

[Help Top](#) | [Return to Policy Manager](#) »

## Nicira Policy Manager Help (beta)

### Contents:

- [Policy Manager Overview](#)
  - [Application Orientation](#)
  - [Quick Setup](#)
  - [Monitors](#)
- [Principal Management](#)
  - [Managing Switches](#)
  - [Hosts](#)
  - [Users](#)
  - [Managing Locations](#)
- [Defining Network Policies](#)
  - [Overview](#)
  - [Basic Policy Editing](#)
  - [Using the Default Policy](#)
  - [Policy Rule Language](#)
- [System Configuration](#)
  - [Web Interface Settings](#)
  - [Configuring DHCP](#)
  - [Configuring the Captive Web Portal](#)
  - [Configuring NAT](#)
  - [Configuring an External Directory Server](#)
- [Switch User Interface](#)
  - [Information Screen](#)
  - [Switch Main Menu](#)
  - [Switch Configuration](#)

**Next to**

[Policy Manager Overview](#)

[Help Top](#) | [Return to Policy Manager](#) »

contact: [support@nicira.com](mailto:support@nicira.com)

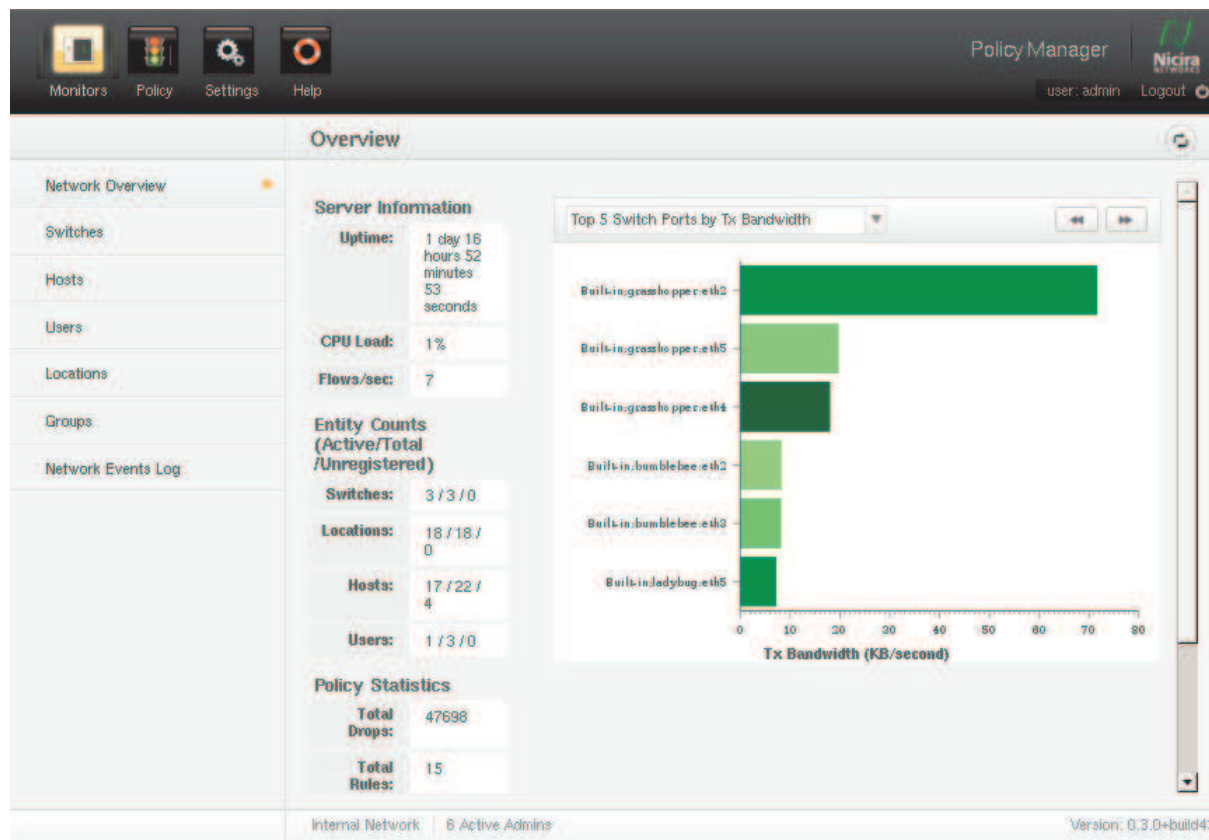
© Copyright 2010

[Help Top](#) | [Return to Policy Manager](#) »

## Policy Manager Overview

### Application Orientation

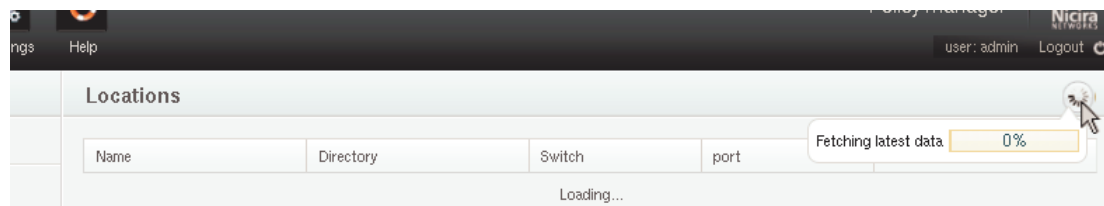
The Policy Manager application is a graphical user interface for viewing and controlling all network policy and configuration state. An example screen shot of the policy manager is shown below.



Functions in Policy Manager are grouped into high-level categories which are available through icons in the top pane. As shown in the example screen shot, these include *Monitors*, *Policy*, *Settings*, and *Help*. Each of these groupings includes multiple pages that can be reached from links displayed in the left side-bar.

Briefly, the *Monitors* section contains a collection of pages for most day-to-day management tasks such as reviewing the system status and managing network principals. The *Policy* section provides a comprehensive interface to the network security policy. The *Settings* section is used to configure the Policy Manager for a particular network setting.

All pages in the Policy Manager are bookmarkable allowing for quick access to any page within the system. Most pages update automatically to keep displayed information consistent with the internal state of the Policy Manager. In addition, all pages have a progress indicator which indicates whether a page is loading, and on mouse-over the progress until the loading is complete (shown below).



The bottom bar of the application shows the network name (configurable from the *Settings* section), the number of users logged on to the application, and the application version.

#### Table O

Policy Ma  
Overview

- Applica  
Orienti
- Quick !
- Monito
- Netv
- Print  
Man  
Page
- Netv

#### Previous:

Nicira Po  
Help (bet

#### Next to

Principal

## Quick Setup

The following steps are necessary for a basic configuration of the Policy Manager.

1. At least one switch must be registered at the Policy Manager. Configuring a switch to work with the Policy Manager is described in [Managing Switches](#).
2. By default, the Policy Manager is configured with a self-signed certificate which is used both for the management interface and the captive web portal. This should be replaced with a valid root-signed cert (see [Web Interface Settings](#)).
3. Hosts that are required for core network operation (such as DNS servers or directory servers) should be registered with the Policy Manager and added to correct host groups. This allows for default connectivity required for host and user authentication. This is described in more detail in [Using the Default Policy](#).
4. To authenticate users over HTTP, the captive web portal must be configured with the domain name of the Policy Controller (see [Configuring the Captive Web Portal](#)).
5. Finally, hosts can be registered manually or as they are discovered and placed into groups for the policy. Managing hosts is described in [Hosts](#) and modifying the network policy in [Defining Network Policies](#).

## Monitors

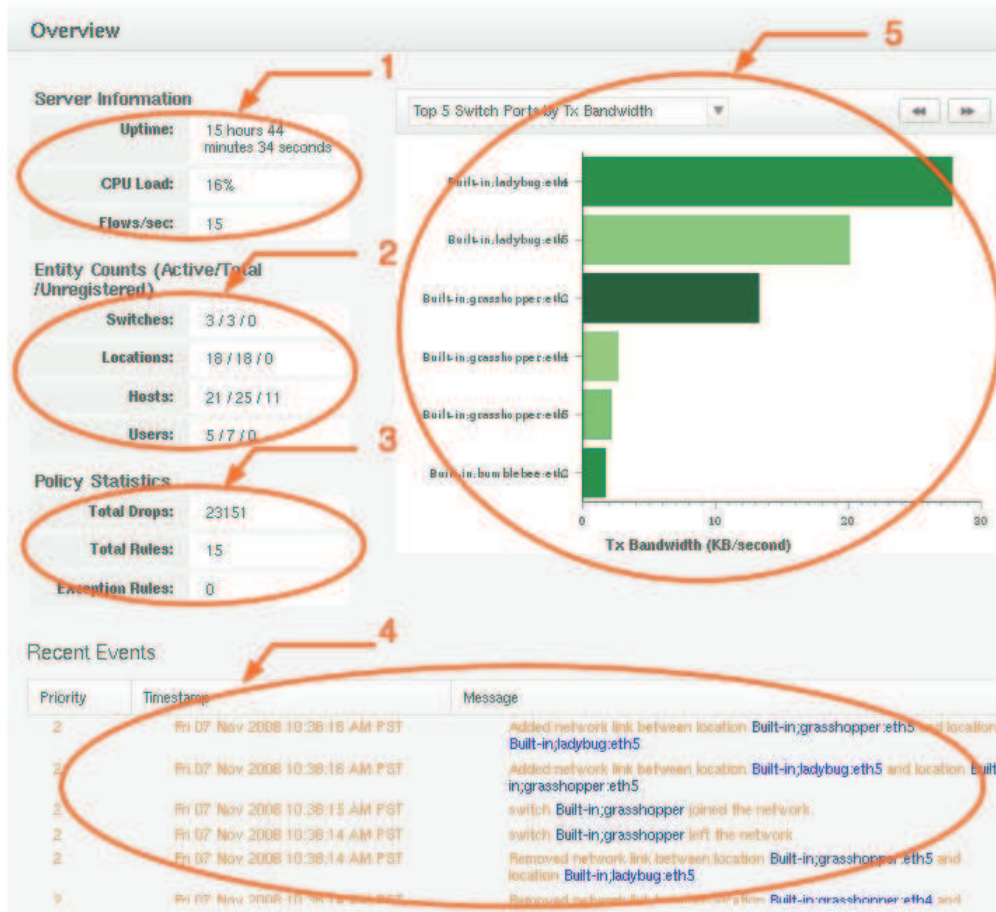
The Monitors section of the Policy Manager application contains the pages where most day-to-day operation of the system takes place. To reach the Monitors section, click on the *Monitors* icon in the navigation bar at the top of the application:



Each of the pages in the *Monitors* subsection are described below.

## Network Overview

The Network Overview page is the default page of the Policy Manager application and provides a summary view of the network state. The major sections are describe below.



1. The *Server Information* fields contain information regarding the Policy Manager server itself. This includes the uptime, CPU load and the number of flows per second that are being processed network-wide.
2. The *Entity Counts* provide an overview of all principals known to the policy manager. For each of the principal types (switch, locations, hosts, and users) the following information is shown:
  - The number of entities currently active on the network.
  - The total number of entities (active or inactive) registered at the Policy Manager.
  - The number of entities that have been observed on the network for which there is no registration information.
3. *Policy Statistics* provide general information regarding the configured network policy. This includes the total number of network flows which have been denied by the policy and the number of rules of the active policy. The number of configured exception rules is also shown (exception rules are described in [Defining Network Policies](#)).
4. *Recent Events* show a list of recent network events. This is only includes events of priority greater than 2 from the Network Event Log (described below in [Network Event Log](#)).
5. The *Heavy-Hitters Graph* contain various load graphs showing the most active network components. Clicking on the left and right double arrows will cycle through the set of available graphs.

### Principal Management Pages

The *Switches*, *Hosts*, *Users*, *Locations*, and *Groups* pages in the *Management* section all deal with viewing and managing principals. These functions merit their own section and are described in detail in [Principal Management](#).

### Network Event Log

The Network Event Log is a running list of network-wide events which may be used for monitoring and debugging network behavior. The events are prioritized from 1–5 where lower numbers are considered to have higher priority. In general, the network event log messages only include the high-level names of principals. Each principal name is a link to the management page for the principal which contains detailed information regarding that principal.

[Help Top](#) | [Return to Policy Manager](#) »

contact: [support@nicira.com](mailto:support@nicira.com)

© Copyright 201

[Help Top](#) | [Return to Policy Manager](#) »

## Principal Management

A primary function of the Policy Manager application is to manage networks principals. A *network principal* is any named entity on the network ([Switches](#) and [Locations](#)) and network clients ([Hosts](#) and [Users](#)).

The policy manager use principals names (as well as conventional identifiers such as IP and MAC addresses) to enforce network policy and provide network visibility.

The policy manager supports the following principal types:

- [Switch](#): A network switch.
- [Location](#): A physical port on a switch. Location names are unique throughout the network.
- [Host](#): An addressable device that sends and receives network traffic. Hosts may have multiple interfaces and addresses.
- [User](#): An account used to identify an authenticated person on the network.

Information associated with principals (such as authorization credentials) are stored in *directories*. The Policy Manager can be configured to work with standard authentication stores such as LDAP or Active Directory. It also has an internal directory called “Built-in”.

It is possible to configure the Policy Manager to use multiple directories. For example, *user* accounts may be both handled by an external authentication store (e.g., LDAP) as well as the “Built-in” directory. In such cases, it is necessary to distinguish which directory a name is from. This is done by prepending the directory name to the principal name. For example, if both the LDAP directory and the “Built-in” directory have the user *John*, they would be represented as *LDAP\_directory\_name:John* and *Built-in:John*, respectively.

## Managing Switches

### Viewing Registered and Discovered Switches

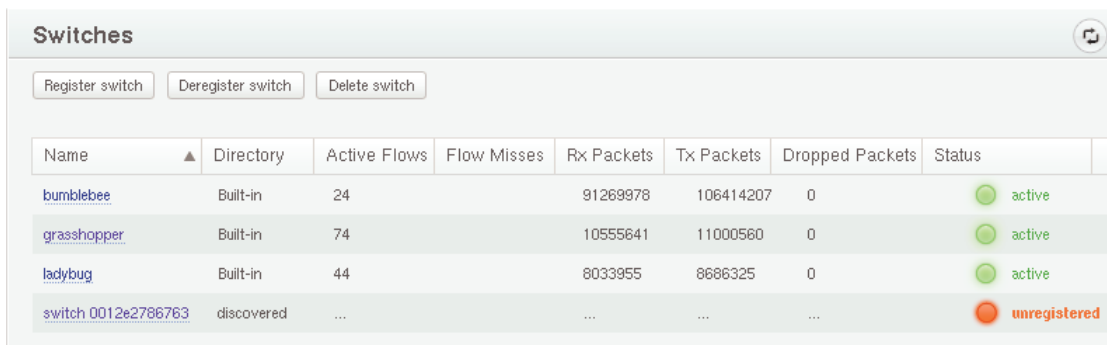
In the *Monitors* tab, click on the *Switches* link on the sidebar to navigate to the switch overview page. The switch overview page displays all registered and discovered switches on the network.

### Registering Switches

Switches configured with the Policy Manager’s IP address should automatically attempt to connect to the Policy Manager. In order for the switch to join the network, it must be registered.

To register a new switch, follow these steps:

1. In the *Monitors* tab, click on the *Switches* link the sidebar.
2. If configured correctly, the new switch should appear in the list of switches as “unregistered”.



Name	Directory	Active Flows	Flow Misses	Rx Packets	Tx Packets	Dropped Packets	Status
<a href="#">bumblebee</a>	Built-in	24		91269978	106414207	0	active
<a href="#">grasshopper</a>	Built-in	74		10555641	11000560	0	active
<a href="#">ladybug</a>	Built-in	44		8033955	8686325	0	active
<a href="#">switch 0012e2786763</a>	discovered	...		...	...	...	unregistered

3. Select the switch by clicking on it (the switch line should be highlighted).
4. Click the *Register Switch* button.
5. In the resulting pop-up, select the “Built-in” directory and enter a name for the switch.

#### Table O

#### Principal

- [Manag](#)
  - [View and Swit](#)
  - [Regi Swit](#)
  - [Rese](#)
- [Hosts](#)
  - [View and Host](#)
- [Regi](#)
  - [Re Di](#)
  - [Re Ne](#)
- [Upd: Bind](#)
- [Man: Grou](#)
- [Users](#)
  - [View and](#)
  - [Regi](#)
  - [Upd: Pass](#)
- [Manag](#)

#### Previou:

[Policy Me Overview](#)

#### Next to

[Defining Policies](#)



6. The switch should now be allowed on the network and managed by the Policy Manager.

## Resetting a Switch

To reboot a switch, click the **Reset Switch** button on the switch details page.

## Hosts

Hosts identify network devices that send and receive network traffic. Policy for host principals is enforced regardless of the host's location or network addresses.

### Viewing Registered and Discovered Hosts

In the *Monitors* tab, click on the *Hosts* link on the sidebar to navigate to the Hosts overview page. This page displays all registered and discovered hosts on the network.

### Registering Hosts

#### Registering a Discovered Host

If an unregistered host is active on the network, the host will appear in the Hosts overview page as a member of the "discovered" directory. The discovered host name will be "host <MAC address>" if the host is connected to the switch L2. Alternately, the discovered hostname will be "host <IP address>" if there is a router or other L3 device between the host and the switch.

To register a host that has been discovered, follow these steps:

1. Click on the host name from the Hosts overview page to navigate to the host details page.
2. Change the directory name from "discovered" to "Built-in". To edit the directory name, click on the edit indicator that appears when hovering over the name.
3. The host is now registered with the static bindings that were detected when the host was seen. To add or modify the host's static bindings, follow the steps outlined below.

#### Registering a New Host

To manually register a new host, follow these steps:

1. From the Hosts overview page, click the *Add Host* button.
2. Select the "Built-in" directory, and enter a name for the host.
3. The host is now registered, however no bindings are set. To add static bindings to the host, follow the steps below.

### Updating Host Bindings

Hosts have *static* and *active* binding attributes. Active bindings represent the address(es) and location(s) the host is currently using on the network. Static bindings tell NOX how to identify name a host when it becomes active on the network. If a host on the network uses a MAC and IP address that does not match a static binding, that host will be placed in a special "discovered" directory that contains all unregistered principals.

It is important to note that hosts are identified by addresses available to the Policy Manager. If they reach a switch controlled by the Policy Manager from behind an L3 router, then they must have at least one IP address to be identified. Hosts that connect directly to Policy Manager controlled switches only need to have their MAC addresses registered.

To modify static bindings for a host, follow these steps:

1. Click on the host name from the Hosts overview page to navigate to the host details page.
2. Locate the Static Bindings section of the host details page to view all static bindings currently registered for the host.
3. A new static binding may be added by clicking the *Add New Binding* button.

1. To set a MAC or IP address for the new binding, double click on the associated field.
4. Static bindings may be removed by selecting the binding to remove (it will be highlighted when selected) and clicking the *Delete Selected* button.

## Managing Host Groups

Host groups can be accessed in the *Monitors* section under the *Groups* and then *Host Groups* links. The default system policy uses a number of host groups which are created at system install time. These include a number of standard host types and roles.

During initial configuration, the administrator should add relevant servers to the appropriate groups. The type of host expected in each group is described below:

1. **DHCP Servers** Networks which use DHCP for allocating IP addresses should add all DHCP servers to this group. If the Policy Manager itself is being used for DHCP it is not necessary to add it to this group.
2. **DNS Servers** All DNS servers.
3. **Controllers** All Policy Manager servers should be registered in this group.
4. **LDAP Servers** Hosts providing directory service needed for authentication (e.g., LDAP or AD servers) must be added to this group.
5. **User Auth Portals** By default the captive web portal is run on the controller in which case there is no need to add hosts to this group. However, if a remote captive portal is used it must be added.
6. **Unrestricted Servers** Any additional host that requires unrestricted connectivity either for principal authentication or otherwise should be added to this group.

Adding and removing hosts from groups can be done by clicking on the group link and using the *Add Member* and *Remove Member* buttons.

## Users

User principals identify a user account on the network. When a user principal authenticates to the network from a host, network access policies for the host are updated to reflect any policies defined for the user.

### Viewing Registered and Active Users

In the *Monitors* tab, click on the *Users* link on the sidebar to navigate to the user overview page. The user overview page displays all registered users in the “Built-in” directory, and all active users in any directory.

### Registering Users

User principals are supported in both the “Built-in” directory and in external directories through LDAP. (For instructions on configuring an external LDAP directory, see [Configuring an External Directory Server](#).) To add a new user in the “Built-in” directory, follow these steps:

1. In the *Monitors* tab, click on the *Users* link on the sidebar.
2. Click the *Add User* button.
3. Select the “Built-in” directory, enter a username, and click *Add*.
4. The user will be created and the user details page will automatically be displayed.
5. User attributes may be set by clicking on the edit icon that appears when hovering over the associated field.
6. To enable a password on the user, follow the instructions for updating user passwords below.

### Updating User Passwords

To update passwords on user principals, follow the steps below:

1. In the *Monitors* tab, click on the *Users* link on the sidebar.
2. Navigate to the User Details page by clicking on the username.
3. Click the *Change Password* button.
4. To set or change the password, enter the new password twice and click *Change Password*.
5. To disable password access for the account, click the *Clear Password* button.

## Managing Locations

Locations identify a port on a switch where one or more hosts can connect. Locations are part of a switch and may not be added or removed.

By default, locations are named using the format <switch name>:<port name>. Locations may be renamed from the Location Details page by following the steps below:

1. In the *Monitors* tab, click on the *Locations* link on the sidebar.

2. Navigate to the location details page by clicking on the location name.
3. Click the edit icon that appears when hovering over the location name attribute to activate the edit dialog.
4. Enter the new name and press enter.

[Help Top](#) | [Return to Policy Manager](#) »

contact: [support@nicira.com](mailto:support@nicira.com)

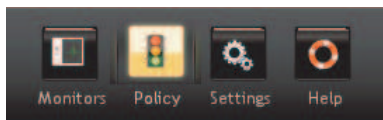
© Copyright 201

[Help Top](#) | [Return to Policy Manager](#) »

## Defining Network Policies

### Overview

Network policies are created and modified in the Policy section of the Policy Manager application. To reach the policy section, click on the Policy icon in the navigation bar at the top of the application:



Policy rules are split into two sub-pages, *System Policy* and *Site Policy*. Generally, System Policy rules are fundamental to the operation of the system, while Site Policy rules are customizations implementing behavior unique to a particular site. All System Policy rules are evaluated before Site Policy rules, so System Policy rules will take precedence during operation.

A default policy is provided with the system. In many cases, the behavior of this policy can be adjusted to match the requirements of the organization by modifying the group membership of groups over which the policy is written. When the default policy is not appropriate, the default rules can be edited. The mechanics of policy editing are the same for all policy pages and are covered in the next section, [Basic Policy Editing](#). The following section, [Using the Default Policy](#), gives a detailed description of the default policy and how to adjust its behavior. Finally the language in which rule specifications are written is described in the [Policy Rule Language](#) section.

### Basic Policy Editing

Both policy pages have the same format, a set of action buttons at the top of the page to manipulate the policy, and a list of rules:

#### Table O

#### Defining Policies

- [Overview](#)
- [Basic P](#)
- [Using t](#)
- [Policy](#)
- [Policy l](#)

#### Previous:

#### Principal

#### Next to

#### System C

**System Policy Rules**

Add Delete Revert Policy Commit Changes

- ▶ "Discovered" auto-authentication Protected
- ▶ Allow all broadcasts Protected
- ▶ Allow all ARP packets Protected
- ▶ Allow all DHCP Protected
- ▶ Allow DNS to DNS servers Protected
- ▶ Allow LDAP server queries from controller Protected
- ▶ Allow unrestricted access to selected servers Protected
- ▶ Deny unauthenticated hosts Protected
- ▶ Allow specified locations to connect to captive portal for user authentication Protected
- ▶ Allow specified IP subnets to connect to captive portal for user authentication
- ▶ Redirect unauthenticated users at the specified locations to the captive portal Protected
- ▶ Redirect unauthenticated users in the specified IP subnets to the captive portal
- ▶ Deny unauthenticated users in the specified IP subnet Protected
- ▶ Deny unauthenticated users at the specified locations Protected

The following action buttons are available:

#### Add

Add a new rule to the policy. The new rule will be inserted above the currently selected rule or at the top of the policy if no rule is selected.

#### Delete

Delete the currently selected rule. If no rule is selected, this button has no effect.

#### Revert Policy

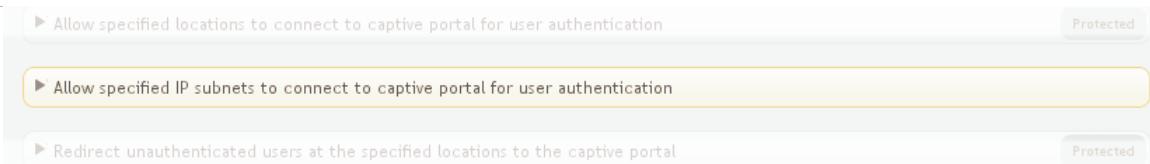
If the policy has been changed, this button discards all changes that have been made since the last commit. It is inactive otherwise.

#### Commit Changes

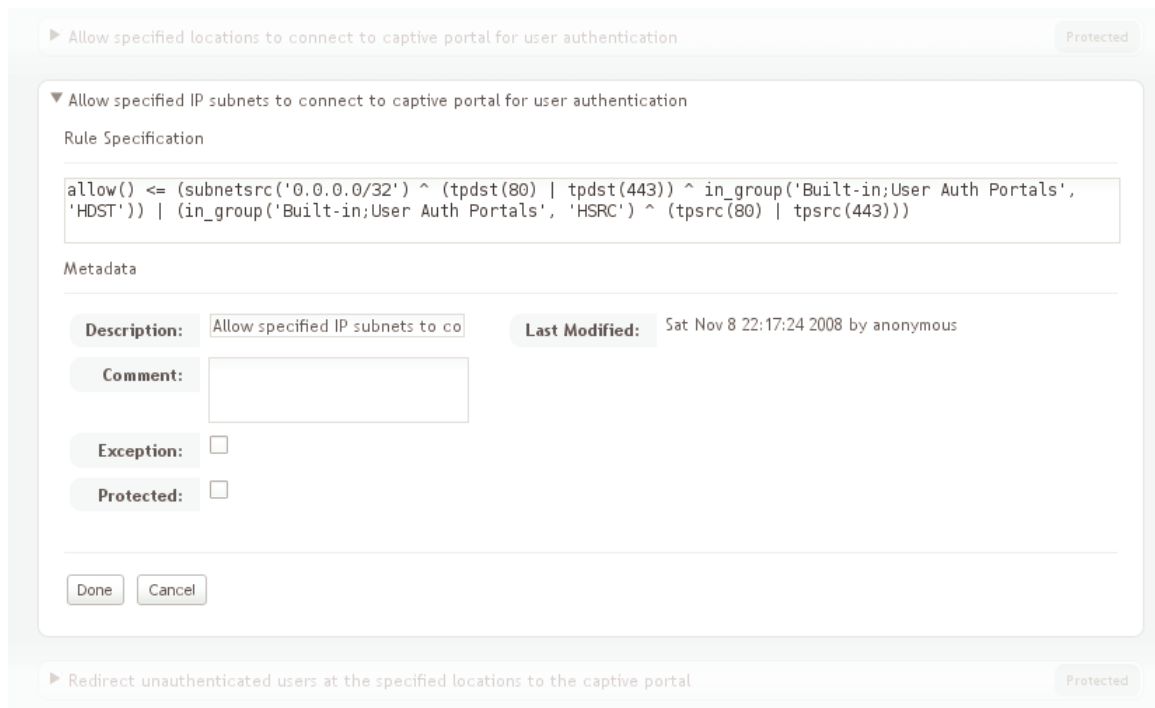
If the policy has been changed, this button commits the changes to the server and makes them active on the network. It is inactive otherwise. **Remember to commit changes before navigating to another page in the browser, or all changes will be lost.**

Policy rules are presented in an ordered list with earlier rules taking precedence over later ones. Initially all rules are shown in a collapsed form, in which only the description or specification of the rule is shown, and most other information about the rule is hidden.

To select a rule to apply one of the action buttons at the top of the screen, click on the rule. The rule will be colored orange to indicate it is the currently selected rule:



Double-clicking on a rule expands the rule so that all information about the rule can be viewed and edited:



The following fields are available in the expanded view:

#### Rule Specification

The specification of the rule in the policy rule language. This language is described in the [Policy Rule Language](#) section.

#### Description

A description of the rule. The collapsed form of the rule displays this text unless it is not specified, in which case the text from the Rule Specification field will be displayed.

#### Comment

A free-form comment that can be used to document the purpose of the rule or for any other purpose.

#### Exception

Sets the rule status to “exception”.

#### Protected

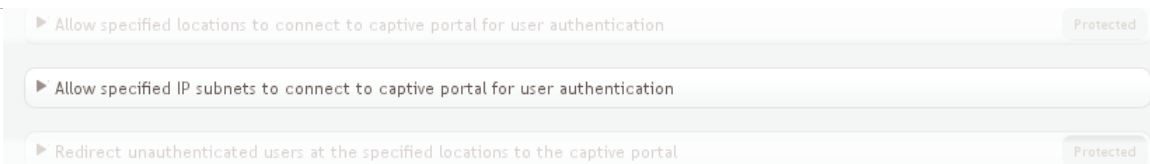
Sets the rule status as “protected”.

#### Last Modified

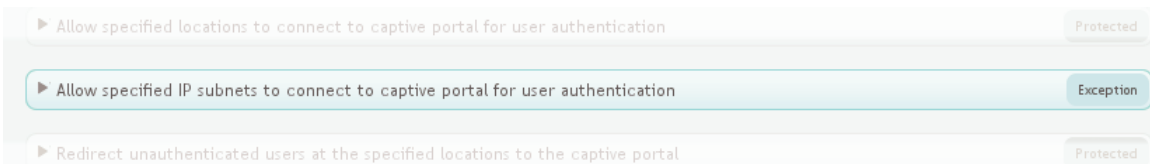
The date, time, and username of the user that last modified the rule. This is generated automatically and can not be edited.

To complete editing of a rule, left-click the “Done” button to locally save any changes that have been made or the “Cancel” button to discard them.

Selecting combinations of the “Exception” and “Protected” changes the state of the rule which in turn affects its appearance and behavior. When neither of the fields are checked, the rule is a “normal rule”. In the collapsed view, it is shown with black text and no special status “badge” on the right-hand side of the rule:



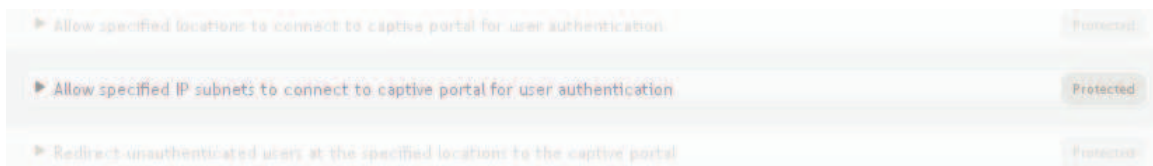
When only the “Exception” field is checked, the rule is an “exception rule”. Marking a rule in this way does not affect the rule’s behavior—it simply provides a visual reminder to operators that it may need further attention. It is shown in a light-blue color in the collapsed view of the rules with a badge indicating the rule is an exception on the right-hand side of the rule:



When only the “Protected” field is checked, it is a “protected rule”. In this state, most of the fields in the expanded form of the rule are no longer editable:



In the collapsed form, the rule description is shown in a light grey and there is a badge indicating the rule is protected on the right-hand side of the rule:



In addition to disabling changes in the expanded view, protected rules can not be selected in the collapsed view and thus can not be deleted.

When both the “Exception” and “Protected” fields are checked, the rule behaves as a protected rule.

Rules are reordered using drag-and drop. To drag a rule, click on the collapsed rule representation, keep the mouse button depressed, and drag the rule to the desired position. While dragging, a smaller version of the rule will move with the cursor to remind you of the rule you are reordering. A dashed line will indicate where the rule will be moved when it is dropped.



Remember that protected rules can not be selected, so they can not be moved by drag-and-drop either. To move a protected rule, it must first be unprotected.

## Using the Default Policy

All but one of the rules of the default policy are contained in the System Policy. This section describes each rule one by one in the order they are presented in the policy, which is also the order in which they are evaluated. Most of the rules are protected because they should not generally need modification. If modification of a rule is required, it must first be set to unprotected.

In the System Policy, the rules are:

### “Discovered” auto-authentication

Authenticates hosts by source MAC address. If the source MAC address is known, the host will be given the associated name. If the MAC address is unknown, a dynamically generated name will be used.

### Allow all broadcasts

Allow broadcast traffic. Broadcast traffic is important for address resolution and service discovery. Many hosts will not operate properly on the network if broadcasts are not allowed. If the behavior of hosts on the network is known in detail, this rule can be replaced with more restrictive rules allowing only the required broadcast traffic.

### Allow all ARP packets

ARP is the “address resolution protocol”. If this protocol is not allowed hosts will not be able to communicate on the network.

### Allow all DHCP

DHCP is the “dynamic host configuration protocol”. This is usually required for hosts to be able to dynamically obtain addresses on the network. If DHCP is not in use, the rule can be deleted.

### Allow DNS to DNS servers

DNS servers allow hosts to lookup network addresses based on more memorable names. This rule restricts DNS to known servers by requiring the DNS servers to be in the ‘Built-in;DNS Servers’ group. This group should be populated with the list of valid DNS servers.

### Allow LDAP server queries from the controller

When the policy manager is used with an external LDAP directory, it must be able to send LDAP queries and receive responses from the LDAP servers. This rule also uses groups to establish valid controllers and LDAP servers. The “Built-in;Controllers” and “Built-in;LDAP Servers” groups are used respectively.

### Allow unrestricted access to selected servers

Some servers may need unrestricted access to the network to be able to serve both authenticated and unauthenticated hosts. To give a host unrestricted access, add it to the “Built-in;Unrestricted Servers” group.

### Deny unauthenticated hosts

This rule denies all communication from hosts that have not been authenticated. Since the first rule of the default policy automatically authenticates all hosts, this should not have any effect with the default policy. However, it marks the point after which all rules can assume that the host involved has been authenticated

### Allow specified locations to connect to captive portal for user authentication

For user authentication using the captive web portal, hosts must be able to reach the captive web portal before the users are authenticated. This rule allows such communication when the host is redirected based

on its location in the network. See the associated redirect rule lower in the policy for details.

Allow specified IP subnets to connect to captive portal for user authentication

As an alternative to specifying locations from which a user must be authenticated at the user authentication portal, a set of IP subnets can be specified. See the associated redirect rule lower in the policy for details. As with the redirect rule, this rule is not protected because there is no default subnet that is valid for all networks.

Redirect unauthenticated users at the specified locations to the captive portal

Redirects HTTP to the captive portal for specific locations on the network when the user of a host is not yet authenticated. Individual locations can be specified by adding them to the “Built-in;User Auth Portal Locations” group. All ports on a switch can be specified by adding the switch to the “Built-in;User Auth Portal Switches” group. Finally, to ensure proper communication, the policy manager host(s) must be added to the “Built-in;User Auth Portals” group.

Redirect unauthenticated users in the specified IP subnets to the captive portal

As an alternative to specifying locations from which user must be authenticated at the user authentication portal a set of subnets can be specified instead. If the source address is within the subnet specified and the user has not been authenticated yet, HTTP will be redirected to the auth portal. As for the previous rule, the policy manager hosts must be specified in the “Built-in;User Auth Portals” group. This rule is not protected because there is no default subnet that will be valid for all networks. The rule should be edited to specify appropriate subnet(s). If it is not changed, it will not match any traffic.

Deny unauthenticated users in the specified IP subnet

For IP subnets where user authentication is required, this rule drops all traffic from a host that does not have an authenticated user. It relies on the groups required by the IP subnet-based redirect rule above.

Deny unauthenticated users at the specified locations

For locations where user authentication is required, this rule drops all traffic from a host that does not have an authenticated user. It relies on the groups required by the location-based redirect rule above.

In the Site Policy, the single default rule is:

Allow all traffic

This rule allows all traffic that hasn’t been denied in the System Policy. Remember that system policy rules always take precedence.

## Policy Rule Language

The rule specification for each policy rules is written in a special rule language. Each rule has the form:

*action* <= *condition*

The *action* part of a rule must be one of:

allow()

Allow matching traffic.

deny()

Deny matching traffic.

authenticate\_host()

Automatically authenticate the sending host.

http\_redirect()

Redirect matching traffic from sender to the captive web portal for user authentication. Note that the condition should limit this to unauthenticated users sending traffic over HTTP.

The *condition* part of a rule specifies the network traffic to which the *action* applies. It consists of one or more primitives matching information about the network connected by logical operators. The primitives are:

dVlan(*vlan tag*)

Flow’s vlan tag. Argument is either an integer in the range 0–4095 specifying a vlan tag, or OFF\_VLAN\_NONE to match flows without a vlan.

dSrc(*mac address*)

Source link layer address. Argument is the address as either an integer or a colon-separated string.

dDdst(*mac address*)

Destination link layer address.

*dltype(data link protocol id)*

Protocol specified in link layer header. Argument is an integer in the range 0–65535.

*nwsrc(address)*

Source network layer address. Argument is the address as either an integer or a string in the normal dotted octet format used for IP addresses.

*nwdst(address)*

Destination network layer address.

*nwproto(network protocol id)*

Protocol specified in network layer header. Argument is an integer in the range 0–255.

*subnetsrc(ip subnet)*

Subnet source IP is a member of. Argument is a CIDR subnet identifier (e.g., '192.168.1.0/24').

*subnetdst(ip subnet)*

Subnet destination IP is a member of.

*tpsrc(port number)*

Source transport port. Argument is an integer in the range 0–65535.

*tpdst(port number)*

Destination transport port.

*locsrc(location name)*

Source location name.

*locdst(location name)*

Destination location name.

*hsrc(host name)*

Source host name.

*hdst(host name)*

Destination host name.

*usrc(user name)*

Source user name.

*udst(user name)*

Destination user name.

*conn\_role(direction)*

Role unidirectional flow plays in the connection. Valid values are 'REQUEST' and 'RESPONSE'.

*protocol(protocol name)*

Convenience method for specifying *dltype*, *nwproto*, and/or transport ports using the associated common protocol name. Currently accepted protocol names are: arp, ipv4, tcp, udp, icmp, ipv4\_icmp, ipv4\_tcp, ipv4\_udp, http, dhcpc, dhcps, dhcp6c, dhcp6s, tcp\_http, ipv4\_tcp\_http, ssh, dns.

*in\_group(group specification, primitive)*

Check whether the flow attribute specified as *primitive* (chosen from the above primitive types with the name in all capitalized letters and no argument in parenthesis) is included in the group specified by *group specification*, which can consist of either a name for a group specified elsewhere or a list of values valid as arguments to the specified primitive type, enclosed in square brackets and separated by commas.

Note that all arguments to primitives—with the exception of plain integers—must be quoted (e.g., *nwsrc*("192.168.1.10") and *tpdst*(80)).

The logical operators are specified on conditions consisting of any of the above primitives or further nested logical expressions. They are in order from highest to lowest precedence:

*~ condition*

Evaluate the logical negation of the specified condition.

*condition1 ^ condition2*

Evaluate the logical AND of two conditions.

*condition1* | *condition2*

Evaluate the logical OR of two conditions.

Operators group from left to right. Parentheses can be used in the expected way to affect grouping and precedence of matching.

[Help Top](#) | [Return to Policy Manager](#) »

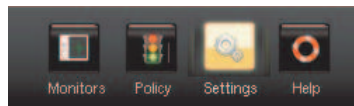
contact: [support@nicira.com](mailto:support@nicira.com)

© Copyright 201

[Help Top](#) | [Return to Policy Manager](#) »

## System Configuration

General system configuration options can be reached from the settings icons on the top pane.



The following subsections describe common configuration tasks.

### Web Interface Settings

It is possible to change the TCP ports used by the Policy Manager's web interface as well as the SSL certificate. These configuration options are available in the *Settings* section under the *Policy Controller* link.

We strongly suggest that the self-signed certificate be replaced with a valid root-signed certificate as soon as possible as this is also used by the captive web portal.

### Configuring DHCP

The Policy Manager can function as a DHCP server. The configuration options for the DHCP server can be found by clicking on the *Settings* tab, and then the *DHCP* link on the left side bar. The DHCP server is not enabled by default. To enable it, you must add at least one IP subnet to the DHCP lease pool under the *Subnets* section.

### General Configuration

General DHCP configuration parameters can be entered under the *General Options* heading. These include the default and maximum DHCP lease times, and the default DNS server to return to DHCP clients. To edit the fields, simply double click on the field values. Note that to save changed you **must** click on the *Commit Changed* button. Failure to do this will result in the loss of all entered data if you navigate away from the page.

### Per Subnet Configuration

The DHCP server can be configured to serve IPs from multiple IP subnet pools. Each subnet may include its own gateway (Router Address), default search domain (Domain Name), and DNS servers. If no DNS server is specified, the default DNS server under the general configuration options is used.

### Fixed Addresses

Fixed Addresses specify a static binding so that the same host will always receive the same IP address. Fixed addresses can only be declared over hosts that have been registered at the Policy Manager.

### Configuring the Captive Web Portal

The captive web portal is used for HTTP-based user authentication (see [Defining Network Policies](#) for instructions on configuring the Policy Manager to redirect unauthenticated users to the captive web portal). To configure the appearance of the login page and the duration of user credentials, click on the *Settings* tab, and then the *Captive Portal* link in the left side bar.

Note that on setup, it is **required** that the *Captive Portal Web Server* field be set to the DNS name or IP address of the Policy Manager.

### Configuring NAT

Any switch port can be configured to perform SNAT (Source Network Address Translation).

Under the *Monitors* tab, click on the *Switches* link and select the target switch. On the switch page, under the *Ports* heading, you will need to choose the port for which you plan to configure NAT.

To enable NAT, simply click on the *enable NAT* link under the *NAT Configuration* heading and specify the external IP address(es) to map the internal addresses to. By default, all traffic sent through the NAT port will be NAT'd, however this can be limited by IP prefix, or port number by clicking on the *limit hosts* or *limit ports* links.

#### Table O

#### System C

- [Web In Setting](#)
- [Config](#)
  - [Gene Conf](#)
  - [Per S Conf](#)
  - [Fixe](#)
- [Config Captiv](#)
- [Config](#)
- [Config Extern Server](#)
  - [Prep Dire](#)
  - [Conf Polic](#)
  - [LDAP Opti](#)

#### Previous:

[Defining Policies](#)

#### Next to:

[Switch U:](#)

In order for the changes to take effect, you must click on the *Commit Changes* button.

## Configuring an External Directory Server

The Policy Manager supports integration with an external directory server (either OpenLDAP or Active Directory) to handle user authentication.

### Preparing your Directory Server

Your directory server must support the following in order to interoperate with the policy manager:

- For group support, the directory must be configured for static group membership. This means that the schema defines group membership as an attribute on either the user object or a group object.
- Read-only search access is required for users and groups in the directory. If searching from an 'anonymous bind' is not permitted, an account for searching must be created. Create this new user with full search access to users and groups in the directory. The user must be able to perform searches with no size limit.

### Configuring the Policy Manager

The following steps describe how to configure the policy manager to use an external directory:

1. Under the *Settings* tab, click on the *Directories* link in the left side bar.
2. Click on *Add New Directory*
3. Enter a name for the directory, select directory type of 'LDAP', and click *Add Directory*
4. Set the configuration values appropriate for your site (see LDAP Directory Options below).
5. Click *Commit Changes*.

### LDAP Directory Options

#### General Options

General options configure which features should be enabled for the directory. LDAP directories only support user and user group principals, and the 'simple\_auth' authentication type.

- *Principals Enabled* Declare policy or group membership for users in this directory, ensure the User field is set to Read-Only.
- *Authentication Types Enabled* Allow authentication for users in this directory, ensure the 'simple\_auth' check box is checked.

#### Server Options

Server options specify how to connect to the external LDAP server. General options applicable to all searches are also found in this section.

- *Server URI <Required>* The full URI to the directory server:

```
ldap[s]://<server>[:<port>]
(e.g., ldap://ldapsrvr.foo.com:389)
```

- *LDAP Version <Required>* The LDAP protocol version to use. Version 3 is highly recommended.
- *Use SSL/TLS <Required>* Encrypt communications using SSL/TLS.

Note: If the deprecated 'ldaps://' protocol is used, communication is always encrypted and this option has no effect.

- *Search Subtree <Required>* If checked, entities will be searched from the entire subtree starting from the Base DN. If unchecked, only entities at the Base DN level will be returned.
- *Follow Referrals <Required>* If checked, referrals returned from the server will automatically be resolved and followed. If unchecked, referrals will be ignored.
- *Browser User DN <Optional>* The DN of the account to bind as for performing searches. If blank, an anonymous bind will be performed.
- *Browser User Password <Optional>* The password to use for binding as the browser user. If the Browser User DN option is not specified, this option has no effect.

#### User Account Options

User account options specify where and how user accounts are defined in the external directory. Many fields are optional, and are only used to display supplementary information in the Policy Manager.

- **User Base DN <Required>** The base DN for performing user account searches.
- **Username Field <Required>** The username attribute on the user entry:

```
Active Directory: sAMAccountName
POSIX: uid
```

- **User Lookup Filter <Optional>** An optional search filter to use when looking up user entries for a provided username. The string `%{username}` will be substituted with the username being searched for:

```
Active Directory example matching either username or email:
(|(sAMAccountName=%{username})(mail=%{username}))
```

If no lookup filter is provided, the following filter is used when looking up users:

```
(<username field>=%{username})
```

- **User Search Filter <Optional>** An optional search filter to append to user entry searches. If provided, the search filter for looking up users will be of the form:

```
(&(<user lookup filter>(<user search filter>))
(e.g., Active Directory: objectClass=person)
```

- **Real Name Field <Optional>** The user real name attribute on the user entry:

```
Active Directory: cn
POSIX: cn
```

- **UID Field <Optional>** The user id (UID) attribute on the user entry:

```
Active Directory:
POSIX: uidNumber
```

- **Phone Field <Optional>** The phone number attribute on the user entry:

```
Active Directory: telephoneNumber
POSIX:
```

- **Email Field <Optional>** The email attribute on the user entry:

```
Active Directory: mail
POSIX: mail
```

- **Location Field <Optional>** The location attribute on the user entry:

```
Active Directory: streetAddress
POSIX:
```

- **Description Field <Optional>** The description attribute on the user entry:

```
Active Directory: description
POSIX: gecos
```

### User Group Options

User group options specify where and how user groups are defined in the external directory. If the Group Base DN option is not specified, user group support will not be enabled on the directory.

- **User Entity Group Attribute <Optional>** The user group attribute on the user entry. Use this option if a user's groups are specified on the user entry:

```
Active Directory: memberOf
(Note: In some schemas, such as Active Directory, groups can be
configured using either the User Entity Group Attribute option or
the Group Base DN option.)
```

- **Group Base DN <Optional>** The Base DN for performing user group searches:

```
(Note: In some schemas, such as Active Directory, groups can be
configured using either the User Entity Group Attribute option or
```

the Group Base DN option.)

- *Group Name Field* <Optional> The group name attribute on the group entry.
- *Group Search Filter* <Optional> An optional search filter to append to user group entity searches. If provided, the search filter for looking up users will be:

```
(&(<group name field>=<group name to look for>)(<group search filter>))  
(e.g., Active Directory: objectClass=group)
```

- *Group Description Field* <Optional> The group description attribute on the group entry.
- *Group Member Field* <Optional> The group membership attribute on the group entry.
- *Group Subgroup Field* <Optional> The subgroup membership attribute on the group entry.
- *Group POSIX Mode* <Optional> If checked, group membership is associated by username. If a 'gidNumber' attribute exists on a user entity, POSIX mode also uses it to associate group membership. If unchecked, group membership is associated by user entry DN, and gidNumber attributes are ignored.

[Help Top](#) | [Return to Policy Manager](#) »

contact: [support@nicira.com](mailto:support@nicira.com)

© Copyright 201

[Help Top](#) | [Return to Policy Manager](#) »

## Switch User Interface

Network switches supplied by Nicira have a user interface that may be used to monitor network behavior and configure certain settings. The user interface to these switches consists of a 16-column, 2-row LCD text display and four buttons, labeled ▲, ▼, ESC, and ENTER, respectively. For easier input, a keyboard may be plugged in to one of the switch's USB ports.

### Information Screen

In ordinary operation, the switch user interface automatically cycles through a series of screens that display information of general interest, such as the switch's host name, the number of flows currently active on the switch, and the amount of traffic passing through the switch. The ▲ and ▼ buttons may be used to manually select a particular screen. Pressing ENTER stops the automatic cycling behavior, freezing the user interface at the current screen for 60 seconds.

### Switch Main Menu

From any of the monitoring screens, pressing ESC brings up a menu with one item per line. The currently selected menu item is indicated by ► at the start of a line. In the menu, the ▲ and ▼ buttons may be used to select an item, ENTER selects the current item, and ESC exits the menu without making a selection.

The menu contains the following items:

#### Exit

Exits the menu without taking any action.

#### Show Version

Displays the version number of the switch software.

#### Configure

Allows the user to change basic switch settings (see below).

After interaction with the menu is complete, the switch returns to the information screen.

## Switch Configuration

Basic switch settings may be configured through the switch UI by selecting Configure from the main menu. This brings up a secondary menu that displays a number of settings, one per screen:

#### Exit

This exits the configuration menu (see below).

#### Mode

May be set to Discovery or In-Band. Select Discovery only if an OpenFlow switch-aware DHCP server is configured in your network.

When Discovery is selected, the remaining settings are disabled, because discovery will automatically select the correct values.

#### Switch IP

The IP address to be used by the switch (e.g. 192.168.0.2).

Changing the switch IP address also changes the switch netmask and gateway (see below) to their most common values.

#### Switch Netmask

The netmask of the switch's local IP network (e.g. 255.255.255.0).

#### Switch Gateway

The IP address of the gateway between the local IP network and external networks (e.g. 192.168.0.1).

#### Controller

NOX's location, in the form TYPE:IP[:PORT], where TYPE is one of the literal strings tcp or ssl, IP is an IP address, and the optional PORT is a TCP port number between 1 and 65535.

#### Table O

#### Switch U:

- Inform
- Switch
- Switch

#### Previou:

#### System C

To change a setting, select it with ▲ and ▼ and push ENTER. The ▲ and ▼ buttons may then be used to cycle individual characters of a setting through the valid values, ENTER to accept the current selection, and ESC to back up. If a USB keyboard is plugged in, then the new setting may be typed directly. After the setting's value is complete, push ENTER when ↵ is displayed to accept the new value. To cancel changes, push ESC repeatedly.

When configuration is complete, push ESC from the menu of settings (or select Exit and push ENTER). At the Save Changes? prompt, select Yes or No with ▲ and ▼ (or by pushing Y or N on an attached USB keyboard) and push ENTER. If Yes is selected, the changes take effect immediately.

[Help Top](#) | [Return to Policy Manager](#) »

contact: [support@nicira.com](mailto:support@nicira.com)

© Copyright 201