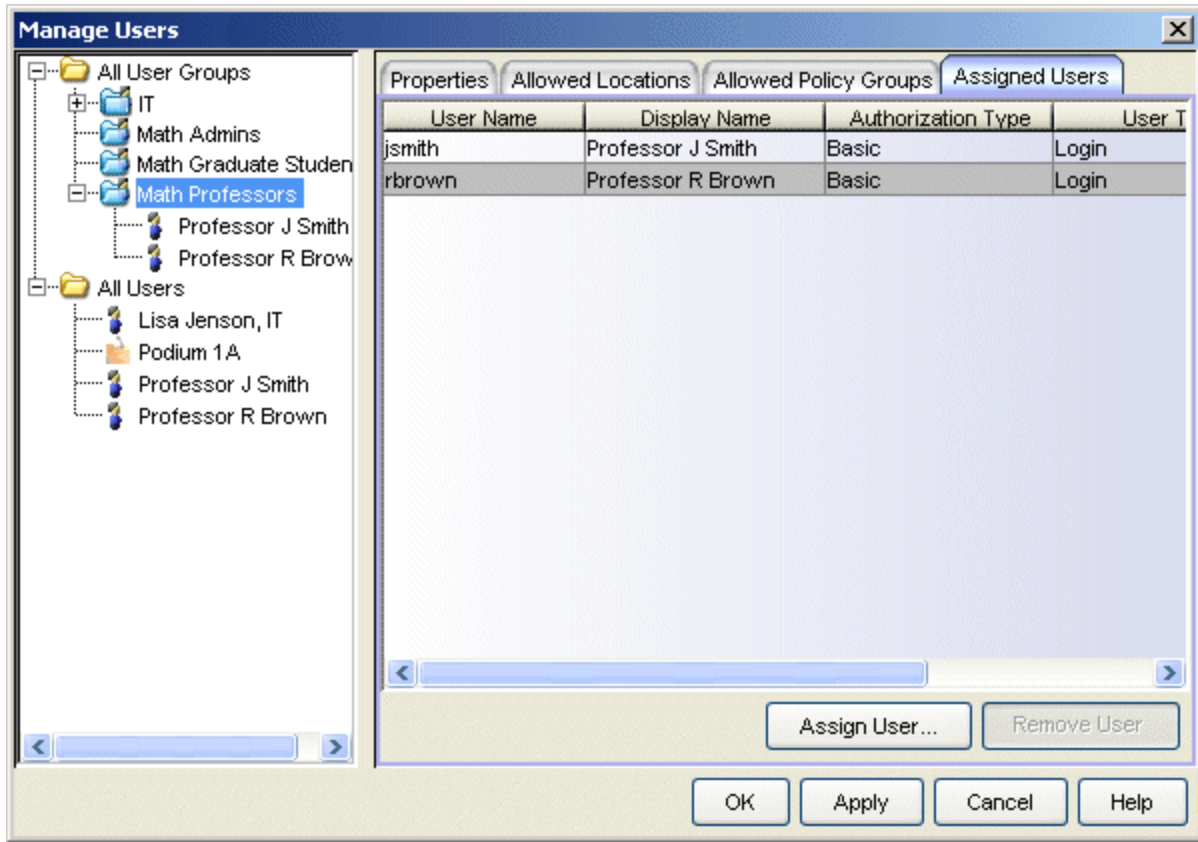
Opens the [Assign Policy Groups window](#) where you can select policy groups to add to the user group's allowed groups.

Remove Policy Groups Button

Select one or more policy groups in the table and click this button to remove the groups.

Assigned Users Tab - User Group

Select a user group in the tree and use the Assigned Users tab to view the users that have been assigned to the user group. To add a new user, click the **Add Users** button. To delete one or more users, select the user(s) in the table and click **Remove Users**.



User Name

The name the user will use to log in to the PCC web page.

Display Name

The user's name that will be displayed on the PCC web page after they log in.

Authorization Type

A login user can be configured with either of the following two authorization types; static IP users are always configured with Basic authorization.

- Admin - Provides access to the PCC web page to:
 - define and schedule policy for allowed locations.
 - configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
 - view a PCC activity log.
- Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - schedule policy for allowed locations (if access to the scheduling functionality was granted).

User Type

A user can be created as one of two types:

- Login - The user authenticates to access the PCC web page and set policies for their allowed locations.
- Static IP - A "podium" computer provides open access to the PCC web page to set policies for allowed locations (usually for that location only).

PCC Login

Indicates whether a PCC Login password has been configured for the user: true or false. If a PCC Login password has not been configured, then LDAP must be configured.

Can Schedule

Indicates whether the PCC user has been granted access to the PCC web page scheduling functionality: true or false.

Assign Users Button

Opens the [Assign Users window](#), where you can select a user to add to the user group.

Remove Users Button

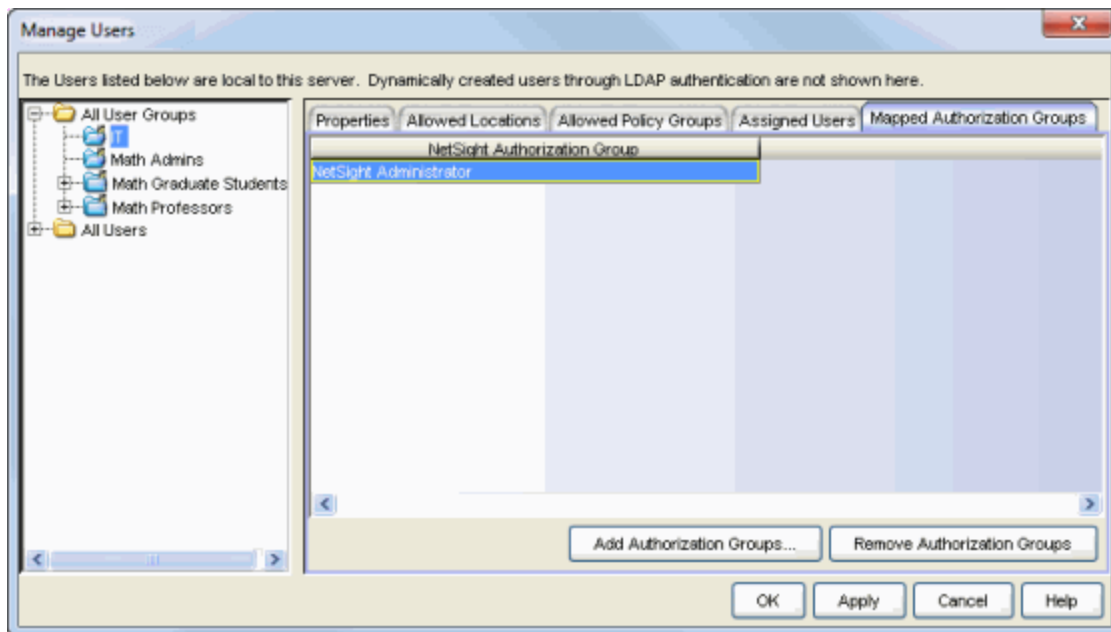
Select one or more users in the table and click this button to delete the user.

Mapped Authorization Groups Tab - User Group

This tab is used in networks configured to allow [LDAP authentication](#) to the PCC web page. PCC users who authenticate to the PCC web page using LDAP authentication are assigned a NetSight authorization group. The authorization group is mapped to a PCC user group using this tab, and the user is allowed

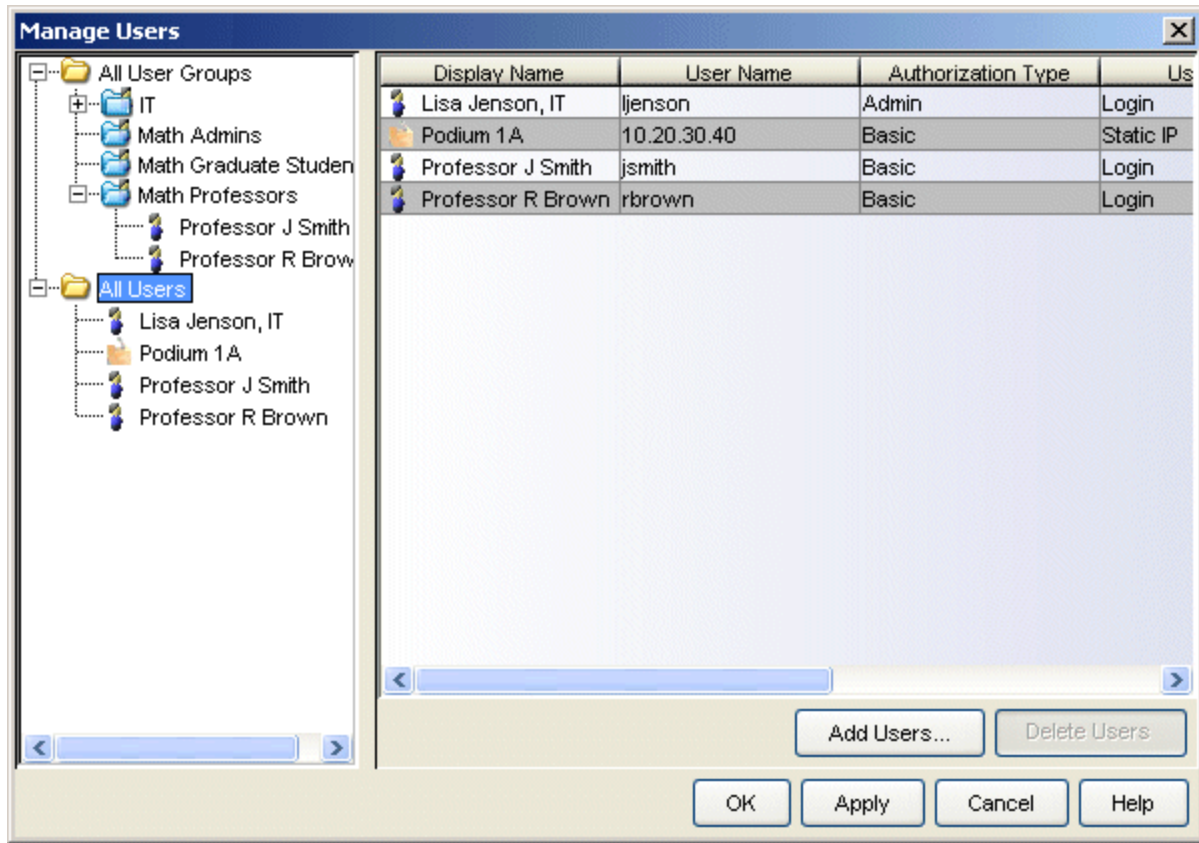
access to the PCC web application according to the locations and policy groups allowed by the user group.

Select a user group in the tree and use this tab to view the NetSight authorization groups mapped to the user group. To add a new authorization group, click the **Add Authorization Groups** button. To remove one or more authorization groups, select the group(s) in the table and click **Remove Authorization Groups**.



All Users View

Select the All Users folder in the left panel of the Manage Users window to view a table of settings for all your PCC users. To add a new user, click the **Add Users** button. To delete one or more users, select the user(s) in the table and click **Delete Users**.



Display Name

The user's name that will be displayed on the PCC web page after they log in.

User Name

The name the user will use to log in to the PCC web page.

Authorization Type

A login user can be configured with either of the following two authorization types; static IP users are always configured with Basic authorization.

- Admin - Provides access to the PCC web page to:
 - define and schedule policy for allowed locations.
 - configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
 - view a PCC activity log.

- Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - schedule policy for allowed locations (if access to the scheduling functionality was granted).

User Type

A user can be created as one of two types:

- Login - The user authenticates to access the PCC web page and set policies for their allowed locations.
- Static IP - A "podium" computer provides open access to the PCC web page to set policies for allowed locations (usually for that location only).

PCC Login

Indicates whether a PCC Login password has been configured for the user: true or false. If a PCC Login password has not been configured, then LDAP must be configured.

Can Schedule

Indicates whether the PCC user has been granted access to the PCC web page scheduling functionality: true or false.

Add Users Button

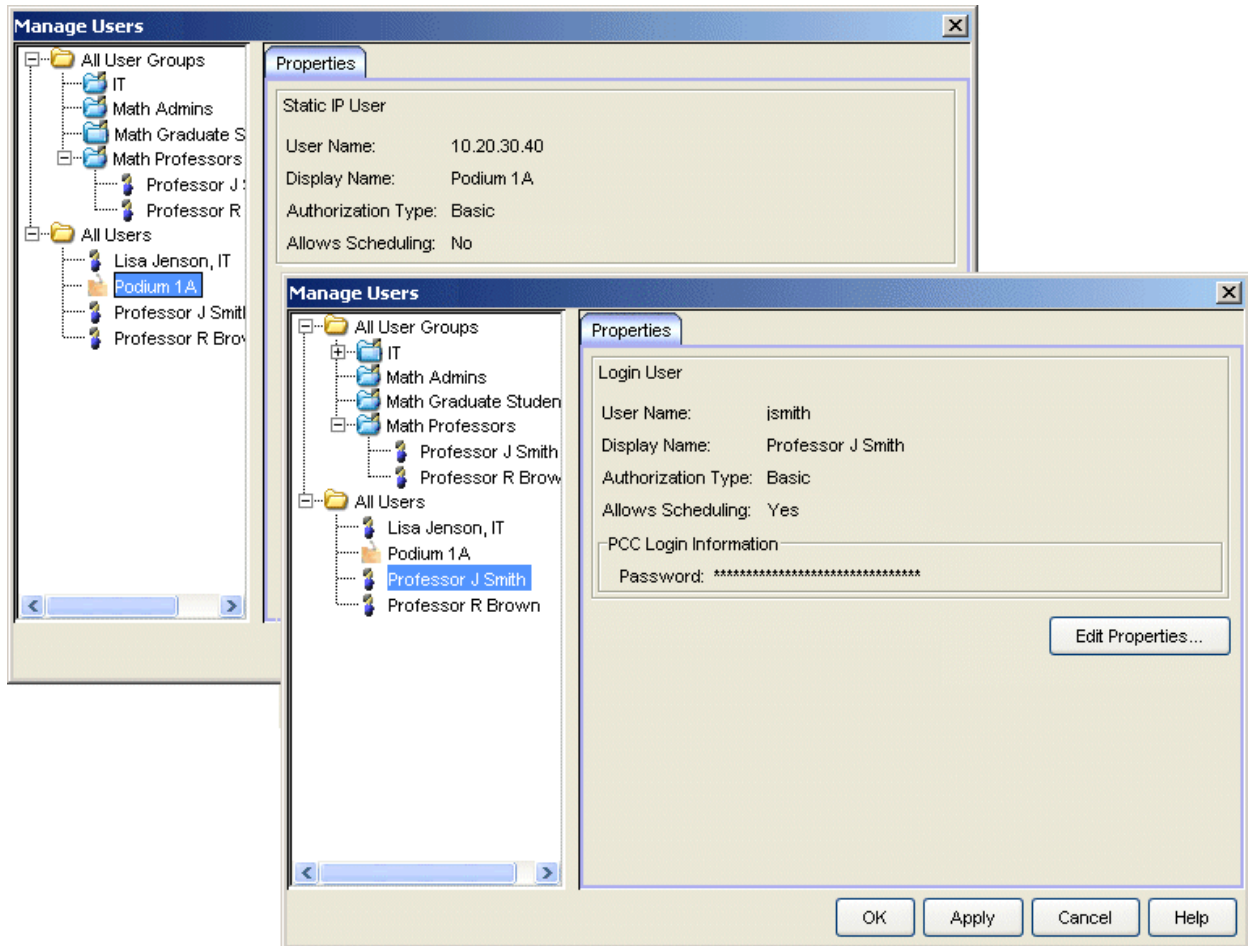
Opens the [Add User window](#), where you can add and configure a PCC user.

Delete Users Button

Select one or more users in the table and click this button to delete the users.

Properties Tab - User

Select an individual user in the left panel of the Manage Users window and use the Properties tab to view and change the user's properties. The fields in this tab vary depending on whether the user is a Login User or Static IP User. Use the Edit Properties button to open the [Edit User window](#) and change the properties.



User Name

For login users, the name the user will use to log in to the PCC web page.
For static IP users, the IP address of the user. This field is not editable.

Display Name

The user's name that will be displayed on the PCC web page, after they log in.

Authorization Type

A login user can be configured with either of the following two authorization types; static IP users are always configured with Basic authorization.

- Admin - Provides access to the PCC web page to:
 - define and schedule policy for allowed locations.

- configure settings for PCC appliance communication with network devices and view NetSight Server communication status.
- view a PCC activity log.
- Basic - Provides access to the PCC web page to:
 - define policy for allowed locations.
 - schedule policy for allowed locations (if access to the scheduling functionality was granted).

Allows Scheduling

Indicates whether the PCC user has been granted access to the PCC web page scheduling functionality.

PCC Login Information


If PCC Login is required for the login user, this field displays the password.

Edit Properties Button

Opens the [Edit User window](#) where you can change the user properties.

OK

Saves your changes to the PCC database and closes the window. Be sure to enforce any changes to the PCC appliances using the **Enforce to**

Appliances button  on the PCC toolbar.

Apply

Saves your changes to the PCC database and leaves the window open.

Cancel

Closes the window without saving any changes.

Related Information

For information on related windows:

- [Add User Window](#)
- [Assign Policy Groups Window](#)
- [Assign Users Window](#)

Scheduling Details

Use this web page to add or edit entries in the [PCC Scheduling web page](#).

Scheduling - Add Entry

Details

Change Location

Location:

Event Title:

Policies:

Start Date/Time:

End Date/Time:

comments:

Revert to Locations Default Policy (if configured)

Revert to Policy:

Enable Recurrence

Enter the type of recurrence:

Repeat Every Week(s)

Mon Tue Wed Thu Fri Sat Sun

Enter the range of recurrence:

Forever

Until

Count

Details

Use these fields to add or edit an entry for the Scheduling web page.

Location

If the user is allowed multiple locations, use the Change Location drop-down arrow to open the Locations Tree and select the desired location. Only the user's allowed locations are displayed in the tree. If the user has only one allowed location, the Locations Tree is not shown at all.

Event Title

Enter a title for the scheduled event.

Policies

Use the drop-down list to select the desired policy to schedule.

Start and End Date/Time

Select the desired start and end date and time. The time is entered in 24-hour notation.

Comments

Use this field to enter any comments you want to add about the event. In the calendar, comments are displayed when you hold your cursor over the event.

Revert to Locations Default Policy

Select this option if you want the location's policy to revert to its default policy at the end of the scheduled event. This option is valid only if a default policy has been configured for the location in the location's [Properties tab](#).

Revert to Policy

Select this option if you want to specify the policy the location will revert to at the end of the scheduled event. Use the drop-down list to select the desired policy.

Enable Recurrence

Select the Enable Recurrence checkbox and then use the fields below to configure recurring schedule entries. On the scheduling web page, recurring events will be highlighted in green until they have occurred, and then they will be displayed as red.

Type of Recurrence

Use the drop-down list to select the desired recurrence interval:

- Day(s) - Configure the entry to occur on a daily basis. The first day is specified by the Start Date and then repeats every n days or every

week day, based on your selection.

- Weeks(s) - Configure the entry to occur on a weekly basis. The first day is specified by the Start Date and then repeats every n weeks for the days selected in the checkboxes.
- Month(s) - Configure the entry to occur on a monthly basis. The first day is specified by the Start Date and then repeats for the specified day each month.

Range of Recurrence

Enter a recurrence range that will be applied to all recurring schedule entries:

- Forever - The scheduled entries will repeat without any end date.
- Until - The scheduled entries will repeat until the date specified.
- Count - The scheduled entries will repeat for the specified number of times.

Related Information

For information on related windows:

- [How to Use the PCC Web Page - Scheduling](#)